Flexible Packet Matching Q&A

Q. What is Flexible Packet Matching?

A. Flexible Packet Matching is a next-generation access control list (ACL) technology that is capable of filtering at a bit-level, deep within IP packets.

Q. Why would I want to use Flexible Packet Matching?

A. Flexible Packet Matching provides the granularity to filter anomalous traffic from networks while minimizing the risk of filtering legitimate business traffic. Flexible Packet Matching provides the means to configure match criteria for any or all fields in a packet's header, as well as bit-patterns within full length of the packet's payload starting with Cisco IOS 15.0(1)M Release. This allows the characteristics of an attack (source port, packet size, byte string) to be uniquely matched and allows a designated action to be taken. Flexible Packet Matching provides a flexible Layer 2-7 stateless classification mechanism. The user can specify classification criteria based on any protocol and any field of the traffic's protocol stack. Based on the classification result, actions such as drop or log can be taken. Note that in Cisco IOS releases prior to IOS 15.0(1)M Release, the search length within each packet is limited to 256 bytes.

Q. How does Flexible Packet Matching fit into the Cisco® Self-Defending Network?

A. Flexible Packet Matching complements technologies such as ACLs, intrusion prevention systems (IPS), and network-based application recognition (NBAR) by giving customers bit-level filtering capabilities to remove anomalous traffic from the network. Flexible Packet Matching is useful because it enables users to create their own stateless packet classification criteria and to define multiple policies with multiple actions.

Q. What is the benefit of using Flexible Packet Matching?

A. Flexible Packet Matching helps minimize the risk of filtering legitimate business traffic, allowing customers to define granular policies to filter malicious traffic based on bits within the packet header or payload associated with the malicious packets. As an example, the slammer worm propagated on User Datagram Protocol (UDP) port 1434. Instead of dropping all UDP 1434 traffic, Flexible Packet Matching provides the capability to look for a 4-byte packet string at an offset of 224 bytes from the IP header.

Q. What Cisco IOS® Software release should I use for Flexible Packet Matching?

A. Flexible Packet Matching is supported on Cisco 800 to 7200 Series and Cisco 7301 routers, beginning with the security image for Cisco IOS Software Release 12.4(4)T. Cisco IOS Software Release 15.0(1)M is recommended.

Q. How do I configure Flexible Packet Matching?

A. Flexible Packet Matching can be configured via the command-line interface (CLI) or loading an Extensible Markup Language (XML) file called Traffic Classification Definition File (TCDF) on the router flash. The Flexible Packet Matching Deployment Guide has complete details on how to configure Flexible Packet Matching via the CLI. For details and sample configurations, visit http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6723/prod_white_paper0900aecd803936f6.shtml

Q. Can I configure Flexible Packet Matching using a GUI?

A. No. Currently, Flexible Packet Matching cannot be configured using a GUI.

Q. I heard that I can configure a Flexible Packet Matching policy using an XML file. Can you provide more information?

A. Yes. The Flexible Packet Matching XML Configuration feature allows the use of XML to define traffic classes and actions to assist in blocking network attacks. The XML file used by Flexible Packet Matching is called the Traffic Classification Definition File (TCDF).

Q. What is a Traffic Classification Definition File?

A. A TCDF is the XML file that is used to define traffic classes and actions (policies) when not using the CLI. The TCDF gives you an alternative to the CLI as a method to define traffic classification behavior. Traffic classification is identical, regardless of the method you use. For more information on TCDFs, visit http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008061d643.html

Q. What are Protocol Header Definition Files (PHDFs)?

A. PHDFs are analogous to stencils. A PHDF outlines the structure of packets in an XML format. The field names that are defined within the PHDFs are used for defining the packet filters. A PHDF is a file that allows the user to take advantage of the flexibility of XML to describe almost any protocol header. The important components of the PHDF are the version, the XML file schema location, and the protocol field definitions. The protocol field definitions name the appropriate field in the protocol header, allow for a comment describing the field, provide the location of the protocol header field in the header (the offset is relative to the start of the protocol header), and provide the length of the field. Standard PHDFs and FPM starting template starter.tcdf need to be loaded first before defining FPM filters. They are available on the router at files: system:/fpm/phdf/ and system:/fpm/tcdf/starter.tcdf

Q. Does Cisco provide a library of common PHDFs?

A. Yes. They can be downloaded from http://www.cisco.com/pcgi-bin/tablebuild.pl/fpm

Q. Can you provide an example of packet structure and the corresponding PHDF?

A. Figure 1 shows the structure of an IP header and the corresponding PHDF.

Figure 1. IP Header and PHDF


```
<?xml version="1.0" encoding="UTF-8"?>
<phdf>
<version>1</version>
<protocol name="ip" description="IP-Protocol">
<field name="version" description="IP-Version">
<offset type="fixed-offset" units="bits"> 0 </offset>
<length type="fixed" units="bits">4</length>
</field>
```

```
<field name="ihl" description="IP-Header-Length">
<offset type="fixed-offset" units="bits">4</offset>
<length type="fixed" units="bits">4</length>
</field>
<field name="tos" description="IP-Type-Of-Service">
<offset type="fixed-offset" units="bits">8</offset>
<length units="bits" type="fixed">8</length>
</field>
<field name="length" description="IP-Packet-Length">
<offset type="fixed-offset" units="bytes">2</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="identification" description="IP-Identification">
<offset type="fixed-offset" units="bytes">4</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="flags" description="IP-Fragmentation-Flags">
<offset type="fixed-offset" units="bytes">6</offset>
<length type="fixed" units="bits">3</length>
</field>
<field name="fragment-offset" description="IP-Fragmentation-Offset">
<offset type="fixed-offset" units="bits">51</offset>
<length type="fixed" units="bits">13</length>
</field>
<field name="ttl" description="IP-TTL">
<offset type="fixed-offset" units="bytes">8</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="protocol" description="IP-Protocol">
<offset type="fixed-offset" units="bytes">9</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="checksum" description="IP-Header-Checksum">
<offset type="fixed-offset" units="bytes">10</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="source-addr" description="IP-Source-Address">
<offset type="fixed-offset" units="bytes">12</offset>
<length type="fixed" units="bytes">4</length>
</field>
<field name="dest-addr" description="IP-Destination-Address">
<offset type="fixed-offset" units="bytes">16</offset>
<length type="fixed" units="bytes">4</length>
</field>
<field name="payload-start" description="IP-Payload-Start">
<offset type="fixed-offset" units="bytes">20</offset>
<length type="fixed" units="bytes">0</length>
</field>
<headerlength type="fixed" value="20"></headerlength>
<constraint field="version" value="4" operator="eq"></constraint>
```

```
<constraint field="ihl" value="5" operator="eq"></constraint>
</protocol>
</phdf>
```

Q. Is the Flexible Packet Matching feature process-switched or Cisco Express Forwarding-switched?

A. The Flexible Packet Matching feature is Cisco Express Forwarding-switched.

Q. Can you provide a practical example of how Flexible Packet Matching can help in combating worm or virus outbreak traffic?

A. As a reactive tool, Flexible Packet Matching can be used to thwart worms, viruses, or attack traffic-the type of traffic that you are still waiting for IPS signatures to be made available for.

Q. What is the performance impact of using Flexible Packet Matching?

A. Performance impact will depend on various factors, such as the number and types of filters, or the protocols involved. An example of the possible performance impact of Flexible Packet Matching can be found toward the end of the Flexible Packet Matching Deployment Guide at http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6723/prod_white_paper0900aecd803936f6.html

Q. What is the difference between NBAR and Flexible Packet Matching?

A. Flexible Packet Matching is a stateless packet classification mechanism, an enhancement to existing ACL capabilities in Cisco IOS Software. NBAR is stateful. With NBAR, flow-identifying information is cached in memory and subsequent packets that match the same flow can receive the same policy action without additional packet inspection/re-inspection. Flexible Packet Matching inspects one packet at a time without keeping context.

Q. How deep into the packet can Flexible Packet Matching inspect?

A. Starting with Cisco IOS 15.0(1)M Release, Flexible Packet Matching feature can look for a string or pattern within full length of the packet's payload. However, in earlier IOS releases, the search length within each packet is limited to 256 bytes.

Q. Can Flexible Packet Matching be used for non-IP protocols?

A. No. Flexible Packet Matching cannot inspect non-IP protocols.

Q. Can Flexible Packet Matching policies be applied on a Bridged Virtual Interface (BVI)?

A. No. Flexible Packet Matching policies cannot be applied on a BVI.

Q. What format does the search string need to be in?

A. The search string used in the regular expressions can be in decimal or hexadecimal format; for example, 17 or 0x11 will yield the same policy match.

Q. Can Flexible Packet Matching policies be deployed without reloading the router?

A. Yes. Flexible Packet Matching policies can be deployed without requiring a reload.

Q. What is the difference between Flexible Packet Matching and ACLs?

A. Flexible Packet Matching is next-generation ACL technology. The two features have the same basic functions, with Flexible Packet Matching allowing classification of traffic at a bit level.

Q. How does Flexible Packet Matching help to detect malicious traffic?

A. Flexible Packet Matching is not used as a detection mechanism. Instead, Flexible Packet Matching is used to filter the malicious traffic.

Q. Does Flexible Packet Matching support stateful traffic?

A. No. Flexible Packet Matching does not maintain state. Flexible Packet Matching is a stateless classification mechanism: next-generation ACL technology.

Q. Is Flexible Packet Matching supported by the Cisco Router and Security Device Manager (SDM), Cisco Configuration Professianal (CCP) or Cisco Security Manager (CSM) management applications?

A. No. Currently, Flexible Packet Matching is not supported by those applications..

Q. Why do I need Flexible Packet Matching if I already have a Cisco IOS IPS and Cisco IOS Firewall enabled?

A. Flexible Packet Matching technology complements Cisco IPS and Cisco IOS Firewall to help remove malicious traffic from the network.

For More Information

For more information about Cisco Flexible Packet Matching, visit http://www.cisco.com/go/fpm. You may also contact your local account representative or send e-mail to ask-stg-ios-pm@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-563935-00 10/09