### 数据分析部分

|  |  |
| --- | --- |
| 数据服务器3台 | 支持集群部署，节点数无限扩大，支持多节点的数据负载均衡；  CPU：配置1颗不小于至强E5 2603（6核12线程）；  内存：>=128G DDR4，实现多通道内存交叉读取；  数据盘：>=SATA 2T\*12；  网卡数量：配置intel高性能千兆控制芯片，不小于2个网口，2个万兆SFP+端口；  拥有不小于6个PCI插槽  MTBF稳定可靠系统测试  稳定可靠MTBF大于5年  配置1+1冗余电源，电源功率不高于600W |
| 核心服务器2台 | 支持集群部署，节点数无限扩大，支持多节点的数据负载均衡；  CPU：配置2颗不小于至强E5 2640；  内存：>=256G DDR4，实现多通道内存交叉读取；  数据盘：>=SATA 4T\*12；  网卡数量：配置intel高性能千兆控制芯片，不小于2个网口，2个万兆SFP+端口；  拥有不小于6个PCI插槽  MTBF稳定可靠系统测试  稳定可靠MTBF大于5年  配置1+1冗余电源，电源功率不高于600W |
| 管理及维护 | 支持中文Web管理界面；支持Web界面在线升级；支持同时接收多台流量设备日志；支持本地“系统维护”，如“用户管理、设备管理、数据库维护等”； |
| ★数据分析 | 支持会话日志，会话日志包含设备编号、接口、访问时间、源地址、目标地址、NAT地址、账号信息、域名、协议类型、7层协议名称、流量、运营商、地理位置一共13个元素。同时采用1:1 的日志输出，完整保留网络中的相关信息。（提供抓图）  支持虚拟身份查询。通过QQ号码，微信ID，邮箱地址，淘宝账号，手机IMEI信息来查询到对应的IP地址（提供抓图）  支持对校园网内无线路由器的SSID查询，查出私搭路由器问题，对可以查看私搭路由器的IP地址（提供抓图）  可以对使用校园网IP的地理位置定位，协助校园网管理者找出私拉校园网线路行为。（提供抓图）  支持“域名地图”，区域URL访问量数据分部图。例如：招生期间，可以看到那个省的用户对校园网主页，招生服务器访问排名。（提供抓图）  提供校内任何IP的用户画像功能。可以分析该用户访问的地理区域，去往各个运营商比例，该用户的TOP协议排名图，用户访问流量趋势图，用访问连接趋势图和该用户访问域名排名、身份信息等。（提供抓图）  支持对任何URL去往运营商统计，并提供比例饼图与统计数值（提供抓图）  支持“流量流向”统计功能，如去往电信、去往移动等，并提供比例饼图与统计数值（提供抓图）  对校内提供HTTP或者HTTPS访问的域名进行统计，发现校内教育网IP使用校外域名的情况。（提供抓图）  须对IPV6的应用层协议进行分析统计并留存日志；  对校内用户访问校外图书馆资源进行统计，提供对图书馆资源流量和下载排名；（提供抓图）  对校内用户下载校外图书馆次数作统计，提供下载排名，发现恶意下载用户。（提供抓图）  TOP域名统计，提供校内用户访问校外的TOP URL统计。  支持标准SQL接口，支持JDBC，ODBC驱动。对于10亿级进行计数统计，完成时间小于60秒。对于10亿级数据进行分组排序，完成时间分钟级。对于10亿级数据进行分组排序，完成时间分钟级。百万条记录表与百亿条记录表等值关联查询分钟级完成。批量导出数据，万兆网环境下，单节点速度大于100MB/秒。对于10亿级数据的同源分析，完成时间分钟级支持跨数据中心查询业务，数据中心元数据变化同步秒级；  支持数据中心个数不小于100个。以流量流向、流量概况、用户画像、7层应用事件反查、访问排序、虚拟身份信息、移动终端识别、用户行为、地理位置、终端用户热力图、IP轨迹、TOP域名、应用流量流向图、URL地图、TOP用户、连接可视化分析和DNS可视化分析等为代表的内置分析工具，为用户提供了全面记录、了解、分析和掌握网络细节和趋势的能力。 |
| IP地址日志 | 可对支持IP地址日志进行查询审计，包含：（对IP上行、下行、总流量、连接数进行记录与分析，对IP流量趋势进行分析等） |
| 七层应用日志 | 可对应用日志进行查询审计，包含：（对上行、下行及总流量进行时间统计，对流量趋势及系统流量进行统计，对应用协议或自定义协议进行分析，对应用连接数进行分析等） |
| 账号日志 | 可对账号日志进行查询审计，包含：（QQ、MSN、POP3、新浪微博/搜狐微博/腾讯微博帐号、淘宝帐号、飞信帐号等登陆时间日志进行记录，URL帐号访问事件进行记录，认证事件日志（Radius、PPPOE）进行记录，节点日志进行记录，DNS日志进行记录，域名访问统计等进行记录） |
| 报表功能 | 报表可自动生成（包含日报、周报、月报等）；  可以根据内容自定义报表并导出； |
| 投标公司提供承诺函 | 承诺能够在中标后一周内提供测试设备上线测试，实现对产品功能的核对。避免真实功能与技术偏离表响应不一致的虚假应答。 |
| 质保期及售后服务 | 设备软件及硬件要求质保期为三年；同时要求投标公司出示厂商的授权及售后服务承诺。 |

