ASA 8.X e mais tarde: Adicionar ou altere uma lista de acessos com o exemplo da configuração GUI ASDM

Índice

Introdução

Este documento explica como usar o Cisco Adaptive Security Device Manager (ASDM) a fim trabalhar com listas de controle de acesso. Isto inclui a criação de uma lista de acessos nova, como editar uma lista de acesso existente e outras funcionalidades com as Listas de acesso.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Ferramenta de segurança adaptável de Cisco (ASA) com versão 8.2.X
- Cisco Adaptive Security Device Manager (ASDM) com versão 6.3.X

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.

Informações de Apoio

As Listas de acesso são usadas primeiramente para controlar o tráfego correm através do Firewall. Você pode permitir ou negar tipos de tráfego específicos com Listas de acesso. Cada lista de acessos contém um número de entradas de lista de acesso (ACE) esse controle o fluxo de tráfego de uma fonte específica a um destino específico. Normalmente, esta lista de acessos é limitada a uma relação para notificar o sentido do fluxo em que deve olhar. As Listas de acesso são categorizadas principalmente em dois tipos largos.

1. Listas de acessos de entrada
2. Lista de acesso externo

As listas de acessos de entrada aplicam-se ao tráfego que incorpora essa relação, e as lista de acesso externo aplicam-se ao tráfego que retira a relação. Notação de entrada/de partida refere à direção de tráfego em termos dessa relação mas não o movimento do tráfego no meio mais altamente e das interfaces de segurança mais baixa.

Para o TCP e as conexões de UDP, você não precisa uma lista de acessos de reservar retornar o tráfego porque a ferramenta de segurança permite todo o tráfego de retorno para conexões bidirecional estabelecidas. Para protocolos sem conexão tais como o ICMP, a ferramenta de segurança estabelece sessões unidirecionais, assim que você precisa-o Listas de acesso de aplicar Listas de acesso à fonte e às interfaces de destino a fim permitir o ICMP nos ambos sentidos, ou necessidade de permitir o motor da inspeção de ICMP. O motor da inspeção de ICMP trata sessões ICMP como conexões bidirecional.

Da versão 6.3.X ASDM, há dois tipos de Listas de acesso que você pode configurar.

1. Regras do acesso da relação
2. Regras globais do acesso

Nota: A regra do acesso refere uma entrada de lista do acesso individual (ACE).

As regras do acesso da relação são limitadas a toda a relação na altura de sua criação. Sem ligá-los a uma relação, você não pode criá-los. Isto difere do exemplo da linha de comando. Com CLI, você cria primeiramente a lista de acessos com o **comando de lista de acesso**, e liga então esta lista de acessos a uma relação com o **comando access-group**. O ASDM 6.3 e mais atrasado, a lista de acessos é criado e limitado a uma relação como uma única tarefa. Isto aplica-se ao tráfego que corre através dessa relação específica somente.

As regras globais do acesso não são limitadas a nenhuma relação. Podem ser configurados

através do guia do gerenciador ACL no ASDM e são aplicados ao tráfego de ingresso global. São executados quando há um fósforo baseado na fonte, no destino, e no tipo de protocolo. Estas regras não replicated em cada relação, assim que salvar o espaço de memória.

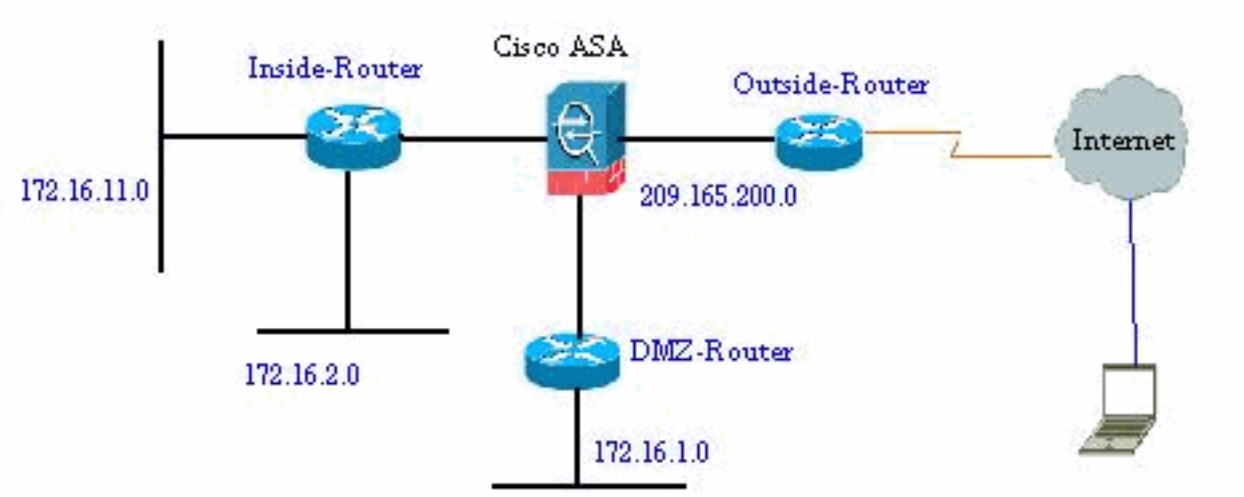
Quando ambas estas regras devem ser executada, as regras do acesso da relação tomam normalmente a precedência sobre as regras globais do acesso.

Configurar

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

Diagrama de Rede

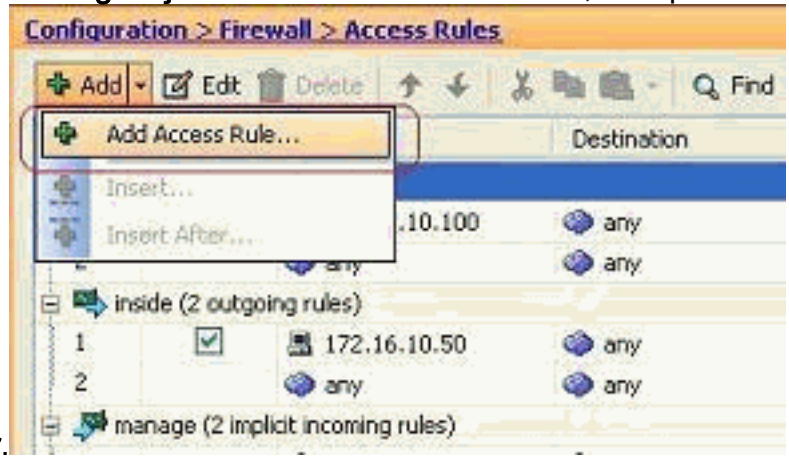
Este documento utiliza a seguinte configuração de rede:



Adicionar uma lista de acessos nova

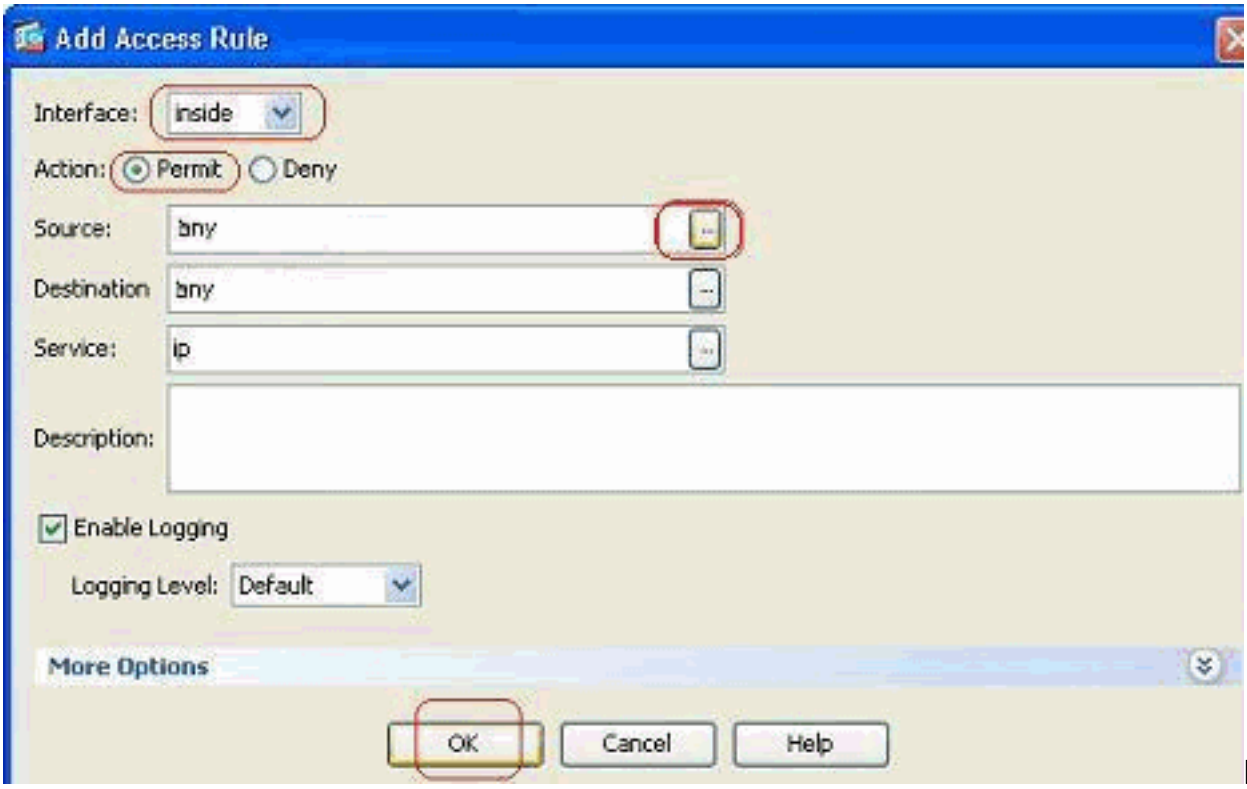
Termine estas etapas a fim criar uma lista de acessos nova com o ASDM:

1. Escolha **regras da configuração > do Firewall > do acesso**, e clique o botão da **regra do acesso adicionar**.



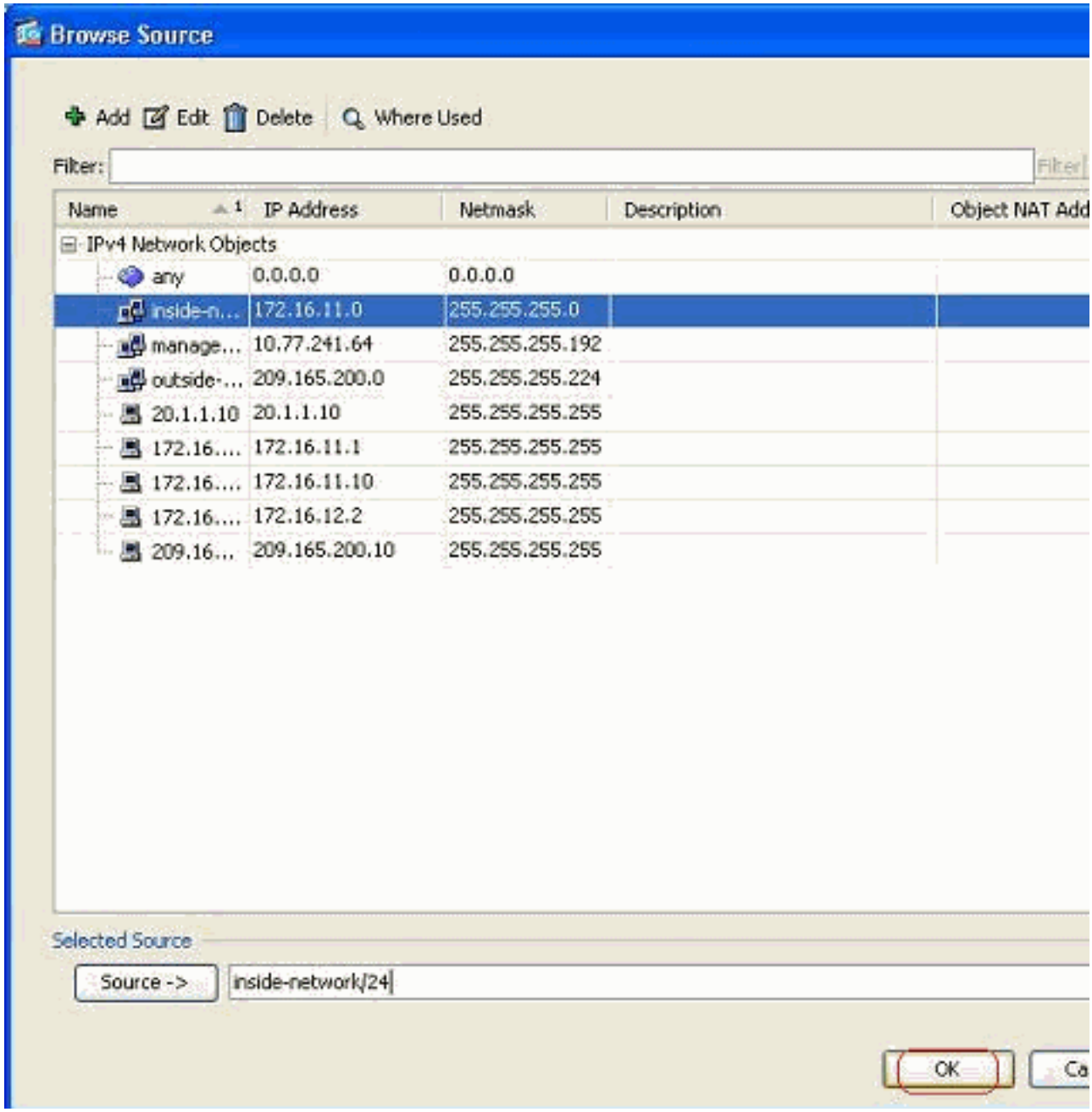
2. Escolha a relação a que esta lista de acessos tem que limitar, junto com a ação a ser executada do tráfego na licença isto é,/negue-a. Clique então o Detailsbutton a fim selecionar a rede da

fonte.

