



Intrusion Prevention System Modules for Integrated Services Routers



Cisco IPS AIM and IPS NME Overview for Technical Decision Marker

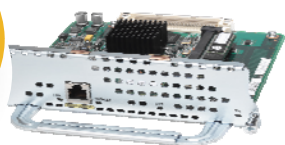
Tina Lam, Product Manager, Cisco Systems
Tom Fulton, TME, Cisco Systems

Agenda

- IPS Modules Overview
- IPS Architecture and Features
- Benefits and Use Cases
- Management and Monitoring
- Signature Update and Threat Alert

Intrusion Prevention System (IPS)

Advanced Integration Module and Network Module



NME-IPS-K9

Cisco 2811, 2821,
2851, 3800



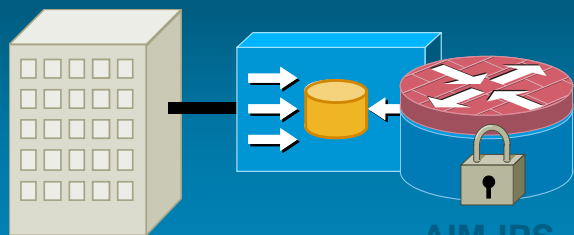
AIM-IPS-K9

Cisco 1841, 2800, 3800

Cisco IOS® Advanced Security
or above

AIM—12.4(15)XY, 12.4(20)T

NME—12.4(20)YA



AIM-IPS
NME-IPS

Accelerated Threat Control for Cisco® ISR

- Enables Inline and promiscuous Intrusion Prevention (IPS)
- Runs same software (CIPS 6.x) and enables same features as Cisco IPS 4200
- Performance improvement by hardware acceleration; dedicated CPU and DRAM to offload host CPU

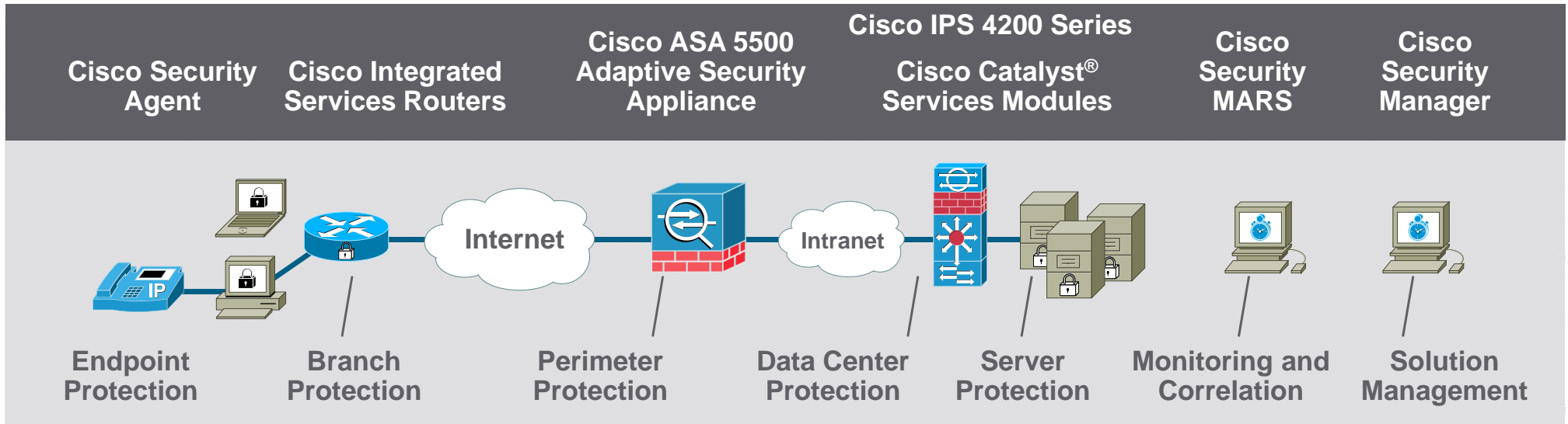
AIM—Up to 45 Mbps

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 Intrusion Prevention Strategy

