ASA/PIX 7.X ：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

本文档介绍如何从应用程序的全局策略中删除默认检查，以及如何启用非默认应用程序的检查。

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思科可适应安全工具(ASA)该运行7.x软件镜像。

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。

相关产品

此配置可能也与运行7.x软件镜像的PIX安全工具一起使用。

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。）

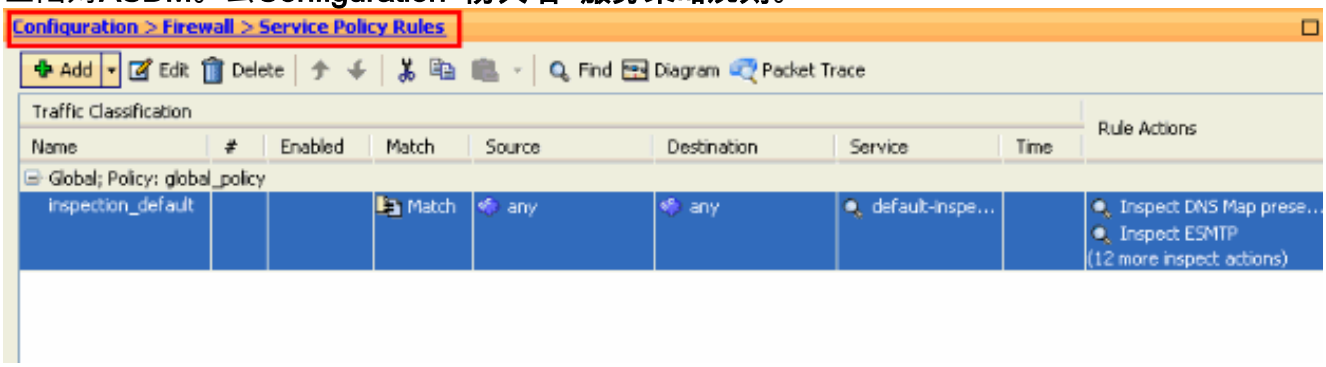
默认策略配置包括以下命令：

```
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
```

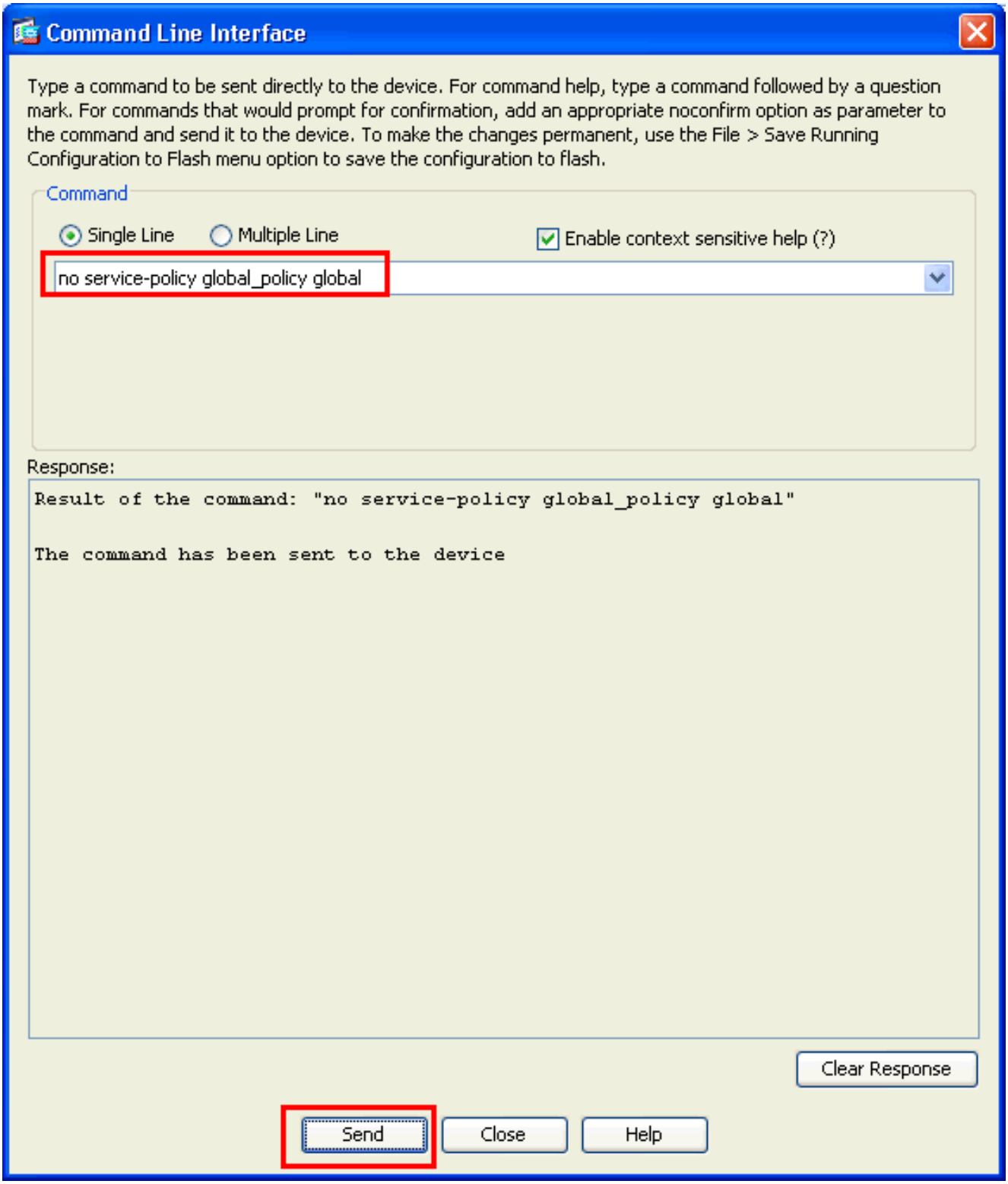
Enable (event)非默认应用检查

完成此步骤启用在思科ASA的非默认应用检查：

1. 登陆对**ASDM**。去**Configuration>防火墙>服务策略规则**。

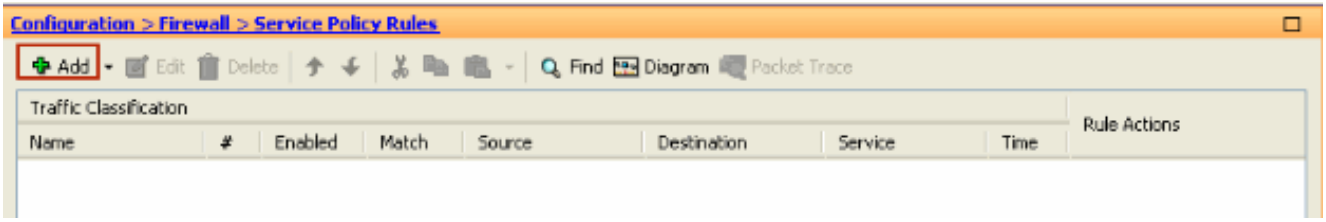


2. 如果要保持包括默认类映射和默认策略映射的全局策略的配置，但是要取消策略全局，请勿去**Tools>命令行界面**并且请使用**服务策略全局策略global命令**取消策略全局。然后，请点击**发送**，因此命令应用对ASA。

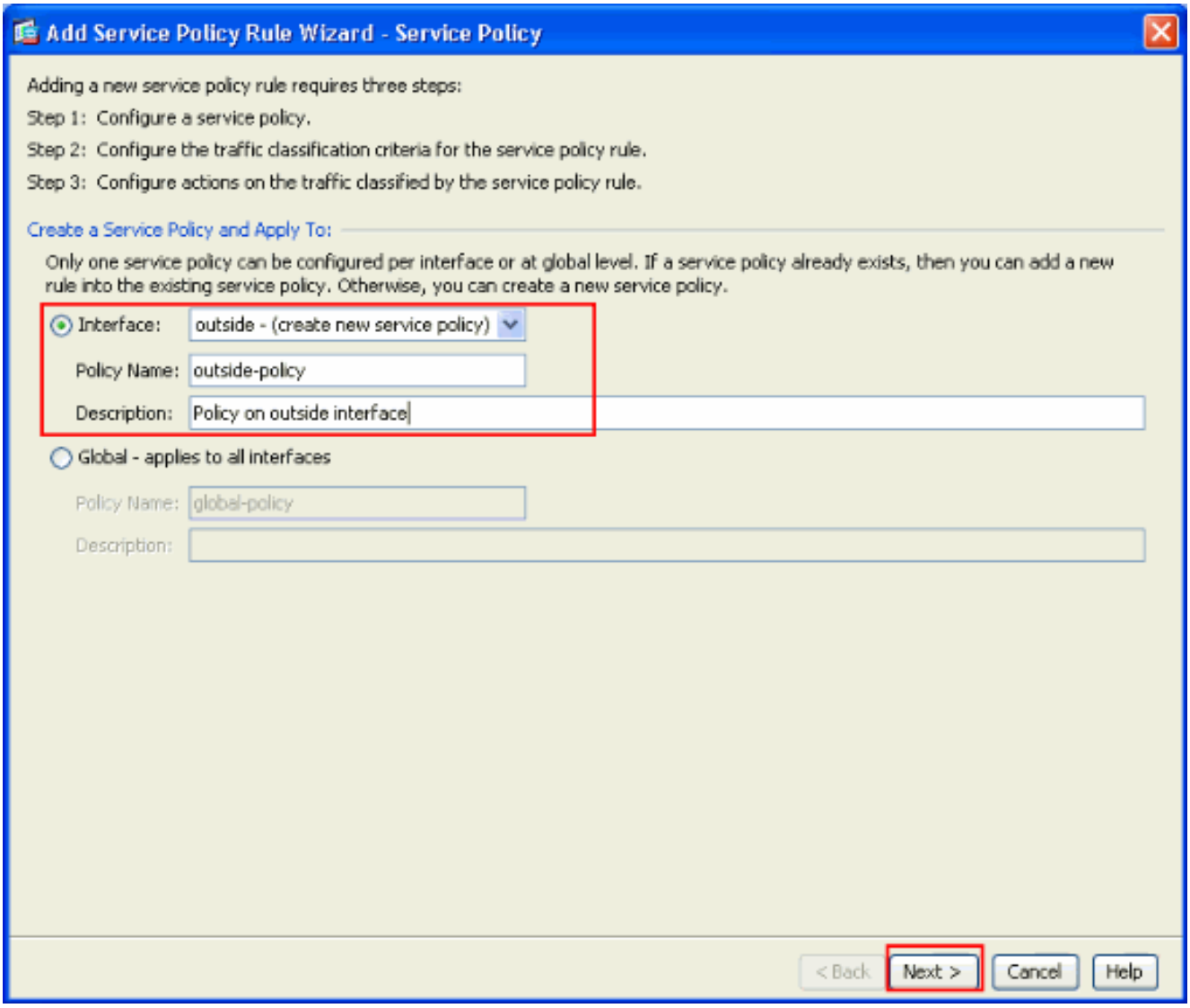


注意： 使用此步骤全局策略在CLI变得隐身在可适应安全设备管理器(ASDM)，但是显示。

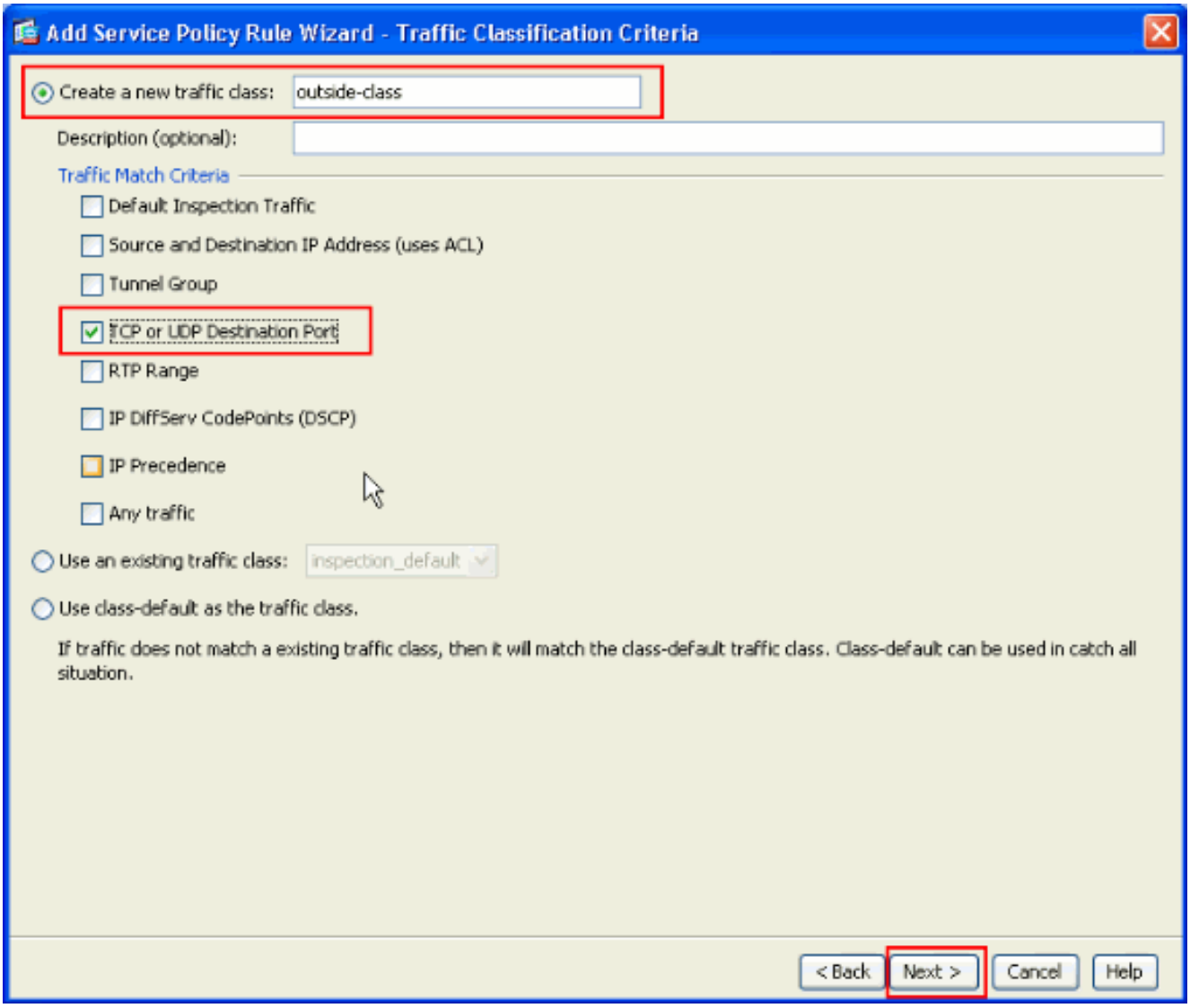
3. 单击**添加**为了添加一项新的策略如显示此处
：



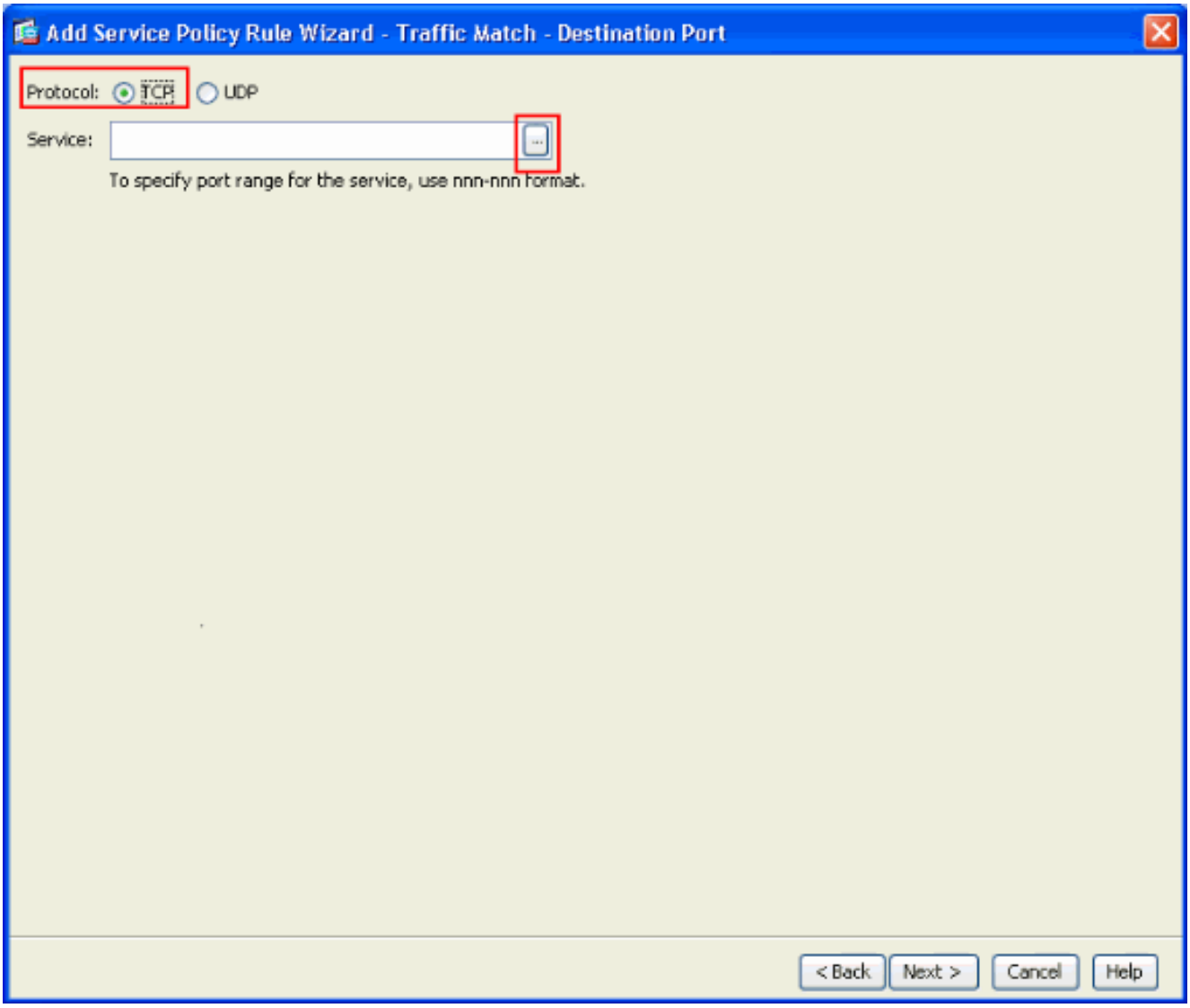
4. 在**接口旁边**确保单选按钮被检查并且选择您要运用从下拉菜单的策略的接口。然后，请提供**策略名称**和**说明**。单击 **Next**。



