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.

Advanced API Protection

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-

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
- Support certificate chain integrity detection for HTTPS sites
- Support the forward of client certificates or related information via X-header for user authentication
- 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 infor - mation (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 and TCP) when deployed behind a load balancer or a proxy
- Support customized rules with global control and scheduling options
- 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 or forwarding
- Support batch operation of site configuration, including site, including site status, security policy alert, web access log status, site security policy, site access control policy
- Support protection for HTTP/HTTPS on the same IP and Port
- Supports extracting real source IP through X-Forward-For/ X-Real-IP, HTTP-specified request headers, TCP option, and Socket
- Automatically blocking/ alert malicious IPs that trigger configured conditions within a statistical period

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
- Support one-click network disconnection to block access to the website when tampering is detected

Network Security Protection

- 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 packet filtering based on source/ destination IP, source/destination security zones, services, and schedules, policy groups and policy optimization features such as hit analysis, redundancy detection, and policy assistant
- 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, IP-real-remote-addr, TCP-real-remote-port, IP-real-romote-addr-family, etc.
- Support HTTP2 in transparent, traction, one-arm and reverse proxy modes

Features (Continued)

- Support using the IPv6 address from the X-Header as client IP in 6to4 scenarios for security protection
- Support HTTPS decryption and IPv6 traffic detection in TAP mode
- Access control policy with time schedule

Policy Auto-learning

- Support detection and protection of IPv4/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 other information
- Support learning mode and protection mode; support auto switching to protection mode after learning
- Supports URL access counting and analysis via minimum/maximum/average access time
- Support exempting specific URLs from the automatic 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 rule based on URL, source IP, HTTP header, request line parameter, and request body; support exception rule based on both global and site-specific rule
- Support adding attacker to blacklist to block subsequent access
- Support IP and URL blacklists, as well as IP, URL, and domain whitelists
- Support dynamic IP whitelists based on schedules
- Support interaction with firewall to issue blacklist
- Support access control based on geoIP
- Support dynamic IP whitelists based on schedules

Deployment

- Support multiple deployment modes, including Transparent proxy mode, TAP mode, reverse proxy mode, one-arm reverse proxy mode and traction mode
- Support attack mitigation in TAP deployment mode
- Support transparent inspection mode without requiring changes to the network configuration, and support security check on MPLS traffic
- Web assets auto-discovery and add discovered sites as protected sites
- Support domain name-based filtering for site 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, Huawei Cloud, Tinayi Cloud, Tencent Cloud
- 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)
- Support multistage bypass
- Support engine detection timeout bypass
- Support overload protection based on hardware bypass in transparent proxy and transparent inspection modes
- Support Fail-open software bypass in transparent, reverse, one-arm, and traction proxy modes

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
- Support caching for HTTP GET, HEAD, POST, and PUT responses

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 role-based privilege management (system administrator, operator, and auditor)
- Administrator login supports multi-factor authentication: username and password, certificate, SMS, email
- Support authentication for administrators via local servers, RADIUS, and TACACS+
- Support device status monitoring, including: summary and detail information of hard disk, storage, CPU utilization and temperature
- Support centralized management via HSM (Hillstone Security Management) , including batch upgrades, rule database and version retrieval, certificate chain access, and site performance data reporting
- Support CLI in the webGUI
- Support system alert rules for CPU usage, memory utilization, and interface bandwidth
- Support operation and maintenance tools such as ping/tcpdump/curl/dpdump (tpdump and dpdump support SSL traffic capture and decryption)

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
- Web security log supports recording non-web attack traffic, with protection actions color-coded for easy identification
- Support manual investigation of suspicious alerts and report false positives to CloudView
- Support deleting web security log
- Support log transfer via FTP
- Configuration log storage and query support up to 12 months
- Support user-defined report
- Support report exported in PDF, DOC, HTML format
- The export of web security log supports filtering based on severity, sub-type and action
- 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

Features (Continued)

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
- Support displaying domain-based hit count and traffic statistics
- Support displaying hardware information including CPU utilization, memory utilization, storage status, chassis temperature, fan status, and power status
- Support displaying CPU and memory utilization for management plane, data plane, and detection engine
- Support displaying Top 10 site hit count, Top 10 site traffic, Top 10 domain hit count, Top 10 domain traffic, Web total traffic, Web engine traffic, Web engine TPS&CPS statistics, concurrent connection, access source, browser statistics, operation system statistics, access time, average time of engine detection, server response time, etc.

