**柳州市工人医院信息安全设备采购项目技术参数**

1. **项目背景**

《中华人民共和国网络安全法》于2017年6月1日正式实施，网络安全有了专门的法律规定；国家卫生健康委员会规划与信息司、国家卫生健康委员会统计信息中心发布《全国医院信息化建设标准与规范》于2018年4月试行，提出了医院信息化建设的标准与规范，其中涉及网络安全建设的要求。与此同时，内外网边界消失。随着各种新兴IT技术的发展与落地，新的攻击形态层出不穷，攻击变得更复杂更隐蔽，攻击手段更加高明，静态防御失效，防御体系容易被绕过，无法对风险进行持续检测；同时随着电子病历、网上诊疗等互联网业务快速发展，重要业务服务器需要对外开放，安全形势将更加严峻。

**二、项目建设内容及要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **数量** | **单位** | **技术参数及性能配置要求** |
| 1 | 云waf | 1 | 套 | 1. 产品采用云端部署模式，基于SaaS形式提供服务；
2. 一级域名防护数量 ≥ 2个；
3. 二级域名防护数量 ≥ 40个；
4. 业务防护带宽峰值 ≥ 100Mbps；
5. 业务访问请求峰值 ≥ 2000QPS；
6. 业务防护日志保存时间 ≥ 180天；
7. 支持用户多角色划分功能，如系统管理员、普通管理员、审计管理员等，各用户角色细粒度的权限管理
8. 支持用户登录采用多种认证方式，可通过本地认证、短信验证码认证、LDAP认证、RADIUS认证、USBkey认证、AD域认证、手机动态口令认证、手机APP、微信小程序中的两种以上认证方式；
9. 支持CNAME接入形式，网站域名以CNAME接入的方式添加到云waf；
10. 支持前台手动添加站点，并可对站点信息进行灵活删改；
11. 支持前台手动上传证书，站点信息引用证书配置可灵活删改；
12. 支持域名状态监控功能，实时监控网站运行状态；
13. 支持黑白名单功能，可基于国家、国内省份等对IP地址进行封禁；
14. 支持回源功能，终端流量不经过云waf，直接转发源站；
15. 支持直通功能，终端流量不经过云waf任何防护策略识别、拦截，直接进行转发；
16. 支持关站功能，终端流量经过云waf时进行拦截，不进行转发；
17. 支持攻击防护功能，有效防御SQL注入、代码注入、跨站点脚本攻击、命令注入攻击、文件包含攻击、CSRF攻击等；
18. 支持网页防篡改功能，可通过备份源站、镜像源站、缓存页面、定时循环扫描技术等多种方式；
19. 支持防爬虫功能，可通过Robot检测、检查浏览器合法性、内容安全监测等多种方式；
20. 支持虚拟化补丁功能，无需更改源站情况下保护漏洞不被攻击者挖掘和利用；
21. 支持防泄露功能，可通过数据替换策略、脱敏和告警措施、拦截指定的HTTP状态码、限制URL未授权访问、限制越权查看漏洞等多种方式实行；
22. 支持CC防护功能，可通过流量过滤、黑白名单机制、验证码验证、负载均衡、DDoS防护等多种方式；
23. 支持攻击告警功能，可通过邮件告警、短信告警、小程序告警、手机APP等多种方式；
24. 支持实时监控和报告，提供实时的监控和日志记录功能，能够对网络流量和攻击事件进行实时分析和报告，为安全管理提供及时的情报和决策支持。
 |
| 2 | 蜜罐 | 1 | 套 | 1. 提供软硬件一体机产品形态，硬件采用标准机架式设备，提供双冗余电源；
2. 内存 ≥ 64GB；
3. 存储空间 ≥ 2TB；
4. 千兆电口 ≥ 4个；
5. 系统伪装高交互节点数量 ≥ 5个；
6. 系统伪装低交互节点数量 ≥ 20个；
7. 业务防护日志保存时间 ≥180天；
8. 支持设备日志按照标准SYSLOG格式或SNMP协议输出到第三方日志服务器；
9. 支持用户多角色划分功能，如系统管理员、普通管理员、审计管理员等，各用户角色细粒度的权限管理；
10. 支持用户登录采用多种认证方式，可通过本地认证、短信验证码认证、LDAP认证、RADIUS认证、USBkey认证、AD域认证、手机动态口令认证、手机APP、微信小程序中的两种以上认证方式；
11. 支持伪装流量转发功能，真实业务系统内部署流量转发服务,将伪装的业务端口流量引流到相应的伪装系统；
12. 支持多种操作系统伪装功能，包含Windows、Linux、MacOS等；
13. 支持多种Web服务伪装，包含IIS、Apache、Nginx等；
14. 支持多种数据库伪装，包含SQLServer、MySQL、Oracle等;
15. 支持多种常用服务，包含FTP、RDP、SSH、SAMBA、TELNET等；
16. 支持自定义服务伪装，可通过服务搭建、业务克隆、网站爬取等多种方式；
17. 支持流量探针功能，检测未使用的端口和IP地址使用情况，对特定业务流量进行重定向；
18. 支持蜜饵投放功能，对系统伪装节点的指定目标路径下发蜜饵文件；
19. 支持文档型蜜饵功能，诱导攻击者打开或下载嵌套宏代码的各类.txt、.doc、.xls、.conf、.xml等后缀的文件；
20. 支持可执行文件型蜜饵功能，诱导攻击者打开或下载嵌套特定代码的各类.exe、.apk、.msi等后缀的文件；
21. 支持压缩包型蜜饵功能，诱导攻击者打开或下载嵌套特定代码的各类.zip、.rar、.7z等后缀的文件；
22. 支持邮件型蜜饵功能，诱导攻击者打开邮件或者下载嵌套特定代码的各类附件；
23. 支持攻击链聚合功能，集中展示各攻击项所处的状态，包括侦察渗透、武器构建、载荷投递、漏洞利用、安装植入、命令控制、目标达成等；
24. 支持攻击者肖像功能，集中展示攻击者基础信息、各类指纹信息、社交账号等；
25. 支持攻击溯源功能，集中展示攻击源IP、攻击类型、持续时间、被攻击的系统伪装节点信息等，并支持攻击报文PCAP包下载；
26. 支持系统反制功能，可获取攻击者常用社交账号；
27. 支持安全报告功能，报告集中展示威胁总览，攻击风险统计，攻击类型统计，攻击源统计等。
 |

