Cisco IPS AIM and IPS NME for Cisco 1841 and Cisco 2800, 2900, 3800 and 3900 Series Integrated Services Routers

The Cisco® Intrusion Prevention System Advanced Integration Module (IPS AIM) and Network Module Enhanced (IPS NME) bring integrated intrusion prevention to enterprise branch offices and expand network security to the edge.

The Cisco IPS AIM for the Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers and the Cisco IPS NME for the Cisco 2811, 2821, 2851, 3825, 3845, 2911, 2921, 2951, 3925 and 3945 Integrated Services Routers bring Cisco IPS to branch offices and small businesses (Figure 1). Cisco IPS is an integral component of the Cisco Self-Defending Network, an architectural solution designed for the evolving security landscape. Security is integrated everywhere, and with the help of a lifecycle services approach, enterprises can design, implement, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls.

With the ever-increasing complexity and sophistication of security threats, every point in the network can be at risk. Cisco IPS accurately identifies, classifies, and stops malicious traffic, including worms, spyware, adware, network viruses, and application abuse. Vigilant protection helps ensure business continuity and minimizes the effect of costly intrusions.

Figure 1. Cisco IPS AIM and IPS NME for Integrated Services Routers

Cisco offers a variety of IPS solutions; the Cisco IPS AIM is made for small and medium-sized businesses (SMBs) and small branch offices, whereas the Cisco IPS NME is for small enterprises and large branch offices. Cisco IPS Sensor Software running on the Cisco IPS AIM and IPS NME provides advanced, enterprise-class IPS functions and meets the ever-increasing security needs of branch offices. The Cisco IPS AIM and IPS NME can scale in performance to match branch-office WAN bandwidth requirements today and in the future. At the same time, the integration of IPS onto the Cisco integrated services router keeps the solution cost low and effective for business of all sizes.

For ease of deployment and monitoring, Cisco IPS solutions offer different device configurations and event viewing options, including the Cisco IPS Device Manager (IDM) for single device management and Cisco IPS Manager Express (IME) for event monitoring for up to 5 IPS modules, Cisco Security Manager for networkwide device configuration and policy deployment, and Cisco Security Monitoring, Analysis and Response System (CS-MARS) for event monitoring and correlation.
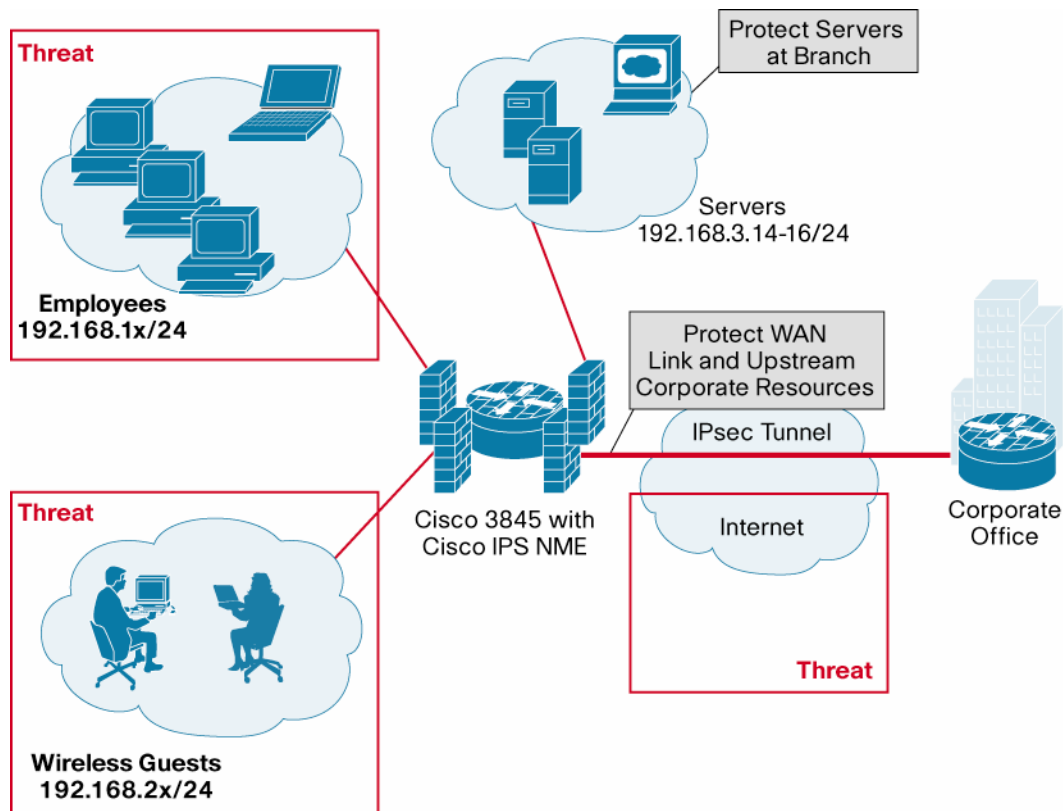
The Cisco IPS AIM and IPS NME for the Cisco 1841 and Cisco 2800, 2900, 3800 and 3900 Series Integrated Services Routers: Integrating IPS in a Full-Service Branch-Office Solution

