Hewlett Packard Enterprise

Data sheet

HPE TippingPoint NX Platform Next Generation Intrusion Prevention Systems

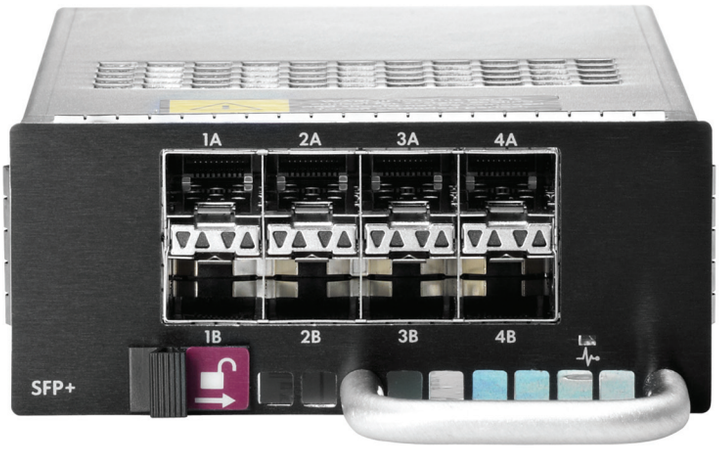
Runs faster than your business

Overview

The HPE TippingPoint NX Platform Next Generation Intrusion Prevention System (NGIPS) achieves a new level of in-line, real-time protection, providing proactive network security that is ideal for data center, core and perimeter deployments for today's and tomorrow's real-world network traffic and data centers. The next-generation architecture provides modular software design that enables the addition of valuable network protection services as NGIPS continues to evolve from first generation IPS technology. The HPE TippingPoint NX Platform represents the highest performing NGIPS in a minimal footprint. This new improved NGIPS platform redefines the next generation of intrusion prevention as a foundation for comprehensive network security across all critical areas in the enterprise.

Key components

Hewlett Packard Enterprise is transforming the enterprise security landscape with the latest network and application security that provide advanced protection against today's sophisticated cyber threats from perimeter to core, to campus and branch offices. The TippingPoint NX Platform Next Generation Intrusion Prevention System (NGIPS) is a key component of this overall offering. The TippingPoint NGIPS platforms uniquely leverage advanced threat research with the powerful correlation of security events and vulnerabilities. By delivering unparalleled visibility across security assets in context of business critical processes and applications we help our customers manage their risk and maximize their security investments.



Benefits and features

Key benefits

- **Proven in-line threat protection:** In 2001, HPE TippingPoint developed the in-line IPS to provide the first proactive, in-line network protection solution that also provided high network performance and availability. Since 2009, HPE TippingPoint has provided NGIPS solutions, with up to 20 Gb/s of protection in just two rack units (2U). The NX represents one of the highest performing NGIPS per rack unit, saving enterprises rack and data center space, power consumption, and cooling costs.
- **Beyond first generation IPS:** The NX Platform enables the convergence of new security services such as:
  - Intelligent blocking via context—HPE TippingPoint Threat Digital Vaccine (ThreatDV), customer-defined IP DNS reputation entries, and location-based policies (perimeter, core, branch office, etc.).
  - Application awareness, visibility, and control with deep packet, and customer-developed protection filters.
  - Content awareness and control for inspecting specific file types and protecting critical information.
  - Integration with HPE Enterprise Security solutions to provide additional security intelligence, visibility, and control across the entire data center.
- **Leading security research teams: HPE TippingPoint DVLabs and Zero Day Initiative (ZDI):** 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 also manages the ZDI program, which is designed to reward worldwide researchers for responsibly disclosing vulnerabilities they discover. Whether from DVLabs internal vulnerability research or the ZDI program, DVLabs passes all vulnerability discoveries to affected software vendors and creates NGIPS filters to protect customers from potential zero-day attacks before vulnerabilities are disclosed to the public.

