ASA/PIX 7.2:使用正規表示式和MPF配置示例阻止某些網站(URL)

目錄

簡介

本文說明如何使用模組化策略框架(MPF)的正規表示式配置思科安全裝置ASA/PIX 7.2，以便阻止某些網站(URL)。

注意：此配置不會阻止所有應用程式下載。對於可靠的檔案塊，必須使用專用裝置（如Websense等）或模組（如ASA的CSC模組）。

ASA不支援HTTPS過濾。ASA無法根據HTTPS流量的正規表示式執行深度資料包檢測或檢查，因為在HTTPS中，資料包的內容是加密的(ssl)。

必要條件

需求

本檔案假設思科安全裝置已設定並正常運作。

採用元件

- 執行軟體版本7.2(2)的Cisco 5500系列調適型安全裝置(ASA)
- 適用於ASA 7.2(2)的Cisco調適型安全裝置管理員(ASDM)版本5.2(2)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可以與運行軟體版本7.2(2)的Cisco 500系列PIX一起使用。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

模組化策略框架概述

MPF提供一致且靈活的方法來配置安全裝置功能。例如，可以使用MPF建立特定於特定TCP應用的超時配置，而不是應用於所有TCP應用的超時配置。

MPF支援以下功能：

- TCP規範化、TCP和UDP連線限制和超時以及TCP序列號隨機化
- CSC
- 應用檢測
- IPS
- QoS輸入管制
- QoS輸出管制
- QoS優先順序隊列

MPF的配置包括四項任務：

1. 確定您要對其應用操作的第3層和第4層流量。如需詳細資訊，請參閱使用第3/4層類別對映識別流量。
2. （僅適用於應用檢測）定義應用檢測流量的特殊操作。有關詳細資訊，請參閱為應用程式檢查配置特殊操作。
3. 將操作應用於第3層和第4層流量。有關詳細資訊，請參閱使用第3/4層策略對映定義操作。
4. 啟用介面上的操作。如需詳細資訊，請參閱使用服務原則將第3/4層原則套用到介面。

正規表示式

正規表示式可以按字面意思完全匹配文本字串，也可以按元字元匹配文本字串，因此您可以匹配文本字串的多個變體。可以使用正規表示式來匹配某些應用程式流量的內容；例如，您可以匹配HTTP資料包中的URL字串。

注意：使用**Ctrl+V**對CLI中的所有特殊字元進行轉義，如問號(?)或製表符。例如，鍵入**d[Ctrl+V]g**在配置中輸入**d?g**。

要建立正規表示式，請使用**regex**命令，該命令可用於需要文本匹配的各種功能。例如，您可以使用

帶有檢測策略對映的模組化策略框架配置用於應用檢測的特殊操作(請參閱policy map type inspect命令)。 在檢測策略對映中，如果您建立了一個包含一個或多個匹配命令的檢測類對映，則可以標識要對其執行操作的流量，或者可以直接在檢測策略對映中使用**match**命令。有些**match**命令可用於使用正規表示式識別資料包中的文本；例如，您可以匹配HTTP資料包中的URL字串。可以在正規表示式類對映中組合正規表示式(請參見class-map type regex命令)。

表1列出了具有特殊意義的元字元。

字元	**說明**	**備註**
.	點	匹配任何單個字元。例如，**d.g**匹配dog、dag、dtg和包含這些字元的任何單詞，如doggonnit。
(exp)	子表達式	子表達式將字元與周圍的字元隔開，以便可以在子表達式上使用其他元字元。例如，**d(o|a)g匹配**dog和dag，但**do|ag匹配**do和ag。子表達式還可以與重複量詞一起使用，以區分用於重複的字元。例如，**ab(xy){3}z匹配**abxyxyxyz。
|	交替	匹配它所分隔的任一表達式。例如，**dog|cat匹配**dog或cat。
?	問號	一個量詞，表示有0或1個先前的表達式。例如，**lo?se**匹配lse或lose。 **注意：**必須輸入**Ctrl+V**，然後呼叫問號，否則將呼叫幫助函式。
*	星號	一個量詞，表示有0、1或任何數量的上一個表達式。例如，**lo*se**匹配lse、lose、loose等。
{x}	重複量詞	準確重複x次。例如，**ab(xy){3}z匹配**abxyxyxyz。
{x,}	最小重複量詞	重複至少x次。例如，**ab(xy){2,}z匹配**abxyxyz、abxyxyxyz等。
[abc]	字元類	匹配方括弧中的任何字元。例如，**[abc]**匹配a、b或c。
[^abc]	否定字元類	匹配方括弧中不包含的單個字元。例如，**[^abc]匹配**除a、b或c以外的任何字元。**[^A-Z]匹配**任何非大寫字母的單個字元。
[a-c]	字元範圍類	匹配範圍內的任何字元。**[a-z]匹配**任何小寫字母。可以混合字元和範圍：**[abcq-z]匹配**a、b、c、q、r、s、t、u、v、w、x、y、z和**[a-cq-z]等**。如果短劃線(-)字元是括弧中的最後一個或第一個字元，則該字元為文字字元：**[abc-]**或**[-abc]**。
""	引號	保留字串中的尾部或前導空格。例如，**"test」會在查詢匹**配時保留前導空格。
^	插入符號	指定行的開始。
\	跳脫字元	與元字元一起使用時，匹配文字字元。例

		如， \[匹配左方括弧。
char	字元	當字元不是元字元時，匹配文字字元。
\r	回車	匹配回車0x0d。
\n	新行	匹配新行0x0a。
\t	頁籤	匹配頁籤0x09。
\f	Formfeed	匹配表單源0x0c。
\xNN	轉義的十六進位制數	匹配十六進位制（精確為兩位數）的ASCII字元。
\NNN	轉義的八進位制數	將ASCII字元匹配為八進位（精確為三位）。 例如，字元040表示一個空格。

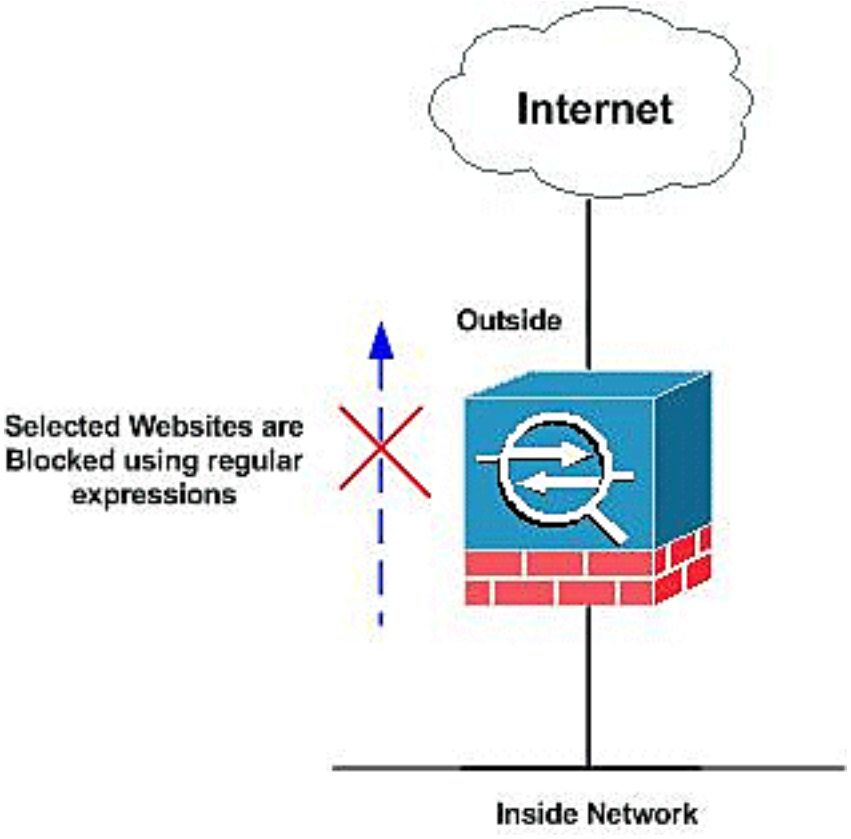
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

ASA CLI配置

ASA CLI配置

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(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
```

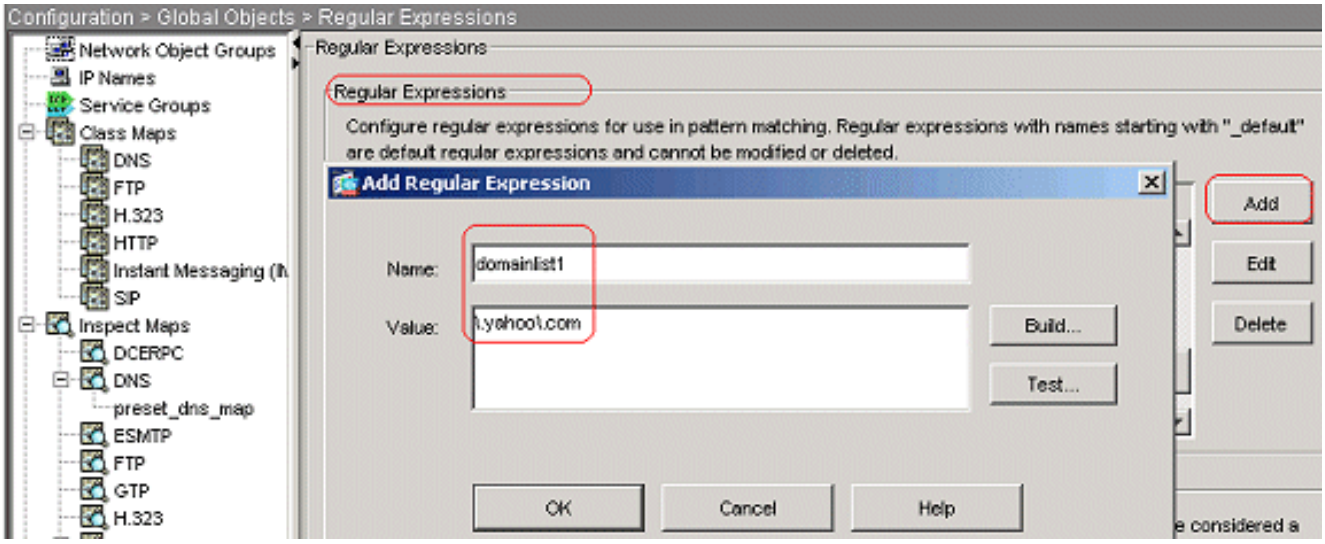
```
to be captured and provided !--- the http version being
used by web browser must be either 1.0 or 1.1 regex
urllist4 ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz])
HTTP/1.[01]"

!--- 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 will be blocked prompt hostname context
Cryptochecksum:e629251a7c37af205c289cf78629fc11 : end
ciscoasa#
```

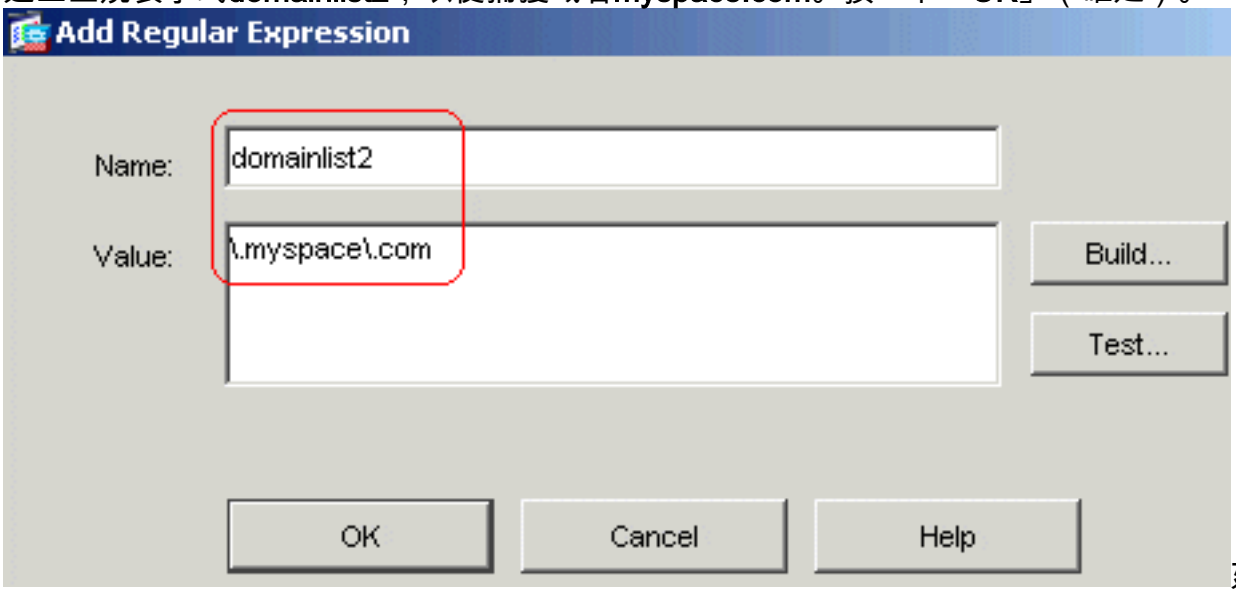
採用ASDM 5.2的ASA配置7.2(x)

完成以下步驟以配置正規表示式，並將其應用到MPF以阻止特定網站：

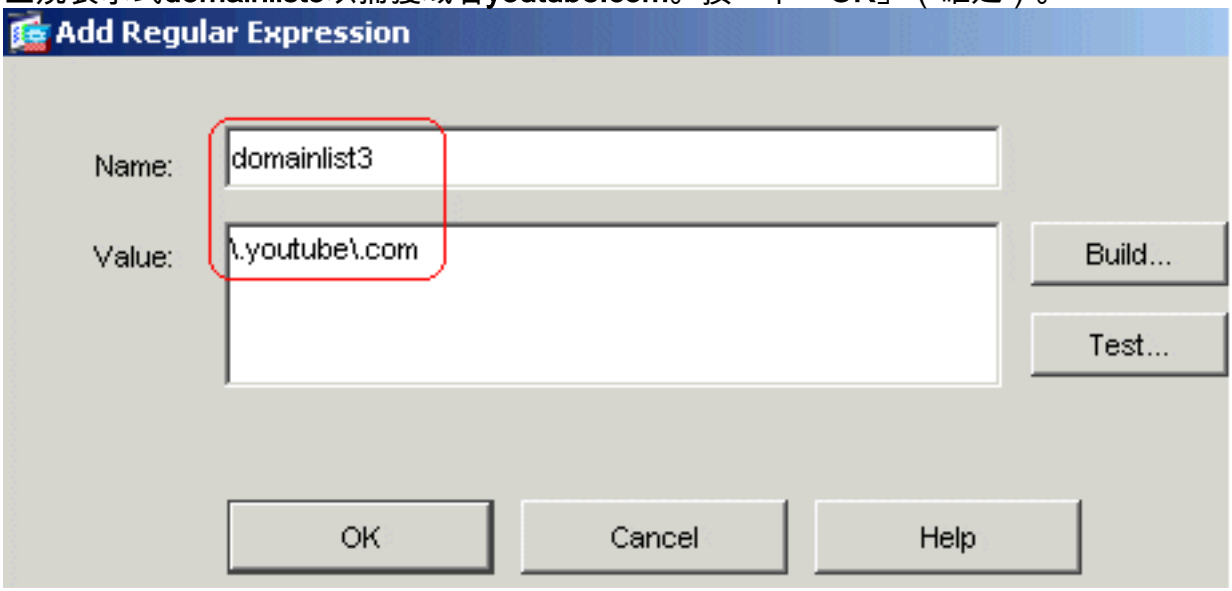
1. **建立正規表示式**選擇**Configuration > Global Objects > Regular Expressions**，然後按一下Regular Expression頁籤下的**Add**以建立正規表示式。建立正規表示式**domainlist1**，以便捕獲域名**yahoo.com**。按一下「**OK**」（確定）。



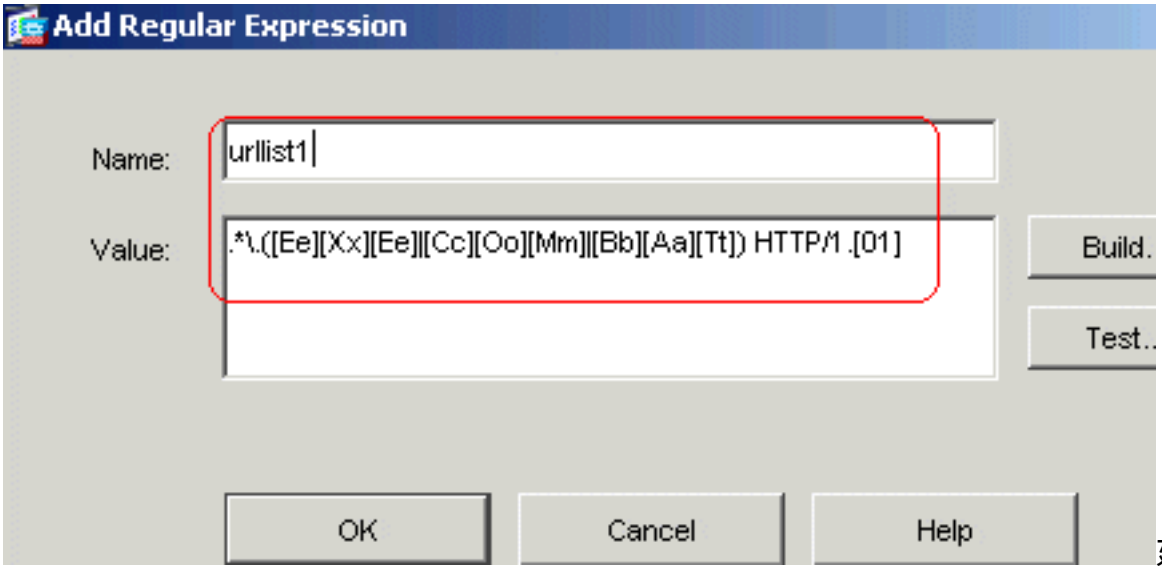
建立正規表示式**domainlist2**，以便捕獲域名**myspace.com**。按一下「**OK**」（確定）。



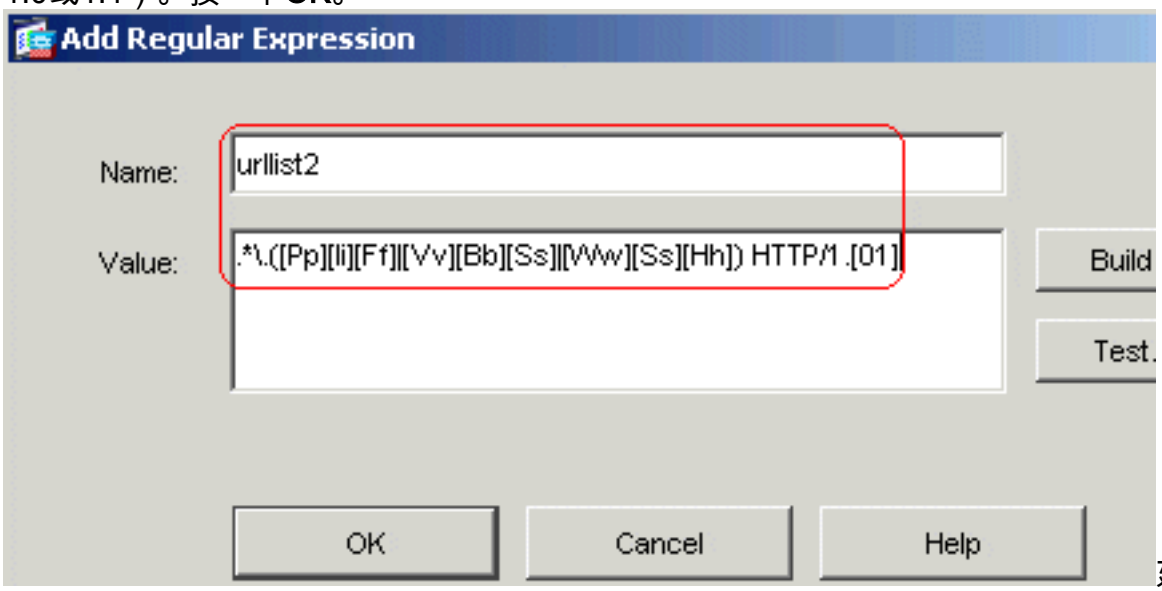
建立正規表示式**domainlist3**以捕獲域名**youtube.com**。按一下「**OK**」（確定）。



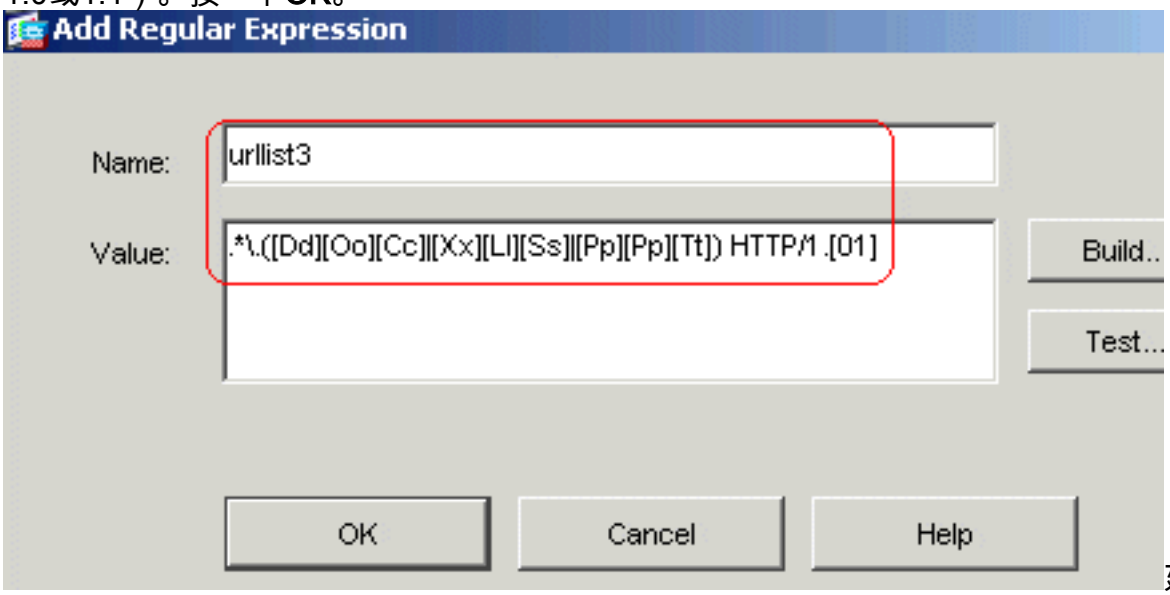
