Cisco Intrusion Prevention System Solutions

Comprehensive, End-to-End Protection

Cisco® Intrusion Prevention System (IPS) solutions accurately identify, classify, and stop malicious traffic, including worms, spyware, adware, network viruses, and application abuse, before they affect business continuity.

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 your network

Collaborative Threat Prevention

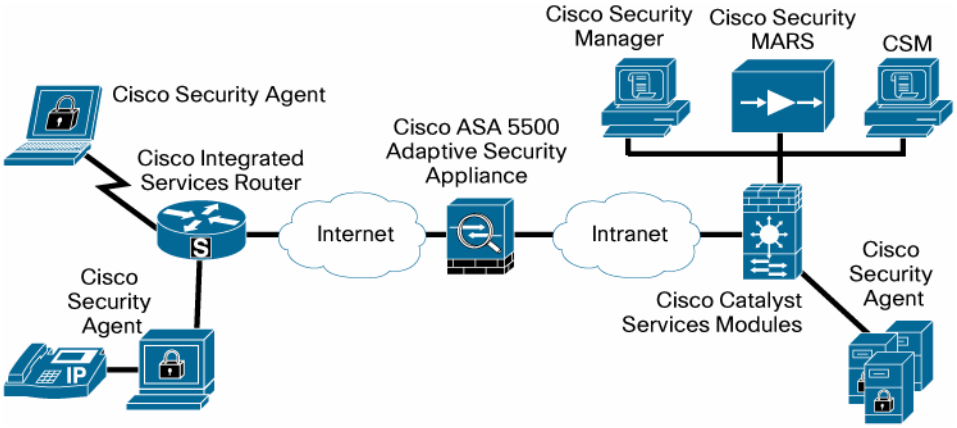
A Cisco IPS solution employs a unique, system wide security ecosystem that assesses and reacts to threats, delivering unmatched network scalability and resiliency. This ubiquitous alliance includes cross-solution feedback linkages, common policy management, multivendor event correlation, attack path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

Proactive Posture Adaptation

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

IPS technology strategically deployed throughout the network provides unmatched end-to-end, day-zero protection (Figure 1). With a Cisco IPS solution, your infrastructure and your business are protected.

Figure 1. Cisco IPS Solutions Deliver Comprehensive Day-Zero Protection Prevention Throughout the Network



Comprehensive Integrated, Collaborative, and Adaptive Network Protection

Today's complex network architectures involve multiple segments, branches, and ingress/egress points-with ever-growing requirements for network access while maintaining security. In this constantly evolving landscape, network security requires more than single-point solutions.

As a core component of the Cisco Self-Defending Network, a Cisco IPS solution delivers comprehensive threat prevention from attacks and threats, regardless of their origin or history. Cisco IPS solutions proactively protect your network through a unique ability to collaborate with other network security resources, ensuring business connectivity across the entire infrastructure. When combined, these elements provide a comprehensive, inline prevention solution, giving you the confidence to detect and stop the broadest range of malicious traffic before it affects business continuity.

Pervasive Network Integration

Cisco IPS solutions integrate into the network, providing unparalleled visibility and network wide threat intelligence. This visibility protects your network from:

- Policy violations-Cisco IPS solutions provide strict control of application usage and policy conformance through traffic inspection, including instant messaging and peer-to-peer applications; strict HTTP enforcement; Port 80 inspection; and traffic filtering based on MIME types and OS fingerprinting. The solutions also provide user and endpoint contextual information.
- Vulnerability exploitations-Cisco IPS solutions stop exploitation of known vulnerabilities in a wide array of operating systems, network services, applications, and protocols, and provide protection from new worms and viruses prior to their vulnerabilities becoming known or published.
- Anomalous activity-Cisco's best-in-class anomaly detection feature detects worms by learning the "normal" traffic patterns of the network, and then scanning for anomalous behavior. Fast-propagating network worms scan the network in order to infect other hosts. For each protocol or service, the anomaly detection program studies what is normal scanning activity, and accumulates this information in a threshold histogram and an absolute scanner threshold. The scanner threshold specifies the absolute scanning rate above which any source is considered malicious.
- Behavioral analysis-Cisco IPS solutions provide the ability to detect infection characteristics based on dynamic learning capabilities of network usage.

Multivector Threat Identification

At the core of Cisco IPS solutions are numerous methods for the inspection and analysis of traffic in Layers 2 through 7. These methods provide comprehensive threat identification, often supporting the development of signatures to a vulnerability prior to the release of an exploit to provide you with day-zero protection. These multivector threat identification methods are described in Table 1.

