防火墙品牌参数要求

为了保障信息系统和网络的安全，结合学校实际情况，借鉴集团其他院校防火墙使用经验，对我校防火墙技术要求及品牌作出如下要求：

技术要求：

1、整机吞吐量：≥20Gbps，网络总带宽≥20Gbps；并发连接数：≥220万，每秒新建连接数：≥15万；设备接口：≥10个千兆电口，≥6个千兆光口，≥2个万兆光口；

2、提供三年IPS特征库、WEB应用防护，网关防病毒，热门威胁库；整机三年硬件质保，软件升级。

3、支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能；（需提供相关功能截图证明）

4、需提供所有接口的多线路接入授权；

5、支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式；支持双机环境下IPSec VPN组网；

6、本次所投产品需提供20个SSL VPN授权，以供校园远程接入使用。

7、支持URL过滤和文件过滤功能，URL过滤支持GET，POST请求过滤和HTTPS网站过滤，文件过滤支持文件上传和下载过滤；

8、为保障防火墙防护质量，防火墙需从云端获取最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；（需提供相关功能截图证明）；

9、支持抵御SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB整站系统漏洞等攻击；10、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；

11、支持在同一个界面对校园内网区域主机以及服务器安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护，支持对所有已被入侵和受控的设备进行风险检测与分析，针对风险可以实现快速响应与处置；支持手动评估功能，自动展示最终的风险；（需提供相关功能截图证明）

品牌要求：根据集团其他院校防火墙使用情况，品牌选择**深信服防火墙**。