ASA/PIX 7.X: Standaard wereldwijde inspectie uitschakelen en geen standaardinspectie voor toepassingen inschakelen met ASDM

Inhoud

Inleiding

Dit document beschrijft hoe de standaardinspectie voor een toepassing uit het algemene beleid kan worden verwijderd en hoe de inspectie voor een niet-standaardtoepassing mogelijk kan worden gemaakt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco adaptieve security applicatie (ASA) die de 7.x software-afbeelding draait.

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.

Verwante producten

Deze configuratie kan ook worden gebruikt met de PIX security applicatie die het 7.x-softwarebeeld draait.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) 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.)

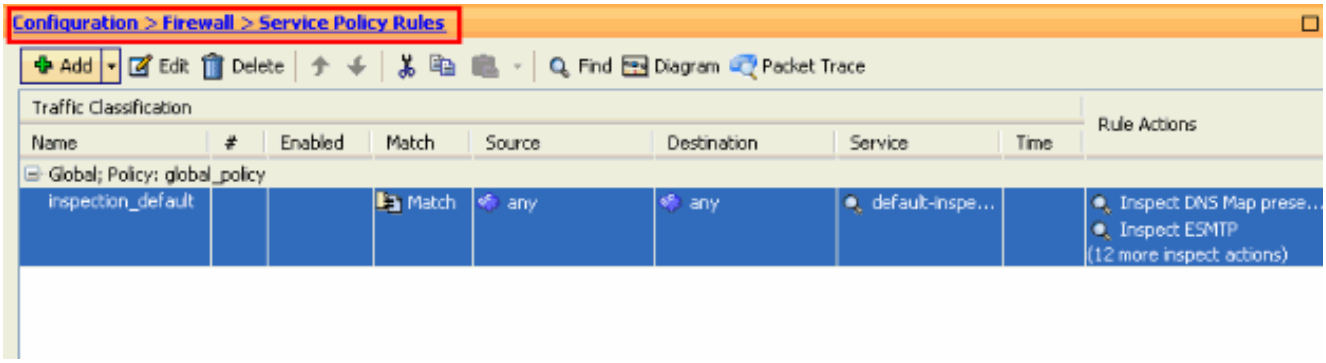
De standaard beleidsconfiguratie bevat deze opdrachten:

```
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
```