Comprehensive Threat Protection for the SDN



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

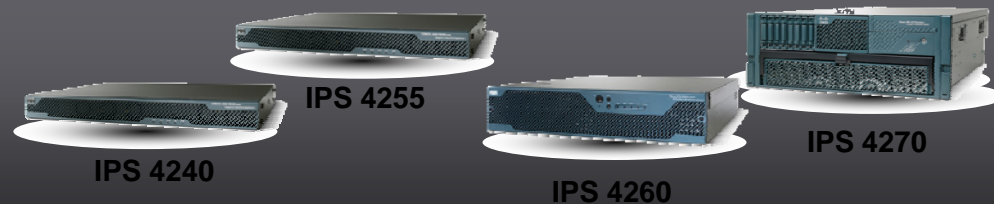
Better Together

- On-box and networkwide 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

Cisco IPS Product Portfolio

IPS 4200 Series

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



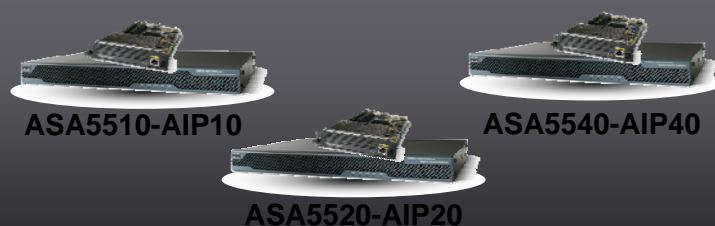
Cisco Catalyst 6500 Series

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

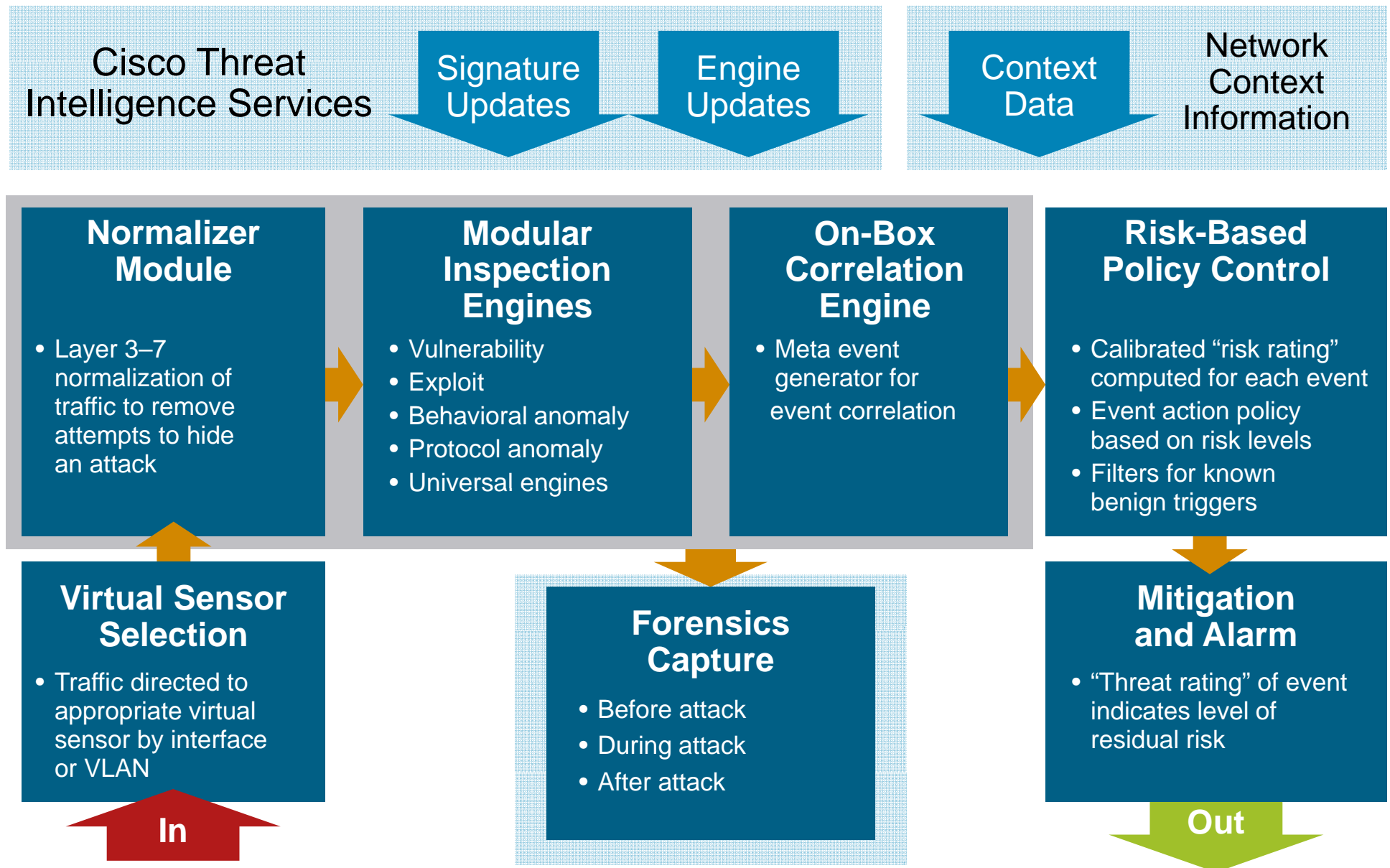
Remote Office/Branch services for scalable remote office protection



