附件1

信息化建设项目技术参数表

**需求科室：某医院 填表时间：2024年3月14日**

|  |  |
| --- | --- |
| 项目名称 | 医院网络安全建设 |
| 预算金额 |  115万元 | 数量/计量单位 | 1项 |
| 经费来源 | 单位自筹 | 是否进口 | 否 |
| 联系人 | 张老师 | 办公电话/手机 | 734071/13571907826 |
| 需求参数提报人 |  | 参数审核人 |  |
| **设备功能要求** |
| 项目以保障医院外联区应用安全及防止病毒侵入局域网为目的，包括：1.建设相应的网络安全实现在外网出口边界进行隔离和访问控制，保护内部网络；2.实现对入侵事件的监控、阻断，保护整体网络各个安全域免受外网常见恶意攻击；3.主动对全网进行漏洞扫描，及时发现局域网中存在的信息安全问题；4.以及对第三方维护人员进行操作时的监控策略。 |
| **软、硬件配置清单** |
| 序号 | 名称 | 数量 | 单位 |
| 1 | WEB应用防火墙 | 1 | 台 |
| 2 | 万兆网络防火墙 | 1 | 台 |
| 3 | 万兆网络入侵检测设备 | 1 | 台 |
| 4 | 堡垒机 | 1 | 台 |
| 5 | 安全隔离网闸 | 1 | 台 |
| 6 | 机架式漏洞扫描设备 | 1 | 台 |
| **技术要求** |
| 序号 | 指标名称 | 技术参数 |
| 医院网络安全建设 | 1 | WEB应用防火墙 | ★1.1 | USB接口：≥2 个；管理口：≥2 个；千兆电口：≥8个；千兆光口：≥ 4个；万兆光口≥ 2个；扩展槽：≥2个；硬盘：≥4T；电源：双冗余电源；吞吐量：≥8Gbps；请求速率：≥6万/s；最大并发连接数：≥280万；光模块：满配单模光模块;含三年特征库升级服务。 |
| 1.2 | 产品系统支持国产化操作系统。 |
| 1.3 | 支持透明流、透明代理、反向代理；支持链路聚合(Channel)部署，提高链路带宽；支持802.1Q协议，在Trunk线路上部署并提供防护。 |
| 1.4 | 支持IPv4和IPv6双协议栈流量过滤防护；支持HTTP2协议；支持代理模式下对HTTP、HTTPS协议的单个连接允许请求数、长连接有效时间、最大空闲连接数和上传文件最大值等数据进行自定义配置。 |
| 1.5 | 支持黑白名单策略，包括IP及URL黑白名单；支持IP访问控制，可根据源目的IP，端口，协议等进行访问控制处理，并可自定义访问过期时长；支持地域访问控制功能，支持根据国家、地区、城市等元素进行地域访问控制，并可自定义访问过期时长。 |
| 1.6 | 支持Web攻击防护功能，包括命令注入攻击，组件漏洞防护、Web扫描防护、XPATH注入防护、XML注入防护、SSI注入防护、JOSN注入防护、LDAP注入防护、webshell防护；支持Web业务控制防御功能，提供针对爬虫、黑链、盗链以及内网代理的防护功能；支持敏感词检测及过滤，自带敏感词库并可进行自定义；支持Web业务加固防御功能，提供弱密码检测、CGI安全、跨站请求伪造等防御功能；支持人机识别功能，可针对自动化攻击进行有效防护；支持会话安全防护、Cookie加固、Cookie加密、会话固定等属性设置。 |
| 医院网络安全建设 | 1 | WEB应用防火墙 | 1.7 | 支持检测并清洗的攻击类型：IP攻击，TCP攻击，UDP攻击，ICMP攻击，DNS攻击，HTTP攻击等20多种DDoS攻击类型。 |
| 1.8 | 支持利用威胁情报建立IP风险画像，提供信誉数据包括不限于DDos攻击、安全漏扫、垃圾邮件、Web攻击、扫描源等。 |
| 2 | 万兆网络入侵检测设备 | ★2.1 | 电源：双冗余电源；吞吐量：≥8Gbps；千兆电口：≥8个；千兆光口：≥ 8个；万兆光口≥ 2个；光模块：满配单模光模块;含三年特征库升级服务。 |
| 2.2 | UNIS T5000-CN40 |
