ASA 8.3 e posterior - Configurar inspeção usando o ASDM

Contents

Introduction

Este documento fornece uma configuração de exemplo para o Cisco Adaptive Security Appliance (ASA) com versões 8.3(1) e posteriores sobre como remover a inspeção padrão da política global de um aplicativo e como habilitar a inspeção para um aplicativo não padrão usando o Adaptive Security Device Manager (ASDM).

Refira ao PIX/ASA 7.x: Desative a inspeção global padrão e ative a inspeção de aplicativos não padrão para a mesma configuração no Cisco ASA com versões 8.2 e anteriores.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no software Cisco ASA Security Appliance versão 8.3(1) com ASDM 6.3.

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.

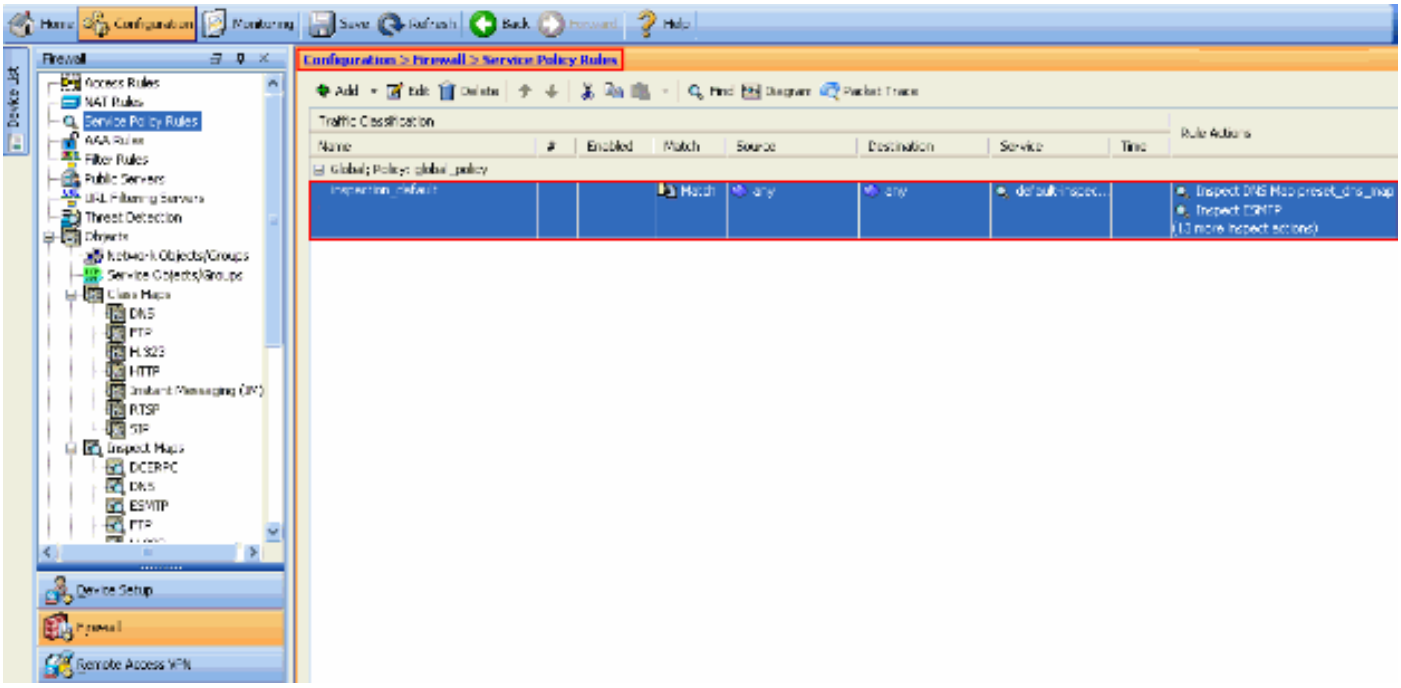
Conventions

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

Política global padrão

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica determinadas inspeções ao tráfego em todas as interfaces (uma política global). Nem todas as inspeções estão habilitadas por padrão. Você pode aplicar apenas uma política global. Para alterar a política global, você deve editar a política padrão ou desativá-la e aplicar uma nova. (Uma política de interface substitui a política global.)

No ASDM, escolha **Configuration > Firewall > Service Policy Rules** para exibir a política global padrão que tem a inspeção de aplicativo padrão como mostrado aqui:

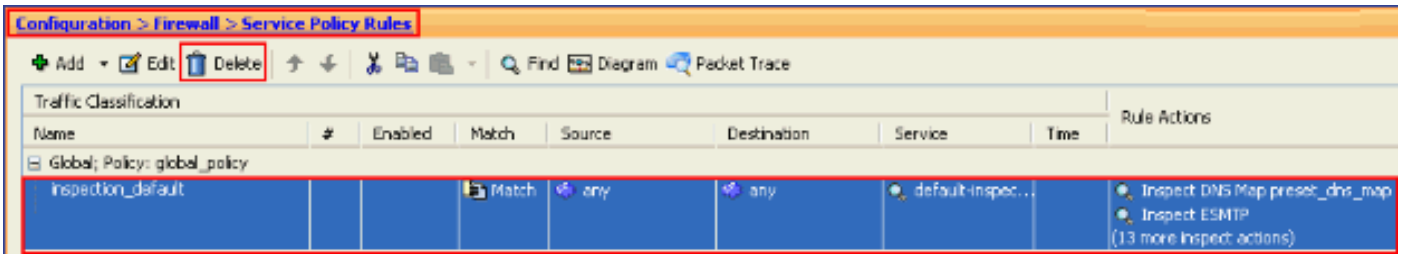


A configuração de política padrão inclui estes comandos:

