**附件1：服务器区防火墙采购项目需求**

**一、采购设备清单**

|  |  |  |
| --- | --- | --- |
| **序号** | **设备名称** | **总数** |
| 1 | 防火墙（含安装实施费用） | 4套 |

**二、参数要求**

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 配置要求 | 实配：千兆电口≥16，万兆光口≥12，40GE接口≥2； SSL VPN并发数≥5000，IPSec VPN隧道≥15000，虚拟防火墙数量≥1000，固态硬盘≥240GB，配置可插拔双电源，冗余风扇；配置三年入侵防御、防病毒、URL过滤、云沙箱升级检测服务； |
|
|
|
|
| 光纤模块要求 | 实配≥6个万兆光模块，2个40GE接口光模块； |
| 性能要求 | 吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万，IPSec吞吐量≥30Gbps，IPS吞吐量≥15Gbps, SSL\_VPN吞吐量≥3Gbps ,SSL代理吞吐量≥6Gbps |
| 策略管控 | 能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、内容安全统一界面进行安全策略配置；  |
| 路由功能 | 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议 |
| 策略路由支持的匹配条件：源IP/目的IP，服务类型，应用类型，用户(组)，入接口，DSCP优先级； |
| 流量控制 | 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等； |
| 支持基于用户，IP的带宽保证；  |
| 支持每IP， 每用户的最大连接数限制，防护服务器； |
| 支持流量整形； |
| 策略管理 | 支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； |
| 支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议； |
| DDoS防护 | 支持HTTP、HTTPS、DNS、SIP等应用层Flood攻击，支持流量自学习功能，可设置自学习时间，并自动生成DDoS防范策略； |
| 支持IP信誉； |
| NAT | 支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； |
| 支持源NAT地址池使用率超限告警； |
| 入侵防御及病毒防护 |  基于特征检测，支持超过8000种特征的攻击检测和防御；（提供功能截图） |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；  |
| 支持恶意域名过滤，实现对C&C进行阻断； |
| 加密流量安全防护 | 支持对HTTPS，POP3S，SMTPS,IMAPS加密流量代理解密后，并进行内容过滤，审计，安全防护； |
| 智能威胁防御 | 支持防火墙与云沙箱，本地沙箱混合联动，敏感文件在本地沙箱检测，普通文件上传到云沙箱，及保护了客户敏感数据有提高了云检测能力；（提供功能截图） |
| 可靠性 | 支持BFD链路检测，支持BFD与VRRP联动实现双机快速切换，支持BFD与OSPF联动实现双机快速切换； |
| 支持HA平滑升级，升级窗口中支持不同版本的软件形成双机热备；  |
| 服务 | 原厂3年7\*10\*ND维保服务 |