The Cisco® IPS 4300 Series

Q. What is the Cisco IPS 4300 Series?

A. The Cisco IPS 4300 Series is a family of 1-rack-unit intrusion prevention sensors delivering more than 1 Gbps of context-aware inspection. The IPS 4300 Series comprises two appliances - the IPS 4345 and IPS 4360, which provide 750 Mbps and 1.25 Gbps of real-world inspection, respectively.

Q. What are the benefits of the Cisco IPS 4300 Series?

A. The Cisco IPS 4300 Series provides high-performance, hardware-accelerated, context-aware intrusion prevention in a compact form factor. Its architecture enables it to scale to meet the performance requirements of a wide range of network deployments - from small branch offices to medium-sized enterprises and campus environments.

Q. What are the inspection and prevention capabilities of the Cisco IPS 4300 Series?

A. The Cisco IPS 4300 Series sensors use the same advanced IPS capabilities available on all Cisco IPS sensors. Cisco IPS Sensor Software Version 7.1 or later provides a comprehensive set of advanced inspections and signatures for known vulnerabilities, as well as next-generation features such as global correlation and reputation-based filtering.

Q. How does the Cisco IPS 4300 Series compare with the Cisco IPS 4200 Series?

A. The Cisco IPS 4300 Series represents a dramatic step forward for the Cisco IPS product line. The Cisco IPS 4200 Series is based upon legacy architecture without hardware acceleration. The Cisco IPS 4300 Series is built upon enterprise-class processors with dedicated IPS acceleration hardware, all within a 1-RU chassis. This combination delivers up to four times the performance density of the IPS 4200 Series. However, both series share the same management plane, which makes policy configuration, event management, reporting, and health and performance consistent across the products.

Q. Does the Cisco IPS 4300 Series support fail open?

A. Yes. The Cisco IPS 4300 Series provides software fail open.

Q. What is the latency?

A. Average latency for the 4360 and 4345 is less than 150μ.

Q. I already have a Cisco Adaptive Security Appliance (ASA) with IPS. Why do I need a Cisco IPS 4300 Series?

A. Cisco ASA with IPS offers a combination of features, including firewall, VPN termination, and intrusion prevention. Both the ASA IPS and the Cisco IPS 4300 Series share a common IPS code base. However, the Cisco IPS 4300 provides greater performance density and deployment flexibility (e.g. SPAN deployments, fail open, etc.) than the ASA IPS product line.

Q. What software version is available on the Cisco IPS 4300 series?

A. The Cisco IPS 4300 Series currently ships with the Cisco IPS Sensor Software Release 7.1(3) E4 image, which is also available for download.

Q. What can I use to manage the Cisco IPS 4300 Series?

A. Several options are available to manage the Cisco IPS 4300 Series sensors:

- The sensor's command-line interface.
- Cisco IPS Device Manager, a graphical user interface on the sensor.
- Cisco IPS Manager Express (IME) 7.2.1 which provides reporting, health management, event management, and configuration for up to 10 IPS devices.
- Cisco Security Manager, which helps enterprises manage and scale security operations to hundreds of devices efficiently and accurately. Its end-to-end tools provide consistent policy enforcement, quick troubleshooting of security events, and summarized reports from across the security deployment.

Q. What are the benefits of migrating from Cisco IPS Sensor Software 6.x to 7.1?

A. Cisco IPS Sensor Software Release 7.0 offers a global correlation feature that delivers near-real-time protection from zero-day malware. At regular intervals, Cisco IPS receives threat updates from Cisco Security Intelligence Operations. The updates contain detailed information about known threats on the Internet, including serial attackers, botnet harvesters, malware outbreaks, and dark nets. The sensor uses this information to filter out the worst attackers before they have a chance to attack critical assets. It then incorporates the global threat data into its system to detect and prevent malicious activity even earlier.

The Cisco IPS Sensor Software 7.1.(3) code base also provides:

- Significantly improved performance for real-world deployment scenarios
- Expanded authentication options
- Support for the following recently released platforms:
  - IPS 4345 and 4360
  - ASA 5585-X with IPS SSP-10, IPS SSP-20, IPS SSP-40, or IPS SSP-60
  - ASA 5500-X Series with IPS SSP

Q. How does a user communicate with the Cisco IPS 4300 Series?

A. Cisco IPS 4300 Series sensors have a management interface that needs to be plugged into the appropriate part of the network. Network settings, including IP address, default gateway, and access list, need to be configured on the Cisco IPS 4300 Series sensor to allow communication.

Cisco IPS 4300 Series sensors also provides users with a command-line interface to configure the sensor with the basic network settings required for IP communication.

Q. What are the orderable PIDs (SKUs) for the IPS 4300 Series?

A. The following PIDs will be available.

Table 1.   Ordering Information

Product Name	Part Number
Cisco IPS 4345 Sensor	IPS-4345-K9
Cisco IPS 4360 Sensor	IPS-4360-K9
Cisco IPS 4345 Sensor (DC Power Version)	IPS-4345-DC-K9
Cisco IPS 4360 Sensor (DC Power Version)	IPS-4360-DC-K9

·din·din· CISCO ™

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

C67-703957-01   10/12