办公网络防火墙性能技术要求

1.性能参数：网络层吞吐量：3G，应用层吞吐量：1G，防病毒吞吐量：500M，IPS 吞吐量：400M，全威胁吞吐量：300M，并发连接数：100 万，HTTP 新建连接数：3 万，IPSec VPN 最大接入数：200，IPSec　VPN 吞吐量：200M。

2.硬件参数：规格：1U，内存大小：4G，硬盘容量：64G SSD，含 IPS 模块 3 年，含物联网安全软件模块 3 年，软件升级 3 年，质保 3 年。

3.其他要求：

含安防平台漏扫及漏扫修复后复核漏扫服务。

产品支持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。

产品支持勒索病毒检测与防御功能。

产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。

产品内置不低于 15000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。

产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为。

产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。

支持展示终端资产列表，可查看终端指纹信息和状态，如 IP、MAC、类型、系统、厂商、终端名称、在线状态、审核状态等。

支持 IoT 协议准入，可识别 ONVIF、MQTT 等 IoT 协议基于协议进行应用层准入，仅允许指定协议入网通信，可设置生效时间、新增单次时间计划和循环时间计划等。

支持标准合规准入，可识别 GB/T 28181、GB 35114 等相关国家标准，基于国家标准进行应用层准入，仅允许符合国家标准的终端入网通信。

该防火墙需要将安全日志同步到原有态势感知平台，进行进一步的溯源分析。

产品支持云威胁情报网关技术，通过全球超过 30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。

产品支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发。