ASA 8.3 y posterior - Configuración de la inspección mediante ASDM

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para Cisco Adaptive Security Appliance (ASA) con las versiones 8.3(1) y posteriores sobre cómo eliminar la inspección predeterminada de la política global para una aplicación y cómo habilitar la inspección para una aplicación no predeterminada mediante Adaptive Security Device Manager (ASDM).

Consulte PIX/ASA 7.x: Inhabilite la Inspección Global Predeterminada y Enable Non-Default Application Inspection para la misma configuración en Cisco ASA con las versiones 8.2 y anteriores.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en la versión 8.3(1) del Cisco ASA Security Appliance Software con 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.

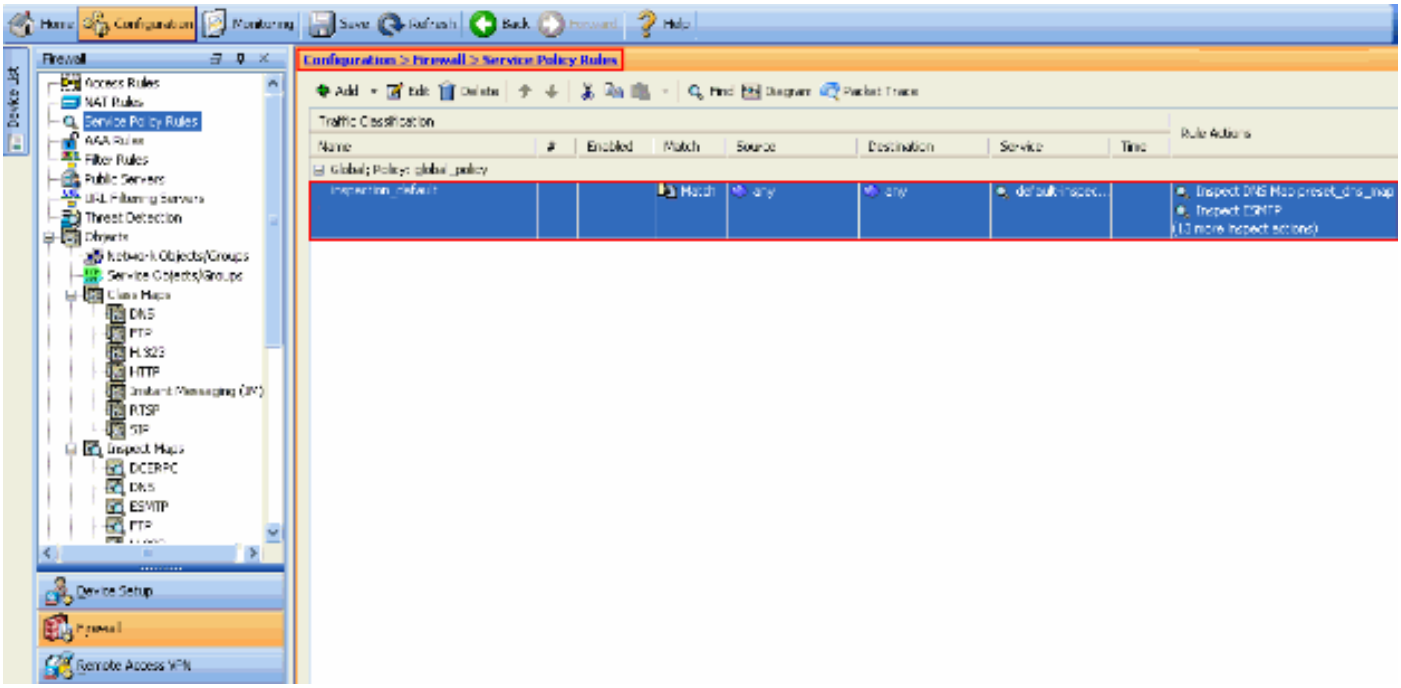
Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Política global predeterminada

De forma predeterminada, la configuración incluye una política que coincide con todo el tráfico de inspección de aplicaciones predeterminado y aplica ciertas inspecciones al tráfico en todas las interfaces (una política global). No todas las inspecciones están habilitadas de forma predeterminada. Sólo puede aplicar una política global. Si desea modificar la directiva global, debe editar la directiva predeterminada o desactivarla y aplicar una nueva. (Una política de interfaz invalida la política global.)

En ASDM, elija **Configuration > Firewall > Service Policy Rules** para ver la política global predeterminada que tiene la inspección de aplicación predeterminada como se muestra aquí:

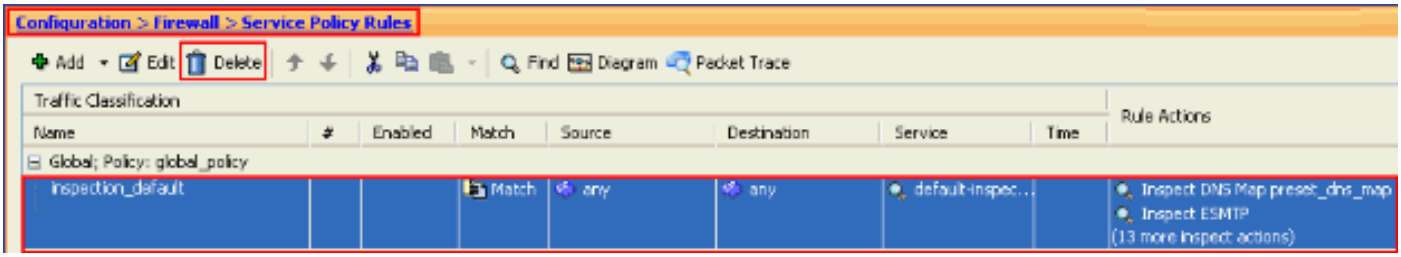


La configuración de política predeterminada incluye estos comandos:

```
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
```

Si necesita inhabilitar la política global, utilice el comando **no service-policy global_policy**. Para eliminar la política global usando ASDM elija **Configuration > Firewall > Service Policy Rules**. A continuación, seleccione la política global y haga clic en **Eliminar**.



Nota: Cuando elimina la política de servicio con ASDM, se eliminan la política asociada y los mapas de clase. Sin embargo, si se elimina la política de servicio mediante CLI, sólo se quita la política de servicio de la interfaz. El mapa de clase y el mapa de política permanecen inalterados.