- **Highest port density for the data center core or anywhere protection is needed:** The new NX Platform NGIPS supports a market-leading number of segments across multiple configurations. The NX Platform can support up to 24 segments of 1GbE, 16 segments of 10GbE, or 4 segments of 40GbE.
- **Proven reliability and redundancy:** The NGIPS platform is designed to deliver unparalleled high availability. This ensures that network traffic always flows at wire speed in the event of network error or internal device failure.
- **High throughput, low latency inspection for data center and core network deployments:** The HPE TippingPoint NX Series is designed for data center and network core protection. For these mission-critical network areas, the HPE TippingPoint NX NGIPS platform delivers automated, in-line inspection up to 20 Gb/s, with a typical latency of less than 40 microseconds, to protect network devices, virtualization software, operating systems, and applications from attack without impeding performance.
- **Unmatched filter accuracy assures that legitimate traffic is not blocked:** HPE TippingPoint uses two simple filter writing rules to guarantee filter accuracy—No False Positives and No False Negatives. That's why our HPE TippingPoint DVLabs security research team focuses on creating filters to protect against entire vulnerabilities, not just known exploits. Vulnerability filters block all exploits of the software vulnerability and provide unmatched levels of accuracy so the NGIPS will not block legitimate traffic while protecting the network.
- **Reduce emergency patching and protect systems from zero-day events:** Our vulnerability filters virtually remove 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. In a recent report, client-side applications were shown to be increasingly difficult to keep patched due to the growing number of vulnerabilities. The NGIPS platform improves IT control through vulnerability protection for unpatched systems and network segmentation to stop the spread of malicious traffic from infected users. The HPE TippingPoint NX Platform NGIPS blocks attacks and allows IT staff to test security patches before deployment.
- **Improve network performance by recapturing misused bandwidth:** The HPE TippingPoint NX Platform NGIPS bandwidth management capabilities 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 in some cases by 40–70 percent.[1]

[1] HP (now Hewlett Packard Enterprise) lab study, June 2012.

- **Easy to install in just minutes, minimizing IT burdens:** The NGIPS Platform significantly reduces the amount of time and resources needed to maintain a healthy network. The NGIPS and security management system (SMS) can both be easily installed in the network, typically in 30 minutes to two hours. The NGIPS 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.
- **Simple but powerful security policies:** The NGIPS allows security administrators to manage security policy with fine granularity. Administrators can set specific network security policies by network segment, by VLAN, or by Classless Inter-Domain Routing (CIDR). In addition, by utilizing the NGIPS platform's reputation capabilities and the Threat Digital Vaccine, customers can now incorporate the use of IP addresses and DNS names into their security policy management.
- **Robust security reporting provides audit details:** Reports from the NGIPS and SMS allow 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.

Key features

- Award-winning proactive network security
- Multiple security services to provide additional security context
- Deep packet inspection with application and content awareness, visibility and control
- Industry-leading security research team—HPE TippingPoint DVLabs
- Automated protection to reduce zero day vulnerabilities and reduce ongoing management time
- Support for a broad set of traffic types
- High efficiency, dual redundant load sharing power supplies reduce power consumption and heat dissipation
- Active and intelligent system-cooling design to minimize power draw, reduce audible noise and maximize thermal performance based on specific system needs
- NEBS and FIPS compatible

Technical specifications

	S2600NX	S5200NX	S6200NX	S7100NX	S7500NX
Performance	Inspection throughput: 3 Gb/s Network throughput: 40 Gb/s Typical latency: <40 microseconds Security contexts: 2,600,000 Connections per second: 300,000 Concurrent sessions: 30,000,000	Inspection throughput: 5 Gb/s Network throughput: 40 Gb/s Typical latency: <40 microseconds Security contexts: 2,600,000 Connections per second: 300,000 Concurrent sessions: 30,000,000	Inspection throughput: 10 Gb/s Network throughput: 40 Gb/s Typical latency: <40 microseconds Security contexts: 4,000,000 Connections per second: 450,000 Concurrent sessions: 60,000,000	Inspection throughput: 15 Gb/s Network throughput: 100 Gb/s Typical latency: <40 microseconds Security contexts: 5,000,000 Connections per second: 450,000 Concurrent sessions: 60,000,000	Inspection throughput: 20 Gb/s Network throughput: 100 Gb/s Typical latency: <40 microseconds Security contexts: 5,000,000 Connections per second: 450,000 Concurrent sessions: 60,000,000
High density I/O modules	Every NX chassis supports up to 4 hot-swappable I/O modules With the NX chassis populated with 4 of the SFP+ NX I/O modules, you can achieve inspection of up to 16 segments of 10GbE, or a combination of 1GbE, 10GbE, and 40GbE segments	Every NX chassis supports up to 4 hot-swappable NX I/O modules With the NX chassis populated with 4 of the SFP+ NX I/O modules, you can achieve inspection of up to 16 segments of 10GbE, or a combination of 1GbE, 10GbE, and 40GbE segments	Every NX chassis supports up to 4 hot-swappable I/O modules With the NX chassis populated with 4 of the SFP+ NX I/O modules, you can achieve inspection of up to 16 segments of 10GbE, or a combination of 1GbE, 10GbE, and 40GbE segments	Every NX chassis supports up to 4 hot-swappable NX I/O modules With the NX chassis populated with 4 of the SFP+ NX I/O modules, you can achieve inspection of up to 16 segments of 10GbE, or a combination of 1GbE, 10GbE, and 40GbE segments	Every NX chassis supports up to 4 hot-swappable I/O modules With the NX chassis populated with 4 of the SFP+ NX I/O modules, you can achieve inspection of up to 16 segments of 10GbE, or a combination of 1GbE, 10GbE, and 40GbE segments
Physical characteristics	Dimensions: 21.75 (d) x 16.8 (w) x 3.5 (h) in. (55.25 x 42.78 x 8.89 cm) Weight: 42 lb. (19.1 kg) Rack units: 2 Includes mounting hardware for 2-post front, 2-post mid, and 4-post quick release slides rail mounting	Dimensions: 21.75 (d) x 16.8 (w) x 3.5 (h) in. (55.25 x 42.78 x 8.89 cm) Weight: 42 lb. (19.1 kg) Rack units: 2 Includes mounting hardware for 2-post front, 2-post mid, and 4-post quick release slides rail mounting	Dimensions: 21.75 (d) x 16.8 (w) x 3.5 (h) in. (55.25 x 42.78 x 8.89 cm) Weight: 42 lb. (19.1 kg) Rack units: 2 Includes mounting hardware for 2-post front, 2-post mid, and 4-post quick release slides rail mounting	Dimensions: 21.75 (d) x 16.8 (w) x 3.5 (h) in. (55.25 x 42.78 x 8.89 cm) Weight: 42 lb. (19.1 kg) Rack units: 2 Includes mounting hardware for 2-post front, 2-post mid, and 4-post quick release slides rail mounting	Dimensions: 21.75 (d) x 16.8 (w) x 3.5 (h) in. (55.25 x 42.78 x 8.89 cm) Weight: 42 lb. (19.1 kg) Rack units: 2 Includes mounting hardware for 2-post front, 2-post mid, and 4-post quick release slides rail mounting
Environment	Operating temperature: 32°F to 104°F (0°C to 40°C) Operating relative humidity: 5% to 95% non-condensing Non-operating/storage temperature: -4°F to 158°F (-20°C to 70°C) Non-operating/storage relative humidity: 5% to 95% non-condensing Altitude: Up to 10,000 ft (3,048 m)	Operating temperature: 32°F to 104°F (0°C to 40°C) Operating relative humidity: 5% to 95% non-condensing Non-operating/storage temperature: -4°F to 158°F (-20°C to 70°C) Non-operating/storage relative humidity: 5% to 95% non-condensing Altitude: Up to 10,000 ft (3,048 m)	Operating temperature: 32°F to 104°F (0°C to 40°C) Operating relative humidity: 5% to 95% non-condensing Non-operating/storage temperature: -4°F to 158°F (-20°C to 70°C) Non-operating/storage relative humidity: 5% to 95% non-condensing Altitude: Up to 10,000 ft (3,048 m)	Operating temperature: 32°F to 104°F (0°C to 40°C) Operating relative humidity: 5% to 95% non-condensing Non-operating/storage temperature: -4°F to 158°F (-20°C to 70°C) Non-operating/storage relative humidity: 5% to 95% non-condensing Altitude: Up to 10,000 ft (3,048 m)	Operating temperature: 32°F to 104°F (0°C to 40°C) Operating relative humidity: 5% to 95% non-condensing Non-operating/storage temperature: -4°F to 158°F (-20°C to 70°C) Non-operating/storage relative humidity: 5% to 95% non-condensing Altitude: Up to 10,000 ft (3,048 m)

Technical specifications (continued.)

	S2600NX	S5200NX	S6200NX	S7100NX	S7500NX
Safety	UL 60950-1; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; EN/IEC 60825-1; ROHS Compliance	UL 60950-1; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; EN/IEC 60825-1; ROHS Compliance	UL 60950-1; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; EN/IEC 60825-1; ROHS Compliance	UL 60950-1; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; EN/IEC 60825-1; ROHS Compliance	UL 60950-1; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; EN/IEC 60825-1; ROHS Compliance
Emissions	FCC Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; CNS 13438 Class A	FCC Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; CNS 13438 Class A	FCC Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; CNS 13438 Class A	FCC Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; CNS 13438 Class A	FCC Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; CNS 13438 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	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	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	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	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
Electrical characteristics AC	Voltage: 100–240 VAC Current (Max. Fused Power): 12/6 A Frequency: 50–60 Power consumption: 750 W (2559 BTU/hour)	Voltage: 100–240 VAC Current (Max. Fused Power): 12/6 A Frequency: 50–60 Power consumption: 750 W (2559 BTU/hour)	Voltage: 100–240 VAC Current (Max. Fused Power): 12/6 A Frequency: 50–60 Power consumption: 750 W (2559 BTU/hour)	Voltage: 100–240 VAC Current (Max. Fused Power): 12/6 A Frequency: 50–60 Power consumption: 750 W (2559 BTU/hour)	Voltage: 100–240 VAC Current (Max. Fused Power): 12/6 A Frequency: 50–60 Power consumption: 750 W (2559 BTU/hour)
Electrical characteristics DC	Voltage: -40/-60 VDC Current (Max. Fused Power): 24/16 A Power consumption: 812 W (2767 BTU/hour)	Voltage: -40/-60 VDC Current (Max. Fused Power): 24/16 A Power consumption: 812 W (2767 BTU/hour)	Voltage: -40/-60 VDC Current (Max. Fused Power): 24/16 A Power consumption: 812 W (2767 BTU/hour)	Voltage: -40/-60 VDC Current (Max. Fused Power): 24/16 A Power consumption: 812 W (2767 BTU/hour)	Voltage: -40/-60 VDC Current (Max. Fused Power): 24/16 A Power consumption: 812 W (2767 BTU/hour)
Management	One 10/100/1000 RJ-45 port Manageable via security management server (SMS), command-line interface, Web browser, HPE TippingPoint IPS Management Information Base (MIB)	One 10/100/1000 RJ-45 port Manageable via security management server (SMS), command-line interface, Web browser, HPE TippingPoint IPS Management Information Base (MIB)	One 10/100/1000 RJ-45 port Manageable via security management server (SMS), command-line interface, Web browser, HPE TippingPoint IPS Management Information Base (MIB)	One 10/100/1000 RJ-45 port Manageable via security management server (SMS), command-line interface, Web browser, HPE TippingPoint IPS Management Information Base (MIB)	One 10/100/1000 RJ-45 port Manageable via security management server (SMS), command-line interface, Web browser, HPE TippingPoint IPS Management Information Base (MIB)

Ordering information

NX IPS models

JC874A	S2600NX, Includes 2 AC power supplies (JC826A) and quick release slide rail kit (JC017A)
JC824A	S5200NX, Includes 2 AC power supplies (JC826A) and quick release slide rail kit (JC017A)
JC873A	S6200NX, Includes 2 AC power supplies (JC826A) and quick release slide rail kit (JC017A)
JC644A	S7100NX, Includes 2 AC power supplies (JC826A) and quick release slide rail kit (JC017A)
JC872A	S7500NX, Includes 2 AC power supplies (JC826A) and quick release slide rail kit (JC017A)

NX I/O modules

JC768A	6-segment Gig-T Copper NX Module
JC769A	6-segment 1GbE SFP Fiber NX Module
JC770A	4-segment 10GbE SFP+ Fiber NX Module
JC771A	1-segment 40GbE QSFP+ Fiber NX Module

Supported transceivers

JC012A	1G SFP LC LX Transceiver Bundle (2 pieces)
JC013A	1G SFP LC SX Transceiver Bundle (2 pieces)
JC009A	1G SFP RJ45 T Copper Transceiver
JC859A	10G SFP+ LC SR Transceiver
JC860A	10G SFP+ LC LR Transceiver
JC858A	40G QSFP+ SR4 850nm Transceiver

Power supplies and accessories

JC825A	NX IPS Fan Module
JC826A	NX IPS 750W AC Power Supply
JC827A	NX IPS 750W DC Power Supply
JC828A	NX IPS CFast Card

BYPASS MODULES	TYPICAL SWITCHING TIME	MAX. PHYSICAL SWITCHING TIME	NORMAL MODE NOMINAL INSERTION LOSS	NORMAL MODE WORST CASE INSERTION LOSS	BYPASS MODE NOMINAL INSERTION LOSS	BYPASS MODE WORST CASE INSERTION LOSS
JC877A–4-Segment Gig-T Copper bypass module	2 ms	10 ms	NA	NA	NA	NA
JC878A–2-segment 1GbE Fiber SR bypass module	3 ms	10 ms	0.7 db	1.65 db	0.8 db	2.0 db
JC879A–2-segment 1GbE Fiber LR bypass module	4 ms	10 ms	0.8 db	1.6 db	0.9 db	1.9 db
JC880A–2-segment 10GbE Fiber SR bypass	3 ms	10 ms	0.7 db	1.65 db	0.8 db	2.0 db
JC881A–2-segment 10GbE Fiber LR bypass	4 ms	10 ms	0.8 db	1.6 db	0.9 db	1.9 db

Resources

For service overview, data sheets, ordering guide, and technical overview
hpe.com/software/services

Hewlett Packard Enterprise Services

HPE ESP Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people. hpe.com/software/espservices

Learn more at
hpe.com/software/ngips

Hewlett Packard Enterprise

4AA4-1063ENW, November 2015, Rev. 4