# 三、项目实施要求

1. 驻场、实施工期要求：合同签订后，**7个工作日内**硬件设备及项目实施人员必须进场，**30个工作日内**完成设备调试及上线。
2. 人员要求：项目实施人员需有**2年以上**同等项目实施经验，项目实施期间，驻场实施人员**不得少于1名**；如需更换驻场实施人员，需提交书面申请，经院方同意才可更换。投标公司实施人员、计划、方案等须经我院方认可才可实施。
3. 除非合同另有规定，竞标文件报价表中有标价的单价和总额价均已包括了实施和完成本项目所需的劳务、材料及其安装损耗、机械、质检（自检）、运输、安装、调试、试运行、缺陷修复、管理、保险、税费、利润等费用，以及合同明示所有责任、义务和一切风险。

# 四、售后服务及其他要求

1. 所有产品要求提供**三年**的免费质保服务，含软硬件维护和系统软件升级、技术支持服务，请详细说明售后服务的内容。
2. 安装调试要求：免费送货上门、安装调试、提供完善的设备使用中文操作手册及图纸、网络详细拓扑图、设备配置及互联记录。
3. 原厂技术人员免费提供售后服务，含电话支持、现场响应、远程操作、网上客服中心等多种方式服务，应做到**7×24小时**全天候电话或微信等常用联系方式响应；在接到设备故障通知后，原厂技术人员应在**30分钟内**响应，远程技术支持无法解决的，**2小时内**需到达现场处理，如现场仍不能解决问题，**24小时内**免费提供同档次或更高档次的备用设备解决问题。
4. 提供**原厂技术人员**定期回访服务，定期通过电话或其他方式回访用户，了解产品使用情况及网络安全情况，须在**每季度第一个月**进行**一次**现场巡检，并形成书面巡检服务报告，加盖有效公章并反馈给我院（要求提供巡检报告模板，内容涉及此项目相关设备的运行情况及现场巡检照片）。

