Cisco Intrusion Prevention Solution Overview

Barbara Fraser
Corporate Consulting Engineering
Today’s Discussion

1. Introduction, Context and Vision
2. Cisco IPS Product Portfolio
3. Cisco IPS Solution Update
4. IPS Application Examples
5. Management and Signature Services
The Evolution of Intent
From Hobbyists to Professionals

Threats Becoming Increasingly Difficult to Detect and Mitigate

- **Testing the Waters:**
  - Basic Intrusions and Viruses

- **Fame:**
  - Viruses and Malware

- **Financial:**
  - Theft and Damage

What’s Next?
The Result: The Growing Costs of Security
Disruption, Loss, and Damage

Disruption Affects Productivity (the CIO Problem)
• Employee Disruption and Application Outages
• Business Process Downtime

Loss Impacts Value (the CFO Problem)
• Risk and Liability Management
• (Non) Compliance Costs

Damage Affects Reputation (the CEO Problem)
• Customer Satisfaction and Retention
• Investor and Partner Confidence
One Recent Survey

Security technologies used by respondents:

- 98% anti-virus software
- 97% firewall technology
- 69% intrusion detection
- 47% intrusion prevention

52% experienced a breach!

Reducing the Grey: Uncertainty Equals Risk and Cost

GOOD: Allow

RELEVANT: Pass and Log

SUSPICIOUS: Pass and Alarm

BAD: Block

NAC
Traffic Shaping
IPS

GOOD: Allow

Monitoring & Correlation

Suspicious: Pass and Alarm

IPS, Anti-X, DDoS, Firewall

BAD: Block

Efficient Operations Effective Security

Inefficient; Highly Manual

Self-Defending Network
Cisco Intrusion Prevention Strategy
Comprehensive Threat Protection for the SDN

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

Adaptive
• Modular inspection engines: Rapid response with minimal downtime
• Behavioral anomaly detection: Protects against day-zero attacks
• Dynamic risk-based threat rating: Adapt threats policy in real time

Collaborative
• Greater confidence through on-box and networkwide correlation
• Greater visibility and effectiveness through network and endpoint collaboration
• Reduced operational costs with a common, solution-based management interface
Today’s Discussion

1. Introduction, Context and Vision
2. Cisco IPS Product Portfolio
3. Cisco IPS Solution Update
4. IPS Application Examples
5. Management and Signature Services
Cisco IPS Product Portfolio
New Cisco IPS 4270 Sensor
Relentless Performance for the Human Network

• Protecting media-rich environments
  4 Gbps of protection for Web content, video, data replication, and other media-rich environments

• Protecting transactional environments
  2 Gbps and 20,000 transactions per second of protection for e-Commerce, voice, IM, and other transactional environments

• Protecting the data center
  High-density interface support that brings high-performance IPS to the data center

New High-Performance IPS from the IPS Market Leader

Source: Infonetics Q2CY07 Network IDS/IPS Market Share
Cisco IPS has been Number 1 market share holder for 4 consecutive quarters
Cisco ASA 5500 Series IPS Edition

Product Highlights
• Integrated Firewall and IPS
• Complete IPS feature set
• Ease of management
• Comprehensive, timely Signature coverage

Benefits
• Ease of deployment
• Ease of manageability
• Highest security protection
• Investment protection
Flexible Deployment: IPS Throughout the Environment

- Holistic network security solution
- IPS at all points in the network
- ASA integration (FW and IPS)
- Branch-office integration (Cisco ISR)
- Common Policy Management
- Comprehensive, timely signature coverage
Today’s Discussion

1. Introduction, Context and Vision
2. Cisco IPS Product Portfolio
3. Cisco IPS Solution Update
4. IPS Application Examples
5. Management and Signature Services
Cisco Intrusion Prevention Services

- **Intelligent Detection**
  - Vulnerability and Exploit specific Signatures
  - Traffic and Protocol Anomaly Detection
  - Heuristics (Statistical based algorithms)
  - Knowledge base Anomaly Detection

- **Precision Response**
  - Risk Management-based Policy
  - On-box Correlation through Meta Event Generator
  - “Trustworthiness” Linkages with the Endpoint

- **Flexible Deployment**
  - Passive and/or Inline with Flexible Response (IDS/IPS)
  - Sensor Virtualization
  - Physical and logical (VLAN) interface support
  - Software and Hardware bypass
Cisco IPS Architecture
Intelligent Detection and Precision Response

Cisco Threat Intelligence Services

Signature Updates

Engine Updates

Context Data

Network Context Information

Attack De-obfuscation
• Normalize inbound traffic to remove attempts to hide an attack

Modular Inspection Engines
• Vulnerability
• Exploit
• Behavioral Anomaly
• Protocol Anomaly

On-box Correlation Engine
• Meta Event Generator for event correlation

Risk-based Policy Control
• Calibrated “Risk Rating” computed for each event
• Event Action policy based on risk categories (e.g. High / Med / Low)
• Filters for known benign triggers

Mitigation and Alarm
• “Threat Rating” of event indicates level of residual risk

Virtual Sensor Selection
• Traffic directed to appropriate virtual sensor by interface or VLAN

Forensics Capture
• Before Attack
• During Attack
• After Attack

IN

OUT
Cisco IPS Intelligent Detection Capabilities: Vulnerability and Exploit-based Signatures

Adware/Spyware
- Perfect Keylogger Activity
- Hotbar Activity

DDOS/DOS
- ICMP/UDP/TCP Floods

Secure Voice
- SIP
- H323
- H225

Web Server
- Apache
- Internet Information Server (IIS)

Network, L2/3/4
- BGP
- DHCP
- DNS
- TCP/UDP
- IP
- IP Fragment

Worm/Virus/Trojan
- Blaster
- Nimda
- Sasser
- Code Red
- Slammer
- Backdoor Frenzy
- Backdoor Beast
- Backdoor Ghost
- Backdoor Illusion
- Backdoor Trojan Spirit
- Backdoor Beast
- Fatso Worm
- Kelvir Worm

P2P/IM
- AIM/ICQ
- AOL
- MSN
- Sametime
- Yahoo
- BitTorrent
- Kazaa
- eDonkey
- Jabber

Reconnaissance
- ICMP host sweeps
- TCP Port Sweeps
- TCP/UDP Combo Sweeps
- UDP Port Sweeps

Email
- POP
- IMAP
- SMTP
- Microsoft Exchange
Real-Time Anomaly Detection for Day Zero Threats

- Anomaly detection algorithms to detect and stop Day-Zero threats
- Real-time learning of normal network behavior
- Automatic detection and policy-based protection from anomalous threats to the network
- **Result:** Protection against attacks for which there is no signature
Real-Time Risk-based Policy
Risk Rating and IPS Policy

A quantitative measure of each threat before IPS mitigation

Risk Rating

- Event Severity: Urgency of threat?
- Signature Fidelity: How Prone to false positive?
- Attack Relevancy: Important to attack target?
- Asset Value of Target: How critical is this destination host?
- Network Context: What additional risk information is available?

= Risk Rating

IPS Policy Action

- RR < 34: Alarm
- RR > 35 and < 84: Alarm and Log Packets
- RR > 85: Deny Attacker

= IPS Policy Action
Endpoint Attack Relevance Visibility
Increasing the Fidelity of Risk-based Policy

- Attack target contextual information used to refine security response
- Contextual information gathered through:
  - Passive OS fingerprinting
  - Static OS mapping for exception handling
  - CSA Linkages
- Dynamic Risk Rating adjustment based on attack relevance
- **Result:** More appropriate and effective security response actions
Network-Endpoint Collaboration
Increasing the Fidelity of Risk-based Policy

- Cisco Security Agent (CSA) provides data on suspicious hosts through Watch List (Network Context)
- IPS Sensor risk sensitivity increased dynamically for suspicious hosts (risk rating increase)
- **Result:** Improved risk management

1. Attacker tries to brute force attack an internal server
2. CSA blocks the attack and adds attacker to its watchlist
3. CSA collaborating with Cisco IPS is able to dynamically elevate the Risk Rating threshold for attacks coming from the attacker
4. Future attacks from hacker are blocked at the IPS device
Threat Rating
Prioritize Incident Response Efforts by Residual Risk

A quantitative measure of each threat after IPS mitigation

IPS Policy:
RR > 85 → Deny Attacker

Risk measurement is updated based on IPS policy actions
• High risk attacks that have been denied no longer require urgent operator attention
• Prioritize incident response on Events with high Residual Risk

Example:
• Event 2: Very high Risk Rating, but denied by policy
  → Low urgency, low Threat Rating
• Event 4: Quite high Risk Rating, but not high enough to deny
  → Higher urgency and Threat Rating

Result: Increased efficiency of response and productivity of operations by automatic prioritization of high risk incidents
Flexible Deployment: Sensor Virtualization
Virtualize Both Policy and Sensor State

- **Flexible Context Definitions**: Ability to define virtualized sensors based on physical interface and VLAN groupings
- **Assignment of Custom Signature / Policy Settings & response actions** to each virtualized sensor

Customized policy on Virtual Sensors based on **VLAN groupings**

Customized policy on Virtual Sensors based on **Interface groupings**
Today’s Discussion

1. Introduction, Context and Vision
2. Cisco IPS Product Portfolio
3. Cisco IPS Solution Update
4. IPS Application Examples
5. Management and Signature Services
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.
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 ASA 5500 with IPS: Threat Protected VPN
Protecting the VPN Threat Vector

Application Firewall and Access Control
- Application Inspection/Control
- Granular, Per-User/Group Access Control
- Protocol Anomaly Detection
- Stateful Traffic Filtering

Worm/ Virus
Spyware
Exploit

Remote Access
VPN User

Unwanted Application
Illegal Access

Comprehensive Endpoint Security
- Pre-Connection Posture Assessment
- Malware Mitigation
- Session/Data Security
- Post-Session Clean-Up

Accurate Enforcement
- Real-Time Correlation
- Risk Rating
- Attack Drop
- Session Removal and Resets

Threat Mitigation
- Malware Detection
- Worm Detection
- Spyware Detection

Leverages Depth of Threat Defense Features to Stop Malicious Worms, Viruses, and More…and Without External Devices or Performance Loss!
Today’s Discussion

1. Introduction, Context and Vision
2. Cisco IPS Product Portfolio
3. Cisco IPS Solution Update
4. IPS Application Examples
5. Management and Signature Services
Small Deployment Management and Troubleshooting: IPS Device Manager

**Device Information**

- Host Name: Ithaca-4240
- IP Address: 10.0.8.72
- IPS Version: 6.0(3)3I184.0
- Device Type: IPS-4240-K9
- IDM Version: 5.8.0.0
- Total Memory: 1803 MB
- Bypass Mode: Auto_off
- Total Data Storage: 0KB
- Missed Packets: 0
- Total Bandwidth: 4

**Interface Status**

- Management: Up, Enabled: Yes, Auto 100: Unplugged
- GigabitEthernet0/0: Up, Enabled: Yes, Auto 1000: Unplugged
- GigabitEthernet0/1: Up, Enabled: Yes, Auto 1000: Unplugged
- GigabitEthernet0/2: Down, Enabled: Yes, Unplugged

**System Resources Status**

- CPU Usage (percent): 9%
- Memory Usage (MB): 420.9 (5.9 GB)

**Alert Counts**

- Info: 734
- Low: 9
- Mod: 0
- High: 3
- TR > 90: 0

**Alert Profiles**

- Alert Profile

IDM is initialized successfully.
Small Deployment Robust Monitoring and Event Viewing: IPS Event Viewer

- Support for IPSv6 through SDEE compatibility
- Customizable Reporting
- Tunable Notification Actions
- Visibility into applied Response Actions, Virtual Sensor ID, Learned DST OS & Threat Rating
Cisco Security Management Suite

Cisco Security Manager

- Simplified Policy Administration
- End-to-End Configuration
- Network-Wide or Device-Specific

Cisco Security Mars

- Rapid Threat Identification and Mitigation
- Topology Awareness
- Data Correlation

- Self-Defending Network

- Integration to Cisco Secure Access Control Server
  - Role-based access control
  - Privilege-based access to management functionality

- With the context of auditing services
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
Summary

• Threats result in disruption, loss, and damage to your organization

• Network Intrusion Prevention is a fundamental element to your security strategy

• Cisco IPS protects your organization from malware and attackers as an integrated, collaborative, and adaptive network solution

• Cisco IPS increases the effectiveness of threat response, reduces operational costs, and increases the efficiency of security operations
Cisco IPS Resources – On the Web

Cisco IPS site: http://www.cisco.com/go/ips
Cisco Services for IPS:
Cisco Security Site: http://www.cisco.com/security/
Cisco Active Update Bulletins:
http://www.cisco.com/offer/newsletter/123668_4/
Cisco Security Advisories and Notices:
http://www.cisco.com/go/psirt