ASF Application Security Firewall

ASF Series application security firewall provides enterprise-grade Web Application Firewall (WAF) and Distributed Denial of Service (DDoS) mitigation solutions, helping protect the critical services of the enterprise data center against the OWASP Top 10 Web attacks, information leakage, Denial of Service (DoS) attacks, DDoS attacks and other security threats.

Array Networks ASF Series employ the sophisticated 64-bit SpeedCore™ multi-core processing architecture, providing comprehensive detection and defense against attacks and threats for business-critical applications. Combined the negative and positive WAF models together, Array Networks ASF Series can not only detect and block latest known attacks and security vulnerabilities, but also effectively prevent "Zero-day" attacks. ASF Series provide granular attack defense control, support automatic learning and dynamic refreshing of defense profiles, and enhance the attack detection accuracy through client source verification mechanisms.

Highlights and Advantages

- As Next-generation Web Application Firewall, ASF Series provide multi-layer security defense for business-critical servers and applications.
- Combined the negative and positive WAF models together, ASF Series can not only detect and block latest known attacks and security vulnerabilities, but also effectively prevent "Zero-day" attacks.
- ASF Series have integrated a sophisticated attack signature library, which can prevent a wide range of attacks, such as SQL injection, PHP injection, XSS, command execution, network crawler/scanner, CSRF, leech, Webshell, sensitive data leakage, session hijacking and protocol violation.
- ASF Series provide Layer 3 to Layer 7 defense for Web servers, including enterprise-grade DDoS mitigation, advanced network access control, whitelist and blacklist, HTTP protocol compliance checks, cookie tampering defense, brute force defense, anti-leech, anti-crawling/scanning, and packet anomaly checks.
- ASF Series support customized attack signatures and flexible deployment modes/defense models, meeting the requirements of various complicated Web applications.
- ASF Series provide a configuration wizard to help quickly build the defense profile based on application characteristics, which reduces the configuration complexity and provisions accurate defense capability.
- ASF Series provide positive WAF to automatically learn the normal traffic to form positive whitelist and refresh the WAF profile dynamically.
- ASF Series provide the traffic baseline learning function to dynamically refresh the rule and option settings of automatic DDoS profiles based on learning results, which simplifies the configuration and enhances the defense accuracy.
- ASF Series support Data Leak Protection (DLP) rules, which can prevent the user's private or sensitive information, such as identity information, mobile phone number, email address, credit card number, from being exposed.
- ASF Series support the virtual patching function, which can convert the scanning results of third-party Web vulnerability scanner (IBM AppScan) into executable security policies (called "Virtual

Patch") and thus reduces the risks caused by vulnerabilities to customers.

- ASF Series support the Web Anti-defacement (WAD) feature to detect the defacement attacks against Web pages in real time and recover the normal pages when defacement occurs, which protects the customer's public image.
- ASF Series provide abundant events logs to help replay attacks and conduct auditing, and support exporting of event logs for external analysis.
- ASF Series provide granular and intuitive graphic monitoring function, which enables the monitoring of the system status, attacks, traffic and packet drops.
- ASF Series provide monitoring reports, advanced service security reports and PCI DSS compliance reports, and support periodic report generation and report customization.
- ASF Series provide role-based administrative privilege control, support external authentication and authorization, and provide administrator audit logs.
- ASF Series support the software and hardware bypass function, which can help avoid service interruption (such as software or hardware fault) caused by a failure of a single ASF device.
- ASF Series provide industry-leading ECC performance and RSA 2048/4096-bit SSL performance.
- ASF Series provide comprehensive IPv6 support, helping solving the problem of IPv4 address exhaustion and promoting the migration to IPv6 adoption.
- ASF Series support XML-RPC and eCloud™ RESTful API, which allow them to integrate Cloud management systems and third-party monitoring and management platforms seamlessly.
- ASF Series employ 64-bit SpeedCore™ multi-core processing architecture, providing industry-leading performance, and support seamless integration with hardware and virtual appliances.
- ASF Series allow up to 32 hardware or virtual appliance to operate as a N+1 cluster, which provides industry-leading high availability and scalability.
- ASF Series use space-efficient, redundant-power hardware appliances that consume 10-35% less power versus alternative solutions.
- ASF Series provide easy-to-use CLI and intuitive WebUI for ease of use and configuration.

Product Function Description

Next-generation Web Application Firewall

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, which cause huge economic and reputation damages.

Array's ASF Series application security 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.

ASF Series adopt an architecture that combines the positive and negative WAF models to allow them provide defense for Web applications at the same time. The negative WAF model defends against the latest known Web attacks by upgrading Array Signature Library from time to time to support the signatures of latest attacks. The positive WAF model learns the characteristics of normal traffic and dynamically refreshes the defense profile, thus halting various kinds of complicated and unknown Web attacks effectively.

Array's ASF Series support the virtual patching function, which can convert the scanning results of third-party Web vulnerability scanner (IBM AppScan) into executable security policies (called "Virtual Patch") and thus reduces the risks caused by vulnerabilities to customers.

Enterprise-grade DDoS Mitigation

ASF Series can mitigate Layer 3 to Layer 7 DDoS attacks in the OSI network model. They can automatically generate defense rules suitable for customers' existing network by learning their traffic baseline, and support multiple source verification mechanisms such as CAPTCHA, session tracking, to accurately distinguish attack sources and legitimate sources to achieve fast response and accurate defense against BOT. The Layer 3 to Layer 7 DDoS attacks mitigated by ASF Series include but not limited to:

- HTTP GET Flood attack
- HTTP POST Flood attack
- HTTP Slowloris attack
- HTTP Slow Post attack
- HTTP ChallengeCollapsar (CC) attack
- HTTP Packet Anomaly attacks

- SSL Handshake attack
- SSL Renegotiation attack
- SSL Packet Anomaly attacks
- DNS Query Flood attack
- DNS Reply Flood attack
- DNS NXDomain Flood attack
- DNS Cache Poisoning attack
- DNS Packet Anomaly attacks
- TCP SYN Flood attack
- TCP SYN-ACK Flood attack
- TCP ACK Flood attack
- TCP FIN/RST Flood attack
- TCP Connection Exhaustion attack
- TCP Fragment Flood attack
- TCP Slow Connection attack
- TCP Abnormal Connection attack
- UDP Flood attack
- UDP Fragment Flood attack
- TCMP Flood attack
- Smurf, Ping of Death, LAND, IP Spoofing, Teardrop, Fraggle, Winnuke, Tracert and other malformed single-packet attacks

Flexible Deployment Options

ASF Series provide flexible deployment options to meet various customer network situations. ASF Series support the following deployment modes:

- **Bridge transparent mode:** ASF connects the network transparently on layer 2. The administrator does not need to change any configuration of the network. Besides, this mode supports the Bypass function, but does not support HTTPS application defense.
- **Bridge proxy mode**: ASF connects the network transparently on layer 2. The administrator needs to modify the network's NAT/Route configurations or DNS resource records to direct the application traffic to the virtual service IP to make sure that the application traffic passes through the ASF appliance physically.
- **Routing transparent mode:** ASF connects the network on layer 3. The administrator needs to draw the requests and responses of the application traffic to the Uplink and Downlink interfaces respectively.
- **Routing proxy mode:** ASF connects the network transparently on layer 3. The administrator needs to modify the network's NAT/Route configuration or DNS resource records to draw the application traffic to the virtual service IP.
- **Out-of-path TAP mode:** The ASF appliance is deployed out of the traffic path. The administrator needs to configure a port mirroring policy on the switch that ASF connects to copy the traffic to the ASF appliance for detection. This mode only detects attacks but does not block attacks. In addition, it does not support HTTPS application defense.

Multi-stage Security Handling

- Before a security incident occurs, Web vulnerabilities scanners are used to scan the applications and scanning results can be quickly converted to executable security policies (called "Virtual Patch"), thus reducing the risks caused by vulnerabilities to customers.
- During a security incident, the ASF Series enforce the defense profiles to detect and block attacks in real time and record detailed audit logs, including suspicious request data and all related interaction data.
- After a security incident, administrators can analyze logs and statistics to tune the defense profiles so as to enhance the defense accuracy and efficiency.

Sophisticated Signature Library

ASF Series have integrated the Attack Signature Library (ASL) regularly released by Array Security Center (ASC). This library includes the predefined signatures of latest known Web attacks, including but not limited to SQL injection, PHP injection, XSS, Crawlers/Scanners, CSRF, leech, Webshell, sensitive data leakage, session hijacking and protocol violations. ASC updates and releases the ASL regularly to add the signatures of new attacks or vulnerabilities, and updates scanner/crawler types, malicious URLs and Webshell characteristics. ASF Series support manual and automatic update of the ASL.

ASF Series allow administrators to build a signature rule set based on the application characteristics such as application type, platform type, database type, and programing language, which suites their applications best and provides highest defense accuracy and performance.

In addition, ASF Series support custom attack signatures and integration of third-party commercial attack signatures.

SSL Offload

ASF Series provide hardware SSL or software based SSL offload capability, which migrates the computing-intensive SSL encryption and decryption workload to the ASF appliances, thus reducing the workload of backend servers and enhancing server performance.

