Today: Branch-Office Security Concerns

Extended Network Boundaries
- Need protection at the edge before threats enter corporate network
- Need to control guest and unmanaged devices

Effect of Compliance on IT
- IT resources leaner at branch than at headquarters
- Regulations such as PCI call for enhanced security between remote offices and headquarters

“Inherited” Security Applications and Infrastructure
- May differ from or lag behind security at headquarters
- Security policies must accommodate without increasing inconsistencies
According to *Infonetics’ the Costs Of Network Security Attack North America 2007*, the Annual Cost of Downtime Can be up to $31M For Large Corporations from Loss of Revenue and Productivity.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Small 20–100 ($K)</th>
<th>Medium 100–1000 ($K)</th>
<th>Large ($K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS Attacks ($K)</td>
<td>$11.7</td>
<td>$39.7</td>
<td>$15,578</td>
</tr>
<tr>
<td>Client Malware ($K)</td>
<td>$8.6</td>
<td>$114.5</td>
<td>$2,633</td>
</tr>
<tr>
<td>Server Malware ($K)</td>
<td>$11.3</td>
<td>$71.4</td>
<td>$13,052</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$31.7K</strong></td>
<td><strong>$225.6K</strong></td>
<td><strong>$31.2M</strong></td>
</tr>
</tbody>
</table>
# Cisco Intrusion Prevention Solution
## Comprehensive Threat Protection for the SDN

<table>
<thead>
<tr>
<th>Integrated</th>
<th>Collaborative</th>
<th>Adaptive</th>
</tr>
</thead>
</table>
| - Multivector protections at all points in the network and desktop and server endpoints | - Cross-solution feedback linkages  
- Common policy management  
- Multivendor event correlation  
- Attack path identification  
- Passive and active fingerprinting  
- Cisco Security Agent-IPS Collaboration | - Anomaly detection with in-production learning  
- Network behavioral analysis  
- On-device and network event correlation  
- Real-time security posture adjustment |

**Cisco Security Agent**

**Cisco Integrated Services Routers**

**Cisco ASA 5500 Adaptive Security Appliance**

**Cisco Catalyst ® Service Modules**

**Cisco IPS 4200 Series Sensors**

**Cisco Security MARS**

**Cisco Security Manager**

---

Cisco © Security Agent

Day Zero Endpoint Protection

Branch Protection

Converged Perimeter Protection

Integrated Data Center Protection

Server Protection

Monitoring, Correlation, and Response

Policy-Based Solution Management

---

- Cross-solution feedback linkages
- Common policy management
- Multivendor event correlation
- Attack path identification
- Passive and active fingerprinting
- Cisco Security Agent-IPS Collaboration

---

- Anomaly detection with in-production learning
- Network behavioral analysis
- On-device and network event correlation
- Real-time security posture adjustment

---

Cisco Catalyst ® Service Modules

Cisco ASA 5500 Adaptive Security Appliance

Cisco Security MARS
All-in-One Security for the WAN

Only Cisco® Security Routers Deliver All of This

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

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
Integrated Threat Control Overview
Industry Certified Security Embedded within the Network

- Secure Internet access to branch, without the need for additional devices
- Control worms, viruses and adware/spyware right at the remote site; conserve WAN bandwidth
- Protect the router itself from hacking and DoS attacks
- Protects data, voice and video, wired and wireless, and WAN acceleration services
Benefits of Integrated IPS on Cisco ISRs

- Provides network-wide, protection from many worms, viruses, and vulnerabilities
- Eliminates the need for a standalone IPS device at branch and small offices
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router
- Supports any routed WAN link; transport agnostic: T1/E1, T3/E3, Ethernet, xDSL, Multiprotocol Label Switching (MPLS), and third-generation (3G) wireless WAN (WWAN), LAN and WLAN links
- Provides defense-in-depth to the perimeter of the network: ICSA-certified Cisco IOS® Firewall, IP Security (IPsec) and Secure Sockets Layer (SSL) VPN, Cisco Network Admission Control (NAC), and URL filtering
- Integrates with data, security, and voice features on Cisco integrated services router
Cisco IOS IPS
Branch Positioning and Use Cases

