玄武盾云 WAF（网站）维护项目需求书

项目名称：玄武盾云 WAF（网站）维护项目

1　项目预算：20000 元

2　投标人资格要求：

（1）必须是在中华人民共和国境内注册的具有独立承担民事责任能力的法人或其它组织，提交有效的营业执照副本复印件。营业执照经营范围应与本项目相关；

（2）具有项目服务的能力，保证能及时对服务项目提供实施、售后等服务；

（3）非广东省内注册的投标人应在广东省内设有经有效工商注册的分支机构，具有营业场所和固定的售后服务队伍，提供有效的营业执照及社保证明材料；

（4）在近三年的商业活动中无违法、违规、违纪、违约行为；本项目不接受联合体报名，不允许分包、转包。

3　项目总体概要

3.1　货物一览表

序号	项目	说明	单位	数量	备注
1	云 WAF 防护	详见以下指标要求	项	1	一年

3.2　详细技术参数要求

说明：带“▲”号条款为评审时的重要技术参数，不作为投标无效条款。如中标后缺少整体架构所必需部件，均由中标方免费提供。

3.2.1 云 WAF 防护 1 套

序号	指标项	指标要求
1	整体要求	▲支持集群化和高可用部署架构，全国范围至少具备 90 个云防护节点。（提供服务平台界面截图并加盖公章，提供现场演示）
2		▲支持通过一体化平台提供云防护和云监测服务，以便在用户需要时将防护站点加入监测系统进行安全自检。（提供服务平台界面截图提供现场演示）
3		支持为每个用户单独创建平台登录账号，用于查看网站的安全防护状况。
4	服务方式	▲系统基于云化 SaaS 架构，无需消耗虚拟机资源或本地物理资源，通过云端服务平台完成站点管理，为用户提供云防护服务。（提供服务平台界面截图并提供现场演示）
5	安全概览	支持通过统一界面展示网站访问次数、拦截攻击次数、网站出入总流量、疑似攻击元 IP 数量，并以时间维度展示攻击与访问趋势图。（提供服务平台界面截图并提供现场演示）
6	站点管理	支持通过服务平台以手工导入和批量导入的方式完成防护站点的添加申请，支持添加 HTTP 和 HTTPS 类型的站点，并支持自主上传网站公钥或和私钥。（提供服务平台界面截图并加盖公章，提供现场演示）
7		▲支持 HTTP 强制跳转 HTTPS，当用户访问 HTTP 端口（如 80）时，支持强制将访

		问牵引至 HTTPS 端口（如 443）（提供服务平台界面截图）
8	访问控制	▲支持区域访问控制，限制国外用户或者国内以市为最低行政单位的区域进行访问控制。（提供服务平台界面截图）
9	防护能力	支持检查提交的报文是否符合 HTTP 协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等；（提供服务平台界面截图）
10		支持对 HTTP 协议合法性进行验证，提供 HTTP 协议防护功能，支持对 HTTP 协议的 URI、HOST、UA、Cookie、Referer、Content、Accept、Range、其他头部和参数在内的元素、参数进行检测与处理。且支持非法编码和解码的灵活控制与处理。
11		支持针对主流 Web 服务器及插件的已知漏洞防护。Web 服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS 等。
12		支持对用户上传的文件后缀名和文件内容进行全方面检查，杜绝 Webshell 的上传和访问；
13		▲支持流量监测的功能，基于用户的访问记录，实时检查被访问页面的安全状况，能够发现更深层次的暗链、Webshell 等安全事件。（提供服务平台界面截图）
14		支持提供攻击防护安全策略，支持对命令注入（包括 SQL 注入、SQL 盲注、代码注入等）、跨站脚本、SSI 指令、路径穿越、远程文件包含、WebShell 防护。
15		▲支持提供信息泄露防护安全策略，包括目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露等。（提供服务平台界面截图）
16	密码强度检测	▲支持对用户登录账户密码进行密码强度检测，支持进行弱口令登录拦截、密码爆破防护、账号爆破防护，并定义请求频率阈值，支持在用户界面展示账户安全状况。（提供服务平台界面截图）
17	一键关停	▲支持一键关停功能，当网站出现紧急安全事件时，可通过浏览器一键完成关停，防止产生恶劣影响。（提供服务平台界面截图）
18	永久在线	▲支持永久在线功能，当网站因为服务器故障、线路故障、电源等问题出现无法连接时，可显示云防护节点中的缓存页面。当在敏感期或特殊时期时，用户网站主动关闭期间可显示缓存页面，增强网站安全性。（提供服务平台界面截图）
19	微信自服务	▲支持通过微信公众号查看网站整体防护态势，包含受攻击域名排行、攻击类型排行、攻击 IP 排行、攻击区域分布等状态信息。（提供服务平台界面截图）
20		▲支持通过微信公众号完成防护配置，包括一键关停、防护模式切换等功能。（提供服务平台界面截图）
21	日志管理	▲支持访问和攻击日志查询与导出功能，可根据域名、URL、客户端 IP、返回码、访问区域、访问时间段进行查询，查询后的日志数据支持下载到本地。（提供服务平台界面截图）
22		▲支持访问与攻击原始日志离线下载功能，可按天进行下载。原始日志包含访问 IP、访问时间、URL、返回码、访问域名等信息. 攻击日志至少保存 6 个月，满足《网络安全法》要求。
23	防护报表	支持查看安全防护报告，包含攻击次数、攻击者区域统计、攻击者 IP 统计、攻击类型分布等报告。（提供报告截图或进行现场演示）
24		支持查看网站访问报告，包含 CDN 加速流量、服务质量综合评价和关键指标信息、异常响应分析、访问区域统计、访问源 IP 统计、访问页面排行、访问终端、响应码分布等统计报告。（提供报告截图并或进行现场演示）
25		支持单个网站生成报表，也支持网站群生成一个汇总报表，支持日报、月报 ，并支持 html、word 格式导出。
26	告警管理	支持根据不同告警级别发送邮件、短信、微信公众号等多种告警方式。（提供服务

		平台界面截图）
27	可视化大屏	▲支持可视化分析大屏，展示访问与攻击流量趋势、受攻击网站排行、攻击源 IP 排行、攻击类型排行等信息。（提供服务平台界面截图）
28		▲支持单个网站可视化分析，包括防扫描告警、总体访问/攻击趋势、攻击源实时分析、IP 追踪、访问量排行、防御能力分析等数据展示与挖掘。（提供服务平台界面截图）
29		▲支持与威胁情报联动，在可视化大屏界面对发现的恶意 IP 进行下钻分析，获取 IP 地理位置、置信度、威胁等级、情报源、历史解析域名等信息。（提供服务平台界面截图）
30	售后服务	一年质保服务

4 其他需求

（1）项目实施阶段安排不少于 1 人现场驻点。

（2）签订合同后必须 3-5 个工作日内到货，安装调试在产品到货后 5 个工作日内开始进行。

（3）实施工期要求不能影响医院正常业务的使用，工期为从合同签订日起，10 个工作日内部署完成。

（4）免费送货上门、安装、调试，并试运行。

（5）投标人提供 7×24 小时电话维护响应服务，如电话不能解决问题，4 小时内现场响应。

5 评分标准

项目评分项	分值
公司证照齐全、合法有效。	**一票否决**
价格部分。	30
公司 2018 年后至今同类项目的业绩经验对比。	10
需求响应度对比。	20
公司技术方案比较。	20
公司提供响应时间比较。	10
公司提供售后服务的内容 (包括质保期、维护保养方案、补充承诺等)比较。	10
合计	**100**