序号	名称	功能参数	数量/单位	单价（元）	总价（元）
1	棚面	1. 提供不少于 22 ㎡的棚面防尘处理，采用氟碳或粉末喷涂，漆面牢固，表面不起尘、耐酸、碱、盐、油类等的腐蚀、耐老化、耐磨、耐压，耐冲击、不吸附灰尘，有较强的自洁能力，以满足计算机设备对尘埃及防火的要求； 2. 提供不少于 22 ㎡的微孔铝天花板，铝天花板规格为 600mm×600mm，配备防尘布； 3. 提供天花板配件，包括但不限于螺帽、螺丝、三角骨连接器、膨胀管、大吊、挂钩、三角龙骨、主龙骨、吊杆等； 4. 提供棚面施工所需的辅助材料。	1 套	10300	10300
2	地面	1. 提供不少于 23 ㎡的地面找平处理，便于铺设防静电地板； 2. 提供不少于 23 ㎡的地板支架，支架高度不低于 20cm； 3. 提供不少于 23 ㎡全钢防静电地板，防静电地板规格为 600mm×600mm，防静电地板厚度不小于 32mm，陶瓷高耐磨贴面，集中载荷≥2950N、极限载荷≥8850N、均布载荷≥12500N/㎡，抗静电性能系统电阻 106--1098Ω，防火 A 级； 4. 提供不少于 20m 的地板边支架，支架进行镀锌防腐处理； 5. 提供防静电地板加固处理，包括门口压边处理及踏步处理，砌块砖基础，混凝土找平压光，防静电地板铺装，不锈钢收口； 6. 提供不少于 10m 的空调防水堰，高度不低于 100mm，铝合金材质； 7. 提供 1 个设备承重底座，定制型 50*50*6 角钢焊接； 8. 提供不少于 20m 的踢脚线，高度不小于 100mm，铝合金材质； 9. 提供地面施工所需的辅助材料。	1 套	32000	32000
3	墙面	1. 提供不少于 56 ㎡的墙面、柱面基础处理及找平； 2. 提供不少于 56 ㎡的墙面喷涂或粉刷防尘漆； 3. 提供墙面施工所需的辅助材料。	1 套	10000	10000
4	接地	1. 提供不少于 20m 的 30mm×3mm 高纯度铜排，铜排纯度不低于 99.97%，含绝缘端子及安	1 套	13000	13000

		装辅材； 2. 提供 1 套等电位接地端子箱； 3. 提供不少于 140m 的 ZR-BVR-6mm²，用于金属吊顶、龙骨、金属墙面板、地板框架连接； 4. 提供不少于 30m 的 ZR-BVR-16mm²，用于机柜等外壳连接； 5. 提供不少于 10m 的 ZR-BVR-50mm²，用于接地主体连接； 6. 提供接地施工所需的辅助材料。			
5	配电	1. 提供不少于 20m 的镀锌桥架，规格为 200mm×100mm； 2. 提供不少于 100m 的镀锌电线管及配件等； 3. 提供 PDU、配电箱电缆； 4. 提供配电施工所需的辅助材料。	1 套	12000	12000
6	门禁监控	1. 提供 1 套机房内监控系统，不低于 200 万像素，POE 供电； 2. 提供 1 套面部识别、指纹及密码三合一的门禁系统，配套锁具。	1 套	4500	4500
7	气体灭火	1. 提供 1 套柜式七氟丙烷灭火装置，包含机柜、钢瓶、启动阀组、压力表、压力信号器、高压连接系统、喷放系统、接线端子等； 2. 七氟丙烷药剂：七氟丙烷气体，无管网设计，七氟丙烷喷射最低为 2.5 兆帕； 3. 点型光电感烟火灾探测器：分布智能型，电子编码，内置 CPU，指示灯 360 度可见； 4. 点型感温火灾探测器：分布智能型，电子编码，内置 CPU，指示灯 360 度可见； 5. 配套火灾声光警报器及编址声光底座，气体释放警报器及紧急启停按钮； 6. 编码器：可对现场总线部件编址、读址、设置、测试等功能，支持 Mini USB 端口供电； 7. 泄压装置：药剂量 X0.00043 为泄压面积，有效泄压面积 0.12 ㎡； 8. 火灾报警控制器（联动型）：壁挂式报警灭火控制器，液晶屏，1 个报警回路，1 个联动回路，满载不小于 40 点，支持报警、打印、联网功能； 9. 壁挂式联动直流供电单元：主备电一体，24V，含电池； 10. 含安装、调试、各类线材、管路及辅料。	1 套	40000	40000
8	机柜	1. 提供 2 套服务器机柜，服务器机柜尺寸为	1 套	7000	7000

		600mm×1000mm×2000mm(W×D×H)，配套PDU； 2. 机柜采用前后网孔门设计，前门单开，后门双开，前后门开孔孔径应不少于7.5mm，前门开孔率不低于80%，后门开孔率不低于80%； 3. 机柜采用前后网孔门设计，门的开合转动灵活、维护方便。前后门应采用外开门方式，前门单开，后门双开，开启角度应不小于150°； 4. 机柜颜色为黑色，整体防护等级应不小于IP20，支持带底座安装、水泥地板安装，防静电地板安装。			
9	空调	1. 提供1套空调，单冷及低温启动； 2. 提供空调制冷剂。	1套	25000	25000
10	电源迁移服务	1. 提供UPS整体迁移服务；	1项	19000	19000
11	设备保护及线路优化	1. 提供配合施工将现有设备做好防护及配合多次迁移； 2. 提供现有各类通信线路梳理、标记标签及迁移等； 3. 提供配套光纤跳线、RJ45跳线等。	1套	8100	8100
12	服务器	1. 国产化CPU，处理器:≥1个; 2. 内存≥DDR4 64G。	3套	30000	90000
13	防火墙	1. 标准2U机架式设备，不少于10个千兆电口，不少于6个千兆光口，包含三年硬件质保； 2. 支持IPv6安全控制策略设置，能针对IPV6的目的/源地址、源服务端口、服务、扩展头属性等条件进行安全访问规则的设置； 3. ★支持终端安全状态检测功能，具备四种以上的终端准入技术(提供功能截图)； 4. 支持静态路由，动态路由，VLAN间路由，单臂路由，组播路由等； 5. 支持PPPoE接入，能够针对每条ADSL链路单独设置保证带宽，并能够设置按需拨号； 6. 支持病毒自定义特征； 7. 支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒； 8. IPSec VPN支持透明、路由、混合模式等工作模式； 9. #支持协同防御功能，要求本项目中防火墙	1套	85000	85000

		与网闸能够实现底层的协同联通，防火墙能够将病毒快照自动同步至网闸，实现一体化防御功能(提供功能截图)； 10. 支持虚拟门户，实现下载文件链接、公司发布信息等； 11. ★支持防护资产漏洞扫描功能，包含云平台漏洞扫描、虚拟化漏洞扫描、数据库漏洞扫描，中间件漏洞扫描、国产化漏洞扫描、大数据 漏洞扫描、API 漏洞扫描以上全部漏洞扫描功能(提供功能截图)； 12. 支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主机的扫描防护； 13. #投标人所投防火墙支持扩展为“防病毒网关系统”，且扩展后的“防病毒网关系统”符合中华人民共和国国家标准 GB/T 35277-2017《信息安全技术防病毒网关安全技术要求和测试评价方法》“增强级”的要求（提供检测机构评级检验为“增强级”的检测报告复印件以及有效期内的证书复印件）； 14. ★投标人所投防火墙至少包含于四个国产化防病毒库引擎，并可以在系统界面进行选择，实现异构杀毒功能(提供功能截图)； 15. 支持对本地抓包文件的管理，包括下载、删除等操作； 16. 支持对 XSS 跨站脚本攻击行为的防护能力； 17. #能够接收主流国产化防病毒系统的病毒日志，自动将日志中的源病毒 IP 添加到阻断策略中(提供功能截图)； 18. 支持对 WEB 认证、LDAP 认证、RADIUS 认证、IP 识别用户的强制下线； 19. #投标人所投防火墙为自主原创产品非 OEM 产品，具备国家信息安全测评中心颁发的自主原创产品测评证书（提供证书复印件）； 20. 必须支持基于 WEB 地址 URL 的策略路由，可实现将不同类型的网站流量智能分配到不同的链路。			
14	网闸	1. 标准机架式设备，内网接口：不少于 4 个千兆电口，不少于 2 个千兆光口，外网接口：不少于 4 个千兆电口，不少于 2 个千兆光口，包含三年硬件质保； 2. 内、外网主机分别具备三系统，即系统 A、	1 套	78000	78000

		系统 B 和备份系统。支持在 WEB 界面上配置启动顺序，在 A 系统发生故障时，可以切换到 B 系统；支持将当前运行系统备份； 3. 支持显示网口运行状态，网口运行状态分别为绿色为启用、红色为掉线、灰色为停止； 4. 支持图形化并发会话数统计，可展示实时、24 小时、1 周的范围内数据统计； 5. #支持审计与告警功能，能够对应用系统近一个月内未登录的用户账号突然登录的异常行为进行审计与告警(提供功能截图)； 6. 支持将网口配置成 VLAN 接口，处理相同 vlan ID 的数据包； 7. 支持基于动态密码+本地密码的双因子认证方式； 8. 文件同步客户端支持 Windows、Linux 等主流操作系统，均具备图形化管理界面； 9. 支持文件传输方向可控，实现单向或双向传输； 10. 支持断点续传；支持首次复制+增量更新、增量传输、发送后删除、发送后转移、改名传输等发送策略； 11. ★能够调用本项目中防火墙的防病毒引擎对通过网闸交换的数据进行病毒查杀与过滤，并且根据病毒查杀情况，动态调整安全隔离策略与安全基线等级，提高跨网数据传输的安全性(提供功能截图)； 12. 支持时间策略；支持文件大小传输限制； 13. 支持文件统计功能，可统计成功文件数、失败文件书、总流量等信息； 14. 审核用户可管理普通用户，包括创建用户，删除用户，设置用户权限，使用空间上限等； 15. 支持 Oracle 数据库 RAC 集群同步； 16. 支持数据容错处理，当数据同步失败时，用户可以查询、恢复、删除未能正常传输的数据； 17. 支持数据库表及字段级的同步；支持同步库中初始数据功能； 18. 支持邮件主题及正文的关键字过滤，以及收件人、发件人地址黑白名单； 19. ★为阻止病毒数据加密穿透防御体系，通过协议代理实现加密数据逆向解密清洗功能(提供功能截图)；			

		20. 支持客户端与网闸间的数字证书方式的身份认证。			
15	入侵防御	1. 标准机架式设备，不少于 4 个千兆电口，包含三年硬件质保和三年特征库升级服务； 2. 内置专业的入侵防御特征库，入侵防御特征数量至少在 14000 条以上； 3. 内置多种规则集，满足不同部署环境下的安全防护需求； 4. 支持多种规则变更部署模式； 5. 支持至少包括规则 ID、规则名称、威胁级别、动作、威胁类型、发布时间等条件进行筛选； 6. 支持双向检测功能，根据双向流量检测攻击，输出检测结果； 7. 支持代理环境部署； 8. ★支持终端虚拟补丁服务和主机防病毒功能，可在漏洞攻击主机之前予以侦测和拦截(提供功能截图)； 9. 支持全局规则白名单和指定源目 IP 对规则白名单； 10. 支持 SQL 注入防护和 XSS 攻击防护，内置 AI 检测模型，利用机器学习技术对 SQL 注入报文进行分析，检测和识别 SQL 注入行为； 11. 支持威胁情报，情报白名单支持新建和批量导入导出操作； 12. #支持对移动终端的系统识别功能，能够对含有恶意应用程序的终端进行网络阻断与告警，至少支持鸿蒙，安卓，IOS 以上全部终端系统的识别与阻断(提供功能截图)； 13. 支持黑白名单，支持黑白名单全局检索，输入条件可直接查询黑白名单记录； 14. 支持 WEB 过滤，对 web 内容，传输文件名称、传输文件内容过滤； 15. #支持对中毒终端传输的 office、wps 文件的内容审计功能，要求可识别协议包括但不限于:HTTPS、SMTP 协议(提供功能截图)； 16. 支持网线模式部署和透明多口桥部署； 17. 支持端口聚合包括手动端口聚合模式和 LACP 聚合模式； 18. 支持策略调优，分析日志自动关联配置可一键修订规则动作和模板响应方式； 19. 支持生产报表；	1 套	64000	64000

		20. 支持威胁分析功能，通过与威胁情报、全流取证、网络负载等信息综合对威胁进行分析判断。			
16	入侵检测	1. 标准机架式设备，不少于 5 个千兆电口，包含三年硬件质保和三年特征库升级服务； 2. 支持 IP 碎片重组、TCP 流重组、TCP 流状态跟踪、2 至 7 层的协议分析、系统应支持工作在非默认端口下的周知服务的协议识别与协议分析能力； 3. 具有抗逃避检测机制，可以针对分片逃逸攻击、重叠逃逸攻击、加入多余或者无用字节逃逸攻击进行有效防范，并且能具体说明； 4. 支持全面的攻击检测能力，可检测常见的 Web 攻击、缓冲溢出攻击、安全漏洞攻击等； 5. 能够检测各种 SQL 注入攻击、XSS 跨站攻击等攻击行为； 6. 具备 Web 界面服务配置能力，可配置启用/停用 http 和 https 服务，支持配置 http 和 https 访问设备 WEB 界面端口； 7. 系统首页提供最近 24 小时内网络发生的展示界面； 8. 提供的攻击特征不应少于 7000 条有效最新攻击特征； 9. 提供检测规则自定义的高级接口，接口具备丰富的协议变量； 10. 支持 TCP 协议攻击特征自定义，提供 tcp_ack、tcp_fin、tcp_flag、等协议变量特征的自定义； 11. 提供对事件的二次检测能力，即对已生成的事件进行二次分析与统计，并根据统计结果进行报警； 12. #支持威胁的实时展示能力，可以将引擎检测到的威胁在威胁展示界面进行实时显示，现实内容需全面丰富(提供功能截图)； 13. 针对产生的告警事件，可以对攻击行为的特征数据包进行提取； 14. 支持根据历史流量数据，可以与实时流量曲线进行同时呈现并形成对比； 15. 支持按照历史流量同期对比和设置流量阈值两种方式配置告警参数，告警级别包含多种类型； 16. 提供事件名称+目的地址+源地址；事件名	1 套	78000	78000

		称+源地址+目的地址的三维交叉报表，能辅助用户快速定位问题； 17. 报表需支持手动立即执行、周期性自动执行两种执行方式； 18. 支持多级部署、集中管理能力，可以添加组件（包括控制中心、引擎），至少支持五级以上部署环境； 19. #系统在检测到攻击行为的同时，可以提取出完整的攻击行为的恶意代码样本文件(提供功能截图)； 20. 支持创建不同的配置管理员，并赋予不同的授权角色，控制管理员的配置权限。			
17	日志审计	1. 标准机架式设备，提供不少于 6 个千兆电口，不少于 2TB 存储容量，包含三年硬件质保； 2. #支持基线检查功能（至少包括外联基线，内联基线，基线学习），通过基线检查功能限定前端安全接入的访问行为(提供功能截图)； 3. 支持通过分布式日志采集器（不限个数）统一管理进行分布式扩展部署； 4. 支持 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹等多种方式完成日志收集功能； 5. 支持 Lotus Domino、Check Point、VMWare 的日志采集任务； 6. 支持 HTTP / HTTPS 协议接口进行采集任务配置实现日志数据采集； 7. 支持通过采集器检测当前日志采集器的资源使用和在线状态进行监测，展示当前采集器日志接收速率、CPU 负载、CPU 使用趋势等； 8. 支持主动采集 oracle、sqlserver、mysql、db2 等数据库日志； 9. #支持账号登录审计功能，对短期内通过多个 IP 登录行为进行审计，发现账号盗用情况并进行短信提示(提供功能截图)； 10. 支持对国内主流国产化数据库进行日志数据采集，包括武汉达梦、人大金仓、南大通用、神州通用等； 11. 支持采集过程中自定义配置带宽大小进行采集速率限制； 12. 支持自定义日志合并规则，支持一键清除合并规则； 13. 支持采集的日志进行存储压缩加密；	1 套	73000	73000

		14. 支持日志范式化，实现对多元异构日志格式的进行统一描述和处理； 15. 支持为未解析日志提供一种简洁在线编辑解析文件视图，做到精准解析； 16. 支持自动识别收集的日志并自动选择范化策略，对不支持的事件类型提供扩展机制，采用自适应解析文件方式进行事件匹配； 17. 支持长日志格式，范式化字段可在分析过程中根据审计和分析的需要灵活扩展，并可参与关联分析及统计报表等； 18. 支持复杂日志的嵌套解析，支持在一个解析插件多次引用正则、json、key-value、等解析方法； 19. 支持日志设备地址和日志解析文件进行绑定关联，实现定向精准解析； 20. 支持基于日志查询任务模式的日志导出功能。			
18	运维审计	1. 标准机架式设备，提供不少于 6 个千兆电口，包含三年硬件质保； 2. 支持 NAT 地址映射部署； 3. 系统内置系统管理员、审计管理员、安全管理员三种角色； 4. 支持管理员帐号设置双因认证、IP/MAC 限制，提升帐号安全性； 5. 支持用户管理，包括添加、删除、启用、禁用、移动、修改功能； 6. 支持用户组管理，包括添加、删除、修改功能； 7. #支持云主机系统逃逸审计检测功能，能够针对逃逸主机进行阻断或锁定操作(提供功能截图)； 8. 支持用户客户端 IP 和 MAC 限制，支持黑白名单两种工作模式； 9. 支持资源管理功能，包括添加、删除、启用、禁用、移动、修改功能； 10. 支持资源组管理功能，包括添加、删除、修改功能； 11. 运维角色支持时间、命令和审批策略； 12. 支持超过角色中时间策略中的时间范围，系统将阻断运维会话； 13. 支持用户、资源与角色关联，形成访问策略； 14. 支持字符、传输、数据库协议的命令规则定义；	1 套	73500	73500