# 五、违约责任

1. 投标方所提供的货物规格、技术标准、材料等质量不合格的，应及时更换，更换不及时的按逾期交货处罚；因质量问题我院不同意接收，投标方应向我院支付违约货款额**5%**违约金并赔偿我院经济损失。
2. 投标方提供的货物如侵犯了第三方合法权益而引发的任何纠纷或诉讼，均由投标方负责交涉并承担全部责任。
3. 因包装、运输引起的货物损坏，按质量不合格处理。
4. 投标方逾期交货的，每天向对方偿付违约货款额**3‰**违约金，但违约金累计不得超过违约货款额**5%** ，超过**30天**对方有权解除合同，违约方承担因此给对方造成的经济损失。
5. 巡检要求：每缺少1次现场巡检记录，投标方应向我院支付违约金**5000元**。
6. 不能按本章第4点要求中按时提供设备备件的，按如下标准支付违约金：
	1. 故障上报**24小时至30小时**内不能免费提供同档次或更高档次的备用设备解决问题，**每超时一小时**支付**500元**违约金；
	2. 故障上报**30小时至35小时**内不能免费提供同档次或更高档次的备用设备解决问题，**每超时一小时**支付**1000元**违约金；
	3. 故障上报**35小时后**不能免费提供同档次或更高档次的备用设备解决问题，**每超时一小时**支付**1500元**违约金。
7. 投标方未按本技术要求和响应文件中规定的其他服务承诺提供售后服务的，每次投标方应按合同合计金额的**5%** 向我院支付违约金。
8. 因投标方设备漏洞或功能缺陷，造成敏感数据泄露，对我院造成经济或名誉损失的，投标方应向医院支付人民币**10万元/次**作为损失赔偿。
9. 厂商驻场工程师人员变更必须得到医院书面同意，否则视为乙方违约，甲方有权按5000元/人/次从合同总款中扣除。

# 六、保密、廉洁协议

1. 双方保证对从另一方取得且无法自公开渠道获得的商业秘密(技术信息、经营信息及其他商业秘密)予以保密。未经该商业秘密的提供方同意，一方不得向任何第三方泄露该商业秘密的全部或部分内容，但法律、法规另有规定或双方另有约定的除外。任何一方违反保密义务的，应承担相应的违约责任并赔偿由此造成的损失。
2. 双方不得以任何方式向第三方泄露本项目的软件技术、设计方案以及功能配置等内容。
3. 不以任何方式向第三方泄露在本协议开发实施过程中获取的经济、技术、数据以及双方其他非公开的信息。
4. 不从事商业贿赂行为，遵守廉洁协议或相关规定。甲方发现乙方有违反廉洁协议或相关规定采用不正当手段进行不正当竞争行为的，或被有关部门生效文书认定有行贿或者受贿行为的，甲方有权解除该业务合同，由此给甲方造成的损失以及发生的一切费用均由乙方承担，甲方有权对乙方实施商业贿赂不良记录，列入“黑名单”，并三年内取消其业务往来资格。
5. 保密期限自合同生效之日起永久有效，如乙方需解除保密协议需向甲方提出书面申请，双方协商同意签字确认后方可解除。

# 七、报价

1. 竞标文件需提供商务、技术、硬件偏离表。
2. 竞标文件报价表价格包含系统软硬件费用、产品安装、调试实施、培训费用、产品升级费用，以及明示所有责任、义务和一切风险。
3. 竞标文件需提供质保期后维保方案及费用。
4. 竞标文件需提供质保期后授权扩容方案及费用。
5. 竞标文件需提供系统详细图文介绍。系统实施验收参照本技术文档及竞标文件提供的图文介绍为依据。

# 八、付款方式

1. 合同完成签订，投标方应提供满足标的的产品并且全部货物送达我院指定地点完成安装和调试，双方签署试运行报告后，支付**30%**的合同款。
2. 所有产品安装、调试完成并上线稳定运行**3个月后**启动验收，验收合格后支付合同款项的60%。
3. 验收**满一年后**，支付**10%**的合同款。