

# Hillstone A-Series

## Next-Generation Firewall



The Hillstone A-Series next-generation firewall features high security performance, expansion as needed, complete advanced threat detection and prevention, and smart and automated policy operation. This future-ready NGFW series is based on a brand new hardware architecture that offers industry-leading application layer performance to meet real-world network security needs. High-density ports ensure excellent access capability, and large storage options offer better visibility and analytics. As part of the ZTNA solution, A-Series NGFW granularly controls the application access with eliminated implicit trust and continuous verification. The Hillstone A-Series NGFW offers complete, advanced defenses against known and unknown threats, coupled with smart, automated and efficient policy operation that makes security operations easy.

## Product Highlights

### Advanced Threat Detection and Protection

The Hillstone A-Series NGFW includes a full arsenal of mechanisms to provide real-time detection and protection across the full lifecycle of network attacks and malwares. Before a breach can even occur, proactive protections like IPS block the vulnerabilities exploitation. IP reputation services block requests from risky sites potentially involved in malware and spamming. URL filtering prevents users from inadvertently accessing sites associated with phishing, malware downloads and other exploits. Anti-virus detects and blocks known malwares at the network level with an advanced signature database that is continuously updated. Anti-spam provides real-time spam classification and prevention for both inbound and outbound traffic.

During a breach, anti-virus plays an important role as well by continuing to detect and block known malwares. A cloud

sandbox provides sophisticated detection and prevention of malicious files through static analysis and pre-processing, followed by behavioral analysis that includes detection of evasive maneuvers. Cloud intelligence then identifies and blocks malicious files, generates logs and reports, and shares threat intelligence back to the cloud.

Completing protections across the full threat lifecycle, the A-Series continues to defend even after a breach has occurred. Hillstone's advanced Botnet C&C prevention feature prevents communication to the control channel, and detect and block bots within the intranet as well.

In addition, A-Series NGFW leverages machine learning technology for intelligent security protection against known and unknown threats, such as intelligent DDoS, DGA, and encrypted traffic detection without decryption.

Further, the system's unified threat detection and analytics engine coordinates across all built-in security mechanisms

## Product Highlights (Continued)

to dramatically enhance efficiency while reducing network latency.

### High-Performance Hardware Architecture

The future-ready A-Series features compact form factor and a powerful computing foundation that ensures high performance with uncompromising security. A-Series NGFWs offer robust performance for firewall throughput, concurrent and new sessions, and blazing fast performance for application layer, which is critical in meeting the needs of current security environments. Powered with Hillstone proprietary hardware acceleration engine, A-Series NGFW high-end models enable fast packet forwarding with high throughput and ultra-low latency by traffic offloading. It also offers a friendly software ecology for third-party integration to support additional security features if desired. All rackmount models feature front and rear ventilation to assist in heat dissipation, which is a concern in networks of almost any size.

### Excellent Access Capability and Storage Expansion

The Hillstone A-Series offers high I/O port density, allowing the NGFW to act as a switch or router as needed, lowering deployment and management costs. In addition, expansion slots are available for a number of A-Series models to further increase performance. Bypass pairs on most A-Series models help ensure business continuity.

All models, including the desktop versions, include a large onboard storage and have expansion options for very-large

hard disk storage up to 2 TB.

With more storage the system can save more logs and data for longer time, enabling deeper analysis. In addition, the expanded storage allows the system to provide richer reports with far more information, including visualized results and actionable recommendations.

Further, with deeper threat analysis the WebUI can display much richer threat detection information, which in turn gives admins better visibility. The increased visibility lets admins quickly zero in on anomalies and other suspicious network events or traffic, analyze them and respond.

### Smart Policy Operation

The A-Series includes intelligent management and operation across the full policy lifecycle, from deployment to management, optimization and operation. The system features automated user policy deployment using RADIUS dynamic authorization. Policy management is made far more efficient through policy groupings based on business requirements. In addition, policies can be aggregated to allow a set of policies to act as a single policy. An innovative policy assistant analyzes traffic patterns and recommends refined policies for faster, easier and more accurate policy management. Policy operation is made more efficient and precise through policy redundancy checks, which identify redundant policies for deactivation or deletion, and policy hit count analysis, that helps further refine and adjust policies.

# Features

## Network Services

- Dynamic routing (OSPF, BGP with graceful restart, 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, tcp full proxy
- NAT and ALG support: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT (IPv4 and IPv6), 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, aggregate policy
- Policy Assistant for service base or application based policy recommendation
- Policy analyzing and invalid policy cleanup
- Comprehensive DNS policy
- Schedules: one-time and recurring
- Support policy import and export
- Support NAT redundancy detection

## 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
- IPS threat packet capture (with expansion storage only)
- ML-based threat detection in encrypted traffic without decryption
- Support protection of brute force attacks including VNC, RDP, SSH, LDAP, IMAP, SMB

- Support protection of sensitive file scanning attack
- Support reverse shell detection

## 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
- Flood attack defense, including ICMP flood, UDP flood, DNS query flood, recursive DNS query flood, DNS reply flood, SYN flood, SIP flood
- ARP spoofing and ND spoofing defense
- Scan and spoof defense, including IP address spoof, IP address sweep, port scan
- Intelligent DoS/DDoS defense with ML-based baseline establishment, including ping of death attack, teardrop attack, IP fragment, IP option, Smurf or Fragile attack, Land attack, large ICMP packet, WinNuke attack
- 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 URL allow list and block list

## Anti-Spam<sup>(1)</sup>

- Real-time Spam Classification and Prevention
- Confirmed Spam, Suspected Spam, Bulk Spam, Valid Bulk
- Protection Regardless of the language, format, or content of the message
- Support both SMTP and POP3 email protocols
- Inbound and outbound detection
- White lists to allow emails from trusted domains

## 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
- URL allow / block list configuration

## 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
- Support DGA 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
- SSL proxy supports IP whitelist and predefined whitelist
- SSL proxy supports session re-use
- Support AD/LDAP server connection via SSL encryption
- Support TLS v 1.2, TLS v 1.3
- 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

## Features (Continued)

- Content filtering for predefined keywords and file contents
- IM identification and network behavior audit
- Filter files transmitted by HTTPS using SSL Proxy and SMB

### Application Control

- Over 6,000 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) and traffic-class 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 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 1,2,5,18,19,20,21,24
- IKEv2 support DH group 1,2,5,14,15,16,18,19,20,21,24
- 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 supports configuration guide. Configuration options includes: route-based or policy based
- IPsec VPN deployment modes: gateway-to-gateway, full mesh, hub-and-spoke, redundant tunnel, VPN termination in transparent mode
- IPsec supports custom ports
- IPsec VPN supports DPD On-Demand mode
- LLB and failover support over IPsec tunnels
- 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, Microsoft Windows, MacOS and Linux
- 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, HA and HA peer mode, twin-mode AA and AP
- IPv6 tunneling: DNS64/NAT64, IPv6 ISATAP, IPv6 GRE, IPv6 over IPv4 GRE, 6RD
- IPv6 routing including static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPv6 support on LLB
- IPS, Application identification, URL filtering, Antivirus, Access control, ND attack defense, iQoS, SSL VPN
- IPv6 jumbo frame support
- IPv6 Radius and sso-radius supports
- IPv6 is supported in Active Directory whitelist
- IPv6 support on the following ALGs: TFTP, FTP, RSH, HTTP, SIP, SQLNETv2, RTSP, MSRPC, SUNRPC
- IPv6 support on distributed iQoS
- Track address detection

### VSYS (only available on rackmount models)

- 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, app monitoring, IP reputation, AV, QoS

### High Availability

- Redundant heartbeat interfaces
- Active/Active peer mode with Hillstone Virtual Redundancy Protocol (HSVRP) support, 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
- Dual HA data link ports

### Twin-mode HA (only available on A3000-IN and above models)

- High availability mode among multiple devices
- Multiple HA deployment modes
- Configuration and session synchronization among multiple devices

