|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **一、采购清单**   |  |  |  |  | | --- | --- | --- | --- | | 序号 | 产品名称 | 数量 | 单位 | |  | 下一代防火墙 | 1 | 台 | |  | 上网行为管理 | 1 | 台 | |  | 安全托管服务 | 5 | 年 | |
| **二、下一代防火墙**  1.性能参数：网络层吞吐量≥100G，应用层吞吐量≥40G，防病毒吞吐量≥19G，IPS吞吐量≥24G，全威胁吞吐量≥16G，并发连接数≥2000万，HTTP新建连接数≥80万。提供但不限于：产品彩页、官网截图、检测报告等相关证明材料。  2.硬件参数：规格：2U，内存大小≥96G，硬盘容量≥480G SSD+960G SSD，接口≥4千兆电口，≥4千兆光口SFP，≥8万兆光口SFP+。提供但不限于：产品彩页、官网截图、检测报告等相关证明材料。  3.提供基于网络区域、网络对象、MAC地址、服务、应用、域名等维度进行访问控制策略设置。  4.提供应用识别和控制功能，可以对不少于9000种应用进行检测与控制。  5.提供DDoS防护功能，对ICMP、UDP、DNS、SYN等协议进行DDOS防护。  6.提供防病毒功能，对压缩病毒文件进行检测和拦截，具备独立的勒索病毒防护模块界面。提供但不限于：产品彩页、官网截图、检测报告等相关证明材料。  7.提供入侵攻击防御功能，内置不低于16000种漏洞规则，  8.提供僵尸主机检测功能，内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。  9.提供Web应用防御功能，内置超过4000种WEB应用攻击特征。  10.提供服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。  11.提供Cookie攻击防护功能，并通过日志记录Cookie被篡改。  12.提供独立的账号安全防护功能，可以展示账号安全相关信息，包括风险业务、风险等级、存在账号入口、存在弱口令、遭受口令爆破、异常登录账号等。  13.提供威胁情报功能，采用云端威胁情报实时同步，对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，对未知威胁情报实现分钟级全网设备下发。  14.提供蜜罐功能，内置伪装业务诱饵，诱捕内外网的攻击行为，并联合云端分析技术溯源和反制。  15.提供和现网（现网深信服安全态势感知产品）联动功能，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。提供供应商承诺函。  16.配备一名在线服务专家，对防火墙设备进行策略检查，并给出策略优化方案，确保设备处于最佳防护状态。  17.提供微信小程序处置功能，支持在微信端对流量日志分析、事件聚合、云端专家研判。  18.具备网络安全应急服务支撑单位甲级资质。提供但不限于：产品彩页、官网截图、检测报告等相关证明材料。  19.提供5年原厂产品质保+软件升级 |
| **三、上网行为管理**  1.性能参数：网络层吞吐量≥30Gb;应用层吞吐量≥15Gb;上下行带宽性能≥15Gb;秒新建连接数≥200000;最大并发连接数≥8000000。提供但不限于：产品彩页、官网截图、检测报告等相关证明材料。  2.硬件参数：规格:2U;接口≥4千兆电口，≥4千兆光口SFP，≥4万兆光口SFP+。提供但不限于：产品彩页、官网截图、检测报告等相关证明材料。  3.提供终端资产管理功能，自动发现接入校园网的终端，包括PC、手机、摄像头、打印机等，并获取IP、Mac、厂商、操作系统等信息，同时支持图形化查看当前内网IP使用情况。  4.提供实时接入状态功能，首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行。  5.提供用户管理功能，支持为师生添加属性（角色、学院、接入位置等），根据师生属性配置上网权限策略、流控策略，审计策略等。  6.提供弱密码防护功能，可设置密码最小长度、复杂度，可设置密码不能与用户名相同、新密码不能与旧密码相同。  7.提供认证管理功能，802.1x认证可对接本地和AD域用户源进行用户名密码认证，师生账号绑定手机号码和微信号实现上网快捷登录认证。  8.提供流量动态调整功能，根据校园网线路的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；其中空闲阈值可自定义。  9.提供加密网页管理功能，支持SSL加密网页的内容检查，针对加密后的钓鱼网站、非法网站，可对师生进行重定向告警。  10.提供网络代理管理功能，实现HTTP、SOCKS4/5上网代理及二级代理；支持代理控制功能，不允许使用外部HTTP代理，不允许使用外部SOCKS4/5代理，不允许在HTTP，SSL一些的标准端口上使用其他协议。  11.提供业务访问审计功能，支持WEB/FTP/SMB类型业务的行为和内容审计；支持服务器外联行为及流量审计。  12.提供多产品联动功能，支持与防火墙系统实现认证联动，实现单点登录；支持与现网深信服安全态势感知产品实现联动，实现资产信息上报。提供供应商承诺函。  13.提供用户认证故障排查功能，针对师生认证的故障进行分析，给出错误详情以及排查建议  14.提供校园网访问质量检测功能，针对校园网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级。  15.具备中国信息安全测评中心颁发的信息安全服务资质（安全开发类二级）。提供证明材料并加盖公章。  **16.**提供5年原厂产品质保+软件升级。 |
| **四、安全托管服务**  1.为学校不少于20个核心资产（数据中心资产IP数量）提供7\*24小时连续性的安全保障，一次性提供五年服务。不论是白天、黑夜、节假日供应商都应该能做到7\*24H在线服务，配置一名经验丰富的安全专家作为专属服务经理，并组建专属微信服务群，实时响应学校咨询的网络安全相关问题。  2.供应商提供不低于以下服务效果的SLA承诺，提供服务承诺函：（1）一般事件：从安全日志产生到通告<1Hour、遏制影响时间<4H、经供应商确认后，准确率达99%、事件闭环率100%；（2）一般威胁：从安全日志产生到通告<2Hour、遏制影响时间<4H、经供应商确认后，准确率达99%、威胁闭环率100%；（3）重大事件：从安全日志产生到通告(MTTD)<30min、遏制影响时间<1H、经供应商确认后，准确率达99%、事件闭环率100%；（4）重大威胁：从安全日志产生到通告(MTTD )<1Hour、响应处置时间(MTTR)<1H、经供应商确认后，准确率达99%、威胁闭环率100%；（5）应急响应：供应商应当满足重大事故应启动应急响应机制，工作时间15分钟之内云端专家进行响应，非工作时间30分钟之内云端专家进行响应，2小时上门处置。  3.安全现状评估：系统与Web漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描。弱口令扫描：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。  4.脆弱性管理：针对服务资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的Web漏洞进行验证，验证漏洞的真实性及分析发生后可造成的危害；对漏洞进行分析并输出可落地的修复方案，通过工单系统跟踪修复情况。要求供应商可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到99%，提供承诺函。  5.安全问题处置：提供7\*24小时威胁分析和鉴定服务，安全告警上传至服务云端平台依托于平台的大数据分析和威胁检测能力实时监测用户网络安全状态，对平台监测到的安全威胁进行分析鉴定，自动生成服务工单，识别到真正的安全威胁。  6.服务要求：提供的服务成果展示门户；具备服务质量可视化展示，供应商能通过可视化的数据，清晰的了解供应商的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，以验证供应商所承诺的服务指标（或称为服务SLA）。  7.安全设备对接与数据采集：供应商安全托管服务云端平台应当支持对接学校网络中已部署的主要安全设备，支持实时接收安全设备检测到的安全事件信息、安全日志数据提供7\*24小时的安全托管服务。提供的安全托管服务云端平台支持对接主要安全设备的能力证明承诺函或者第三方兼容性测试报告。  8.安全合规性要求：供应商云端平台应当做好严格的安全防护，并严格按照《信息安全技术—网络安全等级保护基本要求》完成等级保护测评工作，服务云端平台至少通过等级保护三级测评。  9.服务交付物：服务期间内，提供包括但不限于以下汇报材料和内容：《项目启动会PPT》、《首次分析与处置报告》、《漏洞管理举证报告》、《漏洞清单》、《服务资产表》、《安全服务运营报告》、《应急响应报告》、《事件分析与处置报告》、《安全运营报告》、《安全通告》、《综合分析报告》、《季度汇报PPT》、《年度汇报PPT》。 |
| **五、其他要求**  **1.**本项目谈判总报价包括设备及安全托管服务等所有费用。  **2.**为保证设备的兼容和方便管理，所投设备、服务均应为同一品牌设备且能相互兼容。  **3.**产品必须是按厂家标准配置的整套全新产品，提供人员培训，培训后采购人可熟悉基本操作；  **4.**质量保证期内免费提供维修服务（含人工费、配件费、差旅费等各项费用），所更换的所有零配件全部使用原厂配件；保修期以外一律按响应文件承诺的优惠价收费，提供终身上门维修服务；  **5.**质保期内设备内置软件均免费升级，成交供应商负责所有因系统质量问题而产生的费用。  **6.**必须提供售后服务方案承诺书，售后服务方案包括但不限于：（1）定期回访维护方案；（2）售后服务技术支持（包括售后服务机构、技术人员等）；（3）维修应急预案；（4）零配件储备供应；（5）保修期外维修方案；（6）技术培训等售后服务。 |