ASA/PIX 8.x：允许/阻拦FTP站点使用有MPF的常规表达配置示例

Contents

Introduction

本文档描述了如何配置 Cisco 安全设备 ASA/PIX 8.x，以便通过模块化策略框架 (MPF)，使用正则表达式按服务器名称阻止或允许某些 FTP 站点。

Prerequisites

Requirements

本文假设，配置Cisco安全设备并且适当地运作。

Components Used

本文档中的信息基于以下软件和硬件版本：

- 及以后的Cisco ASA 5500系列自适应安全设备(ASA)该运行软件版本8.0(x)
- ASA的8.x Cisco Adaptive Security Device Manager (ASDM)版本6.x

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is

live, make sure that you understand the potential impact of any command.

Conventions

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提供一个一致和灵活的方式配置安全工具功能。例如，您能使用MPF创建是特定的对特定TCP应用程序的超时配置，与适用于所有TCP应用程序的一个相对。

MPF支持这些功能：

- TCP标准化， TCP和UDP连接限额和超时和TCP序列号随机化
- CSC
- 应用检查
- IPS
- QoS输入策略
- QoS输出策略
- QoS优先级队列

MPF的配置包括四项任务：

1. 识别您要适用动作的第3层和Layer4数据流。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. (仅应用检查。)定义应用检查数据流的特殊动作。有关详细信息，请参阅配置特殊的应用程序检查操作。
3. 适用动作于第3层和Layer4数据流。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. 激活对接口的动作。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。

常规表示

常规表示字面上匹配文本字符串作为一个确切的字符串或使用元字符，因此您能匹配文本字符串的多个变形。您能使用常规表示匹配某一应用数据流内容。例如，您可以匹配 HTTP 数据包中的 URL 字符串。

Note: 请使用**Ctrl+V**为了退出所有在CLI的特殊字符，例如问号(？)或选项。例如，键入 **d[Ctrl+V]g** 以便在配置中输入 d?**g**。

为了创建常规表示，请使用**REGEX**命令。另外， **REGEX**命令可以用于要求文本匹配的多种功能。例如，您能用使用一检查策略映射的使用MPF配置应用检查的特殊动作。请参见**策略映射类型inspect命令**欲知更多信息。

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。使用常规表示，一些**匹配**命令让您识别在信息包的文本。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。有关详细信息，请参阅 class-map type regex 命令。

下表列出了有特殊含义的元字符。

字符	说明	备注
. 。	小点	与任意单个字符相匹配。例如， **d.g匹配**狗、dag、dtg和包含那些字符的所有词，例如doggonnit。
(exp)	Subexpression	subexpression从周围的字符分离字符，因此您能使用在subexpression的其他元字符。例如，**d(o|a)g** 匹配 dog 和 dag，而**|ag** 匹配 do 和 ag。subexpression可能也与重复量词一起使用区分为重复意味着的字符。例如，**ab(xy){3}z** 匹配 abxyxyxyz。
|	叠更	匹配分离的任一个表达式。例如，**dog|cat** 匹配 dog 或 cat。
??	问号	表明的量词有0或1先前的表达式。例如，**lo?se** 匹配 lse 或 lose。 **Note:** 您必须输入**Ctrl+V**然后问号或者帮助功能被调用。
**	星号	表明的量词有0， 1，或者任何数量的先前的表达式。例如，**lo*se** 匹配 lse、lose、loose 等。
{x}	重复量词	正确地重复x时间。例如，**ab(xy){3}z** 匹配 abxyxyxyz。
{x,}	最低的重复量词	重复至少x时间。例如，**ab(xy){2,}z** 匹配 abxyxyz、abxyxyxyz 等。
[abc]	字符类别	匹配在托架的所有字符。例如， **[abc]**匹配a、b或者c。
[^abc]	否定的字符类别	匹配在托架内没有包含的单个字符。例如，除a之外， **[^abc]**匹配所有字符， b，或者c. **[^A-Z]**匹配不是大写字母的任何单个字符。
[a-c]	字符范围组	匹配在范围的所有字符。**[a-z]**匹配所有小写字母。您能混合字符和范围：**[abcq-z]**匹配a， b， c， q， r， s， t， u， v， w， x， y， z，和，因此执行**[a-cq-z]**。只有当它是为时或第一个字符在托架内，破折号(-)字符是字面值的：**[abc-]**或**[-abc]**。
""	引号	落后或导致在字符串的蜜饯空间。例如，当寻找匹配时， “**测试**”保留主导的空间。
^	脱字号	指定线路的初期。
\\	换码字符	当使用与元字符，匹配一个字面值字符。例如， **\ [**匹配左方括号。
字符	字符	当字符不是元字符时，匹配字面值字符。
\r	回车	匹配回车：0x0d.
\	换行符	匹配一新的一行：0x0a.

n		
\ t	选项	匹配一个选项：0x09.
\ f	换页	匹配换页：0x0c.
\ x N N	退出的十六进制数字	匹配使用一十六进制正确地是两个位的一个ASCII字符。
\ N N N	退出的八进制数	以八进制数字匹配 ASCII 字符（必须是三位）。例如，字符040表示空间。