Specifications

	W120S-IN	W320S-IN	W620S-IN	W1120S-IN
				
L4 Throughput (1518 bytes) [1]	2.4 Gbps	4.5 Gbps	13 Gbps	26 Gbps (with 1 x IOC-W-4SFP+-A-IN)
HTTP Throughput [2]	600 Mbps	1 Gbps	1.5 Gbps	3.5Gbps
HTTP New Sessions [2]	1,600	3,500	5,000	8,000
HTTP Maximum Transactions Per Second (TPS) [2]	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 (SFP)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port (SFP)
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-IN IOC-W-2QSFP+-A-IN IOC-W-2MM-BE-A-IN IOC-W-2SM-BE-A-IN
Protected Sites	64	64	256	512
Protected Global Site Services	512	512	1024	4096
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)	17.1×12.6×1.7 in (436.0*320.0*44.0mm)	17.1×12.6×1.7 in (436.0*320.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 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-IN	W3320S-IN	W5620S-IN	W7320S-IN
				
L4 Throughput (1518 bytes) [1]	26 Gbps (with 1 x IOC-W-4SFP+-A-IN)	40 Gbps (with 1 x IOC-W-2QSFP+-A-IN)	55 Gbps (with 1 x IOC-W-2QSFP+-A-IN)	87 Gbps (with 1 x IOC-W-2QSFP+-A-IN)
HTTP Throughput [2]	4 Gbps	5 Gbps	7 Gbps	13 Gbps
HTTP New Sessions [2]	10,000	14,000	22,000	45,000
HTTP Maximum Transactions Per Second (TPS) [2]	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 (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, 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-IN IOC-W-2QSFP+-A-IN IOC-W-2MM-BE-A-IN IOC-W-2SM-BE-A-IN	IOC-W-4SFP+-A-IN IOC-W-2QSFP+-A-IN IOC-W-2MM-BE-A-IN IOC-W-2SM-BE-A-IN	IOC-W-4SFP+-A-IN IOC-W-2QSFP+-A-IN IOC-W-2MM-BE-A-IN IOC-W-2SM-BE-A-IN	IOC-W-4SFP+-A-IN IOC-W-2QSFP+-A-IN IOC-W-2MM-BE-A-IN IOC-W-2SM-BE-A-IN
Protected Sites	512	1024	1024	2048
Protected Global Site Services	4096	8192	8192	32768
Power Specification	100W, Dual AC	280W, Dual AC	280W, Dual AC	320W, 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)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 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-IN	SG-6000-WV04-IN	SG-6000-WV08-IN	SG-6000-WV12-IN
L4 Throughput (1518 bytes) (1)	5 Gbps	10 Gbps	20 Gbps	40 Gbps
HTTP Throughput (2)	1.2 Gbps	2.5 Gbps	5.5 Gbps	8 Gbps
HTTP New Sessions (2)	2,800	5,800	14,000	20,000
HTTP Maximum Transactions Per Second (TPS) (2)	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	64	256	512	512
Protected Global Site Services	256	512	8192	8192

Module Options

				
Module	IOC-W-4SFP+-A-IN	IOC-W-2QSFP+-A-IN	IOC-W-2MM-BE-A-IN	IOC-W-2SM-BE-A-IN
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:

(1) L4 throughput is obtained under WAF disabled, and no protection site configured (with SR-IOV enabled for virtual appliances);

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

Version: EX-08.01-W-Series-V4.0-0126-EN

Hillstone AX-Series:

Application Delivery Controller (ADC)



Hillstone AX Series Application Delivery Controllers (ADCs) are the next generation of enterprise-class application delivery optimization products. The Hillstone ADC supports a full range of load balancing functions, including link load balancing (LLB), server load balancing (SLB) and global server load balancing (GSLB). In addition, the AX Series supports health checks for applications, servers and links, first-level network attack protection, SSL offload, application and data acceleration via caching, and more. The Hillstone ADC can greatly improve the availability and scalability of core applications and business platforms, and effectively improve the operational efficiency of enterprise data centers. Together with Hillstone security products such as next-generation firewalls, the Hillstone ADC can provide end-to-end application delivery and security capabilities for your applications and business operations.

