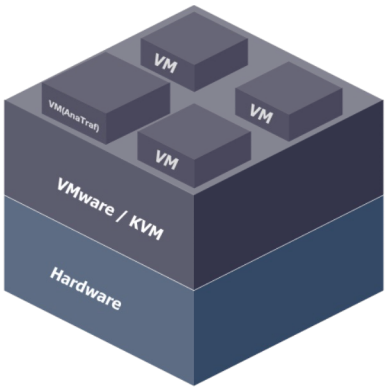
AnaTraf 网络流量分析仪虚拟化

规格表

为网络管理员设计的网络流量分析和故障排除工具

AnaTraf Virtual 是支持 KVM / VMWare / Docker 的虚拟化网络流量分析解决方案。

- 分析并关联OSI 2-7 层所有元数据
- 实时检索和过滤 2-7 层流量
- 历史流量回溯与 pcap 文件导出
- 自定义规则告警与事件推送
- 国内团队提供技术支持服务
- 国产品牌，自主研发



在 Web GUI 分析实时和历史流量

AnaTraf Virtual 提供全面的 OSI 第2至第7层网络流量捕获与分析功能，支持对实时与历史流量的精细化管理与可视化分析。通过简洁直观的Web GUI界面，用户可从网络全貌总览快速深入至单个节点或连接的详细统计，包括 IP/MAC 关联信息、IP 地理位置、应用协议识别、子网间流量交互等。系统支持基于时间轴的历史流量回溯，便于故障定位与趋势分析。

丰富的分析模块

AnaTraf Virtual 集成了集成了 OSI 2-7 层多个分析模块，帮助网络管理员识别网络问题，如微突发、TCP 重传、异常的 TCP 连接、TOP N 活跃用户、应用协议或目标 IP 排名。

网络流量记录和回溯分析

AnaTraf Virtual 支持完整的网络流量记录与深度回溯能力。管理员可通过Web界面进行条件筛选（如端口号、协议类型、IP地址等）并精准提取原始数据包，用于导出分析或配合第三方工具（如 Wireshark）进行深度取证。系统支持长时间存储并配合高速索引机制，确保大流量环境下依然可以秒级检索所需流量。

可扩展的架构和部署灵活性

AnaTraf Virtual 可以安装在具有足够 CPU 和内存的服务器上进行流量捕获和分析，处理性能可以随着 CPU 数量和内存用量的增加而提升。

AnaTraf Virtual	
特性	技术规格
虚拟化	KVM VMWare Docker
最低配置	CPU 核心：≥ 2 cores 内存：≥ 2 GB 硬盘：≥ 20 GB
最大吞吐量	取决于 CPU 性能
平均吞吐量	取决于 CPU 性能
每秒处理报文数量	取决于 CPU 性能
最大并发连接	取决于 CPU 性能
存储历史连接数量	取决于内存大小
存储 IPv4 / IPv6 数量	取决于内存大小