ASA 8.3及更高版本 — 使用ASDM配置檢測

目錄

簡介

本文檔為版本8.3(1)及更高版本的思科自適應安全裝置(ASA)提供配置示例，說明如何從應用程式的全域性策略中刪除預設檢測，以及如何使用自適應安全裝置管理器(ASDM)為非預設應用程式啟用檢測。

請參閱PIX/ASA 7.X:在版本8.2及更低版本的Cisco ASA上，對相同配置禁用預設全域性檢查並啟用非預設應用檢查。

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搭載ASDM 6.3的Cisco ASA安全裝置軟體版本8.3(1)。

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。

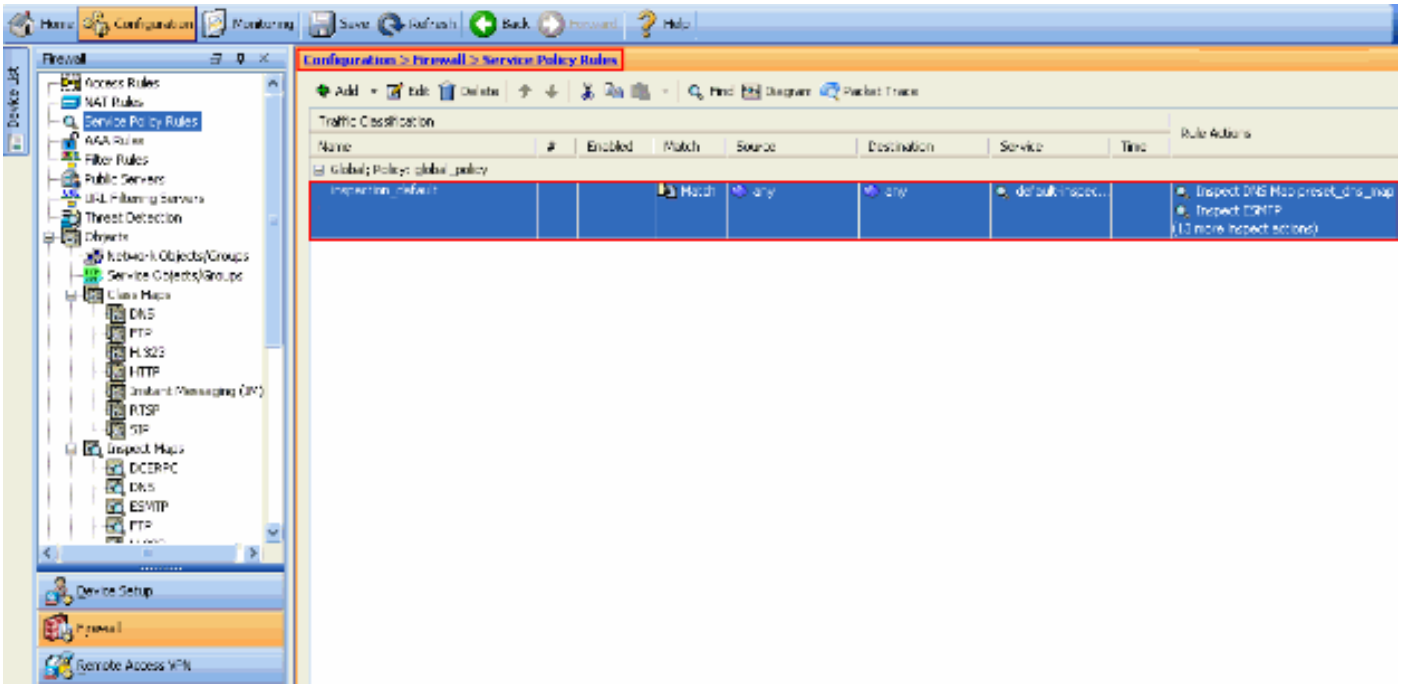
慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

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。）

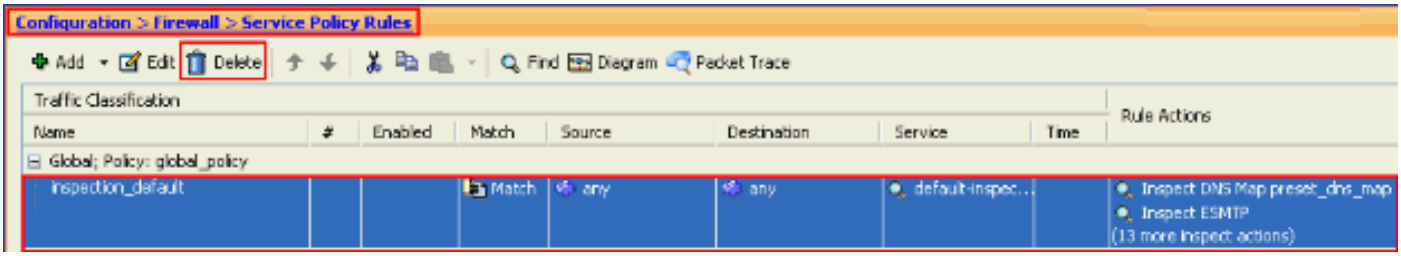
在ASDM中，選擇**Configuration > Firewall > Service Policy Rules**以檢視具有預設應用程式檢查的預設全域性策略，如下所示：



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
```

如果需要禁用全域性策略，請使用**no service-policy global_policy global**命令。若要使用ASDM刪除全域性策略，請選擇**Configuration > Firewall > Service Policy Rules**。然後，選擇全域性策略並按一下**Delete**。



