Array

vAPV

Virtual Application Delivery Controllers

DATASHEET

vAPV Virtual Application Delivery Controllers improve application availability, performance and security while enabling dynamic,flexible and elastic provisioning in cloud and virtual environments.

Powered by Array's 64-bit SpeedCore® platform, vAPV virtual application delivery controllers extend Array's proven application availability, acceleration and security capabilities to virtualized data centers and public/private clouds. Combining the application delivery and traffic management features common to all APV Series products with the flexibility afforded by a virtualized infrastructure, vAPV virtual application delivery controllers enable dynamic pay-as-you-grow scalability and new elastic business models for both development and production environments.

Highlights And Benefits

- Virtual appliances with a software upgrade fromone to eight virtual CPUs to scale-up and scale-outas needed; also available on popular public cloudmarketplaces such as AWS and Azure
- Integrated Layer-4 and Layer-7 server loadbalancing, link load balancing, global serverload balancing, connection multiplexing, SSLacceleration, caching, compression, traffic shaping,DDoS protection, IPv6 and web application security
- High-performance, kernel-level Layer-7 policyengine for enabling customizable application trafficmanagement without impacting performance or scalability
- Industry-leading performance and $/SSL TPSfor 2048-bit SSL with advanced client certificatehandling for secure application support and easyapplication integration
- Multi-level security including a hardened OS,reverse-proxy architecture and kernel-level webfirewall for guarding applications without impacting performance
- Serves as a SAML SP for web Single Sign-On (SSO)to authenticate and streamline user access to web-based and other applications
- Delivers 99.999% application availability, up to 5xapplication acceleration and provides a first line ofdefense for web-enabled applications and cloudservices
- Software SSL offloading from web and applicationservers, and optional hybrid virtual/dedicatedhardware SSL offloading
- Intercepts and decrypts/re-encrypts SSL traffic for3rd-party security appliances
- Intelligently load balances traffic across optimalWAN links to reduce costs and improve theperformance of business-critical applications
- Application-specific certifications, guides andpolicies for rapid deployment and accelerateddelivery of business-critical enterprise applications
- ePolicy™ L7 application scripting and eRoute™ L4routing for custom control of application traffic
- IPv6 gold certified for IPv4 preservation, IPv4/6translation and IPv6 migration
- Array eCloud™ RESTful API and XML-RPC forseamless interaction with cloud managementsystems and 3rd party monitoring solutions
- Integration with VMware vRealize Orchestrator andMicrosoft System Center, as well as OpenStack loadbalancing-as-a-service (LBaaS)
- N+1 clustering for up to 32 virtual instances, singlesystem image and stateful TCP failover for industry-leading availability and scalability
- Familiar CLI, intuitive cloud-friendly WebUI andcentralized management for ease of use andconfiguration

Features

Able to integrate seamlessly with cloud management systems for automated service provisioning, vAPV virtual application delivery controllers are the ideal choice for enterprises, service providers and other seeking scalable and flexible application delivery and load balancing with the ability to improve data center efficiency and enable profitable cloud service offerings.

vAPV virtual ADC appliances include all features and software modules found on Array's APV Series application delivery controller dedicated appliances.

Server Load Balancing

vAPV virtual application delivery controllers ensure 99.999% availability for cloud services and enterprise applications. Leveraging robust distribution algorithms, distributing the workload to multiple processors, health check mechanisms, clustering and failover capabilities, vAPV virtual 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.

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.

2048-Bit SSL Offloading

SSL offloading reduces the number of servers required for secure applications, improves server efficiency and dramatically improves application performance.

Offloading compute-intensive key exchange and bulk encryption, and delivering industry-leading client-certificate performance, SSL acceleration is ideal for scaling secure SaaS services, e-commerce environments and business-critical applications requiring high-volume secure connectivity.

Although more secure than the old 1024-bit standard, 2048-bit keys are five times more compute intensive and can impact both performance and the cost of supporting applications. Array 2048 and 4096-bit software (or optional hybrid) SSL encryption offers unbeatable scalability and performance with the lowest cost per SSL TPS to offset transition costs and improve security without impacting performance.

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.

WebWall Web Application Firewall and DDoS Protection

With WebWall®, Array's suite of web application security capabilities, vAPV virtual 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.

vAPV virtual appliances are security-hardened to protect applications and servers from L4 and L7 DDoS attacks and support content filtering to guard against protocol and application DDoS attacks as well as Syn-flood, tear drop, ping-of-death, Nimda, Smurf and other malicious attacks. vAPV appliances also feature extensive access control lists, network address translation and stateful packet flow inspection – all executed at the kernel level – to guard againstattacks and unauthorized access without impactingperformance 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 Security Assertion Markup Language (SAML) to allow user Single Sign-On (SSO) across multiple applications and subsystems. 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.

Application Acceleration

vAPV virtual 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%, 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 vAPV virtual 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 vAPV 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, vAPV virtual appliances prevent bandwidth-intensive applications from overutilizing 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.

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 vAPV virtual application delivery controllers.

Management & Integration

vAPV virtual application delivery controllers are simple to 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, vAPV virtual appliances support VMware vRealize Orchestrator, automation tools - Ansible, Terraform 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

vAPV virtual appliances support a rich server load balancing and application acceleration feature set optimized for local traffic management. In addition, software SSL acceleration combined with server load balancing and application acceleration create a traffic management solution ideal for SaaS, ecommerce environments and applications requiring a high degree of secure connectivity. vAPV virtual appliances also include link load balancing and support global server load balancing as an option.

Virtual & Physical Appliances

Whether running on Array's AVX Series Network Functions Platform, on common hypervisors or on many popular public cloud marketplaces,vAPV 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 delivery with minimal risk and up-front cost.

Dedicated APV appliances leverage a multi-core architecture, SSDs, software or hardware SSL and compression, energy-efficient components and 10 GigE to create solutions purpose-built for scalable traffic management. The APV6600FIPS model offers FIPS 140-2 Level 2 compliance for organizations that require a higher level of security.

As an option, APV Series dedicated appliances or AVX Series network functions platforms may be deployed with vAPV virtual appliances running in virtual environments to provide hybrid virtual/dedicated hardware SSL offloading.

vAPV 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, Server Application State Protocol (SASP), 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, Mapping Ports ,consistent hash IP, persistent IP + port and port range – All single port TCP applications, NNTP, RADIUS, SMTP, IMAP and POP3, DNS server support – Composite IP application support

Layer 7 Load Balancing

HTTP 0.9/1.0/1.1/2/3, HTTPS, SSH, DNS, FTP, TFTP, RDP, RTSP, SIP-TCP, SIP-UDP, RTSP, ASP, IOT,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 (Direct Access Mode) per VIP – Configurable reverse or transparent proxy mode, triangle mode (Direct Server Response), ICAP – 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 – DNS over TLS (DOT) and HTTPS (DOH) - Global site/service selection – Proximity and IP persistence – Load balancing between multi-site SSL VPN deployments – SNMP pool - 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 vAPV nodes – Active/active, active/standby – Standard VRRP – Configuration synchronization –Application-specific VIP health checks – Stateful session failover (TCP, SSL, persistency) – Automatic ISPfailover - RFC 2338, Floating IP , MAC support - failover decision/health check conditions including, Gateway, CPU overheated, system memory, process, unitfailover, 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, Assigning Multiple IP, Static and port-based NAT, advanced NAT for transparent use of multiple WAN links, Client NAT, Jumbo frame

Acceleration

Application Performance

Dynamic detect – Client connection persistence – Connection multiplexing – TCP buffering – Tune TCP (Idle, Wait, Close, Alive, Window Scale, Sack , MSS, Time Stamp) – IEEE 802.3ad link aggregation

SSL Acceleration (2048 & 4096-bit)

Software SSL processing – SSLv3 and TLSv1.0/1.1/1.2/1.3 – 4096-bit maximum cipher key size (RSA & 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

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 cach

Traffic Shaping

Guarantees application performance – Rate shaping for setting user-defined rate limits (bps, Kbps, Mbps, Gbps and pps, Kpps, Mpps, Gpps) 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 without performance degradation – Proxy-based firewall – TCP syn-flood protection – Flash and surge event protection – DoS protection – HTTP access method control – URL filtering – HTTP/DNS cache for mitigating DDoS – Web Application Firewall – Deep application data inspection for dealing with attacks such as SQL injection and cross-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 poisoning, DNS NXDomain flood ,Tunneling attack – 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, TCP Flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic and exploits.

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

Security Assertion Markup Language (SAML)

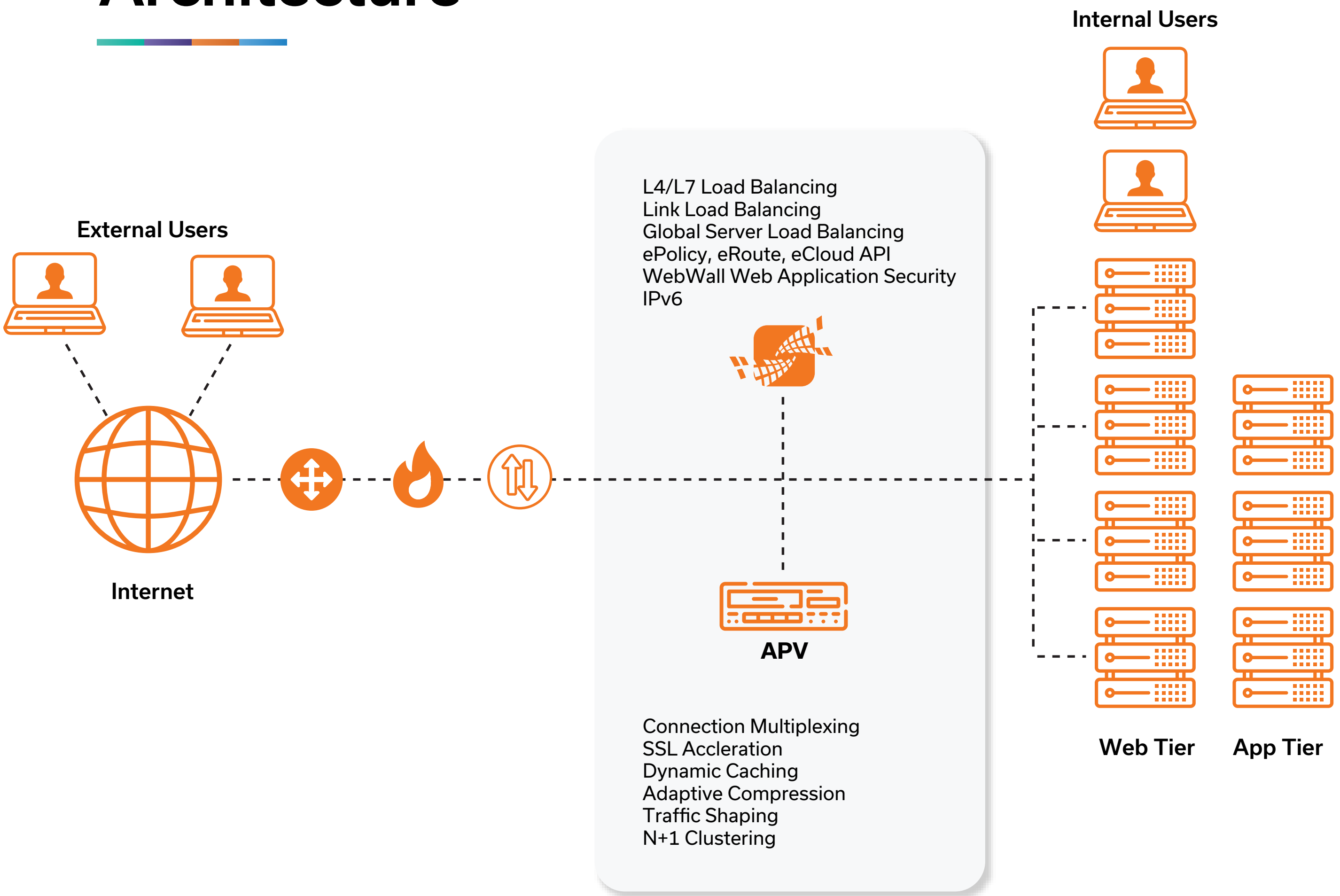
Supports SAML secure application access – Supports web single sign-on (SSO) – Serves as a SAML SP (service provider)

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 account management – E-mail, paging and alerting capability – Multiple configuration files and unit configuration synchronization – Online troubleshooting – Real-time monitoring – Auto clean up of idle resources in high utilization condition – Role-based administration control – HTTP/2 support - multiple configuration files with 2 bootable partitions

Array Application Delivery Architecture



L4/L7 Load Balancing
Link Load Balancing
Global Server Load Balancing
ePolicy, eRoute, eCloud API
WebWall Web Application Security
IPv6

Connection Multiplexing
SSL Accleration
Dynamic Caching
Adaptive Compression
Traffic Shaping
N+1 Clustering

Product Specifications

• Standard ○ Optional

	vAPV
L2, L4 & L7 SLB	●
LLB	●
GSLB	○
L7 Policy Engine	●
ePolicy Scripting	●
eRoute Routing	●
Transparent Proxy	●
SSL (SW)	●
Compression (SW)	●
RAM Caching	●
Traffic Shaping	●
Web Application Security (Including WAF)	●
SAML Support	●
Secure Application Access	●
IPv6 Support	●
Multi-language WebUI	●
Single System Image	●
Fast Failover	●
Clustering (vAPV only)	●
eCloud API & LBaaS Integration	●

vAPV

With the exception of hardware SSL acceleration, vAPV virtual application delivery controllers support all APV features and software options.

Supported Hypervisors (64-bit only)

VMware ESXi 4.1 or Later
XenServer 5.6 or Later
OpenXen 4.0 or Later
KVM 1.1.1-1.8.1 or later
Hyper-V (Windows Server 2012)
Array AVX Series

Virtual Machine Requirements

Supports 1 to 16 Virtual CPUs
Requires Minimum:
4 Virtual Network Adapters
2GB RAM
40GB Disk

Supported Public Cloud Environments

Amazon AWS
Microsoft Azure
VMware vCloud Air
VMware Cloud on AWS
Aliyun

Free Trial

Download a
free 30-day vAPV trial today.

VERSION: JAN-2025-REV-A

Array

699 S. Milpitas Blvd
Milpitas, CA 95035

www.arraynetworks.com

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