

ASA/PIX 7.X: Examen global predeterminado de la neutralización y Inspección de la aplicación no valor por defecto del permiso usando el ASDM

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Política global predeterminada](#)

[Inspección de la aplicación del no valor por defecto del permiso](#)

[Verificación](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo quitar la inspección predeterminada de la política global para una aplicación y cómo habilitar la inspección para una aplicación no predeterminada.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información en este documento se basa en el dispositivo de seguridad adaptante de Cisco (ASA) esos funcionamientos la imagen del software 7.x.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Productos Relacionados](#)

Esta configuración se puede también utilizar con el dispositivo de seguridad PIX que funciona con

la imagen del software 7.x.

Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

Omita la política global

Por abandono, la configuración incluye una directiva que haga juego todo el tráfico del examen de la aplicación predeterminada y aplique ciertos exámenes al tráfico en todas las interfaces (una política global). No todos los exámenes se habilitan por abandono. Usted puede aplicar solamente una política global. Si usted quiere alterar la política global, usted debe editar la política predeterminada o inhabilitarla y aplicar un nuevo. (Una directiva de la interfaz reemplaza la política global.)

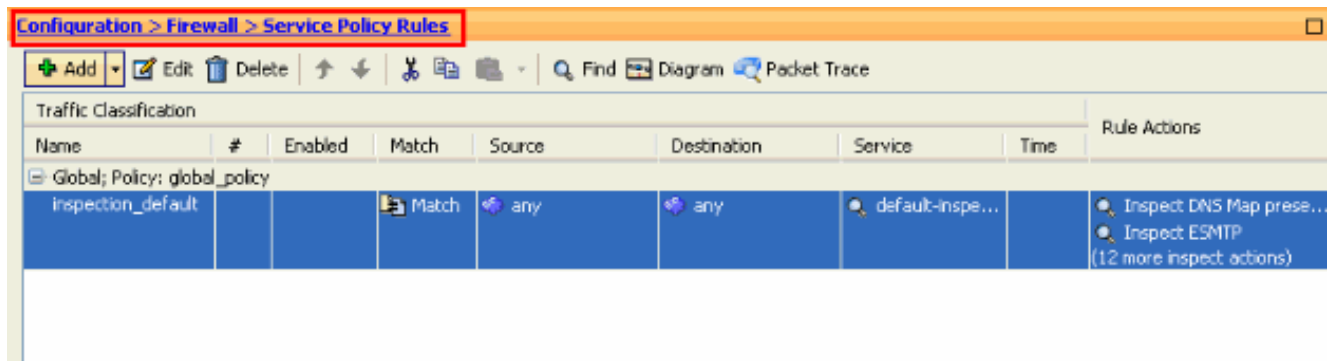
La configuración de la política predeterminada incluye estos comandos:

```
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
```

