WEB应用防火墙（WAF）招标公告

安信农业保险股份有限公司（以下简称“征集人”）现邀请合格的供应商（以下简称“应征人”）就征集人所需项目进行项目征集，征集人将择优选定中选人，欢迎符合条件的应征人前来参与方案比选，现将有关事项公告如下。

1. 征集项目内容
2. 设备数量

WEB应用防火墙（WAF）2台

1. 设备要求

设备及设备附属配件均为原厂提供。

1. 应征人必须具备的条件：
2. 应征人须为原厂商或授权代理商，所投产品品牌为国内外知名品牌，所投服务器产品性能可靠，不少于三年市场应用案例。
3. 应征人必须具有独立法人资格，具有独立承担民事责任的能力，具备相应的经营范围且其注册资金或净资产（所有者权益）必须不小于 1000（含）万元人民币（或等值外币）。
4. 应征人必须具有专业团队，具有较强的售前、售中和售后服务支持能力，提供7\*24报修服务电话及固定的客户服务经理，省会城市、一类城市、直辖市均需要有办事处及备件库。提供全国性服务网点的证明材料。
5. 应证人在最近三年内未因自身任何违约、违法行为及违反商业道德的行为而导致取消参选资格、合同解除或败诉。
6. 法定代表人为同一个人的两个及两个以上法人，母公司与全资子公司/由其控股的子公司，不得同时参加本项目。
7. 法律、行政法规规定的其他条件。
8. 应证人需提供厂商对本项目的授权书。
9. 售后服务要求
10. 应证人应为征集人提供及时周到的系统技术支持。
11. 应证人应确保为甲方提供7\*24小时技术支持服务，响应时间不应该超过1小时，现场响应支持不应超过4小时。
12. 应证人所提供设备保质期均为三年（具有特殊要求的除外），集成商所提供的设备在保质期内因硬件、软件本身质量问题所造成的损坏或无法正常运行，由此产生的维修、更换硬件和软件故障排除等所需一切费用（包括工程师差旅费用等支出）由集成商负责。
13. 应证人应提供相应的备件支持，以便及时更换损坏硬件。
14. 应证人应在质保期后设备生命周期内有义务继续对系统设备提供维保服务，甲方将支付相应费用。
15. 针对以上要求，应证人可提供具体可行的有吸引力的合作方案。
16. 验收
17. 所有设备均需提供安装服务，所采购设备（包括软件）安装都必须由生产厂商授权集成商执行。
18. 安装前由征集人信息技术部协同征集人行政办公室对货物的品牌、数量、包装等方面进行实物验收。征集人提供的所有包装的货物均应完好无损。如遇交付前已拆封的货物，征集人有权拒绝或要求更换。应证人交货时，必需提供所有产品原厂或总代理出具的供货相关证明。
19. 应证人根据征集人技术要求在征集人信息技术部指导下进行设备安装、调试，并由征集人信息技术部进行使用性能方面的验收。
20. 报名方式

有意者请于2019年9月13日之前将标书及相关材料送至以下地址：上海市静安区共和新路3651号 顾晓磊收

联系人：顾晓磊

联系方式：021-66988356 guxl@aaic.com.cn

1. 举报邮箱：[kehufuwu@aaic.com.cn](mailto:kehufuwu@aaic.com.cn)
2. 招标参数要求

|  |  |
| --- | --- |
| 基本需求 | 投标产品应该是经过市场考验的成熟产品，产品上市时间不少于5年。须提供销售许可证或软件著作权证书等有效证明材料。 |
| 专用机架式硬件设备，系统硬件为全内置封闭式结构，稳定可靠，用户界面、配置和管理等，均为中文，易于理解，并有详尽的中文技术文档。 |
| 提供的产品不能少于6个10/100/1000M自适应电口，4个SFP插槽，硬盘不小于1TB；必须内置硬件Bypass。 |
| 提供的产品应用层吞吐量不能小于1Gbps，最大并发连接数不能低于15万，每秒新建事务数不可小于10000tps。 |
| 支持透明部署，旁路部署，反向代理模式以及镜像部署模式。 |
| 产品资质 | 厂商应具备足够的安全运维服务保障能力，获得中国网络安全审查技术与认证中心颁发的信息系统安全运维（三级）服务资质，提供证书复印件证明 |
| 厂商应具备足够的安全应急响应能力，获得CNVD网络安全应急服务支撑单位（国家级）证书，提供证书复印件证明 |
| 厂商应具有漏洞发现能力，至少曾经获得中国信息安全测评中心颁发《中国国家漏洞库-信息安全漏洞提交证明》，不低于4份。 |
| 《计算机信息系统安全专用产品销售许可证》（增强级），提供证书复印件证明 |
| 《计算机软件著作权登记证》，提供证书复印件证明 |
| 中国网络安全审查技术与认证中心的《网络关键设备和网络安全专用产品安全认证证书》，提供证书复印件证明 |
| 具备IPv6证书，提供证书复印件证明 |
| OWASP中国WEB应用防火墙认证证书，提供证书复印件证明 |
| 基于机器学习和语义分析的智能检测引擎，提升SQLi和XSS检测精度 |
| 利用威胁情报建立IP风险画像，提供6类信誉数据（1）恶意IP；（2）漏洞利用源；（3）暴力破解IP  （4）Webshell客户端； （5）扫描器IP； （6）Botnet客户端： （7）Tor地址 （8）代理IP |
| 系统提供可配置的内置规则；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。提供配置界面截图证明 |
| 支持ARP攻击防护，支持MAC地址绑定。提供配置界面截图证明 |
| 支持基于五元组（源IP地址、目的IP地址、源端口、目的端口、协议类型）及接口的网络层访问控制功能。提供配置界面截图证明 |
| 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。提供配置界面截图证明 |
| 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。 |
| 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 |
| 提供盗链防护，应采用Referer和Cookie算法。提供配置界面截图证明 |
| 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 |
| 支持CSRF（跨站请求伪造）防护。提供配置界面截图 |
| 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 |
| 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 |
| 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 |
| 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 |
| 支持内容过滤，提供恶意代码过滤功能 |
| 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。 |
| 支持TCP Flood防护；支持基于阈值及算法配置的HTTP Flood防护。提供配置界面截图证明 |
| 支持对慢速攻击的防护。 |
| 可以与同品牌SaaS扫描服务联动，实现攻击事件的全局动画展示，并实现对问题网站的一键下线功能。要求提供监控平台界面截图 |
| 提供默认策略模板，方便客户快速对站点组及虚拟站点进行web安全防护策略配置。支持严格模板、标准模板及宽松模板。 |
| 支持多达七种的防护动作，包括了继续、通过、阻断、重定向、封禁、清除和替换。可针对不同安全风险提供多种可选方案。提供配置界面截图证明 |
| 支持对攻击源地址的智能阻断，支持永久封禁或者自定义IP封禁时间（秒/分钟/小时），并且可以手工解除解禁。提供配置界面截图证明 |
| 可自定义修改某一策略的默认风险等级 |
| 支持对安全策略的一键式例外配置。提供配置界面截图证明 |
| 支持透明串联部署、旁路部署、镜像检测部署、反向代理部署等多场景部署模式。 |
| 满足IPv6环境部署要求，提供第三方资质证明。 |
| 支持对SSL（HTTPS）加密会话进行分析 |
| 支持基于时间、IP、端口、动作、事件类型、URI、方法等条件的日志查询， |
| 支持基于日志类型选择不同的日志外发配置。提供配置界面截图证明 |
| 支持在安全日志中带有客户端真实IP地址，便于IP溯源。提供配置界面截图证明 |
| 支持日志分时段导出、全部导出或者清空。提供配置界面截图证明 |
| 支持显示接口状态，引擎状态、系统CPU、内存及硬盘使用率，系统当前时间及系统运行时间 |
| 安全事件、业务负载、接口流量、系统负载、封禁IP管理、站点访问量统计的实时和历史数据查看及查询 |
| 支持B/S管理、支持Syslog接口、REST API接口等管理方式 |
| 定期自动升级或者支持手动离线升级功能模块和规则库 |
| 支持自定义HTTPS监听端口，不完全依赖缺省的443端口。提供配置界面截图证明 |
| 能对账户进行安全策略配置，包括口令复杂度和口令生存期。提供配置界面截图证明 |
| 可以限制远程管理的登录IP。提供配置界面截图证明 |
| 支持VRRP等协议的ha部署，实现链路切换、配置同步 |