

# Hillstone T-Series Intelligent Next-Generation Firewall

T3860 / T5060 / T5860



According to the latest research 66 percent of security breaches go undetected for 7-8 months. And, more than 85 percent of breaches originate from the web with drive-by downloads being the top web threat. This implies two things: First, a user does not have to click on anything to become infected with malware; and second, all organizations have infected hosts inside their network.

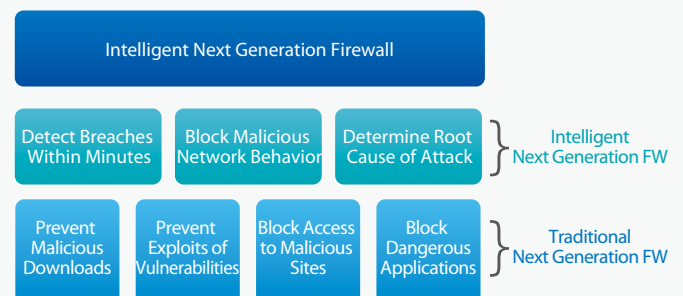
Hillstone's T-Series intelligent Next-Generation Firewall (iNGFW) is an application-aware firewall that continuously monitors the network. It can identify attacks on all operating systems, applications, devices and browsers. It provides visibility into every stage of an attack and it can detect security breaches within minutes/seconds. It prioritizes hosts with the greatest security risks and provides contextual information about the threat. Security administrators can drill-down into the attack, including packet captures, to analyze all threat details.

Hillstone's T-Series is designed for mid to large sized enterprises that need advanced levels of security, enhanced visibility, and continuous network uptime.

## Product Highlights

### Continuous Threat Defense

Hillstone's T-Series intelligent Next Generation Firewall (iNGFW) uses three key technologies to provide continuous threat defense. First, it uses statistical clustering to detect security breaches in near real-time. It prioritizes hosts with the greatest security risks and provides contextual information about the attack. Second, it uses behavioral analytics to detect anomalous network behavior. It provides visibility into every stage of an attack and gives the user multiple opportunities to stop the attack. Finally, it provides forensic analysis so that the user can determine the root cause of the attack. This allows an administrator to make policy changes to prevent similar incursions into his network.



### Statistical Clustering

Hillstone's T-Series closes the gap from initial compromise to detection. It employs a proprietary statistical clustering

algorithm that can quickly detect variants of known malware. Instead of searching for explicit signatures, it analyzes the behavior of malware and looks for recurring combinations of actions that are strongly related to known malware. When a close match is detected the system will send an alert and provide a complete description of the malware including packet captures. It also provides a confidence level and a severity level so that the administrator can take remedial action.

## Behavioral Analytics

Hillstone's T-Series provides visibility into every stage of an attack. It uses machine learning to establish a baseline of normal network activity and it uses big data analytics and mathematical modeling to detect anomalous network behavior that represents attacks at multiple stages in the attack lifecycle. This information is displayed on an intuitive dashboard and provides the user with multiple opportunities to stop the attack. Multiple mitigation technologies are built into the display so that the administrator can quickly limit potential damage while he investigates the abnormal traffic.

## Forensic Analysis

Hillstone's T-Series provides a wealth of evidence that helps an administrator understand the root cause of the attack. Reports and logs provide an audit trail of the progression of attacks from initial compromise to the exfiltration of data. Hosts are prioritized by security risk and assigned a risk factor. The threats that contributed to the risk factor can be examined along with a detailed description of each attack, a confidence level, and packet captures.

## Granular Application Control

Hillstone T-Series firewalls provide fine-grained control of web

applications regardless of port, protocol, or evasive action. It can identify and prevent potential threats associated with high-risk applications while providing policy-based control over applications, users, and user-groups. Policies can be defined that guarantee bandwidth to mission-critical applications while restricting or blocking inappropriate or malicious applications. Applications are classified by: name, category, subcategory, technology and risk. Policies can be created using one or more of these classifications to fine-tune permissible applications for selected users and groups. Policy based routing and bandwidth management can also be created for users/groups based on time of day and application attributes. In addition, selected features within an application (e.g., games, file sharing) can be blocked or bandwidth managed by user/group, time of day, and other criteria.

## Network Risk Index

Hillstone's patented network risk index quantifies the health status of your network. It uses threat information and host risk status to calculate the current risk associated with your network. It provides a multi-dimensional real-time assessment of your network's availability, risk factors, and developing threats. An intuitive dashboard allows IT to make timely security policy adjustments to mitigate threats and maintain network uptime.

## Superior User Experience

Hillstone's Intelligent Next Generation Firewall provides visibility and control of: network applications, network traffic, users and groups, bandwidth utilization, malicious activity, abnormal behavior, risk factors, developing threats and many more network and security attributes. It provides extensive tools for monitoring, reporting, logging, provisioning, and operations management.

## Features

### 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 – connect to SPAN port
- IPv6 Support: Mgt. over IPv6, IPv6 routing protocols, IPv6 tunneling, IPv6 logging and HA
- 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
- 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 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
- Schedules: one-time and recurring
- QoS Traffic Shaping:
  - 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
- Virtual Firewall: Up to 250 vSYS load balanced firewalls
- Load balancing:
  - Weighted hashing, weighted least-connection, and weighted round-robin
  - Session protection, session persistence and session status monitoring
  - Bidirectional 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 and latency
- 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)
  - 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
- SSL VPN tunnel mode 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

## User and Device Identity

- Local user database
- Remote user authentication: LDAP, Radius, Active Directory
- Single-sign-on: Windows AD
- 2-factor authentication: 3rd party support, integrated token server with physical and SMS
- User and device-based policies

## IPS

- 7,000+ signatures, 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/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination)
- Active bypass with bypass interfaces
- Provides predefined template of defense configuration
- Predefined prevention configuration

## Threat Protection

- Breach Detection
  - Near real-time breach detection (seconds/minutes)
  - Detailed description and severity of malware closely resembling attack
  - Pcap files and log files provide corroborating evidence
  - Confidence level provides certainty of attack
- Network Behavior Analysis
  - L3-L7 baseline traffic compared to real-time traffic to reveal anomalous network behavior

- Built-in mitigations technologies include: session limits, bandwidth limits and blocking
- Graphical depiction of anomalous behavior compared to baseline and upper and lower thresholds
- Network Risk Index quantifies the threat level of the network based on the aggregate host index.
- Host Risk Index quantifies the host threat level based on attack severity, detection method, and confidence level.
- Over 1.3 million AV signatures
- Botnet server IP blocking with global IP reputation database
- Flow-based Antivirus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP
- 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
- Proxy avoidance prevention: proxy site category blocking, rate URLs by domain and IP address, block redirects from cache & translation sites, proxy avoidance application blocking, proxy behavior blocking (IPS)
- Inspect SSL encrypted traffic.

## 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

## High Availability

- Redundant heartbeat interfaces
- 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




## 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
- 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

## Product Specification

Specification	SG-6000-T3860	SG-6000-T5060	SG-6000-T5860
			
FW Throughput	10Gbps	20Gbps	40Gbps
IPS Throughput <sup>(1)</sup>	6Gbps	12Gbps	18Gbps
AV Throughput <sup>(2)</sup>	4Gbps	7Gbps	10Gbps
IPSec Thoughtput <sup>(3)</sup>	7Gbps	14Gbps	28Gbps
New Sessions/sec(HTTP)	250K	300K	450K
Maximum Concurrent Sessions	4 million sessions	5 million sessions	6 million sessions
Integrated I/O	2 x GE, 4 x SFP	2 x GE, 4 x SFP	2 x GE, 4 x SFP
Maximum I/O	22 x GE, 4 x 10GE	38 x GE, 8 x 10GE	38 x GE, 8 x 10GE
Expansion Modules	2 x Generic Slot	4 x Generic Slot	4 x Generic Slot
Expansion Module Option	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 x Console Port, 1 x AUX Port, 1 x USB 2.0 Port, 2 x HA, 1 x MGT	1 x Console Port, 1 x AUX Port, 1 x USB 2.0 Port, 2 x HA, 1 x MGT	1 x Console Port, 1 x AUX Port, 1 x USB 2.0 Port, 2 x HA, 1 x MGT
Maximum Power Consumption	2 x 450W Redundancy 2 + 2	2 x 450W Redundancy 2 + 2	2 x 450W Redundancy 2 + 2
Storage	80G SSD, 500G HDD or 1T HDD	120G SSD, 500G HDD or 1T HDD	120G SSD,500G HDD or 1T HDD
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
Dimension (W×D×H)	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	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)
Relative Humidity	10-95%	10-95%	10-95%

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

Specification	IOC-4XFP	IOC-8SFP+	IOC-4SFP+
			
Name	4XFP Extension Module	8SFP+ Extension Module	4SFP+ Extension Module
I/O Ports	4 x XFP, XFP module not included	8 x SFP+, SFP+ module not included	4 x SFP+, SFP+ module not included
Dimension	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)
Weight	2.0 lb (0.9kg)	1.5 lb (0.7kg)	1.5 lb (0.7kg)

(1) IPS Throughput data is obtained under 1M-byte-payload HTTP traffic with test of 32K-byte scanning.

(2) AV Throughput data is obtained under 1M-byte-payload HTTP traffic with file attachment.

(3) IPSec Throughput data is obtained under Preshare Key AES256+SHA-1 configuration and 1400-byte packet size packet .

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R1. Results may vary based on StoneOS® version and deployment.