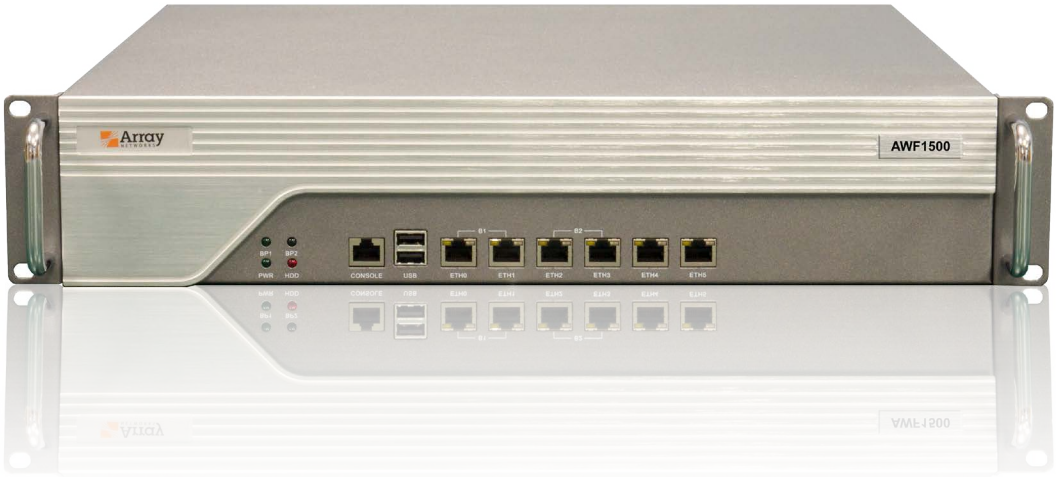
AWF SERIES DATASHEET

WEB APPLICATION FIREWALL

AWF Series Web application firewalls provide industry-leading Web application attack protection, ensuring continuity and high availability of Web applications while reducing security risks.

Array's AWF Series Web application firewalls extend beyond traditional firewalls and intrusion detection systems (IDSs) to provide comprehensive protection for business-critical Web applications. The AWF Series not only detects the complex Web application attacks of today, but also blocks the attack traffic in real time without affecting the normal flow of business data traffic. In addition, the AWF Series provides extremely fine-grained attack detection and analysis capabilities while protecting against the most common Web application threats including SQL injection attacks, Web page tampering, Web site malicious code, and disclosure of sensitive information.

Highlights & Benefits



- Next-generation Web application firewall operates on multiple levels to protect vital Web servers and applications
- Continuous scanning for Web application vulnerabilities and for SQL injection or cross-site scripting and other threats within applications
- DDoS protection via brute force attacks mitigation
- Active incident response including detection, blocking and prevention of intrusion and other attacks, including zero-day detection by abnormal behavior analysis techniques
- Post-incident diagnosis and analysis of security issues to reduce overall security risk and maintain Web site credibility
- Highly refined rules library includes sophisticated protections such as information disclosure protection, embedded Trojan detection and protection, protocol integrity detection, keyword filtering and much more
- Comprehensive Layer 1 through 7 protection for Web servers at the network level, including packet-filtering, URL-based access control, blacklist/whitelist and other protection functions
- Web page tamper-proofing through centralized management and control of all Web tamper-proofing endpoints, with content monitoring, synchronization and publish functions
- Customizable feature library and flexible configuration model to meet the needs of complex Web applications
- Guided configuration with exception rules to reduce installation complexity and errors
- Comprehensive management portal provides visualized monitoring at the system, hardware, attack and tamper-proofing levels
- Role-based authentication at the administrator level to secure configuration and data and allow for auditing
- Logging and log analysis with graphical representation and easy export of logs and statistics

Next-Generation WAF Protection

As applications have increasingly moved to the Web, the servers that host critical business applications have become targets of malicious attacks, tampering and other security incidents that can compromise intellectual property, customer information and other sensitive business data.

Array's AWF Series Web application firewalls protect against the most widespread attack mechanisms while providing active incident response to halt hackers in their tracks, with post-incident analysis and diagnosis to provide guidance for strengthening servers against future attacks.

Continuous Threat Scanning

The AWF Series continuously scans Web application servers for known vulnerabilities, and scans the applications for the existence of SQL injection or cross-site script vulnerabilities as well.

Active Incident Response

During a security incident, the AWF Series effectively detects, blocks, and prevents further intrusion, SQL injection, cross-site scripting and other types of Web application attacks.

Post-Incident Diagnosis and Analysis

After a security incident, the AWF Series diagnoses for critical security issues such as Web site tampering and malicious code, allowing administrators to reduce security risk and maintain the Web servers' credibility.

Sophisticated Rules Library

Based on years of network security research, the AWF Series' highly refined rules library provides a wide variety of protections, including:

- Preventing attacks including SQL injection, cross-site attack, cookie injection, malicious code, buffer overflow and other variant Web server attacks
- Information disclosure prevention
- Web site embedded Trojan protection and detection
- Protocol integrity detection
- CSRF anti-stealing link
- Integrity inspection of HTTP RFC protocol
- Keyword filtering

Comprehensive Server Protection

The AWF Series includes key network firewall features to provide comprehensive Layer 1 through 7 protection for Web application servers. These features include packet filtering, blacklist/whitelist, URL-based access control and other basic protection functions at the network layer.

