Intrusion Prevention System Modules for Integrated Services Routers

Cisco IPS AIM and IPS NME Overview for Business Decision Marker

Tina Lam, Product Manager, Cisco Systems
Organizational Impacts of Security Threats

Security Threats

- Distributed Denial of Service
- Virus out-break
- Random or direct theft
- Break-in, espionage
- Web-site defacement
- Customer information leak

Who Sees the Pain

- Disruption impacts productivity
  - CIO Problem
- Loss Impacts value
  - CFO Problem
- Loss damages customer, shareholder confidence, company reputation
  - CEO Problem
Reducing the Grey:
Uncertainty Equals Risk and Cost

GOOD: Allow

RELEVANT: Pass and Log

SUSPICIOUS: Pass and Alarm

BAD: Block

Inefficient; Highly Manual

Self-Defending Network

Efficient Operations; Effective Security

NAC Traffic Shaping IPS

Monitoring and Correlation

IPS, Anti-X, DDoS, Firewall

GOOD: Allow

Relevant: Pass and Log

Suspicious: Pass and Alarm

BAD: Block
Cisco Intrusion Prevention Strategy

Comprehensive Threat Protection for the SDN

- Cisco Security Agent
- Cisco Integrated Services Routers
- Cisco ASA 5500 Adaptive Security Appliance
- Cisco IPS 4200 Series
- Cisco Catalyst® Services Modules
- Cisco Security MARS
- Cisco Security Manager

**Integrated**

**Location Matters**
- The most diverse line of IPS sensors: the right tool for the right job, anywhere in the network
- IPS integrated into the fabric of the network
- Built on Cisco security and network intelligence

**Adaptive**

**Focused Protection**
- Modular inspection engines: respond rapidly with minimal downtime
- Behavioral anomaly detection: protect against zero-day attacks
- Dynamic risk-based threat rating: adapt threats policy in real time

**Collaborative**

**Better Together**
- On-box and network-wide correlation to provide greater accuracy and confidence
- Endpoint and network sensors sharing live network information
- Reduced operational costs with a common, solution-based management interface
Intrusion Prevention System (IPS)
Advanced Integration Module and Network Module

Accelerated Threat Control for Cisco® ISR

- Enables inline and promiscuous Intrusion Prevention (IPS)
- Runs same software (CIPS 6.1) and enables same features as Cisco IPS 4200
- Performance improvement by hardware acceleration; dedicated CPU and DRAM to offload host CPU
  - AIM—Up to 45 Mbps
  - NME—Up to 75 Mbps
- Device management through Cisco IPS Device Manager (IDM), Cisco Configuration Professional (CCP); network-wide management through Cisco Security Manager (CSM)
- Supported by IPS Manager Express (IME) and CS-MARS on event monitoring and correlation
Cisco IPS Product Portfolio

IPS 4200 Series
Dedicated appliances for high performance, data center, and focused function environments

Cisco Catalyst 6500 Series
Switch Integrated Service Modules for data center and switch integration

ASA 5500 Series
Firewall-integrated for comprehensive security and Unified Threat Management

ISR Series Routers
Remote Office/Branch services for scalable remote office protection

Performance
Branch Needs for Self-Defending Network

**Trends**
- PCI Compliance (Retail); HIPAA (Healthcare); Sarbanes-Oxley/GLBA (Finance)
- Prone to attacks from split tunnels, contaminated laptops and rogue APs

**Security**
- Moves protection to the edge before threats enter corporate or SP network
- Helps to manage unmanaged devices

---

**Threats**
- Employees 192.168.1.x/24
- Wireless Guests 192.168.2.x/24

**Protection**
- Protect Servers at Branch
  - Servers 192.168.3.14-16/24
- Protect WAN Link and Upstream Corporate Resources
  - IPSec Tunnel
- ISR with IPS AIM or IPS NME
- Corporate Office

**Networks**
- Internet
- Upgrade Corporate Resources
- Employees 192.168.1.x/24
- Wireless Guests 192.168.2.x/24

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential
Benefits of Integrated IPS on ISR

- Full feature, high performance threat protection in the Branch or SMB network
- Requires no additional footprint, cabling, and power requirements
- Systems integration with data, security and voice features on ISR
- Supports any routed WAN link—transport agnostic: T1/E1, T3/E3, Ethernet, xDSL, MPLS, 3G WWAN
- Provides defense-in-depth to the perimeter of the network: ICSA-certified Cisco IOS Firewall, IPSec and SSL VPN, NAC, URL Filtering
Securing Cisco Unified Communication Manager and Phones with Cisco IPS

- In-line inspection of voice and video traffic
- Protect infrastructure that voice runs on:
  - Protect Call Management infrastructure from attack
  - Real-time anomaly detection for day-zero threats
  - Drop calls that are coming from IP addresses identified on the Cisco Security Agent “watch list”
- Complements firewall application inspection technology
  - Cisco IPS’ Risk-Based Policy enables easy management of IPS by non-experts

Protection against:
- Application misuse
- DoS/hacking
- Known attacks
- Zero-day attacks
- Viruses/worms, spyware infecting traffic
Cisco High-Performance IPS Applications:

Wireless Intrusion Prevention

- Protect the enterprise from wireless users
  
  High-performance IPS helps protect at WLAN speeds for guest users’ and employees’ infected computers

- Selectively block malicious traffic
  
  Cisco IPS inspection services help enable accurate protection from wireless traffic

- Remove repeat offenders from the network
  
  Cisco IPS and Cisco WLAN Controllers work collaboratively to detect attackers from Layer 2 to Layer 7, and remove repeat offenders from the network
Cisco IPS Manager Express (IME)

All-in-One IPS Management Application for up to Five IPS Sensors

- **Startup Wizard:** Get up and running in just minutes
- **Dashboard:** Put needed information at your fingertips
- **Configuration:** Save time with intuitive interface
- **Reporting:** Create and share security and compliance reports
- **Monitoring:** See what’s happening with real-time and historical security events

At-a-Glance Dashboard

NEW
Cisco Security Manager
Integrated Security Configuration Management

Firewall Management
- Support for PIX®, ASA, FWSM, and Cisco IOS Routers
- Rich FW rule definition: shared objects, rule grouping, and inheritance
- Powerful analysis tools: conflict detection, rule combiner, hit counts, ...

VPN Management
- Support for PIX, ASA, VPNSM, VPN SPA, and Cisco IOS Routers
- Support for wide array of VPN technologies such as DMVPN, Easy VPN, and SSL VPN
- VPN Wizard for Three-Step Point-and-Click VPN Creation

IPS Management
- Support for IPS Sensors, modules and Cisco IOS IPS
- Automatic policy-based IPS Sensor software and signature updates
- Signature Update Wizard allowing easy review/editing prior to deployment

Reduce OpEx
- Unified security management for Cisco devices supporting FW, VPN, and IPS
- Efficiently manage up to 5000 devices per server
- Multiple views for task optimization
  - Device View
  - Policy View
  - Topology View
Cisco Services for IPS
Rapid Signature Updates for Emerging Threats

- Follow-the-Sun Research:
  Extensive around-the-clock research capability gathers, identifies and classifies vulnerabilities and threats

- Rapid Response:
  Signatures are created to mitigate the vulnerabilities within hours of classification

- Human Intelligence:
  Applied Intelligence Reports provide insight and guidance on using IPS technology to protect yourself
Cisco Security IntelliShield Alert Manager Service

Now Includes **IPS Signature-to-Threat Correlation**

- Complete vulnerability and threat information in a single database
- Notification of only those vulnerabilities relevant to a pre-defined infrastructure
- Actionable alerts in a standardized format based on user-customized profiles
- Each vulnerability or threat is analyzed and validated by security analysts
- Vulnerability and threat information is vendor-neutral and objectively graded
- Comprehensive library of over 10,000 threats and vulnerabilities
- Built-in workflow allows easy management of tasks and remediation efforts
Cisco License Manager

- **Automates license management for IPS AIM, IPS NME and more**
- **Increased productivity**
  - Rapidly *roll out* new services—500 licenses deployed in two minutes
  - *Scales* to 30,000 devices
- **Enhanced Security and Virtualization**
  - Role-Based Access Control via user roles
  - Access Control Lists limit access to PAKs and Devices
- **Reduced complexity**
  - Automated licensing workflows
  - License reports aid in audit compliance
- **Investment protection**
  - Full-functionality Java and Perl Software Development Kits (SDK) to integrate with existing applications
- **Faster failure recovery**
  - Restore device licenses from database backup
  - Resend all licenses from Cisco.com and deploy them quickly