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[2023]0007 号/01 包 项目名称：江苏省常州市人民检察院本级检察工作网边界安全接入平台项目 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	防火墙（IPS+防病毒+双电源）	深信服	FW-1000-GA150（千兆）V2.0	性能参数：网络层吞吐量：9Gbps，应用层吞吐量：2Gbps，并发连接数：300 万，新建连接数（CPS）：13 万。硬件参数：规格：2U，内存大小：8G，硬盘容量：64GB SSD，电源：冗余电源，接口：6 千兆电口+4 千兆光口 SFP。CPU：飞腾 FT-1500A（1.5GHz，4 核），操作系统为银河麒麟 V4.0;3 年软硬件维保，3 年特征库升级。开启 IPS 模块，具备入侵防御功能。开启 web 应用防护模块，具备 web 应用防护功能。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。支持策略路由负载来支持基于服务、ISP 地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，总共需要支持加权流量、带宽比例、线路优先等负载均衡调	1	台	106000	106000

				度算法。支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能。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；支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制。支持源地址转换 SNAT，目的地址转换 DNAT 和双向 NAT 等功能， 支持一对一、一对多、多对一等形式的 NAT。支持 IP 内置应用特征识别库，支持不少于 2980 种应用规则，支持对游戏、下载工具、IM 聊天工具、视频软件、股票软件等类型应用进行检测与控制。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，安全特征规则超过 3320 种。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。支持对服务器和客户端的漏洞攻击防				

				护，支持 XSS 攻击、SQL 注入等 WEB 攻击行为进行有效防护；支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等 DoS/DDoS 攻击防护；支持 IP 地址扫描和端口扫描防护；支持 Land、Smurf、WinNuke、Tear Drop、IP 数据块分片传输、超大 ICMP 数据攻击等攻击基于数据包攻击防护；支持 IP 协议异常报文检测和 TCP 协议异常报文检测；支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； 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。支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测；支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便安全策略管控。				
2	防火墙（带 DDOS 防护 +IPS+ 防病毒 +双电源）	深信服	FW-1000-GA150（千兆）V2.0	性能参数：网络层吞吐量：9Gbps，应用层吞吐量：2Gbps，并发连接数：300 万，新建连接数（CPS）：13 万。硬件参数：规格：2U，内存大小：8G，硬盘容量：64GB SSD，电源：冗余电源，接口：6 千兆电口+4 千兆光口 SFP。CPU 为飞腾 FT-1500A	1	台	110000	110000

				（1.5GHz，4 核），操作系统为银河麒麟V4.0;3年软硬件维保，3 年特征库升级。开启 IPS 模块，具备入侵防御功能。开启 web 应用防护模块，具备 web 应用防护功能。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。支持策略路由负载来支持基于服务、ISP 地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，总共需要支持加权流量、带宽比例、线路优先等负载均衡调度算法。支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能。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；支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制。支持源地址转换 SNAT，目的地址转换 DNAT 和双向 NAT 等功能， 支持一对一、一对多、多对一等形式的 NAT。支持 IP 内置应用特征识别库，支持不少于 2980 种				

				应用规则，支持对游戏、下载工具、IM 聊天工具、视频软件、股票软件等类型应用进行检测与控制。支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等 DoS/DDoS 攻击防护；支持 IP 地址扫描和端口扫描防护；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。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，安全特征规则超过 3320 种。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。支持对服务器和客户端的漏洞攻击防护，支持 XSS 攻击、SQL 注入等 WEB 攻击行为进行有效防护；支持对常见应用服务（FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联				

				动封锁，支持自定义封锁时间。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。支持采用无特征AI检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测；支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便安全策略管控。				
3	三层交换机	H3C	S5130-28S-EI	产品类型千兆以太网交换机，网管交换机 传输速率10/100/1000Mbps 交换方式存储-转发 背板带宽336Gbps/3.36Tbps 包转发率96Mpps 端口参数 端口结构非模块化端口数量28个端口描述24个10/100/1000Base-T电口，4个10G BASE-X SFP+万兆光口功能特性 堆叠功能可堆叠VLAN支持基于端口的VLAN，支持基于MAC的VLAN，基于协议的VLAN，支持QinQ，灵活QinQ，支持VLAN Mapping，支持Voice VLAN，支持GVRP QOS支持对端口接收报文的速率和发送报文的速率进行限制，支持报文重定向，支持CAR（Committed Access Rate）功能，每个端口支持8个输出队列，支持端口队列调度（SP、WRR、SP+WRR），支持报文的802.1p和DSCP	2	台	5500	11000

