|  |  |  |
| --- | --- | --- |
| 产品名称 | 数量 | 参数 |
| 防毒墙升级 | 1台（一年） | 目前在用的防毒墙设备软件续费1年 |
| 杀毒软件（PC端） | 188点（一年） | 目前在用的杀毒软件续费1年 |
| 杀毒软件（服务器端） | 1点（一年） | 目前在用的杀毒软件续费1年 |
| 防火墙模块升级 | 1个模块（一年） | 目前在用的防火墙模块续费1年 |
| 防火墙 | 1台 | ★1、标准2U机箱、冗余电源，网络接口≥10个千兆电口、6个千兆光口、2个扩展插槽，硬盘≥64G SSD；★2、最大整机吞吐量≥10Gbps（提供权威第三方机构性能检测报告扫描件并加盖原厂公章）；最大并发连接数≥800万，每秒新建连接数≥15万；本次要求开通IPS模块并含3年特征库升级服务；默认支持IPSec VPN和SSL VPN模块、无需额外付费（≥200个并发用户，提供产品功能截图）；★3、出于可靠性考虑，防火墙需要具备2个操作系统互为备份，且需要支持一个可用于恢复的操作系统，且系统切换可在web页面完成和支持通过外置按键一键切换（提供产品功能截图）；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，支持同一个地址对象中可以包含IP、IP段、IP range、排除地址等多种类型，支持将源MAC作为独立的访问控制条件，防止非法设备接入；★5、支持针对策略中的源、目的地址进行新建限制，可以针对单IP(或地址范围)进行新建控制，支持策略命中数显示，并支持通过安全策略命中数范围查询（提供产品功能截图）；6、支持基于策略的入侵检测与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的入侵防护策略，支持细粒度的自定义IPS特征功能，要求支持DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等17大类应用层协议的自定义，可以精准设置各个协议字段内容，例如字符内容、偏移、长度等细粒度的参数，支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析（提供产品功能截图）；7、支持基于策略的病毒扫描与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的病毒防护策略，支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个接口、多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境，支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性；8、支持主流ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD攻击防护，采用专业高效攻击防护算法，非采用简单的阈值进行攻击防护（提供产品功能截图）；★9、产品采用先进的木马通信通道检测技术，可快速检测出网络中的木马程序；（提供权威第三方机构出具的证明文件）★10、要求产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》(增强级），并提交公安部的检测报告正文首页；产品具备《多核多线程ASIC并行操作系统软件著作权登记证书》；提供中国信息安全测评中心出具的《信息技术产品安全测评证书》,级别：EAL4+，具有网关防病毒技术（包括病毒防范的方法和装置）；（提供证书扫描件）★11、要求生产厂商具备信息系统建设和服务能力CS4等级证书、五星级售后服务认证证书、信息系统安全集成服务资质（一级）、中国通信企业协会会员证书、国家网络与信息安全信息通报机制技术支持单位、业务连续性管理体系认证证书、 CMMI5资质；（提供证书扫描件）★12、投标时提供原厂针对本项目的授权书原件及3年免费售后服务承诺函原件；★备注：需与我院现有防火墙做双机热备,要求提供同型号产品。 |
| 网络安全技术服务 | 一年 | 1. 配合测评公司对测评发现的物理安全风险、主机安全风险、网络安全风险、应用安全风险、安全管理差距等进行安全加固和合规化处理
2. 每年协助院方进行一次应急演练，根据演练形成演练报告，对演练中存在的问题进行总结
3. 服务期内为甲方提供7\*24小时安全产品运维服务。如甲方遇到网络安全问题，乙方须在1小时内到达现场进行应急处理。
4. 每季度开展一次网络安全巡检，针对我院网络及安全设备运行状态进行全面检查，并提供巡检报告和安全建议报告。
 |