Protect Branch PCs from Internet Worms
- Use IPS and Firewall on a Cisco Router for Worm Protection

Move Worm Protection to the Network Edge
- Apply IPS on Traffic From Branch to HQ to Stop Worms and Attacks From Infected Branch PCs
- Satisfy PCI Compliance Requirements

Protect Branch-Office Servers
- Apply IPS and Firewall on Branch Router to Protect Local Servers at the Branch From Attacks
- Avoid Need for a Separate Device to Protect Servers
# Latest Improvements in Cisco IOS IPS
## Cisco IOS 12.4(11)T2 and Later

<table>
<thead>
<tr>
<th>Customer Pain Points</th>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| **Quick Response**   | - NDA (encrypted) signature support and native support for MSRPC and Microsoft SMB signatures  
- Automated signature updates from a local TFTP or HTTP(S) server | - Efficient protection against many new Microsoft and other vulnerabilities, some even before their public release  
- Protection from latest threats with minimal user intervention |
| **Improved Accuracy** | - Risk Rating value in IPS alarms based on signature severity, fidelity, and target value rating  
- Supports Signature Event Action Processor (SEAP) | - Enables accurate and efficient IPS event correlation and monitoring  
- Quick and automated adjustment of signature event actions based on Risk Rating |
| **Manageability**    | - Individual and category-based signature provisioning through Cisco IOS CLI  
- IDCONF (XML) signature provisioning mechanism | - Offers granular customization and tuning of signatures through custom scripts  
- Secure provisioning through CSM 3.1 and Cisco SDM 2.4 over HTTPS |
| **Common Operations**| - Same signature format as the latest Cisco® IPS appliances and modules | - Common operations for Cisco IPS appliances and Cisco IOS® IPS |

## Customer Pain Points

### Quick Response
Reduce Timeline from Vulnerability to Signature Deployment

- NDA (encrypted) signature support and native support for MSRPC and Microsoft SMB signatures
- Automated signature updates from a local TFTP or HTTP(S) server

### Improved Accuracy
Reduced False Positives

- Risk Rating value in IPS alarms based on signature severity, fidelity, and target value rating
- Supports Signature Event Action Processor (SEAP)

### Manageability
Secure, and Simpler Signature Provisioning

- Individual and category-based signature provisioning through Cisco IOS CLI
- IDCONF (XML) signature provisioning mechanism

### Common Operations
From HQ to Branch

- Same signature format as the latest Cisco® IPS appliances and modules
## IPS Solutions on Cisco ISRs

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco IOS IPS</th>
<th>Cisco IPS AIM</th>
<th>Cisco NM-CIDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated CPU/DRAM for IPS</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Inline and Promiscuous Detection and Mitigation</td>
<td>Yes</td>
<td>Yes</td>
<td>No, Promiscuous Mode Only</td>
</tr>
<tr>
<td>Signature Supported</td>
<td>Subset of 2000+ Signatures, Subject to Available Memory</td>
<td>Full Set Signatures (2200+)</td>
<td>Full Set Signatures (2200+)</td>
</tr>
<tr>
<td>Automatic Signature Updates</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Day-zero Anomaly Detection</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Rate Limiting</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Security Agent and Cisco IPS Collaboration</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Meta Event Generator</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Event Notification</td>
<td>Syslog, SDEE</td>
<td>SNMP and SDEE</td>
<td>SNMP and SDEE</td>
</tr>
<tr>
<td>Device Management</td>
<td>CLI, SDM</td>
<td>IOS CLI, IDM</td>
<td>IPS CLI, IDM</td>
</tr>
<tr>
<td>System/Network Management</td>
<td>CSM</td>
<td>CSM</td>
<td>CSM</td>
</tr>
<tr>
<td>Event Monitoring and Correlation</td>
<td>IEV, CS-MARS</td>
<td>IEV, CS-MARS, On-box Meta Event Generator</td>
<td>IEV, CS-MARS, On-box Meta Event Generator</td>
</tr>
</tbody>
</table>

**NOTE:** Only One IPS Solution May Be Active in the Router. All Other Must Be Removed or Disabled.
Lifecycle Security Services
Prepare–Plan–Design–Implement–Operate–Optimize

Operate Phase

Protects Network Information Assets

Cisco® Intellishield Alert Manager
This Comprehensive, Cost-effective Solution Delivers Intelligence to Identify, Prevent, and Quickly Mitigate IT Attacks.