				优先级重新标记 组播管理支 IGMPSnooping/MLDSnooping，支持组播 VLAN 网络管理支持 XModem/FTP/TFTP 加载升级				
4	网络模块	H3C	SFP-XG-SX-MM850-D	万兆多模模块	8	个	850	6800
5	数据安全交换系统	金电网安	多级安全隔离互联平台 MISP V1.0	2U 设备 前后置各 6 个千兆口，2 个光口，2 个 USB 口，双电源，海光-3250，银河麒麟 V10，内部交换带宽 8G,网络吞吐量：1000Mbps，数据库同步吞吐量:10000 条/秒，并发 20000，延时<0.5ms，文件同步吞吐量:500Mbps 支持文件传输，文件同步，数据库访问，数据库同步，视频传输，等功能由 1 个应用后置、1 个应用前置两台台单独的硬件以及可提供源端可信增强模块三个部分组成；两个应用前后置分别部署在网闸两侧，实现在数据交换前后的数据剥离和落地，实现对文件格式的安全检查，包括文件的后缀、PE 格式、内容安全检查等，并对交换文件进行杀毒处理；支持旁路部署；设备宕机或断网不得影响数据传输；产品硬件基于 PTM 可信机制，能够对硬件进行全方位的可信计算。平台操作系统经过安全加固的操作系统，提供内核级主动深度防御。支持 IPV4 与 IPV6；HTTP、SMTP、POP3、FTP、TELNET、SQL、ORACLE、NULL_TCP 等；可定制应用协议检查模块。支持通过对信息流单向、双向定义，对跨系统互联的信息流向进行控制；支持通过用户名口令、	2	套	210000	420000

				IP/MAC 绑定等方式对访问用户身份进行鉴别，确保用户身份的真实性;支持系统间交换的合法数据会进行安全标记，隔离部件会对标记进行判别解析，以确保所交换的数据都是经过授权的；支持标记根据时限要求进行自动更换；具备防非法卸载的能力；基于可信计算理念，利用信任链机制，对系统中所有装载的可执行代码进行控制；提供拔 KEY 锁屏功能，当用户离开时拔除 USB-KEY 自动锁定用户工作环境，解锁时需实现基于硬件 USB-key 的双因素身份认证；提供对白名单中所包含执行程序及脚本文件的防篡改保护，拒绝非授权的修改、删除等操作；支持服务强制访问控制，能够阻止增加、删除、修改系统服务配置信息；支持源端服务器认证，平台中的可信通道只有经过源端安全加固的服务器才可进行数据传输；提供 20 套过平台网站服务器的加固模块；基于可信计算理念，利用信任链机制，对系统中所有装载的可执行代码进行控制；采用主动防御机制，在恶意行为发生前先行进行阻断；以可信名单方式进行可执行程序的验证，确保系统对已知/未知木马、蠕虫、病毒及其变种的防护能力；支持自动扫描信任链更新；支持用户定义信任链更新；支持软件安装自动释放信任链更新机制；支持受控目录内所有文件、子目录保护机制；支持受控目录内建立非受控目录机制；支持可信进程目录操				

