Hillstone Networks

Hillstone E-5000 Series Next-Generation Firewall

NSS LABS RECOMMENDED

ICSA labs CERTIFIED FIREWALL - CORPORATE

E5260 / E5660 / E5760 / E5960

The Hillstone E-5000 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-5000 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-5000 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-5000 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: 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 holing
- 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 [1]
- 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

Features

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-E5260	SG-6000-E5660	SG-6000-E5760	SG-6000-E5960
FW Throughput (Maximum)[2]	16Gbps	25Gbps	32Gbps	40Gbps
IPSec Throughput[3]	8Gbps	15Gbps	18Gbps	25Gbps
Maximum Concurrent Sessions (Standard/ Maximum)	6M	10M	12M	15M
AV Throughput [4]	3.5Gbps	7Gbps	8Gbps	10Gbps
IPS Throughput [5]	5Gbps	12Gbps	15Gbps	18Gbps
New Sessions/s[6]	200,000	400,000	500,000	600,000
IPSec Tunnel Number	20,000	20,000	20,000	20,000
SSL VPN Users (Default/Max)	8/10,000	8/10,000	8/10,000	8/10,000
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	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, 4 x SFP, 2 X SFP+	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	4 x Generic Slot
Expansion Module Option	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M, IOC-2XFP-Lite-M, IOC-4GE-POE, IOC-8SFP+, 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+	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-2XFP-Lite-M, IOC-8SFP+, IOC-4GE-POE, IOC-4SFP+
Maximum Power Consumption	2 x 450W Redundancy 1 + 1	2 x 450W Redundancy 1 + 1	2 x 450W Redundancy 1 + 1	2 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)	2U 17.3 x 20.9 x 3.5 in (440 x530 x 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)	2U 17.3 × 20.5 × 3.5 in (440×520×88 mm)
Weight	27.1 lb (11.8kg)	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℃)	32-104 F (0-40℃)
Relative Humidity	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)

Module Options

Specification	IOC-8GE-M	IOC-8SF P-M	IOC-4GE- B-M	IOC-2XF P-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 slots)	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-8SFP+	IOC-4GE-POE	IOC-4SFP+
Name	8SFP+ Extension Module	4GE PoE Extension Module	4SFP+ Extension Module
I/O Ports	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)
Weight	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 StoneOS5.5R4. 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.