Cisco Services for IPS
Cisco Services for IPS Helps Customers Effectively Maintain Integrity And Privacy of Sensitive Information and Maximize Availability, Reliability, and Stability of Their Network While Controlling Operating Expenses.
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 predefined infrastructure
- Actionable alerts in a standardized format based on user-customized profiles
- Analysis and validation of each vulnerability or threat by security analysts
- Vendor-neutral and objectively graded vulnerability and threat information
- Comprehensive library of more than 10,000 threats and vulnerabilities
- Built-in workflow that allows easy management of tasks and remediation efforts
Cisco Services for IPS
Rapid Signature Updates for Emerging Threats

- Extensive 24-hour research capability gathers, identifies, and classifies vulnerabilities and threats.
- Signatures are created to mitigate the vulnerabilities within hours of classification.
- Signature updates are available to customers at Cisco.com.
# Cisco IOS IPS

Provisioning and Monitoring Options

<table>
<thead>
<tr>
<th>IPS Signature Provisioning</th>
<th>IPS Event Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Up to 5</td>
<td>Up to 5</td>
</tr>
<tr>
<td>More Than 5</td>
<td>More Than 5</td>
</tr>
</tbody>
</table>

- **Same Signature Set:**
  - Option 1: Cisco Security Manager 3.1
  - Option 2: Cisco SDM 2.4 and Cisco Configuration Engine

- **Otherwise:**
  - Single or multiple Cisco Security Manager 3.1 instances

  - Cisco IEV (IPS Event Viewer) or Cisco SDM
  - Cisco Security MARS 4.3.1 or 5.3.1
Cisco IOS IPS Deployment Steps

- **Step 1**: Latest Cisco IPS signature package
  
  http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup

  This package contains a digitally signed signature file that includes all the signatures for entire Cisco IPS product line

- **Step 2**: Select one of the two recommended signature categories (list of signatures): IOS-Basic or IOS-Advanced

- **Step 3**: Use IOS CLI or SDM 2.4 or CSM 3.1 to customize your signature list:
  - Select additional signatures as desired
  - Delete signatures not relevant to the applications you’re running
  - Tune actions of individual signatures (e.g., add “drop” action) as desired
  - Test your custom signature set in a lab setting before actual deployment

For Details, See IOS IPS Configuration Guide at:
Cisco IOS IPS
Ideal for Distributed Worm and Threat Mitigation

Central Signature File Management with Cisco® Security Manager 3.1

Prebuilt or Custom Signature Updates Distributed by Cisco Security Manager 3.1
Cisco Security Manager (CSM) 3.1
Cisco IOS IPS Network-wide Configuration

- Supports Cisco IOS® Software 12.4(11)T2 and later
- Signature file auto update
- Custom signature templates
- Wizards to Create and Update Signatures
- Rollback to previous Signature release and policy configuration
- Cisco® SDM and Cisco® IEV cross-launch
- Filtering based on signature category, release, fidelity or severity
- Copying IPS policies from one device to others
- Cloning signatures to create custom signatures
- Secure provisioning via IDCONF transactions over HTTPS
- Configuration of risk-based automated event action filters and overrides
Cisco Security Manager 3.1
Cisco IOS IPS Signature List View
Cisco SDM v2.4
Extensive Ease of Use Enhancements for IOS IPS

- Auto-update IPS signatures from Cisco.com
- Configure Signature, Risk Rating and Event Action Processor (SEAP) to reduce false positives
- Customize IPS signatures
- Wizard to migrate IPS 4.x format signatures to IPS 5.x/6.0 format
Cisco IOS® IPS Website:
http://www.cisco.com/go/iosips

Cisco IOS IPS enhancements and 5.x signature format support in Cisco IOS Software Release 12.4(11)T or later:

Cisco IOS IPS Data Sheet:

Cisco IOS IPS Deployment Guide:

Cisco Services for IPS: