AnaTraf 网络流量分析仪

网络性能分析与质量监控

云争 YUNZHENG TECH

传统手段 vs 全流量回溯分析

传统手段

- Ping、tracert 等工具专业性强，故障分析周期长。
- 现有的工具受限，有的问题无法分析。比如部分设备无电口无法抓包分析。
- 现有的分析工具只能事后分析故障，无法对故障进行预警以及重现历史故障。

全流量回溯分析

- 图形界面，全面可视化网络。简单、高效、快速定位故障。
- 支持串联、TAP、镜像端口方式采集数据，适用范围广。
- 7×24持续采集、分析网络流量，随时可回溯，重现历史问题。细粒度，检索快。

传统手段弊端

问题难复现、难定位

过一会自己又好了...

告警太多难以分析

粒度粗，检索慢，缺乏原始场景的数据，效率低，最后也懒得看

核心特点

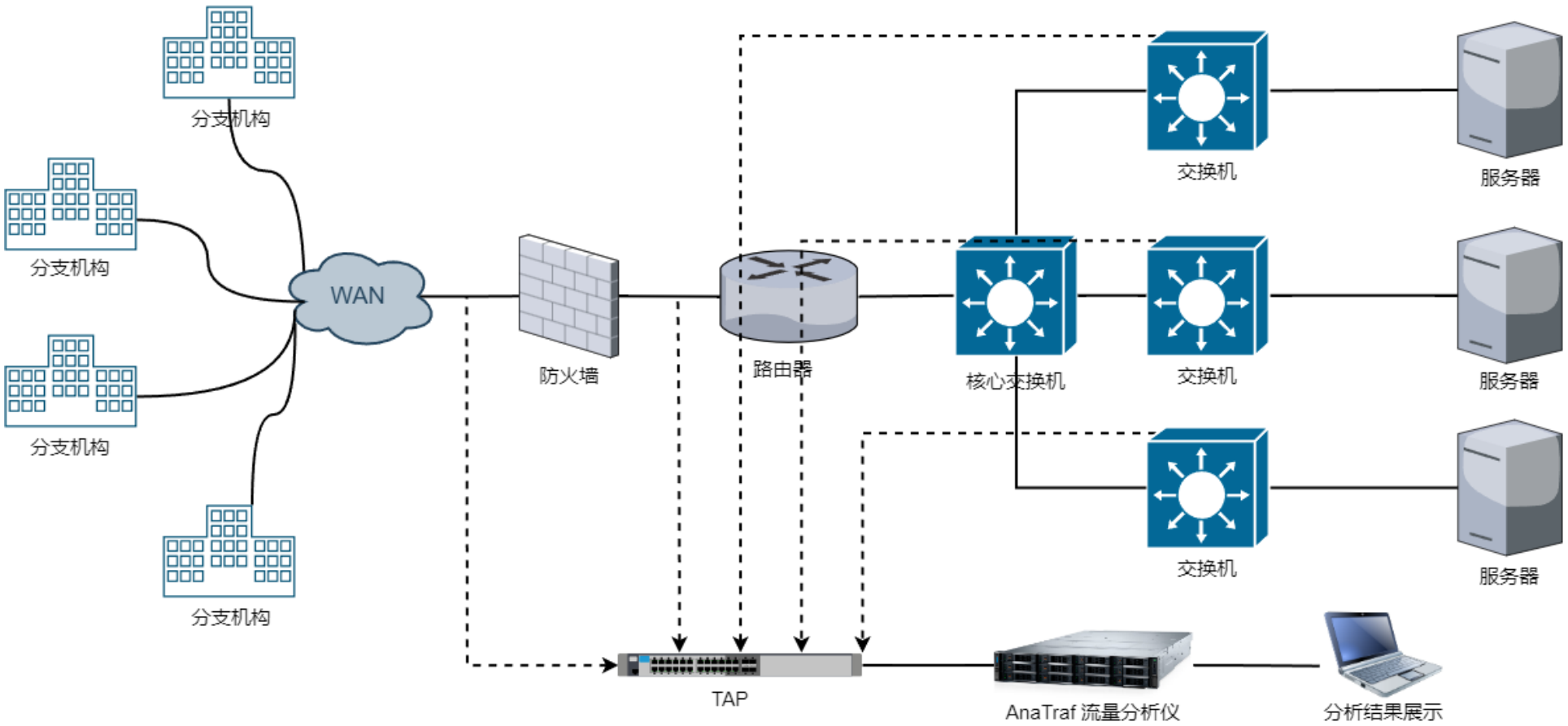
全流量

网络所有原始流量的存储、分析

多点采集与统一分析

多节点流量数据关联分析，迅速发现不同节点间的丢包、重传、延迟等问题

典型部署



主要功能

所有型号的设备具有相同的流量分析功能，不同型号之间只有性能的差异。

流量可视化

- 用户流量可视化
- 应用流量可视化
- 服务器流量可视化
- 在线解码

分析并关联OSI 2-7层所有元数据

全流量回溯

- 全流量存储
- 全流量回溯

实时分析并长期存储流量，提供任意时间点的回溯分析能力

网络性能监控

- 自定义业务监控
- 多点关联故障定位
- 关键性能指标监控

监控网络的持续运行状况和可靠性

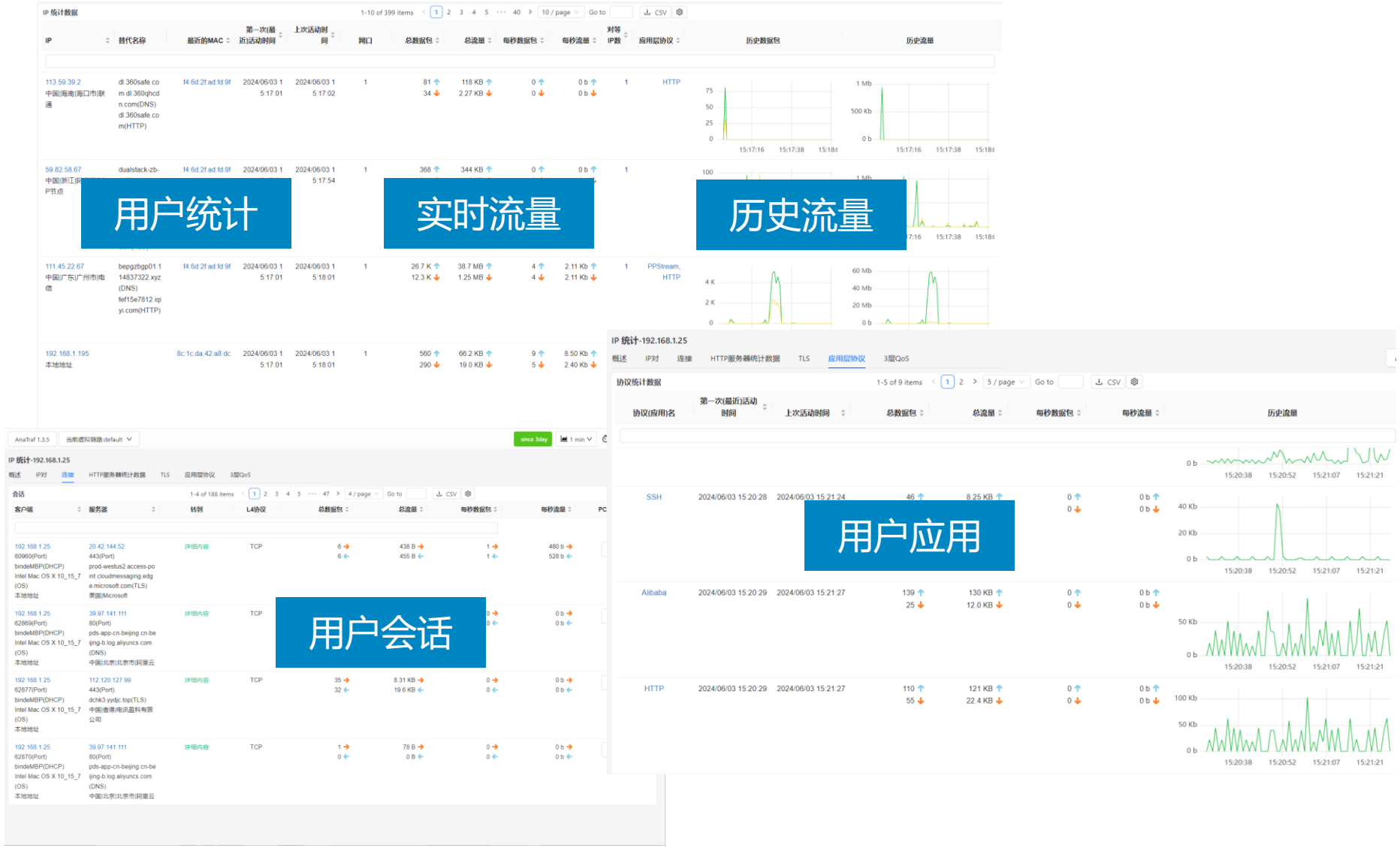
主要功能

1

流量可视化

- **用户流量可视化**
- 应用流量可视化
- 服务器流量可视化
- 在线解码

分析并关联OSI 2-7层
所有元数据



YUNZHENG TECH

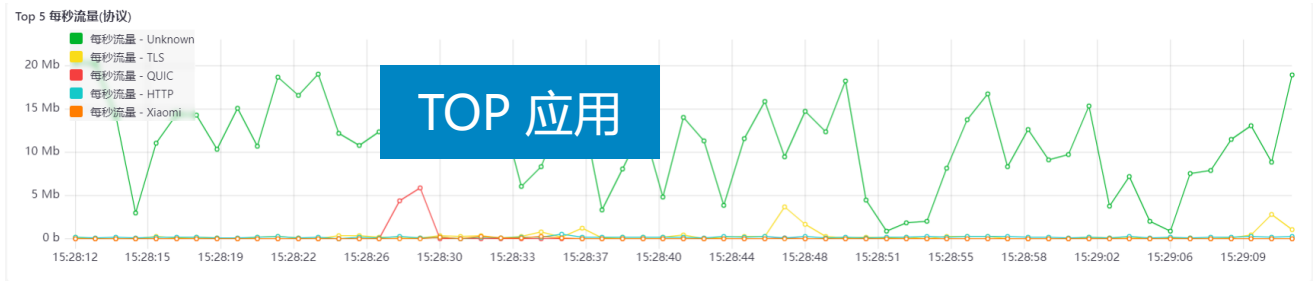
主要功能

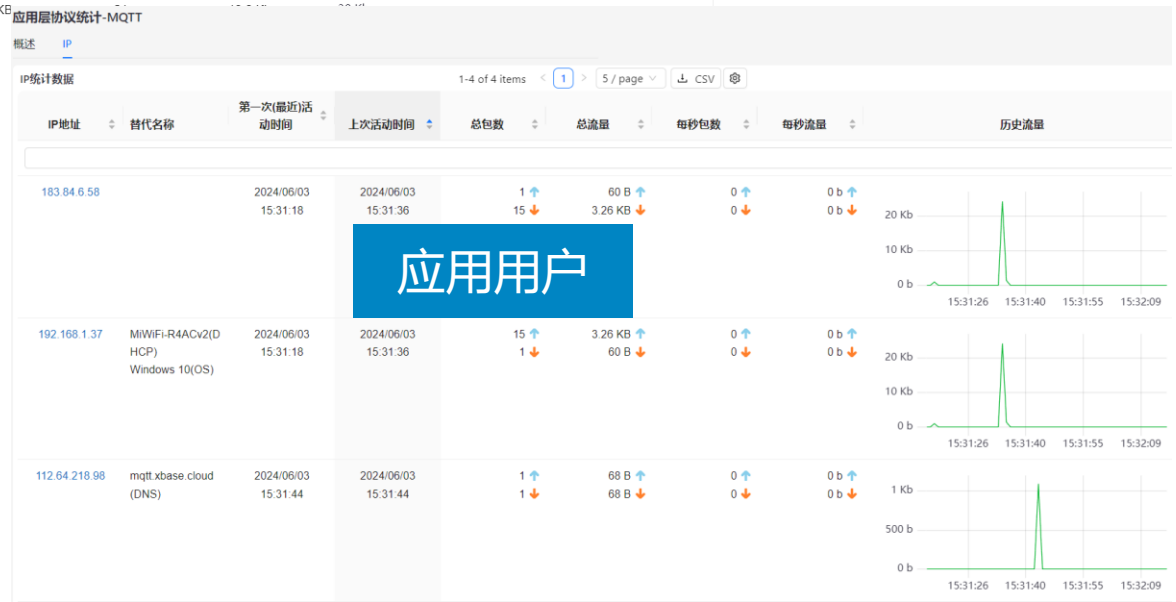
2

流量可视化

- 用户流量可视化
- **应用流量可视化**
- 服务器流量可视化
- 在线解码

分析并关联OSI 2-7层
所有元数据





YUNZHENG TECH

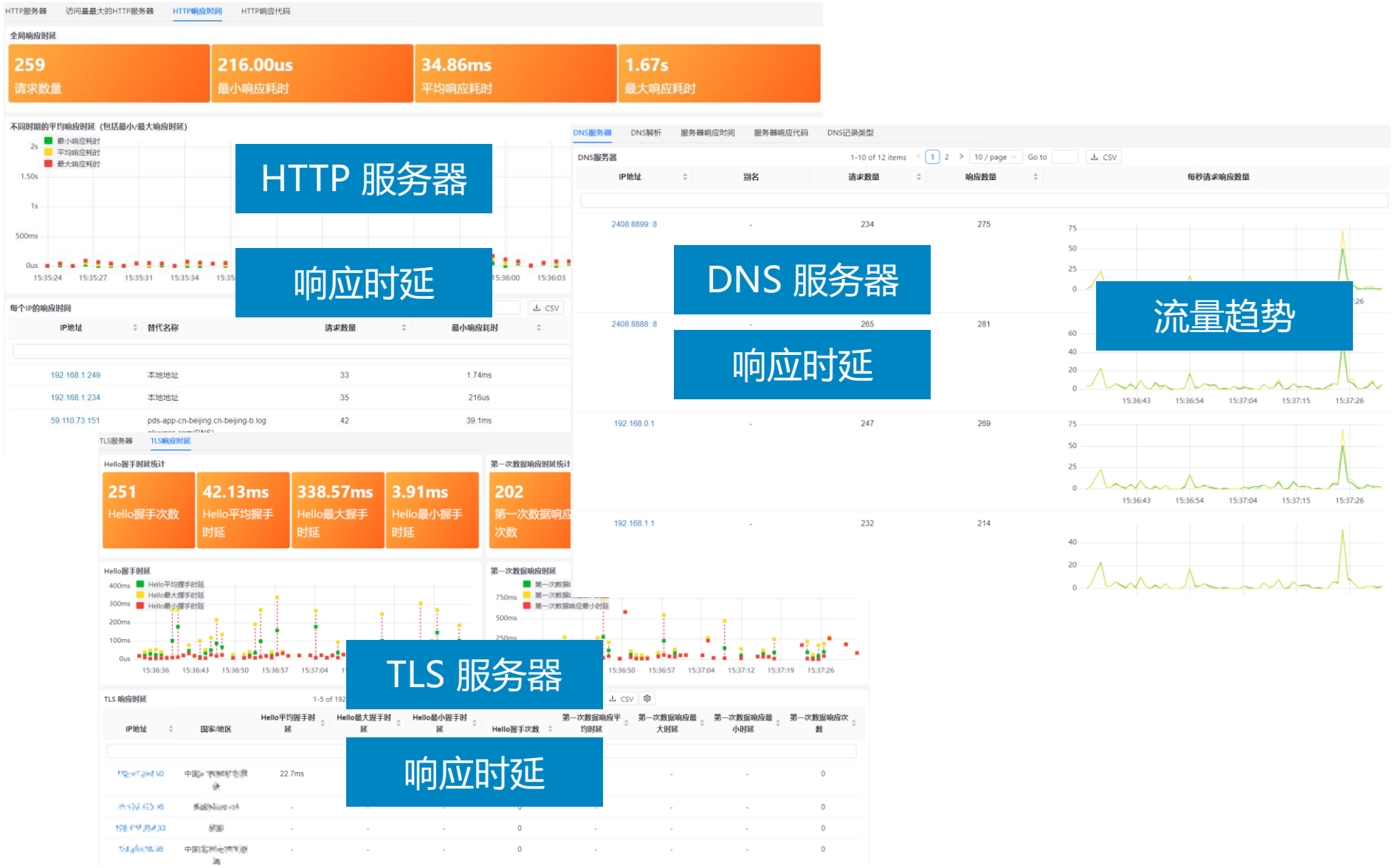
主要功能

3

流量可视化

- 用户流量可视化
- 应用流量可视化
- **服务器流量可视化**
- 在线解码

分析并关联OSI 2-7层
所有元数据



YUNZHENG TECH

主要功能

4

流量可视化

- 用户流量可视化
- 应用流量可视化
- 服务器流量可视化
- **在线解码**

分析并关联OSI 2-7层
所有元数据

数据包在线解码分析

在线预览

时序图

YUNZHENG TECH

主要功能

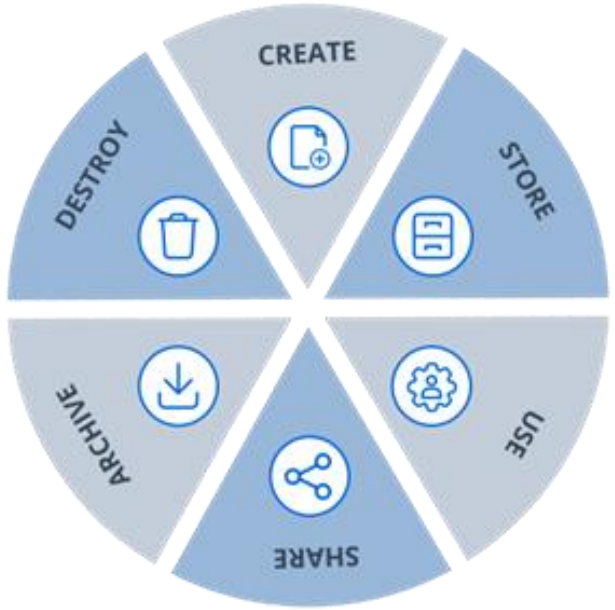
1

全流量回溯

- **全流量存储**
- 全流量回溯

实时分析并长期存储流量，提供任意时间点的回溯分析能力

大容量数据存储与检索



高速捕获

一体化设备，支持旁路、桥接部署。覆盖1G-100G网络。

大容量存储

单设备提供数百TB级原始流量存储。分布式、集群部署提供PB级存储。满足数月以至更长时间的存储需求。

流量回放

支持倍速、过滤、无损回放历史数据包，进行回溯分析。

高效检索

自研高性能内存数据库，数据秒级检索。支持基于网口、VLAN等方式配置虚拟链路接口，每条虚拟链路所有统计数据都是严格区分。

溯源分析

支持数百种协议识别。根据时间、GeoIP、连接等信息快速检索并导出原始报文，提供给安全产品。

主要功能

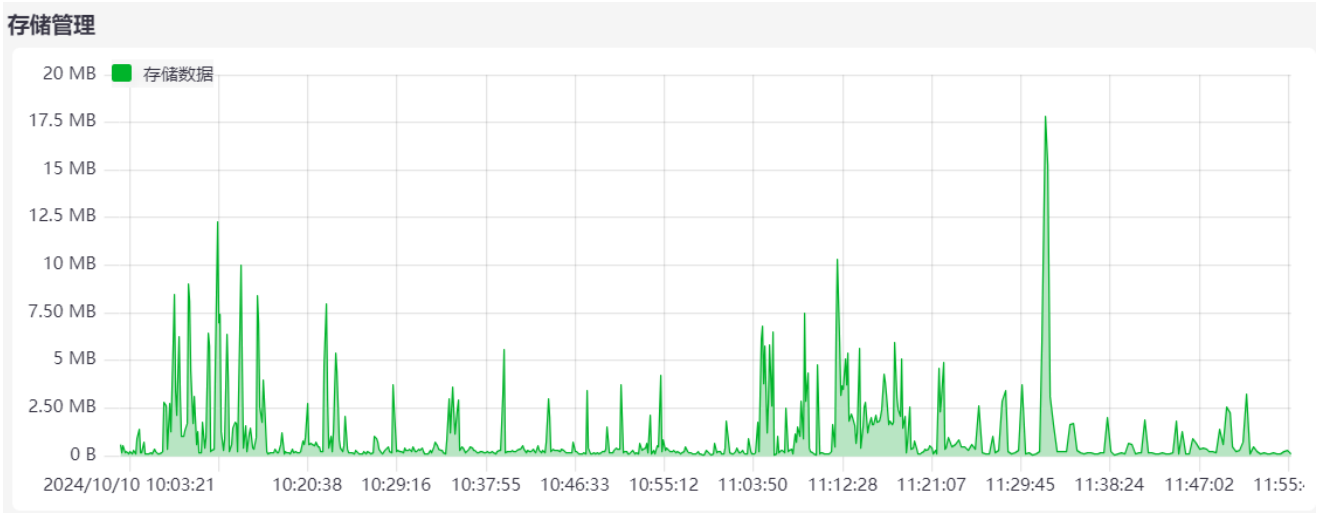
1

全流量回溯

- **全流量存储**
- 全流量回溯

实时分析并长期存储流量，提供任意时间点的回溯分析能力

满足等保测评180天流量回溯分析要求



- 在网络安全等级要求较高的网络中，需要长时间至少180天时间保存原始流量与日志信息。
- 支持长期的全流量、统计信息存储（配置足够的存储空间），满足检索、回溯分析的需求。
- 支持数据包过滤，数据包循环、滚动存储，以及数据包截断存储，节省硬盘空间。

主要功能

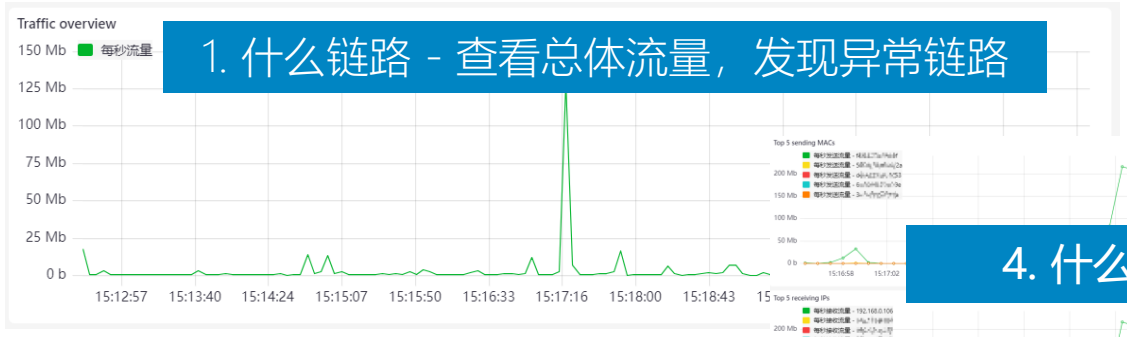
2

全流量回溯

- 全流量存储
- **全流量回溯**

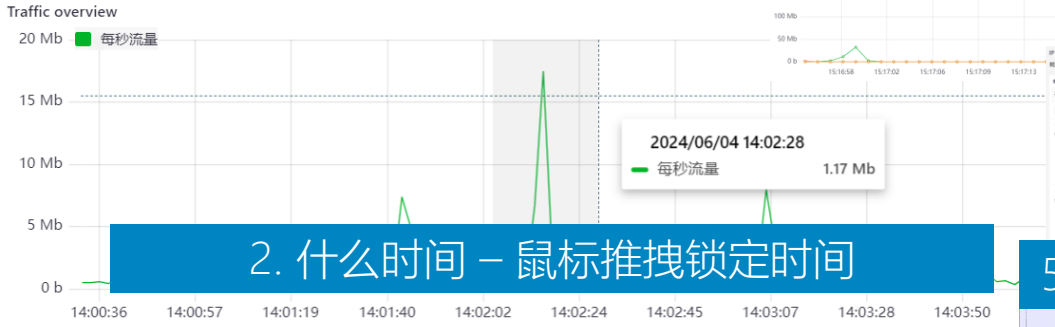
实时分析并长期存储流量，提供任意时间点的回溯分析能力

会话级流量回溯

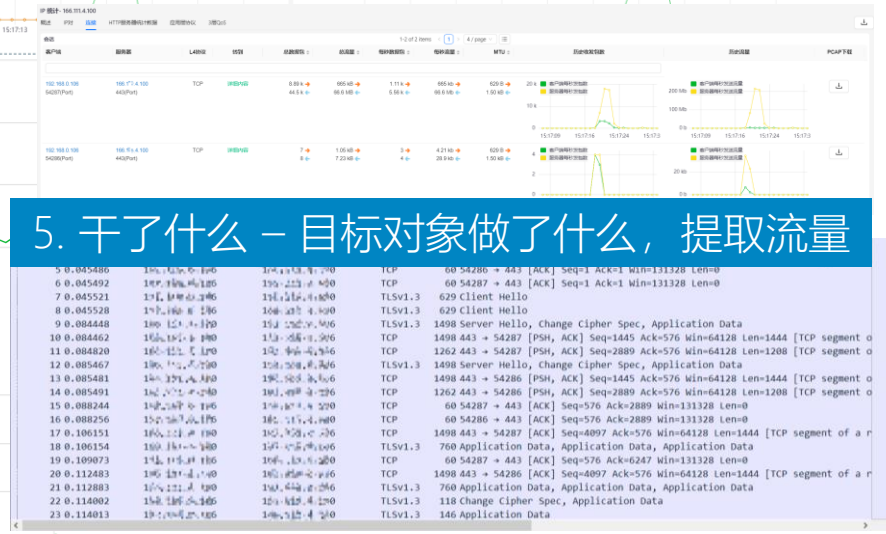


1. 什么链路 - 查看总体流量，发现异常链路

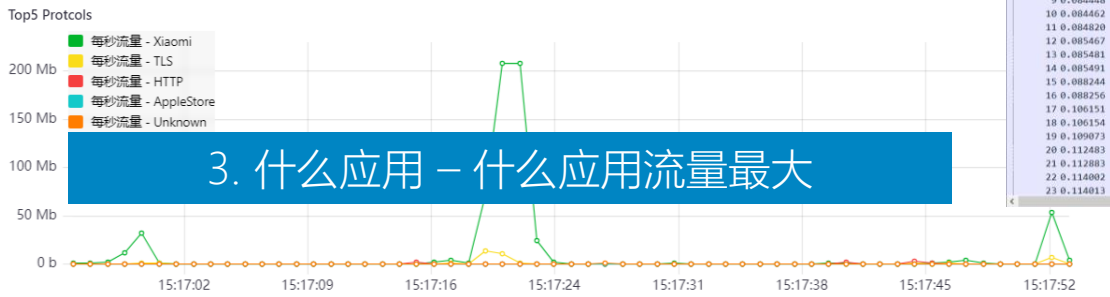
4. 什么人 – 谁在大量产生该应用流量



2. 什么时间 – 鼠标推拽锁定时间



5. 干了什么 – 目标对象做了什么，提取流量



3. 什么应用 – 什么应用流量最大

YUNZHENG TECH

主要功能

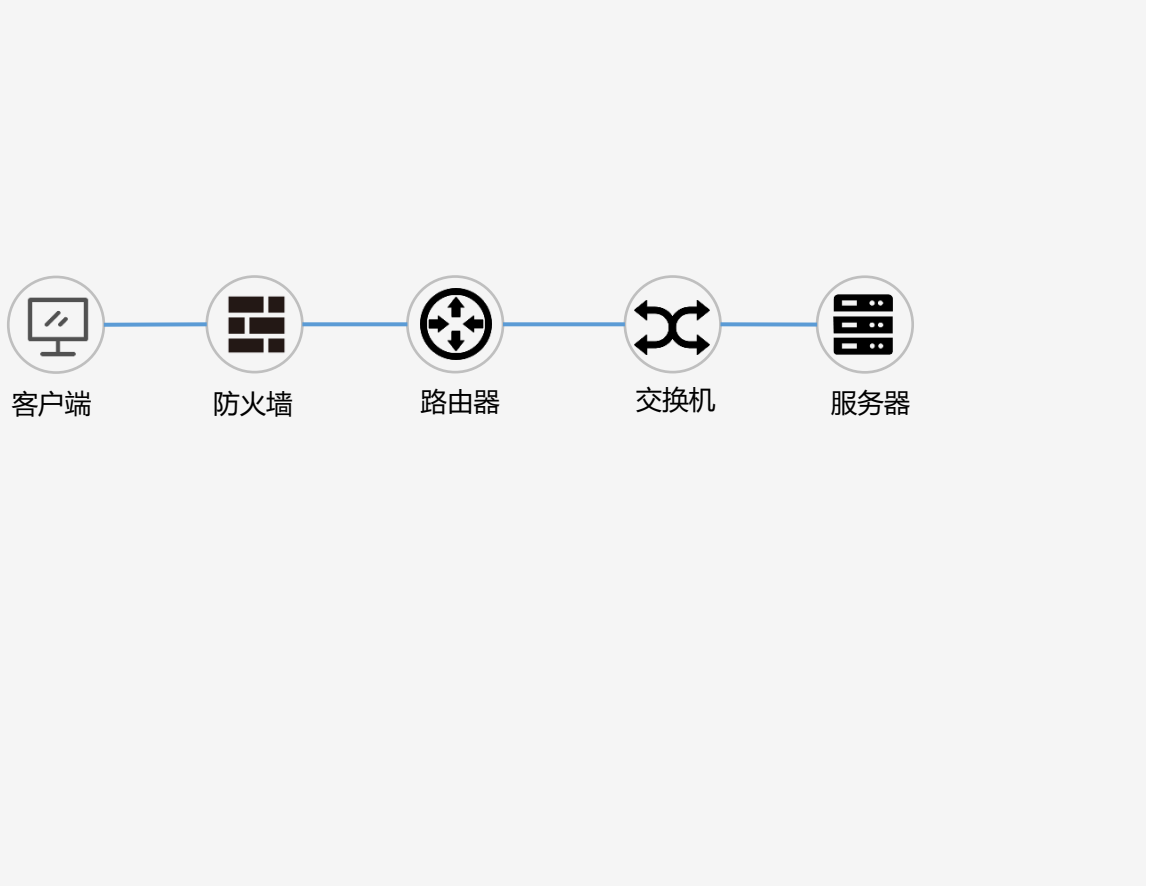
网络性能监控

1

- **自定义业务监控**
- 多点关联故障定位
- 关键性能指标监控

监控网络的持续运行状况和可靠性

自定义业务监控



添加元素

客户端　防火墙　交换机

服务器　路由器

主要功能

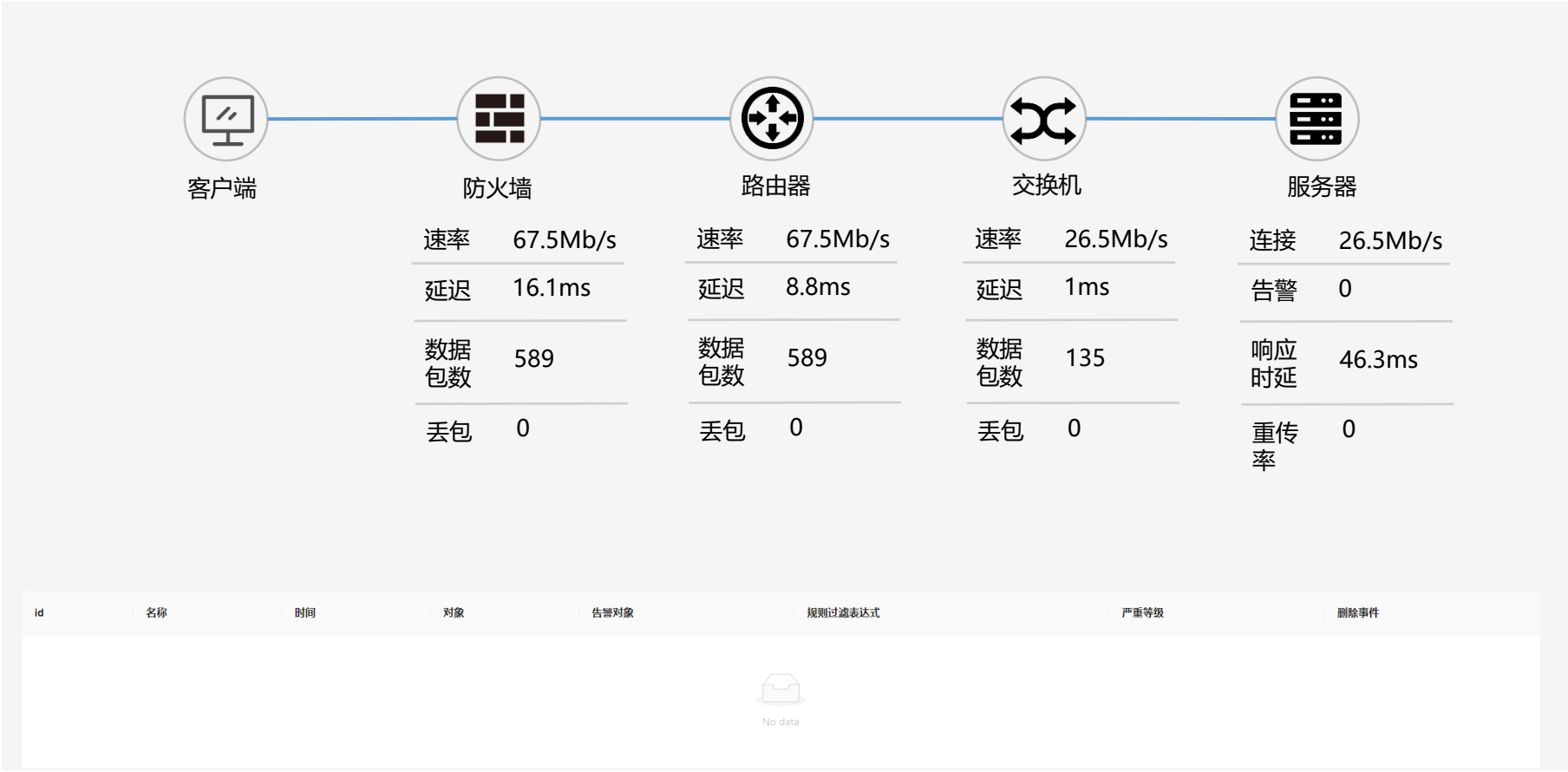
网络性能监控

- 自定义业务监控
- **多点关联故障定位**
- 关键性能指标监控

监控网络的持续运行状况和可靠性

多点关联故障定位

2



主要功能

网络性能监控

3

- 自定义业务监控
- **多点关联故障定位**
- 关键性能指标监控

监控网络的持续运行状况和可靠性

关键性能指标监控

提供数十种应用性能指标参数的统计，并支持查看性能指标在历史的变化趋势。

连接异常

TCP 客户端RST
TCP 服务器RST
TCP 握手

网络性能

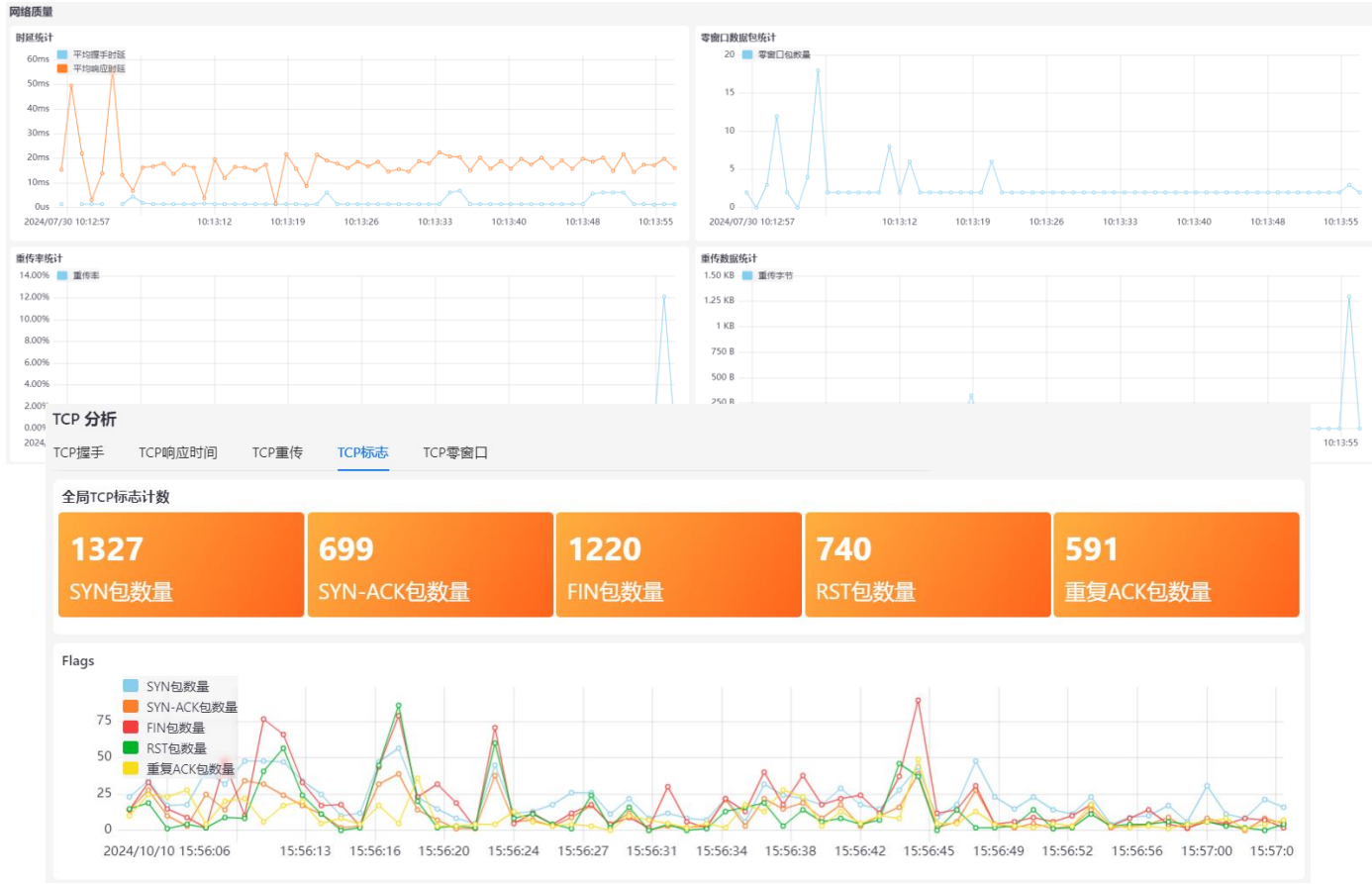
客户/服务网络时延
TCP 响应时延
TCP 重传, 丢包, 乱序

主机性能

客户端Zero Window
服务器Zero Window

应用异常

应用时延
HTTP 响应代码




云争
YUNZHENG TECH