## 技术方案

### 项目背景

许昌市公安局（以下简称“市局”）于2014年投资建成了公网接入链路（以下简称“原链路”）并投入使用，实现了网上警局、网上车管所、公路客运、高德地图等公网业务的接入与信息交换。同时，对接入业务进行了统一监控和管理。

随着物联网电动车业务办理和信息发布、信息采集服务需求日益凸显，为了有效拓宽公安信息通信网（以下简称“公安网”）信息来源的广度，同时，提高公安便民服务业务效率，方便车辆的管理等工作，需对原链路的接入用户支撑能力、数据交互吞吐性能、单点故障避免措施等提出了更高的要求，故需对原链路进行升级设计，并新建物联网电动车智能防盗相关系统（以下简称“本方案“），在保障公安网安全的前提下，满足物联网电动车智能防盗系统的安全接入和信息的高效交换。

### 现状分析

市局原链路建设于2014年，现接入了网上警局、网上车管所、公路客运、高德地图等四项公网业务。原链路设备基本情况如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备名称 | 基本性能 | 采购时间 |
| 1 | 防火墙 | 2U机架式设备  6个SFP插槽，6个10/100/1000MBase-T端口  吞吐量：4.5Gbps  最大并发连接数：220万 | 2014年 |
| 2 | IPS | 2U机架式设备  6个10/100/1000M电口及6个SFP光纤插槽  吞吐量：4Gbps | 2014年 |
| 3 | 单向安全传输系统 | 大文件传输性能：500Mbps  小文件并发数：500 | 2014年 |
| 4 | 三层  交换机 | 24个10/100/1000M电口，4个1000M SFP光口 | 2014年 |
| 5 | 探针 | 最大监控节点数：100个  最大吞吐量：600Mbps | 2014年 |

### 存在问题

1、原链路建设时间至今近4年，存在设备老化，硬件长期运转效率降低等问题。

2、原链路已接入4个公网业务，随着公安网对数据鲜活性和丰富度要求的提高，陆续会有更多的公网业务系统与公安网进行交互，原链路已无法满足大量数据的交互处理的采集实现。

3、原链路缺乏对公网链路中违规访问行为等的监测与审计。

### 升级方案

针对上述存在的三方面的问题，本次市局原链路升级方案设计如下：

1、新增2套单向安全传输系统和2台负载均衡器。一是新增的2套单向安全传输系统严格按照公安部《公安信息通信网边界接入平台安全规范-公网信息采集部分》要求，由导入前置机、单向安全传输设备和导入服务器三部分组成，三部件分工合作，提升系统效率。二是通过2台负载均衡器和原链路单向安全传输系统实现负载，避免单点故障，提升原链路处理性能。其中，2台负载均衡器采取主备方式部署。

2、新增1台防病毒网关，主要用于实现对公网接入链路中的病毒过滤、蠕虫过滤、木马通讯监控、安全漏洞攻击监控以及口令探测监控等。

3、新增1套公网接入数据分析系统，加强对公网接入业务的传输数据的审计。

4、新增1套车联网管理系统，实现对车辆基本信息的管理，车辆异常情况的分析以及车辆轨迹的管理。

#### 拓扑图

此次升级方案拓扑如图 4‑1所示，其中，绿色字体标底设备为本次升级新增设备。



图 4‑1 许昌市公安局公网接入链路升级拓扑图

#### 业务流程



1、公网接入终端经防火墙、IPS、防病毒网关与应用服务区的前置服务器（包括文件服务器、WEB服务器）建立连接，并将采集的数据提交至前置服务器。

2、应用服务区的前置服务器将采集的数据进行文件打包，并采用标准的FTP协议，将文件传输至单向安全传输系统的导入前置机。

3、导入前置机对接收到的文件进行格式过滤、安全检查，将数据通过单向安全传输设备传输至导入服务器。

4、导入服务器接收来自单向安全传输设备的数据文件，检验数据完整性，并向公安网的业务系统提供数据导入服务。

5、公安网业务系统对文件进行拆包、检查与解析处理。

6、对于需要发布在公网的数据，通过人工拷贝的方式发布在应用服务区的前置服务器（包括文件服务器和WEB服务器），再由前置服务器发布到公网相应的服务端。

#### 安全设计

##### 防火墙

防火墙可根据数据包的源地址、目标地址、协议类型、源端口、目标端口以及网络协议等对数据包进行访问控制,可实现基于策略的HTTP、FTP、TELNET、SMTP、POP3等透明代理和深度过滤，能确保终端用户合法有效地使用各种网络资源。

利用NAT地址转换功能，防火墙还可保证公网信息采集和链路的应用服务区内的主机地址不被外部终端获得。

##### IPS

IPS是实时的网络违规自动识别和响应系统。它运行于边界保护区内，通过实时监听网络数据流，识别，记录入侵和破坏性代码流，寻找网络违规模式和未授权的网络访问尝试。该系统安装于防火墙等逻辑隔离设备后，可以对攻击防火墙等设备本身的数据流进行响应，同时可以对穿透防火墙等设备进行攻击的数据流进行响应。

##### 防病毒网关

防病毒网关通过在网络边界对进入内部网络的数据进行病毒扫描，一旦发现病毒就会采取相应的手段进行隔离或查杀。

* 病毒过滤

精确识别邮件病毒、文件传输病毒、网页病毒等，防止病毒通过常见的传播途径进入内部网络。

* 蠕虫过滤

可监测已知蠕虫，还可以在未知蠕虫爆发时进行预警。

* 木马通讯监控

可监控多数常见的木马通讯，可以识别新型木马，包括手机木马。

* 安全漏洞攻击监控

可实时监控/防御针对系统级发起的漏洞攻击，避免因系统漏洞引起业务中断，或称为恶意攻击者“跳板”。

* 口令探测监控

可对常用的网络服务如：SMTP/POP3/IMAP/FTP/HTTP/SMB等进行口令探测，并可触发相应的阻断动作，防止口令探测活动的持续进行。

* 自动阻断

自动阻断网络异常流量，防止蠕虫大量爆发、DoS攻击、邮件风暴造成的网络堵塞，并记录相关日志，以便后期查询排错。

##### 单向安全传输系统

单向安全传输系统数据入公安网由：导入前置机、单向传输设备、导入出服务器三台组成。采用物理方式构造信息单向传输的唯一通道，实现信息单向传输，即信息只能由一个安全域向另一个安全域传输，并保证反方向无任何信息传输或反馈，实现应用服务区与公安网间的数据单向传输。

导入前置机：与导入服务器配合使用，对各应用服务器进行设备认证，通过安全的协议，汇聚各应用服务器上采集到的数据，并对数据进行格式和内容安全检查，最后统一通过单向传输设备设备导入到位于公安网的导入服务器，并进行传输过程的审计。

单向传输设备：利用光的单向性的物理特性，保证数据仅能单向导入。同时，导入前置机、单向传输设备和导入服务器串接部署，单向传输设备只提供导入前置机与导入服务器两个专用设备之间的数据单向导入，不与各种应用服务器交互，避免引入额外的安全风险，并对传输的数据业务进行日志审计。

导入服务器：接收来自单向传输设备的数据文件，检验数据完整性，并向公安网的业务服务器提供认证和数据导入服务；实现对接收的数据进行完整性检查，对异常数据进行阻断并告警；提供业务数据日志审计功能。

##### 公网接入数据分析系统

公网接入数据分析系统主要实现对公网接入链路中传输的文件进行采集以及分析处理。

1、数据采集

数据采集负责实现公网接入业务数据采集和上报处理。

主要采集本次新采购单向安全传输系统传输的文件名、文件内容、文件大小、源IP地址、目的IP地址等数据（但需相关业务系统配合提供相关数据获取接口）。

注意：原链路单向安全传输系统（三合一）因设备采购时间早，不支持采集上述文件数据。

2、数据处理

数据处理负责对采集上报的数据进行处理，包括数据清洗、数据转换、数据校验、数据整合等，然后将数据保存到安全数据池中。同时提供统一的数据共享接口，方便获取数据并进行分析处理，保证系统具有良好的可扩展性。

（1）数据清洗

数据清洗模块支持发现并纠正数据中可识别的错误，包括检查数据一致性，处理无效值和缺失值等，有效地解决数据相互之间的未知冲突，删除不符合要求的数据。不符合要求的数据主要是不完整的数据、错误的数据、重复的数据三大类。

数据清洗是对采集的数据进行剖析和审计的过程，可以明确地展现数据现状及其特点，是建设数据分析系统的重要工作，也是保证采集数据是否正确可靠的根本。为了提升管理效率，针对存在的采集的数据不一致不统一等数据问题进行处理，彻底理清现有数据的内容、结构、模式、数据属性、数据质量等至关重要的内容，从而为构建新的数据模式和建立新的数据管理体系打下基础。

一般需要梳理的数据问题

* 在本次项目活动中使用的数据质量是否可靠。
* 格式是否统一规范。
* 推行的项目是否可以获得所需要的数据源。

数据梳理的方式

* 数据结构分析。大多数的数据都有与之相关联的元数据，它可能存在于相关数据库、数据模型或文本文件中。元数据中所包含的信息可以指示出数据的类型、字段长度，数据是否唯一，或者字段是否为空或为零等。
* 模式匹配。模式匹配可确定字段中的数据值是否有预期的格式。这一方法可以快速地确定字段中的数据与各数据源是否一致，是否符合要求。
* 标准化分析。数据常常来自于不同的来源：不同的业务系统和不同的监控对象。这常常是数据质量问题的根本所在。如果一条数据多次以不同的排列方式出现，则查询和统计报告都必须指出每次报告中所用的数据源和数据名称。

（2）数据转换

数据转换的过程包括数据格式转换、信息代码转换和值转换。按照规则进行数据转换。

需要公网各接入业务厂商配合完成上述数据清洗、数据转换过程。

（3）数据加载

数据加载是将经过整合后的数据插入到相应的数据表中。数据加载过程进行的主要操作是插入操作和修改操作。

各条链路采集的数据通过数据转换后已成为最终进行数据合并的“数据原料”，是准确、安全的有效数据。当然在数据合并的操作中也需要进行数据冗余检查、数据重复检查以及合并之后的数据检查和数据梳理，以确保最终的准确性。

（4）数据接口

提供标准的数据访问接口，以便应用层能够获取数据并进行各种分析处理，保证系统具有良好的可扩展性。本项目建设中通过数据接口将采集到的数据传输至安全数据池中进行统一存储。

3、数据存储

系统将加工处理好的数据存到数据池中，整个系统采用分布式存储系统搭建，采集的数据以副本存储，并将数据存放在不同服务器，避免数据受外界环境影响而导致丢失的问题，确保应用的连续性、可用性。

（1）数据高可靠性：保证所有数据存储在处于不同节点上面，即使集群中的部分节点出现硬件和软件故障，平台能够检测到故障并自动进行数据的备份和迁移，保证数据的安全。

（2）服务高可用性：能够不中断地访问数据，降低平台的不可服务时间。即使出现软硬件的故障、异常和系统升级等情况，服务仍可正常访问。

（3）高吞吐量：运行时系统I/O吞吐量能够随机器规模线性增长，保证响应时间。

（4）高扩展性：保证平台的容量能够通过增加机器的方式得到自动扩展，下线机器存储的数据能够自动迁移到新加入的节点上。

本项目不建设数据存储安全池，由市局已有数据存储安全池提供，存储副本数据保存时长为半年。

4、数据应用

（1）接入业务审批与审计

1）接入业务审批

针对公网接入链路提供相应的业务接入审批流程，具体由业务主管部门发起，具体申请审批内容包括业务主管部门名称、业务应用系统名称、业务类型、业务操作方式、业务主管部门主管人联系方式、数据交换方式、基本协议、数据/文件格式、源/目标IP地址、源/目标端口。

业务主管部门向科信部门提交上述接入业务审批申请，由科信部门进行审批，审批同意后允许业务接入公网链路。

2）接入业务审计

需详细审计公网接入链路上接入业务的行为，且可以形成一定的行为轨迹，针对公网接入业务，需审计具体业务在具体的时间传输的文件、内容、结果等信息。可支持的审计时长为半年。

（2）数据开发与分析

根据采集的数据，设计如下算法模型。

1）数据交换行为监测审计

从对公网接入业务系统的交换频率，产生的流量数据，交换方式，以及交换规则等多维度的综合审计分析，通过交换时间维度和相关业务类型进行差异分析。

通过海量数据分析建模，大部分综合数据交换行为都属于高斯分布的置信区间，而对于置信区间之外的数据交换行为则需要及时预警及锁定分析，防止公安内网数据被违规泄漏行为发生。

2）数据交换透视行为扫描雷达

自动分析统计公网交换数据总量、疑似异常数据交换量和异常数据交换量。根据分析形成可视化的公网数据交换行为透视扫描雷达，从多个视角查询展示公网数据交换行动轨迹，全面的对应公网数据交换行为可视化管控。

5、告警管理

提供统一告警中心和配置管理。

（1）告警中心

提供统一的告警数据的存储与展现，包含：告警定义、告警类型、告警等级。

（2）告警配置管理

告警定义：定义告警事件，同时对每个告警定义其清除告警事件、重复策略和过滤策略。

告警通知策略：设置定义告警通知的策略，定义后，系统可以根据策略设置进行告警通知。

告警类型：对从监测业务角度对告警进行分类，并对告警类型进行定义。

告警等级：定义告警的级别以及显示颜色特征。

6、系统基本管理

提供系统基本管理功能，包括用户、角色、权限、日志等方面。

（1）用户管理

提供系统用户管理。

（2）角色管理

提供系统用户管理，如各级平台管理员角色、业务管理员角色、系统审计员角色等。

（3）权限管理

针对不通角色提供具体权限管理。

（4）日志管理

提供系统日志管理功能，具体为人员操作的日志，包括登录、查询等。

#### 链路监管

公网接入链路作为市局边界接入平台的一部分，需确保与市局现有边界接入平台无缝融合。此次新增的单向安全传输系统需纳入市局已建的集中监控与审计系统统一监管，无缝对接。

##### 探针

探针是监管系统中监控数据采集、预处理和归并的专用硬件设备。它能对监控对象的流量、日志事件、告警、设备信息等众多信息数据进行采集和预处理。具体有以下功能：

* 流量探测功能，支持对平台的流量信息进行探测和处理。
* 设备探测，能够对平台的设备进行探测，探测设备运行状况的信息。
* 事件收集，能够支持SYSlog、snmp等格式的事件信息的集中收集和处理。

##### 集中监控与审计系统

探针把预处理的信息传送到监管系统服务器上，监管系统各部分功能详细说明如下：

注册服务，提供以下功能：

* 平台信息注册：登记接入平台的地域信息、 建设信息 、运维信息 、审批信息、接入平台链路信息和设备信息；
* 业务信息注册：登记业务的主管部门信息 、审批信息、 应用系统信息 、业务扩展信息；
* 使用单位信息注册：登记使用单位的名称、物理位置、负责人等信息；
* 设备信息注册：登记平台内关键设备终端和使用单位终端的网络信息、属性信息、安全信息；
* 接口信息注册：登记业务数据格式接口信息。数据格式接口信息用于描述业务应用系统需要交互的数据格式；

监控服务，提供以下功能：

* 平台监控：监控平台当前运行总体情况
* 流量监测：能够监测整个接入平台以及平台内部各个链路和业务的流量信息
* 异常报警：能够按照接入平台安全策略监控接入平台内部的异常信息并报警
* 在线用户：能够列举接入平台在线用户的个人信息和使用信息
* 统计分析：提供对各类信息的统计分析功能
* 安全处置：能实现与集中监控与审计系统等设备联动，对异常用户的处置

审计服务，提供以下功能：

* 平台审计：审计平台总体历史运行情况
* 用户行为审计：对用户访问时间、行为和个人信息进行审计
* 业务应用审计：对业务应用交换的数据格式进行审计
* 设备安全审计：对用接入平台内部的关键设备运行状态进行审计
* 异常行为审计：对接入平台内部异常行为的网络信息进行审计，并联系用户行为信息帮助实现责任认定。

#### 车联网管理系统

车联网管理系统主要实现车辆基本信息的管理、车辆数据的采集与接收以及车辆轨迹的管理。其主要功能描述如下：

1、车辆基本信息的管理：

（1）车辆基本信息管理：提供对车辆基本信息的管理，包括添加、删除、查询、修改车辆基本信息。

（2）车辆实时位置查询：实时展示一辆或者多辆车辆位置信息。

（3）车辆历史位置查询：提供按时间段或者车辆编号查询车辆。

（4）车辆预警分析：对特定车辆提供系统预警和短信预警的功能。

（5）车辆异常分析：对异常车辆提供分析和筛选。

2、车辆数据采集与接收：

通过数据库、webservice等接口，实现与第三方管理平台的对接，实时获取或接收对方车联网的相关数据。支持将接收的数据实时打包成标准化格式数据，并写入本地数据库中，支持对数据库增量数据打包成标准化格式数据。

系统支持LTE-4G、NB-IOT网或VPN网，支持基于SDK进行二次开发，能够实时接收并解析不同品牌或类型的车联网智能终端数据，支持将接收的数据实时打包成标准化格式数据，并实时写入本地数据库中，支持对数据库增量数据打包成标准化格式数据，实现跨网数据同步和传输交换。

对接收的打包数据文件，通过与公网边界平台同步到公安内网，并在公安内网对数据进行解包，再写入指定的数据库。

三、车辆轨迹管理：

系统能够基于公安网，可根据不同用户、不同角色设定不同的权限，不同权限的用户可管理或查看指定区域、指定企业数据源或其他自定义类别的车辆相关信息。支持与PGIS平台对接，并支持在PGIS平台上调阅查看任意车辆、车辆组或全部车辆的实时位置信息、历史轨迹信息以及车辆的其他信息，包括车联网智能终端设备采集的数据信息。能够按照车联网智能终端设备采集的数据种类分类统计数据，并提供常见的图表分析和报表导出，图表展示方式包括柱状图、炮弹图、饼状图和热力图等。

系统具有权限管理功能，提供增加用户、角色、权限等管理功能。

系统支持与PGIS平台对接，支持与PGIS平台的地图对接，能够在地图上展示轨迹等信息。

系统支持统计各类数据使用情况，提供对车辆的各类数据的统计分析报表，能够实现各种图表的展示。