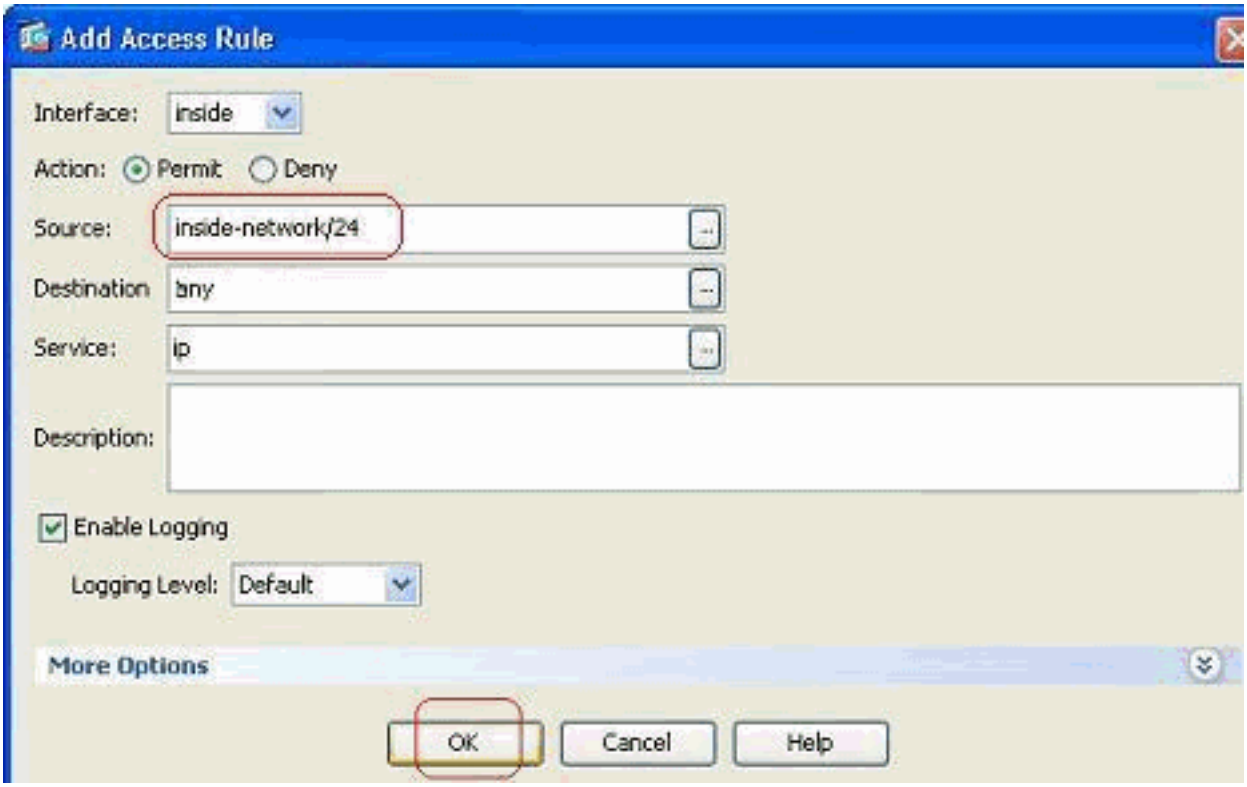


Nota: Está aqui uma explicação resumida dos campos diferentes que são mostrados neste indicador:**Relação** — Determina a relação a que esta lista de acessos é limitada.**Ação** — Determina o tipo da ação da regra nova. Duas opções estão disponíveis. **Permita** permite todo o tráfego de correspondência e **negam a** blocos todo o tráfego de correspondência.**Fonte** — Este campo especifica a fonte do tráfego. Este pode estar qualquer coisa entre um único endereço IP de Um ou Mais Servidores Cisco ICM NT, uma rede, um endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do Firewall ou um grupo de objeto de rede. Estes podem ser selecionados com o **botão Details Button**.**Destino** — Este campo especifica a fonte do tráfego. Este pode estar qualquer coisa entre um único endereço IP de Um ou Mais Servidores Cisco ICM NT, uma rede, um endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do Firewall ou um grupo de objeto de rede. Estes podem ser selecionados com o **botão Details Button**.**Serviço** — Este campo determina o protocolo ou o serviço do tráfego a que esta lista de acessos é aplicada. Você pode igualmente definir um grupo de serviço que contenha um grupo de protocolos diferentes.

3. Depois que você clica o **botão Details Button**, uma nova janela que contenha os objetos de rede existente está indicada. Selecione a **rede interna**, e clique a **APROVAÇÃO**.



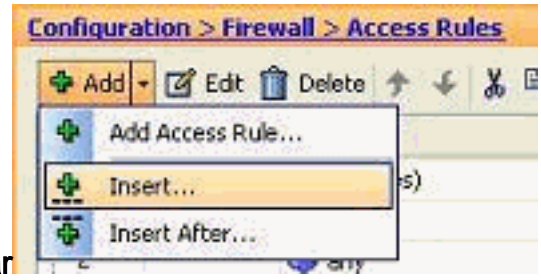
4. Você é retornado ao indicador da **regra do acesso adicionar**. Datilografe **alguns no** campo de destino. e **APROVAÇÃO do** clique a fim terminar a configuração da regra do acesso.



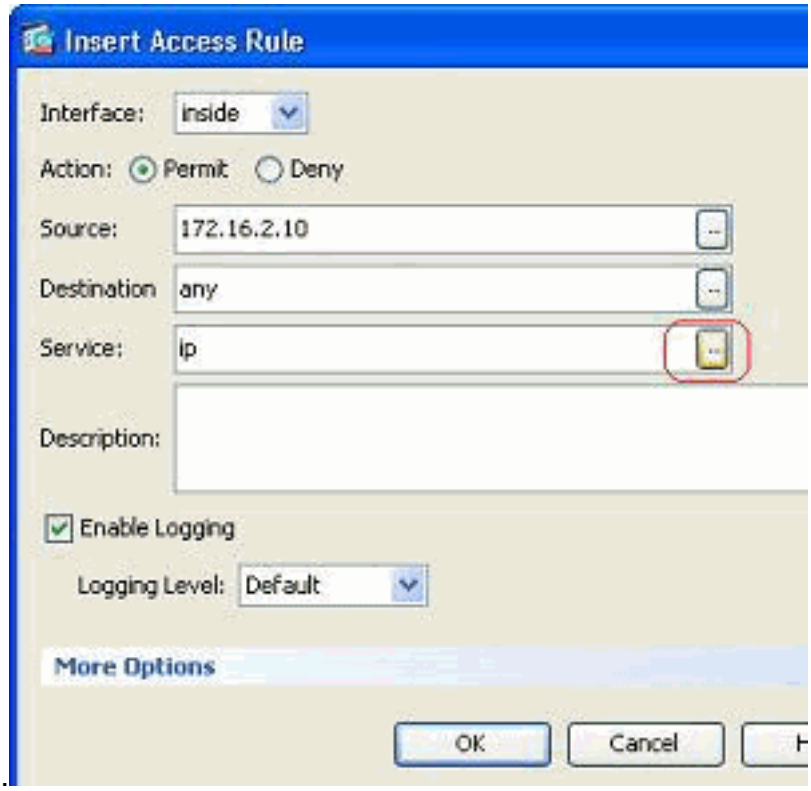
Adicionar uma regra do acesso antes de uma existente:

Termine estas etapas a fim adicionar uma regra do acesso imediatamente antes de uma regra já existente do acesso:

1. Selecione a entrada de lista de acesso existente, e clique a **inserção do** menu suspenso **adicionar**

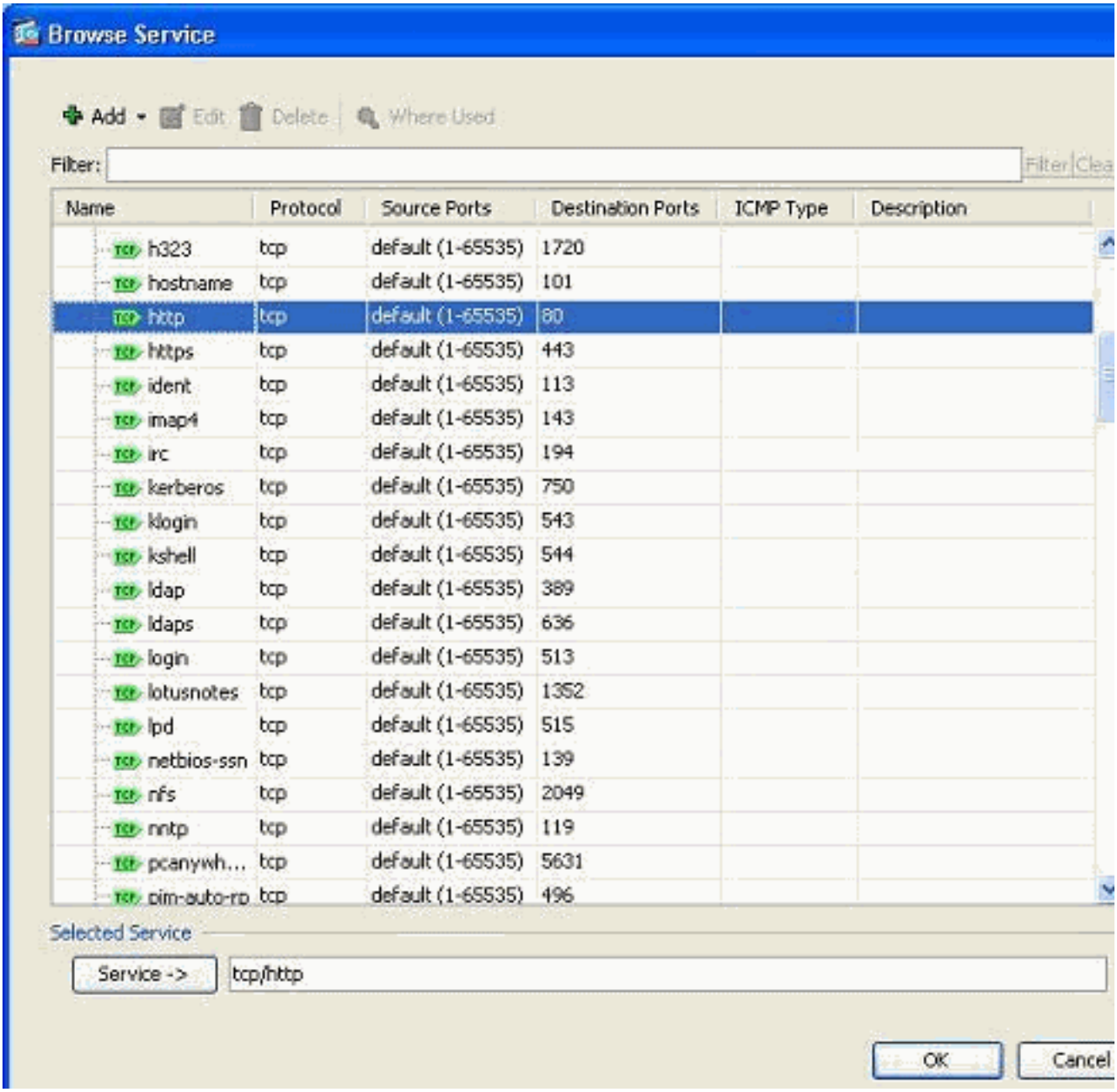


2. Escolha a fonte e o destino, e clique o **botão Details Button do** campo do serviço para



escolher o protocolo.

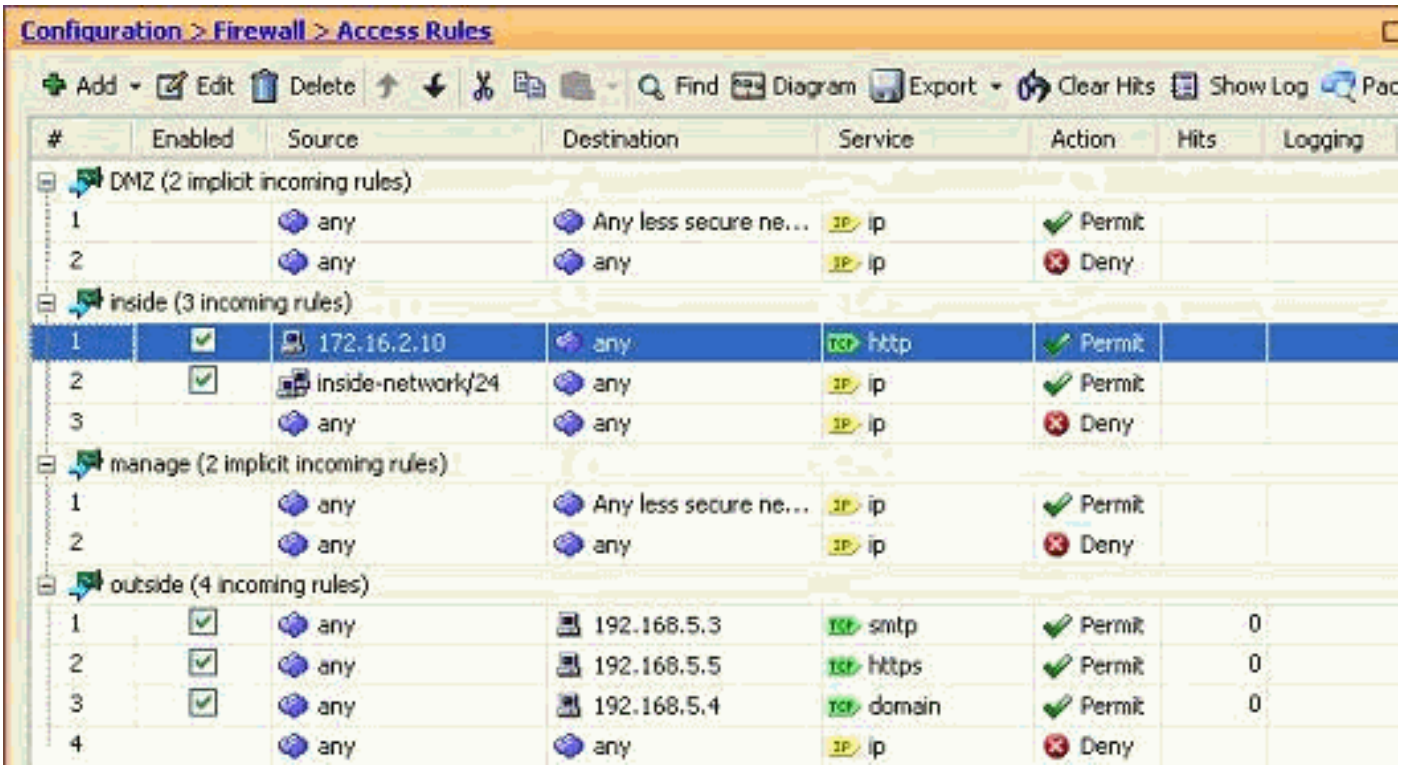
3. Escolha o HTTP o protocolo, e clique a **APROVAÇÃO**.



