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**

**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/SCPF Port scan, ICMP sweep, TCP/UDP/SCPF/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, Stockstress, 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
- White lists to allow emails from trusted domains

**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

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)

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
## Module Options

### Module Options

<table>
<thead>
<tr>
<th>Model</th>
<th>S600</th>
<th>S1060</th>
<th>S1560</th>
<th>S2160</th>
<th>S2660</th>
<th>S3560</th>
<th>S3860</th>
<th>S5560</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS throughput</td>
<td>1 Gbps</td>
<td>3 Gbps</td>
<td>4 Gbps</td>
<td>10 Gbps</td>
<td>14 Gbps</td>
<td>16 Gbps</td>
<td>21 Gbps</td>
<td>50 Gbps</td>
</tr>
<tr>
<td>Maximum Concurrent Connections (TCP)</td>
<td>0.6 Million</td>
<td>1 Million</td>
<td>1 Million</td>
<td>2 Million</td>
<td>2 Million</td>
<td>4 Million</td>
<td>4 Million</td>
<td>8 Million</td>
</tr>
<tr>
<td>New connections per second (TCP)</td>
<td>9,000</td>
<td>35,000</td>
<td>41,000</td>
<td>92,000</td>
<td>120,000</td>
<td>150,000</td>
<td>200,000</td>
<td>485,000</td>
</tr>
<tr>
<td>StoneShield</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage</td>
<td>1T</td>
<td>1T</td>
<td>1T</td>
<td>1T</td>
<td>1T</td>
<td>1T</td>
<td>1T</td>
<td>1T</td>
</tr>
<tr>
<td>Form factor</td>
<td>1U</td>
<td>1U</td>
<td>1U</td>
<td>1U</td>
<td>2U</td>
<td>2U</td>
<td>2U</td>
<td>2U</td>
</tr>
<tr>
<td>Management Ports</td>
<td>2 × USB Port, 1 × Console Port</td>
<td>2 × USB Port, 1 × Console Port</td>
<td>2 × USB Port, 1 × Console Port</td>
<td>2 × USB Port, 1 × Console Port</td>
<td>2 × USB Port 2 × MagiC, 1 × Console Port</td>
<td>2 × USB Port 2 × MagiC, 1 × Console Port</td>
<td>2 × USB Port 2 × MagiC, 1 × Console Port</td>
<td>2 × USB Port 2 × MagiC, 1 × Console Port</td>
</tr>
<tr>
<td>Fixed I/O Ports</td>
<td>4 × GE</td>
<td>4 × GE</td>
<td>4 × GE</td>
<td>4 × GE</td>
<td>4 × GE</td>
<td>4 × GE</td>
<td>6 × GE</td>
<td>6 × GE</td>
</tr>
<tr>
<td>Available Slots for Extension Modules</td>
<td>1 × Generic Slot</td>
<td>1 × Generic Slot</td>
<td>2 × Generic Slot</td>
<td>2 × Generic Slot</td>
<td>2 × Generic Slot</td>
<td>2 × Generic Slot</td>
<td>4 × Generic Slot</td>
<td>N/A</td>
</tr>
<tr>
<td>Latency</td>
<td>&lt; 100 µs</td>
<td>&lt; 100 µs</td>
<td>&lt; 100 µs</td>
<td>&lt; 100 µs</td>
<td>&lt; 100 µs</td>
<td>&lt; 100 µs</td>
<td>&lt; 100 µs</td>
<td>&lt; 100 µs</td>
</tr>
<tr>
<td>Power Supply</td>
<td>AC 100-240V 50/60Hz</td>
<td>AC 100-240V 50/60Hz</td>
<td>AC 100-240V 50/60Hz</td>
<td>AC 100-240V 50/60Hz</td>
<td>AC 100-240V 50/60Hz</td>
<td>AC 100-240V 50/60Hz</td>
<td>AC 100-240V 50/60Hz</td>
<td>AC 100-240V 50/60Hz</td>
</tr>
<tr>
<td>Maximum Power Consumption</td>
<td>1 × 60W</td>
<td>1 × 60W</td>
<td>1 × 60W</td>
<td>250W Redundancy</td>
<td>250W Redundancy</td>
<td>350W Redundancy</td>
<td>350W Redundancy</td>
<td>350W Redundancy</td>
</tr>
<tr>
<td>Dimension (W×D×H, mm)</td>
<td>16.9 × 11.8 × 1.7 in (430×300×44mm)</td>
<td>16.9 × 11.8 × 1.7 in (430×300×44mm)</td>
<td>16.9 × 11.8 × 1.7 in (430×300×44mm)</td>
<td>16.9 × 11.8 × 1.7 in (430×300×44mm)</td>
<td>16.9 × 11.8 × 1.7 in (430×300×44mm)</td>
<td>16.9 × 11.8 × 1.7 in (430×300×44mm)</td>
<td>16.9 × 11.8 × 1.7 in (430×300×44mm)</td>
<td>16.9 × 11.8 × 1.7 in (430×300×44mm)</td>
</tr>
<tr>
<td>Weight</td>
<td>14.3 lb (6.5kg)</td>
<td>14.3 lb (6.5kg)</td>
<td>14.3 lb (6.5kg)</td>
<td>22.0 lb (10kg)</td>
<td>22.0 lb (10kg)</td>
<td>33.3 lb (15kg)</td>
<td>33.3 lb (15kg)</td>
<td>33.3 lb (15kg)</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>5-85% (no dew)</td>
<td>5-85% (no dew)</td>
<td>5-85% (no dew)</td>
<td>5-85% (no dew)</td>
<td>5-85% (no dew)</td>
<td>5-85% (no dew)</td>
<td>5-85% (no dew)</td>
<td>5-85% (no dew)</td>
</tr>
</tbody>
</table>

### Module Options

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O Ports</td>
<td>4 × GE Bypass Ports</td>
<td>4 × GE Bypass Ports</td>
<td>4 × GE Bypass Ports</td>
<td>8 × GE Bypass Ports</td>
<td>8 × GE Bypass Ports</td>
<td>4 × GE and 4 × SFP Ports</td>
<td>4 × GE and 4 × SFP Ports</td>
<td>4 × GE and 4 × SFP Ports</td>
</tr>
<tr>
<td>Dimension</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
</tr>
<tr>
<td>Weight</td>
<td>0.22 lb (0.1kg)</td>
<td>0.22 lb (0.1kg)</td>
<td>0.33 lb (0.15kg)</td>
<td>0.33 lb (0.15kg)</td>
<td>0.55 lb (0.25kg)</td>
<td>0.55 lb (0.25kg)</td>
<td>0.55 lb (0.25kg)</td>
<td>0.55 lb (0.25kg)</td>
</tr>
</tbody>
</table>

### Module Options

<table>
<thead>
<tr>
<th>Model</th>
<th>IOC-S-2SFP+</th>
<th>IOC-S-4SFP+</th>
<th>IOC-S-2SFP+</th>
<th>IOC-S-4SFP+</th>
<th>IOC-S-2SFP+</th>
<th>IOC-S-4SFP+</th>
<th>IOC-S-4GE-B-H</th>
<th>IOC-S-4GE-FSP-H</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O Ports</td>
<td>2 × SFP+ Ports</td>
<td>4 × SFP+ Ports</td>
<td>4 × SFP+ Ports</td>
<td>2 × SFP+ Ports</td>
<td>4 × SFP+ Ports</td>
<td>4 × SFP+ Ports</td>
<td>4 × GE Bypass Ports</td>
<td>4 × GE and 4 × SFP Ports</td>
</tr>
<tr>
<td>Dimension</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
</tr>
<tr>
<td>Weight</td>
<td>0.33 lb (0.15kg)</td>
<td>0.44 lb (0.2kg)</td>
<td>0.88 lb (0.4kg)</td>
<td>0.88 lb (0.4kg)</td>
<td>0.88 lb (0.4kg)</td>
<td>0.88 lb (0.4kg)</td>
<td>0.88 lb (0.4kg)</td>
<td>0.88 lb (0.4kg)</td>
</tr>
</tbody>
</table>

### Module Options

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O Ports</td>
<td>8 × GE Bypass Ports</td>
<td>8 × SFP Ports</td>
<td>8 × SFP Ports</td>
<td>2 × SFP+ Ports</td>
<td>2 × SFP+ Ports</td>
<td>2 × SFP+ Ports</td>
<td>2 × SFP+ Ports</td>
<td>2 × SFP+ Ports</td>
</tr>
<tr>
<td>Dimension</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
<td>1U (Occupies 1 generic slot)</td>
</tr>
<tr>
<td>Weight</td>
<td>0.55 lb (0.25kg)</td>
<td>0.55 lb (0.25kg)</td>
<td>0.33 lb (0.15kg)</td>
<td>0.33 lb (0.15kg)</td>
<td>0.33 lb (0.15kg)</td>
<td>0.44 lb (0.2kg)</td>
<td>0.88 lb (0.4kg)</td>
<td>0.88 lb (0.4kg)</td>
</tr>
</tbody>
</table>

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R3. 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.