附件

**封面**

|  |
| --- |
| 用户需求书  项目名称：上海市公安局新一代移动警务基础设施子系统建设项目用户需求  责任单位： 上海市公安局科技信息化总队  项目负责人： 方伟杰  联系人及电话： 管晓明 22025886，13916251206 |

1. **主要内容**

**（一）背景与现状概述**

对标部局《全国公安移动警务建设总体技术方案（2016版）》和《全国公安移动警务平台升级改造项目建设任务书》等相关规范标准，按照《公安信息化建设“十四五”规划》“建设省级移动警务分平台，着力构建新一代公安移动警务体系”的要求，基于上海公安工作的实际需求为出发点，构建新一代移动警务平台基础设施。

该子系统建设完成后，将满足全市移动警务业务接入、日常监测管理等需求，并在移动警务场景化、实战化、社会化的应用和服务不断丰富背景下，确保平台能力能适应当前“大整合、高共享、深应用”公安信息化发展大势。充分发挥移动警务在公安大数据战略“最后一公里”中的支撑保障作用，推动全市各级公安机关智能化、移动化、融合化应用，全面提升全市公安战斗力水平。

1. **目标与任务**

按照公安科技信息化十四五规划要求，遵循公安大数据智能化建设总体规划，建设上海公安新一代移动警务平台，满足各级公安机关通过智能手机、便携微机等多形态、多功能移动警务终端，通过公众移动通信网等多种无线传输链路，接入公安移动警务平台，在保障网络安全的前提下，开展覆盖更广泛、传输更高效、内容更丰富、操作更智能、信息更安全的移动警务应用。

主要建设任务包括如下五点：

1、移动警务网络基础服务及安全接入通道设施建设

按照《公安信息化“十四五”规划》、《全国公安移动警务平台升级改造项目建设任务书》等部局文件关于“建设完善移动警务基础设施，扩容移动安全接入子平台，完善公安移动信息网，完善基础安全保障，增强智能管理能力”的要求，建设新一代移动警务平台网络基础服务及安全接入通道设施，实现公安移动信息网的智能管理和公安信息网的安全接入。建设内容包括域名服务器、时钟同步服务器、负载均衡、防火墙、入侵检测、安全接入代理网关、移动VPN接入网关、移动VPN接入网关（千兆）等设备。

2、便携微机安全接入基础设施

按照《全国移动警务终端装备“十四五”规划》、《全国公安移动警务平台升级改造项目建设任务书》、《便携式微型计算机移动警务终端接入与应用技术方案》等部局文件要求，丰富便携微机安全接入及应用场景，建设安全访问控制网关、安全访问控制中心等安全接入设备，支撑便携微机终端安全接入。

3、移动警务平台集中管控能力建设

按照《公安信息化“十四五”规划》、《全国公安移动警务平台升级改造项目建设任务书》等部局文件要求，以及《移动警务集中管控系统技术方案（V1.0）》指引，通过集中管控系统及配套区域安全管控体系、统一日志采集系统、网络流量安全审计系统数据采集子系统的建设，汇集各区域流量和日志数据，进行日志审计、关联分析、事件预警与溯源，为运维人员、安管人员提供决策支撑，并针对安全及运维事件设定相应的管控策略下发到区域安全管控系统及时进行响应处理。从业务、运行环境、安全等多个视角对移动警务整体运行情况和安全情况进行全面的态势感知。同时，通过移动警务平台区域管控和集中管控系统的建设，完成《公安网络边界平台集中监管实施方案》中相关信息的级联上报，实现对移动警务中关键边界设备的集中监管和安全态势可视化监测，及时发现潜在威胁，增强移动警务边界的透明度和可控性。

4、移动警务平台安全监测能力建设

按照部局考核要求，以及《公安移动信息网省市级安全监测体系建设方案》指引，通过安全监测体系涉及的安全监测中心-本地流量监测探针、安全监测中心-跨网流量监测探针的建设，监测公安移动信息网部/省/市三级互联通道及公安移动信息网与其他专网传输通道的网络安全风险，形成网络流量数据上报监测或管控系统；通过安全监测中心-综合扫描系统的建设，识别和发现市局公安移动信息网中的各类资产，检查网络中的各类脆弱性风险，将数据上报监测或管控系统，并提供有效的分析修补建议，提升网络环境的整体安全性，切实提升移动警务安全防护效能，规范移动警务安全运营管理与安全风险监测能力。

5、移动警务平台可信计算基础设施建设

按照《全国公安移动警务平台升级改造项目建设任务书》、GA/T 2001-2022《移动警务 可信计算总体技术要求》要求，建设可信管理网关，完善Ⅱ类系统和Ⅲ类系统的可信计算安全防护体系。

1. **技术性能指标与配置要求**

本节为本项目采购设备的具体要求，投标人应逐条响应各项指标要求。设备清单如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 单位 | 数量 | 指标要求 |
| 1 | 负载均衡 | 台 | 2 | 见1 |
| 2 | 域名服务器 | 台 | 1 | 见2 |
| 3 | 时钟同步服务器 | 台 | 1 | 见3 |
| 4 | 防火墙 | 台 | 2 | 见4 |
| 5 | 入侵检测 | 台 | 1 | 见5 |
| 6 | 可信管理网关 | 台 | 2 | 见6 |
| 7 | 统一日志采集系统 | 台 | 1 | 见7 |
| 8 | 网络流量安全审计系统数据采集子系统 | 台 | 1 | 见8 |
| 9 | 安全接入代理网关 | 台 | 1 | 见9 |
| 10 | 移动VPN接入网关 | 台 | 2 | 见10 |
| 11 | 移动VPN接入网关（千兆） | 台 | 1 | 见11 |
| 12 | 安全访问控制网关 | 台 | 1 | 见12 |
| 13 | 安全访问控制中心 | 台 | 1 | 见13 |
| 14 | 移动警务集中管控系统 | 套 | 1 | 见14 |
| 15 | 移动警务区域管控系统 | 套 | 1 | 见15 |
| 16 | 安全监测中心-综合扫描系统 | 套 | 1 | 见16 |
| 17 | 安全监测中心-本地流量监测探针 | 台 | 1 | 见17 |
| 18 | 安全监测中心-跨网流量监测探针 | 台 | 1 | 见18 |
| 19 | 系统集成 | 套 | 1 | 见19 |

1. 负载均衡

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构要求 | 软硬一体化设备，符合国产化要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 内存：16GB |
| 硬盘容量：480GB SSD |
| 电源：冗余电源 |
| 接口：6千兆电口+4万兆光口（含光模块） |
| 性能要求 | 4层吞吐量：≥20Gbps |
| 7层吞吐量：≥14Gbps |
| 4层并发连接数：≥2000万 |
| 7层并发连接数：≥400万 |
| 4层新建连接数：CPS≥30万 |
| 7层新建请求数：RPS≥50万 |
| 功能要求 | 提供包括多数据中心负载均衡、多链路负载均衡、服务器负载均衡。 |
| 实现对各个数据中心、链路以及服务器状态的实时监控，可根据预设规则，将用户的访问请求分配给相应的数据中心、链路以及服务器，进而实现数据流的合理分配，使所有的数据中心、链路和服务器都得到充分的利用。 |
| 支持轮询、加权轮询、最快响应时间、最小连接、最小流量等主流负载均衡算法。 |
| 支持通过编程语言实现自定义的流量编排，对IP、TCP、UDP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作。 |
| 链路负载均衡：  1、链路负载均衡支持轮询、带宽比例、加权最小流量、动态就近性和加权源IP哈希等算法；  2、支持基于五元组条件（源IP地址，源端口，目的IP地址，目的端口，传输层协议号）来进行出站访问的流量调度分发；  3、支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略；  4、支持多种链路检测方法，能够通过PING、TCP、HTTP等方式监控链路的连通性，当某一条链路故障时，可将访问流量切换到其它链路，保障用户业务的持久通畅；  5、支持基于域名的流量调度，针对特定网站选择指定的链路转发（提供设备操作界面截图证明材料）；  6、支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率（提供设备操作界面截图证明材料）。 |
| 服务器负载均衡：  1、支持源IP、Cookie（插入/被动/改写）、HTTP-Header、SSL Session ID等多种会话保持机制，支持跨虚拟服务的会话保持；  2、支持数据输出功能，输出必需包括客户端IP、x-forwarded-For IP、访问时间、访问IP、访问URL、响应时间和资源大小；（提供设备操作界面截图证明材料）  3、支持优先级算法下最少可用节点保障，优先级高的节点故障时会自动进行选举，保证优先级高节点的可用性；  4、支持常见的主动式健康检查功能，提供基于SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS，ORACLE/MSSQL/MYSQL数据库等多种类型的探测判断机制，支持对HTTPS服务进行内容健康检查；  5、支持HTTP被动健康检查，可配置指定检查URL、响应状态码、响应超时时间、统计时间以及可设置异常URL上限，并且能开启/关闭调试日志功能；（提供设备操作界面截图证明材料）  6、支持在同一个虚拟服务下同时配置多个IPv4和IPv6地址；（提供设备操作界面截图证明材料）  7、支持TCP策略，实现三层、四层和七层虚拟服务模式；  8、对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包。（提供设备操作界面截图证明材料） |
| 业务交付优化：  1、支持HTTP缓存功能，利用内存Cache缓存用户频繁访问的web内容，降低后台服务器的负载压力,提升用户访问的响应速度；  2、支持HTTP压缩功能，采用工业标准的GZIP或Deflate算法来压缩HTTP数据，从而减少传输数据量并降低带宽消耗，缩短客户端访问的下载等待时间；  3、支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。 |
| 运维管理：  1、支持全中文管理界面和HTTPS方式登录、用户角色管理、多级授权管理；  2、IPv6支持双栈模式，支持NAT46、NAT64、NAT66等协议转换。（提供设备操作界面截图证明材料 ） |
| 支持串接部署方式和旁路部署方式，支持三角传输模式。 |
| 其他要求 | 1、所投产品支持IPv6。 |

