

AnaTraf 网络流量分析仪

网络性能分析与质量监控

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。

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

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。

核心特点

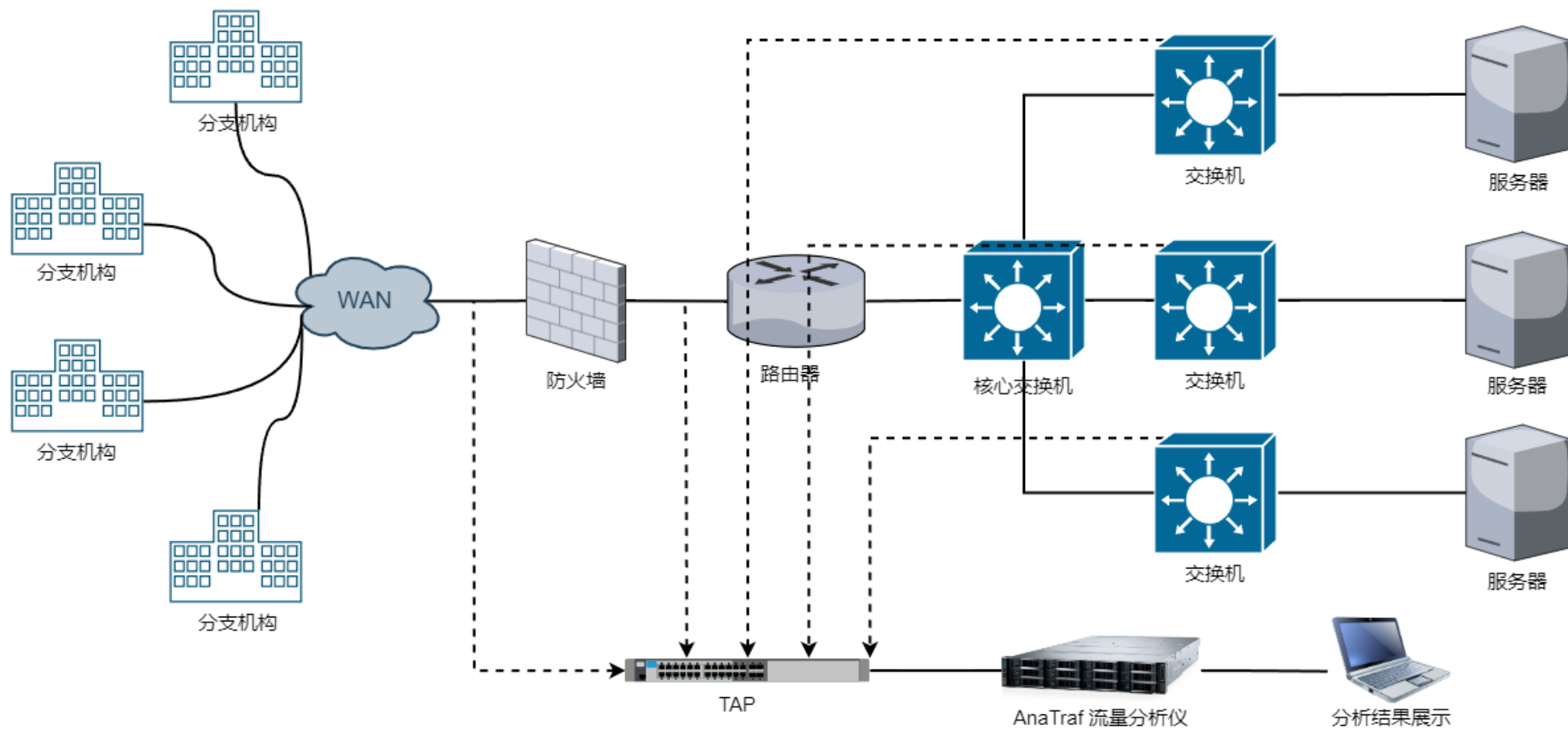
全流量

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

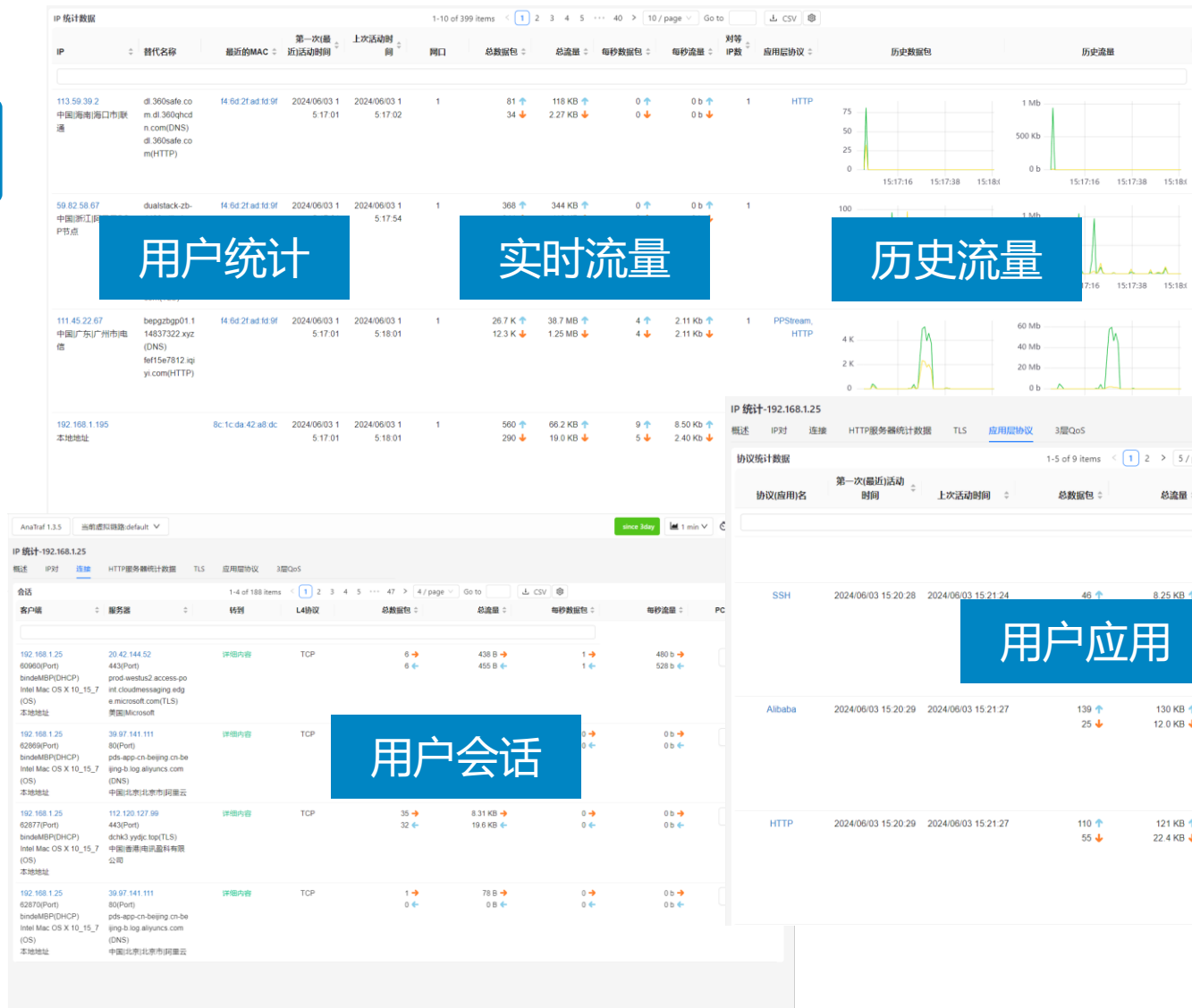


流量可视化

- 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

