



| 应用交付系统 |

vAPV

vAPV是虚拟化应用交付系统，提高了应用可用性、性能和安全性，同时在云及虚拟化环境中提供了灵活部署、动态调整和弹性扩展等能力。vAPV能够在极大地提高企业核心应用和业务平台的可用性、性能以及安全性的同时，降低企业数据中心成本和复杂性。

vAPV虚拟应用交付系统采用华耀先进的64位SpeedCore™多核处理架构，将华耀久经验证的应用可用性、应用加速以及安全能力扩展至虚拟化数据中心和公有云/私有云环境。通过将vAPV系列产品通用的应用交付和流量管理与虚拟化基础架构提供的灵活性相结合，vAPV虚拟应用交付系统可为开发和生产环境提供按需付费的动态可扩展能力和新型弹性业务模型。



SpeedCore™ Platform Benefits

Lock-free multi-core design enables rapid scaling of performance with the addition of cores and processors.

Fault-tolerant design improves overall scalability and stability of the system by isolating and separating application traffic flows.

Content aware traffic engines efficiently accelerate applications and content based on the nature of the application and the type of the content.

亮点与优势

- 按需扩容，云上部署**
 vAPV可支持1~8个vCPU，可按需扩容，且支持在阿里云、华为云、腾讯云、AWS、Azure等常见的公有云上部署。
- 国密算法支持**
 自SM2v1.1版本开始，SM2引入了双证书系统，SSL服务器需具备两个证书：签名证书和加密证书。相应的密钥对为签名密钥对和加密密钥对。支持对SM2虚拟主机上的SSL通信进行加解密。
- 支持TLSv1.3**
 APV实现对TLSv1.3的支持，TLSv1.3已经成为实现安全连接的新的行业标准，因为其在性能和安全性上的优势。相比于之前的TLS版本，TLSv1.3具有显著的性能提升。1-RTT模式，使客户端仅需一个往返交易就可以建立起TLS通道。TLSv1.3的0-RTT复用特性还为再次访问的连接实现了加速。TLSv1.3以其“简易性”实现了更高的安全性。网站在数据保密性和完整性方面更加安全。TLSv1.3的整个握手流程都是加密的，攻击者无法修改任何的握手参数。

 最后，TLSv1.3引入了新的签名算法RSASSA-PSS，消除了早期TLS版本中会影响到签名机制的加密攻击风险。
- 功能强大，不仅仅是负载均衡**
 集成了四层和七层服务器负载均衡、链路负载均衡、全局服务器负载均衡、连接复用、SSL加速、SSL侦听、缓存、压缩、流量整形、DDoS防护、IPv6和Web应用安全等功能。
- 先进的客户端证书处理技术**
 实现安全的应用程序支持和简易集成，为2048位SSL提供行业领先的性能保证和SSL TPS性价比。
- 应用程序多层安全保护**
 安全加固的操作系统、反向代理架构和内核级Web防火墙为应用程序提供多层安全保护，性能不受影响。
- 用户身份验证与流程优化**
 与AAA服务器（包括用于单点登录的SAML、LDAP、RADIUS和OAuth）配合使用，可以对基于Web的应用和其他应用的用户访问进行身份验证和流程优化。
- SSL流量安全保护**
 Web和应用服务器SSL卸载，有效地提升了服务器的运行效率，节省服务器空间，增加投资回报；支持SSL侦听，为第三方安全设备拦截和解密/重加密SSL流量；业界领先的性能、ECC/RSA吞吐和每秒交易数能力、最优SSL性价比，以及用于保障应用支持安全和应用集成简化的高级客户端证书处理功能。
- 定制应用流量控制**
 ePolicy™七层应用脚本和eRoute™四层路由功能提供定制的应用流量控制；通过高性能的内核级七层策略引擎实现定制化的应用流量管理，性能和扩展性不受影响。
- 全面支持IPv6**
 解决IPv4地址耗尽、IPv4/6转换和IPv6迁移问题。
- 高可用性和扩展性**
 支持多达32台硬件或虚拟实例的N+1集群、单系统镜像和TCP失效切换功能，提供行业领先的高可用性和扩展性。

