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, OSPFv3, BGP with graceful restart, RIPv2)
- Static and policy-based routing
- Route controlled by application
- Support Service Level Agreement (SLA)-based WAN path control
- 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: MSRCP, 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-based 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 encyclo-pedia
- 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, appli-cation or protocol
- IP exemption from specific IPS signatures
- IDS sniffer mode
- Predefined prevention configuration
- IPS threat packet capture (with expansion storage only)

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
- Active bypass with bypass interfaces
- Support protection of brute force attacks including VNC, RDP, SSH, LDAP, IMAP, SMB
- Support protection of sensitive file scanning attack
- Support reverse shell detection

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(1)
- 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, domain name and URL
- Support TCP, HTTP, and DNS traffic detection
- Allow and block list based on IP address, domain name, and URL
- Support DGA and DNS tunnel detection
- Support DNS sinkhole

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 TLSV1.0, TLSV1.2, TLSV1.3
- 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
- Content filtering for predefined keywords and file contents
- IM identification and network behavior audit
- Filter files transmitted by HTTPS using SSL Proxy and SMB

Features (Continued)

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
- PnPVPN
- 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 A2715, A2815, A3000 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, OAuth2
- 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
- SSL VPN, ZTNA, WebAuth support Azure Active Directory (AD) authentication
- 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, RestfulAPI, NETCONF
- Central Management: Hillstone Security Manager (HSM), web service APIs
- System Integration: SNMP, syslog, alliance partnerships
- Rapid deployment: USB and email-based zero-touch provisioning(ZTP), local and remote script execution
- Dynamic real-time dashboard status and drill-in monitoring widgets
- Language support: English
- Administrator authentication: Active Directory and LDAP
- Support CLI access from WebUI

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 intranet access
- 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
- Support Restful APIs

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 [2]	1 Gbps	1 Gbps	4 Gbps	5 Gbps	5 Gbps	5 Gbps
NGFW Throughput [3]	400 Mbps	400 Mbps	1.5 Gbps	1.7 Gbps	1.7 Gbps	2.5 Gbps
Threat Protection Throughput [4]	200 Mbps	200 Mbps	800 Mbps	800 Mbps	800 Mbps	2 Gbps
Maximum Concurrent Sessions [5]	450,000	450,000	450,000	450,000	1.5 Million	1.85 Million
New Sessions/s [6]	14,000	14,000	48,000	48,000	48,000	120,000
IPS Throughput [7]	610 Mbps	610 Mbps	3 Gbps	2.8 Gbps	2.8 Gbps	3 Gbps
AV Throughput [8]	550 Mbps	550 Mbps	1.8 Gbps	1.8 Gbps	1.7 Gbps	3.4 Gbps
IPsec VPN Throughput [9]	0.59 Gbps	0.59 Gbps	2.5 Gbps	2.7 Gbps	2.7 Gbps	3 Gbps
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 [10]	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/ 4G Dongle	4G Dongle	Wifi (IEEE802.11a/b/ g/n/ac), 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle
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	AC 100-240 V 50/60 Hz
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-A2715-IN	SG-6000-A2800-IN	SG-6000-A2815-IN
				
Firewall Throughput [2]	10 Gbps	10 Gbps	16 Gbps	16 Gbps
NGFW Throughput [3]	4 Gbps	4.5 Gbps	5 Gbps	5 Gbps
Threat Protection Throughput [4]	2.5 Gbps	2.5 Gbps	2.8 Gbps	2.8 Gbps
Maximum Concurrent Sessions [5]	2.2 Million	2.2 Million	2.4 Million	2.4 Million
New Sessions/s [6]	130,000	130,000	130,000	130,000
IPS Throughput [7]	8 Gbps	9 Gbps	9 Gbps	9 Gbps
AV Throughput [8]	4.5 Gbps	4.5 Gbps	4.5 Gbps	4.5 Gbps
IPsec VPN Throughput [9]	5 Gbps	5.2 Gbps	5.5 Gbps	5.3 Gbps
Virtual Systems (Default/Max)	1/5	1/5	1/5	1/5
SSL VPN Users (Default/Max)	8/4,000	8/4,000	8/4,000	8/4,000
Ipsec Tunnel Number	6,000	6,000	6,000	6,000
Firewall Policy Number	12,000	12,000	12,000	12,000
Management Ports	1 × Console Port, 2 × USB3.0 Ports, 1× MGT Port (RJ45)	1 × Console port, 2 × USB3.0 ports, 1 × HA port (RJ45), 1 × MGT port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1× MGT Port (RJ45)	1 × Console port, 2 × USB3.0 ports, 1 × HA port (RJ45), 1 × MGT port (RJ45)
Fixed I/O Ports [10]	2 × SFP+, 8 × SFP, 8 × GE	8 × SFP, 8 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 8 × GE	8 × SFP, 8 × GE (including 2 bypass pairs)
Wi-Fi/ 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle
Available Slots for Expansion Modules	N/A	1	N/A	1
Expansion Module Option	N/A	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN	N/A	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN
Twin-mode HA	N/A	Yes	N/A	Yes
Local Storage	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
Power Specification	50W, Single AC (default), Dual AC (optional)	60W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)	60W, Single AC (default), Dual AC (optional)
Power Supply	AC 100-240V, 50/60 Hz	AC 100-240V, 50/60 Hz	AC 100-240V, 50/60 Hz	AC 100-240V, 50/60 Hz
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	440 x 320 x 44	440 × 340 × 44.4	440 x 320 x 44	440 × 340 × 44.4
Dimensions (W × D × H, inches)	17.3 x 12.6 x 1.7	17.3 × 13.4 × 1.75	17.3 x 12.6 x 1.7	17.3 × 13.4 × 1.75
Weight	9 lb (4.1 kg)	10.0 lb (4.55 kg)	9 lb (4.1 kg)	10.0 lb (4.55 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)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

Specifications (Continued)

	SG-6000-A3000-IN 	SG-6000-A3600-IN 	SG-6000-A3615-IN 	SG-6000-A3700-IN 	SG-6000-A3800-IN 	SG-6000-A3815-IN 
Firewall Throughput (2)	20 Gbps	20 Gbps	20 Gbps	20/30 Gbps	20/30 Gbps	20 Gbps
NGFW Throughput (3)	5.5 Gbps	5.5 Gbps	5.5 Gbps	6 Gbps	12 Gbps	13 Gbps
Threat Protection Throughput (4)	3 Gbps	3 Gbps	2.95 Gbps	3.1 Gbps	6 Gbps	6.5 Gbps
Maximum Concurrent Sessions (5)	3 Million	4.5 Million	4.5 Million	7 Million	8 Million	8 Million
New Sessions/s (6)	135,000	135,000	135,000	140,000	310,000	310,000
IPS Throughput (7)	10 Gbps	10 Gbps	10 Gbps	10 Gbps	16 Gbps	14 Gbps
AV Throughput (8)	5 Gbps	5.0 Gbps	5 Gbps	5.2 Gbps	9.4 Gbps	10 Gbps
IPsec VPN Throughput (9)	6 Gbps	6 Gbps	6 Gbps	6.5 Gbps	12 Gbps	12 Gbps
Virtual Systems (Default/Max)	1/50	1/100	1/100	1/250	1/250	1/250
SSL VPN Users (Default/Max)	8/4,000	8/8,000	8/8,000	8/10,000	8/10,000	8/10,000
IPsec Tunnel Number	8,000	10,000	10,000	20,000	20,000	20,000
Firewall Policy Number	20,000	20,000	20,000	20,000	40,000	40,000
Management Ports	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)	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 (10)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	8 × SFP, 8 × 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)	8 × SFP, 8 × GE (including 2 bypass pairs)
Wi-Fi/ 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle
Available Slots for Expansion Modules	N/A	N/A	2	1	1	2
Expansion Module Option	N/A	N/A	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-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-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	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-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
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	100W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	75W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Dual AC (default), Dual DC (optional)	90W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240V, 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240V, 50/60 Hz
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	436 × 437 × 44	436 × 437 × 44	436 × 459.5 × 44.4	436 × 437 × 44	436 × 437 × 44	436 × 459.5 × 44.4
Dimensions (W × D × H, inches)	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 18.1 × 1.75	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 18.1 × 1.75
Weight	13.2 lb (6 kg)	13.2 lb (6 kg)	13.7 lb (6.2 kg)	13.4 lb (6.1 kg)	15 lb (6.8 kg)	19.8 lb (8.98 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-A5155-IN	SG-6000-A5200-IN	SG-6000-A5255-IN	SG-6000-A5500-IN	SG-6000-A5555-IN
						
Firewall Throughput [2]	25/50 Gbps	25/50 Gbps	32/65 Gbps	32/65 Gbps	40/80 Gbps	40/80 Gbps
NGFW Throughput [3]	20 Gbps	20 Gbps	20 Gbps	22 Gbps	25 Gbps	27 Gbps
Threat Protection Throughput [4]	10 Gbps	11 Gbps	12 Gbps	14 Gbps	15 Gbps	17 Gbps
Maximum Concurrent Sessions [5]	9 Million	9 Million	15 Million	15 Million	18 Million	18 Million
New Sessions/s [6]	480,000	490,000	600,000	650,000	700,000	700,000
IPS Throughput [7]	20/30 Gbps	21/30 Gbps	25/35 Gbps	27/35 Gbps	30/40 Gbps	32/40 Gbps
AV Throughput [8]	15 Gbps	15 Gbps	20 Gbps	20 Gbps	25 Gbps	25 Gbps
IPsec VPN Throughput [9]	15 Gbps	18 Gbps	20 Gbps	25 Gbps	28 Gbps	30 Gbps
Virtual Systems (Default/Max)	1/250	1/250	1/250	1/250	1/250	1/250
SSL VPN Users (Default/Max)	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
Firewall Policy Number	40,000	40,000	40,000	40,000	60,000	60,000
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), 1 × HA port (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), 2 × HA ports (SFP+)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA port (SFP)
Fixed I/O Ports [10]	6 × SFP+, 16 × SFP, 8 × GE (including 2 bypass pairs)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 bypass pairs)	6 × SFP+, 16× SFP, 8 × GE (including 2 bypass pairs)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 bypass pairs)	6 × SFP+, 16× SFP, 8 × GE (including 2 bypass pairs)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 bypass pairs)
Wi-Fi/ 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle
Available Slots for Expansion Modules	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
Twin-mode HA	Yes	Yes	Yes	Yes	Yes	Yes
Local Storage	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
Power Specification	280W, Dual AC (default), Dual DC (optional)	300W, Dual AC (default), Dual DC (optional)	280W, Dual AC (default), Dual DC (optional)	300W, Dual AC (default), Dual DC (optional)	280W, Dual AC (default), Dual DC (optional)	300W, 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
Form Factor	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 × 437 × 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 × 17.2 × 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)	18.7 lb (8.5 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-A5600-IN	SG-6000-A5800-IN	SG-6000-A6800-IN	SG-6000-A7600-IN
				
Firewall Throughput [2]	60/85 Gbps	80/95 Gbps	200 Gbps	280/320 Gbps
NGFW Throughput [3]	35 Gbps	40 Gbps	55 Gbps	55 Gbps
Threat Protection Throughput [4]	20 Gbps	20 Gbps	30 Gbps	30 Gbps
Maximum Concurrent Sessions [5]	25 Million	30 Million	35 Million	42 Million
New Sessions/s [6]	900,000	1,000,000	900,000	900,000
IPS Throughput [7]	35 Gbps	45/80 Gbps	70 Gbps	70 Gbps
AV Throughput [8]	30 Gbps	32 Gbps	35 Gbps	35 Gbps
IPsec VPN Throughput [9]	36 Gbps	45 Gbps	45 Gbps	45 Gbps
Virtual Systems (Default/Max)	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
IPsec Tunnel Number	20,000	20,000	20,000	20,000
Firewall Policy Number	60,000	80,000	80,000	80,000
Management Ports	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 port (SFP)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA port (SFP)
Fixed I/O Ports [10]	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/ 4G Dongle	4G Dongle	4G Dongle	N/A	N/A
Available Slots for Expansion Modules	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
Twin-mode HA	Yes	Yes	Yes	Yes
Local Storage	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
Power Specification	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
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	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 × 21.3 × 1.7	17.2 × 21.3 × 1.7
Weight	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)
Relative Humidity	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
				
Names	4SFP+ Expansion Module for Back Panel	4SFP Multi-mode Bypass Expansion Module for Back Panel	4SFP Single-mode Bypass Expansion Module for Back Panel	2QSFP+ Expansion Module for Back Panel
I/O Ports (10)	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+
Dimension	1U	1U	1U	1U
Weight	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)

	IOC-A-F-4SFP+-IN	IOC-A-F-8SFP+-IN	IOC-A-F-8GE-IN
			
I/O Ports (10)	4SFP+ Expansion Module for Front Panel	8SFP+ Expansion Module for Front Panel	8GE (including 4 bypass pairs) Expansion Module for Front Panel
Dimension	1U	1U	1U
Weight	0.55 lb (0.25 kg)	0.62 lb (0.28 kg)	0.6 lb (0.27 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 Gbps via additional IOC-A-4SFP+-IN or IOC-A-2QSFP+-IN expansion module. The firewall throughput for A5100-IN/A5155-IN/A5200-IN/A5255-IN/A5500-IN/A5555-IN/A5600-IN/A5800-IN/A7600-IN can be increased to 50/50/65/65/80/80/85/95/320 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) SFP+ ports support SFP+ 10Gbps optical module, SFP 1000Mbps optical module and SFP 1000Mbps copper module; QSFP+ ports support 40GE 1×40Gbps module and can be split to 4 ×10Gbps tunnel.

All perimeter of A2715-IN/A2815-IN/A3615-IN/A3815-IN are obtained with additional IOC-A-F-4SFP+-IN or IOC-A-F-8SFP+-IN front panel expansion module. Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R10. Results may vary based on StoneOS® version and deployment.

Version: EX-08.01-NGFW-A-Series-V5.5R11-0824-EN-01