



2022

畅享连世界

派网功能更新介绍

北京派网软件有限公司

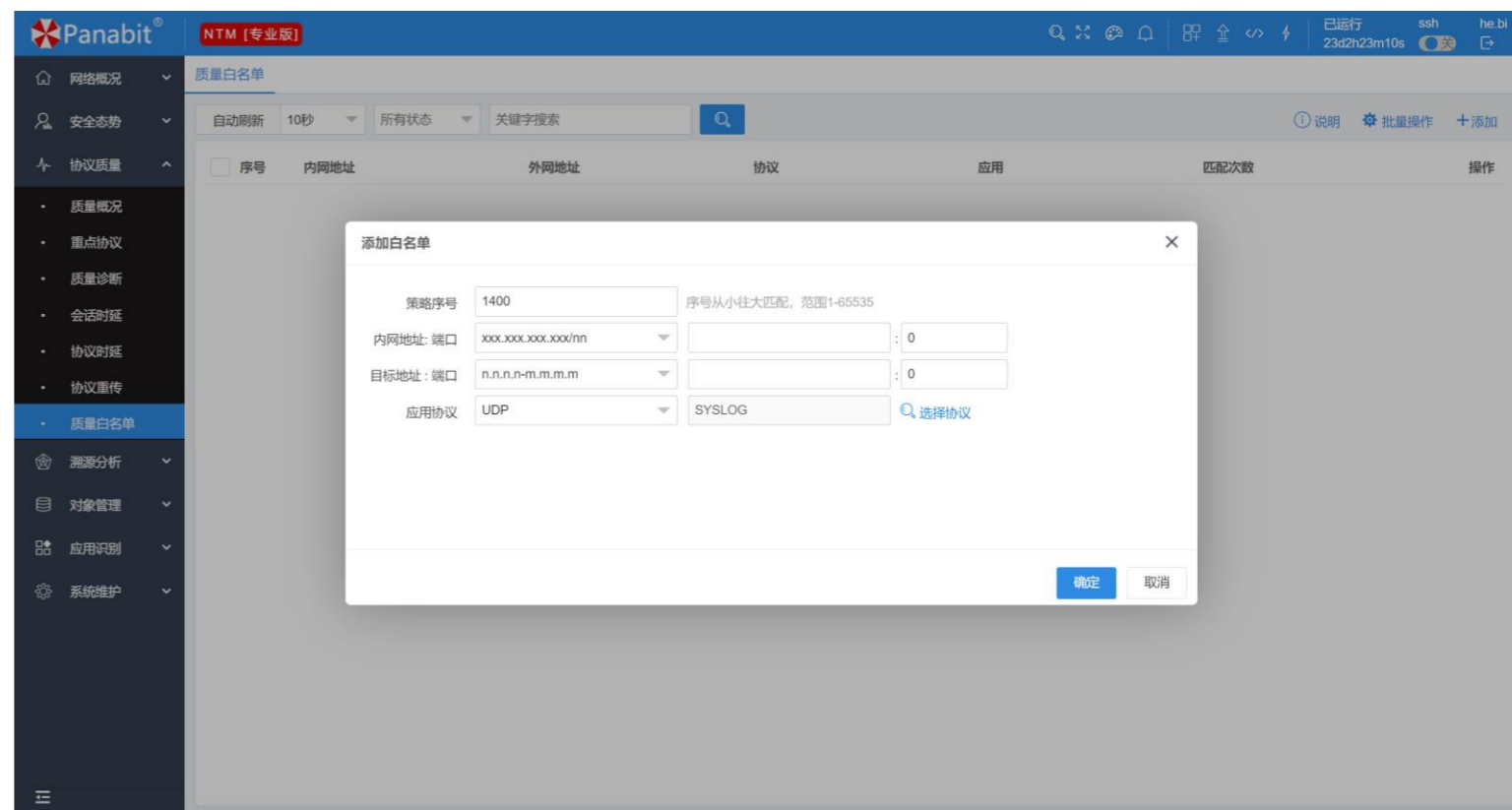
01

NTM更新

- 质量白名单
- 策略告警与通知
- 数据留存策略
- 离线数据包分析

质量白名单：

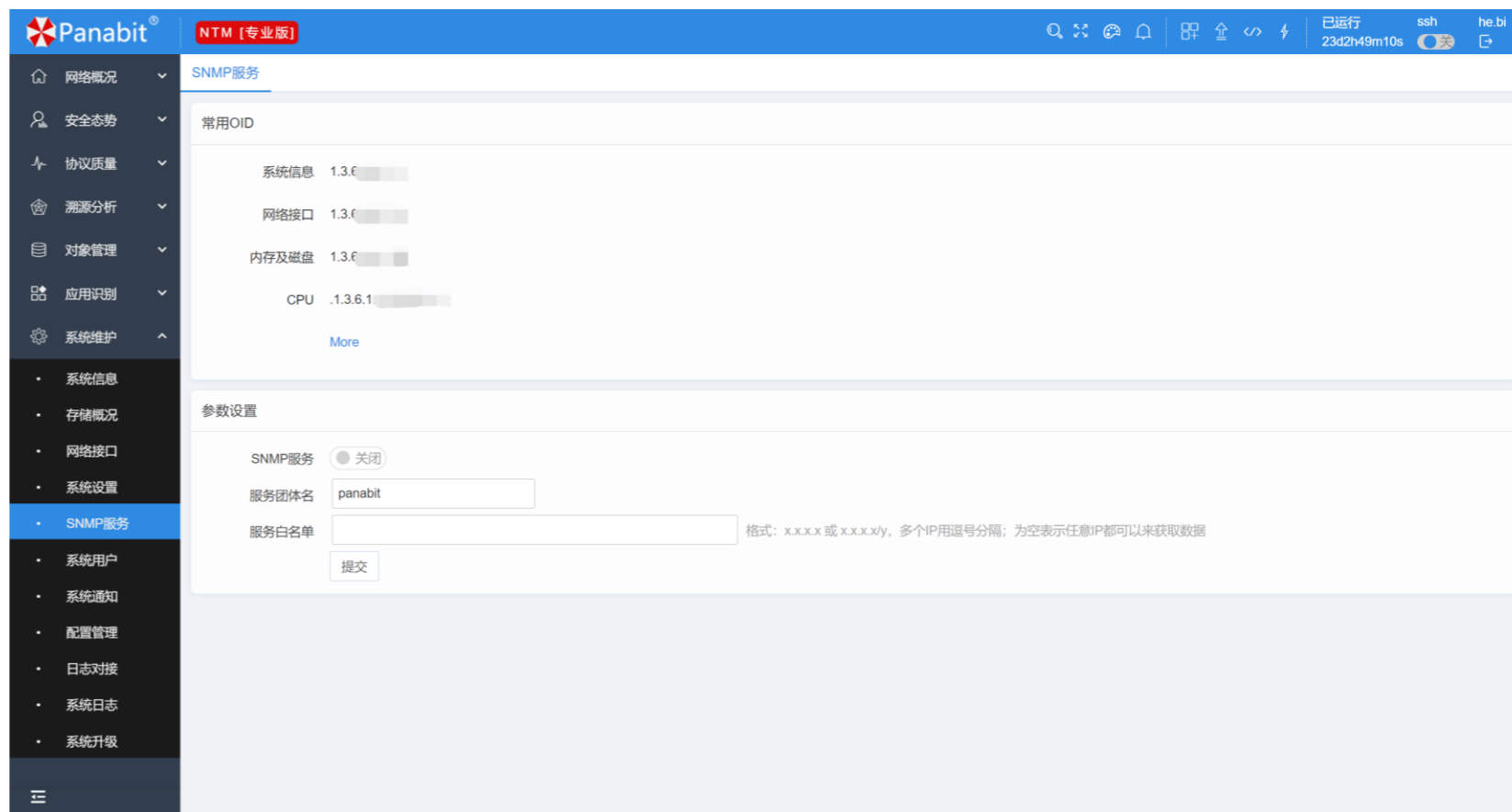
新增协议质量的白名单策略，
匹配策略后的会话将不计入协议
质量的统计中，增加协议质量统
计结果的准确性。

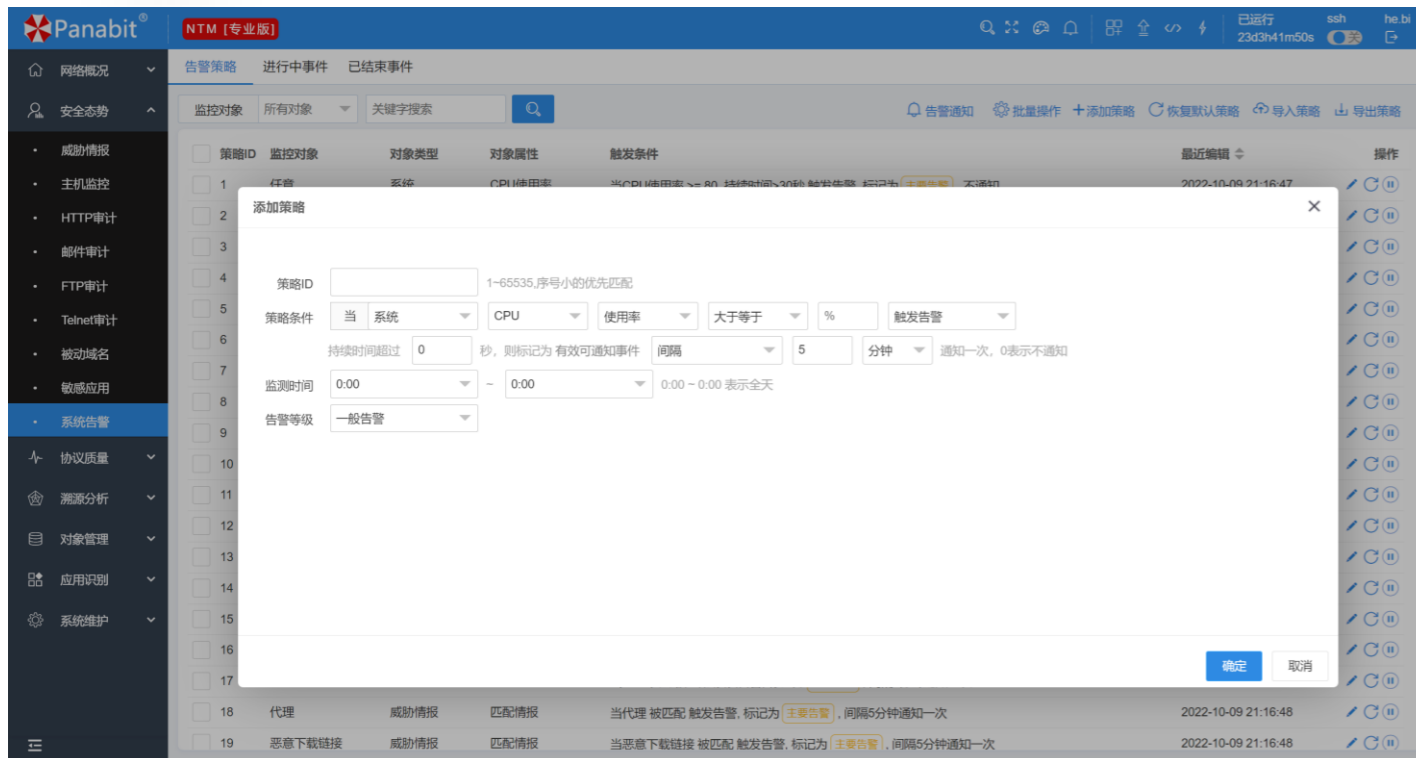


可将单向的UDP协议（例如：syslog），加入质量白名单中，避免NTM将其计入到失败测试中

SNMP服务：

集成SNMP服务，其他网管软件可以通过SNMP协议获取到NTM设备的CPU使用率、内存和硬盘使用率、网卡流入流出速率等信息。





策略告警：

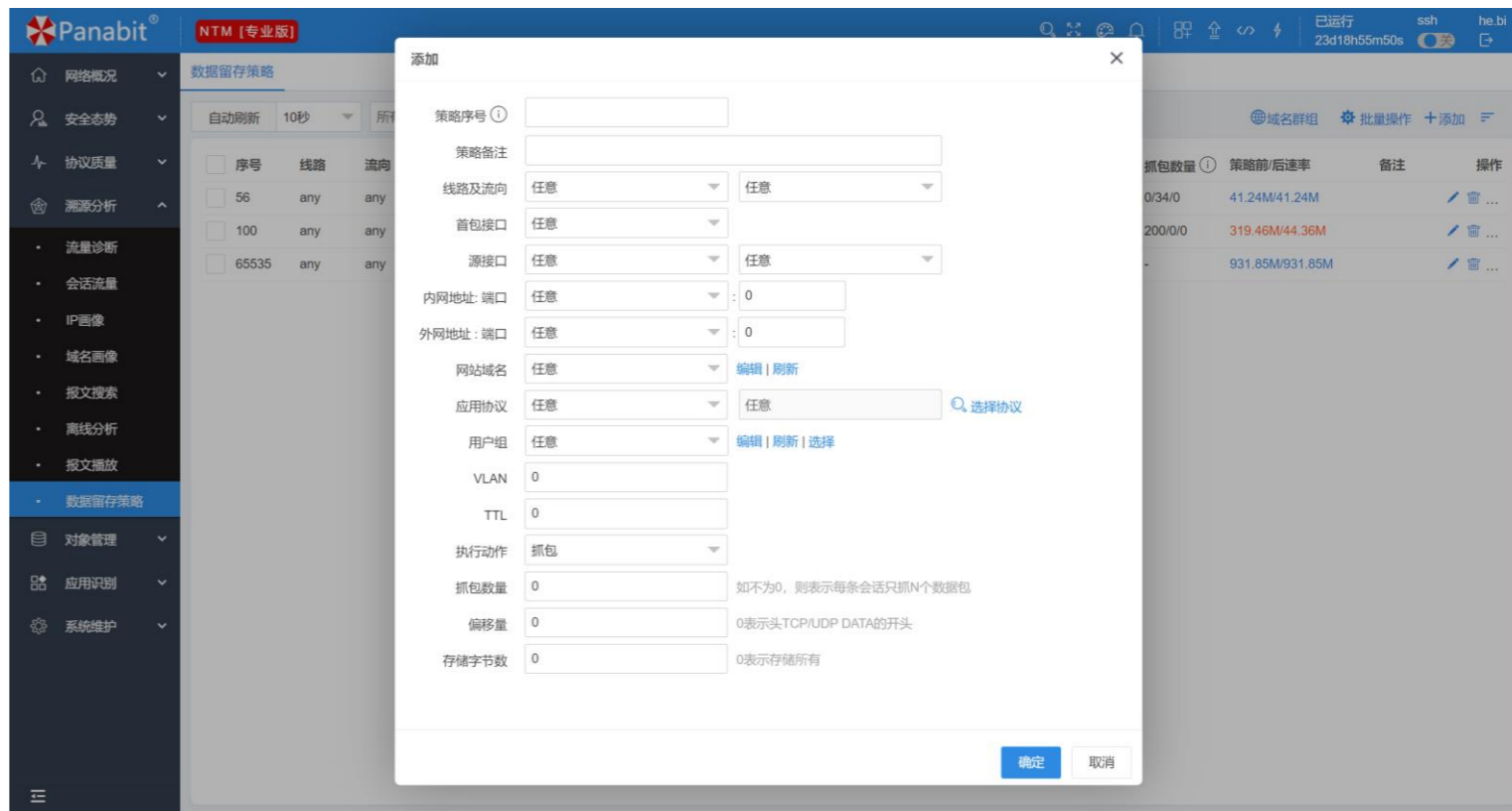
NTM告警建立在策略基础上，用户可以自定义策略，指定需要告警监控的对象。监控的对象可以是NTM系统本身，也可以针对内网IP、应用协议以及威胁情报进行监控。

