**1.云WAF技术要求**

|  |  |  |
| --- | --- | --- |
| **类别** | **名称** | **具体参数要求** |
| **资质要求** | | |
| **厂商资质** | **厂商资质** | 厂商为应用安全联盟成员。 |
| **被防护站点** | | |
| **接入方式** | **接入方式** | 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； |
| 支持智能DNS解析服务选择防护节点，并支持节点之间的自动切换。 |
| **被防护站点** | **被防护站点** | 可同时支持http, https协议 |
| 支持自定义站点端口 |
| 自定义端口数量不限 |
| **SSL支持** | 支持SSLv2, SSLv2/v3, SSLv3、TLS1.0\1.1\1.2 |
| 能够用户自助上传https证书，进行https的加解密，并且能够加密保存在云端 |
| **防护功能** | | |
| **防护体系** | **GEO IP封禁** | 用户可以自助选择需要封禁的地理位置，需要能够封禁海外IP、国内地理位置至少需要精确到省。 |
| **IP访问控制** | 可以针对每个被防护站点，限制访问IP的范围。 |
| **自定义规则** | 且支持自定义规则，规则属性要求支持“检测方向（请求或响应）”、“检测对象（URI/URI-path/Host/参数名/参数/Header-name/Header/Cookie名/Version/请求方法/Request-Body）”、匹配操作、特征签名等丰富要素。 |
| **网站一键下线** | 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” |
| **网站防篡改** | 云WAF提供防篡改功能，在重大事件保障期间，保障被防护站点内容不发生篡改。 |
| **防护功能** | **HTTP协议校验** | 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。 |
| **WEB基础架构防护** | 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。 |
| **WEB资源授权控制** | 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。 |
| 提供爬虫防护，规则库至少可以防护100种以上的爬虫。 |
| 提供盗链防护，应采用Referer和Cookie算法。 |
| **WEB应用安全防护** | 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。 |
| 支持CSRF（跨站请求伪造）防护。 |
| 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。 |
| 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）。 |
| 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。 |
| 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。 |
| 支持内容过滤，提供恶意代码过滤功能 |
| 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。 |
| 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。 |
| **XML防护** | 支持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。 |
| 支持Schema校验。 |
| 支持SOAP校验。 |
| **Web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。 |
| **Web漏洞封堵** | 能够对网站进行漏洞检测，并提供防护前后的漏洞状态对比效果展示。 |
| 能够根据网站漏洞检测结果生成“智能补丁”并下发至防护节点 |
| **DDOS防护** | 默认支持2G的DDoS流量防护 |
| 支持CC攻击防护 |
| 支持大流量攻击防护，如支持SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood 、SSDP Flood、HTTP Flood、DNS Flood，SIP攻击等多种主流攻击类型。 |
| **策略管理** | **策略配置向导** | 至少提供4套默认策略，可以方便用户针对不同的场景快速切换。 |
| **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。 |
| **高可用和扩容** | | |
| **高可用** | **高可用** | 支持为每客户配置独立的WAF防护引擎，隔离不同租户间的访问流量。 |
| 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。 |
| 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。 |
| 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 |
| **弹性扩容** | 云WAF支持弹性扩容，客户流量增加时可以自动增加防护容量 |
| **管理门户、日志和报表** | | |
| **门户** | **用户门户** | 用户可以通过浏览器访问云WAF的自助门户，了解攻防情况，并进行针对性的操作。 |
| **移动端** | 要求原厂提供在移动端安全运维功能，包括当日0时至查看时间的攻击防护情况、自动推送昨日攻击防护简报、查看最近一个月每日攻击防护简报。 |
| 并且能够在移动端上随时调整网站防护策略和网站“一键下线”等操作。 |
| **监控** | **安全态势** | 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 |
| **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。 |
| 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。 |
| 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。 |
| **日志报表** | **日志查询** | 支持基于时间、攻击IP、告警级别等条件的对日志进行查询。 |
| **日志内容源地址溯源** | 支持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。 |
| **日志保存** | 访问日志至少保证能够保存180天。 |
| 告警日志能够保存1年，实时热数据至少能够查询30天以内的。 |
| **报表** | 针对每个防护站点能够提供攻击防护的周报、月报统计。 |

**2.云监测服务要求**

|  |  |  |  |
| --- | --- | --- | --- |
| 类别 | 技术要求 | | |
| 系统的技术要求 | 监测内容与范围 | 能够对网站常见的隐患和安全灾害事故进行监测：漏洞隐患包括Web漏洞和系统漏洞，常见的灾害事故包括挂马网页、篡改网页、含敏感内容网页。 | |
| Web漏洞监测与扫描能力 | 每个月可以对所监测的网站进行至少一次Web漏洞的扫描与检查 | |
| 系统漏洞监测与扫描能力 | 每个月可以对所监测的网站进行至少一次系统漏洞的扫描与检查 | |
| 漏洞验证能力 | 能够提供所有中高危漏洞的验证能力 | |
| IP资产核查能力 | 能够提供针对IP段判活IP及端口的能力，并且在发现资产变更后提供事件验证及通报能力 | |
| 挂马监测能力 | 能够对网站主要页面提供挂马监测能力，根据不同页面的重要等级提供不同频率监测，提供事件验证能力，排除误报 | |
| 篡改监测能力 | 能够对网站主要页面提供篡改监测能力，根据不同页面的重要等级提供不同频率监测，提供事件验证能力，排除误报 | |
| 敏感内容监测能力 | 能够对网站主要页面提供敏感内容监测能力，根据不同页面的重要等级提供不同频率监测，提供事件验证能力，排除误报 | |
| 运营支撑要求 | 能够对监测的站点、监测项、进行配置与管理 | |
| 数据要求 | 要求至少存储备份6个月以上监测数据 | |
| 系统运营要求 | 提供安全态势展示 | 能够按照单位组织架构维度、中国地图维度展示各省、各地级市漏洞曝出多寡的态势，事故曝出多寡的态势 |  |
| 提供运营统计分析 | 能够提供运营概况、各类事件月度分布、漏洞管理效率、行业同比效率等多方面数字统计 | |
| 提供事件管理 | 支持展示挂马、黑链、篡改、敏感内容、DNS解析异常、平稳度监测异常等6种事件的列表及场景详情 | |
| 提供漏洞生命周期管理 | 能够针对资产漏洞列表的每一个漏洞展示漏洞名称、漏洞当前所处状态，漏洞类型、漏洞本身、漏洞验证、漏洞详情、以及漏洞处置建议 | |
| 提供资产管理 | 能够自助管理各省、市甚至各单位组织的网站状况 | |
| 提供即时报表 | 用户可以在任意时刻下载半年内报表，同时支持随时生成某个资产或者某个地域、单位的在线Html格式报表 | |
| 厂商要求 | 厂商与云WAF为同一厂家。 | | |