



# Cisco IOS Intrusion Prevention System (IPS)

An Integrated Threat Control Solution

<http://www.cisco.com/go/iosips>

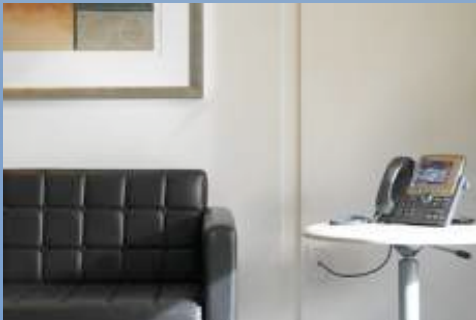


# Today: Branch-Office Security Concerns



## 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

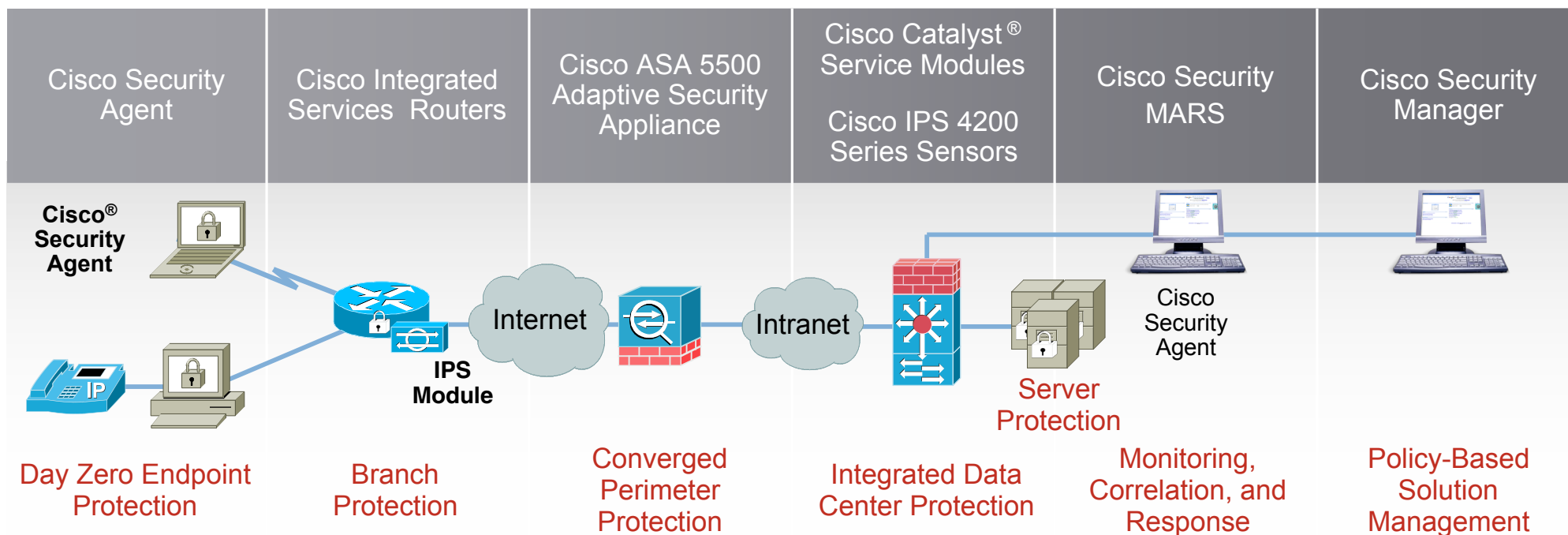
# Cost to the Organization of Different Threats

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.

	Small 20–100	Medium 100–1000	Large
DDoS Attacks (\$K)	\$11.7	\$39.7	\$15,578
Client Malware (\$K)	\$8.6	\$114.5	\$2,633
Server Malware (\$K)	\$11.3	\$71.4	\$13,052
Total	\$31.7K	\$225.6K	\$31.2M

# Cisco Intrusion Prevention Solution

## Comprehensive Threat Protection for the SDN



### Integrated

- Multivector protections at all points in the network and desktop and server endpoints

