ASA/PIX 7.X : Inspection globale par défaut de débronchement et inspection d'application de Non-par défaut d'enable utilisant l'ASDM

Contenu

Introduction

Ce document décrit comment enlever l'inspection par défaut de la stratégie globale pour une application et comment activer l'inspection pour une application de non-par défaut.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur l'appliance de sécurité adaptable Cisco (ASA) ces passages l'image logicielle 7.x.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Cette configuration peut également être utilisée avec les dispositifs de sécurité PIX qui exécutent

l'image logicielle 7.x.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Stratégie globale par défaut

Par défaut, la configuration inclut une stratégie qui apparie tout le trafic par défaut d'inspection d'application et s'applique certaines inspections au trafic sur toutes les interfaces (une stratégie globale). Non toutes les inspections sont activées par défaut. Vous pouvez appliquer seulement une stratégie globale. Si vous voulez modifier la stratégie globale, vous devez éditer la stratégie par défaut ou la désactiver et appliquer un neuf. (Une stratégie d'interface ignore la stratégie globale.)

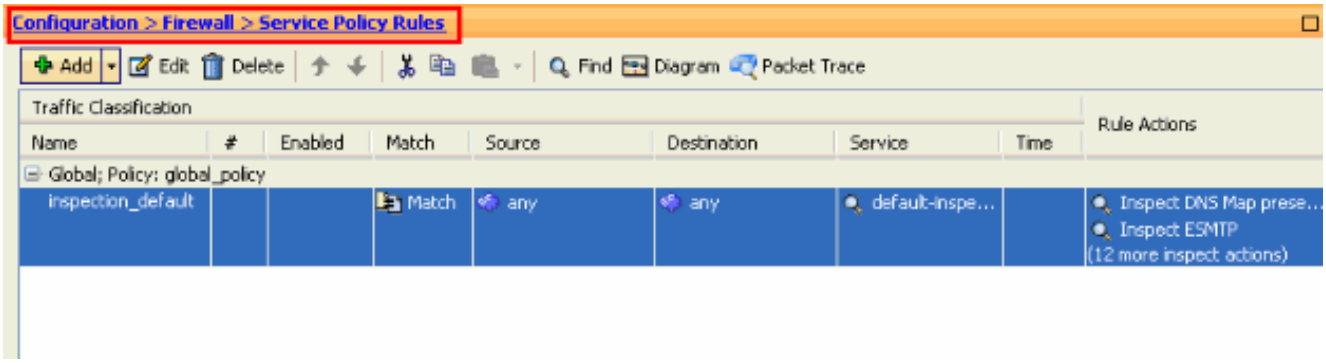
La configuration de stratégie par défaut inclut ces commandes :

```
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
```

