ASA/PIX 7.X: Disable Default Global Inspection and Enable Non-Default Application Inspection Using ASDM

Contents

Introduction

This document describes how to remove the default inspection from global policy for an application and how to enable the inspection for a non-default application.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Adaptive Security Appliance (ASA) that runs the 7.x software image.

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.

Related Products

This configuration can also be used with the PIX Security Appliance that runs the 7.x software image.

Conventions

Refer to 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.)

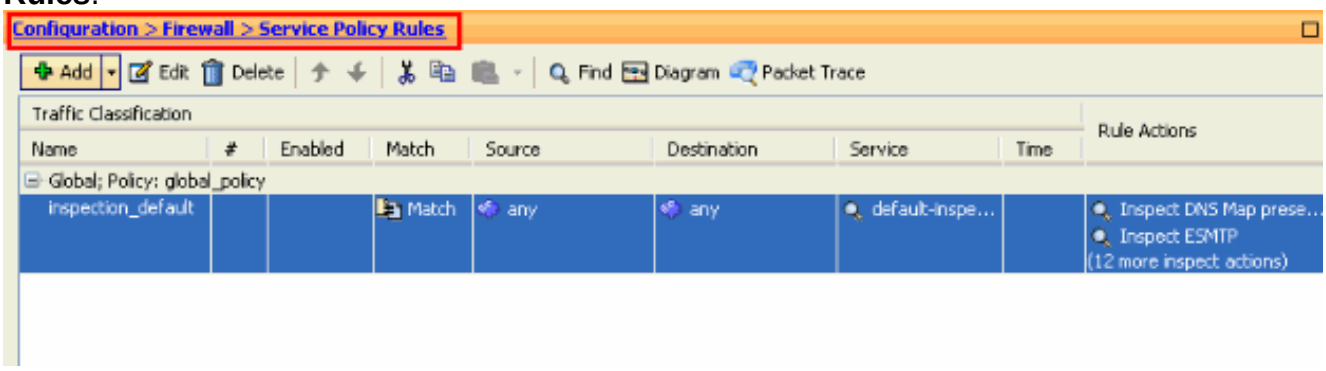
The default policy configuration includes these commands:

```
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
```