With SSL offload capability, ASF Series can perform deep inspection on the HTTP packets, which makes attacks employing encryption methods nowhere to hide.

Comprehensive Server Protection

ASF Series provide comprehensive server protection for servers:

- ASF Series support advanced ACL, which enables traffic control for specified defense objects based on Layer 3 to Layer 7 traffic characteristics.
- ASF Series support the HTTP filter function, which can filter HTTP packets based on HTTP protocol characteristics (such as request method, header, URL, Cookie) and perform deep protocol compliance or security compliance checks against customer Web applications.
- ASF Series provide advanced defense options, such as HTTP Via header masking, response header removal, cookie security settings, Cookie tampering defense, session hijacking defense, error page customization, and URL detection and monitoring.
- ASF Series support the brute force defense function, which effectively prevents customer Websites from brute force attacks.

Web Anti-Defacement

ASF Series provide the Web Anti-defacement (WAD) feature, which can monitor the protected Web page files in real time and cache page contents. When detecting Web page defacement, the ASF Series will automatically restore the tampered Web pages returned by Websites to normal pages, thus protecting public image.

Automatic Learning and Dynamic Profiling

ASF Series provide the positive WAF feature, which can generate positive whitelists based on the characteristics of normal traffic. Administrators can configure the appliances to automatically generate positive whitelists at the specified interval or when the number of incremental learning log count reaches the specified threshold.

ASF Series provide the traffic baseline learning function. After it is enabled, the appliances automatically learn the traffic baseline of defense objects, and support dynamic refreshing the automatic DDoS profiles based on learning results. This not only reduces the manual intervention but enhances the defense accuracy.

Application Security Visibility

- Providing rich event logs to facilitate the replay and audit of attacks.
- Providing WAF attack logs, WAF audit logs, HTTP access logs. DDoS warning logs, DDoS attack logs and HTTP filter logs
- Supporting admin audit logs to facilitate the auditing against administrators.
- Supporting exporting security event logs.
- Providing granular and intuitive graphic monitoring.
- Displaying system status such as CPU usage, RAM usage, disk usage and throughput.
- Displaying attack statistics, covering severity distribution, attack type, attack sources, attack source regions and so on.
- Displaying service traffic statistics, including detailed statistics for the traffic of different protocols.
- Displaying packet drop statistics including the drop reason statistics.
- Displaying service access statistics, including the TopN accessed URLs, client IPs and so on.
- Supporting custom monitoring pages by adding desired monitoring graphs.
- Supporting exporting monitoring graphs manually and generating monitoring report periodically.
- Supporting generating one-time or periodic advanced reports.
- Supporting system status reports, application security status report, PCI DSS compliance reports and so on.

High Availability

ASF Series provide multiple high availability options through which the application on-line time can be maximized and ensures the high availability of application services.

- The Clustering function provides fast fail-over for the two or multiple ASF appliances deployed in routing mode. The ASF appliances can work in active-standby or active-active mode.

- In a network environment deployed with redundancy solution, the administrator can use the external HA solution to provide traffic high availability for the ASF appliance deployed in Bridge transparent or proxy mode.
- Software and hardware bypass functions can avoid traffic interruption caused by failure (such as software and hardware failures) for the ASF appliance deployed in Bridge transparent mode.
- If the ASF appliance is deployed in out-of-path TAP mode, the appliance failure will not lead to service interruption.

Management and Integration

ASF Series are easy to deploy, providing intuitive Web User Interface and easy-to-operate command line interface for configuration management. With the admin tools, network administrators can view the status of system parameters, enable services and implement configuration automation by employing the XML-RPC technology. By employing extensible API interface, administrators can integrate the system management with the 3rd-party monitoring and management system.

To meet the deployment and management requirements of application security in the cloud, Array's eCloud RESTful API provides a script-level interface for cloud management systems to manage and monitor Array devices and assist in interactions between cloud operating systems and virtual machines running Array DDoS mitigation.

Physical and Virtual Appliances

Dedicated ASF Series appliances leverage a multi-core architecture, SSDs, software or hardware SSL and compression, energy-efficient components and 10 GigE or 40 GigE to create solutions purpose-built for scalable application security. Whether running on Array's AVX Series Network Functions Platform, or on common hypervisors, vASF 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 security firewall with minimal risk and up-front cost.

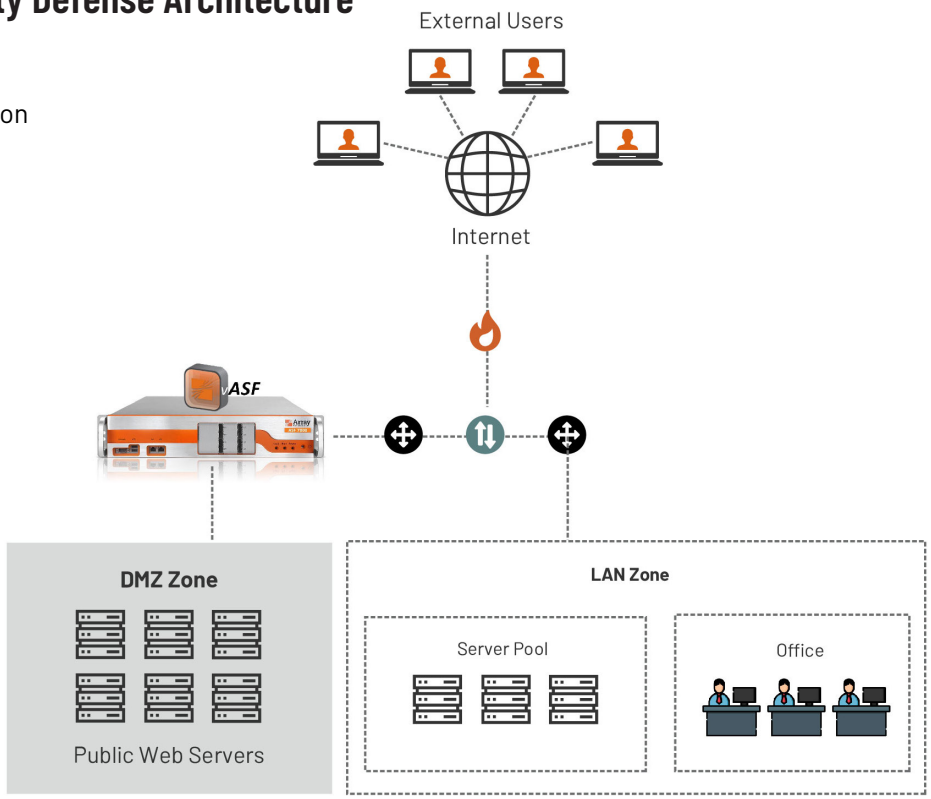
Product Function List

APPLICATION SECURITY	
WAF	• Negative security model • Signature-based defense, preventing SQL injection, XSS, network crawlers, CSRF attacks, leech, Webshell, local/remote file inclusion, command injection, sensitive data leakage, and so on, and supporting one-click signature exclusion. • Identity card information, phone number, email address, bankcard number DLP rules and content filter • CSRF defense, anti-leech, anti-crawling/scanning, and virtual patching • Positive WAF Security Model • Automatic traffic learning, automatic generation of positive whitelists, defense against "Zero-day" attacks, learning the traffic pattern of only trusted sources
Application DDoS Mitigation	• HTTP GET Flood, HTTP POST flood, HTTP Slowloris attack, HTTP Slow POST attack, HTTP CC attack, HTTP Packet Anomaly attacks • SSL Handshake attack, SSL Renegotiation attack, SSL Packet Anomaly attacks • DNS Query Flood, DNS Reply Flood, DNS NXDomain Flood, DNS Cache Poisoning, DNS Packet Anomaly attacks • Client source authentication • Application traffic baseline learning, dynamic refreshing of defense profiles
Advanced Defense Options	• HTTP filter, HTTP Via header masking, removal of HTTP response headers containing backend server information • Cookie tampering defense, session hijacking defense, brute force defense • Web anti-defacement • Inserting httponly and secure attributes into HTTP response cookies • URL detection and URL monitoring • Error page customization and DNS domain statistics • Real source IP detection
Application ACL	• HTTP ACL, DNS ACL, URL whitelists • Static blacklist, static whitelist, dynamic blacklist, dynamic whitelist, GeoIP-based access control

SSL Acceleration	• Hardware SSL acceleration • RSA/ECC/SM2 certification, SSLv3/TLSv1/TLSv1.1/TLSv1.2, and custom cipher suites • Client certificate authentication • SSL session reuse and timeout control • Server Name Indication (SNI)
NETWORK SECURITY	
Network DDoS Mitigation	• TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood, TCP Connection Flood, TCP Fragment Flood, TCP Slow Connection, TCP Abnormal Connection • UDP Flood, UDP Fragment Flood • ICMP Flood • Traffic baseline learning, dynamic refreshing of defense profiles • Client source authentication • IP reputation
Common DoS Attacks and Malformed Single-Packet Attacks	• Smurf, LAND, Fraggle, IP Spoofing, Ping of Death, Teardrop, WinNuke, Tracert • TCP packet with abnormal flag, large UDP packet, ICMP redirect packet, ICMP unreachable packet, large ICMP packet, IP packet with routing record option, IP packet with source routing option, IP packet with Timestamp option
Network ACL	• TCP ACL, UDP ACL, ICMP ACL • Static blacklist, static whitelist, dynamic blacklist, dynamic whitelist, GeoIP-based access control
APPLICATION SECURITY VISIBILITY	
Event Logs	• WAF attack logs, WAF audit logs, HTTP access logs, HTTP violation logs, HTTP filter logs • DDoS warning logs, DDoS attack logs • Log aggregation, security event alert via Email/SNMP
Graphic Monitoring	• Global attack statistics, security group attack statistics, security service attack statistics • Global traffic statistics, traffic statistics of defense objects • Global packet drop statistics, packet drop statistics of defense objects • CPU usage, memory usage, throughput, disk usage • Custom monitoring graphs
Report	• System status monitoring reports, advanced service security status reports, PCI DSS compliance reports • Report customization, periodic reports
APPLICATION AVAILABILITY	
Networking and Deployment	• Link Aggregation, VLAN, MNET • Bridge mode, Routing mode, TAP mode • Static route, RIP/OSPF/BGP dynamic route, policy route
High Availability	• Clustering among up to 32 nodes, Active/Active or Active/Standby working mode • Configuration synchronization • Hardware bypass, software bypass
IPv6	• Full IPv6 support, IPv4 and IPv6 dual stack support • IPv6-ready gold certified
MANAGEMENT	
System	• Centralized management • Supporting secure CLI, WebUI and SSH remote management as well as XML-RPC remote management interfaces, facilitating the integration with third-party management and monitoring platforms • Supporting SNMPv2, SNMPv3 and private MIB file • Syslog (based on UDP or TCP) • User management, admin authentication and authorization, role-based privilege management, admin audit logs • Supporting system alert via Email and SNMP • Supporting multiple configuration files and configuration synchronization between nodes • On-line troubleshooting and real-time monitoring
eCloud RESTful API	Providing interface for cloud management systems to control and monitor hardware and virtual ASF appliances Assisting interaction between components such as virtual machines in CloudOSRemote management of ASF appliancesNotification of events on ASF appliances

ASF Application Security Defense Architecture

- Web Application Firewall
- Application DDoS Mitigation
- Network DDoS Mitigation
- Web Anti-defacement
- Advanced Access Control
- Automatic Learning
- Dynamic Profiling
- Application Visibility
- SSL Acceleration
- IPv6 Support
- N+1 Clustering



Technical Specifications

PRODUCT MODEL ——>

	ASF 1800 Series	ASF 2800 Series	ASF 5800 Series	ASF 7800 Series	ASF 9800 Series
Max Throughput	5 Gbps	10 Gbps	20 Gbps	40 Gbps	80 Gbps
Max. SSL TPS (RSA 2K)	20K	20K	40K	55K	110K
Max. ECC TPS (ECDSA P256)	14K	14K	28K	38K	76K
Bypass card	No bypass card in standard configuration; optional				
Power supply	Dual Power: 100-240VAC, 8-4A, 50-60Hz			Dual Power: 100-240VAC, 10-5A, 50-60Hz	
Dimensions	1U – 17" W x 19.875" D x 1.75" H			2U – 17" W x 22.5" D x 3.5" H	
Weight	18.4 lbs.			29.6 lbs.	
Standards	10/100/1000 Base-TX(GbE), 1000 Base-SX/LX/ZX, 10 GibE, 10 Gig XF SR/LR, IP, SSH, HTTP 1.0/1.1, SSL, SNMP, RS232				
Management	SSH CLI, Direct Console DB9 CLI, SNMP, Single Console per Cluster, XML-RPC, Out of Band Management – RJ45				
Environmental	Operating Temperature: 0 to 45°C; Humidity: 0% to 90%; Non-condensing				
Regulatory Compliance	ICES-003, EN 55024, CISPR 22, AS/NZS 3548, FCC, 47FR part 15 Class A, VCCI-A, CSA, C/US, CE, IEC 60950-1, CSA 60950-1, EN 60950-1				

	Supported Hypervisors (64-bit only)	Virtual Machine Requirements
Virtual version supports all features	• Array AVX Series • VMware ESXi 5.5 or Later • KVM 1.1.1-1.8.1 or later	• Supports at least 2 Virtual CPUs • Minimum Requirement: • 4GB RAM • 40GB Disk

www.arraynetworks.com

VERSION: SEPT-2020-REV-A