

# ASA/PIX 8.x:使用正規表示式和MPF配置示例阻止某些網站(URL)

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[慣例](#)

[背景資訊](#)

[模組化策略框架概述](#)

[正規表示式](#)

[設定](#)

[網路圖表](#)

[組態](#)

[ASA CLI配置](#)

[ASA配置8.x，帶ASDM 6.x](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## [簡介](#)

本文檔介紹如何配置思科安全裝置ASA/PIX 8.x，該裝置使用帶模組化策略框架(MPF)的正規表示式來阻止某些網站(URL)。

**注意：**此配置不會阻止所有應用程式下載。為了可靠地阻止檔案，應使用專用裝置（如Ironport S系列）或模組（如ASA的CSC模組）。

**注意：**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查或檢查，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8.0(x)和更新版本的Cisco 5500系列調適型安全裝置(ASA)
- 適用於ASA 8.x的Cisco調適型安全裝置管理器(ASDM)版本6.x

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8.0(x)及更高版本的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，也可以使用元字元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可轉義CLI中的所有特殊字元，如問號(?)或頁籤。例如，鍵入d[Ctrl+V]?g可在配置中輸入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**使用檢測策略對映的模組化策略框架**來配置應用檢測的特殊操作。有關詳細資訊，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，或者可以直接在檢測策略對映中使用match命令，則可以標識要對其執行操作的流量。有些match命令允許您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。有關詳細資訊，請參閱[class-map type regex](#)命令。

此表列出了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doggonit。
(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abxyxyz。
	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。 <b>注意：</b> 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abxyxyz。
{x,}	最小重複量詞	重複至少x次。例如，ab(xy){2,}z匹配abxyxyz、abxyxyz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字元或第一個字元，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
\x N N	轉義的十 六進位制 數	匹配使用十六進位制的ASCII字元，該十六進位制恰好是兩位數
\N N N	轉義的八 進位制數	匹配八進位制的ASCII字元，該字元恰好為三個數字。例如，字元040表示一個空格。

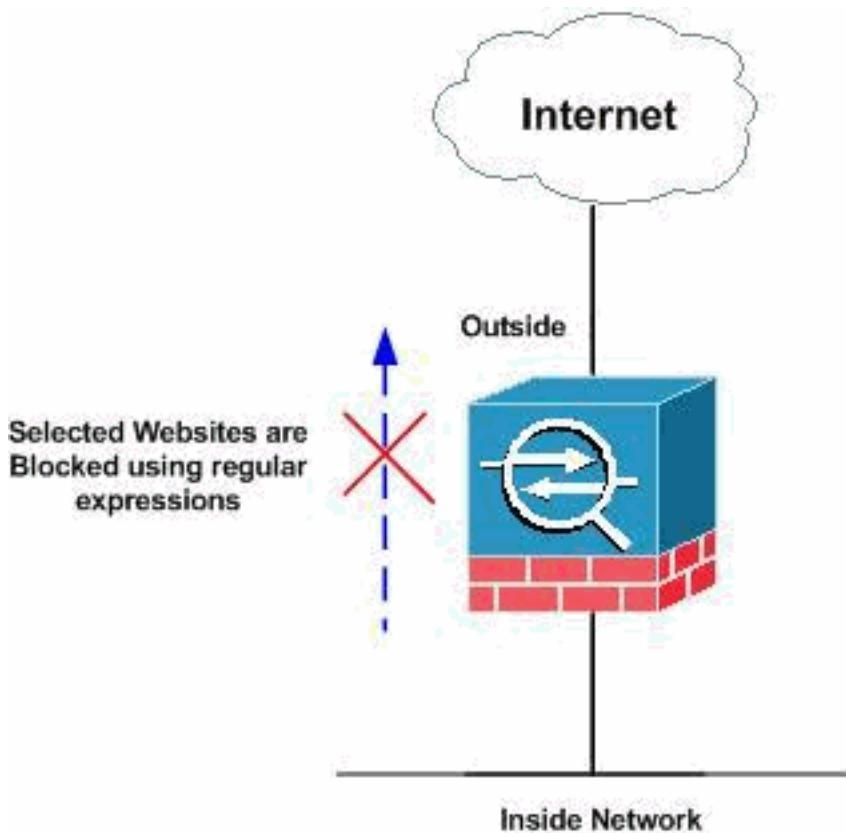
## 設定

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](#)(僅限註冊客戶)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配置8.x，帶ASDM 6.x](#)