### 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
- Radius server issues user security policy via CoA message

### 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
- Administrator authentication: Active Directory and LDAP

## Features (Continued)

### Logs & Reporting

- Logging facilities: local storage; up to 6 months log storage with expansion storage (SSD hard drive), syslog server, Hillstone HSM or HSA
- 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, Wi-Fi 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
- Support policy configuration auditing

### 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)

### Zero Trust Network Access(ZTNA)

- Support end-user access with a Zero-Trust principle
- ZTNA tags support account password and terminal status
- Support Zero-Trust policy configuration based on ZTNA tags and application resources, with optional security protection and data security
- Support application resource management
- Support application resource configuration based on domain name
- Support dynamic adjustment of authorization in policy when the endpoint state changes
- Support application publishing, and displaying authorized applications to end-users over ZTNA portal
- Support single packet authentication(SPA)
- Support domain name level permission management
- Support auto-selection of the optimal gateway
- Support smooth transition from current SSL VPN to ZTNA solution

- Support operating systems including iOS, Android, Microsoft Windows, MacOS and Linux
- Support centralized ZTNA management by HSM, including upload monitoring data and statistics, and accept the configuration delivered

### 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-A200-IN	SG-6000-A200W-IN	SG-6000-A1000-IN	SG-6000-A1100-IN	SG-6000-A2000-IN	SG-6000-A2600-IN
						
Firewall Throughput <sup>(2)</sup>	1 Gbps	1 Gbps	4 Gbps	5 Gbps	5 Gbps	5 Gbps
NGFW Throughput <sup>(3)</sup>	400 Mbps	400 Mbps	1.5 Gbps	1.7 Gbps	1.7 Gbps	2.5 Gbps
Threat Protection Throughput <sup>(4)</sup>	200 Mbps	200 Mbps	800 Mbps	800 Mbps	800 Mbps	1.8 Gbps
Maximum Concurrent Sessions <sup>(5)</sup>	300,000	300,000	300,000	300,000	1 Million	1.2 Million
New Sessions/s <sup>(6)</sup>	15,000	15,000	48,000	48,000	48,000	120,000
IPS Throughput <sup>(7)</sup>	610 Mbps	610 Mbps	3.4 Gbps	3.7 Gbps	3.2 Gbps	4.5 Gbps
AV Throughput <sup>(8)</sup>	550 Mbps	550 Mbps	1.8 Gbps	2.0 Gbps	2.0 Gbps	3.7 Gbps
IPsec VPN Throughput <sup>(9)</sup>	0.62 Gbps	0.62 Gbps	2.5 Gbps	2.7 Gbps	2.7 Gbps	3 Gbps
SSL Proxy Throughput <sup>(10)</sup>	15 Mbps	15 Mbps	250 Mbps	250 Mbps	250 Mbps	750 Mbps
Virtual Systems (Default/Max)	N/A	N/A	N/A	N/A	1/5	1/5
Firewall Policy Number	4000	4000	4,000	4,000	8,000	12,000
SSL VPN Users (Default/Max)	8/128	8/128	8/128	8/128	8/1,000	8/2,000
IPsec Tunnel Number	2,000	2,000	2,000	2,000	4,000	6,000
Management Ports	1 × Console Port, 1 × USB 2.0 Port	1 × Console Port, 1 × USB 2.0 Port	1 × Console Port, 2 × USB3.0 Ports	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)
Fixed I/O Ports <sup>(11)</sup>	1×SFP, 5×GE	1×SFP, 5×GE	4 × GE	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)
Wi-Fi	N/A	IEEE802.11a/b/g/n/ac	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	N/A	N/A	N/A	N/A	N/A	N/A
Expansion Module Option	N/A	N/A	N/A	N/A	N/A	N/A
Twin-mode HA	N/A	N/A	N/A	N/A	N/A	N/A
Local Storage	4 GB	4 GB	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	N/A	N/A	256 GB SSD	256 GB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	14W, Single AC (default)	14W, Single AC (default)	30W, Single AC	30W, Single AC	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V
Form Factor	Desktop	Desktop	Desktop	Desktop	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	180 × 110 × 28	180 × 110 × 28	270 × 160 × 44	270 × 160 × 44	436 × 320 × 44	436 × 320 × 44
Dimensions (W × D × H, inches)	7.1 × 4.3 × 1.1	7.1 × 4.3 × 1.1	10.6 × 6.3 × 1.7	10.6 × 6.3 × 1.7	17.2 × 12.6 × 1.7	17.2 × 12.6 × 1.7
Weight	2.2 lb (0.6 kg)	2.2 lb (0.6 kg)	3.1 lb (1.4 kg)	3.1 lb (1.4 kg)	8.6 lb (3.9 kg)	8.6 lb (3.9 kg)
Working Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

# Specifications (Continued)





	SG-6000-A2700-IN	SG-6000-A2800-IN	SG-6000-A3000-IN	SG-6000-A3600-IN	SG-6000-A3700-IN	SG-6000-A3800-IN
						
Firewall Throughput <sup>(2)</sup>	10 Gbps	16 Gbps	20 Gbps	20 Gbps	20/30 Gbps	20/40 Gbps
NGFW Throughput <sup>(3)</sup>	3 Gbps	4.5 Gbps	5.5 Gbps	5.5 Gbps	6 Gbps	12 Gbps
Threat Protection Throughput <sup>(4)</sup>	2 Gbps	2.8 Gbps	3 Gbps	3 Gbps	3.1 Gbps	6 Gbps
Maximum Concurrent Sessions <sup>(5)</sup>	1.5 Million	1.8 Million	2 Million	3 Million	6 Million	8 Million
New Sessions/s <sup>(6)</sup>	130,000	130,000	140,000	140,000	140,000	310,000
IPS Throughput <sup>(7)</sup>	5 Gbps	8 Gbps	10 Gbps	10 Gbps	10 Gbps	20 Gbps
AV Throughput <sup>(8)</sup>	4.2 Gbps	4.2 Gbps	4.9 Gbps	5.0 Gbps	5.2 Gbps	9.4 Gbps
IPsec VPN Throughput <sup>(9)</sup>	5 Gbps	5.5 Gbps	6 Gbps	6 Gbps	6.5 Gbps	12 Gbps
SSL Proxy Throughput <sup>(10)</sup>	800 Mbps	800 Mbps	950 Mbps	950 Mbps	950 Mbps	2 Gbps
Virtual Systems (Default/Max)	1/5	1/5	1/50	1/100	1/250	1/250
SSL VPN Users (Default/Max)	8/4,000	8/4,000	8/4,000	8/8,000	8/10,000	8/10,000
IPsec Tunnel Number	6,000	6,000	8,000	10,000	20,000	20,000
Firewall Policy Number	12,000	12,000	20,000	20,000	20,000	40,000
Management Ports	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)
Fixed I/O Ports <sup>(11)</sup>	2 × SFP+, 8 × SFP, 8 × GE	2 × SFP+, 8 × SFP, 8 × GE	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)
Wi-Fi	N/A	N/A	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	N/A	N/A	N/A	N/A	1	1
Expansion Module Option	N/A	N/A	N/A	N/A	IOC-A-4SFP+IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN, IOC-A-2QSFP+IN	IOC-A-4SFP+IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN, IOC-A-2QSFP+IN
Twin-mode HA	N/A	N/A	Yes	Yes	Yes	Yes
Local Storage	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	440 x 320 x 44	440 x 320 x 44	436 x 437 x 44	436 x 437 x 44	436 x 437 x 44	436 x 437 x 44
Dimensions (W × D × H, inches)	17.3 x 12.6 x 1.7	17.3 x 12.6 x 1.7	17.2 x 17.2 x 1.7	17.2 x 17.2 x 1.7	17.2 x 17.2 x 1.7	17.2 x 17.2 x 1.7
Weight	9 lb (4.1 kg)	9 lb (4.1 kg)	13.2 lb (6 kg)	13.2 lb (6 kg)	13.4 lb (6.1 kg)	15 lb (6.8 kg)
Working Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

