ASA/PIX 7.2：通过 MPF 使用正则表达式阻止某些网站 (URL) 的配置示例

目录

简介

本文档描述了如何配置 Cisco 安全设备 ASA/PIX 7.2，以便通过模块化策略框架 (MPF) 使用正则表达式来阻止某些网站 (URL)。

注意： 此配置不会阻止任何应用程序下载。要实现可靠的文件阻止，必须使用专用设备（例如 Websense 等）或模块（例如用于 ASA 的 CSC 模块）。

ASA 不支持 HTTPS 过滤。ASA 不能对 HTTPS 流量执行深度数据包检查或基于正则表达式的检查，因为在 HTTPS 中，数据包的内容是加密的 (ssl)。

先决条件

要求

本文档假设已配置 Cisco 安全设备且它能正常工作。

使用的组件

- 运行软件版本 7.2(2) 的 Cisco 5500 系列自适应安全设备 (ASA)
- ASA的Cisco Adaptive Security Device Manager (ASDM)版本5.2(2) 7.2(2)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于运行 7.2(2) 版软件的 Cisco 500 系列 PIX。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

模块化策略框架概述

MPF 提供一种一致且灵活的配置安全设备功能的方式。例如，您可以使用 MPF 创建仅适用于特定 TCP 应用程序的超时配置，而非适用于所有 TCP 应用程序的配置。

MPF 支持以下功能：

- TCP 标准化、TCP 和 UDP 连接限制和超时以及 TCP 序列号随机化
- CSC
- 应用程序检查
- IPS
- QoS输入策略
- QoS 输出管制
- QoS 优先级队列

MPF 的配置包括四项任务：

1. 识别您要应用操作的第 3 层和第 4 层流量。有关详细信息，请参阅使用第 3 层/第 4 层类映射识别流量。
2. （仅限应用程序检查）定义针对应用程序检查流量的特殊操作。有关详细信息，请参阅配置特殊的应用程序检查操作。
3. 将操作应用于第 3 层和第 4 层流量。有关详细信息，请参阅使用第 3 层/第 4 层策略映射定义操作。
4. 在接口上激活操作。有关详细信息，请参阅使用服务策略将第 3 层/第 4 层策略应用到接口。

正则表达式

正则表达式可逐字地完全匹配文本串，或使用元字符以匹配文本串的多个变体。您可以使用正则表达式来匹配某个应用程序流量的内容；例如，您可以匹配 HTTP 数据包中的 URL 字符串。

注意： 请使用 **Ctrl+V** 在 CLI 中对所有特殊字符进行转义，例如问号 (?) 或制表符。例如，键入 **d[Ctrl+V]g** 可在配置中输入 d?g。

要创建正则表达式，请使用 **regex** 命令，此命令可用于各种需要文本匹配的功能。例如，您可以通

过模块化策略框架使用检查策略映射来配置特殊的应用程序检查操作（请参阅 policy map type inspect 命令）。在检查策略映射中，如果您创建包含一个或多个 **match** 命令的检查类映射，则可以识别出要采取操作的流量，也可以直接在检查策略映射中使用 **match** 命令。有些 **match** 命令可以用正则表达式来识别数据包中的文本；例如，您可以匹配 HTTP 数据包中的 URL 字符串。您可以将正则表达式分组到正则表达式类映射中（请参阅 class-map type regex 命令）。

表 1 列出了有特殊含义的元字符。

字符	说明	备注
. 。	点	与任意单个字符相匹配。例如，**d.g** 匹配 dog、dag、dtg 和任何包含这些字符的单词，如 doggonnit。
(exp)	子表达式	子表达式将字符与其周围的字符分隔开，以便在子表达式上使用其它元字符。例如，**d(o|a)g** 匹配 dog 和 dag，而**|ag** 匹配 do 和 ag。子表达式也用重复量词来区分用于重复的字符。例如，**ab(xy){3}z** 匹配 abxyxyxyz。
|	变换	匹配其所分隔的任意一个表达式。例如，**dog|cat** 匹配 dog 或 cat。
?？	问号	一个量词，其表示有 0 个或 1 个先前的表达式。例如，**lo?se** 匹配 lse 或 lose。**注意：** 必须输入 **Ctrl+V** 才能调用问号或其它帮助功能。
**	星号	一个量词，其表示有 0 个、1 个或任意数量的先前的表达式。例如，**lo*se** 匹配 lse、lose、loose 等。
{x}	重复量词	准确重复 x 次。例如，**ab(xy){3}z** 匹配 abxyxyxyz。
{x,}	重复次数最少的量词	重复至少 x 次。例如，**ab(xy){2,}z** 匹配 abxyxyz、abxyxyxyz 等。
[abc]	字符类别	匹配中括号中的任意字符。例如，**[abc]** 匹配 a、b 或 c。
[^abc]	略过的字符类别	匹配不包含在该中括号内的单个字符。例如，**[^abc]** 匹配 a、b 或 c 以外的任何字符。**[^A-Z]** 匹配大写字母以外的任何字符。
[a-c]	字符范围类别	匹配范围中的任意字符。**[[a-z]** 匹配任意小写字母。可混用字符和范围：**[[abcq-z]** 匹配 a、b、c、q、r、s、t、u、v、w、x、y、z，**[a-cq-z]** 也是如此。仅当破折号 (-) 字符是中括号中的最后一个或第一个字符时，它才具有字面意义：**[[abc-]** 或 **[-abc]**。
""	引号	保留字符串中的后置空格或前置空格。例如，**" test"** 保留了在其搜索匹配时的前置空格。
^	脱字号	指定行首。

\\	转义字符	当与元字符一起使用时，可匹配文字字符。例如，\[匹配左方括号。
字符	字符	如果字符并不是元字符，则匹配文字字符。
\r	回车	匹配回车 0x0d。
\n	新行	匹配新的一行0x0a。
\t	选项卡	匹配制表符 0x09。
\f	换页符	匹配换页符 0x0c。
\xNN	转义的十六进制数	以十六进制数字匹配 ASCII 字符（必须是两位）。
\NNN	转义的八进制数	以八进制数字匹配 ASCII 字符（必须三位）。例如，字符 040 代表一个空格。

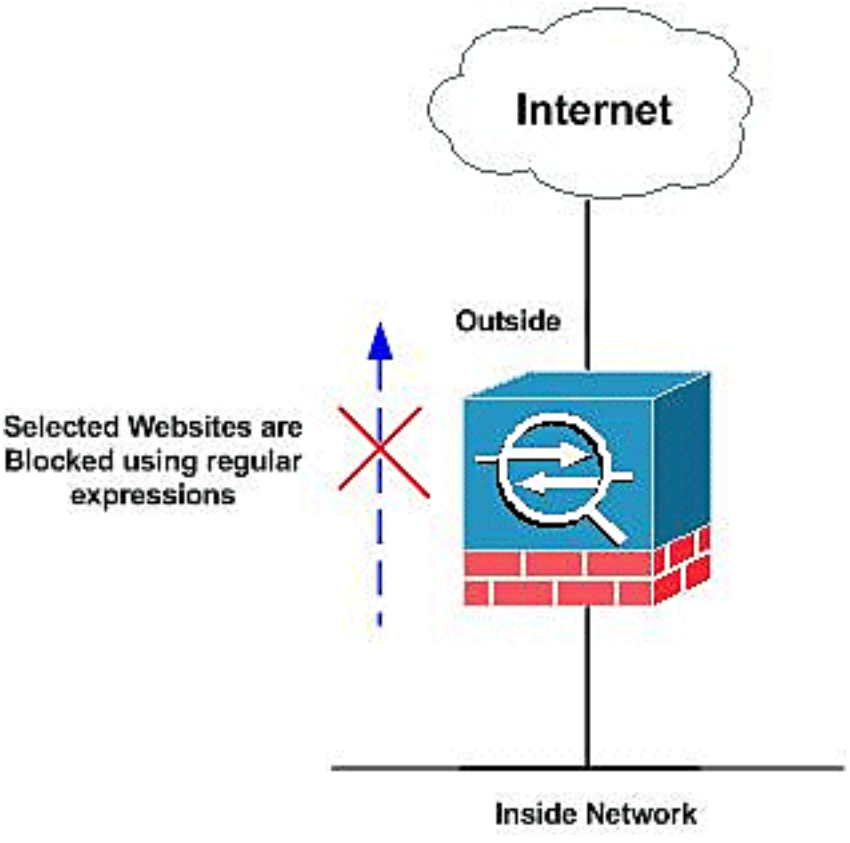
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- ASA CLI 配置
- ASA 配置 7.2(x) 与 ASDM 5.2

