ASA/PIX 8.x : Exemple de configuration de blocage de certains sites Web (URL) à l'aide d'expressions régulières avec MPF

Contenu

Introduction

Ce document décrit comment configurer les dispositifs de sécurité Cisco ASA/PIX 8.x à l'aide d'expressions standards dans le cadre de règles modulaires (MPF) dans le but de bloquer certains sites Web (URL).

Remarque: Cette configuration ne bloque pas tous les téléchargements d'application. Pour le fichier fiable bloquant, une appliance dédiée telle que la série S d'Ironport ou un module tel que le module CSC pour l'ASA devrait être utilisée.

Remarque: Le filtrage HTTPS n'est pas pris en charge sur l'ASA. L'ASA ne peut pas faire l'inspection profonde de paquet ou inspection basée sur l'expression régulière pour le trafic HTTPS, parce que dans HTTPS, le contenu du paquet est chiffré (SSL).

Conditions préalables

Conditions requises

Ce document suppose que l'appliance de sécurité Cisco est configurée et fonctionne correctement.

Composants utilisés

- L'appliance de sécurité adaptable de gamme Cisco 5500 (ASA) cette exécute la version de logiciel 8.0(x) et plus tard
- Version 6.x du Cisco Adaptive Security Device Manager (ASDM) pour ASA 8.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 la gamme Cisco 500 PIX qui exécute la version de logiciel 8.0(x) et plus tard.

Conventions

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

Informations générales

Aperçu modulaire de cadre de stratégie

MPF fournit un cohérent et une façon flexible pour configurer des caractéristiques de dispositifs de sécurité. Par exemple, vous pouvez employer MPF pour créer une configuration de délai d'attente qui est spécifique à une application TCP particulière, par opposition à une qui s'applique à toutes les applications TCP.

MPF prend en charge ces caractéristiques :

- Normalisation de TCP, limites et délais d'attente de connexion de TCP et UDP, et randomisation de numéro de séquence de TCP
- CSC
- Inspection d'application
- IPS
- QoS a entré le maintien de l'ordre
- QoS a sorti le maintien de l'ordre
- File d'attente prioritaire de QoS

La configuration du MPF se compose de quatre tâches :

1. Identifiez la couche 3 et le trafic 4 auquel vous voulez s'appliquer des actions. Référez-vous à identifier le trafic utilisant un pour en savoir plus de class map de la couche 3/4.
2. (Inspection d'application seulement) définissez les actions spéciales pour le trafic d'inspection d'application. Référez-vous à configurer des actions spéciales pour le pour en

savoir plus d'inspections d'application.

3. Appliquez les actions à la couche 3 et le trafic 4. Référez-vous à définir des actions utilisant un pour en savoir plus de carte de stratégie de la couche 3/4.
4. Lancez les actions sur une interface. Référez-vous à s'appliquer une stratégie de la couche 3/4 à une interface utilisant un pour en savoir plus de stratégie de service.

Expression régulière

Une expression régulière apparie des chaînes de texte littéralement comme chaîne précise, ou en employant des métacaractères ainsi vous pouvez apparier de plusieurs variantes d'une chaîne de texte. Vous pouvez employer une expression régulière pour apparier le contenu de certain trafic de l'application ; par exemple, vous pouvez apparier une chaîne d'URL à l'intérieur d'un paquet de HTTP.

Remarque: Employez **Ctrl+V** afin d'échapper à tous les caractères particuliers dans le CLI, tel que le point d'interrogation (?) ou une tableau par exemple, le type **d [Ctrl+V] ? g** afin d'écrire **d ? g** dans la configuration.

Pour la création d'une expression régulière, utilisez la commande d'**expression régulière**, qui peut être utilisée pour différentes caractéristiques qui exigent apparier des textes. Par exemple, vous pouvez configurer des actions spéciales pour l'inspection d'application avec l'utilisation du cadre de stratégie modulaire qui utilise une carte de stratégie d'inspection. Référez-vous au **type de carte de stratégie examinent le** pour en savoir plus de commande. Dans la carte de stratégie d'inspection, vous pouvez identifier le trafic que vous voulez agir au moment si vous créez un class map d'inspection qui contient un ou plusieurs **commandes match** ou vous pouvez utiliser des **commandes match** directement dans la carte de stratégie d'inspection. Quelques **commandes match** vous ont permis d'identifier le texte dans un paquet utilisant une expression régulière ; par exemple, vous pouvez des chaînes de match url à l'intérieur des paquets de HTTP. Vous pouvez grouper des expressions régulières dans un class map d'expression régulière. Référez-vous au pour en savoir plus de commande d'**expression régulière de type de class-map**.

Ce tableau présente les métacaractères qui ont des significations particulières.

Caractère	Description	Notes
.	Point	Correspond à n'importe quel caractère unique. Par exemple, **d.g apparie le** chien, le dag, le dtg, et n'importe quel mot qui contient ces caractères, tels que le doggonnit.
(exp)	Subexpression	Un subexpression isole des caractères des caractères environnants, de sorte que vous puissiez utiliser d'autres métacaractères sur le subexpression. Par exemple, **d (o|**le chien de correspondances **a) g** et le dag, mais **font|**les correspondances **AG** font et AG. Un subexpression peut également être utilisé avec des quantificateurs de répétition pour différencier les caractères signifiés pour la répétition. Par exemple,

		ab(xy){3}z apparie l'abxyxyxyz.
|	Alternance	Apparie l'un ou l'autre d'expression qu'elle sépare. Par exemple, **chien|le cat** apparie le chien ou le cat.
?	Point d'interrogation	Un quantificateur qui indique qu'il y a 0 ou de 1 de l'expression précédente. Par exemple, **lo ? l'expert en logiciel** apparie le LSE ou le perd. **Remarque:** Vous devez écrire **Ctrl+V** et puis le point d'interrogation ou bien la fonction d'aide est appelé.
*	Astérisque	Un quantificateur qui indique qu'il y a 0, de 1 ou un certain nombre d'expression précédente. Par exemple, le **lo*se** apparie le LSE, perdent, lâche, et ainsi de suite.
{x}	Quantificateur de répétition	De la répétition temps exactement x. Par exemple, **ab(xy){3}z** apparie l'abxyxyxyz.
{x,}	Quantificateur minimum de répétition	Temps de la répétition au moins x. Par exemple, **ab(xy){2,}z** apparie l'abxyxyz, abxyxyxyz, et ainsi de suite.
[ABC]	Classe de caractères	Apparie n'importe quel caractère dans les crochets. Par exemple, **[ABC]** apparie a, b, ou C.
[^abc]	Classe de caractères réalisée une inversion	Apparie un caractère unique qui n'est pas contenu dans les crochets. Par exemple, **[^abc]** apparie n'importe quel caractère autre qu'a, b, ou C. **[^A-Z]** apparie n'importe quel caractère unique qui n'est pas une lettre majuscule.
[courant alternatif]	Classe de chaîne de caractère	Apparie n'importe quel caractère dans la plage. **[a-z]** apparie n'importe quelle lettre minuscule. Vous pouvez mélanger des caractères et des plages : **[abcq-z]** apparie a, b, c, q, r, s, t, u, v, W, x, y, z, et ainsi fait **[un-CQ-z]**. Le caractère de tiret (-) est littéral seulement si c'est le bout ou le premier caractère dans les crochets : **[ABC]** ou **[- ABC]**.
""	Guillemets	Conserves traînant ou menant les espaces dans la chaîne. Par exemple, le **« test »** préserve le principal espace

		quand il recherche une correspondance.
^	Caret	Spécifie le début d'une ligne
\	Caractère d'échappement	Une fois utilisé avec un métacaractère, apparie un caractère littéral. Par exemple, **\ [**apparie le crochet de carré de gauche.
car	Caractère	Quand le caractère n'est pas un métacaractère, apparie le caractère littéral.
\ **r**	Retour chariot	Apparie un retour chariot 0x0d
\ **n**	Saut de ligne	Apparie une nouvelle ligne 0x0a
\ **t**	Onglet	Apparie un onglet 0x09
\ **f**	Chargement de page	Apparie une alimentation papier 0x0c
\ xNN	Nombre hexadécimal échappé	Apparie un caractère ASCII qui utilise un hexadécimal qui est exactement deux chiffres
\ NNN	Nombre octal échappé	Apparie un caractère ASCII car octal qui est exactement trois chiffres. Par exemple, le caractère 040 représente un espace.

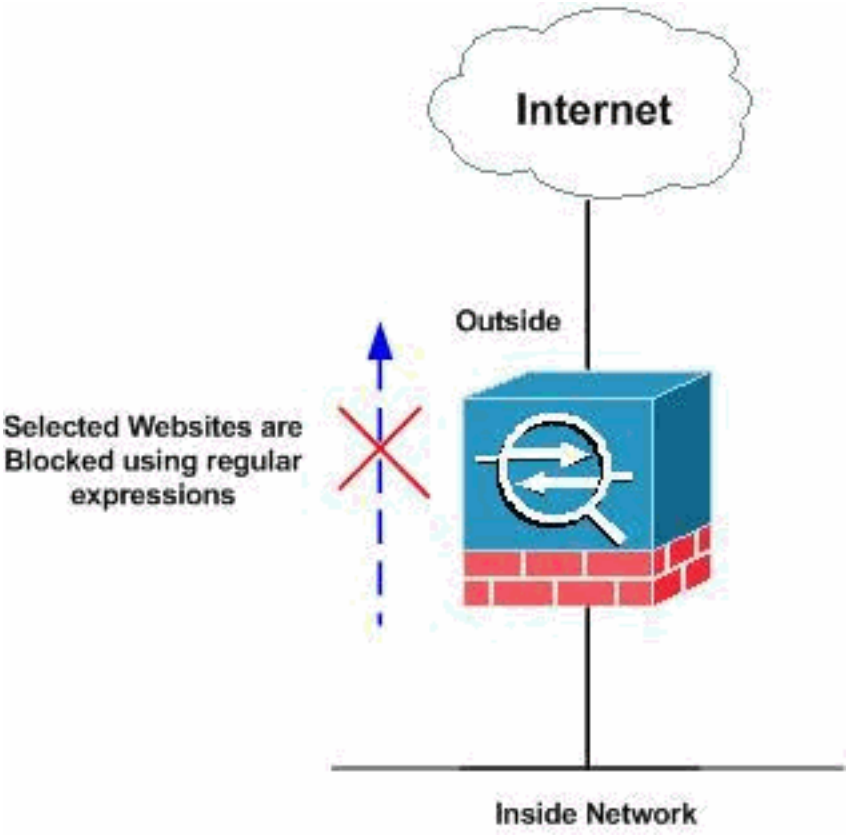
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- Configuration de l'interface de ligne de commande ASA
- Configuration 8.x ASA avec ASDM 6.x

Configuration de l'interface de ligne de commande ASA

Configuration de l'interface de ligne de commande ASA

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa domain-name
default.domain.invalid enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.5 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 90 ip address
10.77.241.142 255.255.255.192 ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
regex urllist1
".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt])
HTTP/1.[01]" !--- Extensions such as .exe, .com, .bat to
be captured and !--- provided the http version being
used by web browser must be either 1.0 or 1.1 regex
urllist2 ".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh])
HTTP/1.[01]" !--- Extensions such as .pif, .vbs, .wsh to
be captured !--- and provided the http version being
used by web browser must be either !--- 1.0 or 1.1 regex
urllist3 ".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt])
HTTP/1.[01]" !--- Extensions such as .doc(word),
```

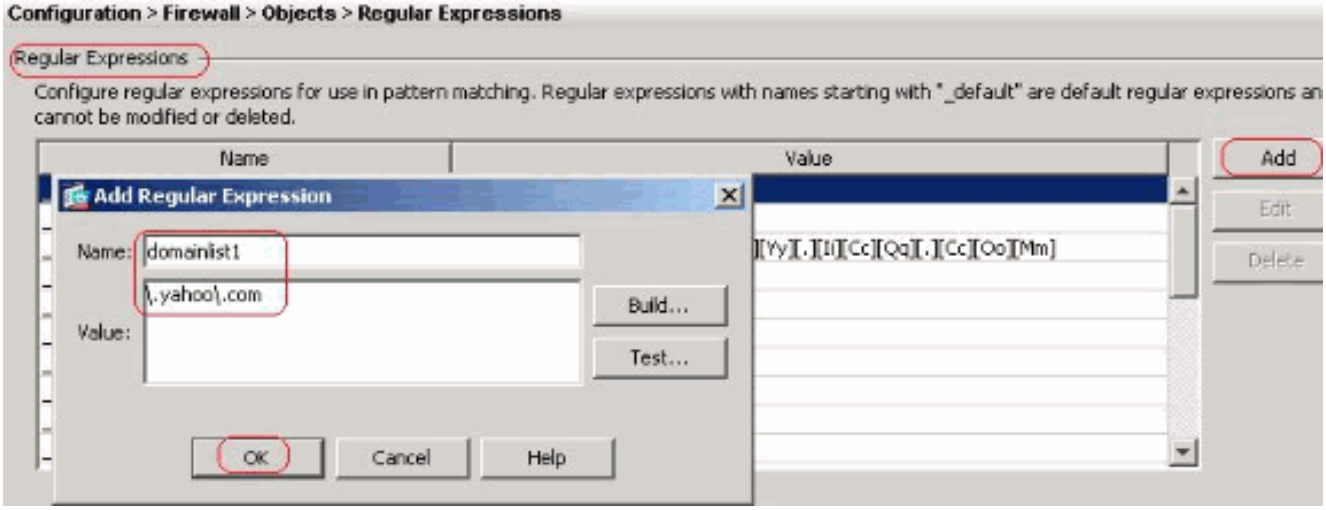
```
.xls(ms-excel), .ppt to be captured and provided !---
the http version being used by web browser must be
either 1.0 or 1.1 regex urllist4
".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz])
HTTP/1.[01]" !--- Extensions such as .zip, .tar, .tgz to
be captured and provided !--- the http version being
used by web browser must be either 1.0 or 1.1 regex
domainlist1 "\.yahoo\.com" regex domainlist2
"\.myspace\.com" regex domainlist3 "\.youtube\.com" !---
Captures the URLs with domain name like yahoo.com, !---
youtube.com and myspace.com regex contenttype "Content-
Type" regex applicationheader "application/.*" !---
Captures the application header and type of !--- content
in order for analysis boot system disk0:/asa802-k8.bin
ftp mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list inside_mpc extended
permit tcp any any eq www access-list inside_mpc
extended permit tcp any any eq 8080 !--- Filters the
http and port 8080 !--- traffic in order to block the
specific traffic with regular !--- expressions pager
lines 24 mtu inside 1500 mtu outside 1500 mtu DMZ 1500
no failover icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin no asdm history enable
arp timeout 14400 route DMZ 0.0.0.0 0.0.0.0
10.77.241.129 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute dynamic-access-policy-
record DfltAccessPolicy http server enable http 0.0.0.0
0.0.0.0 DMZ no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart no crypto isakmp nat-traversal
telnet timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map type regex match-any
DomainBlockList match regex domainlist1 match regex
domainlist2 match regex domainlist3 !--- Class map
created in order to match the domain names !--- to be
blocked class-map type inspect http match-all
BlockDomainsClass match request header host regex class
DomainBlockList !--- Inspect the identified traffic by
class !--- "DomainBlockList". class-map type regex
match-any URLBlockList match regex urllist1 match regex
urllist2 match regex urllist3 match regex urllist4 !---
Class map created in order to match the URLs !--- to be
blocked class-map inspection_default match default-
inspection-traffic class-map type inspect http match-all
AppHeaderClass match response header regex contenttype
regex applicationheader !--- Inspect the captured
traffic by regular !--- expressions "content-type" and
"applicationheader". class-map httptraffic match access-
list inside_mpc !--- Class map created in order to match
the !--- filtered traffic by ACL class-map type inspect
http match-all BlockURLsClass match request uri regex
class URLBlockList ! !--- Inspect the identified traffic
by class !--- "URLBlockList". ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map type inspect http http_inspection_policy
parameters protocol-violation action drop-connection
class AppHeaderClass drop-connection log match request
method connect drop-connection log class
BlockDomainsClass reset log class BlockURLsClass reset
```

