ASA/PIX 8.x: Blokkeer bepaalde websites (URL's) met behulp van reguliere expressies met behulp van een MPF-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco security applicaties ASA/PIX 8.x kunt configureren die reguliere expressies met modulair beleidskader (MPF) gebruikt om bepaalde websites (URL's) te blokkeren.

Opmerking: deze configuratie blokkeert niet alle toepassingsdownloads. Voor betrouwbare bestandsblokkering moet een speciaal apparaat zoals InronPort S Series of een module zoals de CSC-module voor de ASA worden gebruikt.

Opmerking: HTTPS-filtering wordt niet ondersteund op ASA. ASA kan geen diepe pakketinspectie of inspectie doen op basis van regelmatige expressie voor HTTPS-verkeer, omdat inhoud van pakket versleuteld is (SSL).

Voorwaarden

Vereisten

Dit document gaat ervan uit dat Cisco security applicatie is geconfigureerd en correct werkt.

Gebruikte componenten

- Cisco 5500 Series adaptieve security applicatie (ASA) die de softwareversie 8.0(x) en hoger uitvoeren
- Cisco Adaptieve Security Devices Manager (ASDM) versie 6.x voor ASA 8.x

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 Cisco 500 Series PIX die de softwareversie 8.0(x) en hoger uitvoeren.

Conventies

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

Achtergrondinformatie

Overzicht van het beleidskader

MPF biedt een consistente en flexibele manier om de functies van security applicaties te configureren. U kunt bijvoorbeeld MPF gebruiken om een tijdelijke configuratie te maken die specifiek is voor een bepaalde TCP-toepassing, in tegenstelling tot een configuratie die van toepassing is op alle TCP-toepassingen.

MPF ondersteunt deze functies:

- TCP-normalisatie, TCP- en UDP-verbindingslimieten en -onderbreking, en TCP-sequentienummer-randomisatie
- CSC
- Toepassingscontrole
- IPS
- QoS-input-toezicht
- QoS-uitvoertoezicht
- QoS-prioriteitswachtrij

De samenstelling van het MPF bestaat uit vier taken:

1. Identificeer Layer 3 en 4 verkeer waarop u acties wilt toepassen. Raadpleeg het Identificeren van verkeer met een Layer 3/4 Class Map voor meer informatie.
2. (Uitsluitend voor de inspectie van toepassingen) Vaststellen van speciale maatregelen voor het verkeer van de inspectie van toepassingen. Zie Speciale acties voor Toepassingsinspecties configureren voor meer informatie.
3. Toepassen acties op Layer 3 en 4 verkeer. Raadpleeg Handelingen definiëren met een

Layer 3/4 beleidskaart voor meer informatie.

4. Activeert de acties op een interface. Raadpleeg het gedeelte Layer 3/4-beleid toepassen op een interface met een servicebeleid voor meer informatie.

Normale expressie

Een reguliere expressie komt overeen met tekst strings letterlijk als een exacte string, of door het gebruik van metacharacters zodat je meerdere varianten van een tekststring kunt vergelijken. U kunt gebruikmaken van een reguliere expressie om de inhoud van bepaalde toepassingsverkeer aan te passen. U kunt bijvoorbeeld een URL-string in een HTTP-pakket matchen.

Opmerking: Gebruik **Ctrl+V** om alle speciale tekens in de CLI te verwijderen, zoals vraagteken (?) of een tab. Bijvoorbeeld, type **d[Ctrl+V]?g** om **d?g** in de configuratie in te voeren.

Gebruik de opdracht **regex** om een reguliere expressie te maken. Deze opdracht kan worden gebruikt voor verschillende functies waarvoor tekst moet worden aangepast. U kunt bijvoorbeeld speciale acties voor toepassingsinspectie configureren met behulp van het modulaire beleidskader dat een controleleidkaart gebruikt. Raadpleeg de **opdracht** Beleidskaarten inspecteren voor meer informatie. In de kaart van het inspectiebeleid kunt u het verkeer identificeren waarop u wilt reageren als u een kaart van de inspectieklasse maakt die een of meer **overeenkomende** opdrachten bevat of u **wedstrijdopdrachten** rechtstreeks in de kaart van het inspectiebeleid kunt gebruiken. Sommige overeenkomende opdrachten stellen u in staat tekst in een pakket te herkennen met behulp van een reguliere expressie; U kunt bijvoorbeeld URL strings koppelen in HTTP-pakketten. U kunt reguliere expressies groeperen in een class map met reguliere expressies. Raadpleeg de **opdracht** class-map type regex voor meer informatie.

Deze tabel bevat de metacharacters met speciale betekenis.

karakter	**Beschrijving**	**Opmerkingen**
.	punt	Overeenkomsten met één teken. Bijvoorbeeld komt **d.g** overeen met hond, dag, dtg, en elk woord dat die tekens bevat, zoals hondengonnit.
(nl.)	Subexpressie	Een compressie scheidt tekens van omliggende tekens, zodat u andere tekens op de onderdrukking kunt gebruiken. **d(o|a)g** bijvoorbeeld komt overeen met hond en dag, maar **do|ag** overeenkomsten doen en ag. Er kan ook een compressie worden gebruikt met herkende kwantificeringen om een onderscheid te maken tussen de tekens die bij een herhaling moeten worden gebruikt. Bijvoorbeeld, **ab (xy) {3} z** past abxyz aan.
|	Alternatie	Overeenkomsten van een van beide expressies die het scheidt. Bijvoorbeeld **hond |cat** komt overeen met hond of kat.

?	vraagteken	Een kwanfier die aangeeft dat er 0 of 1 van de vorige expressie is. Bijvoorbeeld, **zie?** Zie overeenkomsten verloren of verliezen. **Opmerking:** U moet **Ctrl+V** invoeren en vervolgens het vraagteken of anders wordt de Help-functie opgeroepen.
*	Asterisk	Een kwantificator die aangeeft dat er 0, 1 of een nummer van de vorige expressie is. Bijvoorbeeld, **zie*se** overeenkomsten minder, verliezen, los, etc.
{x}	Herhaal kwantificator	Doe precies x keer. Bijvoorbeeld, **ab (xy) {3} z** past abxyz aan.
{x,}	Minimale herhalingskwantificering	Herhaal dit minstens x keer. Bijvoorbeeld, **ab (xy) {2,} z** past bij abxyz, abxyxyz, enz.
[abc]	Tekenklasse	Overeenkomt een teken in de haakjes. Bijvoorbeeld komt **[abc]** overeen met a, b of c.
[^abc]	Negatieve tekenklasse	Overeenkomsten met één teken dat niet tussen de haakjes zit. Bijvoorbeeld, **[^abc]** komt een ander teken aan dan a, b of c. **[^A-Z]** komt overeen met elk teken dat geen hoofdletter is.
[a-c]	Tekenklasse	Overeenkomst met elk teken in het bereik. **[a-z]** komt overeen met elke kleine letter. U kunt tekens en bereik samenvoegen: **[abcq-z]** komt overeen met a, b, c, q, r, s, t, u, v, w, x, y, z, en **[a-cq-z]**. Het streepje (-) teken is alleen letterlijk als het laatste of het eerste teken in de haakjes is: **[abc-]** of **[-abc]**.
""	Quotentietekens	Houdt het tekenen of uitlopen van spaties in de string vast. De **"test"** behoudt bijvoorbeeld de toonaangevende ruimte wanneer deze op een match is gericht.
^ ^ ^	kleding	Specificeert het begin van een regel
\	Escape-teken	Bij gebruik met een metacharacter komt een letterlijk teken overeen. Bijvoorbeeld **\[** komt overeen met de linkerkant van de beugel.
klusje	karakter	Wanneer een teken geen metacharacter is, past het letterlijke

		teken aan.
\r	wagenoord	Komt overeen met een vervoersretourzending 0x0d
\n	Nieuws	Komt overeen met een nieuwe regel 0x0a
\t	Tab	Overeenkomsten van een tabblad 0x09
\f	Formulier	Overeenkomt een formulierfeed 0x0c
\xNN	Escaped hexadecimal nummer	Overeenkomt een ASCII-teken dat een hexadecimaal gebruikt dat exact twee cijfers bevat
\NNN	Verbroken octaal nummer	Overeenkomst een ASCII-teken als octal dat exact drie cijfers bevat. Het teken 040 vertegenwoordigt bijvoorbeeld een ruimte.

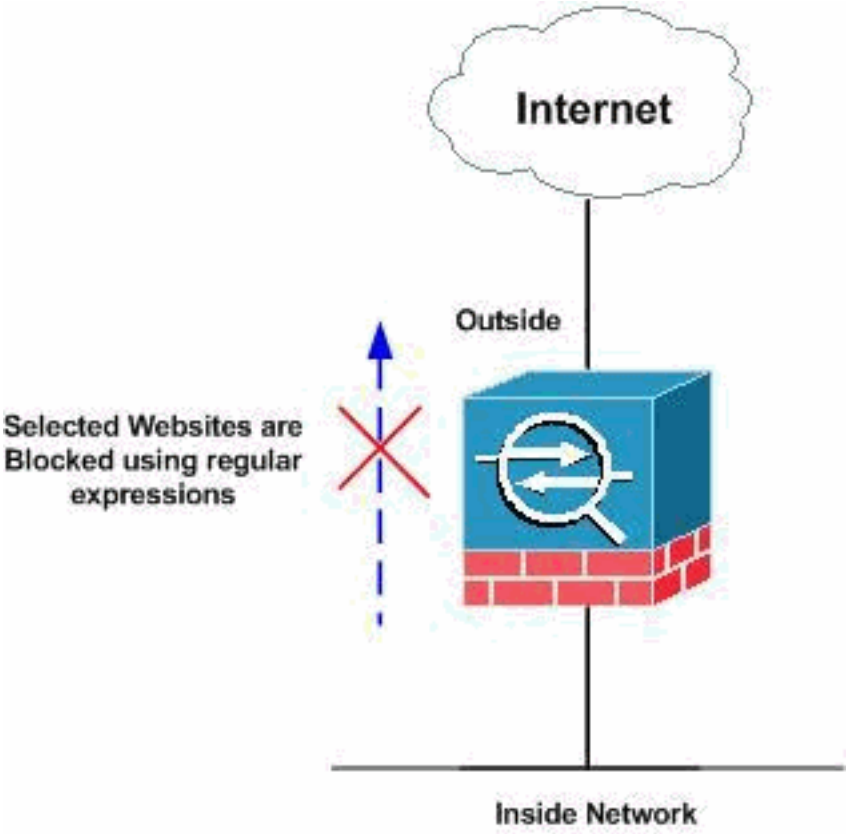
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- ASA CLI-configuratie
- ASA-configuratie 8.x met ASDM 6.x

ASA CLI-configuratie

ASA CLI-configuratie

```
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
```

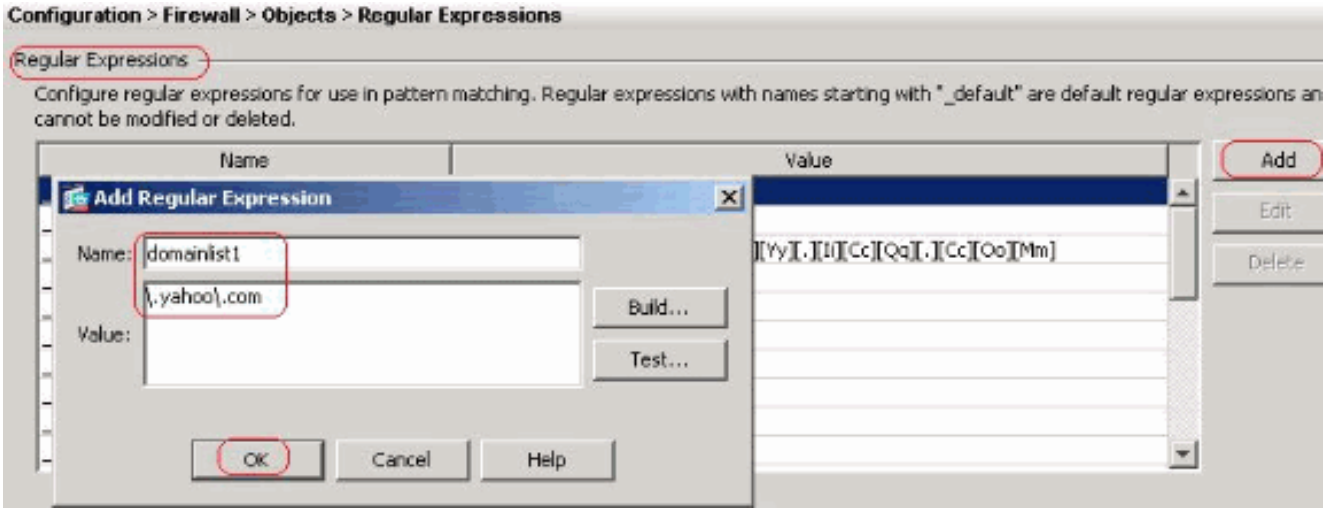
```
!--- and provided the http version being used by web
browser must be either !--- 1.0 or 1.1 regex urllist3
".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt])
HTTP/1.[01]"

!--- 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#
```

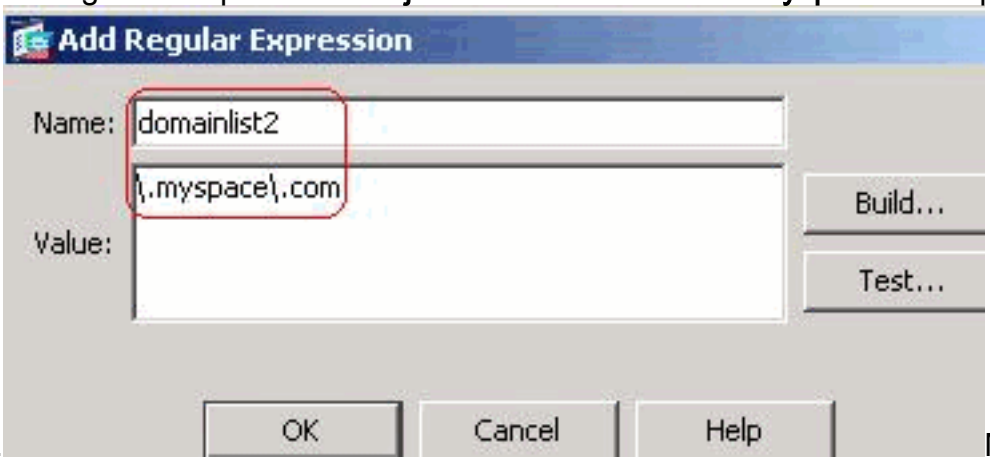
ASA-configuratie 8.x met ASDM 6.x

Voltooi deze stappen om de reguliere expressies te configureren en ze in MPF toe te passen om de specifieke websites zoals aangegeven te blokkeren.

