Q&A

CISCO IPS SENSOR SOFTWARE VERSION 5.0

GENERAL

Q. What are the benefits of Cisco IPS Sensor Software Version 5.0?

A. Cisco® IPS Sensor Software Version 5.0 delivers inline intrusion prevention to stop known and unknown attacks. As part of the Cisco Systems Intrusion Prevention System (IPS) Solution, Cisco IPS Sensor Software Version 5.0 provides the intelligence to accurately detect, classify, and stop malicious applications, viruses, and worms before they can affect your network. Using Cisco's broad threat coverage, Cisco IPS Sensor Software Version 5.0 identifies an extensive range of attacks using multiple inspection and detection capabilities. Cisco's accurate prevention technologies provide the confidence to stop malicious traffic through the use of correlation and validation tools, protecting valuable business-critical data and resources without the fear of dropping valid traffic.

Q. Can Cisco IDS sensors be upgraded to support Cisco IPS Sensor Software Version 5.0 features?

A. Cisco IPS Sensor Software Version 5.0 supports several platforms, including the Cisco IDS 4215, IDS 4235, IPS 4240, IPS 4255, IPS 4250-XL, and the IDSM-2. Cisco IPS Sensor Software Version 5.0 will also be supported on the IDS-4210 and the NM-CIDS (network module for Cisco access routers), in promiscuous IDS mode only.

Q. Does the Cisco IPS Version 5.0 Sensor upgrade require a CD upgrade on existing sensor platforms?

A. No. Cisco IPS Version 5.0 Sensor supports a simple over-the-network upgrade that does not require a CD.

Q. Does the Cisco IPS Sensor Software v5 require a support contract or license?

A. Yes. As with any version of IDS or IPS solution, a support contract is required to obtain support including access to software updates, signature updates, and TAC assistance. With IPS Sensor Software version 5.0 and above, the sensor will also require the presence of a license key to enable the processing of signature updates.

Q. How is the license key obtained?

A. The license can be obtained through either of two methods: 1) manual registration at the Cisco licensing web site (http://www.cisco.com/go/license) or through the automated licensing mechanism provided in the IPS Device Manager.

Q. What type of support contract or service offering is available for IPS devices?

A. Cisco is releasing a new service offering called Cisco Services for IPS. This offering replaces the current SMARTnet offerings.

Q. What is included with Cisco Services for IPS?

A. Cisco Services for IPS includes:

- Access to signature file library and new signature files for each registered IPS
- Notification of availability of new or updated signature files
- Support for licensed operating system software for each registered IPS
- Software updates including maintenance, minor, and major releases
- Access to security engineers at the Cisco Technical Assistance Center (TAC) 24 hours a day, 7 days a week
- Registered access to Cisco.com and its online knowledge base and service request management tools
- Advance replacement of hardware parts, depending on the coverage selected

Q. Which Cisco support offerings entitle the end user to signature file updates?

A. Cisco Services for IPS includes signature file updates, registered access to Cisco.com, access to TAC, operating system updates, and hardware replacement.

Q. How do I obtain Cisco IPS v5 if I do not have a Cisco Services for IPS contract on my existing Cisco IDS sensors?

A. Cisco IPS v5 can be obtained by purchasing IPS-SW-K9-U for users who do not have a Cisco Services for IPS contract.

Note: A valid Cisco Services for IPS contract is required to obtain IPS signatures for the IPS v5 sensor.

Q. Will SMARTnet continue to be an option for IPS after Cisco Services for IPS becomes available?

A. Cisco Services for IPS will replace SMARTnet for IPS.

Q. If I upgrade my sensors to Cisco IPS Sensor Software Version 5.0, will I be entitled to new signature updates on the Cisco IPS Sensor Software Version 5.0 code base?

A. Cisco IPS Sensor Software Version 5.0 requires a valid Cisco SMARTnet® contract in order to obtain incremental signature upgrades.

Q. How do I obtain Cisco IPS Sensor Software Version 5.0 if I do not have a Cisco SMARTnet contract on my existing Cisco IDS sensors?

