报价唯一性

投标分项报价表（实质性格式）

投标分项报价表

项目编号/包号：常采公[2022]0191 号

项目名称：工作网安全防御设备（等保三级一期）　　报价单位：人民币元

序号	分项名称	品牌商标	规格型号	技术参数	数量	单位	投标价格	
							单价	合价
1	核心交换机	H3C	S7506X-S-MF	业务插槽数≥6，整机交换容量≥76Tbps，整机包转发率≥8640Mpps（如官网指标出现两个值，以最小值为准）冗余主控、冗余模块化电源支持标准和扩展 ACL，支持基于 VLAN 的 ACL,支持 Ingress/Egress ACL 支持层次化 QoS（H-QoS），支持三级队列调度，支持队列调度机制，包括 SP、WRR、SP+WRR、WFQ，支持拥塞避免机制，包括 Tail-Drop、WRED 支持 CPU 保护技术，支持 VRRP，支持热补丁，支持硬件 BFD 支持 MAC Tracert，支持 Graceful Restart for OSPF/BGP/IS-IS 以太网支持千兆电口，千兆光口，万兆光口、万兆电口，25G 端口、40G 端口。支持 RIPng、OSPFv3、BGP4+、IS-ISv6 协议，支持 IPv6 策略路由，支持 DHCPv6 功能、IPv6 portal 功能、IPv6 管理功能，支持基于 IPv6 的 VXLAN 二三层互通，支持创建、删除虚拟交换机，将虚拟化系统虚拟成多台交换机实现用户表项叠加，支持物理设备虚拟化实现负载分担，提供工信部权威第三方测试报告。支持安全业务插卡，包含防火墙、负载均衡、应用控制网关、IPS、SSL VPN 等独立板卡。支持 Telemetry 流量可视化功能。支持融合无线 AC 功能,无需独立的 AC 业务板卡,即支持无线 AP 管理功能。支持通过 Python/NETCONF/TCL 等对网络自动化编排，实现 DevOps 自动化运维。内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级。支持 L3 VPN,支持 VLL,支持 VLPS,支持 MCE。支持 IEEE 802.1ae 介质访问控制安全技术。实配双主控，双 1400W 电源，千兆电口≥48，千兆光口≥48，万兆光口≥20，三年质保，要求与现有核心交换机进行双机虚拟化。	1	台	190000	190000
2	防火墙（万兆）	深信服	FW-20000-X2100（万兆）V	产品应用多核并行处理架构，并采用国产处理器和国产操作系统。性能参数：网络层吞吐量≥39Gbps，应用层吞吐量≥9Gbps，并发连接数≥4000 万，新建连接数（CPS）≥23 万。硬件参数：规格：2U，内存大小≥16G，硬盘容量≥128GB SSD，电源：冗余电源，接口≥6 千兆电口+4 千兆光口 SFP+4 万兆光口 SFP+。含 4 个万兆多模光模块。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;支持多维度安全策略设置,可基于时间、用户、应用、IP、域名等内容进行安全策略设置。支持僵尸网络检测功能，防止失陷主机威胁内网扩散。具备至少对 ARP Flood、ICMP Flood、SYN Flood、DNS Flood、UDP Flood 等泛洪类攻击防护的能力，并支持 IP 地址扫描和端口扫描攻击防护；支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御。具备识别与阻断，外部扫描器发起的服务器恶意扫描行为,可对扫描器地址进行自定义封堵。产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护，产品支持≥7200 种特征	2	台	200000	400000

			2.0	规则数量。支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等等检测和防护，产品具备 Web 应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含 SQL 注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL 后门攻击、跨站请求伪造、目录遍历攻击、WEB 整站系统漏洞等应用层攻击行为，安全特征规则≥3320 种。产品支持对多重压缩文件的病毒检测能力，支持不小于 12 层压缩文件病毒检测与处置。支持主备，主主两种模式，产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括 DNS 解析、ARP 探测和 PING 方式。				
3	运维安全管理系统（堡垒机）	天融信	TopSAG（ZX-A）V3	采用国产 CPU，主频不低于 2.0GHz，4 核，2U 机箱，千兆电口≥6 个,千兆光口≥4 个，内存 16GB，硬盘 1TB。2 个可插拔的扩展槽，标配模块化双电源。100 个主机/设备许可；用户数不限制；采用物理旁路部署，不改变现有网络结构 支持用户的增删改查、锁定、激活，进行用户全生命周期管理，支持用户批量导入和导出，采用三员管理，支持系统管理员、安全审计员和安全操作员，并且三员之间权限相互制约，用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP 认证、RADIUS 认证、USBKEY 认证、OTP、短信认证等身份认证方式；支持可知因素和不可知因素的双因素认证。支持中标麒麟、银河麒麟、Windows 等操作系统，支持网络设备、安全设备、数据库等的资产管理支持修改管理协议默认端口，支持资产的批量导入导出，支持资产组的增删改查，支持资产账号手动添加，支持账号的批量导入导出，自动对 Windows、Linux 等设备进行账号改密，改密支持手动和定期任务，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成，支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权，支持会话、指令、剪切板上下行、文件上传下载的约束行为；支持用户会话超时退出；支持用户密码连续鉴权失败锁定，到期自动解锁;支持用户强密码策略,密码长度 8 位以上，包含字母、数字、特殊字符等；支持对用户登录 IP 地址、MAC 地址、时间的限定，支持对运维时间、运维地址、运维操作指令的限定，触发策略后进行告警，支持管理员自定义幽灵账号开启和关闭,支持自动发现运维人员运维过程中创建的后门账号行为,并以列表方式向设备管理员展示托管设备中所有的后门账号信息。设备访问支持最新的 html5 技术，在同一 WEB 窗口页签中，无需 JAVA 应用插件或调用本地应用客户端,即可实现对目标设备的快速运维；支持 SecureCRT、XShell、WinSCP 等客户端直接连接堡垒机进行代理运维目标资产,支持对用户和管理员的认证登录、操作和配置管理进行日志记录,支持对 Windows、VNC 等图形界面的运维操作进行录屏审计，支持图形和字符协议的视频回放,支持对图形和字符协议的操作进行文本记录，如鼠标操作、文本内容操作等，Linux 命令操作等，支持对在线会话的实时监控和即时阻断，避免违规操作，支持全文审计检索。可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯。报表针从会话、指令等多个维度进行统计；系统内置丰富报表统计模板：协议运维排名、资产运维次数 top10、资产运维趋势 top10、用户运维趋势 top10、协议运维趋势、用户运维次数 top10、指令分布 top10、top10 指令资产分布、指令用户分布 top10、	1	台	118000	118000

				指令资产账号分布、指令排名、指令趋势、风险指令次数、风险指令 top10 等多种类型报表模板。支持 HTTPS 方式和 Console 方式进行管理，支持管理口与业务口分离，支持将本机日志、告警日志通过 SYSLOG、邮箱等进行外发和告警，支持配置数据和审计数据的备份、自动清理，支持备份数据通过 FTP 方式远程备份，支持配置时间同步服务器，进行时间自动校对，保障审计的有效性和准确性				
4	日志审计	天融信	TA-LOG（FT-A20）V3	产品采用国产处理器和国产操作系统，主频不低于 2.0GHz，64 核，2U 机架式设备，千兆电口≥2 个，万兆光口≥2 个（含 2 个万兆多模光模块）；采集处理峰值≥20000EPS，日志源数量≥100。支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等。支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集； 支持对每个日志源设置过滤条件规则，自动过滤无用日志； 支持日志转发给第三方系统平台，支持设置多个日志转发 IP 地址，支持转发格式化日志或仅转发原始日志；支持 IPv6/IPv4 双栈环境部署，对 IPv6/IPv4 日志源的日志进行高速采集；支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储、网络存储；支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数；支持 IPv6 日志的全量存储；支持为不同类型日志设置不同的查询条件和显示条件； 支持原始日志全文检索；查询结果可将归一化日志和原始日志同屏对比显示；支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析；支持多种运维管理工具，可对日志源进行 HTTP、HTTPS、SSH、SCP、SFTP、FTP、MYSQL、ORACLE、SQLSERVER 等操作。支持首页展示当日告警情况统计；支持展示当日最新告警 TOP10、TOP30 和 TOP50； 内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别。支持安全告警概况、安全告警趋势的统一展示，实时告警可根据级别、规则类型等进行分类；支持实时告警展示，可根据告警规则、告警级别两个维度进行实时告警监视，并可对刷新事件间隔进行设定；支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备 IP、源 IP、目的 IP 等方式快速检索安全事件告警，检索结果支持 Excel 等格式导出；支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析；支持在告警事件查询界面直接显示触发告警的关联日志，也支持点击跳转到日志查询界面。 支持告警抑制规则设定，防止报警信息短时间内大量发送。 系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应；支持自定义统计日志数据形成报表，支持统计分析报表以 PDF、word、execl、html 等方式导出；支持实时报表、计划报表。支持手动添加日志源，管理员可以对日志源进行查看、批量修改、添加、编辑、删除以及启\禁用的操作；支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息； 系统内置常见安全事件关联分析规则；系统内置多种维度的数据在线分析模型，在数据查询结果界面直接对查询结	1	台	118000	118000

				果数据进行多维度在线数据分析，分析结果实时展示，分析模型包括但不限于树图、散点图、关系图、折线图、时序图、柱状图等。支持用户按角色管理，支持三权分立；支持将日志源管理权限分配给不同的操作管理员，不同用户管理不同日志源的日志，互不干扰；支持设置非法用户访问控制策略； 系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。支持将常用 IP 地址或 IP 地址网段标记为自定义名称，在日志查询界面可以在 IP 列中对应悬浮显示自定义名称；				
5	链路检测	H3C	SWP-IMC7-IMP	国产品牌，与核心交换机同一品牌，支持自动发现网络中的所有网络设备，并在拓扑中显示出来支持拓扑图自定义修改，包括设备、链路等。支持面板视图视图，设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态；并提供基于设备面板的设备、单板、端口配置功能。接收 Syslog，完成基本格式的解析，并入库。提供 Syslog 特征分析及策略注册能力，支持基于统计规则进行聚合生成告警（Trap）支持批量的设备配置备份和恢复。支持向导方式或者任务方式（周期性任务、一次性任务或立即任务）批量的备份、恢复完整的配置文件，也可以批量的下发配置片断。支持设备配置集中管理：配置库包括配置文件和配置片断，配置内容可带有参数，在部署时根据设备的差异设置不同的值；配置文件可部署到设备的启动配置或者运行配置；配置片断只能部署到设备的运行配置； 实现网络 IP 地址自动扫描、统计、分配和管理，同时允许用户手工分配和管理 IP 地址，以达到更加灵活的分配管理。结合 IP 地址段的管理功能，将整个网络的 IP，划入各个不同的 IP 地址段，分别进行管理，并给出详细直观的 IP 分配情况统计图表，使管理员能清楚的了解和掌握整个网络的 IP 使用情况。支持设备软件智能升级。支持网络运行设备的软件版本查询功能，支持先备份后升级，保证一旦升级失败后可以恢复到原有设备软件版本，支持对整个升级过程的可靠性检查，如设备软件版本和设备是否配套，flash 空间是否足够等，确保用户的整个升级操作万无一失。支持不间断业务的软件升级 ISSU。新设备注册，告警注册，新性能指标注册，新 Syslog 解析注册，Mib 编译，第三方设备配置管理-CLI 下发，配置管理-配置备份、软件升级（使用 TCL/ Expect /Perl 模板自定制），第三方设备管理系统集成。平台提供有网络基础管理视图、分级管理视图、快捷业务视图、桌面视图。视图切换方便。极大提高菜单易用性。创建操作员时可以指定有权限的视图和默认登录视图。网络设备管理 license≥100，要求能够对大楼原有网络设备进行管理，可以远程对网络设备端口进行 UP 和 DOWN 管理。	1	套	50000	50000
6	漏洞扫描服务	定制	定制	对网络进行漏洞扫描工作，配合做好漏洞指导整改、复测工作。	6	次	2000	12000
7	等保三级测评	定制	定制	委托具备资质的第三方信息安全等级测评机构（以下简称“测评机构”）对采购人的信息系统进行信息等级保护三级测评，按照信息安全等级保护制度建设要求提出安全整改建议形成《安全整改建议书》，待采购人根据《安全整改建议书》组织完成整改后，测评机构再依据依照《信息系统安全等级保护基本要求》（GB/T 22239-2019）进行复	1	次	80000	80000

	费			测，验证安全整改的结果，最终出具《信息系统安全等级测评报告》。				
合　　计								968000

注：1.本表应按包分别填写。
2.如果不提供分项报价将视为没有实质性响应招标文件。
3.本表行数可以按照项目分项情况增加。
4.上述各项的服务内容如表格中填写不下的，可以逐项另页描述。

投标人名称（加盖公章）：中电鸿信信息科技有限公司

日期：2022 年 10 月 10 日