1. 域名服务器

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 规格：1U标准机架式设备 |
| 内存：16GB |
| 硬盘容量：2TB |
| 电源：冗余电源 |
| 接口：8个千兆电口，可扩展4\*1GE光 |
| 性能要求 | 每秒查询请求处理量≥50000 |
| 每秒进行的域名查找操作次数≥1500次 |
| 功能要求 | 专用DNS服务器，对公安移动信息网信息资源的域名进行管理和解析。  负责分配服务主机域名，并提供域名解析、域名请求转发、递归解析服务，同时为移动互联网、公安视频传输网、公安信息网中共享到公安移动信息网的服务提供域名转换服务。 |
| DNS特性：  1、支持可扩展的DNS权威、递归和缓存管理；  2、支持主辅区转换、辅区更新控制、辅区续期；  3、支持全面的记录类型（A,AAAA,CNAME,MX,NS,PTR,TXT,SRV,SPF等）；  4、支持记录设置生效时间和添加自定义属性；  5、支持URL解析跳转；  6、支持A、AAAA和PTR增删改联动；  7、支持快速智能解析、记录排序；  8、支持多区多视图；  9、支持父域子域支持平铺和层级嵌套展示；  10、支持视图、权威记录、转发区、存根区等资源记录的禁用启用；  11、支持区导入/导出；  12、支持基于视图的存根区、重定向；  13、支持基于视图的多种转发策略（顺序转发、RTT转发、白名单）；  14、支持共享区（多视图资源记录批量管理）、共享记录；  15、支持默认TTL，简化记录设置和管理；  16、支持域名查询控制，全局搜索；  17、支持DNS64，平滑IPv6演进，支持双栈DNS；  18、支持IDN；  19、支持根配置；  20、支持缓存管理；  21、支持完整的AD迁移配合；  22、支持AAAA过滤；  23、支持视图指定ACL 不进行递归查询；  24、支持基于域名解析负载均衡、动态调度；  25、支持基于子网、ISP、地址范围等用户区域配置和静态就近性策略；  26、内置国内主要运营商的地址库，支持基于运营商的解析负载调度；  27、内置主要地区的IP 地址库，支持基于物理位置的解析负载调度；  28、支持静态就近性 、全局可用性、轮询和加权轮询调度算法；  29、支持基于ICMP、UDP、TCP\_SYN、TCP、HTTP、HTTPS、FTP、SMTP 协议的应用健康检测模板定制；  30、可指定发起健康检测的设备节点，支持对应用服务同时调用多个健康检测模板；  31、根据应用健康检测结果进行解析调度，对于宕机的应用进行只告警或者不解析的处理；  32、支持二级域名注册，已注册的域名允许用户自助维护；  33、支持按视图比例负载请求；  34、支持区与视图绑定解析，定向引导解析结果；  35、支持与第三方链路设备联动，并基于链路负载，智能引导链路；  36、流量支持与第三方认证计费系统对接，基于用户身份智能选择上网链路。 |
| 管理特性：  1、全部功能GUI管理（https）；  2、支持审核工作流；  3、支持CLI 管理，支持console、telnet 和SSH 终端连接；  4、支持同Radius、TACACS+、LDAP、AD 域对接；  5、支持地图展示，主管理中心、备管理中心、节点设备拓扑展示云管理，所有设备集中管理；  6、状态展示， 正常、告警、离线、异常等状态分别展示；  7、支持SNMPV2/V3；  8、支持SFTP、Syslog；  9、提供第三方开发接口；  10、支持TFTP文件管理；  11、支持带外管理。 |
| 安全特性：  1、密码超限锁定；  2、支持基于源地址的管理员登入认证；  3、WEB缓存自动失效，保证管理安全；  4、支持DNSSEC，安全加固；  5、支持本地策略；  6、支持基于域名/IP/IP段/IP全地址的解析限速；  7、防范缓存中毒、域名劫持等主要的域名安全威胁；  8、防范伪造缓存的访问控制；  9、内置DNS防火墙，有效防范DNS攻击；  10、执行高性能模式自动切换，高负荷情况下优先保证基础服务能力；  11、支持Servfail防护；  12、密码超限锁定；  13、支持基于源地址的管理员登入认证；  14、自动发现非法DHCP服务器并告警；  15、非法DHCP报文过滤。 |
| 高可用性：  1、主备多管理中心；  2、支持双网卡主备/负载；  3、支持健康检测、宕机切换（Ping、TCP、HTTP、HTTPs多种策略）；  4、支持DNS服务状态同OSPF的联动，保证Anycast高可用；  5、支持基于视图的请求源地址；  6、支持请求源地址线路的监测、故障切换；  7、支持基于视图的失败转发；  8、支持7种网卡绑定模式；  9、定期数据备份，配置回滚；  10、支持统一下发升级文件，不同节点按需完成升级；  11、故障设备的即时替换，数据配置一键恢复。 |
| 日志与统计报告：  1、支持图形化统计报表，TOP IP、TOP 域名、QPS、解析类型、解析成功率、缓存命中率、网络流量监控等统计，支持全节点的总体统计；  2、支持统计报表的按时段历史查询；  3、支持用户操作日志；  4、DNS解析日志支持记录应答结果和解析延时信息；  5、告警阈值设置；  6、日志告警，多种方式发送告警信息。 |
|  |  |

1. 时钟同步服务器

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 规格：标准机架式设备 |
| 外设：北斗卫星接收天线、30米电缆及安装支架 |
| 电源：冗余电源 |
| 接口：4个千兆电口 |
| 性能要求 | 授时精度＜5ms |
| NTP请求量≥10000次/秒 |
| MTBF≥100000小时 |
| 功能要求 | 提供公安移动信息网授时服务。 |
| 支持北斗、CDMA等时间源，智能切换并跟踪各时间源。 |
| 支持NTP、SNTP标准协议。 |
| 支持NTP、SNTP、Telnet、SSH、FTP、SNMP、IPV4、IPV6等网络协议。 |
| 授时模式支持NTP Peer Client/Server Broadcast Multicast； |
| 客户端同步软件支持主流系统平台，主要支持SNTP1，2，3，4等协议，能够与局域网上的时间服务器时间同步。支持系统托盘、开机自动运行、手动设置同步周期。软件可以显示参考时间、原始时间、接收时间、传输时间、本地时间等信息及服务层次、时延、偏差等。 |
| 1PPS脉冲输出：BNC接头，1路，稳定度<=10ns（σ） |
| 支持远程唤醒、定时开关机。 |
| 支持Console模式、Telnet和SSH进行远程管理、配置和升级。 |
| 其他要求 | 1、所投产品具体软件著作权证书，提供证书复印件。 |