```
log !--- Define the actions such as drop, reset or log
!--- in the inspection policy map. policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp policy-map
inside-policy class httptraffic inspect http
http_inspection_policy !--- Map the inspection policy
map to the class !--- "httptraffic" under the policy map
created for the !--- inside network traffic. ! service-
policy global_policy global service-policy inside-policy
interface inside !--- Apply the policy to the interface
inside where the websites are blocked. prompt hostname
context Cryptochecksum:e629251a7c37af205c289cf78629fc11
: end ciscoasa#
```

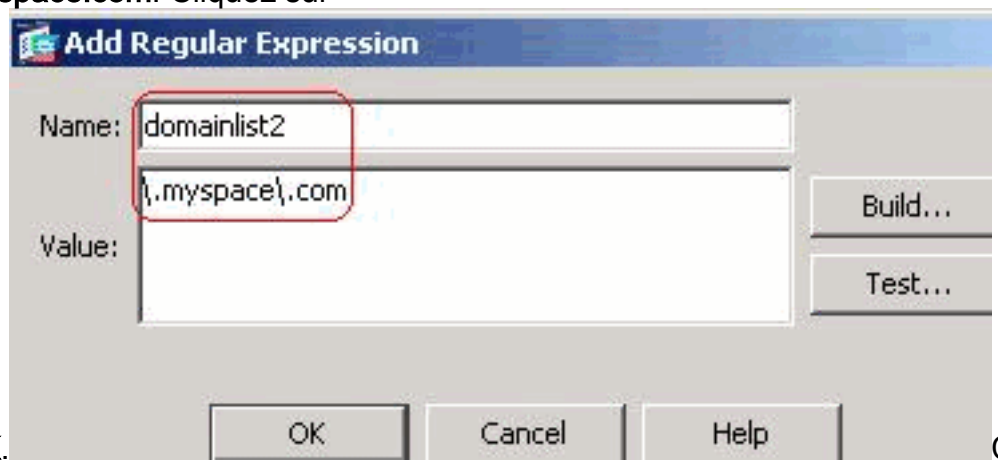
Configuration 8.x ASA avec ASDM 6.x

Terminez-vous ces étapes afin de configurer les expressions régulières et les appliquer dans MPF pour bloquer les sites Web spécifiques comme affichés.

1. **Créez les expressions régulières**Choisissez la **configuration > le Firewall> objecte > des expressions régulières** et clique sur Add sous l'**expression régulière d'**onglet afin de créer des expressions régulières comme affichées.Créez une expression régulière **domainlist1** afin de capturer le nom de domaine **yahoo.com**. Cliquez sur **OK**.

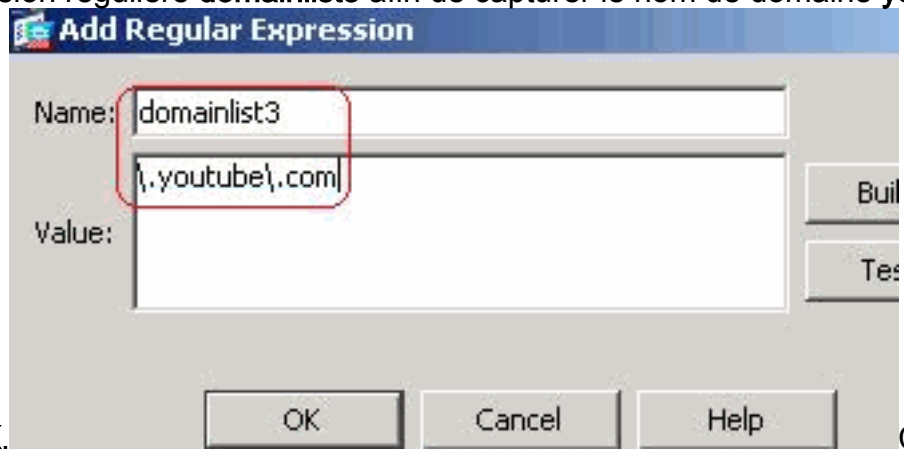


Créez une expression régulière **domainlist2** afin de capturer le nom de domaine **myspace.com**. Cliquez sur **OK**.

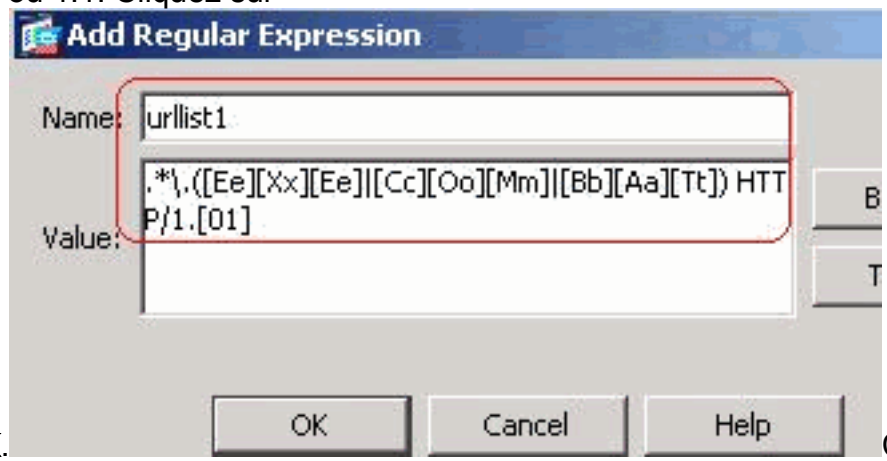


Créez une

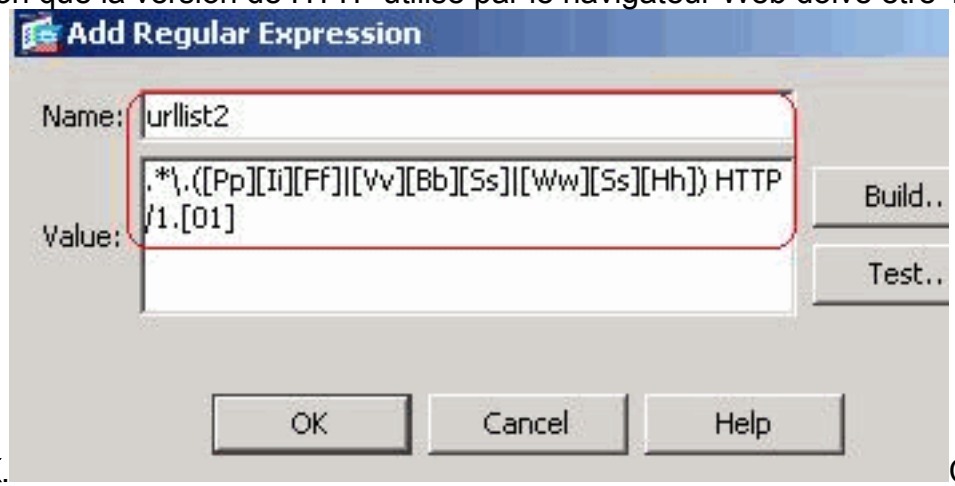
expression régulière **domainlist3** afin de capturer le nom de domaine **youtube.com**. Cliquez sur **OK**.



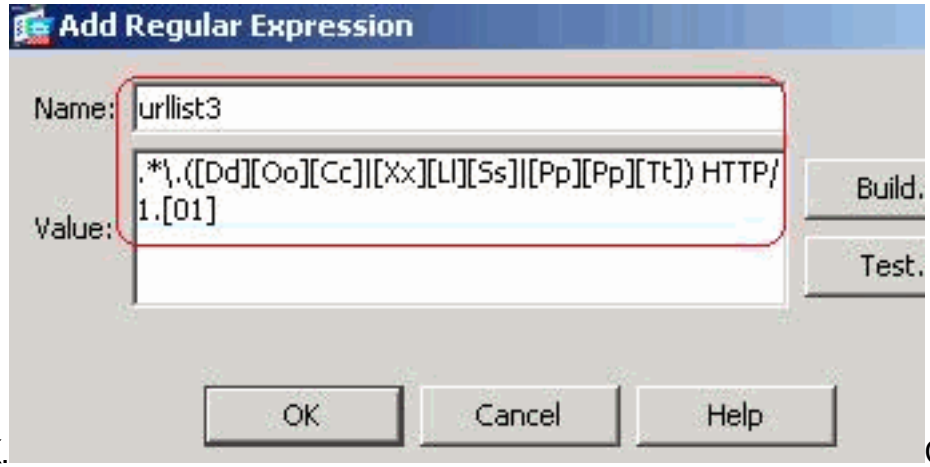
