ASA/PIX 8.x: Allow/Block FTP Sites Using Regular Expressions with MPF Configuration Example

Contents

Introduction

This document describes how to configure the Cisco Security Appliances ASA/PIX 8.x that uses regular expressions with Modular Policy Framework (MPF) in order to block or allow certain FTP sites by server name.

Prerequisites

Requirements

This document assumes that the Cisco Security Appliance is configured and works properly.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5500 Series Adaptive Security Appliance (ASA) that runs the software version 8.0(x)

and later
- Cisco Adaptive Security Device Manager (ASDM) version 6.x for ASA 8.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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Modular Policy Framework Overview

MPF provides a consistent and flexible way to configure security appliance features. For example, you can use MPF to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications.

MPF supports these features:

- TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization
- CSC
- Application inspection
- IPS
- QoS input policing
- QoS output policing
- QoS priority queue

The configuration of the MPF consists of four tasks:

1. Identify the Layer 3 and Layer 4 traffic to which you want to apply actions. Refer to Identifying Traffic Using a Layer 3/4 Class Map for more information.
2. (Application inspection only.) Define special actions for application inspection traffic. Refer to Configuring Special Actions for Application Inspections for more information.
3. Apply actions to the Layer 3 and Layer 4 traffic. Refer to Defining Actions Using a Layer 3/4 Policy Map for more information.
4. Activate the actions on an interface. Refer to Applying a Layer 3/4 Policy to an Interface Using a Service Policy for more information.

Regular Expression

A regular expression matches text strings either literally as an exact string or by the use of metacharacters, so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic. For example, you can match a URL string inside an HTTP packet.

Note: Use **Ctrl+V** in order to escape all of the special characters in the CLI, such as question marks (?) or tabs. For example, type **d[Ctrl+V]g** in order to enter **d?g** in the configuration.

In order to create a regular expression, use the **regex** command. In addition, the **regex** command can be used for various features that require text matching. For example, you can configure special actions for application inspection with the use of the MPF that uses an inspection policy map. Refer to the **policy-map type inspect** command for more information.

In the inspection policy map, you can identify the traffic you want to act upon if you create an inspection class map that contains one or more **match** commands, or you can use **match** commands directly in the inspection policy map. Some **match** commands let you identify text in a packet using a regular expression. For example, you can match URL strings inside HTTP packets. You can group regular expressions in a regular expression class map. Refer to the **class-map type regex** command for more information.

This table lists the metacharacters that have special meanings.

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(exp)	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, **dog|cat** matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note:** You must enter **Ctrl+V** and then the question mark or else the help function is invoked.
*	Asterisk	A quantifier that indicates that there are 0, 1, or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, and so forth.
{x}	Repeat quantifier	Repeat exactly x times. For example, **ab(xy){3}z** matches abxyxyxyz.
{x,}	Minimum repeat quantifier	Repeat at least x times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, and so forth.
[abc	Charac	Matches any character in the brackets.

]	ter class	For example, **[abc]** matches a, b, or c.
[^abc]	Negated character class	Matches a single character that is not contained within the brackets. For example, **[^abc]** matches any character other than a, b, or c. **[^A-Z]** matches any single character that is not an uppercase letter.
[a-c]	Character range class	Matches any character in the range. **[a-z]** matches any lowercase letter. You can mix characters and ranges: **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does **[a-cq-z]**. The dash (-) character is literal only if it is the last or the first character within the brackets: **[abc-]** or **[-abc]**.
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, " **test**" preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.
\	Escape character	When used with a metacharacter, matches a literal character. For example, **\[** matches the left square bracket.
char	Character	When the character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return: 0x0d.
\n	Newline	Matches a new line: 0x0a.
\t	Tab	Matches a tab: 0x09.
\f	Formfeed	Matches a form feed: 0x0c.
\xNN	Escaped hexadecimal number	Matches an ASCII character that uses a hexadecimal that is exactly two digits.
\NNN	Escaped octal number	Matches an ASCII character as octal that is exactly three digits. For example, the character 040 represents a space.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

Note: Selected FTP sites are allowed or blocked using regular expressions.

Configurations

This document uses these configurations:

- ASA CLI Configuration
- ASA Configuration 8.x with ASDM 6.x

ASA CLI Configuration

ASA CLI Configuration

```
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 Configuration 8.x with ASDM 6.x

Complete these steps in order to configure the regular expressions and apply them to MPF in order to block the specific FTP sites:

1. **Determine the FTP server name.**The FTP inspection engine can provide inspection using different criterion, such as command, file name, file type, server, and user name. This procedure uses the server as criterion. The FTP inspection engine uses the server 220 response sent by the FTP site as the server value. This value can be different than the domain name used by the site. This example uses Wireshark to capture FTP packets to the site that is inspected in order to get the response 220 value for used in our regular expression in step 2.Based on the capture the response 220 value for ftp://hp.com is (for example) *q5u0081c.atlanta.hp.com*.
2. **Create regular expressions.**Choose **Configuration > Firewall > Objects > Regular Expressions**, and click **Add** under the Regular Expression tab in order to create regular expressions as described in this procedure:Create a regular expression, *FTP_SITE1*, in order to match the response 220 (as seen in the packet capture in Wireshark or any other tool used) received from the ftp site (for example, ".* hp\.com.*"), and click **OK**.**Note:** You can click **Build** for help on how to create more advanced regular expressions.Once the regular expression is created, click **Apply.**
3. **Create regular expression classes.**Choose **Configuration > Firewall > Objects >**

Regular Expressions, and click **Add** under the Regular Expression Classes section in order to create the class as described in this procedure:Create a regular expression class, *FTP_SITES*, in order to match any of the regular expressions *FTP_SITE1* and *FTP_SITE2*, and click **OK**.Once the class map is created, click **Apply**.

4. **Inspect the identified traffic with class maps.**Choose **Configuration > Firewall > Objects > Class Maps > FTP > Add**, right-click, and choose **Add** in order to create a class map to inspect the FTP traffic identified by various regular expressions as described in this procedure:Create a class map, *FTP_Block_Site*, in order to match the FTP response 220 with the regular expressions you created.If you want to exclude the sites specified in the regular expression, click the **No Match** radio button.In the Value section, choose either a regular expression or a regular expression class. For this procedure, choose the class that was created earlier.Click **Apply**.
5. **Set the actions for the matched traffic in the inspection policy.**Choose **Configuration > Firewall > Objects > Inspect Maps > FTP> Add** in order to create an inspection policy, and set the action for the matched traffic as required.Enter the name and a description for the inspection policy. (For example, *FTP_INSPECT_POLICY*.)Click **Details.**Click the **Inspections** tab. (1)Click **Add**. (2)Click the **Multiple matches** radio button, and choose the traffic class from the drop-down list. (3)Choose the desired reset action to enable or disable. This example enables FTP connection reset for all FTP sites *not matching* our specified sites. (4)Click **OK**, click **OK** again, and then click **Apply**. (5)
6. **Apply the inspection FTP policy to the global inspection list.**Choose **Configuration > Firewall > Service Policy Rules**.On the right side, select the **inspection_default** policy, and click **Edit**.Under the Rule Actions tab (1), click the **Configure** button for FTP. (2)In the Select FTP Inspect Map dialog box, check the **Use strict FTP** check box, and then click the **FTP inspect map for fine control over inspection** radio button.The new FTP inspection policy, *FTP_INSPECT_POLICY*, should be visible in the list.Click **OK**, click **OK** again, and then click **Apply**.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show running-config regex**—Shows the regular expressions that have been configured.
```
ciscoasa#show running-configregex
regex FTP_SITE1 "[Cc][Ii][Ss][Cc][Oo]\.[Cc][Oo][Mm]"
regex FTP_SITE2 ".*hp\.com.*"
```
- **show running-config classmap**—Shows the class maps that have been configured.
```
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**—Shows the policy maps that inspect the HTTP traffic that have been configured.

```
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**—Displays all the policy map configurations, as well as the default policy map configuration.

```
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**—Displays all currently running service policy configurations.

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

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

You can use the **show service-policy** command in order to verify that the inspection engine inspects the traffic and correctly allows or drops them.

```
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: Block Certain Websites (URLs) Using Regular Expressions With MPF Configuration Example**
- **PIX/ASA 7.x and Later: Block the Peer-to-Peer (P2P) and Instant Messaging (IM) Traffic Using MPF Configuration Example**
- **PIX/ASA 7.x: Enable FTP/TFTP Services Configuration Example**
- **Applying Application Layer Protocol Inspection**
- **Cisco ASA 5500 Series Adaptive Security Appliances – Support**
- **Cisco Adaptive Security Device Manager (ASDM)**
- **Cisco PIX 500 Series Security Appliances – Support**
- **Cisco PIX Firewall Software – Support**
- **Cisco PIX Firewall Software Command References**