

# Hillstone E-2000 Series

## Next-Generation Firewall



The Hillstone E-2000 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-2000 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-2000 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-2000 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, Antivirus, 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
- Multicast(PIM-SSM)
- Virtual wire (Layer 1) transparent inline deployment

## Firewall

- Operating modes: NAT/route, transparent (bridge), and mixed mode
- Policy objects: predefined, custom, aggregate policy, 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

## Antivirus

- Manual, automatic push or pull signature updates
- Manually add or delete MD5 signature to the AV database
- MD5 signature support uploading to cloud sandbox, and manually add or delete on local database
- Flow-based Antivirus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB
- Compressed file virus scanning

## Attack Defense

- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment, etc.
- ARP attack defense
- Allow list for destination IP address

## 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
- URL allow / block list configuration

## Cloud-Sandbox

- Upload malicious files to cloud sandbox for analysis
- Support protocols including HTTP/HTTPS, POP3, IMAP, SMTP, FTP and SMB
- Support file types including PE, ZIP, RAR, Office, PDF, APK, JAR, SWF and Script
- 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
- Allow and block list based on IP address or domain name
- Support DNS sinkhole and DNS tunneling detection

## 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
- Support application identification, DLP, IPS sandbox, AV for SSL proxy decrypted traffic of SMTPS/POP3S/IMAPS

## Endpoint Identification and Control

- Support to identify endpoint IP, endpoint quantity, on-line time, off-line time, and on-line duration
- Support 10 operating 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
- User identification and traffic control for remote desktop services of Windows Server

## Data Security

- File transfer control based on file type, size and name
- File protocol identification, including HTTP, FTP, SMTP, POP3 and SMB
- 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 and SMB

## Application Control

- Over 4,000 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

## Server Load Balancing

- Weighted hashing, weighted least-connection, and

## Features (Continued)

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: policy based routing including ECMP, time, weighted, and embedded ISP routing; Active and passive real-time link quality detection and best path selection
- 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
  - IKEv1 support DH group 1,2,5,19,20,21,24
  - IKEv2 support DH group 1,2,5,14,15,16,19,20,21,24
  - 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
- PnVPN
- VTEP for VxLAN static unicast tunnel

### IPv6

- Management over IPv6, IPv6 logging and HA
- IPv6 tunneling: DNS64/NAT64, IPv6 ISATAP, IPv6 GRE, IPv6 over IPv4 GRE
- IPv6 routing including static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, URL filtering, Antivirus, Access control, ND attack defense, iQoS
- Track address detection
- IPv6 jumbo frame support
- IPv6 Radius support
- IPv6 support on the following ALGs: TFTP, FTP, RSH, HTTP, SIP
- IPv6 support on distributed iQoS

### VSYS

- System resource allocation to each VSYS
- CPU virtualization
- Non-root VSYS support firewall, IPsec VPN, SSL VPN, IPS, URL filtering, app monitoring, IP reputation, QoS
- 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 Directory
- 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, force crack prevention, IPv6 support
- Interface based authentication
- Agentless ADSSO (AD Polling)
- Use authentication synchronization based on SSO-monitor
- Support IP-based and 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 log storage with storage models for up to 6 months, 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
- 24/7 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

## Specifications

	SG-6000-E2300	SG-6000-E2800	SG-6000-E2860	SG-6000-E2868
				
<b>FW Throughput</b> <sup>(1)</sup>	2.5 Gbps / 4 Gbps	4.5 Gbps / 6 Gbps	6 Gbps	6 Gbps
<b>IPSec Throughput</b> <sup>(2)</sup>	1 Gbps	3 Gbps	3 Gbps	3 Gbps
<b>AV Throughput</b> <sup>(3)</sup>	700 Mbps	1.2 Gbps	1.2 Gbps	1.2 Gbps
<b>IPS Throughput</b> <sup>(4)</sup>	1 Gbps	1.8 Gbps	1.8 Gbps	1.8 Gbps
<b>IMIX Throughput</b> <sup>(5)</sup>	800 Mbps	2 Gbps	2 Gbps	2 Gbps
<b>NGFW Throughput</b> <sup>(6)</sup>	650 Mbps	850 Mbps	1 Gbps	1 Gbps
<b>Threat Protection Throughput</b> <sup>(7)</sup>	500 Mbps	700 Mbps	800 Mbps	800 Mbps
<b>New Sessions/s</b> <sup>(8)</sup>	50,000	80,000	80,000	80,000
<b>Maximum Concurrent Sessions (Standard/Maximum)</b>	1 Million / 2 Million	1 Million / 2 Million	2 Million	2 Million
<b>IPSec Tunnel Number</b>	2,000	2,000	4,000	4,000
<b>SSL VPN Users (Default/Max)</b>	8 / 1,000	8 / 1,000	8 / 2,000	8 / 2,000
<b>Virtual Systems (Default/Max)</b>	1 / 5	1 / 5	1 / 5	1 / 5
<b>Storage Options</b>	N/A	N/A	N/A	256G / 512G SSD (E2868 / E2868A)
<b>Management Ports</b>	1 x Console Port, 1xUSB port	1 x Console Port, 1xUSB port	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
<b>Fixed I/O Ports</b>	5 x GE, 4 x Combo	5 x GE, 4 x Combo	6 x GE, 4 x SFP	6 x GE, 4 x SFP
<b>Available Slots for Expansion Modules</b>	N/A	N/A	2 x Generic Slot	2 x Generic Slot
<b>Expansion Module Option</b>	N/A	N/A	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M
<b>Power Specification</b>	45W, Single AC or DC, Dual AC Redundant	45W, Single AC or DC, Dual AC Redundant	150W, Single AC or DC, Dual AC Redundant	150W, Single AC, Dual AC Redundant
<b>Power Supply</b>	AC 100-240 V 50/60 Hz DC -40 ~ -60 V	AC 100-240 V 50/60 Hz DC -40 ~ -60 V	AC 100-240 V 50/60 Hz DC -40 ~ -60 V	AC 100-240 V 50/60 Hz DC -40 ~ -60 V
<b>Dimension (WxDxH, mm)</b>	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)	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)
<b>Weight</b>	5.5 lb (2.5 kg)	5.5 lb (2.5 kg)	12.3 lb (5.6 kg)	12.3 lb (5.6 kg)
<b>Temperature</b>	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
<b>Relative Humidity</b>	10-95%(no dew)	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)
<b>Compliance and Certificate</b>	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			

## Module Options

	IOC-8GE-M	IOC-8SFP-M	IOC-4GE-B-M
			
<b>Names</b>	8GE Expansion Module	8SFP Expansion Module	4GE Bypass Expansion Module
<b>I/O Ports</b>	8 x GE	8 x SFP, SFP module not included	4 x GE Bypass (2 pair bypass ports)
<b>Dimension</b>	½U (Occupies 1 generic slot)	½U (Occupies 1 generic slot)	½U (Occupies 1 generic slot)
<b>Weight</b>	1.8 lb (0.8 kg)	2.0 lb (0.9 kg)	1.8 lb (0.8 kg)

### 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;
- (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.

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R8. Results may vary based on StoneOS® version and deployment.