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 seman-

© 2021 Hillstone Networks All Rights Reserved.

Product Highlights (Continued)

tics analysis engine helps further detect threats like SQL injection and cross site scripting, and minimizes false positives. Hillstone WAF's recursive decoding capability also detects attacks that are obscured by multiple encoding. This dual-engine approach significantly improves the accuracy of detection and efficiency in operation.

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

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

Rich Logs for Intelligent Analysis and Reporting

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

Features

Web Application Protection

- Defend against HTTP anomalies
- SSL transparent proxy
- HTTP fast flood and slow flood attacks defense
- Injection attacks defense, including SQL injection, LDAP injection, SSI injection, Xpath injection, Command injection, Remote File Include (RFI) injection, etc.
- Defend against cross-site attacks, including XSS and CSRF attacks
- Semantic analysis based detection of SQL injection and XSS attacks
- Prevention of data leakage, including leakage of server error, database error, Web directory content, code, keyword, etc.
- Prevent leakage of sensitive personal data. Support detection the leakage of personal identification, number of bank card, credit card, and email account. Support desensitization of sensitive information (replace with specified characters)
- Cookie security. Support prevention of cookie tampering and hijacking; support cookie signature and encryption
- Web access control ability, which can defend the behavior of scanning, crawling, and directory traversal
- Support fine-grained control of HTTP access based on client IP, by matching HTTP method, HTTP header, HTTP content type, HTTP protocol version, URI path, etc.
- Support defense against vulnerability attacks to web servers, web framework and web application
- Defense against illegal resource access, including illegal uploads, illegal downloads and hotlinking attacks; support illegal download control based on file size and MIME file type
- Defense against malware, including WebShell and Trojan attacks, etc.
- Defense against brute force attacks
- Support detecting and blocking client by its source IP (via X-forward-for) when deployed behind a load balancer or a proxy
- Support customized rules
- Pre-defined protection policy templates; support customized protection policies
- Real time update of signature databases
- Support API security detection and protection; Support validation based on OpenAPI specification documents
- Support configuring site status as website maintaining

Anti-defacement

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

Network Security Protection

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

IPv6

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

Policy auto-learning

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

Defense Response

- Support learning from the specific URL
- Support alarming only if a trigger behavior is executed
- Support blocking the behavior that break the security rules and responding with an alert page
- Support alert page customization
- Support redirecting the alert page to another URL
- Support adding whitelist (exception rule) via

© 2021 Hillstone Networks All Rights Reserved.

Features (Continued)

security logs, and support exception rules based on URL and source IP
- Support adding attacker to blacklist to block subsequent access
- Support IP and URL whitelist
- Support interaction with firewall to issue blacklist
- Support access control based on geoIP

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

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

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

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

Network and Interface Configuration
- Support static routing
- Support interface aggregation
- Support VLAN sub-interface
- Support multiple vSwitches, virtual-wires

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

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

Log, Report and Alarm
- Rich log information, including device management logs, network security logs, web security logs, tamper-proof logs, access control logs, auto-learning strategy logs, web access logs, etc.
- Support logging all HTTP headers in attack events, including URL, UserAgent, POST content, cookie, etc.
- Support logging server responses
- Supports alarming via e-mail, SNMP, SYSLOG, SMS, etc.
- Support reporting (report templates supported) from multi-dimensions such as security risk overview, site risk details, attack type details, site tampering analysis, site visits, summary of network layer attack, system operation status, etc.
- Support log aggregation according to policy or client IP
- Support intelligent log analysis, including threat analysis and false positive analysis, and optimization of security policy based on analysis results
- Support playback of attack, which can help administrators quickly analyze and locate the threats and attacks in network
- Support deleting web security log
- Support log transfer via FTP
- Support user-defined report
- Support report exported in PDF, DOC format
- Support periodic export of report
- Mail server supports STARTTLS and SSL encrypted transmission
- Support user session tracking to add user name, session identifier and session identity value in logs

Specifications

	SG-6000-WV02	SG-6000-WV04	SG-6000-WV08	SG-6000-WV12
Maximum Throughput (1518 bytes) (vNIC/ SR-IOV) (1)	5G	10G	20G	40G
Maximum Concurrent Sessions (1)	400,000	1,200,000	2,500,000	4,000,000
HTTP Throughput (HTTP GET 512KB file) (2)	1200M	2500M	5500M	8000M
HTTP Concurrent Sessions (HTTP GET 64B file) (2)	100,000	300,000	1,500,000	2,500,000
HTTP New Sessions (HTTP GET 1B file) (2)	2,800	5,800	14,000	20,000
HTTP Maximum Transactions Per Second (TPS) (2)	3,000	6,500	16,000	22,000
HTTP Throughput Reference for Model Selection (2)	250M	650M	1500M	2000M
HTTPS Throughput (3)	200M	400M	900M	1500M
HTTPS New Sessions (3)	400	900	2,200	3,300
HTTPS Maximum Transactions Per Second (TPS) (3)	3,000	6,000	15,000	24,000
HTTPS Throughput Reference for Model Selection (3)	50M	80M	200M	300M
vCPU Support	2 Core	4 Core	8 Core	12 Core
Storage (Min/Max)	100GB/1TB	100GB/1TB	100GB/1TB	100GB/1TB
RAM	4G	8G	16G	24G
Network Interface Support (Minimum / Maximum)	10	10	10	10
Protected Sites	16	32	128	256
Protected IP/PORT Pairs	32	64	1024	1024

NOTES:

(1) Network performance is obtained under WAF disabled, and no protection site configured;

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

(3) HTTPS protection performances are obtained under "Medium protection strategy", TLSv1.2 cipher suite ECDHE-RSA-AES128-GCM-SHA256, key length 2K RSA.

© 2021 Hillstone Networks All Rights Reserved.
Version: EX-08.01-W-Series-V2.7.4-0921-EN