Inhabilitar la inspección global predeterminada para una aplicación

Para inhabilitar la inspección global para una aplicación, utilice la versión *no* del comando **inspect**.

Por ejemplo, para quitar la inspección global de la aplicación FTP a la que escucha el dispositivo de seguridad, utilice el comando **no inspect ftp** en el modo de configuración de clase.

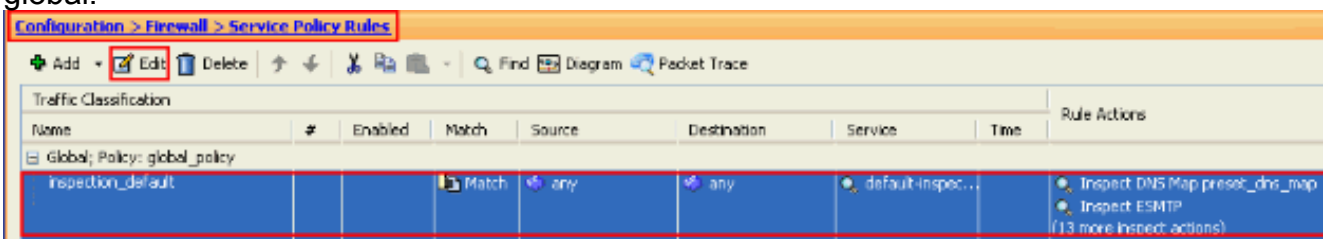
Se puede acceder al modo de configuración de clase desde el modo de configuración de policy map. Para quitar la configuración, utilice la forma *no* del comando.

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

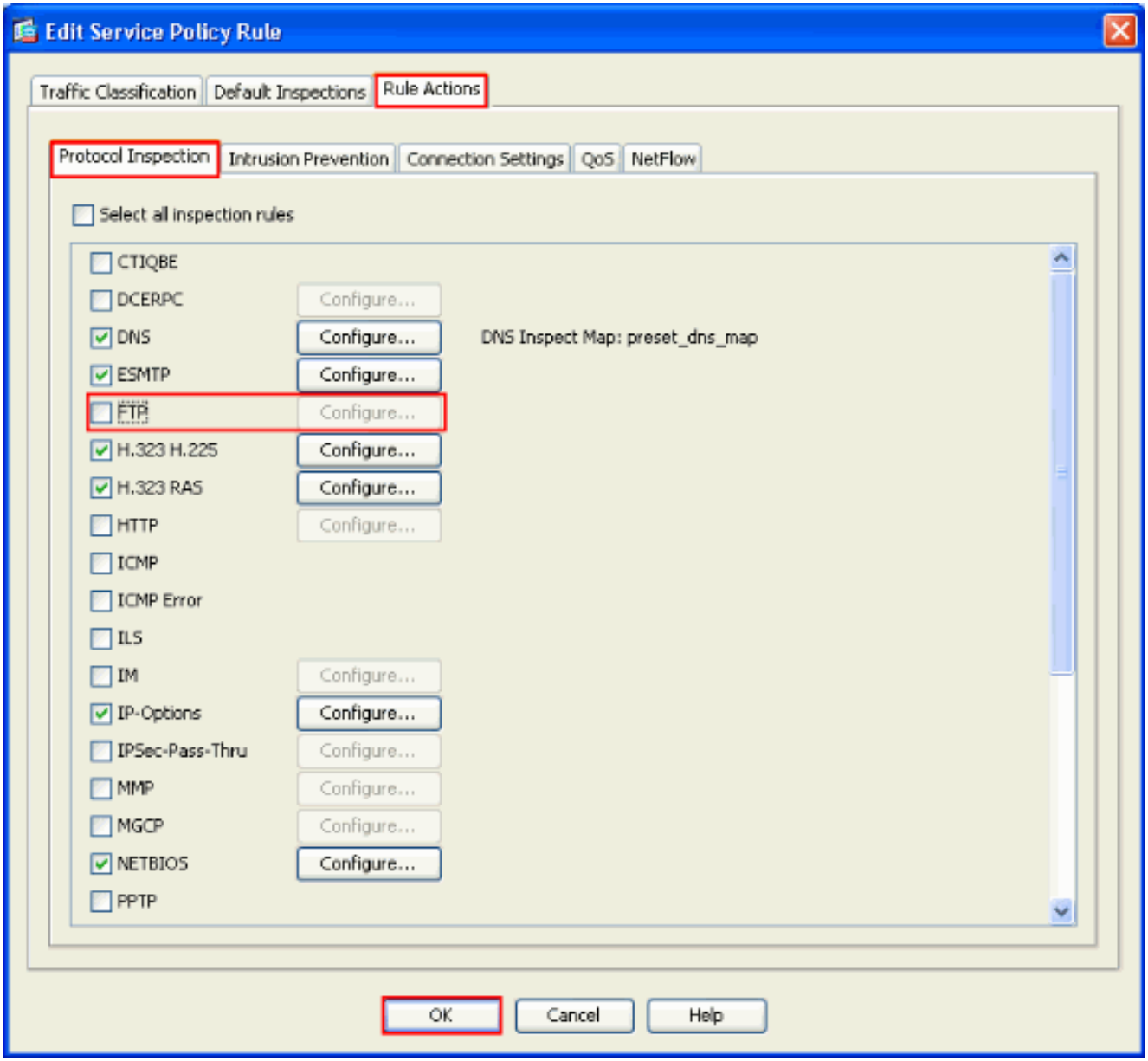
Para inhabilitar la inspección global para FTP mediante ASDM, complete estos pasos:

Nota: Refiérase a Permiso de Acceso HTTPS para ASDM para la configuración básica para acceder al PIX/ASA a través de ASDM.

1. Elija **Configuration > Firewall > Service Policy Rules** y seleccione la política global predeterminada. A continuación, haga clic en **Editar** para editar la directiva de inspección global.



2. En la ventana Edit Service Policy Rule, elija **Protocol Inspection** en la **ficha Rule Actions**. Asegúrese de que la casilla de verificación **FTP** esté desactivada. Esto inhabilita la inspección FTP como se muestra en la siguiente imagen. A continuación, haga clic en **Aceptar** y, a continuación,
Aplicar.



Nota: Para obtener más información sobre la inspección de FTP, consulte PIX/ASA 7.x: Ejemplo de Configuración de Enable FTP/TFTP Services.