Créez une expression régulière **urllist1** afin de capturer les extensions de fichier telles que l'**exe**, la **COM** et la **chauve-souris** à condition que la version de HTTP utilisé par le navigateur Web doive être 1.0 ou 1.1. Cliquez sur **OK**.



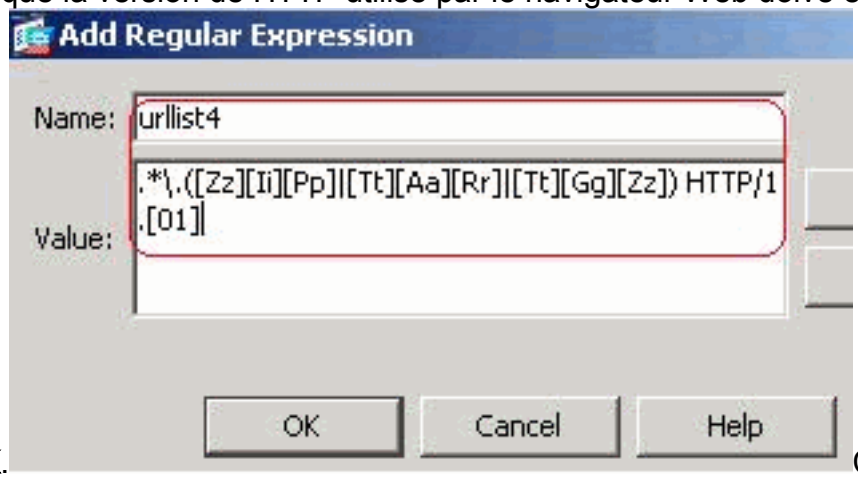
Créez une expression régulière **urllist2** afin de capturer les extensions de fichier telles que **pif**, les **vbs** et le **wsh** à condition que la version de HTTP utilisé par le navigateur Web doive être 1.0 ou 1.1. Cliquez sur **OK**.



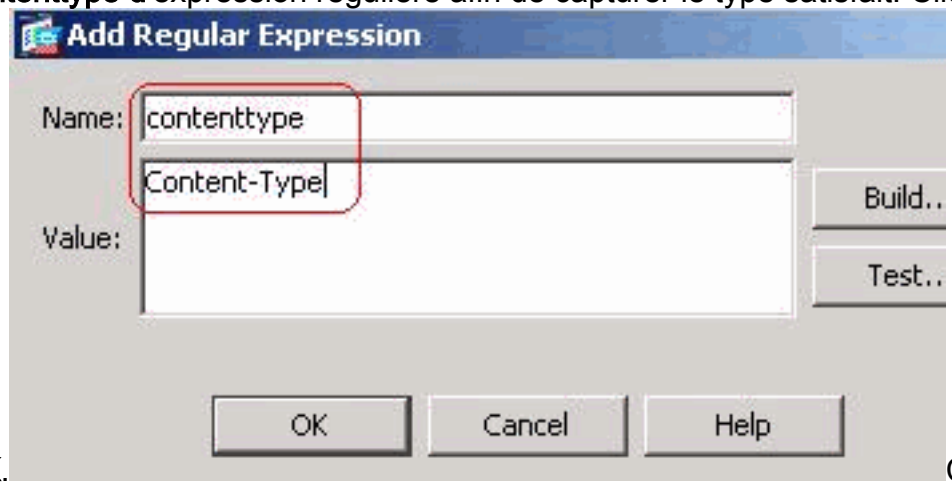
Créez une expression régulière **urllist3** afin de capturer les extensions de fichier telles que la **documentation**, les **xls** et le **PPT** à condition que la version de HTTP utilisé par le navigateur Web doive être 1.0 ou 1.1. Cliquez sur



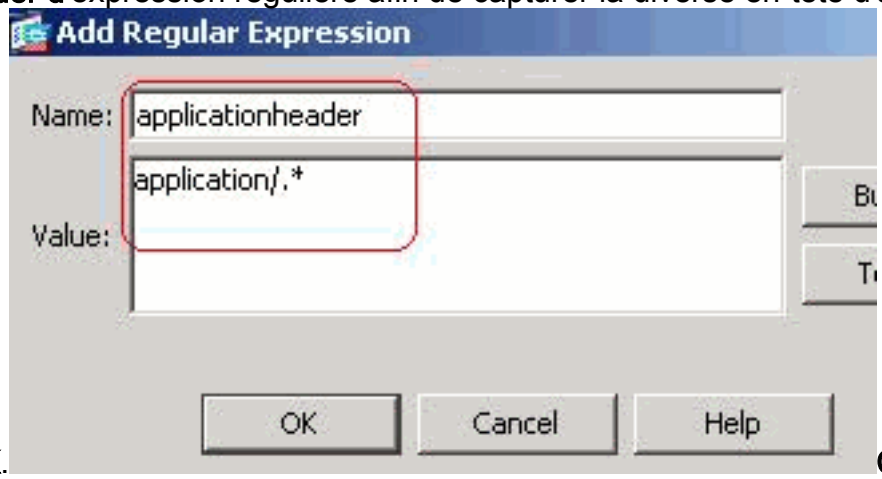
OK. Créez une expression régulière **urllist4** afin de capturer les extensions de fichier telles que le **zip**, le **goudron** et le **tgz** à condition que la version de HTTP utilisé par le navigateur Web doive être 1.0 ou 1.1.



Cliquez sur **OK**. Créez un **contenttype d'**expression régulière afin de capturer le type satisfait. Cliquez sur



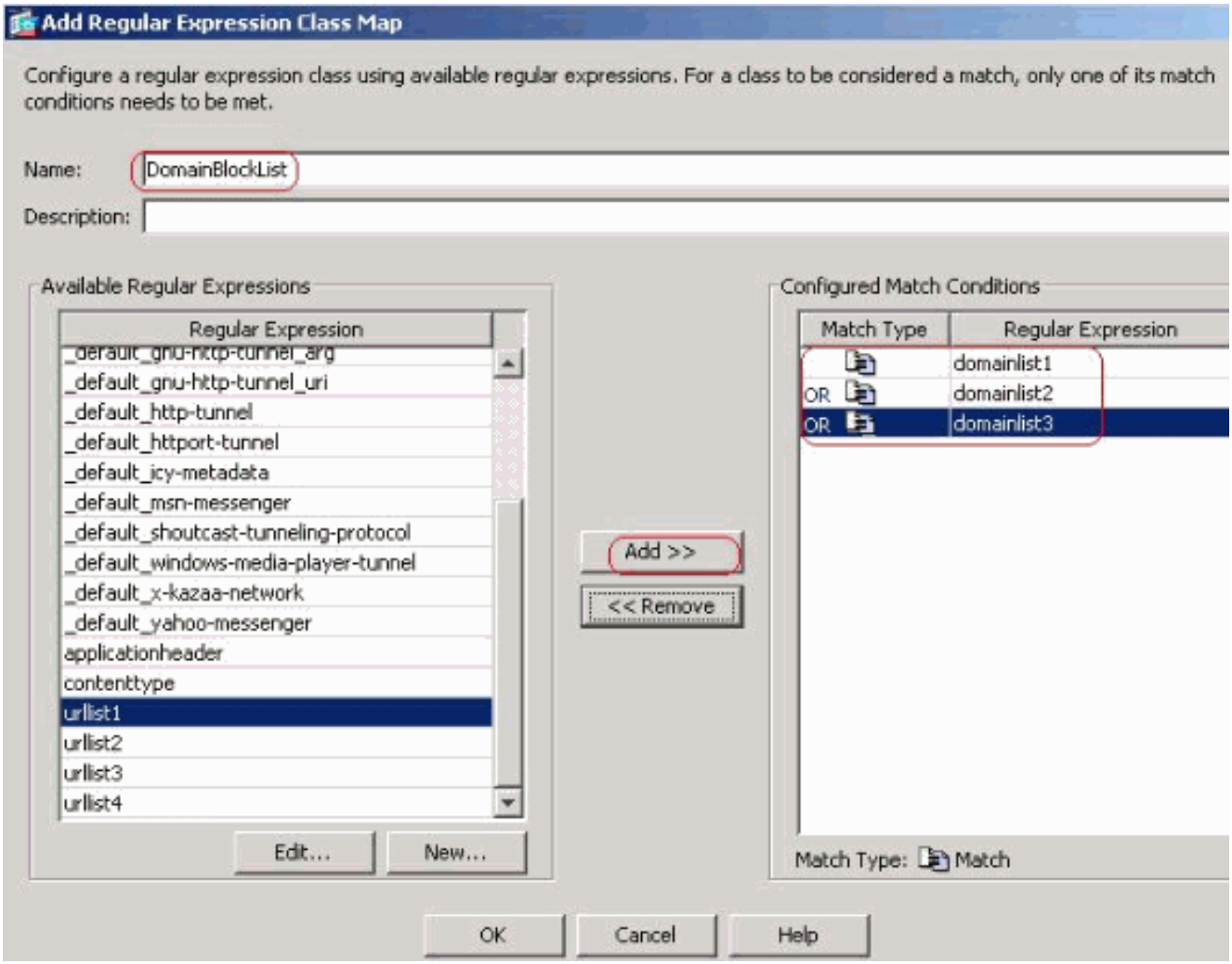
OK. Créez un **applicationheader d'**expression régulière afin de capturer la diverse en-tête d'application.



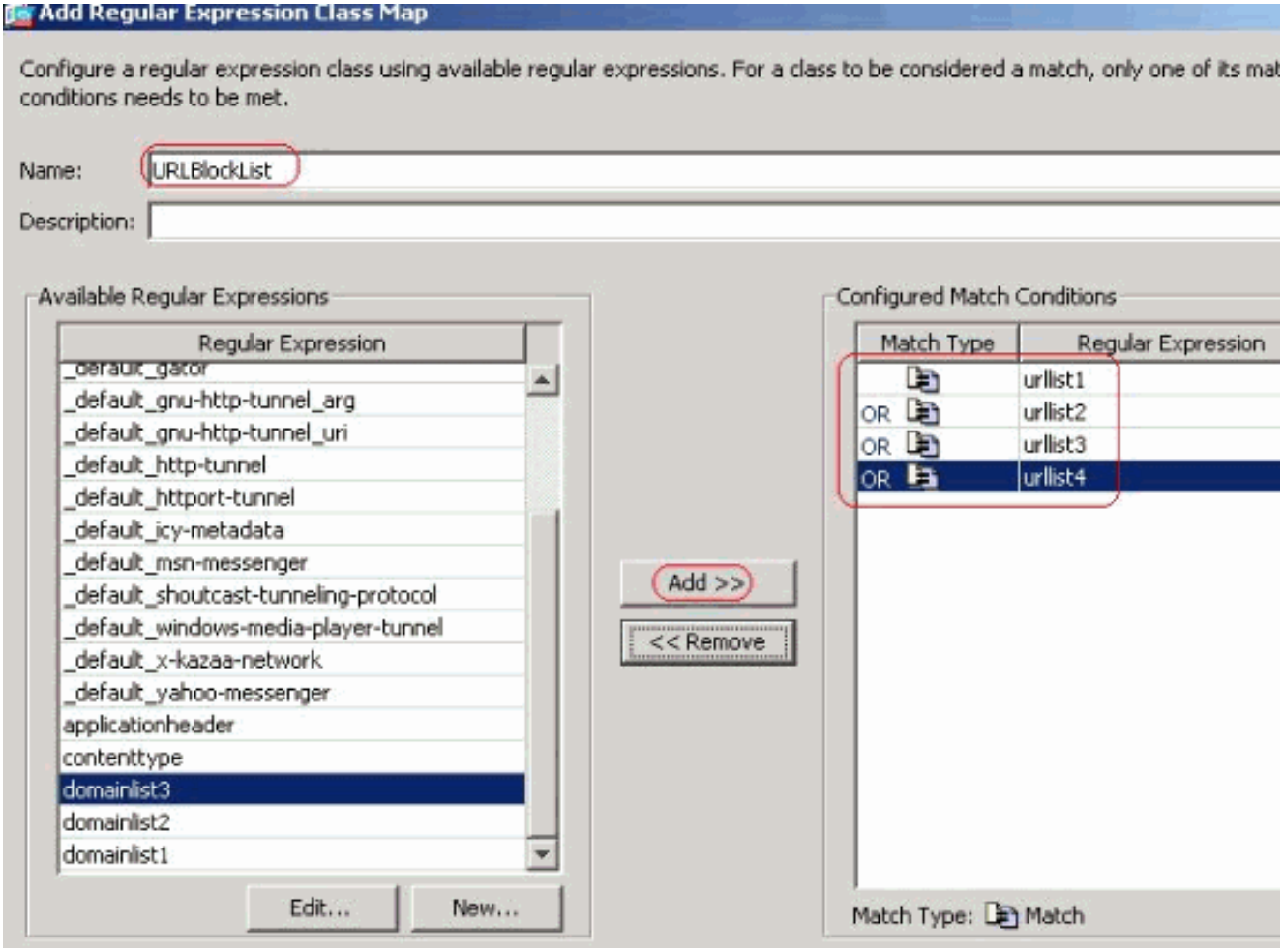
Cliquez sur **OK**. **Configuration**

équivalente CLI