Enable Non-Default Application Inspection

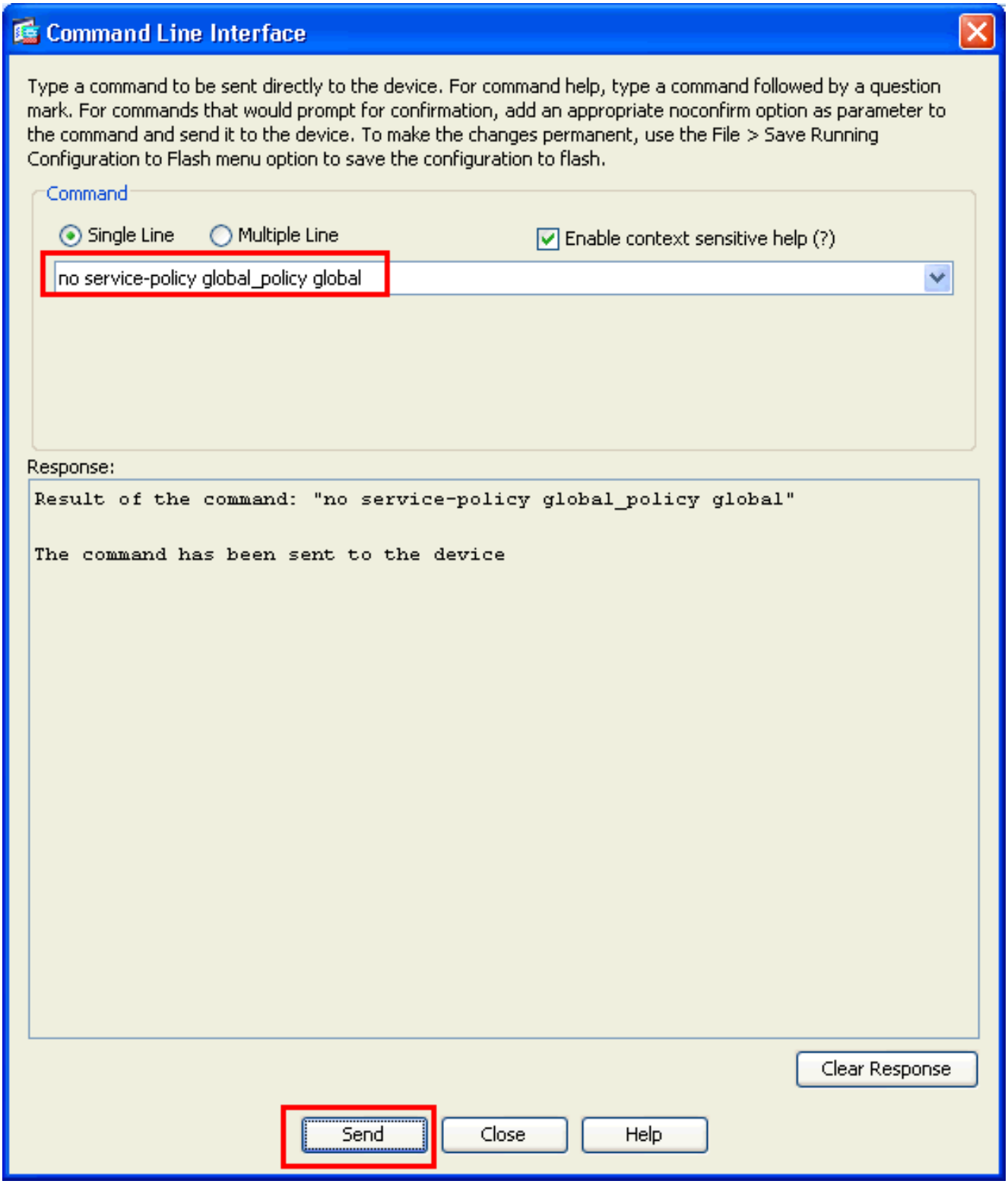
Complete this procedure to enable Non-Default Application Inspection on the Cisco ASA:

1. Login to **ASDM**. Go to **Configuration > Firewall > Service Policy Rules**.



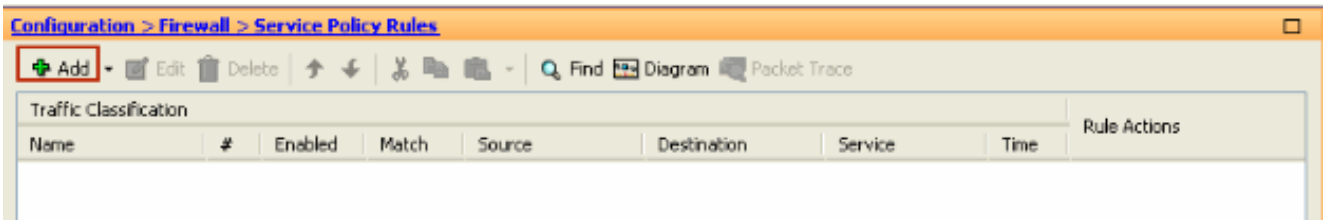
2. If you want to keep the Configuration for Global Policy which includes Default Class-map and

Default Policy-map, but want to remove the policy globally, go to **Tools > Command Line Interface** and use the **no service-policy global-policy global** command to remove the policy globally. Then, click **Send** so the command is applied to the ASA.