1. **Reguliere expressies maken**Kies **Configuration > Firewall> Objects > Reguliere expressies** en klik op **Add** onder het tabblad **Reguliere expressie** om reguliere expressies te maken zoals weergegeven.Maak een **platenlijst van** reguliere expressies**1** om de domeinnaam **yahoo.com** op te nemen. Klik op **OK**.

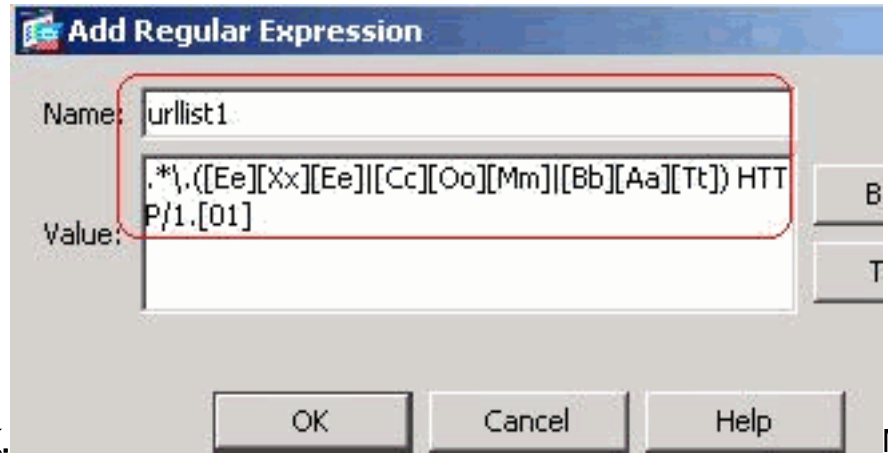


Maak een reguliere expressie **huislijst2** om de domeinnaam **myspace.com** op te nemen. Klik op **OK**.

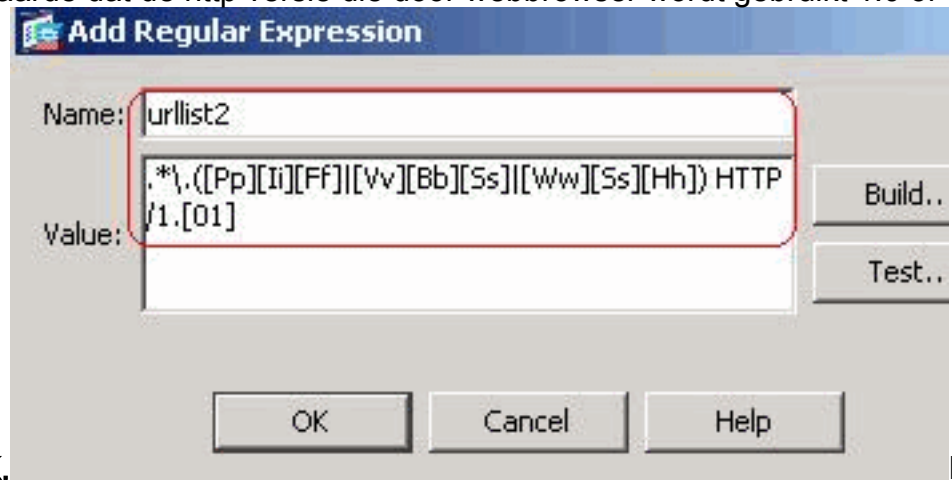


Maak een reguliere expressie **huislijst3** om de domeinnaam **youtube.com** op te nemen. Klik op **OK**.

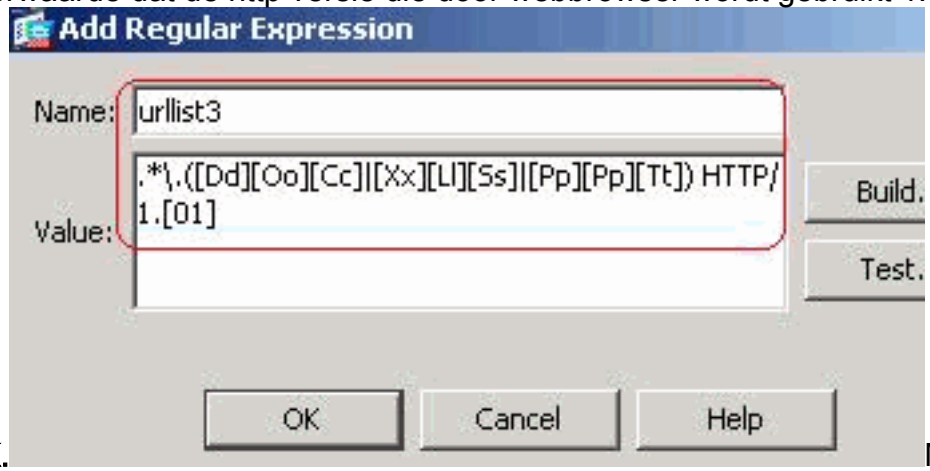
Maak een reguliere expressie **urllist1** om de bestandsextensies op te nemen zoals **exe**, **com** en **bat** op voorwaarde dat de http versie die door webbrowser wordt gebruikt 1.0 of 1.1 moet zijn. Klik



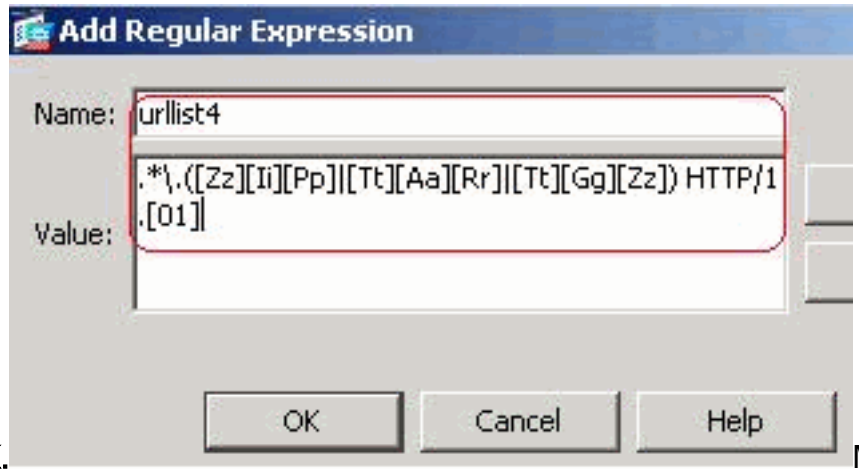
op **OK.** Maak een reguliere expressie **urllist2** om de bestandsextensies op te nemen zoals **pif**, **vbs** en **wsh** op voorwaarde dat de http versie die door webbrowser wordt gebruikt 1.0 of 1.1 moet zijn. Klik



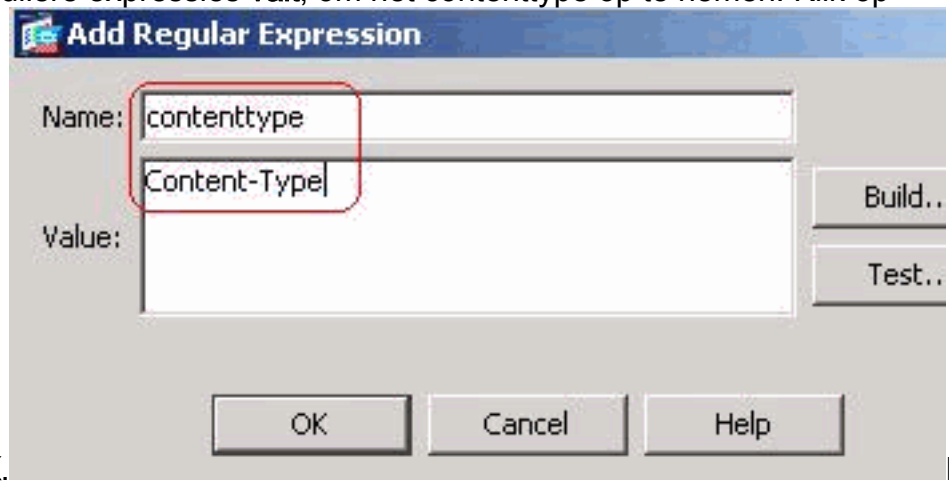
op **OK.** Maak een **urllist3** van reguliere expressies om de bestandsextensies op te nemen zoals **doc**, **xls** en **ppt** op voorwaarde dat de http versie die door webbrowser wordt gebruikt 1.0 of 1.1 is. Klik op



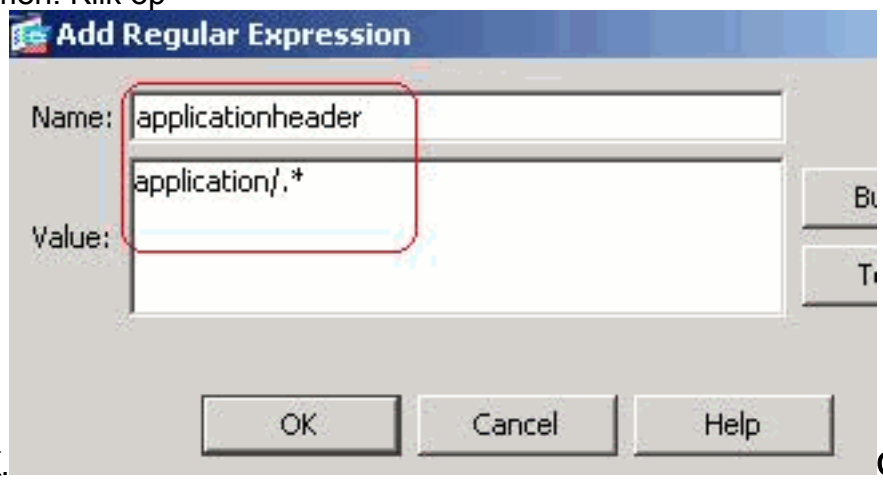
OK. Maak een reguliere expressie **urllist4** om de bestandsextensies op te nemen zoals **zip**, **tar** en **tgz** op voorwaarde dat de http versie die door webbrowser wordt gebruikt 1.0 of 1.1 is. Klik op



OK. Maak een **inhoud** die **binnen** reguliere expressies **valt**, om het contenttype op te nemen. Klik op