4. Você é retornado ao indicador da regra do acesso da inserção. O campo do serviço é enchido com o **tcp/HTTP** como o protocolo selecionado. Clique a **APROVAÇÃO** a fim terminar a configuração da entrada de lista de acesso

nova.

Você pode agora observar a regra nova do acesso mostrada imediatamente antes já da entrada existente para a rede interna.



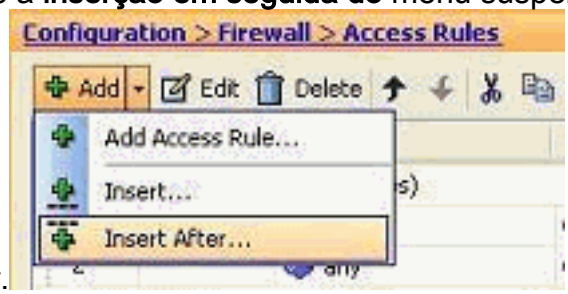
Nota: A ordem das regras do acesso é muito importante. Ao processar cada pacote para filtrar, o ASA examina se o pacote combina algum do critério de regra do acesso em um ordem sequencial e se um fósforo acontece, executa a ação dessa regra do acesso. Quando uma regra do acesso é combinada, não continua a umas regras mais adicionais do acesso e verifica-as outra vez.

Adicionar uma regra do acesso após existente:

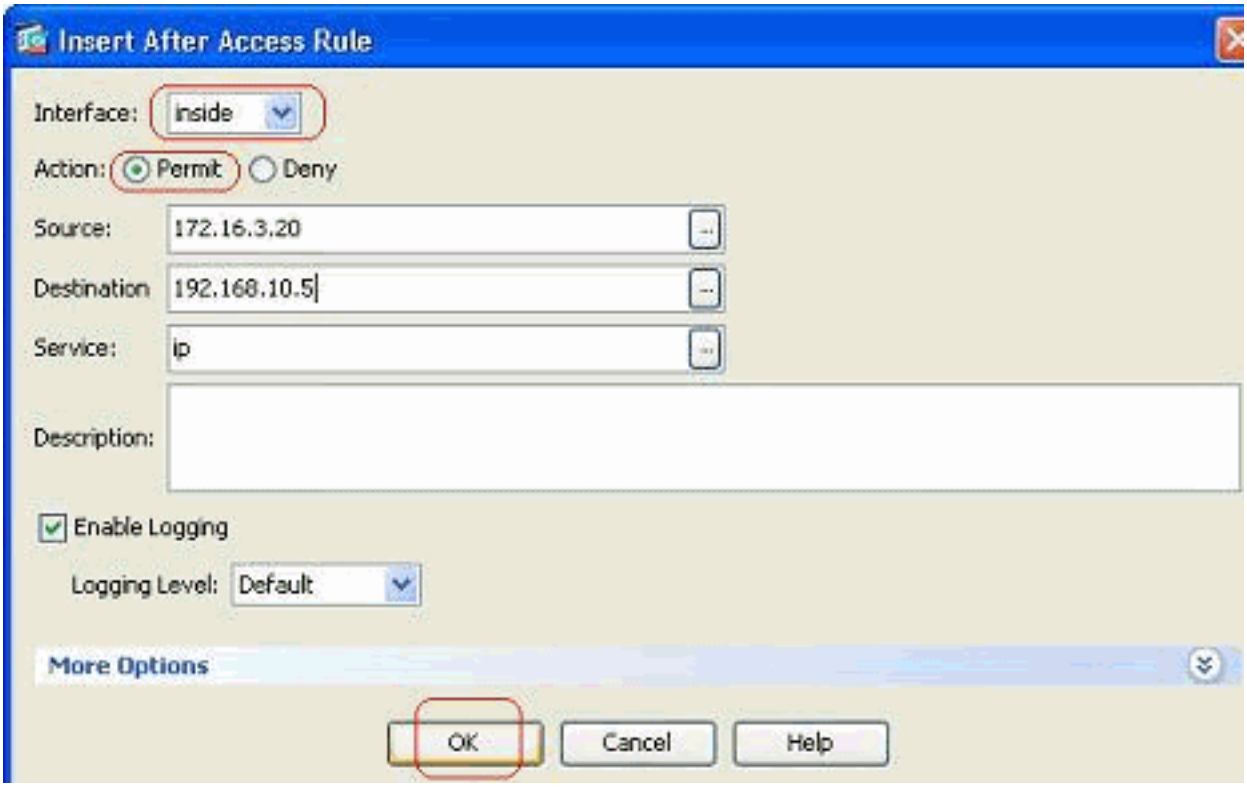
Termine estas etapas a fim criar uma regra do acesso imediatamente depois de uma regra já

existente do acesso.

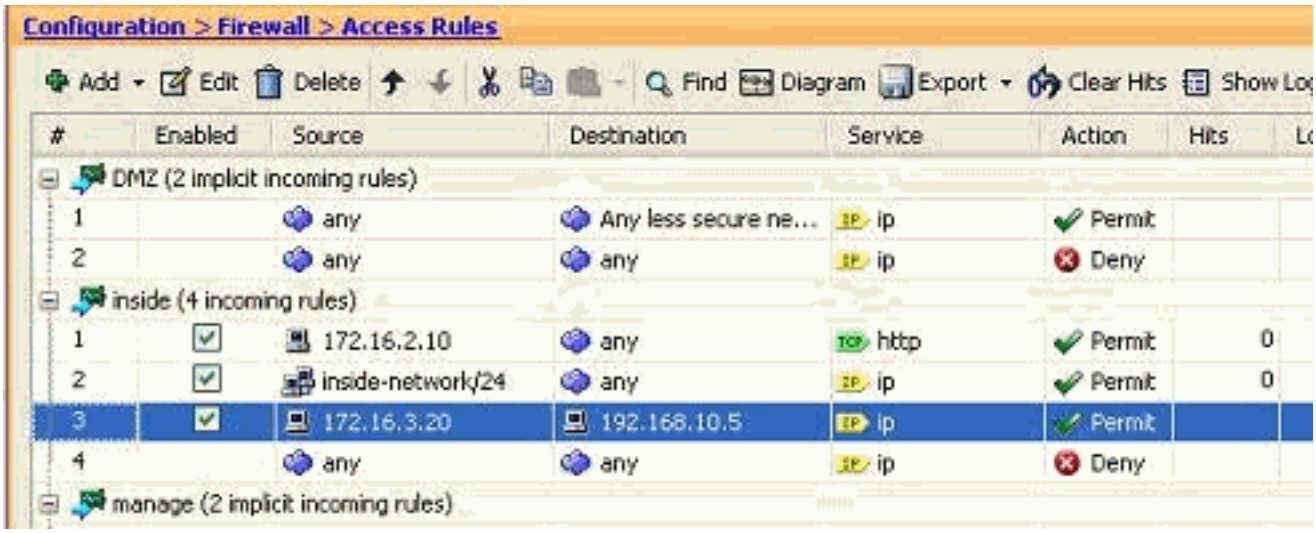
1. Selecione a regra do acesso depois do qual você precisa de ter uma regra nova do acesso, e escolhe a **inserção em seguida do** menu suspenso adicionar.



2. Especifique os campos da relação, da ação, da fonte, do destino e do serviço, e a **APROVAÇÃO do** clique para terminar a configuração esta regra do acesso.

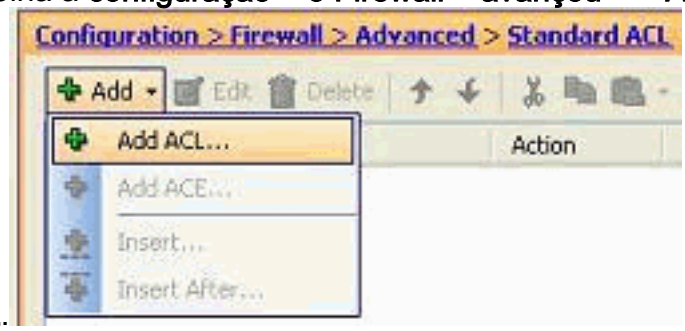


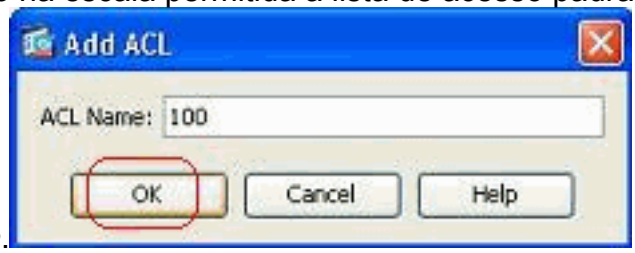
Você pode ver que recentemente a regra do acesso configurado se senta imediatamente depois que já configurada.

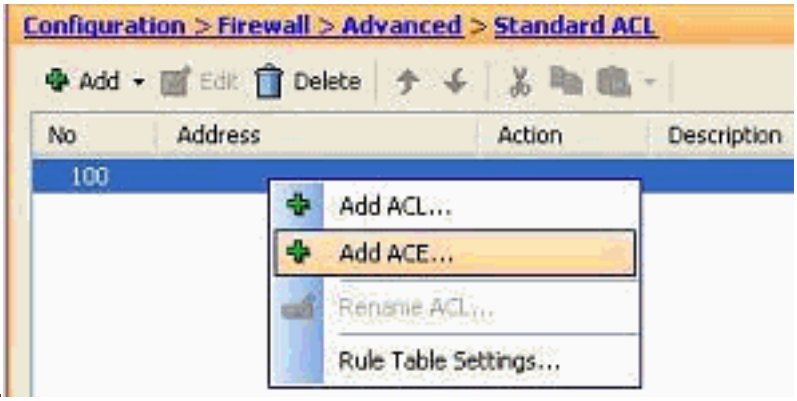


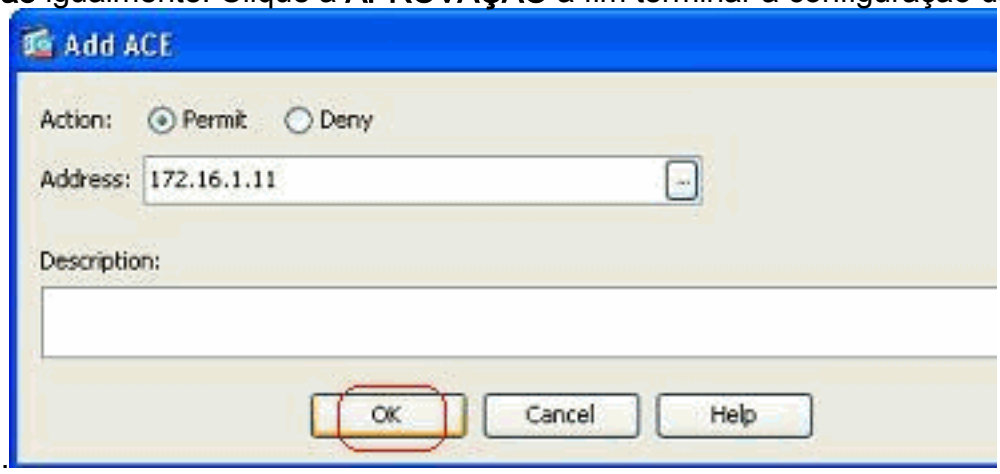
Crie uma lista de acesso padrão

Termine estas etapas a fim criar uma lista de acesso padrão com o ASDM GUI.

1. Escolha a **configuração > o Firewall > avançou > > Add padrão ACL**, e o clique **adiciona o ACL**.


2. Dê um número na escala permitida a lista de acesso padrão, e clique a **APROVAÇÃO**.


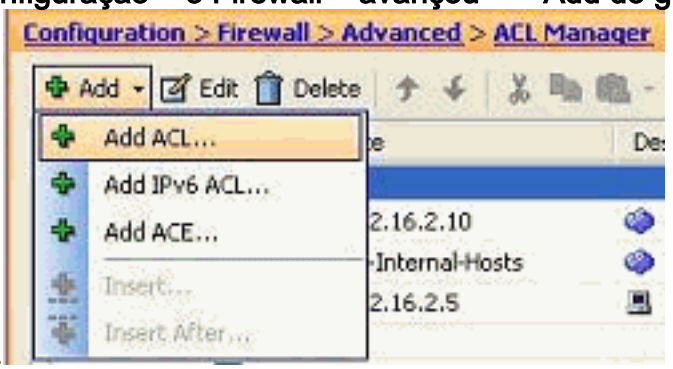
3. Clicar com o botão direito a lista de acessos, e escolha-a **adicionam o ACE** a fim adicionar uma regra do acesso a esta lista de acessos.