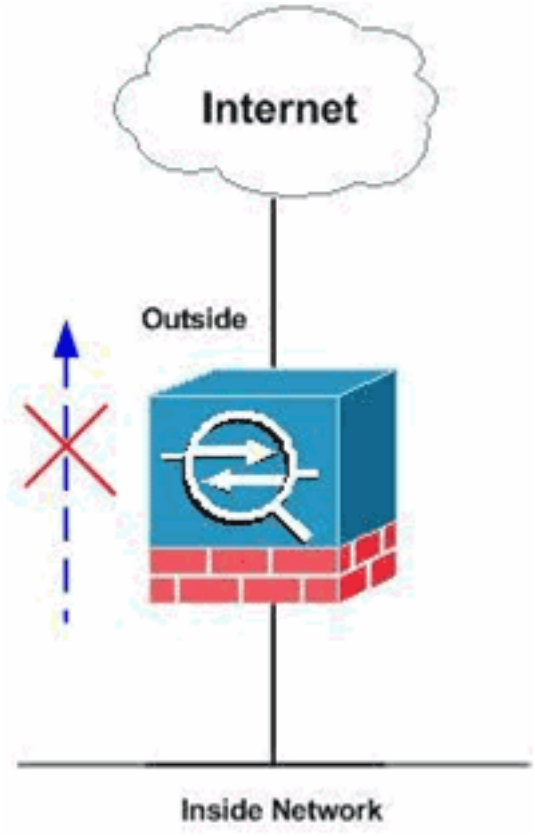
Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 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。

Network Diagram

本文档使用以下网络设置：



Note: 使用常规表示，所选的FTP站点允许或被阻拦。

配置

本文档使用以下配置：

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
```

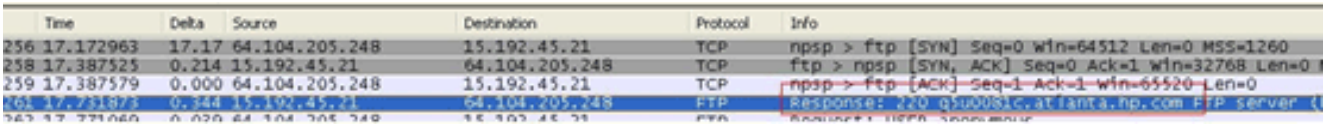
```
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-61557.bin
no asdm history enable
arp timeout 14400

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 与 ASDM 6.x

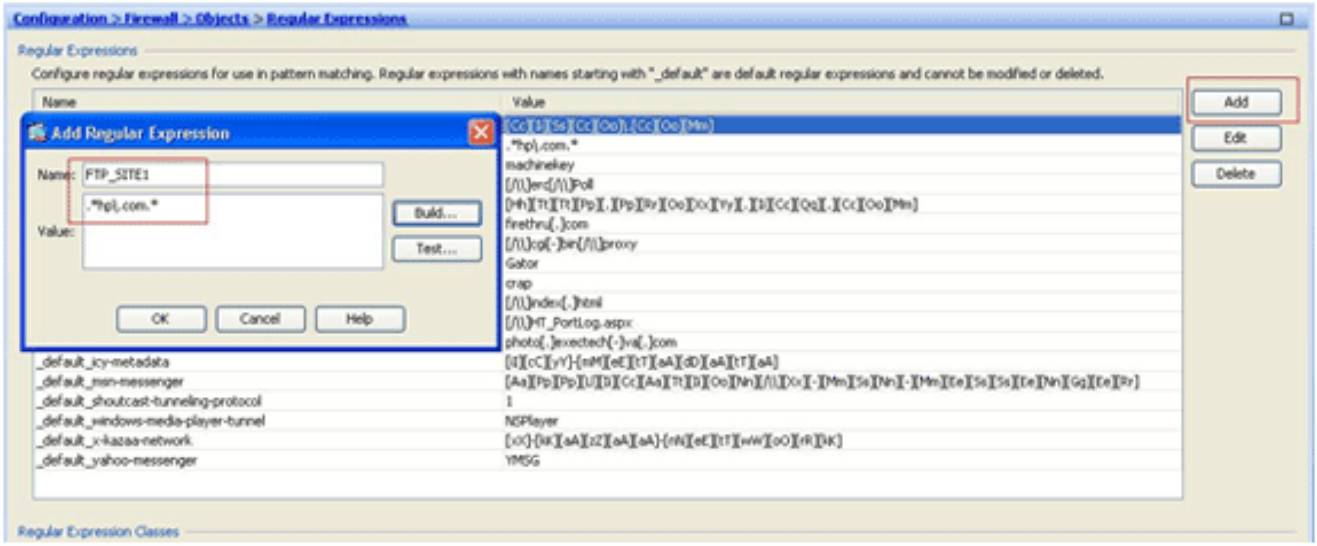
完成这些步骤为了配置常规表示和适用他们于MPF为了阻拦特定FTP站点：

1. **确定FTP服务器名字。**使用另外标准，例如命令、文件名、文件类型、服务器和用户名，FTP检测引擎能提供检查。此程序使用服务器作为标准。FTP检测引擎使用文件传送规约地点发送的服务器220回应作为服务器值。此值跟站点使用的域名可以不同。此示例使用Wireshark获取FTP信息包到检查为了获得回应220值用于我们的在第2.步的常规表示的站点。