Habilitar inspección para aplicación no predeterminada

La inspección HTTP mejorada está desactivada de forma predeterminada. Para habilitar la inspección HTTP en global_policy, utilice el **comando inspect http** bajo class inspection_default.

En este ejemplo, cualquier conexión HTTP (tráfico TCP en el puerto 80) que entre en el dispositivo de seguridad a través de cualquier interfaz se clasifica para la inspección HTTP. *Debido a que la política es una política global, la inspección ocurre sólo cuando el tráfico entra en cada interfaz*.

```
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
```

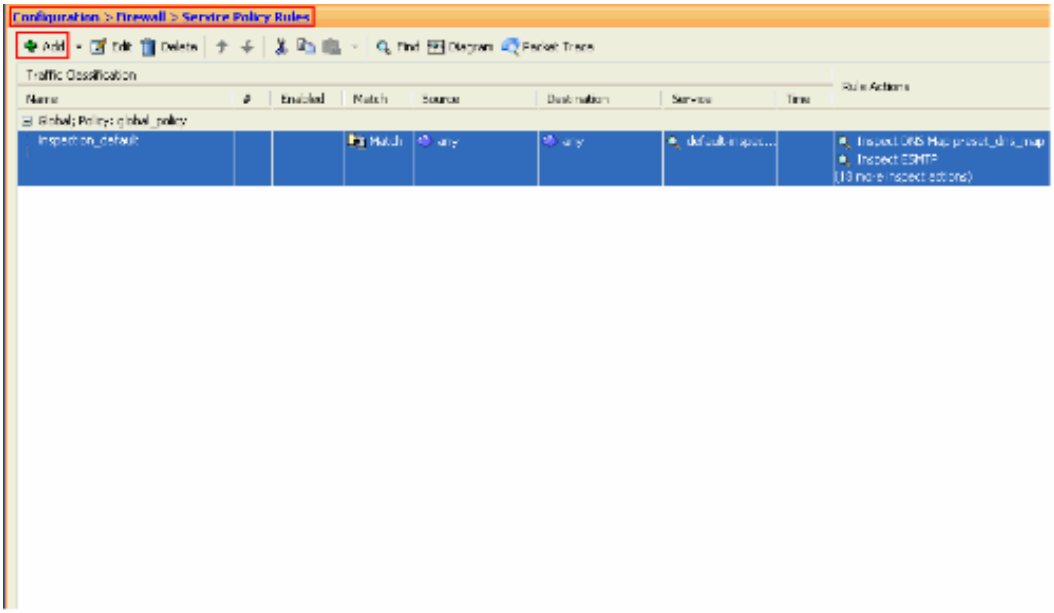
En este ejemplo, cualquier conexión HTTP (tráfico TCP en el puerto 80) que entre o salga del

dispositivo de seguridad a través de la *interfaz externa se clasifica para la inspección HTTP*.

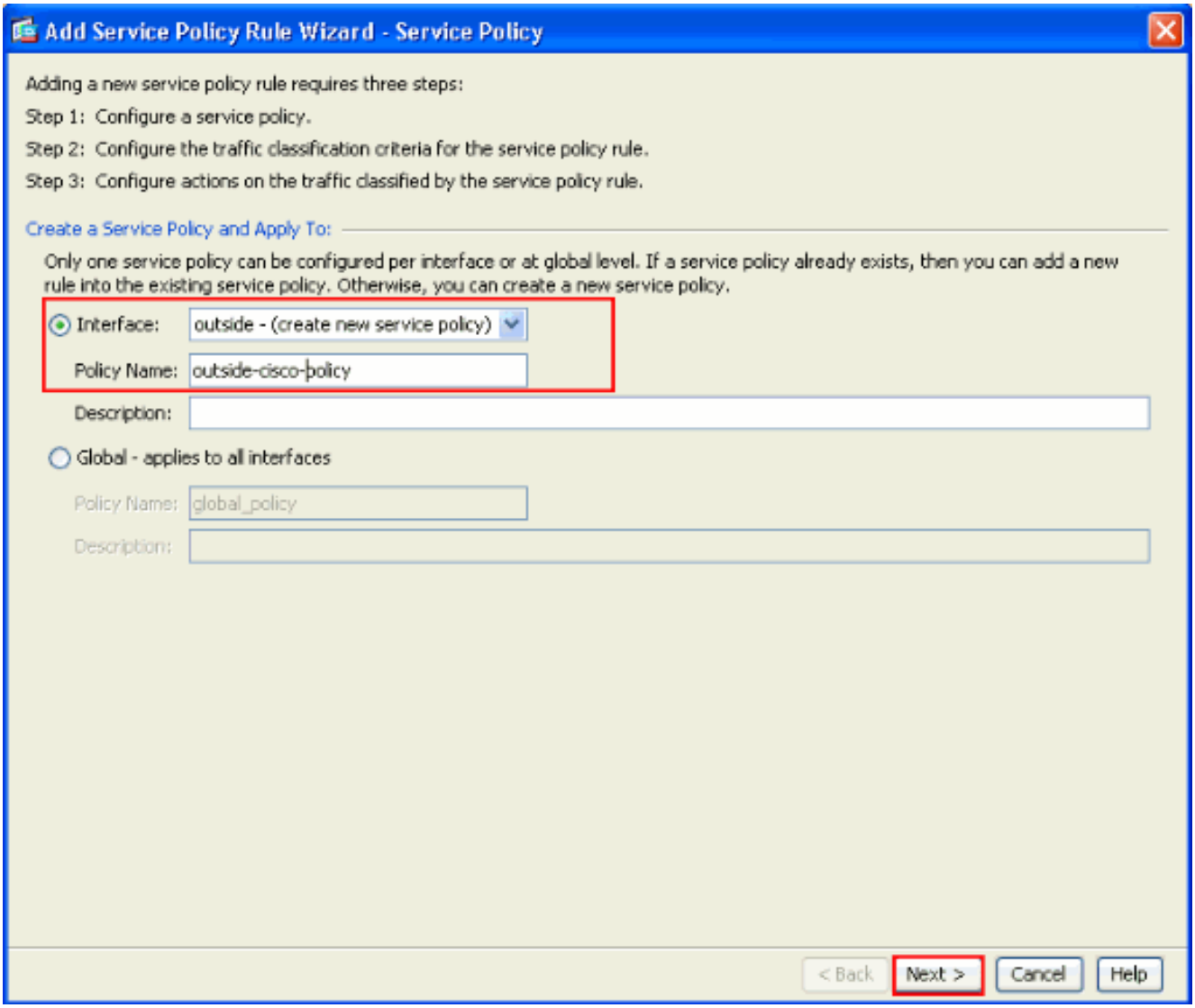
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Realice estos pasos para configurar el ejemplo anterior usando ASDM:

