Hillstone S-Series Network Intrusion Prevention System (NIPS)

S600 / S1060 / S1560 / S2160 / S2660 / S3560 / S3860 / S5560

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. 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

Highlight

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.

Granular Reporting with User Targeted Viewpoints

Hillstone NIPS provides comprehensive visibility based on protocol, application, user and content. It can identify more than 3000 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.

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, upgrade NIPS devices deployed in different branches or locations, with a unified management policy across the network for maximum efficiency.

Key Features

Intrusion Prevention

- 8,000+ 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: 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

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, Overflow etc
- Real-time, online, malware behavior model database update

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
- 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

Anti-Virus

- Manual, automatic push or pull signature updates
- Flow-based Antivirus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP
- Compressed file virus scanning

Attack Defense

- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN Flood, DNS Query Flood defense
- ARP attack defense

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 140 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

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

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
- IP and domain whitelists

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 3,000 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

Quality of Service (QoS)

- 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, Anti-Virus, Access control, ND attack defense

VSYS

- System resource allocation to each VSYS
- CPU virtualization
- Non-root VSYS support firewall, IPSec VPN, SSL VPN, IPS, URL filtering
- VSYS monitoring and statistic

High Availability

- Redundant heartbeat interfaces
- Active/Active and Active/Passive
- 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, console
- Central Management: Hillstone Security Manager (HSM), web service APIs
- Two-factor authentication: username/password, HTTPS certificates file
- System Integration: SNMP, syslog, alliance partnerships
- 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.
- Language support: English

Logs and Reporting

- Logging facilities: local memory and storage, 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
- 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

CloudView

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

Product Specification

Model	S600	S1060	S1560	S2160	S2660	S3560	S3860	S5560
								
IPS throughput(1)	1 Gbps	3 Gbps	4 Gbps	10 Gbps	14 Gbps	16 Gbps	21 Gbps	50 Gbps
Maximum Concurrent Connections (TCP)(2)	0.6 Million	1 Million	1 Million	2 Million	2 Million	4 Million	4 Million	8 Million
New connections per second (TCP)(3)	9,000	35,000	41,000	92,000	120,000	150,000	200,000	485,000
Stoneshield	N/A	N/A	Yes	N/A	Yes	N/A	Yes	Yes
Storage	1T	1T	1T	1T	1T	1T	1T	1T
Form factor	1 U	1 U	1 U	1 U	1 U	2 U	2 U	2U
Management Ports	2×USB Port, 1× Consle Port	2×USB Port, 1× Consle Port	2×USB Port, 1× Consle Port	2×USB Port 2×MGT, 1× Consle Port	2×USB Port 2×MGT, 1× Consle Port	2×USB Port 2×MGT, 1× Consle Port	2×USB Port 2×MGT, 1× Consle Port	2×USB Port 2×MGT, 1× Consle Port
Fixed I/O Ports	4×GE	4×GE	4×GE	4×GE	4×GE	6×GE	6×GE	N/A
Available Slots for Extension Modules	1×Generic Slot	1×Generic Slot	1×Generic Slot	2×Generic Slot	2×Generic Slot	2×Generic Slot	2×Generic Slot	4×Generic Slot
Expansion Module Option	IOC-S-4GE-B-L, IOC-S-4SFP-L	IOC-S-4GE-B-L, IOC-S-4SFP-L	IOC-S-4GE-B-L, IOC-S-4SFP-L	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B IOC-S-2SFP+, IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B IOC-S-2SFP+, IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B IOC-S-2SFP+, IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B IOC-S-2SFP+, IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B	IOC-S-4GE-B-H, IOC-S-4SFP-H, IOC-S-8GE-B-H, IOC-S-8SFP-H, IOC-S-4SFP-B-H, IOC-S-2SFP+-H, IOC-S-4SFP+-H, IOC-S-2SFP+-B-H, IOC-S-4GE-4SFP-H,
Latency	<100 μs	<100 μs	<100 μs	<100 μs	<100 μs	<100 μs	<100 μs	<100 μs
Bypass Support (Default/Max.)	4/8	4/8	4/8	4/20	4/20	6/22	6/22	0/32
Power Supply	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz
Maximum Power Consumption	1×60W	1×60W	1×60W	250W Redundancy 1 + 1	250W Redundancy 1 + 1	350W Redundancy 1 + 1	350W Redundancy 1 + 1	350W Redundancy 1 + 1
Dimension (W×D×H, mm)	16.9 ×11.8×1.7 in (430×300×44mm)	16.9×11.8×1.7 in (430×300×44mm)	16.9×11.8×1.7 in (430× 300×44mm)	16.9×14.8×1.7 in (430×375×44mm)	16.9×14.8×1.7 in (430×375×44mm)	16.9×19.7×3.5 in (430×500×88mm)	16.9×19.7×3.5 in (430×500×88mm)	16.9×19.7×3.5 in (430×500×88mm)
Weight	14.3 lb (6.5kg)	14.3 lb (6.5kg)	14.3 lb (6.5kg)	22.0 lb (10kg)	22.0 lb (10kg)	35.3 lb (16kg)	35.3 lb (16kg)	35.3 lb (16kg)
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)	32-104 F (0-40 °C)	32-104 F (0-40 °C)	32-104 F (0-40 °C)
Relative Humidity	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)

Module Options

Module	IOC-S-4GE-B-L	IOC-S-4SFP-L	IOC-S-4GE-B	IOC-S-4SFP	IOC-S-8GE-B	IOC-S-8SFP	IOC-S-4GE-4SFP
I/O Ports	4×GE Bypass Ports	4×SFP Ports	4×GE Bypass Ports	4×SFP Ports	8×GE Bypass Ports	8×SFP Ports	4×GE and 4×SFP Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.22 lb (0.1kg)	0.22 lb (0.1kg)	0.33 lb (0.15kg)	0.33 lb (0.15kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)

Module	IOC-S-2SFP+	IOC-S-4SFP+	IOC-S-4SFP-B	IOC-S-2SFP+-B	IOC-S-4SFP+-B	IOC-S-4GE-B-H	IOC-S-4GE-4SFP-H
I/O Ports	2×SFP+ Ports	4×SFP+ Ports	4×SFP Bypass Ports	2×SFP+ Bypass Ports	4×SFP+ Bypass Ports	4×GE Bypass Ports	4×GE and 4×SFP Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.33 lb (0.15kg)	0.44 lb (0.2kg)	0.88 lb (0.4kg)	0.88 lb (0.4kg)	0.88 lb (0.4kg)	0.33 lb (0.15kg)	0.55 lb (0.25kg)

Module	IOC-S-8GE-B-H	IOC-S-8SFP-H	IOC-S-4SFP-H	IOC-S-2SFP+-H	IOC-S-4SFP+-H	IOC-S-4SFP-B-H	IOC-S-2SFP+-B-H
I/O Ports	8×GE Bypass Ports	8×SFP Ports	4×SFP Ports	2×SFP+ Ports	4×SFP+ Ports	4×SFP Bypass Ports	2×SFP+ Bypass Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.33 lb (0.15kg)	0.33 lb (0.15kg)	0.44 lb (0.2kg)	0.88 lb (0.4kg)	0.88 lb (0.4kg)

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R3. Results may vary based on StoneOS® version and deployment.

NOTES:(1) IPS Throughput data is obtained under HTTP traffic with all IPS rules being turned on; (2) Maximum Concurrent Connections are obtained under TCP traffic; (3) New Sessions are obtained under TCP traffic.

Version: EX-08.01-NIPS-V3.2.1-0919-EN-01