**web应用防火墙参数**

数量：2套

2U上架设备，双冗余电源，2个USB口；

管理口配置1个RJ-45 Console口，1个10/100/1000 Base-T带外管理口，1个10/100/1000 Base-T HA口；业务口配置4个具备BYPASS功能的10/100/1000Base-T接口，配置扩展含8个SFP光口插槽；

吞吐率，桥模式/512 bytes（双向流量）不低于6G;

最大并发HTTP连接数（桥模式/Get方式/页面大小64 bytes）不低于400万;

每秒新建HTTP连接数（桥模式/Get方式/页面大小64 bytes）不低于60000;

最大HTTP吞吐量（桥模式/Get方式/页面大小512K）不低于5Gbps;

最大HTTP吞吐量（桥模式/POST方式/页面大小512K）不低于5G;

每秒新建HTTP事务数(桥模式/Get方式/页面大小64 bytes)不低于165000;

最大并发HTTPS连接数(桥模式/Get方式/页面大小64 bytes)不低于20000;

每秒新建HTTPS连接数(桥模式/Get方式/页面大小64 bytes)不低于3600;

最大HTTPS吞吐量（桥模式/Get方式/页面大小512K）不低于900Mbps

最大HTTPS吞吐量（桥模式/POST方式/页面大小512K）不低于900Mbps

每秒新建HTTPS事务数(桥模式/Get方式/页面大小64 bytes)不低于20000;

含嵌入式软件、 Web应用防火墙软件一套以及WAF管理控制中心软件一套，质保期不低于5年免费维修，带5年Web应用防护特征库升级授权。

应支持智能部署，上线WAF设备能够自动感知Web网站IP和端口，支持安装向导式部署，按照该部署方式可直接部署完成；

应具备恶意重定向防护功能、人机识别功能、威胁情报功能、双引擎防护功能；

应具蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断；

应具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截；

应具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置；

应具备API防护功能、网站一键关停功能；

应具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响(要求提供界面截图及盖章)；

应具备客户端访问控制功能，预防恶意客户端进行访问频率的多层次恶意访问；

硬件Web应用防火墙产品通过浪涌（冲击）抗扰度测试、雷击抗扰度测试，可提供报告复印件及盖公章；

WAF通过网络关键设备和网络安全专用产品安全认证证书（千兆）。

包含针对1个重要系统的1次风险评估以及1次渗透测试，出具报告。