Cisco IPS 4200 Series Sensors

In today's busy network environments, business continuity relies on effective network intrusion prevention to stop malicious attacks, worms, and application abuse before they affect your data and resources. Cisco® IPS 4200 Series Sensors and Cisco IPS Sensor Software are core components of Cisco's intrusion prevention solution. Using Cisco IPS Sensor Software's inline prevention technology, Cisco IPS 4200 Series Sensors accurately detect, classify, and stop malicious traffic on IPv4 and IPv6 networks.



Product Overview

Cisco IPS 4200 Series Sensors deliver high-performance intelligent detection with precision response, extending the diverse Cisco IPS solution from the network edge to the data center for both IPv4 and IPv6 networks.

Intelligent Detection

Cisco IPS 4200 Series Sensors accurately identify, classify, and stop malicious traffic, before it affects your business.

- Cisco IPS technology is engineered to prevent malicious activity, including worms, directed attacks, distributed denial of service attacks, reconnaissance, and application abuse.
- Built on advanced Cisco security and network intelligence, modular inspection capabilities can detect and prevent threats to the entire network stack, from applications to Address Resolution Protocol (ARP). Cisco IPS technology extends this expertise by providing industry-leading protection from evasion.
- Cisco IPS provides adaptive vulnerability and anomaly detection. Signatures are focused on vulnerabilities, so your ability to detect threats remains intact, even as exploits change. For emerging "day-zero" threats, Cisco IPSs learn about your network, detect behavioral anomalies, and mitigate attacks without a signature update.
- Cisco IPS technology and signature services are developed by an extensive global team of Cisco security experts. These experts conduct on-going research into emerging threats, inspection methods, and prevention strategies, in order to continue to drive up-to-date vulnerability-based signatures and advanced intrusion prevention capabilities.

GoSecure, Inc.
Exhibit 2003
CrowdStrike v. GoSecure
IPR2025-00070
Ex. 2003-001

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Precision Response

Cisco IPS 4200 Series Sensors deliver precision threat-impact analysis, enabling you to respond to threats with confidence.

- Cisco IPS provides you with the most knowledge of potential threat impact by calculating a real-time measurement of risk for every event. An adaptive multidimensional algorithm combines attack details with live network knowledge to produce a calibrated risk measurement.
- Cisco IPS has the richest set of response actions for flexible and precise response policies. You can tailor your IPS policy to each network environment and threat – directly dropping packets, terminating sessions, and rate limiting, or implementing access control and rate limiting on routers and other security appliances throughout the network.
- Cisco IPS threat rating assesses post-response residual risk, enabling incident handlers to focus on the highest-impact events. Risk measurements are updated following an active response to prioritize events with the greatest potential to impact your business.
- Cisco IPS records live, in-depth information on every alert, enabling incident handlers to rapidly diagnose and resolve events. Context data and session logging provide packet-level detail before, during, and after each event.

Intrusion Prevention for the Self-Defending Network

Integrated

- The most diverse line of IPS sensors provide the right tool for the right job, anywhere in the network
- Intrusion prevention is integrated into the fabric of the network
- Solution is built on Cisco security and network intelligence

Adaptive

- Modular inspection engines provide rapid response with minimal downtime
- Behavioral anomaly detection protects against day-zero attacks
- Dynamic risk-based threat rating adapts policy to attacks in real time

Collaborative

- On-box and network-wide correlation provides greater confidence
- Network and endpoint collaboration provide greater visibility and effectiveness
- A common, solution-based management interface helps reduce operational costs

Policy-Based Management

Cisco IPS 4200 Series Sensors reduce the time and effort required to implement security measures by using management and correlation tools that focus on policy, yet provide the granularity you need to fine-tune your IPS configuration.

- Instantly increase your security visibility, and easily define your inspection policy, out of the box, with integrated graphical management and event viewing tools.
- Gain a unified, end-to-end view of your security posture and a holistic approach to security Incident Management, with Cisco Security Monitoring, Analysis, and Response System (MARS).
- Reduce the cost of Change and Configuration Management activities, using the rich Cisco Security Manager (CSM) graphical interface to update policies on thousands of devices in a few simple steps.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Enterprise Resilience

Cisco IPS 4200 Series Sensors are designed to withstand failures and minimize downtime, giving you the assurance that your IPS solutions can bear the most strenuous peaks of your day-to-day operations.

- Built-in, comprehensive monitoring detects potential failures at every level of operation, including devices, services, communications, and monitoring link failures.
- Automated and manual fail-open options enable you to define the right policy for a worst-case scenario, whether no packet should pass unexamined, or your traffic must flow, “no matter what.” Integrated hardware bypass enables you to extend this policy to total system and power failures.

