附件-技术参数及要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **规格参数** | **★**单位 | **★**数量 |
| 一 | **视频图像共享平台服务** | | | |
| **1.1** | **软件服务** |  |  |  |
| 1.1.1 | 视频存储管理软件 | 提供视频共享平台的管理服务，满足不低于6465路视频存储接入。 | 项 | 1 |
| **1.2** | **基础资源服务** |  |  |  |
| 1.2.1 | **公安视频专网** |  |  |  |
| 1.2.1.1 | 视频共享平台服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥20个物理核、主频频率≥2.1GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 1.2.1.2 | 设备接入服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥16个物理核、主频频率≥2.3GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 1.2.1.3 | 视频级联服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥16个物理核、主频频率≥2.3GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 1.2.1.4 | 流媒体服务器 | 1.CPU配置：采用X86架构，配置≥1颗CPU，每颗CPU≥8个物理核、主频频率≥2.1GHz； 2.内存配置：≥32GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 19 |
| 1.2.1.5 | 存储管理服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥12个物理核、主频频率≥2.2GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+2块3840GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 4 |
| 1.2.1.6 | 视频异构接入服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥20个物理核、主频频率≥2.3GHz； 2.内存配置：≥64GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/6/10/50/60，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 12 |
| 1.2.1.7 | 视频异构管理服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥20个物理核、主频频率≥2.4GHz； 2.内存配置：≥64GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/6/10/50/60，2GB缓存带掉电保护； 5.以太网连接：≥4个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 4 |
| 1.2.1.8 | 视频存储集群 | 存储架构：采用分布式文件存储架构的集群，支持多节点并发处理。 1.节点性能：2颗不低于24核ARM处理器，主频≥2.6GHz；内存不低于192GB，DDR4； 2.单存储节点网口：≥2个千兆网口，≥4个万兆光口（含多模光模块）； 3.单存储节点硬盘：主存盘≥33块企业级SATA硬盘，单盘容量≥14TB，≥3块960GB 企业级SSD，节点硬盘满配置；操作系统不占用该硬盘； 4.存储整体可用业务容量≥12500TB； 5.存储节点数要求：为保证存储整体吞吐能力，节点数≥47个； 6.▲内部保护：提供副本或EC容灾保护,支持+2.+3.+4 等EC余配比配置，可支持4节点同时故障，业务不中断，数据不丢失（提供具有 CMA 或 CNAS 标识的第三方检验（检测）机构出具的检验（检测）报告扫描件或关键页（报告封面页、盖章页、说明页））； 7.▲离散存储：将数据呈离散式分布存储到各个存储节点上，磁盘间容量偏差小于2%，节点间容量偏差小于 0.2%（提供具有 CMA 或 CNAS 标识的第三方检验（检测）机构出具的检验（检测）报告扫描件或关键页（报告封面页、盖章页、说明页））； 8.支持根据业务需要配置多种重构速度模式； 9.具备SSD盘磨损度等寿命监控和HDD故障预测告警； 10.存储自身具备数据生命周期管理功能，可根据规则自动删除过期数据并回收资源，无需第三方设备参与； 11.图形化管理，可监控系统.节点.磁盘级别使用状态.网络吞吐等实时运行状态。 12.RAS要求：热插拔硬盘，热插拔式冗余电源.风扇。 | 套 | 1 |
| **二** | **视频图像解析平台服务** | | | |
| **2.1** | **软件服务** |  |  |  |
| 2.1.1 | 公安视频图像解析平台人像算法及应用 | 提供公安视频图像人像解析算法和应用，实现视频专网和公安信息网双网双平台部署运行。提供满足不少于6465路图片流（人体人像）的解析及应用授权，双网双平台按需自行配置软件能力。 （一）在公安视频专网，实现对图片数据按照人脸、人体等不同属性进行全结构化解析，支撑打击破案、治安防控等场景应用。主要功能需包括： 1.图片流解析：支持对公安感知源产生的抓拍图片流进行解析；每路≥并发0.3次/秒，日均过人≥3000张，双网双平台按需自行配置软件能力 2.系统在集群环境中，单个综合管控节点出现异常断电情况时，综合管控服务器不中断；单个视图解析节点出现异常断电情况时，该节点上的接入解析任务可自动调度至其他解析节点上继续运行。 3.系统在集群环境中，单个视图特征库节点出现异常断电情况时，特征库服务器不中断，断电节点恢复后该节点上特征数据不丢失。 4.支持对公安感知源产生的抓拍图片流进行解析,支持对批量的图片中的人脸、行人、机动车、非机动车等目标进行检测、属性提取，并对行人目标进行人脸及人体特征提取。 5.对图片流解析产生的属性及特征数据，应与公安视频图像解析平台视频算法产生的特征模型保持一致，支持与公安视频图像解析平台视频算法产生的特征值及数据在公安网内融合应用。 6.支持布控功能，支持对目标进行范围内布控，找出目标的出现地点以及轨迹，目标一旦出现立即告警，支持长期布控、临时布控、重点区域布控等多种布控模式。 7.支持时空过滤功能，系统能够通过时间和视频源过滤人脸抓拍结果（包含抓拍时间、抓拍视频源、抓拍大图），并能够对抓拍大图进行缩放、下载，并能够对大图中的对象进行裁剪、检索、入库、布控操作。 8.支持把视频源的不同的场景进行打标签，以便更加贴近实际使用场景。包含住宅区、学校、医院、交通枢纽、办公写字楼、商场、娱乐场所、街面 、政府机关等标签分类。 9.系统支持通过深度学习算法模型对检测到的人脸进行多种类型的属性识别，属性识别类别应包括性别（男、女）、帽子款式（无帽子、雷锋帽、其他帽子）、眼镜款式（无眼镜、太阳镜、透明色）、胡型（无胡子、一字胡、山羊胡、其他胡型）、年龄段（老年人、成年人、儿童）、头盔（有、无）、口罩位置（正常佩戴、露出鼻孔、露出嘴巴、未戴口罩）、刘海（有、无）、耳机款式（无耳机、头戴式耳机、其他耳机），并支持基于人脸属性识别结果结合时空过滤条件对人脸抓拍图片库进行检索； 10.系统支持通过深度学习算法模型对检测到的人体进行多种类型的属性识别，属性识别类别包括性别、发型、发色、附属物有无、伞颜色、口罩颜色、帽子款式、帽子颜色、包款式、包颜色、上衣款式、上衣长度、上衣颜色、下装颜色、下装长度、鞋子款式、鞋颜色、上衣纹理、下装纹理、眼镜款式、年龄、人体角度、工作服款式（普通衣服、商务制服、工人服、厨师服、医护服、警服、消防服、美团外卖服、饿了么外卖服）、人员状态、是否抽烟、是否穿反光衣、是否戴口罩，并支持基于属性识别结果结合时空过滤条件对人体抓拍图片库进行检索。 （二）在公安信息网，对视频专网摆渡到公安信息网的解析数据进行分析，结合公安信息网数据构建以视图检索、布控告警、档案应用为核心的智能应用，有效确定人员身份，实现人员和车辆时空轨迹刻画、人员关系、高危人群定位及重点关注人群异常情况分析，实现重点关注对象布控、关系分析及异常事件的预防。主要功能需包括： 1.支持对人脸、人体特征值进行存储，具备按照时间对时空特征库中的特征自动过期，或者根据容量百分比预警删除。 2.支持布控特征库特征管理,支持单布控特征库批量导入人脸特征,支持单布控特征库批量删除人脸特征,支持单布控特征库批量查询获取人脸特征。 3.▲亿级人脸库规模下，以脸搜脸首位命中率不低于99%；前五位命中率不低于99.5%；前十位命中率不低于99.9%。（ 需提供有效的国家安全防范报警系统产品质量监督检验中心或公安部安全与警用电子产品质量检测中心出具的测试报告扫描件证明） 4.支持上传一张图片后自动对图片中的人脸、人体和车辆同时进行检测，用方框标注出检测结果，并支持对未识别的人脸进行手动三点标注与选择、未识别的人体和车辆进行手动框选标注与选择，同时可对图片进行镜像、左转、右转、放大、缩小操作的功能。 5.人像档案基础应用：支持在人像档案中查看人员的身份信息、标签信息、轨迹信息、预警信息、车辆信息等，可分析人员的行为规律。 6.支持将全息档案聚类的结果进行大数据分析，并结合线索发掘出具有嫌疑的目标人或目标车辆，通过与底库数据比对，形成多种人员关系及行为特征挖掘的技战法功能，支持时空档案过滤、频繁过人、时空碰撞、首次出现、感知离开、同行人分析、昼伏夜出、连续出现等多种基本技战法功能。 7.人像档案分析应用：支持对人像档案进行分析，通过挖掘历史数据时间、空间等关系，形成多种技战法功能，提升主动发现潜在风险的能力。 8.算法应具备人脸戴口罩检测性能，人脸戴口罩检出率≥99%，识别准确率≥99.9%,误检率≤0.1%。 9.系统能将检索历史通过节点化图形方式展示检索的时间，区域及搜索图片，并且可以通过点击相应节点重新发起搜索流程。 10.支持布控特征库1:N检索,可将人脸特征在一个或者多个布控特征库进行1：N检索。 11.▲40亿人体抓拍库规模下，上传人体图片进行以图搜图轨迹检索，结果返回平均响应时间不超过3秒。（ 需提供有效的国家安全防范报警系统产品质量监督检验中心或公安部安全与警用电子产品质量检测中心出具的测试报告扫描件证明） 12.系统应能够对个人敏感信息（如：身份证ID等）进行加密和脱敏处理，并支持按用户角色设置敏感信息查看权限，只有授予权限的用户才可以查看到个人敏感信息，否则只能查看到脱敏后的信息；支持通过全局开关控制所有用户的敏感信息查看权限。 13.支持对戴口罩、戴鸭舌帽、戴墨镜的人脸图片进行聚类归档；支持对同一人的青年人脸图片、中年人脸图片、老年人脸图片进行聚类归档。 14.支持关系图谱功能，系统能够通过时间、视图源、人员标签、关系类型（同预警关系、同行关系等）、同行次数等条件查询人员关系图谱，人员关系支持多级拓展，并支持在地图上进行档案人员和相关人员轨迹比对。 15.支持对档案中的抓拍进行人工研判，剔除识别有误的抓拍，提高档案质量，支持查看档案修改记录，对档案进行手动调整后支持回退，避免误操作。 16.支持人员标签，视图源标签，关系标签等多种标签，标签可体现人员基本属性，人员行动规律，人员衣着外貌属性等多个属性标签类别，全方位对公安关注的人员进行标签化刻画，方便使用民警进行群体筛查。 | 项 | 1 |
| 2.1.2 | 公安视频图像解析平台车辆算法及应用 | 提供公安视频图像解析平台车辆算法及应用，实现视频专网和公安内网双网双平台部署。支持不低于1369 路车辆卡口全结构化解析授权。 一、车辆二次识别 1、车牌号码及颜色识别 可提取车辆号牌号码、号牌颜色（可识别包含但不限于黄、白、黑、蓝、绿、新能源绿、新能源黄绿七种颜色车牌），可判断车辆有无牌号。 2、号牌类别识别 可识别大型汽车前号牌、大型汽车后号牌、大型汽车-挂车号牌、小型汽车号牌、教练车号牌、警用车号牌（限定“警”）。 3、车身颜色识别 支持系统能够对抓拍图片中十三种车身颜色（红、黄、绿、蓝、紫、粉、棕、银、橙、金、白、灰及黑）进行识别的功能。 4、车型识别 ▲车型信息识别支持精确到车辆的品牌、型号及年款，具备对车辆头部、尾部照片进行识别，在白天光照正常、夜间补光正常、车辆特征人眼可辨识的条件下，可通过车头照片识别不少于5000多种车型，可通过车尾照片识别不少于3000多种车型。（需提供有效的国家安全防范报警系统产品质量监督检验中心或公安部安全与警用电子产品质量检测中心出具的测试报告扫描件证明） 5、车辆类型识别 ▲支持系统能对抓拍图片中11种车辆类型（轿车、越野车、商务车、面包车、皮卡车、小型货车、大型货车、中小型客车、大型客车、拖拉机、特种车辆）进行识别的功能。（需提供有效的国家安全防范报警系统产品质量监督检验中心或公安部安全与警用电子产品质量检测中心出具的测试报告扫描件证明） 6、车辆特征识别 车体特征识别：可识别天窗、行李架、车身喷字。 车头特征识别：可识别年检标贴数量、左/右侧遮阳板、左/右侧反光、挂件、纸巾盒、摆件、卡片。 车尾特征识别：可识别LED显示屏、抱枕、玩偶、贴纸、纸巾盒、杂物、反光识别特征。 主/副驾区域特征识别：可识别主/副驾驶区域是否有人；主/副驾驶区域人员是否系安全带；主/副驾驶区域人员是否拨打电话。 7、渣土车识别 支持渣土车、渣土车未遮盖识别。 8、危险品车识别 支持危险品车、危险品车无押运员识别。 9、特种车辆识别 支持识别校车、集装箱货车、油灌车、搅拌车、出租车、消防车、公检法车、工程抢险车、军车、渣土车、公交车、长途客车、教练车、救护车、运钞车、环保车、宣传车、禽畜运输车、箱式货车、殡仪车、工业工程车、行政执法车。 二、车辆应用（双网双平台部署） （一）智能搜车 1、综合搜车 综合搜车包括：按车型搜车、按车牌搜车、按类别搜车、特种车辆搜索4种。 2、以图场景搜车（以图搜车） 支持系统上传图片，对场景图片中可识别车辆进行识别分析，选择某一车辆目标，检索出该车或与该车特征相似的车辆所经过的视频监控点位及对应车辆信息，并按相似度排序的功能。 3、人脸搜车 应支持对上传图片中的面部特征进行识别，与过车记录中的车辆内部人员面部进行比对，搜索过车记录的功能。 4、模糊特征搜车 支持选择车头特征或车尾特征条件，检索出符合条件的车辆。 5、批量车牌搜车 批量车牌搜车用户通过系统提供的模板，将车牌号码填入excel模板导入系统，实现批量车牌的搜索功能。 6、同车型搜车 一键上传过车图片后，系统自动识别图片中信息，并与车型库做匹配，搜索在某时空范围内与上传图片相同车型的过车记录。 7、渣土车检索 支持根据是否遮盖、过车时段、搜索位置条件检索出所有过车记录中符合条件的渣土车信息。 8、危险品车检索 支持根据有无押运人员、过车时段、搜索位置条件检索出所有过车记录中符合条件的危险品车信息。 9、冷链运输车检索 主要针对冷链运输车的管控，可根据时间段、区域等条件，检索出所有过车记录中符合条件的冷链运输车信息。 （二）车辆研判 1、初次入城 依据时间、区域、回溯时长等行车信息，快速检索过车记录、筛选出初次入城车辆的功能。 2、落脚点分析 系统支持对目标车辆的历史路径信息进行挖掘，发现车辆可能落脚停留地点的功能。 3、相似车牌串并 支持车牌号码、车辆颜色、相差位数、车辆型号、车辆类别、过车时段、搜索位置条件，筛选出与目标车牌相差1位或2位的车辆。 4、频繁过车 支持过车次数、车辆型号、车辆类别、车辆颜色、车牌号码、过车时段、搜索位置条件，快速筛选限定时间段内、区域内出现次数超过限定次数的车辆。 5、轨迹重现 支持系统对车辆在某时段内的过车数据进行汇总分析，重新绘制行车轨迹。 6、驾乘人脸识别 支持自动提取车辆前排驾乘人员清晰人脸图片，并推送到人脸解析模块进进行比对分析，落地身份信息。 7、遮挡面部 支持系统能够识别前排驾乘人员放下遮阳板遮挡面部的行为。 8、同行分析 支持系统通过车牌号查找出与其同行设定次数的车辆信息。 9、多点碰撞 支持自定义车辆型号、车辆类别、车辆颜色、行驶方向、车牌号码、车牌颜色、过车时段、搜索位置条件进行关联碰撞，筛选出符合多个碰撞条件的车辆。 10、实时目标车辆追踪 支持实时检索出选定号牌的车辆信息及过车图片，并结合地图动态展示。 11、昼伏夜出 支持根据隐匿时间、排除车牌、车辆类别、车辆型号、搜索位置条件，检索出夜间出行、白天隐匿的车辆。 12、双胞胎车检测 支持根据过车时段、车辆类别、车牌号码、搜索位置条件，筛选出过车时间相近、但出现位置不合逻辑的车辆。 13、出入城分析 支持通过设置数据来源、时间范围、出入城卡口、车辆型号、车辆类别等条件检索出严重驻留的车辆目标。 14、滞留车辆管理 支持通过设置数据来源、时间范围、回溯时长、出入城卡口、地区等条件检索出所需目标。 （三）布控稽查 1、精确车牌布控 通过输入布控标题、布控时段、时间范围、区域、接收人、审批人、布控原因等条件，提交布控，完成布控流程闭环。 2、批量车牌布控 通过输入布控标题、号码导入、布控时段、时间范围、区域、接收人、审批人、布控原因等条件，提交布控，完成布控流程闭环。 3、模糊车牌布控 通过输入布控标题、模糊车牌、品牌型号、布控时段、时间范围、区域、接收人、审批人、布控原因等条件，提交布控，完成布控流程闭环。 4、按车型布控 通过输入布控标题、品牌型号、车牌号码、车辆类别、布控时段、时间范围、区域、接收人、审批人、布控原因等条件，提交布控，完成布控流程闭环。 5、以图布控 通过输入布控标题、导入图片、布控时段、时间范围、区域、接收人、审批人、布控原因等条件，提交布控，完成布控流程闭环。 | 项 | 1 |
| 2.1.3 | 公安视频图像解析平台视频算法及应用 | 1.支持前端视频摄像机的接入，对视频、图片接入任务进行管理，包括添加、删除等，支持视频的分屏播放。 2.支持对视频流进行全结构化解析，对视频中的人脸、人体、机动车、非机动车等要素进行检测、跟踪及解析，平均每路日均采集目标数≥16000张，双网双平台按需自行配置软件能力，支持不少于500路视频流全结构化解析。 3.支持对视频流进行解码，对视频中的人脸、行人、非机动车、机动车等目标进行检测、跟踪、属性提取，产生场景大图、目标小图、基于大小图的目标检测框坐标、目标小图在场景大图中的坐标、目标属性、人脸角度等。 4.支持通过视频流解析并提取，人脸特征、人体特征及人脸-人体关联关系。 5.视频流全结构化解析后产生的人脸、人体属性及特征值数据，应与公安视频图像解析平台人像算法中图片流解析算法产生的特征模型一致，支持将视频流全结构化解析后的数据摆渡到公安信息网解析平台进行融合，与公安视频图像解析平台人像算法产生的数据一起在公安信息网实现图搜、聚档等应用。 6.支持设置视频流解析（人脸+人体+非机动车+机动车）ROI区域。 7.支持获取视频流点播RTSP地址，通过此地址点播全结构化视频的同时可携带目标检测框位置信息。 8.支持对视频流进行场景事件解析，发现视频中出现的打架斗殴、人群聚集、违规横幅、人员越线等事件，并输出事件类型、时间、场景大图，支持不少于1500路场景事件解析。 9.支持对视频流进行解码分析输出人群过密、人群滞留、人群入侵、人群聚集、人群分散、人群逆行、社交距离过近等事件告警，告警信息包括告警场景大图和告警位置信息等。同时支持跨线计数功能。 | 项 | 1 |
| 2.1.4 | 智慧公安应用服务 | 依据《公安视频图像智能化建设应用指南》，结合解析平台数据和其他数据，拓展特色化视频图像实战应用，充分发挥视频图像数据价值。基本要求如下： 1.智能机器人：为公安基层提供警务智能机器人，减少重复录入工作；实现无人中台坐席能力；打通部、省、市系统，使业务流转智能自动化，提供不少于10项机器人配置服务。 2.公安地图平台：在公安信息网提供高新区地图18级（pgis标准）矢量地图，深度赋能公安应用；地图平台数据更新服务：提供1年2次矢量地图数据(pgis标准18级)更新服务。提供1年的路况数据更新服务。提供地图平台基础功能升级服务；人员位置大数据服务：包含重点关注区域实时人数、重点关注区域人数预测、重点关注区域实时人流、重点关注区域累计人流、重点关注区域人群热力图、重点关注区域人员画像、城市地块分析等服务。 3.情指勤舆督：以公安运行的“情指勤舆督”模式为牵引，建设情指勤舆督一体化实战平台，实现高新区分局综合态势、专题分析、科所队综合态势、应用导航、警务要素上图、基础服务、警情研判分析应用、实战移动等功能。 4.智慧安防社区：提供智能安防社区系统，建立辖区内小区、场所等基础数据库，掌握辖区内动态大数据，形成对各类动态对象的风险感知及预警。 5.舆情大数据平台：搭建舆情大数据系统，提供舆情的态势感知、线上风险感知的能力，对舆情重点事件、网络安全舆情、重点舆情进行管理，提供舆情导控、共研共判的能力，并支持以报表的形式展示舆情。 6.智慧公安APP：提供智慧公安警务APP，建设集约化工作台，统一集成、整合各类警务业务。 7.业务中枢：提供业务中枢，实现公安应用通用基础业务支撑，实现预警中枢、指令中枢、预案中枢、勤务中枢、时空中枢、评价中枢、任务中枢、位置中枢、统一基础信息等功能，全面提升智慧公安一体化水平。 8.云警务室：提供云警务室系统，实现终端数据传输加密、调证业务数据储存加密、企业信息多渠道核验、支持有效监管与服务企业。 9.数据库平台：提供数据库的运营操作、监控告警、性能分管理；MySQL兼容引擎（计算、存储、配置、管理、决策、调度）；PostgreSQL兼容引擎（计算、存储、配置、管理、决策、调度）等功能 | 项 | 1 |
| **2.2** | **硬件服务** |  |  |  |
| **2.2.1** | **视频专网** |  |  |  |
| 2.2.1.1 | 综合管控节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块240GB SSD硬盘+6块4TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 8 |
| 2.2.1.2 | 视图解析节点（结构化解析） | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.AI卡配置：≥4块Atlas 300I卡； 4.硬盘配置：≥2块240GB SSD硬盘+2块960GB SSD硬盘； 5.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 6.以太网连接：≥2个万兆光口（满配多模光模块）； 7.电源配置：热插拔冗余电源，电源模块满配置； 8.▲服务器管理软件通过信息安全评估，包括保密性、完整性、抗抵赖性、可核查性测试，提供具有 CMA 或 CNAS 标识的第三方检验（检测）出具的服务器管理软件信息安全性测试报告扫描件或关键页（报告封面页、盖章页、说明页）； | 台 | 13 |
| 2.2.1.3 | 视图解析节点（场景化解析） | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.AI卡配置：≥4块Atlas 300V PRO卡； 4.硬盘配置：≥2块240GB SSD硬盘+2块960GB SSD硬盘； 5.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 6.以太网连接：≥2个万兆光口（满配多模光模块）； 7.电源配置：热插拔冗余电源，电源模块满配置； 8.▲服务器管理软件通信息安全评估，包括保密性、完整性、抗抵赖性、可核查性测试，提供具有 CMA 或 CNAS 标识的第三方检验（检测）出具的服务器管理软件信息安全性测试报告扫描件或关键页（报告封面页、盖章页、说明页）； | 台 | 10 |
| 2.2.1.4 | 视图特征库节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.AI卡配置：≥4块Atlas 300I卡； 4.硬盘配置：≥2块240GB SSD硬盘+2块960GB SSD硬盘+8块1920GB SSD硬盘； 5.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 6.以太网连接：≥2个万兆光口（满配多模光模块）； 7.电源配置：热插拔冗余电源，电源模块满配置； 8.▲服务器管理软件通过信息安全评估，包括保密性、完整性、抗抵赖性、可核查性测试，提供具有 CMA 或 CNAS 标识的第三方检验（检测）出具的服务器管理软件信息安全性测试报告扫描件或关键页（报告封面页、盖章页、说明页）； | 台 | 4 |
| 2.2.1.5 | S1标准应用节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+4块10TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 5 |
| 2.2.1.6 | 摆渡服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+4块4TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.1.7 | 接口服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+4块4TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.1.8 | 图片结构化服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥24个物理核、主频频率≥2.1GHz； 2.内存配置：≥256GB DDR4； 3.AI卡配置：≥8块NVIDIA-Tesla T4卡； 4.硬盘配置：≥2块480GB SSD硬盘； 5.RAID卡配置：支持RAID0/1/5/6/10/50/60，2GB缓存带掉电保护； 6.以太网连接：≥2个万兆光口（满配多模光模块）； 7.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 2.2.1.9 | 消息队列服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥24个物理核、主频频率≥2.1GHz； 2.内存配置：≥320GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+1块3840GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.1.10 | 数据存储服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥24个物理核、主频频率≥2.1GHz； 2.内存配置：≥320GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+2块3840GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 4 |
| 2.2.1.11 | Web服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥24个物理核、主频频率≥2.1GHz； 2.内存配置：≥320GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+2块3840GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| **2.2.2** | **公安信息网** |  |  |  |
| 2.2.2.1 | 综合管控节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块240GB SSD硬盘+6块4TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.2 | 视图解析节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.AI卡配置：≥4块Atlas 300V PRO卡； 4.硬盘配置：≥2块240GB SSD硬盘+2块960GB SSD硬盘； 5.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 6.以太网连接：≥2个万兆光口（满配多模光模块）； 7.电源配置：热插拔冗余电源，电源模块满配置； 8.▲服务器管理软件通过信息安全评估，包括保密性、完整性、抗抵赖性、可核查性测试，提供具有 CMA 或 CNAS 标识的第三方检验（检测）出具的服务器管理软件信息安全性测试报告扫描件或关键页（报告封面页、盖章页、说明页）； | 台 | 1 |
| 2.2.2.3 | 视图特征库节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.AI卡配置：≥4块Atlas 300V PRO卡； 4.硬盘配置：≥2块240GB SSD硬盘+2块960GB SSD硬盘+8块1920GB SSD硬盘； 5.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 6.以太网连接：≥2个万兆光口（满配多模光模块）； 7.电源配置：热插拔冗余电源，电源模块满配置； 8.▲服务器管理软件通过信息安全评估，包括保密性、完整性、抗抵赖性、可核查性测试，提供具有 CMA 或 CNAS 标识的第三方检验（检测）出具的服务器管理软件信息安全性测试报告扫描件或关键页（报告封面页、盖章页、说明页）； | 台 | 3 |
| 2.2.2.4 | 融合分析节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥512GB DDR4； 3.AI卡配置：≥4块Atlas 300V PRO卡； 4.硬盘配置：≥2块240GB SSD硬盘+10块3840GB SSD硬盘； 5.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 6.以太网连接：≥2个万兆光口（满配多模光模块）； 7.电源配置：热插拔冗余电源，电源模块满配置； 8.▲服务器管理软件通过信息安全评估，包括保密性、完整性、抗抵赖性、可核查性测试，提供具有 CMA 或 CNAS 标识的第三方检验（检测）出具的服务器管理软件信息安全性测试报告扫描件或关键页（报告封面页、盖章页、说明页）； | 台 | 5 |
| 2.2.2.5 | 融合分析节点（CPU计算） | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥512GB DDR4； 3.硬盘配置：≥2块240GB SSD硬盘+10块3840GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.6 | S1标准应用节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+4块10TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.7 | 摆渡服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+4块4TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.2.8 | 接口服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+4块4TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.2.9 | 消息队列服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥24个物理核、主频频率≥2.1GHz； 2.内存配置：≥320GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+1块3840GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.10 | 数据存储服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥24个物理核、主频频率≥2.1GHz； 2.内存配置：≥320GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+2块3840GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 4 |
| 2.2.2.11 | Web服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥24个物理核、主频频率≥2.1GHz； 2.内存配置：≥320GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+2块3840GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.2.12 | 搜图服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥18个物理核、主频频率≥2.2GHz； 2.内存配置：≥384GB DDR4； 3.AI卡配置：≥2块NVIDIA-Tesla T4卡； 4.硬盘配置：≥2块480GB SSD硬盘； 5.RAID卡配置：支持RAID0/1/10； 6.以太网连接：≥2个万兆光口（满配多模光模块）； 7.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.2.13 | 移动警务应用服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥20个物理核、主频频率≥2.3GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 2.2.2.14 | 情指勤舆督服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块240GB SSD硬盘+2块2TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 2.2.2.15 | 舆情监管大数据服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥4块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 2.2.2.16 | 智慧安防应用服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块240GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 2.2.2.17 | 智慧安防计算服务器 | 1.CPU配置：采用X86架构，配置≥4颗CPU，每颗CPU≥24个物理核、主频频率≥2.3GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+2块1920GB SSD硬盘； 4.以太网连接：≥2个万兆光口（满配多模光模块）； 5.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.2.18 | 智慧安防数据库服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥512GB DDR4； 3.硬盘配置：≥2块240GB SSD硬盘+2块4TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.2.19 | 智慧安防数据中转服务器（视频专网） | 1.CPU配置：采用X86架构，配置≥1颗CPU，每颗CPU≥10个物理核、主频频率≥2.1GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块600GB 10K SAS硬盘，8块6T 7.2K SATA硬盘，4块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.2.20 | 地图平台服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥16个物理核、主频频率≥2.3GHz； 2.内存配置：≥512GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/6/10/50/60； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 4 |