1. 防火墙

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构要求 | 软硬一体化设备，符合国产化要求 |
| 硬件要求 | 规格：标准机架式设备 |
| 内存：32GB |
| 硬盘容量：480GB SSD |
| 电源：冗余电源 |
| 接口：4千兆电口，4个万兆光口（含光模块） |
| 性能要求 | 网络层吞吐量≥45G |
| 应用层吞吐量≥30G |
| 防病毒吞吐量≥3G |
| 全威胁吞吐量≥3G |
| 并发连接数≥800万 |
| HTTP新建连接数≥20万 |
| 功能要求 | 提供L2-L7层各类威胁的检测和防护，能够有效应对传统网络攻击和未知威胁攻击。 |
| 支持多种访问控制，包括基于IP、端口、协议类型、MAC、时间的访问控制策略，能对网络连接数进行控制，基于状态检测技术的访问控制和深度包检测。 |
| 支持抵御地址欺骗、拒绝服务、网络扫描等网络攻击行为。 |
| 支持应用类型控制、应用关键内容控制。 |
| 支持手工或自动IP/MAC地址绑定。 |
| 支持802.1q、RIP、OSPF、BGP、SNMP等协议。 |
| NAT功能支持多对一、一对多和一对一等多种地址转换方式。 |
| 支持IPv4/IPv6双栈工作模式。 |
| 支持多维度流量控制功能，支持基于IP地址、应用、时间设置流量控制策略，保证关键业务带宽日常需求。 |
| 支持基于IP的会话控制策略，实现并发连接数的合理限制。 |
| 提供防病毒能力，能对病毒进行检测和阻断。 |
| 支持URL分类过滤功能。 |
| 支持文件过滤功能。 |
| 支持NTP时间同步，准确记录日志时间。 |
| 提供对日志事件的记录、存储和管理功能，提供以syslog等标准方式输出日志信息；支持对日志的统计分析和报表功能；日志存储至少6个月。 |
| 支持在线、离线等升级方式。 |
| 提供双机热备，包括主-主模式和主-备模式。 |
| 支持透明、路由、混合等多种部署模式。 |
|  |  |

1. 入侵检测

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构要求 | 软硬一体化设备，符合国产化要求 |
| 硬件要求 | 规格：标准机架式设备 |
| 内存：32GB |
| 硬盘容量：480GB SSD |
| 电源：冗余电源 |
| 接口：4个千兆电口、4个万兆光口（含光模块） |
| 性能要求 | 网络层吞吐量≥40G |
| 应用层吞吐量≥20G |
| IPS吞吐量≥5G |
| 并发连接数≥800万 |
| 功能要求 | 支持应用控制功能，可对主流应用进行检测与控制。 |
| 支持URL过滤功能，支持管控非法、违规网站的访问行为。 |
| 支持应用识别功能，可识别主流应用。 |
| 支持https解密功能，可对加密流量进行防护。 |
| 支持IMAP、FTP、RDP、SSH、TELNET等主流应用协议进行深度检测与防护。 |
| 文件过滤功能支持基于文件传输方式、文件类型等维度的管控策略配置。 |
| 内置不低于10000种漏洞规则，支持用户自定义IPS规则。 |
| 支持僵尸主机检测功能，内置僵尸网络特征库，可识别主机的异常外联行为。 |
| 产品支持策略生命周期管理功能，支持对安全策略变更进行统一管理，便于策略的运维与管理。 |
| 产品支持管理员双因素认证功能，用户通过用户名/密码和Key等不同方式登陆产品管理界面。 |
| 产品支持路由模式、透明模式、旁路镜像模式等多种部署方式。 |
|  |  |

1. 可信管理网关

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构要求 | 软硬一体化设备，符合国产化要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| CPU：2颗主频2.5GHz（16核32线程）国产CPU |
| 内存：2\*32GB |
| 硬盘容量：2\*1.2TB |
| 电源：冗余电源 |
| 接口：4个千兆电口 |
| 性能要求 | 可信密码运算SM2签名验签：≥100次/秒 |
| 可信密码运算SM3运算速率：≥50Mbps |
| 可信管理签名应用数：≥10,000 |
| 最大终端连接数：≥100,000 |
| 在线并发数（TPS）：≥300 |
| 可信密码运算SM2签名验签：>100次/秒 |
| 功能要求 | 包含报告管理、基准管理、裁决管理、策略管理、PIK证书服务、安全基线管理以及安全支撑服务等功能。 |
| 可接受上海市公安局移动警务终端可信管理组件生成的可信报告。 |
| 支持对PIK证书、可信基准、可信报告、可信策略进行安全管理。 |
| 支持可信策略管理，支持终端可信计算策略管理，提供策略下发和策略解析，通过可信软件基实现策略执行。 |
| 提供可信证书管理功能，提供可信密码服务，对PIK证书提供申请、下发、更新、注销等管理功能。 |
| 提供安全基线认证，支持对移动警务终端可信基准、终端型号安全基线的生成和在线基线认证。 |
| 提供安全监控和审计功能，具备安全可信日志审计机制和风险告警机制。 |
| 支持对接公安部移动警务可信管理中心，可实现对移动警务终端可信管理报告的上传。 |
| 可部署在上海市公安局移动警务平台公安移动信息网和公安信息网环境。 |
|  |  |

1. 统一日志采集系统

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构要求 | 软硬一体化设备，符合国产化要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 处理器:3.0GHz主频8核16线程国产CPU |
| 内存：32GB内存 |
| 硬盘容量：4TB硬盘 |
| 接口：4个千兆RJ45网口 |
| 性能要求 | 平均页面响应时间：≤2S |
| 统计分析结果查询时间：≤30秒 |
| 并发用户数：≥10个 |
| 每秒可接收日志条数：≥10000条 |
| 功能要求 | 采集上海市局移动警务平台各类设备的运行性能数据和运行日志，并通过kafaka、FTP、SFTP等协议上报到移动警务集中管控系统进行分析展示。 |
| 采集网络设备的运行状态，包括CPU、内存、网络等使用情况以及由系统产生的各类日志信息等。 |
| 采集服务器的运行状态，包括CPU、内存、网络等使用情况以及由系统产生的各类日志信息等。 |
| 采集安全设备的运行状态，包括CPU、内存、网络等使用情况以及由系统产生的各类日志信息等。 |
| 支持通过SNMP、SYSLOG、FTP、KAFKA等协议采集系统运行状态及日志。 |
| 支持SNMP V3协议，支持SNMP OID自定义。 |
| 支持通过KAFKA、FTP等协议将数据上报到区域或集中管控系统。 |
| 支持对采集的数据进行清洗、压缩、归档、缓存功能。 |
| 支持在首页展示实时snmp信息及今日日志采集数和上报数，并可查询历史snmp信息，提供功能截图证明。 |
| 支持展示所有归档策略，包括订阅的主题、日志文件存储策略、归档文件保留天数、使能标志，提供功能截图证明。 |
| 支持归档策略信息修改，包括修改订阅主题的日志源类型、采集协议、日志级别和日志源IP等信息。 |
| 支持列表展示缓存策略，包括订阅的主题、全文搜索引擎地址、集群名称、索引名称、日志保留周期、使能标志等信息，提供功能截图证明。 |
| 支持列表展示上报策略，包括订阅的主题、上报的IP地址、上报端口、上报协议、启用压缩保存、使能标志等信息，提供功能截图证明。 |
| 支持列表展示日志源，包括系统名称、日志源类型、IP地址、采集协议、采集模式、日志扫描周期、最近扫描时间等信息，提供功能截图证明。 |
| 支持日志源发现列表展示，包括系统名称、日志源类型、IP地址、采集协议、发现时间、审核状态等信息。 |
| 支持修改日志源，包括系统名称、日志源类型、日志类型、IP地址、MAC地址、采集协议、分组名、主题、并发数等信息，提供功能截图证明。 |
| 支持归档日志列表展示，包括归档文件名、大小、行数、文件创建日期、日志源类型、采集协议、IP、日志级别、操作等信息，提供功能截图证明。 |
| 支持以图表及列表展示各项采集统计信息，包括日志源类型、采集协议、日志级别等。 |
| 支持SNMP OID 标签库管理，包括字典列表的新增和修改。 |
| 支持备份系统参数及系统数据，并可选择历史备份实施恢复。 |
| 所投产品支持与市局现有移动警务平台监管级联系统无缝对接，提供相关证明文件。 |
| 其他要求 | 1、所投产品适配国产化操作系统和硬件环境 |