| 2.3 | NIDSNX5-HD 6000D-ZF |
| 2.4 | IDS2000-GM-G |
| 2.5 | NT10000-FT-J |
| 2.6 | NT-NIDS3600FT-C-HS |
| ★注：以上设备产品，要求设备厂家将设备端口授权全开放，插槽及光模块配齐，可实现与其它硬件设备互联互通，无需再增加接口卡。设备不做唯一授权指定，不做核心参数约定。 |
| 3 | 万兆网络防火墙 | ★3.1 | 电源：双冗余电源；吞吐量：≥8Gbps；千兆电口：≥8个；千兆光口：≥ 8个；万兆光口≥ 2个；光模块：满配单模光模块;含三年特征库升级服务。 |
| 3.2 | UNIS F5000-CN40 |
| 3.3 | NSFW-12000 |
| 3.4 | DPtech FW1000-TC-G |
| 医院网络安全建设 | 3 | 万兆网络防火墙 | 3.5 | AM3300-3680-FF |
| 3.6 | RZ7000 |
| ★注：以上设备产品，要求设备厂家将设备端口授权全开放，插槽及光模块配齐，可实现与其它硬件设备互联互通，无需再增加接口卡。设备不做唯一授权指定，不做核心参数约定。 |
| 4 | 堡垒机 | ★4.1 | 千兆电口：≥6个；千兆光口：≥4个；console口：≥1个；USB口≥2个；扩展槽≥2个；硬盘≥4T；光模块：满配单模光模块;本次配置：≥300个主机/设备许可，用户数不限制。 |
| 4.2 | 产品系统支持国产化操作系统。 |
| 4.3 | 至少支持系统管理员、安全审计员、运维管理员等角色，同时也可按需分配角色权限，权限间相互制约。 |
| 4.4 | 支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长TOP10、今日告警总数、今日运维指令等信息，方便管理员实时查看系统运行情况掌握资产会话连接情况。 |
| 4.5 | 自动对Windows、Linux等设备进行账号改密，支持手动或定期任务修改密码，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成。 |
| 4.6 | 支持图形化查看账号改密历史记录，查询结果以图表按照时间倒序自上而下展示，每个节点详细记录改密信息及结果；支持每个改密节点可以定位、查看和下载密码信封。 |
| 4.7 | 支持对运维时间、运维地址、运维操作指令、操作行为的限定，触发策略后进行告警、再审、阻断等。 |
| 4.8 | 支持会话请求远程协助，且协同会话保持实时同步。  |
| 4.9 | 支持各种自定义客户端工具，支持通过动作流配置提供广泛的应用接入支持，在不做二次开发的情况下，可灵活扩展且实现帐号口令的代填。 |
| 医院网络安全建设 | 5 | 安全隔离网闸 | ★5.1 | 内端机接口配置：千兆电口：≥6个；千兆光口：≥4个；外端机接口配置：千兆电口：≥6个；千兆光口：≥4个；网络吞吐量：≥5.5Gbps；电源：双冗余电源；光模块：满配单模光模块;并发连接数：≥100万。 |
| 5.2 | 产品系统支持国产化操作系统。 |
| 5.3 | 功能包含安全浏览模块、文件传输模块、文件同步模块、邮件访问模块、数据库访问模块、数据库同步模块、防病毒模块。 |
| 5.4 | 系统应采用“2+1”系统结构，内外端机为TCP/IP网络协议的终点，阻断TCP/IP协议的直接贯通。 |
| 5.5 | 支持http消息头、消息体，支持上下行方向，支持命令及关键字的管控，支持允许、阻断、告警三种处理方式。 |
| 5.6 | 支持网闸同侧数据库之间的数据同步。 |
| 5.7 | 支持数据库同步信息统计，包括每个任务的开始时间、同步成功数、同步失败数、同步忽略数，并能够以图表的方式进行实时可视化展现。 |
| 5.8 | 支持TCP、UDP业务数据统计，可按照秒、分钟展示发送速率、接受速率、连接数。 |
| 6 | 机架式漏洞扫描设备 | ★6.1 | 电源：双冗余电源；千兆电口：≥4个；千兆光口：≥4个；光模块：满配单模光模块;授权数量：≥1000个主机；含三年特征库升级服务。 |
| 6.2 | RSASNX3-HF A-ZF |
| 6.3 | TJCS-GYD-FTS2300A-JL |
| 6.4 | S3300-VSS20P |
| ★注：以上设备产品，要求设备厂家将设备端口授权全开放，插槽及光模块配齐，可实现与其它硬件设备互联互通，无需再增加接口卡。设备不做唯一授权指定，不做核心参数约定。 |
| **经济要求** |
| 序号 | 指标名称 | 详细要求 |
| 1 | 项目周期 | 1.1 | 总体项目周期：项目签署合同后，3个月内完成，提供整体进度明确、合理的项目实施周期和进度表。 |
| 1.2 | 1个月内完成项目建设方案的设计。 |
| 1.3 | 2个月内完成硬件安装、设备连接、策略配置及培训。 |
| 1.4 | 3个月内完成系统验收以及整改。 |
| 2 | 验收条件 | 2.1 | 各项功能满足招标要求 |
| 2.2 | 按实际需求进行培训，产品安装调试后对相关人员统一进行免费培训≥3次。 |
| 3 | 付款条件 | 3.1 | 项目验收完毕支付合同总额的95%，维保期满支付剩余的5%。 |
| 4 | 拓展及迁移 | 4.1 | 系统支持异地迁移及多院区扩展。 |
| 5 | 免费维保期 | 5.1 | 硬件提供三年免费原厂质保、迁移、优化和故障处理服务，时间自项目验收合格之日起算。 |
| 5.2 | 提供投标产品生产厂家售后服务承诺函。 |
| 6 | 方案维护 | 6.1 | 根据医院需求，应用过程中的实际情况进行个性化定制。 |
| 7 | 本地化服务 | 7.1 | 投标方需在西安本地有服务团队，附本地化相关证明资料（不限于租房合同等）。 |
| 7.2 | 系统上线运行时，需提供2个月及2人的实施及驻场指导，直至系统正常运行使用。实施及驻场指导人员:应具备五年以上网络安全类工作经验，具备高级网络工程师、PMP及CISP-PTS\CZTP等网络安全相关资质或认证。 |
| 7.3 | 项目验收后，需提供12个月及1人的驻场指导。驻场人员:应具备三年以上网络安全类工作经验，具备网络工程师中级及CISP\CCSC等网络安全相关资质或认证。 |
| 8 | 免费维保期内服务要求 | 8.1 | 免费维保期内乙方负责提供7x24小时咨询、技术支持；系统出现故障后，自报障时起算，响应时间≤30分钟，到达现场时间≤2小时，并分析故障原因，制定问题的解决方案。 |
| 8.2 | 免费维保期内，系统免费升级系统版本与医院设备的集成融合服务。 |
| 8.3 | 免费维保期内提供每年例行巡检≥4次，提供书面巡检资料。 |
| 8.4 | 免费维保期内提供每年网络安全培训≥4次。并提供2人次CISP认证考试培训。 |
| 8.5 | 系统需要更换位置时，乙方需及时提供迁移服务。 |
| 8.6 | 免费维保期结束后的售后服务费用另行协商，上限费用<成交价的10%。 |
| 8.7 | 在必要情况下，需配合第三方厂商完成相应工作。 |
| 9 | 案例要求 | ＃9.1 | 提供近三年内三甲医院网络安全类项目实施案例，实施案例≥1家，提供合同证明材料。 |
| **实施建议** |
| 序号 | 指标名称 | 详细要求 |
| 1 | 采购方式 | 1.1 | 公开招标。 |
| 2 | 实施要求 | 2.1 | 投标人要做好硬件部署方案，保证安装设备过程中不对甲方业务实际运行进行影响，同时做好应急预案。 |
| 3 | 合同履约要求 | 3.1 | 订立书面合同书，履行备案手续的程序组织实施。于中标通知书发出之日起30日内与中标供应商签订合同书。 |
| 4 | 保密要求 | 4.1 | 遵守部队管理有关规定要求，确保数据安全可控，保障医院运行管理相关的保密信息，签订保密协议，严禁将医院数据和信息外泄、提供给第三方。严禁违规外联。 |