

# Hillstone E-1000 Series Next-Generation Firewall



E1100W / E1600 / E1606 / E1700



The Hillstone E-1000 Series Next Generation Firewall (NGFW) provides comprehensive and granular visibility and control of applications. 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 unauthorized or malicious applications. The Hillstone E-1000 Series NGFW incorporates comprehensive network security and advanced firewall features, provides superior price performance, excellent energy efficiency, and comprehensive threat prevention capability.

## Product Highlights

### Granular Application Identification and Control

The Hillstone E-1000 Series NGFW provides 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. Security Policies can be defined that guarantee bandwidth to mission-critical applications while restricting or blocking unauthorized or malicious applications.

### Comprehensive Threat Detection and Prevention

The Hillstone E-1000 Series NGFW provides real-time protection for applications from network attacks including viruses, spyware, worms, botnets, ARP spoofing, DoS/DDoS, Trojans, buffer overflows, and SQL injections. It incorporates a unified threat detection engine that shares packet details with multiple security engines (AD, IPS, URL filtering, Anti-Virus, Sandbox etc.), which significantly enhances the protection efficiency and reduces network latency.

## 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 – 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: 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/SCTP port scan, ICMP sweep, TCP/UDP/SCIP/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/SFTP
- Compressed file virus scanning

### Attack Defense

- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN Flood, UDP Flood, DNS Query Flood defense, TCP fragment, ICMP fragment, etc.
- 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
- Support multi-language

### 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
- Periodical 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 operation systems including Windows, iOS, Android, etc.
- 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 overrun IP
- Redirect page display after custom interference operation
- Supports blocking operations on overrun 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
- Content filtering for HTTP-GET, HTTP-POST, FTP and SMTP protocols
- 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/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

## Features

### Server Load balancing

- Weighted hashing, weighted least-connection, and weighted round-robin
- Session protection, 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 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

### 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 including static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, URL filtering, 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 mode
- 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
- 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

### IoT Security

- Identify IoT devices such as IP Cameras and Network Video Recorders
- Support query of monitoring results based on filtering conditions, including device type, IP address, status, etc.
- Support customized whitelists

### Wireless (only on E1100W)

- Multi-SSID and wireless traffic control

## Product Specification

Specification	SG-6000-E1100W	SG-6000-E1600	SG-6000-E1606	SG-6000-E1700
				
FW Throughput <sup>(1)</sup>	1Gbps	1Gbps	1Gbps	1.5Gbps/2Gbps
IPSec Throughput <sup>(2)</sup>	600Mbps	600Mbps	600Mbps	700Mbps
AV Throughput <sup>(3)</sup>	300Mbps	300Mbps	300Mbps	400Mbps
IPS Throughput <sup>(4)</sup>	400Mbps	400Mbps	400Mbps	600Mbps
IMIX Throughput <sup>(5)</sup>	200Mbps	200Mbps	200Mbps	600Mbps
NGFW Throughput <sup>(6)</sup>	350Mbps	350Mbps	350Mbps	450Mbps
Threat Protection Throughput <sup>(7)</sup>	300Mbps	300Mbps	300Mbps	400Mbps
New Sessions/s <sup>(8)</sup>	10,000	10,000	12,000	25,000
Maximum Concurrent Sessions (Standard/Maximum)	200k	200k	400k	600k/1M
IPSec Tunnel Number	512	512	1,000	2,000
SSL VPN Users (Default/Max)	8/128	8/128	8/500	8/500
Virtual Systems (Default/Max)	N/A	1/1	1/5	1/5
Management Ports	1 x Console Port 1 x USB Port	1 x Console Port 1 x USB Port	1 x Console Port 1 x USB Port	1 x Console Port 1 x USB Port
Fixed I/O Ports	9 x GE	9 x GE	9 x GE	9 x GE
WiFi	IEEE802.11 a/b/g/n	N/A	N/A	N/A
Maximum Power Consumption	30W	30W	1 x 45W Redundancy 1+1	1 x 45W Redundancy 1+1
Power Supply	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC:100-240V 50/60Hz	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)	Desktop 12.6 × 5.91 × 1.7 in (320×150×44 mm)	1U 17.4 x 9.5 x 1.7in (442 x 241 x 44mm)	1U 17.4 x 9.5 x 1.7in (442 x 241 x 44mm)
Weight	3.3lb (1.5KG)	3.3lb (1.5KG)	5.5lb (2.5kg)	5.5lb (2.5kg)
Temperature	32-104 F (0-40°C)	32-104 F (0-40°C)	32-104F (0-40°C)	32-104F (0-40°C)
Relative Humidity	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)
Compliance and Certificate	CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls			

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) IPSec throughput data is obtained under Preshare Key AES256+SHA-1 configuration and 1400-byte packet size packet; (3) AV throughput data is obtained under HTTP traffic with file attachment; (4) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on; (5) IMIX throughput data is obtained under UDP traffic mix (64 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 and URL filtering enabled; (8) New Sessions/s is obtained under TCP traffic.