一、网络日志审计系统：

（一）硬件规格：

#1.机架式设备，≥8 核国产 CPU，国产操作系统，内存≥64GB，硬盘≥24TB，网卡≥4 个千兆口，≥2 个万兆光口（含相应的模块），冗余电源。

（二）基础要求

1.独立完成审计日志采集，不依赖于设备或系统自身的日志系统；

2.审计工作不影响被审计对象的性能、稳定性或日常管理流程；

#3.支持审计≥300 个数据源，平均每秒日志解析能力 EPS≥15000EPS。

4.审计结果存储于独立存储空间；

5.自身用户管理与设备或主机的管理、使用、权限无关联；

6.提供全中文 WEB 管理界面，无需安装任意客户端软件或插件。

（三）日志采集

#1.支持业内通用标准数据获取方式，包括但不限于 Syslog(UDP、TCP）、目录、远端软件（FTP、SFTP、HDFS、LOCAL）、SNMP（Trap）、数据库（ORACLE、DB2、MYSQL、SQLSERVER）协议日志收集；

2.支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等。

（四）日志分析

1.支持对设备日志查询和聚合分析；

2.系统内置常见安全事件关联分析规则，包括但不限于：统计关联分析；时序关联分析；事件关联分析；互斥关联分析、反向关联分析；

3.支持关联分析过程中随时调用静态对象来快速完成分析模型的构建，避免频繁修改模型内容；

（五）日志检索

1.日志、告警信息查询可根据安全场景自动推荐检索字段，包括但不限于 IP 地址、时间段、服务端口、cmd 进程、可疑进程等。

2.支持根据安全场景自动优化展示安全字段。

（六）用户管理

1.职、权分离，对系统本身进行分角色定义；

2.基于角色的权限管理机制，通过角色定义支持多用户访问；

3.系统自身的健康状况监控，至少包括 CPU、内存、磁盘的利用率；

4.系统自带自身管理日志；

5.支持通过前端页面对产品升级；

（七）质量要求

★提供单独的承诺函，内容如下：

1、我公司承诺，若我公司中标，承诺合同签订前提供原厂售后服务承诺函。

2、我公司承诺，若我公司中标，承诺合同签订前提供 5 年原厂软件升级和硬件维保服务的承诺函。

二、入侵防御系统

（一）基本要求

1、标准机架式设备，配备交流冗余电源，配备液晶屏，设备接口千兆口≥6 个，万兆 SFP+光口≥2 个，满配万兆多模光模块，USB 接口≥2 个，拓展槽位≥5 个，存储≥4T 硬盘；

#2、具有完全自主知识产权的专用安全操作系统。

（二）性能要求

#1、网络层吞吐量≥60G，应用层吞吐量≥20G，最大并发连接数≥1500 万，每秒新增新建最大连接数≥60 万，时延≤40 μs；

#2、入侵攻击特征库数≥1 万，病毒特征库数量≥1200 万，WEB 特征库≥6000，
3、具备国家信息安全测评信息技术产品不低于 EAL4+安全测评证书；
（三）部署模式
1、实现路由模式、透明（网桥）模式、混合模式部署。同时支持串接部署的防御模式以及旁路部署的检测模式。
2、支持 bypass 模式保障设备掉电网络直通。
3、支持 IPV6 动态路由协议、IPV6 对象及策略、IPV6 攻击防范、IPV6 日志审计、IPV6 会话热备等功能。
（四）入侵防御功能
1、入侵规则分类，便捷的制定防护策略。包括但不限于勒索、挖矿、SQL 注入、XSS 注入、webshell、命令代码执行、内存破坏、类型混淆、扫描类攻击等。
2、提供 DoS/DDoS 攻击防护能力，支持 PING/UDP/SYN/ACK/DNS Reply/DNS Req Flood，支持 TCP Port Scan/UDP Port Scan，支持 PING Sweep，支持 ARP Spoof 以及 HTTP GET/HTTP POST FLood 等常见的 DoS/DDoS 的攻击；
3、支持访问控制策略的导入导出，访问控制策略≥1000 条，可基于 IP 地址、端口（单个、多个和范围）、协议、动作（阻断、允许）进行访问策略配置，并可支持是否生成访问控制策略的会话日志生成；
#4、支持对威胁事件分布、入侵事件-攻击类别分布、入侵事件-攻击类别趋势、TOP 入侵事件、TOP 入侵事件目的 IP、TOP 入侵事件源 IP、TOP 源 IP 地理分布等威胁事件的深度分析；
5、具备攻击快照功能，获取攻击数据包，详细记录触发告警的数据特征
6、支持关键文件的识别与阻断，能识别的关键文件类型应包含至少以下几类：文档类如 Excel、PDF、PowerPoint、Word 等，压缩文件类如 ZIP、RAR、TGZ 等，图像类如 BMP、PNG、JPEG 等，音频视频类如 ASF 等，脚本类如 JS、Perl、PYTHON、PHP 等，网页类如 XML、HTML 等。
（五）统计报表
1、支持报表个性化设置功能，至少要支持汇总报表，对比报表，智能报表，综合报表等 4 种以上报表形式。
2、支持报表以天、周、月为单位导出，支持报表导出时间自定义。
（六）质量要求
★提供单独的承诺函，内容如下：
1、我公司承诺，若我公司中标，承诺合同签订前提供原厂售后服务承诺函。
2、我公司承诺，若我公司中标，承诺合同签订前提供 5 年原厂软件及特征码升级和硬件维保服务的承诺函。
三、其他要求
在后续与学校其他安全及应用服务对接时，不收取任何费用。