White Paper

360° Application Security

Holistic Multilayer Security for Web-Based Business Operations

Array Networks ADC, SSL VPN & WAF Solutions

Introduction 3

Holistic Multilayer Security 3

Multilayer Solution-Level Security 6

Security Without Compromise 7

Summary 8

About Array Networks 10

Introduction

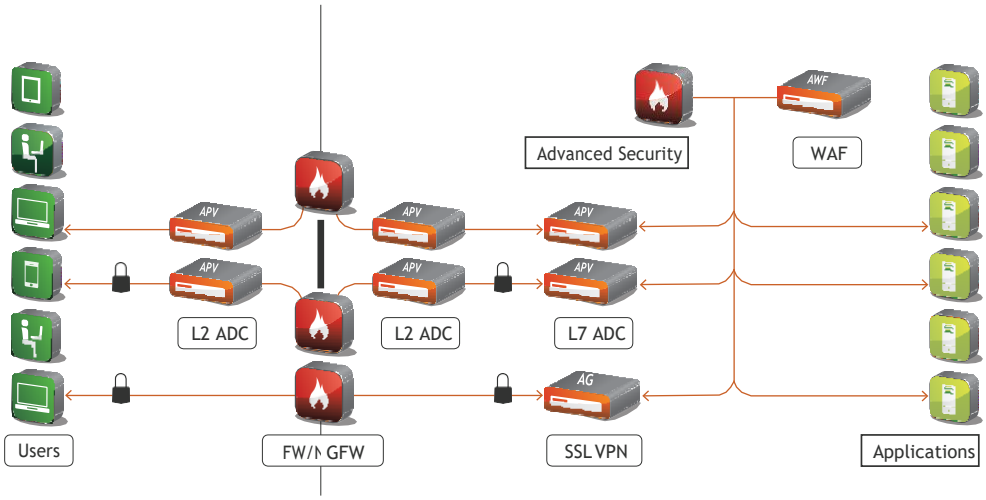
For today's networking and security professional, the risks of attack and data leakage are greater than ever. Web-based business processes, transactions and interactions are experiencing exponential growth; while this is a good thing in terms of driving productivity and opening up new revenue opportunities, the flip side is the potential for increased risk and exposure. From e-commerce and cloud software services, to remote and mobile access, to wireless connectivity and defending the corporate network – each represents an attack vector that must be taken into account to maintain compliance and protect the integrity of business data.

Attempting to tackle these complex requirements piecemeal will no longer suffice. "Siloed" or "stovepipe" security simply creates too many gaps and inconsistencies – which hackers will assuredly use to their advantage to circumvent defenses. In addition, solutions implemented without consideration of the big picture will not only compromise security, they may also compromise productivity when one or more elements are unable to scale. What is needed is a holistic approach – what this paper refers to as 360˚ application security – that addresses all potential attack vectors, and does so in a coordinated manner using an architecture that will scale to meet the needs of a growing business.

Holistic Multilayer Security

The introduction mentioned business operations such as e-commerce, enterprise applications and cloud services, as well as remote, mobile and wireless access and the need to defend the corporate perimeter. It naturally follows that one of the most essential components of 360˚ application security is defining an approach capable of addressing these common attack vectors.

At first glance these vectors may seem quite disparate; however there are several common themes among them that allow them to be addressed in a comprehensive manner. Below is a recommended architecture for holistic multilayer security that incorporates application delivery controllers, traditional or next-generation firewalls, Web application firewalls, and SSL VPNs, as well as optional advanced security.



- **Firewalls & Next-Generation Firewalls** – Firewalls continue to define the outer perimeter for both corporate and data center networks. Whether relying on traditional firewalls or deploying newer next-generation firewalls, scalability is an important consideration. Even the latest and greatest firewalls are limited in terms of throughput, especially for more advanced functions such application inspection, intrusion prevention and malware inspection. By leveraging ADCs such as Array's APV Series to perform Layer-2 load balancing, throughput for advanced security at the network perimeter may be scaled beyond 50 Gbps. In the case of Array APV Series ADCs
– deployed in a validated solution with Array's technology partner SonicWall – SuperMassive next-generation firewalls achieve up to 70 Gbps throughput for advanced firewall security.

- **Application Delivery Controllers** – One of the main challenges facing traditional and next-gen firewalls is encrypted traffic. An increasing amount of traffic on the Internet, as well as the traffic entering and exiting corporate networks and data centers, is encrypted using SSL/TLS (HTTPS). Because the traffic is encrypted, it bypasses the firewall via port 443 without inspection, resulting in the burden for security being passed to some other element in the network. Because SSL traffic is commonly decrypted by ADCs (acting as a front-end proxy for servers), the ADC then becomes the next layer of security for application traffic entering enterprise corporate networks and data centers. Once traffic is decrypted, the ADC can provide a first line of defense for application traffic.

  For instance, Array's ASF provide a stateful packet-inspection firewall that can support over 1000 ACLs without performance degradation and an enterprise class DDoS mitigation designed to prevent DoS/DDoS attack including DNSSEC. ASF also include Web application firewall (WAF) capabilities; however, caution is advised. While ASF can perform deeper level inspection, the capability often comes at the expense of performance. For high- volume workloads, a "best-of-breed" approach that includes a stand-alone Web application firewall capability may be a superior approach.

- **SSL VPNs** – Similar to encrypted HTTPS traffic bound for ADCs that are front-ending servers, SSL VPN access is another class of traffic that traverses port 443 and is invisible to perimeter firewalls. Again, because the firewall is bypassed, the burden for security is passed to the next element in the network. For organizations using Array's AG Series SSL VPN, a combination of end-point security, 2048-bit SSL encryption, advanced AAA and server-side security including passive and active Layer-7 content filtering ensure that only authorized requests and data are passed to back-end servers, applications and networks.

  Another important consideration for remote and mobile access is reduction of attack vectors. Because SSL traffic creates holes in firewalls, it is important to limit the number of connections traversing port 443. With an SSL VPN that is scalable, such as Array's AG Series, remote and mobile access for the entire organization may be consolidated on a single platform. In addition to limiting network exposure, consolidating secure access ensures consistent policies across all users and provides a single pane of glass for managing and monitoring user activity.

- **SSL Encryption** – Utilized to secure a growing portion of all Internet traffic, SSL/TLS is becoming increasingly ubiquitous. However, this security protocol itself is not without its own challenges and vulnerabilities. Recent history provides several examples of SSL-rated vulnerabilities, including Heartbleed, BASH/Shellshock, GHOST, DROWN and others – vulnerabilities associated with the widespread use of OpenSSL technology in networking and security solutions.

  In an effort to mitigate risks associated with this important security layer, Array Networks has engineered a proprietary SSL stack that is unaffected by Heartbleed, BASH/Shellshock, GHOST, DROWN and other OpenSSL vulnerabilities. With Array APV Series ADCs and AG Series SSL VPNs, data in transit is secured over SSL, the SSL protocol is protected against tampering and all SSL traffic is inspected and filtered prior to arriving at back-end servers or undergoing additional security screening.

- **Web Application Firewall** – Beyond firewalls, ADCs and SSL VPNs, Web application firewalls provide an additional layer of security. Because they are deployed behind ADCs and SSL VPNs, WAFs are capable of inspecting all traffic (including SSL traffic that was previously decrypted by the ADC or SSL VPN). When using an ADC and SSL VPN to front end a WAF, a significant number of attacks and malicious requests will have already been addressed – allowing the WAF to operate in its power band providing a deeper level of inspection on a reduced amount of pre-filtered application traffic. In this model, because compute-intensive

WAF tasks are performed on separate appliances, bottlenecks are avoided and security is assured without sacrificing performance or the end-user experience.

Using Array ASF Series Web application firewalls in conjunction with Array APV Series ADCs and Array AG Series SSL VPNs, today's complex Web application attacks can be detected and blocked-in real time without affecting the normal flow of data traffic. In addition, ASF Series appliances provide fine-grained attack detection and analysis capabilities while protecting against common Web application threats including SQL injection attacks, Web page tampering, malicious code and disclosure of sensitive information.

- **Advanced Security** – In addition to Web application firewall capability, many organizations require an even greater degree of security like API authentication and Gateway protection, Client Fingerprinting, Credentials Encryption, HTML field obfuscation etc. in order to ensure compliance and protect sensitive business data. In these cases, additional advanced security may be deployed behind ADCs and SSL VPNs to provide intrusion prevention and detection (IDS/IPS), advanced persistent threat (APT) and malware protection, and email and spam filtering. Again, deployed behind ADCs and SSL VPNs, advanced security appliances are able to provide a final layer of security that may be applied either selectively or to all application data (SSL traffic is already decrypted).

Multilayer Solution-Level Security

While taking a holistic multilayer approach to security is important, it is equally important to ensure component solutions provide layered security. Using the example of Array's APV Series ADCs and AG Series SSL VPNs, security is addressed at every level, from the OS and appliance level and all the way from Layer-2 to Layer-7 of the OSI model.

Every Array appliance is built on a security-hardened OS and platform that only exposes services' ports (no backdoors), explicitly disallows Telnet and is tested and hardened against a range of network attacks including eEye hacking tools, Nessus scans, NMAP, SMURF and local broadcast attacks. In addition Array appliances also feature an SSL stack tuned for both security and performance. Used for all production traffic, Array's proprietary implementation has proven immune to Heartbleed, BASH/Shellshock, GHOST, DROWN and other recent OpenSSL vulnerabilities. What's more, Array's streamlined, buttoned-down SSL stack not only presents fewer attack vectors, it also provides significantly better performance for secure transaction processing.

- **APV Series ADCs** – Layer-3 security includes per-customer interfaces, ingress packet filtering, up to 1000 ACLs, packet drop logs, dynamic access lists and permit-only network access. Layer-4 security includes TCP stateful inspection, packet sanitization, a reverse proxy architecture and syn-cookie protection against TCP syn floods and DOS attacks. Layer-7 security includes URL filtering, configurable access control, application session control, advance routing based on device, region, browser etc. HTTP protocol validation and policy filtering, attack signature filtering, input validation, XSS prevention and virtual patching.

