**附件1：中心机房防火墙技术需求**

**一、主干网络现状**

1、电信主干链路带宽200兆，移动备用链路带宽200兆。后期应考虑两条链路带宽升级的冗余度。

 **2、**公司内网现有PC用户约300（包含若干服务器），无线用户约300（手机、笔记本电脑），为了分流并充分利用移动链路带宽，无线用户通过双链路网关的策略路由设置走移动链路。

 3、公司在用的软件业务系统有常见的网站、邮件、OA、采购、销售、财务、经销商终端管理等，均需提供外网子公司和驻外办事处的业务访问。公司内部无线终端用户应用较多的有：微信、QQ、腾讯会议、钉钉和短视频访问需求等。

 4、提供SSL VPN管理员远程访问功能。

**二、****设备功能要求**

1、设备需以网桥模式部署到当前公司网络出口，需满足当前网络多条互联网线路防护需求，需支持路由模式、虚拟网线和旁路镜像等部署模式，支持双机模式主备模式部署，满足后续网络结构调整要求。

2、访问控制：支持基于网络区域、国家地区、网络对象、MAC地址、服务、应用、域名等维度进行访问控制策略设置。

3、入侵防御：深度检测并识别各类针对漏洞发起的攻击，抵御常见蠕虫、木马、恶意代码、间谍软件等威胁。

4、Web应用防护：支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等WEB攻击类型进行防护。

5、僵尸网络检测：支持对已被植入远控木马或者病毒等恶意软件的终端进行检测，并快速定位失陷主机。

6、DoS/DDoS攻击防护：支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等DoS/DDoS攻击防护。

7、应用访问控制：支持基于IP、端口、服务、应用、用户、时间等多个维度进行细粒度的一体化应用访问控制规则。

8、带宽管理：基于线路、IP地址、上下行通道进行带宽分配和流量控制，保障公司核心业务带宽正常使用。

9、设备支持在线升级软件系统和各类防护软件包。

**三、****详细技术要求**

1、网络层吞吐量≥10G;应用层吞吐量≥5G; IPS吞吐量≥1G;全威胁吞吐量≥1G;并发连接数≥100万;HTTP新建连接数≥6万；SSL VPN并发接入授权≥5个；

2、产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等。

3、支持高级威胁事件分析，并展示热点事件详情，如持续性攻击、黑链、大面积病毒感染、外发攻击等，并将高危事件推送到运维管理员手机微信端进行预警；

4、产品支持独立的账号安全防护模块，具备事前账号脆弱性、事中账号爆破、事后账号失陷的全生命周期安全防护，在设备界面可以详细展示账号安全相关信息，包括风险业务、风险等级、存在账号入口、存在弱口令、遭受口令爆破、异常登录账号登录。

5、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。

6、产品内置超过4500种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。

7、产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。

8、产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口分析等内容，提供安全策略优化建议。

9、产品应具备独立的勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略，支持在设备首页独立展示勒索风险板块。

10、产品支持SD-WAN组网丢包优化功能，优化互联网场景下丢包严重的问题，改善实时类应用的业务访问体验，满足用户业务稳定访问需求。

11、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。

12、产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。

13、产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。

14、产品内置不低于16000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。

**四、****安装调试要求**

1、因防火墙位于公司网络主干通道，投标方需要提前和计算机信息中心沟通需求和策略配置，利用班后（夜晚）时间加班进行切换调试，以免造成内外网业务中断，影响日常业务工作。

2、保证原有防火墙的各项功能、各项配置均能迁移导入到新防火墙。

3、同时应安排技术人员驻厂2-3天协助计算机信息中心实时监测新防火墙工作状态，第一时间解决防火墙切换后的突发问题，保证正常的内外网业务访问。