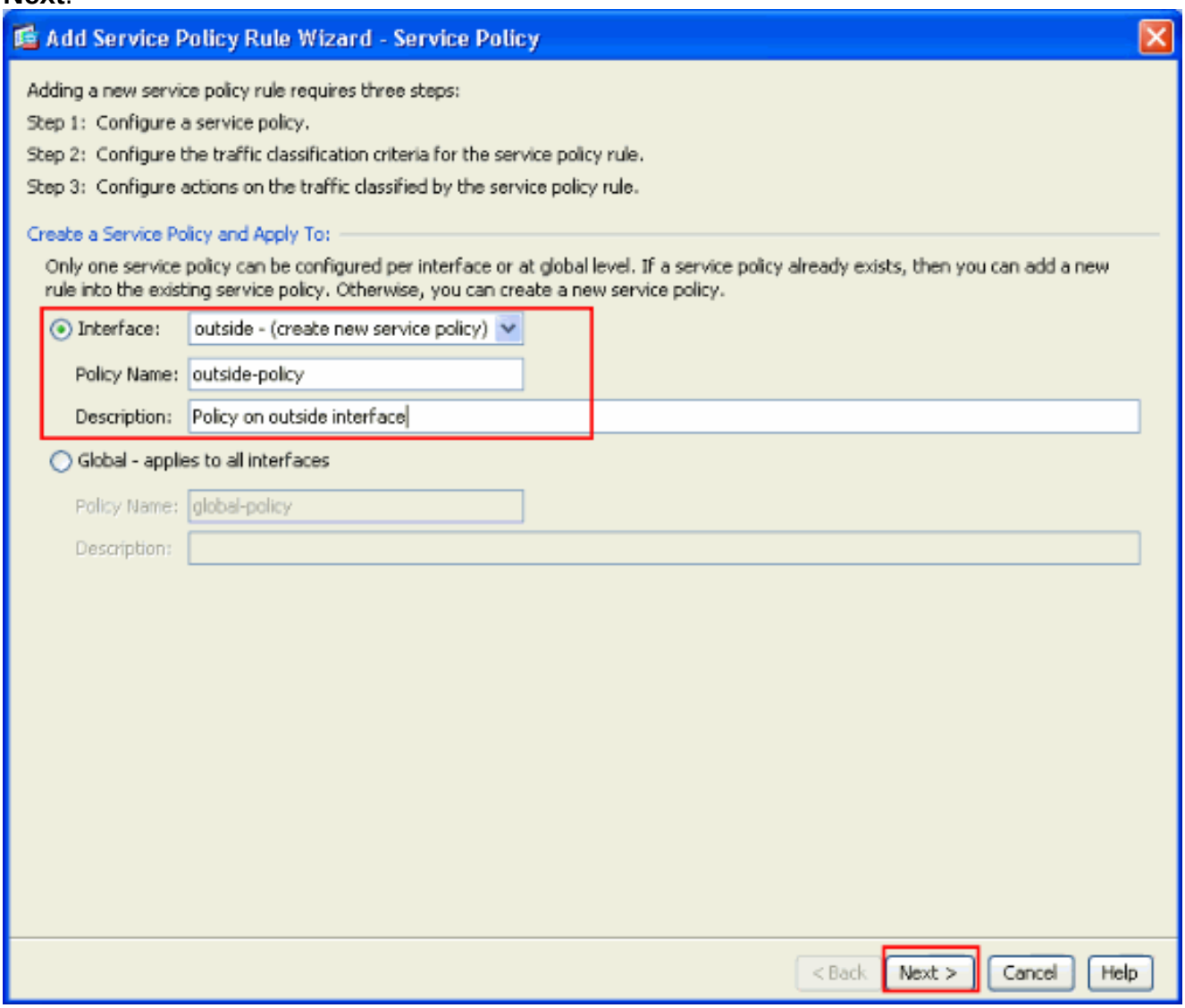


Note: With this step the Global Policy becomes invisible in the Adaptive Security Device Manager (ASDM), but is shown in the CLI.

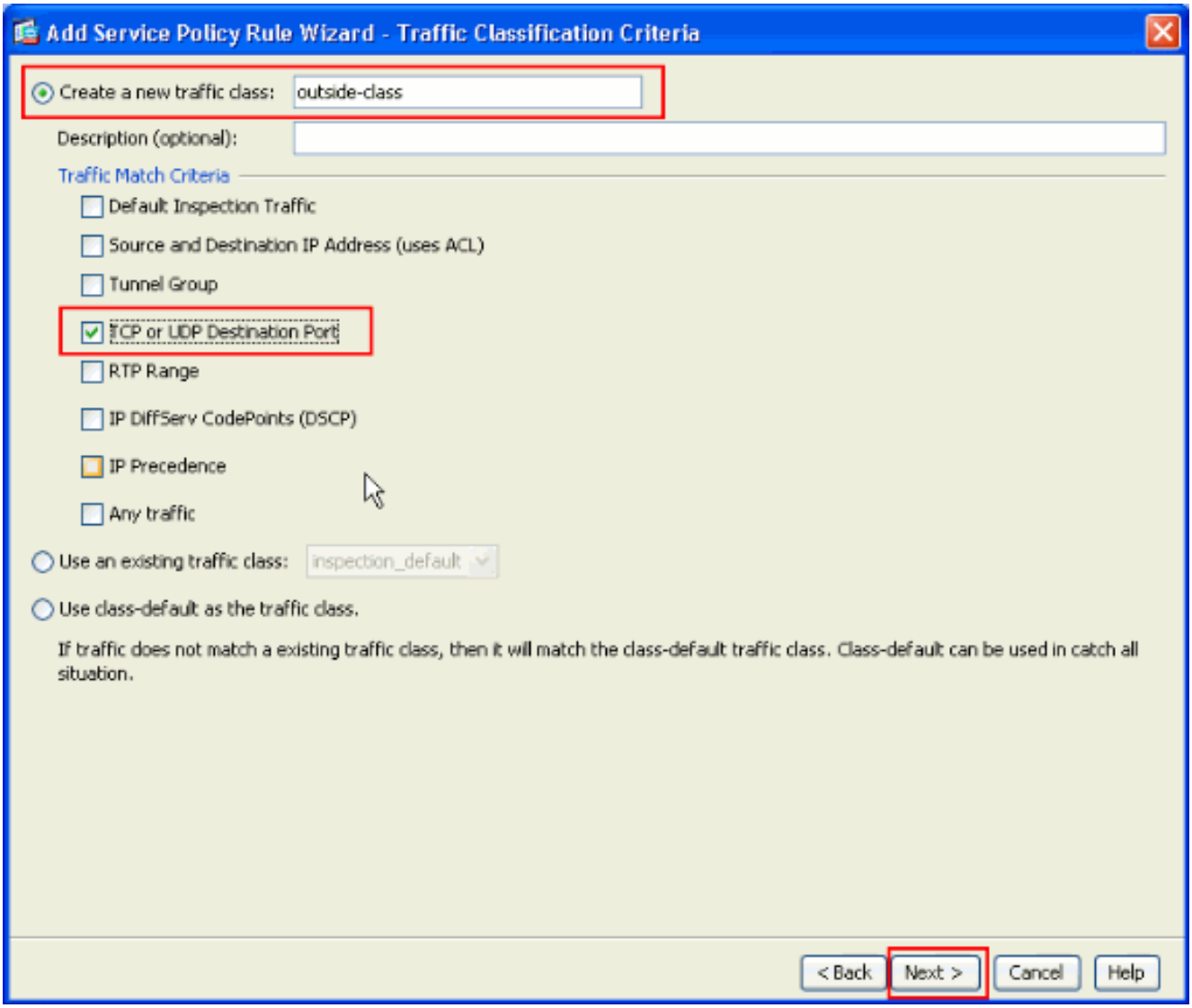
3. Click **Add** in order to add a new policy as shown here:



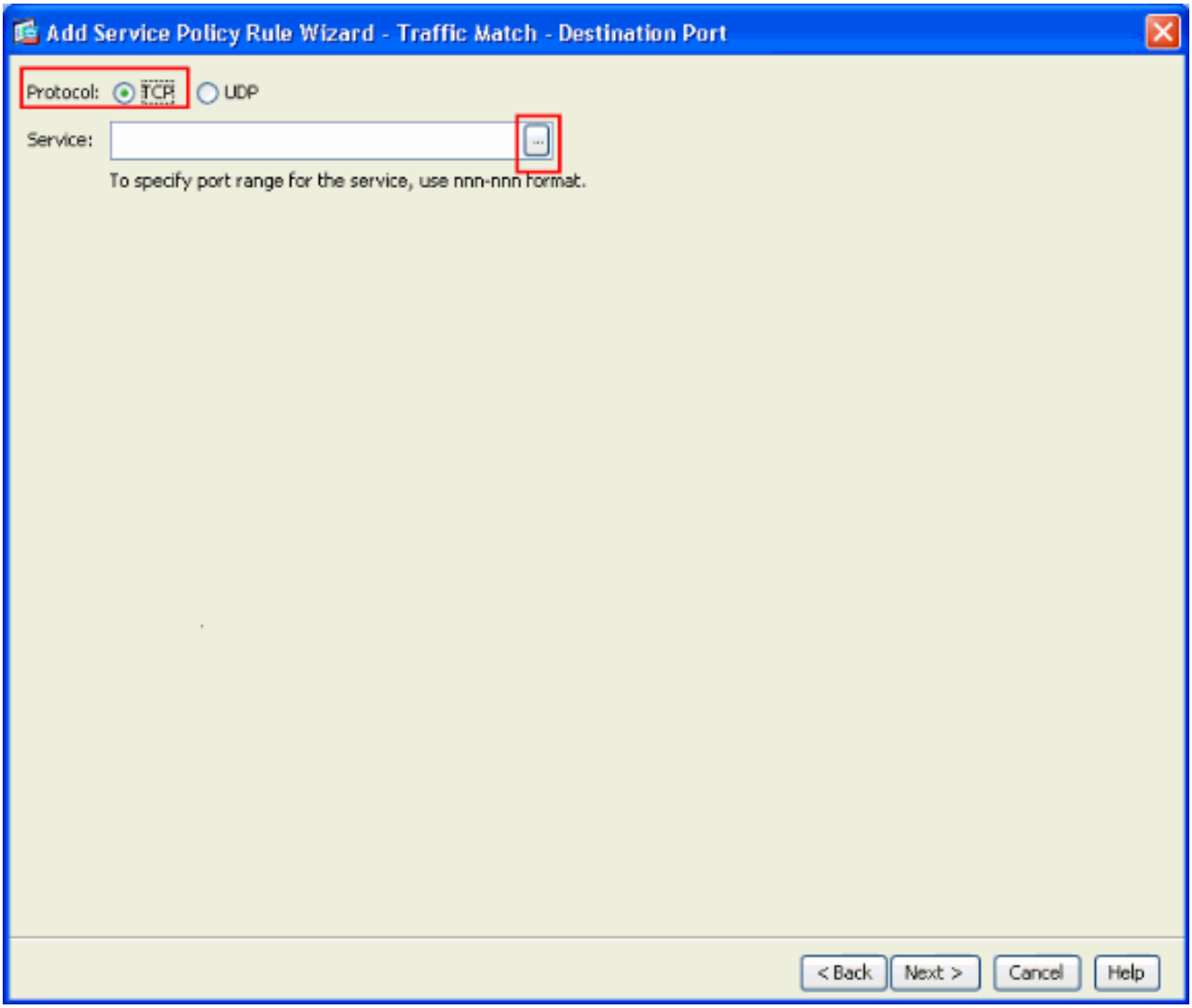
4. Make sure the radio button next to **Interface** is checked and choose the interface you want to apply the policy from the drop-down menu. Then, provide the **Policy Name** and the **Description**. Click
Next.



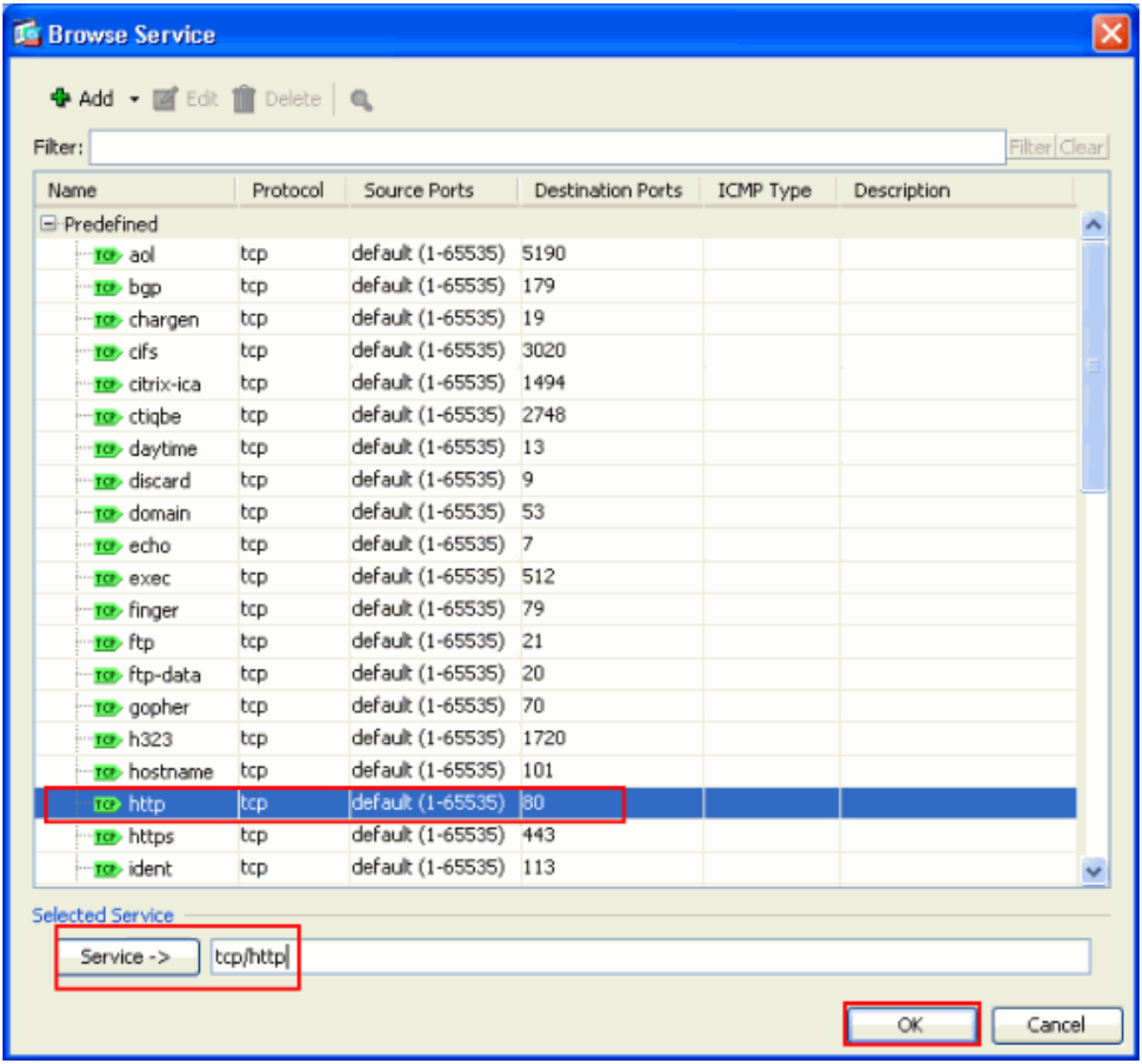
5. Create a new class-map to match the **TCP** traffic as **HTTP** falls under TCP. Click
Next.



