# ASA 8.3 e mais atrasado: Desabilite a inspeção global do padrão e permita a inspeção de aplicativo não-padrão usando o ASDM

## Índice



## Introdução

Este documento fornece uma configuração de exemplo para a ferramenta de segurança adaptável de Cisco (ASA) as versões 8.3(1) e mais tarde como remover a inspeção do padrão da política global para um aplicativo e como permitir a inspeção para um aplicativo não-padrão usando o Security Device Manager adaptável (ASDM).

Refira ao PIX/ASA 7.x: Desabilite a inspeção global do padrão e permita a inspeção de aplicativo não-padrão para a mesma configuração em Cisco ASA com versões 8.2 e anterior.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

A informação neste documento é baseada na versão de software da ferramenta de segurança de Cisco ASA 8.3(1) com ASDM 6.3.

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.

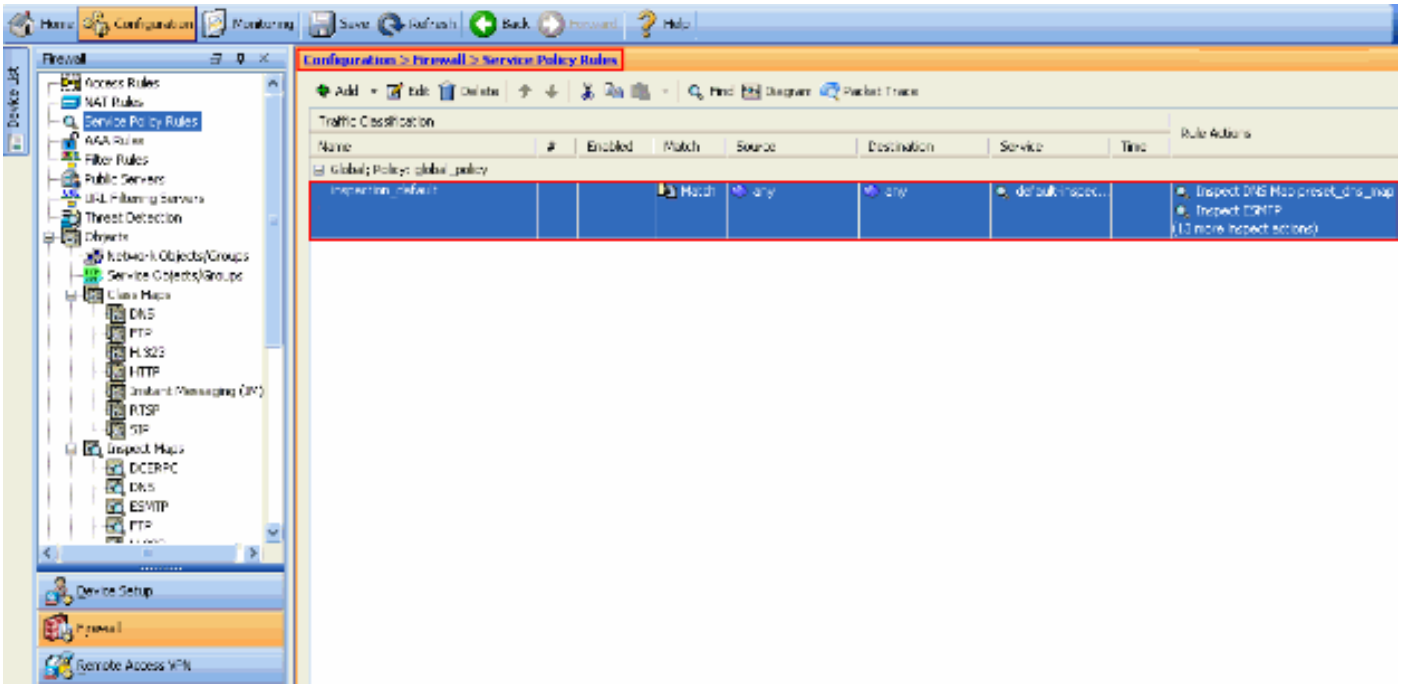
## Convenções

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

# Opte pela política global

Àrevelia, a configuração inclui uma política que combine todo o tráfego da inspeção do aplicativo padrão e aplique determinadas inspeçãos ao tráfego em todas as relações (uma política global). Não todas as inspeçãos são permitidas à revelia. Você pode aplicar somente uma política global. Se você quer alterar a política global, você deve editar a política padrão ou desabilitá-la e aplicar um novo. (Uma política da relação cancela a política global.)

No ASDM, escolha as **regras da configuração > do Firewall > da política de serviços** para ver a política global do padrão que tem a inspeção do aplicativo padrão como mostrado aqui:

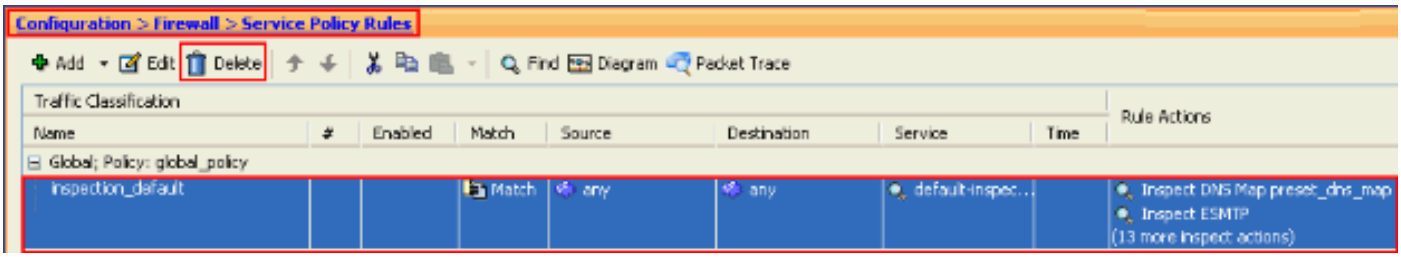



A configuração da política padrão inclui estes comandos:

```
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 você precisa de desabilitar a política global, não use **nenhum comando global do global_policy da serviço-política**. A fim suprimir da política global que usa o ASDM escolha **regras da configuração > do Firewall > da política de serviços**. Então, selecione a política global e clique a **supressão**.




**Nota:** Quando você suprime da política de serviços com ASDM, os mapas associados da política e da classe estão suprimidos. Contudo, se a política de serviços é suprimida usando o CLI somente a política de serviços é removida da relação. O mapa e o mapa de política da classe permanecem inalterados.

