

AnaTraf 网络流量分析仪

全流量回溯分析

为什么需要全流量分析？

- 1 信息安全保障
- 2 满足合规要求
- 3 事件调查取证

全流量

---网络所有原始流量的存储、分析

- 再高级的威胁、攻击都会产生流量
- 网络安全等级保护2.0要求部署全流量回溯
- 还原过程，责任界定

全方向

---网络出口 & 内网核心

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...

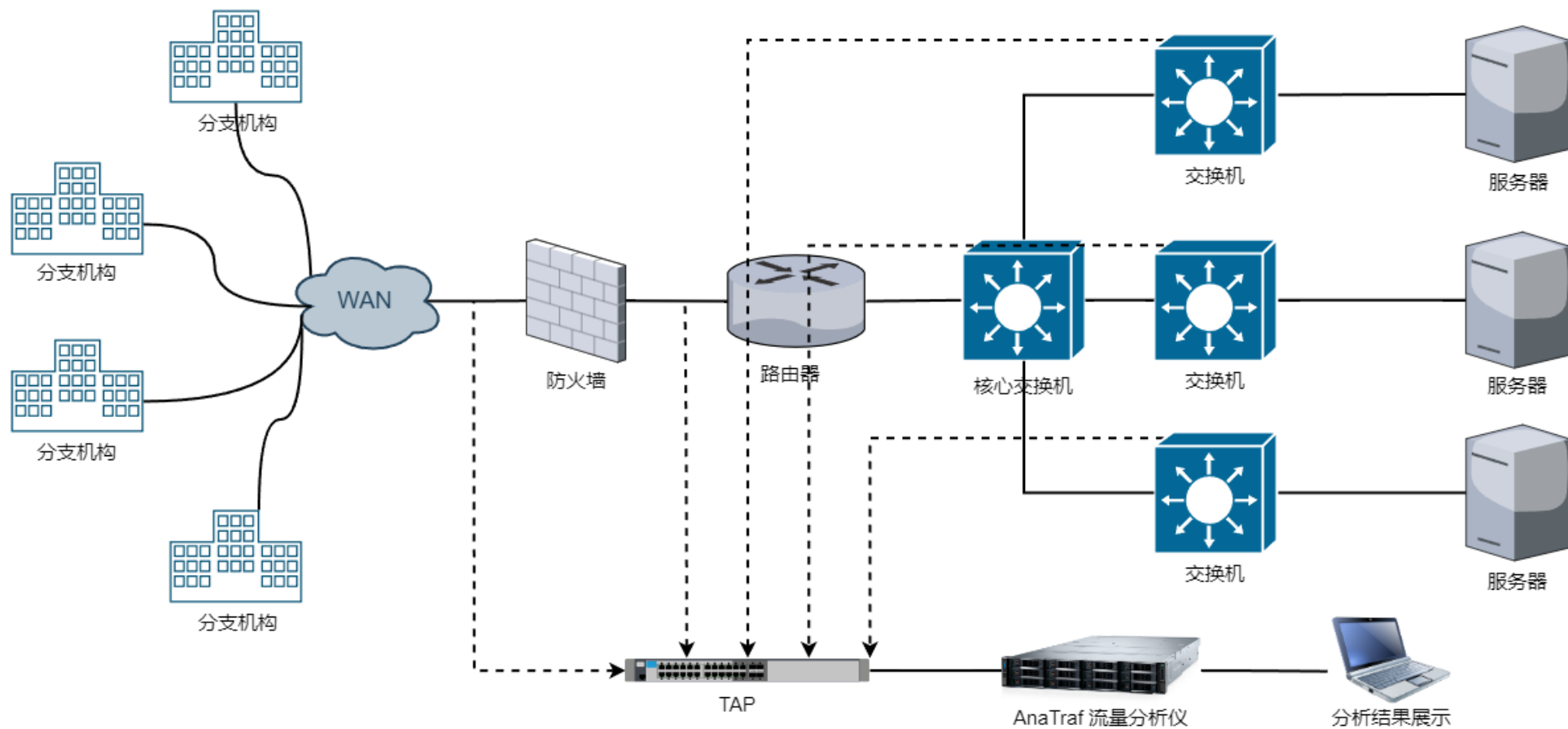
告警太多难以分析

粒度粗，检索慢，缺乏原始场景的数据，效率低，最后也懒得看

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

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
- 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

主要功能

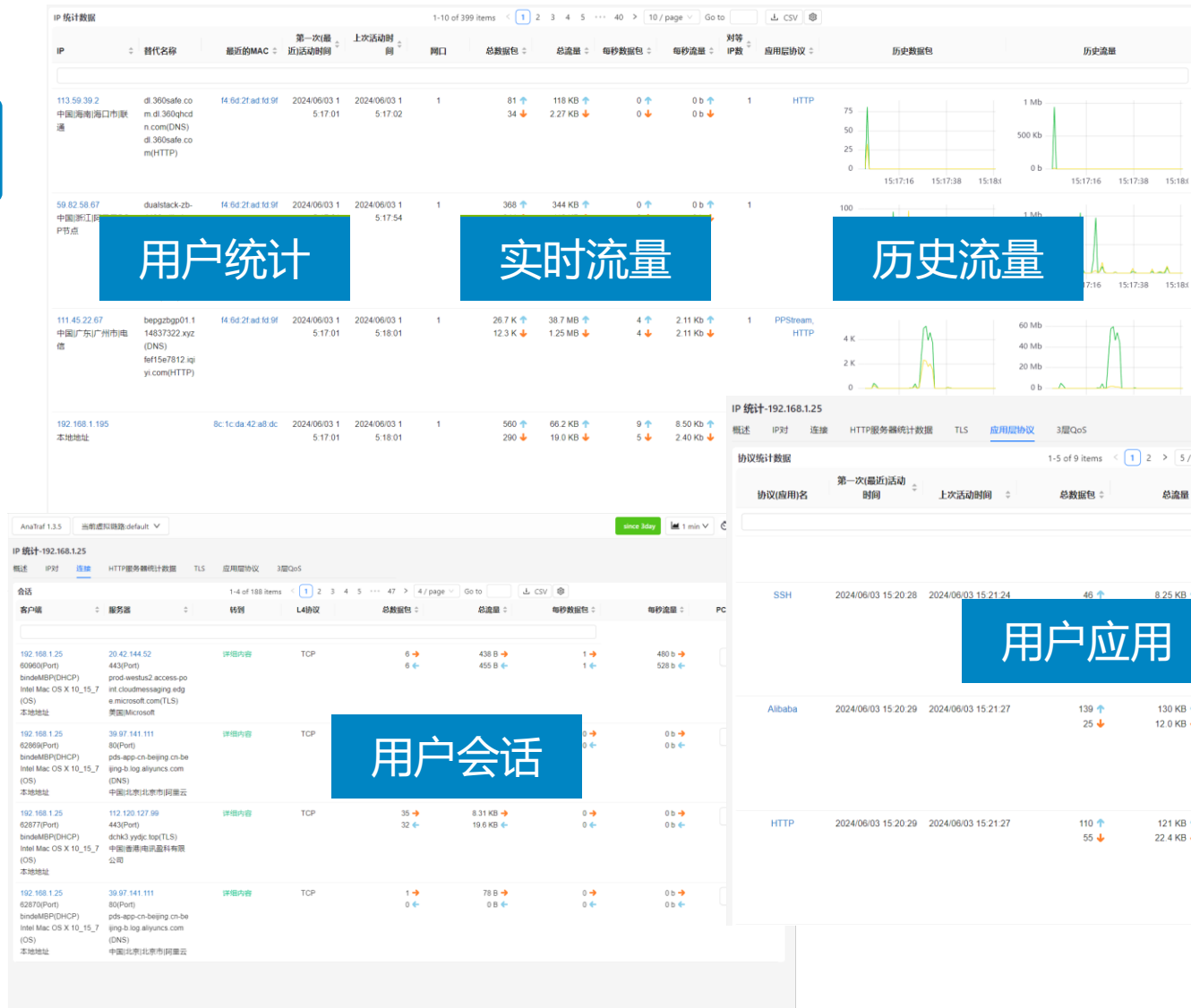


流量可视化

- 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

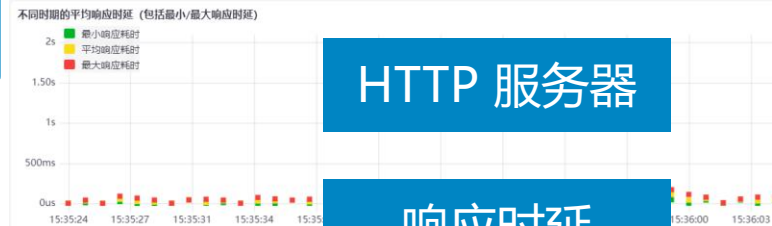
分析并关联OSI 2-7层
所有元数据

3



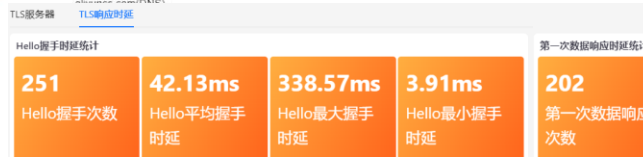
HTTP 服务器

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

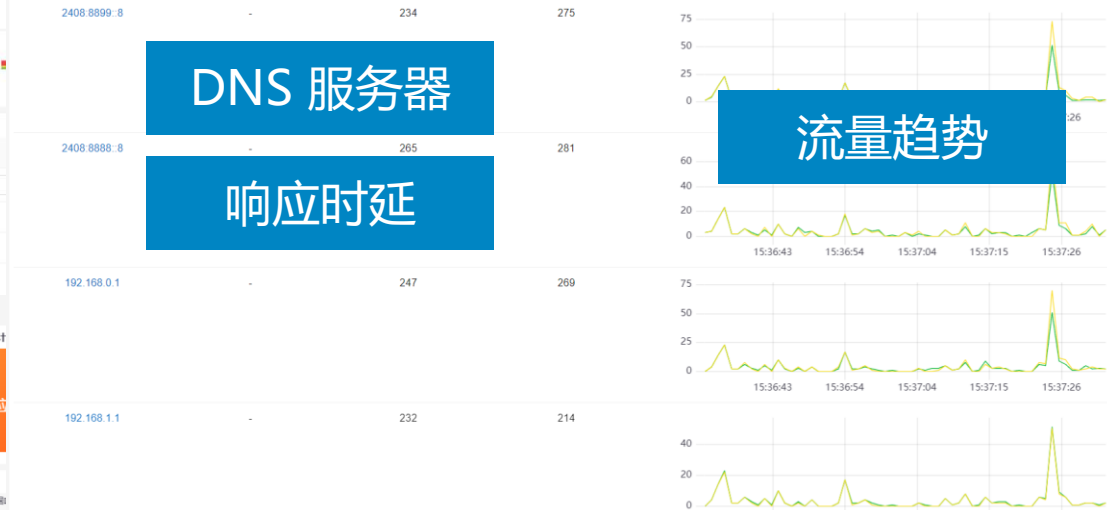
响应时延



DNS 服务器

响应时延

流量趋势



A bar chart with six bars. The first bar is blue, the second is red, the third is green, the fourth is blue, the fifth is red, and the sixth is green. The heights of the bars are approximately 1.5, 2.5, 3.5, 4.5, 5.5, and 4.5 units respectively. A black line connects the tops of the bars, showing an overall upward trend that peaks at the fifth bar and then declines at the sixth.

- 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



在线预览

No. 跳转到指定序号数据包

数据总数: 15

服务器: IP地址 = 192.168.1.111, TCP 端口 = 8080

客户端: IP地址 = 192.168.1.134, TCP 端口 = 57173

1: .

```
3: GET /capture_status?t=1278532291081 HTTP/1.1 Host: 192.168.1.111:8080 Connection: keep-alive Pragma: no-cache Cache-Control: no-cache User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:2.0.1) Gecko/20100101 Firefox/4.0.1 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9
```

5: HTTP/1.1 200 OK Connection: Keep-Alive Content-Length: 647 Content-Type: application/json Date: Thu, 10 Oct 2024 03:51:28 GMT

```
6: {"code": 0, "msg": "successfully", "data": [{"cid": 1, "type": "engine_reserved", "name": "", "status": "stop", "mode": "all_pkt", "pid": 1, "pkt_count": 0, "max_byte": 209715200, "used_byte": 0, "show_count": 0}, {"cid": 3, "type": "engine_reserved", "name": "", "status": "stop", "mode": "all_pkt", "pid": 3, "pkt_count": 0, "max_byte": 209715200, "used_byte": 0, "show_count": 0}, {"cid": 4, "type":
```

8: GET /worker_port_info?t=1728532291086 HTTP/1.1

Accept-Encoding: gzip, deflate Accept-Language: zh-CN

9: HTTP/1.1 200 OK Connection: Keep-Alive Content-Length: 21000 2024 03:51:28 GMT

```
10: {"port_list":[{"port_id":1,"speed_capacity":{"1000,10000"},"port_type":"DPDK","auto_negotiate":true,"duplex":{"Full-duplex"},"link_status":"linkup","current_speed":10000,"100,100,1000","port_type":"DPDK","auto_negotiate":true,"duplex":{"Full-duplex"},"link_status":"linkup","current_speed":1000,"port_id":4,"speed_capacity":{"100,100,10000"},"port_type":"DPDK","auto_negotiate":true,"duplex":{"Full-duplex"},"link_status":"linkup","current_speed":1000,"port_id":6,"speed_capacity":{"100,100,10000"}]}
```

12: GET /current_result_data?engine=1&path=all&t=172853291106 HTTP/1.1 Host: 192.168.1.111:8080 Connection: keep-alive Pragma: no-cache Cache-Control: no-cache Accept: */* Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9

13: HTTP/1.1 200 OK Connection: Keep-Alive Content-Length: 368 Content-Encoding: gzip Content-Type: text/xml Date: Thu, 10 Oct 2024 03:51:28 GMT

14:r...VM...6.Q."0U0.\$o_h.k<....;V...2z.l:7B.>.T...C.qS+..ecKb.gJ.&..9.R.....s.\$I~...){...a.Nq.o.x'.d.i--W...#'.I...`A.tL...9.I.0.4M.C...:&\r/^h.1qbC...

_t=1728532291086 HTTP/1.1

```

: 8080 -> 57173 [PSH, ACK] Seq=781
  Ack=828 Win=501 Len=133
=====

```

P: HTTP/1.1 200 OK (application/json)
7173 → 8080 [ACK] Seq=828 Ack=18

```
Win=256 Len=0
HTTP: GET /current_result_data?
line=1&path=all&t=1728532291106
HTTP/1.1
```

8080 → 57173 [PSH, ACK] Seq=1872
Ack=1263 Win=501 Len=149

```
CP: 57173 → 8080 [ACK] Seq=1263
    Ack=2389 Win=254 Len=0
```



时序图

流重组

主要功能



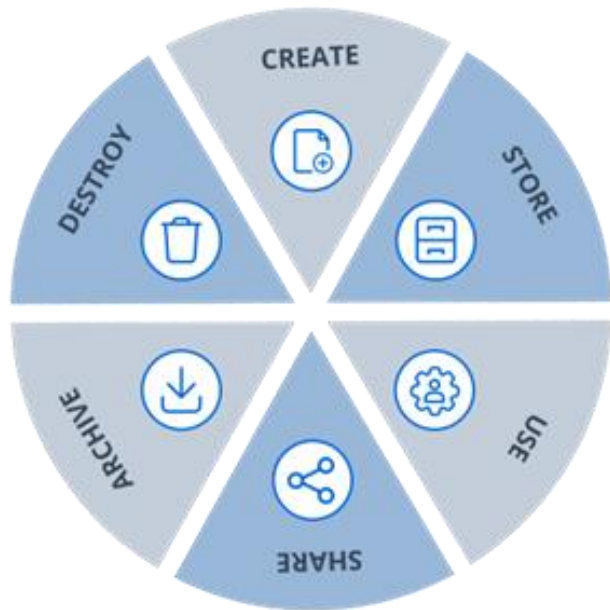
全流量回溯

- 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

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



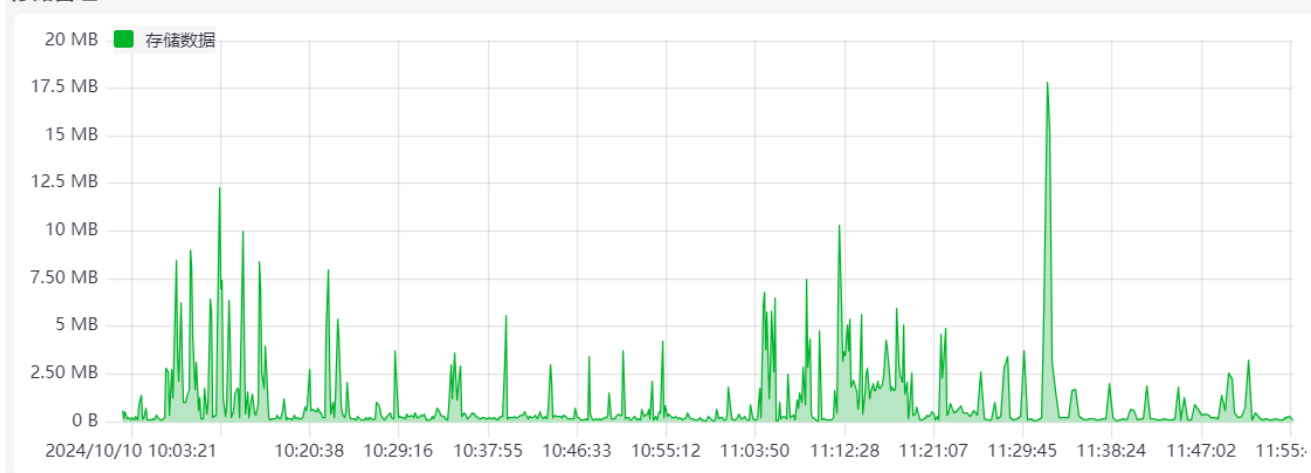
全流量回溯

- 全流量存储
- 全流量回溯
- 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

满足等保测评180天流量回溯分析要求

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。

主要功能



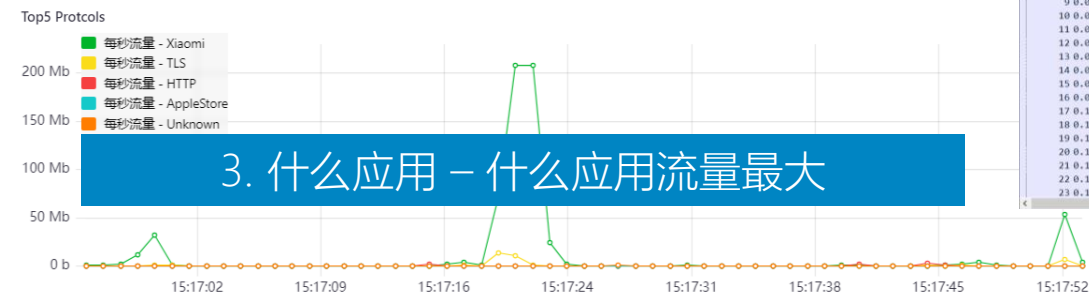
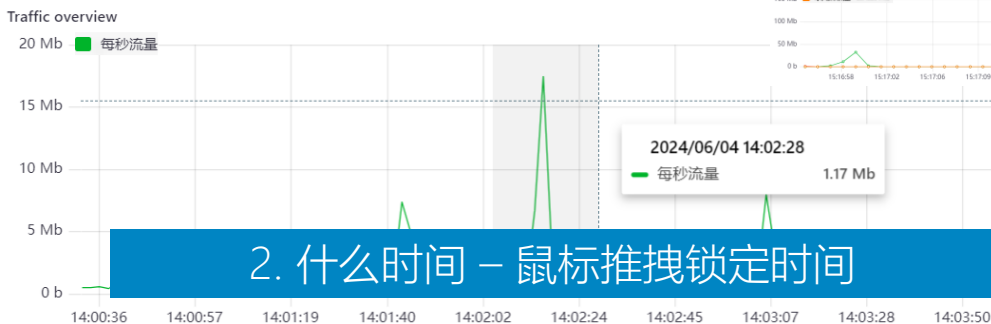
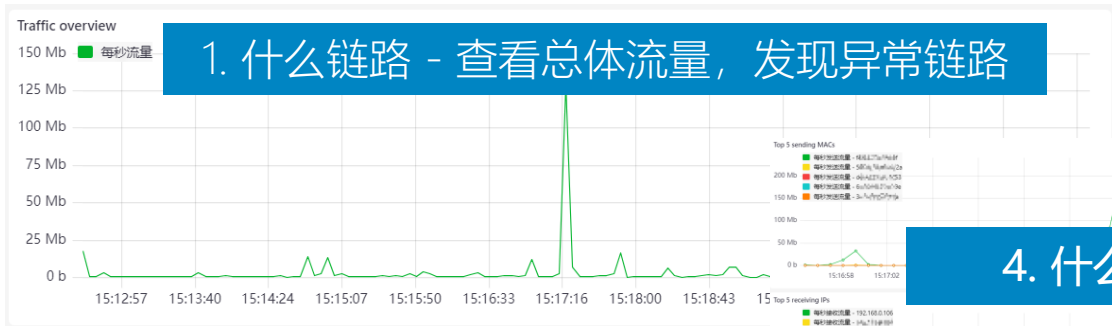
全流量回溯

- 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

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	192.168.1.100	192.168.1.100	TCP	60 54286 -> 443 [ACK] Seq=1 Win=131328 Len=0
6 0.045492	192.168.1.100	192.168.1.100	TCP	60 54287 -> 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
7 0.045521	192.168.1.100	192.168.1.100	TLSv1.3	629 Client Hello
8 0.045528	192.168.1.100	192.168.1.100	TLSv1.3	629 Server Hello, Change Cipher Spec, Application Data
9 0.045548	192.168.1.100	192.168.1.100	TCP	1498 443 -> 54287 [PSH, ACK] Seq=1445 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
10 0.045552	192.168.1.100	192.168.1.100	TCP	1262 443 -> 54287 [PSH, ACK] Seq=2889 Ack=576 Win=64128 Len=1208 [TCP segment of a r...
11 0.045556	192.168.1.100	192.168.1.100	TLSv1.3	1498 Server Hello, Change Cipher Spec, Application Data
12 0.045560	192.168.1.100	192.168.1.100	TCP	1498 443 -> 54286 [PSH, ACK] Seq=1445 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
13 0.045564	192.168.1.100	192.168.1.100	TCP	1262 443 -> 54286 [PSH, ACK] Seq=2889 Ack=576 Win=64128 Len=1208 [TCP segment of a r...
14 0.045568	192.168.1.100	192.168.1.100	TCP	60 54287 -> 443 [ACK] Seq=576 Ack=2889 Win=131328 Len=0
15 0.045572	192.168.1.100	192.168.1.100	TCP	60 54286 -> 443 [ACK] Seq=576 Ack=2889 Win=131328 Len=0
16 0.045576	192.168.1.100	192.168.1.100	TCP	1498 443 -> 54287 [ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
17 0.045580	192.168.1.100	192.168.1.100	TLSv1.3	760 Application Data, Application Data
18 0.045584	192.168.1.100	192.168.1.100	TCP	60 54287 -> 443 [ACK] Seq=576 Ack=6247 Win=131328 Len=0
19 0.045588	192.168.1.100	192.168.1.100	TCP	1498 443 -> 54286 [ACK] Seq=4097 Ack=576 Win=64128 Len=1444 [TCP segment of a r...
20 0.045592	192.168.1.100	192.168.1.100	TLSv1.3	760 Application Data, Application Data
21 0.045596	192.168.1.100	192.168.1.100	TLSv1.3	118 Change Cipher Spec, Application Data
22 0.045600	192.168.1.100	192.168.1.100	TLSv1.3	146 Application Data
23 0.045604	192.168.1.100	192.168.1.100	TLSv1.3	

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

3

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

