**附件1-莆田开放大学网管中心网络安全项目升级等服务项目参数要求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务项** | **参数** | **单价**  **（元）** | **合计**  **（元）** | **备注** |
| 1 | 安全网关（含防火墙、入侵防御、防病毒模块） | 1.标准1U设备，支持双电源；标准配置不低于10个千兆电口及2个光口，1个接口扩展槽位；网络吞吐≥4G，应用吞吐≥600M，最大并发连接数≥30万。含下一代防火墙访问控制、入侵防御、网络防病毒、URL分类管理模块。  2.支持恶意域名过滤，实现对C&C进行阻断；支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护；支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。  3.支持用户流量配额管理；支持基于用户/用户组、应用、URL、ip地址、接口、安全域、VLAN、服务/服务组等对象进行带宽限制；支持每IP，每用户的最大连接数限制，防护服务器；策略路由支持的匹配条件不少于源IP/目的IP，服务类型，应用类型，用户(组)，入接口，DSCP优先级。安全大脑防护版可为客户提供下一代防火墙、防病毒、集中统一运维、定期安全报告等更丰富功能，提供防火墙访问控制、入侵防御、网络防病毒、 URL 分类管理模块，提供三年升级维保服务，通过云端提供安全日志数据的存储，包括IPS日志、AV日志等；提供丰富的安全事件可视化的服务门户，包括移动端服务小程序，提供安全概览、安全报告下载、高危事件、失陷告警等通知提醒；对于不具备维护能力和安全事件处理能力的客户，可以将设备维护、安全事件处理等事宜提交给安全专家进行代维操作，安全专家定期提供报告；支持用户根据需要自定义安全报告模板，支持安全报告按天/周/月和自定义时间段通过邮件、服务号发送用户，报告内容包含网络安全概览、攻击数、已拦截数、攻击趋势、安全事件、失陷主机、防病毒/IPS/URL趋势、设备概况等。设备提供三年维保； |  |  |  |
| 2 | 合规管理平台（含日志审计和堡垒机模块） | 合规系统：CPU：8核、内存：16G、硬盘：128G；网络安全合规管理平台是面向客户网络安全合规领域建设的解决方案级平台，支撑网络安全等级保护业务工作开展、数据监管与分析、安全状况评价、态势呈现及日常工作管理支撑的等级保护综合管理平台。旨在为客户解决在安全制度落地、等级保护测评、网络安全监督检查等方面的问题，产品设计涵盖了合规检查、定级备案、等保自查、安全制度管理、资产管理和漏洞管理等多项功能，有效协助客户建立更规范化的网络安全合规管理体系（支持本地或云化部署，提供日志审计、堡垒机功能，）；日志审计功能：提供统一日志收集、呈现、分析的安全日志管理能力，提供5个日志源授权；运维审计功能：提供集账号管理、身份认证、单点登录、资源授权、访问控制和操作审计为一体的运维安全审计服务，提供20个资产授权；设备提供三年维保； |  |  |  |
| 3 | 等保咨询 | 对莆田市开放大学系统开展差距分析、基线核查等工作，出具差距分析报告。协助莆田市开放大学对营收系统的安全加固。按照上级管理部门要求和等级保护要求协助莆田市开放大学进行管理制度梳理。 |  |  |  |
| 4 | 二级等保测评 | 对莆田市开放大学系统按照等级保护要求展开测评，出具测评报告。 |  |  |  |
| 合计 | | | |  |  |