Hillstone's ADC fully supports IPv6, high-performance clustering and carrier-grade high availability. It is widely used in server load balancing; traffic distribution and business continuity across multiple data centers; link optimization across multiple ISPs; CDN traffic management; and other application optimization and acceleration scenarios. The Hillstone ADC provides industry-leading solutions for government, finance, network operators, education, healthcare and other sectors.

Product Highlights

High-performance Server Load Balancing

Hillstone's AX Series provides server load balancing with high-capacity concurrent and new session processing capabilities. It intelligently adjusts traffic distribution based upon the health status of server nodes, and automatically completes switching to ensure the best user experience as well as application high availability. Hillstone's ADC utilizes Layer 4 to Layer 7 load balancing algorithms and load balancing based on domain names. Intelligent application identification based on characteristics, behavior and other information allows fine-tuning of performance and throughput to support employee productivity. It also supports application-layer content switching and rewrite to improve the availability of both servers and applications.

Intelligent, Efficient and Dynamic Link Load Balancing

Hillstone's AX Series ADC offers enterprise-class link load balancing technology. It features an innovative adaptive link selection control algorithm that can detect link connectivity, bandwidth utilization, delay, packet loss and jitter in real time, and adjust the traffic forwarding rules based upon the actual link quality and performance. Using an intelligent closed loop, the best route can be selected in real time so that problems such as unbalanced link utilization, single point of failure, poor cross-ISP access, wastage of link resources, and other performance problems are eliminated. The Hillstone ADC supports multiple link load balancing modes such as ECMP, ISP routing, dynamic link switching, and application routing to ensure optimal link access and support employee productivity.

High-performance SSL Offload for Secured Applications

Finance, healthcare, e-commerce and other applications are commonly secured via SSL encryption, which adds workload to servers that can impact performance and limit scalability. Hillstone's ADC supports SSL hardware acceleration technology that provides industry-leading 2048-bit SSL processing performance. By offloading SSL traffic to the Hillstone ADC's dedicated SSL processing resources, the server workload is significantly reduced resulting in improved server performance and scalability.

Full-featured IPv6

In addition to IPv6 support, the Hillstone ADC supports IPv6 application layer transformation technology to help IPv4 websites and networks seamlessly upgrade to or interoperate with IPv6. Through intelligent link processing technology, the addressing problem can be solved efficiently. The Hillstone ADC standard configuration comes with a 1T hard drive and supports log storage for the IPv6 application layer transformation.

End-to-end Security Protection

Together with Hillstone Networks' next-generation firewalls, CloudEdge, CloudHive and other security products, the Hillstone ADC can provide end-to-end security protection capabilities from network access to data centers.

SSL Traffic Orchestration

Hillstone's AX Series ADC provides SSL traffic orchestration function including SSL visualization, service chaining, and security device pooling, avoiding redundant encryption/decryption to maximize security devices' performance. With this feature set, users can easily configure SSL traffic service chains tailored to their specific business and traffic requirements. SSL traffic orchestration enables seamless scalability and enhances network elasticity, allowing organizations to adapt effortlessly to evolving demands, and effectively addressing security blind spots and mitigating single points of failure.

Features

Server Load Balancing

- L4 and L7 server load balancing
- HTTP content switching based on URL, HTTP header, cookie, source/ destination IP, destination port, SSL/ TLS protocol and X509 certificate
- HTTP content rewriting, including external link rewriting
- Redirection for HTTP requests
- Supports Kubernetes
- Supports IPv6
- Supports HTTP2.0
- Supports WebSocket protocol
- Supports fast HTTP mode
- Supports ISO 8353 compatible message-based load balancing
- Supports RADIUS load balancing
- Supports MySQL load balancing with read/write splitting
- Supports node-based load balancing
- Supports HTTP Strict-Transport-Security (HSTS)
- Supports network mapping for visibility of relation between virtual servers , service pool, service pool members, and application servers
- Supports TCP template
- HTTPS virtual server supports HTTP redirection
- TOA supports format customization for source address insertion and extraction
- Support resetting the enabled functions when servers are down
- Virtual IP route advertisement over dynamic routing
- MySQL content switching based on source/ destination IP, destination port, database name, database account, and matching string
- Supports clustering up to 32 devices
- Supports SMTP/POP3/IMAP mail server, perform mail load balancing in three different modes: Plaintext, SSL, STARTTLS
- Supports connection number and connection rate limitation per virtual server/source IP
- Supports multiple certificates on a virtual server
- Supports verification of certificate chain integrity
- TCP Option extension supports IP version extraction and passthrough
- Supports displaying context correlation of L7 VS session
- Supports automatically convert iRules scripts (F5) to aRules scripts
- Supports load balancing and aRule programmable scripting for DNS

Server Health Checks

- Predefined and custom health checks for ICMP, TCP, TCP-Echo, TCP-Half-Open, UDP, HTTP, HTTPS, HTTP2, SMTP, POP3, IMAP, DNS (UDP and TCP), FTP, SSL, Radius-Authentication, Radius-Accounting, WebSocket, WebSocket-SSL, SNMP-DCA, SNMP-DCA-Base, SIP-UDP, SIP-TCP, Passive-HTTP, Passive-TCP, MYSQL, MSSQL, Oracle, OceanBase, LDAP, WMI, TiDB, TDSQL- MySQL, Gauss-MySQL, and Third-Party
- HTTPS health check supports specifying TLS version, cipher suite and mutual authentication
- HTTP2 health check supports correlating to SSL template for HTTP2 ciphertext detection
- Supports server resource health check
- Supports passive health check
- Supports display and statistics of health check history
- Health check logs can be delivered through SMTP and SMS

Server Session Persistence

- Source/ destination IP based and TOA based session persistence
- Supports session persistence for URL hash, HTTP/HTTPS, SMTP, POP3, HTTP header hash, session ID, request method, HTTP version, SIP CALL-ID, RDP, and Radius
- Supports session persistence for cookie including cookie hash, cookie insertion, cookie rewriting, and encrypted cookies
- Supports synchronization of session persistence table in a cluster
- Supports Set-cookie encryption and decryption
- Supports export of session persistence table
- Independent persistence profile for session persistence
- Session persistence table supports matching across virtual server + service pool, virtual IP, service pool, global, etc.

Application Acceleration

- HTTP caching (jpg, doc, ppt, xls, html, css, js, pdf, swf, mp3, avi, flv, mp4)
- TCP connection multiplexing
- Supports TCP acceleration
- HTTP compression (doc, ppt, xls, html, css, js)

SSL Inspection

- Software SSL offload; supported versions include SSLv2, SSLv3, TLS 1.0, TLS1.1, TLS1.2, TLS1.3
- SSL hardware acceleration
- Predefined or customized encryption algorithms with priorities
- SSL connection multiplexing
- Supports SSL proxy
- Works in conjunction with BDS, NIPS and WAF to identify encrypted traffic
- Supports mirroring decrypted SSL traffic

SSL Traffic Orchestration

- Supports SSL orchestration for inbound traffic
- Supports decryption, interception and orchestration of TLS1.0, TLS1.1, and TLS1.2 traffic
- Supports interception and orchestration of non-SSL traffic
- Supports bypassing or dropping the in-progress traffic when security devices in the service chain fail
- Supports traffic distribution to security devices
- Supports health check on security devices in the service chain
- Supports traffic orchestration information log
- Supports statistics and display of traffic processed by security devices in the service chain, including new traffic, concurrent traffic, throughput, etc.
- Supports L2 transparent deployment mode
- Service chain selection based on content switching rules
- Supports delivering traffic orchestration policy via Restful API
- Supports automatically bypass traffic to backend service pools for SSL offloading when traffic decryption fails

Link Load Balancing

- Supports IP address library and ISP address library with automatic update
- Policy routing supports domain name and geographic location routing
- Supports configuration of link priority and minimum active links
- Supports IPv6