告警通知：

产生的告警，可以通过微信、企业微信、钉钉、飞书和邮箱等几种方式通知到用户。

数据留存策略：

通过设置数据留存策略，
选取需要的数据进行留存，避免高存储量带来的硬盘空间压力，并增加数据的有效存储时间。



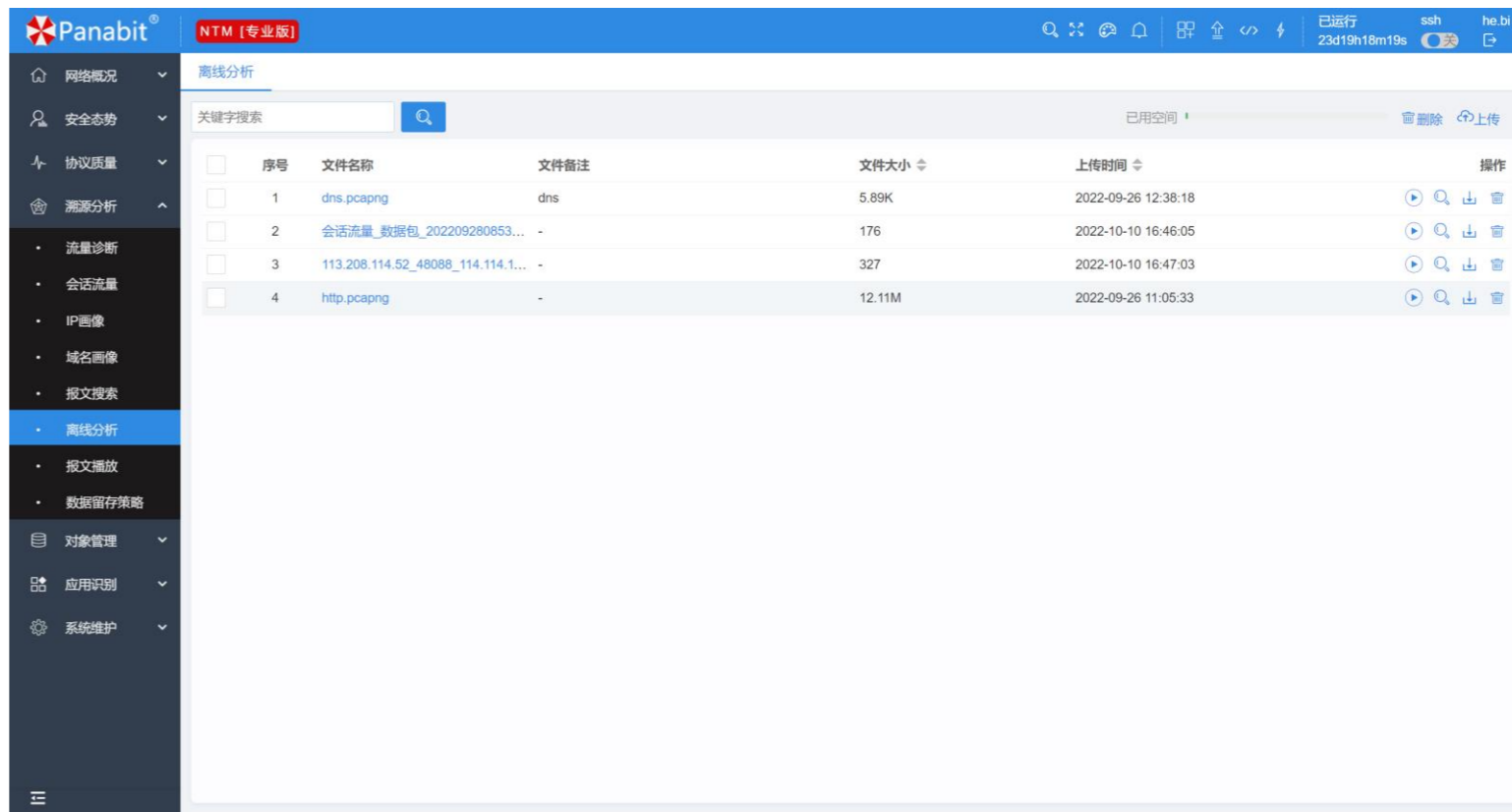
The screenshot displays the Panabit NTM (Professional Edition) web interface. A modal dialog titled '添加' (Add) is open, allowing the configuration of a new data retention strategy. The dialog contains the following fields and options:

- 策略序号 (Strategy ID): A text input field.
- 策略备注 (Strategy Remark): A text input field.
- 线路及流向 (Line and Direction): Two dropdown menus, both set to '任意' (Any).
- 首包接口 (First Packet Interface): A dropdown menu set to '任意' (Any).
- 源接口 (Source Interface): A dropdown menu set to '任意' (Any).
- 内网地址: 端口 (Internal Network Address: Port): Two dropdown menus, both set to '任意' (Any), followed by two input fields for IP and port, both containing '0'.
- 外网地址: 端口 (External Network Address: Port): Two dropdown menus, both set to '任意' (Any), followed by two input fields for IP and port, both containing '0'.
- 网站域名 (Website Domain): A dropdown menu set to '任意' (Any), with links for '编辑' (Edit) and '刷新' (Refresh).
- 应用协议 (Application Protocol): A dropdown menu set to '任意' (Any), with a '选择协议' (Select Protocol) button.
- 用户组 (User Group): A dropdown menu set to '任意' (Any), with links for '编辑' (Edit), '刷新' (Refresh), and '选择' (Select).
- VLAN: An input field containing '0'.
- TTL: An input field containing '0'.
- 执行动作 (Execute Action): A dropdown menu set to '抓包' (Capture).
- 抓包数量 (Capture Quantity): An input field containing '0', with a note: '如不为0, 则表示每条会话只抓N个数据包' (If not 0, it means only N packets are captured per session).
- 偏移量 (Offset): An input field containing '0', with a note: '0表示头TCP/UDP DATA的开头' (0 indicates the start of the TCP/UDP DATA header).
- 存储字节数 (Storage Bytes): An input field containing '0', with a note: '0表示存储所有' (0 indicates storing all).

At the bottom right of the dialog are '确定' (Confirm) and '取消' (Cancel) buttons.

离线分析：

离线数据包分析，支持将外部抓取的PACP文件进行上传分析，以展示会话信息、流量信息、HTTP信息、数据包信息等内容。



序号	文件名称	文件备注	文件大小	上传时间	操作
1	dns.pcapng	dns	5.89K	2022-09-26 12:38:18	播放 搜索 下载 管理
2	会话流量_数据包_202209280853...	-	176	2022-10-10 16:46:05	播放 搜索 下载 管理
3	113.208.114.52_48088_114.114.1...	-	327	2022-10-10 16:47:03	播放 搜索 下载 管理
4	http.pcapng	-	12.11M	2022-09-26 11:05:33	播放 搜索 下载 管理