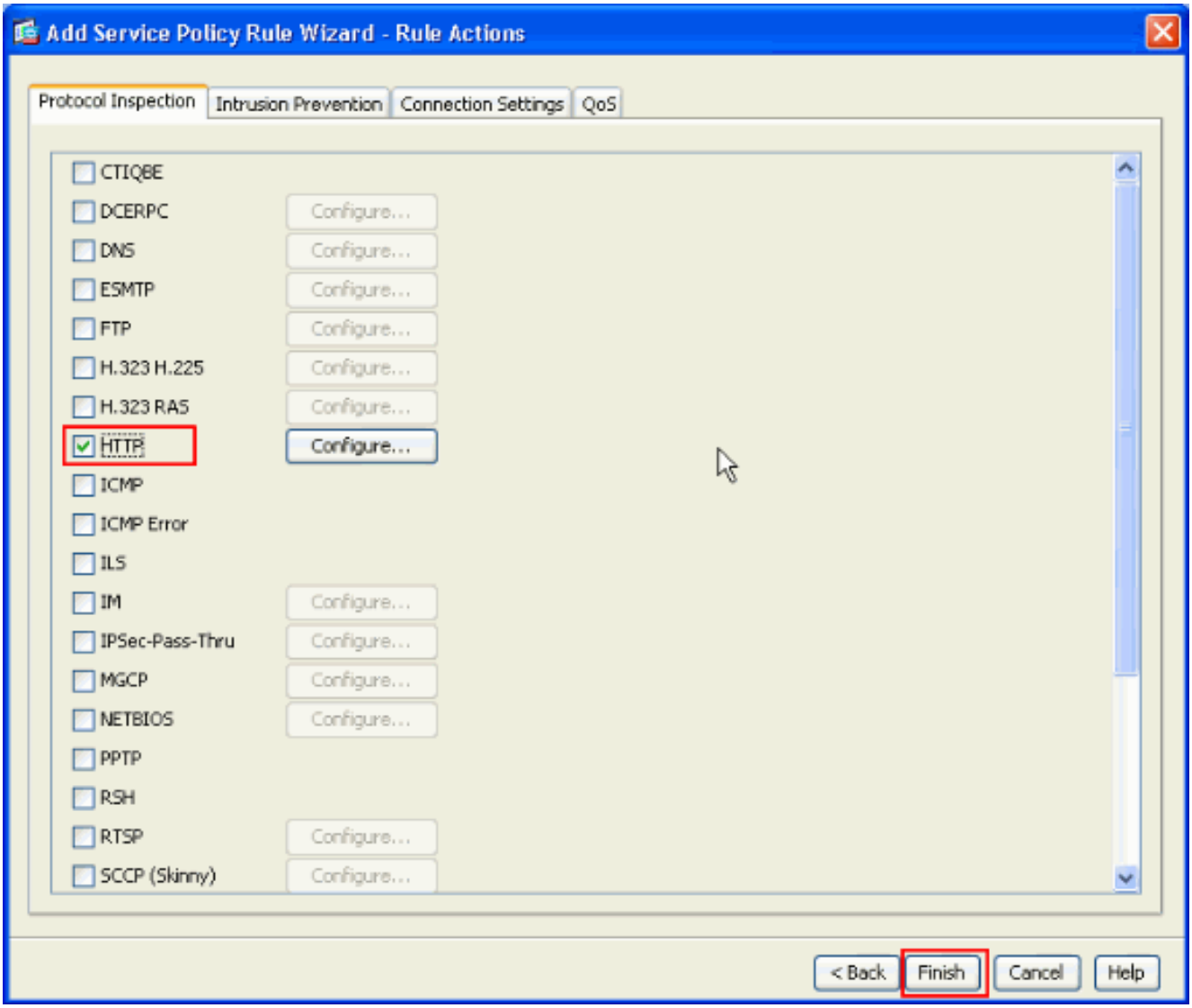
6. Choose **TCP** as the protocol.



