ANATRAF · APPLICATION CASE

AnaTraf 应用案例 —— 某制造业企业

应用案例

某制造业企业拥有三个办公节点，通过专线互联，构成了统一的企业网络体系。企业出口配置为双线接入（各 100Mbps），内部网络为千兆架构，日常用于生产控制、数据上传、远程办公等业务场景。IT 运维人员偶然注意到某些设备存在异常的上传流量，影响了内部网络的稳定性。

面临的问题

出口流量存在突发，影响业务

在日常运营中，IT 人员多次发现出口带宽突然打满，导致部分远程办公及在线系统出现卡顿，严重时影响关键业务系统的正常运行。

无法定位异常上传流量的来源

当运维人员发现“上网卡顿”时，只能通过登录路由器后台查看带宽使用情况，缺乏流量分析工具，无法进一步识别是哪个具体设备引发异常上传，只能靠猜测排查。

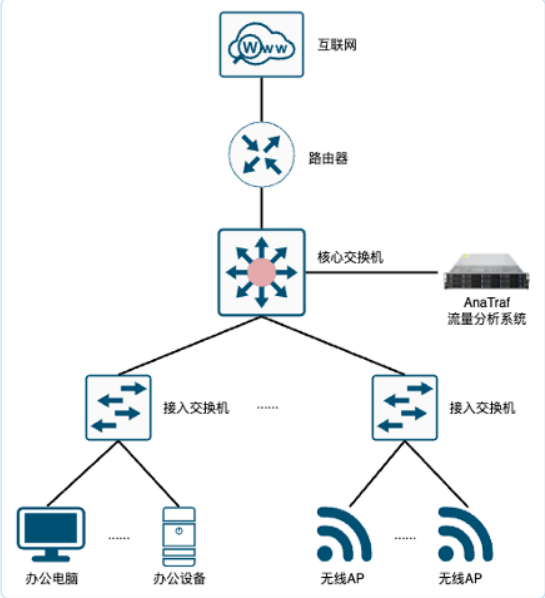
流量无留存，问题无法回溯

异常上传并非持续存在，而是间歇出现。由于路由器不具备流量留存功能，运维人员若未及时观察，事后无法查看是哪台设备、何时、向何处发送了异常流量。

解决方案

该制造业企业在多次尝试排查无果后，客户开始寻找专业的网络可视化与安全分析工具，最终部署了 AnaTraf 网络流量分析系统，对全厂网络流量进行了全面可视化分析与精细化追踪：

- **全网行为可视化能力：**部署于企业网络出口处，自动采集并解析全网流量数据，实现对设备、应用协议、外联行为的实时分析与可视化展示。仅用数分钟便定位到某个 Wi-Fi 接入点存在高频大流量上传行为。在进一步排查后，客户回忆起该台设备曾在去年遭遇勒索软件攻击，虽已进行初步处理，但实际残留的恶意组件可能仍在后台执行数据上传或僵尸网络通信。
- **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。



全网流量可视化与分析示意

客户价值

- **快速定位异常流量源，节省人力排查时间 80% 以上：**无需反复抓包分析，AnaTraf 实现可视化分析、定位，提升问题处理效率。
- **增强网络稳定性：**有效阻断非业务流量，确保关键系统在高峰时段仍有足够带宽资源。
- **提升网络管理效率与可控性：**通过对全网设备行为的监控与可视化管理，可准确还原过去的网络行为轨迹，提升安全事件溯源和复盘效率，增强企业对潜在威胁的预警和响应能力。