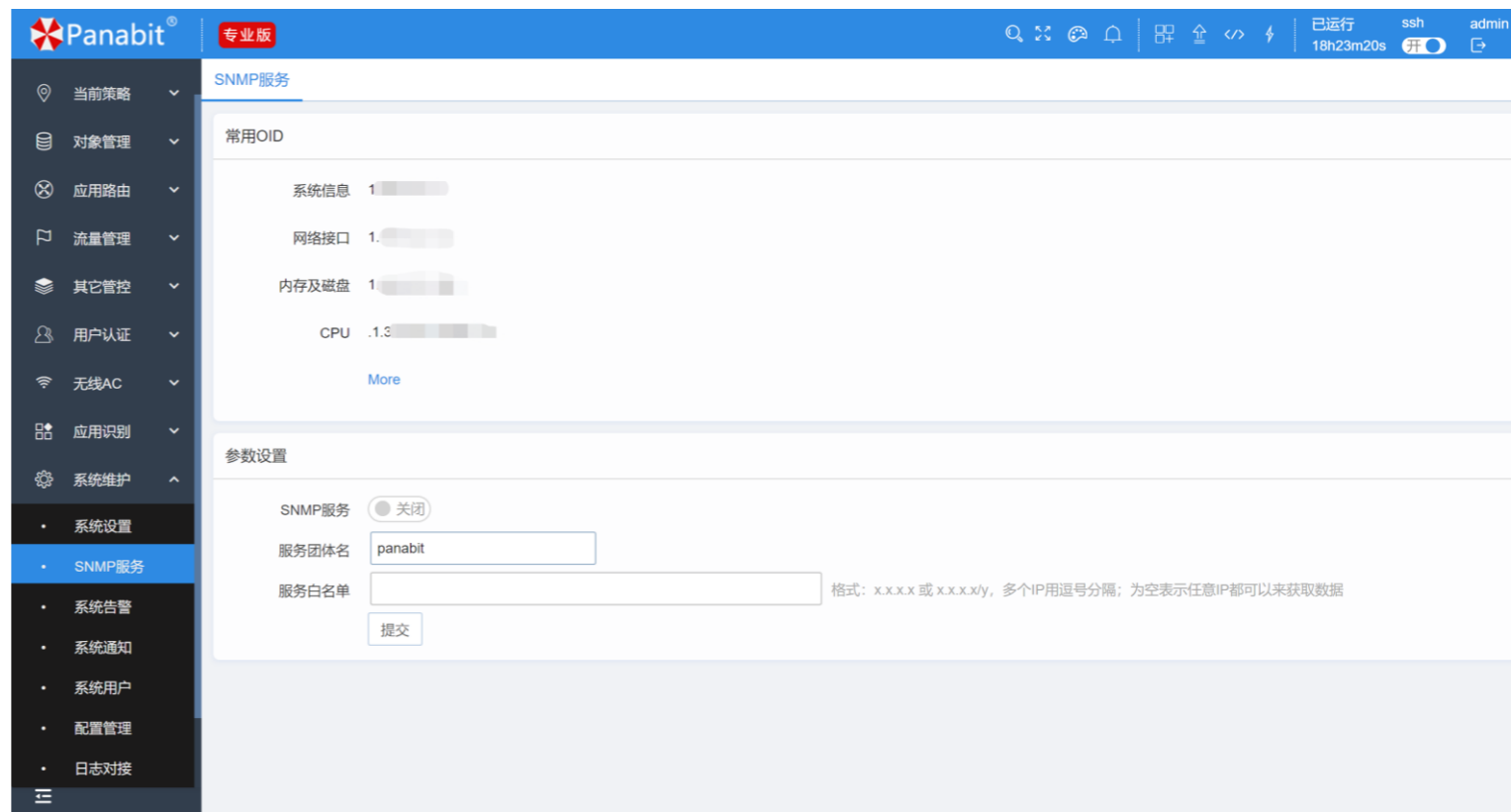
02

Panabit更新

- 5G融合二次鉴权
- iWAN管道模式
- Win&Linux客户端
- 动态 CGNAT

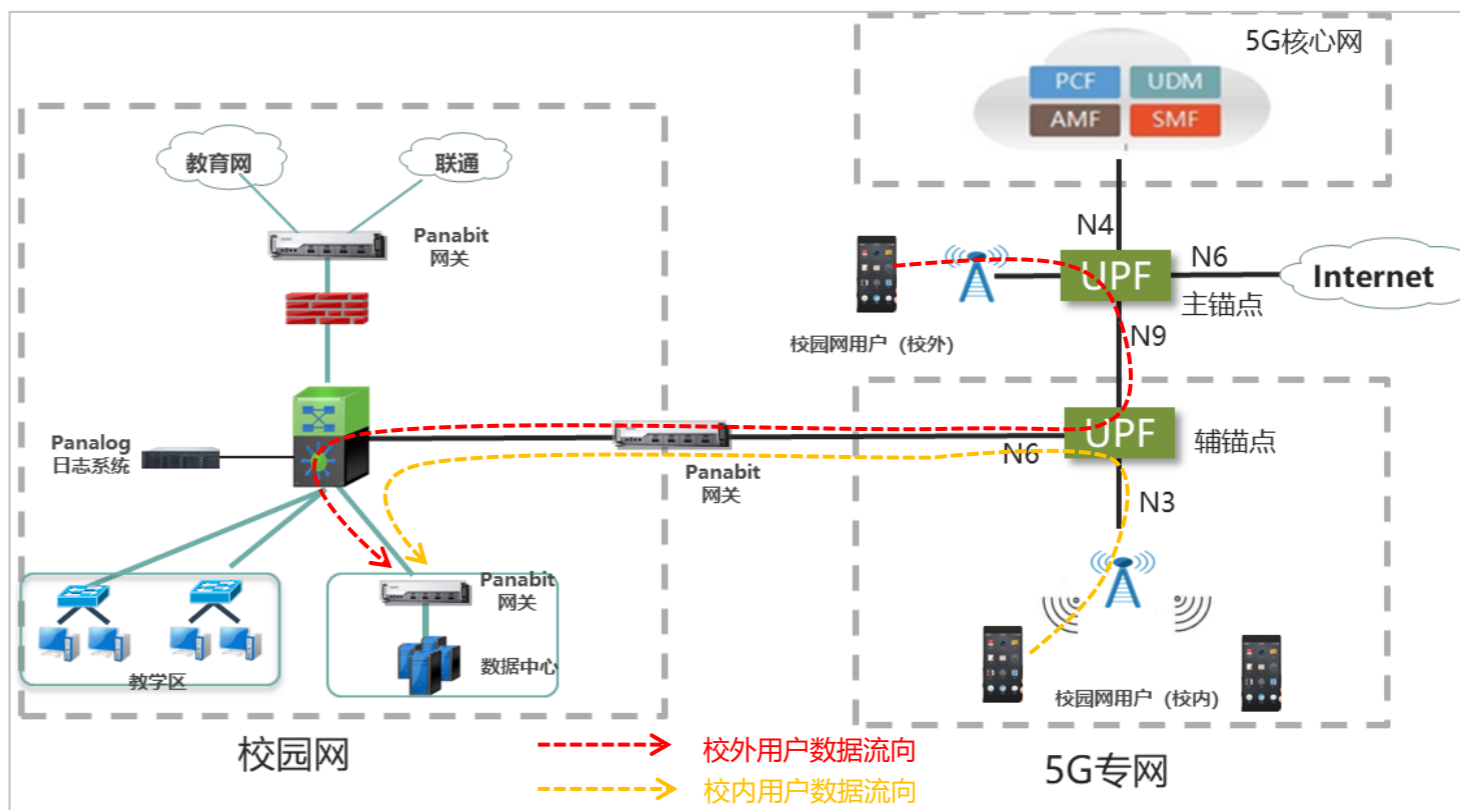
SNMP服务：

集成SNMP服务，其他网管软件可以通过SNMP协议获取到Panabit设备的CPU使用率、内存和硬盘使用率、网卡流入流出速率等信息。



5G融合二次鉴权：

对来访用户的手机号做一次认证，进一步确认来访用户的身份信息是否合法。（称这个过程为“二次鉴权”）



功能开启执行命令：

华为5G识别功能开启：floweye huawei5g config enable=1 auth=1

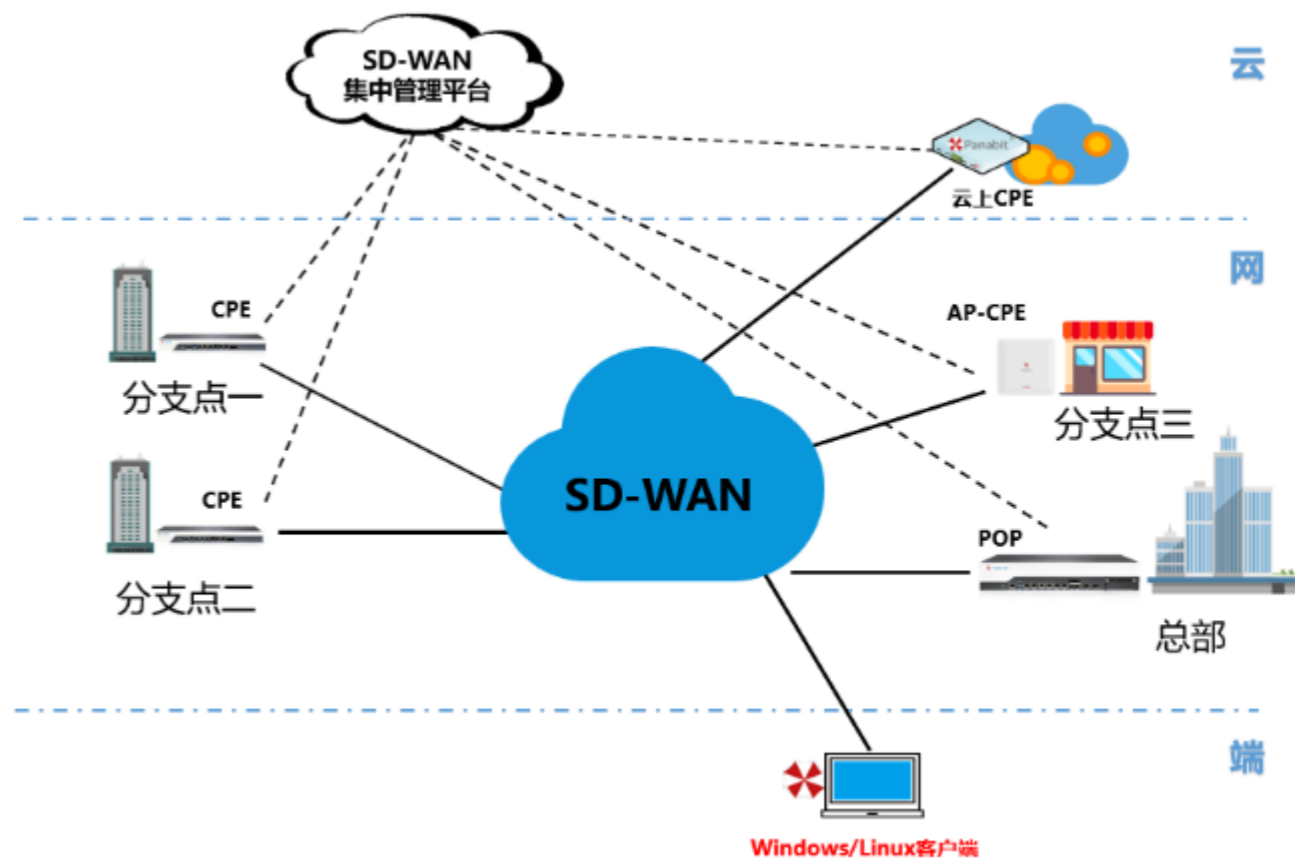
二次鉴权功能开启：floweye huawei5g config enable=1 auth=1 radsvid=N（“N” radius服务的ID）