| 2.2.2.21 | 智能机器人AI服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥24个物理核、主频频率≥2.1GHz； 2.GPU配置：≥1块NVIDIA-Tesla T4卡； 3.内存配置：≥64GB DDR4； 4.硬盘配置：≥2块480GB SSD硬盘 5.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 6.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 7.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.2.22 | 智能机器人服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥16个物理核、主频频率≥2.3GHz； 2.内存配置：≥512GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/6/10/50/60，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.23 | 指挥处置专题业务应用服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥4块240GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 2.2.2.24 | 业务中枢服务器 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥4块240GB SSD硬盘 ； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 1 |
| 2.2.2.25 | MySql-管理节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥64GB DDR4； 3.硬盘配置：≥4块240GB SSD硬盘 ； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.26 | PG-管理节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥64GB DDR4； 3.硬盘配置：≥4块240GB SSD硬盘 ； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.27 | 消息队列服务器-KAFKA | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥4块240GB SSD硬盘 ；+4块2.4T sas硬盘 ； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.28 | 业务系统数据库服务器-MySql-计算存储 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥4块240GB SSD硬盘 +6块3840GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.29 | 业务系统数据库服务器-PG-计算存储 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥48个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥4块240GB SSD硬盘 + 6块1920GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 2.2.2.30 | 摆渡服务器（互联网.公安内网） | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥8个物理核、主频频率≥2.1GHz； 2.内存配置：≥64GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 2.2.2.31 | NAS存储 | 1、支持SAN与NAS一体化 ，支持、IP和FC SAN协议、NAS协议（包括NFS和CIFS）； 2、配置≥2个控制器，可扩展≥16个控制器； 3、存储总物理核心数≥64 核；（SAN存储总物理核心数计算公式：FC 存储总物理核心数=控制器数量×每个控制器处理器数量×单个处理器核数） 4、控制器间互联协议采用PCI-E/IB/RDMA等协议，非FC、IP联邦；控制器支持Active-Active模式； 5、系统内总一级缓存容量配置≥128GB（不含任何性能加速模块、FlashCache、PAM 卡，SSD Cache、SCM 等），控制器缓存具备断电保护功能； 6、配置≥8个10Gb接口，≥8个1Gb接口；双控制器可提供≥6个PCIE插槽，用于主机接口扩展； 7、配置≥4块960G SAS SSD企业级硬盘，≥4块8T NL-SAS企业级硬盘,支持SAS SSD、NL SAS硬盘混插,支持热插拔； 8、最大可扩展总硬盘数不少于 1000 块 9、配置后端磁盘通道带宽≥192Gbps； 10、采用RAID虚拟化技术，支持RAID5,RAID6,RAID-TP（支持故障三块成员盘同时失效，数据不丢&不中断业务）； 11、配置 NAS 功能，配置 NFS、CIFS、NDMP、多租户、目录配额功能；NFS业务支持全局命名空间和日志审计功能； 12、存储支持内置容器，支持存储本地化应用部署， 13、投标人提供多路径软件，提供故障切换和负载均衡功能，兼容 Windows、Linux、VMware、Unix，以及国产操作系统； | 套 | 1 |
| 2.2.2.32 | 对象存储 | 1、存储架构：采用分布式对象存储架构的集群，支持多节点并发处理； 2、节点性能：2颗不低于8核高性能X86处理器或2颗不低于32核ARM处理器，主频≥2.6GHz；内存不低于256GB，DDR4； 3、单存储节点网口：≥4个千兆网口，≥4个万兆光口（含多模光模块）； 4、单存储节点硬盘：主存盘≥12块企业级SATA硬盘，单盘容量≤6TB，≥1块1.6TB企业级SSD，节点硬盘满配置；操作系统不占用该硬盘； 5、存储整体可用业务容量≥100TB，HDD裸容量（不含操作系统盘和缓存盘）≥216TB； 6、存储节点数要求：为保证存储整体吞吐能力，节点数≥3个； 7、▲内部保护：提供副本或EC容灾保护,支持+2.+3.+4 等EC余配比配置，可支持4节点同时故障，业务不中断，数据不丢失（提供具有 CMA 或 CNAS 标识的第三方检验（检测）机构出具的检验（检测）报告扫描件或关键页（报告封面页、盖章页、说明页））； 8、▲节点高可靠：支持动态EC，当节点故障时，自动调整EC配比，确保新数据可靠性不降级；（提供具有 CMA 或 CNAS 标识的第三方检验（检测）机构出具的检验（检测）报告扫描件或关键页（报告封面页、盖章页、说明页））； 9、▲支持数据快速重构，当磁盘或者节点故障之后无需人工干预，数据重建可以做到每TB≤15分钟（提供具有 CMA 或 CNAS 标识的第三方检验（检测）机构出具的检验（检测）报告扫描件或关键页（报告封面页、盖章页、说明页））； 10、▲支持对象存储中的数据进行压缩，，提供具有 CMA 或 CNAS 标识的第三方检验（检测）机构出具的检验（检测）报告扫描件或关键页（报告封面页、盖章页、说明页））； 11、在扩容过程中服务不能中断，扩容后系统具有将原系统的工作负载分配到新增容量上的能力；随着存储节点数的增加，分布式存储性能也随着线性增长； 12、支持同时多个节点的在线升级，升级过程不影响业务对存储的访问，不造成数据丢失； 13、支持多租户，租户间数据相互隔离，可设置访问控制权限，互不影响，支持创建、删除租户，并支持在管理界面重置租户密码； 14、支持不同水位下盘间容量自动进行数据迁移，均衡后各节点间容量误差小于5%；； 15、配置存储配套所需2台存储后端万兆交换机，要求每个节点前后端网络均采用双挂载（万兆交换机：交换容量≥4.8Tbps，包转发率≥2000Mpps；万兆光端口数量≥12个，40GE端口数量≥6个；支持VxLAN、M-LAG技术；支持微分段用于精细化东西向安全隔离）； | 套 | 1 |
| 三 | **视频图像信息数据库服务** | | | |
| **3.1** | **软件服务** |  |  |  |
| 3.1.1 | 公安视频图像信息数据库服务 | 提供公安视频图像信息数据库，支持视频图像信息存储，并接收视频图像解析平台不低于500路视频流解析全结构化图片数据，支撑公安视频图像信息应用的相关基础服务功能。 主要功能需包括： 1.数据汇聚：支持汇聚感知源前端产生的图片流及结构化数据，并实现全量存储； 2.接口管理：符合GA/T 1400《公安视频图像信息应用系统》中的规定，实现采集接口、数据服务接口和级联接口，能够对相关接口进行管理； 3.多视图库接入：支持多个下级视图库的联网接入； 4.▲多视图库上联：支持联网接入多个上级视图库，可基于用户权限对各上级视图库提供差异化服务；（需提供有效的国家安全防范报警系统产品质量监督检验中心或公安部安全与警用电子产品质量检测中心出具的测试报告扫描件证明） 5.大数据支撑：支持对视频图像信息数据进行管理，包含数据检索及组合条件查询； 6.▲容量扩展：支持存储容量的平滑扩展；（需提供有效的国家安全防范报警系统产品质量监督检验中心或公安部安全与警用电子产品质量检测中心出具的测试报告扫描件证明） 7.应用功能：支持联网服务、综合查询等应用功能； 8.管理功能：支持用户管理、运维管理等功能； 9.提供公安视频图像信息数据库视频图像信息接入管理授权≥7882路。 | 项 | 1 |
| **3.2** | **硬件服务** |  |  |  |
| 3.2.1 | **视频专网** |  |  |  |
| 3.2.1.1 | 采集接口接入服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥20个物理核、主频频率≥2.3GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/6/10/50/60，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 11 |
| 3.2.1.2 | 采集接口管理服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥20个物理核、主频频率≥2.4GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/6/10/50/60，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 3.2.1.3 | 视图库网关服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥10个物理核、主频频率≥2.2GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块600GB 10K SAS硬盘，≥10块2000GB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 10 |
| 3.2.1.4 | 级联接口服务器 | 1.CPU配置：采用X86架构，配置≥4颗CPU，每颗CPU≥24个物理核、主频频率≥2.3GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+2块1920GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/6/10/50/60，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 8 |
| 3.2.1.5 | 数据服务接口服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥16个物理核、主频频率≥2.3GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/6/10/50/60，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 3.2.1.6 | 视图库大数据支撑管理节点 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥10个物理核、主频频率≥2.2GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块600GB 10K SAS硬盘，≥8块2400GB 10K SAS硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 3 |
| 3.2.1.7 | 视图库大数据支撑数据节点 | 1.CPU配置：采用ARM架构，配置≥2颗CPU，每颗CPU≥32个物理核、主频频率≥2.6GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+10块8TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/5/10/50，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）+2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 15 |
| 3.2.1.8 | 视图库管理服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥10个物理核、主频频率≥2.2GHz； 2.内存配置：≥128GB DDR4； 3.硬盘配置：≥2块600GB 10K SAS硬盘，≥8块8TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 3.2.1.9 | 中间件服务器 | 1.CPU配置：采用X86架构，配置≥4颗CPU，每颗CPU≥24个物理核、主频频率≥2.3GHz； 2.内存配置：≥256GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘+2块1920GB SSD硬盘； 4.RAID卡配置：支持RAID0/1/5/6/10/50/60，2GB缓存带掉电保护； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 18 |
| 3.2.1.10 | 负载均衡服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥8个物理核、主频频率≥2.1GHz； 2.内存配置：≥64GB DDR4； 3.硬盘配置：≥2块960GB SSD硬盘； 4.RAID卡配置：支持RAID0/1； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 2 |
| 3.2.1.11 | 数据库服务器 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥24个物理核、主频频率≥2.1GHz； 2.内存配置：≥320GB DDR4， 3.硬盘配置：≥2块480GB SSD硬盘，≥2块3840GB SSD硬盘；； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个万兆光口（满配多模光模块）； 6.电源配置：热插拔冗余电源，电源模块满配置； | 台 | 4 |
| 3.2.1.12 | 分布式图片存储集群1 | 存储架构：采用分布式文件存储架构的集群，支持多节点并发处理。 1.节点性能：2颗不低于20核高性能X86处理器或2颗不低于48核ARM处理器，主频≥2.1GHz；内存不低于128GB，DDR4； 2.单存储节点网口：≥2个千兆网口，≥4个万兆光口（含多模光模块）； 3.单存储节点硬盘：≥35块企业级SATA硬盘，单盘容量≥10T；≥1块7.68TB企业级SSD，节点硬盘满配置；操作系统不占用该硬盘； 4.存储整体可用业务容量≥1120TB； 5.存储节点容量要求：为保证存储集群整体吞吐能力，节点数≥6个； 6.内部保护：提供副本或EC容灾保护,支持+2.+3.+4 等EC余配比配置； 7.本次配置需满足单一集群提供不低于任意2块硬盘故障或任意1个存储节点故障的容灾保护功能； 8.支持根据业务需要配置多种重构速度模式； 9.整套存储采用统一命名空间，支持将所有存储节点整合成一个虚拟存储池，并向外提供统一的域名或IP 地址访问服务； 10.支持业务负载均衡功能，可以根据节点连接数、节点吞吐量、轮循、节点综合负载、CPU 使用率等策略进行负载均衡； 11.▲离散存储：将数据呈离散式分布存储到各个存储节点上，磁盘间容量偏差小于2%，节点间容量偏差小于 0.2%（提供具有 CMA 或 CNAS 标识的第三方检验（检测）机构出具的检验（检测）报告扫描件或关键页（报告封面页、盖章页、说明页））； 12.具备内存和SSD缓存技术，冷热数据迁移调度过程中，文件路径不变； 13.具备SSD盘磨损度等寿命监控和HDD故障预测告警； 14.图形化管理，可监控系统、节点、磁盘级别使用状态、网络吞吐等实时运行状态。 15.RAS要求：热插拔硬盘，热插拔式冗余电源、风扇。 | 套 | 1 |
| 3.2.1.13 | 分布式图片存储集群2 | 存储架构：采用分布式文件存储架构的集群，支持多节点并发处理。 1.节点性能：2颗不低于20核高性能X86处理器或2颗不低于48核ARM处理器，主频≥2.1GHz；内存不低于256GB，DDR4； 2.单存储节点网口：≥2个千兆网口，≥4个万兆光口（含多模光模块）； 3.单存储节点硬盘：≥35块企业级SATA硬盘，单盘容量≥14T；≥1块7.68TB企业级SSD，节点硬盘满配置；操作系统不占用该硬盘； 4.存储整体可用业务容量≥8965TB； 5.存储节点容量要求：为保证存储集群整体吞吐能力，节点数≥26个； 6.内部保护：提供副本或EC容灾保护,支持+2.+3.+4 等EC余配比配置； 7.本次配置需满足单一集群提供不低于任意2个节点宕机的容灾保护功能； 8.支持根据业务需要配置多种重构速度模式； 9.整套存储采用统一命名空间，支持将所有存储节点整合成一个虚拟存储池，并向外提供统一的域名或IP 地址访问服务； 10.支持业务负载均衡功能，可以根据节点连接数、节点吞吐量、轮循、节点综合负载、CPU 使用率等策略进行负载均衡； 11.▲离散存储：将数据呈离散式分布存储到各个存储节点上，磁盘间容量偏差小于2%，节点间容量偏差小于 0.2%（提供具有 CMA 或 CNAS 标识的第三方检验（检测）机构出具的检验（检测）报告扫描件或关键页（报告封面页、盖章页、说明页））； 12.具备内存和SSD缓存技术，冷热数据迁移调度过程中，文件路径不变； 13.具备SSD盘磨损度等寿命监控和HDD故障预测告警； 14.图形化管理，可监控系统、节点、磁盘级别使用状态、网络吞吐等实时运行状态。 15.RAS要求：热插拔硬盘，热插拔式冗余电源、风扇。 | 套 | 1 |
| **四** | **视频图像信息网络安全保障服务** | | | |
| 1 | **公安视频专网安全保障服务** | | | |
| 1.1 | 摄像头安全管理系统 | 1.支持资产探测与发现，依托设备应用控制系统（视频安全网关），提供主动扫描、实时检测双引擎探测方式；  2.支持资产管理，支持通过主动扫描、实时检测和手动设置（手工登记、批量导入）等多种手段采集视频专网中的摄像头、PC、NVR等接入设备的资产信息，经过管理人员确认后建立统一的合法资产库；  3 支持威胁检测，通过与视频安全网关联动，对网络内设备运行情况实时监测，对入侵攻击、僵尸木儒、异常流量、非法私接、伪冒、非法业务、资产离线等重要的安全事件进行实时检测；  4.提供精准的态势感知能力，包括总体态势感知大屏，以及分业务视角的态势感知大屏，帮助管理人员直观掌握运营态势、安全态势，提升资产管理与监控管理的效率；  5.前端设备授权≥26000个。  6.视频网前端摄像头资产管理要求（前提条件：保证网络通畅，摄像头状态正常且正常连网，摄像头支持并开启onvif协议。如果由于摄像头原始报文返回的信息无法支撑判定资产类别，不纳入考核）：①平台的可用性＞99%；②平台前端摄像头信息识别覆盖率＞99%；③在2万个IP的规模下，平台资产信息更新时效性＜1天。 | 项 | 1 |
| 1.2 | 摄像头安全管理系统硬件 | 1.CPU配置：采用X86架构，配置≥2颗CPU，每颗CPU≥16个物理核、主频≥2.1GHz； 2.内存配置：≥512GB，DDR4 ECC； 3.硬盘配置：≥1\*240G M.2 SSD ，≥6\*4T STAT，≥2\*960G SSD； 4.RAID卡配置：配置2GB Cache，支持RAID0/1/5/10/50，带掉电保护； 5.以太网连接：≥2个万兆光口；满配光模块； 6.电源配置：热插拔冗余电源。 | 台 | 1 |
| 1.3 | 资产探针 | 1.接口：千兆电口≥6，千兆光口≥2，万兆光口≥2；满配光模块； 2.资产探测授权≥50000； 3.1T存储≥1T，冗余电源； 4.产品可进行存活探测、指纹探测、POC探测； 5.支持扫描范围自定义、选择资产组扫描范围、批量导入扫描范围三种方式添加扫描任务； 6.支持选择任务是否立即下发、支持周期扫描，以天为单位； 7.支持自定义例外节点探测IP及IP段； 8.支持识别IP、端口、网站标题、协议、操作系统、地理位置（国家、区域）等设备指纹； 9.支持超过10万指纹信息。 | 套 | 1 |
| 1.4 | 视频安全网关（视频安全资源池） | 1.100GE光口≥2，万兆光口≥20，40G接口≥2，配置双电源； 2.吞吐量≥160Gbps，支持接入8M码流摄像头≥4750台，接入4M码流摄像头≥9500台，接入2M码流摄像头≥19000台； 3.当风扇模块出现故障时，可以在防火墙不断电的情况下，对风扇模块进行更换；为了避免防火墙过热，要求更换风扇模块所用的时间控制在1分钟内； 4.支持视频业务识别与控制，支持识别国标SIP协议及主流安防厂家的私有协议，只允许授信的视频业务相关流量放行，其它流量全部阻断； 5.支持摄像机入侵防御功能，有效防御蠕虫、木马、僵尸网络、跨站攻击等常见攻击，支持对主流摄像头厂家的私有视频协议的漏洞检测及防护； 6.支持主动扫描摄像机的设备指纹，并自动添加到设备指纹库； 7.支持基于地理位置的流量和威胁分析； 8.支持充当态势感知系统的诱捕/流探针，采集网络流量，上送态势感知系统，构建主动防御的诱捕体系； 9.实配固态硬盘≥240G，实配IPS、AV、URL过滤升级license。 | 台 | 2 |
| 1.5 | 边界防火墙 | 1.万兆光口≥12，40G接口≥2，千兆电口≥12，配置双电源，配置≥240G硬盘，实配IPS、AV、URL过滤升级license； 2.SSL VPN并发数实配100可扩展5000，IPSec VPN隧道≥15000，虚拟防火墙数量≥1000； 3.防火墙吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万； 4.能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、VLANID、内容安全统一界面进行安全策略配置； 5.支持加密流量解密后镜像给第三方设备做审计，安全检测； 6.支持防火墙内置流探针，对网络中的流量进行采集，上送网络安全智能分析系统进行威胁分析。 | 台 | 2 |
| 1.6 | 管理区防火墙 | 1.千兆电口≥12，千兆光口≥8，10G接口≥4，配置双电源，≥240G硬盘，实配IPS、AV、URL过滤升级license； 2.实配SSL VPN并发数100可扩展2000，IPSec VPN隧道≥8000，虚拟防火墙数量≥500； 3.吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万； 4.能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、VLANID、内容安全统一界面进行安全策略配置； 5.支持加密流量解密后镜像给第三方设备做审计，安全检测； 6.支持防火墙内置流探针，对网络中的流量进行采集，上送网络安全智能分析系统进行威胁分析。 | 台 | 2 |
| 1.7 | 业务区防火墙 | 1.配置防火墙吞吐量≥120Gbps，整机可平滑扩展至600Gbps ； 2.配置并发链接数≥8000万，后续整机最大并发连接可扩展到≥4.8亿； 3.配置每秒新建连接数≥240万，后续整机每秒新建连接数可扩展到≥1200万； 4.配置10GE光口≥24个，100GE光口≥2个； 5.除两个主控板外，整机业务扩展插槽≥4；实配业务板，接口板后，剩余扩展插槽数≥2，以便后续业务板、接口板扩容使用； 7.可识别应用层协议数量≥6000种；支持识别国标SIP协议及安防厂家的私有协议； 8.支持BFD链路检测，支持BFD与VRRP联动实现双机快速切换，支持BFD与OSPF联动实现双机快速切换； 9.虚拟防火墙数量实配20可扩展到≥4000，配置双电源。 | 台 | 2 |
| 1.8 | 漏洞扫描 | 1.集成系统扫描、WEB扫描、数据库扫描、基线配置核查、弱口令扫描于一体，且为单独功能模块，提供一体化漏洞检测； 2.支持漏洞库涵盖标准包含但不限于CVE、CVSS、CNVID、CNNVD、CNCVE、Bugtraq 6种； 3.支持60000条以上系统漏洞库，并按照漏洞类别及漏洞威胁程度进行分类，支持并配置无限个资产扫描；  4.漏洞扫描设备支持对终端漏洞和弱口令进行识别； 5.支持SSH、SMB、TELNET、POP、POP3.IMAP、FTP、RSH、REXEC、WSUS、SNMP、RDP的登录扫描，并支持登陆验证； 6.支持会话录制功能，针对已完成的Web扫描，记录之前的登录状态，以方便之后的扫描能够直接进行扫描，无需再进行登录认证； 7.标准型2U机型，标配6个千兆电口，支持扩展1张4电口或4光口插卡，实配≥1T硬盘，实配单交流电源，实配漏洞升级许可license，实配数据库扫描、Web漏洞扫描、系统漏洞扫描、配置核查功能license。 | 台 | 1 |
| 1.9 | 堡垒机 | 1.软硬件一体化设备，标准2U机架式设备，配置接口≥6个千兆电口，≥2个万兆光口（含光模块），扩展插槽≥1个，硬盘：≥4T，RAID 1，内存：≥8G，配置冗余电源； 2.授权资产：1000个；硬件性能：并发字符连接最大≥350个，并发图形连接最大≥200个； 3.系统各模块支持以B/S方式管理，采用https加密方式访问； 4.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； 5.支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期； 6.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、AD域认证、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； 7.支持对用户指定限制登录IP、登录时间段（可循环，如每周一到周五9：00-17：00时）等规则，以确保可信用户登陆系统； 8.支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度必须符合密码策略要求； | 套 | 1 |
| 1.10 | 日志审计 | 1.软硬件一体化设备，标准2U机架式设备，接口配置≥6个千兆电口，≥4个千兆光口，≥2个万兆光口（含光模块），磁盘≥4T，≥10000/秒（峰值：14000/秒），配置冗余电源，授权日志源≥500个； 2.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集； 3.支持通过Agent采集日志数据，支持通过syslog、FTP等多种方式完成日志收集； 4.内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据； 5.支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析； 6.支持日志文件备份到外置存储节点； 7.提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置； | 套 | 1 |
| 1.11 | 数据库审计 | 1.软硬件一体化设备，标准2U机架式设备，硬盘容量：≥4TB，配置网口：≥6千兆电口，≥4个千兆光口，≥2万兆光口（含光模块），≥1个接口扩展插槽，配置冗余电源；数据库实例个数≥250个，SQL处理性能≥100000条SQL/秒，日志检索性能≥2500000条/秒； 2.支持主流数据库Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache、达梦、人大金仓、南大通用、MongDB、K-DB； 3.支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌； 4.支持时间段、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索； 5.深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源IP、源端口、源MAC、目的IP、目的端口、数据库用户、数据库类型、操作类型、SQL语句、SQL模版、客户端程序名、响应码、影响行数、返回行数、SQL预计响应时间；  6.提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能； | 套 | 1 |
| 1.12 | WEB应用防护 | 1.软硬件一体化设备，标准2U机架式设备，接口配置≥4个千兆电口，≥4个千兆光口，≥4万兆光接口（含光模块）；HTTP应用吞吐量≥9Gbps，HTTP最大并发数≥1600万，HTTP最大新建数≥60万； 2.产品采用多核处理架构； 3. 产品支持路由类型、协议类型、网络对象等条件进行自动选路的策略路由； 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； 5. 产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改； 6. 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； 7. 产品内置多种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； 8. 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； 9.产品支持https解密功能，支持TCP代理和SSL代理； | 套 | 2 |
| 1.13 | 安全态势感知（平台） | 1.软硬件一体化设备，标准2U机架式设备，内存≥256GB，硬盘≥12块4TB；≥4个千兆电口，≥4万兆光口（含光模块）； 2.支持主动扫描、被动流量方式识别海康、大华、宇视、华为等IPC、NVR设备； 3.支持大屏轮播及自定义大屏顺序设置和大屏名称。自定义统计周期资产组划分、选择播放大屏及轮播时间间隔，大屏包含全网安全态势感知大屏、安全事件态势、资产态势； 5.支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议； 6.支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作； 7.支持网络安全设备规则，包括网络设备、安全设备、中间件、操作系统等； | 套 | 1 |
| 1.14 | 流量检测探针 | 1.软硬件一体化设备，标准2U机架式设备，配置接口≥4个千兆电口，≥4个千兆SFP光口 ，≥8个万兆SFP光口（含光模块）； 2.网络层吞吐量≥10Gbps，应用层吞吐量≥4Gbps，内存大小≥32G，硬盘容量≥960GB SSD，电源：冗余电源； 3.应具有丰富的安全策略配置，包括：网络攻击、业务脆弱性、僵尸网络检测、主动IP扫描、文件安全、邮件安全； 4.为确保应用识别漏洞分析能力，要求设备能够识别应用类型超过1000种，应用识别规则总数超过3000条，漏洞利用规则特征库数量超过4000条； 5.为防止敏感数据泄密，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤； 6.为实现未知威胁的处理能力，具备同云端安全分析引擎进行联动的能力； 7.支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级； | 套 | 2 |