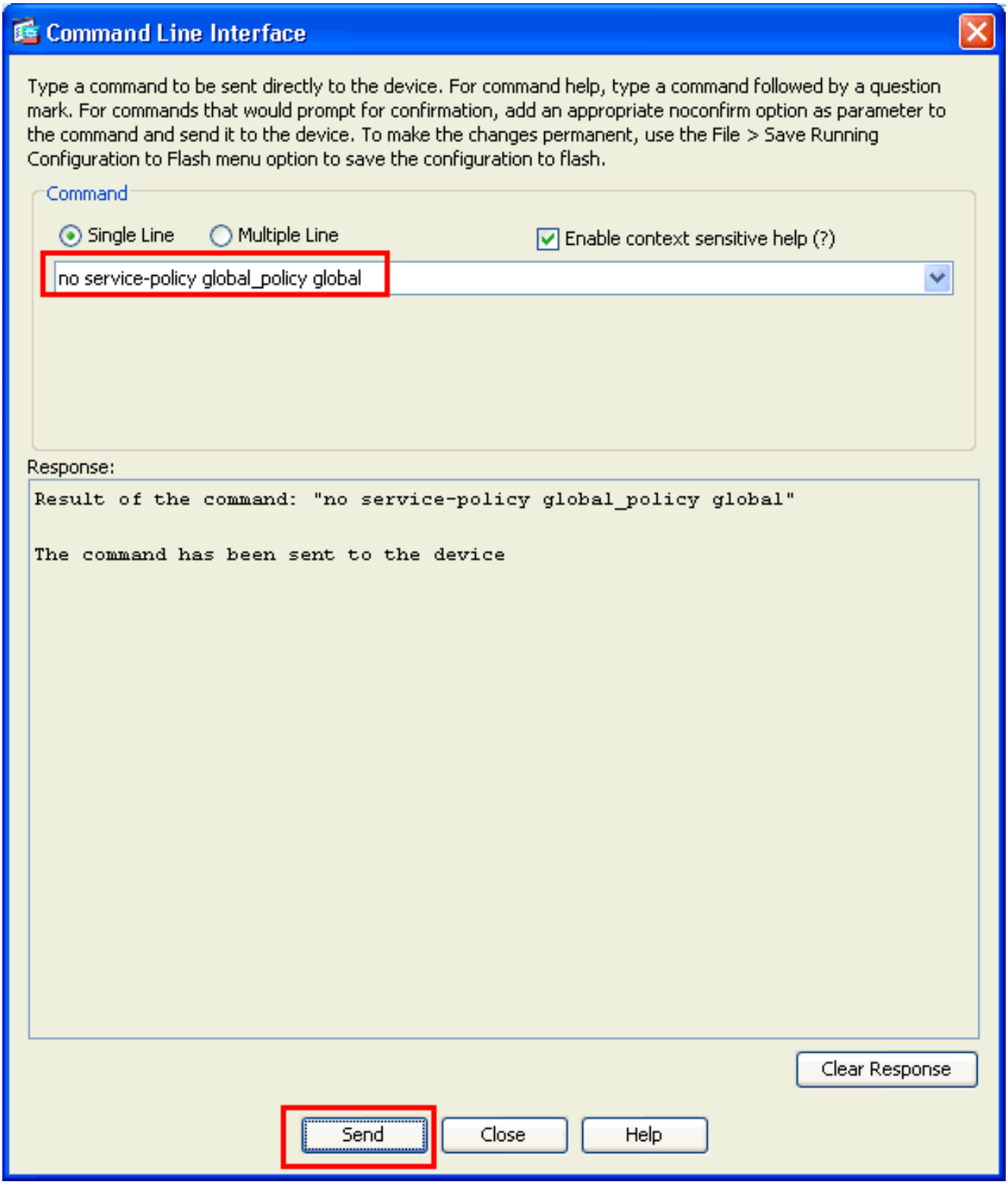
Inspection d'application de Non-par défaut d'enable

Remplissez cette procédure pour activer l'inspection d'application de Non-par défaut sur Cisco ASA :

1. Procédure de connexion à l'**ASDM**. Allez aux **règles de configuration > de stratégie de Pare-feu > de service**.

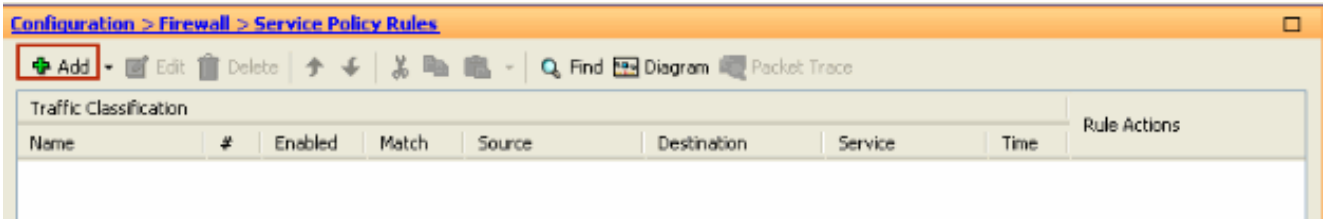


2. Si vous voulez garder la configuration pour la stratégie globale qui inclut le policy-map par défaut de class-map et de par défaut, mais voulez enlever la stratégie globalement, allez aux **outils > à l'interface de ligne de commande** et n'utilisez l'**aucune commande globale de global-stratégie de service-stratégie** d'enlever la stratégie globalement. Puis, le clic **envoient** ainsi la commande est appliquée à
l'ASA.



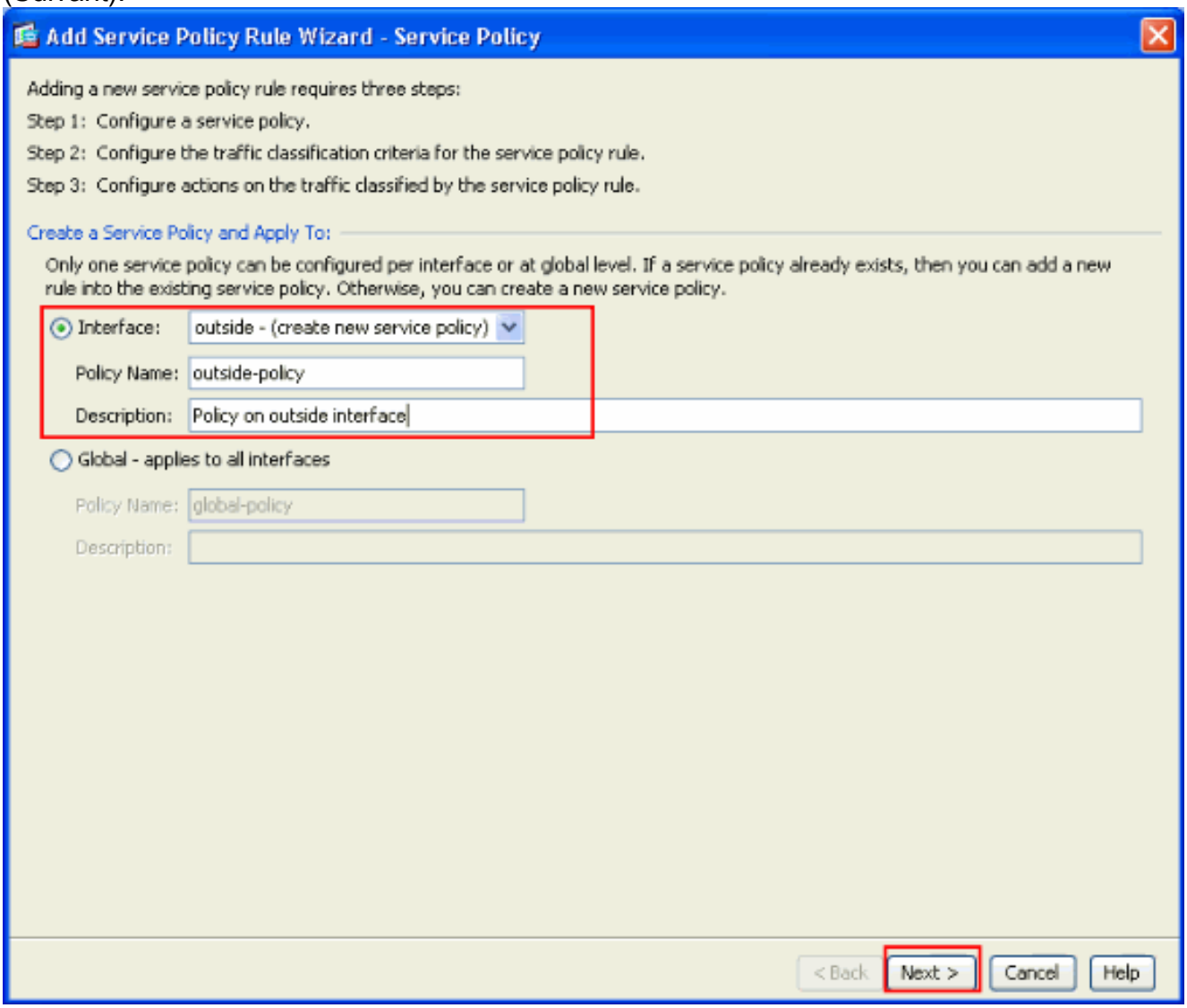
Remarque: Avec cette étape la stratégie globale devient invisible dans Adaptive Security Device Manager (ASDM), mais est affichée dans le CLI.

3. Cliquez sur Add afin d'ajouter une nouvelle stratégie comme affiché ici :

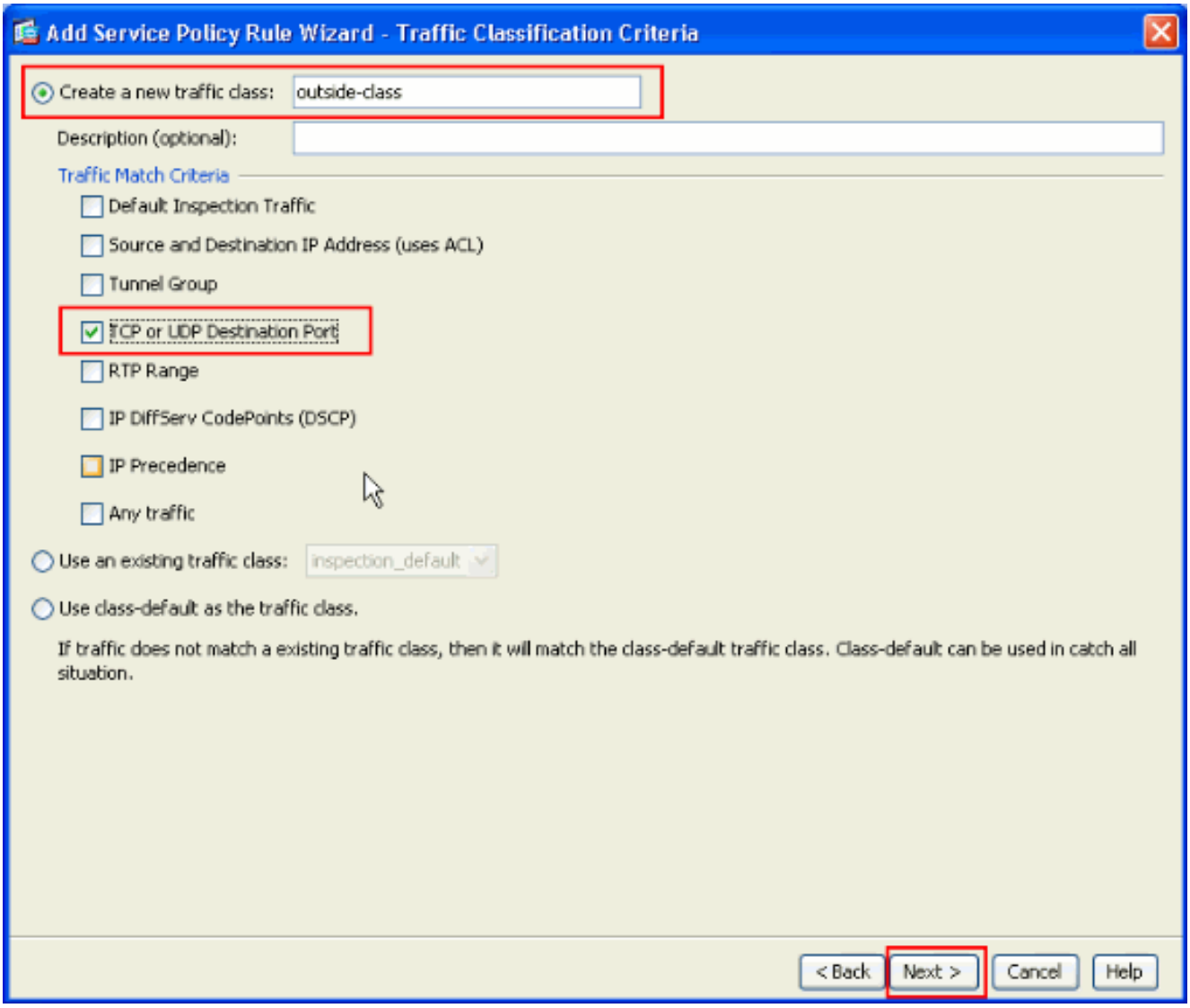


4. Assurez-vous que la case d'option à côté de l'**interface** est vérifiée et choisissez l'interface que vous voulez appliquer la stratégie à partir du menu déroulant. Puis, fournissez le **nom de**

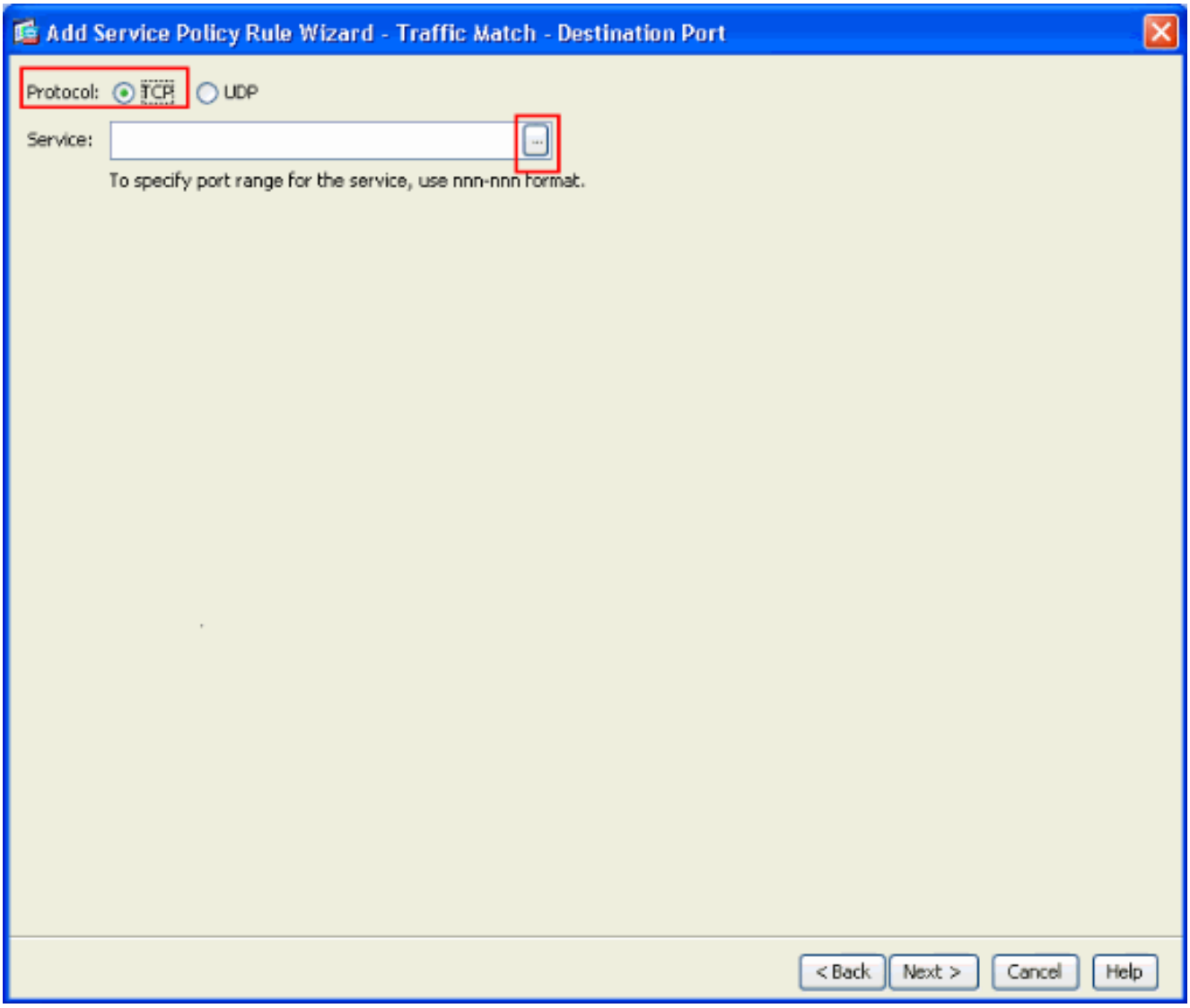
stratégie et la **description**. Cliquez sur **Next**
(Suivant).



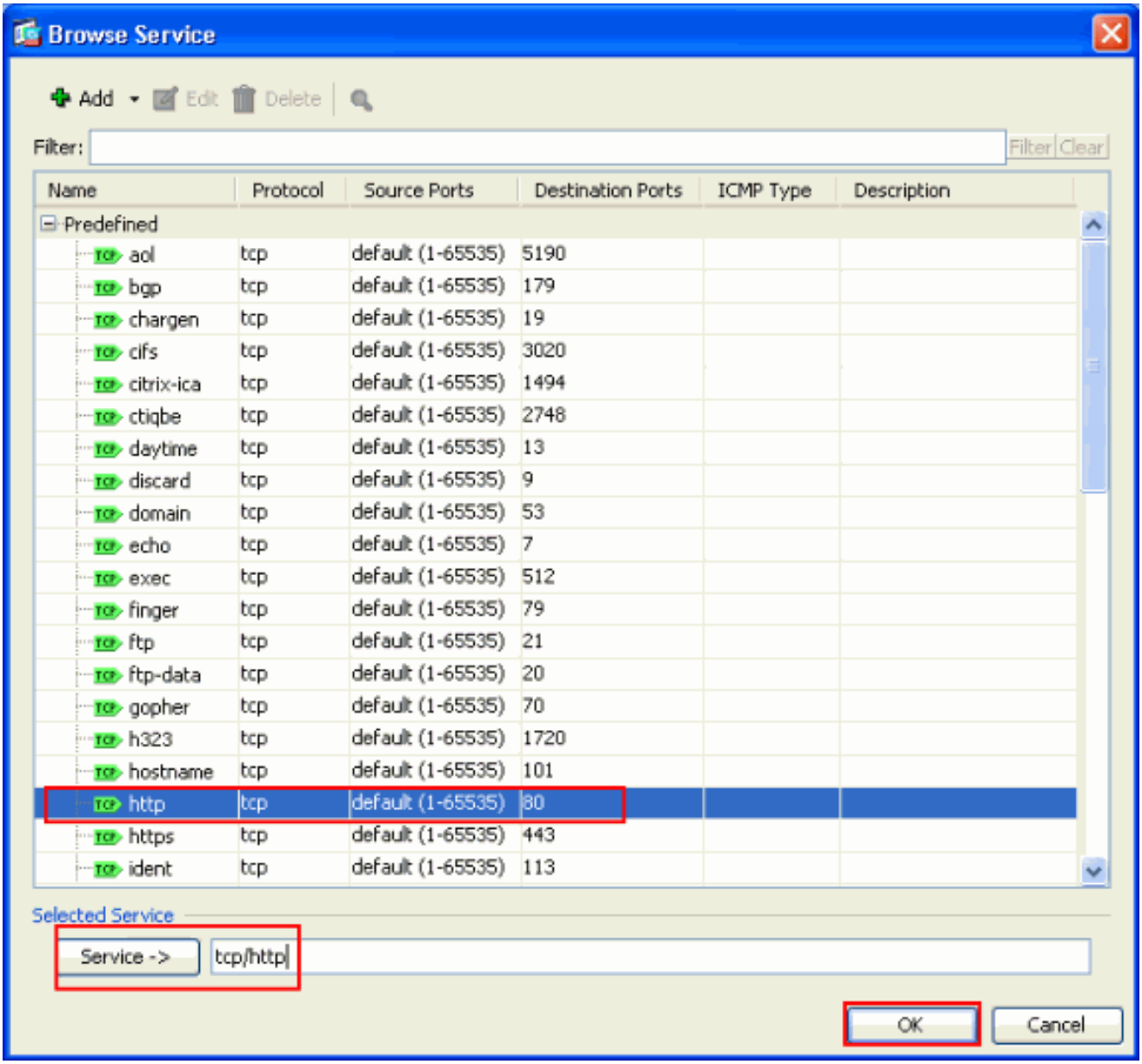
5. Créez un nouveau class-map pour apparier le **trafic TCP** comme le **HTTP** tombe sous le TCP. Cliquez sur **Next**
(Suivant).



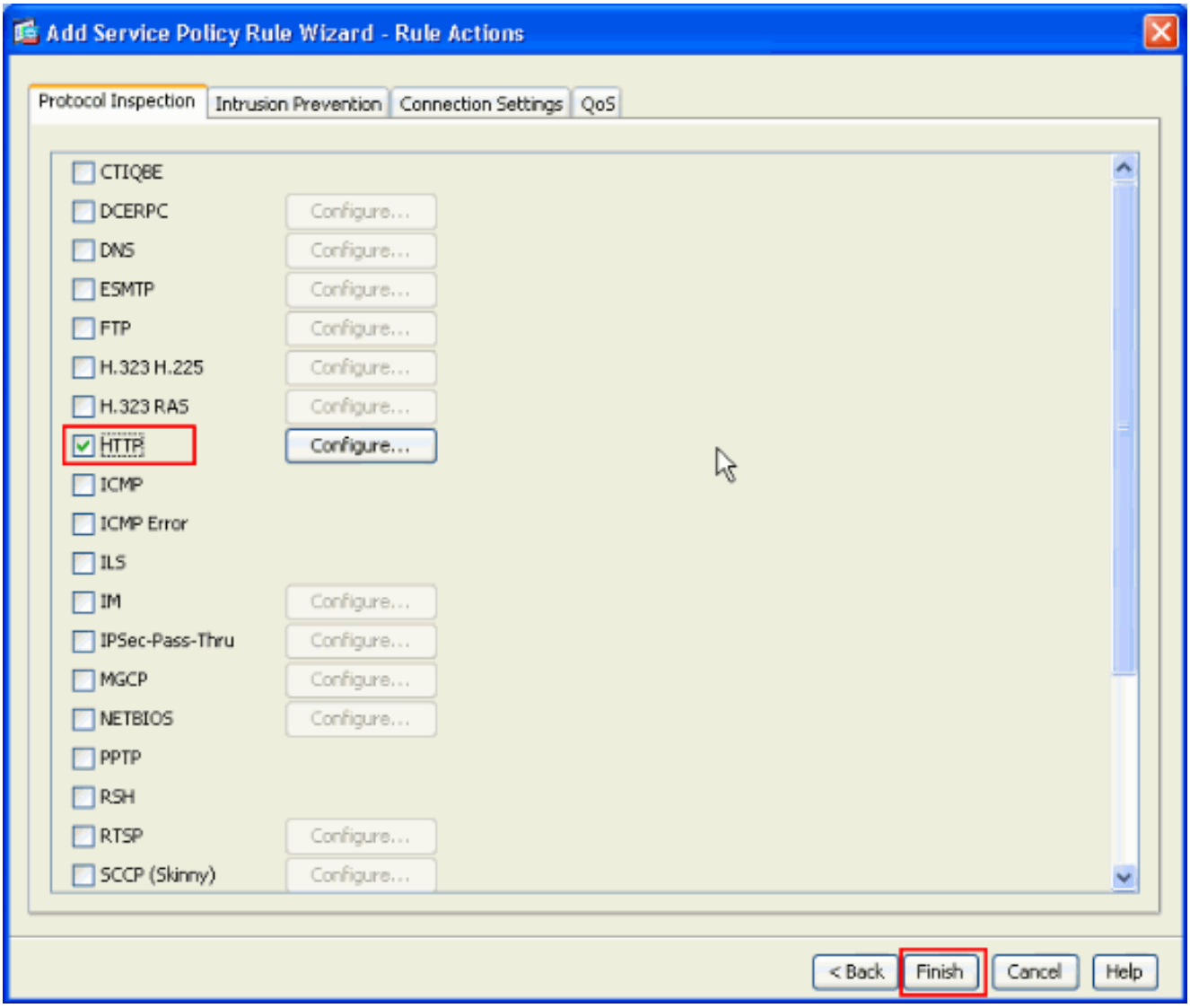
6. Choisissez le **TCP** comme protocole.



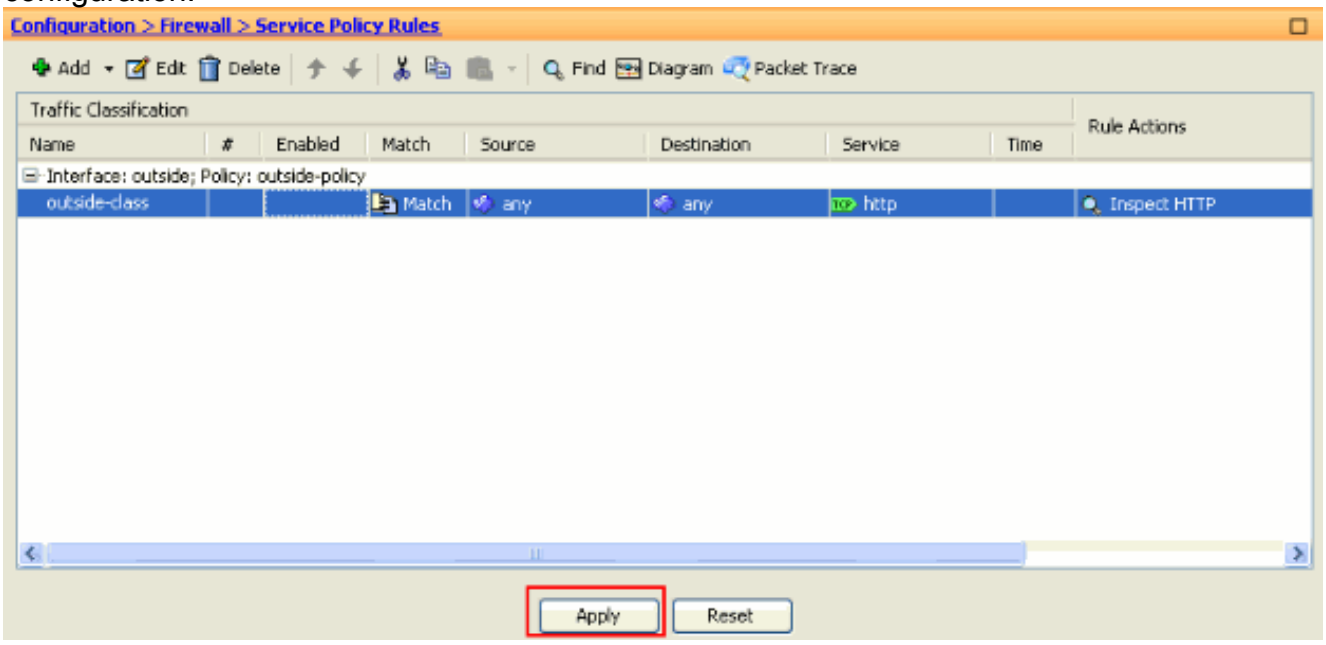
Choisissez le **port HTTP 80** comme service et cliquez sur OK.



7. Choisissez le **HTTP** et cliquez sur Finish.



8. Cliquez sur Apply pour envoyer ces modifications de configuration à l'ASA de l'ASDM. Ceci se termine la configuration.



Vérifiez

Utilisez ces **commandes show** de vérifier la configuration :

- Utilisez la commande de **class-map de passage d'exposition** de visualiser les class map configurés.`ciscoasa# sh run class-map`
```
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class match port tcp eq www !
```
- Utilisez la commande de **policy-map de passage d'exposition** de visualiser les cartes de stratégie configurées.`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 !
```
- Utilisez la commande de service-**stratégie de passage d'exposition** de visualiser les stratégies de service configurées.`ciscoasa# sh run service-policy`
```
service-policy outside-policy interface outside
```

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Références de commandes de gamme de Cisco ASA 5500
- Page de support du Cisco Adaptive Security Device Manager (ASDM)
- Logiciels pare-feu Cisco PIX
- Demandes de commentaires (RFC)
- Dispositifs de sécurité de la gamme Cisco PIX 500
- Application de l'inspection de protocole de la couche applicative
- Références des commandes du pare-feu Cisco Secure PIX
- Support et documentation techniques - Cisco Systems