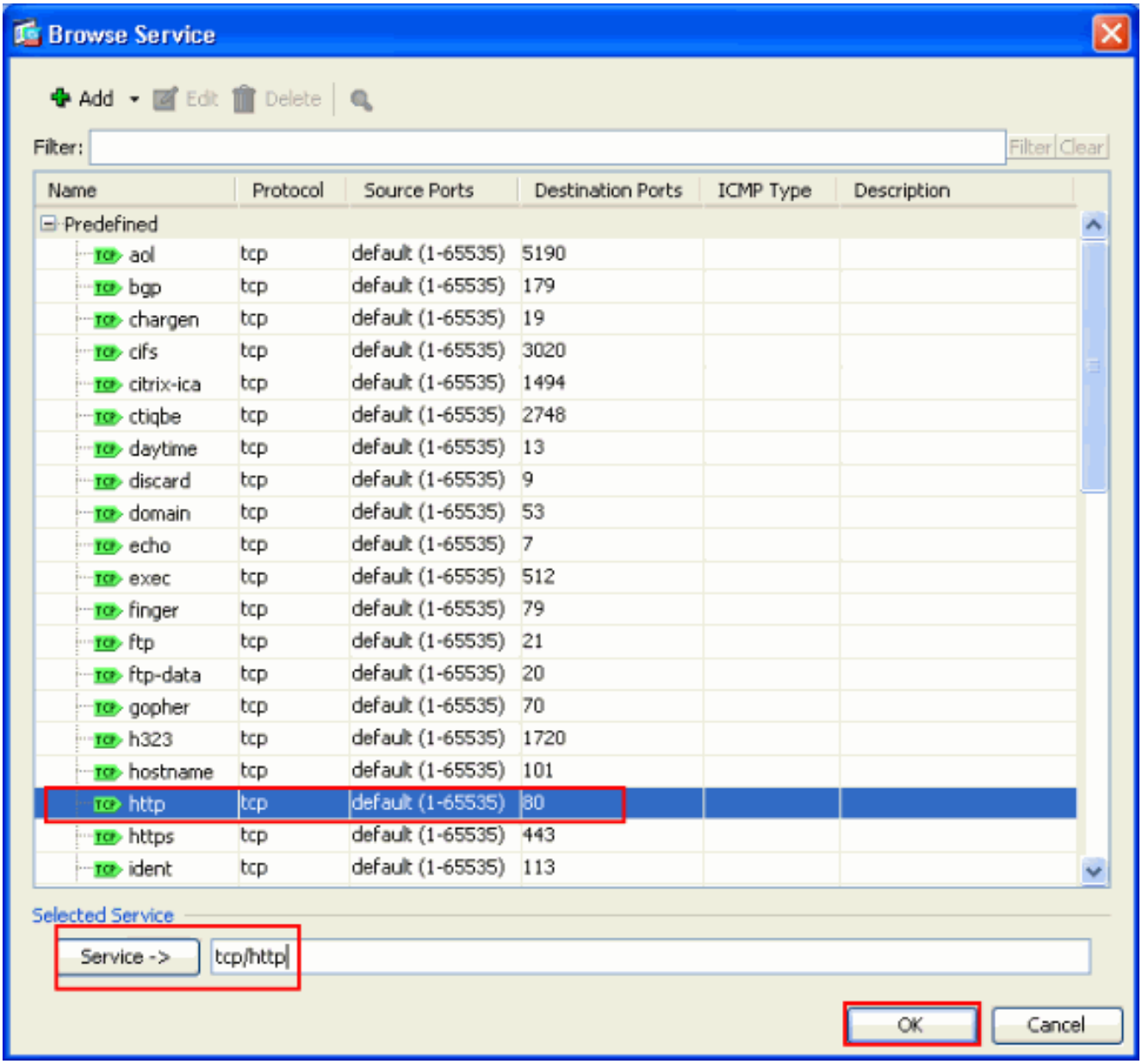
5. 创建新的类映射匹配**TCP数据流， HTTP**属于TCP。单击 **Next**。


Add Service Policy Rule Wizard - Traffic Classification Criteria
Create a new traffic class:
outside-class
Description (optional):
Traffic Match Criteria
Default Inspection Traffic
Source and Destination IP Address (uses ACL)
Tunnel Group
TCP or UDP Destination Port
RTP Range
IP DiffServ CodePoints (DSCP)
IP Precedence
Any traffic
Use an existing traffic class:
inspection_default
Use class-default as the traffic class.
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.
< Back
Next >
Cancel
Help

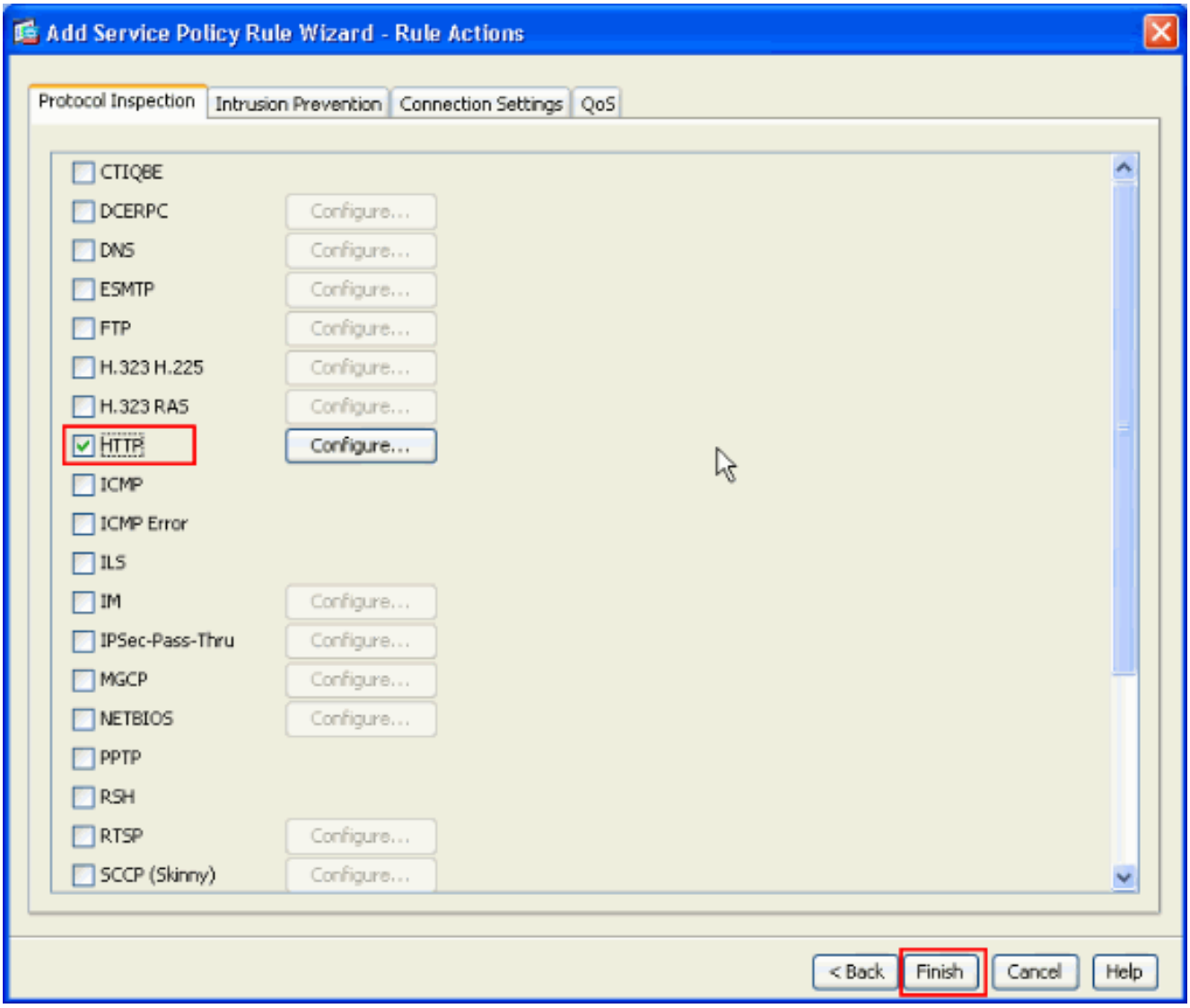
6. 选择TCP作为协议。



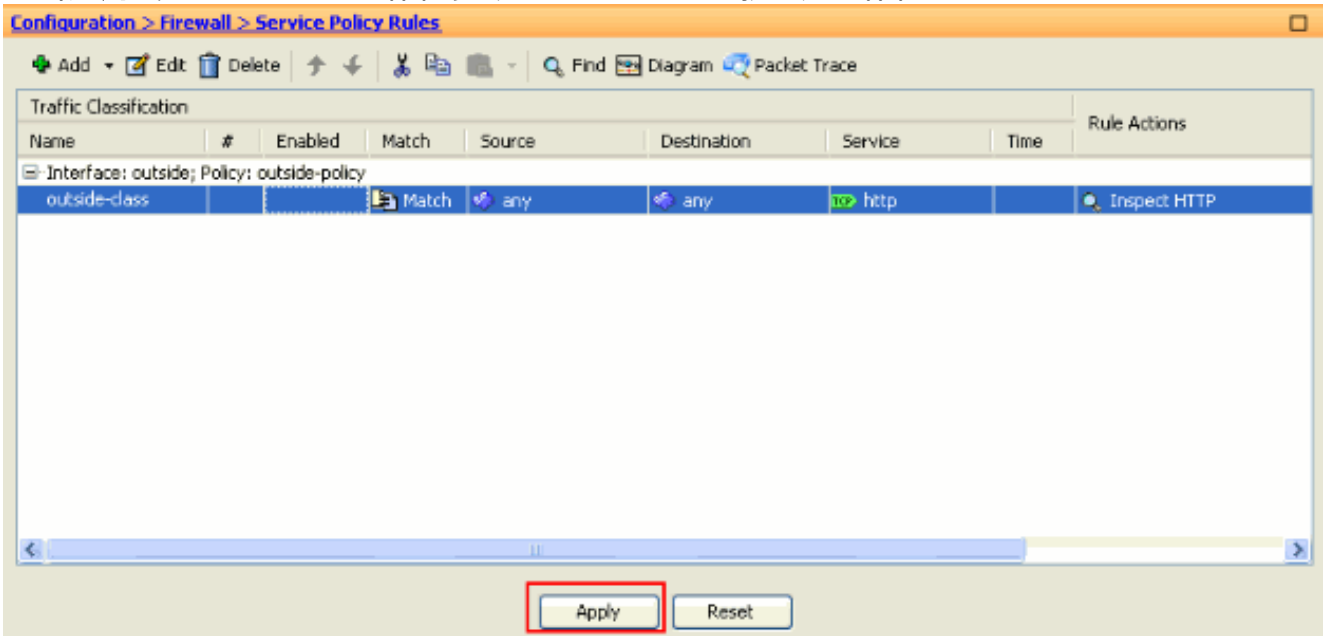
选择**HTTP端口80**作为服务并且点击OK键。



7. 选择**HTTP**并且点击**芬通社**。



8. 单击**应用**发送对ASA的这些配置更改从ASDM。这样就完成了配置。



验证

请使用这些**显示**命令验证配置：

- 请使用**class-map命令的show run**查看配置的类映射。`ciscoasa# sh run class-map`
```
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class match port tcp eq www !
```
- 请使用**policy-map命令的show run**查看配置的策略映射。`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 !
```
- 请使用**service-policy命令的show run**查看配置的服务策略。`ciscoasa# sh run service-policy`
```
service-policy outside-policy interface outside
```

相关信息

- Cisco ASA 5500 系列自适应安全设备
- Cisco ASA 5500系列命令参考
- Cisco Adaptive Security Device Manager (ASDM)支持页面
- Cisco PIX 防火墙软件
- 请求注解 (RFC)
- Cisco PIX 500 系列安全设备
- 应用应用层协议检查
- Cisco Secure PIX 防火墙命令参考
- 技术支持和文档 - Cisco Systems