ASA 8.3 及更高版本：禁用默认全局检查和 Enable (event)非默认应用检查使用ASDM

目录

简介

本文为Cisco可适应安全工具(ASA)提供一配置示例使用可适应安全设备管理器(ASDM)，以版本8.3(1)和稍后如何从应用程序的全局策略删除默认检查和如何启用一非默认应用程序的检查。

请参阅 PIX/ASA 7.x：禁用默认全局检查并且启用相同的配置的非默认应用检查在与版本8.2和以下的Cisco ASA。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据Cisco ASA安全与ASDM 6.3的工具软件版本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。

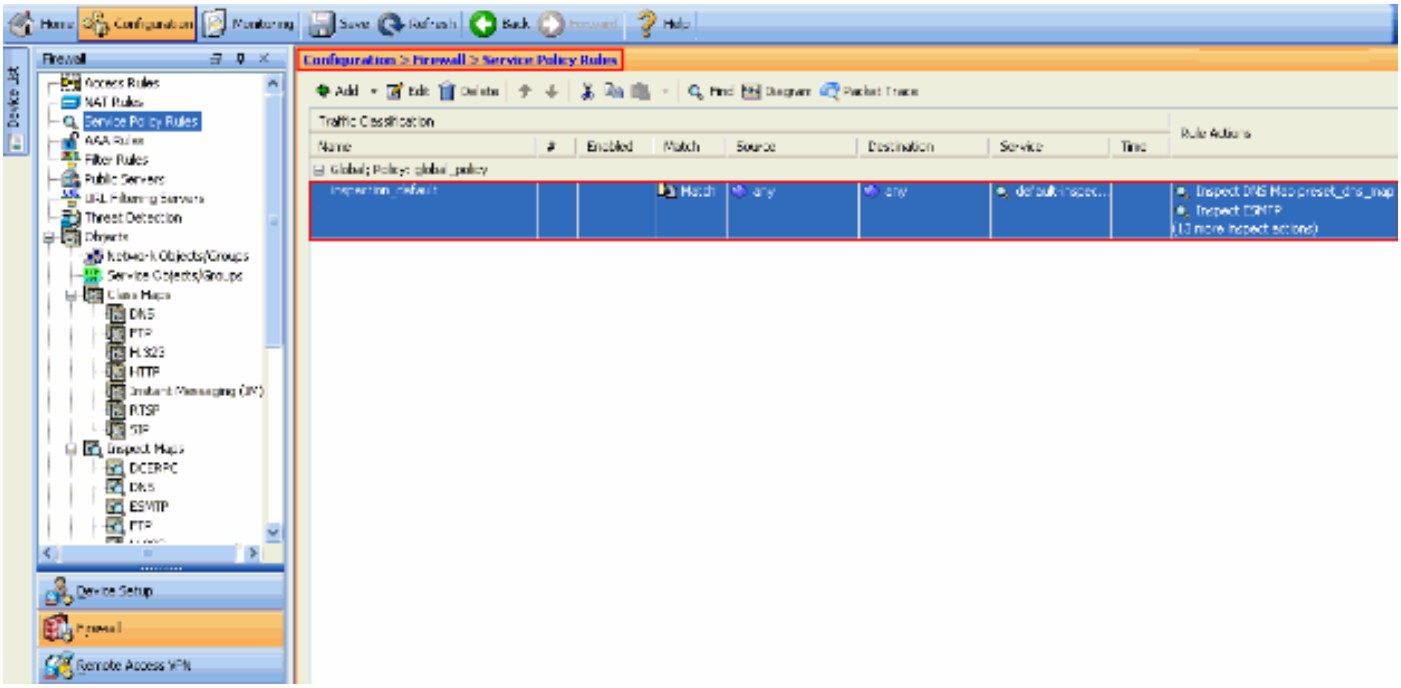
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

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。）

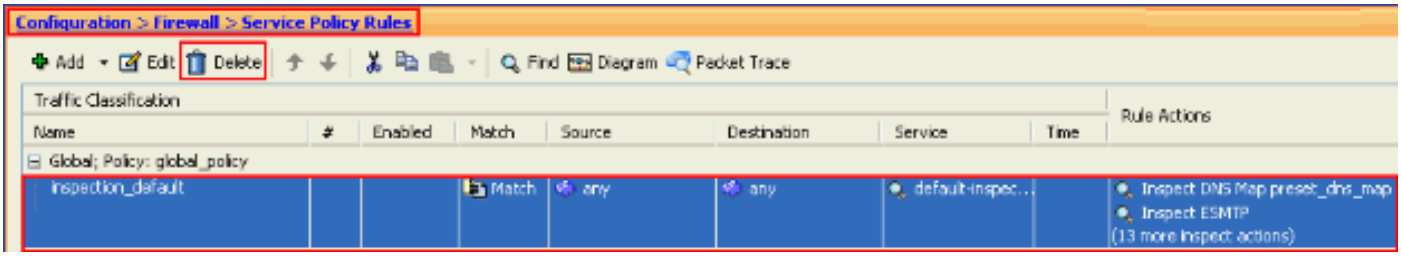
在ASDM，请选择**Configuration>防火墙>服务策略规则**查看有默认应用检查如显示此处的默认全局策略：



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，请勿请使用**服务策略global_policy global命令**。为了删除全局策略使用ASDM请选择**Configuration>防火墙>服务策略规则**。然后，请选择全局策略并且点击**删除**。