## [ASA CLI配置](#)

```
ciscoasa#show running-config
:
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 2KFQnbNIIdI.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配置8.x，帶ASDM 6.x

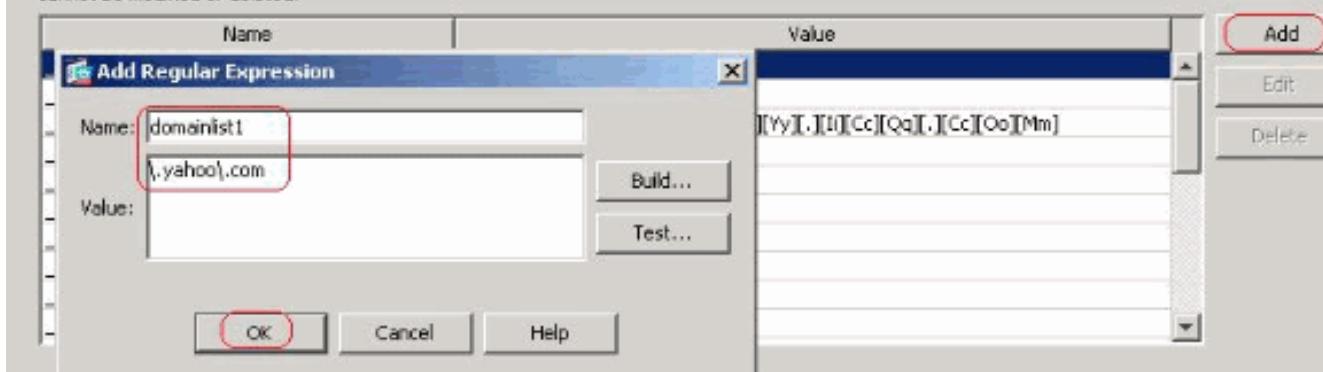
完成以下步驟以配置正規表示式，並將它們應用於MPF以阻止特定網站，如圖所示。

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

Configuration > Firewall > Objects > Regular Expressions

Regular Expressions

Configure regular expressions for use in pattern matching. Regular expressions with names starting with "\_default" are default regular expressions and cannot be modified or deleted.



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



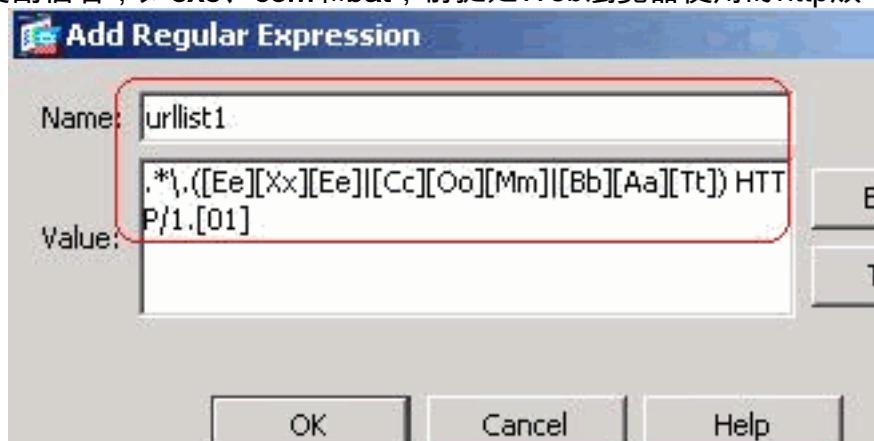
建立正規表示式

domainlist3以捕獲域名youtube.com。按一下「OK」（確定）。



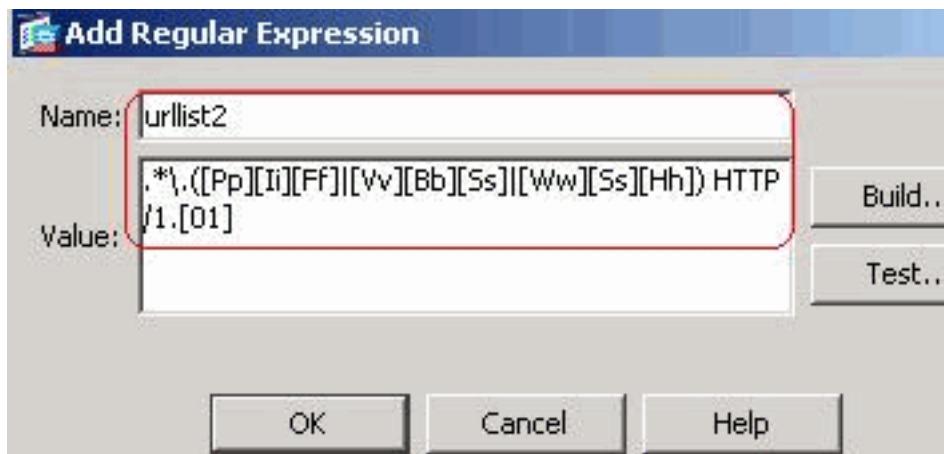
建立一個正規表示式

urllist1，以便捕獲副檔名，如exe、com和bat，前提是Web瀏覽器使用的http版本必須是1.0或



1.1。按一下OK。

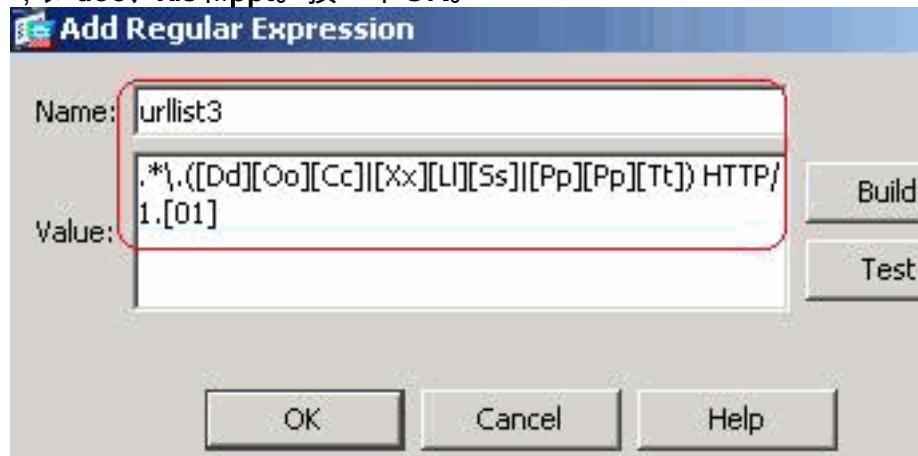
如果由Web瀏覽器使用的http版本必須是1.0或1.1，請建立正規表示式urllist2，以便捕獲副檔名，例如pif、



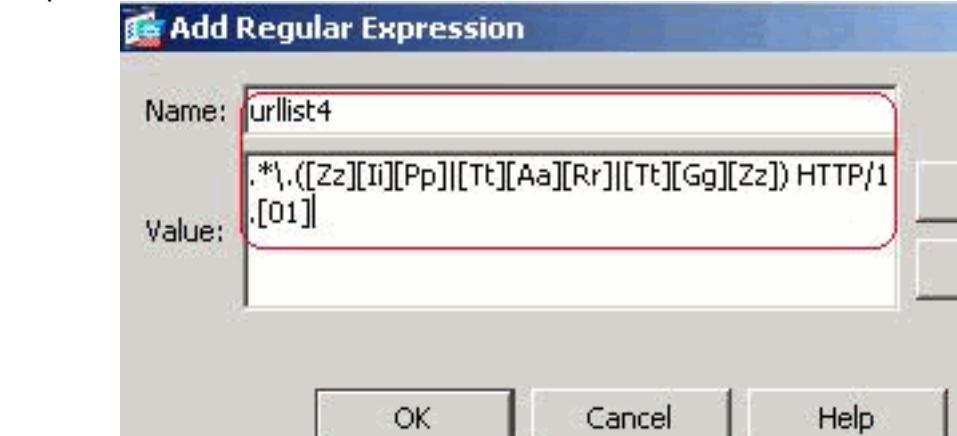
vbs和wsh。按一下OK。

如

果由Web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urlist3，以便捕獲副檔名，如doc、xls和ppt。按一下OK。



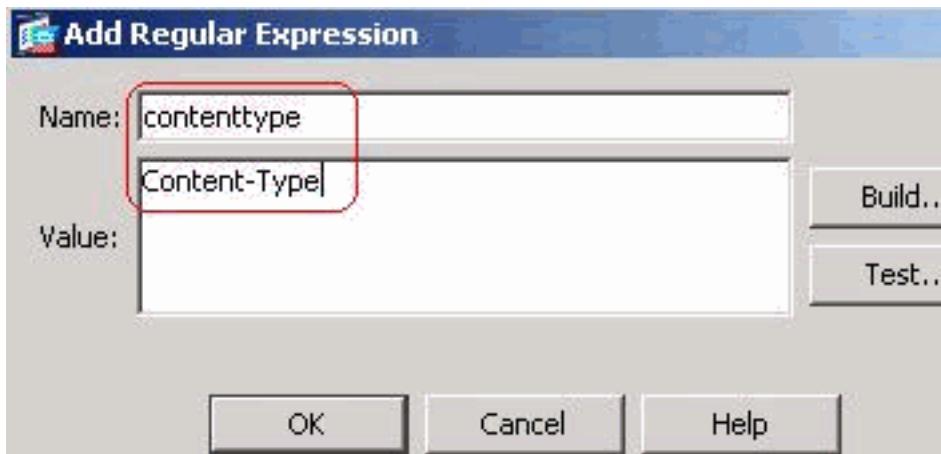
如果由Web瀏覽器使用的http版本必須是1.0或1.1，請建立正規表示式urlist4，以便捕獲副檔名，如zip、tar和tgz。按一



下OK。

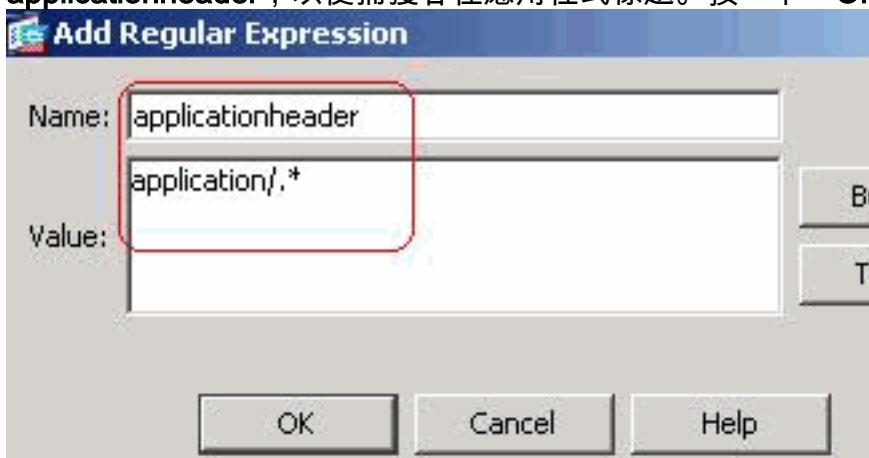
contenttype以便捕獲內容型別。按一下「OK」（確定）。

建立正規表示式



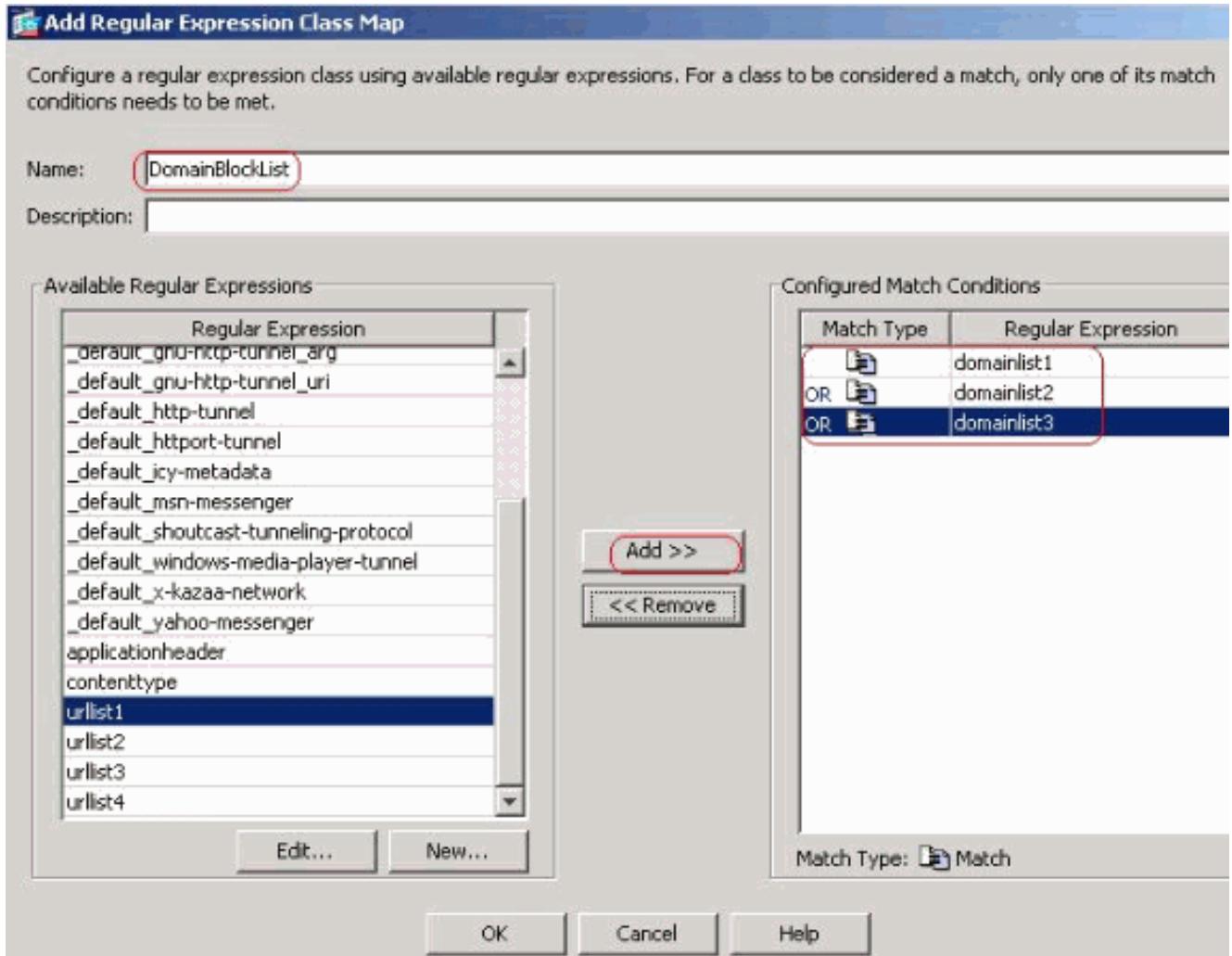
建立正規表示式

applicationheader，以便捕獲各種應用程式標題。按一下「OK」（確定）。

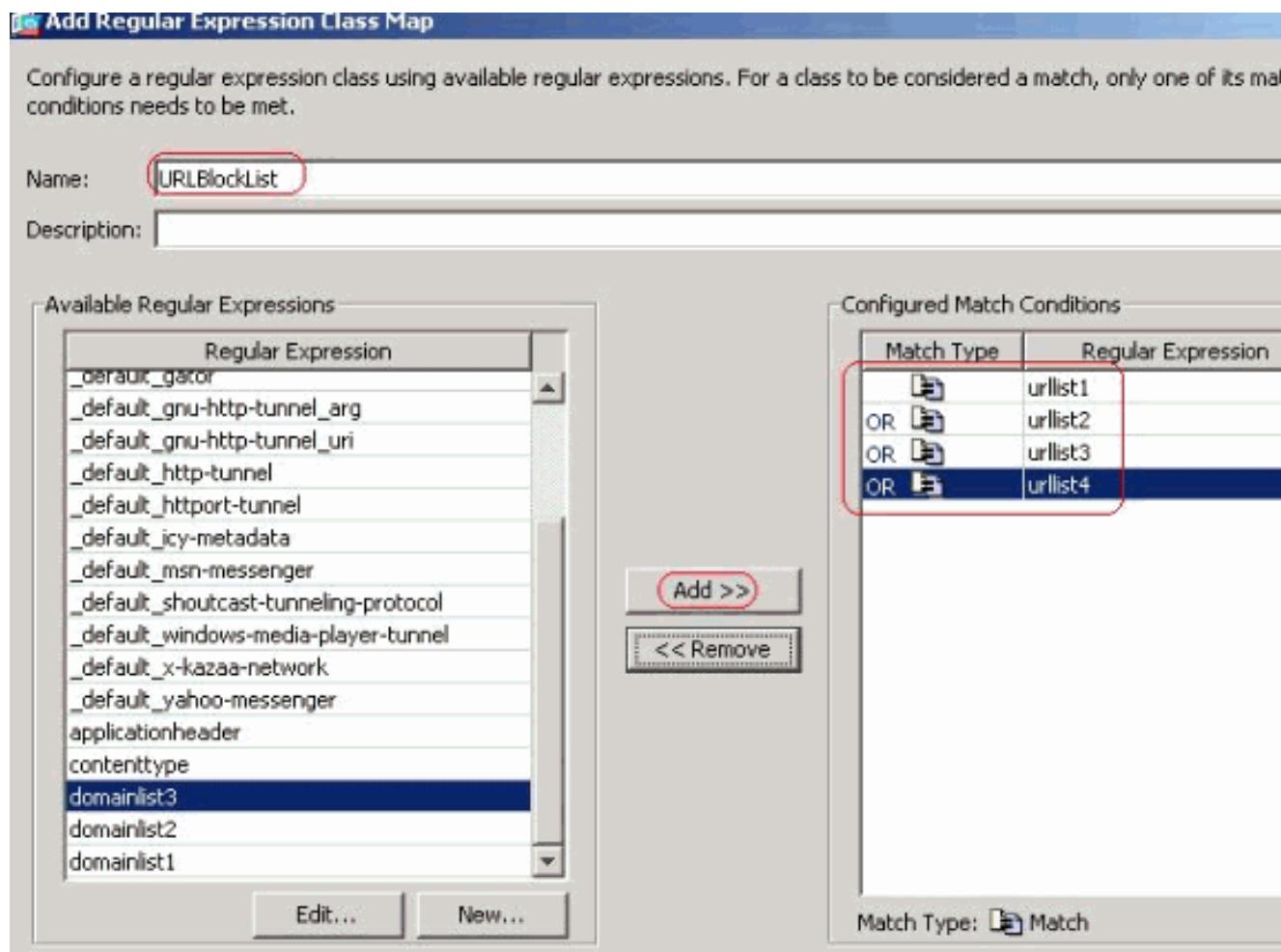


等效的CLI配置

2. 建立正規表示式類選擇Configuration > Firewall > Objects > Regular Expressions，然後按一下Regular Expression Classes頁籤下的Add，以建立各種類，如圖所示。建立正規表示式類DomainBlockList，以便匹配正規表示式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urlist1、urlist2、urlist3和urlist4。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 > Firewall > Objects > Class Maps > HTTP > Add，以建立類對映來檢查由各種正規表示式標識的http流量，如下所示。建立類對映AppHeaderClass，以便將響應報頭與正規表示式捕獲相匹配。

Add HTTP Traffic Class Map

Name:	AppHeaderClass	
Description:		
Match Option:	<input checked="" type="radio"/> Match All	<input type="radio"/> Match Any
Match Type	Criterion	Value

Add HTTP Match Criterion

Match Type:	<input checked="" type="radio"/> Match	<input type="radio"/> No Match
Criterion:	Request Header Field	
Value	Field <input type="radio"/> Predefined: accept <input checked="" type="radio"/> Regular Expression: contenttype Manage...	
Value	<input checked="" type="radio"/> Regular Expression: applicationheader Manage... <input type="radio"/> Regular Expression Class: DomainBlockList Manage...	

OK Cancel Help

按一下「OK」建立類對映BlockDomainsClass，以將請求報頭與正規表示式捕獲相匹配。

Add HTTP Traffic Class Map

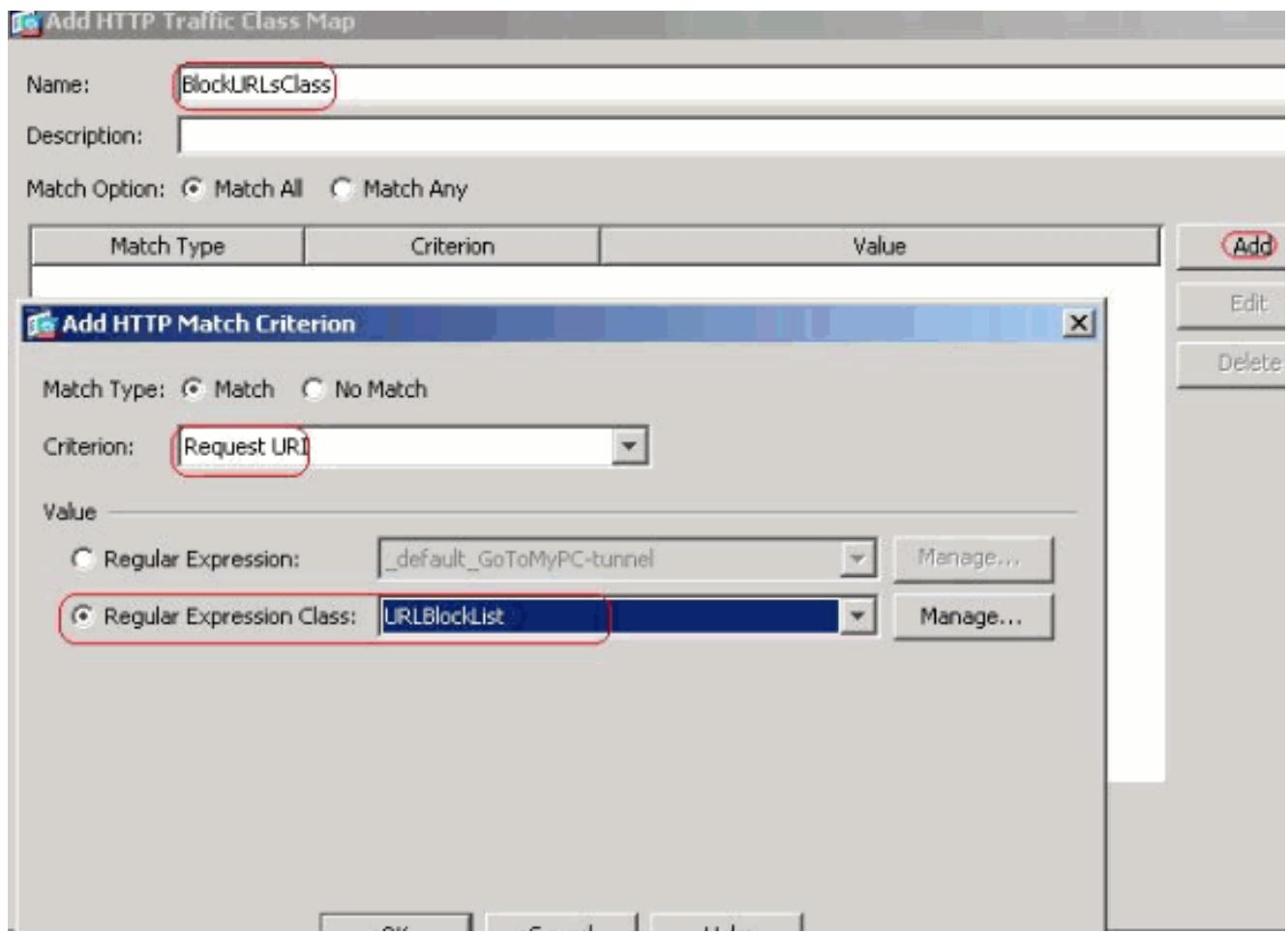
Name:	BlockDomainsClass	
Description:		
Match Option:	<input checked="" type="radio"/> Match All	<input type="radio"/> Match Any
Match Type	Criterion	Value

Add HTTP Match Criterion

Match Type:	<input checked="" type="radio"/> Match	<input type="radio"/> No Match
Criterion:	Request Header Field	
Value	<input type="radio"/> Predefined: host <input checked="" type="radio"/> Regular Expression: contenttype Manage...	
Value	<input type="radio"/> Regular Expression: _default_GoToMyPC-tunnel Manage... <input checked="" type="radio"/> Regular Expression Class: DomainBlockList Manage...	

OK Cancel Help

按一下「OK」（確定）。建立類對映BlockURLsClass，以便將請求URI與正規表示式捕獲相匹配。



按一下「OK」(確定)。等效的CLI配置

- 為檢查策略中的匹配流量設定操作選擇Configuration > Firewall > Objects > Inspect Maps > HTTP，以便建立http\_inspection\_policy，為匹配的流量設定操作，如下所示。按一下「OK」(確定)。

Add HTTP Inspect Map

Name:	http_inspection_policy										
Description:											
<a href="#">Security Level</a>   <a href="#">Details</a>											
<a href="#">Parameters</a> <a href="#">Inspections</a>											
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Match Type</th> <th>Criterion</th> <th>Value</th> <th>Action</th> <th>Log</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="height: 150px;"></td> </tr> </tbody> </table> <div style="float: right; margin-right: 10px;"> <a href="#">Add</a>  <a href="#">Edit</a>  <a href="#">Delete</a>  <a href="#">Move Up</a>  <a href="#">Move Down</a> </div>		Match Type	Criterion	Value	Action	Log					
Match Type	Criterion	Value	Action	Log							
<input type="button" value="OK"/>   <input type="button" value="Cancel"/>   <input type="button" value="Help"/>											

選擇 Configuration > Firewall > Objects > Inspect Maps > HTTP > http\_inspection\_policy ( 按兩下 )，然後按一下 Details > Add，以便為目前建立的各種類設定操作。

Edit HTTP Inspect Map

Name:	http_inspection_policy										
Description:											
<a href="#">Security Level</a>   <a href="#">Details</a>											
<a href="#">Parameters</a> <a href="#">Inspections</a>											
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Match Type</th> <th>Criterion</th> <th>Value</th> <th>Action</th> <th>Log</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="height: 150px;"></td> </tr> </tbody> </table> <div style="float: right; margin-right: 10px;"> <input type="button" value="Add"/>   <input type="button" value="Edit"/> </div>		Match Type	Criterion	Value	Action	Log					
Match Type	Criterion	Value	Action	Log							

將操作設定為 Drop Connection，並為 Criterion as Request Method 和 Value as connect 啟用日

Add HTTP Inspect

Match Criteria

Single Match

Match Type:  Match  No Match

Criterion: Request Method

Value

Method: connect

Regular Expression

Regular Expression: \_default\_GoToMyPC-tunnel

Regular Expression Class: DomainBlockList

Multiple matches

HTTP Traffic Class: AppHeaderClass

Actions

Action:  Drop Connection  Reset  Log

Log:  Enable  Disable

誌記錄。

OK

Cancel

Help

按一下「

OK」將操作設定為Drop Connection，並為AppHeaderClass類啟用日誌記錄。

**Add HTTP Inspect**

Match Criteria

Single Match

Match Type:  Match  No Match

Criterion: Request/Response Content Type Mismatch

Value

Not applicable.

Multiple matches

HTTP Traffic Class: AppHeaderClass

Actions

Action:  Drop Connection  Reset  Log

Log:  Enable  Disable

OK Cancel Help

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

**Add HTTP Inspect**

Match Criteria

Single Match

Match Type:  Match  No Match

Criterion: Request/Response Content Type Mismatch

Value

Not applicable.

Multiple matches

HTTP Traffic Class: BlockDomainsClass

Actions

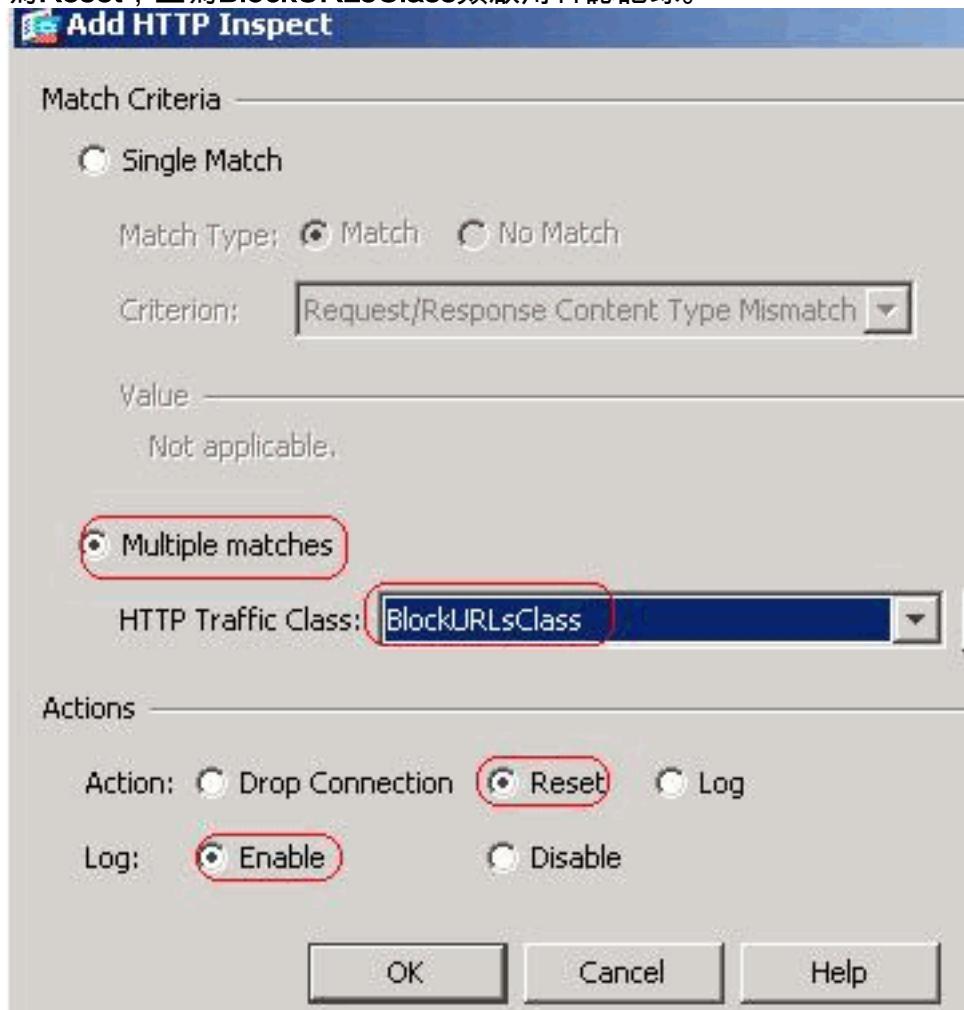
Action:  Drop Connection  Reset  Log

Log:  Enable  Disable

OK Cancel Help

按一下「OK」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

- 將檢測http策略應用到介面選擇Configuration > Firewall > Service Policy Rules > Add > Add Service Policy Rule。



HTTP流量從下拉選單中選擇Interface單選按鈕with inside interface，然後選擇Policy Name as inside-policy。按「Next」（下一步）。

## Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, the new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: inside - (create new service policy) ▾

Policy Name: inside-policy

