Hillstone’s T-Series intelligent Next-Generation Firewall (iNGFW) uses three key technologies to detect advanced attacks and provide continuous threat defense for today’s networks. First, it uses statistical clustering to detect unknown malware, leveraging the patented Hillstone Advanced Threat Detection engine (ATD). Second, it uses behavioral analytics to detect anomalous network behavior, which is based on the Hillstone Abnormal Behavior Detection engine (ABD). Finally, it leverages the Hillstone threat correlation analysis engine to correlate threat events detected by disparate engines – including ATD, ABD, Sandbox and other traditional signature-based threat detection technologies – along with context information to identify advanced threats.

With deep detection and threat analytics capabilities, Hillstone’s iNGFW provides customers with comprehensive visibility of the network risk status, as well as threat details of each host. The Hillstone iNGFW provides administrators with forensic information from different tools and paths, in order to drill down to the root cause of an attack. In addition, the Hillstone iNGFW empowers the administrator with powerful mitigation functions, which can buy time for administrators to examine the forensic data, make an informed decision about the authenticity of the attack, and minimize the business damage.
### Product Highlights

#### Unknown Malware Detection
Hillstone has built a proprietary engine that has analyzed close to a million "known" malware samples. Each sample has been classified and characterized based on multiple dimensions that describe its actions, assets and attributes. In a production environment, when new malware is encountered, it is also analyzed, characterized and classified. Then it is compared to the database of known malware samples that have already been analyzed. The closer the unknown sample matches a known sample - the higher the confidence level that it is a variant of a known malware sample. This process is called "statistical clustering" and provides an accurate method for identifying new malware.

#### Abnormal Behavior Detection
Hillstone's Abnormal Behavior engine continuously monitors the network to learn what normal network traffic looks like for that particular day, time, and month; providing alerts when network activity exceeds calculated thresholds. It uses a 50+ dimensional array to calculate normal network traffic from layer L4-L7, called “behavior modeling.” In addition, it has been trained with real hacking tools to ensure that it will readily recognize malicious activity. These techniques limit false positives and provide the user with multiple opportunities to stop an attack.

#### Rich Forensic Analysis
Hillstone delivers a new way of visualizing and analyzing attacks. Every action taken by a potentially malicious code is automatically linked to steps within the "Kill Chain." It is complemented with rich forensic information that enables the security analyst to determine the origin of the attack, the severity of the attack, and the methodology employed. Hillstone also provides packet capture files, which, when combined with syslog and traffic logs, provide the administrator with a wealth of ancillary information. In addition, user data such as websites visited, applications used, and the risk level of the applications, bring the exploits into sharp focus. Most importantly, Hillstone identifies the exact firewall policy that allowed the attacker to get through the firewall.

#### Preemptive Mitigation
In addition to the ability to make a policy change to prevent an attack, Hillstone has built-in several automatic mitigation features. These features consist of pre-defined templates that automatically slow-down or block an attack if suspicious behavior is detected. The administrator can modify the templates to limit the bandwidth or the number of sessions available to the attacker. He can also adjust the constraints he places on network resources based on the type of attack and the severity level. In cases where the attack is critical and the confidence level is high, mitigation can include a complete blockage of all network resources. And, if a template does not exist or is not active, the administrator can quickly set up a temporary mitigation for that event.

### Features

#### 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
Detect C&C attack using Domain Generation Algorithm (DGA)
Real-time, online, abnormal behavior model database update

#### Threat Visibility and Mitigation
Network risk index, critical assets and host risk status, host and threat risk severity and certainty
Kill chain mapping of threat events on each host
Threat forensic including threat analysis, knowledge base, history and PCAP
Predefined and customized mitigation rules
Support threat whitelist

#### Network Services
Dynamic routing (OSPF, BGP, RIPv2)
Static and Policy routing
Route controlled by application
Built-in DHCP, NTP, DNS Server and DNS proxy
Tap mode – connects to SPAN port
Interface modes: sniffer, port aggregated, loopback, VLANs (B02.1Q and Trunking)

#### L2/L3 switching & routing
Virtual wire (Layer 1) transparent inline deployment

#### Firewall
Operating modes: NAT/route, transparent (bridge), and mixed mode
Policy objects: predefined, custom, and object grouping
Security policy based on application, role and geo-location
Application Level Gateways and session support:
MSRPC, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323 NAT and ALG support: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
NAT configuration: per policy and central NAT table
VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
Global policy management view
Security policy redundancy inspection, policy group, policy configuration rollback
Policy Assistant for easy detailed policy deployment
Policy analyzing and invalid policy cleanup
Comprehensive DNS policy
Schedules: one-time and recurring

#### Intrusion Prevention
Protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
IPS Actions: default, 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/ICMP port scan, ICMP sweep, TCP/UDP/ICMP/ICMP session flooding (source/destination)
Active bypass with bypass interfaces
Predefined prevention configuration

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

#### Attack Defense
Abnormal protocol attack defense
Anti-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

SSL Decryption
Application identification for SSL encrypted traffic
IPS enablement for SSL encrypted traffic
AV enablement for SSL encrypted traffic
URL filter for SSL encrypted traffic
SSL Encrypted Traffic whitelist
SSL proxy offload mode

Endpoint Identification and Control
Support to identify endpoint IP, endpoint quantity, on-line time, off-line time, and on-line duration
Support 10 operational systems
Support query based on IP, endpoint quantity, control policy and status etc.
Support the identification of accessed endpoints quantity across layer 3, logging and interference on overun IP
Redirect page display after custom interference operation
Supports blocking operations on overun IP

Data Security
File transfer control based on file type, size and name
File protocol identification, including HTTP, FTP, SMTP and POP3
File signature and suffix identification for over 100 file types
IM identification and network behavior audit
Filter files transmitted by HTTPS using SSL Proxy

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, reset session, monitor, traffic shaping Identify and control cloud applications in the cloud
Provide multi-dimensional monitoring and statistics for cloud applications, 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/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
Automatic expiration cleanup and manual cleanup of user used traffic

Server Load balancing
Weighted hashing, weighted least-connection, and weighted round-robin
Session persistence, session persistence and session status monitoring
Server health check, session monitoring and session protection

Link Load balancing
Bi-directional link load balancing
Outbound link load balancing includes policy based routing, ECMP and weighted, embedded IPS routing and dynamic detection
Inbound link load balancing supports SmartDNS and dynamic detection
Automatic link switching based on bandwidth, latency, jitter, connectivity, application etc.
Link health inspection with ARP, PING, and DNS

VPN
IPSec VPN
- IPSec Phase 1 mode: aggressive and main ID protection mode
- Peer acceptance options: any ID, specific ID, ID in dialup user group
- Supports IKEv1 and IKEv2 (RFC 4306)
- Authentication method: certificate and pre-shared key
- IKE mode configuration support (as server or client)
- DHCHP over IPSec
- Configurable IKE encryption key expiry, NAT traversal keep alive frequency
Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
Phase 1/Phase 2 Proposal authentication: MDS, SHA1, SHA256, SHA384, SHA512
Phase 1/Phase 2 Diffie-Hellman support: 1,2,5
- XAuth as server and for dialup users
- Dead peer detection
- Replay detection
- Autokey keep-alive for Phase 2 SA
IPSEC VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design)
IPSEC VPN configuration options: route-based or policy based
IPSEC VPN deployment modes: gateway-to-gateway, full mesh, hub-and-spoke, redundant tunnel, VPN termination in transparent mode
One time login prevents concurrent logins with the same username
SSL portal concurrent users limiting
SSL VPN port forwarding module encrypts client data and sends the data to the application server
Supports clients that run iOS, Android, and Windows XP/Vista including 64-bit Windows OS
Host integrity checking and OS checking prior to SSL tunnel connections
MAC host check per portal
Cache cleaning option prior to ending SSL VPN session
L2TP client and server mode, L2TP over IPSec, and GRE over IPSec
View and manage IPSec and SSL VPN connections
pnpVPN
IPv6
Management over IPv6, IPv6 logging and HA IPv6 tunneling, DNS64/NAT64 etc
IPv6 routing including static routing, policy routing, IDIS, RSVP, OSPFv3 and BGP4+
IP, Application identification, Anti-Virus, Access control, ND attack defense, iQoS
Track address detection

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

User and Device Identity
Local user database
Remote user authentication: TACACS+, LDAP, Radius, Active
Single-sign-on: Windows AD
2-factor authentication: 3rd party support, integrated token server with physical and SMS
User and device-based policies
User group synchronization based on AD and LDAP
Support for 80.1x, SSO Proxy
WebAuth page customization
Interface based Authentication
Agentless ADSSO (AD Polling)
Use authentication synchronization based on SSO-monitor
Support MAC-based user authentication

Administration
Management access: HTTP/HTTPS, SSH, telnet, console
Central Management: Hillstone Security Manager (HSM), web service APIs
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
Language support: English

Logs & Reporting
Logging facilities: local memory and storage (if available), 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, URL etc.
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
Three predefined reports: Security, Flow, and network reports
User defined reporting
Reports can be exported in PDF, Word and HTML via Email and FTP

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

www.hillstonenet.com
### Product Specification

<table>
<thead>
<tr>
<th>Specification</th>
<th>SG-6000-T1860</th>
<th>SG-6000-T2860</th>
<th>SG-6000-T3860</th>
<th>SG-6000-T5060</th>
<th>SG-6000-T5860</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW Throughput (11)</td>
<td>8Gbps</td>
<td>10Gbps</td>
<td>20Gbps</td>
<td>25Gbps</td>
<td>40Gbps</td>
</tr>
<tr>
<td>IPS Throughput (12)</td>
<td>3Gbps</td>
<td>4Gbps</td>
<td>8Gbps</td>
<td>12Gbps</td>
<td>18Gbps</td>
</tr>
<tr>
<td>AV Throughput (13)</td>
<td>1.6Gbps</td>
<td>2Gbps</td>
<td>6Gbps</td>
<td>7Gbps</td>
<td>10Gbps</td>
</tr>
<tr>
<td>IPSec Throughput (14)</td>
<td>3Gbps</td>
<td>3.8Gbps</td>
<td>12Gbps</td>
<td>15Gbps</td>
<td>28Gbps</td>
</tr>
<tr>
<td>IMIX Throughput (16)</td>
<td>1.6Gbps</td>
<td>2.1Gbps</td>
<td>8.2Gbps</td>
<td>10.9Gbps</td>
<td>17.4Gbps</td>
</tr>
<tr>
<td>NGFW Throughput (1)</td>
<td>1Gbps</td>
<td>1.5Gbps</td>
<td>5Gbps</td>
<td>8Gbps</td>
<td>12Gbps</td>
</tr>
<tr>
<td>Threat Protection Throughput (17)</td>
<td>600Mbps</td>
<td>900Mbps</td>
<td>2.5Gbps</td>
<td>4Gbps</td>
<td>6Gbps</td>
</tr>
<tr>
<td>New Sessions (9-10)</td>
<td>80K</td>
<td>100K</td>
<td>250K</td>
<td>300K</td>
<td>450K</td>
</tr>
<tr>
<td>Maximum Concurrent Sessions</td>
<td>1.5M</td>
<td>3M</td>
<td>4M</td>
<td>5M</td>
<td>6M</td>
</tr>
<tr>
<td>IPSec Tunnel Number</td>
<td>6,000</td>
<td>10,000</td>
<td>20,000</td>
<td>20,000</td>
<td>20,000</td>
</tr>
<tr>
<td>SSL/VPN Users (Default/Max)</td>
<td>8/4,000</td>
<td>8/6,000</td>
<td>128/10,000</td>
<td>128/10,000</td>
<td>128/10,000</td>
</tr>
<tr>
<td>Virtual Systems (Default/Max)</td>
<td>1/100</td>
<td>1/100</td>
<td>250</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>Integrated I/O</td>
<td>6 x GE, 4 x SFP</td>
<td>6 x GE (1 pair bypass port), 4 x SFP, 2 x SFP+</td>
<td>2 x GE, 4 x SFP</td>
<td>2 x GE, 4 x SFP</td>
<td>2 x GE, 4 x SFP</td>
</tr>
<tr>
<td>Maximum I/O</td>
<td>26 x GE</td>
<td>26 x GE, 2 x 10GE</td>
<td>22 x GE, 4 x 10GE</td>
<td>38 x GE, 8 x 10GE</td>
<td>38 x GE, 16 x 10GE</td>
</tr>
<tr>
<td>Expansion Modules</td>
<td>2 x Generic Slot</td>
<td>2 x Generic Slot</td>
<td>4 x Generic Slot</td>
<td>4 x Generic Slot</td>
<td>4 x Generic Slot</td>
</tr>
<tr>
<td>Management Ports</td>
<td>1 x Console Port, 1 x HA, 1 x MGT, 1 x USB 2.0, 1 x AUX Port</td>
<td>1 x Console Port, 1 x AUX Port, 1 x USB 2.0 Port, 1 x HA, 1 x MGT</td>
<td>1 x Console Port, 1 x AUX Port, 1 x USB 2.0 Port, 2 x HA, 1 x MGT</td>
<td>1 x Console Port, 1 x AUX Port, 1 x USB 2.0 Port, 2 x HA, 1 x MGT</td>
<td>1 x Console Port, 1 x AUX Port, 1 x USB 2.0 Port, 2 x HA, 1 x MGT</td>
</tr>
<tr>
<td>Maximum Power Consumption</td>
<td>1 x 150W Redundancy 1 + 1</td>
<td>1 x 150W Redundancy 1 + 1</td>
<td>2 x 450W Redundancy 1 + 1</td>
<td>2 x 450W Redundancy 1 + 1</td>
<td>2 x 450W Redundancy 1 + 1</td>
</tr>
<tr>
<td>Storage</td>
<td>480GB SSD (960GB SSD Optional)</td>
<td>480GB SSD (960GB SSD Optional)</td>
<td>Dual Storage: 120G (480G or 960G SSD Optional) + 480GB SSD (960GB SSD Optional)</td>
<td>Dual Storage: 120G (480G or 960G SSD Optional) + 480GB SSD (960GB SSD Optional)</td>
<td>Dual Storage: 120G (480G or 960G SSD Optional) + 1T HDD (960GB SSD Optional)</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>
</tr>
<tr>
<td>Dimension (W×D×H, mm)</td>
<td>436 x 366 x 44</td>
<td>436 x 366 x 44</td>
<td>436 x 366 x 44</td>
<td>436 x 366 x 44</td>
<td>436 x 366 x 44</td>
</tr>
<tr>
<td>Weight</td>
<td>12.3 lb (5.6kg)</td>
<td>12.3 lb (5.6kg)</td>
<td>34.2 lb (15.5kg)</td>
<td>34.8 lb (15.8kg)</td>
<td>34.8 lb (15.8kg)</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>10-95% (no dew)</td>
<td>10-95% (no dew)</td>
<td>10-95% (no dew)</td>
<td>10-95% (no dew)</td>
<td>10-95% (no dew)</td>
</tr>
</tbody>
</table>

### Module Options

<table>
<thead>
<tr>
<th>Specification</th>
<th>IOD-8GE-M</th>
<th>IOD-8SFPM</th>
<th>IOD-4GE-B-M</th>
<th>IOD-2SFPM+</th>
<th>IOD-4XFP</th>
<th>IOD-4SFPM</th>
<th>IOD-8SFPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>8GE Extension Module</td>
<td>8SFPM Extension Module</td>
<td>4GE Bypass Extension Module</td>
<td>2SFPM+ Extension Module</td>
<td>4XFP Extension Module</td>
<td>4SFPM Extension Module</td>
<td>8SFPM Extension Module</td>
</tr>
<tr>
<td>I/O Ports</td>
<td>8 x GE</td>
<td>8 x SFP, SFP module not included</td>
<td>4 x GE Bypass (2 pair bypass ports)</td>
<td>2 x SFP+, SFP+ module not included</td>
<td>4 x XFP, XFP module not included</td>
<td>4 x SFP+, SFP+ module not included</td>
<td>8 x SFP+, SFP+ module not included</td>
</tr>
<tr>
<td>Dimension</td>
<td>1/1U (Occupies 1 generic slots)</td>
<td>1/1U (Occupies 1 generic slots)</td>
<td>1/1U (Occupies 1 generic slots)</td>
<td>1 U (Occupies 2 generic slots)</td>
<td>1 U (Occupies 2 generic slots)</td>
<td>1 U (Occupies 2 generic slots)</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>1.8 lb (0.8kg)</td>
<td>2.0 lb (0.9kg)</td>
<td>1.8 lb (0.8kg)</td>
<td>0.7 lb (0.3kg)</td>
<td>2.0 lb (0.9kg)</td>
<td>1.5 lb (0.7kg)</td>
<td>1.5 lb (0.7kg)</td>
</tr>
</tbody>
</table>

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R7. Results may vary based on StoneOS version and deployment.

NOTES: (1) FW throughput data is obtained under single-stack UDP traffic with 1518-byte packet size; (2) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on; (3) AV throughput data is obtained under HTTP traffic with file attachment; (4) IPSec throughput data is obtained under Preeshare Key AES256+SHA-1 configuration and 1400-byte packet size packet; (5) IMIX throughput data is obtained under UDP traffic mix (8 byte : 512 byte : 1518 byte = 5:7:1); (6) NGFW throughput data is obtained under 64 Kbytes HTTP traffic with application control and IPS enabled; (7) Threat protection throughput data is obtained under 64 Kbytes HTTP traffic with application control, IPS, AV, URL filtering, ABD and ATD enabled; (8) New Sessions/s is obtained under TCP traffic.

Version: EX-08.01-IKGFV-5.5R7-0619-EN-01

www.hillstonenet.com