Performance

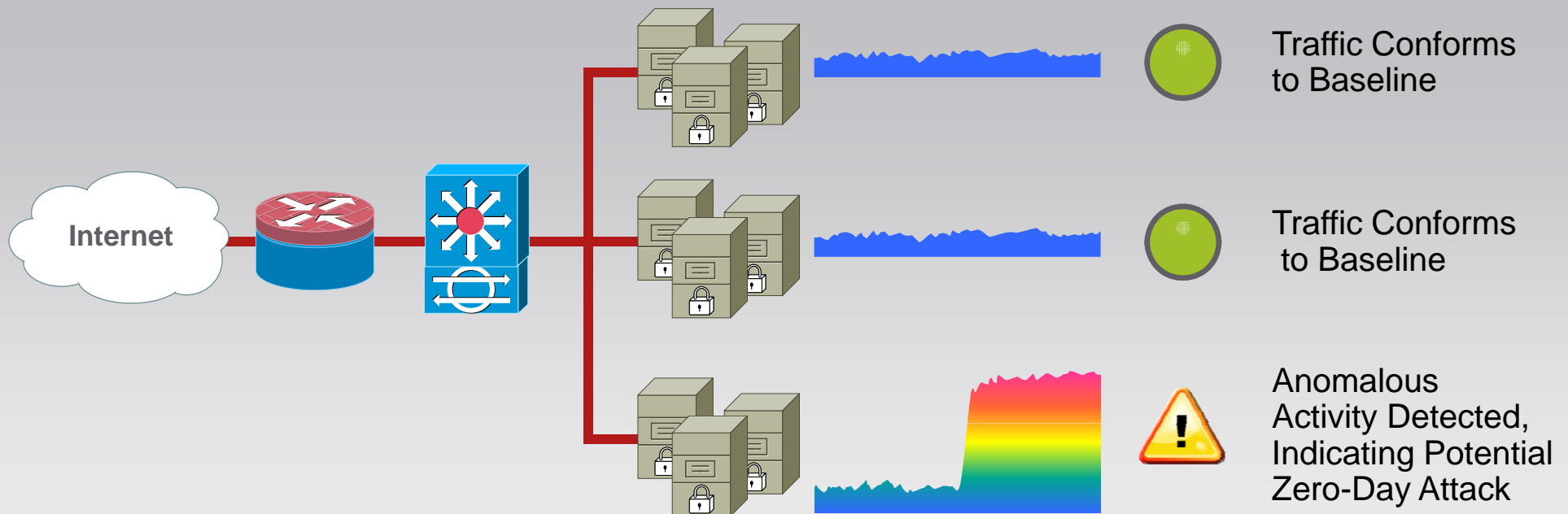
Cisco IPS Architecture

Intelligent Detection and Precision Response

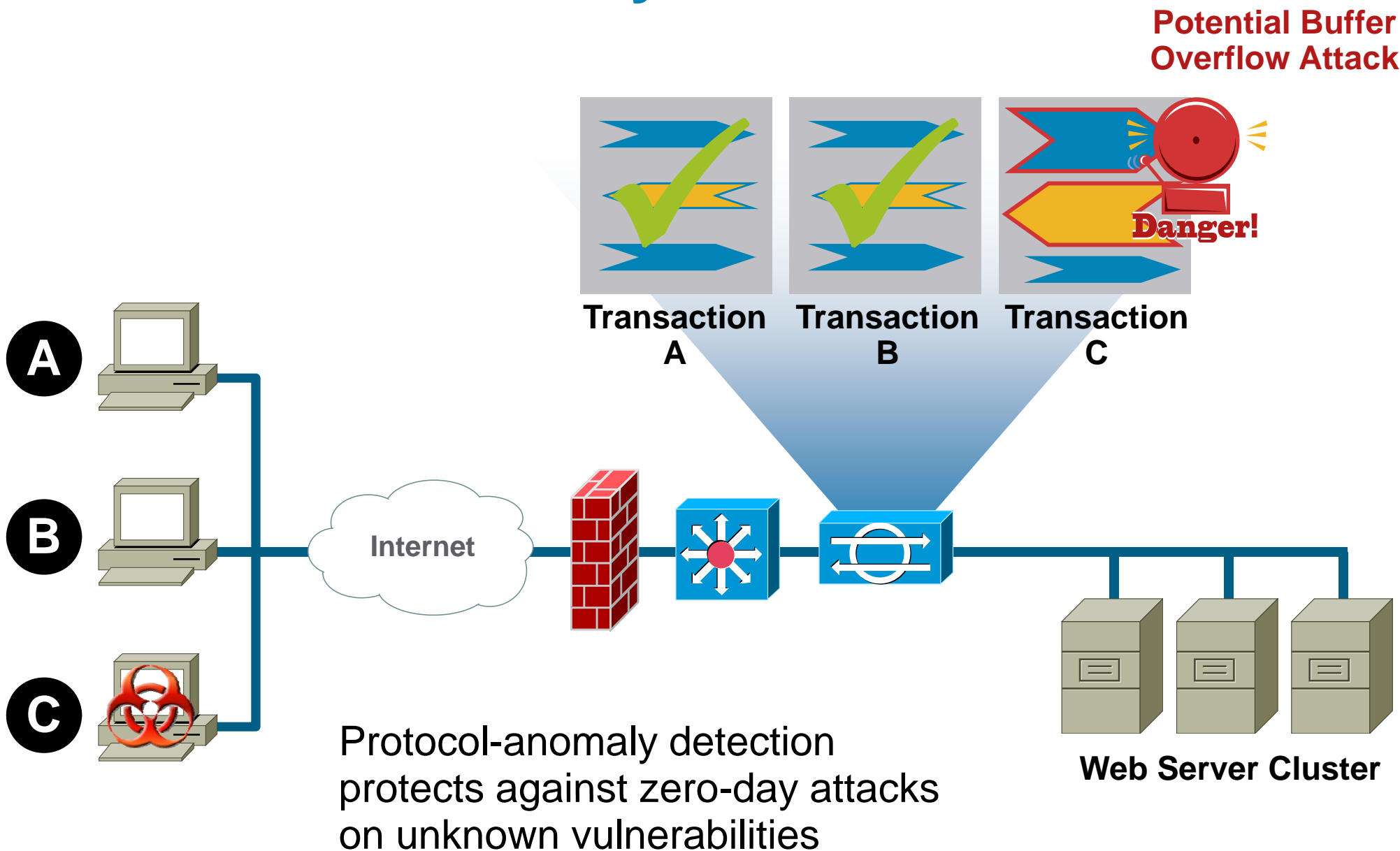


Real-Time Anomaly Detection for Zero-Day Threats

- Anomaly-detection algorithms to detect and stop zero-day 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



Protocol-Anomaly Detection



Comparison: Cisco IOS IPS and Cisco IPS AIM

	Cisco IOS IPS	Cisco IPS AIM/NME
Dedicated CPU/DRAM for IPS	No	Yes
Inline and Promiscuous Detection and Mitigation	No; Inline Mode Only	Yes
Signatures Supported	Subset of 2200+ Signatures, Subject to Available Memory	Full Set of Signatures (3000+)
Automatic Signature Updates	Yes	Yes
Day-Zero Anomaly Detection	No	Yes
Rate Limiting	No	Yes
Cisco Security Agent and Cisco IPS Collaboration	No	Yes
Meta Event Generator	No	Yes
Event Notification	Syslog, SDEE	SNMP and SDEE
Device Management	Cisco IOS CLI, CCP	CIPS CLI, CCP, IDM
System/Network Management	CSM	CSM
Event Monitoring and Correlation	IME, CS-MARS	IME, CS-MARS, On-Box Meta Event Generator

Note: Only one IPS service may be active in the router; all others must be removed or disabled

Comparison: Cisco IPS AIM/ Cisco IPS NME

	Cisco IPS AIM	Cisco IPS NME
Support with ISR Models	Cisco 1841 ISR and Above (Except for 1861)	Cisco 2811 ISR and Above
On-Line Insertion and Removal	No	Yes, with 3845 ISR Only
Performance	Up to 45 Mbps	Up to 75 Mbps
Form Factor	Internal AIM	NME Slot
Management Port	No External Port	External Ethernet Management Port
Initial Cisco IPS Software Version Support*	IPS 6.0(4)	IPS 6.1(1)
Router Cisco IOS Software Version Support	12.4(15)XY, 12.4(20)T	12.4(20)YA

