ANATRAF · APPLICATION CASE

AnaTraf 应用案例 — 多分支机构企业网络分析

应用案例

某全国性服务企业总部与多座城市的分支机构通过专线与 VPN 互联，统一使用 ERP、OA、客服与文件协作等业务系统。跨地域访问路径长、链路与出口策略各异，网络异常往往表现为“分支访问总部慢”或“特定应用间歇不可用”。这类现象既可能出在广域网或运营商链路，也可能出在分支机构本地网段、无线或终端侧，IT 团队缺乏对各侧流量的统一观测手段时，故障定界和复盘尤为困难。

面临的挑战

跨域故障定界难

用户报障时常描述为“连不上总部系统”或“视频会卡顿”，而运维在出口设备上仅能看到带宽占用，难以区分是广域网丢包、延迟，还是分支侧广播、ARP、或某台主机的异常连接行为在消耗资源。

分支侧缺乏细粒度留痕

部分分支仅配备基础网络与安全设备，无长期流量存储与 L7 解析能力。问题间歇出现或已恢复后，仍无法按主机、应用、协议维度还原当时行为，与总部协同排障时缺少共同依据。

安全与合规需可追溯

多地接入、远程办公与第三方驻场增加暴露面。企业需对异常外联、可疑行为具备发现与事后取证能力，并与现有制度下的日志审计要求相衔接，而不能仅依赖单点设备告警。

解决方案

客户在网络改造中采用 AnaTraf 网络流量分析系统。系统支持分布式部署，在总部及重点分支机构核心或汇聚侧以流量镜像、TAP 等方式旁路接入，对各地侧网络流量分别进行采集、存储与可视化分析，不中断现网业务。

- **多节点可视化与协议分析：**各部署点通过深度包检测与应用层识别，呈现业务流、主机与应用的分布及连接质量相关指标。结合 IP 分析、IP Pairs 与连接分析，可在分支或总部侧分别判断时延、重传、会话异常等更贴近问题现场的现象，缩小广域与局域的责任边界。
- **全流量存储与历史报文检索：**在存储策略与容量规划范围内长期留存原始数据，支持按时间、IP、端口、协议等条件检索，必要时提取为 PCAP 供进一步分析，满足故障复盘与安全取证需求，与全流量回溯类场景能力一致。
- **虚拟链路与分域统计：**在具备 VLAN 或分网段划分的场景下，可按指定 VLAN、物理网口或 IP 网段建立虚拟链路，对分支业务网、访客网等流量分类观测，避免“一整张网一个总数”导致的问题被掩盖。
- **告警与检测能力配合：**可配置主机流量等阈值类告警、可疑域名解析等行为类告警，并可结合威胁情报等检测能力，对明显恶意或异常外联进行提示；对告警事件可进一步按源目 IP、端口等维度做流量回溯，支撑溯源分析。

客户价值

- **提升跨域排障效率：**在总部与分支各侧均具备可观测与可检索依据后，能更快判断问题发生在链路、应用还是局部网段，减少电话协调与经验猜测，缩短业务中断或劣化持续时间。
- **加强分支网络可管可控：**各节点具备统一的分析维度与留痕能力，有利于总部规范分支接入行为、复现场景与统一复盘机制。