The Cisco IPS 4300 Series

As users and data leave the corporate boundary and the network access layer becomes more porous, signature-only detection products lead to a one-dimensional response. Only Cisco uses broad network context through every stage of analysis, including victim OS, evasion techniques, attack state across signatures and an industry first: attacker identity, and behavior.

The Cisco® Intrusion Prevention Sensor (IPS) 4300 Series scales to serve a wide range of deployment scenarios, from small offices and branch locations to enterprise data center architectures. With throughput speeds ranging from 1 Gbps to 10 Gbps, each IPS 4300 Series model provides a consistent level of protection. The Cisco IPS 4300 Series delivers hardware-accelerated inspection performance, high port density, and energy efficiency in a 1-RU form factor (Figure 1). With effective, out-of-the-box protection and automated threat management, your critical assets are protected in minutes.

Figure 1.   Cisco IPS 4345 and 4360 Sensors

Advanced Threat Protection

Cisco IPS solutions deliver:

- A wide and deep body of protection, with more than 5500 signatures
- Patented anti-evasion technology to defend and monitor against worms, viruses, Trojans, reconnaissance attacks, spyware, botnets, undesired applications, and malware
- Protocol and behavior analysis for final threat determination
- Cisco Global Correlation to help identify the source of denial of service (DoS), distributed denial of service (DDoS), SYN flood, and encrypted attacks so you can block them
- Specific protections for Unified Communications, WLAN, routing, and switching to help guard the Cisco infrastructure

Ensure Compliance

Cisco IPS solutions help customers move toward compliance with the following privacy and data protection regulations:

- Payment Card Industry (PCI) standard
- European Union privacy protection rules
- U.S. Sarbanes-Oxley Act (SOX)
- U.S. Gramm-Leach-Bliley Act (GLBA)
- NERC Critical Infrastructure Protection (CIP)
- Health Insurance Portability and Accountability Act (HIPAA)

Seamless Network Integration

Cisco IPS technology delivers the most advanced network awareness in the industry. Whether defending the data center, core, or edge, Cisco IPS solutions provide threat protection up to Layer 7. Network Based Flow Affinity feature offers high availability with better integration into the network via standards-based LACP support. To reduce capital expenditures, Cisco IPS solutions are built upon common software architecture and custom hardware platforms that enable deployment anywhere in the Cisco network, including routing, switching, and firewall platforms. A consistent policy and operations framework helps bring the system together to meet compliance and manage risk at a lower operational cost.

Unparalleled Global Correlation

As advanced persistent threats, botnets, and other blended threats evolve, signature-based content inspection alone becomes insufficient. Using 10 years of reputation technology heritage, Cisco IPS is the only IPS to mitigate identified attacks based on source reputation, not just signature firings. With Cisco IPS Global Correlation backed by Cisco Security Intelligence Operations (SIO), Cisco IPS gains visibility into hundreds of additional security parameters, millions of rules, and 100 TB of threat telemetry per day from market-leading email, web, firewall, and IPS devices.

Network-Ready Capabilities

To meet the needs of the most demanding networks, Cisco IPS technology directly integrates into the firewall to deliver multigigabit performance, low latency, and high-availability features. With hardware-accelerated deep packet analysis, the Cisco IPS 4300 Series delivers performance in the 750 Mbps to 1.25 Gbps range to support a variety of applications and deployments. For details on the unique methodology Cisco uses to calculate IPS performance, refer to the Performance of Cisco IPS 4500 and 4300 Series Sensors. Flexible and highly available deployment options include active-active and active-standby configurations; fail-open and fail-closed modes; IDS and IPS modes; and redundant power supplies. The IPS 4300 Series also offers the ability to inspect encapsulated traffic, including GRE, MPLS, 802.1q, IPv4 in IPv4, IPv4 in IPv6, and Q-in-Q double VLAN.

Proven Threat Prevention

With more than $100M invested in security research, 500 threat analysts, and terabytes of threat data fed into Cisco SIO every day, Cisco brings confidence to customer networks. That is why Cisco IPS technology is the most widely deployed commercial IPS technology in the world - and why independent testing agencies recommend Cisco IPS as well.

Complete Control and Real-Time Visibility

Cisco provides management solutions for smaller deployments, as well as enterprise-class coverage. Cisco IPS Manager Express is an all-in-one IPS management and reporting application for up to 10 devices. Cisco Security Manager is an enterprise-class security management application with thousands of real-world deployments.

Both solutions support the Cisco IPS 4300 Series as well as other Cisco sensor appliances, Cisco integrated services routers (ISRs), and Cisco Intrusion Detection Services Modules (IDSMs).

Cisco IPS Manager Express offers:

- Provisioning, monitoring, and troubleshooting
- Drag-and-drop dashboard gadgets for easy customization; personalized views remember user settings to minimize setup time
- Flexible reporting tool that allows custom and compliance reports to be generated in seconds

Cisco Security Manager 4.x offers:

- Flexible processes to incrementally provision new and updated signatures, create IPS policies for those signatures, and then share the policies across devices
- Enhanced reporting and event management support for Cisco's latest IPS features, including Cisco IPS Global Correlation
- Roles-based access control (RBAC) and workflow for error-free deployments and process compliance

Tables 1 and 2 list specifications for Cisco IPS 4300 Series sensors.

