# 第三章 采购内容及要求

**一、项目建设内容清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物名称 | 数量单位 | 技术要求 |
| 1 | 核心交换机 | 2台 | 详见（二）详细技术参数要求 |
| 2 | 边界防火墙 | 2台 | 详见（二）详细技术参数要求 |
| 3 | 日志审计 | 1台 | 详见（二）详细技术参数要求 |
| 4 | 网闸 | 1台 | 详见（二）详细技术参数要求 |
| 5 | 网络准入管理设备 | 1台 | 详见（二）详细技术参数要求 |
| 6 | VPN设备 | 1台 | 详见（二）详细技术参数要求 |
| 7 | 态势感知探针 | 1台 | 详见（二）详细技术参数要求 |

注：

（1）清单中“货物名称”栏中有注明核心产品的，为本项目核心产品；

（2）清单中如有货物属于财库〔2019〕19号文件“节能产品政府采购品目清单”中节能产品强制采购的，投标人须提供经认证的节能产品（认证机构名单：《市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告》2019年第16号）；

（3）技术要求中要求提供证明材料的，如未注明“原件”，均为提供复印件。要求提供的质保，均为投标时提供承诺，供货时提供相关质保证明材料原件。

**二、详细技术参数要求**

**1、核心交换机**

|  |  |
| --- | --- |
| 指标项 | 技术参数 |
| ▲硬件架构 | 1、主控板槽位数≥2，业务板槽位数≥6，电源模块槽位数≥4 ； |
| ▲设备性能 | 2、交换容量≥100Tbps，转发性能≥76000Mpps； |
| 板卡类型 | 3、支持40G/100G混合板：8\*40G+4\*100G,提供官网证明截图。 |
| 板卡要求 | 4、融合全光方案，全光板卡：16\*25G+32\*10G, POE++,提供官网证明截图。 |
| VxLAN | 5、支持VxLAN ，能够实现基于IPv4/IPv6的VxLAN二三层互通（包括分布式网关或集中式网关），支持VxLAN OAM ping 和 tracert； |
| 智能管理 | ★6、支持内置智能图形化管理功能，对于下联设备具备统一管理的功能能够通过图形化界面对组内设备进行配置文件一键下发；对拓扑内的设备或设备组批量进行版本升级，提供证明材料或第三方权威机构测试报告证明； |
| 基础协议 | 7、支持RIPng、OSPFv3、BGP4+、IS-ISv6协议； |
| 虚拟化 | 8、支持横向虚拟化技术，具备四虚一，支持16条40G堆叠链路，堆叠带宽能达到双向1.28T； |
| QOS | 9、每端口支持8个优先级队列，支持SP、WRR、SP+WRR、WFQ队列调度算法； |
| MPLS | 10、支持MPLS L2VPN、VPLS、L3VPN、TE及MCE功能； |
| 安全插卡 | 11、支持FW防火墙和IPS防火墙业务卡； |
| BFD | 12、支持硬件BFD，支持BFD 3ms最小探测间隔，提供第三方权威机构测试报告证明； |
| 安全特性 | 13、支持256位全端口MACSEC加密 |
| 实际配置 | 14、本次配置双主控双电源，≥48个万兆以太光接口， ≥48个千兆以太电接口，提供≥10个千兆多模光模块，提供≥10个万兆多模光模块，≥2根万兆电缆3m堆叠线；  提供5年针对桐乡市梧桐社区卫生服务中心原厂质保服务； |
| 原厂维保 | 15、整机五年原厂技术支持和原厂保修服务，要求硬件设备保修信息为桐乡市梧桐社区卫生服务中心，可以从原厂查询验证。 |
| 其他 | 提供2台42U服务器机柜 |