A. Users without a Cisco SMARTnet contract can obtain Cisco IPS Sensor Software Version 5.0 by purchasing IPS-SW-K9-U. Note: A valid SMARTnet contract is required to obtain IPS signatures for the Cisco IPS Version 5.0 Sensor

Q. If I choose not to upgrade to Cisco IPS Sensor Software Version 5.0, will I continue to receive signature updates on the Cisco IDS Sensor Software Version 4.x code base?

A. Cisco will support signatures on the Cisco IDS Sensor Software Version 4 train for a minimum of one year after the availability of Cisco IPS Sensor Software Version 5.0.

Q. What is Cisco Incident Control System?

A. The Cisco Incident Control System is a premium level service, which 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.

Q. What are the hardware requirements for inline IPS capabilities?

A. A Cisco IPS Version 5.0 Sensor can be configured either in the IPS (inline) mode or the promiscuous IDS mode. If your sensor already has more than one monitoring interface, no additional hardware is required to run Cisco IPS Sensor Software Version 5.0 in the IPS (inline) mode. IPS services require at least one monitoring interface pair (two monitoring interfaces). Cisco provides the option of upgrading sensors with a single monitoring interface to support multiple monitoring interfaces. For more information on the various IDS and IPS sensor platforms and part numbers, please refer to Cisco IPS 4200 Series Data Sheet located at: http://www.cisco.com/go/ips

Q. What are the features delivered by Cisco IPS Sensor Software Version 5.0?

A. A complete description of features supported with Cisco IPS Sensor Software Version 5.0 can be obtained with the product's data sheet, available at: http://www.cisco.com/go/ips

Q. What are the management/monitoring options for Cisco IPS Sensor Software Version 5.0?

A. The following options deliver support for Cisco IPS Sensor Software Version 5.0:

- CLI (embedded in IPS sensor)
- IPS Device Manager (embedded in IPS sensor)
- CiscoWorks VPN/Security Management Solution (VMS)
- CiscoWorks Security Information Management Solution (SIMS)

Q. Where can I obtain more information on CiscoWorks VMS and SIMS?

A. For more information on CiscoWorks VMS, please visit http://www.cisco.com/go/vms. For more information on CiscoWorks SIMS, please visit http://www.cisco.com/go/sims.

Q. How can I obtain more information on late breaking threats and attack mitigation signatures supported on the Cisco IPS Version 5.0 Sensor?

A. The Cisco IPS Alert Center (http://www.cisco.com/go/ipsalert) is a centralized site on Cisco.com that delivers comprehensive information on threats that can be mitigated using Cisco IPS sensors. This site provides the user with detailed information on:

- Breaking News-Provides real-time information on late-breaking threats
- Latest Threats-List of the threats surfaced in the last 7 days
- Active Threats-Threats seen most frequently & pose greatest danger
- Cisco IPS Active Updates-Links to the last 3 IPS Active Update bulletins, the archives of bulletins & the IPS bulletin subscription site
- IPS signature descriptions-through the capability of performing advanced searches on the IPS NSDB (Network Security Data Base) entries

Q. Does Cisco support a site that allows where Cisco IPS users can discuss topics related to IPS?

A. Yes. The Cisco IPS Networking Professionals site allows Cisco IPS users to share questions, suggestions, and information about IPS technologies. This site can be accessed at http://www.cisco.com/go/netpro.

IPS SERVICES TO STOP WORMS AND VIRUSES

Q. Can Cisco IPS Sensor Software Version 5.0 stop worms and viruses from compromising target systems?

A. Yes. Cisco IPS Sensor Software Version 5.0 delivers inline IPS services that have the ability to drop packets and prevent attacks from reaching target systems.

Q. Can a single Cisco IPS device deliver IPS services to multiple subnets on the network?

A. Yes. Multiple monitoring interfaces on a sensor can be paired up such that each interface pair will be capable of supporting a single instance of IPS services. For example, a sensor that supports four monitoring interfaces can simultaneously deliver IPS services to two network subnets.

Q. Can a sensor operate in either the promiscuous-based IDS mode or the inline-based IPS mode?

A. Yes. Cisco IPS Sensor Software Version 5.0 can be installed on a sensing device in either mode.

Q. Can a sensor operate simultaneously in both the promiscuous-based IDS mode and the inline-based IPS mode?

A. Yes. A single IPS device may be configured such that it can operate in a hybrid mode to deliver promiscuous-based IDS and inline-based IPS services, simultaneously. For example, if a device contains five monitoring interfaces, it can be configured to deliver two instances of inline IPS services (through four of the five interfaces) and a single instance of promiscuous IDS operations using the fifth monitoring interface.

Q. What are the various response actions that can be configured on Cisco IPS appliances?

A. Multiple automated response actions include packet drops, connection termination, access control list (ACL) blocking on routers, switches, and firewalls, generation of SNMP traps, and IPS session logging.

Q. What types of packet-drop actions are available with the inline IPS services delivered with Cisco IPS Sensor Software Version 5.0?

A. Cisco IPS Sensor Software Version 5.0 delivers numerous packet-drop actions, including dropping the trigger packet, dropping the entire flow (that contains the trigger packet), and dropping all packets from the attacker's source IP address.

Q. Can multiple response actions be performed simultaneously?

A. Yes. At times (depending on the type of threat, deployment scenario, and other criteria), multiple response actions may be configured to result in effective worm and virus containment.

Q. How does a Cisco IPS Version 5.0 sensor react to sensor software failure?

A. Since the IPS sensors are inline such that packets flow through the sensor, the IPS sensors must support high-availability features to ensure business continuity. Cisco IPS Sensor Software Version 5.0 delivers automated fail-open mechanisms that will allow the sensor to pass packets despite sensor software failure.

Q. Will the fail-open capability operate if a hard disk fails on a sensor?

A. Yes. The sensor can be configured to operate in fail-open mode in the event of a hard disk failure.

Q. Can this fail-open feature be manually configured?

A. The sensor can be manually put into fail open mode for troubleshooting or testing purposes.

Q. How can my existing networking infrastructure add reliability to my IPS deployment?

A. IPS appliances allow network redundancy through the use of spanning tree resolution. Because IPS devices act as layer two bridges, connecting two or more between the same set of switches will allow the switch to determine the correct path to send packets to.

Q. What mechanisms are available to monitor the health of IPS sensors?

A. Cisco IPS Sensor Software Version 5.0 supports Simple Network Management Protocol (SNMP) to deliver alarm information through SNMP traps. SNMP can also be used to query the sensor for critical sensor statistics and health. Sensor health information can also be obtained at the management console.

Q. How can I integrate IPS services into my network infrastructure?

A. Cisco IPS Sensor Software Version 5.0 delivers the industry's first IPS solution that is integrated into Cisco Catalyst switches, with the IDSM-2 module that can be deployed in inline IPS mode.

ACCURATE PREVENTION TECHNOLOGIES

Q. What is accurate prevention technology, being delivered by Cisco IPS Sensor Software Version 5.0?

A. Traditional IPS devices have been prone to generating false alarms. Packets that are dropped based on false alarms can result in network disruption if the dropped packets are required for mission-critical applications downstream of the IPS sensor. The cornerstone of Cisco IPS Sensor Software Version 5.0 minimizing false alarms, such that users can gain a high level of confidence when dropping packets in IPS mode, thereby ensuring business continuity. Crucial features such as Risk Rating and Meta-Event Generator (MEG) allow users to make intelligent decisions when performing IPS drop actions.

Q. What are the main benefits of Risk Rating?

A. Risk Rating provides the user with an indication of the relative risk of the traffic or offending host continuing to access the user's network. This rating can be used either to illuminate the events that require immediate administrator or to provide a means for developing risk-oriented event action policies. The Risk Rating is a calculated number that has four primary components-alert severity rating, signature fidelity rating, attack

relevancy rating, and target value rating. The Risk Rating ranges in value from 0 to 100. The higher the value for a particular event, the greater the accuracy of an inline IPS packet drop action that is associated with that event.

Q. What are the various components of Risk Rating?

A. The event severity rating is a user-modifiable weighted value that characterizes the damage potential of the suspect traffic. The attack relevancy rating is an internal weighted value that characterizes any additional knowledge that the sensor may have about the target of the event. The asset value rating is a user-defined value that represents the user's perceived value of the target host. The signature fidelity rating is a user-modifiable weighted value that characterizes the fidelity of the signature that has detected the suspect activity.

Q. Is the user required to manually specify or tune all Risk Rating components?

A. While these components are user-modifiable, it must be emphasized that the Risk Rating is dynamically generated for each event without making it incumbent upon the user to tune each component. This greatly enhances the user experience by delivering a usable framework that does not require intensive user intervention.

Q. How can the resulting value of an event's Risk Rating be used to enhance the confidence level of inline IPS packet-drop actions?

A. The primary benefit of Risk Rating is the ability to define global thresholds within the range of values that the Risk Rating can assume. When a Risk Rating threshold is defined, global event action overrides can be assigned to the various thresholds. For example, if a Risk Rating threshold of 85 is specified, it can be associated with a packet-drop action such that whenever a Risk Rating value greater than 85 is generated, the malicious activity will be stopped before it can cause damage to critical assets.

Q. What is MEG?

A. Cisco IPS Sensor Software Version 5.0 incorporates advanced sensor-level event correlation that gives security administrators an automated method for enhancing the confidence level of the classification of malicious activity detected by the sensor.

Q. How is MEG different from correlation features that may be delivered by IPS management systems?

A. The effectiveness of IPSs is greatly enhanced when correlation algorithms are embedded in the sensor. The sensor can proactively take automated response actions to effectively stop worms and viruses, immediately after they are identified by the IPS device.

Q. For multifaceted worms that target more than one vulnerability, multiple alarms can result from a single worm outbreak. How can these events be efficiently correlated while assigning the most appropriate mitigation action to the correlated event?

A. Nimda is an example of a worm that exploited multiple vulnerabilities during its propagation across networks, resulting in the triggering of multiple events over a short time span. MEG takes the guesswork out of making an accurate assessment on the occurrence of multifaceted worms, such as Nimda. MEG can consolidate all events pertaining to the worm into a single meta event, called “Nimda”; more importantly, all packets associated with this malicious activity will be dropped, preventing the worm from reaching its target. This is especially critical because the meta event constituents can have low Risk Rating values that would not make them candidates for inline IPS packet drops. But in the context of the meta event that signifies worm activity, these packets can now be confidently dropped.

Q. How can events generated from multiple threat identification techniques be effectively correlated to improve the overall confidence level of the resultant event?

A. MEG can be used to correlate and corroborate events that are generated through the use of the hybrid detection techniques. For example, if a denial of service (DoS) activity is detected through the triggering of a traffic anomaly algorithm and a classical “flood” type of signature, MEG can be used to corroborate one event with the other, thereby delivering a single meta event that indicates a higher likelihood that the DoS activity has actually occurred. This allows the user to make a more informed decision.

Q. How can insight into the lifecycle of a malicious event enhance the confidence level of the resultant event?

A. Historical trend analyses performed to characterize the lifecycle of worms often reveal a certain sequence of actions that are detected just prior to its penetration. These actions may occur in the “probing phase”, when a chain of reconnaissance activities is performed against the target network.

MEG can be used to correlate the precursors to worm penetration with the event pertaining to the worm itself. This increases the confidence level of dropping packets associated with the worm.

MULTI-VECTOR THREAT IDENTIFICATION

Q. What are the main benefits of the Cisco IPS Sensor Software Version 5.0 Application Inspection Engine?

A. Organizations are becoming increasingly dependent on Web services. This increases their exposure to blended application-layer attacks. The detection of misuse and attempts to bypass any implemented Web services security mechanisms requires the ability to process application-layer data. Cisco IPS Sensor Software Version 5.0 delivers an advanced Application Inspection Engine (AIE) that uses sophisticated algorithms to perform application analysis. The Application Inspection Engine allows organizations to use their Cisco IPS sensors to enforce policy decisions based on content detected at the application layer and stop malicious behavior on the network.

Q. Does the IPS sensor have visibility into application-layer attacks that would allow policy decisions to permit/deny such traffic into the network?

A. Application inspection technologies delivered in Cisco IPS Sensor Software Version 5.0 allow enforcement of policy decisions based on content detected at the application layer. This can also be extended to control permitted traffic via user-defined policies.

Q. How does a Cisco IPS device deal with users who are attempting to tunnel unauthorized applications through commonly used ports as a way of subverting corporate security policies?

A. Cisco IPS Version 5.0 Sensor detects and prevents covert channel tunneling through Port 80. For example, a request message can be inspected that indicates traffic is being tunneled through Web ports using the application GoTomypc. Similarly, users can easily disguise the use of file sharing applications such as Kazaa by tunneling the traffic through Port 80. These types of activities can be accurately identified and subsequently stopped. The benefits to the user are increased visibility into activity targeted to subvert corporate security policy, which eventually results in worm mitigation and bandwidth preservation.

Q. Attackers can manipulate HTTP methods to disguise the insertion of malicious code. How can Cisco IPS Version 5.0 Sensor prevent this from happening?

A. Cisco IPS Version 5.0 can be configured to enforce RFC compliance for HTTP methods to prevent such misuse. The users may permit or deny specific HTTP methods (GET or POST, for example) to control HTTP transactions in a detailed manner.

Q. When a worm or virus injection vector is associated with an e-mail attachment that can be characterized with certain commonly used MIME types, how can I ensure that these MIME types are not permitted into my network?

A. Cisco IPS Sensor Software Version 5.0 delivers advanced MIME filtering mechanisms that can accurately classify and stop certain MIME types from causing damage to critical assets.

Q. Attackers have the ability to modify the content of certain MIME types and embed malicious code within the body of a message as a way of disguising attack vectors. How can my IPS sensor prevent this activity?

A. Cisco IPS Version 5.0 has the ability to verify the content header with the actual content. For example, if the MIME type is a JPEG, the IPS sensor can verify that the message body is indeed a JPEG message. This can help prevent attacks where malicious code in contained in a non-JPEG attachment under a JPEG MIME-type-header.

Q. What is the main benefit of Cisco's VoIP engine?

A. With the widespread deployment of VoIP, the infrastructure supporting VoIP implementation must be secured appropriately. Even minimal downtime can result in millions of dollars of lost revenue and greater customer support costs. Cisco IPS Sensor Software Version 5.0 supports a VoIP engine that accurately identifies and prevents attacks in VoIP environments. The protection of voice gateways from attacks such as DoS attacks and buffer overflows helps to ensure business continuity.

Q. How can the VoIP engine help protect my H.323-based voice infrastructure from attacks?

A. Many attacks in VoIP environments are initiated before the actual call is in session, during the period when the call is being set up through the exchange of setup messages. The Cisco VoIP engine helps ensures protocol compliance of H.225 call setup messages. This engine also delivers protection against attacks to voice gateways through advanced buffer overflow and URL overflow mitigation.

Q. Does Cisco IPS Sensor Software Version 5.0 support inspection and mitigation of threats in portions of my network where Multiprotocol Label Switching (MPLS) traffic exists?

A. Cisco IPS Version 5.0 has the ability to look deep into MPLS traffic to stop threats in MPLS environments.

Q. Does Cisco IPS deliver protection from virus activity?

A. Network antivirus capabilities that are supported by Cisco IPS Sensor Software Version 5.0 can accurately classify and prevent virus outbreaks.

Q. How does the Cisco IPS Version 5.0 Sensor deal with traffic that is intentionally modified by an attacker using IPS evasion tools as a way of evading IPS devices?

A. Cisco IPS Sensor Software Version 5.0 supports advanced traffic normalization algorithms to fix traffic through techniques such as fragmentation reassembly and stream normalization.

Q. Can the Cisco IPS Version 5.0 Sensor stop IPv4 attacks in IPv6 environments?

A. The Cisco IPS Version 5.0 Sensor can identify attacks contained in IPv4 traffic that is being encapsulated in IPv6.

FOR MORE INFORMATION

Please visit http://www.cisco.com/go/ips for more information on the Cisco IPS solution. This site includes data sheets, white papers, and solutions guides that will provide more information on Cisco IPS Sensor Software Version 5.0.

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

205404.V_ETMG_KL_9.05

Printed in the USA