APV GSLB
技术白皮书

北京信安世纪科技股份有限公司

2023 年 1 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	2023/1/5	初版	魏建斌	

目录

1 前言

1.1 背景

互联网发展至今已经成为了生活中不可或缺的一部分，从社交、医疗、金融、购物到生活所需都离不开互联网，随着互联网的广泛应用，网络攻击也层出不穷。DNS 域名系统作为互联网的核心服务，同时也是各大重要行业中两地三中心场景的核心服务，自然成为网络攻击的一大主要目标，如果 DNS 服务被攻击，将会造成大面积网络应用瘫痪。除此之外，传统 DNS 存在处理性能差、管理复杂、安全性差等问题，当面临大规模的网络访问时上述隐患将会随之爆发，这会对企业造成不可预估的损失，因此 DNS 服务早已不是简单的地址解析能力可以满足。

随着技术的发展、标准的制定、政策的推动，DNS 作为两地三中心方案中建设的基础设施之一，需要通过 GSLB 技术实现链路优选、多数据中心同步、攻击防护、灾备切换、性能优化、可扩展性强等更多方面的能力来满足服务需求。稳定的域名解析服务是影响业务系统运行的基础，因此，构建高可用的 DNS 服务，需具备完善的容灾、恢复机制、可管理和可扩展等能力至关重要。

1.2 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
SM2 算法	一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

缩略语

缩略语	英文	中文
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
SDNS	Smart Domain Name System	智能域名服务
DNS	Domain Name System	域名服务
DNSSEC	Domain Name System Security Extensions	DNS 安全扩展
TTL	Time To Live	生存时间
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议

2 产品概述

2.1 产品简介

APV GSLB 产品采用自研的高性能体系架构提供安全可靠的智能域名解析能力（简称 SDNS），能够极大地提高企业域名解析服务的可用性、高性能以及安全性的同时，降低企业数据中心软硬件投入成本和网络改造复杂性。随着广域网负载应用需求不断提升，面临的 DNS 安全、DNS 数据中心同步以及 DNS 响应速率等问题也随之增加。因此，APV GSLB 提供 SDNS 服务、DDOS 攻击防护、数据中心同步（国密）与运行监控等功能解决面临的风险。APV GSLB 利用 DPS（就近性系统）功能实现最优线路选择以达到快速响应速率，提升用户体验。并具备安全防护能力，可有效预防 DNS DDOS 攻击、DNS 缓存投毒、DNS 流量劫持等攻击行为，将有助于保护用户业务系统稳定性与可用性。与此同时，为提高运维工作效率，系统提供 DNS 监控与系统运行状态监控，便于资源按需扩展。作为网络世界“道路交通的导航系统”，APV GSLB 不仅仅适用于两地三中心场景，还适用于内外网 DNS 解析以及 DNS 数据防劫持等场景。

不论是大中型企业还是电信运营商，应用 APV GSLB 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安全性和性能，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 GSLB 目前可以提供的信创平台产品如下：

操作系统：银河麒麟、统信等

硬件平台：飞腾、海光等国产平台

2.3 产品架构

产品架构主要分为 DNS 功能、安全防护、系统管理、高可用性、网络、日志审计与监控等部分；

- DNS 功能：支持智能 DNS、DNSSEC、DNS over HTTPS、DNS SLB、LLB DNS 等功能。
- 安全防护：支持 WAF 防火墙、DNS 攻击防御、DDOS 攻击日志、DDOS 黑

名单、ACL 黑名单等功能

- 系统管理：支持系统管理、同步备份、管理员管理、访问控制、分区管理等功能
- 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
- 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。

2.4 主要功能

功能名称	功能说明
DNS 功能	
SDNS 解析	支持根据静态区域策略、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。 支持多种服务池算法，如：轮询、加权轮询、IP 优先、哈希 IP、丢弃以及基于 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（服务池自动失效切换），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，PRT 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：ICMP、TCP、UDP、HTTP 和 HTTPS 类型的健康检查。支持健康检查模板功能 支持数据中心间的健康状态检查。
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
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	使用 TLS 国密加密 TCP 传输协议实现安全传输保护，确保 DNS 请求和响应不会受到攻击而被篡改或伪造。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。
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。
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。
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
DNS SLB	支持 L2-L7 层负载均衡功能，通过定义灵活多样的负载均衡策略，依据丰富的服务器负载均衡算法（包括轮询算法、最少连接算法、最短响应

