ASA/PIX 8.x:使用MPF的正規表示式允許/阻止FTP站點配置示例

目錄

簡介

本文檔介紹如何配置思科安全裝置ASA/PIX 8.x，該裝置使用帶有模組化策略框架(MPF)的正規表示式，以便按伺服器名稱阻止或允許某些FTP站點。

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

本文中的資訊係根據以下軟體和硬體版本：

- 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。

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. 確定要應用操作的第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. （僅限應用檢測。）為應用檢測流量定義特殊操作。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，也可以通過使用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(?)或製表符。**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。此外，**regex**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MPF配置用於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，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。

下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或前面表達式的任何數字。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**」在查詢匹配項時保留前導空格。
^	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	匹配回車符：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	匹配使用十六進位制的ASCII字元，該十六進位制恰好是兩位數。
\NNN	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。

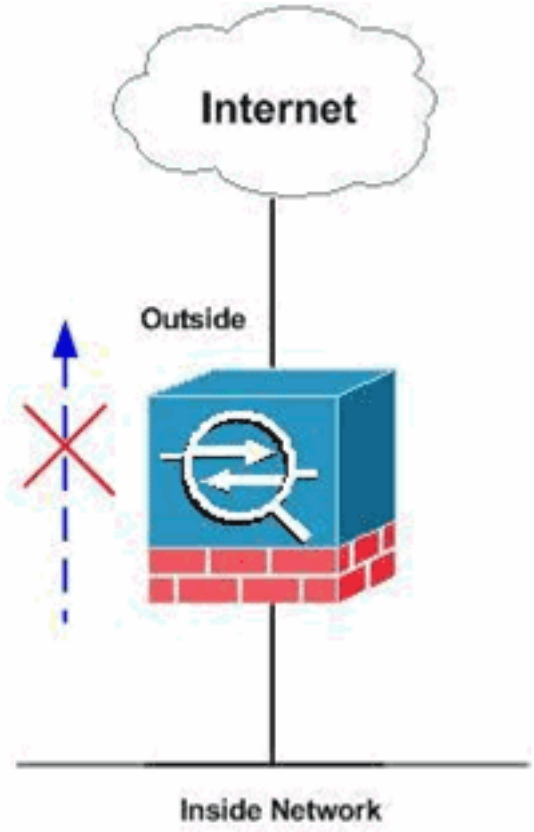
設定

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：



注意：使用正規表示式允許或阻止選定的FTP站點。

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

ASA CLI配置

```
ciscoasa#show run
: Saved
:
ASA Version 8.0(4)
!
hostname ciscoasa
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.66.79.86 255.255.255.224
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.238.26.129 255.255.255.248
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
!--- Write regular expression (regex) to match the FTP
site you want !--- to access. NOTE: The regular
expression written below must match !--- the response
220 received from the server. This can be different !---
than the URL entered into the browser. For example, !---
FTP Response: 220 g1u0103c.austin.hp.com


regex FTP_SITE1 "([0-9A-Za-z])*[Hh][Pp]\.[Cc][Oo][Mm]"
regex FTP_SITE2 "([0-9A-Za-z])* CISCO SYSTEMS ([0-9A-Za-
z])*"

!--- NOTE: The regular expression will be checked
against every line !--- in the Response 220 statement
(which means if the FTP server !--- responds with
multiple lines, the connection will be denied if !---
there is no match on any one line).


boot system disk0:/asa804-k8.bin
ftp mode passive
pager lines 24
logging enable
logging timestamp
logging buffered debugging
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-61557.bin
no asdm history enable
```

```
arp timeout 14400

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 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 sip-provisional-media 0:02:00 uauth 0:05:00
absolute
dynamic-access-policy-record DfltAccessPolicy

http server enable
http 0.0.0.0 0.0.0.0 inside
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart

telnet timeout 5
ssh scopy enable
ssh timeout 5
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept


class-map type regex match-any FTP_SITES
 match regex FTP_SITE1
 match regex FTP_SITE2

! Class map created in order to match the server names !
of FTP sites to be blocked by regex. class-map type
inspect ftp match-all FTP_class_map
 match not server regex class FTP_SITES

! Write an FTP inspect class map and match based on
server !--- names, user name, FTP commands, and so on.
Note that this !--- example allows the sites specified
with the regex command !--- since it uses the match not
command. If you need to block !--- specific FTP sites,
use the match command without the  not  option.


class-map inspection_default
 match default-inspection-traffic

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512

policy-map type inspect ftp FTP_INSPECT_POLICY
 parameters
 class FTP_class_map
  reset log
```

