**采购技术参数及清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 技术条款 | 单位 | 数量 | 单价（元） | 总价（元） |
| 1 | 测评服务 | ★等级保护二级测评及配套文档整理服务，负责全流程完成等保测评的相关工作。提供评测资格证明并加盖公章。 | 项 | 1 | 50，000.00 | 50，000.00 |
| 2 | UPS | 1、额定容量：6KVA，在线式双变换拓朴结构。  2、市电异常状况可以直接用电池启动UPS，满足应急需求。  3、过载能力：100%~110% 10分钟到旁路； 110%~130% 1分钟到旁路；130~150% 30 秒到旁路；>150% 1 秒到旁路  4、UPS必须包含ECO节能模式。  5、UPS主机的输入：  输入电压范围：110-300VAC；  输入频率范围：普通模式：50/60±4Hz；发电机模式：40-70Hz  输入功率因数：≥0.99；  输入谐波失真度：THDi≤4%输入保护：应配置63A以上的空开  6、UPS主机的输出：  输出功率因数：高达1  输出电压：220Vac  效率：94%  输出电压调节：±1%  输出电压失真度：<1% 线性负载，<4% 非线性负载  7、UPS需标配RS232和USB通讯接口，并随机配置RS232和USB线缆，可选配干接点，SNMP，Modbus通讯卡。  8、UPS每组蓄电池数量应可调，应支持每组16-20节电池，且应为连续可调。  ★9、蓄电池保护开关应采用直流断路器，不得采用交流或者交直流断路器。为便于后期维护，保证监控协议与电源主机一致，要求直流断路器与电源主机为同一品牌，提供直流断路器官方网站截图及官网链接并加盖制造商公章或投标专用章。  10、UPS应配置紧急关机接口（EPO）。  11、UPS需标配监控管理软件，应采用C/S架构，提供UPS实时状态监控、事件管理及通知、计划停机和重启、电池管理、UPS监控等软件功能。  12、应标配UPS集中管理软件，可至少集中管理1000台同系列UPS。  13、UPS需标配安全关机软件，可以在市电断电电池耗尽之前，将服务器的重要数据进行保存并安全关机，以避免发生意外断电事故时造成的数据丢失和系统崩溃。  14、可选配温湿度环境监控卡  15、UPS须喷涂三防漆，适应多种严苛使用环境  16、UPS须配置LCD显示屏，丰富的显示和配置内容，便于用户操作维护。  ★17、提供2年电源原厂上门换机服务，不接受送修，上门维修方式。提供原厂售后服务承诺函。  ★18、提供电源合法来源渠道证明。  19、配置12V65AH蓄电池16块后备时间两小时，含配套电池柜。 | 套 | 1 | 33,000.00 | 33,000.00 |
| 3 | 交换机 | 1.交换容量≥1.28Tbps，包转发率≥108Mpps；  2.支持千兆电口≥24个，万兆光口≥4个;  3.为了提高设备可靠性，支持可插拔的双电源；  4.支持4K个VLAN，支持Guest VLAN、Voice VLAN，支持基于MAC/协议/IP子网/策略/端口的VLAN；  5.支持1:1和N:1 VLAN交换功能；  6.支持静态路由、RIP V1/2、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6；  7.支持统一用户管理功能，支持802.1X/MAC/Portal等多种认证方式，支持对用户进行分组/分域/分时的管理，用户、业务可视可控；  8.支持VxLAN功能，支持VxLAN二层网关、三层网关，支持BGP EVPN，实现自动建立隧道；  9.支持WRR、DRR、SP、WRR＋SP、DRR+SP队列调度算法；  10.支持报文的802.1p和DSCP优先级重新标记；  11.支持SNMPv1/v2c/v3，支持RMON；  12.支持网管系统、支持WEB网管特性，支持NetStream；  13.可实现基于Python语言的开放可编程特性，提供开放的编辑语言和更简单的操作方法，实现智能化运维；  14.支持DHCP Snooping，IP Source Guard，SAVI等安全特性；  15.支持防ARP攻击、DOS攻击、ICMP防攻击、CPU防攻击；  16.支持G.8032标准环网协议；  17. 支持Telemetry技术，配合网络分析组件通过智能故障识别算法对网络数据进行分析，精准展现网络实时状态，并能及时有效地定界故障以及定位故障发生原因，发现影响用户体验的网络问题，精准保障用户体验； | 台 | 1 | 23,000.00 | 23,000.00 |
| 4 | 日志审计 | 1、★要求包含主机审计数量≥50，最大可扩展审计主机许可数≥150，可用存储量≥2TB，平均每秒处理日志数≥1200。2U设备，内存≥16G，至少提供6个千兆电口，2个万兆光口；包含日志分析系统软件一套，提供三年硬件质保及软件升级服务，提供产品功能截图并加盖厂商公章。  2、★支持TLS加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量，提供产品功能截图并加盖厂商公章。  3、支持审计对象的定义，包括：审计目标对象、审计行为对象、审计行为执行者对象、审计行为来源对象、审计时间段对象等；  4、支持定义部门和人员的对应关系；支持定义人员与账号的对应关系；  5、可通过自定义聚合规则修改日志的聚合归并逻辑规则，提高日志分析效率，支持归并技术，一段时间内对重复日志进行归并；  6、支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集；  7、支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等，提供产品功能截图并加盖厂商公章。  8、支持DNS、DGA、解码错误、解码失败、解码超时的网络会话分类展现；  9、支持简单易用的日志查询普通模式，根据系统预置的查询条件，根据用户需求查询对应的日志，并且支持查询条件的保存，供后续快捷使用  10、支持个性化定制，支持全系统更换logo与系统名称，支持一键恢复默认。  11、支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射，提供产品功能截图并加盖厂商公章。  12、支持日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量，提供产品功能截图并加盖厂商公章。 | 台 | 1 | 38,000.00 | 38,000.00 |