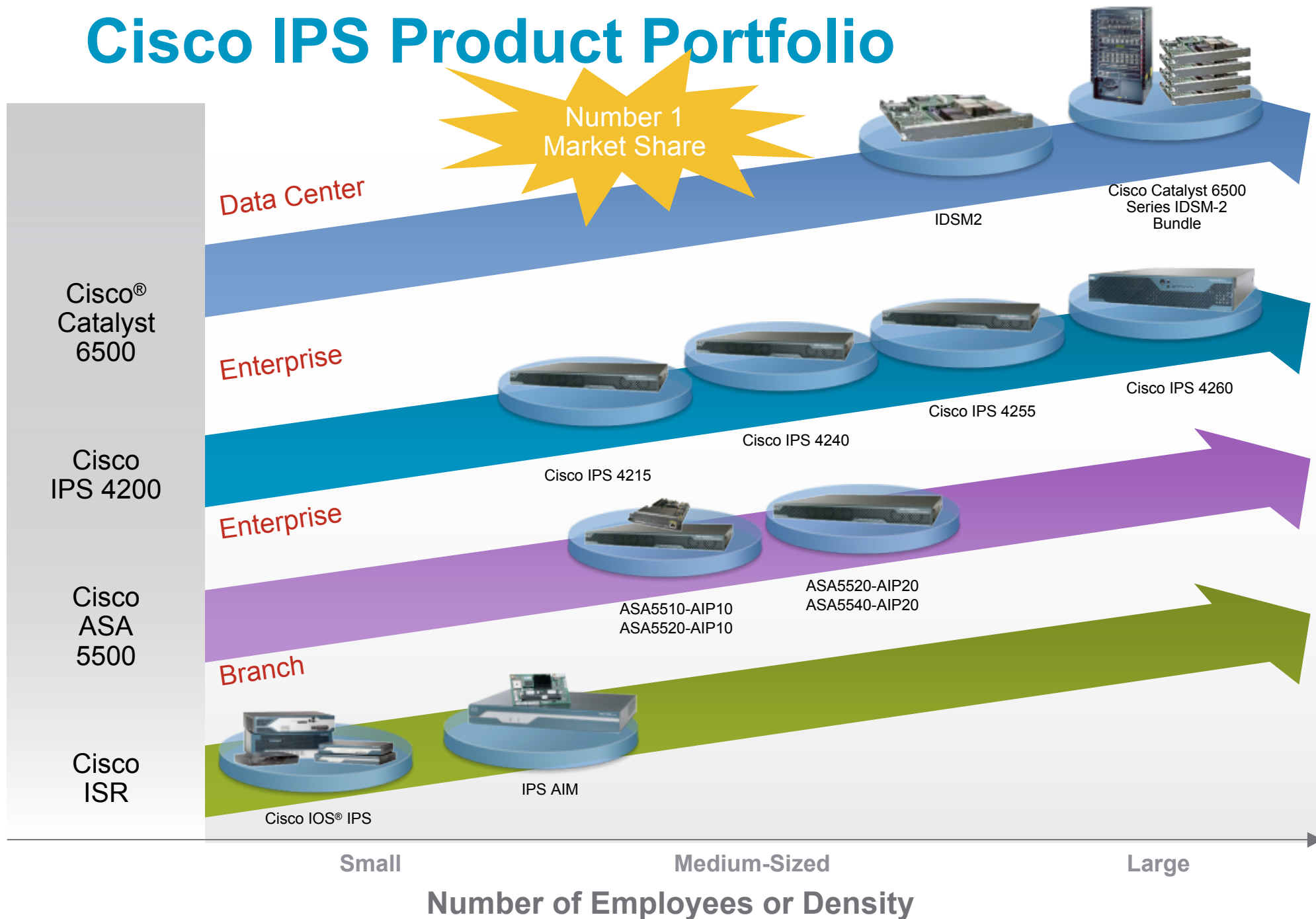
### Collaborative

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

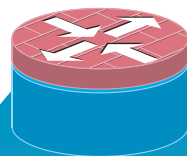
### Adaptive

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

# Cisco IPS Product Portfolio



# All-in-One Security for the WAN



Only Cisco® Security Routers  
Deliver All of This

## Secure Network Solutions



Business  
Continuity



Secure  
Voice

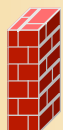


Secure  
Mobility



Compliance

## Integrated Threat Control



Advanced  
Firewall



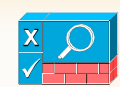
URL  
Filtering



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

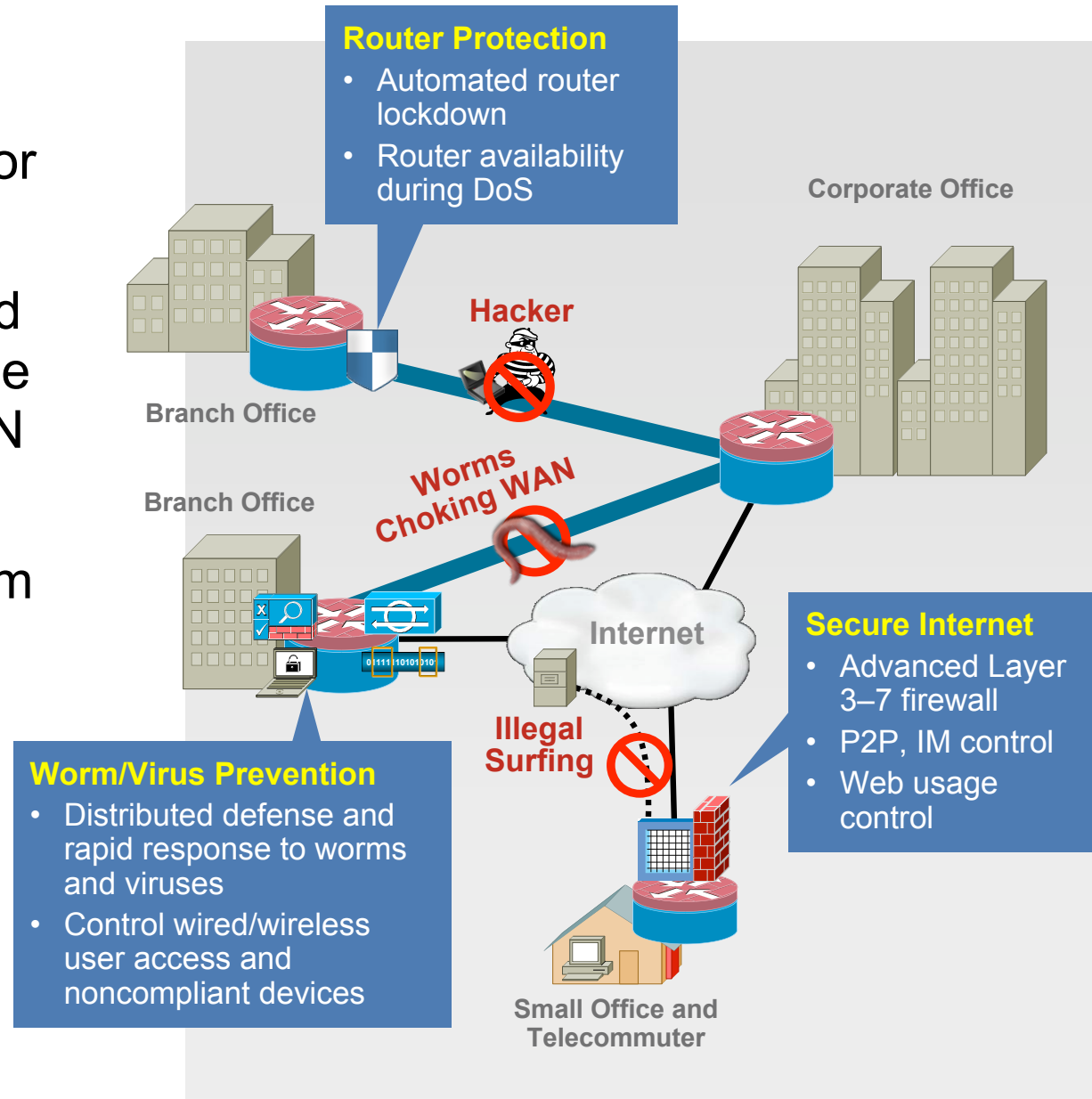


IP SLA

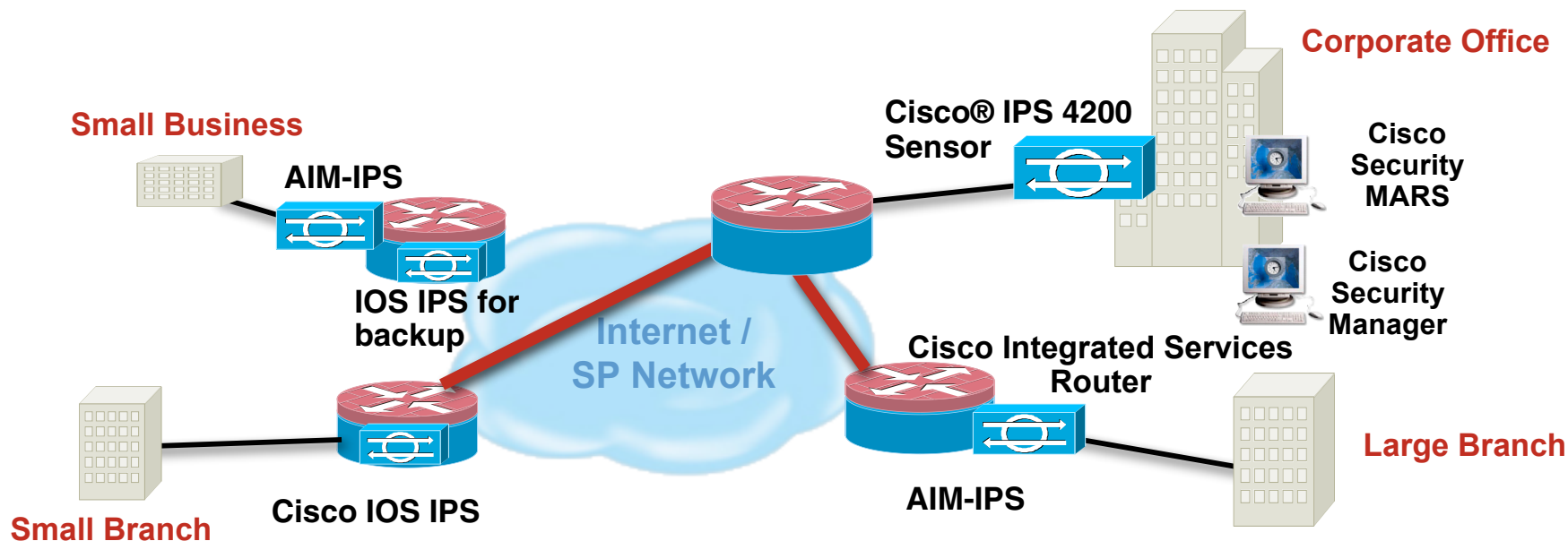
# Integrated Threat Control Overview

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



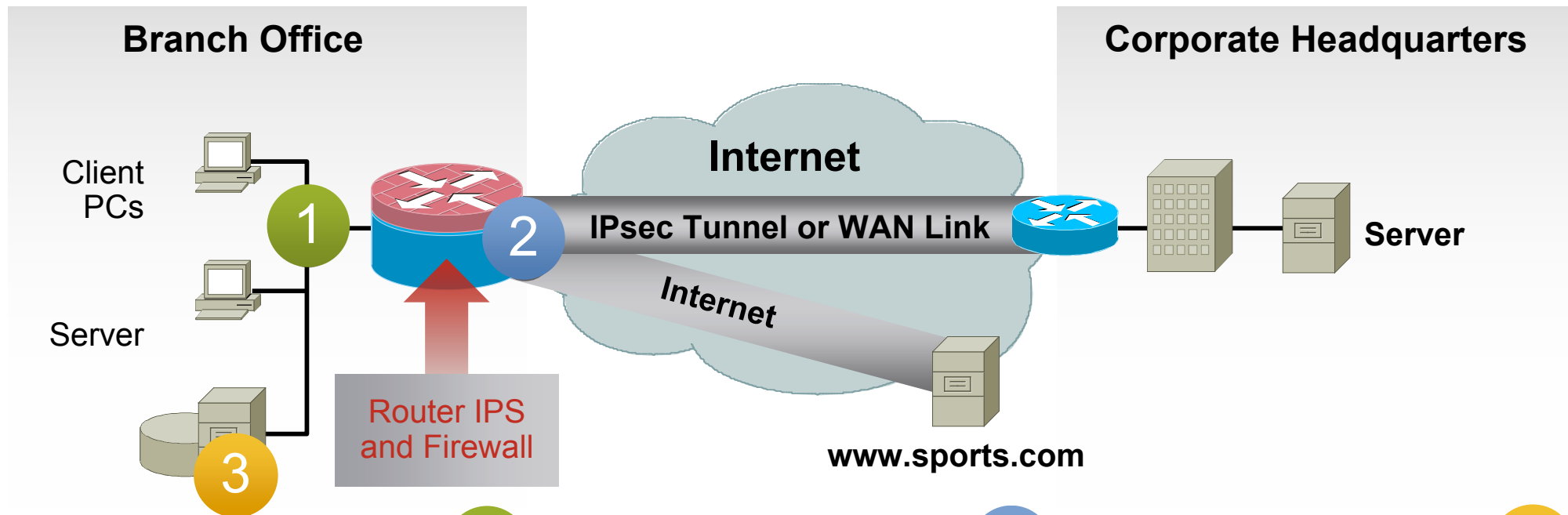
# Benefits of Integrated IPS on Cisco ISRs



- 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