注意： 当您删除与ASDM时的服务策略，相关的策略和类映射删除。然而，如果服务策略删除使用CLI仅服务策略从接口删除。类映射和策略映射保持不可更改。

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。

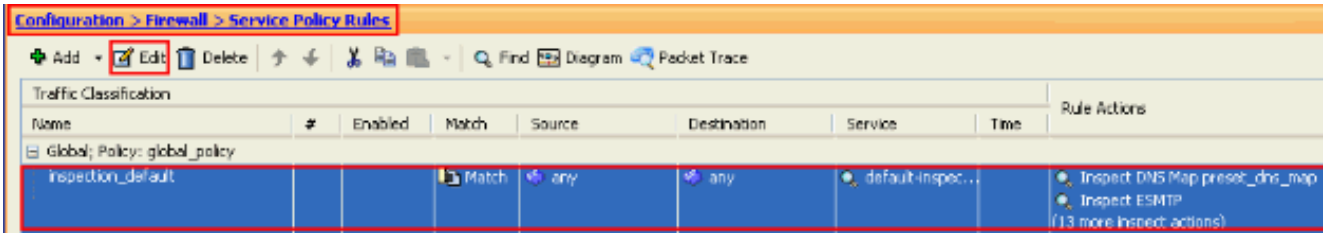
可以从策略映射配置模式访问类配置模式。要删除该配置，请使用该命令的 *no* 形式。

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

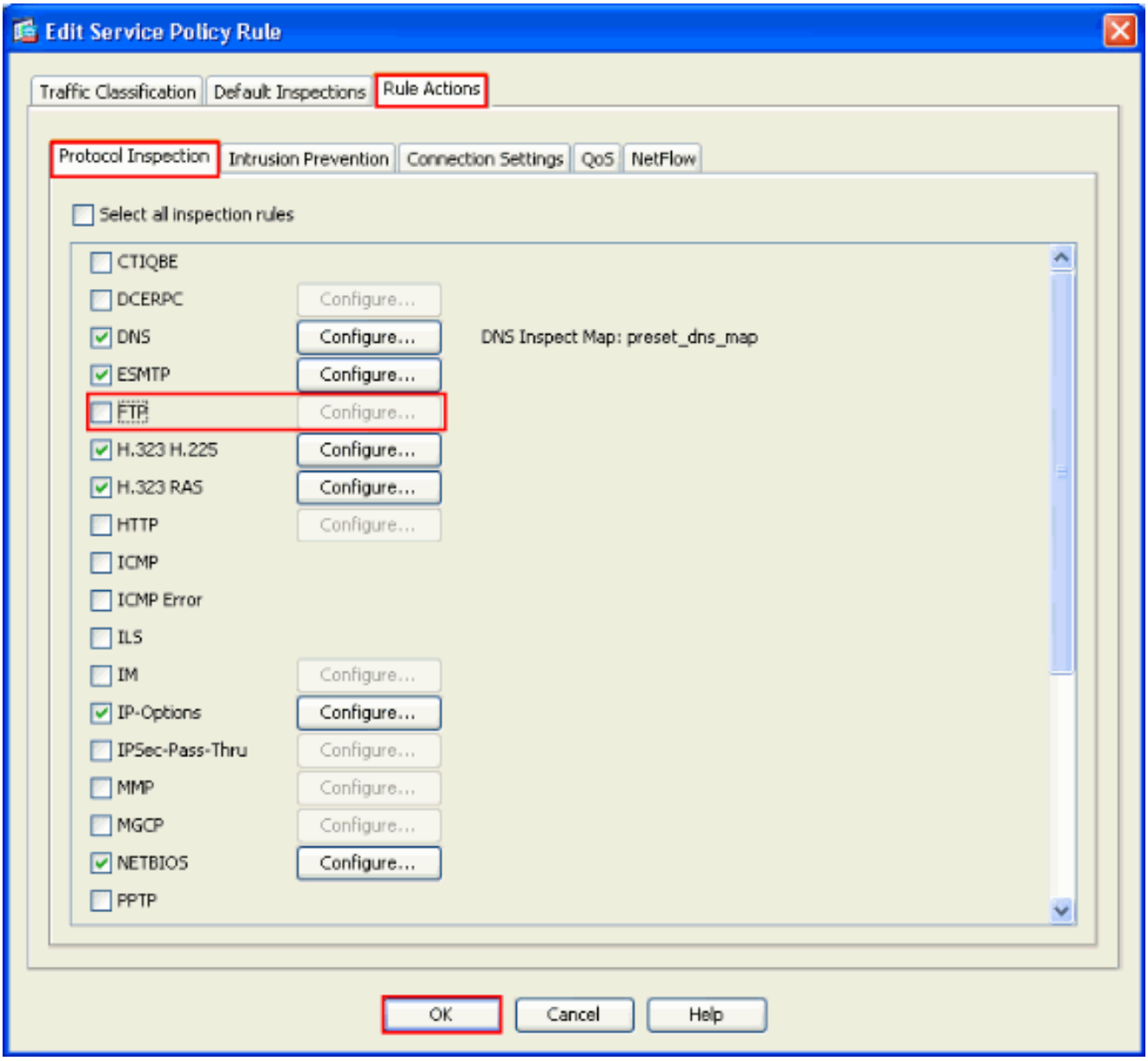
使用ASDM，为了禁用FTP的全局检查，请完成这些步骤：

注意： 请参阅允许 ASDM 的 HTTPS 访问了解基本设置，以通过 ASDM 访问 PIX/ASA。

1. 选择**Configuration>防火墙>服务策略规则**并且选择默认全局策略。然后，请单击**编辑**编辑全局检查策略。



2. 从编辑服务策略规则窗口，请选择**协议检测**在**规则操作**选项卡下。确保**FTP**复选框被不选定。如下镜像所显示，这禁用FTP检查。然后，请点击OK键然后**应用**。



注意： 有关 FTP 检查的详细信息，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。为了启用在global_policy的HTTP检查，请使用**Inspect http**命令在类inspection_default下。

