

AnaTraf 网络流量分析仪

产品介绍

——专业的网络流量分析解决方案提供商

1

网络痛点与产品价值

2

典型应用

3

产品功能介绍

4

产品线介绍

痛点 1:

随着移动通信的普及，以太网数据传输从10G逐步提升至40G、100G，网络运维面临两大挑战：一是如何确保海量数据的可靠传输，二是在网络故障时高效完成海量数据的故障诊断。

全流量采集网络故障期间的全部通信数据并存储至磁盘，借助海量数据索引和高性能内存数据库，实现快速定位问题点并提取分析。

痛点 2:

一次访问跨越接入交换机、核心路由器、防火墙、IDS/IPS、负载均衡和目标服务器，若访问出错，需快速精准定位问题点（如防火墙或负载均衡）以降低损失，这对数据传输维护至关重要。

支持对同一应用在不同采集点的数据进行关联比对分析，从而发现应用中出现的分段丢失、重传以及时延等问题，能够帮助用户快速查找与定位造成应用服务质量下降的网络节点。

痛点 3:

企业生产环境中，网络故障频发且具有突发性和不确定性，这些故障往往短暂出现又迅速恢复，难以复现，现有工具难以实时捕捉异常，各团队间的职责不清导致推诿与延误。

全流量回溯重现故障，以及简单直观的 WEB 界面实时显示L2-L7网络性能和质量指标的趋势、非常详细的统计数据 and 指标。这加快了故障排除并降低了MTTR，明确故障责任界定。

网络痛点与产品价值

传统手段 vs **AnaTraf** 流量分析

传统手段

- Ping、tracert 等工具专业性强，故障分析周期长。
- 使用笔记本进行抓包的传统方法已无法满足多方位捕获的需要。
- 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，分布式采集数据，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，监控丢包、重传、延迟等指标

大容量存储

满足数月以至更长时间的存储需求

运维工程师 网络管理员

- 避免频繁变更抓包点，原始数据包快速取证
- 网络延时、丢包KPI监测，应用性能KPI监测
- 应用访问关系梳理，告警分析处理

- 业务性能下降责任定位，网络、应用责任厘清
- 应用服务失效监测，网络和应用健康报告
- 提高运维的效率，提升运维的质量，改进用户体验

IT 部门负责人

企业

- 快速网络故障排除，缩短停机时间
- 优化网络资源分配

工业网络

- 工控网络协议和流量审计
- 关键事件监测告警
- 故障诊断与快速响应

数据中心

- 快速网络故障排除，减少停机时间
- 优化网络资源分配

IT 系统集成商

- 定制化网络解决方案设计
- 分析和优化客户网络性能

运营商

- 流量监控和管理
- 服务质量（QoS）保障
- 数据分析和报告

1

网络痛点与产品价值

2

典型应用

3

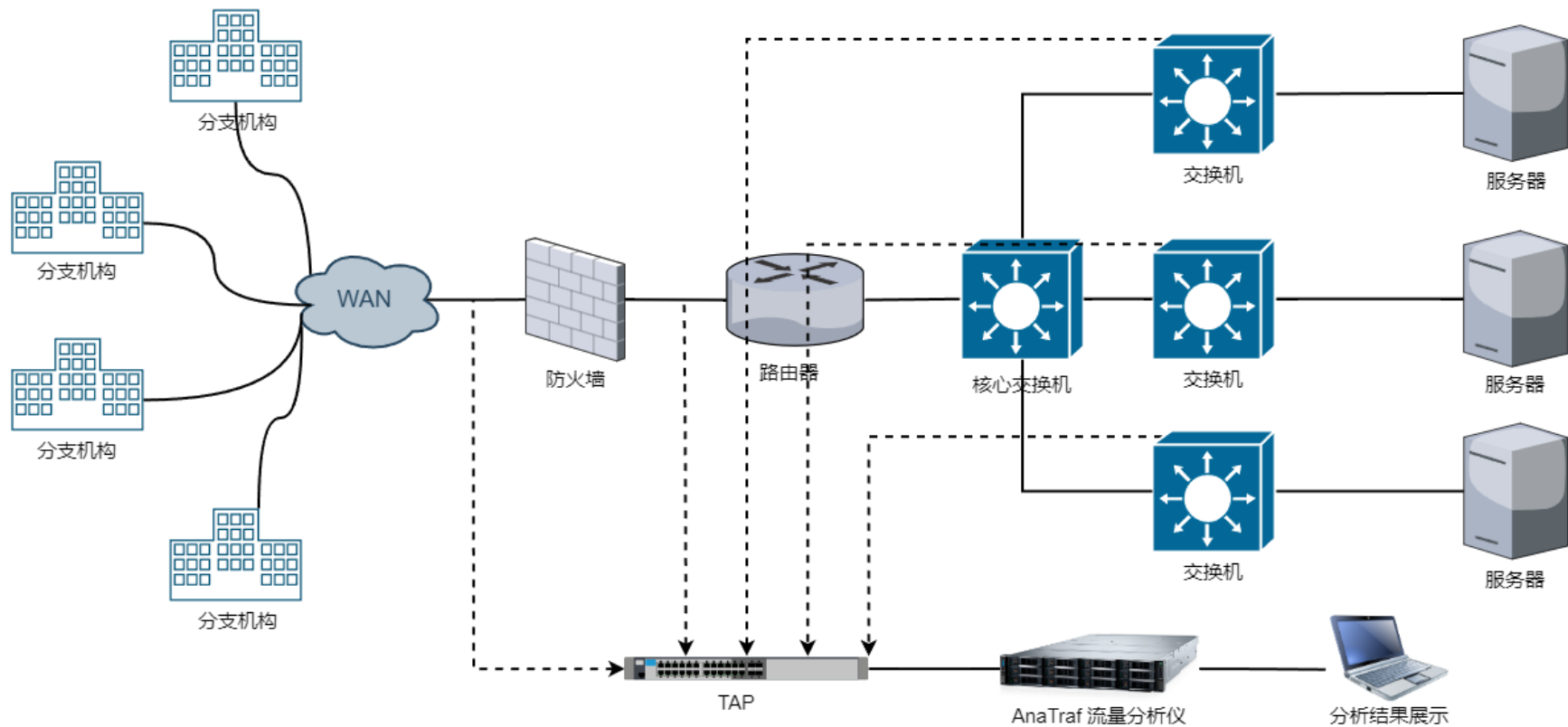
产品功能介绍

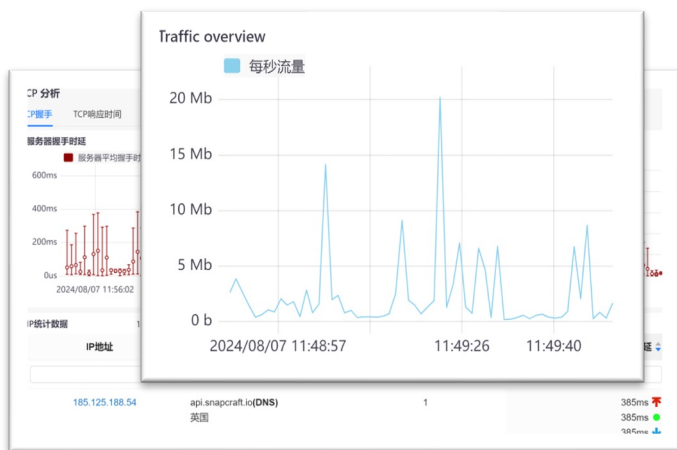
4

产品线介绍

典型部署

- 零侵入，旁路部署不影响生产环境
- 一台分析仪可监控多个网段
- 流量汇聚分析，多点数据关联分析
- 部署灵活



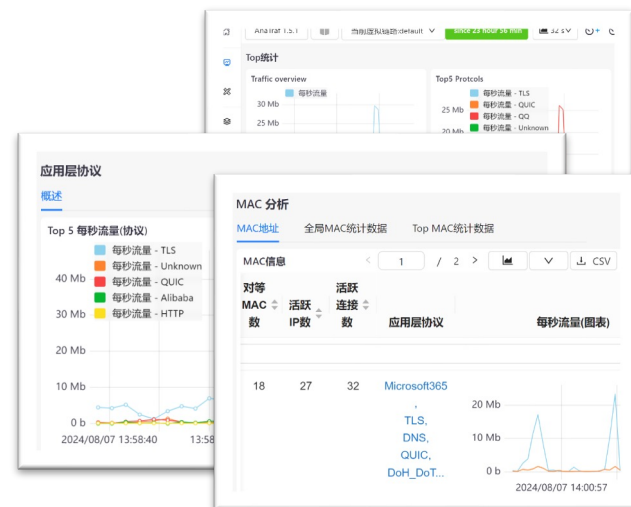


1 发现并解决网络问题

是网络、服务器、客户端还是应用程序的问题？简单直观的 WEB 界面实时显示L2-L7网络性能和质量指标的趋势、非常详细的统计数据和指标。这加快了故障排除并降低了MTTR。

2 基于报文的流量可视化和资产清单

AnaTraf 网络流量分析仪识别和捕获网络中每个设备，服务和协议通信。全面的MAC, ARP, IP, DNS, 端口, 应用协议可视化, 结合实时匹配、过滤和各种导出机制, 帮助您有效, 快速地排除故障。



3 SSL / TLS 服务器连接有效性和故障分析

AnaTraf 网络流量分析仪不仅检测所有SSL/TLS握手和数据响应时间的性能故障排除，还提供协商TLS版本，TLS警告，加密密钥强度和证书有效性信息。这些信息能够帮助您解决问题。

TLS 分析

TLS服务器 TLS响应时延

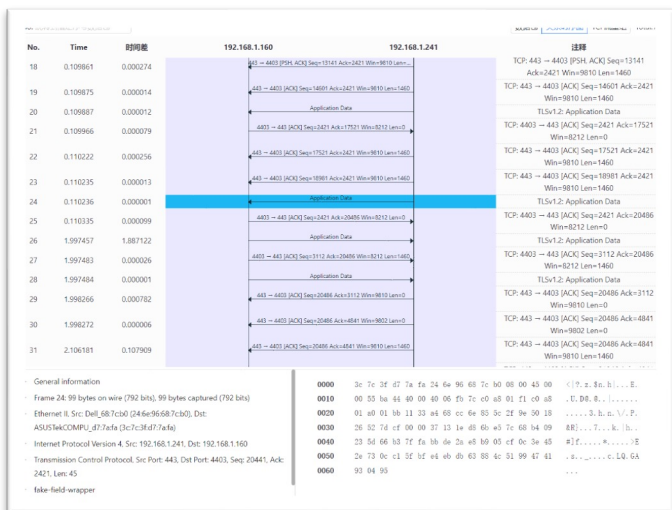
Servers < 1 / 8 > [Icon] [Dropdown] [CSV]

协商的加密算法	TLS版本	证书中服务器名称	证书发布者名称	证书主体名称
∞ TLS_AES_256_GCM_SHA384	TLS 1.3			
c TLS_ECDHE_RSA_WITH	TLS 1.2	*.mail.qq.com,	C=US, O=DigiCert,	C=CN, ST=Guangdo

客户端	防火墙	路由器	交换机	服务器
速率 67.5Mb/s	速率 67.5Mb/s	速率 26.5Mb/s	连接 26.5Mb/s	
延迟 16.1ms	延迟 8.8ms	延迟 1ms	告警 0	
数据包数 589	数据包数 589	数据包数 135	响应时延 46.3ms	
丢包 0	丢包 0	丢包 0	重传率 0	

4 多节点数据关联分析和故障排除

支持对同一应用在不同采集点的数据进行关联比对分析，从而发现应用中出现的分段丢失、重传以及时延等问题，能够帮助用户快速查找与定位造成应用服务质量下降的网络节点。

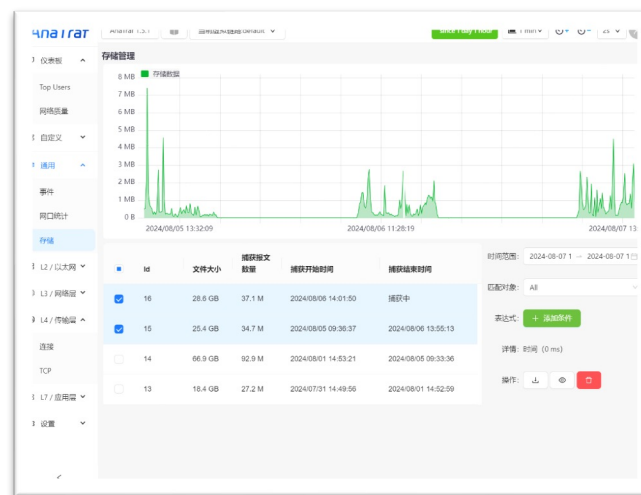


6 流量回溯重现网络故障

无论是出于故障排除、安全，还是一般数据保留的目的，网络数据包都非常有价值。AnaTraf 网络流量分析仪具备网络流量记录和回溯分析功能，在 WEB 界面上简单的点击即可过滤、提取原始流量。提取的流量可以重新导入如IDS / IPS 系统来创建特定的安全事件。

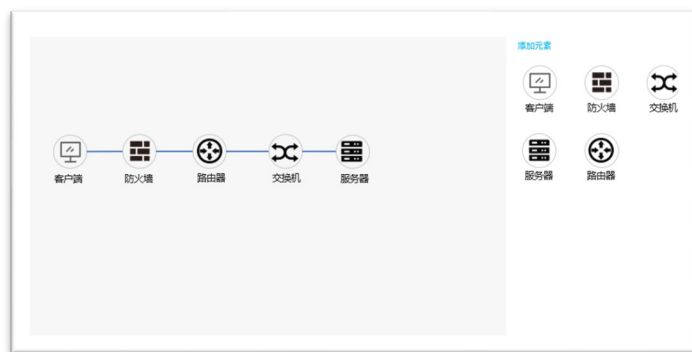
5 快速流量过滤和在线解码分析

AnaTraf 网络流量分析仪通过强大的过滤，帮助网络管理员方便地从实时网络流量或大型 pcap 文件中识别和提取感兴趣的数据包。可以选择特定的 IP、MAC，单个连接进行过滤，完全支持 Wireshark 数据包分析，也可以通过在线解码引擎进行分析。



7 工业以太网协议分析与故障排除

提供多种工业协议分析，包括 PROFINET、IEC 60870-5、IEC 61850、OPC等协议的质量监控和性能分析，防止昂贵的生产停机时间。



8 企业 OA 系统性能分析与质量监控

当企业 OA 系统没有按预期运行时，可以确定是内部还是外部引入了服务(质量)下降，并评估其影响(某些客户端、子网、全公司)。

1

网络痛点与产品价值

2

典型应用

3

产品功能介绍

4

产品线介绍

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

- 2-7 层流量可视化
- 在线解码
- 告警推送

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
- 路径测量

监控网络的持续运行状况
和可靠性

主要功能



流量可视化

- 2-7 层流量可视化
- 在线解码

分析并关联OSI 2-7层
所有元数据

L2 / 以太网 ^

MAC

ARP

VLAN

QoS

数据包统计

突发分析

L3 / 网络层 ^

IP

IP pairs

Geo IP

ICMP

QoS

L4 / 传输层 ^

连接

TCP

L7 / 应用层 ^

应用层协议

HTTP

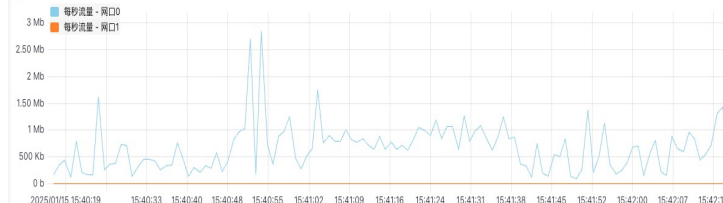
TLS

DHCP

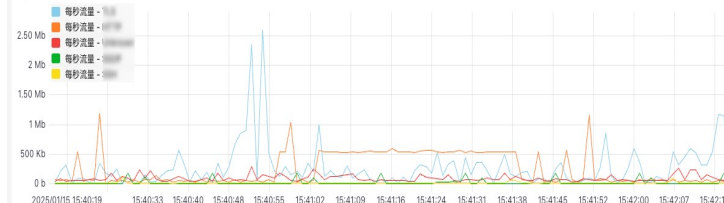
DNS

Top统计

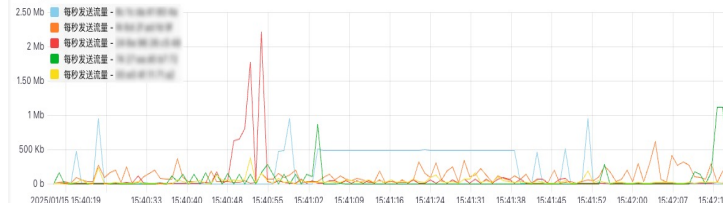
网口流量



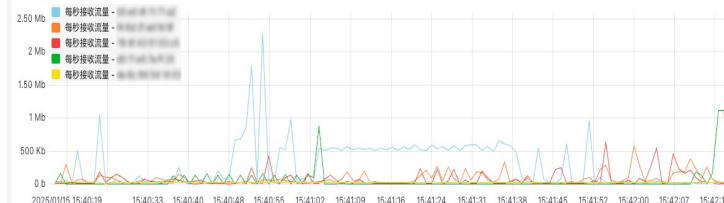
Top 5 应用协议



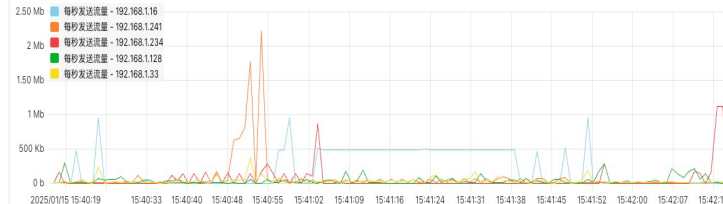
Top 5 发送 MACs



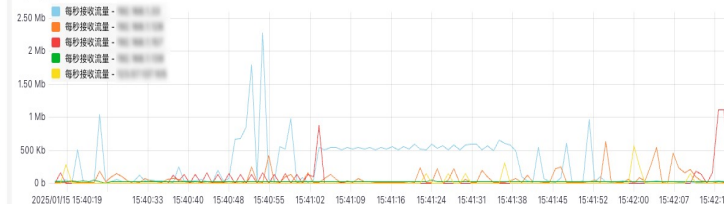
Top 5 接收 MACs



Top 5 发送 IPs



Top 5 接收 IPs



数据包在线解码分析

A bar chart showing the number of people with a university degree in the UK from 1997 to 2007. The x-axis represents the years, and the y-axis represents the number of people in millions. The bars show a general upward trend, with a slight dip in 2006.

Year	Number of people (millions)
1997	2.5
1998	2.8
1999	3.0
2000	3.2
2001	3.5
2002	3.8
2003	4.0
2004	4.2
2005	4.3
2006	4.1
2007	4.2

流量可视化

- 2-7 层流量可视化
- 在线解码
- 告警推送

分析并关联OSI 2-7层 所有元数据



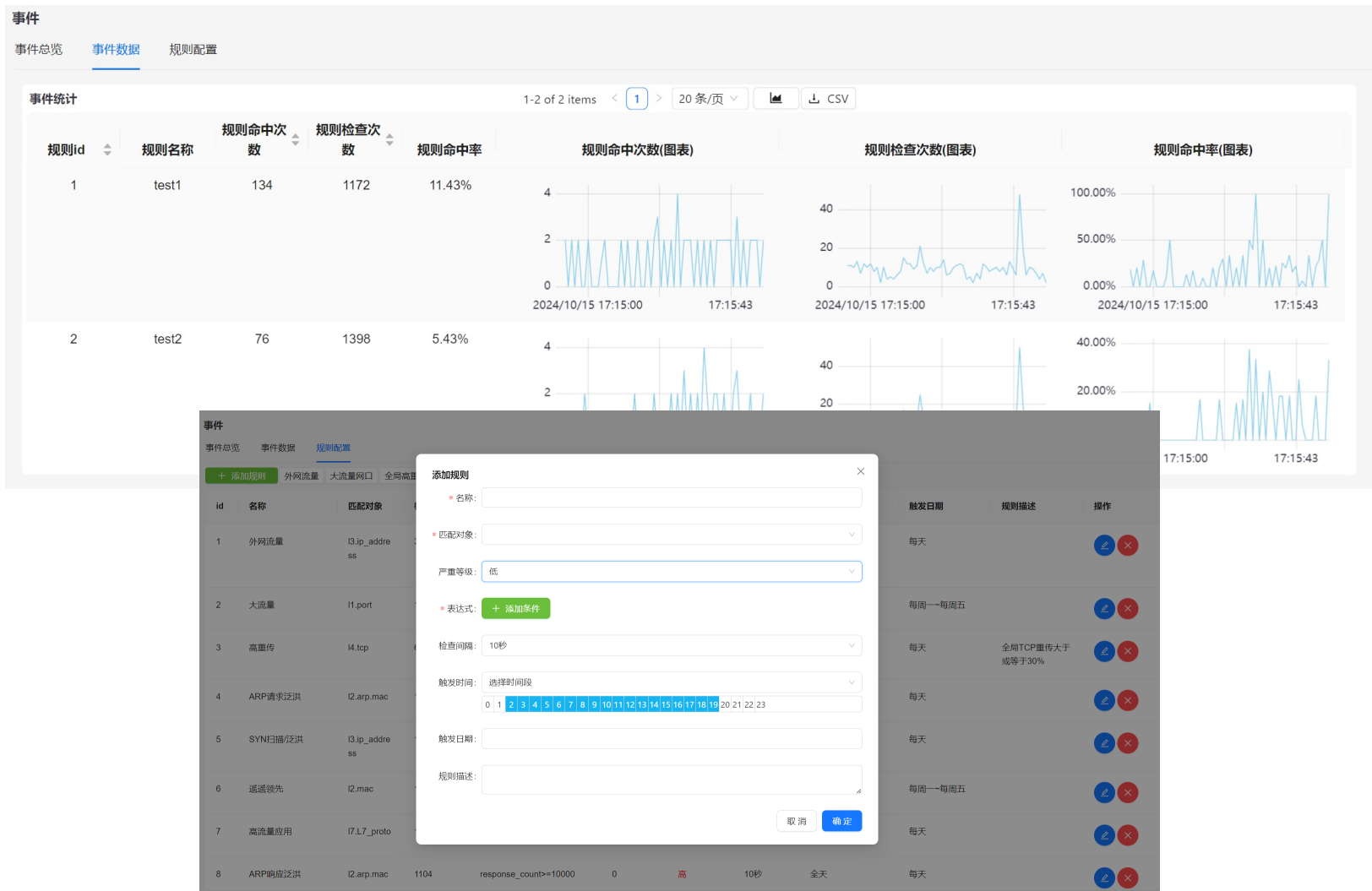
主要功能



流量可视化

- 2-7 层流量可视化
- 在线解码
- 告警推送

分析并关联OSI 2-7层
所有元数据



大容量数据存储与检索

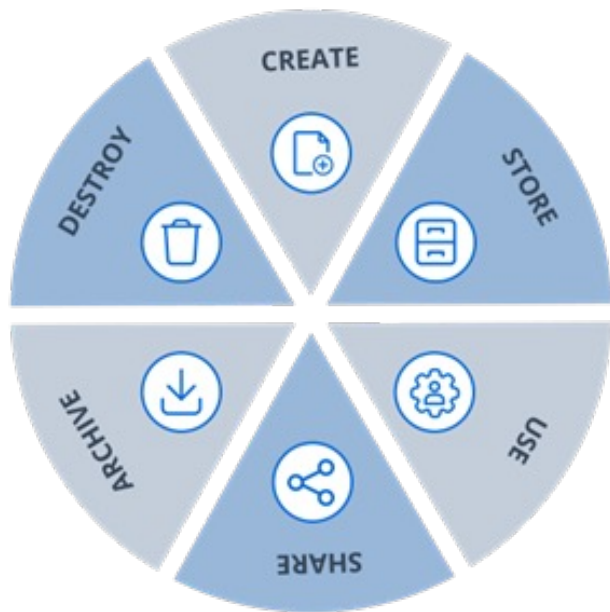
主要功能



全流量回溯

- 全流量存储
- 全流量回溯
- 溯源取证

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



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。

满足等保测评180天流量回溯分析要求

主要功能

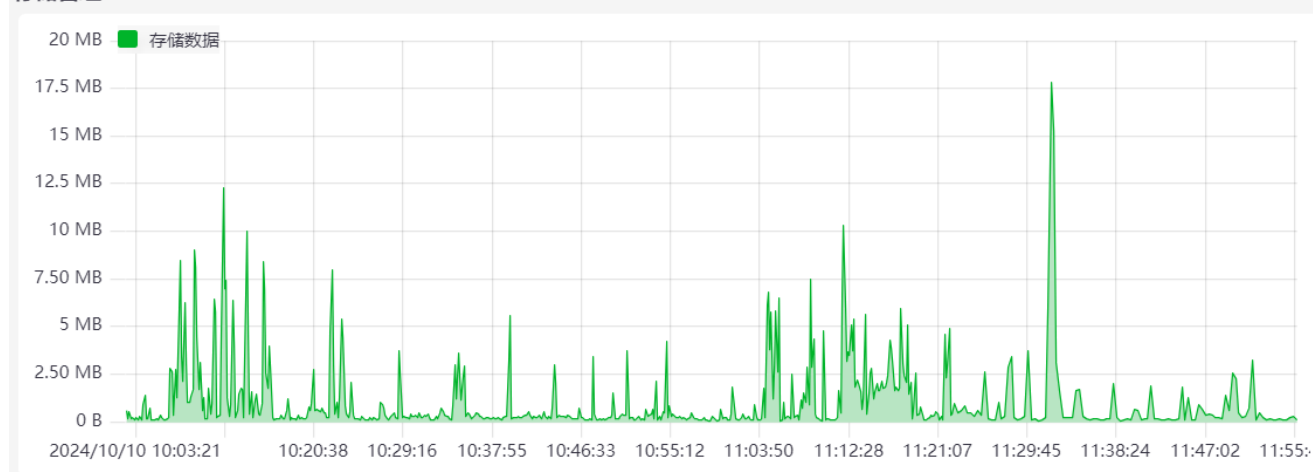


全流量回溯

- 全流量存储
- 全流量回溯
- 溯源取证

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

存储管理



- 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。

会话级流量回溯

主要功能

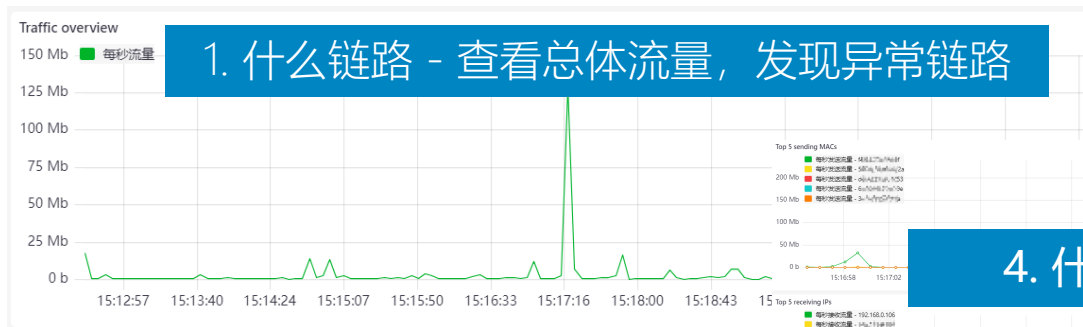


全流量回溯

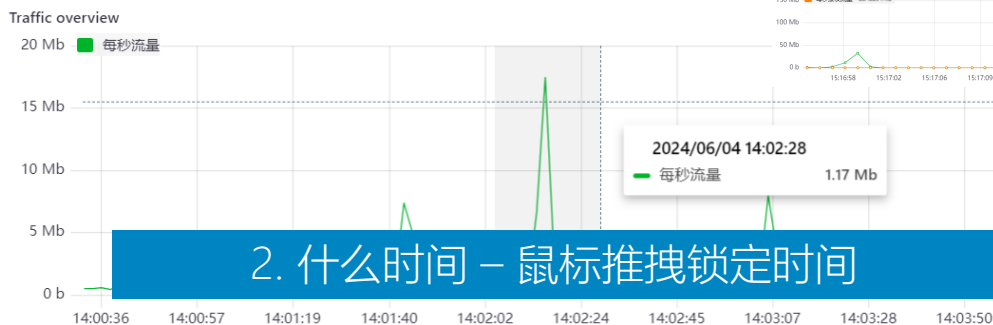
- 全流量存储
- 全流量回溯
- 溯源取证

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

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

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	TCP	1498 443 → 54287 [PSH, ACK] Seq=1445 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
10 0.045558	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...
11 0.045568	192.168.0.100	192.168.0.100	TCP	1498 443 → 54287 [PSH, ACK] Seq=1445 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
12 0.045578	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...
13 0.045588	192.168.0.100	192.168.0.100	TCP	60 54287 → 443 [ACK] Seq=576 Ack=2889 Win=131328 Len=0
14 0.045598	192.168.0.100	192.168.0.100	TCP	60 54286 → 443 [ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
15 0.045608	192.168.0.100	192.168.0.100	TCP	1498 443 → 54287 [PSH, ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
16 0.045618	192.168.0.100	192.168.0.100	TCP	60 54286 → 443 [ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
17 0.045628	192.168.0.100	192.168.0.100	TCP	1498 443 → 54287 [PSH, ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
18 0.045638	192.168.0.100	192.168.0.100	TCP	60 54286 → 443 [ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
19 0.045648	192.168.0.100	192.168.0.100	TCP	1498 443 → 54287 [PSH, ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
20 0.045658	192.168.0.100	192.168.0.100	TCP	60 54286 → 443 [ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
21 0.045668	192.168.0.100	192.168.0.100	TCP	1498 443 → 54287 [PSH, ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
22 0.045678	192.168.0.100	192.168.0.100	TCP	60 54286 → 443 [ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
23 0.045688	192.168.0.100	192.168.0.100	TCP	1498 443 → 54287 [PSH, ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...

3. 什么应用 - 什么应用流量最大



主要功能



全流量回溯

- 全流量存储
- 全流量回溯
- 溯源取证

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

典型溯源取证方式

1

时间段+五元组等条件检索



1. 已知攻击者或被攻击者IP等线索
2. 溯源每条行为记录和攻击行为

2

检索溯源取证导出证据



1. 已知攻击者或被攻击者IP等线索
2. 对攻击行为**取证**，**导出pcap文件**

3

元数据溯源取证



1. 已知协议（HTTP、DNS等）
2. 已知攻击特征（URL、域名等）
3. 通过元数据检索取证

4

数据回放检测取证



1. **0day攻击**溯源取证
2. 对历史数据进行**二次检测**
3. 研究攻击手法

自定义业务监控

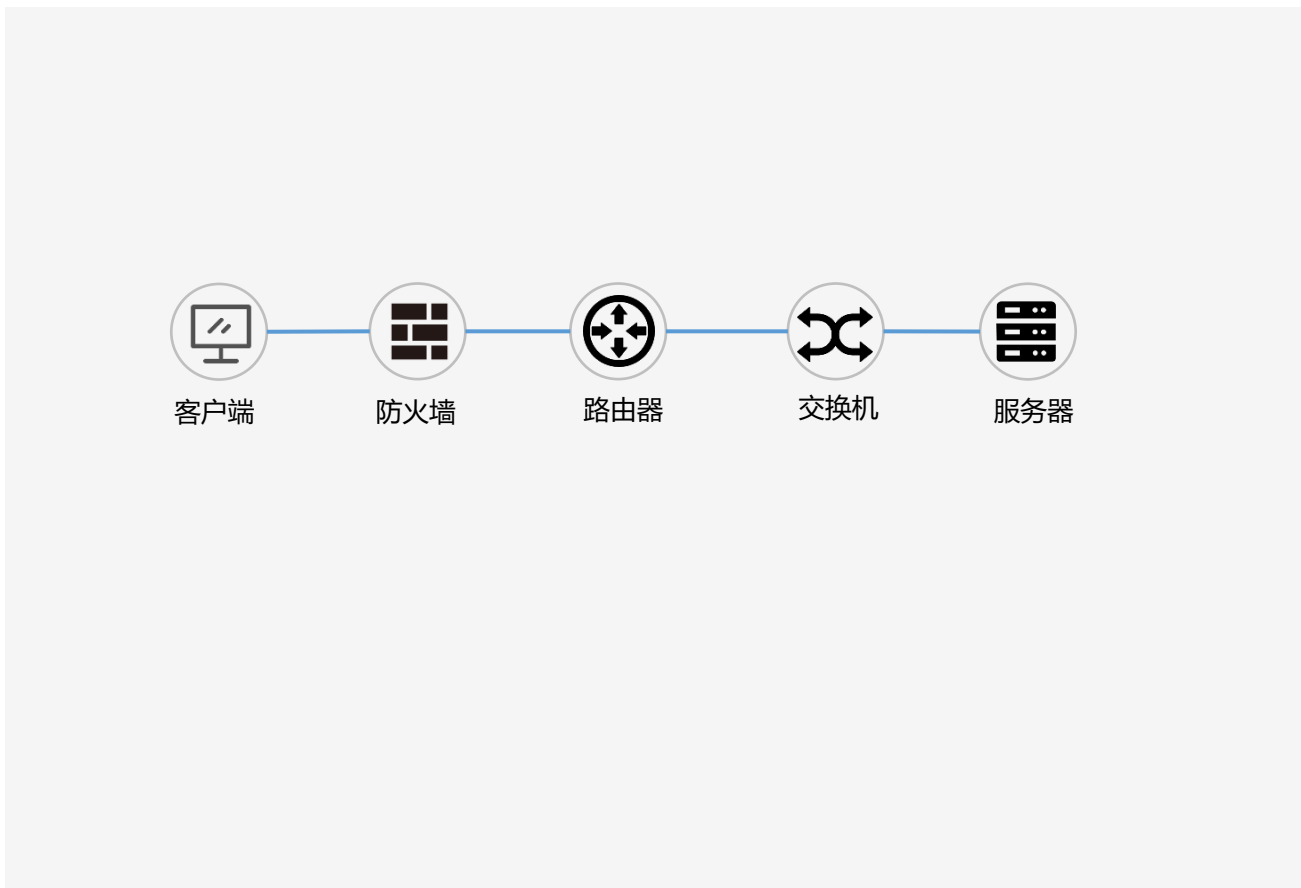
主要功能



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
- 路径测量

监控网络的持续运行状况
和可靠性



添加元素



客户端



防火墙



交换机



服务器



路由器

多点关联故障定位

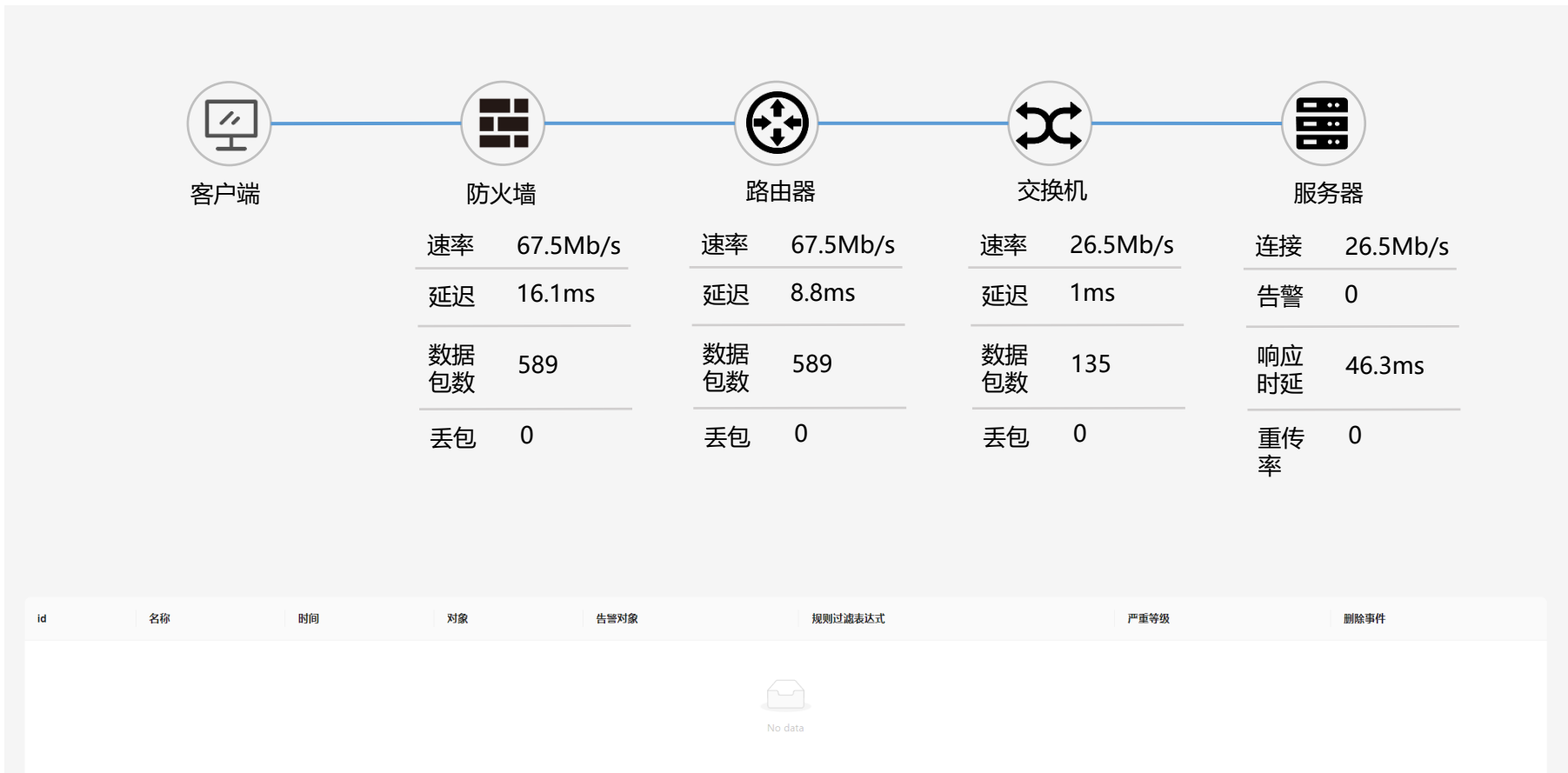
主要功能



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
- 路径测量

监控网络的持续运行状况
和可靠性



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
- 路径测量

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

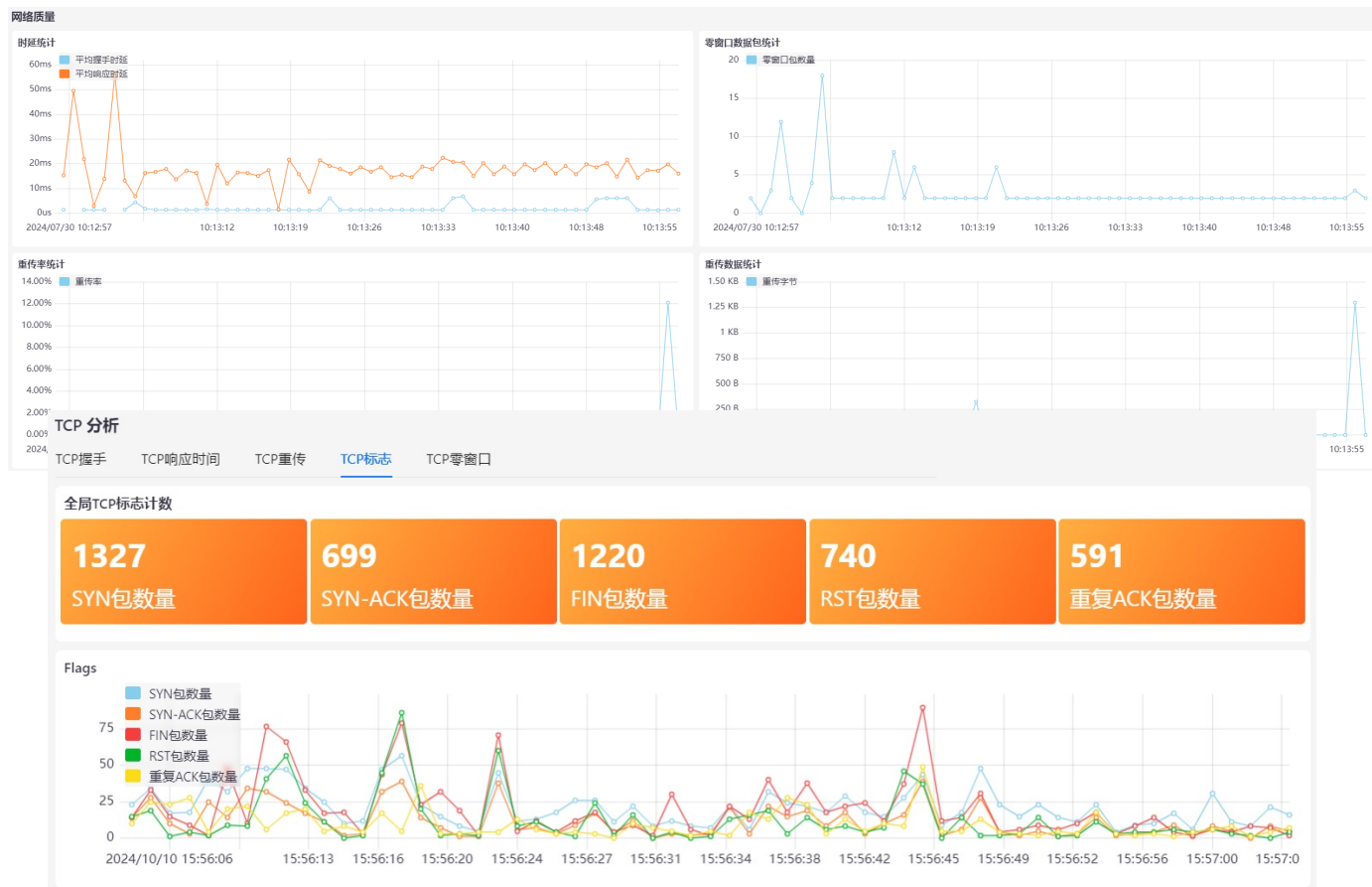
客户/服务网络时延
TCP 响应时延
TCP 重传, 丢包, 乱序

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



路径测量

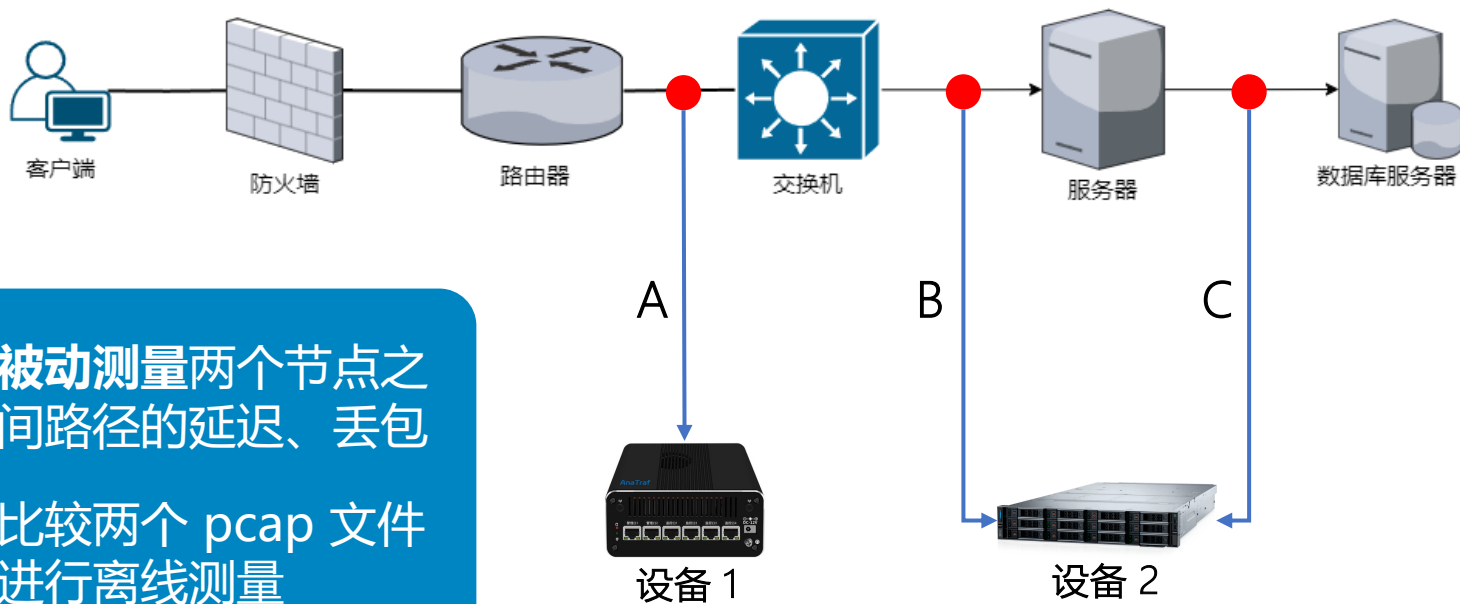
主要功能



网络性能监控

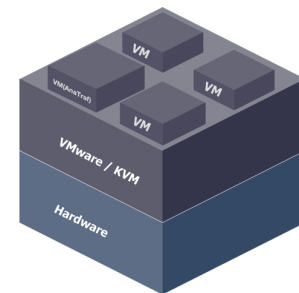
- 自定义业务监控
- 多点关联故障定位
- 关键性能指标监控
- **路径测量**

监控网络的持续运行状况
和可靠性



- **被动测量**两个节点之间路径的延迟、丢包
- 比较两个 pcap 文件进行离线测量
- 单设备与多设备均可进行测量

单设备路径测量: B(虚拟链路) $\rightleftharpoons$ C(虚拟链路)
多设备路径测量: A(设备 1) $\rightleftharpoons$ B 或 C (设备 2)



产品	AnaTraf 便携式	AnaTraf 机架式	AnaTraf 机架式	AnaTraf 机架式	AnaTraf 虚拟化
描述	方便携带, 适用于小型网络	小型网络	大型网络	大型网络	VM Ware / KVM
内存	8 GB	可拓展	可拓展	可拓展	-
存储容量	2 TB	可拓展	可拓展	可拓展	-
管理接口	10/100/1000baseT	10/100/1000baseT	10/100/1000baseT	10/100/1000baseT	-
重量	2kg	NA	NA	NA	-
尺寸	132 x 146 x 60 mm	1U	2U	4U	-

联系专业的售前工程师了解选型以及确认具体的设备配置。