1



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



主要功能



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

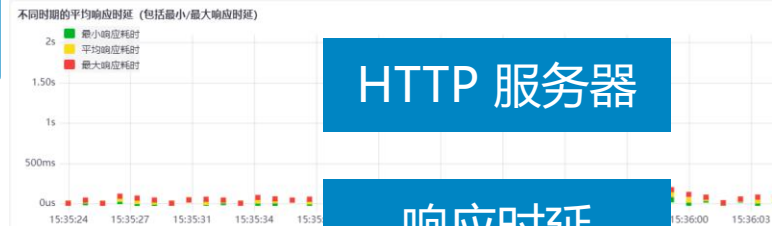
分析并关联OSI 2-7层
所有元数据

3



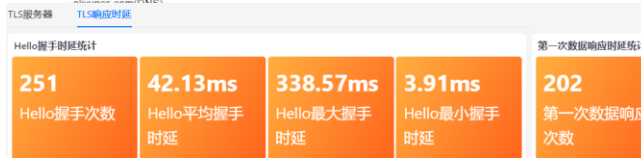
HTTP 服务器

响应时延



每个IP的响应时间

IP地址	替代名称	请求数量	最小响应耗时
192.168.1.249	本地地址	33	1.74ms
192.168.1.234	本地地址	35	216us
59.110.73.151	pds-app-cn-beijing-cn-beijing-b-log	42	39.1ms



TLS 服务器

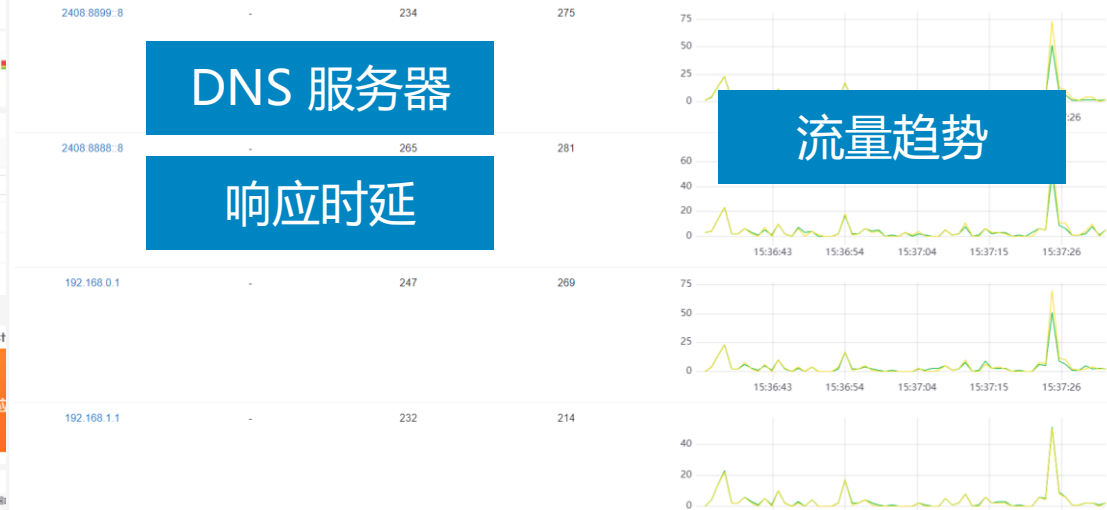
响应时延



DNS 服务器

响应时延

流量趋势



A bar chart showing the number of people with a university degree from 1990 to 2000. The x-axis represents the years, and the y-axis represents the number of people. The bars show a general upward trend, with a slight dip in 1999.

Year	Number of people
1990	10
1991	15
1992	20
1993	25
1994	30
1995	35
1996	40
1997	45
1998	50
1999	48
2000	52

- 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

4



流重组

主要功能



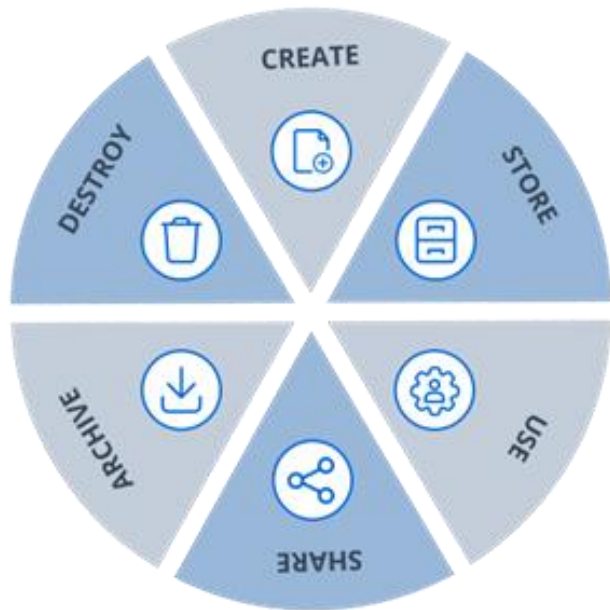
全流量回溯

- 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

1



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

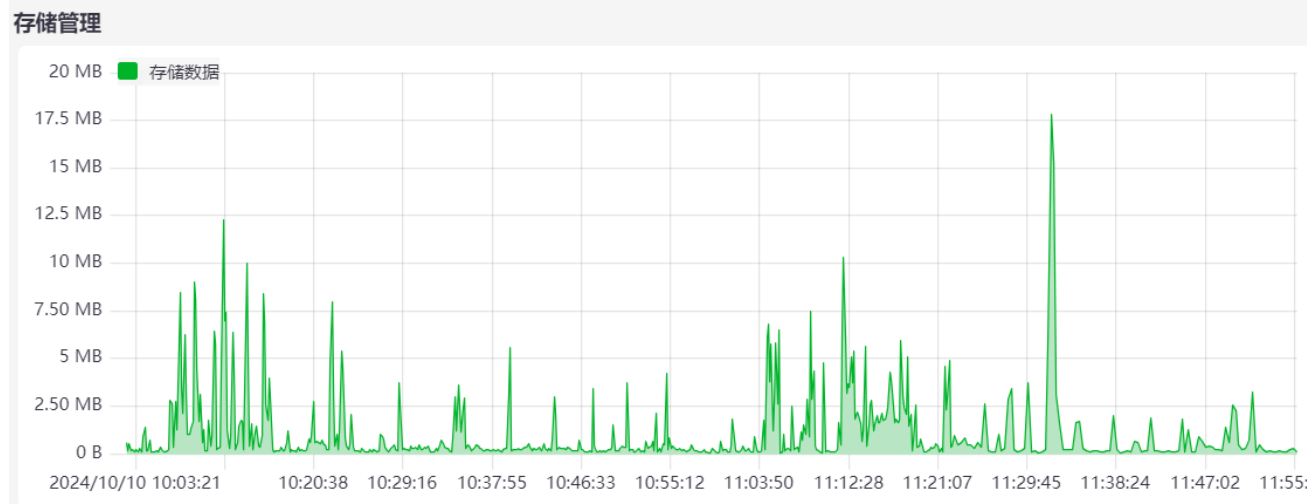


全流量回溯

- 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



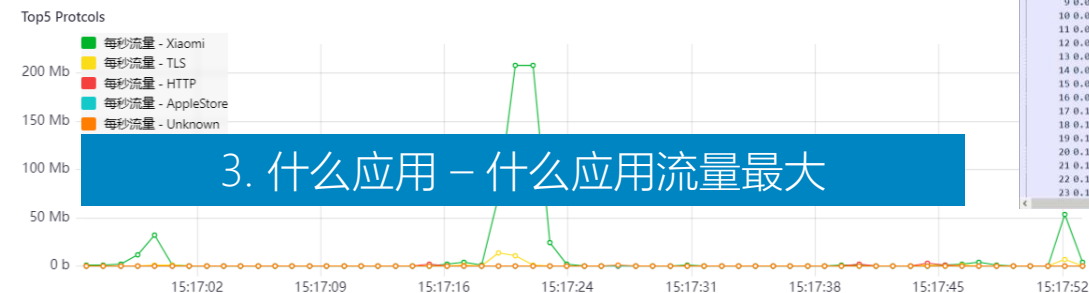
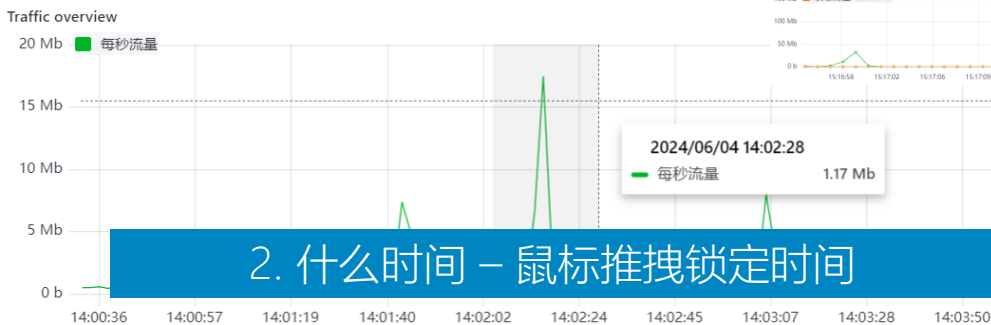
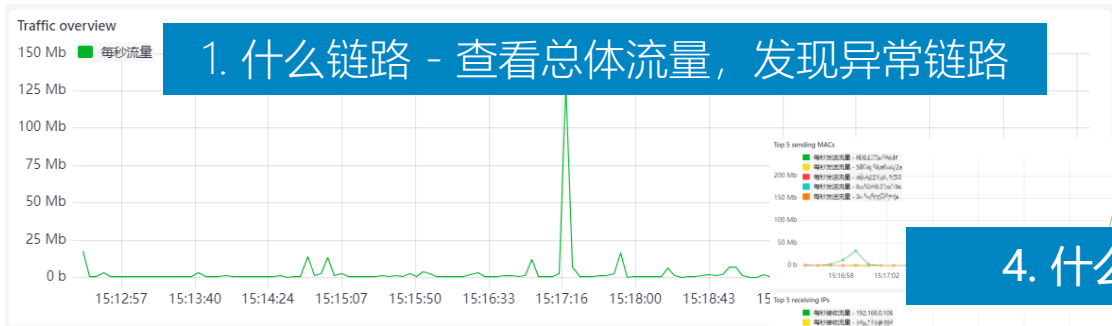
全流量回溯

- 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

2



4. 什么人 - 谁在大量产生该应用流量

5. 干了什么 - 目标对象做了什么，提取流量

5 0.045486	192.168.0.100	192.168.0.100	TCP	60 54286 -> 443 [ACK] Seq=1 Win=131328 Len=0
6 0.045492	192.168.0.100	192.168.0.100	TCP	60 54287 -> 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
7 0.045521	192.168.0.100	192.168.0.100	TLSv1.3	629 Client Hello
8 0.045528	192.168.0.100	192.168.0.100	TLSv1.3	629 Server Hello, Change Cipher Spec, Application Data
9 0.045548	192.168.0.100	192.168.0.100	TLSv1.3	1498 Server Hello, Change Cipher Spec, Application Data
10 0.045556	192.168.0.100	192.168.0.100	TCP	1498 443 -> 54287 [PSH, ACK] Seq=2889 Ack=576 Win=64128 Len=1208 [TCP segment of a r...
11 0.045562	192.168.0.100	192.168.0.100	TCP	1262 443 -> 54287 [PSH, ACK] Seq=2889 Ack=576 Win=64128 Len=1208 [TCP segment of a r...
12 0.045567	192.168.0.100	192.168.0.100	TLSv1.3	1498 Server Hello, Change Cipher Spec, Application Data
13 0.045581	192.168.0.100	192.168.0.100	TCP	1498 443 -> 54286 [PSH, ACK] Seq=1445 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
14 0.045591	192.168.0.100	192.168.0.100	TCP	1262 443 -> 54286 [PSH, ACK] Seq=2889 Ack=576 Win=64128 Len=1208 [TCP segment of a r...
15 0.045644	192.168.0.100	192.168.0.100	TCP	60 54287 -> 443 [ACK] Seq=576 Ack=2889 Win=131328 Len=0
16 0.045656	192.168.0.100	192.168.0.100	TCP	60 54286 -> 443 [ACK] Seq=576 Ack=2889 Win=131328 Len=0
17 0.045651	192.168.0.100	192.168.0.100	TCP	1498 443 -> 54287 [ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
18 0.045654	192.168.0.100	192.168.0.100	TLSv1.3	760 Application Data, Application Data
19 0.045673	192.168.0.100	192.168.0.100	TCP	60 54287 -> 443 [ACK] Seq=576 Ack=6247 Win=131328 Len=0
20 0.045683	192.168.0.100	192.168.0.100	TCP	1498 443 -> 54286 [PSH, ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
21 0.045683	192.168.0.100	192.168.0.100	TLSv1.3	760 Application Data, Application Data
22 0.045682	192.168.0.100	192.168.0.100	TCP	118 Change Cipher Spec, Application Data
23 0.045683	192.168.0.100	192.168.0.100	TLSv1.3	146 Application Data

主要功能



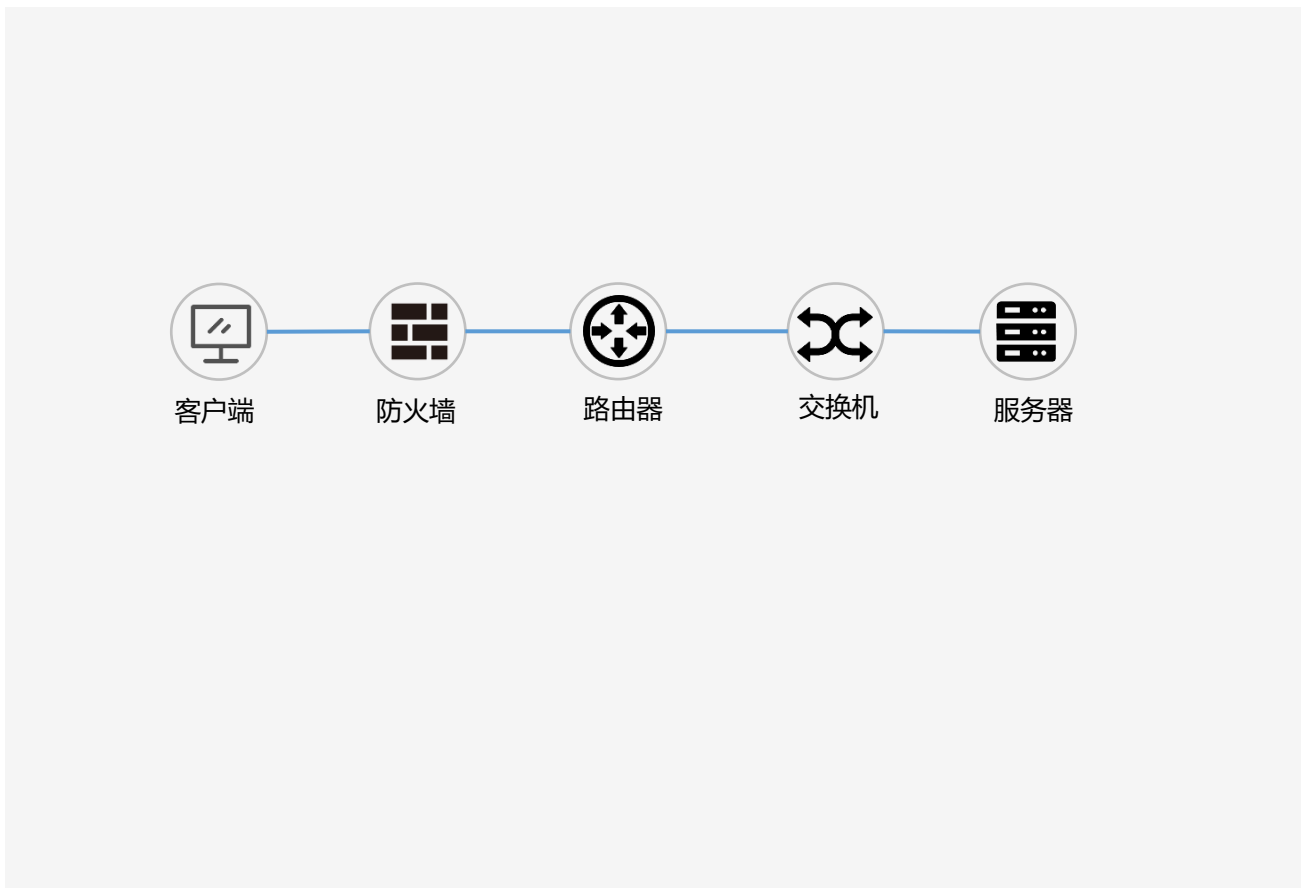
1

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

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



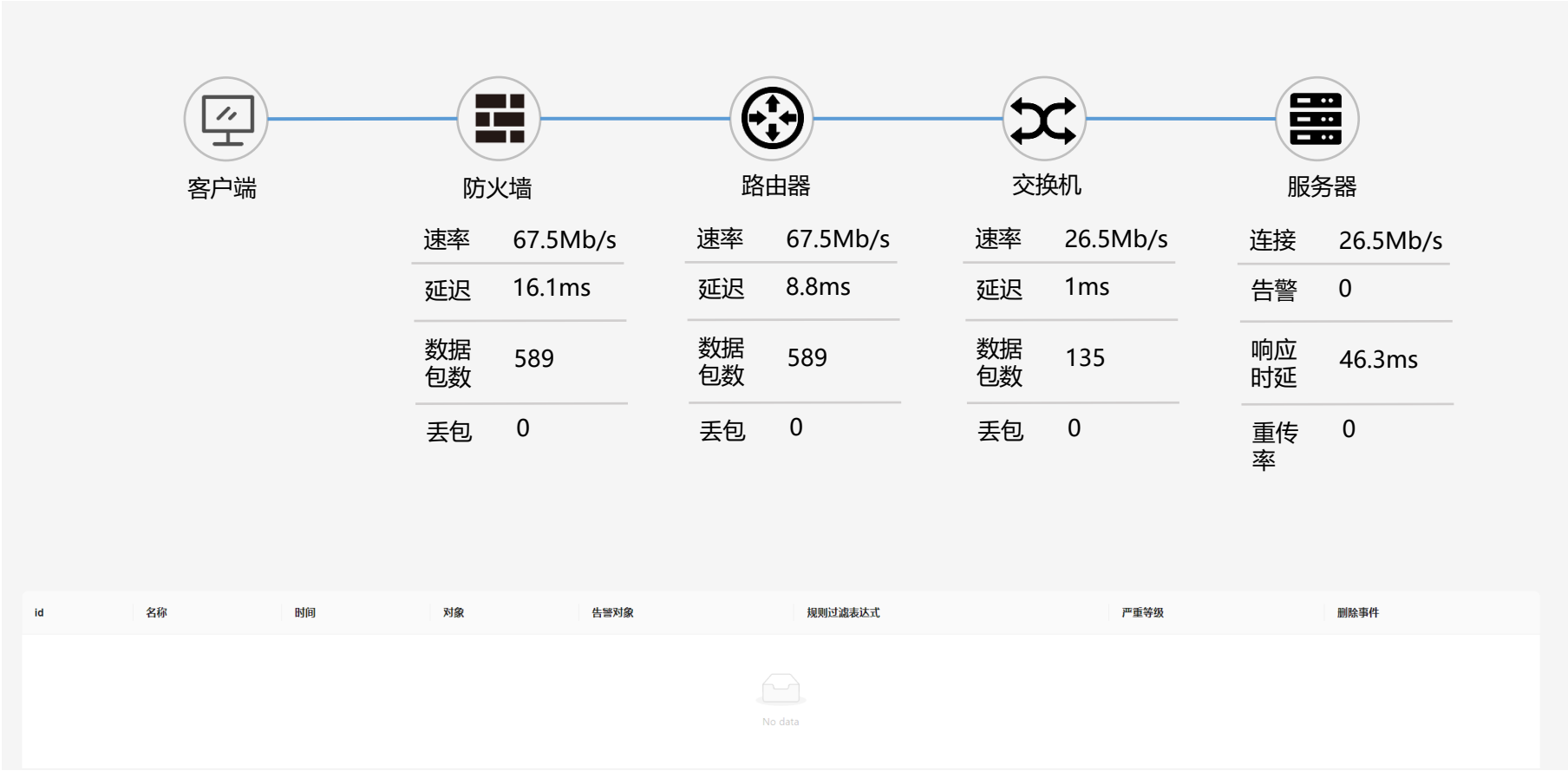
2

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



主要功能



3

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

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