*Both stay current with the latest IPS OS available with IPS 4200 product family

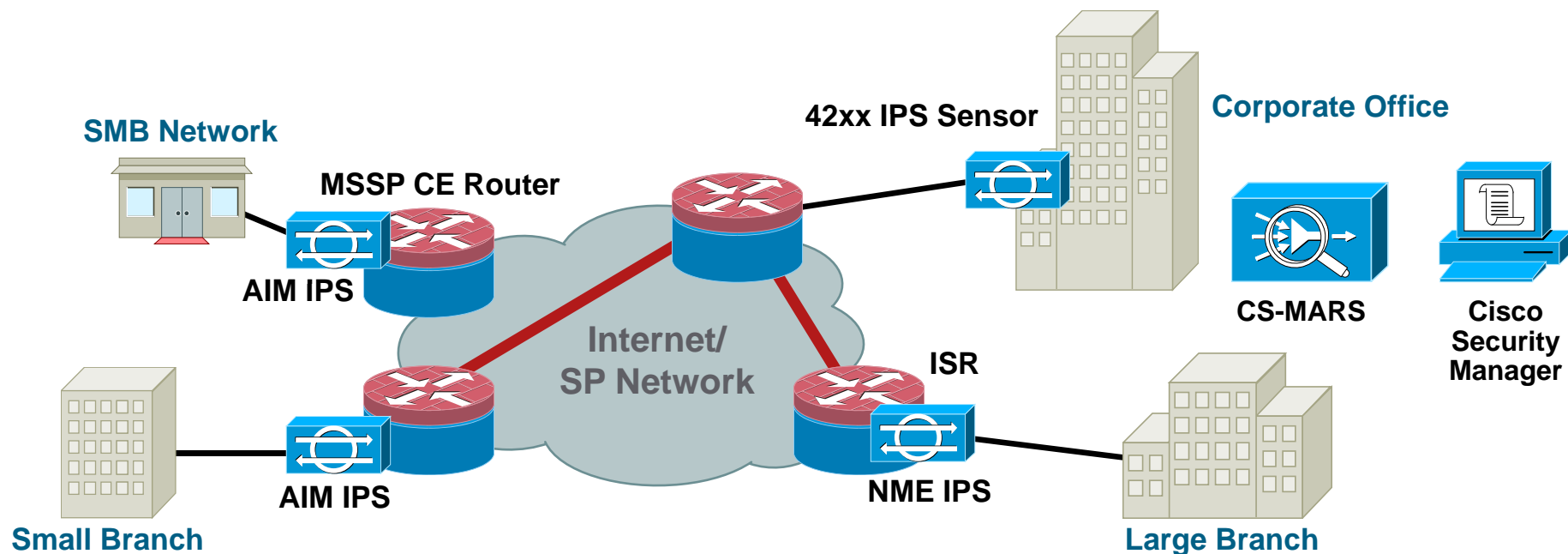
Integrating IPS Modules with Cisco IOS Security Technologies

- Cisco IOS Firewall and IPS Modules are complementary technologies
 - Cisco IOS Firewall blocks unwanted traffic from entry into the network, ensures that applications traffic is legitimate
 - IPS Modules inspect traffic the FW has allowed, as well as traffic from the trusted network, to prevent attacks
- Cisco IOS Firewall provides SYN Flood attack defense
- Cisco IOS Firewall and IPS Modules maintain separate state tables for TCP traffic
 - Resets from one state table force session timeouts in the other

Integrating IPS Modules with Cisco IOS Security Technologies

- Cisco IOS IPS must be disabled when using IPS Module
- IPSec and SSL VPN traffic can be inspected after decryption
- The IPS Modules work with NAC technologies to inspect trusted network traffic
- Frees up CPU and memory resources for other services