By integrating IPS and branch-office routing, Cisco integrated services routers can secure remote branch-office networks from threats originating from the Internet and reduce the WAN link overload from infected hosts at the branch office. The integration of IPS into the branch-office router provides numerous important customer benefits:

- **Dedicated processor to maximize performance:** IPS AIM and IPS NME have their own CPUs and DRAMs for all IPS functions. They offload router CPU from processor-intensive tasks such as deep packet inspection from the host router.
- **Performance:** The Cisco IPS AIM and IPS NME can monitor up to 45 and 75 Mbps of traffic, respectively, and are suitable for T1/E1 and up to T3 environments.
- **Inline and promiscuous modes:** Both inline and promiscuous IPS inspection modes are supported. Inline mode places the IPS module in the packet path and can be configured to drop violated packets.
- **Common management tool for Cisco IPS solution:** The Cisco IPS AIM and IPS NME support Cisco Security Manager, the same management tool the Cisco IPS 4200 Series Sensors supports, allowing you to use one centralized management system for both appliance and router sensors.
- **Flexibility in monitoring interfaces:** The Cisco IPS AIM and IPS NME connect directly to the router backplane and can monitor packets coming in and going out of any router interface, including T1, T3, DSL, ATM, Fast Ethernet, and Gigabit Ethernet.
- **In-band management (AIM only):** An internal Gigabit Ethernet port is used for in-band management of the Cisco IPS AIM command-line interface (CLI) and also for the web-based management application, Cisco IPS Device Manager. You can access the IPS AIM through the router console port or through the Secure Shell (SSH) Protocol to any Layer 3 interface. No physical management port is required.
- **Out-of-band management (NME only):** If you require a separate network for device management, the Cisco IPS NME has an external Gigabit Ethernet port dedicated for console and web-based device manager access.
- **Physical space savings:** The Cisco IPS AIM and IPS NME plug into the integrated services router and save valuable real estate in the wiring closet.
- **Reduced downtime (NME only):** The NME slot(s) on modular integrated services routers are externally accessible and make field installation and replacement very simple. In addition, the Cisco 3945 Integrated Services Router supports online insertion and removal (OIR), which facilitates replacement of like-to-like modules without any power cycle, minimizing the mean time to repair and increasing the overall availability of the router.
- **Simple power and cable management:** Cisco IPS AIM and IPS NME take advantage of the power options of the router, including DC power and redundant power.
- **Security in depth:** The Cisco IPS AIM and IPS NME interoperate with security and WAN optimization features such as VPN, firewall, Network Address Translation (NAT), Web Cache Control Protocol (WCCP), and Cisco Wide Area Application Services (WAAS) as well as all common Cisco IOS® Software functions.

Figure 2 shows and example deployment of Cisco IPS AIM and IPS NME in an Empowered Branch Office.

Figure 2. Deployment Example of Cisco IPS AIM and IPS NME in Empowered Branch

Cisco IPS Advantages

Cisco IPS Sensor Software running on the Cisco IPS AIM and IPS NME includes innovative security technologies that can give you the confidence to take prevention actions on a broader range of threats. These technologies, including global correlation and validation tools, greatly reduce the risk of dropping legitimate traffic.

Pervasive Network Integration

Cisco IPS solutions defeat threats from multiple vectors, including network, server, and desktop endpoints. The solutions extend across Cisco platforms, from purpose-built appliances and integrated firewall and IPS devices to services modules for routers and switches. A Cisco IPS solution protects the network from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic at Layers 2 through 7 -- across the network.

Collaborative Threat Prevention

Cisco IPS employs a unique, system wide security ecosystem that collaborates, assesses, and reacts to threats, delivering excellent network scalability and resiliency. This ubiquitous alliance includes cross-solution feedback linkages, common policy management, multivendor event correlation, attack-path identification, passive and active fingerprinting, and host-based Cisco Security Agent-IPS collaboration.

Proactive Posture Adaptation

As the network threat posture changes, Cisco IPS evolves and adapts to stay ahead of the security landscape, mitigating threats from known and unknown attacks. Extensive behavioral analysis, anomaly detection, policy adjustments, and rapid threat response techniques save time, resources -- and most importantly -- the assets and productivity of your organization.

Easy Management

Installation of the Cisco IPS AIM and IPS NME is as easy as configuring the router to recognize the card. After the IPS AIM and NME are initialized and running, you can modify configurations and push them to the modules from any of the management consoles.