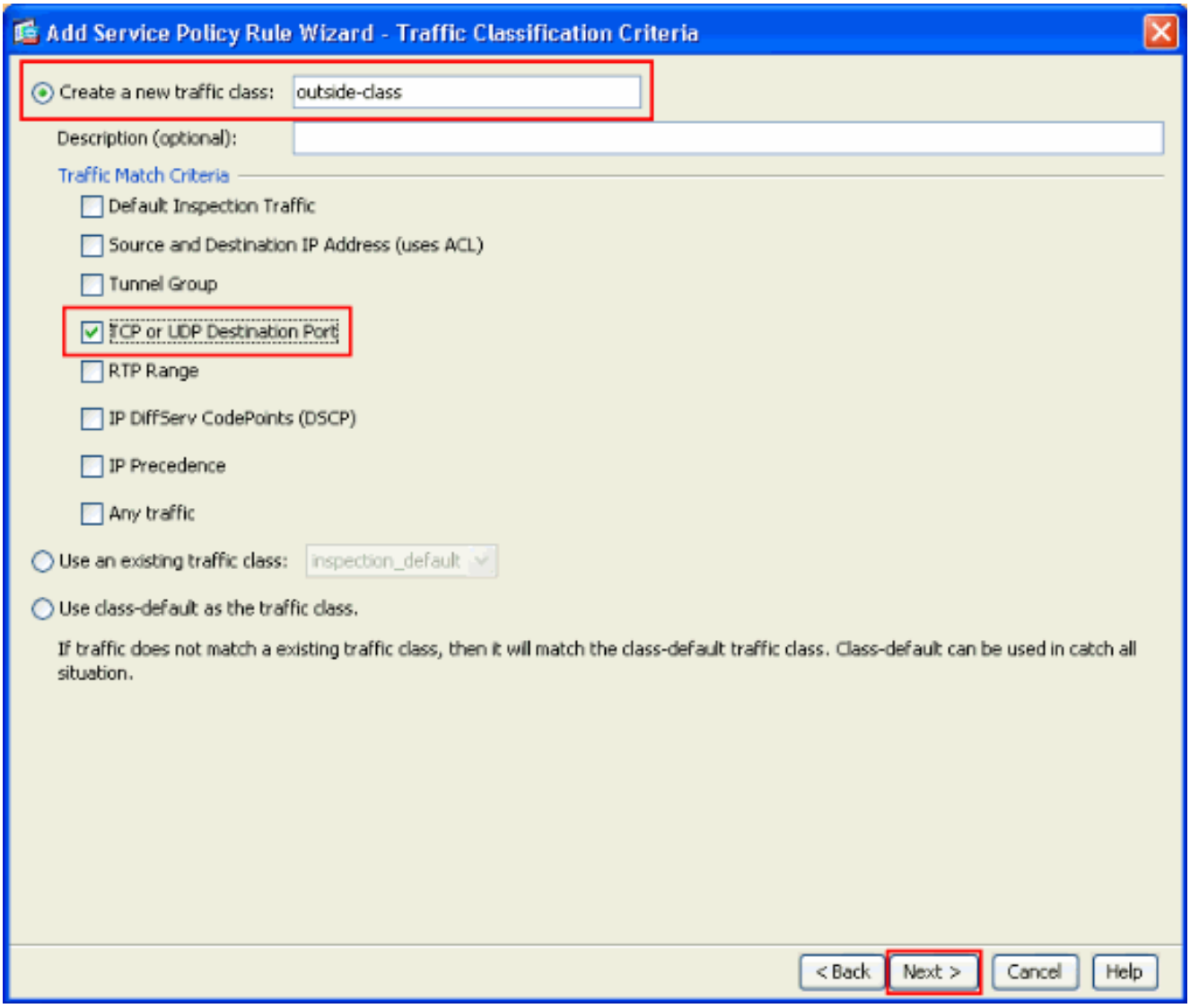
1. Elija **Configuration > Firewall > Service Policy Rules** y haga clic en **Add** para agregar una nueva política de servicio:



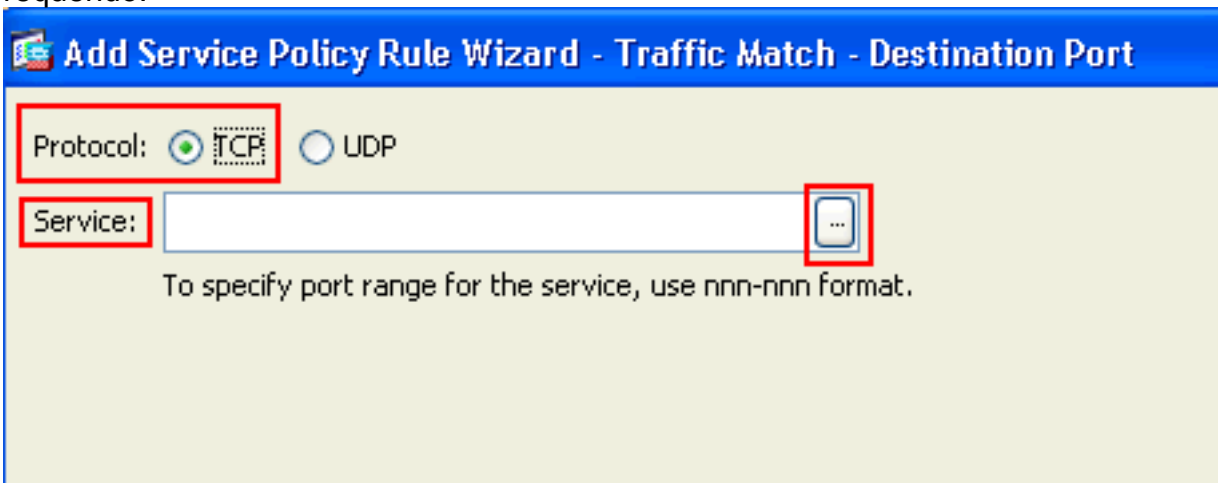
2. En la ventana Asistente para agregar reglas de política de servicio - Política de servicio, elija el botón de opción junto a **Interfaz**. Esto aplica la política creada a una interfaz específica, que es la interfaz **externa** en este ejemplo. Proporcione un nombre de política, que es **outside-cisco-policy** en este ejemplo. Haga clic en Next (Siguiente).