Description:

Global - applies to all interfaces

Policy Name: global\_policy

Description:

≤ Back

Next >

建立類對映httptraffic並檢查源和目標IP地址（使用ACL）。按「Next」（下一步）。

## Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

### Traffic Match Criteria

Default Inspection Traffic

Source and Destination IP Address (uses ACL)

Tunnel Group

TCP or UDP Destination Port

RTP Range

IP DiffServ CodePoints (DSCP)

IP Precedence

Any traffic

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default all situation.

[≤ Back](#)

[Next >](#)

選擇Source and Destination as any with service as tcp-udp/http。按「Next」（下一步）。

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action:  Match  Do not match

Source: any

Destination: any

Service: tcp-udp/http

Description:

**More Options**

Enable Rule

Source Service:  (TCP or UDP service only)

Time Range:

[Back](#) | [Next >](#)

選中HTTP單選按鈕，然後按一下Configure。

## Add Service Policy Rule Wizard - Rule Action

Protocol Inspection | Connection Settings | QoS |

<input type="checkbox"/> CTIQBE	Configure...
<input type="checkbox"/> DCERPC	Configure...
<input type="checkbox"/> DNS	Configure...
<input type="checkbox"/> ESMTP	Configure...
<input type="checkbox"/> FTP	Configure...
<input type="checkbox"/> H.323 H.225	Configure...
<input type="checkbox"/> H.323 RAS	Configure...
<input checked="" type="checkbox"/> HTTP	Configure...
<input type="checkbox"/> ICMP	
<input type="checkbox"/> ICMP Error	
<input type="checkbox"/> ILS	
<input type="checkbox"/> IM	Configure...
<input type="checkbox"/> IPSec-Pass-Thru	Configure...
<input type="checkbox"/> MGCP	Configure...
<input type="checkbox"/> NETBIOS	Configure...
<input type="checkbox"/> PPTP	

≤ Back

Finish

Cancel

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



按一下「Finish」（結束）。

**Configuration > Firewall > Service Policy Rules**

Traffic Classification						
Name	#	Enabled	Match	Source	Destination	Service
Global; Policy: global_policy						
inspection_defau			Match	any	any	default
Interface: inside; Policy: inside-policy			Match	any	any	HTTP
httptraffic	1	<input checked="" type="checkbox"/>	Match	any	any	HTTP

埠8080流量再次選擇Add > Add Service Policy Rule。

## Configuration > Firewall > Service Policy Rules

The screenshot shows the Juniper Firewall configuration interface under the 'Service Policy Rules' section. A context menu is open over a specific rule, with the 'Add Service Policy Rule...' option highlighted and circled in red. The menu also includes 'Edit', 'Delete', 'Insert...', and 'Insert After...' options.

Traffic Classification		
Source	Destination	Service
any	any	default

Below the table, a row shows the rule details: Interface: inside; Policy: inside-policy. The rule number is 1, and it has a checked 'Match' checkbox. The source and destination are both set to 'any'. The service is listed as 'http' with a UDP port range of 1-1024.

按「Next」(下一步)。

### Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then add the new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: inside - inside-policy

Global - applies to all interfaces

Policy Name: inside-policy \*

Description:

Policy Name: global\_policy

Description:

\*Only one service policy is allowed. Existing service policy names cannot be changed.

< Back

Next >

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)。

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

Default Inspection Traffic

Source and Destination IP Address (uses ACL)

Tunnel Group

TCP or UDP Destination Port

RTP Range

IP DiffServ CodePoints (DSCP)

IP Precedence

Any traffic

Add rule to existing traffic class:

Rule can be added to an existing class map if that class map uses access control list (ACL) as its traffic match.

Use an existing traffic class:

Use class-default as the traffic class.

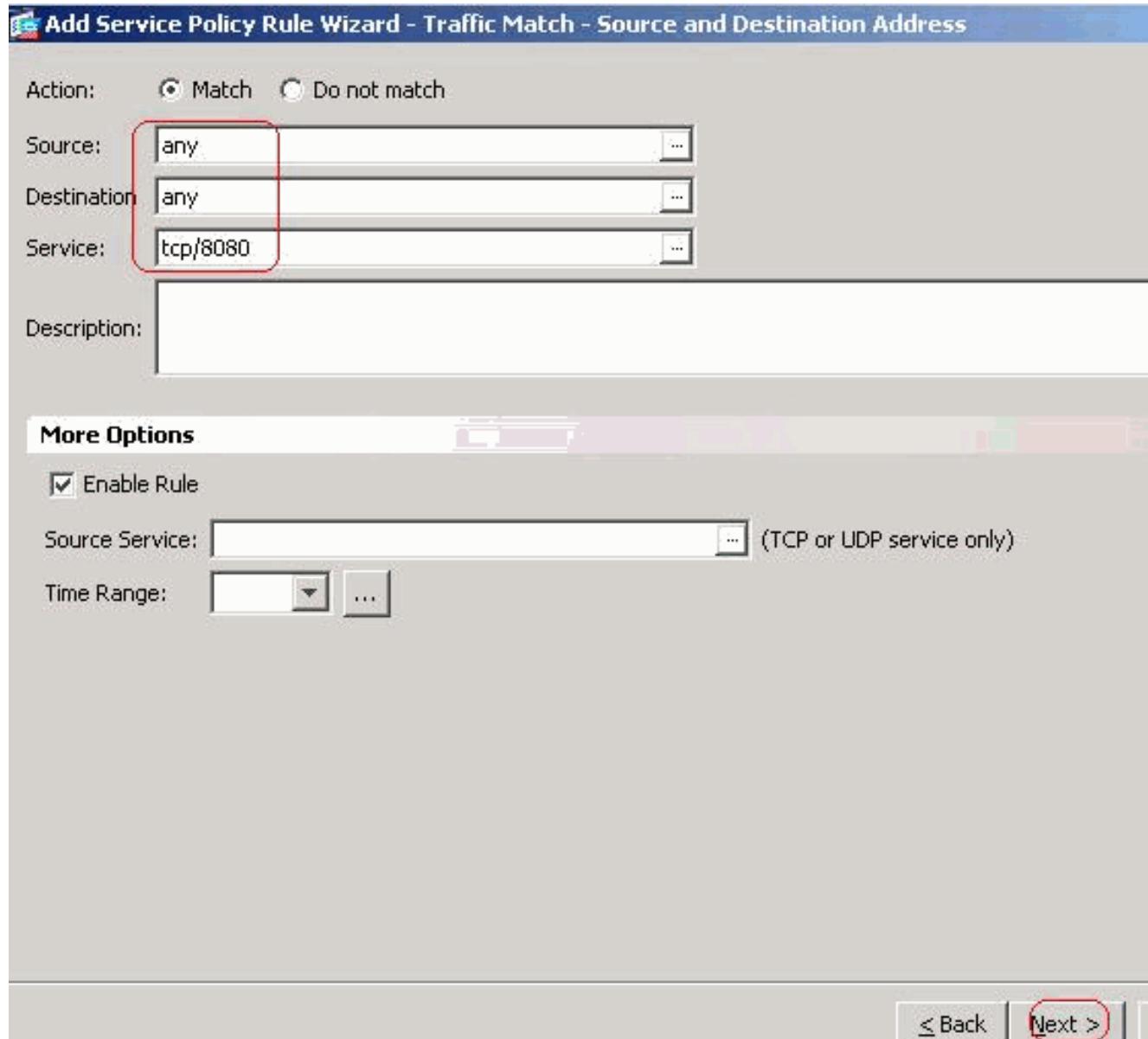
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default all situation.

[≤ Back](#)

[Next >](#)

使用tcp/8080將「Source (來源)」和「Destination (目標)」選擇為「」。按一下「Next」。

。

 Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action:  Match  Do not match

Source: any

Destination: any

Service: tcp/8080

Description:

**More Options**

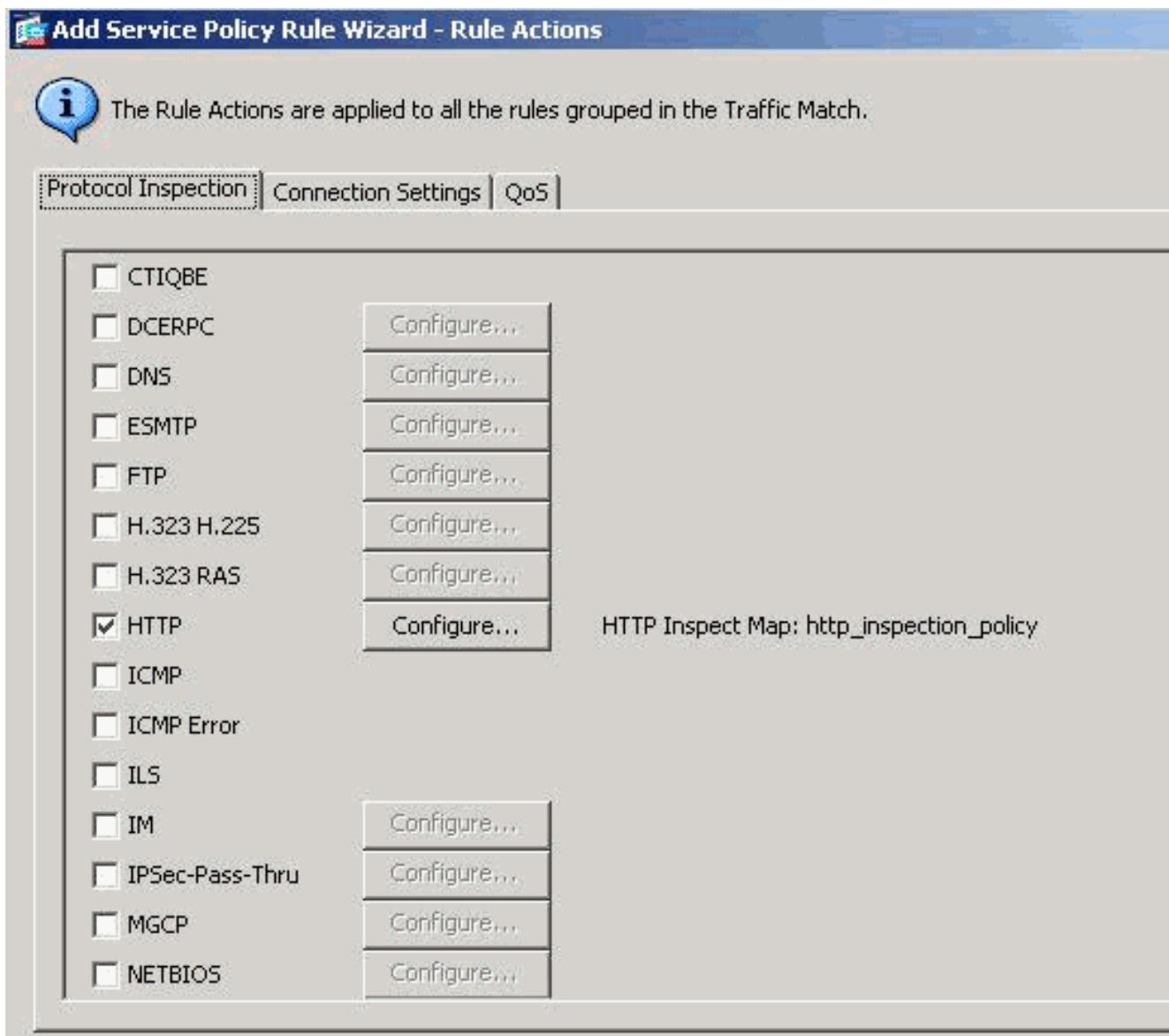
Enable Rule

Source Service:  (TCP or UDP service only)

Time Range:

[\*\*< Back\*\*](#) [\*\*Next >\*\*](#)

按一下「Finish」(結束)。



**Configuration > Firewall > Service Policy Rules**

Traffic Classification						
Name	#	Enabled	Match	Source	Destination	Service
<b>Global; Policy: global_policy</b>						
inspection_default			Match	any	any	default
<b>Interface: inside; Policy: inside-policy</b>						
httptraffic	1	<input checked="" type="checkbox"/>	Match	any	any	UDP http
	2	<input checked="" type="checkbox"/>	Match	any	any	TCP 8080

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|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

- [Cisco ASA 5500系列自適應安全裝置支援](#)
- [思科調適型安全裝置管理員\(ASDM\)支援](#)
- [Cisco PIX 500系列安全裝置支援](#)
- [Cisco PIX防火牆軟體](#)
- [Cisco Secure PIX防火牆命令參考](#)

- [安全產品現場通知 \( 包括PIX \)](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)