Cisco IOS Software
Security: Flexible Packet Matching

Top Security Challenges 2006

1. Data protection
2. Vulnerability security
3. Policy and regulatory compliance
4. Identity theft and information leakage
5. Viruses and worms
6. Risk management
7. Access control
8. User education, training, and awareness
9. Wireless infrastructure security
10. Internal network security and insider threats

According to IDC, increasing sophistication of attacks and complexity of security management will increase the need for more integrated and proactive security solutions.
The Evolution of Threats

**Broad Outbreaks**
- Broad scope
- IT burden
- User challenges

But …
- Automated processes required
- User self-reliance

**Targeted Attacks**
- Narrow scope
- Business loss
- User transparency

But …
- Nearly invisible
- Little user knowledge

**Effect on Productivity**

**Potential Damage**

Antivirus
Layer 3/4 Firewall

Flexible Packet Matching
Intrusion Prevention
Behavioral Analysis
Controlling Internet Threats
The Cost of Downtime

Cost of Downtime

- Employee productivity
- Lost sales opportunity
- Lost customers, loss of reputation
- Cost of restoring system, analysis

Profit-draining potential
A mere minute of downtime can bring big losses.

<table>
<thead>
<tr>
<th>Business application</th>
<th>Estimated outage cost-per-minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply chain management</td>
<td>$11,000</td>
</tr>
<tr>
<td>E-commerce</td>
<td>$10,000</td>
</tr>
<tr>
<td>Customer service</td>
<td>$3,700</td>
</tr>
<tr>
<td>ATM/POS/EFT</td>
<td>$3,500</td>
</tr>
<tr>
<td>Financial management</td>
<td>$1,500</td>
</tr>
<tr>
<td>Human capital management</td>
<td>$1,000</td>
</tr>
<tr>
<td>Messaging</td>
<td>$1,000</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>$700</td>
</tr>
</tbody>
</table>

Source: Alinean, 2004
Self-Defending Network Defined

Efficient Security Management, Control, and Response

Technologies and Security Services to:
- Mitigate the effects of outbreaks
- Protect critical assets
- Ensure privacy
- Security becomes an integral, fundamental network capability.
- Embedded security uses network investment to best advantage.

Operational Control

Confidential Communications

Secure Transactions

Threat Control

Secure Network Platform
Cisco Flexible Packet Matching (FPM)
Cisco Security Router Technologies

Cisco® Security Routers

Secure Network Solutions
- Business Continuity
- Secure Voice
- Secure Mobility
- Compliance

Integrated Threat Control
- Advanced Firewall
- URL Filtering
- Intrusion Prevention
- Flexible Packet Matching
- Network Admission Control
- 802.1x
- Network Foundation Protection

Secure Connectivity
- GET VPN
- DMVPN
- Easy VPN
- SSL VPN

Management and Instrumentation
- SDM
- Role-Based Access
- NetFlow
- IP SLA
Top Security Challenges 2006

1. Data protection
2. Vulnerability security
3. Policy and regulatory compliance
4. Identity theft and information leakage
5. Viruses and worms
6. Risk management
7. Access control
8. User education, training, and awareness
9. Wireless infrastructure security
10. Internal network security and insider threats

Where Cisco® FPM Can Help

Source: CSI/FBI 2006
Computer Crime and Security Survey

According to IDC, increasing sophistication of attacks and complexity of security management will increase the need for more integrated and proactive security solutions.
Cisco Flexible Packet Matching

First Line of Threat Control at Branch Office and Campus

- Cisco® FPM offers a rapid first line of defense against threats and notable worms and viruses.
- Create your own custom filter or use a predefined filter library from Cisco to identify notable attacks and applications.
- Cisco FPM offers Layer 2–7 deep packet inspection with the ability to log or drop.

Cisco.com/go/fpm
Cisco Flexible Packet Matching

Rapid Response to New and Emerging Attacks

- Network managers require tools to filter day zero attacks, e.g., before IPS signatures are available.
- Traditional ACLs are not granular enough – legitimate traffic could be blocked.
  Example: Stopping Slammer with ACLs meant blocking port 1434; i.e., it denied business transactions involving Microsoft SQL.
- Cisco® FPM delivers flexible, granular Layer 2–7 matching.
  Example: Port 1434 + Packet length 404B + Specific pattern within payload → Slammer
- Cisco FPM is useful for security incident response teams for quickly reacting to threats targeting the network.

Flexible Classification and Rapid Response

- Cisco FPM goes beyond static attributes – specify arbitrary bits or bytes at any offset within the entire packet (payload or header).
- Classify on multiple attributes within a packet.
- Set up custom filters rapidly using XML-based policy language.
Cisco FPM Provisioning Using Cisco Security Manager

Centralized Security Management for All Security Devices (Firewall, IPS, Secure Router, etc.)

FlexConfig Option Provisions Cisco® FPM Policies to Multiple Routers and Switches
Cisco FPM Case Study
Blocking Slammer Attack

1. Find the Attack Vector
   (PISRT, SANS, Internet Storm Center, etc.)

2. Define Cisco® FPM Filter Policy

   Class-map type access-control match-all slammer_class
   match field udp dest-port eq 1434
   match field ip length eq 404
   match start udp payload-start offset 196 size 4 eq 0x4011010

   Policy-map type access-control fpm_policy
   class ip_udp_class
   service-policy fpm_udp_policy

3. Deploy Cisco FPM Filter Policy
Cisco Catalyst 6500 Series Supervisor Engine 32 Programmable Intelligent Services Adapter (PISA) Overview

- **NBAR**
  - Application awareness and intelligent classification
  - Multigigabit performance

- **Cisco FPM**
  - Rapid security protection
  - Multigigabit performance

- **Programmable architecture**
  - Transparent new service adoption

- **Full integration with:**
  - IPv4 and IPv6 in hardware
  - Advanced multicast and MPLS
  - Enhanced manageability
  - High availability with NSF/SSO and more
Cisco FPM on Cisco Catalyst 6500 Series Supervisor Engine 32 PISA

Capabilities
- Cisco® FPM accelerated in hardware
- Offers flexible and granular Layer 2–7 pattern matching
- Can inspect up to 8 Kb per packet
- Can block or log traffic

Benefits
- Protects against threats and notable worms and viruses
- Controls day zero threats
- Stops threats at access switch
Cisco FPM – Deployment Scenarios
Cisco FPM in Campus Network

- Protect against worms and viruses at all network entry points:
  - LAN access
  - WAN edge
- Deploy as close to the edge as possible.
- Rapidly respond to new and emerging attacks before they spread to other parts of the network.
Cisco FPM in Branch Office

- Control worms, viruses, and spyware right at the remote site; conserve WAN bandwidth.
- Enforces business policy by blocking communications and file-sharing applications such as Skype and Gnutella.