Cisco Intrusion Prevention Solutions

Proactive Integrated, Collaborative, and Adaptive Network 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 resiliency.

Networks have evolved into complicated architectures, involving multiple segments, branches, ingress and egress points. Due to this constantly changing landscape, network security must provide a solution that works in concert with network devices, servers, and endpoints.

Intrusion prevention is a core element of a successful security solution; however, it must do more than simply drop traffic it deems as a standard threat.

As a core component of the Cisco® Self-Defending Network, Cisco intrusion prevention system (IPS) solutions deliver comprehensive threat prevention from attacks and threats, regardless of their origin or history. Cisco IPS solutions deliver market-leading threat protection through:

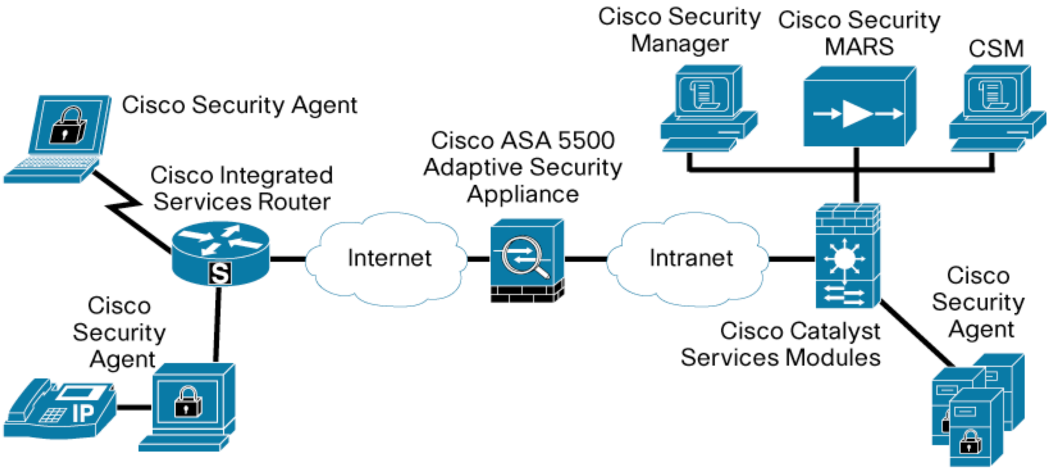
- **Pervasive** n**etwork** i**ntegration**—Cisco IPS solutions defeat threats from multiple vectors, including network, server, and desktop endpoints. The solutions range from purpose-built appliances and integrated firewall and IPS devices to services modules for routers and switches. Cisco IPS solutions protect the network from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic at Layers 2 through 7—across the network. The solutions also simplify deployment and provide contextual analysis through Risk Rating algorithms, giving the user up-to-the-minute security posture information.
- **Collaborative** t**hreat** p**revention**—Cisco IPS solutions employ a unique, system wide security ecosystem that assesses and reacts to threats, delivering unmatched network scalability and resiliency. This collaborative system includes cross-solution feedback linkages, common policy management, multivendor event correlation, attack path identification, passive/active fingerprinting, host-based (Cisco Security Agent) IPS collaboration, load-balancing capabilities, and visibility into encrypted traffic.
- **Proactive** p**osture** a**daptation—**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.

The result is a pervasive, comprehensive, and proactive threat prevention solution that provides end-to-end, day-zero protection of your network.

Integrated Protection Where You Need It the Most

A Cisco IPS Solution delivers inline intrusion prevention capabilities, integrated at key points in the network, allowing for protection of your network's critical assets and data. Figure 1 shows how IPS technology can be strategically deployed throughout the network architecture, providing comprehensive prevention and protection.

Figure 1. Cisco IPS Solutions Deliver Comprehensive Protection Throughout the Network



Pervasive protection is delivered across the network infrastructure, including:

- **Converged perimeter protection**—Cisco ASA 5500 Series Adaptive Security Appliances feature integrated firewall, VPN, and full-featured IPS in a single unified platform, protecting your network as a first line of defense against worms and malicious attacks.
- **Branch protection**—Cisco Integrated Services Routers provide integrated IPS services, protecting against threats before they can enter the network. Threats are identified immediately after de-encryption of terminating VPN traffic, and before they can damage the network or critical assets.
- **Integrated data center protection**—The IDS Services Module 2 (IDSM-2) for the Cisco® Catalyst 6500 Series provides comprehensive intrusion prevention through the integration of security service blades into the fabric of the Catalyst switch.
- **Server/asset and host day-zero protection**—Cisco Security Agent enables day-zero protection of critical assets for endpoints at both the host and server level.
- **Centralized reporting**—Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) monitors, correlates, and mitigates threats, providing increased productivity and simplified regulatory compliance.
- **Centralized management**—Cisco Security Manager provides a powerful, easy-to-use solution to centrally provision all aspects of device configurations and security policies for Cisco IPSs, firewalls, and VPNs.

When combined, these elements provide a comprehensive inline intrusion prevention solution that is capable of detecting and stopping the broadest range of malicious traffic.

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. Policy violations are also managed by assessing 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 detect infection characteristics based on dynamic learning capabilities of network usage.

Multivector Threat Identification

Cisco IPS solutions employ 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 vulnerability signatures prior to the release of an exploit. These multivector threat identification methods include:

- **Rate limiting**—Allows the IPS device to limit certain types of traffic by preventing it from using an excessive amount of bandwidth. This feature can also signal 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). It 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 (for example, an 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 (an HTTP response without an HTTP request, for example).
- **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, and tunneled applications over Port 80. This allows the user to make policy decisions about various traffic types and Multipurpose Internet Mail Extensions (MIME) types to help ensure malicious traffic is disallowed from traversing the network.
- **Anti-IPS evasion techniques**—Provides traffic normalization, IP defragmentation, TCP stream reassembly, and deobfuscation for comprehensive protection against hackers attempting to evade IPSs.
- **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 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, including:

- **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 the IPS 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. This 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 just individual attack mitigation. To provide system wide security, the IPS must scale the protection to other security points throughout that network. Cisco IPS solutions provide unique and 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**—This collaboration 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 as malicious.
- **Cross-solution feedback linkages**—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 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.

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 known and unknown attacks.

- **Anomaly detection/behavioral analysis**—With Cisco IPS solutions, network protection 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 an "on-box" correlation method to deliver accurate worm classification. Cisco IPS Sensor Software 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, providing the ability to implement intrusion prevention in the ways that are the most effective for each specific environment. All solutions are designed for high availability, backed by outstanding customer support, and available in a range of performance levels, from 45 Mbps up to multiple Gbps. Deployment options include dedicated appliances, switch and router modules, and software-based solutions.

The solutions include:

- Cisco IPS 4200 Series Sensors: Deliver intrusion prevention using dedicated, purpose-built devices that protect multiple network segments through the use of up to eight interfaces and support dual operation simultaneously, in both passive and inline modes. The appliance models are:
    - Cisco IDS 4215 Sensor: 80 Mbps
    - Cisco IPS 4240 Sensor: 250 Mbps
    - Cisco IPS 4255 Sensor: 600 Mbps
    - Cisco IDS 4260 Sensor: 1 Gbps

Performance numbers are for tested intrusion detection throughput.

- **Cisco IDSM-2 for the Cisco Catalyst 6500 Series**—Integrates full IPS capabilities into Cisco Catalyst 6500 Series switches using a dedicated module, providing integrated inline protection at 500 Mbps and 2 Gbps with the IDSM-2 Bundle.
- **Cisco IDS Network Module for Cisco access routers**—Integrates traditional intrusion detection into the router using Cisco IPS Sensor Software Version 6.0. This provides added detection, correlation, and identification technology to effectively mitigate against and isolate threats at up to 45 Mbps.
- **Cisco Advanced Inspection and Prevention Security Services Module (AIP SSM) for Cisco ASA 5500 Series Adaptive Security Appliances**—Provides IPS capabilities as part of the Cisco ASA 5500 Series multifunction threat mitigation solution.
- **Cisco IOS IPS**—Provides a focused set of IPS capabilities using Cisco IOS Software on the router.

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.

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, providing 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 the Cisco IOS IPS feature set and Cisco IDS network modules.

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. It is also a prerequisite for the premium service Cisco Incident Control System. 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/ips.

Cisco IPS Sensor Software Version 6.0 is supported on Cisco IDS 4215, 4235, 4240, 4255, and 4260 Sensors; the IDSM-2 for Cisco Catalyst 6500 Series Switches; and the AIP SSM for Cisco ASA 5500 Series Adaptive Security Appliances. It is supported in promiscuous-based IDS mode only for the Cisco IDS Network Module.

For More Information

For more information about Cisco IPS solutions, 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/cgi-bin/tablebuild.pl/ids-ev. This site requires a Cisco.com log in.

For more information about Cisco IOS IPS, visit http://www.cisco.com/en/US/products/ps6634/products_ios_protocol_group_home.html.

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.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**