Global Server Load Balancing

- DNS server supports A, AAAA, NS, CNAME, PTR, MX, TXT, SRV
- DNS server supports recursive forwarding
- DNS server supports DNS Response Policy Zone (RPZ)
- DNS supports transparent proxy deployment
- Supports slave DNS server pool, synchronizing data from master DNS server automatically or manually
- Supports DNS-over-HTTPS (DoH)
- Inbound SmartDNS
- SmartDNS supports IP address library, ISP address library with automatic updates, overloaded link detection and dynamic proximity load balancing, service pool lists and service pool members
- SmartDNS host scheduling algorithms for service pool selection: Round Robin, Weighted Round Robin, Static Proximity, and Global Availability
- SmartDNS host scheduling algorithms for service pool member selection: Round Robin, Weighted Round Robin, IP Hash, Static Proximity, All IPs, Priority, Dynamic Ratio, Global Availability, Backup IP
- SmartDNS supports configuration of multiple served regions per service pool/server (exclusion addresses/regions is allowed)
- Supports clustering multiple devices
- Supports monitoring of virtual server health status
- DNS resolution supports white-and-black list and rate limiting control
- Resource record types include A, AAAA, CNAME, MX, SRV

Features (continued)

- Supports configuring root DNS server
- Supports DNSSEC
- Supports Transaction Signature (TSIG)
- DNS cache supports setting Time-to-Live (TTL), clearing, viewing, and tracking hit statistic
- Supports user-defined syslog format
- Aligned with F5: Optional number of GSLB deployment per data center; Each data center can be enabled/disabled

System Management

- System management via WebUI, Console, Web Console, Telnet and SSH
- Restful API supports
- Supports Ansible for automated operation and maintenance management
- Role-based authorization of administrators, auditors and operators
- Access control on the administrator address for remote management
- Supports WebUI administrators to bind to trust domain, and certificate authentication for administrators
- Configuration for password complexity and minimum length restrictions
- Supports SNTP, and synchronization of system time from multiple NTP servers
- Supports multiple configuration files and configuration file backup and recovery
- Supports hping, tcpdump and curl operation and maintenance tools
- Supports SLB objects partition for administration with different privileges
- Supports continuous system operation during hard disk drive failures
- Supports multi-version image deployment (up to 3 images)
- Supports software and hardware maintenance through soft isolation
- Supports operation and maintenance tools including netstat/ echo/ top, and restart process command
- Download and export configuration files, syslog, and packet capture files through SFTP client

Application Identification

- Application identification based on application characteristics, behavior and related information
- Multi-dimensional application definitions
- Thousands of application signatures
- Application signature database updated in real-time

Log and Monitoring

- Supports a variety of log types, including event logs, network logs, configuration logs, NAT logs, SLB logs, health check logs, etc.
- Supports queries for L4/L7 load balancing logs and global load balancing logs within past hour, past day, past week, and custom time spans up to one week (a maximum of 100,000 entries can be exported)
- Log storage in both local device and server
- Email alarms and log alarms
- Real-time WebUI display of system resource utilization and hardware status
- Monitoring and graphical display of server load balancing status, including traffic, new connections, concurrent connections (established concurrent connections, client concurrent connections, server concurrent connections), requests per second and CPU utilization of virtual servers; supports displaying traffic, new connections, concurrent connections, requests per second, and other historical real-time information of each real server in the server pool
- Supports displaying historical information of the operational status of virtual servers, server pool members, and real servers
- Supports displaying statistical information of hit per second, total hit count, and last hit time for HTTP content switching
- Device status monitoring on mobile devices via CloudView
- Supports forwarding SLB log, health check binary log to HSA
- Supports multi-dimensional statistics and monitoring of HTTP traffic, including URL, client IP, response code, HTTP method, and user agent
- Supports reporting with multiple statistics, including business processing status, load balancing data, etc.
- Supports DNS traffic visualization based on domain/IP, displaying the top 10 total requests, successful resolutions, and failed resolutions
- Supports displaying historical statistical data of DNS traffic for the last hour
- Supports displaying top 10 users by traffic, concurrent connections, and session rate
- Link Aggregation Control Protocol (LACP) supports passive mode
- Supports configuration comparison

