ASA/PIX 7.X: Desabilite a inspeção global do padrão e permita a inspeção de aplicativo não-padrão usando o ASDM

Índice

Introdução

Este documento descreve como remover a inspeção padrão da política global de um aplicativo e como habilitar a inspeção em um aplicativo fora do padrão.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na ferramenta de segurança adaptável de Cisco (ASA) essas corridas a imagem do software 7.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.

Produtos Relacionados

Esta configuração pode igualmente ser usada com a ferramenta de segurança PIX que executa a

imagem do software 7.x.

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 inspeções ao tráfego em todas as relações (uma política global). Não todas as inspeções 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.)

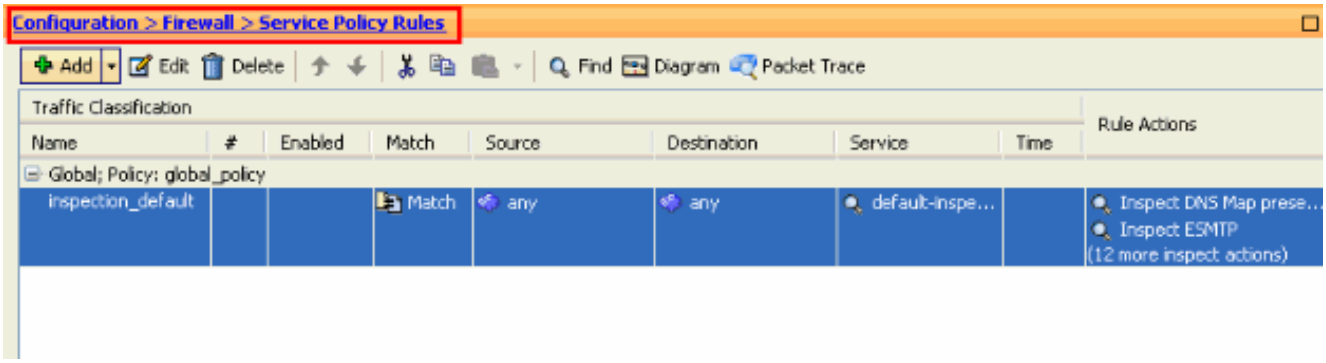
A configuração da política padrão inclui estes comandos:

```
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
```

