APV 应用交付系统
产品白皮书

北京信安世纪科技股份有限公司

2023 年 7 月

知识产权声明

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

北京信安世纪科技股份有限公司

地　址：北京市海淀区建枫路（南延）6 号西三旗金隅科技园 2 号楼信安大厦
邮　编：100096
网　址：http://www.infosec.com.cn
电　话：86-10-68025518
传　真：86-10-68025519
电子邮箱：support@infosec.com.cn

修订记录

修订号	日期	修订内容	编制人	审核人
1.0	2023/7/9	初版	魏建斌	

目录

1 前言

1.1 背景

随着信息技术的快速发展和业务量的不断提高，基于网络数据访问流量的不断激增，尤其金融、大型企业、数据中心、互联网应用等访问，数据日流量已达到了上千、上万 Gb/s 的级别，同时，数据交换过程中会经过网络中错综复杂的环节，且需要提供 24 小时不间断的服务，任何服务中断或通信中的关键数据丢失将会造成不可预估的损失。所以，对应用的运营者来说，任何环节处理不好，都会导致业务无法正常访问或者效率低下。比如：

- 应用系统的性能瓶颈、稳定性、可扩展性等问题
- 跨运营商访问时因路由瓶颈而导致的网络延迟问题
- 宽带和窄带用户并存时的合理分发和访问效率问题
- 应用系统面临网络攻击等问题
- 应用系统整体运行效率和提升用户体验等问题

APV 产品正是面向以上问题提出的一套技术体系，基于广域网优化、链路优化、应用交付控制等领域实现了多数据中心、多条运营链路、多台服务器间的负载流量分发机制。APV 产品除了负载均衡功能外，还注重整个应用交付的各个环节，包括服务端、客户端数据交互过程中的网络节点效率。APV 可以根据用户访问的内容做更精细化的流量分担，可以根据用户自身的信息通过 cookie 等方式做内容交换。APV 能够识别应用，进行 SSL 卸载、SSL 加速、内容压缩、应用防火墙、DDoS 防护等，让应用资源专注于自身业务处理，从而提升系统整

体效率。

1.2 参考标准

《GM/T 0002-2012 SM4 分组密码算法》

《GM/T 0003-2012 SM2 椭圆曲线公钥密码算法》

《GM/T 0004-2012 SM3 密码杂凑算法》

《GM/T 0005-2012 随机性检测规范》

《GM/T 0009-2012 SM2 密码算法使用规范》

《GM/T 0010-2012 SM2 密码算法加密签名消息语法规范》

《GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范》

《GM/T 0018-2012 密码设备应用接口规范》

《GMT 0024-2014 SSL VPN 技术规范》

《GMT 0025-2014 SSL VPN 产品规范》

《GM/T 0028-2014 密码模块安全技术要求》

1.3 术语和缩略语

名词	解释
数据完整性	表明数据没有遭受以非授权方式所作的篡改或破坏
X.509 证书标准	国际电话与电报咨询委员会(CCITT)规定的一种行业标准。在这个标准中提供了一个数字证书的标准格式，规定数字证书必须包含的一些信息：如版本号、序列号、签名算法、有效期限等
SM2 算法	一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。
SSL 协议	为网络通信提供安全及数据完整性的一种安全协议。

缩略语

缩略语	英文	中文
SLB	Sever Load Balancing	服务器负载均衡
LLB	Link Load Balance	链路负载均衡
GSLB	Global Sever Load Balance	全局负载均衡
ARP	Address Resolution Protocol	地址解析协议
NAT	Network Address Translation	地址转换
RTT	Round Trip Time	往返时间
DNS	Domain Name System	域名服务
SSL	Secure Socket Layer	安全套接层协议层。它是网景（Netscape）公司提出的基于 WEB 应用的安全协议
TTL	Time To Live	生存时间
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议

2 产品介绍

2.1 产品简介

APV 设备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。作为一个为企业级应用服务设计的应用交付解决方案，APV 设备代表了新一代的应用负载均衡和性能优化产品，仅仅通过一个功能强大的系统，即可提供高度集成的应用交付功能。

APV 设备可以提供服务器负载均衡（SLB）、链路负载均衡（LLB）以及全局负载均衡（GSLB）并具备万兆级的吞吐效率，以及深层次的应用协议和数字证书字段的分析和内容交换。不论是大中型企业还是电信运营商，应用 APV 设备解决方案，将确保您 7×24 小时的应用可用性，避免系统宕机或网络故障对营业收入带来的影响，并极大提升您的应用效率和性能，显著提高数据中心的效率和投资回报率（Return on Investment，ROI）。

2.2 国产化支持

APV 目前可以提供的信创平台产品如下：

操作系统：银河麒麟、统信 UOS 等

硬件平台：飞腾、海光、兆芯等国产平台

2.3 产品架构

产品架构主要分为服务器负载、链路负载、全局服务器负载、系统管理、高可用性、流量编排、网络、日志审计与监控等部分；

- 服务器负载：支持虚拟服务管理、后台服务/组管理、算法及策略、健康检查配置等功能，主要应用于 L2-L7 层负载方案
- 链路负载：支持入向链路配置、出向链路配置、健康检测、DNS 代理、DNS 策略等功能，主要应用于多运营商线路方案
- 全局服务器负载：支持 DNS 管理、服务管理、就近性探测系统、域名统计、全域名解析等功能，主要应用于两地三中心方案
- 应用安全：WAF、DDoS 防护等功能
- 高可用性：支持节点/域配置、可信链路配置、分组管理、失效切换规则、热备/集群管理等功能
- 流量编排：支持安全服务配置、网络规则配置、数据中心配置、服务链配置、策略管理配置等功能

- 网络：支持接口管理、桥接配置、NAT 配置、域名服务器管理、IPV6 配置等功能
- 日志审计与监控：支持监控告警、日志审计、数据报表、监控看板、数据大屏等功能。
- 配置管理：支持系统管理、管理员管理、访问控制、分区管理等功能

2.4 主要功能

功能名称	功能说明
服务器负载均衡	
服务器负载均衡算法支持	支持丰富的服务器负载均衡算法，如轮询、加权轮询、最小连接数、最快响应时间、哈希、URL、SNMP、Hostname、Cookie、Header、QoS Cookie、QoS Hostname、QoS URL、QoS Network、正则表达式等，来实现真正的合理流量分配。
服务器负载均衡策略支持	支持丰富的四、七层负载均衡策略，包括源 IP、哈希 IP、保持 TCP Option、哈希(IP+Port)、HTTP2、MQTT、 ICMP、保持 URL、插入 Cookie、保持 Cookie、重写 Cookie、嵌入 Cookie、哈希 Cookie、哈希 Header、保持 Hostname、哈希 Query、SSL Session ID、HTTP、FTP、SMTP，POP3，RADIUS、Diameter SID、SIP CID、SIP UID、NTP, DNS, SNMP、RTSP、GTP、SPDY 等多种协议。，
L2 负载均衡	基于 MAC 地址的负载均衡，将来自 VIP 网络接口的数据流导向到多个连接后台服务的网络接口上。L2 负载均衡算法不关心 IP 层、TCP 层和更高层的

	协议。
IP 层负载均衡	基于 APV 虚拟服务 IP 对应到后台应用服务器的 IP 进行三层请求负载分担，将来自用户端请求的 TCP/UDP 数据流负载均衡到的不同服务器。
IPV6 负载支持	支持 IPV6 网络环境，为 IPV6 业务网络提供负载。
非会话保持负载均衡算法	提供轮询、加权轮询、最少连接数、最快响应时间等非持续性负载均衡算法。保障客户端的不同的请求被分配到一个后台服务器组中的不同的服务器上进行处理。
会话保持负载均衡算法	具有多种持续性算法，如基于 IP 地址、基于报头或请求、基于 Cookie、基于 Session ID、URL 算法等，满足特定的客户端发出的请求始终被分配到同一个服务器上进行处理。
多层次的负载均衡策略	针对用户复杂的业务需求，APV 提供超过 22 种负载均衡策略进行支撑。如基础性策略、保持性策略、QOS 策略。尤其是在七层的负载均衡策略方面更加强大，如基于域名、Cookie、网段、报头、Hostname、URL、Header、Regex Path、数字证书、IP 等。 支持通过控制策略实现应用灰度发布，可以对不同 host 设置对应的 path 和 backend 服务，实现精细化业务控制。
全面灵活的健康检查策略	通过对服务器的实时健康检查，保证数据流量会自动绕过故障服务器或不可用服务器。当 APV 的健康检测机制检测到服务器重新恢复正常以后，将使该服务器可以自动回到服务器群之中，所有服务器故障的处理，对进行操作的用户是完全透明的。支持被动式健康检查，可根据对业务流量的观测采样，辅

	助判断应用服务器健康状况；
图片压缩	支持图片优化技术，通过对图片格式的转换，减少传输流量，提升 web 页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的 WebP 或 JPEG 格式，优化加速效果。
虚拟链接	支持虚拟链接功能，无需逻辑编程，通过配置即可实现不同负载均衡方法的多级嵌套。
反向代理模式/透明模式/三角传输模式/桥接模式	APV 支持二层桥接、三角传输模式、三层反向代理模式和透明模式，网络部署结构非常灵活，既可以是单臂结构，也可以是双臂结构。
链路负载均衡	
链路负载均衡	支持进向链路负载均衡（inbound）和出向链路负载均衡(Outbound)算法，包括轮询算法、加权轮询算法、最短响应时间算法、动态探测算法（Dynamic Detect）、最小带宽、最小连接数、HASHIP、HASH IP PORT；同时支持网络就近性(Eroutes)算法，且能够实现动静结合功能。支持最多 32 条出向链路间的负载均衡。
链路探测	支持基于 TCP、UDP、ICMP 方式的动态链路状态探测，可基于线路响应时延动态选路。
智能路由	支持基于域名的智能路由，可基于 DNS 代理实现域名记录查询。 支持基于域名的智能路由，可侦听客户端域名查询结果进行动态选路。
链路健康检查	支持健康检查算法，包括基于 ICMP 协议、DNS 协议、TCP 端口。支持附加

	链路健康检查。 支持远端站点探测机制，可自定义目标探测地址及关联子网，实现基于目标子网健康状态的局部动态选路。支持全路径健康检查方式，无跳数限制。
DNS 透明代理	支持内网用户上网 DNS 透明代理，提升多运营商链路的带宽利用率，并能够实现基于用户网段和域名的调度策略。
DNS 协议劫持	支持 DNS 协议劫持,可自动改写 DNS 响应记录为对应的 NAT 记录，无需编写脚本即可实现。
流量优化调度	支持基于链路负荷情况的优化控制机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。 支持通过优先级、队列以及设定基于应用的带宽限制和带宽容许，确保关键应用能够按时交付。 支持基于五元组条件（源 IP 地址，源端口，目的 IP 地址，目的端口，传输层协议号）来进行出站访问的流量调度分发
全局负载均衡	
DNS 解析	支持根据区域策略、默认策略等选择服务池进行 DNS 解析。 支持同一域名配置多条区域策略，区域策略根据域名和 DNS 解析请求所属的区域确定 SDNS 服务池。支持静态就近性规则，指定网段与区域关联，也支持将 IP 域表关联到 SDNS 区域，批量生成就近性规则。 支持基于 SNMP 的自定义算法进行智能 DNS 解析。

	支持动态检测服务池状态，根据检测结果进行 DNS 解析。 SDNS 监听 IP 地址，DNS 请求报文的目的 IP 地址必须在任意一个监听 IP 地址上，否则会被拒绝访问。
FULL DNS	设备可实现 Full DNS 功能，支持标准 DNS 设备工作模式，包括：可作为智能 DNS 服务器，可作为 DNS 服务器代理，可作为最终 DNS 解析设备，可作为 DNS 转发器（DNS Forwarder）。 提供递归查询、迭代查询功能； 支持标准的 DNS 记录类型，至少包括：A 记录，MX 记录，NS 记录，PTR 记录，SRV 记录，CNAME 记录，TXT 记录，SOA 记录，AAAA 记录。 支持 DNS 缓存功能，当设备收到一个 DNS 服务发送回来的记录响应，就会将它缓存下来。然后，当 APV 设备再次收到访问这条记录的客户请求时，设备会直接将缓存中的记录发送给客户端。
SDNS 健康检查	支持健康检查功能，包括： 支持 SNMP、ICMP、TCP、HTTP 和 HTTPS 类型的健康检查。 支持数据中心间的健康状态检查。
DNSSEC	支持 DNSSEC 签名，对 DNS 查询响应进行数字签名，确保响应的不可否认性和完整性保护，从而防止 DNS 劫持。 支持 DNSSEC 验证，DNS 解析器卸载 DNSSEC 记录请求和签名计算，以验证所接收的 DNS 响应签名是否正确。

	支持 DNSSEC 密钥管理，可集中管理和安全处理 DNSSEC 密钥。
DNS over HTTPS	使用国密 SSL 加密 DNS 以实现安全传输保护。DNS 允许您的网络通过 HTTPS 加密和解析 DNS 查询，而不影响响应（RPS）。 此外，DoH 可以避免客户端在访问时 DNS 被拦截、篡改。
DNS over TLS	确保 DNS 请求和响应不会通过路径上的攻击而被篡改或伪造，应用在 TCP 传输协议上增加 TLS 国密加密。DOT 确保 DNS 客户端和 DNS 服务器之间通信加密与身份验证。
DPS 系统	支持 DPS（就近性探测系统）探测算法支持往返时间（RTT）、丢包率、路由跳数（hops）、mix 等机制。
SDNS 规则	支持动态和静态 DNS ACL 功能，根据指定子网所有客户端、子网客户端受请求个数（RPS）限定。
DNS ECS	通过支持 ECS，系统可以获取发起者的真实地址并将请求发给最优的服务器。
多数据中心同步	支持多数据中心设备间通过国密算法通信实现 DNS 配置同步与健康状态的同步
Epolicy DNS	支持 epolicy 自定义流量脚本。
DNS NAT	支持内网 DNS 服务器返回的 DNS 响应中的解析 IP 地址为不能 从外部访问的内网 IP 地址的场景
HTTP DNS	支持 HTTPDNS 功能，可实现 HTTPDNS 与传统 DNS 协议间的协议转换与混合负载均衡

流量编排	
流量编排	配合负载均衡功能，支持基于策略（如域名等）将流量分发到不同的安全设备的不同业务端口和不同的后端服务器 支持自定义多种安全流量服务链，每种服务链的安全设备种类的数量可以灵活定义；同一种安全设备可以同时属于不同的服务链。
	支持整体安全流量编排，网络架构解耦，实现设备即插即用，无需改造，灵活部署，保障设备高可用，在安全设备池内指定安全设备变更时，不影响安全设备池内其他安全设备以及系统。形成资源池化管理，提升资源利用率，支持平滑横向扩容；
	支持使用主动探测发现并跟踪地址和网段，查看子网内各 IP 地址当前的状态，以及相关安全设备信息。 支持通过 2-7 层的协议对安全设备健康状态进行检查。
	支持对编排流量进行监控，对异常流量可直接进行 Bypass、阻断等操作。支持对安全设备的主动健康探测排查故障并可实现安全设备或设备资源池故障时自动跳过，，提高运维效率，节省运维成本。
	支持基于策略的安全流量编排。根据上下文关联的分流引擎及多元素分类完成流量智能引导，实现流量的按需编排，策略维度包括但不限制以下内容：源地址、目的地址、端口、IP 地理信息、域名、URL、协议等。支持基于应用（http、ftp、dns、ssh、telnet、snmp、ntp、smtp、pop3、imap）对业务进行流量编排。