Table 1.   Cisco IPS 4300 Sensor Specifications

Feature	Cisco IPS 4345	Cisco IPS 4360
Average Inspection Throughput	750 Mbps	1.25 Gbps
Maximum Inspection Throughput	1.8 Gbps	2.4 Gbps
Maximum Connections	750,000	1,700,000
Connections Per Second	30,000	45,000
Average Latency	<150 µ	<150 µ
Threat Protection	25,000+ threats	25,000+ threats
Protocol Anomaly Detection	Yes	Yes
Evasion Identification and Mitigation	Yes	Yes
Application Anomaly Detection	Yes	Yes
Passive OS Fingerprinting	Yes	Yes
Global Correlation	Yes	Yes
Pre-Inspection Reputation Black Lists	Yes	Yes
Reputation-Driven Mitigation Selection	Yes	Yes
Compound Signature Analysis (Disparate Alerts Combine to ID Higher Order Threat)	Yes	Yes
Customizable Signature Ratings: Severity, Fidelity	Yes	Yes
Custom Signature Support	Yes	Yes

Table 2.   Cisco IPS Specifications

Feature	Cisco IPS 4345	Cisco IPS 4360
Management and Monitoring Interface	1 Ethernet 10/100/1000 port	1 Ethernet 10/100/1000 port
CPU	Multicore	Multicore
Memory	8 GB	16 GB
Dual Power Supplies	None	Yes
Data Ports	8 x 1GE	8 x 1GE
Minimum Flash	8 GB	8 GB
Temperature	24.5 to 113ºF (-4 to 45ºC)	24.5 to 113ºF (-4 to 45ºC)
Relative Humidity (Operating)	10 to 90% noncondensing	10 to 90% noncondensing
Altitude (Operating)	0 to 9,921 ft (3024 m)	0 to 9,921 ft (3024 m)
Maximum Peak	30W maximum	90W maximum
Mean Time Between Failure (MTBF)	874,070 hours (100 years)	299,588 hours (31 years)
Dimensions (HxWxD)	1.67 x 16.9 x 15.5 in. (4.24 x 42.9 x 39.5 cm)	1.67 x 16.7 x 19.1 in. (4.24 x 42.9 x 48.4 cm)
Weight	14.92 lb (6.77 kg)	16.82 lb (7.63 kg) with single power supply 18.86 lb (8.61 kg) with dual power supply
Safety	UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001	UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001
Electromagnetic Compatibility (EMC)	CE marking, FCC Part 15 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3	CE marking, FCC Part 15 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3

Ordering Information

To place an order, visit the [Cisco Ordering homepage](). See Table 3 for ordering information.

Table 3.   Ordering Information

Product Name	Part Number
Cisco IPS 4300 Series	
Cisco IPS 4345 Sensor	IPS-4345-K9
Cisco IPS 4345 Sensor (DC power version)	IPS-4345-DC-K9
Cisco IPS 4360 Sensor	IPS-4360-K9
IPS-4360-AC-PWR=	IPS 4360 AC power supply (spare)
Cisco IPS 4360 Sensor (DC power version)	IPS-4360-DC-K9
IPS-4360-DC-PWR=	IPS 4360 DC power supply (spare)
IPS-4360-PWR-BLK=	IPS 4360 power supply blank
IPS 4360 interface card slot blank	IPS-4360-DC-PWR=
IPS 4345 or 4360 hard drive blank	IPS-4300-HD-BLK-M=
IPS-4300-RAILS=	IPS 4345 and 4360 tool-less sliding rail kit

Service and Support

Cisco offers a wide range of service programs to accelerate customer success. These innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services for security, visit http://www.cisco.com/go/services/security.

Cisco Services for IPS

Cisco Services for IPS is an integral part of the Cisco IPS 4300 Series solution and enables operators to receive time-critical signature file updates and alerts. Part of the Cisco Technical Support Services portfolio, Cisco Services for IPS allows your Cisco IPS 4300 Series sensors 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
- Global Threat Correlation reputation feeds
- Registered access to Cisco.com for online tools and technical assistance
- Access to the Cisco Technical Assistance Center
- Cisco IPS software updates
- Advance replacement of failed hardware

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

Export Considerations

Cisco IPS 4300 Series products are subject to export controls. For guidance, 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, please visit the following links:

- Cisco Intrusion Prevention Systems: http://www.cisco.com/go/ips
- Cisco IDS and IPS sensors and software versions that have reached end-of-sale status: http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_eol_notices_list.html
- Cisco Security Manager: http://www.cisco.com/go/csmanager
- Cisco IPS Manager Express: http://www.cisco.com/go/ime

Printed in USA

C78-703956-04 10/13