Hillstone S-Series

Network Intrusion Prevention System (NIPS)

As the threat landscape continues to evolve aggressively, an increasing number of network protection technologies have quickly emerged. Among these various technologies, Intrusion Prevention System (IPS) remains one of the most widely deployed solutions, regardless of platform or form factor. Hillstone Network-based IPS (NIPS) appliance operates in-line, and at wire speed, performing deep packet inspection, and assembling inspection of all network traffic. It also applies rules based on several methodologies, including protocol anomaly analysis and signature analysis to block threats. In addition, NIPS leverages AI technology to achieve DDoS protection and encrypted traffic detection without decryption for intelligent and efficient threat protection. Hillstone NIPS can be deployed in the network to inspect traffic left undetected by perimeter solutions, and is an integral part of network security systems for its high-performance, no compromise, best-of- breed protection capability and broad and flexible deployment scenarios.

Product Highlights

Unparalleled Threat Protection without Performance Compromise

The Hillstone NIPS platform has the most comprehensive high performance inspection engine, combined with the best- of-breed signature partnering with leading technology partners, providing customers the highest threat detection rate with the lowest total cost of ownership (TCO). Hillstone IPS engine has 99.6% blocking rate of static exploits and 98.325% blocking rate of live exploits (reported by NSS Labs).

The Hillstone NIPS platform provides high throughput, low latency and maximum availability to maintain efficient security operations without compromising network performance. NIPS combines protocol analysis, threat reputation and other features that deliver threat protection from Layer 2 to Layer 7, including ARP attack, Dos/DDoS attack, abnormal protocols, malicious URLs, malwares and web attacks.

Ease of Deployment and Centralized Management

Deploying and managing the Hillstone NIPS is simple, with minimum overhead. It can be deployed in the following modes to meet security requirements and ensure optimal network connectivity:

- Active protection (intrusion prevention mode), real time monitoring and blocking.
- Passive detection (intrusion detection mode), real time monitoring and alert.

The Hillstone NIPS can be managed by the Hillstone Security Management Platform (HSM). Administrators can centrally register, monitor, and upgrade NIPS devices deployed in different branches or locations, with a unified management policy across the network for maximum efficiency.

Granular Reporting with User Targeted Viewpoints

Hillstone NIPS provides comprehensive visibility based on protocol, application, user and content. It can identify more than 4,000 applications, including hundreds of mobile and cloud applications.

Bringing multiple sources together, the system can identify contextual information to make proper blocking decisions. With a granular and robust reporting function, it offers visibility across different views:

- Unique templates, based on whether you are a business system administrator, a security administrator or the CIO or executive.
- Organized Threat Content – whether a security, system risk, network threat or traffic view – in order to help you clearly understand the risk and make the right decision.

Features

Intrusion Prevention

- 12,700+ signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
- IPS Actions: monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time
- Packet logging option
- Filter based selection and review: severity, target, OS, application or protocol
- IP exemption from specific IPS signatures
- IDS sniffer mode
- IPv4 and IPv6 rate-based DoS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCIP/ICMP session flooding (source/destination)
- Active bypass with bypass interfaces
- Predefined prevention configuration
- Support web server protection, including CC attack, external link attack, iframe, cross-site request forgery (CSRF) attack, sensitive file scanning attack, etc.
- Support protection of brute force attack including FTP, MSRPC, POP3, SMTP, SUNRPC, telnet, VNC, RDP, SSH, SMB, LDAP, IMAP and HTTP, SVN, CVS, RSH, Mongodb, Oracle, MSsql, NNTP, REDIS, IRC, RTSP, Casandra, Rlogin, FireBird, Kerberos, SIP, RADIUS, DB2, PGSQL, Sybase, REXEC, SOCKET5 protocols
- Support weak password detection for FTP, POP3, SMTP, Telnet, IMAP, HTTP, Cassandra, DB2, PGSQL, RLOGIN, Sybase, REXEC, SOCKET5, NNTP, REDIS, IRC, RTSP protocols
- Support importing/exporting custom weak passwords in the weak password dictionary, with a maximum capacity of 200,000 items
- Support HTTP plaintext password detection
- Threat Details support URI and Attack Data Decoding
- Support MPLS frame inspection
- Support scanning and parsing base64-encoded data
- Detect abnormal encrypted traffic without decryption
- Support global IP whitelist

Threat Correlation Analytics

- Correlation among unknown threats, abnormal behavior and application behavior to discover potential threat or attacks
- Multi-dimension correlation rules, automatic daily update from the cloud

Advanced Threat Detection

- Behavior-based advanced malware detection
- Detection of more than 2000 known and unknown malware families including Virus, Worm, Trojan, Spyware, Overflow etc.
- Real-time, online, malware behavior model database update
- Support mapping detected threats to MITRE ATT&CK tactics

Abnormal Behavior Detection

- Behavior modeling based on L3-L7 baseline traffic to reveal anomalous network behavior, such as HTTP scanning, Spider, SPAM, SSH/FTP weak password, and spyware
- Detection of DDoS including Flood, Sockstress, zip of death, reflect, DNS query, SSL DDos and application DDoS
- Supports inspection of encrypted tunneling traffic for unknown applications
- Real-time, online, abnormal behavior model database update

Antivirus

- Manual, automatic push or pull signature updates
- Flow-based antivirus: protocols include HTTP/HTTPS, SMTP, POP3, IMAP, FTP, SMB, support virus filtering and blocking of files transferred with SMB protocol when resuming from breakpoint
- Compressed file virus scanning
- Intelligent virus detection for PE, ELF, PDF and Microsoft Office files

Attack Defense

- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN Flood, DNS Query Flood defense, SIP Flood defense, etc.
- IP scanning and port scanning
- Intelligent DoS/DDoS defense with ML-based baseline establishment
- Attack defense for Internet Control Message Protocol (ICMP) redirection, ARP, and Malformed Packet

URL Filtering

- Flow-based web filtering inspection
- Manually defined web filtering based on URL, web content and MIME header
- Dynamic web filtering with cloud-based real-time categorization database: over 500 million URLs with 64 categories (8 of which are security related)
- Additional web filtering features:
  - Filter Java Applet, ActiveX or cookie
  - Block HTTP Post
  - Log search keywords
  - Exempt scanning encrypted connections on certain categories for privacy
- Web filtering profile override: allows administrator to temporarily assign different profiles to user/group/IP
- Web filter local categories and category rating override
- Support allow/block list
- Customizable alarm

Anti-Spam

- Real-time spam classification and prevention
- Confirmed spam, suspected spam, bulk spam, valid bulk
- Protection regardless of the language, format, or content of the message
- Support both SMTP and POP3 email protocols
- Inbound and outbound detection
- Whitelists to allow emails from trusted domain/email addresses
- User-defined blacklists

Cloud-Sandbox

- Upload malicious files to cloud sandbox for analysis
- Support protocols including HTTP/HTTPS, POP3, IMAP, SMTP and FTP
- Support file types including PE, ZIP, RAR, Office, PDF, APK, JAR and SWF
- File transfer direction and file size control
- Provide complete behavior analysis report for malicious files
- Global threat intelligence sharing, real-time threat blocking
- Support detection only mode without uploading files

Data Security

- Content filtering: file types include doc, docx, xls, xlsx, ppt, pptx, txt; file protocols include FTP, HTTP(S), SMTP(S), POP3(S), IMAP(S), SMB
- Support file filtering with over 100 file formats
- Support network behavior recording

Botnet C&C Prevention

- Discover intranet botnet host by monitoring C&C connections and block further advanced threats such as botnet and ransomware
- Regularly update the botnet server addresses
- Prevention for C&C IP and domain
- Support TCP, HTTP, and DNS traffic detection
- Support Domain Generation Algorithm (DGA) detection
- IP and domain whitelists
- Support manually/automatically imports multiple C2 threat intelligence, and exporting custom threat intelligence

Features (Continued)

IP Reputation
- Identify and filter traffic from risky IPs such as botnet hosts, spammers, Tor nodes, breached hosts, and brute force attacks
- Logging, dropping packets, or blocking for different types of risky IP traffic
- Regular IP reputation signature database upgrade

Application Control
- Over 4,000 applications that can be filtered by name, category, subcategory, technology and risk
- Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference
- Actions: block, monitor
- Provide multi-dimensional monitoring and statistics for applications running in the cloud, including risk category and characteristics
- Support encrypted application

Quality of Service (QoS)
- Support encrypted application
- Max/guaranteed bandwidth tunnels or IP/user basis
- Tunnel allocation based on security domain, interface, address, user/user group, server/server group, application/app group, TOS, VLAN
- Bandwidth allocated by time, priority, or equal bandwidth sharing
- Type of Service (TOS) and Differentiated Services (DiffServ) support
- Prioritized allocation of remaining bandwidth
- Maximum concurrent connections per IP
- Bandwidth allocation based on URL category
- Bandwidth limit by delaying access for user or IP

IPv6
- Management over IPv6, IPv6 logging and HA
- IPv6 tunneling, DNS64/NAT64 etc.
- IPv6 routing protocols, static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, Antivirus, Access control, ND attack defense

VSYS
- System resource allocation to each VSYS
- CPU virtualization
- Non-root VSYS support IPS, URL filtering, Policy, QoS, etc.
- VSYS monitoring and statistics
- Support backup of all VSYS configurations at once

SSL Proxy
- SSL offload: SSL traffic decryption
- SSL require/ exempt: SSL traffic allowed or block based on the policy rules without decryption
- IP and domain whitelists

Flexible Traffic Analysis and Control
- Support 3 operation modes: Route/NAT (layer 3), Transparent (layer 2) with optional bypass interface, and TAP mode (IDS Mode) with Hillstone Firewall Integration
- Traffic analysis and control based on policy rules by source/destination zone, source/destination IP address, users, service or applications

High Availability
- Redundant heartbeat interfaces
- AP and peer mode
- Standalone session synchronization
- HA reserved management interface
- Failover:
  - Port, local & remote link monitoring
  - Stateful failover
  - Sub-second failover
  - Failure notification
- Deployment Options:
  - HA with link aggregation
  - Full mesh HA
  - Geographically dispersed HA

Visible Administration
- Management access: HTTP/HTTPS, SSH, telnet, netconf, console
- Central Management: Hillstone Security Manager (HSM), web service APIs
- Two-factor authentication: username/password, HTTPS certificates file
- System Integration: SNMP, syslog, alliance partnerships
- Upload threat data to iSource for analysis
- Rapid deployment: USB auto-install, local and remote script execution
- Dynamic real-time dashboard status and drill-in monitoring widgets
- Storage device management: storage space threshold customization and alarm, old data overlay, stop recording
- Support packet upload and reply via WebUI
- Language support: English

Logs and Reporting
- Logging facilities: local storage for up to 6 months, multiple syslog servers and multiple Hillstone Security Audit (HSA) platforms
- Encrypted logging and log integrity with HSA scheduled batch log uploading
- Reliable logging using TCP option (RFC 3195)
- Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets
- Comprehensive event logs: system and administrative activity audits, routing & networking, VPN, user authentications, WiFi related events
- Support displaying attack result and associated user account in threat logs
- Threat log evidence display and highlighting
- Log aggregation: support aggregation of AV and C&C logs
- IP and service port name resolution option
- Brief traffic log format option
- Granular Reporting with User Targeted Viewpoints
  - HA Management/C-level View
  - Business System Owner View
  - Network Security Administrator View

Statistics and Monitoring
- Application, URL, threat events statistic and monitoring
- Real-time traffic statistic and analytics
- System information such as concurrent session, CPU, Memory and temperature
- iQOS traffic statistic and monitoring, link status monitoring
- Support traffic information collection and forwarding via Netflow (v9.0)
- Cloud-based threat intelligence push service
- Geographical distribution of external network attacks

CloudView
- Cloud-based security monitoring
- 24/7 access from web or mobile application
- Device status, traffic and threat monitoring
- Cloud-based log retention and reporting

Specifications

	S1115-IN	S1200-IN	S1215-IN	S1900-IN	S2100-IN
					
IPS Throughput [1]	2 Gbps	3 Gbps	3 Gbps	3 Gbps	5 Gbps
Maximum Concurrent Connections, TCP (Standard/with AEL) [2]	1.2 Million	1.2 Million	1.2 Million	1.2 Million	1.2 Million
New Connections per Second, HTTP [3]	30,000	40,000	40,000	50,000	60,000
Stoneshield	N/A	N/A	N/A	N/A	N/A
Virtual Systems (Default/ Max)	1/5	1/5	1/5	1/5	1/5
Storage [4]	500 GB / 1 TB SSD	500 GB / 1 TB SSD	500 GB / 1 TB SSD	500 GB / 1 TB SSD	500 GB / 1 TB SSD
Form Factor	1U	1U	1U	1U	1U
Management Ports	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA	2 × USB port, 1 × MGT port, 1 × Console port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA	2 × USB Port, 1 × MGT, 1 × Console Port	2 × USB port, 1 × MGT port, 1 × Console port
Fixed I/O Ports	8 × SFP, 8×GE (including 2 pairs Bypass port),	2 ×SFP+, 8 × SFP.8 × GE	8 × GE (including 2 pairs Bypass port), 8 × SFP	8 × GE (including 1 pair Bypass port)	2 ×SFP+, 8 × SFP 8 ×GE
Available Slots for Expansion Modules	1 x Generic Slot	N/A	1 x Generic Slot	N/A	N/A
Expansion Module Option	IOC-S-F-4SFP+-A-IN IOC-S-F-8SFP+-A-IN IOC-S-F-8GE-B-A-IN	N/A	IOC-S-F-4SFP+-A-IN IOC-S-F-8SFP+-A-IN IOC-S-F-8GE-B-A-IN	N/A	N/A
Latency	<300 µs	<300 µs	<300 µs	<70 µs	<350 µs
Bypass Support (Default/Max.)	4/12	N/A	4/12	2/2	N/A
Power Supply	AC 100-240V 50/60 Hz	AC 100~240V 50/60Hz	AC 100-240 V 50/60 Hz	DC-36~-72V AC100-240V50/60Hz	AC 100-240 V 50/60 Hz
Maximum Power Consumption	60W 1 × AC power supply 2 × AC power supply	50W 1 × AC power supply 2 × AC power supply	60W 1 × AC power supply 2 × AC power supply	50W 1 × AC power supply 2 × AC power supply	50W 1 × AC power supply 2 × AC power supply
Dimension (W×D×H, mm)	17.3 × 13.4 × 1.7 in (440 × 340 × 44 mm)	17.3 × 12.6 × 1.7 in (440 × 320 × 44 mm)	17.3 × 13.4 × 1.7 in (440 × 340 × 44 mm)	17.1 × 12.6 × 1.7 in (436 × 320 × 44mm)	17.3 × 12.6 × 1.7 in (440 × 320 × 44mm)
Weight	10.0 lb (4.55 kg)	17 lb (7.7 kg)	10.0 lb (4.55 kg)	14.33 lb (6.5kg)	16.9 lb (7.7kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	10%~95% (no dew)	10-95% (no dew)	10%-95% (no dew)	10%-95% (no dew)

Specifications (Continued)

	S2115-IN	S2300-IN	S2700-IN	S3500-IN	S3805-IN
					
IPS Throughput [1]	5 Gbps	9 Gbps	11 Gbps	15 Gbps	20 Gbps
Maximum Concurrent Connections, TCP (Standard/with AEL) [2]	1.2 Million	3 Million	6 Million	8 Million	12 Million
New Connections per Second, HTTP [3]	60,000	60,000	60,000	140,000	250,000
Stoneshield	N/A	N/A	N/A	N/A	N/A
Virtual Systems (Default/ Max)	1/5	1/5	1/50	1/50	1/50
Storage [4]	500 GB / 1 TB SSD	500 GB / 1 TB SSD	500 GB / 1 TB SSD	1 TB SSD	1 TB SSD
Form Factor	1U	1U	1U	1U	1U
Management Ports	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port
Fixed I/O Ports	8 × SFP, 8 × GE (including 2 pairs Bypass port)	2 × SFP+, 8 × SFP, 16 × GE (including 2 pairs Bypass port)	2 × SFP+, 8 × SFP, 16 × GE (including 2 pairs Bypass port)	2 × SFP+, 8 × SFP, 16 × GE (including 2 pairs Bypass port)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot	N/A	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-S-F-4SFP+-A-IN IOC-S-F-8SFP+-A-IN IOC-S-F-8GE-B-A-IN	N/A	IOC-S-4SFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN IOC-S-2QSFP+-A-IN	IOC-S-4SFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN IOC-S-2QSFP+-A-IN	IOC-S-4SFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN IOC-S-2QSFP+-A-IN
Latency	<300 µs	<300 µs	<300 µs	<300 µs	<300 µs
Bypass Support (Default/Max.)	4/12	4/4	4/4	4/4	8/8
Power Supply	AC 100-240 V 50/60 Hz	AC 100~240V 50/60Hz	AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz
Maximum Power Consumption	60W 1 × AC power supply 2 × AC power supply	100W 1 × AC power supply 2 × AC power supply	100W 1 × AC power supply 2 × AC power supply	100W 2 × AC power supply 2 × DC power supply	280W 2 × AC power supply 2 × DC power supply
Dimension (WxDxH, mm)	17.3 × 13.4 × 1.7 in (440 × 340 × 44 mm)	17.2 × 17.2 × 1.7 in (436 × 437 × 44mm)	17.1 × 17.2 × 1.7 in (436 × 320 × 44mm. Not include expansion module)	17.1 × 17.2 × 1.7 in (436 × 320 × 44mm, Including power module handle)	17.1 × 21.3 × 1.7 in (436 × 542 × 44mm, Including power module handle)
Weight	10.0 lb (4.55 kg)	20.7 lb (9.4 kg)	20.9 lb (9.5kg, Including accessories and all packages)	26.0 lb (11.8kg, Including accessories and all packages)	32.6 lb (14.8kg, Including accessories and all packages)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	10%~95% (no dew)	10%~95% (no dew)	10%~95% (no dew)	10%~95% (no dew)

Specifications (Continued)

	S3900-IN	S3915-IN	S5500-IN
			
IPS Throughput [1]	25/40 Gbps	30 Gbps	45/75 Gbps
Maximum Concurrent Connections, TCP (Standard/with AEL) [2]	12 Million	15 Million	24 Million
New Connections per Second, HTTP [3]	380,000	380,000	550,000
Stoneshield	N/A	N/A	N/A
Virtual Systems (Default/ Max)	1/50	1/50	1/50
Storage [4]	1 TB SSD	1 TB SSD	1 TB SSD
Form Factor	1U	1U	1U
Management Ports	2 × USB port, 1 × MGT port, 1 × Console port, 2 × HA port (SFP+)	2 x USB Port, 1 × MGT port, 1 x Console port, 1 × HA port	2 x USB port, 1 × MGT port, 1 x Console port, 1 × HA port (SFP+)
Fixed I/O Ports	6 × SFP+, 16 × SFP, 8 × GE (including 2 pairs Bypass port)	2 × QSFP+, 16 × SFP+, 8 x GE (including 4 pairs Bypass port)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP+-A-IN IOC-S-2QS-FP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN	IOC-S-4SFP+-A-IN IOC-S-2QSFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN	IOC-S-4SFP+-A-IN IOC-S-2QSFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN
Latency	<300 µs	<300 µs	<300 µs
Bypass Support (Default/Max.)	4/4	8/8	8/8
Power Supply	DC -36~ -72 V AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz
Maximum Power Consumption	280W 2 × AC power supply 2 × DC power supply	280W 2 × AC power supply 2 × DC power supply	320W 2 × AC power supply 2 × DC power supply
Dimension (WxDxH, mm)	17.1 × 21.3 × 1.7 in (436 × 542 × 44mm. Including power module handle)	17.1 × 21.3 × 1.7 in (436 × 542 × 44mm. Including power module handle)	17.1 × 21.3 × 1.7 in (436 × 542 × 44mm)
Weight	32.6 lb (14.8kg, Including accessories and all packages)	32.6 lb (14.8kg, Including accessories and all packages)	32.6 lb (14.8kg, Including accessories and all packages)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10%~95% (no dew)	10%~95% (no dew)	10%~95% (no dew)

Module Options

Module	IOC-S-F-4SFP+-A-IN	IOC-S-F-8SFP+-A-IN	IOC-S-F-8GE-B-A-IN	IOC-S-4SFP+-A-IN
I/O Ports	4 × SFP+ Ports (for Front Panel)	8 × SFP+ Ports (for Front Panel)	8 × GE, including 4 bypass pairs (for Front Panel)	4 × SFP+, SFP+ module not included
Dimension	1U	1U	1U	1U
Weight	0.55 lb (0.25 kg)	0.62 lb (0.28 kg)	0.6 lb (0.27 kg)	2.09 lb (0.96 kg)

Module	IOC-S-2MM-BE-A-IN	IOC-S-2SM-BE-A-IN	IOC-S-2QSFP+-A-IN
I/O Ports	4 × SFP, MM bypass (2 pairs of bypass ports)	4 × SFP, SM bypass (2 pairs of bypass ports)	2 × QSFP+
Dimension	1U	1U	1U
Weight	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)

NOTES:

(1) IPS throughput data is obtained under HTTP traffic with all IPS rules being turned on. The data for S3900-IN/S5500-IN can be increased to 40/75 Gbps via additional IOC-S-2QSFP+-A-IN expansion module;

(2) Maximum concurrent connections are obtained under TCP traffic; and it can be upgraded with Additional Enhanced License (AEL);

(3) New Connections per Second are obtained under HTTP traffic with all IPS rules being turned off.

(4) 1TB storage for S1115-IN, S1200-IN, S1215-IN, S1900-IN, S2100-IN, S2115-IN, S2300-IN and S2700-IN is only available on devices equipped with dual AC power supplies; The actual available space is smaller and may vary depending on the operating system for management space reservation.

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R10. Results may vary based on StoneOS® version and deployment.

Version: EX-08.01-NIPS-V5.5-0925-EN-01