**防火墙技术规格**

|  |  |
| --- | --- |
| 功能及指标要求 | 参数要求 |
| 硬件配置要求 | ★≥6个千兆电口，  ★≥2个千兆光口  （满足上述端口情况下留有）扩展槽数量≥1个，至少可扩展至14个电口或6个光口，并含2个高速USB2.0接口，1个RJ45串口，（需提供设备配置的实物图片证明并盖章） |
| 软件授权配置要求 | 3年病毒库升级、3年IPS库升级，3年协议库升级，3年URL库升级 |
| 电源 | 冗余电源 |
| 尺寸 | 标准机架架构 |
| 产品性能 | 最大并发连接数≥260万 |
| 每秒新建连接数≥40K |
| 吞吐量≥8Gbps |
| 至少支持32个虚拟防火墙 |
| IPSec VPN并发隧道≥300个，SSL VPN并发在线用户数≥300个 |
| IPSec VPN性能≥1.2Gbps |
| 系统要求 | 基于专用多核处理器、非X86硬件架构，Web界面可显示处理器核心数，且各核心均参与工作（需提供截图证明并盖章） |
| 要求具备自主研发的安全操作系统，并提供该安全操作系统的软件著作权 |
| 投标产品必须为现有平台销售产品，并在制造商官方网站上能找到相对应的投标产品型号（需提供官网截图及链接并盖章） |
| 部署方式 | 支持二层模式（透明模式）、三层模式（路由和NAT模式）和混合模式 |
| 网络特性 | 支持链路聚合功能  支持接口状态同步  支持三层接口、Acess接口及Trunk接口 |
| 路由支持 | 支持静态路由，等价路由  支持RIP、RIPng；OSPFv2/v3动态路由协议  支持多链路出站负载，支持基于ISP的智能路由选路 |
| 基础功能 | 访问控制策略支持基于源/目的IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式；  能够识别应用协议数超过3000种  支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP或者目的IP进行连接数控制；  支持组播NAT  支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制；  移动终端支持通过IPSec/SSL VPN方式接入，分支支持通过IPSec VPN方式接入 |
| 入侵防护功能 | 入侵防护漏洞规则特征库数量在5000条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号；（需提供截图证明并加盖厂商公章）  支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间；  可提供最新的威胁情报信息，官方网站每周会进行安全通告，能够对新爆发的流行高危漏洞进行预警和自动检测；（需提供界面截图证明并盖章） |
| 病毒防护 | 支持对HTTP，FTP，SMTP，POP3协议进行病毒文件检测；  支持杀毒白名单功能，可以根据URL或者IP进行排除不检测病毒；  检测到病毒后的操作支持阻断，记录杀毒日志； |
| DDoS攻击防护 | 支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护、支持SYN Flood、ICMP Flood、UDP Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测；  支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为； |
| 安全可视化 | 支持对被保护对象的流量进行分析，发现被保护对象的不同业务流量情况，支持生成和导出相关报告；（需提供界面截图证明并盖章）  支持对被保护对象的流量进行分析，通过对流量日志的统计整理，智能生成包过滤策略，提高运维人员工作效率；（需提供界面截图证明并盖章）  支持自定义统计指定IP/用户组/用户/应用在指定时间段内的攻击事件及审计日志等内容，并形成报表；  支持每天/每周/每月自动生成报表，并将报表自动发送到指定邮箱，可以自定义报表内容；  支持报表以HTML、Excel、PDF等格式导出； |
| 安全监测 | 支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能。  支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计。  支持所有安全设备的安全日志汇总，并能够通过时间、严重等级、动作、ip、用户、特征/漏洞ID等多个条件查询过滤日志。  支持通过命令行的方式对数据流进行分析，帮助迅速定位网络故障（需提供界面截图证明并盖章） |
| 高可用性 | 双机支持A/S，A/A方式部署，支持配置同步，会话同步和用户状态同步。  双机模式下，支持主备两台设备采用同一套IP地址，简化配置，节约公网地址 |
| 系统配置 | 支持管理员权限分级，支持安全管理员、审计员、系统管理员三种权限；  支持自动和手动备份，能够保存5个以上的文件，支持配置回滚（需提供界面截图证明并盖章）  支持NTP协议，可作为NTP Server，也可作为Client设备（需提供界面截图证明并盖章）；  支持针对不同策略、不同流量修改TCP，UDP和ICMP协议的连接超时时间；  支持内置规则库的手动/自动更新；  支持邮件和短信告警； |
| 软件成熟度 | ★具备能力成熟度模型集成认证CMMI5 |
| 安全服务能力资质 | ★具备中国通信企业协会颁发的《中国通信企业协会通信网络安全服务能力评定证书（风险评估一级）》  ★具备中国信息安全认证中心颁发的《信息安全应急处理一级》资质  ★具备中国信息安全认证中心颁发的《信息安全风险评估服务一级》资质  ★厂商为中国保密协会成员单位，并具备其颁发的会员单位证书 |
| 公司体系认证资质 | ★具备中国国家认证认可监督管理委员会颁发的《ISO14001：2004（GB/T24001-2004）环境管理体系认证》资质；  ★具备《QC080000有害物质过程管理体系》资质 |

**法定代表人授权委托书**

徐州市口腔医院总务科：

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_系中华人民共和国合法企业，特授权\_\_\_\_\_\_代表我公司（单位）全权办理针对\_\_\_\_\_\_\_\_\_\_\_\_\_\_的投标、参与开标、评标、签约等具体工作，并签署全部有关的文件、协议及合同，但质疑、投诉事项除外。

我公司（单位）对被授权代表的签名负全部责任。

在撤销授权的书面通知送达你处以前，本授权书一直有效，被授权代表签署的所有文件（在授权书有效期内签署的）不因授权的撤销而失效。

被授权代表情况：

姓名： 性别： 电话：

单位名称（盖章）：

法定代表人（签字或盖章）：

附：

法定代表人身份证件复印件

被授权代表身份证件复印件

**承诺书**

（投标人名称）在此承诺：

本公司对本项目\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_所提供的产品均为原厂全新合格产品，保证所递交的投标文件所反映的内容全部真实可靠，否则将承担由此引起的一切后果和相应的法律责任。

投标人（盖章）：

法定代表人或法定代表人授权代表签字或盖章：