查看状态：floweye huawei5g stat

注：Radius服务的ID可在【对象管理】--【RADIUS】--【服务列表】里查看。

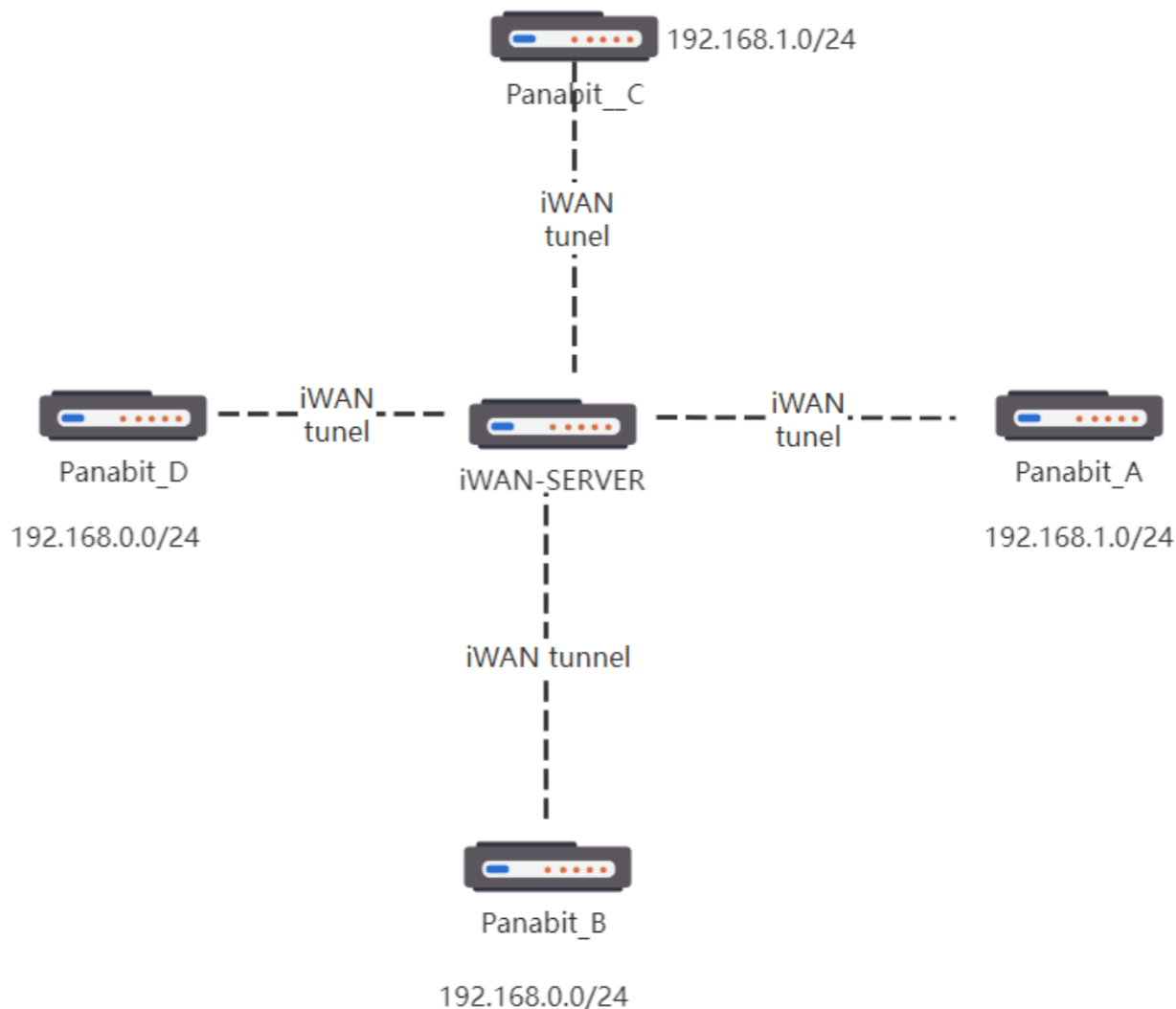
SD-WAN客户端:

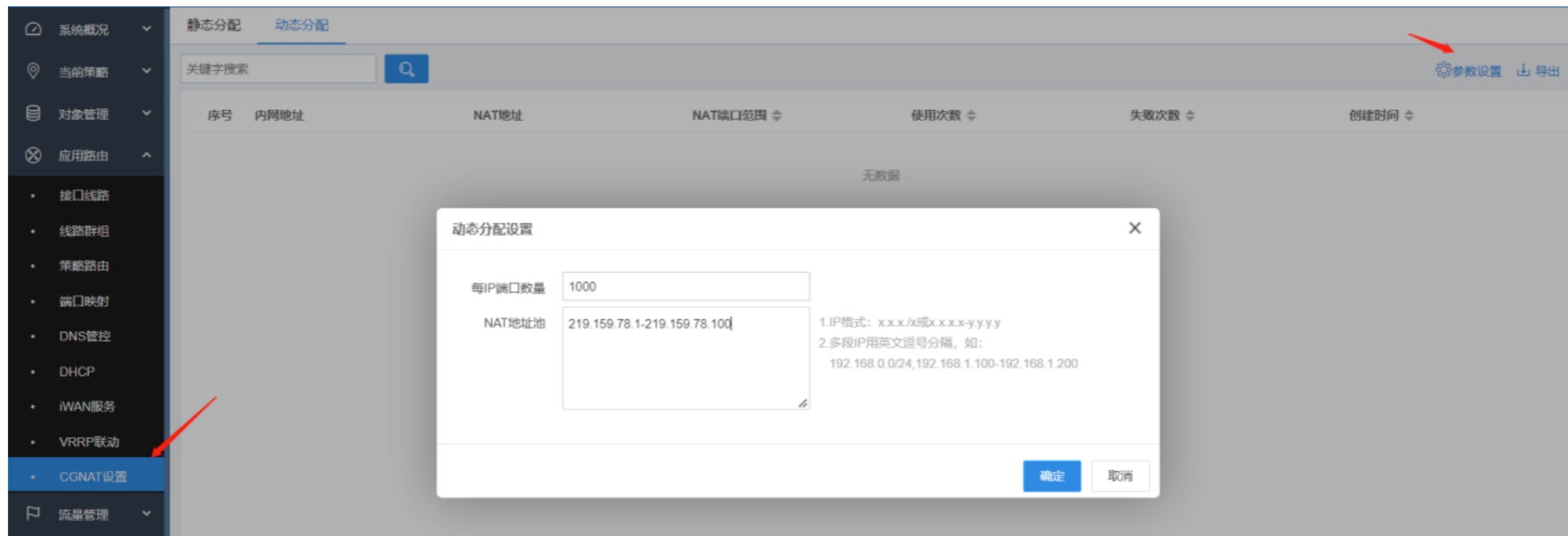
终端到网关的VPN，用于将单个主机与远程网络间进行连接。例如，移动工作者和远程工作者远程接入公司网络。



iWAN管道模式：

新版本中，iWAN引入了管道模式，可以通过配置**管道ID**和**管道方向**进行选路，以解决多分支之间互通时可能存在的地址冲突问题。





CGNAT:

全称Carrier-Grade NAT (运营商级网络地址转换)。在将私网地址（源地址）转换为公网地址后，还会将源端口进行转换，转换后的端口是一段固定且连续的端口范围，主要用于NAT444环境，方便溯源。

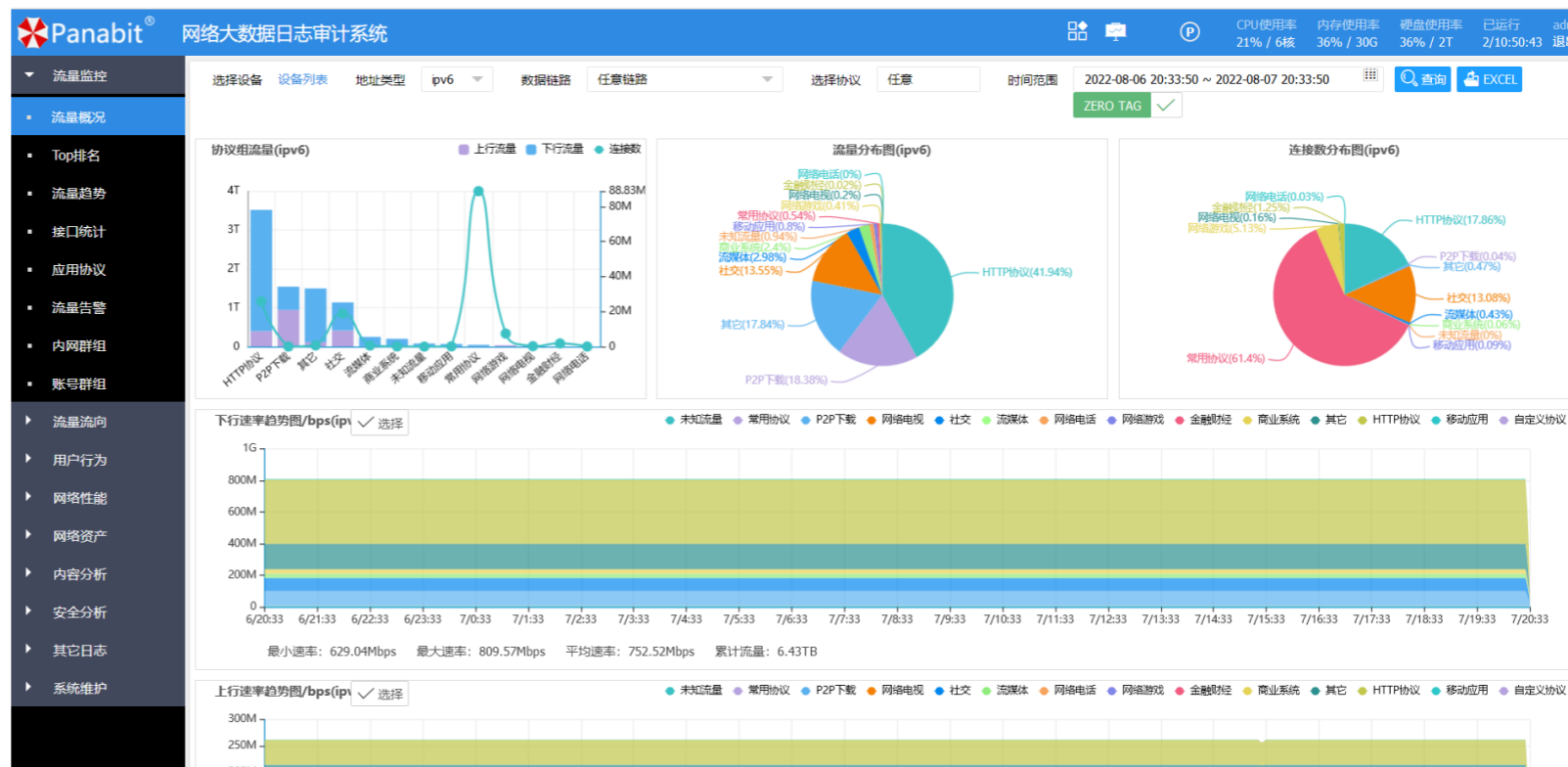
03

Panalog更新

- 全面支持IPv6
- 管理员权属选择
- 会话日志MAC查询
- 用户认证增加类型

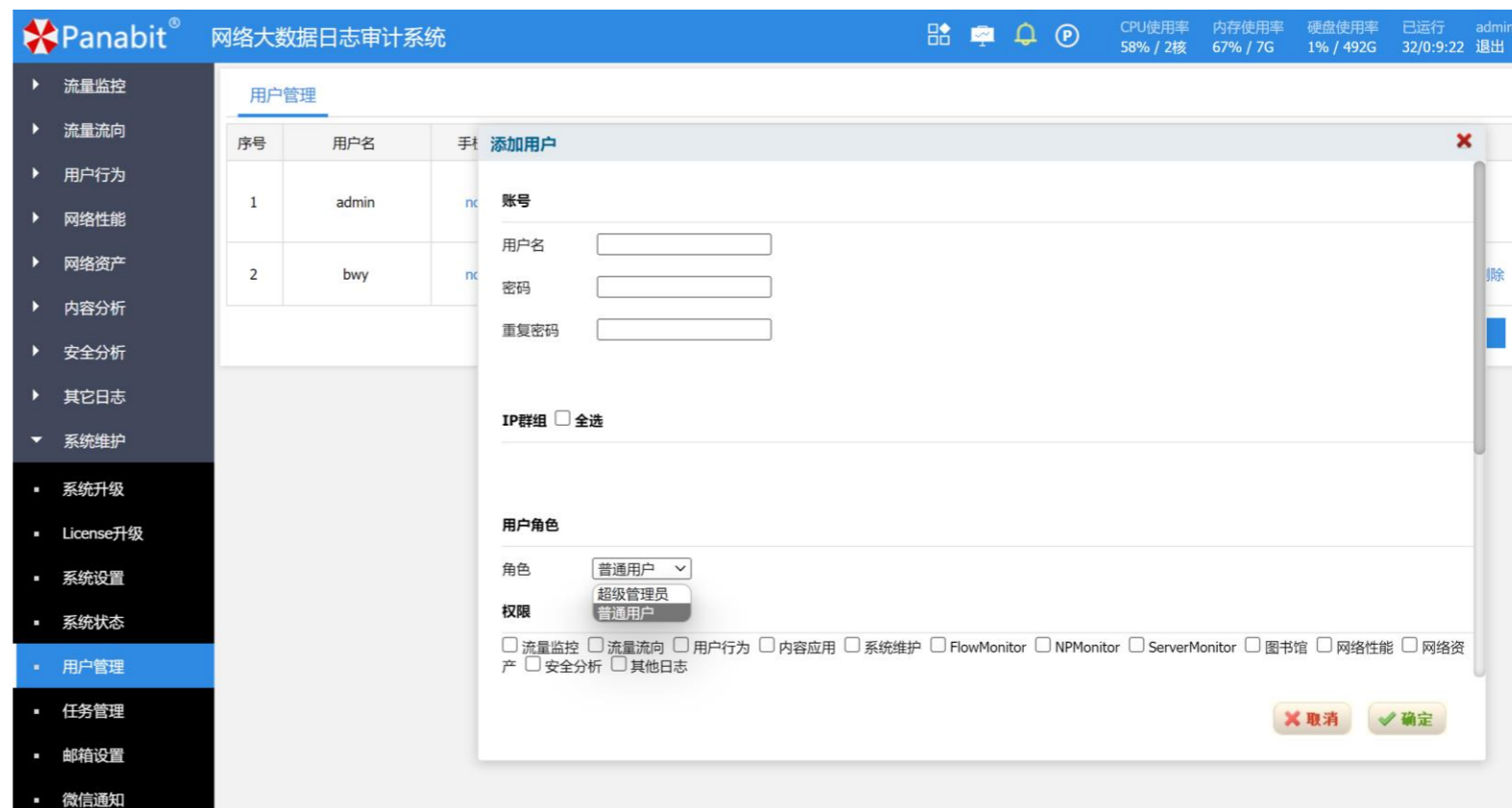
全面支持IPv6:

新版本全面支持IPv6，包括流量监控、流量流向、TOP排名、会话日志、威胁情报匹配等。



管理员权属优化：

添加管理员用户，增加用户角色选择功能，使用户权属清晰，更便于分权管理。



网络大数据日志审计系统

CPU使用率 58% / 2核 内存使用率 67% / 7G 硬盘使用率 1% / 492G 已运行 32/0:9:22 admin 退出

用户管理

序号	用户名	手机
1	admin	nc
2	bwy	nc

添加用户

账号

用户名

密码

重复密码

IP群组 ☐ 全选

用户角色

角色

权限

☐ 流量监控 ☐ 流量流向 ☐ 用户行为 ☐ 内容应用 ☐ 系统维护 ☐ FlowMonitor ☐ NPMonitor ☐ ServerMonitor ☐ 图书馆 ☐ 网络性能 ☐ 网络资产 ☐ 安全分析 ☐ 其他日志

根据MAC地址查询会话日志



会话日志模块，增加
“用户MAC” 为条件的查
询功能。





Panabit®
网络大数据日志审计系统

CPU使用率
29% / 6核

内存使用率
31% / 30G

硬盘使用率
66% / 2T

已运行
32/6:48:

流量监控

流量流向

用户行为

URL查询

域名地图

用户轨迹

用户画像

域名群组

Top域名

域名源数

用户过滤

虚拟身份

微信日志

DNS统计

关键字

用户认证

会话日志

在线账号历史记录IP备注账号信息








选择设备列表选项... 用户账号显示50项 IP地址MAC起始时间2022-09-26结束时间2022-09-27查询EXCEL TXT CSV下载列表

序号	设备	用户账号	访问时间	用户地址	MAC	认证类型
1	65530	yxj	2022-09-27 18:59:35	30.30.0.26	e4-68-a3-86-e0-ac	上线
2	65530	yxj	2022-09-27 18:37:06	30.30.0.26	e4-68-a3-86-e0-ac	上线
3	65530	yxj	2022-09-27 18:33:54	30.30.0.26	e4-68-a3-86-e0-ac	上线
4	65530	yxj	2022-09-27 18:31:40	30.30.0.26	e4-68-a3-86-e0-ac	上线
5	65530	yxj	2022-09-27 18:31:29	30.30.0.25	e4-68-a3-86-e0-ac	上线
6	65530	yxj	2022-09-27 18:31:22	30.30.0.24	e4-68-a3-86-e0-ac	上线
7	65530	yxj	2022-09-27 18:24:38	30.30.0.24	e4-68-a3-86-e0-ac	上线
8	65530	yxj	2022-09-27 18:23:19	30.30.0.24	e4-68-a3-86-e0-ac	上线
9	65530	yxj	2022-09-27 18:22:45	30.30.0.24	e4-68-a3-86-e0-ac	上线
10	65530	yxj	2022-09-27 18:21:28	30.30.0.24	e4-68-a3-86-e0-ac	上线
11	65530	yxj	2022-09-27 18:19:48	30.30.0.24	e4-68-a3-86-e0-ac	上线
12	65530	杨涛	2022-09-27 18:16:09	192.168.10.48	68-ec-c5-ab-06-d5	上线
13	65530	yxj	2022-09-27 17:59:54	30.30.0.24	e4-68-a3-86-e0-ac	上线
14	65530	yxj	2022-09-27 17:49:34	30.30.0.24	e4-68-a3-86-e0-ac	上线

04

AP更新

- WiFi6 SD-WAN
- iWAN五元组分流
- iWAN多线路切换
- iWAN NAT/路由

规格	 PAP-WM320	 PAP-XM320	 PAP-X3380	 PAP-WM110	 PAP-WM210	 PAP-XM220	 PAP-O2267
AP类型	面板AP	吸顶AP	吸顶AP	面板AP	面板AP	吸顶AP	室外AP
整机最大速率	1800Mbps	1800Mbps	3000Mbps	300Mbps	1200Mbps	1200Mbps	1200Mbps
WiFi类型	Wi-Fi 6	Wi-Fi 6	Wi-Fi 6	Wi-Fi 5	Wi-Fi 5	Wi-Fi 5	Wi-Fi 5
最大支持无线接入	512	512	512	32	128	256	256
以太网接口	2	2	3	2	2	2	2

WiFi6 SD-WAN:

在最近发布的小派AP新版本（V4.5_R2P4）中，**WiFi6全系列支持SD-WAN功能。**

新版本中增加了iWAN五元组分流，使得同一接口下的流量，能够基于五元组的策略，分流至SD-WAN或本地线路。



iWAN多线路切换：

新版本支持iWAN多线路备份，在iWAN线路异常后及时切换备线，进一步提升SD-WAN的可靠性。

修改iWAN线路

线路名称

3

服务器IP/域名

172.16.1.1

端口

8003

用户名

123

密码

123

☒ 链路加密

☒ 开启nat

iwan备份

开

1 x

2 x

保存

iWAN线路NAT或者路由的选择:

新版本增加了【开启NAT】的选择按钮，在AP之上还有防火墙等设备时，可以不开启NAT，此时执行的是路由，不影响防火墙等设备对iWAN线路上的终端流量进行管控。

修改iWAN线路

线路名称

1

2

3

4

线路名称

3

服务器IP/域名

172.16.1.1

端口

8003

用户名

123

密码

123

☒ 链路加密

☐ 开启nat

iwan备份

开

1 x

2 x

保存

信号阈值漫游：

对于漫游粘滞的终端，AP能够主动和终端断开连接。

漫游配置

智能漫游

☐ 关闭

检测方式

信号强度低于阈值，则触发漫游

信号阈值

dBm，数值为负数

连续踢线数

次，超过则进入保持周期

漫游保持周期

分钟，该周期内不进行漫游

检测周期

秒

确定

取消



2022

畅享连世界

THANK YOU