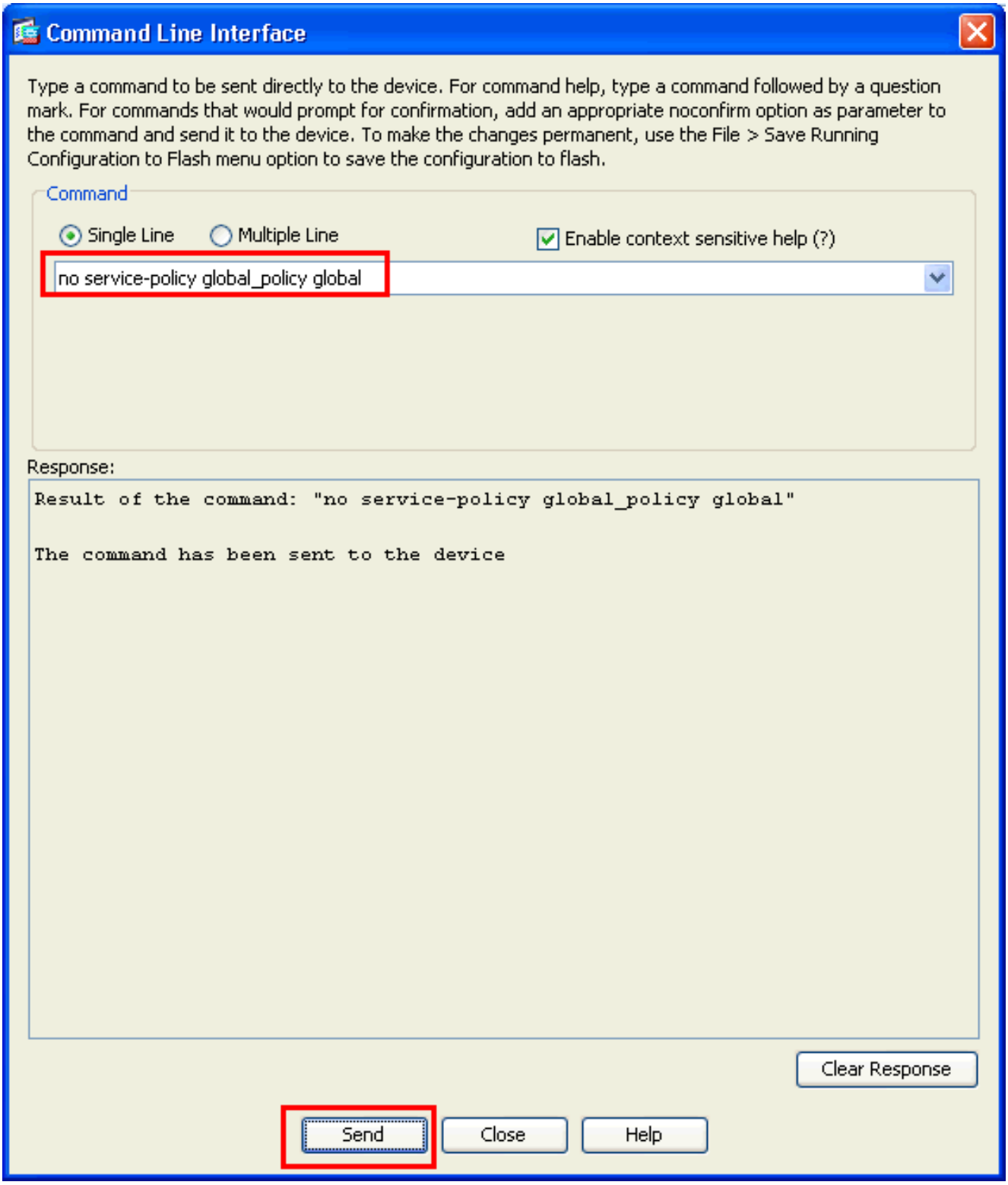
Permita a inspeção de aplicativo não-padrão

Termine este procedimento para permitir a inspeção de aplicativo não-padrão em Cisco ASA:

1. Entre ao **ASDM**. Vá às **regras da configuração > do Firewall > da política de serviços**.

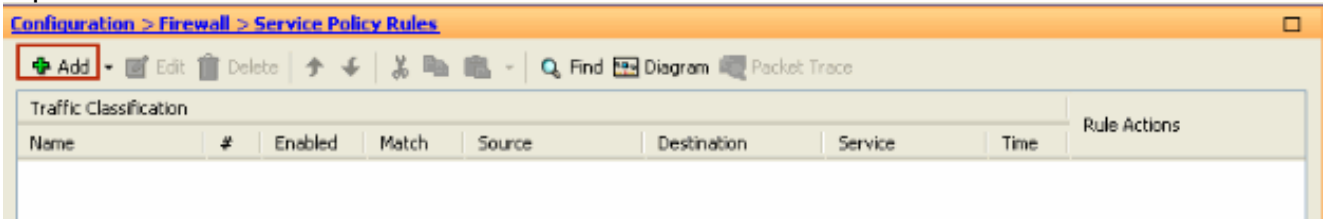


2. Se você quer manter a configuração para a política global que inclui o mapa de classe do padrão e o mapa de política do padrão, mas quer remover globalmente a política, vá às **ferramentas > à interface da linha de comando** e não use **nenhum comando global da global-política da serviço-política** remover globalmente a política. Então, o clique **envia** assim que o comando é aplicado ao
ASA.



