# ASA 8.3以降：ASDMを使用したインスペクションの設定

## 内容



## 概要

このドキュメントでは、アプリケーションのグローバル ポリシーからデフォルトの検査を削除する方法と、Adaptive Security Device Manager（ASDM）を使用してデフォルト以外のアプリケーションの検査を有効にする方法に関する、バージョン 8.3(1) 以降の Cisco 適応型セキュリティ アプライアンス（ASA）の設定例を示します。

詳細は、『PIX/ASA 7.X：デフォルトのデフォルト グローバル インスペクションを無効にして、デフォルト以外のアプリケーションのインスペクションを有効にする』（Cisco ASA バージョン 8.2 以前の同じ構成が対象）を参照してください。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、Cisco ASA セキュリティ アプライアンス ソフトウェア バージョン 8.3(1) と ASDM 6.3 が稼働する環境に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

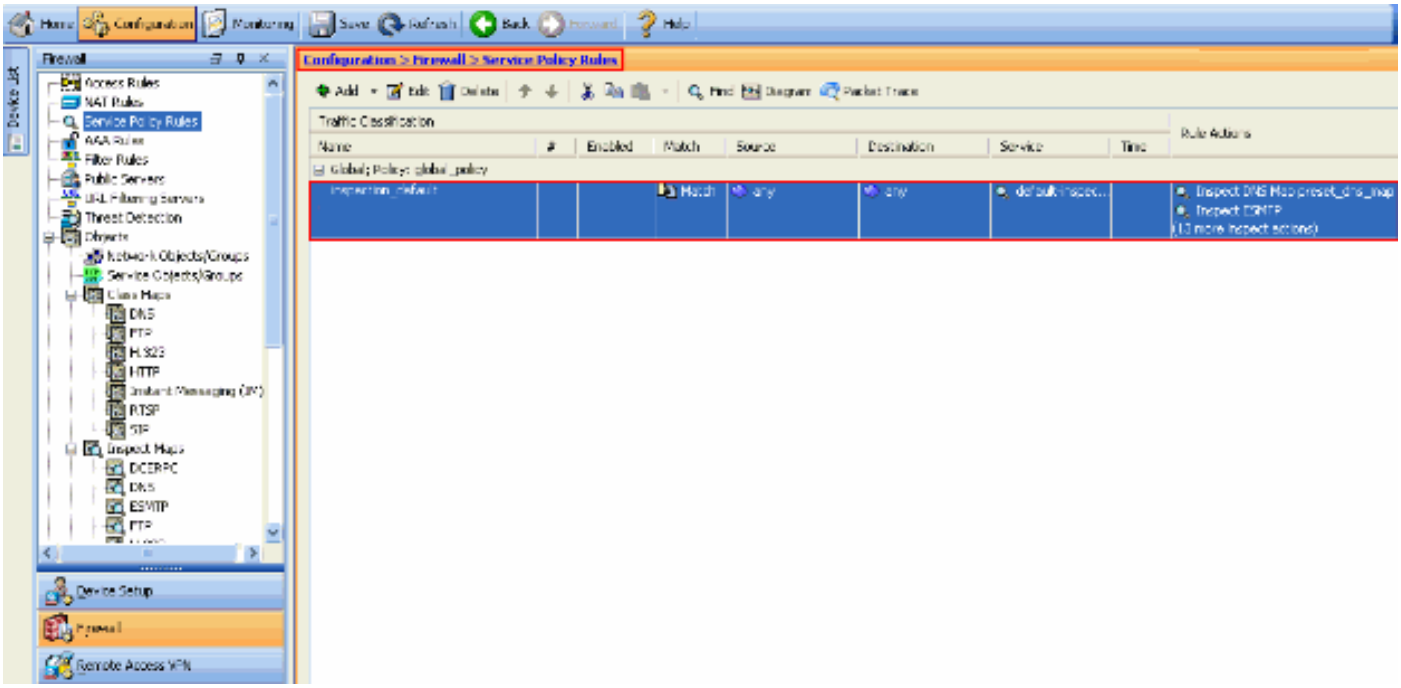
## 表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

# デフォルトのグローバル ポリシー

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーが設定に含まれ、特定のインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。 すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。適用できるグローバル ポリシーは 1 つだけです。グローバル ポリシーを変更する場合は、デフォルト ポリシーを編集するか無効にし、新しいポリシーを適用する必要があります。（インターフェイス ポリシーはグローバル ポリシーに優先します）。

ASDM で、[Configuration] > [Firewall] > [Service Policy Rules] を選択して、以下に示すデフォルトのアプリケーション インスペクションを持つデフォルトのグローバル ポリシーを表示します。

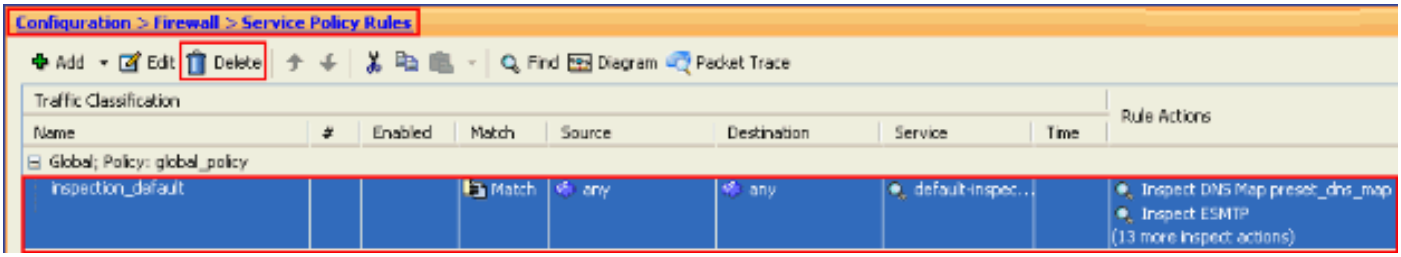



デフォルト ポリシー設定には、次のコマンドが含まれています。

```
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
```

グローバル ポリシーを無効にする必要がある場合は、**no service-policy global_policy グローバル コマンドを使用します。**ASDM を使用してグローバル ポリシーを削除するには、[Configuration] > [Firewall] > [Service Policy Rules] を選択します。次に、グローバル ポリシーを選択し、[Delete] をクリックします。




**注：ASDMを使用**してサービスポリシーを削除すると、関連付けられたポリシーとクラスマップが削除されます。ただし、CLI を使用してサービス ポリシーが 削除された場合は、サービス ポリシーのみがインターフェイスから削除されます。クラス マップおよびポリシー マップは変更されずそのまま残ります。

## アプリケーションのデフォルト グローバル インスペクションを無効にする

アプリケーションのグローバル インスペクションを無効にするには、*inspect* コマンドの **no** バージョンを使用します。

たとえば、セキュリティ アプライアンスでリッスンする FTP アプリケーションのグローバル インスペクションを削除するには、クラス コンフィギュレーション モードで **no inspect ftp** コマンドを使用します。

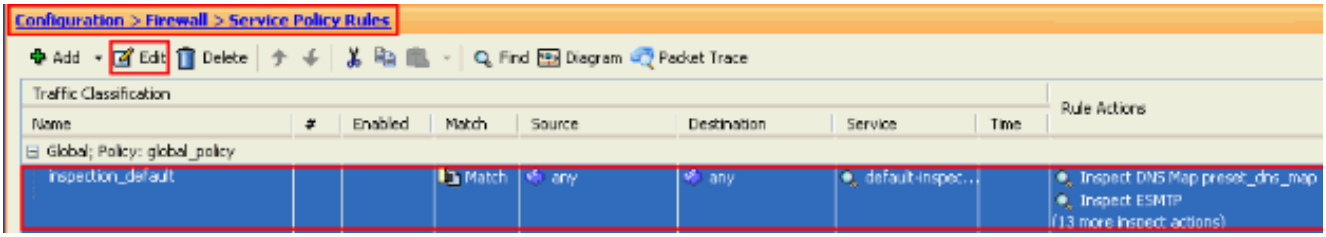
クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの *no* 形式を使用します。

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

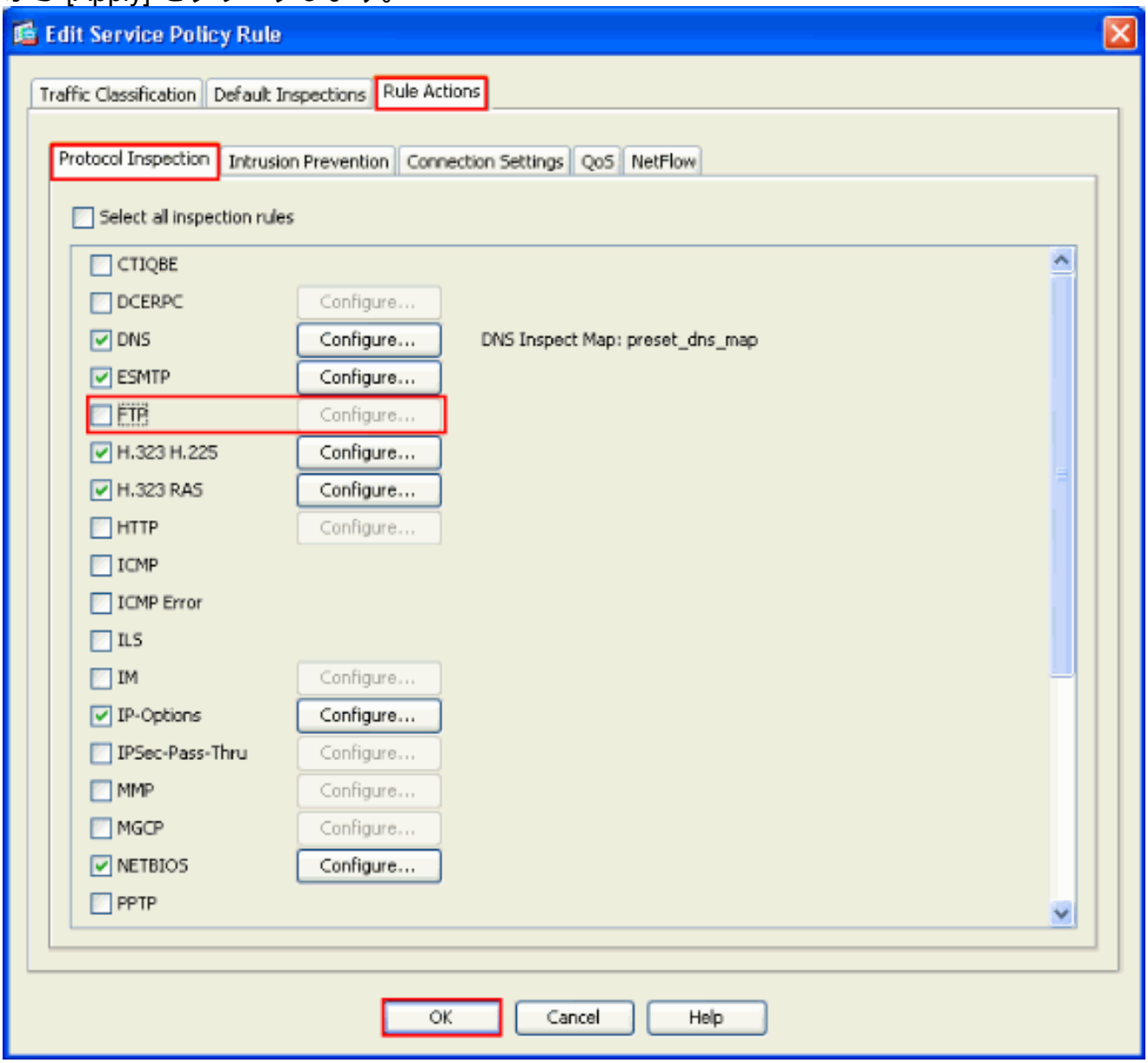
ASDM を使用して FTP のグローバル インスペクションを無効にするには、次の手順を実行してください。

**注：ASDMを介**してPIX/ASAにアクセスする基本的な設定については、『ASDM用のHTTPSアクセスの許可』を参照してください。

1. [Configuration] > [Firewall] > [Service Policy Rules] を選択して、デフォルトのグローバル ポリシーを選択します。次に、グローバル インスペクション ポリシーを編集するには、[Edit] をクリックします。




2. [Edit Service Policy Rule] ウィンドウで、[Rule Actions] タブの [Protocol Inspection] を選択します。[FTP] チェック ボックスがオフになっていることを確認します。これにより、次の画像に示すように、FTP インスペクションが無効になります。次に、[OK] をクリックしてから [Apply] をクリックします。




**注：FTP**インスペクションの詳細については、『PIX/ASA 7.x:FTP/TFTP サービスをイネーブルにする設定例』を参照してください。

## デフォルト以外のアプリケーションのインスペクションを有効にする

拡張 HTTP インスペクションは、デフォルトではディセーブルになっています。global_policy の HTTP インスペクションを有効にするには、クラスの inspection_default 下で **inspect http コマンドを使用します。**

この例では、任意のインターフェイスを通過してセキュリティ アプライアンスに入るすべての

HTTP 接続（ポート 80 の TCP トラフィック）が HTTP インスペクション対象として分類されます。*このポリシーはグローバル ポリシーであるため、インスペクションが発生するのは各インターフェイスにトラフィックが入ったときだけです。*

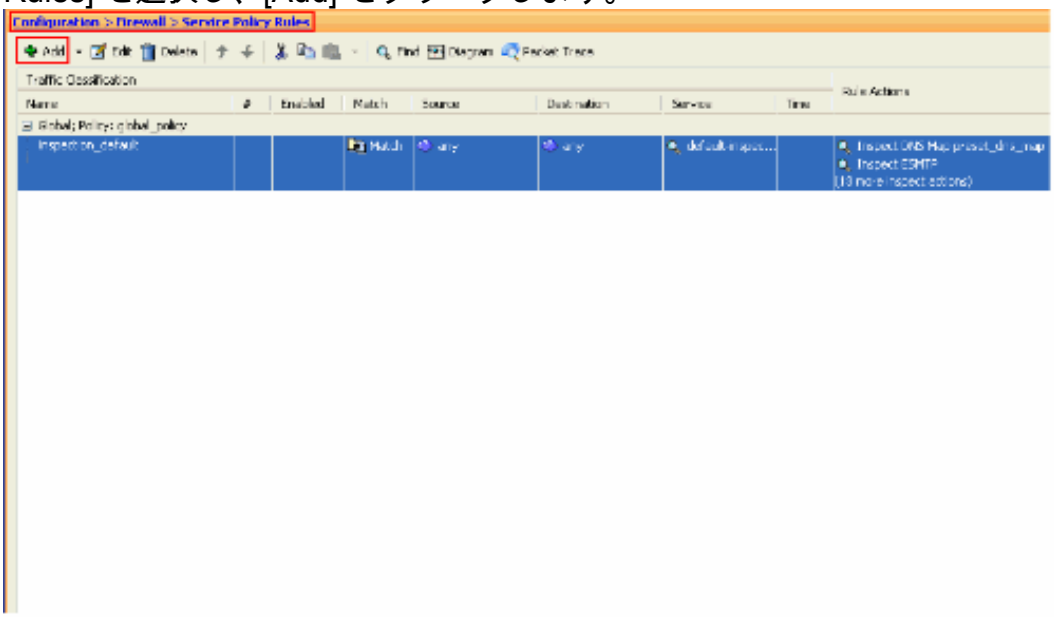
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

*この例では、セキュリティ アプライアンスを出入りする HTTP 接続（ポート 80 の TCP トラフィック）で外部インターフェイスを通過するすべての接続が HTTP インスペクション対象として分類されます。*

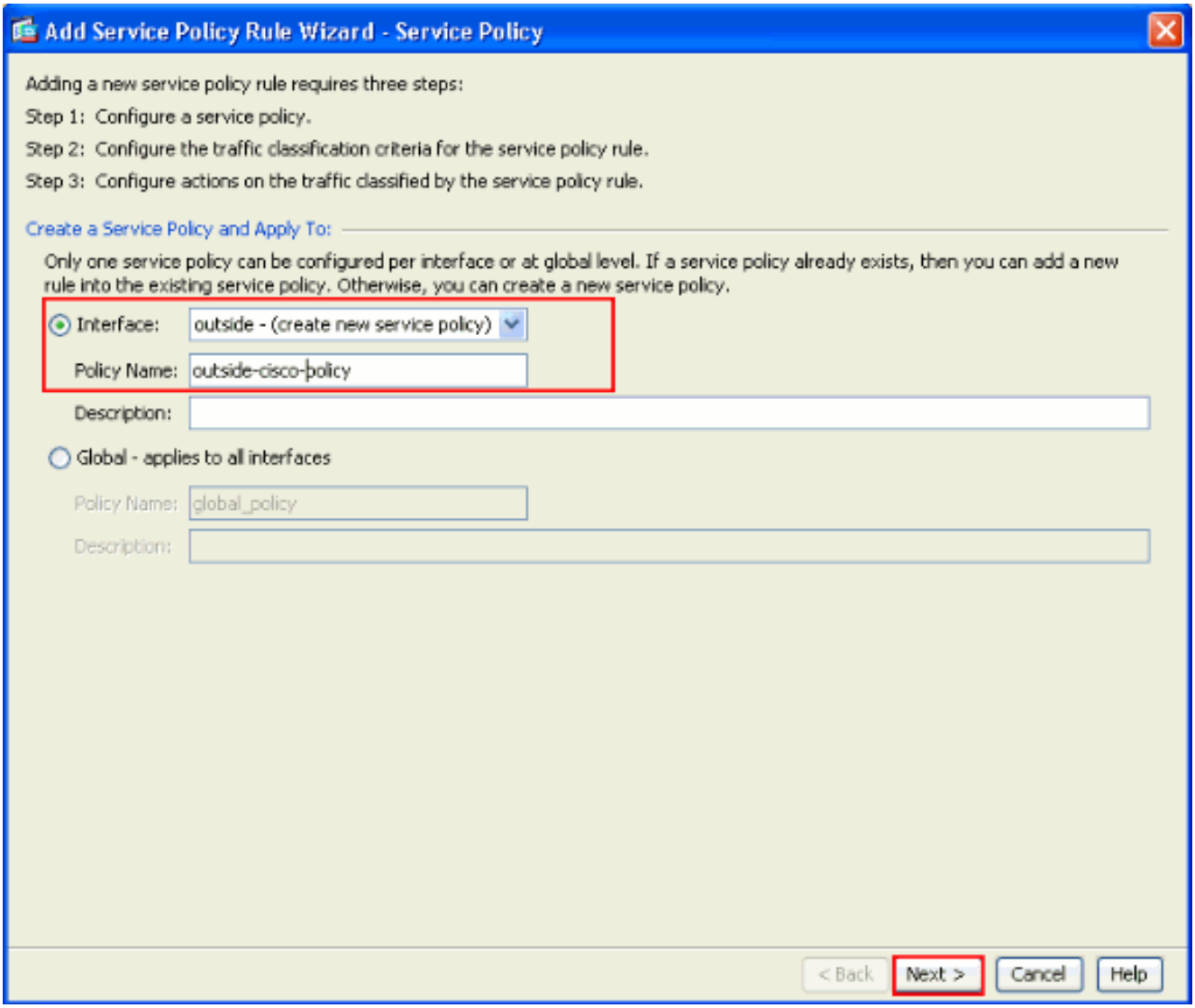
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

ASDM を使用して上記の例を設定するには、次の手順を実行します。

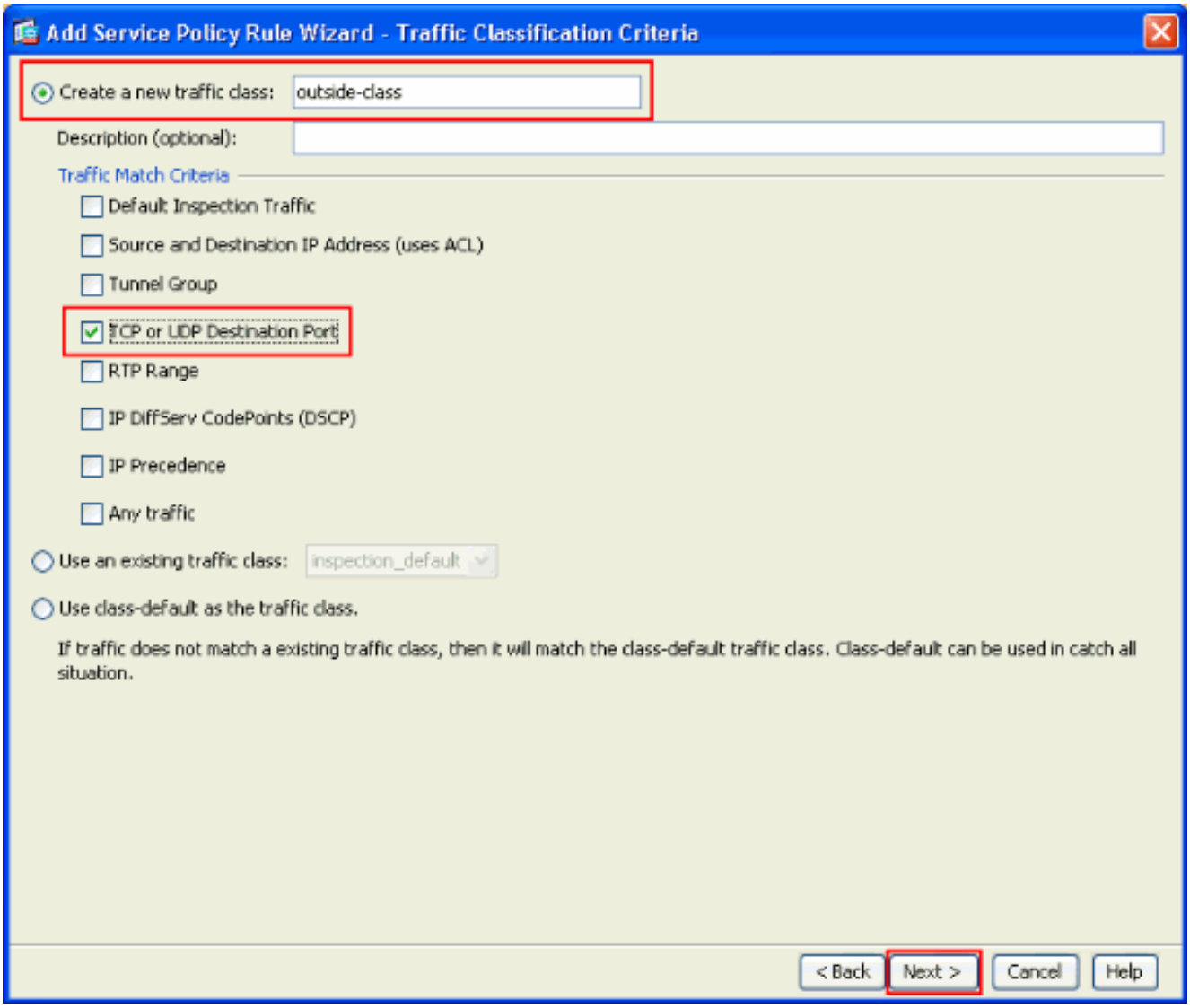
1. 新しいサービス ポリシーを追加するには、[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] をクリックします。



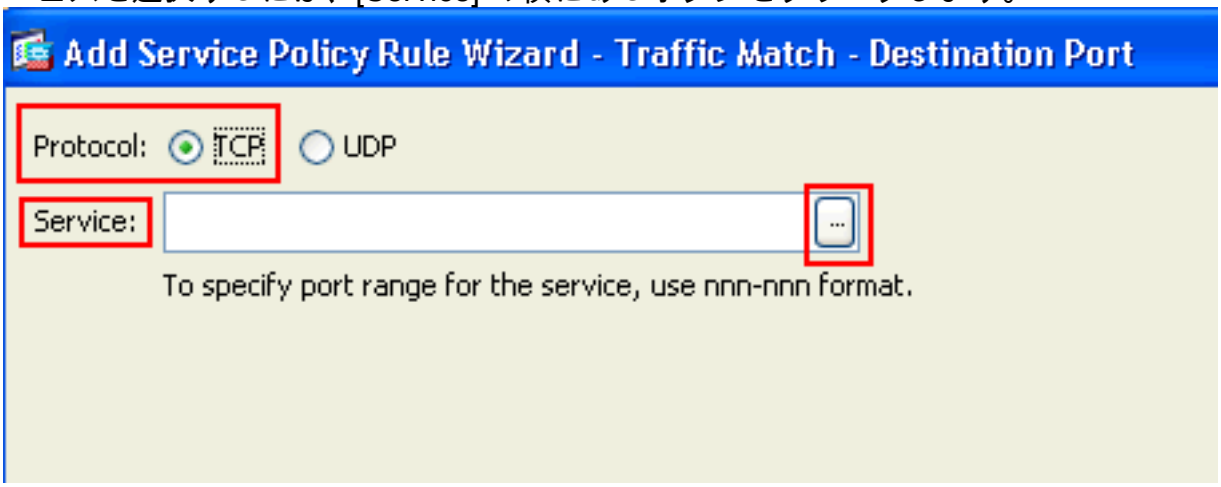

2. [Add Service Policy Rule Wizard - Service Policy] ウィンドウから、[Interface] の横にあるオプション ボタンを選択します。これにより、作成したポリシーが特定のインターフェイス（この例では **Outside interface）に適用されます。**ポリシー名（この例では **outside-cisco-policy）を付けます。**[next] をクリックします。



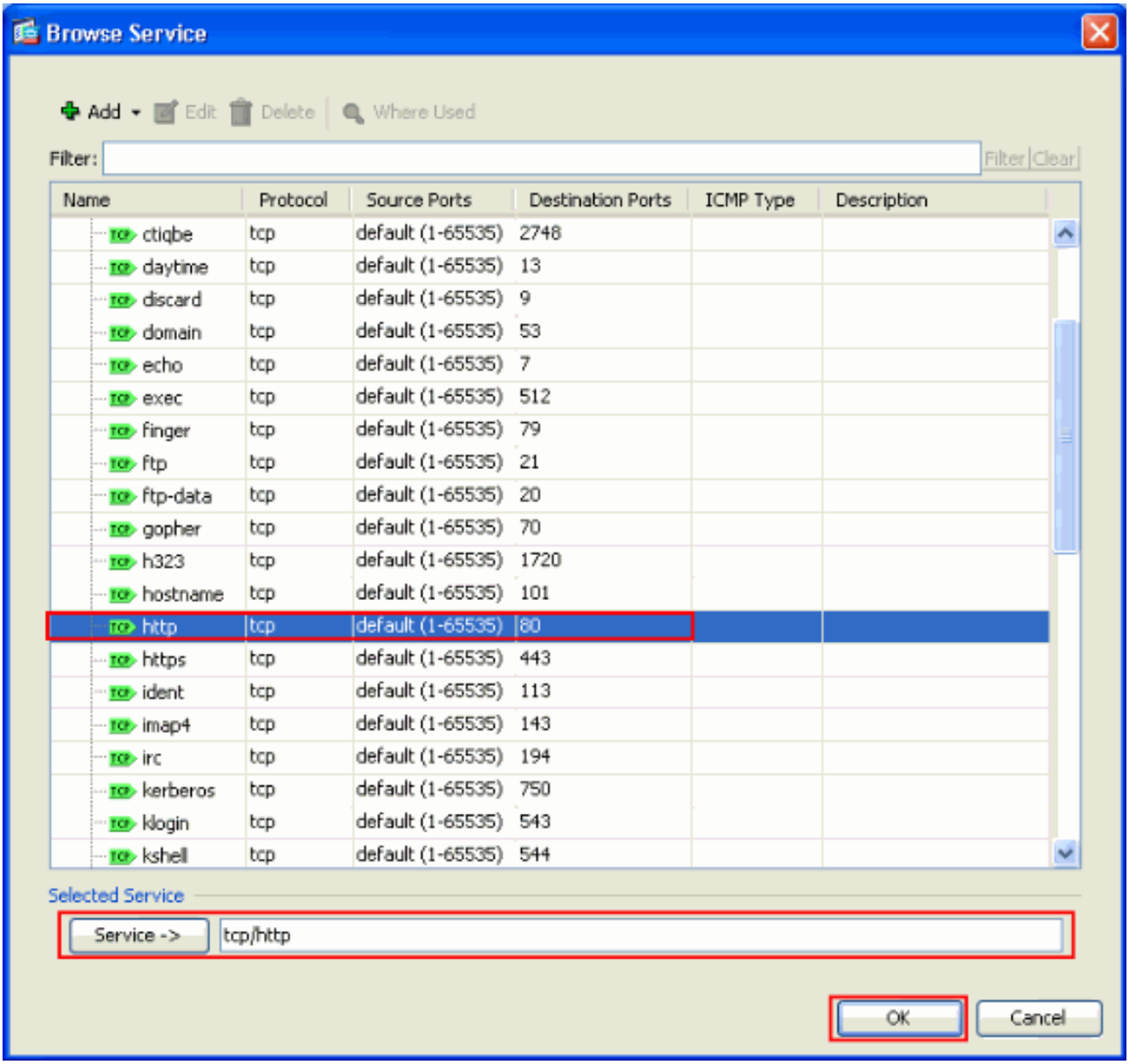

3. [Add Service Policy Rule Wizard - Traffic Classification Criteria] ウィンドウから、新しいトラフィック クラスの名前を指定します。この例で使用する名前は、**outside-class**です。[TCP or UDP Destination Port] の隣のチェック ボックスがオンになっていることを確認して、[Next] をクリックします。



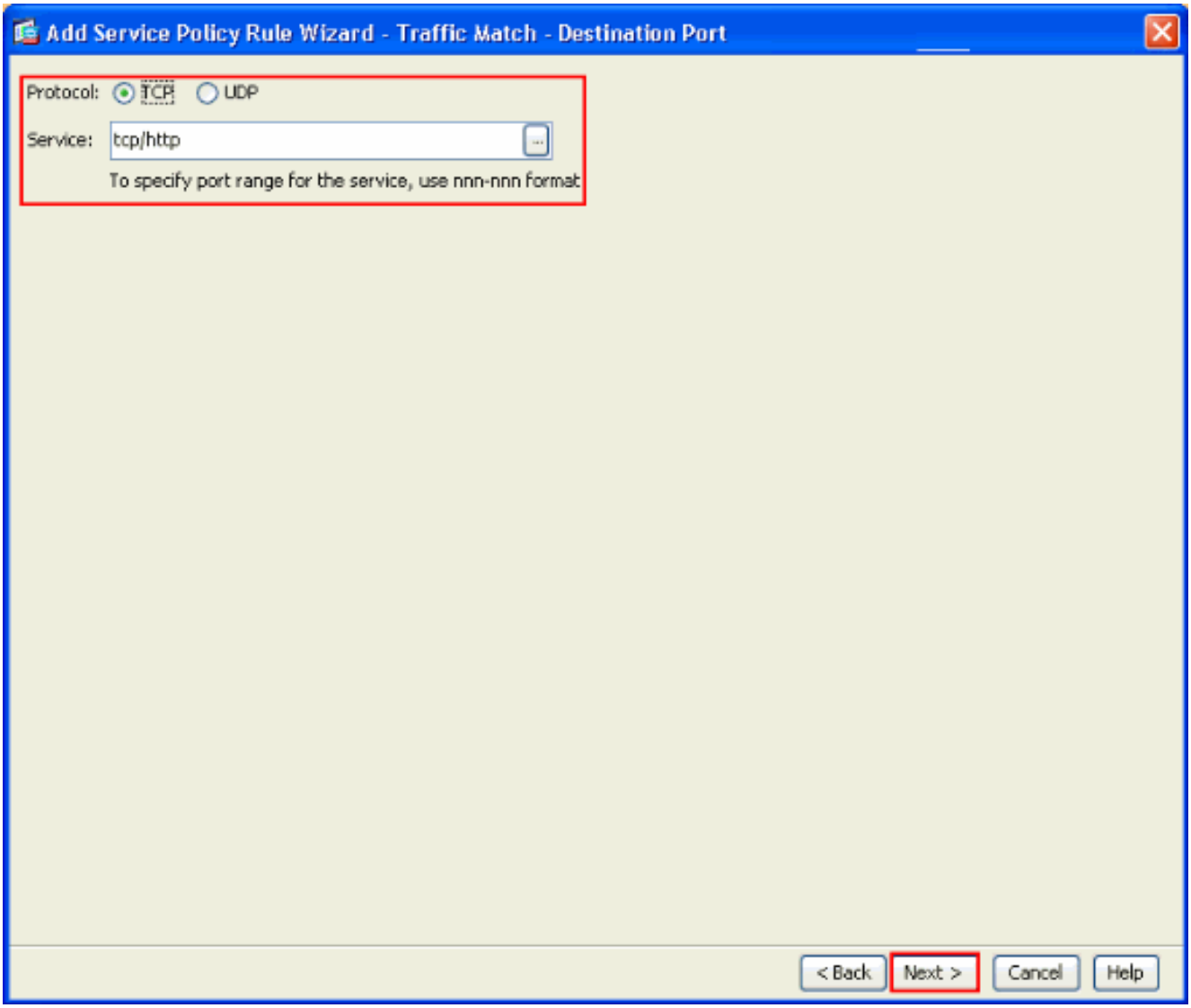

4. [Add Service Policy Rule Wizard - Traffic Match - Destination Port] ウィンドウから、[Protocol] セクションの [TCP] の横にあるオプション ボタンを選択します。次に、必要なサービスを選択するには、[Service] の横にあるボタンをクリックします。



