DATA SHEET

CISCO INTRUSION PREVENTION SYSTEM SOLUTION

The Cisco® Intrusion Prevention System (IPS) is an inline, network-based solution, designed to accurately identify, classify, and stop malicious traffic, including worms, spyware/adware, network viruses, and application abuse, before they affect business continuity.

Utilizing Cisco IPS Sensor software v5, the Cisco IPS solution combines inline prevention services with innovative technologies to improve accuracy. The result is total confidence in the provided protection of your IPS solution, without the fear of legitimate traffic being dropped. The Cisco IPS solution also offers comprehensive protection of your network through its unique ability to collaborate with other network security resources, providing a proactive approach to protecting your network.

The Cisco IPS solution helps users stop more threats with greater confidence through the use of the following:

- **Accurate inline prevention technologies**—Provides unparalleled confidence to take preventive action against a broader range of threats without the risk of dropping legitimate traffic. These unique technologies offer intelligent, automated, contextual analysis of your data and help ensure you are getting the most out of your intrusion prevention solution.
- **Multivector threat identification**—Protects your network from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic in Layers 2 through 7.
- **Unique network collaboration**—Enhances scalability and resiliency through network collaboration, including efficient traffic capture techniques, load-balancing capabilities, and visibility into encrypted traffic.
- **Comprehensive deployment solutions**—Provides solutions for all environments, from small and medium-sized businesses (SMBs) and branch office locations to large enterprise and service provider installations.
- **Powerful management, event correlation, and support services**—Enables a complete solution, including configuration, management, data correlation, and advanced support services. In particular the Cisco Security Monitoring, Analysis, and Response System (MARS) identifies, isolates, and recommends precision removal of offending elements, for a networkwide intrusion prevention solution. And the Cisco Incident Control System prevents new worm and virus outbreaks by enabling the network to rapidly adapt and provide a distributed response.

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.

ACCURATE PREVENTION TECHNOLOGIES

Cisco IPS Sensor software includes innovative technologies that give users the confidence to take prevention actions against a broader range of threats. These technologies, including correlation and validation tools, greatly reduce the risk of dropping legitimate traffic. This extra level of accuracy is achieved through the use of:

- **Cisco Risk Rating**—Offers unprecedented reliability and complete confidence to enable your inline prevention deployment. Traditional intrusion prevention has relied on severity rating as its sole method of determining the potential damage associated with an event; Cisco Risk Rating provides a more accurate representation and risk-balanced assessment of the potential damage per event through the use of four separate values:
  - **Event severity**—A user-modifiable weighted value indicating potential damage per event.
  - **Signature fidelity**—A user-modifiable weighted value indicating accuracy of the signature.

  - **Asset value**—A user-defined value indicating the importance of the attack target.
  - **Attack relevancy**—An internal weighted value based on the susceptibility of the target to this attack type. The aggregate of these values provides a single risk rating for the event. Most of these terms are configured by default and require minimal user involvement.
- **Cisco Meta-Event Generator**—Provides unique correlation of events in order to accurately detect and stop worms. As worms move through your network, they generate many alarms of varying degrees of severity. Cisco Meta-Event Generator links these seemingly unrelated lower-severity alarms into a high-severity, high-risk event, enabling the user to confidently drop the associated packets. Meta-Event Generator achieves this by modeling worm behavior and correlating specific time between events, network behavior, and multiple exploit behavior.

MULTIVECTOR THREAT IDENTIFICATION

At the core of Cisco IPS Sensor software 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. Threat identification methods include:

- **Enhanced virus/malware protection**—New with IPS Sensor software v5.1. Cisco Systems® and Trend Micro have collaborated to provide enhanced, networkwide, inline protection against new viruses, worms, and other malicious software. This enhanced protection is part of a premier service called the Cisco Incident Control System. See the Services section, later in this document, for more information.
- **Rate limiting**—New with IPS Sensor software v5.1. Allows the IPS device to limit certain types of traffic by preventing them from utilizing an excessive amount of bandwidth. This feature can also signal external devices such as Cisco IOS® Software routers to perform rate limiting to accomplish the same function.
- **IPv6 detection**—New with IPS Sensor software v5.1. Enhanced visibility into IPv6 traffic to identify malicious traffic.
- **IP in IP detection**—New with IPS Sensor software v5.1. 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**—Provides protocol decoding and validation for network traffic. Cisco IPS Sensor software v5.0 monitors all of the 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, Domain Name System (DNS), remote-procedure call (RPC), NetBIOS, Network News Transfer Protocol (NNTP), 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. An example would be 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 control of peer-to-peer, instant messaging (IM), and tunneled applications over Port 80. This allows the user to make policy decisions concerning 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**—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 (TAME) policy language.

These techniques allow Cisco IPS Sensor software to address both known and unknown attack types, including:

- **Policy violations**—Reconnaissance activity, misuse activity, and file-sharing threats.
- **Anomalous activities**—Denial-of-service (DoS) activity, where an attempt is made to consume bandwidth or computing resources, resulting in the disruption of normal operations. Examples include Trinoo, TFN, and SYN floods.
- **Vulnerability exploitation**—Back Orifice, failed login attempts, and TCP hijacking.

UNIQUE NETWORK COLLABORATION

Cisco IPS software uses the network to offer enhanced scalability and resiliency through its unique network collaboration. Through communication between Cisco IPS sensors and Cisco network devices, the Cisco IPS solution delivers:

- Load sharing of multi-VLAN traffic through support for 802.1q
- Multiple VLAN protection, also known as "inline on a stick," providing protection and inspection for up to 255 VLAN pairs on a single IPS device interface
- Efficient bandwidth management through Virtual Access Control List (VACL) Capture, Switched Port Analyzer (SPAN), or Remote SPAN (RSPAN) on the switch
- Scaling of up to 8 Gbps of performance through load-balancing algorithms supported on the switch
- High availability of IPS devices delivered through switch interaction using Cisco EtherChannel® technology
- Visibility into encrypted traffic through collaboration with Cisco switches and routers providing VPN decryption services

COMPREHENSIVE DEPLOYMENT SOLUTIONS

Cisco offers a wide range of network IPS deployment solutions, giving customers the ability to implement intrusion prevention in the ways that are the most effective for their environments. All solutions are designed for high availability and backed by outstanding customer support and are 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 are:

- **Cisco IPS 4200 Series sensor appliances**—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 promiscuous and prevention modes. These appliances provide a range of performance, from 80 Mbps up to 8 Gbps, when used in collaboration with Cisco EtherChannel load balancing on Cisco Catalyst® 6500 Series switches. The appliance models and their base performance levels are:
  - Cisco IDS 4215 Sensor: 80 Mbps
  - Cisco IPS 4240 Sensor: 250 Mbps
  - Cisco IPS 4255 Sensor: 600 Mbps
  - Cisco IDS 4250 XL Sensor: 1000 Mbps

Performance numbers are for tested intrusion detection throughput.

- **Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module**—Integrates full IPS capabilities into Cisco Catalyst 6500 Series switches using a dedicated module, providing integrated protection at 600 Mbps.
- **Cisco IDS Network Module for Cisco access routers**—Integrates traditional intrusion detection into the router using Cisco IPS Sensor software v5.0. This provides added detection, correlation, and identification technology to effectively mitigate and isolate threats at up to 45 Mbps.
- **Cisco Advanced Inspection and Prevention Security Services Module for Cisco ASA 5500 Series adaptive security appliances**—Provides IPS capabilities as part of the ASA 5500 Series multifunction threat mitigation solution.
- **Cisco IOS Software 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.
- **CiscoWorks VMS**—A multidevice configuration and alarm management tool offering a unified, scalable view of all security events. With the CiscoWorks VMS solution, events from all types of security devices, including firewalls, VPNs, and IPSs, can be viewed from a single console in a browser-based GUI. Multiple security devices can be configured and managed, making it easier to manage security across the enterprise. Additionally, CiscoWorks VMS provides enhanced security management through the inclusion of flexible reporting and notification, automated updates, and event correlation.
- **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 Software IPS feature set and Cisco IDS network modules.

Event Correlation Solutions

- **Cisco Security Monitoring, Analysis, and Response System (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. MARS, when used in conjunction with Cisco IPS Sensor software v5, provides a total collaborative solution, protecting your entire network infrastructure from attacks, viruses, worms, and other malicious traffic.
- **CiscoWorks Security Information Management Solution (SIMS)**—An event management solution that collects, analyzes, and correlates security event data from across the enterprise. The award-winning CiscoWorks SIMS 3.1 can help you identify and respond to more threats, more effectively, without adding additional staff.

Services

- **Cisco Services for IPS**—A standard service level, providing industry-leading protection through scheduled IPS updates. Providing up-to-date protection from vulnerabilities, exploits, and malicious attacks, Cisco Services for IPS helps ensure you get the most out of your intrusion prevention investment.
- **Incident Control System**—The Cisco Incident Control System prevents new worm and virus outbreaks by enabling the network to rapidly adapt and provide a distributed response. Because the time that it takes a worm or virus outbreak to spread around the world has decreased from days to minutes, a proactive response minutes after an outbreak is detected is necessary to help ensure the safety of enterprise networks. The Cisco Incident Control System provides a solution to meet that need. Collaborating with existing Cisco outbreak prevention solutions, including the Cisco IPS solution, the Cisco Incident Control System provides rapid distribution of worm and virus immunization capabilities throughout the network. This fast, proactive approach prevents worms and viruses from becoming entrenched, thus helping ensure network availability, and decreasing the costs associated with damage cleanup.

The primary features of the system include:

- Up-to-the-moment threat intelligence, as discovered by Trend Micro, an industry-leading antivirus and worm expert
- Rapid response, enabling proactive prevention of worms and viruses
- Empowering of existing Cisco network and security devices to adapt in real-time for a coordinated networkwide response

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

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.

Ordering Information

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 MARS, visit http://www.cisco.com/go/mars.

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

For more information about CiscoWorks VMS, visit http://www.cisco.com/go/vms.

For more information about CiscoWorks SIMS, visit http://www.cisco.com/en/US/products/sw/cscowork/ps5209/index.html.

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.

CISCO SYSTEMS

Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA