附件2：技术要求

|  |  |  |
| --- | --- | --- |
| 防火墙 | | |
| 序号 | 指标项 | 指标参数 |
| 1 | ★硬件参数 | 配置≥6个10/100/1000自适应电口，≥2个SFP插槽，1个Console口；三年原厂硬件质保服务，最少支持20个SSL-VPN用户数 |
| 2 | ★功能授权 | 3年应用识别库、病毒防护特征库库升级服务及威胁情报订阅服务 |
| 3 | ★性能规格 | 网络层吞吐≥10G，并发连接≥200万，每秒新建连接数≥10万 |
| 4 | 地址转换 | 所投产品必须支持全面的NAT转换配置，并至少支持FULL\_CONE模式和SYMMETRIC模式 |
| 5 | 入侵防御 | ▲所投产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“Apache文件漏洞”、“Microsoft Exchange Server远程代码执行漏洞”、“Apache ShardingSphere远程代码执行漏洞”、“Windows SMBv3 Client/Server 远程代码执行漏洞”、“WebLogic远程代码执行漏洞”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息；（提供相关证明材料） |
| 所投产品必须支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持在防火墙间谍软件签名库直接查阅攻击的名称、严重性、描述等信息；间谍软件防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的间谍软件防护 |
| 6 | 路由协议 | ▲支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能（提供相关证明材料） |
| 5 | 网络异常感知 | 所投产品必须支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看详情并自动显示关联日志；可基于网络连接、应用名称、威胁事件处置威胁事件； |
| 所投产品必须支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断 |
| 6 | 病毒防护 | 所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |
| 7 | 策略与处置 | 所投产品必须支持针对“应急响应消息”的手动或自动处置，处置方法至少包括基于漏洞的处置和基于威胁情报的处置 |
| 8 | 运维管理 | 所投产品必须提供可明文或加密方式调用的Restful API，并可指定Restful API使用的本地端口；为确保设备管理的安全性，所投产品必须支持限制特定主机调用Restful API，支持定义第三方设备、平台通过调用Restful API ，至少可配置所投设备的访问控制策略、源NAT策略、目的NAT策略、静态路由、高可用以及区域、地址、服务、时间、用户对象等功能 |
| 所投产品集中管理平台支持安全策略下发、设备统一监控、日志管理、告警管理、报表管理、权限管理等功能。 |
| 9 | 联动功能 | 所投产品支持与单位已有的终端管理软件联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址 |
| 10 | 厂商资质 | ▲所投产品具备公安部《计算机信息系安全专用产品销售许可证》；（提供相关证明材料） |
| ▲厂商具备国家信息安全漏洞库CNNVD颁发的连续2年年度最佳支撑单位证书；（提供相关证明材料并加盖厂商公章） |
|  |  |  |
| 上网行为管理 | | |
| 序号 | 指标项 | 指标要求 |
| 1 | ★硬件参数 | 配置≥6个千兆电口。 |
| 2 | ★功能授权 | 专用安全操作系统与上网行为管理标准软件，三年原厂硬件质保服务和三年软件版本与协议库升级。 |
| 3 | ★性能规格 | 并发连接≥12万，每秒新建连接数≥3000 |
| 4 | 部署模式 | 支持网关模式、镜像模式、网桥模式、多路桥接等方式部署 |
| 支持设备模式选择，可以设置为Portal模式实现Portal服务器功能； |
| 5 | 网络支持 | 能够支持IPv6环境下的网址访问审计、生成分析报表等功能；能够在IPv6环境下，正确审计显示用户的IPv6地址 |
| 6 | 安全管理 | 支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对本地计算资源的消耗。 |
| 支持基于云端大数据安全平台，对恶意URL访问进行封堵和记录日志。 |
| 支持与威胁情报大数据平台对接，能够快速识别、封堵失陷主机、记录日志。 |
| 支持通过恶意软件特征检测方式识别失陷主机并记录日志 |
| 支持接收来自运营管理平台的指令 |
| 7 | 应用管理 | 应用协议库包含的应用数量不低于7100种，应用规则总数不低于30000种。 |
| 可以对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用有独立的分类进行识别控制。 |
| 为规避外发类风险，论坛发帖应不低于3000种，网络存储不低于100种，代理隧道不低于100种。 |
| 为覆盖工作无关应用，移动应用不少于1000种，即时消息应不低于150种，虚拟货币交易平台不低于40种； |
| 8 | 网页管理 | 当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈； |
| 不同网页被阻塞后会跳转不同的阻塞页面；支持用户完全自定义 |
| 支持配置免监控域名，用户在认证前即可访问免监控域名 |
| 9 | 邮件管理 | 能够基于发件人、收件人、主题、内容、附件名维度进行过滤、记录、告警；能够支持SSL加密的SMTP邮件审计； |
| 10 | 数据库审计 | ▲可审计、控制Oracle, MySql, SqlServer, PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询等。（提供相关证明材料） |
| 11 | 协议审计 | 通过HTTPS审计功能，可以针对网站分类、证书颁发者、证书所有者、证书有效期等进行审计，加以控制 |
| 通过NETBIOS审计策略对NETBIOS通信、登录名及文件、目录进行审计和控制 |
| ▲通过审计策略可对DNS、SNMP通信内容进行审计和控制（提供相关证明材料） |
| 12 | 流量管理 | 支持多级虚拟通道，可以将物理带宽分成至少7级虚拟通道，合理分配物理带宽资源 |
| 支持基于用户、时间、应用、源IP、目的IP和服务创建流量控制策略 |
| 支持在设置流量策略后，可根据整体线路空闲情况，允许流量通道内的流量突破策略上限，以提升带宽的高使用率；空闲值可自定义 |
| 可以设定OA、邮件、视频会议的基本带宽保障，保障关键应用必要的带宽资源 |
| 13 | 共享接入 | 可基于源IP、用户、位置、终端台数、PC台数、移动台数、阻塞时间和动作，配置多条共享接入策略 |
| 支持配置禁用PC热点开启功能。禁用时PC仍可以使用网络，但是无法通过随身wifi或笔记本自带功能创建热点。 |
| 14 | 系统管理 | 支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制，避免超级管理员权限过大的弊端。系统管理员和审计员的账号创建，权限变更需要审核员审批才能生效。管理员和审计员的操作会形成日志受审核员监督。 |
| 15 | 厂商资质 | ▲所投产品具备公安部《计算机信息系统安全专用产品销售许可证》；（提供相关证明材料） |
| ▲所投产品厂商具备连续六年《应用安全联盟》证书资质。（提供相关证明材料） |