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
```

```
  inspect tftp
service-policy global_policy global
```

Se precisar desabilitar a política global, use o comando **global no service-policy global_policy**. Para excluir a política global usando o ASDM, escolha **Configuration > Firewall > Service Policy Rules**. Em seguida, selecione a diretiva global e clique em **Excluir**.



Observação: quando você exclui a política de serviço com o ASDM, a política associada e os mapas de classe são excluídos. No entanto, se a política de serviço for excluída usando CLI, somente a política de serviço será removida da interface. O mapa de classes e o mapa de políticas permanecem inalterados.

Desabilitar inspeção global padrão para um aplicativo

Para desabilitar a inspeção global de um aplicativo, use a versão *no* do comando **inspect**.

Por exemplo, para remover a inspeção global do aplicativo FTP ao qual o Security Appliance escuta, use o comando **no inspect ftp** no modo de configuração de classe.

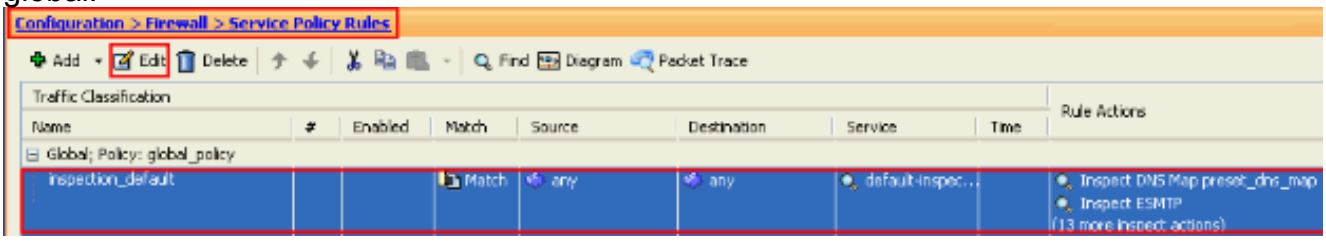
O modo de configuração de classe é acessível a partir do modo de configuração do mapa de política. Para remover a configuração, use a forma *no* do comando.

