配置清单

序号	产品名称	技术参数	数量
1	下一代防火墙	1、★配置：网络层吞吐量≥4G，应用层吞吐量≥2G，防病毒吞吐量≥600M,IPS 吞吐量≥600M,并发连接数≥200万，HTTP 新建连接数≥6 万，接口：千兆电口≥8 个，千兆光口 SFP≥2 个； 2、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式； 3、支持 IPsec VPN 和 SSL VPN 功能； 4、▲产品具备勒索软件通信防护功能；（所投产品需提供具备 CMA 或 CNAS 认证的第三方权威机构关于“勒索软件通信防护”功能项的产品检测报告并加盖投标人公章） 5、支持 ftp 协议命令控制功能,至少包含 delete、rmdir、mkdir、rename、mget、dir、mput、get、put 等，保护对外服务不被恶意篡改； 6、▲产品支持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；（所投产品需提供具备 CMA 认证和 CNAS 认证的第三方权威机构关于“漏洞防扫描”功能项的产品检测报告并加盖投标人公章） 7、产品具备 10000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则； 8、支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御； 9、▲为保证产品的威胁防护能力，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心、软件测评中心之中任意一家检测机构出具关于“未知威胁防护”的证书和检测报告证明功能有效性； 10、▲产品支持 Cookie 攻击防护功能，可通过日志查看 Cookie 变更或篡改信息；（所投产品需提供具备 CMA 认证或 CNAS 认证的第三方权威机构关于“Cookie 攻击防护”功能项的产品检测报告并加盖投标人公章）	1 台
2	日志审计	1、★配置：主机审计许可数≥50，最大可扩展审计主机许可数≥150，可用存储量≥2TB，平均每秒处理日志数（eps）最大性能≥2500，接口：千兆电口≥6 个，万兆光口≥2 个； 2、支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件； 3、▲支持通过正则、分隔符、json、xml 的可视方式进	1 台

		行自定义规则解析，并对对解析结果字段进行新增、合并、映射；（提供产品功能截图，并加盖投标人公章） 4、支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件； 5、支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析； 6、▲为了实现对不同编码格式的解析，产品支持解码小工具按照不同的解码方式解码成不同的目标内容，编码格式包括 base64、Unicode、GBK、HEX、UTF-8 等；（提供产品功能截图，并加盖投标人公章） 7、支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN 账号异常场景分析、Windows 服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析；	
3	终端安全管理系统	1、★配置：配置 PC 授权≥1 套，服务器授权≥1 套； 2、具备高兼容性，在识别到终端存在非适配的第三方软件时可使用兼容模式进行安装，灵活调整 agent 策略，提供流畅的终端体验； 3、▲为避免终端因威胁导致终端无法正常开展业务，产品需支持跳转链接至云端安全威胁响应系统，针对已发生的威胁提供详细的威胁分析、网络行为、静态分析、分析环境和影响分析；（提供具备 CNSA 认证的第三方检测机构出具的功能检测报告复印件，报告包含首页、功能页以及尾页） 4、支持终端全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell 后门、高危漏洞及其各自影响的终端数量； 5、支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录； 6、▲支持全网风险状况展示，如未处理的（勒索）病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞及其各自影响的终端数量；（提供具备 CNSA 认证的第三方检测机构出具的功能检测报告复印件，报告包含首页、功能页以及尾页） 7、▲具备终端侧系统层、应用层行为数据采集能力，数	1 套

		据采集面覆盖 ATT&CK 技术面 163 项；（数据覆盖面需提供相关机构的证明） 8、为了防止挖矿攻击对业务的影响，本次方案需提供挖矿病毒巡检工具，通过内存、进程和启动项来检索病毒相关信息；	
4	网闸	1、★配置：设备为 2U，接口：电口≥6 个，内存≥8G，硬盘≥128G SSD，电源：冗余电源，性能配置：吞吐量≥300M，并发连接数≥5 万； 2、为了便于管理员依据实际网络状况进行相应的部署，设备支持透明、代理及路由三种工作模式； 3、▲设备系统支持多任务的组播代理功能，可穿透三层交换机网络进行部署，支持 PIM 协议；（提供产品功能截图，并加盖投标人公章） 4、支持 Oracle、SQLServer、Mysql、Sybase、DB2、Postgresql 等多种主流国外数据库的同步和国产达梦数据库、人大金仓数据库的同步； 5、▲支持 OPC 协议，支持同步、异步监测数据的传输，只需绑定固定的一个起始端口即可满足动态端口的数据传输。可控制功能代码，比如只允许读取，不能写入等；（提供产品功能截图，并加盖投标人公章） 6、支持 DCS/SCADA 生产网络与办公网络之间的 OPC 应用数据的传输。支持同步、异步监测数据的传输，只需绑定固定的一个起始端口即可满足动态端口的数据传输； 7、支持 MODBUS 协议，可按照需求控制具体功能代码，比如控制线圈、值域范围等； 8、系统提供 ping，traceroute，TCP 端口探测、抓包等工具方便管理员在配置策略或调整网络时排查问题；	1 台
5	服务器	CPU:Intel Xeon 4314(16C,185W,2.4GHz)*2 内存：32G DDR4 内存 3200*4 硬盘:8T SATA*2 阵列卡：高性能 RAID 卡 3108-2（2G) 网卡：千兆电口*4 电源:550W*2	2 台
6	温度调节设备	控制和调节机房湿度的控制设备。	1 台