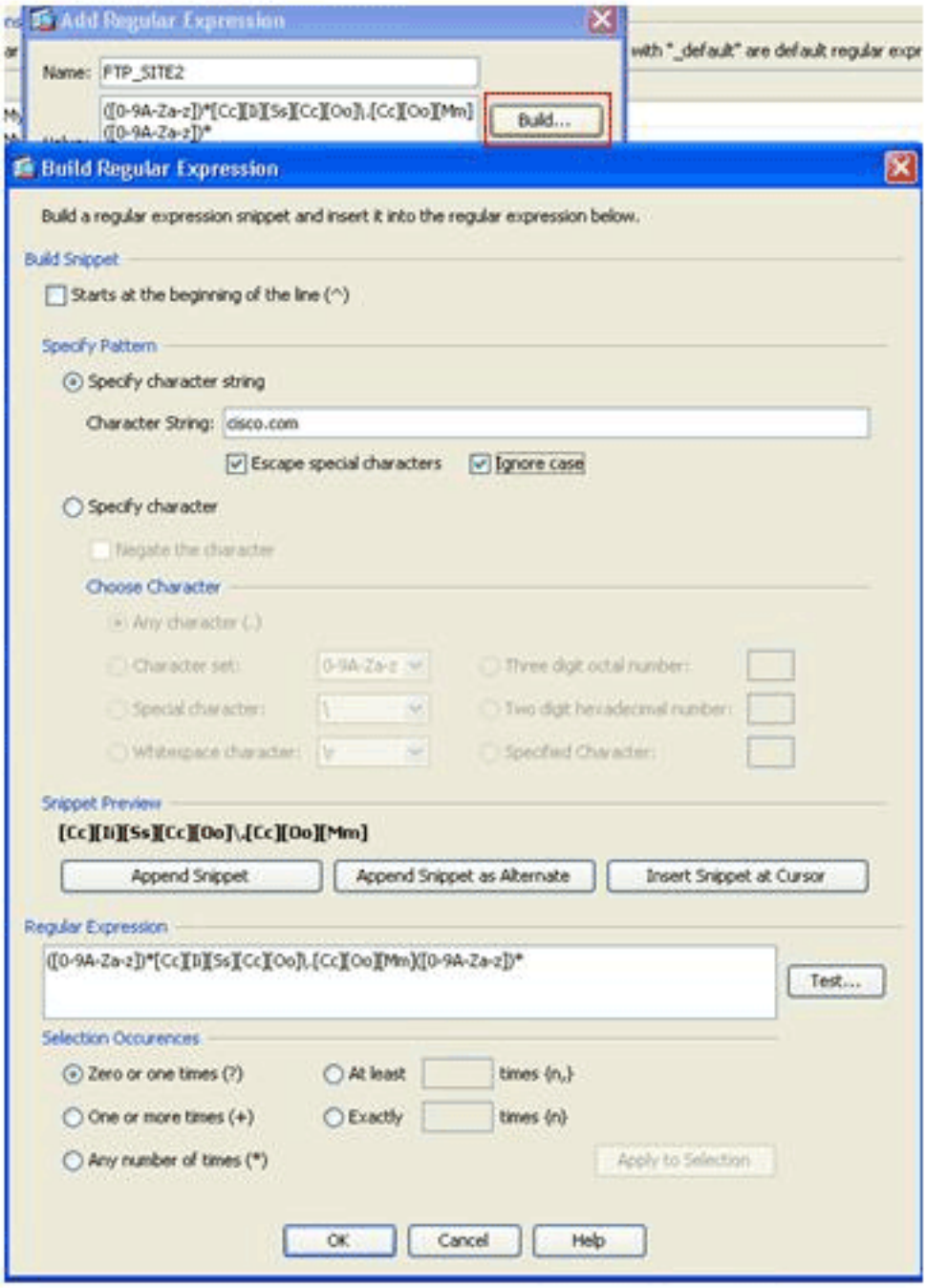


基于捕获ftp://hp.com的回应220值是(例如) *q5u0081c.atlanta.hp.com*。

2. **创建常规表示。**选择**Configuration>防火墙>对象>常规表示**，并且点击**添加**在常规表示选项下为了创建常规表示正如此程序所描述：创建常规表示， *FTP_SITE1*，为了匹配从文件传送规约地点220 (如在Wireshark或其他工具的信息包获取中看到使用)收到的答复(例如，“。* HP \ .com.*")，和点击OK键。