| 5 | 终端安全管理系统 | 1、★端点安全设备包含管理控制平台及终端客户端软件，控制平台可以纯软件形式交付，无需另行提供设备安装部署。客户端直接部署在个人用户主机或是单位服务器中，服务器支持Windows和Linux多种操作系统，本次项目提供30个Windows PC授权，1个Windows或Linux操作系统服务器主机授权；  2、★支持与同厂商的网络防火墙进行安全联动，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息，在网络防火墙管理界面下发一键隔离指令，对终端恶意文件进行隔离，防止病毒进一步扩散，提供产品功能截图并加盖厂商公章。  3、支持客户端的错峰升级或灰度升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴，提供产品功能截图并加盖厂商公章。  4、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑root权限账号、长期未使用账号、半夜登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户，提供产品功能截图并加盖厂商公章。  5、一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果；  6、支持对勒索病毒的家族名、病毒名、加密文件后缀名的链接查询，或者通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具  7、支持插入U盘时主动扫描U盘文件，可直观展示U盘窗口信息展示：剩余空间、总空间，针对U盘窗口操作包括打开、弹出、查杀；  8、支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等，提供产品功能截图并加盖厂商公章。  9、支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、僵尸网络、WebShell后门数量、高危漏洞及其各自影响的终端数量；  10、支持终端客户端软件的启用禁用，重启，支持在管理平台直接卸载客户端软件；  11、流量线详情支持展示该流量线对应的控制策略；图形化显示服务器间流量关系，包括访问详情、流量趋势等，提供产品功能截图并加盖厂商公章。 | 套 | 1 | 36,000.00 | 36,000.00 |
| 6 | 入侵防御 | 1、★网络层吞吐量≥6Gbps，并发连接数≥1800000，新建连接数≥60000，接口不少于6千兆电口+4万兆光口，提供产品功能截图并加盖厂商公章。  2、支持路由模式、透明网桥部署、旁路部署、单臂部署以及混合部署等多种方式。  3、支持静态路由协议，OSPF动态路由协议，路由异常告警功能；支持DHCP中继。  4、★支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能，提供产品功能截图并加盖厂商公章。  5、支持连接会话展示，可针对具体的IP地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体IP的会话记录。  6、★支持同访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间，提供产品功能截图并加盖厂商公章。  7、访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式。  8、访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试，提供产品功能截图并加盖厂商公章。  9、支持P2P、IM、游戏、炒股软件、网银，流媒体，常用邮件以及远程控制软件等的识别和控制，支持识别管控的应用类型超过1200种，应用识别规则总数超过3000条。  10、支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户、子接口和VLAN等因素实现对象的流量控制，提供产品功能截图并加盖厂商公章。  11、内置海量URL分类库，包含非法及不良网站、成人内容、网上购物、微博论坛等分类，实现全面高效的不良网站过滤。  12、支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等DoS/DDoS攻击防护；支持IP地址扫描和端口扫描防护。  13、支持在同一个界面对全网所有服务器的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护。  14、支持产品安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况，提供产品功能截图并加盖厂商公章。  15、支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式，减少配置工作，提高部署效率。  16、支持设备软硬件异常状态监控，可以监控设备CPU、内存、硬盘使用率，并且可监控系统状态、网络接口状态、安全能力监控状态，帮助用户实时了解安全设备运行状况。 | 台 | 1 | 115,000.00 | 115,000.00 |
| 7 | 合计金额 |  | | | | 295,000.00 |

**标注星号（★）条款为必须满足项，不符合任何一项条款，投标无效。**