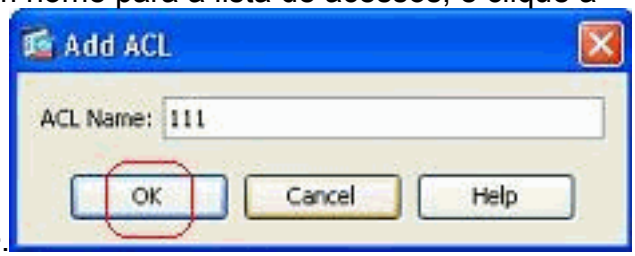
4. Selecione a **ação**, e especifique o **endereço de origem**. Se for necessário, especifique a **descrição** igualmente. Clique a **APROVAÇÃO** a fim terminar a configuração da regra do acesso.


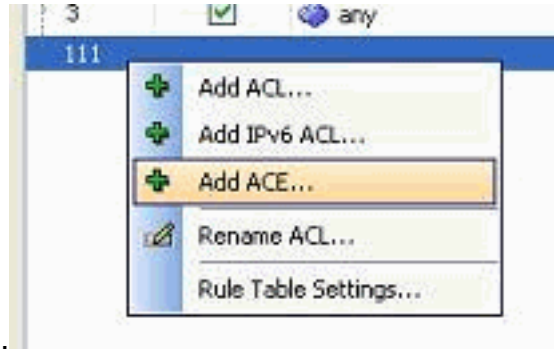
Crie uma regra global do acesso

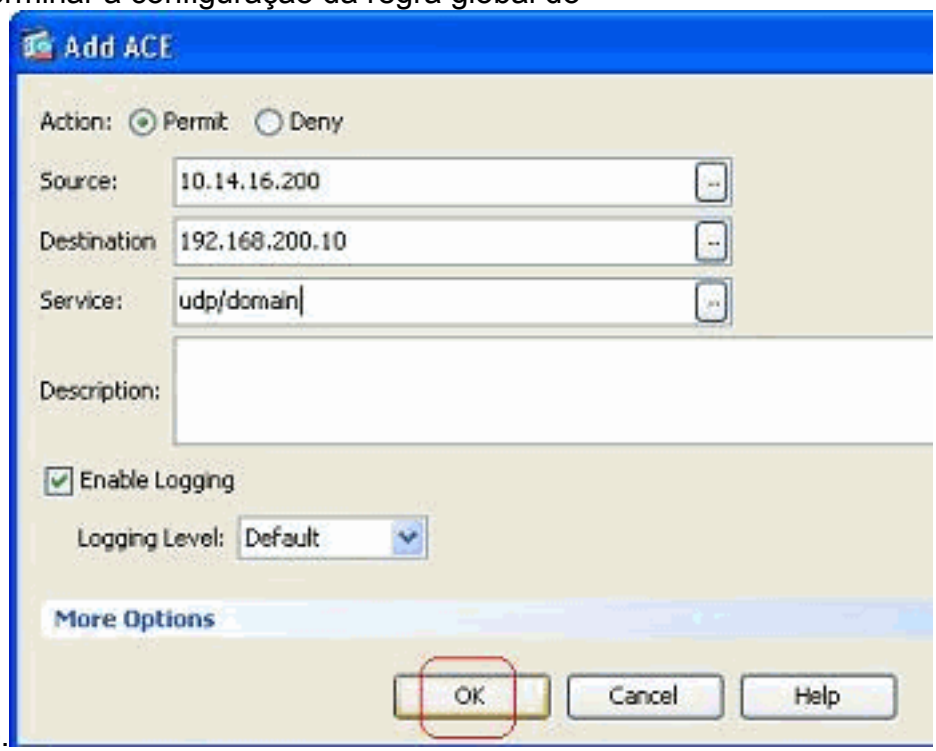
Termine estas etapas a fim criar uma lista de acesso extendida que contenha regras globais do

acesso.

1. Escolha a **configuração > o Firewall > avançou > > Add do gerente ACL**, e o clique **adiciona o** botão **ACL**.


2. Especifique um nome para a lista de acessos, e clique a **APROVAÇÃO**.


3. Clicar com o botão direito a lista de acessos, e escolha-a **adicionam o ACE** a fim adicionar uma regra do acesso a esta lista de acessos.


4. Termine os campos da ação, da fonte, do destino, e do serviço, e a **APROVAÇÃO do** clique a fim terminar a configuração da regra global do acesso.


Você pode agora ver a regra global do acesso, como mostrado.

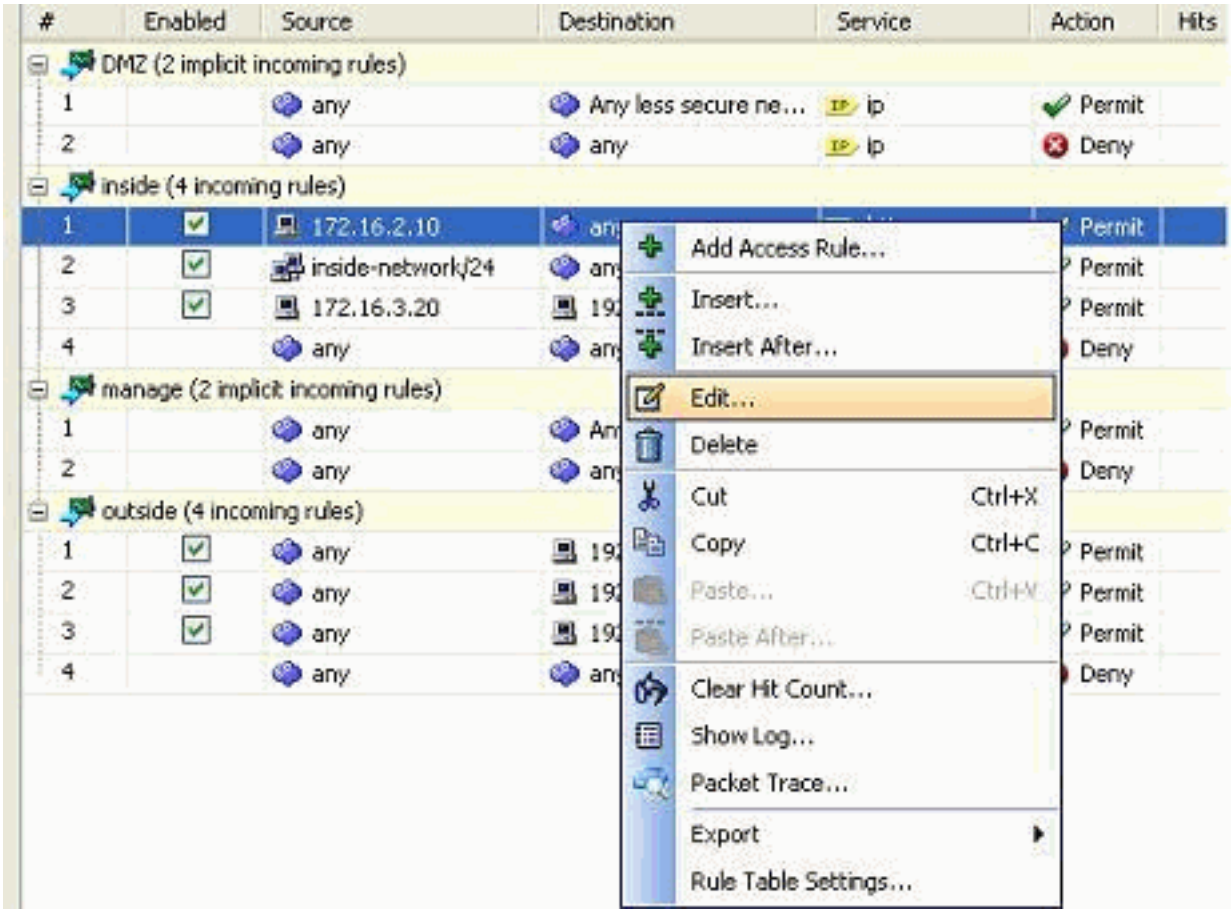
Edite uma lista de acesso existente

Esta seção discute como editar um acesso existente.

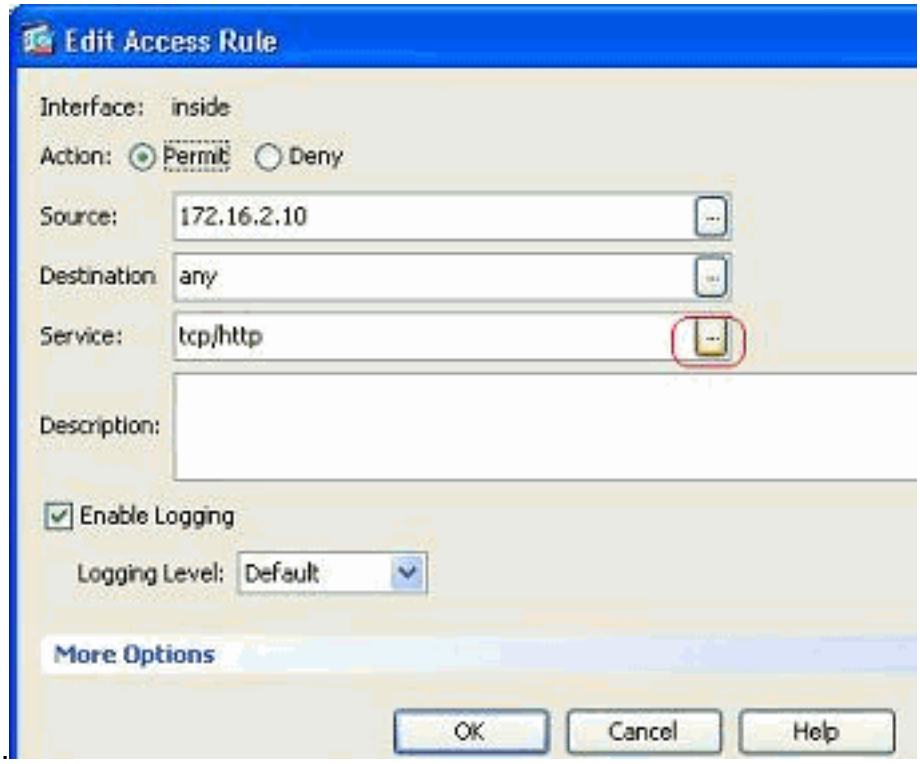
Edite o campo do protocolo para criar um grupo de serviço:

Termine estas etapas a fim criar um grupo de serviço novo.

1. Clicar com o botão direito a regra do acesso que precisa de ser alterada, e escolha-a **editam** a fim alterar essa regra específica do acesso.

