

# Hillstone T-Series Intelligent Next-Generation Firewall

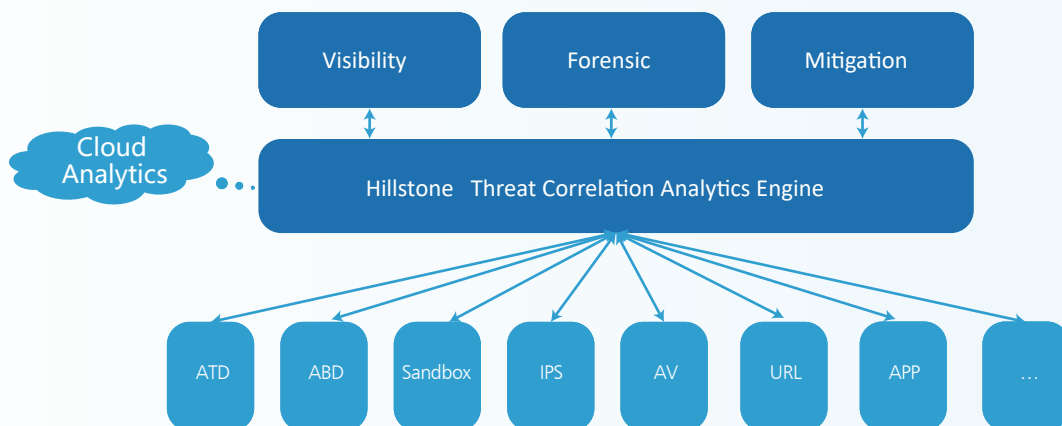


T1860 / T2860 / T3860 / T5060 / T5860



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.

### 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.

### 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.

### 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
- 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

### 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 (802.1Q 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: MSRCP, 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 holding
- Global policy management view
- Security policy redundancy inspection
- Schedules: one-time and recurring

### Intrusion Prevention

- Up to 8000+ signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia <sup>(1)</sup>
- 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/SCTP port scan, ICMP sweep, TCP/UDP/SCIP/ICMP session flooding (source/destination)
- Active bypass with bypass interfaces
- Predefined prevention configuration

### Anti-Virus

- 4 million Antivirus signatures, 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

### 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

### IP Reputation

- Botnet server IP blocking with global IP reputation database

### 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

- Support to identify endpoint IP, endpoint quantity, on-line time, off-line time, and on-line duration
- Support 10 operation systems
- Support query based on IP and endpoint quantity

### File Transfer Control

- File transfer control based on file name, type and size
- File protocol identification, including HTTP, HTTPS, FTP, SMTP, POP3 and SMB protocols
- File signature and suffix identification for over 100 file types

### 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/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

### Server Load balancing

- Weighted hashing, weighted least-connection, and weighted round-robin
- Session protection, session persistence and session status monitoring

### Link Load balancing

- Bi-directional link load balancing
- Outbound link load balancing includes policy based routing, ECMP and weighted, embedded ISP 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
- Server health check, session monitoring and session protection

### 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)
  - DHCP 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: MD5, SHA1, SHA256, SHA384, SHA512

- Phase 1/Phase 2 Diffie-Hellman support: 1,2,5
- XAuth as server mode 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 protocols, static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, 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

### 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 802.1X, SSO Proxy





### 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 via Email and FTP

## Product Specification

| Specification                   | SG-6000-T1860   | SG-6000-T2860   | SG-6000-T3860   | SG-6000-T5060   | SG-6000-T5860  |
|---------------------------------|---|---|---|---|--|
|                                 |  |  |  |                                |                               |
| FW Throughput <sup>(2)</sup>    | 8Gbps   | 10Gbps  | 20Gbps  | 25Gbps  | 40Gbps   |
| IPS Throughput <sup>(3)</sup>   | 3Gbps   | 4Gbps   | 8Gbps   | 12Gbps  | 18Gbps   |
| AV Throughput <sup>(4)</sup>    | 1.6Gbps   | 2Gbps   | 6Gbps   | 7Gbps   | 10Gbps   |
| IPSec Thoughtput <sup>(5)</sup> | 3Gbps   | 3.8Gbps   | 12Gbps  | 15Gbps  | 28Gbps   |
| New Sessions/s <sup>(6)</sup>   | 80K   | 100K  | 250K  | 300K  | 450K   |
| IPSec Tunnel Number             | 6,000   | 10,000  | 20,000  | 20,000  | 20,000   |
| SSL VPN Users (Default/Max)     | 8/4,000   | 8/6,000   | 128/10,000  | 128/10,000  | 128/10,000   |
| Maximum Concurrent Sessions     | 1.5M  | 3M  | 4M  | 5M  | 6M   |
| Integrated I/O                  | 6 × GE, 4 × SFP   | 6 × GE(1 pair bypass port), 4 × SFP, 2 × SFP+                                     | 2 × GE, 4 × SFP   | 2 × GE, 4 × SFP   | 2 × GE, 4 × SFP  |
| Maximum I/O                     | 26 × GE   | 26 × GE, 2 × 10GE   | 22 × GE, 4 × 10GE   | 38 × GE, 8 × 10GE   | 38 × GE, 8 × 10GE  |
| Expansion Modules               | 2 × Generic Slot  | 2 × Generic Slot  | 2 × Generic Slot  | 4 × Generic Slot  | 4 × Generic Slot   |
| Expansion Module Option         | IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M  | IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M  | IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-2XFP-Lite-M                               | IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+, IOC-2XFP-Lite-M (only supported at Slot-3/4), | IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+, IOC-2XFP-Lite-M (only supported at Slot-3/4) |
| Management Ports                | 1 × Console Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port                      | 1 × Console Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port                      | 1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT                 | 1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT   | 1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT  |
| Maximum Power Consumption       | 1 × 150w Redundancy 1 + 1   | 1 × 150w Redundancy 1 + 1   | 2 × 450W Redundancy 1 + 1   | 2 × 450W Redundancy 1 + 1   | 2 × 450W Redundancy 1 + 1  |
| Storage                         | 480G SSD (960G SSD Optional)  | 480G SSD (960G SSD Optional)  | Dual Storage: 120G (480G or 960G SSD Optional) + 480G SSD (960G SSD Optional)     | Dual Storage: 120G (480G or 960G SSD Optional) + 480G SSD (960G SSD Optional)                                     | Dual Storage: 120G (480G or 960G SSD Optional) + 1T HDD (960G SSD Optional)                                      |
| Power Supply                    | AC 100~240V 50/60Hz DC -40~-60V   | AC 100~240V 50/60Hz DC -40~-60V   | AC 100-240V 50/60Hz DC -40 ~ -60V   | AC 100-240V 50/60Hz DC -40 ~ -60V   | AC 100-240V 50/60Hz DC -40 ~ -60V  |
| Dimension (W × D × H)           | 1U 17.2 × 14.4 × 1.7 in (436 × 366 × 44 mm)                                       | 1U 17.2 × 14.4 × 1.7 in (436 × 366 × 44 mm)                                       | 2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)                                      | 2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)  | 2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)   |
| Weight                          | 12.3 lb (5.6KG)   | 12.3 lb (5.6KG)   | 34.2 lb (15.5KG)  | 34.8 lb (15.8 KG)   | 34.8 lb (15.8 KG)  |
| 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%  | 10-95%  | 10-95%  | 10-95%  | 10-95%   |

## Module Options

| Specification | IOC-8GE-M   | IOC-8SFP-M  | IOC-4GE-B-M   | IOC-2XFP-Lite-M   | IOC-4XFP   | IOC-4SFP+   | IOC-8SFP+   |
|---------------|---|---|---|---|--|---|---|
|               |  |  |  |  |  |  |  |
| Name          | 8 GE Extension Module   | 8SFP Extension Module   | 4GE Bypass Extension Module   | 2XFP Extension Module   | 4XFP Extension Module  | 4SFP+ Extension Module  | 8SFP+ Extension Module  |
| I/O Ports     | 8 × GE  | 8 × SFP, SFP module not included  | 4 × GE Bypass (2 pair bypass ports)   | 2 × XFP, XFP module not included  | 4 × XFP, XFP module not included   | 4 × SFP+, SFP+ module not included  | 8 × SFP+, SFP+ module not included  |
| Dimension     | ½ U (Occupies 1 generic slots)  | ½ U (Occupies 1 generic slot)   | ½ U (Occupies 1 generic slot)   | ½ U (Occupies 1 generic slot)   | 1 U (Occupies 2 generic slots)   | 1 U (Occupies 2 generic slots)  | 1 U (Occupies 2 generic slots)  |
| Weight        | 1.8 lb (0.8kg)  | 2.0 lb (0.9kg)  | 1.8 lb (0.8kg)  | 2.0 lb (0.9kg)  | 2.0 lb (0.9kg)   | 1.5 lb (0.7kg)  | 1.5 lb (0.7kg)  |

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R4. Results may vary based on StoneOS® version and deployment.

NOTES: (1)The number of IPS signatures supported varies for each platform based on its hardware capability; (2) FW Throughput data is obtained under single-stack UDP traffic with 1518-byte packet size.(3) IPSec throughput data is obtained under Preshare Key AES256+SHA-1 configuration and 1400-byte packet size packet; (4) AV throughput data is obtained under HTTP traffic with file attachment; (5) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on; (6) New Sessions/s is obtained under TCP traffic.