		15. 支持改密结果自动发送到指定改密计划的管理员邮箱或发送到FTP服务器； 16. #支持对物理SIM卡的硬件特征码进行身份认证与单点登录服务，支持向SIM卡写入联网签名的数字证书，实现数字证书的在线分发和离线分发（提供功能截图）； 17. 支持对改密计划的执行日志进行完整记录； 18. 支持RDP、VNC图形操作行为的审计，图形回放形式还原真实操作过程； 19. 支持在Oracle数据库运维，运维人员对变量进行绑定，执行SQL后，堡垒机系统可审计对应SQL中唯一标识符的具体值，协助审计员分析安全事件； 20. 支持NTP时间同步功能。			
19	漏洞扫描	1. 标准机架式设备，提供不少于6个千兆电口，包含三年硬件质保； 2. 支持IPv4和IPv6环境的部署和扫描，可扫描的IP地址总数量无限制； 3. #支持NAT环境下的用户识别功能，通过逆向地址解析的方式，实现对用户真实IP地址进行扫描(提供功能截图)； 4. 支持对主流操作系统的识别与扫描； 5. 支持对主流数据库的识别与扫描； 6. 支持对主流虚拟化软件平台的识别与扫描； 7. 支持对主流国产应用软件的识别与扫描； 8. #支持对信息资产的安全基线核查阻断功能，对于不符合等保要求配置的信息资产能够阻断其网络连接，信息资产至少包括操作系统、网络设备、安全设备、中间件、数据库(提供功能截图)； 9. 支持对主流SCADA/HMI软件的识别与扫描； 10. 支持对主流PLC、DCS控制器的识别与扫描； 11. 支持对各种Web应用系统的扫描，支持检测SQL注入漏洞、命令注入漏洞、CRLF注入漏洞等； 12. 支持对易通、易思、大汉等web应用系统和第三方组件的扫描 13. 支持Web漏洞特征库大于4000条，漏洞评分支持CVSS3.0标准； 14. 支持漏洞验证功能，在扫描结束后，能够对结果中的重要漏洞进行现场验证，展示漏洞利用过程和风险；	1套	74000	74000

		15. 支持展示 web 安全漏洞信息，按风险级别等维度进行展示，可点击查看漏洞详情，包括漏洞细节，漏洞危害，修复建议，http 头，漏洞验证等； 16. 支持配置变更检查，可以根据实际情况设置任意检查结果作为变更基线； 17. #支持虚拟漏洞补丁功能,能够对有漏洞的信息资产进行漏洞自动化修复(提供功能截图)； 18. 支持检查的内容包括但不限于账号、口令、授权、日志审计、不必要的服务、启动项、注册表、会话设置等配置； 19. 支持下发单独的配置核查、配置变更和变更监测任务； 20. 支持检查项设置权重、规范来源及告警配置； 21. 支持核查脚本的自定义功能，并能按顺序清晰展示脚本使用的命令集合。			
20	测评服务	1. 投标人需严格依据《GB/T22239-2019 信息安全技术网络安全等级保护基本要求》开展基于等保 2.0 的等保三级测评工作，并出具《测评报告》； 2. 投标人需根据系统定级情况以及系统建设情况，协助采购单位起草等保备案材料并完成相关系统在公安机关的备案工作，取得《备案证明》； 3. 投标人须对本项目商用密码应用方案的完整性、准确性、可行性等方面进行分析； 4. ★投标人合作的测评机构需同时取得《网络安全等级测评与检测评估机构服务认证证书》和《商用密码检测机构资质证书》(提供证书复印件)； 5. 依据《信息安全技术 网络安全等级保护基本要求》，测评内容包括但不限于：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理等十个层面开展测评工作； 6. 投标人依据《网络安全等级保护测评过程指南》，从测评准备工作、方案编制工作、现场测评工作、分析与报告编制工作四个方面制定测评工作流程； 7. 提供安全物理环境测评：物理位置的选择、	1 项	96000	96000

		物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。 8. ★投标人合作的测评机构须同时派遣本单位 2 名具备高级网络安全等级测评师证书人员，3 名具备中级网络安全等级测评师证书人员，进行为期三个月的 5*8 小时驻场安全服务，配合该项目的等保基线核查工作（提供等保测评机构服务承诺函及驻场测评师证书复印件）； 9. 投标人需严格依据《GB/T28449-2018 信息安全技术网络安全等级保护测评过程指南》开展现场测评工作，测评方法包括但不限于访谈、核查、工具测试等内容； 10. 投标人根据等级保护安全管理层面相关标准要求，针对采购单位重要系统制定和完善符合等保 2.0 需求的信息安全管理制度。			
合计：					892400.00