### 1 Protect Branch PCs from Internet Worms

Use IPS and Firewall on a Cisco Router for Worm Protection

### 2 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

### 3 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

Customer Pain Points	Features	Benefits
<b>Quick Response</b> Reduce Timeline from Vulnerability to Signature Deployment	<ul style="list-style-type: none"> <li>▪ NDA (encrypted) signature support and native support for MSRPC and Microsoft SMB signatures</li> <li>▪ Automated signature updates from a local TFTP or HTTP(S) server</li> </ul>	<ul style="list-style-type: none"> <li>▪ Efficient protection against many new Microsoft and other vulnerabilities, some even before their public release</li> <li>▪ Protection from latest threats with minimal user intervention</li> </ul>
<b>Improved Accuracy</b> Reduced False Positives	<ul style="list-style-type: none"> <li>▪ Risk Rating value in IPS alarms based on signature severity, fidelity, and target value rating</li> <li>▪ Supports Signature Event Action Processor (SEAP)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Enables accurate and efficient IPS event correlation and monitoring</li> <li>▪ Quick and automated adjustment of signature event actions based on Risk Rating</li> </ul>
<b>Manageability</b> Secure, and Simpler Signature Provisioning	<ul style="list-style-type: none"> <li>▪ Individual and category-based signature provisioning through Cisco IOS CLI</li> <li>▪ IDCONF (XML) signature provisioning mechanism</li> </ul>	<ul style="list-style-type: none"> <li>▪ Offers granular customization and tuning of signatures through custom scripts</li> <li>▪ Secure provisioning through CSM 3.1 and Cisco SDM 2.4 over HTTPS</li> </ul>
<b>Common Operations</b> From HQ to Branch	<ul style="list-style-type: none"> <li>▪ Same signature format as the latest Cisco® IPS appliances and modules</li> </ul>	<ul style="list-style-type: none"> <li>▪ Common operations for Cisco IPS appliances and Cisco IOS® IPS</li> </ul>