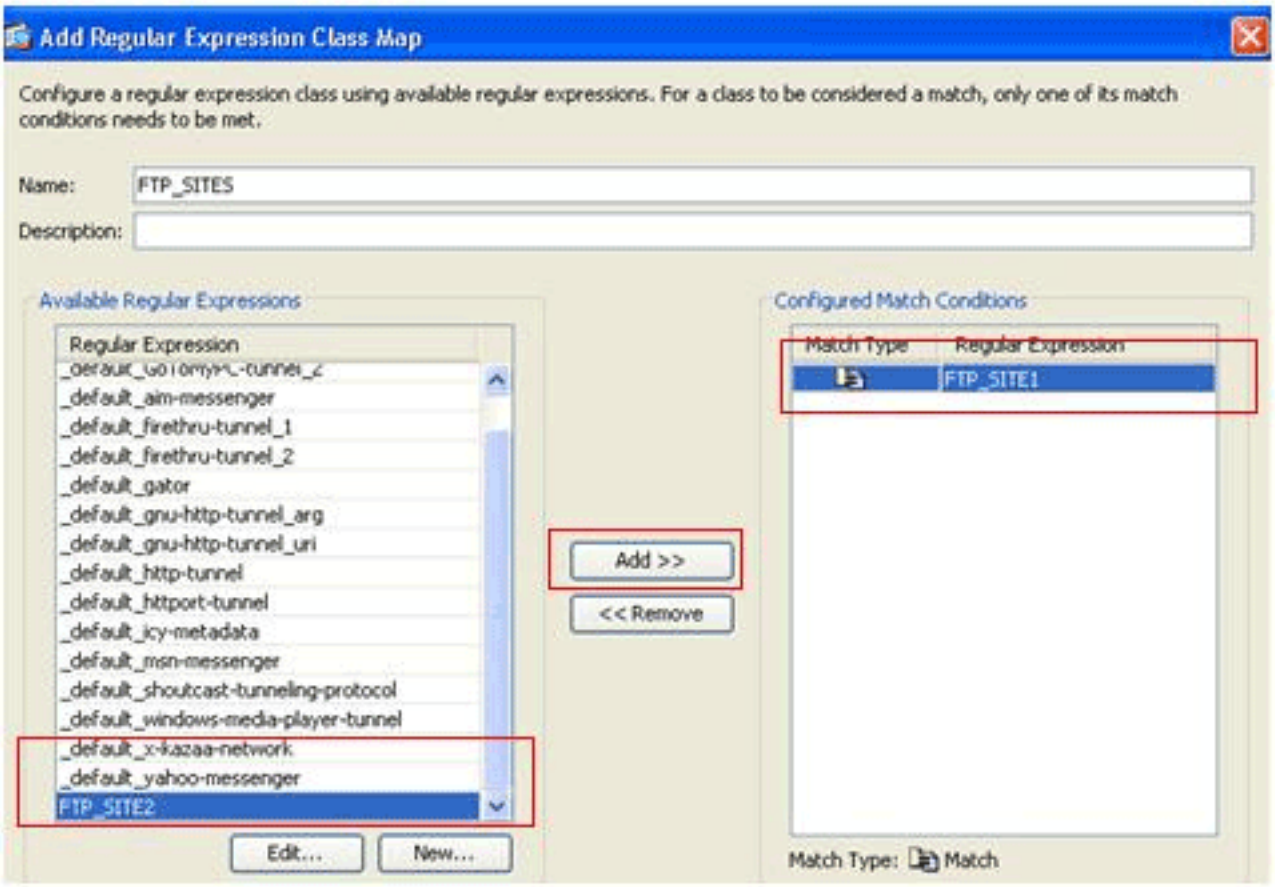


Note: 您能点击帮助的**修造**关于怎样创建更加先进的常规表示。

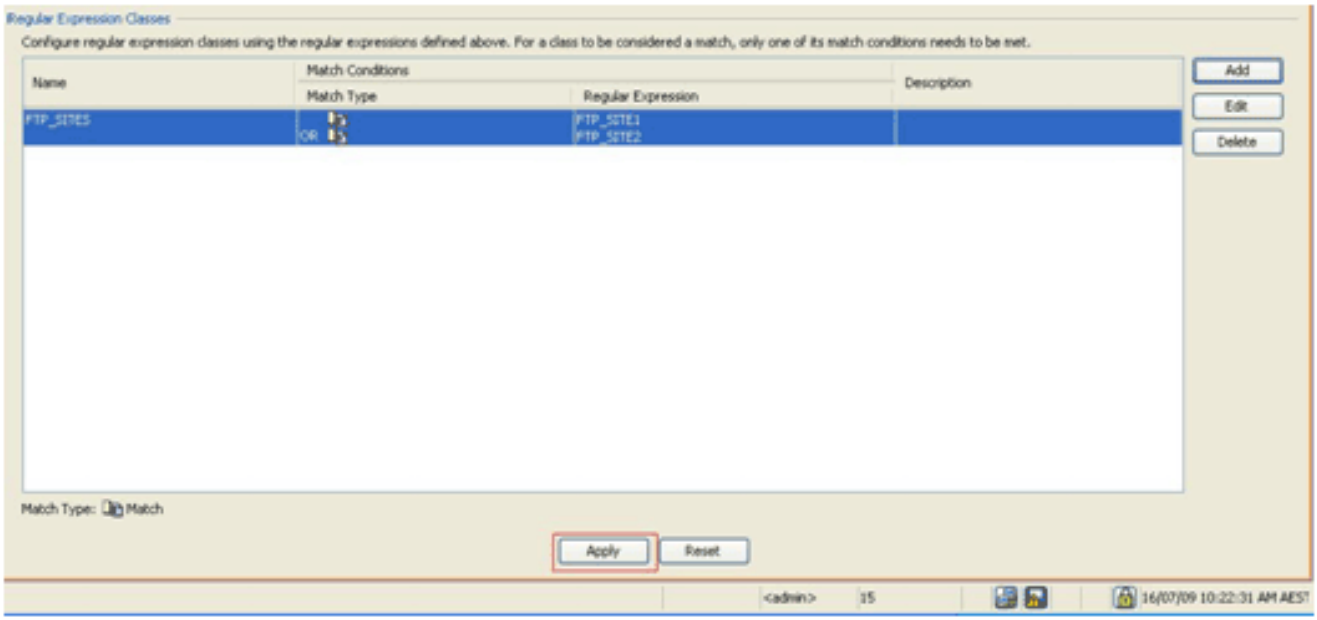


一旦常规表示被创建，请点击**适用。**

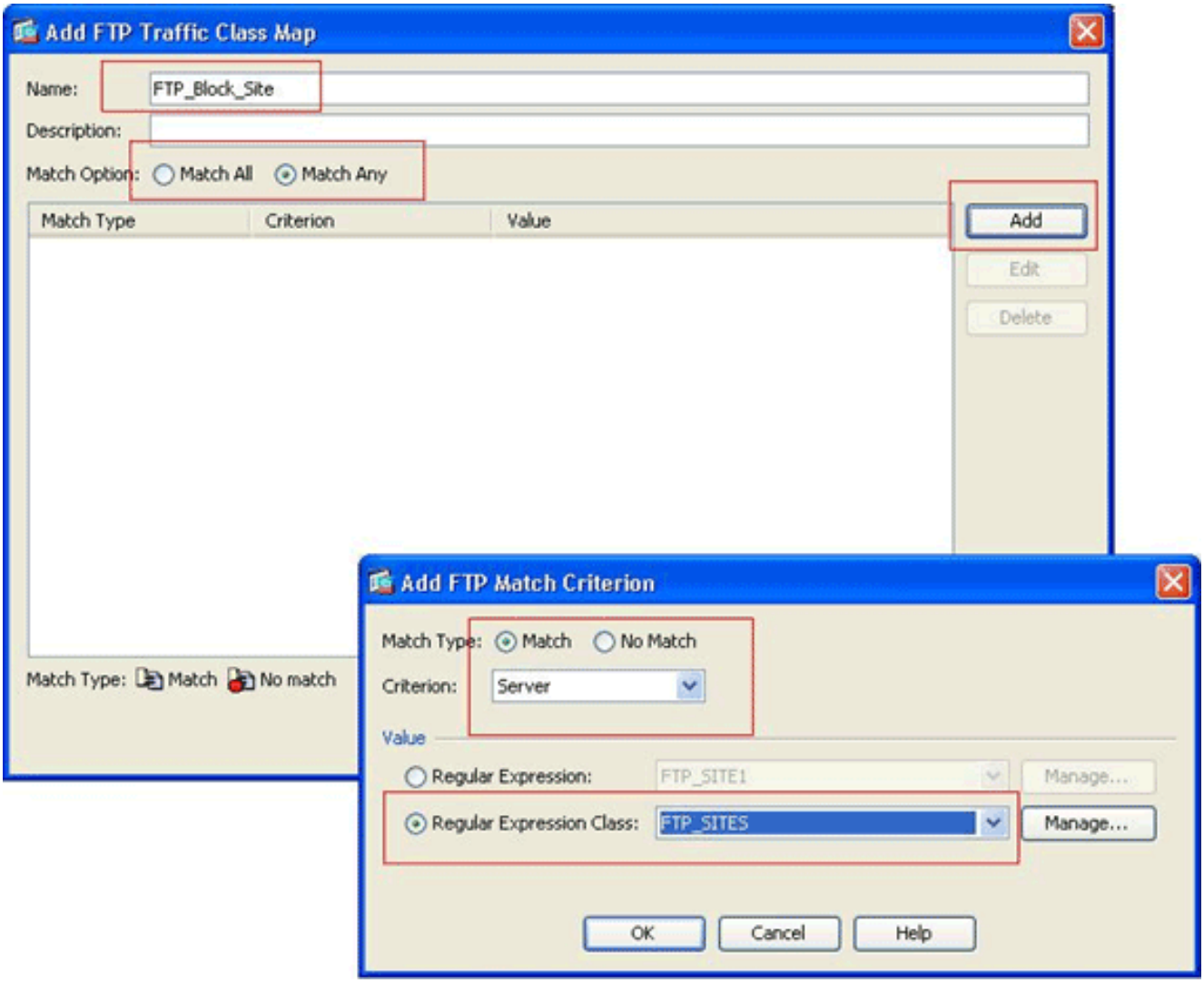
3. **创建常规表示组。**选择**Configuration>防火墙>对象>常规表示**，并且点击**添加**在常规表示组部分下为了创建组正如此程序所描述：创建一个常规表示组， *FTP_SITES*，为了匹配其中任一常规表示*FTP_SITE1*和*FTP_SITE2*，并且点击OK键。



一旦类映射被创建，请点击**适用**。

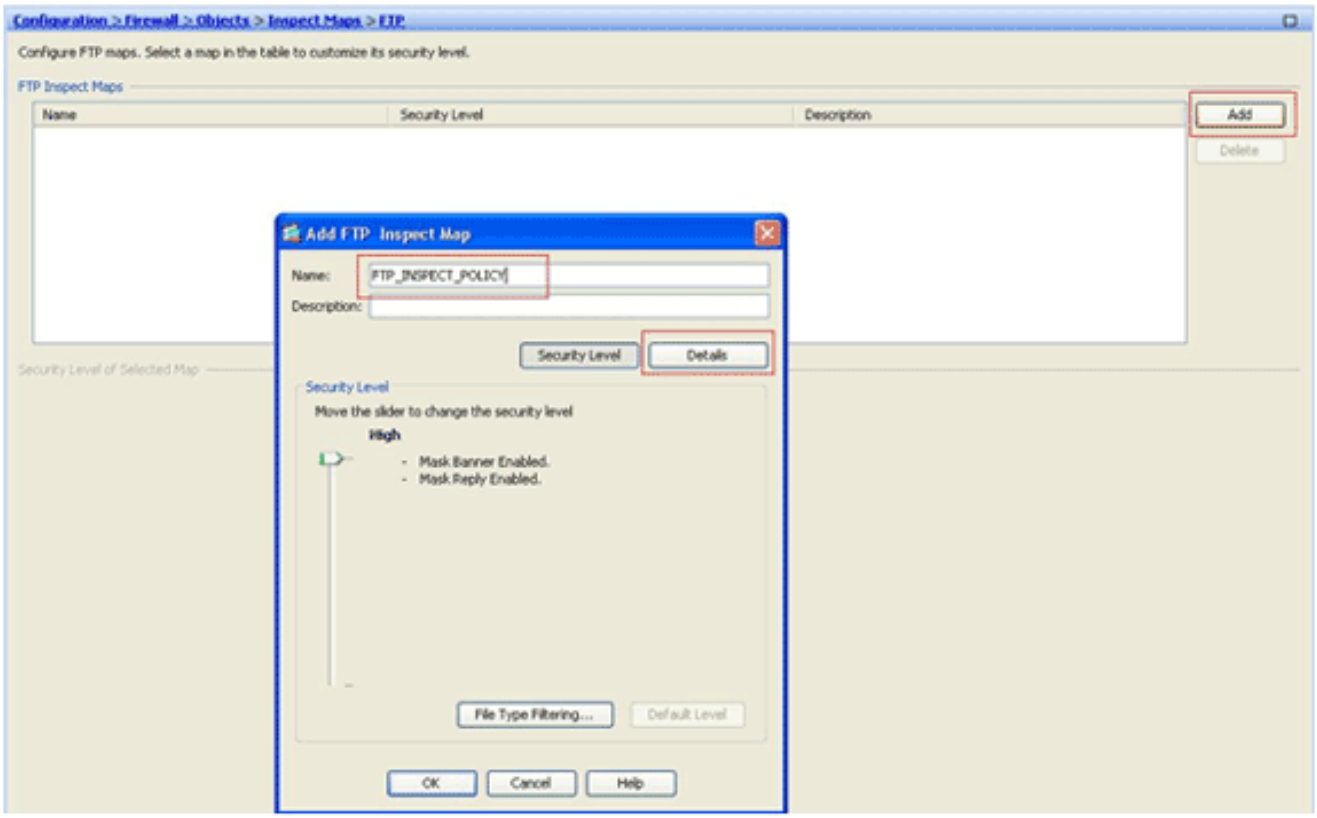


4. **检查与类映射的被识别的数据流。**选择**Configuration>防火墙>对象>类映射> FTP>添加**，用鼠标右键单击，并且选择**添加**为了创建类映射检查多种常规表示确定的FTP数据流正如此程序所描述：创建一个类映射， *FTP_Block_Site*，为了匹配FTP回应220以您创建的常规表示。

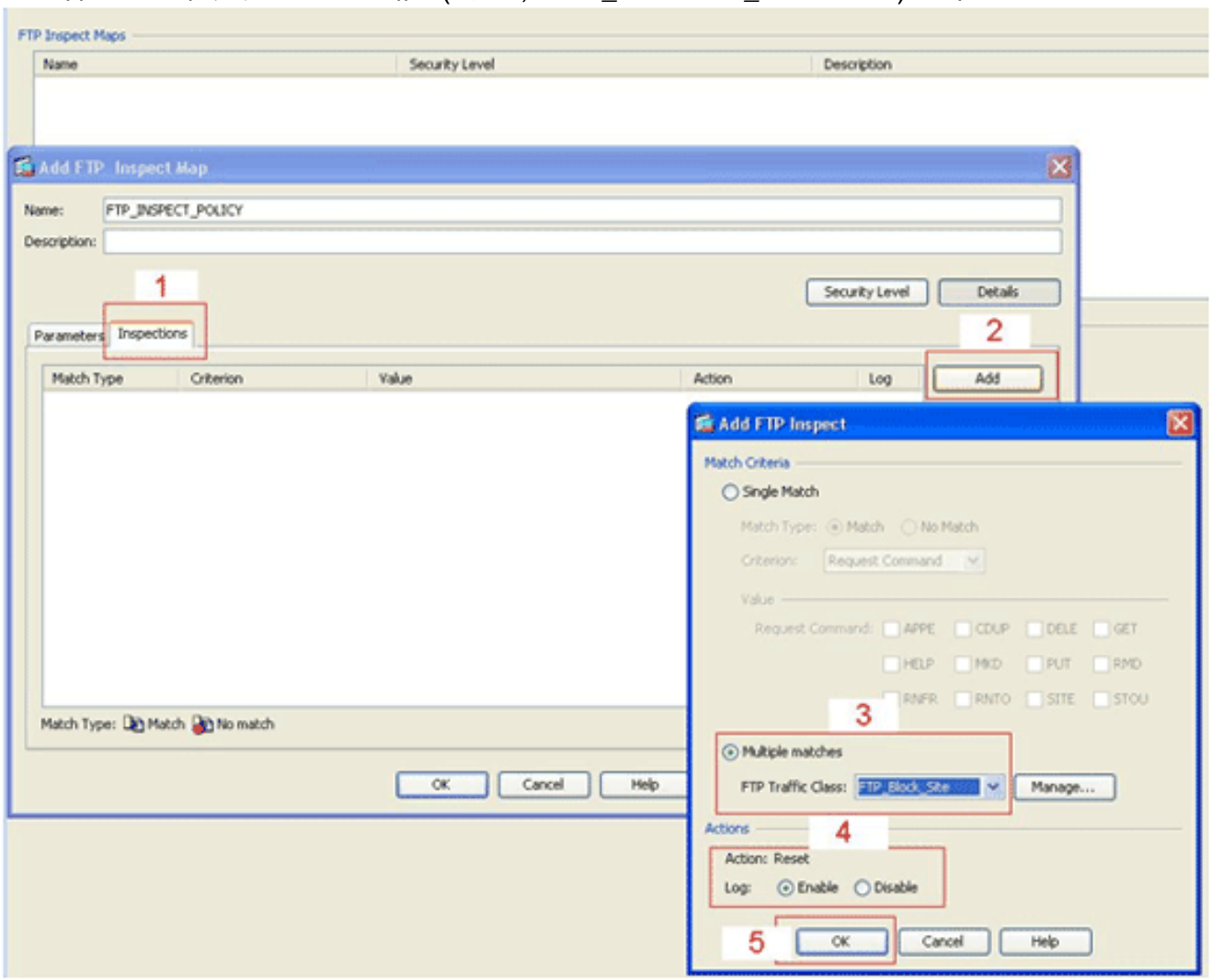


如果要排除在常规表示指定的站点，请勿点击**匹配**单选按钮。在值部分，请选择常规表示或一个常规表示组。对于此程序，请选择被创建前的组。单击 **Apply**。

5. **设置被匹配的数据流的动作在检查策略。**选择**Configuration>防火墙>对象> Inspect映射> FTP>添加**为了创建检查策略，并且设置被匹配的数据流的动作如所需求。