Deployment and Network Configuration

- Supports DNS proxy
- DNS proxy blacklist and whitelist
- Supports Botnet C&C prevention, including domain reputation library and DNS sinkhole capability
- Deployment via one-arm reverse proxy, routing, transparent, or DSR
- Supports static routing, ISP routing, policy routing, and RIP dynamic routing protocol, and supports import of ISP information
- HA AP mode, supports synchronization of configuration (auto/manual), session, health checks, PKI synchronization
- Policy control
- VSYS
- Supports AWS, Azure, Huawei Cloud and Alibaba Cloud (manual deployment only)
- Supports LMS centralized authorization
- Supports VMware / KVM / Xen / Hyper-V virtualization deployment
- QoS
- Session limiting
- Supports anti-DDoS
- Supports centralized management
- Supports programmable script aRules
- Supports SNMP
- Support setting configuration validity scope (local device/ within the cluster)
- Supports cluster manual/automatic configuration synchronization
- Supports cluster bi-directional configuration synchronization: synchronize configuration changes made on any device to the entire cluster or to specific devices within the cluster
- Supports F5 configuration migration tools:
  - F5 LTM module configuration conversion
  - Import and conversion of F5 UCS configuration files without decompression
  - Configuration comparison
  - Output conversion results/ error messages/ operation logs

Specifications

	SG-6000-AX120S-IN	SG-6000-AX220S-IN	SG-6000-AX320S-IN	SG-6000-AX520S-IN
				
L4 Throughput	3 Gbps	16 Gbps	18 Gbps	30 Gbps
L4 Connections/s	40,000	110,000	120,000	270,000
L7 HTTP Throughput	1.5 Gbps	5 Gbps	6 Gbps	10 Gbps
L7 HTTP Requests/s (RPS)	50,000	130,000	130,000	320,000
Concurrent Connections	1 Million	1 Million	3 Million	10 Million
RSA 2K SSL (CPS) (1)	200/950	600/3,500	600/3,500	1,800/8,000
RSA 2K SSL (RPS) (2)	5,000	17,000	17,000	52,000
RSA 2K SSL Throughput (3)	0.4 Gbps	1.5 Gbps	1.8 Gbps	4 Gbps
SSL Acceleration Technology	Hardware	Hardware	Hardware	Hardware
DNS (QPS)	19,000	39,000	40,000	95,000
Storage	480 GB SSD	480 GB SSD	480 GB SSD	960 GB SSD
Memory	4 GB	4 GB	8 GB	16 GB
Management Ports	2 × USB Ports, 1 × MGT Port, 1 × Console Port	2 × USB Ports, 1 × MGT Port, 1 × Console Port	2 × USB Ports, 1 × MGT Port,1 × HA, 1 × Console Port	2 × USB Ports, 1 × MGT Port,1 × HA, 1 × Console Port
GE Ports	8 (includes 1 pair bypass)	8 (includes 1 pair bypass)	16 (includes 2 pairs bypass)	16 (includes 2 pairs bypass)
GE Ports (SFP)	N/A	8	8	8
10GE (SFP+)	N/A	2	2	2, up to 6 with expansion module
40GE Ports (QSFP+)	N/A	N/A	N/A	0, up to 2 with expansion module
Available Slots for Expansion Modules	N/A	N/A	N/A	1
Expansion Module Option	N/A	N/A	N/A	IOC-A-4SFP+-IN IOC-A-2QSFP+-IN IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN
Power Supply	Single/ Dual AC, 100-240V	Single/ Dual AC, 100-240V	Single/ Dual AC, 100-240V	Dual AC, 100-240V, redundant hot-swappable
Frequency	50/60 Hz	50/60 Hz	50/60 Hz	50/60 Hz
Average Power	50W	50W	100W	100W
Height	1U	1U	1U	1U
Dimension (W×D×H)	17.2 x 12.6 x 1.7 in (436 x 320 x 44mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Net Weight	8.6 lb (3.9 kg)	9 lb (4.1 kg)	13.2 lb (6 kg)	15 lb (6.8 kg)
Gross Weight	14.3 lb (6.5 kg)	17 lb (7.7 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)
Storage Temperature	-40-158 °F (-40-70 °C)	-40-158 °F (-40-70 °C)	-40-158 °F (-40-70 °C)	-40-158 °F (-40-70 °C)
Allowed Relative Humidity	10-95%, non-condensing	5-85%, non-condensing	10-95%, non-condensing	10-95%, non-condensing

Specifications (Continued)

	SG-6000-AX1200S-IN	SG-6000-AX2000-IN	SG-6000-AX2000S-IN	SG-6000-AX2200S-IN	SG-6000-AX3200S-IN
					
L4 Throughput	70 Gbps	85 Gbps	85 Gbps	85 Gbps	90 Gbps
L4 Connections/s	700,000	1 Million	1 Million	1 Million	1.3 Million
L7 HTTP Throughput	20 Gbps	30 Gbps	30 Gbps	30 Gbps	35 Gbps
L7 HTTP Requests/s (RPS)	850,000	1.2 Million	1.2 Million	1.2 Million	1.45 Million
Concurrent Connections	20 Million	40 Million	40 Million	40 Million	40 Million
RSA 2K SSL (CPS) [1]	4,200/23,000	5,000	25,000	8,000/40,000	9,000/46,000
RSA 2K SSL (RPS) [2]	130,000	120,000	140,000	200,000	250,000
RSA 2K SSL Throughput [3]	8 Gbps	5.5 Gbps	6 Gbps	12 Gbps	15 Gbps
SSL Acceleration Technology	Hardware	Software	Hardware	Hardware	Hardware
DNS (QPS)	240,000	350,000	350,000	420,000	460,000
Storage	960 GB SSD	1TB HDD	1TB HDD	960 GB SSD	960 GB SSD
Memory	32 GB	64 GB	64 GB	64 GB	64 GB
Management Ports	2 × USB Ports, 1 × MGT Port,2 × HA, 1 × Console Port	2 × USB Ports, 1 × MGT Port,1 × HA, 1 × Console Port	2 × USB Ports, 1 × MGT Port,1 × HA, 1 × Console Port	2 × USB Ports, 1 × MGT Port,1 × HA, 1 × Console Port	2 × USB Ports, 1 × MGT Port,1 × HA, 1 × Console Port
GE Ports	8 (includes 2 pairs bypass)	2 (includes 2 MGT ports), up to 34 ports with expansion modules	2 (includes 2 MGT ports), up to 34 ports with expansion modules	8 (includes 4 pairs bypass)	8 (includes 4 pairs bypass)
GE Ports (SFP)	16	0, up to 32 with expansion module	0, up to 32 with expansion module	0	0
10GE(SFP+)	6, up to 10 with expansion module	0, up to 16 with expansion module	0, up to 16 with expansion module	16, up to 20 with expansion module	16, up to 20 with expansion module
40GE Ports (QSFP+)	0, up to 2 with expansion module	0, up to 8 with expansion module	0, up to 8 with expansion module	2, up to 4 with expansion module	2, up to 4 with expansion module
Available Slots for Expansion Modules	1	4	4	1	1
Expansion Module Option	IOC-AX-4SFP+-IN IOC-AX-2QSFP+-IN IOC-AX-2MM-BE-IN IOC-AX-2SM-BE-IN	IOC-AX-4GE-B-H-IN, IOC-AX-4SFP-H-IN, IOC-AX-8GE-B-H-IN, IOC-AX-8SFP-H-IN, IOC-AX-4GE4SFP-H-IN, IOC-AX-2SFP+-H-IN, IOC-AX-4SFP+-H-IN, IOC-AX-2QSFP+-H-IN	IOC-AX-4GE-B-H-IN, IOC-AX-4SFP-H-IN, IOC-AX-8GE-B-H-IN, IOC-AX-8SFP-H-IN, IOC-AX-4GE4SFP-H-IN, IOC-AX-2SFP+-H-IN, IOC-AX-4SFP+-H-IN, IOC-AX-2QSFP+-H-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
Power Supply	Dual AC, 100-240V, redundant hot-swappable	Dual AC, 100-240V, redundant hot-swappable	Dual AC, 100-240V, redundant hot-swappable	Dual AC, 100-240V, redundant hot-swappable	Dual AC, 100-240V, redundant hot-swappable
Frequency	50/60 Hz	50/60 Hz	50/60 Hz	50/60 Hz	50/60 Hz
Average Power	289W	550W	550W	382W	382W
Height	1U	2U	2U	1U	1U
Dimension (W×D×H)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)	21.7 x 17.3 x 3.5 in (550 x 440 x 88mm)	21.7 x 17.3 x 3.5 in (550 x 440 x 88mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Net Weight	22.5 lb (10.2 kg)	50.7 lb (23 kg)	52.9 lb (24 kg)	22.5 lb (10.2 kg)	22.5 lb (10.2 kg)
Gross Weight	32.6 lb (14.8 kg)	61.7 lb (28 kg)	63.9 lb (29 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)	32-104 °F (0-40 °C)
Storage Temperature	-40-158 °F (-40-70 °C)	-40-158 °F (-40-70 °C)	-40-158 °F (-40-70 °C)	-40-158 °F (-40-70 °C)	-40-158 °F (-40-70 °C)
Allowed Relative Humidity	10-95%, non-condensing	5-90%, non-condensing	5-90%, non-condensing	10-95%, non-condensing	10-95%, non-condensing

