互联网出口防火墙技术参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 技术参数说明 | 数量 | 单位 |
| 1 | 互联网出口防火墙 | 1.网络层吞吐量≥20Gbps，应用层吞吐量≥9Gbps，并发连接数≥200万，新建连接数≥20万。1U机架式设备，接口不少于8千兆电口+2万兆光口SFP+（2块万兆多模模块），实配三年入侵防御、防病毒、Web应用防护特征库升级与硬件质保。  2.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。  3.产品支持DNS透明代理功能，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。  4.产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。  5.产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。  6.产品支持多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。  7.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、风险端口风险等内容，提供安全策略优化建议。  8.产品支持Web管理、串口管理、SSH管理等多种不同方式。  9.产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。  10.产品支持多种自定义条件快速查询安全日志，自定义条件至少包括时间、日志类型、安全日志严重等级等条件。  11.产品支持与院内现网的行为管理、数据库审计等安全设备进行联动，将本地产品产生的安全日志等数据上报至防火墙，并在防火墙上进行威胁展示。  12.产品支持对请求报文头的X-Forward-For字段检测，并对非法源IP进行日志记录和联动封锁。  13.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。（提供产品功能截图并加盖厂商公章）  14.产品支持文件目录防护功能，通过对用户账号进行认证，对网站内容的修改行为进行合法性控制。（提供产品功能截图并加盖厂商公章）  15.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。（提供产品功能截图并加盖厂商公章）  16.产品支持对多重压缩文件的病毒检测能力，支持不小于16层压缩文件病毒检测与处置。（提供产品功能截图并加盖厂商公章）  17.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120万种，可识别主机的异常外联行为。（提供产品功能截图并加盖厂商公章）  18.产品支持对常见Web应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过4500种.（提供产品功能截图并加盖厂商公章）  19.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。（提供产品功能截图并加盖厂商公章）  20.产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。（提供产品功能截图并加盖厂商公章）  21.提供原厂商授权及售后服务承诺书。 | 1 | 台 |