



## vAWF DATASHEET

# Virtual Web Application Firewall

---

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

---

Array's vAWF virtual Web application firewalls extend beyond traditional firewalls and intrusion detection systems to provide comprehensive protection for business-critical Web applications. vAWF 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, vAWF 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 site anti-defacement protection from large-scale and continuous website defacement attacks while consuming few system resources of the Web servers. Also provides automatic website content distribution capability
- Customizable feature library and flexible configuration model to meet the needs of complex Web applications
- Comprehensive management portal provides visualized monitoring at the system, hardware, attack and tamper-proofing levels
- 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
- Built-in lightweight Web vulnerability scanner to help evaluate the security status of websites
- Helps protect public-facing Web applications to meet PCI-DSS requirements
- 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

Array's vAWF virtual 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.

Available for common hypervisors, the vAWF virtual appliances are ideal for organizations seeking to benefit from the flexibility of virtual environments.

## Next-Generation WAF

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 vAWF virtual 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.

## Flexible Deployment Modes

vAWF supports a variety of deployment options to flexibly meet various requirements:

- Inline transparent proxy
- Inline reverse proxy
- Inline flow (bridge mode)
- One-arm reverse proxy
- One-arm mirror detection
- One-arm mirror detection&block

In addition, vAWF supports port linkage, which allows the administrator to group uplink and downlink ports into a single linkage group that maintains a uniform status. In deployments that include a firewall or NGFW, for example, this capability allows the firewall to detect a down link and thus route traffic correctly.

## Multi-Stage Incident Handling

The vAWF 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. 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.

For continuous attacks such as DoS/DDoS and Web attacks the vAWF virtual appliance can be set to block the attack for a specific timeframe. A blacklist rule is automatically generated for the offending source IP; the rule is kept for that timeframe, then deleted.

After a security incident, the vAWF 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 Signature Library

Based on years of network security research, the vAWF virtual WAF's highly refined signature library provides a wide variety of protections, including:

- Preventing attacks including SQL injection, cross-site attack, cookie injection, malicious code, session manipulation, parameter pollution, buffer overflow and other variant Web server attacks
- Up-to-date signatures for scanners and crawlers, and customizable crawler rules, help protect Website contents and intellectual property
- Web site embedded Trojan protection and detection
- CSRF and leech attack detection
- Integrity inspection of HTTP RFC protocol
- Keyword filtering
- File upload/download violation check
- Cloaking server information to prevent website reconnaissance
- Manual and automatic upgrade of the signature library

## Scalable & Granular Web Protection

vAWF includes sophisticated HTTP protocol conformity checks, multiple types of customizable protection rules and per-server/Web host protection profiles to achieve differentiated protections based upon requirements.

## Security Intelligence

The vAWF virtual appliance can synchronize with Array's online security intelligence center for IP reputation data at no cost, or with third-party intelligence service subscriptions, to protect against accidental access to Web sites that are known malware hosts.

## Comprehensive Server Protection

The vAWF 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.

The virtual appliance also supports HTTPS offload/acceleration to relieve server load and allow resources to be used more efficiently, and can provide basic load balancing for Web servers.

In addition, the AWF Series also supports a wide range of HTTP URL normalization methods, such as URL decoding, null byte string termination, mixed case, escaped characters, etc.

## Website Anti-Defacement

Array's AWF Series WAF provides a comprehensive solution (WebKeeper) for website defacement attacks. The solution protects websites from large-scale and continuous website defacement attacks while consuming only a few system resources of the Web servers. It also provides an automatic website content distribution function to allow website administrators to securely distribute routine website content updates and restore web pages that have been tampered with without manual intervention.

## DDoS Protection

Built-in DDoS protection prevents a wide range of Layer 3, 4 and 7 attacks, eliminating the need for a standalone DDoS appliance. vAWF protects against a wide variety of attacks, including (but not limited to):

- Land attacks
- Smurf attacks
- Winnuke
- ICMP flooding
- Port scanning
- SYN flooding
- Connection flooding
- ACK flooding
- SEQ tracking
- Slow attacks
- UDP flooding
- DNS flooding
- HTTP CC attacks
- HTTP flooding

## High Availability

The AWF Series supports High Availability (HA), which employs the Virtual Router Redundancy Protocol (VRRP) to provide service redundancy across multiple AWF appliances. Two or more AWF appliances can work in master/backup or master/master mode. These AWF appliances exchange their health status by sending VRRP advertisements at the specified interval. When the master AWF is down, the backup AWF will take over the packet forwarding.

In addition, the HA function also supports the configuration sync function, which allows administrators to synchronize the configurations from one AWF appliance to another AWF appliance.

## Guided Configuration

Configuration of Web application firewalls has been notoriously more complex than that of network-level firewalls. The vAWF virtual appliance 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 vAWF supports generation of exception rules, with a single click on the log message that is recording the false alarm.

Configuration is further assisted through the auto-learn function. vAWF can automatically learn the hosts running on a server and allow administrators to automatically assign a protection policy to them.

## Visualized Management

The vAWF virtual appliance's powerful equipment monitoring functions allow administrators to monitor, in real time, the associated equipment's operating status, attack threats and system information and statistics such as connections, servers and URLs. This capability allows timely discovery and elimination of network problems, promoting stable operation.

## Role-Based Authentication

Three separate administration roles are supported within the vAWF virtual appliance: Configuration 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 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 of statistics.

## Virtual and Physical Appliances

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.

The AWF Series dedicated appliances feature three models to choose from, supporting from four to eight 1 GbE or 10 GbE interfaces and from 215K to 2.8M 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.

## Topology & Networking

### Topology

Inline (bridge): Transparent proxy mode (inline) – Inline (router): Reverse proxy mode – One-arm (router): Reverse proxy mode – One-arm (mirror): mirror detection/mirror detection&blocking mode (flow)

### Networking Management

Static IP – Bonding (Link Aggregation)/LCAP – Bridge – Trunk (802.1q) – Policy-based route – ARP – NTP – DNS server – Port Linkage – SNAT – DNAT – DHCP – Software bypass

## 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. – Error page and redirect URL customization – HTTPS offloading and acceleration – Supports zero-day attack detection by abnormal behavior analysis technologies – Supports positive security model to configuration automatically by auto-learning – Supports the protection of multiple virtual hosts on one server – Strict protocol validation – Brute force attacks mitigation – Anti-DDoS – Synchronization with Array and 3rd party security intelligence centers

### DDoS Protection

Including but not limited to: Land Attack – Smurf Attack – Winnuke – ICMP Flooding – Port Scanning – SYN Flooding – Connection Flooding – ACK Flooding – SEQ Tracking – Slow Attack – UDP Flooding – DNS Flooding – HTTP Rate Limit – HTTP CC Attack

### Networking Security

Access Control List – IP blacklist/whitelist – URL blacklist/whitelist – Packet filter rule

## Logging, Monitoring & Reporting

**Logging & Monitoring**

Structured system log – SNMP (v2/v3) – CPU usage – Memory usage – Disk usage – HTTP CC number – I/O usage

---

**Reporting**

Supports log query by year, month and week – Supports log query by attack time, site, page, attack type and time, etc. – Supports report exported as .pdf, .html, .csv and .doc

---

**Alerts**

Supports email alerts, SNMP alerts, SMS alerts, and log space alerts

---

## Product Specifications

vAWF*	Flow-Based	Reverse Proxy
Maximum HTTP Throughput/second	800Mbps	425Mbps
Maximum HTTP Connections/second	7,500	4,250
Maximum HTTP Concurrent Connections	900,000	118,000
DDoS Performance	1.4Mpps	1.4Mpps
Request Latency	Sub-millisecond	Sub-millisecond
Number of Protected Web Servers	1024	1024

*Performance numbers are for VMware ESXi 5.5 or later, with 2 vCPUs and 4G vRAM. vAWF performance is dependent on work mode (flow-based, reverse proxy or transparent proxy), hypervisor and configuration (vCPU, vRAM). Performance may vary with test methods or test environment.*

vAWF
AWF virtual Web application firewalls support all AWF features except hardware bypass
Supported Hypervisors
VMware ESXi 5.5 or Later KVM 1.1.1-1.8.1 or later Array AVX Series 2.4 and later
Minimum Virtual Machine Requirements
1 Virtual CPU 2GB RAM





---

[www.array-networks.co.in](http://www.array-networks.co.in)

---

VERSION: MAY-2020-REV-A