ASA 8.3 et versions ultérieures - Configuration de l'inspection à l'aide d'ASDM

Contenu

Introduction

Ce document fournit un exemple de configuration pour Cisco Adaptive Security Appliance (ASA) avec les versions 8.3(1) et ultérieures sur la façon de supprimer l'inspection par défaut de la stratégie globale pour une application et comment activer l'inspection pour une application autre que par défaut à l'aide d'Adaptive Security Device Manager (ASDM).

Référez-vous à PIX/ASA 7.x : Désactivez l'inspection globale par défaut et activez l'inspection des applications non par défaut pour la même configuration sur Cisco ASA avec les versions 8.2 et antérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur le logiciel Cisco ASA Security Appliance version 8.3(1) avec ASDM 6.3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

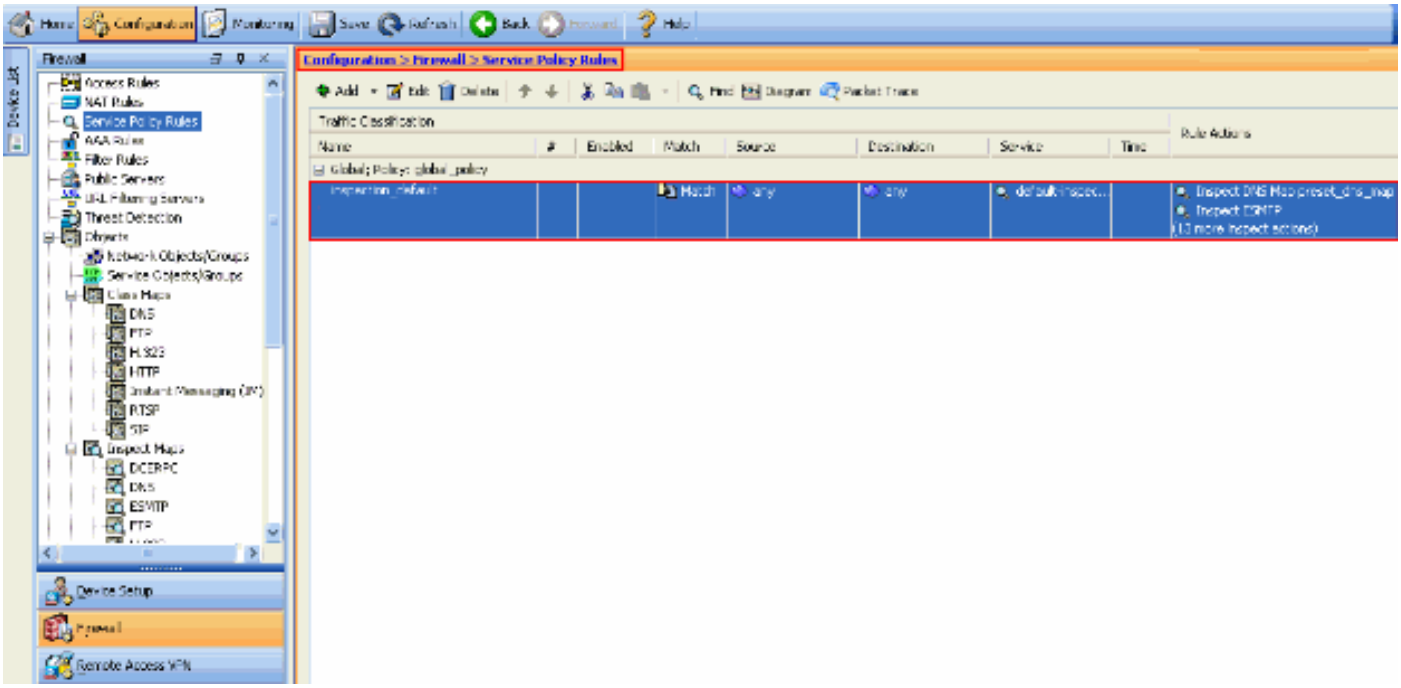
Conventions

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 politique qui correspond à tout le trafic d'inspection d'application par défaut et applique certaines inspections au trafic sur toutes les interfaces (une politique globale). Toutes les inspections ne sont pas activées par défaut. Vous ne pouvez appliquer qu'une seule stratégie globale. Si vous souhaitez modifier la stratégie globale, vous devez soit modifier la stratégie par défaut, soit la désactiver et en appliquer une nouvelle. (Une stratégie d'interface remplace la stratégie globale.)

Dans ASDM, choisissez **Configuration > Firewall > Service Policy Rules** pour afficher la stratégie globale par défaut qui a l'inspection d'application par défaut, comme indiqué ici :

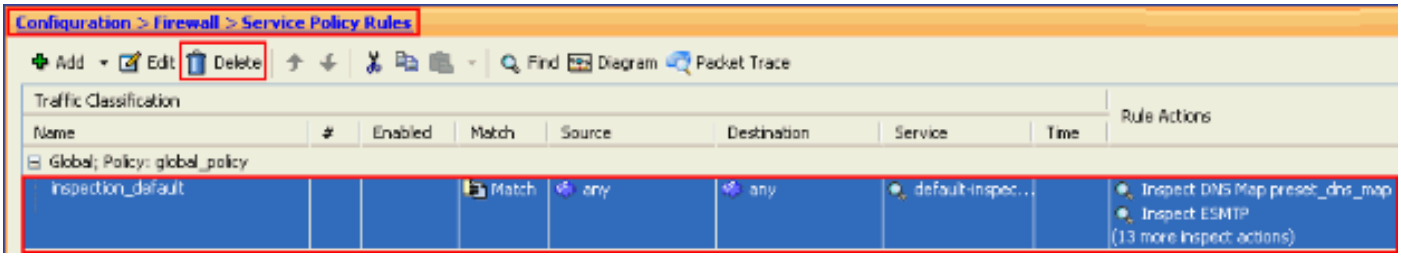


La configuration de stratégie par défaut comprend les commandes suivantes :

```
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
```

Si vous devez désactiver la stratégie globale, utilisez la commande **no service-policy global_policy global**. Afin de supprimer la stratégie globale à l'aide d'ASDM, choisissez **Configuration > Firewall > Service Policy Rules**. Ensuite, sélectionnez la stratégie globale et cliquez sur **Supprimer**.