| 1.15 | 终端安全防护系统 | 1.软硬件一体标准机架式设备，≥2个千兆电口，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，单一管理控制中心可统一管理分别部署在WindowsPC、Windows服务器、Linux服务器以及国产化服务器的客户端软件，配置≥500套服务器授权； 2.提供勒索病毒防护； 3.支持对终端账户信息进行梳理，了解账号权限分布概况以及风险账号分布情况； 4.通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整客户端的资源占用（CPU、IO等），为业务让出资源，不卡业务，对业务零摩擦； 5.支持windows服务器RDP远程登录保护； | 套 | 1 |
| 1.16 | 备份一体机 | 1.提供≥30TB备份容量许可；配置≥2颗CPU，单颗≥32核，≥64GB DDR4配置系统盘≥2\*600 GB SAS硬盘,数据盘≥12\*4T 硬盘，≥4\*GE+2\*10GE； 2.支持数据库备份恢复，包括：Oracle、SQL Server、MySQL、Sybase、DB2、Informix、PostgreSQL、MongoDB、Caché等数据库应用； 3.支持国产芯片服务器平台，支持备份服务端或者客户端部署在龙芯、飞腾、鲲鹏、海光、申威、兆芯等服务器平台上； 4.支持VMware、Hyper-V、Xenserver、Xen、KVM、FusionCompute、FusionCloud（Huawei Cloud Stack）、H3C CAS、OpenStack、CNware、RHV、易捷行云EasyStack、腾讯云TStack、ZStack等虚拟化平台或云平台的备份恢复； 5.支持在线文件备份，支持全量备份、增量备份。支持对Windows、Linux、UNIX平台单文件/目录进行细颗粒度的恢复。备份支持通过名称或通配符进行文件过滤，排除操作系统文件和一些指定扩展名的文件类型； 6.支持断点续传、备份重试、重试间隔设置，可根据网络健壮情况调整时间和次数； 7.支持AES、SM4等加密算法。加密算法可选择CBC、CFB、ECB、OFB等加密模式，对于AES的密钥支持设置128、192、256等长度。 | 台 | 1 |
| 1.17 | 服务器密码机 | 1.对称密钥对数：≥1024个，非对称密钥对数：≥1024对，SM2生成密钥：≥12000对/s；SM2加密：≥2600次/s；SM2解密：≥3000次/s；SM2签名：≥12000次/s；SM2验签，4300次/s； 2.支持密码算法：1）非对称算法：国密SM2；国际RSA1024、RSA2048、RSA3072、RSA4096；2）对称算法：国密SM1、SM4；国际DES、3DES、AES；3）摘要算法：国密SM3；国际SHA1、SHA256、SHA512； 3.扩展能力：集群支持及性能扩展。支持多线程、多任务和性能扩展，多机热备和负载均衡，可多机扩展并行工作； 4.管理功能：采用分级权限管理，管理人员身份凭证信息安全存储在USBKEY中；支持WEB及C/S管理方式，并支持SSL协议确保通信的机密性；支持国密SHH、国密FTP，保证整机运维安全；支持服务器密码机日志完整性保护； | 台 | 2 |
| 1.18 | 签名验签和时间戳二合一服务器 | 1.硬件要求：2U高机架式硬件架构，单电源（可扩容成冗余电源），≥8GB内存，≥2TB硬盘容量，标准配置≥8个以太网千兆电口，支持≥2个接口扩展槽位； 2.SM2算法：签名速度：≥17000次/秒；验签速度：≥15000次/秒；签名速度：≥12000次/秒；验签速度：≥8000次/秒；SM3杂凑算法：≥860Mbps；数字证书验证速度：≥1500次/秒；数字信封制作速度：≥2000次/秒；数字信封解析速度：≥3000次/秒；SM2签名密钥对数量：≥512对；SM2加密密钥对数量：≥512对；对称密钥数量：≥1024个；时间戳签发速度：≥4300次/秒；时间戳验证速度：≥7300次/秒； 3.同时符合GM/T 0029《签名验签服务器技术规范》、GM/T 0033 《时间戳接口规范》、GM/T 0028《密码模块安全技术要求》等相关技术要求； 4.支持多机并行工作模式；支持负载均衡；支持双机热备部署； 5.支持CPU和内存的利用率、磁盘占用率、网络状态、用户登录状态等的实时监控； 6.支持基于SM2算法的时间戳服务，为应用系统提供时间戳签发、验证时间戳服务，实现对数据、消息、文件等多种格式原文数据的时间戳签发服务； 7.支持NPT协议，支持多个第三方时间源的配置管理，能够与第三方授时中心、卫星授权时间源（北斗、GPS）进行时间同步，确保签发时间戳时所获取的时间有效、精确； 8.支持配置记录日志的类型，如运行日志、DEBUG日志、错误日志；支持日志的查询、审计、下载、清除；采用数字签名技术对日志数据进行完整性保护； 9.支持设置访问IP白名单，仅允许白名单内IP访问签名验签服务器； 10.支持数字证书有效性验证策略配置，至少包括验证证书有效期、验证证书签名有效性、验证证书是否在CRL中三种验证策略。 | 台 | 2 |
| 1.19 | 国密VPN综合安全网关 | 1.通过国密VPN产品实现SSL VPN接入，提供支持国密算法的SSL隧道加密连接服务，保证接入的实体身份真实性，通信访问过程的机密性、完整性；提供125个 SSL VPN授权；  2.硬件规格：配置千兆电口≥16， 千兆光口≥4，万兆光口≥6，Combo口≥4；接口扩展槽位≥2；硬盘扩展槽≥2，可支持扩展SSD硬盘≥960GB；配置双电源；  3.性能要求：吞吐量≥15Gbps，应用层吞吐量≥5Gbps，最大并发连接数≥500万，每秒新建连接数≥12万，IPSec VPN隧道≥4000，SSL VPN最大并发用户≥6000；  4.虚拟化能力：支持虚拟防火墙功能，支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；  5.SSL VPN支持页面定制功能特性，包括登录页面、交互信息、提示信息的定制功能； 防火墙在SSLVPN页面上修改用户密码，支持防暴力破解密码；  6.支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。  7.支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署。 | 台 | 2 |
| 1.20 | 国密浏览器 | 1.双算法支持，同时支持国密算法和国际通用算法。对称算法支持 SM4、3DES、AES；非对称算法支持 SM2、RSA（1024、2048、4096）、ECC；杂凑密码算法支持 SM3、SHA\_1、SHA\_256、SHA\_512； 2.支持 SSL 链接，浏览器支持 SSL，TLS，可支持配置国密/国际算法；  3.支持 SSL 单项及双向链接，与 Web 服务器之间建立安全通道，保证 Web 网页访问的安全性；  4.支持基于 SM2算法 、RSA算法的数字证书、数字证书撤销列表（CRL）； 5.支持 NPAPI、PPAPI 控件。 | 项 | 100 |
| 1.21 | 设备证书 | 设备证书（分别为签名验签和时间戳二合一服务器、VPN网关提供证书支撑），有效期3年。 | 项 | 4 |
| 1.22 | 个人证书 | 个人证书（提供运维人员的身份鉴别服务），有效期3年。 | 项 | 100 |
| 1.23 | 智能密码钥匙 | 1.支持ECB、CBC、OFB模式的SM1密码算法； 2.支持SM2密码算法，可在内部进行加解密、签名验签、密钥对生成； 3.支持SM3密码算法； 4.支持ECB、CBC、OFB模式的SM4密码算法； 5.支持数据的安全存储功能； | 台 | 100 |
| 2 | **公安信息网安全保障服务** | | | |
| 2.1 | 出口防火墙 | 1.千兆电口≥12，千兆光口≥8，10G接口≥4，满配光模块；配置双电源，240G硬盘，实配IPS、AV、URL过滤升级license； 2.实配SSL VPN并发数100可扩展2000，IPSec VPN隧道≥8000，虚拟防火墙数量≥500； 3.吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万； 4.能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、VLANID、内容安全统一界面进行安全策略配置； 5.支持加密流量解密后镜像给第三方设备做审计，安全检测； 6.支持防火墙内置流探针，对网络中的流量进行采集，上送网络安全智能分析系统进行威胁分析。 | 台 | 2 |
| 2.2 | 管理区防火墙 | 1.千兆电口≥12，千兆光口≥8，10G接口≥4，满配光模块；配置双电源，240G硬盘，实配IPS、AV、URL过滤升级license； 2.实配SSL VPN并发数100可扩展2000，IPSec VPN隧道≥8000，虚拟防火墙数量≥500； 3.吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万； 4.能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、VLANID、内容安全统一界面进行安全策略配置； 5.支持加密流量解密后镜像给第三方设备做审计，安全检测； 6.支持防火墙内置流探针，对网络中的流量进行采集，上送网络安全智能分析系统进行威胁分析。 | 台 | 2 |
| 2.3 | 业务区防火墙 | 1.万兆光口≥28，40G接口≥4，独立万兆HA口≥2，满配光模块；配置双电源，配置240G硬盘，实配IPS、AV、URL过滤升级license； 2.实配SSL VPN并发数实配100可扩展15000；IPSec VPN隧道≥55000，虚拟防火墙数量≥990； 3.当风扇模块出现故障时，可以在防火墙不断电的情况下，对风扇模块进行更换； 4.吞吐量≥80Gbps，最大并发连接数≥2400万，每秒新建连接数≥80万； 5.能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、VLANID、内容安全统一界面进行安全策略配置； 6.支持加密流量解密后镜像给第三方设备做审计，安全检测； 7.支持防火墙内置流探针，对网络中的流量进行采集，上送网络安全智能分析系统进行威胁分析。 | 台 | 2 |
| 2.4 | 漏洞扫描 | 1.集成系统扫描、WEB扫描、数据库扫描、基线配置核查、弱口令扫描于一体，且为单独功能模块，提供一体化漏洞检测； 2.支持漏洞库涵盖标准包含但不限于CVE、CVSS、CNVID、CNNVD、CNCVE、Bugtraq 6种； 3.支持60000条以上系统漏洞库，并按照漏洞类别及漏洞威胁程度进行分类，支持并配置无限个资产扫描；  4.漏洞扫描设备支持对终端漏洞和弱口令进行识别； 5.支持SSH、SMB、TELNET、POP、POP3.IMAP、FTP、RSH、REXEC、WSUS、SNMP、RDP的登录扫描，并支持登陆验证； 6.支持会话录制功能，针对已完成的Web扫描，记录之前的登录状态，以方便之后的扫描能够直接进行扫描，无需再进行登录认证； 7.标准型2U机型，标配6个千兆电口，支持扩展1张4电口或4光口插卡，实配≥1T硬盘，实配单交流电源，实配漏洞升级许可license，实配数据库扫描、Web漏洞扫描、系统漏洞扫描、配置核查功能license。 | 台 | 1 |
| 2.5 | 堡垒机 | 1.软硬件一体化设备，标准2U机架式设备，配置接口≥6个千兆电口，≥2个万兆光口（含光模块），扩展插槽≥1个，硬盘：≥4T，RAID 1，内存：≥8G，配置冗余电源； 2.授权资产：200个；硬件性能：并发字符连接最大≥350个，并发图形连接最大≥200个； 3.系统各模块支持以B/S方式管理，采用https加密方式访问； 4.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； 5.支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期； 6.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、AD域认证、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； 7.支持对用户指定限制登录IP、登录时间段（可循环，如每周一到周五9：00-17：00时）等规则，以确保可信用户登陆系统； 8.支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度必须符合密码策略要求； | 套 | 1 |
| 2.6 | 日志审计 | 1.软硬件一体化设备，标准2U机架式设备，接口配置≥6个千兆电口，≥4个千兆光口，≥2个万兆光口（含光模块），磁盘≥4T，≥10000/秒（峰值：14000/秒），配置冗余电源，授权日志源≥500个； 2.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集； 3.支持通过Agent采集日志数据，支持通过syslog、FTP等多种方式完成日志收集； 4.内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据； 5.支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析； 6.支持日志文件备份到外置存储节点； 7.提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置； | 套 | 1 |
| 2.7 | 数据库审计 | 1.软硬件一体化设备，标准2U机架式设备，硬盘容量：≥4TB，配置网口：≥6千兆电口，≥4个千兆光口，≥2万兆光口（含光模块），≥1个接口扩展插槽，配置冗余电源；数据库实例个数≥250个，SQL处理性能≥100000条SQL/秒，日志检索性能≥2500000条/秒； 2.支持主流数据库Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache、达梦、人大金仓、南大通用、MongDB、K-DB； 3.支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌； 4.支持时间段、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索； 5.深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源IP、源端口、源MAC、目的IP、目的端口、数据库用户、数据库类型、操作类型、SQL语句、SQL模版、客户端程序名、响应码、影响行数、返回行数、SQL预计响应时间；  6.提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能； | 套 | 1 |
| 2.8 | WEB应用防护 | 1.软硬件一体化设备，标准2U机架式设备，接口配置≥4个千兆电口，≥4个千兆光口，≥4万兆光接口（含光模块）；HTTP应用吞吐量≥9Gbps，HTTP最大并发数≥1600万，HTTP最大新建数≥60万； 2.产品采用多核处理架构； 3. 产品支持路由类型、协议类型、网络对象等条件进行自动选路的策略路由； 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； 5. 产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改； 6. 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； 7. 产品内置多种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； 8. 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； 9.产品支持https解密功能，支持TCP代理和SSL代理； | 套 | 2 |
| 2.9 | 终端安全防护系统 | 1.软硬件一体标准机架式设备，≥2个千兆电口，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，单一管理控制中心可统一管理分别部署在WindowsPC、Windows服务器、Linux服务器以及国产化服务器的客户端软件，配置≥200套服务器授权； 2.提供勒索病毒防护； 3.支持对终端账户信息进行梳理，了解账号权限分布概况以及风险账号分布情况； 4.通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整客户端的资源占用（CPU、IO等），为业务让出资源，不卡业务，对业务零摩擦； 5.支持windows服务器RDP远程登录保护； | 套 | 1 |
| 2.10 | 安全态势感知（平台） | 1.软硬件一体化设备，标准2U机架式设备，内存≥256GB，硬盘≥12块4TB；≥4个千兆电口，≥4万兆光口（含光模块）； 2.支持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击IP、攻击地址、攻击目标和目标手法。支持根据自身业务和安全运维经验自定义告警/事件，以便提高告警的精确度，减少运维成本。 3.支持大屏轮播及自定义大屏顺序设置和大屏名称。自定义统计周期资产组划分、选择播放大屏及轮播时间间隔，大屏包含全网安全态势感知大屏、安全事件态势、资产态势； 4.支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议； 5.支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作； 6.支持网络安全设备规则，包括网络设备、安全设备、中间件、操作系统等； | 套 | 1 |
| 2.11 | 流量检测探针 | 1.软硬件一体化设备，标准1U机架式设备，配置接口≥6个千兆电口，≥4个千兆SFP光口 ，≥2个万兆SFP光口（含光模块）； 2.网络层吞吐量≥2Gbps，内存大小≥8G，硬盘容量≥480GB SSD，电源：冗余电源； 3.应具有丰富的安全策略配置，包括：网络攻击、业务脆弱性、僵尸网络检测、主动IP扫描、文件安全、邮件安全； 4.为确保应用识别漏洞分析能力，要求设备能够识别应用类型超过1000种，应用识别规则总数超过3000条，漏洞利用规则特征库数量超过4000条； 5.为防止敏感数据泄密，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤； 6.为实现未知威胁的处理能力，具备同云端安全分析引擎进行联动的能力； 7.支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级； | 套 | 2 |
| 2.12 | 备份一体机 | 1.提供≥15TB备份容量许可；配置≥2颗CPU，单颗≥32核，≥64GB DDR4配置系统盘≥2\*600 GB SAS硬盘,数据盘≥12\*4T 硬盘，≥4\*GE+2\*10GE； 2.支持主流的数据库备份恢复，包括：Oracle、SQL Server、MySQL、Sybase、DB2、Informix、PostgreSQL、MongoDB、Caché等主流数据库应用； 3.支持主流国产芯片服务器平台，支持备份服务端或者客户端部署在龙芯、飞腾、鲲鹏、海光、申威、兆芯等服务器平台上； 4.支持VMware、Hyper-V、Xenserver、Xen、KVM、FusionCompute、FusionCloud（Huawei Cloud Stack）、H3C CAS、OpenStack、CNware、RHV、易捷行云EasyStack、腾讯云TStack、ZStack等虚拟化平台或云平台的备份恢复； 5.支持在线文件备份，支持全量备份、增量备份。支持对Windows、Linux、UNIX平台单文件/目录进行细颗粒度的恢复。备份支持通过名称或通配符进行文件过滤，排除操作系统文件和一些指定扩展名的文件类型； 6.支持断点续传、备份重试、重试间隔设置，可根据网络健壮情况调整时间和次数； 7.支持AES、SM4等加密算法。加密算法可选择CBC、CFB、ECB、OFB等加密模式，对于AES的密钥支持设置128、192、256等长度。 | 台 | 1 |
| 2.13 | 服务器密码机 | 1.对称密钥对数：≥1024个，非对称密钥对数：≥1024对，SM2生成密钥：≥12000对/s；SM2加密：≥2600次/s；SM2解密：≥3000次/s；SM2签名：≥12000次/s；SM2验签≥4300次/s； 2.支持密码算法：1）非对称算法：国密SM2；国际RSA1024、RSA2048、RSA3072、RSA4096；2）对称算法：国密SM1、SM4；国际DES、3DES、AES；3）摘要算法：国密SM3；国际SHA1、SHA256、SHA512； 3.扩展能力：集群支持及性能扩展。支持多线程、多任务和性能扩展，多机热备和负载均衡，可多机扩展并行工作； 4.管理功能：采用分级权限管理，管理人员身份凭证信息安全存储在USBKEY中；支持WEB及C/S管理方式，并支持SSL协议确保通信的机密性；支持国密SHH、国密FTP，保证整机运维安全；支持服务器密码机日志完整性保护； | 台 | 2 |
| 2.14 | 签名验签和时间戳二合一服务器 | 1.硬件要求：2U高机架式硬件架构，单电源（可扩容成冗余电源），≥8GB内存，≥2TB硬盘容量，标准配置≥8个以太网千兆电口，支持≥2个接口扩展槽位； 2.SM2算法：签名速度：≥17000次/秒；验签速度：≥15000次/秒；签名速度：≥12000次/秒；验签速度：≥8000次/秒；SM3杂凑算法：≥860Mbps；数字证书验证速度：≥1500次/秒；数字信封制作速度：≥2000次/秒；数字信封解析速度：≥3000次/秒；SM2签名密钥对数量：≥512对；SM2加密密钥对数量：≥512对；对称密钥数量：≥1024个；时间戳签发速度：≥4300次/秒；时间戳验证速度：≥7300次/秒； 3.同时符合GM/T 0029《签名验签服务器技术规范》、GM/T 0033 《时间戳接口规范》、GM/T 0028《密码模块安全技术要求》等相关技术要求； 4.支持多机并行工作模式；支持负载均衡；支持双机热备部署； 5.支持CPU和内存的利用率、磁盘占用率、网络状态、用户登录状态等的实时监控；  6.支持基于SM2算法的时间戳服务，为应用系统提供时间戳签发、验证时间戳服务，实现对数据、消息、文件等多种格式原文数据的时间戳签发服务； 7.支持NPT协议，支持多个第三方时间源的配置管理，能够与第三方授时中心、卫星授权时间源（北斗、GPS）进行时间同步，确保签发时间戳时所获取的时间有效、精确； 8.支持配置记录日志的类型，如运行日志、DEBUG日志、错误日志；支持日志的查询、审计、下载、清除；采用数字签名技术对日志数据进行完整性保护； 9.支持设置访问IP白名单，仅允许白名单内IP访问签名验签服务器； 10.支持数字证书有效性验证策略配置，至少包括验证证书有效期、验证证书签名有效性、验证证书是否在CRL中三种验证策略。 | 台 | 2 |
| 2.15 | 国密VPN综合安全网关 | 1.通过国密VPN产品实现SSL VPN接入，提供支持国密算法的SSL隧道加密连接服务，保证接入的实体身份真实性，通信访问过程的机密性、完整性；提供125个 SSL VPN授权；  2.硬件规格：配置千兆电口≥16， 千兆光口≥4，万兆光口≥6，Combo口≥4；接口扩展槽位≥2；硬盘扩展槽≥2，可支持扩展SSD硬盘≥960GB；配置双电源；  3.性能要求：吞吐量≥15Gbps，应用层吞吐量≥5Gbps，最大并发连接数≥500万，每秒新建连接数≥12万，IPSec VPN隧道≥4000，SSL VPN最大并发用户≥6000；  4.虚拟化能力：支持虚拟防火墙功能，支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；  5.SSL VPN支持页面定制功能特性，包括登录页面、交互信息、提示信息的定制功能； 防火墙在SSLVPN页面上修改用户密码，支持防暴力破解密码。  6.支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。  7.支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署。 | 台 | 2 |
| 2.16 | 国密浏览器 | 1.双算法支持，同时支持国密算法和国际通用算法。 对称算法支持 SM4、3DES、AES；非对称算法支持 SM2、RSA（1024、2048、4096）、ECC；杂凑密码算法支持 SM3、SHA\_1、SHA\_256、SHA\_512；  2.支持 SSL 链接，浏览器支持 SSL，TLS，可支持配置国密/国际算法； 3.支持 SSL 单项及双向链接，与 Web 服务器之间建立安全通道，保证 Web 网页访问的安全性； 4.支持基于 SM2算法 、RSA算法的数字证书、数字证书撤销列表（CRL）； 5.支持 NPAPI、PPAPI 控件。 | 项 | 100 |
| 2.17 | 设备证书 | 设备证书（分别为签名验签和时间戳二合一服务器、VPN网关提供证书支撑），有效期不低于3年。 | 项 | 4 |
| 2.18 | 个人证书 | 个人证书（提供运维人员的身份鉴别服务），有效期不低于3年。 | 项 | 100 |
| 2.19 | 智能密码钥匙 | 1.支持ECB、CBC、OFB模式的SM1密码算法； 2.支持SM2密码算法，可在内部进行加解密、签名验签、密钥对生成； 3.支持SM3密码算法； 4.支持ECB、CBC、OFB模式的SM4密码算法； 5.支持数据的安全存储功能； | 台 | 100 |
| 3 | **边界安全服务** | | | |
| 3.1 | **电子政务外网与视频专网的安全边界服务** | | | |
| 3.1.1 | 下一代防火墙 | 1.千兆电口≥12，千兆光口≥8，10G接口≥4，配置双电源，240G硬盘，实配IPS、AV、URL过滤升级license不低于3年； 2.实配SSL VPN并发数100可扩展2000，IPSec VPN隧道≥8000，虚拟防火墙数量≥500； 3.吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万； 4.能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、VLANID、内容安全统一界面进行安全策略配置； 5.支持加密流量解密后镜像给第三方设备做审计，安全检测； 6.支持防火墙内置流探针，对网络中的流量进行采集，上送网络安全智能分析系统进行威胁分析。 | 套 | 1 |
| 3.1.2 | 接入控制系统 | 1.配置≥5个1000M BASE-T接口，千兆光口≥4个，千兆多模光模块≥2个； 每秒事务数（TPS)：≥8000（次/秒），吞吐量：≥16Gbps； 2.支持双操作系统冷备，当常用系统出现故障，可以使用备用系统恢复； 3.准入设备应提供客户端的准入模式和无客户端准入模式，可供自定义部署和管理； 4.准入设备应能对各类接入设备进行准入控制，同时支持最少4种准入方式复用； 5.能够自动收集终端设备，能够自动绘制出网络拓扑图，支持可网管型交换机面板图形化展现各接口状态； 6.支持终端入网的安全基线检查、软件安全检查、账户密码安全检查、环境安全检查等检查项； 7.支持对网络攻击行为的发现和告警，如Smurf入侵、LAND攻击、WINNUK攻击等； 8.内置Radius认证服务，支持证书的本地管理和发放，实现双因素认证； 9.支持对终端接受访问的源地址、接受访问的服务以及接受访问的进程进行管理，只有允许的进程才能接受指定的访问者对指定服务的访问； 10.支持对哑终端设备的基线检查，包含但不限于弱口令扫描、漏洞扫描、高危端口检测、异常流量检测； 11.支持基于设备事件、终端事件、用户事件、访客事件、网络事件、系统事件等自定义告警事件。 | 套 | 1 |
| 3.1.3 | 集控探针 | 1.产品形态：标准机架式设备，千兆电口≥4，专用安全加固Linux操作系统； 2.性能指标：日志采集能力≥200Mbps； 3.支持采集多种设备的运行状态信息； 4.支持对多种设备的流量信息采集； 5.支持SYSLOG协议； 6.支持SNMP v2/SNMP v3协议；  7.支持将数据对接至市局（系统对接等相关信息由采购人负责协调或提供）。 | 套 | 2 |
| 3.1.4 | 视频安全接入系统 | 1.产品形态：标准机架式设备，≥2个以上千兆电口，≥2个万兆光口，配置≥2个万兆光模块，专用安全加固Linux操作系统； 2.性能指标：数据吞吐量≥4000Mbps；数据包丢失率<0.1‰；设备堆叠：支持≥16台设备堆叠； 3.要求可以直接认证内网用户使用的数字证书，支持基于公安U-key的身份认证； 4.支持自主开发的终端认证机制，采用AES加密算法对客户端和终端设备进行认证； 5.支持基于IP地址+MAC地址控制视频服务器的接入； 6.要求能直接支持不少于40多种视频控制协议 ； 7.要求产品具备视频访问控制功能，可设置视频控制信令和视频流分流，支持通过视频控制信令双向、视频流单向传输等多种访问规则对视频访问进行控制； 8.要求产品具备视频协议类型扩充机制，可通过导入视频参数组件增加新的视频协议类型； 9.要求视频安全交换接入系统支持加密视频下载和视频数据验签功能； 10.要求产品具备视频流分发功能，支持将同一路视频流分发给多个不同的客户端查看；  11.支持将数据对接至市局（系统对接等相关信息由采购人负责协调或提供）。 | 套 | 1 |
| 3.1.5 | 视频接入认证系统 | 1.与视频安全交换接入系统配套使用，配置1个100/1000M Base-TX管理接口，≥5个100/1000M Base-TX网络接口,≥2个万兆光口，配置≥2个万兆多模光模块；支持专用安全加固Linux操作系统； 2.性能指标：传输延时≤10ms；数据吞吐量≥4000Mbps；数据包丢失率<0.1‰；支持≥16台设备堆叠； 3.对接入对象（终端、视频服务器等）进行设备认证并与之交互，禁止未认证设备连接； 4.支持厂商协议（海康、大华、华为），可对常见视频协议的命令和参数进行分析和过滤； 5.按照预先注册的视频控制信令的类型、格式和内容，对控制信令进行“白名单”方式的格式检查和内容过滤。 | 套 | 1 |
| 3.1.6 | 视频用户认证系统 | 1.与视频安全交换接入系统配套使用，配置1个100/1000M Base-TX管理接口，≥5个100/1000M Base-TX网络接口，≥2个万兆光口，配置≥2个万兆多模光模块；专用安全加固Linux操作系统； 2.性能指标：传输延时≤10ms；数据吞吐量≥4000Mbps；数据包丢失率<0.1‰；支持≥16台设备堆叠； 3.支持对用户进行身份认证和访问控制，保证仅允许认证通过的用户才能访问已授权的视频资源； 4.支持直接认证警用硬件数字证书或用户名口令，保证仅允许认证通过的用户访问视频资源； 5.支持根据用户权限进行访问控制，确保用户仅能访问已授权的视频资源。 | 套 | 1 |
| 3.1.7 | 安全数据交换节点软件 | 1.交换能力：≥4000Mbps；并发会话：≥30000个；数据库到数据库交换记录数（＞100Kb/记录）：≥20000条/秒；文件数据处理数（＞100Kb/个）：≥20000个/秒； 2.支持服务个数：≥80；文件数据处理吞吐量：≥4000Mbps；应用层数据交换速度（FTP）：≥4000Mbps；数据文件：≥30G； 3.支持关系型数据库数据交换：Oracle、DB2.SQL Server、GreenPlum、Sybase、MYSQL、PostGresql的各种版本，及支持dameng、Gbase、oscar、kingbase等国产数据库，及支持Cassandra、UDB等大数据数据库； 4.支持各种数据库之间的异构数据转换； 5.能够配置行过滤、列转换、身份认证过滤、字段值长度过滤、枚举值过滤、数值范围进行数据交换过滤； 6.支持与Kafka集群直接对接部署，实现Kafka消息队列数据跨网交换，满足海量小文件跨网高性能交换需求； 7.支持通过解析数据库日志文件的技术原理，在不同类型的数据库之间进行数据同步。无需在数据库中创建触发器、存储过程、临时表等对象，实现低干扰的数据采集； 8.支持平面文件与数据库之间的互相转换； 9.数据库同步过程中，支持把交互数据落地为私有格式文件进行落地交换，保障数据库交互的安全性； 10.支持灵活多样的数据库数据获取方式，如：触发器、奉献、快照日志、同表双向、全表同步、升序增量等； | 项 | 2 |
| 3.1.8 | 安全数据交换节点专用硬件 | 1.硬件配置：接口标配1个100/1000M Base-TX管理接口，≥1个100/1000M Base-TX网络接口，≥2个10000M SFP+接口，配置≥2个万兆多模光模块 ；CPU配置：4核或以上处理器，主频≥3.3GHz；内存配置：≥16GB；硬盘配置：≥2TB； 2.主机基础操作系统采用具有多核并行安全操作系统； 3.系统根据安全数据交换软件进行安全裁剪。 | 套 | 2 |
| 3.1.9 | 安全隔离与信息交换系统 | 1.产品形态：标准机架式设备，采用“2+1”系统架构，冗余电源；内外主机均具备6个千兆网络接口、4个千兆光口、4个万兆光口，配置4个千兆多模光模块，4个万兆多模光模块；内、外网分别具有独立的管理接口，而不是通过网络接口管理，也不是通过内网一个管理接口完成全部管理；内、外网分别具有独立的HA口； 2.性能指标：吞吐量≥9Gbps，硬件切换时间＜1ms； 3.内外网主机系统分别支持双系统引导，并可在WEB界面上直接配置启动顺序，在A系统发生故障时，可以随时切换到B系统；且支持系统（包括配置）备份； 4.支持IPv6网络环境； 5.支持文件交换、数据库同步、数据库访问、安全浏览、FTP访问、邮件传输、定制访问、消息传输等功能； 6.支持双机热备、负载均衡功能； 7.支持日志审计，支持SYSLOG。 | 套 | 1 |
| 3.1.10 | 请求服务系统节点软件 | 1.性能指标：并发会话≥30000个，支持服务个数≥60个，传输延时<1秒； 2.支持Soap、xml-rpc、restful等协议的请求响应服务；支持请求转文件（XML文件）和应答转文件（XML文件）； 3.系统支持对SOAP协议的格式检查、病毒查杀及内容过滤；防止数据被窃听、被篡改； 4.支持WSDL格式文件导入，如果发现不符合WSDL格式的请求，系统自动阻断连接并报警； 5.支持安全可靠的Agent-2请求响应服务，同时可以进行服务发布； 6.支持多服务并发访问，支持数据库业务的请求与响应，支持移动应用访问； 7.发送端定制协议交换单元和接收端定制协议交换单元通过信息摆渡方式实现信息内外网间数据收发控制信息的交互，并通过SOAP函数调用进行数据交换； 8.业务配置过程中不对外暴露内网的应用系统及账号密码，保障业务安全性； 9.数据交互过程无协议穿透，交互协议转换成私有格式文件落地交换； 10.支持用户管理、不同用户可以分配管理不同的业务权限； 11.支持对接入业务的监控及管理； 12.支持资源管理，防止非法业务接入； 13.通过设备界面可以对产品进行平滑升级，同时界面展示历史升级记录； 14.通过设备界面可以实时对服务进行测试，了解业务运行情况； 15.与市局现有安全数据交换系统进行联动，对请求的内容进行封装，实现安全隔离下进行请求的传输和转发，最终实现请求与响应业务； 16.支持请求服务行为的审计，包括用户信息审计、行为信息审计、访问内容审计等，可以通过多种组合方式查询。 | 项 | 2 |
| 3.1.11 | 请求服务系统节点专用硬件 | 1.接口配置1个100/1000M Base-TX管理接口，≥1个100/1000M Base-TX网络接口，≥2个10000M SFP+接口，配置≥2个万兆多模光模块 ；CPU配置：4核或以上处理器，主频≥3.3GHz；内存配置：≥16GB；硬盘配置：≥2TB； 2.主机基础操作系统采用多核并行安全操作系统； 3.系统根据安全数据交换软件进行安全裁剪。 | 套 | 2 |
| 3.1.12 | 视频集中监控模块（软件） | 1.在市局原有集中监控与管理系统上升级部署； 2.最大支持监控的视频安全接入系统数量≥32台； 3.最大支持业务注册数量≥100个； 4.最大注册终端数量≥5000个； 5.对视频接入业务以及使用终端的注册； 6.对视频接入业务的监控和管理； 7.对视频安全接入系统的监控； 8.对视频接入业务运行的统计分析； 9.对业务运行和使用用户进行审计分析。 | 项 | 1 |
| 3.1.13 | 三层交换机 | 1.交换容量≥2.5Tbps，包转发率≥1200Mpps； 2.支持万兆SFP+接口≥24个，100GE QSFP28接口≥6个，配置双电源，提供≥40G堆叠电缆； 3.支持端到端的丢包统计，当丢包超过阈值时可触发告警； 4.支持VxLAN功能。 | 台 | 2 |
| 3.2 | **视频专网到公安网边界服务** | | | |
| 3.2.1 | 下一代防火墙 | 1.千兆电口≥12，千兆光口≥8，10G接口≥4，配置双电源，240G硬盘，实配IPS、AV、URL过滤升级license不低于3年； 2.实配SSL VPN并发数100可扩展2000，IPSec VPN隧道≥8000，虚拟防火墙数量≥500； 3.吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万； 4.能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、VLANID、内容安全统一界面进行安全策略配置； 5.支持加密流量解密后镜像给第三方设备做审计，安全检测； 6.支持防火墙内置流探针，对网络中的流量进行采集，上送网络安全智能分析系统进行威胁分析。 | 套 | 2 |
| 3.2.2 | 可信边界安全网关 | 1.标准机架式设备：千兆网口≥4个，万兆光口≥2个； 2.性能：新建连接数：≥3500次/秒，并发连接数：≥100000，SSL事物处理速率：≥4000次/秒，加密宽带吞吐：≥1.5Gbps，整机吞吐≥3G，支持接入用户数：≥50000； 3.支持Windows、Linux、Android、IOS等计算机、移动智能终端的安全接入； 4.支持服务状态自检测,包括服务端引擎检测、客户端自检测、客户端检测日志展示,提高故障诊断能力，便于后期系统运维和故障定位； 5.支持应用保护：保护B/S应用和业务、保护HTTPS应用和业务、保护C/S应用和业务、保护数据库服务、保护视频流服务； 6.支持DNS代理：用户可自定义虚拟DNS服务并自动向客户端下发解析策略； 7.支持多种用户接入认证方式：包含用户名口令、USBkey、用户名+口令+短信、文件数字证书+口令等认证方式；支持第三方接入认证，至少包含LDAP、AD、Radius、TACACS+等认证方式； 8.内置CA模块，支持在网关管理页面进行证书签发管理操作，支持为自助终端签发专用设备证书而不必依赖于第三方CA系统； 9.密码算法支持：支持RSA1024/RSA2048.AES256.SHA-1/SHA-2密码算法，支持国家密码管理局颁布的SM2.SM3.SM4密码算法； 10.支持终端管理：支持自动提取终端设备的设备指纹，设备指纹信息至少包含硬件设备的CPU、硬盘等硬件唯一标识信息；支持自动提取终端设备的IP地址、MAC地址等信息；支持用户和终端绑定认证，包含一对一、一对多、多对一和多对多等模式； 11.支持双机热备和负载均衡。 | 套 | 1 |
| 3.2.3 | 入侵检测系统 | 1.标准机架的专业设备（禁止使用防火墙或UTM的IPS功能替代）；  2.业务口配置 千兆COMBO口≥8， 千兆电口≥4， 千兆光口≥4，万兆光口≥6；  3.IPS检测吞吐量≥12Gbit/s；每秒新建连接数≥25万；最大并发连接数≥1000万；  4.采用国产化的关键芯片(CPU )；  5.能够防范各种应用层攻击，包括但不限于：后门程序，木马程序，间谍软件，蠕虫，僵尸主机，异常代码，协议异常，扫描，可疑行为审计类等，能够对跨站攻击、SQL注入等WEB攻击行为进行有效防护；  6.支持不少于6000种的应用识别能力；  7.实际配置三年ips特征库升级服务，需满足≥240G SSD 硬盘。 | 套 | 1 |
| 3.2.4 | 集控探针 | 1.产品形态：标准机架式设备，4个以上千兆电口，支持专用安全加固Linux操作系统； 2.性能指标：日志采集能力≥200Mbps； 3.支持采集多种设备的运行状态信息； 4.支持对多种设备的流量信息采集； 5.支持SYSLOG协议； 6.支持SNMP v2/SNMP v3协议；  7.支持将数据对接至市局（系统对接等相关信息由采购人负责协调或提供）。 | 套 | 2 |
| 3.2.5 | 视频安全接入系统 | 1.产品形态：标准机架式设备，≥2个以上千兆电口，≥2个万兆光口，配置≥2个万兆光模块，支持专用安全加固Linux操作系统； 2.性能指标：数据吞吐量≥4000Mbps；数据包丢失率<0.1‰；设备堆叠：支持≥16台设备堆叠； 3.要求可以直接认证内网用户使用的数字证书，支持基于公安U-key的身份认证； 4.支持自主开发的终端认证机制，采用AES加密算法对客户端和终端设备进行认证； 5.支持基于IP地址+MAC地址控制视频服务器的接入； 6.要求能直接支持不少于40多种视频控制协议 ； 7.要求产品具备视频访问控制功能，可设置视频控制信令和视频流分流，支持通过视频控制信令双向、视频流单向传输等多种访问规则对视频访问进行控制； 8.要求产品能够抵御各种DOS/DDoS攻击，能够识别和防御Flood、ICMP Flood等攻击； 9.要求产品具备视频协议类型扩充机制，可通过导入视频参数组件增加新的视频协议类型； 10.要求视频安全交换接入系统支持加密视频下载和视频数据验签功能； 11.要求产品具备视频流分发功能，支持将同一路视频流分发给多个不同的客户端查看； 12.支持将数据对接至市局（系统对接等相关信息由采购人负责协调或提供）。 | 套 | 1 |
| 3.2.6 | 视频接入认证系统 | 1.与视频安全交换接入系统配套使用，配置1个100/1000M Base-TX管理接口，≥5个100/1000M Base-TX网络接口，≥2个万兆光口，配置≥2个万兆多模光模块；专用安全加固Linux操作系统； 2.性能指标：传输延时≤10ms；数据吞吐量≥4000Mbps；数据包丢失率<0.1‰；支持≥16台设备堆叠； 3.对接入对象（终端、视频服务器等）进行设备认证并与之交互，禁止未认证设备连接； 4.支持厂商协议（海康、大华、华为），可对常见视频协议的命令和参数进行分析和过滤； 5.按照预先注册的视频控制信令的类型、格式和内容，对控制信令进行“白名单”方式的格式检查和内容过滤。 | 套 | 1 |
| 3.2.7 | 视频用户认证系统 | 1.与视频安全交换接入系统配套使用，配置1个100/1000M Base-TX管理接口，≥5个100/1000M Base-TX网络接口，≥2个万兆光口，配置≥2个万兆多模光模块；支持专用安全加固Linux操作系统； 2.性能指标：传输延时≤10ms；数据吞吐量≥4000Mbps；数据包丢失率<0.1‰；支持≥16台设备堆叠； 3.支持对用户进行身份认证和访问控制，保证仅允许认证通过的用户才能访问已授权的视频资源； 4.支持直接认证警用硬件数字证书或用户名口令，保证仅允许认证通过的用户访问视频资源； 5.支持根据用户权限进行访问控制，确保用户仅能访问已授权的视频资源。 | 套 | 1 |
| 3.2.8 | 安全数据交换节点软件 | 1.交换能力：≥4000Mbps；并发会话：≥30000个；数据库到数据库交换记录数（＞100Kb/记录）：≥20000条/秒；文件数据处理数（＞100Kb/个）：≥20000个/秒； 2.支持服务个数：≥80；文件数据处理吞吐量：≥4000Mbps；应用层数据交换速度（FTP）：≥4000Mbps；数据文件：≥30G； 3.支持主流关系型数据库数据交换：Oracle、DB2.SQL Server、GreenPlum、Sybase、MYSQL、PostGresql的各种版本，及支持dameng、Gbase、oscar、kingbase等国产数据库，及支持Cassandra、UDB等大数据数据库； 4.支持各种数据库之间的异构数据转换； 5.能够配置行过滤、列转换、身份认证过滤、字段值长度过滤、枚举值过滤、数值范围进行数据交换过滤； 6.支持与Kafka集群直接对接部署，实现Kafka消息队列数据跨网交换，满足海量小文件跨网高性能交换需求； 7.支持云对象存储OSS（Object Storage Service），支持云数据仓库 MaxCompute，支持流数据处理平台DataHub等； 8.支持通过解析数据库日志文件的技术原理，在不同类型的数据库之间进行数据同步。无需在数据库中创建触发器、存储过程、临时表等对象，实现低干扰的数据采集； 9.支持平面文件与数据库之间的互相转换； 10.数据库同步过程中，支持把交互数据落地为私有格式文件进行落地交换，保障数据库交互的安全性； 11.支持灵活多样的数据库数据获取方式，如：触发器、奉献、快照日志、同表双向、全表同步、升序增量等； 12.具备多种抗恶意数据攻击能力，如：exe文件过滤、图片文件夹带恶意代码、jpg文件捆绑可执行程序、恶意代码穿透等。 | 项 | 2 |
| 3.2.9 | 安全数据交换节点专用硬件 | 1.硬件配置：接口标配1个100/1000M Base-TX管理接口，≥1个100/1000M Base-TX网络接口，≥2个10000M SFP+接口，配置≥2个万兆多模光模块 ；CPU配置：4核或以上处理器，主频≥3.3GHz；内存配置：≥16GB；硬盘配置：≥2TB； 2.主机基础操作系统采用具有多核并行安全操作系统； 3.支持系统根据安全数据交换软件进行安全裁剪。 | 套 | 2 |
| 3.2.10 | 安全隔离与信息交换系统 | 1.产品形态：标准2U机架式设备，采用“2+1”系统架构，冗余电源；内外主机均具备6个千兆网络接口、4个千兆光口、4个万兆光口，配置4个千兆多模光模块，4个万兆多模光模块；内、外网分别具有独立的管理接口，而不是通过网络接口管理，也不是通过内网一个管理接口完成全部管理；内、外网分别具有独立的HA口； 2.性能指标：吞吐量≥9Gbps，硬件切换时间＜1ms； 3.内外网主机系统分别支持双系统引导，并可在WEB界面上直接配置启动顺序，在A系统发生故障时，可以随时切换到B系统；且支持系统（包括配置）备份； 4.支持IPv6网络环境； 5.支持文件交换、数据库同步、数据库访问、安全浏览、FTP访问、邮件传输、定制访问、消息传输等功能； 6.支持双机热备、负载均衡功能； 7.支持日志审计，支持SYSLOG。 | 套 | 1 |
| 3.2.11 | 请求服务系统节点软件 | 1.性能指标：并发会话≥30000个，支持服务个数≥60个，传输延时<1s； 2.支持Soap、xml-rpc、restful等协议的请求响应服务；支持请求转文件（XML文件）和应答转文件（XML文件）； 3.系统支持对SOAP协议的格式检查、病毒查杀及内容过滤；防止数据被窃听、被篡改； 4.支持WSDL格式文件导入，如果发现不符合WSDL格式的请求，系统自动阻断连接并报警； 5.支持安全可靠的Agent-2请求响应服务，同时可以进行服务发布； 6.支持多服务并发访问，支持数据库业务的请求与响应，支持移动应用访问； 7.发送端定制协议交换单元和接收端定制协议交换单元通过信息摆渡方式实现信息内外网间数据收发控制信息的交互，并通过SOAP函数调用进行数据交换； 8.业务配置过程中不对外暴露内网的应用系统及账号密码，保障业务安全性； 9.数据交互过程无协议穿透，交互协议转换成私有格式文件落地交换； 10.支持用户管理、不同用户可以分配管理不同的业务权限； 11.支持对接入业务的监控及管理； 12.采用BS架构，支持https安全加密访问，同时支持数字证书及用户名密码等安全认证机制增强产品自身安全性； 13.支持资源管理，防止非法业务接入； 14.通过设备界面可以对产品进行平滑升级，同时界面展示历史升级记录； 15.通过设备界面可以实时对服务进行测试，了解业务运行情况； 16.与市局现有安全数据交换系统进行联动，对请求的内容进行封装，实现安全隔离下进行请求的传输和转发，最终实现请求与响应业务； 17.支持请求服务行为的审计，包括用户信息审计、行为信息审计、访问内容审计等，可以通过多种组合方式查询。 | 项 | 2 |
| 3.2.12 | 请求服务系统节点专用硬件 | 1.接口配置1个100/1000M Base-TX管理接口，≥1个100/1000M Base-TX网络接口，≥2个10000M SFP+接口，配置≥2个万兆多模光模块 ；CPU配置：4核或以上处理器，主频≥3.3GHz；内存配置：≥16GB；硬盘配置：≥2TB； 2.主机基础操作系统采用多核并行安全操作系统； 3.系统根据安全数据交换软件进行安全裁剪。 | 套 | 2 |
| 3.2.13 | 三层交换机 | 1.交换容量≥2.5Tbps，包转发率≥1200Mpps； 2.支持万兆SFP+接口≥24个，100GE QSFP28接口≥6个，配置双电源，提供≥40G堆叠电缆； 3.支持端到端的丢包统计，当丢包超过阈值时可触发告警； 4.支持VxLAN功能。 | 台 | 2 |
| 4 | **终端安全服务** | | | |
| **4.1** | 终端安全管控平台部署服务器 | 1.CPU配置：采用X86架构，配置≥1颗CPU，每颗CPU≥8个物理核.主频频率≥2.1GHz； 2.内存配置：≥64GB DDR4； 3.硬盘配置：≥2块480GB SSD硬盘；1块6TB 7.2K SATA硬盘； 4.RAID卡配置：支持RAID0/1/10； 5.以太网连接：≥2个千兆电口； 6.电源配置：热插拔冗余电源，电源模块满配置。 | 台 | 4 |
| 4.2 | 汇聚交换机 | 1.上行速率：≥10000MBps； 2.下行速度：≥1000MBps； 3.端口：千兆电口≥48，万兆光口≥4。 | 台 | 9 |
| 4.3 | 接入交换机 | 1.上行速率：≥1000MBps； 2.下行速度：≥1000MBps； 3.端口：千兆电口≥24，千兆光口≥4。 | 台 | 18 |
| 4.4 | 端隐终端安全系统 | 1、端隐终端安全控制中心  概览-数据中心：可视化呈现终端设备，网络设备以及系统流量分析  概览-网络拓扑：展示当前系统设备连接情况和连接状态  资产管理-终端设备：该模块主要用于展示终端设备信息，信息变更记录等基本内容，同时具有终端设备识别，流量感知以及安全策略响应等安全功能  资产管理-网络设备：该模块主要用于展示网络设备基本信息以及对应端口状态和流量信息。  资产管理-IP管理：该功能模块主要负责系统内IP的信息展示以及管理，主要涉及IP的网域划分，IP所属VLAN，IP状态，IP使用记录情况等信息  资产管理-组织架构：该功能模块主要用于编辑组织架构并管理其关联的终端设备和网络设备信息  终端入网管控：根据终端设备安全状态，实时进行安全管控：主要在设备接入交换机进行ACL规则下发，不符合要求设备直接在交换机上进行流量阻断。（陌生设备接入网络，根据ACL规则直接对设备进行阻断，从最底层隔绝陌生设备数据流量，确保网络安全。对终端设备MAC地址，IP地址以及交换机端口进行绑定，当终端设备IP地址、MAC 地址或者接入端口任一信息发生变化，则对当前设备进行阻断操作，防止私接设备或者乱接设备带来的安全风险。）  数据大屏：重点资产监控，根据组织维度可视化呈现资产数据信息以及风险信息等，包括：终端资产，在线情况，IP资产，告警情况等信息。  策略管理-安全策略：该功能模块主要负责创建应用于终端设备的安全策略，安全策略自动下发，以实现威胁自动化处置、违规外联阻断等安全功能。  策略管理-风险模型：该功能模块基于零信任安全防御，支持终端多维感知、零信任持续可信评估。针对终端设备从终端身份，网络链路，健康状况，脆弱程度，操作行为5个进行安排感知评估。  威胁响应-风险告警：该功能模块主要用于设置告警策略以及通知方式。  威胁响应-告警设置：该功能模块主要用于设置告警策略以及通知方式。  日志-终端日志：该模块可以查看终端设备的访问、操作日志及安全策略的执行详情  日志-管理日志：该模块可以查看管理员在控制中心和系统定期执行操作的日志  2、端隐终端安全客户端  违规阻断：从终端网络驱动层，对数据流量进行管控，确保违规外联发生之前进行阻断  威胁感知：客户端从对所有出入设备流量、终端系统安全环境等进行安全感知并将信息及时上报到控制中心安全模块，协同安全策略和风险模型对客户端进行安全管控，确保终端环境安全  信息探测：同步终端设备信息：系统版本、硬盘存储等信息  3、功能可用性要求  前提条件：保证视频网和信息网网络通畅，终端状态正常且正常连网，交换机接受到的数据包完整。  （1）具体要求：  ①客户端安装覆盖要求：公安视频网终端和公安信息网终端，安装覆盖率＞99%。基于分局提供的全量终端清单进行安装。  ②违规外联要求：所有安装了安全平台软件的终端，违规外联阻断率＞99%。因为软件问题导致未及时识别和阻断违规外联行为的，一经发现，立即整改。  ③终端准入要求：基于分局提供的全量信息网和视频网终端和哑终端清单，进行白名单准入管理，新加入终端需经过分局审核后加入白名单。非法终端阻断率＞99%。  ④资产管理要求：安装了客户端的终端，资产识别率＞99%，哑终端能够通过交换机进行ip、mac（视频网无法获取MAC）识别，接入本次项目新更换的交换机的哑终端资产识别覆盖率＞99%，部分资产信息自动入网时候需要手工补充：所属组织、责任人姓名、责任人电话、所处位置、设备类型(服务器、摄像头、pc电脑等）。  ⑤平台时效性要求：在终端设备数量2000规模下，平台资产信息更新时效性≤1天。  ⑥平台可用性要求：平台整体可用性＞99%。  4、特殊不受管控情况：  无法安装客户端的终端统一按照哑终端处理。  ①哑终端同时接入多个网络导致的违规外联,如哑终端通过分线器同时接入多个网络、哑终端设备具有无线连接功能同时接入多个网络。  ②pc终端通过私自获取卸载码，卸载终端安全客户端，然后接入其他网络的情况。  ③人为非法修改终端安全交换机配置导致的违规外联情况：修改ACL配置、修改交换机端口配置、擅自修改配置文件导致解析失败等。  ④交换机同时接入多个网络导致的违规外联。  ⑤终端设备通过NAT设备后再接入终端安全系统，如摄像头通过运营商网络接入到终端安全系统，运营商的网络有3层设备，导致摄像头的Mac无法监听到，如果运维人员通过电脑接入摄像头的网口，终端安全系统无法感知限制。  ⑥网络规划管理不完整导致的违规外联：根据分局提供的网络要求划分好的VLAN需要全量进行管理，未纳入管理部分的VLAN出现违规外联。  ⑦由于断电或者其他问题导致终端安全交换机功能缺失导致的违规外联。  5、分局网络满足以下前提条件：  ①分局需明确交换机等网络设备管理职责，不存在混用情况。  ②分局需明确当前网络拓扑结构，并严格按照网络划分进行管理，包括：网络区域划分的IP地址段和VLAN等信息。  ③需分局提供全部网络区域的设备数量、关联MAC地址和IP地址等信息的清单，如主机，交换机、摄像头、硬盘录像机、会议主机和其他相关接入设备。  ④在合同期间不能随意变更网络拓扑，以及交换机、路由器接入方式，如需变动请提前告知我方进行相应的配置和处理，避免网络接入遗漏。 | 套 | 2 |
| 4,5 | 终端授权 | 支持被管控终端数量（公安信息网） | 台 | 2300 |
| 4.6 | 支持被管控终端数量（公安视频专网） | 台 | 200 |
| **5** | **网络设备服务** | | | |
| **5.1** | **公安视频专网网络资源池服务** | | | |
| 5.1.1 | 分局核心交换机 | 1.交换容量≥387Tbps;包转发率≥115200 Mpps;  2.主控引擎与交换网板硬件分离,主控板故障或者更换不影响整机转发性能，支持业务板槽位数≥4；独立交换网板槽位数≥6； 3.支持风扇框数量≥3，电源槽位数≥4；整机散热风道为前后风道； 4.支持M-LAG或vPC等类似技术 5.为保证端口不间断进行数据转发，要求设备支持微突发检测功能，识别网络中潜在的拥塞风险； 6.支持VXLAN over IPv6.IPv6 VXLAN over IPv4功能； 7.支持Telemetry、Ip报文分片重组功能； 8.支持VxLAN OAM: VxLAN ping, VxLAN tracert功能； 9.实配双主控，独立交换网板≥6个，电源≥4个，万兆光端口≥48个，单台设备配置≥12个万兆多模光模块、≥12个万兆单模光模块； 10.为保证设备可靠性，集群或堆叠支持带外管理方式（主控板上提供专用GE端口用于集群或堆叠协议报文传送）；如主控板卡不支持，需单独配置一块业务板卡用于集群或堆叠带外管理。 | 台 | 1 |
| 5.1.2 | 视频专网核心交换机 | 1.交换容量≥645Tbps，包转发率≥230400Mpps； 2.主控引擎与交换网板物理分离，主控引擎≥2；独立交换网板≥6；整机业务板槽位数≥8； 3.交换网板与业务板散热相互独立，提升散热效率； 4.支持硬件BFD（Bidirectional Forwarding Detection）3.3ms检测间隔； 5.设备单台配置：双主控板，独立交换网板≥6，电源≥8个，万兆光口≥48个，100GE接口≥72个，100GE专用堆叠线缆5M； 6.支持并配置Netstream，支持M-LAG或vPC等类似技术； 7.支持RDMA和RoCE.； 8.支持独立的监控板，支持1+1热备，且不占用业务槽位； 9.为保证设备可靠性，集群或堆叠支持带外管理方式（主控板上提供专用GE端口用于集群或堆叠协议报文传送）；如主控板卡不支持，需单独配置一块业务板卡用于集群或堆叠带外管理。 | 台 | 2 |
| 5.1.3 | 运营商视频汇聚交换机 | 1.交换容量≥250Tbps，包转发率≥14000Mpps； 2.主控引擎与交换网板物理分离，主控引擎≥2；独立交换网板≥2；整机业务板槽位数≥4，主控槽位与业务线卡槽位宽度相同，为全宽槽位； 3.支持真实业务流的实时检测技术，秒级快速故障定位； 4.设备单台配置：双主控板、双电源冗余备份，万兆光口≥48个，100GE光口≥6，提供≥100GE堆叠电缆； | 台 | 2 |
| 5.1.4 | 管理区接入交换机 | 1.交换容量≥2.5Tbps，包转发率≥1200Mpps； 2.支持万兆SFP+接口≥24个，100GE QSFP28接口≥6个，配置双电源，提供≥40G堆叠电缆； 3.支持端到端的丢包统计，当丢包超过阈值时可触发告警； 4.支持VxLAN功能； | 台 | 2 |
| 5.1.5 | 业务接入交换机 | 1.交换容量≥4.8Tbps，包转发率≥2000Mpps； 2.10GE光端口数量≥48个，40GE/100GE端口数量≥6个； 3.支持M-LAG技术、支持微分段； 4.支持VxLAN OAM: VxLAN ping, VxLAN tracert； 5.支持Netstream； 6.实配双电源，提供≥40GE堆叠电缆； | 台 | 14 |
| 5.1.6 | 存储万兆交换机 | 1.交换容量≥4.8Tbps，包转发率≥2000Mpps； 2.万兆光端口数量≥48个，100GE端口数量≥6个； 3.支持VxLAN、M-LAG技术；支持微分段用于精细化东西向安全隔离。 | 台 | 12 |
| 5.1.7 | 存储管理交换机 | 1.交换容量≥1.2Tbps，包转发率≥250Mpps； 2.支持千兆电口≥48个，万兆SFP+接口≥4个； 3.配置标准USB接口，支持U盘快速开局； | 台 | 5 |
| 5.1.8 | BMC交换机 | 1.交换容量≥1.2Tbps，包转发率≥250Mpps； 2.支持千兆电口≥48个，万兆SFP+接口≥4个； 3.支持业务扩展插槽数≥1，扩展支持8个SFP+端口或4个40GE QSFP+端口； 4.配置标准USB接口，支持U盘快速开局； 5.支持Telemetry技术； | 台 | 6 |
| 5.1.9 | 100GE多模光模块 | 100GBase-SR4光模块-QSFP28-100G-多模模块(850nm,0.1km,MPO) | 个 | 130 |
| 5.1.10 | 万兆单模光模块 | 光模块-SFP+-10G-单模模块(1310nm,10km,LC) | 个 | 20 |
| 5.1.11 | 万兆单模光模块 | 光模块-SFP+-10G-单模模块(1550nm,80km,LC) | 个 | 8 |
| 5.1.12 | 万兆多模光模块 | SFP+-10G-多模模块(850nm,0.3km,LC) | 个 | 700 |
| 5.1.13 | 千兆电模块 | 电模块-SFP-GE-电接口模块(100m,RJ45) | 个 | 35 |
| 5.1.14 | 统一运维平台软件 | 1.系统支持大规模网络管理能力，支持交换机、WLAN、路由器、防火墙、服务器、存储、GPON、eLTE、IP话机、摄像头等设备的统一监控管理； 2.支持跨厂商设备管理，支持管理华为、Cisco、Juniper、H3C、Aruba厂商设备； 3.系统使用B/S架构，支持IE、Firefox、Chrome等主流浏览器，支持完全自主的操作系统、数据库； 4.系统支持告警信息中包含与故障关联的信息（如端口故障需关联呈现端口信息、故障信息、链路拓扑信息、历史流量信息、维护经验等）； 5.系统支持提供SNMP、FTP、Restful等丰富的北向接口，可提供告警、性能、资源等数据给上层应用系统； 6.提供网络设备节点授权许可≥100个,网络设备流量分析许可≥10个，实配SLA功能，存储设备许可≥50个，服务器管理许可≥600个，操作系统及应用 (实例数量)≥500个； | 套 | 1 |
| 5.1.15 | 统一运维平台硬件 | 配置不低于：2\*5218R-20Core/2.1GHz CPU,8\*32GB内存,2\*960G SSD，2\*1920 SSD,2\*8T,2\*10GE光口 | 台 | 1 |
| **5.2** | **公安信息网网络资源池服务** | | | |
| 5.2.1 | 公安内网核心交换机 | 1.交换容量≥645Tbps，包转发率≥230400Mpps； 2.主控引擎与交换网板物理分离，主控引擎≥2；独立交换网板≥6；整机业务板槽位数≥8； 3.支持风扇框数量≥3，交换网板与业务板散热相互独立，提升散热效率； 4.支持硬件BFD（Bidirectional Forwarding Detection）3.3ms检测间隔； 5.设备单台配置：双主控板，独立交换网板≥6，电源≥8个，万兆光口≥48个，40GE接口≥36个，40GE专用堆叠线缆5M； 6.支持并配置Netstream，支持M-LAG或vPC等类似技术； 7.支持RDMA和RoCE； 8.支持独立的监控板，支持1+1热备，且不占用业务槽位； 9.为保证设备可靠性，集群或堆叠支持带外管理方式（主控板上提供专用GE端口用于集群或堆叠协议报文传送）；如主控板卡不支持，需单独配置一块业务板卡用于集群或堆叠带外管理。 | 台 | 2 |
| 5.2.2 | 管理区接入交换机 | 1.交换容量≥2.5Tbps，包转发率≥1200Mpps； 2.支持万兆SFP+接口≥24个，100GE QSFP28接口≥6个，配置双电源，提供≥40G堆叠电缆； 3.支持端到端的丢包统计，当丢包超过阈值时可触发告警； 4.支持VxLAN功能； | 台 | 2 |
| 5.2.3 | 业务接入交换机 | 1.交换容量≥4.8Tbps，包转发率≥2000Mpps； 2.10GE光端口数量≥48个，40GE/100GE端口数量≥6个； 3.支持M-LAG技术； 4.支持VxLAN OAM: VxLAN ping, VxLAN tracert； 5.支持硬件BFD3.3ms检测间隔； 6.支持Netstream； 7.实配双电源，提供≥40GE堆叠电缆； | 台 | 8 |
| 5.2.4 | BMC交换机 | 1.交换容量≥1.2Tbps，包转发率≥250Mpps； 2.支持千兆电口≥48个，万兆SFP+接口≥4个； 3.支持业务扩展插槽数≥1，扩展支持8个SFP+端口或4个40GE QSFP+端口； 4.配置标准USB接口，支持U盘快速开局； 5.支持Telemetry技术； | 台 | 5 |
| 5.2.5 | 40GE多模光模块 | 40GBase-eSR4光模块-QSFP+-40G-多模模块(850nm,0.3km,MPO) (可对接4个SFP+) | 个 | 50 |
| 5.2.6 | 万兆单模光模块 | 光模块-SFP+-10G-单模模块(1550nm,80km,LC) | 个 | 4 |
| 5.2.7 | 万兆多模光模块 | SFP+-10G-多模模块(850nm,0.3km,LC) | 个 | 260 |
| 5.2.8 | 千兆电模块 | 电模块-SFP-GE-电接口模块(100m,RJ45) | 个 | 30 |
| 5.2.9 | 统一运维平台软件 | 1.系统支持大规模网络管理能力，支持交换机、WLAN、路由器、防火墙、服务器、存储、GPON、eLTE、IP话机、摄像头等设备的统一监控管理； 2.支持跨厂商设备管理，支持管理华为、Cisco、Juniper、H3C、Aruba厂商设备； 3.系统使用B/S架构，支持IE、Firefox、Chrome等主流浏览器，支持完全自主的操作系统、数据库； 4.系统支持告警信息中包含与故障关联的信息（如端口故障需关联呈现端口信息、故障信息、链路拓扑信息、历史流量信息、维护经验等）； 5.系统支持提供SNMP、FTP、Restful北向接口，可提供告警、性能、资源等数据给上层应用系统； 6.提供网络设备节点授权许可≥50个,网络设备流量分析许可≥10个，实配SLA功能，存储设备许可≥5个，服务器管理许可≥200个，操作系统及应用 (实例数量)≥200个，实配软件订阅服务不低于3年； | 套 | 1 |
| 5.2.10 | 统一运维平台硬件 | 配置不低于：2\*5220-18Core/2.2GHz CPU,12\*32GB内存,2\*480G SSD，2\*1920G SSD ,2\*10GE光口 | 台 | 1 |
| **6** | 机房及链路服务 | | | |
| 6.1 | 机房服务 | | | |
| 6.1.1 | 机房服务 | 提供专属物理隔离机房服务，提供满足本项目需求的服务器机柜，单机柜满足6Kw的用电需求，不低于40个；提供满足本项目需求的网络机柜，单机柜满足3Kw的用电需求，不低于5个。以上机柜均需提供配套的市电、油机、UPS、空调等机房配套环境和设施。 | 年 | 3 |
| 6.1.2 | 机房运维服务 | 提供7\*24小时机房驻场运维服务，需负责项目硬件设备的日常管理、问题受理、响应、处理和转交等方面的服务，实时监控机房运行环境，及时处理异常情况，定期巡检数据中心硬件设备，排除隐患。 | 年 | 3 |
| 6.2 | 链路服务 | |  |  |
| 6.2.1 | 前端汇聚链路 | 公安前端链路汇聚：满足7882路前端数据全量集中，提供链路汇聚传输服务，带宽≥90G，需满足业务需求，在服务期内保障服务范围内的视频、图像数据接入稳定流畅。 | 年 | 3 |
| 6.2.2 | 视频专网专线 | 数据中心至公安视频专网链路，带宽≥10G，一主一备，需满足业务需求，在服务期内保障服务范围内的视频、图像数据接入。 | 年 | 3 |
| **7** | **运维服务** | | | |
| 7.1 | 安全运维服务 | 1.提供安全咨询服务：根据网络安全法、数据安全法、等级保护、关键信息基础设施管理条例等合规咨询服务，按照等级保护定级备案流程，协助进行定级备案工作，遵照等级保护基本要求要求，通过对系统的技术与管理的角度进行差距分析，并提交整改方案，协助整改，最终帮助用户系统符合相关要求。服务周期：每年开展1次。 2.提供安全评估服务：对系统进行安全评估。在授权和监督下，模拟黑客的攻击手法，对指定的目标网站进行非破坏性的漏洞检测和攻击测试，查找应用、网络层面等存在的漏洞，评估网站网络安全。服务周期：每年开展2次。 3.提供应急演练服务：在真实网络环境下，模拟黑客组织对目标系统进行网络渗透/攻防，试图非法入侵，检验信息系统安全保护能力，对演练过程中发现的问题形成演练总结报告及整改方案；以模拟演练或者桌面推演的方式检验应急预案的完整性、可行性，提高应急处理能力。服务周期：每年开展1次。 4.提供应急响应服务：根据事件类别，提供全年的应急响应服务，通过远程和现场支持的形式协助客户对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等。紧急事件主要包括：勒索病毒、病毒和蠕虫事件、黑客入侵事件、数据泄露、挖矿事件等。服务周期：按需提供。 5.提供安全巡检服务：开展安全设备的性能指标、功能指标和硬件状态等进行定期巡检，记录指标值。针对指标产生的异常告警进行确认、分析，查找异常原因，提供解决方案，协解完成安全整改和修复。梳理网络和业务资产，针对网络收集的流量和日志进行安全审计和分析，及时发现网络攻击和异常行为。服务周期：每季度开展1次安全巡检服务，每年不少于4次。 6.提供重要时期保障服务：为确保在重保期间业务系统持续、稳定的运行，确保重要业务操作行为的可审计，抵御黑客、恶意代码、病毒等对用户信息系统的攻击与破坏，防止对用户信息系统的非法、非授权访问、恶意篡改、挂马等等，在重大活动时期（两会、国庆等），通过派遣专业工程师开展安全检查、驻场保障以及应急值守等，对重要系统进行安全保障，服务期内每年不低于20人/天。 7.提供安全培训：安全培训服务覆盖信息安全意识、信息安全技能、信息安全管理等多方面。主要为管理人员提供安全管理、安全意识培训，为安全技术人员提供安全技术、网络安全趋势培训。服务周期：每年提供不少于4课时培训内容。 | 年 | 3 |