Cisco IPS Software

Product Overview

Cisco IPS Software is the industry's leading network-based intrusion prevention software. It provides intelligent, precise, and flexible protection for your business by accurately identifying, classifying, and preventing malicious traffic before it can affect your business productivity.

Table 1. Cisco IPS Software Features

Feature	Description

Intelligent	• Layer 2–7 inspection
	  ◦ True stateful inspection
	  ◦ Full stream reassembly
	  ◦ Protocol decoding
	  ◦ Tunneling protocol inspection
	• Vulnerability-based protection
	• Day-zero protection
	  ◦ Unknown vulnerabilities Unknown exploits
	  ◦ Unknown exploit variants
	  ◦ Day-zero worms
	• Protocol anomaly detection
	• Statistical anomaly detection
	• Application anomaly detection
	• Statistical analysis engine
	• Evasion protection
	• Custom signatures

Precise	• Inline prevention
	  ◦ Drop packet
	  ◦ Drop flow
	  ◦ Deny attacker
	  ◦ Log attacker
	  ◦ Log victim
	  ◦ Modify packet
	  ◦ Terminate session
	  ◦ TCP reset
	  ◦ Rate limit
	• Network-integrated prevention
	  ◦ Block attacker Block connection
	  ◦ Rate limit
	  ◦ Supported devices: Firewalls, Routers, Switches, Wireless LAN controllers
	• Dynamic default blocking
	  ◦ Real-time risk rating
	  ◦ Adjustable risk tolerance
	  ◦ OS information
	  ◦ Session information

Feature	Description
Flexible	• Deployment options ◦ Inline ◦ Promiscuous ◦ Hybrid (inline and promiscuous) ◦ Appliance ◦ Integrated with firewall ◦ Integrated with router ◦ Integrated with switch ◦ Virtual sensor VLAN pairs • Modular design ◦ Signature updates ◦ Inspection capabilities updates ◦ Management software updates ◦ Performance improvements • Cisco IPS Manager Express • Cisco Security Management Suite ◦ Cisco Security Manager ◦ Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)

Intelligent

Cisco IPS Software is the core of Cisco IPS solutions. The software is built on advanced Cisco security and network expertise to provide intelligent inspection, as well as day-zero and evasion protection.

Cisco IPS Software inspection technology is engineered to prevent sophisticated malicious activity, whether it takes the form of worms, targeted espionage, data theft, or denial of service. These modular inspection capabilities are completely stateful, and can detect and prevent threats to the entire network stack, from applications to Address Resolution Protocol (ARP). The result is that Cisco IPS Software is not just a simple pattern-matching technology; it understands your traffic.

Day-zero protection is central to the Cisco IPS Software architecture. Inspection capabilities are geared towards addressing vulnerabilities, as opposed to the exploits that attack them. This gives the software an advantage in dealing with undiscovered and undisclosed vulnerabilities, as well as new exploits for known vulnerabilities: An exploit for a single vulnerability can be written an unlimited number of ways. Using vulnerability-based signatures coupled with sophisticated inspection modules for protocol, statistical, and application anomaly detection, Cisco IPS Software can identify and prevent threats before they are fully understood by the security community, and recorded in the wild.

Cisco IPS Software also provides unparalleled protection from evasion. Whether they’re hoping to disrupt your business or steal data, sophisticated attackers commonly use techniques that are designed to get past IPS technologies, without being detected and stopped. But the intelligent Cisco IPS Software design provides the industry’s best protection from evasion, through rigorous decoding modules and in-depth protocol analysis. Cisco IPS Software decodes and analyzes network data in the same manner as the client or server in the conversation would, so attempts to obscure attacks or sneak past your security controls are stopped before they reach their targets.

New exploits emerge every day, are easily modified, and change rapidly in the wild. By understanding the protocols and vulnerabilities that those exploits target, Cisco IPS Software protects your business from the problems, not the symptoms.

