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 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.

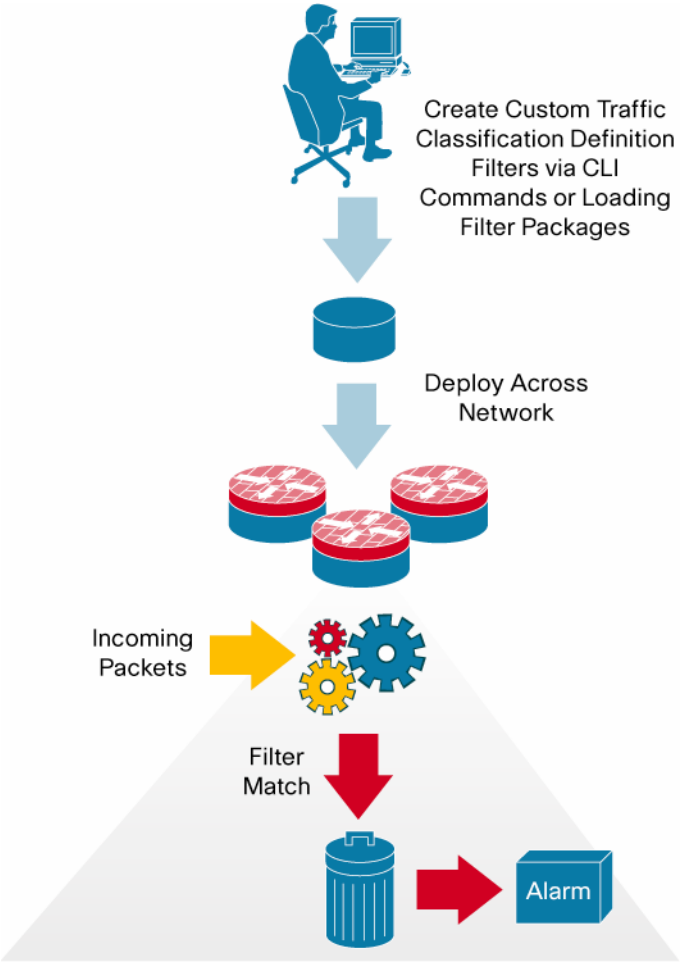
Solution

Cisco Flexible Packet Matching provides network and security administrators with a powerful and subscription-free tool available within Cisco IOS Security to inspect and filter traffic as it enters the network. The feature supports inspection of packets to match for characteristics of an attack and to take appropriate actions. It uses a flexible Layer 2 through Layer 7 stateless classification mechanism where 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 matching traffic.

The feature introduces the concept of Traffic Classification Definition Filters (TCDFs) which allows defining simple string and/or regular-expression style flexible patterns to match anywhere within packets going through a router interface in any direction, Each filter also specifies the starting position and length of the portion within each packet to search for the specified pattern. Starting with Cisco IOS 15.0(1)M Release, the search length may cover the whole packet; however, the search length is limited to 256 bytes within each packet in previous IOS releases.

A single traffic classification filter can match any pattern within anywhere in packets and may be defined via CLI using FPM keywords and the fields provided in the standard (Cisco provided) or custom created Protocol Header Definition Files (PHDFs) and/or one or more filters (written in XML) can be put into a a package file, downloaded to and stored on the router and then loaded via FPM CLI. It is also possible to load multiple package files containing any number of filters. Starting with Cisco IOS 15.0(1)M Release, Filters in FPM packages provided by Cisco will be encrypted and stored into a file called eTCDF (encrypted Traffic Classification Definition File) and may be used to protect the router against exploits of certain vulnerabilities in IOS such as those announced by Cisco PSIRT. These filters are decrypted just before they are loaded into search pattern tables created and maintained in the router's memory. Encrypted or plain text TCDF packages can be loaded from the router flash or directly from a local server accessible via TFTP, FTP or HTTP(S) via CLI. It is also possible to configure the router to update those files automatically from the local server on a periodic basis. Regardless of the loading method and order, filters are optimized into an efficient structure that will analyze each packet only once for all FPM search strings or regular-expressions that are loaded. all filters are merged into a single regular-expression based search pattern table to allow parallel and quick scanning for all filters at the same time, through a single scan of each packet. 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. High-level custom scripting for PHDFs is supported via standard XML editors.

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 Network Access Control (NAC), Cisco intrusion prevention systems (IPS), network-based

protocol recognition, and ACLs, network operators have a best-of-breed selection of IOS features to identify and control traffic flows in a network.

Platform Support

Cisco IOS Flexible Packet Marching (FPM) feature is available in certain software feature sets on the 87x routers, Integrated Services Routers, 720x and 7301 routers listed in Table 2. Starting with Cisco IOS 15.0(1)M Release, IOS FPM feature is also supported on the 88x, 89x routers and next generation Integrated Services Routers with an optional license that enables use of that and other features when installed, as shown in Table 3.

Table 1. FPM Feature Availability based on IOS Image Types

Product Family	Platforms Supported	IOS Images (Feature Sets) Supported
800	871, 876, 877, 878	Advanced Security (Default image)
1800	1801, 1802, 1803, 1811, 1812, 1841, 1861	Advanced Security, Advanced Enterprise, and Advanced IP Services
2800	2801, 2811, 2821, 2851	Advanced Security, Advanced Enterprise, and Advanced IP Services
3800	3825, 3845	Advanced Security, Advanced Enterprise, and Advanced IP Services
7200	7204VXR, 7206VXR	Advanced Security, Advanced Enterprise, and Advanced IP Services
7301	7301	Advanced Security, Advanced Enterprise, and Advanced IP Services

Table 2. FPM Feature Availability based on Optional Feature Licenses

Product Family	Platforms Supported	Feature License Supported
800	881, 887, 888, 891, 892	IPBase (No additional license required)
1900	1941	Security
2900	2901, 2911, 2921,2951	Security
3900	3925,3945	Security

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies. For more information, visit http://www.cisco.com/go/services.

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

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 C78-560355-01 11/09