**2、边界防火墙**

|  |  |
| --- | --- |
| 指标项 | 技术参数 |
| 硬件规格 | 信创设备；标准2U机箱，冗余电源；≥1T存储容量的企业级硬盘，2个USB接口，支持液晶屏；提供5年入侵防御特征库升级服务和5年病毒防护特征库升级服务以及5年硬件质保。 |
| ▲接口要求 | 板载≥8个千兆电口，≥4个千兆光口，≥8个万兆光口（4个万兆20KM单模模块及光纤跳线，6个万兆多模模块及光纤跳线），≥1个扩展插槽，1个Console口 |
| ▲性能要求 | 网络层吞吐量≥40G，并发连接≥1000万，应用层吞吐≥30G，IPS吞吐量≥10G,AV吞吐量≥15G,每秒新建连接数30万 |
| 路由协议 | 支持IPv4和IPv6双协议栈，具备DNS、DHCP、MAC、静态路由、策略路由、RIP、RIPng、OSPF、OSPFv3、ISIS、BGP、IPSec VPN、SSL VPN、GRE VPN、DS-Lite、6in4隧道、VXLAN、BFD、接口联动等功能。 |
| 访问控制 | 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制。支持基于用户视角的安全访问控制技术，并支持地理区域对象的导入以及重复策略的检查。 |
| 策略分析 | 所投产品必须支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略推荐定可以指定策略流量，分析后自动生成源地址精度更高的安全策略。能够基于源地址精确合并和源地址子网合并，并自动生成策略名称、源对象、目的对象和服务对象。（提供功能截图） |
| 共享上网检测 | ★所投产品必须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（提供功能截图）。 |
| 网元管理 | ★所投产品支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如WAF安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）的方法编排给组内所有网元（提供功能截图）。 |
| 服务链编排 | 所投产品支持灵活的服务链编排功能（服务量管理），支持串接链和旁路链，支持网元组的方向和目的位置设置。（提供功能截图）。 |
| 服务链监控 | ★所投产品支持对编排的流量（服务链）进行监控，以图形化的形式展示出服务链中的流量大小。（提供CNAS认可检测机构出具的针对软件功能的检测报告关键页证明） |
| 病毒防护 | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万。 |
| 入侵防御 | 所投产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID等信息在漏洞攻击特征中体现）详细信息。 |
| SSL解密 | 所投产品必须支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密，同时支持将解密后流量镜像到其他设备进行分析统计。  ★解密后的数据会进入到高级功能中进行扫描，用以实现加密流量的安全防护，（提供CNAS认可检测机构出具的针对软件功能的检测报告关键页证明） |

**3、日志审计**

|  |  |
| --- | --- |
| 指标项 | 技术参数 |
| 性能要求 | 授权资产数≥150个授权永不过期，每秒事务处理数≥4000个。 |
| ▲硬件要求 | 标准2U硬件 ≥1个Console口  USB口： ≥USB2.0\*2  信创芯片+操作系统  网口：千兆电口≥6，千兆光口≥4  内存：≥16G  硬盘：≥6T机械硬盘  电源：国标1+1冗余电源 |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需代码开发。 |
| 日志收集 | 支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。（提供截图证明） |
| 日志分析 | 具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件（提供相关截图证明） |
| 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展。 |
| ★三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件（提供带有CMA或CNAS或CAL标识国家认证认可的第三方检测机构出具检测报告复印件） |
| 应用性能监控  （APM） | 支持监测目标主机的CPU利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息 。（提供带有CMA或CNAS或CAL标识国家认证认可的第三方检测机构出具检测报告复印件） |
| 资产管理 | ★资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。（提供带有CMA或CNAS或CAL标识国家认证认可的第三方检测机构出具检测报告复印件） |
| 部署方式 | 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据。 |

**4、网闸**

|  |  |
| --- | --- |
| 指标项 | 技术参数 |
| 硬件规格 | 硬件配置：2U机箱，内、外主机配置分别如下信创设备，内存 ：8GB，硬盘：64GB +4TB，内、外主机分别配备显示屏，冗余电源；2个USB口；默认包含5年维保。 |
| ▲性能要求 | 网络层吞吐≥1Gbps，应用层吞吐≥950Mbps，应用层并发性能≥10万条，视频并发数≥400路（2M码流） |
| ▲接口要求 | 内网以及外网接口规格各要求：≥6个10/100/1000Base-T端口（含1个管理口，1个HA口，4个业务口），≥4个SFP插槽,≥2个扩展插槽，1个Console口，2个USB口； |
| 硬件架构 | ★支持双系统冗余架构，可通过WEB页面进行主备系统切换，当主系统发生故障或需要升级时可切换至备系统进行工作。(提供证明截图) |
| 安全管理 | 系统管理员具备多种认证方式：支持用户名/口令、Radius、LDAP、浏览器证书、U-KEY等多种认证管理方式。 |
| 系统内置调试工具，包括但不限于：trace、connect、tcpdump、ping、arp。 |
| 便捷运维 | 提供可视化dashboard，在首页可直观展示近7天文件同步个数、数据库同步条数、TCP、UDP请求数、文件流量、数据库流量、TCP、UDP流量情况。 |
| 文件交换 | 具备文件断点续传，同时支持文件并发数量设置，大幅度提升文件传输性能，充分利用硬件资源。 |
| ★文件交换支持传送优先级，可根据文件大小、新旧、文件名、后缀、缓时传输等多种方式进行优先级排序传输。(提供证明截图) |
| 数据库同步 | ★数据库同步支持无客户端方式同步，无客户端方式同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安全任何第三方软件，可以在网闸系统上完成数据库同步配置）。(提供证明截图) |
| 数据库访问 | ★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。（提供证明截图） |
| TCP/UDP访问 | 支持TCP、UDP业务数据统计，可按照秒、分钟展示发送速率、接受速率、连接数，并且可按照图表进行展示。 |
| 安全防护 | 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，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，提供高中低不同级别阻断策略。（提供证明截图） |

**5、网络准入管理设备**

|  |  |
| --- | --- |
| 指标项 | 技术参数 |
| 性能要求 | 支持最高并发1万并发用户上网准入请求，含≥1000个授权数授权永不过期。 |
| ▲硬件要求 | 2U机架式，2\*16核32线程CPU，≥16G\*8内存，≥8T\*2机械硬盘，标配≥2个千兆电口，≥2个万兆光口，800W冗余电源。 |
| 安全可视化 | 支持运维总览视图可查看性能监控指标、网关时延趋势、主机拓扑、接入情况、API调用时延、应用访问趋势、调用段访问趋势等信息，并是系统主机点击进入二级主机概览界面显示主机运维详情。  ★支持故障总览视图覆盖账号、终端、主机、自身服务、外部服务5大方面故障监控，可通过图表显示故障分类、账故障趋势和故障列表，并是通过点击分类信息进入二级页面，查看对应信息的总览和故障信息等数据。 （提供截图证明） |
| 用户管理 | 具备账户权限三权分立模式，可对系统管理员、安全保密管理员、安全审计员三类账户的权限进行精细化管控，审计账户运维操作。  支持自定义创建用户角色并定义角色权限，支持自定义扩展用户账号字段，基础包括：用户名、姓名、邮箱、手机号、身份证号、备注等。（提供截图证明） |
| 组织管理 | 支持对单个部门组织设置门户地址，实现按照部门分配不同的门户地址，支持自定义扩展组织机构字段，基础包括：组织名称、责任人、联系人、联系人电话等。（提供截图证明） |
| 账号源 | 支持与第三方身份目录对接实现身份信息同步，内置与LDAP、钉钉、浙政钉（仅浙江使用）、企业微信、飞书、派拉、阿里云盾IDaaS的同步模板，提供定制对接能力。（提供截图证明） |
| 消息通知 | ★支持为各种场景配置短信（阿里云短信、大汉三通、腾讯云短信、亿美短信、联通短信、天翼终端短信）、钉钉、邮箱发送通道，用于身份认证、忘记密码、otp认证、运维告警、用户账号过期、用户密码通知等信息的发送（提供截图证明） |
| 级联部署 | 支持查看下级中心数量、部署终端数量、全网在线数量、终端在线率、授权使用率等数据。  支持连接上级中心、支持自定义上级中心连接地址与端口。  支持查看下级列表、支持对下级中心的连接请求进行审批。  支持设置级联时上下级数据传输速度、支持设置级联时下级下载升级包的速率。 |
| 模块管理 | 支持将agent拆分成多个独立的客户端模块，各模块之间独立维护；新的能力模块支持以升级的形式同步到终端，不用重新安装agent。（提供截图证明） |
| 身份认证 | 集成账号管理和认证管理功能，支持多因子认证方式，实现针对不同组织采用不同认证方式，支持针对终端和用户风险行为分析，作为上网动态准入条件，支持在终端和用户存在风险行为时，进行用户下线，能够及时回收网络准入权限，有效保护网络安全。（提供截图证明） |

**6、VPN设备**

|  |  |
| --- | --- |
| 指标项 | 技术参数 |
| ▲设备规格要求 | IPSEC性能参数：加密最大流量（Mbps）≥120，理论并发隧道数（Tunnel）≥300；SSL性能参数：最大理论加密流量（Mbps）≥600，最大理论建议并发用户数≥1200。  硬件参数：规格≥1U，内存大小≥16G，硬盘容量≥480G SSD，电源：冗余电源，接口≥6千兆电口+4千兆光口SFP。  需提供不少于50套零信任接入授权。 |
| 网络部署 | 为了满足灵活部署的要求，综合网关应支持IPV4/IPV6双栈网络IP配置，可自主选择配置LAN口或WAN口。 |
| 应用打开方式 | 支持配置点击工作台的业务应用即可直接拉起对应的CS程序进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持统信UOS、麒麟kylin、中科方德等操作系统；（需提供产品功能截图） |
| 客户端国产终端兼容性 | ★为了保障用户在国产化终端上的正常业务访问，零信任客户端应兼容主流国产硬件CPU的国产操作系统终端，需提供国产操作系统与零信任厂商的兼容性证明，包括但不限于麒麟V10×龙芯、麒麟V10×龙芯LoongArch、麒麟V10×飞腾、麒麟V10×鲲鹏、麒麟V10×兆芯、麒麟V10×海光、麒麟V10×海思麒麟；统信V20×龙芯（3A3000、3A4000）、统信V20×龙芯（3A5000）、统信V20×飞腾、统信V20×鲲鹏、统信V20×海光、统信V20×兆芯、中科方德×飞腾、中科方德×海光、中科方德×兆芯、中科方德×龙芯3A5000等。 |
| 自适应认证 | 为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、账号在该地点首次登录、账号在新地点登录、账号在非常用地点登录、闲置帐号登录、弱密码登录、异常时间登录等。 |
| 用户密码安全规则支持自定义 | 1、支持管理员自定义用户密码组合方式是否需要包含字母、数字、特殊字符；2、支持管理员根据情况自行选择密码能否包含用户名、新密码不能与历史前N次密码重复、密码不能包含连续重复字符的次数、密码能否包含键盘连续排序字符等安全规则。 |
| 服务隐身 | 1、为了最大程度缩小网络、业务暴露面，零信任平台需提供单包授权能力（SPA），支持UDP+TCP组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口，不会出现敲门放大漏洞。  ★2、PC端和移动端均支持通过安全码激活客户端为授权客户端，从而可进行SPA敲门和连接，安全码支持共享码、一人一码和一次一码等多种模式，支持短信分发安全码，保障业务的安全性。不同安全码模式均应同时支持PC端和移动端使用。（需提供产品功能截图及第三方权威检测机构出具的带CNAS标识的检测报告证明） |
| 虚拟IP | ★支持共享、独享虚拟IP池模式，以虚拟IP方式，访问真实的业务系统，虚拟IP支持IPv4、IPv6地址，当虚拟IP池分配超过一定比例时，零信任系统可向管理员发送邮件告警，支持将虚拟IP分配日志通过第三方syslog的方式同步到网络威胁分析设备。（需提供产品功能截图及第三方权威检测机构出具的带CNAS标识的检测报告证明） |
| 设备巡检 | 零信任支持对设备自身的安全状态和策略配置进行巡检、打分，统计检查的正常项、异常项和告警项，支持在设备上查看及下载巡检报告。报告应至少包含检测项、检查状态、存在的问题描述、建议改进措施等。 |

**7、态势感知-探针**

|  |  |
| --- | --- |
| 指标项 | 技术参数 |
| ▲硬件与性能要求 | 本次服务要求提供流量采集服务，组件以硬件形式提供。规格要求：吞吐性能≥1Gbps。  硬件参数：规格≥1U，内存大小≥8G，硬盘容量≥128G SSD，电源：单电源，接口配置不少于6千兆电口+4千兆光口SFP。 |
| 部署要求 | ★为保障区域医疗安全运营一体化，要求此次提供设备可以无缝对接桐乡市卫生健康局统一安全运维平台。（需提供厂商盖章证明材料） |
| 违规访问 | 支持IP，IP组，服务，访问时间等定义违规访问策略，主动建立针对性的业务和应用访问逻辑规则，针对目标IP（组）已开放的服务，白名单策略只允许白名单里的IP（组）在指定的时间内访问，其他时间或其他IP的访问均被视为违规，黑名单策略禁止黑名单里的IP（组）在指定的时间内访问，否则将被视为违规。 |
| WEB智能检测 | ★支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等自定义配置启用，针对命令注入检测、SQL注入检测等类型支持自定义高检出、低误报模式。（需提供截图证明） |
| 网站攻击检测 | 支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞、自定义WAF规则、WAF云防护等网站攻击检测。 |
| 漏洞利用攻击检测 | 支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Media漏洞攻击、Network Device、Shellcode漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击、IPS云防护等服务漏洞攻击检测。（需提供截图证明） |
| 支持Application漏洞攻击、File漏洞攻击、Shellcode漏洞攻击、System漏洞利用攻击、Web Activex、Web Browser、IPS云防护等客户端漏洞攻击检测。 |
| 旁路阻断 | 支持基于IP和域名的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断，支持24小时/7天/最近30天/永久或者自定义时间阻断威胁。（需提供截图证明） |
| 日志传输模式 | ★支持5种场景的日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。（需提供截图证明） |

**三、其他要求**

|  |  |
| --- | --- |
| 内容 | 说明与要求 |
| 项目工期 | 合同签订之日起 15日历天内完成供货、安装及调试完毕 |
| 安装、调试要求 | 1、按照采购单位的要求对原有设备进行搬迁，并正常运行；  2、对机房线路进行整理，规范、清晰的做好分类标记；  3、对所有设备进行安装和调试，以确保能够稳定运行。 |
| 质保 | 1、要求所有产品质保五年。  质保期从项目验收通过之日起计算。保修期内，设备硬件故障，免费维修，对不能修复的设备负责免费更换。如有投标货物原厂免费质保期或投标人另行承诺的免费质保期超过五年的，以原厂免费质保期或投标人另行承诺的免费质保期为准。投标人必须保证所有设备为原装正规渠道行货，序列号可查，有原厂服务，如有需要则提供正规渠道等证明,所有产品均原包装到用户，当场开箱验货,并无条件接收整个项目监理的统一管理,同时提供该设备相关技术参数的说明。如不符招标书技术要求的，采购人有权要求由采购人指定的第三方作检测并有权退货，相关检测费用及由退货产生的一切后果由中标人承担。  2、保修期内，能够提供 7x24 小时售后服务。  系统有故障时，维修人员须12小时内响应，24小时内及时赶到现场解除故障;不能修复的，用同类型设备替换，以保障系统正常运行。在质保期内，与质保和维修等相关的费用由中标人负责。  出现故障后，中标供应商如未按上述要求进行响应，采购人可以采取必要的补救措施，由此产生的风险和费用将由中标供应商承担。 |
| 付款方式 | 合同签订后7个工作日内付合同金额40%的预付款，项目验收通过后30日历天内付清余款 |
| 招标代理费 | 本项目招标代理费为7758元，中标人在领取中标通知书时以电汇或转账方式汇入代理公司账户，各供应商在报价中自行考虑(收款单位:浙江博宏工程管理咨询有限公司桐乡分公司;开户银行:中国建设银行股份有限公司桐乡支行;银行账号33001637227053005286) |