**梧州市中医医院信息安全维保服务项目**

**技术参数附件**

1. 项目概况：

随着医疗行业数字化转型的深入推进，医院信息系统等核心业务平台的普及，医疗数据已成为医院运营与患者服务的核心资产。然而，医疗行业面临的网络安全威胁日益严峻，勒索软件攻击、数据泄露、系统瘫痪等事件频发，严重威胁患者隐私安全、诊疗秩序及医院声誉。

目前医院的网络安全设备已过保了6-7年，网络安全存在重大的安全隐患，为保障业务连续性和数据安全的必要举措。通过持续性的安全监测、漏洞修复、应急响应及技术升级等维保服务，可帮助医院动态应对新型威胁，加固防御体系，同时满足监管合规要求，降低运营风险。

# 需求参数表响应表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 设备大类 | 设备型号 | 产品描述 | 数量 | 响应内容 | 响应情况 |
| 1 | 上网行为管理 | 深信服AC-1700-ZR | 设备吞吐量 300Mbps;支持用户数 1200，并发会话数 300,000;网络接口具备6 个千兆电口 | 1项 |  |  |
| 2 | VPN | 深信服VPN-1000-B1120D | 吞吐量:500Mbps  防火墙代理理论并发会话数目:600000  SSL最大加密流量:250Mbps  SSL理论并发用户数:1000个  IPSec加密最大流量:110Mbps  内存:2GB  4电4光 | 1项 |  |  |
| 3 | 防火墙 | 360网神  NSG7000-TG10 | 网络处理能力>14G并发连接≥300 万，每秒新建连接 22 万/秒，双电源，，6个10/100/1000M 自适应电2，8个10/100/1000BASE-T(100m，RJ45):前面板SFP插 槽 :配置液晶器示屏升级服务， | 1项 |  |  |
| 4 | 防火墙 | 华为Secoway USG5530s | 性能指标:  防火墙吞吐量:吞吐量>10Gbps;  最大并发连接数>300万:  每秒新建连接数>10万:  IPSec VPN吞吐>7Gbps:  IPSEC VPN隧道数≥15000，SSL VPN隧道数>500.配置8个千兆光口、4个千兆电口、4个千兆ombo 端口:支持接口扩展，支持万兆接口，扩展插槽 | 1项 |  |  |
| 5 | 防火墙 | 华为USG6101 | 并发连接数 200000，吞吐量 600Mbps，网络端口 4GE，VPN支持 支持，入侵检测 支持入侵防护。 | 1项 |  |  |
| 6 | 防火墙 | H3C SecPath F1000-AI-80 | 1. 采用非X86 64位多核高性能处理器和高速存储器，高度≥1U,Flash≥8G,内存≥16G  2.应用层吞吐量≥6Gbps，网络层吞吐量≥20Gbps最大并发连接数≥1000万，每秒新建连接数≥15万  3.提供≥2个MGMT接口，≥14个千兆电口，≥8个千兆光口，≥8个万兆光口，≥2个USB接口，提供以上接口后剩余扩展槽位≥4个，≥2个硬盘扩展槽,,实配冗余双交流电源 | 1项 |  |  |
| 7 | 防火墙 | H3C SecPath F1000-AI-90 | 整机吞吐量>25Gbps，并发连接数>1000万，新建连  接数>24万;  配置>14个千兆电口，>8个千兆光口，>8个万兆光  口;满足上述接口后，支持>4接口扩展模块;  配置>3年IPS、AV防病毒特征库授权;配置>1块  500GB HDD 硬盘模块，可支持双硬盘;  配置25套SSL VPN用户并发授权 | 1项 |  |  |
| 8 | 防火墙 | 锐捷RG-RSR10 | 传输速率：10/100Mbps 3GE(2GE电+1GE光) | 1项 |  |  |
| 9 | 信息安全审计平台 | 天锐锋  OSAG-3000R | 信息安全审计平台 | 1项 |  |  |
| 10 | 网闸 | 伟思信安ViGap200AE | 伟思信安ViGap200AE | 1项 |  |  |
| 11 | 安全隔离与信息交互系统 | 安盟信息嵌入式软件 | 安盟信息嵌入式软件 | 1项 |  |  |
| 12 | 杀毒软件授权服务器端 |  | 系统漏洞扫描、补丁修复管理、终端基线检查、资产盘点、资产主动发现、轻补丁漏洞免疫、弱密码检测  件实时监控、勒索诱饵防护、静态文件AI引擎、动态勒索行为AI引擎、勒索攻击对抗、无文件攻击防护、RDP二次认证、SSH二次认证、可信进程防护、关键目录加固、Webshell防护、无文件攻击防护  恶意文件检测、暴力破解检测、网端联动杀毒  终端行为数据采集、（单品）高级威胁行为检测（IOA）、（单品）攻击进程链可视化展示（单品）威胁狩猎、应用安全防护（RASP）、内存马检测等  文件急速隔离，终端一键隔离，感染文件修复，病毒处置响应，网端深度联动（SIP、AF、AC、XDR），全网威胁定位、主机流量采集； 简便运维：外设管控、违规外联检测、广告弹窗（高级版），授权≥20个 | 1项 |  |  |
| 13 | 杀毒软件授权PC端 |  | 系统漏洞扫描，补丁修复管理、终端基线检查，资产盘点，资产主动发现，轻补丁漏洞免疫；文件实时监控、勒索诱饵防护、静态文件AI引擎、动态勒索行为AI引擎、勒索攻击对抗、无文件攻击防护、RDP二次认证、可信进程防护、关键目录加固  恶意文件检测、暴力破解检测、网端联动杀毒（SIP、AC、AF、XDR）终端行为数据采集、（单品）高级威胁行为检测（IOA）、（单品）攻击进程链可视化展示（单品）威胁狩猎、内存马检测等，文件急速隔离、终端一键隔离、感染文件修复、病毒处置响应、域名隔离、进程阻断、网端深度联动（与SIP、AC、AF、XDR）、全网威胁定位，外设管控、违规外联检测、远程桌面、广告弹窗拦截（高级版）、屏幕水印、应用管控。授权≥500个 | 1项 |  |  |

