Array

ASF Application DDoS Mitigation

DATASEET

Product Function Description

Combination of Detection and Cleaning

ASF Series provides a high-performance DDoS engine, which can accurately detect and identify Layer 3 to Layer 7 DDoS attacks and DoS attacks with the help of session tracking and source verification mechanisms.

After detecting DDoS attacks, ASF Series will generate and execute automatic blacklist to quickly clean the malicious traffic in the mixed traffic for the defense objects.

In addition, ASF Series allows attack detection and traffic cleaning to be deployed together or separately.

Enterprise-grade DDoS Mitigation

ASF Series provide Layer 3 to Layer 7 DDoS mitigation, capable of mitigating volumetric DDoS attacks, protocol-based DDoS attacks, and application layer attacks with latency of microseconds.

ASF Series supports providing granular and unique DDoS mitigation for different applications using DDoS profiles. Once defense objects are created, automatic DDoS profiles will provide the default DDoS mitigation for them. The traffic baseline learning function then allows the appliance to learn the traffic baseline of the applications and thus dynamic refresh the defense parameters for the automatic profiles. In this way, the automatic profiles can adapt to the traffic pattern changes with time agilely and achieve accurate DDoS identification and mitigation including defense against "Zero-day".

To maximize the defense accuracy including BOT protection and reduce false positives, ASF Series supports multiple source verification mechanisms, such as CAPTCHA, session tracking, and first packet drop.

The DoS and DDoS attacks that ASF Series can mitigate include but not limited to:

- HTTP GET Flood
- HTTP POST Flood
- HTTP Slowloris
- HTTP Slow POST
- HTTP Challenge Collapsar (CC)
- HTTP packet anomalies
- SSL Handshake attack
- SSL Renegotiation attack
- SSL packet anomalies
- DNS Query Flood
- DNS Reply Flood
- DNS NXDomain Flood
- DNS Cache Poisoning
- DNS packet anomalies
- TCP SYN Flood
- TCP SYN-ACK Flood
- TCP ACK Flood
- TCP FIN/RST Flood
- TCP Connection Exhaustion
- TCP Fragment Flood
- TCP Slow Connection attack
- TCP Abnormal Connection attack
- UDP Flood
- UDP Fragment Flood
- ICMP Flood
- 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 mode:

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 and modify the route configuration of the server to route server responses to the ASF Downlink interface.

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.

In addition, ASF Series support traffic diversion, which diverts suspicious traffic to the ASF appliance for inspection based on policy and BGP routing. ASF Series support traffic injection to inject normal traffic back to the network after cleaning malicious traffic based on policy routing.

SSL Offload

ASF Series provide hardware SSL or software based SSL offload capability, which migrate 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 make attacks employing encryption methods nowhere to hide.

ASF Series support RSA, ECC and SM2 certifications and TLSv1.2, TLSv1.1, TLSv1.0 and SSLv3.0 protocols.Client authentication and session reuse are supported.

Comprehensive Web Security

Besides the DDoS/DoS attacks, customers' applications are also confronted with all kinds of Web attacks, such as SQL injection, XSS, cookie/session hijacking, parameter tampering and so on.

ASF Series also integrated the Web Application Firewall (WAF) module with the DDoS mitigation. The WAF module support negative and positive security model. The negative security model supports signature-based defense, data leakage prevention, CSRF defense, anti-crawling/scanning, content filtering, and virtual patching. The positive model supports learning the application characteristics and user behaviors and generating positive whitelists to allow only normal traffic to pass and deny all the other traffic. ASF appliance is preinstalled with Attack Signature Library (ASL), which can be updated manually or automatically. Array Networks release ASL at a regular basis.

ASF Series provide HTTP security profile to execute HTTP protocol compliance checks and provide more HTTP security options to harden the security of applications. In addition, ASF Series provide application rate limit ACL to ensure the stable running of the applications.

Application Security Visibility

- Providing rich event logs to facilitate the replay and audit of attacks.
- Providing DDoS attacks as well as HTTP access logs and other types of HTTP violation logs.
- Supporting exporting security event logs.
- Providing granular and intuitive graphic monitoring.
- Displaying real-time and historical 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 allowing administrators to manage desired monitoring graphs.
- Supporting exporting monitoring graphs manually and generating monitoring report periodically.
- Supporting generating advanced system status, application security status, and PCI DSS compliance reports.

High Availability

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

- The Clustering function provides fast failover 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 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 & 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, on common hypervisors or on many popular public cloud marketplaces, 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 security firewall with minimal risk and up-front cost.

Product Function List

APPLICATION DDOS MITIGATION

HTTP DDoS Mitigation	• HTTP GET Flood, HTTP POST flood, HTTP Slowloris attack, HTTP Slow POST attack • HTTP Packet Anomaly attack (Anomaly method, Anomaly request-line, Anomaly host, Anomaly connection, Anomaly content-length, Anomaly range) • HTTP source verification
SSL DDoS Mitigation	• SSL Handshake attack, SSL Renegotiation (asymmetry) attack • SSL Packet Anomaly attack (cipher suites mismatch, handshake version mismatch, record version bad, record type bad, handshake type bad, handshake length bad, encrypt/decrypt error, ssl host stop, send data error, cipher suites bad, send data to card/sw error, get random error, big number operation failed) • Session tracking
DNS DDoS Mitigation	• DNS Query Flood, DNS Reply Flood, DNS NXDomain Flood, DNS Cache Poisoning • DNS packet length check, DNS TTL check • DNS Packet Anomaly attack (Message length out of limit, IP TTL out of limit, SrcPort & DstPort both 53, Header too short, Invalid opcode, Unused flag set, Invalid rcode, Null query, ANCOUNT is not zero in DNS query, AA bit set in DNS query, TC bit set in DNS query, RA bit set in DNS query, Unexpected end, Pointer loop, Null name, Label length error, Label length too large, Invalid label type, RR TYPE error, reserved for QTYPE only, RR CLASS error, QTYPE ANY in DNS query, CLASS is not IN) • DNS source verification
Advanced Web Security	• Signature-based defense, Cookie/session tampering defense, CSRF defense, crawling/scanning defense, virtual patching, HTTP protocol compliance checks, Brute force defense, Web antidefacement, Signature Library manual/auto update, Custom Signatures, Error page customization
Application ACL	• HTTP Rate Limit ACL, DNS Rate Limit ACL, URL Whitelist • Automatic IP whitelist/blacklist
SSL Acceleration	• Hardware SSL acceleration, RSA/ECC/SM2 certification, SSLv3/TLSv1/TLSv1.1/TLSv1.2, and custom cipher suites • Client certificate authentication, Session reuse

NETWORK DDOS MITIGATION

TCP/UDP/ICMP 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 • Source verification, Session tracking • IP reputation
Defense Against DoS and Malformed packets	• Smurf, LAND, Fraggle, IP Spoofing, Ping of Death, Teardrop, WinNuke, Tracert • IP packet with routing record option, IP packet with source routing option, IP packet with Timestamp option, TCP packet with abnormal flag, large UDP packet, ICMP redirect packet, ICMP unreachable packet, large ICMP packet
Network ACL	• TCP Rate Limit ACL, UDP Rate Limit ACL, ICMP Rate Limit ACL • Manual IP whitelist/blacklist, Automatic IP whitelist/blacklist, Geolocation-based IP blacklist

POLICY ENFORCEMENT

Defense Object	• Security Service: provides application DDoS defense for it. • Security Group: provides network DDoS defense for it.
Profile	• Automatic DDoS profile/Manual DDoS Profile • Application/network DDoS profile • Defense Mode – Block , detect
Dynamic Profiling	• Application Traffic Baseline learning • Network Traffic Baseline learning • Dynamic refreshing of automatic DDoS profile based on learning results

APPLICATION SECURITY VISIBILITY

Event Logs	• DDoS Attack logs, DDoS Warning logs • HTTP violation logs (WAF logs, filter logs, audit logs) • Log aggregation

	• Security alert via Email/SNMP • Exporting logs to external Syslog servers
Graphic Monitoring	• Global attack statistics, security group attack statistics, security service attack statistics • Global traffic statistics, security group/service traffic statistics • Global drop statistics, security group/service drop statistics • CPU usage, memory usage, disk usage, throughput • Custom monitoring graphs
Reporting	• System status monitoring reports, service security status report, PCI DSS compliance report • Report customization, periodic report generation

APPLICATION AVAILABILITY

Networking and Deployment	• Link aggregation, VLAN, MNET • Bridge mode, Routing mode, TAP mode; transparent and proxy defense model • Static routing, RIP/OSPF/BGP dynamic routing, 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 • IPv6-ready gold certified

MANAGEMENT

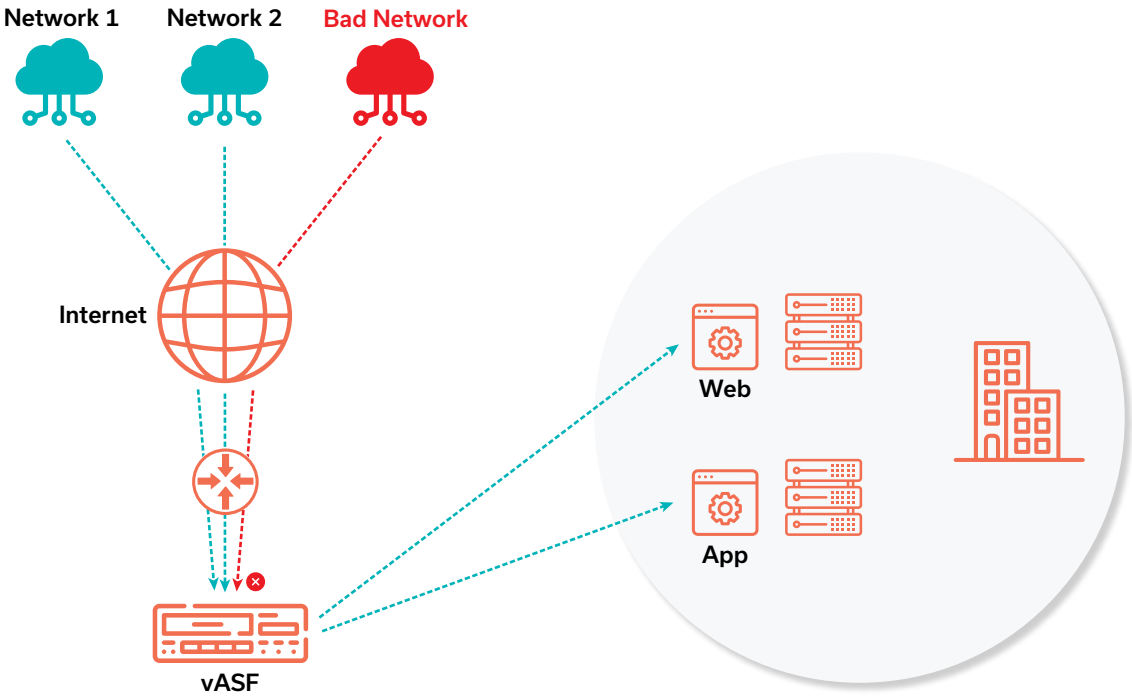
System	• Secure and intuitive CLI, WebUI and SSH remote management • Supporting XML-RPC remote management interfaces

- 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
- System alert via Email and SNMP
- Online troubleshooting and real-time monitoring

eCloud REST API

- Interface for cloud management systems to control and monitor hardware and virtual ASF appliances
- Assists interaction between components such as virtual machines in CloudOS
- Remote management of ASF appliances
- Notification of events on ASF appliances

Application DDoS Mitigation Deployment Scenario



Technical Specifications

• Standard o Optional

	ASF 1800 Series	ASF 2800 Series	ASF 5800 Series	ASF 7800 Series	ASF 7800 Series
Max Throughput	5 Gbps	10 Gbps	20 Gbps	40 Gbps	80 Gbps
SSL TPS (RSA 2K)	15 K	15 K	40 K	55 k	110 K
Max. ECC TPS (ECDSA P256)	14 K	14 K	28 K	38 K	76 K
1 GbE Copper	•	•	•		
1 GbE Fiber			o		
10 GbE Fiber		•	•	•	•
40 GbE Fiber					o
Power supply	Dual Power: 100-240VAC, 8-4A, 50-60Hz			Dual Power: 100-240VAC, 10-5A,50-60Hz	
Weight	18.4 lbs.	18.4 lbs.	18.4 lbs.	29.6 lbs.	29.6 lbs.
Dimensions	1U –17"Wx 19.875" D x 1.75" H			2U – 17" W x 22.5" D x 3.5" H	
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				
Safety	CSA, C/US, CE, IEC 60950-1, CSA 60950-1, EN 60950-1				
Support	Support Gold, Silver and Bronze Level Support Plans				
Warranty	1 Year Hardware, 90 Days Software				

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