Benefits of Integrated IPS on ISR

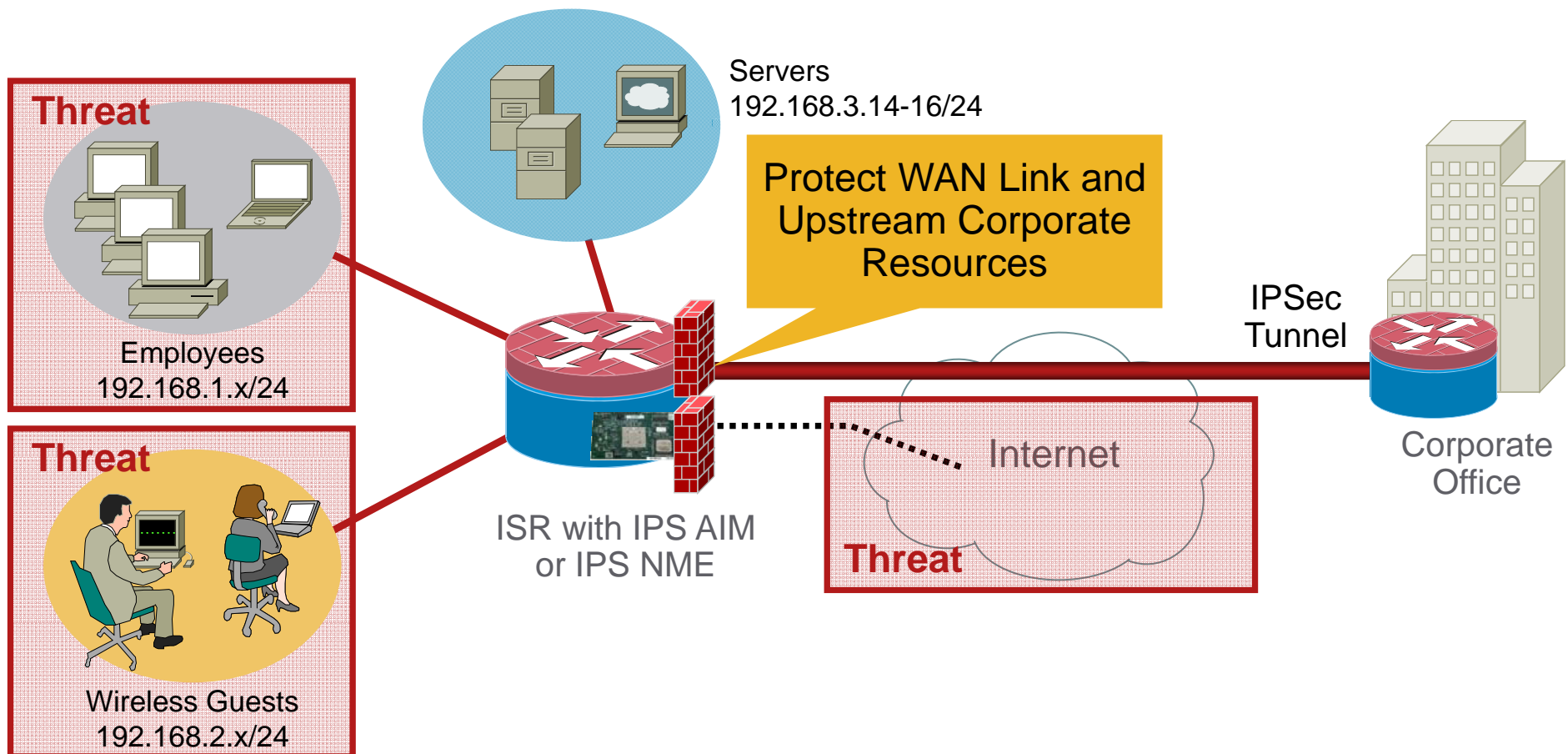


- Full feature, high performance threat protection in the Branch or SMB network
- Requires no additional foot print, cabling, and power requirements
- Systems integration with data, security and voice features on ISR
- Supports any routed WAN link—transport agnostic: T1/E1, T3/E3, Ethernet, xDSL, MPLS,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

Use Case 1

Protect WAN Link and Corporate Offices

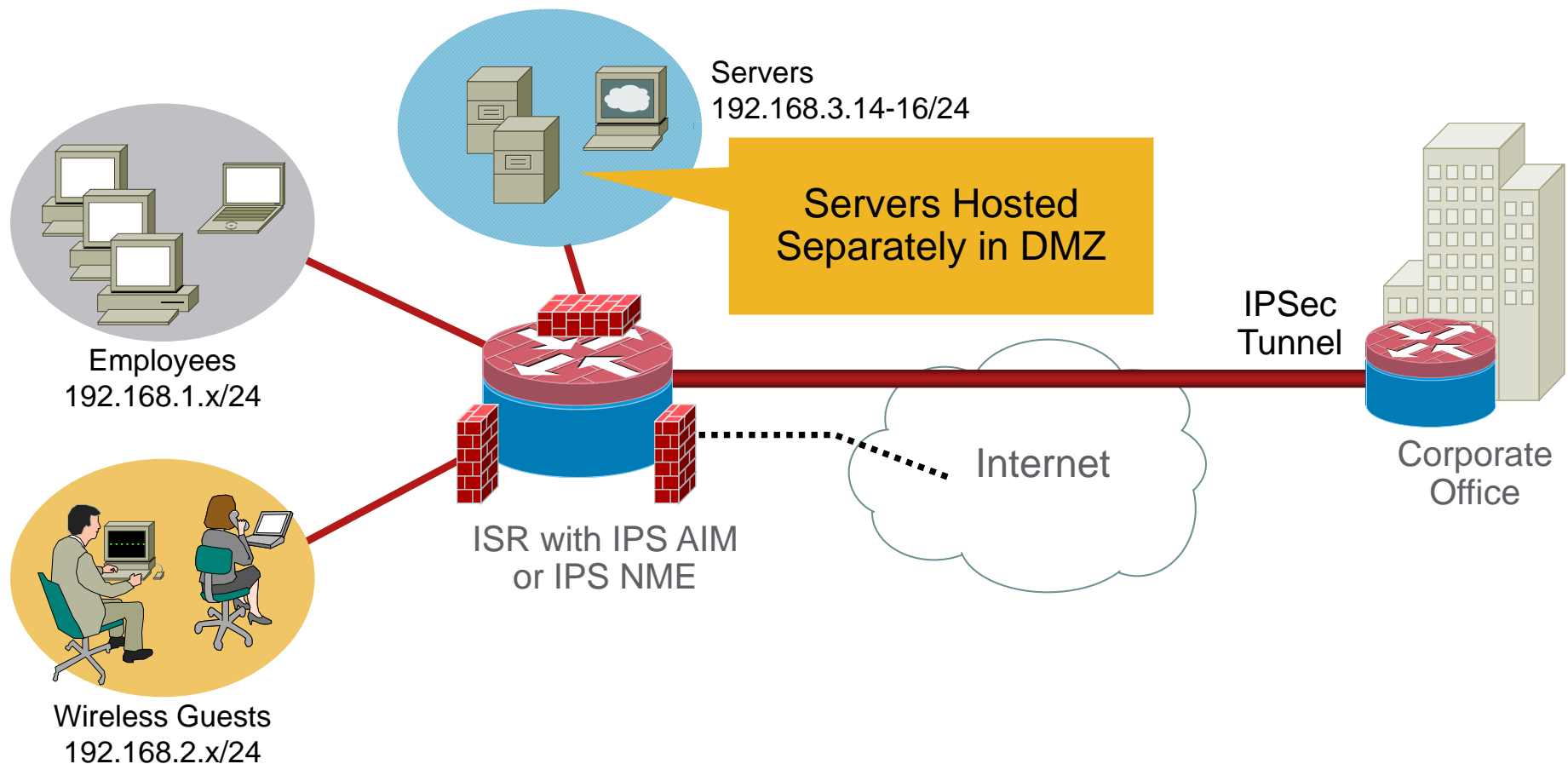
- Branch office LANs are prone to attacks from Internet by split tunnels, contaminated laptops and rogue APs
- Stops worms and trojan horses before they enter corporate or SP network
- Moves attack protection to the network edge
- Helps to secure less secure devices