注意：使用ASDM刪除服務策略時，將刪除關聯的策略和類對映。但是，如果使用CLI刪除服務策略，則只會從介面中刪除服務策略。類對映和策略對映保持不變。

禁用應用程式的預設全域性檢查

要禁用應用程式的全域性檢查，請使用**inspect**命令的*no版本*。

例如，要刪除對安全裝置偵聽的FTP應用程式的全域性檢查，請在類配置模式下使用**no inspect ftp**命令。

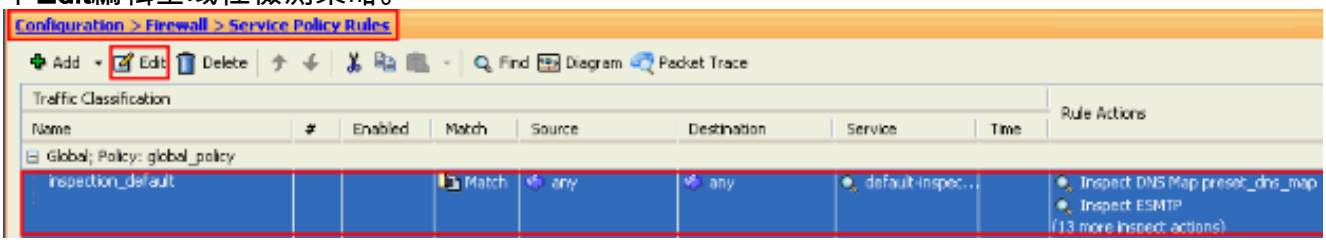
可從策略對映配置模式訪問類配置模式。若要移除組態，請使用命令的*no*形式。

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

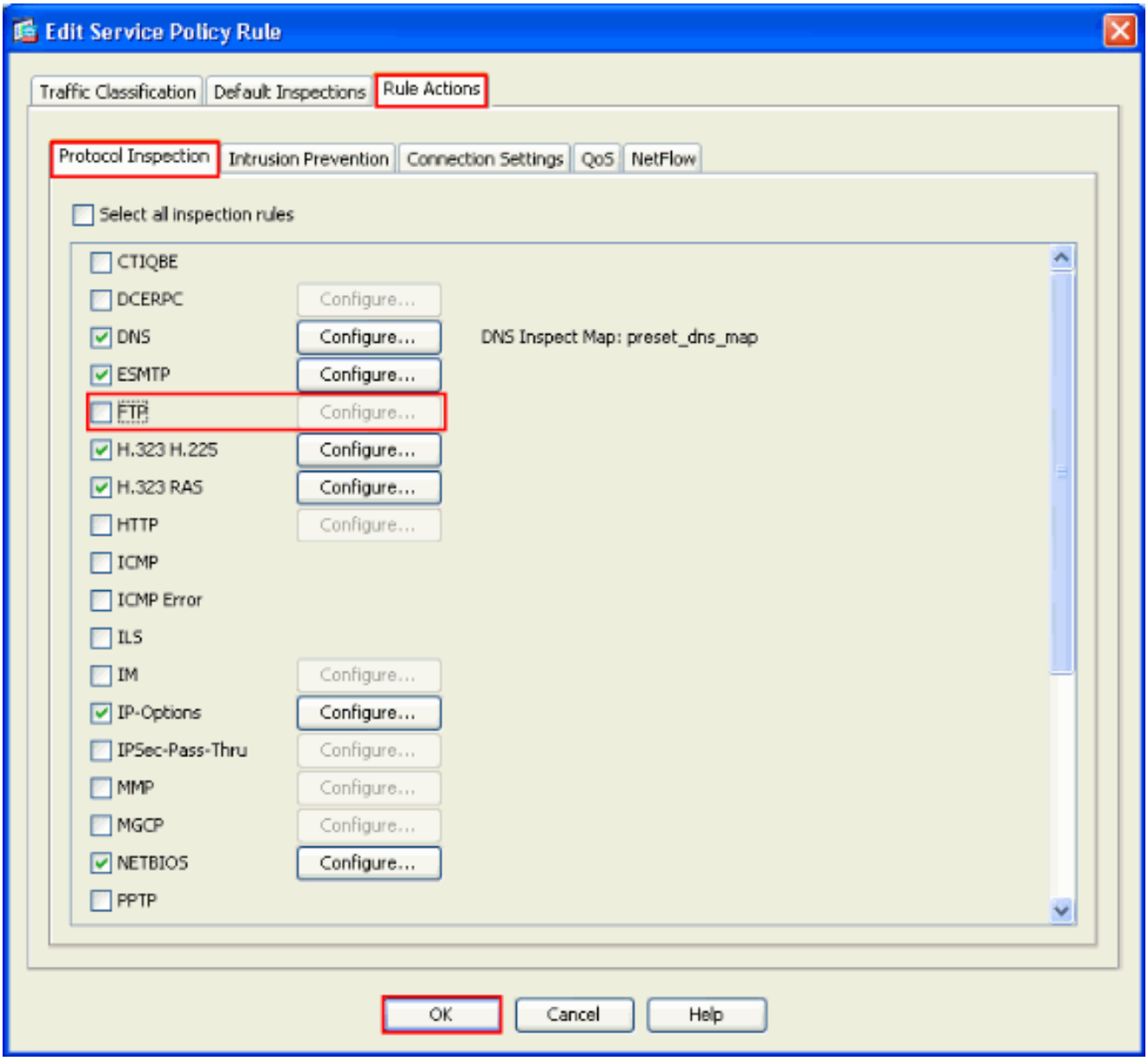
要使用ASDM禁用FTP全域性檢查，請完成以下步驟：

注意：請參閱允許ASDM的HTTPS訪問以瞭解基本設定，以便通過ASDM訪問PIX/ASA。

1. 選擇**Configuration > Firewall > Service Policy Rules**，然後選擇預設全域性策略。然後，按一下**Edit**編輯全域性檢測策略。



2. 在Edit Service Policy Rule視窗中，選擇**Rule Actions**頁籤下的**Protocol Inspection**。確保未選中**FTP**霰取方塊。這將禁用FTP檢測，如下圖所示。然後，按一下「**OK**」，然後「**Apply**」。



注意：有關FTP檢測的更多資訊，請參閱PIX/ASA 7.x:啟用FTP/TFTP服務配置示例。

為非預設應用程式啟用檢測

預設情況下，增強型HTTP檢測處於禁用狀態。要在global_policy中啟用HTTP檢查，請使用class inspection_default下的**inspect http**命令。

在本示例中，通過任何介面進入安全裝置的任何HTTP連線（埠80上的TCP流量）都屬於HTTP檢查類別。*由於策略是全域性策略，因此只有在流量進入每個介面時才進行檢查。*

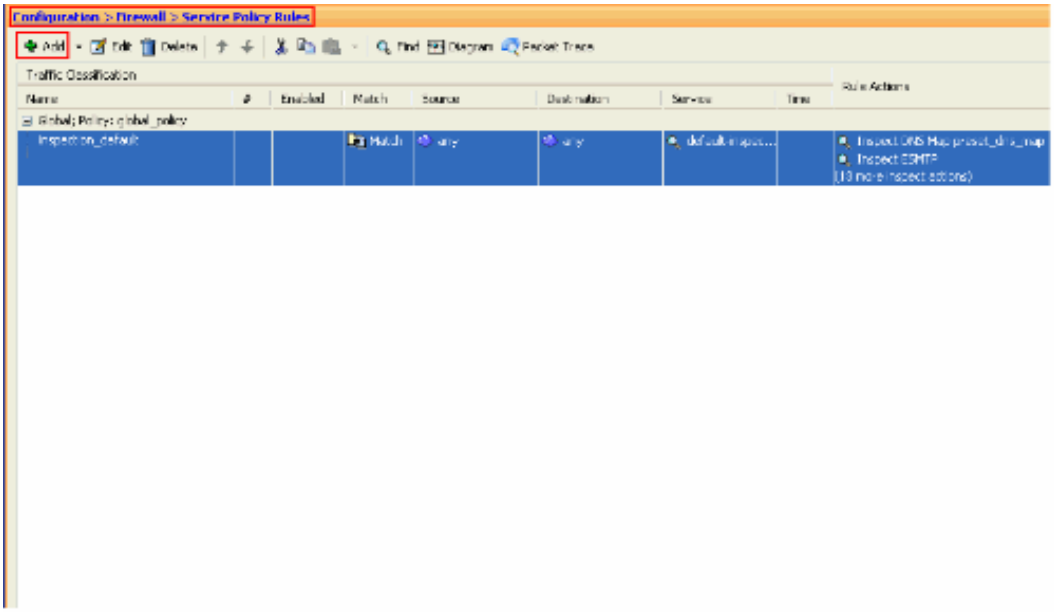
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

在本例中，通過外部介面進入或退出安全裝置的任何HTTP連線(埠80上的TCP流*量)都分類為HTTP檢測*。

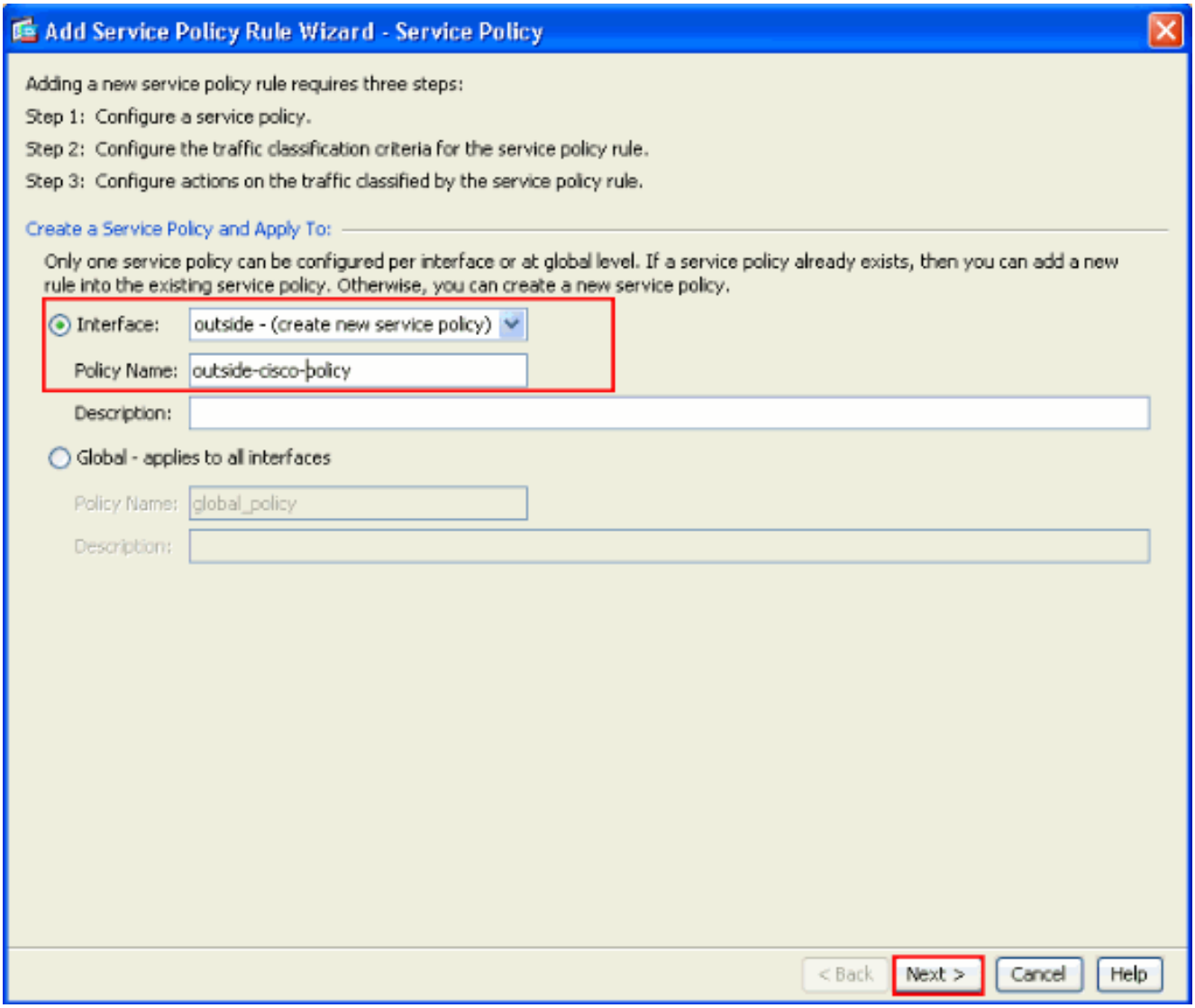
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

要使用ASDM配置上述示例，請執行以下步驟：

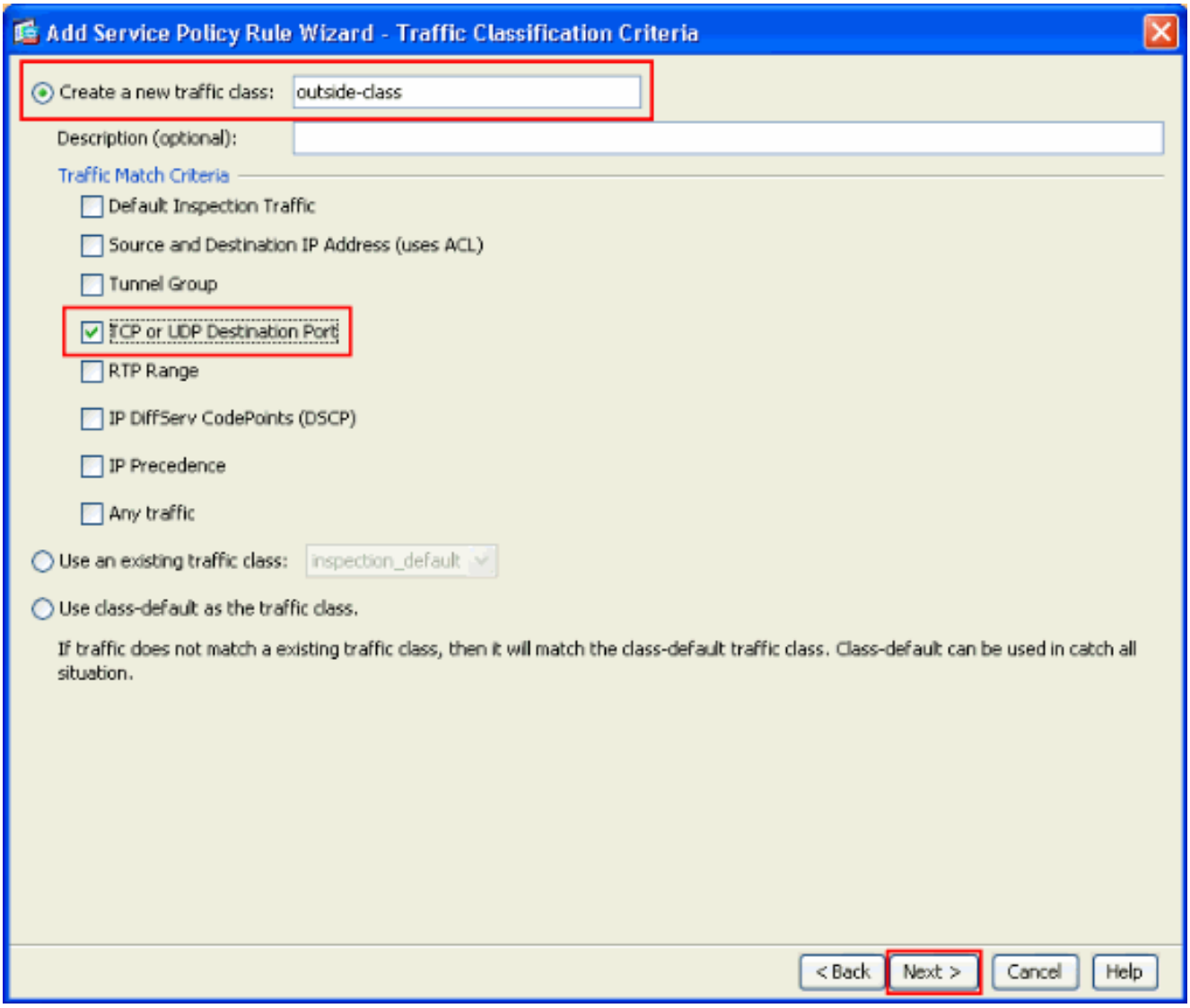
1. 選擇**Configuration > Firewall > Service Policy Rules**，然後按一下**Add**以新增新服務策略：



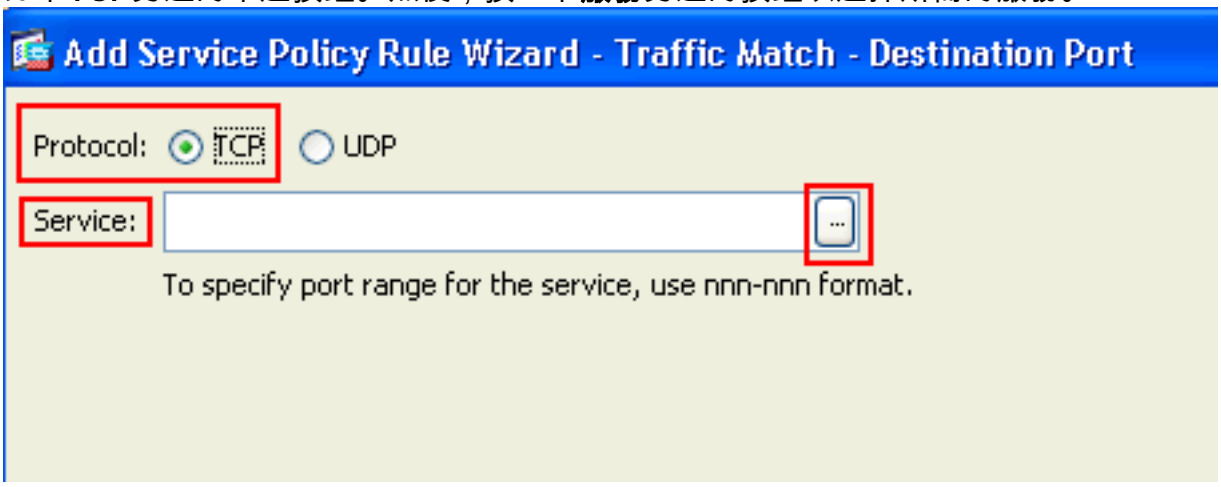
2. 在Add Service Policy Rule Wizard - Service Policy視窗中，選擇**Interface**旁邊的單選按鈕。這會將建立的策略應用於特定介面，在本例中為**Outside**介面。提供一個策略名稱，在本例中為**outside-cisco-policy**。按「**Next**」（下一步）。



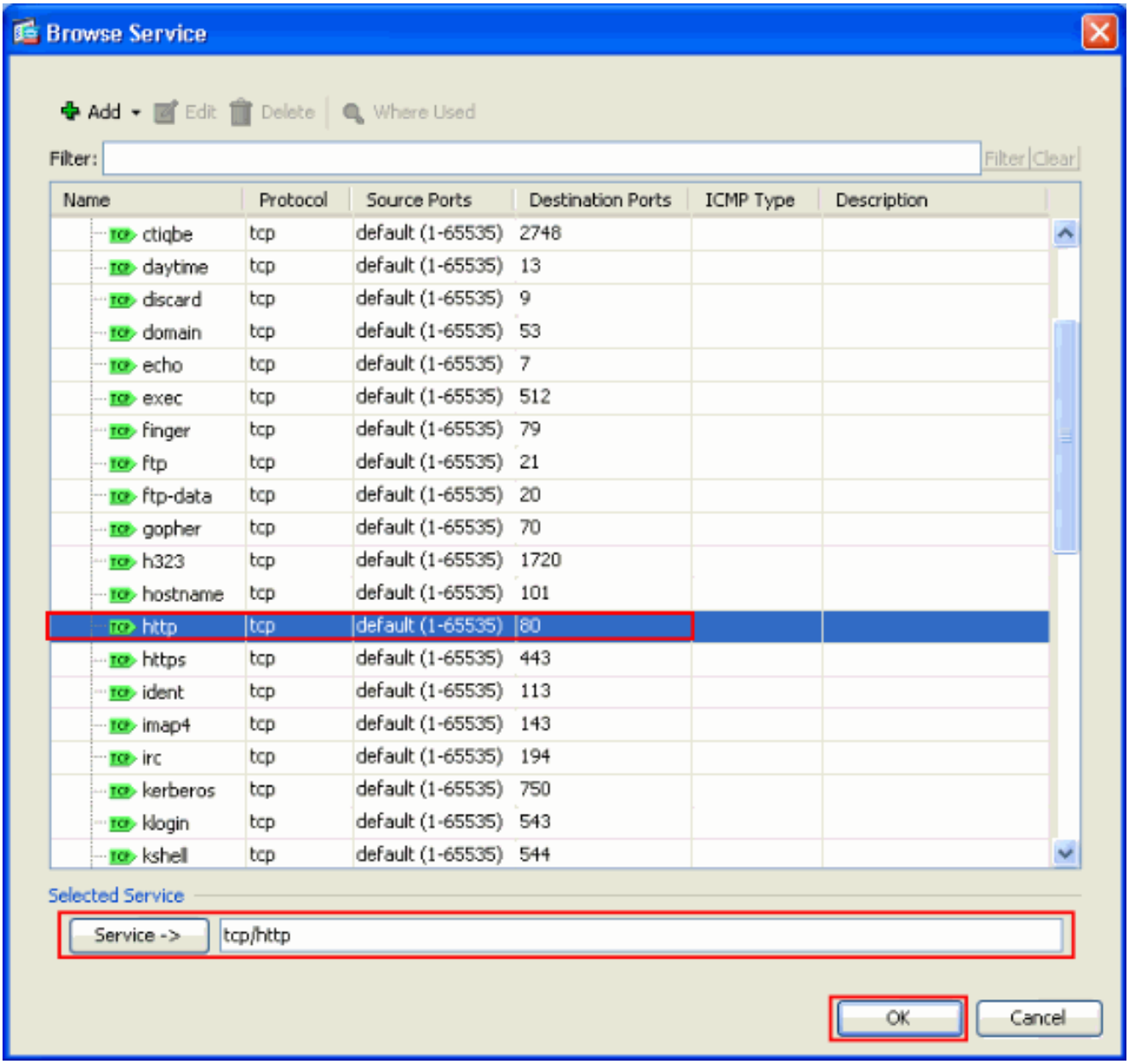
3. 在「新增服務策略規則嚮導 — 流量分類標準」視窗中，提供新的流量類名稱。此示例中使用的名稱為**outside-class**。確保選中**TCP or UDP Destination Port**旁邊的覈取方塊，然後按一下**Next**。



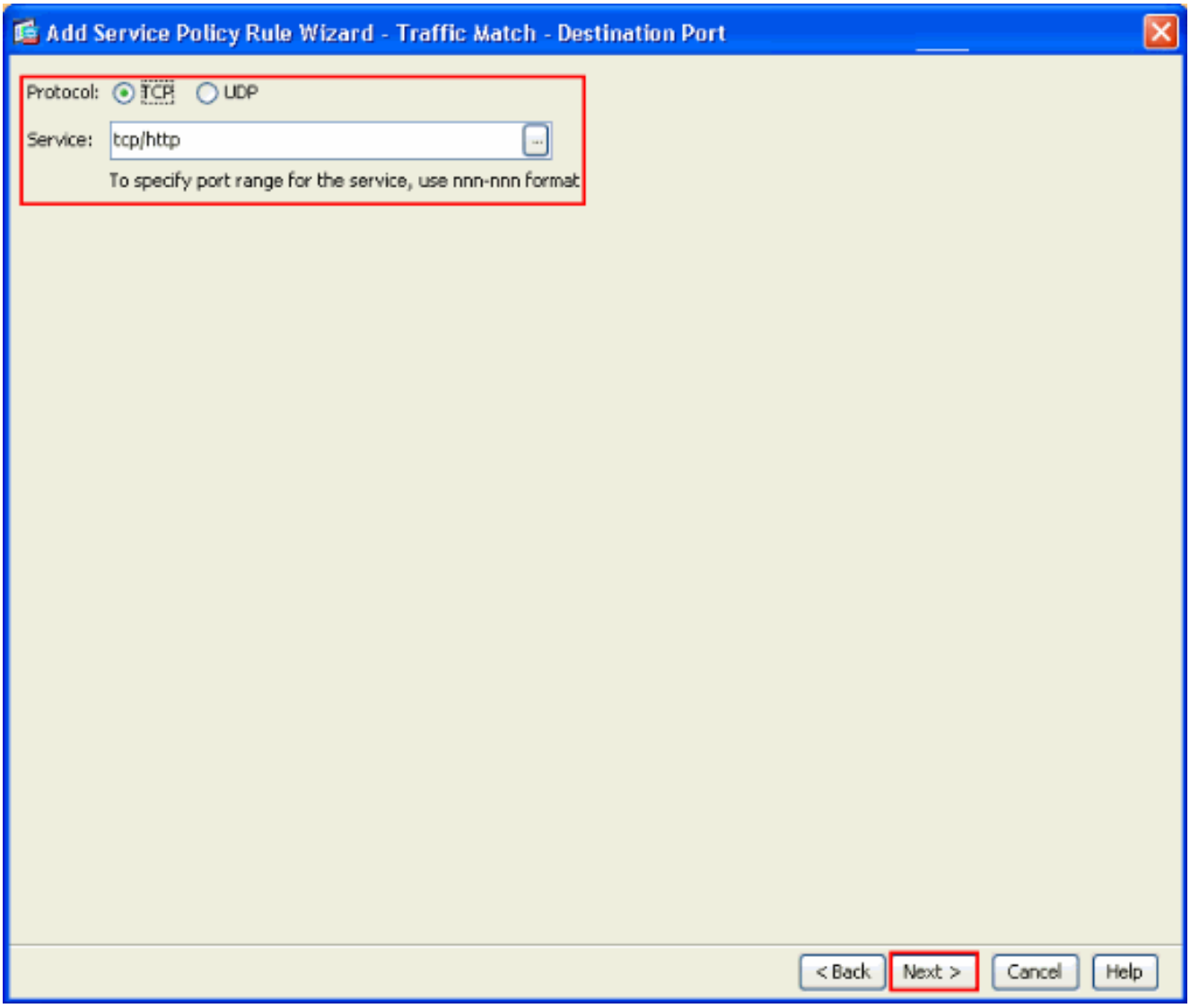
4. 在Add Service Policy Rule Wizard - Traffic Match - Destination Port視窗中，選擇**Protocol**部分下**TCP**旁邊的單選按鈕。然後，按一下**服務**旁邊的按鈕以選擇所需的服務。



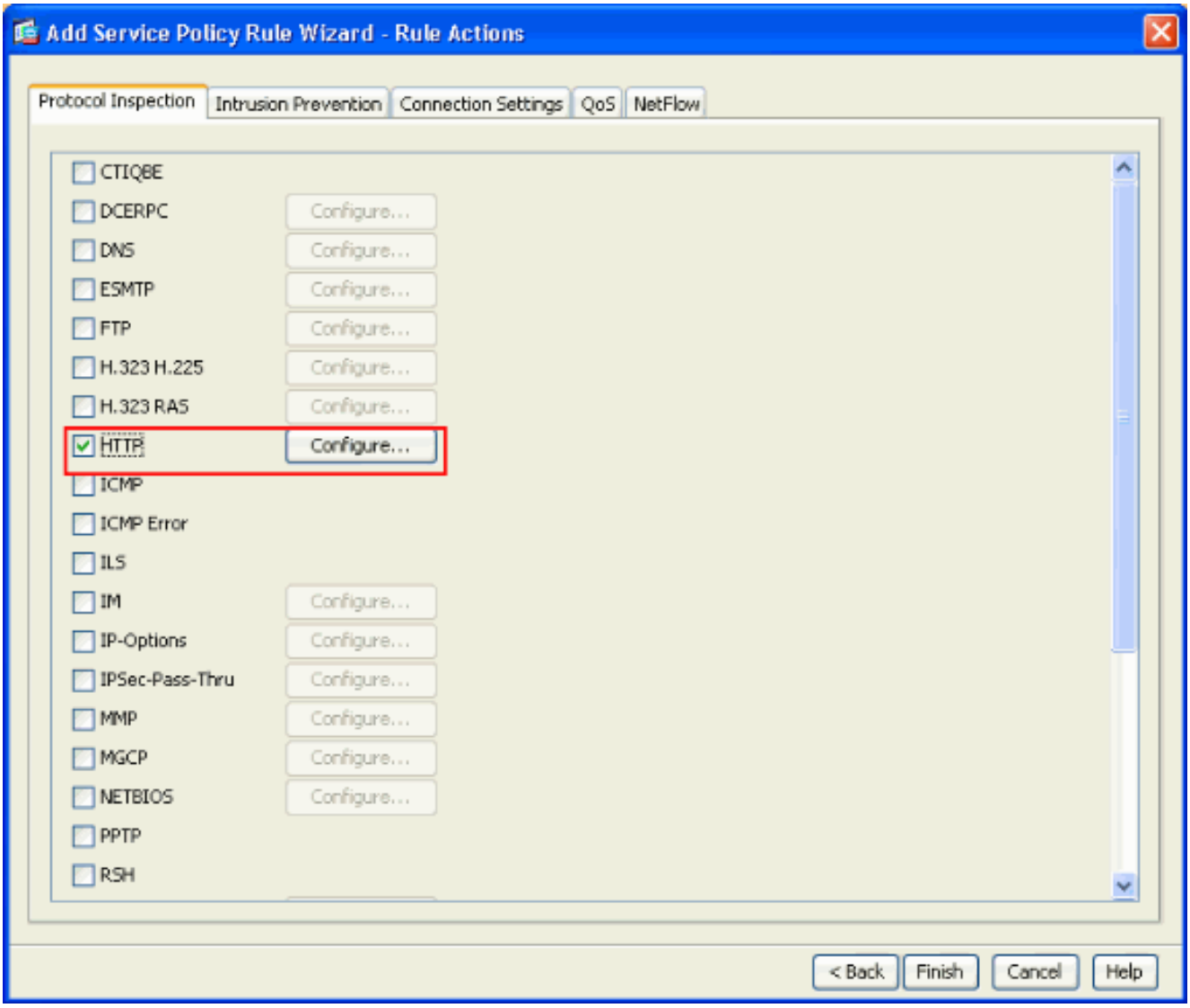
5. 在「瀏覽服務」視窗中，選擇**HTTP**作為服務。然後，按一下**OK**。



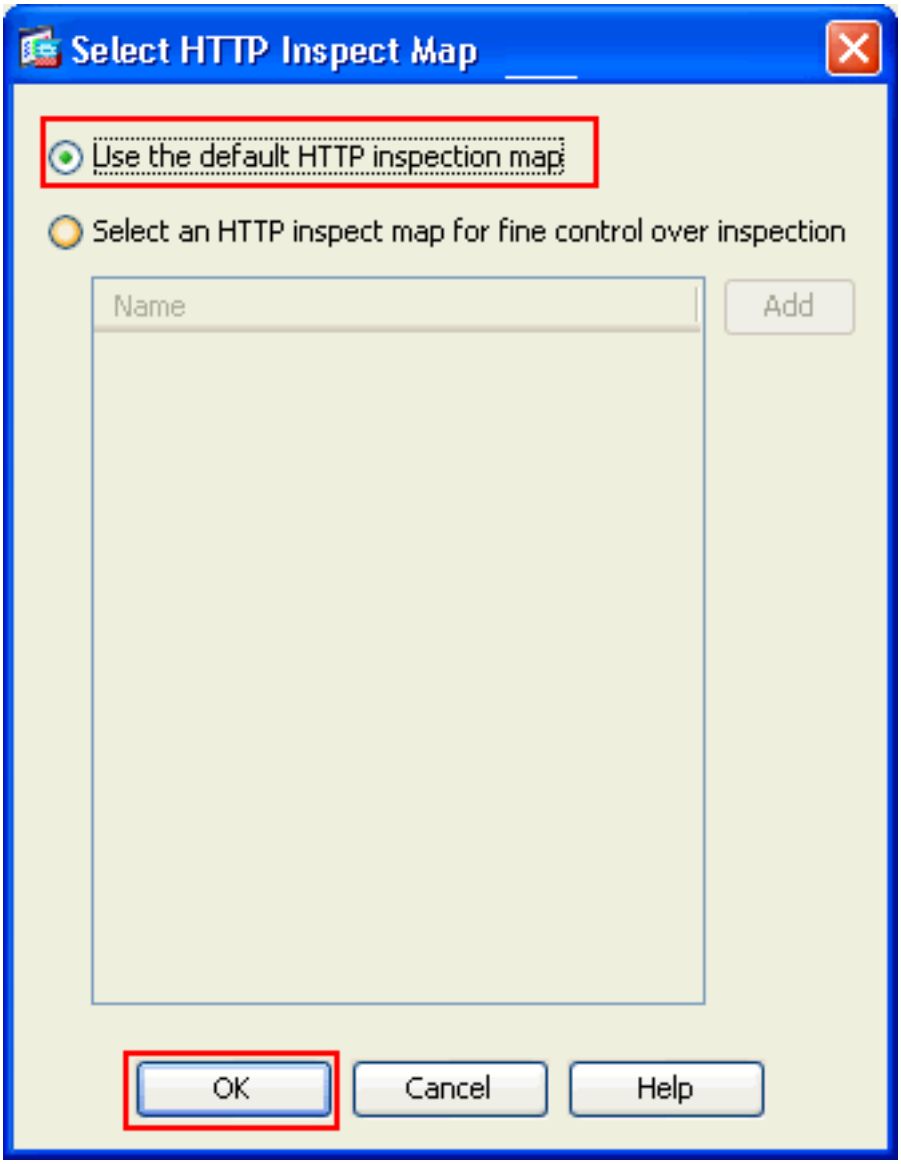
6. 在Add Service Policy Rule Wizard - Traffic Match - Destination Port視窗中，您可以看到所選的服務是**tcp/http**。按「**Next**」（下一步）。



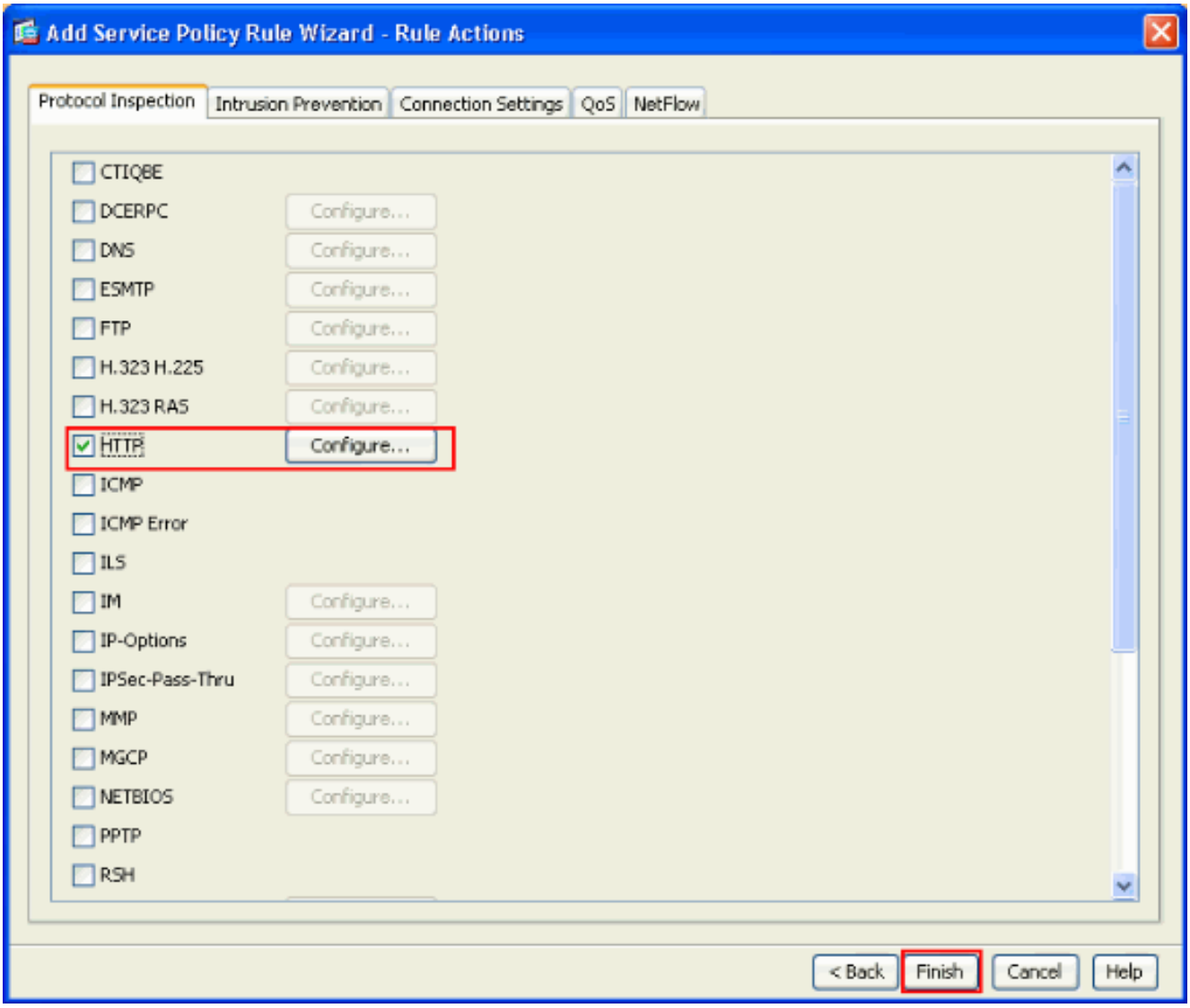
7. 在「新增服務策略規則嚮導 — 規則操作」視窗中，選中**HTTP**旁邊的覈取方塊。然後，點選**HTTP**旁邊的**Configure**。