## Inspeção global do padrão do desabilitação para um aplicativo

A fim desabilitar a inspeção global para um aplicativo, não use *nenhuma* versão do **comando inspect**.

Por exemplo, a fim remover a inspeção global para o aplicativo de FTP que a ferramenta de segurança escuta, use o **nenhum inspecionam o comando ftp no** modo de configuração de classe.

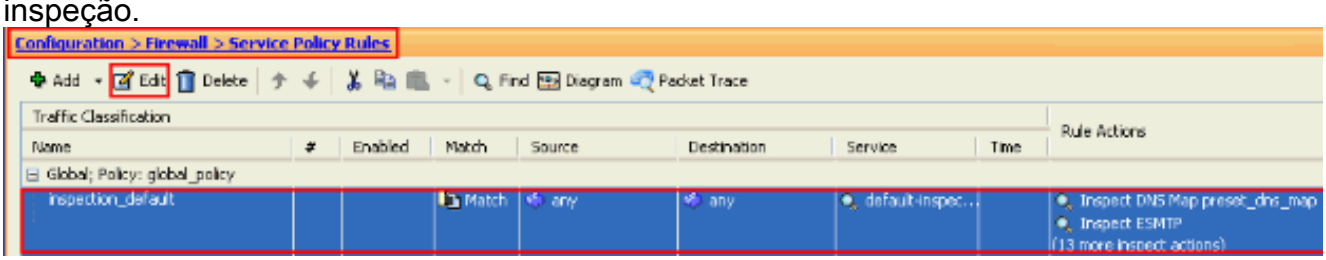
O modo de configuração de classe é acessível do modo da configuração de mapa de política. A fim remover a configuração, não use *nenhum* formulário do comando.

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

A fim desabilitar a inspeção global para o FTP usando o ASDM, termine estas etapas:

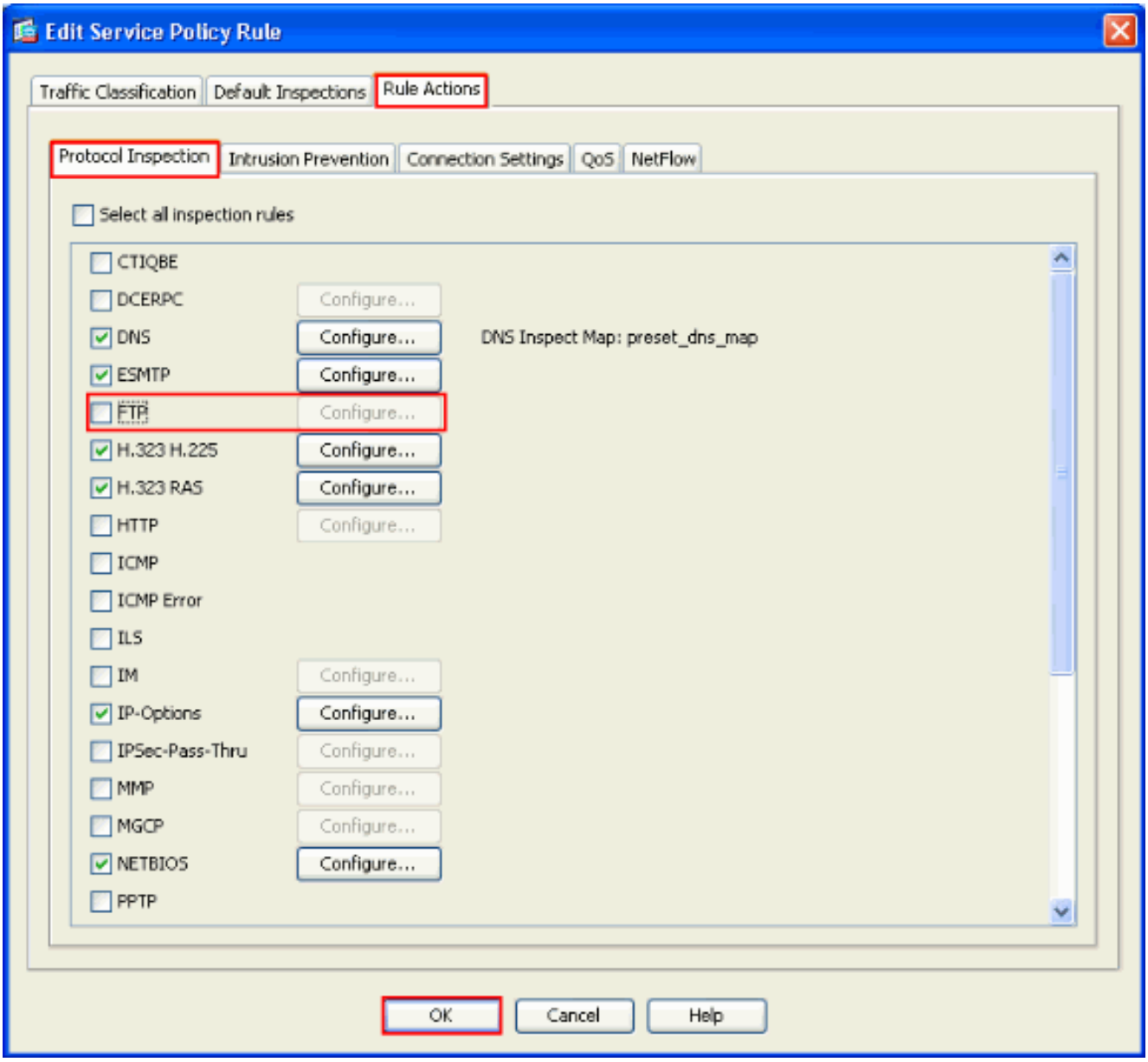
**Nota:** Refira permitir que o acesso HTTPS para o ASDM para configurações básicas a fim alcançar o PIX/ASA com o ASDM.

1. Escolha **regras da configuração > do Firewall > da política de serviços** e selecione a política global do padrão. Então, o clique **edita** para editar a política global da inspeção.




2. Do indicador da regra da política de serviços da edição, escolha a **inspeção do protocolo** sob a aba das **ações da regra**. Certifique-se que a caixa de verificação **FTP** está desmarcada.

Isto desabilita a inspeção FTP segundo as indicações da imagem seguinte. Então, a **APROVAÇÃO do** clique e **aplica-se**
então.




**Nota:** Para obter mais informações sobre da inspeção FTP, refira [PIX/ASA 7.x: Permita o exemplo de configuração dos serviços FTP/TFTP](#).

## Permita a inspeção para o aplicativo não-padrão

A inspeção aumentada HTTP é desabilitada à revelia. A fim permitir a inspeção HTTP no global_policy, use o comando **HTTP da inspeção** sob o inspection_default da classe.

Neste exemplo, toda a conexão de HTTP (tráfego TCP na porta 80) que entra a ferramenta de segurança através de qualquer relação é classificada para a inspeção HTTP. *Porque a política é uma política global, a inspeção ocorre somente enquanto o tráfego incorpora cada relação.*

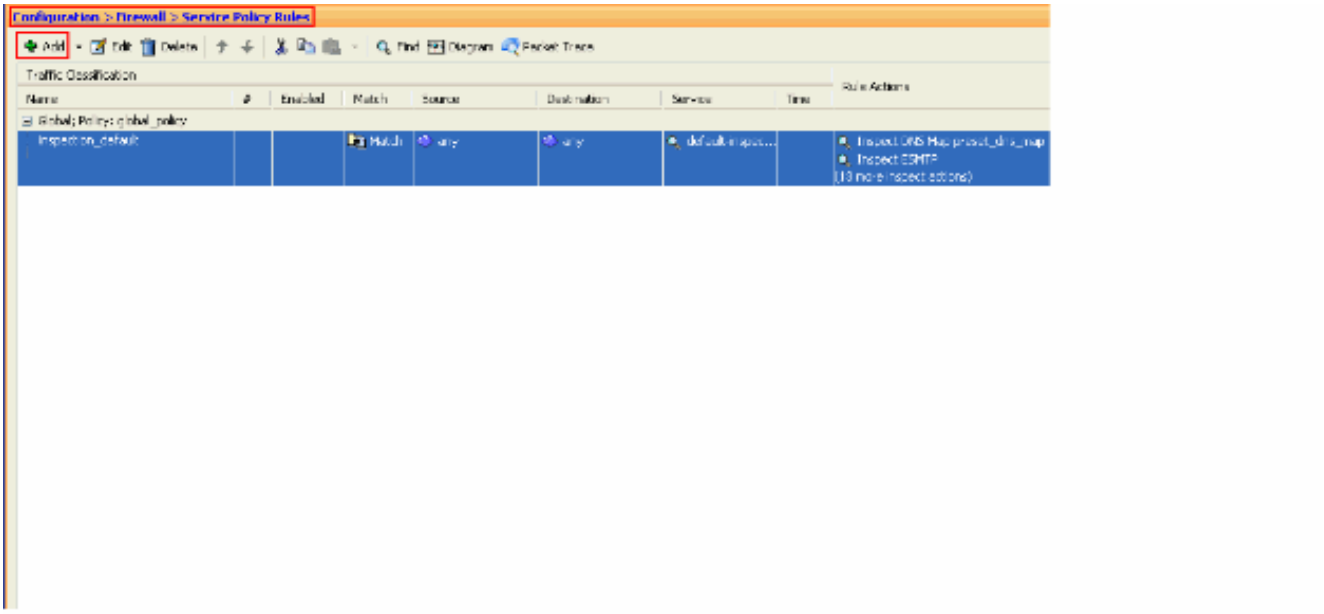
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

Neste exemplo, toda a conexão de HTTP (tráfego TCP na porta 80) que entra ou retira a ferramenta de segurança através da *interface externa é classificada para a inspeção HTTP*.

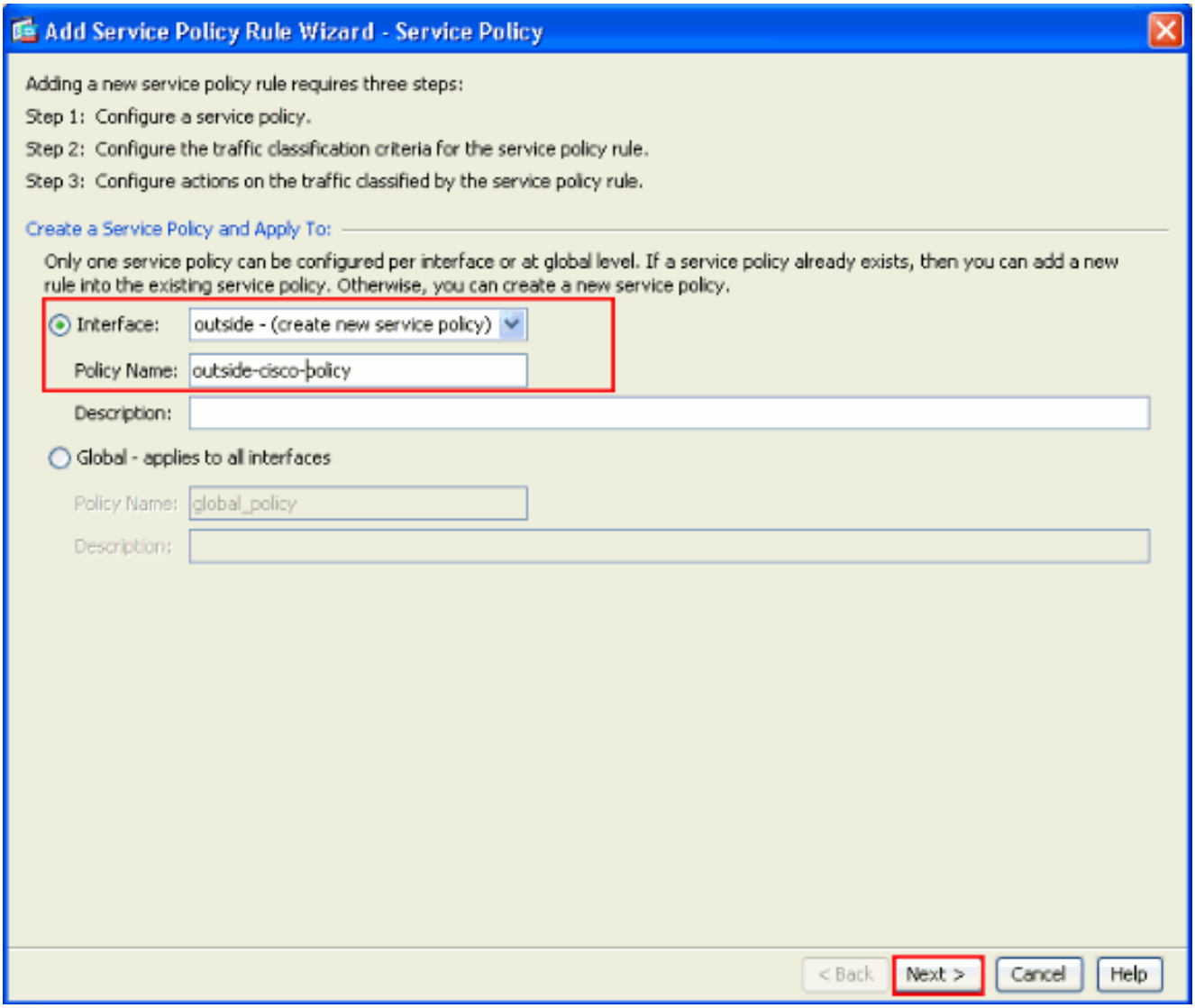
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Execute estas etapas a fim configurar o exemplo acima usando o ASDM:

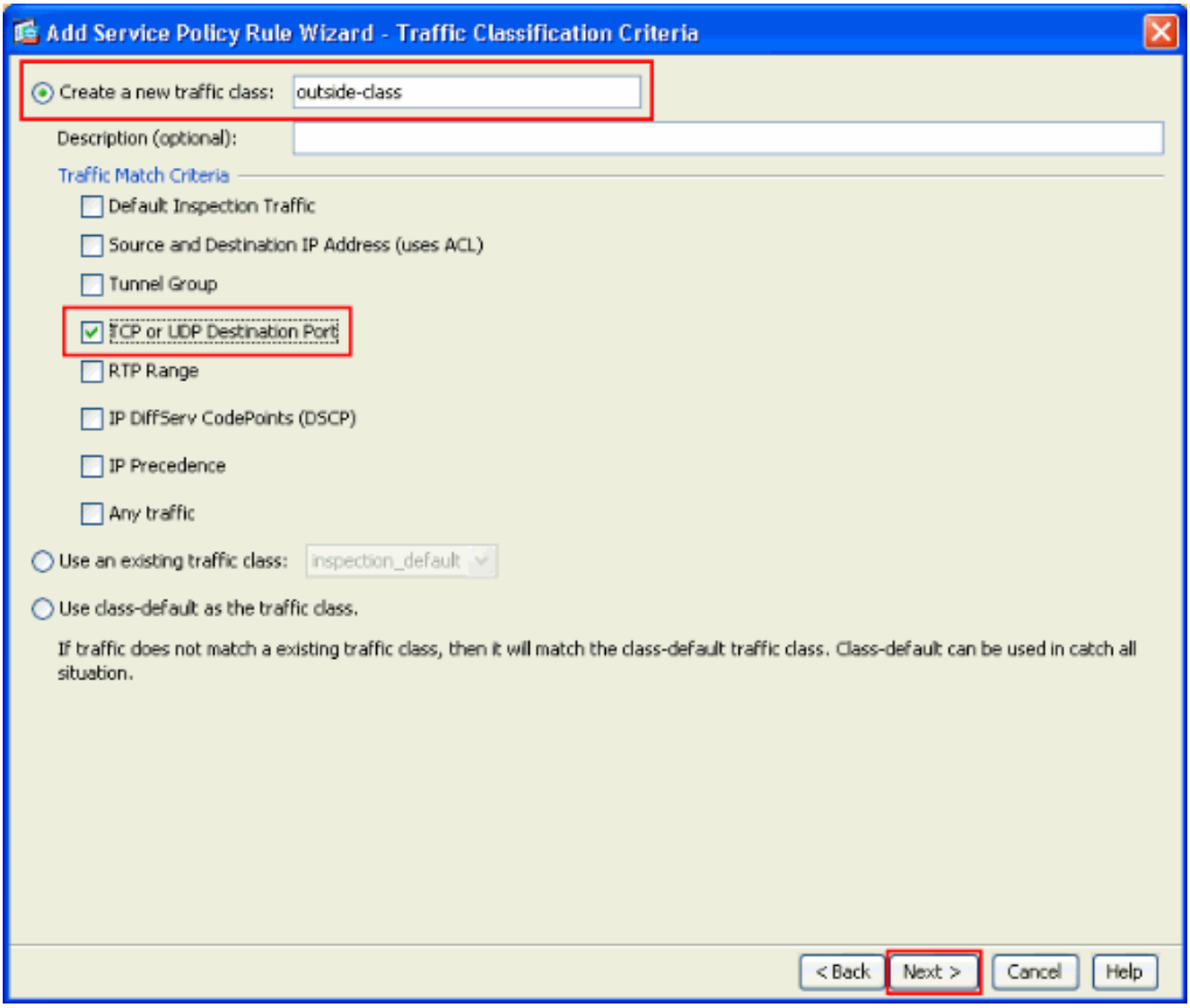
1. Escolha **regras da configuração > do Firewall > da política de serviços** e o clique **adiciona** a fim adicionar uma política de serviços nova:



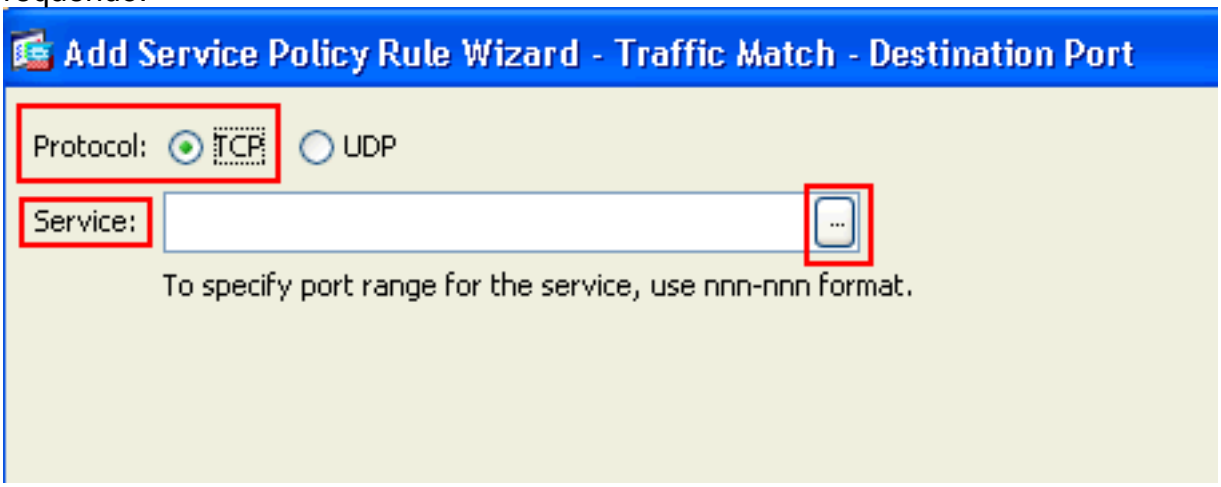

2. Do assistente da regra da política de serviços adicionar - O indicador da política de serviços, escolhe o botão de rádio ao lado da **relação**. Isto aplica a política criada a uma relação específica, que seja a **interface externa n**este exemplo. Forneça um nome da política, que seja parte-Cisco-**política n**este exemplo. Clique em Next.



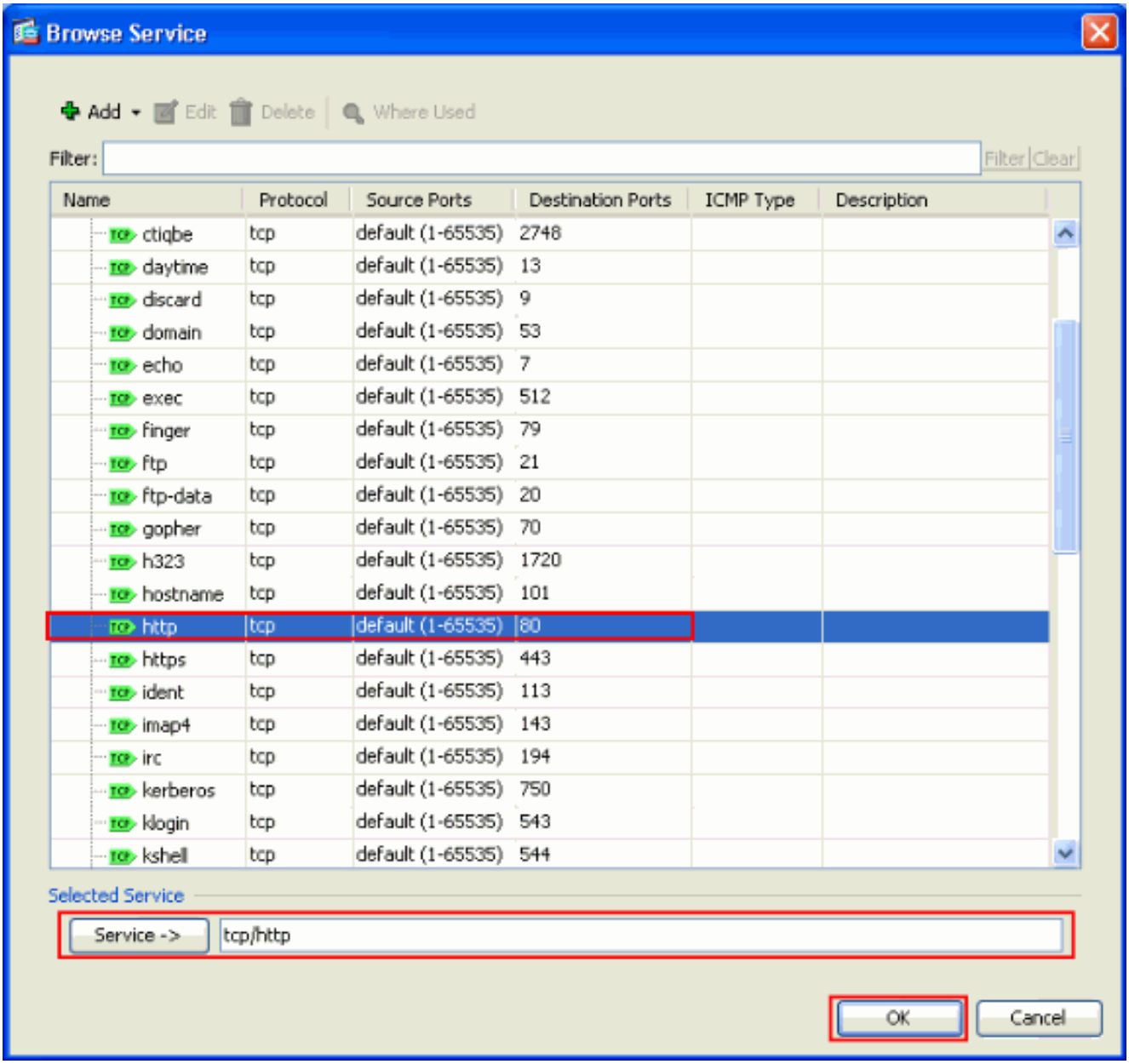

3. Do assistente da regra da política de serviços adicionar - Os critérios do indicador da Classificação de tráfego, fornecem o nome de classe de tráfego novo. O nome usado neste exemplo é parte-**classe**. Assegure-se de que a caixa de verificação ao lado do **TCP ou da porta de destino de UDP** esteja verificada e clique-se **em seguida**.



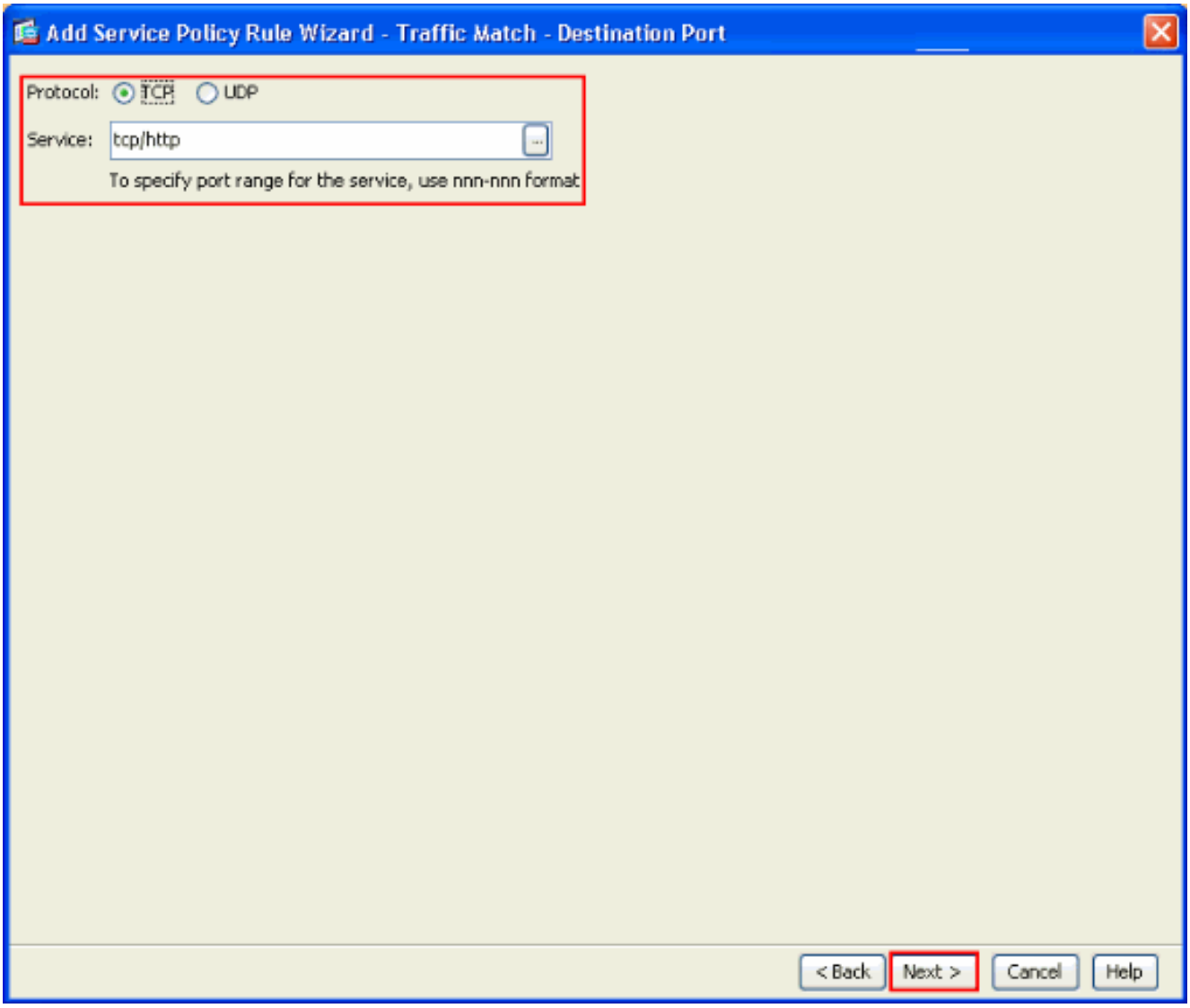

4. Do assistente da regra da política de serviços adicionar - Fósforo do tráfego - O indicador da porta do destino, escolhe o botão de rádio ao lado do **TCP** sob a **seção de protocolo**. Então, clique o botão ao lado do **serviço** a fim escolher o serviço requerido.



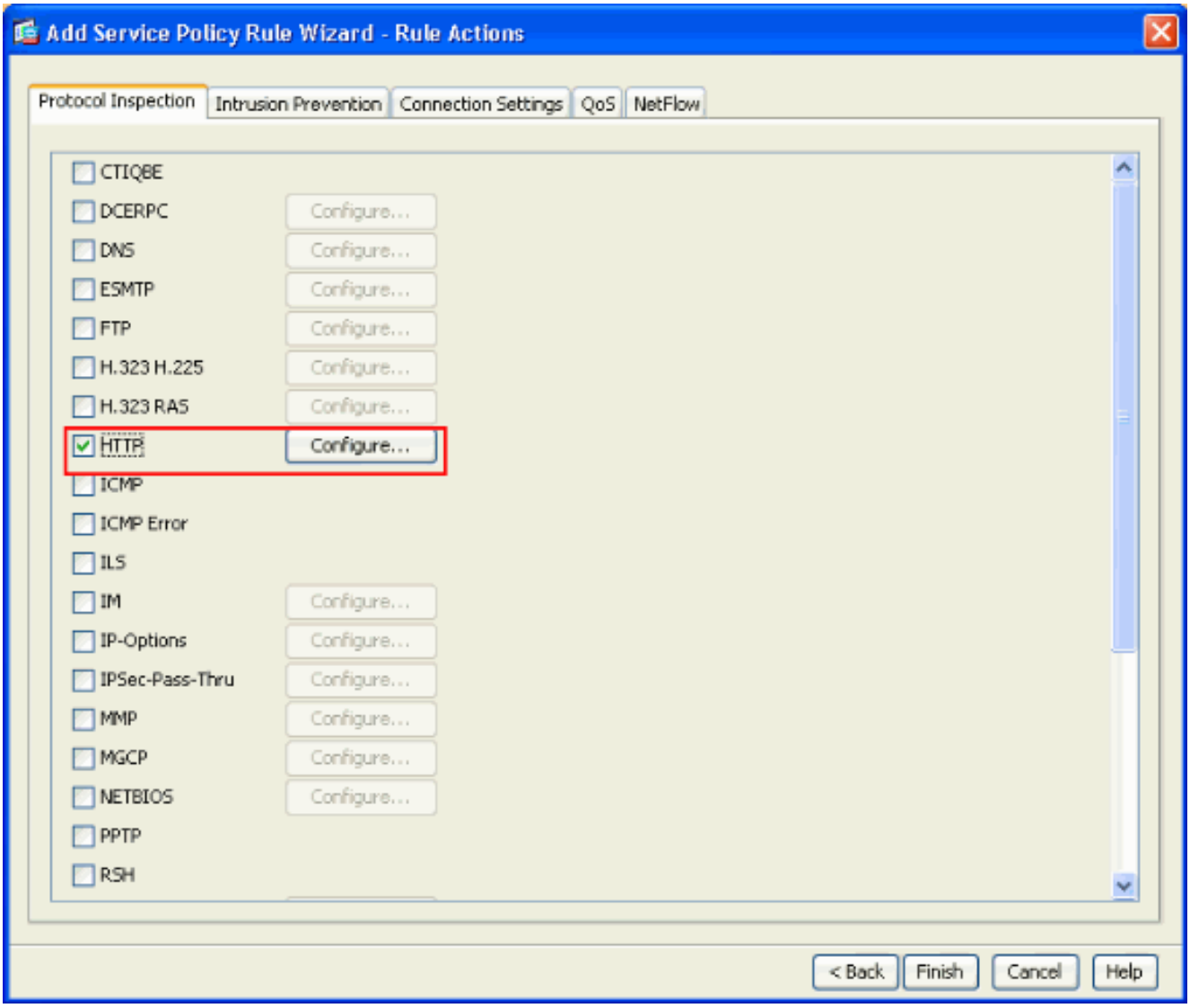

5. Da consultação preste serviços de manutenção ao indicador, escolhem o **HTTP** como o serviço. Então, **APROVAÇÃO do** clique.



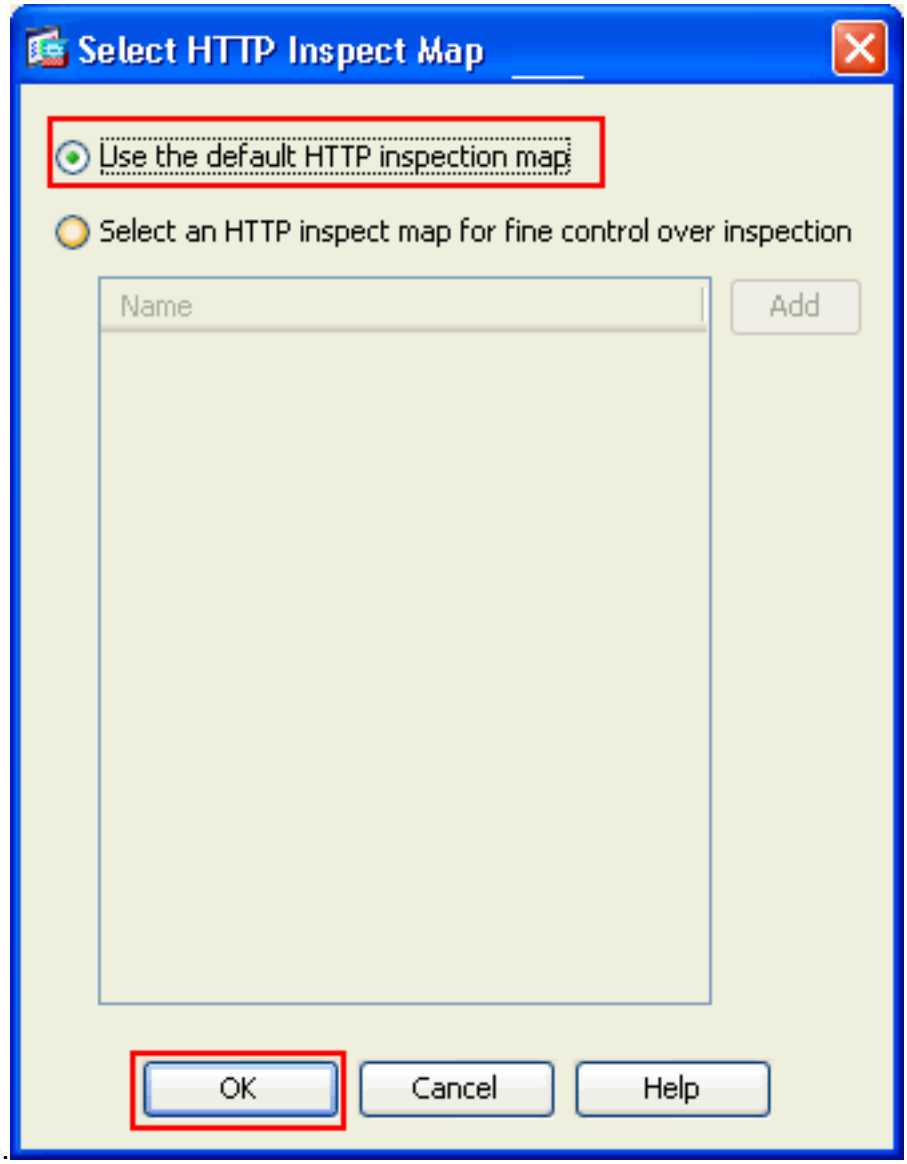

6. Do assistente da regra da política de serviços adicionar - Fósforo do tráfego - Indicador da porta do destino, você pode ver que o **serviço** escolhido é **tcp/HTTP**. Clique em Next.




7. Do assistente da regra da política de serviços adicionar - Ordene o indicador das ações, verifique a caixa de verificação ao lado do **HTTP**. Então, o clique **configura** ao lado do **HTTP**.

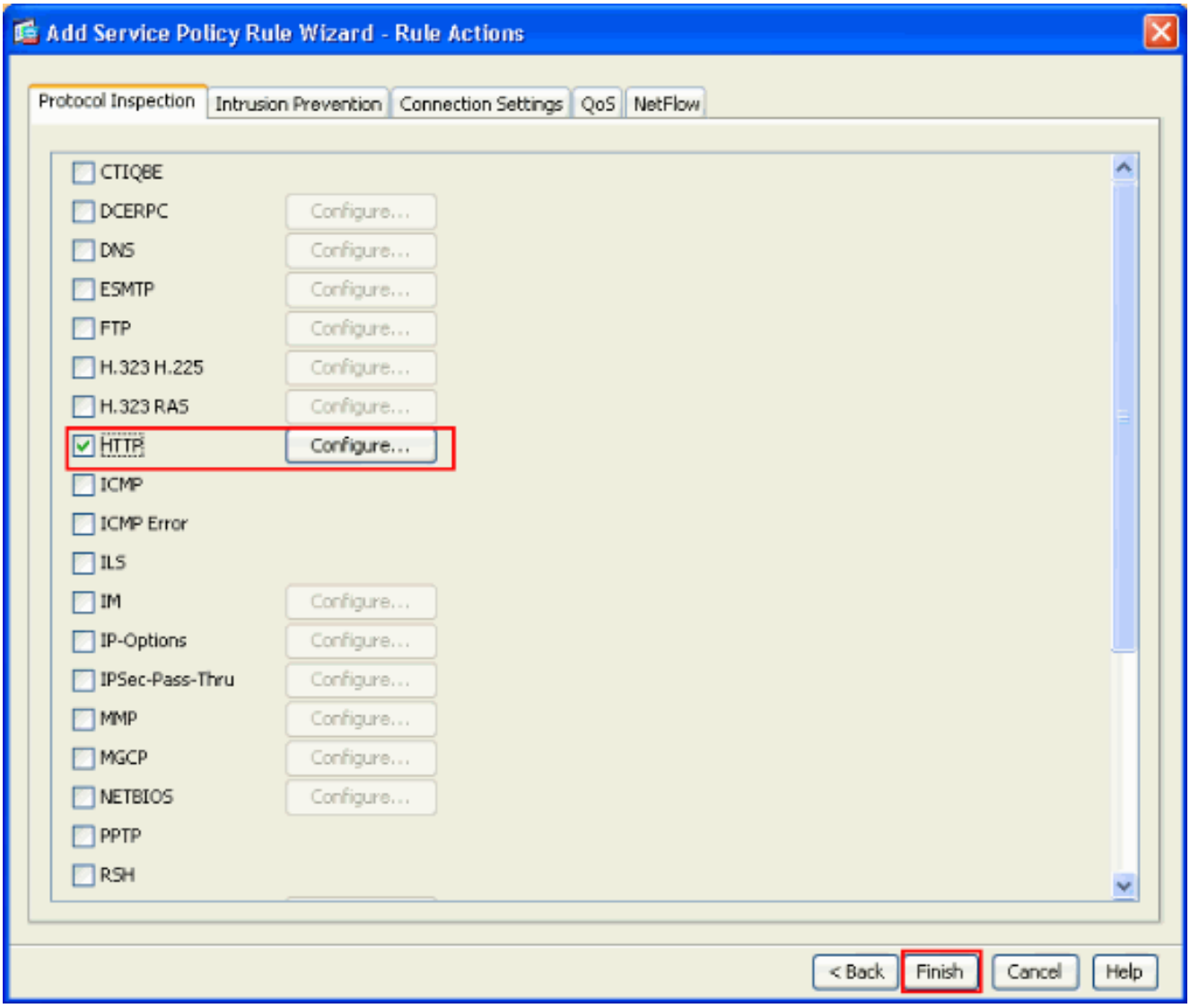



8. Do HTTP seleto inspecione o indicador do mapa, verificam o botão de rádio ao lado do **uso o mapa da inspeção do padrão HTTP**. A inspeção do padrão HTTP é usada neste exemplo. Então, **APROVAÇÃO do**

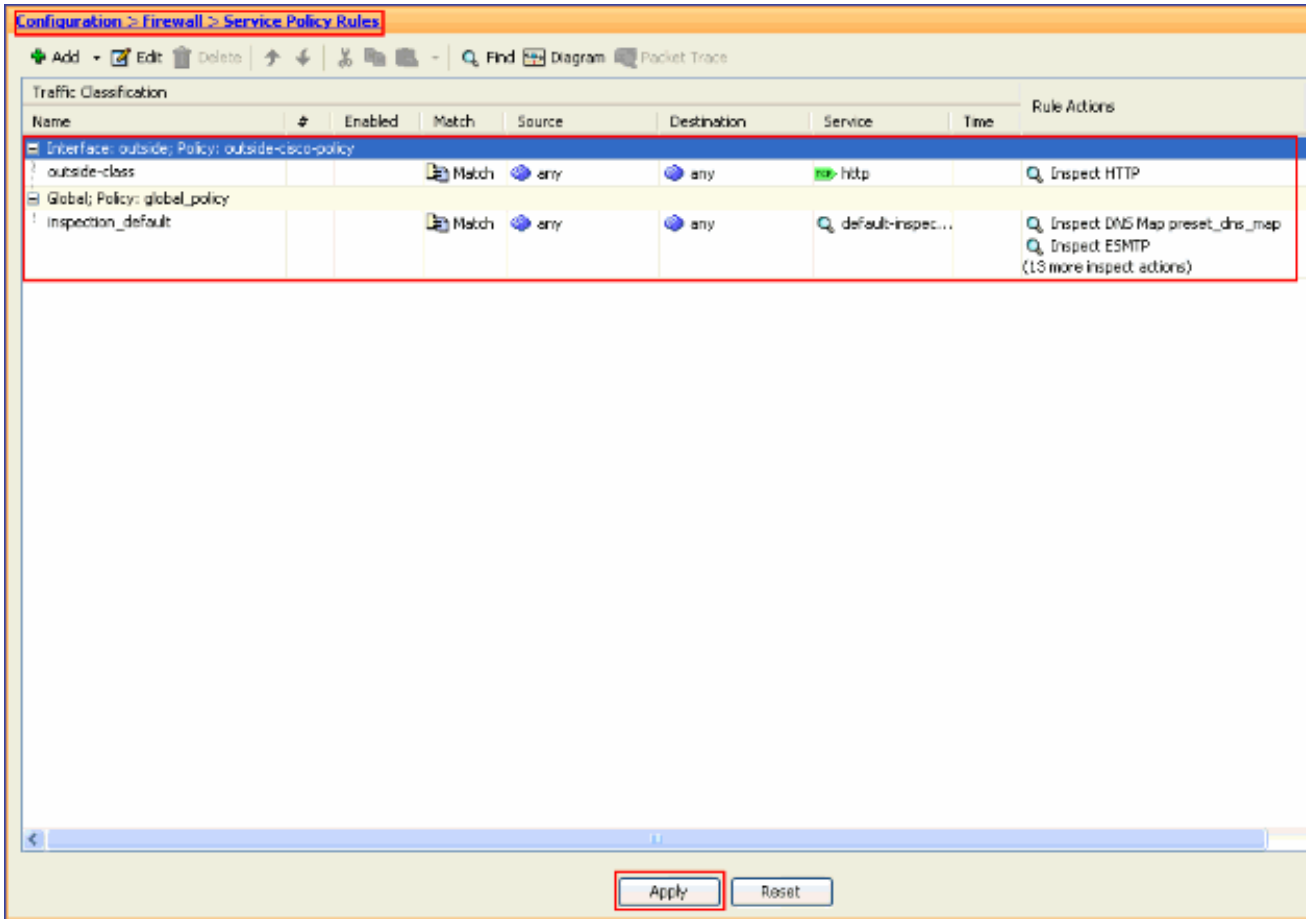



clique.

9. Clique em Finish.




10. Sob **regras da configuração > do Firewall > da política de serviços**, você verá a parte-Cisco-**política** recentemente configurada da política de serviços (para inspecionar o HTTP) junto com a política de serviço padrão já atual no dispositivo. O clique **aplica-se** a fim aplicar a configuração a Cisco
ASA.




# Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Adaptive Security Device Manager
- Solicitações de Comentários (RFCs)
- Aplicando a inspeção do protocolo de camada do aplicativo
- Suporte Técnico e Documentação - Cisco Systems