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
```

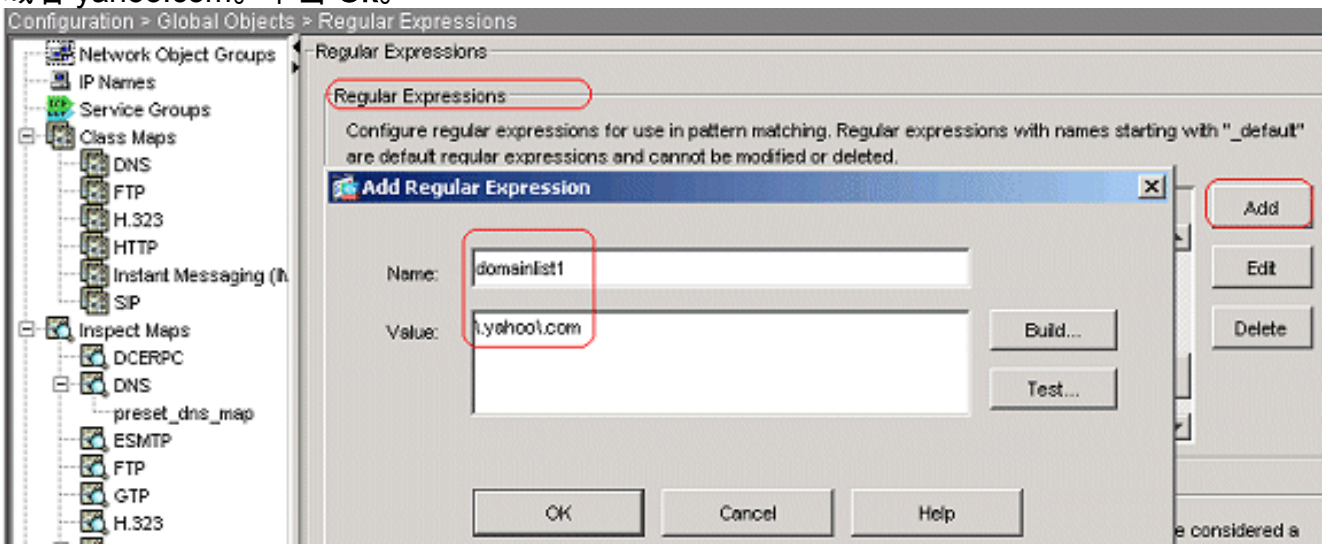
```
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute dynamic-access-policy-
record DfltAccessPolicy http server enable http 0.0.0.0
0.0.0.0 DMZ no snmp-server location no snmp-server
contact snmp-server enable traps 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#
```

ASA 配置 7.2(x) 与 ASDM 5.2

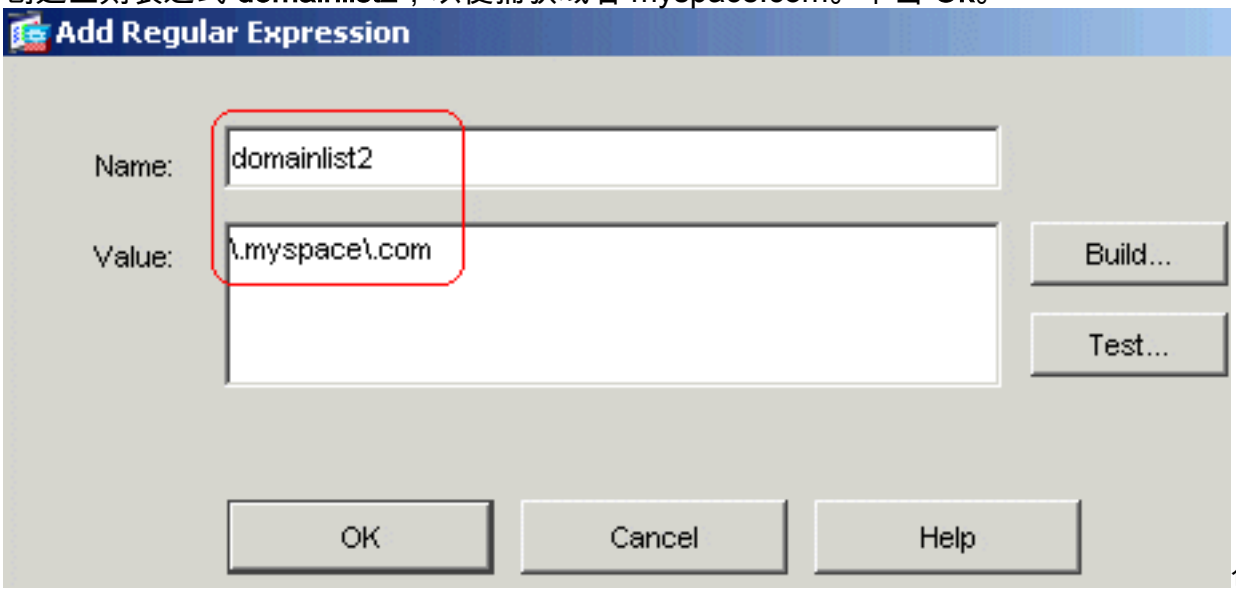
要配置正则表达式并将其应用于 MPF 以便阻止特定网站，请完成以下步骤：

1. **创建正则表达式**选择 **Configuration > Global Objects > Regular Expressions** 并单击“Regular Expression”选项卡下的“Add”，以便创建正则表达式。创建正则表达式 **domainlist1**，以便捕获

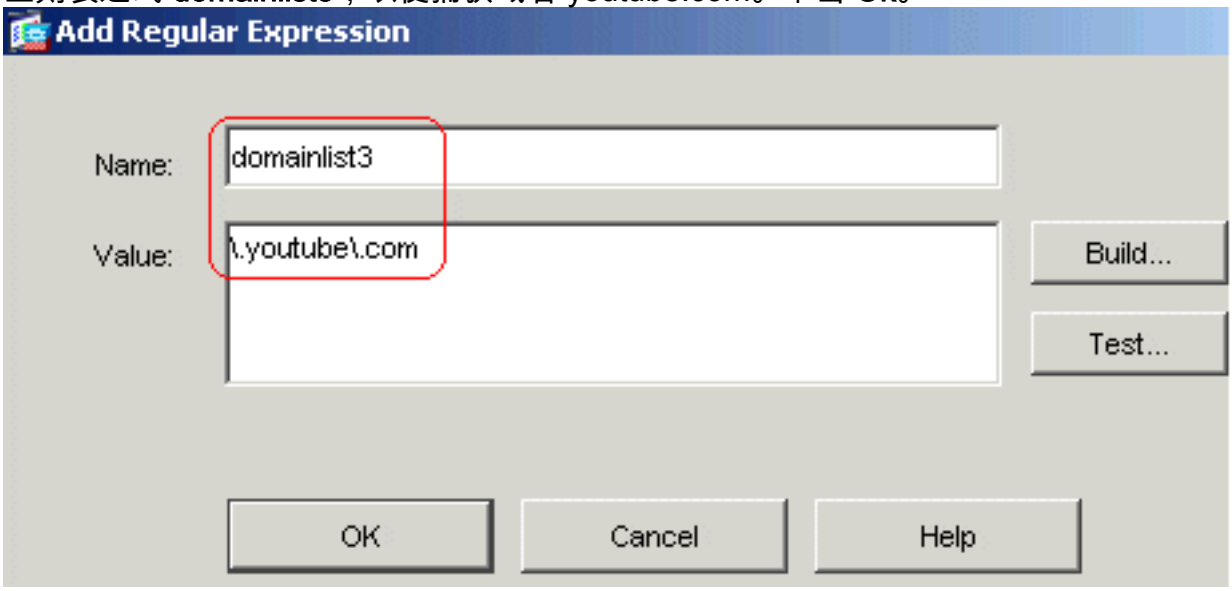
域名 yahoo.com。单击 **Ok**。



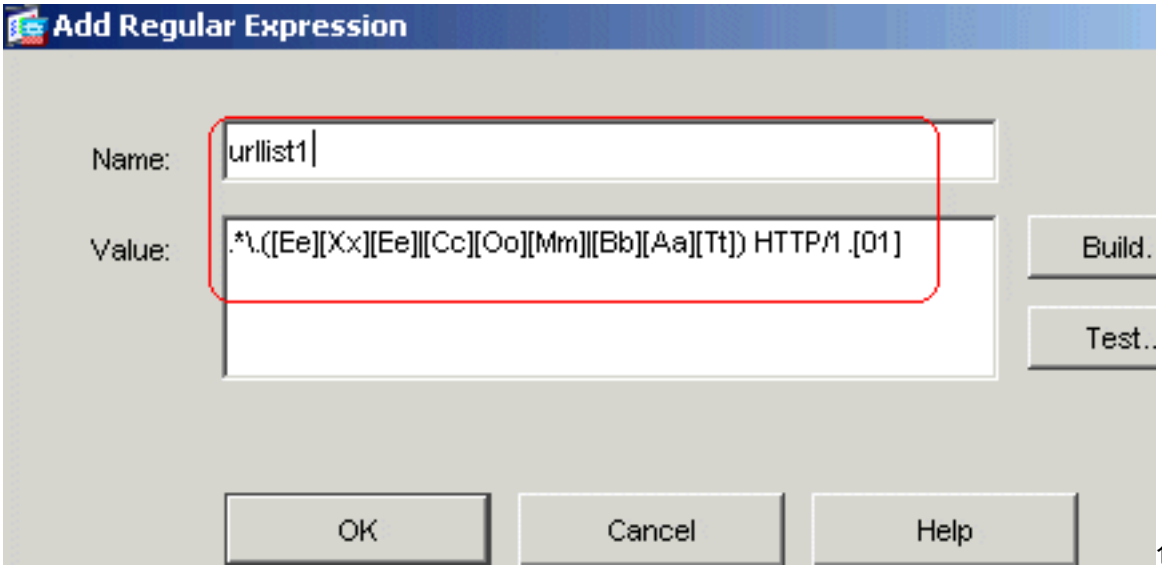
创建正则表达式 **domainlist2**，以便捕获域名 myspace.com。单击 **Ok**。