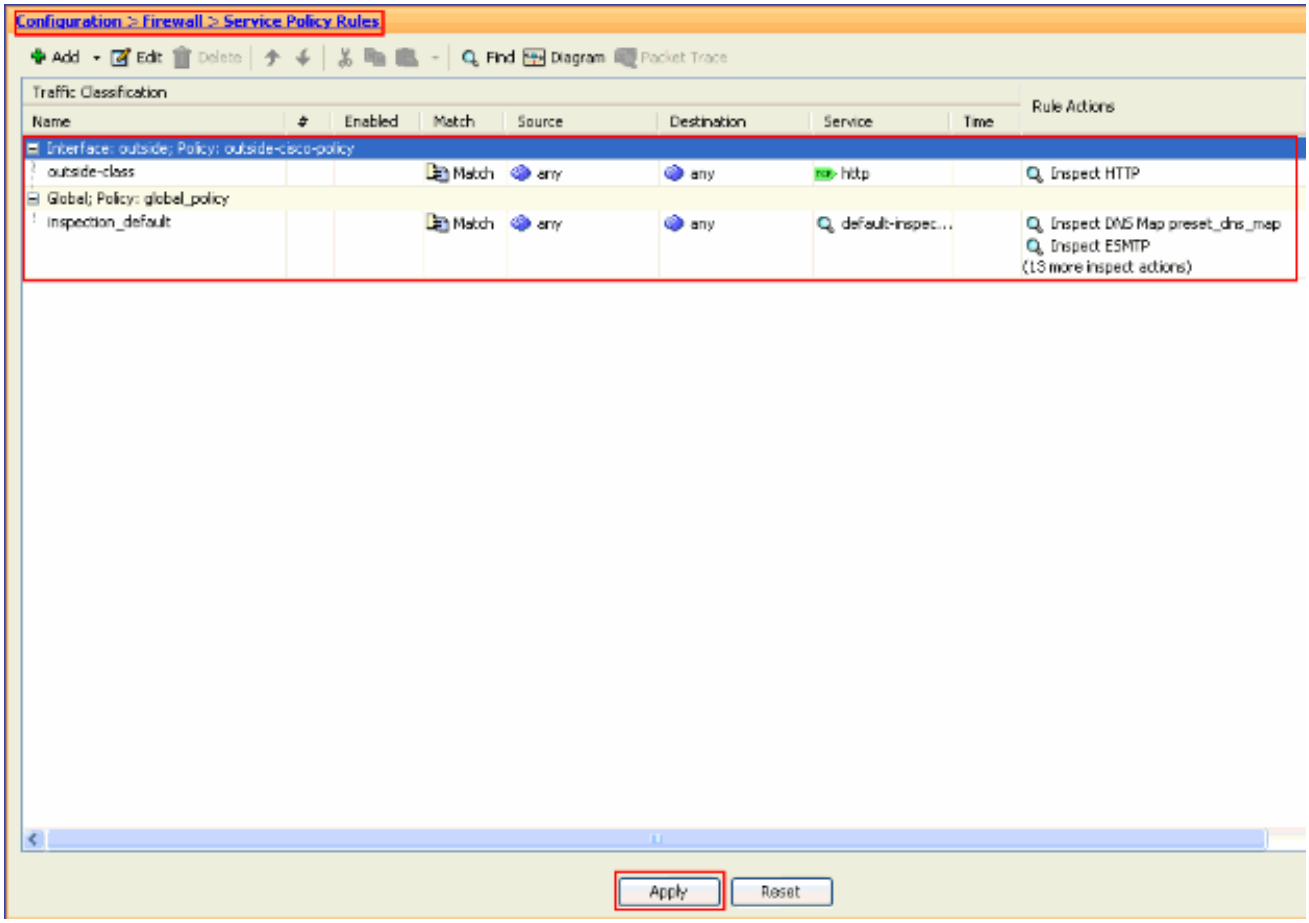
8. 在「選擇HTTP檢查對映」視窗中，選中**使用預設HTTP檢查對映**旁邊的單選按鈕。本示例中使用的是預設HTTP檢測。然後，按一下**OK**。



9. 按一下「**Finish**」（結束）。



10. 在**Configuration > Firewall > Service Policy Rules**下，您將看到新配置的Service Policy **outside-cisco-policy**（檢查HTTP）以及裝置上已經存在的預設服務策略。按一下**Apply**以將配置應用到Cisco ASA。



相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 思科調適型資安裝置管理員
- 要求建議 (RFC)
- 應用應用層協定檢查
- 技術支援與文件 - Cisco Systems