上网行为管理系统业务需求

一、系统核心功能

本次拟建设的上网行为管理系统，将聚焦学生网络滥用问题的精准破解，核心功能应基于成熟技术研发，确保实用性、稳定性与可操作性。优先考虑已在多所高校落地应用并验证效果的系统。系统应至少满足以下功能需求：

（一）境外 IP 自动识别与地理标注

系统可自动识别用户访问的目标 IP 是否为境外地址，并准确标注其所属国家或地区，支持 200+国家/地区的归属地判断。在监控界面中以“境外”标签明确标识，便于快速筛选和分析。

（二）跨境访问日志全要素留存

完整记录跨境访问的关键信息，包括：用户账号、终端 IP、访问时间、目的 IP、国家归属、访问的完整 URL、网页标题、搜索关键词等。日志存储周期不少于 12 个月，支持高效查询与回溯。

（三）高危行为实时监控与告警

内置境外高危网站情报库，可自动识别并告警以下行为：

1.访问涉黄、涉赌、诈骗类境外站点；

2.连接挖矿、木马、远程控制等恶意服务器；

3.使用 Shadowsocks、OpenVPN 等工具进行非法翻墙。 系统支持策略联动，可对高风险行为实施自动阻断。

（四）可视化统计与一键生成报告

提供多维度跨境访问统计视图，包括全球热力图、国家访问排名、高频账号清单等。支持按院系、部门、时间段生成《跨境访问报告》，一键导出，10 秒内完成取证，格式符合教育行业合规检查要求。

（五）其他主要功能

1.日志统计

（1）所有日志：所有日志展示所有上网行为日志，含用户账号、访问时间、源 IP、目的 IP、源端口、目的端口、应用协议、动作、上下行流量等信息查询，以及导出日志功能。

（2）网页标题：网页标题包含用户上网行为中抓取的网页标题审计信息的查询及导出功能。

（3）搜索日志：搜索日志包含用户上网行为中抓取的搜索日志、关键字等信息的查询及导出功能。

（4）账号登录：账号登录包含用户上网行为中抓取的用户 QQ 登录等信息的查询及导出功能。

（5）支持至少一年以上的日志数据存储，快速为溯源分析提供数据查询。

2.数据分析

（1）基本上网行为动态，智能分析和数据采集，形成直观的数据图展示。

（2）深层次内容分析，上网行为管理基于用户身份的分析功能，外置/本地化日志、统计与报表。

3.流控策略

（1）流控策略包含对上网策略控制，应用控制、地址控制的定义与规则。

（2）自定义上网应用、HTTP 协议流量控制，支持带宽速率限制，针对告警应用进行流量阻断

（3）限制软件应用的上网流量，支持禁止视频、音乐、下载、P2P 等无关流量

（4）tcp 协议，udp 协议访问 url 过程全记录，并可针对违法网站进行阻断、限速限制。

4.策略执行

（1）支持分布式部署和旁路模式，配置各种管理规则，策略自动分发

（2）支持远程自动升级、日志存储、日志维护等

5.接口扩展

提供多种定制接口，实现强大的二次开发能力，及与第三方平台对接和扩展的能力。

6.全面的数据采集

使用日志分析工具对采集到的日志数据进行分析，包括检测异常活动、识别潜在的安全威胁等。根据需求和合规性要求，定期生成报表，包括日志统计报表、安全事件报告等。

7.问题排查和分析

通过对日志数据的分析和查询，可以快速定位和解决系统问题，提高系统的稳定性和可靠性。

8.联动其他产品管控

基于流控策略的审计规则，同时支持 AAA，BRAS 做深度的联动管控，如强制下线，页面告警，微信通知，禁止认证，黑名单等控制处理。

9.高稳定的算法分析

全内存运算方式保证了事件分析极高的效率和实时性，无缝对接石斧系列产品（AAA，BRAS），无论在分析速度、分析维度、灵活性、IO 抗压能力，系统业务兼容方面都占优势。另外，在关联算法方面，石斧日志审计管理系统有如下独到之处：

（1）标准化之上的关联规则，适应性强

（2）可定制性强，几乎可根据通用事件的任何字段进行关联

10.可维护性及可扩展性

系统具有对自身的维护配置功能，如：系统参数设置、系统日志管理等。 硬件系统采用模块结构，保证系统内存、CPU 及储存容量的扩展；硬件配置的升级不会引起软件的修改和开发；每个组件都可以横向扩展，通过增加设备满足业务需求。

二、设备核心参数

设备应至少满足以下参数需求：

1.性能要求：2U 可上架，2 个 SFP+万兆光口，6 个 RJ45 千兆电口，带宽处理能力≥10Gbps，每秒新建连接数≥70 万，会话数≥500 万，在线用户数≥3000 个，冗余交流电源，在线并发用户数≥3000 个。

2.日志同时支持数据库和文件两种保存方式;支持与认证计费系统联动同步 IP 和账号。

3.支持 DPI 七层应用识别，支持互联网常见应用协议识别，支持即时通讯，网页，邮件，P2P 下载，视频，游戏等协议及应用，页面可显示图表显示识别结果。

4.支持按应用协议/应用分类统计出口流量使用情况。

5.支持审计日志，日志需要详细记录上网五元组和账号，时间，URL，NATIP,NAT 端口，应用类别，应用名称，日志至少可以保留 6 个月以上，日志文件支持自动压缩。

6.支持跨境统计分析，对访问境外的目标 IP，域名，账号，应用等进行分类统计，提供图表展示，并可导出访问境外的账号，目标 IP，域名的统计数据，包括请求数及流量等；支持对跨境流量进行实时监控，可通过全球地图直接地显示目录跨境的访问请求，并对跨境访问的用户，国家，目标 IP，域名等进行排名统计。

7.支持翻墙统计，对翻墙的应用协议、账号和翻墙的时间段进行统计，并对翻墙的用户根据翻墙次数进行排名，提供图表展示，并可导出翻墙的账号，应用协议的统计数据，包括请求数及流量。

8. 支持日志文件，审计日志，备份日志，系统日志自动清除功能，可定义保留天数。