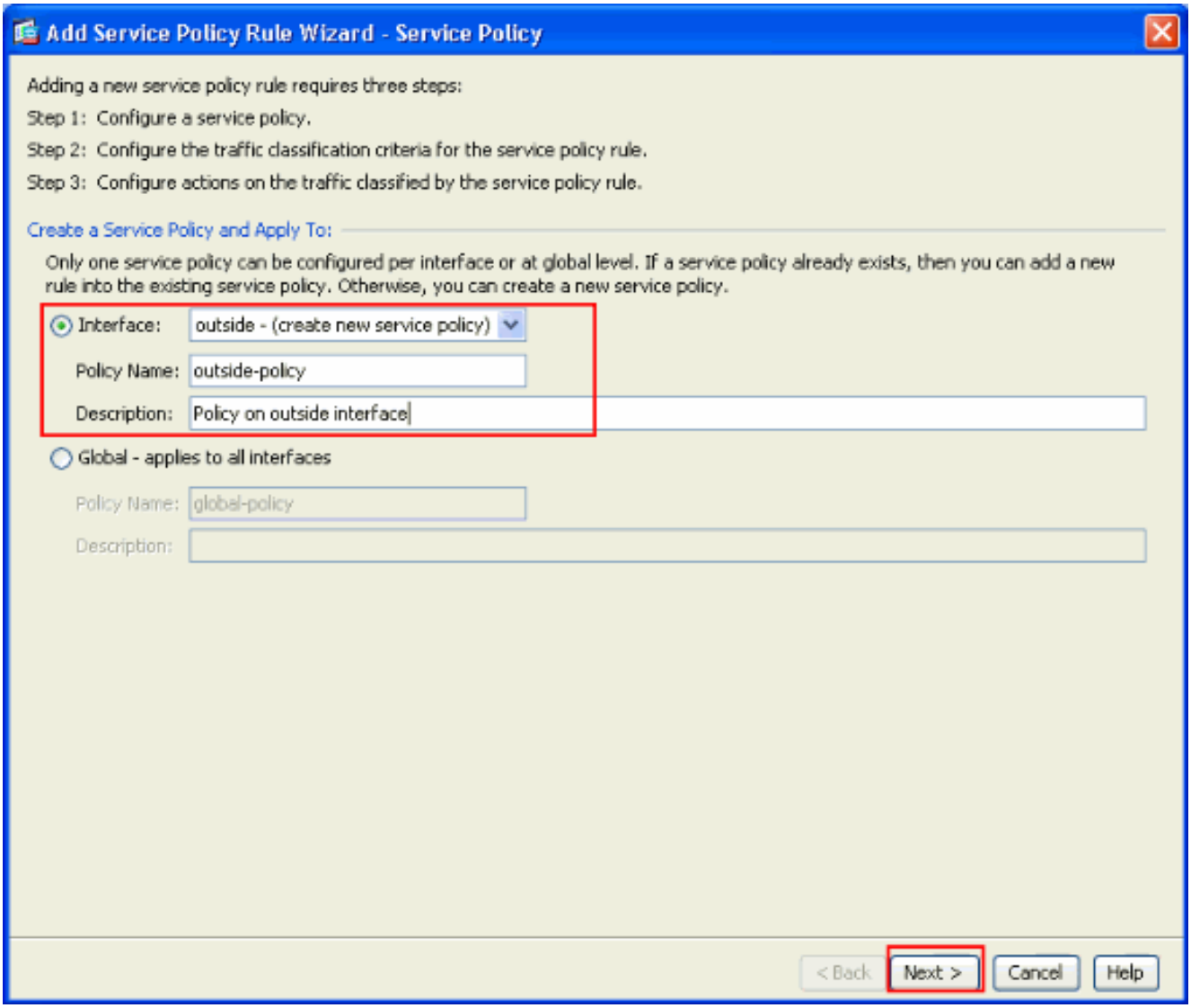
Nota: Com esta etapa a política global torna-se invisível no Security Device Manager adaptável (ASDM), mas é mostrada no CLI.

3. O clique **adiciona** a fim adicionar como mostrado uma política nova aqui:

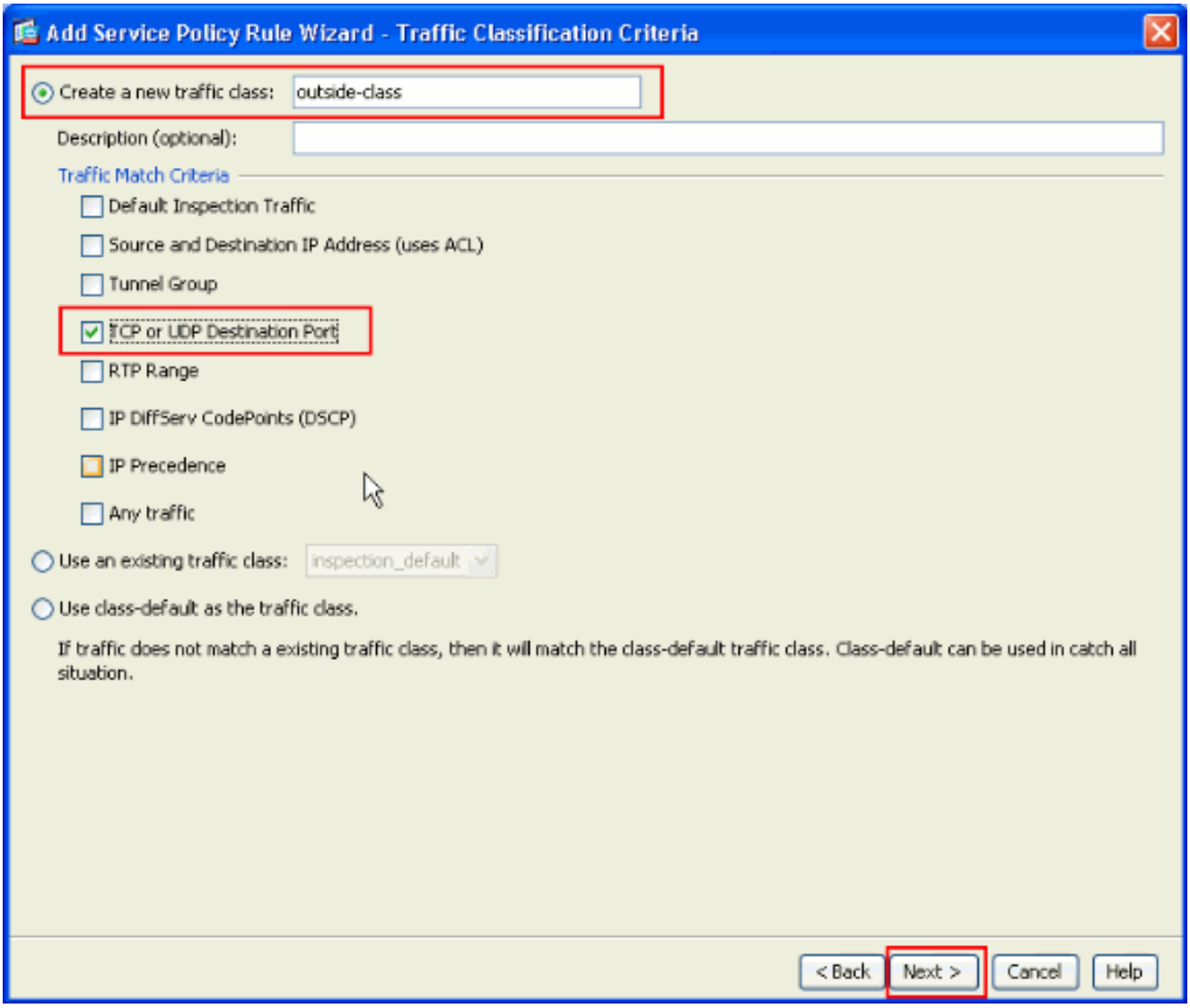


4. Certifique-se que o botão de rádio ao lado da **relação** está verificado e se escolha da relação que você quer aplicar a política do menu suspenso. Então, forneça o **nome da política** e a

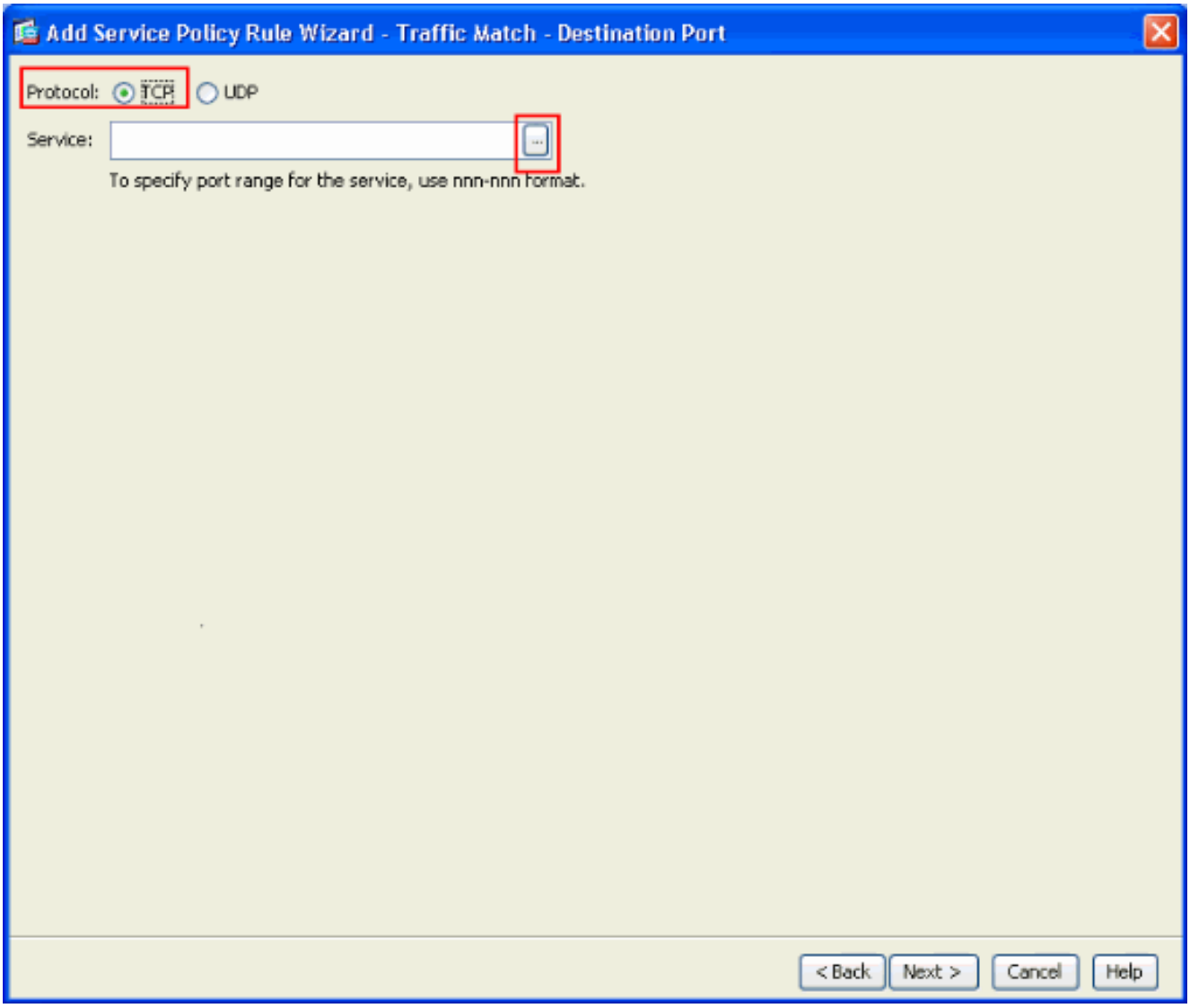
descrição. Clique em
Next.