Use Case 2

Protect Servers at Remote Sites

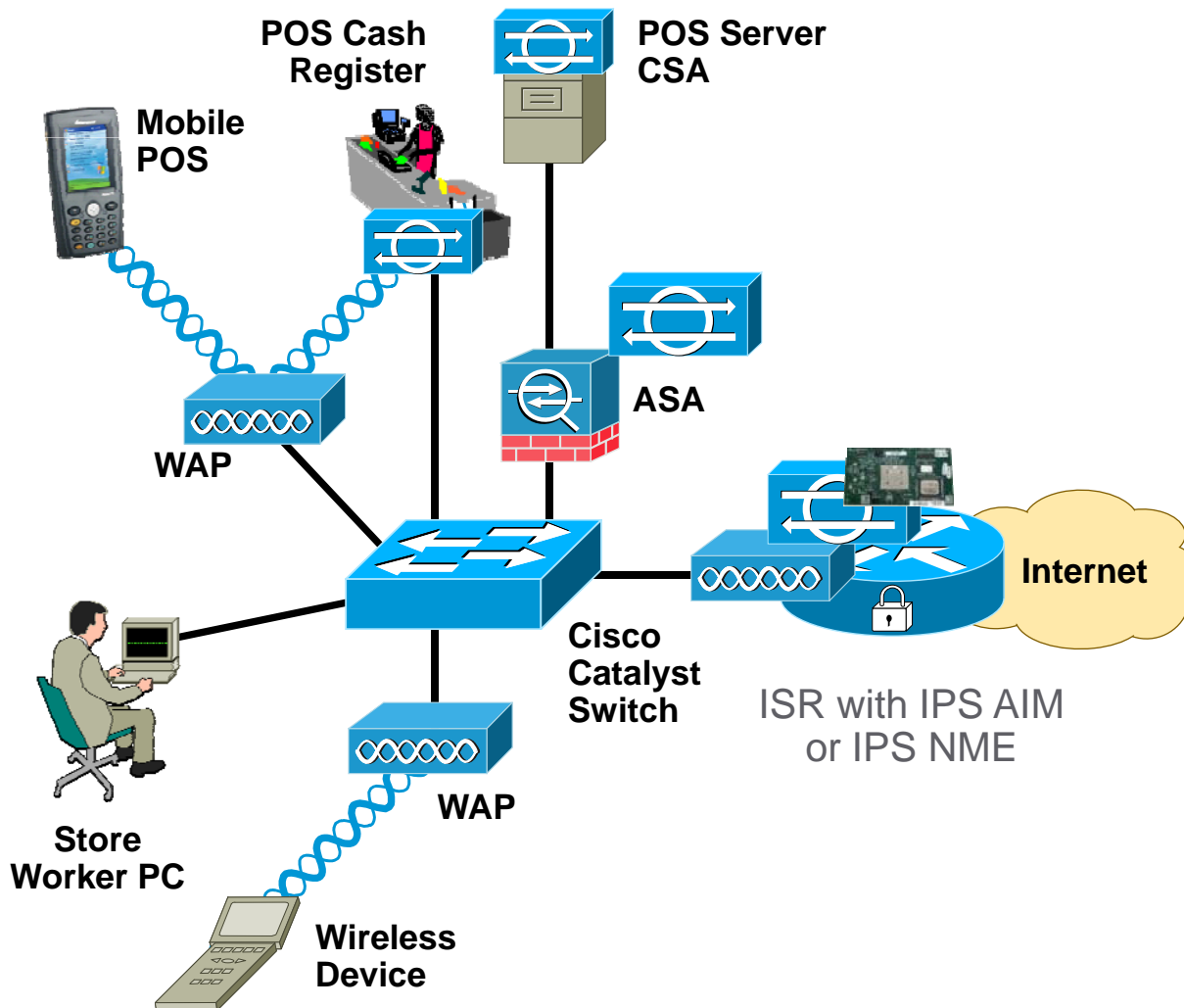
- Branch office LANs are prone to attacks from Internet by split tunnels, contaminated laptops and rogue APs
- Stops worms and trojan horses before they enter corporate or SP network



Use Case 3

Enhances Corporate Compliance Requirements

PCI Compliance (Retail); HIPAA (Healthcare);
Sarbanes-Oxley/GLBA (Finance)



- Provides Intrusion Prevention in depth, as part of PCI Compliant Self Defending Network
- Enhances PCI Requirement 11
- Event correlation provides audit trail for tests and validation exercises
- Integrates with Cisco IOS FW, IPSec, SSL VPN and other Cisco IOS security technologies for complete solution
- Offloads all IPS inspection from router CPU
- Filters inspected traffic via ACLs

Managing and Monitoring IPS Modules

- Configuration and deployment services
- Alert collection, aggregation, and correlation
- Signature and inspection updates
- Threat mitigation

Device-Level Management

- Small Deployment
(One to Five Sensors)
 - IPS Device Manager
 - IPS Manager Express
 - Cisco Configuration Professional
(X-launch IDM)
- Low Alarm Rates
 - IPS Manager Express

Multi-Device Management

- Medium/Large Deployments
(Hundreds to Thousands of
Security Devices)
 - Cisco Security Manager
- High Alarm Rates
 - CS-MARS

