2022

畅享连世界

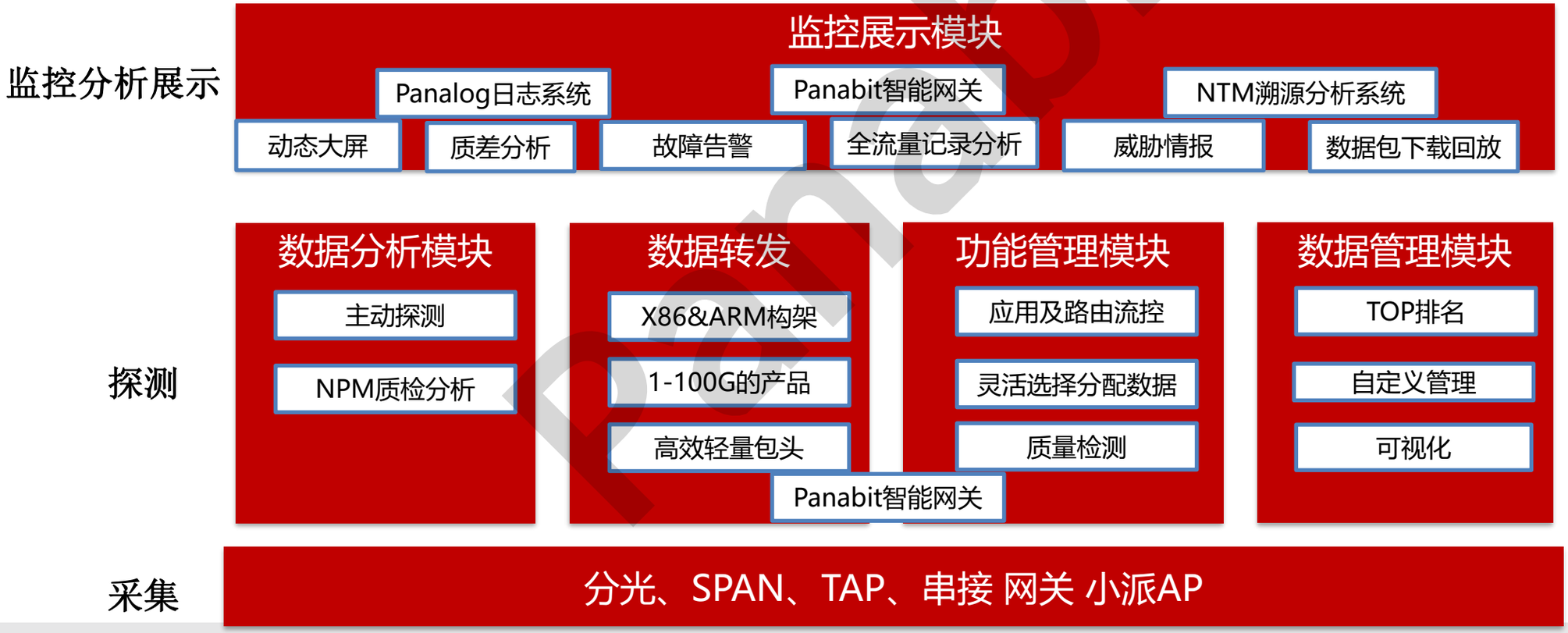
派网遥测功能讲解

01

派网遥测特点介绍

Panabit遥测简介

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。



派网遥测特性

数据流量灵活调度

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

业务级故障定位

探针作为测量单位进行质量监测

主动检测目标网络质量

网络会话溯源，原始数据包溯源回放

精确的协议识别

精确的协议识别1400+，现网识别率95%

应用协议实时更新

丰富的流量可视化

可视化流量，连接趋势，应用IP排名

原始数据包之间的交互，自定义协议
管理

高性能稳定运行

双OS保护，毫秒级切换

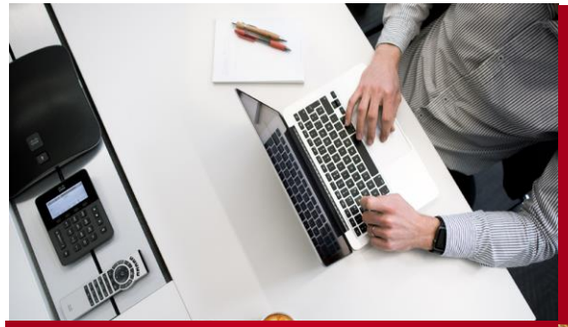
1-100G硬件应对不同的场景

全流量分析

基于五元组，应用，域名，url，地理
位置等进行大数据分析溯源满足等保
2.0的需求

支持原始数据包分析，回放，下载

Panabit遥测特点



传输安全性

原始包溯源

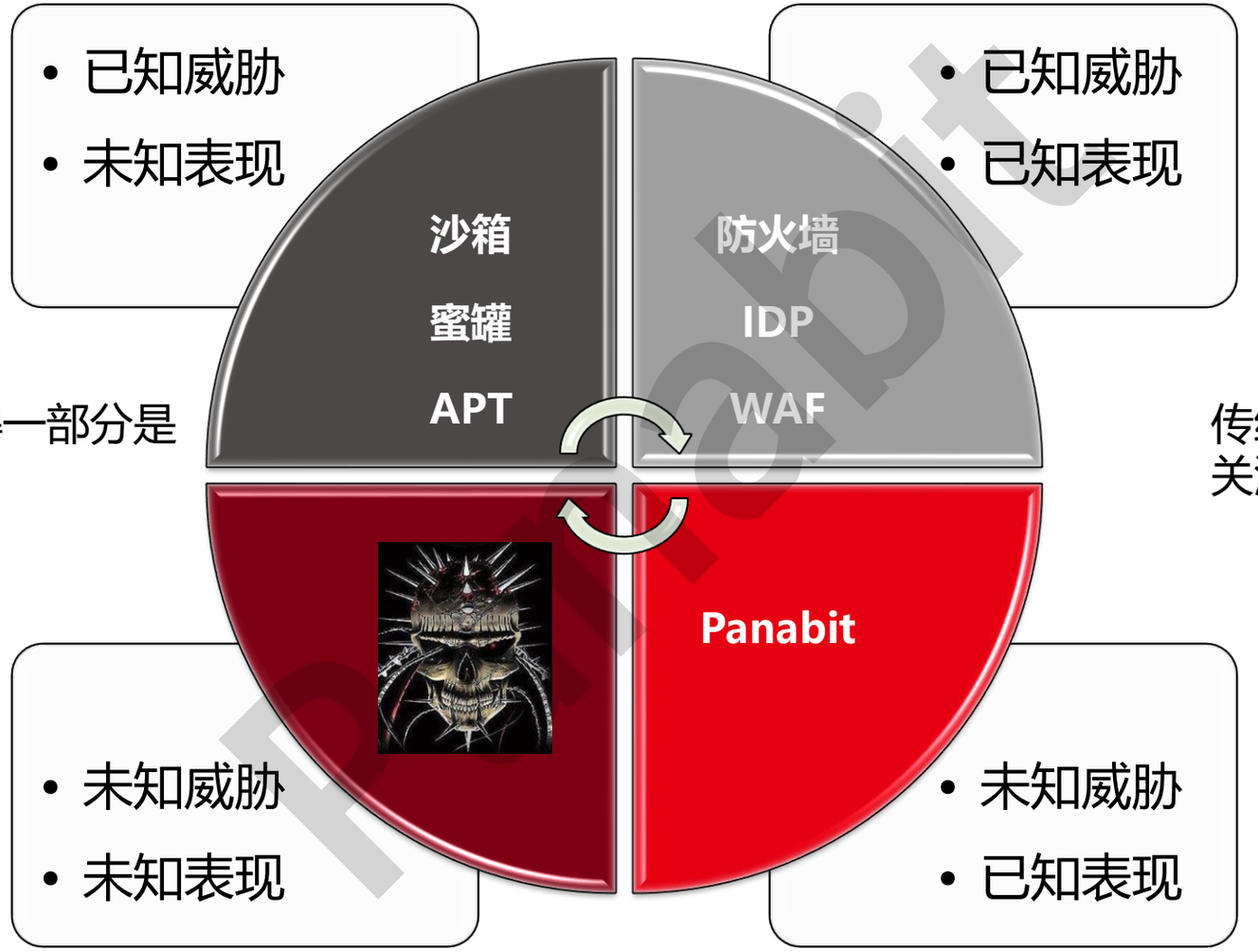
灵活调度性

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。

Panabit遥测全流量分析

Panabit®



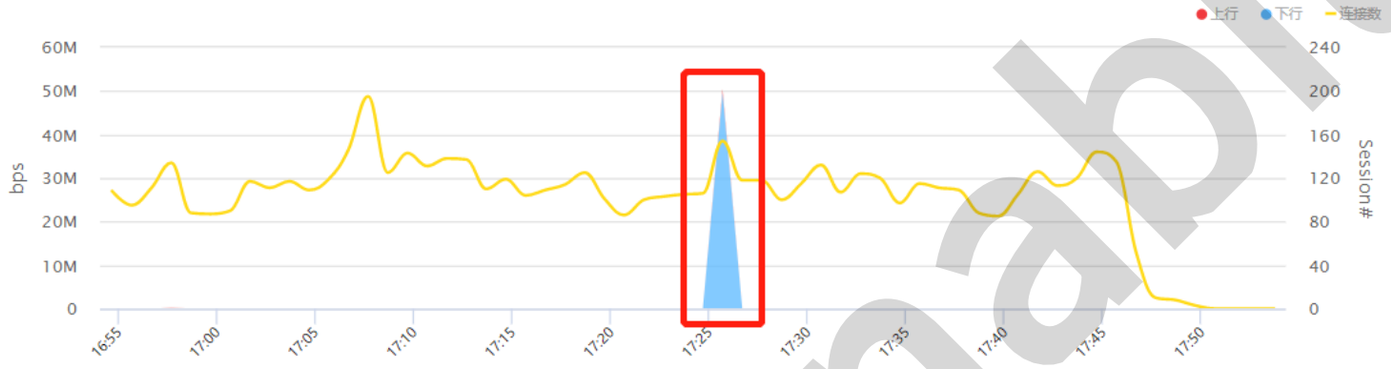
全流量分析相当重要得一部分是对**未知流量的探索**

传统安全的黑名单理念更关注于已知流量的表现

Panabit遥测流量诊断

流量诊断

源IP	x.x.x.x	源端口	0-65535	目标IP	x.x.x.x	目标端口	0-65535	传输协议	任意	应用协议	未知协议
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	2021-06-10 16:54:41 - 2021-06-10 17:54:41										



序号	应用协议	总请求数	上行	下行
1	未知应用	6150	30.42M	376.04M

1 总共 1

序号	源IP	总请求数	上行	下行
1	192.168.10.100	1069	120.25K	82.64K
2	192.168.0.199	507	6.33M	0
3	192.168.100.21	466	4.94M	11.90K
4	192.168.8.21	426	3.40M	17.94K
5	192.168.1.10	389	686.92K	16.74K

1 2 总共 57

序号	目标IP	总请求数	上行	下行
1	120.76.239.144	1336	318.83K	99.66K
2	112.124.51.144	1144	16.12M	106
3	185.209.85.193	1043	117.18K	82.64K
4	1.255.255.254	386	4.04M	0
5	210.12.171.196	380	111.45K	0

1 2 3 ... 7 总共 187

序号	目标域名	总请求数	上行	下行

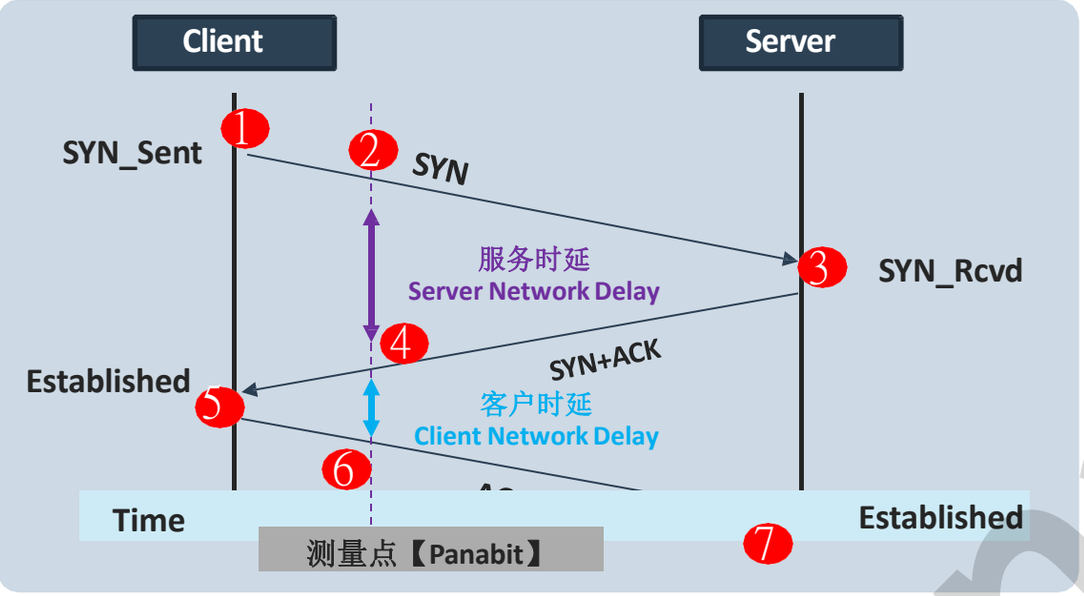
无数据

Panabit遥测NPM延时

Panabit,NPM延时参数展示

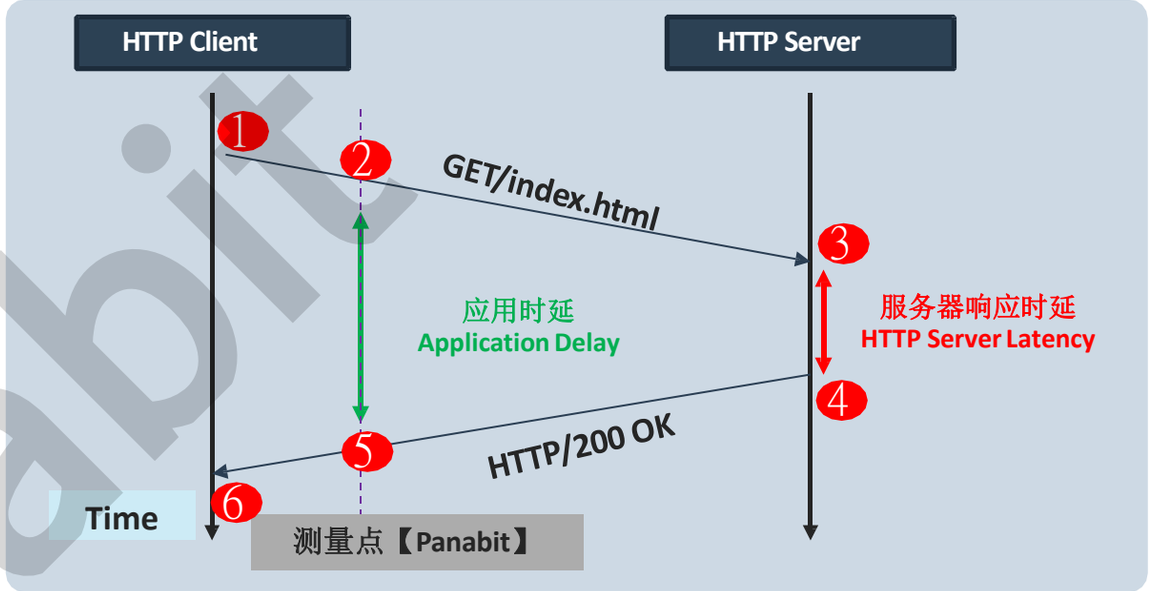
应用	协议	状态	首包接口	连接	地理位置	策略路由	接口线路	时长	客户时延	服务时延	应用时延	上行报文	下行报文	最大包长	MSS	流量	HOST
其它头条视频	tcp	OK	em5	源:100.64.6.169:41980 目:182.242.51.151:80	云南昆明|电信			84	92.82	19.72	26.00	0/2	12/1395	661/1258	1460	1310/1752992	v26.toutiaovod.co...
其它头条视频	tcp	OK	em5	源:100.64.6.169:41976 目:182.242.51.151:80	云南昆明|电信			87	41.82	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	dig.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...			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:49.4.19.226:443	北京|电信/联通/...			15	8.25	40.00	40.76	0/3	0/6	631/1258	1460	1357/4655	logservice.hicloud....

Panabit遥测NPM延时



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



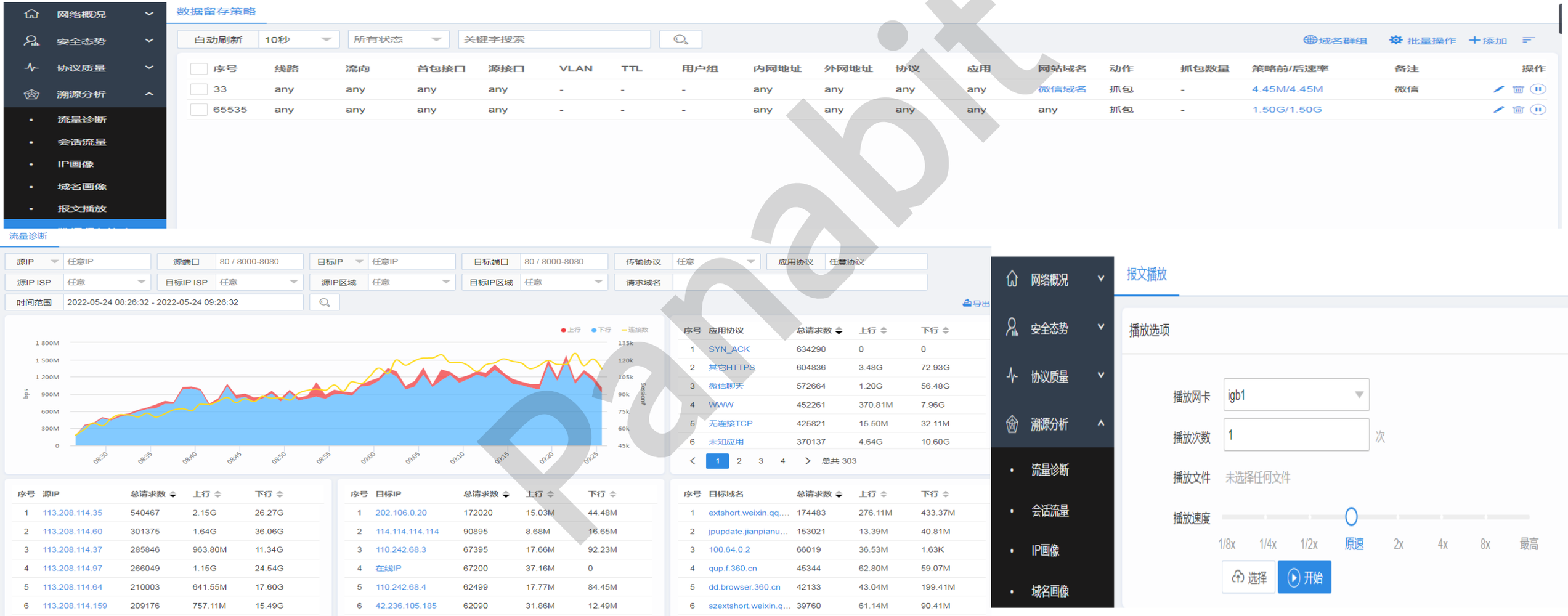
时间点2:智能网关记录接收Client的HTTP/GET包的时间戳
时间点5:智能网关记录接收Server的HTTP/200OK包的时间戳

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	测量点至应服务器的网络时延（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



02

典型场景

遥测基本概念

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

Panabit网关

- 流量可视化实时监控
- 自定义管理
- 遥测隧道
- 故障定位及报警
- 主动探测
- 数据流量多份分配

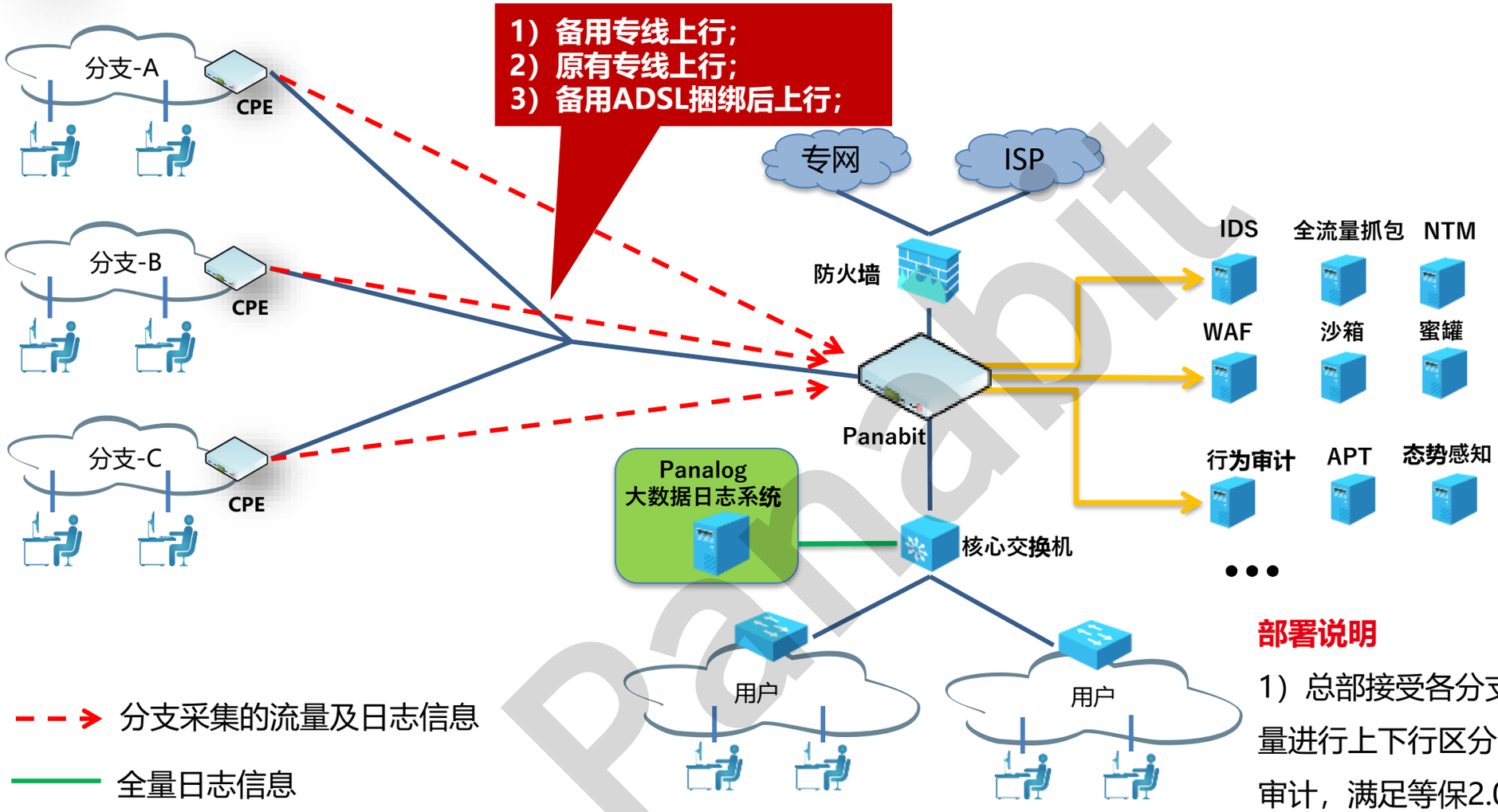
Panalog

- 可视化流量监控及查询
- 质差分析
- 五元组会话DNS url存储
- url DNS 去向地域
  异常诊断等信息分析
- 安全分析，威胁情报

NTM

- 原始数据包深度分析
- 原始数据包下载回放
- 威胁情报
- 质差分析诊断
- 遥测隧道服务端
- 全流量数据包存储

典型场景一：大型网络多分支数据采集+分析

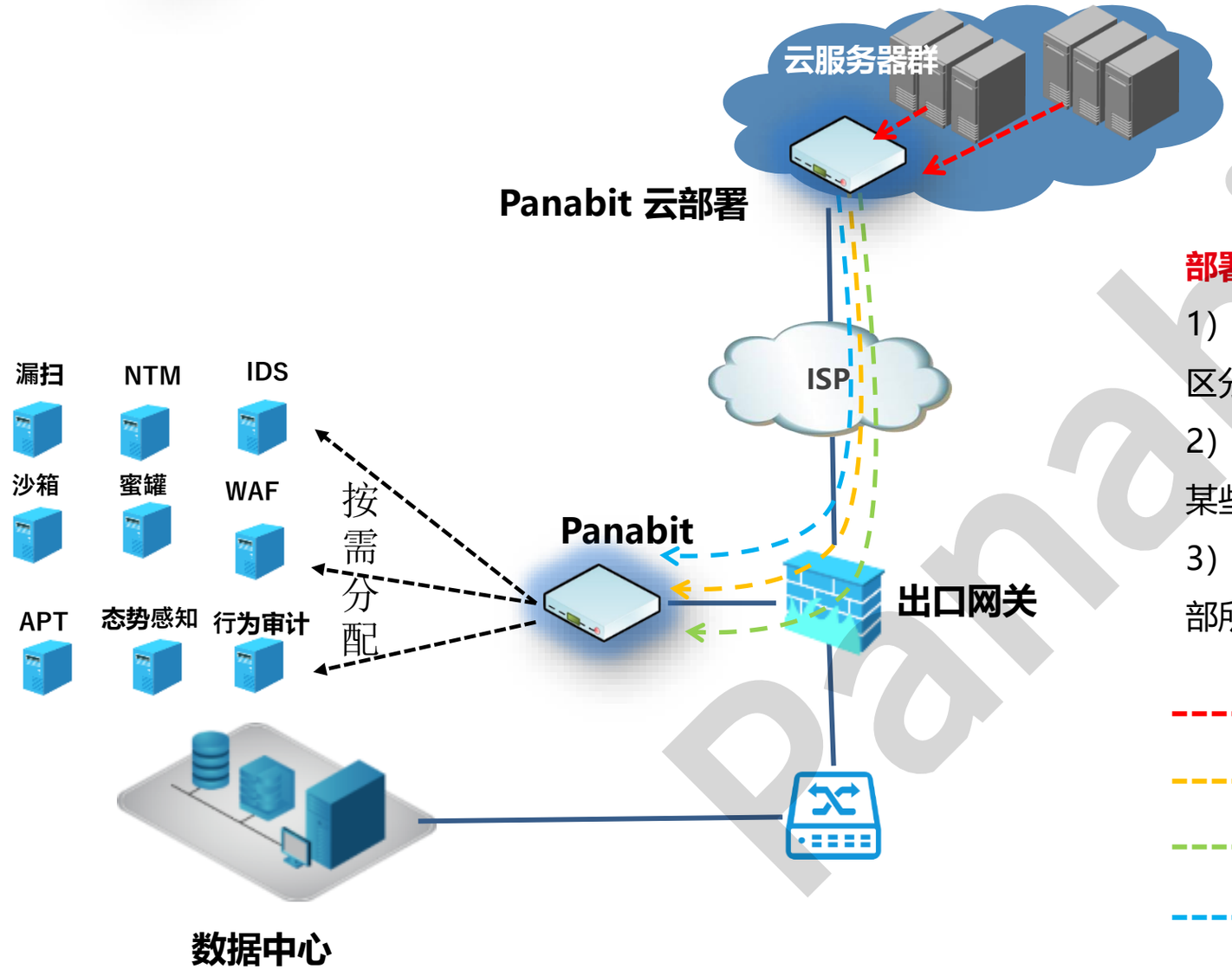


部署说明

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



部署说明

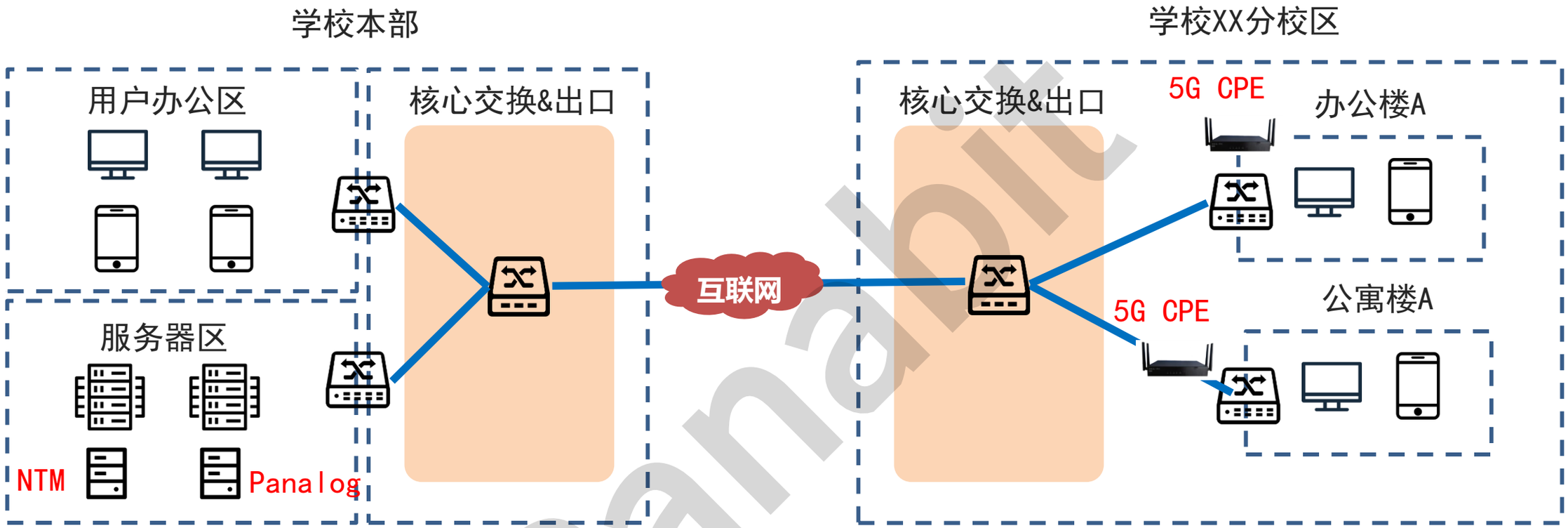
1）云端虚拟化部署Panabit采集云端内所有服务器南北向流量，并区分上下行

2）对流量进行筛选，去掉等低价值流量，或者可以根据需求，保留某些关键应用

3）将筛选后的流量，通过iWAN传输到总部进行进一步分析，与总部所有安全设备进行对接

- 镜像流量
- 筛选后的上行流量
- 筛选后的下行流量
- 全量日志

场典型场景三：通过5GCPE遥测采集数据+分析



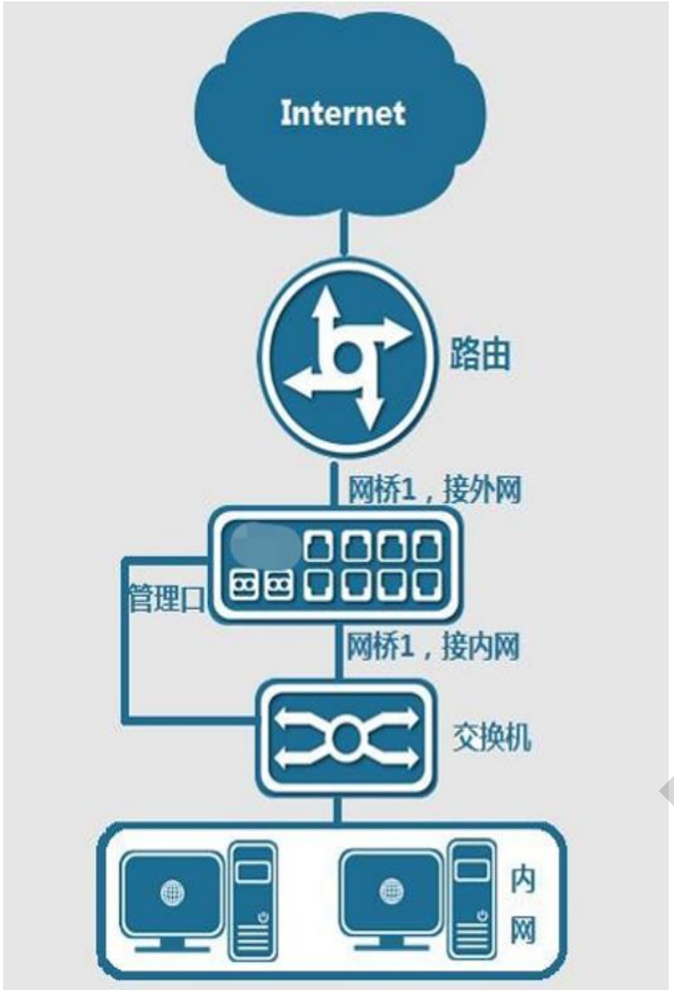
部署说明

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和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

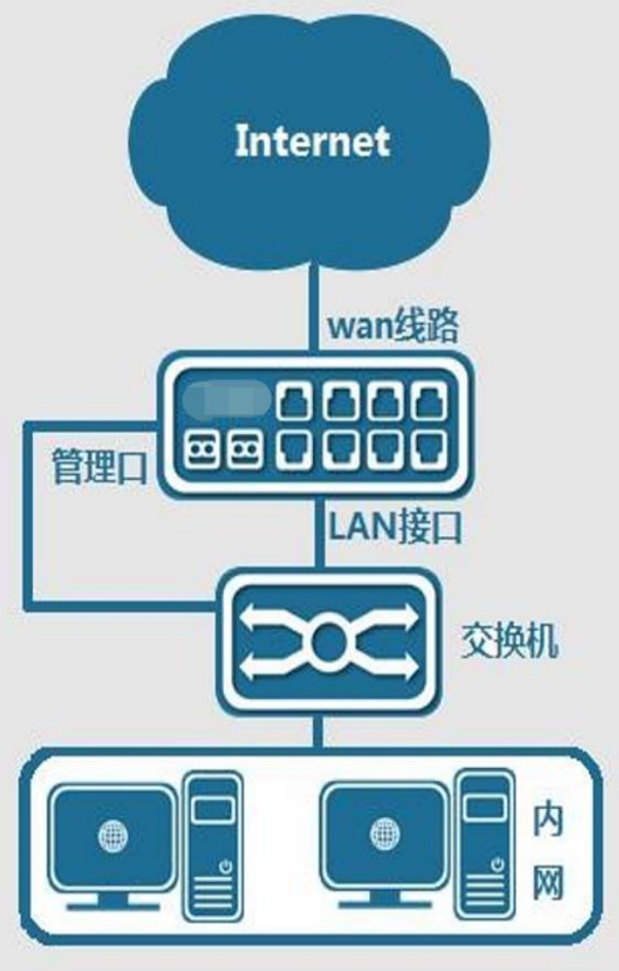
部署方式

探针部署



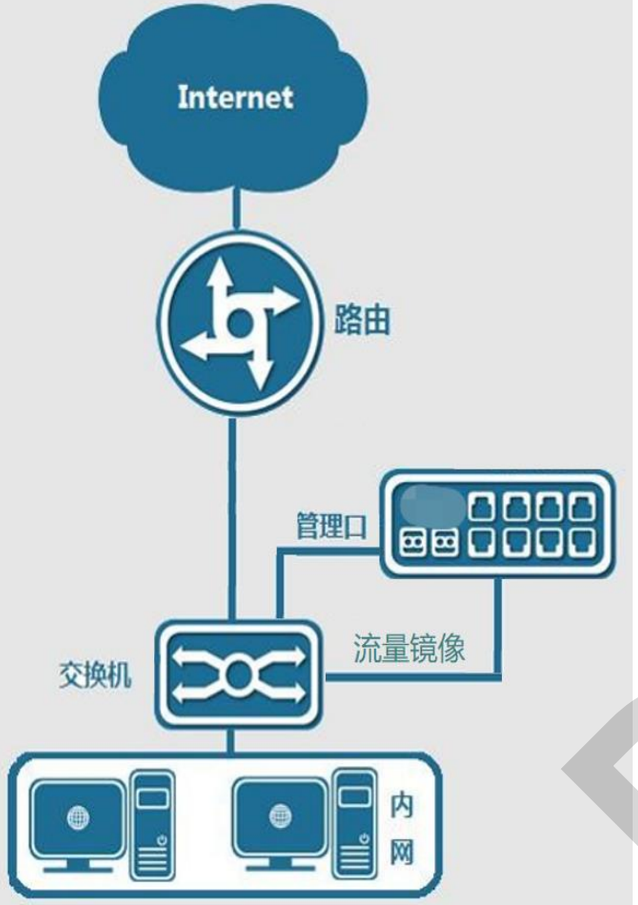
网桥模式				
网络管理	**应用路由**	**网络优化**	**上网行为管理**	**可视化应用服务**
接入用户管理	SD-WAN组网	负载均衡	IP用户画像	流量可视化
接入流量管理	策略路由	重要IP带宽保障	用户虚拟身份	IP用户可视化
遥测功能	认证计费功能	重要网站和应用保障	上网行为日志查询	应用可视化
过滤黄赌毒等恶意网站	DHCP功能	DNS智能控制	上网日志信息回溯	连接可视化
精细化业务分流	NAT功能	业务级质量监测/故障定位	上网流量信息对比	趋势对比可视化

探针部署



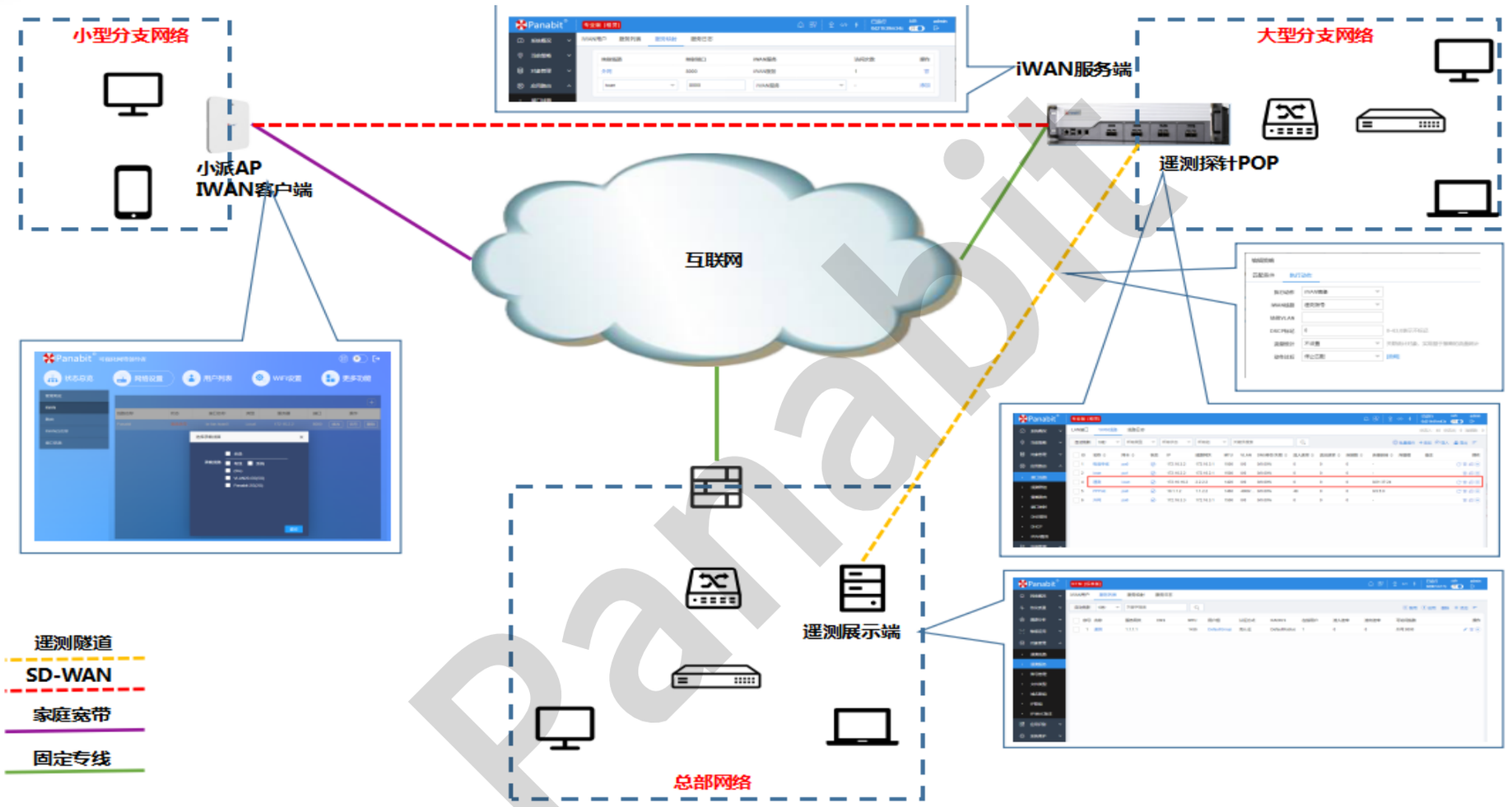
网关模式				
网络管理	**应用路由**	**网络优化**	**上网行为管理**	**可视化应用服务**
接入用户管理	SD-WAN组网	负载均衡	IP用户画像	流量可视化
接入流量管理	策略路由	重要IP带宽保障	用户虚拟身份	IP用户可视化
遥测功能	认证计费功能	重要网站和应用保障	上网行为日志查询	应用可视化
过滤黄赌毒等恶意网站	DHCP功能	DNS智能控制	上网日志信息回溯	连接可视化
精细化业务分流	NAT功能	业务级质量监测/故障定位	上网流量信息对比	趋势对比可视化

探针部署

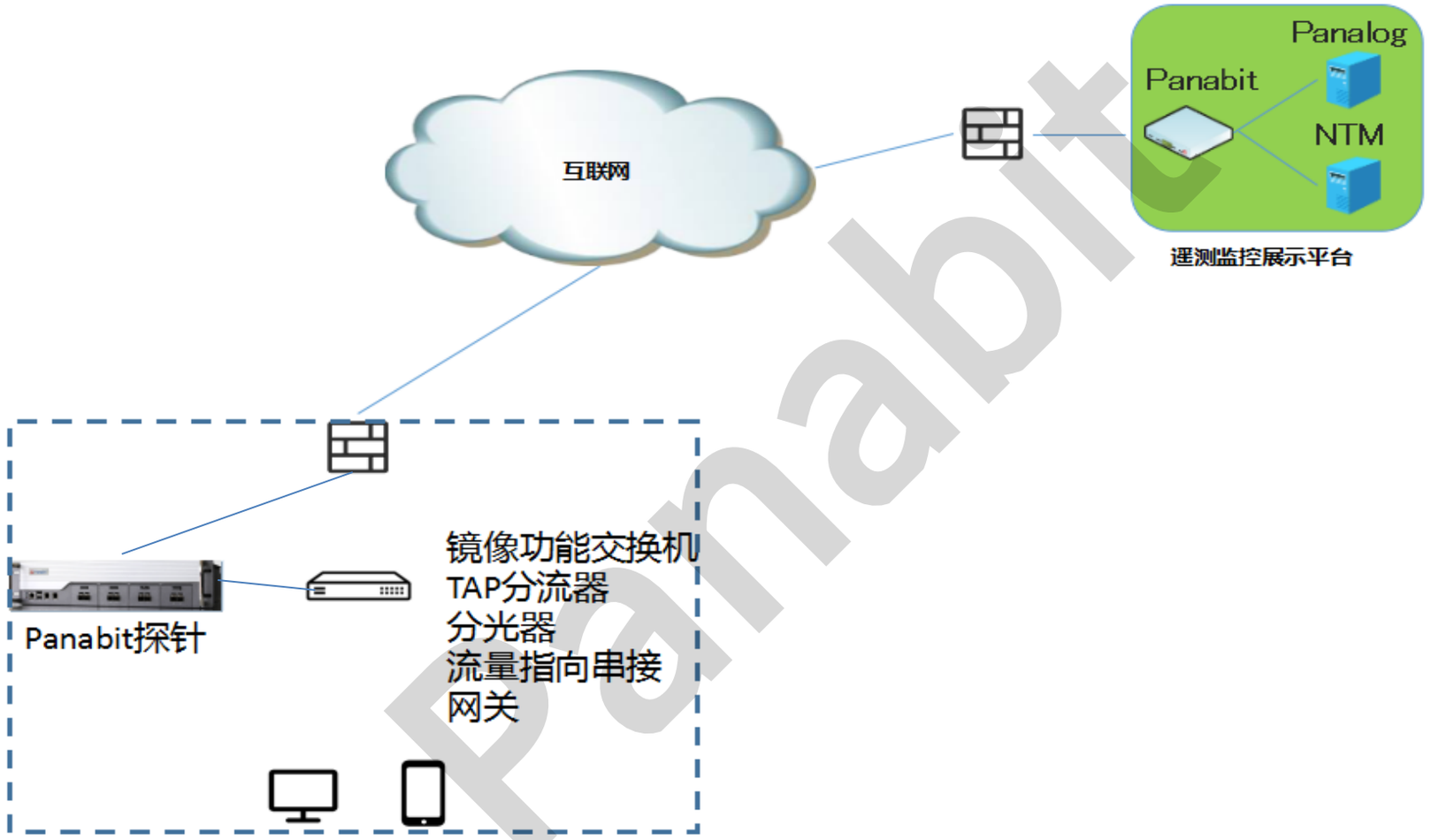


旁路模式			
网络管理	**网络优化**	**上网行为管理**	**可视化应用服务**
TCP重置	业务级质量监测/故障定位	IP用户画像	流量可视化
遥测功能		用户虚拟身份	IP用户可视化
		上网行为日志查询	应用可视化
		上网日志信息回溯	连接可视化
		上网流量信息对比	趋势对比可视化

采集器-小派AP



采集器-其它采集



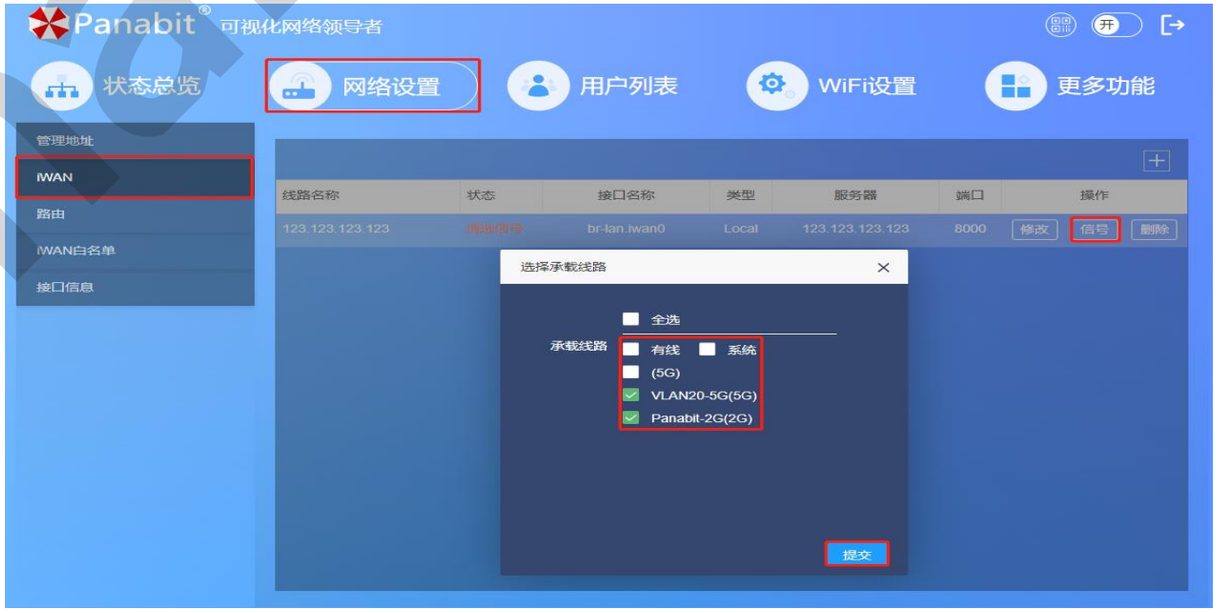
Panabit®

04

遥测配置

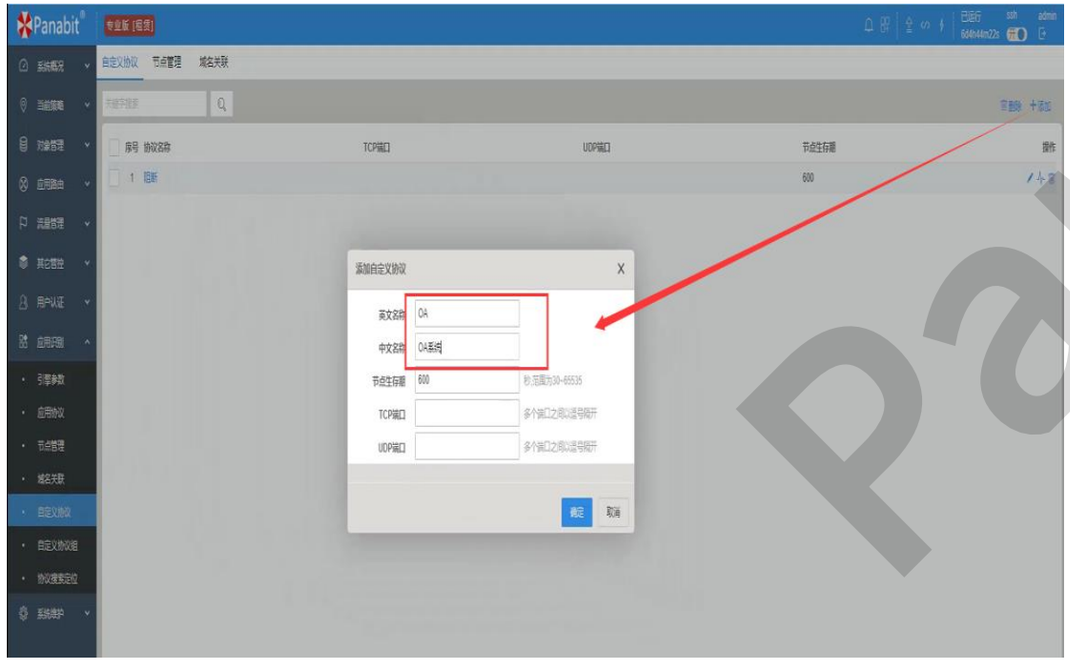
流量采集-小派AP

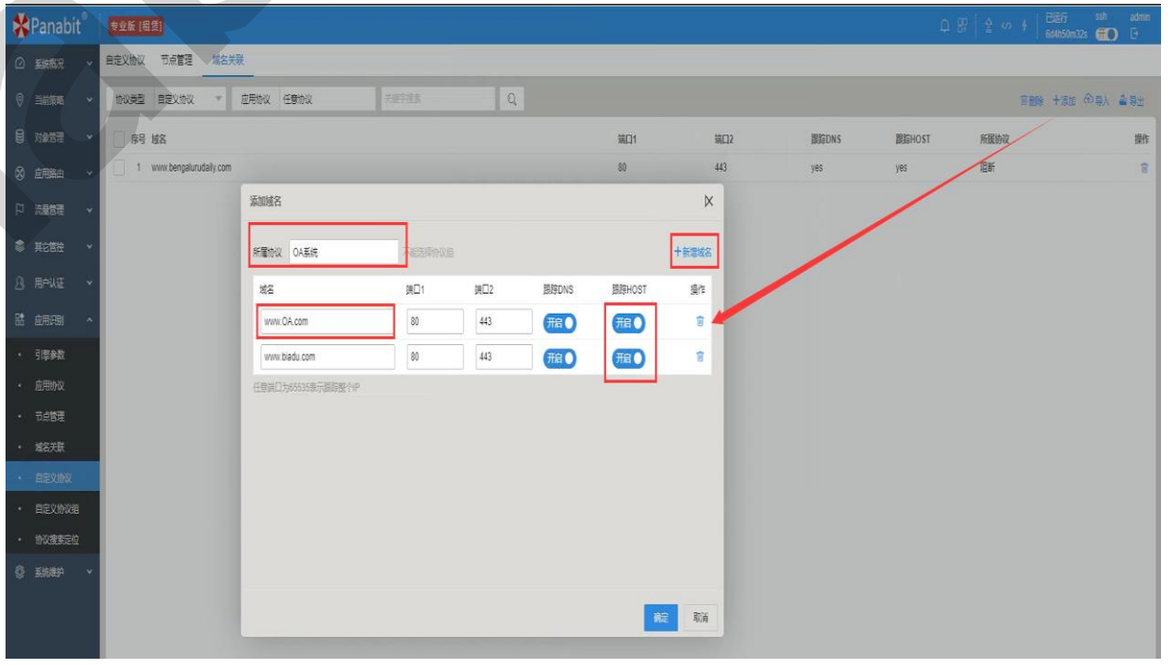
1	连接WiFi或者是LAN2口，电脑配置192.168.166.X/24的IP，通过https://192.168.166.254登录AP。
2	进入网络设置——》iWAN，点击添加，填写iWAN相关的信息
3	选择走iWAN的信号或者是有线接口。配置完成之后即可连接iWAN。



Panabit-自定义对象域名

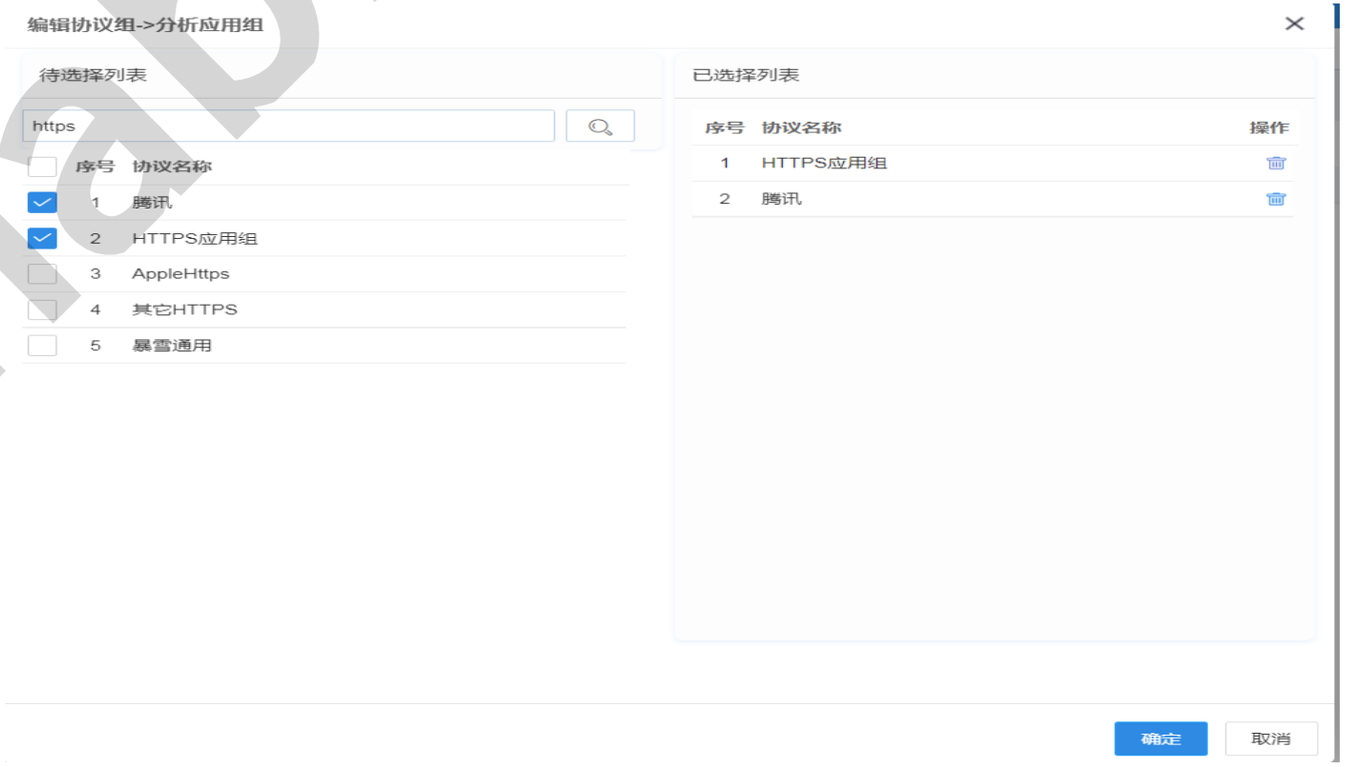
1	创建自定义协议	进入【应用识别】-【自定义协议】，在右上角点击【添加】按钮，输入中英文名称
2	关联域名	进入【域名关联】，点击【添加】按钮。选择所属协议，开启“跟踪host”





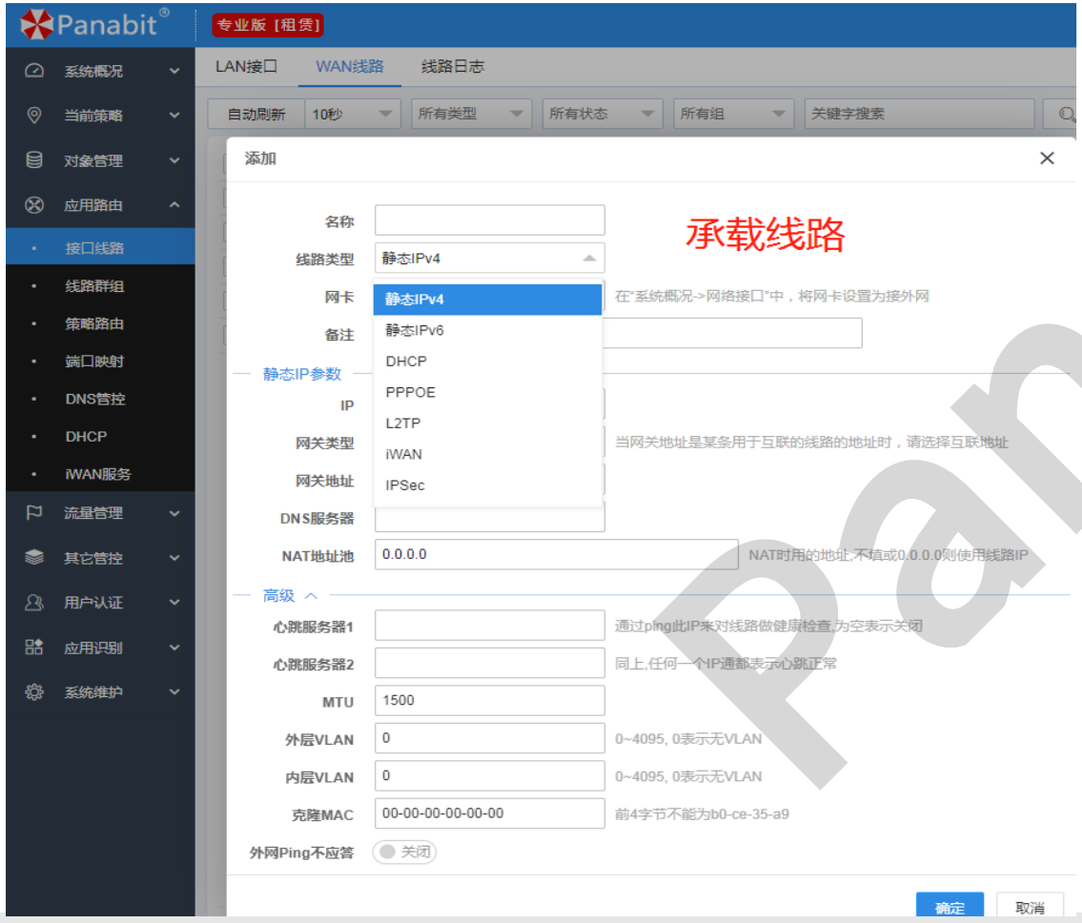
Panabit-自定义对象自定义归类

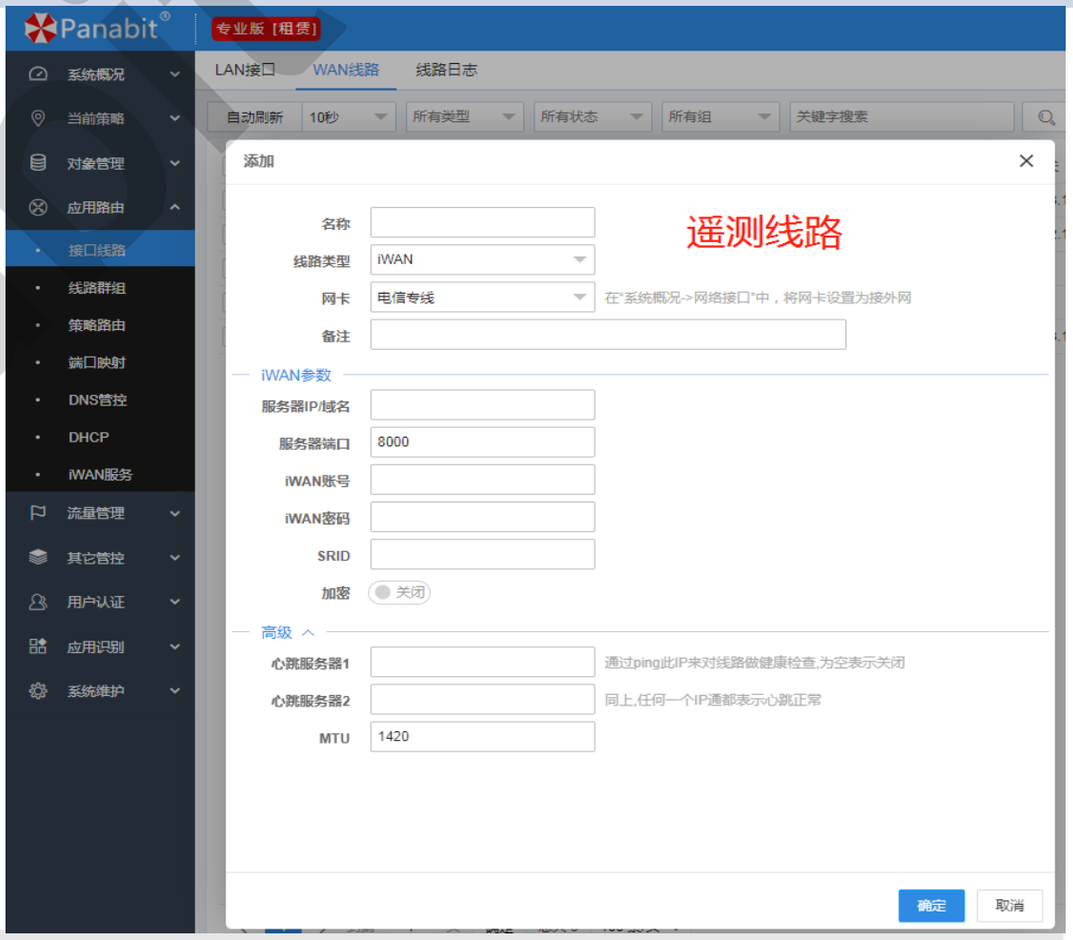
1	创建自定义协议组	进入【应用识别】-【自定义协议组】，点击右上角【添加】，输入自定义协议组的中英文名称
2	选择用遥测的应用重新归类	在弹出的窗口选择相应的业务协议，如我们之前创建的域名或者协议库中的特征名称如HTTPS应用组等需要分析的内容。点击【确定】



遥测隧道-探针客户端

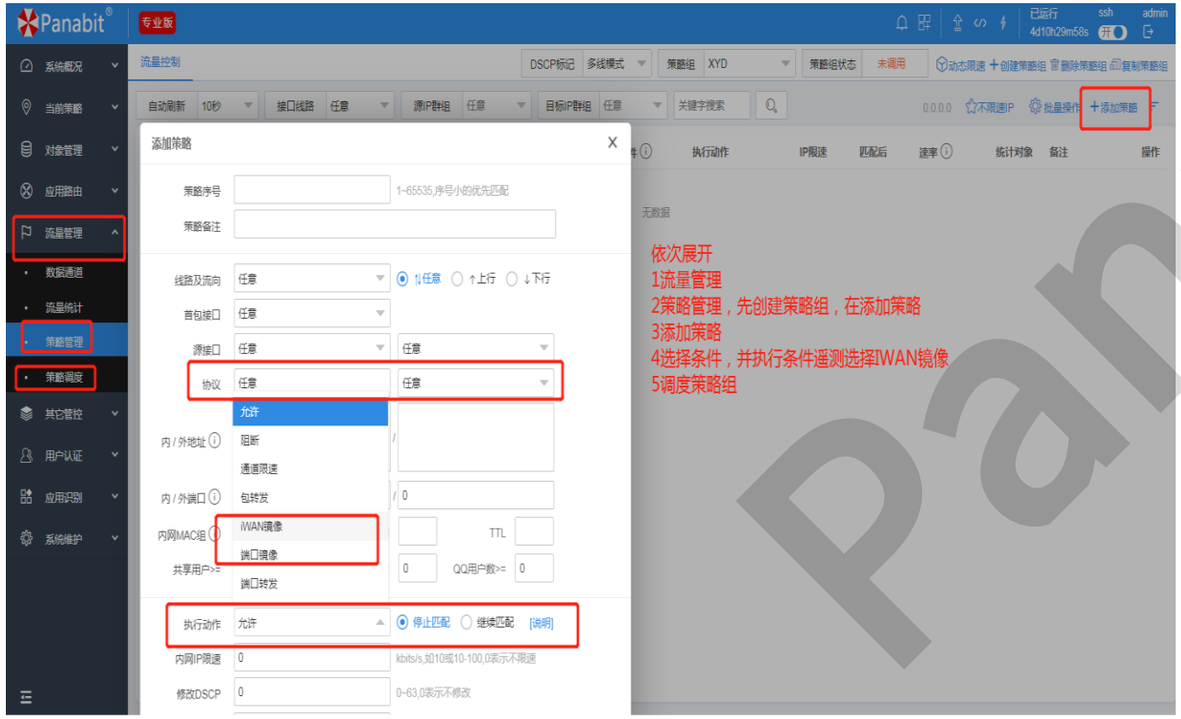
1	创建承载线路	【应用路由】-【接口线路】-【WAN线路】中创建承载线路，线路类型根据实际情况选择。
2	创建遥测隧道	【应用路由】-【接口线路】-【WAN线路】中创建承载线路，线路类型选择IWAN，并填写服务IP端口帐号等信息。

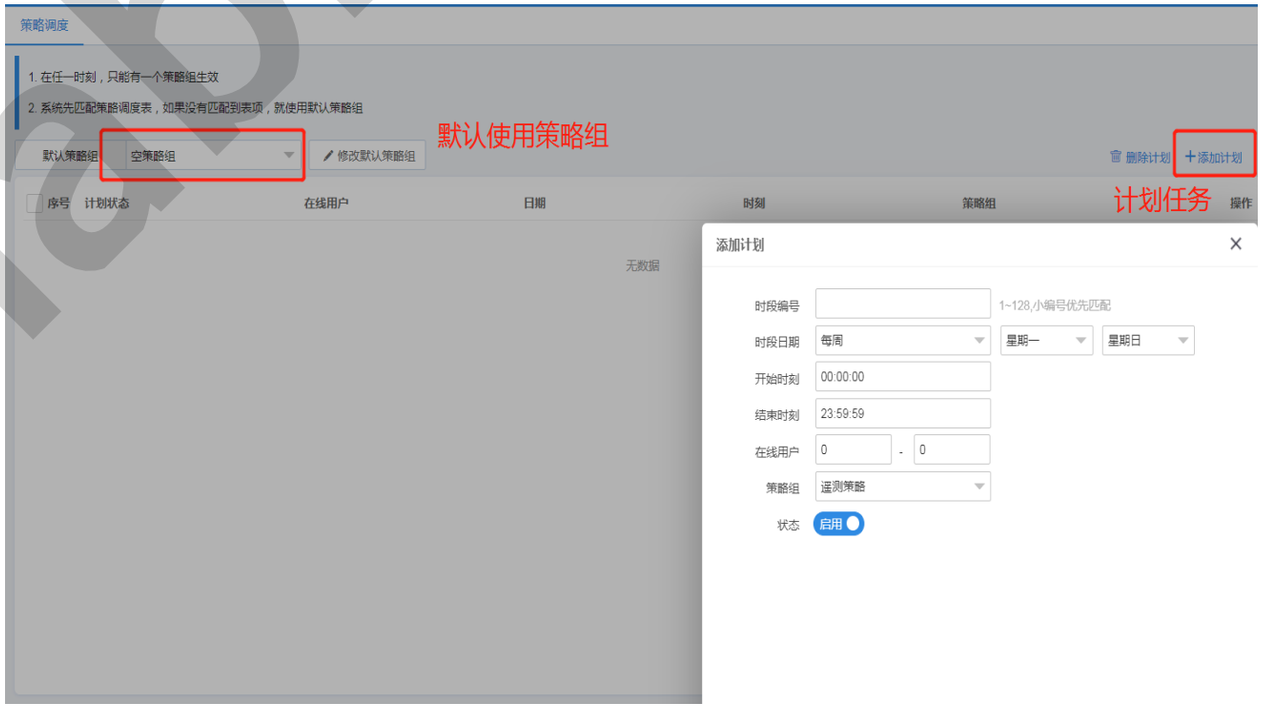




Panabit-灵活调度

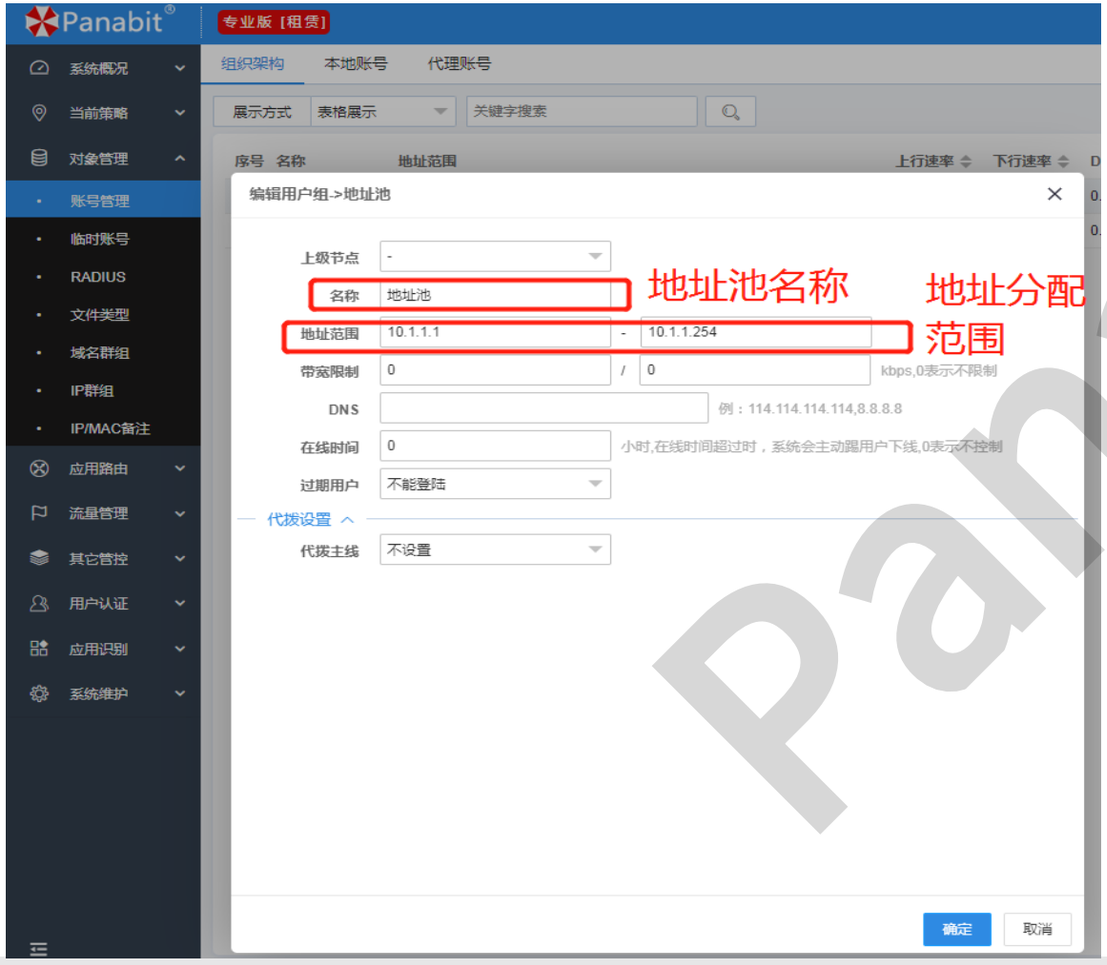
1	创建策略组-添加策略	在【流量管理】-【策略管理】中点击【创建策略组】。在弹出窗口中输入框中输入新创建策略组的名称，右上角点击添加策略。
2	选择条件执行动作	在弹出窗口中【策略序号】输入序号，序号越小越优先，选择五元组或接口流量首包接口，应用协议作为条件，执行动作遥测选择IWAN镜像，也可镜像到某网卡。
3	调度策略组	在【流量管理】-【策略调度】，可执行缺省调度，也可以选择基于时间等方式进行调度。

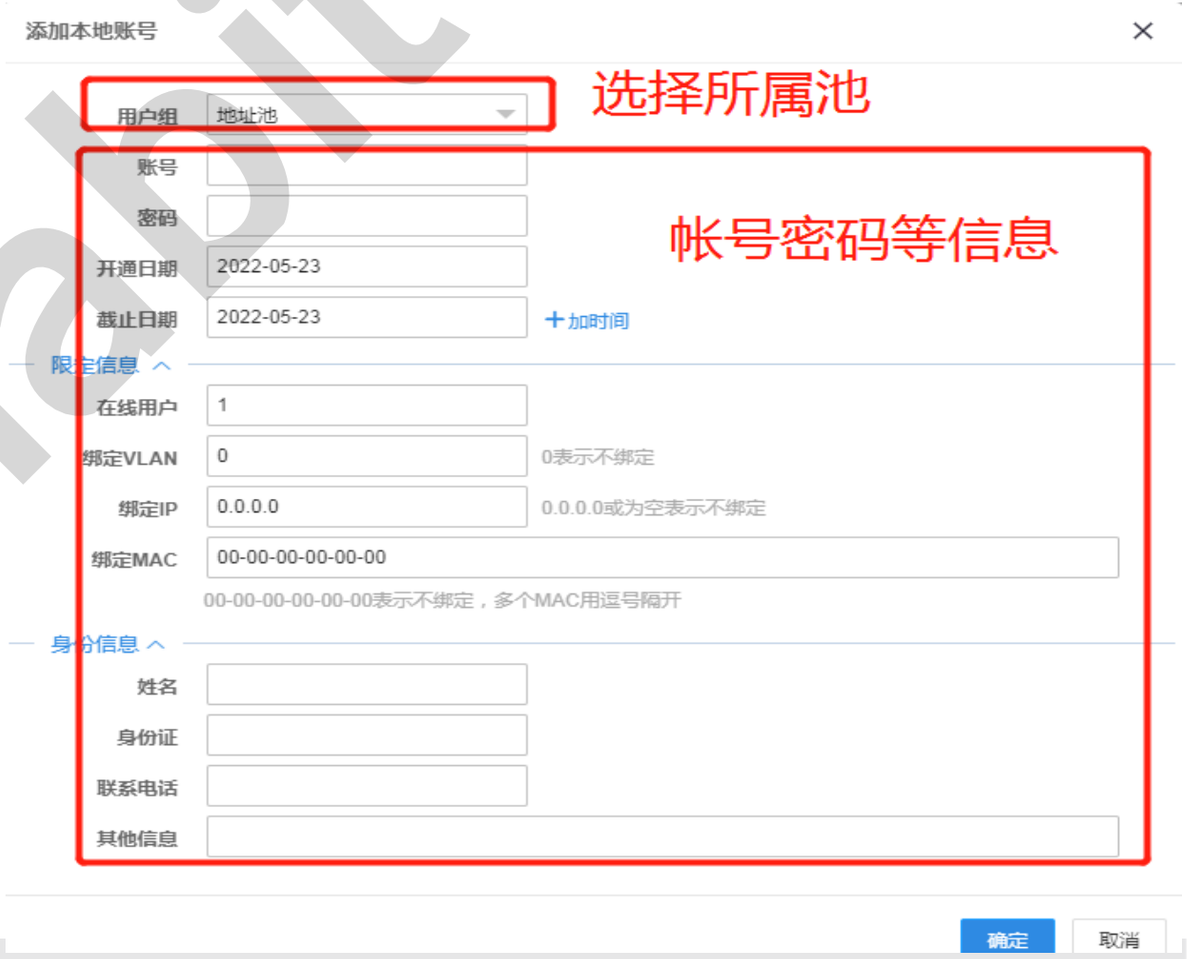




遥测隧道-服务端Panabit网关

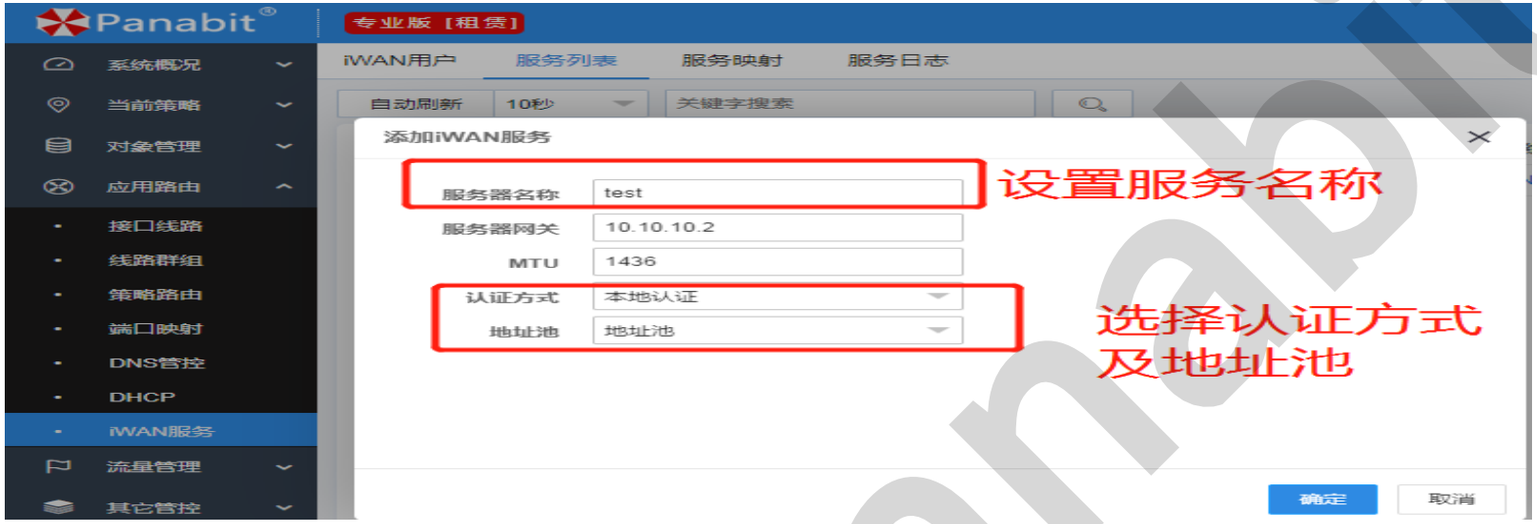
1	创建地址池	在【对象管理】-【账号管理】-【组织架构】中，点击【添加】按钮，创建地址池
2	创建帐号	在【对象管理】-【账号管理】-【本地帐号】创建帐号，并设置帐号归属地址池





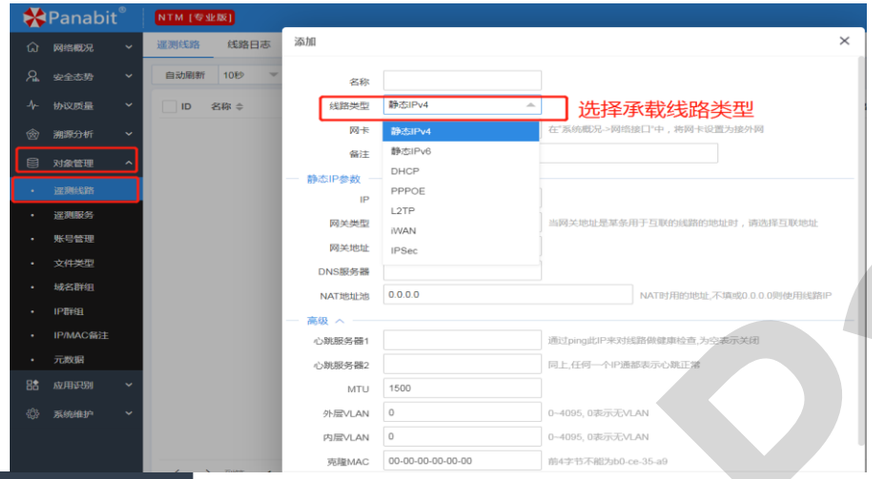
遥测隧道-服务端Panabit网关

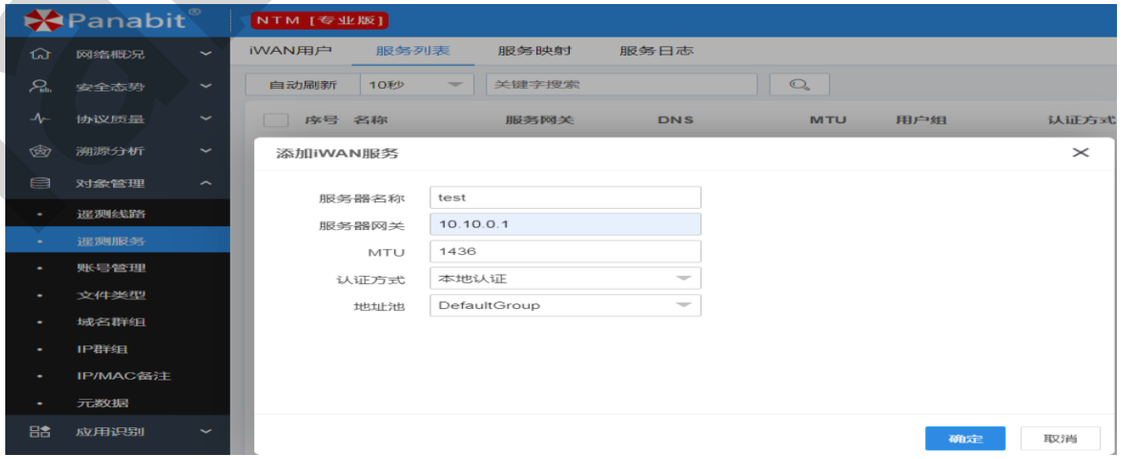
1	创建隧道服务	在【应用路由】-【iWAN服务】-【服务列表】-点击【添加】按钮。
2	添加映射端口	在【应用路由】-【iWAN服务】-【服务映射】中，设置该服务绑定的线路与端口信息。

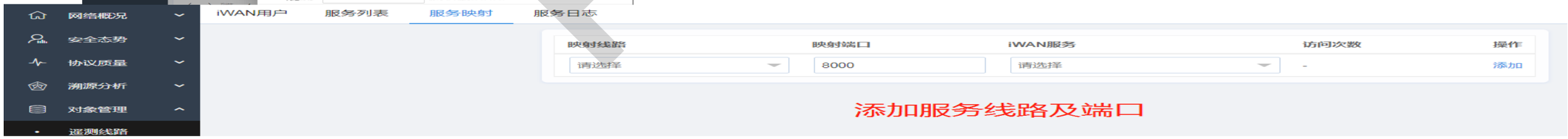


遥测隧道-服务端NTM网络全流量

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。

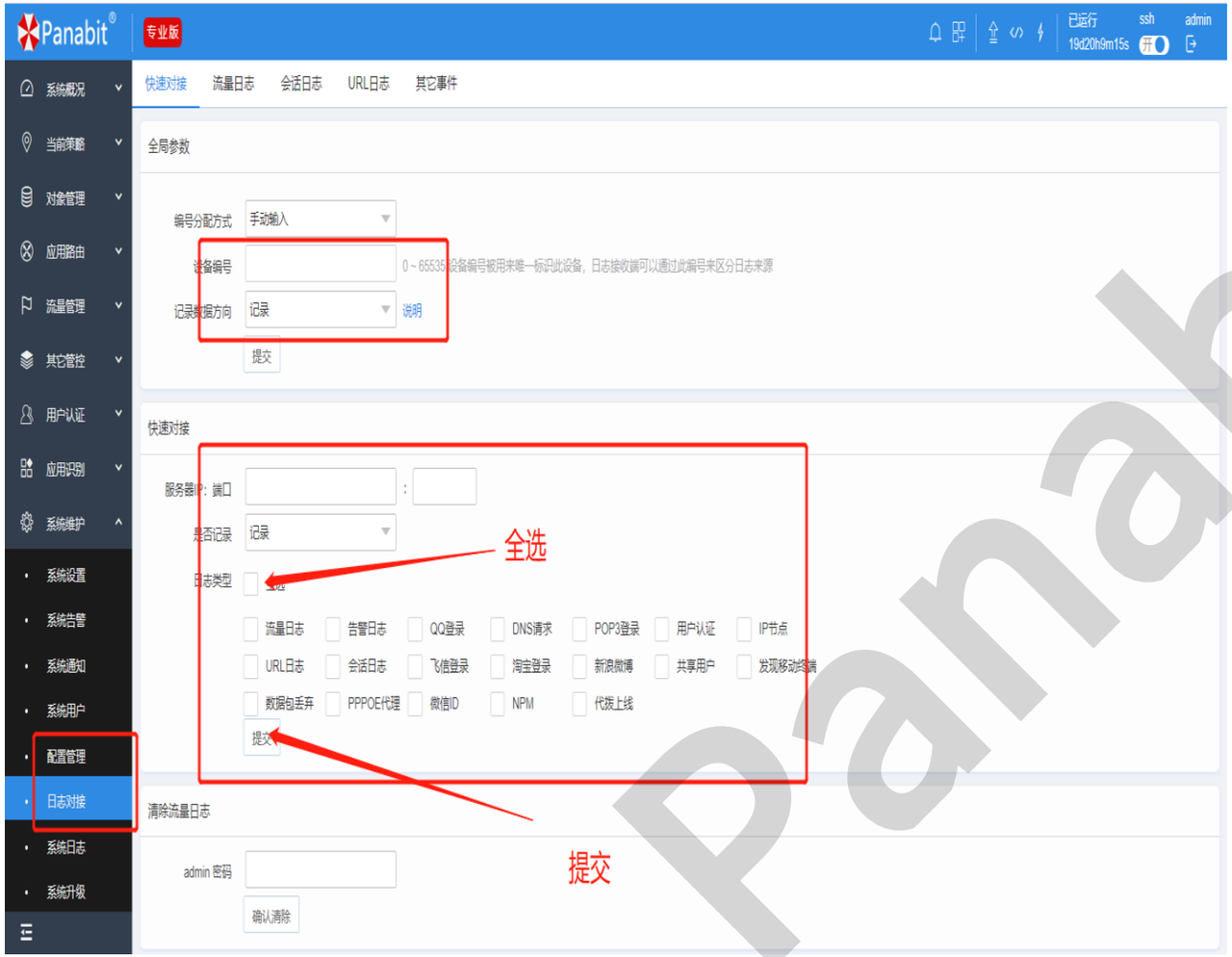






添加服务线路及端口

监控展示平台-Panabit-Panalog对接配置



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；

监控展示平台-Panabit-Panalog对接配置

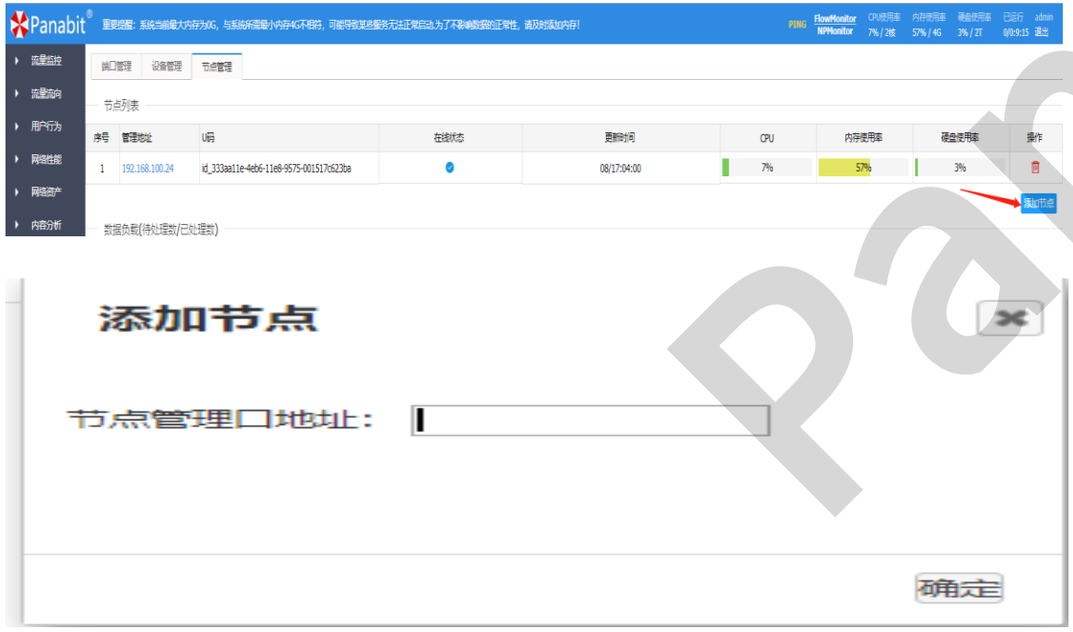
Panalog接收端口设置

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。

监控展示平台-Panabit-Panalog对接配置

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；



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

Panabit®

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。

Panalog-挖矿查询

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：

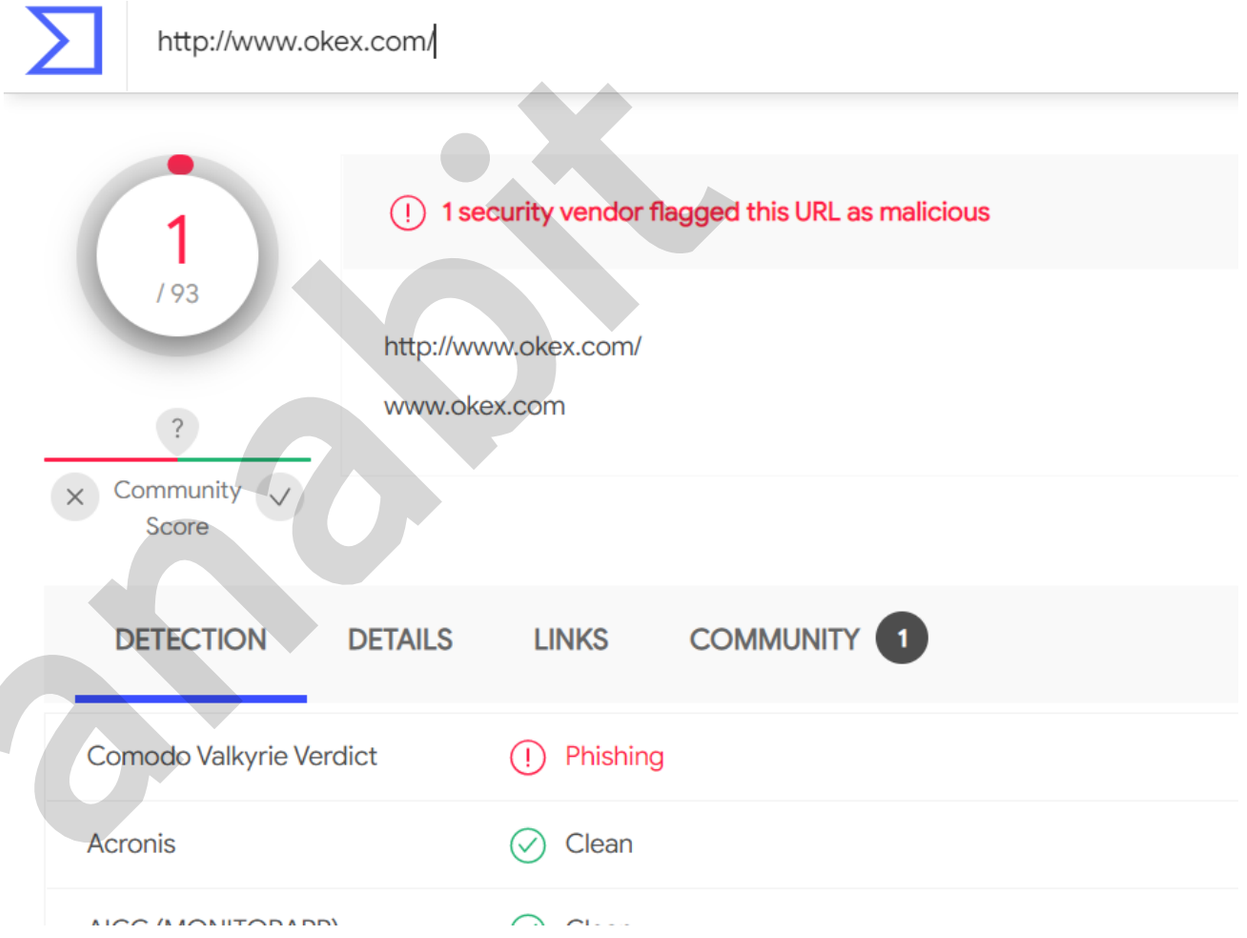
访问排名　用户排名　更新数据

选择设备 列表选项...　用户账号　用户IP　域名　URI　类别 bitcoin

起始时间 2021-12-08 11 时　结束时间 2021-12-09 11 时　查询

序号	URL	访问次数	类别	来源
1	k1pool.com/ 情报校验	1645	bitcoin	Panabit
2	www.okex.com/ 情报校验	741	bitcoin	Panabit
3	asia2.ethermine.org/ 情报校验	163	bitcoin	Panabit
4	cn.eth.k1pool.com/ 情报校验	52	bitcoin	Panabit
5	crypto.com/ 情报校验	28	bitcoin	Panabit
6	us1.ethpool.org/ 情报校验	26	bitcoin	Panabit
7	freebitco.in/ 情报校验	16	bitcoin	Panabit

Panalog-挖矿查询



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。

Panalog-挖矿查询

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”

NTM-Apache Log4j2漏洞查询

2022

畅享连世界

THANK YOU