# IPS Solutions on Cisco ISRs

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

**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.

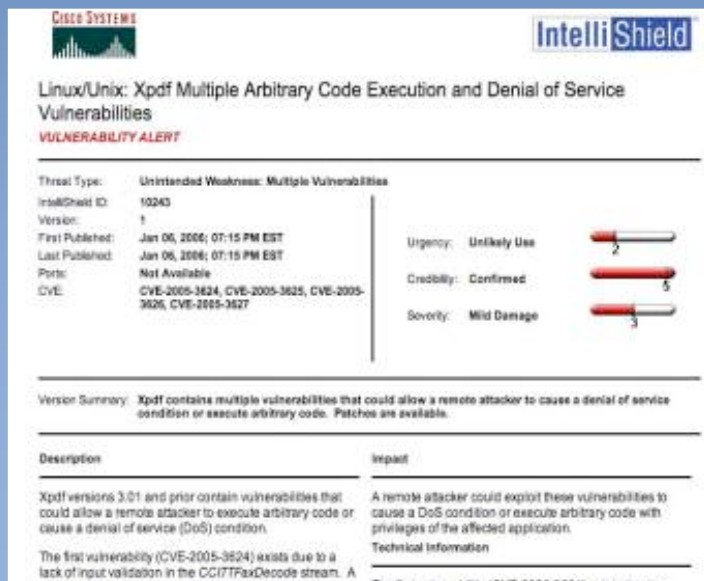
# Cisco Security IntelliShield Alert Manager Service

## Now Includes IPS Signature-to-Threat Correlation



Alert ID	Headline	Published	Version	Urgency	Credibility	Severity	Body
1096	Microsoft Edge: Multiple XSS Vulnerabilities	Apr 26 2004 3:00 PM	1	Unlikely	Confirmed	Low	Info
6966	Twitter: Open Redirect	Apr 26 2004 2:25 PM	1	Unlikely	Confirmed	Low	Info
9037	Linux/Unix: Multiple Arbitrary Code Execution Vulnerabilities	Apr 26 2004 2:10 PM	30	Unlikely	Confirmed	Low	Info
6499	Linux/Unix: Multiple Arbitrary Code Execution Vulnerabilities	Apr 26 2004 2:05 PM	17	Unlikely	Confirmed	Low	Info
7274	Linux/Unix: Multiple Arbitrary Code Execution Vulnerabilities	Apr 26 2004 2:05 PM	22	Unlikely	Confirmed	Low	Info
7296	Linux/Unix: Multiple Denial of Service Vulnerabilities	Apr 26 2004 1:50 PM	22	Unlikely	Confirmed	Low	Info
7140	Linux/Unix: Multiple Denial of Service Vulnerabilities	Apr 26 2004 1:50 PM	9	Unlikely	Confirmed	Low	Info
9042	Linux/Unix: Multiple Denial of Service Vulnerabilities	Apr 26 2004 12:40 PM	10	Unlikely	Confirmed	Low	Info
7265	Apache: Multiple Denial of Service Vulnerabilities	Apr 26 2004 12:40 PM	6	Unlikely	Confirmed	Low	Info
7266	Apache: Multiple Denial of Service Vulnerabilities	Apr 26 2004 12:30 PM	1	Unlikely	Confirmed	Low	Info
7180	Apache: Multiple Denial of Service Vulnerabilities	Apr 26 2004 12:30 PM	4	Unlikely	Confirmed	Low	Info
7181	Apache: Multiple Denial of Service Vulnerabilities	Apr 26 2004 12:21 PM	1	Unlikely	Confirmed	Low	Info
7182	Linux: Multiple Denial of Service Vulnerabilities	Apr 26 2004 11:40 AM	1	Unlikely	Confirmed	Low	Info
7183	Linux: Multiple Denial of Service Vulnerabilities	Apr 26 2004 9:50 AM	4	Unlikely	Confirmed	Low	Info
7184	Linux: Multiple Denial of Service Vulnerabilities	Apr 26 2004 9:40 AM	6	Unlikely	Confirmed	Low	Info
7185	Linux: Multiple Denial of Service Vulnerabilities	Apr 26 2004 9:30 AM	2	Unlikely	Confirmed	Low	Info
5490	Linux: Multiple Denial of Service Vulnerabilities	Apr 26 2004 9:20 AM	4	Unlikely	Confirmed	Low	Info
7186	Linux: Multiple Denial of Service Vulnerabilities	Apr 23 2004 8:10 PM	1	Unlikely	Confirmed	Low	Info
7187	Linux: Multiple Denial of Service Vulnerabilities	Apr 23 2004 2:10 PM	2	Unlikely	Confirmed	Low	Info
7243	Linux: Multiple Denial of Service Vulnerabilities	Apr 23 2004 1:21 PM	1	Unlikely	Confirmed	Low	Info

- **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 Systems** **IntelliShield**

**Linux/Unix: Xpdf Multiple Arbitrary Code Execution and Denial of Service Vulnerabilities**

**VULNERABILITY ALERT**

Threat Type: Unintended Weakness: Multiple Vulnerabilities

IntelliShield ID: 10243

Version: 1

First Published: Jan 06, 2006; 07:15 PM EST

Last Published: Jan 06, 2006; 07:15 PM EST

Port: Not Available

CVE: CVE-2005-3624, CVE-2005-3625, CVE-2005-3626, CVE-2005-3627

Urgency: Unlikely Use

Credibility: Confirmed

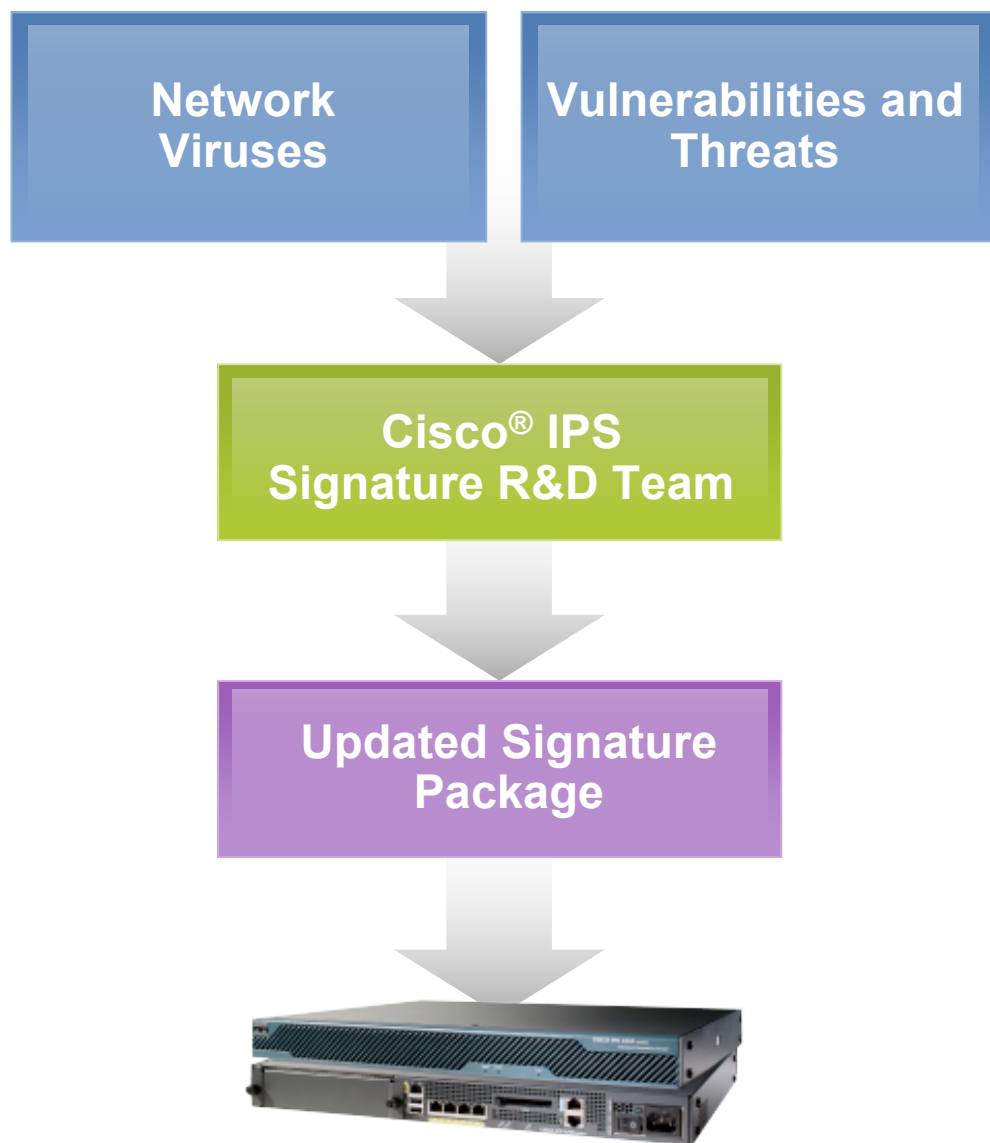
Severity: Mild Damage

**Version Summary:** Xpdf contains multiple vulnerabilities that could allow a remote attacker to cause a denial of service condition or execute arbitrary code. Patches are available.

Description	Impact
Xpdf versions 3.01 and prior contain vulnerabilities that could allow a remote attacker to execute arbitrary code or cause a denial of service (DoS) condition.	A remote attacker could exploit these vulnerabilities to cause a DoS condition or execute arbitrary code with privileges of the affected application.
The first vulnerability (CVE-2005-3624) exists due to a lack of input validation in the CCITTFaxDecode stream. A	Technical Information

# 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](http://Cisco.com).

# Cisco IOS IPS

## Provisioning and Monitoring Options

IPS Signature Provisioning		IPS Event Monitoring		
Up to 5	More Than 5	1	Up to 5	More Than 5
Cisco SDM 2.4	<b>Same Signature Set:</b>  Option 1: Cisco Security Manager 3.1  Option 2: Cisco SDM 2.4 and Cisco Configuration Engine  <b>Otherwise:</b>  Single or multiple Cisco Security Manager 3.1 instances	Cisco IEV (IPS Event Viewer)  or  Cisco SDM	Cisco IEV	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

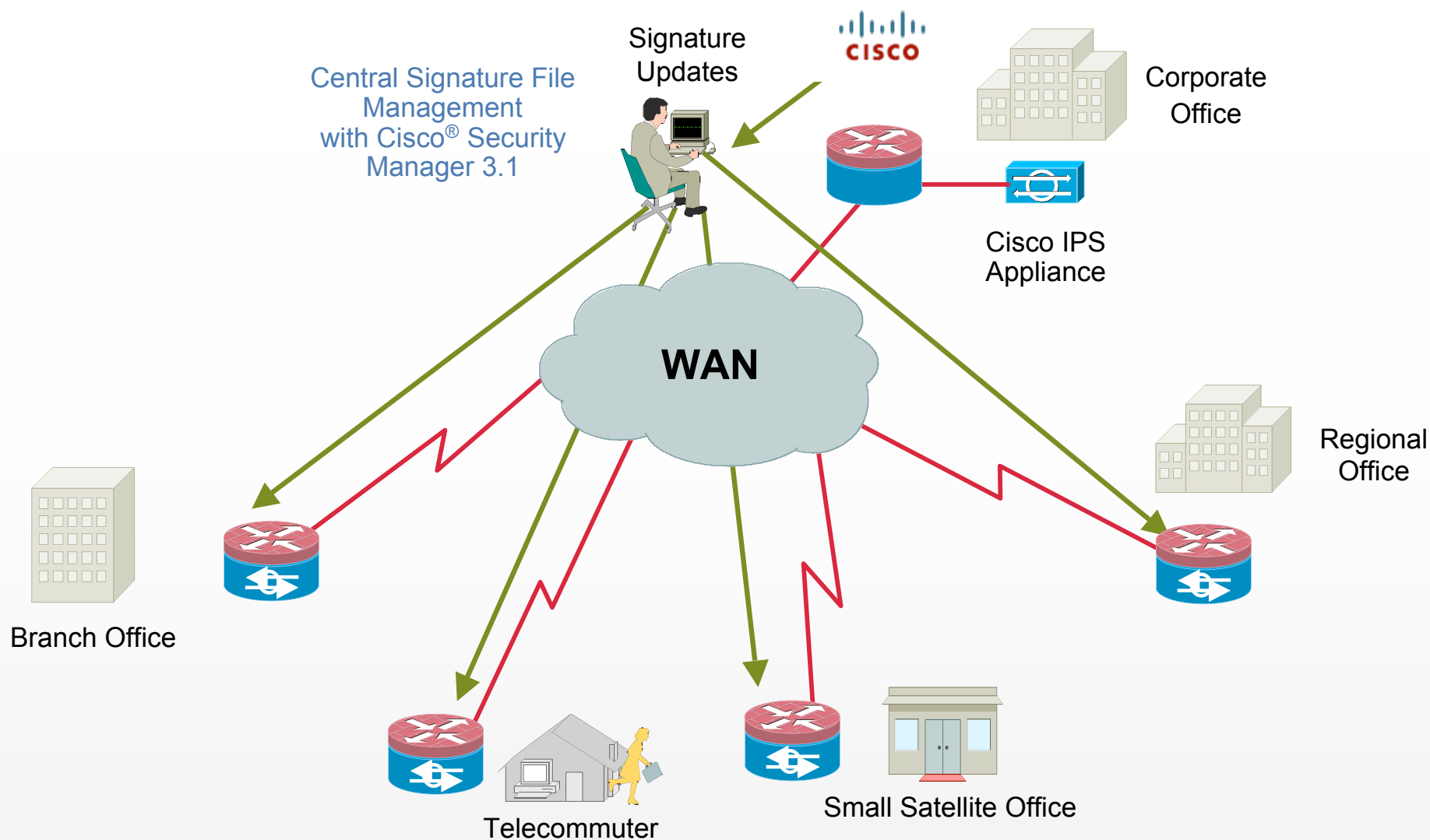
Test your custom signature set in a lab setting before actual deployment

For Details, See IOS IPS Configuration Guide at:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips\\_v5.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips_v5.htm)

# Cisco IOS IPS

## Ideal for Distributed Worm and Threat Mitigation



➡ 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

The screenshot shows the Cisco Security Manager 3.1 interface. The title bar indicates the user is connected to 'dattas-w2k06'. The menu bar includes File, Edit, View, Policy, Map, Tools, and Help. The left sidebar contains a tree view with the following structure:

- Devices
  - Filter: -- none --
  - Location
    - All
      - 10.89.33.71
      - 10.89.33.72
      - ios74-4
      - ios74-new
      - sensor39
      - Test-72
- Firewall
- IPS
- IOSIPS
  - Signatures
  - Event Actions
    - Event Action Filters
    - Event Action Overrides
    - Network Information
    - Event Action Settings
  - General Settings
  - IOS IPS Rules
  - Sensor Update
- NAT
- Site to Site VPN
- Remote Access VPN

The main area displays the 'Signatures' list for 'Device: Test-72' and 'Policy: Signatures'. The filter is set to 'Filter (Enabled = "True")' with 'Column: Enabled' and 'Criteria: True'. The table below lists the signatures:

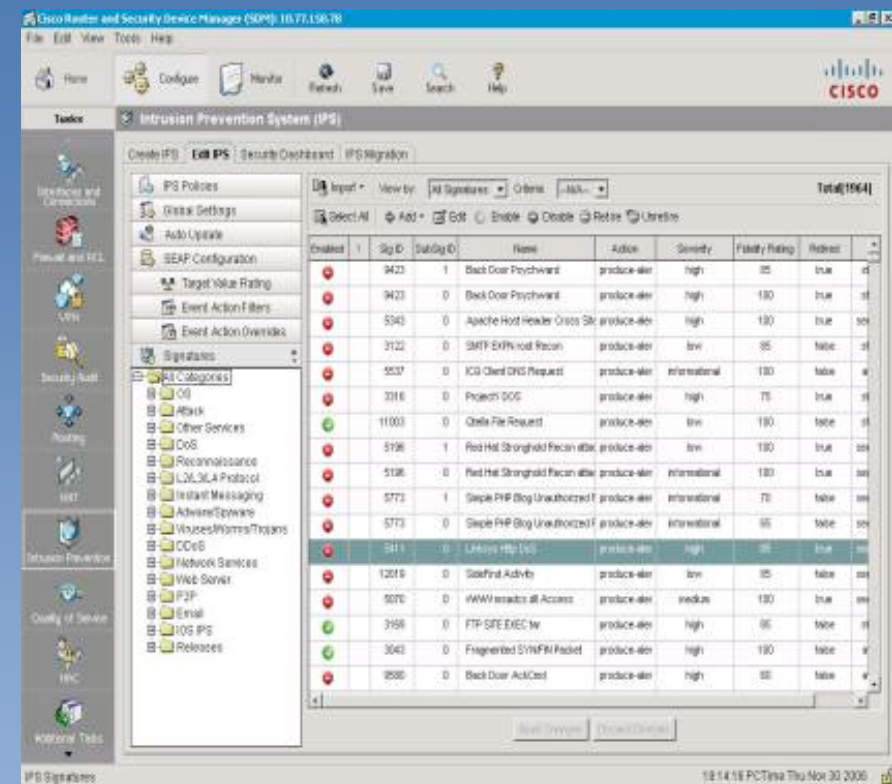
ID	Sub	Name	Actions	Severity	Fidelity	Source
1330	11	TCP Drop - Bad Checksum	produce-alert	informational	100	default
1330	12	TCP Drop - Bad Checksum	produce-alert	informational	100	default
1330	13	TCP Drop - Bad Checksum	produce-alert	informational	100	default
1330	14	TCP Drop - Bad Checksum	produce-alert	informational	100	default
1330	15	TCP Drop - Bad Checksum	produce-alert	informational	100	default
1330	16	TCP Drop - Bad Checksum	produce-alert	informational	100	default
1330	17	TCP Drop - Bad Checksum	produce-alert	informational	100	default
1330	18	TCP Drop - Bad Checksum	produce-alert	informational	100	default
1600	0	ICMPv6 zero length option	produce-alert	informational	75	default
1601	0	ICMPv6 option type 1 violation	produce-alert	informational	75	default
1602	0	ICMPv6 option type 2 violation	produce-alert	informational	75	default
1603	0	ICMPv6 option type 3 violation	produce-alert	informational	75	default
1605	0	ICMPv6 option type 5 violation	produce-alert	informational	75	default
1607	0	IPv6 multi-crafted fragments	produce-alert	informational	75	default
2100	0	ICMP Network Sweep w/Echo	produce-alert	informational	100	default
2101	0	ICMP Network Sweep w/Timest...	produce-alert	informational	100	default
2102	0	ICMP Network Sweep w/Addre...	produce-alert	informational	100	default
2152	0	ICMP Flood	produce-alert	informational	100	default

The bottom right corner of the window has a 'Save' button.

# 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 Collateral

- **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:**  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips\\_v5.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips_v5.htm)
- **Cisco IOS IPS Data Sheet:**  
[http://www.cisco.com/en/US/products/ps6634/products\\_data\\_sheet0900aecd803137cf.html](http://www.cisco.com/en/US/products/ps6634/products_data_sheet0900aecd803137cf.html)
- **Cisco IOS IPS Deployment Guide:**  
[http://www.cisco.com/en/US/products/ps6634/products\\_white\\_paper0900aecd8062acfb.shtml](http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd8062acfb.shtml)
- **Cisco Services for IPS:**  
[http://www.cisco.com/en/US/products/ps6076/serv\\_group\\_home.html](http://www.cisco.com/en/US/products/ps6076/serv_group_home.html)