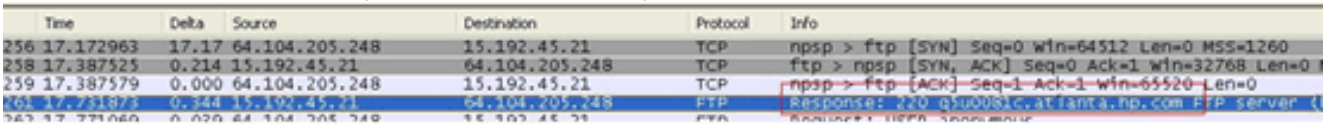
```
! Policy map created in order to define the actions !---
such as drop, reset, or log. policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect h323 h225 inspect h323 ras inspect netbios
inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip
inspect xdmcp inspect icmp inspect ftp strict
FTP_INSPECT_POLICY

!--- The FTP inspection is specified with strict option
!--- followed by the name of policy. service-policy
global_policy global prompt hostname context
Cryptochecksum:40cefb1189e8c9492ed7129c7577c477 : end
```

ASA配置8.x，帶ASDM 6.x

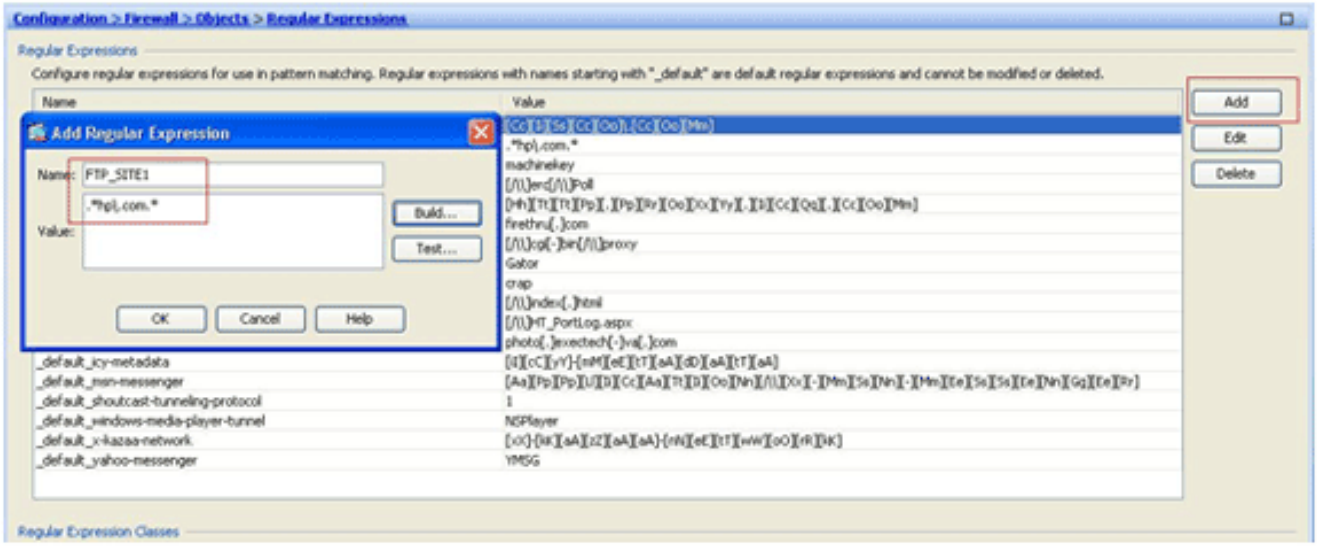
完成以下步驟，設定正規表示式，並將其套用到MPF，以阻擋特定的FTP站點：

1. **確定FTP伺服器名稱。**FTP檢查引擎可以使用不同的條件提供檢查，例如命令、檔名、檔案型別、伺服器和使用者名稱。此過程使用伺服器作為條件。FTP檢測引擎使用FTP站點傳送的伺服器220響應作為伺服器值。此值可以不同於站點使用的域名。此示例使用Wireshark捕獲到要檢查的站點的FTP資料包，以獲取響應220值，以便在步驟2中的正規表示式中使用。

