主要技术参数参考

★标示核心参数，不满足将视为无效投标。参数中还包括“无标示的普通参数、#标示的重点参数”，均不作为废标项，均是扣分项，扣减分值依次是1分、2分。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 1. 下一代防火墙（4台） | | | |
|  | ★ | 基本要求 | 标准2U机架式设备，冗余电源；  千兆电口≥6个，万兆光口≥4个；  串口≥1个，USB口≥2个  存储容量≥1T；产品为专业的下一代防火墙产品； |
|  | ★ | 性能要求 | 设备网络层吞吐量≥10G，应用层吞吐量≥3Gbps；  并发连接数≥220W，新建连接数≥15W；  SSL VPN最大并发接入数≥1000，SSL最大加密流量≥300Mbps；IPSec VPN推荐接入隧道数≥1000，IPSec VPN加密速度≥300Mbps； |
|  | ★ | 特性授权 | 设备应包含防火墙基本功能（NAT、路由、访问控制ACL、IPSec VPN、抗D、会话控制、用户认证、流控、双机等）、URL过滤、内容安全（杀毒功能）、IPS功能、失陷主机检测、产品联动、风险分析、威胁情报功能。 |
|  |  | 部署方式 | 支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
|  |  | 链路探测 | 具备链路故障检测功能，通过ARP、DNS、PING协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率。（需提供产品功能截图证明） |
|  | # | 网络服务 | 具备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 |
|  |  | 应用控制 | 产品内置应用特征识别库，支持不少于10000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。 |
|  |  | 防病毒 | 支持对HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP协议进行病毒检测和查杀，支持最大16层的压缩文件查杀。（需提供产品功能截图证明） |
|  | # | 具备勒索软件通信防护功能，提供具备CNAS（中国合格评定国家认可委员会）资质的第三方权威机构关于“勒索软件通信防护”产品功能检测报告。 |
|  | # | Web应用防御 | 支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞。（需提供产品功能截图证明） |
|  |  | 支持网站防篡改功能，可防止攻击者非授权修改网站目录文件。（需提供产品功能截图证明） |
|  | # | 支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用。（需提供产品功能截图证明） |
|  | # | 策略生命周期管理 | 支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。（需提供产品功能截图证明） |
|  |  | 高可用性 | 支持主主、主备两种双机模式部署。 |
|  |  | 规则库升级 | 安全规则库支持在线自动升级、手动升级、云端实时升级等多种方式。 |
|  |  | 资质要求 | 要求所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。 |
|  |  | 要求所投产品的生产厂商为国家信息安全漏洞共享平台(CNVD)技术组成员，提供有效证书的复印件。 |
|  | # | 要求所投产品通过ICSA Labs 防火墙品类产品认证，提供有效证明材料。 |
|  |  | 要求所投产品在IDC在2019年 UTM品类市场占有率排名前三，提供有效证明材料。 |
|  |  | 所投产品的生产厂商具备云安全成熟度成熟度模型CS-CMMI 5认证，提供证书复印件并加盖厂商公章。 |
|  |  | 售后服务保障 | 保修期3年，提供原厂商针对本项目的服务授权承诺函正本 |