Specifications: Virtual Appliance

	SG-6000-AX02-IN	SG-6000-AX04-IN	SG-6000-AX08-IN	SG-6000-AX12-IN
CPU	2 Core	4 Core	8 Core	12 Core
HDD (min., max.)	20 GB, 1 TB	20 GB, 1 TB	20 GB, 1 TB	20 GB, 1 TB
Memory	4 GB	8 GB	16 GB	24 GB
Maximum Interfaces	10	10	10	10
L4 Throughput (KVM SRIOV)	5 Gbps	10 Gbps	20 Gbps	30 Gbps
L4 Throughput (Virtio)	2 Gbps	2 Gbps	2 Gbps	2 Gbps
L7 HTTP Throughput (KVM SRIOV)	4 Gbps	7.5 Gbps	15 Gbps	22 Gbps
L7 HTTP Throughput (Virtio)	2 Gbps	2 Gbps	2 Gbps	2 Gbps
L4 Connections/s	120,000	160,000	400,000	550,000
L7 HTTP Connections/s	60,000	150,000	300,000	450,000
Concurrent Connections	1 Million	3 Million	6 Million	9 Million
ECDHE RSA 2K SSL (CPS) (KVM SRIOV) [1]	700	1,500	4,000	6,500
ECDHE RSA 2K SSL (CPS) (Virtio)	700	700	700	700
ECDHE RSA 2K SSL (RPS) (KVM SRIOV) [2]	10,000	20,000	55,000	85,000
ECDHE RSA 2K SSL (RPS) (Virtio)	9,500	9,500	9,500	9,500
ECDHE RSA 2K SSL Throughput (KVM SRIOV) [3]	900 Mbps	1.5 Gbps	4 Gbps	4.4 Gbps
ECDHE RSA 2K SSL Throughput (Virtio)	800 Mbps	800 Mbps	800 Mbps	800 Mbps

Module Options

Module	IOC-AX-4GE-B-H-IN	IOC-AX-4SFP-H-IN	IOC-AX-8GE-B-H-IN	IOC-AX-8SFP-H-IN	IOC-AX-4GE4SFP-H-IN	IOC-AX-2SFP+-H-IN
I/O Ports	4 x GE Bypass Ports	4 x SFP Ports	8 x GE Bypass Ports	8 x SFP Ports	4 x GE and 4 x SFP Ports	2 x SFP+ 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)	1U (Occupies 1 generic slot)
Weight	0.33 lb (0.15 kg)	0.33 lb (0.15 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)	0.33 lb (0.15 kg)

Module	IOC-AX-4SFP+-H-IN	IOC-AX-2QSFP+-H-IN	IOC-A-4SFP+-IN	IOC-A-2QSFP+-IN	IOC-A-2MM-BE-IN	IOC-A-2SM-BE-IN
I/O Ports	4 x SFP+ Ports	2 x QSFP+ Ports	4 x SFP+, SFP+ module not included	2 x QSFP+	4 x SFP, MM bypass (2 pairs of bypass ports)	4 x SFP, SM bypass (2 pairs of bypass ports)
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U	1U	1U	1U
Weight	0.44 lb (0.2 kg)	N/A	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) Connection: Request=1:1; The data of AX120S-IN/AX220S-IN/AX320-IN/AX520S-IN/AX1200S-IN/AX2200S-IN/AX3200S-IN can be increased to 950/3,500/3,500/8,000/23,000/40,000/46,000 with SSL license;

(2) In the test, Requests Per Second uses Maximum Possible; Connection: Request=1: N;

(3) The RSA key length is 2048Bit, and the encryption suite is AES256-SHA256

Version: EX-08.01-ADC-V4.4-1225-EN-01

HAFS
Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY V vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision