**云WAF服务项目（2年：2023-2024年度）需求书**

# 项目名称

项目名称：云WAF服务项目（2年：2023-2024年度）项目

# 采购清单

采购设备及数量如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 配置描述 | 数量 |
| 1 | 云WAF防护 | 配置详见3.1.1 | 1 |

# 参数要求

## 3.1.1、云waf防护

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **具体参数要求** |
| 1 | **性能要求** | 支持2年20个域名的防护 |
| 2 | **服务方式** | 支持通过修改DNS CNAME解析的方式把流量牵引到云端WAF，防护后把请求指回到源站； |
| 3 | 支持智能DNS解析服务选择防护节点，并支持节点之间的手动切换。 |
| 4 | **高可用** | 支持为客户配置独立的WAF防护引擎，隔离不同租户间的访问流量。 |
| 5 | 支持云端防护引擎的冗余部署，保障云WAF的高可用性。单台引擎出现问题的时候另一台引擎可以自动接管。 |
| 6 | 防护节点支持本地电信级机房、CDN、公有云部署等多种方式，保障云waf服务的稳定性和高可用。 |
| 7 | 能够满足客户网站部署多线需求及防护节点省内就近防御 |
| 8 | **应急响应** | 重要0day漏洞出现后，能够第一时间内帮助客户确认是否存在，并能够在云WAF上进行临时封堵防护。需要提供相应证明 |
| 9 | **防护功能** | 支持HTTP协议校验。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。提供配置界面截图证明 |
| 10 | 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 插件应覆盖:dedecms、phpmyadmin、PHPWind、shopex、discuz、ecshop、vbulletin、wordpress等，提供Java反序列化漏洞（Jboss）防护插件。提供配置界面截图证明。 |
| 11 | 支持完善的漏洞攻击防御库，应支持定期漏洞收集和挖掘升级能力，产品厂商支持获得漏洞情报的一线咨讯。 |
| 12 | 支持HTTP访问控制功能，可以提供针对HTTP元素和客户端的组合访问控制策略。支持对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK TRACE、SEARCH、CONNECT。提供配置界面截图证明 |
| 13 | 提供爬虫防护，规则库至少可以防护100种以上的爬虫。提供配置界面截图证明或者爬虫列表 |
| 14 | 提供盗链防护，应采用Referer和Cookie算法。提供配置界面截图证明 |
| 15 | 支持对注入（包括SQL注入、LDAP注入、XPATH注入及命令行注入）、XSS、SSI指令、路径穿越、远程文件包含、WebShell防护。提供配置界面截图证明 |
| 16 | 支持CSRF（跨站请求伪造）防护。提供配置界面截图 |
| 17 | 设备的漏洞防护库应有专业漏洞挖掘团队维护，漏洞挖掘团队须有对系统漏洞进行发现、验证、以及提供应急服务的技术能力。 |
| 18 | 支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要，禁止上传以下文件类型：PE(windows Executable File)、ELF(linux Executable File)、PHP web shell、Linux shell、Power shell(windows Script File)、Java shell、Asp shell、Perl shell、Python shell及Ruby shell。提供配置界面截图证明 |
| 19 | 支持非法下载防护，可以根据文件大小、MIME类型及文件扩展名灵活定义下载限制策略，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等），提供配置界面截图证明 |
| 20 | 支持Cookie安全机制，包括Cookie加密和Cookie签名的防护算法。支持过期兼容时间配置以及\*配置。提供配置界面截图证明 |
| 21 | 支持信息泄露防护，提供针对服务器状态码进行过滤和伪装的安全策略。提供配置界面截图证明 |
| 22 | 支持暴力破解防护，可针对指定URL进行暴力破解防护，支持多种方式的登陆，支持referer检测，支持阈值和检测周期的设置。提供配置界面截图证明 |
| 23 | 支持识别判定自动扫描行为，在设定周期内采集发送端向网站服务器发送的访问请求消息和网站服务器向发送端返回的响应消息，将设定周期等分为至少两个子周期，依次统计每个子周期内访问请求消息个数，确定发送端请求可信度，判定发送端是否发生了自动扫描的行为。须提供国家权威机构（如工业和信息化部、经济和信息化委员会或国家知识产权局）证明材料，加盖厂家公章。 |
| 24 | 支持敏感信息过滤，对用户的个人隐私信息（信用卡卡号、手机号、身份证号码）泄露进行检测、阻断或替换。 |
| 25 | 支持XML防护，包括XML基础校验（包括最大树深度、元素名长度、元素个数、子节点个数等参数配置）、Schema校验以及SOAP校验。提供配置界面截图证明。 |
| 26 | 支持扫描防护，基于专利技术实现的Web扫描防护，支持以统计算法分析扫描行为的扫描防护。提供配置界面截图证明和专利证书复印件 |
| 27 | **区域访问控制** | 支持区域访问控制，用户可自助选择需要封禁的地理位置，能够封禁海外IP、国内地理位置至少需要精确到省。提供配置界面截图证明 |
| 28 | **IP信誉** | 厂商应建立自身的恶意网站信息库，并与非盈利组织(威胁软件阻止stopbadware协会、信息安全产业RSA协会或中国区域科学协会RSAC）进行信息交换，确保恶意网站信息库的准确性，提供信息交换证明并厂商盖章。 |
| 29 | 支持威胁情报协同防护，与威胁情报强大的IP信誉库联动实现IP信誉封禁功能。 |
| 30 | **IP访问控制** | 支持IP访问控制，可以针对每个被防护站点限制访问IP的范围。提供配置界面截图证明 |
| 31 | **一键下线** | 支持一键下线功能，紧急时刻用户可以自助在门户（web门户、移动端）立刻执行被防护网站的下线动作，也可以选择“恢复上线” |
| 32 | **自助回源** | 支持一键回源，用户可以自助在门户（web门户、移动端）将网站指回源站暂停防护，也可以选择指向防护节点恢复防护。 |
| 33 | **永久在线** | 支持永久在线，当网站出现故障或者在敏感时期，用户可切换成云防护中的缓存页面，增强网站稳定性和安全性。 |
| 34 | **策略管理** | 支持策略模板配置，至少提供4套默认策略模板，可以方便用户针对不同的场景快速切换。提供截图证明 |
| 35 | **例外策略** | 支持对安全策略的一键式例外配置，用户可以自助在用户门户上一键添加。提供配置界面截图证明 |
| 36 | **策略优化** | 支持策略优化功能，采用智能算法定期分析待优化策略配置，由运营团队定期优化策略配置从而减少误报漏报。 |
| 37 | **分权分域** | 支持用户门户同一客户下的账号分权分域，主账号管理所有网站，多个子账号分管不同网站。 |
| 38 | **安全风险大屏** | 展示客户所有被防护站点的整体安全态势，包括：在地图中实时展示出当前攻击情况；统计最近一段时间内访问、告警趋势；TOP5 被攻击URL；TOP5攻击源IP |
| 39 | **实时监控** | 对单个被防护站点：按年统计每天的被攻击安全情况，集中整体展示。提供截图证明 |
| 40 | 对单个被防护站点：对被攻击TOP10 的URL进行逐层向下钻取，了解此URL下的TOP10攻击源IP，再针对其下的某个源IP，了解其主要的攻击手段。便于安全排查工作的展开，提供配置界面截图证明 |
| 41 | 对单个被防护站点：在地图中可以整体了解攻击源IP的地理位置分布。提供截图证明 |
| 42 | **日志源地址溯源** | 支持日志内容源地址溯源，在安全日志中带有客户端真实IP地址，便于IP溯源，并能够显示出攻击IP的地理位置 |
| 43 | **防护报表** | 可查看安全防护报告，能够针对每个防护站点能够提供攻击防护的周报、月报统计，并提供自定义选择时间跨度和站点生成报表。 |
| 44 | **资格要求** | 厂商需具备中国信息安全测评中心颁发的信息安全服务资质证书-安全开发类二级以上，提供盖章证明的证明文件。 |
| 45 | 厂商获得ITSS信息技术服务标准符合性证书-云服务二级以上，提供盖章证明的证明文件。 |
| 46 | 厂商通过ISO20000的安全认证，认证范围包括向外部客户提供整体安全解决方案、安全软件的设计、开发和运行维护，硬件的运行维护，安全相关的SaaS及运营服务，提供盖章证明的证明文件。 |

# 实施服务要求

供应商需要拥有完善的服务团队、技术能力和服务管理工具，为本项目设备提供售后服务，服务内容包括：

1. 提供7\*24小时快速上门服务和2小时内快速响应服务；
2. 不影响原有业务运行情况，完成网站云防护迁移割接工作；
3. 服务期内，免费提供网站评估监测及网站安全应急响应服务；
4. 提供策略优化、配置调整、规则更新、问题处理、技术咨询安全事件通告等常规技术支持服务；
5. 实时监测感知持续性攻击事件，并及时响应和对抗，同时在重大节会期间提供更高级别的安全响应服务；
6. 按院方要求按时提供相关安全防护报表数据。