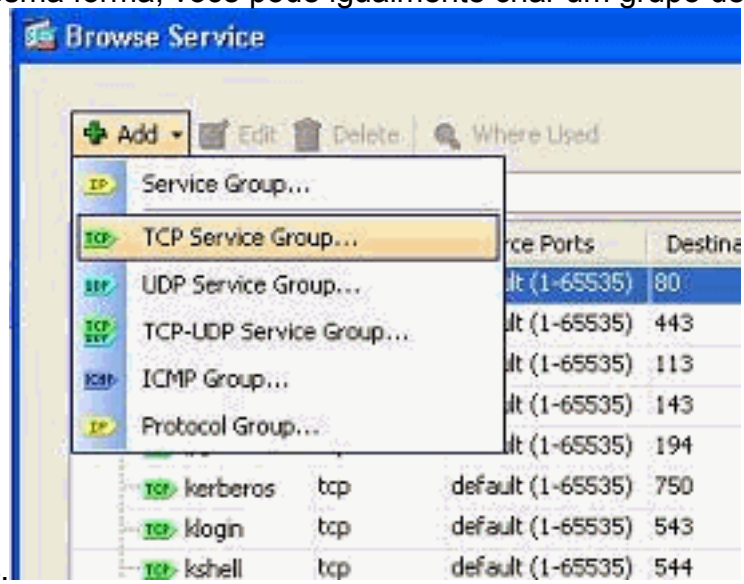


2. Clique o **botão Details Button** a fim alterar o protocolo associado com esta regra do

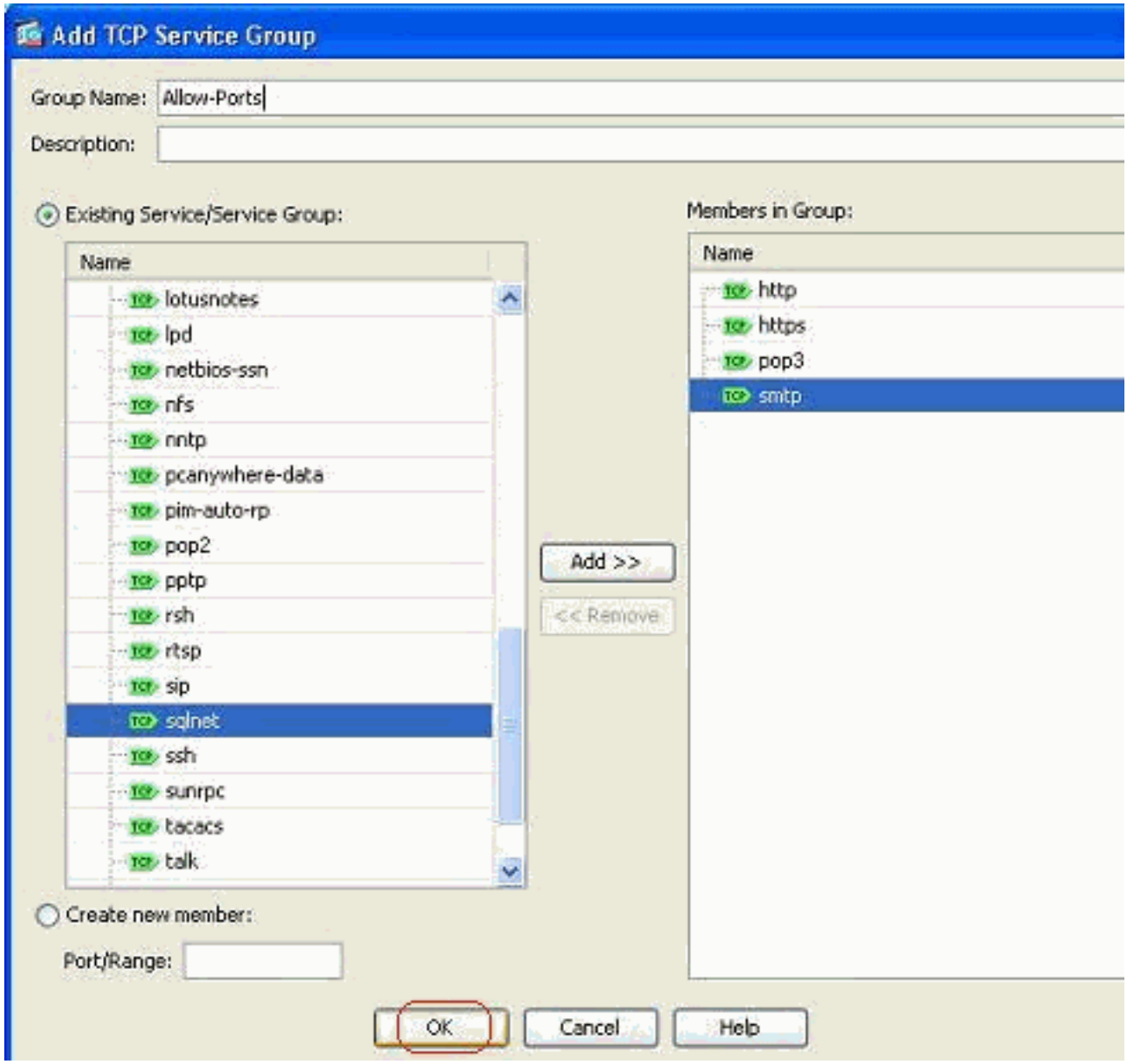


acesso.

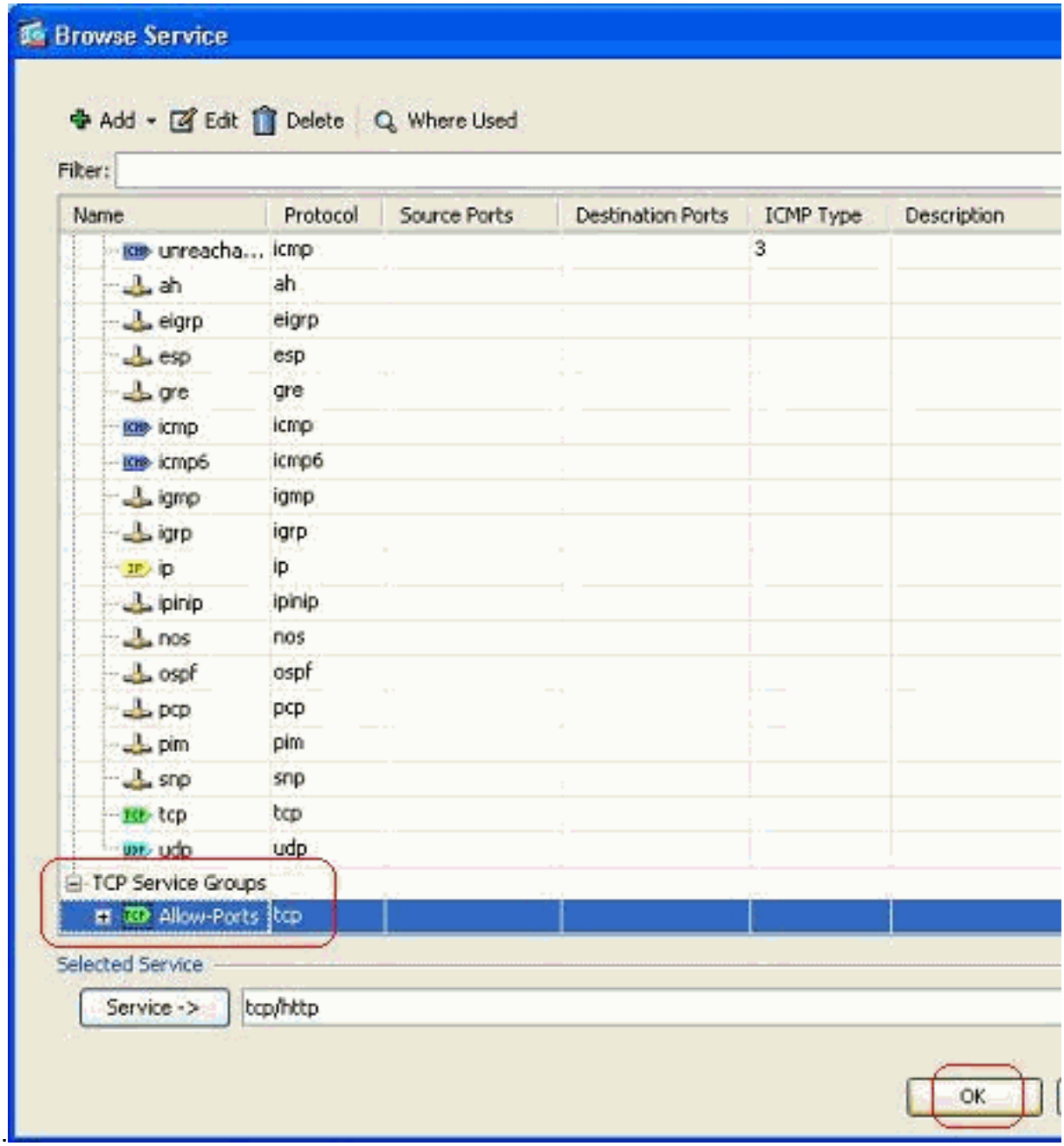
3. Você pode selecionar qualquer protocolo a não ser o HTTP se for necessário. Se há somente um único protocolo a ser selecionado, a seguir não há nenhuma necessidade de criar o grupo de serviço. É útil criar um grupo de serviço quando há uma exigência identificar os protocolos NON-adjacentes numerosos a ser combinados por esta regra do acesso.Escolha **adicionam > grupo de serviço TCP** a fim criar um grupo de serviço novo TCP.**Nota:** Da mesma forma, você pode igualmente criar um grupo de serviço novo UDP ou grupo ICMP e etc.



4. Especifique um nome para este grupo de serviço, selecione o protocolo no menu do lado esquerdo, e o clique **adiciona** a fim movê-los para os membros no menu do grupo no lado direito. Os protocolos numerosos podem ser adicionados como membros de um grupo de serviço baseado na exigência. Os protocolos são adicionados um por um. Os membros são adicionados afinal, **APROVAÇÃO do**
clique.

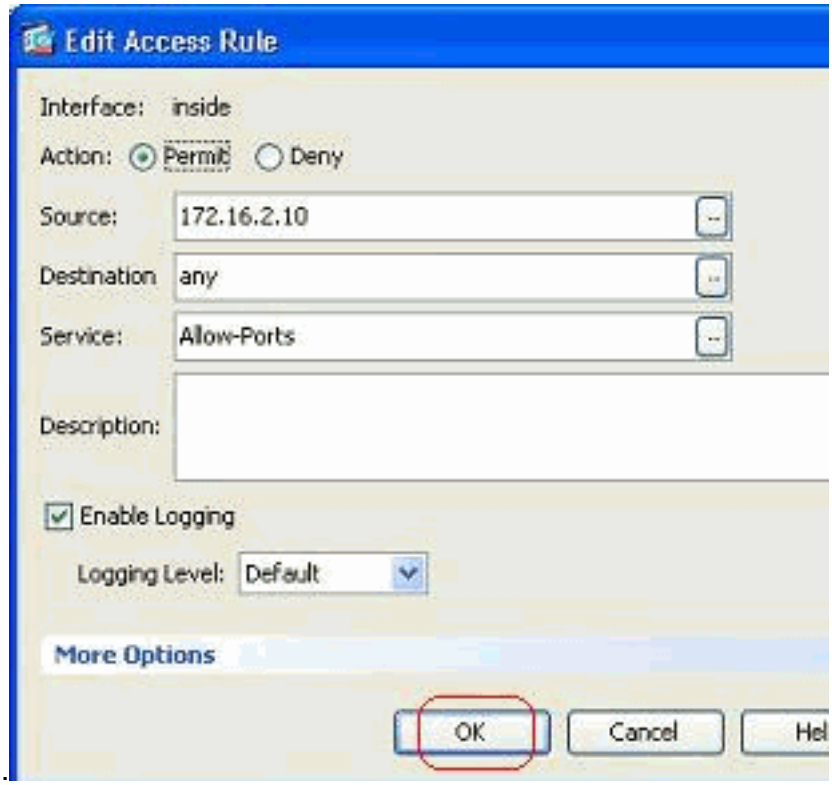


5. O grupo de serviço recém-criado pode ser visto sob os **grupos de serviço da** aba **TCP**. Clique o **botão OK** para retornar ao indicador da regra do acesso da



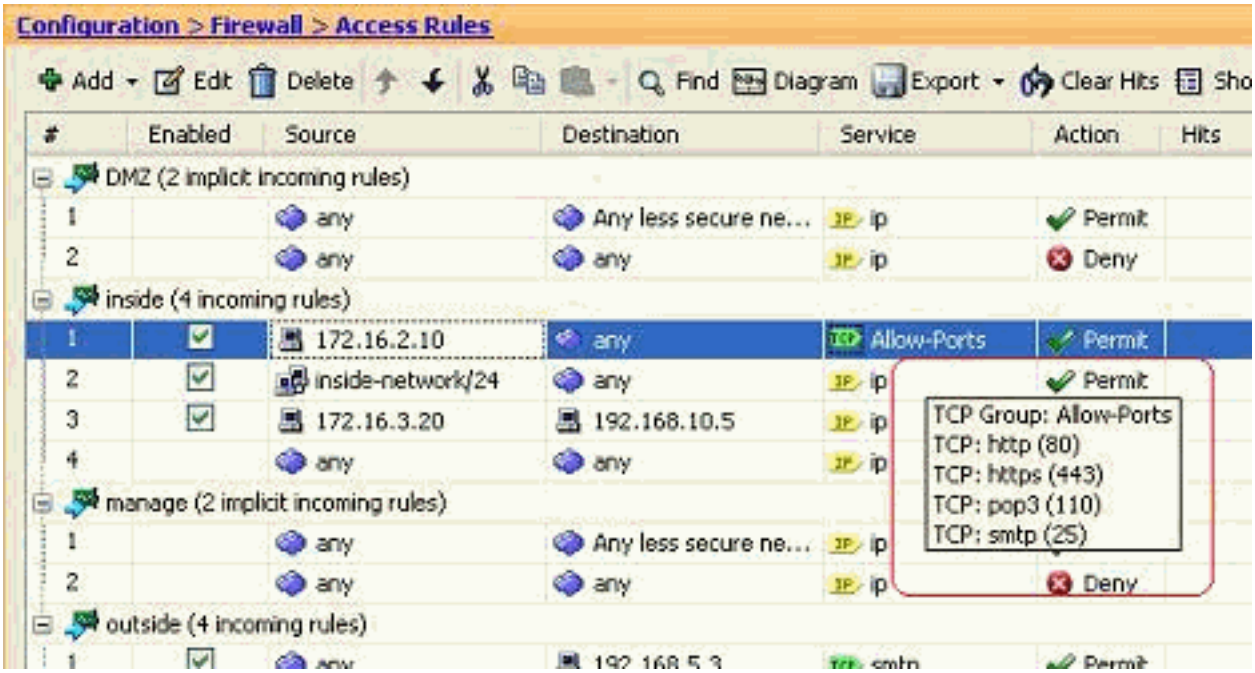
edição.

6. Você pode ver que o campo do serviço está povoado com o grupo de serviço recém-criado. **APROVAÇÃO do** clique a fim terminar a



edição.

7. Paira seu rato sobre esse grupo de serviço específico a fim ver todos os protocolos associados.

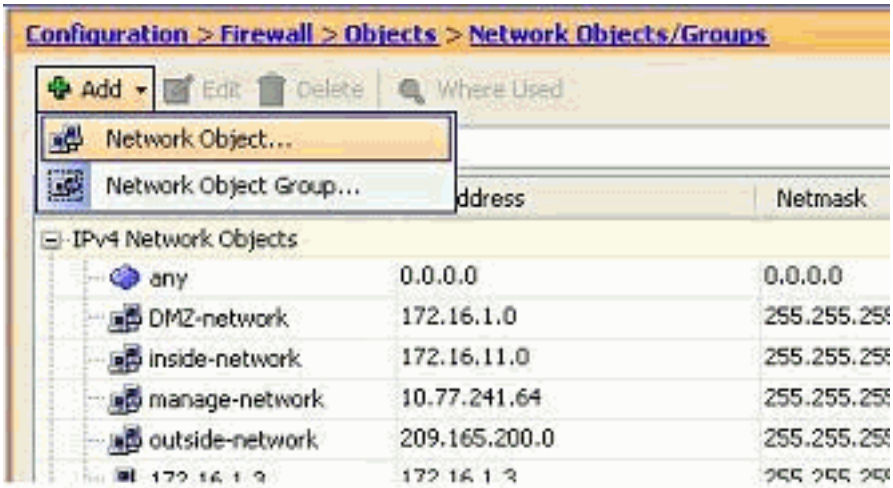


Edite a fonte/campos de destino para criar um grupo de objeto de rede:

Os grupos de objetos são usados para simplificar a criação e a manutenção das Listas de acesso. Quando você agrupa como objetos junto, você pode usar o grupo de objetos em um único ACE em vez de ter que incorporar separadamente um ACE para cada objeto. Antes que você crie o grupo de objetos, você precisa de criar os objetos. Na terminologia ASDM, o objeto é chamado objeto de rede e o grupo de objetos é chamado grupo de objeto de rede.

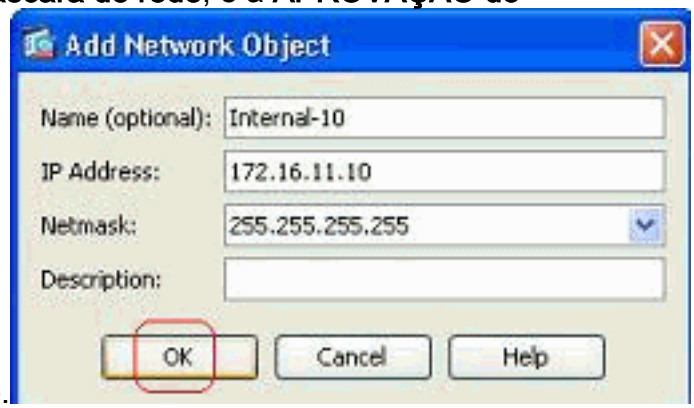
Conclua estes passos:

1. Escolha o **> Add da configuração > do Firewall > dos objetos > dos objetos de rede/grupos**, e clique o **objeto de rede** a fim criar um objeto de rede



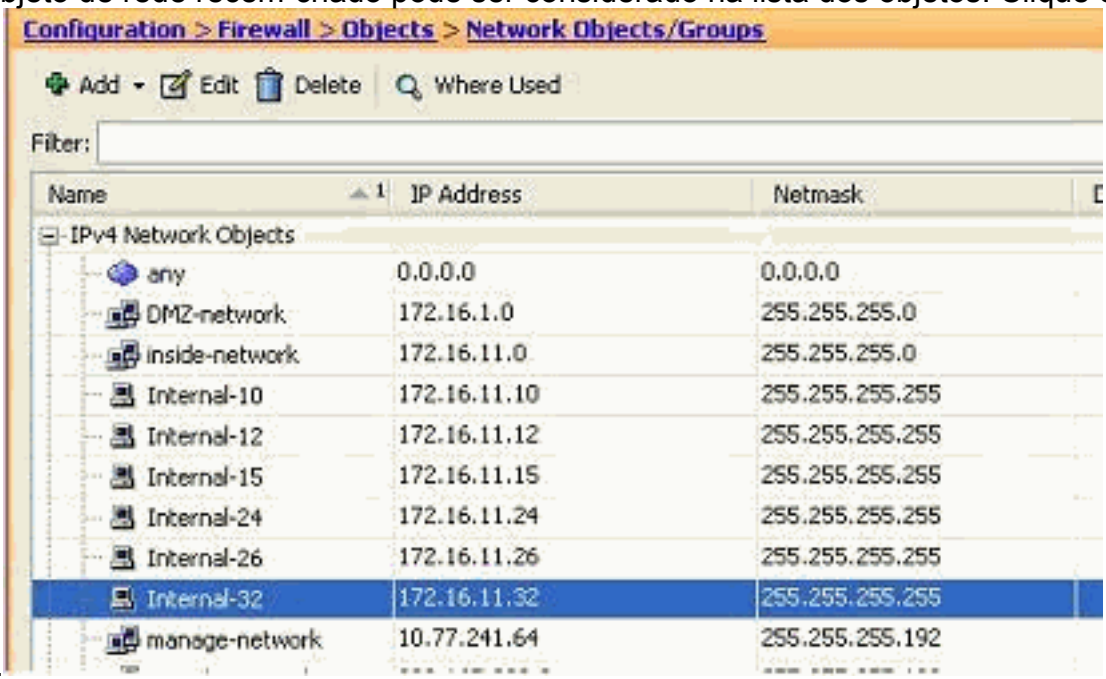
novo.

2. Preencha os campos do **nome**, do **endereço IP de Um ou Mais Servidores Cisco ICM NT** e da **Máscara de rede**, e a **APROVAÇÃO do**



clique.

3. O objeto de rede recém-criado pode ser considerado na lista dos objetos. Clique em

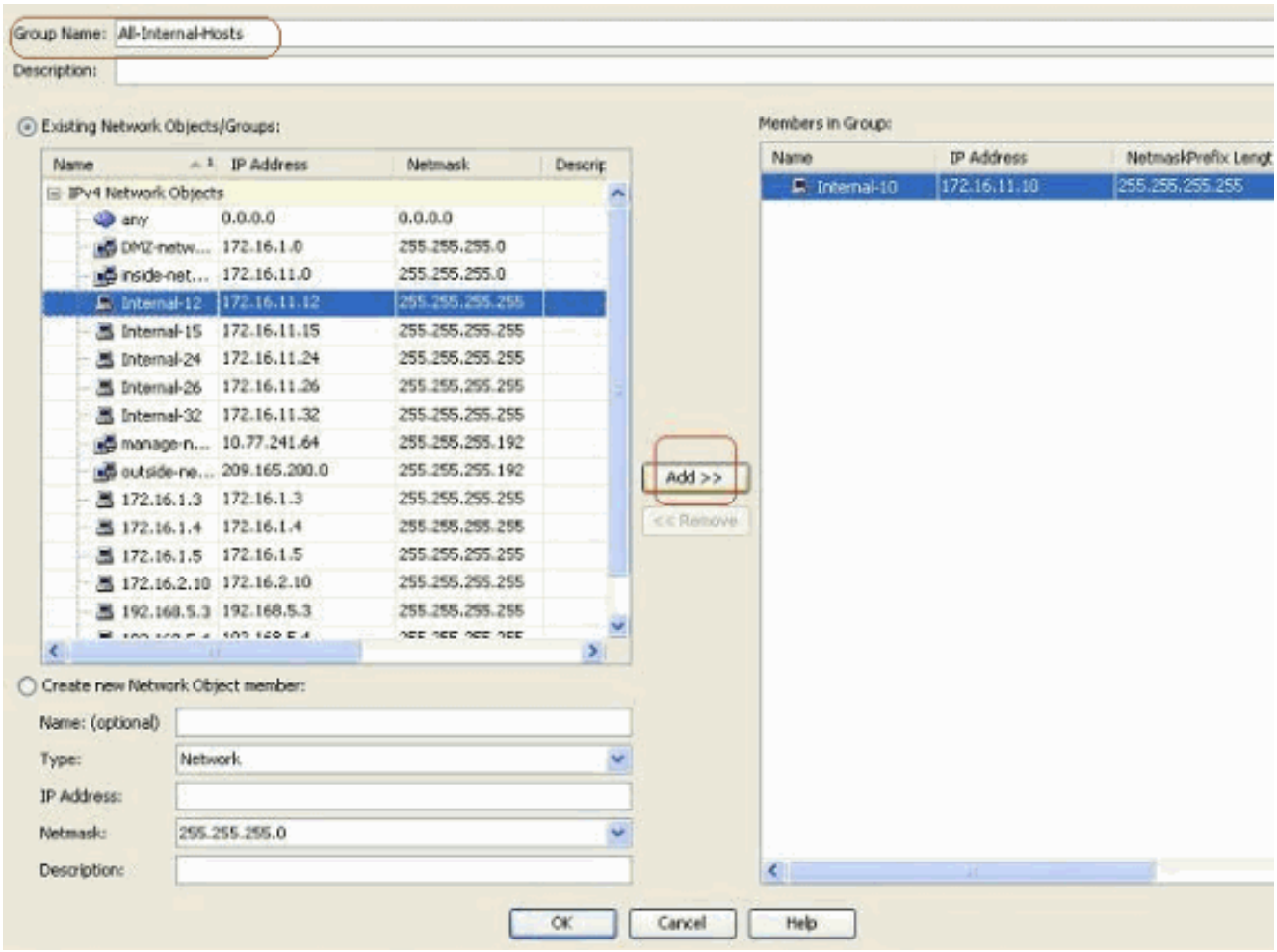


OK.

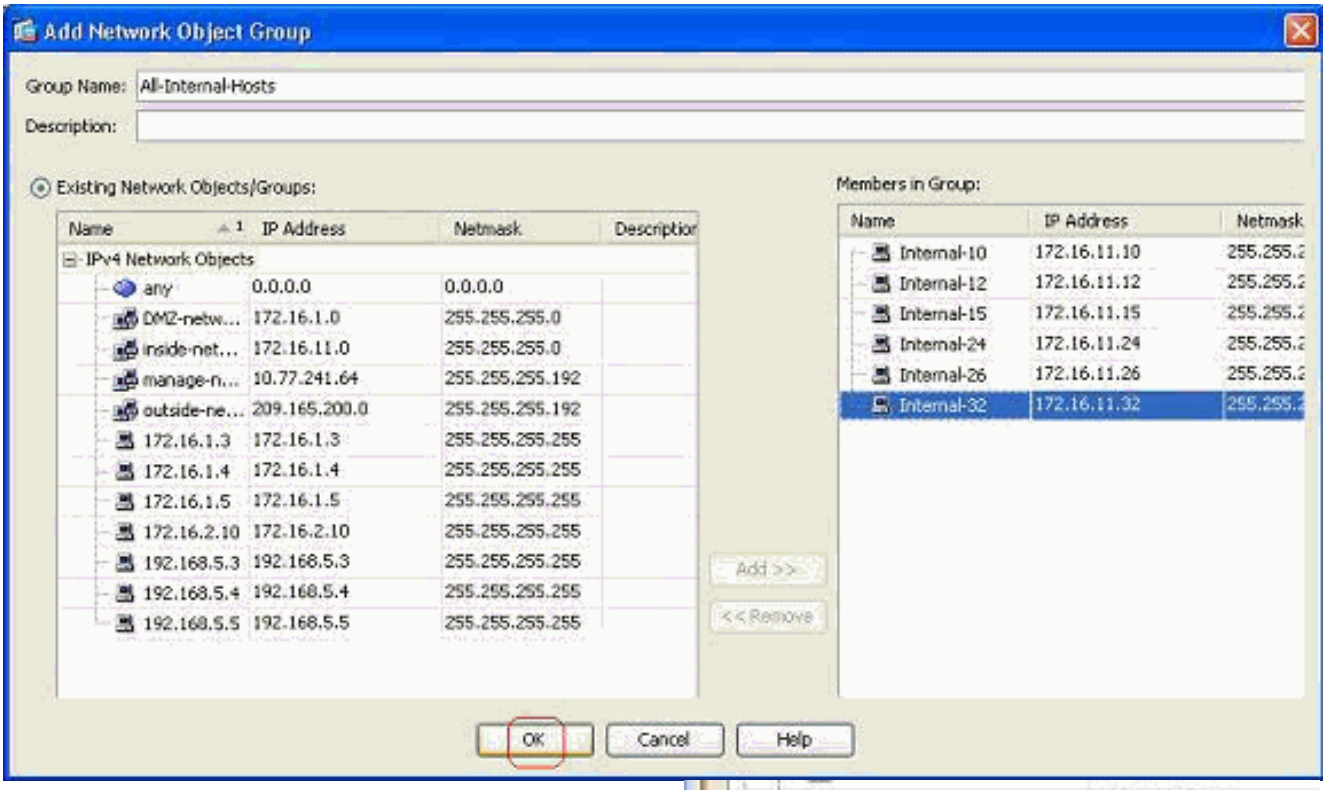
4. Escolha o **> Add da configuração > do Firewall > dos objetos > dos objetos de rede/grupos**, e clique o **grupo de objeto de rede** a fim criar um grupo de objeto de rede

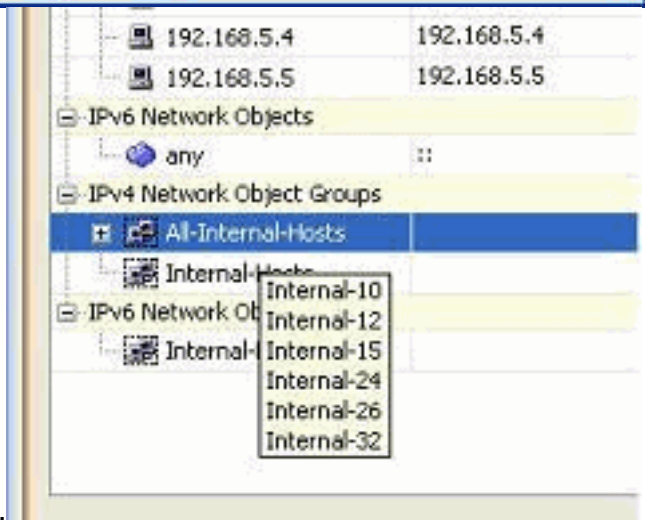
novo.

5. A lista disponível de todos os objetos de rede pode ser encontrada no painel esquerdo do indicador. Selecione objetos de rede individual, e clique o **botão Add** a fim fazer-lhes membros do grupo de objeto de rede recém-criado. O nome do grupo deve ser especificado no campo atribuído para
ele.



6. **APROVAÇÃO do** clique depois que você adiciona todos os membros dentro para agrupar.

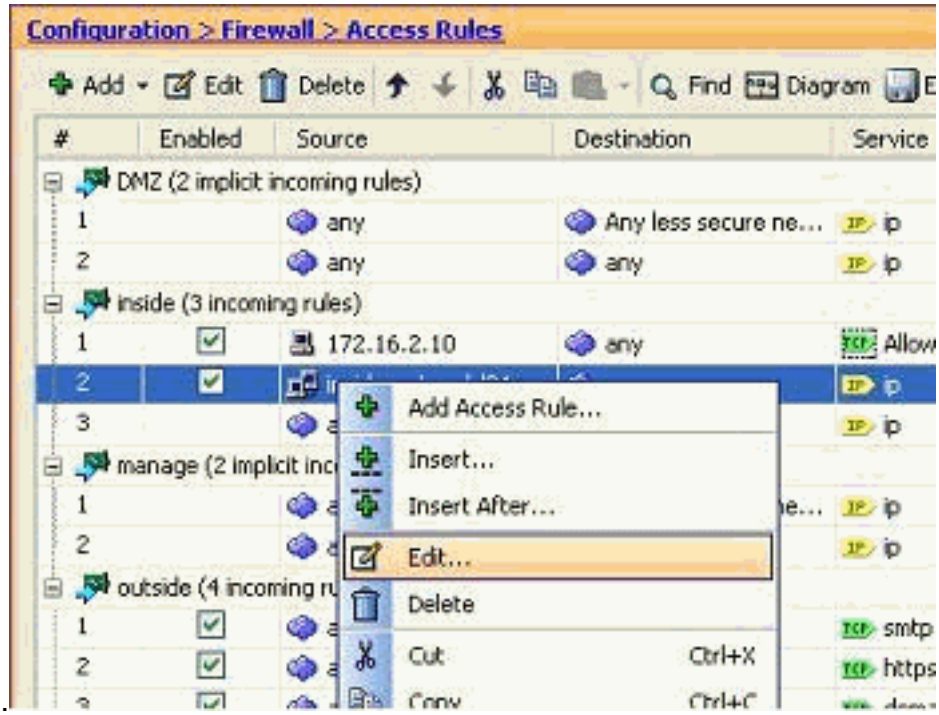




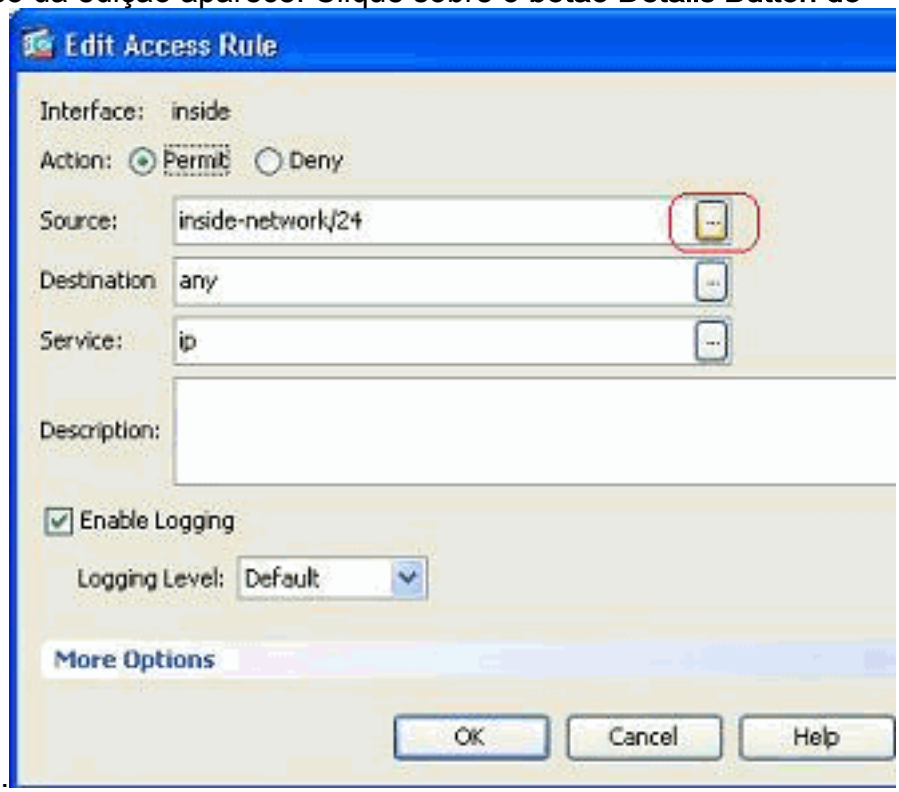
Você pode agora ver o grupo de objeto de rede.

7. A fim alterar toda a fonte/campo de destino de uma lista de acesso existente com um objeto do grupo de rede, para clicar com o botão direito a regra específica do acesso, e para

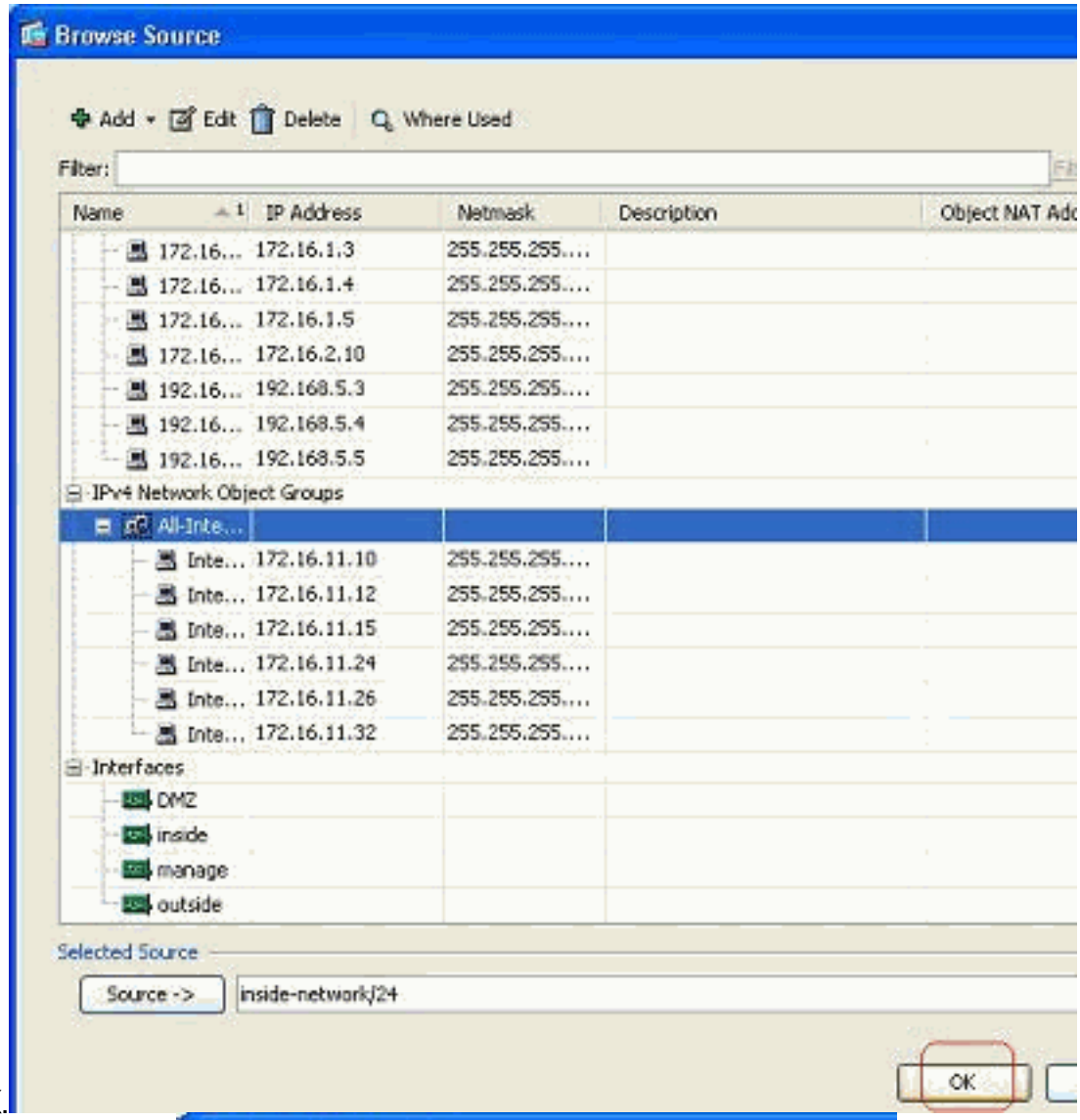
escolhê-la **edite**.



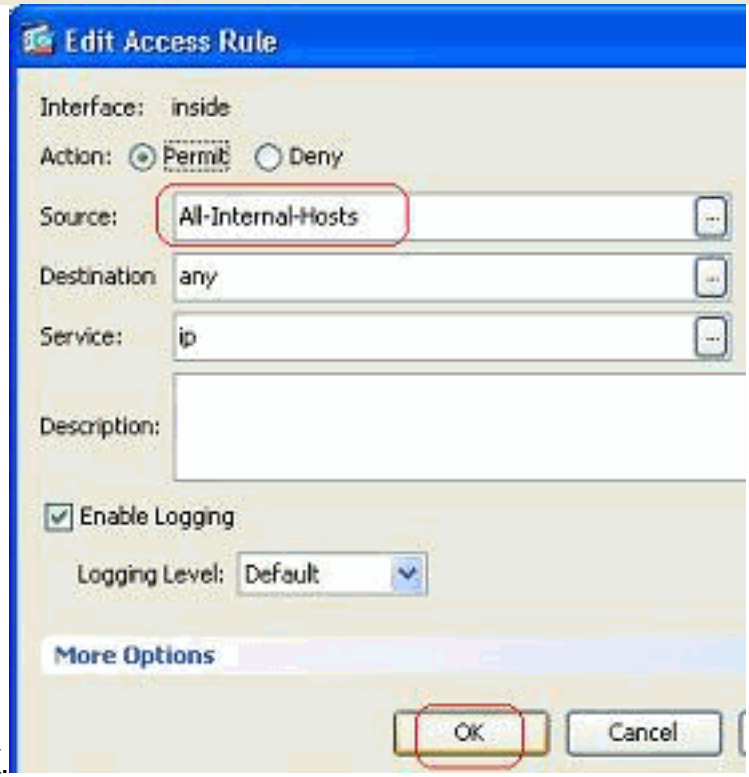
8. O indicador da regra do acesso da edição aparece. Clique sobre o **botão Details Button do** campo de fonte a fim alterá-lo.



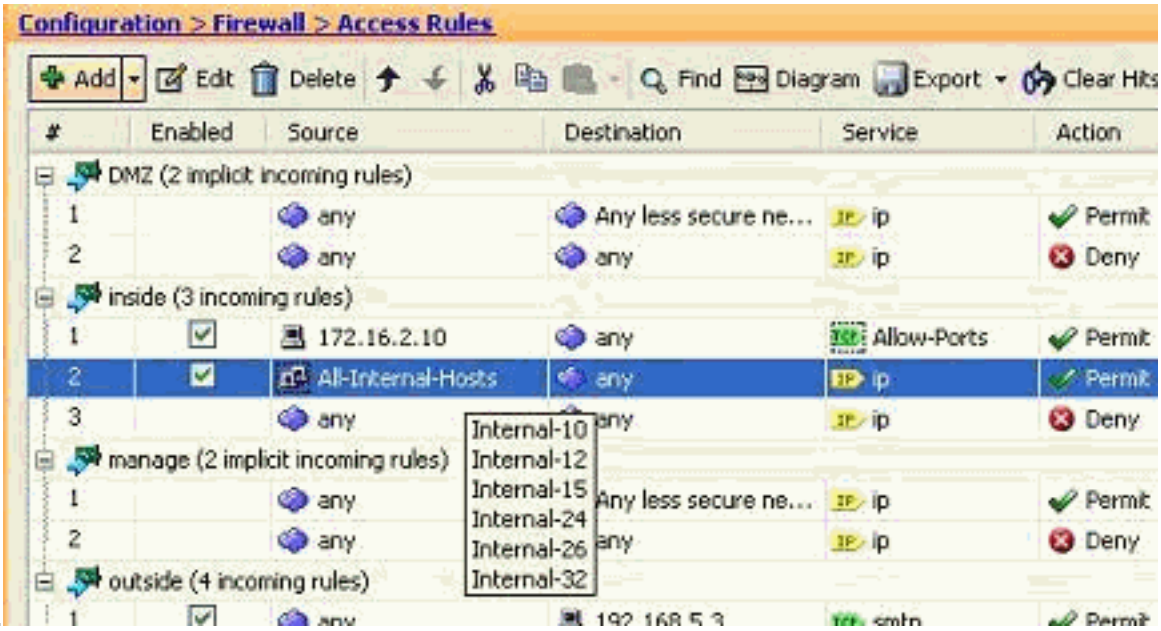
9. Selecione o grupo de objeto de rede dos Todo-Interno-**anfitriões**, e clique o **botão**



OK.