```
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#no inspect ftp
```

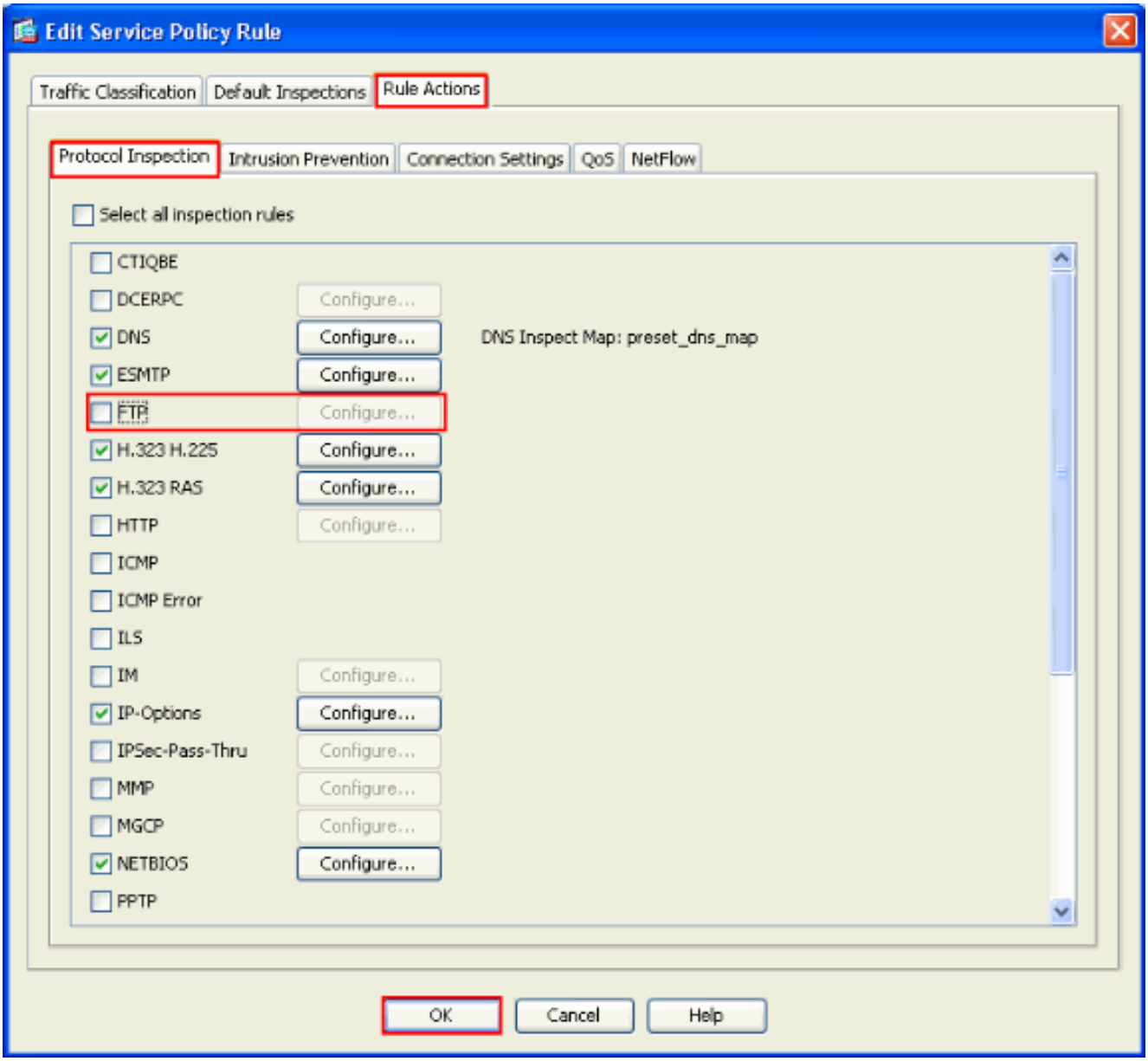
Para desabilitar a inspeção global para FTP usando o ASDM, faça o seguinte:

Observação: consulte Permitindo Acesso HTTPS para ASDM para obter as configurações básicas para acessar o PIX/ASA por meio do ASDM.

1. Escolha **Configuration > Firewall > Service Policy Rules** e selecione a política global padrão. Em seguida, clique em **Editar** para editar a política de inspeção global.



2. Na janela Editar regra de política de serviço, escolha **Inspeção de protocolo** na guia **Ações da regra**. Verifique se a caixa de seleção **FTP** está desmarcada. Isso desabilita a inspeção de FTP como mostrado na próxima imagem. Em seguida, clique em **OK** e em **Aplicar**.



