ASA 8.3 y posterior: Examen global predeterminado de la neutralización y Inspección de la aplicación no valor por defecto del permiso usando el ASDM

Contenido

Introducción

Este documento proporciona una configuración de muestra para el dispositivo de seguridad adaptante de Cisco (ASA) con las versiones 8.3(1) y después cómo quitar el examen predeterminado de la política global para una aplicación y cómo habilitar el examen para una aplicación no valor por defecto usando el Administrador de dispositivos de seguridad adaptante (ASDM).

Consulte PIX/ASA 7.x: Inhabilite el examen global predeterminado y habilite la Inspección de la aplicación no valor por defecto para la misma configuración en Cisco ASA con las versiones 8.2 y anterior.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión de software del dispositivo de seguridad de Cisco ASA 8.3(1) con el ASDM 6.3.

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.

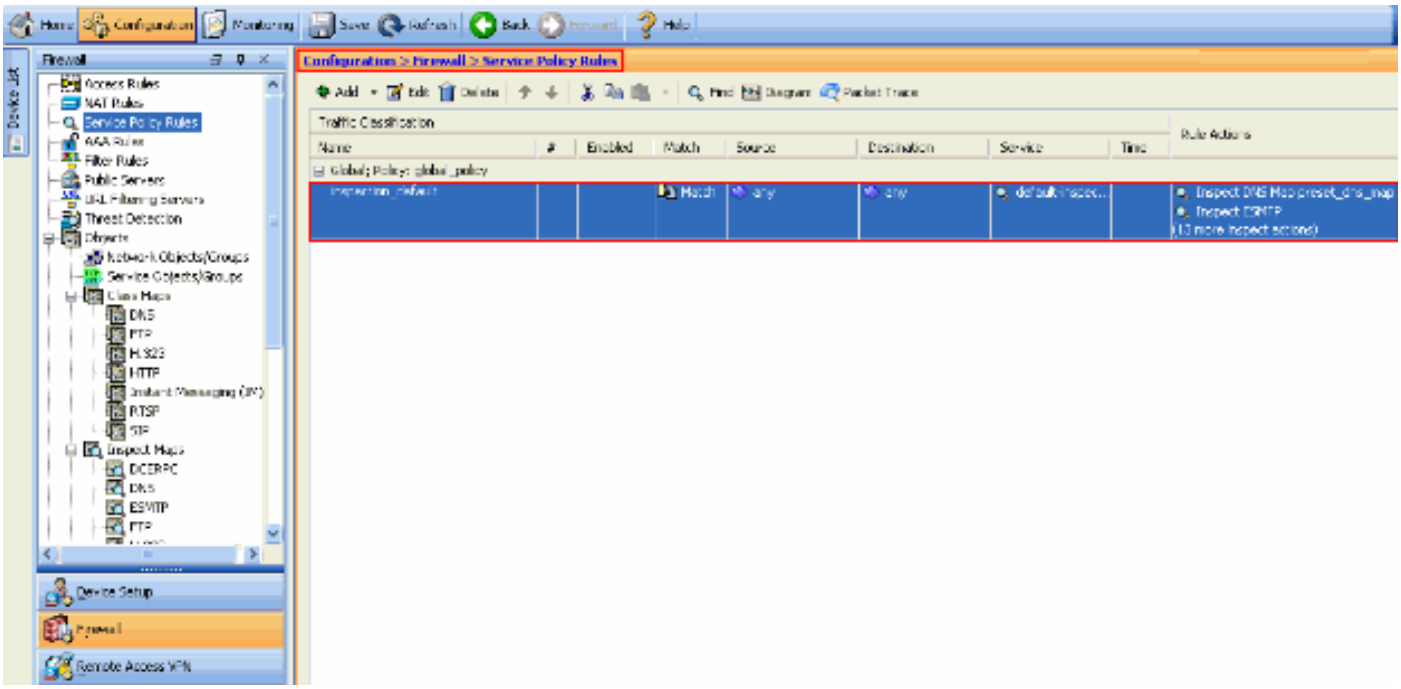
Convenciones

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

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.)

En el ASDM, elija las **reglas de la configuración > del Firewall > de la política de servicio** para ver la política global predeterminada que tiene el examen de la aplicación predeterminada como se muestra aquí:

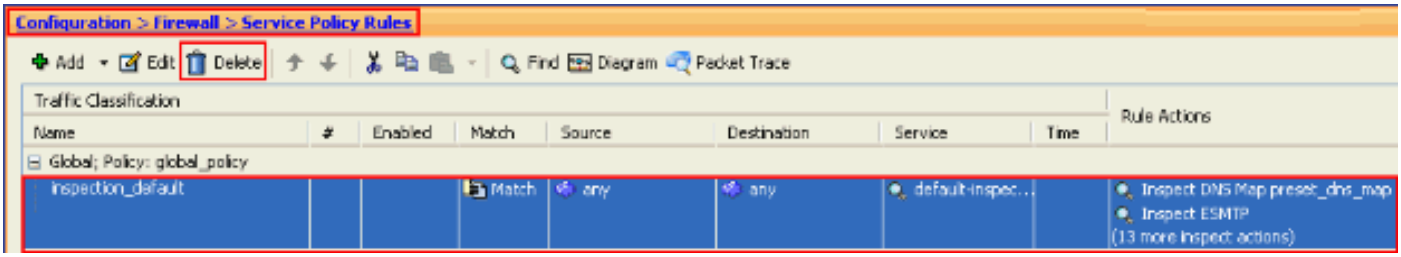


La configuración de la política predeterminada incluye estos comandos:

```
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
```

Si usted necesita inhabilitar la política global, no utilice el **ningún comando global del global_policy de la servicio-directiva**. Para borrar la política global usando el ASDM elija las **reglas de la configuración > del Firewall > de la política de servicio**. Entonces, seleccione la política global y haga clic la **cancelación**.



Nota: Cuando usted borra la política de servicio con el ASDM, se borran las correspondencias asociadas de la directiva y de la clase. Sin embargo, si la política de servicio se borra usando el CLI solamente la política de servicio se quita de la interfaz. La correspondencia y la correspondencia de políticas de la clase permanecen sin cambiar.

Examen global predeterminado de la neutralización para una aplicación

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

Por ejemplo, para quitar el examen global para la aplicación FTP la cual el dispositivo de seguridad escucha, utilice el **ningún examinan el comando ftp** en el modo de configuración de clase.

