

# 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. 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.

Further, the system's unified threat detection and analytics engine coordinates across all built-in security mechanisms to dramatically enhance efficiency while reducing network latency.

## Product Highlights (Continued)

### 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. 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.



**Intrusion Prevention**



**IP Reputation**



**URL Filtering**



**Anti-Spam**



**Anti-Virus**



**Cloud Sandbox**



**Botnet C2 Prevention**

# Hillstone Networks Cyber Security Ecosystem

The A-series Next Generation Firewalls are part of a larger ecosystem of Cyber Security solutions by Hillstone Networks. Besides the barrage of Cyber Attacks enterprises must deal with daily, digital transformation also needs attention?



## Rapidly Evolving Infrastructure

In today's digitally transformed landscape, data centers have evolved beyond traditional on-premises confines, extending into the realms of cloud computing and edge devices. Combined with work-from-anywhere adoption, the result is a target-rich environment where hackers and nefarious actors now have an expansive attack surface and corresponding attack vectors.



## Fast Changing Threat Landscape

The expansive attack surface has become a goldmine and multi-stage, multi-layer attacks occur daily. Attackers are becoming more skilled and creative in their methods by using the same cutting-edge AI/ML tools to hone their art and deliver more sophisticated attacks. Ransomware, supply chain attacks, and zero-day vulnerabilities remain significant areas of concern.



## Increasing Complexity and Cost

Multifold increases in attack surfaces, frequency, and variety of attacks, along with complex network topology and deployment, are not necessarily matched by corresponding budget growth for security initiatives. Skill gaps are ubiquitous. CISOs are under pressure to provide increased protection while seeking available and qualified personnel and holding firms to a budget line.

## Integrative Cybersecurity

Hillstone's Integrative Cybersecurity eliminates gaps in protection that put your enterprise at risk and reduces layers of complexity and cost, from technology to solutions, to their delivery and functionality, across vendors and platforms. Hillstone's Integrative Cybersecurity solutions bring coverage, control, and consolidation to secure the digital transformation at global scale:

### What is Integrative Cybersecurity?

Coverage, Control and Consolidation are the core tenets of an integrative cybersecurity solution.

**Coverage** – The mandate of the modern enterprise is to utilize the technology and infrastructure needed to grow and thrive. From containers to clouds and servers to SaaS, an integrative cybersecurity strategy provides adaptive protection for any environment, ensuring resilience against evolving threats.

**Control** – Maintaining the security and performance of enterprise technology is an exhausting balancing act. The right solution for the business isn't always the most recent or most-popular version, but it always needs to be secure. An integrative cybersecurity approach is adaptive and puts the enterprise in control.

**Consolidation** – Complex environments have attack surfaces that sprawl and edges that evaporate. Mitigating every attack vector with individual solutions creates opaque and siloed security operations that are both porous and inefficient. An integrative cybersecurity approach reduces complexity through consolidation.

# Hillstone Networks CyberSecurity Ecosystem

(Continued)