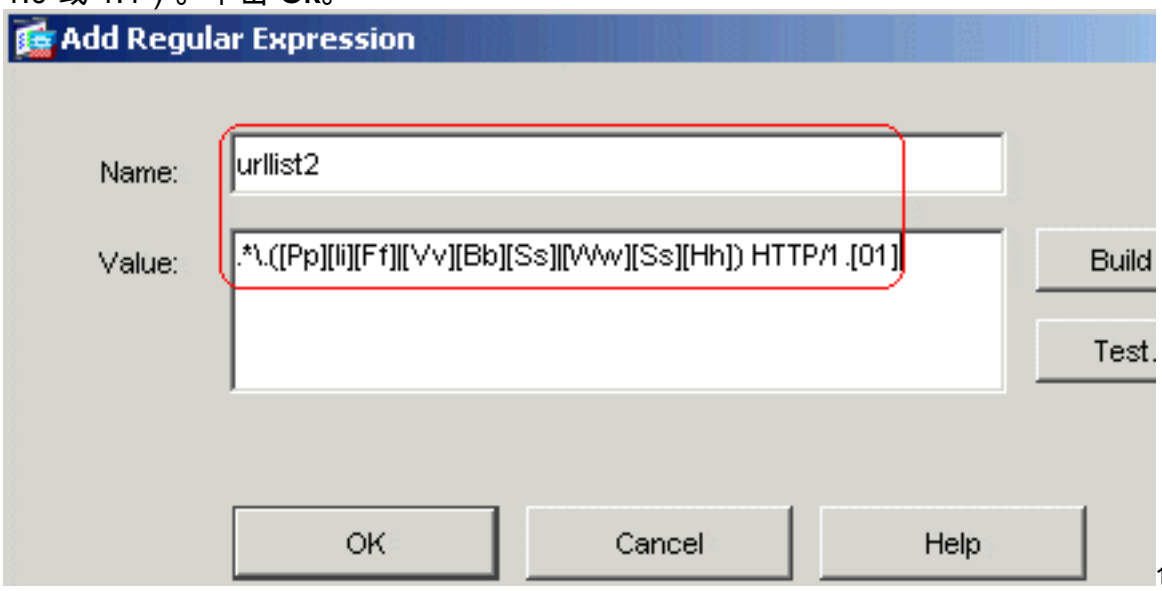
创建正则表达式 **domainlist3**，以便捕获域名 youtube.com。单击 **Ok**。



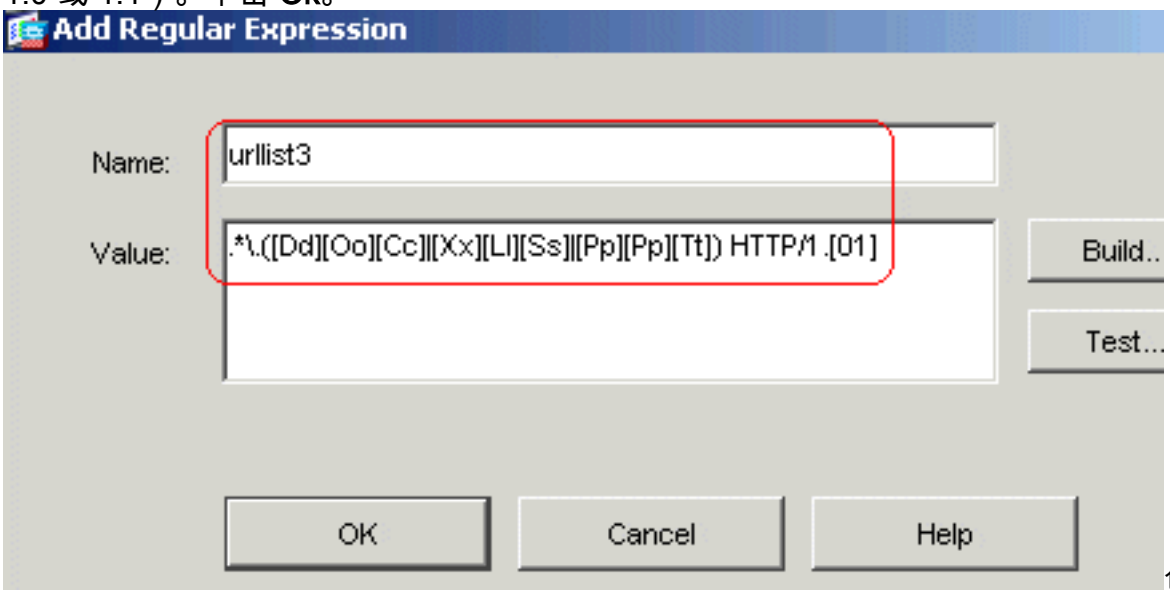
创建正则表达式 **urllist1**，以便捕获 exe、com、bat 等文件扩展名（假设 Web 浏览器使用的 http 版本是 1.0 或 1.1）。单击 **Ok**。



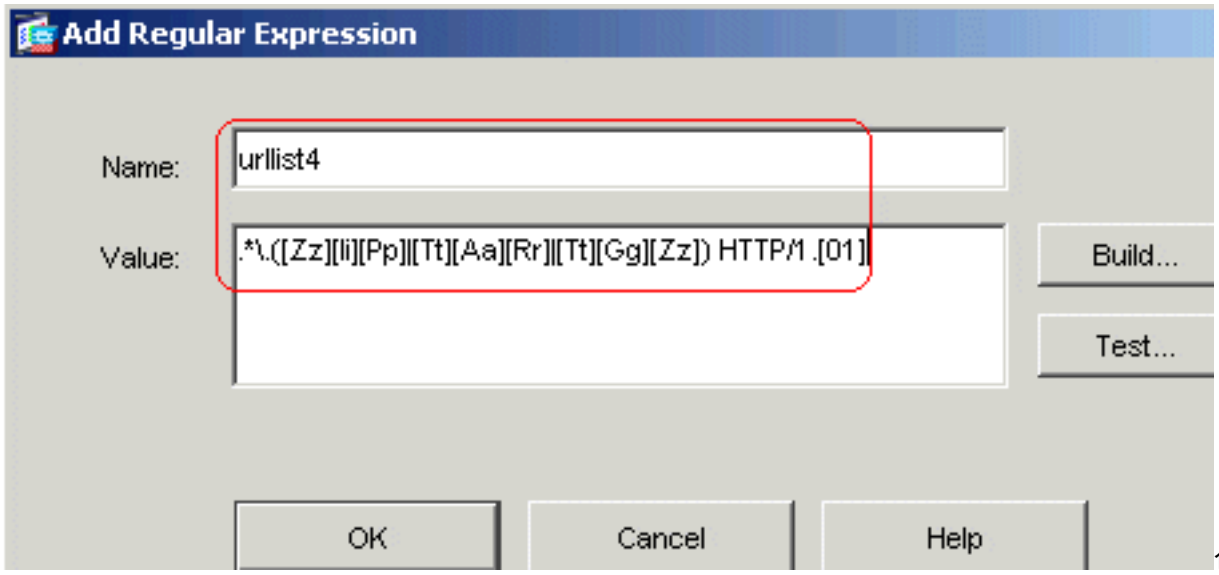
创建正则表达式 **urllist2**，以便捕获 pif、vbs、wsh 等文件扩展名（假设 Web 浏览器使用的 HTTP 版本是 1.0 或 1.1）。单击 **Ok**。



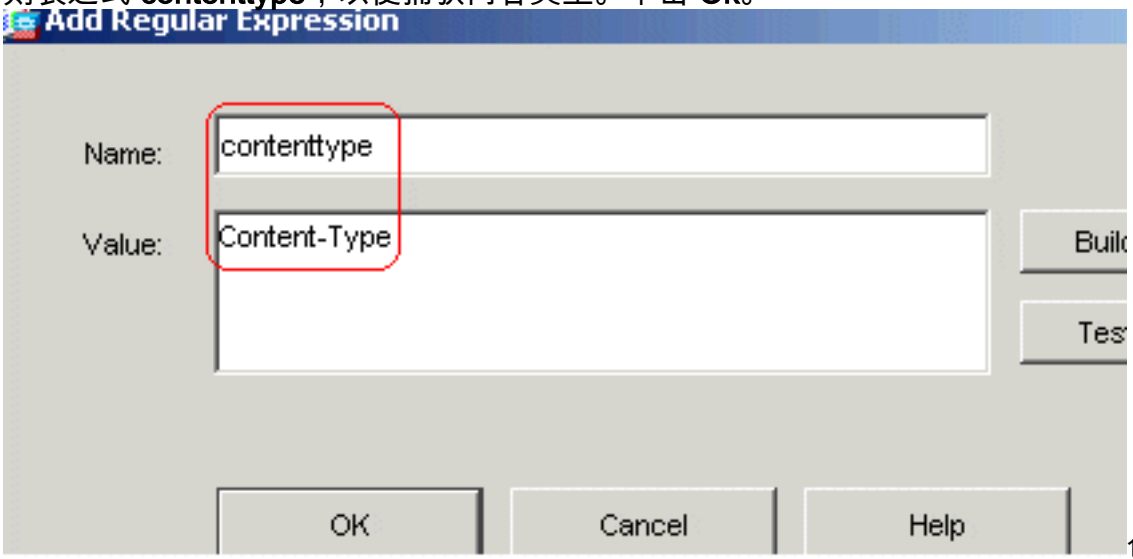
创建正则表达式 **urllist3**，以便捕获 doc、xls、ppt 等文件扩展名（假设 Web 浏览器使用的 HTTP 版本是 1.0 或 1.1）。单击 **Ok**。



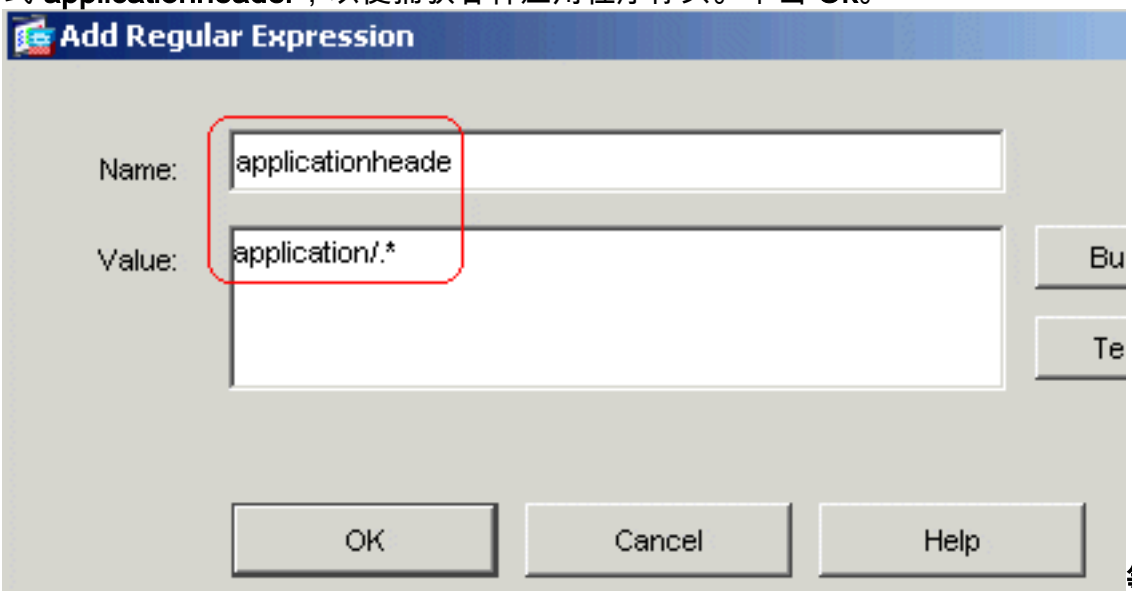
创建正则表达式 **urllist4**，以便捕获 zip、tar、tgz 等文件扩展名（假设 Web 浏览器使用的 HTTP 版本是 1.0 或 1.1）。单击 **Ok**。



创建正则表达式 **contenttype**，以便捕获内容类型。单击 **Ok**。

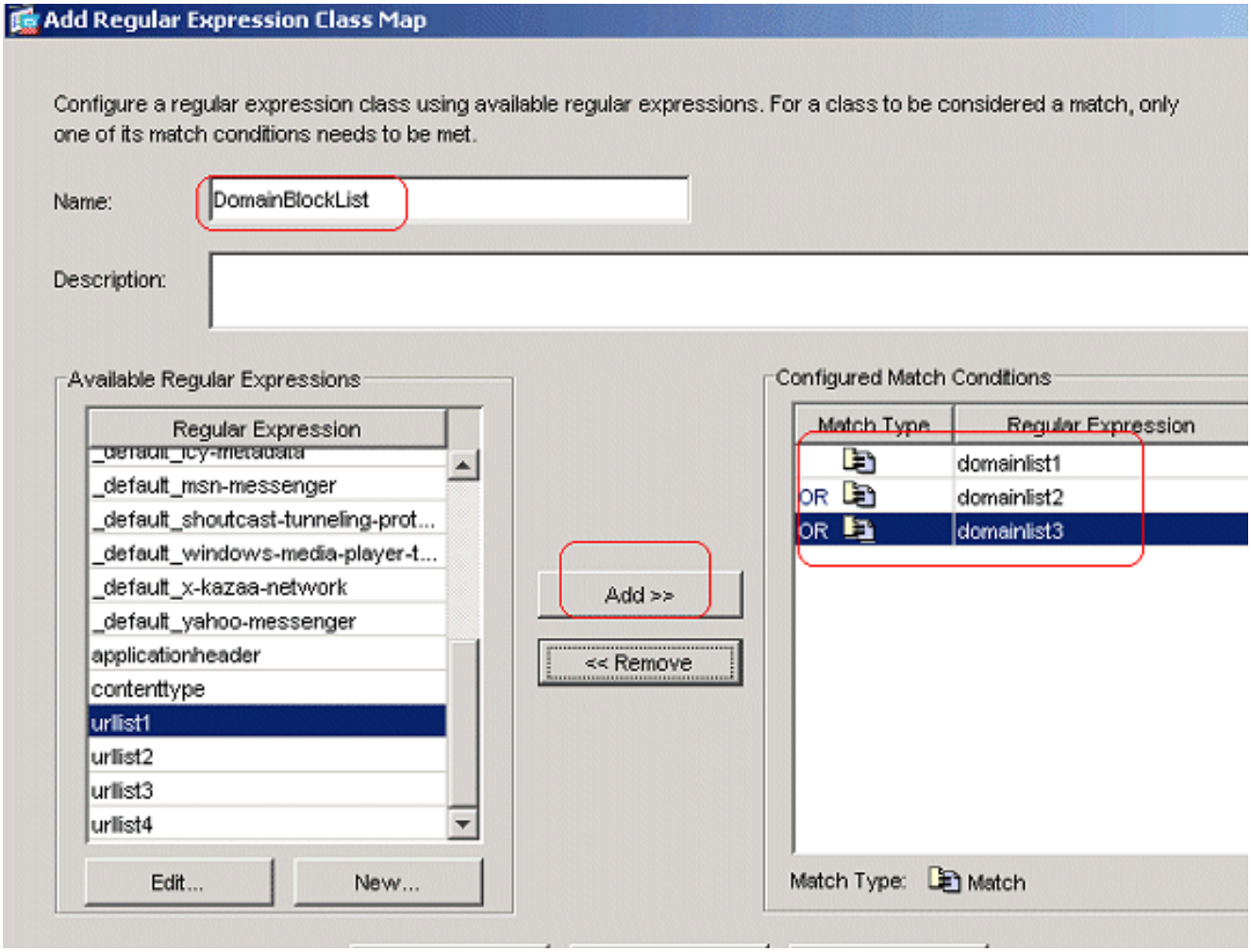


创建正则表达式 **applicationheader**，以便捕获各种应用程序标头。单击 **Ok**。

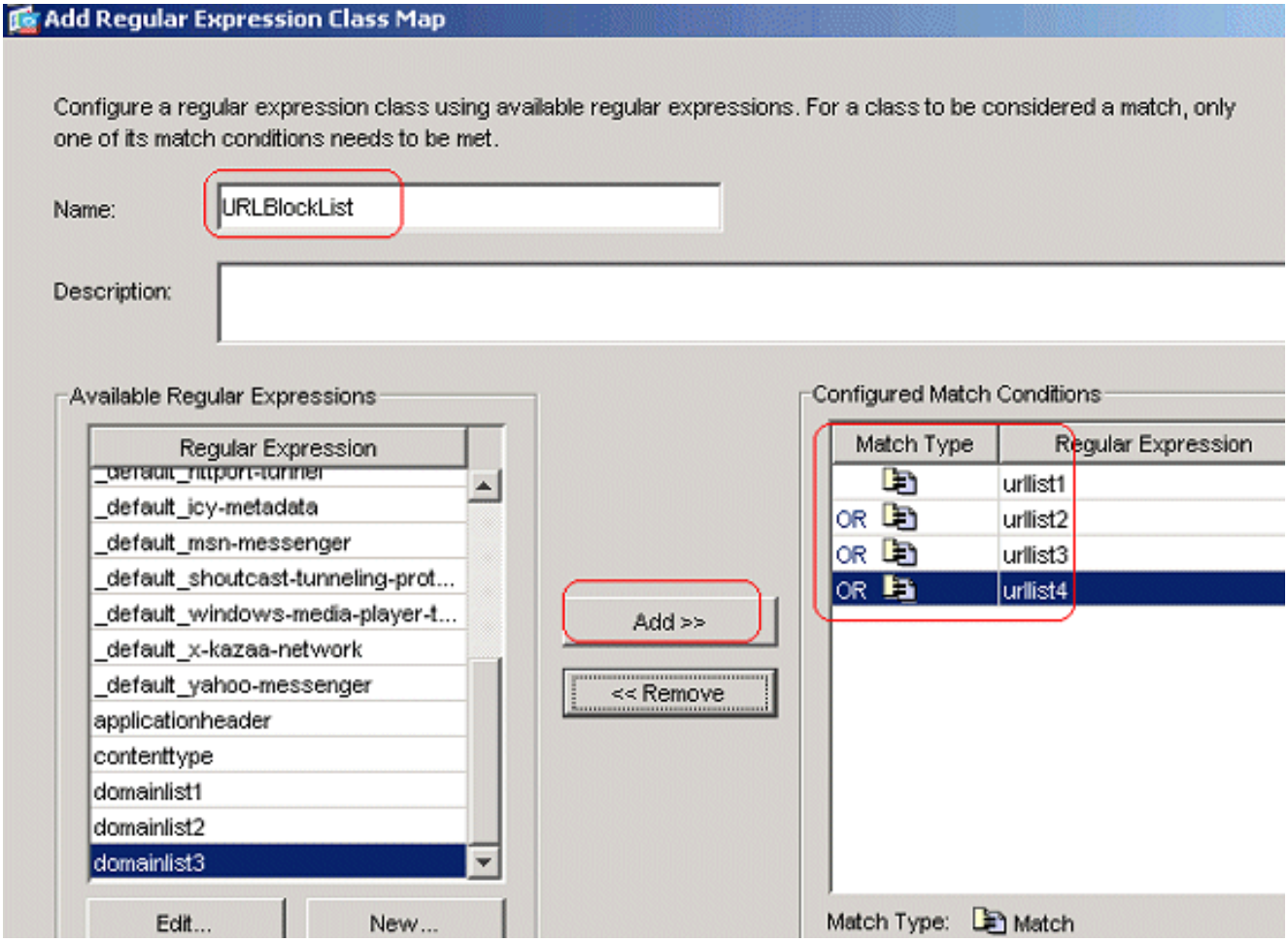