Primary Management Features

Primary management features include the following:

- **Cisco IPS Device Manager:** Used for configuring network and switch IPS sensors, the Cisco IPS Device Manager provides a scalable foundation to configure multiple sensors concurrently using group profiles.
- **Cisco IPS Manager Express:** This application is used for monitoring IPS events generated by up to 5 IPS devices.
- **Cisco Security Manager:** Integrated monitoring is used to capture, store, view, correlate, and report on events from network IPS, switch IPS, host IPS, firewalls, and routers.
- **CS-MARS:** This application offers a family of high-performance, scalable appliances for threat management, monitoring, and mitigation.

Cisco IPS AIM Product Summary

Product Numbers

Table 1 gives the part numbers and descriptions of the Cisco IPS AIM and IPS NME.

Table 1. Cisco IPS AIM and IPS NME Part Numbers

Product Part Number	Description
AIM-IPS-K9	Cisco Intrusion Prevention System Advanced Integrated Module for Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers
NME-IPS-K9	Cisco Intrusion Prevention System Network Module Enhanced for Cisco 2811, 2821, 2851, 2911, 2921, 2951, 3800 and 3900 Series Integrated Services Routers.

Supported Platforms

One Cisco IPS AIM or IPS NME is supported per Cisco Integrated Services Router. Table 2 lists the supported router platforms.

Table 2. Supported Router Platforms

Router	Cisco IPS AIM	Cisco IPS NME
Cisco 1841 and 2801	Yes; up to 1 per platform	No
Cisco 2811, 2821, and 2851	Yes; up to 1 per platform	
Cisco 3825 and 3845	Yes; up to 1 per platform	
Cisco 2911, 2921, and 2951	No	Yes (requires adapter card)
Cisco 3925 and 3945	No	Yes (requires adapter card)

Cisco IOS Software Feature Sets and Release

Table 3 lists the required Cisco IOS feature sets and releases for Cisco IPS AIM and IPS NME on the Cisco 1841, 2800 and 3800 series Integrated Services Routers Note that, IPS NME on the Cisco 2900 and 3900 Integrated Services Routers does not require a Security Feature license.

Table 3. Supported Cisco IOS Software Feature Sets for Cisco IPS AIM and IPS NME on the Cisco 1841, 2800 and 3800 series Integrated Services Routers

Cisco IOS Software Feature Sets
Cisco IOS Advanced Security
Cisco IOS Advanced IP Services
Cisco IOS Advanced Enterprise Services

Table 4 lists the supported Cisco IOS Software releases.

Table 4. Supported Cisco IOS Software Releases for Cisco IPS AIM and IPS NME

Product Part Number	Minimum Cisco IOS Software Release
AIM-IPS-K9	12.4(20)T
NME-IPS-K9	12.4(22)T on 2800 and 3800 series routers 15.0(1)M on 2900 and 3900 series routers

Cisco IPS Sensor Software and Signature Licenses

Cisco IPS AIM and IPS NME run Cisco IPS Sensor Software. Table 5 lists the minimum required releases.

Table 5. Supported Cisco IPS Sensor Software Release for Cisco IPS AIM and IPS NME

Product Part Number	Minimum Cisco IPS Software Release
AIM-IPS-K9	6.0(3)
NME-IPS-K9	6.1(1)

To upgrade to the latest Cisco IPS Sensor Software, go to the Software Center for Cisco Secure Software: http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto/.

You must have a valid Cisco Services for IPS service contract per sensor in order to install signature updates on the Cisco IPS AIM and IPS NME. The IPS application software enforces the licensing requirement and helps ensure that only sensors covered by an active Cisco Services for IPS support contract process signature updates.

Cisco Services for IPS

Cisco Services for IPS protect and ensure the effectiveness of the Cisco Intrusion Prevention System Advanced Integration Module (AIM) and the Cisco Intrusion Prevention System Network Module Enhanced (IPS NME) by providing frequent threat protection updates and Cisco SMARTnet support in a single comprehensive service offering. Supported by the Cisco Global Security Intelligence organization, Cisco Services for IPS delivers continuously updated, comprehensive, and accurate detection technology to identify and block fast-moving and emerging threats before they damage your network assets.

Cisco Services for IPS provides:

- Up-to-the-minute threat and vulnerability protection through frequent IPS intelligence, signature, and detection engine updates from Cisco Global Security Intelligence Engineering
- Cisco Global Correlation and Reputation filtering that improves the accuracy of threat recognition and blocking, and overall IPS effectiveness

- Access to Cisco IntelliShield Search Access feature for detailed research on the latest threats and vulnerabilities correlated with IPS signatures
- Ongoing Cisco IPS operating system software updates and upgrades for improved security, performance , device management, and investment protection
- Around-the-clock global access to the Cisco Technical Assistance Center (TAC)
- Access to the extensive Cisco.com knowledge base and tools
- Advanced hardware replacement ranging from next-business-day parts replacement to around-the-clock, 2-hour parts replacement with on-site field engineering support

For more information about Cisco Services for IPS, visit http://www.cisco.com/go/services/ips.

