采购包 1：

标的名称：防火墙,上网行为管理

<table>
<tr><td>序号</td><td>参数性质</td><td>技术参数与性能指标</td></tr>
<tr><td>1</td><td>★</td><td>一、采购清单
<table>
<tr><td>序号</td><td>产品名称</td><td>数量</td><td>单位</td></tr>
<tr><td>1</td><td>下一代防火墙</td><td>1</td><td>台</td></tr>
<tr><td>2</td><td>上网行为管理</td><td>1</td><td>台</td></tr>
<tr><td>3</td><td>安全托管服务</td><td>5</td><td>年</td></tr>
</table></td></tr>
<tr><td>2</td><td>★</td><td>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≥16G，IPS 吞吐量≥20G，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，系统盘≥480G SSD，数据盘≥960G SSD，接口≥4 千兆电口，≥4 千兆光口 SFP，≥8 万兆光口。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.提供应用识别和控制功能，可以对应用进行检测与控制。
4.提供 DDoS 防护功能，对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。
5.提供防病毒功能，对压缩病毒文件进行检测和拦截。
6.提供入侵攻击防御功能，深度检测并抵御各类针对漏洞发起的攻击。
7.提供僵尸主机检测功能，可识别主机的异常外联行为。
8.提供 Web 应用防御功能，支持常见 Web 攻击防护。
9.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。
10.提供 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。
11.提供威胁情报功能，威胁情报实时同步到设备，对威胁流量就近进行实时检测&拦截。
12.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。
13.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。
14.提供移动端运维功能，支持通过微信、邮件、APP 等对安全事件预警。
15.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。
16.提供 5 年原厂产品质保+软件升级，提供供应商承诺函并附作证材料。</td></tr>
<tr><td>3</td><td>★</td><td>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</td></tr>
</table>

		能≥15Gb;每秒新建连接数≥20 万;最大并发连接数≥800 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;接口≥4 千兆电口，≥4 千兆光口，≥4 万兆光口。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.提供实时接入状态功能，首页可视化分析展示用户、流量、行为的情况。 4.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。 5.提供上网认证管理功能，要求支持现网深信服上网行为管理产品用户账户及用户信息、策略及配置等的无缝、完整导入，保证信息、策略导入新设备后，无丢失、篡改、错乱等现象。提供供应商承诺函。 6.提供上网免认证功能，实现终端无感知认证上网效果；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。 7.提供流量动态调整功能，支持基于用户、用户组、时间等条件分配带宽资源，支持流控通道实时可视化。 8.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。 9.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。 10.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。 11.具备中国信息安全测评中心颁发的信息安全服务资质证书（安全开发类二级或二级以上）。提供证明材料并加盖公章。 12.提供 5 年原厂产品质保+软件升级，提供供应商承诺函并附作证材料。
4	★	**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，提供五年服务。提供 7*24H 在线服务，配置至少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。提供供应商承诺函。 2.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。 3.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%，提供供应商承诺函。 4.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。 5.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，清晰的了解供应商的服务水平。 6.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。 7.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》。
5		**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。