AnaTraf 云争 YUNZHENG TECH

全流量溯源分析

什么是全流量？

------网络所有**原始流量**的存储、分析

为什么需要全流量?

1. 信息安全保障：再高级的威胁、攻击都会产生流量
2. 满足合规要求：网络安全等级保护2.0要求部署全流量回溯
3. 事件调查取证：还原过程，责任界定

传统手段弊端

问题难复现、难定位

过一会自己又好了

告警太多无法分析

粒度粗，检索慢，缺乏原始场景的数据，效率低，最后也懒得看

安全问题难以追溯

只有日志信息，无法做到对攻击的完整取证和溯源

传统手段 VS 全流量回溯分析

- 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。

- √ 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。

万无一失的办法

------**网络全流量分析**

全方向

- 网络出口
- 内网核心

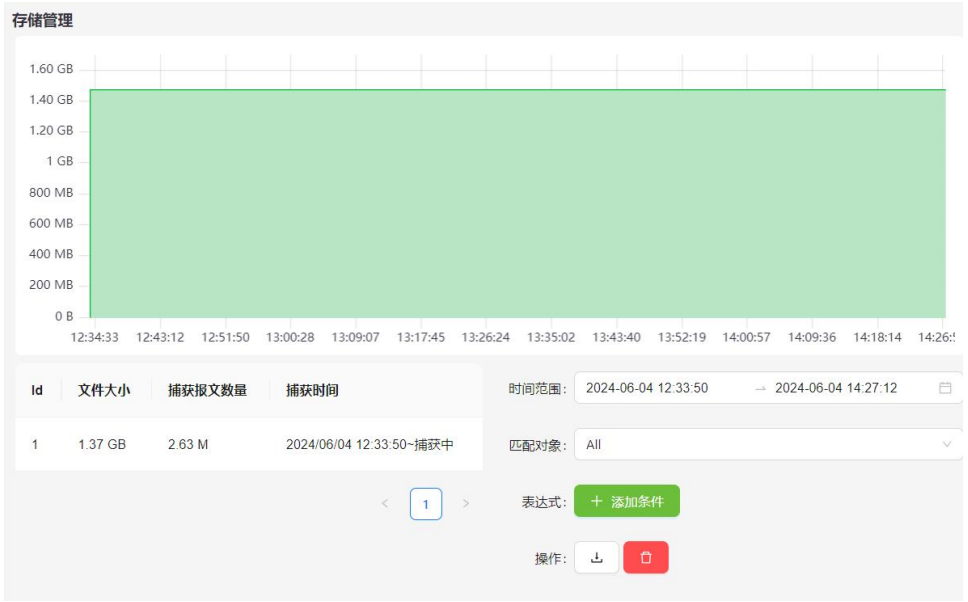
+

全流量

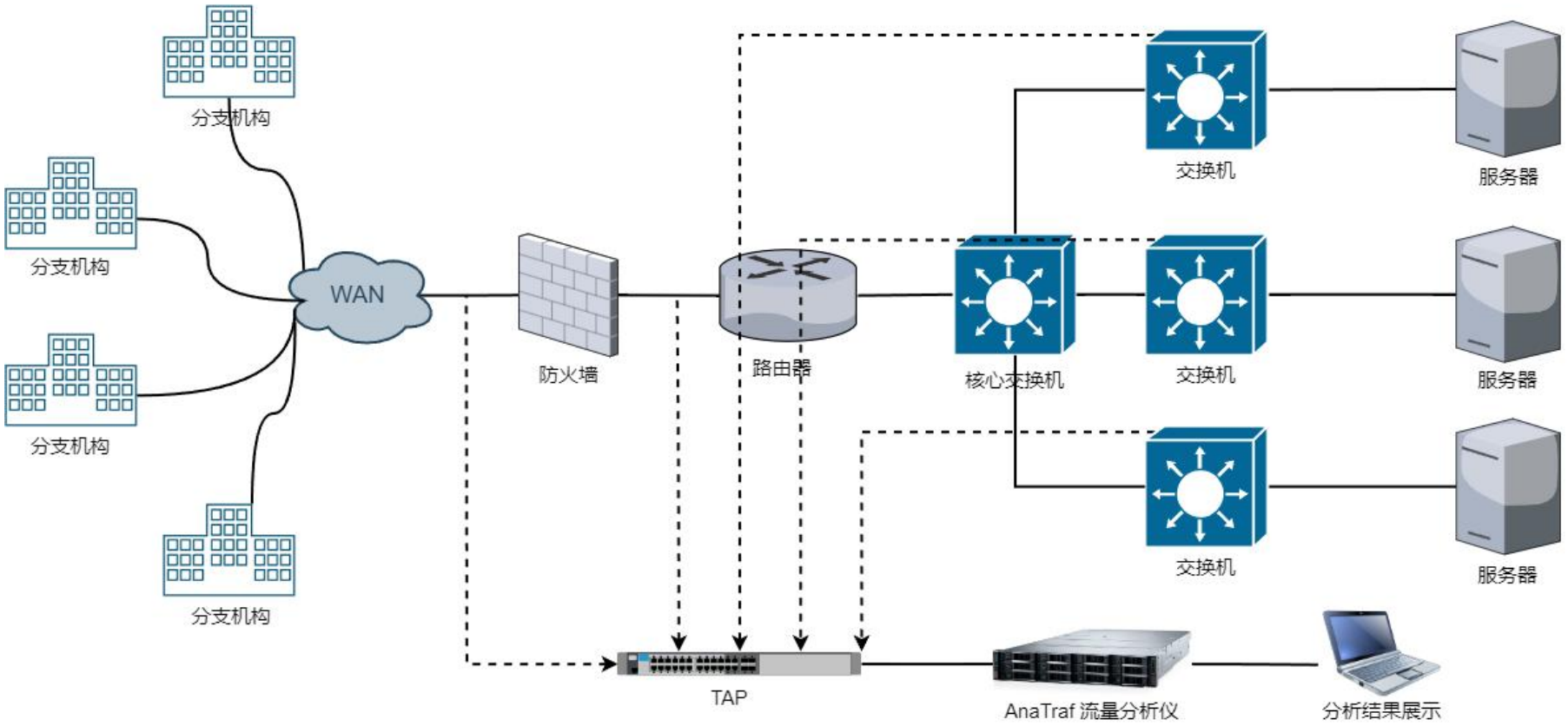
- 流量分析
- 协议识别
- 全数据存储

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。



典型部署



主要功能

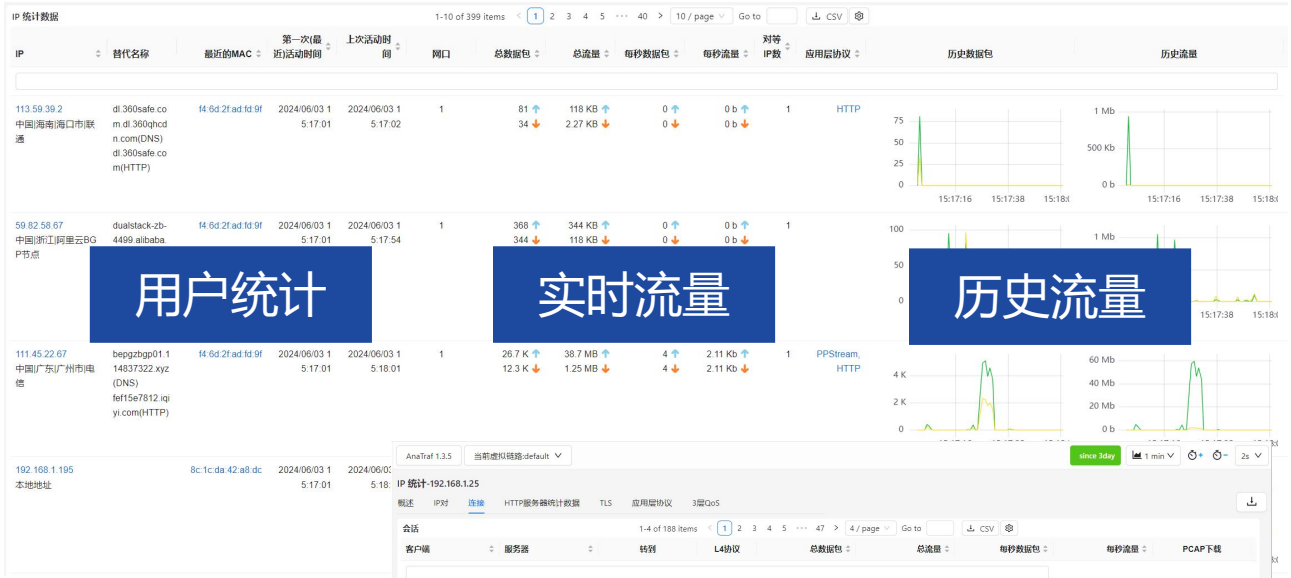
流量可视化

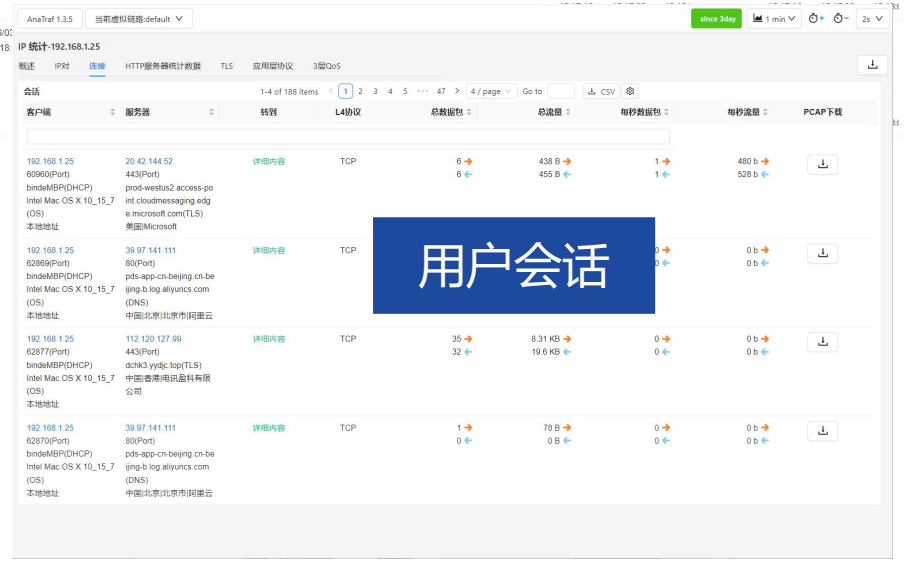
- 2-7层流量透视
- 用户流量可视化
- 应用流量可视化
- 服务器流量可视化

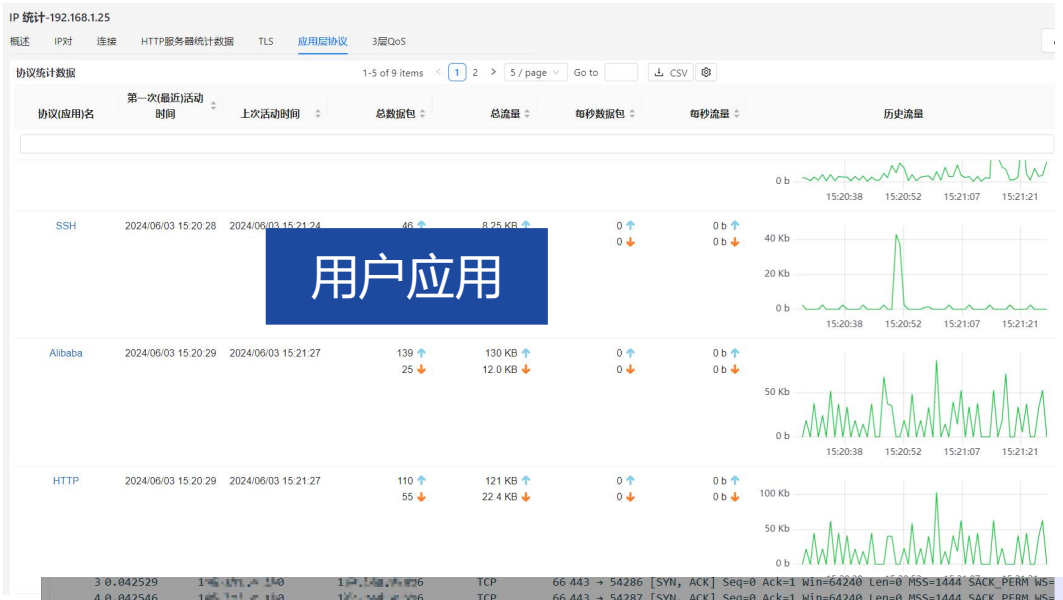
流量回溯分析

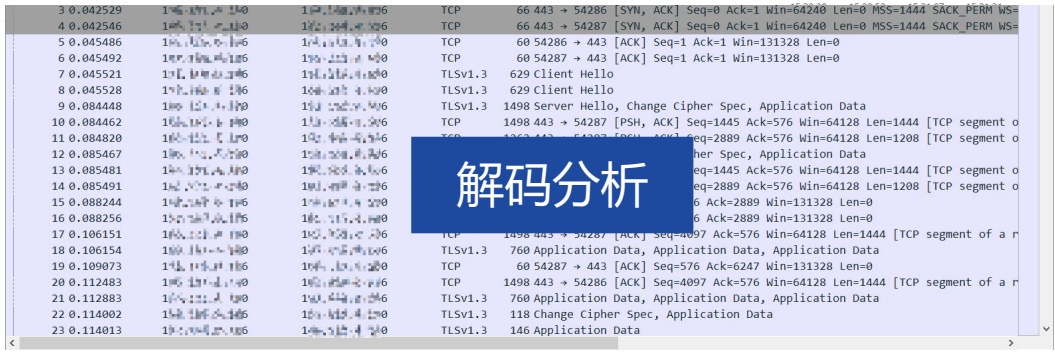
- 深度钻取
- 秒级响应
- 网络取证
- 故障重现
- 全流量留存

用户流量可视化



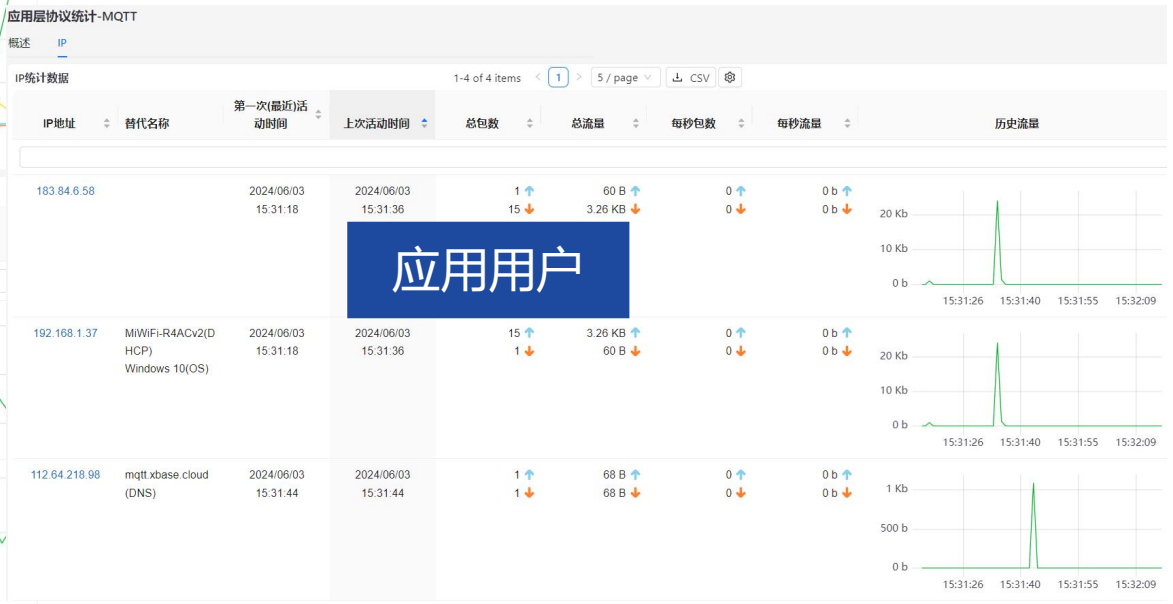






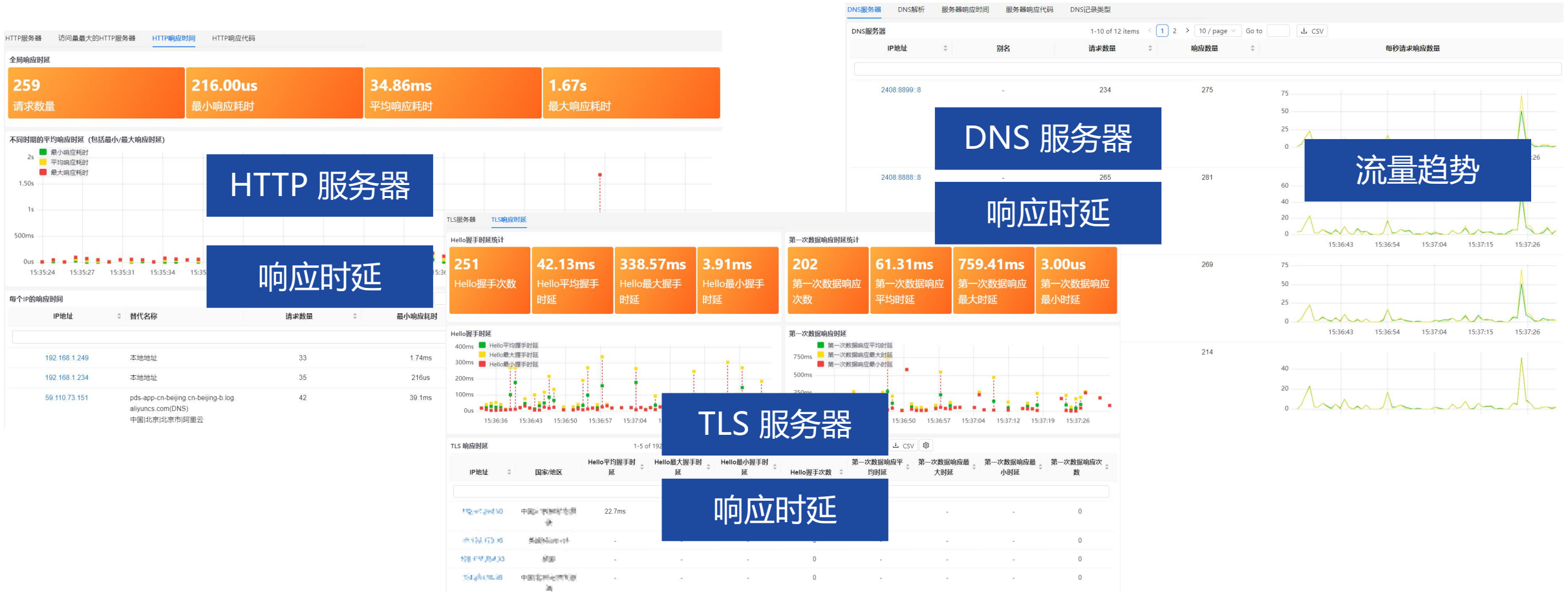
AnaTraf 云争 YUNZHENG TECH

应用流量可视化



AnaTraf 云争 YUNZHENG TECH

服务器流量可视化



全流量回溯分析

全流量存储

- 长期全流量留存
- 自定义存储策略
- 自定义流量过滤

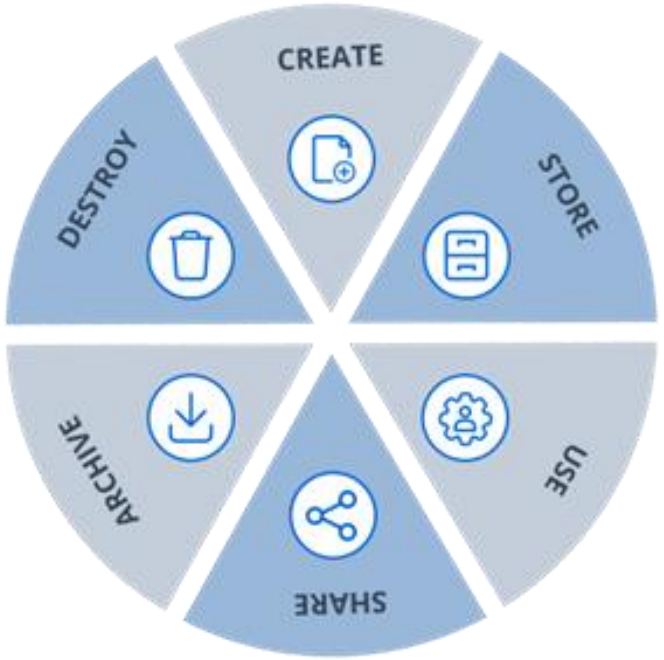
流量回溯

- 深度钻取，秒级响应
- 交互式图表
- 数据包在线解码引擎

网络取证

- 回查历史的异常行为
- 原始流量提取

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

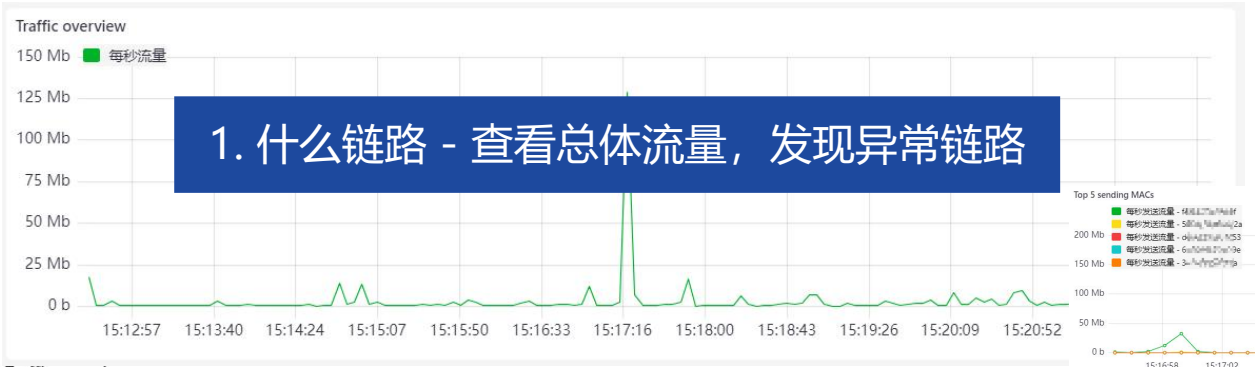
自研高性能内存数据库，数据秒级检索。
支持基于网口、VLAN等方式配置虚拟链路接口，每条虚拟链路所有统计数据都是严格区分。

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。

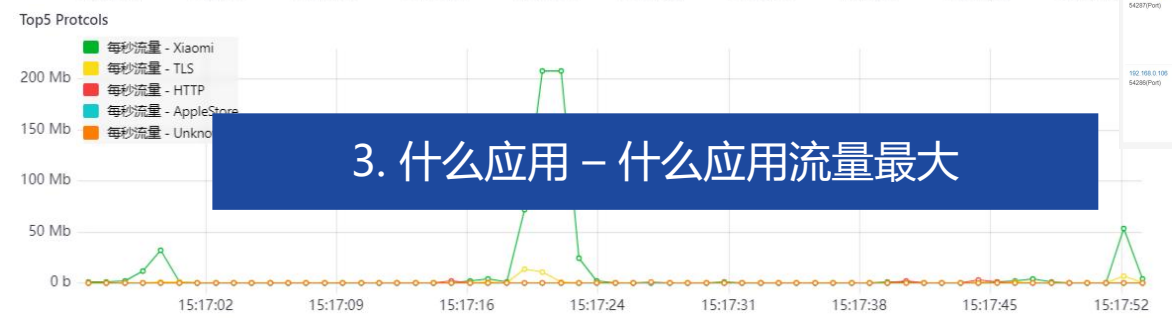
全流量回溯分析功能

会话级流量溯源分析取证

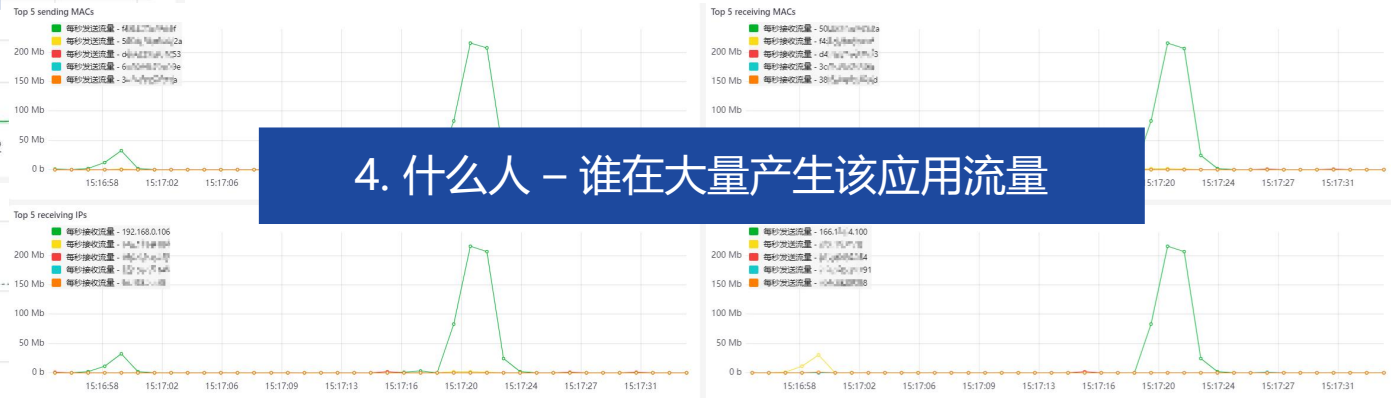


1. 什么链路 - 查看总体流量，发现异常链路

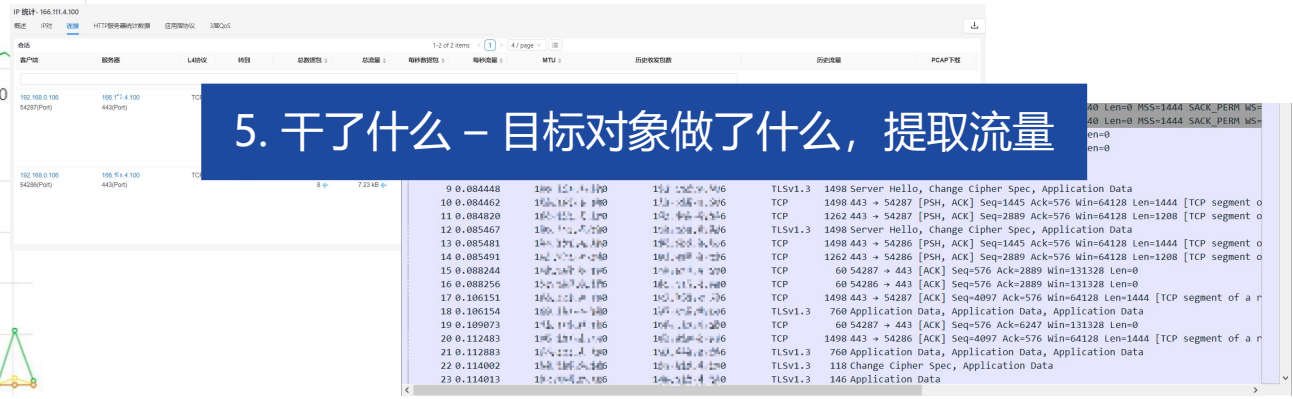
2. 什么时间 – 鼠标推拽锁定时间



3. 什么应用 – 什么应用流量最大



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

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
2	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
2	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

全流量回溯分析功能

YUNZHENG TECH

数据包在线解码分析

No. 跳转到指定序号数据包 Total:27

No.	Time	Length	Source	Destination	Protocol	Info
1	0.000000	66	192.168.1.144	192.168.1.16	TCP	53414 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000717	66	192.168.1.16	192.168.1.144	TCP	80 → 53414 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	0.001314	60	192.168.1.144	192.168.1.16	TCP	53414 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
4	0.001440	400	192.168.1.144	192.168.1.16	HTTP	GET /status/port HTTP/1.1
5	0.001976	60	192.168.1.16	192.168.1.144	TCP	80 → 53414 [ACK] Seq=1 Ack=347 Win=64128 Len=0
6	0.001986	216	192.168.1.16	192.168.1.144	TCP	HTTP/1.1 200 OK
7	0.048192	60	192.168.1.144	192.168.1.16	TCP	53414 → 80 [ACK] Seq=347 Ack=163 Win=131072 Len=0
8	0.093942	1322	192.168.1.16	192.168.1.144	HTTP	HTTP/1.1 200 OK (application/json)
9	0.138736	60	192.168.1.144	192.168.1.16	TCP	53414 → 80 [ACK] Seq=347 Ack=1431 Win=129792 Len=0
10	2.358042	400	192.168.1.144	192.168.1.16	HTTP	GET /status/port HTTP/1.1
11	2.359916	216	192.168.1.16	192.168.1.144	TCP	HTTP/1.1 200 OK
12	2.408872	60	192.168.1.144	192.168.1.16	TCP	53414 → 80 [ACK] Seq=693 Ack=1593 Win=131328 Len=0
13	2.409620	1322	192.168.1.16	192.168.1.144	HTTP	HTTP/1.1 200 OK (application/json)
14	2.454390	60	192.168.1.144	192.168.1.16	TCP	53414 → 80 [ACK] Seq=693 Ack=2861 Win=130048 Len=0
15	3.555555	519	192.168.1.144	192.168.1.16	HTTP	POST /status/reset_stream HTTP/1.1 (application/json)
16	3.556330	214	192.168.1.16	192.168.1.144	TCP	HTTP/1.1 200 OK
17	3.608024	60	192.168.1.144	192.168.1.16	TCP	53414 → 80 [ACK] Seq=1158 Ack=3021 Win=129792 Len=0
18	3.608700	83	192.168.1.16	192.168.1.144	HTTP	HTTP/1.1 200 OK (application/json)

- General information
- Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
- Ethernet II, Src: XiaomiMobile_ab:1f:53 (d4:da:21:ab:1f:53), Dst: AnntecTechno_1:80:4a (8c:1c:da:41:80:4a)
- Internet Protocol Version 4, Src: 192.168.1.144, Dst: 192.168.1.16
- Transmission Control Protocol, Src Port: 53414, Dst Port: 80, Seq: 347, Ack: 1431, Len: 0
- Wireshark Columns

```
0000   8c 1c da 41 80 4a d4 da 21 ab 1f 53 08 00 45 00   ...A.J..!..S..E.
0010   00 28 53 4c 40 00 7f 06 24 93 c0 a8 01 90 c0 a8   .(SL@...$.......
0020   01 10 d0 a6 00 50 43 f6 2c 68 7e 05 03 80 50 10   .....PC.,h~...P.
0030   01 fb 67 0e 00 00 00 00 01 10 d0 a6               ..g.........
```

HTTP记录分析

IP	URL	时间	域名	文件名	文件大小	请求方式
192.168.1.111	http://bepshbgp01.114837322.xyz/download/11345674.xlsx	2024/7/12 10:23:45	bepshbgp01.114837322.xyz	11345674.xlsx	12.5KB	GET
192.168.1.234	http://dcpsj.dlb.mob.com/download/image.png	2024/7/12 11:15:30	dcpsj.dlb.mob.com	image.png	8.7KB	GET
192.168.1.249	http://s.f.qh-lb.com/download/tmp3.png	2024/7/12 12:05:20	s.f.qh-lb.com	tmp3.png	5.3MB	GET
192.168.1.195	http://entry.apm.music.ntes53.netease.com/download/video.mp4	2024/7/12 13:42:50	entry.apm.music.ntes53.netease.com	video.mp4	45.2KB	GET
192.168.1.195	http://entry.apm.music.ntes53.netease.com/download/2024-06-28-09-58-25-085.pcap	2024/7/12 14:18:10	entry.apm.music.ntes53.netease.com	2024-06-28-09-58-25-085.pcap	20.1KB	GET

AnaTraf 云争 YUNZHENG TECH

THANKS! 谢谢!

www.anatraf.com