				作机制；采用驱动控制模式，可对服务器上使用的移动介质进行控制；基于可信计算理念，对服务器上使用的移动介质的病毒木马可直接免疫；支持对访问操作的 IP 地址、端口、内容（格式检查）进行控制，确保跨系统操作的安全性；可通过专用客户端和平台主动获取两种方式提供安全的数据库同步功能；提供多种主流数据库（SQL、ORACLE、DB2、MYSQL 等）的单、双向数据交换；支持同步表双向检索功能；无需修改数据库表结构，不涉及到代码修改及二次开发；同步粒度可以达到表内具体字段；支持多种增量同步方式，可分别定义增加、删除、修改的传输方式；支持数据一对一、一对多、多对多的单向或双向交换和同步。提供对多种主流数据库（SQL、ORACLE、DB2、MYSQL 等）数据库系统的安全访问；支持用户查询、修改、添加、删除等操作；支持全表复制、增量更新、全表更新等；支持对用户、操作、目标数据库等策略控制。支持 HTTP 协议访问；访问控制对象：源地址、目标地址、源端口、目的端目、域名、URL、访问方式等；内容过滤：关键字（采用自主研发的下推自动机的高效过滤算法）；脚本过滤：Javascript、Applet、ActiveX 等;支持对基于 HTTP 的 SOAP 协议进行过滤，确保访问的安全；其他过滤策略：文件类型、页面提交方式等。提供安全的文件传输功能，支持 FTP、NFS、SAMBA 等文				

				件传输协议；支持 FTP 对传输文件的类型过滤;支持 FTP 指令控制；支持 FTP 文件名黑白名单控制；支持 FTP 传输文件大小控制。可通过专用客户端和平台主动获取两种方式提供安全的文件同步功能；支持 windows 平台和 linux 平台;支持不同任务设置不同的扫描间隔和扫描的时间段；支持任务优先级控制；支持实时扫描、多对一传输、增量传输；支持目录内子目录同步，至多支持 32 级目录；支持中文文件名或目录同步；支持传输后删除源文件；提供详细的日志审计；支持对格式类型进行特征过滤，并允许用户通过样本文件自定义格式类型；支持文件在线编辑、在线预览等操作；支持文件分享功能，可设置到期时间和提取密码。实现视频网络与信息通信网的网络隔离，切断所有基于网络协议的连接；支持多种视频硬件平台，如摄像头、DVR（数字硬盘机）、流媒体服务器、视频服务器等设备；支持标准 SIP 协议支持 RTSP 协议；支持用户基于标准 TCP、UDP 开发的自定义协议软件；无需对自定义协议软件进行二次修改开发；可以根据需求开发新的专用协议处理过滤功能。支持 MAC 强制访问控制通道，针对被访问端文件进行类别和等级标记，通过标记匹配才能正常访问文件。支持可信网络连接，平台中各设备通过可信网络连接进行数据传输；支持应用端可信模块部署，部署可信模块后可保证应用				

				进程的安全可靠，并通过可信网络连接进行数据传输；基于 Bonding 模块技术，使多网口冗余，可实现链路备份冗余的工作模式，支持 lacp、负载均衡、主备模式；可实现多套平台互相冗余的应用模式，支持跨定级管理中心的双机热备及整套链路的双机热备。支持 SNMP 协议，可与标准网管平台无缝兼容；能够针对读团体字、系统位置、系统联系人等参数进行自定义；支持 SYSLOG 协议，可与标准日志服务器平台无缝兼容，可实时发送设备运行状态；				
6	网络准入控制	天融信	TopNAC(HG-B10)	海光-3230/4 核,统信服务器操作系统 V20,2U,6 个千兆电口、4 个千兆光口和 2 个万兆光口,冗余电源,2 个扩展槽位,最大同时在线数 1000,默认包含 200 点客户端授权采用专用硬件架构与专用安全操作系统。系统部署简单，支持旁路或串联部署，支持命令行与 B/S 模式管理，提供系统首页图形化展示功能，可展示设备面板状态、CPU 状态、内存状态、硬盘状态、在线用户、报警统计等信息。可靠性：设备提供硬件 BYPASS 功能，支持双操作系统冷备、双机热备，在单机模式下，提供独立系统逃生工具。支持 802.1X、Portal、透明网关、策略路由等多种准入模式选择，单设备情况下可进行混合准入模式应用。提供客户端认证及手机短信认证方式，客户端认证可与第三方 AD 域、LDAP 服务器进行用户信息同步；手机短信认证可与短信	1	台	100000	100000