等效 CLI 配置

2. **创建正则表达式类**选择 **Configuration > Global Objects > Regular Expressions** 并单击“Regular Expression Classes”选项卡下的“Add”，以便创建各种类。创建正则表达式类 **DomainBlockList**，以便匹配以下任意正则表达式：domainlist1、domainlist2 和 domainlist3。单击 **Ok**。

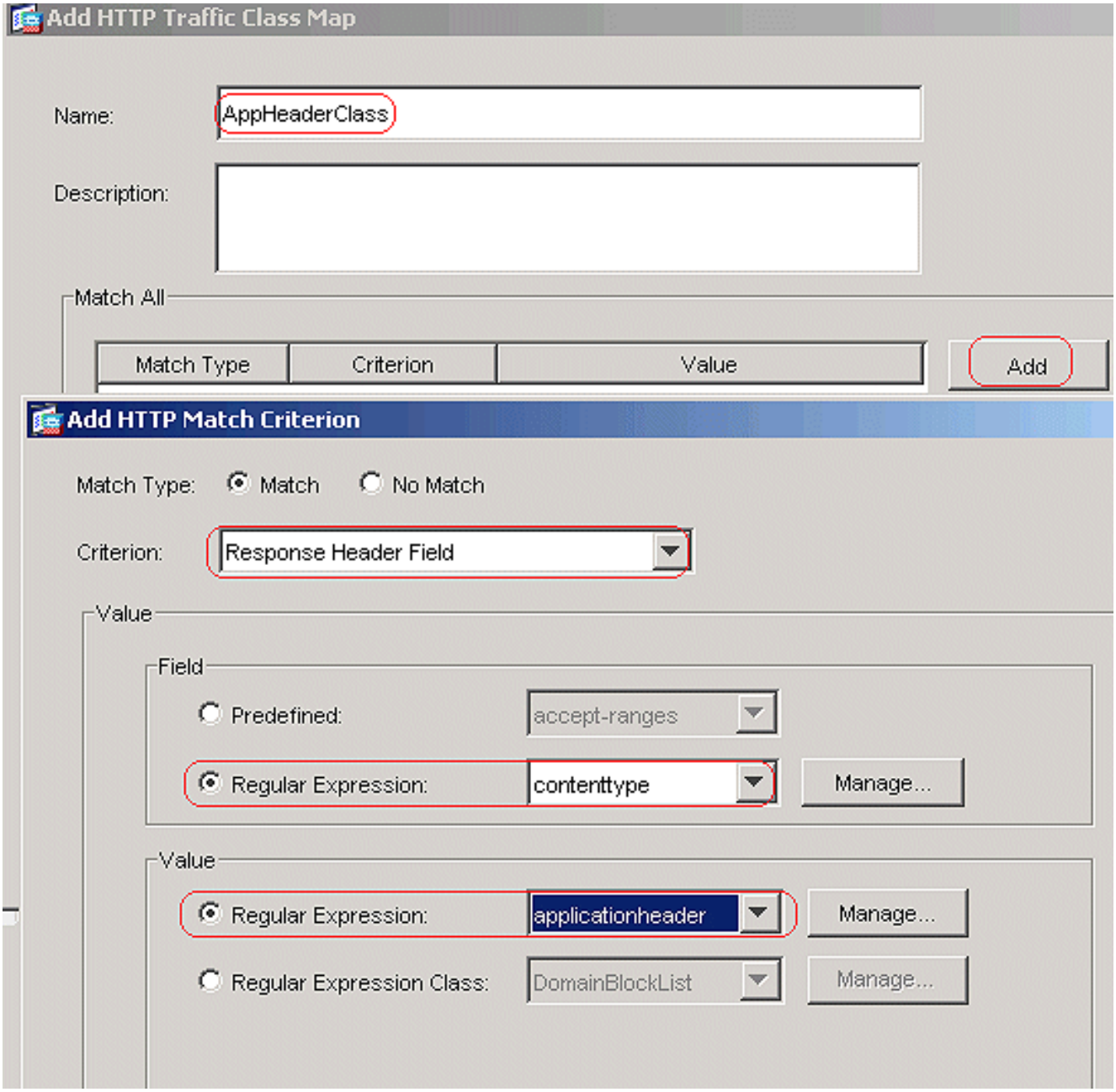


创建正则表达式类 **URLBlockList**，以便匹配以下任意正则表达式：urllist1、urllist2、urllist3 和 urllist4。单击 **Ok**。

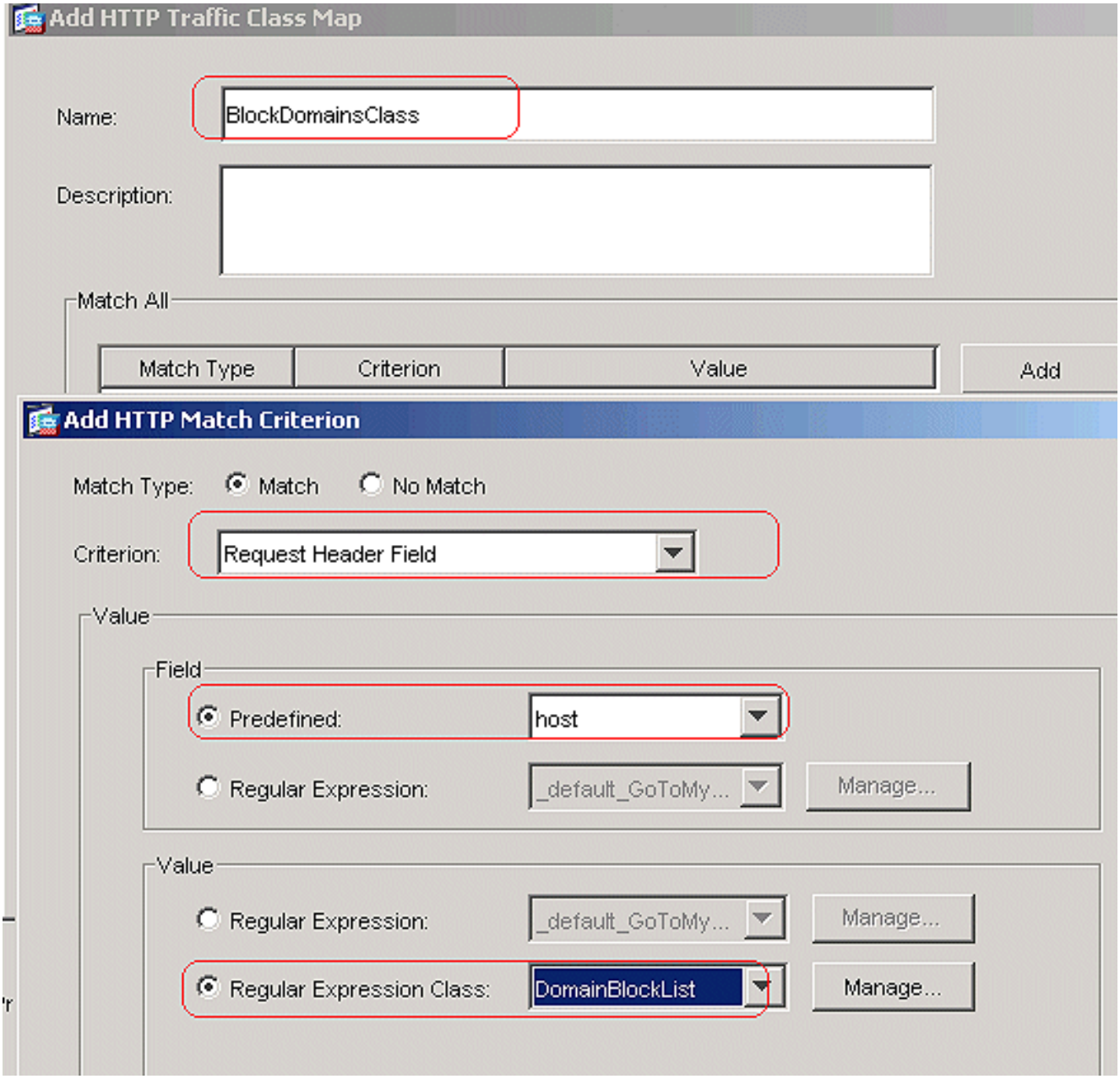


等效 CLI 配置

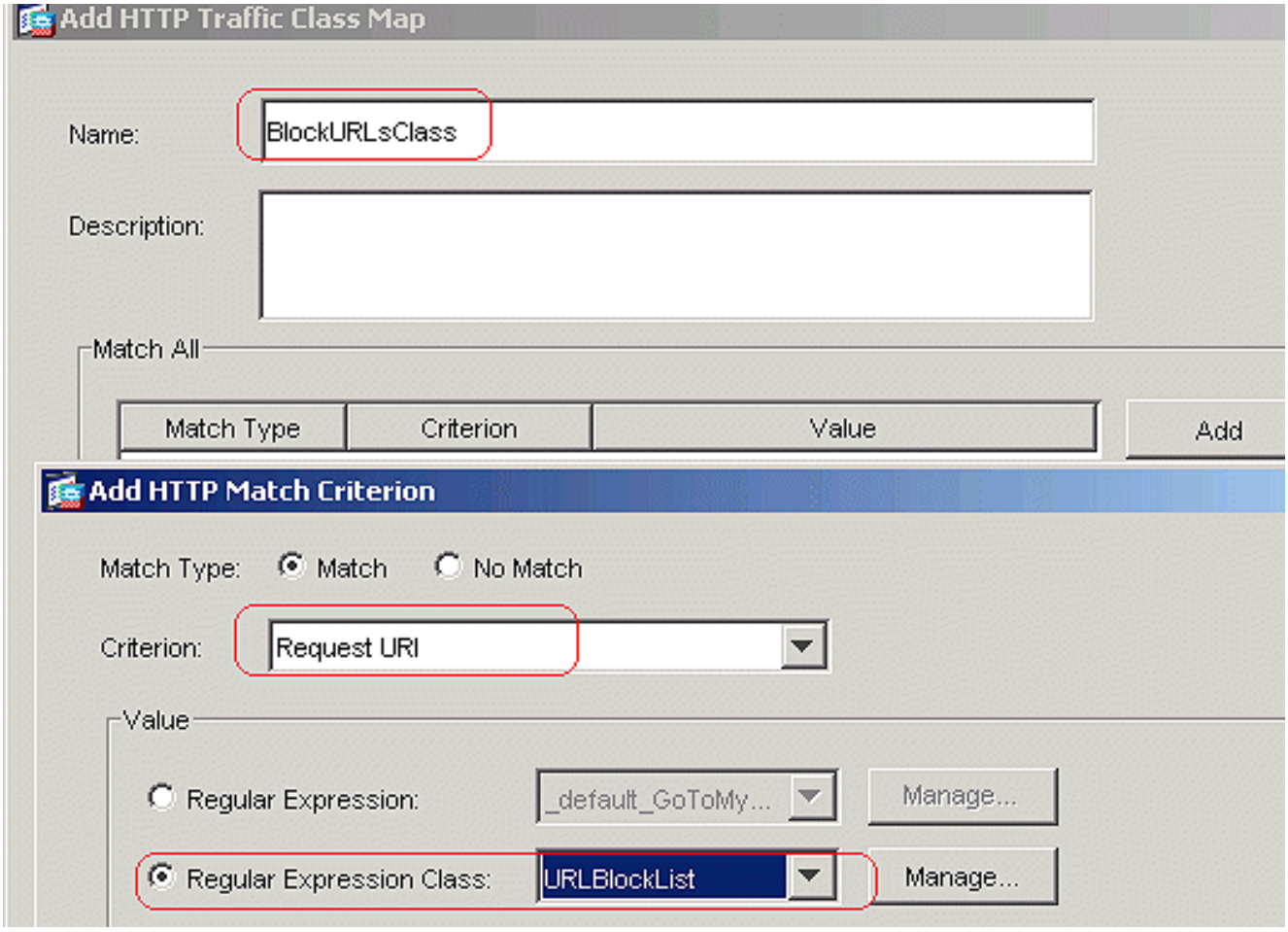
3. **检查由类映射识别出的流量**选择 **Configuration > Global Objects > Class Maps > HTTP > Add**，以便创建类映射，用来检查由各种正则表达式识别出的 HTTP 流量。创建类映射 **AppHeaderClass**，以便用正则表达式捕获来匹配响应标头。



单击 **Ok**。创建类映射 **BlockDomainsClass**，以便用正则表达式捕获来匹配请求标头。

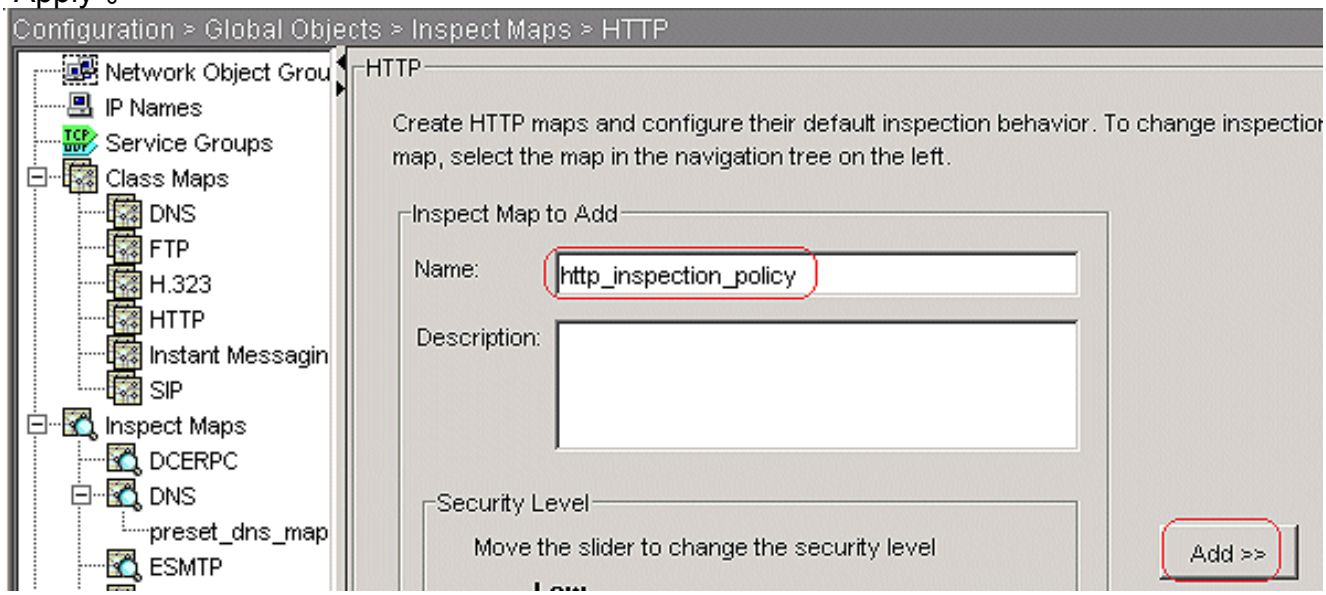


单击 **Ok**。创建类映射 **BlockURLsClass**，以便用正则表达式捕获来匹配请求 URI。

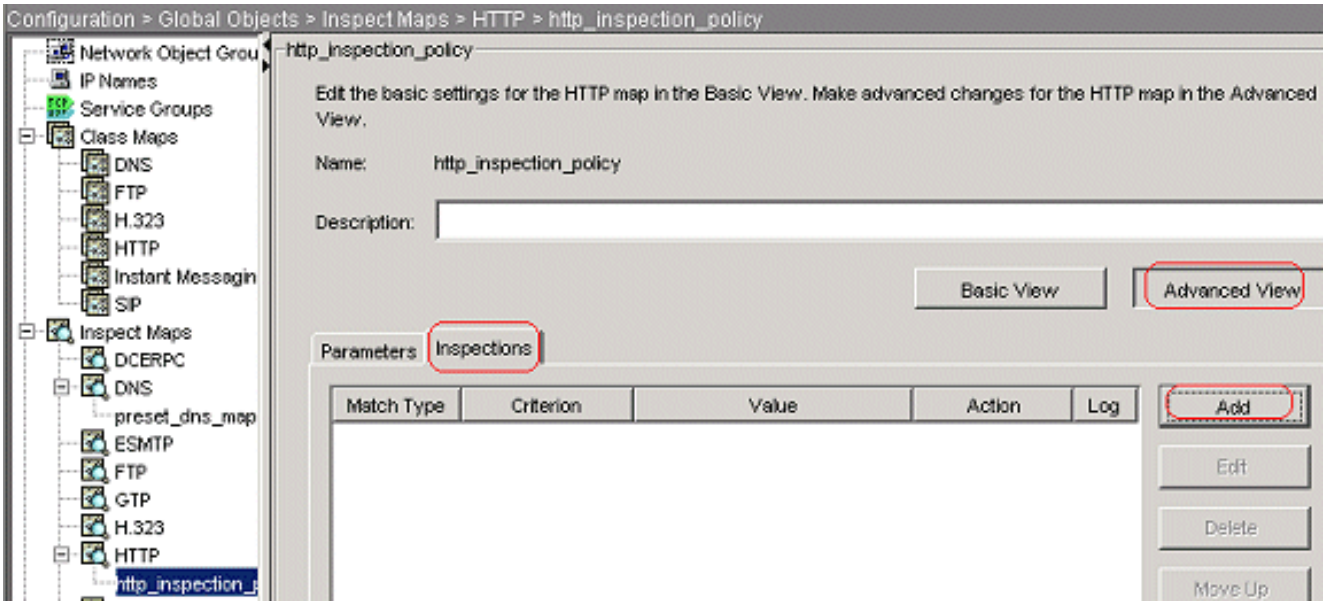