	支持安全 SSL 流量可检：消除安全盲点，集中设备加解密，节省安全设备加解密消耗，规避利用 SSL 绕过安全设备；SSL 流量编排吞吐量大于 30 Gpbs、SSL 流量编排每秒新建连接数大于于 50k。
	对流量流经的安全设备进行编排，无需调整物理链路，可根据业务需求提供差异化安全服务，分配不同属性的用户流量经过不同动态服务链中安全设备，减少无需经过的设备产生不必要损耗，提升访问效率。
	支持安全设备松耦合，同种安全设备不再与单一厂商绑定。
	支持与已部署 SDN 架构的企业组合“全网统一智能流量编排方案”。
	APV 流量编排可按照不同策略（如 3 层、2 层、ICAP、TAP 等）对安全设备分组， 二层安全设备：IPS、WAF、APT、NDLP、AV 等 三层安全设备：NGFW、WAF 等 ICAP 安全设备：WSA、NGFW、GGSN、WAF 等 TAP（端口镜像）安全设备：IDS、AV、DLP 等
	支持自定义多种安全流量服务链，每种服务链的安全设备种类的数量可以灵活定义；同一种安全设备可以同时属于不同的服务链；。
	支持展示流量编排逻辑拓扑以直观地了配置信息中各单位之间的逻辑关系，如流量编排配置中流量类型、安全设备资源池、安全服务、服务链、编排策略和后台真实服务间的逻辑联系 支持为网络，地址池等资源列表自动添加自定义属性列，可以灵活添加备注信息，对安全设备的地址进行管理

SSL 功能	
B/S 应用安全代理	支持 B/S 模式的安全代理，HTTPS 方式。
C/S 应用安全代理	支持 C/S 模式的安全代理，TCPS 方式。
SSL 加速	全面提升 SSL 的处理性能，解决当前单向、双向 SSL 处理的瓶颈，可以极大地减轻 CPU 处理 SSL 加解密运算的工作，提高系统接入速度。
SSL 卸载	通过将应用访问过程中 SSL 的加解密过程转到 APV 之上，从而减少服务器端的性能压力，提升客户端的访问响应速度。
HTTP 压缩	硬件 HTTP 压缩，符合国际 HTTP 标准压缩规范。自动识别客户端对压缩算法的支持，并依次实现动态压缩。提高窄带宽访问应用的速度、保证服务质量。
WEB 高速缓存	基于内存的反向代理 Web 高速缓存功能，可以有效降低服务器的访问压力。
TCP 交付安全	支持 TCP+SSL/TLS 的安全传输通道交付服务，可以满足基于 SSL/TLS 安全协议的 TCP 网络应用系统，或是无安全策略的传统 TCP 网络应用系统，实现传输通道的快速安全保障与加速。
连接复用技术	连接复用技术改善现有系统的总体性能，其技术原理是自动实现 HTTP 1.0 到 HTTP 1.1 的转换；TCP/IP 协议栈在处理长连接时具有更好的性能；将 Web 流量的多个短连接合并为一个长连接，改善了服务器的性能。
双向 SSL 身份认证	支持双向 SSL 认证方式，客户端证书与服务器证书双方均需要相互认证。
单向 SSL 身份认证	支持单向 SSL 认证方式，只需要认证服务器证书。

重定向	支持用户请求重定向、响应重定向。
基于证书要素的访问控制	支持基于证书主题、证书有效期的访问控制，可限制指定类型证书的访问。
支持国际 SSL 协议标准	支持 SSL3.0、TLS1.0、TLS1.1、TLS1.2 等国际标准。
对称算法	支持 SM4、DES、AES 等多种对称算法。
非对称算法	支持 SM2、RSA 等多种非对称算法。
摘要算法	支持 SM3、SHA-1、SHA256、MD5 等多种摘要算法。
支持证书高密钥长度	RSA 支持 1024、2048、4096 位。
SSL 加密强度	支持 56 至 256 多种强度算法，可强制使用高安全性算法。
证书有效期验证	支持证书有效期验证。
证书状态验证	支持证书作废状态的 CRL 方式验证； 支持 OCSP 在线验证证书作废状态。
证书废止列表 CRL	可以为每个信任 CA 单独配置 CRL 验证机制；支持发布点方式的 CRL 和非发布点方式的 CRL；支持以 LDAP、FTP、HTTP 方式获取 CRL；支持 CRL 的动态获取。
证书格式	支持标准 X509V3 证书格式； 支持各大 CA 运营机构的证书； 支持中文 DN 证书。
支持与后台服务器加密通信	支持后台服务器为 SSL 类型，在内网以加密方式传输。

多站点证书	系统可以配置多个站点证书，不同的服务可以配置不同的站点证书。
支持站点证书 PKCS#10 方式证书申请	支持站点证书 PKCS#10 方式申请与导入。
多级证书链	支持多级证书信任链，即多级 CA 配置。
多信任域支持	支持配置多个信任的 CA 证书。
证书解析并向后台传递	可解析并传递以下证书信息：证书签发者、证书主题、证书序列号、证书有效期、指定证书扩展、证书实体即整张证书信息。
证书信息后传方式	支持以 Header、Cookie、URL 等方式传送证书信息到后台应用。
支持后台服务类型	支持 TCP 之上 4-7 层的所有应用服务。
访问控制	按照通道/认证方式进行访问控制，为每个资源定义多个访问控制策略，按照资源、通道/认证方式、用户证书 DN 或部分 DN 设定访问控制策略。
身份鉴别	
支持对接其他身份管理系统	通过组映射的方式，对接外部身份管理系统（Radius、LDAP、SAML、OAuth 等）完成本地资源的授权管理和访问控制。
基于 SAML 协议框架的用户身份鉴别	SAML 认证基于 SAML 2.0（Security Assertion Markup Language，安全断言标记语言）标准实现。在 SAML 框架下实现 SAML IdP（Identity Provider，身份提供者）和 SP（Service Provider，服务提供者）。
基于 OAuth 协议框架的用户身份鉴别	APV 支持使用一个第三方 OAuth 服务器进行用户认证。
LDAP/RADIUS	支持使用 LDAP/RADIUS 进行认证和授权。支持 LDAP v3 协议的所有 LDAP 服务器，包括 OpenLDAP 和活动目录（Active Directory，AD）。

	一个虚拟站点支持配置 32 个 LDAP/RADIUS 服务器。考虑到冗余性，每个服务器可以有三个主机。如果使用多个 LDAP/RADIUS 服务器，将使用主机轮询（Round Robin，rr）负载均衡来进一步提高性能。
应用安全	
WAF 防火墙	内建基于状态检测的防火墙，可抵御 DoS、SYN Flood、Buffer Overflow Attacks、Parser Evasion Attacks、Directory Traversal Attacks 等恶意攻击。
	通过正向安全模型支持人工智能(AI)参与的自动流量学习，对正常网页访问的行为（URL 路径、URL 参数、HTTP 方法、Cookie、Referrer、SOAP 动作，上传与下载的文件格式等），通过正常应用流量的特征，形成正向白名单，建立“行为安全基线”。基于学习结果动态配置，适应客户实际网络环境的防护阈值，提高攻击判定准确性。 内置自动学习模型通过对用户访问行为，访问流量、访问方式、访问地址分布等特征的学习，支持将学习结果用于动态刷新防护对象的自动 DDoS 模板，减少人工干预，提高防护准确性。
	支持 Bot 检测与防护：系统将会采集客户端运行环境信息，通过反插 JavaScript 脚本和动态内容 Cookie 判断请求等综合判定当前客户端是否为机器人。如果请求被判定为 BOT 攻击，系统则执行相应处理动作。支持通过 Mobile SDK 对手机 APP 进行 bot 防护。