				服务器联动，在终端入网认证时下发验证码。支持终端信息绑定认证，可检查入网终端 IP、终端 MAC、用户名、交换机 IP、交换机端口、终端硬件 ID 等多要素信息。支持访客入网管理，访客接入由受访人员（固定用户）协助其进行注册、账户创建等操作，并提供临时入网终端有效期管理，可设置在网时限。支持同账户多在线管理，可设置同一用户名同时在线数量，并对用户名超过在线数进行处理。IP 冲突管理，当入网终端与已在线终端出现 IP 冲突时可选择：不处理或强制下线已在线的终端；支持准入设备黑/白名单管理，可根据所应用的不同准入模式，设置黑/白名单终端 IP、MAC、协议、端口、VLAN 号等信息，以便针对该名单中设备进行入网控制。支持入网终端健康检查，对检查项可进行权重、修复向导自定义设置，检查项包括：系统时间检查、系统运行时长检查、Guest 用户检查、AD 域域名检查、Windows 文件共享检查、Windows 防火墙检查、系统运行时间、操作系统版本、系统补丁、必须/禁止运行进程检查、必须/禁止运行服务检查、必须/禁止安装软件检查、Windows 桌面屏保检查、杀毒软件版本（天融信 EDR、小红伞、瑞星、金山毒霸、卡巴斯基、诺顿、360 杀毒）等。支持终端接口外设监控，可对终端所有接口外设实施启停用控制，对 USB 设备添加 USB 硬件 ID 和设备信息，可设置例外项。				

				支持终端非法外联监控，可判断通过 http、telnet、ping 三种方式检测主机违规外联行为，给予违规处理方式（不处理、重启、断网、提示），并信息提示。支持资产管理功能，可管理不同类型入网资产；提供交换机网络设备管理功能，可查看交换机设备接口状态、主机连接等详细信息。对入网资产可发现、可审批入网。 提供终端解绑、资产登录、报警、系统、终端认证、健康检查等详细日志信息，可采取图形化方式统计分析，并自定义模板进行报表定时输出。诊断分析，可通过系统调试信息及抓包分析功能定位问题；系统具备良好的使用体验与可管理性，支持系统界面与登录界面 LOGO 的自定义导入，可自由设置产品显示名称。管理员可进行准入系统的维护、升级、诊断分析等操作，支持图形化方式展示各类型数据所占磁盘状态，并提供备份、恢复、清理功能。				
7	网络数据防泄漏系统（DLP）	天融信	TopDLP(FT-B30N)	飞腾-2000(2.6GHz,4 核),统信服务器操作系统 V20,2U,默认含 1 个管理口、1 个 HA 口、4 个千兆电口和 4 个千兆光口,冗余电源,3 个扩展槽位,可参考 7 层最大检测吞吐 200M；支持即插即用功能。不管设备的管理 IP 如何配置，只要将流量引入数据网口，即可产生敏感数据泄漏事件报表。支持 SMTP、IMAP、POP3 协议，可解析主题、正文、附件、发件人、收件人、	1	台	150000	150000

				抄送人、密送人；支持 SSL 加密协议解析（阻断模式）；支持 FTP 协议监控，识别敏感数据。支持 DNS、TELNET、NNTP 协议检测；无需配置协议详细端口，即可实现对网络传输协议（http、https、smtp、pop3、imap）识别检测；支持按文件类型进行识别，支持文本类格式、图片格式、电子表格格式、演示格式、多媒体格式、压缩文件格式、加密文件格式；支持识别的加密文件格式不少于 6 种；支持的压缩文件格式不少于 10 种；支持图片格式，如 bmp，jpg，tif，tif2，png；支持识别自定义文件类型；支持的压缩文件格式内容提取，如 rar，zip，tar，gz，7z，bz2，lzh，rar5，xz；支持识别嵌套在文档中的图片类型；支持文本类文档、office 系列文档、代码类文档、嵌套文档（office 文档互相嵌套 2 层之内）内容提取；通过单独部署 OCR，实现对 bmp，，tif，tif2，png 类型的图片内容检测；支持数据库指纹方式精确识别敏感内容；支持对文档学习生成敏感数据指纹，精确识别敏感内容；支持数据库指纹功能，支持 Oracle、MySQL 数据库类型的指纹学习，精确识别敏感内容；支持指纹任务定时任务计划；支持数据库共享方式生成指纹库；支持机器聚类，手动、自动				

