**前注：**

1.根据《政府采购进口产品管理办法》及政府采购管理部门的相关规定，下列采购需求中标注进口产品的货物均已履行相关论证手续，经核准采购进口产品，但不限制满足招标文件要求的国内产品参与竞争。未标注进口产品的货物均为拒绝采购进口产品。

2.政府采购政策（包括但不限于下列具体政策要求）：

（1）如属于《节能产品政府采购品目清单》中政府强制采购的节能产品，则投标人所投产品须具有市场监管总局公布的《参与实施政府采购节能产品认证机构目录》中的认证机构出具的、处于有效期内的节能产品认证证书。

（2）如涉及商品包装和快递包装，投标人应当执行《关于印发〈商品包装政府采购需求标准（试行）〉、〈快递包装政府采购需求标准（试行）〉的通知》（财办库〔2020〕123号）、《安徽省财政厅关于贯彻落实政府绿色采购有关政策的通知》（皖财购〔2023〕853号）的要求，提供符合需求标准的绿色包装、绿色运输，同时，采购人将对包装材料和运输环节作为履约验收条款进行验收。

3.如采购人允许采用分包方式履行合同的，应当明确可以分包履行的相关内容。

4.下列采购需求中：标注▲的产品（核心产品），投标人在投标文件《主要中标标的承诺函》中填写名称、品牌、规格、型号、数量、单价等信息。

**一、采购需求前附表**

|  |  |  |
| --- | --- | --- |
| **序号** | **条款名称** | **内容、说明与要求** |
| 1 | 付款方式 | 合同生效并具备实施条件 5 个工作日内，采购人付至合同价的70%（中标人须提供等额预付款担保），项目经验收合格且相关资料齐备己移交后，一次性付清合同价款。  注：  （1）中标人未按规定提供预付款担保的，视为放弃预付款；  （2）预付款担保要求：如采用银行保函、担保机构出具的保函（担保机构担保）均须满足无条件见索即付条件。 |
| 2 | 供货及安装地点 | 安徽省体育局训练基地管理中心，具体按采购人指定地点。 |
| 3 | 供货及安装期限 | 自合同生效之日起，30个日历日内完成供货、安装、调试等所有工作内容。 |
| 4 | 免费质保期 | 采购需求未明确的，质量保证期为验收合格之日起3年；采购需求中明确的按采购需求执行。 |

**二、货物需求**

**（一）指标重要性表述：**

|  |  |  |
| --- | --- | --- |
| **标识重要性** | **标识符号** | **代表意思** |
| 关键指标项 | **★** | 废标项，不满足作无效标处理 |
| 重要指标项 | ■ | 评分项，详见评分办法 |
| 无标识项 | / | 5条（含）以上不满足的，投标无效 |
| 注：  （1）如某项标识中包含多条技术参数或要求，则该项标识所含内容均需满足或优于招标文件要求，否则不予认可。  （2）“所属行业”栏标注为“/”的项为所投设备配套的工程或服务，无需在《中小企业声明函》 中列明。 | | |

（二）**技术参数及要求**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **技术参数及要求** | **数量** | **所属**  **行业** | **是否为核心产品** | **备注** |
| 1 | 下一代防火墙(包含入侵防御和防病毒模块) | 1.标准1U机架设备，吞吐量≥35G，应用层吞吐量≥20G，IPS吞吐量≥2.5G，并发连接数≥410万，新建连接数≥18万，接口≥16千兆电口、≥6万兆光口。  2.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。  3.■产品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**（投标文件中提供产品功能截图证明）**。  4.产品支持对不少于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。  5.产品支持多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。  6.■产品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**（投标文件中提供产品功能截图证明）**。  7.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生**（投标文件中提供产品功能截图证明）**。  8.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。 | 1台 | 软件与信息传输业 | 否 |  |
| 2 | VPN | 1.标准1U机架设备，最大理论加密流量（Mbps）≥300，最大理论并发用户数≥400，最大理论https并发连接数（个）≥15000，理论https新建连接数（个/秒）≥60，接口≥6千兆电口、≥2千兆光口。可提供不少于50个零信任接入授权。  2.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。  3.■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Windows、macOS、统信UOS、麒麟kylin、Ubuntu等主流操作系统；针对Windows系统，还应支持拉起CS应用时携带启动参数，自动访问管理员设定的地址**（投标文件中提供产品功能截图证明）**。  4.对于一些主要在主站点中点击使用的子站点WEB业务系统，且子站点跟主站点业务系统权限一致的场景，为简化管理员配置，零信任系统应支持开启依赖站点功能。为方便业务快速上线，还应支持自动采集站点功能对依赖站点进行梳理。  5.■为方便管理员统筹查看管理零信任系统的整体运行状态，支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告**（投标文件中提供产品功能截图证明）**。  6.在零信任控制台封装的应用需支持单点登录录制功能，自动为APP用户填入管理员配置的接入地址及用户名账号等信息。  7.■应支持检查设备是否开启自动备份功能**（投标文件中提供产品功能截图证明）**。 | 1台 | 软件与信息传输业 | 否 |  |
| 3 | 终端威胁防御系统 | 1.本次要求产品纯软交付。包括控制平台，并提供不少于4个服务器授权。  2.交付内容包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；同时也支持硬件管理平台交付。  3.■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**（投标文件中提供产品功能截图证明）**。  4.支持基于系统内置弱密码字典和自定义弱密码字典的检查功能，弱密码检测支持至少包括SSH、RDP、MySQL、Tomcat、Redis等应用类型，可按照空密码、自定义弱密码、密码长度小于8、字符种类小于3等常见弱密码类型进行分类查看。  5.具备基于本地缓存信誉检测与全网信誉检测，构建全网信誉库的检测引擎，做到内网一台威胁，全网感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率，减少终端资源开销。  6.支持禁止黑客工具启动，包含但不限于：xuetr、ProcessHacker、PCHunte、Mimikatz等自启动，可以防止黑客攻击。  7.可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低3种防护级别。  8.■支持windows服务器RDP远程登录保护，可开启RDP远程登录二次认证，以防止黑客对服务器的入侵**（投标文件中提供产品功能截图证明）**。  9.统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RSSH、SMB和MSSQL类型进行封堵并自定义爆破阈值，可对封停时间进行自设置。 | 1套 | 软件与信息传输业 | 否 |  |
| 4 | 堡垒机 | 1.标准1U机架设备，包含运维授权数≥50，最大可扩展资产数≥150，图形运维最大并发数≥100，字符运维最大并发数≥200，内存≥8G，至少具备6千兆电口。  2.支持字符协议：SSHv1、SSHv2、TELNET，图形协议：RDP、VNC，文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板等。  3.■支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入**（投标文件中提供产品功能截图证明）**。  4.用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、短信认证（移动云mas)、AD域/LADP认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证。  5.内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴。  6.支持生成授权报表和可访问外部资源报表，报表详细展示用户和资源的授权关系，并提供EXCEL、WORD、PDF、HTML等格式导出。  7.■支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作**（投标文件中提供产品功能截图证明）**。  8.全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计。  9.支持双人复核登录，登录时必须经过第二人授权后才能登录，第二人可通过远程授权或同终端授权两种方式实现授权。 | 1台 | 工业 | 否 |  |
| 5 | ▲WEB应用防火墙(WAF) | 1.标准1U机架设备，网络层吞吐量≥20G，HTTP应用层吞吐量≥800M，HTTP新建连接数≥10万，HTTP并发连接数≥350万，内存≥8G，硬盘容量≥128G SSD，接口≥8千兆电口、≥2万兆光口。  2.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。  3.产品内置超过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。  4.■产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁**（投标文件中提供产品功能截图证明）**。  5.产品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。  6.产品支持X-Forworded-For字段检测，并对非法源IP进行日志记录和联动封锁。  7.产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。 | 1台 | 软件与信息传输业 | 是 |  |
| 6 | 日志审计 | 1.标准2U机架设备，默认包含主机审计许可证书数量≥50，可用存储量≥2TB，平均每秒处理日志数（eps）≥2500，接口≥6千兆电口、≥2万兆光口（含万兆光模块）。  2.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于800种日志对象的日志数据采集。  3.■持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射，以满足除内置解析规则之外未被覆盖的日志类型的解析**（投标文件中提供产品功能截图证明）**。  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**（投标文件中提供产品功能截图证明）**。  5.支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析。  6.支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达不低于350条，支持自定义关联分析规则。  7.支持TLS加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量  8.■支持POC测试工具一键生成数据,验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险**（投标文件中提供产品功能截图证明）**。（  9.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。 | 1台 | 工业 | 否 |  |
| 7 | 物理环境 | 1. 监控1套  （1）分辨率: 最低支持1080p全高清；  （2）像素：400万；  （3）维护服务：一年内免费保修。 | 1套 | 工业 | 否 |  |
| 2. 门禁1套  （1）支持卡类型:支持密码、IC卡、生物识别（指纹、面部识别等）；  （2）工作温度: -20℃至60℃，适合大多数气候环境；  （3）联网能力:支持TCP/IP及WIFI联网方式；  （4）提供一年质保。 |
| 3. 动环监控系统1套  （1）数字化温湿一体、温度精度<0.5℃、湿度精度<3%RH、前端液晶显示，RS485上联；  光电离子型烟雾探测器，光学米宫设计、采用低功耗CMOS微处理器、具有手动测试、手动复位功能、吊顶安装；  （2）漏水传感器在软件3D图中实时显示，报警出现时在软件相应位置变红、设置漏水报警阈值等；  （3）通过精密空调提供的通讯接口及通讯协议进行二次解析整合监控、监控空调的风机、压缩机、加湿器、出回风温度等；  （4）机房动环监控系统主平台软件；BS架构，远程WEB管理。支持云端接入、短信报警。具备集信息采集、分析统计、数据报表、权限管理、策略执行、自动控制、远程通信、智能告警（电话、短信、邮件、语音广播、声光报警）等综合服务。 |
| 8 | 安全服务 | **★**1.质保期限内（3年），每月开展1次的安全检查服务，内容包含：渗透测试、配置核查、漏洞扫描等；每年一次网络安全培训**（投标文件中提供书面承诺）**。  **★**2.质保期限内（3年），提供7\*24小时的信息安全应急响应服务，接到信息安全事件通知后，在30分钟进行应急响应，并提供包括现场服务、远程技术支持在内的各种必要应急响应手段。发生异常问题，1小时内完成异常问题上报，处理完后再出具正式报告**（投标文件中提供书面承诺）**。  **★**3.质保期限内（3年），重要时期（如国庆、两会、省市级攻防演练等）提供7\*24小时网络安全值守工作**（投标文件中提供书面承诺）**。 | 1项 | / | / |  |