Precise

Cisco IPS Software provides precise prevention and analysis, to help you confidently protect your assets in today's threat environment.

With the richest set of response actions available in an intrusion prevention system, Cisco IPS Software can prevent malicious activity in accordance with your policy, and in the manner most effective for each threat. Cisco IPS Software prevention options include dropping or modifying packets and flows, denying attackers, terminating sessions, and rate limiting. These capabilities can be performed directly by a Cisco IPS device, or can be provided through integration with other network technologies.

Cisco IPS Software also provides precise, in-depth threat analysis. An adaptive multidimensional algorithm combines attack details with live network knowledge to produce a calibrated risk measurement for each event. That risk measurement is the key to effective threat prevention. The default recommended prevention policy automatically takes the correct prevention action based on the risk rating of each threat, but you can also adjust your threat tolerance, assuming a more aggressive or permissive threat posture to meet your policy needs.

Not all threats behave the same way. Some are small and targeted, some spread from host to host, and some are networkwide. Cisco IPS Software allows you to stop all of the different types of threats where they originate, with the prevention approach that works best.

Flexible

Cisco IPS Software is extremely flexible, enabling you to deploy, update, and manage your intrusion prevention strategy to meet the needs of your business without introducing new risk and change management costs.

Cisco IPS Software is available in the widest variety of deployment options of any IPS technology. Whether you're looking to deploy dedicated appliances or integrate IPS capabilities into your access control, routing, or switching technologies, the same full-featured Cisco IPS Software can be implemented throughout your network. This enables you to deploy IPS capabilities anywhere your traffic flows, as opposed to having to redesign and redirect your traffic to dedicated "choke points."

Cisco IPS Software features a modular design with full-system update capabilities, so you can update any facet of your software—maximizing your investment, while minimizing the impact to your business. Whether it's new signatures, new inspection capabilities, new management features, or new performance improvements, this modular design greatly decreases the operational cost of ongoing enhancements to your security posture.

Cisco IPS technologies, and a customizable dashboard for monitoring security events and sensor health. If you're looking for a comprehensive, unified solution across security technologies, the Cisco Security Management Suite is a management framework designed for scalable policy administration and enforcement for the Cisco Self-Defending Network. This integrated solution can simplify and automate the tasks associated with security management operations across security technologies, including configuration, monitoring, analysis, and response.

In a broad and rapidly changing threat environment, Cisco IPS Software provides you with the design and management flexibility to tailor your security posture to your needs.

Ordering Information

Table 1 lists ordering information for Cisco IPS Software.

Table 2. Ordering Information for Cisco IPS Software

Part Number	Description
IPS-SW-K9-U	Cisco IPS Software

Cisco Services for IPS

Cisco Services for IPS is an integral part of the Cisco Self-Defending Network to protect and continuously enhance the effectiveness of the Cisco Intrusion Prevention solution. Supported by Cisco's 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 impact your organization.

Cisco Services for IPS provides:

- Frequent IPS intelligence and signature and detection engine updates from Cisco Global Security Intelligence Engineering for up-to-the-minute threat and vulnerability protection
- Access to Cisco IntelliShield Search Access feature for IPS signatures that provides detailed research on the latest threats and vulnerabilities correlated with IPS signatures
- Ongoing Cisco IPS operating system software updates and upgrades for improved security, increased performance, improved device management, and enhanced capabilities.
- Around-the-clock, global access to the Cisco Technical Assistance Center (TAC)
- Access to the extensive Cisco.com knowledgebase and tools
- Advance hardware replacement (options range from next-business-day parts replacement, to 24 x 7, 2 hour parts replacement with on-site field engineering support)

For more information on Cisco Services for IPS, please visit http://www.cisco.com/en/US/products/ps6076/serv_home.html.

For More Information

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

For more information about the Cisco Security Management Suite, visit http://www.cisco.com/en/US/netsol/ns647/networking_solutions_sub_solution_home.html

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.

Printed in USA C78-459828-00 03/08

