天津市公安局视图库和视综平台建设项目需求书

**一、项目背景**

近年来，天津市公安局在全市大力推进视频监控网建设，现已在重点道路、路口路段以及重点部位等处建设了治安电子卡口、微卡口以及人脸抓拍卡口等前端感知设备，对过往车辆和人员照片进行实时获取、解析并开展相应的技战法应用。同时，在公安信息网内建设有图像侦查应用平台，汇聚全市两抢、盗窃非机动车以及入室盗窃等案件的视频图像数据，开展案件串并、分析研判等工作。由于上述系统分属不同厂商承建，各系统之间相互独立、自成体系，各类数据标准不统一，难以实现数据上的互联互通，在一定程度上制约了视频图像资源应用效能的充分发挥。

鉴于上述背景并结合天津公安实际，按照公安部相关要求和标准规范，我总队拟开展视图库和视综平台建设项目，整合汇聚全市车辆和人脸抓拍数据资源，开展数据清洗治理，建设视频图像信息数据库，并在公安信息网内实现与部级库对接，为公安部大数据平台、我局相关业务警种及相关应用平台提供视频图像数据支撑；建设视频图像信息综合应用平台，关联公安业务数据，开发符合本地实战需求的智能应用模型，为公安实战和各类安保维稳提供强有力的视频图像服务支撑。

**二、商务需求**

★1.该项目整体建设周期须不超过60天，起始时间按签订合同日期开始计算。

2.该项目整体运维期为3年，起始时间按项目通过专家验收日期开始计算。

★3.项目运维期内，在硬件条件满足的情况下，投标供应商须无偿进行视图资源的接入和处理；针对采购人提出的应用需求，须无偿进行定制开发；针对软件算法和平台功能的更新，须无偿进行升级。

★4.项目运维期内，第1年,投标供应商须派驻至少10名研发及运维工程师驻场，根据用户实战应用需求进行功能优化，同时保证系统稳定性。第2年和第3年，投标供应商须派驻至少5名运维工程师驻场，负责现场的维护工作，出现故障保证在半小时内完成修复。驻场工程师工作时间按照采购人要求执行，如遇重大节日安保任务时，驻场工程师须按照采购人要求进行维护值守；涉及到项目开发需派专业开发人员在24小时内响应，48小时到达现场。

5.该项目一年的故障总时长不得超过12小时。

6.技术需求书中第1项“视频图像信息数据库”--“功能要求”--“2.应用功能”--“2）注册保活：支持视图库-注册、注销、校时、保活等视图库上下联功能；支持分析系统-注册、注销、校时、保活等分析系统与视图库互联功能；支持应用平台-注册、注销、校时、保活等应用平台与视图库互联功能。”——须提供国家权威机构出具的检测报告。

7. 技术需求书中第1项“视频图像信息数据库”，投标供应商须具有在全国其他省、直辖市公安机关建设的“省级视频图像信息数据库”，并与“公安部视频图像信息数据库”对接的成功案例——须提供由省级公安机关出具的用户报告并加盖用户公章。

8. 技术需求书中第1项“视频图像信息数据库”和第3项“视频图像信息综合应用平台” ——须提供该产品对应的计算机软件著作权登记证书。

9.技术需求书中第3项“视频图像信息综合应用平台”--“功能要求”-- “2.应用功能”—“4）综合分析：包括同行人分析、人员落脚点分析、频繁过人分析、车辆轨迹分析、车辆落脚点分析、频繁过车分析、昼伏夜出分析、区域碰撞分析以及与公安业务数据关联应用的技战法等” ——须提供国家权威机构出具的检测报告。

10. 技术需求书中第3项“视频图像信息综合应用平台”--“功能要求”-- “2.基础应用功能” —“10）支持查看资源消耗情况，可查看整体及分类型（活动目标、人脸、人体、车辆）的总资源路数、动态资源路数、剩余资源路数及剩余资源百分比数据。” --须提供国家权威机构出具的检测报告。

11. 技术需求书中第3项“视频图像信息综合应用平台”--“功能要求”-- “3. 视频结构化汇聚应用” —“6）暂存架支持列表显示选定文件夹内存档文件缩略图及图片信息，可按加入时间或采集时间排列，支持根据暂存架内文件的信息生成多个目标（人或车辆）的轨迹或单条多目标轨迹。” --须提供国家权威机构出具的检测报告。

12.技术需求书中第5项“服务器1” -- “11）当图片直存的数据库被破坏时，可进行恢复。” --须提供国家权威机构出具的检测报告。

13.技术需求书中第7项“服务器3” -- “8）支持《公安视频图像信息应用系统》中的GA/T 1400-2017协议；” ——须提供国家权威机构出具的检测报告。

14.技术需求书中第12项“（核心产品）结构化数据存储检索设备” -- “7）需支持人脸、人体、车辆等结构化数据、半结构化数据（特征值）混合接入、存储、应用。” ——须提供国家权威机构出具的检测报告。

15.技术需求书中第12项“（核心产品）结构化数据存储检索设备”--“12）单台设备支持不少于20亿数据的存储、查询检索，50个用户并发，查询检索效率不低于4.5亿条数据/s，以图搜图效率不低于2000万条模型/s。” ——须提供国家权威机构出具的检测报告。

16.技术需求书中第13项“视频图像结构化设备” -- “2）支持算法资源管理，包括支持根据需求进行硬件计算资源预分配，达到任务秒级处理，支持对突发的任务进行计算资源动态分配，算法资源动态管理，支持通过界面展示查看每种算法已使用/预分配的总资源。” --须提供国家权威机构出具的检测报告。

17.技术需求书中第17项“木马检测系统”--须具备“公安部颁发的《计算机信息系统安全专用产品销售许可证》，系统软件应具备国家版权局颁发的《计算机软件著作权登记证书》”——须提供加盖厂商公章的相关证明材料。

18.技术需求书中第22项“日志审计”--须具备“数据传输安全性资质要求：传输安全网关服务端和客户端设备经国家密码管理局检测，具备国家密码管理局颁发的商用密码型号证书”——须提供加盖厂商公章的相关证明材料。

19.该项目建设完成后，边界安全内容须按照公安部《公安信息网边界接入平台安全规范》的要求通过专业测评机构测评。

**三、技术需求**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 采购项名称 | 数量 | 技术要求 |
| 1 | 视频图像信息数据库 | 2套 | 1. 第1套部署在视频专网内，按照GA/T 1400-2017标准汇聚、清洗、存储全市视频监控网内产生的车辆、人脸视图解析数据，通过边界接入平台向部署在公安信息网内的视频图像信息数据库共享数据。其中，车辆数据为车辆原始URL地址、结构化描述信息和特征值信息等视图解析数据，人脸数据为人脸小图、大图原始URL地址、结构化描述信息和特征值信息等视图解析数据。按照每天1000万张人脸抓拍数据、1.2亿张车辆抓拍数据，存储时长不少于90天进行设计。 2. 另1套部署在公安信息网内，除通过边界接入平台接收视频监控网的视图解析数据外，还需汇聚、清洗、存储图侦应用平台中的涉案视频图像，解析生成符合GA/T 1400-2017标准的涉案视图解析数据。目前，图侦应用平台中已有7万余起“两抢”、“盗窃电动车”案件信息，包含6.7万段涉案视频片段和13.4万张涉案图片，共计约20TB；为满足3年内所有案事件视图数据存储，需配置不小于100TB存储空间； 案事件视图数据需长期存储。   **功能要求：**  **1.接口功能**  1）视图库支持接口功能，包括采集接口、数据服务接口、级联接口。  2）视图库接口协议应符合GA/T 1400.4-2017中的规定。  3）消息头中的conent-type头字段应设为application/VIID+JSON。  4）应提供接口权限配置管理能力；应能实现对各接口的权限控制，保证库内数据的安全。  **2.应用功能**  应用功能包括注册保活、对象CRUD操作、布控与告警、订阅与通知和联网服务等功能。  1）需支持基于GA/T 1400-2017标准的采集、级联接口管理，提供统一的ETL工具，将以人脸、车辆为主的视图数据汇聚接入公安视频图像信息数据库。  2）注册保活：支持视图库-注册、注销、校时、保活等视图库上下联功能；支持分析系统-注册、注销、校时、保活等分析系统与视图库互联功能；支持应用平台-注册、注销、校时、保活等应用平台与视图库互联功能。  3）对象CRUD操作：支持视图库对象CRUD操作，包括对象读取操作，采集设备与采集系统对象的CUD操作，视频卡口和车道对象的创建、更新、删除操作，视频图像信息对象的CUD操作，视频案事件对象的CUD操作，视频图像分析规则的CUD操作。  4）布控与告警：支持视图库布控与告警功能，支持布控、撤控、修改布控范围和布控时间，支持基于图像对人员、车辆、物品等进行布控；  支持接收布控指令，当发现与布控特征属性相符合的目标对象时应发送告警信息给到布控方；支持基于对象特征属性及其组合进行精确布控和模糊布控；支持本级和跨级布控，实现跨级的人脸、车辆布控，及报警信息的接收；需提供人脸、车辆维度的布控功能，并对布控结果进行实时告警反馈。  5）订阅与通知：支持订阅、取消订阅和修改订阅时间；支持订阅视频案事件对象目录、视频案事件对象、卡口目录、车道目录、采集设备和采集系统的目录及状态、自动采集的视频图像对象信息，并能实现自动同步。  6）联网服务：支持多个下级视图库的联网接入，支持联网接入多个上级视图库，可基于用户权限对上级各视图库提供差异化服务；支持通过逐级订阅下级联网服务对象，下级视图库的卡口、车道、采集设备和采集目录等信息，构建视图库联网拓扑架构；支持同级视频专网视图库和同级公安网视图库的互联。  7）查询功能：支持库内数据的本级和分布式查询，实现跨级的人脸、车辆、人体的属性查询和以图搜图；需提供基于属性字段的条件查询能力；提供以图片内容为对象的目标检索能力。  **3.管理功能**  管理功能包括存储管理、用户管理、设备管理、运维管理、日志管理和时钟同步等功能。  1）存储管理：应支持设置视频图像信息对象的存储时间及周期；支持存储容量的平滑扩展；支持配置数据的导入和导出；支持业务数据的备份和恢复。  2）用户管理：应支持用户注册及身份认证；支持用户访问控制及授权策略。  3）设备管理：应符合GA/T 1400.3-2017中的有关规定。  4）运维管理：应符合GA/T669.7-2008及其他相关国家标准、行业标准的要求，提供视图库运维管理功能；支持数据的出入库统计，针对每条订阅，支持记录各下级不符合标准的数据量。需可提供丰富的、个性化的数据统计呈现能力，提供对数据级联、数据汇聚、数据治理、数据服务等的管理功能。  5）日志管理：支持记录系统运行日志和操作日志，运行日志包括视图库服务模块的启动、停止，系统用户的注册、注销、对象删除操作等信息，且运行日志和操作日志存储时间均不少于6个月。  6）时钟同步：应支持基于NTP/SNTP协议与NTP时钟源同步。  7）其余功能应符合GA/T 1400.3-2017中的有关规定。  **4.性能要求：**  1.并发性能  1）并发接收图像对象的速度不小于212张/s。  2）并发接入系统用户数不少于25个。  3）视图库管理的视频图像信息对象不少于234个。  4）视图库管理的视频分析规则对象不少于217个。  5）视图库管理的视频案事件对象不少于217个。  6）视图库支持的并发处于布控状态的布控对象或订阅状态的订阅对象不少于220个。  2.存储对象格式  1）支持存储、管理JPEG、JREG2000、BMP、PNG、TIF格式的图像资源。  2）支持存储管理SVAC、H.264、H.265、MJPEG-4、MJPEG-2、MJPEG格式的视频资源，可兼容CIF、2CIF、4CIF、D1、720P、1080P、4k或以上视频分辨率，视频文件格式应支持.ps、.avi、.ts、.mp4。  3）支持存储管理SVAC、G.711a、G.711u、G.723、G.729格式的音频资源。  3.检索性能  视图库的简单条件查询应在5s内完成，模糊查询和复杂条件组合查询应在7s内完成。  4.其余性能应符合GA/T 1400.3-2017中的有关规定。 |
| 2 | 视频图像信息数据库可视化软件 | 1套 | 1）应支持从结构化数据存储检索设备中进行人员、车辆等数据进行抽取，结合可视化组件，包括图表、柱状图、饼状图、地区分布趋势等，进行数据可视化展示。  2）应支持从视频图像信息综合应用平台数据库中抽取配置数据、日志信息、操作记录等，进行平台操作运维的可视化展示。  3）应支持对接视图库业务系统，有机集成了多种数据缓存服务。  4）应支持多种类型数据库对接能力，保证可视化系统与相关的业务系统的有效对接及可视化展示，包括但不限于SQL Server、Oracle、MySQL、PostgreSQL、Hadoop等主流的数据库。  5）应支持强大的可视化平台和组件库，可用于构建多种专业的数据可视化系统，以适应不同场景的用途。 6）应支持集群式运行，提供优异的可视化渲染输出性能以及平稳的系统运行效果。 7）应支持结合地图数据&地图服务软件，提供可视化地图展示。  8）地图应至少支持天津市0-19级的显示级别。  9）实现海量批处理和高速流处理，为用户决策判断提供全面的数据支持。  10）需支持可视化的视觉聚焦点，并实现多屏选型设计，提供精彩的视觉体验。 11）地图应支持要素数据服务，应至少包括各级道路、公共设施、城市建筑、行政区划、海洋边界、警务人员、警务车辆、摄像头等要素数据，从而用二、三维方式模拟城市的真实建设环境。  12）支持采集数据的关联分析以及数据二次加工能力的定制开发。  13）提供辅助数据分析工具，包括体系化、专业化的分析算法模块及辅助数据模型，可针对现有数据，进行时间/空间/层级结构等多维度分析。 |
| 3 | 视频图像信息综合应用平台 | 2套 | 分别部署在视频专网和公安信息网内。  **功能要求：**  视频图像信息综合应用平台主要包括接入、基础应用、视频结构化汇聚应用和管理等功能模块。  1.接入功能  1）支持GB/T 28181-2016协议，支持与共享平台进行对接。  2）支持通过GA/T 1400-2017中规定的数据服务接口进行视图库的接入。  3）支持基于硬盘物理数据接口、USB接口等多种通用接口，接入离线视频图像信息采集设备。  4）支持接入统一的认证与鉴权系统。  5）应支持按照相关标准的规定接入PGIS服务系统，实现与警综平台等系统的连接。  2.基础应用功能  1）视频监控基本应用：应符合GA/T 669.7-2008中的规定，具有视频浏览、录像下载/回放、云镜控制等视频监控基本应用功能。  2）查询检索：支持基于视频图像信息对象特征属性，进行关键字模糊检索、对象属性组合的查询与检索；支持基于车牌号码、车型、过车时间、过车位置等机动车特征属性及其组合的查询与分析，如车辆号牌的模糊与精确查询，车辆轨迹分析、时空碰撞分析等。  3）综合分析：包括同行人分析、人员落脚点分析、频繁过人分析、车辆轨迹分析、车辆落脚点分析、频繁过车分析、昼伏夜出分析、区域碰撞分析以及与公安业务数据关联应用的技战法等；  4）布控告警：支持对特定移动目标对象的特征属性（如车牌号码、车型、车身颜色等）及其组合通过视图库进行本级或跨级在线布控，具备布控设置、接收告警、布控撤除等功能。  5）视频图像案事件管理：支持对视频按时间段创建、更新及删除；支持对不同视频图像信息对象的特征属性进行标注；支持自动获取警综平台、执法办案系统等系统中的相关案事件目录信息，并完整地导入案件的编号、分类、时间、地点、简要案情等信息；支持视频案事件分析报告的自动生成和打印输出；应能根据视频案事件类型、作案手段工具、犯罪嫌疑人特征等关键属性对视频案事件进行串并分析；应支持对视频案事件对象特征属性进行查询和检索；应能根据视频案事件类型、处理阶段、所属区域、时间范围等不同特征进行统计分析，并生成统计报表。  6）需提供地图应用模块，实现视图数据的时空关系分析和可视化应用，对关注人员、关注车辆的轨迹分析类功能须结合城市路网数据在地图上客观还原展现行进路线。 7）需提供丰富的应用终端，包括PC端的BS和CS客户端以及移动客户端，以具备可扩展性的框架提供实用的视频应用工具，满足公安用户日常视频警务应用。  8）应提供与其他公安业务数据结合，构建各类应用模型、可视化的智能建模工具。  9）支持对视频解析任务类型（活动目标、人脸、人体、车辆）、优先级、加速比、分析时间段以及所属分组进行设置，且支持查看资源消耗情况。  10）支持查看资源消耗情况，可查看整体及分类型（活动目标、人脸、人体、车辆）的总资源路数、动态资源路数、剩余资源路数及剩余资源百分比数据。  3.视频结构化汇聚应用功能，此功能在视频专网内实现。  1）按照GA/T 1400-2017中规定的数据属性、字段、应用等规范要求，制定标准数据及应用服务接口，将该平台与我市各分局建设的视频结构化系统进行数据和应用服务对接，在数据层面进行标准化统一，形成全市范围内各分局视频结构化信息数据能够可识、可看、可用。同时将市局平台作为全市视频结构化数据应用功能的发起点，建立跨区应用模型，针对各分局的视频结构化数据、视频结构化系统功能，进行全市范围内数据应用。  2）全市范围内跨区域活动目标检索：支持按照时间段、监控点（支持树形选点和地图选）、目标属性等条件进行活动目标（人、车）精确或模糊检索。其中，人的属性应至少包含性别、是否戴眼镜、是否戴帽子、上衣类型、下装类型、是否戴口罩、发型、是否背包、是否拎东西、是否骑车、年龄段等；车的属性应至少包含车辆号牌、车辆品牌、车辆颜色、车牌类型、是否黄标车、是否打电话、是否打开遮阳板、是否悬挂危险品标志、是否系安全带等。由该平台设置检索目标信息，向相应分局视频结构化系统发起指令，并将检索信息返回至该平台进行展现。  3）全市范围内跨区域目标以图搜图：支持按照时间段、监控点（支持树形选点和地图选）等条件进行活动目标（人、车）以图搜图，由该平台上传单张或者多张图片，向相应分局视频结构化系统发起指令，并将比对结果返回至该平台进行展现。  4）支持从搜索结果中选择图片进行以图搜图，或将搜索结果中的图片添加到多图搜索。  5）支持暂存架功能，支持将搜索结果中的图片添加到暂存架，对暂存架可通过设置文件夹进行分组，可以同时暂存多个分组的目标图片，并进行暂存架的相应操作应用。  6）暂存架支持列表显示选定文件夹内存档文件缩略图及图片信息，可按加入时间或采集时间排列，支持根据暂存架内文件的信息生成多个目标（人或车辆）的轨迹或单条多目标轨迹。  7）全市范围内跨区域目标布控预警：支持按照布控时间段、监控点（支持树形选点和地图选）等条件进行活动目标（人、车）布控，布控需支持按目标属性布控和目标图片布控，由该平台上传布控目标，向相应分局视频结构化系统发起指令，并将预警信息返回至该平台进行展现。  8）可以对视频结构化的建设成效-数据总量、每日数据量、其他数据分析、近30天每天监控点数据量等进行展示。  9）权限和日志管理：支持对系统内用户权限分配及应用授权管理。支持对系统操作、配置相关动作的日志进行查询；支持按用户名、用户IP、系统平台类型、操作模块、用户所属部门，当天、本周、本月或者人工选择的时间段进行查询和导出。  4.管理功能  1）支持进行平台用户管理，进行用户注册及身份认证，用户访问控制，角色管理，用户授权策略等。  2）需提供运维管理，运维管理：应符合GA/T669.7-2008及其他相关国家标准、行业标准的要求，提供视综平台运维管理功能。  3）需可实现算法的调度管理，支持算法的手动或按任务切换。  4）日志应包括运行日志和操作日志，存储时间不少于6个月。  **性能要求：**  1）支持用户数不少于10万，并发用户数不少于10000，支持集群和平滑扩容等高可用特性。  2）支持管理不低于2000部门，3万角色，2万个组织树。  3）图像编码格式应支持JPEG、JPEG2000、BMP、TIF等格式。  4）视频编码格式应用SVAC、H.265、H.264、MEPG-4、MEPG-2、MJPEG等格式。  5）消息接收端与发送端之间的文本信息延迟不大于2s的条件下，视频图像信息对象特征属性及其组合的简单查询检索应在5s内完成，模糊查询检索应在7s内完成。  6）支持不低于500个以图搜图任务并行下发，以图搜图效率不低于每秒3亿条模型，需支持人脸以图搜图时间段不少于30天，车辆以图搜图不少于15天。  7）支持不少于1000张图片/秒的并发调用及下发性能。 |
| 4 | 硬件设备 | 1项 | 投标供应商需按照条款1-3的全部需求进行测算，提供不少于需求条款5-16所列硬件设备，同时须承诺若在实施过程中，若不满足条款1-3的需求须另加硬件设备，由中标供应商自行承担费用。 |
| 5 | 服务器1 | 2台 | 用于图片存储。  1）设备应配置≥两颗64位多核处理器；  2）内存配置≥8GB内存，内存支持扩展到≥256GB； 3）设备应标配≥4个千兆网口，可增扩≥2个万兆口或≥4个光纤接口，可增扩2个SSD固态硬盘； 4）可接入硬盘≥24块3.5英寸SATA/SAS硬盘；  5）应支持FCSAN、IPSAN、NAS存储功能 6）一个控制器内支持双系统，当主系统异常时，能从备系统启动。  7）支持RAID0、RAID1、RAID2、RAID3、RAID4、RAID5、RAID10、RAID50、JBOD等。  8）支持对视音频、图片进行混合直存。支持不低于600MBps图片并发输入，同时不低于600MBps图片并发输出。  9）内置管理软件，支持平台服务宕机时，不影响存储业务。  10）支持存储空间虚拟化管理，可根据用户业务分配通用、文件、视频、图片等类型存储空间；  11）当图片直存的数据库被破坏时，可进行恢复。  12）具备当设备发生磁盘、网络、电源、RAID、温度超限、风扇等故障时，发出声光指示的功能。 |
| 6 | 服务器2 | 32台 | 1）2U双路标准机架式服务器  2）CPU配置应不低于2颗Xeon® Silver 4114×2或同等性能处理器；  3）内存配置应不低于64GB，支持16根内存插槽，最大支持扩展至2TB内存 4）硬盘配置应不低于2块600GB 10K 2.5寸 SAS硬盘，最高可支持12块3.5寸（兼容2.5寸）热插拔SAS/SATA硬盘 5）支持SAS\_HBA卡，支持RAID 0/1/10 6）支持PCIE扩展：最大可支持6个PCIE扩展插槽 7）网口配置应不低于2个千兆电口 8）其他接口应不少于1个RJ45管理接口，4个USB 3.0接口，1个VGA接口 |
| 7 | 服务器3 | 1台 | 用于案事件视图数据存储。  1）设备应配置≥两颗64位多核处理器；  2）内存配置≥8GB内存，内存支持扩展到≥256GB； 3）设备应标配≥4个千兆网口，可增扩≥2个万兆口或≥4个光纤接口，可增扩2个SSD固态硬盘； 4）可接入硬盘≥24块3.5英寸SATA/SAS硬盘；  5）应支持FCSAN、IPSAN、NAS存储功能 6）一个控制器内支持双系统，当主系统异常时，能从备系统启动。  7）支持RAID0、RAID1、RAID2、RAID3、RAID4、RAID5、RAID10、RAID50、JBOD等。 8）支持 《公安视频图像信息应用系统》中的GA/T 1400-2017协议；  9）支持按毫秒级自定义时间段进行视频精准检索、回放、下载，回放支持豪秒级定位回放、关键帧回放、回放暂停、倍速快放、慢放等； 10）支持视图转换，能将指定时间段视频按时间间隔抽帧转换成图片。 |
| 8 | 服务器4 | 7台 | 1）2U双路标准机架式服务器  2）CPU配置应不低于2颗Xeon® Silver 4114或同等性能处理器（10核，2.2GHz） 3）内存配置应不低于256GB，支持16根内存插槽，最大支持扩展至2TB内存 4）硬盘配置应不低于2块600GB 10K 2.5寸 SAS硬盘，4块960G SSD硬盘,8块 6T 7.2K 3.5 寸 SATA硬盘。最高可支持12块前置3.5寸（兼容2.5寸）热插拔SAS/SATA硬盘，可选支持4块后置2.5寸热插拔硬盘。 5）支持RAID\_4G卡，支持RAID 0/1/10/5/50/6/60,4G缓存 6）支持PCIE扩展：最大可支持6个PCIE扩展插槽 7）网口配置应不低于2个千兆电口，2个万兆光口 8）其他接口应不少于1个RJ45管理接口，4个USB 3.0接口，1个VGA接口 |
| 9 | 服务器5 | 30台 | 1）2U双路标准机架式服务器 2）CPU配置应不低于2颗Xeon® Silver 4114或同等性能处理器（10核，2.1GHz） 3）内存配置应不低于32GB，支持16根内存插槽，最大支持扩展至2TB内存 4）硬盘配置应不低于2块600GB 10K 2.5寸 SAS硬盘，最高可支持12块3.5寸（兼容2.5寸）热插拔SAS/SATA硬盘 5）支持SAS\_HBA卡，支持RAID 0/1/10 6）支持PCIE扩展：最大可支持6个PCIE扩展插槽 7）网口配置应不低于2个千兆电口 8）其他接口应不少于1个RJ45管理接口，4个USB 3.0接口，1个VGA接口 |
| 10 | 服务器6 | 1台 | 1）2U双路标准机架式服务器 2）CPU配置应不低于2颗Intel Xeon E5-2640v4或同等性能处理器（10核，2.1GHz） 3）内存配置应不低于32GB，支持16根内存插槽，最大支持扩展至2TB内存 4）硬盘配置应不低于3块1TB 3.5吋7.2K 12Gb SAS热拔插硬盘，最高可支持12块3.5寸（兼容2.5寸）热插拔SAS/SATA硬盘 5）支持2GB Cache、12Gb RAID卡，支持RAID0/1/5/6/10/50 6）支持PCIE扩展：最大可支持6个PCIE扩展插槽 7）网口配置应不低于2个千兆电口 8）其他接口应不少于1个RJ45管理接口，4个USB 3.0接口，1个VGA接口 |
| 11 | 硬盘 | 72块 | 硬盘尺寸3.5英寸；空间不小于6000G；转速不小于7200RPM。 |
| 12 | ▲结构化数据存储检索设备 | 17台 | 1）CPU不小于2颗64位多核处理器； 2）内存不小于512G； 3）硬盘配置应不小于：960G SSD×2和4T 7.2K SATA×6； 4）网卡支持不小于10GbE×2/1GbE×2。  5）需基于Hadoop构架，提供存储、资源管理、批处理、流计算、全文检索等基础组件环境。  6）基础组件环境需可与数据层软件实现解耦；  7）需支持人脸、人体、车辆等结构化数据、半结构化数据（特征值）混合接入、存储、应用。  8）应支持对人脸/车辆进行条件秒级查询,简单条件查询应在5s内完成，模糊查询和复杂条件组合查询应在7s内完成。 9）应支持通过单个或多个模型数据进行相似度的匹配检索； 10）应支持轨迹信息统计；  11）应支持基于目标特征数据进行区域内数据碰撞检索；  12）单台设备支持不少于20亿数据的存储、查询检索，50个用户并发，查询检索效率不低于4.5亿条数据/s，以图搜图效率不低于2000万条模型/s。 13）应支持集群线性扩容，实现存储与性能弹性扩展； 14）应支持数据保存多个副本，并提供容错机制，实现副本丢失自动恢复  15）支持自动生成并展示布控库数据统计、 非布控库数据统计、抓拍详情数据分析和预警详情数据分析四类图表。  16）应支持通过BMC管理口，可获取取硬件模块的工作状态信息，包括模块温度、风扇转速、电源状态、硬盘状态、内存、CPU、网络带宽、空间使用情况和机箱的温度等；  17）应支持1+1冗余电源模式，电源支持热插拔，不影响系统应用；支持电源+BBU模式，当断电时，自动切换内置BBU支持服务器继续运行，同时BBU能发送断电信号，服务器内置的大数据服务根据此信号自动关闭，保证数据正常落盘不会丢失；  18）支持集群线性扩展数据存储容量和系统计算能力；支持在正常提供服务的情况下对集群进行扩容，即增加集群服务器数量。当集群中任意节点发生故障时，集群可保持正常工作且数据不会丢失；支持动态扩容。 |
| 13 | 视频图像结构化设备 | 7台 | 硬件性能参数：  1）处理器配置应不低于2颗E5-2680V4 CPU（14核2.4Ghz）； 2）需配置不低于8张GPU卡，单张GPU卡性能：单精度浮点运算能力不低于5.5TeraFLOPS，整数运算能力不低于22TOPS，显存不低于8GB，显存带宽不低于192GB/秒； 3）内存应不低于192GB DDR4； 4）硬盘应配置不小于1个480GB SSD； 5）应支持不小于16块2.5英寸硬盘或SSD，支持热插拔。  功能参数：   1. 需部署人脸检测算法、人脸结构化解析算法、车辆结构化解析算法。   2）支持算法资源管理，包括支持根据需求进行硬件计算资源预分配，达到任务秒级处理，支持对突发的任务进行计算资源动态分配，算法资源动态管理，支持通过界面展示查看每种算法已使用/预分配的总资源。  3）人脸结构化解析算法须按照GA/T 1400-2017协议进行结构化解析，人脸结构化属性最少需包括：年龄段、性别、是否微笑、戴眼镜、戴口罩；支持一个画面中两眼瞳距18像素点以上的32张人脸同时进行检测。  4）车辆结构化分析算法须按照GA/T 1400-2017协议进行结构化解析，车辆结构化属性最少需包括车牌号码、车牌类型、车牌颜色、车牌状态、车辆颜色、是否临牌车、车辆正背向、车辆类型、车辆主/子品牌、主/副驾驶安全带、主/副驾驶遮阳板、打手机、危险品车、渣土车、渣土车是否未盖板、黄标车、三轮车是否有棚、挂件、天窗站人、行李架、备胎、是否有天窗、车身喷字、纸巾盒、摆件、贴标、卡片、副驾驶是否无人/是否怀抱婴儿等。  5）单台设备图片分析（检测、结构化、建模、比对）不低于1200张/秒。  6）支持对图片中的正向车辆进行以图搜图建模功能，支持对图片中的背向车辆进行以图搜图建模功能； 7）应支持使用视频中的人员截图或目标人员照片在监控视频中抓拍形成的图像库中搜索相似人员，得到相似度并排序；  8）应支持跨硬件平台，兼容物理服务器、虚拟机、Docker等多种资源平台；  9）应支持良好的开放性，支持通过协议将服务开放给第三方。  10）应支持多个设备智能分析单元通过级联方式形成集群系统；  11）应支持对设备进行在线升级，支持对集群系统内所有视频图像结构化设备进行一键升级。 |
| 14 | 交换机1 | 5台 | 1）机架式全网管三层交换机； 2）不小于48个千兆电口，4个万兆SFP+光口； 3）不小于1个业务扩展槽，2个电源模块槽位，2个风扇模块槽位； 4）交换容量不小于598Gbps； 5）包转发率不小于252Mpps； 6）支持交直流供电； 7）需支持支持RIP/OSPF/BGP/IS-IS/VRRP，IPv6，VLAN，流量控制，ACL，QoS，端口镜像，环网RRPP/ERPS； 8）需支持SNMP V1/V2c/V3网管。 |
| 15 | 交换机2 | 1台 | 1）支持不少于24个10/100/1000Base-T以太网端口，4个100/1000 SFP，4个万兆SFP+，2个QSFP+堆叠口；  2）交流供电，电源前置，支持RPS冗余电源；  3）交换容量不小于598Gbps/5.98Tbps；  4）包转发率不小于222Mpps。 |
| 16 | 万兆光模块 | 32个 | 1）SFP光模块；  2）多模万兆双纤双向；  3）TX850nm/10G,RX850nm/10G,LC；  4）距离不小于300m。 |
| 17 | 木马检测系统 | 1套 | 1）总体要求：分布式网络全流量采集与威胁检测软硬一体化终端，支持针对全网数据流量进行恶意代码与恶意行为检测，要求采取旁路部署，支持通过镜像端口方式进行全流量采集，具备策略配置、威胁检测、协议还原、文件解析、敏感信息检测和告警上报功能，包含三年木马文件检测特征库及僵尸主机特征库升级服务。  2）端口要求：2U机架式，配置至少包括2个扩展槽位，6个千兆电口，4个千兆光口，标配模块化双冗余电源。  3）性能要求：最大并发连接数不少于300万，最大流量数据吞吐能力不小于4Gbps。  4）策略配置功能要求：支持自定义威胁检测规则，支持导入及编辑规则文件；具备白名单管理功能，列入白名单的对象不进行检测。  5）威胁检测功能要求：支持本地实时发现与识别恶意程序、恶意域名、黑IP、黑网址、黑邮箱、Web攻击、特种木马、信息泄露，TCP劫持、WebShell攻击等威胁类型，具备高级持续性威胁（APT）监测能力；支持对外联控制端使用服务器IP、域名、特征码进行检测，能够通过单包、多包、单流、多流等多种技术手段相结合进行综合判定，一旦匹配特征库地址即可认定终端为受控主机，可以确认木马种类、受控机情况、木马外联信息等；  6）支持通过自动学习网络流量中包含的各种可疑C&C IP/URL进行木马回连检测，快速识别网络中存在的恶意回连行为，包含回连主机IP、服务器IP、时间、行为等。  7）协议还原功能要求：要求能够识别http、https、ftp、smtp、pop3、DNS、IMAP、IP会话等主流协议报文并进行数据重组还原；支持对网络数据流中的HTTP协议进行多方向、多维度的关联判定，用以确认受控服务器及控制端背景信息；对于网络数据流中的远程访问控制类协议进行解析，结合行为规则，进行中转机判定。  8）文件解析功能要求：支持doc, xls, ppt, swf, pdf, java, rar, zip, rar, exe, vbs, scr, html等多种文件解析，提供沙箱支持对常见文件的病毒检测。  9）敏感信息检测功能要求；支持用户输入关心的敏感关键字词，对浏览网页、查看邮件内容及附件、文档中存在的敏感关键字词进行报警，支持用户自定义相关敏感信息权值、网址及途径。  10）告警上报功能要求：支持通过syslog方式向日志审计系统上报木马检测系统发现的安全威胁告警事件。  11）系统管理功能要求：支持本地SSH和Web管理界面，具备远程配置、状态监控及性能告警等管理功能。 |
| 18 | WAF | 2套 | 1）总体要求：提供针对各类WEB应用攻击的检测和防护能力，能够对HTTP/HTTPS协议进行深入解析，实时监测往返流量，支持透明、代理模式、旁路部署、单臂部署、策略路由部署方式，支持链路绑定，上线设备能够自动探测获取Web应用系统IP和端口，  2）具备协议配置、蜜罐监测、合规检测、应用管控、区域管控和终端管控功能，含三年特征库升级服务。  3）端口要求：标准机架式设备，包括2个扩展槽位，6个千兆电口，4个千兆光口，单电源。  4）性能要求：并发连接不少于120万。吞吐率数据不小于1Gbps。  5）协议配置功能要求：支持对Web相关应用协议进行自定义，并提供详细协议分析变量配置功能。  6）蜜罐监测功能要求：具蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断。  7）合规检测功能要求：具备业务合规检测功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截。  8）应用管控功能要求：具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置。具备网站一键关停功能，通过一键设置关停网站。  9）区域管控功能要求：具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响。  10）终端管控功能要求：具备客户端访问控制功能，预防恶意客户端进行访问频率的多层次恶意访问。  11）攻击取证功能要求：支持获取Web安全事件的原始攻击信息，支持NAT环境下的用户识别能力。  12）系统管理功能要求：支持本地SSH和Web管理界面，具备设备集中管理功能，可实现设备分布式部署、集中式监控管理。 |
| 19 | 大数据安全网关 | 1套 | 1）总体要求：提供针对大数据分析平台的访问控制能力，支持基于硬件的底层虚拟化技术，各个业务集群虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的CPU、内存、接口等资源，含三年特征库更新服务。  2）端口要求：标准机架式，配置4个万兆光口和4个千兆电口，双电源，不少于1个扩展插槽。  3）性能要求：设备吞吐量18G，并发连接数350万  4）访问控制策略：需支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略。支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每IP总连接数控制、每IP新建连接数控制。  5）行为控制要求：需支持基于DPI和DFI技术的应用特征识别及行为控制。  6）带宽管理：需支持基于线路和多层通道嵌套的带宽管理。  7）路由要求：需支持静态路由、动态路由（RIP、OSPF、BGP4）。支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。  8）负载均衡：需支持链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法。  9）链路检查要求：需支持通过ICMP、TCP、DNS和HTTP协议实现对链路可用性的多重健康检查。  10）NAT要求：需支持源NAT、目的NAT、静态NAT，支持一对一、一对多和多对多等形式的NAT。支持各种应用协议的NAT穿越：FTP、TFTP、H.323、SQL\*NET。  11）统计要求：应该提供基于流量的TOP100用户和TOP100应用的流量曲线图，流量曲线图的统计周期包括小时、天、7天和30天。提供基于并发会话数量的TOP100用户和TOP100应用的并发数量曲线图，并发数量曲线图的统计周期包括小时、天、7天和30天。 |
| 20 | 堡垒主机 | 1套 | 1）面向内部技术人员运维操作监控与审计的软硬一体化机架式设备，具备主机管理、权限控制、运维审计、账号认证等功能。  2）端口要求：标准机架式设备，至少包括4个千兆电口。1个扩展插槽，1T硬盘，可扩展万兆接口模块。配置不小于100个主机/设备许可。  3）数据库命令审计：需实现数据库命令级审计，支持的数据库类型包括：Oracle（支持ORACLE RAC）、SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、teradata，不需采用数据镜像方式实现，以免增加部署的复杂性和网络负担。  4）运维管理功能要求：需要支持RDP、VNC图形操作行为的审计，图形回放形式还原真实操作过程。需要支持RDP、VNC图形操作过程中键盘输入操作记录和鼠标点击行为记录，并支持开启或关闭键盘输入审计功能。RDP协议需要支持windows服务端开启安全层SSL加密，加密级别符合FIPS标准，允许运行使用网络级别身份验证的远程桌面的计算机连接，以满足运维过程安全性的更高要求。需要支持web页面防跳转功能，进行http/https访问过程中，运维人员仅允许访问授权地址。需要支持会话协议回放空闲时间过滤，应用发布图像操作回放支持操作空闲过滤（可设置无操作多长时间开始过滤）。  5）账户管理功能：需要支持通过账号核查报表统计幽灵账号、僵尸账号、孤儿账号，快速发现账号异常情况。需要支持幽灵账号报表，对资源账号进行统计分析，便于及时发现非法建立的资源账号。需要支持僵尸报表，统计周期内登录次数低于某一阀值的用户账号和资源账号。孤儿账号报表，能够统计未建立任何访问策略授权关系的用户账号和资源账号。  6）身份认证功能要求，具备双因素认证，支持对不同用户设置不同认证方式组合的双因素认证。需要支持用户属性中手机号码和邮箱地址作为主账号身份登录。能够限制用户同一时间只能从一个IP登录。需要支持用户忘记登录密码时，可通过邮件或短信方式获取验证码，验证通过后重置登录密码。  7)批命令执行：需要支持TELNET、SSH协议使用SecureCRT工具批量登录目标资源，并支持对多台主机批量执行操作指令。 |
| 21 | 漏洞扫描 | 1套 | 1）软硬一体化机架式设备，支持IPv4、IPv6双协议栈扫描，具备系统漏扫和Web漏扫能力，具备策略定义，任务调度和中断续扫功能，含三年特征库升级服务。  2）端口要求：1U机架式，至少包括1个可插拨的扩展槽和4个千兆电口。  3）性能要求：任务不限制IP数量，能够并发扫描不少于40个IP地址，漏洞扫描方法应不少于45000种。  4）漏洞扫描能力要求：支持多种协议口令猜测，包括SMB、Snmp、IMAP、Rlogin、RDP、Sybase、Tomcat、Telnet、Pop3、SSH、Ftp、RDP、SQL Server、DB2、MySQL、Oracle、WebLogic、WebCAM等。允许外挂用户字典配置文件；支持对主流数据库的识别与扫描，包括：Oracle、Sybase、SQL Server、DB2、MySQL等；支持云平台扫描，漏洞覆盖OpenStack 、KVM、Vmware、Xen等主流的云计算平台；支持phpmyadmin、WordPress 等开源架构系统扫描，支持python的多个模块的漏洞扫描，如audioop模块 、rgbimg模块的漏洞；支持扫描IPv6环境中的设备及系统。  5）策略定义功能要求：需要支持灵活的扫描策略自定义功能，提供策略编辑向导和详细漏洞信息，支持以系统类型、漏洞类型、危险级别、CVE等不同视图显示漏洞，支持策略的导入、导出、修改以及合并。支持对意外中断（网络中断、设备断电）的扫描任务恢复后继续进行扫描。  6）与第22项日志审计系统为不同品牌，支持实时事件数据报送。 |
| 22 | 日志审计 | 1套 | 1）授权方式：按照事件数据存储模块节点数量授权，本次配置1个节点4TB并发数据处理能力授权，无管理安全资产数量及日志源数量限制。  2）性能参数：单节点平均事件数据采集入库能力不少于20000EPS，集群版本峰值不低于50000EPS，10亿条事件存储规模下条件查询完成时间不超过2秒。  3）传输安全网关服务端功能要求：包含用于搭建分布式可信链路的标准机架式数据采集网关服务端1个，配置千兆电口不少于6个；严格遵循国家密码管理局相关规范，内置经国家密码管理局审批的硬件密码卡，密钥存储在密码卡安全存储区，而非本地文件系统；支持国产商用密码算法SM1\SM2\SM3\SM4，SM1/SM4会话密钥≥1024，双证书密钥对数量≥64，支持双WNG物理噪声源芯片保障随机数质量；支持国密密码套件，包括但不限于ECDHE\_SM1\_SM3、ECC\_SM1\_SM3、RSA\_SM1\_SM3、ECDHE\_SM4\_SM3、ECC\_SM4\_SM3、RSA\_SM4\_SM3；支持以标准PKCS10、PKCS7、自定义数字信封机制导入加密密钥，具备密钥分级管理和备份机制。  4）传输安全网关客户端功能要求：包含用于搭建分布式可信链路的标准机架式数据采集网关客户端端2个，配置千兆电口不少于2个；严格遵循国家密码管理局相关规范，内置经国家密码管理局审批的硬件密码卡，密钥存储在密码卡安全存储区，而非本地文件系统；具备终端认证、数据采集、日志转发和事件上报功能，兼容SYSLOG、SNMP、WMI等日志数据协议，支持按照国产商用密码算法SM1\SM2\SM3\SM4实现采集数据加密传输。  实时数据处理功能要求：具备基于分布式计算与存储架构的非结构化数据实时处理能力，支持流式数据实时导入，提供基于事件索引的相似度匹配、部分匹配及模糊匹配检索能力，提供非结构化数据关联关系建模，具备数据容量和处理性能弹性扩展能力，具备数据高可用性，提供基于B/S架构的数据管理配置功能，支持存储策略、分区策略、全文索引、任务分发、数据备份、数据恢复和性能监测，提供SQL兼容和Restful查询接口实现非结构化数据检索。  5）敏感数据存储功能要求：提供具备完全自主知识产权的安全数据库管理系统软件，用于资产信息、安全告警及安全配置等敏感数据存储管理。具备存储加密功能，实现对数据库表空间、用户表数据、索引数据及读写日志的底层存储加密。具备专用数据库管理客户端，提供数据查询加密传输功能，采用经认证的国标加密算法，对应用完全透明，支持ODBC、JDBC、ADO.NET 等主流开发接口，符合SQL92国际数据库规范的要求。  6）安全事件关联分析功能要求：采用分布式大数据计算架构，支持针对多维度海量安全事件数据规则建模和关联分析，支持快速部署和分布式弹性扩展，兼容高性能实时数据流计算引擎与离线数据批处理引擎。具备安全场景关联分析、关联规则的引用和嵌套、实时数据和历史数据的关联分析等功能，支持攻击链条阶段智能识别，支持威胁情报碰撞与溯源分析。需能够自定义增加、下发和导入关联分析规则。需具备可视化在线关联规则编辑器，能够对规则进行各种编辑和自定义。  7）异常行为智能分析功能要求：要求采用分布式大数据计算框架，支持针对未知安全威胁的海量事件数据行为建模和异常分析，支持快速部署和分布式弹性扩展，兼容高性能实时数据流计算引擎与离线数据批处理引擎。需具备数据过滤、行为建模、基线管理、事件分析、事件查询等功能；具备个体和群组对照两种模式，具备计数函数、唯一性计数函数、最大/最小函数、平均数函数、求和函数、稀有函数等建模方式，支持以部门、个人、资产、资产群等为单位建立多维度基线，支持动态的自学习的基线模型建立，能够自动识别工作日、休息日、节假日和其它类型模型；具备可视化行为模型编辑器，能够对模型进行各种编辑和自定义。  7）资产管理功能要求：能够将被管理资产按照多种维度进行分组、分域管理，并显示分组资产总数等信息。支持自定义资产标签，可以为每个标签指定一种颜色，对资产标签进行分组管理。  8）探针管理功能要求：支持对接入的网络安全态势集控探针运行状态和工作性能的统一管理，支持新建和维护集控探针基本信息，支持对集控探针CPU、内存、磁盘、系统负载、网络性能等运行状态和性能等进行监测及设置告警阈值。  9）事件范化功能要求：具备可视化日志范化编辑界面，实现对异构日志格式的统一化描述，范式化字段可根据审计需要灵活扩展，并可参与关联分析；范式化字段至少应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源MAC地址、源端口、操作、目的地址、目的MAC地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；支持渐进式日志范化，可根据分析需要对部分字段内容进一步进行内容提取具备日志范式化功能。  10）事件检索功能要求：可通过设置时间段、查询条件、特定字段集或关键字符进行检索查询，支持对查询结果进行自动刷新。需对查询到的结果通过列表字段自定义显示或趋势图显示，并能对趋势图进行拖放  11）告警管理功能要求：支持告警信息检索、告警规则设定、告警结果导出。应具备告警抑制功能，支持手动配置告警抑制规则的时间范围及合并数目，并支持抑制规则的实时启用和停用。  12）自定义报表功能要求：：支持按照天/月/季/年等时间周期生成报表，支持将自定义格式的统计报表生成综合安全报告。在报表中能够以柱状图、曲线图、饼状图方式统计。  13）安全报警情况，并支持报表及报告的自动派发。需支持报表报告的导出，导出的格式至少包括：PDF、HTML、图片、WORD、RTF、CSV等。  14）自定义仪表盘功能要求：支持配置界面的可视化管理，支持自定义监控组件对资产、事件、告警等进行多维度监控，可依据用户需求添加、修改和删除监控组件。  威胁情报管理功能要求：具备对多源异构的安全情报采集及威胁情报关联分析能力，在关联分析中能够将平台采集到的各种安全事件与威胁情报进行碰撞比对。  知识库管理功能要求：内置安全知识库至少包括事件库、案例库、应急预案库，同时具备安全知识的管理功能，允许用户在平台的使用过程中对知识库进行不断丰富和完善。  15）系统管理功能要求：具备系统管理员、安全操作管理员和审计管理员三类管理员和相应用户，并支持管理员创建用户和角色。支持安全操作管理员为用户赋予相应权限角色。同时，平台需对角色可以访问的资源进行细粒度的权限划分。  16）系统集成要求：与第18项WAF、第19项大数据安全网关、第23项安全数据交换系统为不同品牌，并且确保系统的兼容性。 |
| 23 | 安全数据交换系统 | 1套 | 设备参数：  1.标准2U机架式设备；由非信任端服务器和信任端服务器两台设备组成，部署于安全隔离网闸前后，用于数据安全交换；  2.单台设备提供不少于4个10/100/1000Mbps（电口），2个万兆多模光纤接口（含同等数量的光模块）；  3.采用基于Linux内核的安全加固多核并行操作系统，保证设备系统安全；  4.应用吞吐量≥1.6Gbps；  5.数据库交换并发表≥4096；  6.最大数据文件≥40G；  7.无故障运行时间>50000小时；  设备功能：  1.支持ORACLE、SQLSERVER、DB2、SYBASE、MYSQL等主流数据库的同步，可实现异构数据库同步，对数据库所在操作系统无任何要求；  2.数据库支持多种同步方式：触发器方式，全表采集方式，同表双向的数据同步，删除源数据方式；  3.支持断点续传功能，在出现断电或传输中断等情况下，能够保证系统恢复时，交换的数据能重传或续传且不出数据丢失现象；  4.符合《信息安全等级保护制度》三级要求，支持系统管理员、审计管理员、安全管理员的三权分立管理模式；  5.系统提供高级任务调度功能，包括：任务带宽调度，任务执行周期/频率调度，任务优先级调度等，为重要业务应用的可靠执行提供技术手段支持；  6.系统可根据时间、任务名称、任务类型等信息，在系统界面上展示出详细的数据统计结果；  7.系统可根据统计间隔、统计类型、时间段及任务名称等信息对任务数据进行分析，并可生成可视化的柱状图、趋势图、对比图，便于系统操作人员进行管理；  8.系统支持对传输任务的源端文件策略、病毒查杀、同步周期、带宽分配等内容进行配置；  9.系统支持通过系统界面对病毒库进行升级操作；  10.系统具有数据整合服务系统功能、安全数据流系统功能、数据库同步系统功能。  11.系统支持服务转发功能，需要使用请求服务的用户必须在系统中注册用户信息，用户信息包括用户名、密码、访问IP段等；对用户可以访问的WebService资源进行注册，未经注册的资源将不允许访问；对用户访问WebService资源的请求参数和响应内容进行过滤，采用关键字过滤的方式检查请求参数的响应内容，对不合法的请求或响应不允许传输； |
| 24 | 安全隔离网闸 | 1套 | 设备参数：  1.标准机架式设备，采用2+1双主机架构和专用硬件隔离技术；  2.采用基于Linux内核的安全加固多核并行操作系统；  3.系统硬件架构采用高可靠性设计；保证基于硬件的可信任计算体系；  4.提供液晶面板，实时显示设备运行各项状态指标（包括设备厂家、型号、状态等）；  5.提供不少于8个10/100/1000Mbps（电口），2个万兆多模光纤接口（含同等数量的光模块）；  6.内部系统交换带宽≥10Gbps；  7.应用层数据传输率≥6Gbps；  8.系统并发连接数≥50000；  9.无故障运行时间＞50000小时。  设备功能：  1.采用“2+1”的硬件架构，提供多种主流数据库的单、双向数据交换；  2.基于专用客户端与网闸安全连接方式，发送、接收应用数据；  3.无需修改数据库表结构，不涉及到代码修改；  4.支持多种增量方式；可分别定义增加、删除、修改的数据传输；  5.数据传输可选SSL加密，链路安全；  6.数据传输高度可靠，采用缓存确认机制进行保证；  7.基于专用客户端与网闸安全连接方式，发送、接收应用数据；  8.文件传输采用KFM技术，监控文件服务器系统内核、捕获文件变化；  9.系统支持一键还原功能，在系统出现严重配置错误、系统损坏时可通过后台管理员操作将系统还原成初始状态；  10.系统自带证书服务功能，可生成服务器证书、用户证书用于加密认证；  11.为保证系统兼容性，安全隔离网闸需与第23项安全数据交换系统为同一品牌。 |
| 25 | 集控探针 | 1套 | 设备参数：  1.标准机架式设备；  2.提供不少于4个10/100/1000Mbps（电口）；  3.采用基于Linux内核的安全加固多核并行操作系统；  4.应用吞吐量：500Mbps；  5.监控管理业务>6000；  6.最大审计用户数≥10000；  7.稳定性运行时间(MTBF)>50000小时。  设备功能：  1.部署于外部网络系统中，用于平台内部设备状态获取以及设备管理；  2.不与内部网络之间存在任何网络连接，规避网络旁路风险；  3.每条独立链路配置一台，用于链路中设备监管，支持SYSLOG v2/SNMP v3、Telnet、ICMP协议方式的数据和信息采集； |
| 26 | 防火墙 | 1套 | 2U机箱；  配置2个万兆光口，4个千兆光口和6个千兆电口，2个可插拔的扩展槽；  标配模块化双冗余电源；  防火墙吞吐率：24Gbps；并发连接数：500万；三年质保。 |
| 27 | 入侵防御系统 | 1套 | 2U机箱；  配置2个万兆光口，4个千兆光口和6个千兆电口，1个可插拔的扩展槽；  标配模块化双冗余电源，三年质保，三年攻击规则库升级许可；  整机吞吐率：24Gbps，最大并发连接数：300万，IPS吞吐率：5Gbps |
| 28 | 可信边界安全网关 | 1套 | 标准2U机箱，双冗余电源；5个10/100/1000M Base-TX；2个万兆SFP插槽，2个千兆SFP插槽，默认100个SSL VPN并发用户，可通过选购许可进行扩展；VPN隧道数12000条；最大并发SSL连接数：450万；每秒新建连接数：3500次/秒；SSL事务处理速率：4000次/秒；加密带宽吞吐量：10000Mbps/秒；最大接入用户数>50000；SSL转发延迟<0.4ms。 |