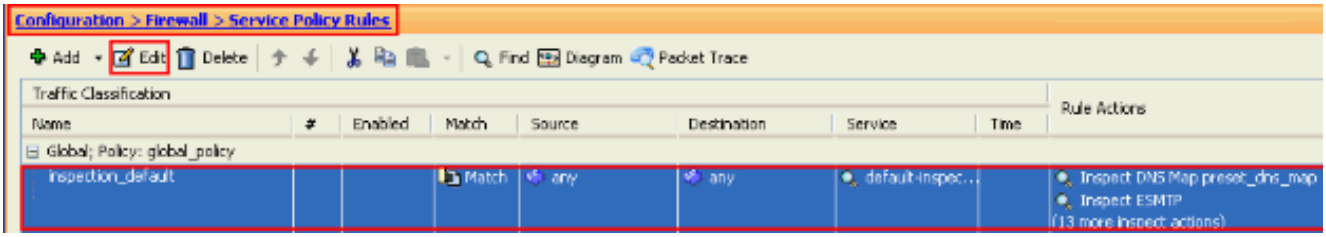
El modo de configuración de clase es accesible del modo de la configuración de correspondencia de políticas. Para quitar la configuración, no utilice la *ninguna* forma del comando.

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

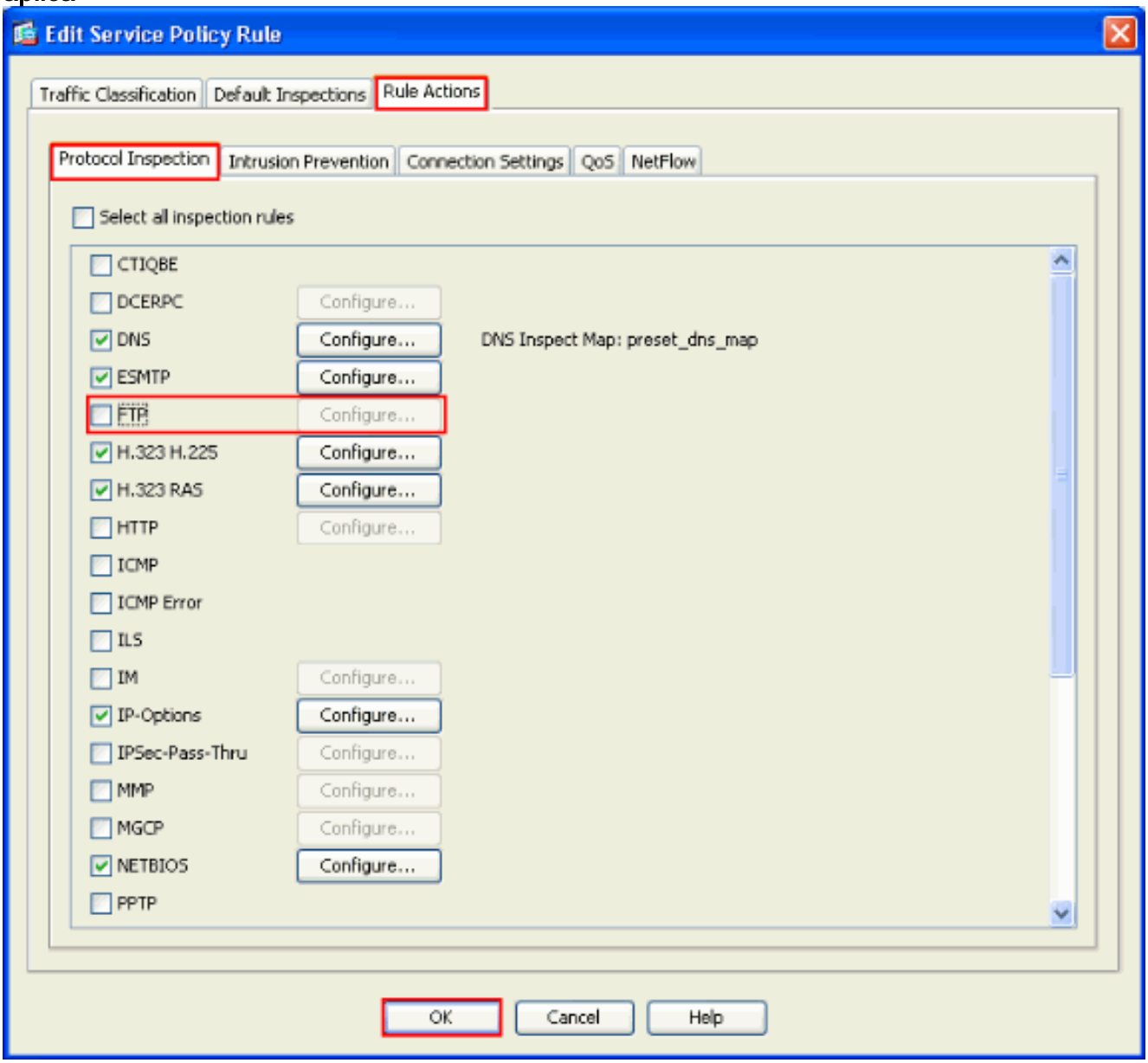
Para inhabilitar el examen global para el FTP usando el ASDM, complete estos pasos:

Nota: Refiera a permitir que el acceso HTTPS para el ASDM para las configuraciones básicas para acceder el PIX/ASA con el ASDM.

1. Elija las **reglas de la configuración > del Firewall > de la política de servicio** y seleccione la política global predeterminada. Entonces, el tecleo **edita** para editar la directiva global del examen.



2. De la ventana de la regla de la política de servicio del editar, elija el **examen del protocolo** bajo **acciones de la regla que** se desmarca cuadro se aseegura la casilla de verificación **FTP**. Esto inhabilita el examen FTP tal y como se muestra en de la imagen siguiente. Entonces, la **AUTORIZACIÓN del** tecleo y entonces **se aplica**.



Nota: Para más información sobre el examen FTP, refiera al [PIX/ASA 7.x: Habilite el ejemplo de configuración de los servicios FTP/TFTP](#).

Habilite el examen para la aplicación no valor por defecto

El examen aumentado HTTP se inhabilita por abandono. Para habilitar el examen HTTP en el global_policy, utilice el comando **HTTP de la inspección** bajo inspection_default de la clase.

En este ejemplo, cualquier conexión HTTP (tráfico TCP en el puerto 80) que ingresa el dispositivo

de seguridad a través de cualquier interfaz se clasifica para el examen HTTP. *Porque la directiva es una política global, el examen ocurre solamente mientras que el tráfico ingresa cada interfaz*.

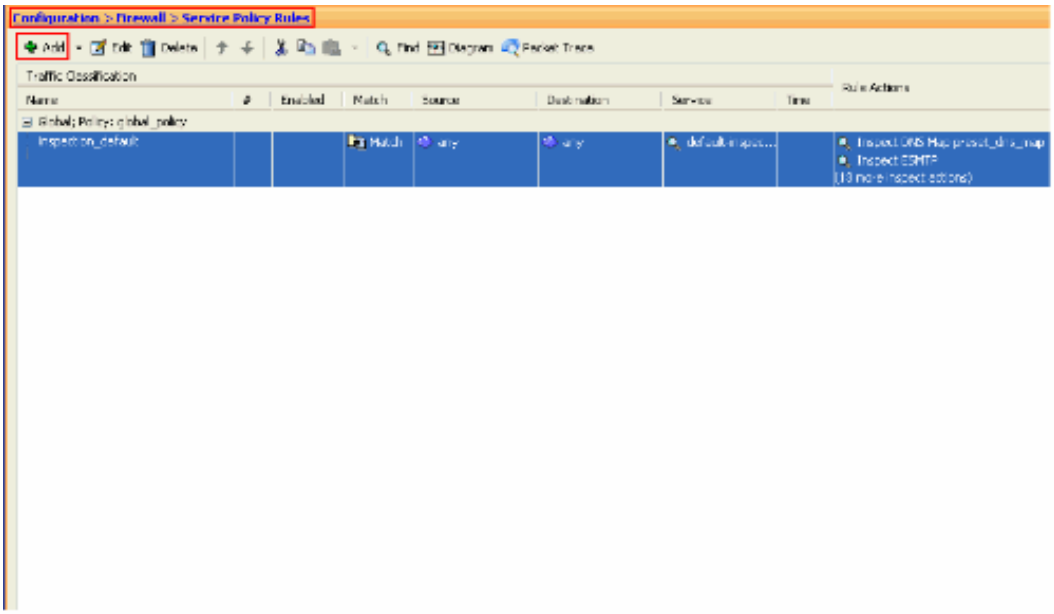
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

En este ejemplo, cualquier conexión HTTP (tráfico TCP en el puerto 80) que ingresa o sale el dispositivo de seguridad a través de la *interfaz exterior se clasifica para el examen HTTP*.

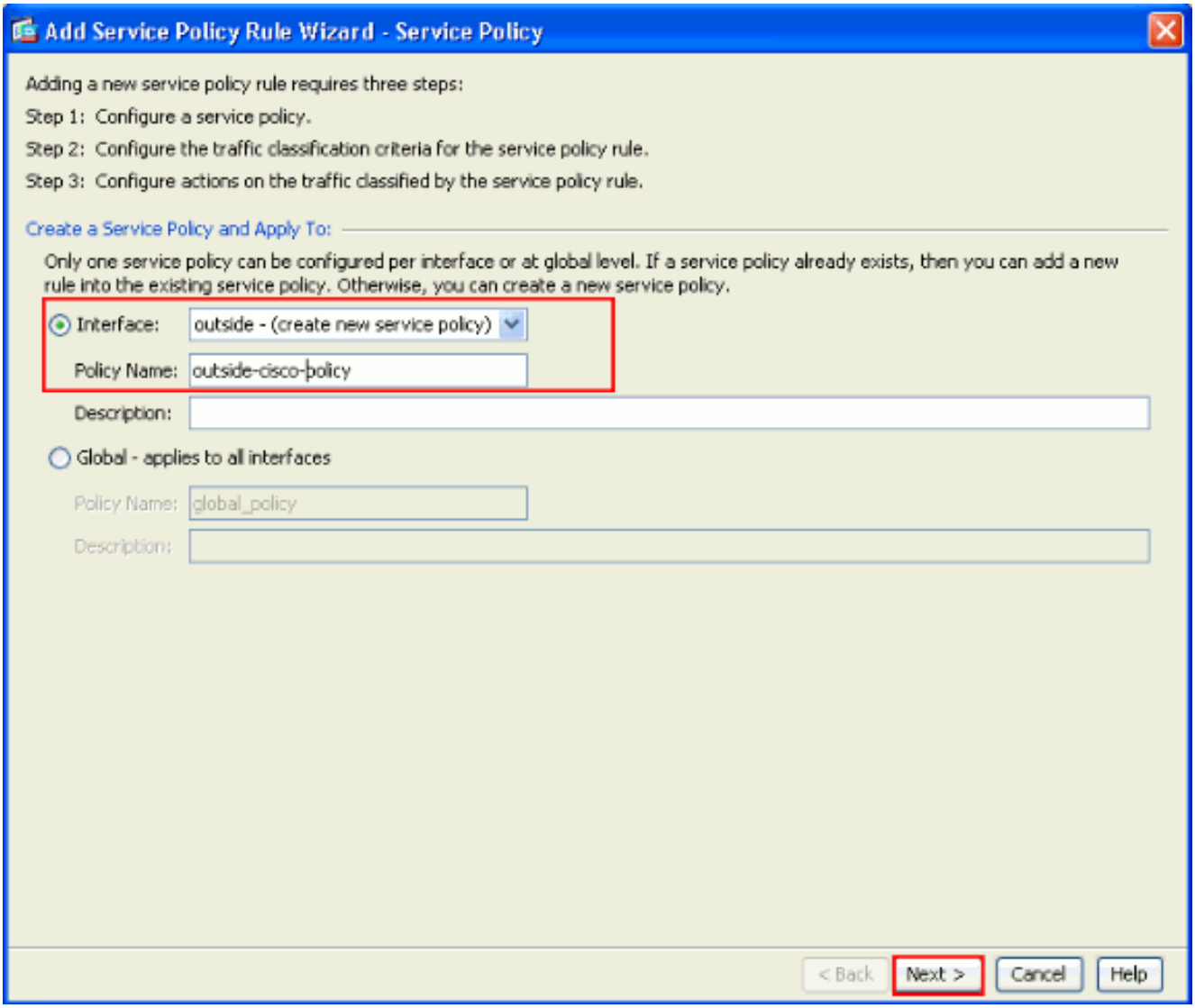
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Realice estos pasos para configurar el ejemplo antedicho usando el ASDM:

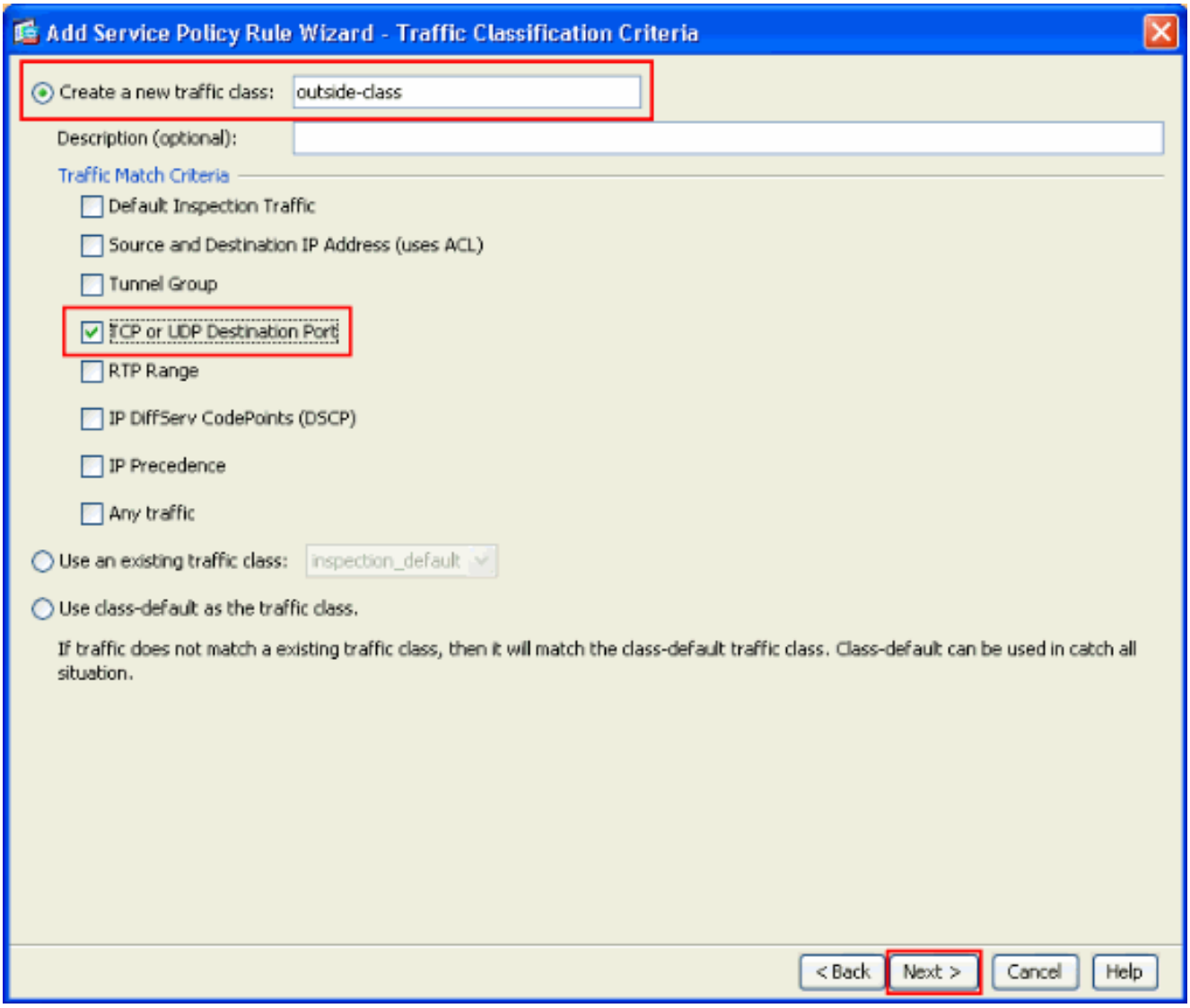
1. Elija las **reglas de la configuración > del Firewall > de la política de servicio** y el tecleo **agrega** para agregar una nueva política de servicio:



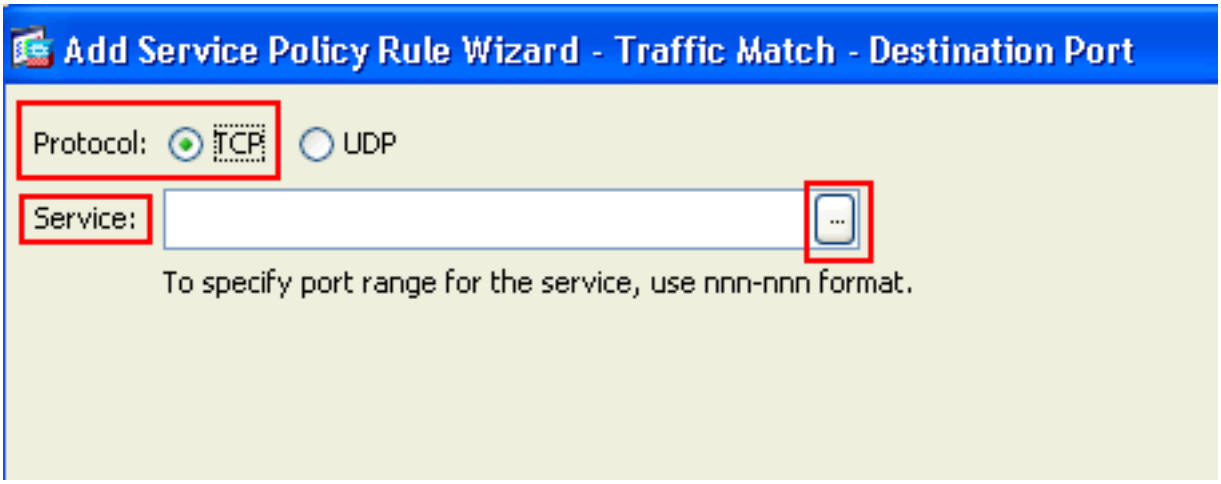
2. Del Asisitente de la regla de la política de servicio del agregar - La ventana de la política de servicio, elige el botón de radio al lado de la **interfaz**. Esto aplica la directiva creada a una interfaz específica, que es la **interfaz exterior** en este ejemplo. Proporcione un nombre de la directiva, que es exterior-Cisco-**directiva** en este ejemplo. Haga clic en Next (Siguiente).