Observação: para obter mais informações sobre a inspeção de FTP, consulte [PIX/ASA 7.x: Exemplo de Configuração de Habilitação de Serviços de FTP/TFTP.]

Habilitar inspeção para aplicativo não padrão

A inspeção de HTTP aprimorada está desabilitada por padrão. Para habilitar a inspeção HTTP em global_policy, use o comando **inspect http** em class inspection_default.

Neste exemplo, qualquer conexão HTTP (tráfego TCP na porta 80) que entra no Security Appliance por meio de qualquer interface é classificada para inspeção HTTP. *Como a política é uma política global, a inspeção ocorre somente quando o tráfego entra em cada interface*.

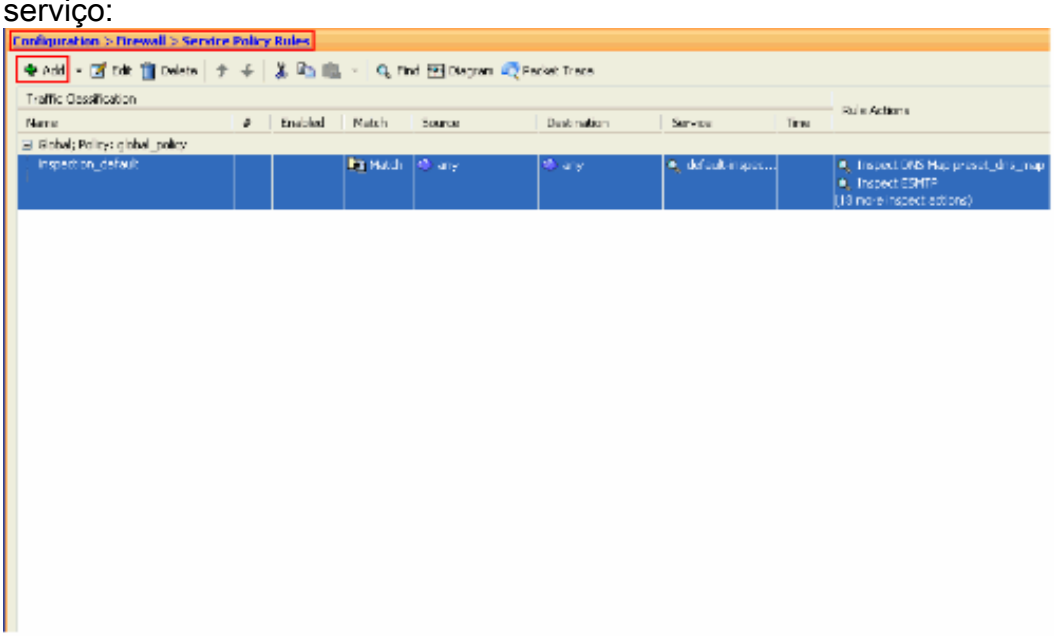
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