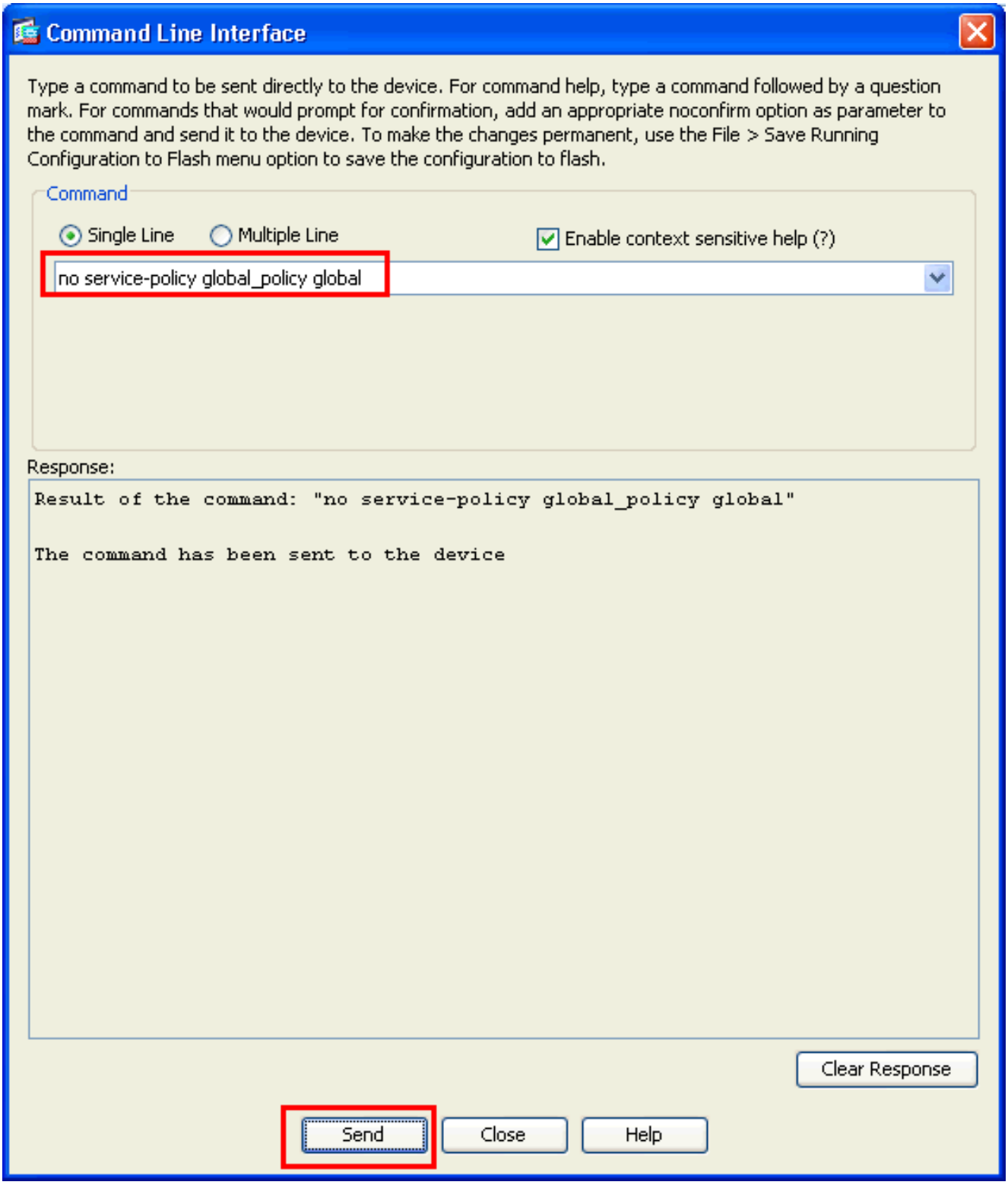
Toepassingsinspectie zonder standaardinstelling inschakelen

Voltooi deze procedure om een niet-standaardinspectie van toepassingen op Cisco ASA mogelijk te maken:

1. Aanmelden bij **ASDM**. Ga naar **Configuration > Firewall > Service Policy rules**.

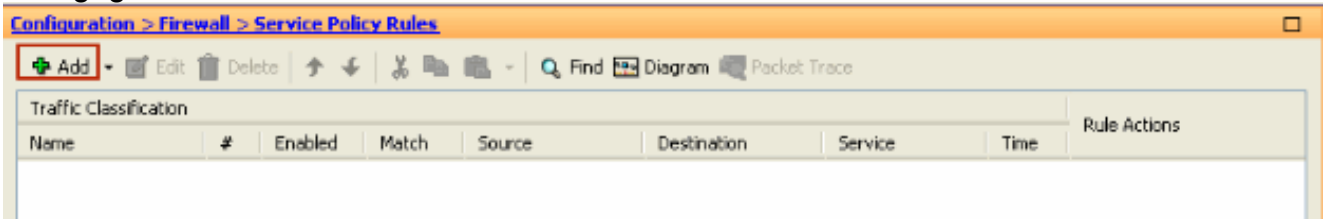


2. Als u de Configuration for Global Policy wilt behouden, die Default Class-map en Default Policy-map bevat, maar het beleid mondiaal wil verwijderen, gaat u naar **Gereedschappen > Opdrachtlijn-interface** en gebruikt u de **mondiale** opdracht **van** mondiaal **beleid zonder service-beleid** om het beleid wereldwijd te verwijderen. Klik vervolgens op **Verzend** zodat de opdracht van toepassing is op de
ASA.