				抓取大量无序文档样本进行聚类分析，手动生成推荐规则；支持识别文档多层嵌套方式逃避检测行为；支持识别文件加密方式逃避检测行为；支持图片类型文件嵌入敏感信息的检测；支持识别文件多层压缩方式逃避检测行为，包含识别压缩文件的嵌套层数，并根据设定的阈值阻断；支持识别文档页眉、页脚、批注信息隐藏敏感信息的行为；支持识别修改文件扩展名方式逃避检测的行为；满足实际工作所需要的复杂策略，单条策略可以包含多个规则，内部规则之间可以通过 “AND/OR”，“条件”以及“排除”的逻辑组合在一起。不仅能够基于内容来制定策略，还能结合发送者/接收者，文件特征，通讯协议等来制定策略，支持针对特定数据内容，如：关键字、文件类型、文件大小、协议条件进行例外处理。提供大量的预定义策略模板，可以在模板策略的基础上，派生自定义策略。支持 IPV6 地址管理系统，支持 IPV6 路由配置，IPV6 地址管理 DLP 设备				
8	日志审计	绿盟	LAS NX3-HFA/V2.0	CPU:飞腾 FT-2000(2.6GHz,4 核)，操作系统：银河麒麟 V10，内存：32GB,硬盘：4TB+128GB,网络接口:1 个管理口,6 个千兆电口和 4 个千兆光，日志源授权数≥40。整机规格：1U 机箱；支持的	1	台	110000	110000

				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。支持的数据采集方式包括但不限于 SYSLOG、RSYSLOG、SNMP Trap、FTP、ODBC、JDBC、Net flow、WMI、二进制数据、专用 Agent 等方式采集日志。支持采集的设备厂家包括但不限于：NSFOCUS(绿盟科技)、Venustech(启明星辰)、Topsec(天融信)、DBAPPSecurit(安恒)、SANGFOR(深信服)、Hillstone(山石网科)、东软、瑞星、金山、网康、360网神、Dptech(迪普)、艾科网信、Imperva、Juniper(瞻博网络)、F5、Symantec(赛门铁克)、Deep Security(趋势科技)、MaAfee(迈克菲)、Fortinet(飞塔)、Windows、Linux/Unix、Cisco(思科)、HUAWEI(华为)、H3C(华三)、中兴、Apache、nginx 、IIS、WebLogic、Vmware、Kvm、Xen、OpenStack、Hyper-V、华为FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind 等。能实现海量日志数据的采集并保存原始日志数据。支持界面配置即可完成未识别日志接入，无需编写 xml；支持规则自适应日志接入，支持将新接收的日志信息与系统内置规则、自定义规则进行匹配，将匹配度最高的规则与接收				

				到的日志进行关联，完成自动接入；系统应能够实现范式化日志的枚举值管理，实现对范式化日志字段的灵活翻译；系统应支持日志源监控能力，包括采集器维度及资产维度的监控，资产维度支持展示资产详细信息。提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源 IP 信息；支持按类型、按日期(天)，手动、自动备份日志。支持设置日志存储备份策略，可设置备份周期、备份日志类型。支持日志备份远程服务器，如传送到 FTP 服务器。支持日志存储扩展，如 NFS 网络共享存储扩展。支持实时日志查询、历史日志查询。持全文检索、模糊检索、正则检索等多种方式。支持日志检索结果存储为日志监控视图。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。支持多源事件关联分析能力，包括单源过滤模式、多源时序模式和多源关联模式；支持基于事件分类的告警规则，支持短信、声音、邮件、界面提示等多种告警方式。支持告警抑制。支持资产监控，支持根据设备类别对资产进行分类，根据 IP 可下钻至资产的整体数据、告警及关联事件。支持资产标签，且至少 6 种标签以上，				

				根据标签可快速查询资产。支持资产以拓扑图形式展示，鼠标移动至资产图标可展示对应的资产信息。能够按照多种维度统计日志信息。支持统计分析报表与多种文件格式导出。支持自定义报表目录、LOGO 等。				
9	单向光闸	金电网安	单向导入系统 UniWay V5	2U 机箱　兆芯 KX-U6780A 银河麒麟 V10，冗余电源，内外端机 6 个 10/100/1000Base-T(RJ45)接口，2 个 SFP+万兆接口，含一个 MAN 口，一个 HA 口，一个扩展槽，一个 VGA 口，2 个 USB 接口；采用 “2+1”系统架构，由两个主机系统和一个单向导入隔离部件组成；入隔离部件采用 UPET 单向无反馈通信技术，保证物理信道绝对单向的情况下，实现数据高效、可靠传输；防止任何形式的信息从信任网络泄露。采用流控技术，实现可靠的单向无应答数据传输，两个主机之间不允许有应答包传输，支持流量控制；统基于加固安全操作平台，为主机提供深度防御；采用多级安全多核多线程并行安全操作系统；能够对两个主机系统提供多层次、高强度的安全防护，保护其重要进程、文件、数据不受黑客侵袭；采用对象互斥和线程守护技术，保护主要进程的安全性和稳定性。IPv4 和 IPv6，持专用客户端或 FTP、SFTP、NFS、SMB 方式实现单向文件传输；FTP、SFTP 传输方式：支持发送端为 client，接收端为 client 模式；支持发送端为 client，接收端为	2	台	120000	240000

				server 模式；支持发送端为 server，接收端为 client 模式；支持发送端为 server，接收端为 server 模式。支持/自动文件传输；支持文件增量单向传输；支持一对多或多对一传输；支持文件类型过滤；支持文件内容过滤；支持防病毒；支持文件大小过滤；支持文件名长度过滤；支持大文件传输；支持文件发送接收统计；支持文件备份重传；支持文件类型过滤和黑白名单；支持文件每秒文件传输限制；支持查看文件同步状态。采用基于专用客户端与网闸安全连接方式，提供多种主流数据库（SQLS、ORACLE、MYSQL、GBASE、KINGBASE 等）的单向传输，同步粒度可以达到表内具体字段；支持条件同步；支持外键表同步；支持多种增量同步方式，可分别定义增加、删除、修改的传输方式；支持异构数据结构以及代码语义的转换规则定义；支持数据整合业务；支持数据一对一、一对多、多对多的单向同步；支持数据备份重传功能；支持数据传输统计；支持防病毒。单向 UDP 传输功能可支持用户基于单向 UDP 传输开发的自定义协议应用；支持 UDP 组播传输。支持数据临时存放在本地磁盘；支持自动检测未正常传输的数据；支持传输数据备份功能。隔离部件之间采用光单向传输，为保证可靠性和安全性，单向传输所用的数据传输线不允许裸露在设备之外，可实现多台设备互相冗余的应用模式；基于				

				Bonding 模块技术，使一端机多网口冗余，可实现链路备份冗余的工作模式，支持 lacp、负载均衡、主备模式；三权分立：安全管理流程主要由安全管理员、系统管理员和安全审计员通过安全管理中心执行，分别实施系统维护、安全策略制定和部署、审计记录分析和结果响应等；管理端采用 B/S 结构，通过内端和外端专用的管理口进行配置，禁止通讯网口登录管理页面；支持指纹认证登录；支持角色切换，实现多种部署模式；支持界面超时设置；支持客户端 IP 和 MAC 白名单设置。支持 SYSLOG 协议，可与标准日志服务器平台无缝兼容，可实时发送设备运行状态，可查看系统 CPU、内存，磁盘使用率等信息，单向传输速率：4Gbps；系统整体时延：<5ns；丢包率：<10-10；误码率：<10-7				
合　　计								1253800.0

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）：江苏移动信息系统集成有限公司

日期：2023年2月2日