附件1：

**采购需求**

一、项目概况

1.项目名称：2025年网站安全云防护服务

2.预算金额：人民币5.45万元；超过采购预算金额（最高限价）的投标，按无效投标处理。

3.服务期（交货期）：合同签订之日起七日内完成交货调试，产品整体服务期限一年。

4.交付形式：提供管理平台账号、密码。

二、项目用途

为采购人网站系统提供网站安全综合云端防护服务，将Web应用攻击防护能力、智能DNS解析能力、DDoS防护能力、CDN加速能力、安全运营能力以及统一的配置管理综合到同一云端安全防护体系中，为采购人提供一站式综合Web安全云端防护服务。

为采购人指定的4个域名提供服务期内的网站安全云防护服务，包含其中1个域名的重保只读服务。

三、项目需求

1、采购网站安全云防护系统为4个域名提供网站安全防护，服务时间一年。

2、采购重保只读模块为1个域名提供重要时期的防篡改功能，服务时间一年。

|  |  |  |
| --- | --- | --- |
| 系统描述 | 功能 | 数量 |
| 网站安全云防护系统 | 提供4个域名一年的网站安全云防护服务，服务内容包含以下内容：  1.Web攻击防护服务，包含：SQL注入、跨站攻击、伪造请求攻击、后门植入、上传漏洞攻击、路径遍历等WEB漏洞攻击防护；  2.DDoS攻击共享型防护服务，包含：SYN Flood、ACK Flood、UDP Flood、ICMP Flood等攻击类型的防护，DDoS防御带宽不超过10Gbps；  3.高防DNS服务，当客户通过NS方式接入到防护系统中，即可支持对DNS的DDoS的攻击防护，DNS防御带宽不超过30Gbps；  4.网站缓存加速，包含对静态资源：HTML、JS、图片、CSS等文件的缓存加速；  5.单域名防护套餐包含免费150G正常业务流量；当流量超出时可按需购买安心流量包，若未购买安心流量包导致流量超出将回源处理；  6.正常业务请求并发为：2000QPS，说明：不含CC防护模块。  7.提供安卓&IOS版本慧御云防护平台手机客户端，支持防护配置、报表查看、一键关站、一键回源等操作；  8.包含1个非标端口配置，可支持除80、443之外的端口（21、22、445、3389等不支持）；  9.一年售后服务，防护周期内的防护引擎、防护规则免费升级服务、7x24小时电话支持服务、产品远程技术支持：包含防护接入（NS、CNAME接入咨询、客户网站特殊配置接入咨询）、防护过程中产品问题支持等。 | 4个 |
| 重保只读模块 | 为用户提供1个域名一年的重保只读服务;在重保时期通过该功能的提供，为用户体现网站防篡改价值。通过该功能的部署，可为客户网站提供永久在线功能，确保其不因篡改导致重大影响。 | 1个 |

四、技术参数要求

1.网站安全云防护系统参数要求：

1. 产品形态交付：
2. 提供云端防护账号交付，以 SaaS 服务的方式为用户提供网站安全防护服务；（非硬件盒式WAF、非盒式抗DDoS攻击产品、非集成WAF及抗D功能的防火墙类产品，非虚拟机化WAF。）
3. Web攻击防护：
4. 对SQL注入、跨站攻击、伪造请求攻击、后门植入、上传漏洞攻击、路径遍历等Web漏洞攻击进行防护。
5. 支持服务器隐身，使得黑客无法获取服务器真实IP地址，防止黑客对服务器的各种攻击。
6. 支持HTTPS网站防护。
7. 支持HTTP/HTTPS协议合规性检查，包括畸形报文、HTTP版本检查、报文头缺失、请求方法限制、协议违规等。
8. 支持服务器敏感信息泄露防护，包括服务器类型信息、服务器版本信息、敏感路径信息泄露、网站源码泄露等。
9. 应能识别和阻断SQL注入攻击、Cookie 注入攻击、命令注入、跨站脚本攻击、文件包含攻击、LDAP注入、XPATH注入、爬虫攻击、Struts2命令执行攻击等常见的WEB攻击，防止网站敏感信息泄露或网站内容被恶意篡改。
10. 支持ASP木马、JSP木马、PHP木马、一句话木马、菜刀工具等多种形式的WEB Shell后门的上传防护。
11. 支持对Appscan、Awvs、Pangolin、Burpsuite、Nikto等扫描器的扫描防护。
12. 支持HTTP参数污染、00截断、URL编码绕过、Unicode编码绕过、 ASCII码绕过、字符串拼接绕过、hex编码绕过、大小写混杂字符绕过、多空格绕过、注释串绕过等多种绕过攻击防护。
13. ★支持安全头部设置，避免因安全头部缺失产生安全漏洞。包含X-Frame-Options、X-XSS-Protection、Content-Security-Policy、Strict-Transport-Security、Access-Control-Allow-Origin、X-Content-Type-Options、Secure、HttpOnly。(需提供界面截图并加盖原厂公章)
14. ★支持细粒度的WEB防护配置，至少支持对24大类Web安全漏洞类型对设置白名单，当设置生效后，针对某URL的该类WEB攻击不在防护。(需提供界面截图并加盖原厂公章)
15. ★支持自定义防护页面功能，即当检测到4、5开头的响应码时可以跳转到指定URL以提高服务感受和搜索引擎SEO。(需提供界面截图并加盖原厂公章)
16. DDOS攻击防护：
17. 通过共享带宽对不超过10Gbs的DDoS攻击进行防护;针对的攻击类型包含SYN Flood、ACK Flood、UDP Flood、ICMP Flood等。
18. ★支持对SYN Flood攻击、TCP Flood攻击、ACK Flood攻击、UDP Flood攻击、ICMP Flood攻击、RST Flood攻击等常见的流量型DDOS攻击进行清洗。(需提供界面截图并加盖原厂公章)
19. ★支持对TCP/UDP/IP等类型的畸形报文攻击进行防护、支持对Smurf攻击、Land攻击、Fraggle攻击、Ping of Death攻击等DDOS攻击进行流量清洗。(需提供界面截图并加盖原厂公章)
20. 高防DNS:
21. ★支持智能 DNS 解析。(需提供界面截图并加盖原厂公章)
22. 支持针对DNS的攻击防护，如：DNS Query Flood攻击、DNS replay food攻击等流量型攻击。
23. ★支持网站NS方式接入，即由防护平台提供DNS域名解析，至少提供A记录解析、AAAA记录解析、CNAME记录解析等DNS解析方式。(需提供界面截图并加盖原厂公章)
24. 一键关站：
25. ★支持一键关闭外部对源站的访问，达到一键关站的效果，并可以指定关站响应码（301,302时可以指定跳转URL）或者制定响应页面，默认响应403。(需提供界面截图并加盖原厂公章)
26. CDN加速缓存：
27. 支持对单个URL或者全站进行手工缓存刷新控制的功能。
28. 有全国性的缓存节点机房，按照最小响应时间，最优访问服务等智能缓存算法为用户自动选择缓存节点机房，以提升用户访问效果。
29. 支持数据压缩，即对传输的页面文件进行数据压缩以提高传输效率。
30. 支持永久在线，即在您的页面不可访问时自动提供您的网站快照，避免用户流失，有利于搜索引擎快照收录。
31. 支持缓存兼容性优化，开启后可使PC端和移动端仍可展现不同尺寸的浏览器适配页面。
32. ★支持浏览器缓存加速功能，即将待访问的内容缓存在访问者浏览器上，用户无需请求服务器即可完成对网站页面文件的访问。(需提供界面截图并加盖原厂公章)
33. ★支持URL缓存黑白名单功能，可以对特定URL进行是否缓存进行控制。(需提供界面截图并加盖原厂公章)
34. ★支持对CSS、JS、图片、静态HTML、首页、多媒体文件、文档类型、压缩文件等类型进行缓存。(需提供界面截图并加盖原厂公章)
35. 双栈协议：
36. 支持IPv4、IPv6双协议并存。
37. 源站无需做任何改动，即可支持IPv6访问可达。(需提供界面截图并加盖原厂公章)
38. 访问控制：
39. ★对不同国家和中国的不同省市能否访问保护网站进行访问控制，并能够基于IP地址添加例外访问黑白名单。(需提供界面截图并加盖原厂公章)
40. 对图片、音频、视频、压缩文件、可执行文件等内容进行防盗链访问控制，并允许设置IP地址段例外策略。
41. 对包含特定的 USER-Agent字段内容的访问进行访问控制。
42. ★对在特定时间段内某IP地址或IP地址段是否能够访问特定URL进行访问控制。(需提供界面截图并加盖原厂公章)
43. 扫描防护：
44. ★扫描防护帮助网站自动阻断包含指定特征的访问请求，例如请求源IP在短期内发起多次Web攻击或目录遍历攻击、请求源IP来自常见扫描工具或恶意扫描攻击IP库。(需提供界面截图并加盖原厂公章）
45. 防盗链：
46. ★防止别人或其他站点通过一些技术手段绕过本站的资源展示页面，盗用本站的图片、exe文件、音视频文件、压缩包静态资源。(需提供界面截图并加盖原厂公章）
47. 国密算法适配：
48. ★支持上传国密证书，包含签名证书和加密证书。(需提供界面截图并加盖原厂公章）
49. 移动运维：
50. ★支持安卓/IOS版手机APP运维客户端，可支持手机接入防护、一键关站（一键处置）、一键回源、WEB防火墙开启/关闭、缓存开关设置、账号管理等功能。(需提供界面截图并加盖原厂公章）
51. 安全报表：
52. 支持自定义时间段的报表功能，能直观的显示本周及历史周网站遭受的WEB攻击、CC攻击等攻击情况。
53. 支持月度简报功能，能每月定时向指定邮箱发送月度简报，展示网站安全防护情况。
54. 内容包括拦截漏洞数、本周遭受的CC攻击数、攻击次数最多的IP、受攻击最多的域名，WEB攻击的趋势报表、遭受的CC攻击的趋势报表，WEB攻击方式TopN、遭受CC攻击的URL TopN，WEB攻击源IP全国分布位置，CC攻击源全国分布位置等内容，安全支持PDF、CSV格式导出下载。(需提供界面截图并加盖原厂公章）
55. 产品资质：
56. 具备《计算机软件著作权登记证》，提供证书复印件证明。
57. 具备《网络安全产品认证证书》，提供证书复印件证明。
58. ★具备《信息技术产品安全测试证书》。（需提供证书复印件加盖原厂公章）
59. ★具备全国范围CDN经营，《增值电信业务经营许可证》。（需提供证书复印件加盖原厂公章）

2、重保只读模块参数要求：

1. 可以提前通过爬虫缓存用户网站页面文件，在重保期间即使源站服务器出现WEB攻击、网页被篡改、服务器宕机、网络线路故障、网站服务异常等问题，依然可以通过缓存页面强制对外提供完整的静态缓存页面访问服务。
2. ★用户可以自定义镜像URL、非镜像URL、开始镜像时间、重保时间段等参数，同时可以格式化镜像数据。(需提供界面截图并加盖原厂公章)