**梧州市中医医院信息安全维保服务价格表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目内容** | **数量** | **价格** |
| **1** | 一、服务清单内容详见需求参数表响应表  二、服务细则：（1）原厂远程技术支持服务  提供7×24小时电话技术咨询支持（包含电话、邮件、远程桌面支持）；  （2）快速备件先行更换服务  经过原厂工程师定位问题为硬件故障需更换硬件后，要求原厂备件先到现场进行更换，再将坏件寄回，对所维保设备所产生的维修费、配件费、日常检查保养费由成交服务商承担；  （3）软件版本升级服务  维保期间，提供维保网络安全设备的免费软件升级服务，如软件补丁（BUG Fixes）、更新软件（Updates），进行软件版本的评估和风险分析，并保证升级后的系统能够稳定的运行；  （4）在线支持服务  维保期间，供应商需提供原厂7\*24小时在线支持服务，包含但不限于微信、QQ、原厂论坛灯；  （5）巡检服务  要求在服务内，定期提供原厂网络安全设备巡检服务，通过原厂专业的网络巡检工具针对维保设备进行巡检，并在巡检后一周内提交巡检报告，如发现隐患，需协调人员进行处理，排除隐患；提供每年不少于4次现场巡检服务，并提供巡检服务总结报告。  （6）问题咨询  维保期间，业主可能不定期向中标服务商进行问题咨询，在中标服务商无法解答的情况下，需协调原厂工程师解决业主咨询的问题；  （7）为保证维保服务质量，供应商必须保证提供的维保产品配件是正规渠道的原厂产品配件，并且与采购人原部件品牌、型号相同，如发生相关纠纷，由竞标人解决并承担全部责任，与采购人无关，为确保中标商可提供原厂商备品备件，竞标人竞标时必须提供产品原厂商提供的《原厂服务承诺书》，否则竞标无效。  （8）在中标服务商中标30天内，必须提供原厂授权许可证，用于项目验收。 | 1年 |  |