	时间算法、散列算法等），来实现真正的合理流量分配。
	支持主动健康检查和被动健康检查策略，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。可支持 DNS 类型的健康检查与基于 TCP、UDP 连接提供通用脚本的健康检查
LLB DNS	支持入向链路负载均衡（inbound）和出向链路负载均衡(Outbound)算法，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。 入向链路的 DNS 服务会对已配置的域名进行解析，解析的结果包含 ISP1 或 ISP2 的 IP 地址，它们都对应着同一个设备或同一个后台服务。如果其中一个 ISP 的链路不通，DNS 服务器将不会把该 ISP 的 IP 放到解析结果中。
	支持健康检查算法，包括基于 DNS 协议。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。 支持指定链路 HC 策略（状态）与指定域名健康状态关联
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、域名、带宽的调度策略。

安全防护	
WAF 防火墙	内建基于状态检测的防火墙，可抵御 SYN Flood、Buffer Overflow Attacks、Parser Evasion Attacks 等恶意攻击。
DDoS 攻击防御	支持 DNS DDoS 防护功能，可根据域名请求类型、响应类型、记录类型、记录内容设置 QPS/PerIP 防护基线，支持防御 DNS 查询 Flood、防御 DNS 响应 Flood 等。
DDOS 攻击日志	所有 DDoS 攻击都会被记录到 DDoS 攻击日志，日志可到处本地。
DDOS 黑名单	DDoS 黑名单记录系统探测到的最近 2000 条攻击记录
ACL 黑名单	ACL 黑名单里记录所有被完全禁止访问的 IP 地址，如果一个 IP 地址被加入 ACL 黑名单，来自该地址的所有报文都会被丢弃。
系统管理	
云原生平台	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，并提供详细方案。
Segmentation	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。
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。

恢复出厂设置	系统具有恢复默认设置功能，方便使用。
软件升级	提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。
数据统计	支持对 CPU、内存、磁盘 IO、网络连接数、服务等资源使用情况信息的图形化统计。 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、数据压缩比例、DNS 业务监控（DNS 服务状态、实时 QPS、时段 QPS、域名解析排行、类型、递归数、解析成功率等）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。
同步备份	支持全量配置、增量配置同步、实时配置同步、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。可为不同管理员基于“域”授权不同的管理权限
网络配置	
接口配置	支持根据网口动态展示接口数量
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。支持 NAT64/DNS64 与 NAT46/DNS46。
高可用性	
集群	对本身设备的集群采用 HA，支持 Active-Active、Active-Standby 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
Email 系统告警	支持通过 Email 方式将管理员预设的告警信息发送至指定邮箱，完成对设备的监控。

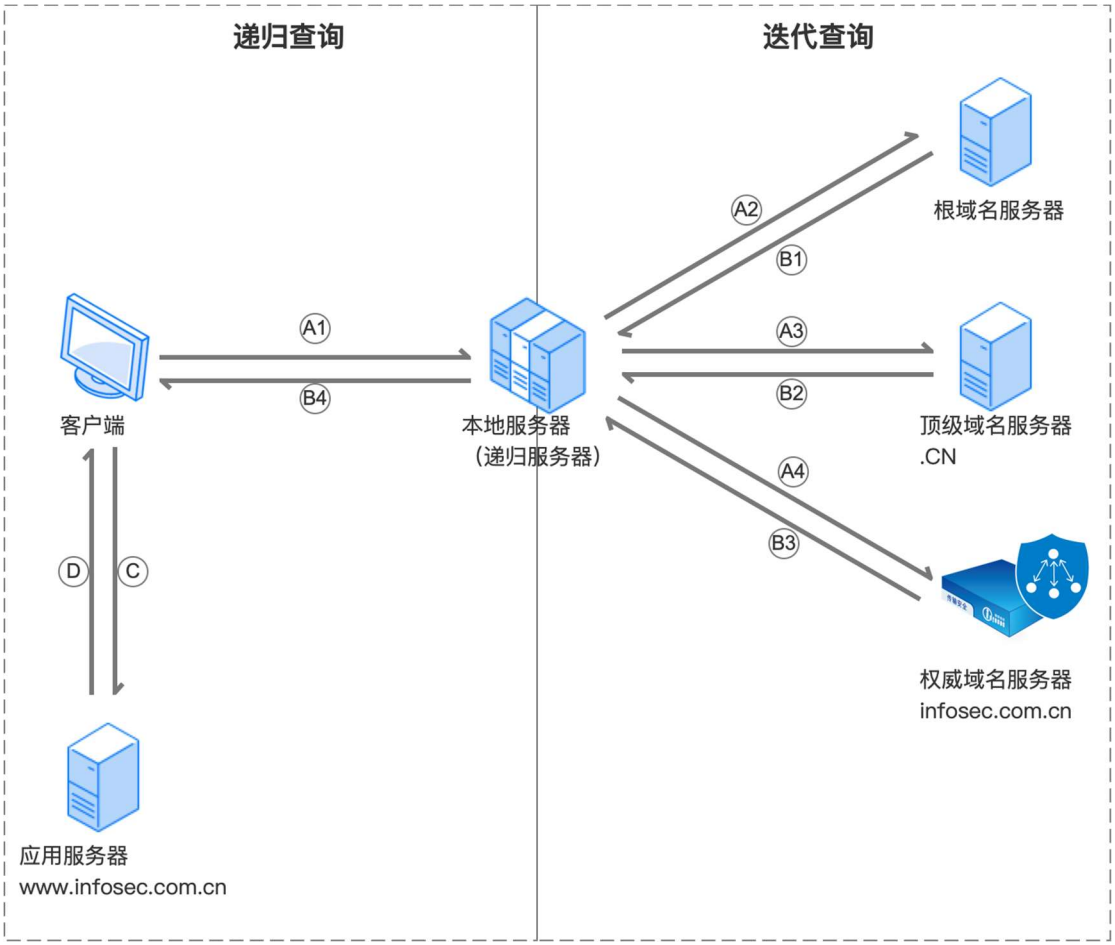
配置管理	
CLI/WebUI	同时支持支持命令行和 Web 管理界面。
XMLRPC	支持使用 XMLRPC，通过命令行方式，对 APV GSLB 进行查询和配置。
Restful API	支持通过 Restful API 命令行接口对 APV GSLB 进行管理，支持运行单个命令以及批量运行。

2.5 DNS 工作原理

2.5.1 DNS 解析原理

递归查询：DNS 服务器收到一个域名解析请求时，如果所要检索的资源记录不在本地，DNS 服务器将和自己的上一层服务器交互，获得最终的答案，并将其返回给客户。

迭代查询：DNS 服务器收到解析请求，首先在本地的数据库中查找是否有相应的资源记录，如果没有，则向客户端提供另外一个 DNS 服务器的地址，客户端则再次把解析请求发送给新的 DNS 服务器地址。



1. 客户端向所配置的本地服务器发出解析 infosec.com.cn 域名的 DNS 请求报文（A1）。

2. 本地服务器收到请求后，先查询本地缓存。若没有查到该域名对应记录，则本地服务器向所配置的根域名服务器发出请求解析.cn 域名的 DNS 请求报文(A2)。

3. 根域名服务器收到查询请求后，通过查询得到.cn 顶级域名所对应顶级域名服务器，然后向本地服务器返回应答报文（B1）。

4. 本地服务器在收到根域名服务器的 DNS 应答报文，得到.cn 顶级域名所对应的顶级域名服务器地址后，再次向对应的顶级域名服务器发送一条请求解析 infosec.com.cn 域名的 DNS 请求报文（A3）。

5. 顶级域名服务器在收到 DNS 请求报文后，先查询自己的缓存，若没有该域名的记录项，则查询 infosec.com.cn 所对应的权威域名服务器，然后向本地服务

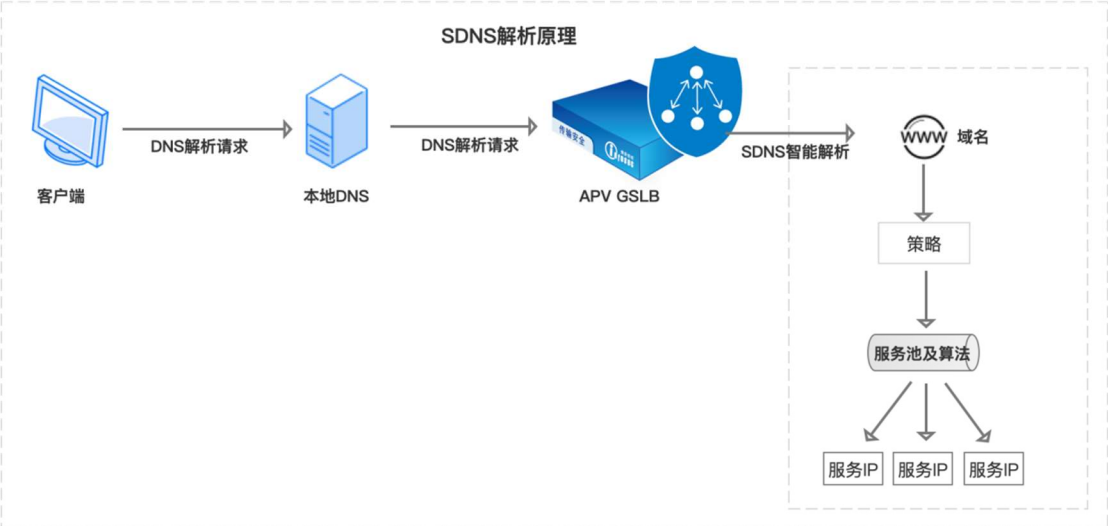
器返回一条应答报文（B2）。

6. 本地服务器收到顶级域名服务器的 DNS 应答报文，得到 infosec.com.cn 三级域名所对应的权威域名服务器后，再次向对应的权威域名服务器发送一条请求解析 infosec.com.cn 域名的 DNS 请求报文（A4）。

7. infosec.com.cn 权威域名服务器在收到 DNS 请求报文后，在 DNS 区域数据库中查找，最终得出 infosec.com.cn 域名所对应的 IP 地址。然后向本地服务器返回一条 DNS 应答报文（B3）。

8. 本地服务器收到权威服务器返回的 IP 地址后进行缓存，并向 DNS 客户端返回一条 DNS 应答报文（B4），告诉客户端 infosec.com.cn 域名的 IP 地址，访问应用服务器（C），应用服务器响应请求（D）。

2.5.2 SDNS 解析原理



1. 客户端发送 DNS 解析请求到本地 DNS 服务器以解析域名

2. 经过一系列查询，本地 DNS 服务器得知 APV GSLB 为该域名的授权 DNS 服务器，然后将 DNS 解析请求转发给 SDNS 处理。

3. SDNS 做出智能解析，挑选健康可用的服务 IP 返回给本地 DNS 服务器。

4. 本地 DNS 服务器将解析结果返回给客户端。

SDNS 智能解析的流程如下：

1. SDNS 根据 DNS 解析请求的域名找到命中的 SDNS 策略。

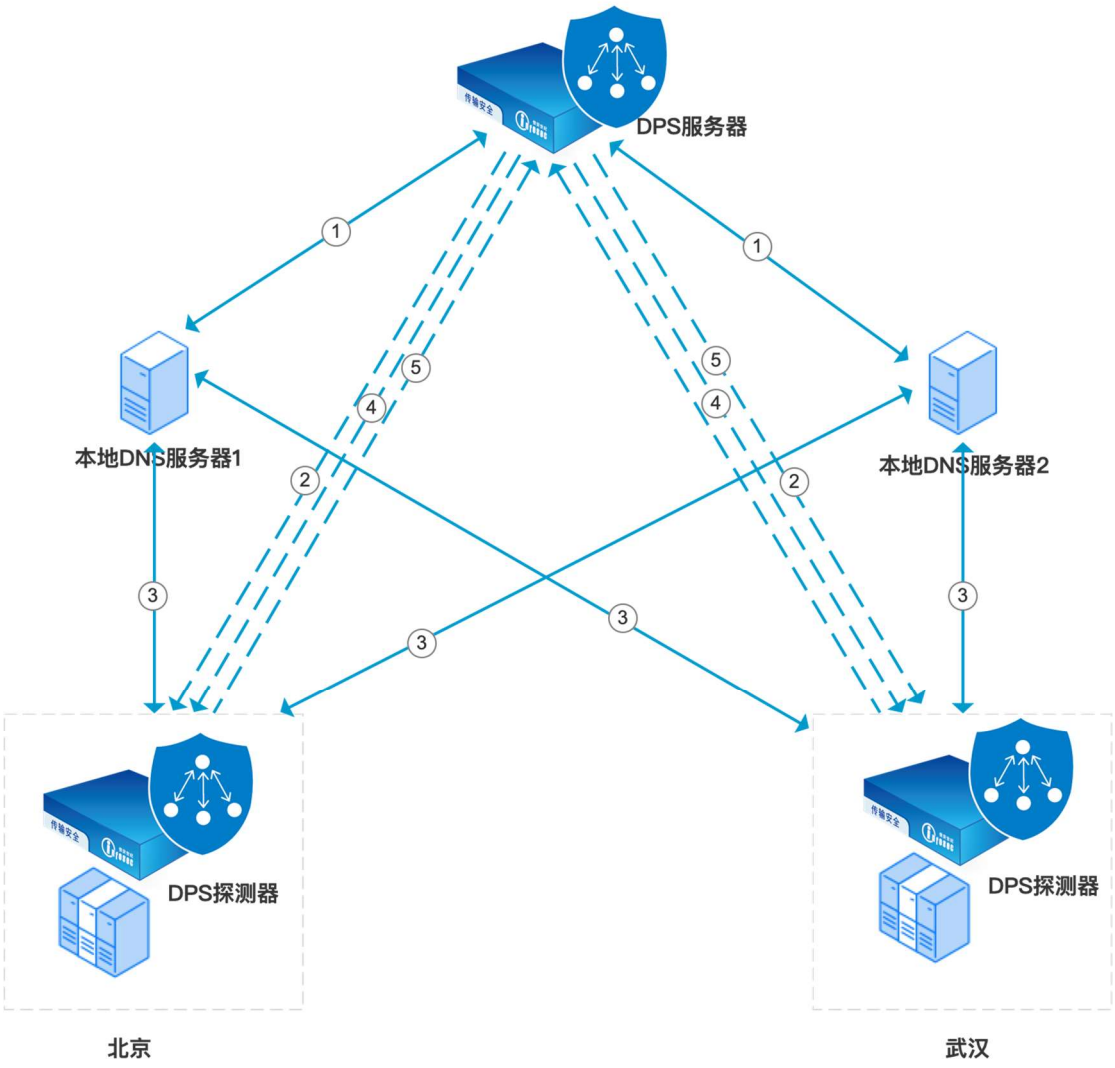
2. SDNS 根据命中的策略找到命中的服务池。

3. SDNS 根据命中服务池的算法和健康状态确定命中的服务 IP。

4. SDNS 将命中的 SDNS 服务 IP 返回给本地 DNS 服务器。

2.5.3 DPS 就近性原理

DPS 为 APV GSLB 提供链路探测功能，通过 DPS 线路探测功能为 SDNS 提供最优线路选择。



5. DPS 服务器收集本地 DNS 的 IP 地址

6. DPS 服务器将本地 DNS 列表通告给个站点 DPS 探测器

7. DPS 探测器探测与每个本地 DNS 的距离信息

8. DPS 服务器从 DPS 探测器查询本地 DNS 距离信息

9. DPS 探测器将本地 DNS 距离信息通告给 DPS 服务器

3 产品特性

3.1 丰富的 DNS 功能

- 超高 DNS 查询响应性能（RPS），通过自研技术架构、多核处理等方式，显著提高权威 DNS 性能。
- 全域名解析，支持 A、AAAA、PTR、MX、NS 和 CNAME 等类型的 DNS 解析请求。
- 丰富的解析策略，支持以解析请求所属区域确定 SDNS 服务池的区域策略和无法获取所属区域确定 SDNS 服务的默认策略。
- 支持服务池功能，通过多种服务池算法、自动失效切换、自动抢占、手动切换等功能实现服务池的高效与可用性。
- 丰富的健康检查，支持 ICMP、TCP、UDP、HTTP 和 HTTPS 等健康检查。并具备优化调度机制，通过 DNS 将域名解析为 IP 地址，并探测应用服务的健康状态，将访问调度至最佳的应用服务器。
- 支持动态与静态 DNS ACL 规则，通过包过滤可有效限制和拒绝基于源、目的地址和端口的访问；通过限制查询请求个数，可将超过出的请求直接丢弃。
- 支持 DNS 缓存功能，可立即响应客户端请求，减少 DNS 响应延迟；
- 支持 DNSSEC 安全扩展，具备签名/验签、密钥管理等功能
- 支持 DNS over HTTPS 功能，通过 HTTPS 协议实现域名解析通信安全，而不影响 DNS 每秒响应。
- 支持 DNS over TLS 功能，通过 TCPS 协议实现域名解析通信安全，而不影

响 DNS 每秒响应。

- 从优化的系统架构、精细的管理权限以及严密的攻击防范达到全方位可靠的安全策略，最大限度保障 DNS 系统安全稳定运行。可有效预防 DNS DDOS、LDNS 缓存中毒以及 DNS 反射放大攻击等其他的 DNS 攻击。
- 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。
- 支持云部署，可在阿里云、华为云、腾讯云等常见公有云上软件部署

3.2 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 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。

- **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。

3.3 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 DDoS、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。

3.4 可维护性

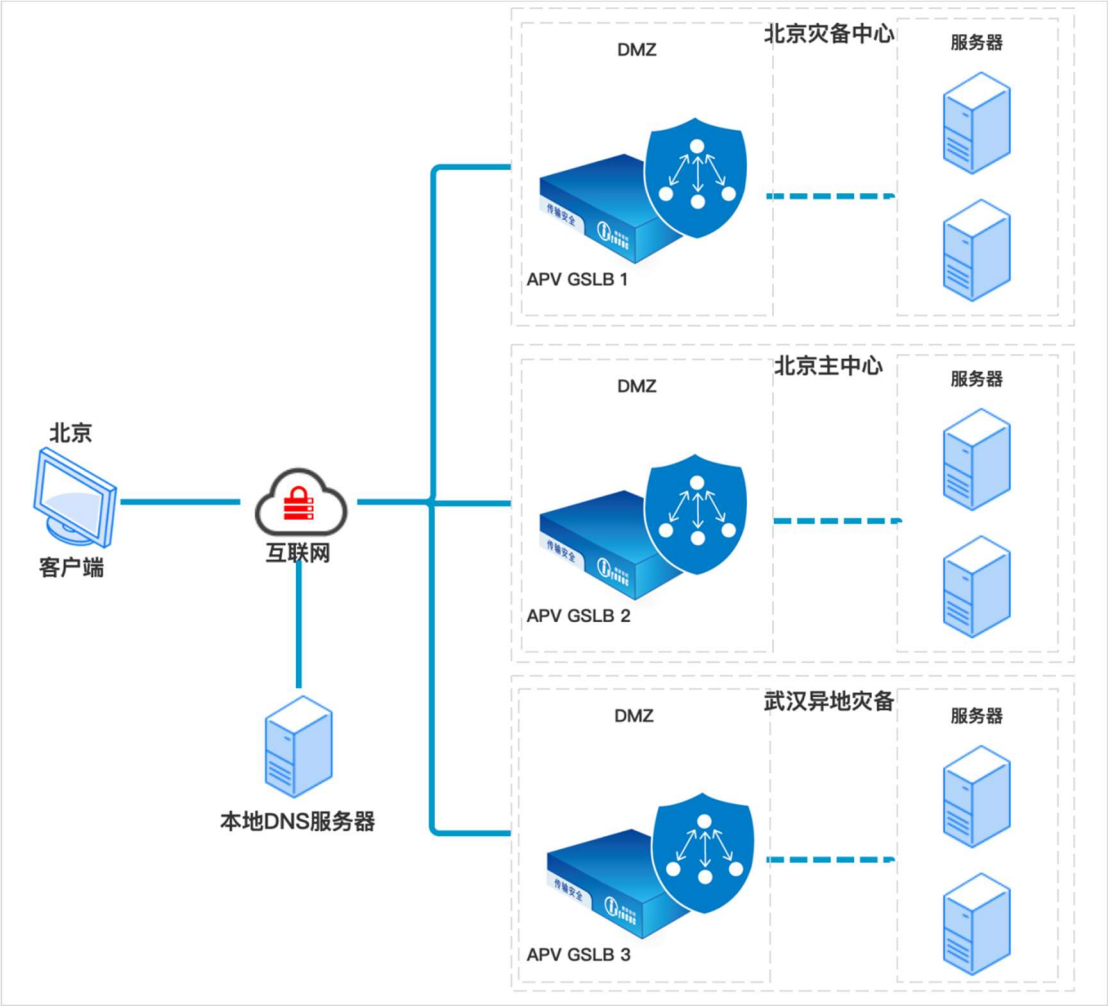
- APV 支持多种语言管理界面，提供快速配置功能，可通过 Web 图形管理界面或简单易用的命令行界面，进行直观的配置和管理，实时监控图表，为排查问题、决策分析等提供参考依据；

- 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；
- 支持按需授权，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；

4 典型场景

4.1 多数据中心场景（GSLB）

广域网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。



4.1.1 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最近的 APV 设备发送对应的域名解析结果。

✓ 安全可靠的后台服务

APV 设备同步采用 ICMP、TCP、HTTP、HTTPS 等丰富的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。

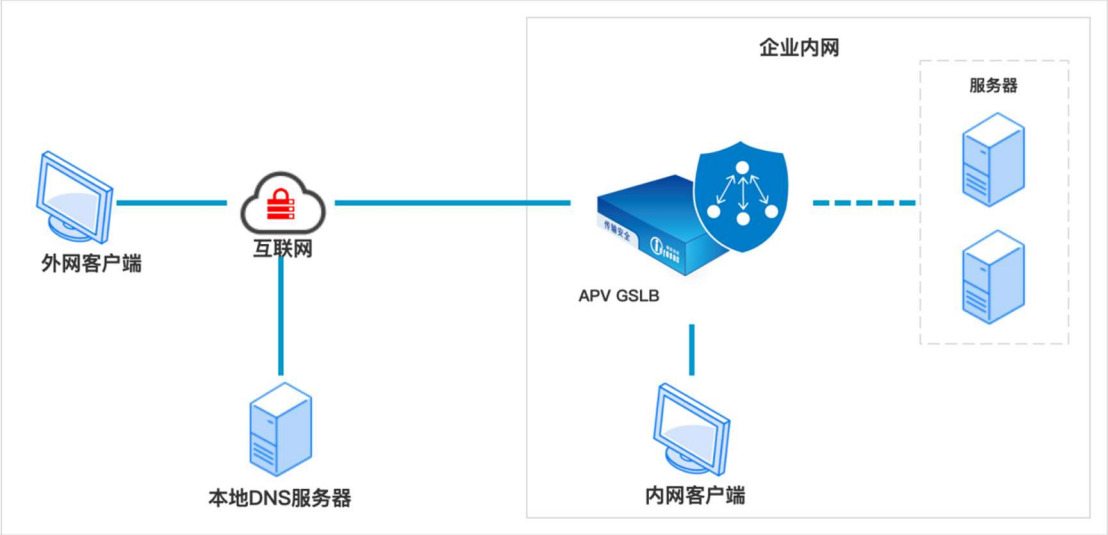
✓ 数据安全同步

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。

4.2 内外网 DNS 融合场景

该场景主要应用于中小型企业内外网域名解析需求。APV GSLB 设备既可做权威域名解析服务器为外网用户提供解析服务，又可做本地域名解析服务器为内

网用户提供解析服务，并且提供客户端与 APV GSLB 通信使用加密协议实现传输加密，确保 DNS 解析数据机密性与完整性。



4.2.1 方案优势

✓ 多功能 APV 设备

单台 APV GSLB 设备可为内网用户既可做权威域名解析服务器为外网用户提供解析服务，又可做本地域名解析服务器为内网用户提供解析服务，并且实现无改造应用。

✓ 安全可靠的后台服务

APV 设备采用 ICMP、TCP、HTTP、HTTPS 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。

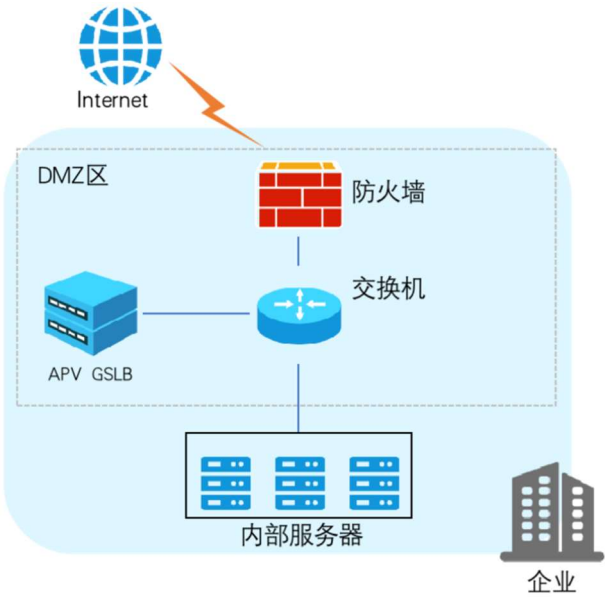
✓ 解析数据安全传输

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。

5 部署方式

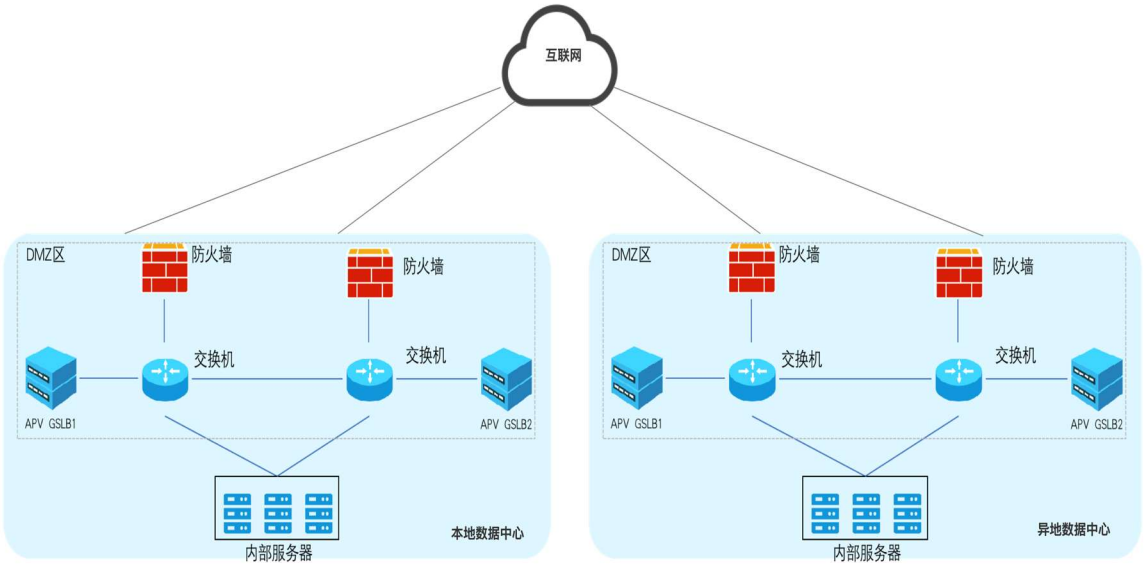
5.1 单机部署方式



单机方式特点介绍：

- 单机部署可节省采购成本，但存在单点故障隐患，无需改造网络架构，主要适用于中小型企业。

5.2 多数据中心部署方式



多数据中心特点介绍：

- 多数据中心部署方式，可预防单点故障，采用防火墙和核心交换机冗余保证 DNS 系统的进一步可靠性，主要适用于两地三中心。

6 产品资质

- 公安部销售许可
- 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
- ……