Neste exemplo, qualquer conexão HTTP (tráfego TCP na porta 80) que entra ou sai do Security Appliance através da *interface externa é classificada para inspeção HTTP*.

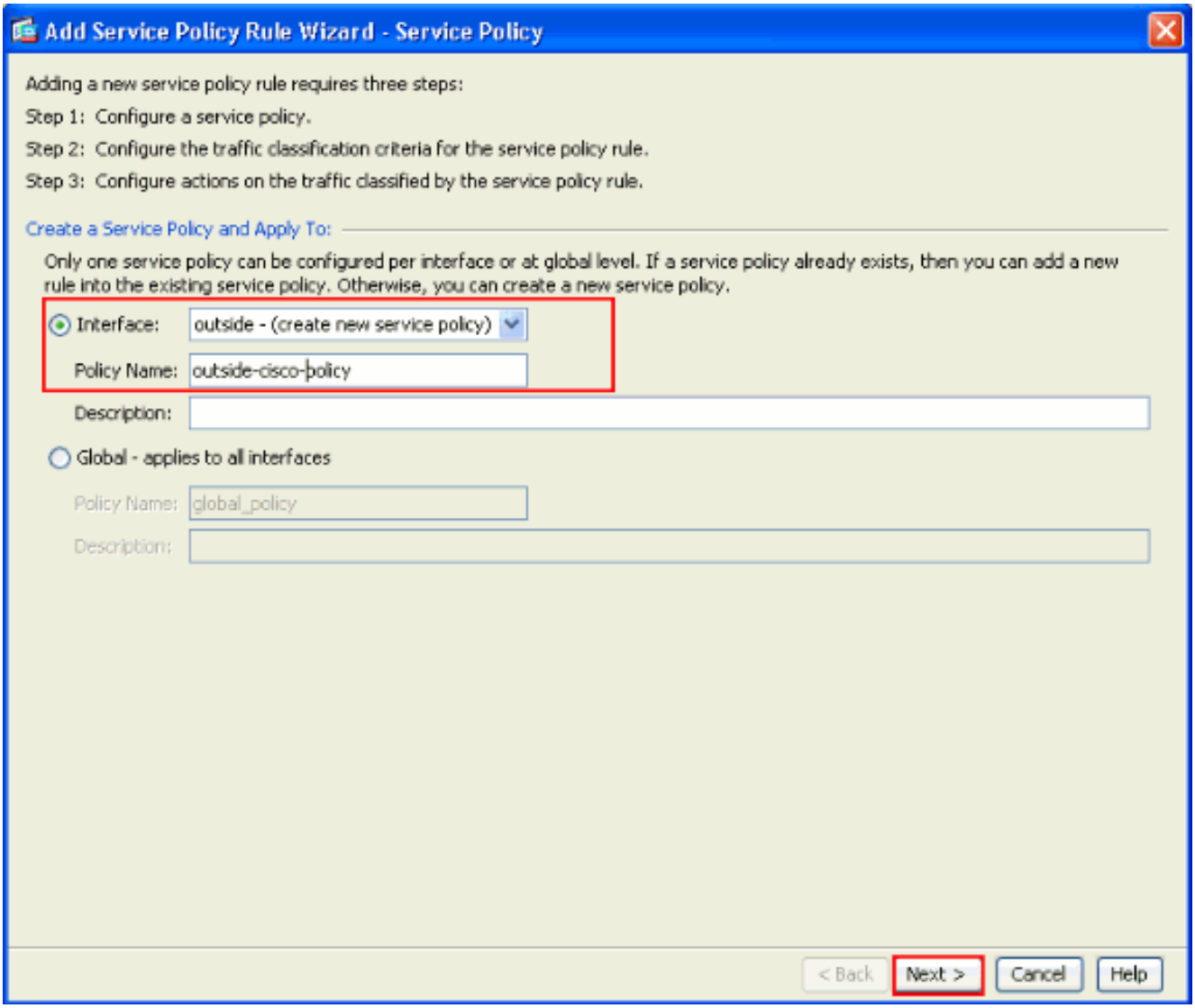
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Execute estas etapas para configurar o exemplo acima usando ASDM:

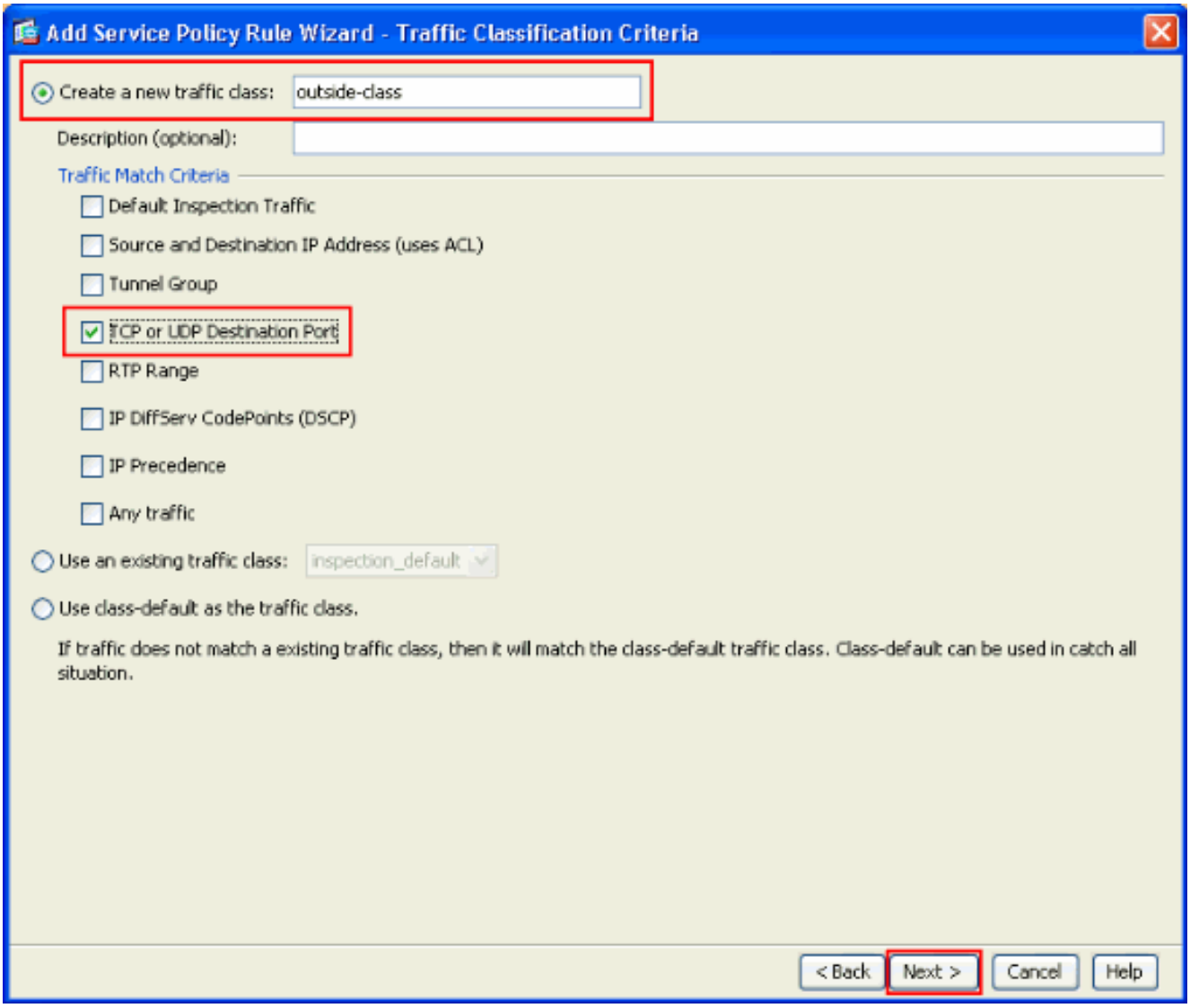
1. Escolha **Configuration > Firewall > Service Policy Rules** e clique em **Add** para adicionar uma nova política de serviço:



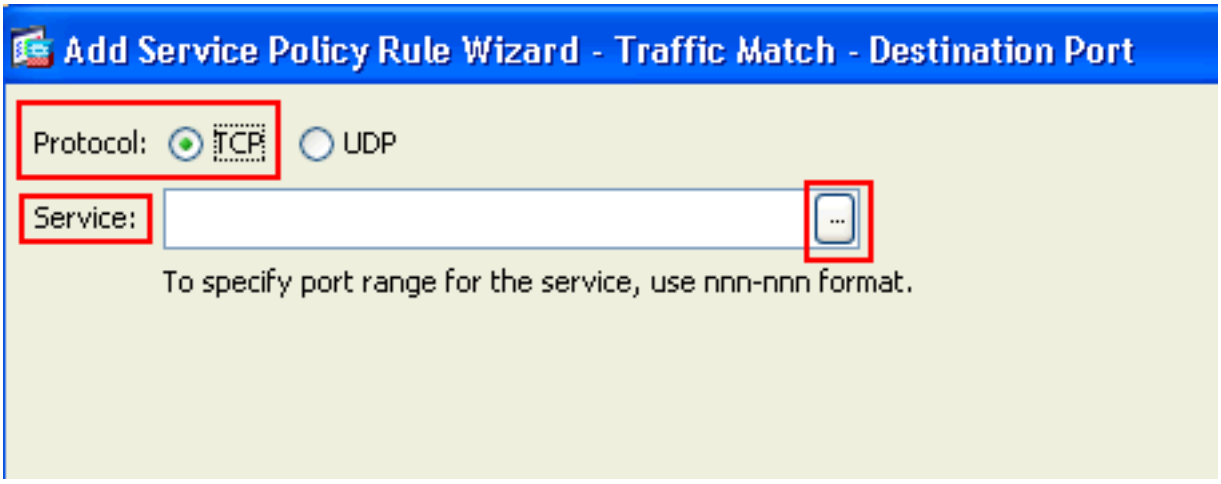
2. Na janela Add Service Policy Rule Wizard - Service Policy, selecione o botão de opção ao lado de **Interface**. Isso aplica a política criada para uma interface específica, que é a interface **externa** neste exemplo. Forneça um nome de política, que é **outside-cisco-policy** neste exemplo. Clique em Next.



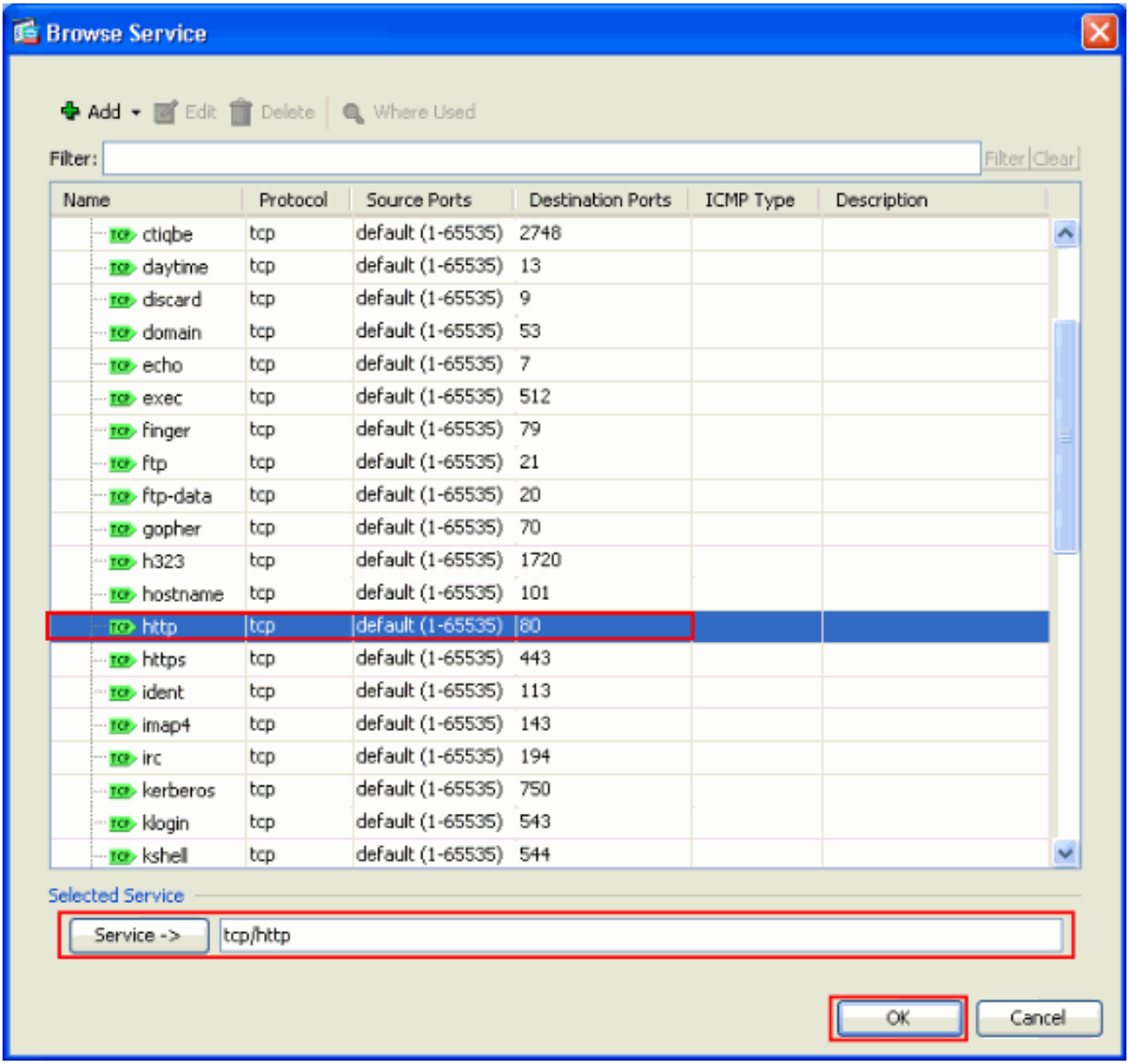
3. Na janela Add Service Policy Rule Wizard - Traffic Classification Criteria, forneça o novo nome da classe de tráfego. O nome usado neste exemplo é **fora da classe**. Verifique se a caixa de seleção ao lado de **TCP ou UDP Destination Port (Porta de destino TCP ou UDP)** está marcada e clique em **Next (Avançar)**.



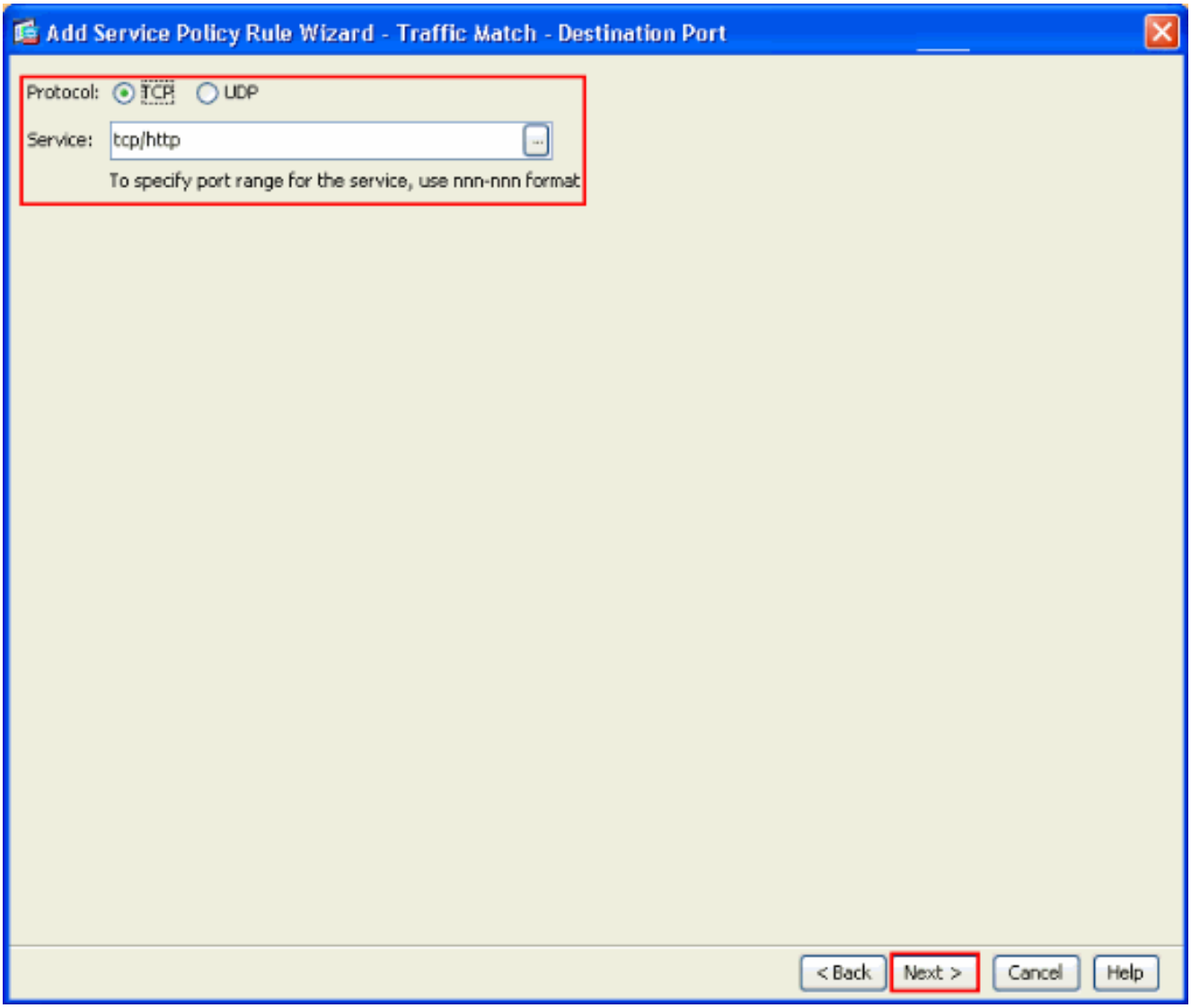
4. Na janela Add Service Policy Rule Wizard - Traffic Match - Destination Port (Assistente para adicionar regra de política de serviço - correspondência de tráfego - Porta de destino), escolha o botão de opção ao lado de **TCP** na seção **Protocol (Protocolo)**. Em seguida, clique no botão ao lado de **Serviço** para escolher o serviço necessário.



