ASA/PIX 8.x：允许/阻拦FTP站点使用有MPF的常规表达配置示例

目录

简介

本文档描述了如何配置 Cisco 安全设备 ASA/PIX 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。

先决条件

要求

本文档假设 Cisco 安全设备已经过配置并工作正常。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 以后Cisco 5500系列可适应的安全工具(ASA)该运行软件版本8.0(x)和
- ASA的8.x Cisco Adaptive Security Device Manager (ASDM) 6.x版

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。

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. 识别需要应用操作的第 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

正则表达式可以逐字匹配某个具体的文本串，也可以使用元字符来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** 以便在配置中输入 **d?g**。

要创建正则表达式，请使用 **regex** 命令。此外，**regex** 命令还可用于各种需要进行文本匹配的功能。例如，您可以通过 MPF（使用检查策略映射）对特定操作进行配置，使之适合于应用程序检查。有关详细信息，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** 命令可以使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。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
. 。	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，表示前面已有 0 个、1 个或任意数量的表达式。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。如果破折号 (-) 字符是中括号中的最后一个或第一个字符，那么它只有字面意义：**[[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	匹配新行：0x0a.

\ t	选项卡	匹配制表符：0x09.
\ f	换页符	匹配换页：0x0c.
\ x N N	转义的十六进制数	匹配使用十六进制的 ASCII 字符（必须正好两位数）。
\ N N N	转义的八进制数	以八进制数字匹配 ASCII 字符（必须是三位）。例如，字符 040 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：

注意： 使用正则表达式允许或阻止所选 FTP 站点。

配置

本文档使用以下配置：

- ASA CLI 配置
- ASA 配置 8.x 与 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 与 ASDM 6.x

要配置正则表达式并将其应用于 MPF 以阻止特定 FTP 站点，请完成以下步骤：

1. **确定 FTP 服务器名称。**FTP 检测引擎能够使用其他标准（如命令、文件名、文件类型、服务器和用户名）进行检测。此步骤使用服务器作为标准。FTP 检测引擎使用 FTP 站点传送的服务器 220 响应作为服务器值。此值可能不同于站点所使用的域名。此示例使用 Wireshark 来捕获传送到被检测站点的 FTP 数据包，以获取用在步骤 2 的正则表达式中的响应 220 值。例

如，根据捕获情况来看，ftp://hp.com 的响应 220 值为 *q5u0081c.atlanta.hp.com*。

2. **创建正则表达式。**选择 **Configuration > Firewall > Objects > Regular Expressions**，然后单击 Regular Expression 选项卡下的 **Add**，以便根据此步骤中的描述创建正则表达式：创建正则表达式 *FTP_SITE1*，以匹配从 FTP 站点（例如 .* hp\.com.* ）收到的响应 220（参见 Wireshark 或任何其他已使用工具中的数据包捕获），然后单击 **OK**。**注意：** 您可以单击 **Build** 以获取有关如何创建更高级正则表达式的帮助。创建正则表达式后，请单击 **Apply**。
3. **创建正则表达式类。**选择 **Configuration > Firewall > Objects > Regular Expressions**，然后单击 Regular Expression Classes 部分下的 **Add**，以便根据此步骤中的描述创建正则表达式类：创建正则表达式类 *FTP_SITES*，以匹配正则表达式 *FTP_SITE1* 和 *FTP_SITE2* 中的任何一个，然后单击 **OK**。创建类映射后，请单击 **Apply**。
4. **检查由类映射识别出的流量。**选择 **Configuration > Firewall > Objects > Class Maps > FTP > Add**，右键单击并选择 **Add**，以便创建类映射来检查此步骤中描述的各种正则表达式所识别出的 FTP 流量：创建类映射 *FTP_Block_Site*，以便将 FTP 响应 220 与您所创建的正则表达式进行匹配。如果要排除正则表达式中的指定站点，请单击 **No Match** 单选按钮。在 Value 部分，选择正则表达式或正则表达式类。对于此步骤，请选择之前创建的类。单击 **Apply**。
5. **为检查策略中的已匹配流量设置操作。**选择 **Configuration > Firewall > Objects > Inspect Maps > FTP> Add**，以便创建检查策略，并根据需要为匹配的流量设置操作。输入检查策略的名称和说明。（例如，*FTP_INSPECT_POLICY*。）单击 **Details**。单击 **Inspections** 选项卡。(1)单击 **Add**。(2)单击 **Multiple matches** 单选按钮，然后从下拉列表中选择流量类。(3)选择需要启用或禁用的重置操作。此示例为 *不符合*指定站点的所有 FTP 站点启用了 FTP 连接重置。(4)依次单击 **OK**、**OK** 和 **Apply**。(5)
6. **将检查 FTP 策略应用于全局检查列表。**选择 **Configuration > Firewall > Service Policy Rules**。在右侧选择 **inspection_default** 策略，然后单击 **Edit**。在 Rule Actions 选项卡 (1) 下，单击 FTP 的 **Configure** 按钮。(2)在 Select FTP Inspect Map 对话框中，选中 **Use strict FTP** 复选框，然后单击 **FTP inspect map for fine control over inspection** 单选按钮。此时会在列表中看到新的 FTP 检查策略 *FTP_INSPECT_POLICY*。依次单击 **OK**、**OK** 和 **Apply**。

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 FTP_SITE1 "[Cc][Ii][Ss][Cc][Oo]\.[Cc][Oo][Mm]" regex FTP_SITE2 ".*hp\.com.*"`
- **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 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** - 显示用来检查已配置 HTTP 流量的策略映射。`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 policy-map** - 显示所有策略映射配置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`

故障排除

本部分提供的信息可用于对配置进行故障排除。

您可以使用 **show service-policy** 命令来验证检测引擎是否检查流量并正确保留或丢弃流量。

```
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
```

相关信息

- 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 及更高版本：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 – 支持
- Cisco 自适应安全设备管理器 (ASDM)
- Cisco PIX 500 系列安全设备 – 支持
- Cisco PIX 防火墙软件 - 支持
- Cisco PIX 防火墙软件命令参考
- 技术支持和文档 - Cisco Systems