如果網路瀏覽器使用的http版本必須是1.0或1.1，請建立正規表示式urllist1，以便捕獲副檔名，如**exe**、**com**和**bat**。按一下**OK**。



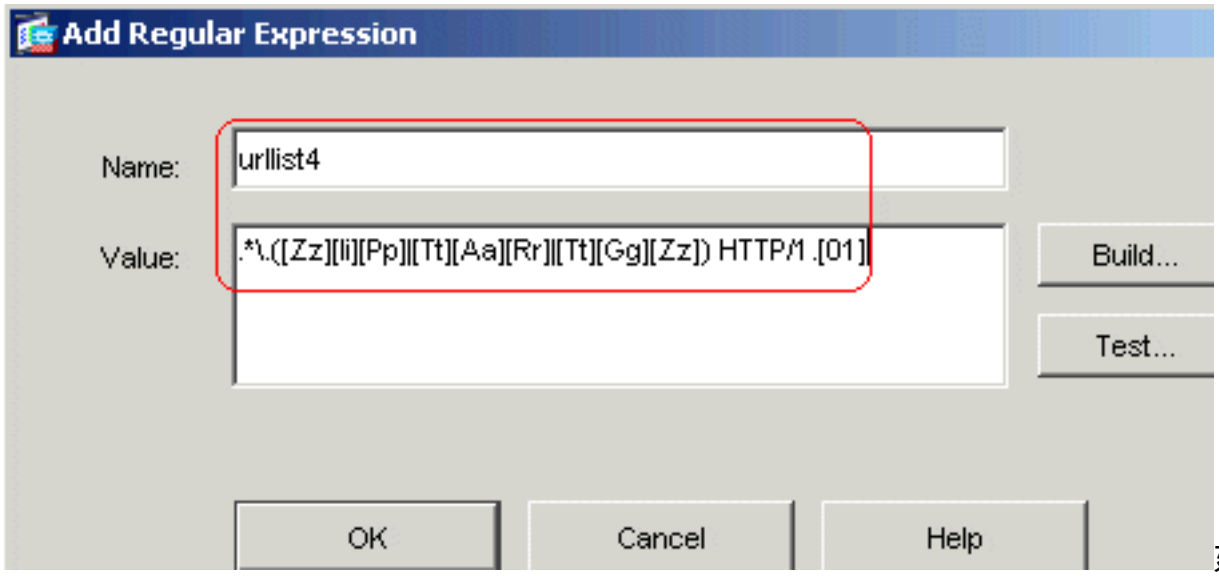
建立一個正規表示式urllist2，以便捕獲副檔名，如**pif**、**vbs**和wsh（前提是Web瀏覽器使用的HTTP版本是1.0或1.1）。按一下**OK**。



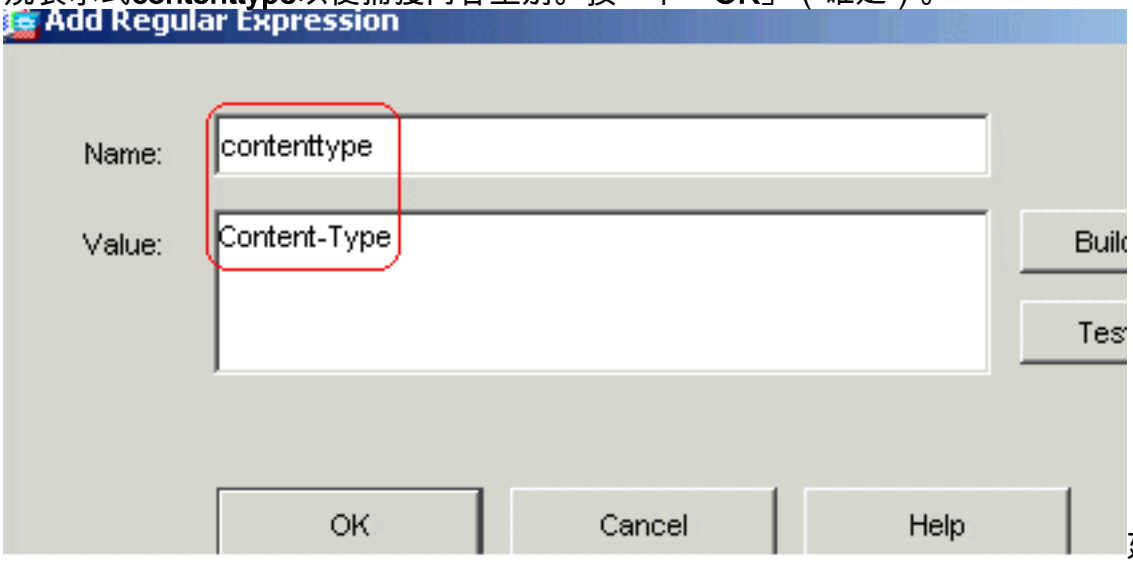
建立一個正規表示式urllist3，以便捕獲副檔名，如**doc**、**xls**和ppt（如果Web瀏覽器使用的HTTP版本是1.0或1.1）。按一下**OK**。



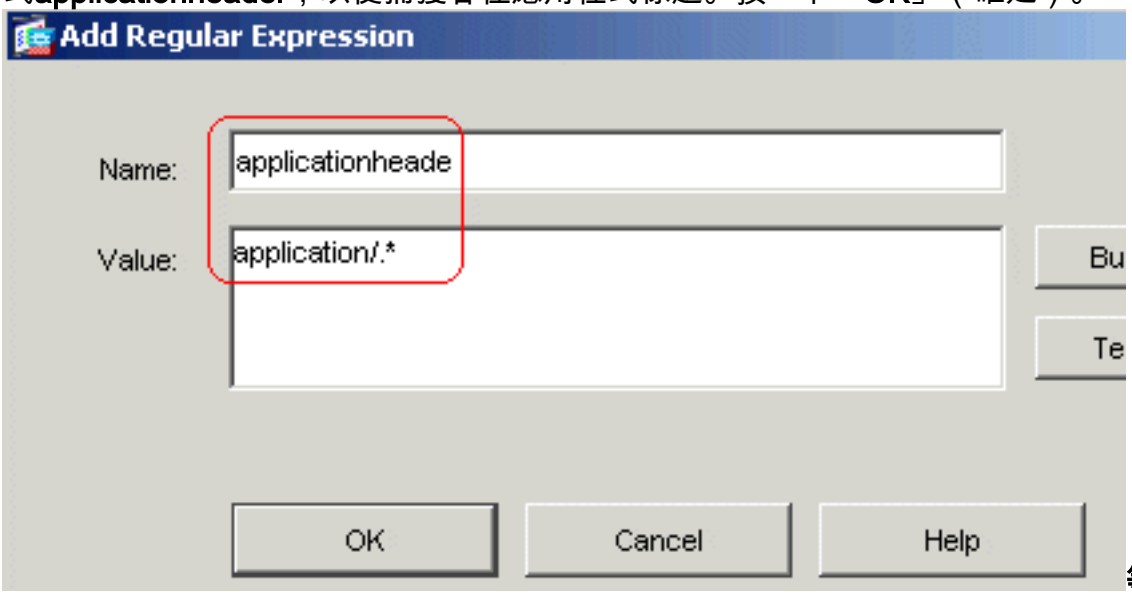
建立正規表示式urllist4，以擷取檔案擴充模組，例如**zip**、**tar**和**tgz**，前提是Web瀏覽器使用的HTTP版本是1.0或1.1。按一下**OK**。



建立正規表示式**contenttype**以便捕獲內容型別。按一下「**OK**」（確定）。

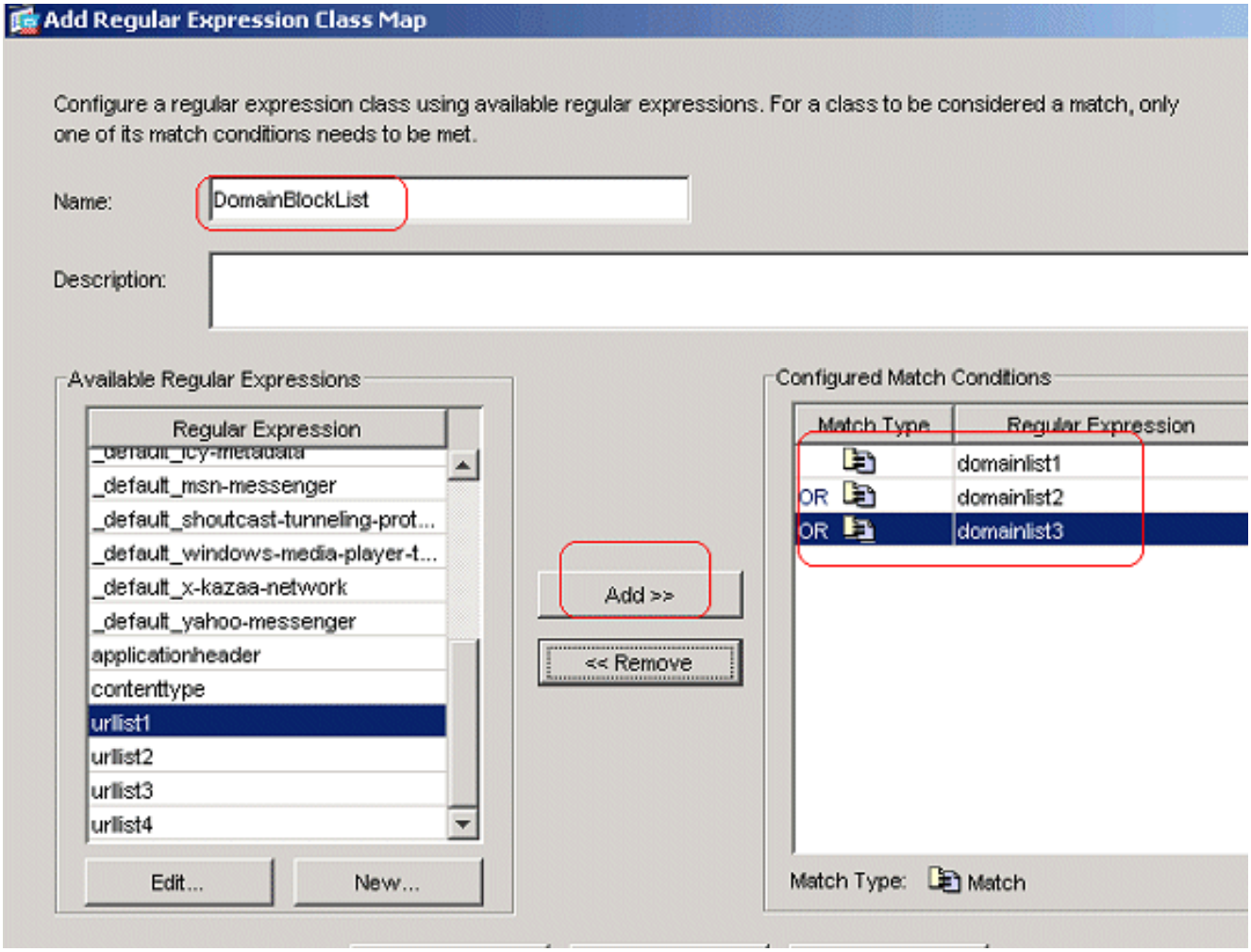


建立正規表示式**applicationheader**，以便捕獲各種應用程式標題。按一下「**OK**」（確定）。

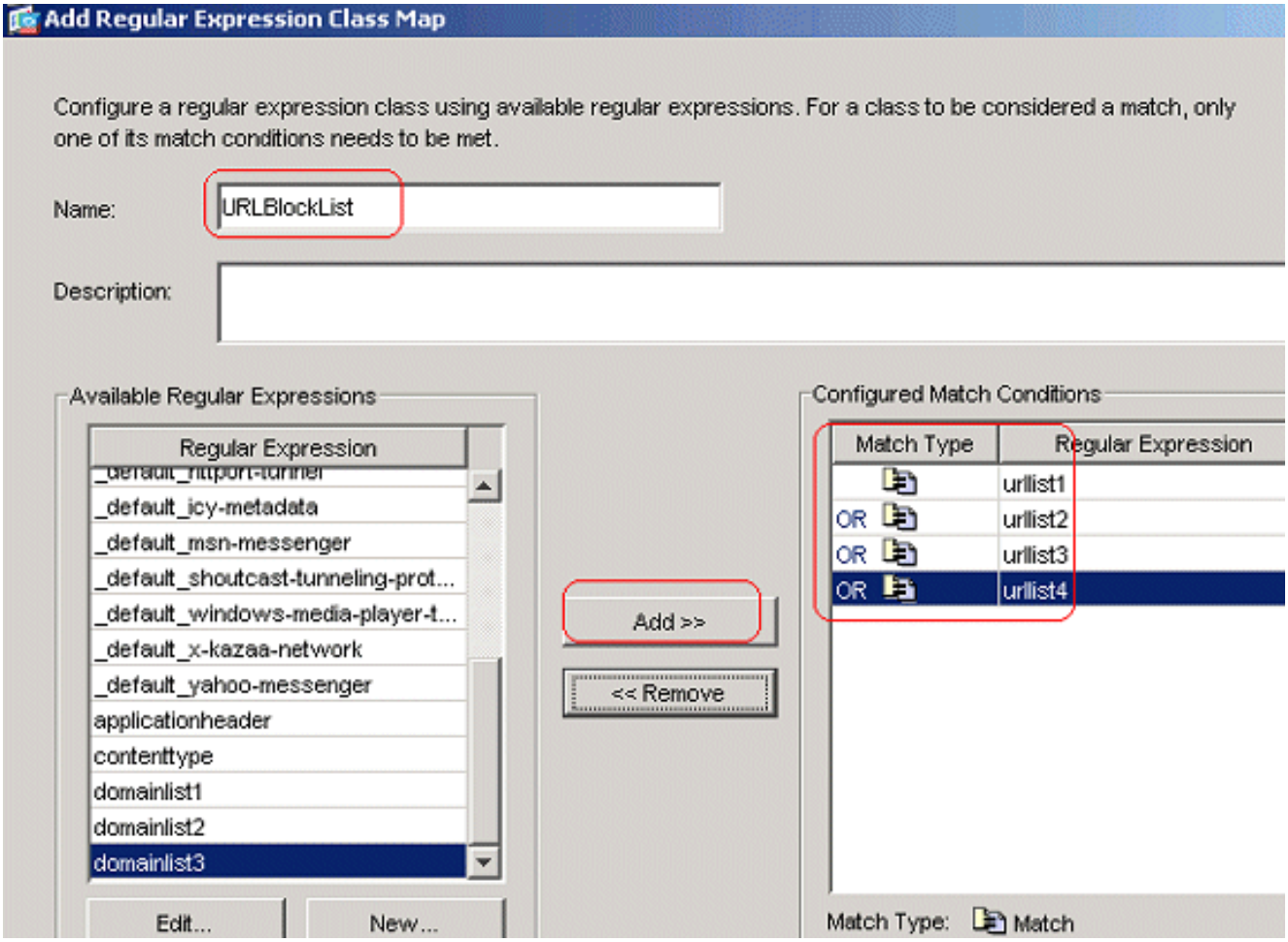


等效的CLI配置

2. **建立正規表示式類**選擇**Configuration > Global Objects > Regular Expressions**，然後在**Regular Expression Classes**頁籤下按一下**Add**以建立各種類。建立正規表示式**類DomainBlockList**，以便匹配任何正規表示式：domainlist1、domainlist2和domainlist3。按一下**確定**。

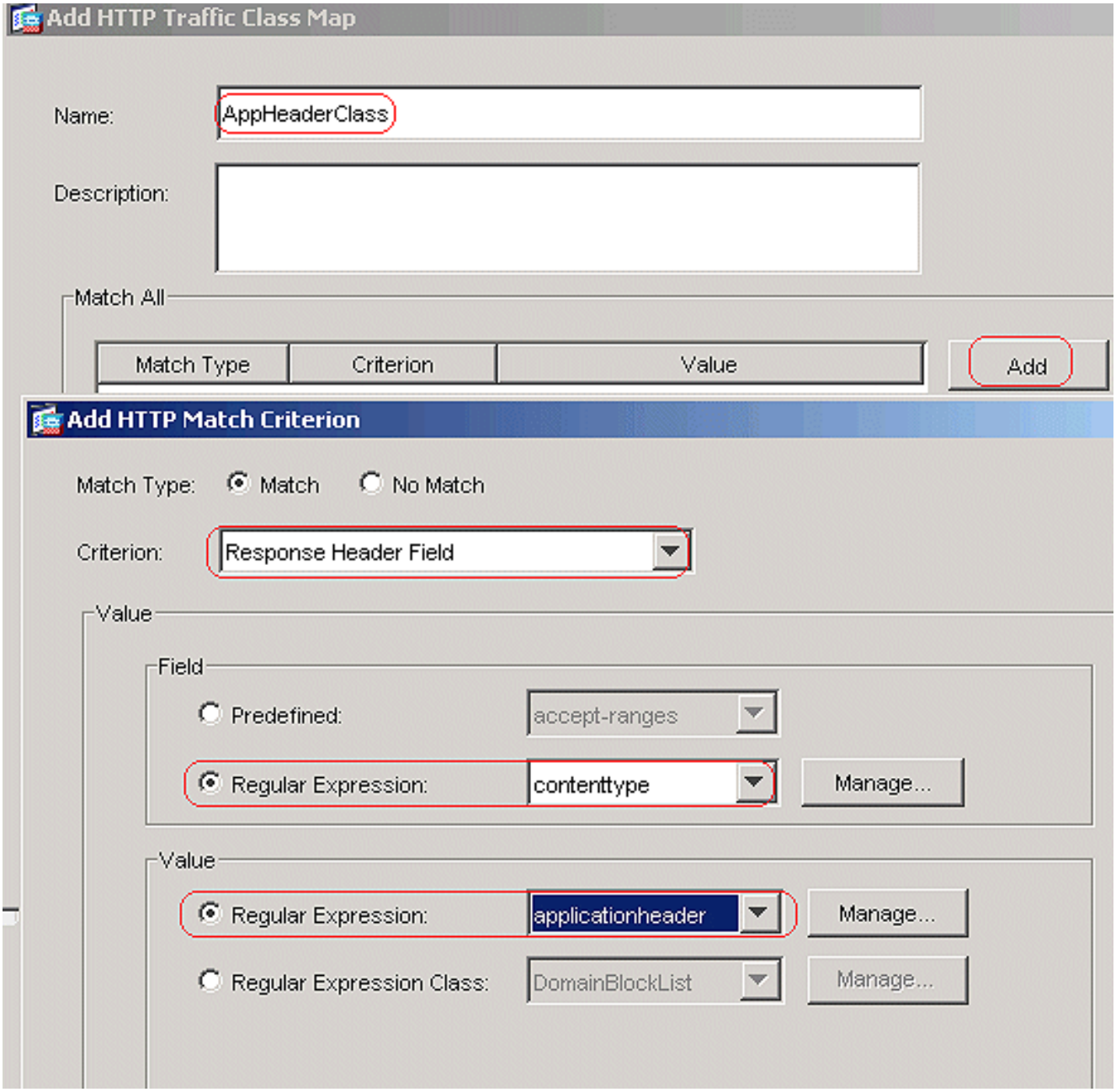


建立正規表示式**類URLBlockList**，以便匹配任何正規表示式：urllist1、urllist2、urllist3和urllist4。按一下**確定**。

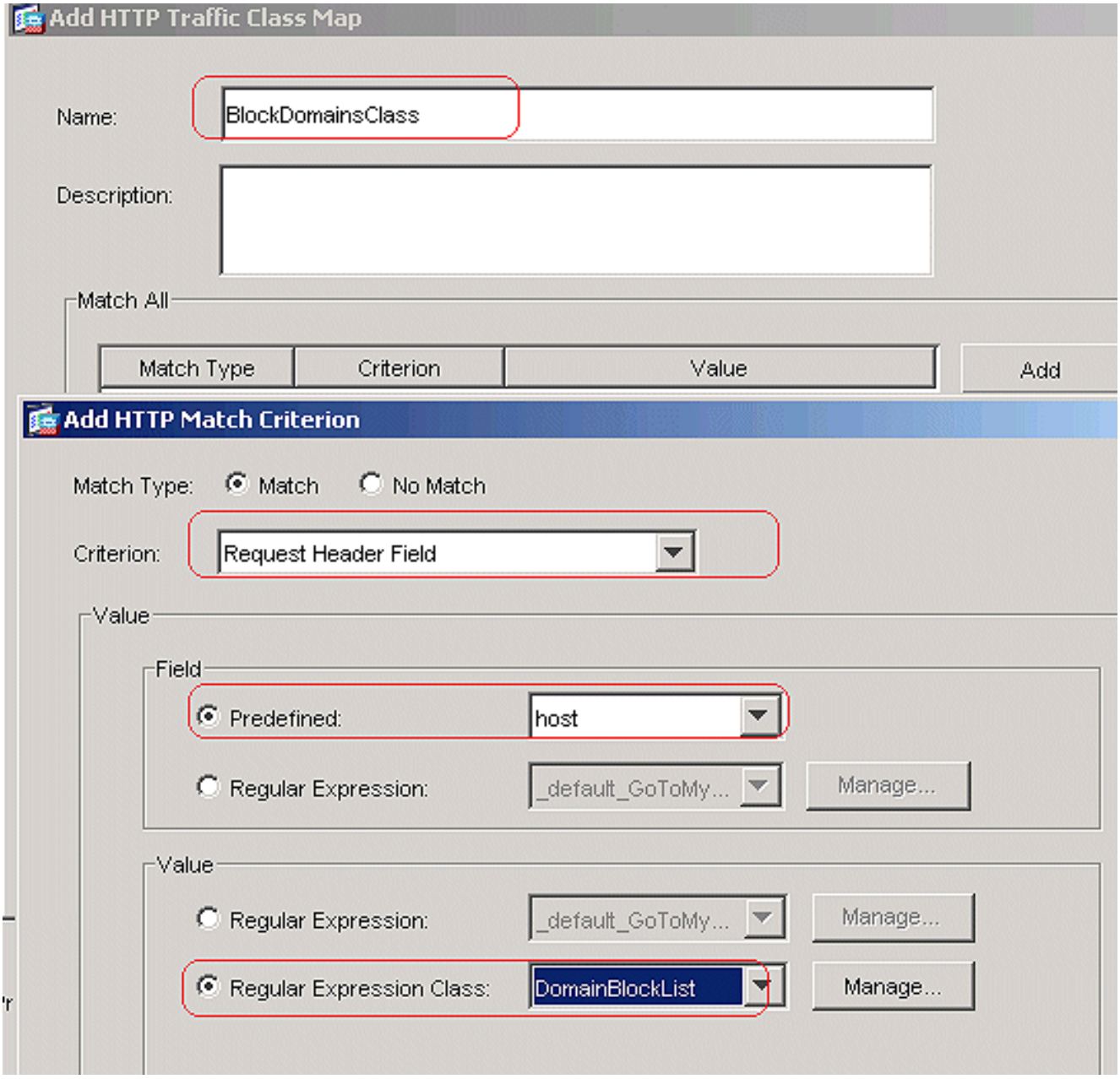


等效的CLI配置

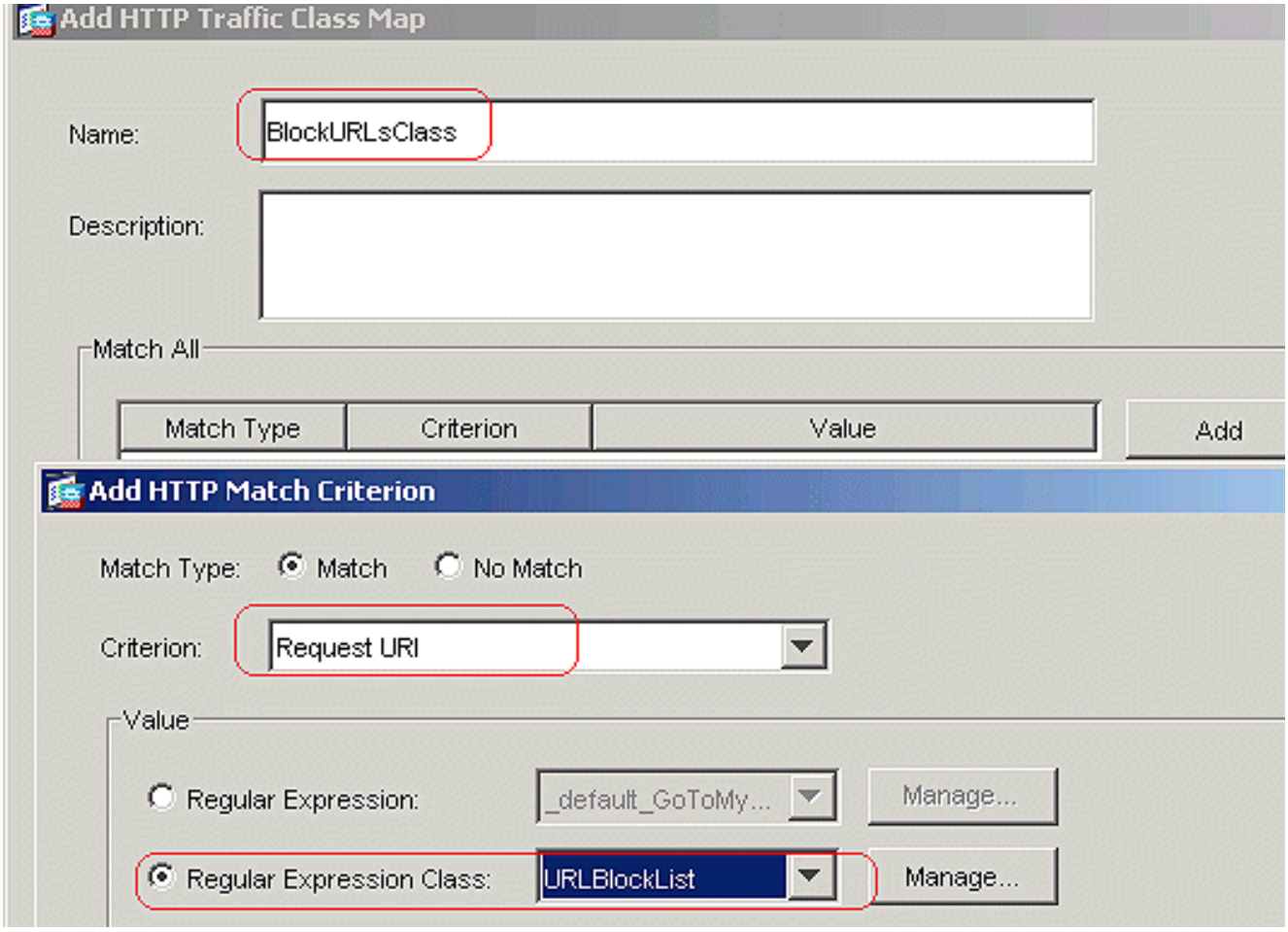
3. **使用類別對映檢查已識別的流量**選擇**Configuration > Global Objects > Class Maps > HTTP > Add**，以建立類對映來檢查由各種正規表示式識別的HTTP流量。建立類對映**AppHeaderClass**，以便將響應報頭與正規表示式捕獲相匹配。



按一下「**OK**」（確定）。建立類對映**BlockDomainsClass**，以將請求標頭與正規表示式捕獲相匹配。

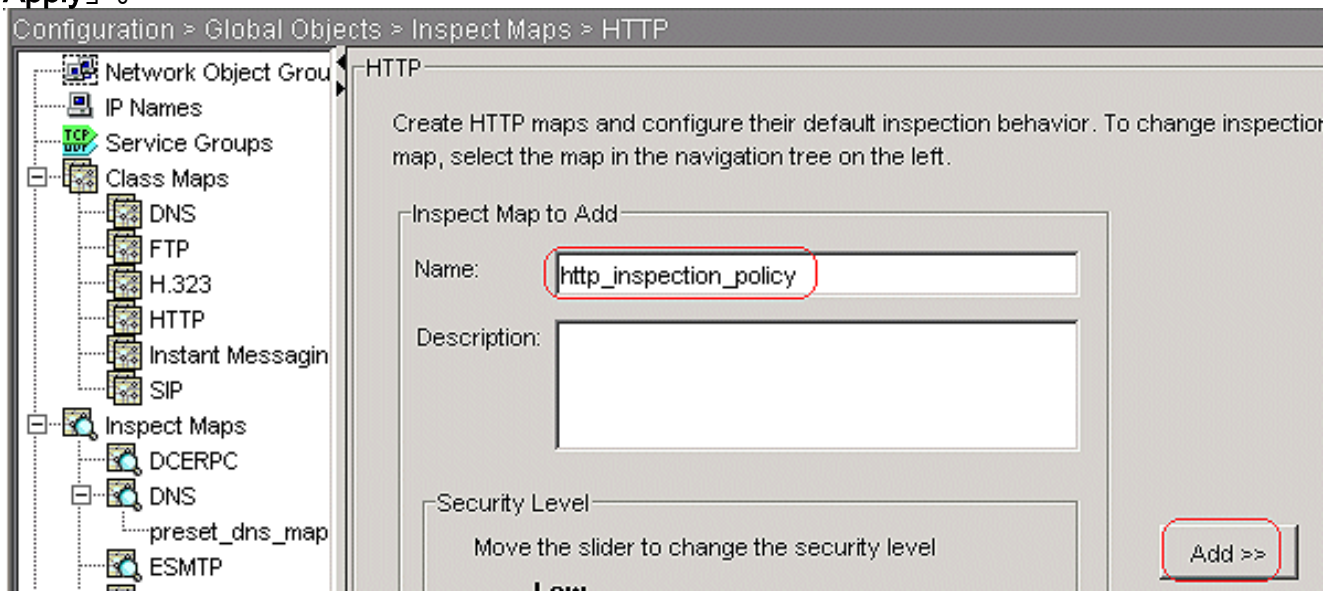


按一下「**OK**」（確定）。建立類對映**BlockURLsClass**，以便使用正規表示式捕獲匹配請求URI。

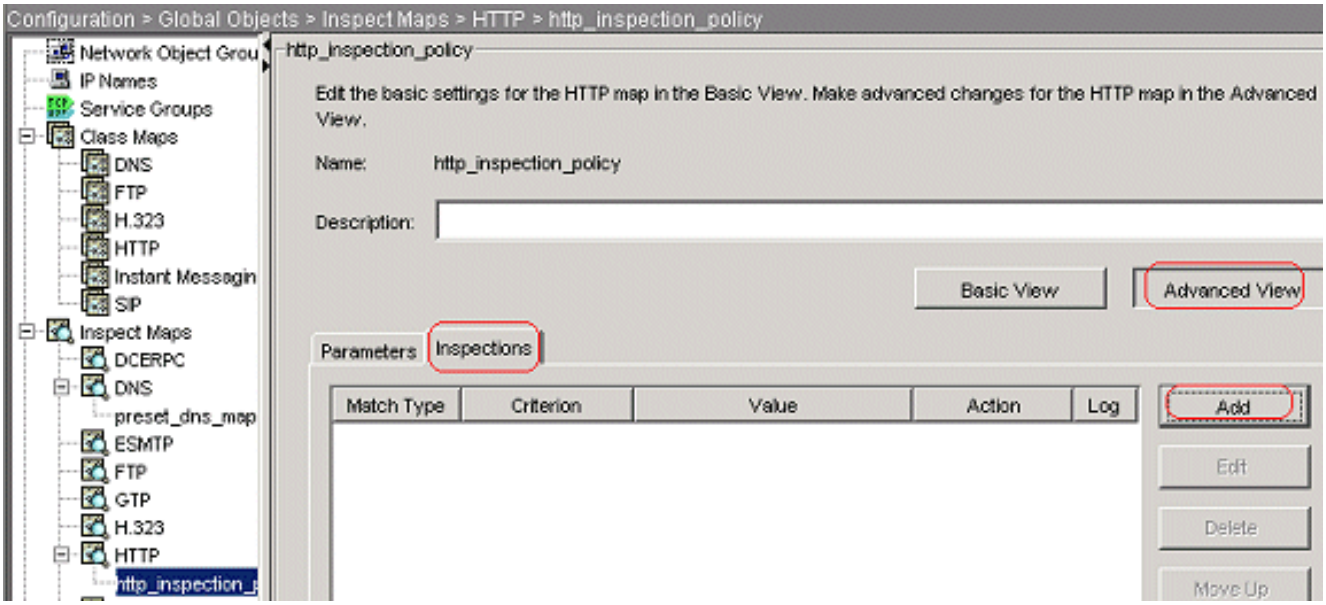


按一下「OK」（確定）。**等效的CLI配置**

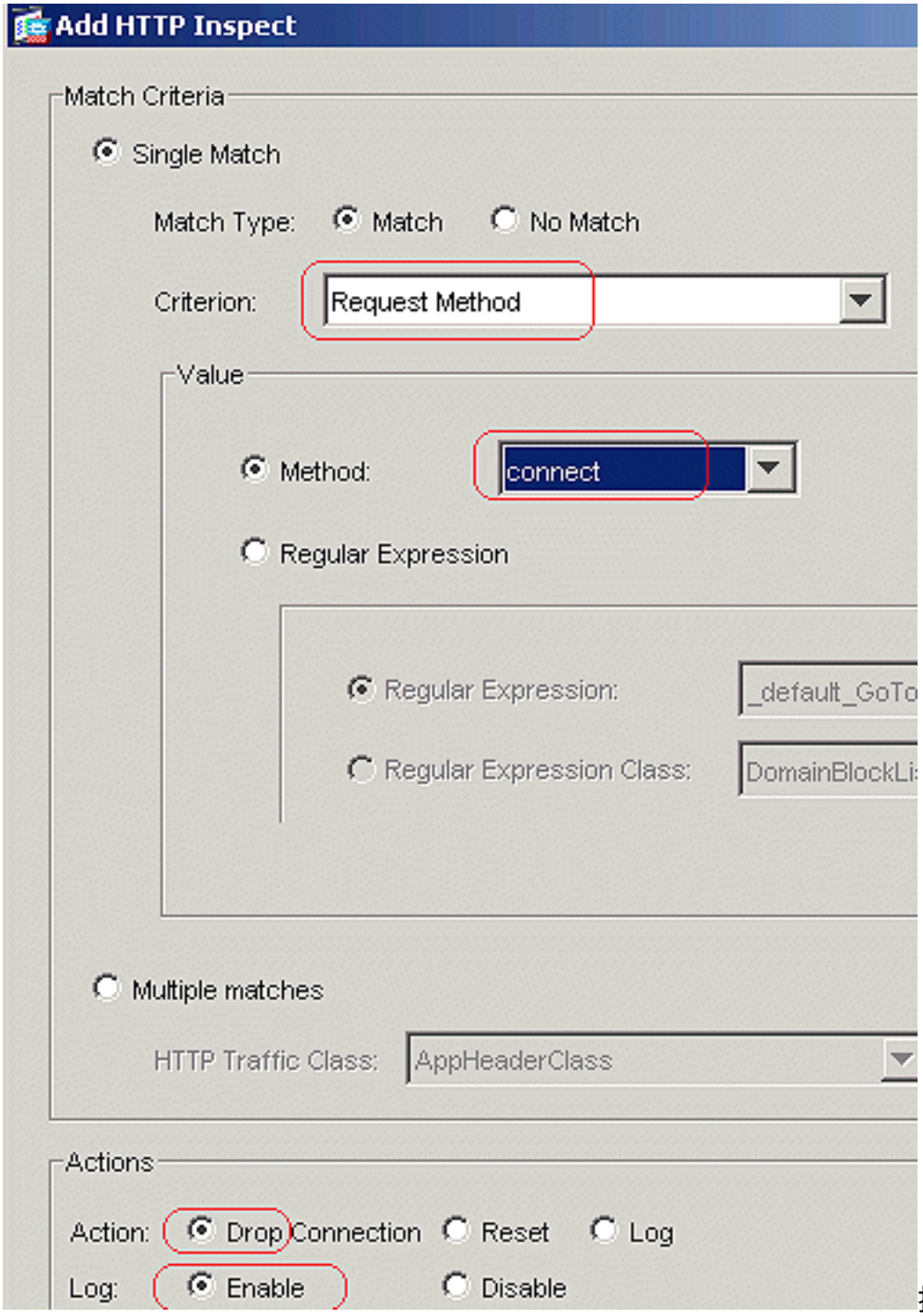
4. **為檢查策略中的匹配流量設定操作**選擇**Configuration > Global Objects > Inspect Maps > HTTP**，以便建立**http_inspection_policy**，為匹配的流量設定操作。按一下「**Add**」和「**Apply**」。



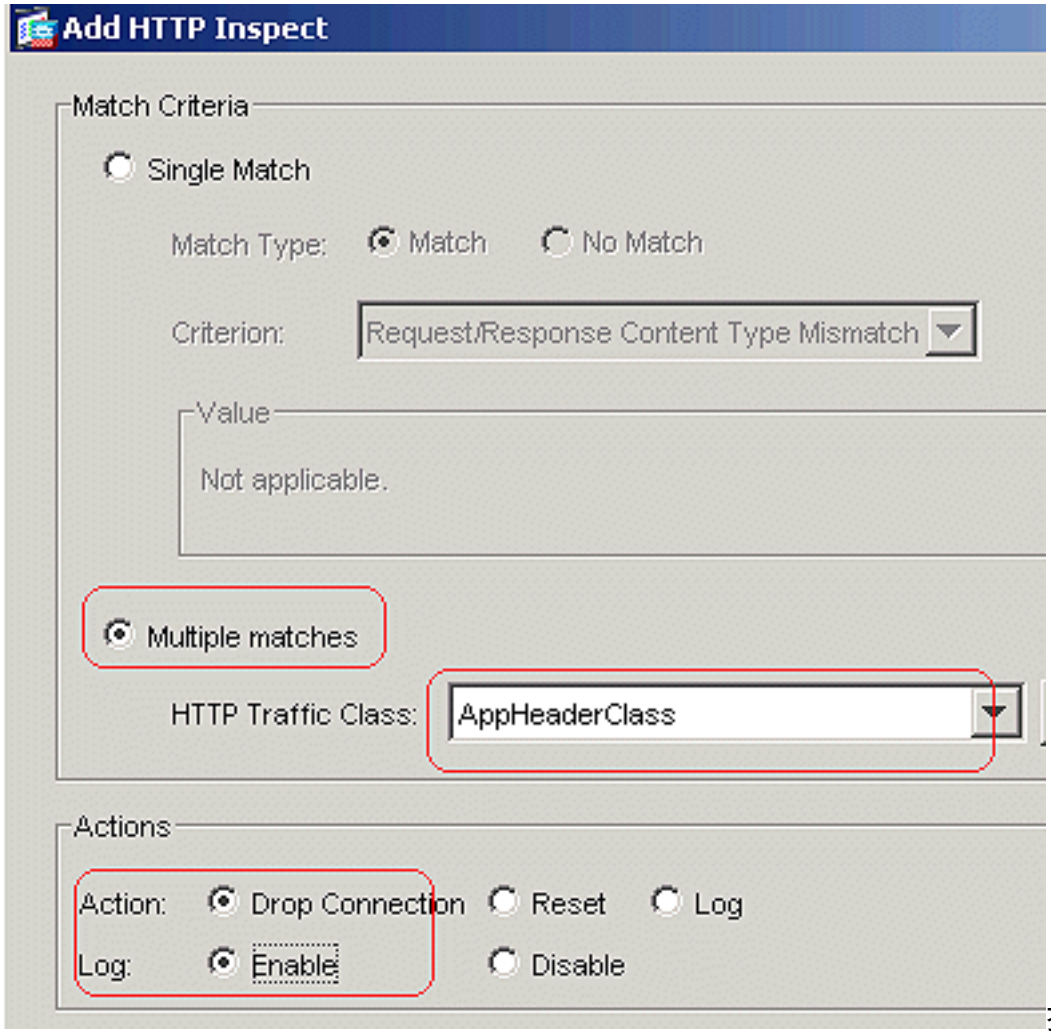
選擇**Configuration > Global Objects > Inspect Maps > HTTP > http_inspection_policy**，然後點選**Advanced View > Inspections > Add**，以便為目前建立的各種類設定操作。



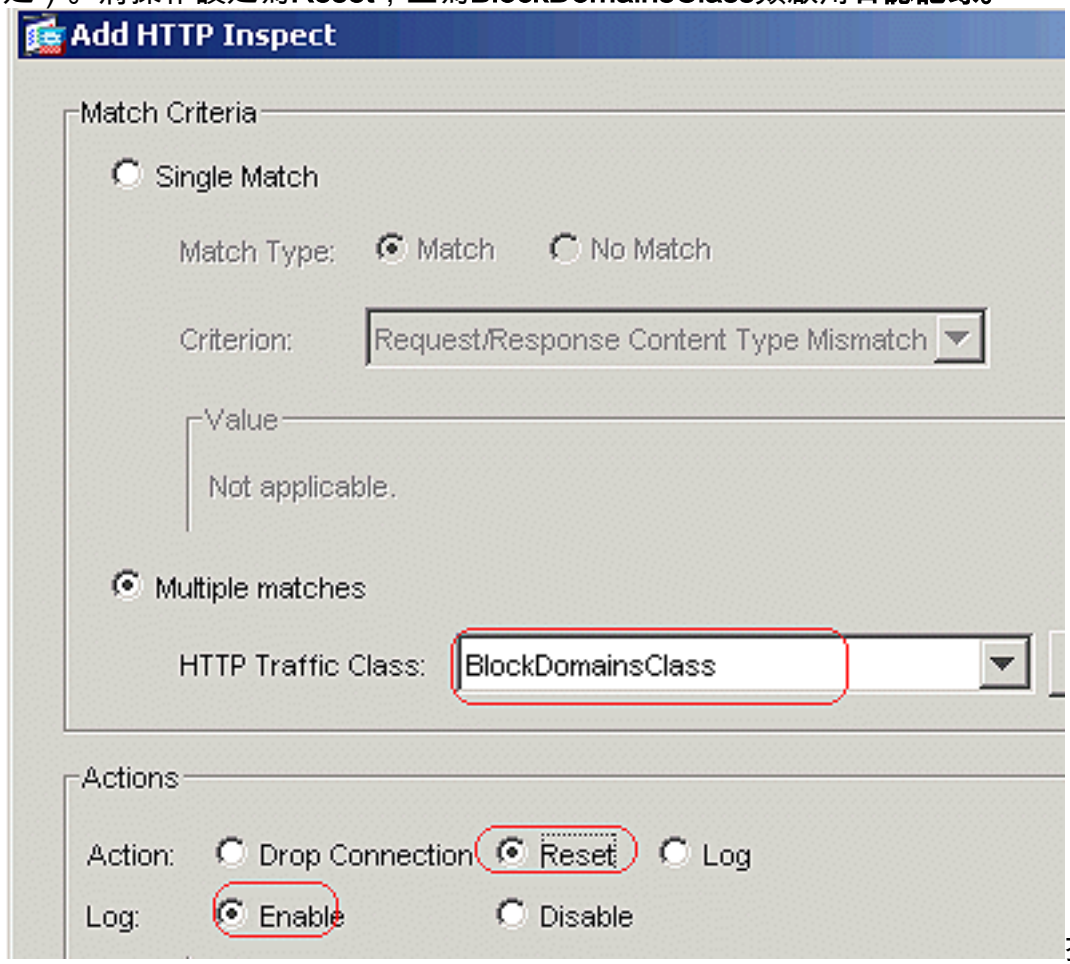
按一下「**OK**」（確定）。將操作設定為**Drop Connection**;**為**Criterion as Request Method和Value as **connect啟用日誌記錄**。



按一下「OK」（確定）。將操作設定為Drop Connection，並為AppHeaderClass類啟用日誌記錄。

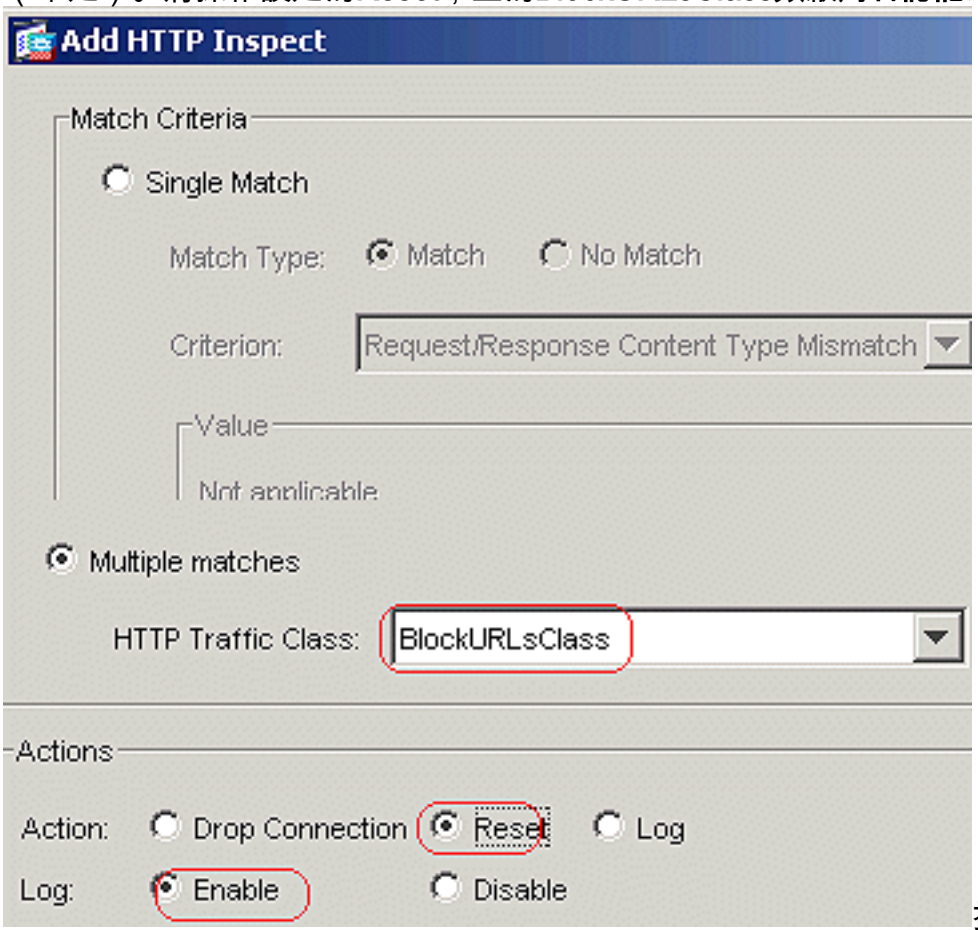


按一下「**OK**」（確定）。將操作設定為**Reset**，並為**BlockDomainsClass**類啟用**日誌記錄**。



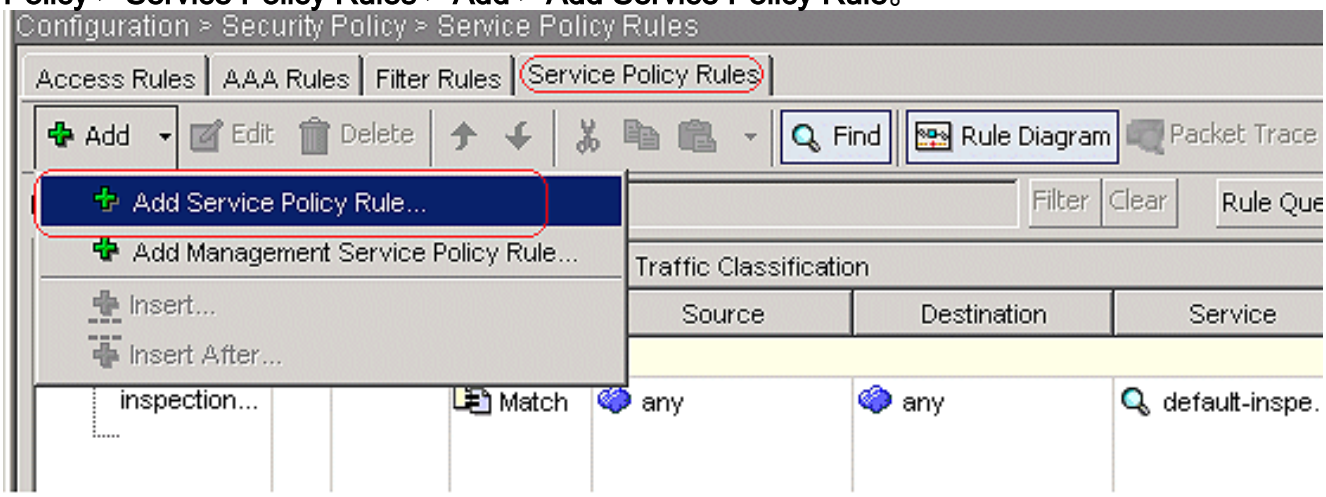
按一下「**OK**」

（確定）。將操作設定為**Reset**，並為**BlockURLsClass**類啟用**日誌記錄。**

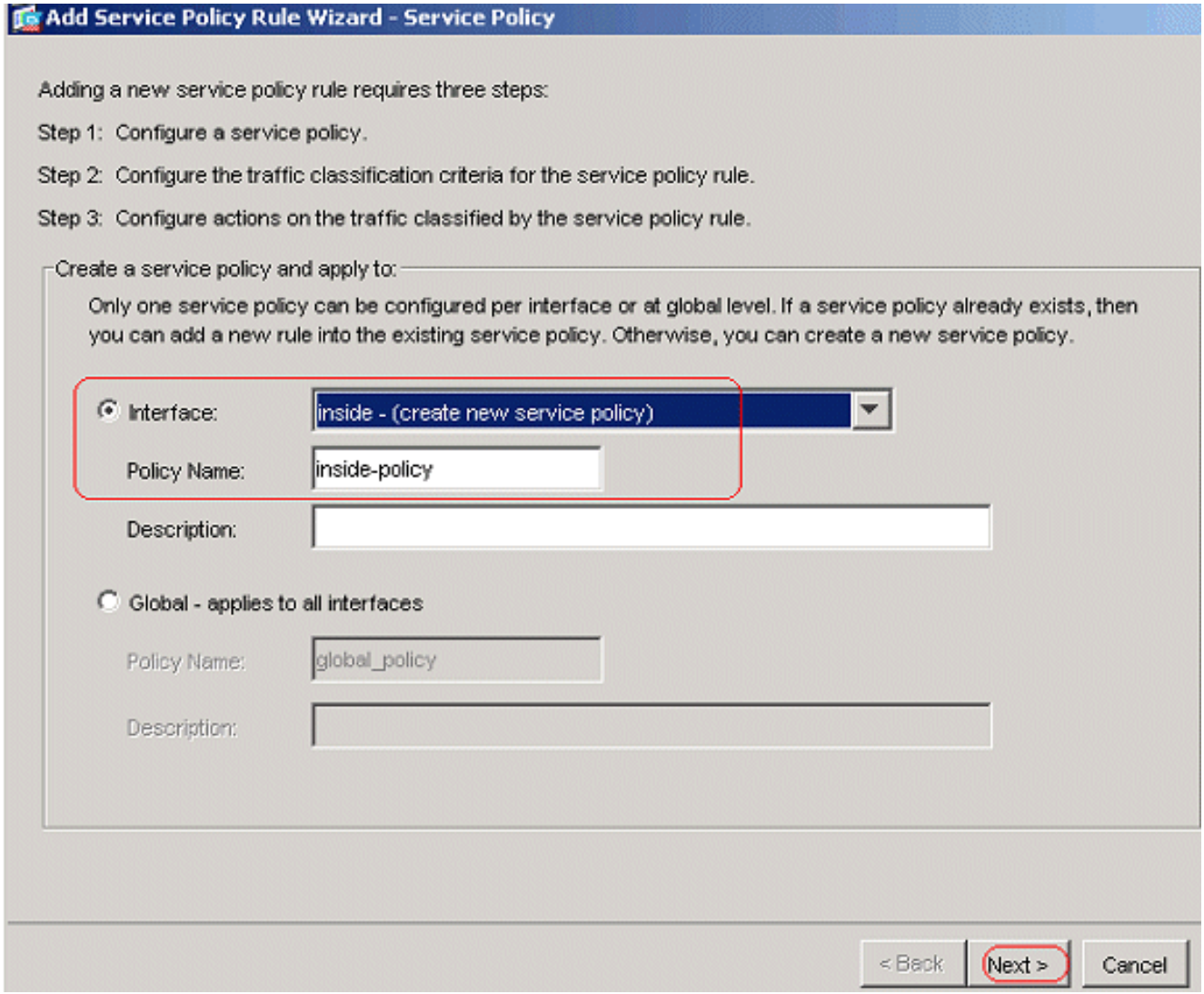


按一下「**OK**」（確定）。按一下「**Apply**」。**等效的CLI配置**

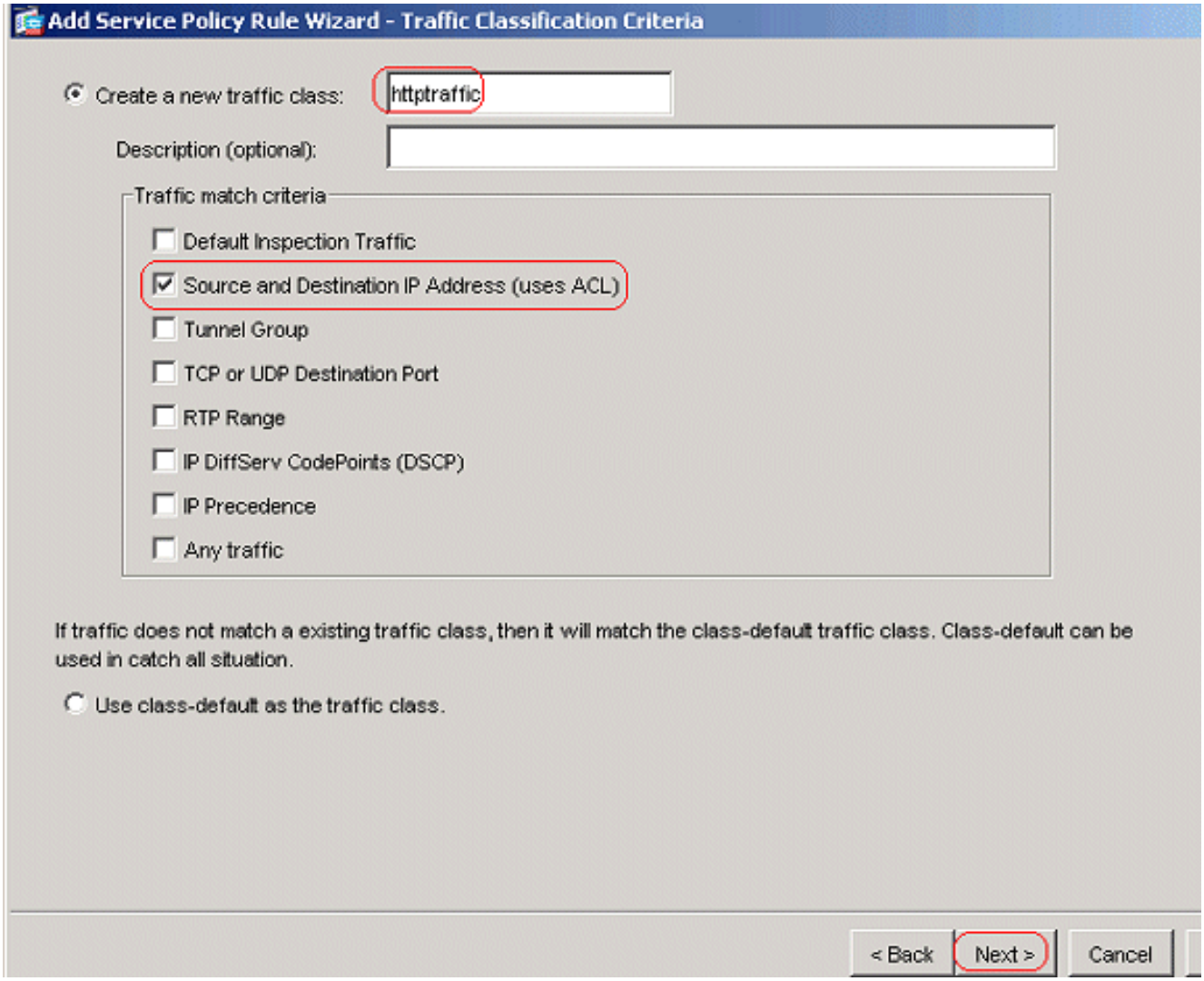
5. **將檢測http策略應用到介面**在Service Policy Rules頁籤下，選擇**Configuration > Security Policy > Service Policy Rules > Add > Add Service Policy Rule**。



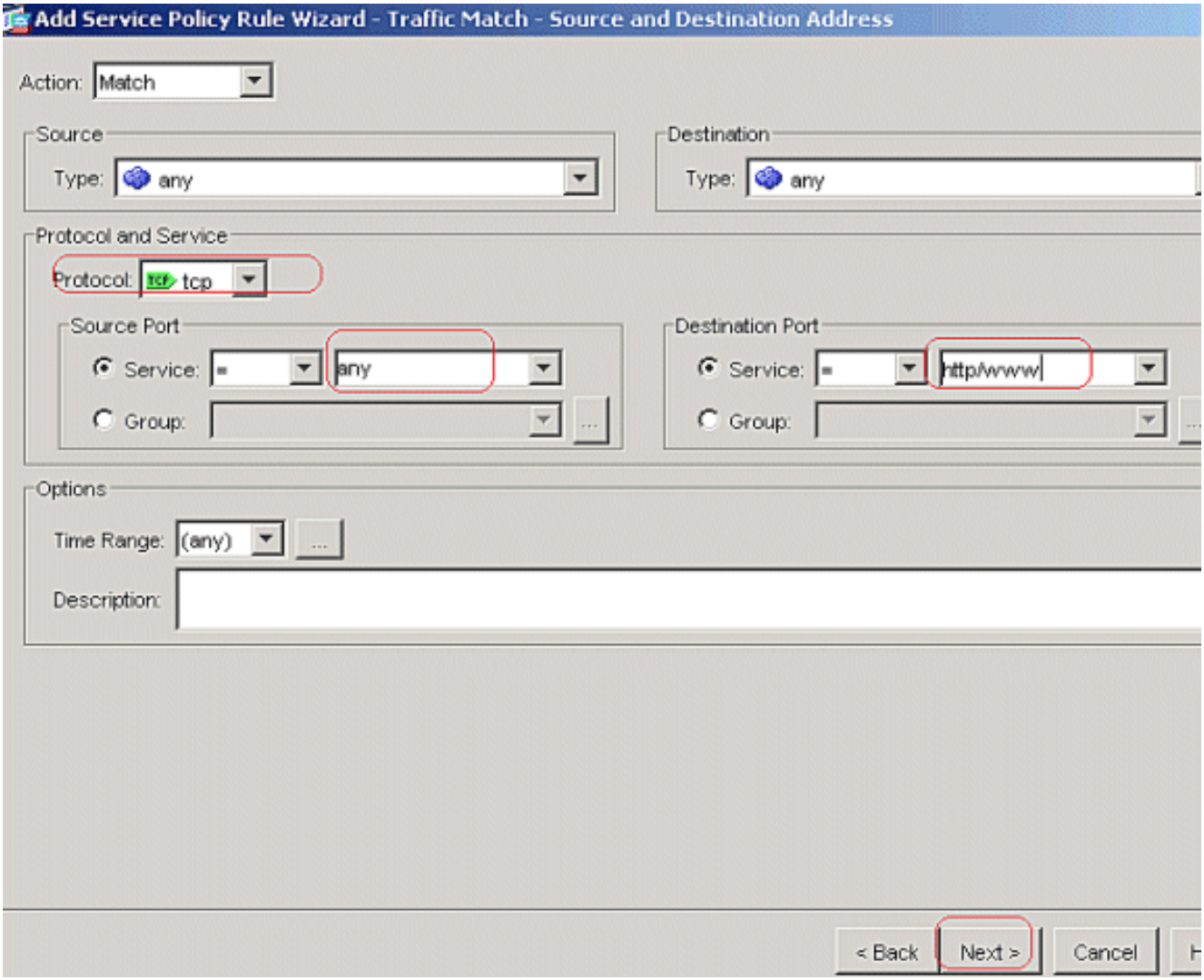
HTTP流量從下拉選單中選擇**Interface**單選按鈕，其中包含**inside**介面，並選擇Policy Name作為**inside-policy**。按「**Next**」（下一步）。



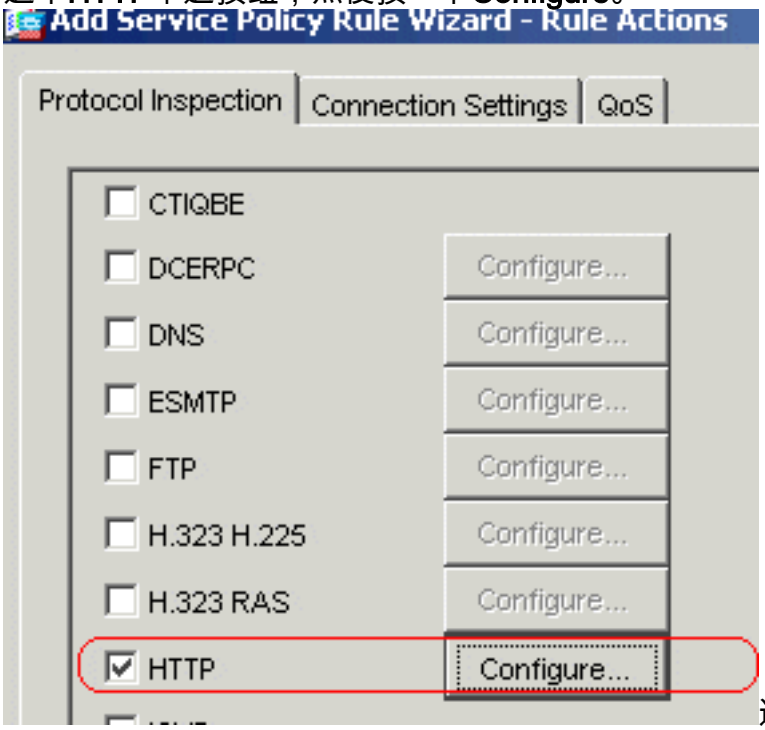
建立類對映**httptraffic**，然後檢查**源IP地址和目標IP地址（使用ACL）**。 按「**Next**」（下一步）。



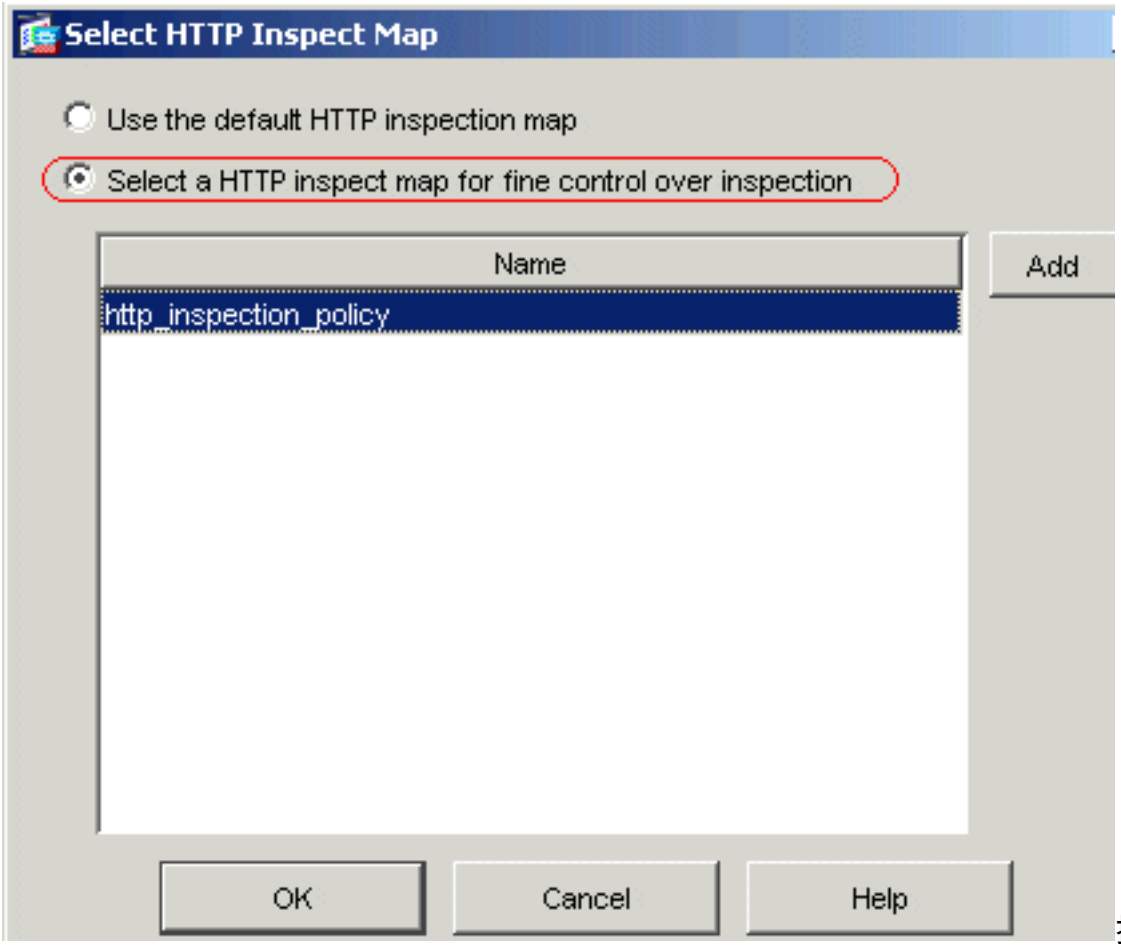
選擇Source和Destination作為**any**,TCP埠作為**HTTP**。按「**Next**」（下一步）。



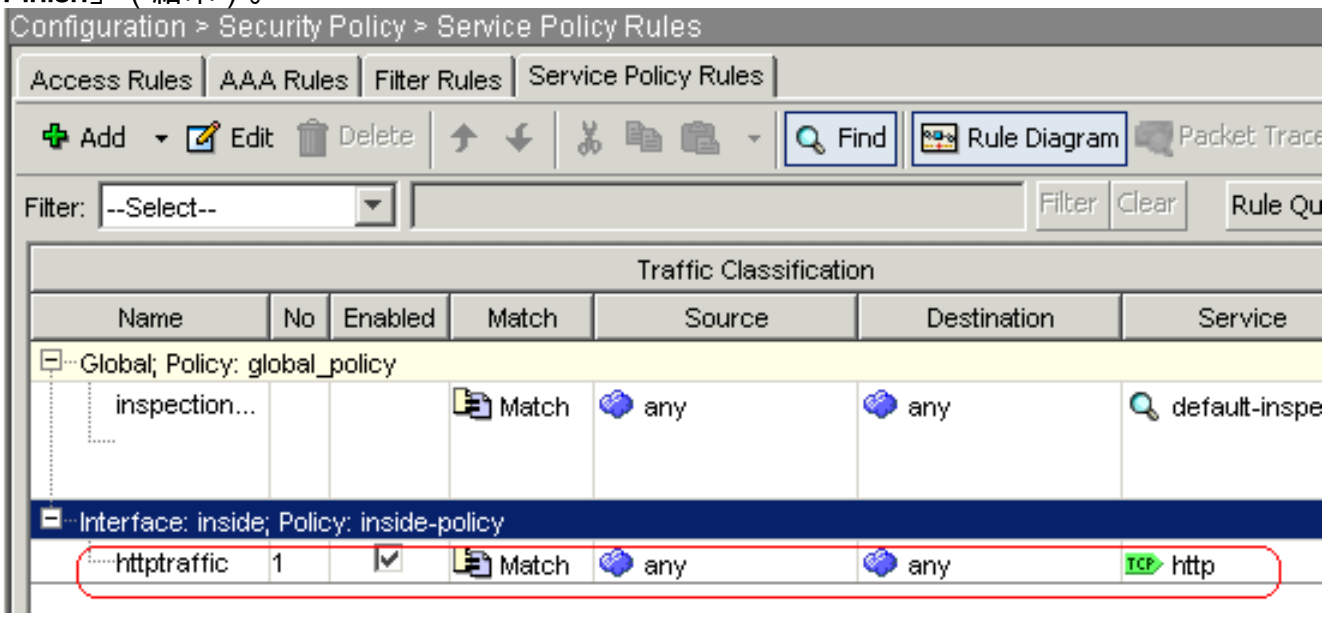
選中HTTP單選按鈕，然後按一下Configure。



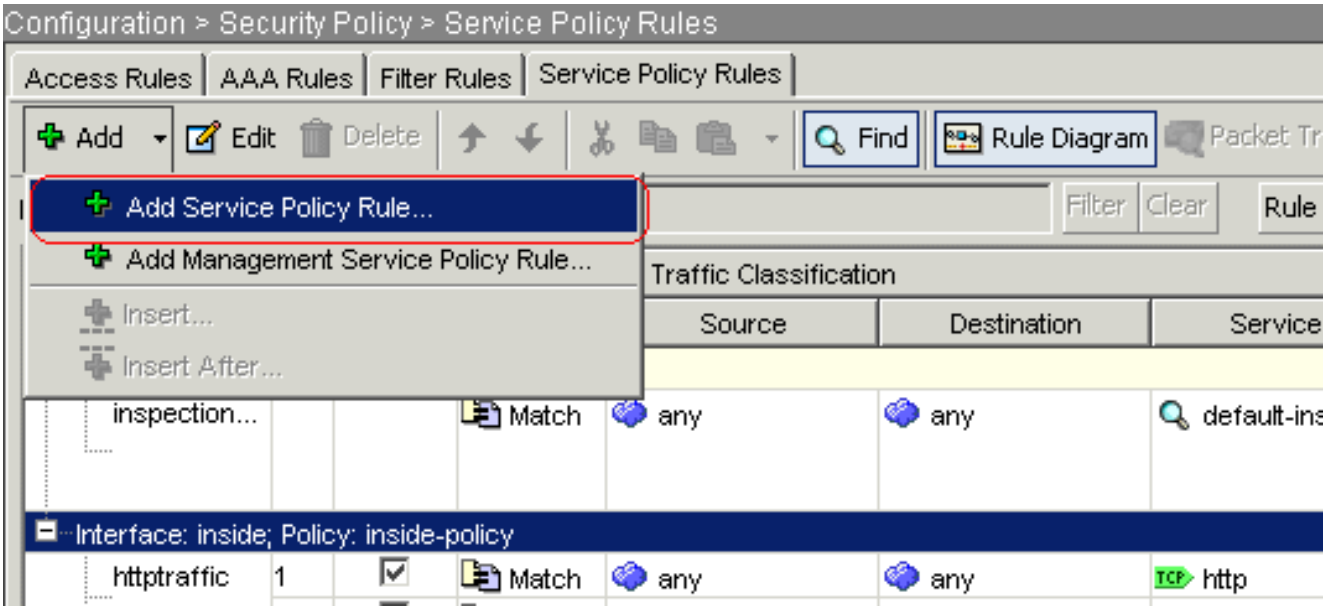
選中Select a HTTP inspect map for the control of inspection單選按鈕。按一下「OK」（確定）。



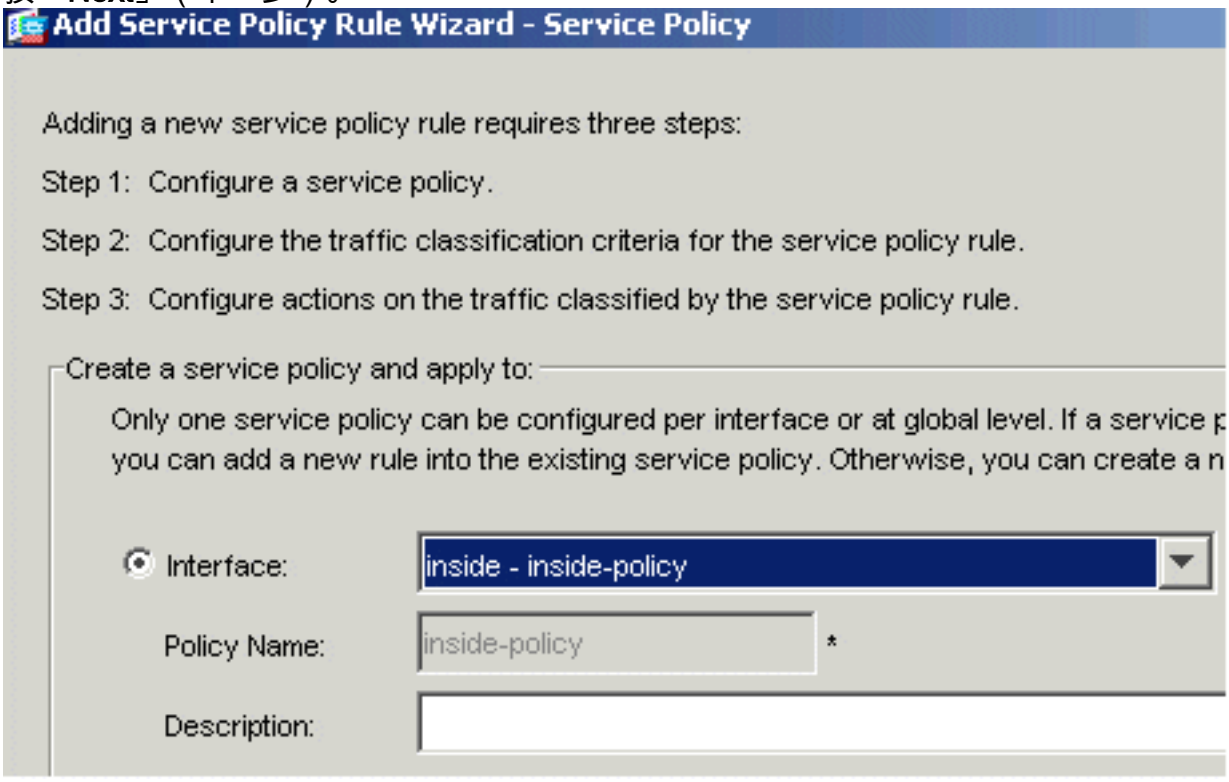
按一下「Finish」（結束）。



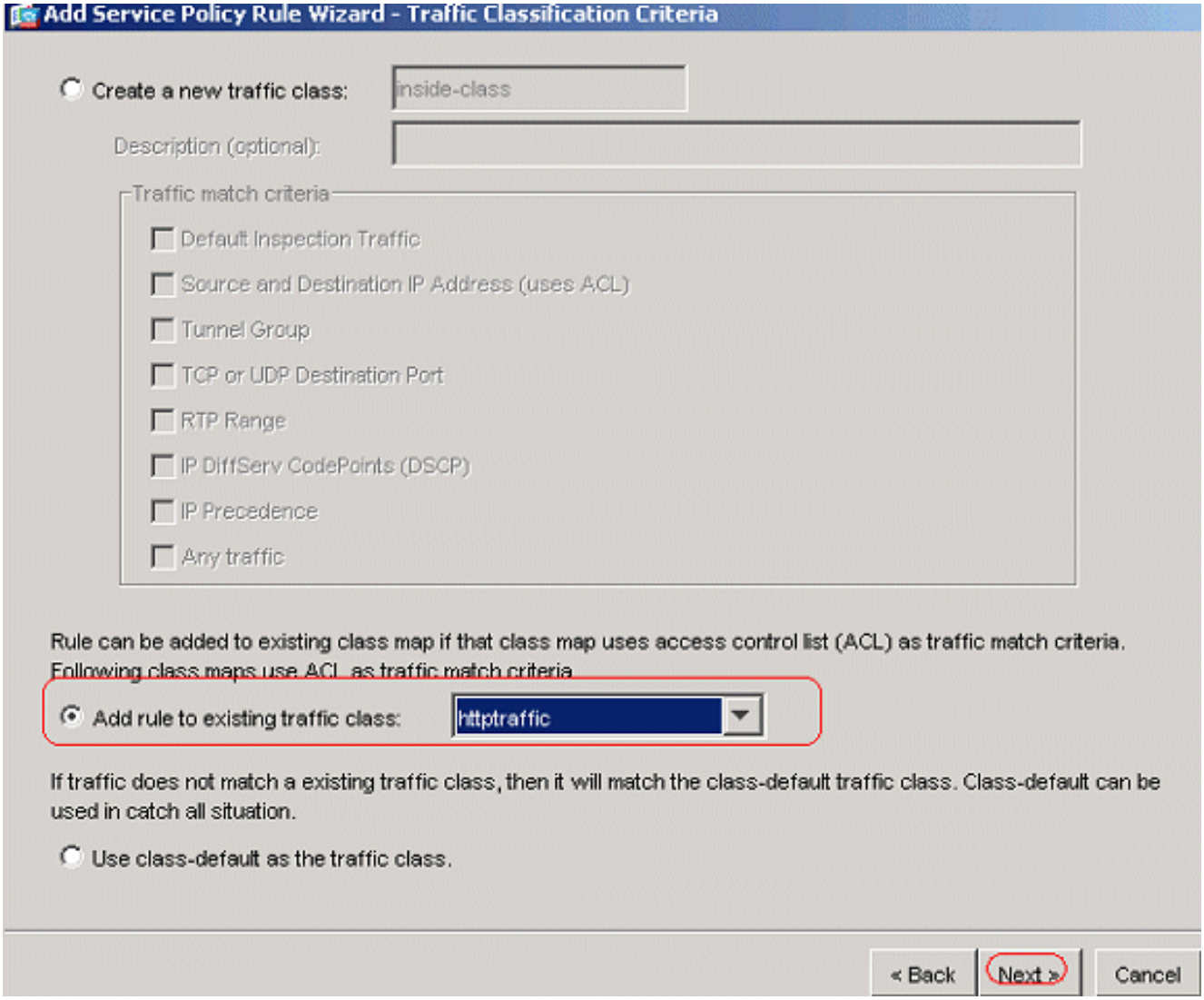
埠8080流量再次按一下Add > Add Service Policy Rule。



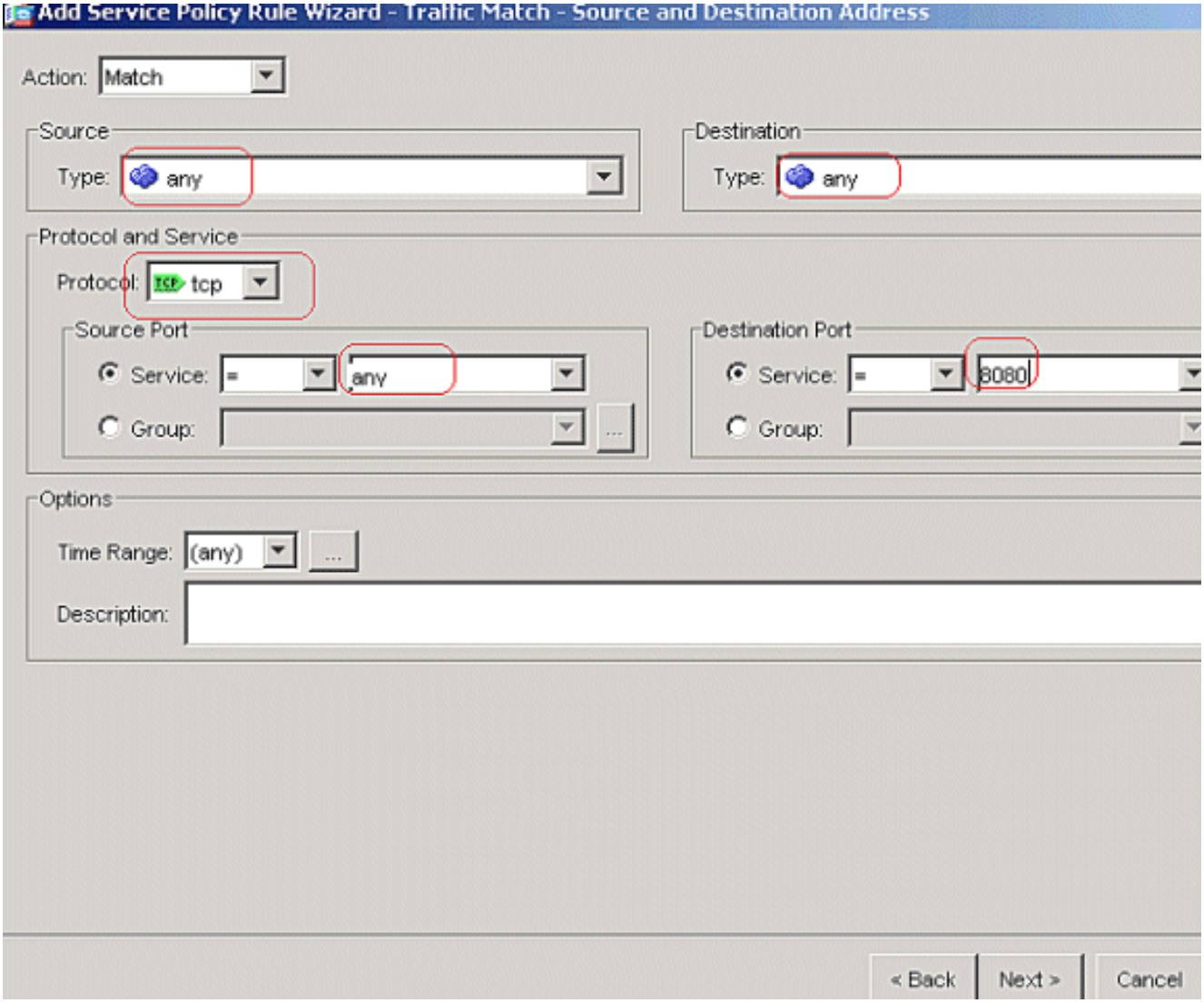
按「**Next**」（下一步）。



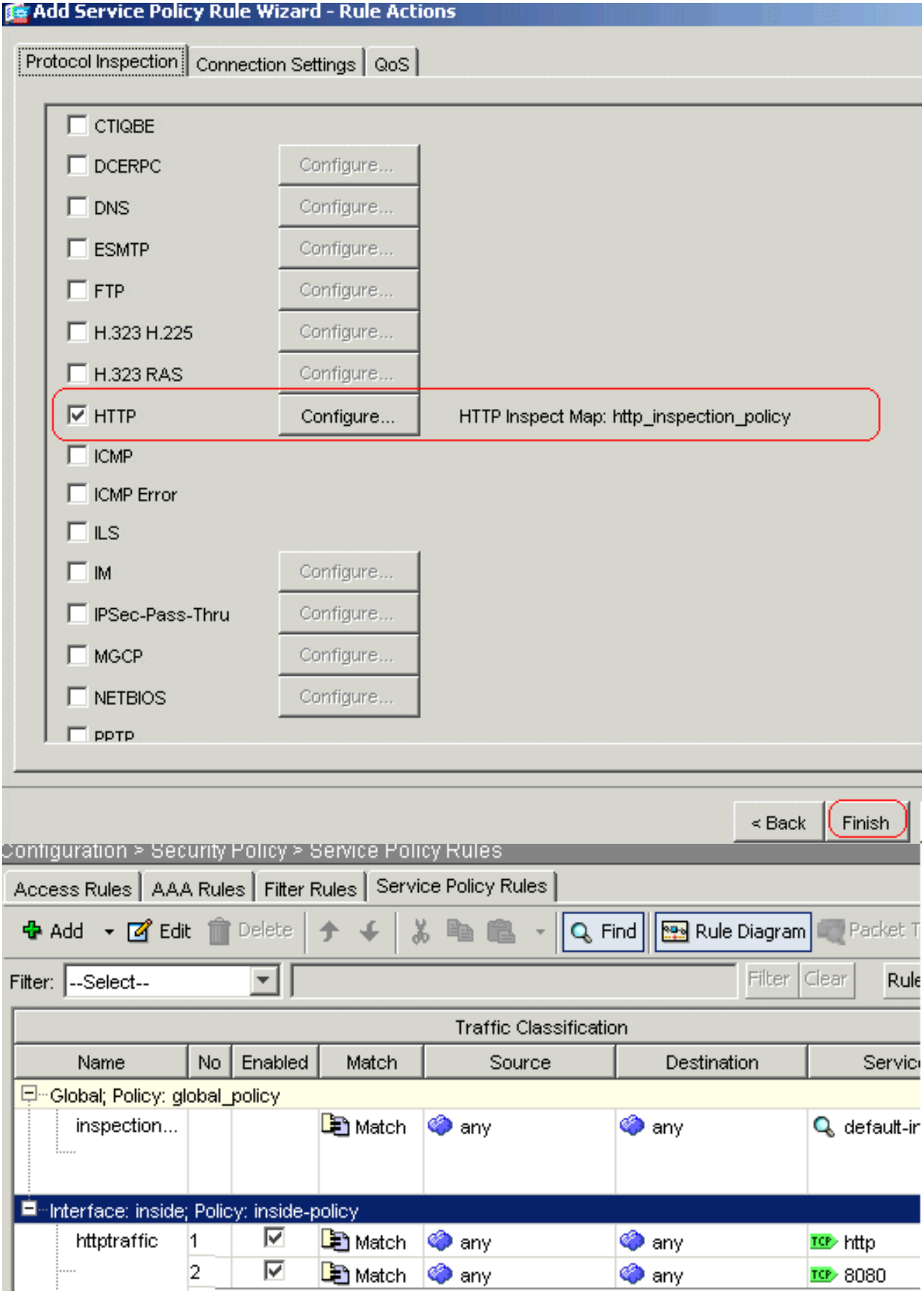
選擇**Add rule to existing traffic class**單選按鈕，然後從下拉選單中選擇**httptraffic**。按「**Next**」（下一步）。



選擇Source and Destination as **any**,TCP埠為**8080**。按「**Next**」（下一步）。



按一下「**Finish**」（結束）。



按一下「Apply」。等效的CLI配置

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- **show running-config regex** — 顯示已配置的正規表示式

```
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#
```

- **show running-config class-map** — 顯示已配置的類對映

```
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#
```

- **show running-config policy-map type inspect http** — 顯示檢查已配置的http流量的策略對映

```
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#
```

- **show running-config policy-map** — 顯示所有策略對映配置以及預設策略對映配置

```
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#
```

- **show running-config service-policy** — 顯示當前運行的所有服務策略配置

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

- **show running-config access-list** — 顯示安全裝置上運行的訪問清單配置

```
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#
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug http** — 顯示HTTP流量的調試消息。

相關資訊

- 思科自適應安全裝置支援頁面
- 思科調適型安全裝置管理員(ASDM)支援頁面

- Cisco 500系列PIX支援頁面
- 技術支援與文件 - Cisco Systems