ASA 8.3及更高版本 — 使用ASDM配置检测

目录

简介

本文档为8.3(1)版及更高版本的思科自适应安全设备(ASA)提供配置示例，说明如何从应用的全局策略中删除默认检测以及如何使用自适应安全设备管理器(ASDM)启用非默认应用的检测。

请参阅PIX/ASA 7.X:对于8.2及更低版本的Cisco ASA上的相同配置，禁用默认全局检测并启用非默认应用检测。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于带ASDM 6.3的思科ASA安全设备软件版本8.3(1)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

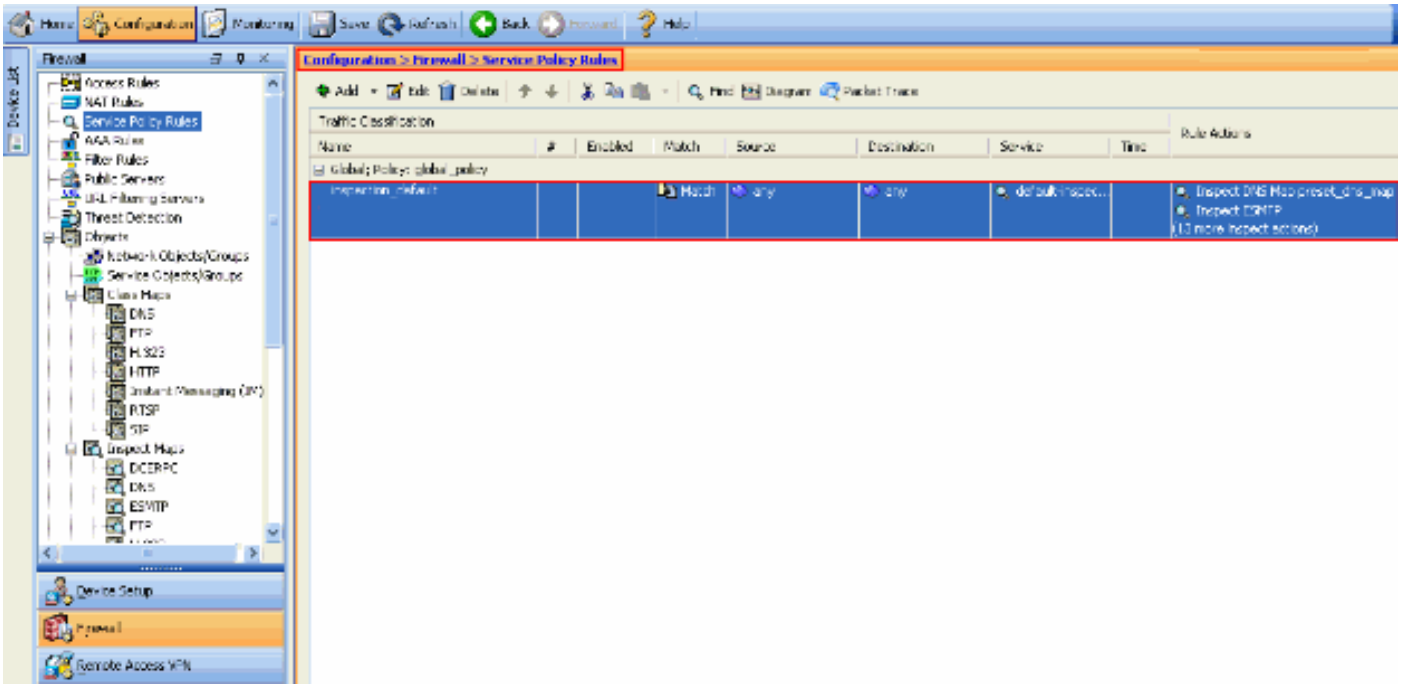
有关文档约定的更多信息，请参考 Cisco 技术提示约定。

默认全局策略

默认情况下，配置包含的策略（全局策略）与所有默认应用程序检查数据流相匹配，并可对所有接

口上的数据流应用特定检查。 默认情况下，并非所有检查都会启用。只能应用一个全局策略。如果希望修改全局策略，则必须编辑默认策略或禁用该策略并应用新的策略。（接口策略将覆盖全局策略。）

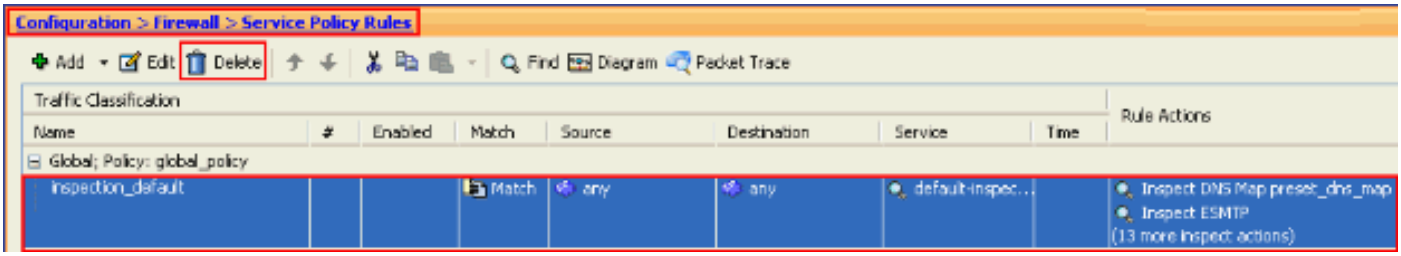
在ASDM中，选择**Configuration > Firewall > Service Policy Rules**以查看具有默认应用检测的默认全局策略，如下所示：



默认策略配置包括以下命令：

```
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
```

如果需要禁用全局策略，请使**用no service-policy global_policy全局命**令。要使用ASDM删除全局策略，请选择**Configuration > Firewall > Service Policy Rules**。然后，选择全局策略并单击**删除**。



