附件1

包一：门户网站WAF（西部数据）

1、安全防护域名（包括一级域名2个、二级域名10个）及IP防护:

WAF支持云模式、独享模式和ELB模式三种部署模式，本次项目要求使用云模式进行部署。3年服务期内可按采购方的要求变更模式重新进行部署。

2、HTTP/HTTPS业务防护:

WAF可以防护HTTP/HTTPS业务，通过对HTTP/HTTPS请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

3、支持Web Socket/Web Sockets协议：

WAF支持Web Socket/Web Sockets协议，且默认为开启状态。

4、域名备案检查

WAF云模式支持域名备案检查，添加防护域名时，WAF会检查域名备案情况，未备案域名将无法添加到WAF。

5、PCI DSS/PCI 3DS合规认证和TLS

TLS支持TLS v1.0、TLS v1.1和TLS v1.2三个版本和五种加密套件，可以满足各种行业客户的安全需求。

WAF支持PCI DSS和PCI 3DS合规认证功能。

6、支持添加泛域名:

泛域名是指带1个通配符“\*”且以“\*.”号开头的域名。

7、非80、443标准端口防护:

WAF支持防护采用Web Socket（默认为开启状态）/HTTP/HTTPS协议的Web应用，WAF可以防护标准的80，443端口外，还支持非标准端口的防护

8、Web基础防护规则

覆盖OWASP（Open Web Application Security Project，简称OWASP）TOP 10中常见安全威胁，通过预置丰富的信誉库，对漏洞攻击、网页木马等威胁进行检测和拦截。

1）、全面的攻击防护

支持SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击检测和拦截。

2）、Webshell检测

防护通过上传接口植入网页木马。

3）、识别精准

内置语义分析+正则双引擎，黑白名单配置，误报率更低。

支持防逃逸，自动还原常见编码，识别变形攻击能力更强。

默认支持的编码还原类型：url\_encode、Unicode、xml、OCT（八进制）、HEX（十六进制）、html转义、base64、大小写混淆、javascript/shell/php等拼接混淆。

4）、深度检测

深度反逃逸识别（支持同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等的防护）。

5）、header全检测

支持对请求里header中所有字段进行攻击检测。

9、CC攻击防护：

CC攻击防护规则支持通过限制单个IP/Cookie/Referer访问者对防护网站上特定路径（URL）的访问频率，精准识别CC攻击以及有效缓解CC攻击。支持人机验证、阻断、动态阻断和仅记录防护动作。

1）、策略配置灵活

可以根据IP、Cookie或者Referer字段名设置灵活的限速策略。

2）、阻断页面可定制

阻断页面可自定义内容和类型，满足业务多样化需要。

10、精准访问防护：

基于丰富的字段和逻辑条件组合，打造强大的精准访问控制策略。

1）、支持丰富的字段条件

支持IP、URL、Referer、User Agent、Params、Header等HTTP常见参数和字段的条件组合。

2）、支持多种条件逻辑

支持包含、不包含、等于、不等于、前缀为、前缀不为等逻辑条件，设置阻断或放行策略。

11、IP黑白名单设置，支持批量导入IP地址/IP地址段：

添加始终拦截与始终放行的黑白名单IP/IP地址段，增加防御准确性。支持批量导入IP地址/IP地址段。

12、网页防篡改：

1），当WAF接收到正常的访问请求时，直接将缓存的网页返回给Web访问者，加速请求响应。

2），如果攻击者篡改了网站的静态网页，WAF将缓存的未被篡改的网页返回给Web访问者，保证Web访问者访问的是正确的页面。

3），WAF将对页面路径下的所有子文件进行防护。例如，对“www.example.com/admin”静态页面配置了网页防篡改规则，则WAF将防护“/admin”路径下所有子文件。

13、误报屏蔽：

对于误报情况，可以添加白名单对误报进行忽略，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。

14、隐私屏蔽：

通过Web安全防护配置隐私屏蔽规则。隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。

包二：精神卫生质控中心网站WAF(阿里云）

1、提供云服务器，配置要求：16G内存、10M独享带宽、100G硬盘。

2、云服务器单实例服务可用性99.975%，数据可靠性99.9999999%。

3、云服务器支持宕机迁移无感知、数据快照、自动告警等功能。

4、云服务器支持三副本专业存储策略，消除单点故障，保证数据可靠性。

5、成熟的网络虚拟化技术和网卡绑定技术保证网络高可用性。

6、云防火墙支持微信远程运维，管理端口无需向互联网暴露，免受暴破攻击困扰。

7、云防火墙支持攻击者视角的漏洞扫描能力，一键梳理云上资产的风险状况。

8、云防火墙支持入侵防御系统(IPS)和虚拟补丁技术，对云上资产的互联网暴露漏洞精准防护。

9、云防火墙支持入侵防御日志，对外部入侵活动和主动外联活动进行实时审计。

10、云防火墙采用 SDN 技术，提供公有云上的 SaaS 化防火墙，实现云上资产自动识别和一键开关，进行简单策略配置即可使用，提供无需部署成本的云防火墙功能。

11、云防火墙具备主备容灾机制，保障性能稳定可靠，充分发挥 SaaS 化服务优势，支持带宽、资产及存储等弹性扩展，实现按需分配，平滑扩展。

12、云防火墙具备当访问控制规则生效并命中后，云防火墙会记录被命中流量的五元组信息，并反馈用户对应规则，便于用户安全运维，在出现故障时，用户可以根据日志留存快速排障并修复。

13、云防火墙具备记录用户在云防火墙的操作情况及内容，包括所有账户的登录操作、云防火墙开关操作、针对规则的新增、删除、编辑操作，提升用户管理效率，降低管理成本。

14、云防火墙具备基于对公网 IP 配置的访问控制规则，从而封堵或观察有威胁的访问目的流量，也可以阻断外部威胁访问源对云上资产发起的攻击行为。

15、WAF支持OWASP TOP 10 威胁防护，如SQL注入攻击、XSS攻击、CSRF跨站请求伪造，Webshell木马上传威胁等攻击防护；

16、WAF支持云端自动更新Web 0day漏洞的防护规则；

17、WAF支持HTTP(80、8080端口)、HTTPS(443、8443端口)的业务防护；

18、WAF支持基于全球地理位置的地域封禁功能；

19、WAF支持紧急模式CC防护；

20、WAF支持自定义CC防护策略，包括基于IP和Session的CC防护策略，5条/域名；

21、WAF支持基于IP，URL路径，Referer，User-Agent，Cookie、Body等参数的自定义防护策略，10条/域名；

22、WAF支持IP黑名单管理，1000条/域名；

23、WAF支持网页防篡改，10条/域名；

24、WAF支持敏感数据防泄漏，5条/域名；

25、WAF支持泛域名防护；

26、WAF支持正常业务请求QPS:2500；

27、WAF支持一级域名个数：1；

28、WAF支持二级域名个数：10；

29、WAF支持传统通过 DNS 配置模式接入，更联合腾讯负载均衡推出全新接入模式，通过旁路部署和攻击清洗实现高效转发、高效防护，转发和安全分离，保障业务稳定安全。

30、WAF支持爬虫 Bot 行为管理，基于 AI+ 规则库的网页爬虫及 Bot 机器人管理，协助企业规避恶意 Bot 行为带来的站点用户数据泄露、内容侵权、竞争比价、库存查取、黑产 SEO、商业策略外泄等业务风险问题。

31、WAF支持AI+ Web 应用防火墙，基于 AI+ 规则的 Web 攻击识别，防绕过，低漏报，低误报，精准有效防御常见 Web 攻击，如 SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造，Webshell木马上传等 OWASP 定义的十大 Web 安全威胁攻击。

32、WAF支持业务风控方案，控制 IP 访问，避免网页篡改带来的负面影响，防止敏感数据泄漏，避免 DNS 恶意劫持带来的数据窃取及金融损失问题等。

33、WAF支持CC 攻击防护，多维度自定义精准访问控制、配合人机识别和频率控制等对抗手段，高效过滤垃圾访问及缓解 CC 攻击问题。

34、WAF支持全量日志支持，提供全量日志实时存储和查询服务，保障业务情况安全可控可视，助力等保合规合法。

35、WAF支持0day 漏洞虚拟补丁，7\*24小时监测，主动发现并响应，24小时内下发高危 Web 漏洞，0day 漏洞防护虚拟补丁，受护用户无需任何操作即可获取紧急漏洞，0day 漏洞攻击防护能力，有效缩短漏洞响应周期。

WAF支持支持防护节点30线独享 BGP IP 链路接入，节点智能调度，有效解决访问延迟问题，保障1-18线城市用户的站点访问速度，实现对网站访问速度影响无感知的安全防护部署。

附件2

成都市第四人民医院

网站WAF市场调研基本信息表

|  |  |
| --- | --- |
| **厂商基本信息表** | |
| 挂网调研名称 | 网站WAF市场调研 |
| 报名公司名称（需附营业执照复印件） |  |
| 报名人姓名及联系方式 |  |
| 案例 | 文字描述 |
| 公司企业类型（另附佐证材料） | 大型企业（ ） 中型企业（ ） 小型企业（ ） 微型企业（ ） 监狱企业（ ） 其他 注：“是”打√ |
| 供应商相关资质 | 文字描述 |
| 报价情况（可单独报价） | 包一：门户网站WAF 元/年  包二：质控中心网站WAF 元/年 |