Cisco IOS Flexible Packet Matching

Value-Added Security Services in Cisco IOS Software

Integrated Router Security Solutions

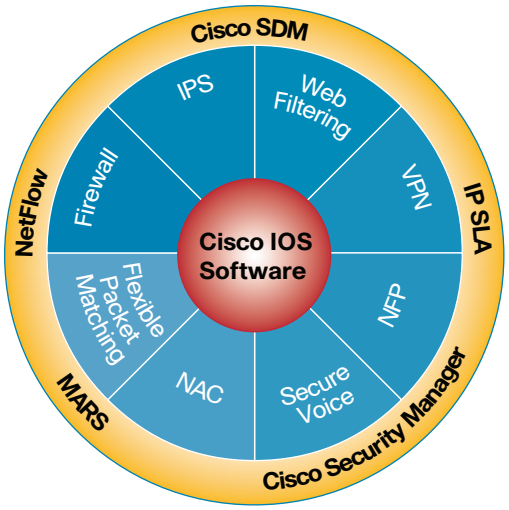
Comprehensive network security features in Cisco routers help companies protect their infrastructures, devices, and important information, while reducing costs

Networks are experiencing increasingly sophisticated attacks (worms, viruses, and Trojan horses, among others) that require mitigating tools that are as flexible as possible. Network security administrators must be able to stop these attacks immediately. Cisco IOS Flexible Packet Matching (FPM) protects against existing and emerging threats at all network entry points, from the branch office to the enterprise to the campus.

Cisco IOS FPM takes access control lists (ACLs) a step further by inspecting deep within the packet at the bit and byte level

Cisco IOS FPM is an important component of the integrated threat-control framework in Cisco IOS® Software, and complements Cisco IOS IPS by supporting custom filters that can be defined and deployed more rapidly than IPS signatures or antivirus updates. It gives network security administrators powerful tools with which to identify miscreant traffic and immediately drop it or log it for audit purposes.

Cisco FPM uses a flexible set of classes and policies that provides pattern-matching capability for more granular and customized packet filters, bringing Layer 2–7 bit/byte matching capability deep into the packet at any offset within the packet header and payload. In short, Cisco FPM provides a rapid first line of defense against network threat and most notable worms and viruses.



Cisco IOS Flexible Packet Matching FPM provides the following benefits:

- Rapidly responds to new and emerging attacks before they spread to other parts of the network
- Filters anomalous traffic targeting the network by classifying traffic based on multiple attributes within a packet
- Protects the network from sophisticated attacks using flexible and granular Layer 2-7 matching on any bit at any offset within the packet header or payload
- Enforces business policy by blocking communications and file-sharing applications such as Skype and Gnutella
- Addresses Day Zero attacks by defining and deploying custom filters before antivirus or IPS signatures have a chance to update
- Leverages a predefined filter library from Cisco to easily identify notable attacks and applications

Business/Security Challenges	The Cisco Solution
Sophisticated Attacks	Cisco IOS Flexible Packet Matching (FPM) can mitigate common attacks based on characteristics that have evolved beyond current filtering tools such as ACLs with limited matching criteria.
Rapid Mitigation	Cisco IOS Flexible Packet Matching (FPM) can be deployed rapidly so you can stop attacks immediately without waiting for a vendor to develop a signature (IPS) or new code enhancements (ACL).
Finer Level of Detail	Cisco IOS FPM goes beyond static attributes, allowing you to specify arbitrary bits or bytes at any offset within the entire packet (header or payload), minimizing inadvertent blocking of legitimate business traffic.
Business Security Compliance	Cisco IOS Flexible Packet Matching (FPM) can help ensure corporate network security compliance by blocking peer-to-peer (P2P) applications such as Skype and file-sharing applications such as Gnutella which have the ability to work on any network, regardless of the types of NAT, proxy, firewall, or IPSs that are put in place.

Where Cisco IOS Flexible Packet Matching can be deployed

Cisco IOS Flexible Packet Matching (FPM) is designed to protect against existing and emerging threats at the entry point into your network. Cisco IOS Flexible Packet Matching (FPM) can be deployed anywhere that the ability to perform classification upon unique bit/byte patterns within IP packets can provide an effective attack-mitigation strategy. It is not intended to replace an effective IDS/IPS deployment strategy. However, under circumstances where a unique packet-classification scheme can be developed, and an IDS/IPS signature is not available (or is not deployed) and ACLs or firewalls cannot provide the appropriate responses, FPM may fulfill the required filtering services. For example, using FPM you can block Skype and other P2P applications, worms, viruses, and new and existing attacks. In order to apply an FPM policy, you must first determine the characteristics of the attack or the application to block and then use this information to develop your match-criteria within an FPM policy. Some of these examples are shown in the next page.

Cisco IOS Flexible Packet Matching

Value-Added Security Services in Cisco IOS Software

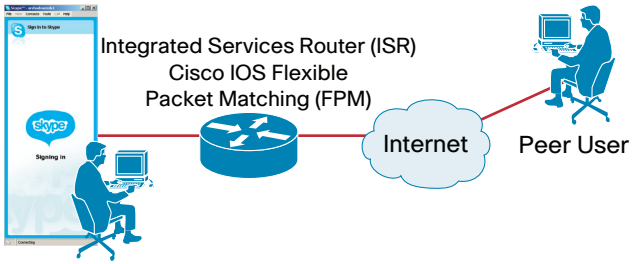
Cisco Flexible Packet Matching (FPM) to block Skype or other P2P applications

Cisco IOS Flexible Packet Matching (FPM) can be used to block peer-to-peer VoIP applications (for example, Skype) to protect the corporate network because they can work on any network, regardless of the types of NAT, proxy, firewall, or IPS that are in place.

To block Skype, take the following steps:

1. Initiate a Skype call.
2. Skype routes the call through the Internet. Capture packet flow using a Network Protocol Analyzer and derive match pattern from the packet flow (unique string of bytes located at a certain offset into the packet).
3. Write Cisco FPM policy. (Please refer to the "Getting Started with Cisco IOS FPM" guide at http://www.cisco.com/go/fpm)
4. Skype calls should now be blocked and packets are no longer seen on the network protocol analyzer

Figure 2. Cisco IOS Flexible Packet Matching (FPM) Blocking Skype

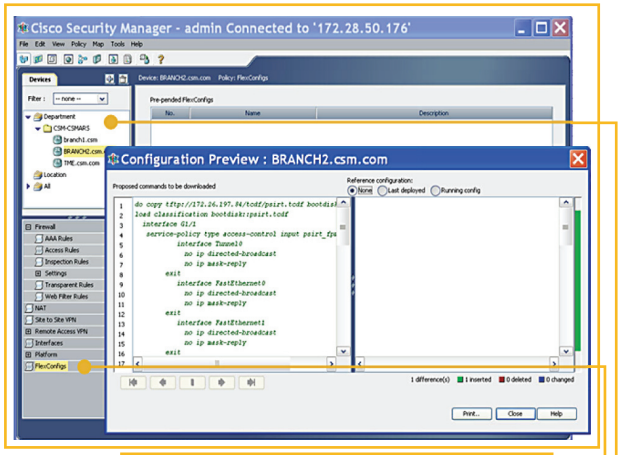


1. User initiate Skype call to peer user
2. Skype first register and then route the call through the Internet regardless of current configuration in router (NAT, Firewall, etc.).
3. Packets can be captured using a Network Protocol Analyze Match pattern is derived from the packet (unique string of bytes located at a certain offset into the packet
4. PHDF files are loaded—Load two XML files describing the protocol stack (IP and TCP)
5. Filter is configured—Using the appropriate fields from the protocols described in their PHDF files, matching pattern traffic class and its associated policy-map “drop” action is configured
6. Policy is applied to the appropriate interface.
7. Skype calls should be blocked and packets are no longer seen at the Network Protocol Analyzer

Deploying Cisco IOS Flexible Packet Matching (FPM) Using Cisco Security Manager

Cisco IOS Flexible Packet Matching (FPM) policy can be provisioned from Cisco Security Manager using a FlexConfig template for multiple devices. Cisco Security Manager is a powerful but very easy-to-use solution to centrally provision all aspects of device configuration and security policies for Cisco firewalls, VPNs, IPS, and FPM.

Figure 2. Cisco IOS Flexible Packet Matching (FPM) Positioning Using Cisco Security Manager



Cisco IOS Flexible Packet Matching (FPM) to block Slammer

Slammer is a worm that exploits a connectionless UDP protocol rather than a connection-oriented TCP protocol. The entire work fits in a single packet. Using similar steps as in the Skype example, Cisco IOS Flexible Packet Matching (FPM) policy can be created to and applied at the necessary interface to block such worms and minimize the impact to business.

Figure 1 Blocking Slammer Attack