AnaTraf 应用案例 —— 医院网络回溯分析系统应用

Application

随着医院信息化水平的不断提升，越来越多的医疗机构构建了基于电子病历的统一信息平台，实现门诊、住院、检验、检查等关键业务系统的互联互通。这些系统的正常运行高度依赖于底层网络的稳定、高效和安全。网络一旦发生异常，将直接影响到挂号、诊疗、药品调配、数据上传等多个核心业务流程，对患者体验和医疗质量造成严重影响。

面临的挑战

网络故障定位困难

医院广泛开展"互联网+医疗"服务，例如预约挂号、远程会诊等功能。由于跨网段、跨云平台的访问路径复杂，一旦出现服务不可用现象，难以判定问题出在医院本地网络、云服务平台，还是中间通信链路。

终端接入无序，存在安全隐患

医院内部存在多种终端设备（如笔记本、外部厂商设备等）临时接入的现象。这些终端可能成为病毒传播、网络攻击的入口，尤其是在缺乏细粒度流量监控时，难以及时发现并隔离风险。

解决方案

为应对上述挑战，AnaTraf 提供了一种针对医院网络的网络流量回溯分析方案。

多维可视化流量监控： AnaTraf 部署于医院核心交换机，通过流量镜像获取全部网络通信数据，基于其深度包检测（DPI）能力，实时展示网络中的业务流、主机交互、协议分布及性能指标。运维人员可一目了然掌握各业务系统的通信状态与健康状况，提前识别异常趋势。

全流量回溯与历史还原： AnaTraf 支持长期存储原始通信数据包，可按主机、端口、协议等维度快速查询历史流量，帮助网络安全取证和业务故障分析。

事件自动告警与隐患排查： 支持设置自定义规则进行告警，对网络中的异常行为（大量连接请求、广播风暴等）发出告警。监控网络中的设备，建立资产白名单，实时监测非法设备的接入，协助 IT 人员精准处置。

客户价值

优化网络资源与业务体验： 通过对应用性能指标和网络行为的持续分析，医院能够基于数据优化网络结构和带宽分配，为远程医疗、智能终端等新业务场景提供坚实的网络支撑。

缩短故障排查时间： 利用深度数据分析和快速问题定位功能，减少了故障排查时间，提高了生产效率和响应速度。

加强安全防护与合规保障： 实现对所有接入设备和通信行为的全面掌控，及时发现网络异常行为。同时，为数据溯源和合规审计提供详细依据，助力医疗信息安全管理体系建设。