Array

Application Delivery Controllers

DATASHEET

APV x850 Series next-gen ADCs provide high port densities for consolidating services and optimizing availability, performance and security for cloud services and enterprise applications.

Powered by Array's 64-bit SpeedCore® architecture, APV x850 Series next-generation application delivery controllers (ADCs) cost-effectively drive industry-leading performance and consolidated ADC services with a robust set of availability, acceleration and security features to deliver unmatched overall value. Available as high-performance, high-port-density appliances that feature the latest in hardware acceleration and energy-efficient components, APV x850 Series ADCs are engineered to boost application performance in modern data center environments and speed ROI for service provider, enterprise and public sector organizations.

Highlights And Benefits

- Dedicated appliances from 20 Gbps to 40 Gbps support port densities up to 32 1 GbE copper or fiber, or up to 16 10G fiber to scale-up and scale-out as needed
- Integrated Layer-4 and Layer-7 server load balancing, link load balancing, global server load balancing, connection multiplexing, SSL acceleration, SSL intercept, caching, compression, traffic shaping, DDoS protection, IPv6 and web application security
- High-performance, kernel-level Layer-7 policy engine to enable customizable application traffic management without impacting performance or scalability
- Multi-level security including a hardened OS, forward- or reverse-proxy architecture and kernel-level web firewall for guarding applications without impacting performance
- Secure Application Access to authenticate and streamline user access to web-based and other applications in conjunction with AAA servers including SAML, LDAP, RADIUS and OAuth for Single Sign-On
- Delivers 99.999% application availability, up to 5x application acceleration and provides a first line of defense for web-enabled applications and cloud services
- Offloads SSL processing from web and application servers for increased efficiency, capacity and return on investment (ROI)
- Intercepts and decrypts/re-encrypts SSL traffic for 3rd-party security appliances, allowing full inspection
- Industry-leading performance and ECC/RSA throughput and transactions per second, and the industry's best overall SSL performance/price ratio, with advanced client certificate handling for secure application support and easy application integration
- Intelligently load balances traffic across optimal WAN links to reduce costs and improve the performance of business-critical applications
- Application-specific certifications, guides and policies for rapid deployment and accelerated delivery of business-critical enterprise applications
- ePolicyTM L7 application scripting and eRouteTM L4 routing for custom control of application traffic
- IPv6 gold certified for IPv4 preservation, IPv4/6 translation and IPv6 migration
- Array eCloudTM RESTful API and XML-RPC for seamless interaction with cloud management systems and 3rd party monitoring solutions
- Integration with VMware vRealize Orchestrator and Microsoft System Center, as well as OpenStack load balancing-as-a-service (LBaaS)
- Space-efficient, redundant-power hardware appliances that consume 10-35% less power versus alternative solutions
- Familiar CLI, intuitive cloud-friendly WebUI and centralized management for ease of use and configuration

Features

Server Load Balancing

APV x850 Series application delivery controllers ensure 99.999% availability for cloud services and enterprise applications. Leveraging robust distribution algorithms, health check mechanisms, clustering and failover capabilities, APV Series appliances maintain connections, ensure persistence, direct traffic away from failed servers and intelligently distribute application services across multiple servers for optimized performance and availability. APV Series can load balance traffic for a wide variety of protocols at Layers 2, 3, 4 and 7, including WebSocket and WebSocket Secure.

Layer-7 Policy Engine

Customized traffic management is often a trade-off between performance, control and ease-of-use. Unlike ADCs that rely on complex, compute-intensive scripting to enable custom Layer-7 policies, Array supports a vast library of policies that are hard-coded at the kernel level, are configurable with point-and-click simplicity via the WebUI or CLI, and can be combined and nested to create advanced customized application traffic management. With Array's unique approach to Layer-7 traffic management, customers get the best of all worlds: ease of use, granular control and superior performance and scalability.

