产品线		产品型号
日志审计	日志审计系统	SIP-Logger-A600
全网AC	全网行为管理系统	AC-1000-SK2100-GY

产品说明	数量
1、性能要求：包含主机审计许可证书数量≥50，可用存储量≥2TB（RAID1 模式），平均每秒处理日志数（eps）最大性能≥2500。 2、硬件要求：2U，内存≥16G，硬盘容量≥128G minisata+2T SATA*2，单电源，接口≥6千兆电口+2万兆光口SFP+。 3、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于800种日志对象的日志数据采集。 4、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、SFTP、文件\文件夹读取、Kafka等多种方式完成日志收集。 5、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，以满足除内置解析规则之外未被覆盖的日志类型的解析。（需提供截图并加盖投标人公章） 6、支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件。 7、支持POC测试工具一键生成数据,验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险。（需提供截图并加盖投标人公章） 8、支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN账号异常场景分析、Windows服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析。 9、支持等保合规检测，用户可自查设备是否满足等保要求。（需提供截图并加盖投标	1
1、性能要求：网络层吞吐量≥10Gb，带宽性能≥1Gb，支持用户数≥1500。 2、硬件要求：1U设备，内存≥8GB，硬盘容量≥ 128GB MSATA+480G SSD，接口≥6千兆电口+2千兆光口SFP。 3、为保证运维老师可以实时查看学校终端的上网情况，产品需支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行。（需提供截图并加盖投标人公章） 4、为便于运维老师实时查看学校的web访问质量，保障校内师生能进行流畅的web访问，产品需支持针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级。 5、产品需支持图形化查看当前内网IP使用情况，帮助运维老师减少人工维护IP表的工作量。 6、为避免校内师生访问不良网站、不良应用，产品需内置应用识别规则库，支持超过9000种以上应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制。 7、为避免P2P应用大量占用学校带宽，产品需支持通过抑制P2P的下行丢包，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。（需提供截图并加盖投标人公章） 8、为提高学校带宽使用率，产品需具备流量管控功能，支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略。 9、为能够快速定位用户认证故障问题，产品需支持针对用户认证的故障进行分析，给	1
合计	

单位	审核含税单价（元）	审核含税总价（元）
台	45000	45000
台	70000	70000
		115000