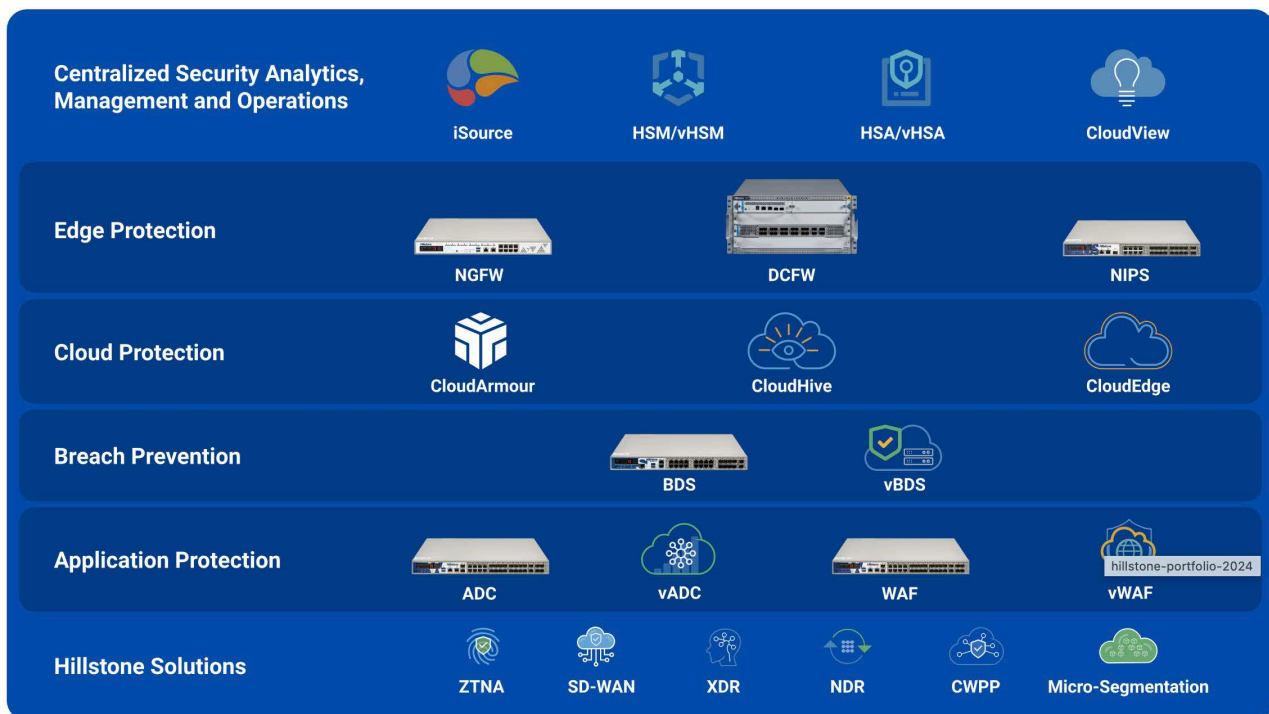
Management of Enterprise Cyber Security has matured. Hillstone Networks includes the Hillstone Security Manager, iSource, CloudView and Hillstone Security Audit platform. These overlay the perimeter, virtual and cloud environments within the enterprise.

**The key areas of focus are:**

- **Edge Protection** including our Next Generation Firewalls, Data Centre Firewalls and Network Intrusion Prevention Systems
- **Cloud Protection** including Cloud Armour, CloudHive and CloudEdge. These cover Virtual environments, Cloud and Hybrid Cloud
- **Breach Prevention** providing deeper protection in the data center and the network using Machine Learning
- **Application Protection** which includes security in conjunction with load balancing your critical servers and applications

**Our ecosystem expands with these Integrative Cyber Security solutions:**

- Zero Trust Network Access including SASE
- SD-WAN
- XDR or Extended Detection & Response
- Cloud Workload Protection Platform - CWPP
- Micro-Segmentation



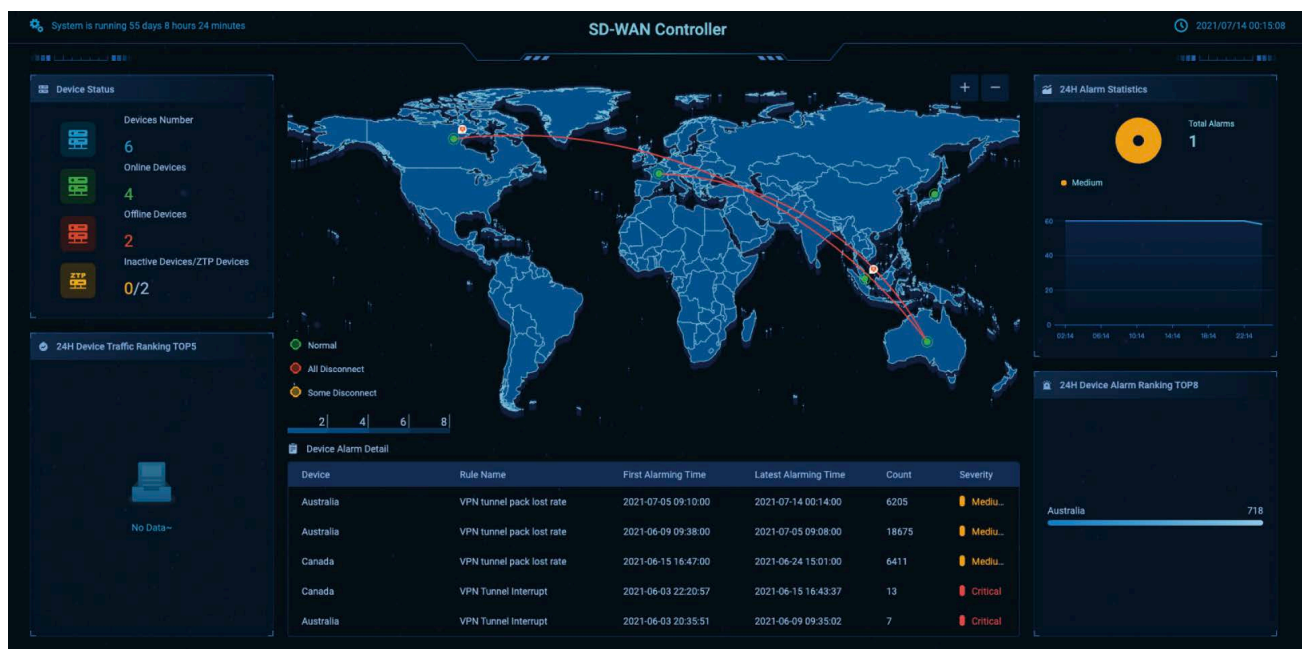
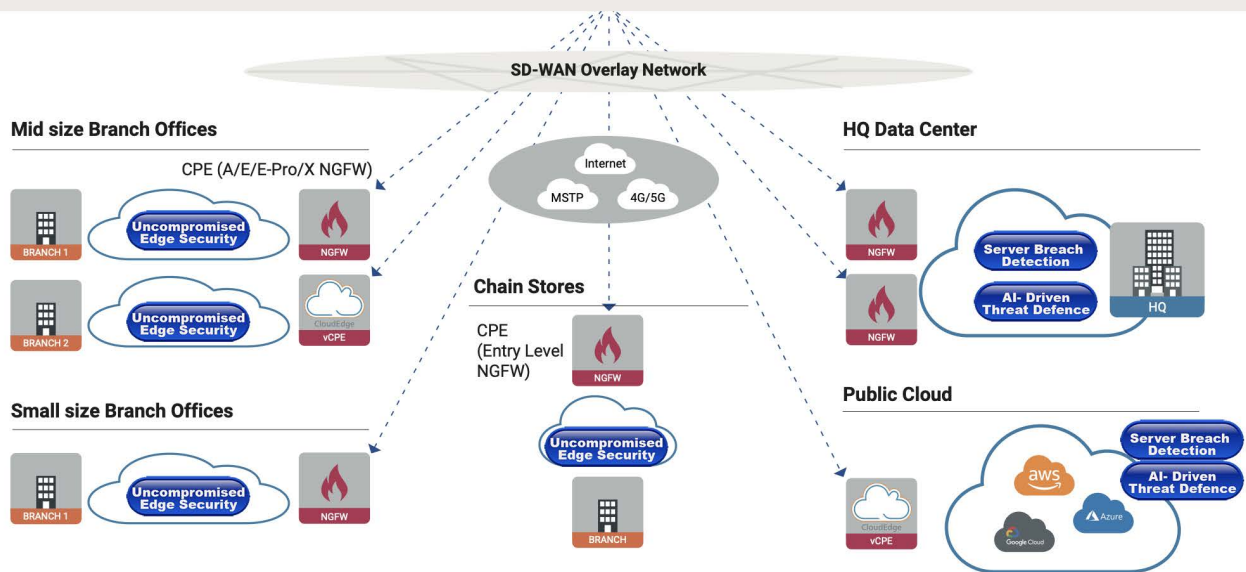
For the figure above note the following acronyms:

