**日志审计设备采购要求**

1、2U机架式国产设备,千兆电口≥6，千兆光口≥4，扩展槽位≥2,内存≥16G,系统盘≥120G SSD，数据盘≥4T，USB接口≥2，日志采集处理平均速度≥3000EPS,console口≥1,冗余电源，自带液晶屏，日志源授权≥50个。含3年维保升级服务；

2、系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。支持将常用IP地址或IP地址网段标记为自定义名称，在日志查询界面可以在IP列中对应悬浮显示自定义名称；

3、支持独立展示每个被采集源最近24小时的日志数量趋势，便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态；

4、支持首页以全国地图、全球地图展示最近24小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定区域的日志详细信息；

5、支持在日志查询结果上针对源IP、目的IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源IP和目的IP（公网地址）还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果；

6、支持自定义统计日志数据形成报表，支持统计分析报表以PDF、word、execl、html等方式导出；支持实时报表、计划报表。

7、支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息；

8、支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过Agent采集日志数据。支持日志备份存储。具备较好的日志分析功能。

9、日志源：支持主流安全产品、网络产品（路由器、交换机等）、服务器、存储、数据库等。

10、支持对日志流量非常大但是日志重要程度低的syslog类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；

11、为确保产品安全厂商具备较好的应急响应能力，在使用过程中不会给业务系统带来安全风险，安全厂商需通过TL9000质量管理体系认证，且具备国家互联网应急中心颁发的网络安全应急服务支撑单位（甲级）证书。（提供权威机构颁发的相关证书复印件或扫描件，并加盖制造商公章佐证。）