Hillstone E Series Next-Generation Firewall

Hillstone E Series next generation firewalls provide visibility and 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. Hillstone E-Series firewalls incorporate comprehensive network security and advanced firewall features. They provide superior price performance, excellent energy efficiency, and a smaller size when compared to competing products.

Product Highlights

Granular Application Control

Hillstone E 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.

Proactive Threat Protection

Hillstone E Series firewalls provide real-time protection for application and network attacks including viruses, spyware, worms, botnets, ARP spoofing, DoS/DDoS, Trojans, buffer overflows, and SQL injections. It incorporates a unified malware detection engine that shares packet details with multiple security defenses (IPS, URL filtering, and Anti-Virus), which significantly reduces latency.

Visibility and Control

Hillstone E Series provides visibility and control of network traffic. An intuitive user interface displays all applications traversing the network along with application categories and bandwidth. An administrator can quickly choose an application and see all the users who are accessing that application along with bandwidth consumption. If a particular user is of interest the administrator can see all the applications that user is using - now and in the past. Inappropriate applications can be blocked or limited by bandwidth or time of day. Multiple reports show top applications, top users, top URLs, top URL categories, top threats, etc.

www.hillstonenet.com
Phone: 1-800-889-9860

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: MSRCP, 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 holing
- 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/SCIP/ICMP session flooding (source/destination)
- Active bypass with bypass interfaces
- Predefined prevention configuration

Threat Protection

- 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 encryption 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/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

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-E1600	SG-6000-E1700	SG-6000-E2300
			
FW Throughput (Maximum)	1Gbps	1.5Gbps / 2Gbps	2.5Gbps / 4Gbps
IPSec Throughput[1]	600Mbps	700Mbps	1Gbps
Maximum Concurrent Sessions (Standard/ Maximum)	200K	600K/1M	1M/2M
AV Throughput [2]	300Mbps	400Mbps	700Mbps
IPS Throughput [3]	400Mbps	600Mbps	1Gbps
New Sessions/s[4]	10,000	25,000	50,000
IPSec Tunnel Number	512	2,000	2,000
Maximum SSL VPN Users	128	500	1,000
Management Ports	1 x Console Port	1 x Console Port	1 x Console Port
Fixed I/O Ports	9 x GE	9 x GE	5 x GE, 4 x Combo
Available Slots for Extension Modules	No	No	No
Expansion Module Option	No	No	No
Maximum Power Consumption	30W	45W	45W
Power Supply	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz DC -40 ~ -60V	AC 100-240V 50/60Hz DC -40 ~ -60V
Dimension (W × D × H, mm)	Desktop 12.6 × 5.91 × 1.7 in (320 × 150 × 44 mm)	1U 17.4 x 9.5 x 1.7 in (442 x 241 x 44 mm)	1U 17.4 x 9.5 x 1.7 in (442 x 241 x 44 mm)
Weight	3.3lb (1.5kg)	5.5 lb (2.5kg)	5.5 lb (2.5kg)
Temperature	32-104 F (0-40℃)	32-104 F (0-40℃)	32-104 F (0-40℃)
Relative Humidity	10-95% (no dew)	10-95%(no dew)	10-95%(no dew)

Specification	SG-6000-E2800	SG-6000-E3660	SG-6000-E3960	SG-6000-E5260
				
FW Throughput (Maximum)	4.5Gbps / 6Gbps	8Gbps	10Gbps	16Gbps
IPSec Throughput[1]	3Gbps	3Gbps	4Gbps	8Gbps
Maximum Concurrent Sessions (Standard/ Maximum)	1M/2M	1M/2M	4M	6M
AV Throughput [2]	1.2Gbps	2Gbps	2.5Gbps	3.5Gbps
IPS Throughput [3]	1.8Gbps	3Gbps	4Gbps	5Gbps
New Sessions/s[4]	80,000	120,000	150,000	200,000
IPSec Tunnel Number	2,000	6,000	10,000	20,000
Maximum SSL VPN Users	1,000	4,000	6,000	10,000
Management Ports	1 x Console Port	1 x Console Port, 1 x AUX Port, 1 MGT, 1 x USB Port,1 x AUX Port	1 x Console Port, 1 x AUX Port, 1 MGT, 1 x USB Port,1 x AUX Port	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1 x MGT

Specification	SG-6000-E2800	SG-6000-E3660	SG-6000-E3960	SG-6000-E5260
Fixed I/O Ports	5 x GE, 4 x Combo	6 x GE, 4 x SFP	6 x GE, 4 x SFP, 2 X SFP+	4 x GE, 4 x SFP, 2 X SFP+
Available Slots for Extension Modules	No	2 x Generic Slot	2 x Generic Slot	4 x Generic Slot
Expansion Module Option	No	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M, IOC-4GE-POE	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M, IOC-4GE-POE	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M, IOC-2XFP-Lite-M, IOC-4GE-POE, IOC-8SFP+, IOC-4SFP+
Maximum Power Consumption	45W	1 x 150W Redundancy 1 + 1	1 x 150W Redundancy 1 + 1	1 x 450W Redundancy 1 + 1
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
Dimension (W × D × H, mm)	1U 17.4 x 9.5 x 1.7 in (442 x 241 x 44 mm)	1U 17.2 x 14.4x 1.7 in (436 x 366 x 44 mm)	1U 17.2 x 14.4x 1.7 in (436 x 366 x 44 mm)	1U 17.3 x 20.9 x 3.5 in (440 x530 x 88 mm)
Weight	5.5 lb (2.5kg)	12.3lb (5.6kg)	12.3lb (5.6kg)	27.1 lb (11.8kg)
Temperature	32-104 F (0-40℃)	32-104 F (0-40℃)	32-104 F (0-40℃)	32-104 F (0-40℃)
Relative Humidity	10-95%(no dew)	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)

Specification	SG-6000-E5660	SG-6000-E5760	SG-6000-E5960
			
FW Throughput (Maximum)	25Gbps	32Gbps	40Gbps
IPSec Throughput[1]	15Gbps	18Gbps	25Gbps
Maximum Concurrent Sessions (Standard/Maximum)	10M	12M	15M
AV Throughput [2]	7Gbps	8Gbps	10Gbps
IPS Throughput [3]	12Gbps	15Gbps	18Gbps
New Sessions/s[4]	400,000	500,000	600,000
IPSec Tunnel Number	20,000	20,000	20,000
Maximum SSL VPN Users	10,000	10,000	10,000
Management Ports	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1 x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1 x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1 x MGT
Fixed I/O Ports	4 x GE, 4x SFP	4 x GE, 4x SFP	4 x GE, 4 x SFP
Available Slots for Extension Modules	4 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-8SFP+, IOC-4GE-POE, IOC-4SFP+	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-2XFP-Lite-M, IOC-8SFP+, IOC-4GE-POE, IOC-4SFP+	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-2XFP-Lite-M, IOC-8SFP+, IOC-4GE-POE, IOC-4SFP+
Maximum Power Consumption	1 x 450W Redundancy 1 + 1	1 x 450W Redundancy 1 + 1	1 x 450W Redundancy 1 + 1
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, mm)	2U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)	2U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)	2U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)
Weight	27.1 lb (12.3kg)	27.1 lb (12.3kg)	27.1 lb (12.3kg)
Temperature	32-104 F (0-40℃)	32-104 F (0-40℃)	32-104 F (0-40℃)
Relative Humidity	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)

Specification	SG-6000-E1100W	SG-6000-E1100WG3w
		
FW Throughput (Maximum)	1Gbps	1Gbps
IPSec Throughput[1]	600Mbps	600Mbps
Maximum Concurrent Sessions (Standard/ Maximum)	200K	200K
AV Throughput[2]	300Mbps	300Mbps
IPS Throughput[3]	400Mbps	400Mbps
New Sessions/s[4]	10,000	10,000
IPSec Tunnel Number	512	512
Maximum SSL VPN Users	128	128
Management Ports	1 × console port	1 × console port
Fixed I/O Ports	9 × GE	9 × GE
WiFi	IEEE802.11a/b/g/n	IEEE802.11a/b/g/n
3G	NA	WCDMA
Maximum Power Consumption	30W	30W
Power Supply	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz
Dimension (W × D × H, mm)	Desktop 12.6 × 5.91 × 1.7 in (320 × 150 × 44 mm)	Desktop 12.6 × 5.91 × 1.7 in (320 × 150 × 44 mm)
Weight	3.3lb (1.5kg)	3.3lb (1.5kg)
Temperature	32-104 F (0-40℃)	32-104 F (0-40℃)
Relative Humidity	10-95% (no dew)	10-95% (no dew)

Module Options

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-4GE-POE	IOC-4SFP+
				
Name	4XFP Extension Module	8SFP+ Extension Module	4GE PoE Extension Module	4SFP+ Extension Module
I/O Ports	4 x XFP, XFP module not included	8 x SFP+, SFP+ module not included	4 x GE with PoE	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)	1 U (Occupies 2 generic slots)
Weight	2.0 lb (0.9kg)	1.5 lb (0.7kg)	0.9 lb (0.4kg)	1.5 lb (0.7kg)

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.0R3. Results may vary based on StoneOS® version and deployment.

NOTES:(1) IPSec throughput data is obtained under Preshare Key AES256+SHA-1 configuration and 1400-byte packet size packet; (2) AV throughput data is obtained under HTTP traffic with file attachment; (3) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on; (4) New Sessions/s is obtained under TCP traffic.