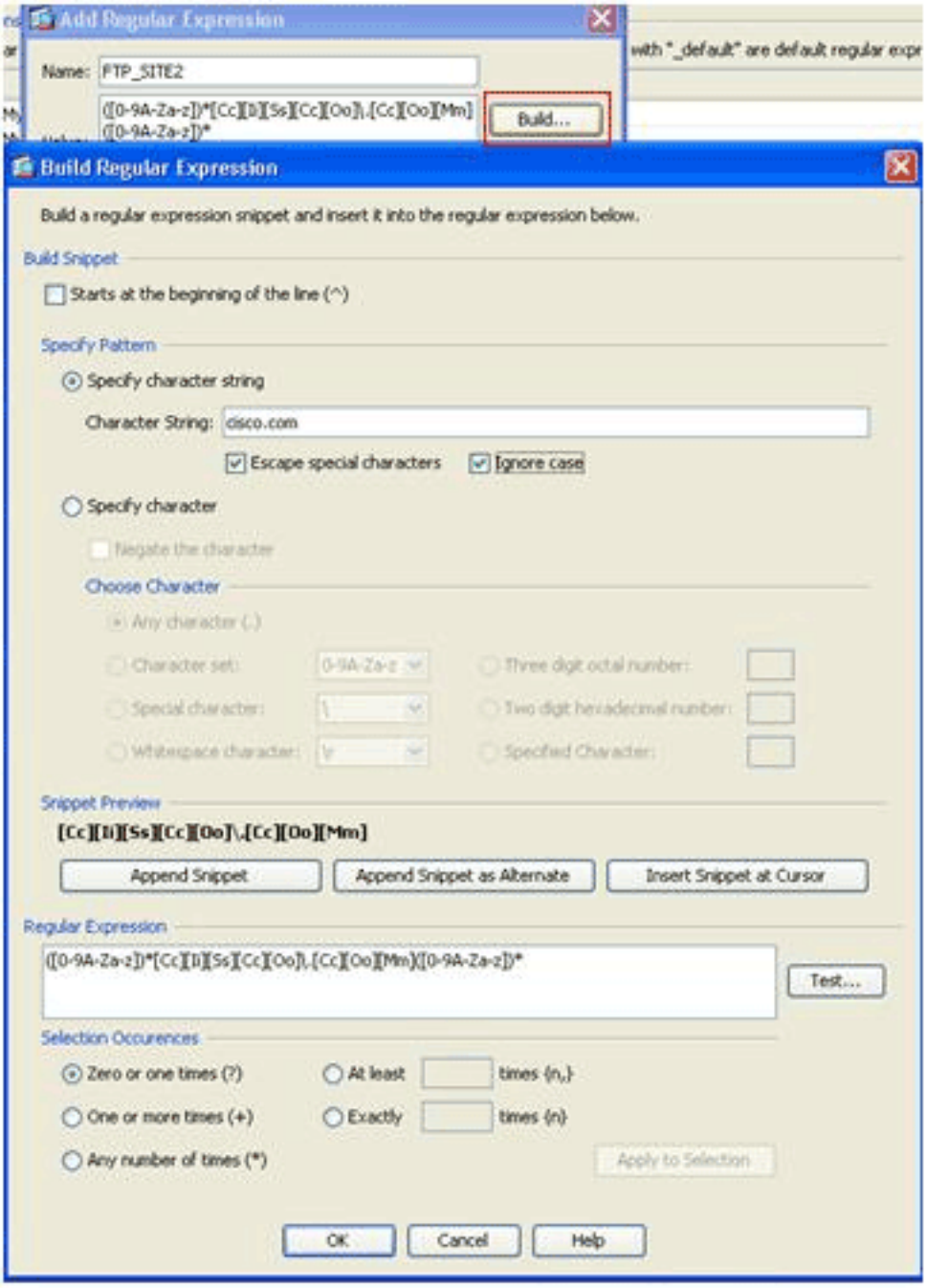


根據捕獲結果，ftp://hp.com的響應220值為（例如）*q5u0081c.atlanta.hp.com*。

2. **建立正規表示式。**選擇**Configuration > Firewall > Objects > Regular Expressions**，然後在「Regular Expression」頁籤下按一下**Add**，以建立正規表示式，如以下過程所述：建立正規表示式*FTP_SITE1*，以匹配從ftp站點接收的響應220（如「。* hp\.com.*」），然後按一下**OK**。

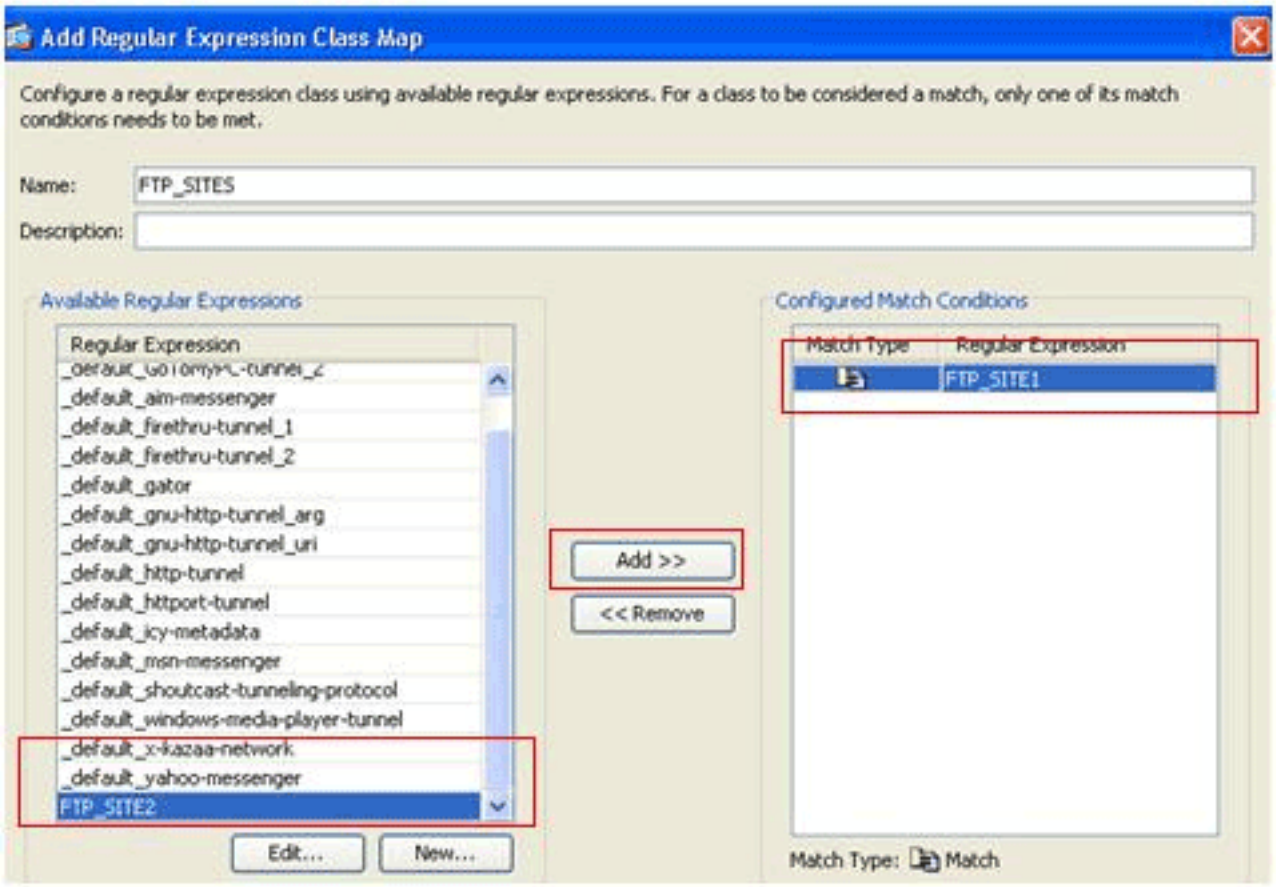


注意：可以按一下**生成**以獲得有關如何建立更高級正規表示式的幫助。

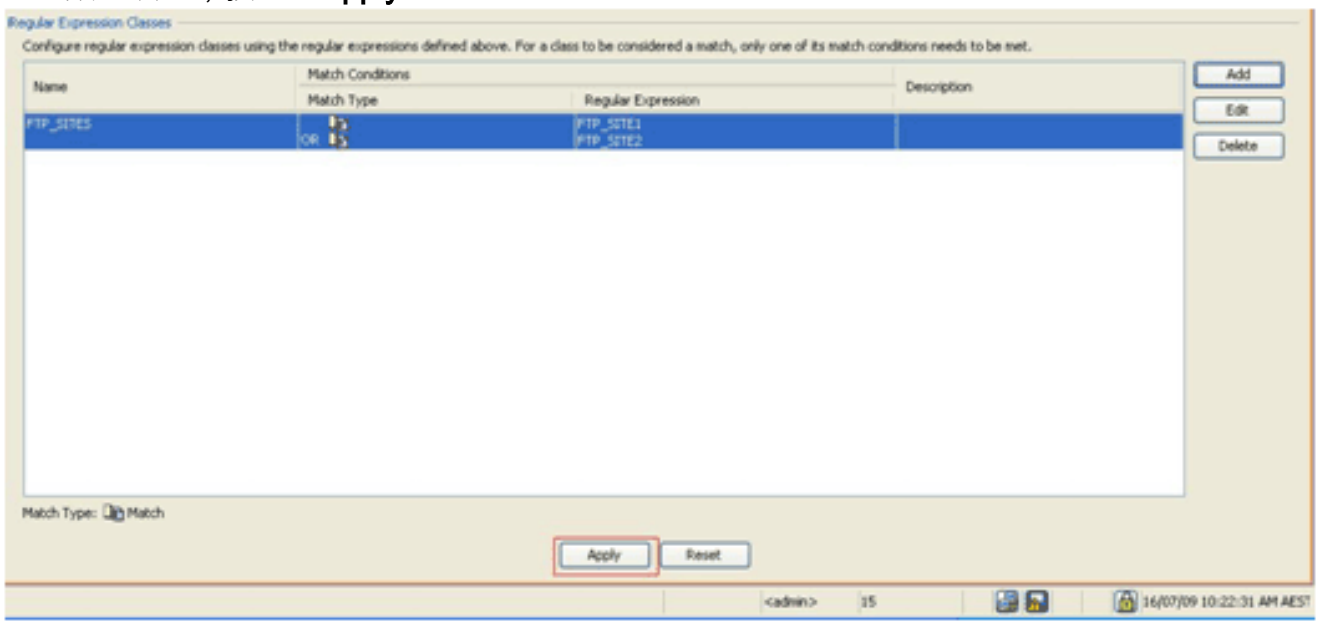


建立正規表示式後，按一下**Apply**。

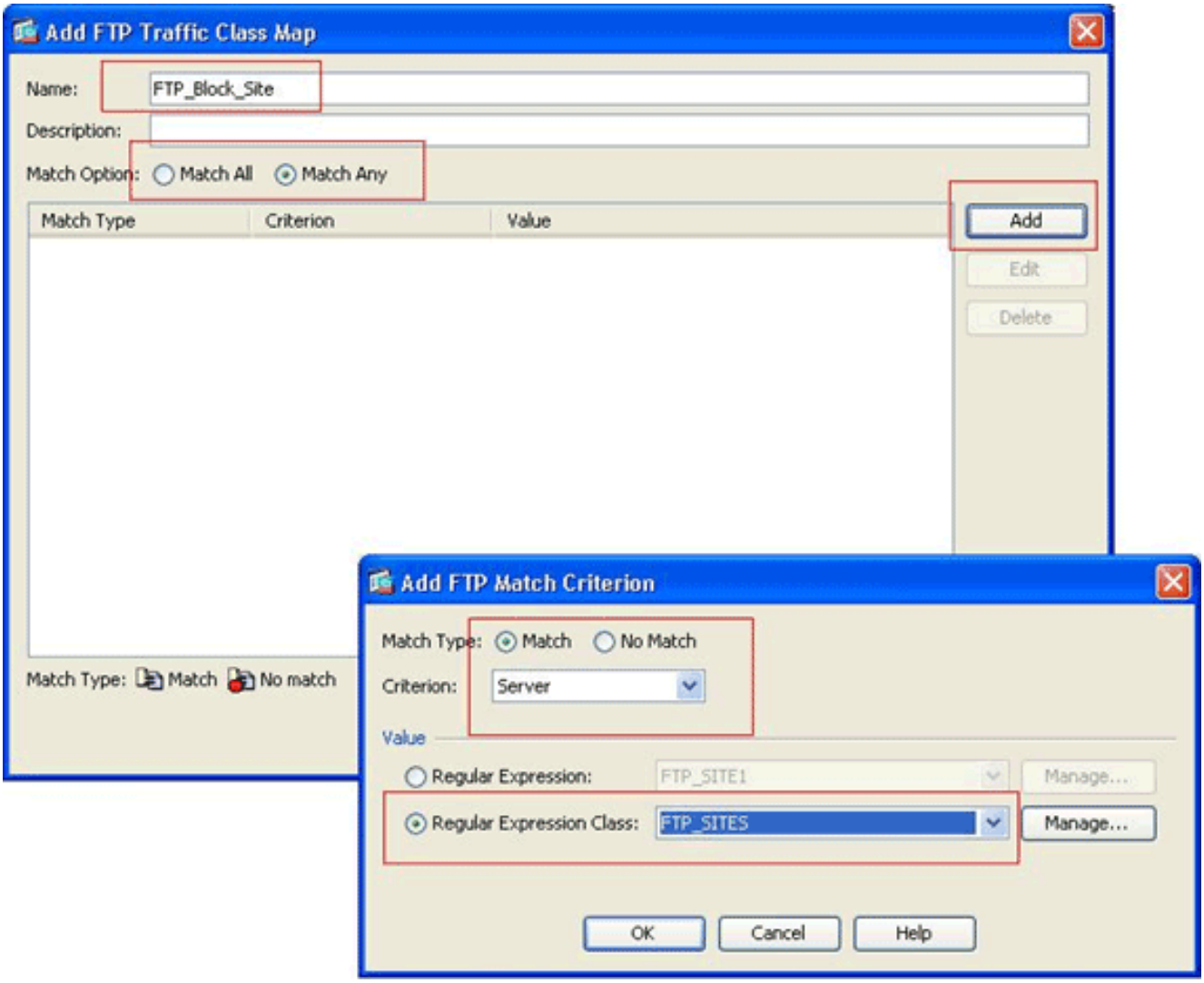
3. **建立正規表示式類。**選擇**Configuration > Firewall > Objects > Regular Expressions**，然後在Regular Expression Classes部分下按一下**Add**，以便按以下過程所述建立類：建立正規表示式類*FTP_SITES*，以匹配任意正規表示式*FTP_SITE1*和*FTP_SITE2*，然後按一下*OK*。



建立類對映後，按一下**Apply**。

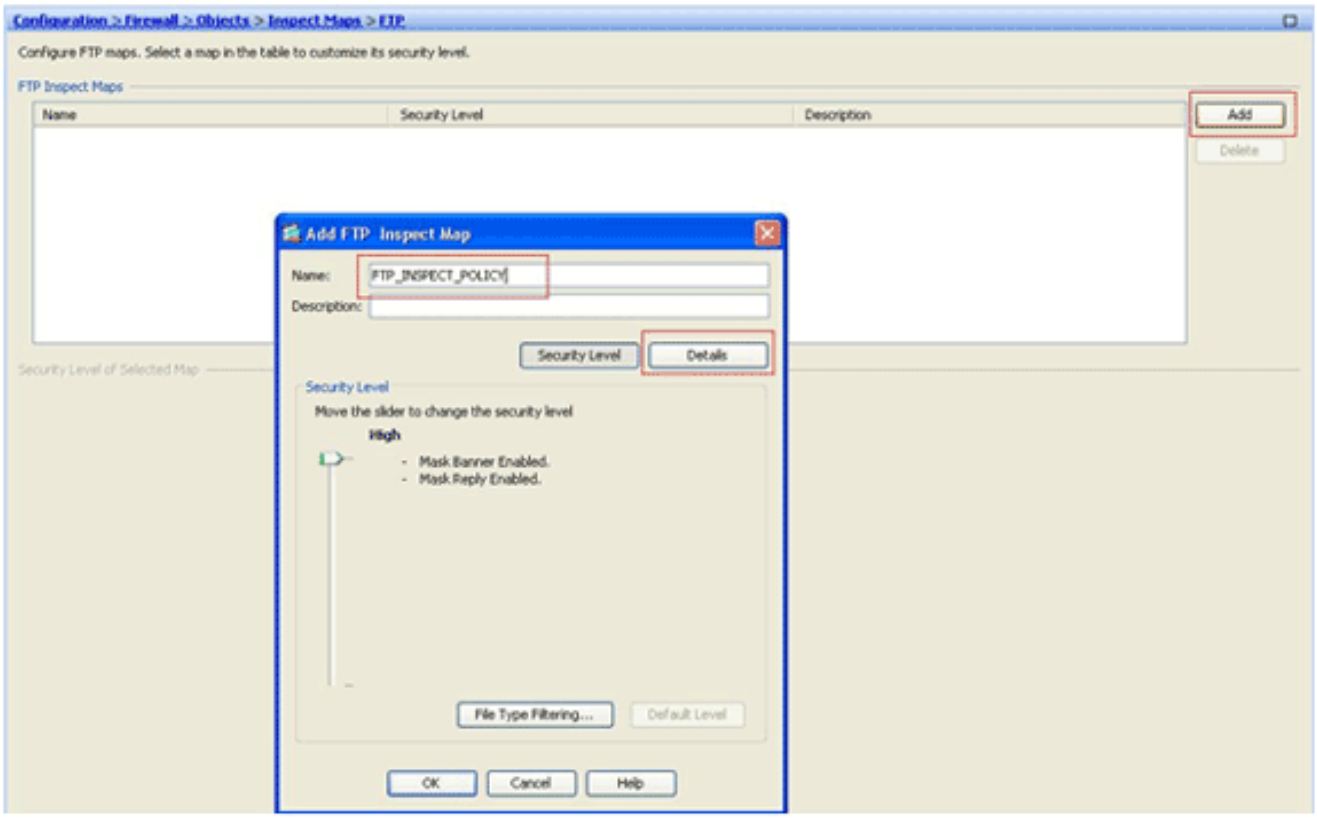


4. **使用類別對映檢查已識別的流量。**選擇**Configuration > Firewall > Objects > Class Maps > FTP > Add**，按一下右鍵，然後選擇**Add**以建立類對映來檢查由各種正規表示式標識的FTP流量，如以下過程所述：建立類對映*FTP_Block_Site*，以將FTP響應220與您建立的正規表示式匹配。

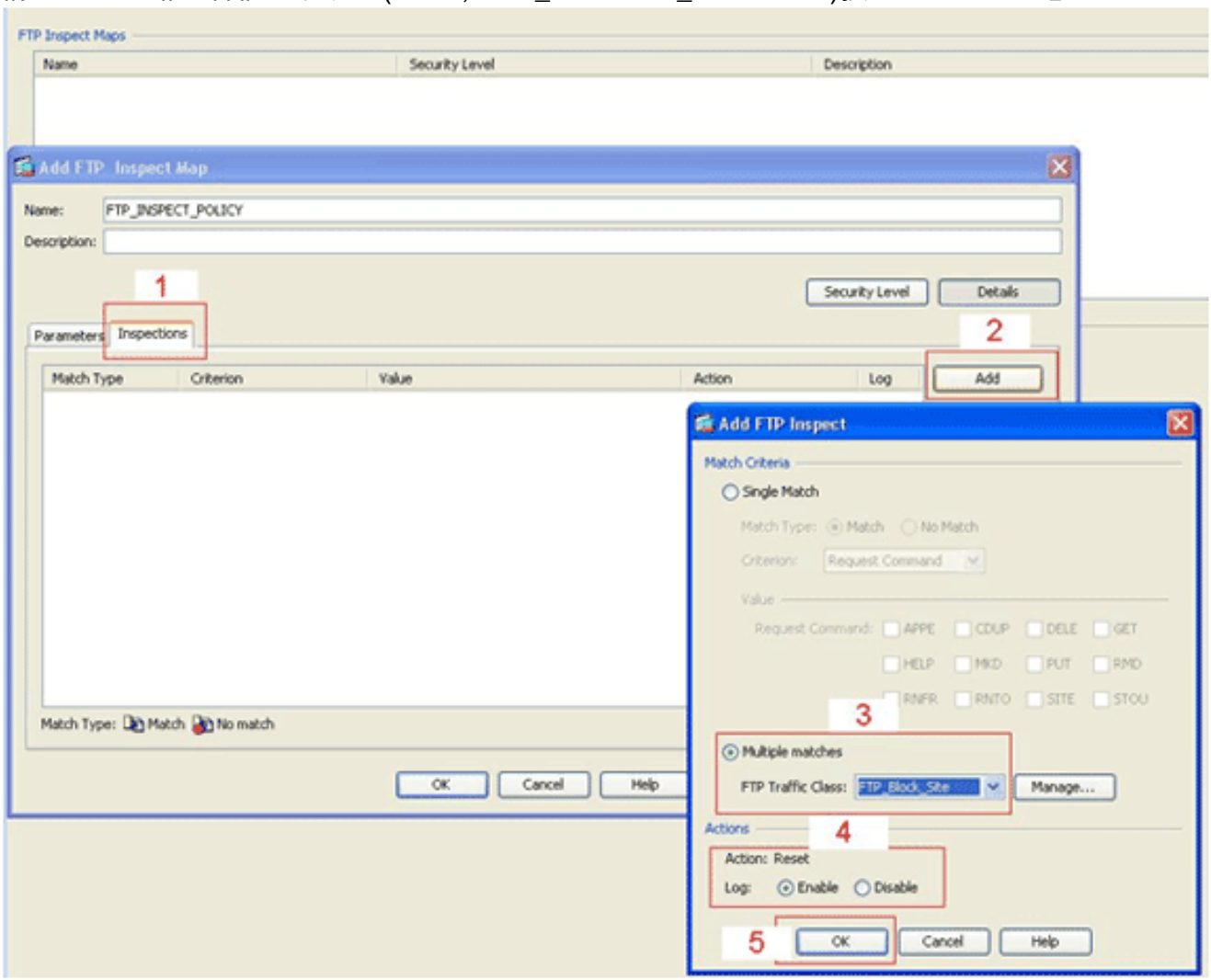


如果要排除正規表示式中指定的站點，請按一下**No Match**單選按鈕。在「值」部分中，選擇正規表示式或正規表示式類。對於此過程，請選擇之前建立的類。按一下「**Apply**」。

5. **為檢測策略中的匹配流量設定操作。**選擇**Configuration > Firewall > Objects > Inspect Maps > FTP> Add**以建立檢測策略，並根據需要為匹配的流量設定操作。



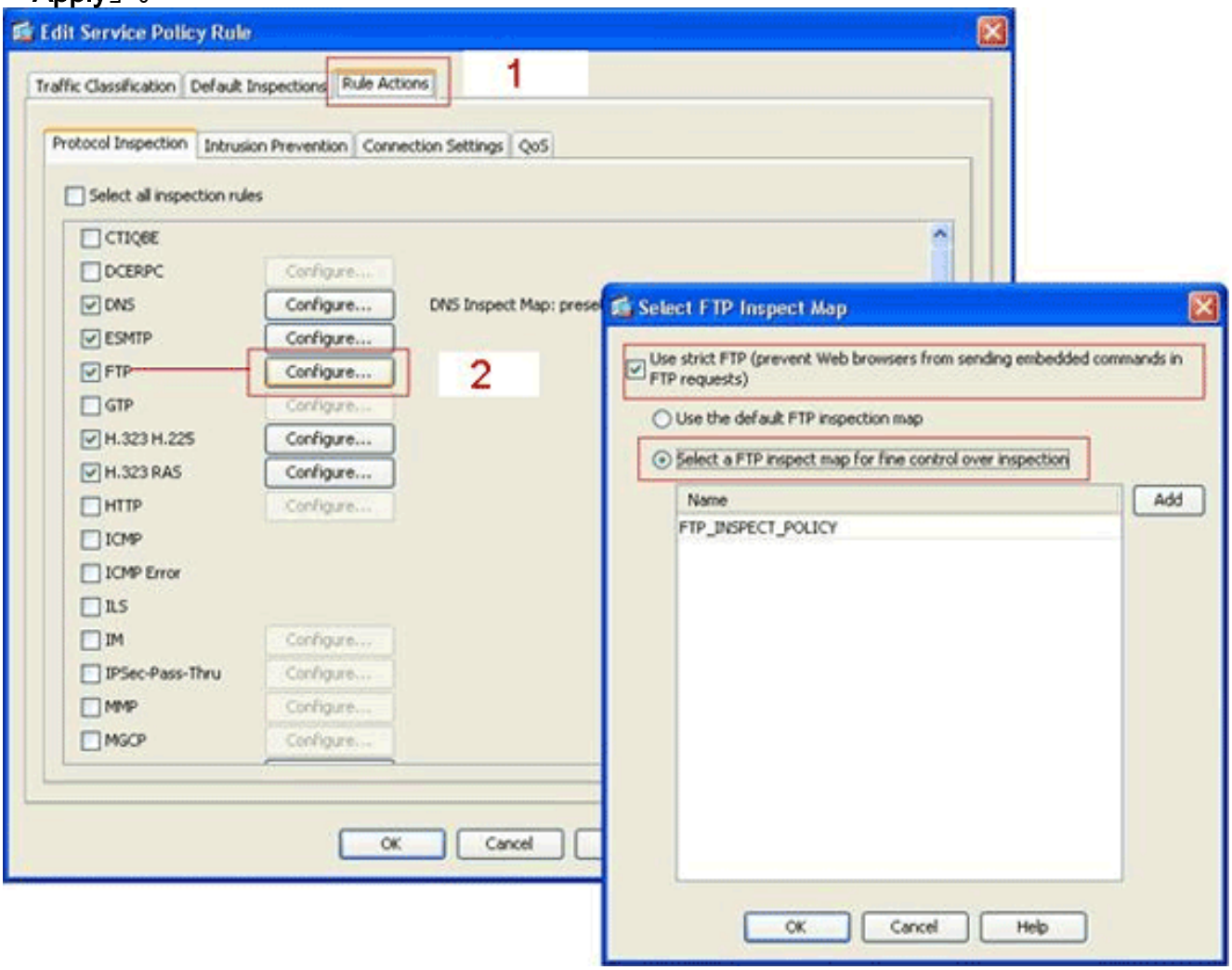
輸入檢查策略的名稱和說明。(例如，*FTP_INSPECT_POLICY*。)按一下「**Details**」。



按一下**Inspections**頁籤。(1)按一下「**Add**」。(2)按一下**Multiple matches**單選按鈕，然後從下拉選單中選擇流量類。(3)選擇要啟用或禁用的所需重置操作。此示例為與我們指定站點不匹配

的所有FTP站*點啟用*FTP連線重置。(4)按一下「**OK**」，再次按一下「**OK**」，然後按一下「**Apply**」。(5)

6. **將檢測FTP策略應用於全域性檢測清單。**選擇**Configuration > Firewall > Service Policy Rules**。在右側，選擇**inspection_default**策略，然後按一下**Edit**。在「Rule Actions」頁籤(1)下，按一下FTP的**Configure**按鈕。(2)在「選擇FTP檢查對映」對話方塊中，選中**Use strict FTP**覈取方塊，然後按一下**FTP檢查對映以精細控制檢查**單選按鈕。新的FTP檢測策略*FTP_INSPECT_POLICY*應顯示在清單中。按一下「**OK**」，再次按一下「**OK**」，然後按一下「**Apply**」。



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-configregex
regex FTP_SITE1 "[Cc][Ii][Ss][Cc][Oo]\.[Cc][Oo][Mm]"
regex FTP_SITE2 ".*hp\.com.*"
```

- **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 FTP_SITES
 match regex FTP_SITE1
 match regex FTP_SITE2
```

```
class-map type inspect ftp match-all FTP_Block_Site
 match not server regex class FTP_SITES
class-map inspection_default
 match default-inspection-traffic
!
```

- **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 ftp
!
policy-map type inspect ftp FTP_INSPECT_POLICY
 parameters
  mask-banner
  mask-syst-reply
 class FTP_Block_Site
  reset log
 !
```

- **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 ftp FTP_INSPECT_POLICY
 parameters
  mask-banner
  mask-syst-reply
 class FTP_Block_Site
  reset log
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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
  inspect ftp strict FTP_INSPECT_POLICY
!
```

- **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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

您可以使用**show service-policy**命令驗證檢查引擎是否檢查流量並正確允許或丟棄流量。

```
ciscoasa#show service-policy

Global policy:
```

```
Service-policy: global_policy
  Class-map: inspection_default
    Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
    Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0
    Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0
    Inspect: netbios, packet 0, drop 0, reset-drop 0
    Inspect: rsh, packet 0, drop 0, reset-drop 0
    Inspect: rtsp, packet 0, drop 0, reset-drop 0
    Inspect: skinny , packet 0, drop 0, reset-drop 0
    Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0
    Inspect: sqlnet, packet 0, drop 0, reset-drop 0
    Inspect: sunrpc, packet 0, drop 0, reset-drop 0
    Inspect: tftp, packet 0, drop 0, reset-drop 0
    Inspect: sip , packet 0, drop 0, reset-drop 0
    Inspect: xdmcp, packet 0, drop 0, reset-drop 0
    Inspect: ftp strict FTP_INSPECT_POLICY, packet 40, drop 0, reset-drop 2
```

相關資訊

- ASA/PIX 8.x:使用正規表示式和MPF配置示例阻止某些網站(URL)
- PIX/ASA 7.x及更高版本：使用MPF配置示例阻止對等(P2P)和即時消息(IM)流量
- PIX/ASA 7.x:啟用FTP/TFTP服務配置示例
- 應用應用層協定檢查
- Cisco ASA 5500系列調適型安全裝置 — 支援
- 思科調適型安全裝置管理員(ASDM)
- Cisco PIX 500系列安全裝置 — 支援
- Cisco PIX防火牆軟體 — 支援
- Cisco PIX防火牆軟體命令參考