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
```

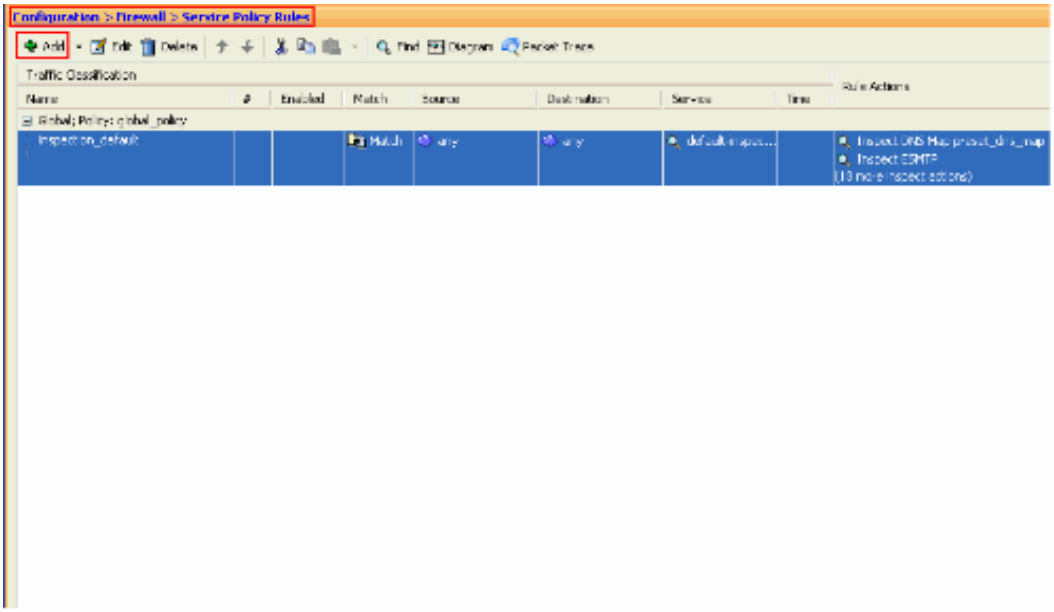
在本示例中，通过外部接口进入或流出安全设备的所有 HTTP 连接（端口 80 上的 TCP 数据流）*都将归类为需要进行 HTTP 检查*。

```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
```

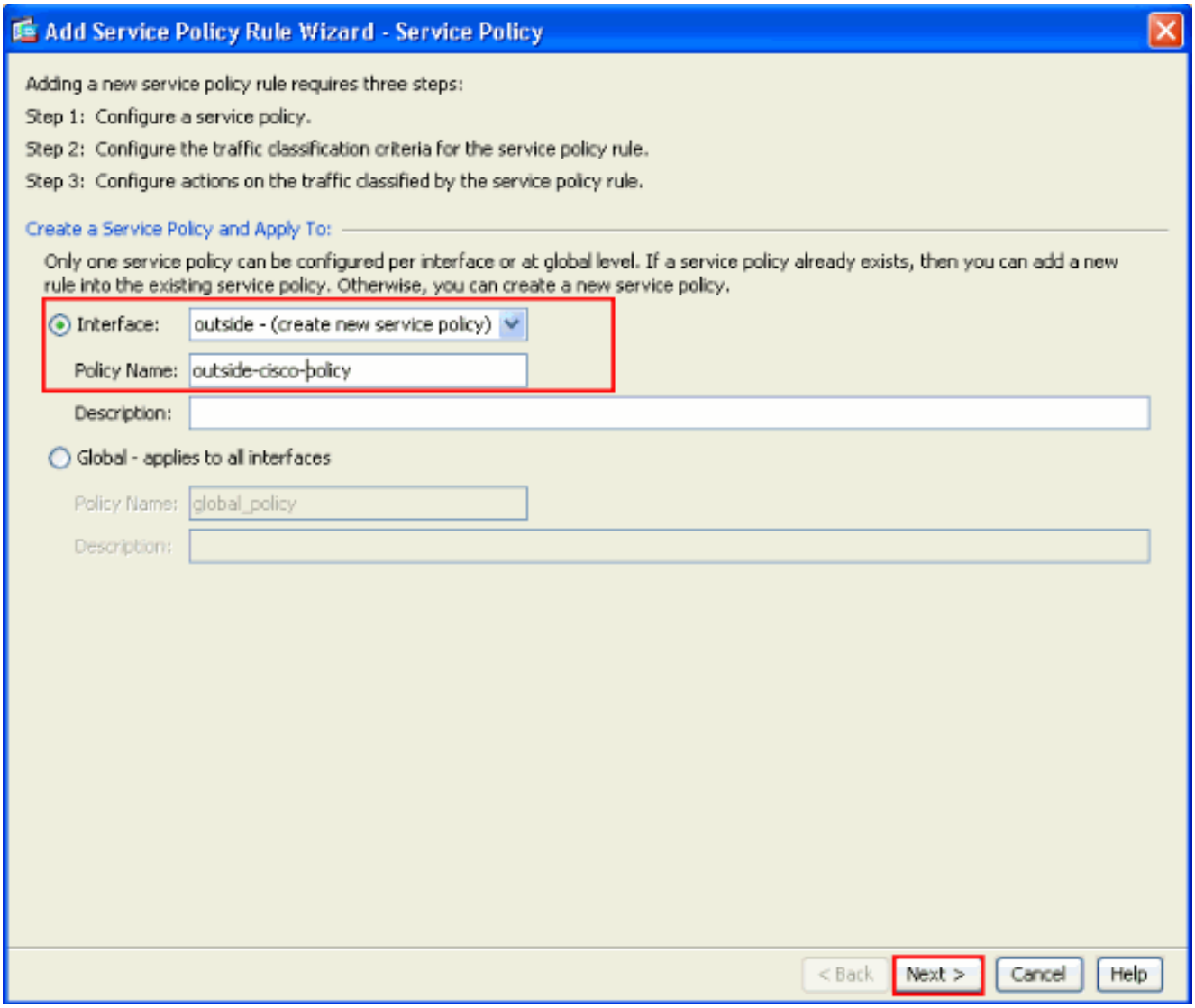
```
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

使用ASDM，执行这些步骤为了配置上述示例：

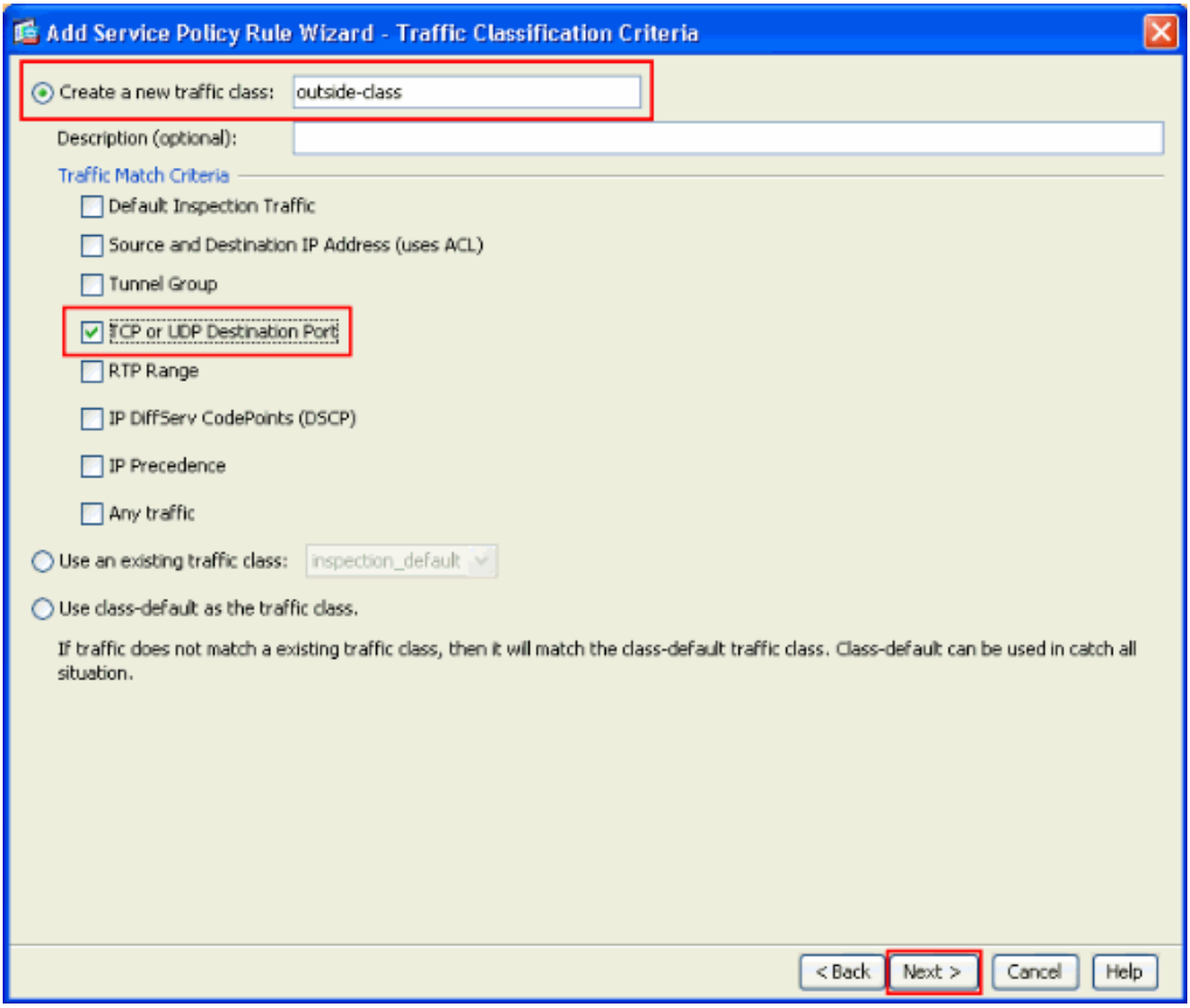
1. 选择**Configuration>防火墙>服务策略规则**并且单击**添加**为了添加一个新的服务策略：



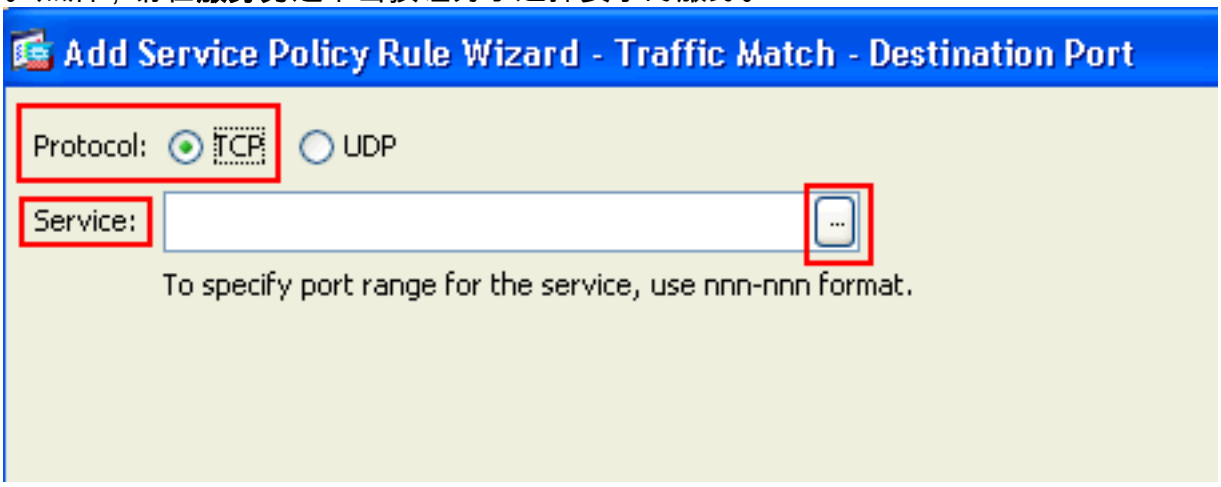
2. 从添加服务策略规则向导-服务策略窗口，在**接口旁边**选择单选按钮。这运用策略创建对一个特定接口，是在本例中的**外部接口**。提供一策略名称，是在本例中的外部思科**策略**。单击**Next**。



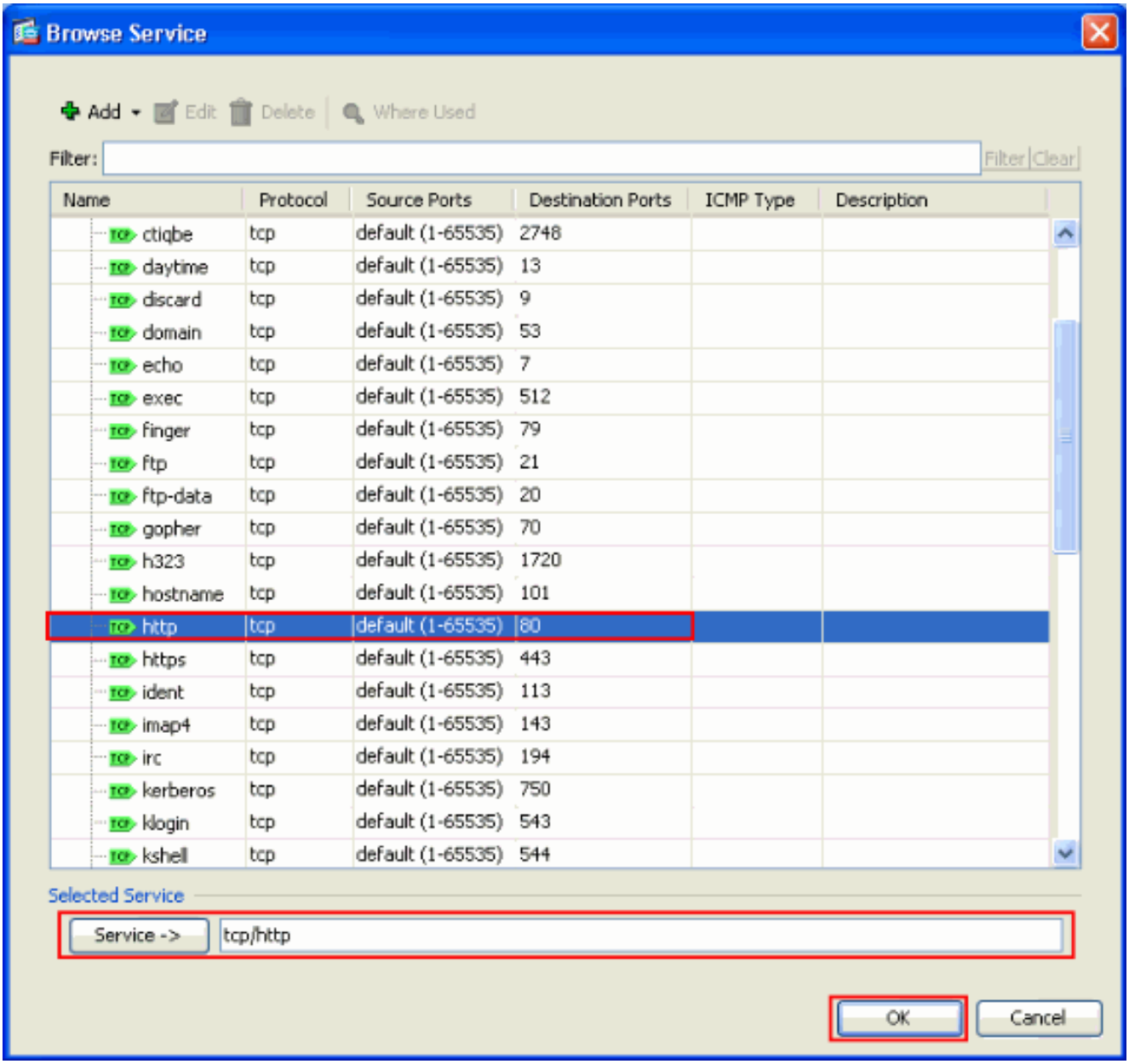
3. 从添加服务策略规则向导-数据流分类标准窗口，提供新数据流类名称。用于此示例的名称是外部**中集集团**。保证在**TCP或UDP目的端口旁边的**复选框被检查并且**其次**单击。



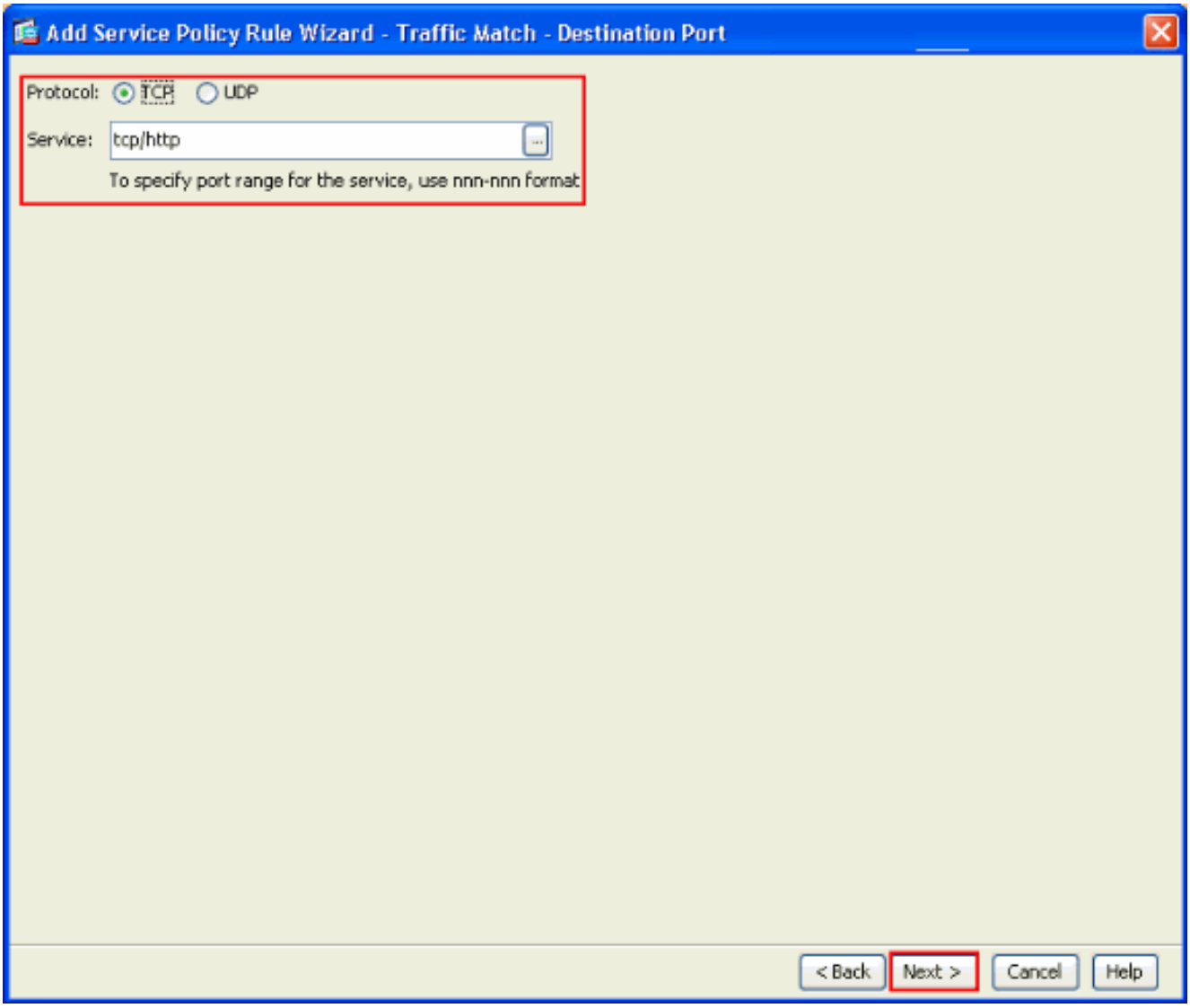
4. 从添加服务策略规则向导-流量匹配-目的地端口窗口，在**TCP旁边**选择单选按钮在**协议部分**下。然后，请在**服务旁边**单击按钮为了选择要求的服务。



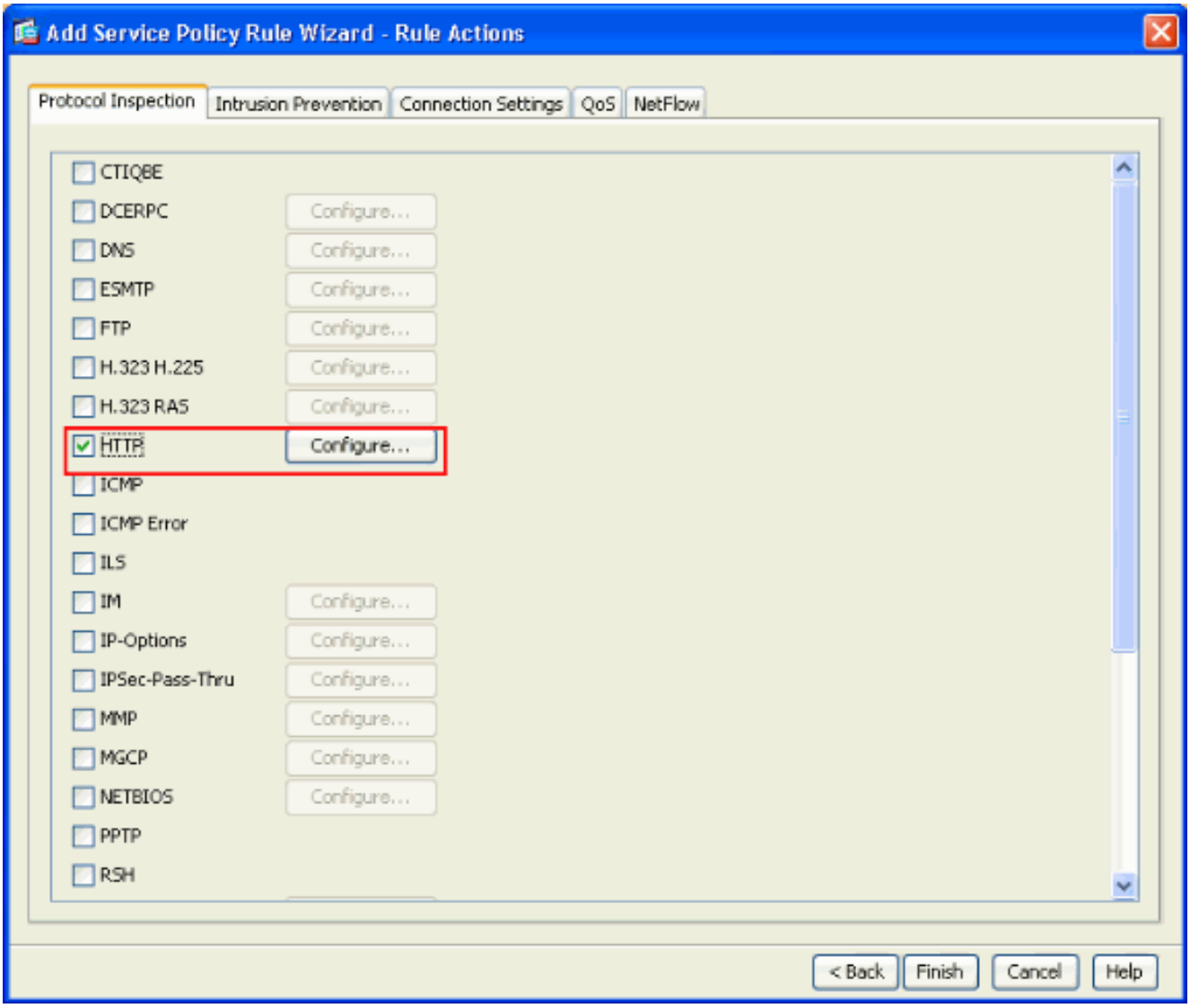
5. 从浏览Service窗口，请选择**HTTP**作为服务。然后，单击**OK**。



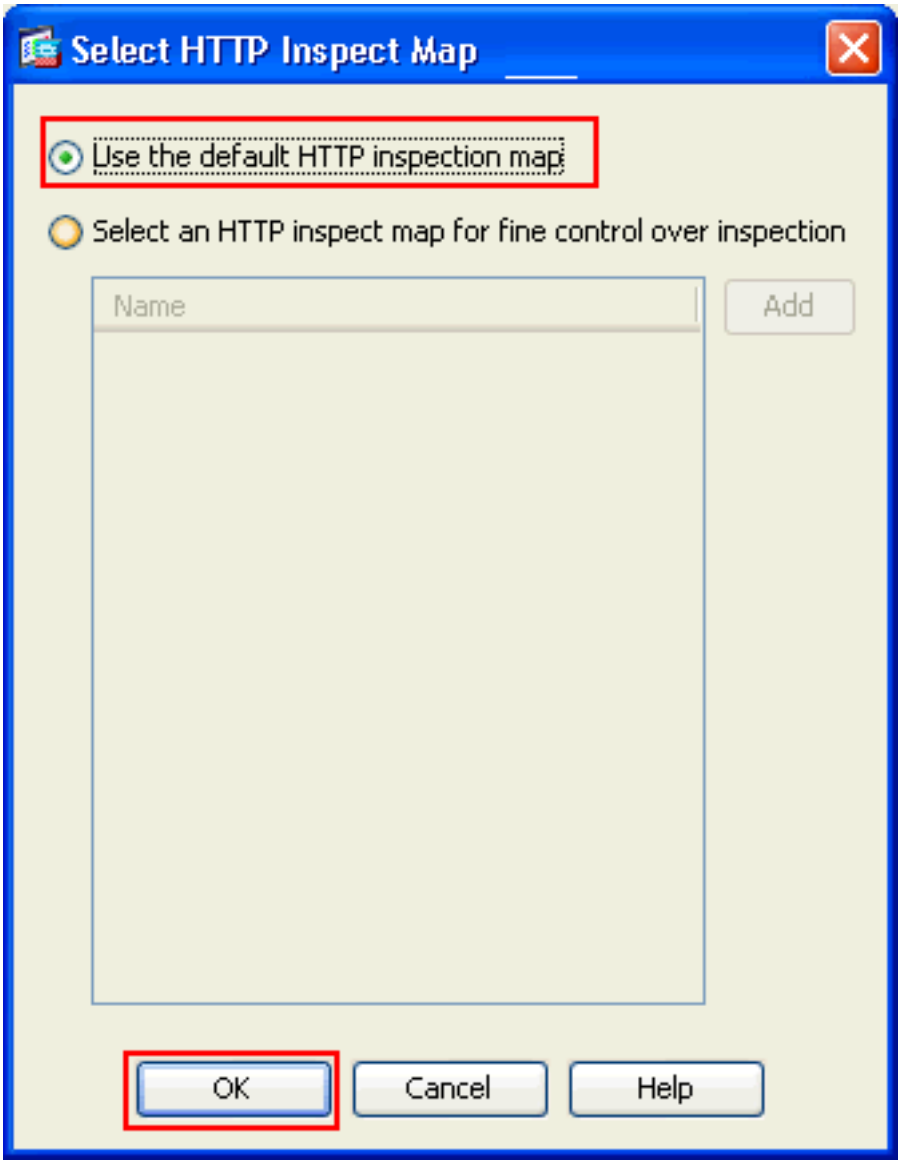
6. 从添加服务策略规则向导-流量匹配-目的地端口窗口，您能看到选择的**服务**是tcp/http。单击**Next**。



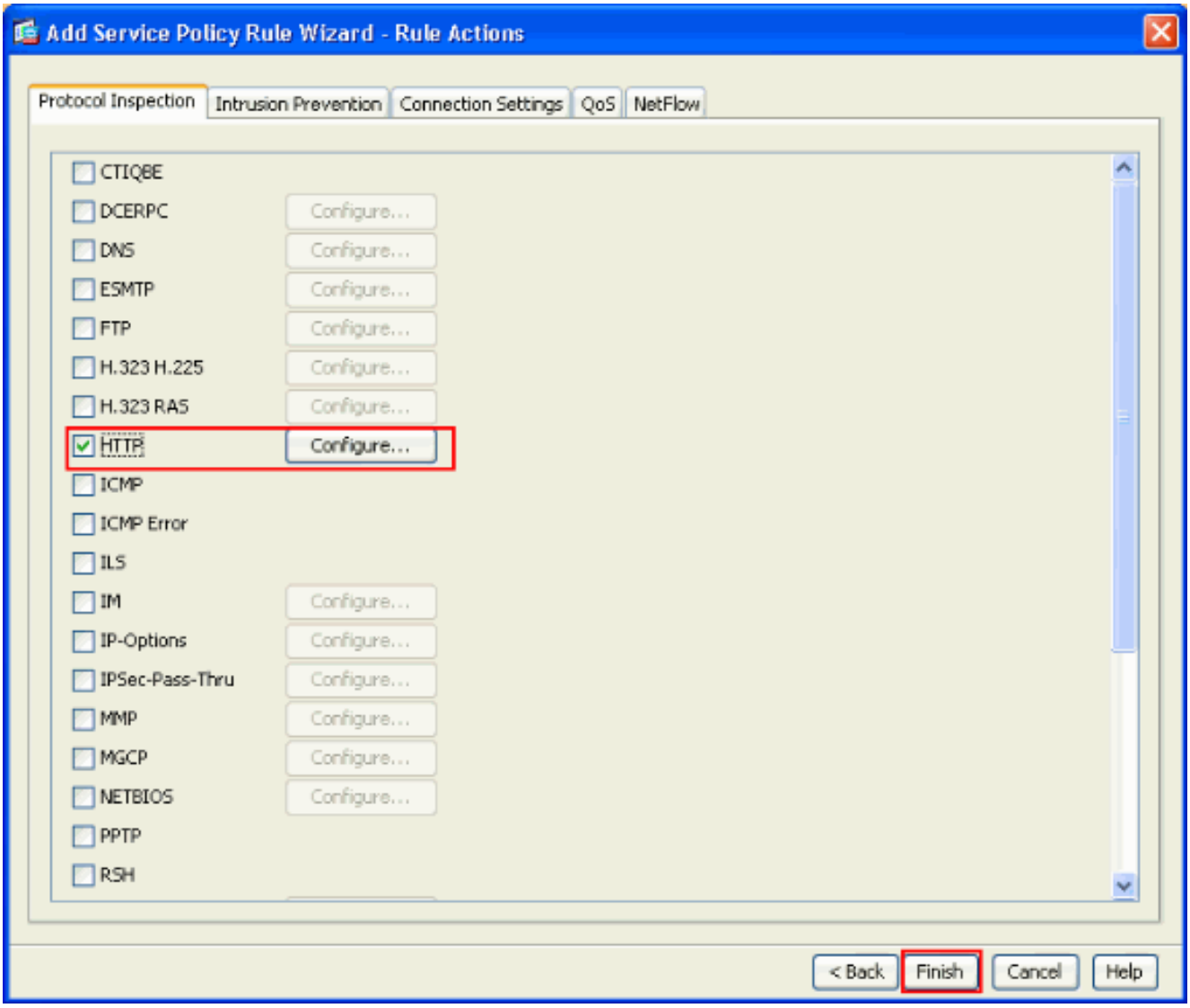
7. 从添加服务策略规则向导-规定操作窗口，在**HTTP旁边**检查复选框。然后，请单击在**HTTP旁边配置**。



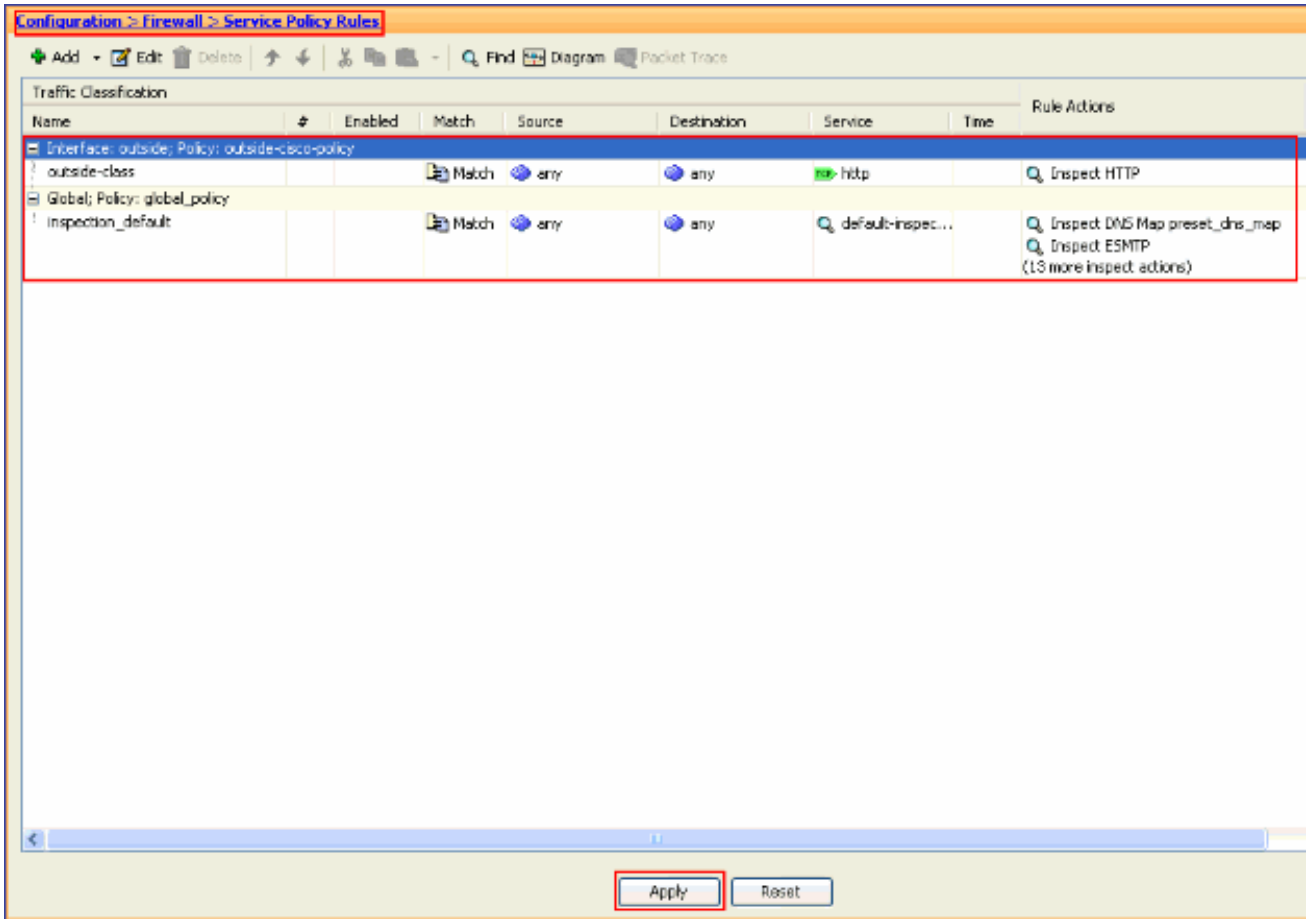
8. 从Map窗口挑选HTTP的Inspect，请在**使用旁边**检查单选按钮**默认HTTP检查地图**。默认HTTP检查用于此示例。然后，单击**OK**。


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. 根据**Configuration>防火墙>服务策略规则**，您与默认服务服务策略一起最近将看到配置的服务策略外部思科**策略**(检查HTTP)已经在设备。单击**应用**为了运用配置到思科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