



2022

可视化网络领导者

# 实战--NTM全数据留存在校园网的应用

北京派网软件有限公司



# 目录

01

实战1：多校区智能遥测应用

02

实战2：分析校园网卡顿问题

03

实战3：全流量分析在护网时应用



01

# NTM在多校区智能遥测应用

在网络维护的过程中，有时候需要Wireshark抓包分析。例如：分校区某个公寓楼里面的数据包，进行某个IP的故障定位。

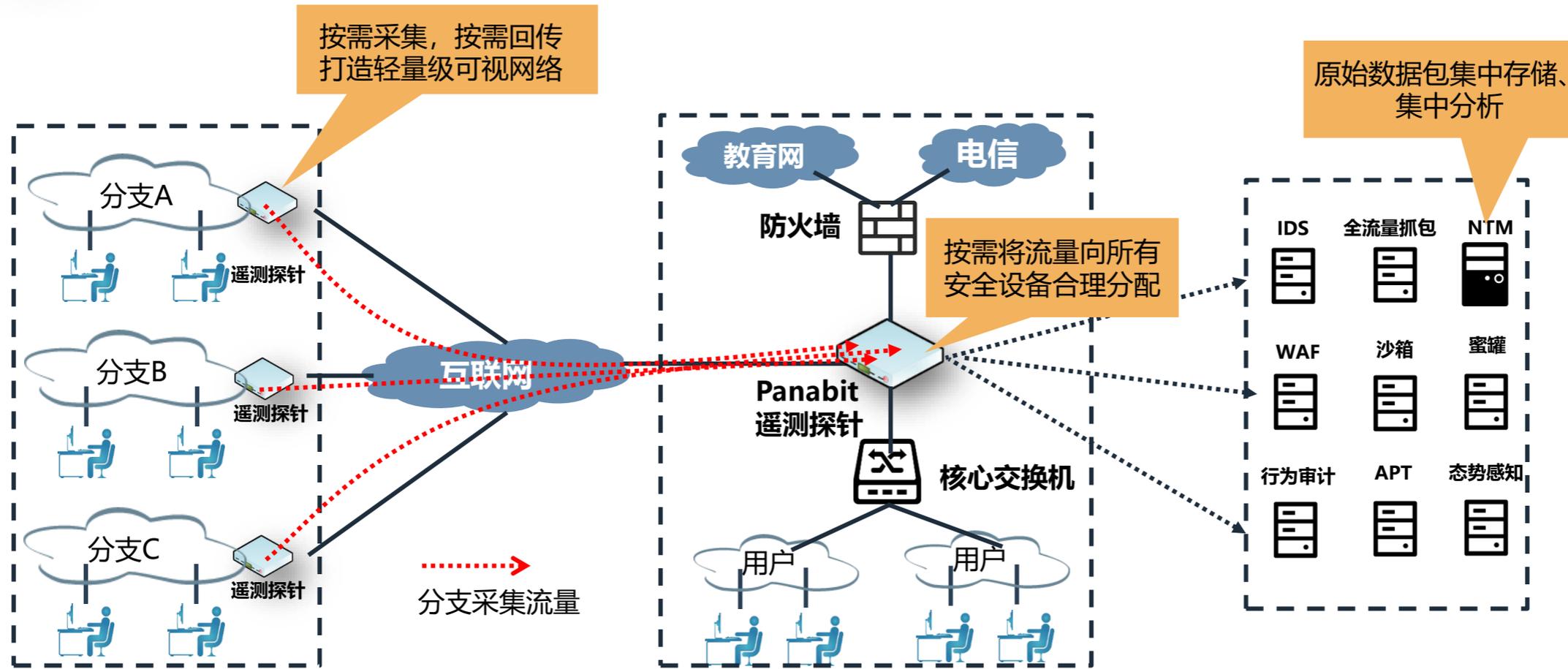
### 以往操作

需要先到分校区，然后再到公寓楼，通过Wireshark进行抓包分析。抓包过程中，会产生大量“垃圾”数据包。

### 遥测操作

通过遥测功能，无论人在哪里，都可以将分校区的某些数据“抓包”到总校区进行NTM分析。而且是剔除干扰，基于“数据流”的抓包

# 场景一：分校区数据采集+分析



遥测探针可以组成一张遥测网络，远端的探针采集的流量可以顺利回传至总部；  
总部遥测探针可以将流量按需分给所有安全设备；

## 1. 基于应用的遥测功能;

通过Panabit DPI功能, 实现把某个应用进行遥测, 解决了全量数据遥测时候数据量大的问题。

## 2. 支持SD-WAN组网

支持SD-WAN功能, 只要网关可以通, 便可以实现应用遥测, 解决了专线费用贵的问题。

## 3. 免费提供智能遥测功能

智能遥测功能为Panabit设备的标准功能, 不需要购买额外的License授权。



# 实战：分校区某台PC，流量抓包分析



报文解析 报文交互 元数据 报文播放

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	10.3.9.162	10.3.53.100	TCP	78	25292 款 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=
2	0.000001	10.3.9.162	10.3.53.100	TCP	78	[TCP Out-Of-Order] 25292 款 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460
3	0.000242	10.3.53.100	10.3.9.162	TCP	78	80 款 25292 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_I
4	0.000243	10.3.53.100	10.3.9.162	TCP	78	[TCP Out-Of-Order] 80 款 25292 [SYN, ACK] Seq=0 Ack=1 Win=28960 L
5	0.000332	10.3.9.162	10.3.53.100	TCP	70	25292 款 80 [ACK] Seq=1 Ack=1 Win=14848 Len=0 TSval=2843248861 TS
6	0.000335	10.3.9.162	10.3.53.100	TCP	70	[TCP Dup ACK 5#1] 25292 款 80 [ACK] Seq=1 Ack=1 Win=14848 Len=0 T
7	0.064442	10.3.9.162	10.3.53.100	HTTP	732	GET /images/ztrrg.png HTTP/1.0
8	0.064446	10.3.9.162	10.3.53.100	TCP	732	[TCP Retransmission] 25292 款 80 [PSH, ACK] Seq=1 Ack=1 Win=14848
9	0.065893	10.3.53.100	10.3.9.162	TCP	70	80 款 25292 [ACK] Seq=1 Ack=663 Win=30336 Len=0 TSval=1600556517 1
10	0.065896	10.3.53.100	10.3.9.162	TCP	70	[TCP Dup ACK 9#1] 80 款 25292 [ACK] Seq=1 Ack=663 Win=30336 Len=0
11	0.074198	10.3.53.100	10.3.9.162	TCP	1518	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]

> Frame 11: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits)  
 > Ethernet II, Src: 0c:da:41:49:5b:ed (0c:da:41:49:5b:ed), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)  
 > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1999  
 > Internet Protocol Version 4, Src: 10.3.53.100, Dst: 10.3.9.162  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 25292, Seq: 1, Ack: 663, Len: 1448

```

0000  88 df 9e 39 2a 01 0c da 41 49 5b ed 81 00 07 cf  ...9*...A I[....
0010  08 00 45 00 05 dc de 07 40 00 3f 06 05 09 0a 03  ..E.....@ .?.....
0020  35 64 0a 03 09 a2 00 50 62 cc 04 a1 53 e3 c8 ee  5d....Pb ...S...
0030  81 e9 80 10 00 ed d9 bc 00 00 01 01 08 0a 5f 66  ....._f
0040  8d ed a9 78 89 1d 48 54 54 50 2f 31 2e 31 20 32  ...x..HTT P/1.1 2
0050  30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65  00 OK..Da te: Tue
0060  2c 20 31 32 20 41 70 72 20 32 30 32 32 20 30 32  , 12 Apr 2022 02
0070  3a 33 37 3a 31 34 20 47 4d 54 0d 0a 53 65 72 76  :37:14 GM T..Serv
0080  65 72 3a 20 2a 0d 0a 58  er: *****.X
0090  2d 46 72 61 6d 65 2d 4f 70 74 69 6f 6e 73 3a 20  -Frame-Op tions:
00a0  53 41 4d 45 4f 52 49 47 49 4e 0d 0a 58 2d 58 53  SAMEORIGI N..X-XS
00b0  53 2d 50 72 6f 74 65 63 74 69 6f 6e 3a 20 31 3b  S-Protect ion: 1;

```

通过遥测抓包，分析10.3.9.162访问内网服务器的每一个动作，便于我们进行故障定位。

# 实战：分校区某台PC，流量抓包分析



报文解析

报文交互

元数据

报文播放

应用

连接时间	2022-04-12 10:40:04 - 2022-04-12 10:40:04	协议	TCP
源MAC	00:50:00:00:00:00:00:99:e9	目标MAC	88:df:97:93:2a:01
源IP:端口	10.3.9.162:25292	目标IP:端口	10.3.9.100:80
源	Packets: 26 Bytes: 3160 Databytes: 1324	目	Packets: 30 Bytes: 32306 Databytes: 30190
TCP Flags	SYN: 4, SYN_ACK: 0, ACK: 52, FIN: 0, PSH: 0, RST: 0, URG: 0	Method	GET
Status code	200	Cookie	
Host	www. .edu.cn	X-forward	2001:da8:2 :2b61:d9f7
Referer		URL	/images/ztrrg.png HTTP/1.0
User-Agent			

交互过程

Source	Destination
<pre>88 df 9e 39 2a 01 00 50 56 80 99 e9 81 00 0f a9 08 00 45 00 00 3c f7 8f 40 00 40 06 f0 20 0a 03 09 a2 0a 03 35 64 62 cc 00 50 c8 ee 7f 52 00 00 00 00 a0 02 39 08 de 36 00 00 02 04 05 b4 04 02 08 0a a9 78 88 dd 00 00 00 01 03 03 09</pre>	<pre>Num: 1. 2022/04/12 10:40:04 78 bytes ...9*..PV..... ..E....@.@... ....5db..P...R.. ....9..6..... ...x.....</pre>

同时，也可以看到客户端和服务端通讯，详细的报文交互详细数据。

# 实战：分校区某台PC，流量抓包分析

报文解析 报文交互 **元数据** 报文播放

展示方式	按属性
> x_forwarded_for	
▼ user_agent	
⊕ 报文7	Mozilla/5.0 (Linux; Android 11; LSA-AN00 Build/HONORLSA-AN00; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.0.0 Mobile Safari/537.36 MicroMessenger/8.0.21.2120(0x28001553) Process/toolsmp WeChat/arm64 Weixin NetType/4G Language/zh_CN ABI/arm64
> time	
▼ response.code	
⊕ 报文113	200
> request.uri.query	
> request.uri.path	
> request.uri	
▼ request.method	
⊕ 报文7	GET
> request.line	
⊕ 报文7	http://service.l[redacted]edu.cn/v2/static/js/chunk-0cd27d20.82b96a780af526e4fc81.js?v=1650423608517

## 元数据分析：

对相关报文元数据进行统计，发现数据包相关属性。从而对数据包有更多信息了解。

例如：这是一个用户通过华为荣耀60（LSA-AN00），使用微信工具访问内网service.\*.edu.cn的一个HTTP数据包，通过get模式从服务器上获得数据，并且访问成功。

# » Tips1: 如何节约回传带宽

匹配条件

执行动作

策略序号	<input type="text"/>	1~65535,序号小的优先匹配
策略备注	<input type="text"/>	
线路及流向	<input type="text" value="任意"/>	<input type="text" value="任意"/>
首包接口	<input type="text" value="任意"/>	
源接口	<input type="text" value="任意"/>	<input type="text" value="任意"/>
内网地址: 端口	<input type="text" value="任意"/>	: <input type="text" value="0"/>
外网地址: 端口	<input type="text" value="任意"/>	: <input type="text" value="0"/>
协议	<input type="text" value="任意"/>	<input type="text" value="任意"/>
内网MAC组	<input type="text" value="任意"/>	<a href="#">[说明]</a>
VLAN	<input type="text" value=""/>	0表示忽略此条件
TTL	<input type="text" value=""/>	0表示忽略此条件
共享用户>=	<input type="text" value="0"/>	个, 0~255, 0表示忽略
移动设备>=	<input type="text" value="0"/>	个, 0~255, 0表示忽略

基于端口、IP地址、应用协议等条件设置回传数据

选择协议

输入协议名称进行搜索

- 应用协议
  - 任意协议
  - 未知协议
  - + HTTP协议
  - + 常用协议
  - + P2P下载
  - + 网络电视

可按照协议类型选取

匹配条件

执行动作

执行动作	<input type="text" value="iWAN镜像"/>	
iWAN线路	<input type="text" value="iwan"/>	
转发VLAN	<input type="text" value=""/>	
DSCP标记	<input type="text" value="0"/>	0~63,0表示
流量统计	<input type="text" value="不设置"/>	关联统计
动作过后	<input type="text" value="停止匹配"/>	<a href="#">[说明]</a>

# » Tips2: 如何节约NTM硬盘

策略序号

策略备注

线路及流向

首包接口

源接口

源地址: 端口  :

目标地址: 端口  :

应用协议

用户组

VLAN

TTL

执行动作

## 选择协议

输入协议名称进行搜索

- 应用协议
  - 任意协议
  - 未知协议
  - HTTP协议
  - 常用协议
  - P2P下载
  - 网络电视
  - 社交
  - 金融财经
  - 流媒体

用户组

VLAN

TTL

执行动作

抓包数量

可按照协议类型选取

可以设置抓包数量

### 基本概念

CPE（Customer Premise Equipment）客户终端设备。

Panabit 5G CPE设备是一款支持4G/5G SIM卡的Panabit网关设备，同时具备了目前Panabit智能应用网关的所有功能。



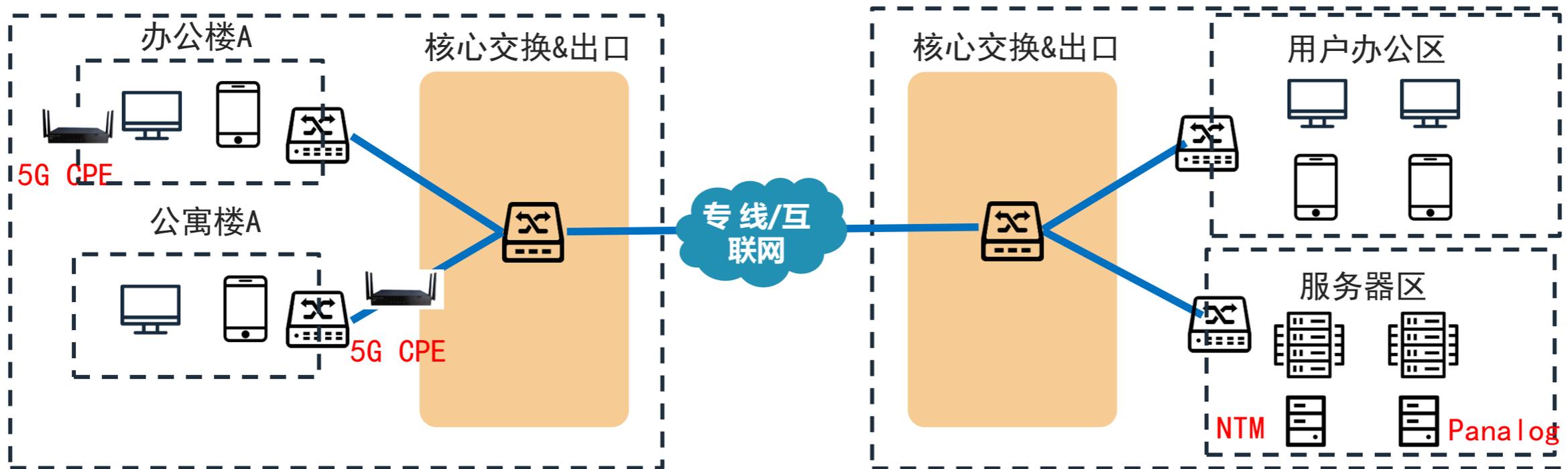
### XX大学使用网络现状分析

1. XX大学分校区缺乏IT人员，本地无法做到网络维护和故障定位；
2. 网络病毒爆发时候，分校区和总校区的专线跑满，无法进行远程维护；
3. 缺少主动预警手段，工作比较被动；

## 场景二：5G CPE在遥测的应用

学校XX分校区

学校本部



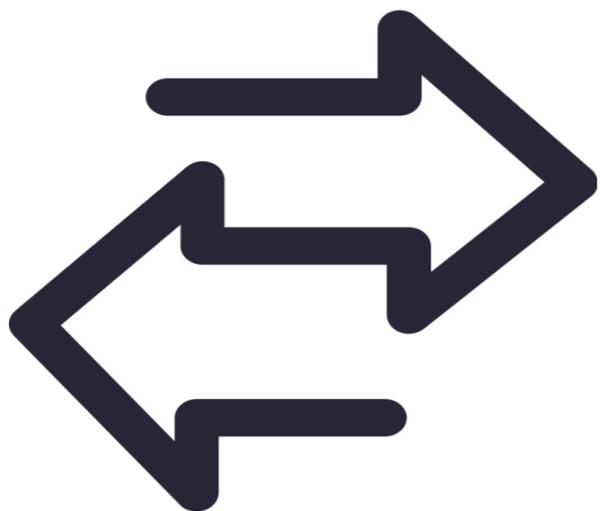
### 部署说明

1. 在分校区的重点汇集交换机或者楼宇处部署Panabit 5G CPE设备;
2. 在学校本部部署云平台 and Panalog 和 Panabit NTM 系统;
3. 通过遥测功能, 将分校区的某些数据“抓包”到总校区进行NTM分析。



02

## NTM分析校园网卡顿问题



**场景1：校园网访问互联网卡顿分析**

**场景2：互联网访问校园网服务器卡顿分析**

序号	应用名称	最大时延	最小时延	平均时延
1	其它HTTP上传	6587.853 ms	0.053 ms	1217.805 ms
2	Office365	3467.394 ms	137.021 ms	443.218 ms
3	QQMail	123.725 ms	37.677 ms	98.496 ms
4	Oracle	1025.406 ms	0.977 ms	96.969 ms
5	腾讯文档	94.656 ms	32.417 ms	94.656 ms
6	QQ游戏	84.119 ms	0 ms	84.119 ms
7	歪歪语音/Bigolive	82.907 ms	63.269 ms	78.154 ms
8	Google搜索/服务	78.551 ms	63.547 ms	77.995 ms
9	QQ聊天	50.431 ms	0 ms	50.431 ms
10	百度云盘	524.912 ms	1.266 ms	38.517 ms
11	Windows补丁	197.38 ms	0.711 ms	38.228 ms
12	伪IE下载	3139.013 ms	0.217 ms	37.416 ms
13	Apex英雄	4260.801 ms	0.004 ms	36.69 ms
14	SNMP	7818.372 ms	0.002 ms	32.424 ms
15	腾讯	84.721 ms	12.215 ms	29.861 ms

## 协议时延算法:

客户时延+服务时延+应用时延

## 常规使用:

这里主要看“平均时延”，如果该时延比较大，说明这个业务整体体验感不大好，需要进行优化。



### 协议重传:

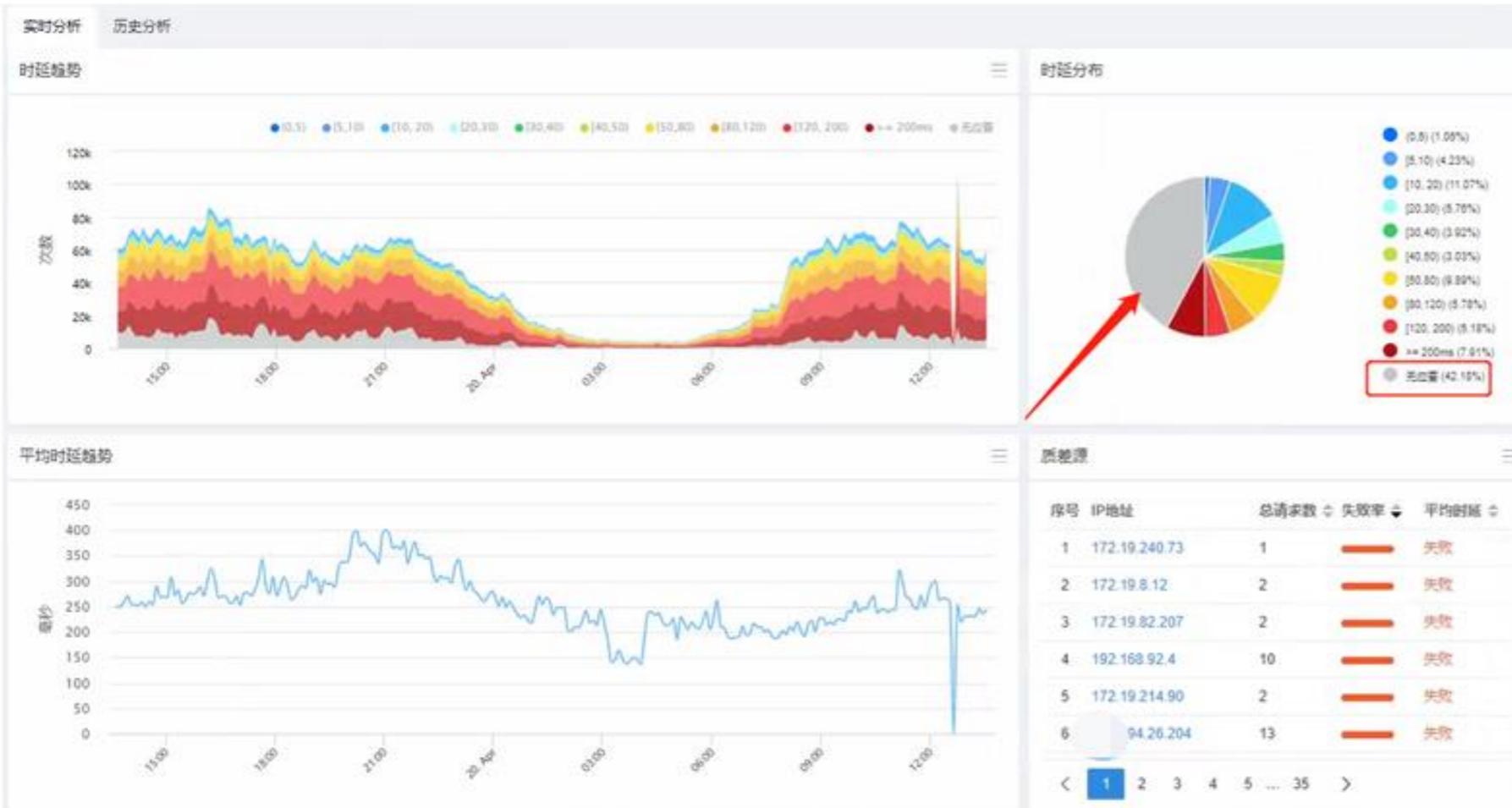
指TCP连接建立后, 由于通讯超时或者TCP序列不对产生的重传包。

### 常规使用:

如果某类应用的重传率非常高, 用户体验感肯定不好。

校内网访问互联网应用协议重传 Dashboard

# 案例1：校园网访问微信卡顿NTM分析



## 第一步：微信时延分析

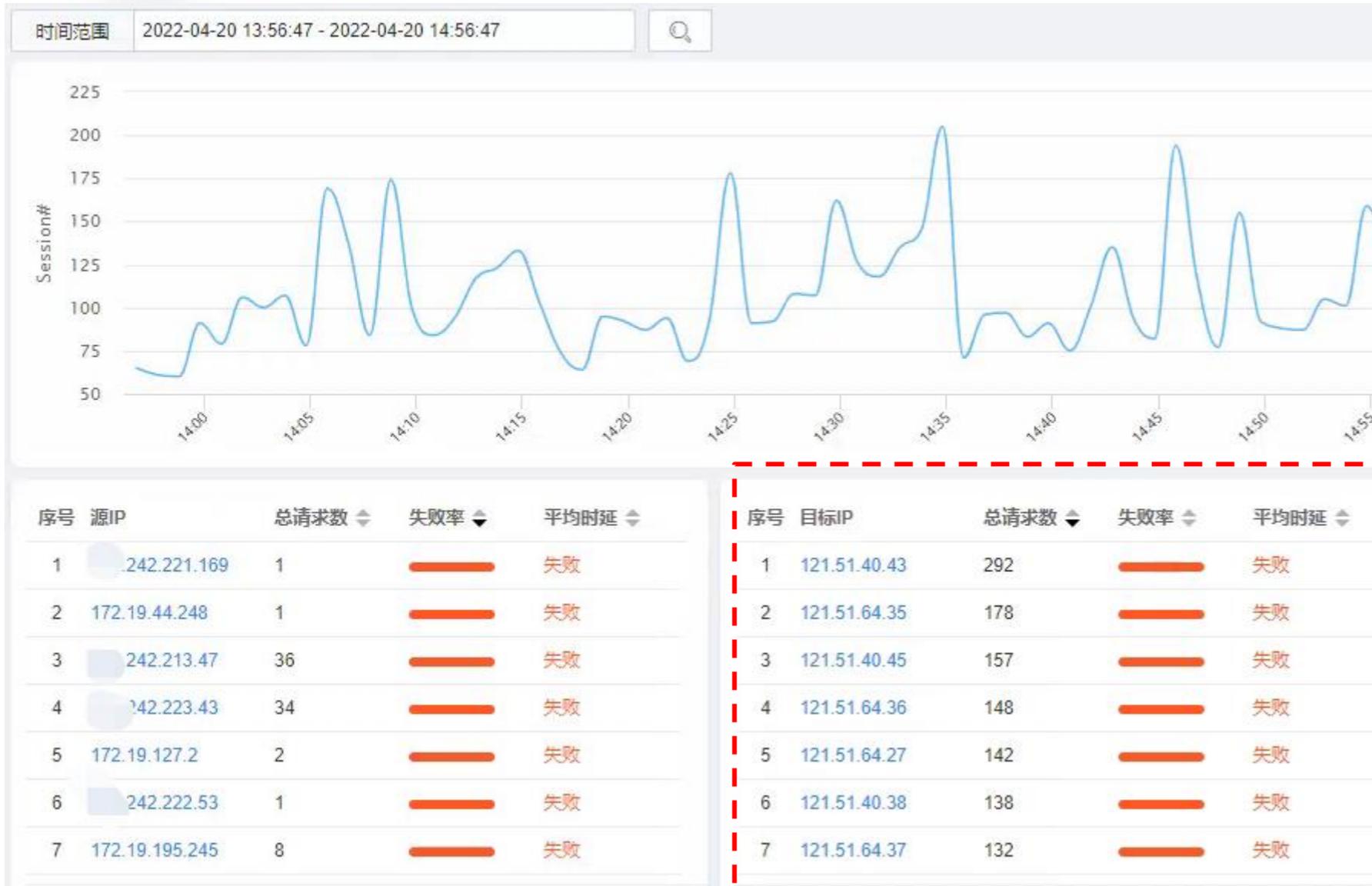
### NTM分析

通过时延分析，发现微信的未应答数量非常多，高达42.18%

### 解决思路：

需要对“未应答”数据包进行分析，找出相关原因

# 案例1：校园网访问微信卡顿NTM分析



## 第二步：“未应答”数据包分析

通过NTM对微信“未应答”数据包进行分析，发现相关目标地址主要集中在121.51.0.0/16这个网段。

# 案例1：校园网访问微信卡顿NTM分析

报文解析 报文交互 元数据 报文播放

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	172.18.240.151	121.51.40.43	TCP	74	55452 款 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1360 SACK_PERM=1 TSval=3776825006 TSecr=0
2	0.995753	172.18.240.151	121.51.40.43	TCP	74	[TCP Retransmission] 55452 款 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1400 SACK_PERM=1 TS
3	5.999667	121.51.40.43	172.18.240.151	TCP	60	[TCP ACKed unseen segment] 8080 款 55452 [RST, ACK] Seq=1 Ack=929054312 Win=0 Len=0

Sequence number (raw): 0  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 929054312 (relative ack number)  
Acknowledgment number (raw): 3362233137  
0101 .... = Header Length: 20 bytes (5)  
> Flags: 0x014 (RST, ACK)  
Window: 0  
[Calculated window size: 0]  
[Window size scaling factor: -1 (unknown)]  
Checksum: 0x1602 [unverified]

```
0000 64 a0 e7 40 0a 41 00 94 a1 21 c2 06 08 00 45 00    d..@.A... !...E.
0010 00 28 91 7d 40 00 ff 06 ac 49 79 33 28 2b ac 12    .().@.... Iy3(+..
0020 f0 07 1f 00 48 0c 00 00 00 00 48 67 0b 31 50 14    ..P
```

## 第三步：“未应答”数据包进行报文解析

通过报文解析，发现3个报文。

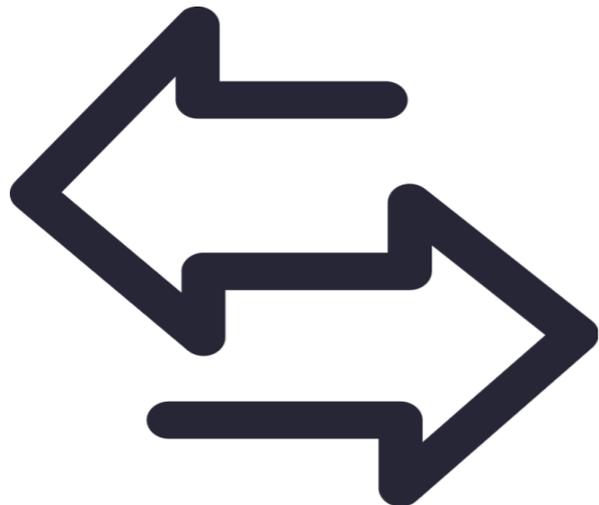
1. 是客户端对微信服务器进行请求，但服务器没有回应（没看到回包）。
2. 客户端重新请求，但服务器直接进行重置，同时告诉客户端window窗口为0

## 结论：

腾讯服务器对该请求进行拒绝

## 问题解决：

由于这个用户微信“未响应”数据包的目标地址基本上集中在121.51.0.0/16这个网段，怀疑出口ISP到这个网段的问题，更换121.51.0.0/16的路由选择，让到121.51.0.0/16数据包走另外一个ISP，这个问题得以解决。



**场景1：** 校园网访问互联网卡顿分析

**场景2：** 互联网访问校园网服务器卡顿分析

# 场景2：校内服务器访问质量分析

自动刷新	10秒	排序方式	连接数	主机组	所有组	关键字搜索	+	添加	↶	↷	导入	导出	列表	分离	卡片
统一身份认证系统				主页服务器				网上服务大厅							
477	37	0	22.04 ms	329	2166	0	2.78 ms	319	99	0	49.84 ms				
连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延				
5.66K	229.93K	2.57M	103.56M	56	21.64M	11.97M	4.21G	338	419.63K	505.29M	120.97G				
流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量				
OA服务器				就业系统				教学云主页							
221	151	0	26.40 ms	186	20	0	18.82 ms	106	811	0	4.70 ms				
连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延				
2.20K	1.47M	503.77K	214.39M	870	175.58K	1.15M	34.16M	8.35M	128.74K	325.80G	66.97G				
流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量				
教务管理系统				资产管理系统				招生系统							
100	8	0	9.70 ms	50	69	2	89.15 ms	21	0	0	5.65 ms				
连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延				
1.12K	22.86K	844.11K	17.50M	79.96K	107.96K	767.03M	1.46G	0	0	0	21.45M				
流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量				

内置服务器系统时延Dashboard，可随时查看服务器的连接数、失败率、时延、流量等信息。

# 场景2：校内服务器访问质量分析



某台服务器访问时延Dashboard

# 场景2：校内服务器访问质量分析



序号	域名	总请求次数	DNS请求次数	HTTP请求次数	HTTPS请求次数	HTTP20x	HTTP30x	HTTP40x	HTTP50x
1	www.t.edu.cn	172352	63338	108926	88	105583	514	2722	0
2	service.t.edu.cn	161110	1130	159833	147	158293	959	549	0
3	auth.t.edu.cn	141369	1057	140224	88	17768	122315	103	0
4	jwgl.t.edu.cn	36334	512	5201	30621	0	5199	1	0
5	apiucloud.t.edu.cn	35796	406	34932	458	32923	0	1956	3
6	ucloud.t.edu.cn	24028	904	22235	889	18476	3360	384	0
7	huorong.t.edu.cn	13593	4044	119	9430	119	0	0	0
8	yjxt.t.edu.cn	12960	7258	5702	0	4704	495	43	150
9	360.t.edu.cn	12117	1228	10889	0	270	10554	51	0
10	oa.t.edu.cn	9293	138	9022	133	6321	10	2690	0
11	teac.t.edu.cn	8514	242	3	3	4914	325	214	2383
12	news.t.edu.cn	8216	3212	5002	2	3729	261	1011	0
13	imgservice.t.edu.cn	7433	434	6990	9	6924	36	27	0
14	reservation.t.edu.cn	6369	559	5790	20	3986	1796	0	0
15	zsb.t.edu.cn	6072	86	5984	2	5402	25	556	0
16	scs.t.edu.cn	5877	114	5762	1	4392	575	795	0
17	my.t.edu.cn	5510	951	4559	0	2825	1377	352	2
18	jwglweixin.t.edu.cn	5387	1030	4357	0	3806	446	104	0

资产热度排名

资产访问排名

资产状态码排名

## HTTP状态码描述

分类	分类描述
1**	信息，服务器收到请求，需要请求者继续执行操作
2**	成功，操作被成功接收并处理 例如：200请求成功。一般用于GET与POST请求
3**	重定向，需要进一步的操作以完成请求 例如：301/302，请求的资源移动到新URI，返回信息会包括新的URI
4**	客户端错误，请求包含语法错误或无法完成请求 例如：404，服务器无法根据客户端的请求找到资源（网页）
5**	服务器错误，服务器在处理请求的过程中发生了错误 例如：503，由于超载或系统维护，服务器暂时的无法处理客户端的请求

根据状态码，可以对服务器访问情况有所评估和判断。

例如：某服务器的HTTP数据包里面包含大量500或者503，说明服务器内部错误，或者由于超载或系统维护，无法完成客户端请求。

例如：某服务器HTTP数据包里面包含301/302状态码，说明资源被重定向，如果重定向的资源有问题，用户访问也会存在问题。

# 案例2：访问服务器慢，如何进行定位？

源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传/包数	下行重传/包数	重置	流量	请求域名	状态	操作
3.9.250:63692	3.58.19:443		TCP	其它HTTPS	4/8	8/16	0/1	2092/13978	jwgl.b...edu.cn		数据包
3.9.250:50406	3.58.19:443		TCP	其它HTTPS	4/8	7/14	0/1	2092/13598	jwgl.b...edu.cn		数据包
3.9.250:28721	3.58.19:443		TCP	其它HTTPS	4/8	7/14	0/1	2092/13774	jwgl.b...edu.cn		数据包
3.9.250:43959	3.58.19:443		TCP	其它HTTPS	4/8	7/14	0/1	2092/13780	jwgl.b...edu.cn		数据包
3.9.250:14391	3.58.19:443		TCP	其它HTTPS	4/8	7/14	0/1	2092/13780	jwgl.b...edu.cn		数据包
1.9.250:30221	0.3.58.19:80		TCP	WWW	1/2	1/2	0/0	884/436	jwgl.b...t.edu.cn 302		数据包
1.9.250:48014	0.3.58.19:80		TCP	WWW	1/2	1/2	0/0	884/436	jwgl.b...edu.cn 302		数据包
3.9.250:45385	0.3.58.19:80		TCP	WWW	1/2	1/2	0/0	884/436	jwgl.b...edu.cn 302		数据包
3.9.250:39216	0.3.58.19:443		TCP	其它HTTPS	4/8	11/22	0/1	2212/25084	jwgl.t...edu.cn		数据包
3.9.250:59214	0.3.58.19:443		TCP	其它HTTPS	4/8	11/22	0/1	2212/25096	jwgl.t...edu.cn		数据包

**案例背景：**网络中心接到投诉，说用户访问校内某台服务器特别慢，需要进行排查。

**NTM分析：**通过NTM分析，发现用户访问存在HTTP 302报文，同时该服务器的重传率非常高，大约50%左右。但这个重传是如何导致的呢？

# 案例2：访问服务器慢，如何进行定位？

报文解析

报文交互

元数据

报文播放

报文显示过滤器

No.	Time	Source	Destination	Protocol	Length	Details
8	0.000573	3.9.250	3.58.19	TCP	442	[TCP Transmission] 48014
9	0.000654	3.58.19	3.9.250	HTTP	218	HTTP/1.1 302 Found
10	0.000656	3.58.19	3.9.250	TCP	218	[TCP Out-Of-Order] 80 致命
11	0.001136	3.9.250	3.58.19	TCP	70	48014 致命 80 [FIN, ACK] S
12	0.001138	3.9.250	3.58.19	TCP	70	[TCP Out-Of-Order] 48014 致命
13	0.001187	3.58.19	3.9.250	TCP	70	80 致命 48014 [ACK] Seq=15
14	0.001189	3.58.19	3.9.250	TCP	70	[TCP Dup ACK 13#1] 80 致命

```
> Frame 9: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits)
> Ethernet II, Src: 00:50:56:b5:82:7d (00:50:56:b5:82:7d), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4018
> Internet Protocol Version 4, Src: 3.58.19, Dst: 3.9.250
> Transmission Control Protocol, Src Port: 80, Dst Port: 48014, Seq: 1, Ack: 373, Len: 148
```

√ Hypertext Transfer Protocol

> HTTP/1.1 302 Found\r\n

Cache-Control: no-cache\r\n

> Content-length: 0\r\n

Location: https://jwgl. edu.cn/jsxsd/framework/xsMain.jsp\r\n

Connection: close\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.000083000 seconds]

[Request in frame: 7]

[Request URI: http://jwgl. edu.cn/jsxsd/framework/xsMain.jsp]

## HTTP302分析

通过NTM报文解析，发现该报文里面HTTP 302是把通过HTTP访问该服务器的数据包重定向到HTTPS访问。

访问慢不应该是这个原因，对其他报文进行深入分析

# 案例2：访问服务器慢，如何进行定位？

报文序号	报文时间	源地址	目的地址	协议	源端口	目的端口	描述
0	0.015193	10.3.58.19	10.3.9.250	TCP	101	443	[TCP Out-Of-Order] 443 数据 53957 [FIN, PSH, ACK] Seq=767
1	0.015500	10.3.9.250	10.3.58.19	TCP	70	443	53957 数据 443 [ACK] Seq=736 Ack=6369 Win=43008 Len=0
2	0.015500	10.3.9.250	10.3.58.19	TCP	70	443	[TCP Dup ACK 31#1] 53957 数据 443 [ACK] Seq=736 Ack=6369
3	0.015719	10.3.9.250	10.3.58.19	TLSv1.2	101	443	Encrypted Alert
4	0.015726	10.3.9.250	10.3.58.19	TCP	101	443	[TCP Retransmission] 53957 数据 443 [PSH, ACK] Seq=736
5	0.015761	10.3.58.19	10.3.9.250	TCP	64	443	443 数据 53957 [RST] Seq=6369 Win=0 Len=0
6	0.015762	10.3.58.19	10.3.9.250	TCP	64	443	443 数据 53957 [RST] Seq=6369 Win=0 Len=0
7	0.015763	10.3.9.250	10.3.58.19	TCP	70	443	53957 数据 443 [FIN, ACK] Seq=767 Ack=6369 Win=43008
8	0.015764	10.3.9.250	10.3.58.19	TCP	70	443	[TCP Out-Of-Order] 53957 数据 443 [FIN, ACK] Seq=767
9	0.015822	10.3.58.19	10.3.9.250	TCP	64	443	443 数据 53957 [RST] Seq=6369 Win=0 Len=0
10	0.015822	10.3.58.19	10.3.9.250	TCP	64	443	443 数据 53957 [RST] Seq=6369 Win=0 Len=0

0101 .... = Header Length: 20 bytes (5)

> Flags: 0x004 (RST)

Window: 0

[Calculated window size: 0]

[Window size scaling factor: 128]

Checksum: 0x575e [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

## NTM报文解析一看的更深入，看的更明白

通过对重传率高的会话进行抓包分析，发现具体原因。例如：本案例中有大量 win=0, Len=0的数据包，说明是因为服务器的缓存区基本满了，无法再接受数据。也推断出该重传是因为服务器负载太重，导致的无法响应。

# 案例3：国外用户访问服务器卡顿，如何办？

会话时延

源IP 任意IP 源端口 80 / 8000-8080 目标IP 任意IP 目标端口 80 / 8000-8080 传输协议 任意 应用协议 WWW

源IP ISP 其它 目标IP ISP 任意 源IP区域 任意 目标IP区域 任意 请求域名 r...t.edu.cn

客户时延>= ms 服务时延>= ms 应用时延>= ms 时间范围 2022-04-23 19:37:05 - 2022-04-23 20:37:05 连接类型 所有

请求时间	源IP	目标IP	目标地理位置	传输协议	应用协议	客户时延	服务时延	应用时延	流量(前10秒)	请求域名
2022-04-23/19:45:50	38.20.179.54638	55.81.80		TCP	WWW	1011.62	0.36	1.03	1787/1378	r...t.edu.cn 302
2022-04-23/19:50:32	38.14.194.5028	55.81.80		TCP	WWW	1053.44	0.28	14.54	1156/42242	r...t.edu.cn 200
2022-04-23/19:52:50	28.235.82.57421	55.81.80		TCP	WWW	172.81	0.27	1.13	1654/1414	r...t.edu.cn 302
2022-04-23/20:00:07	1.2.27.36452	55.81.80		TCP	WWW	213	0	30.95	627/5874	r...t.edu.cn 200
2022-04-23/20:00:10	1.2.27.36468	55.81.80		TCP	WWW	204.52	4.65	34.52	627/14364	r...t.edu.cn 200
2022-04-23/20:00:12	1.2.27.36472	55.81.80		TCP	WWW	210.69	0.26	22.86	627/15383	r...t.edu.cn 200
2022-04-23/20:00:14	1.2.27.36486	55.81.80		TCP	WWW	140.86	0.25	21.17	627/16556	r...t.edu.cn 200
2022-04-23/20:00:16	1.38.2.27.36496	55.81.80		TCP	WWW	160.6	0.2	25.4	627/20905	r...t.edu.cn 200

**案例背景：**网络中心接到投诉，说国外用户访问校内某台服务器特别慢，需要进行排查。

**NTM时延分析：**在“会话时延”选型里，源ISP选择“其他”，请求域名选择对应服务器的域名，进行时延分析，发现客户时延比较大，基本判断为从国外到校园网的问题。

# 案例3：国外用户访问服务器卡顿，如何办？

源IP 任意IP 源端口 80 / 8000-8080 目标IP 任意IP 目标端口 80 / 8000-8080 传输协议 任意 应用协议 WWW

源IP ISP 其它 目标IP ISP 任意 源IP区域 任意 目标IP区域 任意 请求域名 see...edu.cn

时间范围 2022-04-23 19:10:45 - 2022-04-23 20:10:45 连接类型 所有

其它	时间	源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传/包数	下行重传/包数	重置	流量	请求域名
电信	4-23/19:13:17	3.9.163.63606	3.55.125.80		TCP	WWW	1/2	7/14	0/0	1456/18504	see.L...edu.cn 200
联通	4-23/19:13:17	3.9.163.63614	3.55.125.80		TCP	WWW	1/2	2/4	0/0	1444/4562	see.t...edu.cn 200
移动	4-23/19:13:17	3.9.163.63612	3.55.125.80		TCP	WWW	1/2	1/2	0/0	1412/2196	see...edu.cn 200
铁通	4-23/19:13:17	3.9.163.63610	3.55.125.80		TCP	WWW	1/2	1/2	0/0	1430/2094	see...t.edu.cn 200
教育网	4-23/19:13:17	3.9.163.63608	3.55.125.80		TCP	WWW	1/2	1/2	0/0	1436/1870	see.t...edu.cn 200
鹏博士	4-23/19:13:17	3.9.163.63602	3.55.125.80		TCP	WWW	1/2	11/22	0/0	1440/31928	see.t...edu.cn 200
阿里云	4-23/19:13:17	3.9.163.63604	3.55.125.80		TCP	WWW	1/2	182/364	0/0	1436/26776	see.t...edu.cn 200
科技网	4-23/19:13:17	3.9.163.63588	3.55.125.80		TCP	WWW	1/2	12/24	0/0	1566/34736	see.t...edu.cn 200
京东云	4-23/19:13:22	3.9.163.64814	3.55.125.80		TCP	WWW	1/2	7/14	0/0	1342/18504	see.b...edu.cn 200
	4-23/19:13:22	3.9.163.64820	3.55.125.80		TCP	WWW	1/2	3/6	0/0	1328/7084	see.t...du.cn 200
	4-23/19:13:22	3.9.163.64818	3.55.125.80		TCP	WWW	1/2	2/4	0/0	1330/4562	see.t...edu.cn 200

**案例背景：**网络中心接到投诉，说国外用户访问校内某台服务器特别慢，需要进行排查。

**NTM重传分析：**在“会话流量”里面，源ISP选择“其他”，请求域名选择对应服务器的域名，进行重传分析，发现重传率也比较高，大约50%左右。



# 案例3：国外用户访问服务器卡顿，如何办？



报文解析

报文交互

元数据

报文播放

报文显示过滤器

71	0.302979	55.230	3.9.163	TCP	1518	[ACK] Seq=41993 Ack=670 Win=30720 Len=1448 TSval=111195073
72	0.302980	55.230	3.9.163	TCP	1518	[TCP Out-Of-Order] 80 字节 6148 [ACK] Seq=39097 Ack=670 Win=30720 Len=1448 T
73	0.302981	55.230	3.9.163	TCP	1518	[TCP Out-Of-Order] 80 字节 6148 [ACK] Seq=40545 Ack=670 Win=30720 Len=1448 T
74	0.302983	55.230	3.9.163	TCP	1518	[TCP Retransmission] 80 字节 6148 [PSH, ACK] Seq=41993 Ack=670 Win=30720 Len=
75	0.303062	55.230	3.9.163	TCP	70	6148 字节 80 [ACK] Seq=670 Ack=43441 Win=23552 Len=0 TSval=3831575646 TSecr=
76	0.303064	55.230	3.9.163	TCP	70	[TCP Dup ACK 75#1] 6148 字节 80 [ACK] Seq=670 Ack=43441 Win=23552 Len=0 TSva
77	0.303186	55.230	3.9.163	TCP	1518	80 字节 6148 [ACK] Seq=43441 Ack=670 Win=30720 Len=1448 TSval=1111950730 TSe
78	0.303187	55.230	3.9.163	TCP	1518	80 字节 6148 [ACK] Seq=44889 Ack=670 Win=30720 Len=1448 TSval=1111950730 TSe
79	0.303188	55.230	3.9.163	TCP	1518	[TCP Out-Of-Order] 80 字节 6148 [ACK] Seq=43441 Ack=670 Win=30720 Len=1448 T
80	0.303190	55.230	3.9.163	TCP	1518	80 字节 6148 [ACK] Seq=46337 Ack=670 Win=30720 Len=1448 TSval=1111950730 TSe
81	0.303190	55.230	3.9.163	TCP	1518	80 字节 6148 [ACK] Seq=47785 Ack=670 Win=30720 Len=1448 TSval=1111950730 TSe
82	0.303192	55.230	3.9.163	TCP	1518	[TCP Out-Of-Order] 80 字节 6148 [ACK] Seq=44889 Ack=670 Win=30720 Len=1448 T
83	0.303193	55.230	3.9.163	TCP	1518	[TCP Out-Of-Order] 80 字节 6148 [ACK] Seq=46337 Ack=670 Win=30720 Len=1448 T
84	0.303195	55.230	3.9.163	TCP	1518	80 字节 6148 [ACK] Seq=49233 Ack=670 Win=30720 Len=1448 TSval=1111950730 TSe
85	0.303196	55.230	3.9.163	TCP	1518	80 字节 6148 [ACK] Seq=50681 Ack=670 Win=30720 Len=1448 TSval=1111950730 TSe
86	0.303197	55.230	3.9.163	TCP	1518	[TCP Out-Of-Order] 80 字节 6148 [ACK] Seq=47785 Ack=670 Win=30720 Len=1448 T

```

[iRTT: 0.000466000 seconds]
[Bytes in flight: 14480]
[Bytes sent since last PSH flag: 2896]
TCP Analysis Flags
  [Expert Info (Warning/Sequence): This frame is a (suspected) out-of-order segment]

```

**分析：**通过报文解析，发现重传的原因是有大量的TCP Out\_of\_Order数据包和TCP Retransmission  
 TCP Out\_of\_Order的原因分析：一般来说是网络拥塞或者数据包传输路径不同，导致顺序包抵达时间不同，延时太长，或者包丢失，需要重新组合数据单元。  
 TCP Retransmission原因分析：由于数据包传输超时引发的数据重传。

**结论：**数据包在传输过程中存在大量丢包，导致重传，因此属于传输过程中的问题。

## 案例3：国外用户访问服务器卡顿，如何办？



### 问题判断：

依据1：会话时延里面，客户时延比较大，说明在建立TCP时候，从客户端到服务器需要比较长时间，说明数据包在网络层传输质量不好。

依据2：TCP建立成功后，进行HTTP传输，但HTTP的重传比较多，大约有50%的重传，通过NTM报文解析，发现大量的TCP Out\_of\_Order数据包和TCP Retransmission，也说明是网络拥塞或者数据包传输路径不同，导致顺序包抵达时间不同，延时太长，或者包丢失，需要重新组合数据单元。

### 结论：

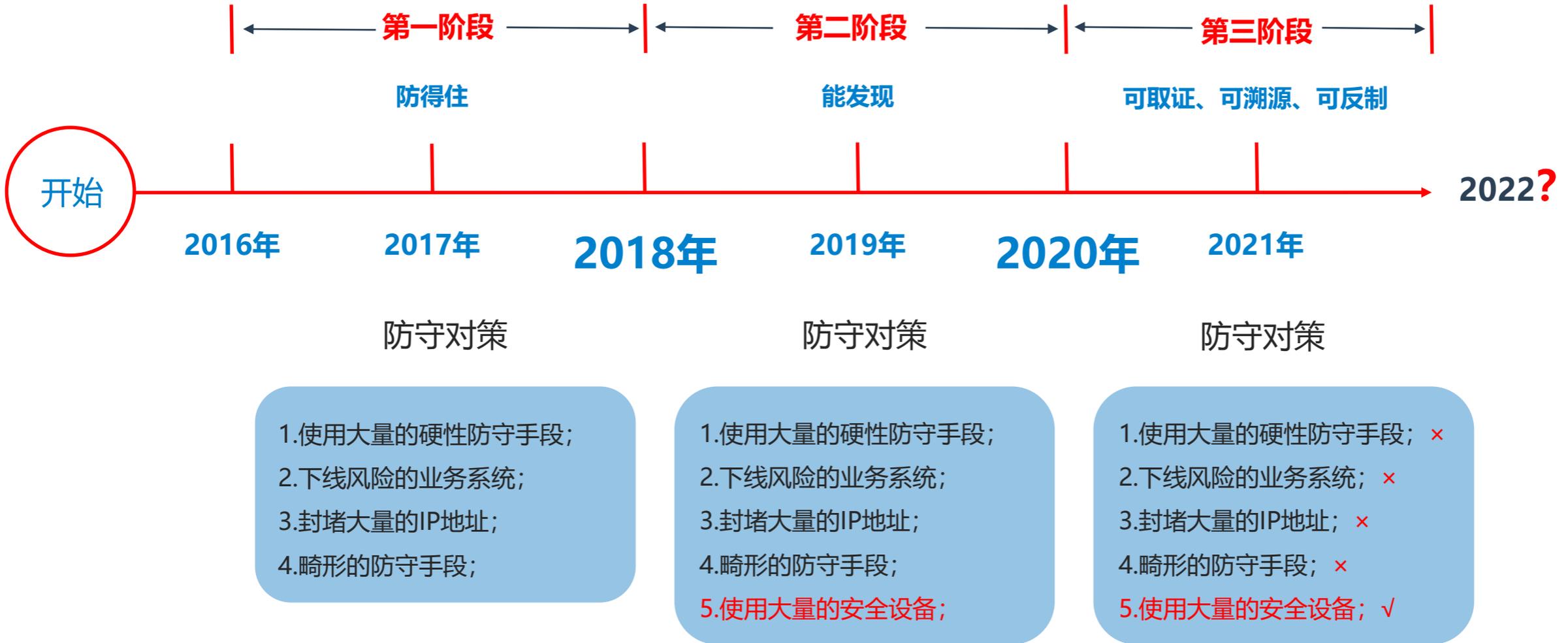
该问题不是服务器的问题，属于从客户端到服务器的网络问题。



03

## 全流量数据分析在护网时的应用

# 护网的三个阶段



# 护网期间，防守方加分项目

类别	得分标准	赋值规则	赋值上线	备注
发现类	发现攻击者进入逻辑隔离业务内网区事件	100分/次	1000分	提供的证据必须与攻击方提供的证据相吻合的 <b>详细分析报告</b> (时间、IP、日志、处置结果等)
消除类	处置异常账号	普通用户：应用层5分，系统层10分，数据库10分，网络设备25分。管理员用户：得分*2	500分	提供包含 <b>确凿证据的详细分析报告</b> (创建时间、访问日志、登录日志、处置结果等)，由裁判组研判后给分
应急处理类	积极配合应急组工作，根据线索能快速准确定位危害系统， <b>能提供充分的日志记录，配合执法机关有效固定证据完成勘验</b>	能高效配合完成应急工作的，得分300；配合一般的，得分200；差的-100	/	最高300分，最低-100分
追踪溯源类	对网络攻击事件的进行成功溯源， <b>提交有效证据材料构成证据链</b> ，还原完整攻击路径，证实攻击者的攻击行为	境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客	/	提供包含 <b>确凿证据</b> 的详细分析报告 (时间、平台截图、访问日志、告警详情等)

PS: 加分项目不止这几个，这里只是摘抄几个举例说明。

# 实战：护网期间，全流量数据留存可以作什么？



会话流量

源IP 任意IP 源端口 80 / 8000-8080 单个IP 10.3.8.211 目标端口

源IP ISP 任意 目标IP ISP 任意 源IP区域 任意 目标IP区域

时间范围 2022-04-19 08:29:41 - 2022-04-19 09:29:41 连接类型 所有

<input type="checkbox"/>	请求时间	源IP	目标IP	目标地理位置	传输协议	应用协议
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:57039	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:57037	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:57030	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:21561	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:57033	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	2.48.59:57036	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:57029	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:57028	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:57015	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:57017	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	48.59:57021	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/>	2022-04-19/08:29:41	2.48.59:57025	10.3.8.211:80		TCP	SYN_ACK

通过全流量的数据留存，发现从外网对内网一台服务器的端口扫描  
(很不幸，端口扫描不是加分项)

# 实战：护网期间，全流量数据留存可以作什么？



源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传/包数	下行重传/包数	重置 ⓘ	流量 ⓘ
9/08:29:41	55.30:39522	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:41	55.30:39524	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:41	55.30:39523	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	55.30:39525	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	55.30:39526	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	55.30:39527	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:44	55.30:39529	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:44	55.30:39530	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:44	55.30:39528	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:45	55.30:39538	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:45	55.30:39537	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:45	55.30:39536	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388

通过全流量的数据留存，发现从外网对内网一台数据库服务器的流量非常有规律。  
这个是啥原因呢？有可能是加分项目吗？

# 实战：护网期间，全流量数据留存可以作什么？



报文解析 报文交互 元数据 报文播放

报文显示过滤器

4	0.000323	240.5	10.3.55.30	TCP	78	[TCP Out-Of-Order] 1433 5129
5	0.000415	.55.30	10.3.240.5	TCP	70	51294 1433 [ACK] Seq=1 Ack=1
6	0.000416	.55.30	10.3.240.5	TCP	70	[TCP Dup ACK 5#1] 51294 1433
7	0.000617	.55.30	10.3.240.5	TDS	292	TDS7 login
8	0.000630	.55.30	10.3.240.5	TCP	292	[TCP Retransmission] 51294 1433
9	0.001315	10.3.240.5	10.3.	TDS	194	Response
10	0.001316	10.3.240.5	10.3.	TCP	70	1433 51294 [FIN, ACK] Seq=12
11	0.001330	10.3.240.5	10.3.	TCP	194	[TCP Out-Of-Order] 1433 5129

Packet Number: 1

Window: 0

▼ TDS7 Login Packet

> Login Packet Header

> Lengths and offsets

Client name: F XTBGYY

Username: byoaselect

Password: bylect

App name: jTDS

Server name: 10.3.240.5

Library name: S

Database name: RDSYS 710013

00b0	54 00 42 00	47 00 59 00	59 00 62 00	79 00 6f 00	T.B.G.Y.Y	b.y.o.
00c0	61 00 73 00	65 00 6c 00	65 00 63 00	74 00 83 a5	a.s.e.l.e.c.t.	
00d0	32 a5 53 a5	b3 a5 92 a5	f3 a5 63 a5	f3 a5 93 a5	2.S.....c....	
00e0	e2 a5 6a 00	54 00 44 00	53 00 31 00	30 00 2e 00	..j.T.D.S	.1.0...
00f0	33 00 2e 00	32 00 34 00	30 00 2e 00	35 00 6a 00	3..2.4.0	...5.j.
0100	54 00 44 00	59 00 59 00	44 00 59 00	59 00 59 00	T.D.S.D.	S.V.S

## NTM分析

外网某IP对数据库进行进行**连续**的登录操作。

登录的用户名为 “byoaselect”

# 实战：护网期间，全流量数据留存可以作什么？



报文解析 报文交互 元数据 报文播放

报文显示过滤器

4	0.000323	10.3.240.5	55.30	TCP	78	[TCP Out-Of-Order
5	0.000415	55.30	10.3.240.5	TCP	70	51294 数 1433 [
6	0.000416	55.30	10.3.240.5	TCP	70	[TCP Dup ACK 5#1]
7	0.000617	55.30	10.3.240.5	TDS	292	TDS7 login
8	0.000630	55.30	10.3.240.5	TCP	292	[TCP Retransmissi
9	0.001315	10.3.240.5	10.3.5	TDS	194	Response
10	0.001316	10.3.240.5	10.3.0	TCP	70	1433 数 51294 [
11	0.001330	10.3.240.5	10.3.5	TCP	194	[TCP Out-Of-Order

## Token - Error

Token length: 104

SQL Error Number: 18456

State: 1

Class (Severity): 14

Error message length: 21 characters

Error message: 攀儿桐 byoaselect 鋼海緯澶辨觸鉅

Server name length: 25 characters

Server name: WIN-6F1CSPSJSQM\MSSQL2018

Process name length: 0 characters

Line number: 1

## > Token - Done

0050	00 18 48 00	00 01 0e 15	00 28 75 37	62 20 00 27	..H.....	(u7b .'
0060	00 62 00 79	00 6f 00 61	00 73 00 65	00 6c 00 65	.b.y.o.a.	s.e.l.e
0070	00 63 00 74	00 27 00 20	00 7b 76 55	5f 31 59 25	.c.t.'. .	{vU_1Y%
0080	84 02 30 10	57 00 40 00	40 00 24 00	36 00 46 00	O W T N	- 6 F

## NTM分析

外网某IP对数据库进行进行**连续**的登录操作。数据库服务器进行响应，提示token 错误，同时，返回错误提示。

## 加分项目：

加分类别：发现类

加分标准：发现账号异常

加分：数据库账号10分，上限为500分



# 实战：护网期间，全流量数据留存可以作什么？



报文解析 报文交互 元数据 报文播放

报文显示过滤器

15	0.005422	242.47	10.112.48.129	MySQL	135	Request Query
16	0.006288	10.112.48.129	242.47	MySQL	183	Response
17	0.006590	242.47	10.112.48.129	MySQL	136	Request Query
18	0.007432	10.112.48.129	242.47	MySQL	184	Response
19	0.007736	242.47	10.112.48.129	MySQL	136	Request Query
20	0.008592	10.112.48.129	242.47	MySQL	183	Response

> Frame 17: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits)  
> Ethernet II, Src: d0:94:66:67:17:8d (d0:94:66:67:17:8d), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4068  
> Internet Protocol Version 4, Src: 242.47, Dst: 10.112.48.129  
> Transmission Control Protocol, Src Port: 46710, Dst Port: 3306, Seq: 302, Ack: 413, Len: 66

MySQL Protocol

Packet Length: 62

Packet Number: 0

Request Command Query

Command: Query (3)

Statement: select skill\_order from knowledgePoint where skill\_id = '111'

```
0000  88 df 9e 39 2a 01 d0 94 66 67 17 8d 81 00 0f e4  ...9*..f g.....
0010  08 00 45 00 00 76 16 2d 40 00 40 06 ed 31 0a 03  ..E..v.-@ .@.l..
0020  f2 2f 0a 70 30 81 b6 76 0c ea d8 0c f5 b6 5d db  ./..p0..v. ....].
0030  cd 9c 80 18 00 ed de e1 00 00 01 01 08 0a 2d 2a  .....- *
0040  b9 6b 92 38 ac 40 3e 00 00 00 03 73 65 6c 65 63  .k.8.@>.. ..selec
0050  74 20 73 6b 69 6c 6c 5f 6f 72 64 65 72 20 66 72  t skill_o rder fr
```

## NTM分析

外网某IP对数据库进行进行root登录操作。登录成功后，进行数据库相关操作。

## 加分项目：

加分类别：追踪溯源类

加分标准：对网络攻击事件的进行成功溯源，提交有效证据材料构成证据链，还原完整攻击路径，证实攻击者的攻击行为

加分：境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客



报文解析 报文交互 元数据 报文播放

展示方式 按属性

- > command
- > charset
- > warnings
- > version
- > user
- > unused
- > thread\_id
- > response\_code
- > request
- ✓ query

⊕ 报文9	SET AUTOCOMMIT = 0
⊕ 报文11	BEGIN
⊕ 报文13	select 棍斤拷棍斤拷棍斤拷, 棍斤拷棍斤拷棍斤拷棍斤拷棍斤拷 from timu where id = 15
⊕ 报文15	select skill_order from knowledgePoint where skill_id = '347'
⊕ 报文17	select skill_order from knowledgePoint where skill_id = '851'
⊕ 报文19	select skill_order from knowledgePoint where skill_id = '863'
⊕ 报文21	select skill_order from knowledgePoint where skill_id = '142'
⊕ 报文23	select skill_order from knowledgePoint where skill_id = '817'
⊕ 报文25	select skill_order from knowledgePoint where skill_id = '167'
⊕ 报文27	select skill_order from knowledgePoint where skill_id = '796'
⊕ 报文29	COMMIT

## NTM分析

通过元数据分析，将同一会话里面的报文进行数据还原，还原相关操作的细节。

### 加分项目：

加分类别：追踪溯源类

加分标准：对网络攻击事件的进行成功溯源，提交有效证据材料构成证据链，还原完整攻击路径，证实攻击者的攻击行为

加分：境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客

# 实战：护网期间，全流量数据留存可以作什么？





2022

可视化网络领导者

THANK YOU