### 数据捕获部分

数据捕获设备：1台

|  |  |
| --- | --- |
| ★性能参数 | 最大吞吐量 >=80Gbps, 并发连接数 >=1600万, 每秒新建会话数 >=100万/秒, PPS（包转发率）>=2800万, 网络接口：4个千兆电口，6个万兆SFP+光口，2个40Ge的QSFP+光口; |
| 捕获链路 | 支持的N（N>=12）条物理链路，数目和硬件接口数有关，不受软件限制, 支持对整个系统进行全局策略管理和分析统计, 支持对各条链路进行独立的分析统计, 支持4条虚拟链路，基于物理接口、IP组定义并对其统计; |
| 协议识别 | 支持对2～7层流量的识别能力（IPV4和IPV6），特别是针对第 7层的应用识别能力，能够识别主要应用协议，并逐级细分P2P下载、网络视频、网络电话、游戏、HTTP协议的子类别和具体客户端名称, 支持国内各类常见协议>=1000种，其中大型游戏>=300种，移动APP应用>=200种，现网协议识别率 >= 95%,支持DPI、DFI、节点跟踪、主动探测、加密分析等多种技术，对已经采用加密技术的P2P类应用，BT、迅雷、Skype、eDonkey、Qvod、PPFilm、百度影音等精确识别, 可以区分迅雷、网际快车等下载工具的HTTP下载和IE浏览器下载, 支持“迅雷增强识别”，改进对迅雷加密流量识别, 支持“P2P智能识别”，改进P2P加密协议识别, 协议精细分类且必须包含：移动浏览器（iPhone手机上网）、应用商店（安卓市场、手机报等）、云服务、网络支付（招商银行、兴业银行等）、移动游戏（手机游戏、iPad游戏）, 支持虚拟身份的识别，如QQ号码、MSN帐号、POP3帐号、新浪微博、百度贴吧等; |
| 移动终端识别 | 自动对移动终端型号进行识别，不依赖特征库, 移动终端信息统计，如访问IP、首次访问时间、最近访问时间, 对移动设备的网络访问进行分析识别, 支持黑名单，当误识别时，将时别错误的终端类型放入黑名单，避免误识别; |
| PC共享检测 | 能够及时检测通过路由共享上网的PC个数, 能够检测出路由器后PC所使用的Windows版本类型, 可以根据PC终端个数做条件，对流量做识别检测; |
| ★监控统计 | 可提供整个系统、各链路的流量和连接数统计图表, 可提供最近10分钟流量、累计流量、并发连接数统计图表, 实时显示各协议组的当前速率、连接数等统计信息，自动刷新, 可提供最近一天、最近一周和最近一月的流量趋势图表, 可提供上行流量、下行流量、并发连接数的“三日对比”趋势图, 支持TOP应用排序, 支持TOP用户排序,可实时显示每一个IP流量速率和当前各个应用的速率明细, 可实时显示某个IP的当前速率及连接明细，以便于异常流量诊断, 可提供IP对应的身份信息，QQ号码、MSN帐号、POP3帐号、微博帐号等, 可根据应用速率、流量和连接数等条件进行排序, 可实时显示某个应用下的Top用户, 可提供在线并发连接、连接新建和删除速率等数据的趋势图表, 可提供在线IP数和共享用户趋势图表, 可选择两个或多个应用协议进行趋势图分析对比 支持“移动终端”信息统计，包含手机类型、访问IP和时间等, 支持TOP连接排序，可以指定应用和IP条件进行IP（内网IP和外网IP均可）连接数排名统计，以快速定位攻击或被攻击IP; |
| 升级服务 | 年升级次数承诺总计不少于10次, 对于用户要求识别的非加密类应用协议，承诺在72小时内完成特征库升级支持, 支持逆向升级（版本回退）; |
| 安全防护 | 支持“内网伪IP”防护功能； 检测并控制内网中毒设备伪装大量假IP攻击网络的行为, 支持“垃圾包”检测及过滤功能, 支持“IP分片”攻击检测及过滤功能, 支持对异常流量IP的实时查询、日志反查功能; |
| 数据镜像 | 支持端口镜像功能；可根据设置条件将类如迅雷、网桥设备上行方向、某IP/IP段、iPhone手机上网流量、未知协议等流量等镜像至指定网络接口，与第三方审计设备联动，便于用户做精细化、个性化的数据分析, HTTP管控中，特别支持将WWW访问流量转发至指定网络接口，供第三方审计设备深入分析用户的网站访问习惯、兴趣等运营数据; |
| 其它功能 | 支持云平台集中管理设备，支持VLAN，支持VLAN Trunk，支持QinQ，“应用分流”功能中支持VLAN-Tag；支持PPPOE帐号识别与IP关联统计功能；支持Radius帐号识别与IP关联统计功能；支持MAC黑名单功能；支持iftop功能，用来监控从某个网卡流入流量大的的Top IP，定位外网攻击源；支持ADSL定时重播；支持针对Gn接口数据包的解码，含GTP-C和GTP-U解码分析； |
| 和认证联动 | 可以旁路或串接模式下，深度分析认证服务器RADIUS数据包，找到帐号和IP地址对应关系；自动对相应IP做深度的检测与分析； |
| 投标公司提供承诺函 | 承诺能够在中标后一周内提供测试设备上线测试，实现对产品功能的核对。避免真实功能与技术偏离表响应不一致的虚假应答。 |
| 质保期限 | 设备软件及硬件要求质保期为三年；同时要求投标公司出示厂商的授权及售后服务承诺。 |