* **采购需求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **技术参数** | **数量** | **单位** |
| **1** | 安全隔离与信息交换系统 | 1.★应用层吞吐量≥5Gbps，提供2U机架式设备,提供双电源，支持液晶屏；内网接口：千兆电口≥6个，千兆光口≥4个，万兆光口≥2个，Console口≥1个， USB口≥2个，扩展槽位≥1个；外网接口：千兆电口≥6个，千兆光口≥4个，万兆光口≥2个，Console口≥1个， USB口≥2个，扩展槽位≥1个；提供三年硬件质保服务。  2.采用“2+1”模块结构设计，即包括外网主机模块、内网主机模块和隔离交换模块，内外端机为网络协议终点，彻底阻断各种网络协议。支持IPV4/IPV6双栈接入。  3.支持双系统冗余架构，可通过WEB页面进行主备系统切换。  4.▲支持智能备份功能，可灵活设置备份周期，备份个数，为节省磁盘空间占用，当配置无变化时，不进行重复备份。（提供功能截图，加盖厂商公章）  5.支持系统内置调试工具，包括但不限于：trace、connect、tcpdump、ping、arp。  6.文件同步支持FTP、SFTP、SMB、NFS等协议，同时可设置服务器加密方式。  7.用户也可自行上传文件生成特征过滤，过滤文件特征类型。  8.支持数据库同步线程数配置，提升数据库同步性能。  9.支持管理员账户密码可灵活设置密码长度，密码强度，同时可制定哪些特殊字符可以包含在密码中。  10.支持对附件及其附件类型进行过滤控制，邮件内容过滤、文档重建、病毒过滤。  11.支持MySQL、ORACLE、SQLServer、DB2、SYBASE、POSTGRESQL、达梦、神通、人大金仓等数据库的访问  12.安全FTP模块支持病毒扫描文件大小限制、文件类型大小限制、关键字过滤文件大小限制。  13.安全浏览支持域名控制、源端控制、URL过滤、命令过滤、文件大小限制、用户认证。  14.▲支持文件断点续传，同时支持文件并发数量设置。（提供功能截图，加盖厂商公章）  15.支持TCP、UDP定制服务；支持源地址绑定、网络接口地址绑定功能。  16.支持工业SCADA网络OPC协议、MODBUS协议、IEC104协议等。  17.支持28181、DB33标准、具备终端模式。  18.具有auditor账号组，该组内用户登录以后，只可以查看日志相关内容，日志具备外发功能。  19.数据库库名控制、数据库表控制，可以根据用户与数据库表对应关系，进行相应数据库操作过滤。  20.支持双机热备及多机热备功能，内外网主机分别具备独立的HA口。  21.支持异构双引擎病毒模块，可根据用户需求选择需要的病毒引擎。  22.支持云查杀模式，可联动云端文件鉴定中心，预判文件安全风险，防止恶意文件通过网闸进入内网。  23.支持防护阈值设置、防护动作设置，可以根据阈值设置条件，自动触发防护动作。  24.安全FTP支持最大并发连接数、单个IP最大并发数设置，灵活限制数据通道是否在1024以下端口使用。  25.支持tcpflood、udpflood攻击防护。  26.防护动作可自定义永久、时间锁定等。  27.支持设定防护范围，根据地址、端口、每秒最大连接数、每秒包个数等参数。  28.支持按照功能模块，灵活开启告警功能，支持邮件告警、日志告警、SNMP等告警方式。  29.网闸调试技术工程师需熟悉并熟练操作档案管理软件，保证安全隔离与信息交换系统与档案管理软件无缝衔接，必须保证实现用户要求的网络隔离及数据交换功能方可验收付款。 | **1** | **套** |
| **2** | 防火墙 | 1.★吞吐量≥8G，并发连接≥200万，每秒新建连接数≥10万，千兆电口≥8个，千兆光口≥2个，万兆光口≥2个，扩展插槽≥2个，Console口≥1个，提供三年硬件质保服务。提供三年病毒防护特征库升级服务、入侵防御特征库升级服务及威胁情报订阅服务升级服务。  2.▲能够提供VxLanTunnelEndPoint模式接入VxLAN网络，可作为VXLAN二、三层网关；能够提供MAC、VXLANNetworkIdentifie、VxLanTunnelEndPoint静态绑定。（提供功能截图，加盖厂商公章）  3.支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。  4.▲支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器，设备模块至少包括配置、时间、流量、URL过滤、内容过滤、邮件过滤、行为、威胁等，重要性等级至少包括紧急、警报、严重、错误、告警、通知、信息、调试八种。（提供功能截图，加盖厂商公章）  5.能够提供多个物理口基于热备、802.3ad、轮询变为一个逻辑接口，能够提供基于TCP/UDP、源目的MAC地址、IP地址和MAC地址组合实现负载备份。  6.能够提供策略路由、动态多播路由、ISP路由。  7.能够提供源地址和目的地址均为IPv4地址时，能够把目的地址转换成服务器地址，可探测服务器存活状态。  8.能够提供DNS代理功能，可将指定范围内的DNS请求自动重定向至管理员指定的DNS服务器。  9.能够提供IPv6下策略路由、动态路由。  10.能够提供高可靠性配置，包括主备、主主模式；同时能够提供接口联动、接口权重配置、链路状态探测。  11.能够提供基于源目的安全域、源用户、源目的地址、源目的地区、服务、应用、隧道、时间、VLAN等、方式访问控制策略，可对国家和地区对象，能够提供对冗余的策略进行检查。  12.能够提供基于IPv6安全域、IP地址、应用的会话限制，限制内容包括每IP新建和并发、所有IP新建和并发，可设置方向。  13.能够提供基于端口和MAC的802.1x认证。  14.针对邮件能够基于发件人、收件人等关键字的过滤，包括接收、发送、双向类型。  15.能够提供DHCP防护功能。  16.能够提供基于安全域的IP欺骗防护，可关联IP地址和安全域。  17.能够提供对HTTP/SMTP/POP3/IMAP/SMB/FTP六种协议进行反病毒查杀，可上传、下载、双向，能够进行阻断或日志记录。  18.文件过滤能够对压缩文件进行解压查杀，最大实现6层戒解压层数。  19.反病毒功能提供基于MD5的自定义签名、病毒例外。  20.▲按照主机和威胁情报统计失陷主机数、风险主机数、威胁情况、告警信息；并在界面能够查看木马后门、窃密木马、远控木马等威胁的排行；失陷主机统计结果包含主机IP地址、威胁类别、命中数、动作、发生时间、情报来源、资产等。（提供功能截图，加盖厂商公章）  21.能够在一条安全策略中设置行为管控、文件过滤、漏洞防护、邮件过滤、内容过滤、联动终端管控等安全功能选项。  22.实现双系统备份，可记录多个历史配置文件。  23.实现加密的WebUI页面管理以及设备管理界面内的命令行管理。  24.在WEB管理界面内置抓包工具，可设置抓包数量、接口、IP地址，并实现设置表达式。  25.能够提供路由模式、交换模式、旁路模式、桥模式及多种方式混合模式部署。  26.与本项目中配置的终端安全管理系统联动，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。 | **1** | **套** |
| **3** | **日志审计系统** | 1.★事件处理能力≥3000EPS。千兆电口≥6个，Console接口≥1个，硬盘容量≥4T，日志源授权节点≥35个，提供三年硬件质保服务；  2.能够审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙、等）配置日志、运行日志、告警日志等；  3.可对各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等；以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计。  4.可通过syslog、SNMP Trap、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能。  5.设备可自动生成安全运维报告，包括日常日志分析和运维分析报告。  6.实现告警归并，有效抑制重复告警，归并规则可自定义。  7.具备关联规则引擎，关联规则能够引用外部资源，包括地址资源、时间资源、端口资源，以及用户自定义资源。  8.关联规则实现规则嵌套和引用，通过多规则联合，可精确识别复杂安全事件和场景。  9.必须具备单事件关联和多事件关联，能够针对多个不同类型不同来源的安全事件进行综合关联分析。  10.提供对关联规则进行监控，了解该规则命中历史情况分析。  11.关联规则触发后能够通过多种方式进行告警，实现发邮件、发送syslog、执行命令使设备协同工作、发送SNMP Trap等方式发送告警，并能够在动作中引用事件的属性变量  12.提供自定义创建仪表框架，能够根据需要在框架内添加不同的仪表板组件（数值、折线、面积、柱图、饼图、环状图、地图、组件、URL、文本、图片、列表等），实现组件位置自由摆放，组件大小自由拖曳等。  13.可根据运维需要随时调整已创建的仪表板，编辑仪表板展示条件，调整大小和位置、新增组件等；可针对仪表板的任一元素进行下钻，查看原始日志。  14.提供仪表板导入导出功能，实现仪表板共享，可将仪表板共享给其他用户。  15.可将统计结果保存为仪表板、报表和策略。  16.用户可自定义事件搜索查询条件，并可保存为策略，以树形结构进行组织，形成一个搜索分析策略树；每个查询场景都可以查询策略的形式进行存储。  17.用户点击事件任意属性字段，可以该字段为条件对事件进行统计分析，并展示Top 20排序，排序实现正序和倒序  18.▲日志进行归一化处理并可保留原始日志，方便用户对关键日志快速定位和事后取证。（提供功能截图，加盖厂商公章）  19.▲实现对资产IP地址的地理信息进行管理，实现单个IP、IP段设置行政区及经纬度，实现地图显示。（提供功能截图，加盖厂商公章） | **1** | **套** |
| **4** | **终端安全管理系统** | 1.★提供30个客户端授权，需要支持Windows及国产化操作系统，包含防病毒、补丁管理、主机防火墙、终端管控、移动存储管理、终端审计功能，提供三年升级服务。  2.支持定时公告功能，可配置开机显示、周期显示和立即推送。  3.▲管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性。（提供功能截图，加盖厂商公章）  4.支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。  5.支持根据不同分组实现客户端轻量化模式一键切换功能。  6.▲支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。（提供功能截图，加盖厂商公章）  7.支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。  8.支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护。  9.支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。  10.支持对停服系统补丁管理，支持统计即将停服的操作系统，显示操作系统、版本类型、系统位数、停服日期、终端数和升级建议，可直接下发策略进行升级。  11.支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞CVE编号、漏洞CNNVD编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。  12.支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标IP，支持输入IP范围。  13.支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限，并支持生效时间设置。  14.支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。  15.支持终端进程红名单、黑名单、白名单功能。可保护核心进程不被结束。  16.支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理。支持例外白名单添加。  17.▲支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。（提供功能截图，加盖厂商公章）  18.可对通过蓝牙、网页的外发文件进行管控，不断开网络和蓝牙本身的连接  19.支持对网卡进行防护，支持阻止终端修改IP地址、使用动态IP地址、热点创建和IPV6地址使用等，可自定义提示内容和生效时间。  20.支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、取消注册、导出注册列表等。  21.支持移动存储介质外出管理，并可以设置外出使用权限与有效时间。  22.支持对系统性能监控 - 监控系统CPU，内存，磁盘使用情况，可以设置告警阈值。  23.支持对硬件变更监控，监控系统硬件变更情况。  24.支持进程流量监控，可以通过设定阀值和指定进程的方式，监控终端进程流量的信息，可针对异常情况进行断网处理并产生审计日志。  25.监控针对终端的端口异常访问行为进行监控，上报审计日志。  26.监控针对终端的ARP攻击扫描行为进行监控，上报审计日志。 | **1** | **套** |

* **售后及其他服务要求**

对项目售后服务的要求

* 本项目要求本地服务，投标供应商需提供本地注册经营地址包括分公司、办事处、售后服务中心等正规合法机构。
* 在服务期内，应始终通过现场服务、电话服务、远程服务等方式提供快速、高效的维护服务。
* 服务期内须提供所供软件系统的系统BUG修复、系统性能优化等服务。
* 协助提供系统数据备份服务，并定期检验数据备份的有效性。
* 投标人在投标时须提出软件系统及运行环境的定期维护计划，对采购人要求的不定期维护提出响应措施。
* 实施系统维护或修改设计后，应在1周内更新有关技术文档并提交采购人。
* 技术支持方面，提供7×24小时的技术咨询服务，每年提供至少2次对系统运行状况的评估服务，提供每月1次巡视服务，检测软件系统及运行环境的运行情况。
* 故障响应方面，提供7×24小时的故障服务受理；对重大故障提供7×24小时的现场支援；故障服务的响应时间小于1小时；中断时间不能超过3小时。