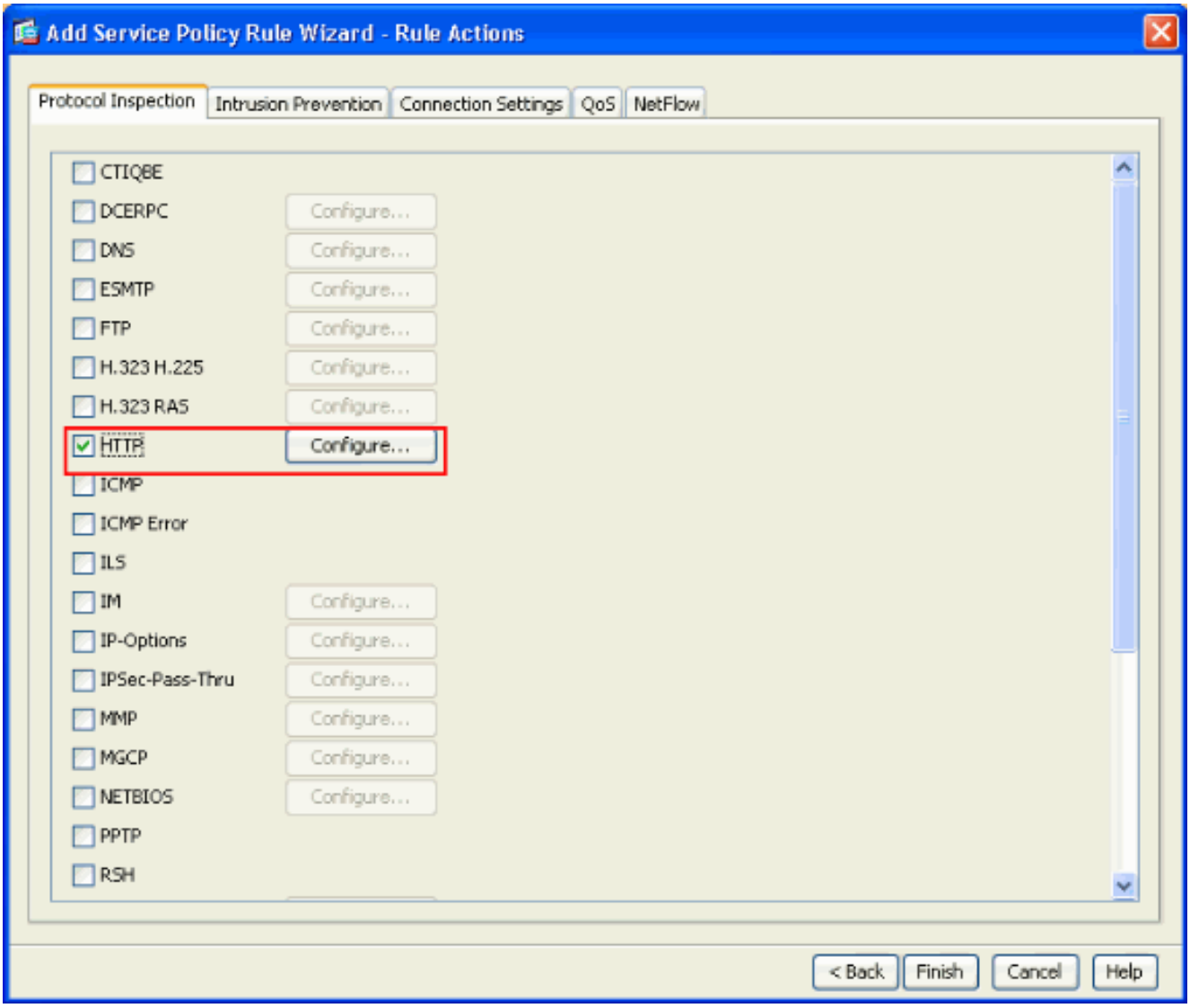
5. Na janela Procurar serviço, escolha **HTTP** como o serviço. Em seguida, clique em **OK**.



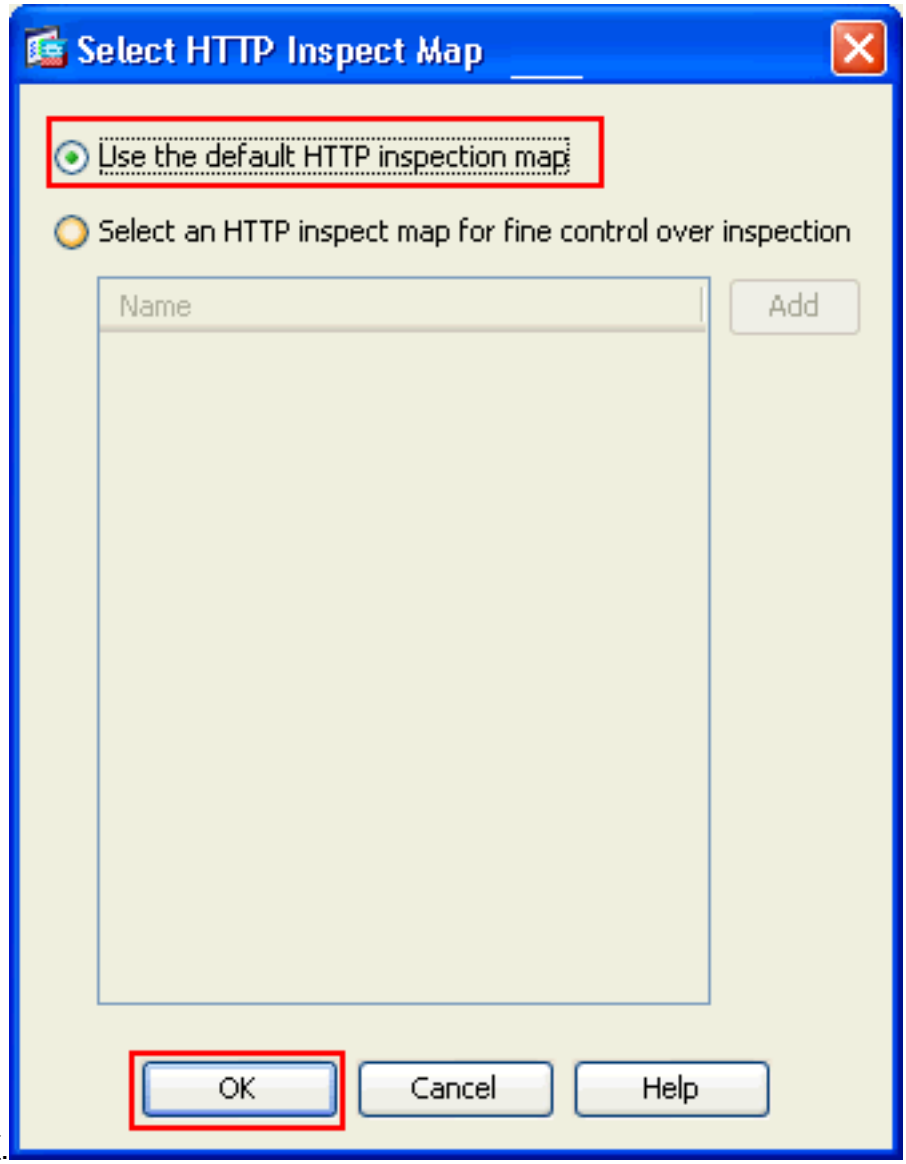
6. Na janela Add Service Policy Rule Wizard - Traffic Match - Destination Port (Assistente para adicionar regra de política de serviço - correspondência de tráfego - Porta de destino), você pode ver que o **Serviço** escolhido é **tcp/http**. Clique em
Next.



7. Na janela Add Service Policy Rule Wizard - Rule Actions (Assistente para adicionar regra de política de serviço - Ações da regra), marque a caixa de seleção ao lado de **HTTP**. Em seguida, clique em **Configurar** ao lado de **HTTP**.

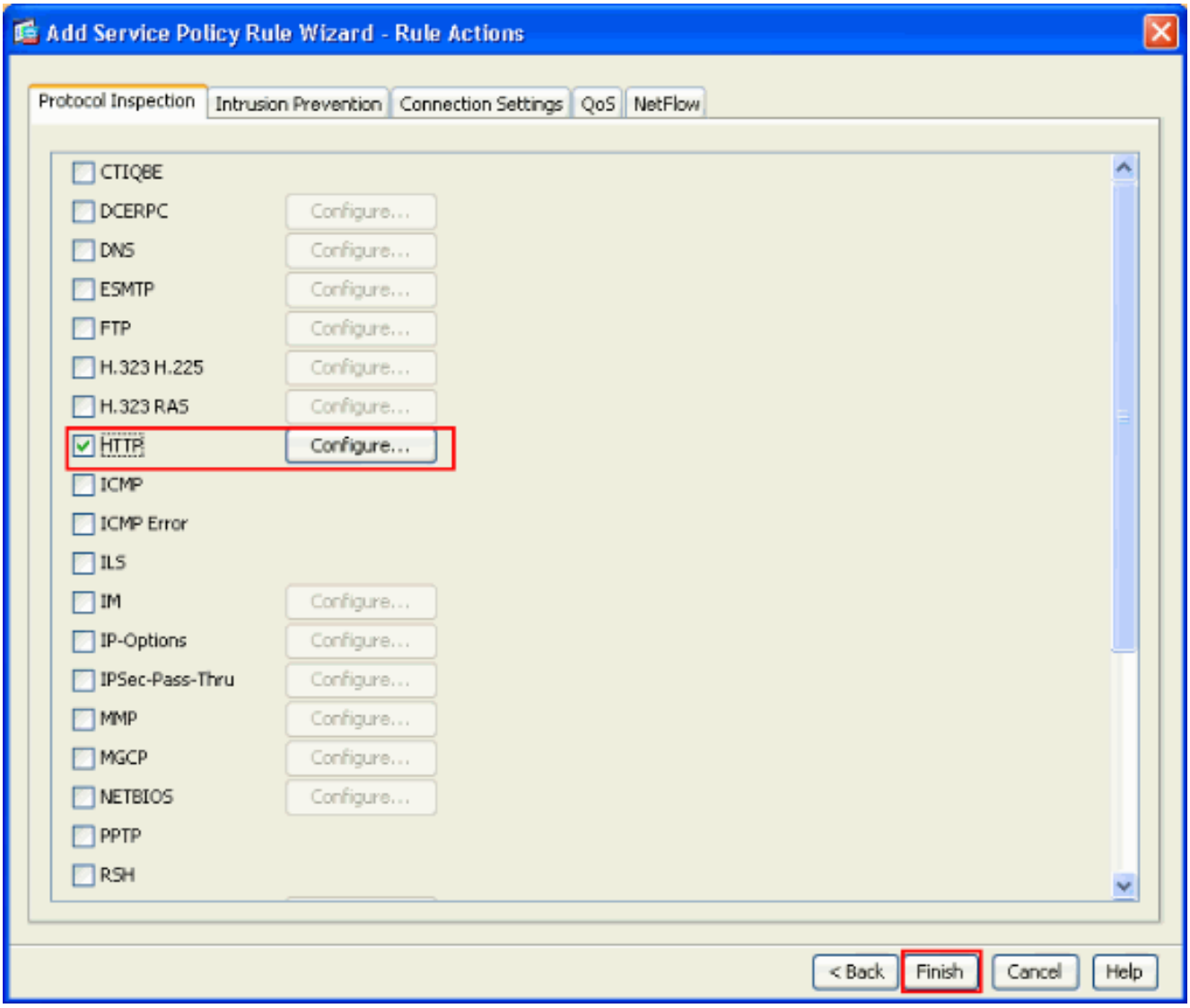


