

附件

我校计划对校园网出口互联网网络安全防护能力实施升级，使其满足新一代网络安全要求，并具备支撑学校 1.5G 流量带宽的能力,具体需求如下：

产品名称	性能参数	单位	数量
防火墙	标准机架式设备，配置国产化操作系统，国产化 CPU，内存≥32G，≥10 个千兆电口，≥8 个千兆光口（满配千兆多模光模块），≥4 个万兆光口（满配万兆多模光模），系统盘 msata 卡≥16G；≥4TB 硬盘；双电源模块；防火墙吞吐≥20G，并发连接≥1000 万，新建连接≥25 万/秒。含现有终端威胁防御系统 3 年联动管控授权； 功能要求： 1、支持基于单个资产以折线图方式展示安全事件趋势，对其安全事件进行举证，并对其访问流量及次数进行展示，从而可判定资产是否已失陷；提供产品功能截图并加盖制造商公章 2、支持多元组的访问控制规则，支持基于源 MAC、源端口、服务、时间、域 URL 等多个元素进行访问控制，支持域名的访问控制； 3、为提高学校业务访问效率，支持作为 DNS 服务器可依据访问地址来源将服务器域名解析为内部地址或外部地址，同时支持通过配置多条转换策略，实现内网资源服务器的负载均衡，提供产品功能截图并加盖制造商公章； 4、支持 NAT 地址池探测，支持 NAT 策略冲突、包含、冗余检测，并支持 NAT 策略命中数统计；提供产品功能截图并加盖制造商公章； 5、访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址，提供产品功能截图并加盖制造商公章； 6、支持威胁地图大屏功能，可以单独开启/关闭威胁地图；支持依地图形式展示攻击信息，可以详细展示攻击链路与方向，支持安全事件实时播报，展示当日风险资产统计、最近 1 小时攻击源（TOP5）、基于高中低的攻击趋势，提供产品功能截图并加盖制造商公章； 7、提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度检索； 8、支持策略变更信息管理功能，支持查看变更策略、变更动作、变更时间、修改人、登陆 IP，支持对变更前后的策略进行直观对比，并能一键还原配置；提供产品功能截图并加盖制造商公章 9、支持独立的入侵防护规则特征库，特征总数在 12000 条以上，能对常见漏洞进行安全防护；支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御，病毒特征库规模超过 200 万；支持独立 WAF 模块，支持安全优先、标准策略、应用优先安全策略，Web 攻击规则库总数在 6000 条以上，可设置记录报文开关，支持基于 ID，CVE 编号，描述的规则搜索；逐项提供产品功能截图并加盖制造商公章 10、支持与现有终端威胁检测系统联动，获取终端威胁检测系统资产信息，提供资产 IP、资产状态、安全状态、资产详情等信息，并可对资产按照安全状态、资产类别、操作系统等分类进行统计，提供防火墙和终端威胁检测系统厂家承诺函； 11、支持基于 IPV4/V6 源地址、目的地址动态五元组黑名单功能，支持动态黑名单批量添加、导入，支持命中数统计；提供产品功能截图并加盖制造商公章 12、内置用户身份管理系统，实现基于用户的访问控制。支持 RADIUS、TACACS、LDAP 等多种认证协议和认证方式。在用户管理方面，实现分级、分组、权限、继承关系等功能； 13、支持对内网资产的 telnet、ssh、rdp 等常用的远程控制协议进行跟踪，支持对内网资产提供 socks5 代理的情况进行跟踪； 14、支持对每类型日志容量上限设置，达到容量上限后可选择自动覆盖或停止存储，支持	台	1

	按天导出日志，并显示文件大小；提供产品功能截图并加盖制造商公章； 15、项目终验合格后，免费提供三年原厂质保服务及 IDP 攻击规则特征库三年升级许可、专业版快速查杀病毒库三年升级许可、Web 应用防护特征库三年升级服务许可。 16、所投产品具有 CCC 中国国家强制性产品认证证书、中国环境标志产品认证证书。		
日志审核分析	标准机架式设备，配置国产化操作系统，国产化 CPU，≥6 个千兆电口+4 个千兆光插槽（含 2 个光模块）；1 个 console 口，2 个 USB 口，≥2 个扩展槽位；≥16G 内存，数据盘≥4T；系统盘≥256G mSATA；单电源；日志采集处理均值≥1000EPS，含 50 日志源。 功能要求： 1、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志数据采集。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。 2、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， 3、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、支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数，对应产品软件提供带有 CNAS 认证的第三方检测报告证明并加盖制造商公章； 5、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。支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析，对应产品软件提供带有 CNAS 认证的第三方检测报告证明并加盖制造商公章； 6、支持多种运维管理工具，可对日志源进行 HTTP、HTTPS、SSH、SFTP、FTP 等操作。 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、支持亿级数据交互式多条件查询，百亿级日志查询响应时间小于 5s，千亿级日志查询时间小于 10s，对应产品软件提供带有 CNAS 认证的第三方检测报告证明并加盖制造商公章； 9、项目终验合格后，免费提供三年原厂质保服务。 10、为保证交付质量和自主可控能力，投标人所投安全产品制造商具备有效期内的《国产化信息系统集成和服务能力等级证书》LS4 级；	台	1
上网行为管理	标准机架式设备，配置国产化操作系统，国产 CPU，硬盘：≥4T，内存：≥16G，≥8 个千兆电口，≥4 个千兆光口（含 2 个千兆多模模块），1 个 console 口，2 个 USB 接口，≥2 个扩展槽，支持 2 对电口 Bypass；单电源；带宽性能：≥350M，推荐用户数：≥1500 人；最大并发连接数：≥100W；含现有终端威胁防御系统 3 年联动管控授权； 功能要求： 1、用户拥有多个网络区域访问权限时，可以实现用户在任意时刻只能访问一个网络，切换网络需要用户点击切换按钮，无需管理员干预，在不影响多网络使用的同时，实现网络逻辑隔离，加强网络访问安全。可支持自定义 7 个网络区域。可支持根据域名划分网络区域。 2、支持流量白名单，过滤掉不关注资产流量，白名单类型包括 IP、端口、邮箱、域名等。 3、支持基于应用层服务和 SAAS 的策略路由，可基于 IP、国家列表、ISP 自动地址表和域名来控制目的地址； 4、可对接入的移动终端区分出 IOS 终端、安卓终端、三星终端，并可以根据所区分出的终端类型设置告警和拒绝动作。 5、对于 Windows PC 端的外联行为进行检测，包括拨号行为，使用双网卡，无线网卡，连接非法 WIFI，4G 网卡，使用非法网关，连接外网，使用代理，以及自定义非法外联，等行为进行检测，对违规的用户可禁止上网。支持控制 Windows PC 端访问指定的 IP 地址范围，或者不允许访问指定 IP 地址范围；	台	1

	6、支持临时账号自动申请功能，方便外来的临时用户使用。支持自动审核和管理员手动审核的核定方法将临时帐户加入到组织结构中。支持网页发送和邮件方式通知临时用户账号和密码 7、支持临时账户、绑定账户、认证账户等多种用户身份的有效期设置，支持过期冻结、支持无流量自动下线。 8、可通过 NetbIOS 协议扫描内网的主机信息，扫描结果将列出每个主机的 IP 地址、MAC 地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理，提供产品功能截图并加盖制造商公章。 9、支持短信认证、微信认证、钉钉认证、企业微信认证、二维码认证、刷卡认证； 10、能够提供流量适用排名，提供前 50 名用户流量适用情况，并支持趋势图、黑名单、显示活跃服务等操作。通过黑名单可以直接强制某个流量异常用户下线或者快速修改带宽。 11、支持 10000 条以上的应用特征数量，支持论坛、微博发帖关键字过滤，支持搜索引擎关键字过滤，支持邮件内容、正文标题，支持包含制定关键字的页面过滤，提供产品功能截图并加盖制造商公章。 12、基于个人的所有行为监控报表，包括：网页标题记录、发帖记录、网页评论记录、在搜索引擎上的搜索记录、网页文件上传记录、URL 访问记录、即时通讯的登录信息/聊天内容/文件传输记录、邮件记录（详细内容、附件）、FTP 登录信息/上传记录/下载记录； 13、支持与现有服务器业务的终端检测防御系统联动，实现安装了终端检测防御系统的终端才能入网，没有安装的不允许入网。提供终端检测防御系统及上网行为管理系统厂家承诺函。 14、项目终验合格后，免费提供三年原厂质保服务及三年系统版本升级、URL 库及应用特征库升级许可。 15、为保证交付质量和自主可控能力，投标人所投安全产品制造商具备有效期内的《国产化信息系统集成和服务能力等级证书》LS4 级；		
--	--	--	--