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