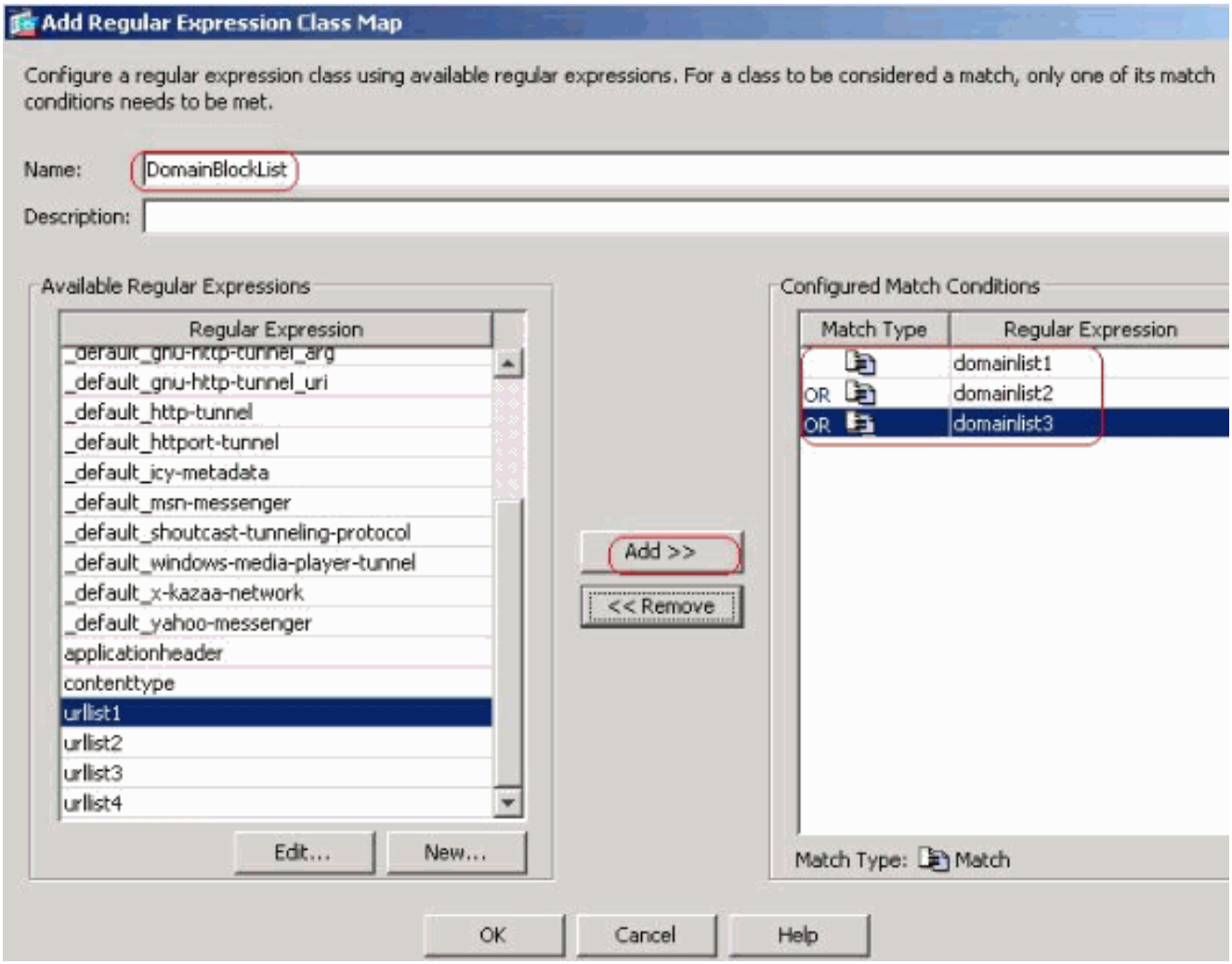


OK. Maak een **toepassingsheader van** reguliere expressies om de verschillende toepassingsheader op te nemen. Klik op

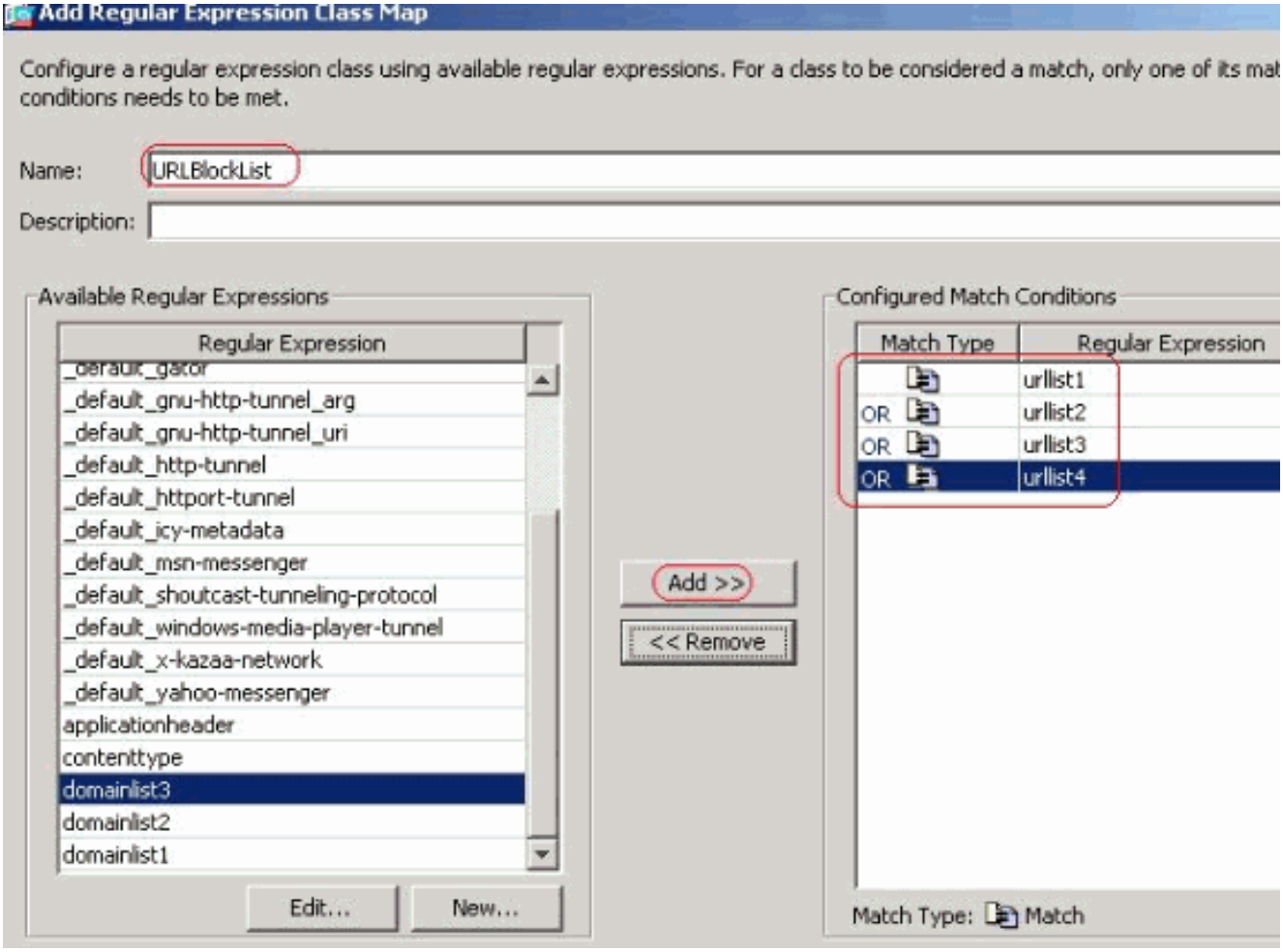


OK. **Compatibele CLI-configuratie**

2. **Reguliere expressieklasse maken**Kies **Configuration > Firewall > Objects > Reguliere expressies** en klik op **Add** onder het tabblad **Reguliere expressie class** om de verschillende klassen te maken zoals weergegeven.Maak een reguliere expressieklasse **DomainBlockList** om een van de reguliere expressies domeinlist1, domainlist2 en domainlist3 aan te passen. Klik op
OK.

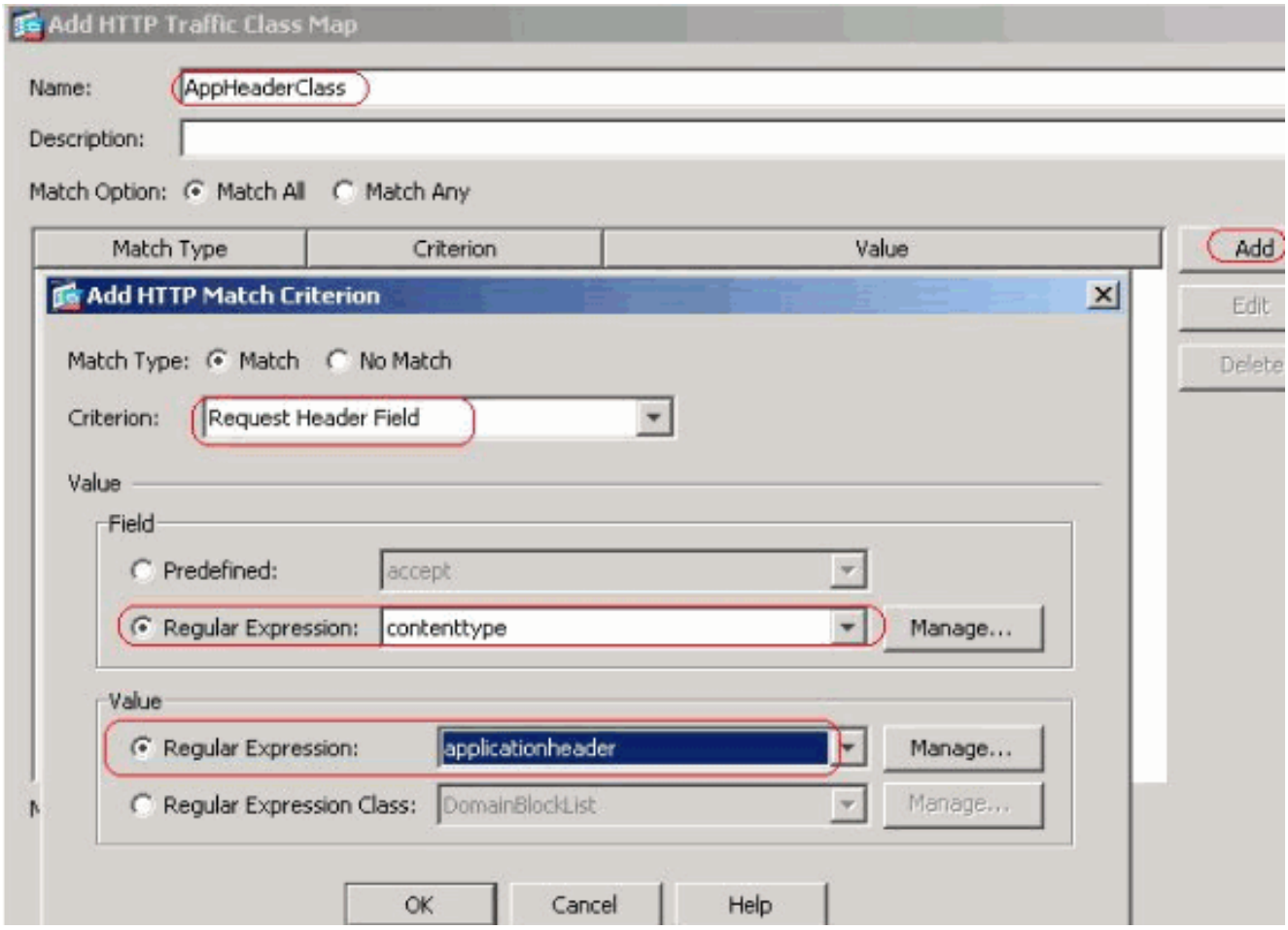


Maak een expressieklasse **URLBlockList** om een van de reguliere expressies urllist1, urllist2, urllist3 en urllist4 aan te passen. Klik op
OK.

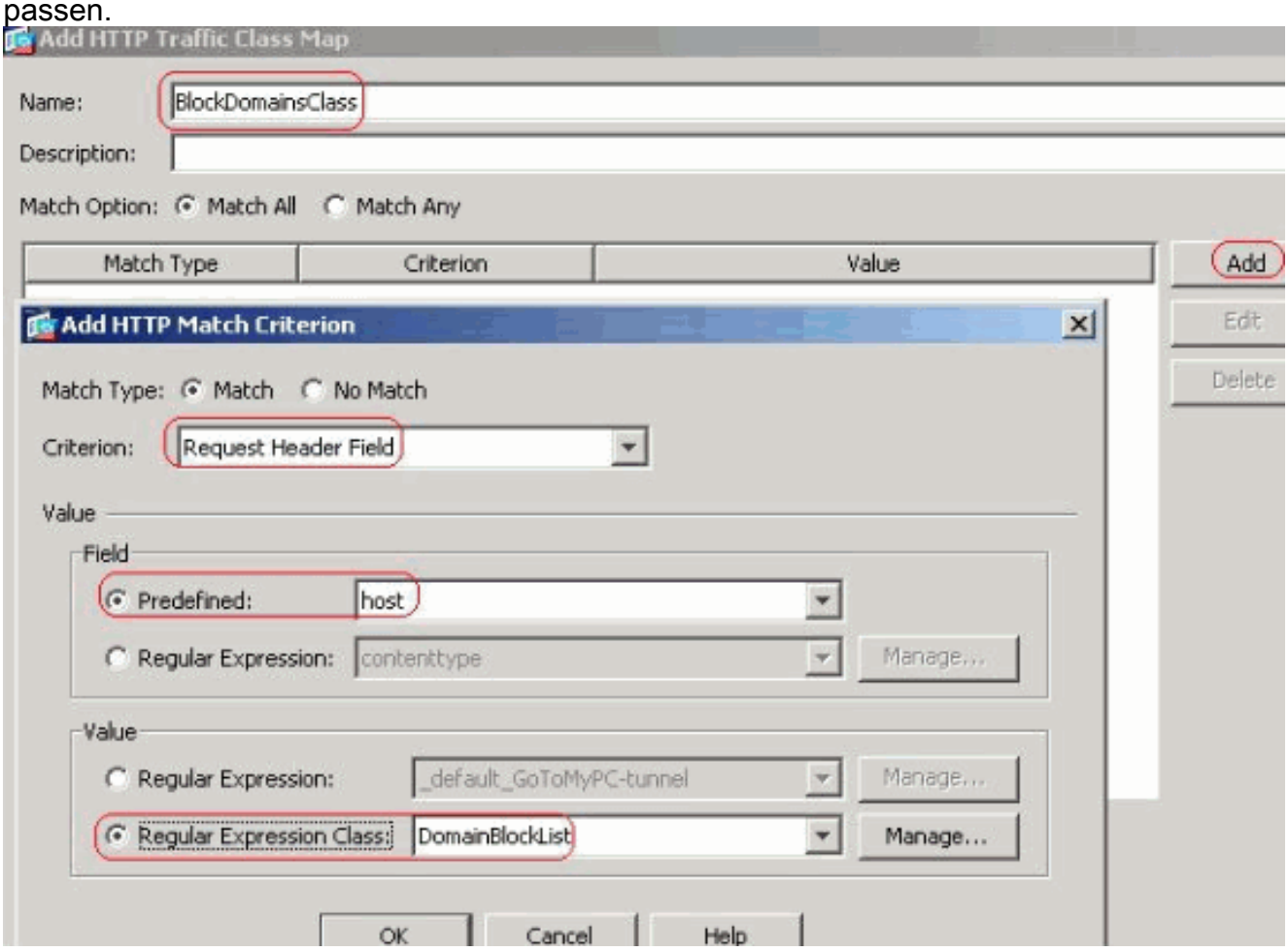


Compatibele CLI-configuratie

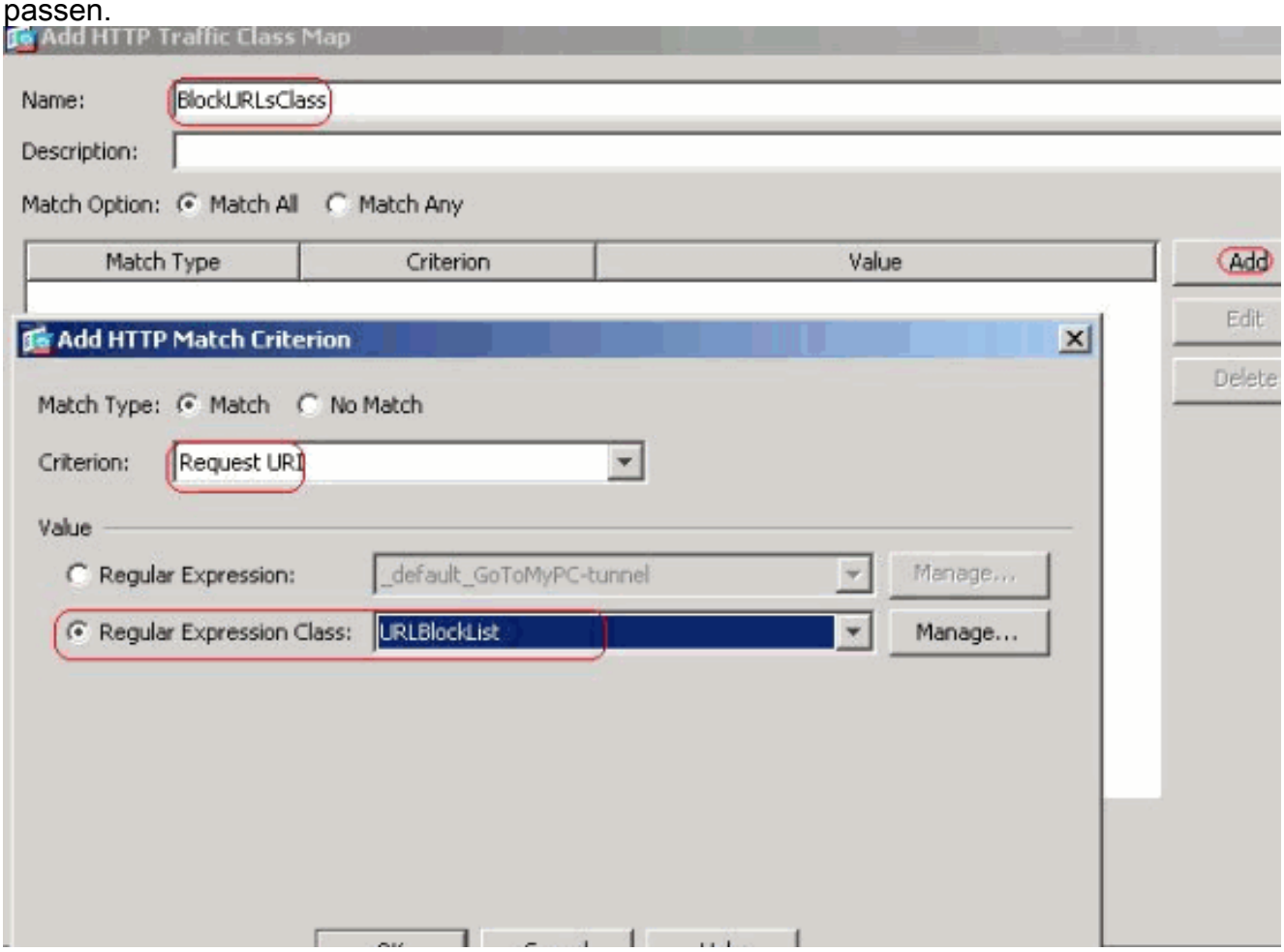
3. **Controleer het geïdentificeerde verkeer met Klasse maps**Kies **Configuration > Firewall > Objects > Class Maps > HTTP > Add** om een class map te maken voor het inspecteren van het http verkeer dat geïdentificeerd is door verschillende reguliere expressies zoals getoond.Maak een class-kaart **AppHeaderClass** om de antwoordheader met reguliere expressies aan te
passen.



Klik op **OK**Maak een class map **BlockDomainsClass** om de request header met reguliere expressies aan te
passen.

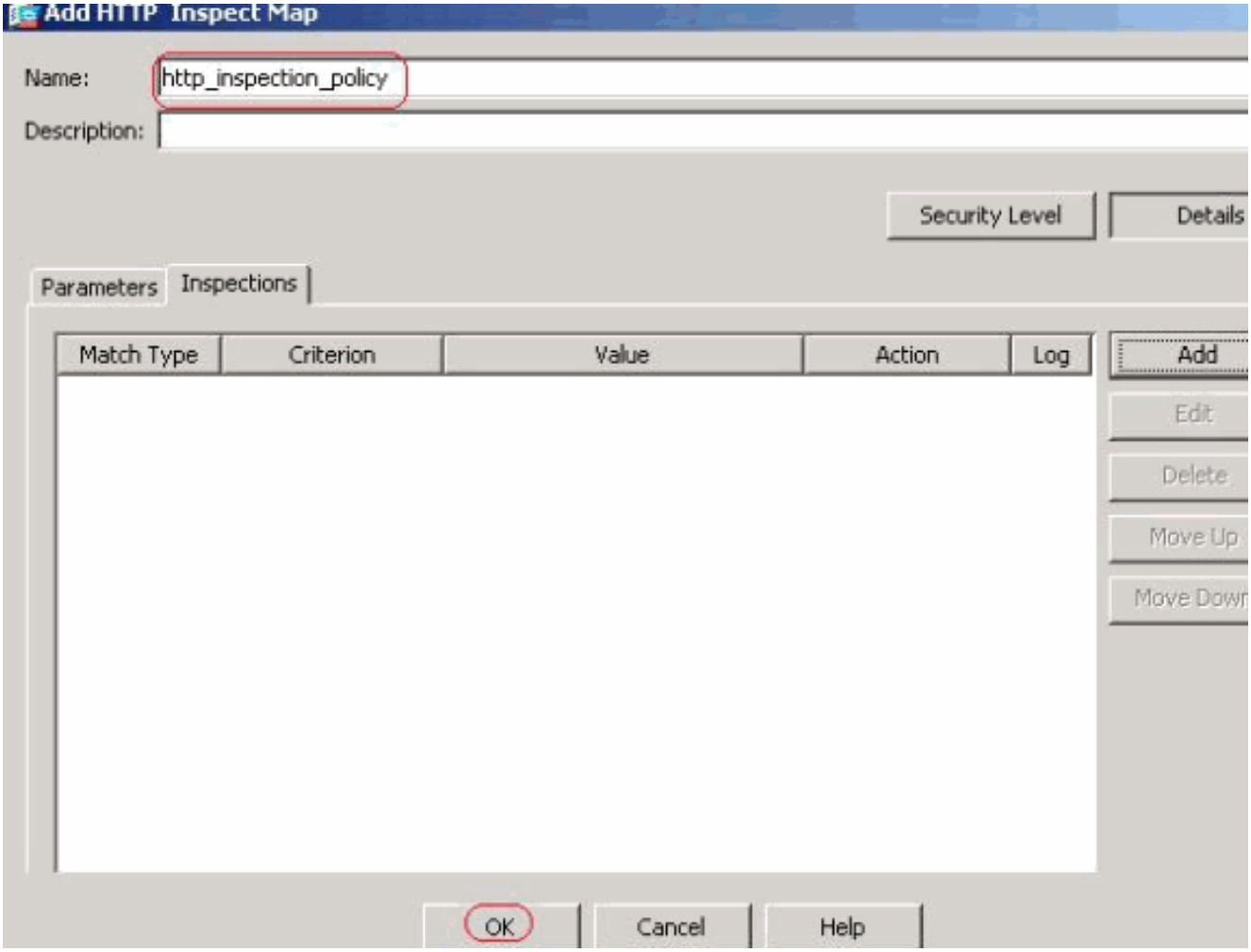


Klik op **OK**.Maak een class map **BlockURLsClass** om de request uri met reguliere expressies aan te
passen.

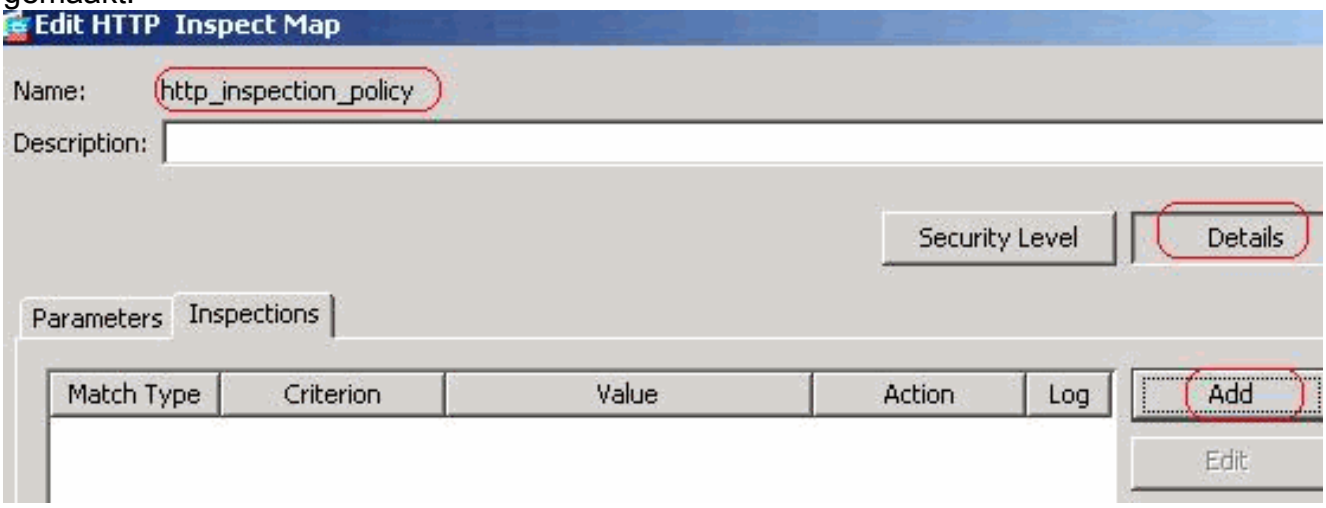


Klik op **OK**.**Compatibele CLI-configuratie**

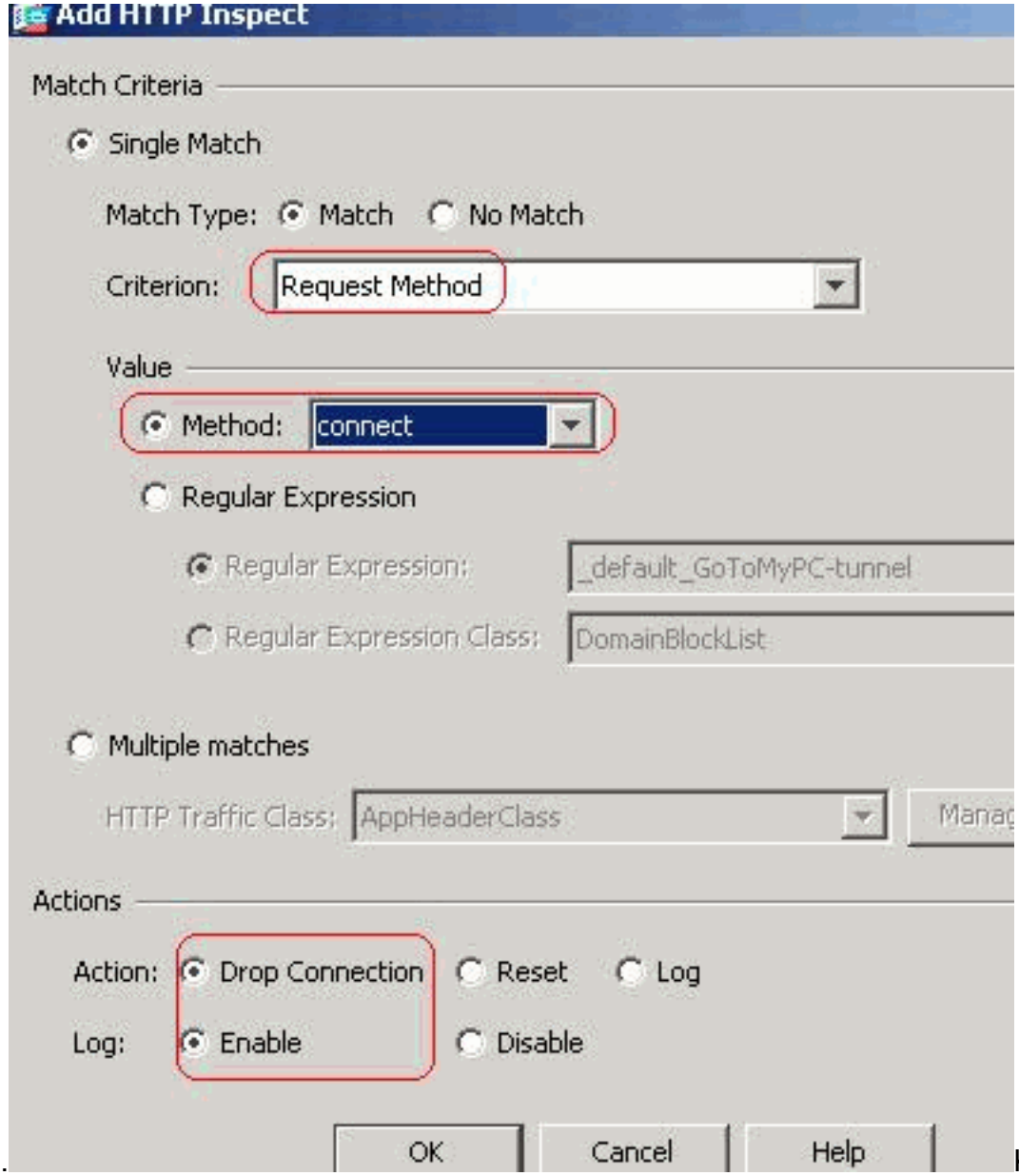
4. **Vaststellen van de maatregelen voor het gecompenseerde verkeer in het inspectiebeleid**Kies **Configuration > Firewall > Objects > Inspect Maps > HTTP** om een **http_inspection_policy** te maken om de actie voor het gematchte verkeer in te stellen zoals wordt getoond. Klik op **OK**.



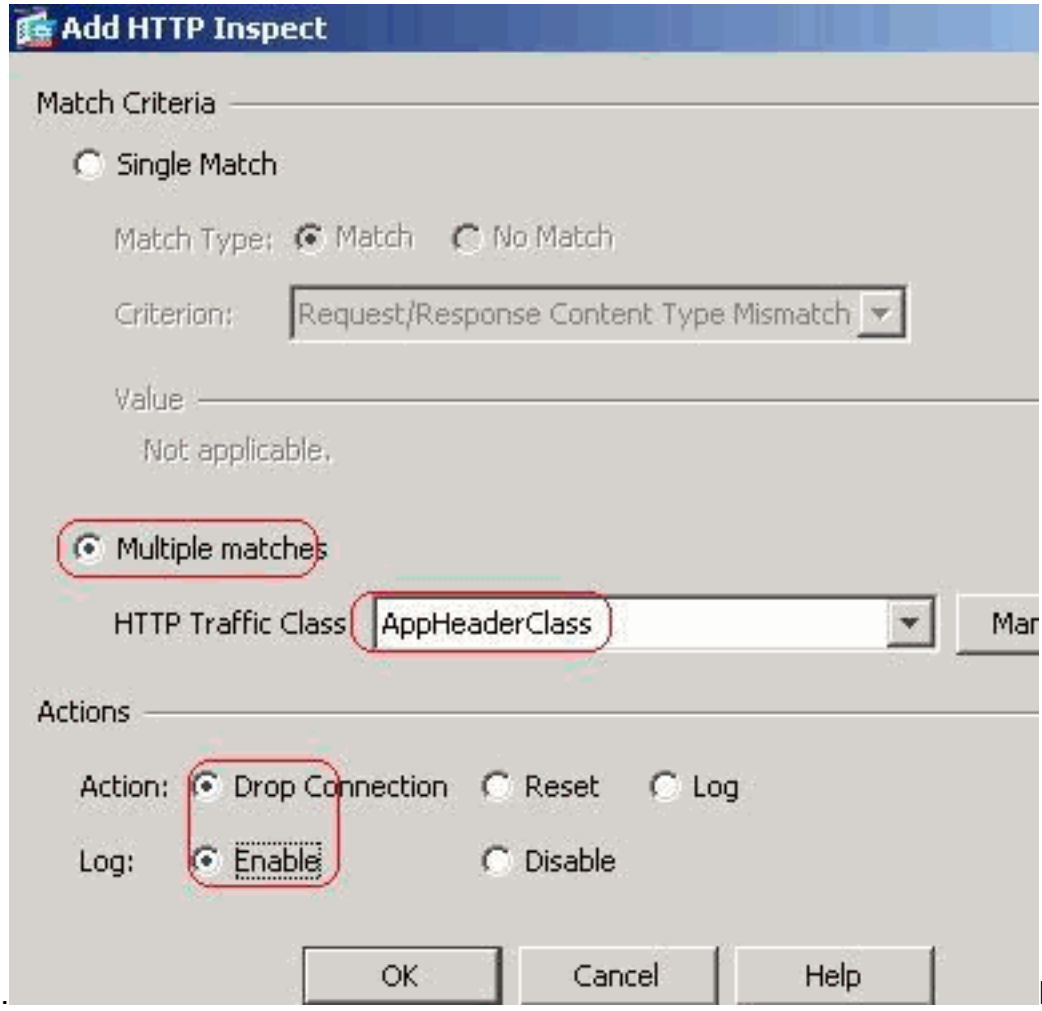
Kies **Configuration > Firewall > Objects > Inspect Maps > HTTP > HTTP_inspection_policy (dubbelklik)** en klik op **Details > Add** om de acties voor de verschillende klassen in te stellen die tot nu toe zijn
gemaakt.



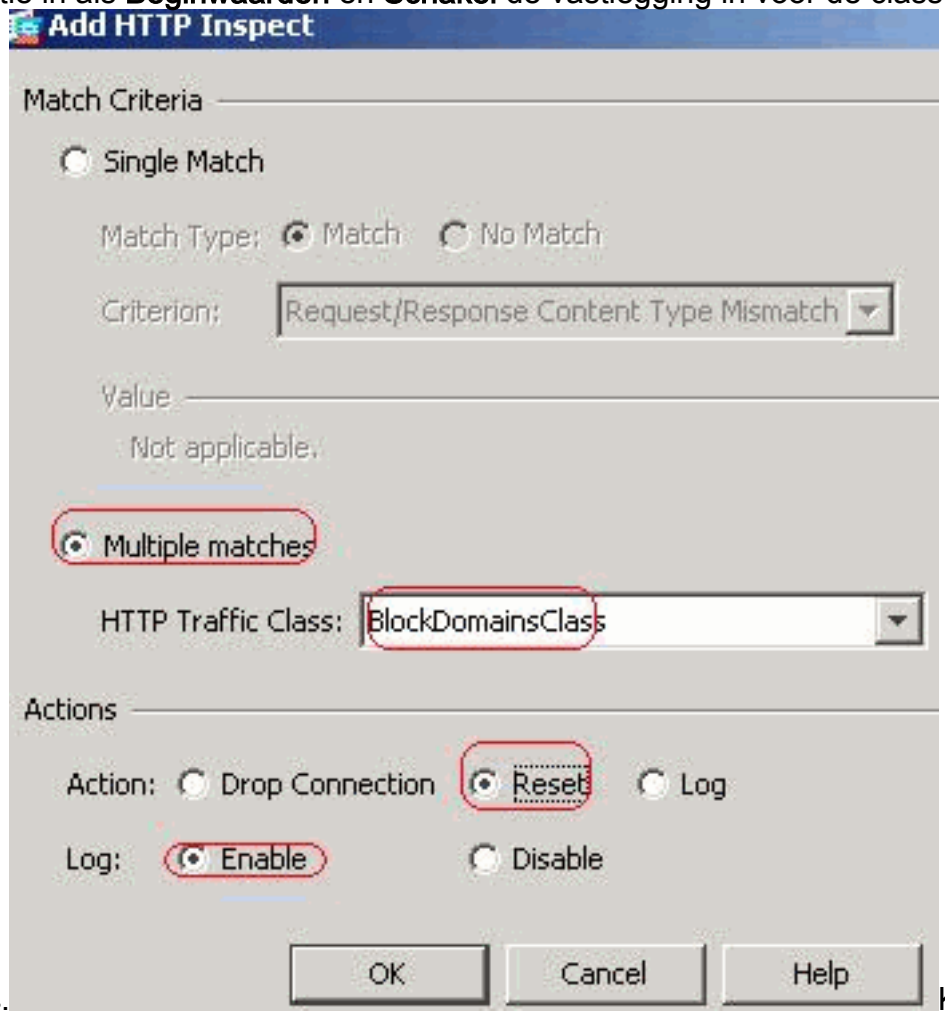
Stel de actie in als **Drop Connection** en de vastlegging voor het criterium **inschakelen** als aanvraag-methode en waarde voor



aansluiting. Klik op **OK**Stel de actie in als **Drop Connection** en **Schakel** de vastlegging in voor de klasse

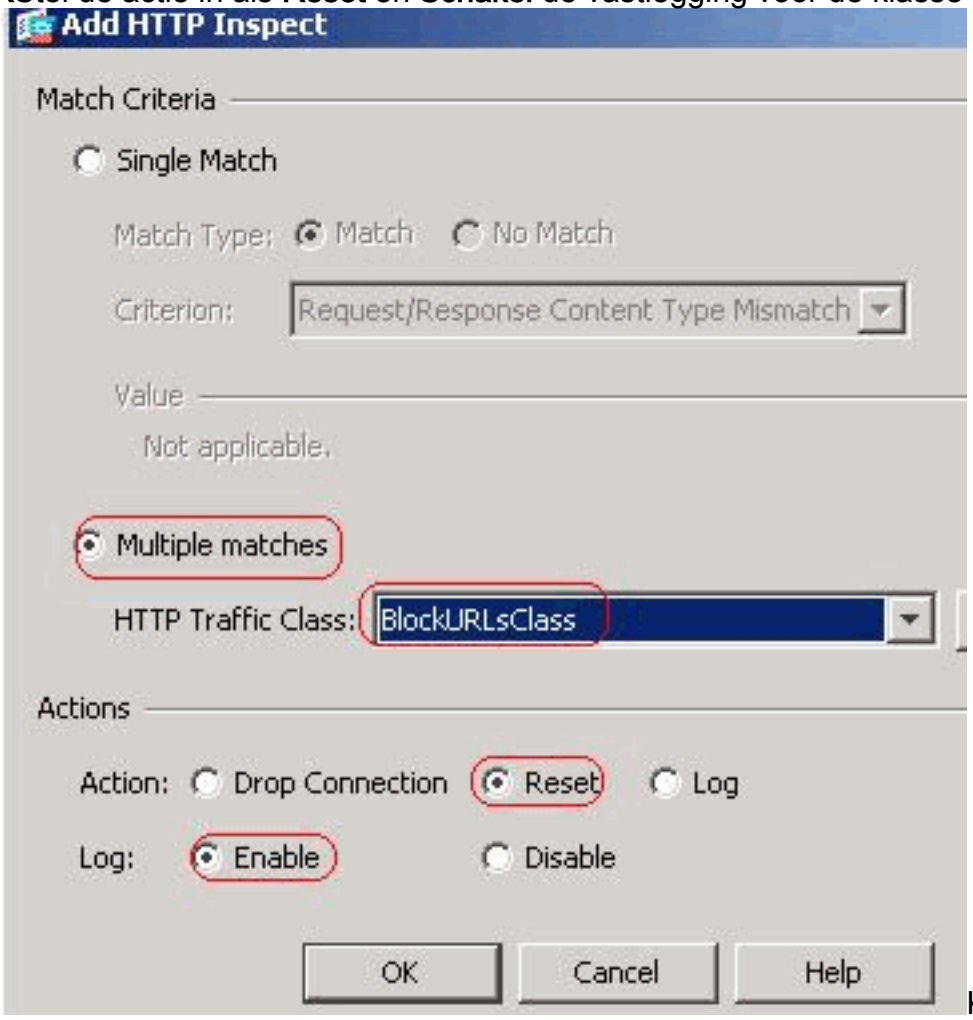


AppHeaderClass. Klik op **OK**.Stel de actie in als **Beginwaarden** en **Schakel** de vastlegging in voor de class



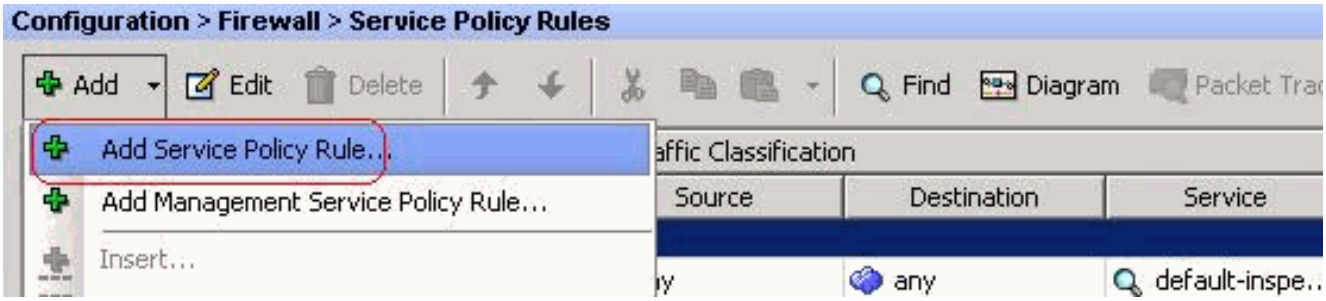
BlockDomainClass. Klik op

OKStel de actie in als **Reset** en **Schakel** de vastlegging voor de klasse **BlockURLsClass**

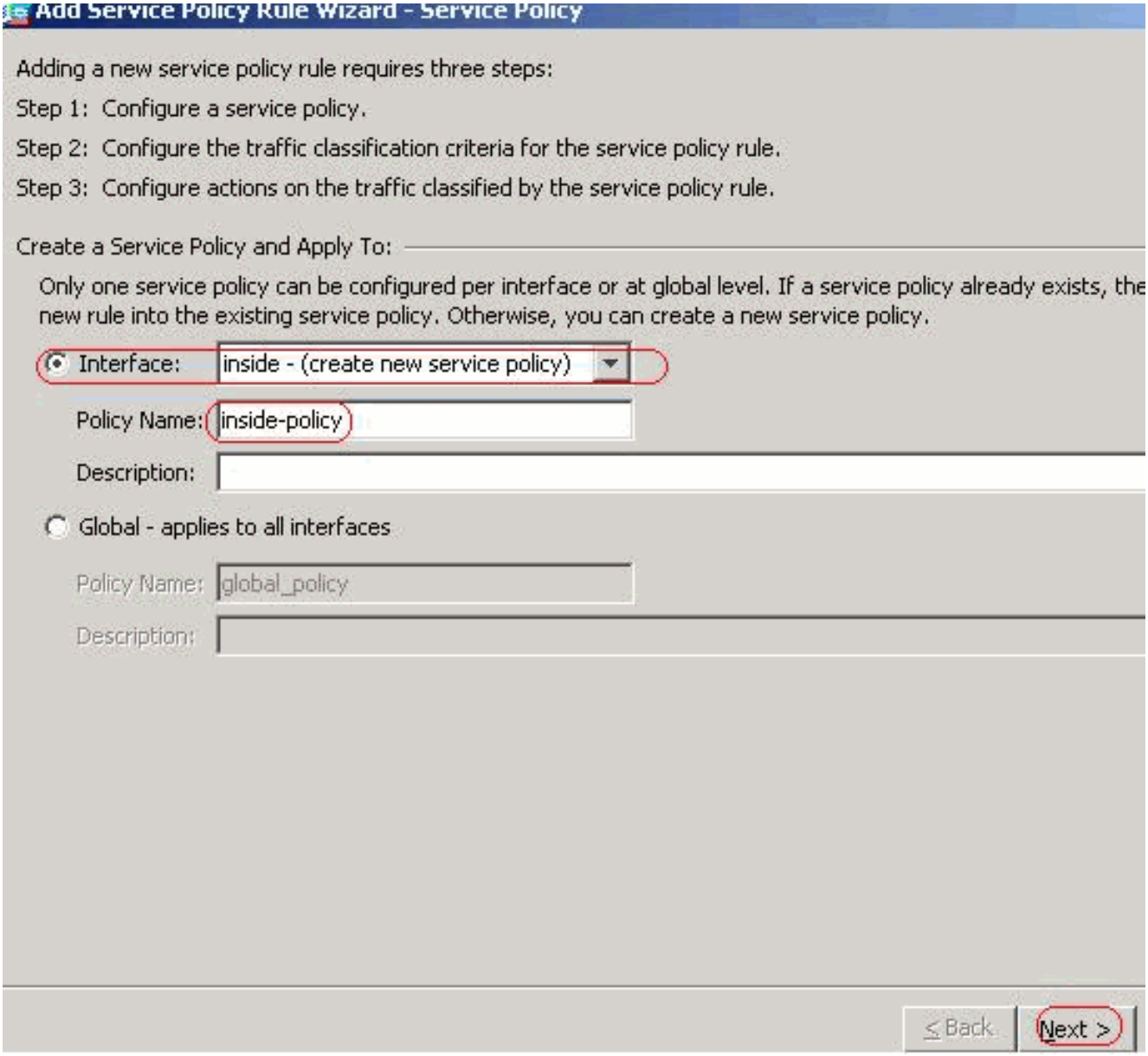


in. Klik op **OK**.Klik op **Toepassen**.**Compatibele CLI-configuratie**

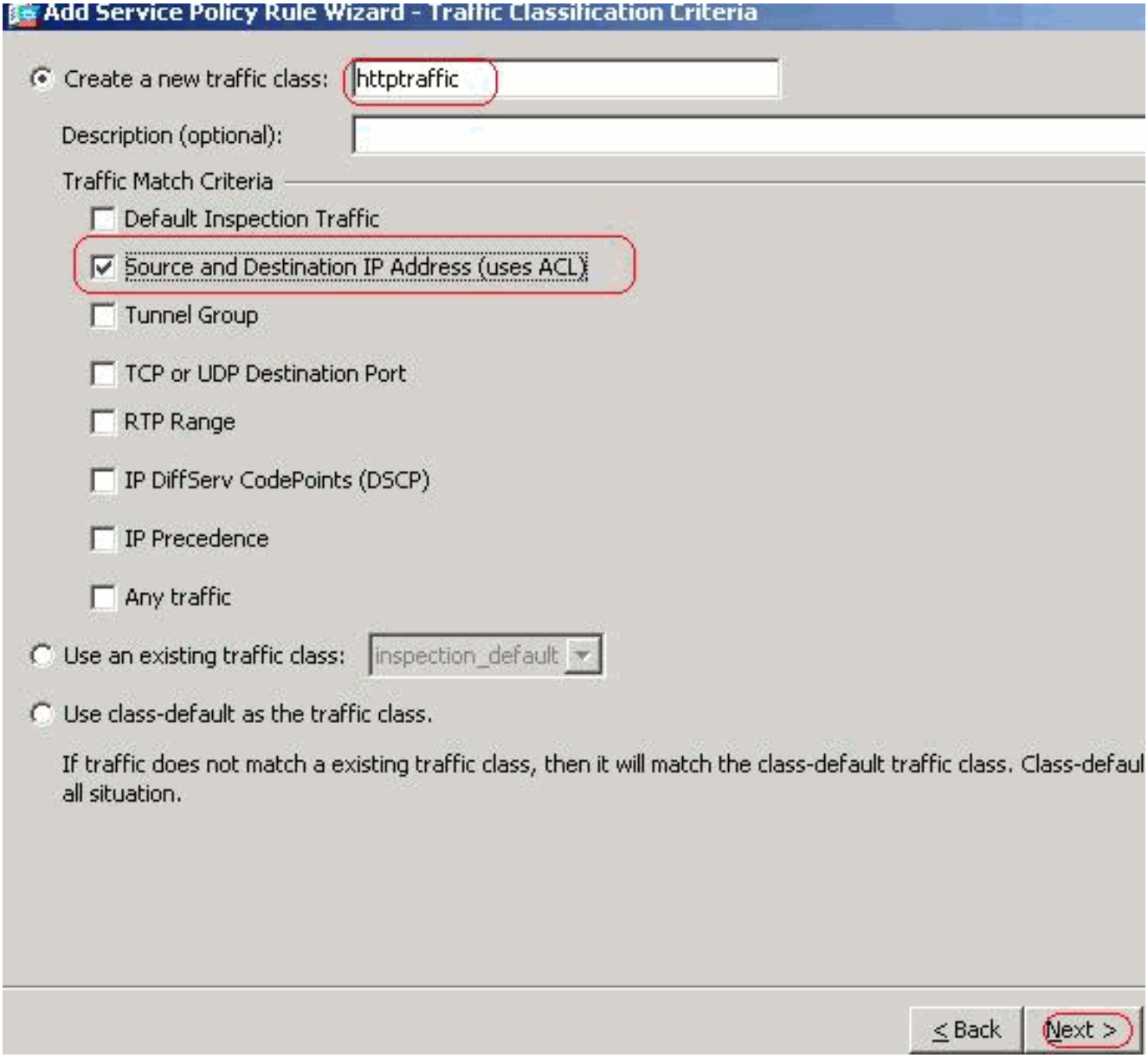
5. **Pas het http-beleid op de interface toe**Kies **Configuration > Firewall > Service Policy Rules > Add > Service Policy Rule**.



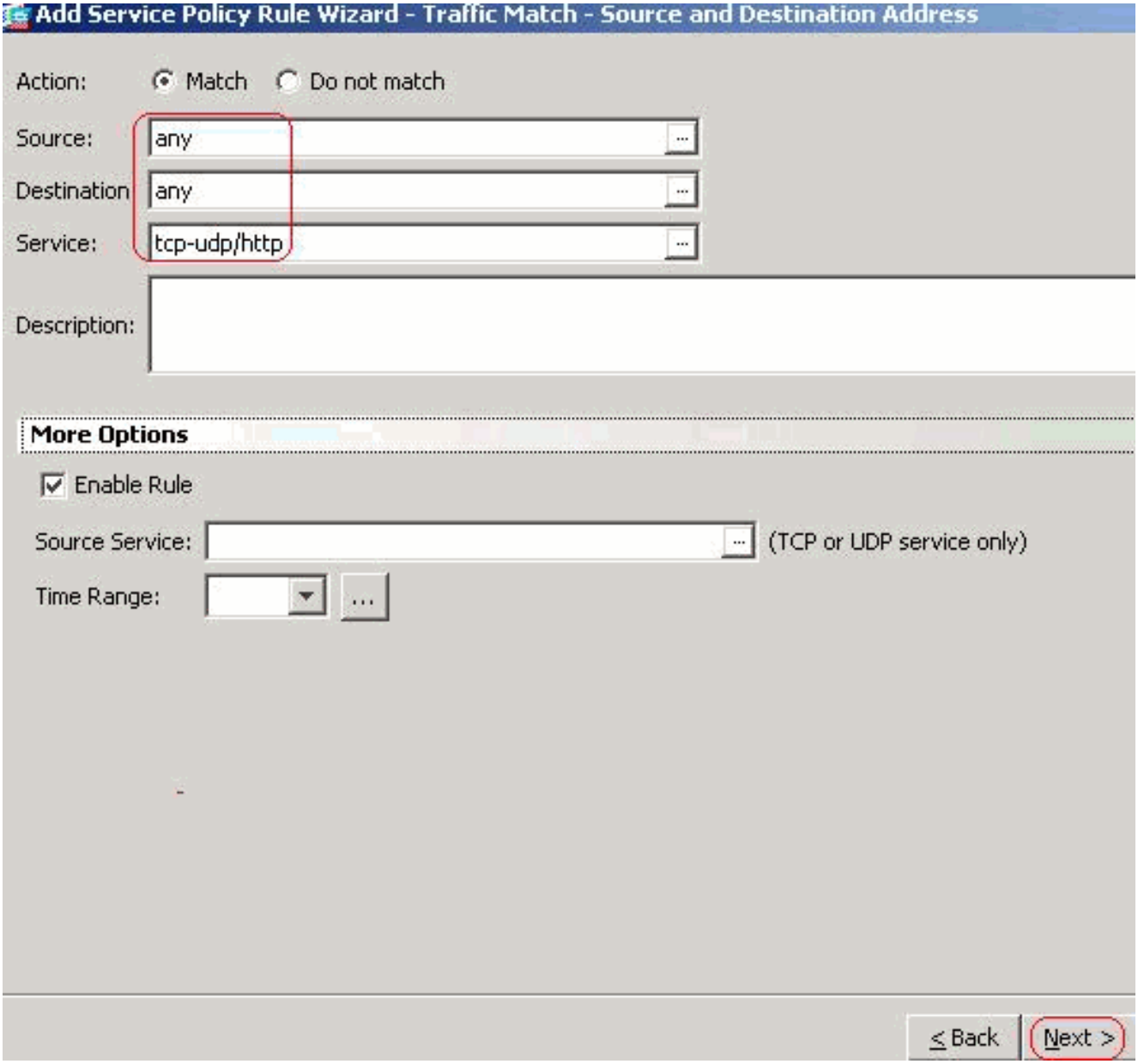
HTTP-verkeer Kies de knop **Interface** met interne interface in het uitrolmenu en de beleidsnaam als **binnenbeleid**. Klik op **Volgende**.



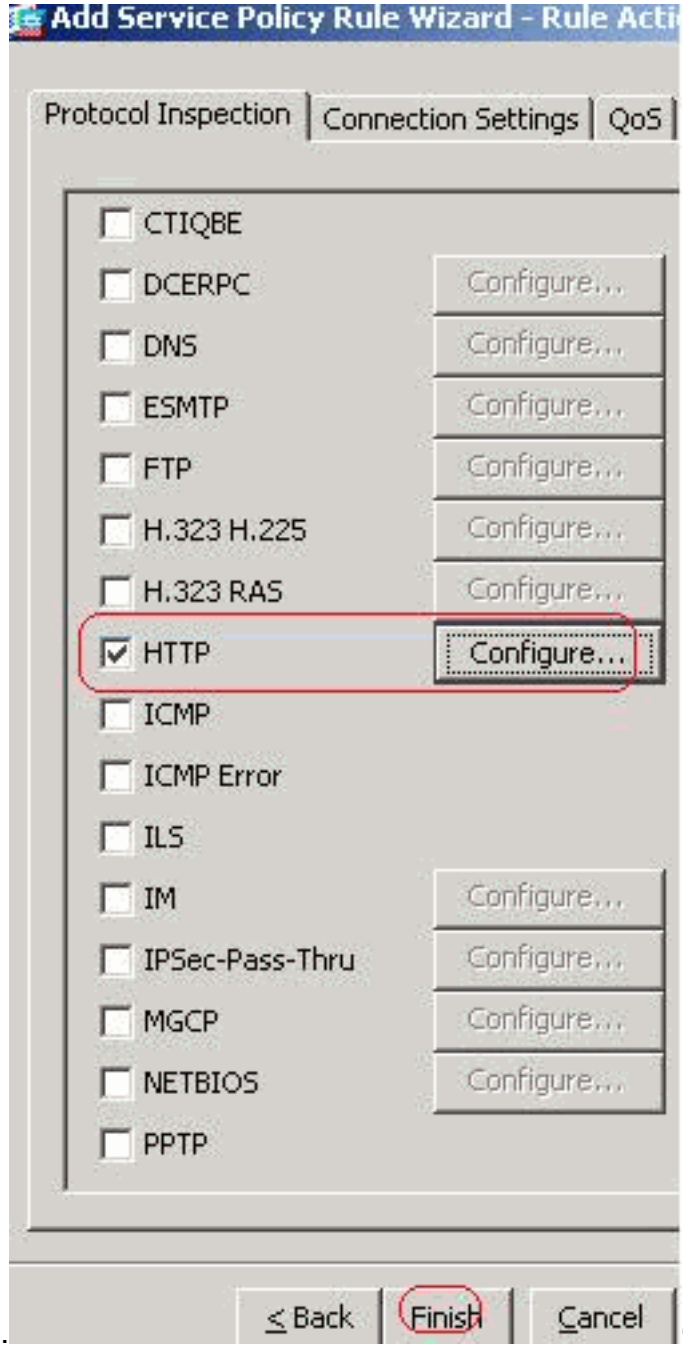
Maak een class map **httptraffic** en controleer het **IP-adres Bron** en **Bestemming (gebruikt ACL)**. Klik op
Volgende.



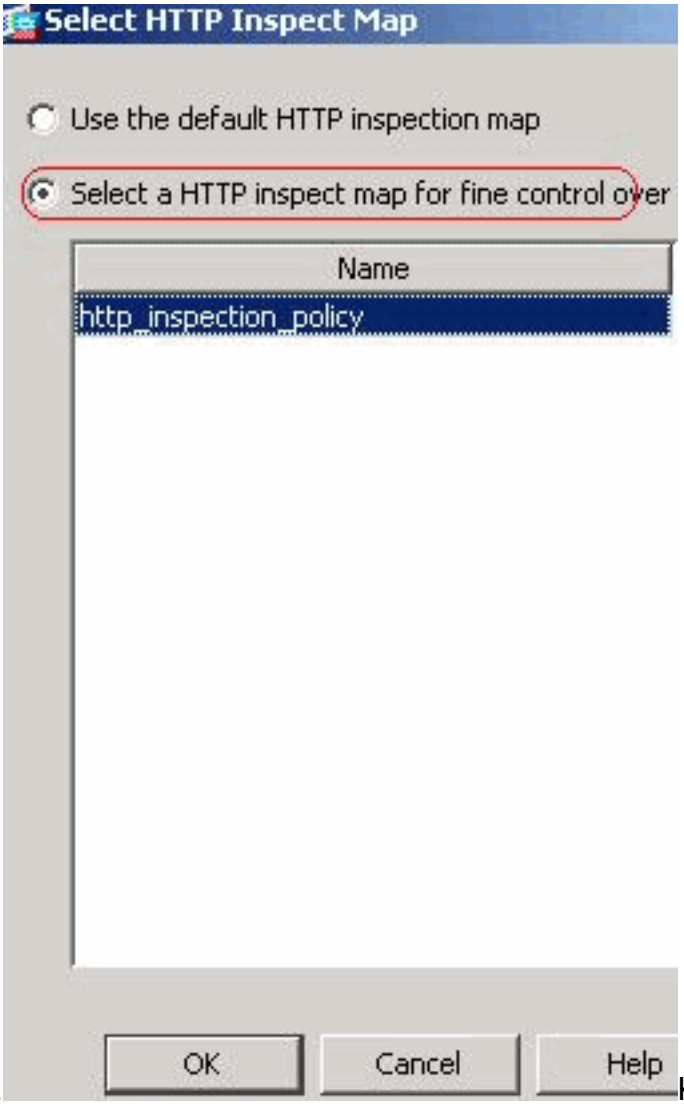
Kies de bron en de bestemming zoals elk met de service als **tcp-udp/http**. Klik op **Volgende**.



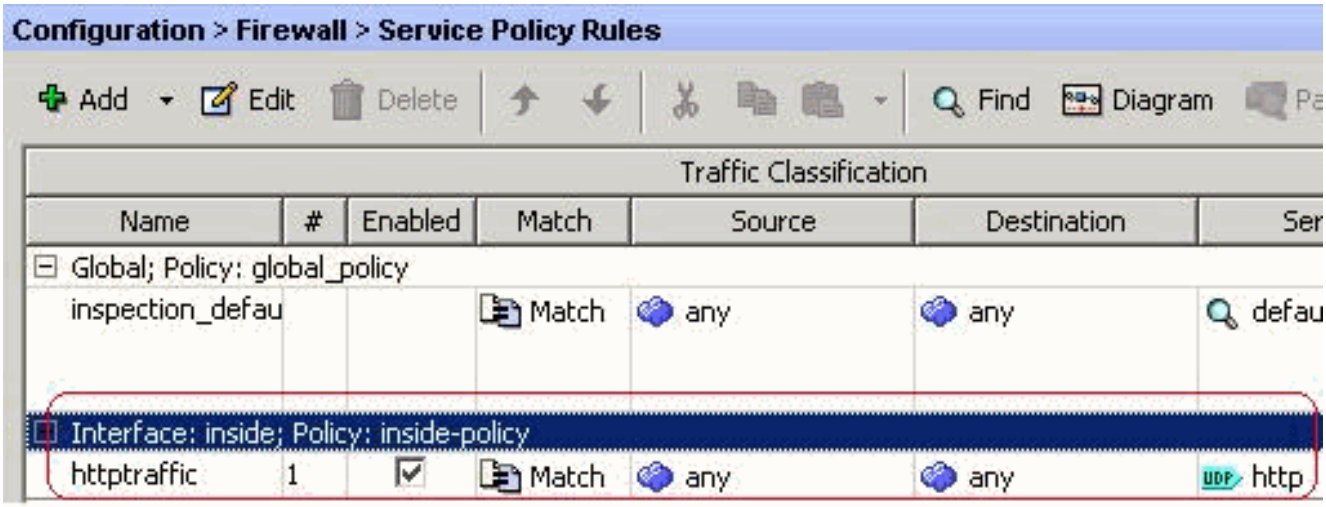
Controleer de **HTTP**-radioknop en klik op



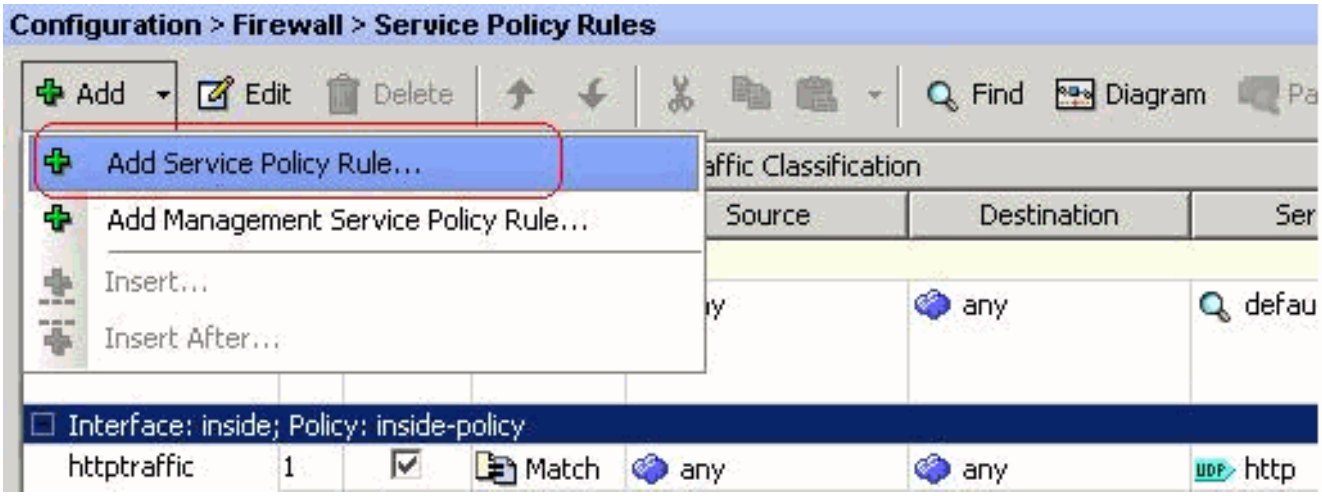
Configureren. Controleer de radioknop **Selecteer een HTTP-inspectiekaart voor de controle op de inspectie** zoals aangegeven. Klik



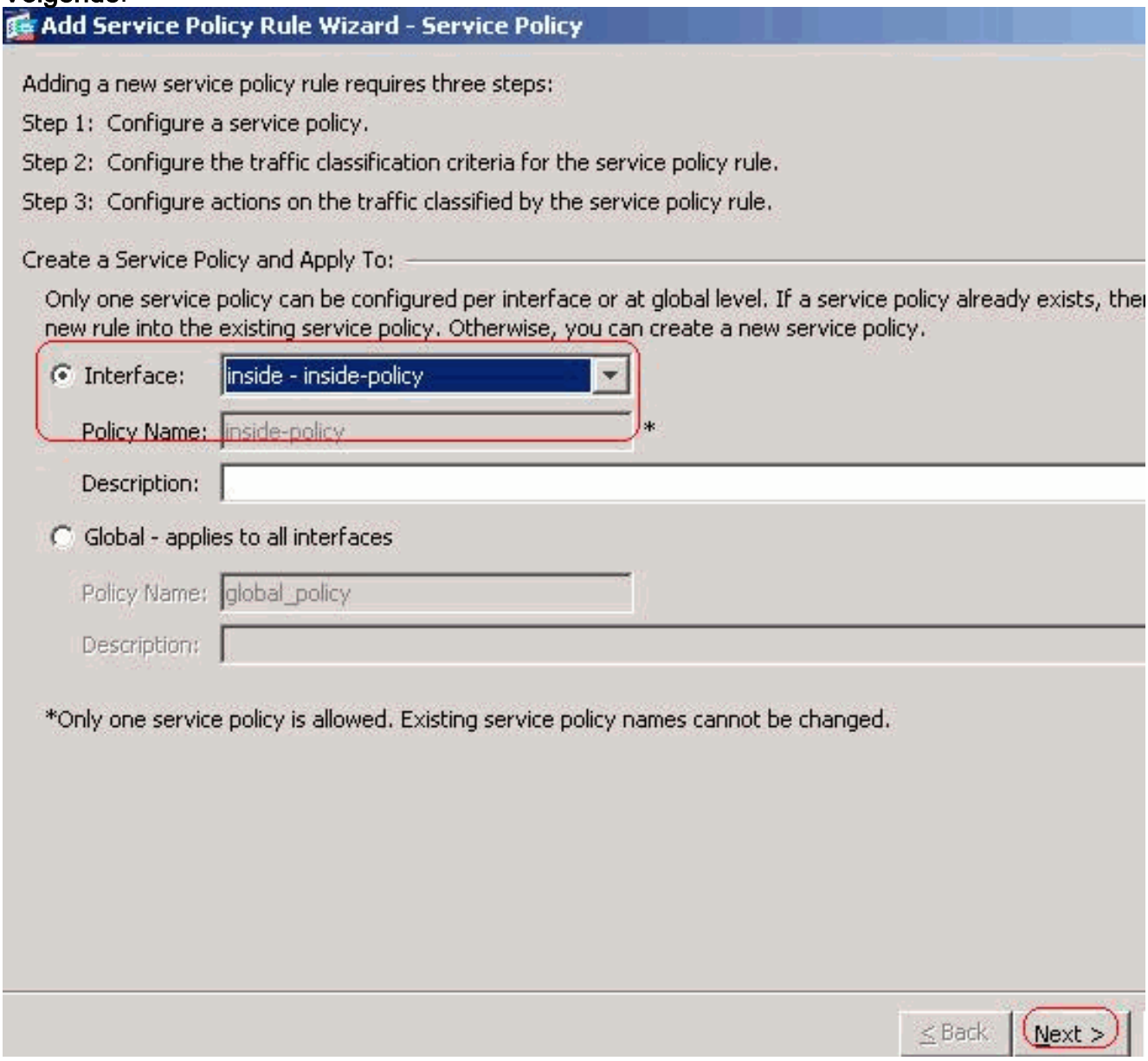
op **OK**.Klik op **Voltooien**.



