防火墙参数要求：

1. ★标准第二代防火墙，三层吞吐量≥2Gbps，应用层吞吐量≥250M；并发连接数≥80W，新建连接≥1.5W；

2. 硬件规格：采用标准X86架构，高度1U，单电源；网络接口≥4个千兆电口。

3. 要求具有独立的漏洞攻击库、实时漏洞库、应用识别库、数据泄露防护库、web应用防护库

4. 支持与安全感知平台进行联动，将日志汇总给安全感知平台进行统一分析和管理，支持通过安全感知平台联动下发访问控制策略

5. 支持根据国家/地区来进行地域访问控制；

6. ▲支持采用无特征AI检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于AI技术的病毒检测报告；（需提供相关功能截图证明并加盖厂商公章）

7. 为保障安全可靠性，避免因设备宕机而引起网络故障，支持主备模式部署，实现高可用；

8. ▲支持对网站黑链进行检测，支持windows和Linux系统下的网页防篡改功能；（需提供相关功能截图证明并加盖厂商公章）

9. DDoS攻击防护：支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护、支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测。

10. 可展示全网实时热点安全事件，并凸显内网已发生的安全事件，点击可跳转至安全事件详情，展现攻击者IP、归属地、严重等级、影响的服务器、攻击事件等信息

11. 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能；

12. ▲支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞；（需提供相关功能截图证明并加盖厂商公章）

13. 提供安全报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，可以查看到有效攻击行为次数和攻击趋势。

14. 厂商是微软安全响应中心计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护（需提供相关证明资料加盖生产厂家公章）

15. 厂商具备计算机信息系统安全专用产品销售许可证；

16. 厂商具备软件开发成熟度CMMI 5级认证，提供证书复印件并加盖厂商公章