	支持网页代码动态混淆：网页代码动态混淆功能支持自动识别应用服务响应网页中的非跨域 URL 地址、JavaScript 代码等，并对这些内容进行动态混淆封装，也可识别 HTML 页面中的 HTML 注释信息并进行隐藏
	支持客户端敏感信息动态混淆：用户通过浏览器访问时，通过客户端敏感信息动态混淆功能支持对终端用户通过 Form 表单提交的数据（账号密码），通过 AJAX 交的数据，以及通过 Fetch 提交的数据内容进行混淆，提升中间人攻击的难度，从而防止中间人攻击、请求伪造、窃听或篡改请求数据包等行为
	支持 WAAP 安全防护能力，支持根据具体 url 配置安全防护策略，包括是否拦截策略、逃逸策略、BOT 防护策略。配置包含执行模式、逃避、机器人防御、服务器技术等关键配置项。
DDoS 防护	设备的 DDoS 攻击防御功能针对三个协议层的 DDoS 攻击提供攻击探测和防御机制，为服务器负载均衡业务提供更高一层的安全防护。 支持基于业务流量模型自动化设定七层 DDoS 安全防护策略，自动触发防护机制。 支持 DNS DDoS 防护功能，可自动过滤攻击流量并基于记录类型进行统计
	支持流量限速攻击防护，可以基于 IP 地址、MAC 地址和接口级限速、支持 IP 地址、MAC 地址黑名单、白名单
	支持攻击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，监控和记录攻击日志：PUSH/ACK Flood、FIN/RST Flood、连接 Flood、UDP Flood
网络配置	
接口配置	支持根据网口动态展示接口数量
DHCP 支持	支持 DHCP 功能，IP 地址池容量 20 万。在自动分配地址之前，自动检测下该 IP 地址是否已经占用。支持 IP 地址冲突检测，冲突地址隔离和隔离冲突地址定期回收功能。
NAT 支持	支持静态 NAT、网络地址端口 NAT 转换、地址池的动态 NAT 转换、目的 IP 的地址转换。最大支持大于 1024 条 NAT 策略。 支持基于地址池（pool）的地址转换。设备能将内网网段映射为指定的公网地址池（NAT pool），而非一个公网 IP 的方式。支持智能、均匀的选取地址池中的地址资源。
动态路由协议支持	支持 RIPv1、RIPv2 和 OSPF。
IPV6 支持	支持 IPV6，设备需兼容 IPV4 与 IPV6 网络并存，支持设备和后台服务支持 IPV6 to IPV4 与 IPV4 to IPV6 模式下的地址转换。
高可用性	
集群	针对本身设备的高可用性，支持 Active-Active、Active-Standby、N+M 模式，以达到系统本身的高可用性，最多可以做到 32 台设备的集群。支持心跳

	集群部署，通过心跳线连接支撑两台设备之间进行集群。
节点管理	支持对 HA 域中的每台设备进行管理
分组管理	支持浮动 IP 分组，保证设备切换的一致性和灵活性，浮动 IP 的切换按照分组进行，每个浮动 IP 必须加入浮动 IP 分组实现状态切换。同一个分组中的所有浮动 IP 在同一时刻保持相同状态。
链路配置	HA 可靠链路通过多种通信链路交互各自的状态信息，从而确保通信的高可靠性。通信链路分为 FFO 链路、主链路、备用链路。
心跳检测	支持双机热备部署方式，可自动同步配置并支持 FFO 专用心跳线双机 failover 切换功能，能够及时发现设备故障，实现无缝快速故障切换。
失效切换规则（failover）	在 HA 域中，HA 模块会对系统状态和网络状况进行健康检查。当健康检查的结果表明节点出现故障并满足定义的分组切换条件时，要进行切换操作
日志审计与监控	
本地日志主机	本地 syslog 主机可以为每个日志级别存储最多 50,000 条系统日志。
日志服务器	为了使管理员能够存储所有历史系统日志以备将来进行系统故障排除，日志功能允许将指定日志级别的系统日志消息发送并存储在远程日志服务器上；
标准化日志格式	APV 支持 RFC 5424syslog 功能。 支持四种标准 APV HTTP 访问日志格式：组合、WELF、正常和扫描等。
精细化日志类型	APV 设备支持以下日志记录类型： • 访问日志：记录认证和会话、Web 访问、TCP 应用和注销以及 HTTP 请求和响应的信息。每次访问内部网络资源都会生成一个日志条目。 • 管理日志：记录通过 CLI 或 WebUI 对设备进行配置的操作信息。 通过上述两种日志进行建模，可以实现对用户（包括管理员用户）的所有访

	问、操作行为的监控和审计。
SNMP 监控和管理	APV 设备支持 SNMP v1、v2 和 v3 版本，维护并提供自有 SNMP MIB 供管理员对设备进行监控和管理
	支持与交换机联动，主动采集交换机信息，包括端口信息、接口信息、路由信息、ARP /ND 信息等，实现网络管理可视化
数据统计	智能监控告警系统支持对 CPU 使用率、内存使用率、硬盘使用率、磁盘 IO、网络连接数、NTP、电源和 CPU 的温度、风扇等资源使用情况信息的图形化监控统计分析。 支持大屏展示，能够显示新建连接数、并发连接数、吞吐情况、SSL 新建和 SSL 吞吐数据、SSL 卡使用率、压缩卡数据压缩比例等信息 具备 E-mail、SNMP Trap 等告警方式，管理员可基于业务需求选择告警触发事件，当业务触发条件时，会自动向管理员发送告警信息。
配置管理	
CLI/WebUI	同时支持命令行和 WebUI 管理界面。
XMLRPC	支持使用 XMLRPC，通过命令行方式，对 APV 进行查询和配置。
Restful API	支持通过 Restful API 命令行接口对 APV 进行管理，支持运行单个命令以及批量运行。
云原生平台支持	支持云原生环境下的负载均衡功能集成管理，支持 K8S、OpenStack 等云平台，通过云平台支持应用服务地址和端口的发现和注册，并自动在应答设备上配置生效，保持应用服务地址和端口与应答设备上的配置一致。

	支持识别 K8S 集群的 POD 和服务状态的脚本，实现 4-7 层的应用服务路由。可以对 4 层业务设置 monitor 进行健康检查，并且针对 7 层业务可以设置健康检查的 path、timeout、interva 等。
	支持容器环境下的应用和服务自动编排，能够清晰明确展示对应的 configmap 配置脚本，可以调用 AS3 自动化运维脚本进行业务地址和端口的配置下发。
分区管理支持	分区功能可以通过一台物理设备服务多个租户，不同租户的管理、业务分发系统都相互独立，实现了多租户环境下的业务隔离，从而降低租户拥有成本。系统支持的分区总数取决于系统内存，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。
系统备份/恢复	可以备份当前服务配置，保证系统瘫痪时的快速恢复。各分区可独立恢复备份不影响其他分区业务。
软件升级	支持多重引导，设备支持四个引导分区，提供供软件一键自动版本升级更新。各分区可独立实现操作系统升级不影响其他分区业务。
同步备份	支持全量配置、增量配置同步、实时配置同步、启动配置同步、配置回退等
三权分立	支持管理员角色管理、多级授权管理、支持 AAA 认证、授权模式。