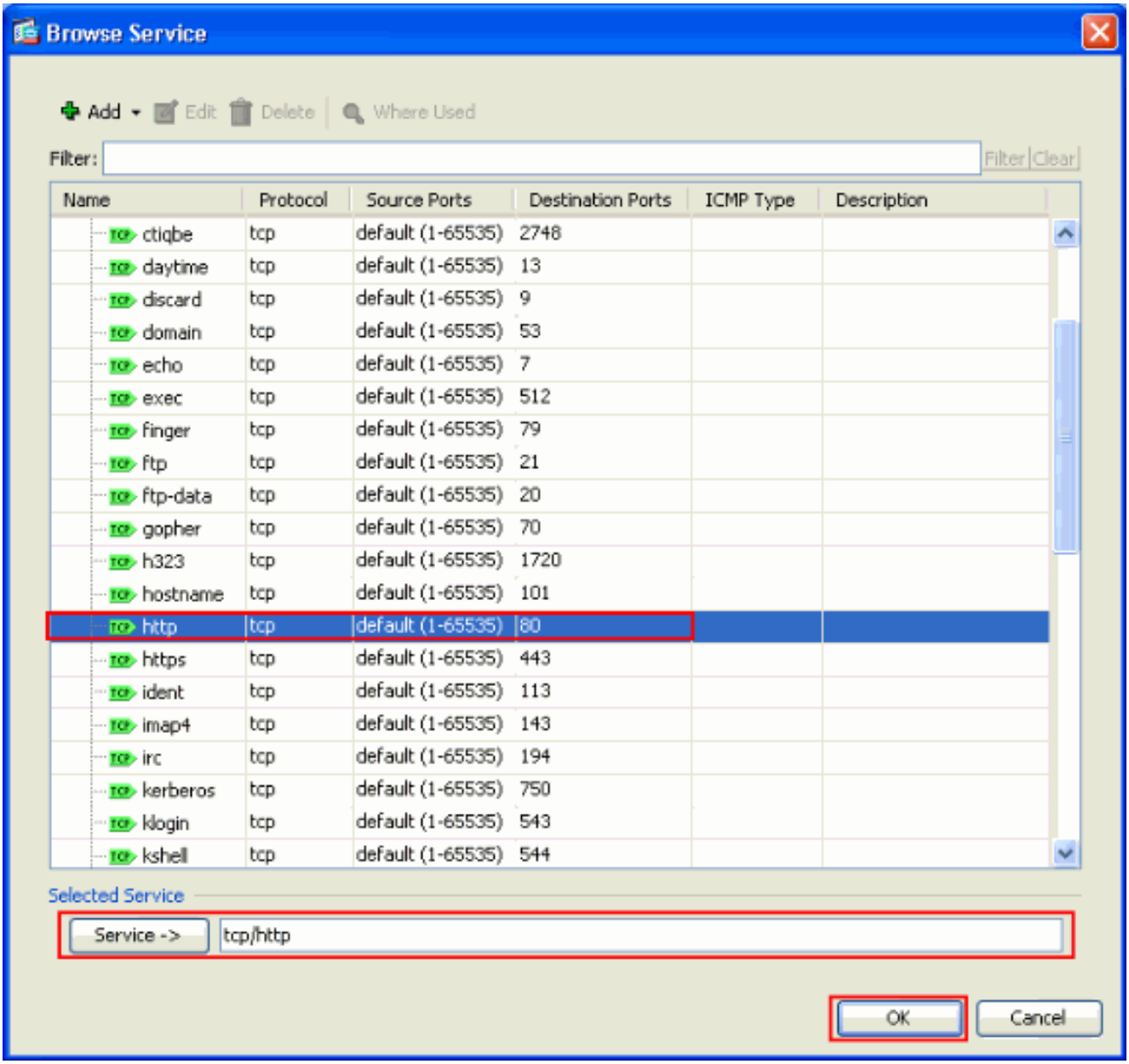
3. Del Asisitente de la regla de la política de servicio del agregar - La ventana de los criterios de Clasificación de tráfico, proporciona el nuevo nombre de clase de tráfico. El nombre usado en este ejemplo es exterior-**clase**. Asegúrese de que la casilla de verificación al lado del **TCP o del puerto de destino UDP** esté marcada y haga clic **después**.



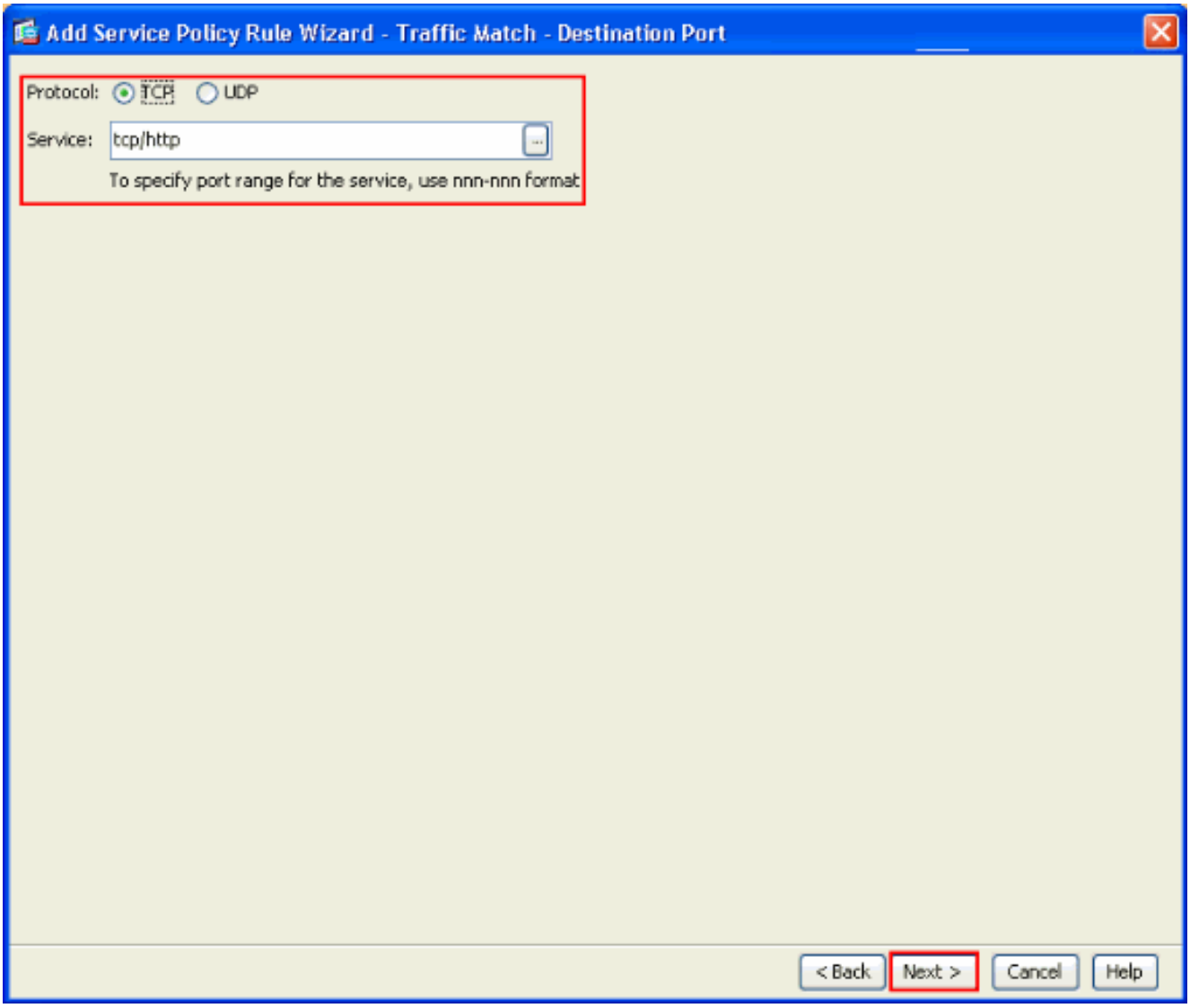
4. Del Asisitente de la regla de la política de servicio del agregar - Coincidencia del tráfico - La ventana del puerto destino, elige el botón de radio al lado del **TCP** conforme a la **sección de protocolo**. Entonces, haga clic el botón al lado del **servicio** para elegir el servicio solicitado.



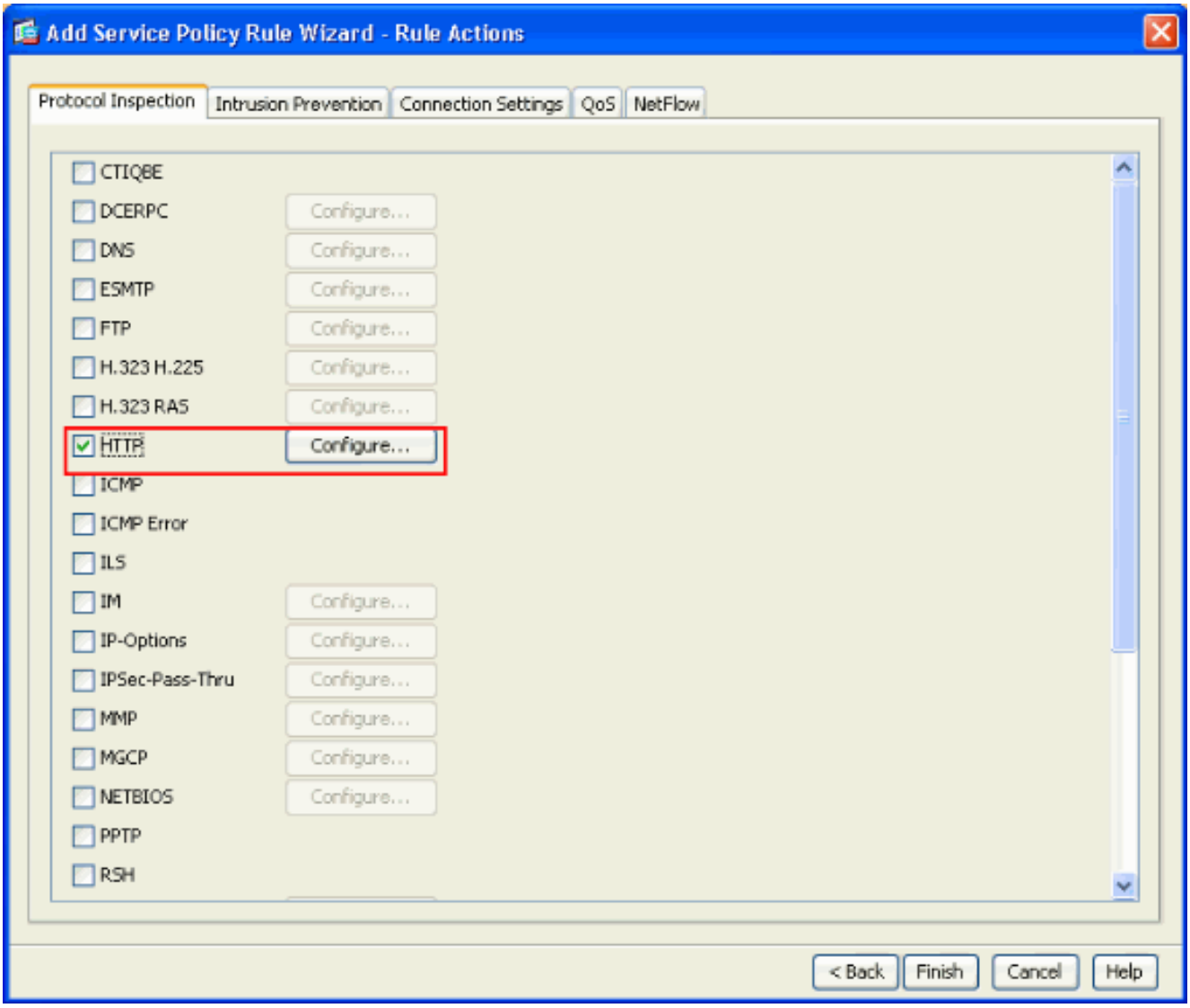
5. De la ojeada mantenga la ventana, eligen el **HTTP** como el servicio. Entonces, **AUTORIZACIÓN del**
tecleo.



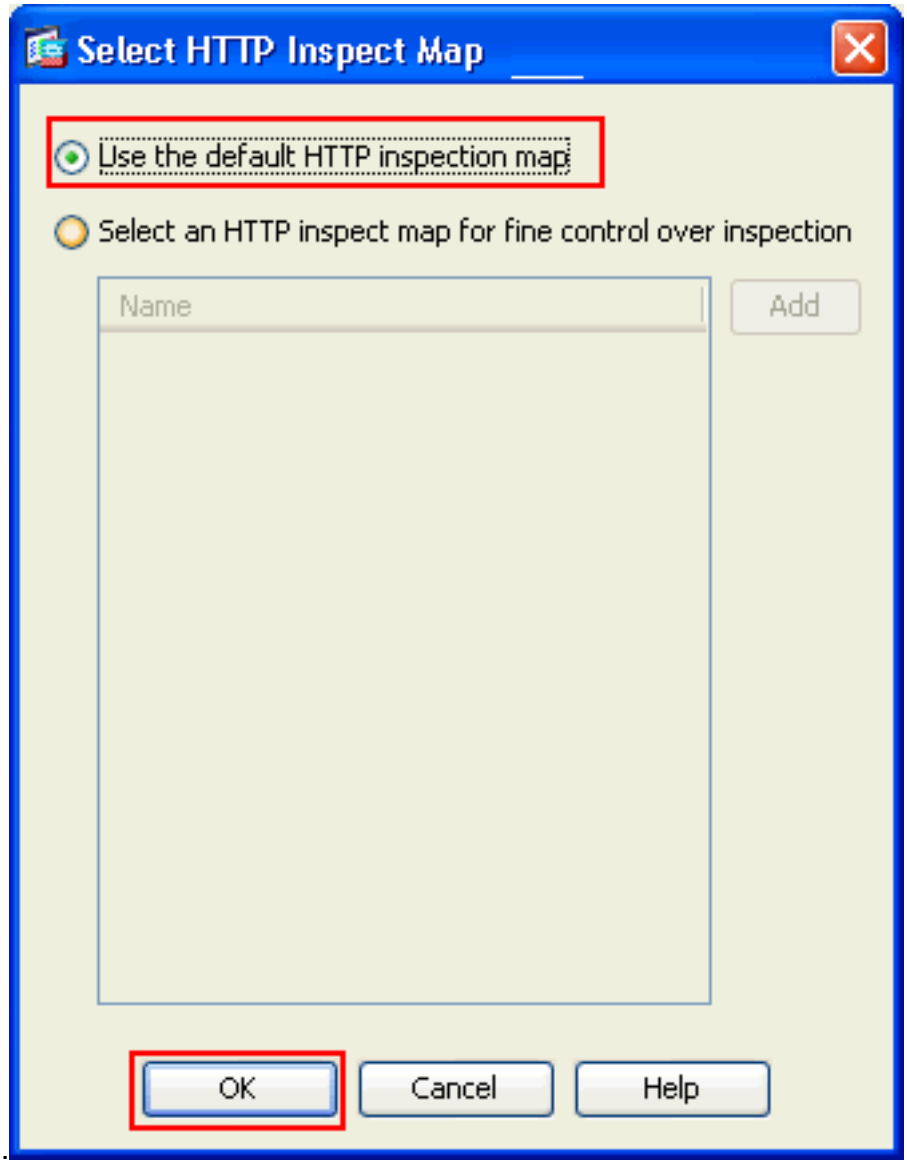
6. Del Asisitente de la regla de la política de servicio del agregar - Coincidencia del tráfico - Ventana del puerto destino, usted puede ver que el **servicio** elegido es **tcp/HTTP**. Haga clic en Next
(Siguiente).



7. Del Asisitente de la regla de la política de servicio del agregar - Gobierne la ventana de las acciones, marque la casilla de verificación al lado del **HTTP**. Entonces, **configuración del** tecleo al lado del
HTTP.

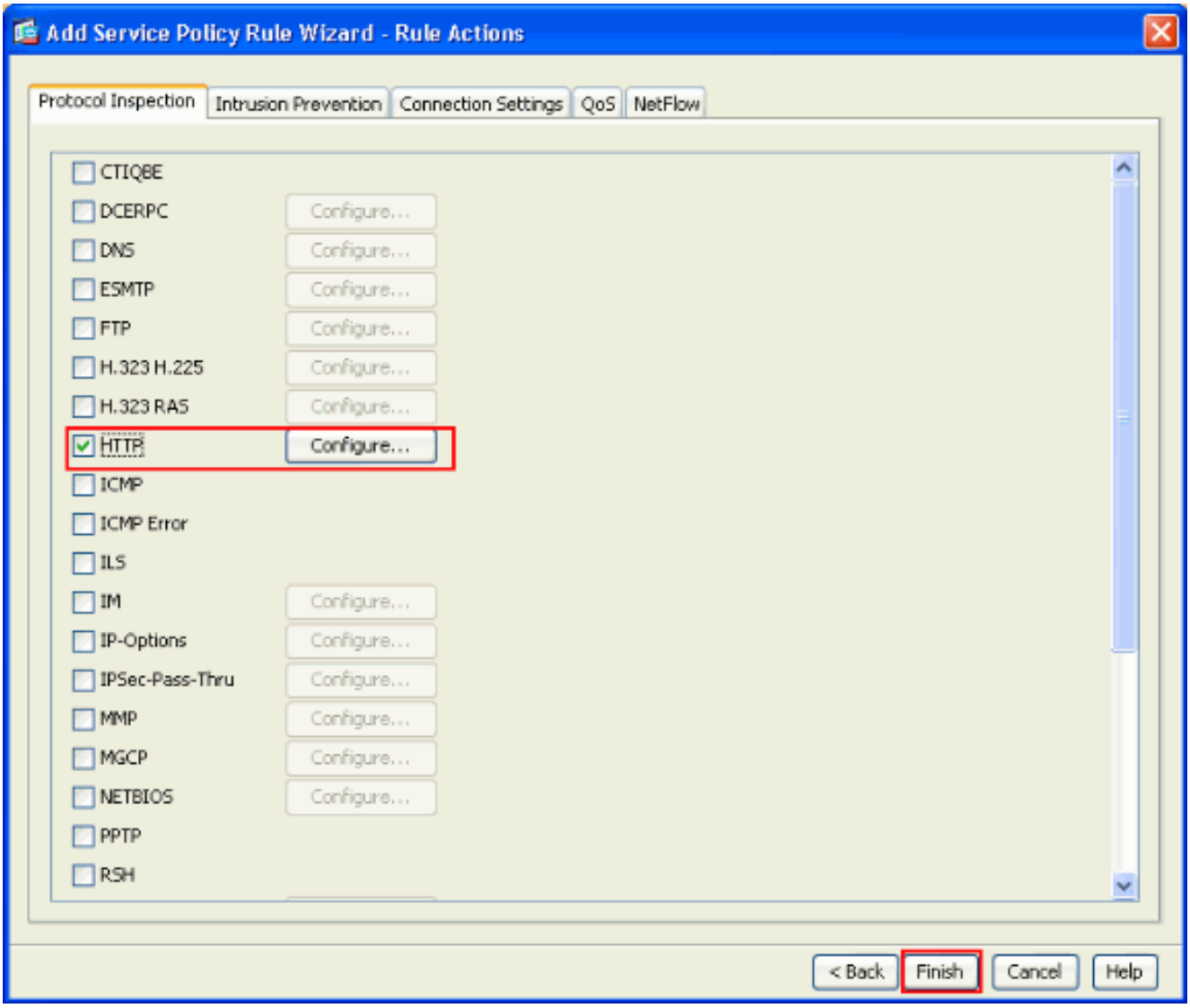


8. Del HTTP selecto examine la ventana del mapa, marcan el botón de radio al lado del **uso la correspondencia del examen del valor por defecto HTTP**. El examen del valor por defecto HTTP se utiliza en este ejemplo. Entonces, **AUTORIZACIÓN del**

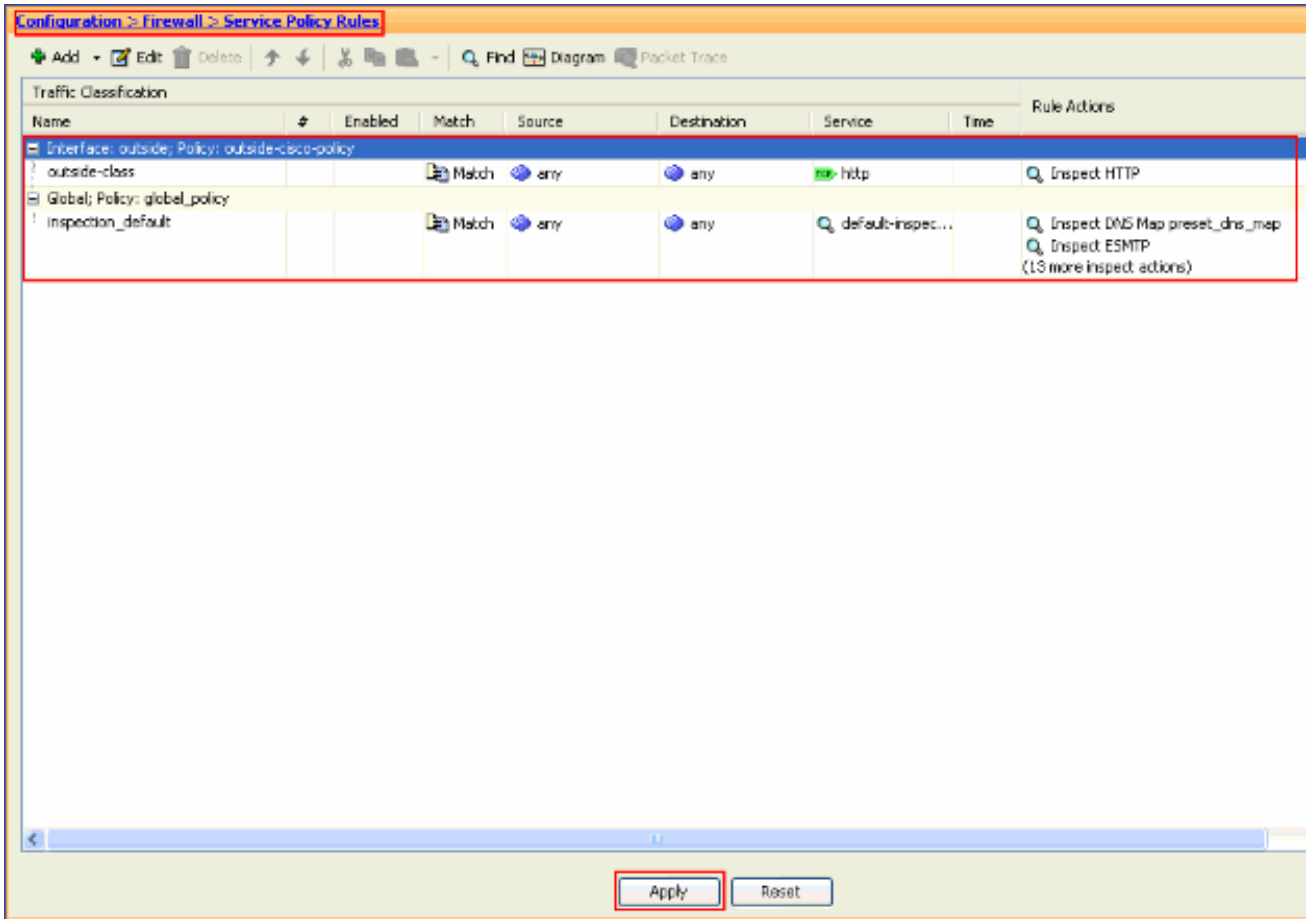


tecleo.

9. Haga clic en Finish (Finalizar).



10. Bajo **reglas de la configuración > del Firewall > de la política de servicio**, usted verá la exterior-Cisco-**directiva** nuevamente configurada de la política de servicio (examinar el HTTP) junto con la directiva de servicio predeterminado ya presente en el dispositivo. El tecleo **se aplica** 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 del examen del Application Layer Protocol
- Soporte Técnico y Documentación - Cisco Systems