Cisco IPS 4200 Series Sensors

In today's busy network environment, business continuity relies on effective network intrusion prevention to stop malicious attacks, and application abuse before they affect your data and resources.

Cisco® IPS 4200 Series Sensors are core components of Cisco's intrusion prevention solution. Cisco IPS 4200 Series Sensors accurately detect, classify, and stop malicious traffic while delivering safe assured network continuity and protection.

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, through the entire attack lifecycle and at all layers of the application stack.

- Built on advanced Cisco security and network intelligence, modular inspection capabilities can detect and prevent threats to the entire network stack, from Address Resolution Protocol (ARP) to complex enterprise level applications. Cisco IPS technology protects against advanced application evasions and can normalize even the most fragmented of network traffic.

- Cisco IPS provides adaptive vulnerability and anomaly detection. Cisco has focused its signatures on the potential abuse of vulnerabilities, so your ability to detect threats remains intact, even as exploits change. For emerging "zero-day" threats, a Cisco IPS sensor learns about your network, detects both protocol and behavioral anomalies, and can mitigates attacks without a signature update.

- Cisco IPS led the IPS industry into the use of reputation feeds through the use of Global Correlation. Global Correlation harnesses the power of Cisco Security Intelligence Operations, the world's largest threat monitoring network, to achieve unprecedented threat management efficacy. Global threat information is turned into actionable intelligence, such as reputation scores, can also be used for black listing and driving dynamic threat responses. Using Global Correlation, Cisco IPS can stop twice the amount of malicious activity that traditional signature-only IPS technologies can, and with fewer false positives. Cisco Global Correlation updates every five minutes and thus the Cisco IPS can also adjust to changing threat conditions 100 times faster than signature updates alone.

Precision Response

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

- Cisco IPS sensors provide you with the most knowledge of potential threat impact by calculating a real-time measurement of risk for every event and a post attack follow up analysis of the remaining threat. An adaptive multidimensional algorithm combines attack and attacker details with live global and network knowledge to produce a calibrated risk measurement which drives a unique response according to attacker and target visibility.

- Cisco IPS sensors have 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 sensors act with the deepest network and device level visibility, recording 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 provides 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 zero-day attacks

- Dynamic risk-based threat rating adapts policy to attacks in real time

- Collaborative

- On-box, network wide, global 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 define your inspection policy, with integrated graphical management and event viewing tools.

- Reduce the cost of change and configuration management activities, using the rich Cisco Security Manager graphical interface to update policies on thousands of devices in a few simple steps.

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 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.

Figure 1.   Deployment Scenarios for Cisco IPS 4200 Series Sensors
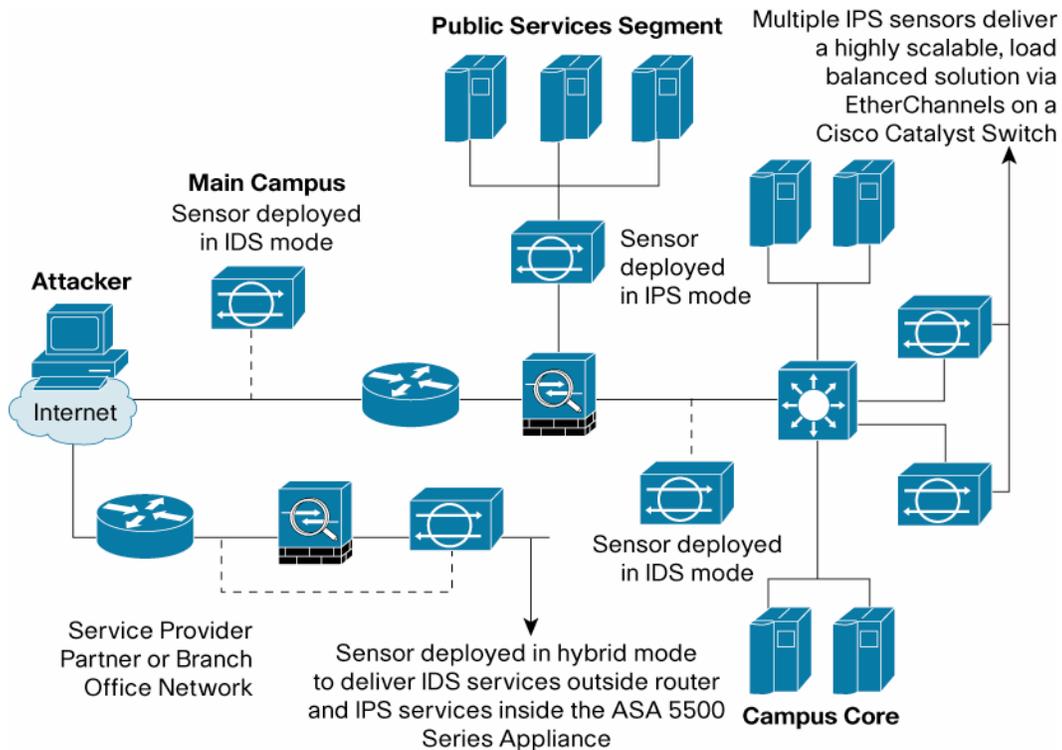
Delivering Performance

Cisco IPS 4200 Series Sensors are designed to meet the rigors of a broad range of applications and network use. In recognition of the rapid growth of Internet based applications, Cisco has created two metrics to measure IPS performance. These networked applications pose different and varying demands on resources such as connection rates, concurrent connections, flow length, transaction size, etc. Additionally these web based applications can act as a vector for the introduction of threats or the path for critical data loss.

