Overview

Models

HP S660N 750 Mbps 5 Gig-T/5 1Gb Fiber Segments IPS	JC019A
HP S1400N 1.5 Gbps 5 Gig-T/5 1Gb Fiber Segments IPS	JC020A
HP S2500N 3Gbps 5 Gig-T/1 10GbE/5 1GbE Fiber Segments IPS	JC021A
HP S5100N 5Gbps 5 GigT/1 10GbE/5 1GbE Fiber Segments IPS	JC022A
HP S6100N 8Gbps IPS	JC577A

Key features

- Industry-proven proactive network security
- Up-to-date and broad IPS protection
- Industry-leading security research team—DVLabs
- Reduced overall security costs and complexity
- Security compliance best practices

Product overview

The HP S Intrusion Prevention System (IPS) N Series achieves a new level of inline, real-time protection, providing proactive network security for today's and tomorrow's real-world network traffic and data centers. The IPS platform's next-generation architecture adds significant capacity for deep packet traffic inspection, and its modular software design enables the addition of valuable network protection services to its proven intrusion prevention solution. This new industry-leading IPS platform redefines intrusion prevention as a foundation for comprehensive network security.

Features and benefits

Technical features

- Intrusion prevention system (IPS): The IPS N series achieves a new level of inline, real-time protection, providing proactive network security for today's and tomorrow's real-world network traffic and data centers. Its architecture adds significant capacity for deep packet traffic inspection, and its modular software design enables the convergence of additional security services.
- Proven inline threat protection: Since 2001, we have been laser-focused on creating IPS solutions that provide proactive inline network protection while delivering high network performance and availability. No network security solution remains inline if it compromises network performance or uptime. According to a 2008 study by Infonetics Research, more enterprise IPS users have chosen our inline IPS solutions than any other.
- New extensible security framework provides a foundation for growth: The IPS platform includes an extensible security framework that has a modular software design built to support faster development and deployment of new IPS filter packages, security services, and partner security solution integrations.
- New IPS security services: The IPS N series enables the convergence of new security services such as customer-defined IP DNS reputation entries, our Reputation Digital Vaccine Service, our Web Application Digital Vaccine (DV) Service, location-based policies (perimeter, core, etc.), and customer-developed protection filters.
- Modular design for solutions integration: The modular design of the IPS platform enables integration with partner security solutions such as vulnerability assessment and vulnerability management (VA/VM) products, forensics solutions, security information management (SIM) systems, and network-based anomaly detection (NBAD) products.
- Support for a broad set of traffic types: The IPS platform supports a wide variety of traffic types and protocols. It provides uncompromising IPv6 and IPv4 simultaneous payload inspection and support for related tunneling variants (4in6, 6in4, and 6in6). It also supports inspection of IPv6 and IPv4 traffic with VLAN and MPLS tags, mobile IPv4 traffic, GRE and GTP (GPRS tunneling), and jumbo frames, which gives IT administrators the flexibility to deploy IPS protection wherever it is needed.

