**第三部分 技术参数**

1、上网行为管理

1.1、产品配置、性能要求：

万兆SFP+光接口≥4；硬盘空间≥1TB；适用带宽≥5G；≥双电源；支持IPV6；特征库升级服务≥1年。（以上要求提供产品截图加盖厂商公章）

1.2、功能要求：

|  |  |
| --- | --- |
| 部署方式 | 支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备。 |
| 系统管理 | 支持WEB图形化接口进行设备配置和管理；可通过谷歌、火狐、IE、360等浏览器访问设备。 |
| 必须支持采用公开的SSH客户端远程访问设备，必须支持采用pc自带超级终端通过设备串口管理设备。 |
| 必须支持CONSOL管理。 |
| 管理权限分立，可根据需要灵活定制管理员角色。 |
| 支持只允许特定ip访问、控制设备。 |
| 系统监控 | 实时提供设备性能图形化监控（包括CPU、内存、接口磁盘占有率。） |
| 实时提供网络上下行流量图形化监控；至少保留24小时流量状态趋势图。 |
| 实施提供网络应用排名、用户流量排名、应用流量趋势、用户流量趋势。 |
| 实时提供各类告警信息（包括行为违规告警、设备异常告警、） |
| 应用协议 | FTP、SMTP、TFTP、IMAP等常用协议。 |
| WEB下载、HTTP多线程下载、伪IE下载等多种方式的HTTP下载行为。 |
| 新浪视频、优酷视频、腾讯视频、酷六视频、搜狐视频等。 |
| 迅雷、BT、电驴、网际快车、QQ旋风等。 |
| PPLive、风行网络电视、QQLive、UUsee网络电视等。 |
| PC游戏、手机游戏。 |
| 股票、期货软件等。 |
| 流量管理 | 支持通道化的QoS，支持基于源地址、用户、服务、应用、时间进行带宽控制，并支持配置保障带宽、限制带宽、带宽借用、每IP带宽、流量限额、带宽优先级等QoS动作，时间选择支持基于日计划、周计划、单次计划等。 |
| 支持4级层次化QoS、支持多级用户/用户组嵌套。 |
| 支持用户（用户组）+应用（应用组）+时间等条件的组合进行多线路带宽管理。 |
| 支持进行IP、整机会话限制；支持日流量限额、时长限额，超过阈值提供弹窗提示且可自定义；支持流量和时长的月限额。 |
| 行为审计 | 支持网络社区应用管控的精细化管理，例如可管控“所有行为”、“登录”、“网页浏览”、“发表”、“上传”等行为，并提供web配置界面截图。 |
| 支持即时通讯应用管控的精细化管理，例如微信的“所有行为”、“语音”、“发消息”、“收消息”、“登录”、“发文件”等行为，并提供web配置界面截图。 |
| 支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息，提供web界面截图。 |
| 用户管理 | 与我校深澜认证系统对接；支持excel文件导入。 |
| 与我校深澜认证系统对接；支持excel文件导入。 |
| 支持用户+ IP+MAC绑定 |
| 制定策略限制接入共享主机数量，同时可建立白名单。 |
| 支持终端类型（PC，android，苹果）识别，可识别手机操作系统和IP地址，并可将其添加到信任列表或者拒绝上网。 |
| 以IP范围设置上网区域、可对不通区域灵活管理。 |
| 网页管理 | 根据URL进行网址访问管理,实现阻断、记录、告警。 |
| 内置URL分类库，URL库可在线升级；可广泛识别恶意网站、违法网站。 |
| 过滤包含特定关键字的网络帖子和网页评论；禁止发布不良信息发布。 |
| 可识别HTTP网页的文件上传和文件下载，并对文件的上传和下载进行过滤。 |
| 加密网页进行识别和过滤，防止用户访问钓鱼网站、SSL 加密的色情、反动网站等。 |
| 邮件外发管理 | 基于发件人、收件人、主题、内容、附件名、附件大小维度进行记录、告警、过滤。 |
| 根据邮件附件的内容进行邮件发送的过滤。 |
| 必须能够基于关键字识别和过滤使用SSL加密的Webmail邮箱外发邮件的行为。 |
| 根据邮件标题、正文、附件名、文件指纹触发延迟审计。 |
| 统计报表 | 可监控到设备运行的天数,确保设备中间无重启,无宕机；可监控至少24小时内带宽分布、流量构成比例。 |
| 可查询到网页访问、论坛发帖,webmail、邮件收发、应用访问、应用流量历史日志。 |
| 可生成网页访问、论坛发帖,webmail、邮件收发、应用访问、应用流量等各种统计报表。 |
| 根据用户流量、时长、应用、网页进行排名统计。 |
| 可将报表中心相关内容转换为Excel、PDF报表。 |
| 至少保存3个月上网行为日志。 |
| 资质要求 | 具有计算机信息系统安全专用产品销售许可证，提供有效证书复印件。具有信息安全风险评估服务资质，提供有效证书复印件。具有工信部ITSS全权成员单位证书，提供有效证书复印件。 |
|  |  |

2、日志审计系统

2.1、产品配置性能要求：

本次项目配置100个日志源许可；日志采集峰值：35000EPS，日志采集均值：20000EPS，综合处理峰值：35000EPS，综合处理均值：20000EPS；数据存储能力：压缩加密存储，压缩比不低于10:1；日志存储不低于10000条/M ；支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于10s（以上要求提供产品截图加盖厂商公章）

2.2、功能要求：

|  |  |
| --- | --- |
| 数据采集 | 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26类300种日志对象的日志数据采集。 |
| 对于尚未支持的设备类型日志进行新增采集支持，在页面上传升级文件或增加配置文件即可；支持主动、被动相结合的数据采集方式；支持Telnet\SSH、Syslog、SNMP Trap、Netflow、JDBC、SSH、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，支持限制速率设置为1000条/秒、3000条/秒和5000条/秒等； （提供产品截图加盖厂商公章） |
| 数据存储 | 支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储、网络存储。 |
| 支持根据设备重要程度设置独立设置每个被采集源的数据存储时间为1个月、3个月、6个月和永久保存等参数。（提供产品截图加盖厂商公章） |
| 支持自定义存储位置，支持多盘并行存储，当磁盘满后自动切换存储位置，支持磁盘阵列、SAN、NAS等外部高性能存储。 |
| 告警管理 | 内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则。 |
| 支持告警概况、告警趋势的统一展示，实时告警可根据级别、规则类型等进行分类。 |
| 支持邮件、声音、短信、命令行等多种告警方式，支持报警内容引用字段变量参数。 |
| 统计报表 | 系统支持智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应。（提供产品截图加盖厂商公章） |
| 报表支持基于全国地图、全球地图进行访问源、访问目的追踪。 |
| 数据查询 | 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； |
| 支持等于、不等于、大于、小于、正则表达式等查询条件；支持多条件组合查询；支持为不同类型日志设置不同的查询条件和显示条件；支持原始日志全文检索。 |
| 支持在一个日志源查询结果列表中以IP为条件直接跳转到其他日志源类型中进行查询；支持在查询结果页面上直接下钻二次查询，快速定位关键日志，还可以返回上次查询条件。 |
| 日志源管理 | 支持手动添加日志源，管理员可以对日志源进行查看、添加、编辑、删除以及启\禁用的操作。 |
| 支持为日志源指定类型、名称、IP地址、收集节点、收集方式、以及日志源启停状态等属性信息。 |
| 系统管理 | 支持用户按角色管理，支持三权分立；将日志源管理权限分配给不同的操作管理员，不同用户管理不同日志源的日志，互不干扰。 |
| 支持设置非法用户访问控制策略；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。 |
| 资质要求 | 产品获得公安部计算机信息系统安全产品销售许可证（行标三级）以及公安部信息安全产品检测中心出具产品检验报告。所提供的产品检验报告须符合《信息安全技术 日志分析产品安全技术要求 GA/T 911-2010》检验规范，并提供完整的检测报告复印件（行标三级）。产品获得国家保密科技测评中心检测并获得涉密信息系统产品检测证书，需符合《涉及国家秘密的信息系统安全监控与审计产品技术要求》中日志收集与分析的相关要求，并提供完整的检测报告复印件。计算机软件著作权登记证书。 |
| 厂商资质 | 产品厂商应具备CMMI5资质证书。产品厂商应具备通信行业质量管理体系认证证书TL9000认证。 |

3、数据库审计系统

3.1、产品配置性能要求：

要求采用专用硬件平台和专用操作系统（非Windows平台）；默认包含4个10/100/1000BASE-T电口采集口，1个扩展槽位；500G，内置硬盘存储日志；≥双电源；吞吐率≥500Mbps；支持IPV6不限制数据实例授权数量；不限制监听口授权数量（以上要求提供产品截图加盖厂商公章）

3.2、功能要求：

|  |  |
| --- | --- |
| 数据库审计 | 设备可独立完成审计数据采集，不依赖于数据库自身的日志系统，审计结果存储于独立存储空间。 |
| 审计工作不影响数据库的性能、稳定性或日常管理流程。 |
| 支持审计ORACLE、SQL Server、MY SQL、DB2、Sybase、Informix、Postgresql、Kingbase、Cache、Gbase、Dameng、Teradata、Oscar、Mongodb等各类主流数据库系统。（提供产品截图加盖厂商公章） |
| 系统内置SQL语法解析器，可通过正则与非正则方式分析SQL语句的操作类型、操作对象等信息。 |
| 支持对数据库DML、DCL、DDL语句的审计，可审计的事件基本信息包括：源地址、目的地址、源端口、目的端口、源MAC、目的MAC、源用户、目的用户、源国家、目的国家、源区域、目的区域、源城市、目的城市、VLANID、时间等。 |
| 支持数据库绑定变量审计，可通过分析、提取语句中绑定变量，审计出访问数据库的源主机名、源主机用户，可监测还原SQL操作语句包括源IP地址、目的IP地址、访问时间、MAC地址、数据库用户名、客户端名称、服务端名称、数据库操作类型、数据库表名、字段名等。 |
| 支持对访问数据库的源地址、目的地址、SQL操作响应时间、数据库操作成功、失败的审计。 |
| 支持数据库账号登陆成功、失败的审计。 |
| 支持SQL操作审计，可审计数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物等。 |
| 数据库防护 | 支持对针对数据库的XSS攻击行为、SQL注入攻击行为进行审计，并进行实时报警（提供产品截图加盖厂商公章） |
| 审计关联 | 支持中间件环境下的SQL语句关联到HTTP操作，HTTP操作关联到HTTP-ID，实现中间件环境下的审计追溯（提供产品截图加盖厂商公章） |
| 支持数据库审计事件与WEB业务系统事件的关联功能，可将审计到的数据库事件，与web服务器、客户端IP地址等信息关联起来。 |
| 统计报表 | 支持WORD、PDF、CVS、EXCEL、HTML等格式导出报表。 |
| 支持邮件方式自动发送报表。 |
| 支持频率趋势图、概率统计图、饼图方式进行报表展现，并可导出统计结果报表。 |
| 支持自定义报表，可以根据客户需求定制更多有实际意义的报表。 |
| 告警管理 | 支持通过邮件、syslog、SNMP等方式进行告警。 |
| 支持对告警信息的发送方式进行设置，以防止告警信息过多，增加邮件服务器压力，至少具备单条发送、归并发送两种方式。 |
| 支持告警信息同时发送到多个管理对象。 |
| 支持告警阀值设置，可设置内容包括：连接数值、流量阀值、系统状态阈值（例如：CPU阀值设置、硬盘空间阀值空间设置、内存空间阀值设置等） |
| 支持报警事件插件的配置管理，例如：事件接收、外发、统计分析、存储等插件（提供产品截图加盖厂商公章） |
| 支持系统报警规则修改，可自定义报警规则，并定义告警级别、处理方式：系统阻断/放行（旁路）、防火墙联动阻断/放行。 |
| 系统管理 | 系统应提供配置向导，简化策略配置过程。 |
| 支持WEB登录锁定配置，可自定义用户名/密码尝试次数和登录锁定时间。 |
| 支持WEB登录超时自动登出功能，可自定义WEB端登录超时时间。 |
| 支持静态密码认证，并对密码的复杂性进行强制要求，比如大小写、数字、特殊字符、长度等。 |
| 支持角色自定义功能，可对角色权限进行细粒度划分，权限可控制到菜单级。 |
| 支持双操作系统，当常用系统出现故障可以使用备用系统恢复（提供产品截图加盖厂商公章） |
| 支持系统状态的监控功能，可监控系统的CPU、内存、磁盘、网口、运行状态等信息。 |
| 支持审计系统与管理系统一体化，不需要安装额外的管理软件，不需要单独的管理设备，无需在被审计系统上安装任何代理。（提供产品截图加盖厂商公章） |
| 升级方式 | 提供系统升级功能，能够通过升级包的方式实现升级。 |
| 接口支持 | 支持Syslog方式向外发送审计日志。 |
| 支持SNMP Trap方式向外发送审计日志。 |
| 支持NTP时间同步。 |
| 支持以SNMP方式，将系统运行状态提供给第三方网管系统。 |
| 支持原始数据包留存，可通过sftp方式从设备中取得已记录的原始数据包。 |
| 单点部署 | 支持旁路镜像模式部署，不影响数据库性能和网络架构，网络审计产品的故障不影响被审计系统的正常运行。 |
| 规则策略 | 支持审计规则的优先级的调整，以防止误报、漏报等发生。 |
| 支持审计策略的自定义，可将时间、源IP、目的IP、协议、端口、登陆账号、命令作为响应条件进行策略设置。 |
| 支持数据采集规则定义，对于不关心的数据可以不采集，有效保证系统审计的稳定性与针对性。 |
| 产品资质 | 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》国标增强级。具备IPv6 Ready Logo Phase-2证明文件。具备中国信息安全测评中心颁发的EAL3+证书。 |
| 厂商资质 | 产品厂商应具备环境管理体系14000认证。产品厂商应具备通信行业质量管理体系认证证书TL9000认证。产品厂商应具质量管理体系认证证书ISO9001认证。 |