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

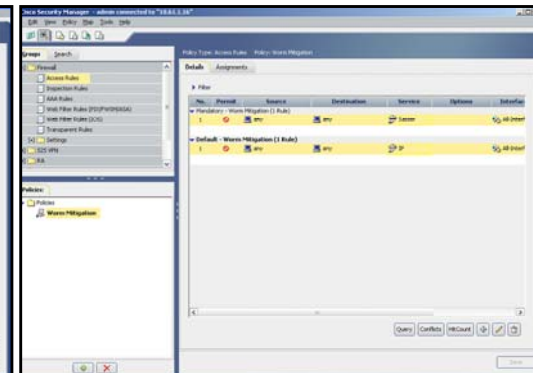
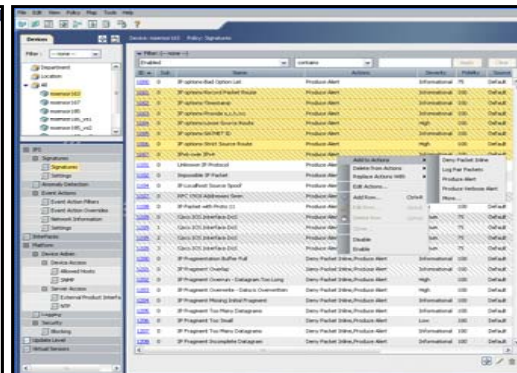
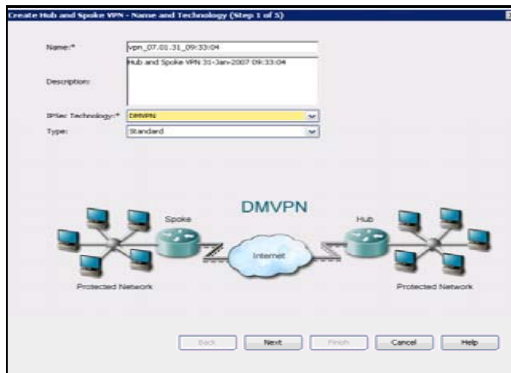
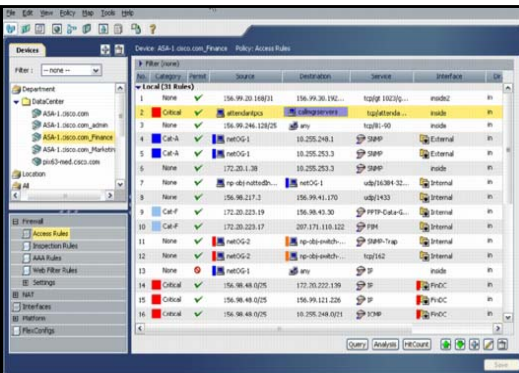
The screenshot displays the Cisco IPS Manager Express (IME) dashboard. The interface is divided into several sections:

- Sensor Health - Corp-IPS:** Two circular gauges showing sensor health and network security health.
- Interface Status - Corp-IPS:** A table showing interface status for various GigabitEthernet and Management interfaces.
- Top Attackers:** A horizontal bar chart showing the top attackers, with the highest being 'tacker.bad.com'.
- Top Victims:** A pie chart showing the distribution of top victims, with the highest being '6.16.12.104 (712) 20%'.
- Top Signatures:** A table showing the top signatures, including 'Cisco Margarita Dos' with 747 hits.
- RSS Feed - Cisco Security Alerts:** A list of security alerts, including 'TCP Vulnerabilities in Multiple Non-IOS Cl...' and 'Cisco Video Surveillance IP Gateway and...'

The dashboard also includes navigation tabs for 'Health Dashboard' and 'Traffic Dashboard', and a bottom navigation bar with icons for 'Top Attackers', 'Network Security', 'Top Applications', 'CPU, Memory & Load', 'Top Victims', 'Top Signatures', and 'Attacks Over Time'.

Cisco Security Manager

Integrated Security Configuration Management



Firewall Management

VPN Management

IPS Management

Reduce OpEx

- 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, ...

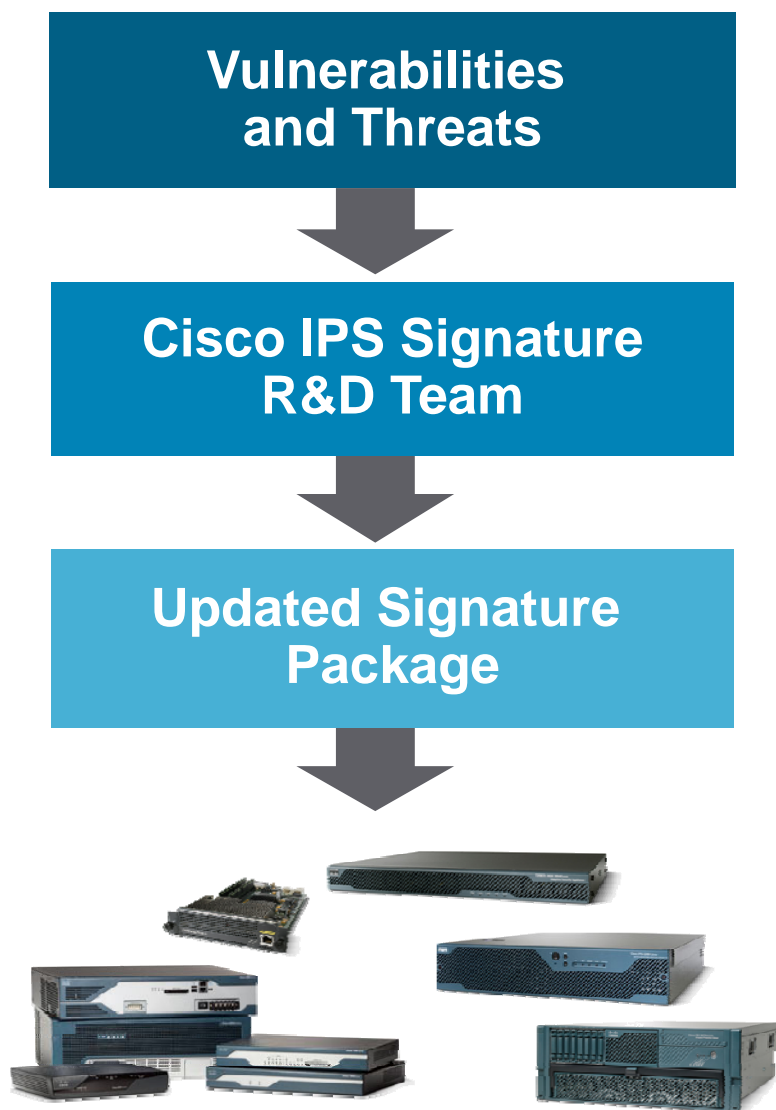
- Support for PIX, ASA, VPNSM, VPN SPA, and Cisco IOS Routers
- Support for wide array of VPN technologies such as, DMVPN, Easy VPN, and SSL VPN
- VPN Wizard for Three-Step Point-and-Click VPN Creation