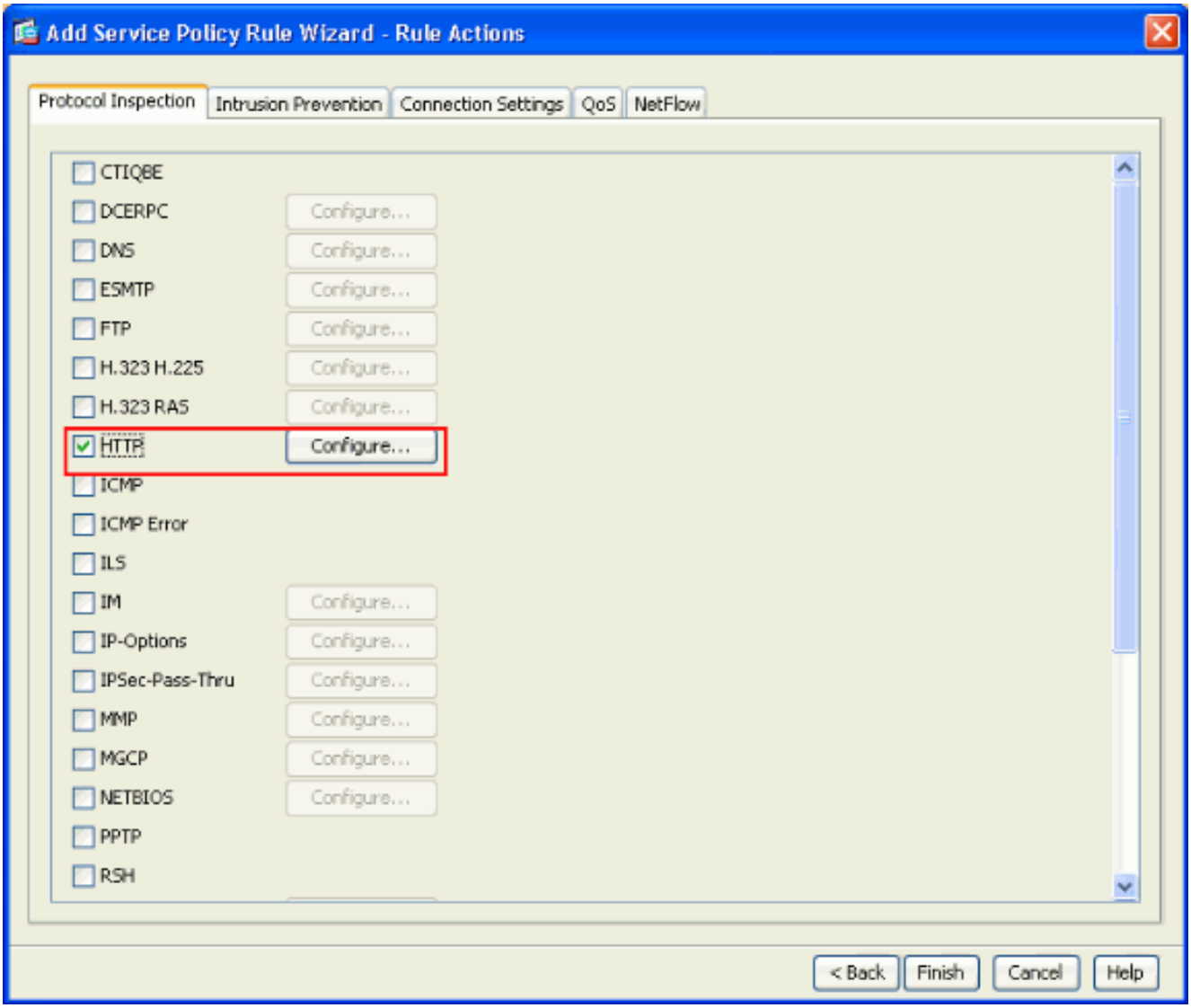

5. [Browse Service] ウィンドウで、サービスとして [HTTP] を選択します。次に、[OK] をクリックします。



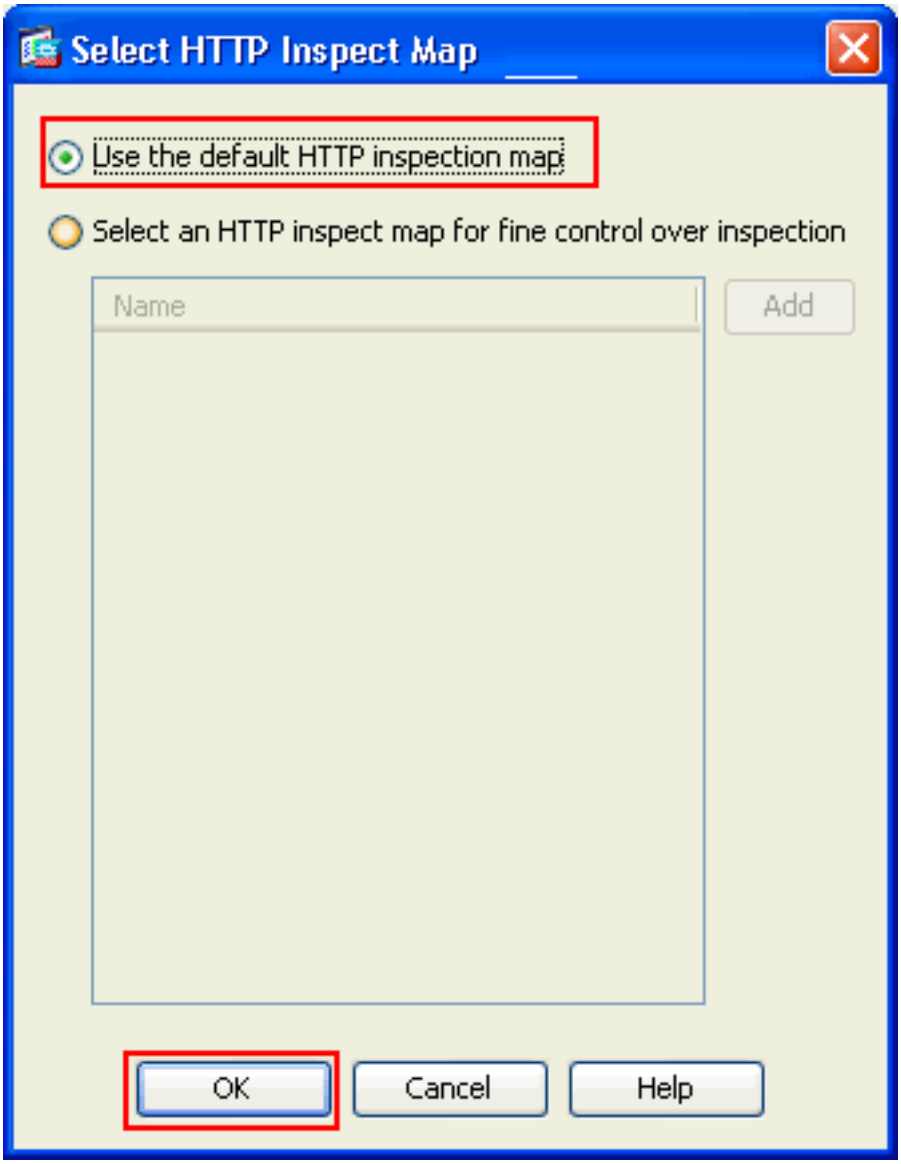

6. [Add Service Policy Rule Wizard - Traffic Match - Destination Port] ウィンドウで、選択された [Service] が **tcp/http であることを確認できます。**[next] をクリックします。



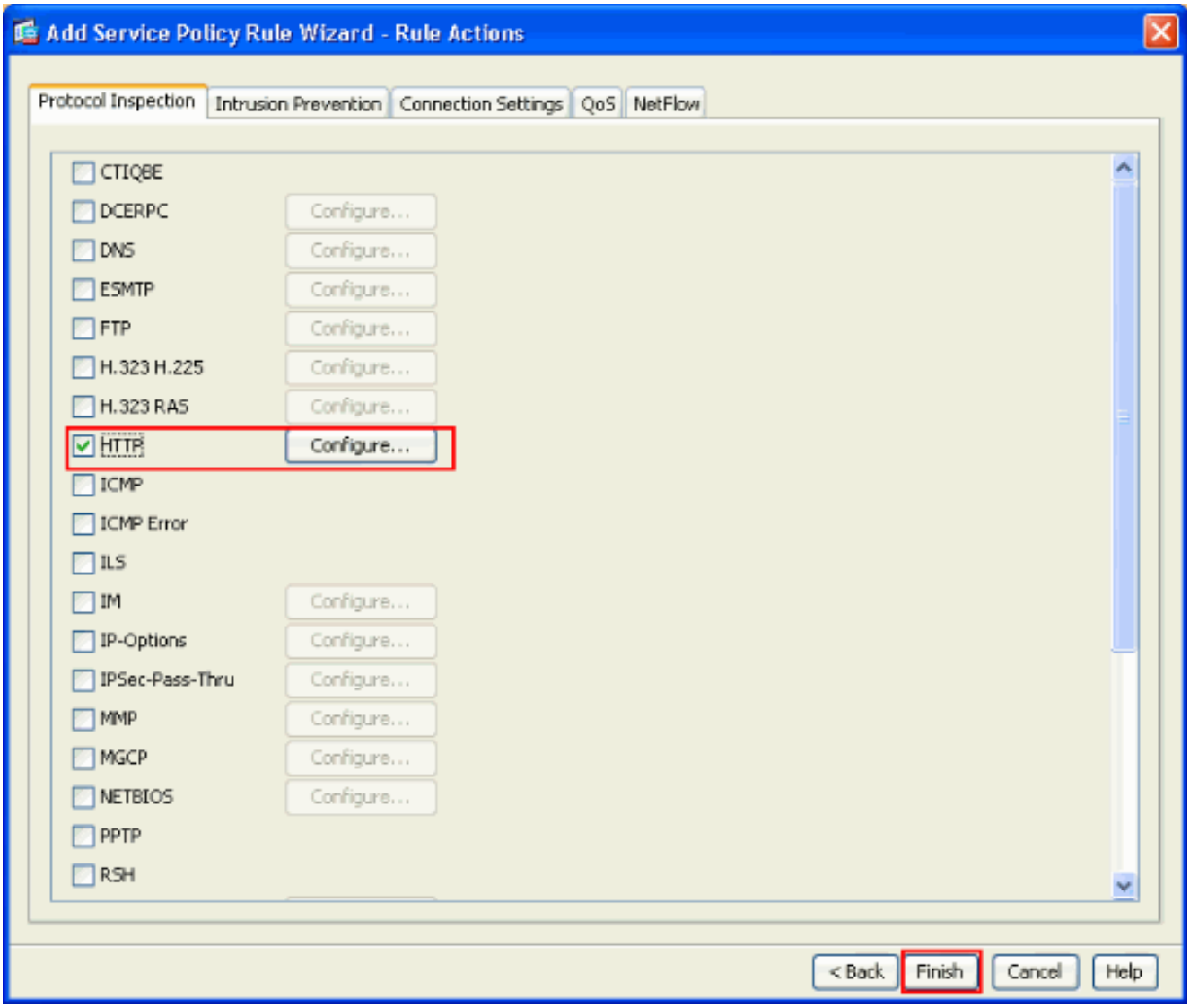

7. [Add Service Policy Rule Wizard - Rule Actions] ウィンドウから、[HTTP] の隣にあるチェックボックスをオンにします。次に、[HTTP]の横にある [Configure] をクリックします。



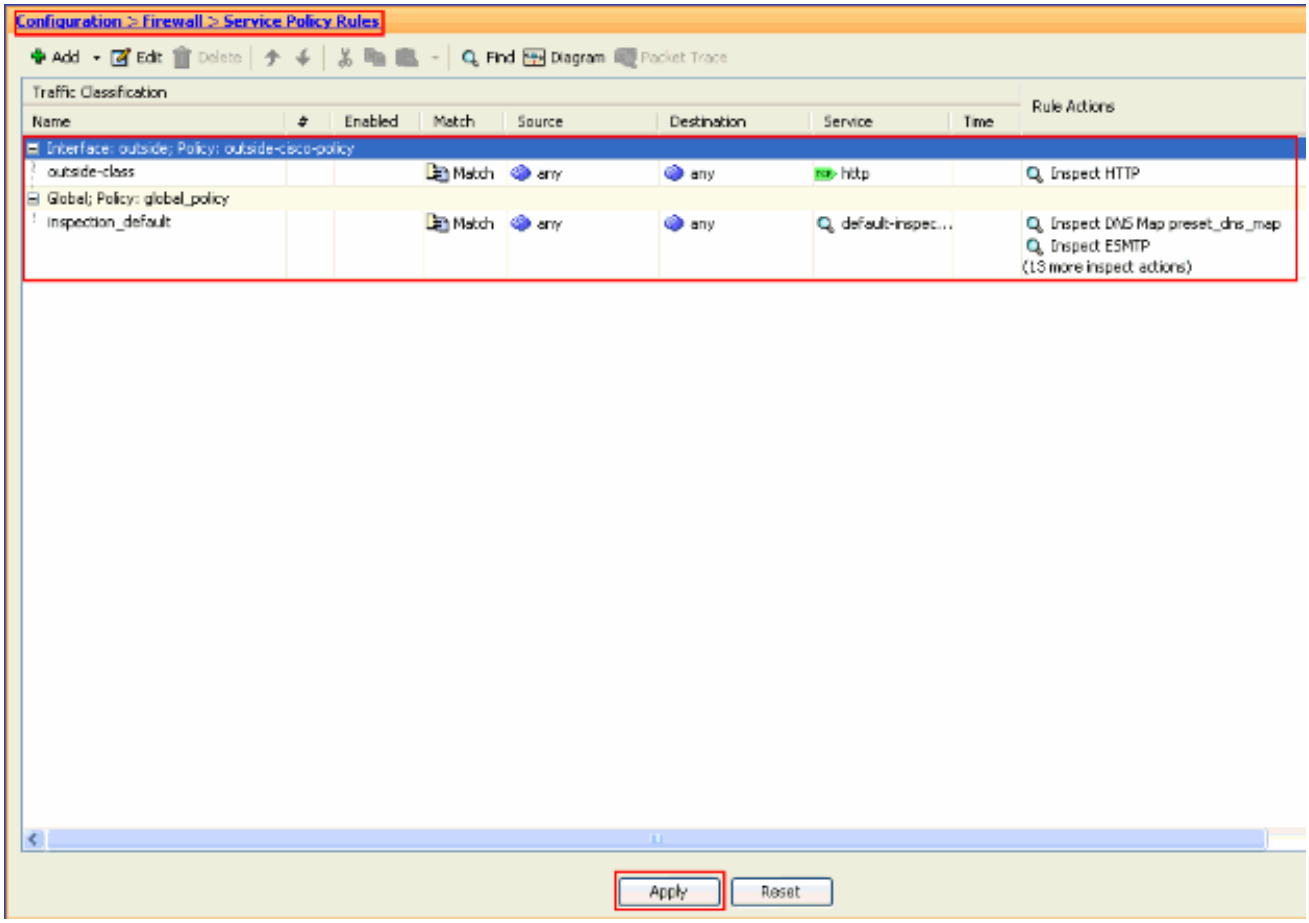

8. [Select HTTP Inspect Map] ウィンドウから、[Use the Default HTTP inspection map] の横にあるラジオ ボタンをオンにします。この例では、デフォルトの HTTP インスペクションを使用します。次に、[OK] をクリックします。




9. [Finish] をクリックします。




10. [Configuration] > [Firewall] > [Service Policy Rules] で、新しく設定したサービス ポリシーである outside-cisco-policy（HTTP インスペクション用）が、アプライアンスに既に存在するデフォルトのサービス ポリシーとともに表示されます。[Apply] をクリックして Cisco ASA に設定に適用します。




# 関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco Adaptive Security Device Manager
- Requests for Comments (RFCs)
- アプリケーション層プロトコル検査の適用
- テクニカル サポートとドキュメント – Cisco Systems