**南昌市中心血站****网络安全防护升级采购项目**

**技术标准和要求**

因我站现有的防火墙和上网行为管理等设备由于使用年限较长，目前已无法对特征库和固件进行更新，难以满足现有的网络安全管理需求，特采购相关设备和服务进行升级改造。具体技术标准和要求如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品类型** | **产品规格** | **数量** |
| 1 | 防火墙 | 1. 机架式独立硬件设备，系统硬件为全内置封闭式结构，多核架构设计MIPS架构**（需提供CPU型号、频率）**，功能采用模块化结构设计，加电即可运行，启动过程无须人工干预；
2. 最大功率≥25W；内置硬件、软件Bypass机制，在设备流量异常、突增、异常断电、重启等情况时，可自动切换到Bypass状态，当设备恢复时，可自动切换回工作状态；
3. 标配接口千兆SFP光接口数量≥4个；10M/100M/1000M自适应电接口数量≥14个；
4. 接口无路由/交换/LAN/WAN等固化区分，均可作为二三层接口使用；
5. 网络吞吐量不小于9Gbps，IPS、AV、上网行为、WAF等功能开开时应用过滤吞吐不小于500Mbps；
6. 支持接口虚拟化功能，使用VRF功能可以从系统层面隔离不同VRF组里的流量信息和路由信息，使用VRF功能可以作为MPLS组网里的MCE设备。不同VRF下的接口可以配置相同的IP地址；**（提供原厂盖章截图证明）**
7. 支持邮箱内容、IM内容、网页访问、外发文件、终端进程列表、USB读写拷贝审计，审计解决数据核心资产泄露问题**（提供原厂盖章截图证明）**；
8. 支持应用模型识别技术，可定义识别模式的宽松程度，有效和准确识别网络应用；检测引擎支持智能、快速和关闭识别模式**（提供原厂盖章截图证明）**；
9. 支持路由模式、透明（网桥）模式、混合模式、旁路模式；旁路部署支持加入多个物理接口；部署模式切换无需重启设备；
10. 支持7元组的链路负载均衡策略，负载均衡接口支持接口和接口组，支持基于域名进行链路负载，负载算法包括但不少于优先级和权重，负载均衡接口支持pppoe、dhcp、tunnel、物理接口等三层接口；
11. 支持IPv6/v4双栈，支持IPv6安全策略；支持IPv6静态路由，IPv6隧道，包括IPv6手工隧道、isatap、6to4等隧道模式；
12. 支持自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；
13. 支持在设备旁路部署时针对违规上网行为进行阻断过滤**（提供原厂盖章截图证明）**
14. 支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断；
15. 支持IPSec VPN、SSL VPN、Gre VPN，支持手机、平板电脑等移动终端VPN接入。
 | 2 |
| 2 | 日志审计 | 1. 1U标准机架式设备，硬盘：≥4TB HDD，网口：6\*千兆电口，单电源，自带50个日志源的审计；
2. 提供统计分析功能，包括但不限于日志统计、审计统计、告警统计，能够对审计事件风险等级分布、审计事件风险趋势、审计事件类型占比、审计事件日志源占比等提供详细的图形化统计；
3. 提供日志查阅功能，支持日志合并查阅，可按照一定组合条件将日志进行合并查询，能够查阅事件分类、事件子分类、日志源、主机名、源IP、目的IP等详情；
4. 支持审计策略配置，可根据审计对象配置审计策略，默认审计策略全部启用，包括但不限于数据库审计、登录审计、操作系统审计、账户审计等规则分类；
5. 提供告警发送记录，能记录每一个告警信息的发送过程，内容包括告警方式、告警时间、告警内容、告警结果、操作等；
6. 提供通用网络配置，可提供不低于3种DNS服务配置，可同时配置IPv4和IPv6地址，并且能够检测出当前DNS服务的联通性是否正常，保证DNS服务的有效性；
7. 提供系统重启、系统关机、系统复位管理，可提供不低于2种系统复位方式，在复位过程中要求使用登录密码安全保护，避免产生误操作；
8. 支持用户双因子认证，保障用户的安全性**（提供原厂盖章截图证明）**；
9. 支持产品自身防护功能，防止产品被恶意扫描，并锁定恶意IP，阻断恶意IP访问**（提供原厂盖章截图证明）**；
10. 提供配置备份和恢复，可提供配置文件本地备份，可详细记录当前备份配置文件的时间、版本、文件大小，可选择对已备份的配置文件进行下载和还原，并且支持对配置文件进行导入操作，在导入过程中要求使用文件密码安全保护，避免产生误操作**（提供原厂盖章截图证明）**；
11. 提供存储管理，可提供新加入磁盘发现，支持识别磁盘类型、序列号、厂家、磁盘状态、磁盘大小，并能够将磁盘加入到当前数据存储中，同时具备数据存储切换能力，将日志数据切换至大容量存储，对数据存储进行动态扩容**（提供原厂盖章截图证明）**。
 | 1 |
| 3 | 威胁发现工具 | 1. 服务工具需具备资产梳理功能**（提供原厂盖章截图证明）**；
2. 可主动识别内网资产清单并对访问关系进行梳理，并生成业务流拓扑**（提供原厂盖章截图证明）**；
3. 工具可在4个VLAN中释放至少128个蜜罐**（提供原厂盖章截图证明）**；
4. 蜜罐类型支持只创建IP与端口的四层蜜罐，也支持可高交互式蜜罐；
5. 对现有网络拓扑进行深度评估，找出潜在的单点故障、带宽瓶颈等问题。根据评估结果，调整网络架构，合理划分 VLAN，优化网络流量走向，提升网络的可靠性与可用性。
6. 完成大楼整体无线网络改造，预计材料包含：一套万兆接口无线控制器；49只放装式无线AP（WIFI6，2+2双频）；4只面板式无线AP（WIFI6，2+2双频）；3台24口POE交换机；标准42U网络机柜一台；网线、光纤等辅材若干，并包含施工。
 | 1 |
| 4 | 专用翻墙行为监测产品 | 1、2U机架式设备，配置≥1个console口， ≥2个USB接口， ≥8个千兆电口，≥2个千兆光口， ≥2个万兆光口， 支持≥1对电口Bypass，冗余电源，≥2个扩展槽位,应用层监测带宽：≥600M， 整机网络吞吐量：≥3G；2、支持路由模式，旁路模式、网桥模式、混合模式部署，对可疑翻墙终端实时阻断网络连接；3、支持http代理、https透明代理、全透明代理、二级代理、DNS代理、dns缓存；4、对于多IP 的DNS解析，支持根据用户的来路而做出智能化的处理，然后把智能化判断后的 IP 返回给用户，而不需要用户进行选择，以此精准发现并阻断内网中对违规域名的访问；5、支持IPv4和IPv6在一个系统版本内，同时支持V4和V6网络；支持接口配置ipv6地址、支持ipv6地址簿、支持ipv6策略路由、NAT64、NAT66等相关配置；6、支持通过识别翻墙软件流量特征，对翻墙软件进行审计和管控，从而实现审计和管控上网用户的翻墙行为，内置翻墙软件特征支持30种以上；7、支持通过资产扫描，对网络中的所有资产进行识别和分类，对可疑的翻墙终端快速定位；8、支持通过 ID 磁卡识别用户身份，并可对用户进行流量控制、访问控制、行为审计等**（提供能够证明上述功能的具备 CNAS 或 CMA 标识的检测报告扫描件，并加制造商公章佐证，并保留中标后测试功能的权利）**9、支持对 TCP、UDP、ICMP、TCP SYN 超时时间，无回应 UDP 超时时间设置并能支持按照新建会话与总会话比例设置老化开始或者结束**（提供能够证明上述功能的具备 CNAS 或 CMA 标识的检测报告扫描件，并加制造商公章佐证，并保留中标后测试功能的权利）** | 1 |
| 5 | 网络安全管理及制度咨询服务 | 结合《江西省卫生健康系统落实党委(党组)网络安全工作责任制评价内容和标准(试行)》的相关要求，梳理单位现有的网络安全管理制度，形成一套符合单位实际情况且满足合规性要求的制度体系材料。 | 1 |
| 6 | 翻墙行为应急处置 | 基于专用加密流量监测产品和检测分析工具（至少提供200套，每套工具软件独立封闭）提供人员配合针对异常跨境访问行为进行响应支持，及时发现、定位并配合进行处置服务，同时就异常跨境访问行为配合用户制定相应管理制度。 | 1 |
| 7 | 售后服务 | 1.服务期限：提供自验收合格之日起3年免费软硬件升级及售后服务。2. 现场服务承诺：每月至少一次预防性巡检维护（包含设备清洁、日志分析、配置优化等）；中标后建立本地备件库，储备不低于设备总值10%的常用备件；故障响应：7×24小时技术支持，2小时内工程师抵达现场（主城区）；重大问题提供"先替换后维修"服务，故障设备48小时内修复。3.多厂商协作机制设立统一技术接口人，由中标方指定项目经理全权对接信息科；当故障涉及多系统时，需主动配合其他厂商进行联合诊断（提供系统日志、接口参数等）；禁止以"其他厂商责任"为由拒绝初步处置，需共同完成初步故障隔离；每季度参与由信息科组织的多厂商运维协调会。4.服务质量保障每次维护需提供带水印照片的电子版维护报告（含设备状态、配置变更记录、隐患分析）；每年开展两次网络安全应急演练，模拟多厂商协同处置场景；建立知识转移机制，每年为信息科提供不少于16课时的专业培训。5.责任界定条款设备维保范围延伸至上下游关联系统接口；因系统升级导致其他厂商设备异常的，须在8小时内提供兼容性解决方案；争议性故障由第三方检测机构判定责任，责任方承担全部检测费用及违约金。6.违约条款每出现一次推诿情况，扣除合同金额1%作为违约金响应超时每分钟罚款200元，单次故障最高罚金不超过合同总额5%；累计三次服务不达标，采购方有权单方面终止合同并追索赔偿。7.服务延续机制服务期满前三个月提供设备健康状态评估报告；移交完整知识库（含拓扑图、密码矩阵、应急预案等）。 | 1 |