- 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

- 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

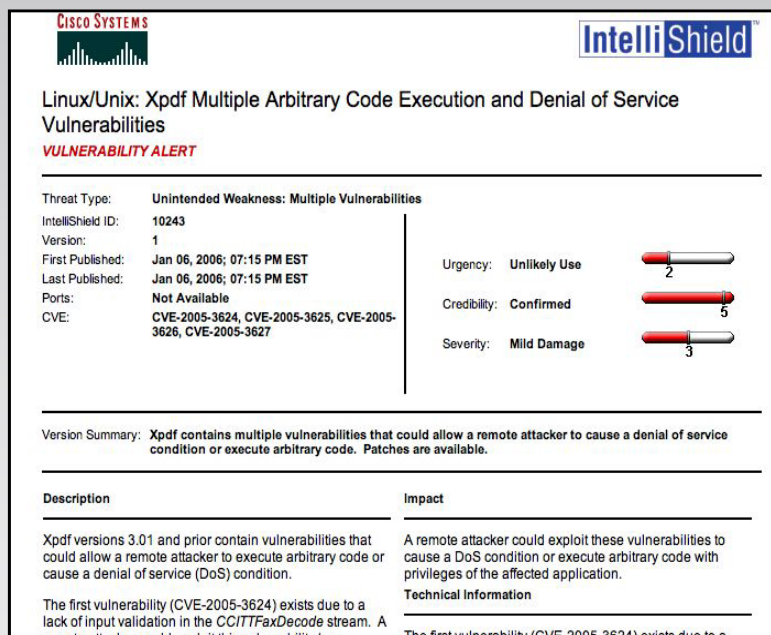
Rapid Signature Updates for Emerging Threats



- **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**



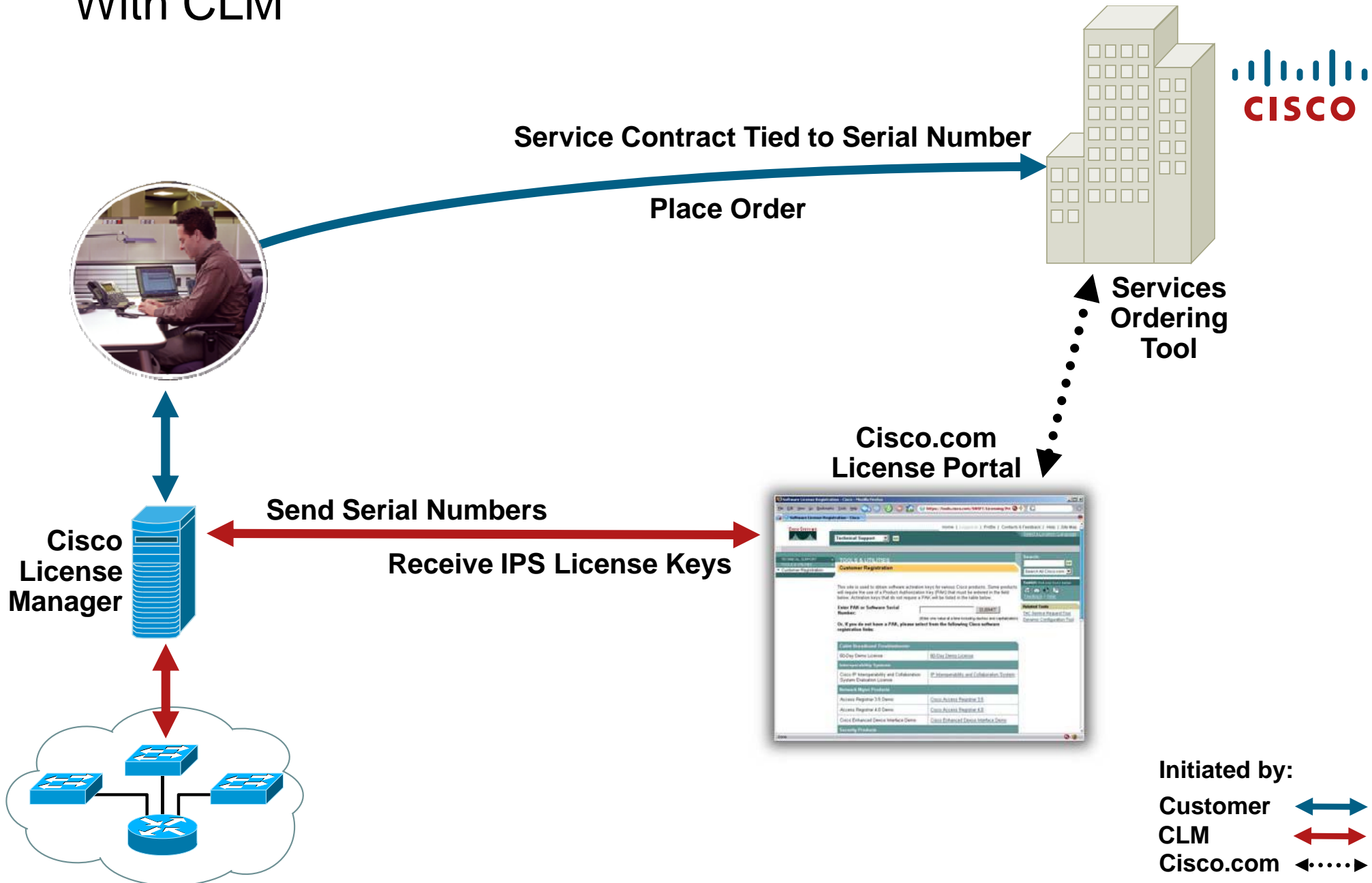
- Complete vulnerability and threat information in a single database
- Notification of only those vulnerabilities relevant to a pre-defined infrastructure
- Actionable alerts in a standardized format based on user-customized profiles
- Each vulnerability or threat is analyzed and validated by security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

Activation Workflow

With CLM





CISCO