ASA 8.3 und höher - Konfigurieren der Inspektion mithilfe von ASDM

Inhalt

Einleitung

Dieses Dokument enthält eine Beispielkonfiguration für die Cisco Adaptive Security Appliance (ASA) mit Version 8.3(1) und höher, in der erläutert wird, wie die Standardprüfung für eine Anwendung aus der globalen Richtlinie entfernt wird und wie die Überprüfung für eine nicht standardmäßige Anwendung mithilfe des Adaptive Security Device Manager (ASDM) aktiviert wird.

Weitere Informationen finden Sie unter PIX/ASA 7.X: Deaktivieren Sie die globale Standardinspektion, und aktivieren Sie für dieselbe Konfiguration auf der Cisco ASA mit Version 8.2 oder früher die Nicht-Standard-Anwendungsinspektion.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA Security Appliance Software Version 8.3(1) mit ASDM 6.3.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

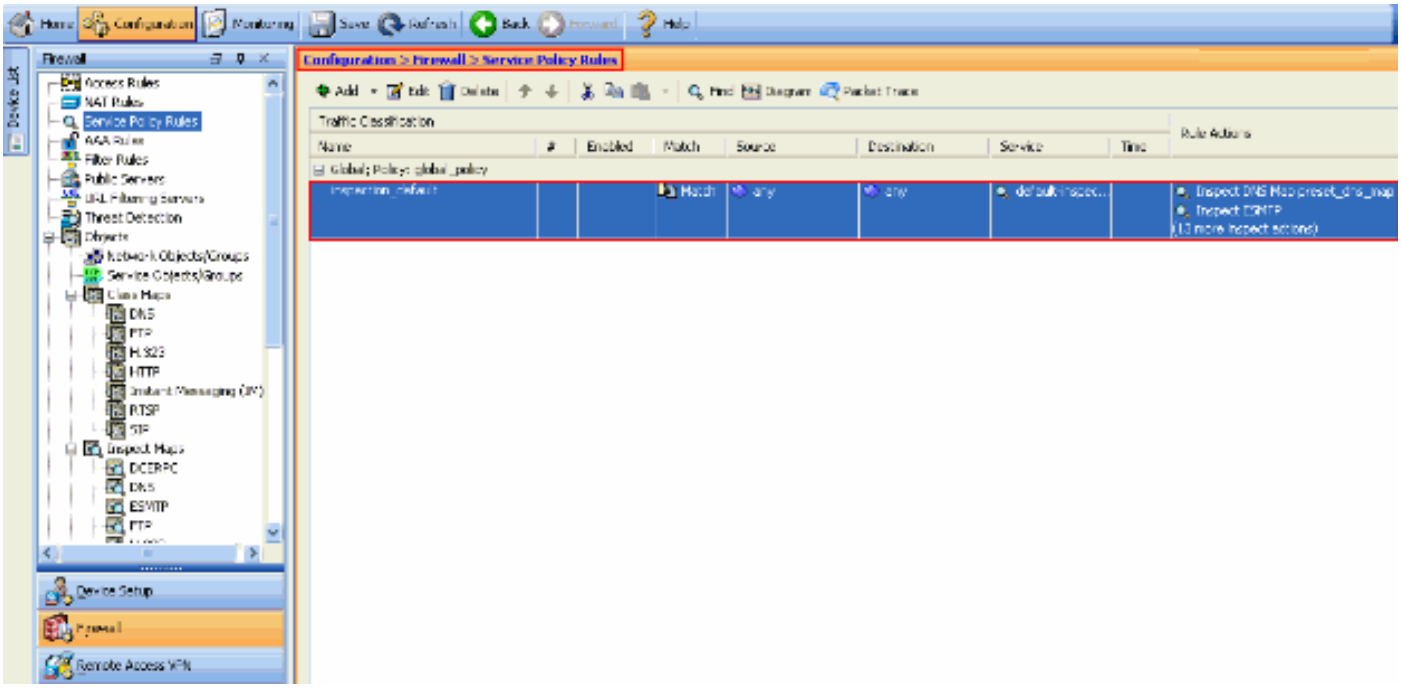
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den 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.)

Wählen Sie im ASDM **Configuration > Firewall > Service Policy Rules** (Konfiguration > Firewall > Service-Richtlinienregeln) aus, um die globale Standardrichtlinie anzuzeigen, deren Standardanwendungsinspektion wie folgt lautet:

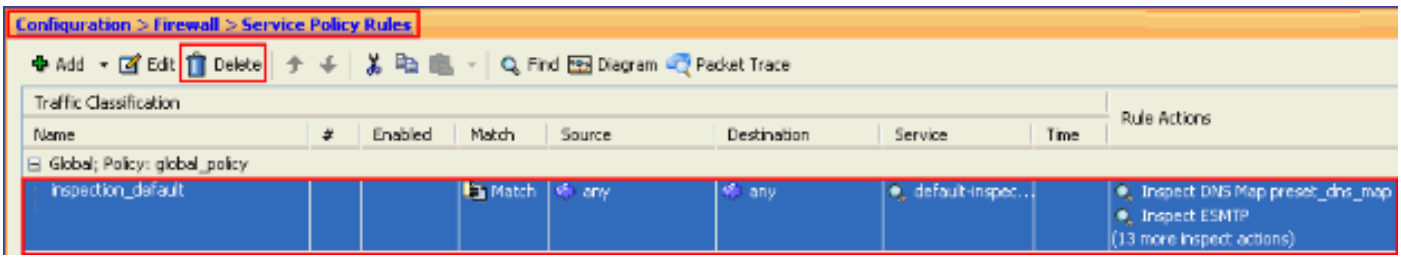


Die Standardrichtlinienkonfiguration umfasst die folgenden Befehle:

```
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
```

Wenn Sie die globale Richtlinie deaktivieren müssen, verwenden Sie den globalen Befehl **no service-policy global_policy**. Um die globale Richtlinie mithilfe von ASDM zu löschen, wählen Sie **Configuration > Firewall > Service Policy Rules aus**. Wählen Sie anschließend die globale Richtlinie aus, und klicken Sie auf **Löschen**.



Hinweis: Wenn Sie die Service-Richtlinie mit ASDM löschen, werden die zugehörigen Richtlinien- und Klassenzuordnungen gelöscht. Wenn die Dienstrichtlinie jedoch mithilfe der CLI gelöscht wird, wird nur die Dienstrichtlinie von der Schnittstelle entfernt. Die Klassenzuordnung und Richtlinienzuordnung bleiben unverändert.

Deaktivieren der globalen Standardüberprüfung für eine Anwendung

Um die globale Überprüfung für eine Anwendung zu deaktivieren, verwenden Sie die *no*-Version des Befehls **inspect**.

Um z. B. die globale Überprüfung für die FTP-Anwendung zu entfernen, an die die Sicherheits-Appliance überwacht, verwenden Sie den Befehl **no inspect ftp** im Klassenkonfigurationsmodus.

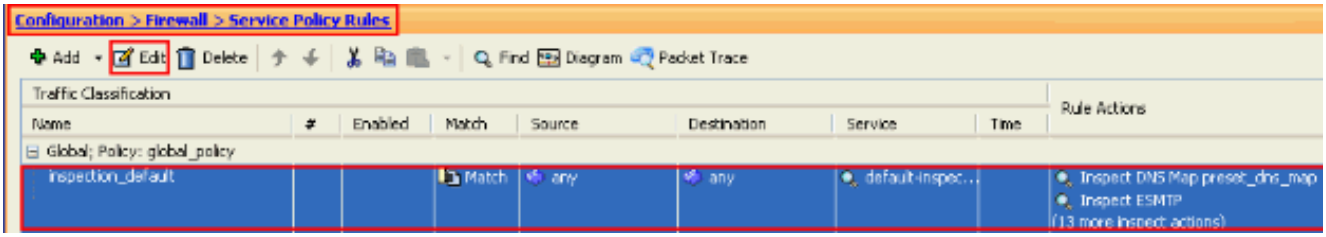
Der Klassenkonfigurationsmodus kann über den Konfigurationsmodus für die Richtlinienzuordnung aufgerufen werden. Um die Konfiguration zu entfernen, verwenden Sie die *no*-Form des Befehls.

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

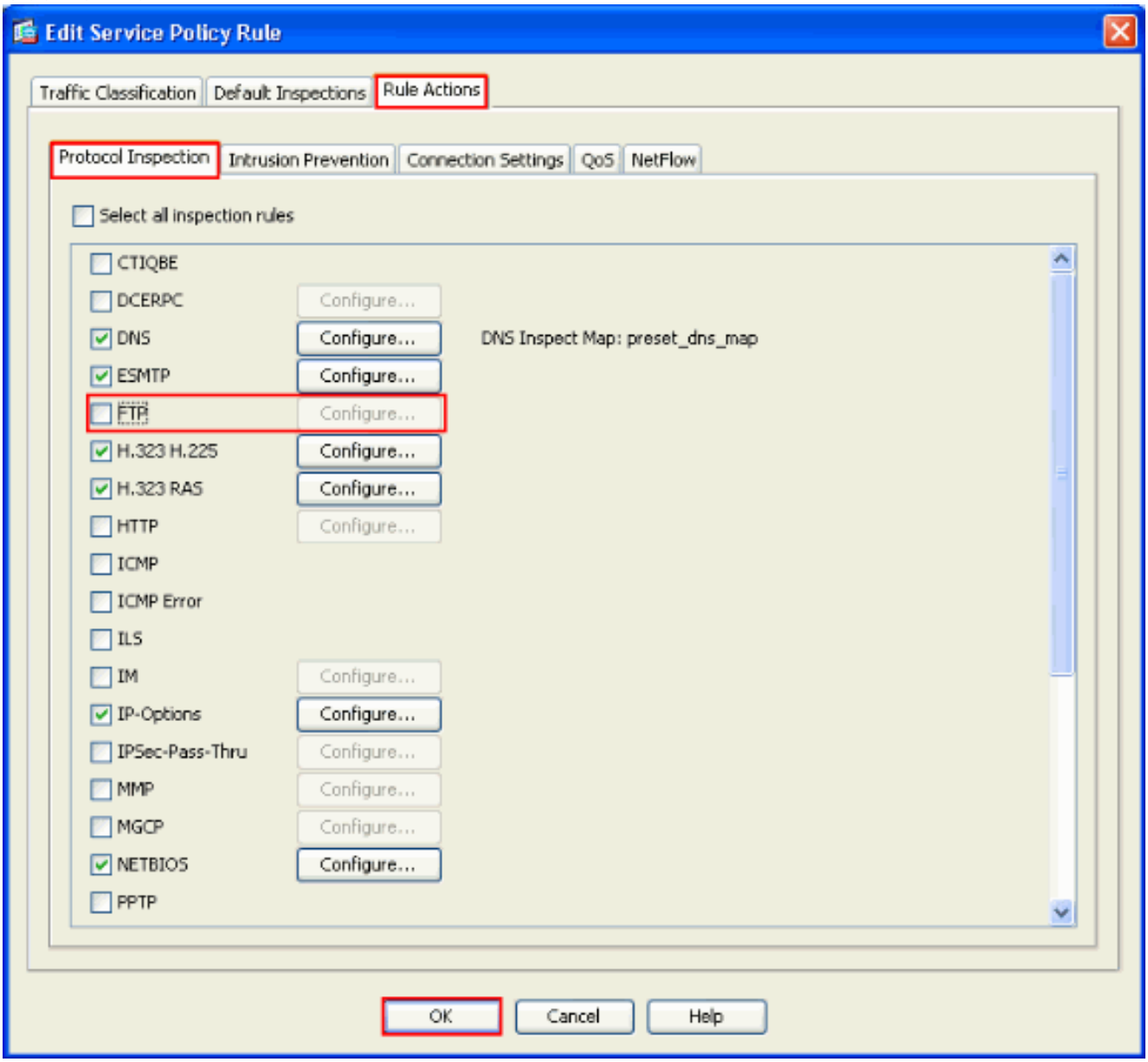
Gehen Sie wie folgt vor, um die globale Überprüfung für FTP mithilfe von ASDM zu deaktivieren:

Hinweis: Unter Zulassen von HTTPS-Zugriff für ASDM finden Sie grundlegende Einstellungen, um über ASDM auf PIX/ASA zuzugreifen.

1. Wählen Sie **Konfiguration > Firewall > Service Policy Rules** (Regeln für **Service-Richtlinien**) aus, und wählen Sie die globale Standardrichtlinie aus. Klicken Sie dann auf **Bearbeiten**, um die globale Überprüfungsrichtlinie zu bearbeiten.



2. Wählen Sie im Fenster "Edit Service Policy Rule" (Servicerichtlinienregel bearbeiten) auf der Registerkarte **Rule Actions (Regelaktionen)** die Option **Protocol Inspection (Protokollüberprüfung)** aus. Stellen Sie sicher, dass das Kontrollkästchen **FTP** deaktiviert ist. Dadurch wird die FTP-Prüfung wie im nächsten Bild gezeigt deaktiviert. Klicken Sie dann auf **OK** und dann auf **Übernehmen**.



Hinweis: Weitere Informationen zur FTP-Prüfung finden Sie unter PIX/ASA 7.x: Aktivieren des Konfigurationsbeispiels für FTP-/TFTP-Dienste.

Überprüfung für nicht standardmäßige Anwendung aktivieren

Die erweiterte HTTP-Überprüfung ist standardmäßig deaktiviert. Um die HTTP-Überprüfung in global_policy zu aktivieren, verwenden Sie den Befehl **inspect http** unter class inspect_default.

In diesem Beispiel wird jede HTTP-Verbindung (TCP-Datenverkehr an Port 80), die über eine beliebige Schnittstelle in die Sicherheits-Appliance gelangt, für die HTTP-Prüfung klassifiziert. *Da es sich bei der Richtlinie um eine globale Richtlinie handelt, erfolgt die Überprüfung nur, wenn der Datenverkehr in die einzelnen Schnittstellen eingeht*.

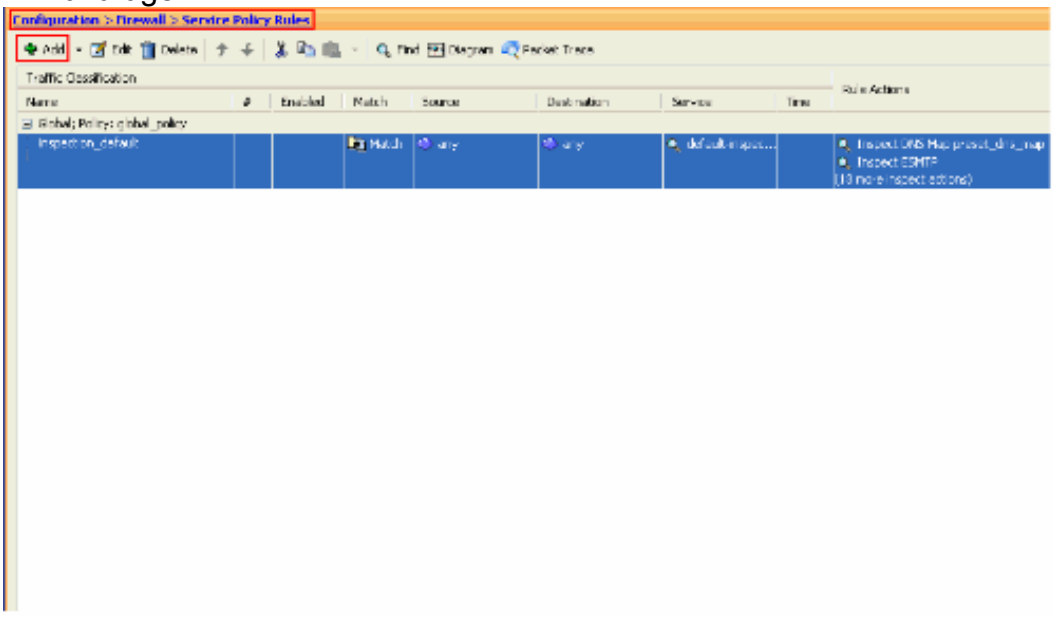
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

In diesem Beispiel *wird* jede HTTP-Verbindung (TCP-Datenverkehr an Port 80), die über die *externe Schnittstelle* in die Sicherheits-Appliance eingeht oder diese verlässt, *für die HTTP-Überprüfung klassifiziert*.

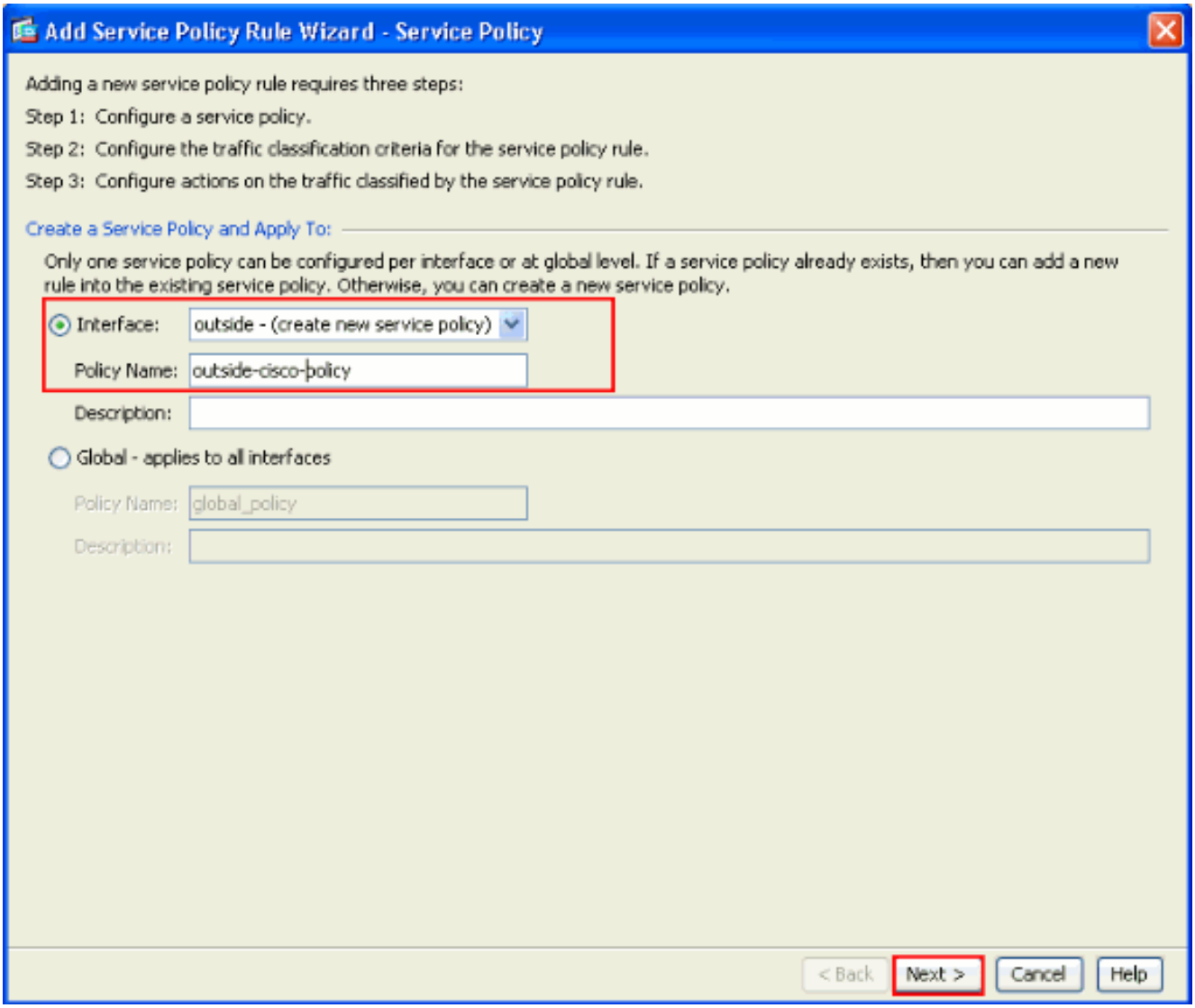
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Führen Sie die folgenden Schritte aus, um das obige Beispiel mithilfe von ASDM zu konfigurieren:

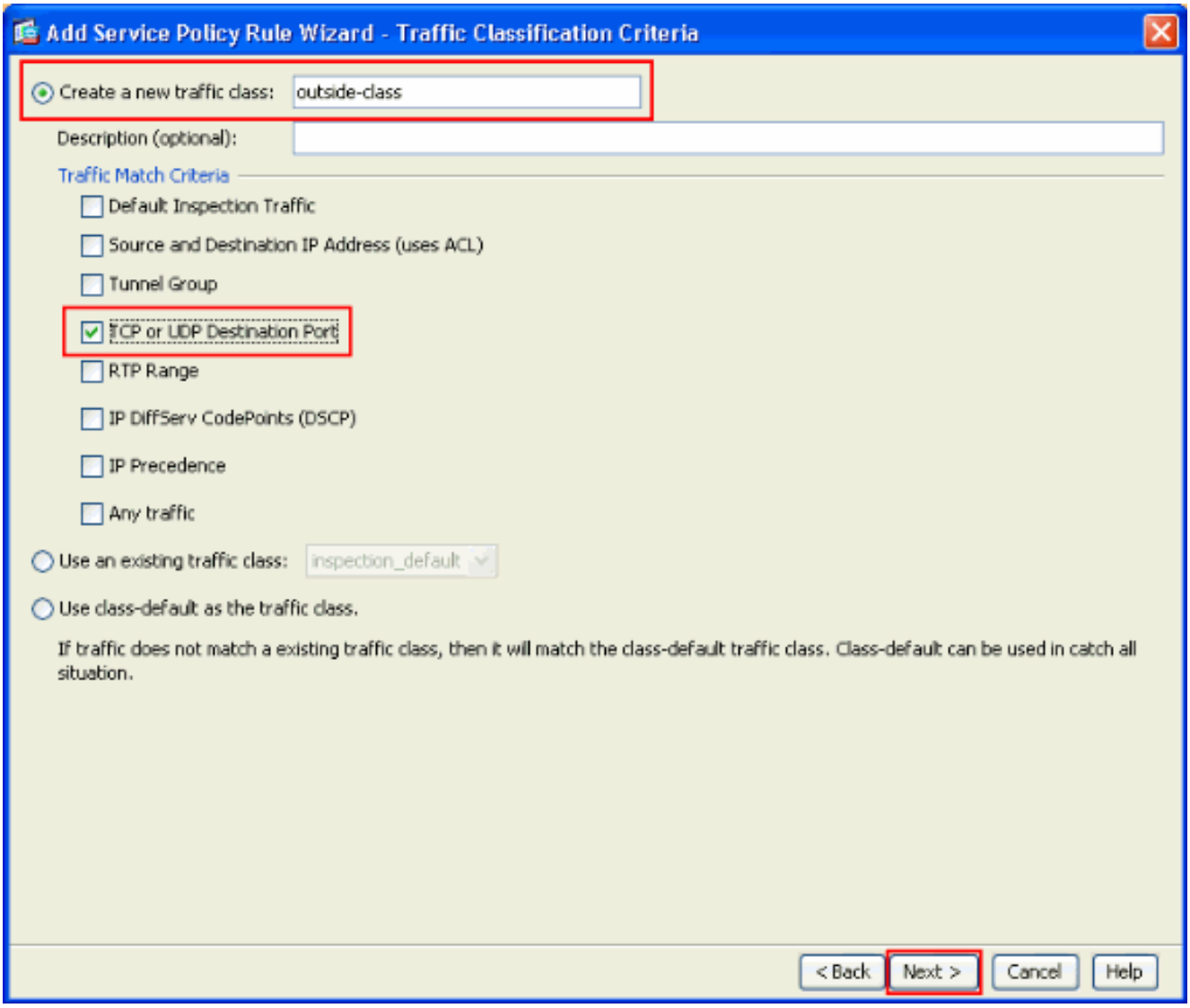
1. Wählen Sie **Konfiguration > Firewall > Service Policy Rules** und klicken Sie auf **Add**, um eine neue Service-Richtlinie hinzuzufügen:



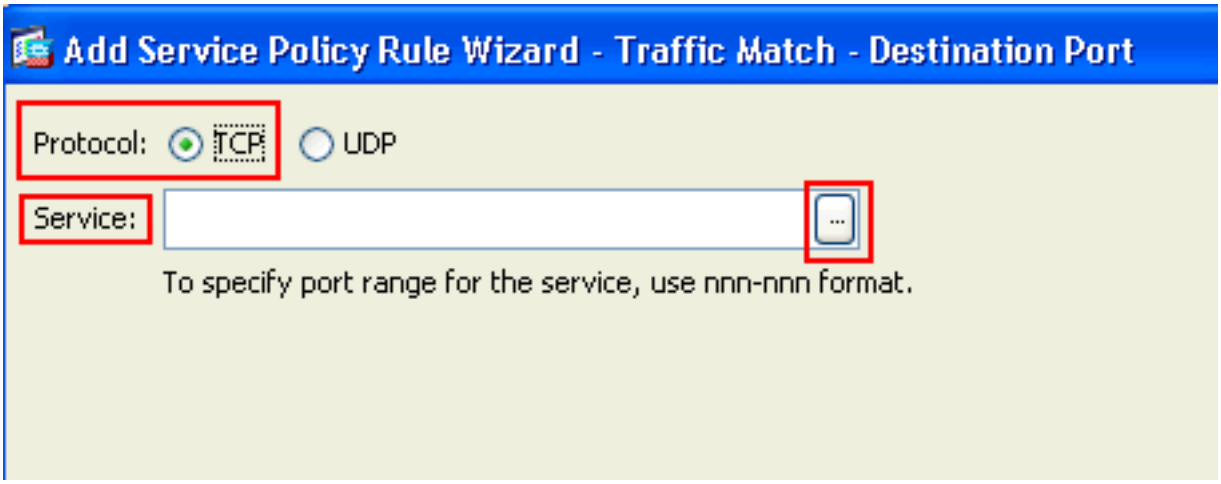
2. Wählen Sie im Fenster Assistent für die Hinzufügen von Service-Richtlinienregeln - Servicerichtlinie das Optionsfeld neben **Schnittstelle aus**. Damit wird die Richtlinie auf eine bestimmte Schnittstelle angewendet, die in diesem Beispiel die **externe** Schnittstelle ist. Geben Sie einen Richtliniennamen ein, der in diesem Beispiel **außerhalb von cisco-policy** liegt. Klicken Sie auf **Weiter**.



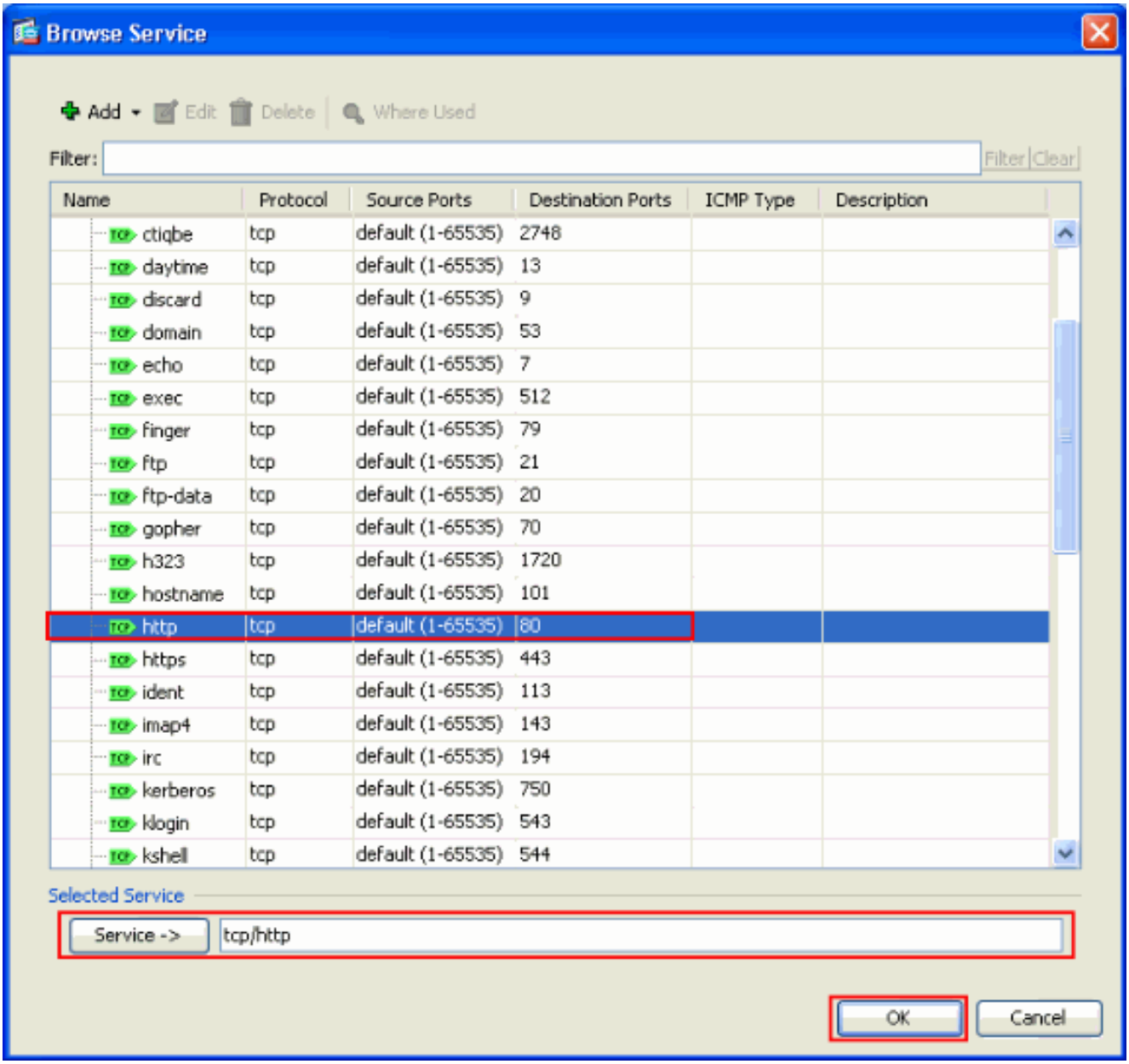
3. Geben Sie im Fenster Add Service Policy Rule Wizard - Traffic Classification Criteria (Hinzufügen von Service-Richtlinienregeln - Klassifizierungskriterien) den neuen Namen der Verkehrsklasse an. Der in diesem Beispiel verwendete Name ist **Fremdklasse**. Stellen Sie sicher, dass das Kontrollkästchen neben **TCP- oder UDP-Zielport** aktiviert ist, und klicken Sie auf
Weiter.



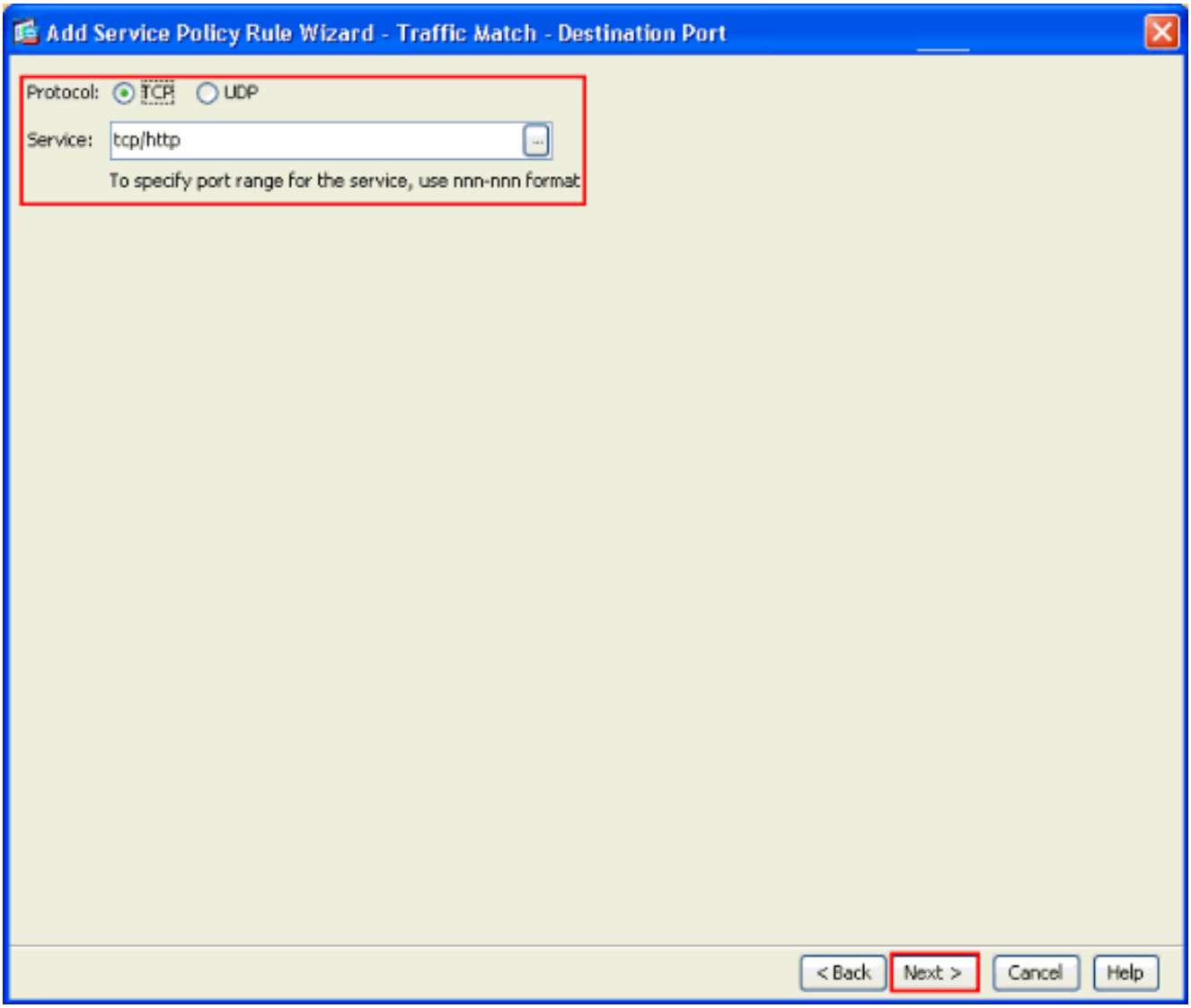
4. Wählen Sie im Abschnitt "**Protokoll**" im Fenster "Assistent für die Richtlinie zum Hinzufügen von Services - Datenverkehrszuordnung - Ziel-Port" das Optionsfeld neben **TCP** aus. Klicken Sie dann auf die Schaltfläche neben **Service**, um den gewünschten Service auszuwählen.



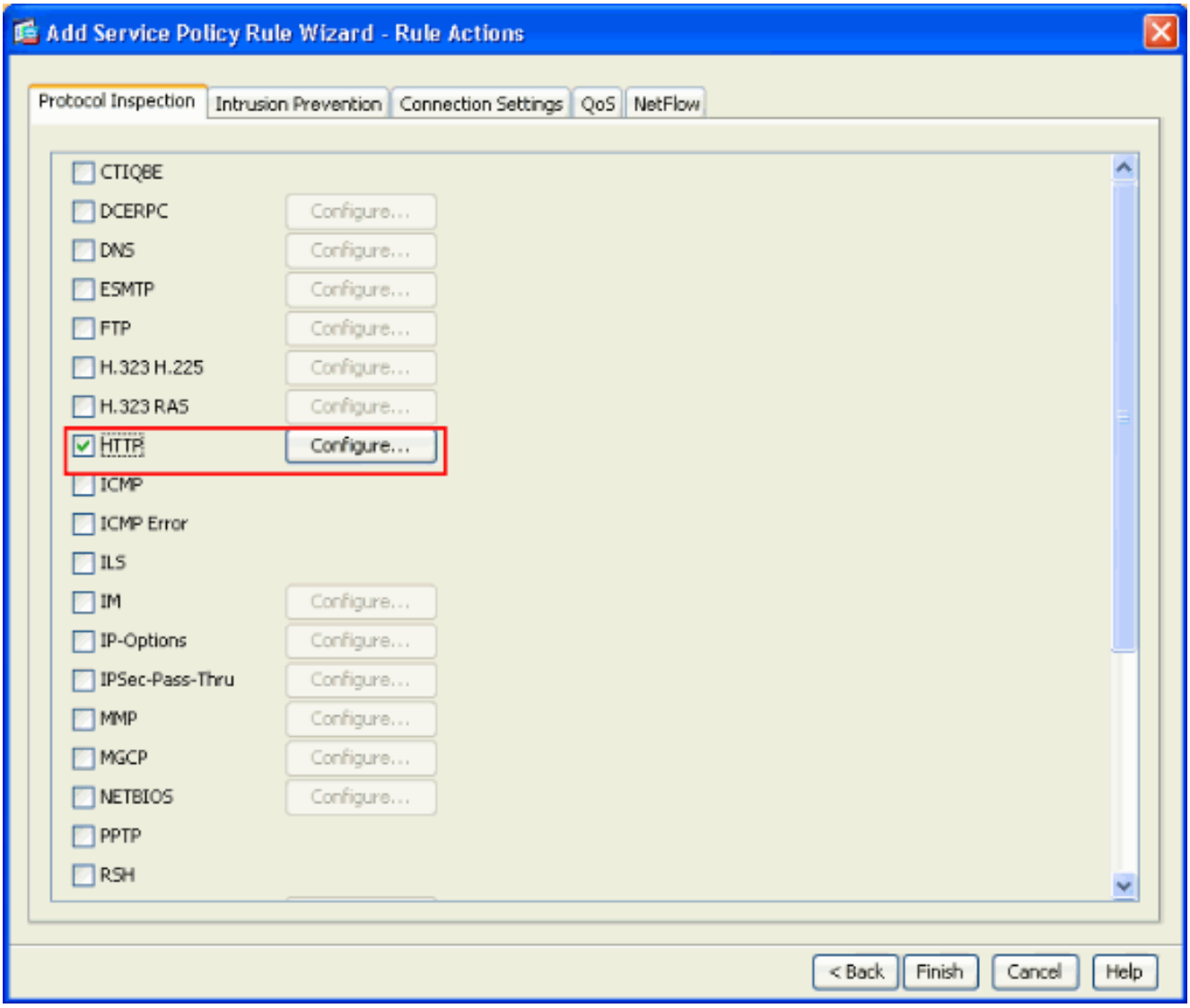
5. Wählen Sie im Fenster Service durchsuchen die Option **HTTP** als Service aus. Klicken Sie anschließend auf
OK.



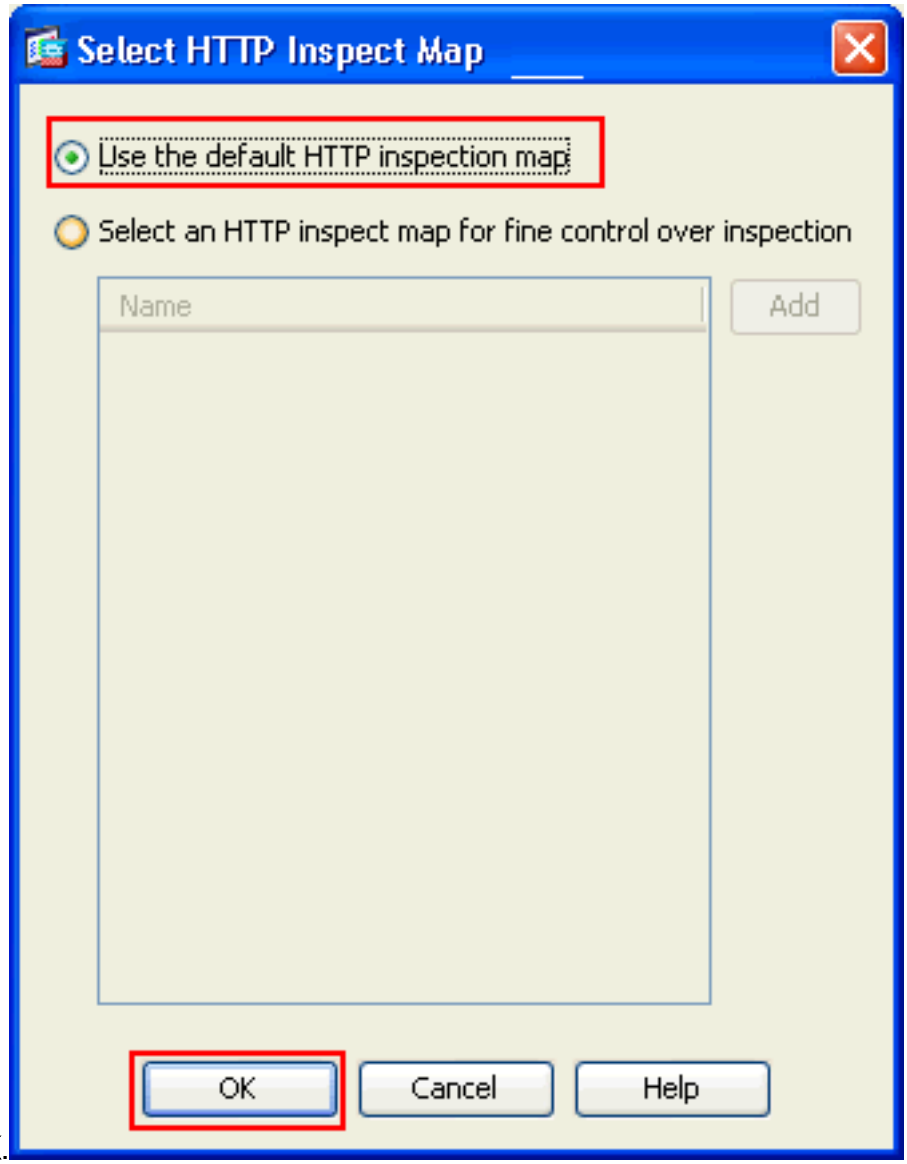
6. Im Fenster Assistent für die Richtlinie für das Hinzufügen von Services - Datenverkehrszuordnung - Zielport können Sie sehen, dass der ausgewählte **Service tcp/http** lautet. Klicken Sie auf **Weiter**.



7. Aktivieren Sie im Fenster Assistent für das Hinzufügen von Service-Richtlinien - Regelaktionen das Kontrollkästchen neben **HTTP**. Klicken Sie dann neben **HTTP** auf **Konfigurieren**.

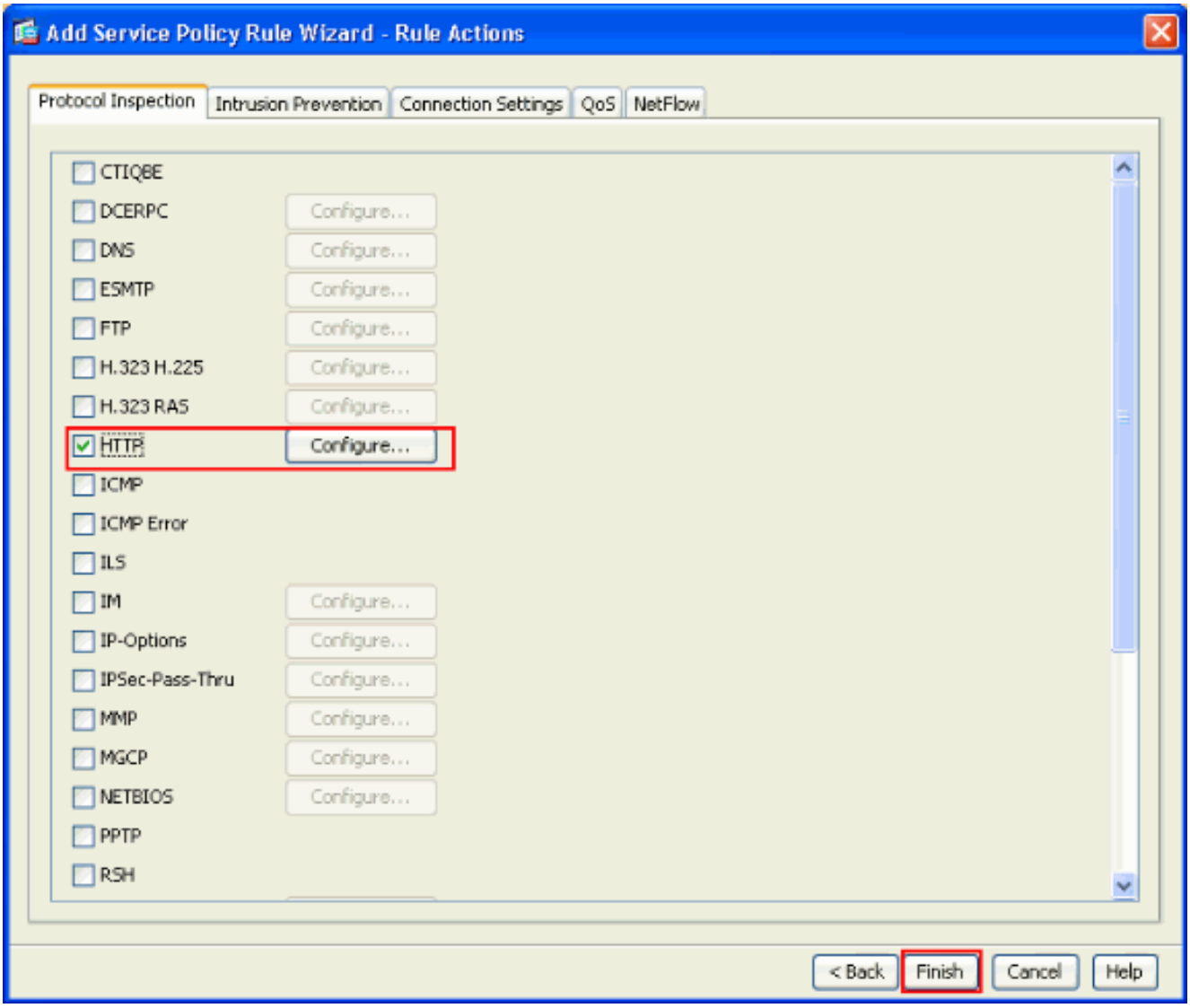


8. Aktivieren Sie im Fenster Select HTTP Inspect Map (HTTP-Inspektionszuordnung auswählen) das Optionsfeld neben **Use the Default HTTP Inspection Map (Standard-HTTP-Inspektionszuordnung verwenden)**. In diesem Beispiel wird die HTTP-Standardprüfung verwendet. Klicken Sie anschließend auf

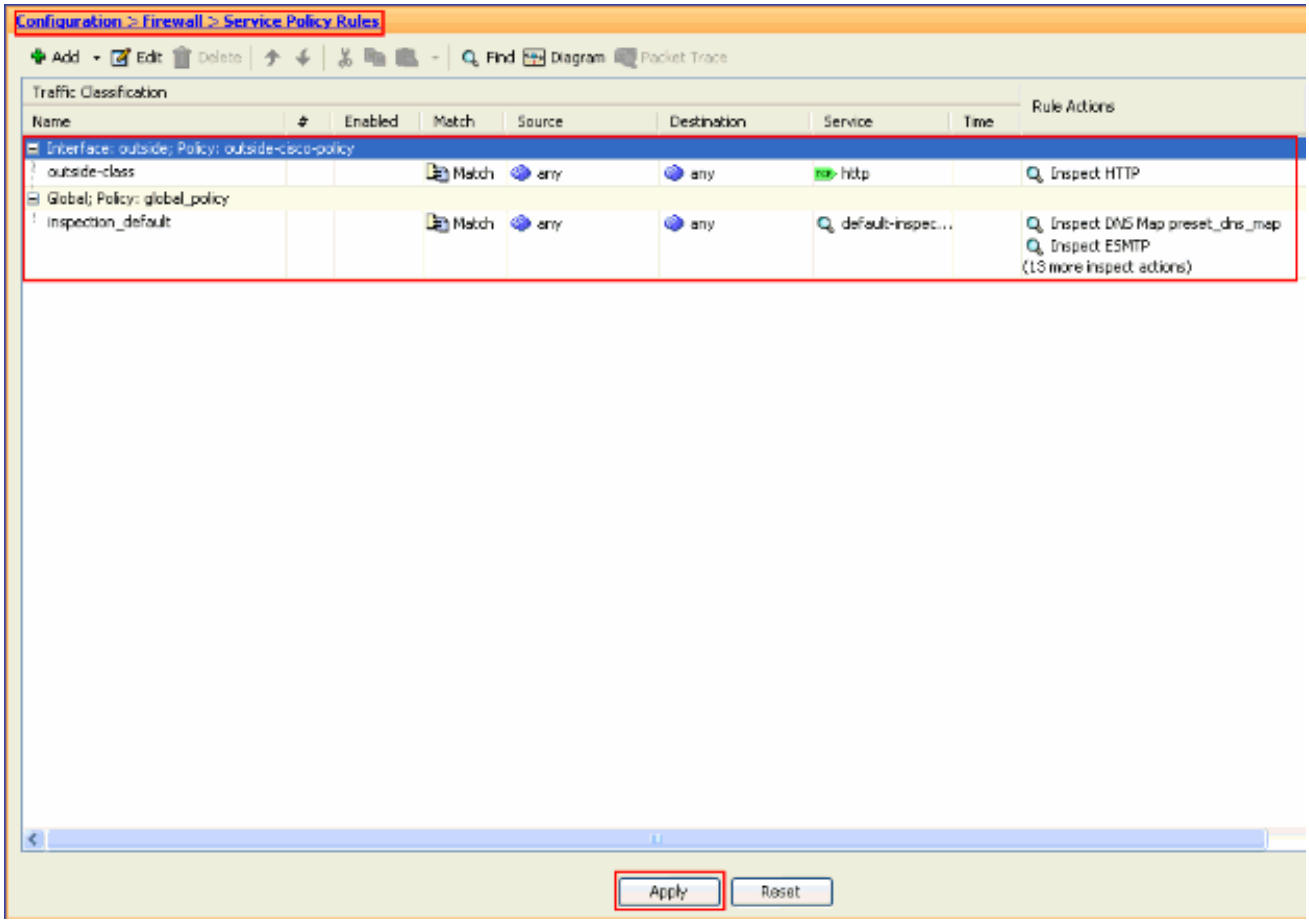


OK.

9. Klicken Sie auf **Fertig stellen**.



10. Unter **Configuration > Firewall > Service Policy Rules** (Konfiguration > Firewall > Service-Richtlinienregeln) sehen Sie die neu konfigurierte Service-Richtlinie **außerhalb von Cisco** (zum Überprüfen von HTTP) zusammen mit der auf der Appliance bereits vorhandenen Standard-Service-Richtlinie. Klicken Sie auf **Apply**, um die Konfiguration auf die Cisco ASA anzuwenden.



Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco Adaptive Security Device Manager
- Anforderungen für Kommentare (RFCs)
- Anwenden der Protokollüberprüfung auf Anwendungsebene
- Technischer Support und Dokumentation für Cisco Systeme