|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **招标参数** | **数量** | **单位** |
| 1 | 下一代防火墙 | 1.网络接口≥8千兆电口+2千兆光口SFP，内存≥4G，提供硬盘≥128G SS； 2.吞吐量≥4G，IPS吞吐量≥600M，并发连接数≥200万，新建连接数≥6万；3年质保服务；提供3年的WEB应用防护识别库、IPS特征库、僵尸网络防护库、实时漏洞分析识别库和URL&应用识别库、威胁情报规则库、提供本地设备网络杀毒功能与更新服务； 3.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; ▲4.支持对不少于9160种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。（需提供功能截图证明材料，并加盖厂商公章) ▲5.支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。（需提供功能截图证明材料，并加盖厂商公章)  ▲6.内置超过4580种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。（需提供功能截图证明材料，并加盖厂商公章)  7.支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型。 8.支持管控非法、违规网站的访问行为，具备海量的URL分类库;支持基于文件传输方式、文件类型等维度的管控策略配置。 威胁展示。（需提供功能截图证明材料及厂商承诺函，并加盖厂商公章) 9.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。 | 1 | 台 |
| 2 | 安全隔离与信息交换系统 | 1.吞吐量≥300Mbps，并发连接数≥10W。“双主机+隔离卡”架构，单主机硬件信息≥6千兆电口，内存≥16GB，硬盘≥960G SSD冗余电源； 2.采用“2+1”结构，内外端机都采用安全的LINUX操作系统，内外端机之间采用FPGA隔离卡及光纤线路连接 3.专有协议通信.设备内外端之间不允许有任何TCP/IP等网络协议，在采用专用隔离卡的基础上，使用API进行原始数据交换，支持各类上层应用的数据摆渡。 4.应用文件传输:支持基于FTP、NFS、SFTP、Samba等方式的文件同步;同一个目录的文件双向同步;备份、复制及移动传输模式 ▲5.数据库同步支持Oracle：11g/12c/19c、SQL Server：2008/2012/2016/2019、MySQL：5/5.6/8、DB2：v9/v11、Sybase：15/16、PostgreSQL：9及国产人大金仓：V7/V8/V8R6、达梦: 7等主流同构异构数据库同步功能，并且支持基于向导式的数据库同步任务配置。(提供截图和证明材料，并加盖原厂公章) ▲6.音视频协议支持国际主流视频控制协议SIP、RTMP、GB28181；音视频数据流单向传输；音视频信令双向交换；(提供截图和证明材料，并加盖原厂公章) 7.自带的防病毒能对来往应用数据进行病毒查杀，有效的保护了来往的数据、文件、音视频、图片的安全。 | 1 | 台 |
| 3 | 日志分析管理系统 | 1.产品不少于6个千兆电口，2个万兆口SFP+，支持单电源， 2U机箱，硬盘容量不少于128G minisata+2T SATA\*2。配置不少于50个日志接入授权，最大可扩展审计主机许可数不少于150，日志处理性能不少于 2500EPS。提供3年硬件质保和软件升级服务。 ▲2.支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、SFTP、文件\文件夹读取、Kafka(提供截图和证明材料，并加盖原厂公章)等多种方式完成日志收集； 3.内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型至少达到200种。 ▲4.支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，同时支持转发已解析日志和原始日志的两种日志（需提供截图证明并加盖原厂商公章）。 5.支持自定义过滤条件检索，支持对模糊ip、多个ip、ip地址段、应用、协议、MAC地址等其他字段精准检索，至少支持AND、OR、NOT三种运算符； 日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量。 ▲6.支持拓扑管理，能够基于拓扑图的资产相关数据信息快速查看资产评分、安全事件分布、告警分布等，支持通过拓扑下钻查看对应资产的关联事件、审计事件、日志数量。（需提供截图证明并加盖原厂商公章）。 7.支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。 8.支持内置日志接入配置指导、典型日志事件介绍、安全经验等，并支持自定义创建增加知识库内容。 9.内置主机安全报表（linux）、主机安全报表（windows）、数据库安全报表、网络设备安全报表、应用安全报表五种；支持自定义时间导出报表。 | 1 | 台 |
| 4 | 统一端点安全管理系统 | 1.产品纯软件交付，包含管理控制中心软件及终端客户端软件，单一管理控制中心可统一管理分别部署在WindowsPC、Windows服务器、Linux服务器以及国产化服务器的客户端软件；授权≥2个服务器端点安全软件；配置3年软件升级； ▲2.基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御.（需提供功能截图证明材料，并加盖厂商公章)  3.具备自研的基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种。 4.支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴。 5.支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和终端账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示。 ▲6.提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。 （需提供功能截图证明材料，并加盖厂商公章)  7.支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz的自启动，可以防止黑客攻击。 8.支持自定义拦截终端软件弹窗，可在终端设置自动拦截骚扰弹窗开关。，支持分组的USB存储是管控防护启用，不允许指定终端分组下的终端使用USB存储设备； 9.支持对终端账户信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、可疑root权限账号、长期未使用账号、夜间登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户 ▲10.支持对Windows停更的系统提供专项防护，包括0day漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能；（需提供截图证明并加盖原厂商公章）； | 1 | 套 |