



Data Sheet

Cisco Flexible Packet Matching

Cisco® Flexible Packet Matching is a next-generation packet filtering feature introduced in Cisco IOS® Software Release 12.4(4)T. Flexible Packet Matching enables filtering, at a bit level, deep within the packet. When networks are under attack, access control lists (ACLs) are deployed at the network edge as the first line of defense.

CHALLENGE

Malicious attacks against networks are increasing in frequency and sophistication. To counter these attacks, tools are needed that are as flexible as possible and that can provide packet inspection capabilities at different levels. Many of the tools available today do not allow deep packet inspection. These tools are constrained to specific fields in well-known protocol headers. If an attack uses a field outside the limited range of inspection provided by these tools, it is difficult to classify and defend against the attack.

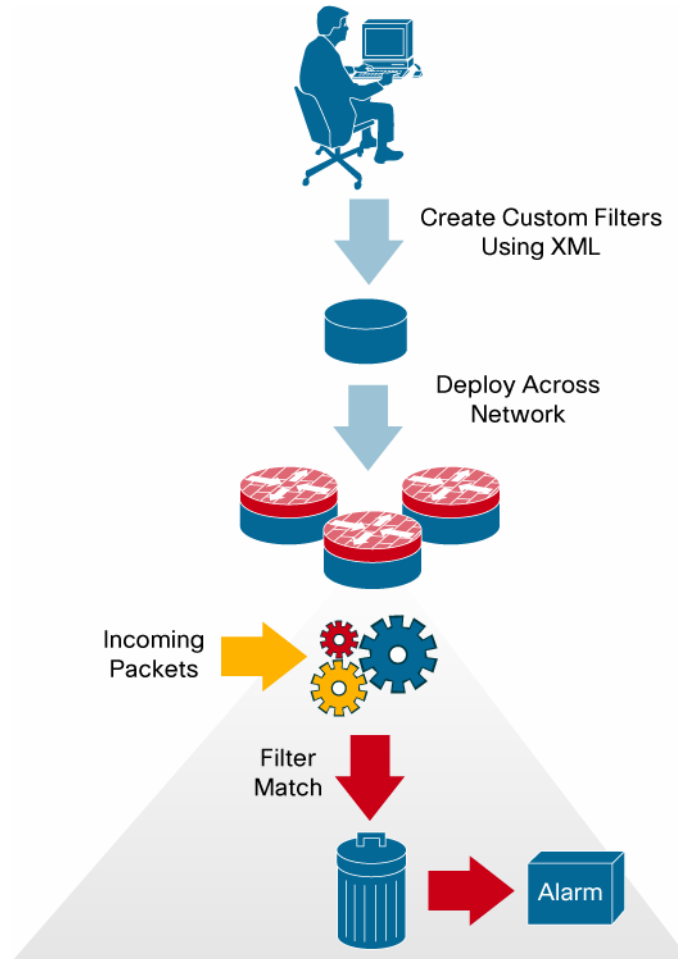
Cisco Flexible Packet Matching provides network and security administrators with powerful tools to filter traffic as it enters the network and to immediately drop and/or keep a log for auditing purposes. Flexible Packet Matching allows network and security administrators to specify custom patterns to match on, deep within the packet header or payload. The feature introduces the concept of protocol header definition files (PHDFs), which give names to offset locations within a packet, thereby increasing the usability of Flexible Packet Matching. Ready-made definitions for standard protocols are included via PHDF, making it easy to deploy out of the box, at run time. High-level custom scripting for PHDFs is supported via standard XML editors.

SOLUTION

Cisco Flexible Packet Matching provides the means to inspect packets for characteristics of an attack, and to take appropriate actions (log, drop, or ICMP unreachable). Flexible Packet Matching provides a flexible Layer 2 through Layer 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 on the classified traffic.

Figure 1 shows how Flexible Packet Matching works.

Figure 1. Cisco Flexible Packet Matching



PROTOCOL HEADER DEFINITION FILE (PHDF)

The custom scripting available for packet classification is done with PHDFs. The PHDF defines the structure of a particular packet and adds the protocol inspection capabilities to Cisco IOS Software. The field names that are defined within the PHDFs are used for defining the packet filters. A PHDF enables 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. A PHDF also helps in configuration simplicity by defining certain “always match” criteria as constraints.

MANAGEMENT OPTIONS

The Cisco Flexible Packet Matching feature is managed via the Cisco IOS CLI, a full-featured CLI that provides device configuration over a Secure Shell (SSH) Protocol connection.

INTEGRATION WITH OTHER SECURITY DEPLOYMENT SOLUTIONS

When using the Cisco Flexible Packet Matching feature in combination with other Cisco packet inspection technologies such as Cisco intrusion prevention systems (IPSs), network-based protocol recognition, and ACLs, network operators have a best-of-breed selection of tools to identify and control traffic flows in a network.

ORDERING INFORMATION

Flexible Packet Matching is introduced in Cisco IOS Software Release 12.4(4)T. The feature will only be available in Advanced Security, Advanced IP Services, and Advanced Enterprise Software packages. The supported hardware platforms are listed below:

- Cisco 871 integrated services routers
- Cisco 1700 Series modular access routers
- Cisco 1800 Series integrated services routers
- Cisco 2600 Series multiservice routers
- Cisco 2600XM Series multiservice routers
- Cisco 2800 Series Integrated Services Routers
- Cisco 3700 Series multiservice routers
- Cisco 3800 Series integrated services routers
- Cisco 7200 Series universal services routers
- Cisco 7301 routers

For ordering details or more information on Cisco Flexible Packet Matching, visit: <http://www.cisco.com/go/fpm>

For more information on Cisco IOS router security, visit: <http://www.cisco.com/go/routersecurity>

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R) 205233.BM_ETMG_KS_10.05