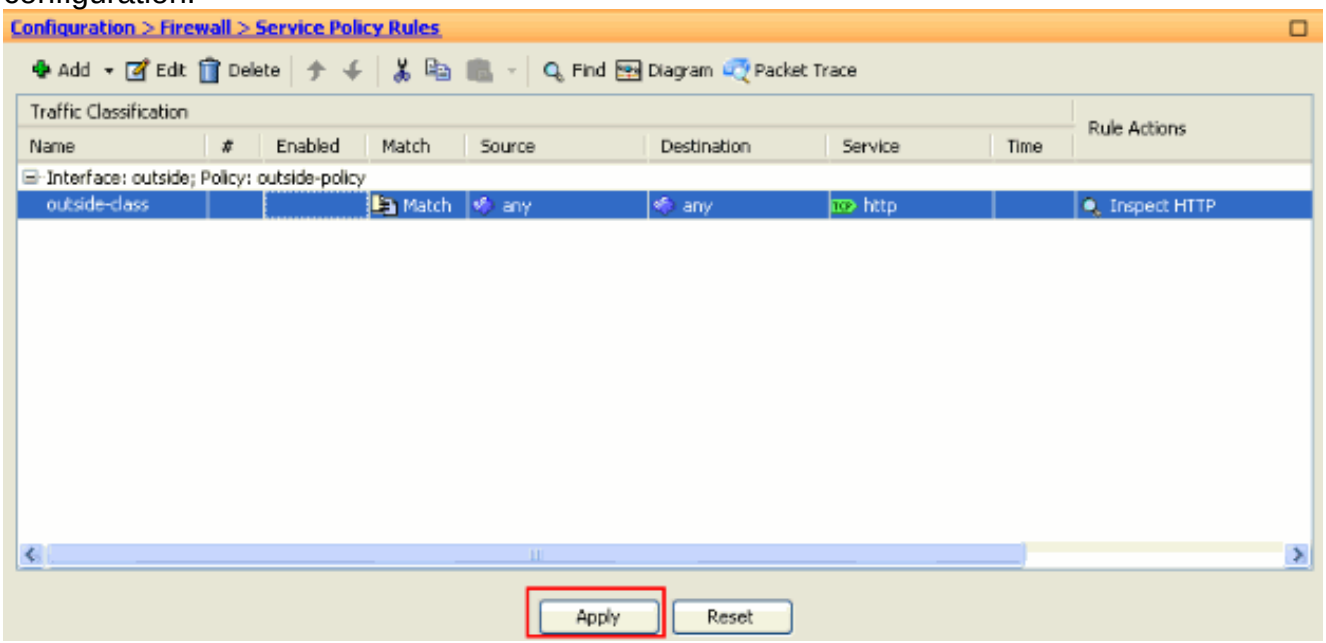
Choose **HTTP port 80** as the Service and click **OK**.



7. Choose **HTTP** and click **Finish**.



8. Click **Apply** to send these configuration changes to the ASA from the ASDM. This completes the
configuration.



Verify

Use these **show** commands to verify the configuration:

- Use the **show run class-map** command to view the class maps configured.
```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class match port tcp eq www !
```
- Use the **show run policy-map** command to view the policy maps configured.
```
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 the **show run service-policy** command to view the service policies configured.
```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

Related Information

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500 Series Command References
- Cisco Adaptive Security Device Manager (ASDM) Support Page
- Cisco PIX Firewall Software
- Requests for Comments (RFCs)
- Cisco PIX 500 Series Security Appliances
- Applying Application Layer Protocol Inspection
- Cisco Secure PIX Firewall Command References
- Technical Support & Documentation - Cisco Systems