单击 Ok。**等效 CLI 配置**

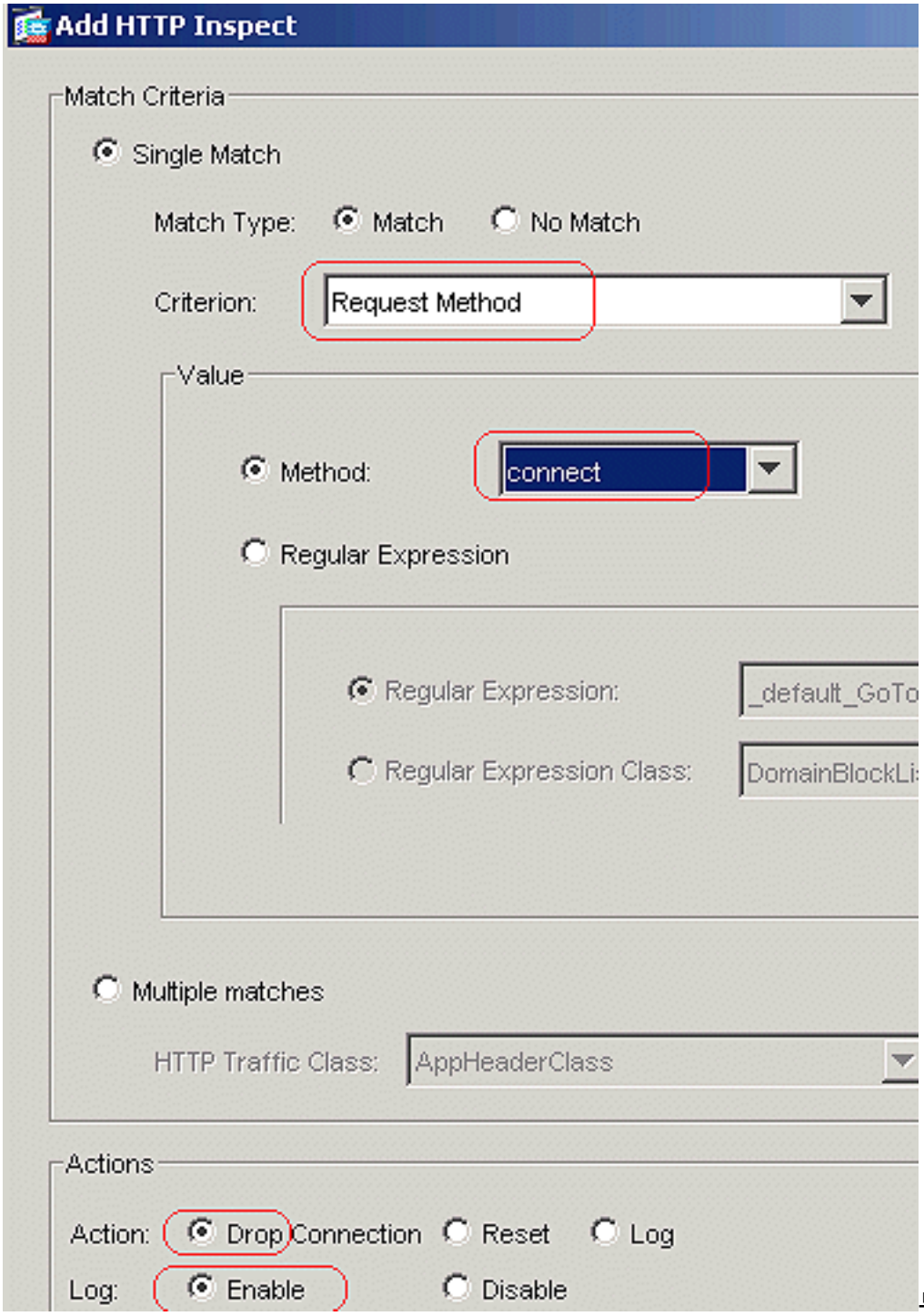
4. **为检查策略中匹配的流量设置操作**选择 **Configuration > Global Objects > Inspect Maps > HTTP**，以便创建 http_inspection_policy，用来为匹配的流量设置操作。单击 **Add**，然后单击“Apply”。



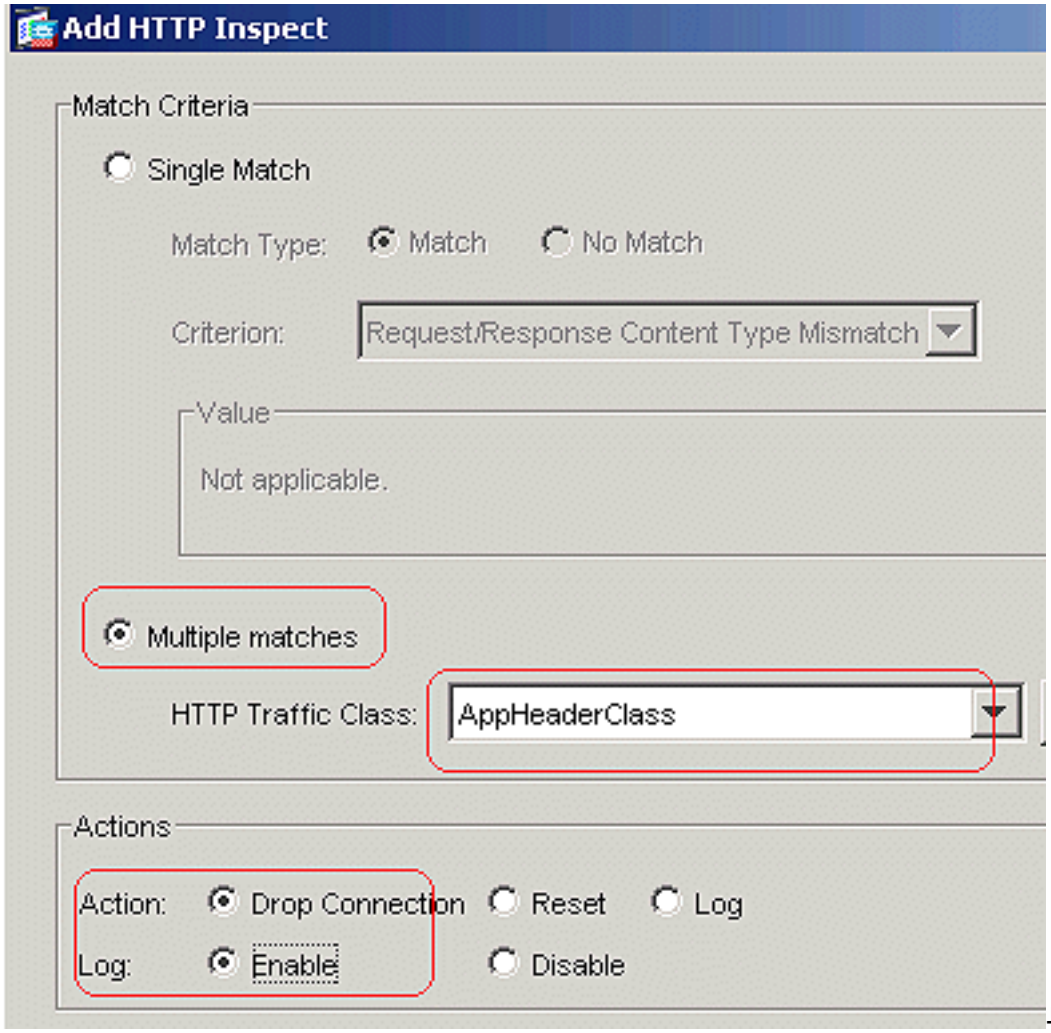
选择 **Configuration > Global Objects > Inspect Maps > HTTP > http_inspection_policy**，然后单击“Advanced View”>“Inspections”>“Add”，以便为目前为止创建的各种类设置操作。



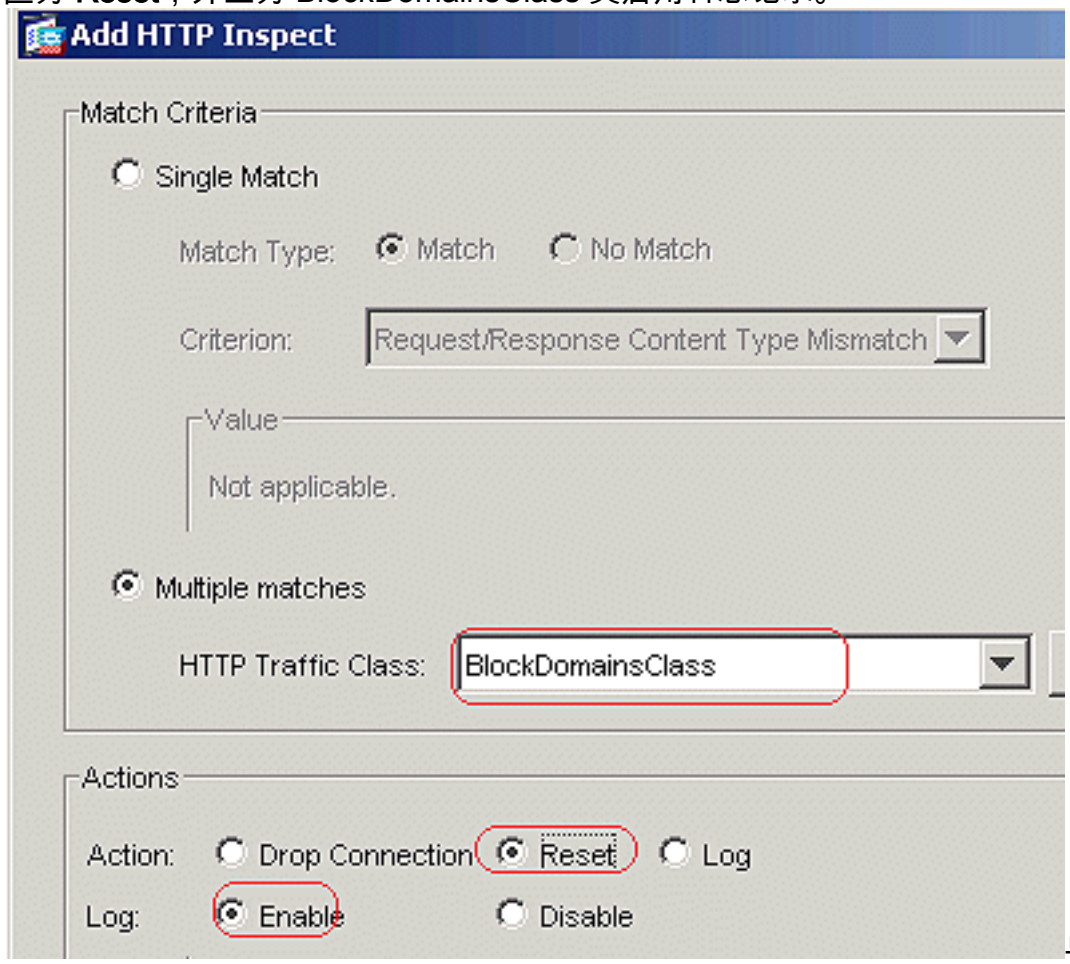
单击 **Ok**。将操作设置为 **Drop Connection**；为“Criterion”为“Request Method”且“Value”为“connect”的流量**启用**日志记录。



单击 **Ok**。将操作设置为 **Drop Connection**，并且为 AppHeaderClass 类启用日志记录。

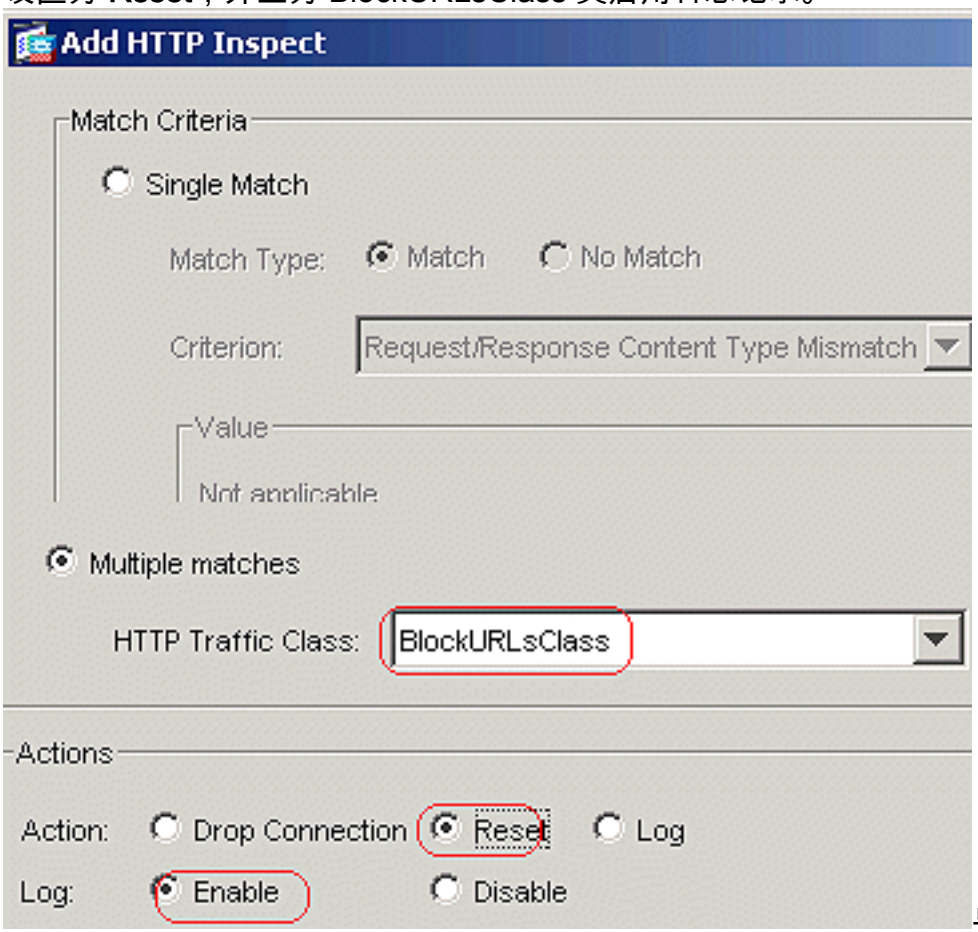


单击 **Ok**。将操作设置为 **Reset**，并且为 BlockDomainsClass 类启用日志记录。



单击 **Ok**。将操作

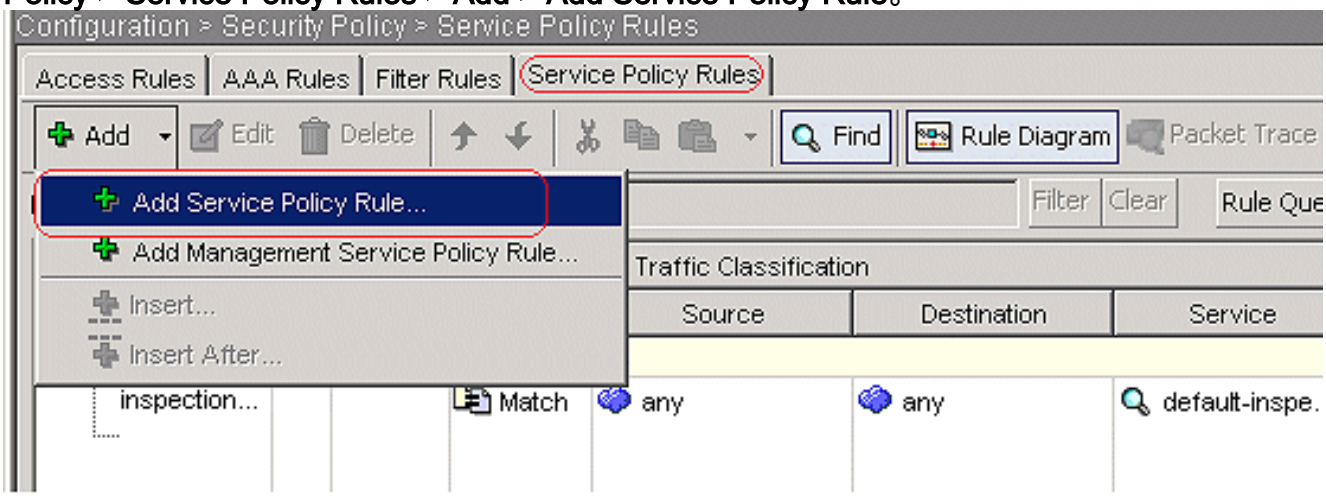
设置为 **Reset**，并且为 BlockURLsClass 类启用日志记录。



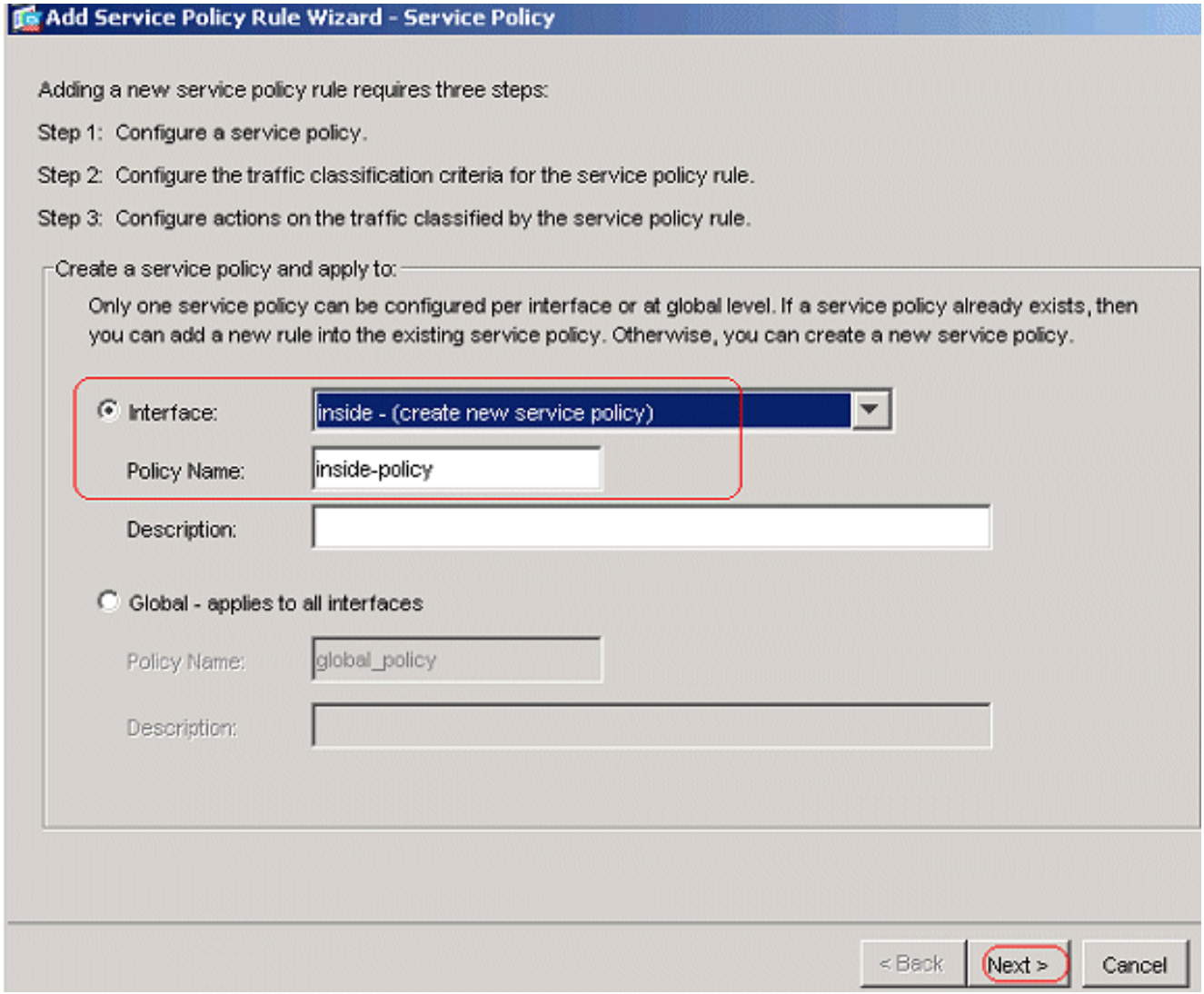
单击 **Ok**。单击 **Apply**。

等效 CLI 配置

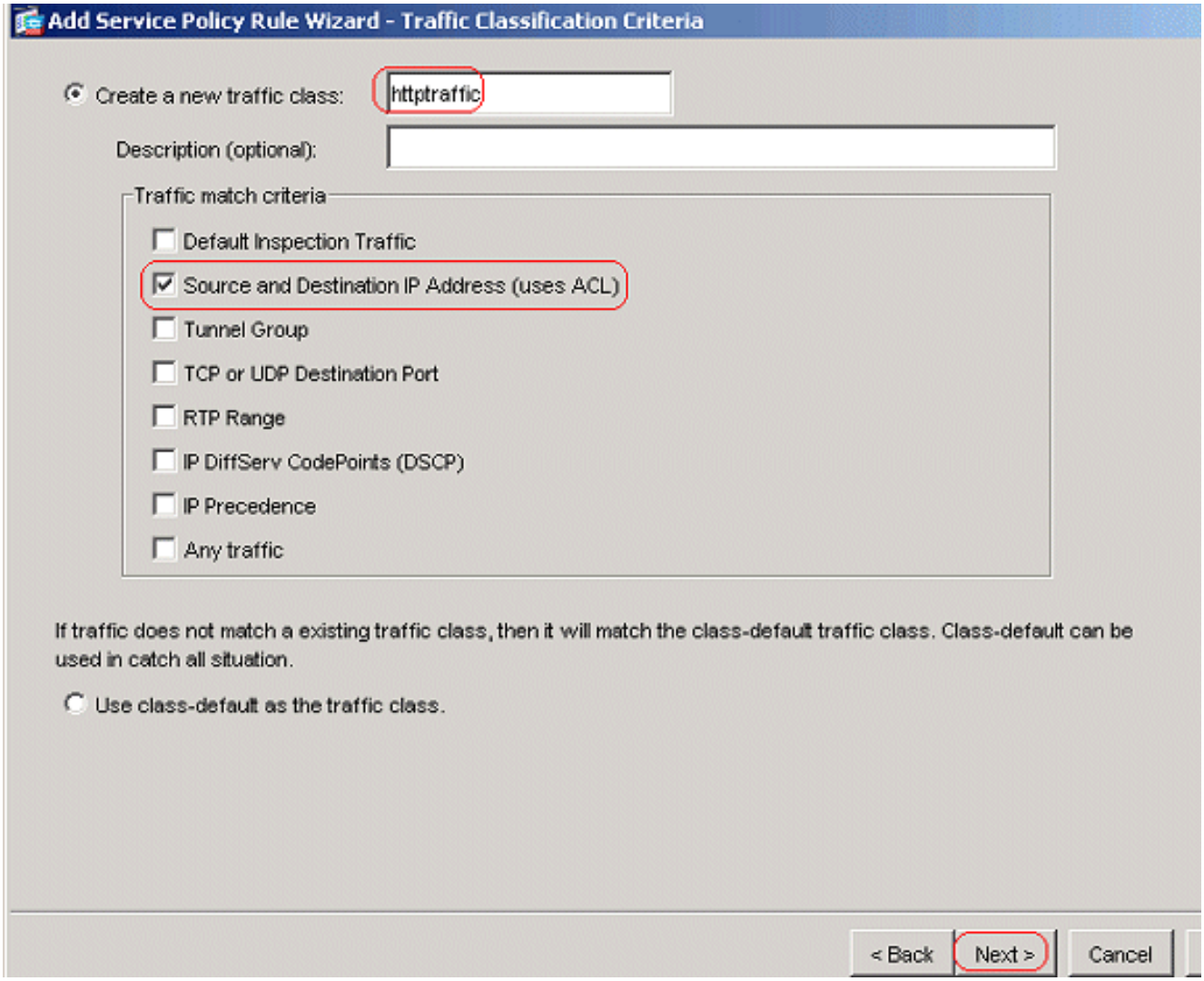
5. **向接口应用检查 http 策略**在“Service Policy Rules”选项卡下选择 **Configuration > Security Policy > Service Policy Rules > Add > Add Service Policy Rule**。



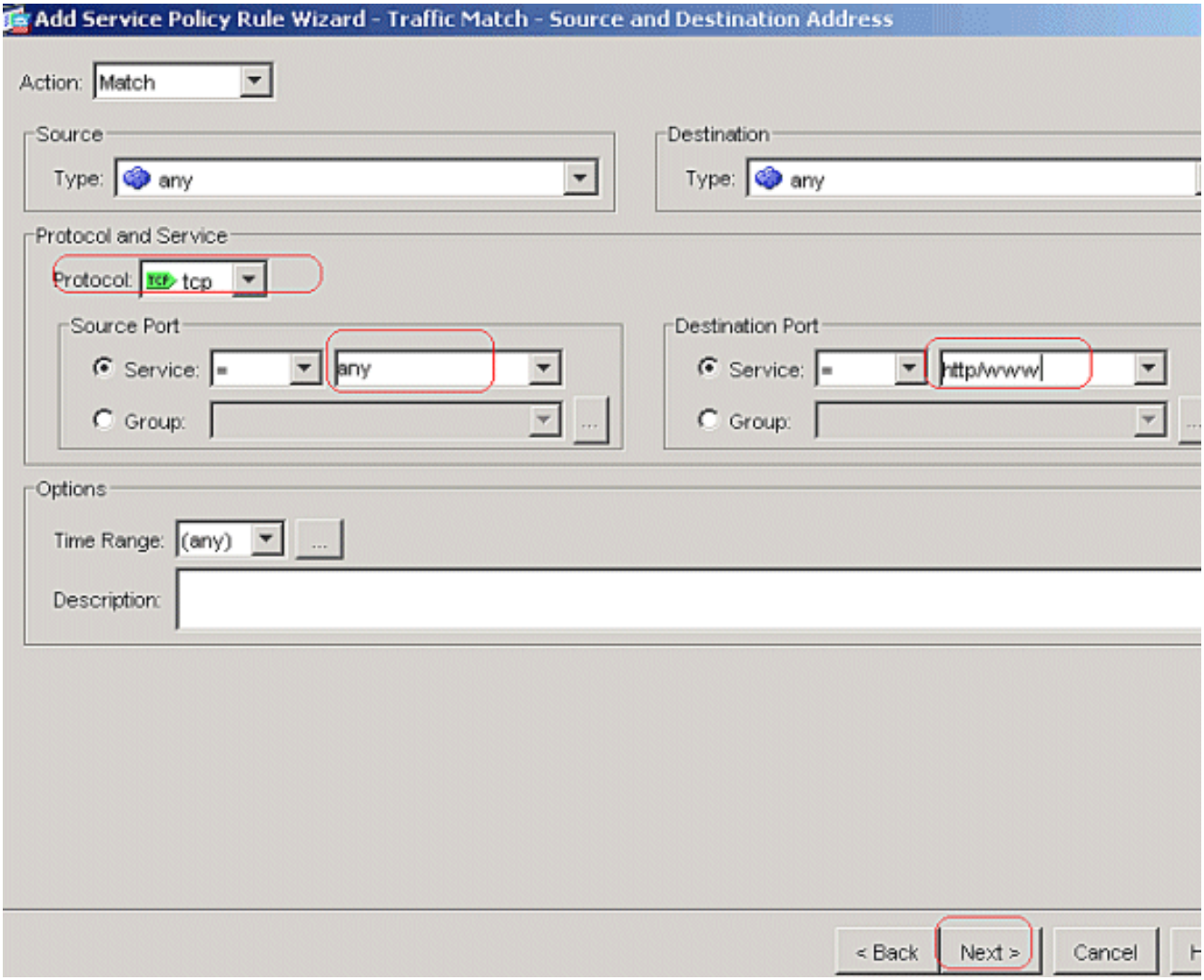
HTTP 数据流从下拉菜单中选择内部接口的 **Interface** 单选按钮，然后选择“Policy Name”作为 inside-policy。单击 **Next**。



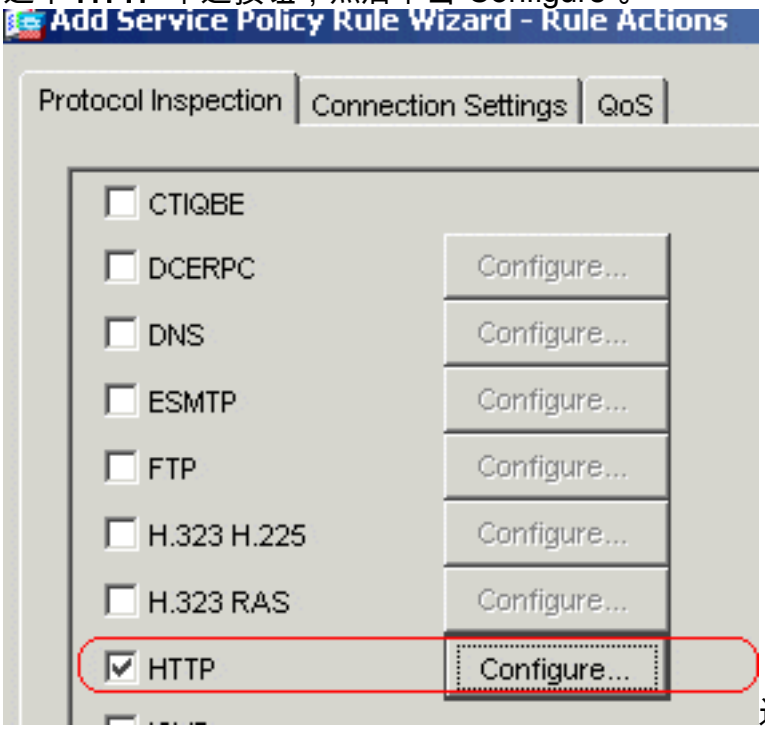
创建类映射 **httptraffic**，然后选中“Source”和“Destination IP Address”（使用 ACL）。单击 **Next**。



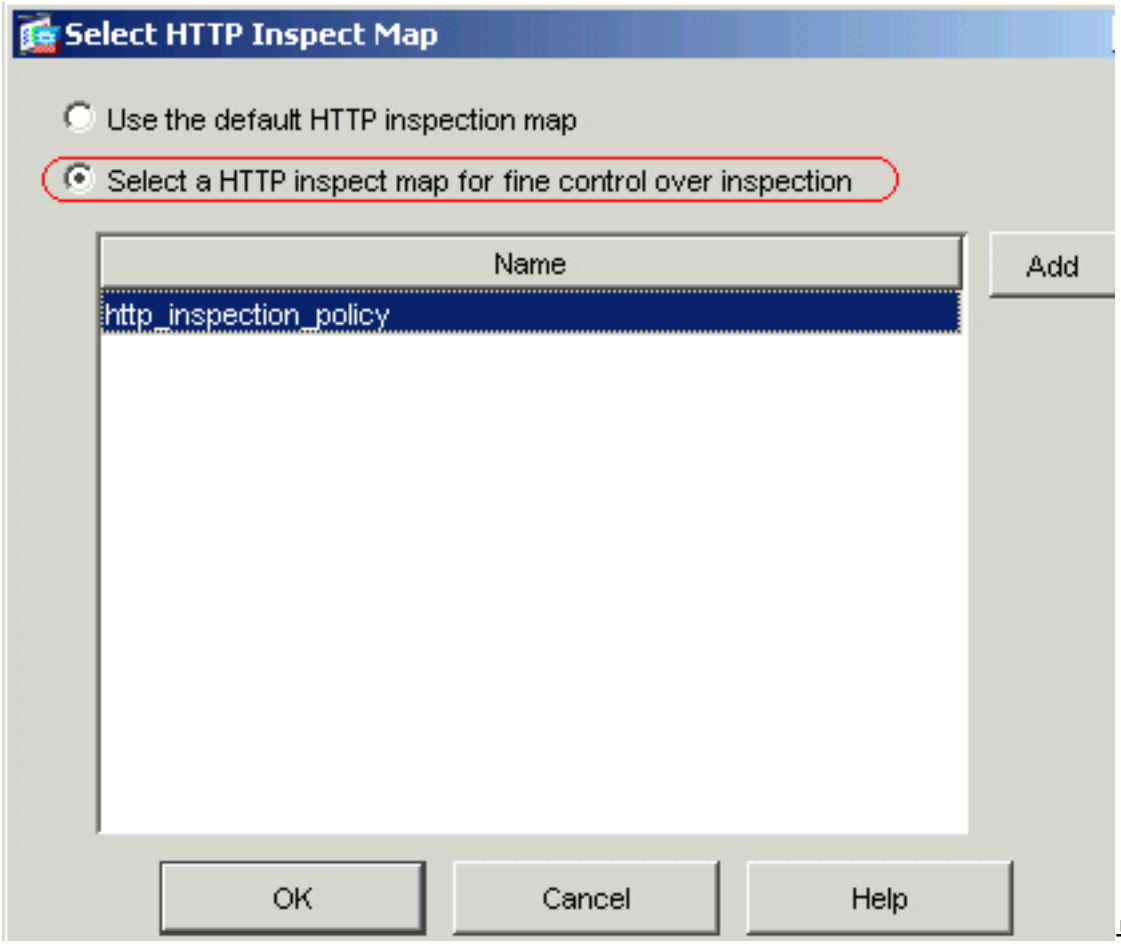
将“Source”和“Destination”设置为 **any**，并将“TCP port”设置为“HTTP”。单击 **Next**。



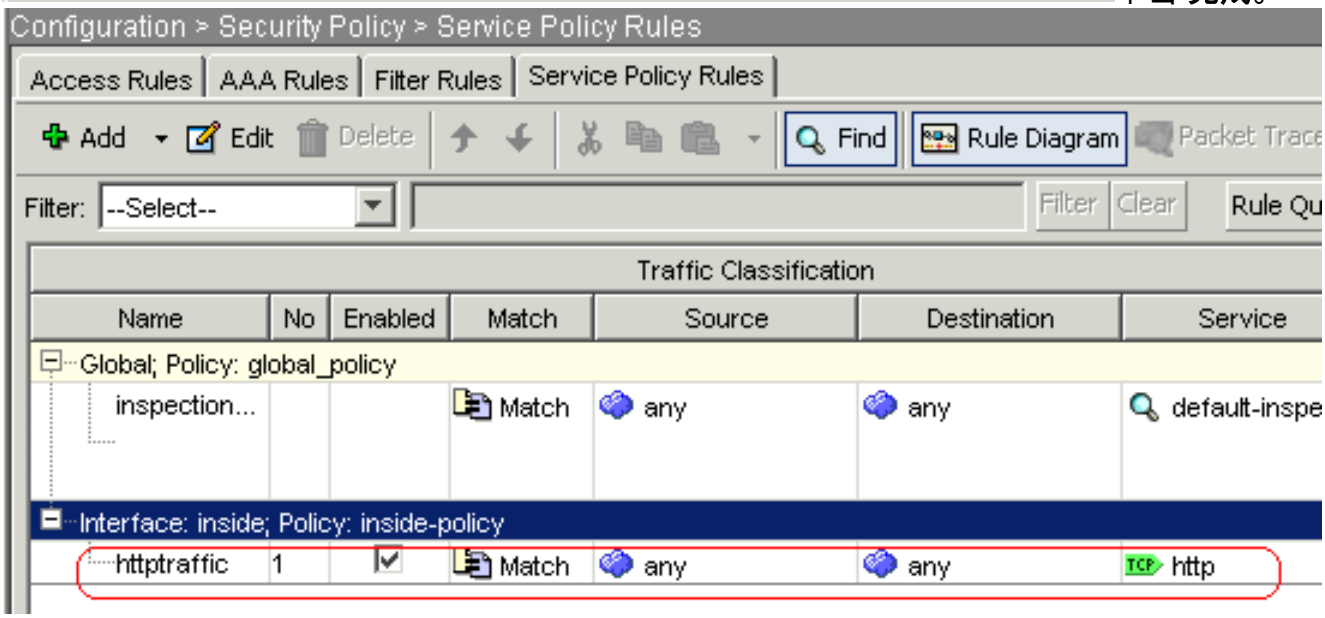
选中 HTTP 单选按钮，然后单击“Configure”。



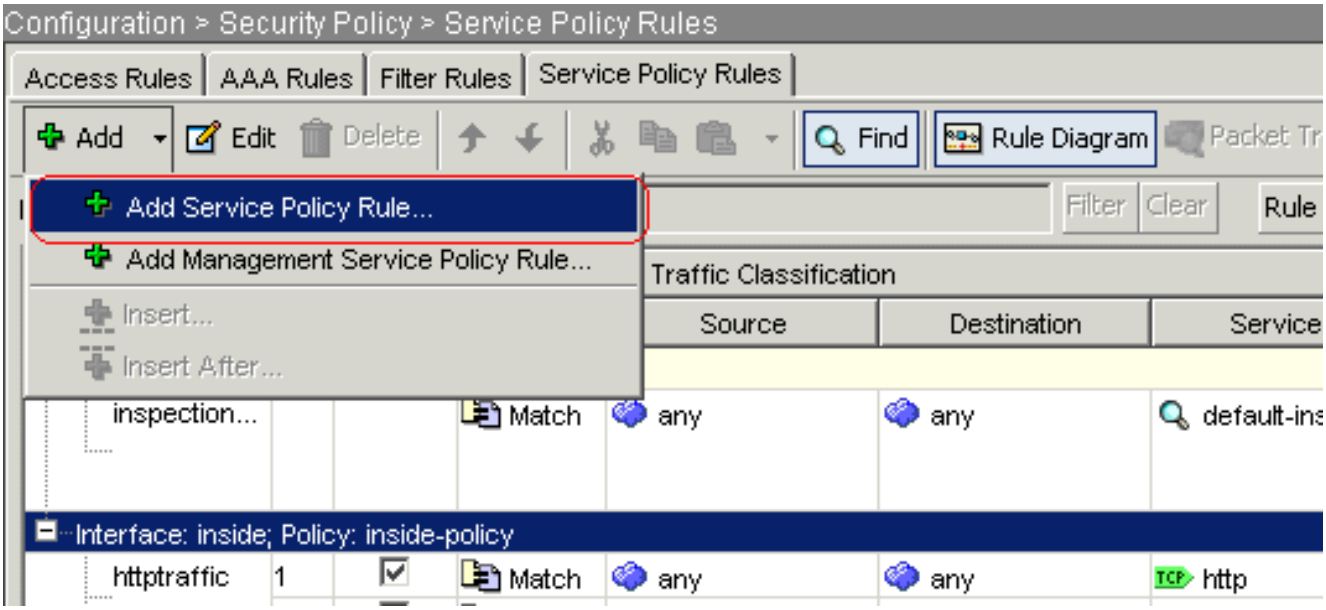
选中 Select a HTTP inspect map for the control over inspection 单选按钮。单击 Ok。



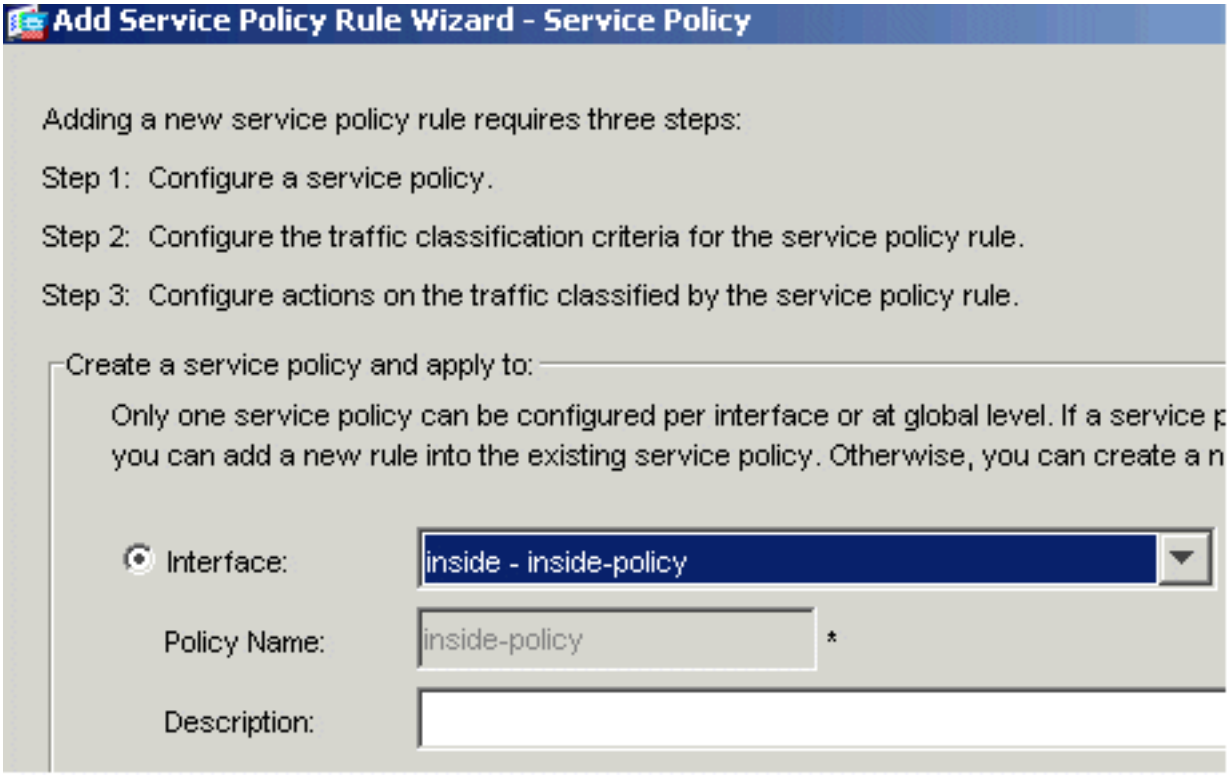
单击 **完成**。



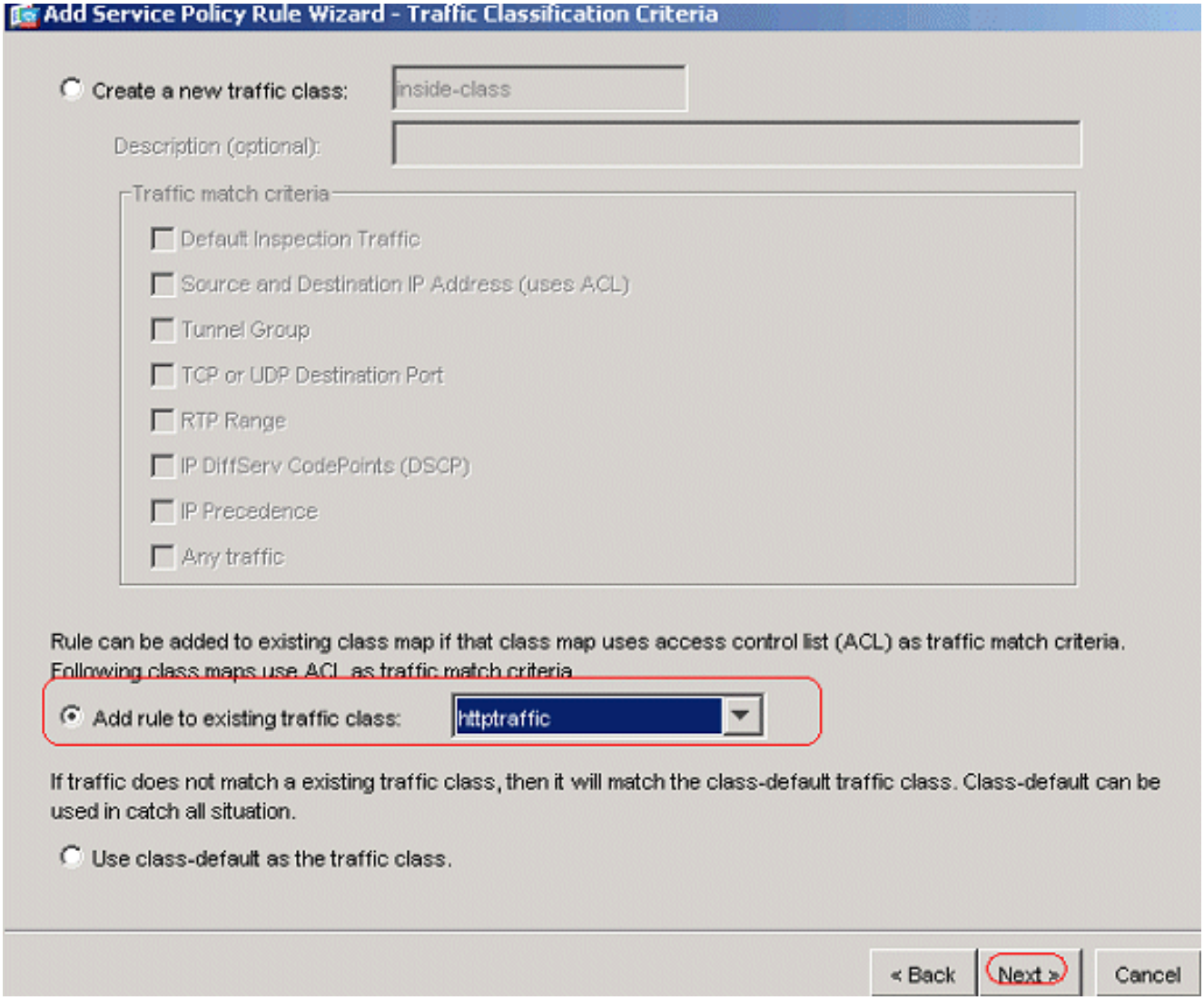
端口 8080 流量再次单击 **Add > Add Service Policy Rule**。



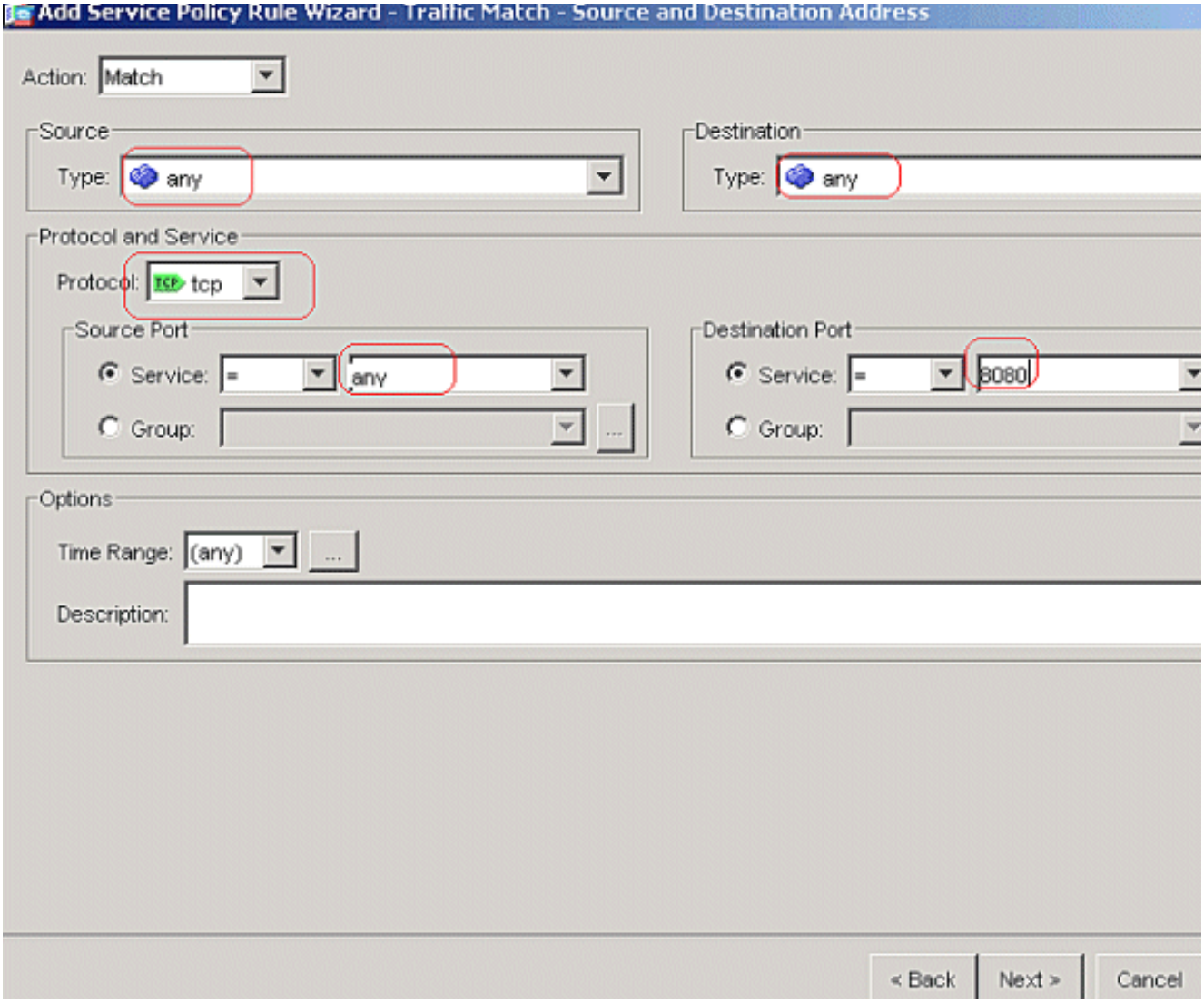
单击 **Next**。



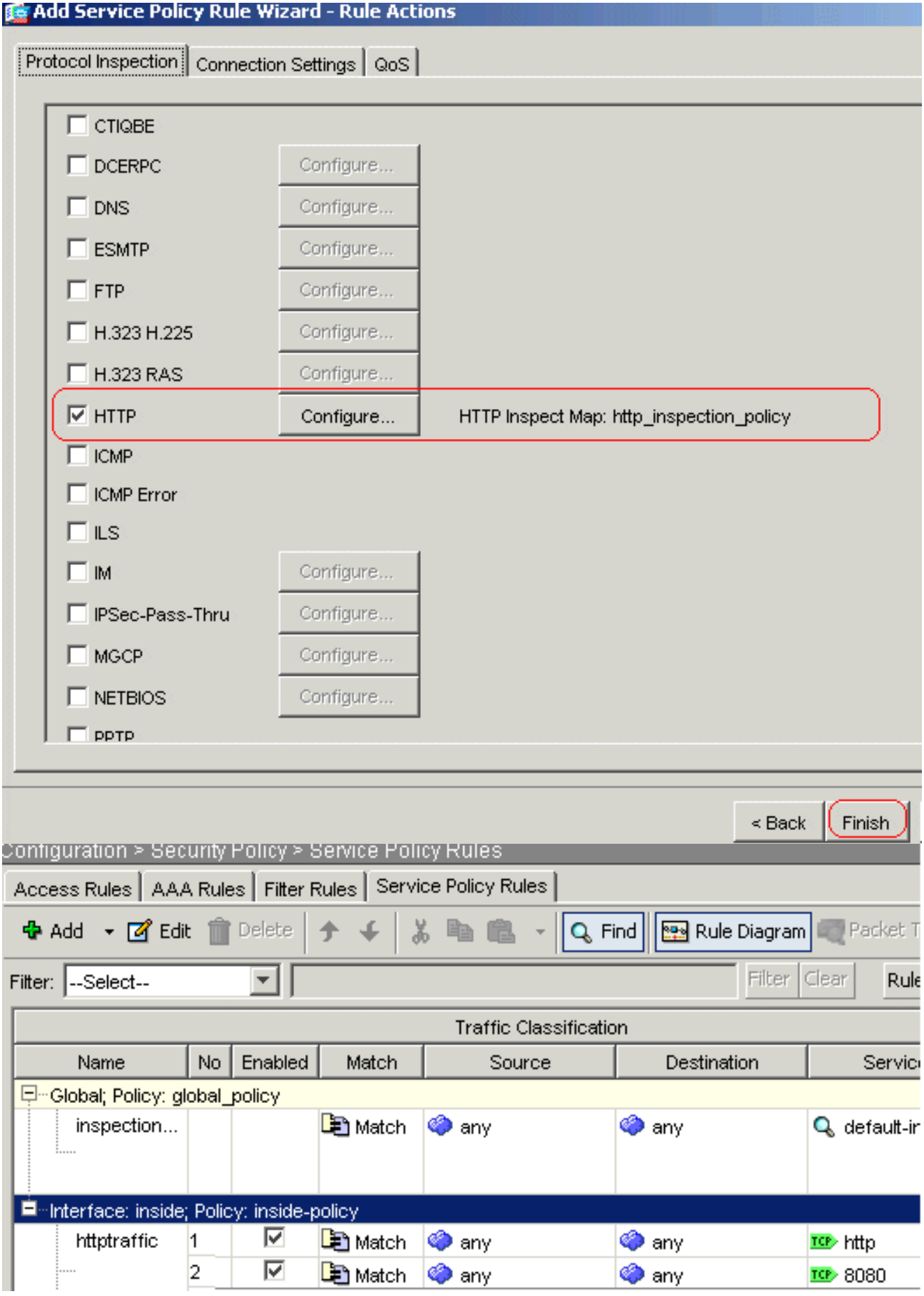
选择 **Add rule to existing traffic class** 单选按钮，然后从下拉菜单中选择“httptraffic”。单击 **Next**。



将“Source”和“Destination”设置为 **any**，并将“TCP port”设置为“8080”。单击 **Next**。


Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address
Action: Match
Source
Type: any
Destination
Type: any
Protocol and Service
Protocol: tcp
Source Port
Service: = any
Group:
Destination Port
Service: = 8080
Group:
Options
Time Range: (any)
Description:
< Back
Next >
Cancel

单击 **完成**。



单击 Apply。等效 CLI 配置

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show running-config regex**—显示已配置的正则表达式`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**—显示已配置的类映射`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**—显示用来检查已配置的 http 流量的策略映射`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**—显示所有策略映射配置以及默认的策略映射配置`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**—显示当前正在运行的所有服务策略配置`ciscoasa#show running-config service-policy service-policy global_policy global service-policy inside-policy interface inside`
- **show running-config access-list**—显示在安全设备上运行的访问列表配置`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#`

故障排除

本部分提供的信息可用于对配置进行故障排除。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug http**—显示 HTTP 流量的调试消息。

相关信息

- Cisco 自适应安全设备支持页
- Cisco Adaptive Security Device Manager (ASDM)支持页面

- Cisco 500 系列 PIX 支持页
- 技术支持和文档 - Cisco Systems