ASA 8.3 en hoger - Inspectie configureren met ASDM

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor Cisco adaptieve security applicatie (ASA) met versies 8.3(1) en hoger hoe de standaardinspectie van mondiaal beleid voor een toepassing kan worden verwijderd en hoe de inspectie voor een niet-standaard toepassing kan worden uitgevoerd met behulp van Adaptieve Security Devices Manager (ASDM).

Raadpleeg PIX/ASA 7.X: Standaard wereldwijde inspectie uitschakelen en niet-standaard toepassingsinspectie inschakelen voor dezelfde configuratie op Cisco ASA met versies 8.2 en eerder.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA security applicatie versie 8.3(1) met ASDM 6.3.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

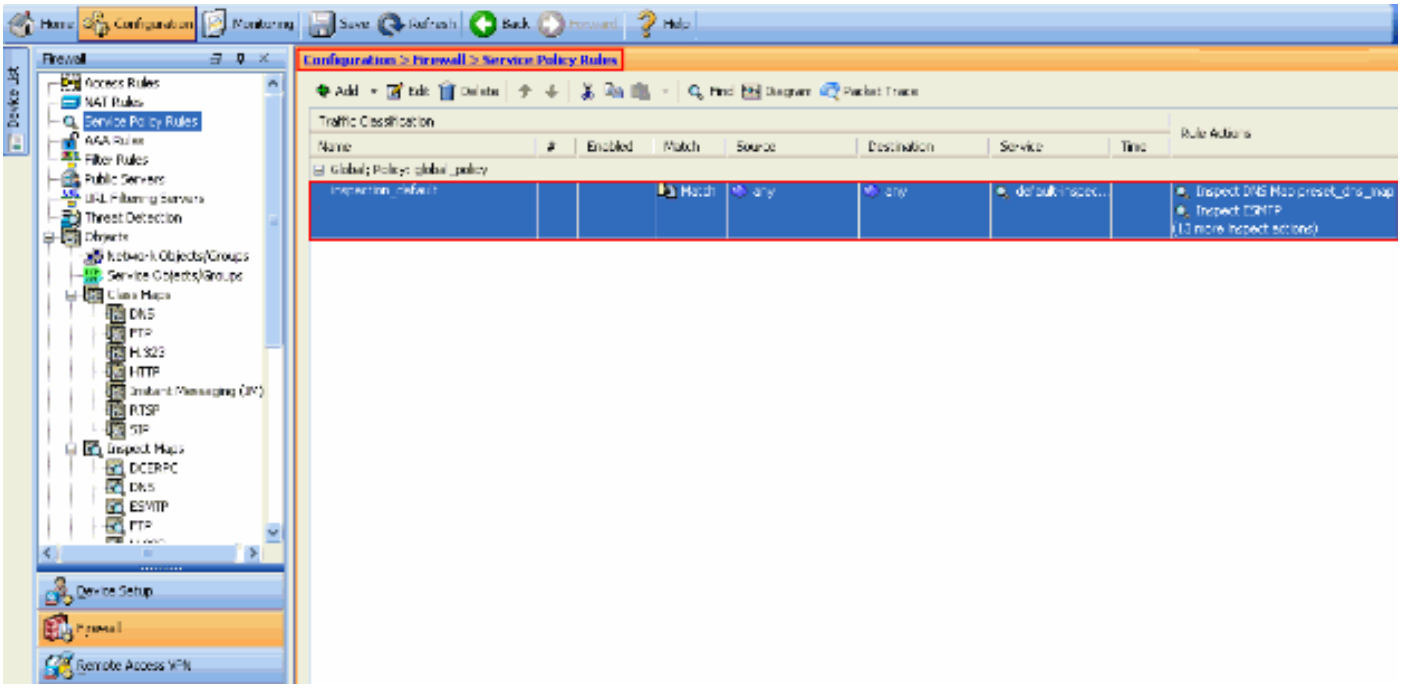
Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Standaard mondiaal beleid

Standaard omvat de configuratie een beleid dat overeenkomt met al het standaard toepassingsinspectieverkeer en past de configuratie bepaalde inspecties op alle interfaces toe (een mondiaal beleid). Niet alle inspecties zijn standaard ingeschakeld. Je kunt maar één mondiaal beleid toepassen. Als u het algemene beleid wilt wijzigen, moet u het standaardbeleid bewerken of uitschakelen en een nieuw beleid toepassen. (Een interfacebeleid heeft voorrang op het mondiale beleid.)

In ASDM, kies **Configuration > Firewall > Service Policy Regels** om het standaard wereldwijde beleid te bekijken dat de standaard toepassingsinspectie heeft zoals hieronder wordt getoond:

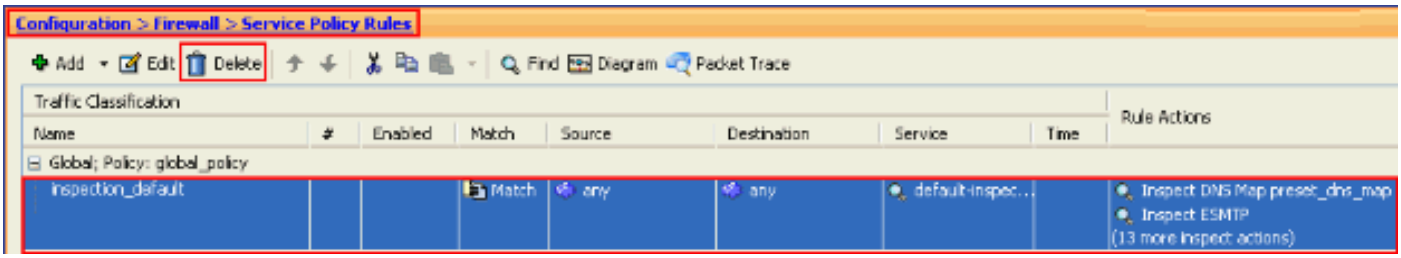


De standaard beleidsconfiguratie bevat deze opdrachten:

```
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
```

Als je het globale beleid moet uitschakelen gebruik de **geen service-beleid global_policy** opdracht. Als u het wereldwijde beleid wilt verwijderen met ASDM, kiest u **Configuration > Firewall > Service Policy Regels**. Selecteer vervolgens het algemene beleid en klik op **Verwijderen**.



Opmerking: wanneer u het servicepakket met ASDM verwijdert, worden de bijbehorende beleidslijnen en klassenkaarten verwijderd. Als echter het servicebeleid met CLI is verwijderd, wordt alleen het servicebeleid uit de interface verwijderd. De klassenkaart en de beleidskaart blijven ongewijzigd.

Standaard wereldwijde inspectie voor een toepassing uitschakelen

Om mondiale inspectie voor een toepassing uit te schakelen, gebruikt u de *geen* versie van de **inspectie-**opdracht.

Om bijvoorbeeld de algemene inspectie voor de FTP-toepassing te verwijderen waarnaar het security apparaat luistert, gebruikt u de opdracht **no-inspect ftp** in klasse-configuratiemodus.

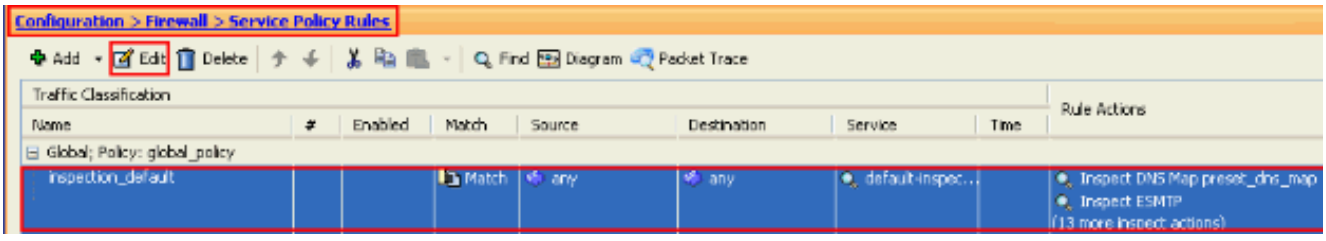
De configuratiemodus van de klasse is toegankelijk vanuit de configuratie van de beleidskaart. Gebruik de opdracht om de configuratie te verwijderen.

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

Voltooi de volgende stappen om wereldwijde inspectie voor FTP uit te schakelen met ASDM:

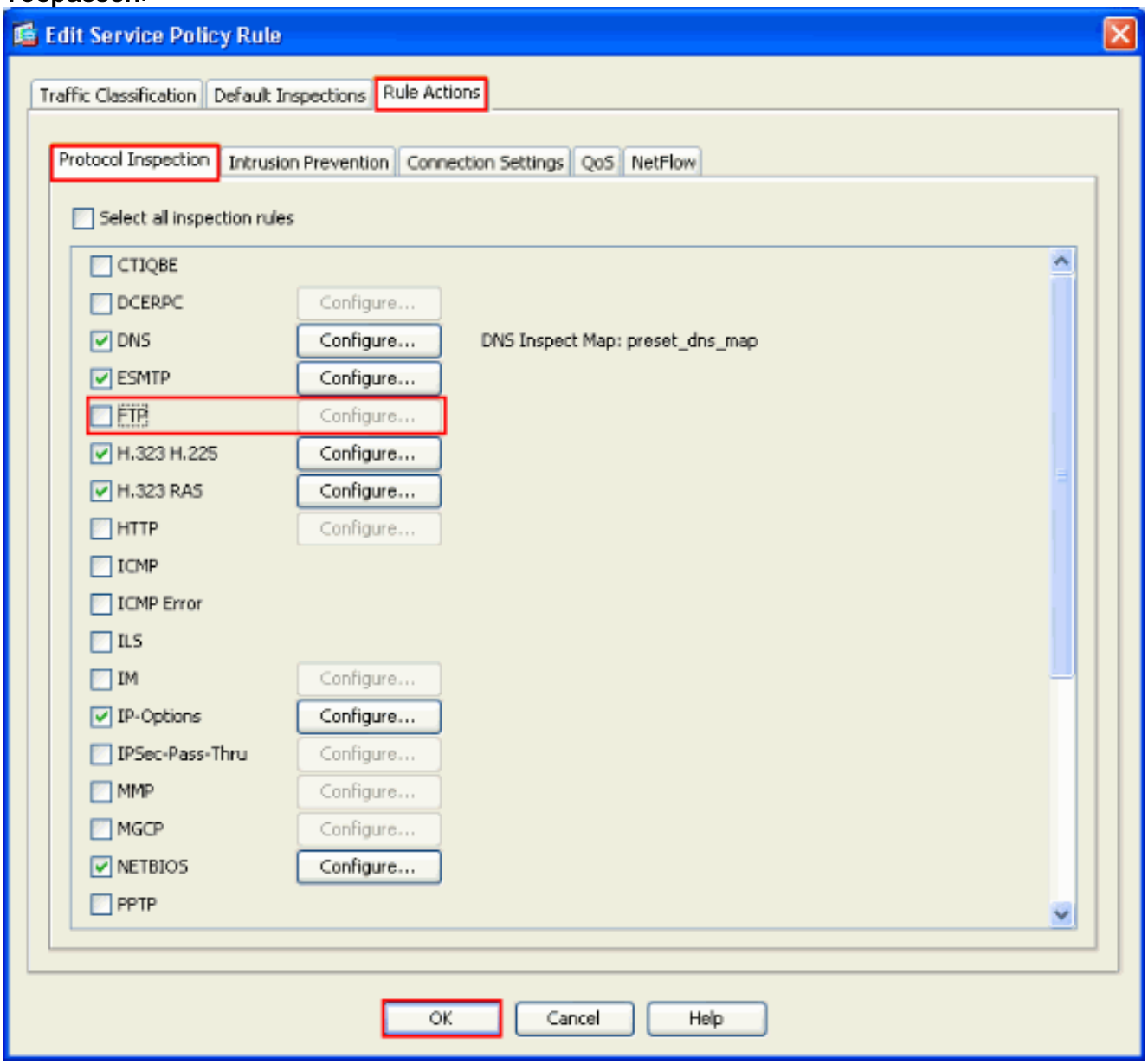
Opmerking: Raadpleeg HTTPS-toegang voor ASDM voor basisinstellingen om toegang te krijgen tot de PIX/ASA via ASDM.

1. Kies **Configuration > Firewall > Service Policy Regels** en selecteer de optie mondiaal standaardbeleid. Klik vervolgens op **Bewerken** om het algemene inspectiebeleid te bewerken.



2. Selecteer in het venster Service Policy Rule de optie **Protocol Inspectie** onder het tabblad **Regel**. Controleer of het vakje **FTP** is ingeschakeld. Hiermee wordt de FTP-inspectie

uitgeschakeld zoals in de volgende afbeelding wordt weergegeven. Klik vervolgens op **OK** en **Toepassen**.



Opmerking: Raadpleeg voor meer informatie over FTP-inspectie PIX/ASA 7.x: Configuratievoorbeeld FTP/TFTP-services inschakelen.

Inspectie inschakelen voor niet-standaard toepassing

Uitgebreide HTTP-inspectie is standaard uitgeschakeld. Om HTTP inspectie in global_policy mogelijk te maken, gebruik de opdracht **http** onder class inspection_default.

In dit voorbeeld wordt elke HTTP-verbinding (TCP-verkeer op poort 80) die het security apparaat via een interface ingaat, geclassificeerd voor HTTP-inspectie. *Omdat het beleid een mondiaal beleid is, komt de inspectie slechts voor als het verkeer elke interface ingaat.*

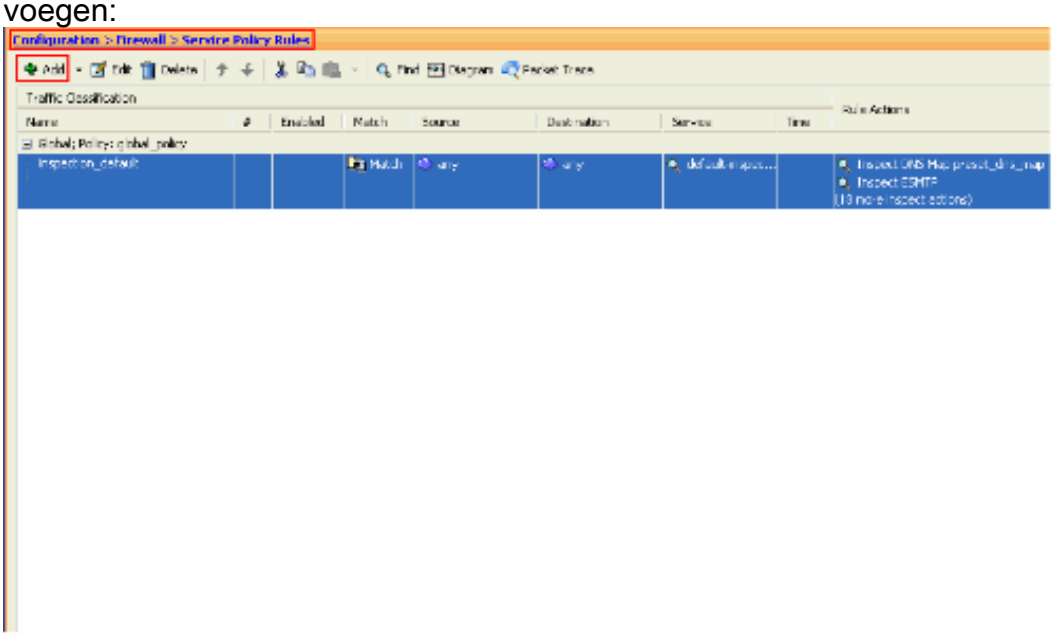
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

In dit voorbeeld *wordt* elke HTTP-verbinding (TCP-verkeer op poort 80) die het security apparaat binnenkomt of verlaat via de *externe interface geclassificeerd voor HTTP-inspectie*.

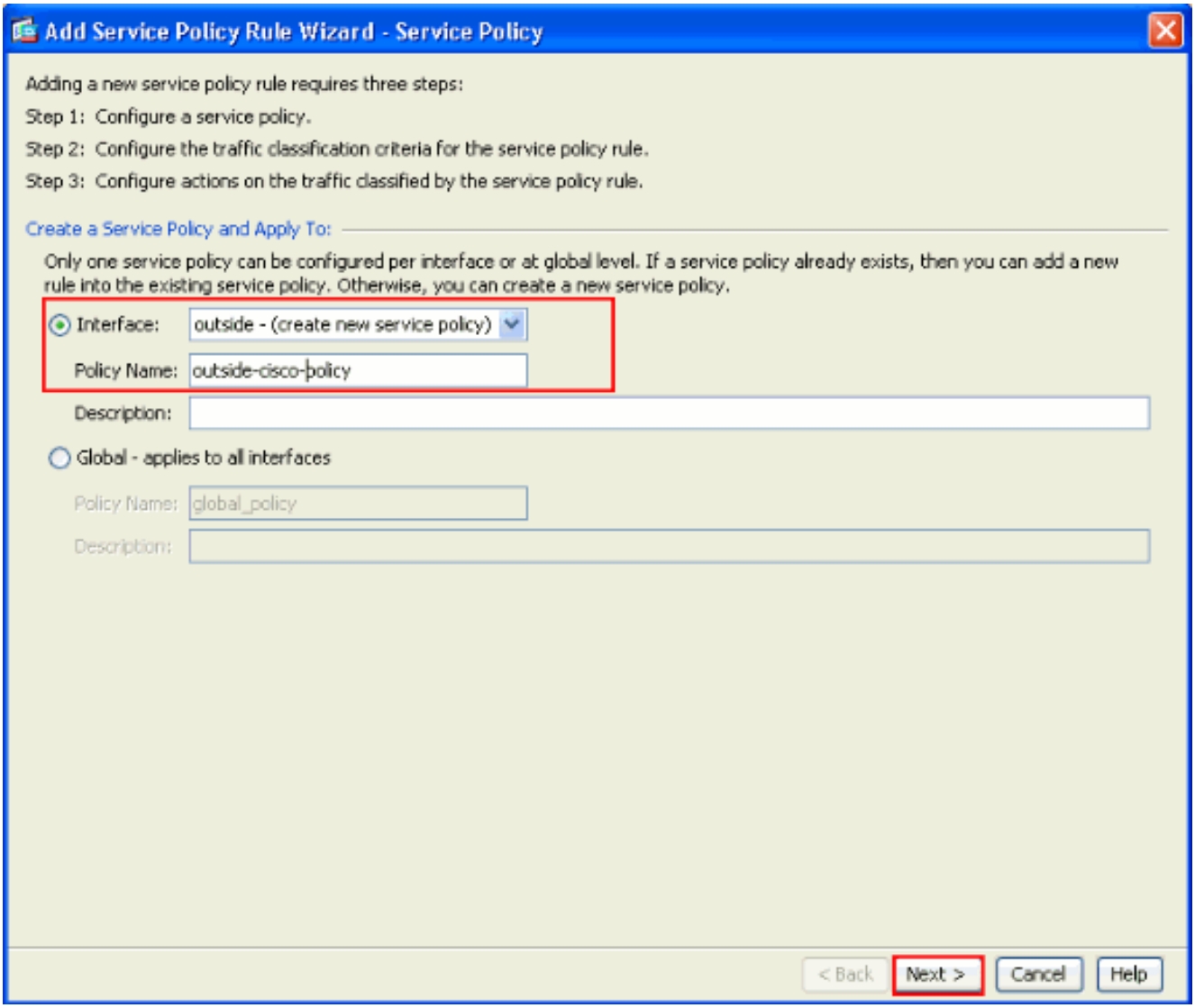
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Voer deze stappen uit om het bovenstaande voorbeeld te configureren via ASDM:

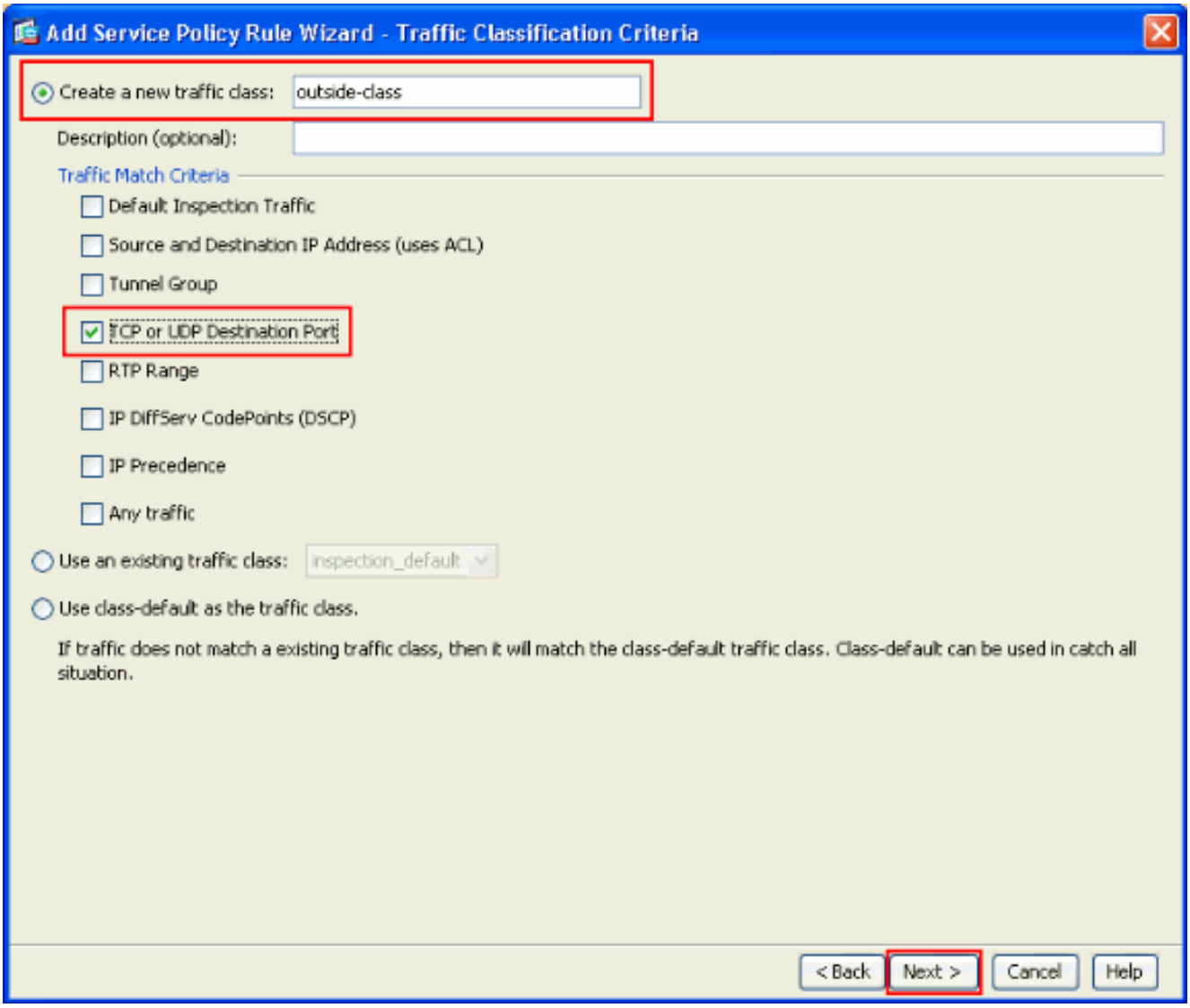
1. Kies **Configuration > Firewall > Service Policy Regels** en klik op **Add** om een nieuw servicebeleid toe te voegen:



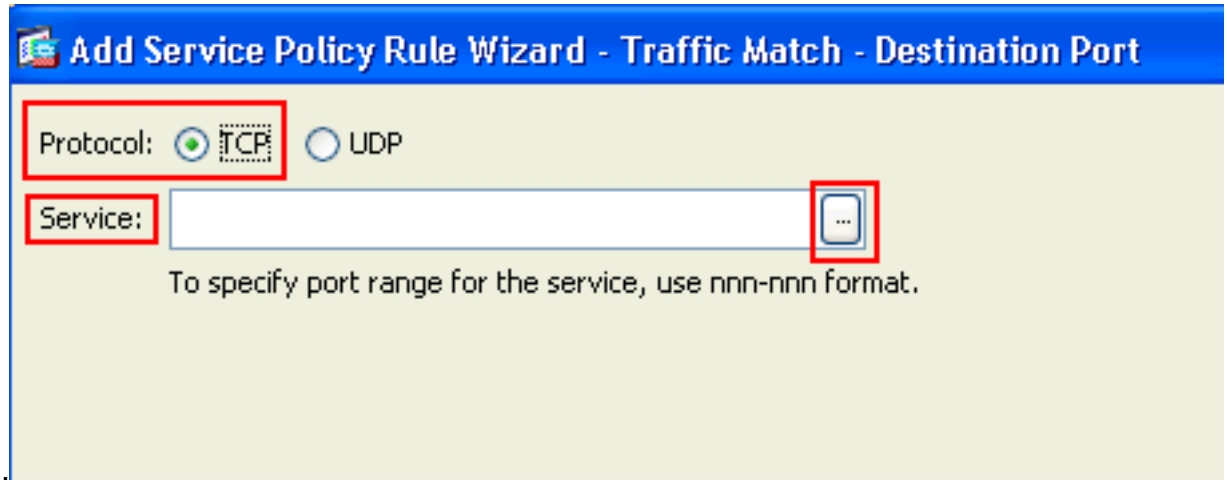
2. Kies in het venster Service Policy Wizard - Service Policy de radioknop naast **interface**. Dit past het beleid toe dat op een specifieke interface is gecreëerd, de interface buiten in dit voorbeeld. Geef een beleidsnaam op, die **buiten-cisco-beleid** in dit voorbeeld is. Klik op **Volgende**.



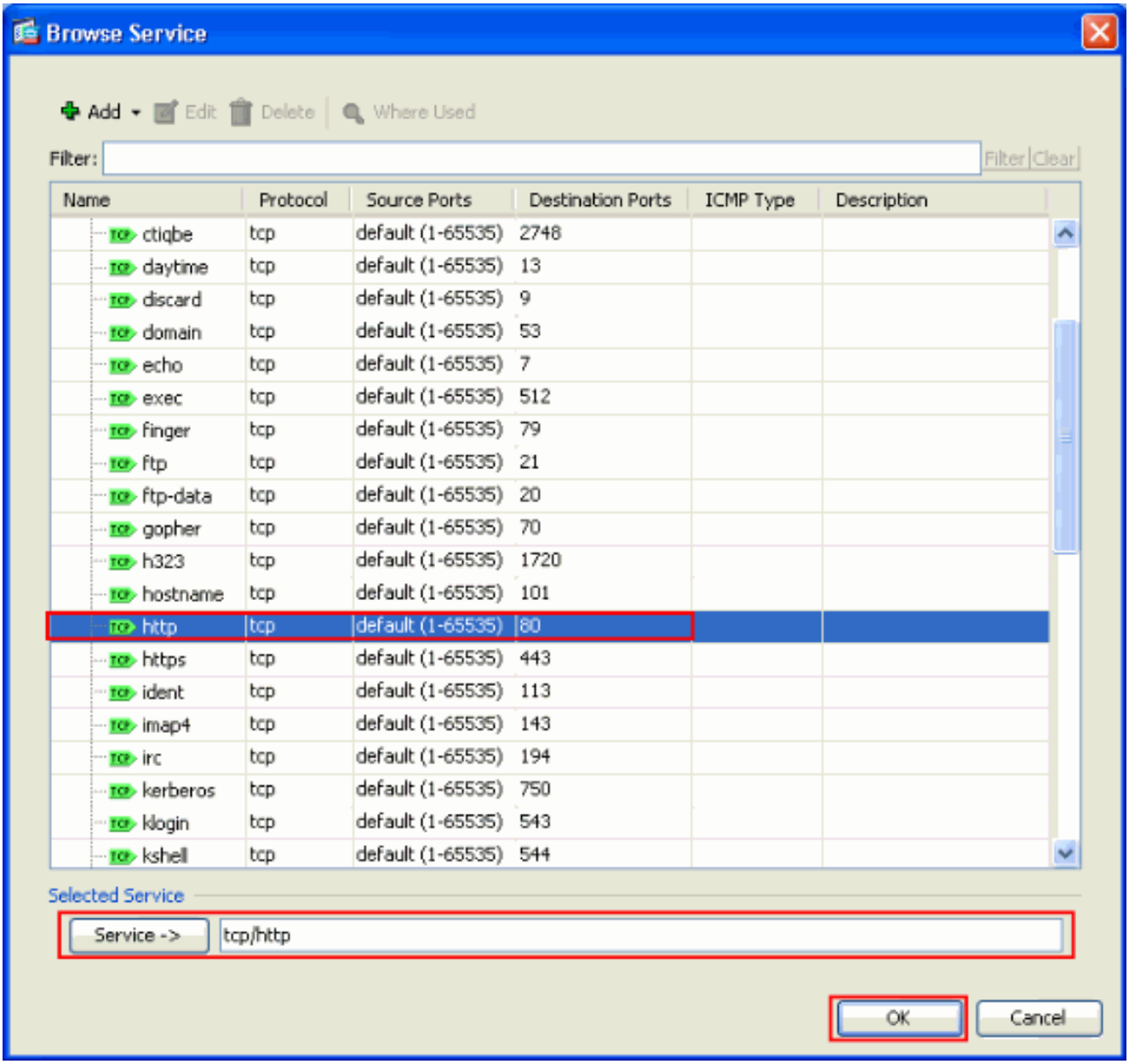
3. Van de wizard Servicebeleid toevoegen - Verkeersclassificatiecriteria - geeft u de naam van de nieuwe verkeersklasse op. De naam die in dit voorbeeld wordt gebruikt is **van buiten klasse**. Zorg ervoor dat het aankruisvakje naast **TCP- of UDP-doelpoort** is ingeschakeld en klik op
Volgende.



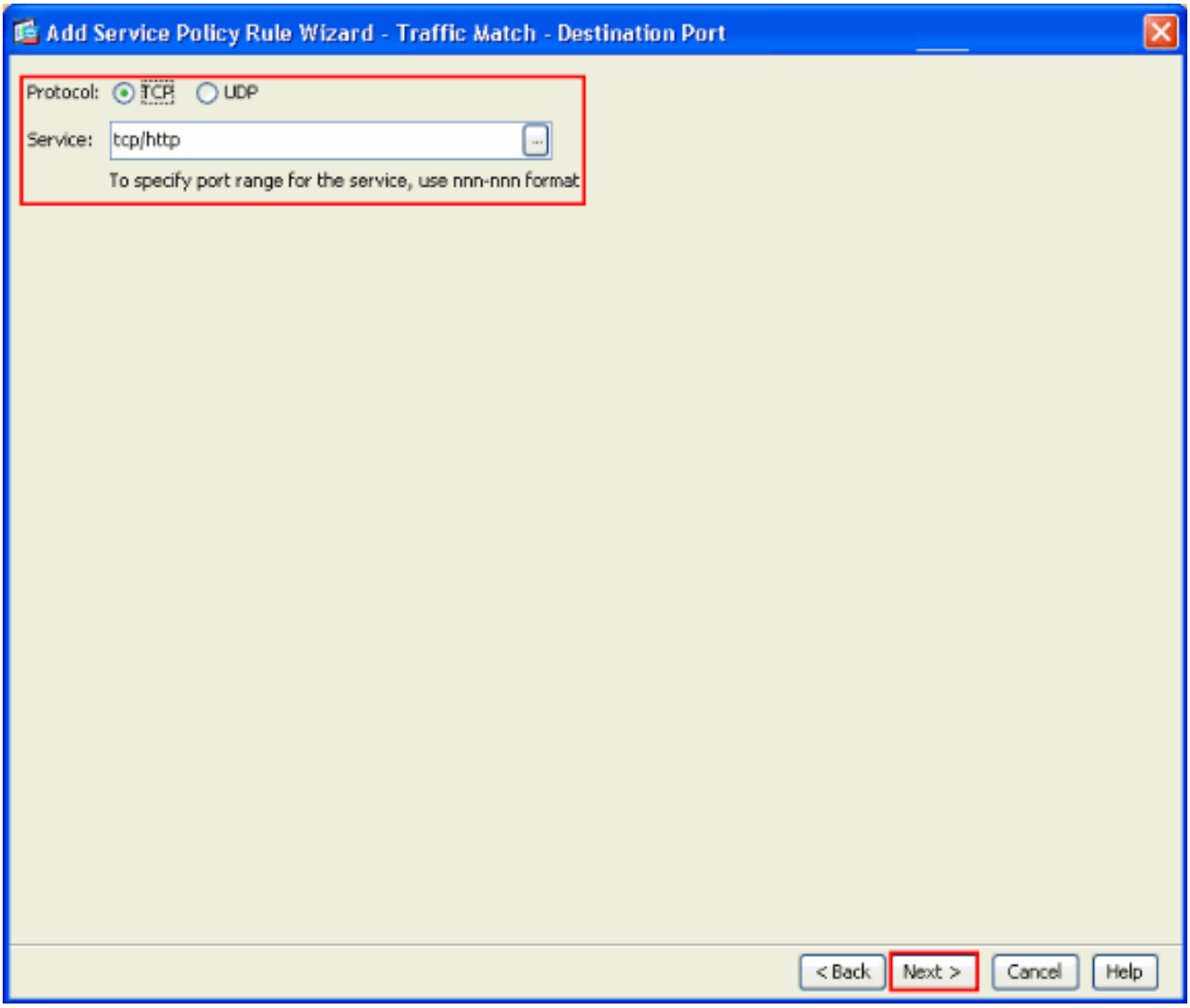
4. Kies in het venster Add Service Policy Rule - Traffic Match - Destination Port de radioknop naast **TCP** onder de sectie **Protocol**. Klik vervolgens op de knop naast **Service** om de gewenste service te kiezen.



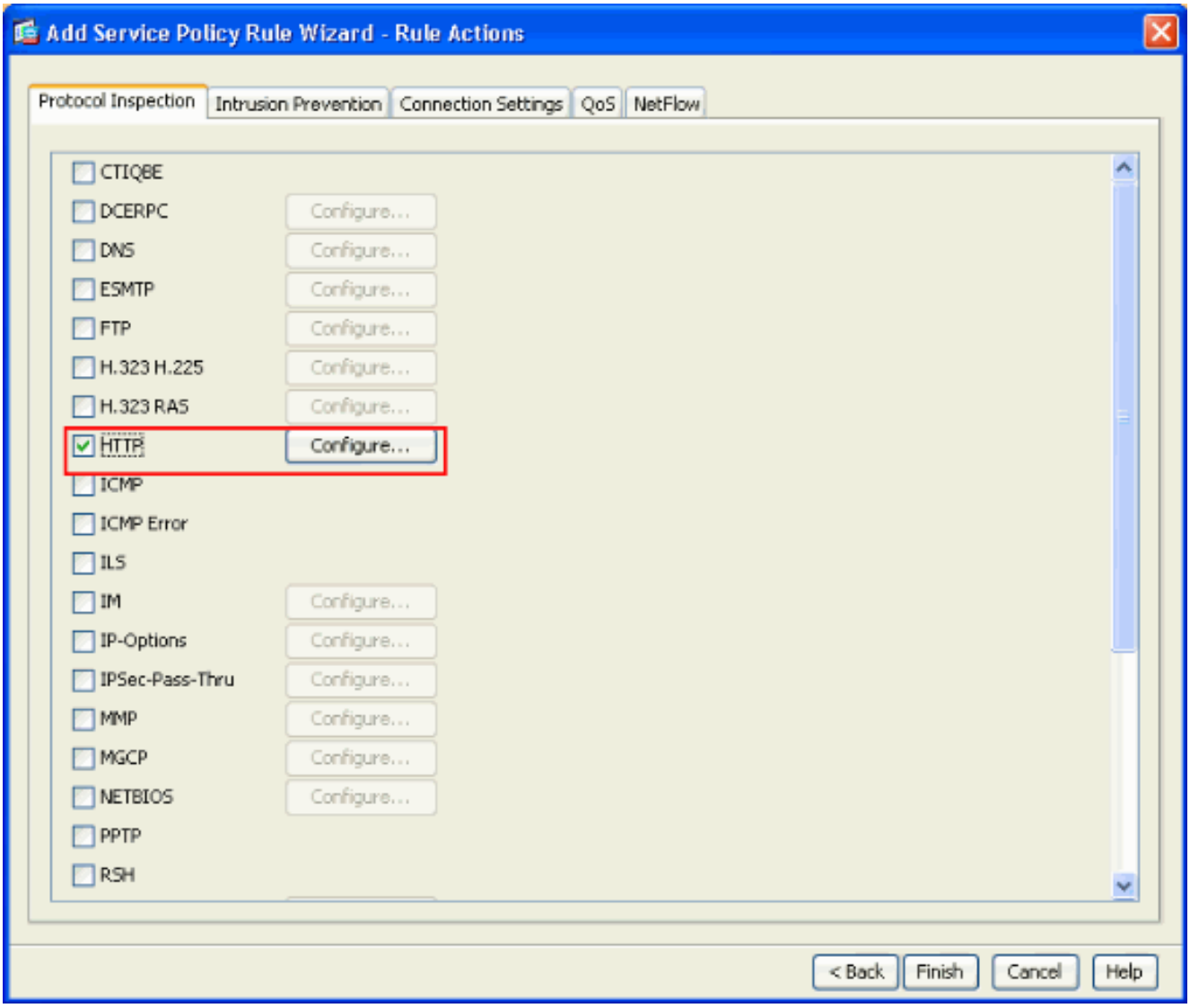
5. Kies **HTTP** als service in het venster Bladeren service. Klik vervolgens op **OK**.



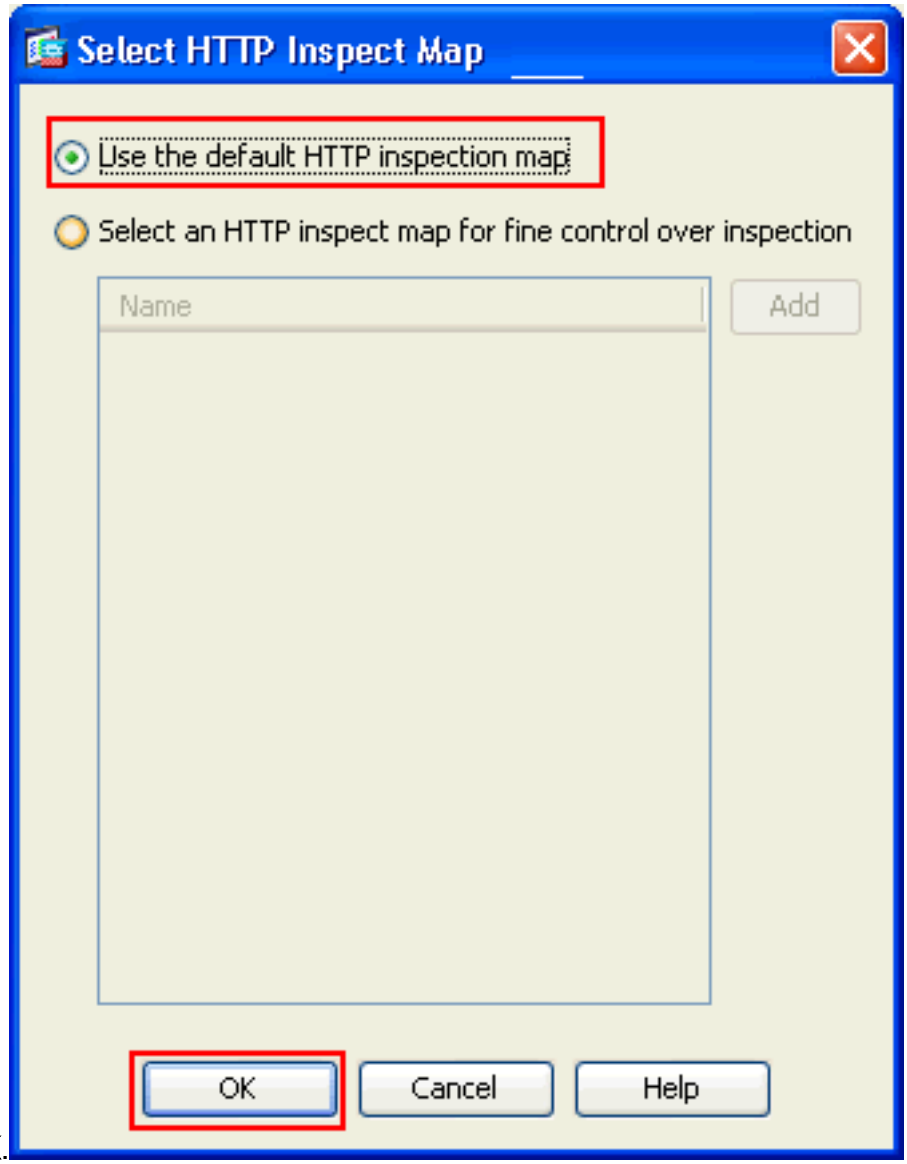
6. Van de Wizard Toevoegen Service Policy - Traffic Match - Destination Port venster kunt u zien dat de gekozen **service tcp/http** is. Klik op **Volgende**.



7. Van de Wizard Toevoegen Service Policy - Regel Handelingen, controleer het aankruisvakje naast **HTTP**. Klik vervolgens op **Configureren** naast **HTTP**.

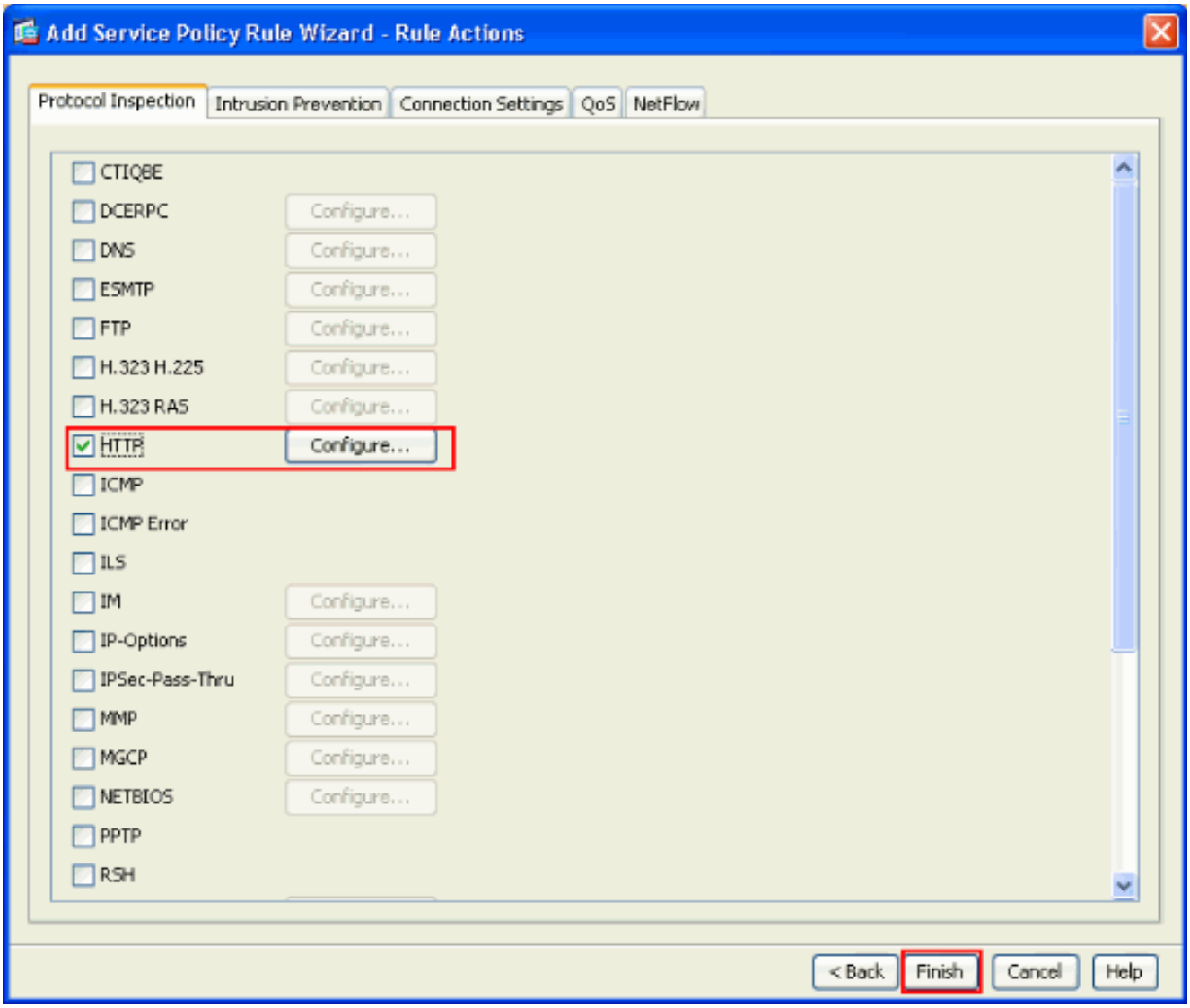


8. Controleer in het venster Select HTTP Inspect Map de radioknop naast **Gebruik de standaard HTTP-inspectiekaart**. De standaard HTTP inspectie wordt in dit voorbeeld gebruikt. Klik vervolgens op

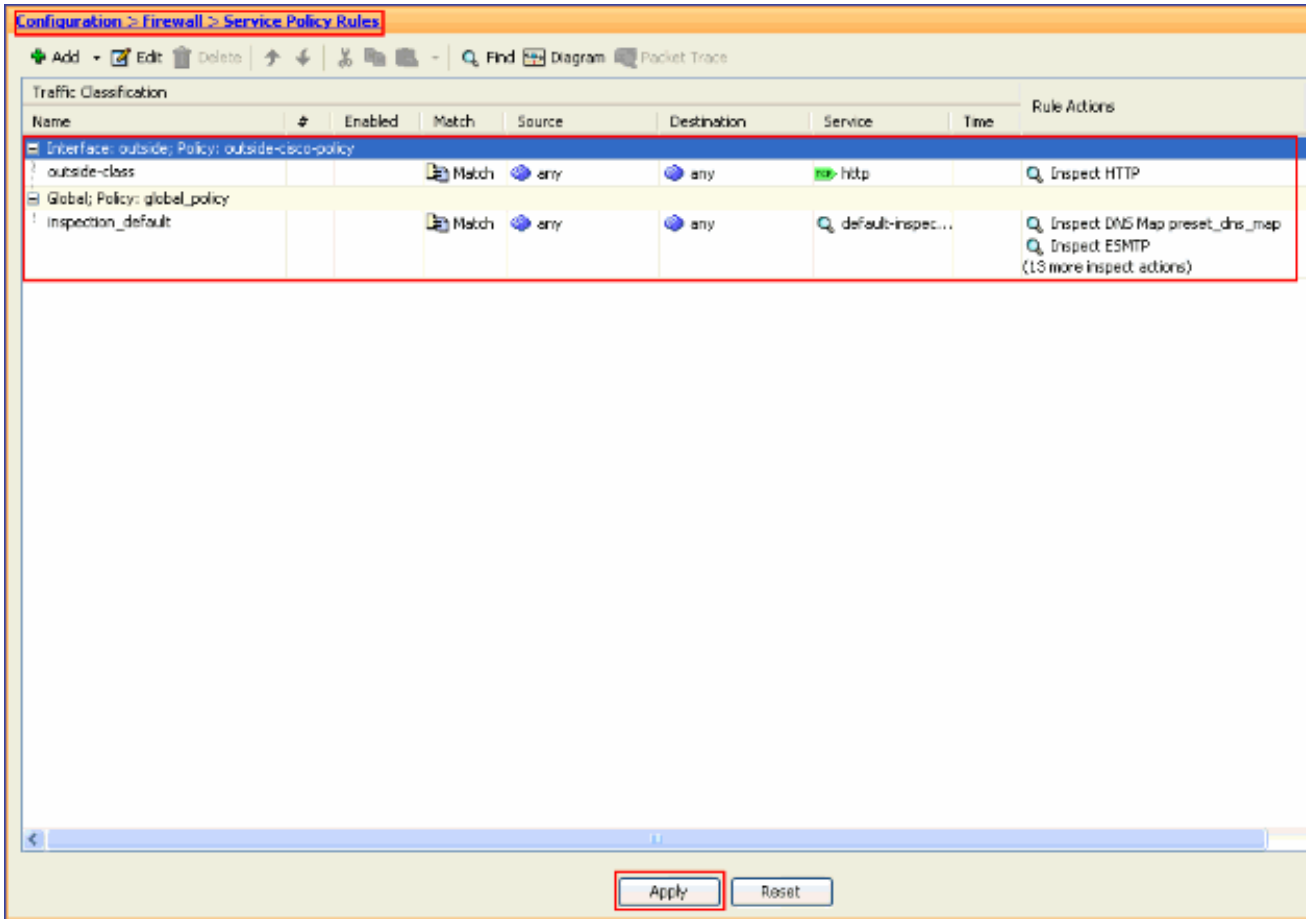


OK.

9. Klik op **Voltooien**.



10. Onder **Configuration > Firewall > Service Policy Regels**, ziet u het nieuwe geconfigureerde servicebeleid **buiten-cisco-beleid** (om HTTP te inspecteren). Dit geldt ook voor het standaard servicepakket dat al op het apparaat aanwezig is. Klik op **Toepassen** om de configuratie op Cisco ASA toe te passen.



Gerelateerde informatie

- Adaptieve security applicaties van Cisco ASA 5500 Series
- Cisco adaptieve security apparaatbeheer
- Verzoeken om opmerkingen (RFC's)
- Toepassend Application Layer Protocol-inspectie
- Technische ondersteuning en documentatie – Cisco Systems