注意：使用ASDM删除服务策略时，关联的策略和类映射将被删除。但是，如果使用CLI删除服务策略，则仅从接口删除服务策略。类映射和策略映射保持不变。

禁用应用程序的默认全局检查

要禁用应用程序的全局检查，请使用 **inspect 命令的** *no 版本*。

例如，要删除对安全设备监听的 FTP 应用程序的全局检查，请在类配置模式下使用 **no inspect ftp 命令。**

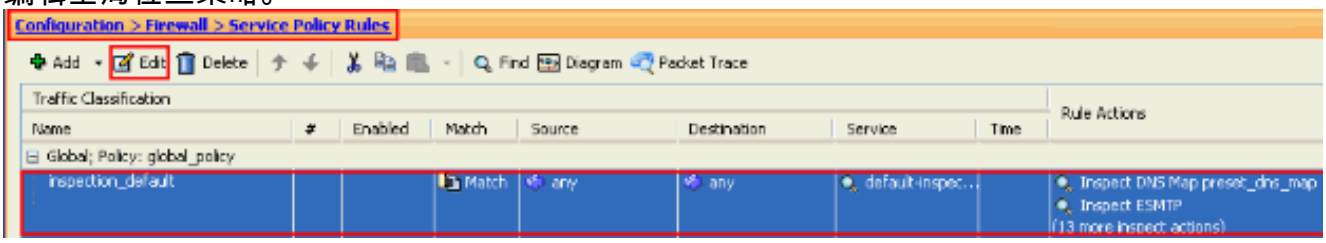
可以从策略映射配置模式访问类配置模式。要删除该配置，请使用该命令的 *no 形式*。

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

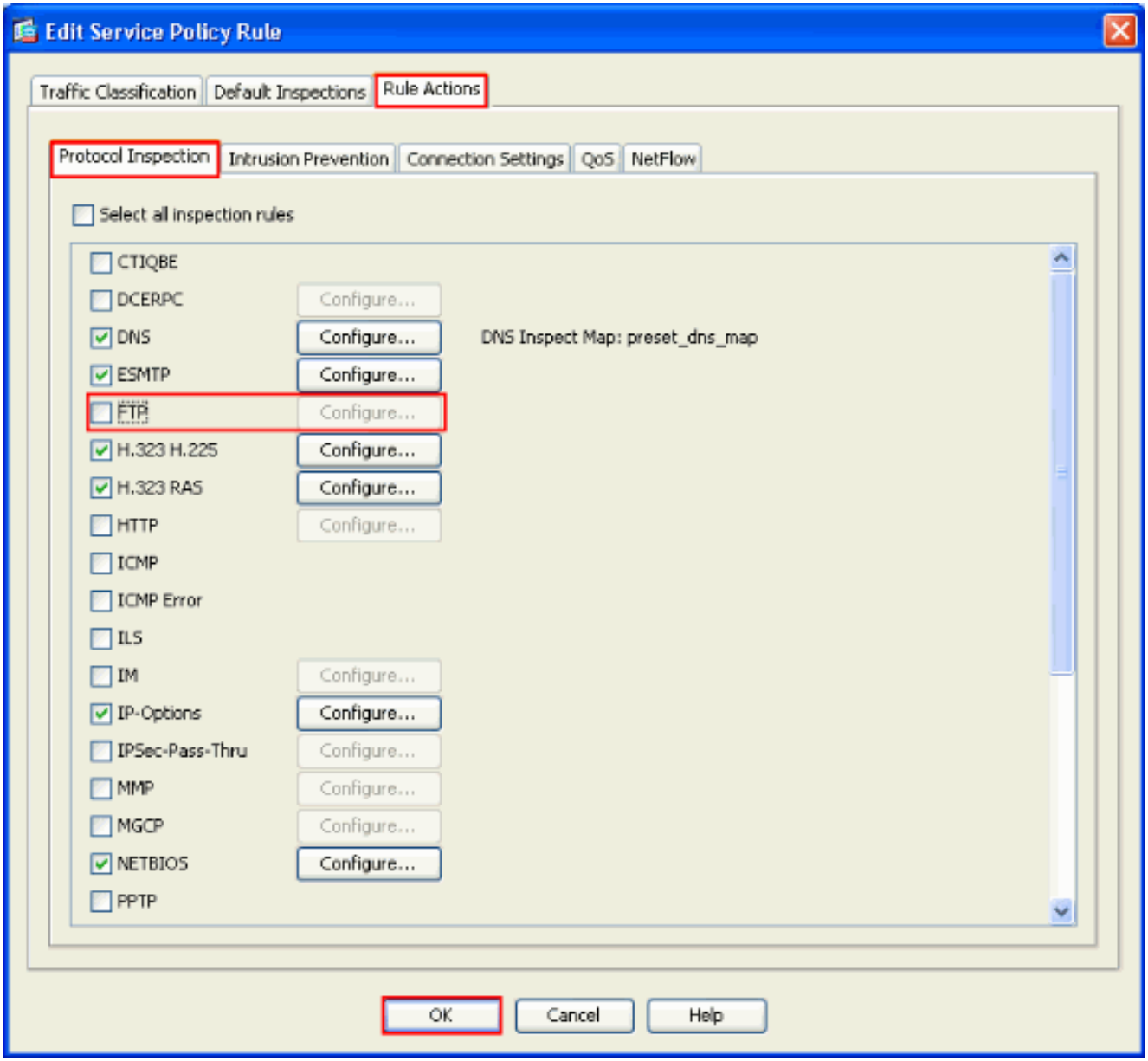
要禁用使用ASDM的FTP全局检查，请完成以下步骤：

注意：要通过ASDM访问PIX/ASA，请参阅允许ASDM的HTTPS访问以获取基本设置。

1. 选择**Configuration > Firewall > Service Policy Rules**并选择默认全局策略。然后，单击**Edit**以编辑全局检查策略。



2. 从Edit Service Policy Rule窗口，在Rule Actions选项卡**下选**择Protocol Inspection**。确保未选中FTP**复选框。这会禁用FTP检测，如下一个映像所示。然后，单击**OK(确**定)，然**后单击Apply**。



注：有关FTP检测的详细信息，请参阅PIX/ASA 7.x:启用 FTP/TFTP 服务配置示例。

启用非默认应用程序的检查

默认情况下，增强型 HTTP 检查处于禁用状态。要在global_policy中启用HTTP检测，请在class inspection_default下使**用inspect http**命令。