Web Page Tamper-Proofing

To support Web page tamper-proofing, the AWF Series supports centralized management and control of all Web page tamper-proofing endpoints, and provides content monitoring, synchronization and publishing functions. Because it uses driver-level folder protection technology, and uses an event-triggered mechanism, it occupies very few system resources.

Each time a user accesses a protected Web page, such as a login page, the AWF Series checks the page integrity before permitting access, thus preventing access to contaminated pages.

Guided Configuration

Configuration of Web application firewalls has been notoriously more complex than that of network-level firewalls. The AWF Series provides configuration guidance in order to assist network administrators in accurately configuring and setting up the Web application firewall. For example, false alarms are frequently encountered during set-up. The AWF Series supports generation of exception rules, with a single click on the corresponding strategy that is generating the false alarm.

Visualized Management

The AWF Series' powerful equipment monitoring functions allow administrators to monitor, in real time, the associated equipment's working condition, attack threats and other system information. This capability allows timely discovery and elimination of network problems, promoting stable operation.

Role-Based Authentication

Three separate administration roles are supported within the AWF Series: Administrator, account administrator and audit administrator. Assignment of distinct roles can assist in meeting quality standards and audit needs of regulatory and other requirements.

Logging and Log Analysis

The AWF Series' logging function records the admin, Web site access, attack, Web page tamper-proofing, audit and other logs. For applications requiring high volumes of logs or long-term logging, an external log server can be supported.

The advanced log analysis system displays multiple types of logs in graphical format, and supports export of the logs in various formats to facilitate collection fo statistics.

AWF Series Appliances

The AWF Series features three models to choose from, supporting from four to eight 1 GbE or 10 GbE interfaces and from 800K to 2M concurrent connections per second, depending on model. The AWF appliances leverage next-generation processors and memory, energy-efficient components and 10 GigE to create solutions purpose-built for scalable Web application security.

Available for common hypervisors, the vAWF virtual appliances are ideal for organizations seeking to benefit from the flexibility of virtual environments, offer infrastructure services and new elastic business models or evaluate Array application delivery with minimal risk and up-front cost.

Feature Specifications

Topology and Networking

Topology	Bridge mode – Transparent/reverse proxy mode (inline) – Router mode – Reverse proxy mode (inline) – Passive mode
Networking Management	Static IP – Bonding (Link Aggregation)/LCAP – Bridge – Trunk (802.1q) – Policy-based route – ARP – DNS server

Security

Web Security	Protection against cookie injection, command injection, XSS, etc. – Blocking invalid file upload, such as Web shell upload – Filtering sensitive words in HTTP request and response body – Blocking information leakage, malicious code, weak password attacks, etc. – Limiting the action of Web crawler and scanner – Traffic blocking: redirection to error page, TCP reset, redirect to URL; block source address, etc. – HTTPS offloading and acceleration – Support zero-day attack detection by abnormal behavior analysis technologies – Support positive security model to configuration automatically by self-learning – Support the protection of multiple virtual hosts on one server – Strict protocol validation – Brute force attacks mitigation – Anti-DDoS
Networking Security	Access Control List – IP blacklist/whitelist – URL blacklist/whitelist

Logging, Monitoring & Reporting

Logging & Monitoring	Structured system log – SNMP (v2/v3) – CPU usage – Memory usage – Disk usage – HTTP CC number – I/O usage
Reporting	Support log query by year, month and week – Support log query by attack time, site, page, attack type and time, etc. – Support report exported as .pdf, .html, .csv and .doc

Product Specifications

AWF Series Model	1500	3500	5500
Fixed I/O	6x1GbE	6x1GbE	2x1GbE
Optional LAN Interfaces (1GbE Copper)	4	4 or 8	4 or 8
Optional LAN Interfaces (10GbE Fiber)	4xSFP	4xSFP, 8xSFP	4xSFP, 8xSFP, 2xXE
Bypass Pair	2	2 (up to 4)	2 (up to 6)
Maximum Throughput (Single 32KB HTML page)	600Mbps	1.2Gbps	5Gbps
L3 Maximum Throughput (Mixed Traffic)	2.5Gbps	4Gbps	9Gbps
Maximum Requests per Second (Keep-Alives Enabled)	10,000	30,000	60,000
Maximum Concurrent Connections	800K	1M	2M
Number of Protected Web Servers	32	256	1024
Dimensions	2U: 17.7” W x 16.9” D x 3.5” H	2U: 17.7” W x 16.9” D x 3.5” H	2U: 17.7 W x 16.9” D x 3.5” H
Maximum Power Draw	250W	350W	350W
Power Supply Redundancy	No	Yes	Yes
Weight	6.6 lbs.	6.6 lbs.	17.6 lbs.
Environmental	Operating Temperature: 5º to 40ºC. Operating Humidity: 20% to 90%		

	Supported Hypervisors (64-bit only)	Virtual Machine Requirements
vAWF *vAWF virtual application delivery controllers support all AWF features.*	VMware ESXi 4.1 or Later KVM 1.1.1-1.8.1 or later	2 Virtual CPUs 2GB RAM

1371 McCarthy Blvd. Milpitas, CA 95035 | Phone: (408) 240-8700 Toll Free: 1-866-MY-ARRAY | www.arraynetworks.com

VERSION: NOV-2015-REV-A