ASA/PIX 7.X:禁用預設全域性檢查並使用ASDM啟用非預設應用程式檢查

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[相關產品](#)
[慣例](#)
[預設全域性策略](#)
[啟用非預設應用檢測](#)
[驗證](#)
[相關資訊](#)

簡介

本文檔介紹如何從應用程式的全域性策略中刪除預設檢測，以及如何為非預設應用程式啟用檢測。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據執行7.x軟體映像的思科調適型安全裝置(ASA)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可以與運行7.x軟體映像的PIX安全裝置一起使用。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

預設全域性策略

預設情況下，配置包含與所有預設應用檢測流量匹配並將某些檢測應用於所有介面上的流量的策略（全域性策略）。 並非所有檢查都預設啟用。只能應用一個全域性策略。如果要修改全域性策略，必須編輯或禁用預設策略並應用新策略。（介面策略覆蓋全域性策略。）

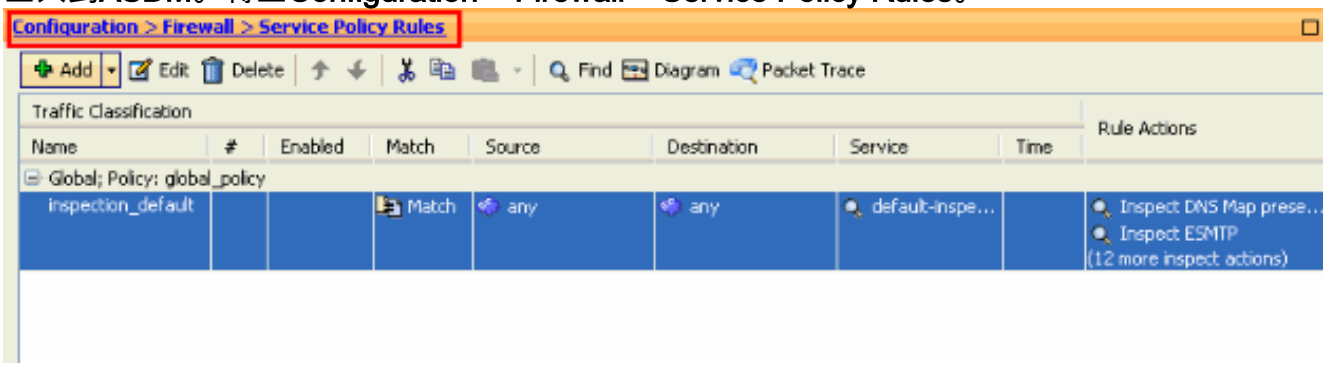
預設策略配置包括以下命令：

```
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
```

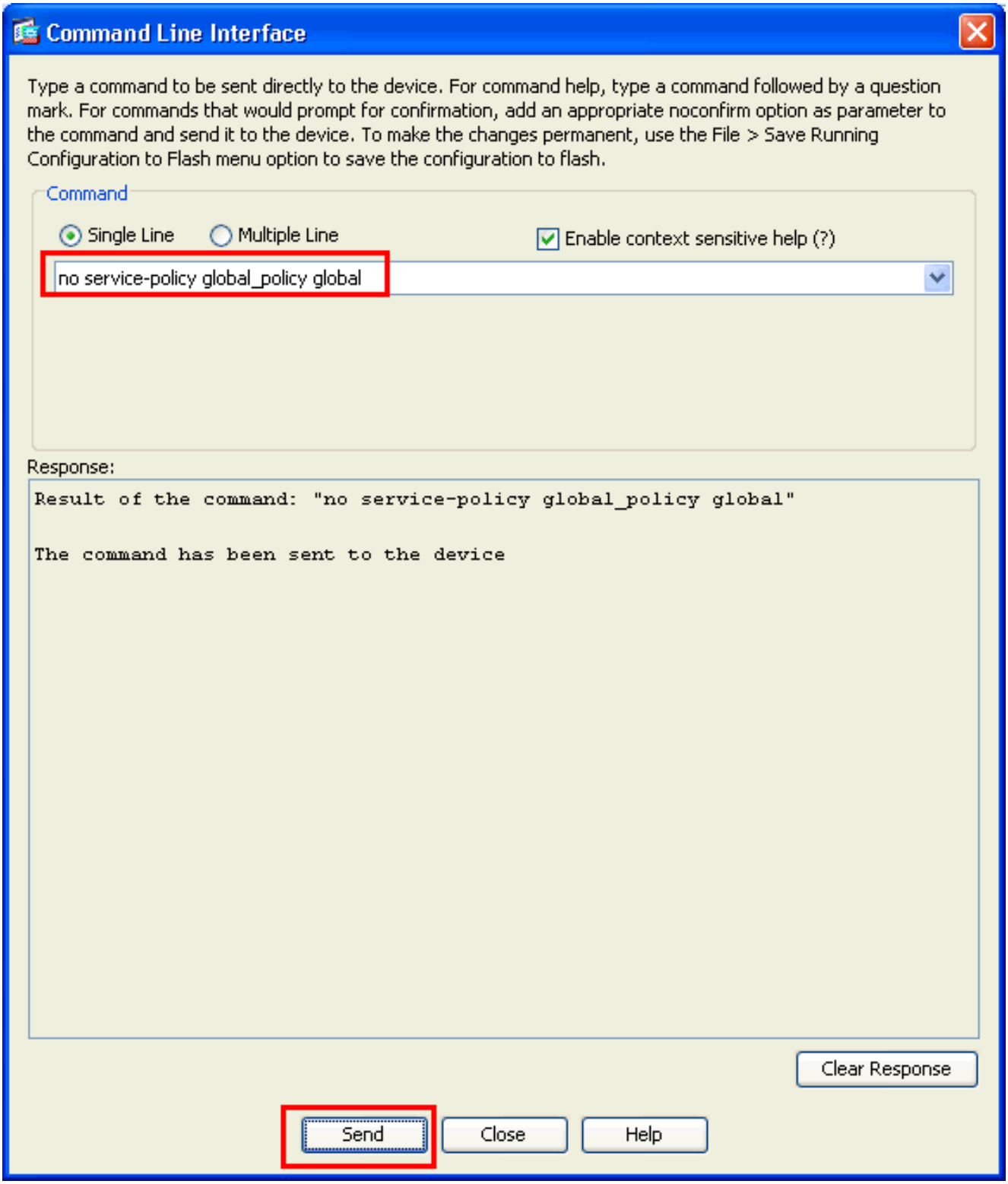
啟用非預設應用檢測

完成以下步驟即可在Cisco ASA上啟用非預設應用檢測：

1. 登入到ASDM。轉至Configuration > Firewall > Service Policy Rules。

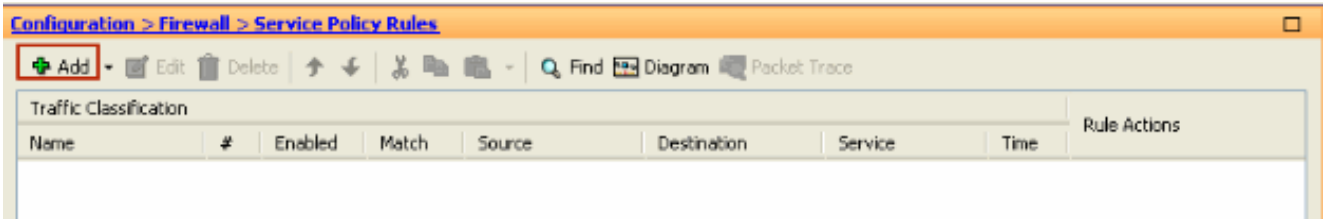


2. 如果要保留包括預設類對映和預設策略對映的全域性策略配置，但希望全域性刪除該策略，請轉到Tools > Command Line Interface，並使用no service-policy global-policy global命令全域性刪除該策略。然後，按一下Send，將命令應用到ASA。

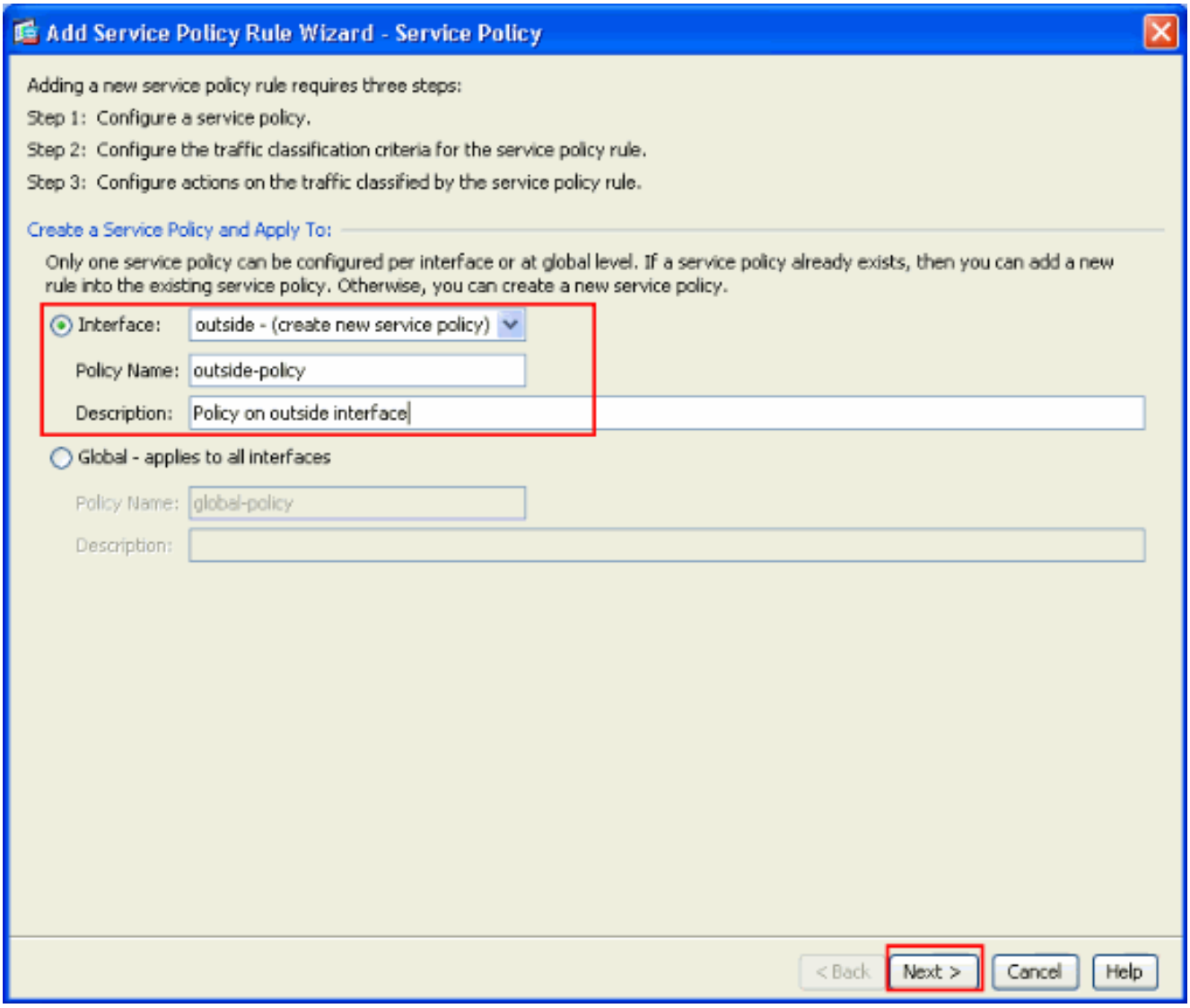


注意：通過此步驟，全域性策略在自適應安全裝置管理器(ASDM)中變得不可見，但在CLI中顯示。

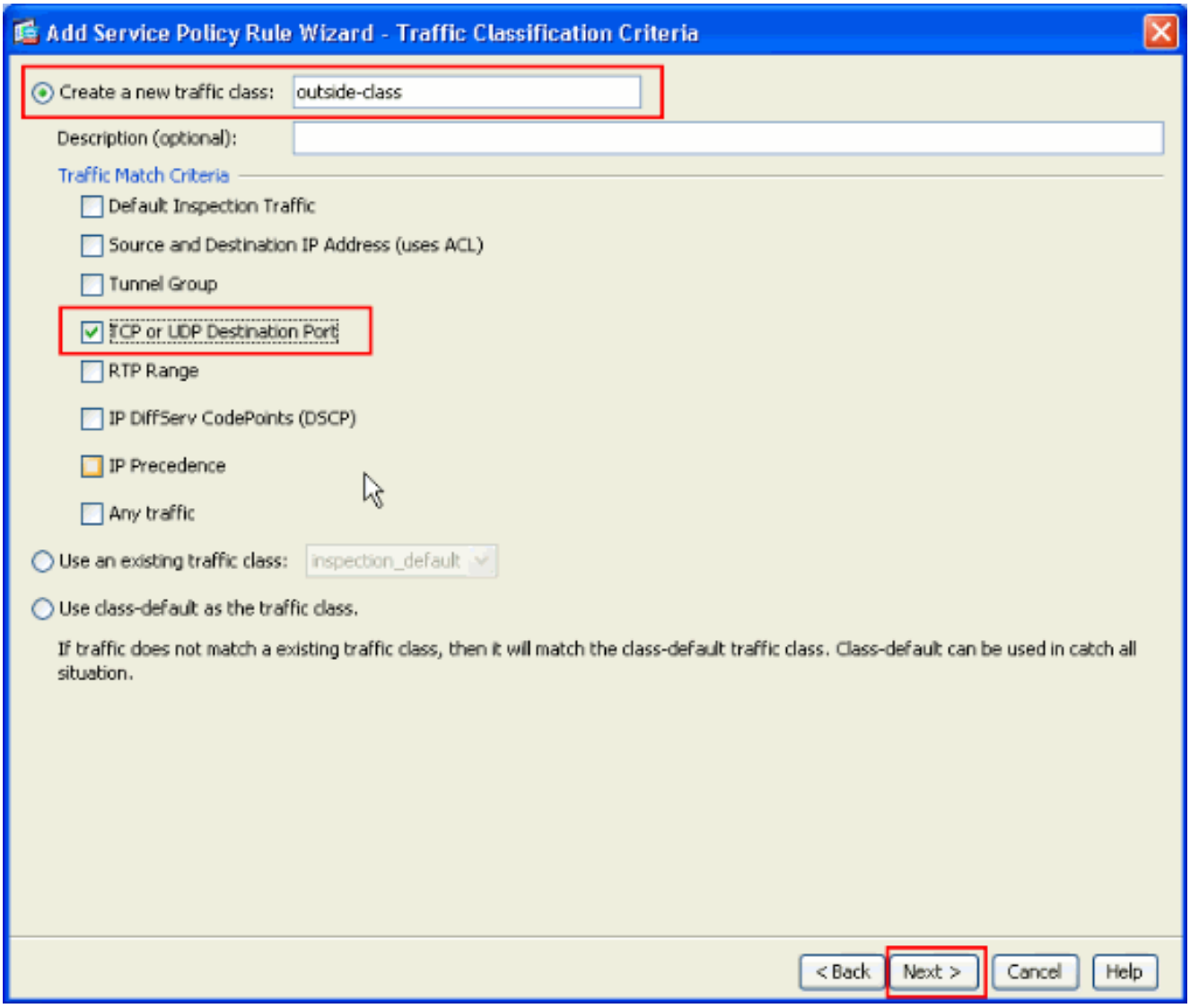
3. 按一下**Add**以新增新策略，如下所示：



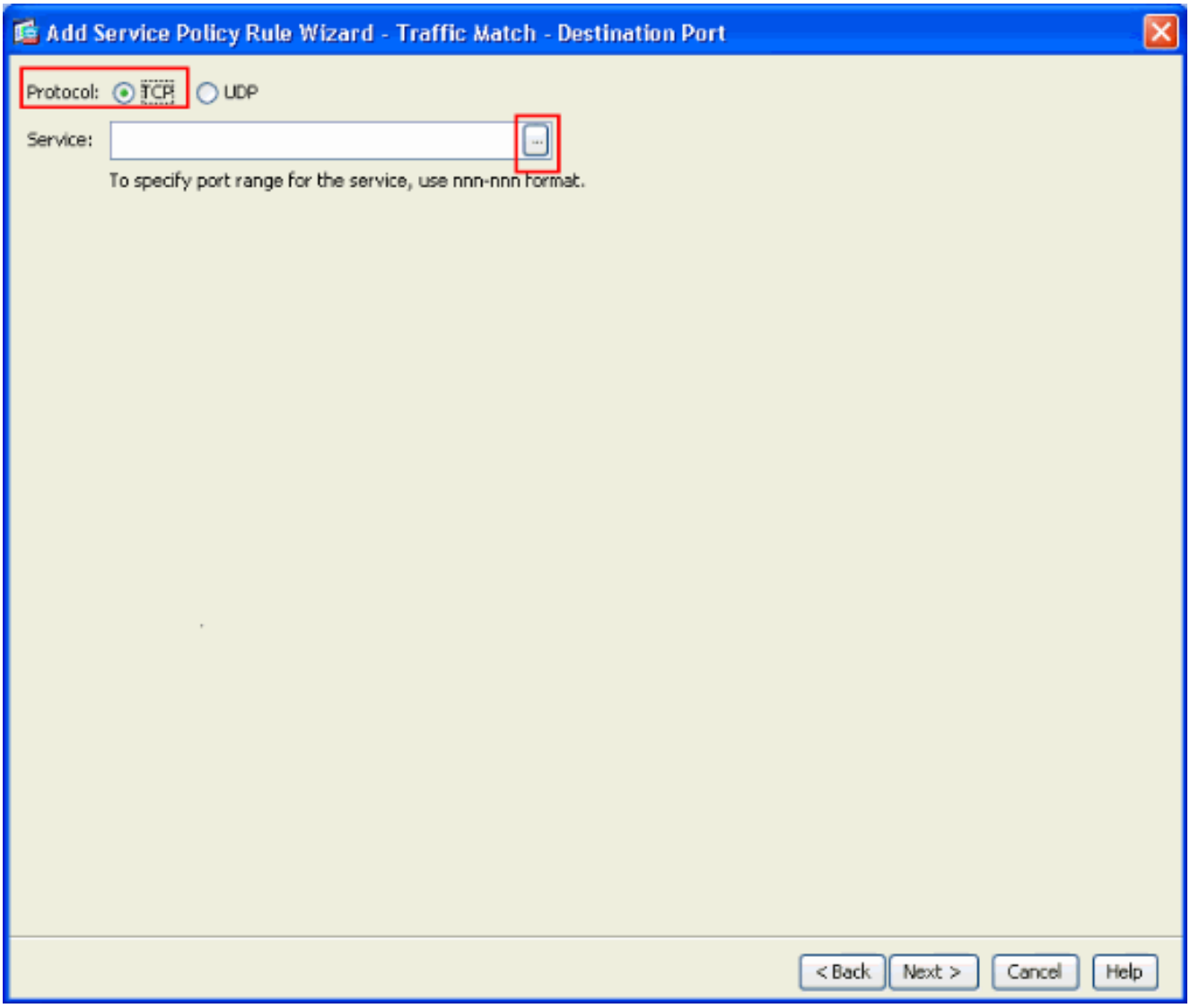
4. 確保選中**Interface**旁邊的單選按鈕，然後從下拉選單中選擇要應用策略的介面。然後，提供**策略名稱**和**說明**。按「**Next**」（下一步）。



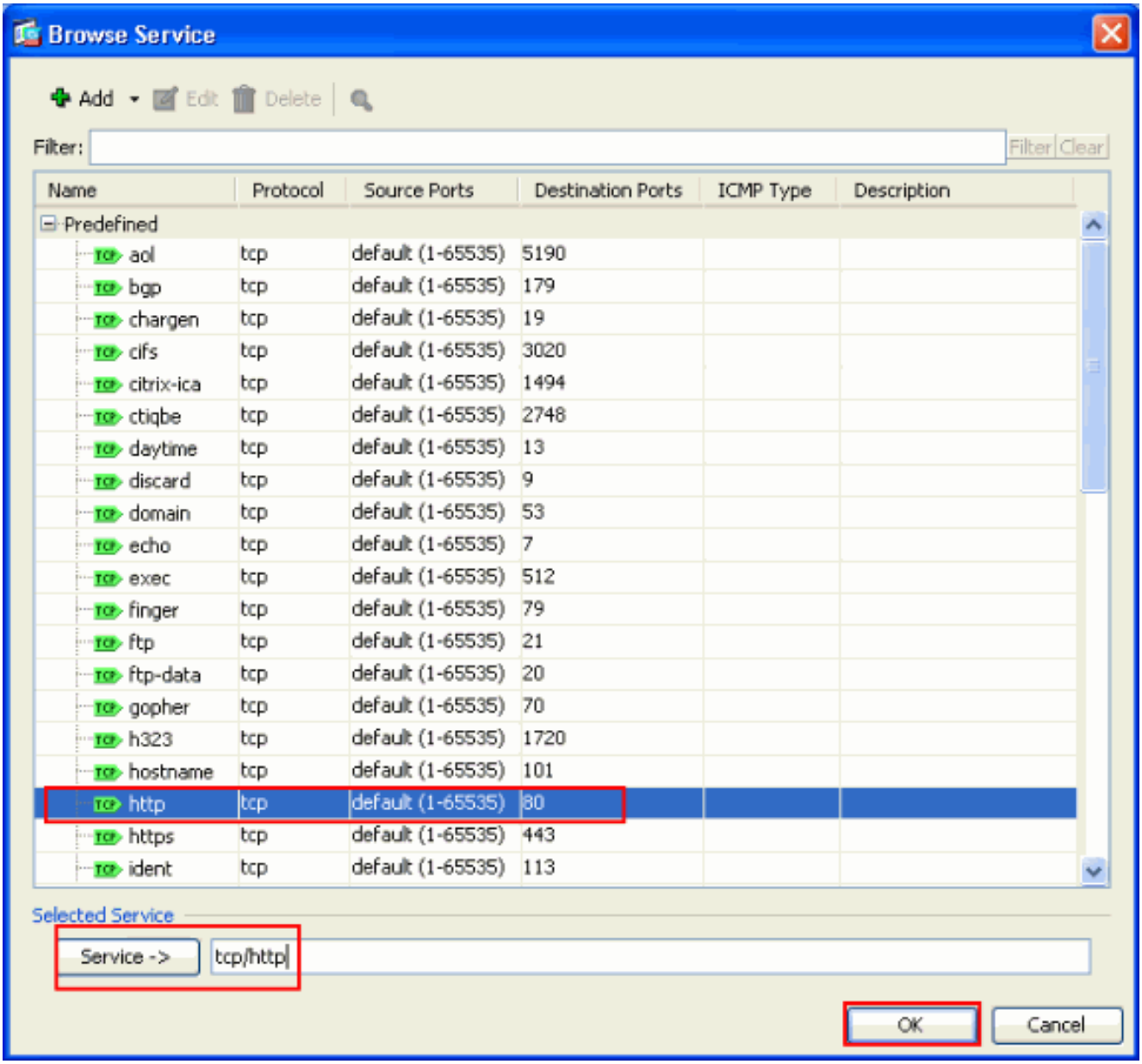
5. 建立一個新的類對映以匹配**TCP流量**，因為**HTTP**屬於TCP。按「**Next**」（下一步）。


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

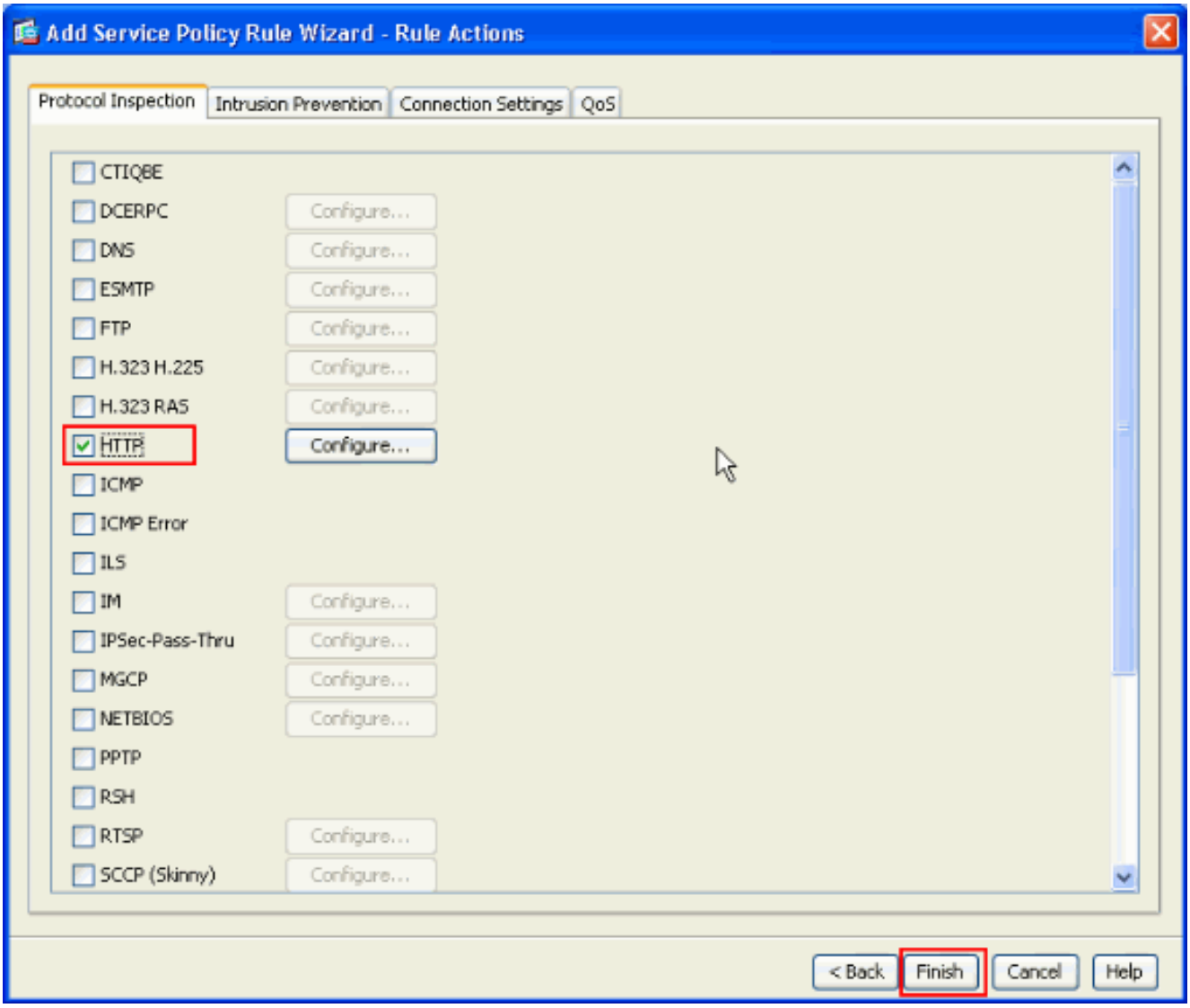
6. 選擇TCP作為協定。



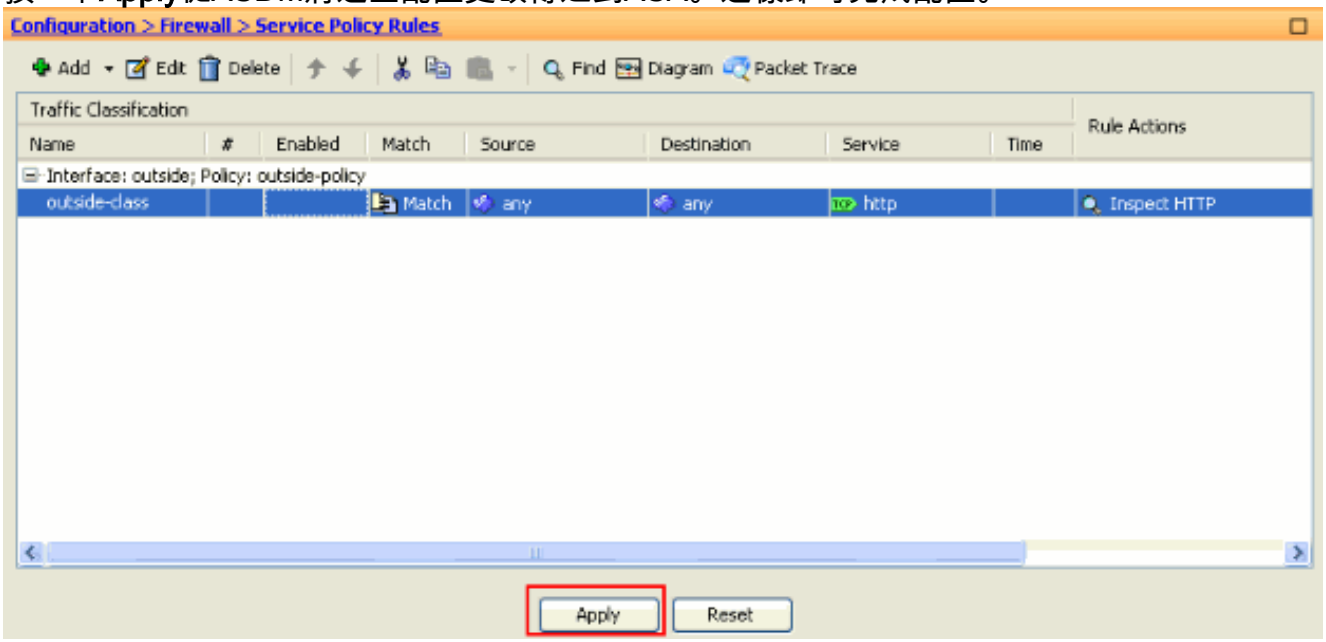
選擇**HTTP port 80**作為Service（服務），然後按一下**OK**。



7. 選擇**HTTP**，然後按一下**Finish**。



8. 按一下**Apply**從ASDM將這些配置更改傳送到ASA。這樣即可完成配置。



驗證

使用以下**show**命令驗證設定：

- 使用**show run class-map**命令檢視已配置的類對映。

```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class
match port tcp eq www
!
```

- 使用**show run policy-map**命令檢視配置的策略對映。

```
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
!
```

- 使用**show run service-policy**命令檢視配置的服務策略。

```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- Cisco ASA 5500系列命令參考
- 思科調適型安全裝置管理員(ASDM)支援頁面
- Cisco PIX防火牆軟體
- 要求建議 (RFC)
- Cisco PIX 500系列安全裝置
- 應用應用層協定檢查
- Cisco Secure PIX防火牆命令參考
- 技術支援與文件 - Cisco Systems