Remarque : lorsque vous supprimez la stratégie de service avec ASDM, la stratégie associée et les mappages de classes sont supprimés. Cependant, si la stratégie de service est supprimée à l'aide de l'interface de ligne de commande, seule la stratégie de service est supprimée de l'interface. La carte de classe et la carte de stratégie restent inchangées.

Désactiver l'inspection globale par défaut pour une application

Afin de désactiver l'inspection globale pour une application, utilisez la commande *no* version de la **commande inspect**.

Par exemple, afin de supprimer l'inspection globale pour l'application FTP à laquelle le dispositif de sécurité écoute, utilisez la commande **no inspect ftp** en mode de configuration de classe.

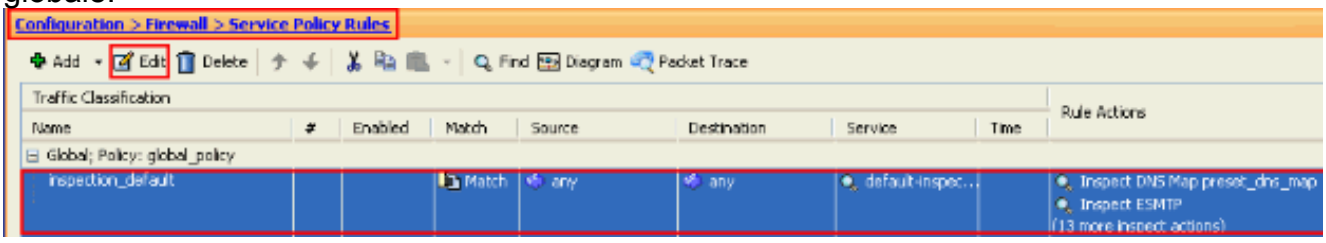
Le mode de configuration de classe est accessible à partir du mode de configuration de la carte de stratégie. Afin de supprimer la configuration, utilisez la forme *no* de la commande.

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

Afin de désactiver l'inspection globale pour FTP à l'aide d'ASDM, complétez ces étapes :

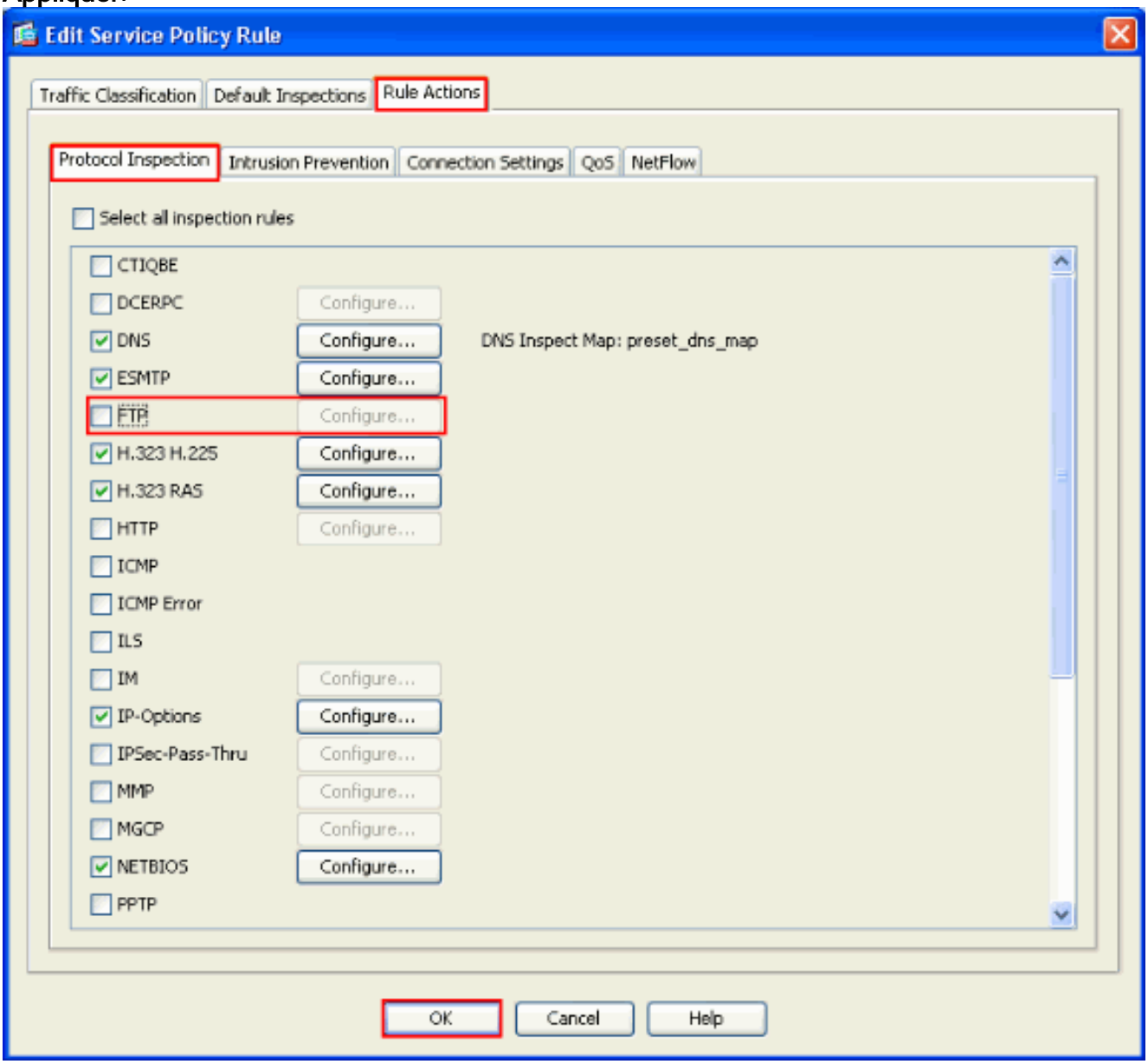
Remarque : Reportez-vous à Autoriser l'accès HTTPS pour ASDM pour les paramètres de base afin d'accéder au PIX/ASA par l'intermédiaire d'ASDM.

1. Choisissez **Configuration > Firewall > Service Policy Rules** et sélectionnez la stratégie globale par défaut. Ensuite, cliquez sur **Modifier** pour modifier la stratégie d'inspection globale.



2. Dans la fenêtre Modifier une règle de stratégie de service, sélectionnez **Inspection de protocole** sous l'onglet **Actions de règle**. Assurez-vous que la case **FTP** est décochée. Ceci désactive l'inspection FTP comme indiqué dans l'image suivante. Cliquez ensuite sur **OK**,

puis sur
Appliquer.



Remarque : Pour plus d'informations sur l'inspection FTP, référez-vous à PIX/ASA 7.x : Exemple de configuration de l'activation des services FTP/TFTP.

Activer l'inspection pour une application non par défaut

L'inspection HTTP améliorée est désactivée par défaut. Afin d'activer l'inspection HTTP dans global_policy, utilisez la commande **inspect http** sous class inspection_default.

Dans cet exemple, toute connexion HTTP (trafic TCP sur le port 80) qui entre dans l'appliance de sécurité via n'importe quelle interface est classée pour inspection HTTP. *Comme la stratégie est une stratégie globale, l'inspection se produit uniquement lorsque le trafic entre dans chaque interface*.

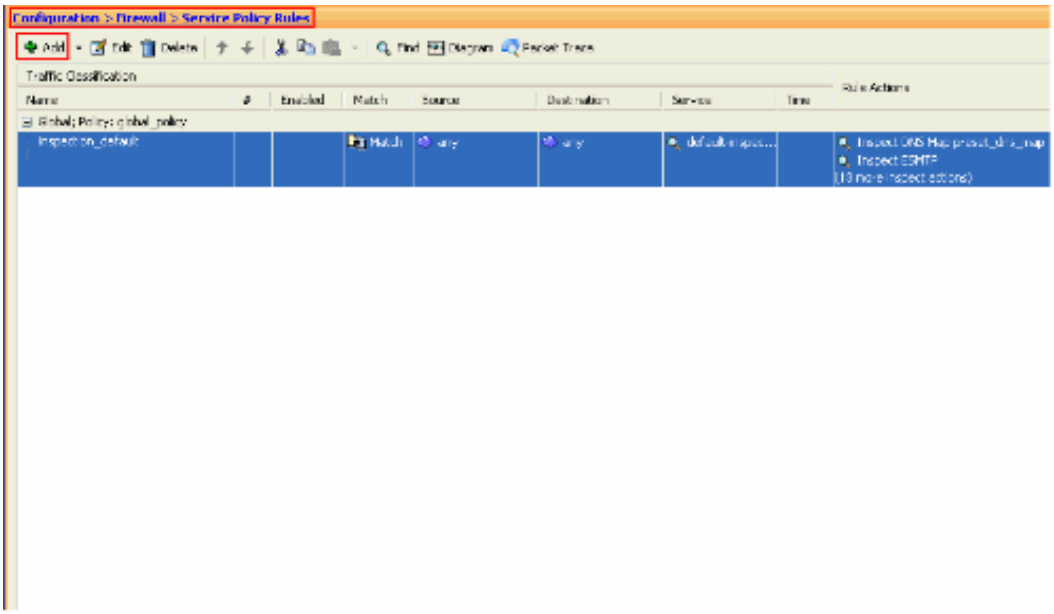
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
```

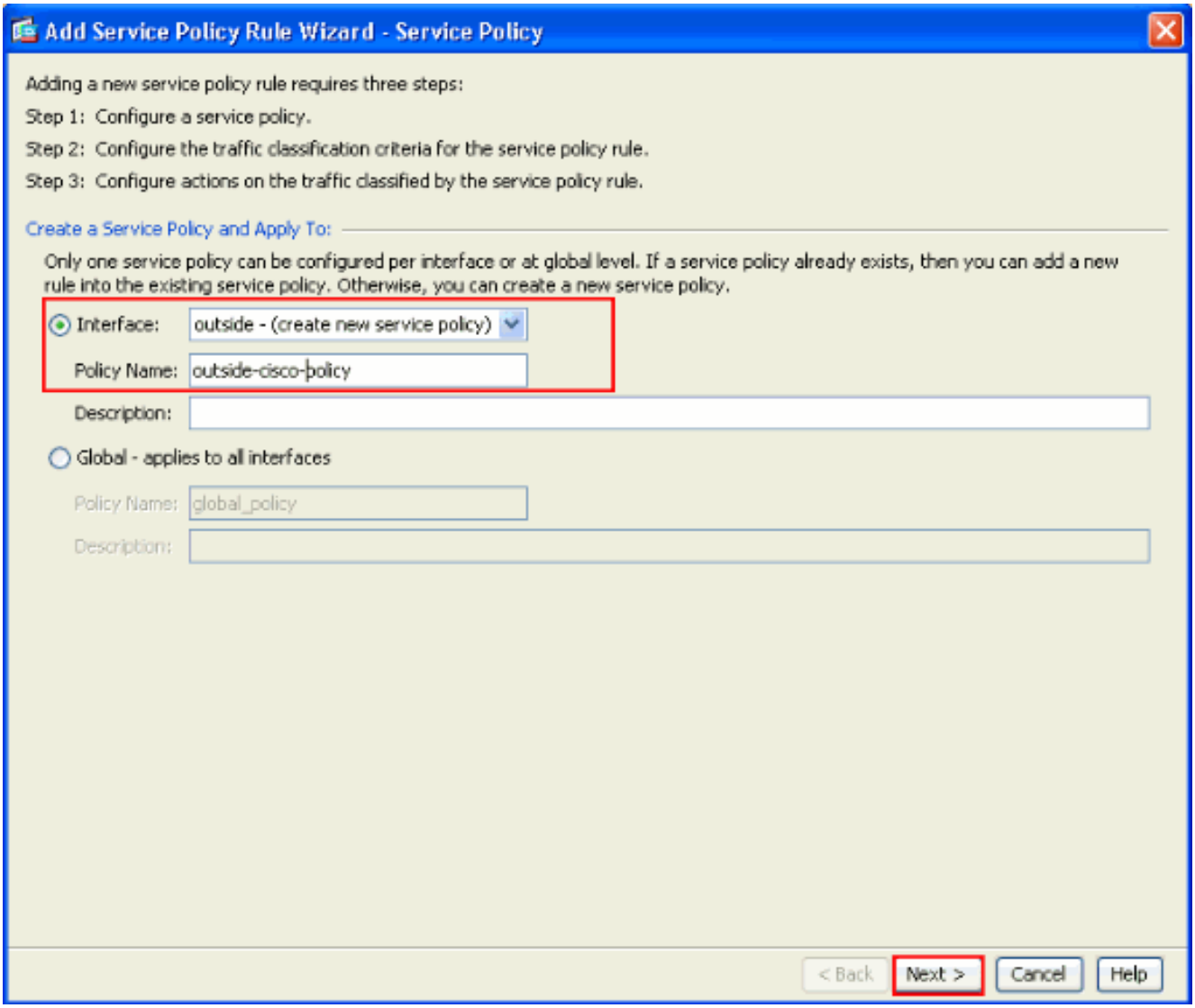
```
ASA2(config)#service-policy global_policy global
```

Dans cet exemple, toute connexion HTTP (trafic TCP sur le port 80) qui entre ou sort du dispositif de sécurité via l'*interface externe est classée pour inspection HTTP*.

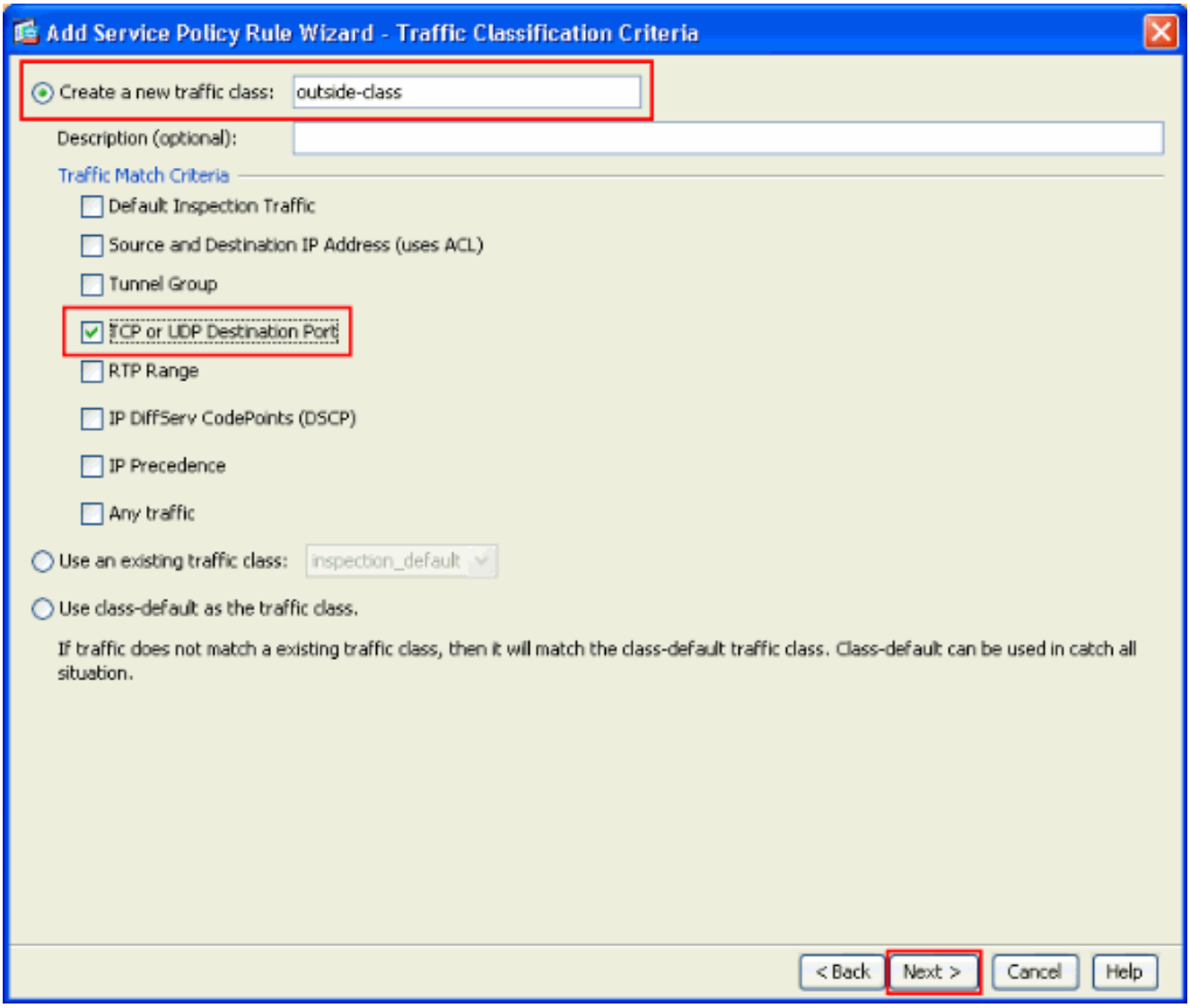
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Pour configurer l'exemple ci-dessus à l'aide d'ASDM, procédez comme suit :

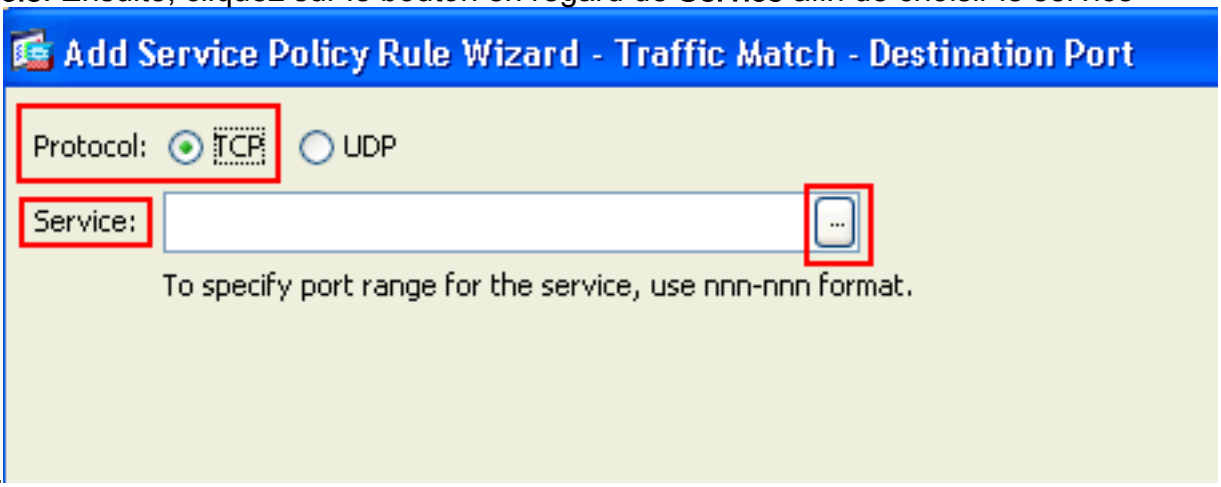