SSL/TLS Acceleration & Offloading

The majority of internet traffic is now protected by SSL/TLS encryption, which ensures data privacy and integrity; however, SSL/TLS comes with a cost in terms of processing compute-intensive 2048-bit encryption. Array SSL offloading reduces the number of servers required for secure applications, improves server efficiency and dramatically improves application performance. The APV Series also simplifies SSL certificate/key management to enable intelligent content management and routing.In addition, the APV Series provides SSL acceleration to offload compute-intensive key exchange and bulk encryption, and delivers industry-leading client- certificate performance. SSL acceleration is ideal for scaling secure SaaS offerings, e-commerce environments, and business-critical applications that require high-volume secure connectivity.

The APV Series' SSL/TLS engine includes advanced security to minimize the possibility of attacks, thus further enhancing the security of applications and servers. For example, if an SSL renegotiation attack is detected, the APV Series can disable SSL renegotiation or enable rate limiting. Secure SSL renegotiation is also supported. In addition, some applications may support only SSL 3.0 or TLS 1.x, which have proven to be vulnerable to attacks. The APV Series can bridge from current SSL/TLS versions to provide improved client side security without requiring changes to the server or application. APV Series SSL/TLS processing is performed in hardware to provide high performance and capacity, as well as industry-leading TCO.

SSL Intercept

SSL-encrypted data traffic is increasing rapidly, which can place data centers and enterprises at risk – in many cases, encrypted traffic cannot be inspected by security appliances such as firewalls, IDS/IPS, data loss prevention and deep packet inspection, thus bypassing these important security measures. Array's SSL Intercept capability decrypts SSL traffic, allowing 3rd-party appliances to inspect them fully, then re-encrypts before forwarding the traffic to its destination. Flexible deployment options include L2 or L3 mode, integrated or distributed mode, forward or reverse proxy, and load balancing across multiple 3rd-party security appliances. In addition, an APV Series ADC can operate as a Webagent service to implement explicit forward proxy mode for additional security.

As an option, the Webroot BrightCloud Threat Intelligence Service is available for the APV Series. BrightCloud includes reputation services that protect users from malicious sites, as well as a web classification service to allow blacklisting of inappropriate sites and/or whitelisting of sites for which traffic must flow without inspection due to regulatory and other requirements – such as financial or healthcare sites that contain confidential personal information.

WebWall Web Application Firewall and DDoS Protection

With WebWall®, Array's suite of web application security capabilities, APV Series application delivery controllers can protect against distributed denial of service (DoS/ DDoS) and malformed URL attacks and allow a wide range of

Layer 2 through Layer 7 protective policies to be stacked atop one another for increased security. DDoS protection features machine learning for anomaly detection and automatic configuration of threshold values. APV appliances also feature extensive access control lists, network address translation and stateful packet flow inspection – all executed at the kernel level – to guard against attacks and unauthorized access without impacting performance or scalability.

In addition, integrated web application firewall capabilities provide deep application data inspection – beyond IP and TCP headers – to deal with attacks such as SQL injection and cross-site scripting. Deployable in front of multiple web or application servers, Array's web application firewall detects and responds to signatures for known application vulnerabilities and is programmable to deal with future threats.

Secure Application Access

Web-based and other applications typically require secure authentication in order to grant access to users; however, when users require access to multiple applications, or applications include subsystems that also require authentication, the process of logging in can become cumbersome and difficult. The APV Series supports Secure Application Access and multiple AAA methods including Security Assertion Markup Language (SAML), LDAP, RADIUS and OAuth to allow users to Single Sign-On (SSO) just once, and gain access to all applications for which they are authorized; Single Log Out closes all active logins at session's end. Serving as a SAML SP, the APV Series interacts with a SAML IdP (such as Array's AG Series SSL VPN) to securely authenticate the user, thus simplifying and streamlining access

Link Load Balancing & GSLB

Link load balancing (LLB) and global server load balancing (GSLB) ensure 99.999% availability for wide area network (WAN) connections and geographically dispersed sites and hybrid cloud environments. Link load balancing with end-to-end health monitoring and dynamic routing detects outages and monitors performance in real time to distribute traffic across multiple WAN connections for a premium, always on end-user experience. Ideal for geographically distributed applications, multi-site architectures and hybrid cloud applications, global server load balancing directs traffic away from failed data centers or cloud services and intelligently distributes services between sites based on proximity, language, capacity, load and response times for maximum performance and availability. In addition, Array's GSLB supports mixed health check relationships across SDNS service pools, as well as EDNS-client-subnet to provide improved resolution services and thus improve the user experience.

