|  |  |  |
| --- | --- | --- |
| 参数性质 | 序号 | 技术参数与性能指标 |
|  | 1 | **防火墙（1套）**  ★（1）标准机架式设备，冗余电源，配置≥6个千兆电口,≥6个千兆光口，不少于6个万兆光口，网络层吞吐量≥50Gbps，应用层吞吐量≥40Gbps；新建连接数≥35万，并发连接数≥1200万，IPSec VPN 隧道数≥2000，IPSec VPN 吞吐≥3G，具有SSL VPN 能力。  （2）内置专用操作系统，支持静态路由，动态路由（OSPF、RIP、BGP、ISIS等），VLAN间路由，单臂路由，组播路由等。  （3）支持链路负载均衡和链路健康检查，支持轮询、加权轮询、就近选路、优先级、带宽比率等多种链路负载均衡算法，支持备用选路算法，支持链路过载保护；  （4）支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。  （5）支持策略命中数显示及策略变更信息管理，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。（需提供产品功能截图证明或第三方检测报告，并加盖公章）  （6）支持主流IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、NTP泛洪攻击防护。  （7）支持与入侵防御联动，获取设备上的威胁检测结果，实现动态阻断并可自定义阻断时间。（需提供产品功能截图证明并加盖公章）  （8）支持行为分析功能，对新建连接数、并发连接数、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；支持行为分析监控展示，可展示不同行为分析策略的实时数据和基线数据趋势。  （9）支持多对一、一对多和一对一等NAT方式以及NAT44 、NAT64、NAT66地址转换方式。  （10）支持虚拟防火墙的创建、启动、关闭、删除功能；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、安全策略等功能。  （11）支持通过学习资产的访问流量、访问次数数据，生成资产行为画像，实际行为出现偏差时判定异常并产生告警。（需提供产品功能截图证明或第三方检测报告，并加盖公章）  （12）要求所投产品具备《网络关键设备和网络安全专用产品目录》相应的认证证书或检测证书，提供证明文件；  **（13）本次产品要求提供原厂质保服务3年。** |
|  | 2 | **上网行为管理（1套）**  ★（1）标准机架式设备，冗余电源，配置不少于2个千兆电口，不少于6个万兆光口，网络层吞吐量≥20Gbps，应用层吞吐量≥15Gbps；带宽性能≥10Gb，并发连接数≥800万，支持用户数≥100000。  （2）部署模式支持路由模式、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。透明、路由模式下支持将多条链路带宽进行捆绑。支持配置基于用户和应用均为任意的5元组的IPv6策略。  （3）支持创建用户组、用户，各分组能继承父组策略，用户能继承组的策略。  （4）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；支持流量和时长的月限额。（需提供产品功能截图证明并加盖公章）  （5）支持多种认证方式，包括本地用户名密码、第三方服务器、短信认证、二维码认证等。  （6）支持周期性将http流量重定向到指定公告页面，能够为上网用户在浏览器进行网站浏览时周期性的对其展示公告页面；公告页面可指定url使用外部公告页面，重定向公告页面的周期可自定义重定向间隔时间，或是自定义访问次数到达指定次数后进行重定向，以及在指定时间内访问网站到达指定次数后进行重定向到公告页面。（需提供产品功能截图证明并加盖公章）  （7）支持对僵尸网络主机进行识别，发现风险后，可对风险主机进行阻断、冻结或者告警处置。  （8）设备内置海量预分类的URL地址库，能够针对：网上购物、成人内容、求职招聘、宗教、在线影音及下载、游戏资讯、网上聊天、个人网站及博客、色情、赌博、非法药物、风水命理、娱乐场所、汽车、餐饮、钓鱼及恶意网站、网上银行、在线支付等各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制。  （9）DHCP静态分配：支持配置DHCPv4固定地址的IP-（MAC/Option82/主机名）绑定；  （10）从内网整体网络的宏观角度展现网络使用概况、上网目的地分布、热门应用流量分布、网站类型分析、终端类型分析、在线人群趋势、违规行为统计等多维度全方位展现网络的使用综合态势；  （11）要求所投产品具备《网络关键设备和网络安全专用产品目录》相应的认证证书或检测证书，提供证明文件  （12）本次产品要求提供3年原厂维保服务及规则库升级许可的承诺。 |
|  | 3 | **项目团队要求**  为保证本项目的交付质量，在系统实施期间，投标人必须派遣至少1名项目经理、4名网络安全技术工程师（提供人员认证证书（项目经理证书：PMP认证、信息系统项目管理师、CCRC信息安全保障人员认证证书CISAW；团队成员证书：注册信息安全工程师CISP）及在所在单位近3个月的社保缴纳证明）协助项目管理、系统安装、调试、集成测试、培训上线，并随时响应用户的各种技术需求。  同时，为保障服务质量，投标人应根据现场需求提供定期（包括风险评估、优化改善、特殊时段驻场等）或不定期（故障响应、请求响应、保障服务等）的技术支持。 |
|  | 4 | **业务保障要求**  为保障业务连续性，投标人具备在2小时内到场服务并提供专项备品备件的能力，需提供承诺函。  投标人需提供系统应急方案，确保在突发紧急状况下能够快速响应，缩短业务系统中断时间，降低系统风险。 |
|  | 5 | **设备巡检要求**  质保期内，每季度定期提供设备全面巡检服务，记录设备的运行状态，发现并排除系统故障，调整系统运行参数，保证系统运行在良好状态。及时响应我校的调试、优化及故障排除，确保服服务范围内设备无故障、稳定运行，并交付《巡检报告》。 |
|  | 6 | **项目实施**  （1）投标人根据陕西邮电职业技术学院实际情况提供完善的核心网络架构规划，如网络拓扑图、IPV6地址规划等，并提供设计、施工方案，按照校方要求对所有安全设备配置进行调整及优化工作。  （2）项目施工包含设备安装部署、设备所需光模块，辅材及人工等。  （3）服务期内对校园网络资产全面梳理（内容包含：IP、终端/服务器、网络安全设备等），资产可通过自动或手动配置新增，资产信息全面收录到防火墙集中监控；资产发生变更时，根据上报的信息进行确认更新。  （4）服务期内对资产进行统计和管理，可实时查看资产详情、漏洞详情、脆弱等级、安全状态、所处位置、风险等级/安全评分、安全防护策略，并对资产进行分组和防护优化。  （5）服务期内根据服务器数据报文流量进行统计（提供日报/周报），包括各个服务器的服务器IP、上行流量、下行流量、总流量以及新建会话数。 |
|  | 7 | **项目验收要求**  拟制详细的设计、施工方案，方案中应至少包含但不限于设计详细的网络优化建议、实施计划方案、完善的培训售后方案等。验收资料包括但不限于以下内容：  1、网络优化建议  2、实施计划方案  3、运维巡检方案  4、网络拓扑、网络资产清单  5、设备配置资料  6、项目自检报告 |