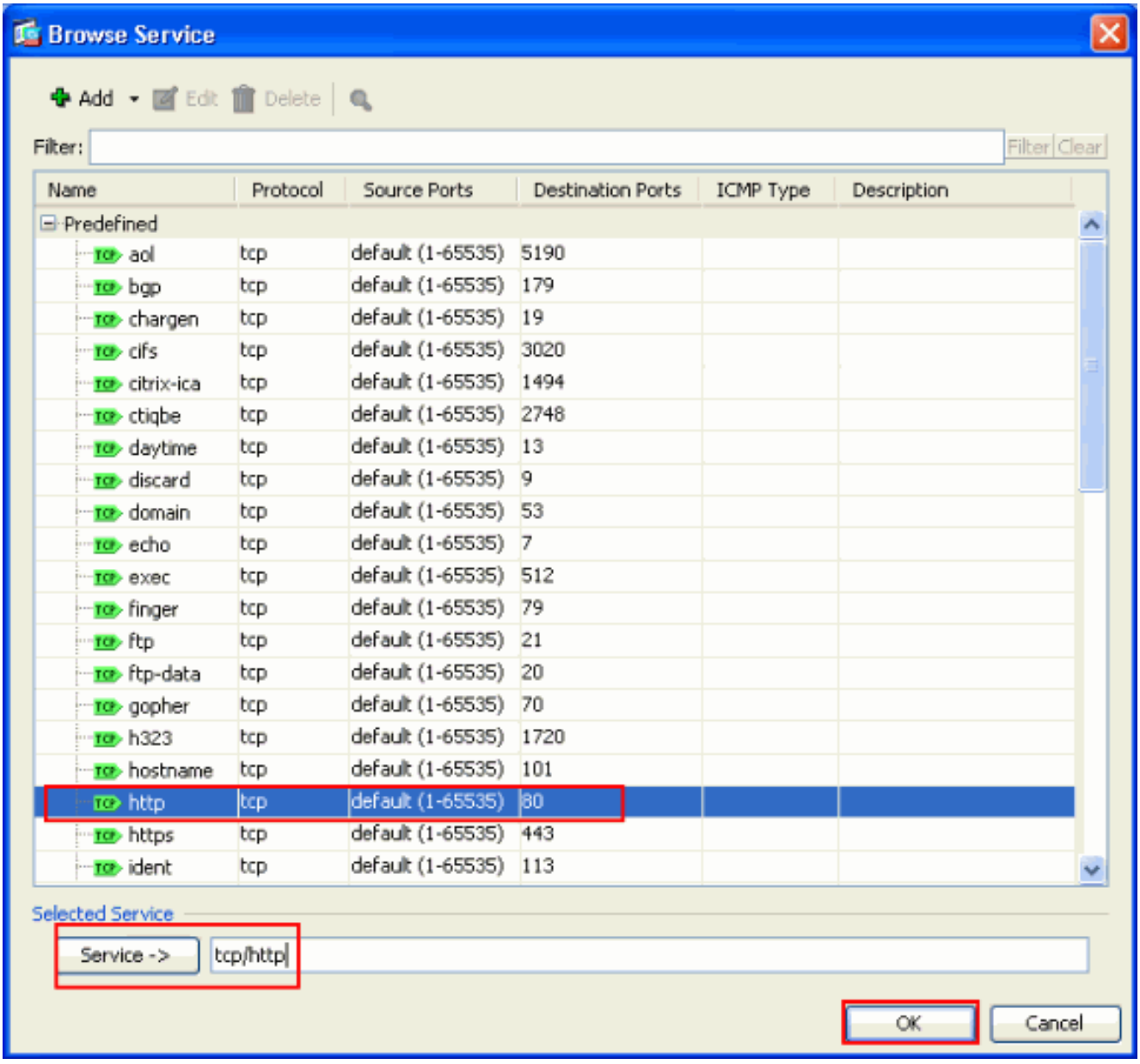
5. Crie um mapa de classe novo para combinar o **tráfego TCP** como o **HTTP** cai sob o TCP. Clique em
Next.