在本示例中，通过任何接口进入安全设备的所有 HTTP 连接（端口 80 上的 TCP 数据流）都将归类为需要进行 HTTP 检查。*由于该策略为全局策略，因此，只有当数据流进入每个接口时才会进行检查*。

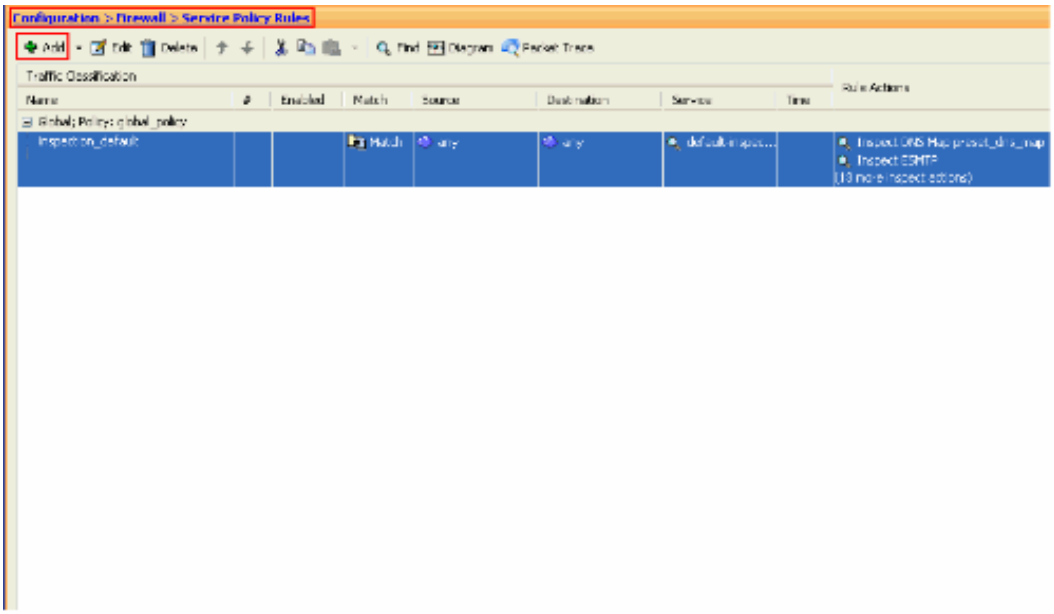
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

在本示例中，通过外部接口进入或流出安全设备的所有 HTTP 连接（端口 80 上的 TCP 数据流）*都将归类为需要进行 HTTP 检查*。

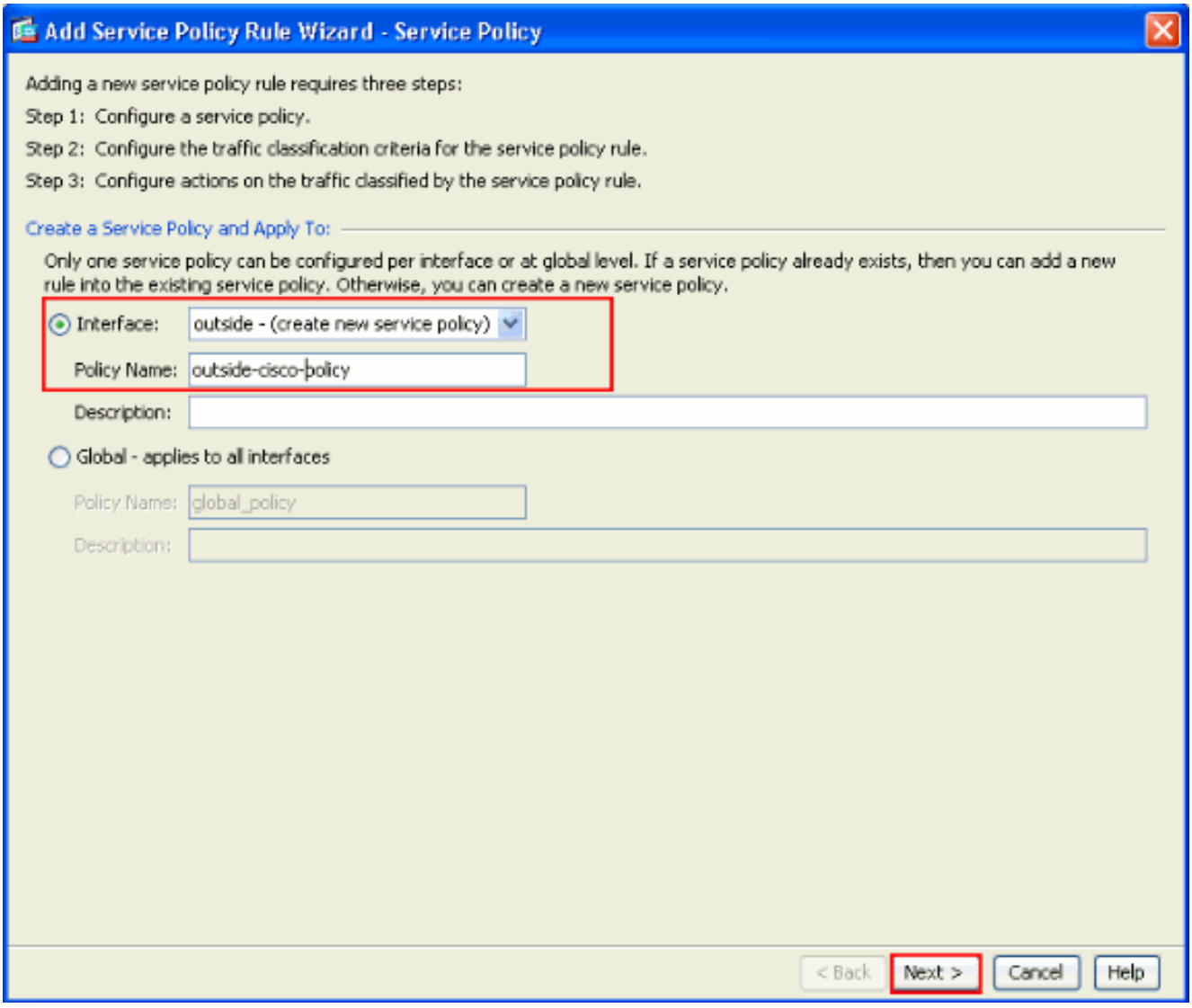
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

要使用ASDM配置上述示例，请执行以下步骤：

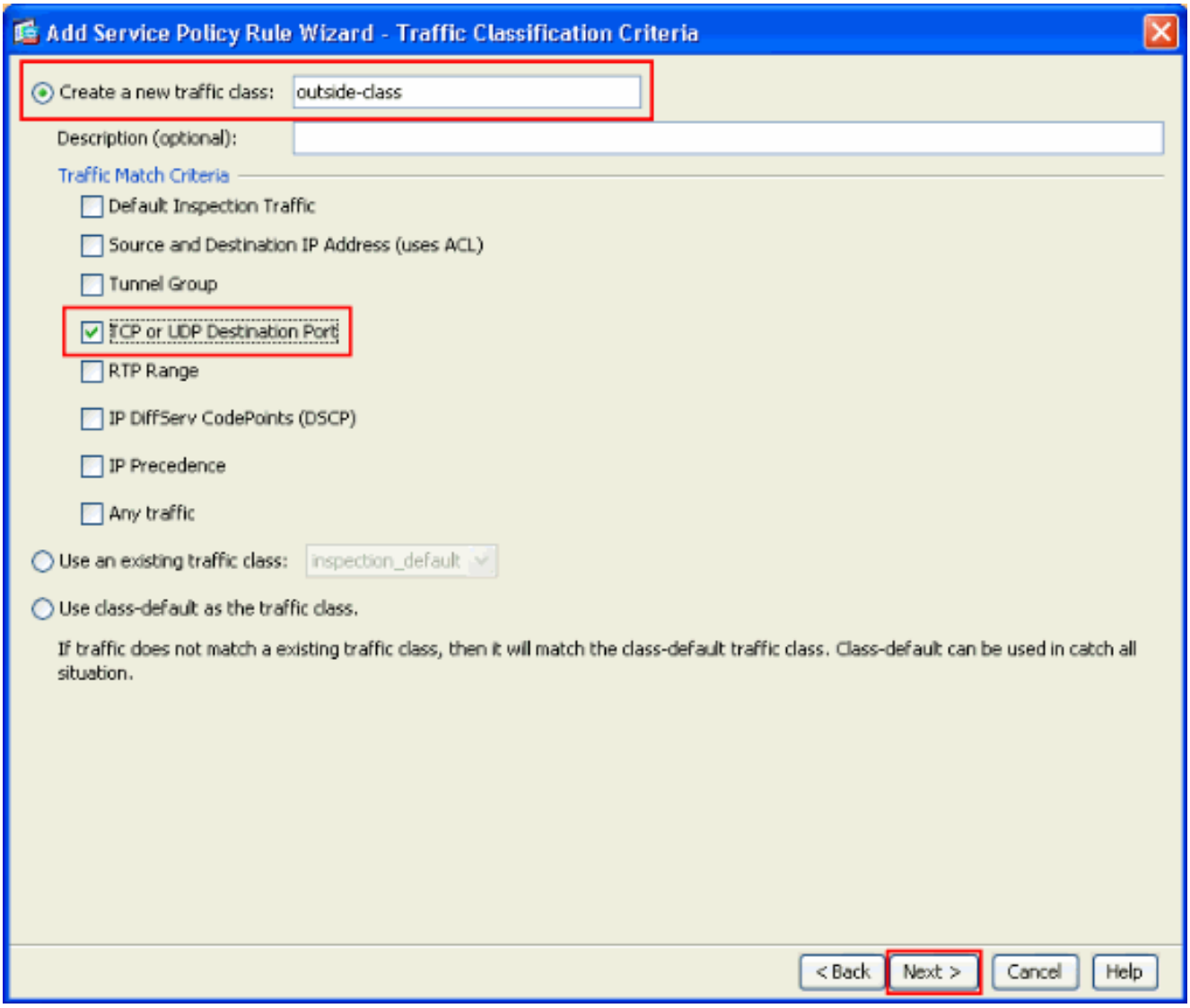
1. 选择**Configuration > Firewall > Service Policy Rules**，然后单击**Add**以添加新的服务策略：



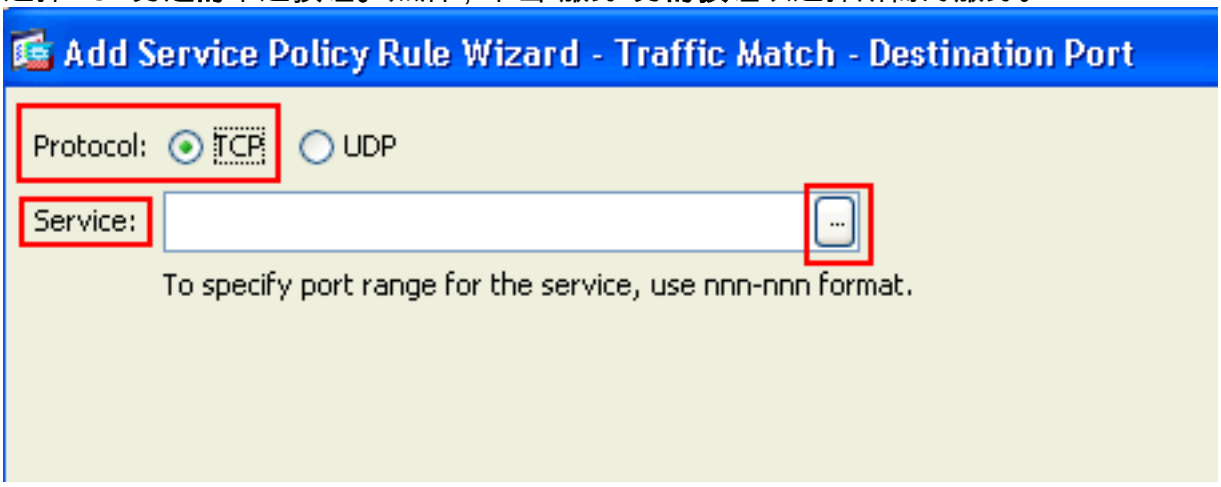
2. 从Add Service Policy Rule Wizard - Service Policy窗口，选择Interface旁的单选按钮。这会将创建的策略应用到特定接口，即本例中的**外部**接口。提供策略名称，在本**例中为外部**cisco-policy。单击 **Next**。



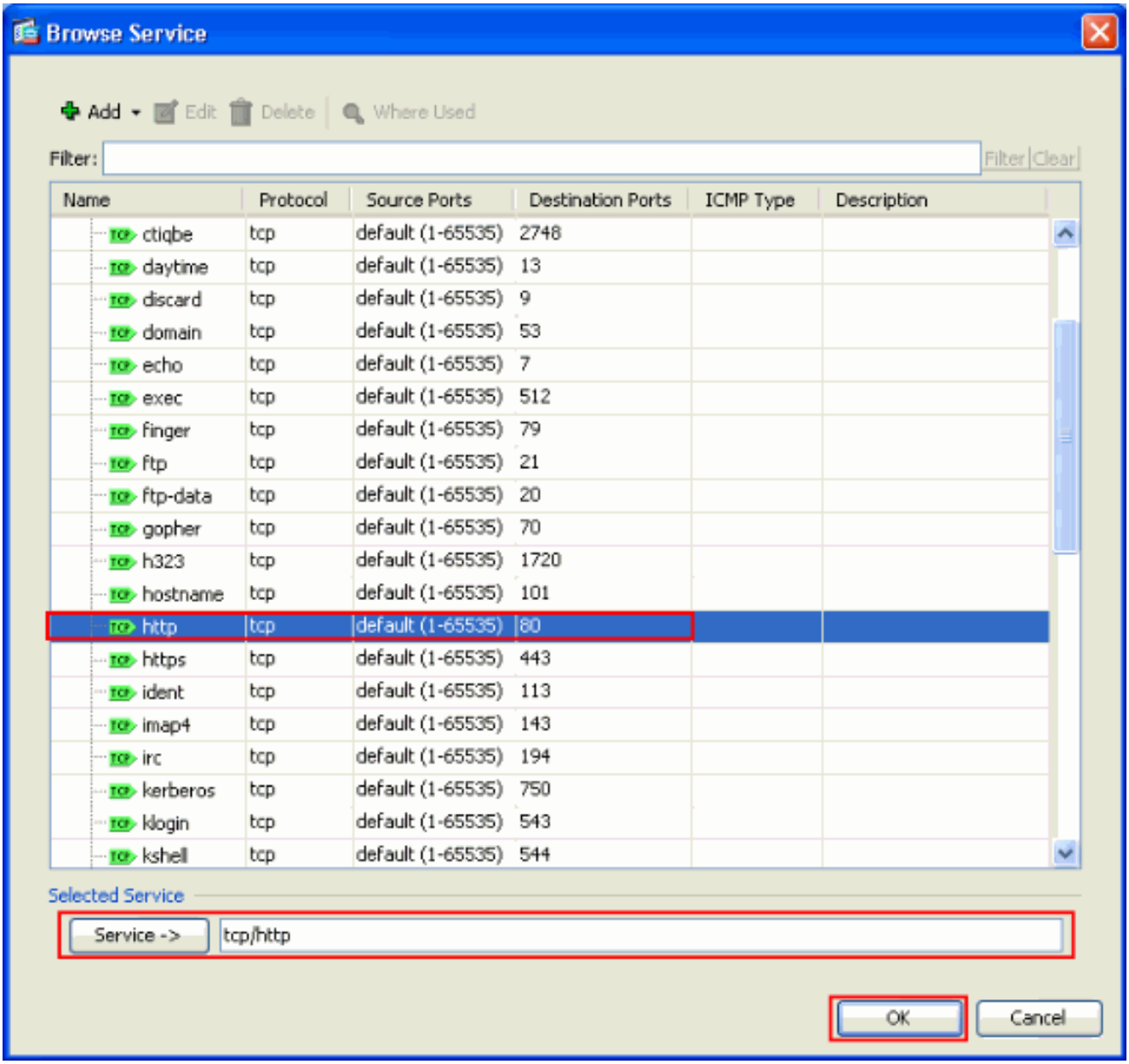
3. 从Add Service Policy Rule Wizard - Traffic Classification Criteria窗口，提供新的流量类名。本示例中使用的名称**为outside-class**。确保选中TCP或UDP Destination Port旁**的复选框，然**后单击“下**一步”**。



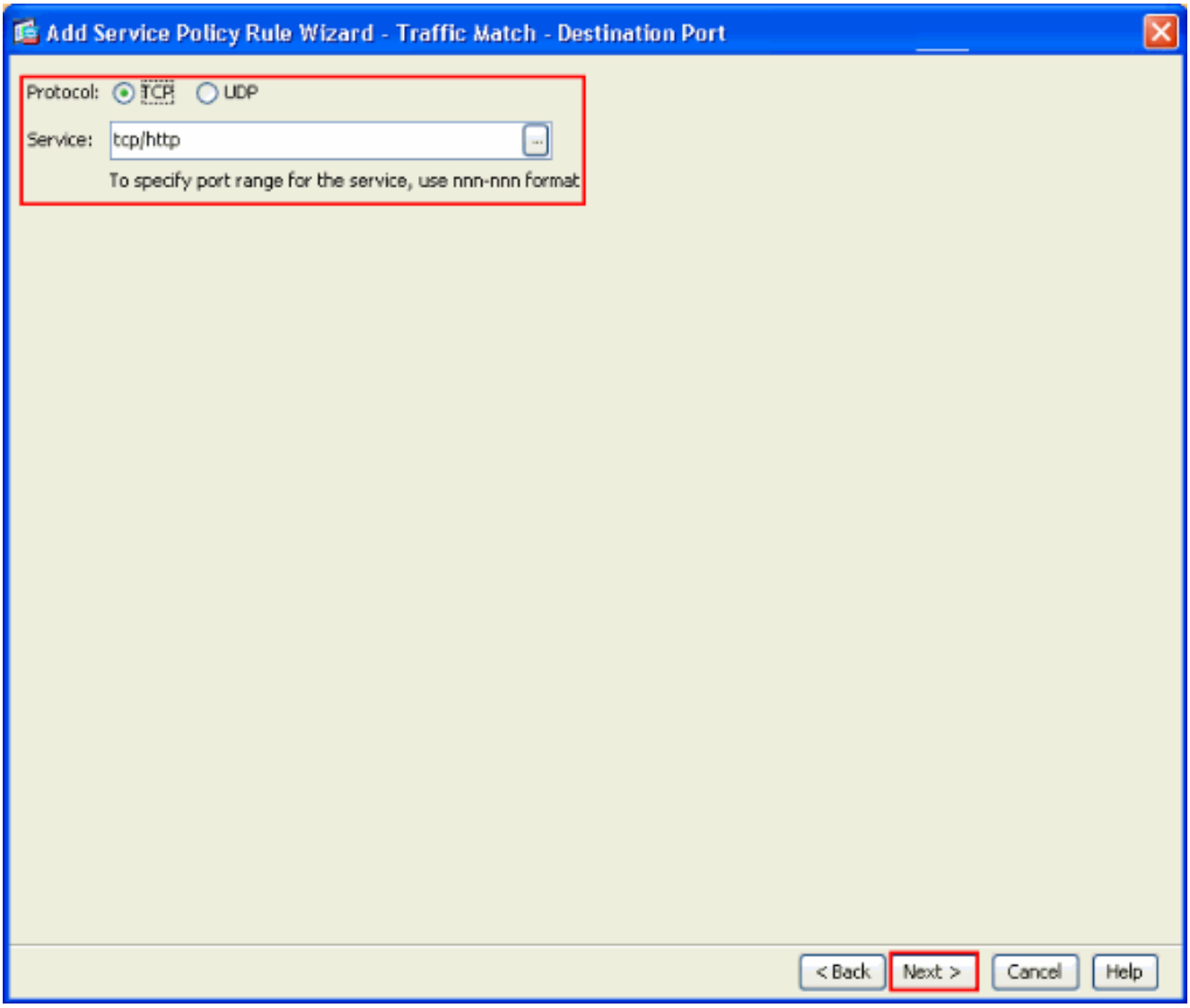
4. 从Add Service Policy Rule Wizard - Traffic Match - Destination Port窗口，在Protocol部分下选择TCP旁**边的**单选按钮。然后，单击“服务”旁**的按**钮以选择所需的服务。



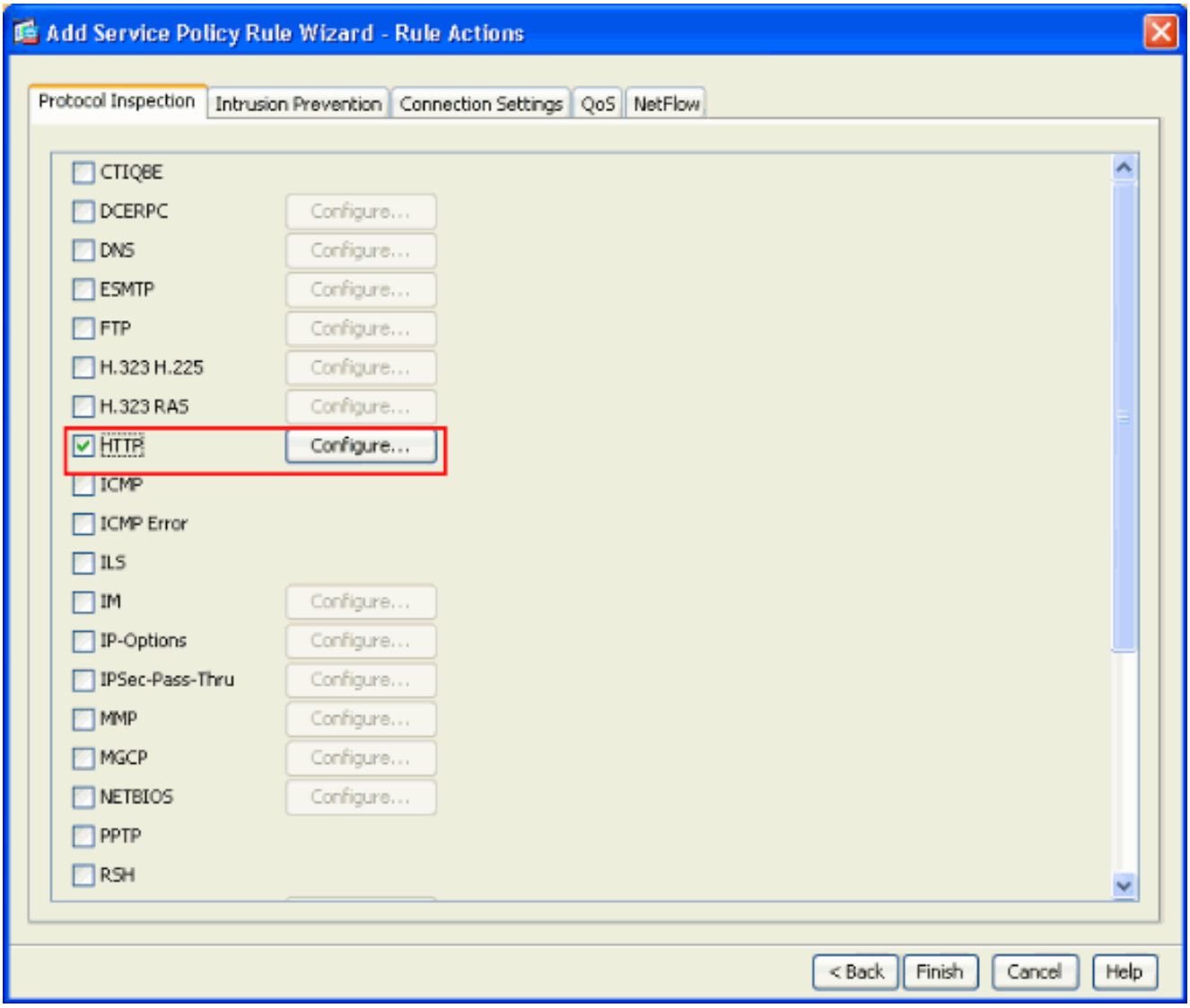
5. 从“浏览服务”窗口中，选**择HTTP**作为服务。然后，单击**OK**。



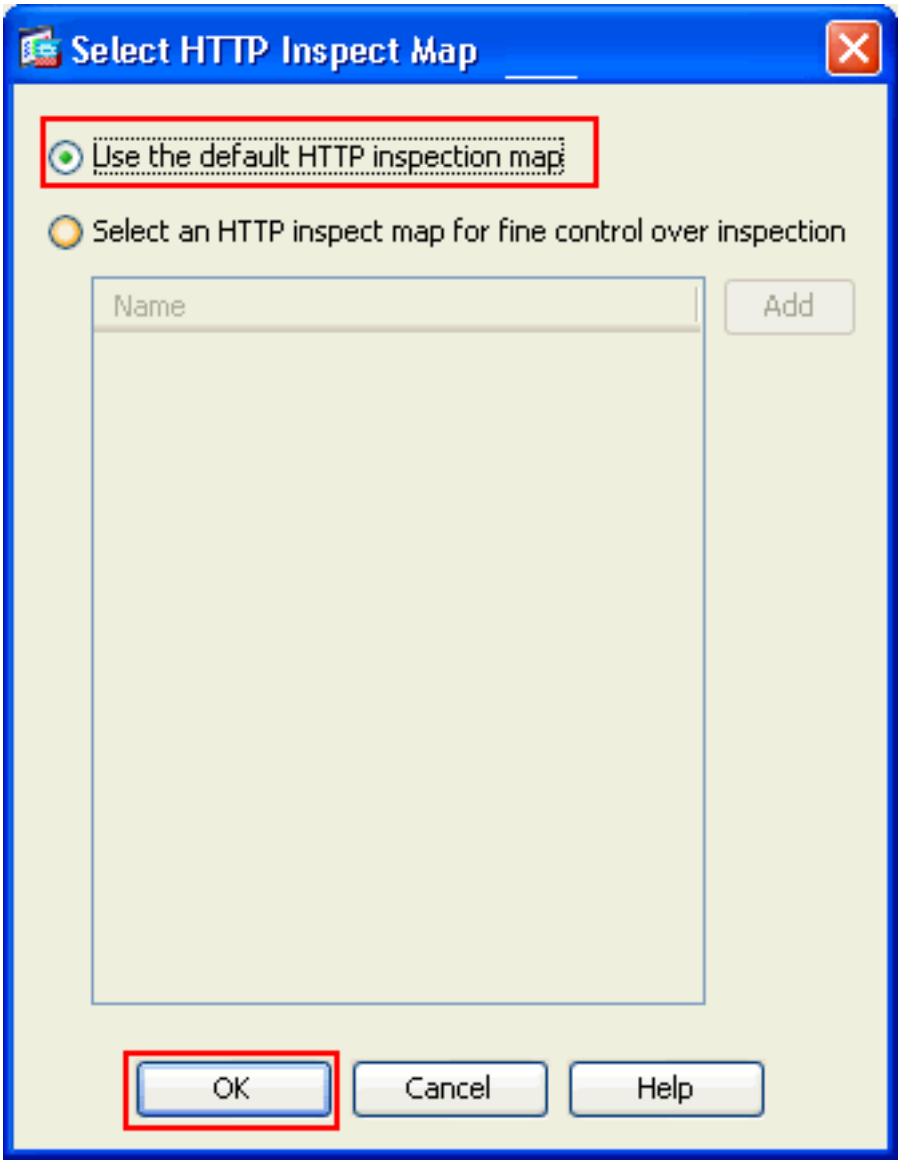
6. 从“添加服务策略规则向导 — 流量匹配 — 目标端口”窗口中，可以看到选**择的**服务是**tcp/http**。单击 **Next**。



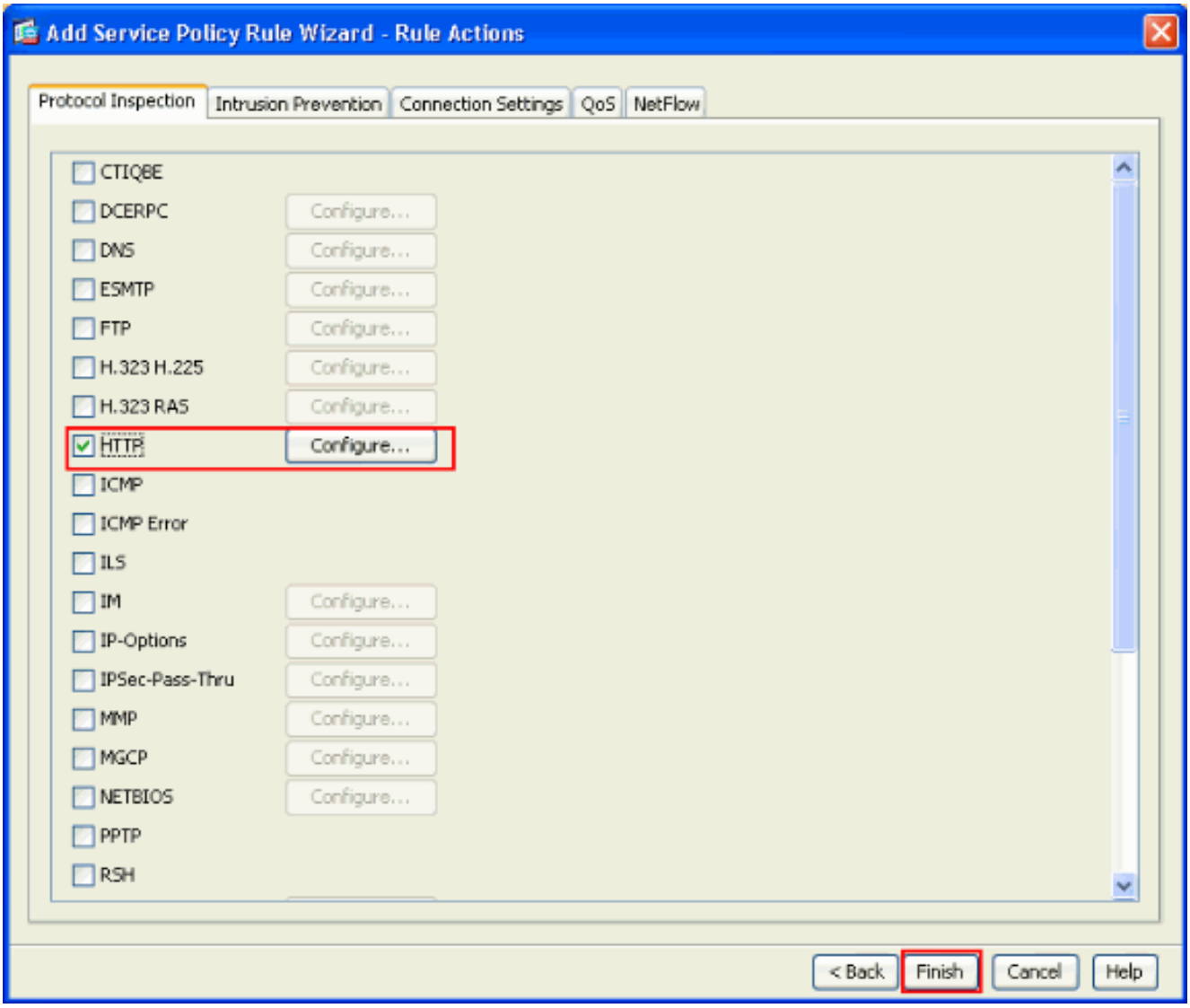
7. 在Add Service Policy Rule Wizard - Rule Actions窗口中，选中HTTP旁的复**选框**。然后，单击**HTTP旁**边的**Configure**。



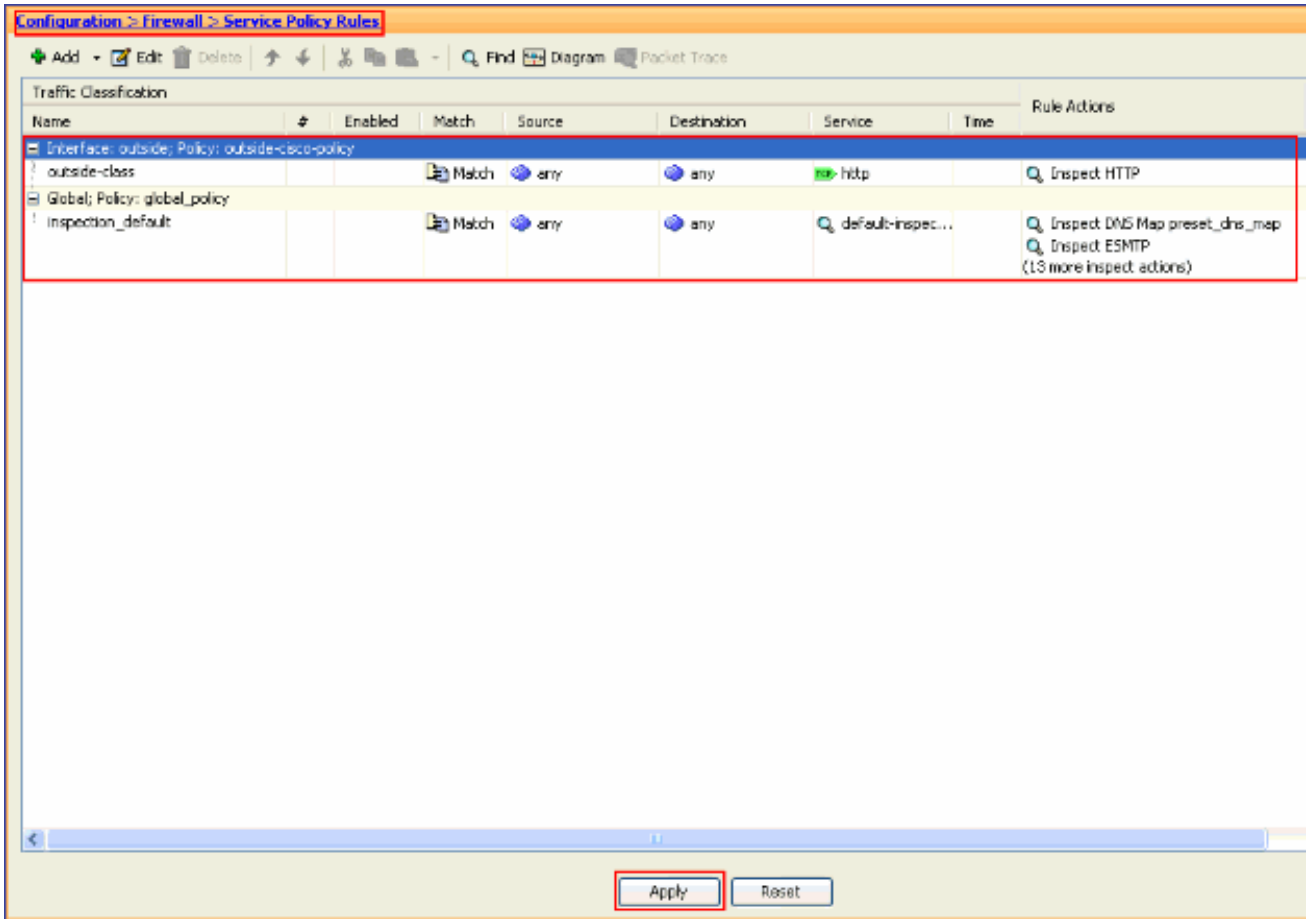
8. 在Select HTTP Inspect Map窗口中，选中Use the Default HTTP inspection map旁**的单选按钮**。本示例中使用默认HTTP检测。然后，单击**OK**。


Select HTTP Inspect Map
Use the default HTTP inspection map
Select an HTTP inspect map for fine control over inspection
Name
Add
OK
Cancel
Help

9. 单击 **完成**。



10. 在**Configuration > Firewall > Service Policy Rules**下，您将看到新配置的Service Policy outside-cisco-policy（**用于检查HTTP）以及设备上已存在的默认服务策略。**单击**Apply**以将配置应用到Cisco ASA。



相关信息

- Cisco ASA 5500 系列自适应安全设备
- Cisco 自适应安全设备管理器
- 请求注解 (RFC)
- 应用应用层协议检查
- 技术支持和文档 - Cisco Systems