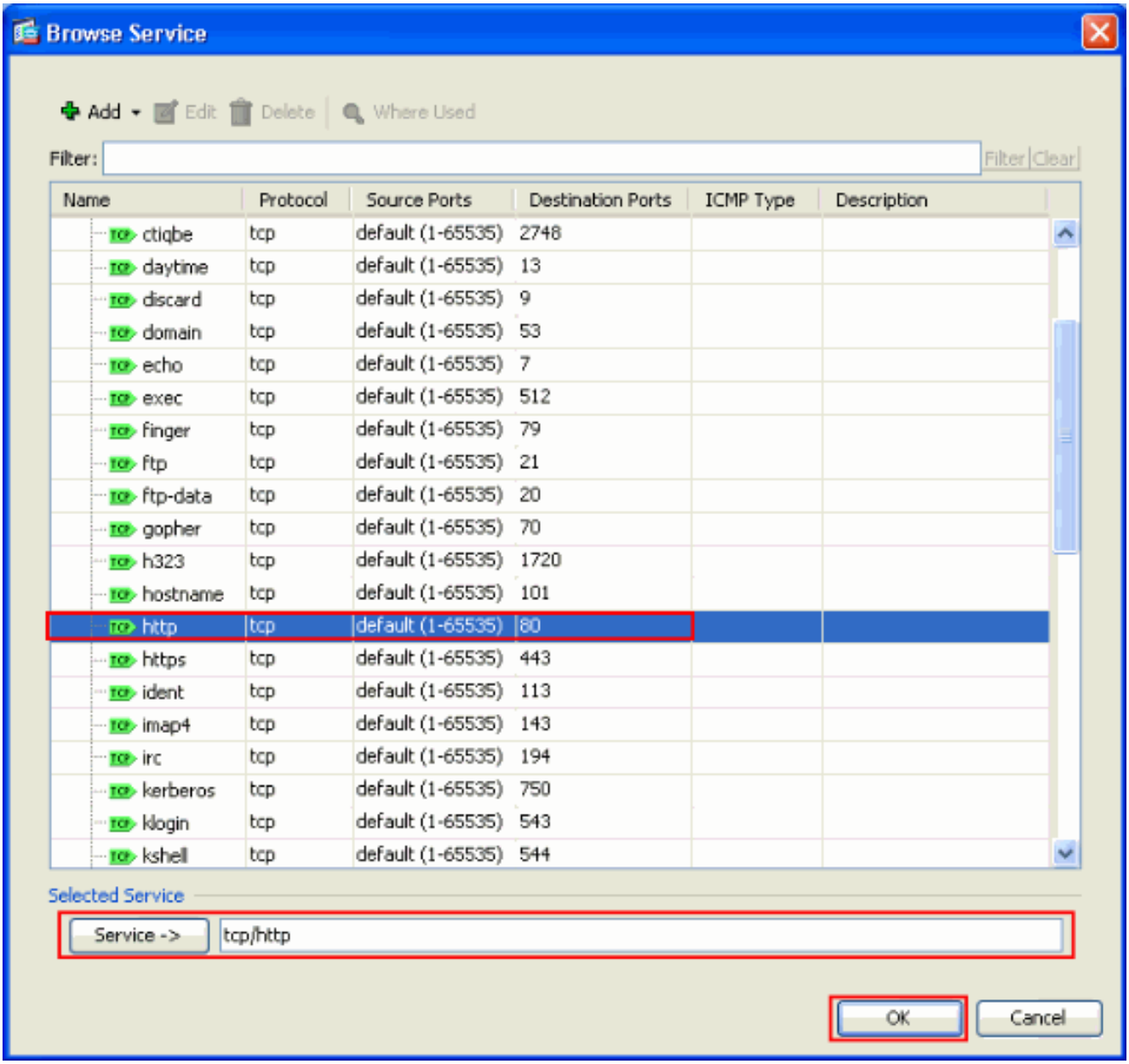
3. En la ventana Asistente para agregar reglas de política de servicio - Criterios de clasificación de tráfico, proporcione el nuevo nombre de clase de tráfico. El nombre utilizado en este ejemplo es **outside-class**. Asegúrese de que la casilla de verificación junto a **TCP o UDP Destination Port** esté marcada y haga clic en **Next**.



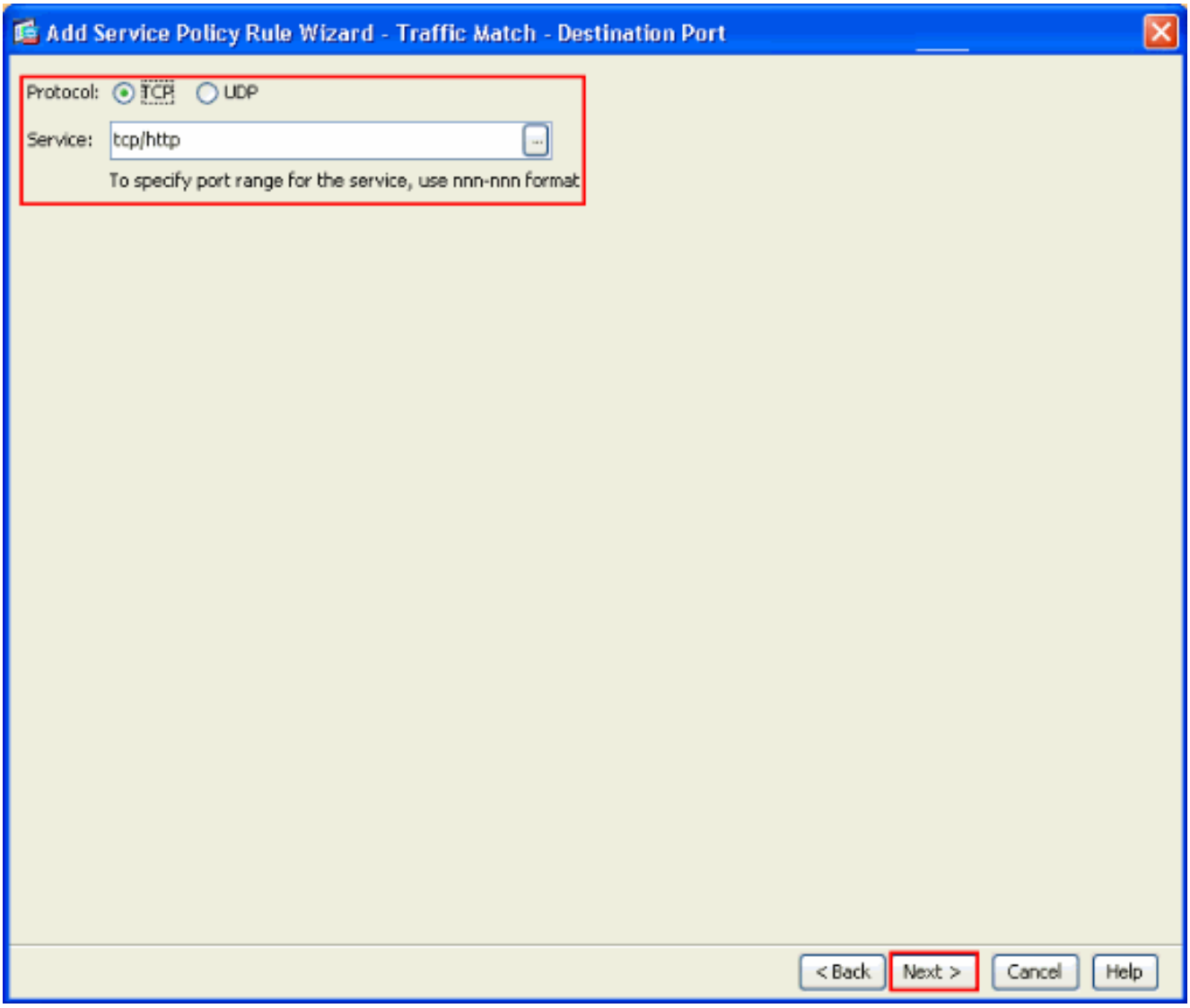
4. En la ventana Add Service Policy Rule Wizard - Traffic Match - Destination Port , elija el botón de opción situado junto a **TCP** en la sección **Protocol**. A continuación, haga clic en el botón situado junto a **Servicio** para elegir el servicio requerido.



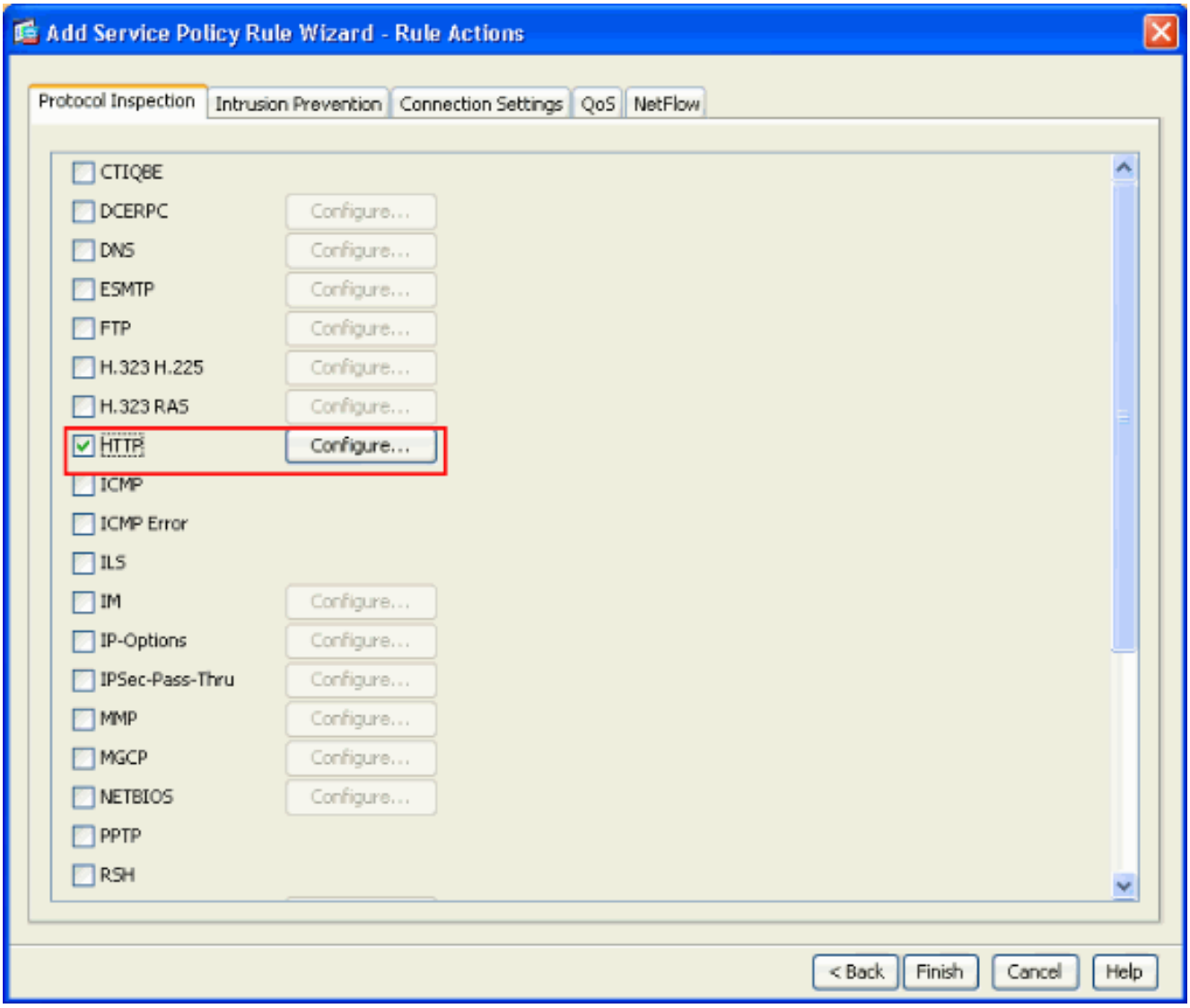
5. En la ventana Browse Service, elija **HTTP** como servicio. A continuación, haga clic en **Aceptar**.



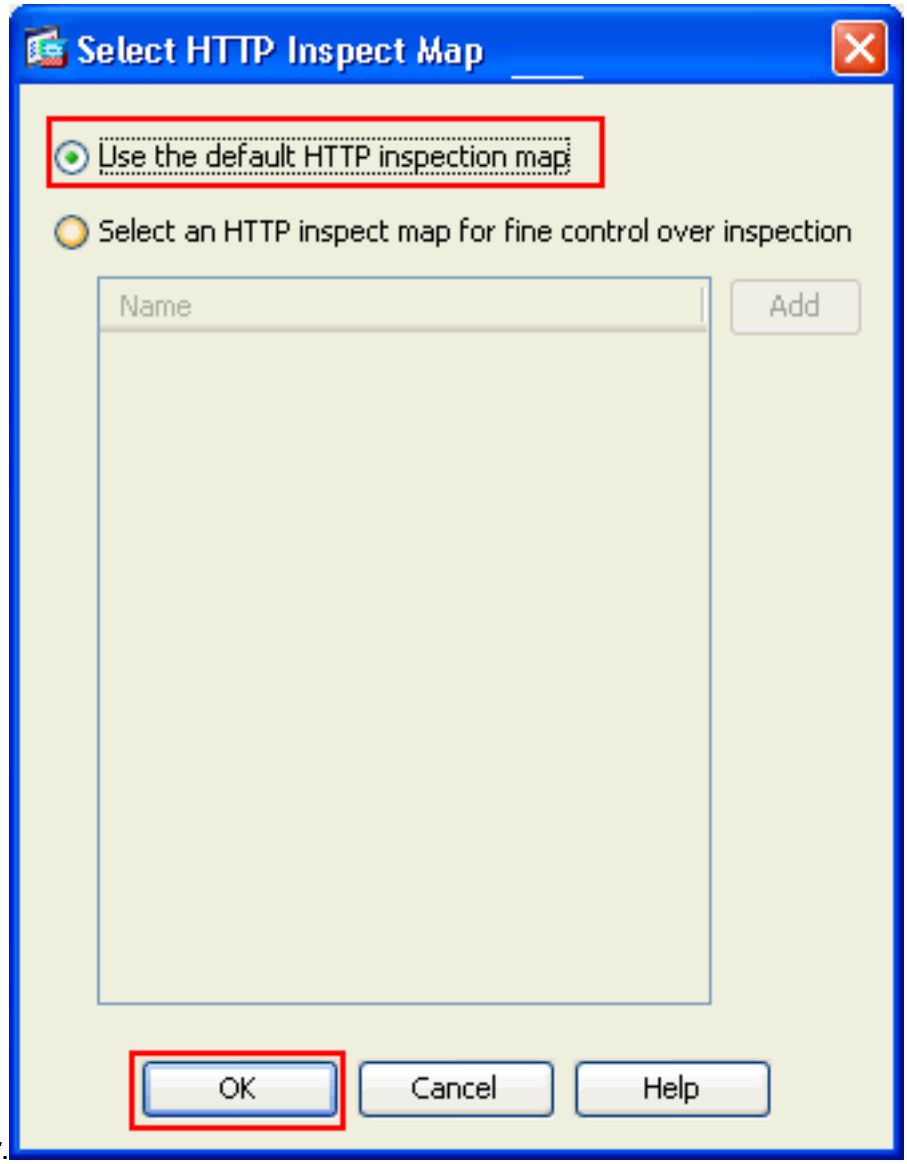
6. En la ventana Asistente para agregar reglas de política de servicio - Coincidencia de tráfico - Puerto de destino, puede ver que el **servicio** elegido es **tcp/http**. Haga clic en Next (Siguiente).



7. En la ventana Asistente para agregar reglas de política de servicio - Acciones de regla, active la casilla de verificación situada junto a **HTTP**. A continuación, haga clic en **Configurar** junto a
HTTP.

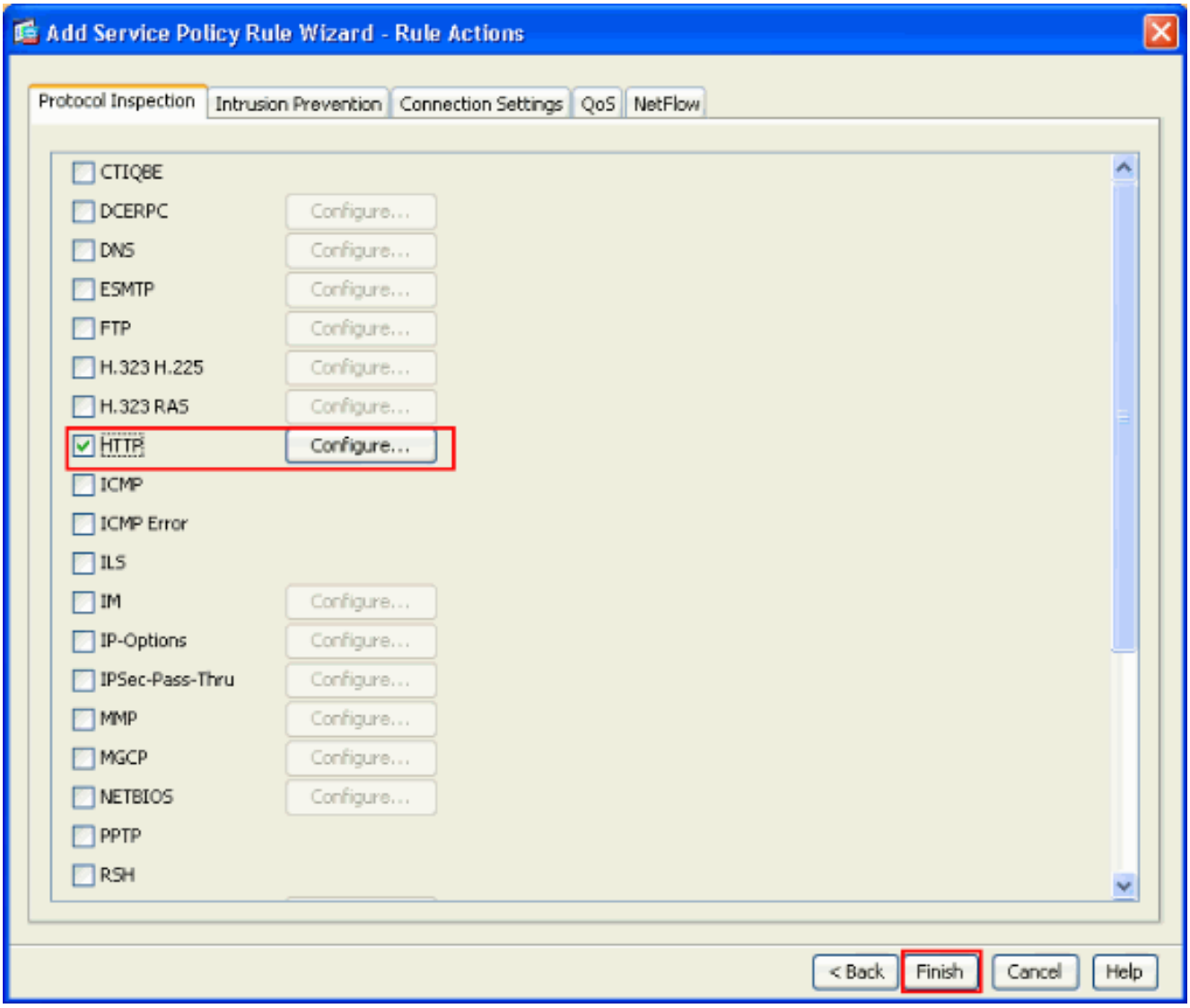


8. En la ventana Select HTTP Inspect Map, verifique el botón de opción situado junto a **Use the Default HTTP Inspection Map**. En este ejemplo se utiliza la inspección HTTP predeterminada. A continuación, haga clic en

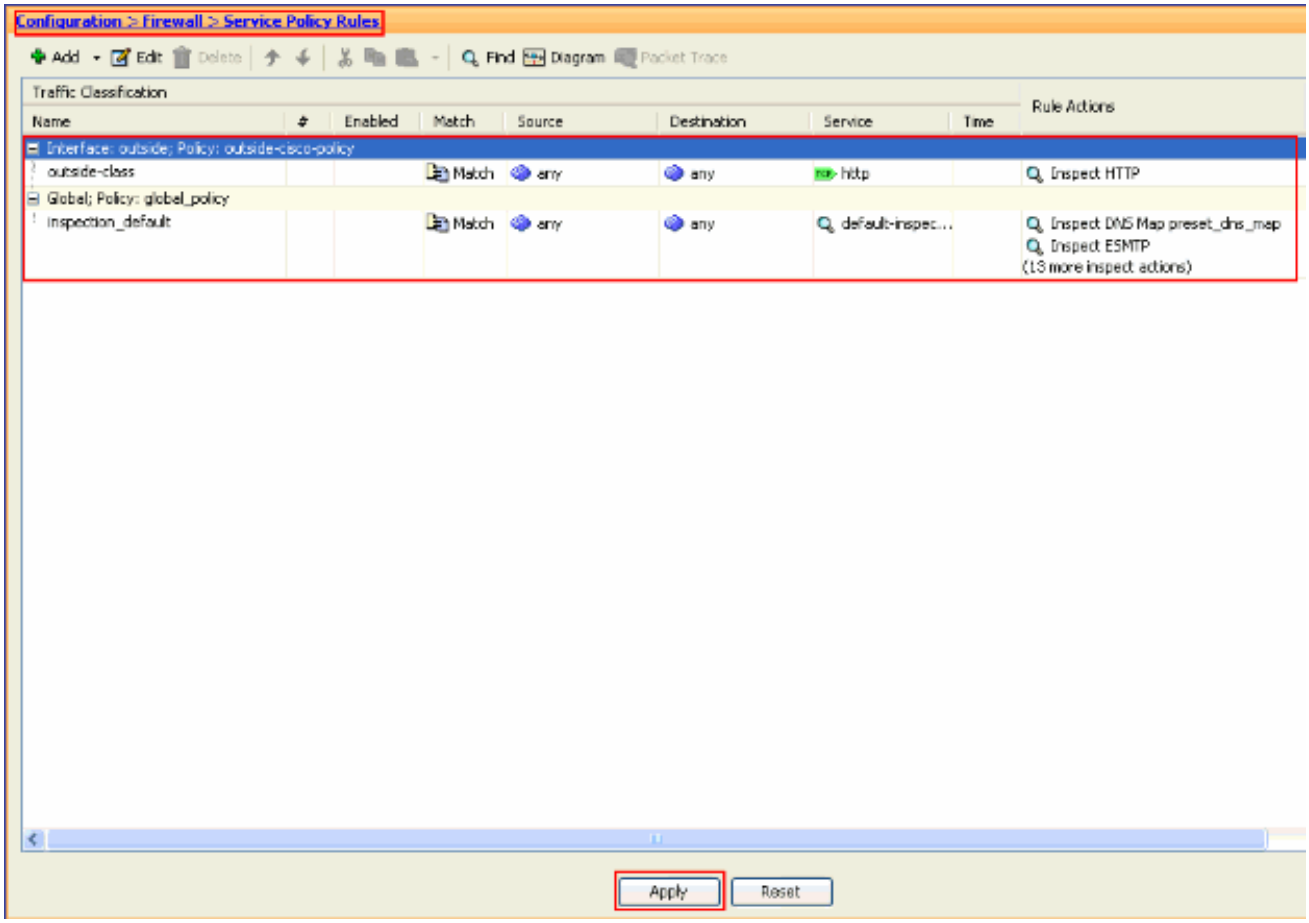


Aceptar.

9. Haga clic en Finish (Finalizar).



10. En **Configuration > Firewall > Service Policy Rules**, verá la política de servicio recientemente configurada **outside-cisco-policy** (para inspeccionar HTTP) junto con la política de servicio predeterminada que ya está presente en el dispositivo. Haga clic en **Aplicar** para aplicar la configuración a Cisco
ASA.



Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Adaptive Security Device Manager
- Solicitudes de Comentarios (RFC)
- Aplicación de la Inspección del Protocolo de Capa de Aplicación
- Soporte Técnico y Documentación - Cisco Systems