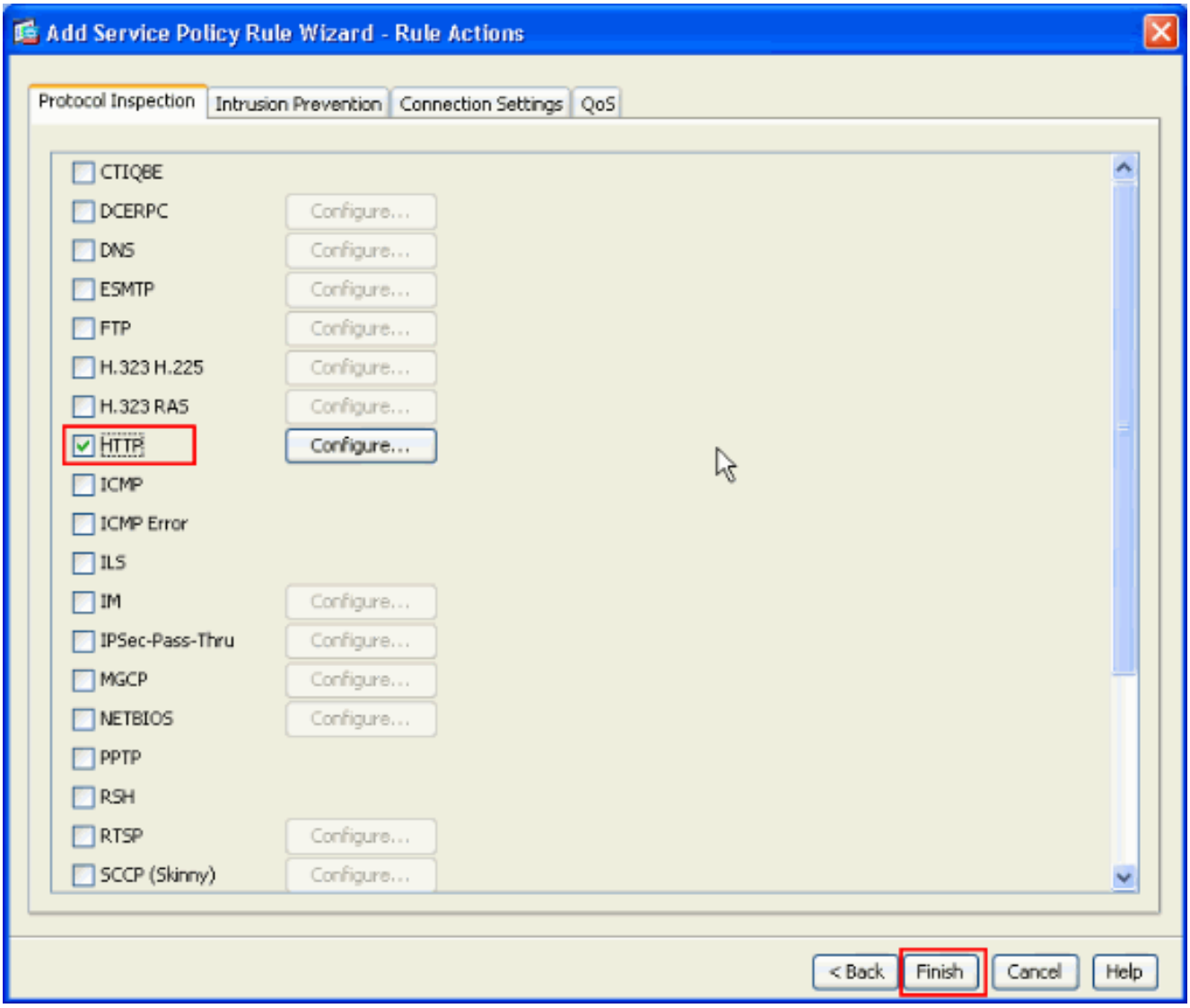
6. Escolha o **TCP** como o protocolo.



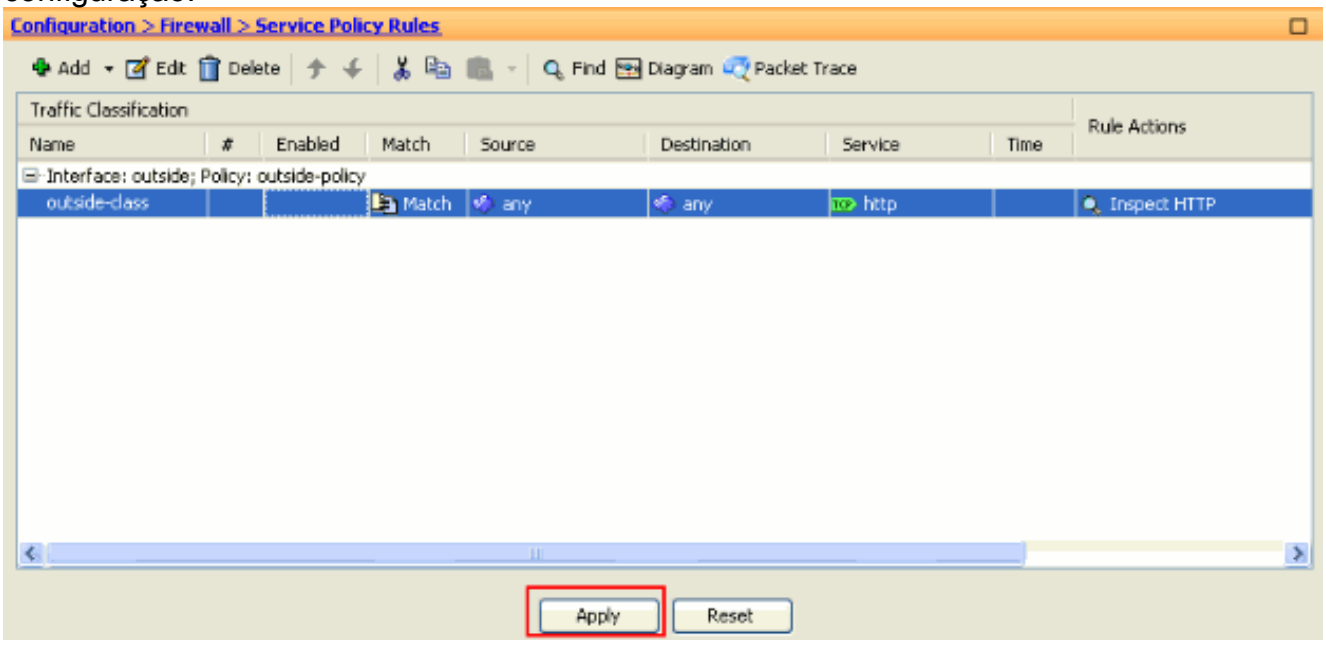
Escolha a **porta de HTTP 80** como o serviço e clique a **APROVAÇÃO**.



7. Escolha o **HTTP** e clique o **revestimento**.



8. O clique **aplica-se** para enviar estas alterações de configuração ao ASA do ASDM. Isto termina a configuração.



Verificar

Use estes **comandos show** verificar a configuração:

- Use o **comando class-map da corrida da mostra** ver os mapas da classe configurados.
```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class match port tcp eq www !
```
- Use o **comando policy-map da corrida da mostra** ver os mapas da política configurados.
```
ciscoasa# sh run policy-map
!
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
policy-map outside-policy description Policy on outside interface class outside-class
inspect http !
```
- Use o **comando service-policy da corrida da mostra** ver as políticas de serviços configuradas.
```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Referências de comandos do 5500 Series de Cisco ASA
- Página de suporte do Cisco Adaptive Security Device Manager (ASDM)
- Cisco PIX Firewall Software
- Solicitações de Comentários (RFCs)
- Cisco PIX 500 Series Security Appliances
- Aplicando a inspeção do protocolo de camada do aplicativo
- Referências do comando Cisco Secure PIX Firewall
- Suporte Técnico e Documentação - Cisco Systems