3 产品特性

3.1 多种负载均衡及丰富的策略算法

- 支持服务器负载、链路负载、全局负载等多种负载均衡方式
- 支持动态与静态负载均衡调度算法。具备轮询、加权轮询、最小连接数、最快响应时间、哈希、URL、SNMP、Hostname、Cookie、Header、QoS Cookie、QoS Hostname、QoS URL、QoS Network、正则表达式等负载均衡算法。不同调度算法所实现的负载均衡效果不同，可以根据具体的应用场景，采用不同的算法。
- 支持主动和被动健康检查方式，并具备丰富的健康检查策略，基于 ICMP、TCP、UDP、HTTP、HTTPS、FTP、SNMP、DNS、Radius、SIP、RTSP、LDAP、ORACLE、MSSQL、MYSQL 等多种服务器健康检查方式，且设备能够支持通过 SCRIPT-TCP、SCRIPT-UDP 应用脚本方式，对服务器的 FTP, SMTP, LDAP, RADIUS, POP3, DNS, TELNET 等多种应用进行检查。
- 支持丰富的四、七层会话保持功能，包括基于 PI、HI、CHI、Persistent TCP Option、Hash (IP+Port)、Persistent URL、Insert Cookie、Persistent Cookie、Rewrite Cookie、Embed Cookie、Hash-Cookie、Hash Header、Persistent Hostname、Hash Query、SSL Session ID、Raduname、Radsid、Diametersid、Sipcid、Sipuid 等多种会话保持技术

3.2 部署架构重塑，流量编排安全可控

- 支持整体安全流量编排，网络架构解耦，实现设备即插即用，无需改造，灵

活部署，保障设备高可用，形成资源池化提升资源利用率，支持平滑横向扩容；

- 支持基于策略智能排查故障，提高运维效率，节省运维成本；
- 支持安全 SSL 流量可检：消除安全盲点，集中设备加解密，节省安全设备加解密消耗，规避利用 SSL 绕过安全设备；
- 支持流量流经的安全设备编排，无需调整物理链路，可根据业务需求提供差异化安全服务，减少无需经过的设备产生不必要损耗，提升访问效率；
- 支持安全设备松耦合，同种安全设备不在与单一厂商绑定。
- 支持与已部署 SDN 架构的企业组合“全网统一智能流量编排方案”

3.3 SSL 与服务器负载均衡无缝结合

- 针对整个应用系统，将 SSL 与负载均衡整合，减少了一个网络节点，减少系统故障点，更便于维护，系统响应延迟更小；
- 在统一对外的 SSL 服务中，可应用 APV 的 7 层负载均衡功能，将多种业务系统整合统一对外发布，提升用户体验，减少系统开支。

3.4 强大的 SSL 安全功能

- 身份鉴别高安全性，支持 SSL/TLS 协议族，支持单、双向身份认证，支持高强度加密算法，为应用提供可靠的身份认证方案，支持多种证书状态验证模式，包括 CRL（支持 LDAP、FTP、HTTP 协议）、OCSP 方式；
- 支持标准的 PKCS#10 证书请求、X509V3 证书，支持国内外各大证书运营商的证书；

- 支持多种网络通信协议，与多种网络应用系统无缝集成，支持所有基于 TCP 协议之上的应用，包括 HTTP、FTP 等多种常用协议；
- 支持应用重定向功能，能根据用户证书属性进行应用重定向，限制或允许特定证书对应用的访问。

3.5 支持国密标准

- 支持国家密码管理局颁布的规范《GMT 0024-2014 SSL VPN 技术规范》《GMT 0025-2014 SSL VPN 产品规范》;
- 支持国际标准算法，支持国家密码管理局提供的国密 SM2/SM3/SM4 算法；产品完全自主可控。

3.6 虚拟化分区与云部署

- 采用 Segmentation 技术实现单台设备最高支持 1024 个虚拟分区，分区之间实现逻辑隔离，并且具备独立配置管理。
- 可在阿里云、华为云、腾讯云等常见公有云上软件部署

3.7 IPV6 支持

IPV6 解决方案为客户的应用交付提供了 IPv6-to-IPv4 和 IPv4-to-IPv6 转换技术，帮助客户将应用业务平滑和无缝迁移到 IPv6 网络，解决 IPv6 升级改造过程中遇到的“IPv6 天窗”等问题，提供与 IPv4 应用交付一致的性能、稳定性和高可用性，为用户提供最佳的应用体验。

IPv6 网关产品系列针对客户的应用、网络和基础设施的 IPv6 改造提供了提供如下解决方案：

- **IPv6 应用交付**

该解决方案为客户的应用交付提供了 IPv6-to-IPv4 和 IPv4-to-IPv6 转换技术，帮助客户将应用业务平滑和无缝迁移到 IPv6 网络，解决 IPv6 升级改造过程中遇到的“IPv6 天窗”等问题，提供与 IPv4 应用交付一致的性能、稳定性和高可用性，为用户提供最佳的应用体验。

- **IPv6 智能 DNS 服务器**

该解决方案可以帮助客户完成域名系统（DNS）的 IPv6 改造，根据客户的网络和应用状态智能选择最佳解析结果，有效提升域名系统解析性能和应用访问效率。

- **IPv4/IPv6 边界网关**

该解决方案提供 NAT64/DNS64 和 NAT46/DNS46 功能，帮助客户实现 IPv4 网络和 IPv6 网络之间的智能转换，从而实现互联互通。

3.8 提高整体安全性

- 支持非法访问隔离，隔离对后台服务器的非法访问，全面的智能分析和控制功能（流量控制、应用重定向、ACL），实现按需访问；
- 内建基于状态检测防火墙，可抵御 DoS、SYN Flood、Buffer Overflow Attacks、Parser Evasion Attacks、Directory Traversal Attacks 等恶意攻击；
- 全面的高性能网络地址转换（NAT），支持静态的基于端口的 FWD，隔离企业内网和外网，保护系统内网安全；
- 多种管理方式，产品支持主控端口方式管理、远程 SSH 管理、远程 Web 界

面管理等多种方式，且可开启或关闭远程管理方式，产品支持多管理用户、支持一般查询和配置权限分级。

3.9 可维护性

- APV 支持多种语言管理界面，提供快速配置功能，可通过 Web 图形管理界面或简单易用的命令行界面，进行直观的配置和管理，实时监控图表，为排查问题、决策分析等提供参考依据；
- 强大的审计功能，提供包括系统、操作、访问和调试的详细日志记录，可帮助管理员进行迅速的故障排查；
- 支持 SNMP、SYSLOG、RMON 和 Email 告警等功能，便于第三方网络管理软件集成，保障系统稳定运行；
- 具有按需授权，能在不升级硬件的情况下增加负载均衡模块，具有高度灵活性和可扩展性；
- 支持 epolicy 七层应用脚本与 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流量管理，且性能和扩展性不受影响；

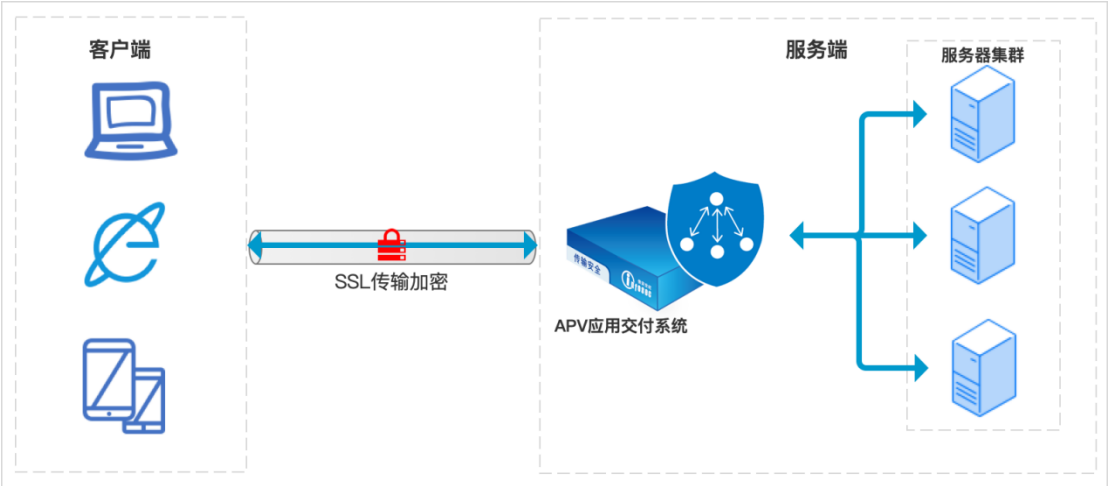
3.10 众多的高安全/高可用性应用案例

- 在网上银行、网上支付、网络财务等高安全、高可用性需求的应用案例众多；
- 在金融、政府、能源、烟草、教育等众多行业广泛应用，支持多种业务系统和办公系统，为用户核心业务提供负载均衡同时提供 SSL 卸载能力；

4 典型场景

4.1 服务器负载均衡（SLB）

当应用服务流量剧增，造成服务响应压力过高时，可采用 APV 产品的负载模式，设备支持 OSI 模型中二层、三层、四层和七层的负载均衡。二层负载均衡基于网络接口。三层负载均衡基于服务器 IP 地址。四层负载均衡与 TCP 或 UDP 端口有关。七层负载均衡是基于应用层的信息，如 URL、HTTP 表头或 Cookie。通过多种负载算法、健康检查、会话保持等功能，保障数据流量均衡分发，缓解单台业务服务器压力，同时支持 SSL 卸载能力，确保数据传输安全。



4.1.1 方案优势

✓ 安全可靠的应用级负载

当应用访问流量激增时，单台服务器已无法满足的业务访问带来的压力，此时，应用 APV 设备通过对应用服务进行轮询、加权、最小连接数或哈希等多种负载算法实现流量均衡分发，有效缓解单台设备的流量压力；还能对服务器进行健康状态检查，确保每台应用服务健康可靠。为提高应用服务的响应效率，APV

会记录访问的会话状态，以解决用户在一定时间内重复访问进行重新连接造成的性能损耗。

✓ SSL 安全传输加固

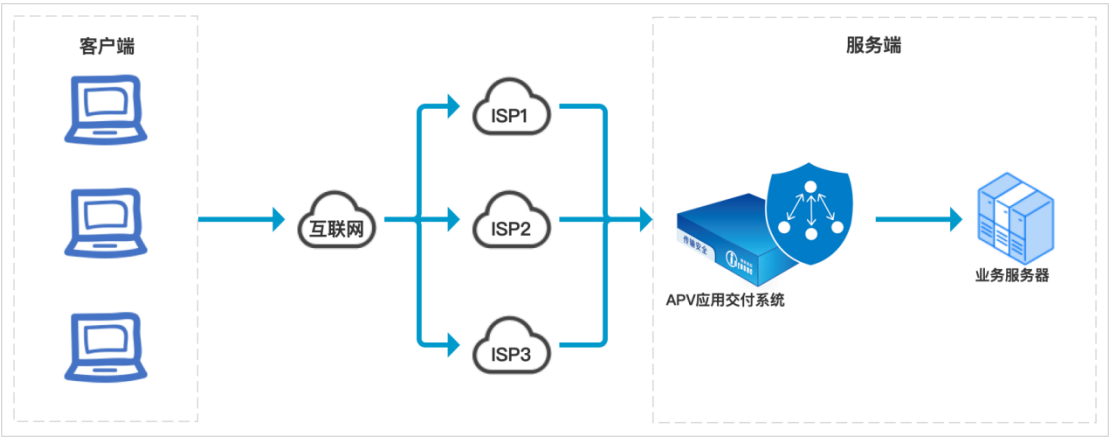
APV 设备不仅可以实现服务器负载均衡，还可以实现应用的 SSL 卸载能力，通过 APV 与客户端建立 SSL 连接，实现数据传输加密，确保通信数据的机密性与完整性。

✓ 数据同步

多台 APV 设备做集群，并且可手动或自动同步配置策略、会话状态、应用服务等。

4.2 链路负载均衡（LLB）

链路负载均衡分为 Outbound 与 Inbound 两种情况，Inbound 链路负载均衡主要解决的是位于互联网外部的用户如何在访同企业内部网站和业务系统时动态地在多条链路上平衡分配，并在一条链路中断时能够智能地自动切换到另一条可用链路；



Outbound 链路负载均衡主要解决的是企业内部业务系统访问外部互联网服务时如何在多条不同的链路中动态分配和负载均衡的问题。

4.2.1 方案优势

- 入向链路稳定可靠性

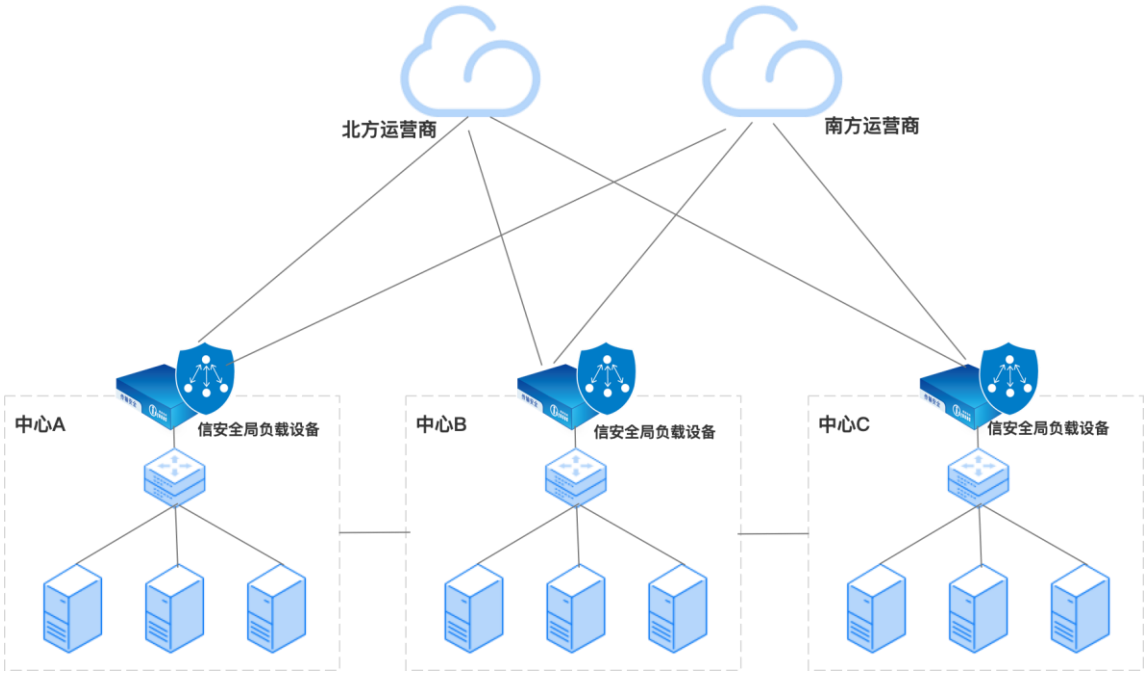
当网络有多家运营商时，可分别把运营商的地址对应到同一个设备或同一个后台服务上，通过 ARP、ICMP、TCP、DNS 等多种健康检查方式与轮询、加权轮询、就近性算法等负载均衡算法的组合实现最优链路的选择，提高网络链路可靠性。

- 出向链路最优选择

当数据流出时，APV 会根据多种健康检查状态与负载均衡算法组合，选择网络负载最小的线路发送数据，提高响应效率与容错机率。

4.3 全局负载均衡（GSLB）

全局负载均衡主要应用在多数据中心的场景。通过应用 GSLB 技术可以使外部互联网用户接入距离较近的数据中心，提升响应效率；可以在多个数据中心之间进行同步备份、健康检查等，当探测到某个数据中心发生故障时，GSLB 可将流量引流致其他数据中心进行 DNS 处理，从而提高服务的可靠性。



4.3.1 方案优势

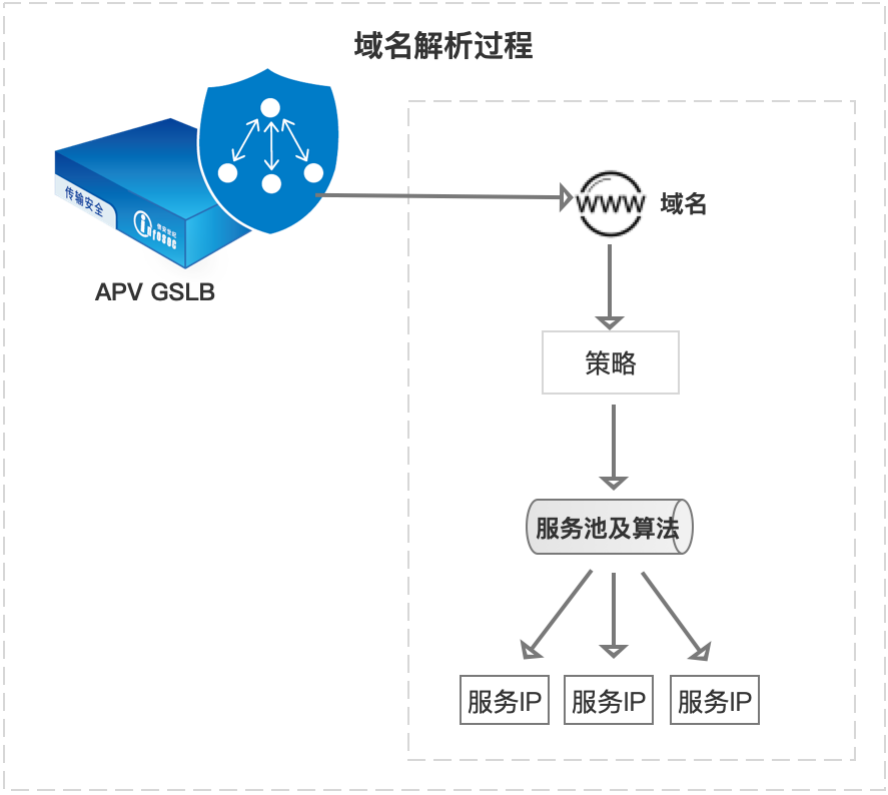
✓ 提升响应速率

当客户端发送域名解析请求后，由本地服务器进行迭代查询，同时各站点 DPS 探测器通过往返时间、丢包率、路由跳数或混合等方式探测与每个本地 DNS 的距离信息并上报 DPS 服务器，根据探测状态决定由哪台 APV 设备发送对应的域名解析结果。

✓ 安全可靠的后台服务

做 DPS 距离探测时，APV 设备会同步采用 ICMP、TCP、HTTP、HTTPS 或 SNMP 数据收集模板等健康检查方式对后台服务进行状态检测，确保后台服务安全可用。

同时，APV 设备可以将多个解析 IP 地址添加到一个服务池，并根据服务池算法与策略确定返回的服务 IP，为确保服务池的可靠性，APV 具备服务池失效自动切换、手动切换以及抢占功能，保证返回解析 IP 的可靠。



✓ 解析数据安全传输

传统 DNS 在发出域名解析请求时，通常以明文的形式发出，在传输过程中数据会产生篡改、泄露等安全问题。因此，APV GSLB 为解决该问题提供了 DNS over HTTPS、DNS over TLS 安全传输能力，确保 DNS 解析数据在传输过程中安全可靠，避免受到攻击篡改与泄露问题。

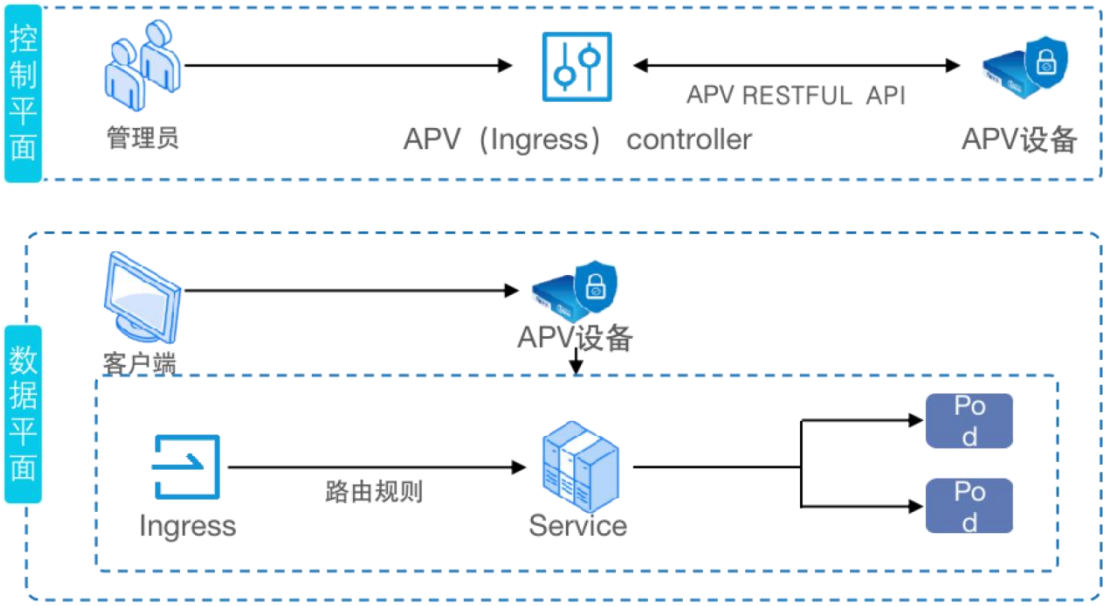
✓ 数据安全同步

各个数据中心通过建立国密传输通道实现业务数据、健康状态等信息进行实时、增量同步。

4.4 云部署场景

支持云原生环境下的负载均衡功能集成管理，支持 K8S、OpenStack LBaaS 等云平台，并提供详细方案。LBaaS (Load Balancer as a service)指负载均衡

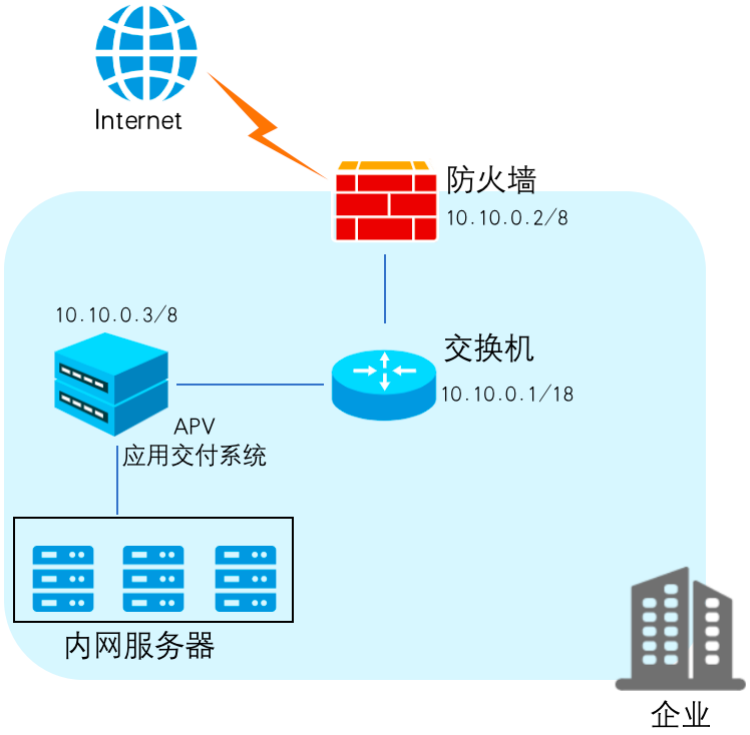
作为服务，为用户提供集群负载解决方案通过 OpenStack 配置 APV，进而使 APV 能处理租户的业务流量。Kubernetes 支持用户通过其提供的 CLI 或者 API 接口来管理 APV 设备。



- 客户端将请求发送到 APV 设备上
- 控制器会不断的跟 Kubernetes API 打交道，实时感知后端 Service，Ingress 等的变化
- 控制器感知到后端 Service，Ingress 等变化后，会把其变化的内容翻译成 APV 的相应命令，通过 APV 提供的 RESTful API 实时传递给 APV 设备
- APV 根据用户在 controller 设定的负载规则选择流量要到达的 Pod

5 部署方式

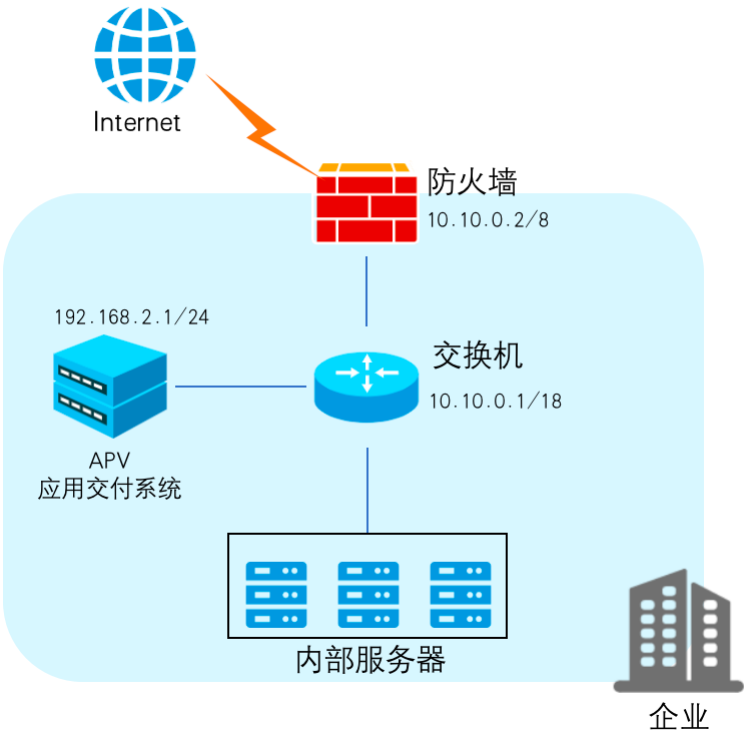
5.1 双臂部署方式



双臂方式特点介绍如下：

- **“双臂串行”**部署使用 APV 设备的两个接口来分别处理所有入站和出站的流量。在该场景中，一个接口连接到 Internet（或其他一些出站设备，例如网关路由器、防火墙等），另一个接口连接到安全的内部网络。该种部署方式需改变网络拓扑环境。
- 访问应用服务器使用的地址均归属于由 APV 应用交付系统分配的虚拟地址，负载将流量均衡分发到应用服务器间从而提高应用服务器区域的处理效率。
- APV 应用交付系统与用户客户端之间通讯建立在加密隧道基础之上，即使网络中存在信息窃取的非法行为，也只能获取到加密后的信息且无法解析信息内容，保证了应用系统用户信息隐私安全。

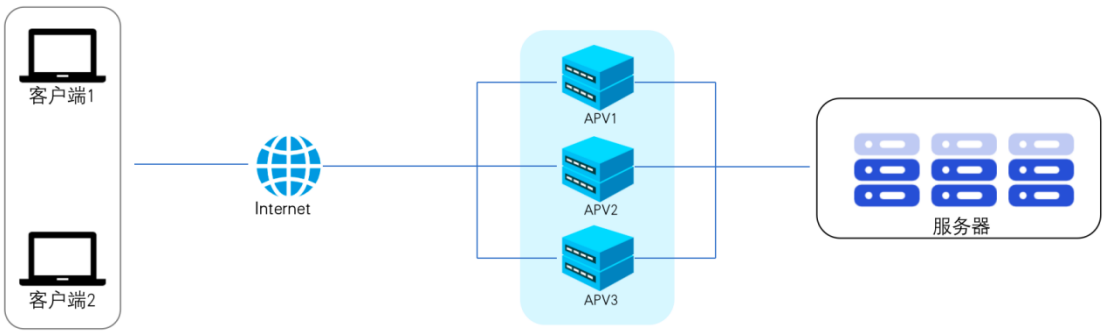
5.2 单臂部署方式



单臂方式特点介绍：

- **“单臂并行”**部署使用 APV 设备上的一个接口出入站，该部署方式无需改造网络架构。

5.3 集群部署模式



集群技术允许两台或更多的 APV 设备相互连接组成一台逻辑设备，对外提供一个 VIP，以便为本地站点提供高可靠性和高可用性。

6 产品规格

6.1 产品型号

产品型号	APV2860	APV5860	APV7860
设备形态	1U	1U	2U
四层吞吐	30Gbps	60Gbps	220Gbps
网络端口（可选配）	支持千兆电口、千兆光口、万兆光口	支持千兆电口、千兆光口、万兆光口	支持千兆电口、千兆光口、万兆光口、40G 光口、100G 光口
电源	双电源	双电源	双电源
工作电压	100-240VAC	100-240VAC	100-240VAC
最大功率	80W	300W	850W
尺寸（MM）	435mm（W）× 537mm（D）× 44.5mm（H）	435mm（W）× 537mm（D）× 44.5mm（H）	435mm（W）× 537mm（D）× 88.9mm（H）
重量	8.35 公斤（18.4 磅）	8.35 公斤（18.4 磅）	13.6 公斤（30.0 磅）

产品型号	产品描述	端口配置	性能参数
APV7860	模块化 2U 设备 双电源 850W 国产海光 32 核 64 线程 CPU 1T HDD 硬盘 128G 内存 银河麒麟 V10 国产操作系统 支持双机 HA 和集群部署。	4 个 100G 光口 16 个 10G 光口 (配多模光模块)	七层每秒请求数 944 万 RPS 最大四层并发连接数 2.2 亿 最大四层吞吐量 220Gbps 最大七层吞吐量 200Gbps SSL 最大并发连接数 1500 万 SSL 每秒新建连接数 9.9 万/TPS（RSA 2K 密钥） SSL 卸载能力 9.9 万/TPS（RSA 2K 密钥） DHCP IP 地址容量 20 万

7 产品资质

- 公安部销售许可（增强级）
- 计算机软件著作权登记证书
- IPV6 Ready Logo 认证
- 中国国家强制性产品认证证书
- 信息技术产品安全测试证书
- 电信设备进网许可证