Application Acceleration

APV Series appliances leverage multiple acceleration technologies and optimizations to deliver a premium end-user experience for a wide range of applications and data services. In-memory caching increases server efficiency and improves seek and response times by over 500%, hardware or software compression can reduce bandwidth utilization and end-user response times by more than half and TCP connection multiplexing aggregates millions of short-lived client connections into persistent fast lanes that increase server efficiency by up to 70% while improving application performance.

ePolicy L7 Application Scripting

Where Array's Layer-7 policy engine cannot meet application traffic management requirements, ePolicy scripting allows transactions and content to be manipulated to achieve traffic distribution that improves data center efficiency and mitigates the effect of delivering applications over the internet.

eRoute L4 Routing

Using eRoute, inbound and outbound WAN traffic may be load balanced across multiple ISP links based on preset and user-defined algorithms and directed across routes optimized for maximum stability and performance. Additional L4 traffic management features include VLANs, port forwarding, port and link redundancy and the ability to bundle multiple low-cost links to improve bandwidth utilization and reduce costs.

Application-Specific Certifications

In conjunction with ISVs and application developer partners, Array APV Series appliances have been certified to provide load balancing, acceleration and security for enterprise applications such as Microsoft Lync 2010 and 2013, Microsoft Exchange 2010/2013/2016, SAP, Oracle, eClinicalWorks and others. Leveraging deployment guides, businesses can take the guesswork out of application delivery. Following simple step by step instructions, IT can rapidly and confidently configure APV appliances for optimized delivery of business critical applications.

Traffic Shaping & QoS

Traffic shaping optimizes application traffic on WAN links to improve bandwidth utilization and end-user response times. Supporting user-defined policies, APV Series appliances prevent bandwidth-intensive applications from over-utilizing WAN links and ensure essential applications are prioritized to meet service level agreements. Used in conjunction with link load balancing, global server load balancing and QoS features such as filters and class-based queuing, traffic shaping can dramatically improve application performance.
conjunction with link load balancing, global server load balancing and QoS features such as filters and class-based queuing, traffic shaping can dramatically improve application performance.

IPv6 Support

For organizations needing an IPv6 web presence, server load balancing protocol translation (SLB-PT) transforms existing IPv4 web sites into IPv6 compatible sites and greatly reduces the need for duplicate equipment, content and management. Where there is a need to make the most of depleted IPv4 resources, NAT and dual NAT (dual-stack IPv6) allow multiple clients to utilize a single IPv4 address. In migration environments, Array IPv6 solutions support both NAT64 and DNS64 to enable IPv6 clients to connect with IPv4 servers and content. To ensure a consistent application experience across IPv4 and IPv6 clients and networks – and to enable fully-capable, next-generation solutions – IPv6 feature parity is supported for all Array APV Series application delivery controllers.

Management & Integration

APV Series application delivery controllers are simpleto install and offer intuitive configuration and management via a cloud-friendly, intuitive WebUI and a familiar command line interface. Using the administration tool kit, network managers can view the status for a wide range of system parameters, enable services on the fly and automate configuration using XML-RPC or RESTful API. Leveraging extensible APIs, application and network intelligence can be integrated with third-party and cloud monitoring and management or exported for optimizing complementary data center systems. In addition, APV Series appliances support VMware vRealize Orchestrator and Microsoft System Center integration for intelligent command and control of virtualized application infrastructure.

eCloud API & OpenStack Integration

To meet the deployment and management requirements of load balancing and application delivery 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 load balancing. For cloud providers and enterprises leveraging the OpenStack architecture for cloud management and automation, Array's integration with OpenStack load balancing-as-a-service (LBaaS) creates a standardized means to rapidly integrate with and control Array technology.

