New Array Networks Software Guards Against Distributed Denial of Service, Provides Visibility into Encrypted Traffic and Enables Multi-Site Redundancy for Hybrid Cloud Deployments

Latest OS version adds DDoS attack protection, SSL intercept and enhanced GSLB

MILPITAS, Calif.—March 21, 2017 -- Array Networks Inc., a global leader in application delivery networking, announces its latest software version, a release for Array's vAPV and APV Series application delivery controllers (ADC) with new features to guard against DDoS attacks, intercept SSL-encrypted streams to provide visibility into encrypted traffic, and support enhanced global server load balancing (GSLB) for multi-site high availability spanning both public and private clouds.

DDoS Attack Protection

2016 was the worst year on record for distributed denial of service attacks, and recent history indicates it is a pattern that will continue unabated.[1] To establish an additional front in the fight against DDoS, Array APV Series ADCs now feature integrated DDoS protection that prevents attacks at the application, session and network layers. Supporting protocols including DNS, HTTP, SSL, TCP, UDP, ICMP and IP, key capabilities include machine learning for anomaly detection and auto-configuration of threshold values, suspect client filtering and verification, alarms and attack prevention measures such as rate limiting, resetting and black listing.

"With digital transformation an imperative for enterprises worldwide, IDC is seeing an increased focus on multi-cloud strategies that enable business agility and competitive advantage," said Brad Casemore, director of research for datacenter networking at IDC. "One consequence is that added complexity accrues to application delivery and security, the latter exacerbated by the seemingly inexorable rise of DDoS attacks. With its latest software release, Array Networks is not only helping its customers protect against the rising tide of DDoS attacks, but it's also enabling them to manage the growth of encrypted HTTPS traffic through SSL intercept and providing enhanced global server load balancing (GSLB) for hybrid-cloud application delivery."

SSL Intercept

Due to an increase in encrypted HTTPS traffic, inspecting data and preventing attacks poses a significant challenge for today's security professionals. Array's new SSL intercept capability solves this challenge by decrypting HTTPS traffic on a high-performance scalable platform, making clear text traffic available to Array or third-party security services and devices, and re-encrypting traffic in a manner that is transparent to clients and servers. With the ability to operate at Layer 2 or Layer 3 in active or passive modes, and the ability to support whitelist bypass, cache simulated server certificates and load balance security devices, Array APV Series ADCs with

integrated SSL intercept may be deployed anywhere in the network to enhance security for HTTPS encrypted traffic.

Global Server Load Balancing

With the emergence of data center architectures that span private data centers and public and private clouds, multi-site redundancy is quickly becoming a networking essential. Building on existing GSLB functionality integrated in Array APV Series ADCs, this APV version adds new enhancements designed to better facilitate hybrid cloud deployments. New features include DNS NAT, GeoIP database, multi-alive datacenter, DNSSEC and SDNS HTTPS health checks.

Network Functions Platform & Service Chaining

The new and enhanced capabilities in this latest OS version are ideal candidates for service chaining on Array's AVX Series Network Functions Platform. The AVX Series – a purpose-built hardware platform for hosting virtual appliances and virtual network functions – allows networking and security services to operate in a highly agile shared environment without sacrificing the guaranteed performance offered by traditional appliances. By deploying Array's vAPV virtual ADCs on the AVX Series platform, traffic flows may be routed through load balancing, SSL intercept, DDoS, WAF, GSLB and other network and security functions as needed to assure availability, security and performance for mission critical applications.

"App delivery has always been about providing performance, availability and security for mission-critical applications; however, security is moving to the forefront," said Paul Andersen, director of marketing at Array Networks. "The new APV version enhancements build on Array's world-class SSL stack and integrated Web firewall to provide customers with a comprehensive set of features for application-level security. More specifically, the new SSL intercept capability is an essential component of our strategy to allow customers and partners to build holistic solutions on the AVX Series platform that span both Array and third-party security functions."

About Array Networks

Array Networks is a global leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore® software, Array solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 250 employees worldwide and is a profitable company with strong investors, management and revenue growth. Poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, Red Herring and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity. To learn more, visit: www.arraynetworks.com

[1] http://www.circleid.com/posts/20170228_so_long_farewell_the_worst_ddos_attacks_of_2016/

Press Contact:
Kirsten Ashton
PAN Communications for Array Networks
(407) 734-7332
arraynetworks@pancomm.com