2. **Créez les classes d'expression régulière**Choisissez la **configuration > le Pare-feu > les objets > les expressions régulières** et cliquez sur Add sous les **classes d'expression régulière d'**onglet afin de créer les diverses classes comme affichées.Créez une classe **DomainBlockList d'**expression régulière afin d'apparier les expressions régulières l'unes des domainlist1, domainlist2 et domainlist3. Cliquez sur **OK**.

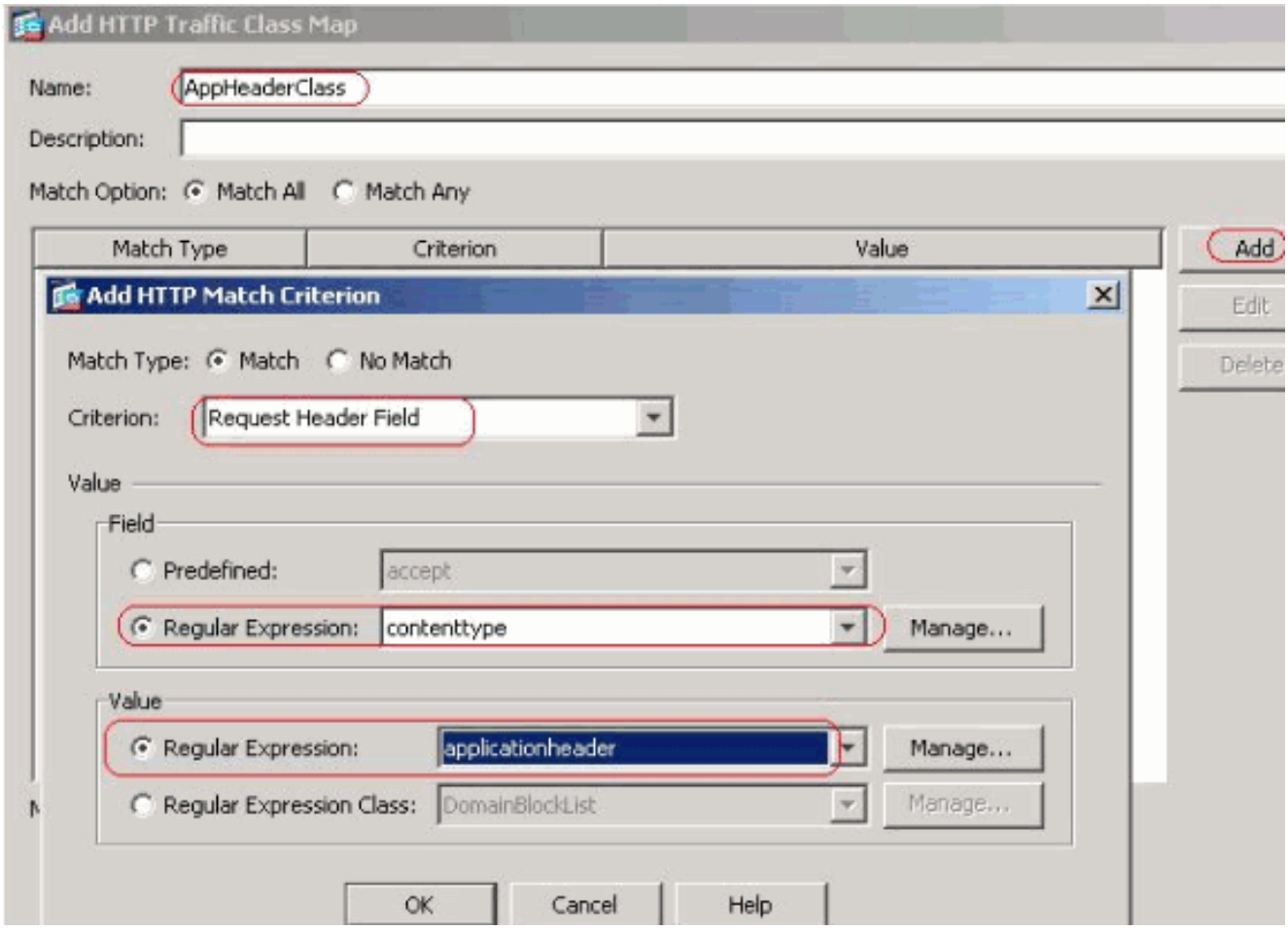


Créez une classe **URLBlockList d'**expression régulière afin d'apparier les expressions régulières l'unes des urllist1, urllist2, urllist3 et urllist4. Cliquez sur **OK**.

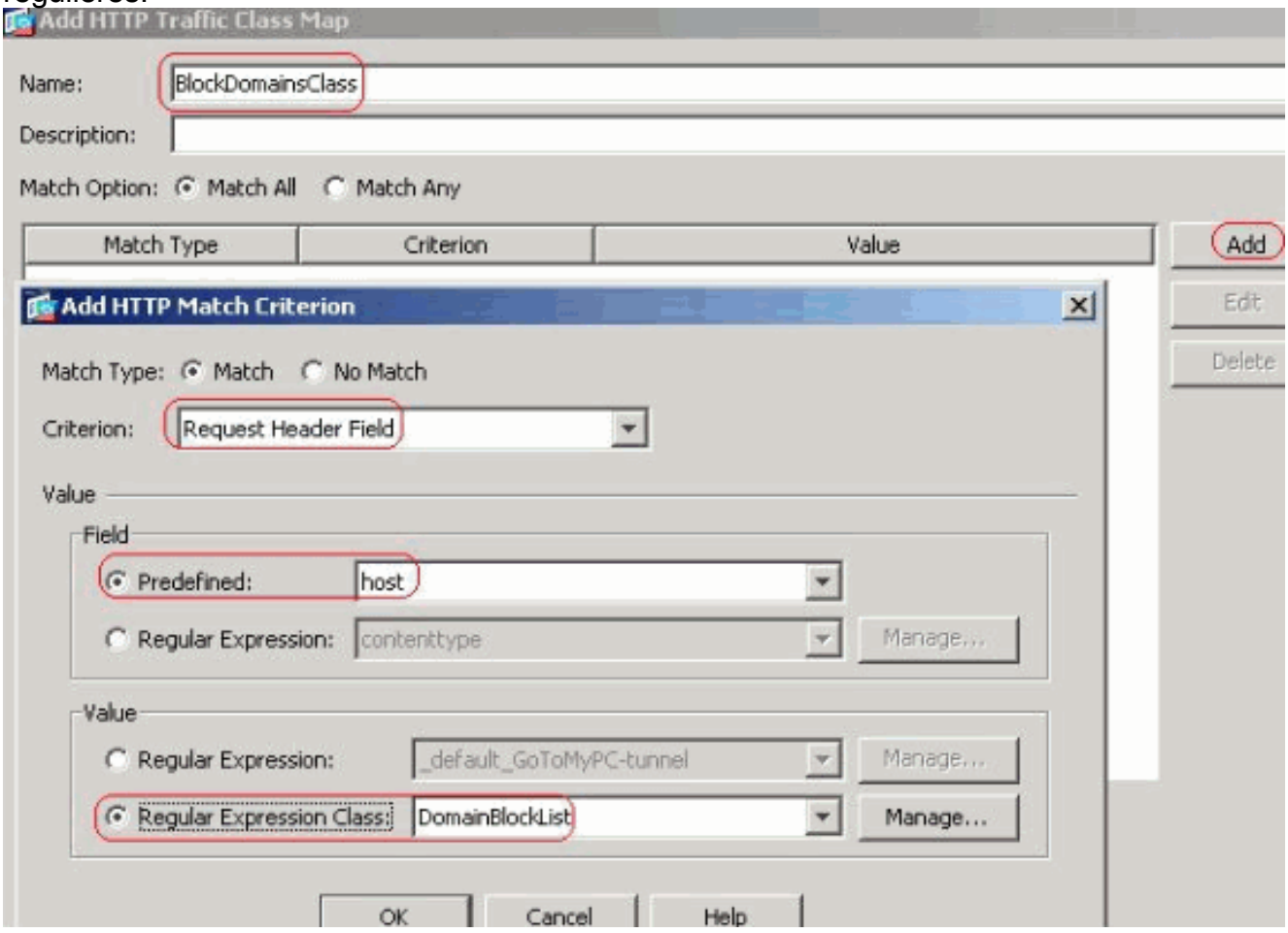


Configuration équivalente CLI

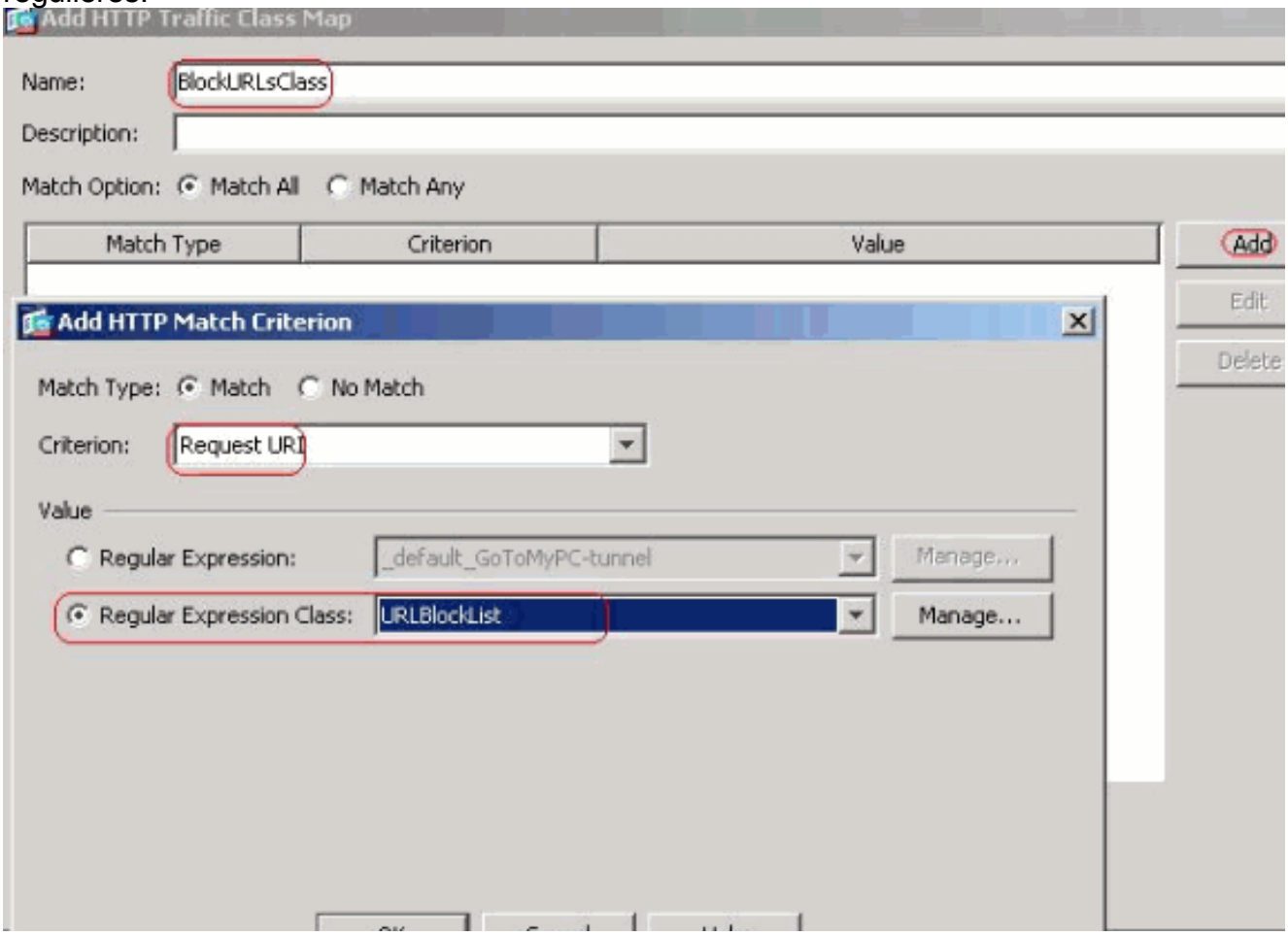
3. **Examinez le trafic identifié avec des class map**Choisissez la **configuration > le Pare-feu > les objets > les class map > le HTTP > ajoutent** afin de créer un class map pour examiner le trafic http identifié par de diverses expressions régulières comme affichées.Créez un class map **AppHeaderClass** afin d'apparier l'en-tête de réponse avec des captures d'expressions régulières.



Cliquez sur OKCréez un class map **BlockDomainsClass** afin d'apparier l'en-tête de demande avec des captures d'expressions
régulières.

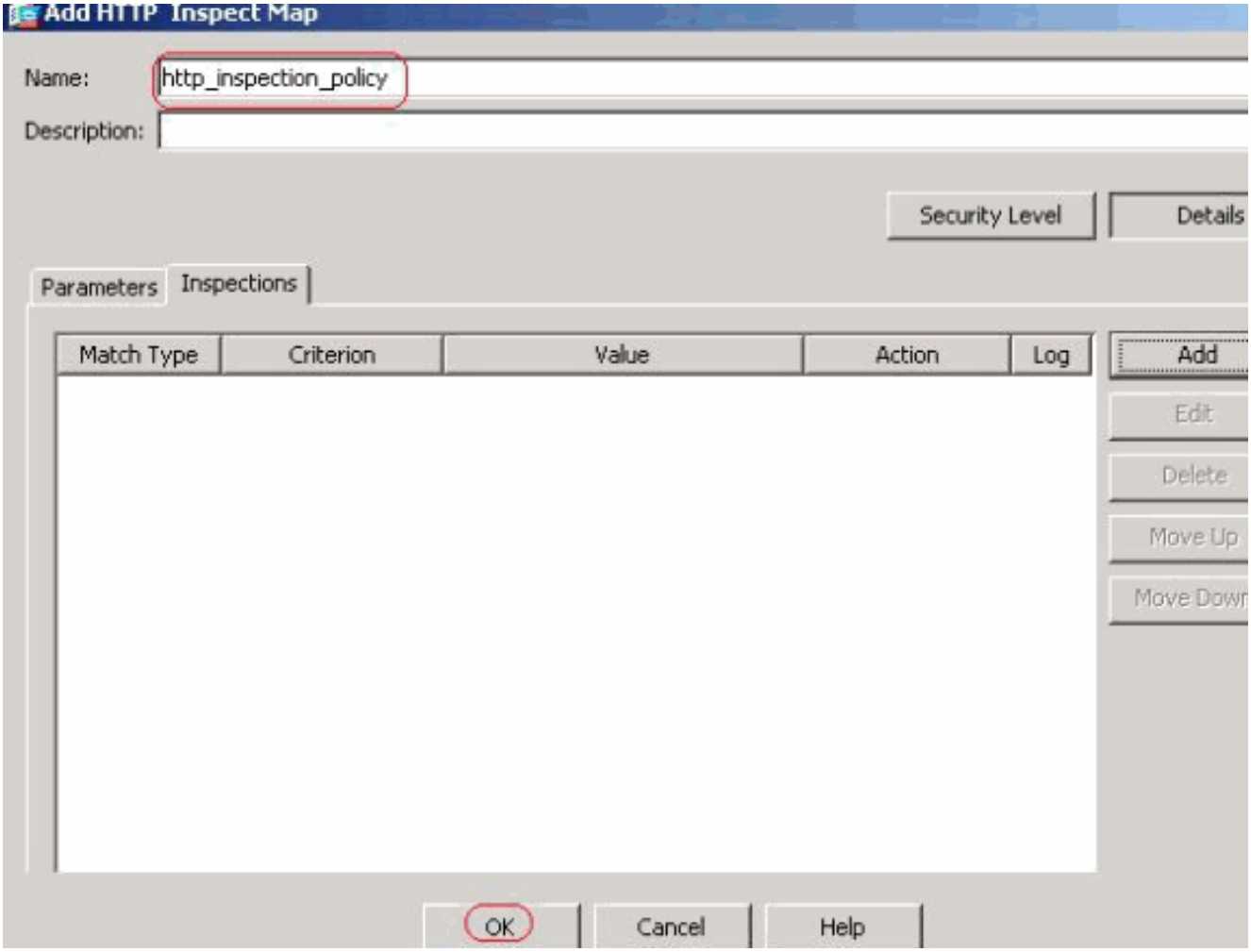


Cliquez sur **OK**.Créez un class map **BlockURLsClass** afin d'apparier l'uri de demande avec des captures d'expressions
régulières.

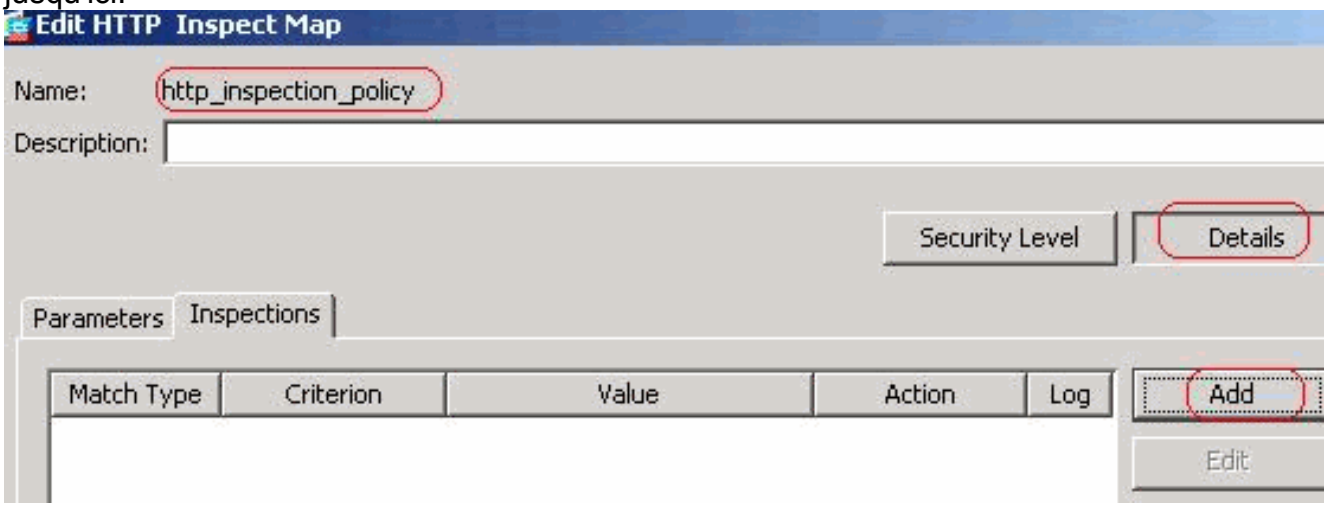


Cliquez sur **OK**.**Configuration équivalente CLI**

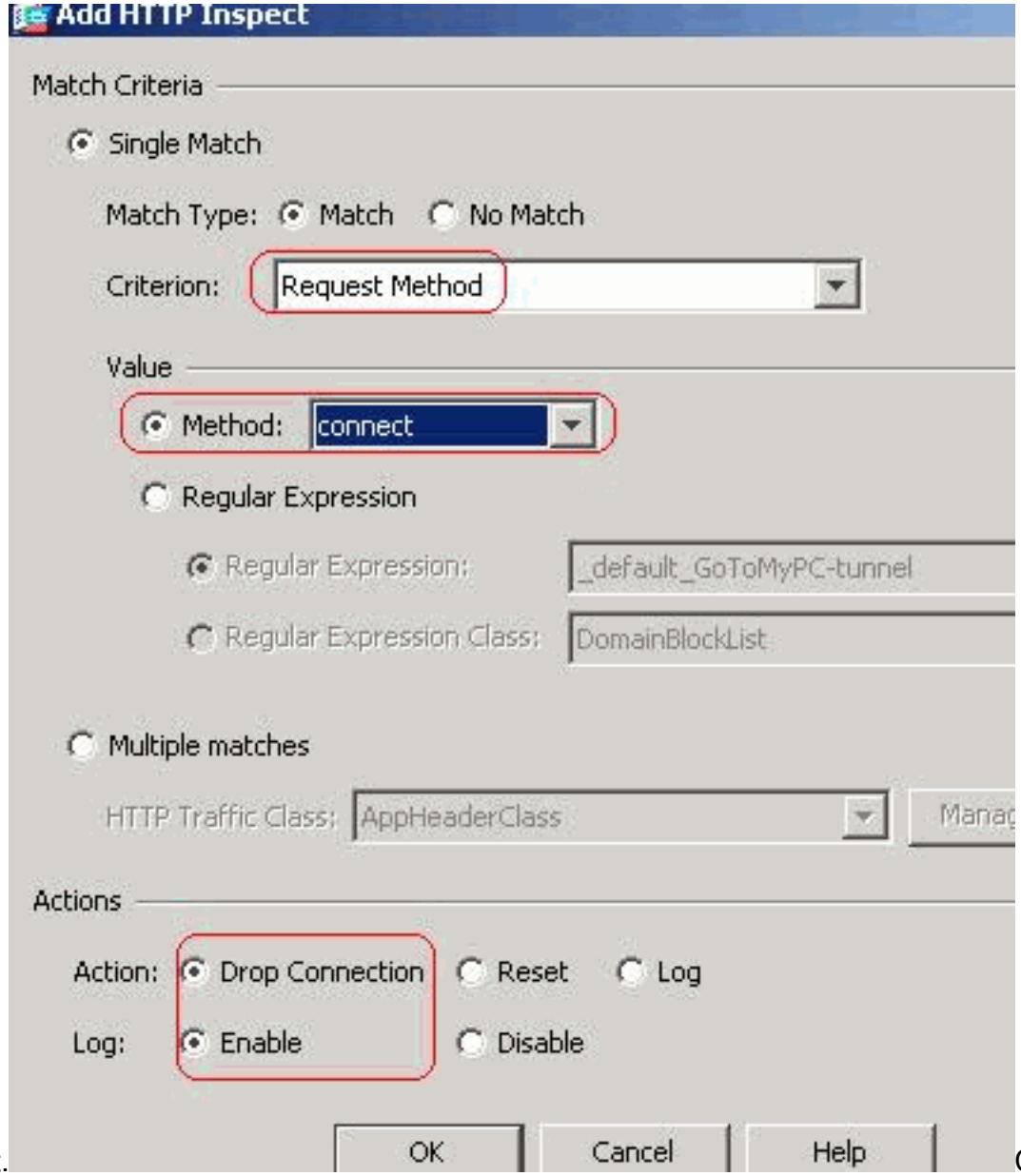
4. **Placez les actions pour le trafic apparié dans la stratégie d'inspection**Choisissez la **configuration > le Pare-feu > les objets > examinent des cartes > le HTTP** afin de créer un **http_inspection_policy** pour placer l'action pour le trafic apparié comme affiché. Cliquez sur **OK**.