**三、报价要求**

本项目报投标总价，并同时报出分项报价，投标总价包含完成所投项目所产生的一切费用，投标人自行考虑报价风险。

**四、备品备件及专用工具**

1.备品备件：中标人提供能够满足质量保证期内的设备维修要求的备品备件，备品备件应是新品。

2.专用工具：中标人提供设备安装、调试、验收、维修、保养所必要的专用工具、仪器、仪表等工具。

**五、安装调试、验收试验及质量保证**

1.中标人在设备安装地点负责安装、调试。

2.具体设备验收标准和程序按采购人要求执行，下列验收程序可参照执行：

2.1 采购人和相关部门按照招标文件和投标文件承诺进行验收。招标文件没有规定和投标文件没有相应承诺的，按照下列原则进行验收：有国家标准的按照国家标准验收，没有国家标准的按行业标准验收，无行业标准的按地方或企业标准验收，中标人予以配合。涉及需要由质检或行业主管部门验收的项目，采购人须约请相关部门和专家参加项目验收。所有需要质检部门进行检测才能使用的设备，投标报价中必须包含首次检测费用。

2.2货物在验收时，中标人应提供发票、制造厂家出具的产品合格证书、装箱清单等,涉及进口的部件须提供中国海关进口货物报关单、完税证明及商检证明等材料；提供有关货物的保养修理所需的各种随机工具及全部有关技术文件（外文应提供中文翻译资料，下同）、操作使用说明书、质保书、保修证明、维护手册及技术性指导资料以及根据中国相关法律规定制造、销售报价货物（包括主要部件和材料）所必备的各种证书 (如产品质量检验报告、国家相关检测机构出具的检验报告等）等文件汇集成册交付采购人和应由中标人提供的必要文件。

2.3 中标人应根据采购人使用单位的技术要求提供相应的产品。由中标人所提供的设备部件间的连线和插接件均应视为设备内部器件，包含在相应的设备之中。

2.4 运行测试及最终验收。在系统安装、调试结束后，采购人对其进行全面的测试，对测试中暴露出来的问题，中标人应及时进行整改，系统最终测试完毕经验收合格后，采购人应向中标人签发最终验收证明。

2.5 中标人应向采购人提供安装调试过程中的各种文档资料,以便采购人今后能掌握操作和维护方法。依据合同与合同有关条件、本招标文件的技术规范、系统配置要求、设备技术文件和系统说明书，以及国家和省部级等要求进行验收，验收分为预验收和竣工验收。

3.如设备在验收时有一个或多个指标未能达到要求而属于中标人责任时，则中标人自费采取有效措施，在规定时间内使之达到保证指标。如在规定的时间内仍达不到合格标准时，则中标人应向采购人赔偿。

**六、包装运输**

1.中标人负责设备包装、办理运输和保险，将设备安全运抵交货地点。

2.设备制造完成并通过试验后应及时包装，否则应得到切实的保护，确保其不受污损。

3.在包装箱外应标明采购人的订货号、发货号。

4.各种包装应能确保各零部件在运输过程中不致遭到损坏、丢失、变形、受潮和腐蚀。

5.包装箱上应有明显的包装储运图示标志。

6.整体产品或分别运输的部件都要适应运输和装载的要求。

7.随产品提供的技术资料应完整无缺。

**七、技术培训**

1.为使合同设备能正常安装和运行，由中标人提供相应的技术培训，并免收采购人培训费用。培训内容应与工程进度相一致。

2.培训的时间、人数、地点等具体内容由双方商定，内容至少包括：设备原理、使用、维护、运行操作、常见故障处理等。

3.采购需求里有特别规定的，以采购需求中的需求为准。

**八、质保及售后服务**

1.自双方签订《验收报告》起进入免费质保期。

2.在质保期间内，非采购人过失和故意并且在正常使用的情况下发现商品有缺陷，中标人将免费修理或替换该设备；在质保期间内，非采购人过失和故意并且在正常使用的情况下设备发生故障，中标人应及时提供免费服务。