8. Na janela Selecionar mapa de inspeção HTTP, marque o botão de opção ao lado de **Usar o mapa de inspeção HTTP padrão**. A inspeção HTTP padrão é usada neste exemplo. Em

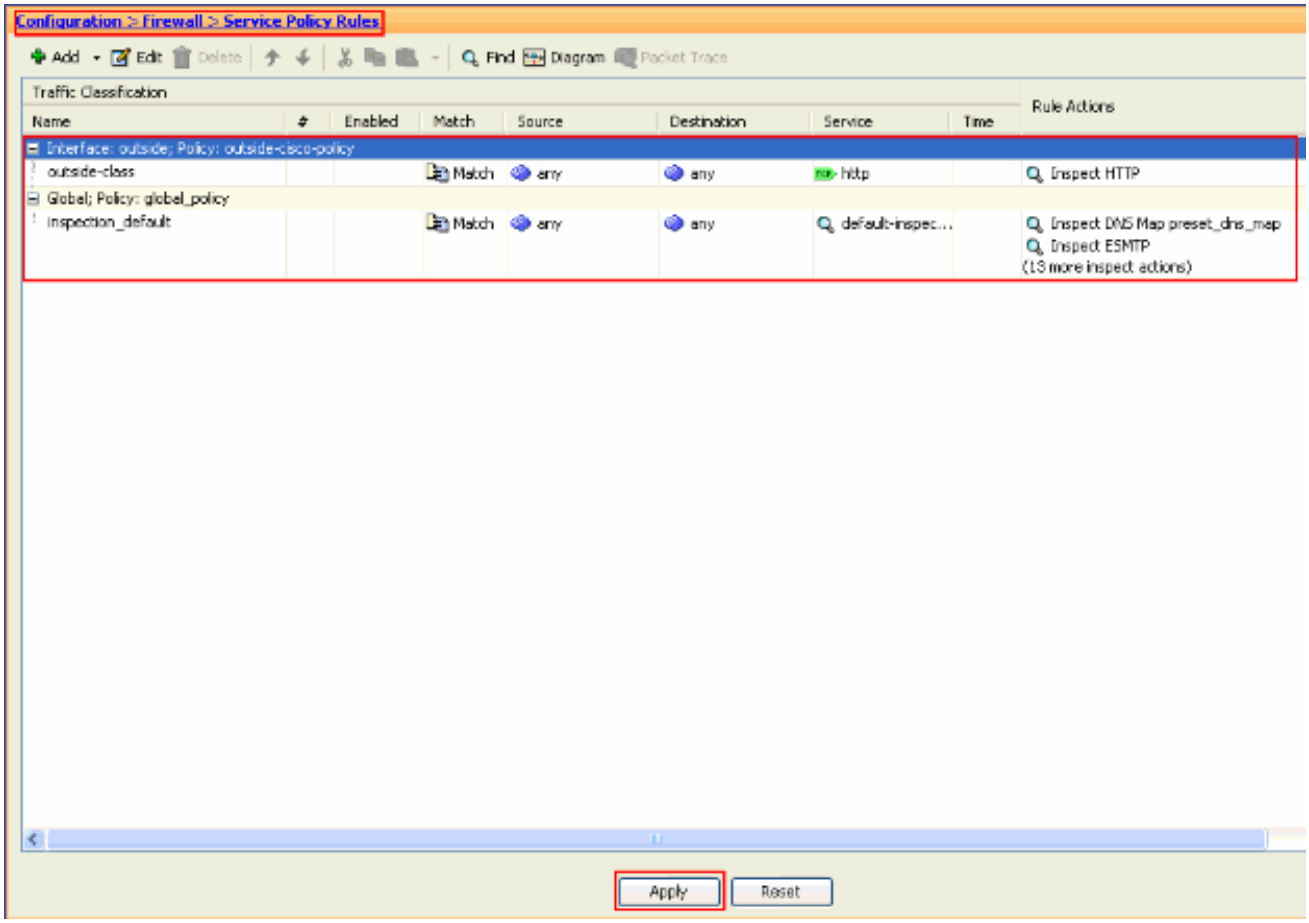


seguida, clique em **OK**.

9. Clique em **Finish**.



10. Em **Configuration > Firewall > Service Policy Rules**, você verá a Política de serviço recém-configurada **fora da cisco-policy** (para inspecionar HTTP) junto com a política de serviço padrão já presente no dispositivo. Clique em **Apply** para aplicar a configuração ao Cisco ASA.



Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Cisco Adaptive Security Device Manager
- Solicitações de Comentários (RFCs)
- Aplicação da Inspeção do Protocolo da Camada de Aplicação
- Suporte Técnico e Documentação - Cisco Systems