|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **指标子项** | **技术及功能要求** |
| 1 | ★设备硬件要求 | 硬件架构 | 专用独立硬件设计，部署简单 |
| 接口 | ≥2个千兆接口 |
| 存储空间 | ≥2TB |
| 2 | ★性能 | 日志处理速率 | 二进制NAT日志≥30,000EPS； |
| SYSLOG日志≥3000EPS； |
| 3 | 设备监控 | 设备监控要求 | 支持设备的可用性状态，包括CPU、内存、硬盘（包括NFS存储） |
| 支持各类型日志磁盘存储占比统计 |
| 支持各类型日志接收趋势统计 |
| 持各设备日志接收趋势统计 |
| 支持对发送日志的设备状态监控 |
| 支持自定义监控面板和监控内容 |
| 4 | 日志管理 | 日志管理要求 | 支持通过以下种类进行日志浏览并可自定义查询条件，包括：事件日志、网络日志、配置日志、IPS日志、威胁日志、安全日志 、会话日志、策略路由日志、NAT日志(含NAT444)、URL日志 、IM（包含移动QQ、微信）上下线日志、论坛发帖日志、邮件日志、Ftp日志。 |
| 支持第三方日志的收集和查询 |
| 支持颜色区分日志级别 |
| 支持多条件组合查询 |
| 支持URL字段的全文检索 |
| 支持后台任务查询和邮件通知 |
| 支持查询条件记忆 |
| 支持查询条件的保持 |
| 5 | 统计报表 | 统计报表要求 | 支持统计的报表内容包括：系统资源、设备日志条数排名、设备日志所用空间排名、日志条数排名、日志所有空间排名、源IP日志量排名、目的IP日志量排名、日志接收趋势排名、威胁攻击次数、会话日志APP访问量、 URL访问量等排名 |
| 支持按照天、周、月、季等周期生成周期性统计报表，统计粒度可达到分钟、小时和天，并能够通过邮件发送给指定人员。 |
| 6 | 系统管理 | 系统管理要求 | 支持自动磁盘清理 |
| 支持分布式设置 |
| 支持NFS功能 |
| 持可信主机设备 |
| 7 | 日志管理 | 日志管理要求 | 支持FTP和SFTP设置 |
| 支持日志备份 |
| 支持日志导入 |
| 支持日志清理 |
| 支持日志转发 |
| 8 | 兼容性要求 | 兼容性要求 | 支持记录现网出口防火墙的安全日志、会话日志、NAT日志等日志信息 |
| 9 | 设备售后服务 | 设备售后服务 | 提供5年的硬件质保和软件升级售后维保服务 |
| 10 | 产品资质 | 销售许可证 | 公安部颁发的《计算机信息系统安全专用产品销售许可证》安全审计平台 日志分析（一级），提供证书文件复印件并加盖原厂公章有效 |
| 软件著作证书 | 具备计算机软件著作权登记证书，提供证书文件复印件并加盖原厂公章有效 |