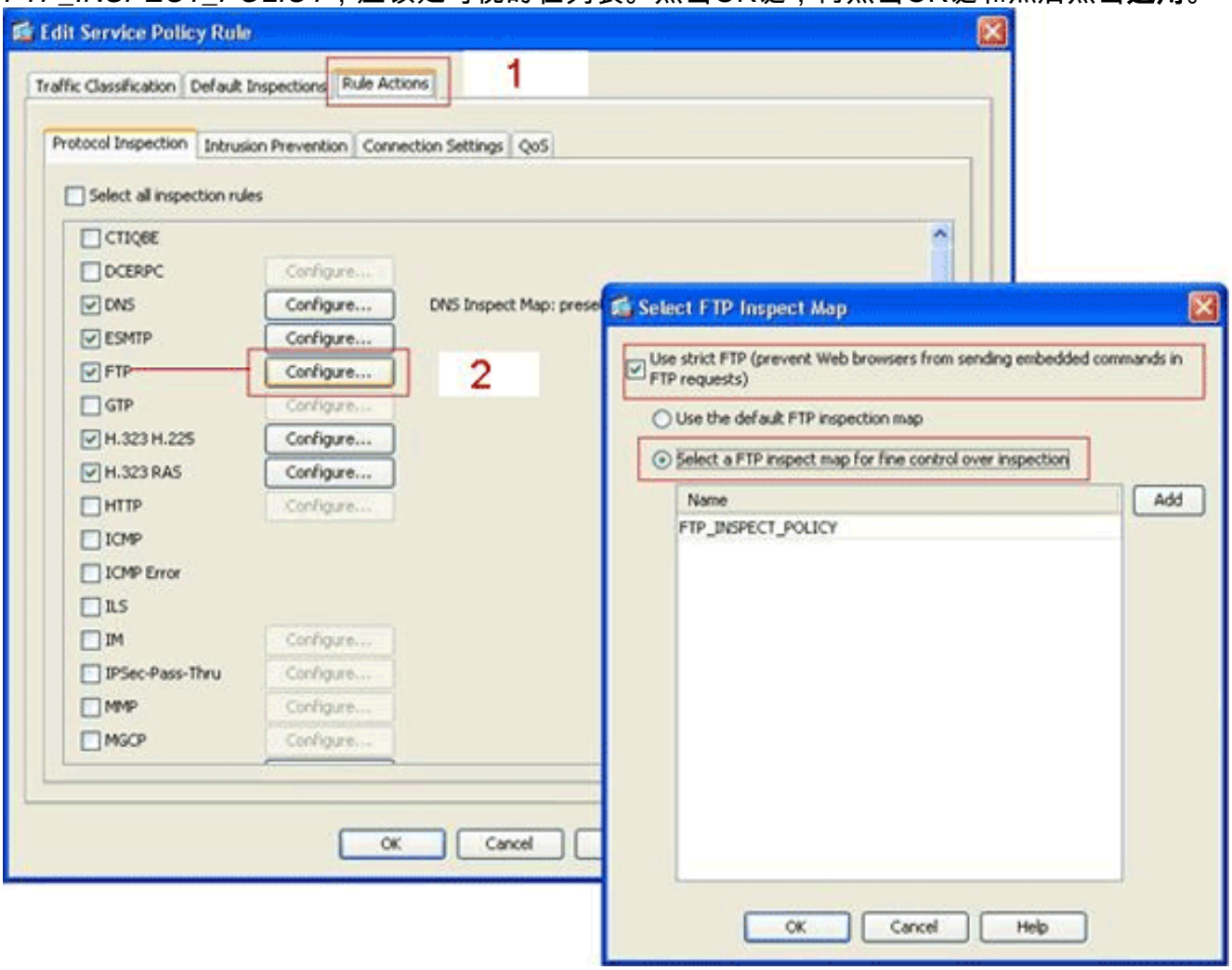
输入名字和一个说明的检查策略。(例如， *FTP_INSPECT_POLICY*。)单击 **Details**。



点击**检验**选项。(1)单击 **Add**。(2)点击**多匹配**单选按钮，并且从下拉列表选择话务类别。(3)选择期望重置动作对enable (event)或禁用。不*匹配*所有FTP的站点的此示例enable (event)

FTP连接重置我们指定的站点。(4)点击OK键，再点击OK键和然后点击**适用**。(5)

6. **运用检查FTP策略于全局检查列表。**选择**Configuration>防火墙>服务策略规则**。在右侧，请选择**inspection_default**策略，并且点击**编辑**。在规则动作下请选中(1)，点击FTP的**Configure (配置)按钮**。(2)在挑选FTP Inspect Map对话框中，请检查**使用严格的FTP**复选框，然后点击**更细微的控制的FTP Inspect映射对检查**单选按钮。新的FTP检查策略，*FTP_INSPECT_POLICY*，应该是可视的在列表。点击OK键，再点击OK键和然后点击**适用**。



Verify

Use this section to confirm that your configuration works properly.

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** —显示配置了的常规表示。

```
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** —显示配置了的类映射。

```
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策略映射类型Inspect http** —显示检查HTTP数据流配置了的策略映射。

```
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策略映射**—显示所有策略映射配置，以及默认策略映射配置。

```
ciscoasa#show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map type inspect 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**—显示所有当前运行的服务策略配置。

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

Troubleshoot

本部分提供的信息可用于对配置进行故障排除。

您能使用**policy命令的show service**为了验证检测引擎检查数据流和正确地给或者丢弃他们。

```
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
```

Related Information

- ASA/PIX 8.x：通过 MPF 使用正则表达式阻止某些网站 (URL) 的配置示例
- PIX/ASA 7.x和以后：使用MPF阻塞对等(P2P)和即时消息(IM)数据流配置示例
- PIX/ASA 7.x：启用 FTP/TFTP 服务配置示例
- 应用应用层协议检查
- Cisco ASA 5500系列自适应安全设备–技术支持
- Cisco Adaptive Security Device Manager (ASDM)
- Cisco PIX 500系列安全设备–技术支持
- 思科PIX防火墙软件–技术支持
- 思科PIX防火墙软件命令参考