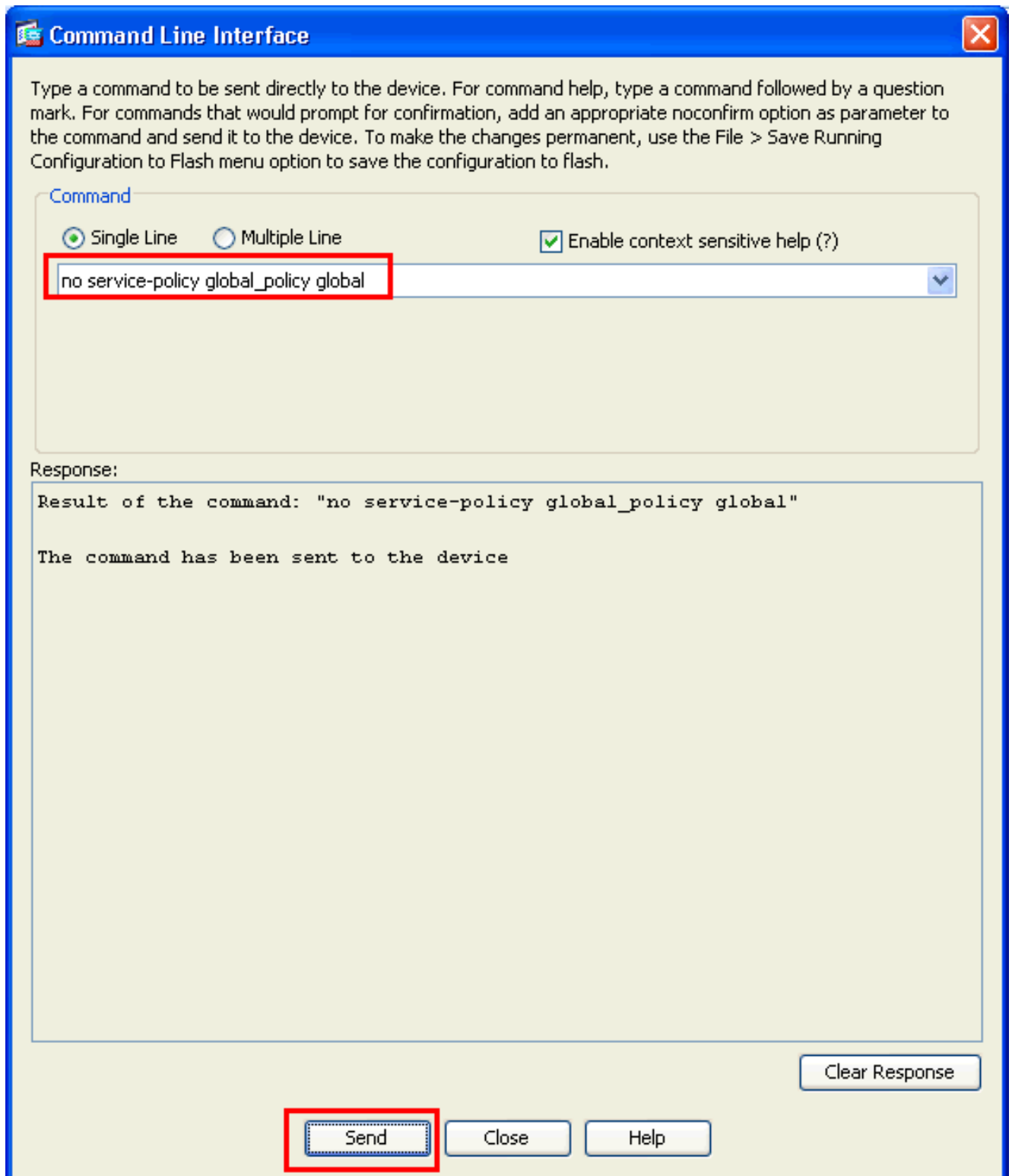
Inspección de la aplicación del no valor por defecto del permiso

Complete este procedimiento para habilitar la Inspección de la aplicación no valor por defecto en Cisco ASA:

1. Inicie sesión al ASDM. Vaya a las **reglas de la configuración > del Firewall > de la política de servicio**.

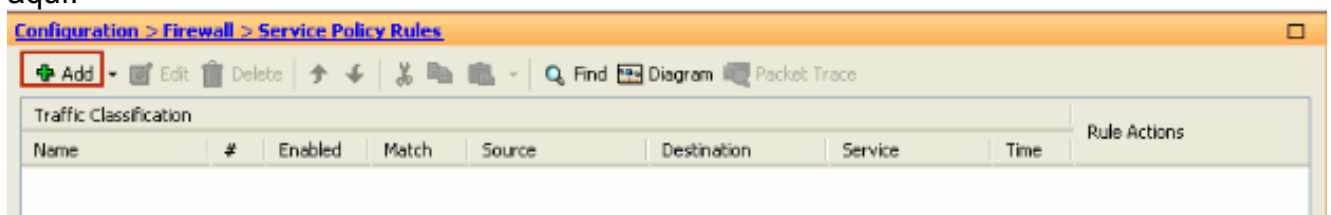


2. Si usted quiere guardar la configuración para la política global que incluye el Clase-mapa predeterminado y el Directiva-mapa del valor por defecto, pero quiere quitar la directiva global, vaya a las **herramientas > a la interfaz de línea de comando** y no utilice el **ningún comando global de la política global de la servicio-directiva** de quitar la directiva global. Entonces, el tecleo **envía** así que el comando se aplica al ASA.



Nota: Con este paso la política global llega a ser invisible en el Administrador de dispositivos de seguridad adaptante (ASDM), pero se muestra en el CLI.

3. El tecleo **agrega** para agregar una nueva directiva como se muestra aquí:



4. Asegurese el botón de radio al lado de la **interfaz** se marca y eligen la interfaz que usted quiere aplicar la directiva del menú desplegable. Entonces, proporcione el **nombre de la**

directiva y la descripción. Haga clic en Next (Siguiete).

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: outside - (create new service policy) ▼

Policy Name: outside-policy

Description: Policy on outside interface

Global - applies to all interfaces

Policy Name: global-policy

Description:

< Back **Next >** Cancel Help

5. Cree un nuevo clase-mapa para hacer juego **tráfico TCP** como el **HTTP** baja bajo el TCP. Haga clic en Next (Siguiete).

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

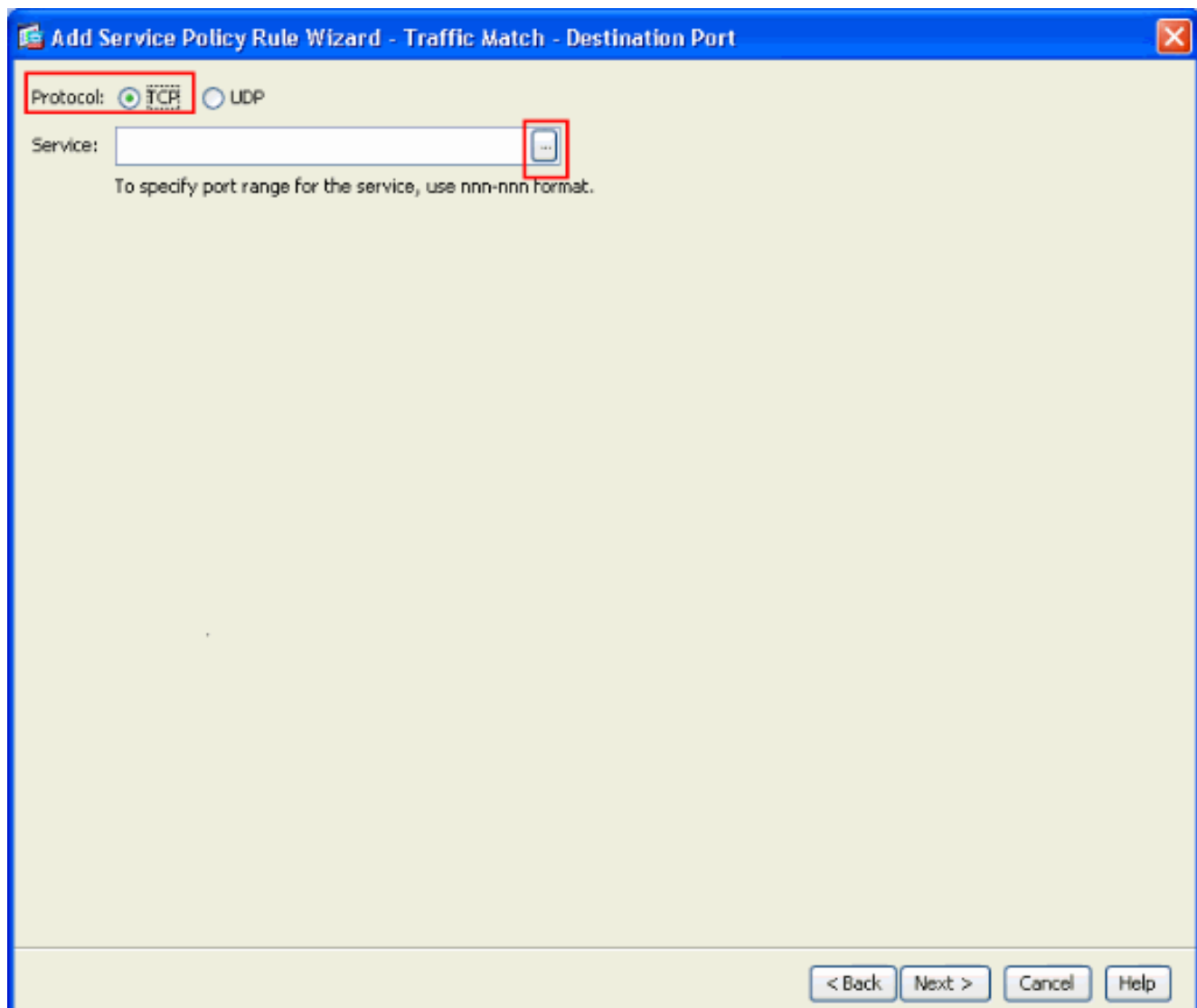
Use an existing traffic class:

Use class-default as the traffic class.

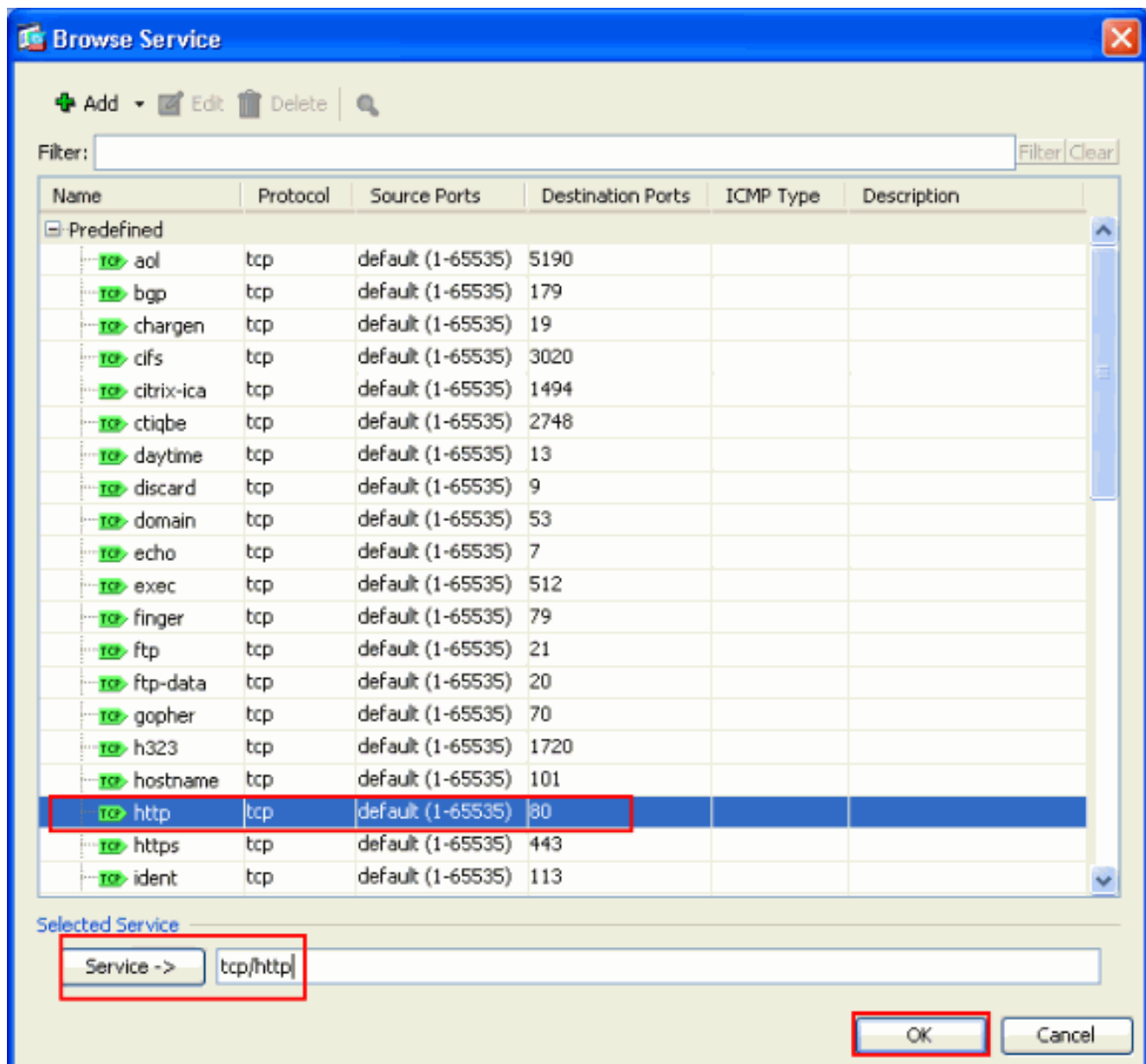
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

< Back **Next >** Cancel Help

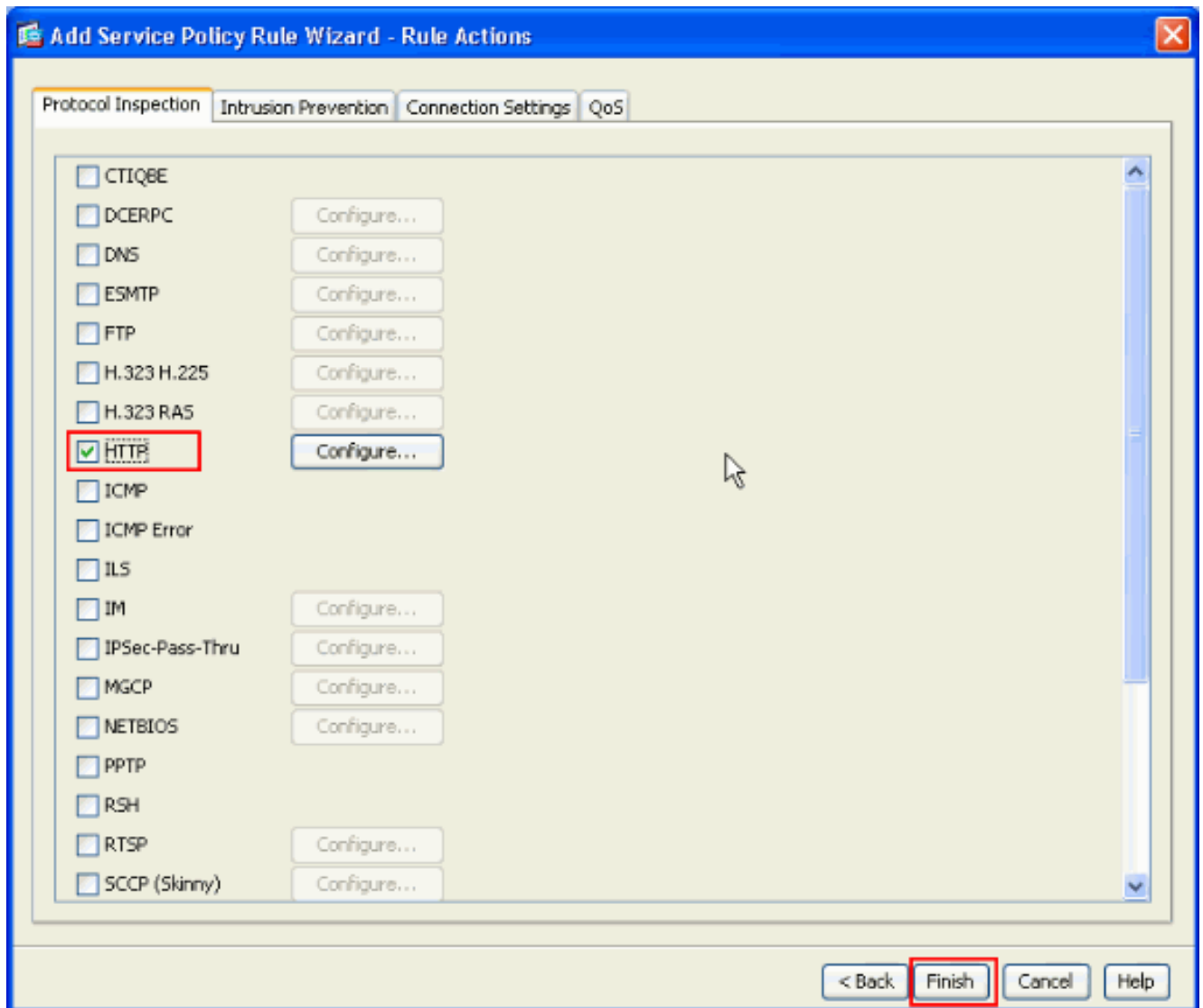
6. Elija el **TCP** como el protocolo.



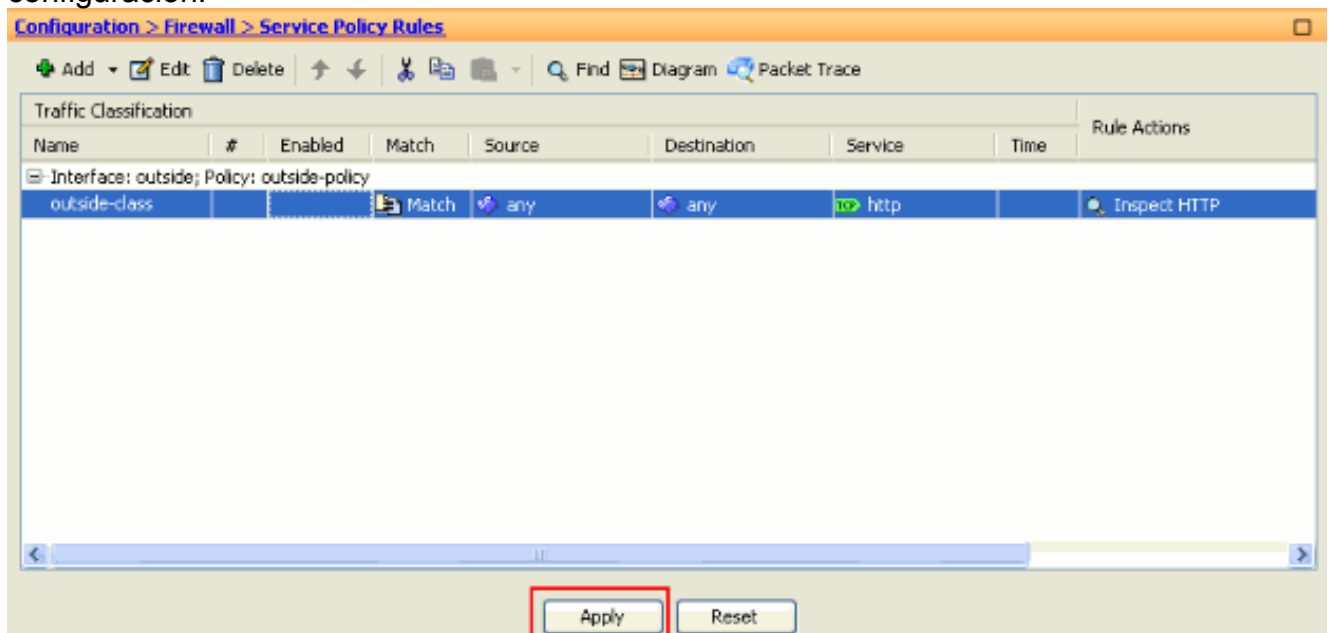
Elija el puerto HTTP 80 como el servicio y haga clic la **AUTORIZACIÓN**.



7. Elija el HTTP y el clic en Finalizar.



8. El tecleo **se aplica** para enviar estos cambios de configuración al ASA del ASDM. Esto completa la configuración.



Verificación

Utilice estos comandos show de verificar la configuración:

- Utilice el comando **class-map** del funcionamiento de la demostración de ver las correspondencias de la clase configuradas.

```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class match port tcp eq www !
```

- Utilice el comando **policy-map** del funcionamiento de la demostración de ver las correspondencias de políticas configuradas.

```
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 !
```

- Utilice el comando **service-policy** del funcionamiento de la demostración de ver las políticas de servicio configuradas.

```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

[Información Relacionada](#)

- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Referencias de comandos de las 5500 Series de Cisco ASA](#)
- [Página de soporte del Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Cisco PIX Firewall Software](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Dispositivos de seguridad Cisco PIX de la serie 500](#)
- [Aplicación del examen del Application Layer Protocol](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)