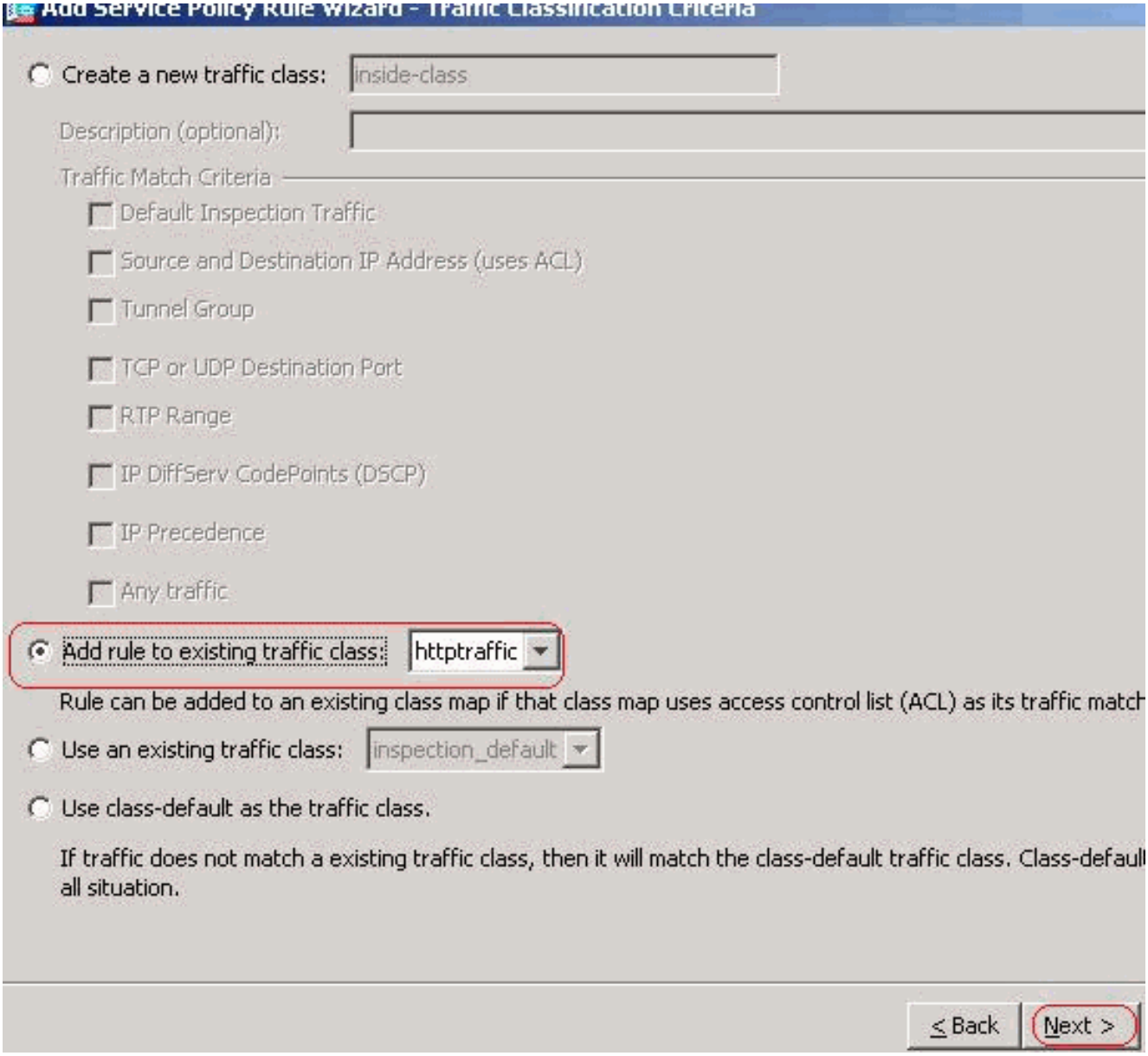
Port 8080-verkeer Kies opnieuw **Add > Add Service Policy Rule**.



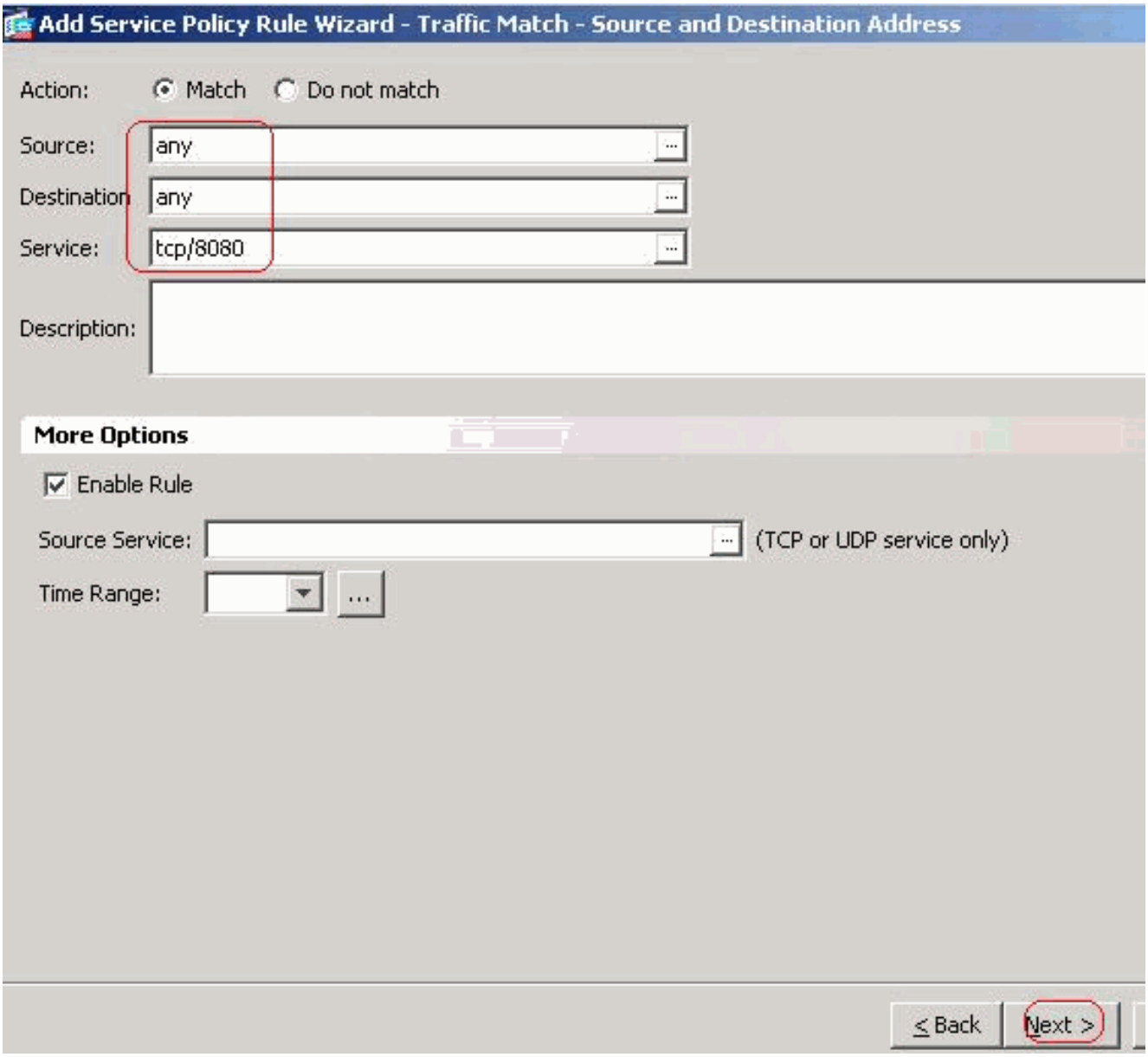
Klik op
Volgende.



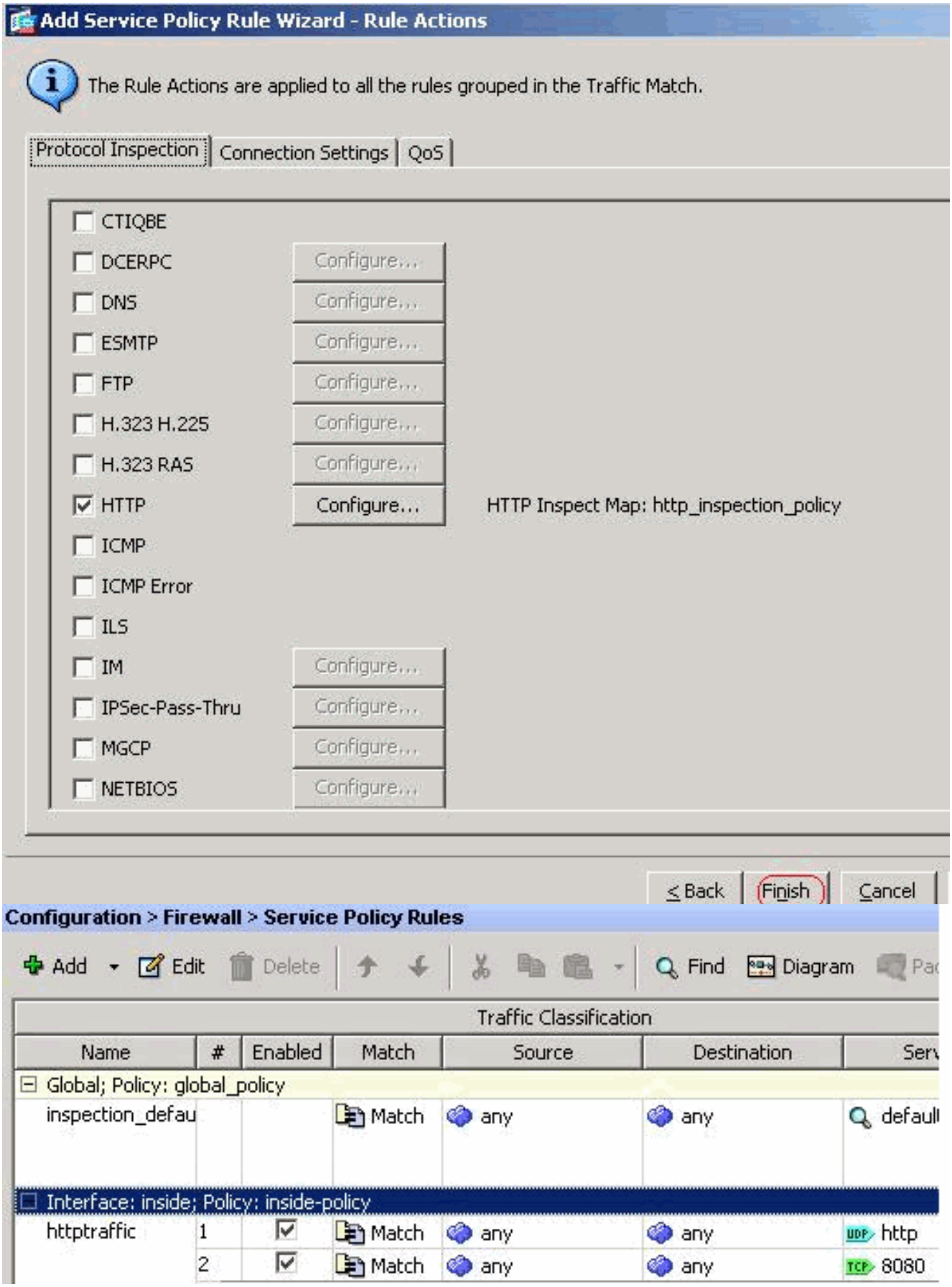
Kies de radioknop **Voeg regel aan bestaande verkeersklasse toe** en kies **httptraffic** in het uitrolmenu. Klik op
Volgende.



Kies de bron en de bestemming zoals gebruikelijk met **tcp/8080**. Klik op **Volgende**.



Klik op
Voltooien.



Klik op **Toepassen**.**Compatibele CLI-configuratie**

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **tonen in werking stellen-in werking stellen regex**-Toont de regelmatige expressies die zijn gevormd

```
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#
```

- **toon in werking stellen-in werking stellen-enig klembord**-toont de class kaarten die zijn gevormd

```
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#
```

- **toon in werking stellen-enig beleid-in kaart type inspectie http**—toont de beleidskaarten die het http verkeer inspecteren dat is gevormd

```
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#
```

- **toon in werking stellen-beslist politiek-kaart**-toont alle beleid-kaart configuraties evenals de standaard beleid-kaart configuratie

```
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#
```

- **toon in werking stellen-klaar dienst-beleid**-Beeldingen alle momenteel in werking gestelde de dienstbeleidsconfiguraties

```
ciscoasa#show running-config service-policy
service-policy global_policy global
service-policy inside-policy interface inside
```

- **Toon in werking stellen-beslist toegang-lijst**-Toont de toegang-lijst configuratie die op het veiligheidsapparaat loopt

```
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#
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug http**—toont de debug-berichten voor HTTP-verkeer

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- Ondersteuning van Cisco Adaptieve Security Devices Manager (ASDM)
- Cisco PIX 500 Series security applicaties
- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems