|  |  |  |
| --- | --- | --- |
| 项目名称 | **内、外网DNS安全系统** | |
| 1. **功能要求** | | |
| 1、用户与访问管理 | | 1、平台支持三权管理，且登录认证及密码管理需满足等保三级要求；  2、权限细颗粒化管理、可根据不同用户（组）、角色分配不同的管理权限；  3、支持双因子认证功能，除用户名密码认证外，其他认证不限于短信验证码、微信（限外网）、Ukey等技术；  4、支持访问控制，平台能支持黑、白名单登录； |
| 2、DNS权威功能 | | 1、支持权威智能解析，可根据不同区域的来源IP地址进行智能DNS解析，得到不同的查询解析结果；  2、支持A、AAAA、NS、MX、CNAME、NAPTR、SRV、PTR、TXT、DNAME、SPF、CAA等多种类型记录的解析；  3、支持根据出口运营商、业务不同建立不同区域（正向、反向）管理；  4、支持对多地址的轮询和排序解析；  5、内网DNS能建立院内权威域名解析。摆脱对host文件的依赖，优化运维方式；  6、外网DNS能建立院内权威，优化服务器访问管理。 |
| 3、DNS递归功能 | | 1、支持递归智能解析，可根据不同ISP线路，终端可以对同一域名解析出不同的IP结果；  2、支持对不存在（或者恶意域名）域名解析结果的重定向；  3、可以基于域名进行DNS解析调度；  4、内网DNS能递归解析医保等关键业务相关的域名；  5、外网DNS能递归解析国内、国外的业务相关的域名； |
| 4、DNS安全管理 | | 1、支持对单IP（域名）、多IP（域名）进行限速；  2、能防范NDS隧道攻击，防止数据泄露；  3、能防范DDos攻击、放大攻击、禁止DNS ANY类型请求；  4、能防止对平台进行DNS缓存窥探攻击，及能对DNS缓存进行安全管理；  5、能防范DNS反射攻击；  6、能识别DNS递归攻击，对攻击行为给予禁封和限速；  7、有系统防火墙功能，支持UDP、TCP五元组常规防火墙过滤设置；  8、平台自带（或嵌套第三方）域名情报库，并能自动更新情报库，能自动识别判定恶意的域名，并能自动拦截解析；  9、支持自定义的域名库（黑、白名单）管理；  10、平台支持自助申请审核域名的功能。支持域名的使用跟随项目实施的全生命周期管理；  11、平台支持网卡数据捕获，方便网络故障排查； |
| 5、报表与日志管理 | | 1、支持对平台所有操作能有日志记录可审计，转发、180天容量查询；  2、支持对系统日志管理记录可审计、转发、180天容量查询；  3、支持解析日志查询分析，能查询时间、客户端源IP、查询目的域名、查询类型及解析状态等内容。并支持日志备份、转发、180天容量查询；  4、支持域名排行，IP排行、解析状态、解析类型、QPS、解析成功率、缓存命中率、并发递归数、设备网卡流量信息等统计查询；   1. 能对DNS域名解析自动（手动）生成详细报告； |
| **二、部署和管理**  1、内、外网平台要求双机部署，实现高可用。可负载均衡部署、集群部署、云化等部署方式  2、★能监测平台自身（CPU、内存、磁盘等）运行状态，遇到平台故障能告警提示，同时不影响客户端的上网使用；  3、平台能联动医院现有时钟同步服务器，使平台及管控的终端按一定频率同步时间。  4、平台自身需满足等保三级相关要求；  5、平台支持WEB中文管理界面（HTTP/HTTPS），界面友好、操作简易；  6、支持手动和自动备份平台配置，可支持FTP和TFTP自动备份；  7、提供开发接口与其他产品相结合联动，并配合院方作相应定制开发，例如防火墙的策略下发、人事系统账号统一管理接口、国密改造、态势感知系统相联动等等。 | | |
| 1. **资质及服务**   1. ★提供三年原厂保修及相关技术服务。  2. 中国国家信息安全产品认证证书。  3. 提供原厂DNS系统的部署安装调试以及对本院管理人员、使用人员的使用培训。  4. 必须具有所投产品的原厂商针对本项目的授权函原件和公司的售后服务承诺函原件。  5. ISO9001质量管理体系证书。  6. 产品厂家必须具备该产品的《计算机软件著作权登记证书》。 | | |