Table 1. Cisco IPS Solution Multivector Threat Identification Methods

Feature	Benefits
Rate Limiting	• Allows the IPS device to limit certain types of traffic by preventing it from utilizing an excessive amount of bandwidth. • Signals external devices such as Cisco IOS® Software-based routers to perform rate limiting to accomplish the same function.
IPv6 Detection	• Enhanced visibility into IPv6 traffic makes it easier to identify malicious traffic.
IP in IP Detection	• Identifies malicious traffic within mobile IP traffic.
Stateful Pattern Recognition	• Identifies vulnerability-based attacks through the use of multipacket inspection across all protocols, thwarting attacks that hide within a data stream.
Protocol Analysis	• Cisco IPS solutions provide protocol decoding and validation for network traffic. • Cisco IPS Sensor Software Version 6.0 monitors all major TCP/IP protocols, including but not limited to IP, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP). • Cisco IPS Sensor Software also provides stateful decoding of application-layer protocols such as FTP, Simple Mail Transfer Protocol (SMTP), HTTP, SMB, Domain Name System (DNS), remote procedure call (RPC), NetBIOS, Network News Transfer Protocol (NNTP), generic routing encapsulation (GRE), and Telnet.
Traffic Anomaly Detection	• Provides anomaly identification for attacks that may cover multiple sessions and connections, using techniques based on identifying changes in normal network traffic patterns (i.e. ICMP flood with a predefined number of ICMP packets within a certain amount of time).
Protocol Anomaly Detection	• Identifies attacks based on observed deviations in the normal RFC behavior of a protocol or service (i.e. HTTP response without an HTTP request).
Layer 2 Detection	• Identifies Layer 2 Address Resolution Protocol (ARP) attacks and man-in-the-middle attacks, which are prevalent in switched environments.
Application Policy Enforcement	• Provides deep analysis and control of a broad set of applications, including: • Peer-to-peer • Instant messaging • Tunneled applications over Port 80 • Allows the user to make policy decisions about various traffic types and Multipurpose Internet Mail Extensions (MIME) types to help ensure that malicious traffic is disallowed from traversing the network.
Anti-IPS Evasion Techniques	• Traffic normalization • IP defragmentation • TCP stream reassembly • De-obfuscation
Customizable Policies	• Gives users the flexibility to create new policies or modify existing policies to meet their unique security objectives, using the innovative Cisco Threat Analysis Micro Engine policy language.

Risk Rating

Cisco IPS solutions provide unparalleled contextual analysis of data to determine its threat and eliminate false positives. This innovative technology is called Risk Rating. Risk Rating increases the accuracy and confidence of IPS packet drop actions by delivering a risk-balanced approach to classifying threats. Risk Rating employs a unique multidimensional algorithm that takes into account several terms, listed in Table 2.

Table 2. Risk Rating Features

Risk Rating Component	Description

Event Severity	A user-modifiable weighted value that characterizes the damage potential of the suspect traffic
Signature Fidelity	A user-modifiable weighted value that characterizes the fidelity of the signature that has detected the suspect activity
Asset Value	A user-defined value that represents the user's perceived value of the target host
Attack Relevancy	An internal weighted value that characterizes any additional knowledge that the sensor may have about the target of the event

The resulting risk rating is an integer value that is dynamically applied to every IPS signature, policy, or anomaly detection algorithm. The higher the value, the greater the security risk of the trigger event for the associated alert. The result is a mechanism that allows the user to develop policies for the prevention of network attacks or to better characterize events for prioritization of further investigation. The user is empowered to make more intelligent decisions on inline IPS actions while virtually eliminating the possibility of dropping valid traffic.

Threat Rating

New with Cisco IPS Sensor Software Version 6.0, the Threat Rating feature provides a single view of the threat environment of the network. Threat Rating can minimize alarms and events through the ability to customize the viewer to only show events with a high Threat Rating value. The Threat Rating value is derived as follows:

- Dynamic adjustment of event Risk Rating based on success of response action
- If response action was applied, Risk Rating is deprecated (TR < RR)
- If response action was not applied, Risk Rating remains unchanged (TR = RR)

The result is a single value by which the threat risk is determined. This eases the management of alarms and determination of risk on the network.

Collaborative Threat Prevention

Protecting the network requires an IPS solution that delivers more than individual attack mitigation. To provide system wide security, the IPS must scale the protection to other security points throughout the network. Cisco IPS solutions provide unique, unparalleled protection through the ability to determine network resource information, and to collaborate and communicate with those resources. Cisco IPS solutions include:

• IPS/Cisco Security Agent collaboration-Collaboration between Cisco IPS solutions and Cisco Security Agent provides in-depth protection by communicating endpoint information to the IPS for contextual analysis. In addition using the Cisco Security Agent Watch List, the IPS is able to quarantine suspicious hosts. The result is protection on the network from hosts that the endpoint has deemed malicious.

- Cross-solution feedback-Alarmed network traffic can be communicated with other network security devices and tools to provide a system wide protection from attacks on single segments.
- Passive/active fingerprinting-Contextual endpoint profiling based on passive OS fingerprinting and/or static mapping is added to the values within the Risk Rating algorithm to determine block action thresholds. This automated, contextual analysis makes it easier to determine the legitimacy of an attack and reduces false positives.

- Attack-path identification-When using Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) as part of an IPS solution, attacks can be visually displayed and policies can be updated in real time to secure the network.
- Multivendor event correlation-Using Cisco Security MARS, Cisco IPS sensors, and other security devices together provides network wide visibility and information correlation.

Adaptive Behavior

To protect against today's sophisticated attacks and deliver true day-zero protection, the security measures of a network must be capable of understanding the network, and assessing suspicious attacks based on their malicious nature without prior knowledge of those attacks. Cisco IPS solutions adapt to the network, providing protection that is specific and unique to every individual network.

- Anomaly detection/behavioral analysis-New with Cisco IPS Sensor Software Version 6.0, protection of your network from malicious worms and DoS attacks can be automated, based on the sensor's ability to learn network behavior, and alarm when traffic patterns deviate from determined normal patterns. Although normal traffic can be configured statically, the sensor's ability to protect from day-zero attacks using these intelligent engines delivers unprecedented protection, beyond traditional policy-based network security.
- On-device and network event correlation-Cisco Meta Event Generator provides "on-box" correlation methods to deliver accurate worm classification. Cisco IPS Sensor Software Version 6.0 incorporates advanced sensor-level event correlation and knowledge base anomaly detection that gives security administrators an automated method for enhancing the confidence level in the classification of malicious activity detected by the IPS sensor. This provides a mechanism that allows for corresponding actions to deliver network wide containment of worm and virus injection vectors, as well as worm propagation.

Integrated Deployment Options

Cisco offers a wide range of network IPS deployment solutions, enabling customers to implement intrusion prevention in ways that are most effective for their environments. All solutions are designed for high availability and backed by outstanding customer support. Deployment options include dedicated appliances, switch and router modules, and software-based solutions (Table 3).

Table 3. Cisco IPS Solutions

Product	Description	Performance
Cisco IPS 4200 Series Sensor	Dedicated hardware appliance platform	• Cisco IPS 4240 Sensor: 250 Mbps • Cisco IPS 4255 Sensor: 600 Mbps • Cisco IPS 4260 Sensor: 1 Gbps • Cisco IPS 4270 Sensor: 4 Gbps
Cisco IDS Services Module 2 (IDSM-2)	IPS Security Module for Cisco Catalyst 6500 Series Switches	• 500 Mbps
Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM)	IPS Security Module for the Cisco ASA 5500 Series Adaptive Security Appliance	• AIP-SSM 10: up to 225 Mbps, depending on host ASA • AIP-SSM 20: up to 500 Mbps, depending on host ASA • AIP-SSM 40: up to 650 Mbps, depending on host ASA
Cisco IPS Advanced Integration Module (AIM-IPS)	Cisco network module for Cisco access routers, providing IPS capability	• Up to 45 Mbps, depending on the host ISR
Cisco IPS Network Module (NME-IPS)	Cisco network module for Cisco access routers, providing IDS capability	• Up to 75 Mbps, depending on the host ISR
Cisco IOS IPS	Focused set of IPS capabilities using Cisco IOS Software on the router	• Varies

Powerful Management, Event Correlation, and Services

Cisco uses a range of management and correlation tools and support services to provide an effective and complete IPS solution, regardless of deployment size or environment.

Table 4. Cisco IPS Solution Tools and Services

Solution	Product
Management Solutions	• **Command-line interface (CLI):** A full-featured Cisco IOS Software-like CLI that provides device configuration over a Secure Shell (SSH) Protocol connection. • **Cisco IPS Device Manager:** A single device manager that provides a secure, browser-based GUI for configuration and alarm viewing. Cisco IPS Device Manager can be easily accessed from practically any desktop, regardless of the operating system being used. The result is rapid access to data from systems throughout the enterprise. The familiar browser interface enhances ease of use, and with Secure Sockets Layer (SSL), data security is maintained. • **Cisco Security Management Solution:** A powerful but easy-to-use solution to centrally provision all aspects of device configurations and security policies for Cisco IPSs, firewalls, and VPNs. The solution is effective for managing even small networks consisting of fewer than 10 devices, but also scales to efficiently manage large-scale networks composed of thousands of devices. Scalability is achieved through intelligent policy-based management techniques that can simplify administration. • **Cisco Router and Security Device Manager (SDM):** An intuitive, Web-based device manager that provides easy and reliable deployment and management of Cisco access routers, including Cisco IOS IPS, Cisco AIM, and Cisco NM-CIDS.
Enterprise IPS Monitoring and Event Correlation Solutions	• **Cisco Security MARS:** An appliance-based solution that correlates data from across the enterprise and uses your existing network and security investments to identify, isolate, and recommend precision removal of offending elements. When used in conjunction with Cisco IPS Sensor Software Version 6.0, Cisco Security MARS provides a total collaborative solution, protecting your entire network infrastructure from attacks, viruses, worms, and other malicious traffic.
Services	• **Cisco Services for IPS:** As a part of the Cisco Technical Support Services portfolio, Cisco Services for IPS combines Cisco SMARTnet® services with access to IPS signatures into one comprehensive service program that features the following deliverables: ◦ Access to Cisco IPS signatures for a broad range of threats with standard release intervals ◦ Access to operating system software updates such as Cisco IPS Sensor Software Version 6.x ◦ Access to the Cisco Technical Assistance Center, any time, anywhere in the world ◦ Access to Cisco.com and Cisco knowledge base ◦ Options for advanced hardware replacement with or without a field engineer to replace failed hardware For IPS-enabled mitigation devices, this service is required to process signature updates. For more information about Cisco Services for IPS, visit http://www.cisco.com/en/US/products/ps6076/serv_group_home.html

Other Features

- Auto and manual sensor bypass configuration-High availability can be achieved through numerous mechanisms for Cisco IPS sensors. Resiliency and redundancy can be delivered through unique network collaboration; for example, Hot Standby Router Protocol (HSRP) configuration and Cisco EtherChannel® load balancing on Cisco Catalyst switches can divert traffic to a secondary IPS device upon the failure of a primary device. Cisco IPS Sensor Software Version 6.0 also delivers on-box bypass mechanisms that allow the IPS sensor to automatically assume a fail-open condition upon certain types of sensor failure. This bypass mechanism can also be configured manually. The manual configuration requires the user to switch the sensor into bypass mode to achieve the fail-open condition. The result is increased reliability of the IPS device.
- Support for Security Device Event Exchange (SDEE)-SDEE is a standardized IPS communications protocol developed by Cisco for the IDS Consortium at ICSA. Through SDEE, Cisco IPS Sensor Software Version 6.0 delivers a flexible, standardized API to the IPS sensor, facilitating the integration of third-party management and monitoring solutions

with the Cisco IPS solution. This gives users a choice of third-party solutions to monitor events generated by Cisco IPS sensors.

- Extensions to monitoring and notification mechanisms through the delivery of sensor alerts using SNMP traps-In addition to existing alarm formats, Cisco IPS Sensor Software Version 6.0 offers users a tool for transmitting IPS alarms from the sensor to monitoring tools that require alarms to be generated in Simple Network Management Protocol (SNMP) format. SNMP can also be used to poll the IPS sensor for critical diagnostic and status information that gives the user vital signs of the sensor's health.

System Requirements

Inline IPS services require more than one monitoring interface on Cisco IPS 4200 Series sensors. For information on upgrade options, please refer to the Cisco IPS 4200 Series data sheet at http://www.cisco.com/go/4200.

Cisco IPS Sensor Software Version 6.0 is supported on Cisco 4240, 4255, 4260, and 4270 Sensors; the IDSM-2 for Cisco Catalyst 6500 Series Switches; the AIP SSM for Cisco ASA 5500 Series Adaptive Security Appliances; and the IPS Advanced Integration Module (AIM) on Cisco access routers. It is supported in promiscuous-based IDS mode only for the Cisco IDS Network Module.

For More Information

For more information about Cisco IPS Sensor Software Version 6.0, contact your local account representative or visit http://www.cisco.com/go/ips.

Resources

Cisco IPS Alert Center: Provides instant access to specific information about threats, including potential countermeasures and related vulnerabilities. For more information, visit http://www.cisco.com/go/ipsalert.

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

For more information about Cisco ASA 5500 Series Adaptive Security Appliances, visit http://www.cisco.com/go/asa.

For more information about Cisco Security MARS, visit http://www.cisco.com/go/mars or http://www.cisco.com/en/US/products/ps6241/index.html.

For more information about Cisco Security Manager, visit http://www.cisco.com/go/csmanager.

The Cisco IPS Event Viewer (IEV) can be used for monitoring up to 5 IPS sensors. To download Cisco IEV, visit http://www.cisco.com/pcgi-bin/tablebuild.pl/ids-ev.

For more information about Cisco IOS IPS, visit http://www.cisco.com/warp/public/732/Tech/security/intrusion.

For more information about Cisco Security Manager, visit http://www.cisco.com/go/csmanager.

For more information about Cisco SDM, visit http://www.cisco.com/en/US/products/sw/secursw/ps5318/index.html.

For more information about the Cisco Incident Control System, visit http://www.cisco.com/go/ics.

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 C78-389284-03 10/08