Overview

- New threat suppression engine (TSE): The IPS platform employs a new TSE to keep pace with the changing threats and evolving demands of today's enterprise networks and data centers. The TSE architecture utilizes custom ASICs and high-performance network processors to perform total packet flow inspection at Layers 2 through 7, performing thousands of checks on each packet flow simultaneously and delivering a significant deep packet inspection capacity increase for new and future security services.
- Proven reliability and redundancy: The IPS platform is designed to deliver unparalleled high availability. This helps ensure that network traffic flows at wire speed in the event of a network error, an internal device error, or even a complete power loss. There are two complementary high-availability modes of operation—Intrinsic High Availability and Stateful Network Redundancy—that deliver outstanding uptime and availability for both the IPS platform and the SMS devices.
- Built-in high-availability features: The IPS platform has multiple features for Intrinsic High Availability, including dual hot-swappable power supplies; watchdog timers to continually monitor the security and management engines, so that if an internal error is detected, the IPS can automatically fail open; and Zero Power High Availability (ZPHA) options, so in the event of a power loss, the IPS interfaces can switch over to the ZPHA relay, allowing all traffic to pass unimpeded.
- Redundant configuration options: Two IPS platforms can be provisioned using redundant links in a transparent active-active or active-passive high-availability mode. Because an IPS platform acts as a "bump in the wire," does not have an IP address, and does not participate in routing protocols, it can be deployed in existing network designs without changing their configurations, including high-availability routing protocols such as VRRP, OSPF, and HSRP, which are passed transparently by the IPS.
- High throughput inspection for data center and core network deployments: The IPS N Series is designed for data center and network core protection. For these mission-critical network areas, our HP core controller solution combined with a pool of IPS platforms delivers automated inline inspection up to 20 Gbps to protect network devices, virtualization software, operating systems, and applications from attack without impeding performance.
- Low application latency means no degradation of the end-user experience: The IPS platform's unique design means that packet flows are fully inspected and move unimpeded through the platform with typical latency of less than 80 microseconds, independent of the number of filters or security services that are enabled. This eliminates any noticeable application performance impact from an end-user perspective.
- Unmatched filter accuracy means legitimate traffic is not blocked: We use two simple filter writing rules to deliver filter accuracy—No False Positives and No False Negatives. That's why our DVLabs security research team focuses on creating filters to guard entire vulnerabilities, not just known exploits. Vulnerability filters block all exploits for a software vulnerability and provide unmatched levels of accuracy, so the IPS will not block legitimate traffic while protecting the network.
- Virtual patching protects unpatched systems: DVLabs creates vulnerability filters that block all exploits for a given software vulnerability, creating a "virtual patch." These vulnerability filters protect vulnerabilities in virtualization software, operation systems, and applications, and are not exploit specific. They behave like a network-based virtual software patch to protect downstream hosts from network-based attacks on unpatched vulnerabilities.
- Purpose-built hardware and software: Blocking cyber attacks at multi-gigabit speeds with extremely low latency requires purpose-built hardware and software. While other solutions use general-purpose hardware and processors that are simply unable to perform without degrading network performance, our IPS platform provides thorough threat protection at multi-gigabit speeds, with very low latency.
- Leading security research team—Digital Vaccine Labs (DVLabs): DVLabs is the premier security research team for vulnerability discovery in the security industry. The team consists of industry-recognized researchers who apply cutting-edge engineering and analysis in their daily operations. DVLabs is a leader in annual vulnerability discoveries and creates vulnerability filters that are delivered to customers' IPS platforms through the Digital Vaccine Service.
- ThreatLinQ security portal: ThreatLinQ is a service that allows our IPS customers to view the latest threats across the globe from data that is collected from a global network of Lighthouse monitoring devices and from the collection of data from thousands of customer IPS platforms. ThreatLinQ is available to all our customers and provides valuable data that can enable enterprises to more effectively hone their network security policies to meet the demands of the latest threat trends.
- Industry's fastest threat protection keeps ahead of threats: Our Digital Vaccine Service provides evergreen (always up to date) protection against emerging threats. Digital Vaccines are delivered to customers twice a week, or immediately when critical vulnerabilities emerge, and they can be deployed automatically with no IT interaction required. They are created not only to address specific exploits, but also to counter potential attack permutations, protecting customers from zero-day threats.
- Zero-Day Initiative (ZDI) delivers leading zero-day threat protection: DVLabs manages the ZDI program, which is designed to reward worldwide researchers for responsibly disclosing the vulnerabilities they discover. Whether from the DVLabs internal

vulnerability research or the ZDI program, DVLabs passes all vulnerability discoveries to affected software vendors and creates IPS filters to protect customers from potential zero-day attacks before vulnerabilities are disclosed to the public.

- Comprehensive IPS threat and vulnerability coverage for outstanding protection: The combination of talent, research, and security intelligence from the world-class DVLabs research team; over 1,200 researchers in the ZDI program; ThreatLinQ global threat monitoring from thousands of sites; and security community partners like SANS Institute, CERT, and NIST—all combine to provide the broadest threat and vulnerability coverage for outstanding industry-leading protection.
- Full attack surface threat protection: The HP IPS N series provides outstanding vulnerability coverage, including protection of network devices, virtualization software, operating systems, enterprise and Web applications, and industrial control system networks. From Microsoft® operating systems to SCADA and VoIP filters, and many more, HP TippingPoint solutions provide true network protection for today's complex enterprise IT environments.
- Reputation DV Service eliminates "known bad" traffic: The optional Reputation Digital Vaccine (Rep DV) Service provides IPv4, IPv6, and Domain Name System (DNS) security intelligence feeds from a DVLabs global reputation database, so customers can actively enforce and manage reputation security policies using the IPS platform. The IPS platform acts as an enforcement point, inspecting traffic in real time, identifying "known bad" traffic, and enforcing Rep DV security policies.
- IPS automated, proactive protection eliminates most manual event follow-up: Automated policy enforcement virtually eliminates the need to respond to myriad alerts (some real and some false), or to clean up after cyber attacks have compromised network resources. IT security costs are reduced by eliminating ad hoc patching and alert response while simultaneously increasing IT productivity and profitability through bandwidth savings and protection of critical applications.
- Eliminate emergency patching and protect systems from zero-day events: Our vulnerability filters virtually eliminate the need for ad hoc and emergency patching. By protecting software vulnerabilities, IT staff can implement software patches using a regular, scheduled process instead of costly, disruptive emergency patching. The IPS N series blocks attacks and allows IT staff to test security patches before deployment.
- Improve control of end-user desktops: Most IT teams cannot adequately control end-user desktops. In a recent report, client-side applications were shown to be increasingly difficult to keep patched due to the growing number of vulnerabilities. The IPS platform improves IT control through vulnerability protection for unpatched systems and network segmentation to stop the spread of malicious traffic from infected users, all while notifying the administrator about where attacks originate.
- Improve network performance by recapturing misused bandwidth: The IPS N series has bandwidth management capabilities that stop rogue applications like peer-to-peer and streaming media from running rampant throughout the network. By continually cleansing the network of malicious and unwanted traffic, network performance is accelerated for mission-critical applications. And rate-shaping rogue applications can increase bandwidth availability, in some cases by as much as 40 to 70 percent.

  • Easy to install in just minutes, reducing IT burdens: The IPS platform significantly reduces the amount of time and resources needed to maintain a healthy network. The IPS and security management system (SMS) can both be easily installed in the network, typically in 30 minutes to two hours. The IPS is designed for network transparency and is deployed seamlessly into the network with no IP address or MAC address, so it can immediately begin filtering out malicious and unwanted traffic.
- Easy-to-manage solutions reduce IT staff workload: The SMS easily discovers, monitors, configures, diagnoses, and reports on multiple IPS platforms. It features a simple, state-of-the-art secure Java client interface that enables "big-picture" analysis with trending reports, correlation and real-time graphs on traffic statistics, filtered attacks, network hosts and services, as well as IPS inventory and health.
- Flexible local management options: Every IPS unit also has an embedded local security manager (LSM) and command-line interface (CLI). The LSM is a Web GUI management application that provides administration, configuration, and reporting capabilities in an easy-to-use, secure Web interface.
- Automated Digital Vaccine updates reduce ongoing management time: Automated Digital Vaccine (DV) download and distribution capabilities reduce the time required to manage the IPS platform. The SMS allows for manual DV download and distribution, or automated DV download and manual distribution.
- Simple but powerful security policies: The IPS N series allows security administrators to manage security policy with fine granularity. Administrators can set specific network security policies by network segment, VLAN, or Classless Inter-Domain Routing (CIDR). In addition, by utilizing the IPS platform's reputation capabilities and the Reputation Digital Vaccine, customers can now incorporate the use of IP addresses and DNS names into their security policy management.
- Automated enforcement of security policies for compliance: The IPS N series can be a critical component in any IT compliance program. It addresses many compliance program objectives, including vulnerability management with the Digital Vaccine Service and network-monitoring objectives with the security management system. In addition, the IPS may provide a

"compensating control," where a requirement is not specifically satisfied with other solutions or processes.

- Robust security reporting provides auditor details: Reporting from the IPS and SMS allows administrators to show internal and external auditors how the network is protected from the latest threats. In addition to meeting regulatory and internal compliance requirements, organizations can have the best security enforcement available for their networks.

Warranty and support

- 1-year warranty: with advance replacement and 30-calendar-day delivery (available in most countries)
- Electronic and telephone support: limited electronic and telephone support is available from HP; refer to: www.hp.com/networking/warranty for details on the support provided and the period during which support is available
- Software releases: refer to: www.hp.com/networking/warranty for details on the software releases provided and the period during which software releases are available for your product(s)

Technical Specifications

HP S660N 750 Mbps 5 Gig-T/5 1Gb Fiber Segments IPS (JC019A)

Ports	10 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only	
	10 fixed Gigabit Ethernet SFP ports	
Physical characteristics	Dimensions	24(d) x 16.87(w) x 3.42(h) in. (60.96 x 42.86 x 8.69 cm) (2U height)
	Weight	29.1 lb. (13.2 kg)
Mounting	19 or 23 in. wide rack ears provided	
Performance	Latency	< 80 µs
	IPS/IDS throughput	750 Mbps
	Network throughput	750 Mbps
	Security contexts	1,200,000
	Connections per second	115,000
	Concurrent sessions	6,500,000
Environment	Operating temperature	32°F to 104°F (0°C to 40°C)
	Operating relative humidity	5% to 95%, noncondensing
	Nonoperating/Storage temperature	-4°F to 158°F (-20°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
Electrical characteristics	Voltage	100-240 VAC
	Current	8/5 A
	Frequency	50/60 Hz
Safety	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; ROHS Compliance	
Emissions	FCC Class A; VCCI Class A; EN 55022 Class A; AS/NZS 3548 Class A; ICES-003 Class A	
Immunity	ESD	EN 61000-4-2
	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2
	Flicker	EN 61000-3-3
Management	Security Management Server (SMS); command-line interface; Web browser; HP TippingPoint IPS MIB	
Notes	Performance footnotes:	

- IPS/IDS throughput represents the inspection throughput levels measured with recommended security profiles.
- Network throughput represents the maximum throughput levels that can be achieved with the use of traffic forwarding.
- Typical latency is measured on packet sizes up to 1518 bytes.

- Concurrent network sessions is the maximum number of concurrent network sessions that can be supported by the IPS.
- Security contexts is the maximum number of sessions with security state that can be supported by the IPS.

Services

Refer to the HP website at: www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.

HP S1400N 1.5 Gbps 5 Gig-T/5 1Gb Fiber Segments IPS (JC020A)

Ports	10 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only	
	10 fixed Gigabit Ethernet SFP ports	
Physical characteristics	**Dimensions**	24(d) x 16.8(w) x 3.42(h) in. (60.96 x 42.67 x 8.69 cm) (2U height)
	Weight	29.1 lb. (13.2 kg)
Mounting	19 or 23 in. wide rack ears provided	
Performance	**Latency**	< 80 μs
	IPS/IDS throughput	1.5 Gbps
	Network throughput	1.5 Gbps
	Security contexts	1,200,000
	Connections per second	115,000
	Concurrent sessions	6,500,000
Environment	**Operating temperature**	32°F to 104°F (0°C to 40°C)
	Operating relative humidity	5% to 95%, noncondensing
	Nonoperating/Storage temperature	-4°F to 158°F (-20°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
Electrical characteristics	**Voltage**	100-240 VAC
	Current	8/5 A
	Frequency	50/60 Hz
Safety	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; ROHS Compliance	
Emissions	FCC Class A; VCCI Class A; EN 55022 Class A; AS/NZS 3548 Class A; ICES-003 Class A	
Immunity	**ESD**	EN 61000-4-2
	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2
	Flicker	EN 61000-3-3

Technical Specifications

Management	Security Management Server (SMS); command-line interface; Web browser; HP TippingPoint IPS MIB
Notes	Performance footnotes: • IPS/IDS throughput represents the inspection throughput levels measured with recommended security profiles. • Network throughput represents maximum throughput levels that can be achieved with the use of traffic forwarding. • Typical latency is measured on packet sizes up to 1518 bytes. • Concurrent network sessions is the maximum number of concurrent network sessions that can be supported by the IPS. • Security contexts is the maximum number of sessions with security state that can be supported by the IPS.
Services	Refer to the HP website at: www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.

HP S2500N 3Gbps 5 Gig-T/1 10GbE/5 1GbE Fiber Segments IPS (JC021A)

Ports	10 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 10 fixed Gigabit Ethernet SFP ports 2 XFP 10-GbE ports (IEEE 802.3ae Type 10GBASE-LR); Duplex: full only	
Physical characteristics	Dimensions	24(d) x 16.88(w) x 3.42(h) in. (60.96 x 42.88 x 8.69 cm) (2U height)
	Weight	31.5 lb. (14.29 kg)
Mounting	19 or 23 in. wide rack ears provided	
Performance	Latency	< 80 µs
	IPS/IDS throughput	3 Gbps
	Network throughput	15 Gbps
	Security contexts	2,600,000
	Connections per second	230,000
	Concurrent sessions	10,000,000
Environment	Operating temperature	32°F to 104°F (0°C to 40°C)
	Operating relative humidity	5% to 95%, noncondensing
	Nonoperating/Storage temperature	-4°F to 158°F (-20°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
Electrical characteristics	Voltage	100-240 VAC
	Current	8/5 A
	Frequency	50/60 Hz
Safety	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; ROHS Compliance	
Emissions	FCC Class A; VCCI Class A; EN 55022 Class A; AS/NZS 3548 Class A; ICES-003 Class A	
Immunity	ESD	EN 61000-4-2

	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2
	Flicker	EN 61000-3-3
Management	Security Management Server (SMS); command-line interface; Web browser; HP TippingPoint IPS MIB	
Notes	Performance footnotes:	

- IPS/IDS throughput represents the inspection throughput levels measured with recommended security profiles.
- Network throughput represents the maximum throughput levels that can be achieved with the use of traffic forwarding.
- Typical latency is measured on packet sizes up to 1518 bytes.
- Concurrent network sessions is the maximum number of concurrent network sessions that can be supported by the IPS. The measured number was limited by the available test equipment.
- Security contexts is the maximum number of sessions with security state that can be supported by the IPS.

Services	Refer to the HP website at: www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.	

HP S5100N 5Gbps 5 GigT/1 10GbE/5 1GbE Fiber Segments IPS (JC022A)

Ports	10 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only	
	10 fixed Gigabit Ethernet SFP ports	
	2 XFP 10-GbE ports (IEEE 802.3ae Type 10GBASE-LR); Duplex: full only	
Physical characteristics	Dimensions	24(d) x 16.88(w) x 3.42(h) in. (60.96 x 42.88 x 8.69 cm) (2U height)
	Weight	31.5 lb. (14.29 kg)
Mounting	19 or 23 in. wide rack ears provided	
Performance	Latency	< 80 µs
	IPS/IDS throughput	5 Gbps
	Network throughput	15 Gbps
	Security contexts	2,600,000
	Connections per second	230,000
	Concurrent sessions	10,000,000
Environment	Operating temperature	32°F to 104°F (0°C to 40°C)
	Operating relative humidity	5% to 95%, noncondensing
	Nonoperating/Storage temperature	-4°F to 158°F (-20°C to 70°C)

Technical Specifications

	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
Electrical characteristics	Voltage	100-240 VAC
	Current	8/5 A
	Frequency	50/60 Hz
Safety	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; ROHS Compliance	
Emissions	FCC Class A; VCCI Class A; EN 55022 Class A; AS/NZS 3548 Class A; ICES-003 Class A	
Immunity	ESD	EN 61000-4-2
	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2
	Flicker	EN 61000-3-3
Management	Security Management Server (SMS); command-line interface; Web browser; HP TippingPoint IPS MIB	
Notes	Performance footnotes: • IPS/IDS throughput represents the inspection throughput levels measured with recommended security profiles. • Network throughput represents the maximum throughput levels that can be achieved with the use of traffic forwarding. • Typical latency is measured on packet sizes up to 1518 bytes. • Concurrent network sessions is the maximum number of concurrent network sessions that can be supported by the IPS. The measured number was limited by available test equipment. • Security contexts is the maximum number of sessions with security state that can be supported by the IPS.	
Services	Refer to the HP website at: www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.	

HP S6100N 8Gbps IPS (JC577A)

Ports	10 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only	
	10 fixed Gigabit Ethernet SFP ports	
	2 XFP 10-GbE ports (IEEE 802.3ae Type 10GBASE-LR); Duplex: full only	
Physical characteristics	Dimensions	24(d) x 16.88(w) x 3.42(h) in. (60.96 x 42.88 x 8.69 cm) (2U height)
	Weight	31.5 lb. (14.29 kg)
Mounting	19 or 23 in. wide rack ears provided	
Performance	Latency	< 80 µs
	IPS/IDS throughput	8 Gbps*
	Network throughput	15 Gbps

Technical Specifications

	Security contexts	2,600,000
	Connections per second	230,000
	Concurrent sessions	10,000,000
Environment	Operating temperature	32°F to 104°F (0°C to 40°C)
	Operating relative humidity	5% to 95%, noncondensing
	Nonoperating/Storage temperature	-4°F to 158°F (-20°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
Electrical characteristics	Voltage	100-240 VAC
	Current	8/5 A
	Frequency	50/60 Hz
Safety	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; ROHS Compliance	
Emissions	FCC Class A; VCCI Class A; EN 55022 Class A; AS/NZS 3548 Class A; ICES-003 Class A	
Immunity	ESD	EN 61000-4-2
	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2
	Flicker	EN 61000-3-3
Management	Security Management Server (SMS); command-line interface; Web browser; HP TippingPoint IPS MIB	
Notes	Performance footnotes:	

- *IPS/IDS throughput represents the inspection throughput levels measured with recommended security profiles. The S6100N IPS provides inspection throughput up to 9.5 Gbps
- Network throughput represents the maximum throughput levels that can be achieved with the use of traffic forwarding.
- Typical latency is measured on packet sizes up to 1518 bytes.
- Concurrent network sessions is the maximum number of concurrent network sessions that can be supported by the IPS. The measured number was limited by available test equipment.
- Security contexts is the maximum number of sessions with security state that can be supported by the IPS.

Services	Refer to the HP website at: www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.

Accessories

HP S Intrusion Prevention System (IPS) N Series accessories	Mounting Kit	
	HP Slide Kit Quick Release	JC017A

To learn more, visit: www.hp.com/networking