Hardware Specifications

Table 8 gives hardware specifications of the Cisco IPS AIM and IPS NME.

Table 6.   Table 8 Hardware Specifications of Cisco IPS AIM and IPS NME

Feature	Cisco IPS AIM	Cisco IPS NME
Hardware Features		
Monitoring and management ports	1 internal Gigabit Ethernet port	1 external Gigabit Ethernet port
Physical Specifications		
Dimensions (H x W x D)	5.25 x 0.95 x 3.25 in. 13.3 x 2.41 x 8.26 cm	7.12 x 6.50 x 1.62 in. 18.1 x 16.5 x 4.1 cm
Weight	0.6 lb (0.27 kg)	1.0 lb (0.45 kg)
Operating humidity	5 to 95% noncondensing	
Operational temperature	• 32 to 104°F • 0 to 40°C	
Nonoperating temperature	• –40 to 185°F • –40 to 85°C	
Operational altitude	• 0 to 10,000 ft • 0 to 3000m	

Regulatory Compliance, Safety, EMC, Telecom, and Network Homologation

When installed in a Cisco 1800 (modular), 2800, 3800, 2900 or 3900 Series Router, the IPS AIM and IPS NME do not change the standards (Regulatory Compliance, Safety, EMC, Telecom, or Network Homologation) of the router itself. Refer to data sheets for the Cisco, 1800 (modular), 2800, 3800 2900 or 3900 Series Routers.

Performance Specifications

Cisco IPS AIM and IPS NME can run up to 45 and 75 Mbps, respectively. Performance varies with the platform under test, traffic profile, and services running concurrently on the platform.

Feature Specifications

Table 9 gives feature specifications of the Cisco IPS AIM and IPS NME.

Table 7.   Feature Specifications of Cisco IPS AIM and IPS NME

Feature	Cisco IPS AIM and IPS NME
Standard monitoring interface	Router internal bus
Standard command and control interface	AIM: Internal Gigabit Ethernet port for in-band management NME: External Gigabit Ethernet port for out-of-band management
Optional interface	No
Stateful pattern recognition	Yes

Feature	Cisco IPS AIM and IPS NME
Heuristic detection	Yes
Anomaly detection	Yes
Sweeps or floods	Yes
Denial-of-service (DoS) mitigation	Yes
Worms or viruses	Yes
Common gateway interface (CGI) or web attacks	Yes
Buffer overflow protection	Yes
Remote-procedure call (RPC) attack detection	Yes
IP fragmentation attacks	Yes
Internet Control Message Protocol (ICMP) attacks	Yes
Simple Message Transfer Protocol (SMTP), Send Mail, Internet Message Access Protocol (IMAP), or Post Office Protocol (POP) attacks	Yes
FTP, SSH, Telnet, and rlogin attacks	Yes
Domain Name System (DNS) attacks	Yes
TCP hijacks	Yes
Windows or NetBIOS attacks	Yes
TCP application protection	Yes
Network Timing Protocol (NTP) attacks	Yes
Customizable signatures using signature microengine technology	Yes
Automated signature updates	Yes
Alarm summarization	Yes
Support for 802.1q traffic	Yes
IP Security (IPsec) or Secure Sockets Layer (SSL) between sensor and management console	Yes
Encrypted signature packages	Yes
SSH for remote administration	Yes
Serial Control Protocol (SCP) support for secure file transfer	Yes
IP Fragmentation and Reassembly	Yes
TCP Stream Reassembly	Yes
Unicode Deobfuscation	Yes
Router access-control-list (ACL) modifications	Yes
Firewall policy modifications	Yes
Switch ACL modifications	Yes
Session termination with TCP resets	Yes
IP session logging or session replay	Yes
Alarm display	Yes
Email alerts	Yes
E-page alerts	Yes
Customizable script execution	Yes
Multiple alarm destinations	Yes
Third-party tool integration	Yes
IPS active update bulletins	Yes
Web user interface (HTTPS)	Yes
Command-line interface (CLI; console)	Yes
CLI (Telnet or SSH)	Yes
CiscoWorks VPN Security Management Solution support	Yes

Feature	Cisco IPS AIM and IPS NME
Redundant power supply	Yes, only for Cisco 3845 and 3945
Monitoring link failure detection	Yes
Communications failure detection	Yes
Services failure detection	Yes
Device failure detection	Yes

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies. For more information, visit http://www.cisco.com/go/services.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.