Product Editions

APV x850 Series hardware appliances support two product editions. AppVelocity supports a rich server load balancing and application acceleration feature set optimized for local traffic management. The AppVelocity-E edition is purpose-built to provide industry-leading throughput and transactions per second for elliptic curve cryptography (ECC) traffic. ECC is increasingly used as an alternative to RSA encryption. AppVelocity-E models deliver enhanced security for HTTPS traffic and superior ECC performance, along with the same, robust feature set included in AppVelocity-S. All AppVelocity product editions include link load balancing and support global server load balancing as an option.

Physical Appliances

APV x850 Series appliances leverage a multi-core architecture, SSDs, software or hardware SSL and compression, energy-efficient components and high density 1 GigE and/or 10 GigE to create solutions purpose-built for scalable traffic management.

APV x850 Series Specifications

Availability

Layer 2-7 Policy & Group Management	Multi-level virtual service policy routing – Static, default and backup policies and groups – Layer 2-7 application routing policies – Layer 2-7 server persistence – Application load balancing based on round robin, weighted round robin, least connections, RTSP, shortest response, minimum misses, SNMP, QoS DNSdomain and DNS security extensions
Layer 2-3 Load Balancing	IP/MAC based load balancing for any IP protocol – Round robin, persistent IP and return to sender – Firewall, IPS/IDS, anti-spam, anti-virus and composite applications – L2 bridging support
Layer 4 Load Balancing	TCP, TCPS and UDP protocols – Round robin, weighted round robin, least connections and shortest response – Persistent IP, hash IP, consistent hash IP, persistent IP + port and port range – All single port TCP applications, RADIUS and DNS server support – Composite IP application support
Layer 7 Load Balancing	HTTP, HTTPS, DNS, FTP, RDP, RTSP, SIP-TCP, SIP-UDP, RTSP, Radauth, Radacct, Diameter, and WebSocket – L7 content switching (QoS network and client port - SSL and SIP session ID - HTTP URL, host name, cookie and any header - hash header, cookie and query) – URL redirect and HTTP request/response rewrite – HTTP request filter – DDoS protection
Server Persistence	Source + destination IP, Client IP, SSLID, HTTP header, URL, cookie, application – Individual session control
Content Routing & Switching	One arm, configurable reverse or transparent proxy mode per VIP – Configurable reverse or transparent proxy mode, triangle mode – Nested L7 and L4 policies – Combine L7 and L4 policies
Global Server Load Balancing	Application availability from multiple locations worldwide – DNS DoS protection – DNSSEC man-in-the-middle protection – Global site/service selection – Proximity and IP persistence – Load balancing between multi-site SSL VPN deployments – SNMP pool – Mixed health check instance relationships – EDNS-client-subnetsupport - full DNS – A, MX, AAAA, CNAME, PTR, SOA etc.
Link Load Balancing	Outbound: round robin, weighted round robin, shortest response time, target proximity/dynamic detection – Inbound: round robin, weighted round robin, target proximity/dynamic detection – Integrated DNS – Outbound DNS proxy

ePolicy L7 Application Scripting	Customize SLB policies and collaborate with SLB methods to realize load balancing among real services – Analyze packet contents of HTTP, simple object access protocol (SOAP), extensible markup language (XML) and diameter protocols – Receive, send, analyze, and discard generic TCP and TCPS packets – Perform pattern matching for text data – Control TCP connections – Monitor and take statistics of traffic
eRoute L4 Routing	Policy-based routing based on port, source/destination IP, UDP protocols, TCP – RIPv1, RIPv2 and BGP, OSPF support – Return to sender (RTS)/IP flow persistence – Port forwarding, link aggregation and port redundancy – Transparent to VPN remote access
Application, Server & Link Health Checks	ARP, ICMP, TCP, HTTP/HTTPS, DNS, Radius, MySQL, MsSQL, RTSP, SIP single port/protocol health checks – Multi-port health checks – Health checks by protocol and content verification – Link health checks based on physical port, ICMP and user-defined L4 – Next gateway health checks, destination path health checks – Ensure availability and performance of applications over WAN links from a single point of management – Scriptable customer-defined composite health checks
Clustering / High Availability	Up to 32 nodes – Active/active, active/standby – Standard VRRP – Configuration synchronization – Application-specific VIP health checks – Stateful TCP failover – Fast failover via USB ports – Automatic ISP failover - RFC 2338, Floating IP , MAC support - failover decision/health check conditions including, Gateway, CPU overheated, system memory, process, unit failover, group failover - multiple communication links
Single System Image	Create a single VIP (single ADC instance) out of any number of dedicated, virtualized or virtual APV appliances – Enable ultimate flexibility in scaling out.
IPv6	Full IPv6 support – DNS64 & NAT64 – Dual Stack Lite – IPv6 to IPv4 and IPv4 to IPv6 NAT and full IPv6 addressing – IPv6-ready gold certified
Networking	Link aggregation, VLAN/MNET, NTP – Static and port-based NAT, advanced NAT for transparent use of multiple WAN link
Link Load Balancing	Outbound: round robin, weighted round robin, shortest response time, target proximity/dynamic detection – Inbound: round robin, weighted round robin, target proximity/dynamic detection – Integrated DNS – Outbound DNS proxy

Acceleration

Application Performance	Dynamic detect – Client connection persistence – Connection multiplexing – TCP buffering – IEEE 802.3ad link aggregation

SSL Acceleration (2048 & 4096-bit)	Hardware SSL processing – SSLv3 and TLSv1.0/1.1/1.2/1.3 – 4096-bit maximum cipher key size (RSA or ECC) – End-to-end security (Server-side SSL communication) – SSL session reuse and timeout control – Cipher strength reduction – Customizable cipher suite order – Customizable SSL error pages – Sharable to multiple SLB services – SSL selfcheck – Server name indication (SNI)
Compression	Hardware or software accelerated – Virtualized compression – Inline HTTP processing – Compresses HTML, XML, Java scripts and CSS – Compresses Microsoft file formats(DOC, XLS, PPT) and PDF
Caching	Virtualized, memory-based cache – HTTP 1.1 compliant, policy-based cache
Traffic Shaping	Guarantees application performance – Rate shaping for setting user-defined rate limits on critical applications – QoS for traffic prioritization – Supports CBQs and borrow and unborrow bandwidth from queues – Advanced ACL (SLB QoS) – Supports QoS filters based on ports and protocols including TCP, UDP and ICMP

Security

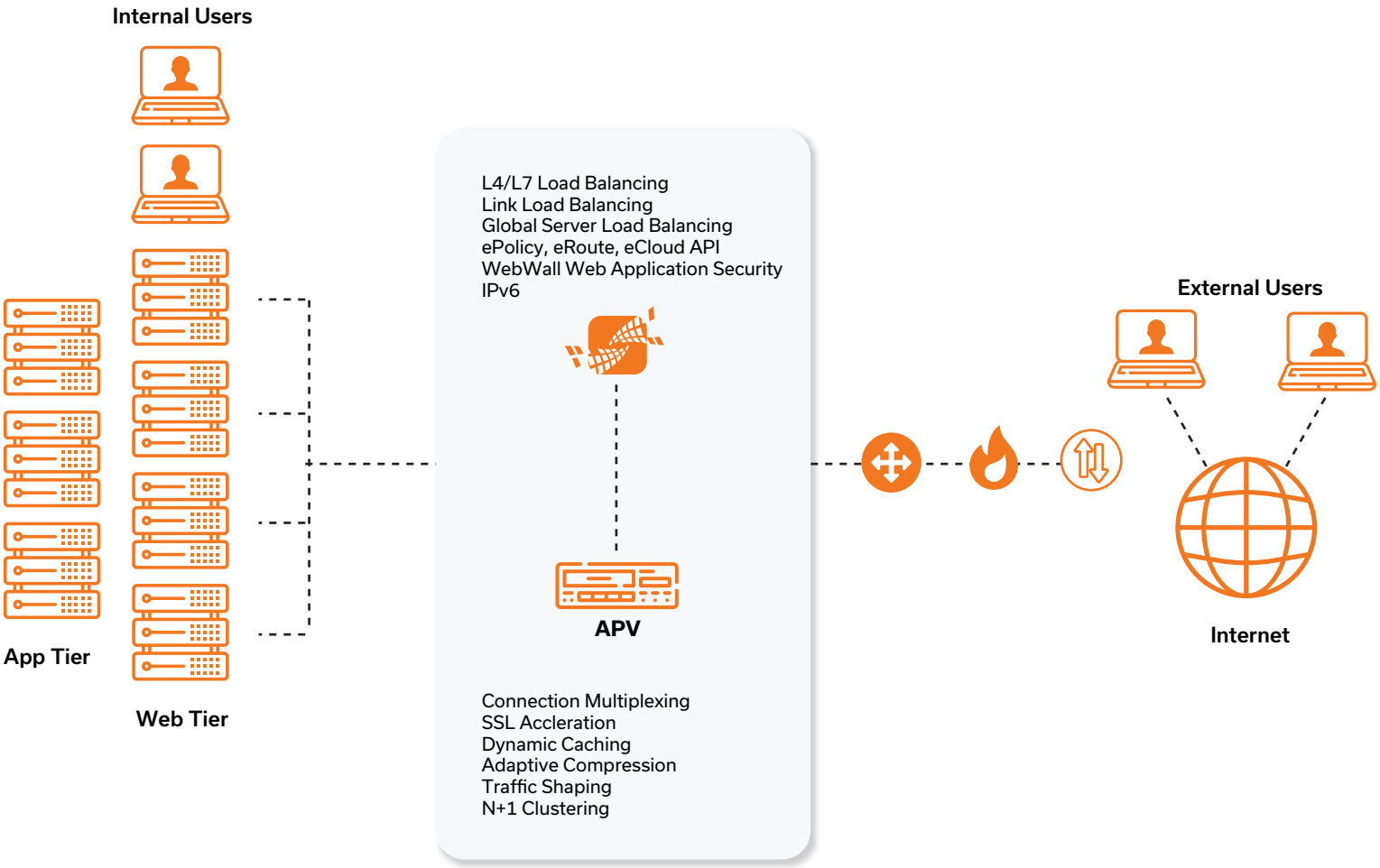
WebWall Web Application Security	Hardened OS – Secure access only, access control based on client certificate information and access method – Customer configurable SSL/TLS version, cipher suite and minimum cipher strength – Tamper-proof key and certificate protection – WebWall stateful packet-inspection firewall – Over 1000 ACL rules withoutperformance degradation – Proxy-based firewall – TCP syn-flood protection – Flashand surge event protection – DoS protection – HTTP access method control – URLfiltering – HTTP/DNS cache for mitigating DDoS – Web Application Firewall – Deepapplication data inspection for dealing with attacks such as SQL injection andcross-site scripting – Detects and responds to known application vulnerabilities –Programmable to deal with future threats
DDoS Protection (SLB)	Protection and Logging: Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapsar (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ACK flood, FIN/RST flood, Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic
SSL Intercept	L2 or L3 mode, integrated or distributed mode, forward or reverse proxy mode – Webagent service

Client-Server Certificate Management	CSR and private key generation – Self-signed certificate support – Import certificate and private key – Import certificate format – Extensive certificate support – Certificate backup and restore – Wildcard certificate support – Server Name Indication (SNI)
Client Certificate Authentication & Authorization	Turbo client certificate verification – Root and intermediate CA import – Basic client certificate verification – Certificate chain support – Certificate revocation list (HTTP, FTP, LDAP) – Online certificate status protocol (OCSP, HTTP/HTTPS) – Certificate-based access control – Inside SSL server, two-way certificates
Client Certificate Application Integration	Parse client certificate field information with different language/encoding – Pass individual field/group and field/customer format to back-end applications – HTTP header, URL and cookie – Integrated with proxy rewrite – Detailed SSL statistics
Secure Application Access	AAA support for Security Assertion Markup Language (SAML), LDAP, RADIUS and Open Authorization (OAuth) protocols – Supports definition of multiple AAA methods for multifactor authentication – Supports web single sign-on (SSO) and web single logoff (SLO) – Serves as a SAML SP (service provider) – Supports restriction on number of sessions, session timeout and session reuse

Management

System	Centralized cluster management – Secure CLI, WebUI and SSH remote management – XML-RPC for integration with 3rd party management and monitoring – SNMP V2/V3 and private MIBs – Syslog (UDP or TCP) – Administrator and operator accountmanagement – E-mail, paging and alerting capability – Multiple configuration files andunit configuration synchronization – Online troubleshooting – Real-time monitoring –Role-based administration control – HTTP/2 support – Top 10 statistics for users of IP,TCP, UDP and ICMP traffic - multiple configuration files with 2 bootable partitions
eCloud AP	Interface for cloud management systems to control and monitor hardware and virtual APV appliances – Assists interaction between components such as virtual machines in CloudOS environments – Remote management of APV appliances – Notification of events on APV appliances – eCloud demo integrated on APV appliance – Supports integration with OpenStack Load Balancing-as-a-Service(LBaaS), VMware Cloud Orchestrator (vCO) and Microsoft System Center standards

Array Application Delivery Architecture



Product Specifications

• Standard o Optional

	AppVelocity	AppVelocity-E	
	APV 2850/5850	APV 2850	APV 5850
L2, L4 & L7 SLB	•	•	•
LLB	•	•	•
GSLB	o	o	o
L7 Policy Engine	•	•	•
ePolicy Scripting	•	•	•
eRoute Routing	•	•	•
Transparent Proxy	•	•	•
SSL (HW)		•	•
Compression (SW)	•	•	•
Compression (HW)		o	o
RAM Caching	•	•	•
Traffic Shaping	•	•	•
Web Application Security (Including WAF)	•	•	•
DDoS Protection	•	•	•
Secure Application Access	•	•	•
IPv6 Support	•	•	•
Multi-language WebUI	•	•	•
Single System Image	•	•	•
Fast Failover	•	•	•
Clustering	•	•	•
eCloud API & LBaaS Integration	•	•	•

	APV2850	APV5850
Max. L4 Throughput	20 Gbps	40 Gbps
Max. SSL Throughput	15 Gbps	30 Gbps
Max. SSL TPS (RSA 2K)	20K	40K
Max. ECC TPS (ECDSA P256)	14K	28K
1 GbE Copper	up to 32	up to 32
1 GbE Fiber	up to 32	up to 32
10 GbE Fiber	up to 16	up to 16
Power Supply	Dual Power: 90-264VAC, 8-4A, 50-60Hz	
Typical Power Consumption (W)	174	
BTUs/Hour	484	
Dimensions	1U – 17.24″ W x 23.54″ D x 3.46″ H	
Weight	18.4 lbs.	
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	Gold, Silver and Bronze Level Support Plans	
Warranty	1 Year Hardware, 90 Days Software	

VERSION: APR-2019-REV-A

1371 McCarthy Blvd.
Milpitas, CA 95035

www.arraynetworks.com

+1-866-MY-ARRAY
+1 408-240-8700