1. Choisissez **Configuration > Firewall > Service Policy Rules** et cliquez sur **Add** afin d'ajouter une nouvelle stratégie de service
   :
   
2. Dans la fenêtre Ajouter une règle de stratégie de service - Stratégie de service, sélectionnez la case d'option en regard de **Interface**. Ceci applique la stratégie créée à une interface spécifique, qui est l'interface **externe** dans cet exemple. Indiquez un nom de stratégie, qui est **outside-cisco-policy** dans cet exemple. Cliquez sur **Next**
   (Suivant).



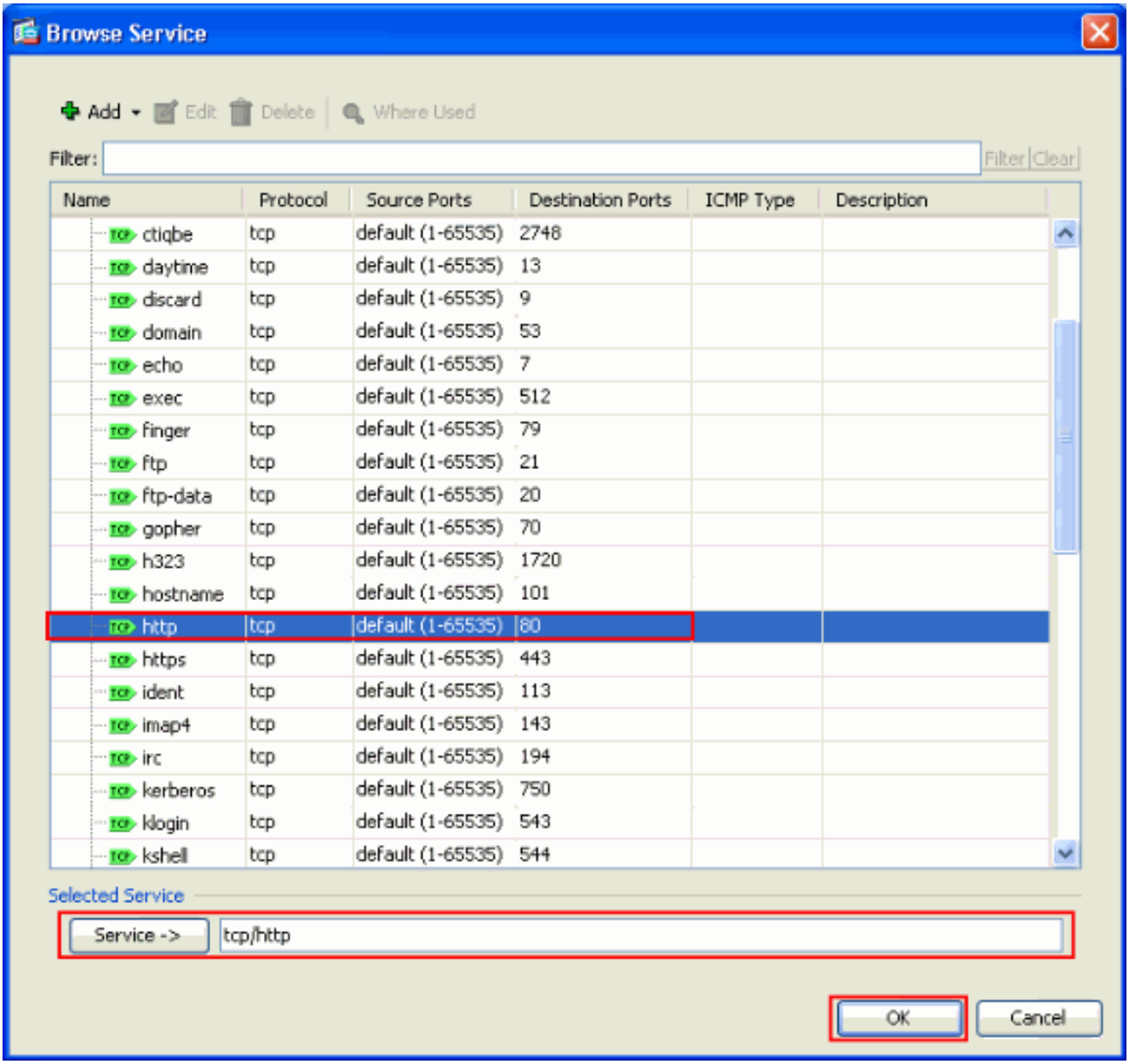
3. Dans la fenêtre Assistant Ajout de règle de stratégie de service - Critères de classification du trafic, indiquez le nouveau nom