Cisco Intrusion Prevention: Cisco IPS 4500 Series

Protect your data center and network aggregation points with context-aware intrusion prevention.

Attackers target data used by a variety of custom and commercial applications. Signature-only detection products can provide only a one-dimensional - and sometimes incorrect - response. Only Cisco uses broad network context through every stage of analysis, including passive OS fingerprinting, evasion techniques, and attack state across signatures, as well as - an industry first - attacker identity, location, and behavior. These state of the art techniques protect infrastructure and applications from advanced persistent threats (APT's) and other sophisticated attacks for superior security protection.

The Cisco IPS 4500 Series delivers hardware-accelerated inspection, real-world performance, high port density, and energy efficiency in an expansion-ready chassis for future growth and investment protection. Its small form factor and low power consumption were specifically engineered for space-challenged data center environments. With highly effective, out-of-the-box protection and automated threat management, your critical data center assets are protected in minutes.

Figure 1. Cisco IPS 4500 Series

Context-Driven Protection for Critical Internal Applications

The modern enterprise runs a wide array of mission-critical commercial and highly customized applications. The data within those applications is a high-value target for attackers, yet access to that data is what drives the productivity and success of the enterprise. The challenge is providing full and rich access to authorized users while protecting the integrity of the data center infrastructure and applications. Context-driven intrusion prevention is essential for full protection. Consider these scenarios:

- **SQL injection or dynamic database query tool(s)?** If your IPS can only provides one action when a SQL injection signature fires, it lacks context awareness. Cisco IPS technology can determine the proper level of action even after a signature has fired.
- **Target-scanning malware or working IT member?** A large number of pings are emanating from a traveling salesperson's laptop. Is it a bot seeking targets, or is it an IT team member trying to help troubleshoot access to the customer relationship management (CRM) system?
- **An employee experimenting with a script or targeted attack?** Should there be an all-hands investigation or a simple logging of events? A context-driven IPS knows the difference.

- **Random jitter or obfuscated attacks?** Some types of traffic scrambling and evasive activity do not typically occur on enterprise networks. Only Cisco provides direct reports on that activity and offers specific tuning to address attacks.

Compliance Met and Risk Averted

Commercial groups and government organizations have legal obligations to protect data from alteration, theft, and illicit access. Cisco's context-driven intrusion prevention enables secure applications and continued secure operations. Common regulations include:

- Retail industry and more: Payment Card Industry Data Security Standard (PCI DSS)
- U.S. publicly traded companies: U.S. Sarbanes-Oxley Act (SOX)
- EU-based companies: European Union Privacy Protection Rules
- Utilities: NERC Critical Infrastructure Protection (CIP)
- U.S. commercial entities: Health Insurance Portability and Accountability Act (HIPAA)

Seamless Network Integration

A critical component of the Cisco SecureX framework, Cisco IPS provides the most advanced network awareness in the industry. Whether defending the data center, network core, or Internet edge, Cisco IPS technology provides application- and infrastructure-centric protection. To reduce capital expenditures, Cisco IPS solutions are built upon a common software architecture that enable deployment anywhere in the Cisco network, including routing, switching, and firewall platforms. A consistent policy and operations framework help bring the system together to meet compliance requirements and manage risk at a lower operational cost.

Unparalleled Global Correlation

As advanced persistent threats (APTs), botnets, and other blended threats evolve, signature-based content inspection alone becomes insufficient to identify and mitigate threat activity. With 10 years of reputation technology experience, Cisco IPS with Global Correlation is the only IPS to mitigate identified attacks based on source reputation - not just a simple signature firing. Cisco IPS Global Correlation backed by Cisco Security Intelligence Operations (SIO) gathers information from hundreds of security parameters, millions of detection rules, and 100 TB of threat telemetry per day from market-leading email, web, firewall, and IPS devices - giving the Cisco IPS unprecedented visibility into real-time threats.

Network-Ready Capabilities

The Cisco IPS 4500 Series provides low latency and high-availability features to meet the needs of the most demanding networks. With hardware-accelerated deep packet analysis, the Cisco IPS 4500 Series delivers multi-gigabyte performance with dedicated space available for future IO and performance expansion. 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 or fail-closed modes; IDS and IPS operational modes; and redundant power supplies. Network Based Flow Affinity feature offers high availability with better integration into the network via standards-based LACP support. The system can also inspect encapsulated traffic, including generic routing encapsulation (GRE), Multiprotocol Label Switching (MPLS), 802.1q, IPv4 in IPv4, IPv4 in IPv6, and Q-in-Q double VLAN.

Proven Threat Prevention

With more than US $100 million invested in security research, 500 threat analysts, and terabytes of threat data fed into Cisco SIO every day, Cisco IPS backed by Cisco SIO brings confidence to customer networks by contextually analyzing a signature firing to determine the correct response action. Cisco is the only commercial IPS vendor to openly disclose its signature database to expose the best-in-class asset protection. This is why the award-winning Cisco IPS is the most widely deployed commercial IPS technology in the world.

Complete Control and Real-Time Visibility

Cisco provides IPS management solutions for deployments of all sizes, from a small business to 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. A fully functional on-box CLI is available as well.

Cisco IPS Manager Express and Cisco Security Manager support the Cisco IPS 4500 Series as well as other Cisco IPS Sensors.

Cisco Security Manager 4.x offers:

- Flexible processes to provision new and updated signatures incrementally, 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 Global Correlation
- Role-based access control and workflow to ensure error-free deployments and process compliance

Cisco IPS Manager Express offers:

- Provisioning, monitoring, and troubleshooting
- Drag-and-drop dashboard gadgets, which provide easy customization
- Personalized views that remember user settings to minimize setup time
- A flexible reporting tool for generating custom and compliance reports in seconds
- Predefined location-specific tuning templates

Table 1 lists the specifications of the Cisco IPS 4500 Series.

Table 1. Cisco IPS 4500 Series IPS Solution Specifications

Feature	Cisco IPS 4510	Cisco IPS 4520*	Cisco IPS 4520-XL
Average Inspection Throughput (Mbps)	3 Gbps	5 Gbps	10 Gbps
Maximum inspection throughput (Mbps)	5 Gbps	10 Gbps	20 Gbps
Maximum Connections	3,800,000	8,400,000	16,800,000
Connections per Second	72,000	100,000	200,000
Average Latency	<150 µ	<150 µ	<150 µ
Threat Protection	25,000+ threats	25,000+ threats	25,000+ threats
Protocol Anomaly Detection	Yes	Yes	Yes
Evasion Identification and Mitigation	Yes	Yes	Yes
Application Anomaly Detection	Yes	Yes	Yes
Passive OS Fingerprinting	Yes	Yes	Yes
Global Correlation	Yes	Yes	Yes

Feature	Cisco IPS 4510	Cisco IPS 4520*	Cisco IPS 4520-XL
Pre-Inspection Reputation Black Lists	Yes	Yes	Yes
Reputation-Driven Mitigation Selection	Yes	Yes	Yes
Compound Signature Analysis (disparate alerts combine to ID higher order threat)	Yes	Yes	Yes
Customizable Signature Ratings: Severity, Fidelity	Yes	Yes	Yes
Custom Signature Support	Yes	Yes	Yes

* Single module 4520

Table 2 provides Cisco IPS specifications.

Table 2. Cisco IPS Specifications

Feature	Cisco IPS 4510	Cisco IPS 4520	Cisco IPS 4520-XL
Management and Monitoring Interface	Ethernet 10/100/1000 port	Ethernet 10/100/1000 port	Ethernet 10/100/1000 port
CPU	Dual multi-core	Dual multi-core	Dual multi-core
Memory	24 GB	48 GB	48 GB
Data Ports	6-port 10/100/1000, 4-port 1 or 10 Gigabit Ethernet SFP+	6-port 10/100/1000, 4-port 1 or 10 Gigabit Ethernet SFP+	6-port 10/100/1000, 4-port 1 or 10 Gigabit Ethernet SFP+
Minimum Flash	2 GB	2 GB	2 GB
Temperature	Operating 32 to 104℉ (0 to 40℃) Nonoperating -40℉ to 158℉ (-40℃ to 70℃)	Operating 32 to 104℉ (0 to 40℃) Nonoperating -40℉ to 158℉ (-40℃ to 70℃)	Operating 32 to 104℉ (0 to 40℃) Nonoperating -40℉ to 158℉ (-40℃ to 70℃)
Relative Humidity (Operating)	Operating 10% to 90% Nonoperating 5% to 95%	Operating 10% to 90% Nonoperating 5% to 95%	Operating 10% to 90% Nonoperating 5% to 95%
Altitude (Operating)	Operating 0 to 10,000 ft (3,050 m) Nonoperating 0 to 30,000 ft (9,144 m)	Operating 0 to 10,000 ft (3,050 m) Nonoperating 0 to 30,000 ft (9,144 m)	Operating 0 to 10,000 ft (3,050 m) Nonoperating 0 to 30,000 ft (9,144 m)
Dimensions (HxWxD)	3.47 x 19 x 26.5 in. (8.8 x 48.3 x 67.3 cm)	3.47 x 19 x 26.5 in. (8.8 x 48.3 x 67.3 cm)	3.47 x 19 x 26.5 in. (8.8 x 48.3 x 67.3 cm)
Weight	50 lb (22.7 kg) with 1 SSP and 1 power supply module; 62 lb (28.20 kg) with SSP, IPS SSP, and 2 power supply modules	50 lb (22.7 kg) with 1 SSP and 1 power supply module; 62 lb (28.20 kg) with SSP, IPS SSP, and 2 power supply modules	75 lb (34.02 kg) with 2 SSP's, and 2 power supply modules
Safety	UL 60950-1, CAN/CSA-C22.2 No. 60950-1 EN 60950-1, IEC 60950-1, AS/NZS 60950-1	UL 60950-1, CAN/CSA-C22.2 No. 60950-1 EN 60950-1, IEC 60950-1, AS/NZS 60950-1	UL 60950-1, CAN/CSA-C22.2 No. 60950-1 EN 60950-1, IEC 60950-1, AS/NZS 60950-1
Electromagnetic Compatibility (EMC)	FCC[1] Part 15 (CFR[2] 47) Class A EN55022 Class A with CISPR22 Class A AS/NZS[3] CISPR22 Class A VCCI[4] Class A CISPR 24 EN50082-1 EN55024 EN61000-3-2 EN61000-3-3 EN61000-6-1 KN22 Class A KN24 ICES003 Class A	FCC[1] Part 15 (CFR[2] 47) Class A EN55022 Class A with CISPR22 Class A AS/NZS[3] CISPR22 Class A VCCI[4] Class A CISPR 24 EN50082-1 EN55024 EN61000-3-2 EN61000-3-3 EN61000-6-1 KN22 Class A KN24 ICES003 Class A	FCC[1] Part 15 (CFR[2] 47) Class A EN55022 Class A with CISPR22 Class A AS/NZS[3] CISPR22 Class A VCCI[4] Class A CISPR 24 EN50082-1 EN55024 EN61000-3-2 EN61000-3-3 EN61000-6-1 KN22 Class A KN24 ICES003 Class A
	[1] FCC = Federal Communications Commission [2] CFR = Code of Federal Regulations [3] AS/NZS = Standards Australia/Standards New Zealand [4] VCCI = Voluntary Control Council for Information Technology Equipment (Japan)	[1] FCC = Federal Communications Commission [2] CFR = Code of Federal Regulations [3] AS/NZS = Standards Australia/Standards New Zealand [4] VCCI = Voluntary Control Council for Information Technology Equipment (Japan)	[1] FCC = Federal Communications Commission [2] CFR = Code of Federal Regulations [3] AS/NZS = Standards Australia/Standards New Zealand [4] VCCI = Voluntary Control Council for Information Technology Equipment (Japan)

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 4500 Series	
Cisco IPS 4510	IPS-4510-K9
Cisco IPS 4520	IPS-4520-K9
Cisco IPS 4520-XL[*]	IPS-4520-XL-K9
Spare Cards	
Cisco IPS 4510 Spare Card	IPS-4510-SSP-K9=
Cisco IPS 4520 Spare Card	IPS-4520-SSP-K9=

[*] Dual card 4520 model.

Service and Support

Cisco offers a wide range of service programs to accelerate customer success. These innovative services 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 4500 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 4500 Series 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 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 4500 Series appliances 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 about Cisco IPS solutions, visit http://www.cisco.com/go/ips.

For information about Cisco IDS and IPS sensors and software versions that have reached end-of-sale status, visit http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_eol_notices_list.html.

For more information about Cisco Security Manager and Cisco IPS Manager Express, visit:

- http://www.cisco.com/go/csmanager
- http://www.cisco.com/go/ime

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 C78-712063-05 10/13