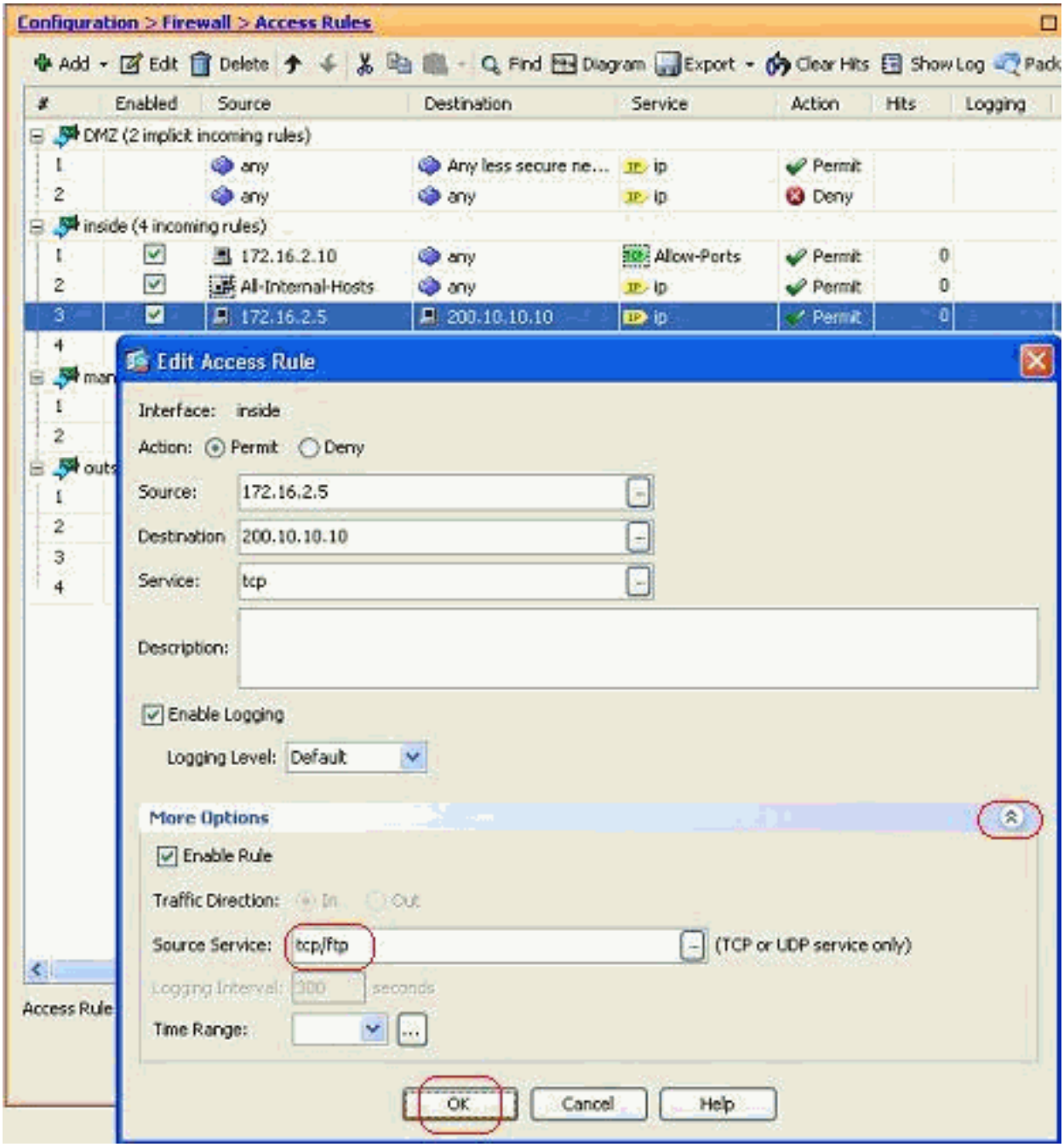
10. Clique em **OK**.
11. Paira seu rato sobre o campo de fonte da regra do acesso a fim ver os membros do

grupo. 

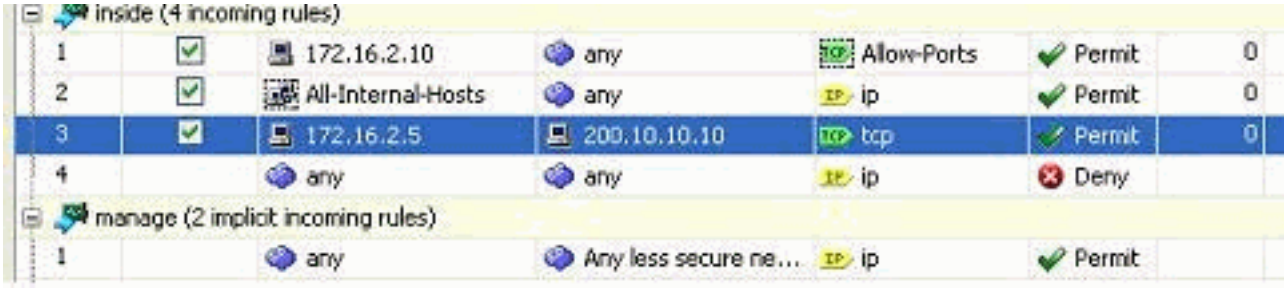
Edite a porta de origem:

Termine estas etapas a fim alterar a porta de origem de uma regra do acesso.

1. A fim alterar a porta de origem de uma regra existente do acesso, para clicar-la com o botão direito, e para escolhê-la **edite**.O indicador da regra do acesso da edição aparece.



2. Clique **mais** botão da gota-para baixo das **opções** a fim alterar o campo do serviço da fonte, e clique a **APROVAÇÃO**.Você pode ver a regra alterada do acesso, como mostrado.

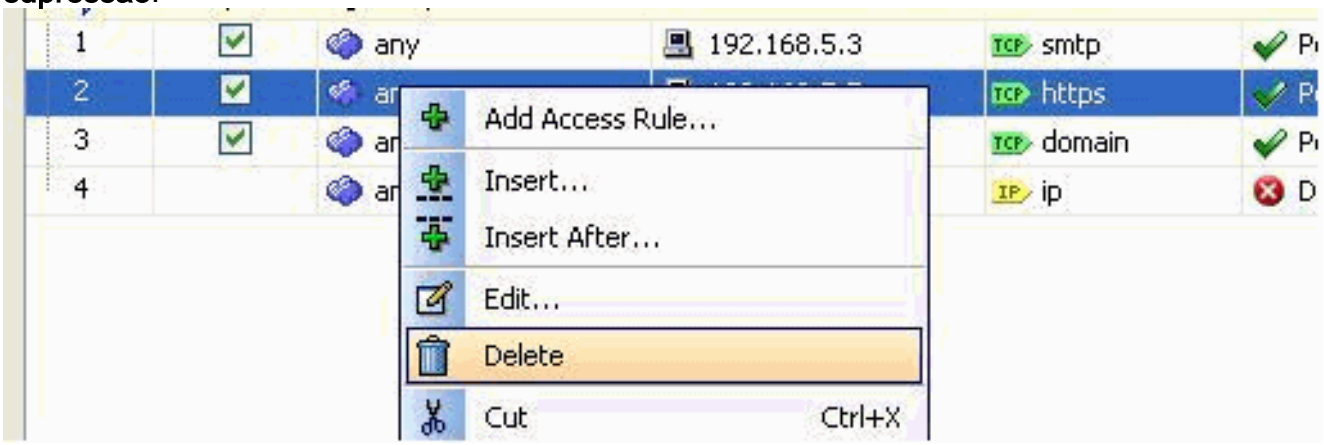


Suprima de uma lista de acessos

Termine estas etapas a fim suprimir de uma lista de acessos:

1. Antes que você suprima de uma lista de acesso existente, você precisa de suprimir das entradas de lista de acesso (as regras do acesso). Não é possível suprimir da lista de

acessos a menos que você suprimir primeiramente de todas as regras do acesso.Clicar com o botão direito a regra do acesso a ser suprimida, e escolha a **supressão**.



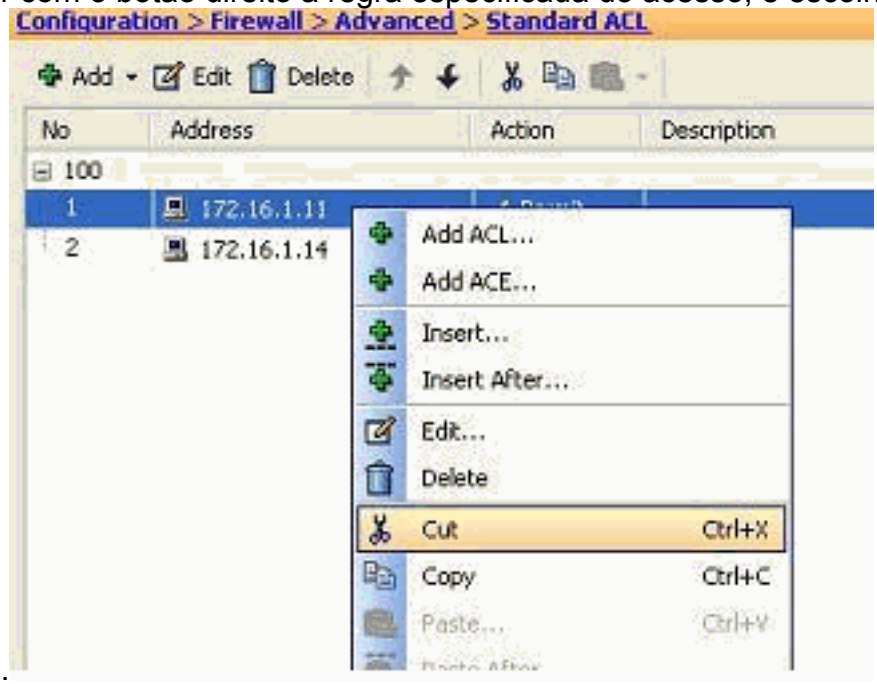
2. Termine a mesma operação da supressão em todas as regras existentes do acesso, e então selecione a lista de acessos e escolha a **supressão** a fim suprimir d.

Exporte a regra do acesso

As regras do acesso ASDM ligam a lista de acessos com a interface respectiva quando o gerente ACL seguir todas as listas de acesso extendida. As regras do acesso que são criadas com o gerente ACL não ligam a nenhuma relação. Estas Listas de acesso são usadas geralmente com a finalidade de NAT-isento, do VPN-filtro e de similar outras funções onde não há nenhuma associação com a relação. O gerente ACL contém todas as entradas que você tem na seção das **regras da configuração > do Firewall > do acesso**. Além, o **gerente ACL** igualmente contém as regras globais do acesso que não são associadas a nenhuma relação. O ASDM é organizado de tal maneira que você pode exportar uma regra do acesso de toda a lista de acessos para outra facilmente.

Por exemplo, se você precisa uma regra do acesso que seja já parte de uma regra global do acesso a ser associada com uma relação, você não precisa de configurar outra vez aquele. Em lugar de, você pode executar uma operação do **corte & da pasta** para conseguir este.

1. Clicar com o botão direito a regra especificada do acesso, e escolha o **corte**.



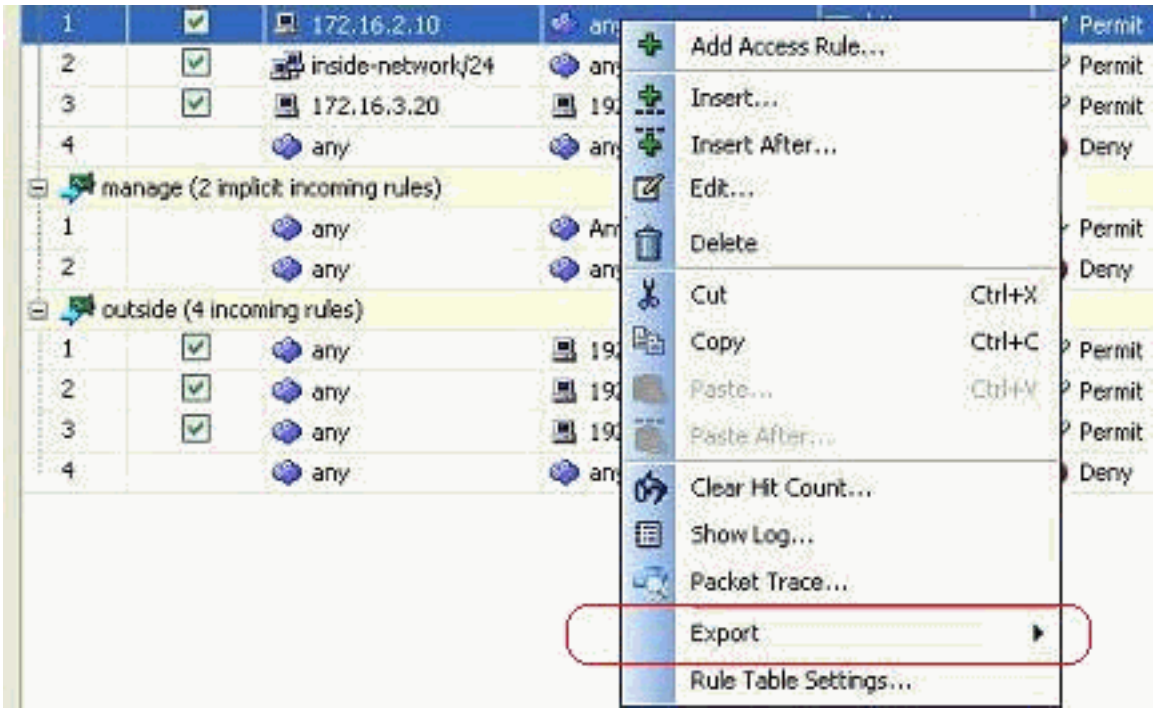
2. Selecione a lista de acessos exigida em que você precisa de introduzir esta regra do acesso. Você pode usar a **pasta na** barra de ferramentas para introduzir a regra do acesso.

Exporte a informação da lista de acessos

Você pode exportar a informação da lista de acessos para um outro arquivo. Dois formatos são apoiados para exportar esta informação.

1. Formato do Comma Separated Value (CSV)
2. Formato HTML

Clicar com o botão direito algumas das regras do acesso, e escolha a **exportação** a fim enviar a informação da lista de acessos a um arquivo.



Está aqui a informação da lista de acessos mostrada no formato HTML.

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

Verificar

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

Troubleshooting

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

Informações Relacionadas

- Exemplos e TechNotes da configuração ASDM
- Exemplos de configuração e Technotes ASA
- Suporte Técnico e Documentação - Cisco Systems