de classe de trafic. Le nom utilisé dans cet exemple est **outside-class**. Assurez-vous que la case à cocher en regard de **TCP ou UDP Destination Port** est cochée et cliquez sur **Next (Suivant)**.



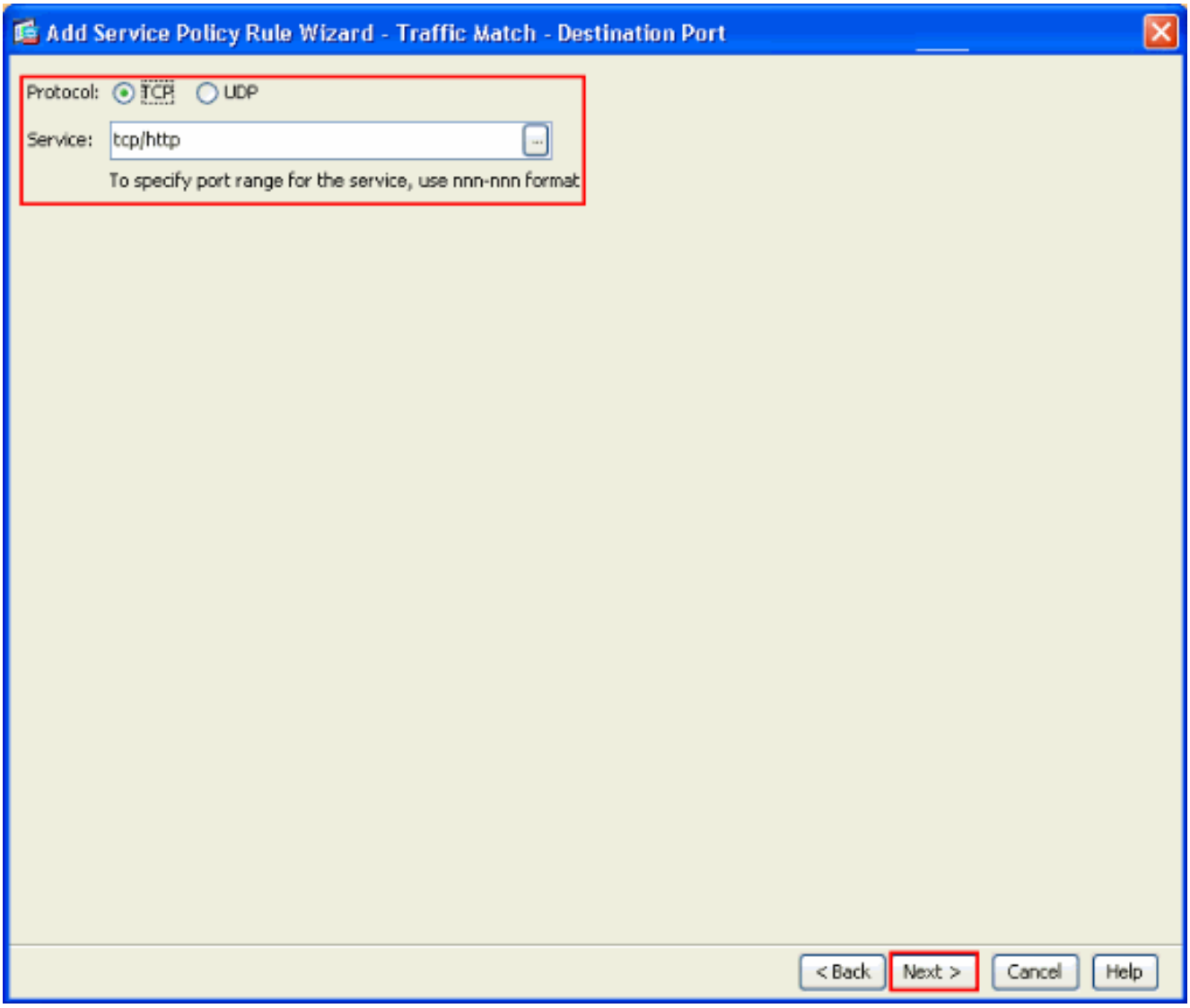
4. Dans la fenêtre Assistant Ajout de règle de stratégie de service - Correspondance du trafic - Port de destination, sélectionnez la case d'option en regard de **TCP** sous la section **Protocole**. Ensuite, cliquez sur le bouton en regard de **Service** afin de choisir le service requis.



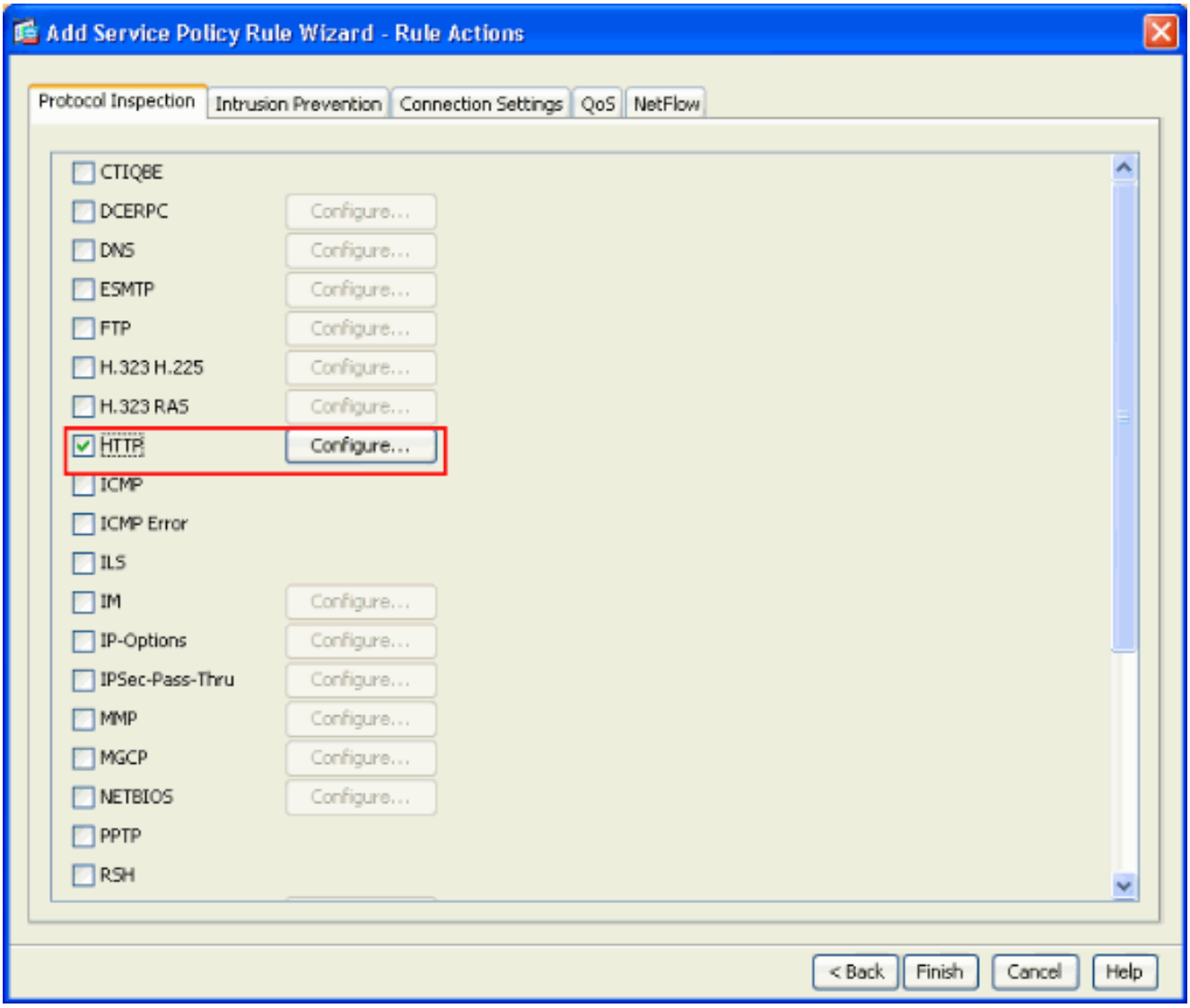
5. Dans la fenêtre Browse Service, sélectionnez **HTTP** comme service. Cliquez ensuite sur **OK**.



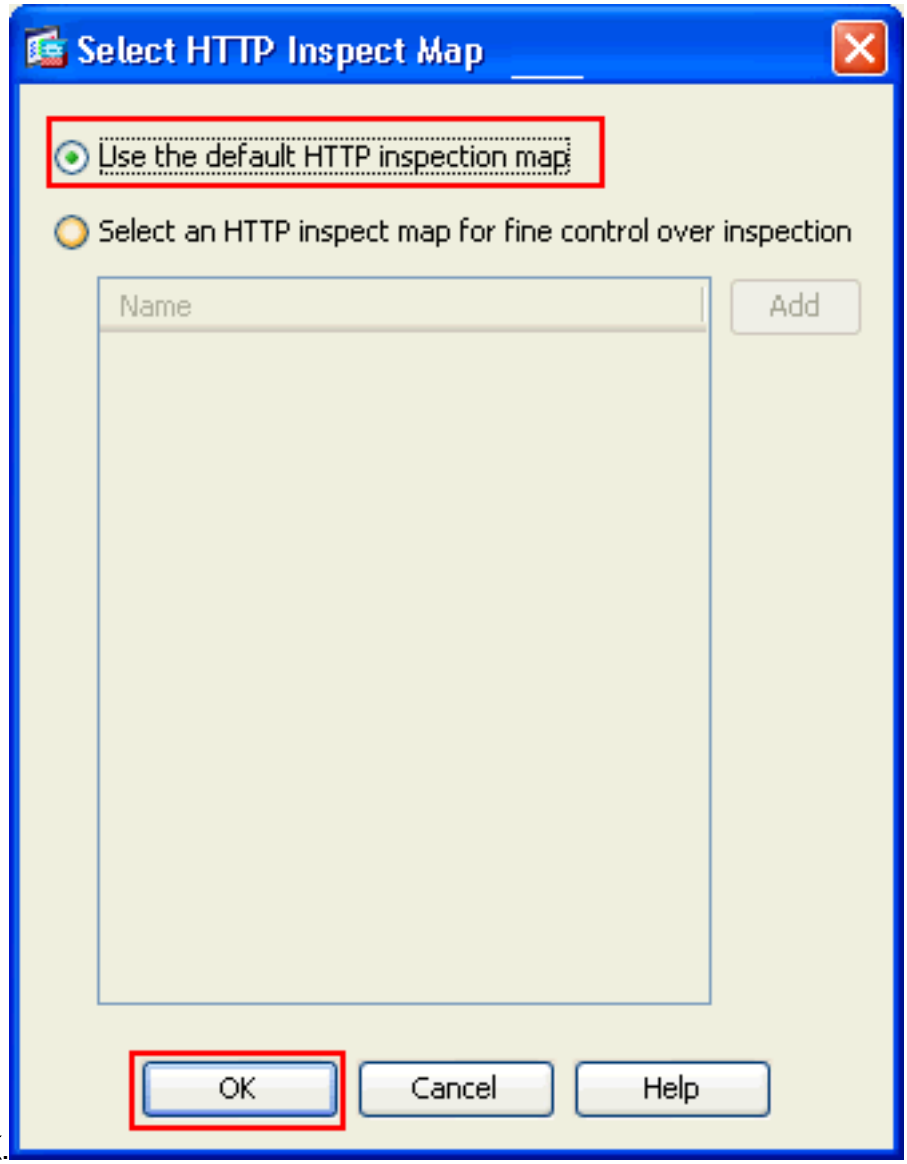
6. Dans la fenêtre Assistant Ajout de règle de stratégie de service - Correspondance du trafic - Port de destination, vous pouvez voir que le **service** choisi est **tcp/http**. Cliquez sur **Next** (Suivant).



7. Dans la fenêtre Add Service Policy Rule Wizard - Rule Actions, cochez la case en regard de **HTTP**. Ensuite, cliquez sur **Configurer** en regard de **HTTP**.

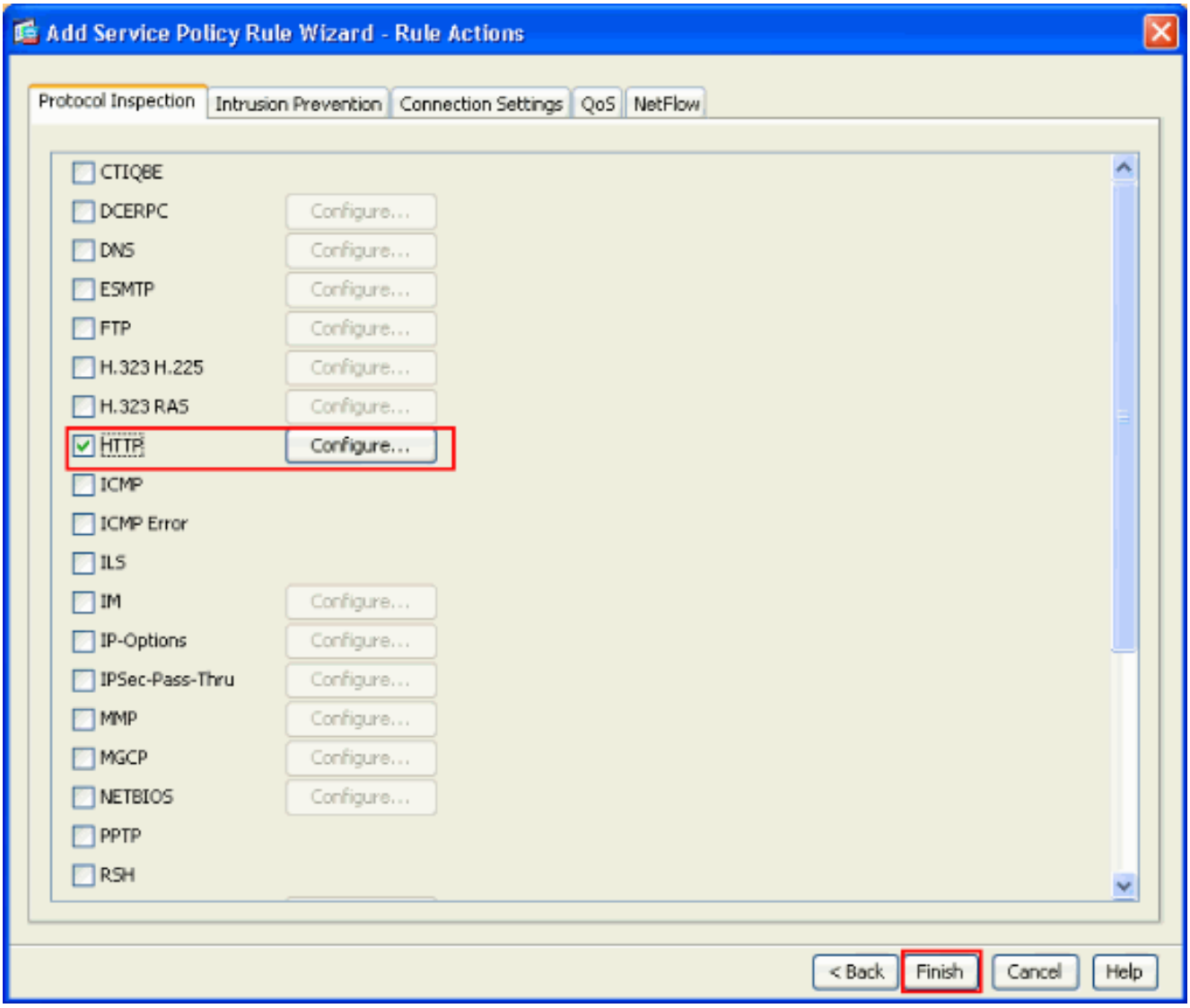


8. Dans la fenêtre Select HTTP Inspect Map, cochez la case d'option **Use the Default HTTP inspection map**. L'inspection HTTP par défaut est utilisée dans cet exemple. Cliquez ensuite

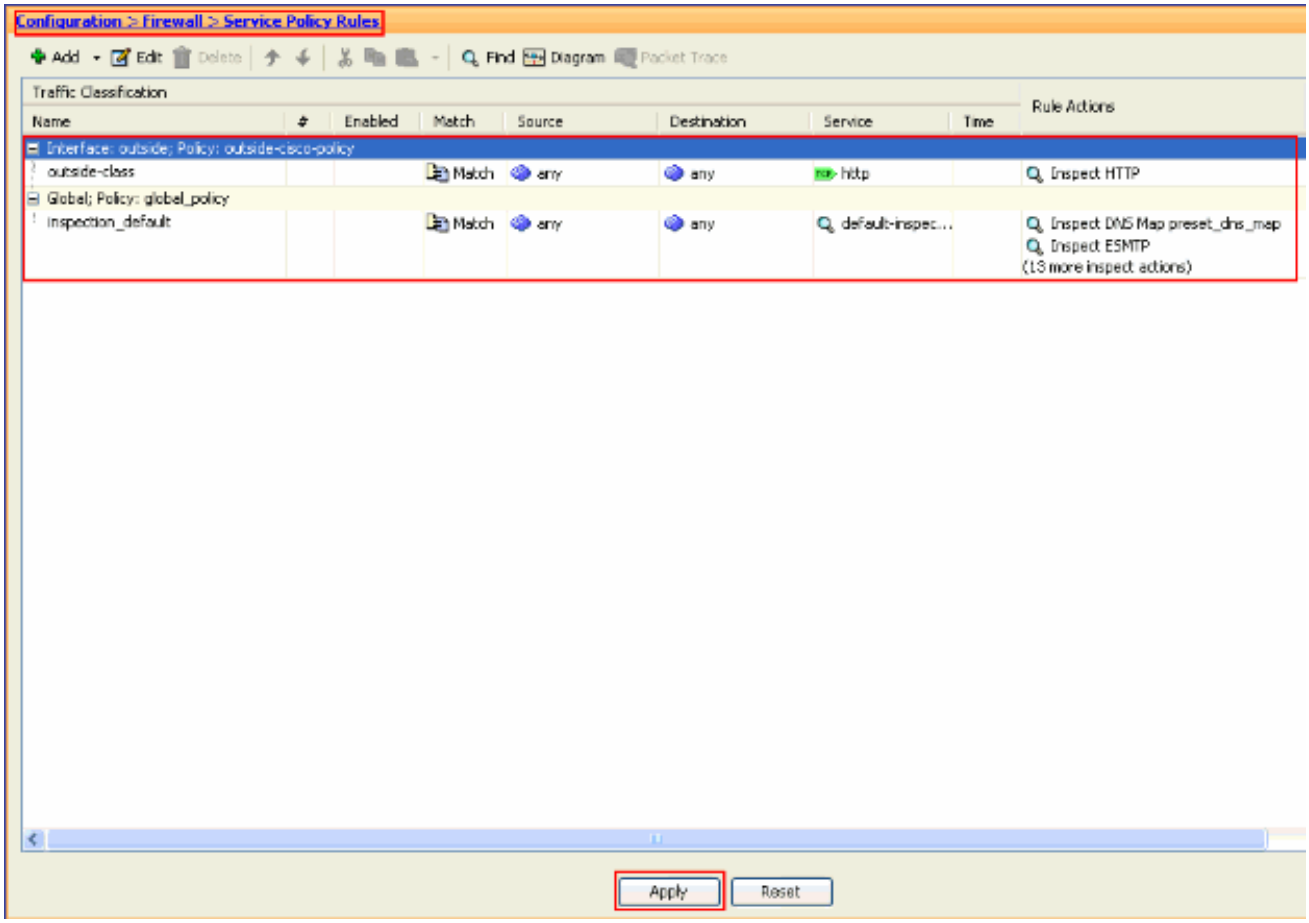


sur **OK**.

9. **Cliquez sur Finish.**



10. Sous **Configuration > Firewall > Service Policy Rules**, vous verrez la nouvelle stratégie de service **outside-cisco-policy** (pour inspecter HTTP) ainsi que la stratégie de service par défaut déjà présente sur l'appliance. Cliquez sur **Apply** afin d'appliquer la configuration à Cisco
ASA.



Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Cisco Adaptive Security Device Manager
- Demandes de commentaires (RFC)
- Application de l'inspection du protocole de couche application
- Support et documentation techniques - Cisco Systems