项目概况：

本次项目为续保一年主站云安全服务，保障各级用户对系统的正常访问。

技术参数：

**（PS：技术部分要求是对项目需求清单中所列项目的详细功能、性能或配置要求，分为实质性条款和非实质性条款，其中实质性条款不允许负偏离，否则作为无效报价）**

**实质性条款：**

|  |  |
| --- | --- |
| 厂商资质 | * 产品生产厂商具备工信部颁发的中华人民共和国增值电信业务经营许可证（互联网接入服务业务（全国）、内容分发网络业务类（全国）（需提供证书复印件，加盖原厂公章）
 |
| 产品资质 | * 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》（网站安全云防护平台类（增强级））（需提供证书复印件，加盖原厂公章）
 |

**非实质性条款：**

|  |  |
| --- | --- |
| 产品资质 | * 具备《计算机软件著作权》（云安全、云防护类）（需提供证书复印件，加盖原厂公章）
 |
| * 具备数据中心联盟颁发的《可信云云分发证书》
 |
| * 具备全球顶级认证CSA CSTR 云安全标准认证证书（需提供证书复印件，加盖原厂公章）
 |
| * 具备公安部监制的三级《信息系统安全等级保护备案证明》（需提供证书复印件，加盖原厂公章）
 |
| * 具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书CNNVD》（需提供证书复印件，加盖原厂公章）
 |
| 产品成熟度 | * 2019年1月1日后（以合同签订时间为准），产品生产厂商具有江苏省教育行业网络安全服务项目业绩3个及以上。（需提供合同证明文件）
 |
| 产品部署 | 无需对原有网络拓扑进行任何更改，需将CNAME别名指向云防护平台。 |
| 智能DNS | * DNS负载均衡：支持根据客户不同服务的运营商智能选择不同的DNS进行解析，并支持解析负载功能。提供截图证明，加盖原厂公章
 |
| https网站防护支持 | * 支持HTTPS网站防护，可支持SSL证书上传到防护服务器。提供截图证明，加盖原厂公章
 |
| 同站多域名绑定 | * 同站多域名绑定：支持同站点多域名的防护。提供截图证明，加盖原厂公章
 |
| Web防火墙 | 能够防止SQL注入、XSS跨站、文件注入、代码执行、文件包含、远程命令、特殊攻击、恶意采集等Web攻击 |
| Webshell防护 | 使用WebShell进行攻击尝试和试图访问WebShell的IP地址将被屏蔽，可在整站设置中修改屏蔽时间 |
| IP黑白名单 | 可根据IP地址，建立黑名单或白名单，阻止或者允许特定IP进行访问，可对屏蔽的IP进行时间设置 |
| 智能攻击识别 | 精准识别上百种自动化扫描和攻击软件，并阻断其所有请求 |
| 后台锁 | * 禁止非授权IP访问网站后台管理地址或重要页面。提供截图证明，加盖原厂公章
 |
| 防盗链 | 保护网站图片、压缩包等资源文件不被其它站点盗用 |
| DDoS防御 | 防御流量峰值不超过5G的 DDoS攻击，保证网站在DDoS攻击下正常使用 |
| CC防护 | 能防御大规模CC攻击，CC攻击流量清洗率可达到99% |
| 安全评级云 | 可根据攻击者IP的历史行为对恶意IP可能的攻击进行预先拦截和防护 |
| 缓存黑白名单 | 设置必须缓存的URL列表（白名单）及禁止缓存的URL列表（黑名单） |
| 拦截黑白名单 | 设置不进行防护的IP地址（IP白名单）、不允许访问的IP地址（IP黑名单）和不经过防护的URL地址（URL白名单） |
| 日志下载 | * 根据《网络安全法》需留存网站访问的日志，需提供日志下载功能，并区分原始日志，攻击日志和CC攻击日志下载。提供截图证明，加盖原厂公章
 |
| 网站访问情况 | * 包括请求数、总流量、网站浏览人数，搜索引擎引导量，遭受攻击次数等，并能按时间端统计的网站访问量。提供截图证明，加盖原厂公章
 |
| 网站安全状况 | 包括各种攻击发生次数，攻击IP、来源（国家）等 |
| 网站安全评级 | * 网站安全、危险等评级，可显示历史攻击次数。提供截图证明，加盖原厂公章
 |
| 防护效果 | * 为保证监测防护的时效性和准确性，要求平台可以和安全联盟的数据能够进行实时对接，提供截图证明，加盖原厂公章
 |
| CC攻击统计 | CC攻击详情和CC攻击实时动态 |
| 攻击扫描统计 | * 可显示攻击者的扫描情况，包括时间、攻击URL，攻击者IP及归属地，攻击类型等。提供截图证明，加盖原厂公章
 |
| 攻击统计数据 | TOP5攻击来源国家、TOP5攻击来源城市、TOP5攻击来源IP（国内）、TOP5攻击来源IP（国外） |
| 实时防御和追踪 | 基于世界地图和中国地图两种视角，动态展现攻击源位置对网站发起的各种方式攻击，攻击类型用不同颜色的动态线条来表示，包括恶意扫描器探测攻击、SQL注入攻击、文件注入攻击、WebSell攻击、XSS跨站攻击、远程命令攻击、代码执行攻击、恶意采集攻击、本地/远程文件包含攻击、特殊攻击、CC攻击和其它攻击，动态滚动的实时攻击数据包括攻击IP、攻击来源城市、攻击目标等。 |