1. 网络流量安全审计系统数据采集子系统

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构要求 | 软硬一体化设备，符合国产化要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 处理器：3.0GHz主频8核16线程国产CPU |
| 内存：32GB |
| 硬盘容量：4TB |
| 接口：4个千兆RJ45网口、2个万兆光口 |
| 性能要求 | 平均页面响应时间：≤3S |
| 支持流量解码吞吐量：≥5Gbps |
| 功能要求 | 采集上海市局移动警务平台的网络流量数据，并通过kafka、FTP等方式将元数据推送到移动警务集中管控系统进行综合分析。 |
| 流量采集：收集并分析网卡上的数据，将生成的信息以NF9（NetFlow v9）的格式存盘或导入到流量分析模块中； |
| 流量分析：  1) 链路层协议分析，依据以太网的封包格式还原解析出源MAC、目的MAC、网络层协议类型、网络层数据包大小等信息。根据上层协议类型分组统计输出网络流量、数据包长分布等信息；  2) 网络层协议分析，还原解析出ARP、IP和ICMP协议数据元字段并进行统计分析；  3) 传输层协议分析，还原解析出TCP和UDP协议报文字段元数据并进行深度分析，至少包括： TCP通讯对的延迟；TCP通讯对的重传率、任意时间段内TCP 第一次握手(SYN)超时端口分布、TCP正常流量-脏流量对比、TCP结束状态类型分析等；  4) 应用层协议分析，还原解析出DNS、FTP、HTTP、HTTPS等协议报文字段元数据并进行深度分析，其中DNS协议按DNS请求响应每个会话统计输出一条信息、FTP协议需统计FTP连接会话并还原出传送的文件副本、HTTP协议需对请求头深度解析还原出refer/query/cookie/http\_client\_ip等关键信息并按会话进行统计分析。 |
| 数据处理：支持对流量分析数据进行压缩、清洗、填充等处理。 |
| 支持将流量分析结果数据通过fka、FTP等方式报送至区域或集中管控系统； |
| 首页支持图形化展示系统运行情况，包括内存、CPU、磁盘的利用率，提供功能截图证明。 |
| 协议配置支持链路层、网络层、控制层和应用层协议，提供功能截图证明。 |
| 流量查看功能支持UDP、ICMP、TCP、IGMP等协议在不同时间点的流量情况，提供功能截图证明。 |
| 数据过滤功能支持配置BPF过滤条件、单个文件输出大小、原始报文保存等信息，提供功能截图证明。 |
| 数据关联支持地理位置信息的关联，包括关联字段、关联信息描述、启用状态、操作等信息，提供功能截图证明。 |
| 数据推送支持Kafka设置、服务器设置、主题分区设置，其中主题分区设置支持配置输出协议、Topic主题、分区、推送状态，提供功能截图证明。 |
| 系统管理功能支持用户管理、角色管理、时间配置、FTP配置、SNMP配置、Syslog配置、备份管理和升级管理。 |
| 升级管理功能支持系统回滚操作，默认回滚最新升级的版本。 |
| 备份管理支持配置备份、配置恢复、备份导入和备份导出。 |
| 支持操作日志、故障日志、登录日志和系统日志的查询。 |
|  |  |

1. 安全接入代理网关

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 处理器：2.40GHz主频8核16线程CPU |
| 内存：16GB内存、8GB CF卡 |
| 硬盘容量：1TB |
| 接口：2个千兆网口、6个万兆光口 |
| 性能要求 | 国密SM4算法多通道实测吞吐量：≥2Gbps |
| 功能要求 | 支持RSA、SM2、SM4主流密码算法； |
| 支持IP+MAC+端口号+协议的绑定； |
| 支持与VPN网关进行多通道连接和各通道流量均匀分配； |
| 支持B /S、C/S应用和FTP、HTTP、HTTPS、UDP各种协议类型应用的接入，支持多种服务系统的同时接入； |
| 支持虚拟接入服务，可配置服务名称、均匀分配启用、VPN服务端、用户证书和运行日志，提供功能截图证明。 |
| 支持Watchdog配置，管理员可根据网关机器类型选择相应的选项，提供功能截图证明。 |
| 支持基于数字证书的高强度认证；对传输信息进行加密。 |
| 支持虚拟接口管理，可配置、修改、删除虚拟接口。 |
| 支持证书配置管理，包括生成证书请求、用户证书配置、用户证书链配置、证书备份恢复，提供功能截图证明。 |
| 支持证书链配置管理，包括上传、删除。 |
| 支持虚拟接入服务管理，包括服务名、状态、动作、路由缓存和日志等信息，提供功能截图证明。 |
| 支持虚拟接入服务参数配置，可配置服务器地址、端口、隧道模式、加密算法、压缩、通讯协议、日志等信息，提供功能截图证明。 |
| 支持虚拟接入服务日志管理、包括日志查看、查询和下载。 |
| 证书配置支持硬件证书、用户证书和证书链配置。 |
| 通道选择支持来源网络地址（子网掩码、MAC地址、端口号）、目的网络地址（子网掩码、端口号）、协议、通道信息，提供功能截图证明。 |
| 支持系统备份，可以将系统中所有管理员所作过的配置和相应数据进行备份，以便在必要时做系统恢复时使用。 |
| 支持加密访问请求，并对接市局已建设移动VPN安全接入网关构建虚拟通道实现安全接入，提供相关对接方案。 |
| 支持与市局已建设安全接入代理网关热备部署，提供相关热备方案 |
| 资质要求 | 1、所投产品具备第三方检测报告，提供报告复印件。 |

1. 移动VPN接入网关

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 处理器：2颗2.6GHz主频的12核/24线程CPU |
| 内存：32GB |
| 硬盘容量：4TB |
| 接口：1个加密卡备用槽、2个千兆电口、6个万兆光口 |
| 性能要求 | 在线用户数：≥20000 |
| 并发用户数：≥10000 |
| 网络吞吐量（TCP协议）：≥5Gbps |
| 功能要求 | Android客户端和Windows客户端仅支持以隧道模式接入； |
| 客户端支持自动检测更新和升级； |
| 客户端支持运行日志一键上报； |
| 客户端支持开机自启动和快速重连； |
| 服务端支持加密算法自定义配置； |
| 支持RSA和SM2证书同时接入； |
| 服务端资源配置支持指定客户端类型访问设置； |
| 服务端支持配置导入导出功能； |
| 服务端支持两台设备配置同步 |
| 移动接入服务支持HTTP、HTTPS、TCP和VPN等资源配置，提供功能截图证明文件 |
| 支持对接外接权限系统开展权限验证，提供功能截图证明。 |
| 支持虚拟接口管理，可添加、修改和删除虚拟接口。 |
| 支持证书配置管理，包括生成站点证书请求、站点证书管理、证书链配置和黑名单管理。 |
| 提供生成证书请求界面，包括站点名称、机构、部门、电子邮件、密钥类型、密钥位数、证书DN项唯一性和私钥密码，提供功能截图证明。 |
| 服务状态支持查看服务运行时间、运行日志、连接日志、虚拟网卡状态、双机热备状态、开机启动状态等信息，提供功能截图证明。 |
| 资源管理支持配置资源名称、类型、主机名、资源掩码、端口、URI、客户端类型、代理类型等信息，提供功能截图证明。 |
| 支持查看在线用户信息，包括状态、客户端证书CN、实际IP地址、绑定虚拟IP、客户端环境、上传下载数据量、接入时间等信息，提供功能截图证明。 |
| 移动接入服务支持配置封装类型、黑名单验证、二级代理地址、虚拟网网段、加密算法、源地址转换、设置证书编码等信息，提供功能截图证明。 |
| VPN运行模式支持：单线程、多线程和多进程三种模式。 |
| 支持客户端管理，包括客户端名称、平台、版本、上传时间、状态等信息。 |
| 支持系统升级和远程维护。 |
| 支持配置导出功能，可以将系统中所有管理员所作过的配置和相应数据进行导出备份，以便在必要时做系统恢复时使用。 |
| 支持流量监控统计功能，可以统计网络接口的流量情况，可提供列表展示和图标展示。 |
| 支持链路聚合实现高可用性，可配置聚合接口、模式、IP、掩码、状态等信息，提供功能截图证明。 |
| 支持纳入市局现有移动警务平台监管级联系统监管，提供相关监管对接方案。 |
| 支持利用本次采购的负载均衡产品实现与市局现有移动VPN接入网关负载部署，提供相关负载实现方案。 |
|  |  |

1. 移动VPN接入网关（千兆）

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构要求 | 软硬一体化设备，符合国产化要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 处理器：3.0GHz主频8核16线程国产CPU |
| 内存：16GB |
| 硬盘容量：2TB |
| 接口：4个千兆RJ45网口、2个万兆光口 |
| 性能要求 | 在线用户：≥20000 |
| 并发用户：≥10000 |
| 网络带宽：≥3Gbps |
| 功能要求 | Android客户端和Windows客户端仅支持以隧道模式接入； |
| 客户端支持自动检测更新和升级； |
| 客户端支持运行日志一键上报； |
| 客户端支持开机自启动和快速重连； |
| 服务端支持加密算法自定义配置； |
| 支持RSA和SM2证书同时接入； |
| 服务端资源配置支持指定客户端类型访问设置； |
| 服务端支持配置导入导出功能； |
| 服务端支持两台设备配置同步 |
| 移动接入服务支持HTTP、HTTPS、TCP和VPN等资源配置，提供盖原章的截图证明文件 |
| 支持对接外接权限系统开展权限验证，提供功能截图证明。 |
| 支持虚拟接口管理，可添加、修改和删除虚拟接口。 |
| 支持证书配置管理，包括生成站点证书请求、站点证书管理、证书链配置和黑名单管理。 |
| 提供生成证书请求界面，包括站点名称、机构、部门、电子邮件、密钥类型、密钥位数、证书DN项唯一性和私钥密码，提供功能截图证明。 |
| 服务状态支持查看服务运行时间、运行日志、连接日志、虚拟网卡状态、双机热备状态、开机启动状态等信息，提供功能截图证明。 |
| 资源管理支持配置资源名称、类型、主机名、资源掩码、端口、URI、客户端类型、代理类型等信息，提供功能截图证明。 |
| 支持查看在线用户信息，包括状态、客户端证书CN、实际IP地址、绑定虚拟IP、客户端环境、上传下载数据量、接入时间等信息，提供功能截图证明。 |
| 移动接入服务支持配置封装类型、黑名单验证、二级代理地址、虚拟网网段、加密算法、源地址转换、设置证书编码等信息，提供功能截图证明。 |
| VPN运行模式支持：单线程、多线程和多进程三种模式。 |
| 支持客户端管理，包括客户端名称、平台、版本、上传时间、状态等信息。 |
| 支持系统升级和远程维护。 |
| 支持配置导出功能，可以将系统中所有管理员所作过的配置和相应数据进行导出备份，以便在必要时做系统恢复时使用。 |
| 支持流量监控统计功能，可以统计网络接口的流量情况，可提供列表展示和图标展示。 |
| 支持链路聚合实现高可用性，可配置聚合接口、模式、IP、掩码、状态等信息，提供功能截图证明。 |
| 支持纳入市局现有移动警务平台监管级联系统监管，提供监管对接方案。 |
| 支持利用本次采购的负载均衡产品实现与市局现有移动VPN接入网关负载部署，提供负载实现方案 |
| 其他要求 | 所投产品适配国产化操作系统和硬件环境 |

1. 安全访问控制网关

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 处理器：3.0GHz主频8核16线程CPU |
| 内存：64GB |
| 硬盘容量：4TB |
| 接口：2个千兆电口，4个万兆光口，2个万兆bypass光口 |
| 性能要求 | 支持同时在线会话:≥30000 |
| 支持并发会话数（非通道模式）:≥8000/秒 |
| 支持并发会话数（通道模式）:≥2000/秒 |
| 功能要求 | 网关支持对接控制中心开展注册管理，包括网关名称、服务地址、端口、机构、区域、集群、在线状态和检索标签等信息，提供功能截图证明。 |
| 支持本地IP地址、掩码和静态路由的配置； |
| 支持在本地进行网关寻址地址和服务端口的配置； |
| 支持与控制中心之间进行双向认证的加密控制通信通道的建立； |
| 支持接受控制中心的配置统一管理和设备信息的上报更新； |
| 支持单包授权功能，默认情况下网关系统的服务端口对所有终端关闭，只有进行了单包验证的客户端才可以进行TCP连接； |
| 支持TCP和UDP双栈基于国密算法的加密通道连接； |
| 支持路由模式转发、网桥模式和SNAT转发模式； |
| 支持bypass功能；通过万兆Bypass网口实现硬件级的链路逃生功能。在网关软件系统故障或者硬件故障的情况下，启用Bypass端口备用电路保障业务连通。 |
| 支持后端服务TCP和UDP服务资源的代理。 |
| 支持单包授权、APP流量代理、双向认证和加密传输、基于访问域的动态访问控制等功能，提供公安部检验报告证明复印件。 |
| 支持配置安全访问控制中心的寻址IP和端口，配置后网关自动在对应地址的控制中心上进行注册上线，并接受管理。 |
| 网关支持在访问控制中心侧进行访问域网关配置，支持网关信息修改和查询。 |
| 网关客户端支持终端软硬件信息，并且可以基于读取终端信息进行账户和终端设备的绑定申请。 |
| 网关客户端支持用户名密码登录和数字证书登录，提供支持对接上海市局现有移动警务数字证书的证明文件。 |
| 读取app可以读取到的终端软硬件信息，并且可以基于读取终端信息进行账户和终端设备的绑定申请 |
| 网关支持系统备份和系统还原，并可查看备份历史记录和还原历史记录。 |
| 网关支持配合控制中心开展集群部署。 |
| 其他要求 | 所投产品适配国产化操作系统和硬件环境 |

1. 安全访问控制中心

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 处理器：3.0GHz主频8核16线程CPU |
| 内存：64GB |
| 硬盘容量：4TB |
| 接口：4个千兆电口、4个万兆光口 |
| 性能要求 | 支持最大用户数：≥30000 |
| 支持新建用户会话数：≥2000个/秒 |
| 功能要求 | 支持通过组织机构和自定义部署区域对访问控制网关进行集中注册和集中管理，支持基于服务地址、服务端口、集群状态、在线状态、检索标签等属性信息进行查询过滤，提供截图证明复印件； |
| 支持网关部署区域的个性化自定义于管理网关进行关系绑定； |
| 支持基于网关列表进行网关的快速启停和服务端口修改操作； |
| 支持应用管理和被管理应用的单点登录功能，注册管理的第三方应用的登录状态可以由控制中心维护，提供单点登录能力，应用客户端无需进行额外的登录动作; |
| 支持基于组织机构的人员管理，管理内容包括：用户名、姓名、人员类型、所属机构、检索标签、状态、在线状态、创建时间等内容，支持人员账户信息列表的表格导入和导出； |
| 支持终端设备的类型、终端IMEI号码、操作系统、系统版本等终端信息的集中列表管理，支持列表信息的导入和导出； |
| 支持自定义标签管理，可以将标签与人员、设备和人员+终端设备的人机关系、资源、网关等对象进行关联，方便进行检索。 |
| 支持人员、终端设备以及人员+终端设备绑定的访问主体管理； |
| 支持人员+终端设备的绑定申请的管理，系统管理员可以基于绑定申请进行绑定关系的审批； |
| 支持IP策略和时间策略的管理；时间策略包括起止时间区间和起止时间区间内的星期策略。 |
| 支持基于访问主体、访问客体和访问策略进行关联配置访问域，同一个访问域中的访问主体可以访问对应的访问客体。访问主体可以由用户、设备或用户+设备绑定主体构成。访问客体由应用资源和网关构成。 |
| 支持配置访问域的的域类型、域名称、成员范围、启用状态、检索标签等信息。 |
| 支持人员-资源的关联资源检索，包括人员所对应资源的机构、服务名称、地址端口、协议、部署区域和检索标签，提供盖章的功能截图证明。 |
| 支持配套认证认证客户端软件的接入，支持基于移动警务数字证书的认证方式； |
| 客户端软件支持已经认证用户的访问权限查看，包括可访问的网关IP、资源IP和端口； |
| 资源管理支持配置服务资源的所属机构、服务名称、服务地址、服务协议、服务端口、部署区域、联系人、会话签注、检索标签、有效期等信息，提供功能截图证明； |
| 支持会话签注功能，可在安全访问控制网关在进行业务数据转发的时候将应用的会话标识插入到HTTP-header中，便于后续应用层网关进行数据发起方的身份溯源和检控； |
| 客户端软件支持便携式微型计算机移动警务终端认证和接入管理； |
| 客户端软件支持安卓、嵌入式、Linux等类型操作系统，支持UOS系统和麒麟系统的服务器或虚拟机的接入管控； |
| 支持单包授权功能，默认情况下控制中心系统的服务端口对所有终端关闭，只有进行单包验证通过的客户端和网关系统才可以进行加密连接。 |
| 其他要求 | 所投产品适配国产化操作系统和硬件环境 |

1. 移动警务集中管控系统

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 功能要求 | 支持数据接入、处理和治理，提供资产管理、模型管理、身份管理、知识管理、事件管理、安全审计、运行监测、态势感知和级联管理等功能。 |
| 数据接入：支持KAFKA/MQ/JDBC/ODBC/HTTP/ HTTPS/ FTP/SFTP等各种协议数据接入。实现对各类专业设备的资源数据、参数数据、告警数据、性能数据、日志数据的统一采集和管控，屏蔽不同厂家、不同型号设备接口的差异。 |
| 数据处理：  1、提供可视化数据处理流程管理工具，支持将数据提取、清洗、关联、比对、标识、分发等不同的节点以DAG的形式组织起来，形成数据处理流程，提供功能截图证明。  2、提供数据处理任务管理功能，支持将各类数据处理流程配置成数据处理任务，支持数据处理任务调度执行和状态监控，提供功能截图证明。 |
| 数据治理：  1、支持数据资产管理，包括数据资源目录管理和数据血缘管理。  2、支持数据安全管理，包括数据分级分类管理和数据权限管理。  3、支持数据质量管理，及时发现、监测定位、跟踪解决各类数据质量问题，形成数据质量问题的闭环处理，以保证数据质量的稳定可靠和数据运维管理等。  4、支持数据运维管理，采集数据接入、处理、组织和服务等各项任务的状态信息，对异常状态进行告警和处置，实现对各任务的实时监控和管理。 |
| 模型管理：  1、提供可视化离线建模工具，支持分布式离线运算和跨库运算，数据加载后，支持纯内存表运算、实体表与内存表关联运算、实体表与实体表关联运算等多种运算方式，并将生成的结果输出到kafka,hive,elasticsearch等多种存储，提供功能截图证明  2、数据分析人员可利用该工具提供的建模算子，通过设置算子的参数，以及节点之间的数据流向，完成模型设计与运行工作，提供功能截图证明 |
| 资产管理：  1、支持资产类别、资产属性、资产关系三位一体的动态资产数据模型管理，实现资产模型数据的可定义、可编辑、可动态扩展，提供功能截图证明  2、支持资产实例管理，包括对不同类别的资产实例、资产关系、资产变更记录数据的同步入库、变更维护、查询检索，导入导出，提供功能截图证明  3、资产关系管理，支持关系编码、关系名称、匹配模式、关联类型、关系描述、关系状态和相关操作管理，提供功能截图证明 |
| 身份管理：  1、支持组织机构的数据信息管理，包括查询、注册、变更、注销、同步等功能。  2、支持各类人员数据信息管理，包括注册、修改、注销、查询、同步及与组织机构关联等功能。 |
| 安全审计：支持行为合规、运维操作、实体安全等安全审计，包括模型查询和审计记录查询与研判处置。 |
| 事件管理：支持安全事件管理，包括信息安全事件模型查询、事件处置预案管理、安全事件查询与处置等。 |
| 知识管理：支持内部IP地址库、漏洞信息库、恶意IP库为等各安全知识数据的管理与维护。 |
| 运行监测：  1、支持对设备、网络、终端、应用等各类资产的运行状态监测，发现异常告警通知管理员处置。  2、设备运行状态监测包括设备的类型、名称、区域、当前状态、IP地址、运维厂家、CPU、内存、存储、历史事件等信息，提供功能截图证明。 |
| 级联管理：支持与本地的区域管控系统横向级联及其他集中管控系统的纵向级联，同步用户、终端、网络、应用、服务、事件数据。 |
| 系统兼容：支持与市局现有移动警务平台监管级联系统对接，提供相关证明文件。 |
| 态势感知：支持以全局的视角呈现用户、终端、网络、应用、服务等维度的态势信息。 |
| 用户态势支持展示用户访问热点应用、用户活跃趋势、用户数分布、活跃用户信息。 |
| 终端态势支持展示终端流量使用情况、终端数分布情况。 |
| 网络态势支持展示网络负荷分布、重点设备监控情况。 |
| 应用态势支持展示应用使用情况、活跃用户情况、热度应用情况。 |
| 服务态势支持展示服务信息总览、资源异常信息监控情况。 |
| 终端状态监测支持查看平台已注册移动终端的状态信息，包括终端数量、终端ID、终端类型、绑定号码、姓名、单位、绑定状态、设备型号、系统版本号、SN号、在线/丢失状态和最后连接时间，提供功能截图证明。 |
| 资源状态监测支持查看平台已注册资源服务的状态信息。包括资源数量、异常资源数、资源标识、资源名称、资源类型、资源状态和监控状态。提供功能截图证明。 |
| 用户画像支持描述用户的基本信息（含机构、警种、岗位变动等信息）、关联终端信息（含终端标识、类型、型号、IP、IMEI、手机号、证书号等信息）、安全卡资产信息（含安全卡标识、状态、类型、证书SN、申请时间、暂停时间、撤销时间等信息）。提供功能截图证明。 |
| 设备画像支持描述设备的基础信息和变更信息。 |
| 终端在线分析支持查看各单位终端配备情况、使用情况等统计信息。 |
| 生产厂商具备公安网接入条件，可在紧急保障时提供研发级的远程支撑能力。 |
| 支持对接公安部移动警务监管中心，提供相关证明文件。 |
| 符合《公安网络边界平台集中监管实施方案》关于级联上报模块的要求，实现对移动警务边界平台的集中监管和安全态势可视化监测，及时发现潜在威胁，增强移动警务边界的透明度和可控性。 |
| 性能要求 | 登录时间：≤3秒 |
| 页面响应时间：≤2秒 |
| 查询时间：≤5秒 |
| 页面数据更新时间：默认5秒 |
| MTTF（MeanTimeToFailure，平均无故障时间）：≥2000小时 |
| MTTR（MeanTimeToRepair，平均修复时间）：≤4小时 |
| 系统操作并发用户数：≥200 |

1. 移动警务区域管控系统

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 功能要求 | 符合《全国公安移动警务建设总体技术方案（2016版）》、《移动警务集中管控系统技术方案》的区域管控要求，提供资产管理、身份管理、运维配置、安全控制、级联管理等功能模块。 |
| 资产管理：支持与集中管控系统同步资产数据模型，实现资产模型数据的可定义、可编辑、可动态扩展。支持资产实例管理，包括对不同类别的资产实例、资产关系、资产变更记录数据的同步入库、变更维护、查询检索，导入导出。 |
| 身份管理：支持组织机构的数据信息管理，包括查询、注册、变更、注销、同步等功能。支持各类人员数据信息管理，包括注册、修改、注销、查询、同步及与组织机构关联等功能。 |
| 集中运维：提供统一认证，管理员通过统一入口登陆，便可以登陆登出已经在区域管控系统中注册管控要素或其依赖的系统，对管控要素的运行参数、安全策略等配置数据进行导出、导入、备份和恢复等管理。 |
| 安全控制：可对管控要素下发安全控制指令并验证指令执行结果，应急处置安全事件，阻断正在发生的安全事件或避免事件再次发生。 |
| 级联管理：支持与本地的集中管控系统横向级联，同步用户、终端、网络、应用、服务、事件数据。 |
| 采用基于云原生架构的微服务框架设计，具有较高的兼容性，可以部署在市局提供的虚拟化或云环境中。 |
| 资产管理可以查看资产名称、资产编号、资产标识、录入人、创建时间、采集时间、启用时间、资产状态、资产备注、安全等级、所属部门、IP地址等信息。 |
| 资产属性管理支持维护属性名称、数据类型、数据范围、属性单位、可编辑情况、状态等信息。 |
| 设备状态监测可查看平台已注册硬件物理设备的状态信息，包括当前状态、设备名称、平台区域、设备类型、IP地址、归属单位、运维厂家、CPU、内存、存储空间、历史事件等信息，提供功能截图证明。 |
| 应用状态监测可查看平台已注册移动应用的状态信息，包括I、II、III类应用数量和分布。 |
| 终端状态监测可查看平台已注册移动终端的状态信息，包括终端ID、类型、绑定号码、姓名、单位、绑定状态、型号、版本号、组件厂商、SN号、在线、丢失状态、最后连接时间等信息，提供功能截图证明。 |
| 资源状态监测，可查看平台已注册资源服务的状态信息，包括资源标识、资源名称、资源类型、资源状态和监控状态等信息。 |
| 支持人员信息管理，包括人员类型、姓名、身份证号、机构、岗位、在职状态等信息，并支持查阅变更记录，提供功能截图证明。 |
| 平台级联支持上报数据概览，包括平台、机构人员、移动应用、网络设施、应用支撑、安全事件、服务资源等数量信息，提供功能截图证明。 |
| 安全控制模块可查看、配置、管理针对不同维度不同对象的策略模板，并添加下发任务。策略模板包括策略ID、模板名称、订阅设备、策略场景、策略内容等信息，提供功能截图证明。 |
| 支持系统升级和备份恢复功能。 |
| 性能要求 | 登录时间：≤3秒 |
| 页面响应时间：≤2秒 |
| 查询时间：≤5秒 |
| 页面数据更新时间：默认5秒 |
| MTTF（MeanTimeToFailure，平均无故障时间）：≥2000小时 |
| MTTR（MeanTimeToRepair，平均修复时间）：≤4小时 |
| 每秒可接收日志条数≥1000条 |

1. 安全监测中心-综合扫描系统

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 处理器：8核16线程CPU |
| 内存：16GB |
| 硬盘容量：256GB |
| 接口：4个千兆电口、4个千兆光口 |
| 性能要求 | 单套系统支持≥15个B类IP地址范围的并发扫描 |
| 系统扫描时网络带宽平均占用<5Mbps |
| 单套系统针对有效IP数量为5千点网络的资产发现与识别周期<1小时 |
| 单套系统最大可扫描资产数量≥5万点（在线有效IP） |
| 功能要求 | 识别和发现本地移动信息网中的各类资产，全面检查网络中的各类脆弱性风险，支持各项数据的统计分析与大屏展示。 |
| 支持与监测或管控系统对接，数据上报到监测或管控系统。 |
| 能够对网络内部的资产进行快速发现和自动识别与分类，能够自动区分终端PC、应用服务器，网络设备（含交换机、路由器、网络边界设备、网络安全设备等）以及物联网设备等类别，支持资产类别、操作系统类型识别，支持网络设备与物联网设备的品牌、型号等信息的识别。 |
| 支持资产发现、漏洞检测、弱口令检测，并配合监测或管控系统形成资产库等。 |
| 采用主动式远程网络空间测绘技术实现，不需要进行镜像数据分析，不需要部署客户端等代理程序。 |
| 综合扫描系统验证漏洞的准确性并提供有效的分析修补建议，提升网络环境的整体安全性。 |
| 支持对资产特征进行自动聚类分析，支持人工设定某一类特征的设备指定设备的资产类型、品牌等信息。 |
| 能够在不影响业务正常运行的前提下检测网络中设备和应用的简单口令或出厂默认口令，包含数据库、SSH、TELNET、FTP、RDP等应用以及常见中间件等的弱口令检测。 |
| 能够对网络中设备和应用进行漏洞检测，包含常见操作系统、数据库应用以及常见中间件应用漏洞进行检测。 |
| 能够检测网络中私自接入的无线类设备，能够检测设备的双网卡接入；能够通过扫描方式对终端通过智能手机、双网卡、网络代理等方式的非法外联行为进行检测。 |
| 分级部署支持自上而下的检测任务与策略统一下发、检测结果的自下而上的自动汇总。 |
| 支持分级管理及分布式部署等方式。 |

1. 安全监测中心-本地流量监测探针

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构要求 | 软硬一体化设备，符合国产化要求 |
| 硬件要求 | 规格：2U标准机架式设备 |
| 处理器：3.0GHz主频8核16线程国产CPU |
| 内存：16GB |
| 硬盘容量：480GB SSD硬盘 |
| 接口：4个千兆电口、2个万兆光口 |
| 性能要求 | 网络层吞吐量：≥3Gbps |
| 应用层吞吐量：≥1.2Gbps |
| 功能要求 | 采集上海市局移动警务平台的网络流量数据，并通过kafka、FTP等方式将元数据推送到监测或集控系统进行综合分析。 |
| 支持全流量数据抓取、解析和分析能力 |
| 解析协议可支持FTP、DNS、SMB、SNMP、DHCP、ICMP、SSH、RDP、LDAP、Telnet、Kerberos、Redis、Web类及Mail类等19种主流数据协议； |
| 支持网络脆弱性识别能力，包括FTP漏洞攻击、Web类弱密码风险、非Web类弱密码风险和数据库风险识别等能力； |
| 支持网络入侵检测识别能力，包括扫描探测、口令爆破、Web攻击、恶意邮件、后门攻击、Webshell检测、应用漏洞攻击、通用组件漏洞攻击以及网络横向攻击检测等； |
| 支持威胁情报检测能力，包括APT情况告警、Rootkit告警、感染型病毒、蠕虫病毒、木马病毒、勒索病毒、挖矿病毒、恶意下载等； |
| 系统默认自带常规风险分析模型并支持自定义构建模型，可支持基于语法引擎分析、恶意流量行为分析、UEBA用户行为分析和日志关联分析等。 |
| 其他要求 | 所投产品适配国产化操作系统和硬件环境 |

1. 安全监测中心-跨网流量监测探针

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构要求 | 软硬一体化设备，符合国产化要求 |
| 硬件要求 | 规格：标准机架式设备 |
| 处理器：3.0GHz主频8核16线程国产CPU |
| 内存：32GB |
| 硬盘容量：4TB |
| 接口：4个千兆RJ45网口、2个万兆光口 |
| 性能要求 | 支撑平均页面响应时间：≤3S |
| 支持流量解码吞吐量：≥5Gbps |
| 功能要求 | 采集上海市局移动警务平台的网络流量数据，并通过kafka、FTP等方式将元数据推送到监测或管控系统进行综合分析。 |
| 安全监测中心-跨网流量监测探针负责出市流量采集，并对其进行预处理和上报。 |
| 静态规则检测，支持对接并在监测或管控系统形成各类Web攻击、异常流量相关安全检测日志。 |
| 风险分析，支持对接并在监测或管控系统形成基于攻击源相关安全检测日志。 |
| 资产梳理，自动识别区域网段内资产信息，形成资产清单。 |
| 应用访问内容检测，识别流量中包含的具体应用类型、域名信息、应用协议、DNS信息、令牌信息和访问的URL特性等，形成审计日志。 |
| 流量元数据采集，基于TCP、UDP、 FTP、HTTP、DNS、POP3、SMTP、SMB等协议采集流量的原始数据，并上报监测中心进行分析。 |
| 文件还原，支持从HTTP、FTP、Mail等协议解析流量包中文件信息，并进行文件还原。 |
| 首页支持图形化展示系统运行情况，包括内存、CPU、磁盘的利用率，提供功能截图证明。 |
| 支持将流量分析结果数据通过fka、FTP等方式报送至区域或集中管控系统；支持Kafka设置、服务器设置、主题分区设置，其中主题分区设置支持配置输出协议、Topic主题、分区、推送状态，提供功能截图证明。 |
| 系统管理功能支持用户管理、角色管理、时间配置、FTP配置、SNMP配置、Syslog配置、备份管理和升级管理。 |
| 升级管理功能支持系统回滚操作，默认回滚最新升级的版本。 |
| 备份管理支持配置备份、配置恢复、备份导入和备份导出。 |
| 支持操作日志、故障日志、登录日志和系统日志的查询。 |
| 其他要求 | 所投产品适配国产化操作系统和硬件环境 |

1. 系统集成

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 系统集成 | 1、完成所有硬件设备的安装与调试，完成所有软件产品部署、联调等工作，应可根据用户要求进行定制。在项目集成和实施过程中必需保证不影响现有系统的稳定运行。  2、需根据公安部建设要求，充分考虑、设计并提供移动警务系统日常管理运维所需的整体技术保障软硬件环境。  3、在项目实施过程中，应同步考虑并提供系统整体部署上线所需的数据库及中间件等，需提供项目实施所需（不限于）六类网线、光纤线以及系统搭建所需各类辅助材料。  4、应全面适配并兼容新一代移动信息网基于国产化环境的服务器或虚拟化平台。  5、应按照用户方需要提供界面化的运维监控页面，以便于故障和性能的监控。  6、本项目采集的日志信息要满足部局规范、满足用户提出的采集规范，能按要求上传至各级集控审计平台。 |

**（四）项目进度**

项目整体建设周期为自合同签订之日起至2026年10月31日前完成全部建设内容并通过验收。

具体进度安排如下：

1、设备交货，合同生效后45日内全部设备到货，要求：

（1）设备到货后将提供的货物全部运抵采购方指定地点，经采购方签收确认。

（2）设备到货清点时，成交供应商需提供设备制造商对采购的所有设备（含配件）的产品序列号。

（3）采购方收货后根据设备的技术规格要求和质量标准，对设备进行检查验收，如果发现数量不足或有质量、技术等问题，成交供应商应负责按照采购方的要求采取补足、更换或退货等处理措施，并承担由此发生的一切损失和费用。

2、要求成交供应商在设备到货后120日内完成全部软硬件设备上线部署和系统测试，并具备试运行条件；试运行期不少于60日后成交供应商向采购人提请验收。

**（五）实施和技术服务要求**

1、成交供应商需提供成功实施其技术方案所必需的技术支持和工程服务，包括系统设计、工程设计、项目管理、工程实施、验收、培训等，并需提交详细的工程服务方案。

2、成交供应商应保持项目团队稳定。未经用户方同意，项目负责人在项目整体验收前不得变更。

3、本项目系统集成质量控制和文档需满足公安部对移动警务建设相关技术要求。

4、设备安装和调试

成交供应商负责所有设备的安装调试，组织专业技术人员在设备保修期内进行现场安装、调试，及时解决出现的质量问题，具体要求如下：

（1）要求成交供应商负责设备安装机房的环境检测和电路测试，对于不满足设备安装要求的机房环境和电源、电路等，成交供应商负责提出符合设备安装条件的解决方案。

（2）设备安装和联网调试由成交供应商负责，提交用户一个可使用、稳定可靠的系统。

（3）设备安装过程中所需的网线、光纤、电缆、接头、工具及仪器仪表均由成交供应商提供，所需费用由成交供应商自行承担。

5、培训

成交供应商负责技术培训，在设备安装调试前成交供应商组织一次基本培训，培训内容主要包括设备功能、性能、参数配置等，并讲解和演示产品的性能、结构、工作原理，使采购方正确掌握使用和维护的基本技能。

6、其他技术要求

（1）成交供应商针对本项目的投标产品免费质保期内由原厂商提供服务。成交供应商提供的安全接入代理网关、移动VPN接入网关、安全访问控制网关、安全访问控制中心、移动警务集中管控系统、移动警务区域管控系统等设备需能够与市局现有移动警务系统平台无缝对接，实现联动操作。

（2）成交供应商对任何陈述的条款答复都需符合实际指标与客观事实，任何隐瞒或不尊重事实的阐述均有可能承担被拒绝接受或废除投标资格或合同的风险。在项目实施过程中，采购方将在认为必要时，对成交供应商所响应满足的某项功能或指标要求成交供应商配合进行测试、检查并核实。

7、项目实施团队要求

（1）成交供应商需指定项目负责人负责本项目的实施活动，项目负责人具备信息系统项目管理师证书优先考虑。项目团队成员应包括项目负责人在内的5人以上的专业服务团队，其中技术人员具有CISP证书的优先考虑（附名单简介、证书及社保缴纳证明材料）。

（2）免费质保期内，成交供应商提供3人以上固定的维护队伍（附名单简介及社保缴纳证明材料），其中包括1名驻场运维人员，驻用户现场提供运维服务（驻场地点：武宁南路128号，至少5\*8小时驻场服务，节假日或重大活动保障期间应根据科技信息化总队要求，提供驻场保障），提供这名工程师的工作简历，并得到最终用户的确认。成交供应商如需更换驻场工程师需事先与最终用户协商确定。

8、售后服务

（1）系统及设备的免费质保期应从本项目验收通过之日起计算，免费质保期为3年（36个月）。

（2）要求成交供应商需免费提供本项目采购的所有设备3年或以上原厂保修以及7×24×4的备件先行服务（即每周7天每天24小时响应用户硬件故障申请，并保证在接到用户申请4小时内备件到达用户现场），2小时内修复，内容包括但不限于保修期限、保修条件、保修范围和备件先行服务等方面。

（3）要求成交供应商提供3年或以上免费的系统维护服务，免费质保期内，成交供应商需提供每周7天、每天24小时的电话响应服务，并在接到用户维护通知后1小时内赶到现场、作出响应，2小时内完成系统维护服务。

（4）免费质保期内，当设备故障时，故障设备维修无法在24小时内恢复的，需提供同型号的备件顶替，不得影响网络和安全系统的正常运行，同时设备中硬盘等存储介质需交由用户方保管。

（5）免费质保期内，成交供应商需承诺提供服务，定期（每月至少1次）对用户的系统进行巡检，并协助用户对隐患和故障进行解决和追查。

（6）若用户在免费质保期内对软硬件环境进行调整，成交供应商应免费完成相关集成工作，包括但不限于将硬件设备及应用软件部署至不同公安业务网络等。

**（六）投标单位、招标方案及投标书应答要求**

1. 投标单位要求

供应商具备ISO9001质量体系认证、CCRC信息安全服务资质认证证书的优先考虑。

1. 投标书应答要求

（1）该项目为“交钥匙”工程，项目中涉及的各个环节需在方案中一并考虑。

（2）供应商在标书中需按要求制作详细的设备规格、技术参数偏离表。

（3）供应商需提供详细的响应方案，包括设备配置、设备部署、业务流程、运行维护、人员培训、售后服务等内容。方案内容需符合用户实际需求，并满足公安部移动警务相关规范要求。

1. 报价要求

（1）供应商应提供详细的报价，包括软硬件采购、集成或人工等费用。

（2）供应商应提供详细的报价清单，包括：每个项目的名称、型号、单价、数量、总价。报价按单项开列，最终费用以人民币报价、结算。

（3）供应商应单列系统集成费，并明确费用的组成、比例和计取方法。

（4）供应商报价应为含税价。

**（七）项目验收要求**

1、本项目系统建设和验收工作应符合《公安信息化建设“十四五”规划》和《移动警务系统 总体技术要求（GA/T 1561-2019）》相关要求。

2、成交供应商完成的项目应达到的质量标准应符合国家、地方及相关政府管理部门和行业与本项目有关的各项技术标准、规范要求，并满足实际需求，前述标准、规范等不一致的，以要求高（严格）的为准。

3、验收形式由招标方指定，成交供应商需配合验收相关工作，验收所需费用（测试费、等保测评费等）包含于本项目报价中。

成交供应商需提供整个系统包括设备的测试与验收的方案和详细的验收计划。成交供应商应对每个设备及整体系统进行完善的测试（包括系统功能测试和性能测试）和自验收，提供测试文档和自验收文档。验收相关资料：所有验收文件、测试报告、配置文档、设备技术资料及使用说明书，资料要提交完整的两套，以作设备留档备案。