Flexible Deployment

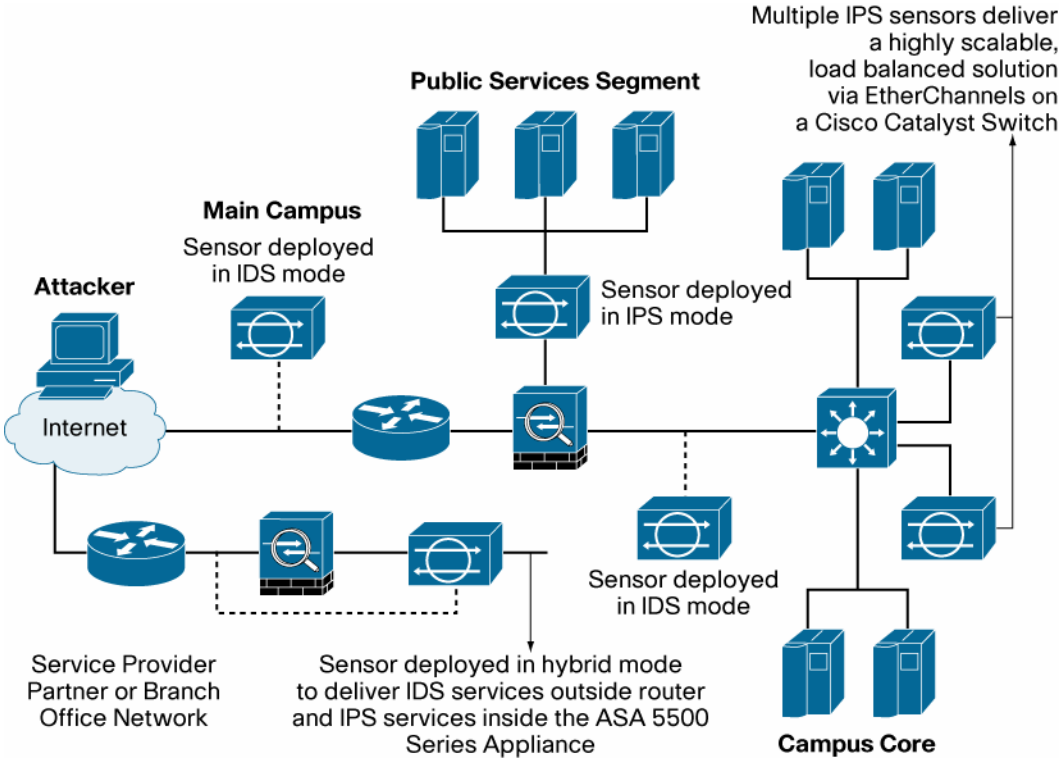
As part of the most diverse line of IPS technologies available, Cisco IPS 4200 Series Sensors can be deployed in a variety of IPv4 and IPv6 network environments. The wide range of performance and interface configurations in the IPS 4200 Series enable you to achieve effective intrusion prevention with unparalleled flexibility throughout the edge, campus, and data center.

- Cisco IPS 4200 Series Sensors can be deployed in an inline IPS configuration, a promiscuous IDS configuration, or both inline and promiscuous simultaneously.
- Your critical assets on IPv4 and IPv6 networks can be protected with a single Cisco IPS 4200 Series Sensor for maximum deployment flexibility and lower total cost of ownership. Cisco IPS 4200 Series Sensors provide investment protection for customers planning or considering migration to IPv6 or hybrid IPv4 and IPv6 networks.
- Appliances in the Cisco IPS 4200 Series are available in a variety of multiple-interface configurations, featuring copper and fiber gigabit ethernet, and 10 gigabit ethernet interfaces. You can also configure thousands of logical interfaces and implement intrusion prevention within your VLAN environment, giving you the design flexibility to address all of your deployment requirements, from simple to complex.
- Cisco IPS technologies also feature industry-leading virtualization capabilities. Virtual sensors enable the virtualization of both the configuration and the sensor state.

As shown in Figure 1, sensors can be placed on almost any enterprise network segment where security visibility is required to effectively stop worms and viruses.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 1. Deployment Scenarios for Cisco IPS 4200 Series Sensors



Delivering Performance

Cisco IPS Sensors are designed to meet the rigors of a broad range of applications and network use. In today's contemporary enterprise, applications are leveraging the Internet as never before. Voice over IP, E-Commerce, streaming video and Web 2.0 enable higher productivity and employee collaboration. These networked applications pose different and varying demands on resources such as connection rates, concurrent connections, flow length, transaction size etc. From a performance perspective, there is a spectrum of application types ranging from media-rich environments that feature converged content to highly transactional environments populated by rapid-fire, lightweight connections.

