ASA 8.3 and Later: Disable Default Global Inspection and Enable Non-Default Application Inspection using ASDM

Contents

Introduction

This document provides a sample configuration for Cisco Adaptive Security Appliance (ASA) with versions 8.3(1) and later on how to remove the default inspection from global policy for an application and how to enable the inspection for a non-default application using Adaptive Security Device Manager (ASDM).

Refer to PIX/ASA 7.X: Disable Default Global Inspection and Enable Non-Default Application Inspection for the same configuration on Cisco ASA with versions 8.2 and earlier.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco ASA Security Appliance Software version 8.3(1) with 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.

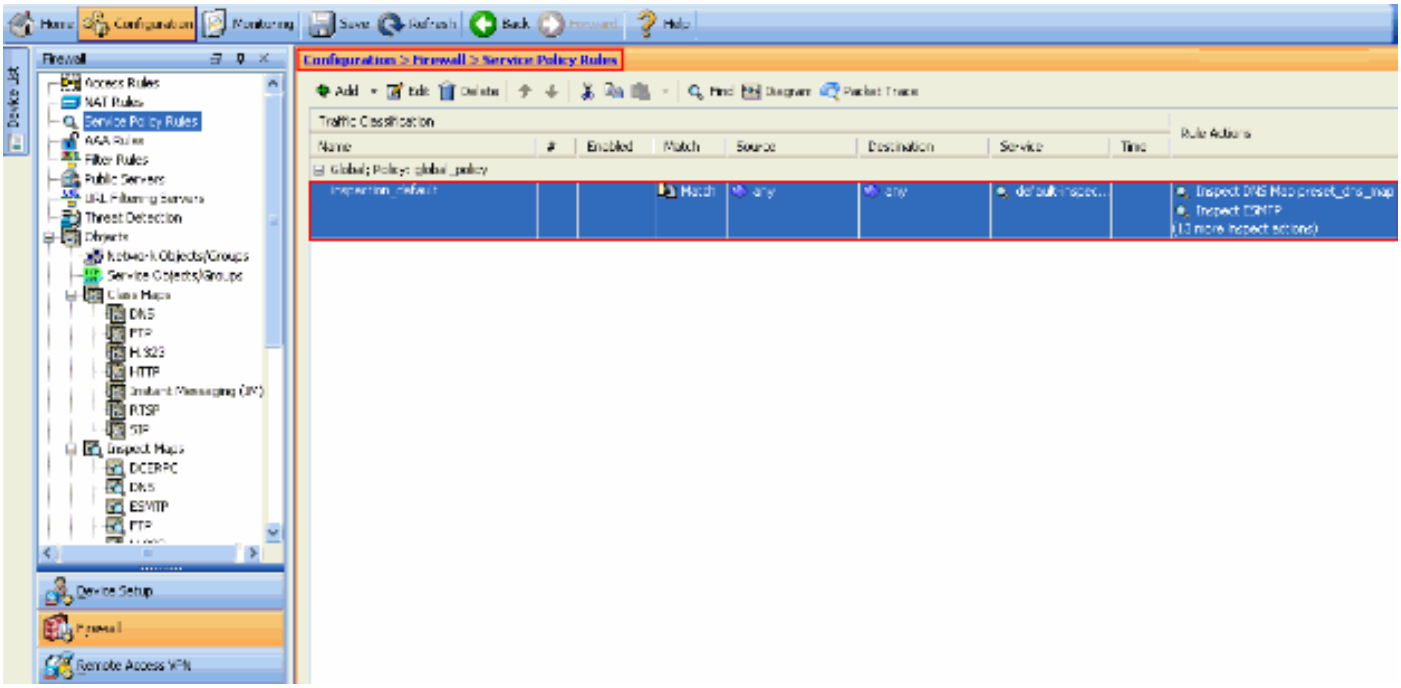
Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Default Global Policy

By default, the configuration includes a policy that matches all default application inspection traffic and applies certain inspections to the traffic on all interfaces (a global policy). Not all inspections are enabled by default. You can apply only one global policy. If you want to alter the global policy, you must either edit the default policy or disable it and apply a new one. (An interface policy overrides the global policy.)

In ASDM, choose **Configuration > Firewall > Service Policy Rules** to view the default global policy that has the default application inspection as shown here:

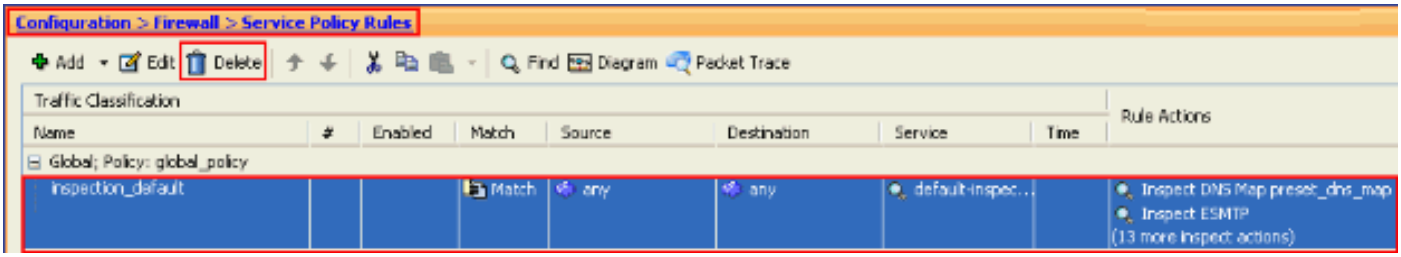


The default policy configuration includes these commands:

```
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
```

If you need to disable the global policy, use the **no service-policy global_policy global** command. In order to delete the global policy using ASDM choose **Configuration > Firewall > Service Policy Rules**. Then, select the global policy and click **Delete**.



Note: When you delete the service policy with ASDM, the associated policy and class maps are deleted. However, if the service policy is deleted using CLI only the service policy is removed from the interface. The class map and policy map remain unchanged.

Disable Default Global Inspection for an Application

In order to disable global inspection for an application, use the *no* version of the **inspect** command.

For example, in order to remove the global inspection for the FTP application to which the security appliance listens, use the **no inspect ftp** command in class configuration mode.

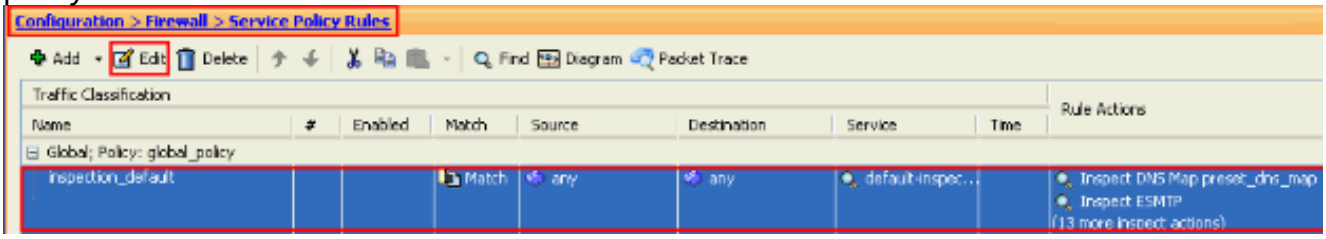
Class configuration mode is accessible from the policy map configuration mode. In order to remove the configuration, use the *no* form of the command.

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

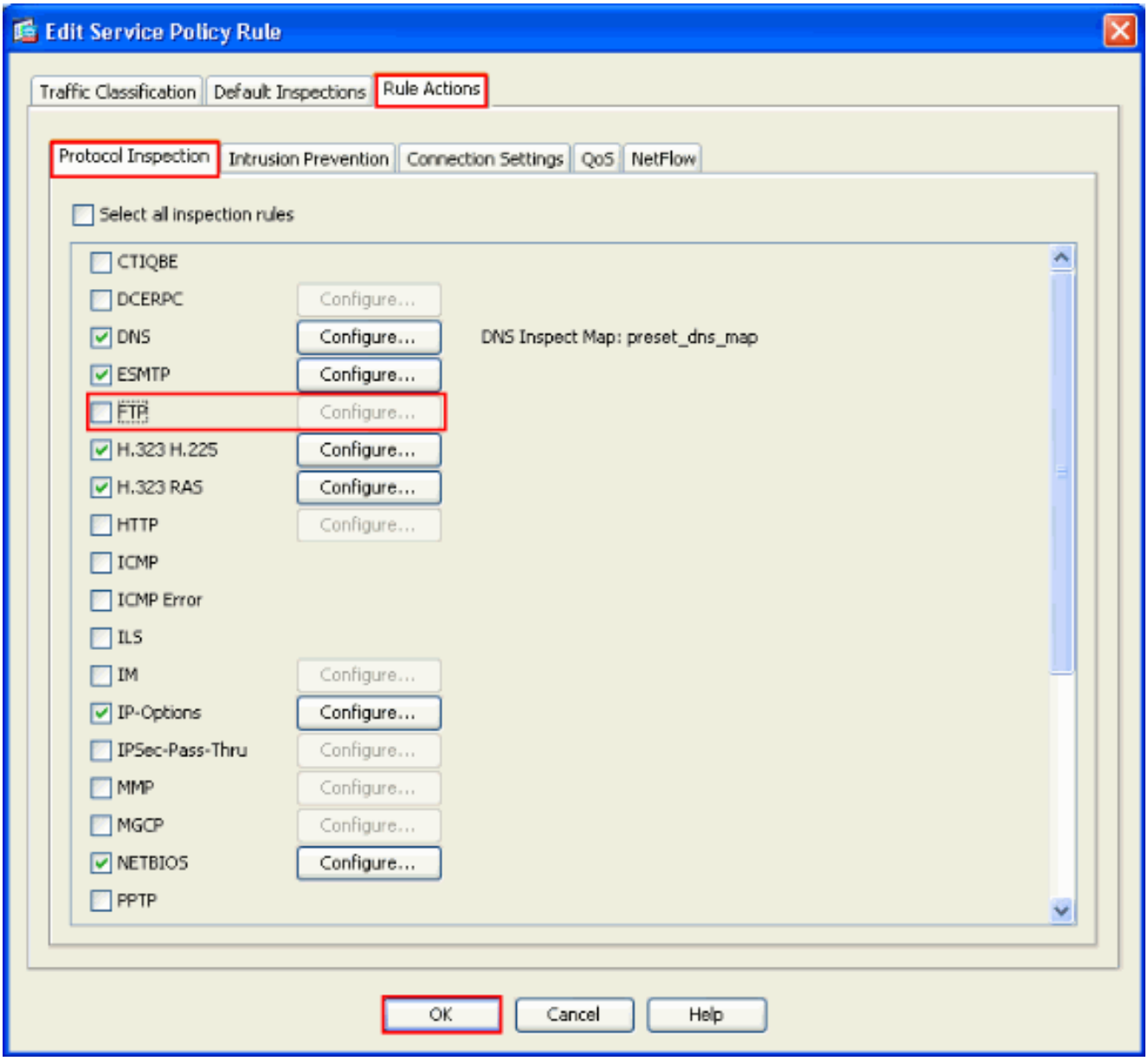
In order to disable global inspection for FTP using ASDM, complete these steps:

Note: Refer to Allowing HTTPS Access for ASDM for basic settings in order to access the PIX/ASA through ASDM.

1. Choose **Configuration > Firewall > Service Policy Rules** and select the default global policy. Then, click **Edit** to edit the global inspection policy.



2. From the Edit Service Policy Rule window, choose **Protocol Inspection** under the **Rule Actions** tab. Make sure the **FTP** check box is unchecked. This disables FTP inspection as shown in the next image. Then, click **OK** and then **Apply**.



Note: For more information on FTP inspection, refer to PIX/ASA 7.x: Enable FTP/TFTP Services Configuration Example.

Enable Inspection for Non-Default Application

Enhanced HTTP inspection is disabled by default. In order to enable HTTP inspection in global_policy, use the **inspect http** command under class inspection_default.

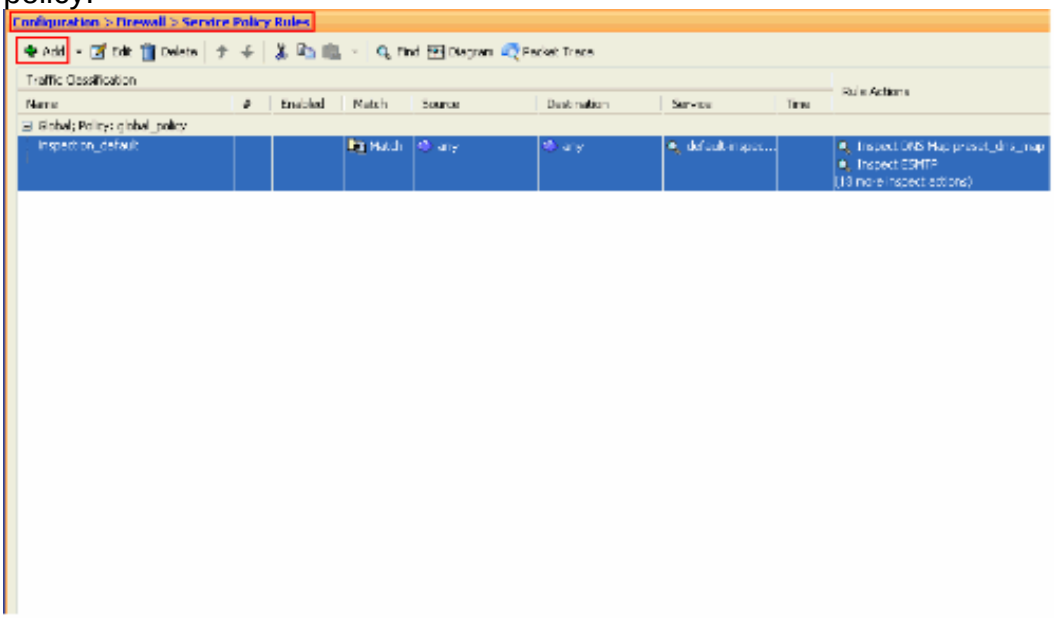
In this example, any HTTP connection (TCP traffic on port 80) that enters the security appliance through any interface is classified for HTTP inspection. *Because the policy is a global policy, inspection occurs only as the traffic enters each interface*.

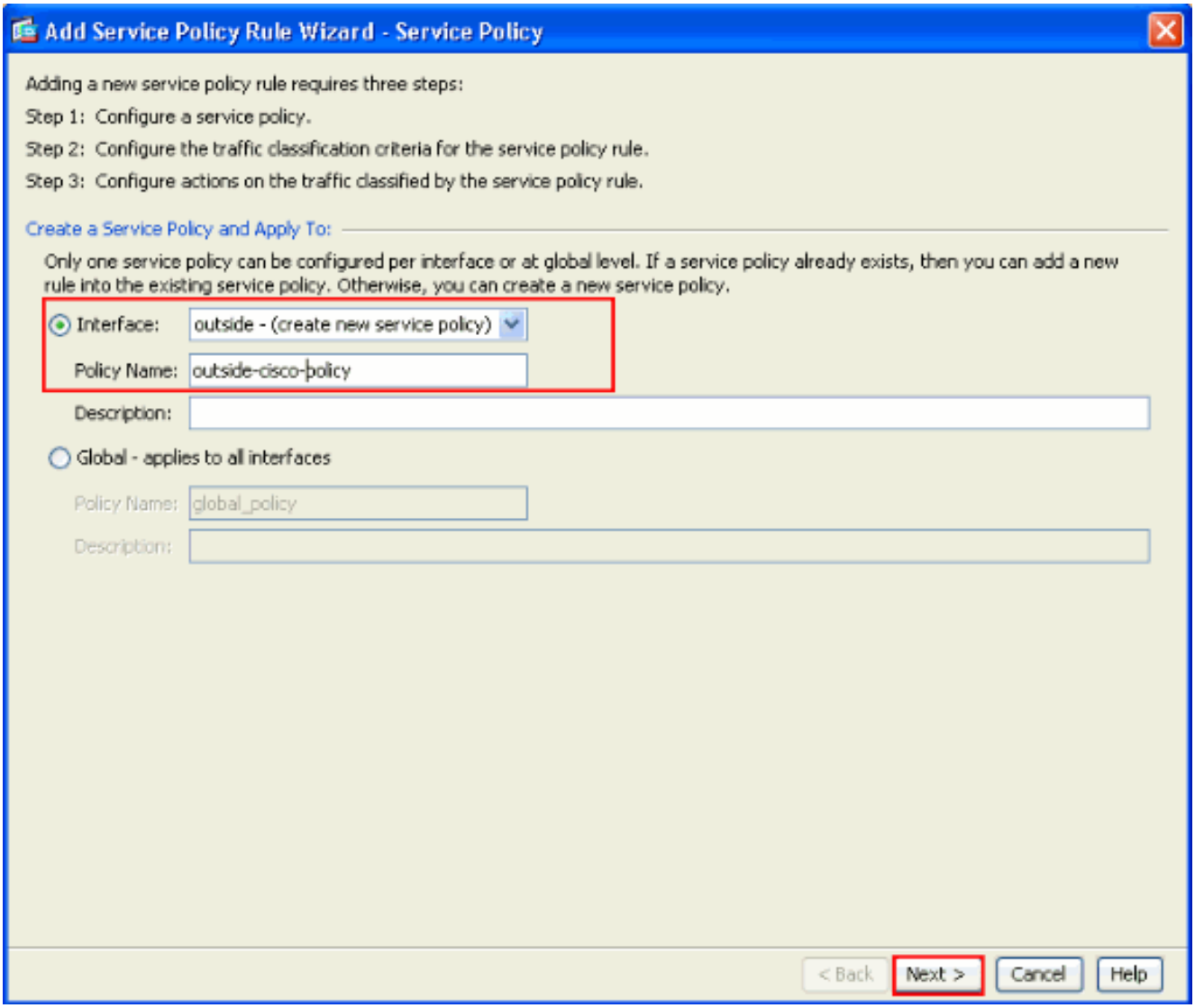
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

In this example, any HTTP connection (TCP traffic on port 80) that enters or exits the security appliance through the *outside interface is classified for HTTP inspection*.

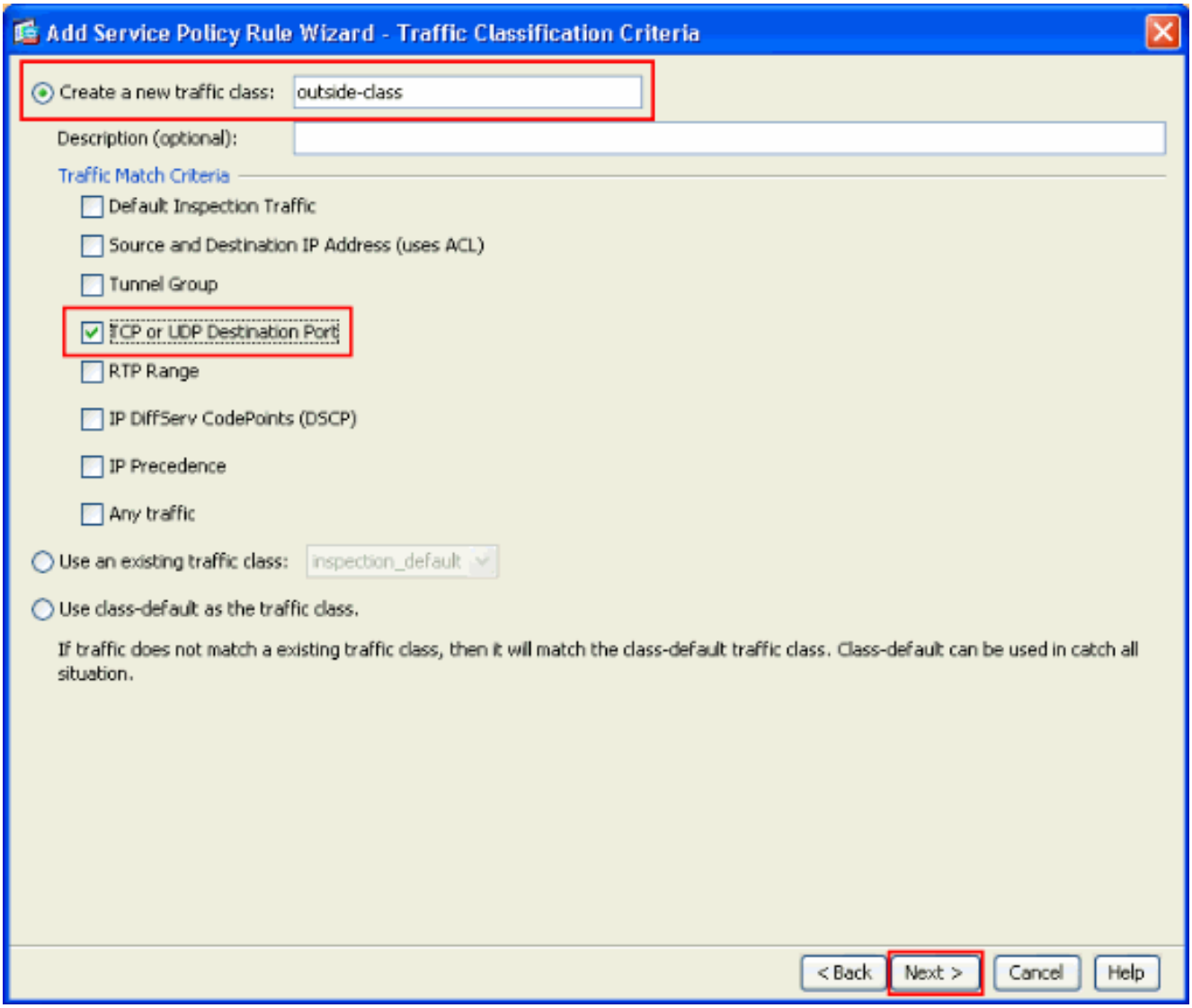
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Perform these steps in order to configure the above example using ASDM:

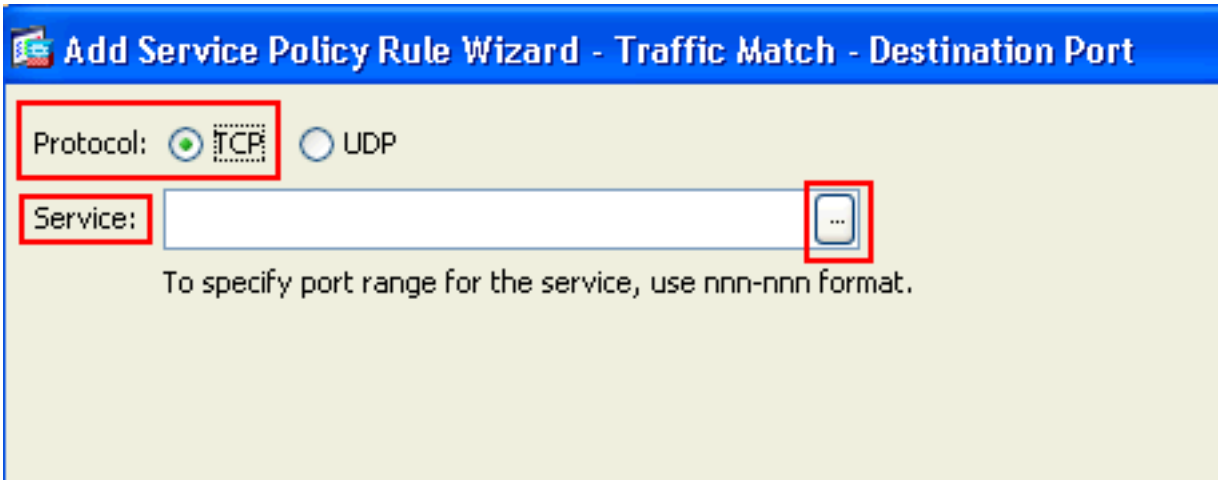
1. Choose **Configuration > Firewall > Service Policy Rules** and click **Add** in order to add a new service
   policy:
   
2. From the Add Service Policy Rule Wizard - Service Policy window, choose the radio button next to **Interface**. This applies the policy created to a specific interface, which is the **Outside** interface in this example. Provide a policy name, which is **outside-cisco-policy** in this example. Click
   Next.



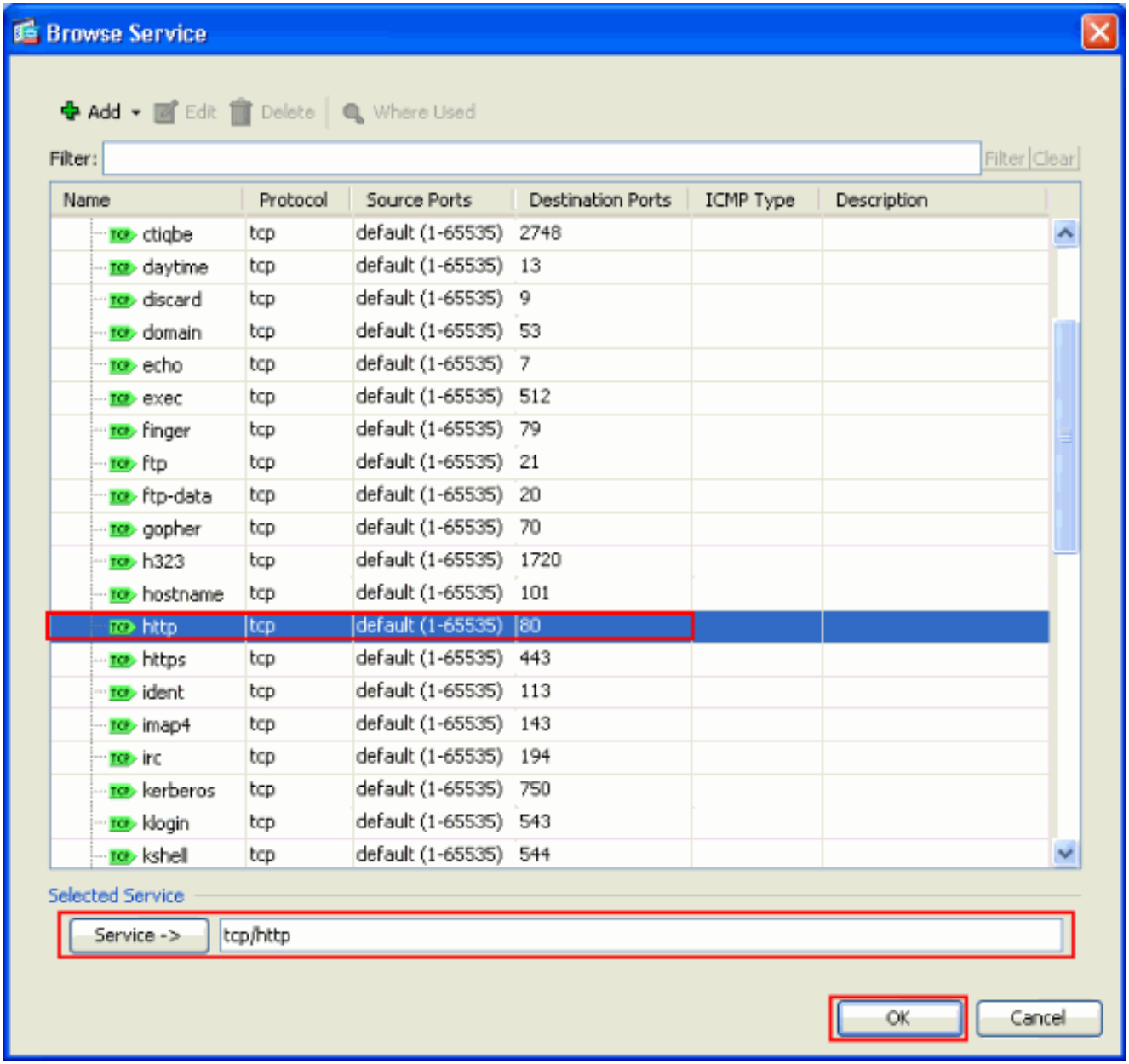
3. From the Add Service Policy Rule Wizard - Traffic Classification Criteria window, provide the new traffic class name. The name used in this example is **outside-class**. Ensure that the check box next to **TCP or UDP Destination Port** is checked and click **Next**.



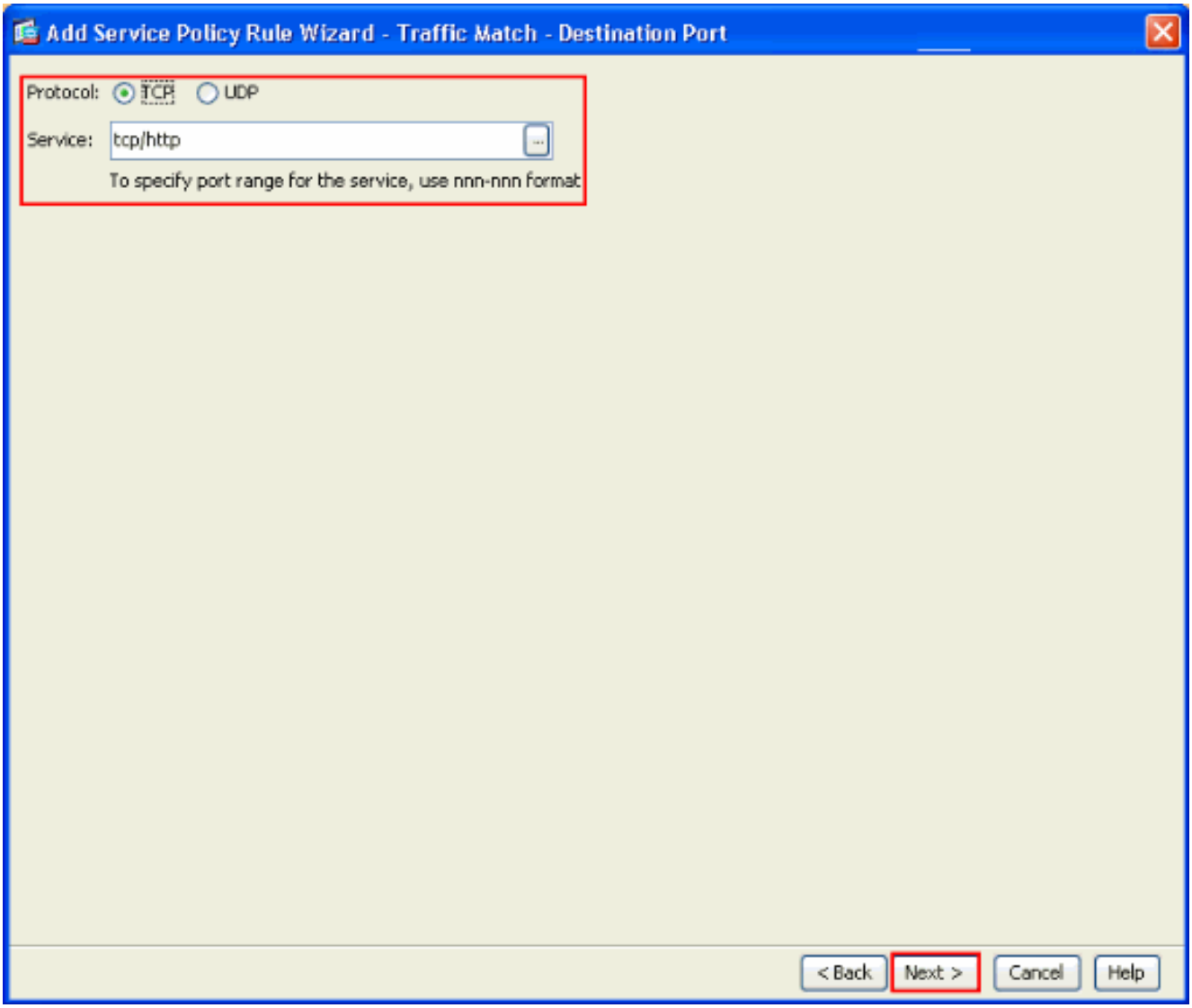
4. From the Add Service Policy Rule Wizard - Traffic Match - Destination Port window, choose the radio button next to **TCP** under the **Protocol** section. Then, click the button next to **Service** in order to choose the required service.



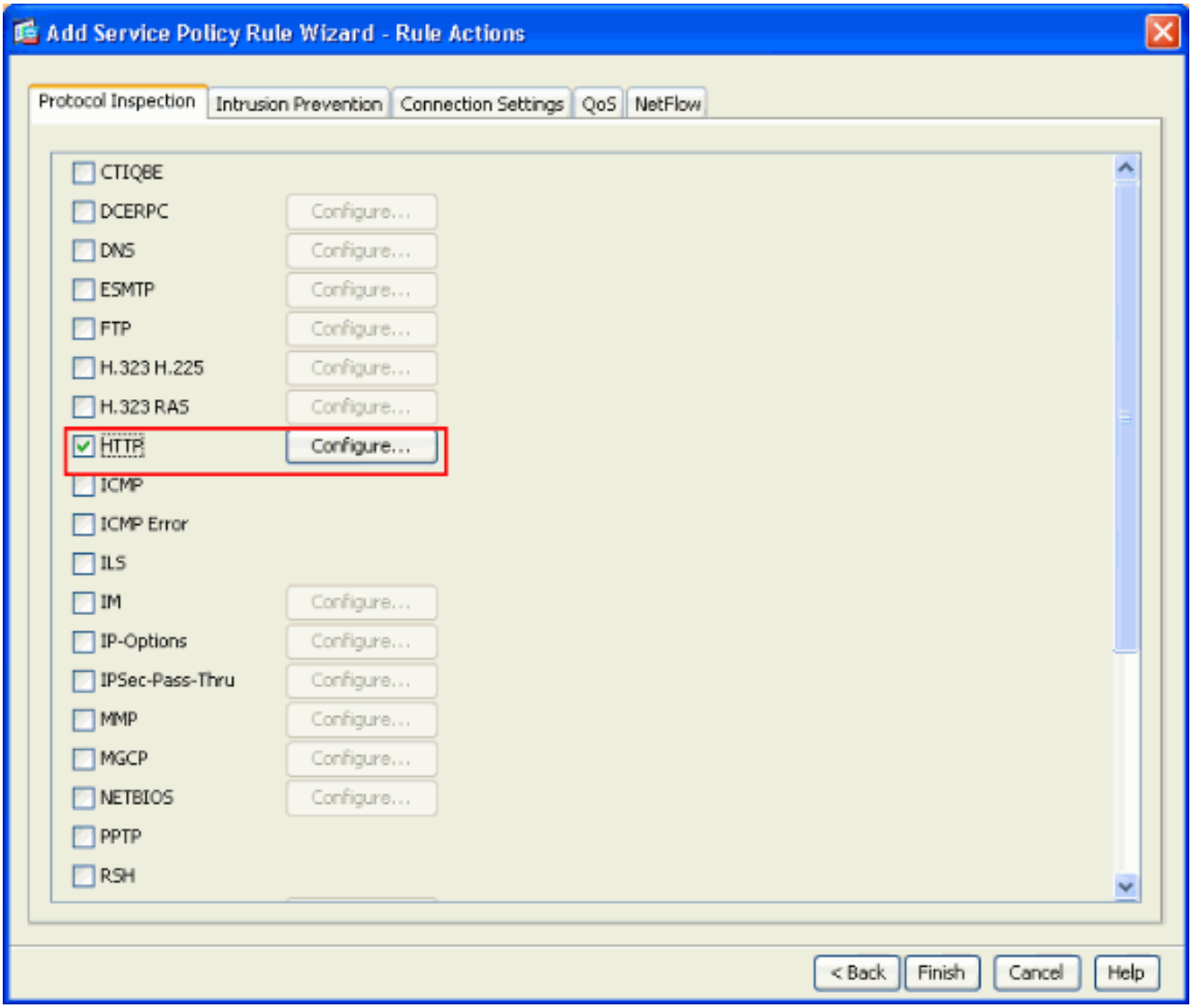
5. From the Browse Service window, choose **HTTP** as the service. Then, click **OK**.



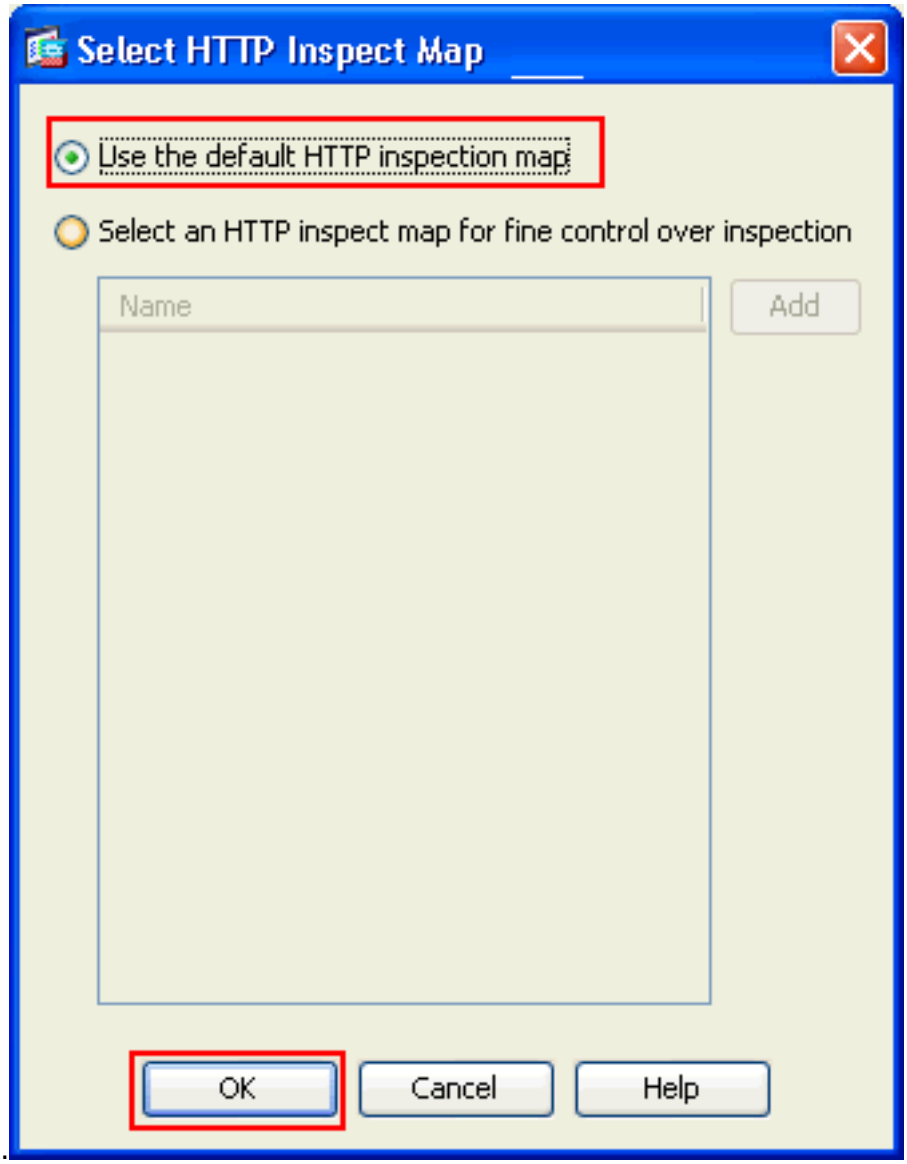
6. From the Add Service Policy Rule Wizard - Traffic Match - Destination Port window, you can see that the **Service** chosen is **tcp/http**. Click **Next**.



7. From the Add Service Policy Rule Wizard - Rule Actions window, check the check box next to **HTTP**. Then, click **Configure** next to **HTTP**.

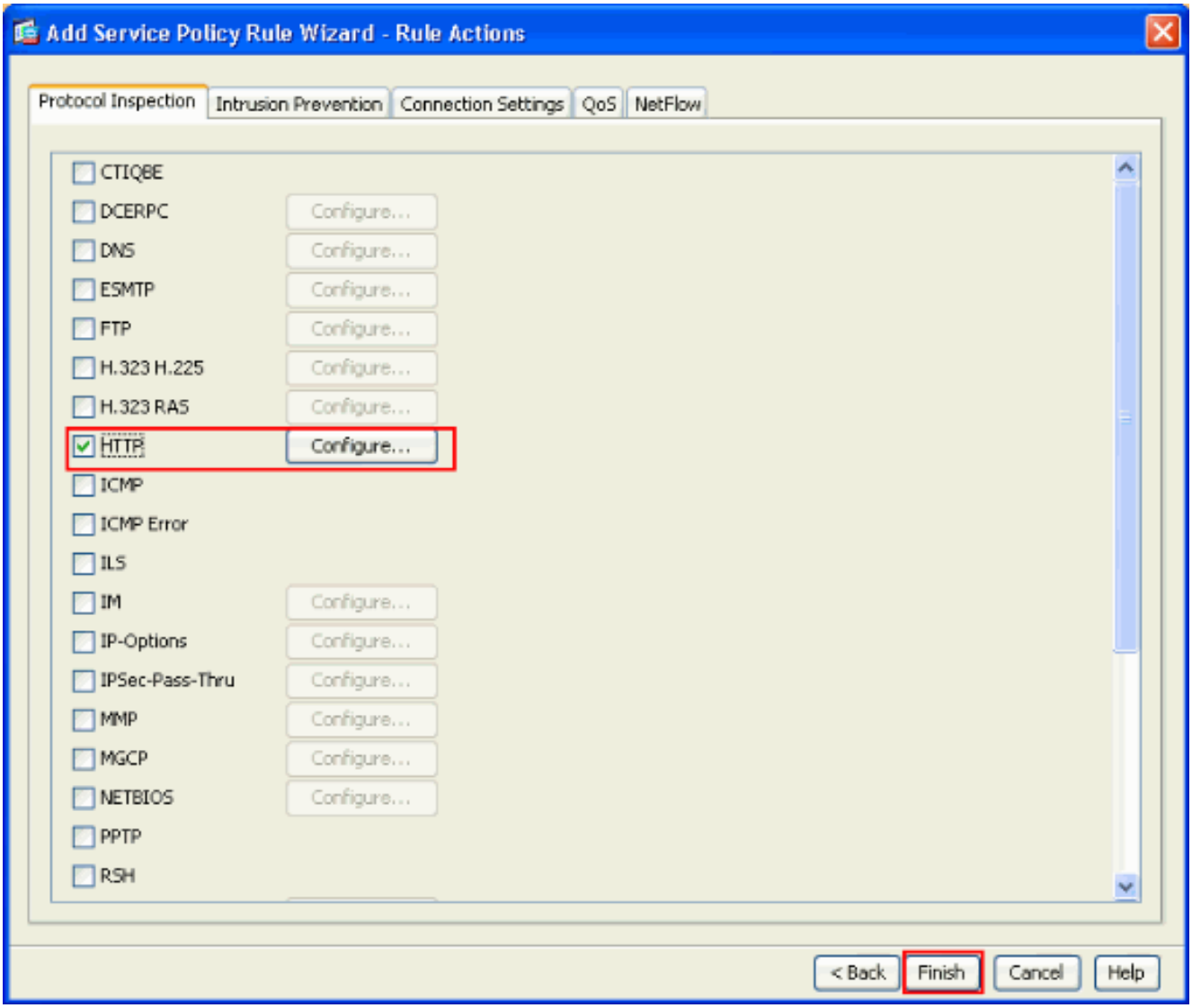


8. From the Select HTTP Inspect Map window, check the radio button next to **Use the Default HTTP inspection map**. The default HTTP inspection is used in this example. Then, click

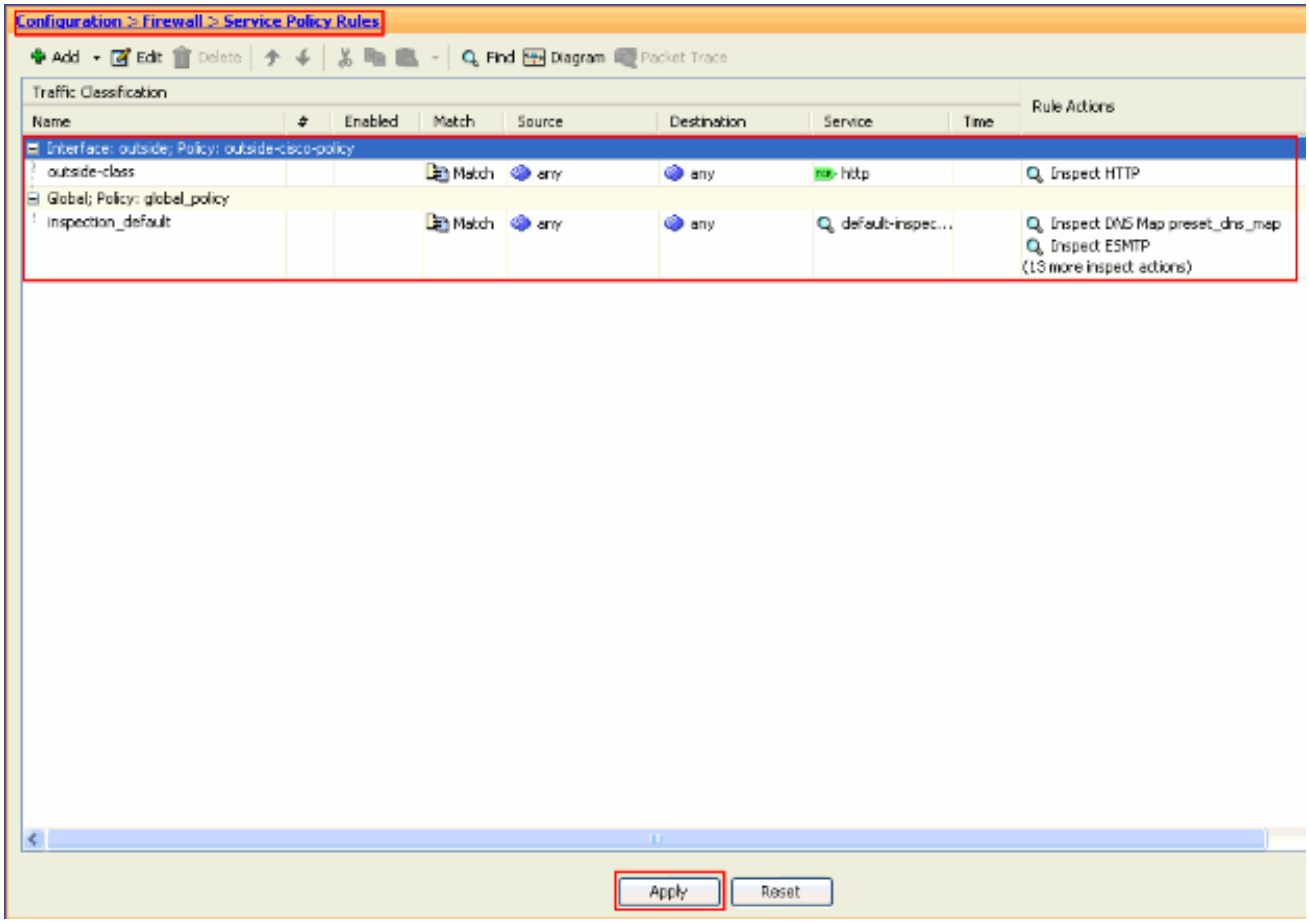


OK.

9. Click **Finish**.



10. Under **Configuration > Firewall > Service Policy Rules**, you will see the newly configured Service Policy **outside-cisco-policy** (to inspect HTTP) along with the default service policy already present on the appliance. Click **Apply** in order to apply the configuration to the Cisco
ASA.



Related Information

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Adaptive Security Device Manager
- Requests for Comments (RFCs)
- Applying Application Layer Protocol Inspection
- Technical Support & Documentation - Cisco Systems