**WEB 应用防火墙参数**

|  |  |
| --- | --- |
| **指标项** | **招标参数要求** |
| 配置要求 | 产品必须为专业性WEB应用防火墙设备及专业性WEB应用防火墙资质；1U机架式设备，双电源，128G SSD硬盘，提供1个10/100M管理接口、1个10/100/1000M HA口， 4个千兆电口、2个千兆光口、2个万兆光口，支持2个扩展插槽，三年特征库升级服务。 |
| 设备最大HTTP并发连接数不小于300万，设备网络层吞吐8G，设备每秒新建HTTP连接数不少于4万。 |
| 接入模式 | 应支持旁路部署、单臂模式部署； |
| 应支持透明模式、代理模式同时部署方式（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）； |
| 应支持Web应用识别，支持感知服务器的域名、操作系统、Web服务器类型、编程语言、中间件、服务器IP及端口等（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）； |
| 应支持安装向导式部署，按照该部署方式可直接部署完成； |
| 应支持NAT环境下的用户识别能力(要求提供界面截图)； |
| 应支持大屏展示能力，可满足客户对WAF产品大屏展示要求(要求提供界面截图)； |
| Web攻击防护 | 应具备Web恶意扫描防护的检测与防御能力，专利级别防护能力 (要求提供界面截图)； |
| 上报日志中有日志解码工具，通过解码工具可准确查看攻击语句，有利于用户查看和分析攻击日志(要求提供界面截图)； |
| 设备具有对外提供API接口能力，可通过API接口给设备下发策略(要求提供界面截图)； |
| ★应具备人机识别功能，能够有效防止机器人攻击（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）；具备点对点流量识别技术，可识别机器人攻击并进行过滤，提供国家第三方机构出具的证明文件复印件， |
| 应具备CSRF防护及自学习功能，能够有效防止CSRF攻击及通过自学习可减少CSRF配置（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）； |
| 产品支持未知威胁的检测和防护能力，具备0day攻击防御能力； |
| 应具备TCP协议检测，可对TCP层协议攻击进行检测与防护（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）； |
| ★应具备自定义事件检测，支持自定义网络特征事件检测，可支持HTTP层、TCP层、IP层等协议自定义，有利于对用户业务系统遇到攻击进行检测与防护（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）；具备针对DNS服务的防御方法的技术能力，提供国家第三方机构出具的证明文件复印件； |
| ★支持协议识别及解码能力，应支持:URL解码、XML解码、JSON解析、Base64解码、Unicode解码、十六进制转换、斜杠反转义、CHR解码、UTF-7解码，支持解析7层以上混合编解码能力，可实现对多层编码攻击的检测（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）；同时提供国家第三方机构出具的非法网站过滤方法的技术证明文件复印件； |
| 产品支持语义防护、AI智能防护、算法防护功能,，提供人工智能安全分析平台软件著作权登记证书复印件； |
| ★应具蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）；同时提供国家第三方机构出具的滤除网络攻击流量的方法的技术证明文件复印件； |
| 应具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截(要求提供界面截图)； |
| 应具备API防护，可支持API协议合规、API访问速率限制等功能（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）； |
| 应具备Shiro反序列化、代码注入、PHP反序列化、XML防护、COOKIE防护及自学习等应用安全防护能力（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）； |
| 应具备客户端访问控制功能，预防恶意客户端进行访问频率的多层次恶意访问(要求提供界面截图)； |
| 应支持HTTP协议合规自学习，通过自学习结果可查看URL最大长度、查询字符串最大长度、请求头最大长度、COOKIE最大个数、协议字段最大个数、协议字段名最大长度、POST表单参数最大个数等（要求提供TTL、CNAS、MA、ilac-MRA检测盖章报告证明）； |
| 升级管理 | 应支持手动执行产品升级； |
| 应支持自动执行产品升级，不需要用户每次手动升级特征库； |
| 公司网站应提供产品离线升级包下载； |
| 应对登陆用户提供防暴力猜解功能； |
| 资质要求 | 产品具备《网络关键设备和网络安全专用产品安全认证证书》，提供相关证明文件； |
| 厂商具备CNAS标识的业务连续性管理体系认证证书，提供证书复印件。 |