# Specifications (Continued)

	SG-6000-A5100-IN	SG-6000-A5200-IN	SG-6000-A5500-IN	SG-6000-A5600-IN	SG-6000-A5800-IN	SG-6000-A6800-IN	SG-6000-A7600-IN
							
Firewall Throughput <sup>(2)</sup>	25/50 Gbps	32/65 Gbps	40/80 Gbps	60/85 Gbps	80/95 Gbps	200 Gbps	280/320 Gbps
NGFW Throughput <sup>(3)</sup>	20 Gbps	20 Gbps	25 Gbps	29 Gbps	32 Gbps	40 Gbps	45 Gbps
Threat Protection Throughput <sup>(4)</sup>	10 Gbps	12 Gbps	15 Gbps	18 Gbps	20 Gbps	22 Gbps	24 Gbps
Maximum Concurrent Sessions <sup>(5)</sup>	8 Million	12 Million	13 Million	20 Million	25 Million	30 Million	42 Million
New Sessions/s <sup>(6)</sup>	350,000	400,000	500,000	800,000	930,000	900,000	900,000
IPS Throughput <sup>(7)</sup>	20/25 Gbps	20/35 Gbps	25/40 Gbps	35/60 Gbps	45/75 Gbps	70 Gbps	70 Gbps
AV Throughput <sup>(8)</sup>	12 Gbps	12 Gbps	15 Gbps	20 Gbps	25 Gbps	25 Gbps	25 Gbps
IPsec VPN Throughput <sup>(9)</sup>	15 Gbps	20 Gbps	28 Gbps	36 Gbps	45 Gbps	45 Gbps	45 Gbps
SSL Proxy Throughput <sup>(10)</sup>	3 Gbps	5 Gbps	5 Gbps	8.5 Gbps	8.5 Gbps	8.5 Gbps	8.5 Gbps
Virtual Systems (Default/Max)	1/250	1/250	1/250	1/500	1/500	1/500	1/500
SSL VPN Users (Default/Max)	8/10,000	8/10,000	8/10,000	8/10,000	8/10,000	8/10,000	8/10,000
IPsec Tunnel Number	20,000	20,000	20,000	20,000	20,000	20,000	20,000
Firewall Policy Number	40,000	40,000	60,000	60,000	80,000	80,000	80,000
Management Ports	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 2 × HA ports (SFP+)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 2 × HA ports (SFP+)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 2 × HA ports (SFP+)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA port (SFP)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA port (SFP)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA ports (SFP)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA ports (SFP)
Fixed I/O Ports <sup>(11)</sup>	6 × SFP+, 16 × SFP, 8 × GE(including 2 bypass pairs)	6 × SFP+, 16 × SFP, 8 × GE(including 2 bypass pairs)	6 × SFP+, 16 × SFP, 8 × GE(including 2 bypass pairs)	2 × QSFP+, 16 × SFP+, 8 × GE(including 4 bypass pairs)	2 × QSFP+, 16 × SFP+, 8 × GE(including 4 bypass pairs)	4 × QSFP28 (or 2 × QSFP+, 2 × QSFP28), 12 × SFP+, 8 × SFP+/SFP	4 × QSFP28 (or 2 × QSFP+, 2 × QSFP28), 12 × SFP+, 8 × SFP+/SFP
Wi-Fi	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	1	1	1	1	1	1	1
Expansion Module Option	IOC-A-4SFP+IN, IOC-A-2QSFP+IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+IN, IOC-A-2QSFP+IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+IN, IOC-A-2QSFP+IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+IN, IOC-A-2QSFP+IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+IN, IOC-A-2QSFP+IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+IN, IOC-A-2QSFP+IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+IN, IOC-A-2QSFP+IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN
Twin-mode HA	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Local Storage	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB
Expansion Storage Options	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	280W, Dual AC (default), Dual DC (optional)	280W, Dual AC (default), Dual DC (optional)	280W, Dual AC (default), Dual DC (optional)	300W, Dual AC (default), Dual DC (optional)	300W, Dual AC (default), Dual DC (optional)	310W, Dual AC (default), Dual DC (optional)	310W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44	436 × 542 × 44	436 × 542 × 44
Dimensions (W × D × H, inches)	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 21.3 × 1.7	17.2 × 21.3 × 1.7
Weight	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	20.3 lb (9.2 kg)	20.3 lb (9.2 kg)
Working Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing



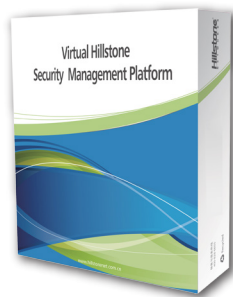
## Module Options

	IOC-A-4SFP+-IN	IOC-A-2MM-BE-IN	IOC-A-2SM-BE-IN	IOC-A-2QSFP+-IN
				
<b>Names</b>	4SFP+ Expansion Module	4SFP Multi-mode Bypass Expansion Module	4SFP Single-mode Bypass Expansion Module	2QSFP+ Expansion Module
<b>I/O Ports <sup>(11)</sup></b>	4 × SFP+, SFP+ module not included	4 × SFP, MM bypass (2 pairs of bypass ports)	4 × SFP, SM bypass (2 pairs of bypass ports)	2 × QSFP+
<b>Dimension</b>	1U	1U	1U	1U
<b>Weight</b>	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)

### NOTES:

- (1) Anti-Spam feature is not available on SG-6000-A200-IN and SG-6000-A200W-IN;
- (2) Firewall throughput data is obtained under UDP traffic with 1518-byte packet size. The firewall throughput for A3700-IN/A3800-IN can be increased to 30/40 Gbps via additional IOC-A-4SFP+-IN expansion module. The firewall throughput for A5100-IN/A5200-IN/A5500-IN/A5600-IN/A5800-IN/A7600-IN can be increased to 50/65/80/85/95/320 Gbps via additional IOC-A-2QSFP+-IN expansion module;
- (3) NGFW throughput data is obtained under 64 Kbytes HTTP traffic with application control and IPS enabled;
- (4) Threat protection throughput data is obtained under 64 Kbytes HTTP traffic with application control, IPS, AV and URL filtering enabled;
- (5) Maximum concurrent sessions is obtained under HTTP traffic;
- (6) New sessions/s is obtained under HTTP traffic;
- (7) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on;
- (8) AV throughput data is obtained under HTTP traffic with file attachment;
- (9) IPsec throughput data is obtained under Preshare Key AES256+SHA-1 configuration and 1400-byte packet size;
- (10) SSL proxy throughput data is obtained using AES128-GCM-SHA256 with all IPS rules being turned on;
- (11) SFP+ ports support SFP+ 10Gbps optical module, SFP 1000Mbps optical module and SFP 1000Mbps copper module; QSFP+ ports support 40GE 1×40Gbps module and 4×10GE 4×10Gbps modules.
- All parameters of A6800-IN and A7600-IN are based on StoneOS5.5R8. Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R9. Results may vary based on Stone-OS® version and deployment.

# Hillstone Security Management Platform



Hillstone's Security Management Platform enhances network security by allowing businesses to segment their networks into multiple virtual domains. Domains can be based on geography, business unit or security function. It provides the versatility needed to manage Hillstone's infrastructure while simplifying configuration, accelerating deployment cycles, and reducing management overhead.

## Product Highlights

### Multi-Domain Security

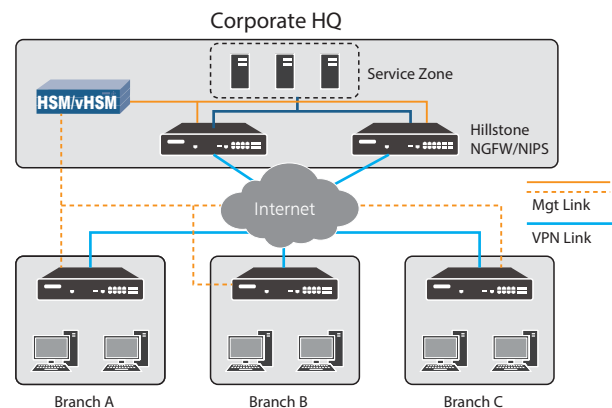
Most companies face security challenges when their business spans offices located in several regions or countries. Multiple security gateways, multiple sites requiring different security policies and multiple administrators can quickly create a complex security environment. Organizations need the tools to manage global security policies while allowing regional administrators to manage devices and users in their geographic location or business division. Hillstone's Security Manager allows the primary administrator to segment security management into multiple virtual domains. It provides the security, visibility, and control required by organizations while reducing management costs, simplifying configuration, and accelerating deployment cycles.

### SD-WAN

HSM serves as the centralized Security Manager in Hillstone's SD-WAN solution, offers centralized policy management and global visibility, allowing one-click set-up and deployment of SD-WAN networking from a central console.

### Simplified Provisioning and Management

Hillstone's Multi-Domain Security Management simplifies the provisioning of new devices. It allows a primary administrator to create groups of devices for other administrators to monitor and manage. The primary administrator can download global policies, security updates, and policy updates, while local administrators provide policies for local devices, users, and groups. Administrator also can lock the using rules and object configuration to improve the security and reliability of device configuration.



# Features

## Domain Based Management

- Segregate networks into multiple virtual domains based on location, business unit or security function
- Define global security policy templates and assign them to virtual domains
- Multiple global security policies may be created
- Virtual domains share global security policies and generate separate policies for specific users/groups and devices
- Shared objects can be assigned and used across domains

## Role-based Administration

- Administrators assigned to specific domains and devices
- Hierarchical role-based management (administrator, operator, auditor) inherit different privileges
- Multiple administrators can work on separate domains simultaneously

## Centralized Management

- Single security console manages multiple domains
- Graphical interface to view, create and manage all domains
- Create groups of devices for administrators to manage
- Assign global policies to multiple management domains
- Create role based administrators to manage policies and devices
- Device registration supported by IP, domain name or template
- Detect redundant policies, useless objects, and policy hits
- Create policy snapshots and rollback policies
- Support policy assistant
- Centralized management of route, NAT and security policies
- Centralized management of IPS/AV/SLB/URL/iQoS policy
- Centralized management of firewall password
- AAA Server, user, role configuration management
- Supports virtual appliance management

## Centralized Monitoring

- Monitor all multi-domain system components including Hillstone NGFW, CloudEdge, NIPS, sBDS, ADC and HSA from a central location
- Monitor device availability including CPU, memory, concurrent sessions, and traffic from each domain
- Monitor VPN topography graphs for each registered device
- View network status and VPN link alerts
- Monitor security events from each domain including IP, URLs, applications, and threats
- View trends for device traffic, user traffic, application traffic
- Monitor license and signature update status for devices
- View Top 10 Threats, and Top 10 URLs accessed, last 1 hour threat stats, last 1 hour alarm stats

## Log Management

- Logs produced for device traffic, system resource utilization, security events, data security, application usage and device upgrade
- Logs may be filtered by device
- Logs produced for HSM system
- Logs can be exported for historical log queries and backups
- Support log forwarding to third-party syslog server

## Configuration Management

- Device IP, domain name, and template registration
- Device software version number
- Device configuration file comparison
- Configuration file backup and recovery
- Support to lock configuration file of device
- IPS, APP, AV, URL signature upgrade configuration centralized management
- Support Firewall HA, including HA cluster management for Hillstone firewalls in Active-Passive/Active-Active/Active-Peer modes, HA groups relationship and status display

## VPN Network Monitoring

- VPN topology monitoring
- Network status monitoring
- Link interruption alarm

## System Management

- Time zone configuration, support for daylight saving time
- HSM file system automatically fix
- Configuration synchronization prompt
- HSM system password protection

## High Availability

- Support HSM HA deployment, Master/Slave roles
- Preemption mode
- Monitor/Log Synchronization
- Automatic Synchronizing and Manual Synchronizing
- Master/Slave Switchover Alarm

## Distributed Deployment

- Standalone/Master/Slave modes
- Register up to 16 slave devices on one master device
- Memory alarm, CPU alarm, disk alarm, and slave device offline alarm display on master device

## Centralized Reporting

- More than 30 built-in report templates
- Customized reporting: detailed and merged logging report with custom filters by event severity, firewall, protocol, source/destination IP, source/destination port, user, application/service, ingress interface, rule/policy number, action, close reason.
- Reports available in HTML and PDF format

## Alerts

- Multiple types of alerts including real-time and threshold-based alerts
- Device security event alerts
- vHSM do not support SMS Alert

## IPv6

- IPv6-compliant security policy, NAT, address book configuration & management
- IPv6 log collection and query
- IPv6 monitoring data collection and presentation

## Device Inspection

- Manual inspection, regular inspection, intelligent inspection
- Batch inspection

## Ticketing System

- Ticket creation, processing, review and deployment
- Ticket batch import and review
- Policy redundancy check
- Device auto identification
- Provide API to connect with other ticketing system

## SD-WAN Management

- VPN Star Networking and Mesh Networking
- VPN network management
- Device and link status monitoring
- Support branch device onboarding via ZTP, customizable ZTP template
- Easy SD-WAN business deployment

## vHSM

- Support VMware WorkStation, EXSi, KVM
- Support AWS platform

# Specifications

## HSM Appliance Specification

	HSM-500-D4	HSM-100-D4
Log Performance	5,000 EPS	2,500 EPS
Devices Supported (Default / Max.) <sup>(1)</sup>	15 / 500	15 / 150
Storage Capacity	4 TB	2 TB
Fixed I/O Ports	2 x GE	2 x GE
RAID Levels	RAID 5	RAID 0
Power Supply	Single/dual 550W	Single 450W
Height	1U	1U

## Virtual Appliance (vHSM) Specification

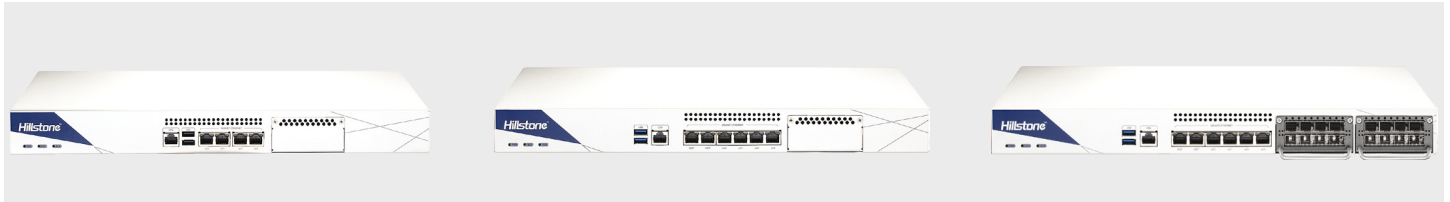
	15/25	15/100	15/500	15/1000
Log Performance	1,000 EPS	2,000 EPS	5,000 EPS	10,000 EPS
vCPU Requirement	4	8	18	24
Memory Requirement	4 GB	16 GB	32 GB	64 GB
Port Requirement	2 ports	2 ports	2 ports	2 ports
Hard Disk Requirement (Min.)	100 GB	2 TB	4 TB	8 TB
Virtual Environment Requirement	VMware Workstation/EXSi or KVM			

### NOTES:

(1) The default number of devices that HSM manages is only valid with the HSM platform license. It can be extended to the maximum number with the HSM extension license.

# Hillstone S-Series

## Network Intrusion Prevention System (NIPS)



As the threat landscape continues to evolve aggressively, an increasing number of network protection technologies have quickly emerged. Among these various technologies, Intrusion Prevention System (IPS) remains one of the most widely deployed solutions, regardless of platform or form factor.

Hillstone Network-based IPS (NIPS) appliance operates in-line, and at wire speed, performing deep packet inspection, and assembling inspection of all network traffic. It also applies rules based on several methodologies, including protocol anomaly analysis and signature analysis to block threats. Hillstone NIPS can be deployed in the network to inspect traffic left undetected by perimeter solutions, and is an integral part of network security systems for its high-performance, no compromise, best-of-breed protection capability and broad and flexible deployment scenarios.

### Product Highlights

#### Unparalleled Threat Protection without Performance Compromise

The Hillstone NIPS platform has the most comprehensive high performance inspection engine, combined with the best-of-breed signature partnering with leading technology partners, providing customers the highest threat detection rate with the lowest total cost of ownership (TCO). Hillstone IPS engine has 99.6% blocking rate of static exploits and 98.325% blocking rate of live exploits (reported by NSS Labs).

The Hillstone NIPS platform provides high throughput, low latency and maximum availability to maintain efficient security operations without compromising network performance. NIPS combines protocol analysis, threat reputation and other features that deliver threat protection from Layer 2 to Layer 7, including ARP attack, Dos/DDoS attack, abnormal protocols, malicious URLs, malwares and web attacks.

#### Granular Reporting with User Targeted Viewpoints

Hillstone NIPS provides comprehensive visibility based on protocol, application, user and content. It can identify more than 4,000 applications, including hundreds of mobile and cloud applications.

Bringing multiple sources together, the system can identify contextual information to make proper blocking decisions. With a granular and robust reporting function, it offers visibility across different views:

- Unique templates, based on whether you are a business system administrator, a security administrator or the CIO or executive.
- Organized Threat Content – whether a security, system risk, network threat or traffic view – in order to help you clearly understand the risk and make the right decision.

## Product Highlights (Continued)

### Ease of Deployment and Centralized Management

Deploying and managing the Hillstone NIPS is simple, with minimum overhead. It can be deployed in the following modes to meet security requirements and ensure optimal network connectivity:

- Active protection (intrusion prevention mode), real time monitoring and blocking.
- Passive detection (intrusion detection mode), real time monitoring and alert.

The Hillstone NIPS can be managed by the Hillstone Security Management Platform (HSM). Administrators can centrally register, monitor, and upgrade NIPS devices deployed in different branches or locations, with a unified management policy across the network for maximum efficiency.

## Features

### Intrusion Prevention

- 12,700+ signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
- IPS Actions: monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time
- Packet logging option
- Filter based selection and review: 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
- Support web server protection, including CC attack, external link attack, iframe, cross-site request forgery (CSRF) attack, sensitive file scanning attack, etc.
- Support protection of brute force attack including FTP, MSRPC, POP3, SMTP, SUNRPC, telnet, VNC, RDP, SSH, SMB, LDAP and IMAP
- Support weak password detection for FTP, MSRPC, POP3, SMTP, SUNRPC and telnet
- Threat Details support URI and Attack Data Decoding
- Support MPLS frame inspection
- Support scanning and parsing base64-encoded data

### Threat Correlation Analytics

- Correlation among unknown threats, abnormal behavior and application behavior to discover potential threat or attacks
- Multi-dimension correlation rules, automatic daily update from the cloud

### Advanced Threat Detection

- Behavior-based advanced malware detection
- Detection of more than 2000 known and unknown malware families including Virus, Worm, Trojan, Spyware, Overflow etc
- Real-time, online, malware behavior model database update

### Abnormal Behavior Detection

- Behavior modeling based on L3-L7 baseline traffic to reveal anomalous network behavior, such as HTTP scanning, Spider, SPAM, SSH/FTP weak password, and spyware
- Detection of DDoS including Flood, Sockstress, zip of death, reflect, DNS query, SSL DDoS and application DDoS
- Supports inspection of encrypted tunneling traffic for unknown applications
- Real-time, online, abnormal behavior model database update

### Antivirus

- Manual, automatic push or pull signature updates
- Flow-based antivirus: protocols include HTTP/HTTPS, SMTP, POP3, IMAP, FTP/SFTP, SMB, support virus filtering and blocking of files transferred with SMB

- protocol when resuming from breakpoint
- Compressed file virus scanning

### Attack Defense

- Abnormal protocol attack defense
- Anti-DDoS/DDoS, including SYN Flood, DNS Query Flood defense
- ARP attack defense
- IP scanning and port scanning

### 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 allow/block list
- Customizable alarm

### Anti-Spam

- Real-time spam classification and prevention
- Confirmed spam, suspected spam, bulk spam, valid bulk
- Protection regardless of the language, format, or content of the message
- Support both SMTP and POP3 email protocols
- Inbound and outbound detection
- Whitelists to allow emails from trusted domain/email addresses
- User-defined blacklists

### 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

### Data Security

- Web content filtering and file content filtering
- Support file filtering with over 100 file formats
- Support network behavior recording



## Features (Continued)

### 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
- Regular IP reputation signature database upgrade

### 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, monitor
- Provide multi-dimensional monitoring and statistics for applications running in the cloud, including risk category and characteristics
- Support encrypted application

### Quality of Service (QoS)

- Support encrypted application
- 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

### 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, Antivirus, Access control, ND attack defense

### VSYS

- System resource allocation to each VSYS
- CPU virtualization
- Non-root VSYS support IPS, URL filtering, Policy, QoS, etc.
- VSYS monitoring and statistics
- Support backup of all VSYS configurations at once

### SSL Proxy

- SSL offload: SSL traffic decryption
- SSL require/ exempt: SSL traffic allowed or block based on the policy rules without decryption

### Flexible Traffic Analysis and Control

- Support 3 operation modes: Route/NAT (layer 3), Transparent (layer 2) with optional bypass interface, and TAP mode (IDS Mode) with Hillstone Firewall Integration
- Traffic analysis and control based on policy rules by source/destination zone, source/destination IP address, users, service or applications

### High Availability

- Redundant heartbeat interfaces
- AP and peer 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

### Visible Administration

- Management access: HTTP/HTTPS, SSH, telnet, console
- Central Management: Hillstone Security Manager (HSM), web service APIs
- Two-factor authentication: username/password, HTTPS certificates file
- 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
- Storage device management: storage space threshold customization and alarm, old data overlay, stop recording.
- Language support: English

### Logs and Reporting

- Logging facilities: local storage 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
- Comprehensive event logs: system and administrative activity audits, routing & networking, VPN, user authentications, WiFi related events
- Support displaying attack result and associated user account in threat logs
- Log aggregation: support aggregation of AV and C&C logs
- IP and service port name resolution option
- Brief traffic log format option
- Granular Reporting with User Targeted Viewpoints
  - HA Management/C-level View
  - Business System Owner View
  - Network Security Administrator View







### 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)
- Cloud-based threat intelligence push service
- Geographical distribution of external network attacks







### 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

## Specifications

	S600-IN 	S1060-IN 	S1200-IN 	S1560-IN 	S1900-IN 	S2100-IN 
IPS Throughput <sup>(1)</sup>	1 Gbps	3 Gbps	3 Gbps	4 Gbps	3.8 Gbps	5 Gbps
Maximum Concurrent Connections, TCP (Standard/with AEL) <sup>(2)</sup>	1 Million / 2 Million	1 Million / 2 Million	1.2 Million	1 Million / 2 Million	1.2 Million	2 Million
New Connections per Second, TCP <sup>(3)</sup>	17,800	31,000	40,000	32,000	49,000	64,000
Stoneshield	N/A	N/A	N/A	Yes	N/A	N/A
Virtual Systems (Default/Max)	0/5	0/5	0/5	0/5	0/5	0/5
Storage	1T	1T	500 GB	1T	500 GB	500 GB
Form Factor	1U	1U	1U	1U	1U	1U
Management Ports	2 x USB Port, 1 x Console Port	2 x USB Port, 1 x Console Port	2 x USB port, 1 x MGT port, 1 x Console port	2 x USB Port, 1 x Console Port	2 x USB Port, 1 x MGT, 1 x Console Port	2 x USB port, 1 x MGT port, 1 x Console port
Fixed I/O Ports	4 x GE (including 2 pairs Bypass port)	4 x GE (including 2 pairs Bypass port)	2x SFP+, 8 x SFP, 8 x GE	4 x GE (including 2 pairs Bypass port)	8 x GE (including 1 pair Bypass port)	2x SFP+, 8 x SFP, 8 x GE
Available Slots for Expansion Modules	1 x Generic Slot	1 x Generic Slot	N/A	1 x Generic Slot	N/A	N/A
Expansion Module Option	IOC-S-4SFP-L-IN IOC-S-4GE-B-IN	IOC-S-4SFP-L-IN IOC-S-4GE-B-IN	N/A	IOC-S-4SFP-L-IN IOC-S-4GE-B-IN	N/A	N/A
Latency	<100 μs	<100 μs	<300μs	<100 μs	<70μs	<350 μs
Bypass Support (Default/Max.)	4/8	4/8	N/A	4/8	2/2	N/A
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100~240V 50/60Hz	AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz
Maximum Power Consumption	1 x 60W	1 x 60W	50W 1 x AC power supply (default) 2 x AC power supply (optional)	1 x 60W	50W 1 x AC power supply (default) 2 x AC power supply (optional)	50W 1 x AC power supply (default) 2 x AC power supply (optional)
Dimension (W×D×H, mm)	16.9 × 11.8 × 1.7 in (430×300×44mm)	16.9 × 11.8 × 1.7 in (430×300×44mm)	17.3 × 12.6 × 1.7 in (440× 320× 44mm)	16.9 × 11.8 × 1.7 in (430×300×44mm)	17.1×12.6×1.7 in (436× 320× 44mm)	17.3×12.6×1.7 in (440×320×44mm)
Weight	14.3 lb (6.5 kg)	14.3 lb (6.5 kg)	17 lb (7.7 kg)	14.3 lb (6.5 kg)	14.33 lb (6.5kg)	16.9 lb (7.7kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	5-85% (no dew)	5-85% (no dew)	10%~95%(no dew)	5-85% (no dew)	10%~95% (no dew)	10%~95% (no dew)

# Specifications (Continued)

	<b>S2300-IN</b> 	<b>S2700-IN</b> 	<b>S3500-IN</b> 	<b>S3900-IN</b> 	<b>S5500-IN</b> 	<b>S5560-IN</b> 
<b>IPS Throughput <sup>(1)</sup></b>	9 Gbps	12 Gbps	17 Gbps	25 Gbps	45 Gbps	50 Gbps
<b>Maximum Concurrent Connections, TCP (Standard/with AEL) <sup>(2)</sup></b>	3 Million	6 Million	8 Million	12 Million	24 Million	8 Million / 10 Million
<b>New Connections per Second, TCP <sup>(3)</sup></b>	61,000	65,000	135,000	320,000	652,000	664,000
<b>Stoneshield</b>	N/A	N/A	N/A	N/A	N/A	Yes
<b>Virtual Systems (Default/Max)</b>	0/5	0/50	0/50	0/50	0/50	0/100
<b>Storage</b>	500 GB	500 GB	1T	1T	1T	1T
<b>Form Factor</b>	1U	1U	1U	1U	1U	2U
<b>Management Ports</b>	2 x USB Port, 1 x MGT port, 1 x Console Port , 1 HA port	2 x USB Port, 1 x MGT port, 1 x Console Port , 1 HA port	2 x USB Port, 1 x MGT port, 1 x Console Port , 1 HA port	2 x USB port, 1 x MGT port, 1 x Console port , 2 HA port (SFP+)	2 x USB port, 1 x MGT port, 1 x Console port , 1 HA port (SFP+)	2 x USB Port, 2 x MGT, 1 x Console Port
<b>Fixed I/O Ports</b>	2 x SFP+, 8 x SFP, 16 x GE (including 2 pairs Bypass port)	2 x SFP+, 8 x SFP, 16 x GE (including 2 pairs Bypass port)	2 x SFP+, 8 x SFP, 16 x GE (including 2 pairs Bypass port)	6 x SFP+, 16 x SFP, 8 x GE (including 2 pairs Bypass port)	2 x QSFP+, 16 x SFP+, 8 x GE (including 4 pairs Bypass port)	N/A
<b>Available Slots for Expansion Modules</b>	N/A	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot	4 x Generic Slot
<b>Expansion Module Option</b>	N/A	IOC-S-4SFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN IOC-S-2QSFP+-A-IN	IOC-S-4SFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN, IOC-S-2QSFP+-A-IN	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN	IOC-S-4GE-B-H-IN, IOC-S-4SFP-H-IN, IOC-S-8GE-B-H-IN, IOC-S-8SFP-H-IN, IOC-S-4SFP-B-H-IN, IOC-S-2SFP+-H-IN, IOC-S-4SFP+-H-IN, IOC-S-2SFP+-B-H-IN, IOC-S-4GE-4SFP-H-IN
<b>Latency</b>	<300μs	<300 μs	<300μs	<300 μs	<300 μs	<100 μs
<b>Bypass Support (Default/Max.)</b>	4/4	4/4	4/4	4/4	8/8	0/32
<b>Power Supply</b>	AC 100~240V 50/60Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz
<b>Maximum Power Consumption</b>	100W 1 x AC power supply (default) 2 x AC power supply (optional)	100W 1 x AC power supply (default) 2 x AC power supply (optional)	100W 2 x AC power supply (default) 2 x DC power supply (optional)	280W 2 x AC power supply (default) 2 x DC power supply (optional)	320W 2 x AC power supply (default) 2 x DC power supply (optional)	350W Redundancy 1 + 1
<b>Dimension (W×D×H, mm)</b>	17.2 × 17.2 × 1.7 in (436x 437x 44mm)	17.1×17.2×1.7 in (436x 320x 44mm, No including expansion module)	17.1×17.2×1.7 in (436x 320x 44mm, Including power module handle)	17.1×21.3×1.7 in (436x542x44mm)	17.1×21.3×1.7 in (436x542x44mm)	16.9 × 19.7 × 3.5 in (430×500×88mm)
<b>Weight</b>	20.7 lb (9.4 kg)	20.9 lb (9.5kg, Including accessories and all packages)	26.0 lb (11.8kg, Including accessories and all packages)	32.6 lb (14.8kg)	32.6 lb (14.8kg)	35.3 lb (16 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)	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)	10%~95% (no dew)	5-85% (no dew)

## Module Options

Module	IOC-S-4SFP-L-IN	IOC-S-4GE-B-IN	IOC-S-4GE-B-H-IN	IOC-S-4GE-4SFP-H-IN	IOC-S-8GE-B-H-IN
I/O Ports	4 x SFP Ports	4 x GE Bypass Ports	4 x GE Bypass Ports	4 x GE and 4 x SFP Ports	8 x GE Bypass Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.22 lb (0.1 kg)	0.33 lb (0.15 kg)	0.33 lb (0.15 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)

Module	IOC-S-8SFP-H-IN	IOC-S-4SFP-H-IN	IOC-S-2SFP+-H-IN	IOC-S-4SFP+-H-IN	IOC-S-4SFP-B-H-IN
I/O Ports	8 x SFP Ports	4 x SFP Ports	2 x SFP+ Ports	4 x SFP+ Ports	4 x SFP Bypass Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.55 lb (0.25 kg)	0.33 lb (0.15 kg)	0.33 lb (0.15 kg)	0.44 lb (0.2 kg)	0.88 lb (0.4 kg)

Module	IOC-S-2SFP+-B-H-IN	IOC-S-4SFP+-A-IN	IOC-S-2MM-BE-A-IN	IOC-S-2SM-BE-A-IN	IOC-S-2QSFP+-A-IN
I/O Ports	2 x SFP+ Bypass Ports	4 x SFP+, SFP+ module not included	4 x SFP, MM bypass (2 pairs of bypass ports)	4 x SFP, SM bypass (2 pairs of bypass ports)	2 x QSFP+
Dimension	1U (Occupies 1 generic slot)	1U	1U	1U	1U
Weight	0.88 lb (0.4 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)

### NOTES:

- (1) IPS throughput data is obtained under HTTP traffic with all IPS rules being turned on;
- (2) Maximum concurrent connections are obtained under TCP traffic; and it can be upgraded with Additional Enhanced License (AEL);
- (3) New Connections per Second are obtained under TCP traffic with all IPS rules being turned on.
- Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R5. Results may vary based on StoneOS® version and deployment.

# Hillstone W-Series

## Web Application Firewall



Hillstone W-Series Web Application Firewall (WAF) provides enterprise-class, comprehensive security for web servers, applications and APIs. It defends against attacks at both the network and application layers, providing protections against DDoS, the OWASP Top 10 threats, and bot attacks, for example. In addition, the WAF validates APIs against the schema defined in OpenAPI, and automatically generates positive security model policies to detect and defend against attacks and misuse.

Hillstone WAF combines traditional rules-based detection with innovative semantics analysis. This dual-engine approach significantly increases accuracy while minimizing false positives. Hillstone WAF also leverages machine learning technology to fine tune security policies and block unknown threats and attacks. Further, logs can be automatically aggregated across multiple dimensions to allow admins to easily identify suspicious anomalies or locate false positives, and then further refine policies as needed.

## Product Highlights

### Comprehensive Web Application Security

Hillstone Web Application Firewall (WAF) provides complete security of web-based applications and APIs for enterprises and other organizations. It detects and defends against attacks at both the network layer (such as DDoS attacks, flood attacks, scan and spoof, etc.), and at the application layer (such as the OWASP Top 10 risks including injection attacks, cross site scripting (XSS) attacks, injection, etc). Hillstone WAF automatically discovers web servers and related assets and puts them under protection. With this capability, Hillstone WAF covers the entire web estate even when it scales, which helps improve operational efficiencies and deliver faster time-to-value.

As the digital transformation continues to evolve, APIs play a more and more important role in application development and integration. The popularity of APIs potentially exposes additional attack surfaces, such as excessive data exposure, lack of resources and rate limiting, injection and XSS attacks among API calls, etc. Based on the schema defined in the OpenAPI files, Hillstone WAF helps validate and generate positive security model policies to detect those threats in APIs.

### Improved Detection Accuracy and Efficiency with Dual Engines

Hillstone WAF integrates the industry's most innovative semantics analysis with traditional WAF detection engines. Combined with traditional rules-based detection, the semantics analysis engine helps further detect threats like SQL injection and cross site scripting, and minimizes false pos-

### Advanced API Protection

[www.HillstoneNet.com](http://www.HillstoneNet.com)

## Product Highlights (Continued)

itives. Hillstone WAF's recursive decoding capability also detects attacks that are obscured by multiple encoding. This dual-engine approach significantly improves the accuracy of detection and efficiency in operation.

### Machine-Learning-Driven Security Rule Optimization and Unknown Attack Defense

In addition to general protection based on rules and scripts for known attacks, Hillstone WAF's auto-learning capability helps mitigate never-before-seen exploits to protect specific applications from zero-day attacks. Its ML-based model learns from the data of normal traffic such as parameter length, cookie, HTTP methods, etc., tunes itself based on the test results as well as input from administrators, and continues updating the learning models and optimizing WAF rules as applications evolve. It significantly reduces operational

overhead by eliminating the troubleshooting of false positives and manual policy tuning.

### Rich Logs for Intelligent Analysis and Reporting

Hillstone WAF provides administrators and operators high visibility and comprehensive report with threat analysis, traffic analysis, attack breakdown and threat control. Its log aggregation capability allows logs to be aggregated from multiple dimensions, which helps operators easily identify suspicious anomalies or find false positives from logs, and then tune the policies accordingly.

## Features

### Web Application Protection

- Defend against HTTP anomalies
- SSL transparent proxy
- HTTP fast flood and slow flood attacks defense
- Injection attacks defense, including SQL injection, LDAP injection, SSI injection, Xpath injection, Command injection, Remote File Include (RFI) injection, etc.
- Defend against cross-site attacks, including XSS and CSRF attacks
- Semantic analysis based detection of SQL injection and XSS attacks
- Prevention of data leakage, including leakage of server error, database error, Web directory content, code, keyword, etc.
- Prevent leakage of sensitive personal data. Support detection the leakage of personal identification, number of bank card, credit card, and email account. Support desensitization of sensitive information (replace with specified characters)
- Cookie security. Support prevention of cookie tampering and hijacking; support cookie signature and encryption
- Web access control ability, which can defend the behavior of scanning, crawling, and directory traversal
- Support fine-grained control of HTTP access based on client IP, by matching HTTP method, HTTP header, HTTP content type, HTTP protocol version, URI path, etc.
- Support defense against vulnerability attacks to web servers, web framework and web application
- Defense against illegal resource access, including illegal uploads, illegal downloads and hotlinking attacks; support illegal download control based on file size and MIME file type

- Defense against malware, including WebShell and Trojan attacks, etc.
- Defense against brute force attacks
- Support detecting and blocking client by its source IP (via X-forward-for) when deployed behind a load balancer or a proxy
- Support customized rules
- Pre-defined protection policy templates; support customized protection policies
- Real time update of signature databases
- Support API security detection and protection; Support validation based on OpenAPI specification documents
- Support advanced anti-crawler and bot traffic detection based on device fingerprint, CAPTCHA verification for suspicious traffic, and traffic blocking based on device fingerprint
- Support configuring site status as website maintaining
- Support batch operation of site configuration

### Anti-defacement

- Support two operating modes: learning mode and protection mode
- Similarity comparison of protected contents
- Support customized protected static web page types; support exception URL list for tamper resistance; Support duration and time setting for protection
- Support synchronization with servers and establish baseline by the built-in sync engine.
- Support monitoring of tampering and normal modification
- Support forensic of tampering

### Network Security Protection

- Support virtual patching based on vulnerability scan results or imported reports
- Defense against DoS attacks, including: Ping of Death attacks, Teardrop attack, IP fragmentation attack, Smurf and Fraggle attack, Land attack, ICMP large packet attack, etc.
- Defense against DNS query flooding attacks, support configuring alert level according to the source and destination address
- Protection against TCP abnormalities
- Protection against IP scanning/spoofing and port scanning
- Protection against flooding, including: ICMP flood, UDP flood, SYN flood, etc.
- Support IP reputation and blocking malicious IP
- Support policy control based on HTTP header, including: Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, Cookie, etc.
- Support HTTP2 in reverse proxy mode
- Support HTTPS decryption and IPv6 traffic detection in TAP mode

### IPv6

- Optimization of access control policy
- Support IPv4, IPv6 dual stack deployment. IPv4 and IPv6 addresses can be added as protected sites simultaneously

### Policy Auto-learning

- Support detection and protection of IPv6 traffic
- Intelligent learning of the traffic to the protected site, and tune the policies based on the learning results
- Learned contents including: dynamic URL address, URL parameter, HTTP access method, cookie and



## Features (Continued)

other information

- Support learning mode and protection mode; support auto switching to protection mode after learning

### Defense Response

- Support learning from the specific URL
- Support alarming only if a trigger behavior is executed
- Support blocking the behavior that break the security rules and responding with an alert page
- Support alert page customization
- Support redirecting the alert page to another URL
- Support adding whitelist (exception rule) via security logs, and support exception rules based on URL and source IP
- Support adding attacker to blacklist to block subsequent access
- Support IP and URL whitelist
- Support interaction with firewall to issue blacklist
- Support access control based on geoIP

### Deployment

- Support multiple deployment modes, including Transparent proxy mode, TAP mode, reverse proxy mode, one-arm reverse proxy mode and traction mode
- Web assets auto-discovery
- Support default site
- Support configuring non-interface IP to the site and ARP response in one-arm reverse proxy mode and reverse proxy mode
- Support graphical deployment wizard

### Virtualized Offering

- Supported Hypervisors: VMware, KVM, Openstack and Xen
- Support built-in Agent, such as VMware Tools and Cloud-init
- Support AWS, Azure, AliCloud
- Support HA deployment in public cloud environment (AliCloud, AWS)
- Support license management through LMS system
- Support Restful API
- Support hot-swappable NIC, SR-IOV and elastic scaling

### High Availability

- Active/ passive mode
- Active/ Active Peer Mode
- Support software Bypass (in transparent proxy mode)

### Application Acceleration and Server Load Balancing

- Support web Cache, page compression and TCP Multiplexing, SSL unloading, SSL proxy
- Support SSL hardware acceleration
- Support server load balancing (in reverse proxy mode), including weighted round-robin, least connection and IP Hash algorithm
- Server load balancing support IPv6
- Support server health check. Support customizing the URL object used by the health check
- Support using X-header as load balancing IP

### Network and Interface Configuration

- Support static routing
- Support interface aggregation
- Support VLAN sub-interface
- Support multiple vSwitches, virtual-wires
- Support LLDP

### Authentication

- Multi-level authorization, predefined roles including system administrators, operators, auditors, etc.
- Support local authentication, Radius and TACAS-C+

### Device Management

- Multiple management methods including: HTTP, HTTPS, SSH, Console, etc. Support configuration of trusted management host
- Support device status monitoring, including: summary and detail information of hard disk, storage, CPU utilization and temperature
- Support centralized management and firmware upgrade through Hillstone Security Management System (HSM)
- Support operation and maintenance tools such as ping/tcpdump/curl

### Log, Report and Alarm

- Rich log information, including device





management logs, network security logs, web security logs, tamper-proof logs, access control logs, auto-learning strategy logs, web access logs, etc.





- Support logging all HTTP headers in attack events, including URL, UserAgent, POST content, cookie, etc.
- Support logging server responses
- Supports alarming via e-mail, SNMP, SYSLOG, SMS, etc.
- Support reporting (report templates supported) from multi-dimensions such as security risk overview, site risk details, attack type details, site tampering analysis, site visits, summary of network layer attack, system operation status, PCI DSS compliance, etc.
- Support log aggregation according to policy or client IP
- Support intelligent log analysis, including threat analysis and false positive analysis, and optimization of security policy based on analysis results
- Support playback of attack, which can help administrators quickly analyze and locate the threats and attacks in network
- Support manual investigation of suspicious alerts and report false positives to CloudView
- Support deleting web security log
- Support log transfer via FTP
- Support user-defined report
- Support report exported in PDF, DOC format
- Support periodic export of report
- Mail server supports STARTTLS and SSL encrypted transmission
- Support user session tracking to add user name, session identifier and session identity value in logs
- Support sending reports via FTP and email
- Support weak password detection

### Dashboard

- Support full-screen display of statistical and detailed information of threats and risks
- Support displaying top threat events and the latest threat events
- Support displaying site threats by severity
- Support displaying the total number of sites and risky sites
- Support displaying site traffic trend

# Specifications

	W120S	W320S	W620S	W1120S
				
HTTP Throughput	600 Mbps	1 Gbps	1.5 Gbps	3.5Gbps
HTTP New Sessions	1,600	3,500	5,000	8,000
HTTP Maximum Transactions Per Second (TPS)	2400	5,500	7,000	10,000
Storage	480G SSD	480G SSD	480G SSD	480G SSD
RAM	4G	4G	8G	16G
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port	2 x USB Ports, 1 x MGT Port, 1 x Console Port	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port (SPF)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port (SPF)
Fixed I/O Ports	8 x GE (including 1 bypass pair)	8 x GE (including 1 bypass pair)	2 x SFP+, 8 x SFP, 16 x GE (including 2 bypass pairs)	2 x SFP+, 8 x SFP, 16 x GE (including 2 bypass pairs)
Available Slots for Expansion Modules	N/A	N/A	N/A	1
Expansion Module Option	N/A	N/A	N/A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A
Protected Sites	8	16	32	64
Protected IP/PORT Pairs	64	64	128	512
Power Specification	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Dual AC
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz
Form Factor	1U	1U	1U	1U
Dimension(WxDxH)	17.1x12.6x1.7 in (436.0*320.0*44.0mm)	17.1x12.6x1.7 in (436.0*320.0*44.0mm)	17.1x17.2x1.7 in (436.0*437.0*44.0mm)	17.1x17.2x1.7 in (436.0*437.0*44.0mm)
Weight	14.3 lb (6.5 kg)	14.3 lb (6.5 kg)	20.7 lb (9.4 kg)	26 lb (11.8 kg)
Operating Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10%-95% non-condensing	10%-95% non-condensing	10%-95% non-condensing	10%-95% non-condensing

	W1520S	W3320S	W5602S	W7320S
				
HTTP Throughput	4 Gbps	5 Gbps	7 Gbps	13 Gbps
HTTP New Sessions	10,000	14,000	22,000	45,000
HTTP Maximum Transactions Per Second (TPS)	15,000	22,000	33,500	70,000
Storage	480G SSD	960G SSD	960G SSD	960G SSD
RAM	16G	32G	32G	64G
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port (SPF)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 2 x HA Ports (SFP+)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 2 x HA Ports (SFP+)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port (SFP+)
Fixed I/O Ports	2 x SFP+, 8 x SFP, 16 x GE (including 2 bypass pairs)	6 x SFP+, 16 x SFP, 8 x GE (including 2 bypass pairs)	6 x SFP+, 16 x SFP, 8 x GE (including 2 bypass pairs)	2 x QSFP+, 16 x SFP+, 8 x GE (including 4 bypass pairs)
Available Slots for Expansion Modules	1	1	1	1
Expansion Module Option	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A
Protected Sites	128	256	512	512
Protected IP/PORT Pairs	512	1024	1024	4096
Power Specification	100W, Dual AC	280W, Dual AC	280W, Dual AC	300W, Dual AC
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz
Form Factor	1U	1U	1U	1U
Dimension(WxDxH)	17.1x17.2x1.7 in (436.0*437.0*44.0mm)	17.1x17.2x1.7 in (436.0*437.0*44.0mm)	17.1x17.2x1.7 in (436.0*437.0*44.0mm)	17.1x17.2x1.7 in (436.0*437.0*44.0mm)
Weight	26 lb (11.8 kg)	32.6 lb (14.8 kg)	32.6 lb (14.8 kg)	32.6 lb (14.8 kg)
Operating Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10%-95% non-condensing	10%-95% non-condensing	10%-95% non-condensing	10%-95% non-condensing

## Specifications: Virtual Appliance

	SG-6000-WV02	SG-6000-WV04	SG-6000-WV08	SG-6000-WV12
HTTP Throughput	1.2 Gbps	2.5 Gbps	5.5 Gbps	8 Gbps
HTTP New Sessions	2,800	5,800	14,000	20,000
HTTP Maximum Transactions Per Second (TPS)	3,000	6,500	16,000	22,000
vCPU Support	2 Core	4 Core	8 Core	12 Core
Storage (Min/Max)	100 GB/1 TB	100 GB/1 TB	100 GB/1 TB	100 GB/1 TB
RAM	4 GB	8 GB	16 G	24 G
Maximum Network Interface Support	10	10	10	10
Protected Sites	16	32	128	256
Protected IP/PORT Pairs	32	64	1024	1024

## Module Options



Module	IOC-W-4SFP+-A	IOC-W-2QSFP+-A	IOC-W-2MM-BE-A	IOC-W-2SM-BE-A
I/O Ports	4 x SFP+ Ports	2 x QSFP+ Ports	MM Bypass (2 pairs of bypass ports)	SM Bypass (2 pairs of bypass ports)
Dimension	1U	1U	1U	1U
Weight	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)

### NOTE:

HTTP protection performances are obtained under protection site configured and "Medium Protection Strategy" used.