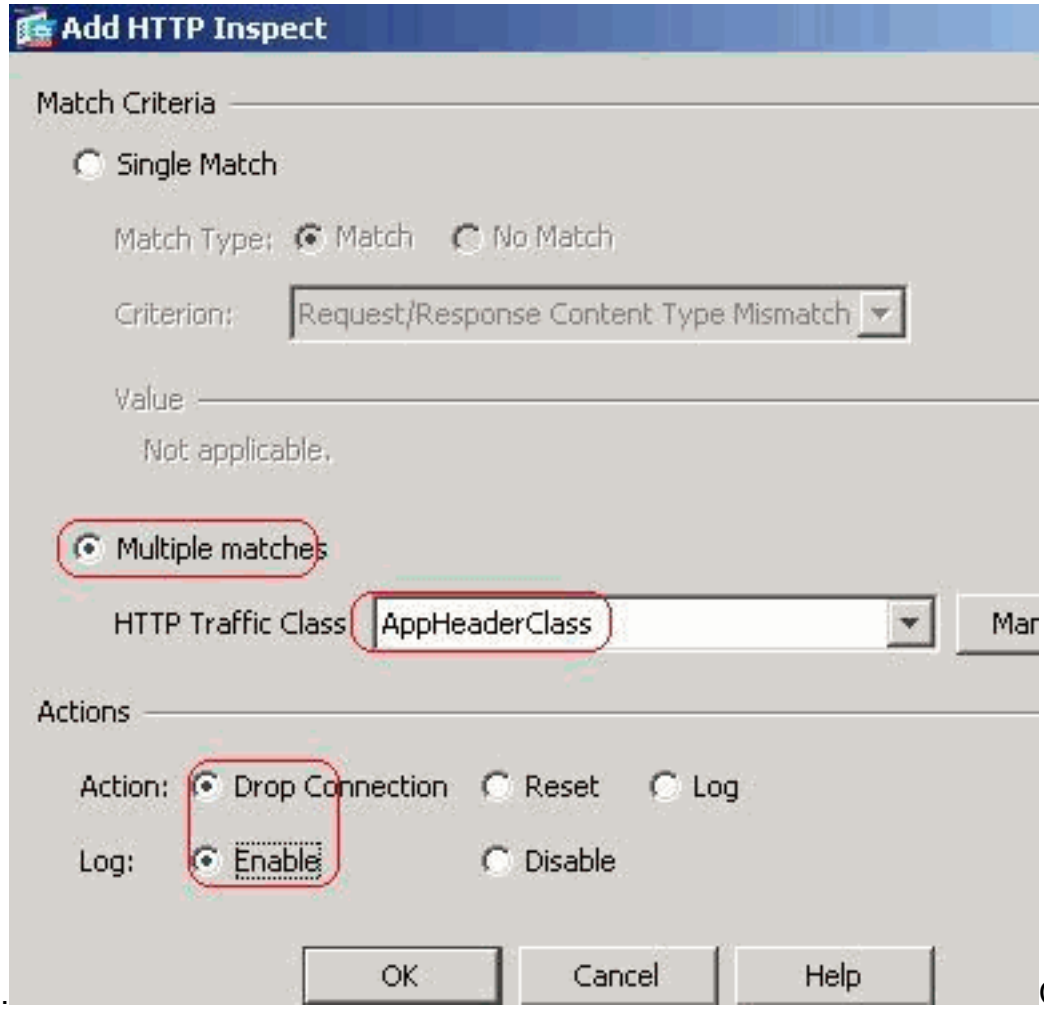
Choisissez la **configuration > le Pare-feu > les objets > examinent des cartes > le HTTP > le http_inspection_policy (double-cliquer)** et les **détails de** clic **> ajoutent** afin de placer les actions pour les diverses classes créées
jusqu'ici.



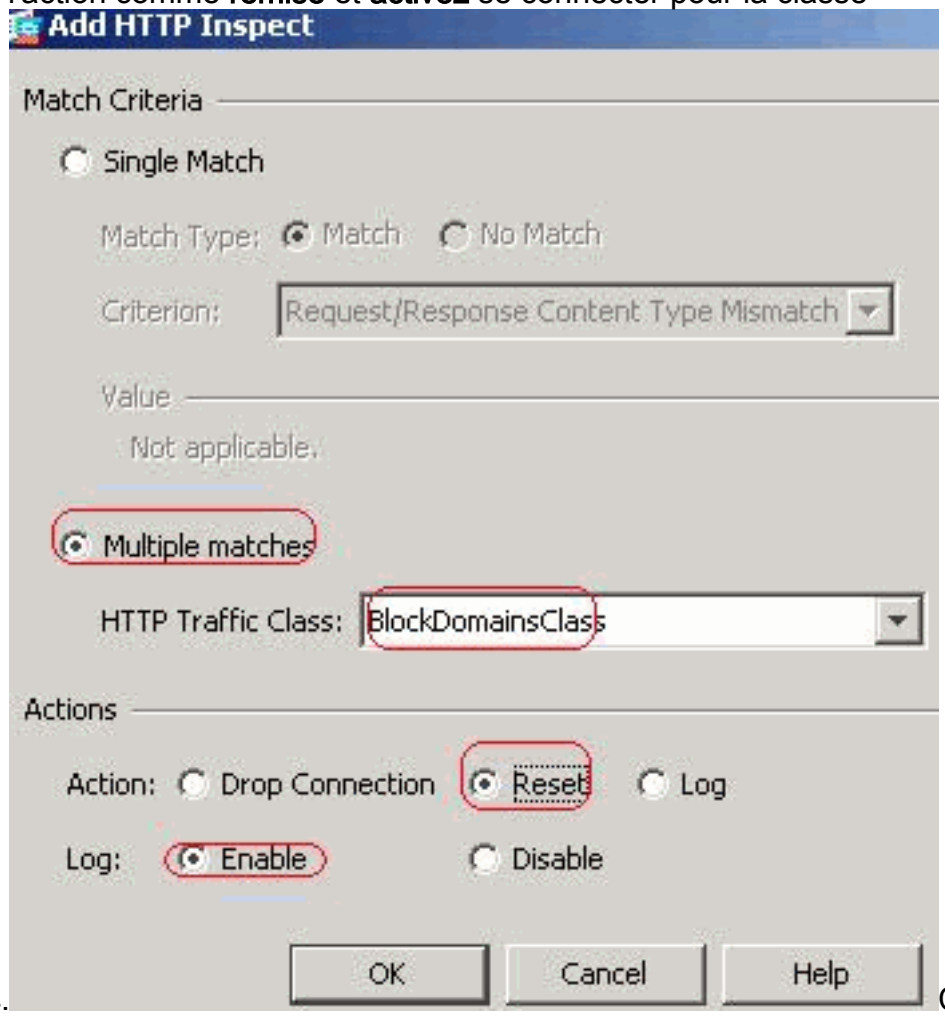
Placez l'action comme **connexion de baisse** et **activez** se connecter pour le critère comme méthode et valeur de demande comme se



connectent. Cliquez sur OKPlacez l'action comme **connexion de baisse** et **activez** se connecter pour la classe

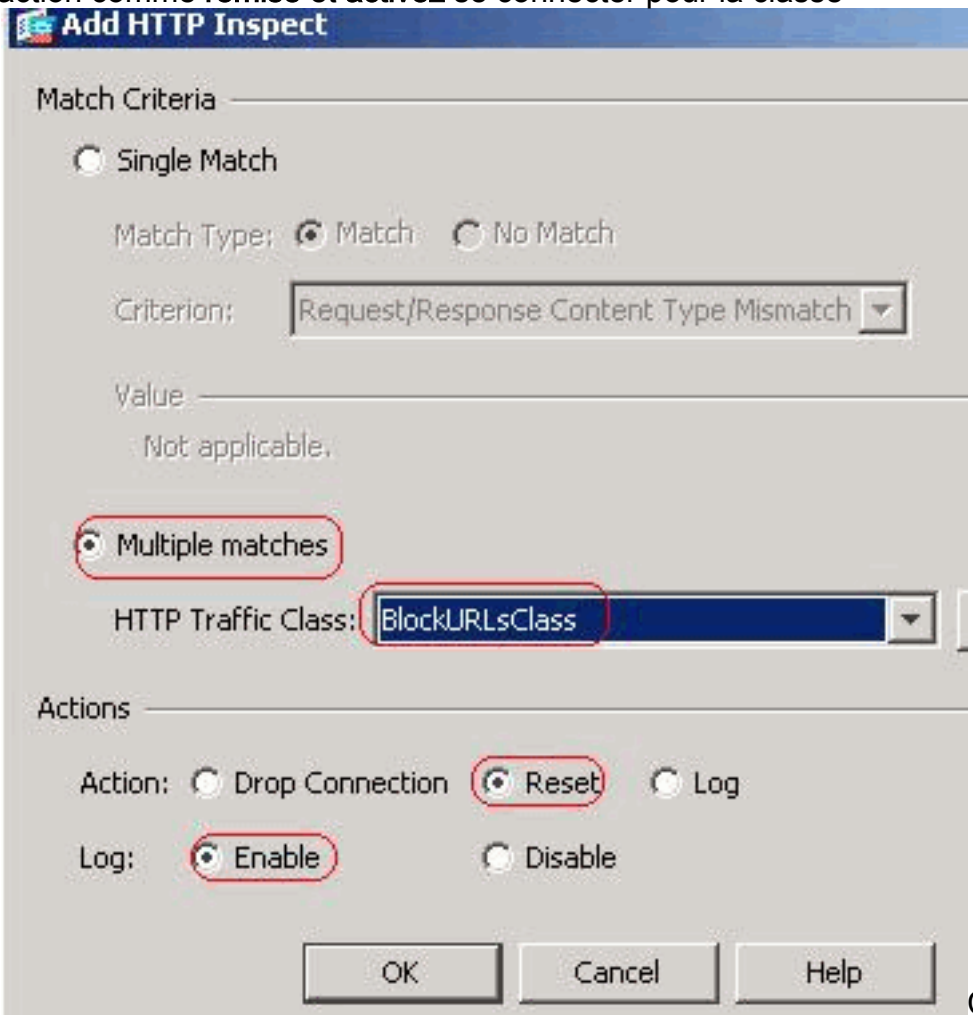


AppHeaderClass. Cliquez sur **OK**.Placez l'action comme **remise** et **activez** se connecter pour la classe



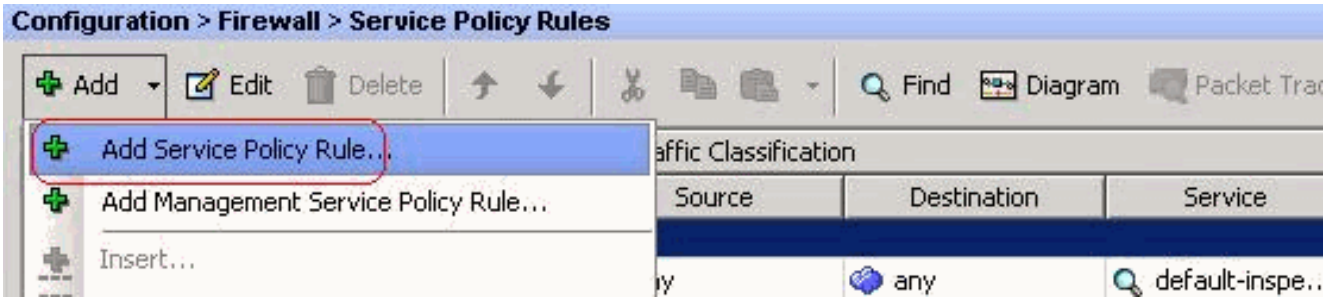
BlockDomainsClass. Clique

z sur OKPlacez l'action comme **remise** et **activez** se connecter pour la classe

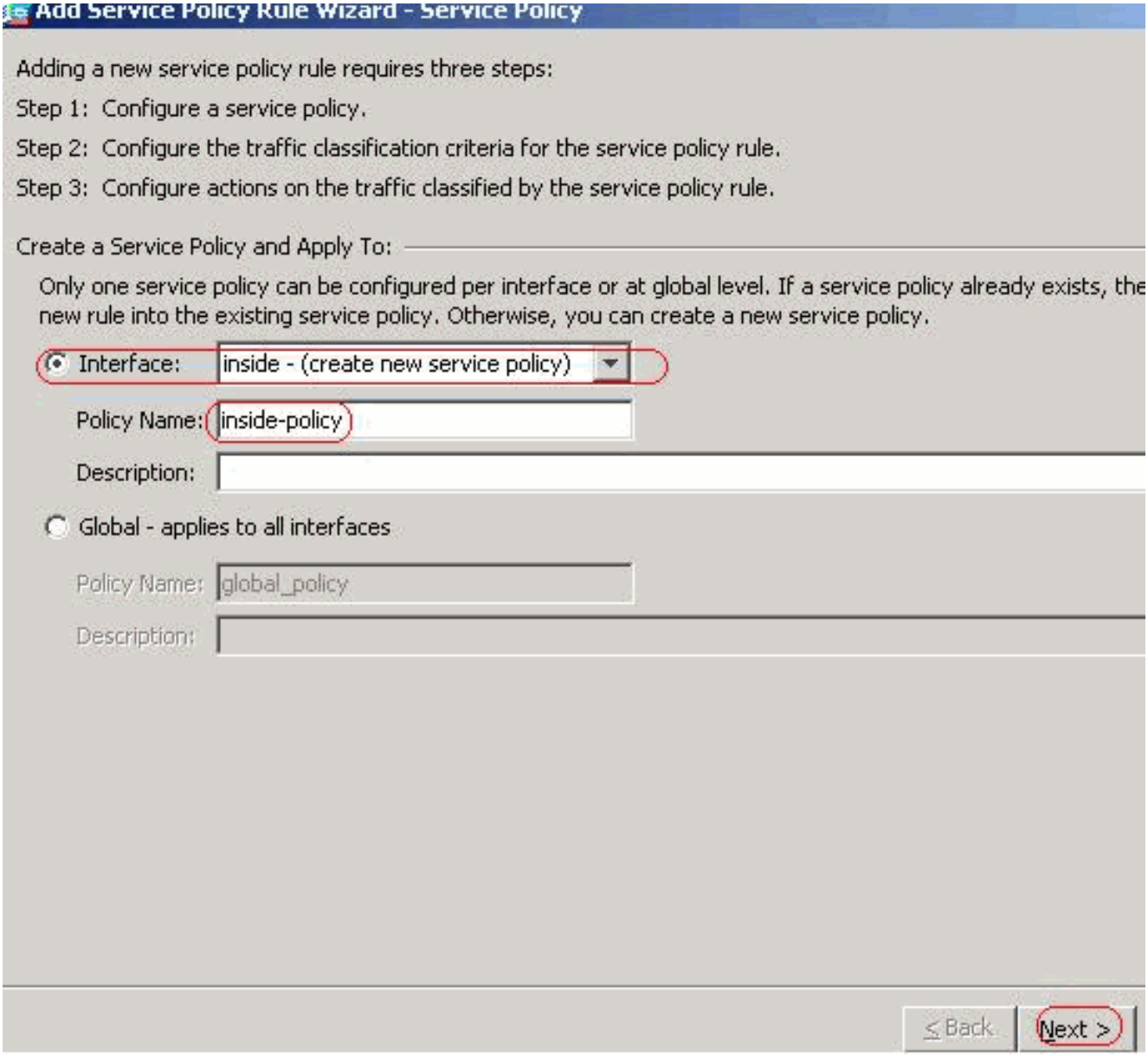


BlockURLsClass. Cliquez sur **OK**.Cliquez sur **Apply**.**Configuration équivalente CLI**

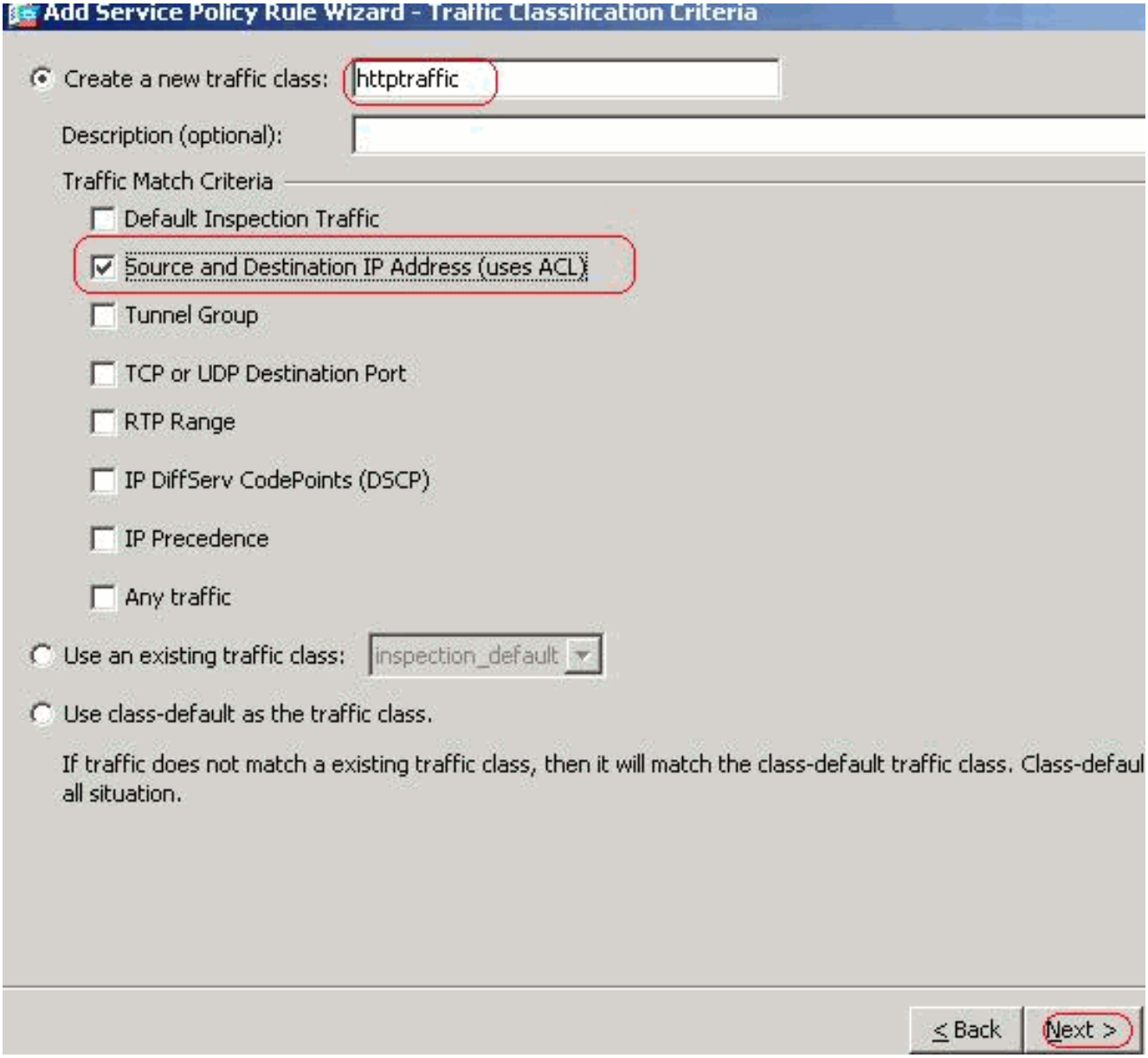
5. **Appliquez-vous la stratégie de HTTP d'inspection à l'interface**Choisissez les **règles de configuration > de stratégie de Pare-feu > de service > ajoutent > ajoutent la règle de stratégie de service**.



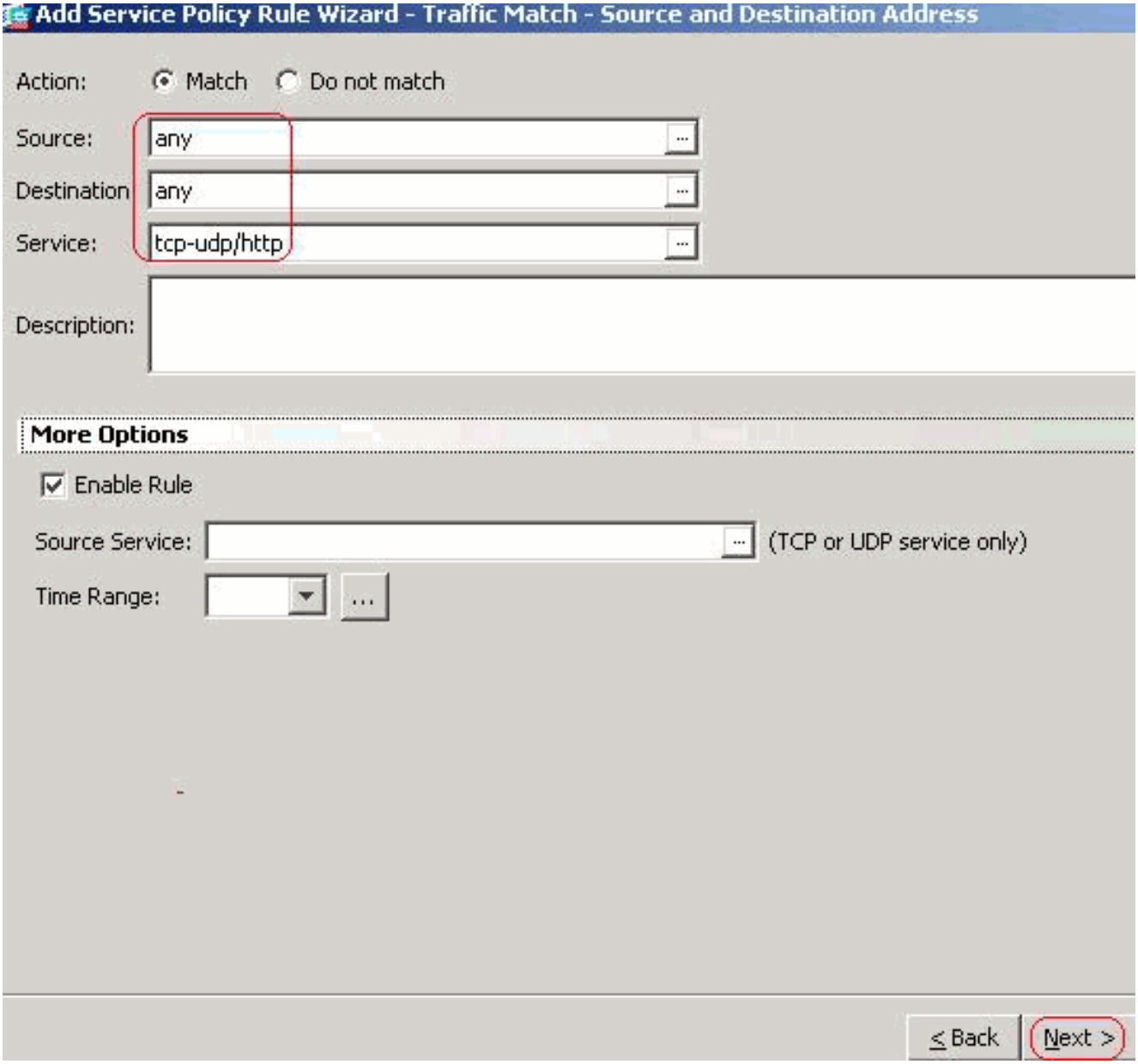
Trafic HTTP Choisissez la case d'option d'**interface** avec l'interface interne du menu et du nom de stratégie de baisse vers le bas comme à l'intérieur-**stratégie**. Cliquez sur **Next** (Suivant).



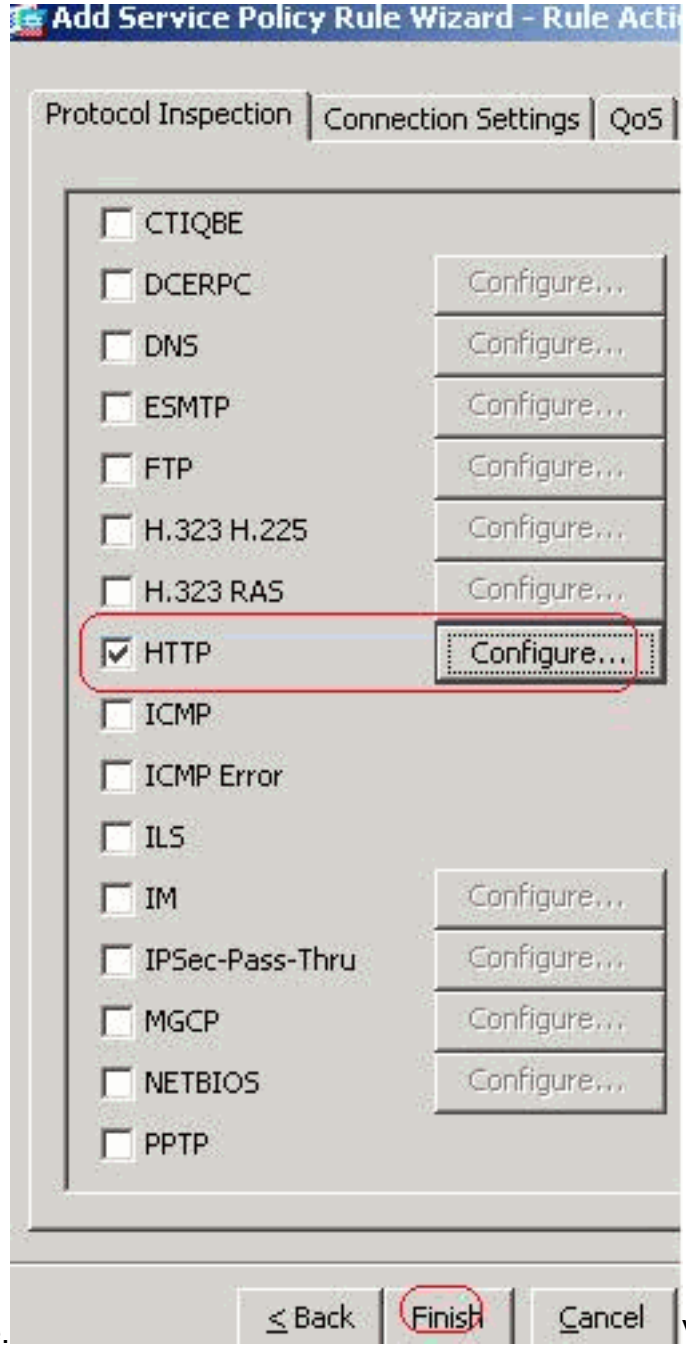