- NGFW - Next Generation Firewall
- HSM - Hillstone Security Manager
- HSA - Hillstone Security Audit Platform
- DCFW - Data Center Firewall
- BDS - Breach Detection System
- ADC - Application Delivery Controller
- WAF - Web Application Firewall

# Hillstone Networks CyberSecurity Ecosystem

(Continued)

## SD-WAN Architecture:



## Features

### Network Services

- Dynamic routing (OSPF, BGP, RIPv2)
- Static and policy routing
- Route controlled by application
- Built-in DHCP, NTP, DNS Server and DNS proxy
- Tap mode – connects to SPAN port
- Interface modes: sniffer, port aggregated, loopback, VLANS (802.1Q and Trunking)
- L2/L3 switching & routing
- Multicast (PIM-SSM)
- Virtual wire (Layer 1) transparent inline deployment

### Firewall

- Operating modes: NAT/route, transparent (bridge), and mixed mode
- Policy objects: predefined, custom, aggregate policy, object grouping
- Security policy based on application, role and geo-location
- Application Level Gateways and session support: MSRPC, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
- NAT and ALG support: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- NAT configuration: per policy and central NAT table
- VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holding
- Global policy management view
- Security policy redundancy inspection, policy group, policy configuration rollback, aggregate policy
- Policy Assistant for service based or application based policy generation
- Policy analyzing and invalid policy cleanup
- Comprehensive DNS policy
- Schedules: one-time and recurring
- Support policy import and export

### 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)

### 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
- ARP spoofing and ND spoofing defense
- Scan and spoof defense, including IP address spoof, IP address sweep, port scan
- DoS/DDoS defense, 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
- 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
- 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 4,000 applications that can be filtered by name, category, subcategory, technology and risk
- Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference
- Actions: block, reset session, monitor, traffic shaping

## Features (Continued)

- 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), 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 1,2,5,19,20,21,24
  - IKEv2 support DH group 1,2,5,14,15,16,19,20,21,24
  - XAuth as server mode and for dialup users
  - Dead peer detection
  - Replay detection
  - Autokey keep-alive for Phase 2 SA

- IPsec VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design)
- IPsec VPN 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
- 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
- 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 support
- 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/Passive, Active/Active 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
- Dual HA data link ports

### Twin-mode HA (only available on 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
- 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

### 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

## Features (Continued)

- 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)

### 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	SG-6000-A200W	SG-6000-A1000	SG-6000-A1100	SG-6000-A2000	SG-6000-A2600
<b>Firewall Throughput</b> <sup>(2)</sup>	1 Gbps	1 Gbps	4 Gbps	5 Gbps	5 Gbps	5 Gbps
<b>NGFW Throughput</b> <sup>(3)</sup>	300 Mbps	300 Mbps	1.2 Gbps	1.2 Gbps	1.2 Gbps	1.8 Gbps
<b>Threat Protection Throughput</b> <sup>(4)</sup>	200 Mbps	200 Mbps	800 Mbps	800 Mbps	800 Mbps	1.6 Gbps
<b>Maximum Concurrent Sessions</b> <sup>(5)</sup>	300,000	300,000	300,000	300,000	1 Million	1.2 Million
<b>New Sessions/s</b> <sup>(6)</sup>	15,000	15,000	48,000	48,000	48,000	120,000
<b>IPS Throughput</b> <sup>(7)</sup>	610 Mbps	610 Mbps	3.4 Gbps	3.7 Gbps	3.2 Gbps	4.5 Gbps
<b>AV Throughput</b> <sup>(8)</sup>	550 Mbps	550 Mbps	1.8 Gbps	2.0 Gbps	2.0 Gbps	3.7 Gbps
<b>IPsec VPN Throughput</b> <sup>(9)</sup>	0.62 Gbps	0.62 Gbps	2.5 Gbps	2.7 Gbps	2.7 Gbps	3 Gbps
<b>SSL Proxy Throughput</b> <sup>(10)</sup>	15 Mbps	15 Mbps	250 Mbps	250 Mbps	250 Mbps	750 Mbps
<b>Virtual Systems (Default/Max)</b>	N/A	N/A	N/A	N/A	1/5	1/5
<b>Firewall Policy Number</b>	4000	4000	4,000	4,000	8,000	12,000
<b>SSL VPN Users (Default/Max)</b>	8/128	8/128	8/128	8/128	8/1,000	8/1,000
<b>IPsec Tunnel Number</b>	512	512	2,000	2,000	4,000	6,000
<b>Management Ports</b>	1 × Console Port, 2 × USB 2.0 Ports	1 × Console Port, 2 × USB 2.0 Ports	1 × Console Port, 2 × USB3.0 Port	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)
<b>Fixed I/O Ports</b>	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)
<b>Wi-Fi</b>	N/A	IEEE802.11a/b/g/n/ac	N/A	N/A	N/A	N/A
<b>Available Slots for Expansion Modules</b>	N/A	N/A	N/A	N/A	N/A	N/A
<b>Expansion Module Option</b>	N/A	N/A	N/A	N/A	N/A	N/A
<b>Twin-mode HA</b>	N/A	N/A	N/A	N/A	N/A	N/A
<b>Local Storage</b>	4 GB	4 GB	8 GB	8 GB	8 GB	8 GB
<b>Expansion Storage Options</b>	N/A	N/A	256 GB SSD	256 GB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD
<b>Power Specification</b>	24W, Single AC (default)	24W, Single AC (default)	30W, Single AC	50W, Single AC	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)
<b>Power Supply</b>	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
<b>Form Factor</b>	Desktop	Desktop	Desktop	Desktop	Rackmount, 1U	Rackmount, 1U
<b>Dimensions (W × D × H, mm)</b>	180 × 110 × 28	180 × 110 × 28	270 × 160 × 44	270 × 160 × 44	436 × 320 × 44	436 × 320 × 44
<b>Dimensions (W × D × H, inches)</b>	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
<b>Weight</b>	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)
<b>Working 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% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

# Specifications (Continued)

	 <b>SG-6000-A2700</b>	 <b>SG-6000-A2800</b>	 <b>SG-6000-A3000</b>	 <b>SG-6000-A3600</b>	 <b>SG-6000-A3700</b>	 <b>SG-6000-A3800</b>
<b>Firewall Throughput <sup>(2)</sup></b>	10 Gbps	16 Gbps	20 Gbps	20 Gbps	20 / 40 Gbps	20 / 40 Gbps
<b>NGFW Throughput <sup>(3)</sup></b>	2.59 Gbps	2.6 Gbps	1.8 Gbps	1.8 Gbps	1.8 Gbps	3.7 Gbps
<b>Threat Protection Throughput <sup>(4)</sup></b>	1.73 Gbps	1.83 Gbps	1.6 Gbps	1.6 Gbps	1.6 Gbps	2.8 Gbps
<b>Maximum Concurrent Sessions <sup>(5)</sup></b>	1,500,000	1,800,000	2 Million	3 Million	6 Million	8 Million
<b>New Sessions/s <sup>(6)</sup></b>	130,000	130,000	140,000	140,000	140,000	310,000
<b>IPS Throughput <sup>(7)</sup></b>	5 Gbps	5 Gbps	8.3 Gbps	8.5 Gbps	8.6 Gbps	17.5 Gbps
<b>AV Throughput <sup>(8)</sup></b>	4.2 Gbps	4.2 Gbps	4.9 Gbps	5.0 Gbps	5.2 Gbps	9.4 Gbps
<b>IPsec VPN Throughput <sup>(9)</sup></b>	5 Gbps	5.5 Gbps	6 Gbps	6 Gbps	6.5 Gbps	12 Gbps
<b>SSL Proxy Throughput <sup>(10)</sup></b>	800 Mbps	800 Mbps	950 Mbps	950 Mbps	950 Mbps	2 Gbps
<b>Virtual Systems (Default/Max)</b>	5	5	1/5	1/50	1/100	1/100
<b>SSL VPN Users (Default/Max)</b>	8/1,000	8/1,000	8/2,000	8/4,000	8/6,000	8/8,000
<b>IPsec Tunnel Number</b>	6,000	6,000	8,000	10,000	16,000	20,000
<b>Firewall Policy Number</b>	12,000	12,000	20,000	20,000	20,000	40,000
<b>Management Ports</b>	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 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)
<b>Fixed I/O Ports</b>	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)
<b>Wi-Fi</b>	N/A	N/A	N/A	N/A	N/A	N/A
<b>Available Slots for Expansion Modules</b>	N/A	N/A	N/A	N/A	1	1
<b>Expansion Module Option</b>	N/A	N/A	N/A	N/A	IOC-A-4SFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2MM-BE, IOC-A-2SM-BE
<b>Twin-mode HA</b>	N/A	N/A	Yes	Yes	Yes	Yes
<b>Local Storage</b>	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB
<b>Expansion Storage Options</b>	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD
<b>Power Specification</b>	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)
<b>Power Supply</b>	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
<b>Form Factor</b>	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
<b>Dimensions (W × D × H, mm)</b>	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
<b>Dimensions (W × D × H, inches)</b>	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
<b>Weight</b>	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)
<b>Working 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% 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-A5200	SG-6000-A5500	SG-6000-A5600	SG-6000-A5800
Firewall Throughput <sup>(2)</sup>	32/65 Gbps	40/80 Gbps	60/85 Gbps	80/95 Gbps
NGFW Throughput <sup>(3)</sup>	15.84 Gbps	17.12 Gbps	30.84 Gbps	31.94 Gbps
Threat Protection Throughput <sup>(4)</sup>	11.37 Gbps	10.43 Gbps	19.13 Gbps	18.43 Gbps
Maximum Concurrent Sessions <sup>(5)</sup>	12,000,000	12,000,000	20,000,000	24,000,000
New Sessions/s <sup>(6)</sup>	400,000	500,000	800,000	930,000
IPS Throughput <sup>(7)</sup>	20/35 Gbps	25/40 Gbps	35/60 Gbps	45/75 Gbps
AV Throughput <sup>(8)</sup>	12 Gbps	15 Gbps	20 Gbps	25 Gbps
IPsec VPN Throughput <sup>(9)</sup>	20 Gbps	28 Gbps	36 Gbps	45 Gbps
SSL Proxy Throughput <sup>(10)</sup>	5 Gbps	5 Gbps	8.5 Gbps	8.5 Gbps
Virtual Systems (Default/Max)	250	250	500	500
SSL VPN Users (Default/Max)	8/10,000	8/10,000	8/10,000	8/10,000
IPsec Tunnel Number	40,000	40,000	40,000	40,000
Firewall Policy Number	40,000	60,000	60,000	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), 1 × HA port (SFP)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA port (SFP)
Fixed I/O Ports	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)
Wi-Fi	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	1	1	1	1
Expansion Module Option	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE
Twin-mode HA	Yes	Yes	Yes	Yes
Local Storage	64 GB	64 GB	64 GB	64 GB
Expansion Storage Options	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD
Power Specification	289W, Dual AC (default), Dual DC (optional)	289W, Dual AC (default), Dual DC (optional)	382W, Dual AC (default), Dual DC (optional)	382W, 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 × 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
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)
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+	IOC-A-2MM-BE	IOC-A-2SM-BE	IOC-A-2QSFP+
Names	4SFP+ Expansion Module	4SFP Multi-mode Bypass Expansion Module	4SFP Single-mode Bypass Expansion Module	2QSFP+ Expansion Module
I/O Ports	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)

### NOTES:

- (1) Anti-Spam feature is not available on SG-6000-A200 and SG-6000-A200W;
- (2) Firewall throughput data is obtained under UDP traffic with 1518-byte packet size. The firewall throughput for A3700 and A3800 can be increased from 20 Gbps to 40 Gbps via additional IOC-A-4SFP+ 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.

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R9. Results may vary based on StoneOS® version and deployment.