④ **AG Series SSL VPNs** – End-point security includes scans for personal firewalls, anti-virus software, browsers, OSs, service packs and patches and the ability to remediate non-compliant clients. Advanced AAA includes support for LDAP, Microsoft AD, RADIUS, RSA SecurID, LocalDB, SSL client certificates and multi-factor authentication including RSA, Duo, Swivel and Syferlock. Layer-7 security includes Web resource mapping with deep packet inspection, as well as buffer overflow protection, syn-flood protection, URL filtering and configurable access control.

APV Series ADCs	AG Series SSL VPNs
Security-Hardened OS & Platform	
Security & Performance-Tuned Proprietary SSL Stack	
Layer-3 Stateful Packet Filtering	End-Point Security
Layer-4 TCP Stateful Inspection	Advanced AAA
Layer-7 Content Filtering, WAF & DDoS	Deep Packet Inspection & Web Resource Mapping

Security Without Compromise

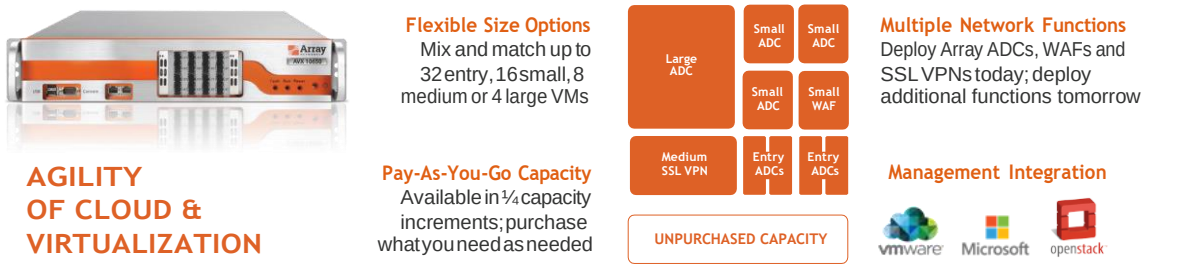
Every security architecture is a balancing act. Higher levels of security mean a higher likelihood that productivity is impacted – and a higher likelihood that performance is compromised. Similarly, system administrators often prefer one product solution that integrate a number of security functions – as they take up less space and simplify deployment and management. However, functional integration often comes at the expense of both performance and the end-user experience.

Array AVX Series virtualized appliances eliminate these trade-offs, providing an integrated platform that supports multiple instances of ADC, SSL VPN, WAF and third party security solutions with guaranteed performance. As an example, two virtual appliances could be configured as ADCs, one or two virtual appliances could be configured for SSL VPN and one or two virtual appliances could be configured for WAF. Depending on capacity purchased on the AVX platform, additional VMs could be made available for 3rd party security solutions or the size of VMs could be increased to adapt to increases in application traffic.

Because each virtual appliance is assigned dedicated CPU, SSL cores, memory and interfaces, and because dedicated resources are assigned for hypervisor management, each networking and security function supports guaranteed performance. And because each CPU-intensive security function is

operating as a "best-of-breed" solution, holistic multi-layer security may be implemented without impacting performance or the end-user experience. With Array's AVX, high-performance multi-layer security may be implemented in a single appliance that simplifies deployment and simultaneously reduces costs associated with space, power and cooling.

For cloud and virtualized data centers, the AVX allows Array's holistic, multi-layer security architecture to be implemented at a logical level – with traffic routed through networking and security functions as needed on a single integrated platform. What's more, by leveraging Array's eCloud™ RESTful API, configuration and deployment of virtual networking and security functions on the AVX may be automated using either proprietary cloud management or orchestration products from prominent 3rd party providers such as OpenStack Neutron, VMware vRealize Orchestrator and Microsoft System Center Configuration Manager.



Summary

In today's world of cloud and mobile computing and applications that run in data centers around the world, the number of attack vectors that organizations must defend against is growing exponentially. In order to successfully defend business critical applications and sensitive corporate data, organizations must adopt a holistic multilayer security architecture that not only provides defense in depth, but also delivers security in a manner that scales in terms of both manageability, performance and the end-user experience.

Deploying Array APV Series ADCs, AG Series SSL VPNs and ASF Series Web application firewalls – either as standalone appliances or as integrated solutions on Array AVX Series virtualized appliances – provides a 360˚ application security solution that protects the network perimeter, scans both unencrypted and encrypted traffic, guards cloud services and enterprise applications, unifies remote and mobile access while preventing data leakage and provides a framework for integrating and scaling advanced 3rd party security solutions.

With Array Networks, security is assured via a scalable multilayer architecture that provides guaranteed performance, reduces cost and complexity and provides a seamless path towards next-generation cloud and virtual environments.

About Array Networks

Array Networks is a leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore® software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, IDC and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.

© 2021 Array Networks India Private Ltd. All rights reserved. Array Networks, the Array Networks logo, AppVelocity, eCloud, ePolicy, eRoute, SpeedCore and WebWall are all trademarks of Array Networks India Private Ltd. in India and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Array Networks assumes no responsibility for any inaccuracies in this document. Array Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.