NOTE: *Every deployment scenario is different and IPS performance will vary based on live traffic profiles. Users should test with as much live traffic as possible to assess your network's individual characteristics.*

To reflect these internet focused deployment scenarios, Cisco has established a "Media Rich" and "Transactional" measurement suite to measure our system's anticipated performance. These tests are based on pure HTTP traffic.

Media-Rich

Media-rich environments are characterized by content delivered by HTTP. 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 a higher number of connections, in this case HTTP 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.

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

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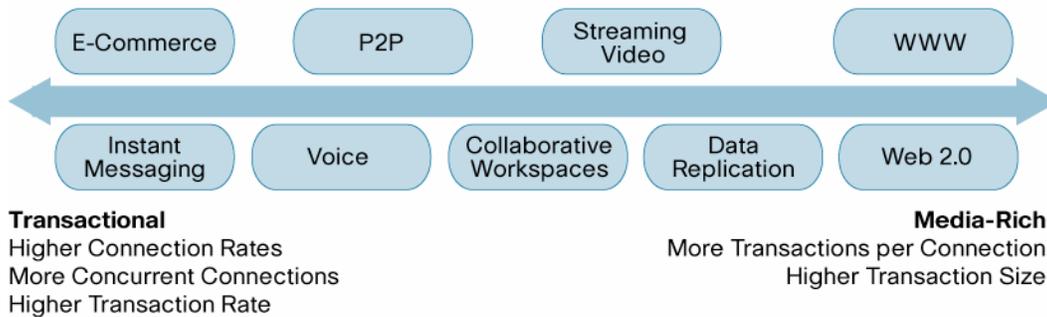
Product Specifications

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

Table 1. Product Specifications

	Cisco IPS 4240	Cisco IPS 4255	Cisco IPS 4260	Cisco IPS 4270
Performance: Media-rich (see NOTE above)	300 Mbps	600 Mbps	2 Gbps	4 Gbps
Performance: Transactional (see NOTE above)	250 Mbps	500 Mbps	1 Gbps	2 Gbps
Standard monitoring interface	Four 10/100/1000BASE-TX	Four 10/100/1000BASE-TX	10/100/1000BASE-TX	Four 10/100/1000BASE-TX or four 1000BASE-SX
Standard command and control interface	10/100BASE-TX	10/100BASE-TX	10/100/1000BASE-TX	10/100/1000BASE-TX
Optional monitoring interfaces	None	None	• Four 10/100/1000BASE-TX (up to 9 monitoring interfaces) • Two 1000BASE-SX (up to 4 fiber monitoring interfaces) • One 2-Port 10Gigabit Ethernet Interface Card, SR (optional)	• Four 10/100/1000BASE-TX • Two 1000BASE-SX (fiber) (up to 16 total monitoring interfaces) • One 2-Port 10Gigabit Ethernet Interface Card, SR (optional)
Redundant power supply	No	No	Optional	Yes
Automated hardware fail- open	Yes**	Yes**	Yes*	Yes*
Form factor	One rack unit	One rack unit	Two rack units	Four rack units
Height	1.72 in. (4.37 cm)	1.72 in. (4.37 cm)	3.45 in. (87.6 mm)	6.94 in. (17.6 cm)
Width	17.25 in. (43.82 cm)	17.25 in. (43.82 cm)	17.14 in. (435.3 mm)	19 in. (48.3 cm)
Depth	14.5 in. (36.83 cm)	14.5 in. (36.83 cm)	20 in. (508 mm)	26.5 in. (67.3 cm)
Weight	20 lb (9.07 kg)	20 lb (9.07 kg)	40 lb (18.14 kg) (when fully loaded)	80 lb (36.3 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	47 to 63 Hz, single-phase	47 to 63 Hz, single-phase	47 to 63 Hz, single-phase	50 to 60 Hz, single-phase

	Cisco IPS 4240	Cisco IPS 4255	Cisco IPS 4260	Cisco IPS 4270
Operating current	3.0A	3.0A	8.9A (100 VAC), 4.5A (200 VAC)	12.0A (100 VAC), 4.9A (200 VAC)
Operating temperature	0 to 40℃ (32 to 104℉)	0 to 40℃ (32 to 104℉)	10 to 35℃ (50 to 95℉)	10 to 35℃ (50 to 95℉)
Nonoperating temperature	−20 to 65℃ (−4 to 149℉)	−20 to 65℃ (−4 to 149℉)	−40 to 70℃ (−104 to 158℉)	−40 to 70℃ (−104 to 158℉)
Operating relative humidity	10 to 85% (noncondensing)	10 to 85% (noncondensing)	10 to 85% (noncondensing)	10 to 90% (noncondensing)
Nonoperating relative humidity	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)
Heat dissipation @ full power	614.2 Btu/hr	614.2 Btu/hr	648 Btu/hr	1893 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
IPS-2X10GE-SR-INT	2-Port 10Gigabit Ethernet Interface Card, SR,

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 Cisco IPS solutions, enabling 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 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/ps6498/index.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.