

# ASA/PIX 7.X: Deaktivieren Sie die globale Standardinspektion, und aktivieren Sie nicht standardmäßige Anwendungsinspektion mit ASDM.

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Zugehörige Produkte](#)

[Konventionen](#)

[Globale Standardrichtlinie](#)

[Nicht standardmäßige Anwendungsinspektion aktivieren](#)

[Überprüfen](#)

[Zugehörige Informationen](#)

## [Einführung](#)

In diesem Dokument wird beschrieben, wie die Standardüberprüfung für eine Anwendung aus der globalen Richtlinie entfernt wird und wie die Überprüfung für eine nicht standardmäßige Anwendung aktiviert wird.

## [Voraussetzungen](#)

### [Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

### [Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance (ASA), die das 7.x-Software-Image ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Zugehörige Produkte

Diese Konfiguration kann auch mit der PIX Security Appliance verwendet werden, die das 7.x-Software-Image ausführt.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## Globale Standardrichtlinie

Standardmäßig enthält die Konfiguration eine Richtlinie, die dem gesamten standardmäßigen Anwendungsinspektionsverkehr entspricht und bestimmte Überprüfungen auf den Datenverkehr an allen Schnittstellen anwendet (eine globale Richtlinie). Nicht alle Überprüfungen sind standardmäßig aktiviert. Sie können nur eine globale Richtlinie anwenden. Wenn Sie die globale Richtlinie ändern möchten, müssen Sie entweder die Standardrichtlinie bearbeiten oder deaktivieren und eine neue Richtlinie anwenden. (Eine Schnittstellenrichtlinie überschreibt die globale Richtlinie.)

Die Standardrichtlinienkonfiguration umfasst die folgenden Befehle:

```
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
```

## Nicht standardmäßige Anwendungsinspektion aktivieren

Gehen Sie wie folgt vor, um eine Nicht-Standard-Anwendungsinspektion auf der Cisco ASA zu aktivieren:

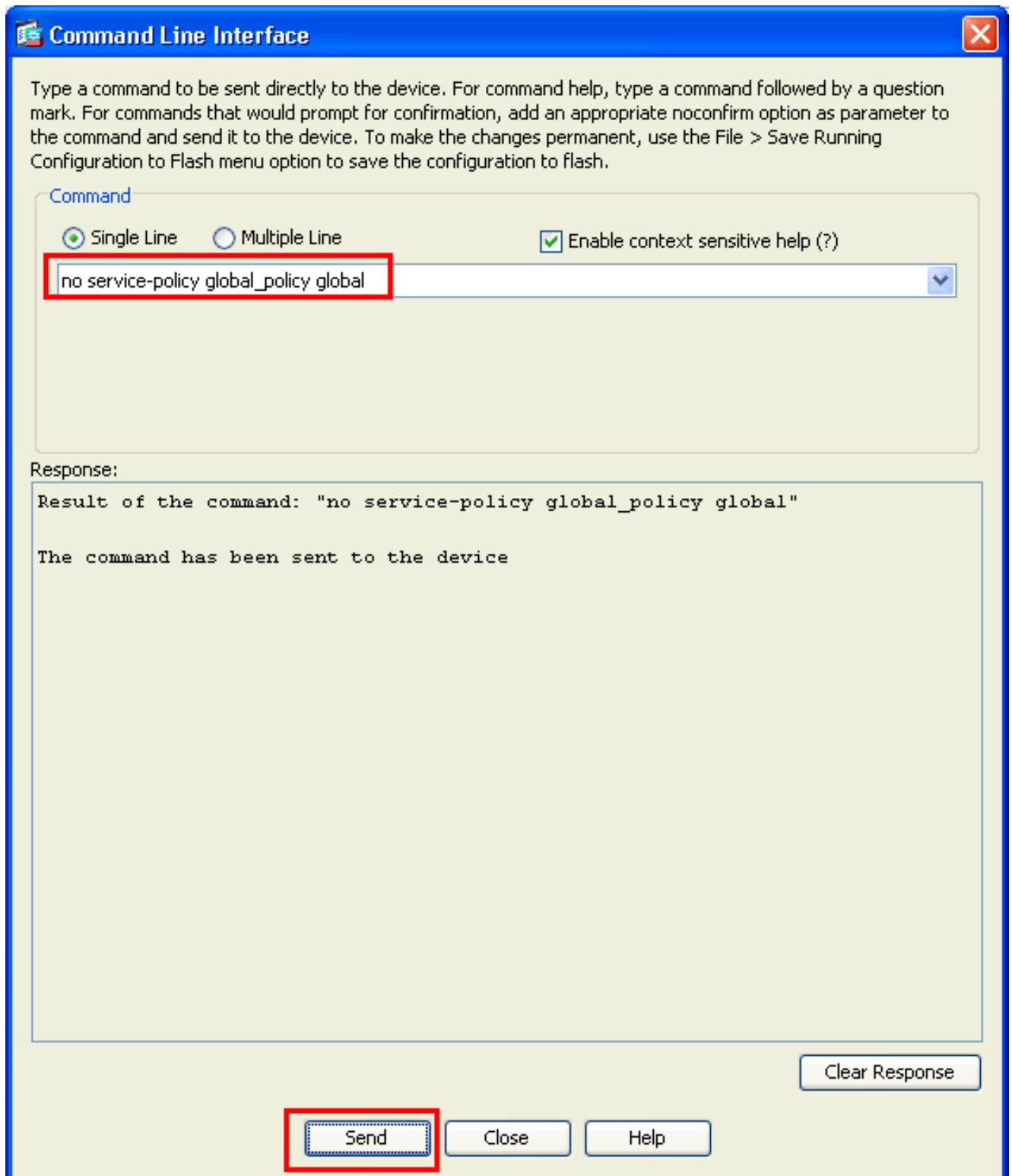
1. Melden Sie sich beim **ASDM an**. Gehen Sie zu **Konfiguration > Firewall > Service Policy Rules**.

Configuration > Firewall > Service Policy Rules

+ Add   Edit   Delete   ↑ ↓   Copy   Paste   Find   Diagram   Packet Trace

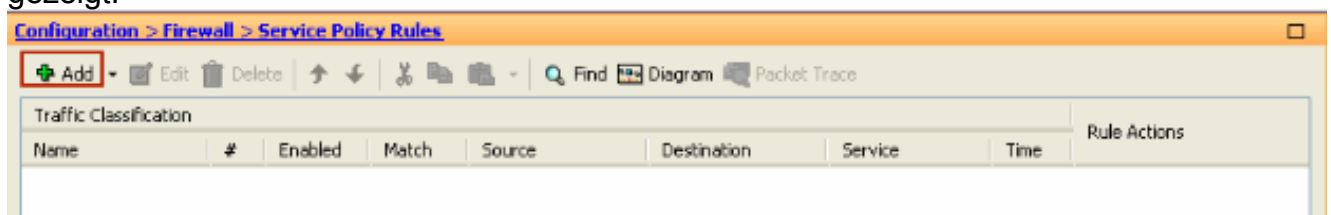
Traffic Classification								Rule Actions
Name	#	Enabled	Match	Source	Destination	Service	Time	
Global; Policy: global_policy								
inspection_default			Match	any	any	default-inspe...		Inspect DNS Map prese... Inspect ESMTTP (12 more inspect actions)

2. Wenn Sie die Konfiguration für globale Richtlinien beibehalten möchten, die die Standard-Klassenzuordnung und die Standard-Richtlinienzuordnung enthält, die Richtlinie aber global entfernen möchten, gehen Sie zu **Extras > Befehlszeilenschnittstelle** und verwenden Sie den Befehl **no service-policy global-policy**, um die Richtlinie global zu entfernen. Klicken Sie anschließend auf **Senden**, um den Befehl auf die ASA anzuwenden.



**Hinweis:** Bei diesem Schritt wird die globale Richtlinie im ASDM (Adaptive Security Device Manager) nicht mehr angezeigt, sondern in der CLI angezeigt.

3. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen, wie hier gezeigt:



4. Stellen Sie sicher, dass das Optionsfeld neben **Interface (Schnittstelle)** aktiviert ist, und wählen Sie im Dropdown-Menü die Schnittstelle aus, die Sie für die Richtlinie verwenden

möchten. Geben Sie dann den **Richtliniennamen** und die **Beschreibung** ein. Klicken Sie auf **Weiter**.

**Add Service Policy Rule Wizard - Service Policy**

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

**Interface:** outside - (create new service policy) ▾

Policy Name: outside-policy

Description: Policy on outside interface

**Global - applies to all interfaces**

Policy Name: global-policy

Description:

< Back **Next >** Cancel Help

- Erstellen Sie eine neue Klassenzuordnung, die dem **TCP**-Datenverkehr entspricht, wenn **HTTP** unter TCP fällt. Klicken Sie auf **Weiter**.

**Add Service Policy Rule Wizard - Traffic Classification Criteria**

Create a new traffic 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

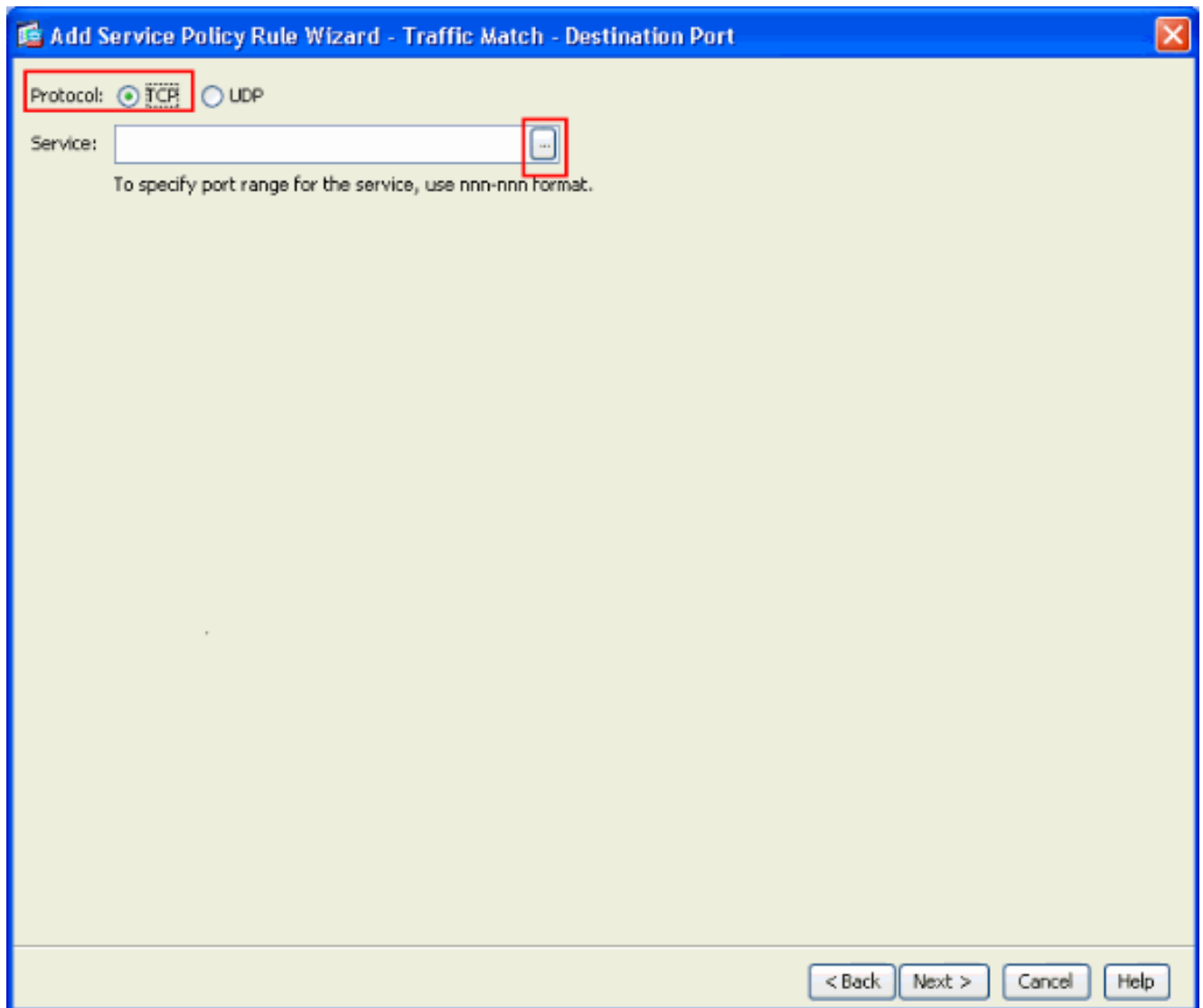
Use an existing traffic class:

Use class-default as the traffic class.

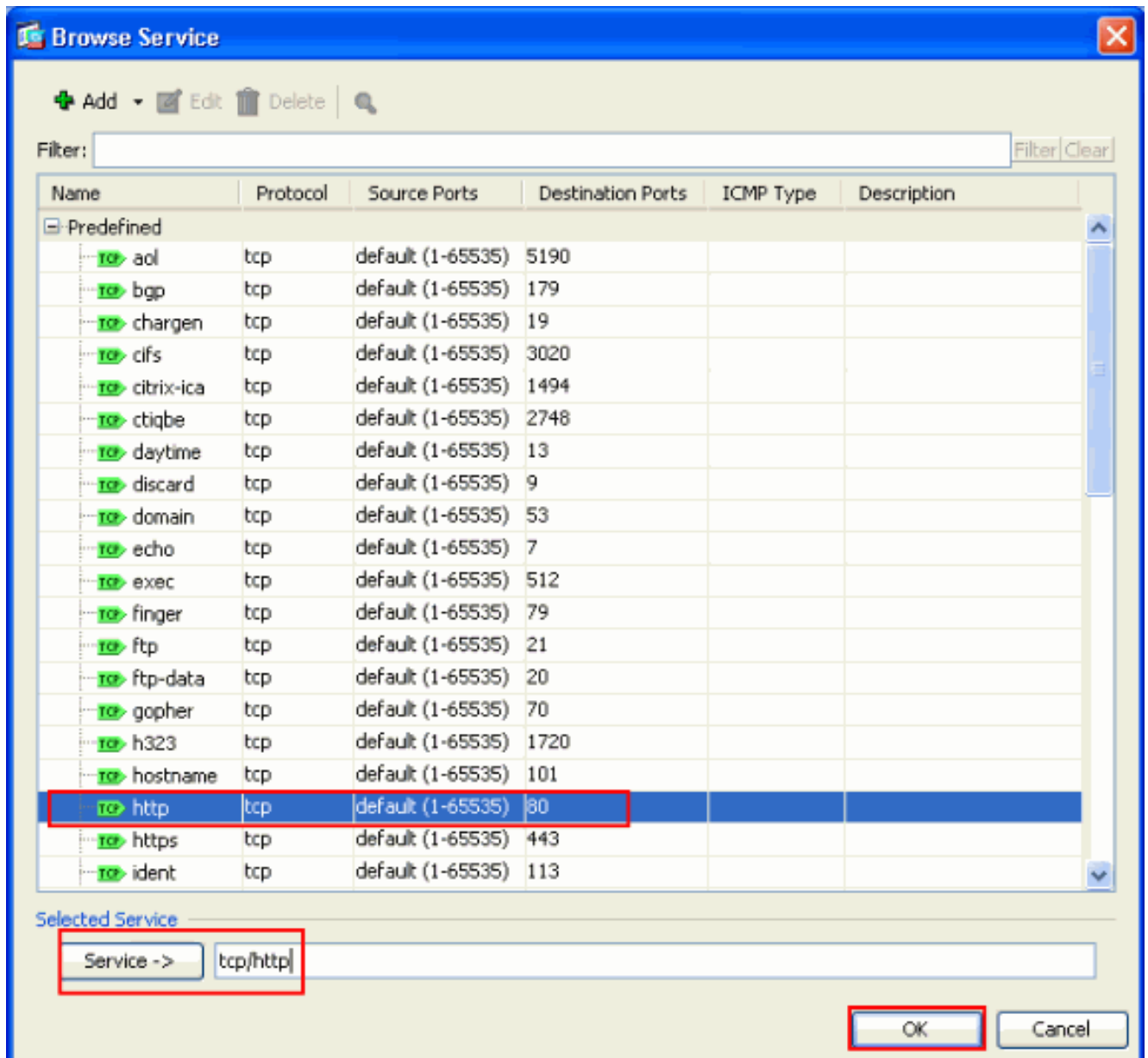
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

< Back **Next >** Cancel Help

6. Wählen Sie **TCP** als Protokoll aus.

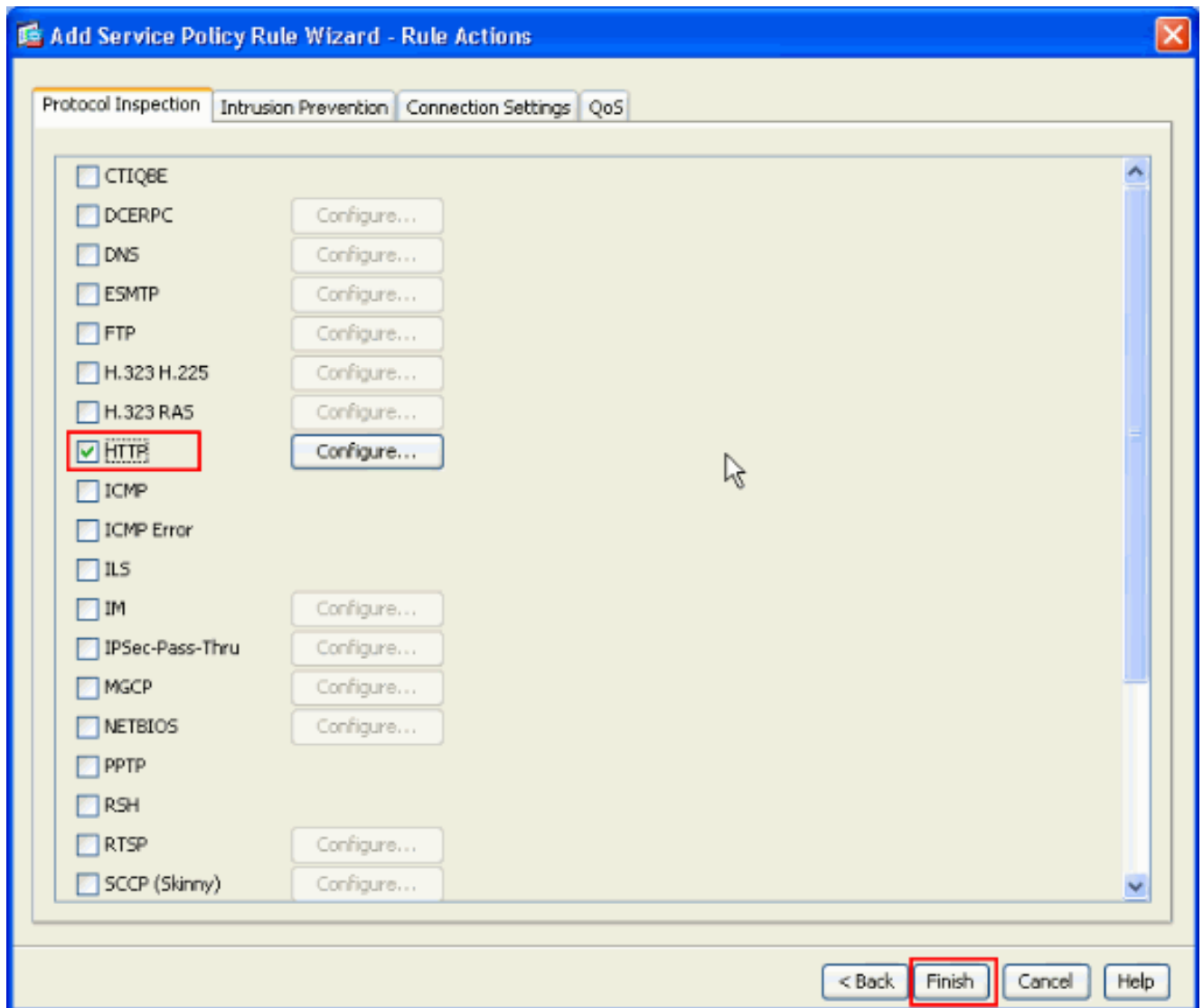


Wählen Sie **HTTP-Port 80** als Service aus, und klicken Sie auf **OK**.

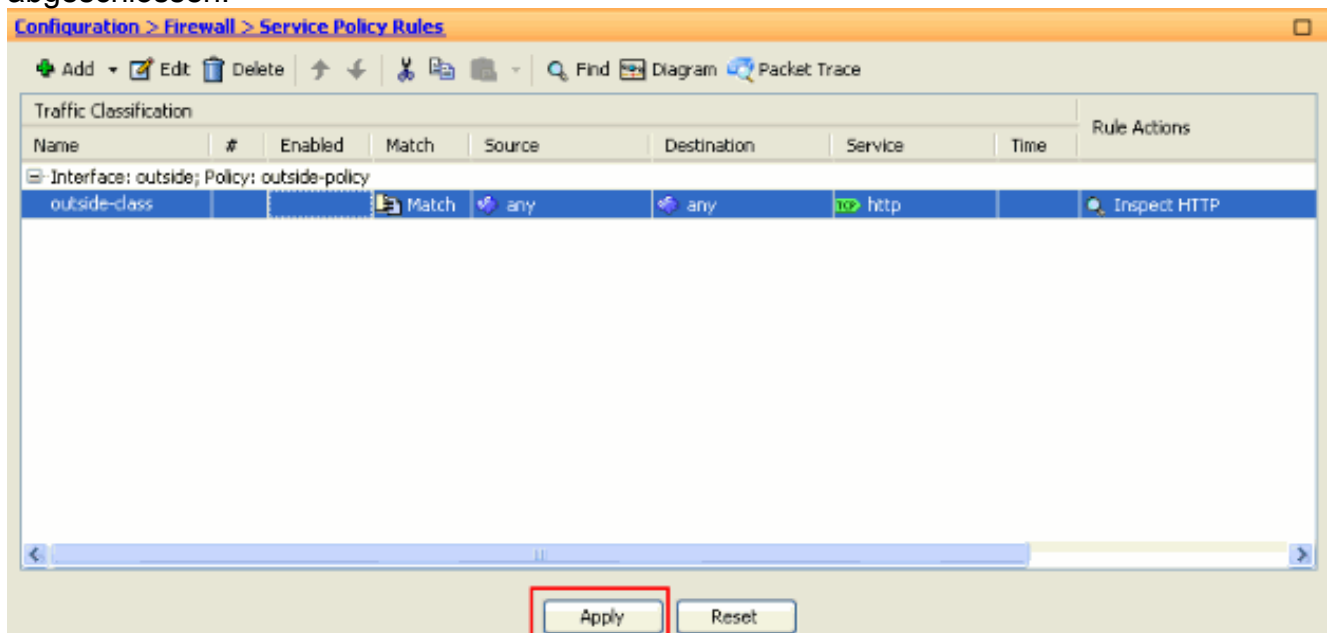


7. Wählen Sie **HTTP** aus, und klicken Sie auf **Fertig stellen**.





8. Klicken Sie auf **Apply**, um diese Konfigurationsänderungen vom ASDM an die ASA zu senden. Damit ist die Konfiguration abgeschlossen.



Überprüfen

Verwenden Sie die folgenden **show**-Befehle, um die Konfiguration zu überprüfen:

- Verwenden Sie den Befehl **show run class-map**, um die konfigurierten Klassenzuordnungen anzuzeigen.

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

- Verwenden Sie den Befehl **show run policy-map**, um die konfigurierten Richtlinienzuordnungen anzuzeigen.

```
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  
!
```

- Verwenden Sie den Befehl **show run service-policy**, um die konfigurierten Service-Richtlinien anzuzeigen.

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

## [Zugehörige Informationen](#)

- [Cisco Adaptive Security Appliances der Serie ASA 5500](#)
- [Cisco Serie ASA 5500 - Befehlsreferenzen](#)
- [Support-Seite für Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Cisco PIX Firewall-Software](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Cisco Security Appliances der Serie PIX 500](#)
- [Anwenden der Protokollüberprüfung auf Anwendungsebene](#)
- [Cisco Secure PIX Firewall - Befehlsreferenzen](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)