Cisco IPS technology evaluates a diverse suite of metrics in both "media-rich" and "transactional" environments, enabling you to anticipate true IPS performance based on the unique characteristics of your real-world environment.

Media-Rich

Media-rich environments are characterized by content. Content seen on most popular Websites falls on the media-rich end of the spectrum, as do video content and file transfers. If your environment is driven by access to large amounts of data and converged, immersive experiences, your environment is more media-rich.

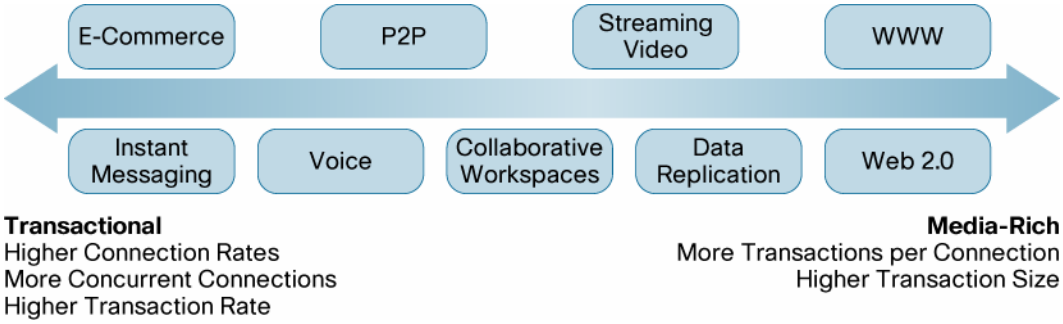
Transactional

Transactional environments are characterized by connections. Many types of e-commerce environments fall on this end of the spectrum, as can instant messaging and voice. If your environment is driven by connection-intensive applications and small transaction sizes, your environment is more transactional.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 2 shows the spectrum between media-rich and transactional environments.

Figure 2. Network Environment Spectrum: Transactional to Media-Rich



Product Specifications

Table 1 lists product specifications for the Cisco IPS 4200 Series.

Table 1. Product Specifications

	Cisco IPS 4270	Cisco IPS 4260	Cisco IPS 4255	Cisco IPS 4240
				
Performance: Media-Rich	4 Gbps	2 Gbps	600 Mbps	300 Mbps
Performance: Transactional	2 Gbps	1 Gbps	500 Mbps	250 Mbps
Standard Monitoring Interface	Four 10/100/1000BASE-TX or Four 1000BASE-SX	10/100/1000BASE-TX	Four 10/100/1000BASE-TX	Four 10/100/1000BASE-TX
Standard Command and Control Interface	10/100/1000BASE-TX	10/100/1000BASE-TX	10/100BASE-TX	10/100BASE-TX
Optional Monitoring Interfaces	• Four 10/100/1000BASE-TX • Two 1000BASE-SX (fiber) (up to 16 total monitoring interfaces)	• Four 10/100/1000BASE-TX (up to 9 monitoring ints) • Two 1000BASE-SX (up to 4 fiber monitoring interfaces)	None	None
Redundant Power Supply	Yes	Optional	No	No
Automated Hardware Fail Open	Yes*	Yes*	Yes**	Yes**
Form Factor	Four rack unit	Two rack unit	One rack unit	One rack unit
Height	6.94 in. (17.6 cm)	3.45 in. (87.6 mm)	1.72 in. (4.37 cm)	1.72 in. (4.37 cm)
Width	19 in. (48.3 cm)	17.14 in. (435.3 mm)	17.25 in. (43.82 cm)	17.25 in. (43.82 cm)
Depth	26.5 in. (67.3 cm)	20 in. (508 mm)	14.5 in. (36.83 cm)	14.5 in. (36.83 cm)
Weight	80 lb (36.3 kg)	40 lb (18.14 kg) (when fully loaded)	20 lb (9.07 kg)	20 lb (9.07 kg)
Rack-Mountable	Yes	Yes	Yes	Yes
Auto-Switching	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
Frequency	50–60 Hz, single-phase	47–63 Hz, single-phase	47–63 Hz, single-phase	47–63 Hz, single-phase
Operating Current	12A (100 VAC), 4.9A (200 VAC)	• 8.9A (100 VAC) • 4.5A (200 VAC)	3.0A	3.0A

Ex. 2003-005

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

	Cisco IPS 4270	Cisco IPS 4260	Cisco IPS 4255	Cisco IPS 4240
Operating Temperature	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)	0 to 40°C (32 to 104°F)	0 to 40°C (32 to 104°F)
Nonoperating Temperature	–40 to 70°C (-104 to 158°F)	–40 to 70°C (-104 to 158°F)	–20 to 65°C (-4 to 149°F)	–20 to 65°C (-4 to 149°F)
Operating Relative Humidity	10 to 90% (noncondensing)	10 to 85% (noncondensing)	10 to 85% (noncondensing)	10 to 85% (noncondensing)
Nonoperating Relative Humidity	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)
Heat Dissipation @ Full Power	1893 Btu/hr	648 Btu/hr	614.2 Btu/hr	614.2 Btu/hr

* With bypass interface card
** With third-party products

Ordering Information

Table 2 lists ordering information for Cisco IPS 4200 Series Sensors. To place an order, visit the Cisco Ordering Home Page.

Table 2. Ordering Information

Product Number	Product Description
IPS-4240-K9	Cisco IPS 4240 Sensor (chassis, software, SSH, four 10/100/1000BASE-TX interfaces with RJ-45 connector)
IPS4240-DC-K9	Cisco IPS 4240 NEBS-Compliant Sensor with DC power (chassis, software, SSH, four 10/100/1000BASE-TX interfaces with RJ-45 connector)
IPS-4255-K9	Cisco IPS 4255 Sensor (chassis, software, SSH, four 10/100/1000BASE-TX interfaces with RJ-45 connector)
IPS-4260-K9	Cisco IPS 4260 Sensor (chassis, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector)
IPS-4260-4GE-BP-K9	Cisco IPS 4260 Sensor with an included 4-GE copper NIC with hardware bypass (chassis, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector , and four 10/100/1000BASE-TX interfaces with built-in bypass)
IPS-4260-2SX-K9	Cisco IPS 4260 Sensor with an included NIC card (chassis, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector, and two fiber interfaces)
IPS4270-20-K9	Cisco IPS 4270 Sensor (chassis, redundant power, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector)
IPS4270-20-4GE-K9	Cisco IPS 4270 Sensor (chassis, redundant power, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector, and four 10/100/1000BASE-TX interfaces)
IPS4270-20-4SX-K9	Cisco IPS 4270 Sensor (chassis, redundant power, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector, and four fiber interfaces)
IPS-4GE-BP-INT=	Spare 4-port copper interface card with built-in hardware bypass for the Cisco IPS 4260 and 4270
IPS-2SX-INT=	Spare 2-port fiber interface card for the Cisco IPS 4260 and 4270

CE Marking

EMC-FCC (CFR 47 Part 15) Class A, CISPR 22 Class A, EN 55022 Class A, EN 55024, EN61000-3-2, EN61000-3-3, VCCI Class A, AS/NZS 3548 Class A, CE marking, ICES-003 Class A, FCC Part 15 (CFR7 47) Class A, EN50082-1, EN61000-6-1, Safety-UL 60950, CSA 22.2 No.60950, IEC 60950, EN 60950, AS/NZS 3260, CE marking; EN 60950, IEC 60950

Cisco Services for IPS

Cisco Services for IPS is an integral part of the Cisco Intrusion Prevention solution and enables operators to receive time-critical signature file updates and alerts. As part of the Cisco Technical Support Services portfolio, Cisco Services for IPS offers a comprehensive security service that

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

allows your Cisco IPS solution to stay current on the latest threats so that malicious or damaging traffic is accurately identified, classified, and stopped. Cisco Services for IPS features include:

- Signature file updates and alerts
- Registered access to Cisco.com for online tools and technical assistance
- Access to Cisco Technical Assistance Center (TAC)
- Cisco IPS software updates
- Advance replacement of failed hardware

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

Export Considerations

Cisco IPS 4200 Series sensors are subject to export controls. For guidance, please refer to the export compliance Website at http://www.cisco.com/wwl/export/crypto/.

For specific export questions, contact export@cisco.com.

Additional Information

For more information about Cisco IPS solutions, including modules for Cisco switches and routers, visit http://www.cisco.com/go/ips.

For more information about Cisco Security Manager (IPS management) and Cisco Security MARS, visit http://www.cisco.com/go/csmanager and http://www.cisco.com/go/mars.

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Printed in USA C78-436667-02 11/08

Ex. 2003-007

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.