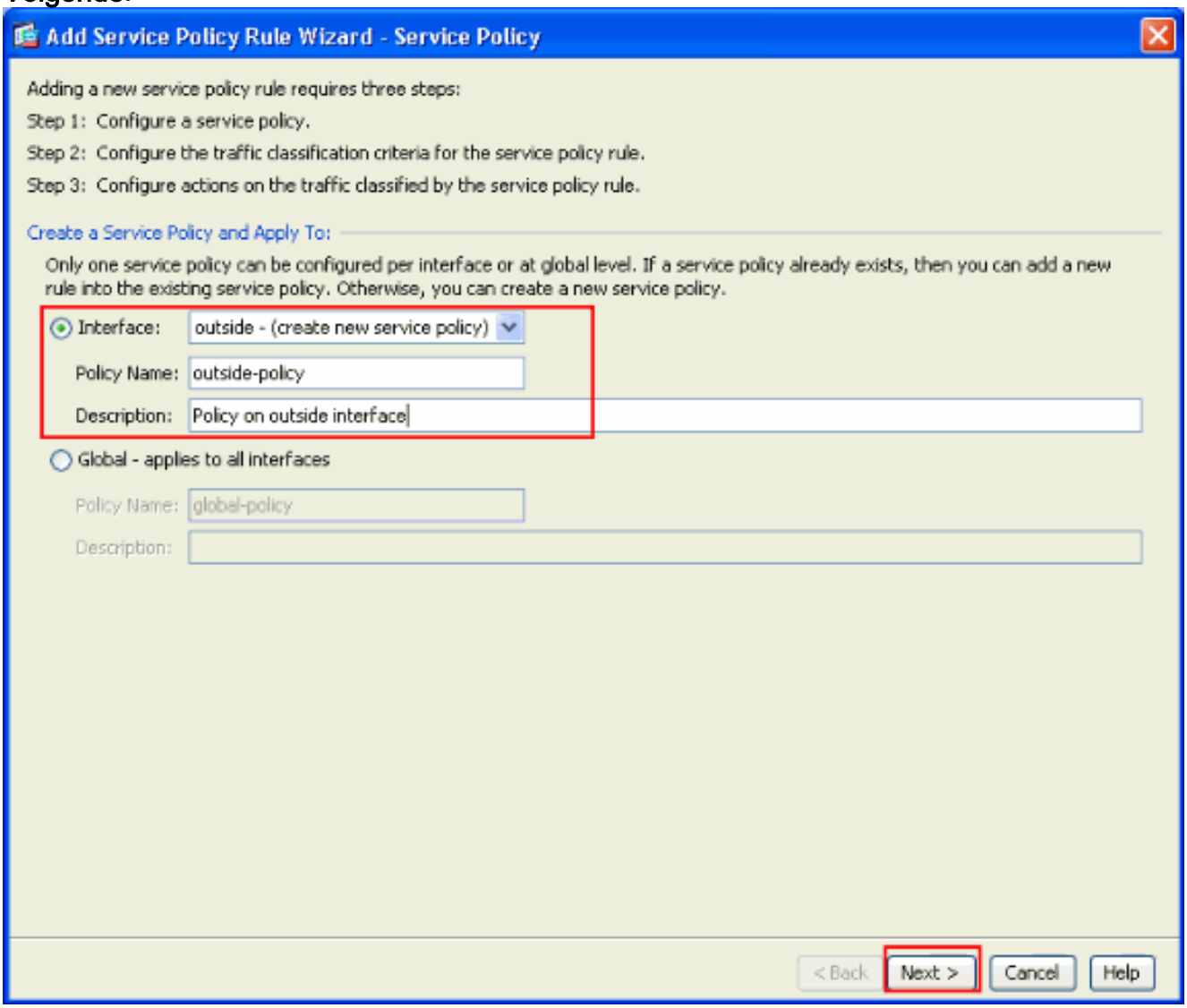
Opmerking: bij deze stap wordt het Global Policy onzichtbaar in de Adaptieve Security ApparaatManager (ASDM), maar wordt weergegeven in de CLI.

3. Klik op **Toevoegen** om een nieuw beleid toe te voegen zoals hieronder wordt weergegeven:

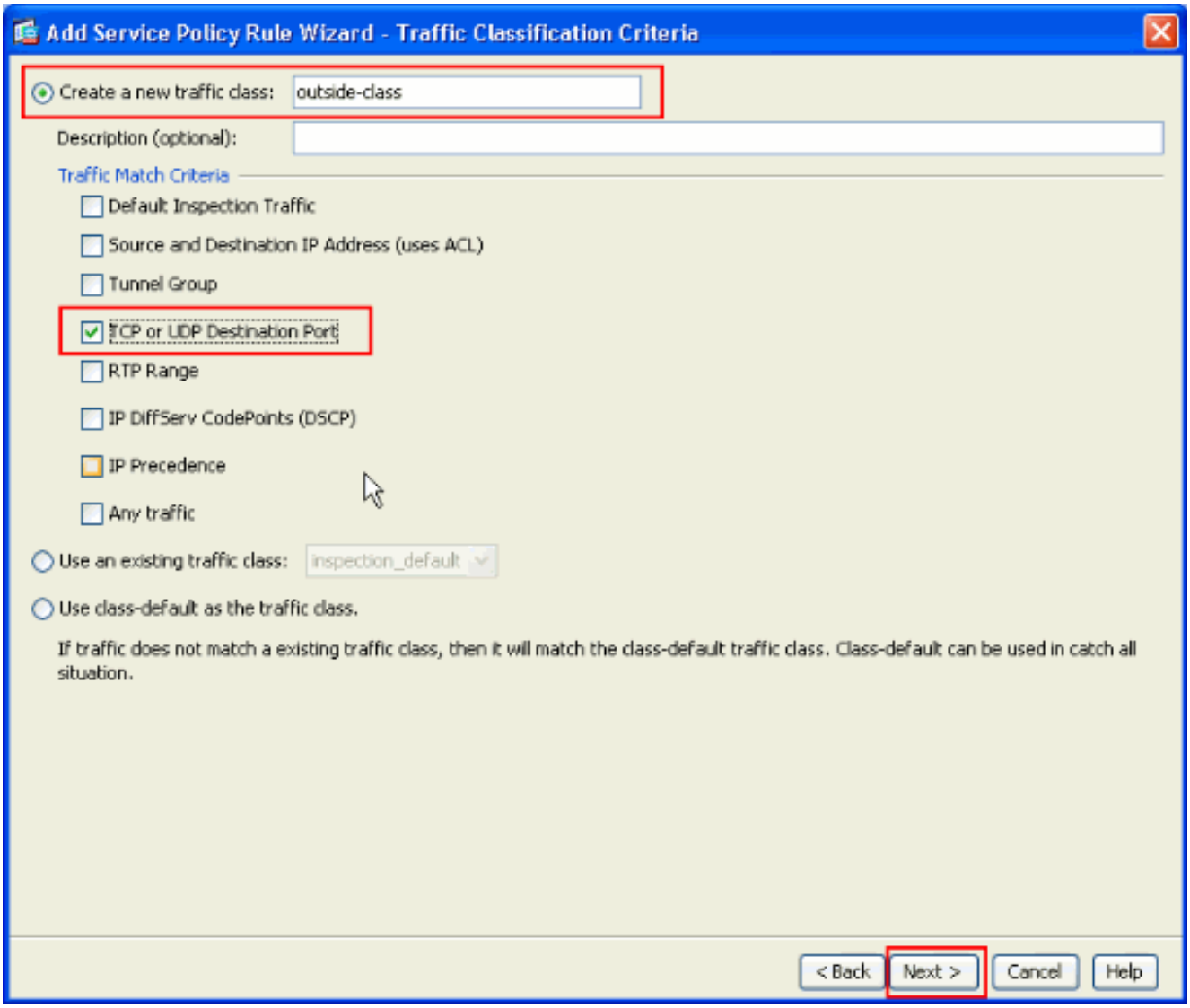


4. Zorg ervoor dat de radioknop naast **Interface** is ingeschakeld en kies de interface die u het beleid wilt toepassen in het vervolgkeuzemenu. Typ vervolgens de **beleidsnaam** en de

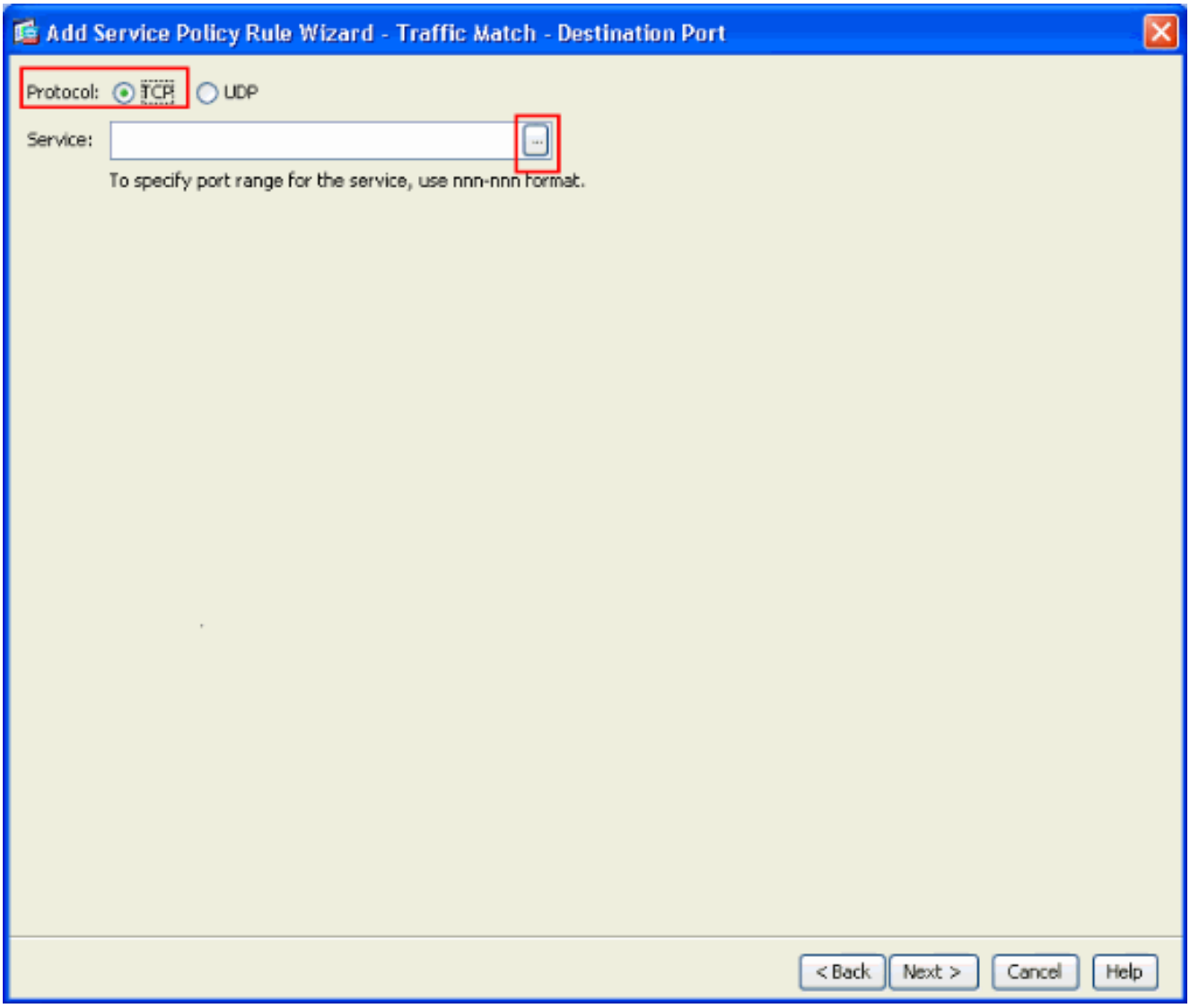
beschrijving. Klik op
Volgende.



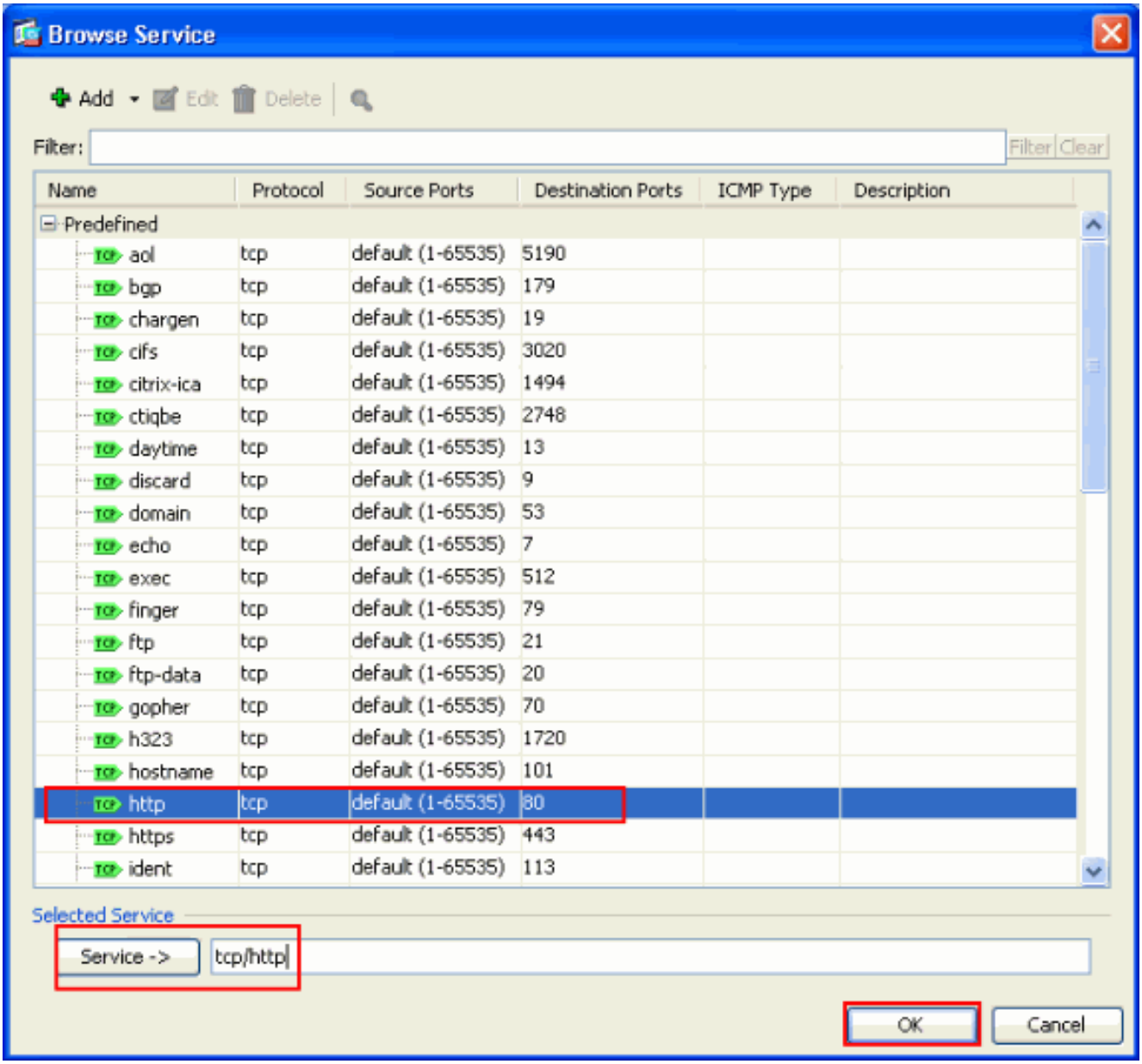
5. Maak een nieuwe class-map om het **TCP-**verkeer aan te passen als **HTTP** onder TCP valt. Klik op
Volgende.



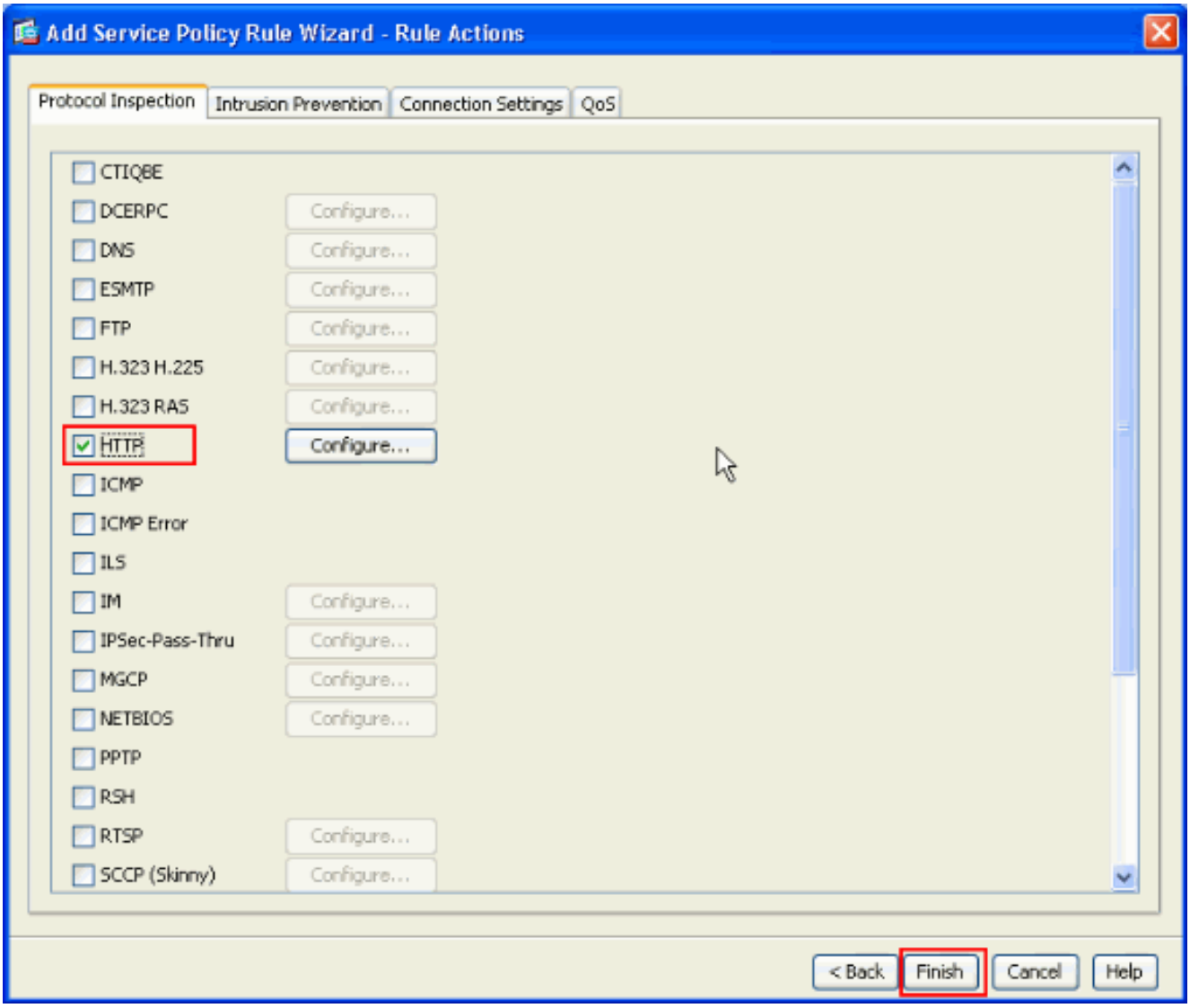
6. Kies **TCP** als het protocol.



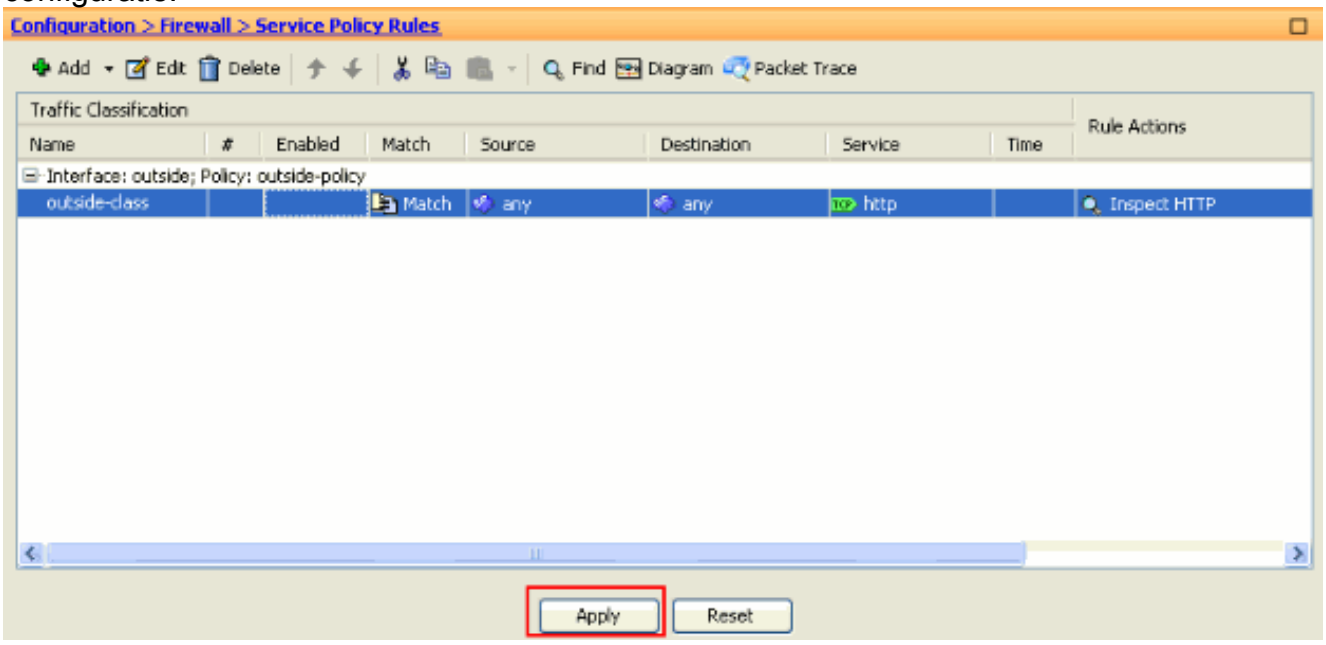
Kies **HTTP poort 80** als de service en klik op **OK**.



7. Kies **HTTP** en klik op **Voltooien**.



8. Klik op **Toepassen** om deze configuratieveranderingen in de ASA in de ASDM te verzenden. Dit voltooit de configuratie.



Verifiëren

Gebruik deze knoppen om de configuratie te controleren:

- Gebruik de opdracht **show run class-map** om de geconfigureerde class-maps te bekijken.
```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class
match port tcp eq www
!
```
- Gebruik de opdracht **Show run beleid-map** om de geconfigureerde beleidskaarten te bekijken.
```
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
!
```
- Gebruik de opdracht **showrun service-beleid** om het geconfigureerde servicebeleid te bekijken.
```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- Cisco ASA 5500 Series Opdrachtreferenties
- Ondersteuning van Cisco Adapter Security Apparaat Manager (ASDM) pagina
- Cisco PIX-firewallsoftware
- Verzoeken om opmerkingen (RFC's)
- Cisco PIX 500 Series security applicaties
- Toepassend Application Layer Protocol-inspectie
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Technische ondersteuning en documentatie – Cisco Systems