产品描述

通过与云管理系统无缝集成来实现自动化服务，vAPV虚拟应用交付系统是企业、服务提供商和其他寻求灵活可扩展的应用交付和负载均衡用户的理想选择，vAPV能够提高数据中心效率并实现可盈利的云服务。

vAPV虚拟应用交付系统具有APV系列硬件应用交付系统的所有功能和软件模块。

国密算法支持

APV系列对ECC椭圆曲线和SM2国密算法的全面支持，为用户在节约存储、带宽以及计算成本的前提下，提供更好更安全保障。ECC可以大幅提升SSL性能，使CPU利用率降低高达60%，而且华耀自主研发的SSL硬件加速技术，在处理复杂的ECC运算时，很好的保证了性能。APV支持多种ECC曲线，满足用户在不改变现有类型证书的前提下，直接选择多种ECC密码套件，适用不同的应用场景。自

SM2v1.1版本开始，SM2引入了双证书系统，SSL服务器需具备两个证书：签名证书和加密证书。而且，APV支持对HTTP和HTTPS服务器的SM2改造，使用户可以在不影响现有业务的前提下，增加对国密标准的支持。

服务器负载均衡

APV系列应用交付系统为云服务和企业应用提供99.999%的可用性保证。通过健全的流量分配算法、健康检查机制、

产品描述

检查机制、集群和失效切换能力，APV系列支持多种连接保持、会话持续方式，支持将故障服务器上的流量及时切换到正常工作的服务器上，并对应用服务在多个服务器上进行智能分配，有效提升了服务性能和可用性。

链路负载均衡和全局服务器负载均衡

链路负载均衡和全局服务器负载均衡功能确保了广域网连接、地域分散站点和混合云环境高达99.999%的可用性。链路负载均衡提供端到端的健康监控和动态路由机制，实时地探测链路中断故障和监控性能，确保将流量在多条广域网链路上智能分配，以提供优质和永远在线的终端用户体验。对于地域分散式的应用、多站点架构和混合云应用环境，全局服务器负载均衡是最佳的选择。全局服务器负载均衡使流量远离故障的数据中心或云服务，并依据就近性、语言、容量、负载以及响应时间等原则将服务智能地分配到不同的站点，力求最大化性能和可用性。

SSL/TLS 加速与卸载

现在，大多数的互联网流量都采用SSL/TLS加密协议以确保数据的隐私性和完整性，却不可避免地增加了对计算密集型任务（如2048位加密）的处理成本。APV系列的SSL卸载功能可以减少确保应用安全所需的服务器数量，从而提高服务器的效率，大幅提升应用的性能。APV系列还简化了SSL证书/密钥管理，以提供智能的内容管理和基于内容路由。APV系列提供的SSL加速功能可以替代服务器进行计算密集型的密钥交换和批量解密任务，并提供行业领先的客户端证书性能，通过硬件处理SSL/TLS加解密，提供高SSL性能、高SSL并发以及行业领先的总体拥有成本（TCO）。APV系列的SSL/TLS引擎进行了安全加固，降低了被攻击的可能性，因此进一步提升了应用和服务器的安全性。

SSL侦听

APV系列的SSL侦听功能能够解密SSL流量，将流量转发给第三方安全设备进行全面检查，再重新加密后转发到目的地址。

APV系列可以选配WebRoot BrightCloud威胁情报服务。BrightCloud可以提供两种服务：1) 信誉服务，用于防止用户访问恶意网站；2) 网站分类服务，用于将不当网站加入黑名单进行侦听，或根据管理规定和其他要求将不需要进行流量侦听的网站加入白名单，例如包含个人私密信息的金融或者医保网站。

集成web应用防火墙

APV系列集成了Web应用防火墙，能够提供IP和TCP头部以

外的深度报文检测，阻止SQL注入和跨站脚本等攻击。Web应用防火墙可以部署在多种Web和应用服务器前，对常见的应用漏洞特征码进行探测和响应，且支持自定义规则应对潜在威胁。

APV系列经过安全加固，保护应用和服务器不受四层和七层分布式拒绝服务攻击，支持内容过滤以阻止协议和应用DDoS攻击，如SYN Flood、Teardrop、Ping-of-Death、尼姆达病毒、Smurf、其它恶意攻击等。

七层策略引擎

定制化流量管理常常会导致性能、可控性和易用性的降低。业界ADC产品主要通过编制脚本定制七层策略，这种方式配置复杂，且对计算性能要求很高。APV系列的策略库集成在内核层，通过简单的点击WebUI界面或CLI就可以完成配置，而且支持通过关联和嵌套来创建高级的定制化应用流量管理。采用独有的七层流量管理方式，用户可以得到最佳的流量管理体验，即简单易用、细粒度控制、优越的性能和扩展性。

流量整形和服务质量（QoS）

流量整形功能优化了WAN链路上的应用流量，改善了带宽使用率和终端用户响应时间。APV系列支持用户自定义策略，以防止带宽密集型应用过度占用WAN链路带宽，保证核心业务优先使用带宽资源，从而提高服务质量。通过与链路负载均衡功能、全局负载均衡功能以及QoS功能（过滤器和基于类的队列）配合使用，流量整形能够显著地改善应用性能。

IPv6 支持

服务器负载均衡-协议转换可以帮助企业将现有的IPv4 Web站点转换为IPv6兼容站点，大大降低了对重复设备、内容和管理的需求。网络地址转换和双栈网络地址转换（IPv4-IPv6双栈）可以允许多个客户端共用同一IPv4地址。在IPv4向IPv6迁移场景中，华耀IPv6解决方案NAT64和DNS64可以允许IPv6客户端访问IPv4服务器和内容。此外，APV提供自动化配置工具，可以帮助客户快速解决“IPv6”天窗问题。

eCloud™ API与OpenStack集成

为满足云环境中负载均衡和应用交付的部署和管理需求，华耀eCloud™ API为云管理系统提供脚本级接口，以方便监控和管理华耀设备，并协助云操作系统与运行负载均衡的虚拟机进行交互。对于使用OpenStack架构实现产品描述云管理和自动化的云服务提供商和企业，可以通过华耀提

产品描述

提供的OpenStack LBaaS集成方法快速实现华耀负载均衡的集成和管理。

分区管理

分区管理功能实现了多用户环境下SLB/SSL业务隔离，一台物理设备可以同时服务多个租户，不同租户的用户管理系统和业务分发系统相互独立，从而有效降低服务的运维成本，提高资源利用率。系统还支持为分区配置高可用性（HA）功能，系统管理员可以为每个分区配置浮动IP 分组和失效切换规则实现故障时的分区业务切换。

系统最多可支持1024个分区，即一台物理设备可以同时为最多1024个租户提供相互独立的SLB和SSL业务。通过用户管理系统，系统管理员可以为每个分区分配专属的管理员以及IP、接口和VLAN等资源。每个分区都可以作为一个租户提供一套SLB/SSL 服务。

应用可视化

在系统的运行过程中，实时把握系统的运行状态对于及时的排障、保证系统的不间断服务具有重要意义。了解

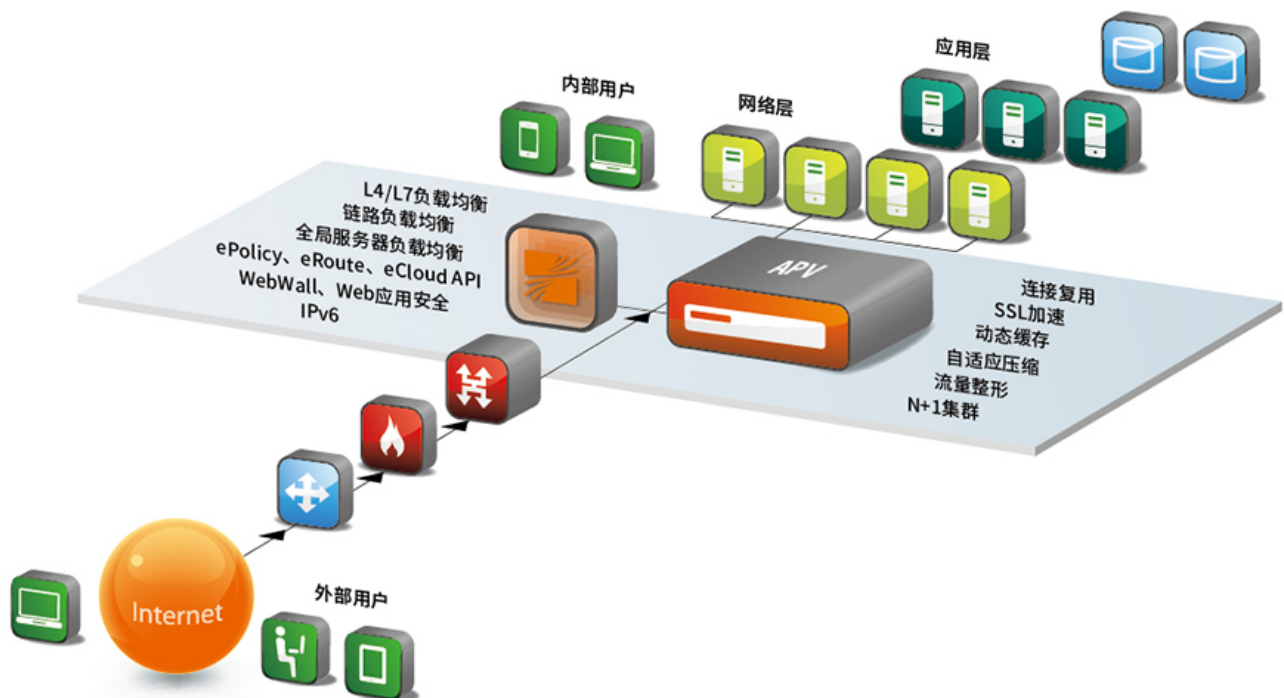
系统的运行状态需要收集大量的数据，IT部署往往会采用分布式的、容错的架构，增加了数据收集和数据分析提取的难度。

APV设备基于WebUI和ELK软件两种平台提供SLB TCP、SLB HTTP、SSL、LLB和SDNS业务的应用可视化。WebUI和ELK平台将分散的系统资源、配置和应用数据进行集中记录、存储和挖掘后，将分析后的数据以直观、可视的方式展示出来。运营维护人员可以进行可视化的应用管理，随时了解应用交付情况，快速有效地获取系统状态以及定位问题。

产品版本

vAPV虚拟应用交付系统支持健全的服务器负载均衡和应用加速功能，是优化的本地流量管理解决方案。此外，软件SSL加速、服务器负载均衡和应用加速功能，为SaaS、电子商务和其他对安全连接要求较高的应用提供了一个理想的流量管理方案。vAPV支持选配链路负载均衡和全局服务器负载均衡功能。

产品架构



产品功能

应用可用性

二至七层策略和服务组管理	多层虚拟服务策略路由，静态、默认、备份策略和服务组，二至七层应用路由策略，二至七层服务保持，基于轮询、加权轮询、最少连接数、最短响应时间、SNMP、QoS DNSdomain、DNSSEC等算法的应用负载均衡
二至三层负载均衡	基于IP或MAC地址的负载均衡，适用于所有基于IP协议的应用，轮询、保持IP算法和原路返回机制（RTS），适用于防火墙、IPS/IDS、垃圾过滤、反病毒以及混合应用程序，支持二层桥接模式
四层负载均衡	TCP、TCPS和UDP协议负载均衡，支持轮询、加权轮询、最少连接数、最短响应时间算法，支持Persistent IP、Hash IP、Consistent Hash IP、Persistent IP+端口和端口段保持算法，支持所有单端口TCP应用程序、RADIUS、DNS服务器，支持混合IP应用
七层负载均衡	HTTP/HTTPS、DNS、FTP/FTPS、SIP、RTSP、RDP、RADIUS、Diameter、TCP/TCPS、UDP、IP协议负载均衡，七层内容交换（QoS Network、Clientport、SSL Session ID、SIP Session ID、HTTP URL、host name、cookie、任意header、Hash Header、query等算法），URL重定向、HTTP请求/响应改写，HTTP请求过滤，DDoS防护
服务器保持	基于源+目的IP、客户端IP、SSL Session ID、HTTP header、URL、cookie、应用信息的保持，单独会话控制
内容路由和交换	支持单臂结构，每个虚拟IP可单独配置透明或反向代理模式，可选反向代理、透明或三角模式，四层和七层策略嵌套，四层和七层策略共用
全局服务器负载均衡	全球多地域应用的高可用性，DNS DoS攻击防护，DNSSEC中间人攻击防护，全球站点/服务选择，基于就近性规则和IP持续性选择站点，支持采用SSL VPN部署的多站点间负载均衡，服务池支持SNMP算法
链路负载均衡	出向：轮询、加权轮询、最短响应时间和就近性/动态探测，入向：轮询、加权轮询、最短响应时间和就近性/动态探测，集成DNS，出向DNS代理
ePolicy™七层应用脚本	自定义SLB策略并与SLB算法配合实现后台服务的负载均衡，支持分析HTTP、SOAP、XML和Diameter等协议报文内容，支持接收、发送、分析和丢弃普通TCP和TCPS报文，支持对文本数据进行模型匹配，支持TCP连接控制，支持流量的监控与统计
eRoute四层路由	基于源/目的IP、端口、协议（TCP/UDP）的策略路由，RIPv1、RIPv2和OSPF动态路由，RTS、IPflow路由，端口转发、链路聚合和端口冗余备份，路由对VPN远程接入不可见

产品功能

应用可用性	
应用、服务器和链路健康检查	HTTP/HTTPS、TCP/TCPs、UDP、Script-TCP/TCPs/UDP、ICMP、DNS、RADIUS、SIP、RTSP、MySQL、MsSQL、LDAP协议的单个端口或协议本身的健康检查，支持多端口健康检查，基于协议和内容验证的健康检查，基于物理端口状态、ICMP、TCP和DNS的链路健康检查，支持下一跳网关健康检查、目的路径健康检查，支持单点管理多条WAN链路，确保应用的可用性和性能，支持脚本自定义组合健康检查
集群	多达32个节点，Active/Active与Active/Standby部署方式，配置同步，特定应用的虚拟IP健康检查，动态TCP失效切换，基于USB端口的快速失效切换，自动ISP链路失效切换
单系统映像	多台硬件设备或虚拟设备通过一个虚拟IP实现应用容量扩展、性能提升和可用性的增强，扩展灵活
IPv6	IPv6完整支持，DNS64和NAT64，IPv4和IPv6双协议栈支持，IPv4-IPv6与IPv6-IPv4网络地址转换和完整IPv6寻址，IPv6金牌认证
组网	链路聚合、VLAN/MNET、NTP——支持静态地址转换、基于端口的地址转换及智能地址转换实现透明使用多条WAN链路
加速	
应用性能	动态探测，客户端连接保持，连接复用，TCP缓存，IEEE 802.3ad链路聚合
SSL加速（2048和4096位加密）	硬件SSL处理，SSLv3、TLSv1、TLSv1.1、TLSv1.2、SM2v1.1，最大4096位RSA密钥，最大512位ECC密钥，端到端安全（服务器端SSL通信），SSL会话复用和超时控制，可自定义最低加密强度，自定义算法集组合，自定义SSL错误页面，双向SSL证书，多个SLB服务可共享，SSL自动校验，服务器名称指示（SNI）
压缩	硬件或软件加速，虚拟化压缩，内联HTTP代理，支持HTML、XML、Java scripts、CSS压缩，支持压缩微软文件格式（DOC、XLS、PPT）和PDF
缓存	高性能内存级HTTP缓存，兼容HTTP/1.1、HTTP/2，基于高级策略的缓存控制，基于缓存指令改写的客户端浏览器缓存控制
流量整形	应用性能保证，支持速率整形，允许用户自定义重要应用的速率限制，使用QoS对流量分级，支持基于类的队列和队列带宽的借出、借入，支持高级访问控制列表（SLB QoS），支持基于端口、TCP、UDP和ICMP协议的QoS过滤

产品功能

安全

WebWall和Web应用安全

固化操作系统，仅允许安全连接访问，支持基于客户端证书信息和访问方法的接入控制，可自定义SSL/TLS版本、算法集组合和最低加密强度，密钥和证书防篡改保护，WebWall状态报文探测防火墙，支持1000条以上的ACL规则，性能不受影响，基于代理的防火墙，TCP SYN Flood防护，Flash及Surge事件防护，DoS防护，HTTP访问方法控制，URL过滤，支持HTTP/DNS缓存缓解DDoS攻击，Web应用防火墙（WAF），深度应用数据检查以阻止SQL注入和跨站脚本等攻击，探测和回应已知应用漏洞，支持自定义规则应对潜在威胁

DDoS防护（SLB&GSLB）

防护和记录攻击日志：协议攻击：SSL无效报文、SSL握手攻击、SSL重协商、HTTP无效报文，应用攻击：HTTP慢速攻击、HTTP Flood攻击、长表格提交、Challenge Collapsar、Hashdos、DNS NXdomain Flood，网络攻击：SYN Flood、ICMP Flood、Ping of Death、Smurf、IP Option Flood，支持HTTP ACL、DNS ACL和ACL黑名单防护方式，监控和记录攻击日志：PUSH/ACK Flood、FIN/RST Flood、连接Flood、UDP Flood

SSL侦听

L2或L3模式、集成式或分布式、正向或反向代理，Webagent服务

客户端-服务器证书管理

支持RSA、ECC和SM2证书类型，以及CSR和私钥，支持自签证书，可以导入证书和私钥，支持扩展证书，支持证书备份与恢复，支持通配型证书，支持服务器名称指示（SNI），每个虚拟主机可以导入多种证书类型，每种证书可以导入三个，支持同时激活一个RSA、一个ECC和一对SM2证书

客户端证书认证与授权

快速客户端证书验证，可以导入根证书和中级CA证书，基本客户端证书验证，支持证书链，证书吊销列表（HTTP、FTP、LDAP方式）、支在线证书状态验证（OCSP：HTTP/HTTPS），基于证书的访问控制，支持内部SSL服务器、双向证书验证

客户端证书应用整合

解析不同语言和编码的客户端证书字段，支持通过HTTP header、URL和cookie传递单个字段/组以及字段格式或自定义的格式到后台应用，集成代理改写，提供详细的SSL统计数据

应用访问认证

AAA支持安全声明标记语言（SAML）、LDAP、RADIUS和开放授权（OAuth）协议，支持使用多种AAA方法的多因素验证，支持Web单点登录（SSO）和Web单点注销（SLO），支持作为SAML SP（服务服务提供商），支持对会话数、会话超时和会话重用进行限制

管理

系统

集中式集群管理，提供安全的CLI、WebUI和SSH远程管理，提供XML-RPC远程管理接口便于与第三方产品管理和监控集成，支持SNMPv2、SNMPv3和私有MIB，Syslog（基于UDP或TCP），管理员和操作员账户管理，支持电子邮件、传呼、告警功能，支持多配置文件和节点间配置同步，在线故障排除，实时监控，基于角色的权限管理，支持HTTP/2

eCloud™API接口

提供eCloud API接口，用于对接云管理系统，实现APV硬件和虚拟设备的控制和监控，协助虚拟机等组件在CloudOS操作系统内实现交互，远程管理APV系列，APV系列事件通知，集成eCloud演示，支持集成OpenStack LBaaS、VMware Cloud Orchestrator (vCO)和Microsoft System Center标准

产品规格

	支持的虚拟化平台 (64位)	支持的云平台	虚拟机配置要求
vAPV 除了硬件SSL加速之外, vAPV虚拟应用交付系统 支持所有APV特性	VMware ESXi 4.1或更高版本 XenServer 5.6或更高版本 OpenXen 4.0或更高版本 KVM 1.1.1~1.8.1及更高版本 Hyper-V (Windows Server 2012或 更高版本) 华耀AVX系列	阿里云、华为云、腾讯云、移动云、 金山云、亚马逊AWS、微软Azure、 IBM Softlayer、Vmware vCloud Air	支持1~8个虚拟CPU 最低配置需求: 4个虚拟网络适配器 2GB内存 40GB硬盘



北京华耀科技有限公司 ●

地 址: 北京市朝阳区亮马桥路40号
二十一世纪大厦B座1001-1017室
邮 编: 100125
电 话: 010-84446688
传 真: 010-84447566
技术支持: 400-600-7878
售前咨询: marketing@arraynetworks.com.cn
售后支持: support@arraynetworks.com.cn
渠道支持: channel@arraynetworks.com.cn

上海办事处

地 址: 上海市长宁区红宝石路500号
东银中心A栋1702室
邮 编: 200120
电 话: 021-68877222
传 真: 021-68878216

广州办事处

地 址: 广州市天河区珠江新城花城大道85号
高德置地广场A座2904
邮 编: 510623
电 话: 020-38251185
传 真: 020-38251123

www.arraynetworks.com.cn



关注华耀科技官方服务号