Créez un class map **httptraffic** et vérifiez la **source** et l'**adresse IP de destination (ACL d'utilisations)**. Cliquez sur **Next**
(Suivant).



Choisissez la source et la destination aussi avec le service que le TCP-**UDP/HTTP**. Cliquez sur **Next**
(Suivant).

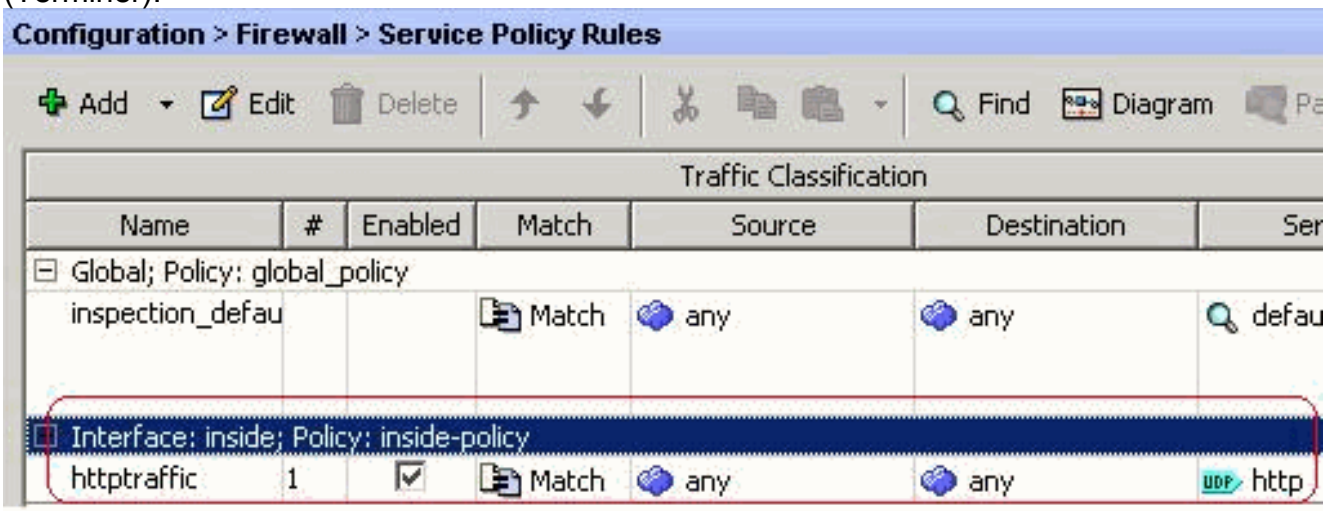


Vérifiez la case d'option de **HTTP** et cliquez sur

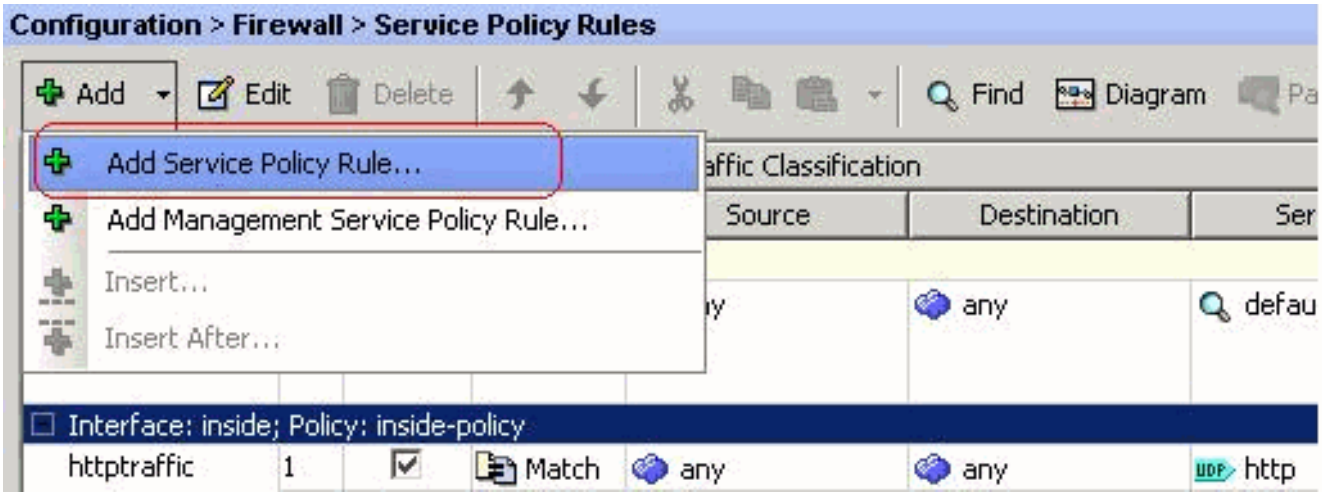


Configure. Vérifiez la case d'option **sélectionnent un HTTP examinent la carte pour assurer le contrôle de l'inspection** comme

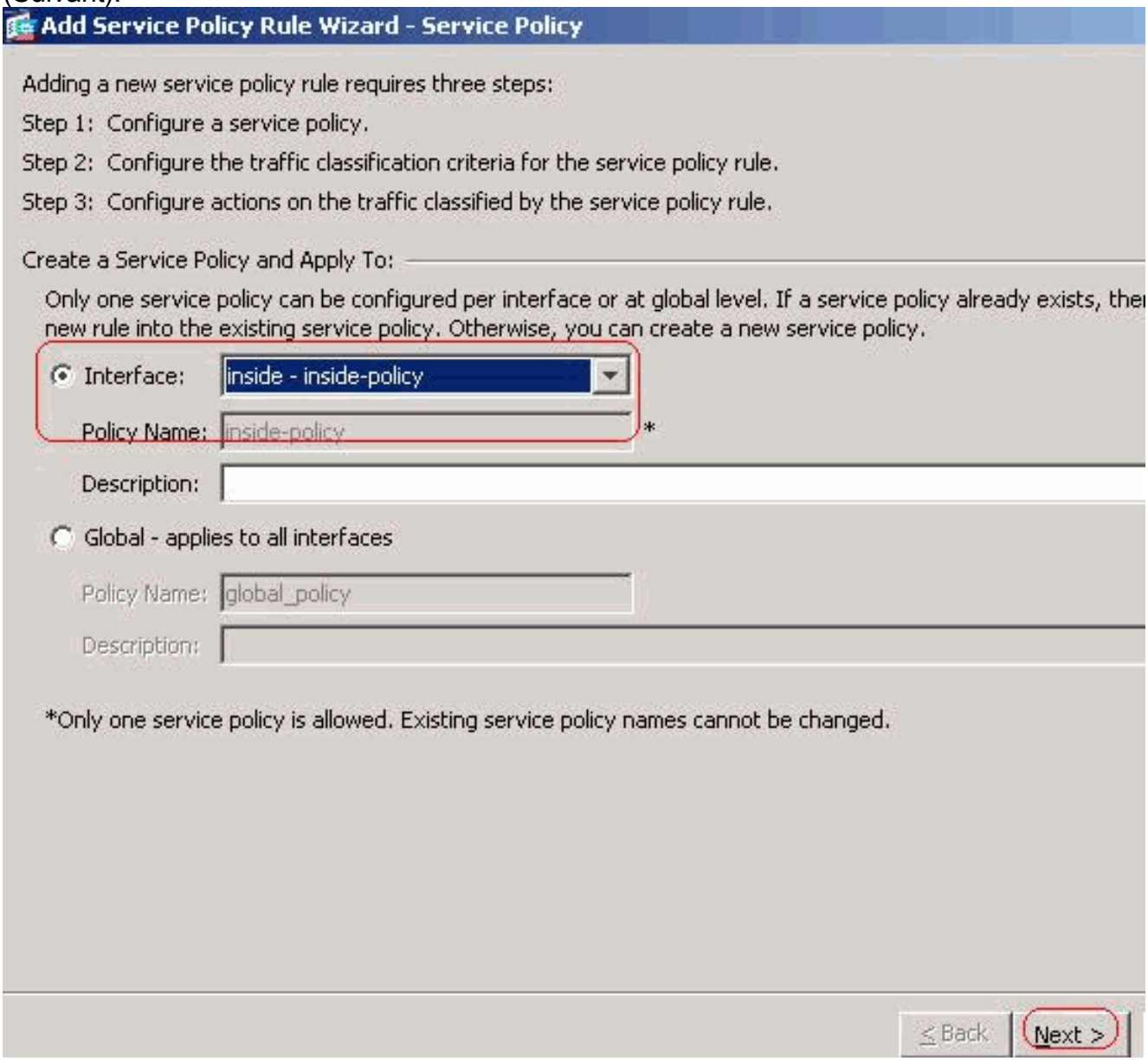
affichée. Cliquez sur **OK**.Cliquez sur **Finish** (Terminer).



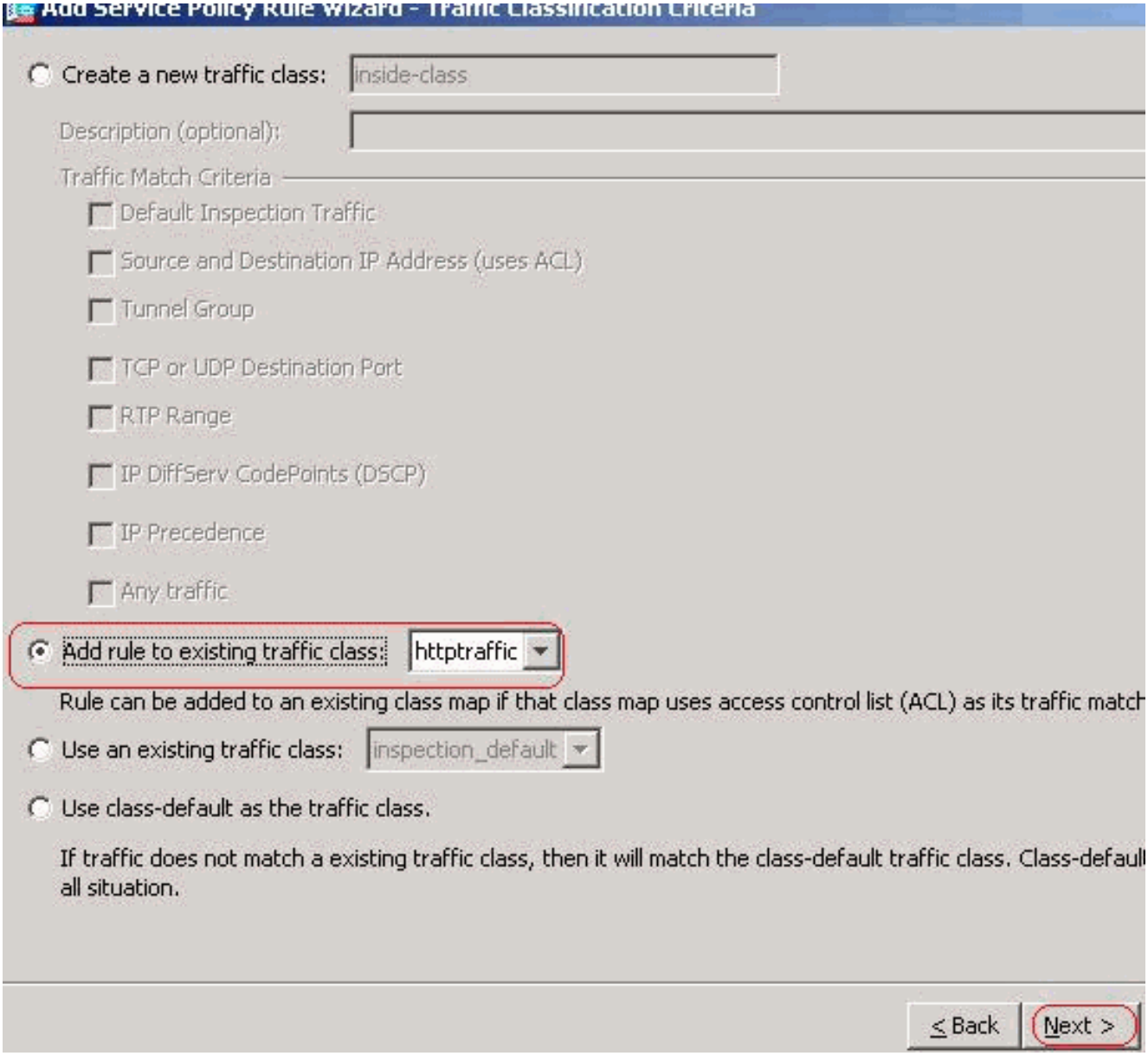
Le trafic du port 8080 De nouveau, choisissez **ajoutent > ajoutent la règle de stratégie de service**.



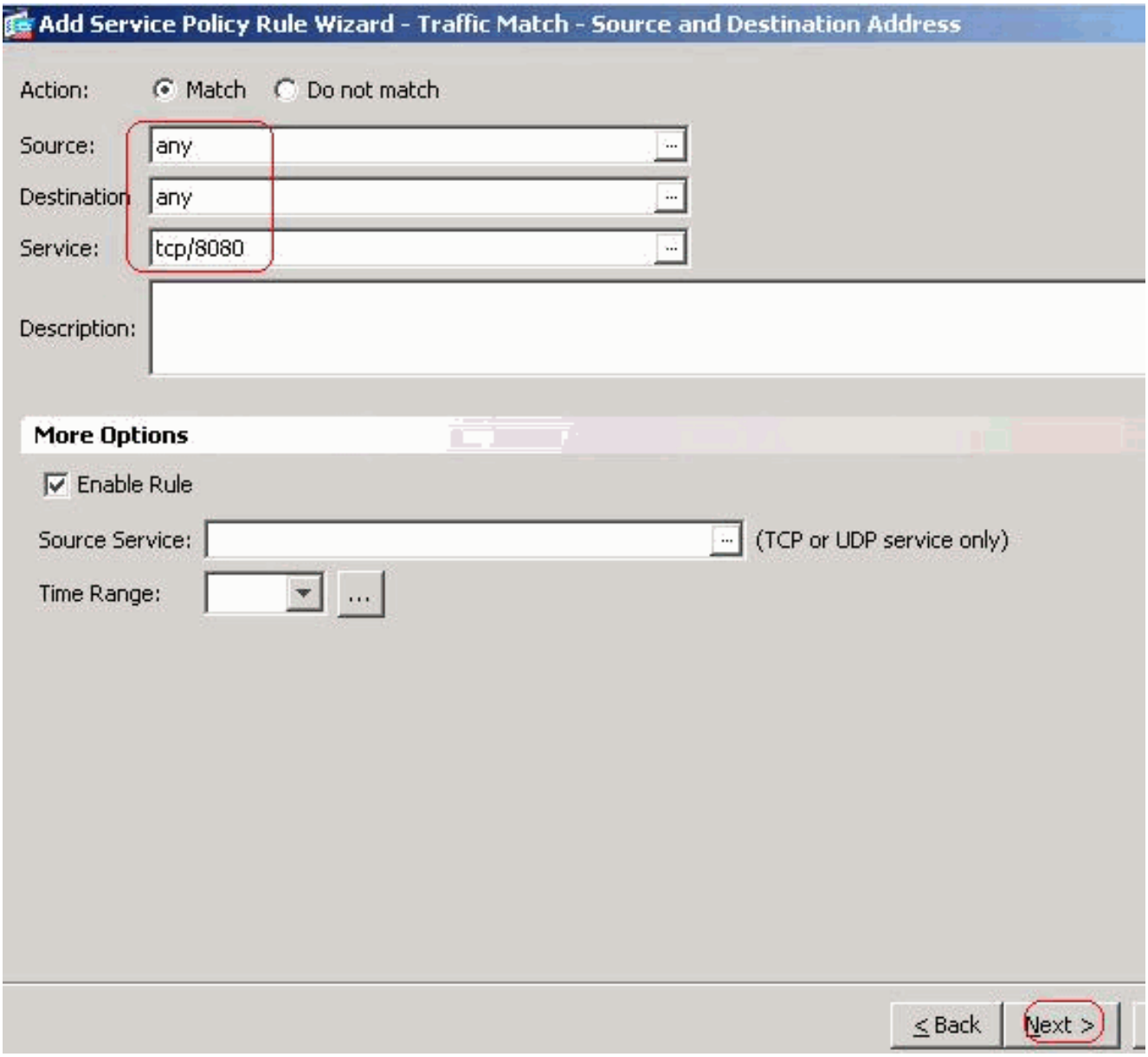
Cliquez sur **Next**
(Suivant).



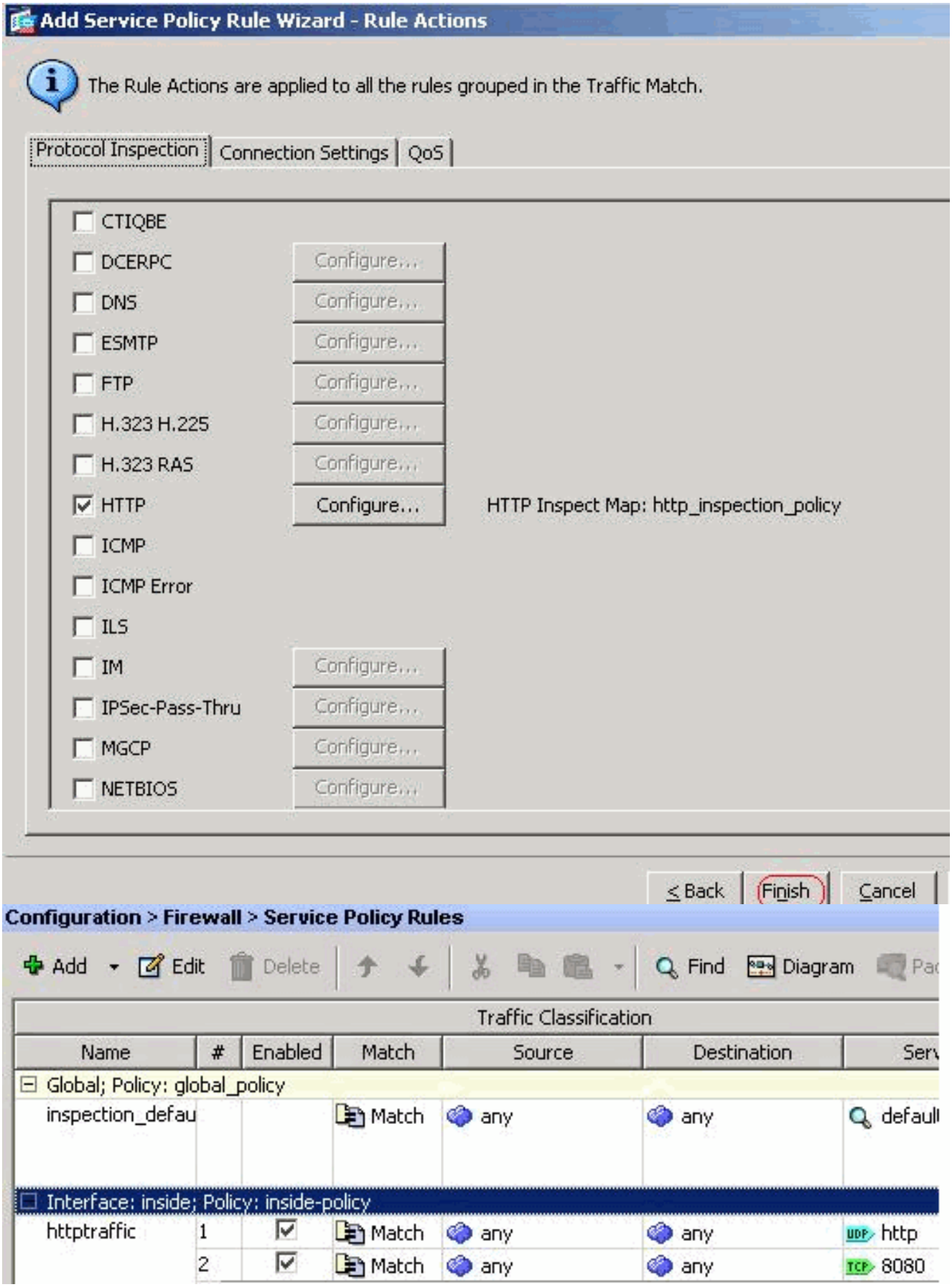
Choisissez la case d'option **ajoutent la règle à la classe existante du trafic** et choisissent **httptraffic du** menu de baisse vers le bas. Cliquez sur **Next**
(Suivant).



En choisissez la source et la destination en tant qu'avec **tcp/8080**. Cliquez sur **Next** (Suivant).



Cliquez sur **Finish** (Terminer).



Cliquez sur **Apply**.**Configuration équivalente CLI**

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **expression régulière de show running-config** — Affiche les expressions régulières qui ont été configurées`ciscoasa#show running-config regex regex urllist1 ".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt]) HTTP/1.[01]" regex urllist2 ".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh]) HTTP/1.[01]" regex urllist3 ".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt]) HTTP/1.[01]" regex urllist4 ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz]) HTTP/1.[01]" regex domainlist1 "\.yahoo\.com" regex domainlist2 "\.myspace\.com" regex domainlist3 "\.youtube\.com" regex contenttype "Content-Type" regex applicationheader "application/.*" ciscoasa#`
- **class-map de show running-config** — Affiche les class map qui ont été configurés`ciscoasa#show running-config class-map ! class-map type regex match-any DomainBlockList match regex domainlist1 match regex domainlist2 match regex domainlist3 class-map type inspect http match-all BlockDomainsClass match request header host regex class DomainBlockList class-map type regex match-any URLBlockList match regex urllist1 match regex urllist2 match regex urllist3 match regex urllist4 class-map inspection_default match default-inspection-traffic class-map type inspect http match-all AppHeaderClass match response header regex contenttype regex applicationheader class-map httptraffic match access-list inside_mpc class-map type inspect http match-all BlockURLsClass match request uri regex class URLBlockList ! ciscoasa#`
- **policy-map type inspect http de show running-config** — Affiche les cartes de stratégie qui examine le trafic http qui ont été configurés`ciscoasa#show running-config policy-map type inspect http ! policy-map type inspect http http_inspection_policy parameters protocol-violation action drop-connection class AppHeaderClass drop-connection log match request method connect drop-connection log class BlockDomainsClass reset log class BlockURLsClass reset log ! ciscoasa#`
- **policy-map de show running-config** — Affiche toutes les configurations de la carte de stratégie aussi bien que configuration de la carte de stratégie par défaut`ciscoasa#show running-config policy-map ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map type inspect http http_inspection_policy parameters protocol-violation action drop-connection class AppHeaderClass drop-connection log match request method connect drop-connection log class BlockDomainsClass reset log class BlockURLsClass reset log policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp policy-map inside-policy class httptraffic inspect http http_inspection_policy ! ciscoasa#`
- **service-stratégie de show running-config** — Affiche tous qui exécutent actuellement des configurations de politique de service`ciscoasa#show running-config service-policy service-policy global_policy global service-policy inside-policy interface inside`
- **liste d'accès de show running-config** — Affiche la configuration de liste d'accès qui fonctionne sur les dispositifs de sécurité`ciscoasa#show running-config access-list access-list inside_mpc extended permit tcp any any eq www access-list inside_mpc extended permit tcp any any eq 8080 ciscoasa#`

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **mettez au point le HTTP** — Affiche les messages de débogage pour le trafic http

Informations connexes

- Assistance des dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Support du Cisco Adaptive Security Device Manager (ASDM)
- Assistance des dispositifs de sécurité de la gamme Cisco PIX 500
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems