Panabit®

北京派网软件有限公司

Panabit 上网行为管理用户手册

畅享连世界,致力于可视可控的云网一体化交付

- 文档版本　1.1.0
- 发布日期　2024-03-01

电话:400-773-3996
网址:www.panabit.com
地址:北京市海淀区中关村软件园二期新兴产业联盟大厦一层

版权声明

版权修订

派网保留不预先通知客户而修改本文档所含内容的权利。

责任限定

派网对于您的使用或不能使用本产品而发生的任何损害不负任何赔偿责任，包括但不限于直接的、间接的、附加的个人损害或商业损失或任何其他损失。

文档获取

可通过访问 Panabit 技术论坛获取相关文档：https://bbs.panabit.com。

意见反馈

我们非常欢迎和珍惜您的意见和建议，请通过下列方式反馈您对产品及文档的意见和建议。

- 通过电子邮件反馈，请发送至 support@panabit.com。
- 通过 https://bbs.panabit.com 网站在线反馈。
- 通过客户服务电话 400-773-3996 热线电话反馈。

北京派网软件有限公司

地址：北京市海淀区西北旺东路 10 号院 10 号楼中关村新兴产业联盟大厦一层

邮编：100094

网址：https://www.panabit.com

前言

文档概述

本文档主要介绍 Panabit 上网行为管理产品（以下简称“Panabit”）的安装部署及使用维护等内容。

读者对象

本文档的读者对象主要包括：

- 网络规划人员
- 网络维护人员
- 网络管理人员
- 对本产品有兴趣的网络爱好者

符号约定

在本文中可能出现下列标志，它们所代表的含义如下：

标志	意义
 危险	此标志表示如不避免会造成死亡或严重伤害等高等级风险。
 警告	此标志表示如不避免可能造成死亡或严重伤害等中等级风险。
 注意	此标志表示如不避免可能造成轻微或中度伤害等低等级风险。
 须知	提醒操作中应该注意的事项，不当的操作可能会导致数据丢失或者设备损坏，但不涉及人身伤害。
 说明	对文档内容的描述进行必要的补充和说明。

在本文中会出现图形界面格式，它们所代表的含义如下。

格式	意义
【】	实心方头括号“【】”表示窗口名、菜单名、按钮和子模块名，如“点击【三日对比】”。
<注释 n>	粗体、带尖括号的注释+数字，**<注释 n>**表示对页面部分模块的说明与解释，如：**<注释 6>** 显示提醒信息，比如是否有新版本等。
>	尖括号“>”用于隔开多级菜单，【系统概况】>【网络概况】表示【系统概况】菜单下的【网络概况】菜单。

示例约定

由于各个系统的配置不同、版本升级等原因，可能造成本文档中的部分内容与用户实际使用的系统显示信息不一致。实际使用中请以设备显示的内容为准。

修订记录

文档版本	发布日期	修改说明	修订人员
1.0.0	2023.09.28	第一次正式发布	李青梅，张晓东，王鹏，派网售后服务中心
1.1.0	2024.03.01	第二次正式发布	李青梅，张晓东

目录

1. 产品概述

随着数字化不断发展，终端数量迅速增加，人们在享受信息交互便利的同时，上网行为管控缺失、涉密信息泄露、网络威胁等问题也日益突显。对上网行为的管理与审计，对终端及应用的识别与控制成为亟待解决的问题。

Panabit 上网行为管理支持上网行为管理、行为审计、负载均衡、统一上网认证、威胁情报、协议识别、流量控制、访问控制、应用分流、DNS 管控、SD-WAN 组网、业务级质量监测和故障定位等功能，支持全量日志 1:1 溯源分析和 180 天审计日志本地存储，以及对接公安网监：公共无线上网管理平台，满足客户对网络流量细粒度可视、可控、可审计的核心需求。

1.1. 产品定位

Panabit 上网行为管理产品是基于国产平台自主研发的高性能网络行为管控与上网行为审计产品，针对基于网络的上千种应用部署精细化的控制策略，解决客户带宽分配不合理、上网权限管理缺失、上网日志记录缺乏等问题。专门为运营商、政府、教育、企业提供高性能、高可用性、功能丰富的全网行为管理解决方案。

1.2. 关键特性

1.2.1. 开放的操作系统

Panabit 上网行为管理使用自主研发的数据面操作系统 PanaOS，由 PanaOS 承担驱动、内存管理、任务调度等数据面核心任务，通过虚拟化技术实现了数据层面和控制层面分离。PanaOS 赋予了 Panabit 上网行为管理软件的高稳定性，为客户提供一体化解决方案打下坚实基础。

1.2.2. 精准的应用识别

Panabit 上网行为管理主攻七层应用识别技术，在现网保持着超过 95%的流量识别率，可以识别和控制常见的 14 大类 1000 多种应用。

除了传统的 DPI、DFI 外，Panabit 上网行为管理还使用了节点跟踪、主动探测及协议多状态机等识别技术来保障识别率。借由互联网助力，Panabit 拥有业内庞大的测试队伍和最全面的测试环境，这是 Panabit 始终保持快速的未知应用样本获取速度、精确的协议识别率的生态基础。

1.2.3. 1:1 全量日志留存

Panabit 上网行为管理具备 1:1 全量日志留存能力，这意味着能够完整记录和存储每个员工的上网会话日志。全量日志留存的能力可以提供更全面的审计和溯源功能，帮助企业满足合规性要求，并在需要时进行调查和取证。全量日志留存还可以提供更准确的数据分析和报告生成，帮助企业做出更具针对性的决策和优化措施。

1.3. 应用场景

Panabit 上网行为管理通过对用户网络的识别、管控和分析，实现用户和终端、应用和流量的可视可控。主要应用如下：

1.3.1. 实名认证场景

Panabit 上网行为管理支持上网接入认证，包括不限于：本地认证、短信认证、微信认证，并支持结合 AD 域和 LDAP 等多种认证方式，将互联网行为与真实人员关联，便于定位互联网行为的主体。

Panabit 上网行为管理还能自定义配置认证页面，自定义认证的黑白名单对象，过滤非法匿名用户，放行合法用户。

1.3.2. 用户上网行为管控场景

Panabit 上网行为管理可应用于组织对其成员的行为管理中，基于用户和应用分时段对用户上网行为进行管控。工作时间优先保障客户视频会议、文件传输、即时通信等关键应用的访问速率，限制视频网站、游戏网站等工作之外应用的访问速率。

1.3.3. 出口网关场景

使用 Panabit 上网行为管理作为一体化网关进行组网，可节省成本，满足网络安全和行为管控的需求。

1.3.4. 大数据管理运营场景

部署 Panabit 上网行为管理后，可将用户上网行为进行清晰直观地展示和分析，包括业务质量分析、用户画像、域名画像等，有助于网络管理人员挖掘现网数据价值，制定更有针对性的网络管理、运营策略。

1.3.5. 网络安全合规审计场景

当出现重大网络安全事故后，需要及时进行源头追溯，避免下一次事故的发生。Panabit 上网行为管理记录下来的 1:1 会话日志，可以用于网络安全法的审计，也可以用于故障的定位和追溯。

2. 设备安装

本章节主要介绍 Panabit 上网行为管理硬件安装的流程、安装准备工作和设备参数介绍以及设备的部署方式及注意事项。

2.1. 安装流程

介绍 Panabit 上网行为管理硬件设备的安装流程，便于提前熟悉整个安装过程。

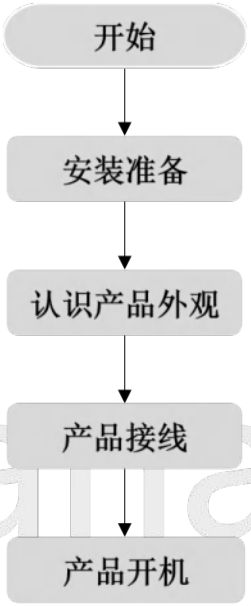


图 2-1 Panabit 上网行为管理安装流程图

2.2. 安装准备

2.2.1. 环境要求

产品安装之前仔细检查安装环境，可以保证设备安装的顺利进行以及安装后设备的良好运行。

编号	项目	检查要求
1	选址	设备安装位置不宜在温度过高或过低、有灰尘、有有害气体、易燃、易爆及电压不稳定的环境中，应避开经常有大震动或强噪声的地方。
2	电压	110V～230V

3	温度	0～45℃
4	湿度	5%～85% 无冷凝
5	电源	交流 110V～230V 电源，接通电源之前，请保证您的电源有良好的接地措施。

表 2-1 安装环境快速检查表

2.2.2. 产品外观

Panabit 上网行为管理产品外观如**图 2-2** 所示，产品面板包含的接口基本一致，具体以实际收货设备为准。

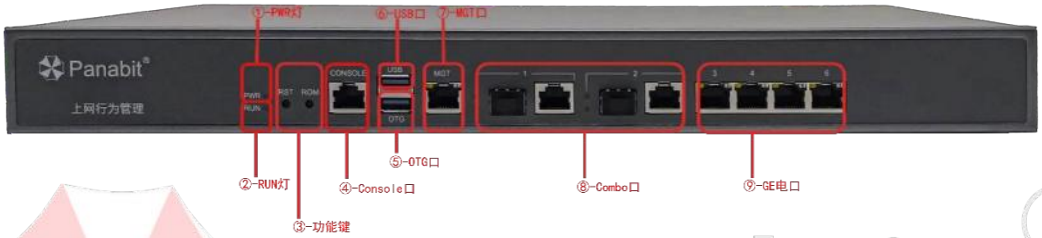


图 2-2 Panabit 上网行为管理接口示意图

编号	接口/按键	说明
①	PWR 指示灯	电源状态指示灯，当设备处于开机时，该状态灯呈绿色。 常灭：电源模块不在位或出现故障。 绿色/蓝色常亮：电源模块供电正常。
②	RUN 指示灯	设备运行状态指示灯。 常灭：设备未上电或者故障 绿色/蓝色闪烁：设备正常工作。
③	功能键	RST：复位键，长按将设备恢复出厂设置。 ROM：用于刷新设备固件。 **⚠注意** 恢复出厂设置，会造成设备配置和 license 丢失，请务必在复位前对配置文件和 license 文件进行备份。
④	Console 口	通过 Console 口登录设备命令行界面进行管理设备。供连接超级终端等终端软件使用，可以通过该口对设备进行管理。
⑤	OTG 口	主要用于更新设备固件。
⑥	USB 口	USB 接口用于连接键盘、U 盘等。

⑦	MTG 口	千兆电口，设备的管理端口，不承载业务数据，用于对设备进行 Web 管理等。
⑧	Combo 口	千兆光电复用端口，用于传输业务流量，可自定义配置为 WAN 口、LAN 口、网桥接口等。以太网光接口指示灯： 常灭：光纤链路没有建立连接 绿色常亮：光纤链路已经建立 1000Mbps 的连接 绿色闪烁：光纤链路正在以 1000Mbps 的速率收发数据
⑨	GE 电口	千兆电口，用于传输业务流量，可自定义配置为 WAN 口、LAN 口、网桥接口等。以太网电接口指示灯： 常灭：对应接口处于未连接状态 绿色常亮：端口已经建立千兆连接 绿色闪烁：端口千兆收发数据 黄色常亮：端口已经建立十兆/百兆连接 黄色闪烁：端口十兆/百兆收发数据

表 2-2 Panabit 上网行为管理接口说明表

2.3. 接线方式

不同的业务需求接线方式存在差别，请按照规划的网络拓扑进行设备接线，在开始接线前，请进行如下自检：

1. 查看机箱外观，是否因为运输有损坏。
2. 查看机箱外部螺丝是否齐全，是否松动。
3. 摇晃机箱，判断机箱内部是否有异物。

2.4. 设备开机

连接电源线后，打开背面开关。此时前面板的 PWR 灯（绿色，电源指示灯）和 RUN 灯（绿色，设备运行状态指示灯）点亮，说明设备正常工作。检查每个网卡都插上模块和光纤或者网线，查看各接口的状态灯是否都正常。

3. 设备部署

本章介绍了 Panabit 上网行为管理的基础配置，包括设备的登录、升级与几种部署方式的基础配置方法。

3.1. 设备登录

3.1.1. 登录 WEB 控制台

作为一款 B/S 架构的产品，Panabit 上网行为管理可通过管理口（MGT）进行 Web 登录，并通过 Web 管理页面进行全部管理动作。系统的 Web 管理界面支持 Microsoft Edge、FireFox、Chrome 等市面主流的浏览器，建议使用 Chrome，推荐最小屏幕分辨率为 1280x1024。

图 3-1 设备首次登录拓扑

说明

首次登录设备时，可以使用电脑通过网线直连 Panabit 上网行为管理的 MGT 口，MGT 口的默认地址为 192.168.0.200，子网掩码为 255.255.255.0。

操作步骤

步骤 1 将电脑的 IP 地址更改为与设备 MGT 口相同的网段。

1. 选择【控制面板】>【网络与 Internet】>【网络与共享中心】。
2. 单击【更改适配器设置】，进入【网络连接】界面。
3. 单击右键，选择【属性】。
4. 选择【Internet 协议版本 4（TCP/IPv4）】，单击【属性】。
5. 选择【使用下面的 IP 地址】，将子网掩码设置为 255.255.255.0。

6. 单击【确定】

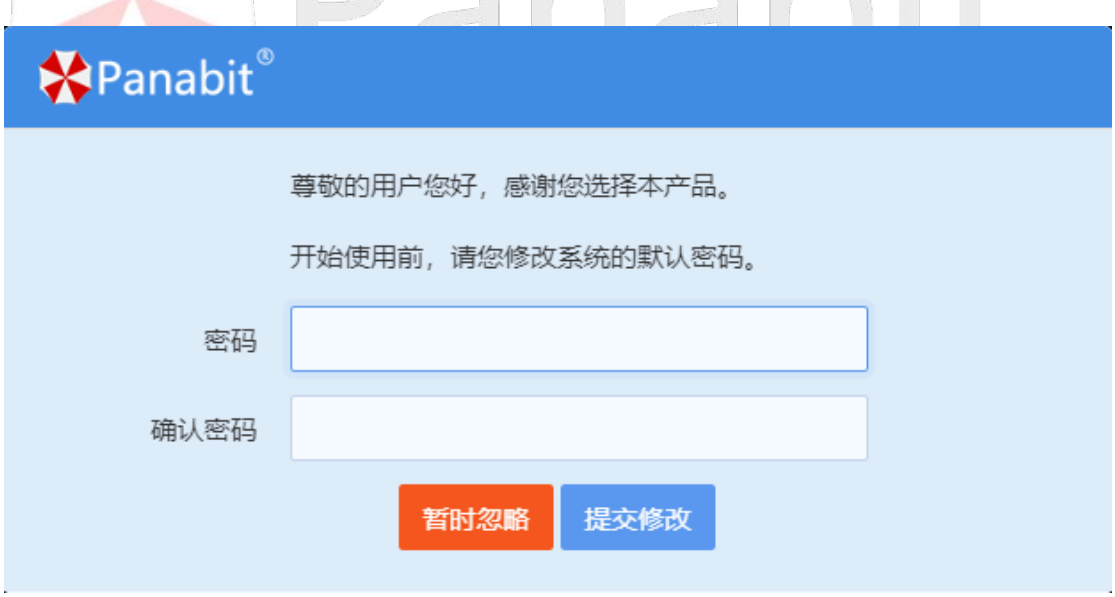
步骤 2 打开浏览器，输入设备默认地址 https://192.168.0.200，进入登录页面。

步骤 3 输入默认用户名 admin，密码 admin，登录 WEB 控制台。

——结束

3.1.2. 修改密码

请在首次登录时，进行密码的修改。首次登录设备后，系统将提示您修改系统的默认密码，输入并确认新密码即可。



如需手动进行密码的修改，请按照以下步骤执行。

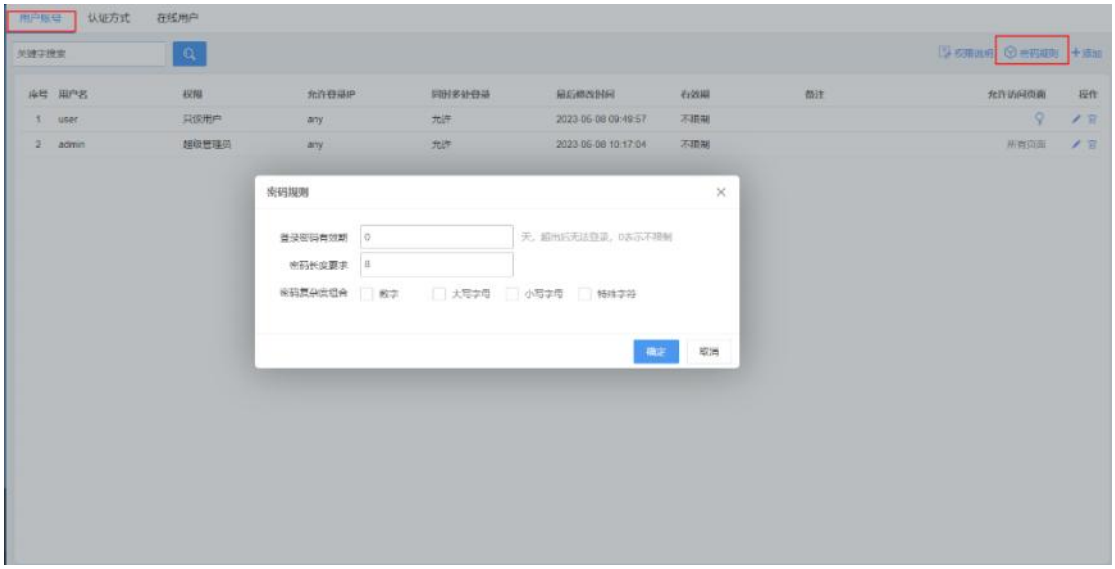
操作步骤

步骤 1 打开浏览器，输入设备默认地址 https://192.168.0.200，进入登录页面。

步骤 2 输入默认用户名 admin，密码 admin，登录 WEB 控制台。

步骤 3 选择首页功能列表中的【系统维护】>【系统用户】

步骤 4 选择页面上方的【用户账号】，单击【密码规则】，设置密码规则。



说明

- 有效期尽量不超过一个月。
- 长度尽量超过 8 位。
- 密码复杂度组合尽量全选。

配置示例：设置密码有效期为 7 天，密码长度不低于 8 位，密码必须包含数字、大小写字母及特殊字符。

步骤 5 单击【确定】。

步骤 6 选择首页功能列表中的【系统维护】>【系统用户】。

步骤 7 单击用户名后的 图标，进入修改密码界面，按设置好的密码规则填写新密码。

步骤 8 单击【确定】。

——结束

3.1.3. 修改管理口地址

管理口地址修改后，请使用 https://[新的管理口地址] 进行设备的登录。

操作步骤

步骤 1 打开浏览器，输入设备默认地址 https://192.168.0.200，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

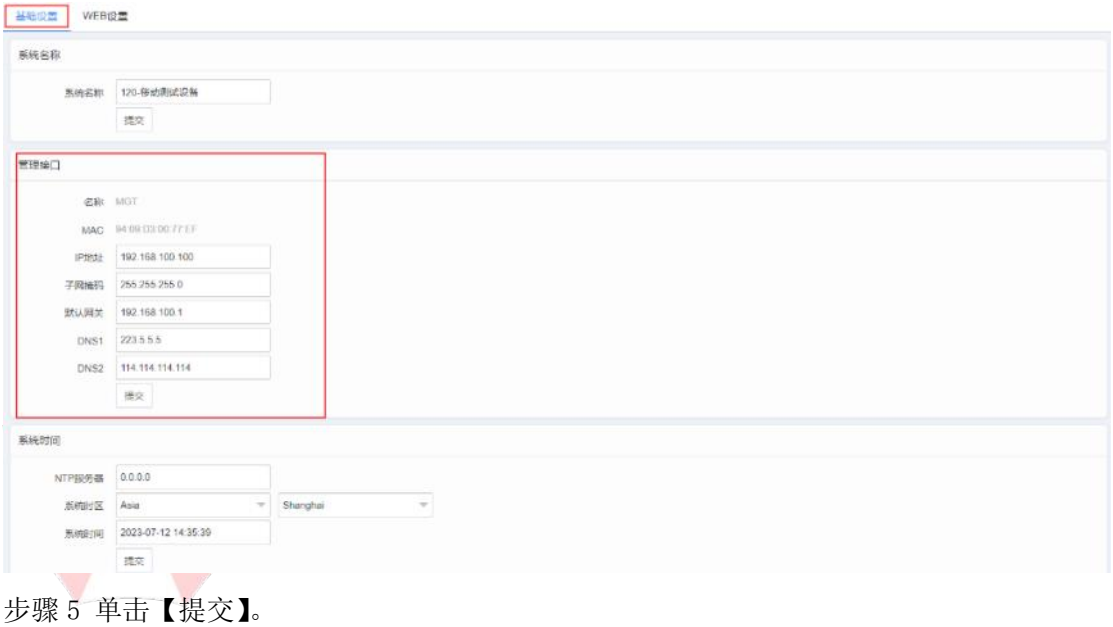
步骤 3 选择首页功能列表中的【系统维护】>【系统设置】，

步骤 4 选择页面上方的【基础设置】，进入管理口修改页面。

说明

如无特殊情况，请确保管理口配置的地址能够访问互联网。

配置示例：将管理口地址修改为 192.168.100.100/24，网关为 192.168.100.1，DNS1 为 223.5.5.5，DNS2 为 114.114.114.114。



步骤 5 单击【提交】。

——结束

3.1.4. License 导入

导入已购买的 License，开启设备关键功能。一般情况下，系统默认已导入 License，如需手动导入，可参考本节。

前提条件

已完成首次登录设备配置，具体操作请参见登录 WEB 控制台。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【系统维护】>【系统升级】，进入授权导入页面。

步骤 4 单击【导入授权】，导入下载好的 license 文件。

注意

- 系统时间一定要在使用许可时间之内，否则会出现内网用户掉线的情况。
- 如要进行系统升级操作，请确保在升级许可时间内进行操作，否则将无法升级。

——结束

3.1.5. 系统升级

升级前请检查系统当前的软件版本是否为最新，如非最新版本，建议升级到官方发布的最新版本。

说明

用户可通过如下几种方式获取升级包：

- 通过 Panabit 技术论坛 https://bbs.panabit.com 下载。
- 通过 Panabit 官网下载中心：https://www.panabit.com/download 下载。
- 通过客户服务电话 400-773-3996 或联系当地的技术人员获取。

Panabit 官网下载中心中所展示的，即为当前最新版本。

升级的操作会让网络中断几秒钟，在现网环境中升级时需谨慎，建议在无业务运行的夜间或周末进行系统升级操作。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

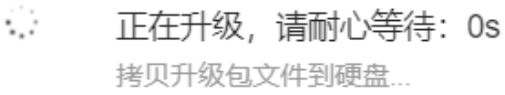
步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【系统维护】>【系统升级】，进入系统升级页面。

步骤 4 单击【升级系统】，上传下载好的升级包文件。

步骤 5 升级包上传后，在弹出的页面中单击【确定】。

步骤 6 等待升级完成。



——结束

3.2. 网关部署

将 Panabit 上网行为管理以网关的形式，部署在网络的出口，主要为网络提供内网 DHCP、PPPOE 认证、Web 认证、高性能 NAT、多链路负载均衡等服务。

3.2.1. 应用案例

某客户的办公网 IP 为 192.168.100.0/24，Panabit 上网行为管理的 eth1 作为 WAN 口（100.100.100.1）连接外网，eth2 作为 LAN 口（192.168.100.1）连接内网。

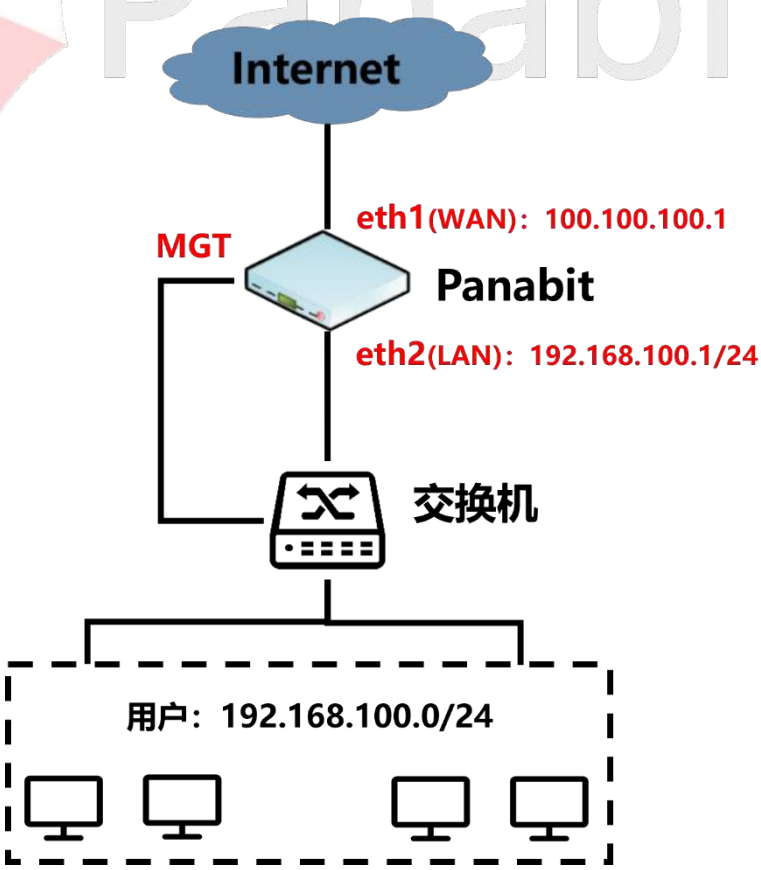


图 3-2 网关部署

3.2.2. 配置步骤

开启配置前，需要确定各接口的角色及 IP 地址。设备的所有参数（除设备登录时进行的改动外），均为出厂时的缺省配置。

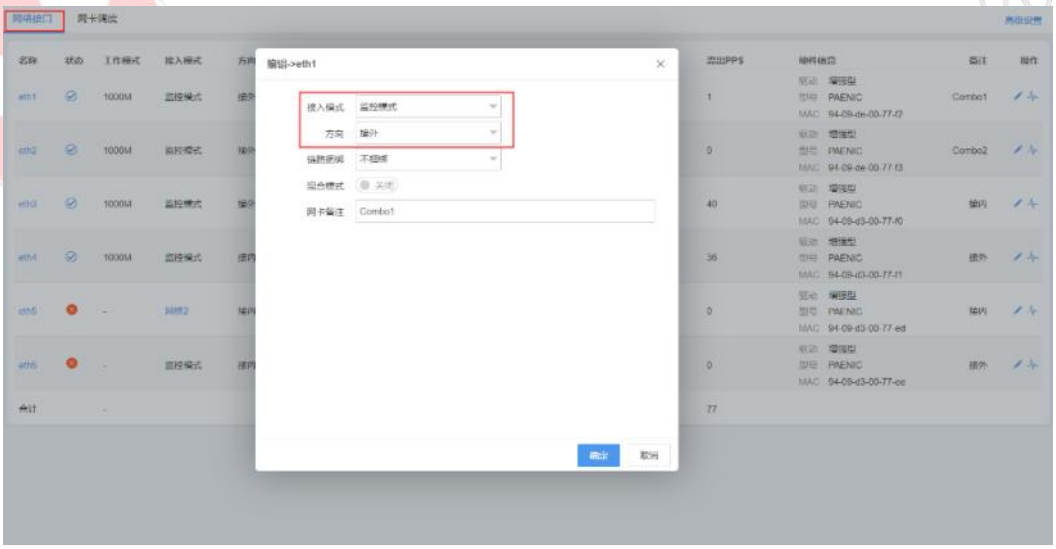
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

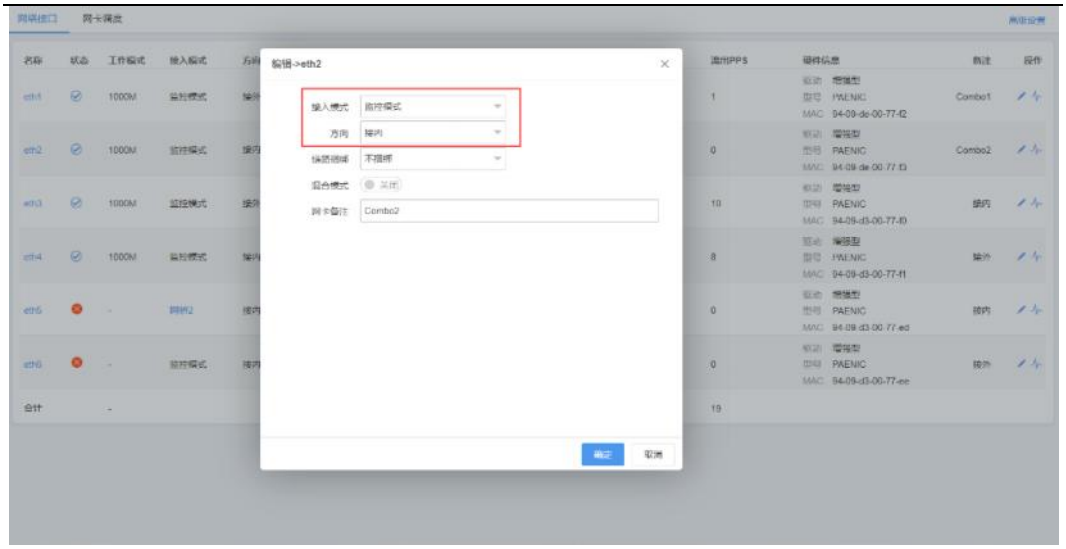
步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 配置数据网卡。

1. 选择左侧功能列表中的【网络管理】>【网卡设置】。
2. 选择页面上方的【网络接口】，进入数据网卡配置页面。
3. 单击 eth1 右侧操作列的 图标，在弹出的窗口中，“接入模式”设置为“监控模式”，“方向”设置为 “接外”。

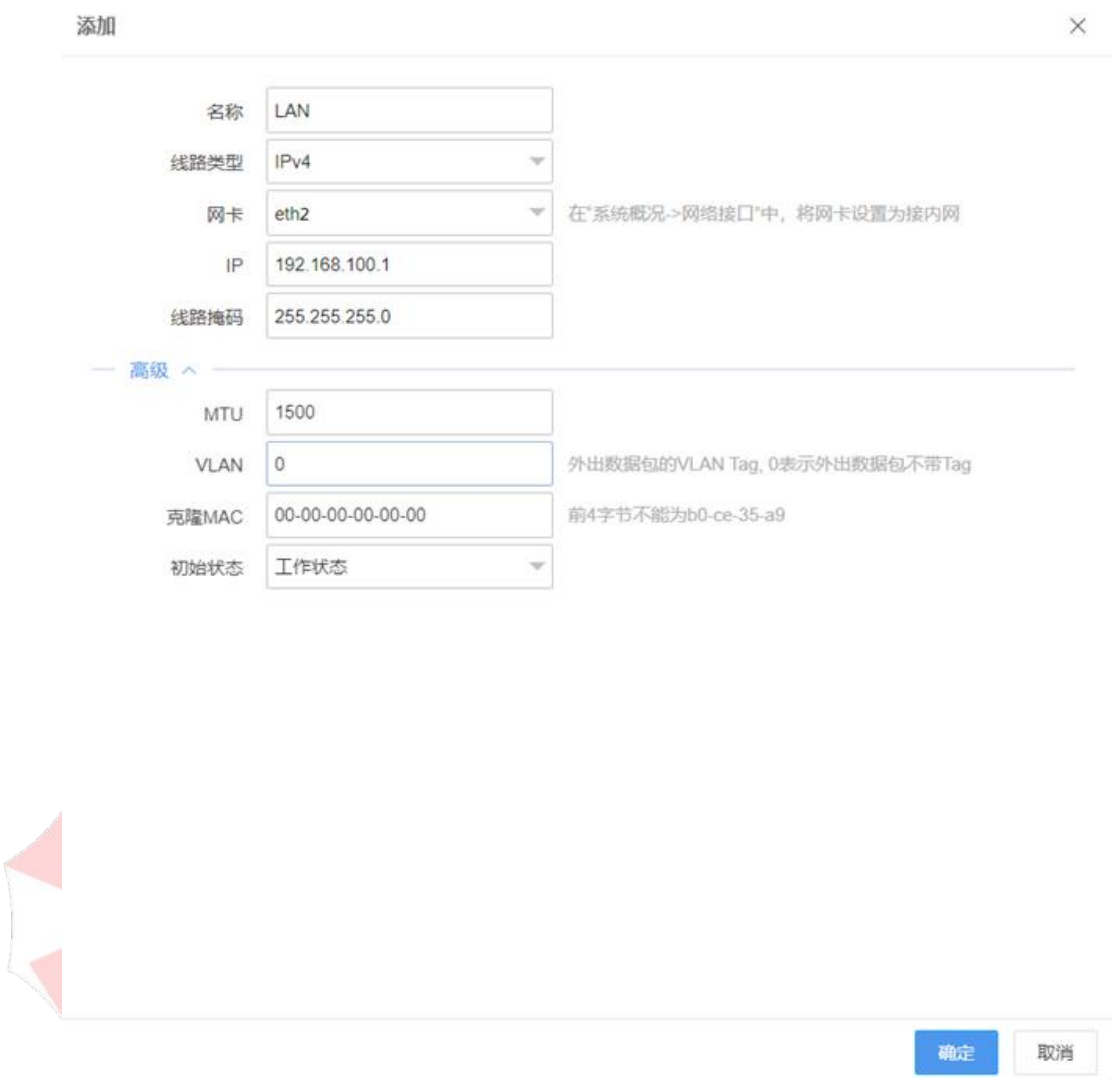


4. 单击 eth2 右侧操作列的 图标，在弹出的窗口中，“接入模式”设置为“监控模式”，“方向”设置为“接内”。



步骤 4 配置 LAN 口。

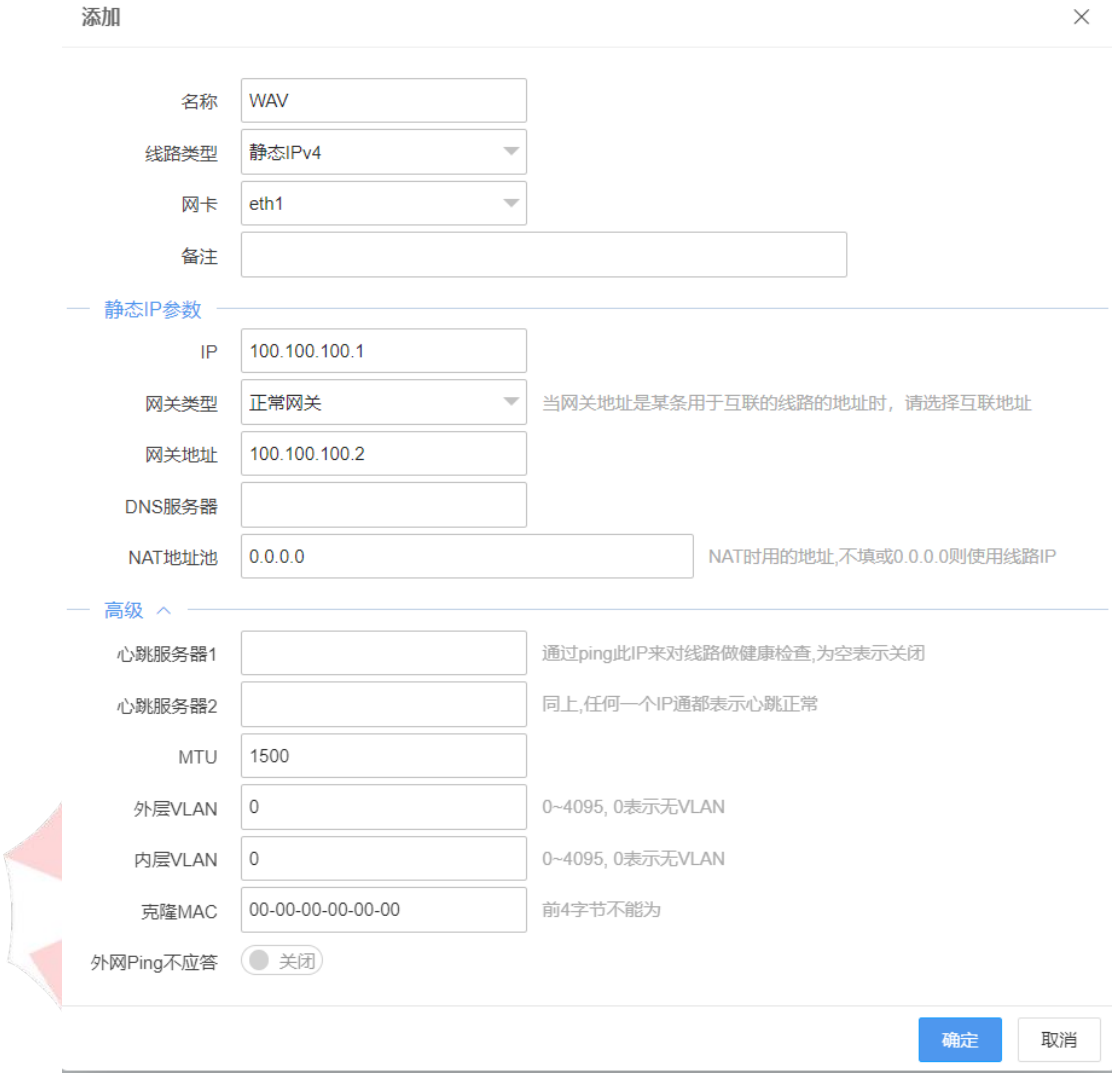
1. 选择左侧功能列表中的【网络管理】>【LAN/WAN】。
2. 选择页面上方的【LAN 接口】，进入 LAN 接口配置页面。
3. 单击右上角的【添加】，可根据实际业务选择单个添加或批量添加。
4. 在弹出的窗口中配置线路名称为“LAN”，网卡选择 eth2，IP 地址为 192.168.100.1，掩码为 255.255.255.0，其余不变。



5. 单击【确定】完成配置。

步骤 5 配置 WAN 线路。

1. 选择左侧功能列表中的【网络管理】>【LAN/WAN】
2. 选择页面上方的【WAN 线路】，进入 WAN 线路配置页面。
3. 单击右上角的【添加】，可根据实际业务选择单个添加或批量添加。
4. 在弹出的窗口中配置线路名称为“WAN”，网卡选择 eth1，IP 地址为 100.100.100.1，网关为 100.100.100.2，其余不变。



5. 单击【确定】。

说明

当网络出口不是固定 IP，只有 PPPoE 拨号线路时，线路类型请选择“PPPoE”，然后填入 PPPoE 的账号密码；同理，线路类型也可选择 DHCP 等方式。

步骤 6 配置默认路由。

1. 选择左侧功能列表中的【网络管理】>【IPv4 路由/NAT】。
2. 单击右上角的【添加】，在弹出的窗口中配置策略序号为 1000 的策略路由，“执行动作”为“NAT”，“NAT 线路”为“WAN”，其余不变。

3. 单击【确定】。

——结束

3.3. 网桥部署

以网桥的形式，串接在核心交换机与出口之间，网桥相对上下联设备来说是完全透明的。主要用来做流量控制、上网行为管理以及网络分流等。

3.3.1. 应用案例

某用户的办公网 IP 为 192.168.100.0/24，Panabit 上网行为管理作为透明网桥部署在网络出口，以便后续对用户的办公网络进行流量的分析与管控。

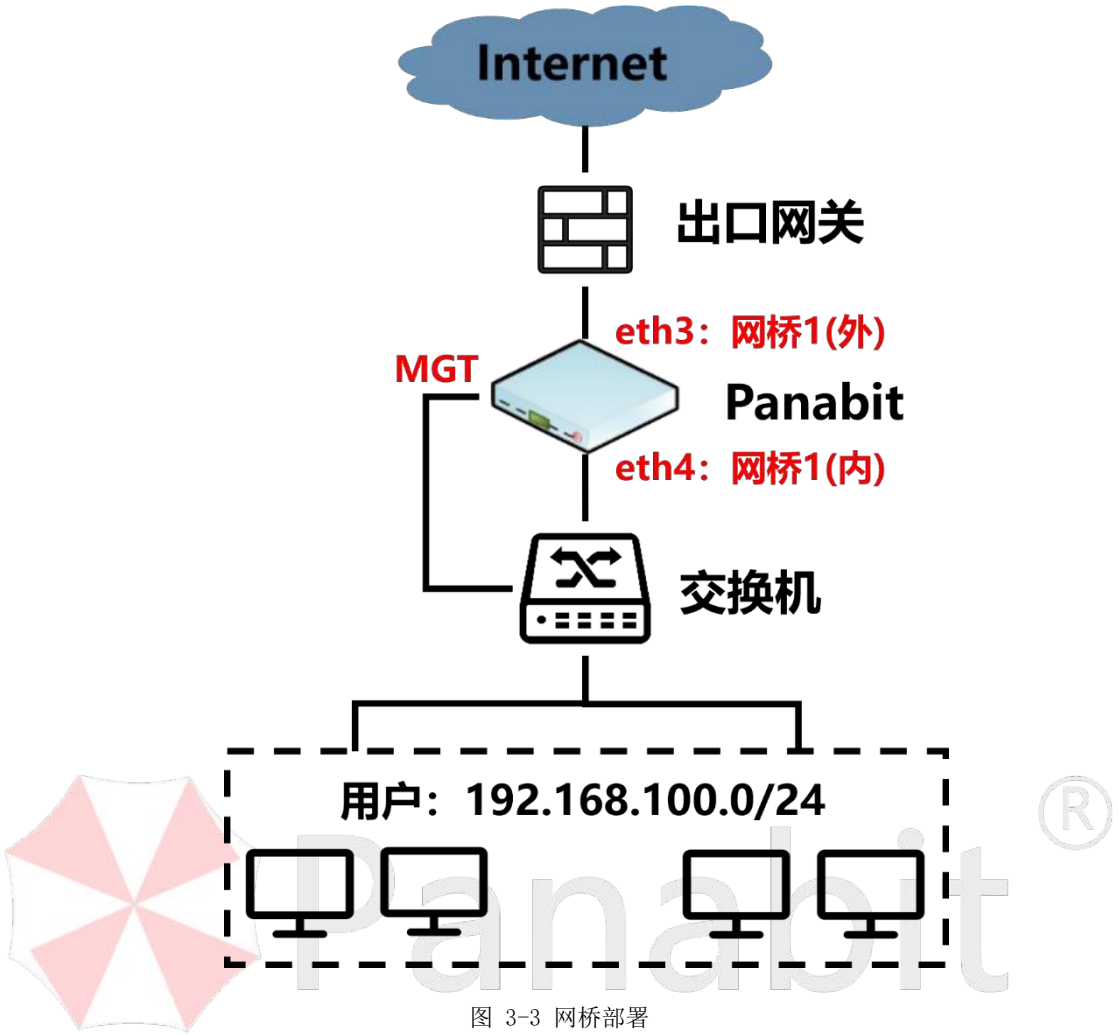


图 3-3 网桥部署

3.3.2. 配置步骤

开始配置前，设备的所有参数（除设备登录时进行的改动外），均为出厂时的缺省配置。

须知

1. 确定各接口的角色。设置网桥时，每两个数据接口为一组网桥，将一个设置为“接内网”，另一个设置为“接外网”，并且互为对端接口，这里需要注意的是每一对网桥的组成必须是两张网卡就相当于两口 2 层交换机一样，一进一出。
2. 配置一对网桥并正确接线。

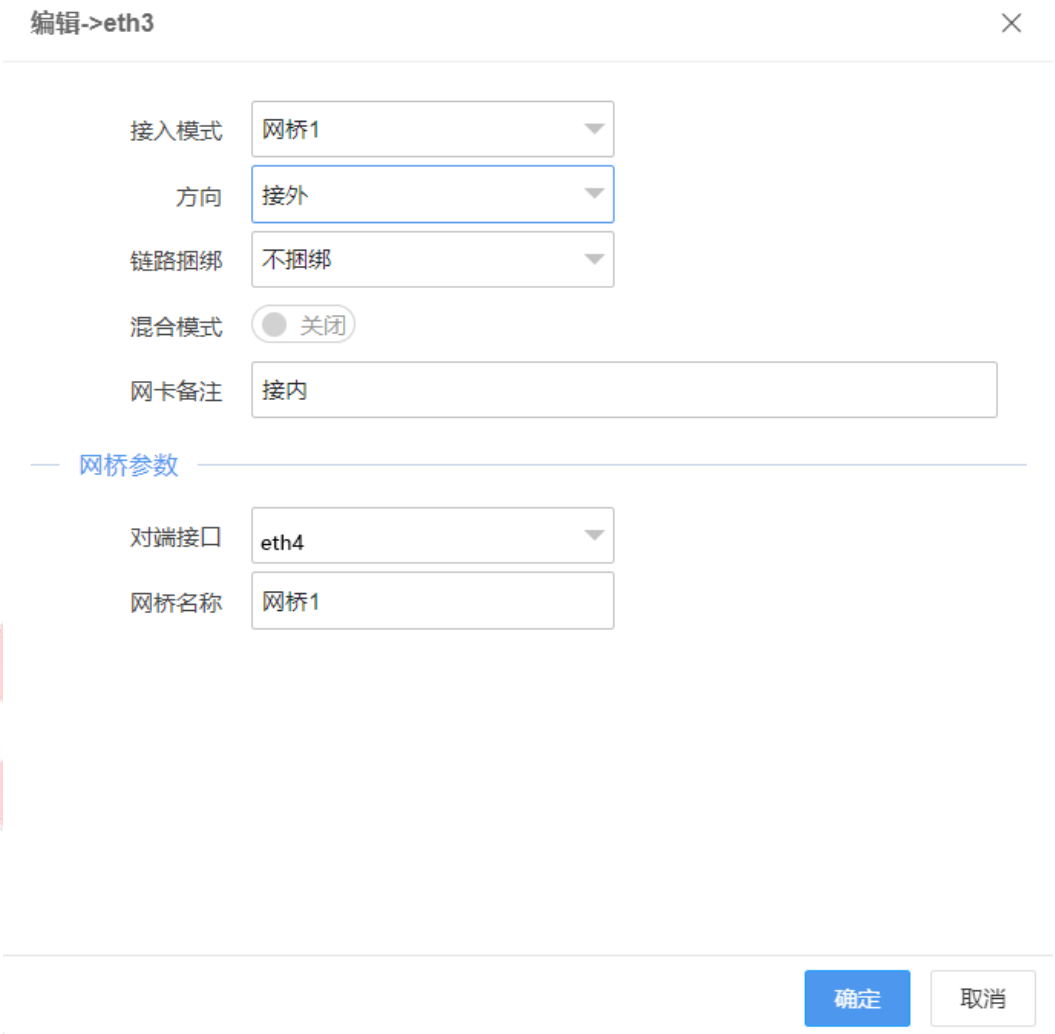
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

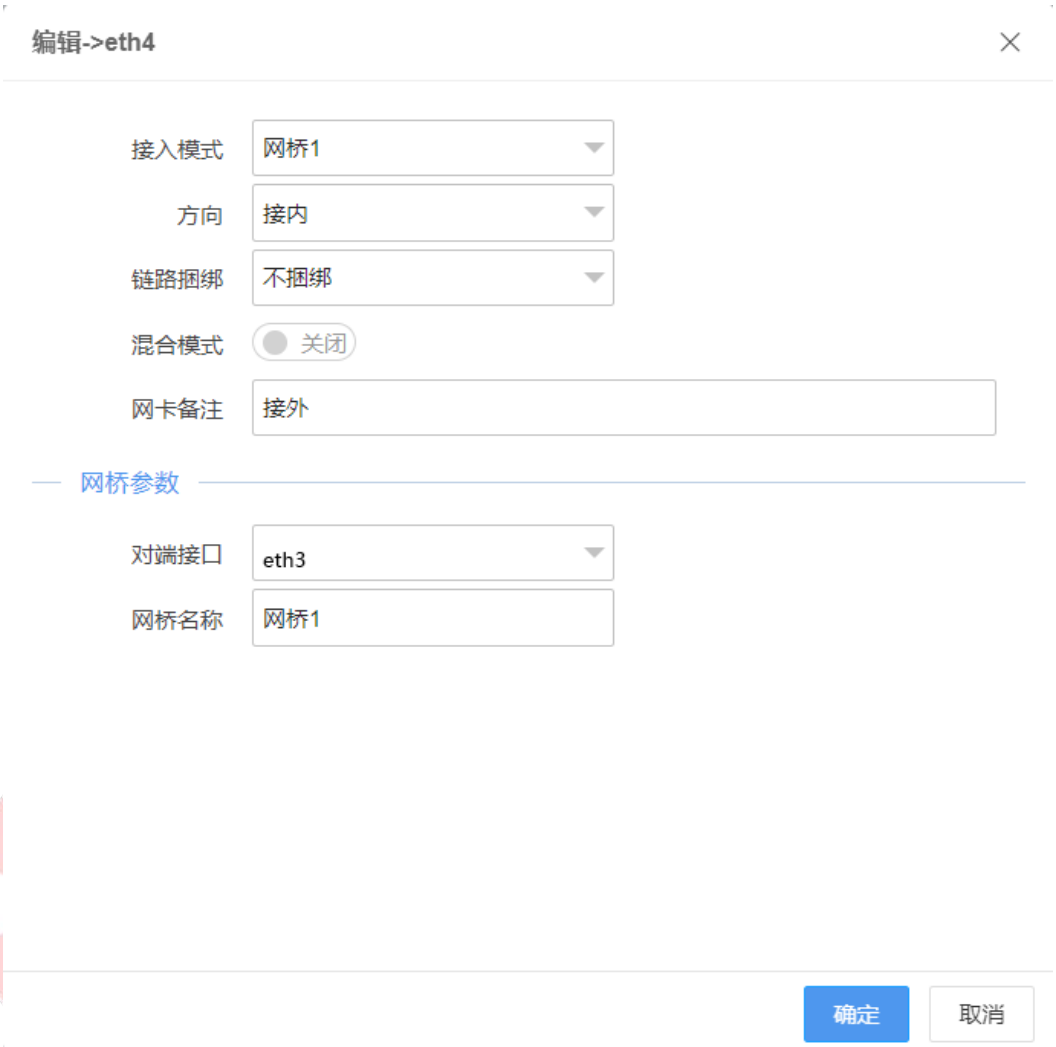
步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 配置数据网卡。

1. 选择左侧功能列表中的【网络管理】>【网卡设置】。
2. 单击 eth3 右侧操作列的 图标，在弹出的窗口中，接入模式选择“网桥 1”，方向选择“接外”，对端接口选择“eth4”。



3. 单击 eth4 右侧操作列的 图标，在弹出的窗口中，接入模式选择“网桥 1”，方向选择“接内”，对端接口选择“eth3”。



步骤 4 单击【确定】，完成配置。

步骤 5 选择【流量概况】>【在线用户】，通过显示的 IP 来确认网桥的方向设置是否正确。

- 如【在线用户】里显示的都是用户侧的 IP，则网桥方向设置正确。
- 如【在线用户】里显示的都是公网 IP，则需要调整网络接口的网桥设置方向。

——结束

3.4. 旁路部署

数据通过镜像或者分光的方式将流量牵引到Panabit 的监控接口，Panabit 在旁路分析数据报文，并存储用户上网日志，对数据做进一步汇总分析。

3.4.1. 应用案例

某用户的办公网 IP 为 192.168.200.0/24，服务器区的 IP 为 192.168.100.0/24，Panabit 上网行为管理旁挂在核心交换机，通过 eth5 口接收核心交换机的镜像数据。

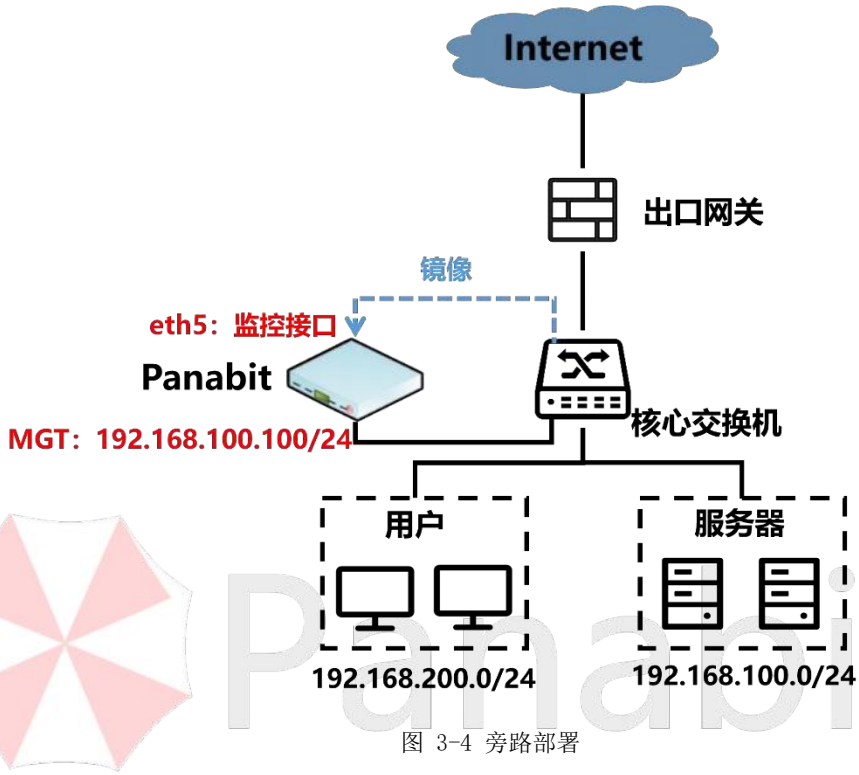


图 3-4 旁路部署

3.4.2. 配置步骤

开始配置前，设备的所有参数（除设备登录时进行的改动外），均为出厂时的缺省配置。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名和密码，登录 WEB 控制台。

步骤 3 配置数据网卡。

1. 选择左侧功能列表中的【网络管理】>【网卡设置】。
2. 点击 eth5 右侧操作列的 图标，在弹出的窗口中，“接入模式”选择“监控模式”，“方向”选择“接内”。

步骤 4 （可选）配置伪 IP 防护功能。

说明

旁路部署在一定条件下可不开启伪 IP 防护功能。

1. 上下行流量分开镜像

旁路部署的情况下，我们也可以通过交换机将网络的上行流量和下行流量分别镜像到 Panabit 的两个不同网卡，由此来区分流量的上下行：

- 针对上行数据做分析，交换机镜像“出”的数据，Panabit 接入位置设置“接内网”。
- 针对下行数据做分析，交换机镜像“入”的数据，Panabit 接入位置设置“接外网”。

2. 开启网卡混合模式

很多情况下，我们可能无法确切地知道内网合法的 IP 地址段，因此无法通过设置【伪 IP 防护】来区分上下行，此时可以通过开启【网卡混合模式】来进行区分。

设置方法：

选择【系统维护】>【网络接口】，点击网卡右侧的编辑按钮，开启混合模式。

在没有设置【伪 IP 防护】的情况下，开启网卡混合模式后，系统根据会话的源地址和目的地址流量来决定上下行，源->目方向为上行，目->源方向为下行，并且以会话的源地址创建内网在线用户（TCP 会话根据三次握手确定源地址，UDP 会话根据首包确定源地址）。

1. 选择左侧功能列表中的【应用识别】>【引擎参数】。
2. 选择上方栏目中的【合法 IP 列表】，点击右侧的 +添加 按钮，在弹出的窗口中先后填入 192.168.100.0/24，192.168.200.0/24。
3. 单击【确定】
4. 选择页面上方的【引擎参数】，点击“伪 IP 防护功能”后的按钮，使其变成  状态，开启此功能。

——结束

4. 使用指南

本章节主要介绍 Panabit 上网行为管理 WEB 控制台各模块的功能，包含流量概况、安全态势、行为审计、协议质量、溯源分析、网络管理等；并介绍主要典型场景的配置指南，包含 WEB 认证、行为管理、链路负载、虚拟专网、无线 AC、对接公安网监：公共无线上网管理平台等。

说明

使用指南所有配置均是基于 WEB 控制台，请提前登录设备，具体操作请参见设备登录。

4.1. WEB 控制台页面介绍

登录 Panabit 上网行为管理 WEB 控制台，进入首页，详情如图 4-1 所示。

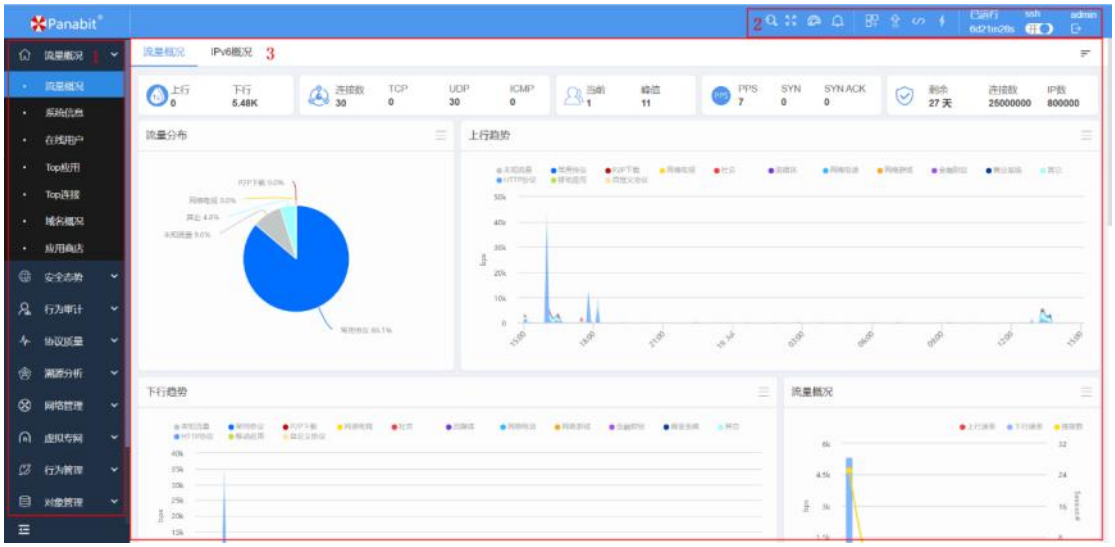


图 4-1 WEB 控制台首页

参数序号	参数说明
<注释 1>	功能列表
<注释 2>	工具栏
<注释 3>	可视化与配置界面

表 4-1 WEB 控制台首页说明

4.1.1. 功能列表

功能列表位于首页左侧，主要包括流量概况、安全态势、行为审计、协议质量、溯源分析、

网络管理、虚拟专网、行为管理、对象管理、应用识别、系统告警、系统维护等，每个菜单下均有二级子菜单，二级子菜单下含有三级子菜单。

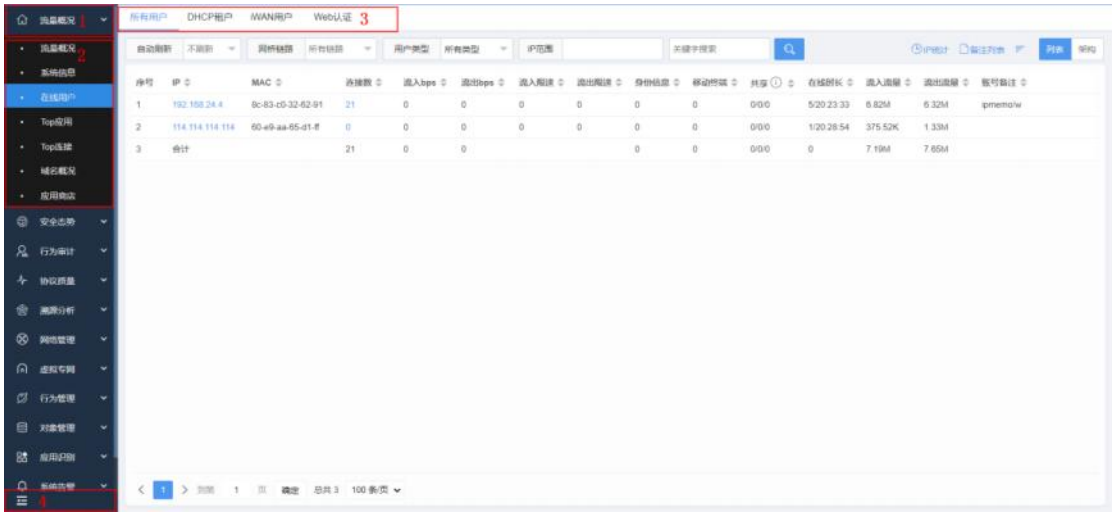


图 4-2 功能列表

参数序号	参数说明
<注释 1>	功能列表一级菜单。
<注释 2>	功能列表二级子菜单。
<注释 3>	功能列表三级子菜单。
<注释 4>	功能列表一级菜单收起/展开键。位于功能列表下方，单击按钮可以收起菜单，再次单击可展开。

表 4-2 功能列表说明

4.1.2. 工具栏

工具栏集成了多种协助运维的工具，能帮助客户快速便捷地进行主题更换、系统升级、命令执行等。

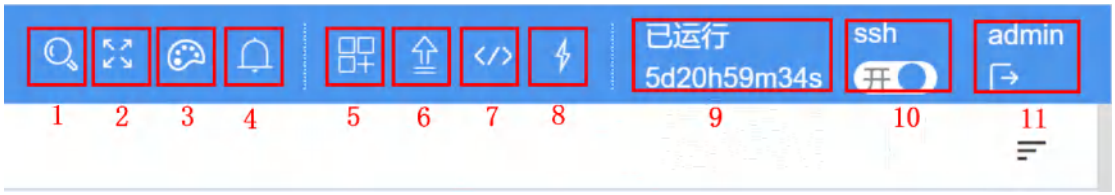
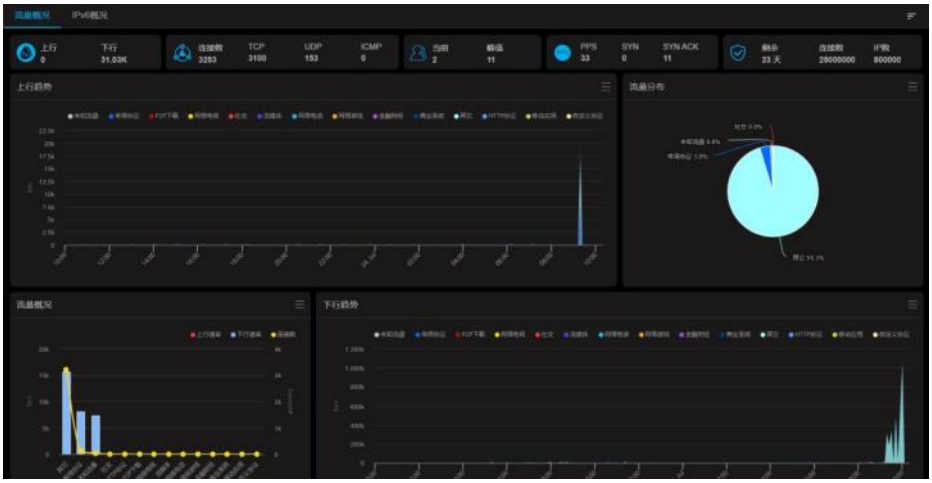
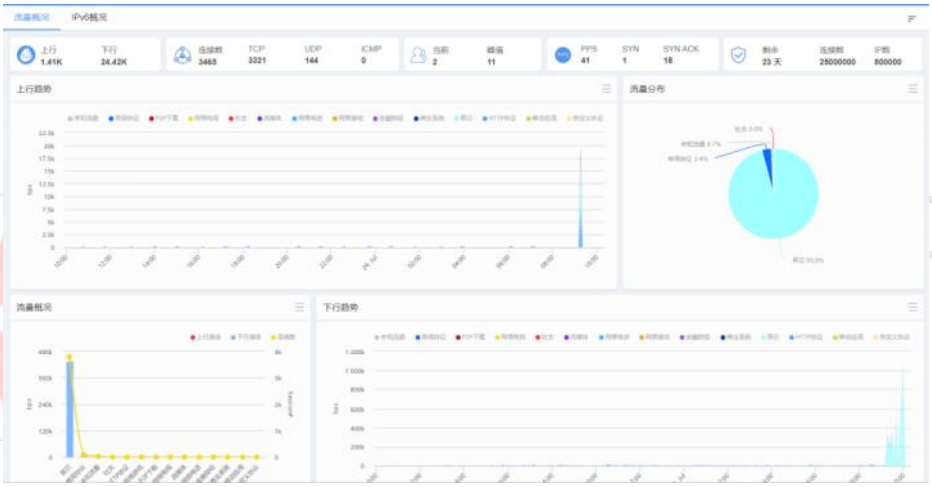


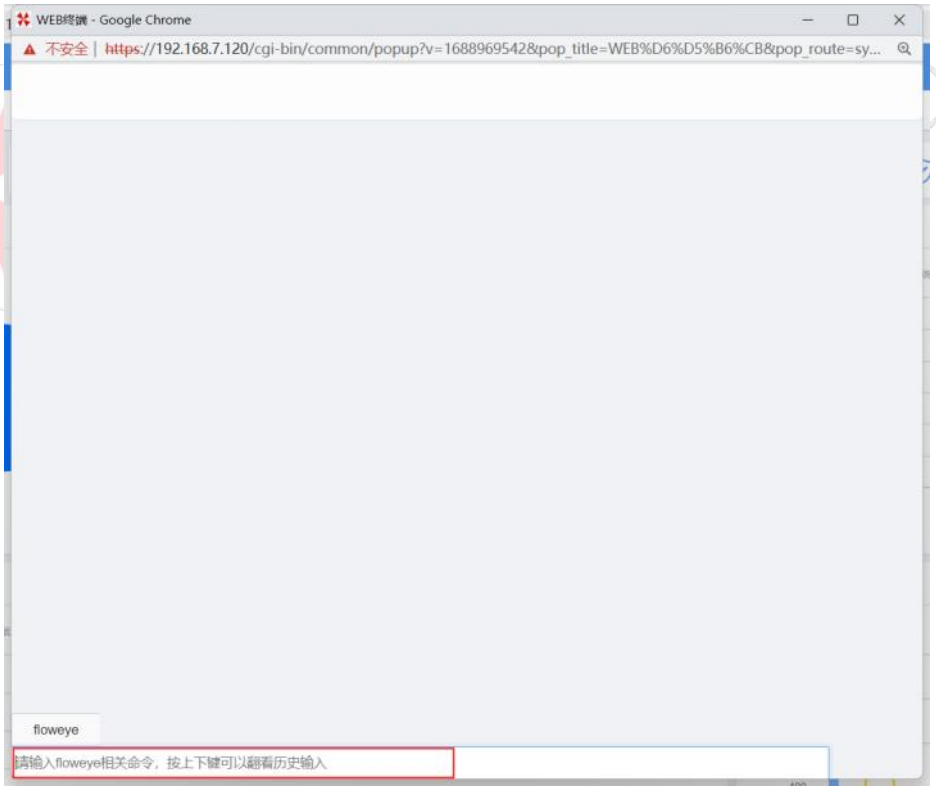
图 4-3 工具栏

参数序号	参数说明
<注释 1>	搜索工具，可输入关键字搜索系统的功能。

〈注释 2〉	全屏工具，单击后页面进入全屏模式，按【Esc】键可退出全屏模式。
〈注释 3〉	主题工具，单击可切换深色/浅色主题。  
〈注释 4〉	消息提醒工具，显示提醒信息，比如是否有新版本等。
〈注释 5〉	应用商店，应用商店是提供安装插件 APP 的平台，这些 APP 是额外功能的扩展，或者帮助运维设备的小工具。鼠标移至  上，会显示常用的 APP。
〈注释 6〉	升级中心，单击  ，可更新软件版本、License。

〈注释 7〉

命令行工具，单击</>，可执行后台命令。



〈注释 8〉

ping 工具，单击图标，可做网络 ping 测试。

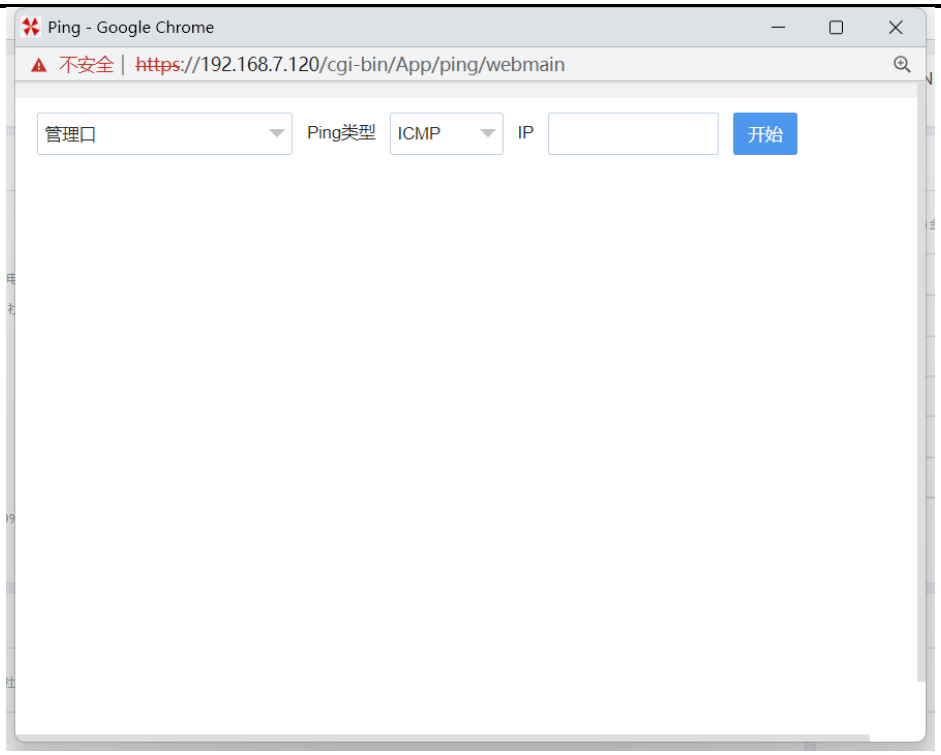
	
<注释 9>	设备运行时间，即操作系统启动到当前的累计时间。
<注释 10>	SSH 开关，白色为开启，灰色为关闭。开启后，可以通过 SSH 工具登录系统后台。
<注释 11>	显示当前登录账号，点击后即可退出管理页面。

表 4-3 工具栏说明

4.1.3. 可视化与配置界面

可视化与配置界面主要针对左侧的功能列表展示其具体功能，用户可根据业务需要自定义可视化界面展示内容，或是对设备进行配置。

4.1.3.1. 自定义仪表盘内容及顺序

鼠标悬停或单击 后，显示仪表盘列表，勾选后，主界面会按照列表的顺序显示被勾选的仪表盘，单击并长按鼠标左键拖拽，可重新排列每个仪表盘的顺序。

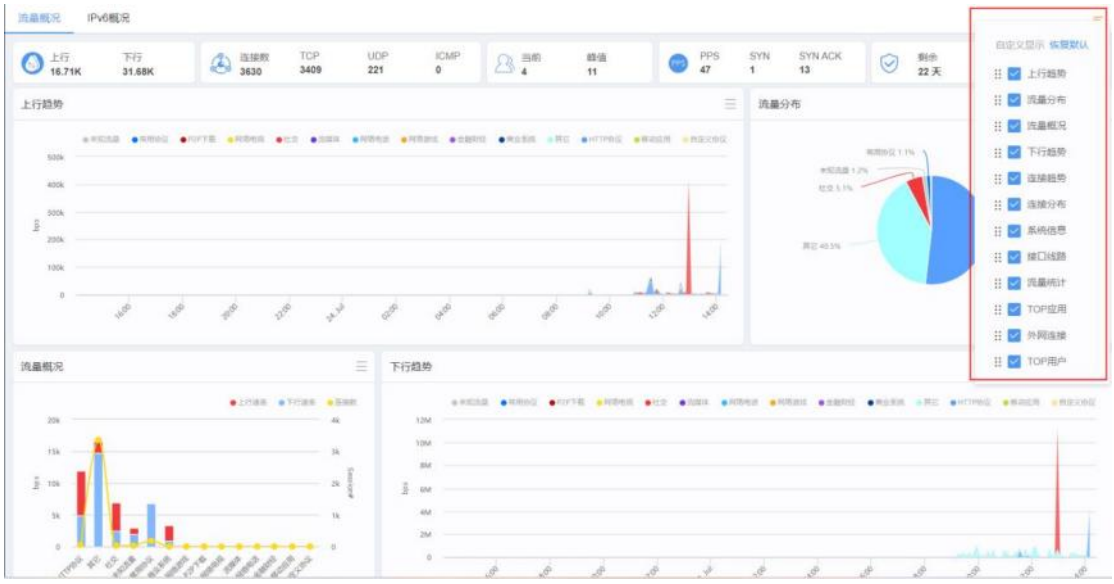


图 4-4 自定义主界面仪表盘

4.1.3.2. 列表内容排序

可视化界面中，以列表显示的页面，大部分都可以选择优先关注的列进行排序，单击 可以进行升序或降序。

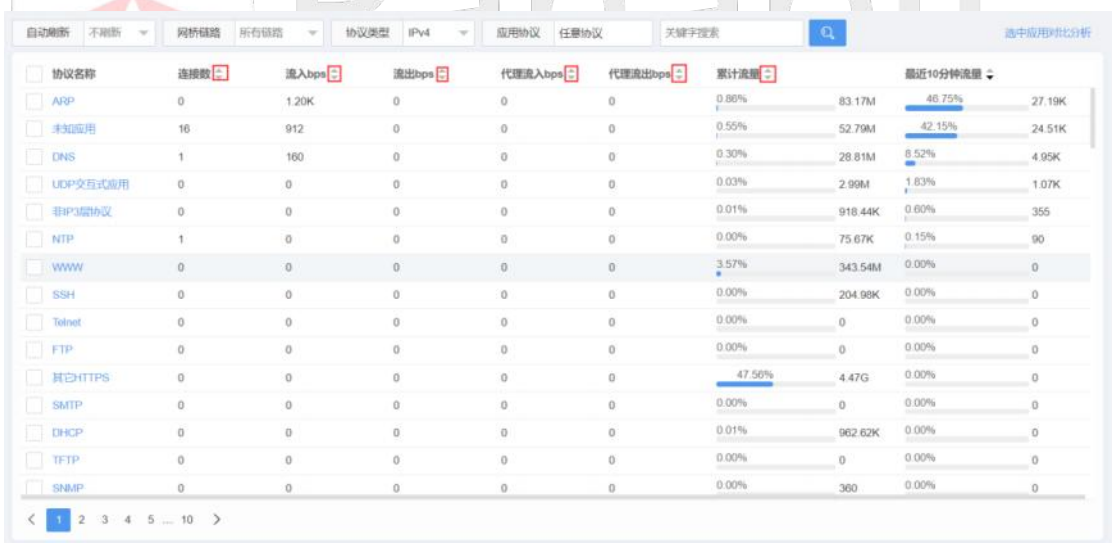


图 4-5 列表内容排序

4.1.3.3. 自定义图表内容

对于有多个内容集合的折线图，可单击每个内容的名称，○变灰则不显示，○有颜色填充则显示。单击图标 ☰ ，可选择仪表盘内容展示时间或隐藏仪表盘。

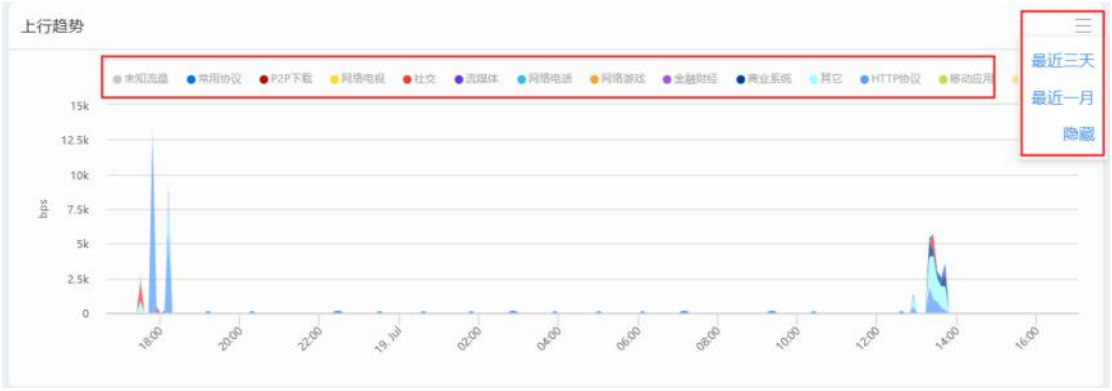


图 4-6 折线图内容筛选

4.1.3.4. 配置原则

在所有的配置界面中，如果有 确定 按钮，则配置完毕后，需要点击该按钮方能使其生效，否则配置不会被保存。

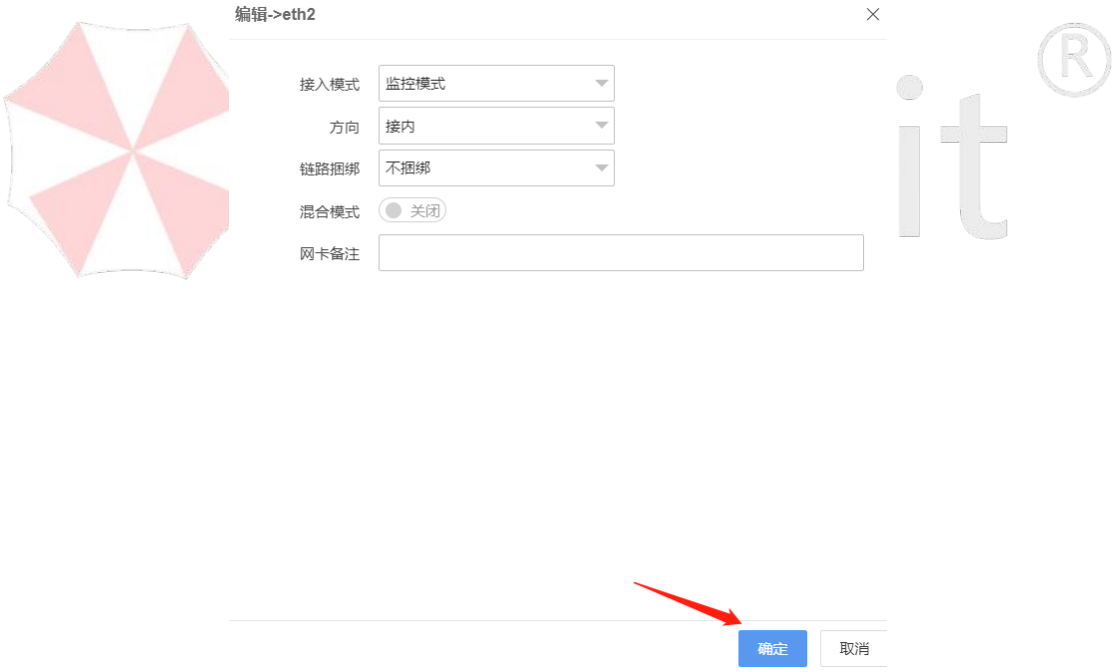


图 4-7 配置保存界面

注意

- 点击【确定】配置完毕后，新的配置会立即生效！
- 在更改配置前请对配置进行备份，备份方法见配置管理。
- 提交配置前，请务必核对配置信息是否正确无误。

4.2. 流量概况

流量概况是用户登录系统后的默认展示页面，展示了系统所监控网络的整体概览。流量概况支持基于 IPv4、IPv6 应用协议显示其上/下行流量，连接趋势、流量连接、分布情况等。

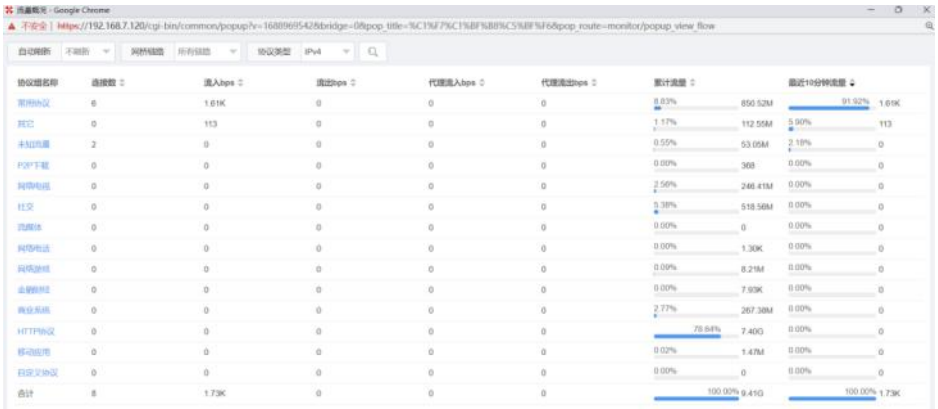
4.2.1. 流量概况

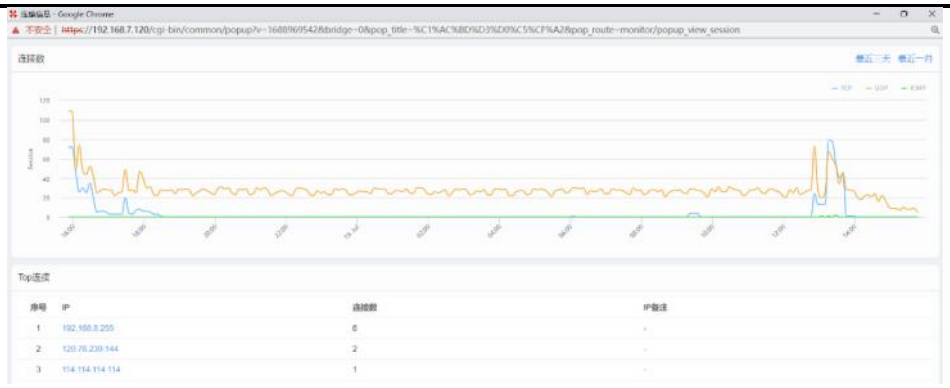
步骤 1 选择【流量概况】>【流量概况】。

步骤 2 选择页面上方的【流量概况】或【IPv6 概况】查看流量使用详情。

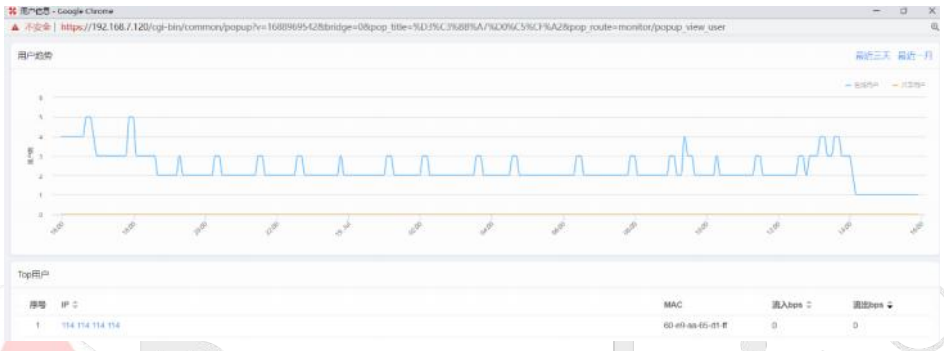
图 4-8 流量概况

图 4-9 IPv6 概况

参数名称	参数说明
上行/ 下行	通过该设备的上下行实时流量，单击，可查看当前应用分类的上/下行流量详情页面。 
连接数	统计设备接入流量的当前连接总数，以及 TCP/UDP/ICMP 连接数。单击，可查看连接趋势和 TOP 连接内网 IP 的详情页面。



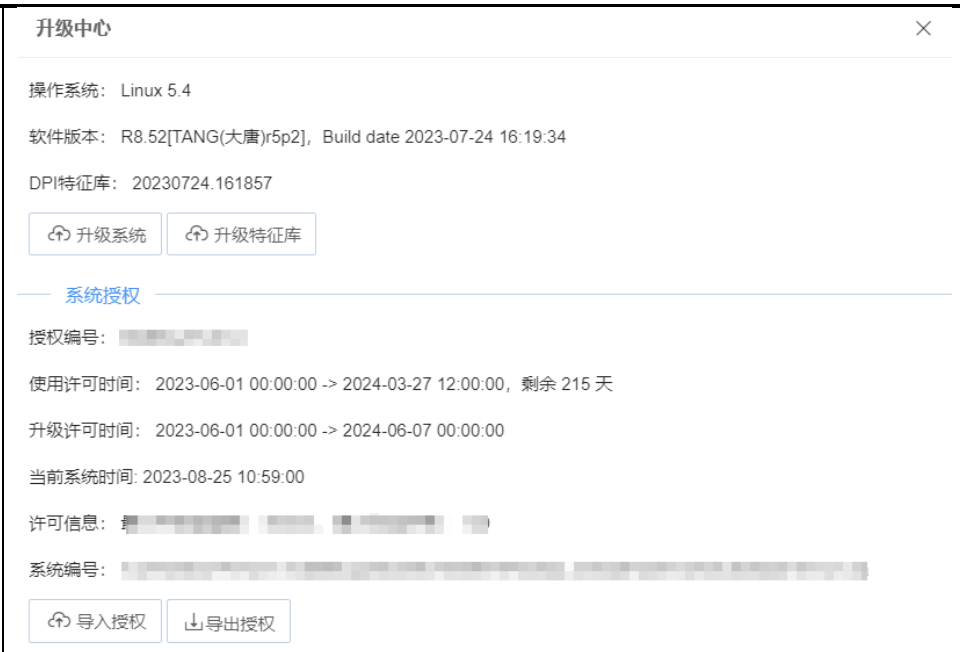
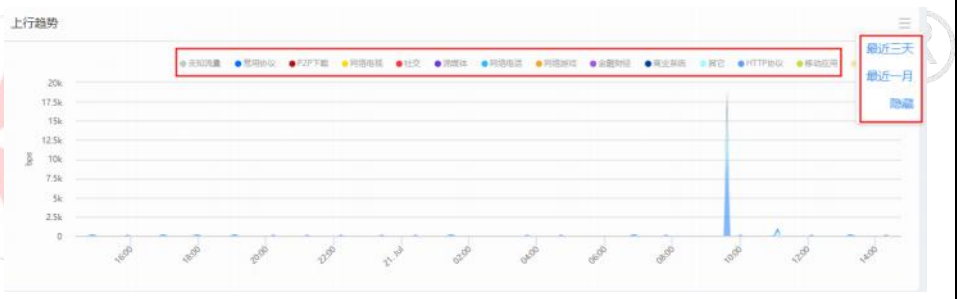
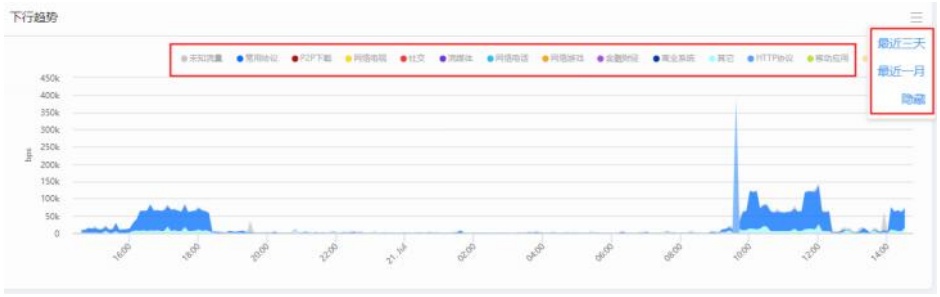
用户信息	当前在线用户数/峰值在线用户数，单击，可查看用户在线趋势和内网 TOP 用户的流量详情页面。
PPS	统计当前设备流入流量的 PPS 总数，分别统计 SYN 报文和 SYN ACK 报文当前的数量。单击 PPS ，可查看 PPS 趋势、SYN 报文趋势和 SYN ACK 报文趋势详情页面。
升级中心	设备当前 License 状态。单击 ，可查看系统和 License 详情页面，并且可进行系统升级或更新 License。

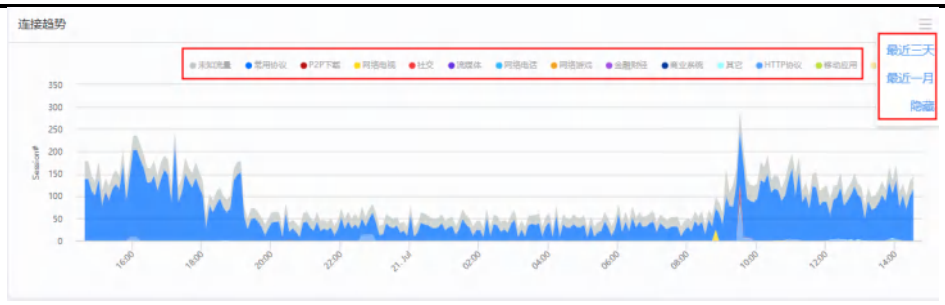


说明

SYN：当前通过设备报文中同步序列编号字段 SYN 数量。

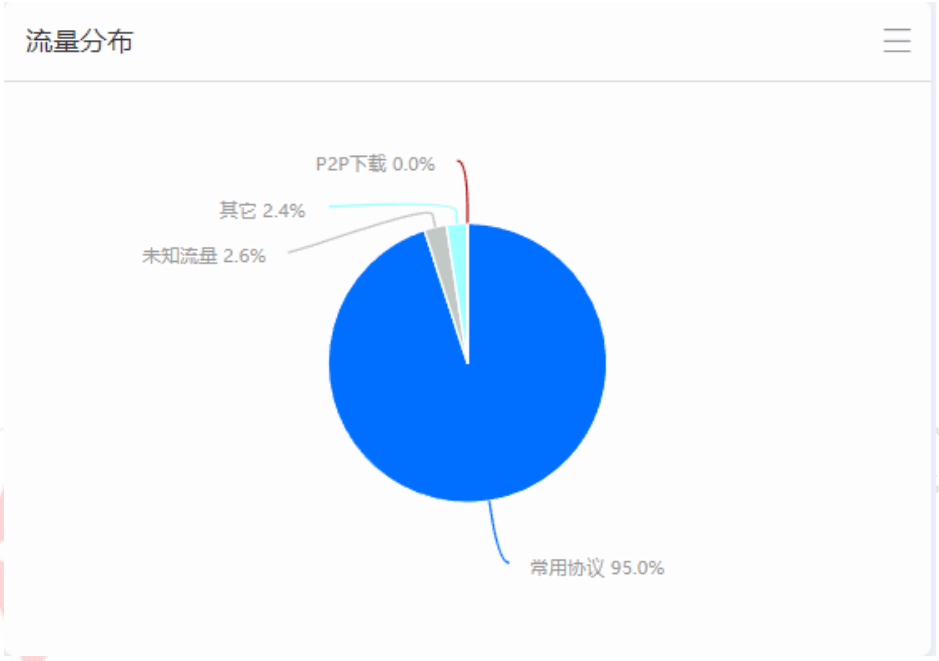
SYN ACK：当前通过设备报文中同步确认字段 SYN ACK 数量

	
上行趋势	展示最近 24 小时/最近三天/最近一月通过设备基于应用协议的上行流量趋势，可单击应用协议类型名称进行筛选。 
下行趋势	展示最近 24 小时/最近三天/最近一月通过设备基于应用协议的下行流量趋势，可单击应用协议类型名称进行筛选。 
连接趋势	展示最近 24 小时/最近三天/最近一月通过设备基于应用协议的所有会话并发趋势，可单击应用协议类型名称进行筛选。



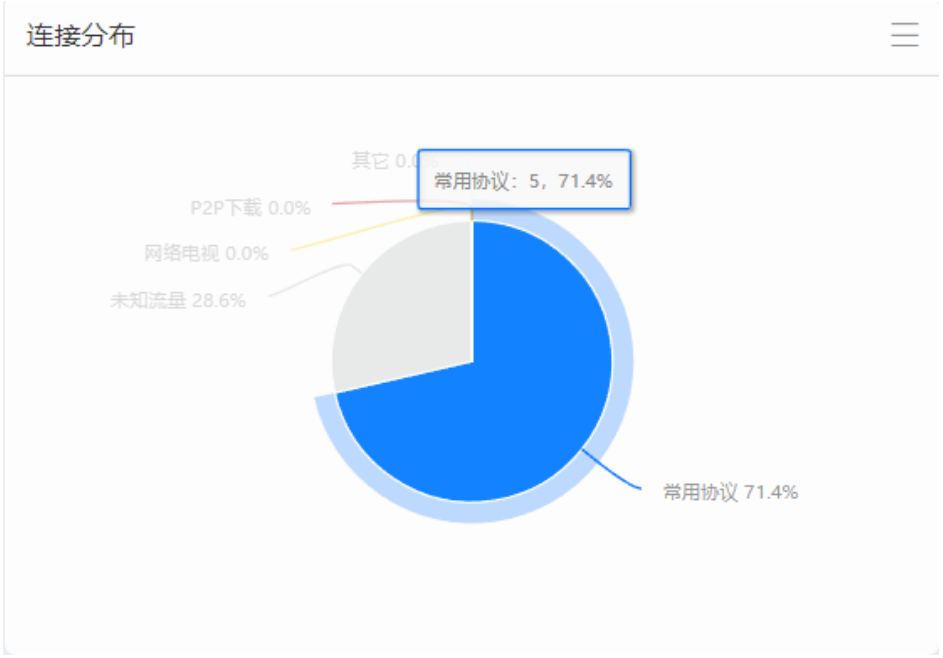
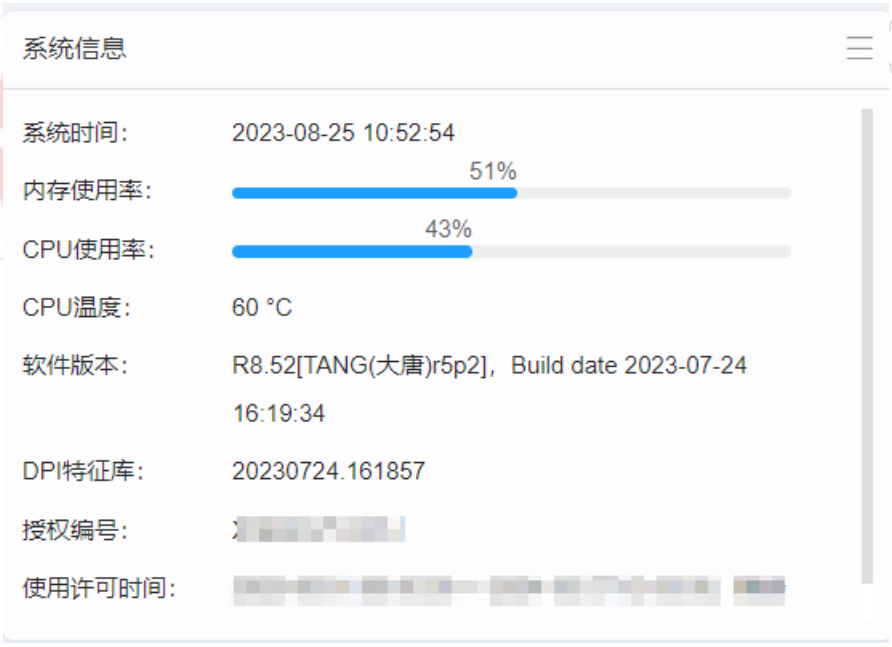
流量分布

展示最近 10 分钟内各个应用流量累计占比。



流量概况

展示当前设备各个应用的流量和连接情况。蓝色代表下行速率，红色代表上行速率，曲线图代表各应用的连接数。

连接分布	展示当前各个应用的连接占比。 
系统信息	展示当前设备系统信息。 
接口线路	展示当前设备 LAN 和 WAN 接口信息。

流量统计

展示 TOP7 应用大类的当前速率及流量占比。

TOP 应用

展示 TOP7 应用的速率。

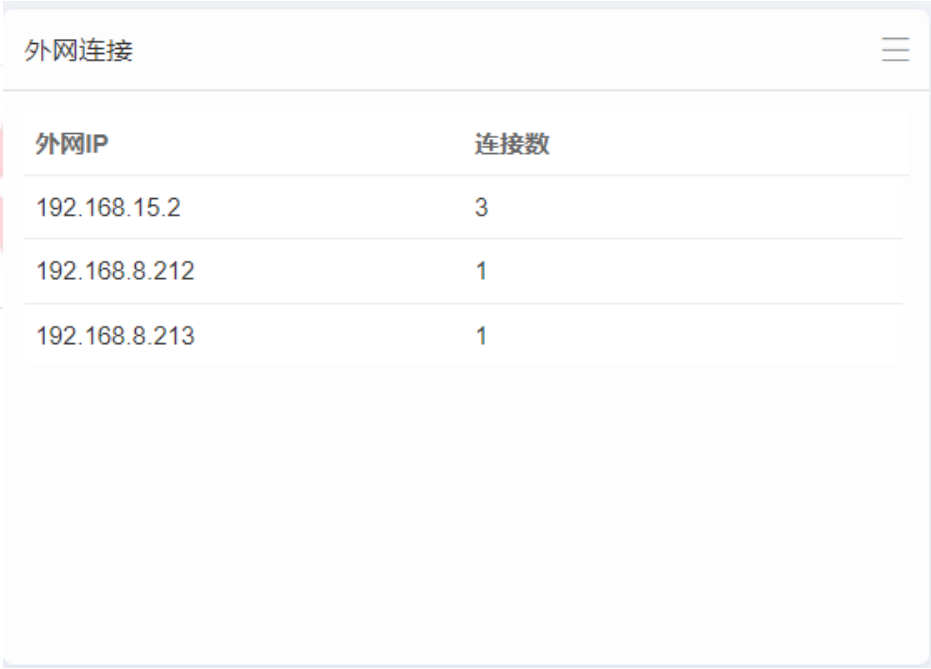
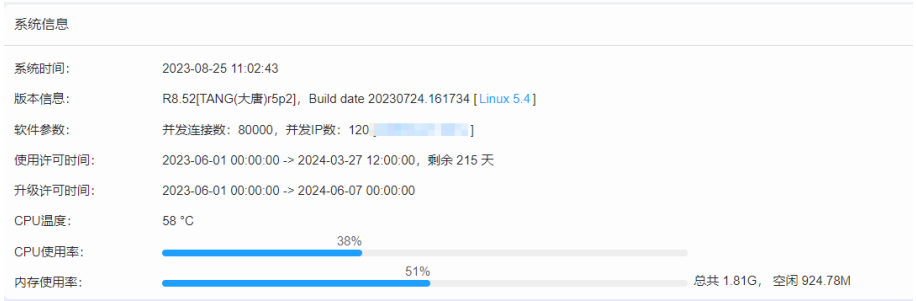
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>外网用户</td><td>展示 TOP7 的目标 IP 连接数。 
</td></tr>
<tr><td>TOP 用户</td><td>展示 TOP7 的内网用户速率。</td></tr>
</table>

表 4-4 流量概况参数说明

4.2.2. 系统概况

系统概况展示系统自身的信息，包括软件信息、硬件使用情况以及网络概览。

步骤 1 选择左侧功能列表中的【流量概况】>【系统信息】。

参数名称	参数说明
系统信息	显示当前的系统版本、license 规格、内存使用情况等信息。 
连接新建	显示当前连接创建的数量，以及最近 24 小时/最近三天/最近一月连接创建的趋势。 
在线用户	显示当前内网用户数量，以及最近 24 小时/最近三天/最近一月内网用户在

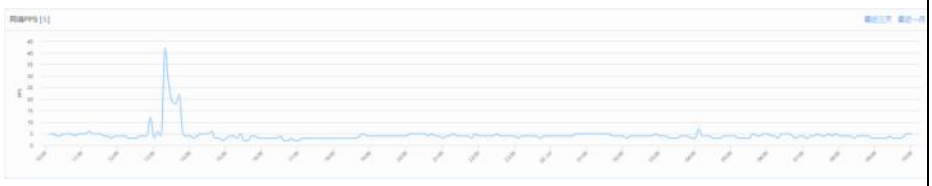
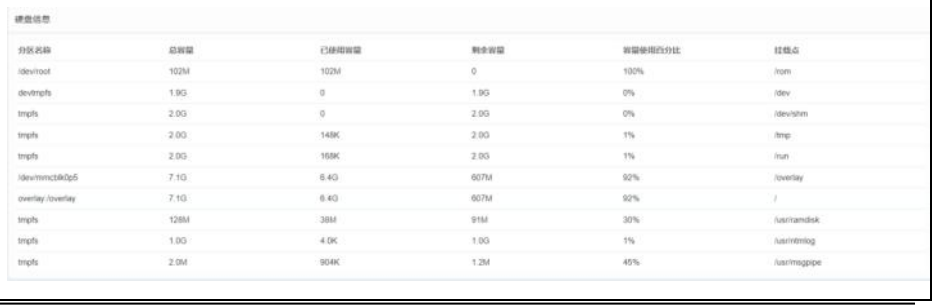
	线趋势。 
网络 PPS	显示当前设备的 PPS 值，以及最近 24 小时/最近三天/最近一月的 PPS 趋势（PPS 即 packet per second，每秒钟有多少数据包经过）。 
SYN PPS SYNACK PPS	显示当前设备的 TCP 三次握手中 SYN 报文和 SYNACK 报文的 PPS 值，以及最近 24 小时/最近三天/最近一月的趋势。 
CPU 使用率 CPU 温度	显示当前设备的 CPU 使用率和 CPU 温度，以及最近 24 小时/最近三天/最近一月的趋势。 
硬盘信息	显示当前设备硬盘容量使用情况及挂载点。 

表 4-5 系统概况参数说明

4.2.3. 在线用户

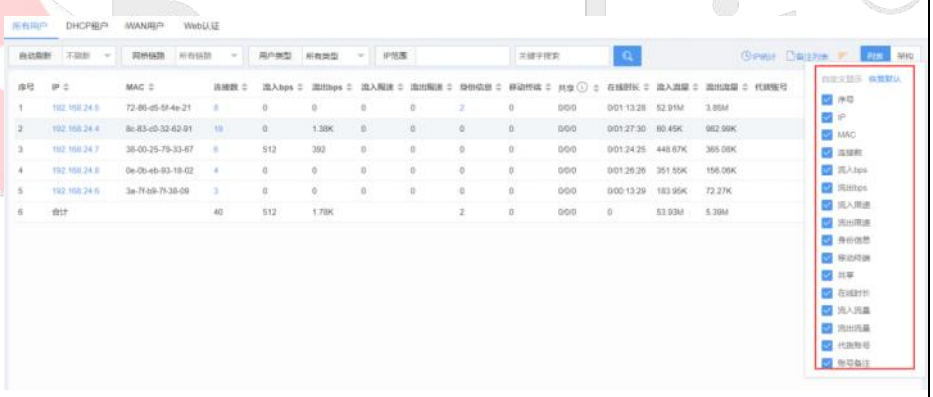
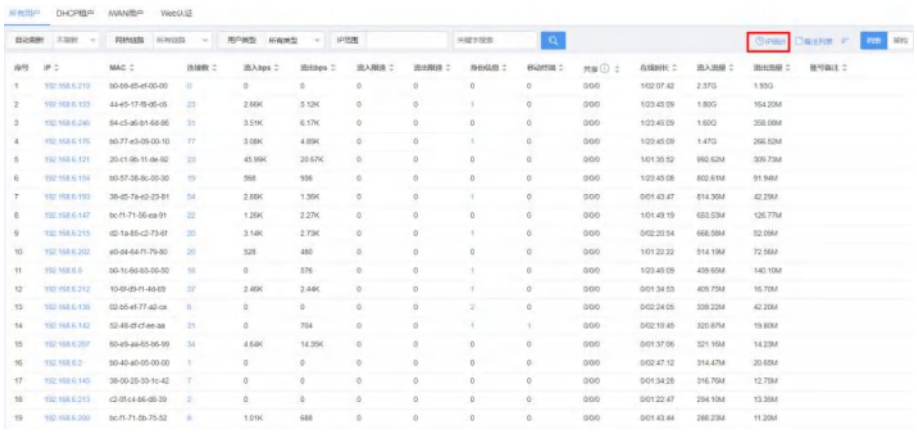
在线用户功能主要展示接入此设备的所有用户基本信息，其中包括直连方式、DHCP 用户、iWAN 用户、Web 认证用户等，并支持对单个用户进行备注、监测与控制。

4.2.3.1. 所有用户

所有用户界面主要展示用户的流量使用详情，并支持对单个 IP 或 MAC 进行备注。

步骤 1 选择【流量概况】>【在线用户】。

步骤 2 选择页面上方的【所有用户】。

参数名称	参数说明
自定义显示	自定义显示用户信息，鼠标悬停或单击 后，可勾选需要在列表中呈现的信息。 
IP 统计	统计在线用户的流量信息，并可对没有流量的空闲 IP 设置自动删除时间。 

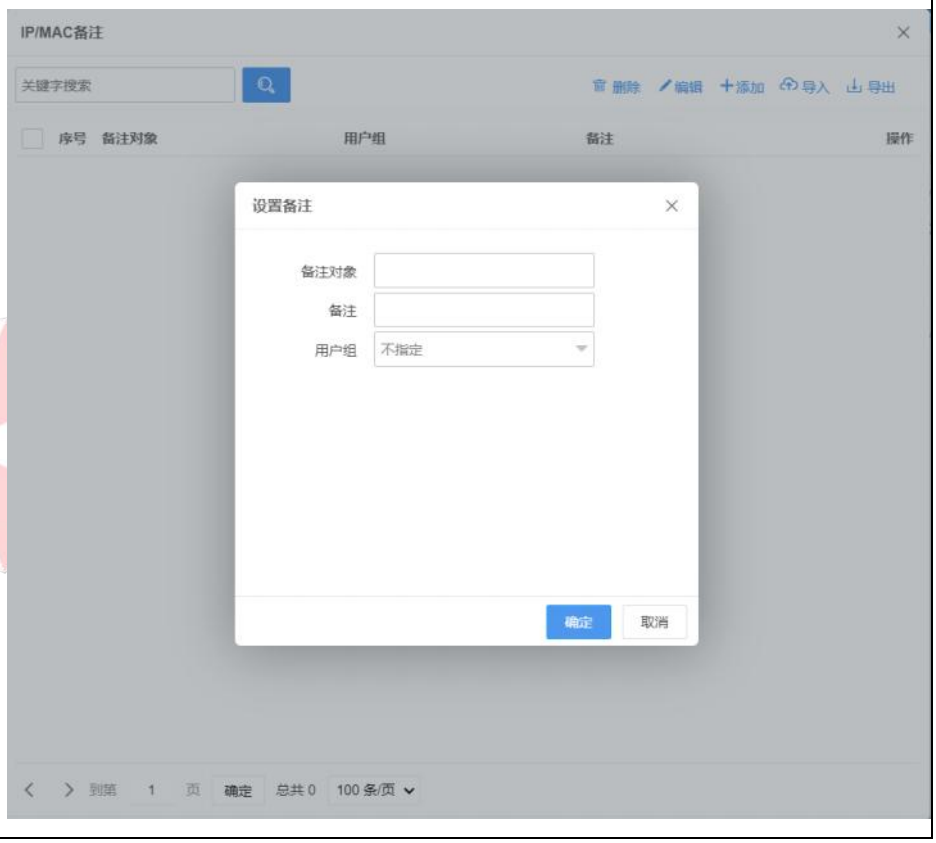
	
备注列表	支持对单个 IP 或 MAC 进行备注，备注信息支持字母，数字，中文或特殊字符，支持导入与导出功能。 

表 4-6 所有用户参数说明

将鼠标悬停在【IP】信息任意位置，每行最右侧出现此 IP 的编辑按钮。

图 4-10 IP 编辑详情页

参数名称	参数说明

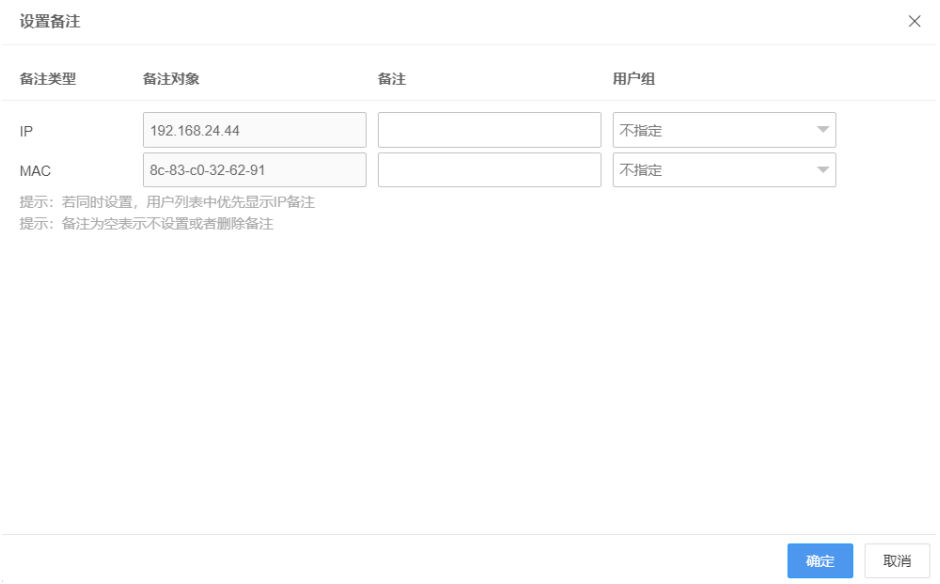
删除会话	单击  ，删除此 IP 会话。
IP 备注	单击  ，可对此 IP 进行备注并指定用户组。 
IP 档案	单击  ，进入 IP 档案详情页面。
IP 画像	单击  ，进入 IP 画像详情页面，具体参数请参见 IP 画像。

表 4-7 IP 编辑详情页参数说明

点击【IP】列的某个具体 IP 名或单击每行最右侧  ，可弹出 IP 档案页面，包含流量概况、连接信息、对端概况、虚拟身份、共享用户、移动终端、账号信息。

参数名称	参数说明
流量概况	实时展示 IP 的请求协议及流量使用详情。 
连接信息	实时展示 IP 当前的全部会话，并可基于既定条件筛选相应的连接信息。 

	说明 上行报文：××/××=上行重传数据包数量/上行总数据包数量 下行报文：××/××=下行重传数据包数量/下行总数据包数量 最大包长：××/××=上行最大包长/下行最大包长 流量：××/××=上行流量/下行流量 速率：××/××=上行速率/下行速率
对端概况	实时展示与当前 IP 建立连接的所有对端 IP，并进行统计。 
虚拟身份	实时展示当前内网 IP 下发现的虚拟身份，可统计的虚拟身份有 QQ 号码、微信 ID、邮箱账号等。  流量概况 连接信息 对端概况 虚拟身份 共享用户 移动终端 账号信息 序号 身份类型 身份信息 最近使用时间 1 微信ID 279 25 2021-06-16 14:51:05 2 QQ号码 115 48 2021-06-16 15:05:02
共享用户	实时展示此 IP 下的私接用户，精准定位私接用户数量。
移动终端	实时展示当前内网 IP 下发现的移动终端类型信息。如果认为该类型不准确，可以通过“拉黑”操作忽略该移动终端类型。  流量概况 连接信息 对端概况 虚拟身份 共享用户 移动终端 账号信息 序号 终端类型 最近访问 操作 1 DUB-TL00 2021-06-16/15:15:04 拉黑
账号信息	实时展示当前内网 IP 对应的账号信息，账号信息的来源有本地认证、radius 认证、IP/mac 备注、radsnif、pppoesnif 等。“踢线”操作可以清除 IP 和账号的对应关系。 

表 4-8 IP 档案参数说明

4.2.3.2. DHCP 租户

DHCP 租户界面主要展示 DHCP 租户的 MAC、IP、用户名、出租时间和租期等信息。

步骤 1 选择【流量概况】>【在线用户】。

步骤 2 选择页面上方的【DHCP 租户】。

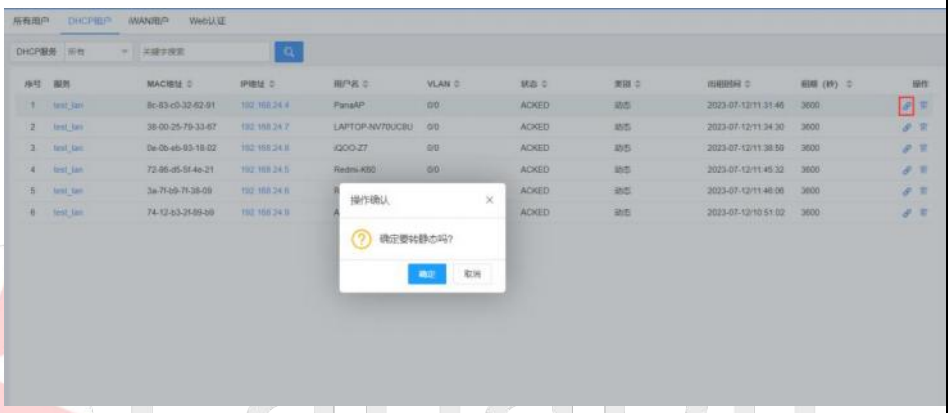
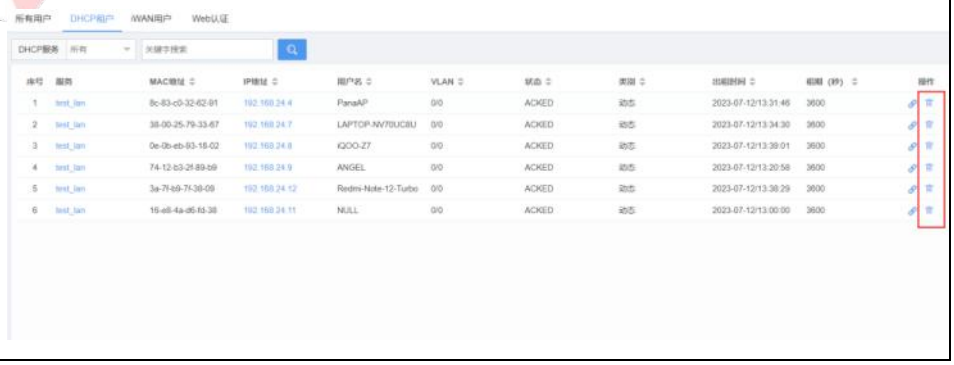
参数名称	参数说明
转静态	将 DHCP 服务分配的动态 IP 地址与该用户 MAC 进行绑定，当该 MAC 下线并再次上线请求地址时，依然分配此 IP。 
删除	将该 IP 地址用户强制下线。 

表 4-9 DHCP 租户参数说明

4.2.3.3. iWAN 用户

iWAN 用户页面主要展示用户的 IP、网关地址、上/下行速率、时延等信息，支持强制下线用户。

步骤 1 选择【流量概况】>【在线用户】。

步骤 2 选择页面上方的【iWAN 用户】。

参数名称	参数说明
自定义显示	根据需求显示单 IP 用户信息，鼠标悬停或单击 后，可勾选需要在列表中呈现的信息。 
强制下线	将该 iWAN 用户强制下线。 

表 4-10 iWAN 用户参数说明

4.2.3.4. Web 认证

Web 用户页面主要展示用户的 IP、MAC、限速、在线时间等信息，支持强制下线用户。

步骤 1 选择【流量概况】>【在线用户】。

步骤 2 选择页面上方的【Web 认证】。

参数名称	参数说明
强制下线	将 Web 认证用户强制离线。 

表 4-11 Web 认证参数说明

4.2.4. TOP 应用

TOP 应用将识别到的应用流量进行展示，并可根据不同条件进行排序与筛选，还可以对选中的应用协议进行对比分析。

步骤 1 选择【流量概况】>【TOP 应用】。

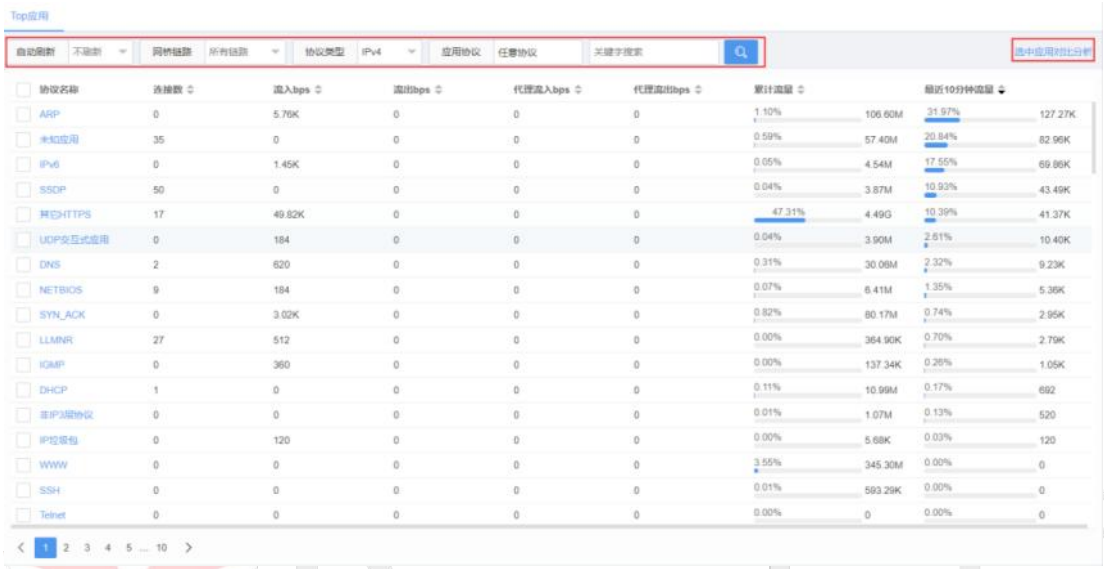


图 4-11 TOP 应用详情

参数名称	参数说明
排序显示	单击 ，可对每列数据进行正序或倒序排序。
自动刷新	应用流量统计结果刷新时间，可选择不刷新或以 5s/10s/20s/60s 为周期进行刷新。
网桥链路	基于网桥链路进行筛选。
IP 类型	根据统计流量协议类型筛选，可选择 IPv4 或 IPv6。
应用协议	可根据应用协议筛选。

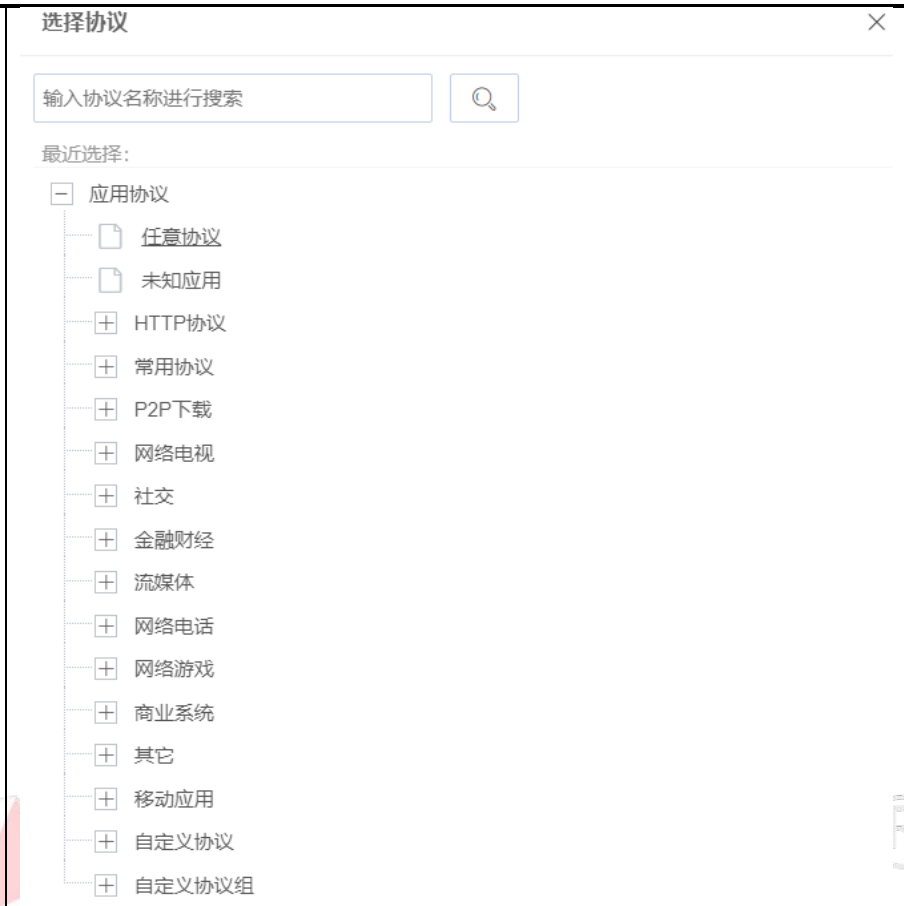
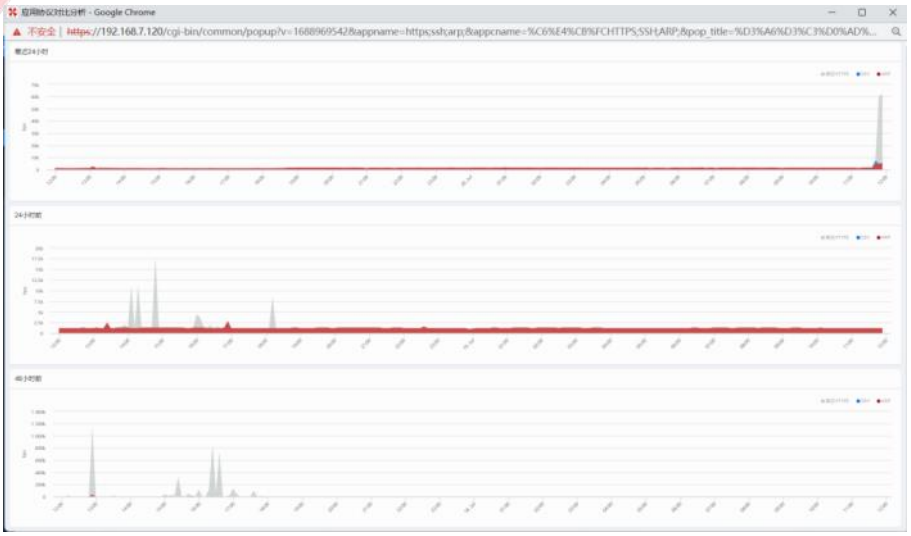
	
关键字搜索	根据 TOP 应用的关键字进行搜索。
选中应用对比分析	将选中的应用流量进行 24 小时内，24 小时前，48 小时前的趋势对比。 

表 4-12 TOP 应用参数说明

4.2.5. TOP 连接

TOP 连接展示每个 IP 在线用户实时连接数，并可以为单个 IP 用户进行信息备注或画像。

步骤 1 选择【流量概况】>【在线用户】。

步骤 2 选择页面上方的【TOP 连接】。

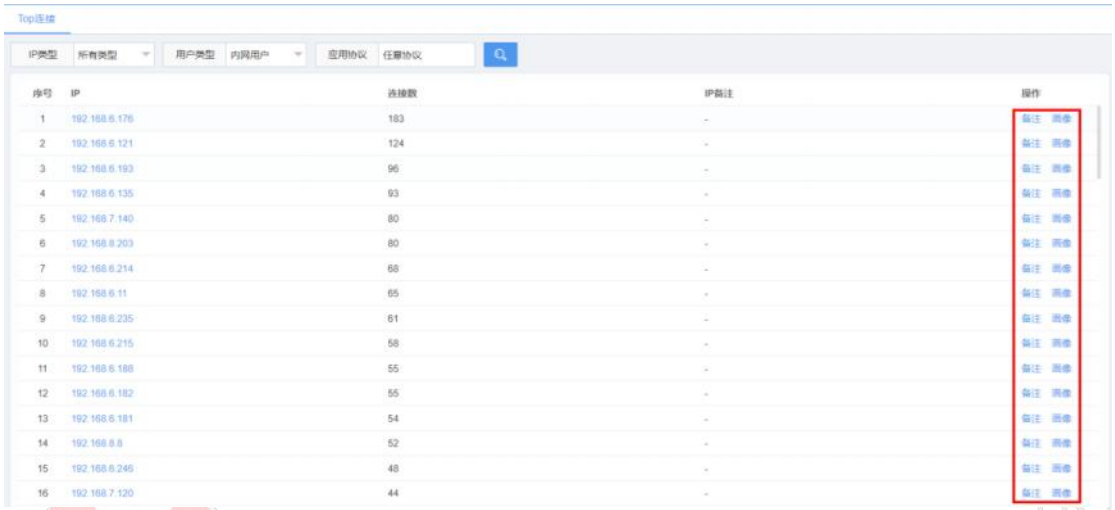
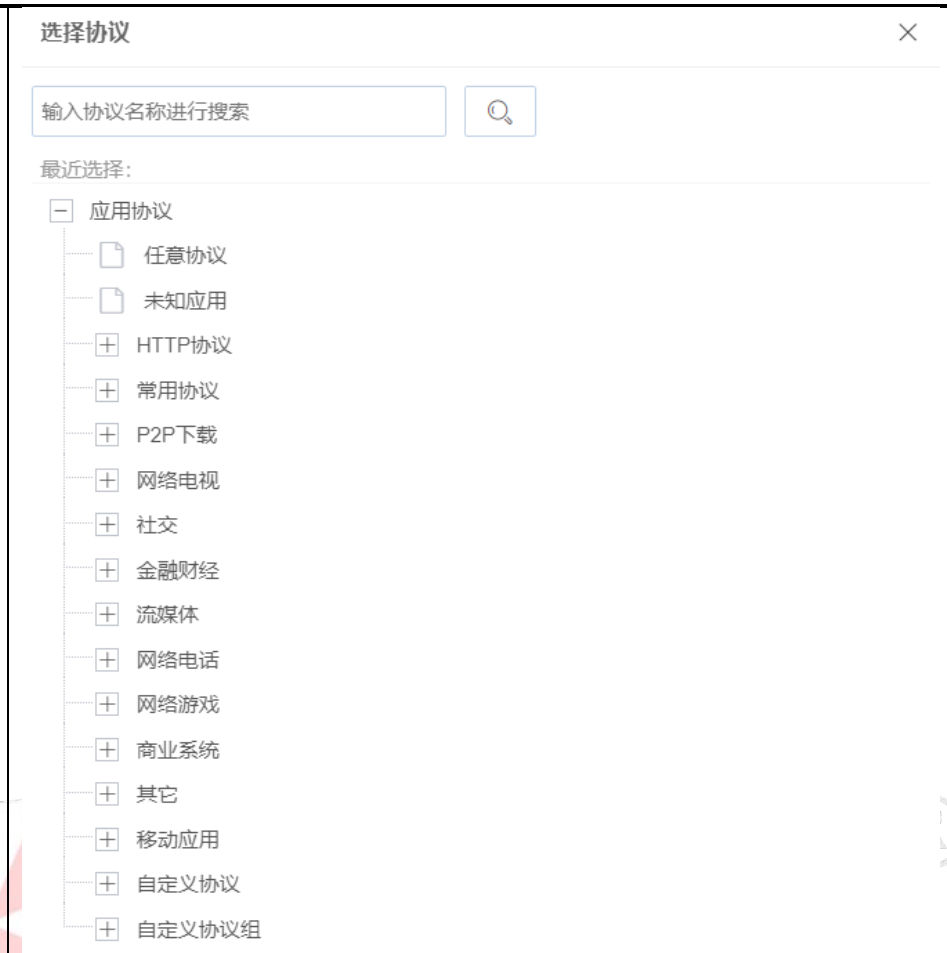


图 4-12 TOP 连接详情

参数名称	参数说明
IP 类型	可根据 IPv4 或 IPv6 筛选。
用户类型	可根据内网或外网筛选。
应用协议	可根据选择的应用协议来筛选有相关连接的 IP 用户。

	
IP 备注	单击【备注】，可对单 IP 添加备注信息，支持数字，字母，中文以及特殊字符。 
画像	单击【画像】，可查看该 IP 用户访问行为详情，详见 IP 画像。

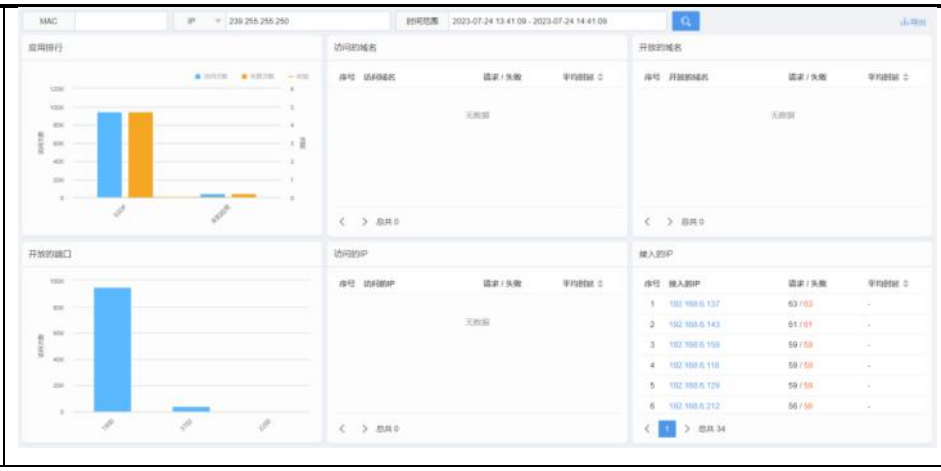


表 4-13 TOP 连接参数说明

4.2.6. 域名概况

域名概况主要对被请求的域名进行统计与展示，并精细化展示域名请求结果。

4.2.6.1. 实时请求

实时请求页面展示了实时域名请求的 IP、位置、最后访问时间、次数、结果等信息。

步骤 1 选择【流量概况】>【域名概况】。

步骤 2 选择页面上方的【实时请求】。

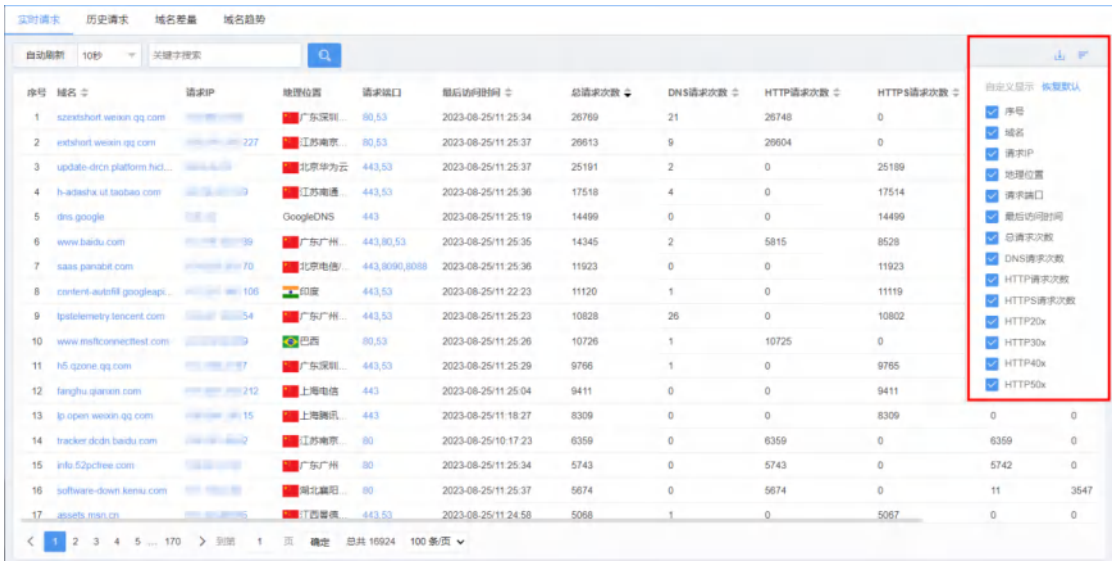


图 4-13 实时请求详情

参数名称	参数说明
自动刷新	域名请求统计结果刷新时间，可选择不刷新或以 5s/10s/20s/30s/60s 为周

	期刷新。
关键字搜索	域名统计中的关键字。
自定义显示	鼠标悬停或单击 后，勾选需要在列表中呈现的域名信息。 **说明** HTTP 20X：HTTP 状态码 200-209，用于表示域名请求成功。 HTTP 30X：HTTP 状态码 300-309，用于已经移动的文件并且常被包含在定位头信息中指定新的地址信息。 HTTP 40X：HTTP 状态码 400-409，用于指出客户端的错误。 HTTP 50X：HTTP 状态码 500-509，用于指出服务器错误。
导出	将统计结果或筛选后的统计结果导出。

表 4-14 实时请求参数说明

4.2.6.2. 历史请求

历史请求页面展示了历史域名请求的 IP、位置、次数、结果等信息。

步骤 1 选择【流量概况】>【域名概况】。

步骤 2 选择页面上方的【历史请求】。

图 4-14 历史请求详情

参数名称	参数说明
源 IP	发出请求报文的源 IP。
源端口	发出请求报文的源端口号。
目标 IP	发出请求报文的目标 IP。
目标端口	发出请求报文的目标端口号。
请求域名	被请求的目标域。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。

时间范围	根据时间范围搜索相应域名请求。
自定义显示	鼠标悬停或点击 后，可勾选需要在列表中呈现的域名信息。
导出	将统计结果或筛选后的统计结果导出到本地。

表 4-15 历史请求参数说明

4.2.6.3. 域名差量

域名差量可以同时查询和展示在指定的两个时间段内，指定条件的域名访问，并且计算出每个域名在两个时间段间的访问差量。

步骤 1 选择【流量概况】>【域名概况】。

步骤 2 选择页面上方的【域名差量】。

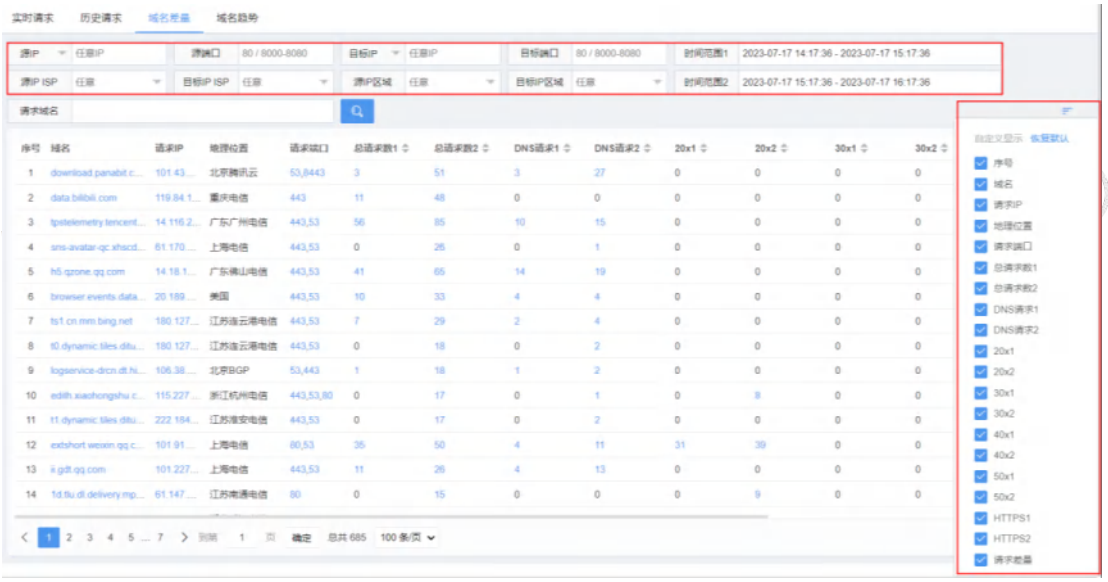


图 4-15 域名差量详情

参数名称	参数说明
单个 IP	发出请求报文的源 IP。
源端口	发出请求报文的源端口号。
目标 IP	发出请求报文的目标 IP。
目标端口	发出请求报文的目标端口号。
请求域名	被请求的目标域名。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商。
时间范围 1	时间范围搜索相应域名请求显示为总请求数 1。
时间范围 2	根据时间范围搜索相应域名请求显示为总请求数 2。

自定义显示	鼠标悬停或单击 后，可勾选需要在列表中呈现的域名信息。

表 4-16 域名差量参数说明

4.2.6.4. 域名趋势

域名趋势可以按照既定条件筛选活跃域名数及域名请求数。

步骤 1 选择【流量概况】>【域名概况】。

步骤 2 选择页面上方的【域名趋势】。

图 4-16 域名趋势详情

参数名称	参数说明
单个 IP	发出请求报文的源 IP。
源端口	发出请求报文的源端口号。
目标 IP	发出请求报文的目标 IP。
目标端口	发出请求报文的目标端口号。
请求域名	被请求的目标域名。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
时间范围	根据时间范围搜索相应域名请求。

表 4-17 域名趋势参数说明

4.2.7. 应用商店

Panabit 应用商店模块提供 APP 功能扩展平台，当用户需要这些特定功能时，通过下载和安装应用商店的 APP，来获取相关功能设置界面。APP 不使用时也可卸载。

Panabit 应用商店 APP 下载地址：https://www.panabit.com/download 。

应用商店内的各类 APP，参见应用商店 APP。

4.2.7.1. 我的应用

在【我的应用】页面能查看已安装的应用，并能对应用执行“启用”、“禁用”、“删除”等操作。

步骤 1 选择【流量概况】>【应用商店】。

步骤 2 选择页面上方的【我的应用】。

图 4-17 我的应用详情

参数名称	参数说明
排序方式	可根据“APP 名称”、“APP 版本”、“使用次数”对已安装 APP 进行排序。
APP 类型	可根据“网络接入”、“网络管理”、“运维工具”、“第三方接口”、“默认分类”筛选已安装的 APP。
APP 状态	可根据“启用”、“禁用”、“可更新”等状态筛选已安装的 APP。
关键词搜索	通过关键词搜索已安装的 APP。
启用/禁用	单击 启用，可“启用”或“禁用”当前 APP
删除	单击，可删除已安装的 APP
安装升级	单击 安装升级，可将下载到本地的 APP 进行上传安装、升级。

表 4-18 我的应用参数说明

4.2.7.2. 应用商店

通过应用商店可查看所有应用的版本号及状态，并能对应用执行“安装”、“打开”、“重装”等操作。

步骤 1 选择【流量概况】>【应用商店】。

步骤 2 选择页面上方的【应用商店】。

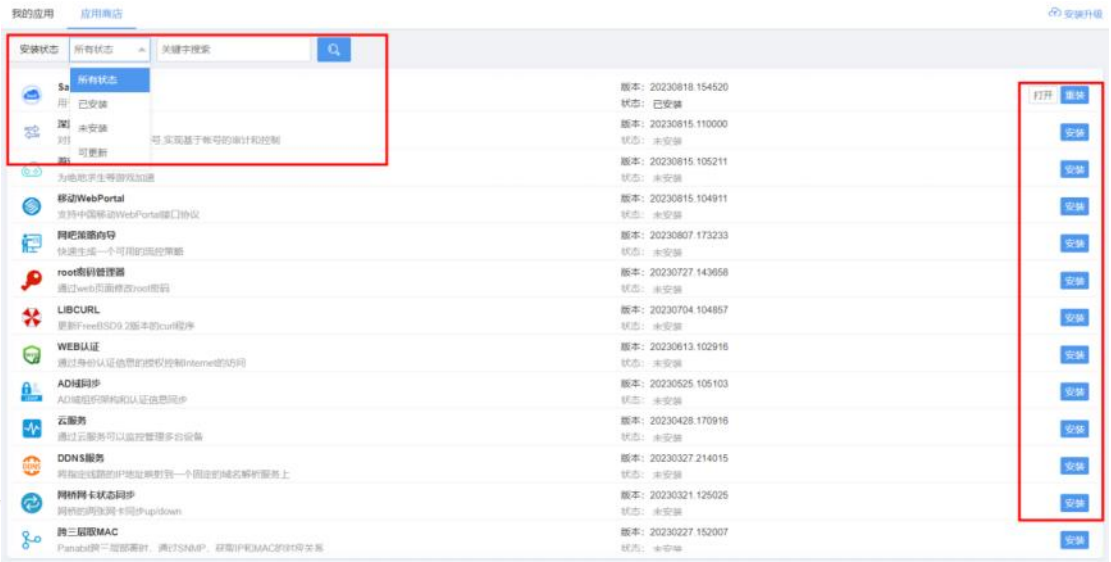


图 4-18 应用商店详情

4.2.8. 态势大屏

态势大屏是以应用协议为维度，实时展示应用的信息。

步骤 1 选择【流量概况】>【态势大屏】。

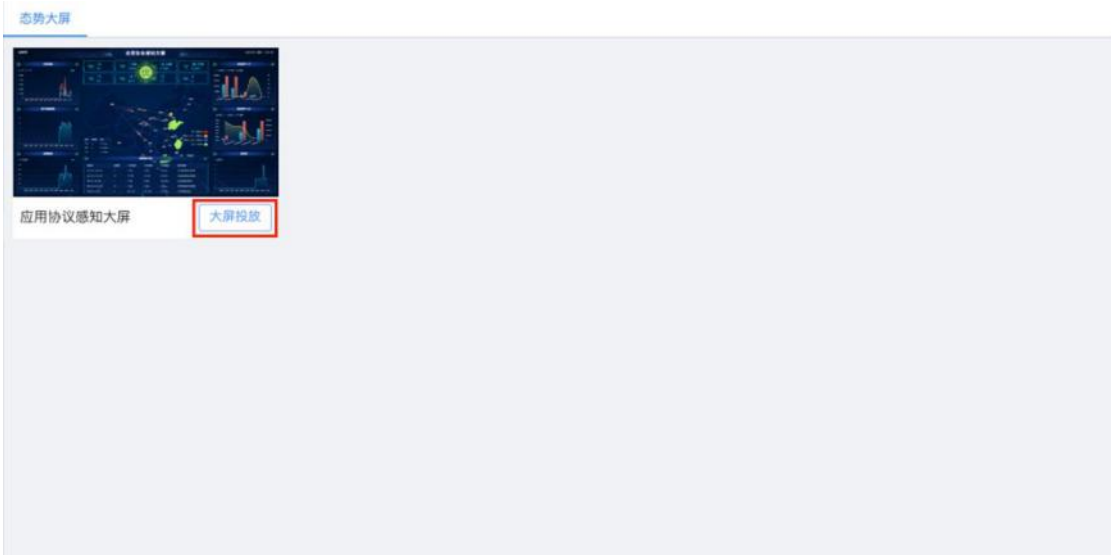


图 4-19 态势大屏详情

图 4-20 态势大屏主界面

说明

1. 地图省份区域为目标 IP 所在地。
2. 区域颜色根据平均时延情况分为四种：

- 绿色（优）：<=200ms
- 蓝色（良）：200ms-800ms
- 橙色（中）：800ms-2000ms
- 红色（差）：>2000ms

3. 点击区域可设置中心点，即设备所在地，中心点圆圈大小根据连接数变化而变化。
4. 地图上动态箭头为流量传输过程，箭头指向方向为目标 IP 所在地。

参数名称	参数说明
协议类型	支持对指定应用协议监控，上图中指定为“钉钉”。
应用流量	该应用协议当前速率，折线图展示十分钟内某一时间点的速率，单位：分:秒。
质量趋势	该应用协议当前平均时延，折线图展示十分钟内某一时间点的平均时延，横坐标为时间点，单位：分:秒，纵坐标为时延大小，单位：ms。
重传率	该应用协议当前重传包比例，折线图展示十分钟内某一时间点的重传率，横坐标为时间点，单位：分:秒，纵坐标为重传率 ，单位：%。
服务端 IP	该应用所在服务器 IP 地址，地理位置有国旗展示。
用户在线数量	会话统计源 IP 数量，折线图展示十分钟内某一时间点的源 IP 数量，横坐标为时间点，单位：分/秒，纵坐标为用户在线数量。
访问用户	用户的上下行速率，点击后按总速率大小从高到低排序，柱状图展示十分钟内某一时间点的源 IP 的上下行速率大小，横坐标为源 IP，纵坐标为速率，单位：bps。
质差用户	用户平均时延情况，柱状图为上下行流量大小，折线为平均时延，点击后按时延从高到低排列，横坐标为源 IP，纵坐标左侧为平均时延，单位：ms，右侧为上下行流量大小，单位：Byte。
源 IP 数	等同于“用户在线数量”。
连接数	当前总连接数。
上行/下行速率	等同于“应用流量”。
目标 IP 数	服务器 IP 个数。
关联域名数	点击可查看访问目标 IP 地址关联的域名。
目标端口数	所有服务器绑定的端口数，点击可显示具体端口号。
平均时延	等同于“质量趋势”。

表 4-19 应用协议感知大屏参数说明

4.3. 安全态势

安全态势能够为用户提供综合性的安全状况评估，包括威胁情报、主机监控和敏感应用等模块，用户可以快速发现网络中可能存在的威胁与隐患，确保网络的安全性。

4.3.1. 威胁情报

威胁情报呈现情报的命中趋势及类型，让客户了解网络中的潜在风险。

4.3.1.1. 情报概况

情报概况页面展示了各类威胁情报的命中情况，以及命中的源目 IP 地址。

步骤 1 选择【安全态势】>【威胁情报】。

步骤 2 选择页面上方的【情报概况】。

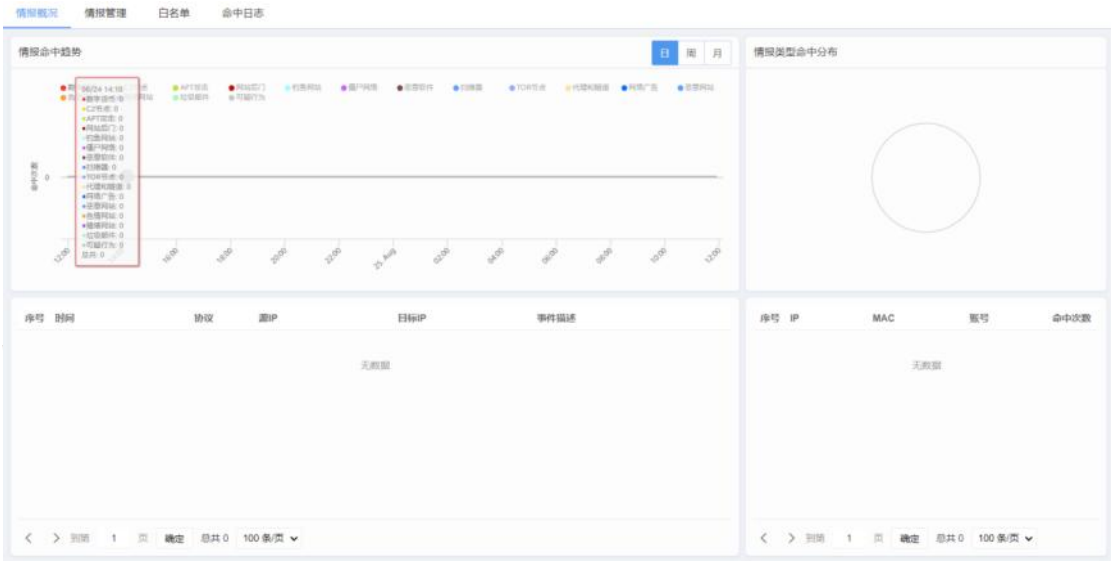


图 4-21 情报概况详情

参数名称	参数说明
筛选方式	可根据日/周/月搜索情报概况。 可根据威胁情报类型搜索相关情报。

表 4-20 情报概况参数说明

4.3.1.2. 情报管理

情报管理模块支持向 Panabit 官方威胁情报库自动同步情报类型，或手动导入情报类型，并能实现对情报类型的监测，阻断，日志记录。

步骤 1 选择【安全态势】>【威胁情报】。

步骤 2 选择页面上方的【情报管理】。

图 4-22 情报管理详情

参数名称	参数说明
自动刷新	情报命中情况刷新时间，可选择不刷新或以 5s/10s/20s/60s 为周期刷新。
关键字搜索	根据威胁情报类型关键字进行搜索。
监测	单击按钮 启用，开启对该类威胁情报的流量进行监测，关闭则禁用。
阻断	单击按钮 启用，开启对该类威胁情报的流量进行阻断，关闭则禁用。
记录日志	当会话命中威胁情报库时，会产生溯源日志信息。 单击按钮 启用，开启对该类威胁情报的日志记录，关闭则禁用。
类型说明	单击 ⓘ，可查看该情报类型的详细说明。 
手动导入	手动导入情报类型库文件。
自动同步	单击 ，开启自动同步，向 Panabit 官方情报库同步情报类型成员相关信息，关闭则不同步。

表 4-21 情报管理参数说明

4.3.1.3. 白名单

通过白名单功能，对指定 IP 或域名的流量不纳入威胁情报统计结果中，也不会进行阻断。

步骤 1 选择【安全态势】>【威胁情报】。

步骤 2 选择页面上方的【白名单】。

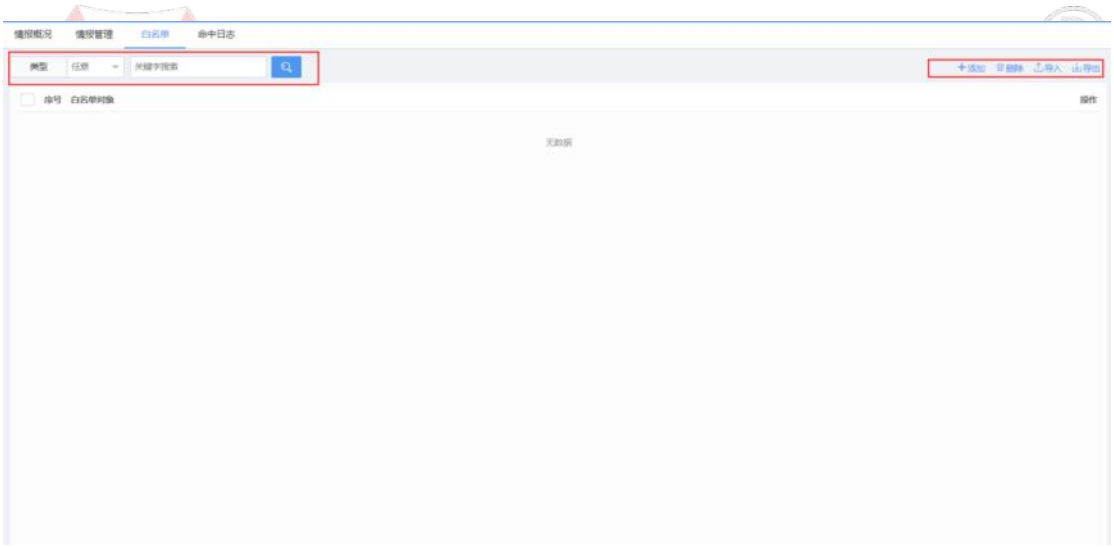


图 4-23 白名单详情

参数名称	参数说明
类型	根据 IP 或域名搜索相应白名单。
关键字搜索	可根据配置白名单的关键字搜索相应白名单。
添加	单击 +，添加白名单，格式 0.0.0.0 识别为 IP 地址，其他识别为域名。

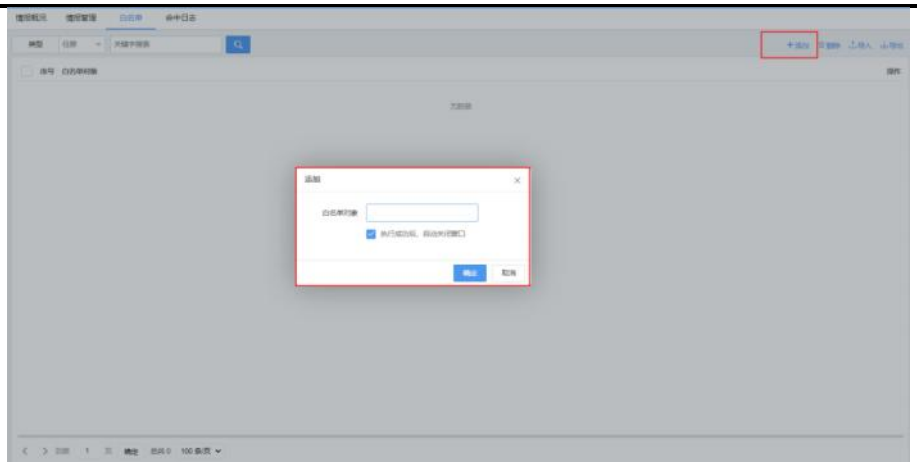
	
删除	删除选中的白名单。
导入	手动导入白名单文件。
导出	将配置好的白名单导出至本地。

表 4-22 白名单参数说明

4.3.1.4. 命中日志

命中日志页面主要展示命中威胁情报库的会话日志信息，包括源 IP、目标 IP、事件描述等。

步骤 1 选择【安全态势】>【威胁情报】。

步骤 2 选择页面上方的【命中日志】。

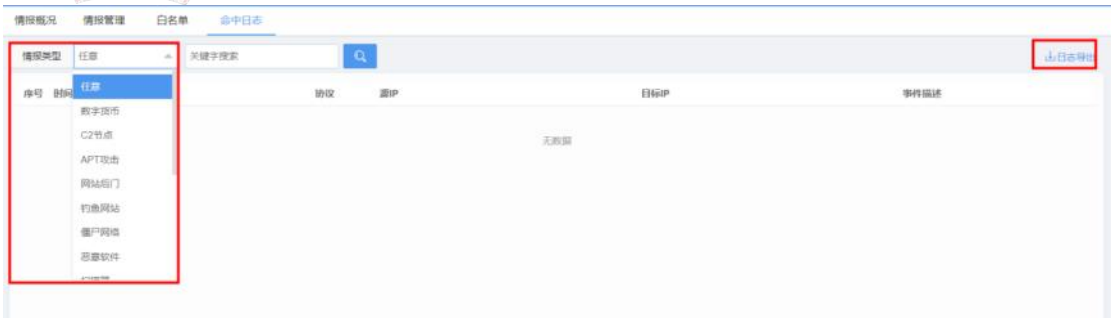


图 4-24 命中日志详情

参数名称	参数说明
情报类型	根据情报类型搜索相应日志。
关键字搜索	根据日志信息中的关键字搜索相应日志。
日志导出	将命中日志导出到本地。

表 4-23 命中日志参数说明

4.3.2. 主机监控

主机监控支持基于指定单个或多个 IP/域名进行监控，可监控用户连接数、PPS、连接失败率、平均时延信息、流入/流出速率、流入/流出流量等信息。

步骤 1 选择【安全态势】>【主机监控】。

图 4-25 主机监控详情

参数名称	参数说明
自动刷新	主机监控结果刷新频率，可选择不刷新或以 5s/10s/20s/60s 为周期刷新。
主机组	选择主机组并对组内 IP 用户进行监控。
关键字搜索	根据主机中的关键字搜索相应主机。
排序方式	根据需求排列卡片内容的先后顺序。 
添加	单击 +，添加主机主或主机，添加主机时需要先添加主机组，再选择主机组添加主机。主机组与主机名称，可使用数字，字母，中文，特殊符号等。 
导入	将本地配置好的主机监控信息导入设备。
导出	将设备配置好的主机监控信息导出到本地。
列表	主机监控信息以主机组，主机两级菜单列表展示。

	
分离	主机监控信息以主机组、主机分离展示。 
卡片	主机监控信息以卡片展示。 

表 4-24 主机监控参数说明

在【卡片】视图下，单击任意主机/主机组名称，可进入当前 IP 或域名（组）的详细数据视图，展示其流量、性能、协议、连接等详情页面。

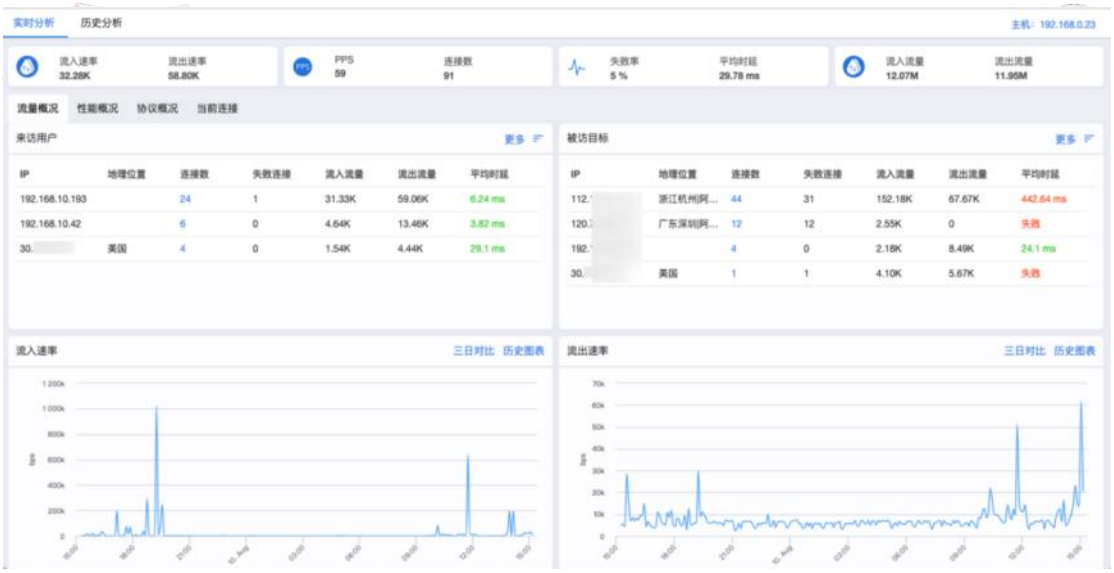


图 4-26 实时分析详情

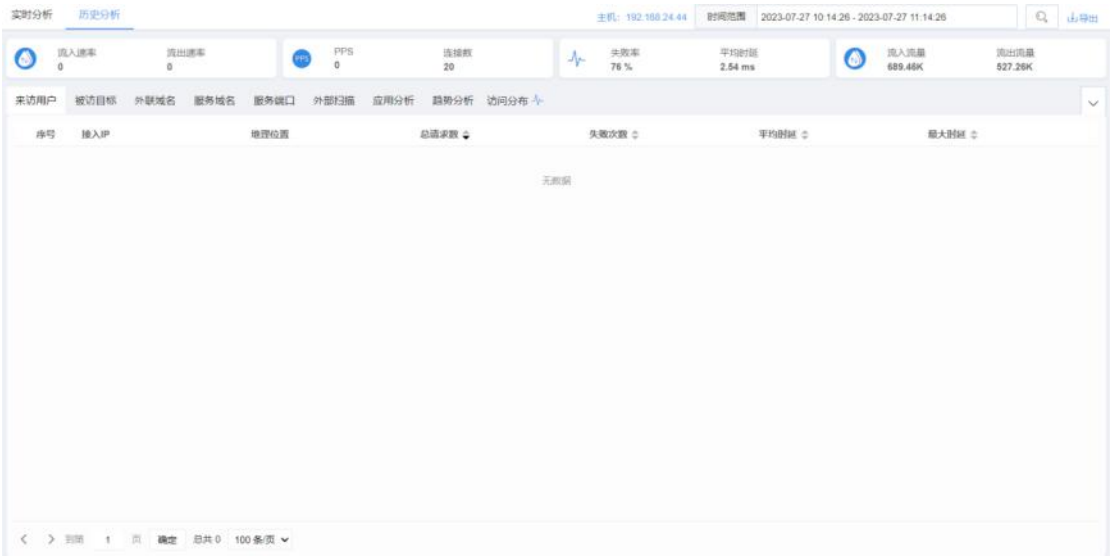
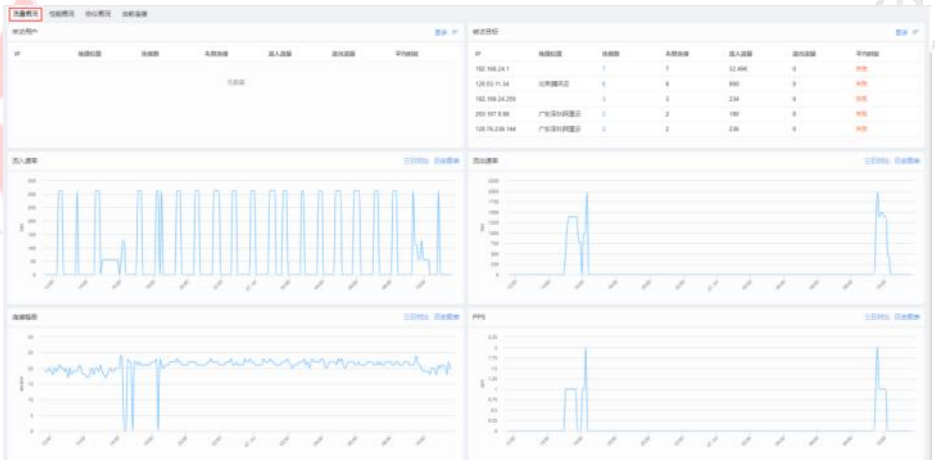


图 4-27 历史分析详情

参数名称	参数说明
流量概况	展示当前主机/主机组的流量和连接情况。包括来访用户、被访目标、流入/流出速率、连接数、PPS。 
性能概况	展示当前主机/主机组的整体时延详情。 

协议概况	展示当前主机/主机组的连接情况和流入/流出流量详情。 
当前连接	展示当前主机/主机组应用协议的实时连接详情。 
来访用户	访问此主机/主机组的接入 IP，地理位置、访问次数、时延等信息。
被访目标	此主机/主机组访问过的 IP 地址，地理位置、访问次数、时延等信息。
外联域名	此主机/主机组对外访问的域名请求详情及请求结果。
服务域名	访问主机/主机组的域名请求详情及请求结果。
服务端口	访问此主机/主机组的所有端口的访问次数、传输协议、应用协议、时延概况。
外部扫描	此主机/主机组访问过的端口 IP、次数、位置、时间。
趋势分析	此主机/主机组的连接趋势及时延趋势。
访问分布	访问此主机/主机组来源的中国及世界分布情况。

表 4-25 卡片视图参数说明

4.3.3. 敏感应用

敏感应用是对于网络会话中的 VPN 隧道或敏感协议进行监控统计，并对相应会话进行基本的解析诊断。

4.3.3.1. 实时概况

实时概况页面主要通过隧道类型和图表类型展示敏感流量的实时统计结果。

步骤 1 选择【安全态势】>【敏感应用】。

步骤 2 选择页面上方的【实时概况】。

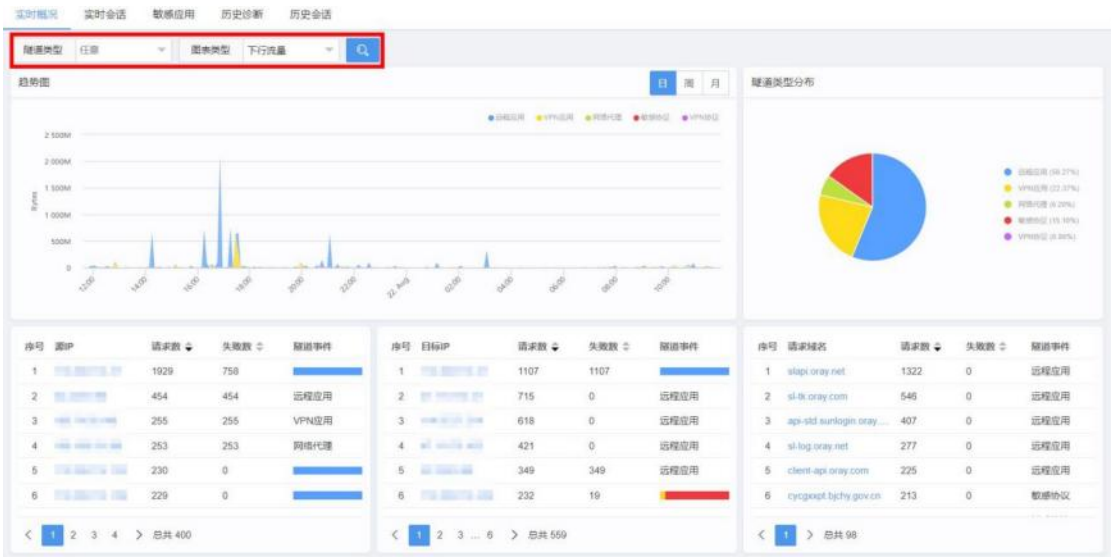


图 4-28 实时概况详情

参数名称	参数说明
隧道类型	根据隧道协议类型搜索相应敏感应用。
图表类型	根据上行、下行、连接数搜索相应敏感应用。

表 4-26 实时概况参数说明

4.3.3.2. 实时会话

实时会话页面主要展示命中敏感应用库的实时会话溯源结果，包括 IP、端口、域名、传输协议和隧道类型等信息。

步骤 1 选择【安全态势】>【敏感应用】。

步骤 2 选择页面上方【实时会话】。

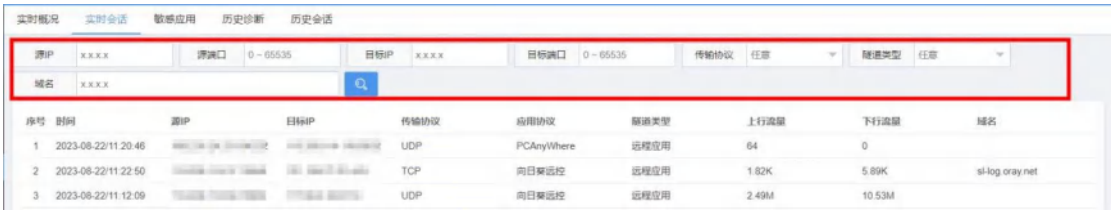


图 4-29 实时会话详情

参数名称	参数说明
源 IP	会话源 IP。
源端口	会话源端口。
目标 IP	会话目标 IP。
目标端口	会话目标端口。

传输协议	会话传输协议。
隧道类型	会话隧道类型。
域名	会话访问域名。

表 4-27 实时会话参数说明

4.3.3.3. 敏感应用

敏感应用页面可根据应用类型和时间范围展示应用的连接趋势、请求详情和时延概况。

步骤 1 选择【安全态势】>【敏感应用】。

步骤 2 选择页面上方【敏感应用】。

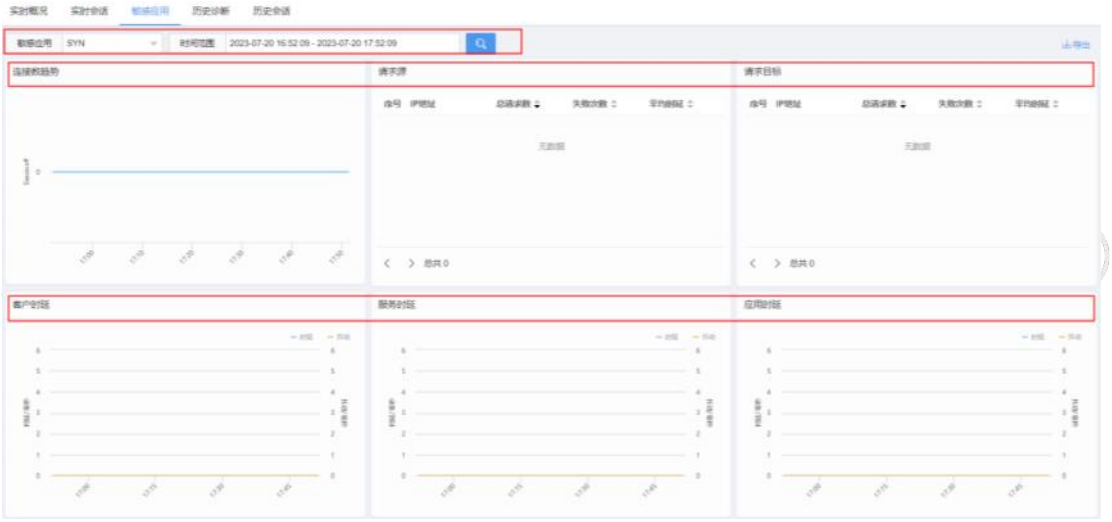


图 4-30 敏感应用详情

参数名称	参数说明
敏感应用	根据敏感应用类型搜索其连接数趋势、请求源信息、请求目标信息、客户时延、服务时延、应用时延。敏感应用包含如下类型： 
时间范围	根据任意时间段搜索其连接数趋势、请求源信息、请求目标信息、客户时延、服务时延、应用时延。

连接数趋势	该敏感应用的连接数趋势图。
请求源	该敏感应用的源地址列表，按照请求数排序。
请求目标	该敏感应用的目标地址列表，按照请求数排序。
客户时延	客户端至测量点的网络时延，客户时延过大表示内网环境延迟过大。
服务时延	测量点至服务器的网络时延，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，应用时延过大表示服务提供商提供服务的延迟过大。

表 4-28 敏感应用参数说明

4.3.3.4. 历史诊断

历史诊断页面主要展示对敏感应用的历史诊断信息，可基于既定条件进行筛选并导出筛选结果。

步骤 1 选择【安全态势】>【敏感应用】。

步骤 2 选择页面上方【历史诊断】。

图 4-31 历史诊断详情

参数名称	参数说明
MAC	会话源 MAC。
源 IP	会话源 IP。
源端口	会话源端口。
目标 IP	会话目标 IP。

目标端口	会话目标端口。
传输协议	会话传输协议。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
时间范围	会话产生的时间范围。
隧道类型	会话的隧道类型。
请求域名	会话的访问域名。
导出	支持将历史诊断信息导出到本地。

表 4-29 历史诊断参数说明

4.3.3.5. 历史会话

历史会话页面主要展示与敏感应用相关的会话信息，包含 IP、位置、协议、隧道、域名等信息。

步骤 1 选择【安全态势】>【敏感应用】。

步骤 2 选择页面上方【历史会话】。

图 4-32 历史会话详情

参数名称	参数说明
MAC	会话源 MAC。
源 IP	会话源 IP。
源端口	会话源端口。

目标 IP	会话目标 IP。
目标端口	会话目标端口。
传输协议	会话传输协议。
时间范围	会话产生的时间。
隧道类型	会话隧道类型。
请求域名	会话访问域名。
连接类型	连接结果的成功或失败。
条件关系	搜索条件之间的与/或/非关系。

表 4-30 历史会话参数说明

4.4. 行为审计

行为审计针对用户做出的浏览网页、收发邮件、文件传输、远程登录中产生的 HTTP、HTTPS、DNS、FTP、Telnet、IMAP、SMTP 等协议进行监控审计。

4.4.1. HTTP 审计

超文本传输协议（Hypertext Transfer Protocol，HTTP）是一个简单的请求——响应协议，它通常运行在 TCP 之上，指定了客户端发送给服务器的消息以及得到的响应，HTTP 审计是对经过设备的 HTTP 会话进行统计与日志留存。

4.4.1.1. HTTP 诊断

HTTP 诊断页面主要展示 HTTP 会话信息，可基于既定条件进行会话筛选并导出筛选结果。

步骤 1 选择【行为审计】>【HTTP 审计】。

步骤 2 选择页面上方的【HTTP 诊断】。

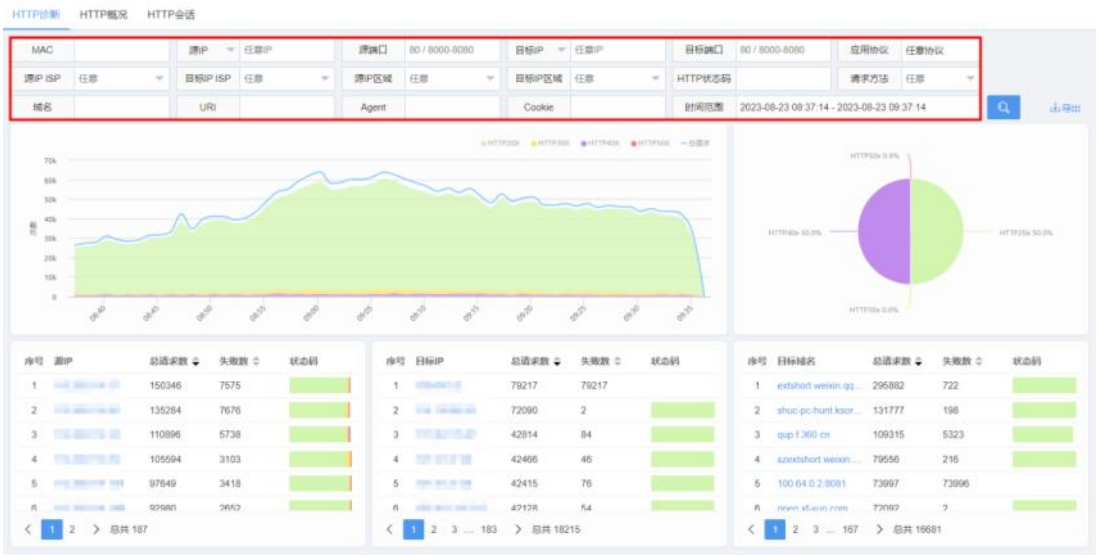


图 4-33 HTTP 诊断详情

参数名称	参数说明
MAC	HTTP 会话源 MAC。
源 IP	HTTP 会话源 IP。
源端口	HTTP 会话源端口。
目标 IP	HTTP 会话目标 IP。
目标端口	HTTP 会话目标端口。
应用协议	HTTP 会话基于应用协议。
源 IP ISP	发出请求报文源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
HTTP 状态码	HTTP 20X：HTTP 状态码 200-209，用于表示域名请求成功。 HTTP 30X：HTTP 状态码 300-309，用于已经移动的文件并且常被包含在定位头信息中指定新的地址信息。 HTTP 40X：HTTP 状态码 400-409，用于指出客户端的错误。 HTTP 50X：HTTP 状态码 500-509，用于指出服务器错误。
请求方法	get 方法是发送一个请求来取得服务器上的某一资源。 post 方法是向 URL 指定的资源提交数据或附加新的数据。
域名	会话请求访问的域名。
X-Forward	是用来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务器的客户端最原始的 IP 地址的 HTTP 请求头字段。

Agent	Agent 代理信息。
URL	会话中携带的 URL 信息。
Cookie	用于在 Web 浏览器和 Web 服务器之间传输数据的小型文本文件。TELNET
导出	支持将 HTTP 诊断结果导出到本地。

表 4-31 HTTP 诊断参数说明

4.4.1.2. HTTP 概况

HTTP 概况页面将产生 HTTP 请求会话的源 IP、目标 IP 按请求次数降序排名，并以柱状图展示。

步骤 1 选择【行为审计】>【HTTP 审计】。

步骤 2 选择页面上方的【HTTP 概况】。

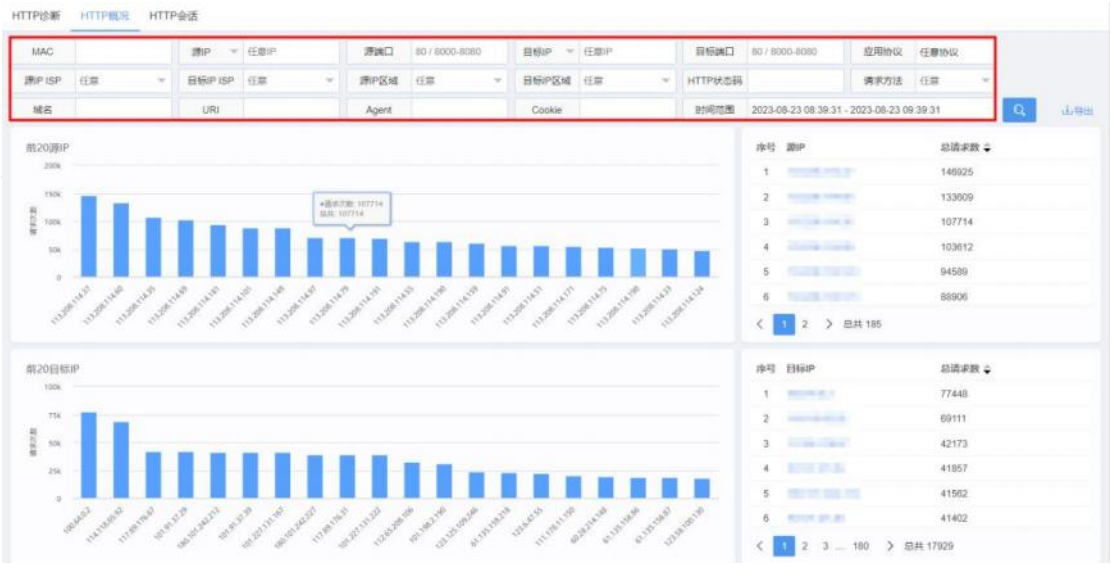


图 4-34 HTTP 概况详情

参数名称	参数说明
MAC	HTTP 会话源 MAC。
源 IP	HTTP 会话源 IP。
源端口	HTTP 会话源端口。
目标 IP	HTTP 会话目标 IP。
目标端口	HTTP 会话目标端口。
应用协议	HTTP 会话基于应用协议。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。

源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
HTTP 状态码	HTTP 20X：HTTP 状态码 200-299，用于表示域名请求成功。 HTTP 30X：HTTP 状态码 300-399，用于已经移动的文件并且常被包含在定位头信息中指定新的地址信息。 HTTP 40X：HTTP 状态码 400-499，用于指出客户端的错误。 HTTP 50X：HTTP 状态码 500-599，用于指出服务器错误。
请求方法	get 方法是发送一个请求来取得服务器上的某一资源。 post 方法是向 URL 指定的资源提交数据或附加新的数据。
域名	会话请求访问的域名。
X-Forward	是用来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务器的客户端最原始的 IP 地址的 HTTP 请求头字段。
Agent	Agent 代理信息。
URL	会话中携带的 URL 信息。
Cookie	用于在 Web 浏览器和 Web 服务器之间传输数据的小型文本文件
导出	支持将 HTTP 诊断结果导出到本地

表 4-32 HTTP 概况参数说明

4.4.1.3. HTTP 会话

HTTP 会话页面主要展示每条会话的时间、IP、位置、协议、请求方法及状态等信息，便于后续的审计和溯源。

步骤 1 选择【行为审计】>【HTTP 审计】。

步骤 2 选择页面上方【HTTP 会话】。

图 4-35 HTTP 会话详情

参数名称	参数说明

MAC	会话源 MAC 信息。
源 IP	会话源 IP 信息。
源端口	会话源端口信息。
目标 IP	会话目标 IP 信息。
目标端口	会话目标端口信息。
应用协议	会话相关应用协议信息。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
HTTP 状态码	HTTP 20X：HTTP 状态码 200-209，用于表示域名请求成功。 HTTP 30X：HTTP 状态码 300-309，用于已经移动的文件并且常被包含在定位头信息中指定新的地址信息。 HTTP 40X：HTTP 状态码 400-409，用于指出客户端的错误。 HTTP 50X：HTTP 状态码 500-509，用于指出服务器错误。
请求方法	get 方法是发送一个请求来取得服务器上的某一资源。 post 方法是向 url 指定的资源提交数据或附加新的数据。
域名	会话请求访问的域名。
X-Forward	是用来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务器的客户端最原始的 IP 地址的 HTTP 请求头字段。
Agent	Agent 代理信息。
URI	会话中携带的 URI 信息。
Cookie	用于在 Web 浏览器和 Web 服务器之间传输数据的小型文本文件。
导出	支持将 HTTP 会话条目结果导出到本地。

表 4-33 HTTP 会话参数说明

4.4.2. HTTPS 审计

HTTPS 审计是对经过设备的 HTTPS 会话进行统计与日志留存。HTTPS（全称：Hypertext Transfer Protocol Secure），是以安全为目标的 HTTP 通道，在 HTTP 的基础上通过传输加密和身份认证保证了传输过程的安全性。

4.4.2.1. HTTPS 诊断

HTTPS 诊断页面主要展示 HTTPS 会话的诊断结果，包含流量情况和请求详情可基于多种条件进行会话筛选。

步骤 1 选择【行为审计】>【HTTPS 审计】。

步骤 2 选择页面上方的【HTTPS 诊断】。

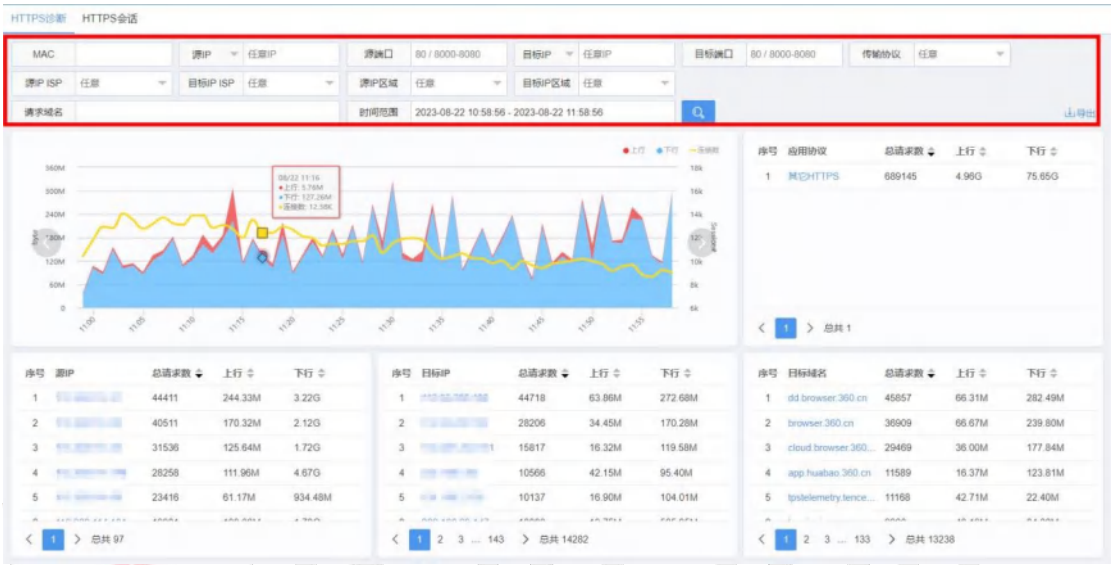


图 4-36 HTTP 诊断详情

参数名称	参数说明
MAC	HTTPS 会话源 MAC。
源 IP	HTTPS 会话源 IP。
源端口	HTTPS 会话源端口。
目标 IP	HTTPS 会话目标 IP。
目标端口	HTTPS 会话目标端口。
传输协议	HTTPS 会话基于的传输协议。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
请求域名	会话请求访问的域名。
导出	HTTPS 诊断信息可导出到本地。

表 4-34 HTTPS 诊断参数说明

4.4.2.2. HTTPS 会话

HTTP 会话页面主要展示每条会话的时间、IP、位置、协议、时延、流量等信息，便于后续的审计和溯源。

步骤 1 选择【行为审计】>【HTTP 审计】。

步骤 2 选择页面上方的【HTTPS 会话】。

图 4-37 HTTP 会话详情

参数名称	参数说明
MAC	HTTPS 会话源 MAC。
源 IP	HTTPS 会话源 IP。
源端口	HTTPS 会话源端口。
目标 IP	HTTPS 会话目标 IP。
目标端口	HTTPS 会话目标端口。
传输协议	HTTPS 会话基于的传输协议。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
请求域名	请求访问的域名地址。
连接类型	会话连接结果，成功/失败。
条件关系	搜索条件之间的或/与/非关系。
上行字节	上行流量的字节数。
导出	HTTPS 诊断信息可导出到本地。

表 4-35 HTTPS 会话参数说明

4.4.3. DNS 审计

DNS 审计是对经过设备的 DNS 会话进行统计与日志留存。DNS 代表域名系统（Domain Name System），它将域名与 IP 地址相互映射，帮助我们使用易记的域名来访问网站。

4.4.3.1. DNS 诊断

DNS 诊断主要对 DNS 交互会话进行审计与溯源，并将相关会话的上/下行流量、连接数以可视化趋势图的方式展示。

步骤 1 选择【行为审计】>【DNS 审计】。

步骤 2 选择页面上方的【DNS 诊断】。

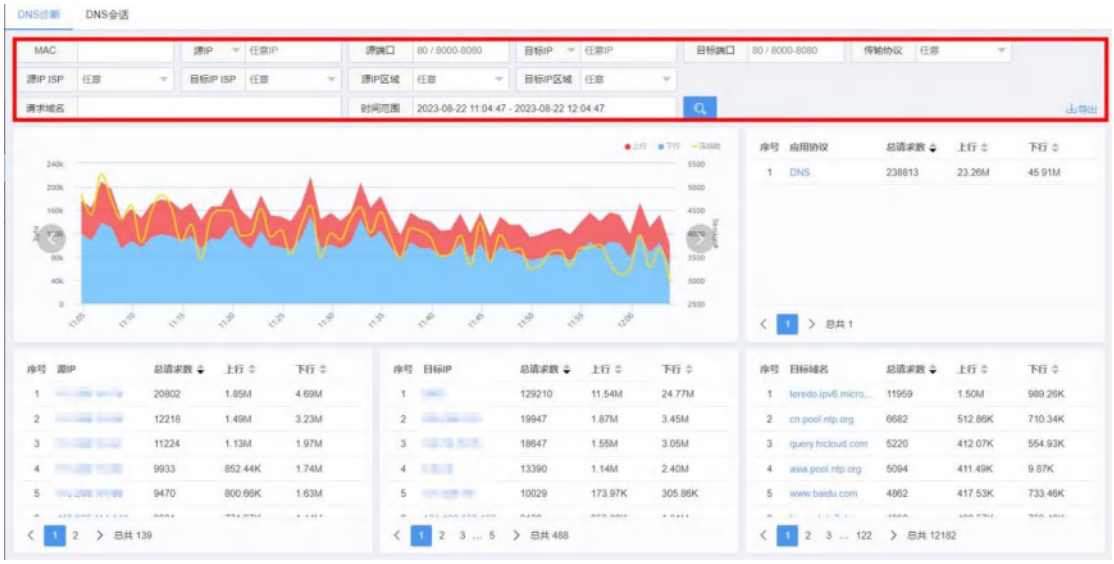


图 4-38 DNS 诊断详情

参数名称	参数说明
MAC	DNS 会话源 MAC。
源 IP	DNS 会话源 IP。
源端口	DNS 会话源端口。
目标 IP	DNS 会话目标 IP。
目标端口	DNS 会话目标端口。
传输协议	DNS 会话基于传输协议。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文的源 IP 的所在区域。

目标 IP 区域	发出请求报文的目标 IP 所在区域。
请求域名	请求访问的域名。
导出	支持将 DNS 会话诊断结果导出。

表 4-36 DNS 诊断参数说明

4.4.3.2. DNS 会话

DNS 会话页面主要展示每条会话的时间、IP、位置、协议、时延、流量等信息，便于后续的审计和溯源。

步骤 1 选择【行为审计】>【DNS 审计】。

步骤 2 选择页面上方【DNS 会话】。

图 4-39 DNS 会话详情

参数名称	参数说明
MAC	DNS 会话源 MAC。
源 IP	DNS 会话源 IP。
源端口	DNS 会话源端口。
目标 IP	DNS 会话目标 IP。
目标端口	DNS 会话目标端口。
传输协议	DNS 会话基于的传输协议。
请求域名	请求访问的域名。
连接类型	会话连接结果，成功/失败。
条件关系	搜索条件之间的或/与/非关系。
上行字节	上行流量的字节数。
导出	支持将 DNS 会话结果导出。

表 4-37 DNS 会话

4.4.4. FTP 审计

文件传输协议（File Transfer Protocol，FTP）是用于在网络上进行文件传输的一套标准协议，FTP 审计是对经过设备的 FTP 会话进行统计与日志留存。

4.4.4.1. 实时查询

实时查询页面主要展示 FTP 实时会话信息，包含 MAC，IP、端口号，使用用户名，下载动作与下载文件名等信息。

步骤 1 选择【行为审计】>【FTP 审计】。

步骤 2 选择页面上方的【实时查询】。

图 4-40 实时查询详情

参数名称	参数说明
MAC	FTP 发起方 MAC 地址。
IP	FTP 会话源 IP 或目标 IP。
用户名	进行 FTP 动作时使用的用户名。
FTP 动作	使用 FTP 进行的操作，包括 UNKN、STOR、RETR、DELE、RMD、RNFR、RNTO。
附件名称	使用 FTP 操作的对象文件。

表 4-38 实时查询参数说明

4.4.4.2. FTP 概况

FTP 概况页面将产生 FTP 请求会话的源 IP、目标 IP 按请求次数降序排名，并以柱状图展

示。

步骤 1 选择【行为审计】>【FTP 审计】。

步骤 2 选择页面上方的【FTP 概况】。

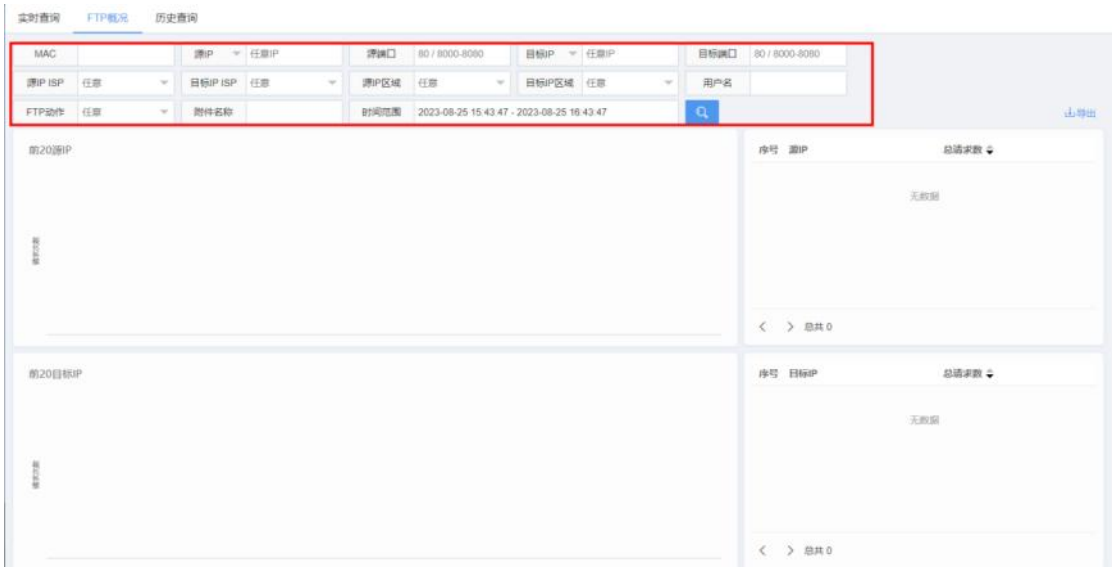


图 4-41 FTP 概况详情

参数名称	参数说明
MAC	FTP 会话源 MAC。
源 IP	FTP 会话源 IP。
源端口	FTP 会话源端口。
目标 IP	FTP 会话目标 IP。
目标端口	FTP 会话目标端口。
应用协议	FTP 会话基于传输协议。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
用户名	进行 FTP 动作时使用的用户名。
FTP 动作	使用 FTP 进行的操作，包括 UNKN、STOR、RETR、DELE、RMD、RNFR、RNTO。
附件名称	使用 FTP 操作的对象文件。

表 4-39 FTP 概况参数说明

4.4.4.3. 历史查询

历史查询主要展示 FTP 会话的历史日志审计信息，包含 MAC、IP、用户名和 FTP 动作等信息。

步骤 1 选择【行为审计】>【FTP 审计】。

步骤 2 选择页面上方的【历史查询】。

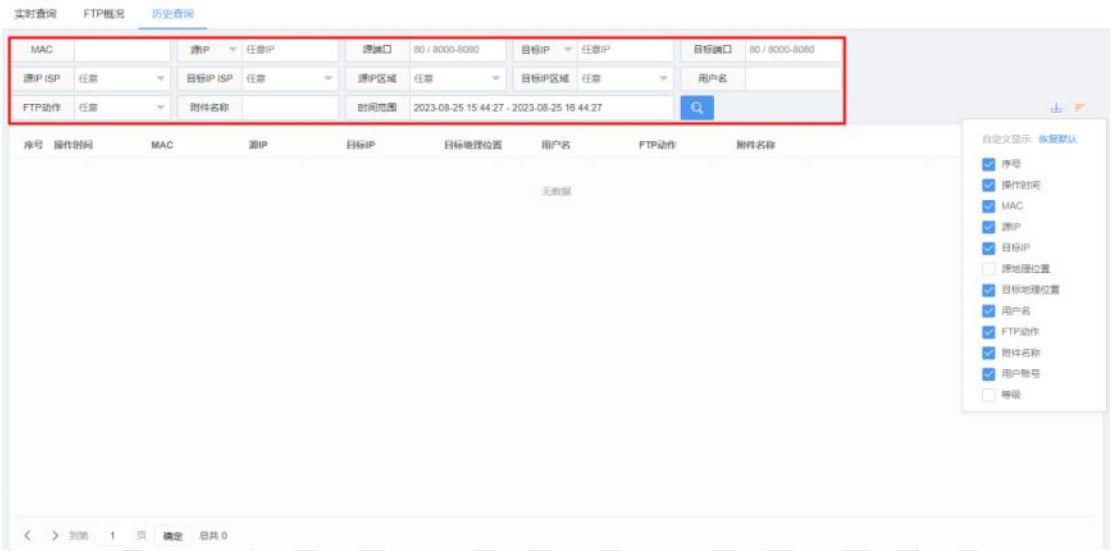


图 4-42 历史查询详情

参数名称	参数说明
MAC	FTP 会话源 MAC。
源 IP	FTP 会话源 IP。
源端口	FTP 会话源端口。
目标 IP	FTP 会话目标 IP。
目标端口	FTP 会话目标端口。
应用协议	FTP 会话基于传输协议。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
用户名	进行 FTP 动作时使用的用户名。
FTP 动作	使用 FTP 进行的操作，包括 UNKN、STOR、RETR、DELE、RMD、RNFR、RNTO。
附件名称	使用 FTP 操作的对象文件

表 4-40 历史查询参数说明

4.4.5. Telnet 审计

Telnet 是 Internet 远程登录服务的标准协议和主要方式，Telnet 审计是对经过设备的 Telnet 会话进行统计与日志留存。

4.4.5.1. 实时查询

实时查询页面主要展示实时 Telnet 会话信息，包含 MAC、IP、端口号、使用用户名、执行命令和操作时间等信息。

步骤 1 选择【行为审计】>【Telnet 审计】。

步骤 2 选择页面上方的【实时查询】。

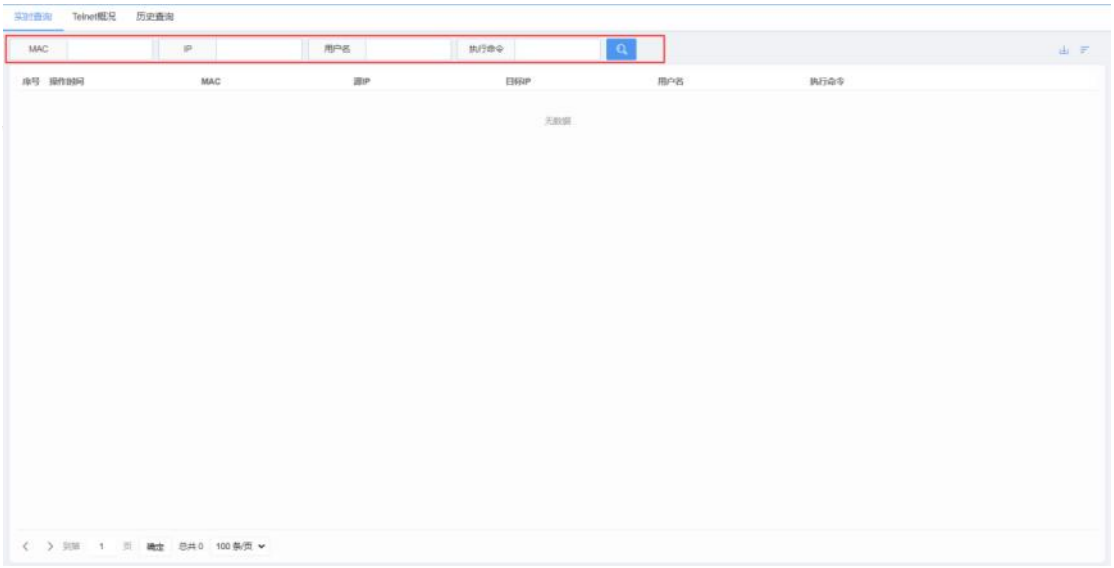


图 4-43 实时查询详情

参数名称	参数说明
MAC	Telnet 发起方 MAC 地址。
IP	Telnet 会话源 IP 或目标 IP。
用户名	进行 Telnet 远程登录使用的用户名。
执行命令	登录设备后执行的操作命令，如 ps/do/ls 等。

表 4-41 实时查询参数说明

4.4.5.2. Telnet 概况

Telnet 概况页面将产生 Telnet 请求会话的源 IP、目标 IP 按请求次数降序排名，并以柱状图展示。

步骤 1 选择【行为审计】>【Telnet 审计】。

步骤 2 选择页面上方的【Telnet 概况】。

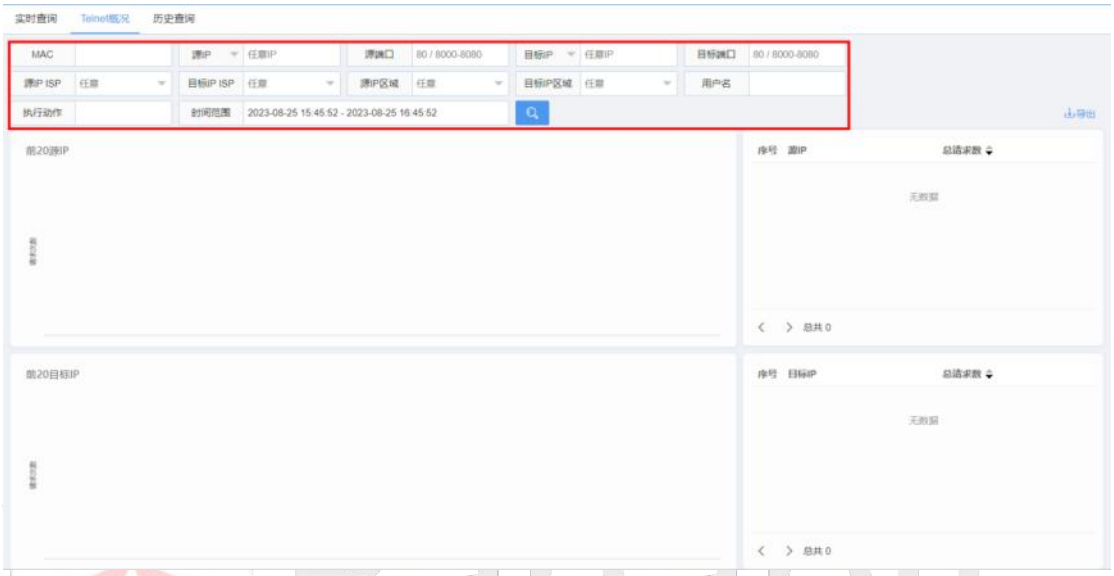


图 4-44 Telnet 概况详情

参数名称	参数说明
MAC	Telnet 会话源 MAC。
源 IP	Telnet 会话源 IP。
源端口	Telnet 会话源端口。
目标 IP	Telnet 会话目标 IP。
目标端口	Telnet 会话目标端口。
应用协议	Telnet 会话基于传输协议。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
用户名	进行 Telnet 远程登录使用的用户名。
执行动作	登录设备后执行的操作命令，如 spy/df/ls 等。

表 4-42 Telnet 概况参数说明

4.4.5.3. 历史查询

历史查询主要展示 Telnet 会话的历史日志审计信息，包含 MAC、IP、用户名和执行命令等信息。

步骤 1 选择【行为审计】>【Telnet 审计】。

步骤 2 选择页面上方的【历史查询】。

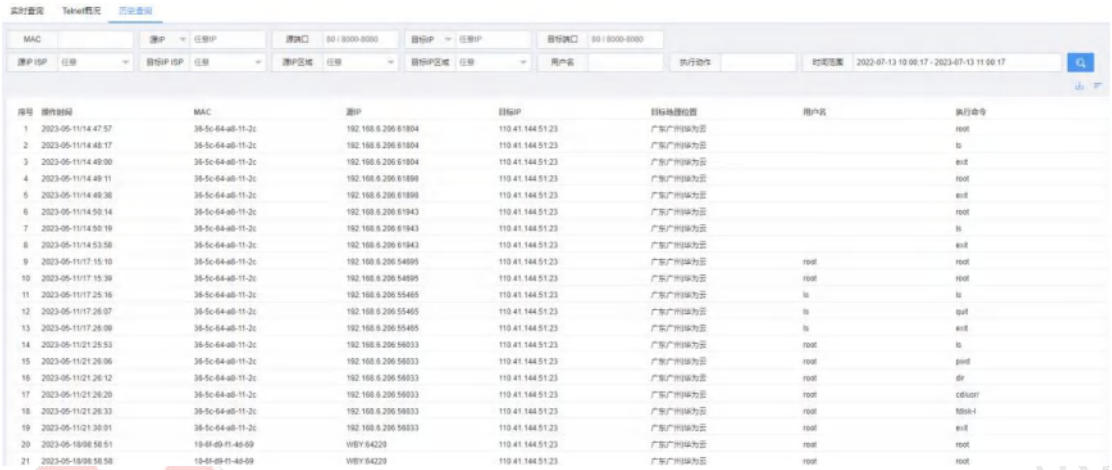


图 4-45 历史查询详情

参数名称	参数说明
MAC	Telnet 会话源 MAC。
源 IP	Telnet 会话源 IP。
源端口	Telnet 会话源端口。
目标 IP	Telnet 会话目标 IP。
目标端口	Telnet 会话目标端口。
应用协议	Telnet 会话基于传输协议。
源 IP ISP	发出请求报文的源 IP 的 ISP 运营商名称。
目标 IP ISP	发出请求报文的目标 IP 的 ISP 运营商名称。
源 IP 区域	发出请求报文的源 IP 的所在区域。
目标 IP 区域	发出请求报文的目标 IP 所在区域。
用户名	进行 Telnet 远程登录使用的用户名。
执行动作	登录设备后执行的操作命令，如 ps/df/ls 等。

表 4-43 历史查询参数说明

4.4.6. 邮件审计

邮件审计是对常用邮件协议，如 SMTP、POP3、IMAP 等进行审计与日志留存。

4.4.6.1. 实时查询

实时查询页面主要展示实时邮件会话信息，包含 MAC、IP、使用邮件协议，邮件摘要信息。

步骤 1 选择【行为审计】>【邮件审计】。

步骤 2 选择页面上方【历史查询】。

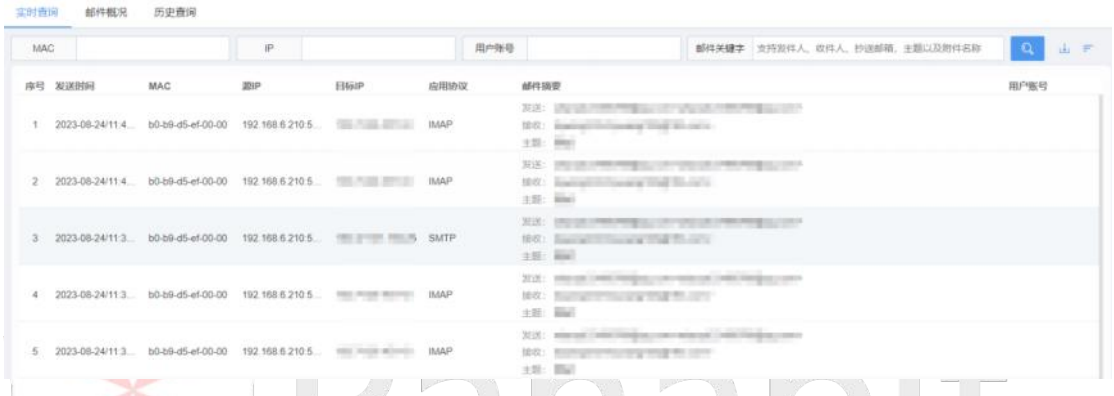


图 4-46 实时查询详情

参数名称	参数说明
MAC	邮件发起方 MAC 地址。
IP	邮件会话源 IP 或目标 IP。
邮件关键字	发件人、收件人、抄送邮箱、主题以及附件内容。

表 4-44 实时查询参数说明

4.4.6.2. 邮件概况

邮件概况页面将产生邮件会话的源 IP、目标 IP 按请求次数降序排名，并以柱状图展示。

步骤 1 选择【行为审计】>【邮件审计】。

步骤 2 选择页面上方【邮件概况】。

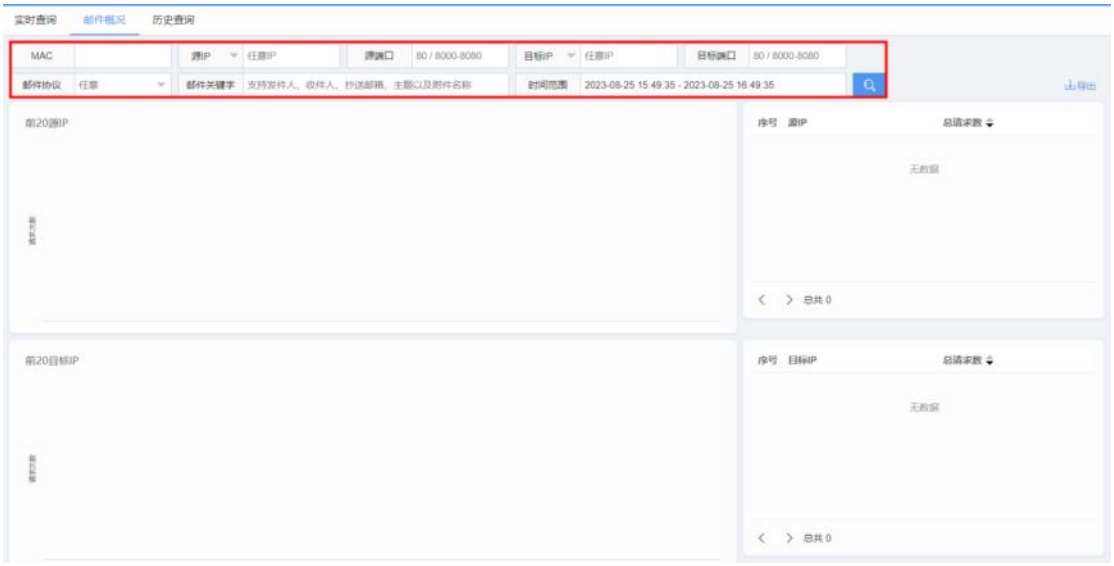


图 4-47 邮件概况详情

参数名称	参数说明
MAC	邮件会话源 MAC。
源 IP	邮件会话源 IP。
源端口	邮件会话源端口。
目标 IP	邮件会话目标 IP。
目标端口	邮件会话目标端口。
邮件协议	支持 SMTP、POP3、IMAP 三种邮件协议。
邮件关键字	发件人、收件人、抄送邮箱、主题以及附件内容。

表 4-45 邮件概况参数说明

4.4.6.3. 历史查询

历史查询主要展示邮件会话的历史日志审计信息，包含 MAC、IP、协议、邮件摘要等信息。

步骤 1 选择【行为审计】>【邮件审计】。

步骤 2 选择页面上方的【历史查询】。

图 4-48 历史查询详情

参数名称	参数说明
MAC	邮件会话源 MAC。
源 IP	邮件会话源 IP。
源端口	邮件会话源端口。
目标 IP	邮件会话目标 IP。
目标端口	邮件会话目标端口。
邮件协议	支持 SMTP、POP3、IMAP 三种邮件协议。
邮件关键字	发件人、收件人、抄送邮箱、主题以及附件内容。

表 4-46 历史查询参数说明

4.4.7. 用户认证

用户认证主要展示当前设备用户登录、登出的实时概况和认证日志。

4.4.7.1. 实时概况

实时概况展示当前设备的总登录/登出数、最近的登录/登出数及最近三天、最近一月的登录/登出趋势。

步骤 1 选择【行为审计】>【用户认证】。

步骤 2 选择页面上方的【实时概况】。

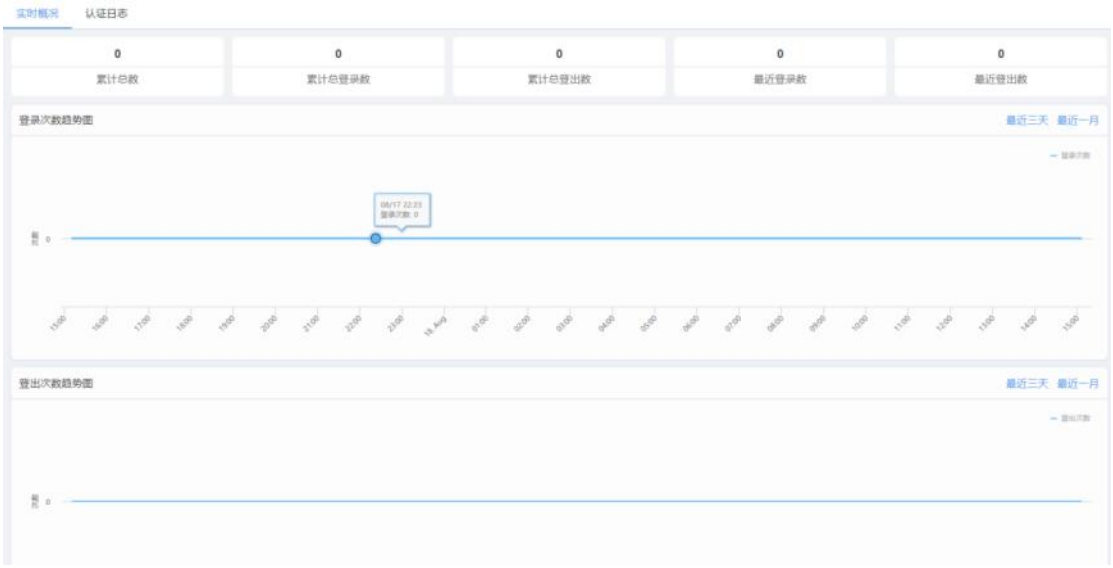


图 4-49 实时概况详情

4.4.7.2. 认证日志

认证日志展示用户的登录地址、MAC、账号、类型及操作时间。

步骤 1 选择【行为审计】>【用户认证】。

步骤 2 选择页面上方的【认证日志】。

图 4-50 认证日志详情

参数名称	参数说明
账号	用户登录设备的账号。
MAC	用户登录设备的 MAC。
日志类型	可选择“任意”、“登录”、“退出”。
用户 IP	用户登录设备的 IP。

表 4-47 认证日志参数说明

4.5. 协议质量

协议质量可以对各类应用协议的网络质量，包括时延、失败率等进行实时或历史的可视化

分析展示。

4.5.1. 质量概况

质量概况是基于源 IP 的时延分析，其结果以可视化趋势图与饼图方式呈现。

步骤 1 选择【协议质量】>【质量概况】。

图 4-51 实时分析详情

图 4-52 历史分析详情

参数名称	参数说明
实时分析	对实时会话的时延，平均时延，连接失败率进行分析统计，不同时延段按不同颜色表示。
历史分析	对历史会话的时延，平均时延，连接失败率进行分析统计，不同时延段按不同颜色表示。

质差源	质量分析统计会话样本的源 IP。
质差目标	质量分析统计会话样本的会话 IP。

表 4-48 质量概况参数说明

4.5.2. 质量诊断

质量诊断是基于源目 IP、目标域名、应用协议的连接数、连接失败次数、平均时延的诊断信息。

步骤 1 选择【协议质量】>【质量诊断】。

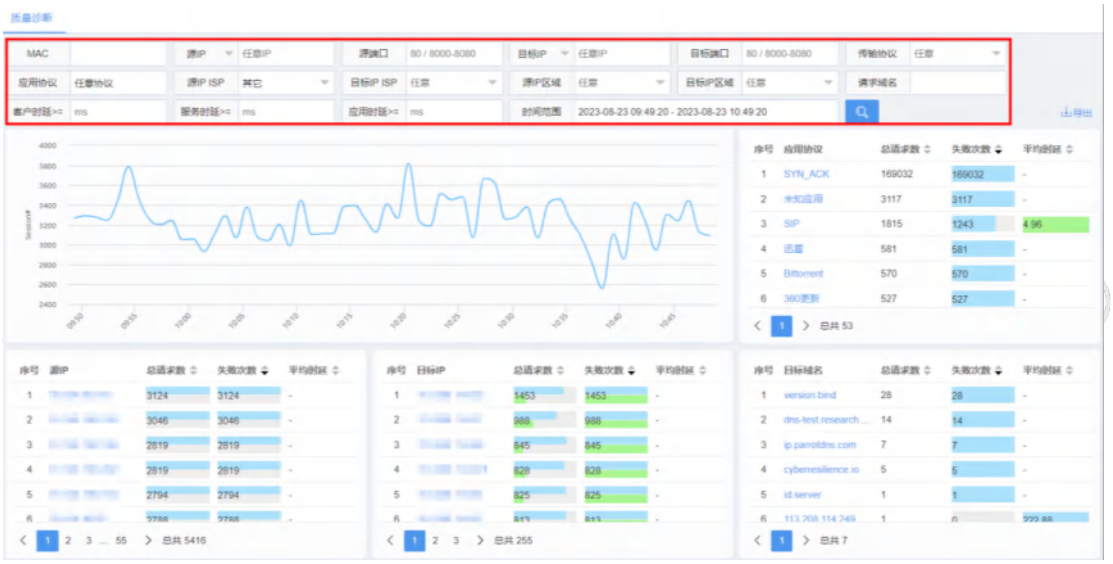


图 4-53 质量诊断详情

参数名称	参数说明
MAC	会话源 MAC。
源 IP	会话源 IP。
源端口	会话源端口。
目标 IP	会话目标 IP。
目标端口	会话目标端口。
传输协议	会话基于传输协议。
应用协议	会话基于的应用协议。
源 IP ISP	产生会话的源 IP 的 ISP 运营商名称。
目标 IP ISP	产生会话的目标 IP 的 ISP 运营商名称。
源 IP 区域	产生会话的源 IP 的所在区域。
目标 IP 区域	产生会话的目标 IP 所在区域。

请求域名	请求访问的域名。
客户时延	客户端至测量点的网络时延，客户时延过大表示内网环境延迟过大。
服务时延	测量点至服务器的网络时延，服务时延过大表示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，应用时延过大表示服务提供商提供服务的延迟过大。

表 4-49 质量诊断参数说明

4.5.3. 会话时延

会话时延是对 TCP、UDP、ICMP 三种会话时延的统计结果。

步骤 1 选择【协议质量】>【会话时延】。

图 4-54 会话时延详情

参数名称	参数说明
MAC	会话源 MAC。
源 IP	会话源 IP。
源端口	会话源端口。
目标 IP	会话目标 IP。
目标端口	会话目标端口。
传输协议	会话基于传输协议。
应用协议	会话基于的应用协议。
源 IP ISP	产生会话的源 IP 的 ISP 运营商名称。

目标 IP ISP	产生会话的目标 IP 的 ISP 运营商名称。
源 IP 区域	产生会话的源 IP 的所在区域。
目标 IP 区域	产生会话的目标 IP 所在区域。
请求域名	请求访问的域名。
客户时延	客户端至测量点的网络时延，客户时延过大表示内网环境延迟过大。
服务时延	测量点至服务器的网络时延，服务时延过大表示运营商提供的承载网络延迟过大。
连接类型	连接结果成功或失败。

表 4-50 会话时延参数说明

4.5.4. 协议时延

协议时延是对应用协议相关会话时延情况，上/下行速率，连接失败率等进行监控。

步骤 1 选择【协议质量】>【协议时延】。

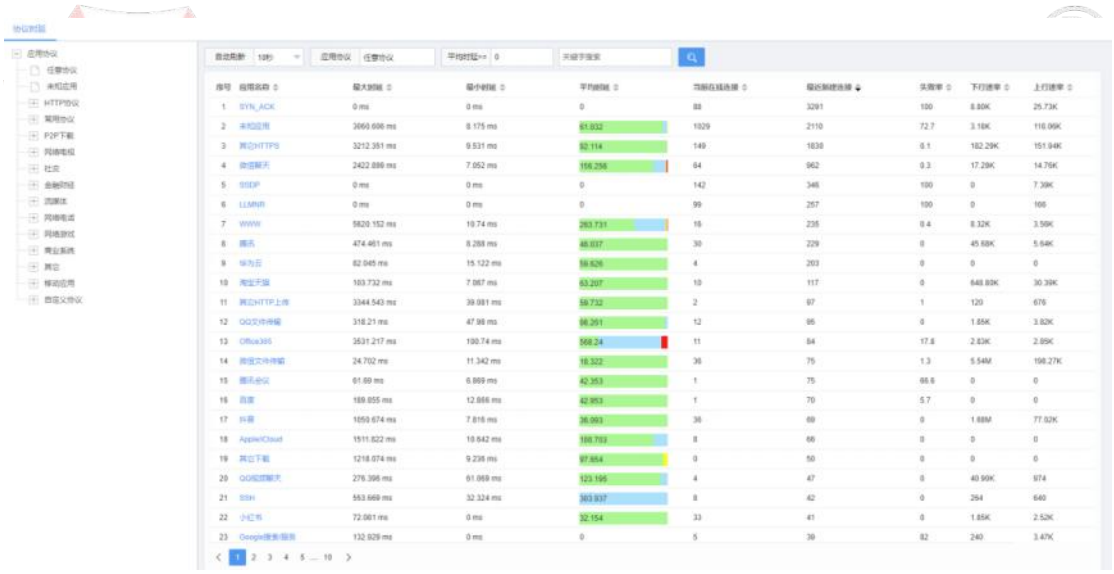


图 4-55 协议时延详情

参数名称	参数说明
自动刷新	统计结果刷新频率，可选择不刷新或以 5s/10s/20s/60s 为周期刷新。
应用协议	需要监控的应用协议名。
平均时延	一段时间内统计该应用协议时延的平均值。

表 4-51 协议时延参数说明

4.6. 溯源分析

溯源分析是基于流量、会话、IP 及域名的溯源分析及诊断。当发生网络事件时，客户可以通过溯源分析迅速进行故障定位。

4.6.1. 流量诊断

流量诊断功能是基于全流量的溯源分析及诊断，支持对流量诊断结果按照既定条件进行查询，快速发现可能存在的异常 IP 或应用。

步骤 1 选择【溯源分析】>【流量诊断】。

图 4-56 流量诊断详情

参数名称	参数说明
MAC	会话源 MAC。
源 IP	会话源 IP。
源端口	会话源端口。
目标 IP	会话目标 IP。
目标端口	会话目标端口。
传输协议	会话基于传输协议。
源 IP ISP	产生会话的源 IP 的 ISP 运营商名称。
目标 IP ISP	产生会话的目标 IP 的 ISP 运营商名称。
源 IP 区域	产生会话的源 IP 的所在区域。
目标 IP 区域	产生会话的目标 IP 所在区域。
请求域名	请求访问的域名。

表 4-52 流量诊断参数说明

4.6.2. 会话流量

会话流量功能是基于全会话的溯源分析及诊断，支持对流量诊断结果按照既定条件进行查询。

步骤 1 选择【溯源分析】>【会话流量】。

图 4-57 会话流量详情

参数名称	参数说明
MAC	会话源 MAC。
源 IP	会话源 IP。
源端口	会话源端口。
目标 IP	会话目标 IP。
目标端口	会话目标端口。
传输协议	会话基于传输协议。
请求域名	请求访问的域名。
应用协议	会话基于的应用协议。
连接类型	会话连接结果，成功/失败。
条件关系	搜索条件之间的或/与/非关系。
上行字节>=	搜索大于等于此上行字节的会话流量诊断结果。
下行字节>=	搜索大于等于此下行字节的会话流量诊断结果。
上行包数>=	上行数据包个数，搜索大于等于此上行包数的会话流量诊断结果。

下行包数>=	下行数据包个数，搜索大于等于此下行包数的会话流量诊断结果。
源 IP ISP	产生会话的源 IP 的 ISP 运营商名称。
目标 IP ISP	产生会话的目标 IP 的 ISP 运营商名称。
源 IP 区域	产生会话的源 IP 的所在区域。
目标 IP 区域	产生会话的目标 IP 所在区域。
请求域名	请求访问的域名。
导出	支持将会话流量诊断结果按照搜索条件进行导出。

表 4-53 会话流量参数说明

4.6.3. IP 画像

IP 画像是基于应用流量、域名访问、开放域名、开放端口、IP 访问次数、外到内的接入 IP 等对 IP 用户进行画像，方便客户更了解自身网络用户的典型特征，发现潜在风险。

步骤 1 选择【溯源分析】>【IP 画像】。

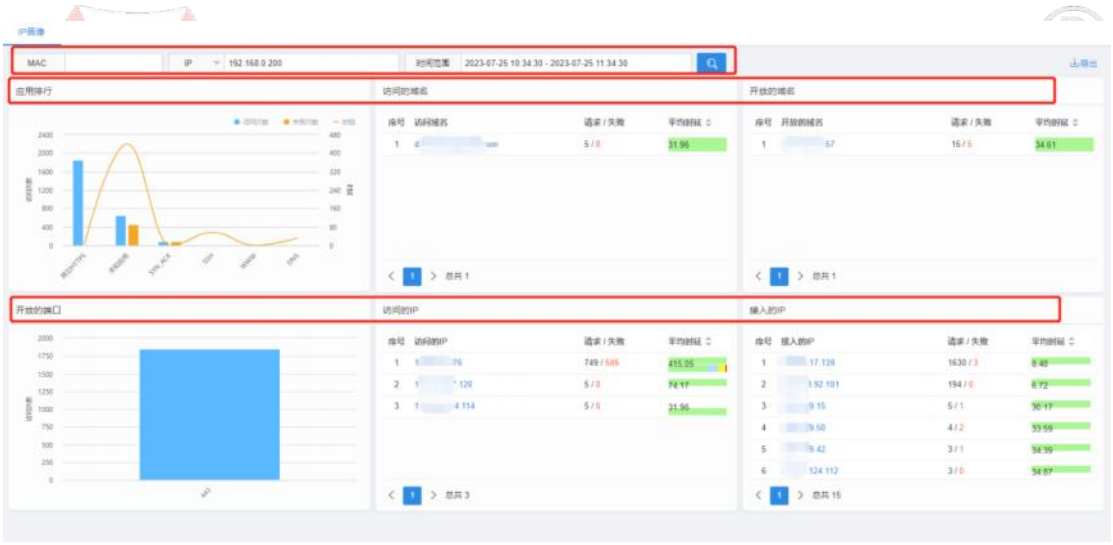


图 4-58 IP 画像详情

参数名称	参数说明
MAC	会话源 MAC。
IP	会话源 IP/目标 IP。
应用排行	默认按访问次数降序排列，显示指定查询时间范围内访问的前 8 个应用对应的 访问次数、访问失败次数以及时延。
访问的域名	默认按请求次数降序排列，显示诊断 IP 指定时间范围内，主动访问的域名、请求/失败次数以及平均时延。

开放的域名	默认按请求次数降序排列，显示诊断 IP 指定时间范围内，被访问域名、请 求/失败次数以及平均时延。
开放的端口	显示诊断 IP 指定时间范围内，开放的端口以及被访问的次数；
访问的 IP	默认按请求次数降序排列，显示诊断 IP 指定时间范围内，访问对应 IP 的次数、请求/失败次数以及平均时延。
接入的 IP	默认按请求次数降序排列，显示诊断 IP 指定时间范围内，连接到诊断 IP 的其他 IP、请求/失败次数以及平均时延。

表 4-54 IP 画像参数说明

4.6.4. 域名画像

域名画像功能支持对访问域名按照既定条件进行查询，对域名进行画像，方便客户了解自身网络用户访问频次较高的域名，对用户上网行为进行管控。

步骤 1 选择【溯源分析】>【域名画像】。

图 4-59 域名画像详情

参数名称	参数说明
源 IP	会话源 IP。
源端口	会话源端口。
目标 IP	会话目标 IP。
目标端口	会话目标端口。
源 IP ISP	产生会话的源 IP 的 ISP 运营商名称。
目标 IP ISP	产生会话的目标 IP 的 ISP 运营商名称。
源 IP 区域	产生会话的源 IP 的所在区域。

目标 IP 区域	产生会话的目标 IP 所在区域。
请求域名	请求访问的域名。
访问最多用户	访问该域名的 TOP 8 用户。
最多访问服务器	该域名被访问的 TOP 8 服务器（包含 DNS 服务器）。
最慢访问用户	访问该域名时，时延最大的 TOP 8 用户。
最慢访问服务器	该域名被访问时，时延最大的 TOP 8 服务器（包含 DNS 服务器）。
连接分布	访问该域名的连接类型分布，按照 DNS、HTTPS、HTTP（包含 HTTP20X、HTTP30X、HTTP40X、HTTP50X）分类。
连接趋势	访问该域名的连接数趋势图，按照 DNS、HTTPS、HTTP（包含 HTTP20X、HTTP30X、HTTP40X、HTTP50X）分类。
时延趋势	访问该域名的平均时延趋势图，按照 DNS 时延与非 DNS 时延分别统计。
世界范围内分布 中国范围内分布	访问该域名用户的地理位置分布范围（世界范围内和中国范围内）。 

表 4-55 域名画像参数说明

4.7. 网络管理

4.7.1. 概述

网络管理模块，涵盖了 Panabit 的各种基础网络配置，包括接口设置、路由规则以及其他网络设置等。

4.7.1.1. 逻辑接口

Panabit 上网行为管理中，所有创建的线路都是逻辑接口，包括所有的 WAN 线路类型、LAN 接口类型、iWAN 服务等，总共可以创建 32 个逻辑接口。

1. 逻辑接口和网络接口（物理网卡）的关系：网络接口用来承载逻辑接口，一个网络接口可以承载多个逻辑接口，每个逻辑接口有自己的 MAC 地址。
2. LAN 接口类型的线路和 DHCP 服务必须配置在接内网的网络接口上。WAN 线路类型的逻辑接口必须配置在接外网的网络接口上。
3. iWAN 服务是一个特殊的逻辑接口，承载在 WAN 线路上。但它是一个对内的逻辑接口，接入的流量会创建内网 IP 对象，详情请参见 iWAN。

4.7.1.2. 策略路由

策略路由是 Panabit 的路由控制模块，该模块的策略决定了数据报文转发的方式和方向，支持的工作方式有：IPv4 路由/NAT、IPv6 路由。与传统路由相比较，基于应用的路由是该功能模块最大的亮点。

每一条策略路由主要由三个要素组成:“策略序号”、“匹配条件”、“执行动作”。

图 4-60 策略路由详情

说明

1. 策略路由是基于会话的，首先创建了会话才会匹配策略路由。
2. 配置了应用协议条件的策略路由，由于应用识别的原理、应用的特性和不破坏连接一致性的原则，不能 100%保证匹配策略。
3. 做基于应用的策略路由，执行动作为 NAT 的效果是最好的。
4. 网桥模式部署，也可以使用策略路由，只需要在接外网的网卡上创建可以访问互联网的 WAN 线路即可。

4.7.2. 网卡设置

该页面显示当前设备的数据接口（物理网卡）状态，并可以对数据接口做配置。

4.7.2.1. 网络接口

网络接口支持对网卡进行编辑，设置网卡接入模式和方向等。

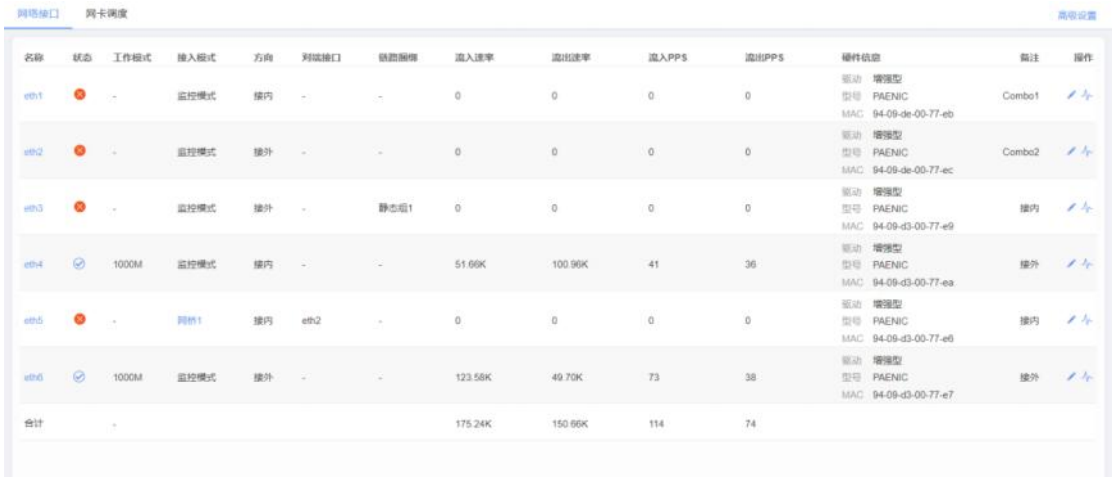
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

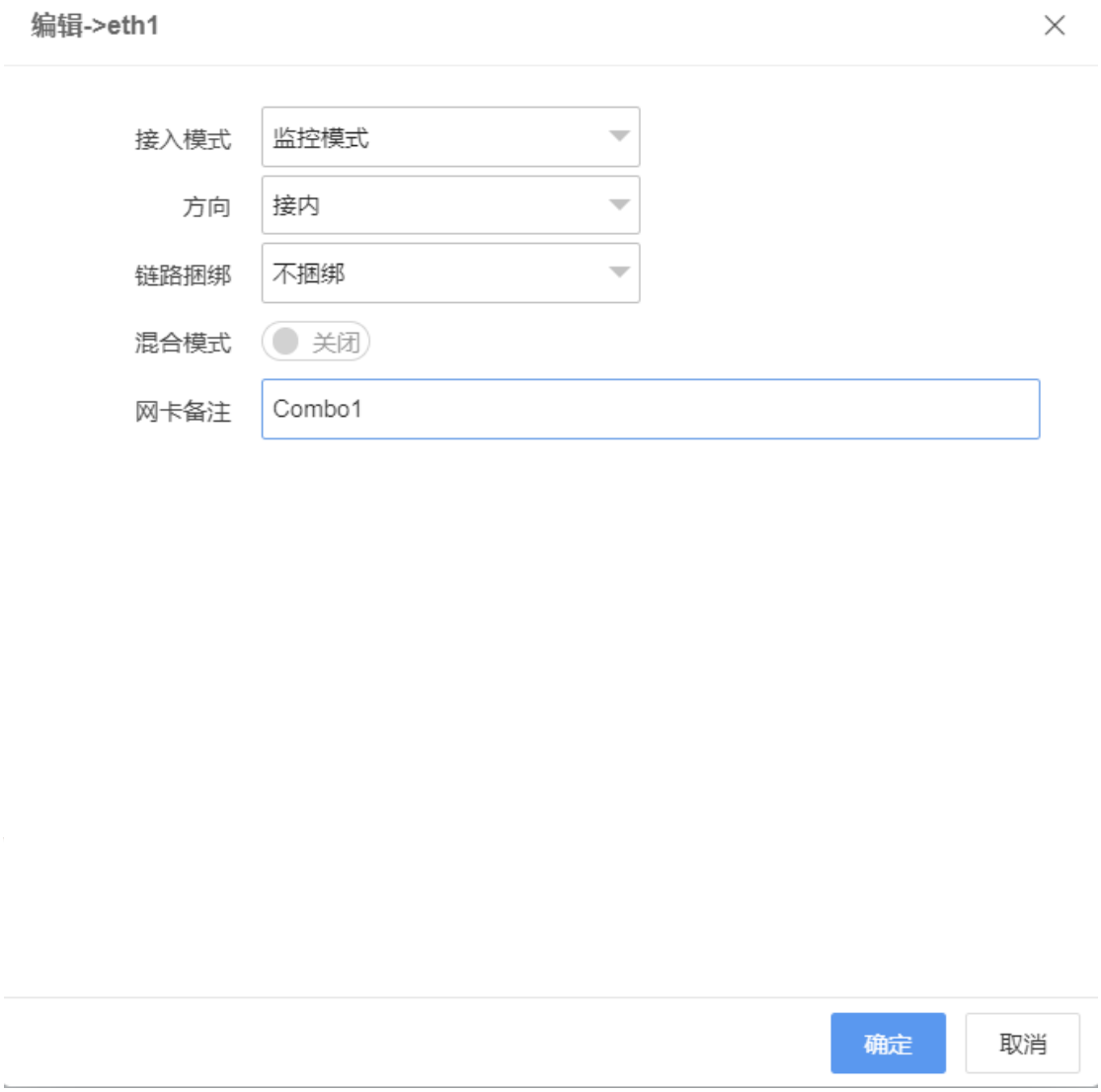
步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【网卡设置】。

步骤 4 选择页面上方的【网络接口】。



步骤 5 单击当前网卡操作列的 ，可编辑当前网卡。



参数名称	参数说明
接入模式	监控模式：网卡的普通接入模式，对流经网卡的流量进行监控统计，一般用于网关模式、旁路模式部署。 网桥：一个网桥由一对网卡组成，一个为“接内网”， 另一个为“接外网”，并且互为对端接口。默认情况下对流经的数据透明转发，不做干预，一般用于串接模式部署。  ● 对端接口：定义该组网桥中的另一接口。

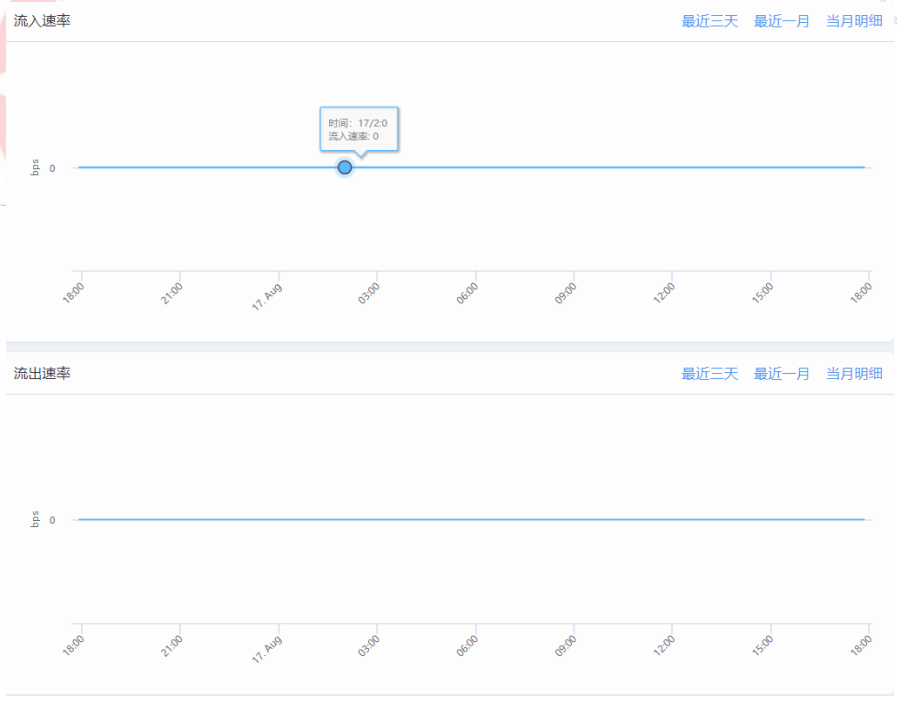
	● 网桥名称：定义网桥的名称。
方向	网卡的接入方式，可选择“接内”、“接外”。LAN 接口、DHCP 等的接口设置为“接内”，WAN 线路、对外网提供服务（NAT，DNS 管控等）的接口设置为“接外”。 ● 设置为“接内”，那么流入这个网卡的流量，将被统计为上行流量。 ● 设置为“接外”，那么流入这个网卡的流量，将被统计为下行流量。
链路捆绑	将网卡设置为一组链路组，其效果是同链路组的所有网卡在发包时采用轮询等机制，轮流发送数据包。 不捆绑：不进行捆绑操作。 链路组： ● 捆绑协议：可选择“静态捆绑”、“LACP”。 ● 老化模式：可选择“慢速模式”、“快速模式”。 ● 被动模式：可“开启”或“关闭”被动模式。 **说明** ● 静态捆绑：手工指定多个网卡作为链路组的成员，通过网卡的物理连接状态来确定网卡是否可用来负载流量。 ● LACP：手工指定多个网卡作为链路组的成员，通过使用 LACP 协议和对端确认网卡是否可用来负载流量。
工作模式	可以调整网卡的速率，一般建议用自适应。
混合模式	可“开启”或“关闭”混合模式。见旁路部署。
网卡备注	为网卡添加补充说明。

步骤 6 单击网卡名称或操作列的，弹出网卡档案页面。

参数设置 当前状态 实时流量 历史趋势 网卡内参

名称 igb0
接入模式 监控模式
方向 接内
驱动 增强型
型号 I210_COPPER
状态
工作模式 自适应
当前速率 NONE
MTU 1500
MAC 3C:EC:EF:90:81:85
流入速率 0
流出速率 0
流入PPS 0
流出PPS 0

参数名称	参数说明
参数设置	通过参数设置可对网卡进行编辑。 
当前状态	当前状态主要呈现网卡的各种参数一览。 名称 igb0 接入模式 监控模式 方向 接内 驱动 增强型 型号 I210_COPPER 状态 工作模式 自适应 当前速率 NONE MTU 1500 MAC 3C:EC:EF:90:81:85 流入速率 0 流出速率 0 流入PPS 0 流出PPS 0

实时流量	实时流量展示当前网卡 24 小时内的流入/流出速率。 
历史趋势	展示当前网卡的流入/流程速率和 PPS。 

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>网卡内参</td><td>展示网卡的参数。
● Missed Packets：网卡丢包。
● Receive Length Errors(roc)：有超过网卡 MTU 的数据包，引起丢包。
● Crc errors：网卡或网线存在问题。
上面三个参数的增长，一般与硬件有关。</td></tr>
</table>

——结束

4.7.2.2. 网卡调度

网卡调度可调整不同的 CPU 单元，对不同网卡队列的数据包进行处理。

操作步骤

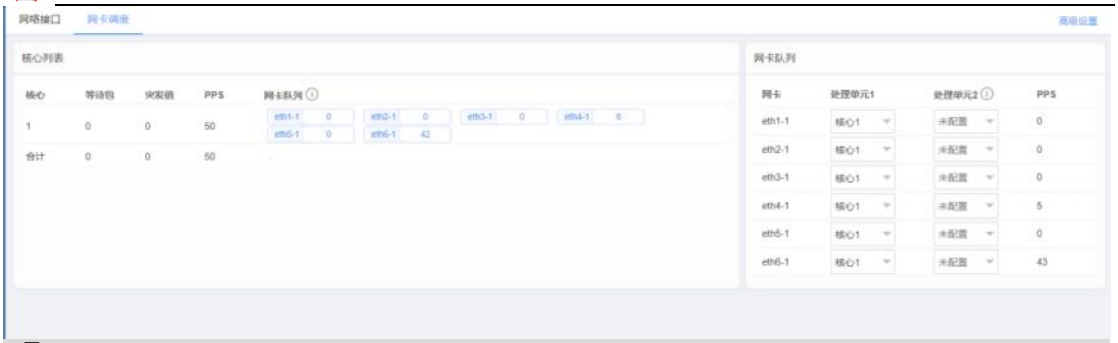
步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【网卡设置】。

步骤 4 选择页面上方的【网卡调度】。

步骤 5 在网卡队列页面设置处理单元或用鼠标左键长按 eth1-1 0 图标进行拖拽，来进行网卡调度。



说明

- 每一个 CPU 单元可理解为一个独立的 CPU 内核，每个千兆网卡有 1 个队列，每个万兆网卡有 2 个队列，每个 100G 网卡有 4 个队列。
- 由于每个 CPU 单元可以处理的数据是有上限的，因此在调整网卡调度时，我们要尽量让不同的 CPU 单元处理不同的网卡队列，如果某个网卡空载没带业务，那么就不会消耗 CPU 的性能。因此，需要根据实际情况合理调度，尽量让所有的 CPU 单元都工作起来，让设备性能保持最佳状态。

——结束

4.7.3. LAN/WAN

4.7.3.1. WAN 线路

WAN 线路是设备连接到广域网（Wide Area Network）的逻辑接口，用于连接到外部网络，通常是互联网或其他外部 WAN。

- IP 地址：WAN 线路通常需要配置一个唯一的 IP 地址，以便与外部网络通信。这个 IP 地址通常由互联网服务提供商（ISP）分配，可能是静态或动态分配的。
- 路由和 NAT：WAN 线路上的路由和网络地址转换（NAT）配置，对于连接内部网络与外部网络而言非常重要。它们允许上网行为管理设备将数据包从内部网络传输到外部网络，同时保护内部网络的安全性。

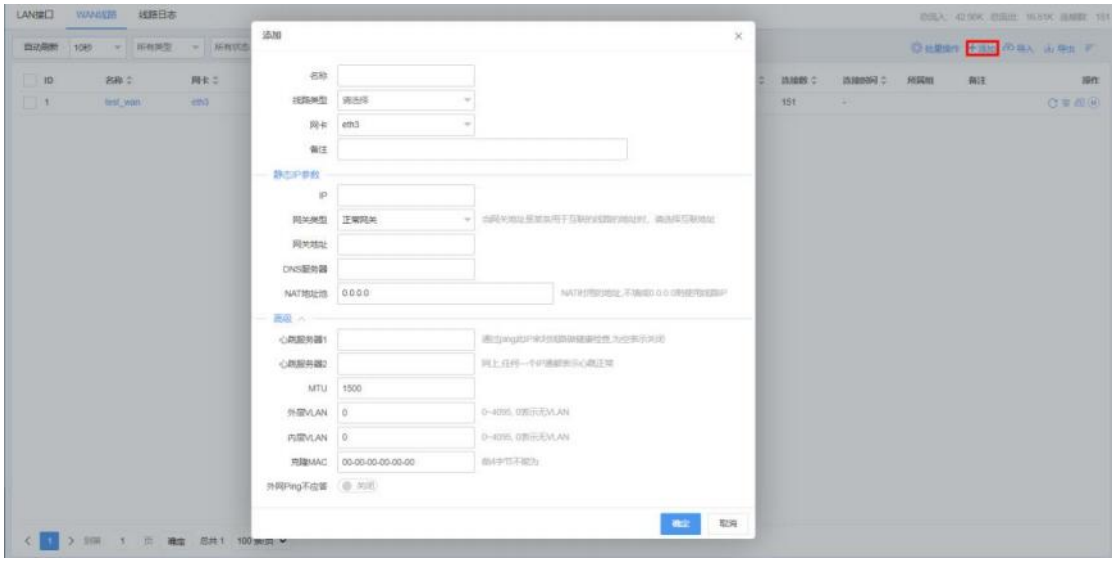
操作步骤

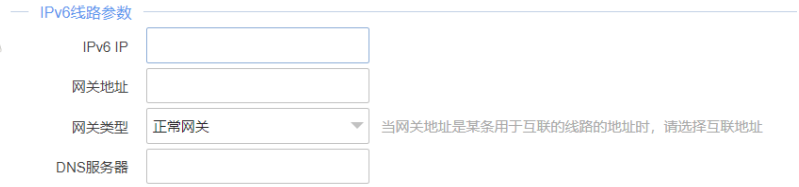
步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【LAN/WAN】>【WAN 线路】。

步骤 4 单击页面右上角【添加】，弹出添加 WAN 线路页面。



参数名称	参数说明
名称	自定义 WAN 线路名称。
线路类型	WAN 线路类型，可选择“静态 IPv6”、“静态 IPv4”、“DHCP IPv4”、“PPPoE”、“iWAN”、“L2TP”、“IPsec”、“GREWAN”。
网卡	选择承载该 WAN 线路的物理网卡，网卡需提前设置为“接外网”
备注	对 WAN 线路的补充说明。
IPv6 线路参数	 IPv6 IP：设置线路的 IPv6 IP。 网关地址:线路对端的网关地址。 网关类型: ● 正常网关：一般的网关类型。 ● 互联网关：当网关地址是某条用于互联的线路的地址时，请选择互联网关。 DNS 服务器：当设置 DNS 管控策略的时候，这个选项才会起作用。
静态 IP 参数	 IP：IPv4 的 IP。

	网关地址:线路对端的网关地址。 网关类型: ● 正常网关：一般的网关类型。 ● 互联网关：当网关地址是某条用于互联的线路的地址时，请选择互联地址。 DNS 服务器：当设置 DNS 管控策略的时候，这个选项才会起作用。 NAT 地址池：NAT 时用的地址，不填或 0.0.0.0 则使用线路 IP。
PPPoE 参数	 PPPoE 账号/密码：输入 PPPoE 账号/密码 BRAS 名称：如果填写，只接受同名的 BRAS 服务。 Service 名称 ：如果填写，只接受同名的服务。 重拨等待时间：单位秒，避免频繁拨号而被运营商封线。
iWAN 参数	具体请参见配置 iWAN 线路。
L2TP 参数	具体请参见配置 L2TP 线路。
IPsec 参数	具体请参见配置 IPsec 线路。
GRE WAN	 IP：指定本地网络的 IP 地址。 对端地址：另一个网络的 IP 地址，该网络与本地网络之间将建立隧道。 心跳间隔：隧道设备之间周期性发送心跳消息的时间间隔。这些心跳消息用于确认隧道的活动状态。0~255，0 表示关闭. 隧道校验：通过验证机制来确认隧道的状态和可用性。通过发送测试数据包或心跳消息来检查隧道是否正常工作。可“开启”或“关闭”。 隧道关键字： 在配置隧道时使用的标识符，以便在设备之间唯一标识隧道。取值为 0-4294967295。
心跳服务器 1	通过 ping 此 IP 来对线路做健康检查，为空表示关闭。

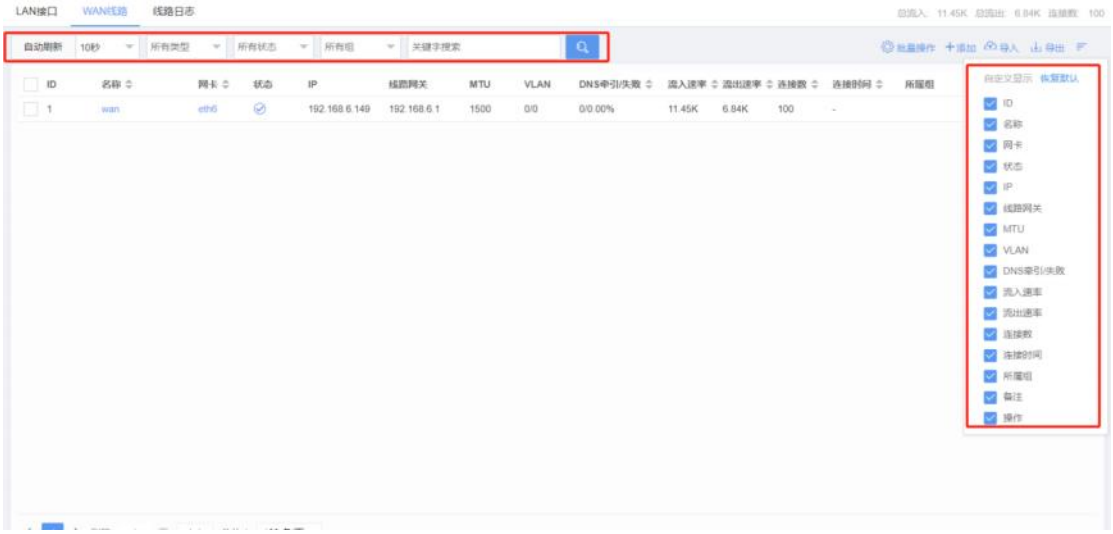
心跳服务器 2	通过 ping 此 IP 来对线路做健康检查，为空表示关闭。与心跳服务器 1 任何一个 IP 通都表示心跳正常。
MTU	定义数据的最大传输单元。
外层 VLAN	定义从该接口出去的数据报文所携带的外层 VLAN 标记，0 表示外出的数据不带修改 VLAN 标记，与进入接口时的 VLAN 保持一致。 取值：0~4095，0 表示无 VLAN。
内层 VLAN	定义从该接口出去的数据报文所携带的内层 VLAN 标记，0 表示外出的数据不带修改 VLAN 标记，与进入接口时的 VLAN 保持一致。 取值：0~4095，0 表示无 VLAN。
克隆 MAC	不使用自身携带的 MAC 地址，而是使用自定义手工输入的 MAC 地址。 格式：00-00-00-00-00-00，前 4 字节不能为空。
外网 Ping 不应答	可选择“开启”或“关闭”。

步骤 5 单击【确定】。

说明

- 线路类型请根据现网实际选择。当网络出口不是固定 IP，只有 PPPoE 拨号线路时，线路类型请选择“PPPoE”，然后填入 PPPoE 的账号密码；同理，线路类型也可选择 DHCP 等方式。其他的 VPN 线路类型，如 iWAN、IPsec 等，请参见虚拟专网。
- 当有多条线路时，需多次进行添加。

成功添加后，可以在【WAN 线路】页面查看线路详情。



参数名称	参数说明
自定义显示	鼠标悬停或单击 后，可勾选需要在列表中呈现的信息。
自动刷新	线路详情的刷新时间，可选择不刷新或以 5s/10s/20s/60s 为周期进行刷新。
条件搜索	可根据线路类型、线路状态、线路所在组的名称以及线路关键字筛选符合条件的线路。
ID	WAN 线路的 ID，用于唯一标识一条 WAN 线路。
名称	WAN 线路的名称。
网卡	承载 WAN 线路的物理网卡。
状态	WAN 线路状态。为正常连接；为禁用状态；为连接失败。
IP	WAN 线路的 IP 地址。
线路网关	WAN 线路的网关 IP 地址。
MTU	WAN 线路的 MTU。
VLAN	WAN 线路携带的内/外层 VLAN 标记。
DNS 牵引/失败	DNS 牵引的次数，以及失败率。
流入速率	WAN 线路当前实时的流入速率。
流出速率	WAN 线路当前实时的流出速率。
连接数	WAN 线路当前实时的连接数。
连接时间	对于 VPN 类型的线路（iWAN、IPsec 等），显示其连接时长。
所属组	WAN 线路所属的 WAN 群组。
备注	WAN 线路的备注。
操作	：重拨当前线路。 ：删除当前线路。 ：复制当前线路参数，添加一条 WAN 线路。 / ：禁用或启用当前线路。

查看状态	查看当前线路的详细档案。 ● 当前状态：当前 WAN 线路的状态。  ● 参数设置：对当前 WAN 线路的参数进行编辑。  ● TOP 应用：显示该 WAN 线路承载流量的应用组成。 

序号	协议名称	流出速率	流入速率	总速率
1	其它HTTPS	251	2.94K	3.19K
2	IMAP	816	1.47K	2.28K
3	QQ聊天	193	1.14K	1.33K
4	SYN_ACK	1.05K	0	1.05K
5	钉钉	313	249	562
6	其它HTTP上传	239	239	478

- 实时流量：显示该 WAN 线路 1 小时内的实时流入流出速率统计。

- 历史趋势：显示该 WAN 线路历史流量的流入流出速率与连接数趋势统计，可查看“最近三天”、“最近一月”和“当月明细”。

- 线路日志：显示该 WAN 线路的事件记录，如线路激活、断开等。

	
快速编辑	与上面的参数设置类似，对当前 WAN 线路的参数进行编辑。 

——结束

4.7.3.2. LAN 接口

LAN 接口是指网关设备上连接到局域网（Local Area Network）的逻辑接口。

- IP 地址：网关的 LAN 口通常需要配置一个 IP 地址，该地址用于在局域网内标识上网行为管理设备。这个 IP 地址通常用于内部设备将数据包发送到上网行为管理，以便进一步路由到外部网络。
- DHCP 服务：LAN 接口可以配置动态主机配置协议（DHCP）服务，以自动分配 IP 地址给

内部设备。这样，内部设备可以自动获取 IP 地址、子网掩码、网关地址等信息。

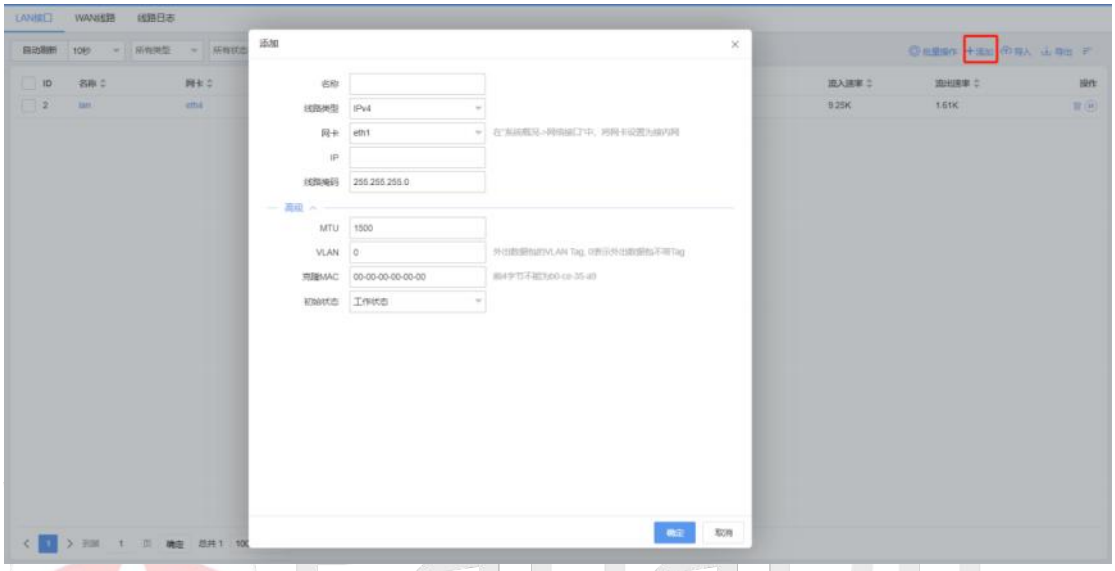
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

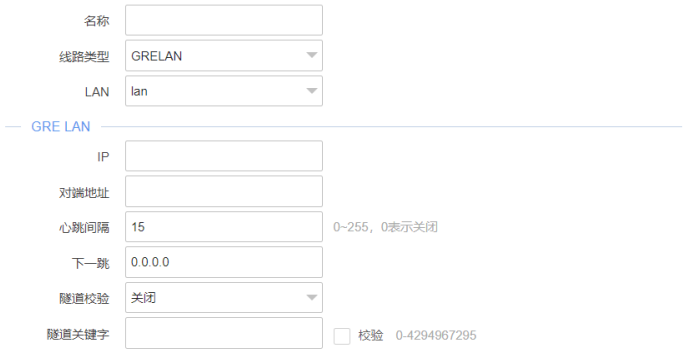
步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【LAN/WAN】>【LAN 接口】。

步骤 4 单击页面右上角【添加】，弹出添加 LAN 接口页面。

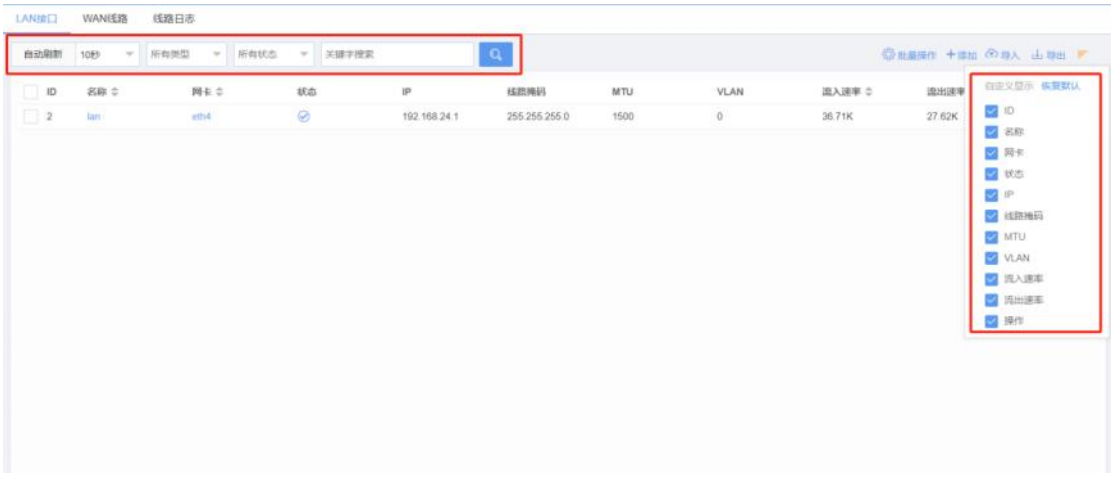


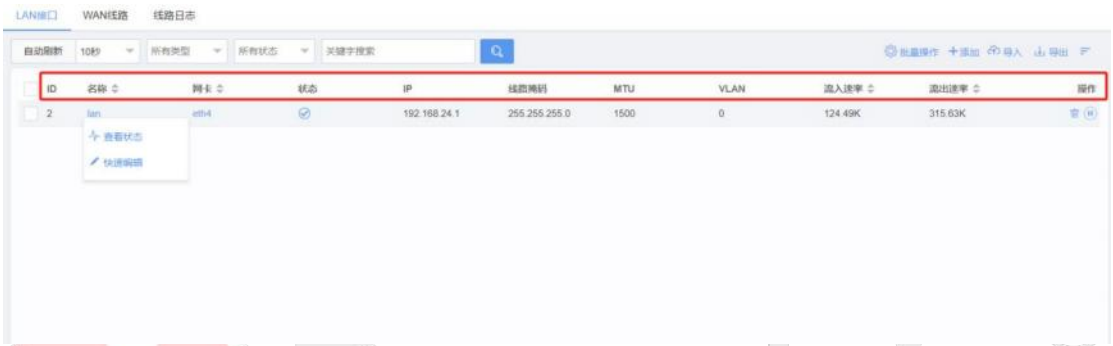
参数名称	参数说明
名称	自定义 LAN 线路名称。
线路类型	可设置为“IPv4”、“IPv6” 、“VRRP-IPv4” “GRELAN”
网卡	选择承载该 LAN 线路的物理网卡，网卡需提前设置为“接内网”。
IP/IPv6 IP	IPv4 或 Pv6 的 IP 地址。
线路掩码	IP 地址的掩码。
IPv6 无状态地址分配	 地址分配：可选择“开启”或“关闭”。 分配 VLAN：若配置，则只给指定 VLAN 分配地址。 DNS1：主 DNS 服务器的 IPv6 地址。 DNS2：备用 DNS 服务器的 IPv6 地址。
VRRP-IPv4	参见 VRRP 联动。

GRE LAN	 LAN：选择 GRE 隧道的承载线路。 IP：GRE LAN 的 IP 地址。 对端地址：另一个网络的 IP 地址，该网络与本地网络之间将建立隧道。 心跳间隔：隧道设备之间周期性发送心跳消息的时间间隔。这些心跳消息用于确认隧道的活动状态。0~255，0 表示关闭。 下一跳：当 LAN 与对端地址不是同一网段时使用，通过 LAN 路由到对端地址的下一跳 IP 隧道校验：通过验证机制来确认隧道的状态和可用性。通过发送测试数据包或心跳消息来检查隧道是否正常工作。可“开启”或“关闭”。 隧道关键字： 在配置隧道时使用的标识符，以便在设备之间唯一标识隧道。取值为 0-4294967295。
MTU	定义数据的最大传输单元。
VLAN	外出数据包的 VLAN Tag，0 表示外出数据包不带 Tag。
克隆 MAC	不使用自身携带的 MAC 地址，而是使用自定义手工输入的 MAC 地址。 格式：00-00-00-00-00-00，前 4 字节不能为 b0-ce-35-a9。
初始状态	可选择“工作状态”或“待机状态”。

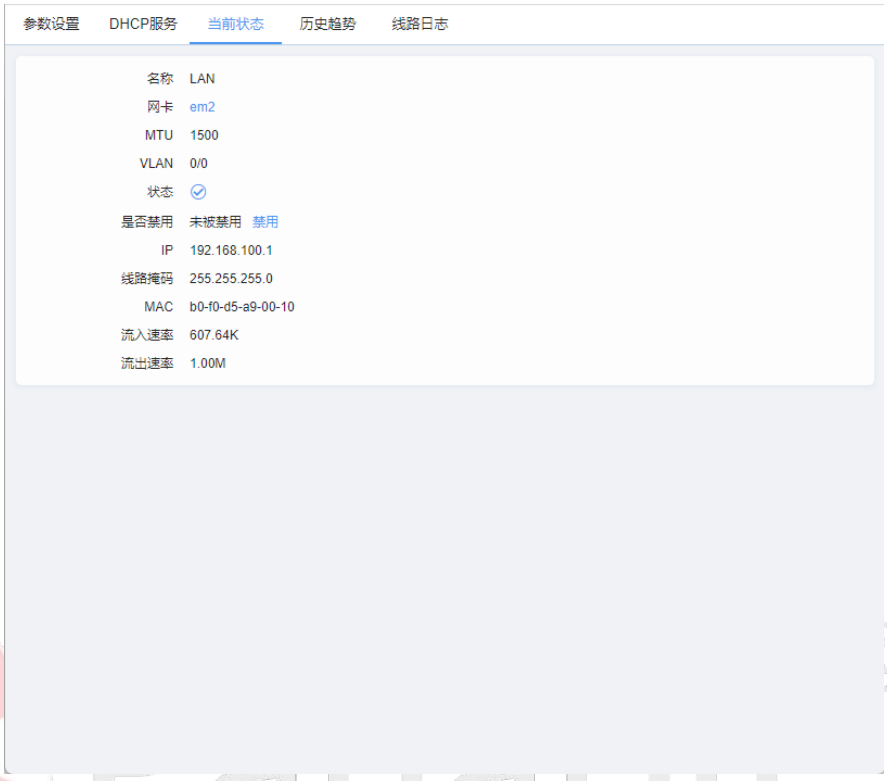
步骤 5 单击【确定】。

成功添加后，可以在【LAN 接口】页面查看线路详情。

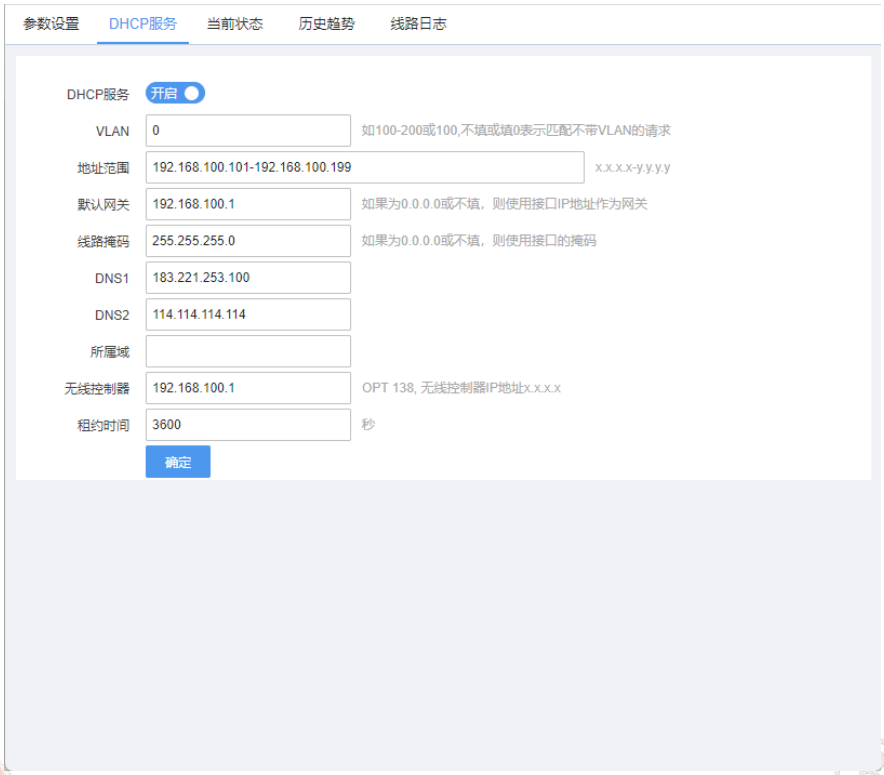




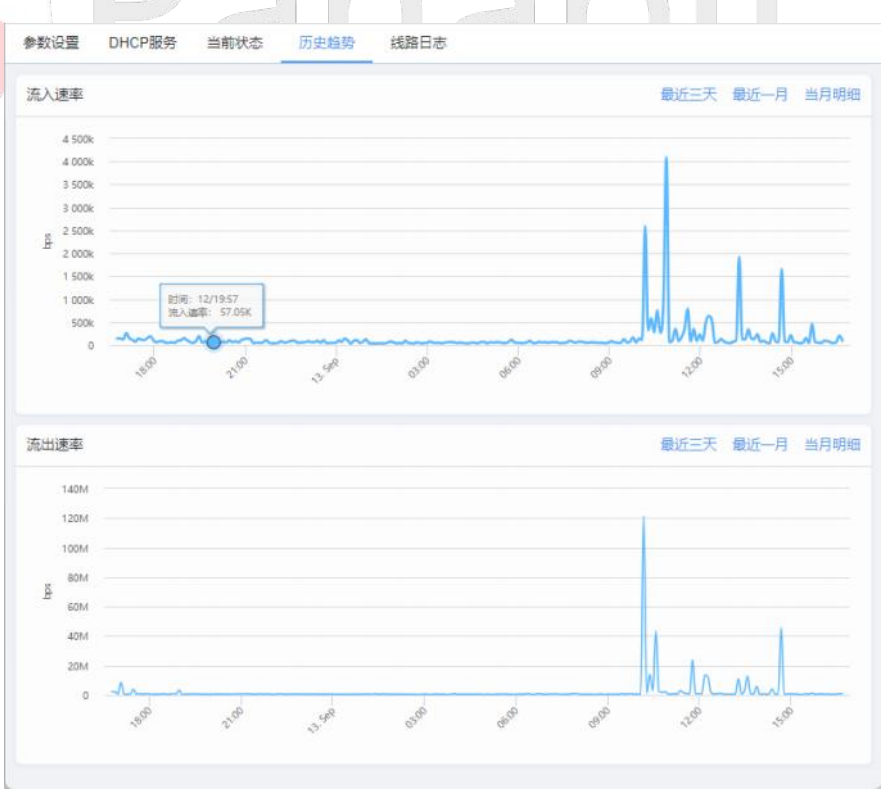
参数名称	参数说明
自定义显示	鼠标悬停或单击 后，可勾选需要在列表中呈现的信息。
自动刷新	线路详情的刷新时间，可选择不刷新或以 5s/10s/20s/60s 为周期进行刷新。
条件搜索	可根据线路类型、线路状态以及线路关键字筛选符合条件的线路。
ID	LAN 接口的 ID，用于唯一标识一条 LAN 线路。
名称	LAN 线路的名称。
网卡	承载 LAN 线路的物理网卡。
状态	LAN 线路状态。为正常连接；为禁用状态；为连接失败。
IP	LAN 线路的 IP 地址。
线路掩码	LAN 线路 IP 地址的掩码。
MTU	LAN 线路的 MTU。
VLAN	LAN 线路携带的 VLAN 标记。
流入速率	LAN 线路当前实时的流入速率。
流出速率	LAN 线路当前实时的流出速率。
操作	：删除当前线路。

	⏸ / ▶：禁用或启用当前线路。
查看状态	查看当前线路的详细档案。 ● 当前状态：当前 LAN 线路的状态。  ● 参数设置：对当前 LAN 线路的参数进行编辑。 

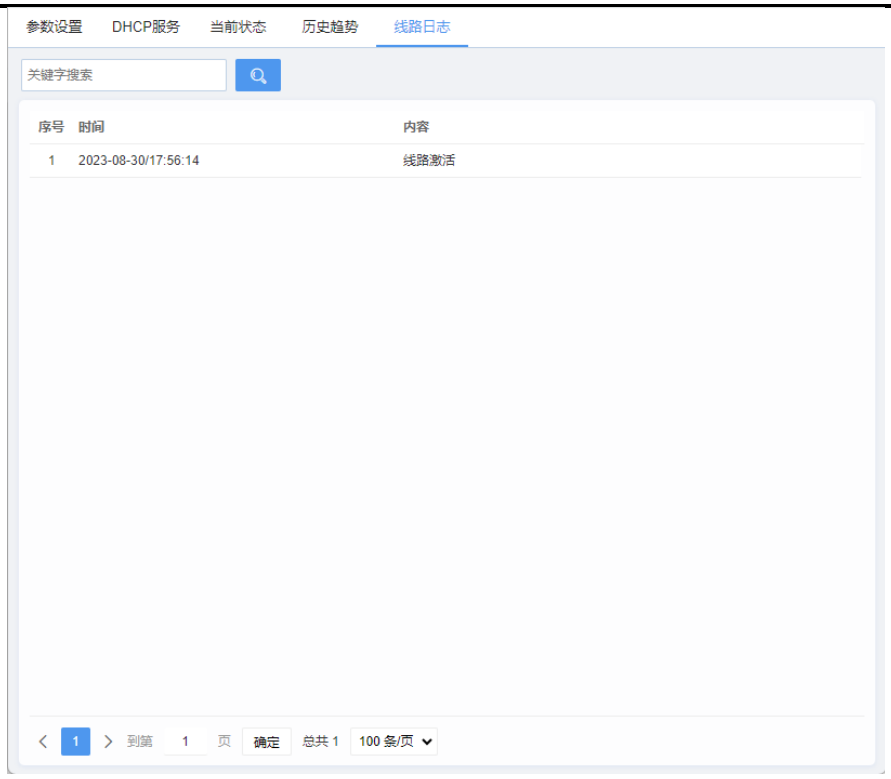
- DHCP 服务：在 LAN 线路上对 DHCP 服务进行配置，参见 DHCP 服务。



- 历史趋势：显示该 LAN 线路历史流量的流入流出速率趋势统计，可查看“最近三天”、“最近一月”和“当月明细”。

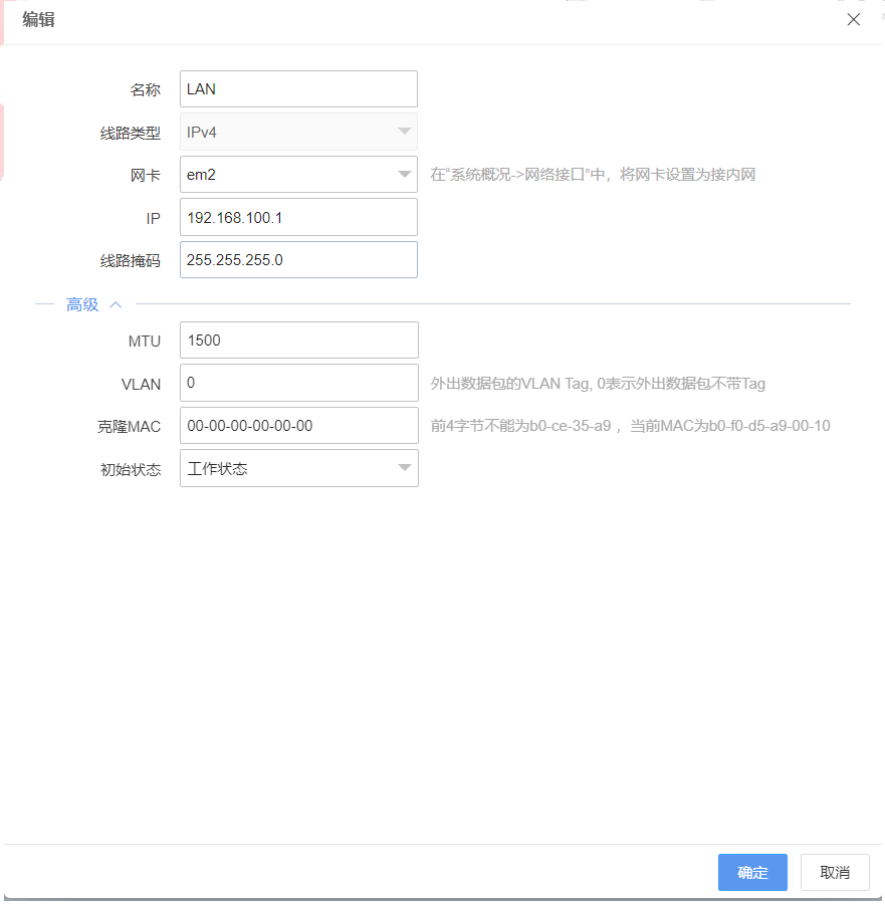


- 线路日志：显示该 LAN 线路的事件记录，如线路激活、断开等。



快速编辑

与上面的参数设置类似，对当前 LAN 线路的参数进行编辑。



——结束

4.7.3.3. 线路日志

查看所有 LAN/WAN 类型线路的事件记录，并可根据关键字进行搜索。

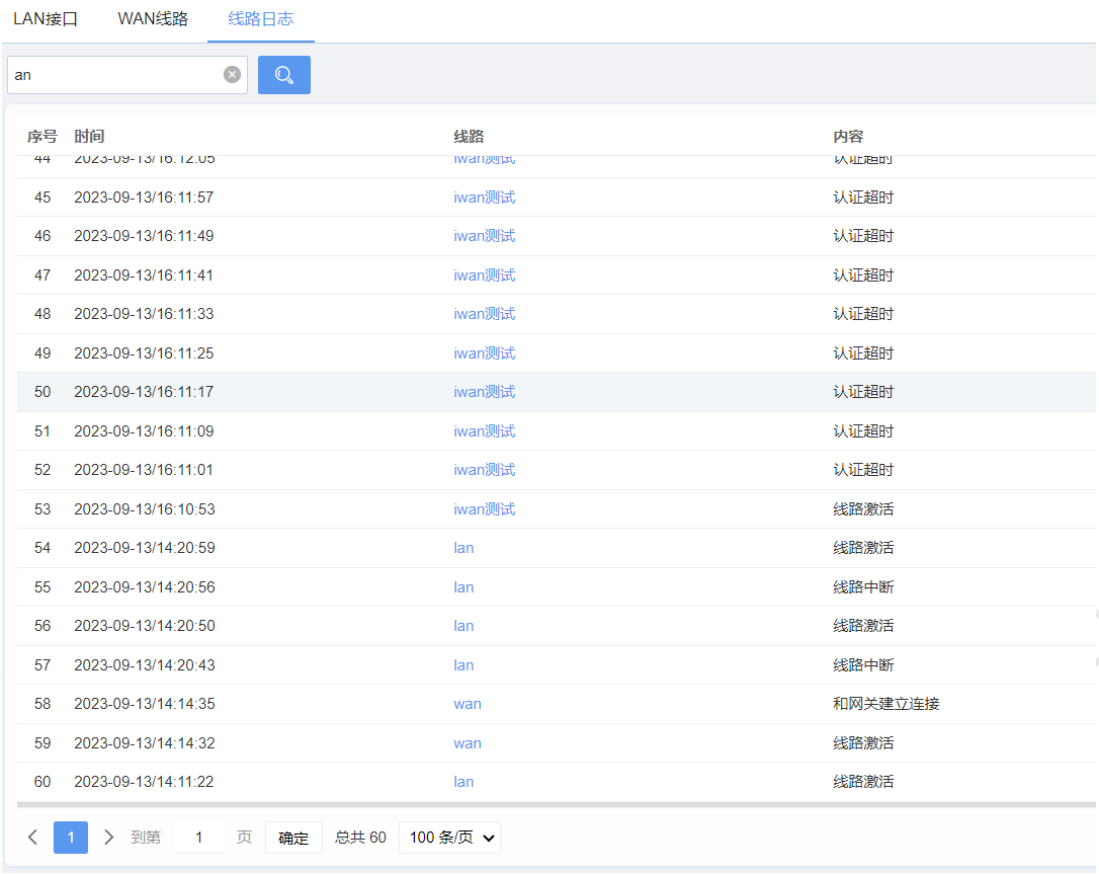


图 4-61 线路日志详情

4.7.4. WAN 群组

WAN 群组可以对多条 WAN 线路进行捆绑，数据包会根据策略分摊到多条 WAN 线路上转发，实现基于连接的多线路负载均衡。WAN 群组的配置，请参见链路负载。

4.7.5. IPv4 路由/NAT

IPv4 路由/NAT 是 Panabit 策略路由的一种，可以根据不同的策略和条件来动态地选择数据包的路径，以满足网络性能、安全性和服务质量的要求。

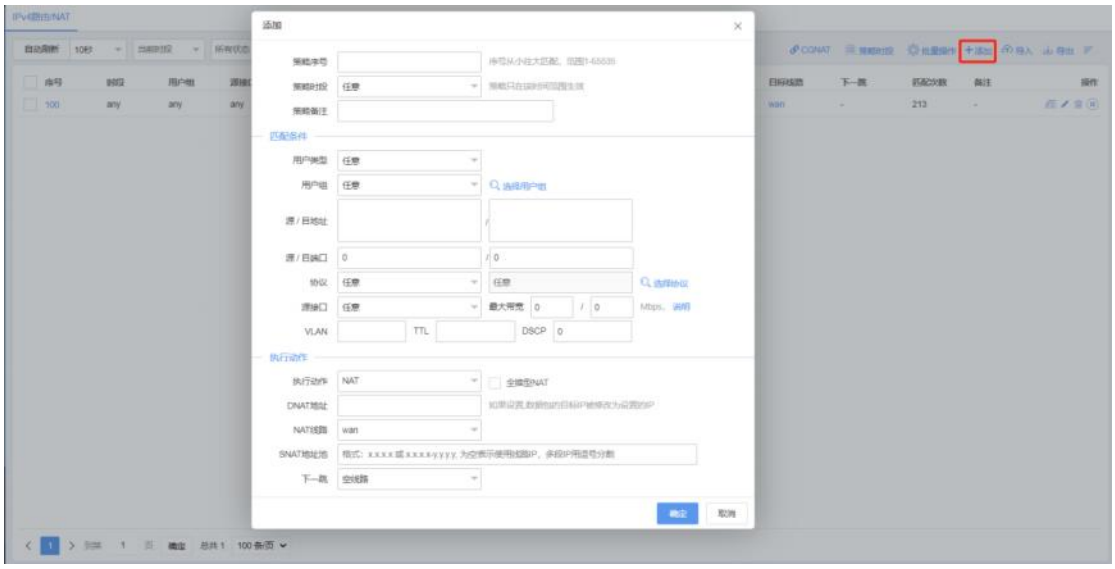
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

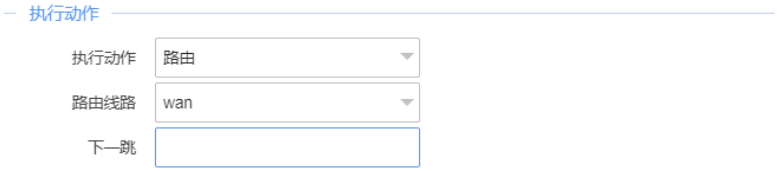
步骤 3 选择【网络管理】>【IPv4 路由/NAT】。

步骤 4 单击页面右上角【添加】，弹出添加策略路由页面。



参数名称	参数说明
策略序号	策略的编号，系统将按照编号从小到大的方式依次执行策略表，该编号不可上下移动。 取值：1~65535。编号越小，优先级越高。
策略时段	设置策略生效的时间范围。
策略备注	对该策略的补充说明。
用户类型	可设为代拨用户、非代拨用户，或者任意。
用户组	用户组织架构中的分组，详见组织架构。
源/目的地址	源地址：匹配源 IP 地址，该地址为 xxx.xxx.xxx.xxx/nn 或 n.n.n.n-m.m.m.m 或是 IP 群组、用户组、用户账号。 目的地址：匹配访问目标 IP 地址，该地址为 xxx.xxx.xxx.xxx/nn 或 n.n.n.n-m.m.m.m 或是 IP 群组。
源/目的端口	源端口：匹配源 IP 的端口号。 目的端口：匹配访问目标服务的端口号。
协议	传输协议：对传输层协议进行匹配，可选择 TCP、UDP、ICMP。 应用协议：对应用进行匹配，该“应用协议”为 Panabit 自身携带的应用特征库，可以选择协议库的某一个应用或某一个分类。
源接口	选择某个内网物理接口或逻辑 LAN 接口进行匹配。
最大带宽	如果参数不为 0，表示当目标线路下行流量超过设定的最大带宽参数时

	该策略路由自动失效，会继续匹配下一条路由策略。
VLAN	匹配数据报文的 VLAN-Tag，0 表示对任意 VLAN 均有效。
TTL	匹配数据包的 TTL 值。
DSCP	匹配 DSCP 值。
执行动作	当数据报文与上述的策略条件相匹配后所执行的动作。匹配策略路由的会话，会做 NAT、DNAT、CGNAT、路由、走代拨其中一种动作。 NAT：指对匹配会话的数据包进行源地址转换，并从指定的线路进行数据转发。 ● 全锥型 NAT：从内网的｛IP:端口｝发送出来的请求，NAT 设备会为之分配一个固定的公网｛IP:端口｝，同时产生一个内网主机的内网｛IP:端口｝与公网｛IP:端口｝映射关系，任何一个外网主机都可以通过这个公网｛IP:端口｝，实现访问位于内网的主机设备功能。 **说明** Panabit 的全锥型 NAT 特性如下： 1. 目标端口为 1024 以下的会话，不会触发全锥型 NAT 动作，即便策略里指定了也不生效。 2. 针对一些知名目标端口，如 5353，1900，也会忽略。 3. 如果会话触发了全锥形 NAT 策略，Panabit 在做 SNAT 的同时，将外网 IP 和 NAT 端口动态映射到内网 IP 和内网端口上，这个映射在这条触发映射的会话周期内一直存在，可通过命令 **floweye dynpm config ttl=xxx** 调整映射老化时间。 4. 动态端口映射条目有限制，与设备型号有关系。使用 floweye dynpm stat 可以查看当前已经分配条目（count）和支持的最大条目（pool_size）； 5. 如果内存允许，可以在/etc/PG.conf 里通过设置 DYNPM_POOLSZ 变量来扩大最大可支持的动态端口映射条目。 ● NAT 线路：可以选择 WAN 线路、WAN 线路群组 、“空线路”，选择“空线路”表示数据从网桥转发 。 ● SNAT 地址池：x.x.x.x 或 x.x.x.x-y.y.y.y，为空则表示使用线路 IP，多段 IP 用逗号隔开。 ● 下一跳：指定数据转发的下一跳。下一跳为空，动作后的数据报文则向路由线路的网关地址转发。如果不为空，数据报文则向所选择线路的网关转发。

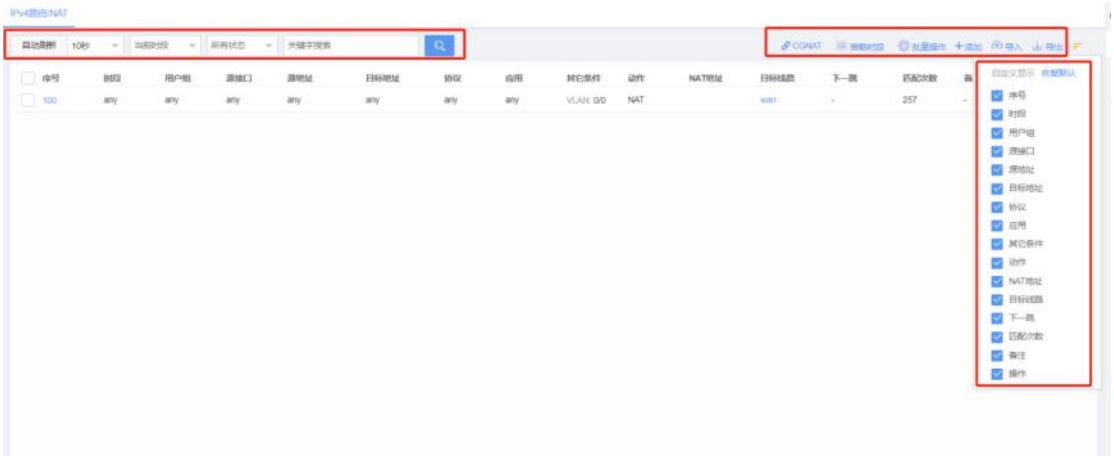
	DNAT：源地址被转换为 WAN 线路的地址，并且目标地址被转换成 DNAT 地址选项框内的地址，DNAT 地址选项框如果不填目标地址则被转换成 WAN 线路网关地址。 ● DNAT 地址：如果设置，数据包的目标 IP 被修改为设置的 IP。 CGNAT：源地址和源端口按照 CGNAT 的设置规则进行转换。参见 CGNAT 设置。 路由：对匹配会话的数据包不改变其源地址，并从指定的线路进行数据转发。  ● 路由线路：可以选择 WAN 线路，或者一个 LAN 接口。 ● 下一跳：指定数据转发的下一跳。LAN 线路是没有网关的，所以要填写 LAN 对端的互联地址。 走代拨：匹配了代拨策略的用户进行源地址转换，并从相应的代拨线路做数据转发。

步骤 5 单击【确定】。

说明

1. 一般情况下，需要添加一条默认路由，即条件均为 any，执行动作为 NAT 至 WAN 线路的路由，保证用户能够正常上网。
2. 策略路由的匹配顺序为按序号从小到大进行匹配，为方便添加其他路由，默认路由的序号需尽可能大。
3. 添加策略路由后，可以在页面中查看策略的匹配次数，对策略的操作（添加、禁用、启用等）会重置所有路由的匹配次数。

成功添加后，可以在【IPv4 路由/NAT】页面查看路由详情。



参数名称	参数说明
自定义显示	鼠标悬停或单击 后，可勾选需要在列表中呈现的信息。
自动刷新	线路详情的刷新时间，可选择不刷新或以 5s/10s/20s/60s 为周期进行刷新。
条件搜索	可根据生效时段、路由状态以及路由关键字筛选符合条件的线路。
CGNAT	进入 CGNAT 设置。
策略时段	设置策略生效的时段，可在添加策略路由时调用。 
批量操作	对选中的路由进行批量操作，可进行禁用、启用、删除。
添加	添加一条策略路由。
导入	根据配置文件，导入策略路由。

	
导出	导出当前策略路由的配置文件，可下载至本地。

——结束

4.7.6. IPv6 路由

与 IPv4 路由类似，IPv6 路由也属于策略路由的一种，模块不涉及 NAT。

说明

配置 IPv6 策略路由前，请选择【应用识别】>【引擎参数】，开启 IPv6 流量识别。

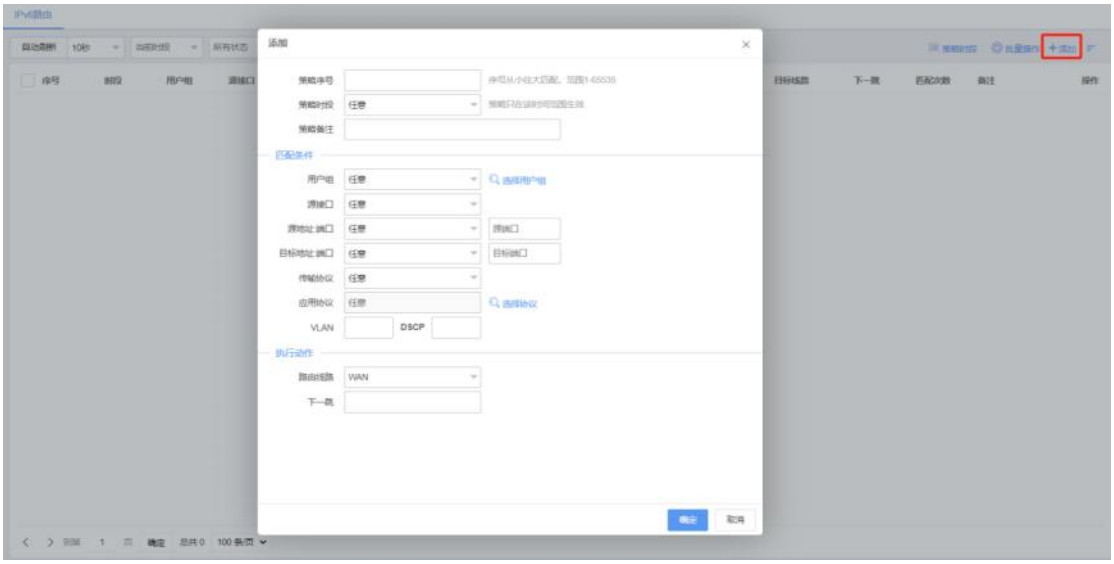
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【IPv6 路由】。

步骤 4 单击页面右上角【添加】，弹出添加策略路由页面。



参数名称	参数说明
策略序号	策略的编号，系统将按照编号从小到大的方式依次执行策略表，该编号不可上下移动。 取值：1~65535。编号越小，优先级越高。
策略时段	设置策略生效的时间范围。
策略备注	对该策略的补充说明。
用户组	用户组织架构中的分组，详见组织架构。
源地址:端口	源地址：匹配源 IP 地址，该地址为网络/前缀或 IP 群组。 源端口：匹配源 IP 的端口号。
目标地址:端口	目标地址：匹配访问目标 IP 地址，该地址为网络/前缀或 IP 群组。 目标端口：匹配访问目标服务的端口号。
传输协议	对传输层协议进行匹配，可选择 TCP、UDP、ICMP。
应用协议	对应用进行匹配，该“应用协议”为 Panabit 自身携带的应用特征库，可以选择协议库的某一个应用或某一个分类。
VLAN	匹配数据报文的 VLAN-Tag，0 表示对任意 VLAN 均有效。
DSCP	匹配 DSCP 值。
执行动作	当数据报文与上述的策略条件相匹配后所执行的动作，该模块为“路由”。 ● 路由线路：可以选择 WAN 线路，或者一个 LAN 接口。 ● 下一跳：指定数据转发的下一跳。LAN 线路是没有网关的，所以要填写 LAN 对端的互联地址。

步骤 5 单击【确定】

——结束

4.7.7. 端口映射

4.7.7.1. 概述

通过建立内外网地址与端口号的映射关系，使外网用户可以通过特定的外网地址和端口号来访问内网资源。这种映射关系是通过进行端口映射来实现的，即在网络地址转换（NAT）线路上开放指定的端口，并配置该端口收到的数据包应该被转发到内网的特定 IP 地址和端口。这样一来，外网用户就能够直接访问内网的资源。同样，为了确保内网资源的可访问性，需要在内网上相应地开放相应的端口或服务。

须知

因为端口映射是外网地址和内网地址建立映射关系，所以使用该功能时，一般情况下，外网地址需要为公网地址，上网行为管理设备要作为网关进行使用。

说明

1. 从外网发起方的角度看，其做了目标 IP 或者目标 IP+目标端口的转换。从 Panabit 自身角度上看，内网服务器仍然是使用从内到外的NAT模型，仍然是从内到外的源地址转换。因此我们在连接信息里看到映射会话的首包接口是某个 LAN 接口。
2. 端口映射回流 

开启后，内网用户通过公网 IP 访问内网服务器时，直接走内网转发；如果没有开启回流，数据包就会先转发到运营商，再从运营商回到 Panabit 上，Panabit 再回给内网用户。

4.7.7.2. 应用案例

某用户网络拓扑如下图所示。需要将小派 AP 的管理地址+端口（192.168.25.9:443）映射至外网地址+指定端口（192.168.6.220:8443）。通过外网对小派 AP 的管理地址进行远程访问。

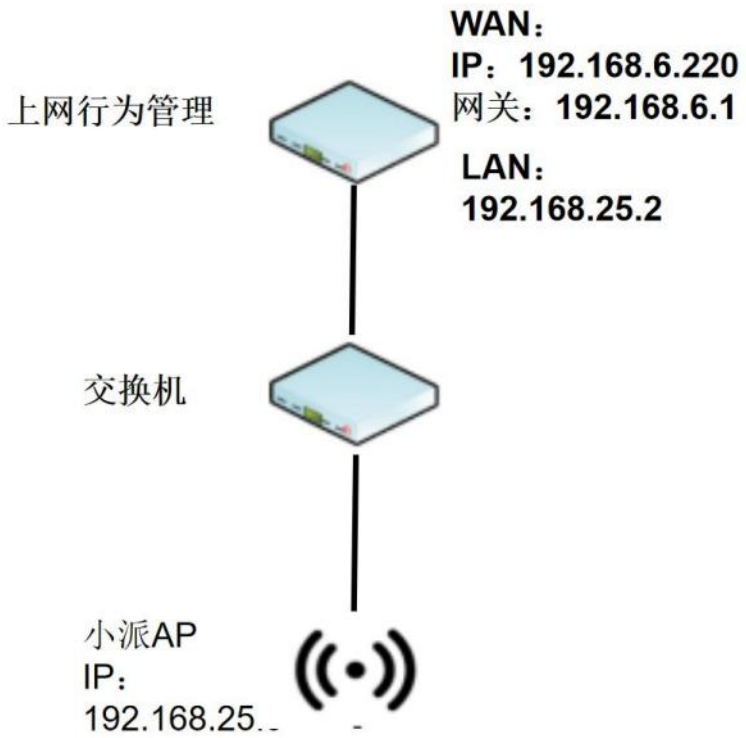


图 4-62 案例拓扑

4.7.7.3. 配置步骤

4.7.7.3.1. 配置 WAN 线路

通过此操作，配置 WAN 线路，具体操作请参见配置 WAN 线路。

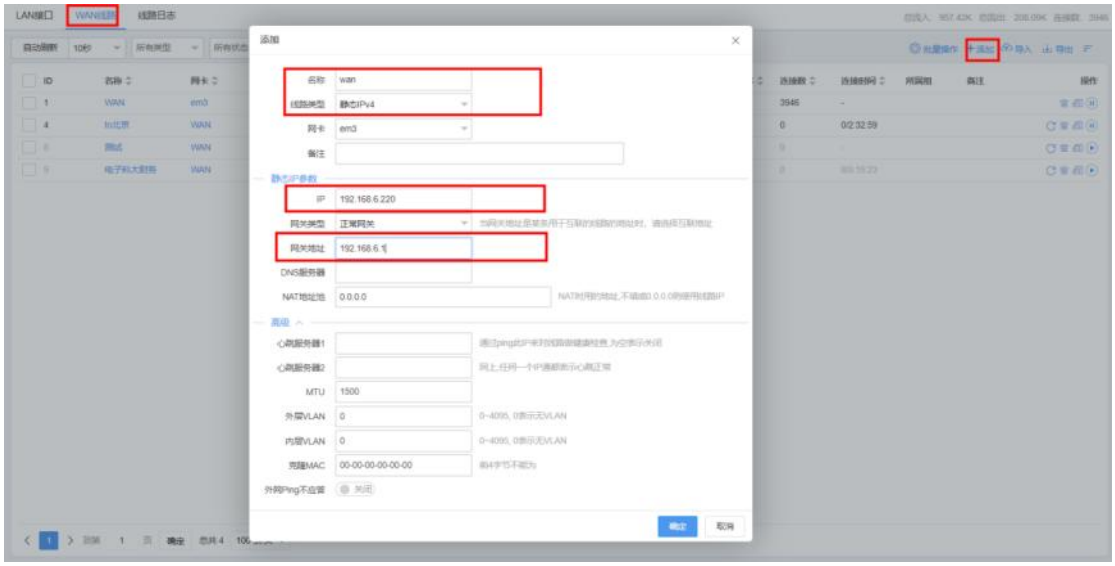
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【LAN/WAN】>【WAN 线路】。

步骤 4 单击页面右上角【添加】，新增 WAN 线路。



配置示例：线路名称设为“wan”，线路类型设为“静态 IPv4”，IP 设为“192.168.6.220”，网关地址设置为“192.168.6.1”。

步骤 5 单击【确定】。

——结束

4.7.7.3.2. 配置 LAN 线路

通过此操作，添加一条 LAN 线路，被映射的主机应当指向此 LAN 接口作为主机网关，并保证能正常通讯。

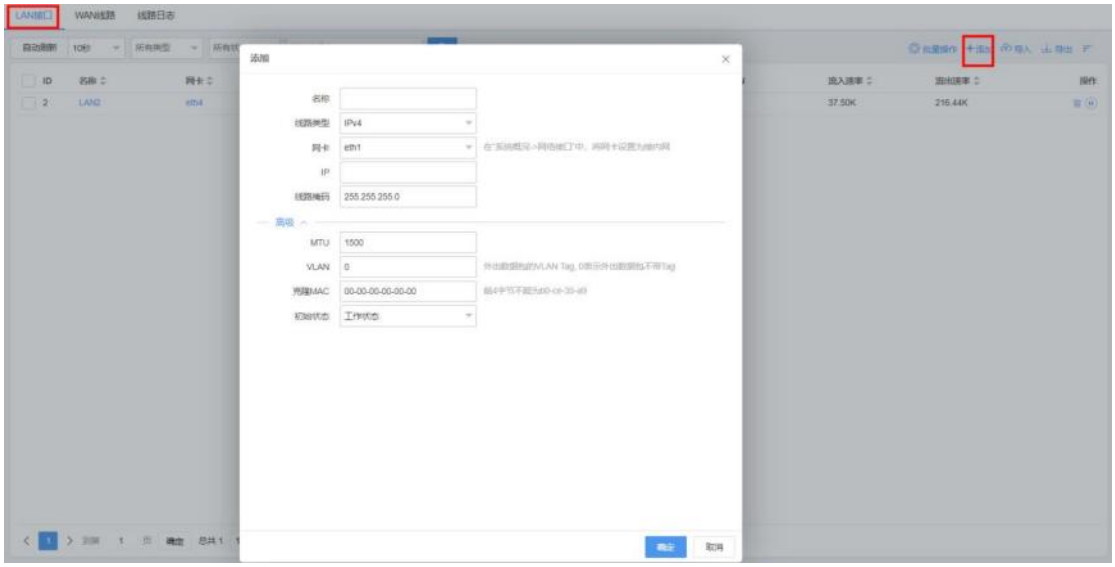
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【LAN/WAN】>【LAN 接口】。

步骤 4 单击页面右上角【添加】，添加 LAN 线路。



配置示例：线路名称设为“lan”，线路类型设为“IPv4”，IP 设为“192.168.25.2”。

步骤 5 单击【确定】。

——结束

4.7.7.3.3. 配置默认路由

通过此操作，添加一条默认路由，使被映射的主机能够正常出网。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【IPv4 路由/NAT】。

步骤 4 单击页面右上角【添加】， 添加默认路由。

配置示例：策略序号设为“100”，条件均为任意，执行动作选择“NAT”，NAT 线路选择上面步骤中创建的“wan”。

步骤 5 单击【确定】。

——结束

4.7.7.3.4. 配置端口映射

通过此操作，添加端口映射策略。

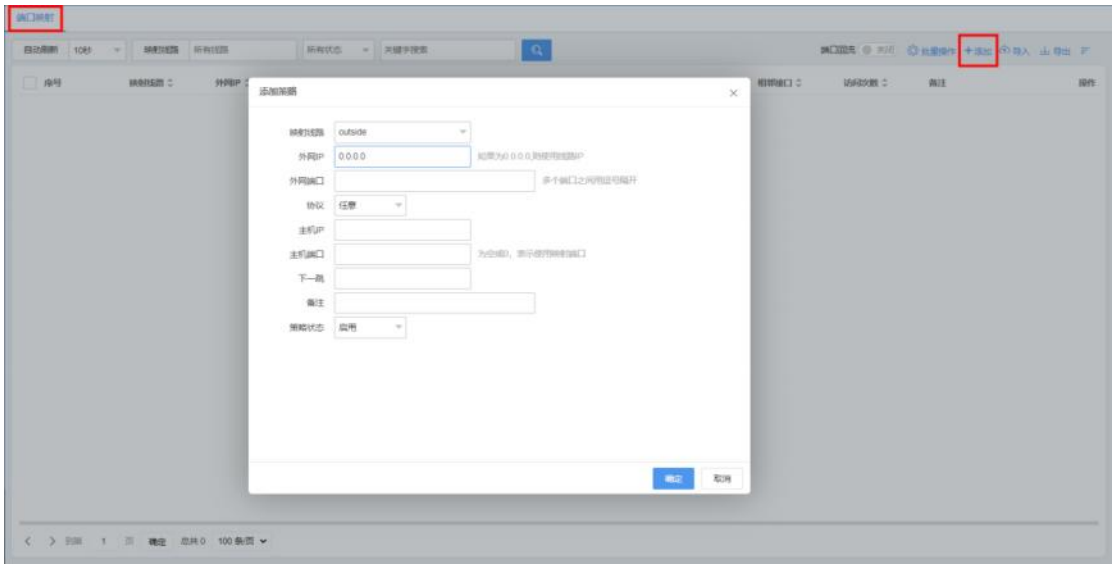
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【端口映射】。

步骤 4 单击页面右上角【添加】，添加端口映射策略。



参数名称	参数说明
映射线路	选择需要建立对应映射关系的 WAN 线路。
外网 IP	默认 0.0.0.0，即使用 WAN 线路 IP。如 WAN 线路有多个公网 IP 可以进行填入指定。
外网端口	选择需要映射的公网端口可以用（设置不连续端口用逗号分隔，设置连续端口用短横线连接，例如 80,8080 或 8081-8090）。
协议	选择 TCP 或者 UDP，任意为所有协议。
主机 IP	需要映射的内网主机 IP。
主机端口	需要映射的内网主机端口。格式参考外网端口，若为 0，则使用外网端口所填写的所有端口。
下一跳	默认为 0.0.0.0，如果内网映射主机的网关不是 Panabit 的 LAN 接口，则需要指定 LAN 接口对端网络设备的 IP 地址
备注	为端口映射添加备注说明。
策略状态	是否启动该规则。

配置示例：我们这里映射派网的小派 AP 为例，小派 AP 主机 IP 为 192.168.25.9，管理界面端口为 443。映射线路选择“wan”，外网端口填写“8443”，主机 IP 填写“192.168.25.9”，主机端口为“443”。

配置好端口映射策略后，外网用户通过 WAN 线路的地址:端口号（192.168.6.220:8443）即可访问小派 AP。

步骤 5 单击【确定】。

——结束

4.7.8. DHCP 服务

4.7.8.1. 概述

DHCP 服务可以给客户机分配动态 IP 地址，并将 IP 地址进行集中管理。分配的 IP 地址有固定的租期时间，超时将收回。支持将为客户机分配的动态 IP 地址与客户机 MAC 绑定，将动态地址转为静态地址。

Panabit 的 DHCP 服务，依赖于 LAN 接口，每个 LAN 接口相当于一个 DHCP 服务器。

4.7.8.2. 配置步骤

4.7.8.2.1. 配置 LAN 线路

通过此操作，添加一条 LAN 线路，作为 DHCP 服务承载线路，LAN 线路 IP 地址为 DHCP 网关地址。

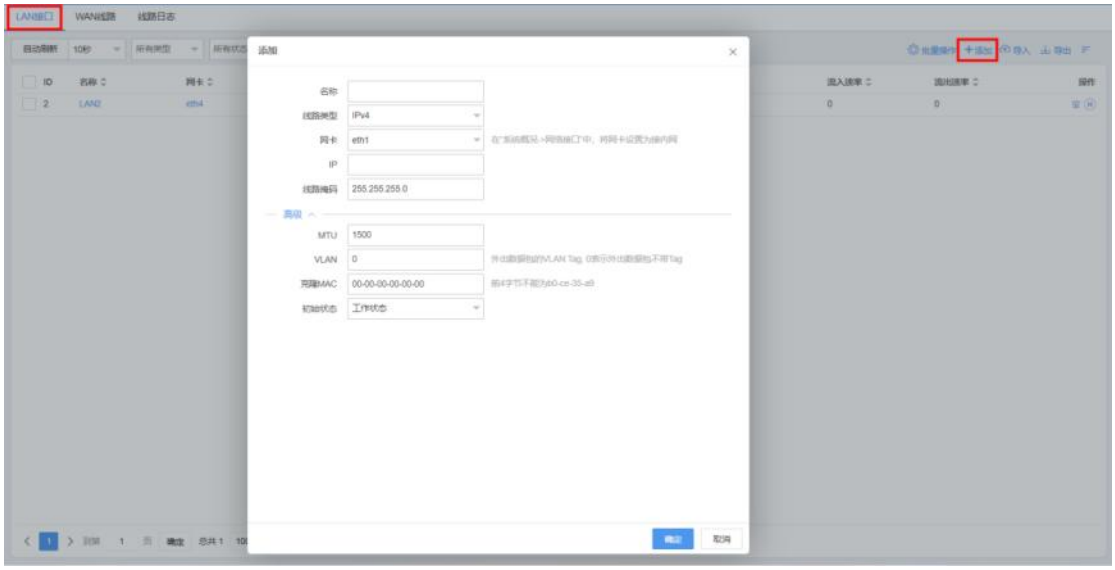
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【LAN/WAN】>【LAN 接口】。

步骤 4 单击页面右上角的【添加】，添加 LAN 线路。



步骤 5 单击【确定】

——结束

4.7.8.2.2. 配置 DHCP 服务

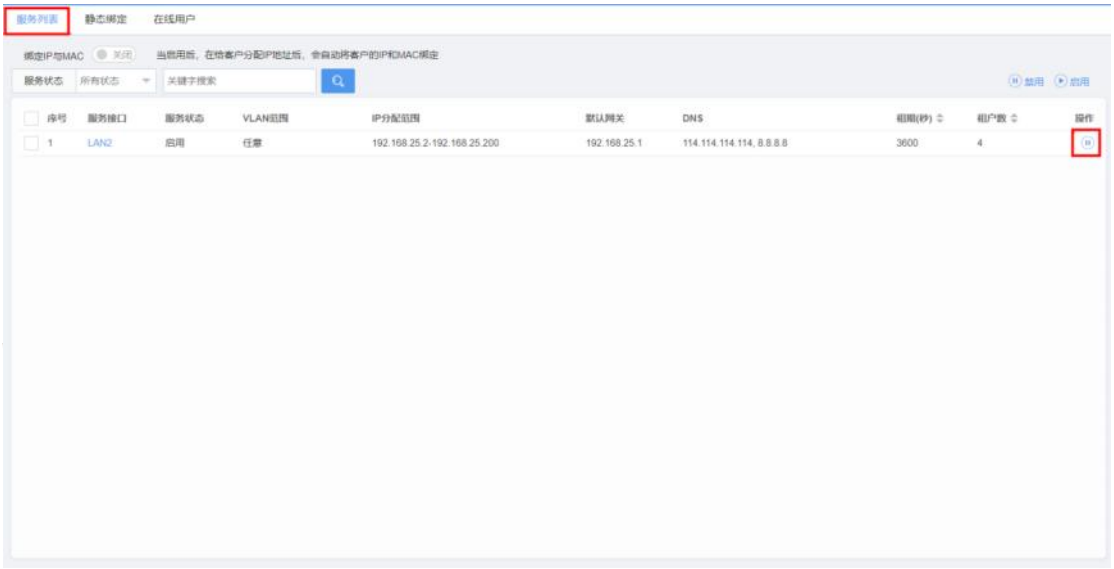
通过此操作开启线路的 DHCP 服务，完成将地址池 IP 地址与客户机 MAC 地址的绑定。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【DHCP 服务】>【服务列表】。

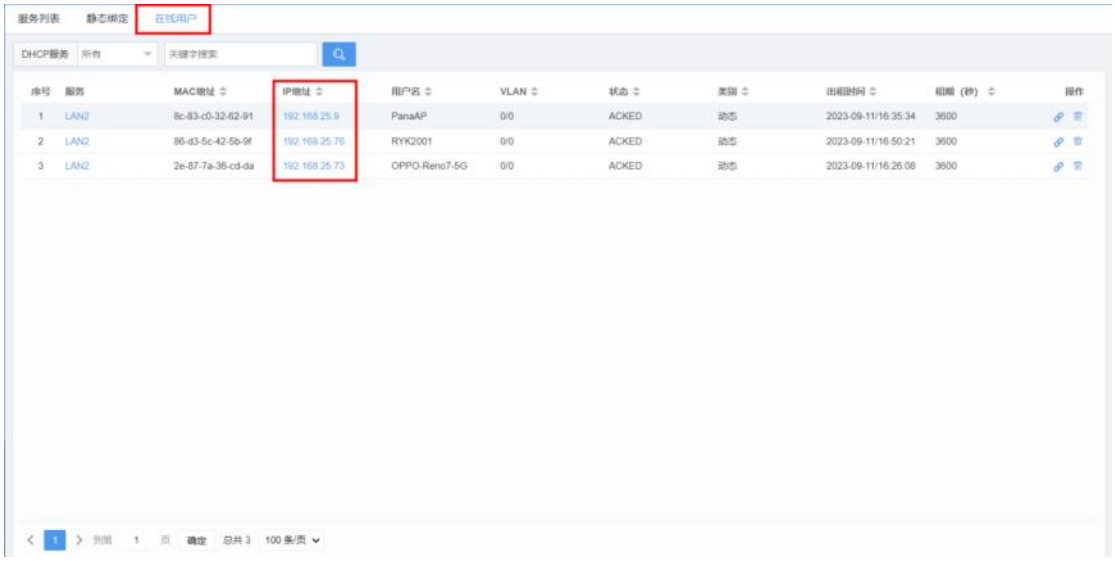


步骤 4 选择已创建的 LAN 线路操作列，开启此线路的 DHCP 服务。

步骤 5 点击服务接口的名称，进入 DHCP 的配置页面进行设置，点击【确定】提交。

参数名称	参数说明
DHCP 服务	开启或关闭此 LAN 口的 DHCP 服务。
VLAN	可以为一个固定值，或者一个范围值，如 100 或 100-200，不填或填 0 表示只响应不带 VLAN 的 DHCP 报文请求。
地址范围	向 DHCP 客户端分配的地址范围。
默认网关	DHCP 服务器分配给客户端的网关。
线路掩码	DHCP 服务器分配给客户端的网络掩码。
DNS1	DHCP 服务器分配给客户端的主 DNS 服务器。
DNS2	DHCP 服务器分配给客户端的次 DNS 服务器。
所属域	DHCP 服务器分配给客户端的域名。
无线控制器	DHCP 服务器分配给客户端的 AC 地址。
租约时间	DHCP 的租约时间。

选择【网络管理】>【DHCP 服务】>【在线用户】，通过【在线用户】可查看分配给客户机的 IP 地址。



——结束

4.7.8.2.3. 配置静态绑定

通过静态绑定， DHCP 服务器将特定的 IP 地址分配给特定的客户端设备，并将此 IP 地址与客户端设备的 MAC 地址绑定在一起。绑定后，特定的客户端设备将始终获得相同 IP 地址，而不是每次都获得一个不同的动态分配的 IP 地址。

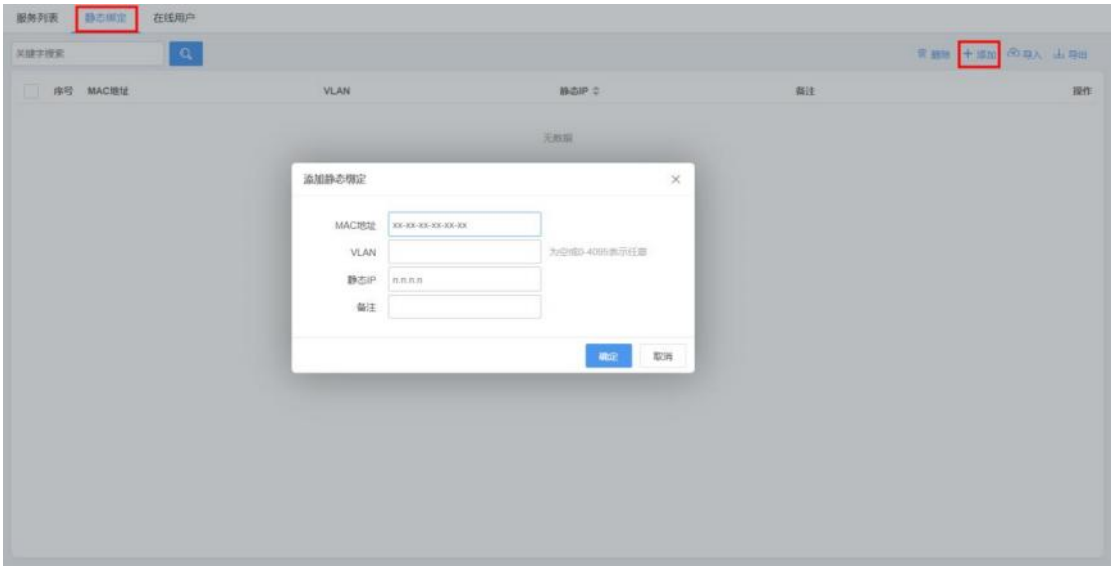
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【DHCP 服务】>【静态绑定】。

步骤 4 单击【添加】，将地址池 IP 地址与客户机 MAC 地址绑定，每次向该 MAC 分配地址时将固定分配静态地址。



参数名称	参数说明
MAC 地址	填写被绑定设备的 MAC 地址。
VLAN	被绑定设备的所属 VLAN。
静态 IP	为被绑定设备固定分配的 IP 地址。
备注	为静态绑定添加说明。

步骤 5 单击【确定】。

——结束

4.7.9. VRRP 联动

4.7.9.1. 概述

VRRP 是虚拟路由冗余协议，主要目的在于解决局域网中配置静态网关出现单点故障的问题。局域网中的多台路由器，通过 VRRP 选举其中一个路由器作为默认出口。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器，它负责转发数据包到这些虚拟 IP 地址。一旦主路由器不可用，备份路由器角色会立即切换为主路由器。

- VRR 报文：只有一种报文：ADV 报文（Advertisement），目的 IP 地址是 224.0.0.18，目的 MAC 地址是 01-00-5e-00-00-12，源 IP 是承载 LAN 接口 IP，源 MAC 是 VRRP 线路的 MAC 的组播报文。
- VRRP 关键的三个配置，优先级（1-255）、VRRP ID、VRRP 抢占。
- VRRP 关键的两个状态，master 和 backup。

Panabit 的 VRRP 工作逻辑：

1. 只有 master 状态才会发送 VRRP ADV 报文，发送间隔为 1s。
2. 默认情况下，Panabit 为 master 状态。
3. 当 VRRP 是 backup 状态时，启动 ADV 报文监控，当收到有价值的 ADV 报文，会刷新超时时间，否则不刷新。ADV 报文超时后，切换到 master 状态；
4. VRRP 抢占只有在 backup 的状态下才起作用，即对比 VRRP ADV 报文中的优先级，当收到优先级比自己低的 VRRP ADV 报文，则不会刷新 VRRP ADV 报文超时时间，等到 ADV 报文超时后，切换到 master 状态。
5. 当两台设备均为 master 状态时，产生选举，选举失败则变成 backup 状态。选举失败的条件有：（优先级大于自己）（优先级等于自己，但是 VRRP 报文源地址大于自己）。
6. 当 backup 切换到 master 时会马上发送一个 ARP 免费报文。

4.7.9.2. 应用案例

某用户网络拓扑如下图所示。两台 Panabit 之间配置一组 VRRP，分别有一条 WAN 线路。正常状态时，主机线路能够正常转发，备机则不转发；当主机 VRRP 主备进行切换时，线路不转发数据；当主备恢复正常时，线路能转发数据。

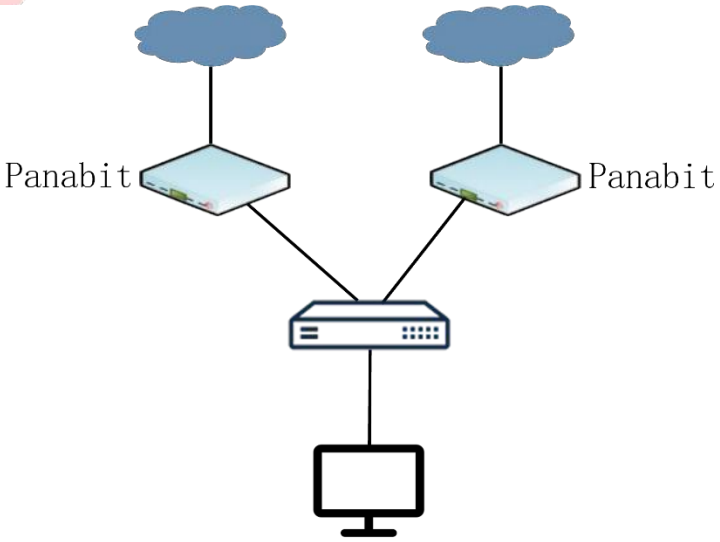


图 4-63 案例拓扑

4.7.9.3. 配置步骤

VRRP 联动需要有主、备两台上网行为管理设备，所有的操作都需要同时在两台设备上进行

配置。

4.7.9.3.1. 配置 LAN 线路

通过此操作，分别为主/备上网行为管理设备建立一条 LAN 线路作为 VRRP LAN 的承载线路。

具体操作请参见 LAN 接口。

4.7.9.3.2. 配置 VRRP 接口

通过此操作，添加 VRRP 主机/备机，配置 VRRP 抢占。

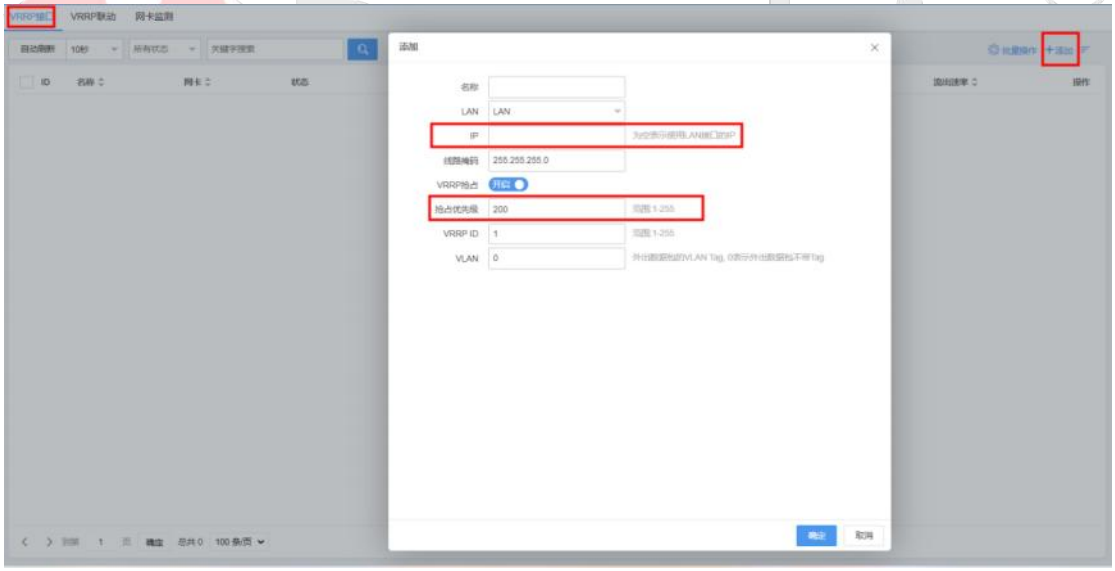
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【VRRP 设置】>【VRRP 接口】。

步骤 4 单击页面右上角的【添加】，新增 VRRP 接口。



参数名称	参数说明
名称	自定义 VRRP 接口名称。
LAN	选择承载 VRRP 接口的 LAN 线路。
IP	VRRP 接口 IP，为空表示使用 LAN 接口的 IP。
线路掩码	接口 IP 的网络掩码。
VRRP 抢占	可设为“开启”或“关闭”。
抢占优先级	取值:1-255，255 为最高优先级，且不会自动抢占。

VRRP ID	取值:1-255
VLAN	外出数据包的 VLAN Tag，0 表示外出数据包不带 Tag

配置示例：主设备 VRRP LAN 设置为“LAN 主”，IP 为“1.1.1.3”，VRRP 抢占为“开启”，抢占优先级为“200”。备设备 VRRP LAN 设置为“LAN 备”，IP 为“1.1.1.3”，VRRP 抢占为“开启”，抢占优先级为“100”。

步骤 5 单击【确定】。

——结束

4.7.9.3.3. 配置 DHCP 服务（可选）

通过此操作，开启主/备设备 VRRP LAN 线路的 DHCP 服务。具体操作请参见 DHCP 服务，分别为主/备设备的 VRRP LAN 线路开启 DHCP 服务。

4.7.9.3.4. 配置 VRRP 联动

通过此操作，分别在主/备设备上开启 VRRP 状态与接口线路的联动功能。

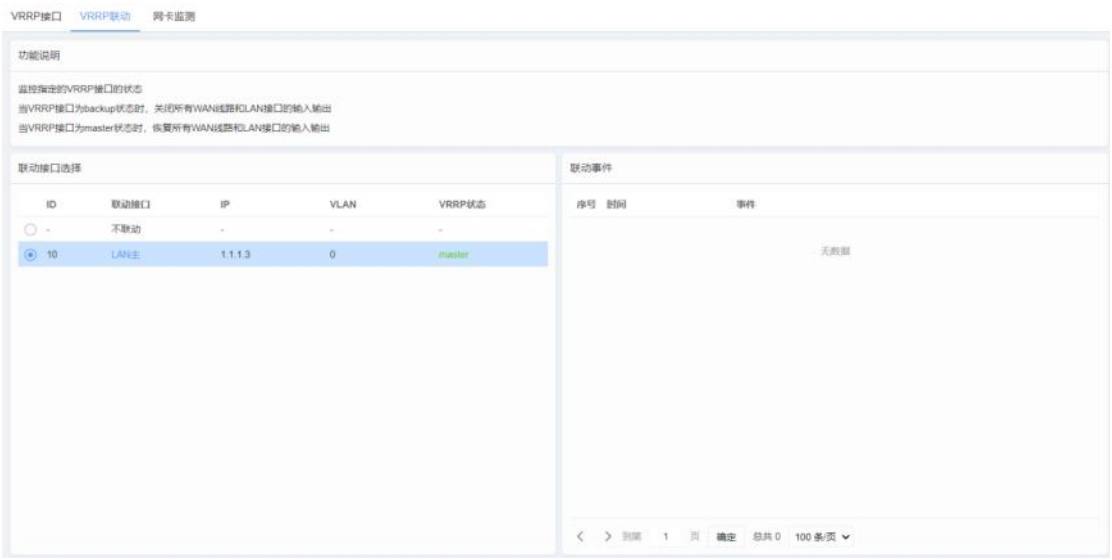
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【VRRP 设置】>【VRRP 联动】。

步骤 4 主备机分别选择配置 VRRP 接口步骤中创建的 VRRP LAN 接口。



说明

【联动事件】中，“待机状态”标识当前主机的 VRRP 为主机模式，“工作状态”表示当前主机的 VRRP 为备机模式。

——结束

4.7.10. CGNAT 设置

4.7.10.1. 概述

CGNAT（Carrier-Grade NAT）主要应用于运营商级的网络地址转换，CGNAT 在实现 NAT 的同时可以大大降低日志量，提升日志溯源的效率。CGNAT 在将私网地址（源地址）转换为指定的公网地址后，源端口也要在一段固定且连续的端口范围内进行转换。

CGNAT 的工作模式有静态和动态两种：

- 静态 CGNAT，手动指定内网 IP 与公网 IP+端口范围的对应关系。在进行 NAT 转换时，列表中指定的源 IP、NAT 后的端口范围，会分配在列表中指定的范围内。
- 动态 CGNAT，自动分配内网 IP 与公网 IP+端口范围的对应关系。在进行 NAT 转换时，会根据 WAN 线路 IP 进行动态分配端口范围并且会生成对应关系表，该功能主要是方便 NAT 后，根据 NAT 的端口来溯源。

4.7.10.2. 配置静态 CGNAT

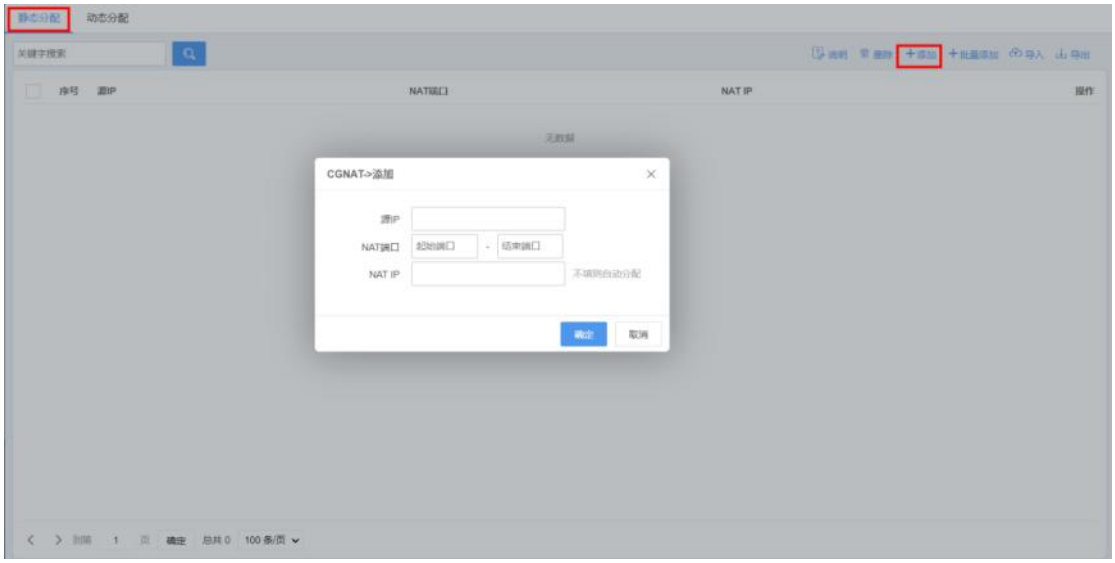
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

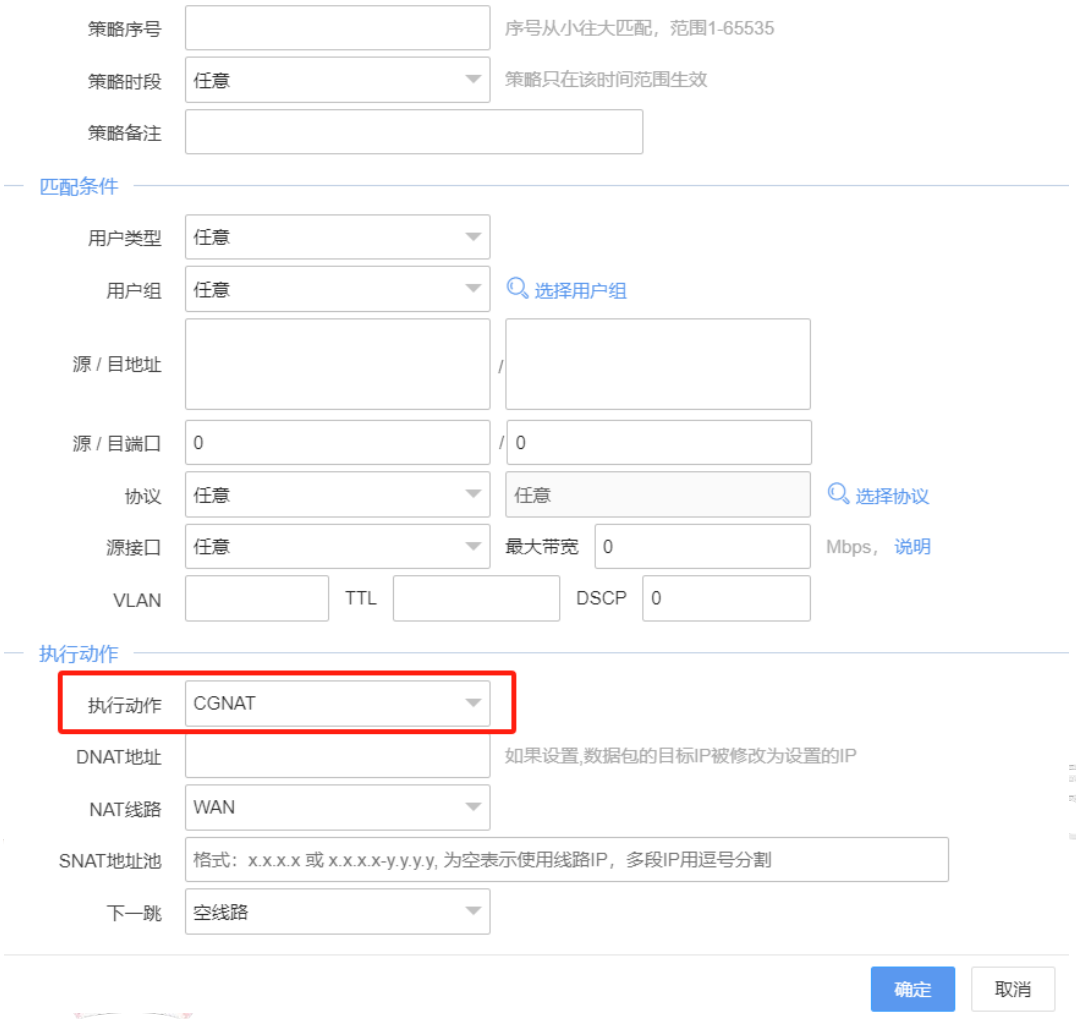
步骤 3 选择【网络管理】>【CGNAT 设置】>【静态分配】。

步骤 4 单击页面右上角的【添加】，弹出新增 CGNAT 页面。



参数名称	参数说明
源 IP	内网 IP。
NAT 端口	指定端口号区间。
NAT IP	填写 NAT IP。

步骤 5 选择【网络管理】>【IPv4 路由/NAT】，单击页面右上角【添加】，弹出添加策略路由页面。



步骤 6 选择匹配条件，匹配条件需包含步骤 4 中设置的内网 IP，执行动作需选择“CGNAT”，NAT 线路为步骤 4 中填写 NAT IP 所在的 WAN 线路，单击【确定】。

——结束

4.7.10.3. 配置动态 CGNAT

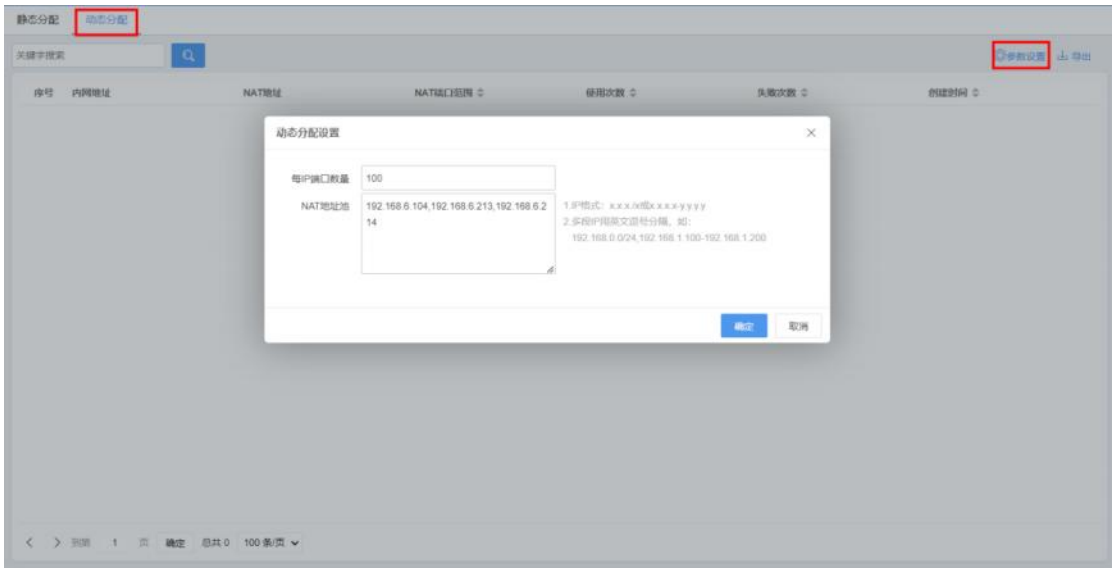
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【CGNAT 设置】>【动态分配】。

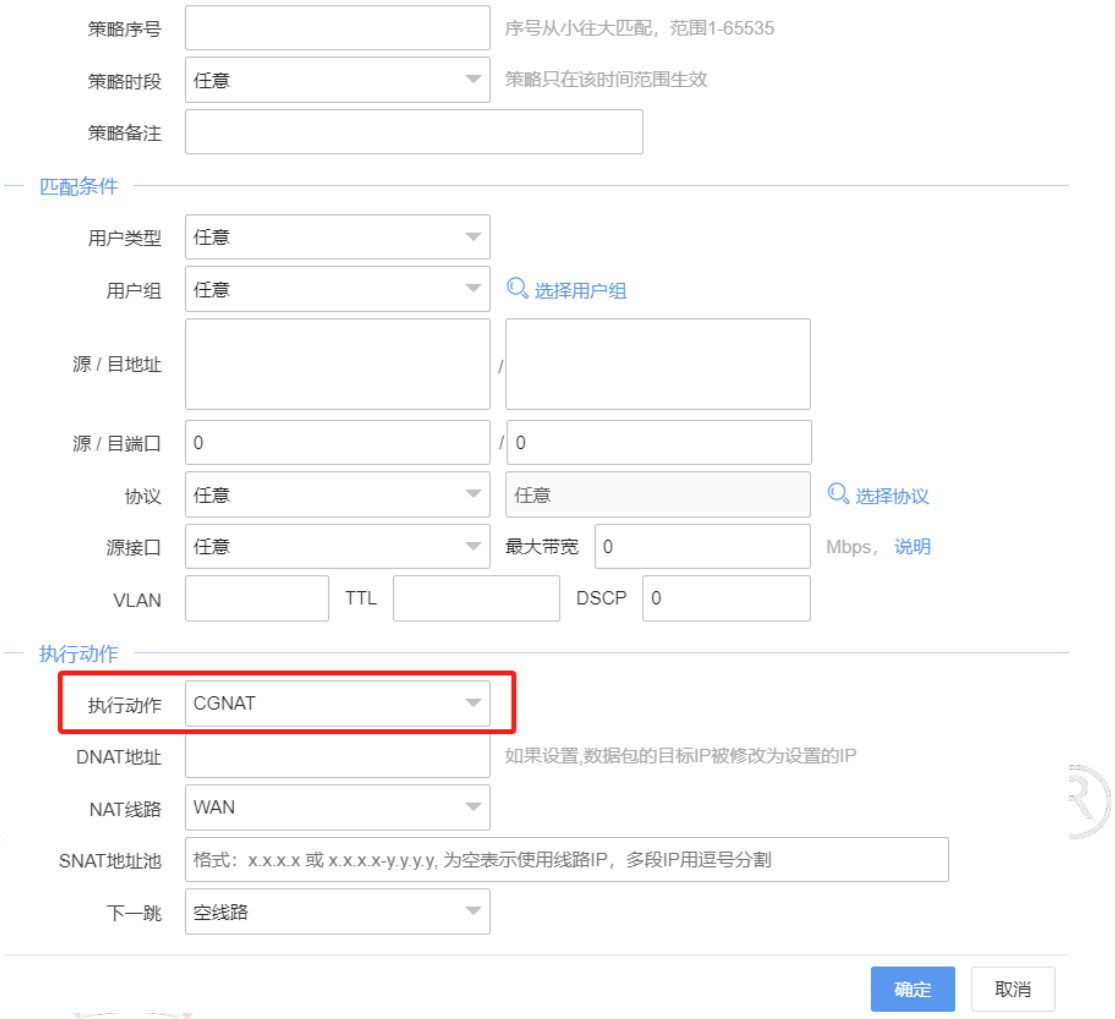
步骤 4 单击页面右上角的【参数设置】，弹出动态分配设置页面。



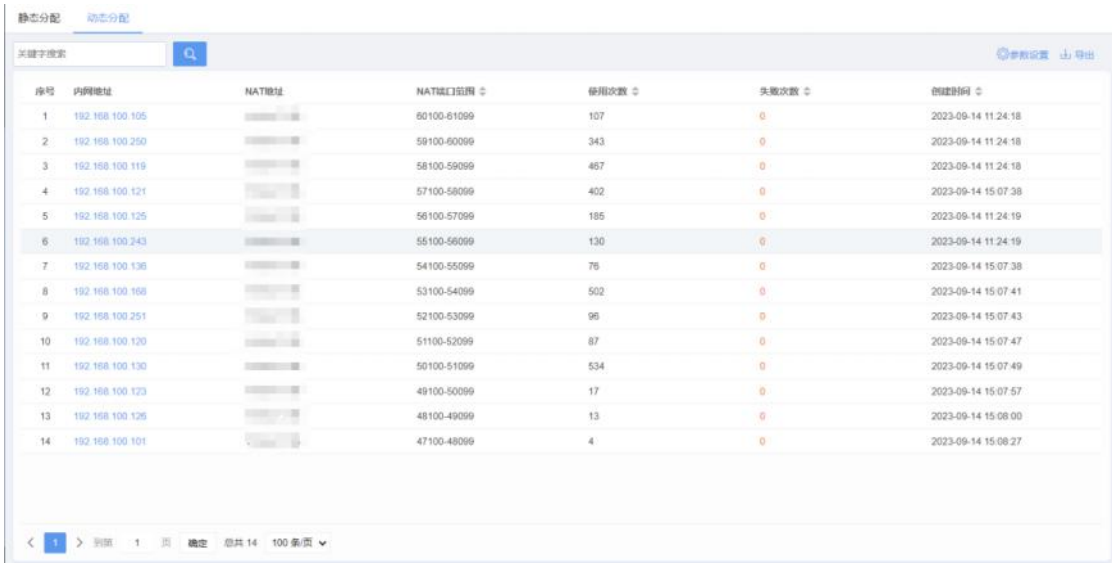
参数名称	参数说明
每 IP 端口数量	端口数量少于 100 时，系统会自动默认为 100。
NAT 地址池	● IP 格式：x.x.x.x/x 或 x.x.x.x-y.y.y.y ● 多段 IP 用英文逗号分隔，如：192.168.0.0/24,192.168.1.100-192.168.1.200

步骤 5 选择【网络管理】>【IPv4 路由/NAT】。

步骤 6 单击页面右上角【添加】，弹出添加策略路由页面。



步骤 6　选择匹配条件，执行动作需选择“CGNAT”，NAT 线路为步骤 4 中填写 NAT 地址池所在的WAN线路，单击【确定】。回到【动态分配】，可查看NAT地址与端口分配的具体情况。



——结束

4.8. WEB 认证

4.8.1. 概述

Panabit 上网行为管理的 WEB 认证模块，主要对网络接入的终端设备进行身份认证，未通过认证的用户不允许出网，为网络资源的设备提供足够的保护，从而来降低网络安全风险。Panabit 支持本地认证、短信认证、微信认证，并支持结合 AD 域和 LDAP 等多种认证方式。认证功能在网关模式和网桥模式下可以使用。

4.8.1.1. WEB 认证一般流程

当用户访问网络时，通过普通的浏览器就能进行准入的身份认证，用户在使用浏览器上网时，会强制访问到认证服务器即 Portal 服务器进行身份认证，只有身份认证通过后，才能访问网络资源。

下图是标准 Web 认证的流程图，便于我们理解 Web 认证如何完成工作，工作流程如下：

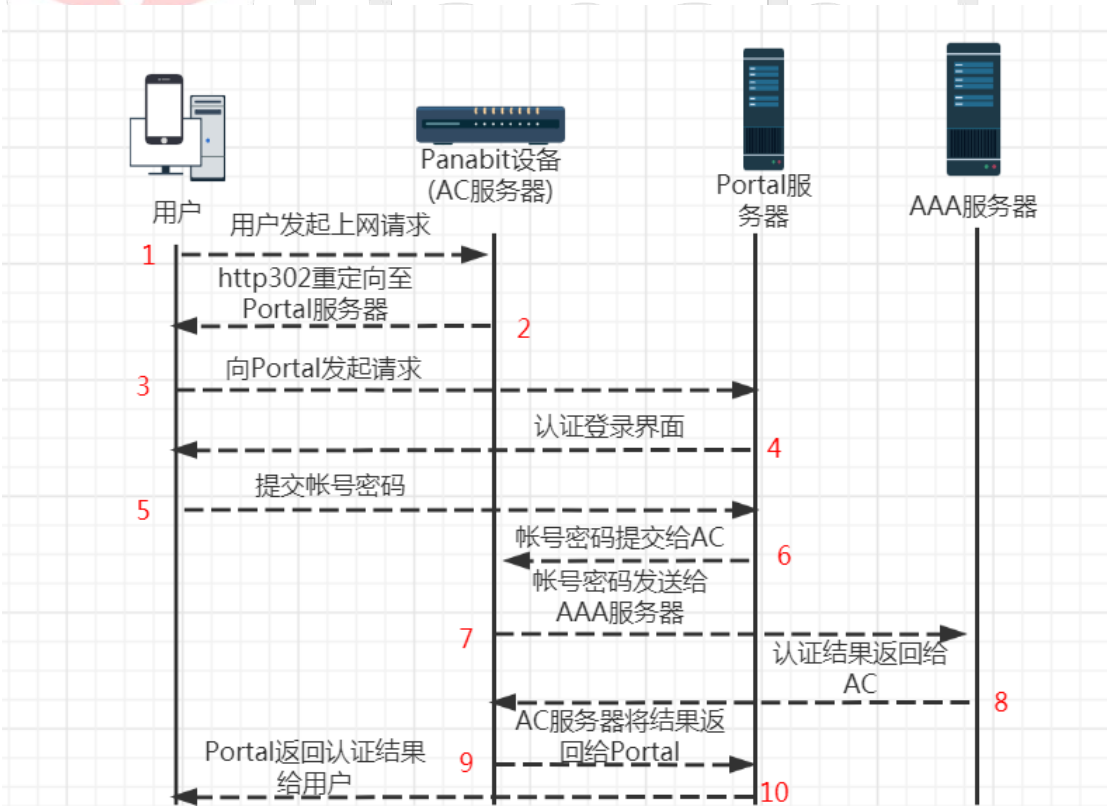


图 4-64 WEB 认证流程图

参数序号	参数说明

<注释 1>	用户连接网络发起上网请求，且经过上网行为管理设备，HTTPS 请求会把 client hello 转发给内部 SSL Server 接口。
<注释 2>	上网行为管理设备进行判断，如未完成认证，发送 HTTP 302 重定向 URL 给用户进行认证，HTTPS 会将自己颁发的证书域名发送给用户，这里需要注意，我们访问的域名必须是真实存在的域名，否则重定向无法完成，如是 HTTPS 域名，电脑和手机端浏览器都会弹出证书告警。
<注释 3>	用户向 Portal 发起请求，如是 HTTPS 域名，之前弹出的警告需选择继续浏览。
<注释 4>	Portal 返回认证信息界面给到用户。
<注释 5>	用户输入需填写的相关内容，进行认证，如是 HTTPS 域名，之前弹出的警告需选择继续浏览才能收到认证信息界面。
<注释 6>	Portal Server 向 Panabit 上网行为管理设备请求，请求中携带用户名和密码等关键信息。
<注释 7>	上网行为管理设备发送 Access-Request 请求给 AAA 服务器，如是本地认证则内部完成账号认证。
<注释 8>	AAA 服务器响应 Access-Accept，返回认证结果给 Panabit 设备，如是本地认证则内部完成账号认证。
<注释 9>	上网行为管理设备将结果返回给 Portal。
<注释 10>	Portal 将认证结果返回给用户。

表 4-56 WEB 认证流程说明

4.8.1.2. 认证涉及设备清单

在上面的认证流程中，涉及以下四类设备角色，如下表所示。

设备角色	用途	设备/系统
用户	上网用户	PC、手机等终端
接入控制器	用于判断用户是否完成认证，发送 HTTP 302 重定向到 Portal Server 的 URL	Panabit 上网行为管理设备
Web Portal 服务器	给用户提供登录用户密码的提交 URL，并回应确认收到认证结果，向 AC 设备发起认证请求。	1. Panabit 管理口提供 Portal 服务。 2. 独立 CMCCportal 提供 Portal 服务。

		3. 其他 Portal 服务器。
AAA 服务器	用于存储用户账号，到期时间、计费套餐等信息。	1. Panabit 本地认证。 2. RAAS 认证计费系统。 3. 其他 AAA 系统。

4.8.1.3. WEB 认证基本参数

Panabit 的 WEB 认证功能，需要通过在应用商店安装【WEB 认证】APP 来实现。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名和密码，登录 WEB 控制台。

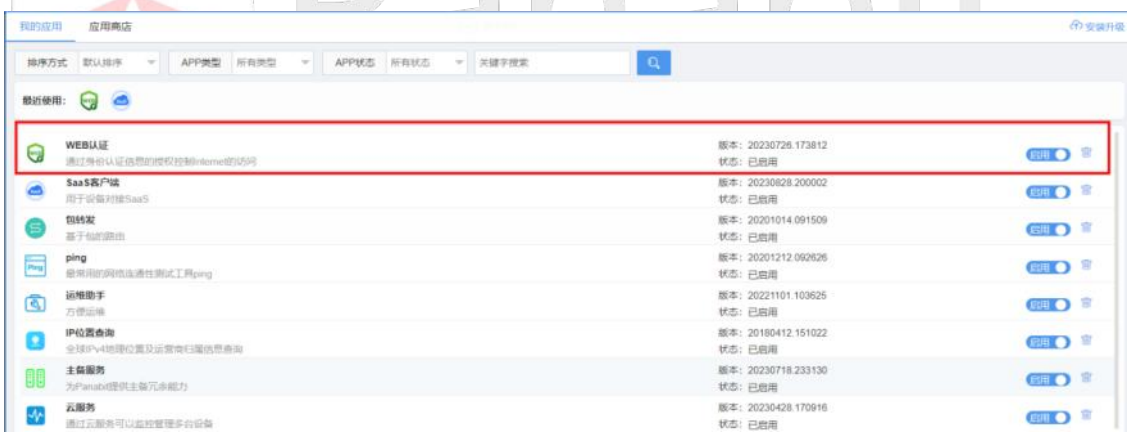
步骤 3 选择【流量概况】>【应用商店】>【应用商店】。

步骤 4 在 APP 列表找到“WEB 认证”APP，单击【安装】。

说明

应用商店 APP 的安装，需要管理口能连接外网。

步骤 5 选择【流量概况】>【应用商店】>【我的应用】，启用 WEB 认证。



步骤 6 单击【WEB 认证】名称，弹出功能配置界面。

参数名称	参数说明
Web 认证	可选择“打开”或“关闭”。开启后未认证的用户会话不允许通过 Panabit。
去掉 URL 中的客户端 IP	在生成中的 URL 去掉客户端的 IP，主要用于解决 URL 导致微信白屏问题。
HTTPS 跳转	可选择“打开”或“关闭”。打开后支持 https 页面的跳转。
免认证 IP	可以选择一个 IP 群组，会话的源地址或目的地址如属于这个群组，那么会话被允许通过 Panabit。
免认证 MAC	添加 MAC，在免认证 MAC 地址表内的 MAC 会话运行通过 Panabit
免认证协议	默认为空，可选择特征库协议或自定义协议，选择协议后，会话如果属于这个协议，那么允许此会话通过 Panabit。
成功后显示页面	认证成功后显示指定页面，如为空则显示原始页面。
登录后弹出注销页面	选择“是”浏览器右下角会有一个弹框，用户认证后可以通过关闭弹 框主动下线；选择“否”用户 IP 无流量后自动下线。
账号登录错误限制	设置多少秒内输入错误 3 次后拒绝登录。
多账号登录限制	设置“是”，后续登录相同账号不能登录，选择“否”后续登录相同账号会踢掉之前登录的账号。
关闭修改密码功能	客户端登录时无修改密码框。

不允许找回密码	只针对 RASS 为 AAA 计费时使用，用户无法通过找回密码界面找回密码。
PortalURL	认证 Portal 的 URL 地址，默认使用管理口 Portal 的 URL。
PortalIP	授权管理权限 Portal 服务器，比如第三方认证服务器对用户发送下线指令，如果不是所填，不响应指令。
本地账号	用户信息放在本机Panabit，在【对象管理】>【账号管理】里添加账号。
Radius 认证	与第三方 radius 服务器对接认证。
AD/LDAP	与 AD 域服务器对接认证。
第三方认证	通过修改 PortalURL 的选项激活，认证的 portal 页面地址，默认为本地认证 界面，即本地认证；使用第三方 portal 页面地址后自动切换到第三方认证。
手机短信认证	通过与手机短信平台对接，通过手机号码与短信验证码认证上网。
微信认证	与微信公众号对接进行认证，主要目的是让用户关注公众号。

须知

1. 配置时，首先需满足在不开认证的情况下，客户端都能上网。
2. WEB 认证服务模块均和管理口有关，因此客户端和管理口 IP 必须能通讯。
3. 与第三方对接时，Panabit 提供 API 接口，第三方必须和 API 接口对接。

4.8.1.4. WEB 认证其他参数

通过 Web 认证，还可记录用户的 MAC 地址，并对认证界面进行配置和管理。

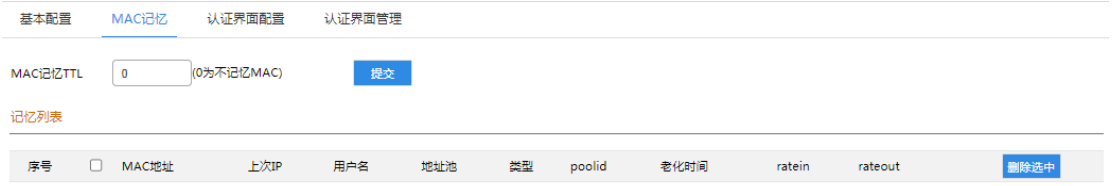


图 4-65 MAC 记忆详情

图 4-66 认证界面配置详情

图 4-67 认证界面管理详情

参数名称	参数说明
MAC 记忆	当某用户认证成功后，记录该用户的 MAC，只要用户在上网行为管理设备没有下线，即使该用户更换了 IP 地址，也无需重新认证。
认证界面配置 / 管理	可以对本地的认证页面做自定义处理，比如背景，认证框显示位置等等。

表 4-57 WEB 认证其他参数说明

4.8.2. 应用场景

4.8.2.1. 统一实名认证管理

Panabit 上网行为管理支持本地用户名密码认证、Portal 认证、结合 AD 域和 Radius 等多种认证方式，满足用户统一认证需求。同时可与市面主流的 AAA 系统实现对接。

4.8.2.2. 网监对接

Panabit 上网行为管理满足无线上网场所与当地网监部门对场所的监管要求。实现上网行为管理、用户认证、网监对接一体化方案，降低各设备对接难度。满足当地网监部门监管要求，一次对接，多次复用。网监对接的设置，请参见对接公安网监：公共无线上网管理平台。

4.8.3. 应用案例：本地账号认证

Panabit 上网行为管理提供了简单的账号存储服务，相当于用户信息放在 Panabit 设备上，无需与 AAA 对接。本地账号认证包括本地账号、临时账号及动态密码认证。

4.8.3.1. 配置流程

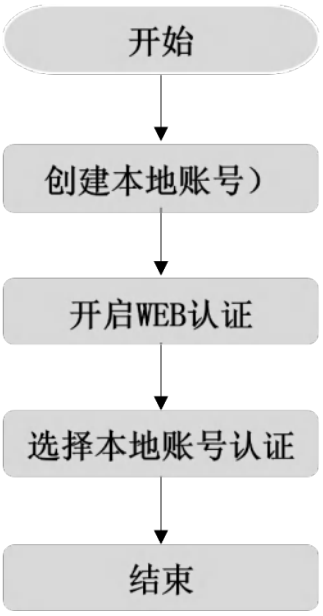


图 4-68 本地账号认证配置流程

4.8.3.2. 配置前提

- 设备已经以网关模式或网桥模式部署，参见网关部署、网桥部署。
- 已创建用户组并添加本地账号，具体请参见组织架构、本地账号。
- 已创建临时账号，具体请参见临时账号。
- 已获取动态账号及密码，具体请参见动态密码。

4.8.3.3. 配置步骤

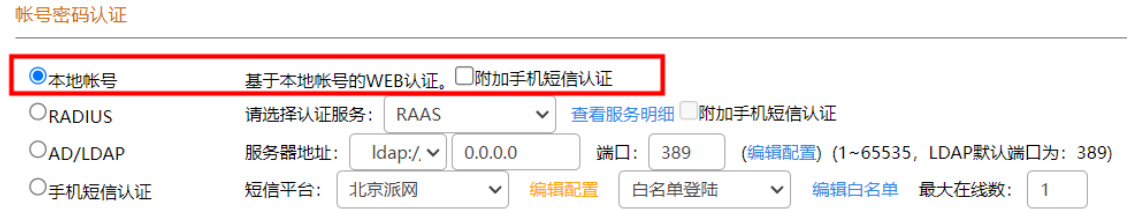
操作步骤

步骤 1 选择【流量概况】>【应用商店】>【我的应用】。

步骤 2 单击【WEB 认证】名称，弹出功能配置界面。

步骤 3 完成基本参数配置，具体请参见基本配置。

步骤 5 账号密码认证栏目选择【本地账号】。



步骤 6 单击【提交】。

——结束

4.8.4. 应用案例：对接 AAA 服务器认证

AAA 服务器大多使用标准 RADIUS 协议，本节以 RAAS 为例。

4.8.4.1. 配置流程

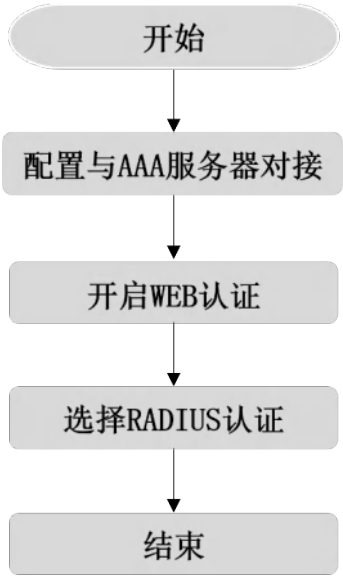


图 4-69 对接 AAA 服务器认证配置流程

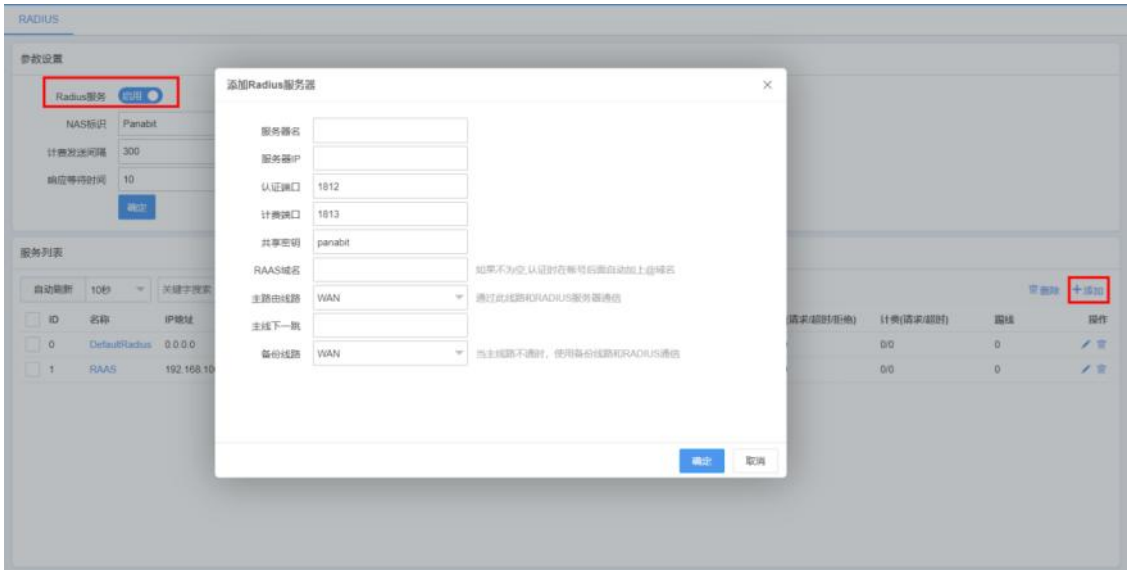
4.8.4.2. 配置前提

设备已经以网关模式或网桥模式部署，参见网关部署、网桥部署。

4.8.4.3. 配置步骤

操作步骤

步骤 1 配置上网行为管理设备 AAA 服务器对接，具体请参见 RADIUS。



步骤 2 选择【流量概况】>【应用商店】>【我的应用】。

步骤 3 单击【WEB 认证】名称，弹出功能配置界面。

步骤 4 完成基本参数配置，具体请参见基本配置。

步骤 5 账号密码认证栏目选择【RADIUS】。

步骤 6 认证服务选择【RAAS】。

步骤 7 单击【提交】。

——结束

4.8.5. 应用案例：手机短信认证

Panabit 上网行为管理支持通过与手机短信平台对接，用户在弹出的 Portal 界面输入手机验证码进行认证，下面以派网提供的短信平台为例。

4.8.5.1. 配置流程

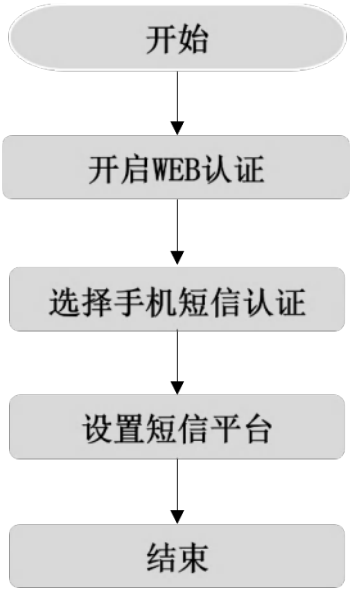


图 4-70 手机短信认证配置流程

4.8.5.2. 配置前提

设备已经以网关模式或网桥模式部署，参见网关部署、网桥部署。

4.8.5.3. 配置步骤

操作步骤

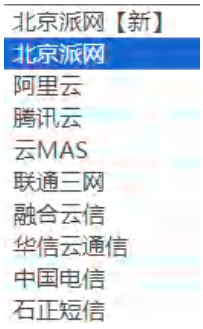
步骤 1 选择【流量概况】>【应用商店】>【我的应用】。

步骤 2 单击【WEB 认证】名称，弹出功能配置界面。

步骤 3 完成基本参数配置，具体请参见基本配置。

步骤 4 账号密码认证栏目选择【手机短信认证】。

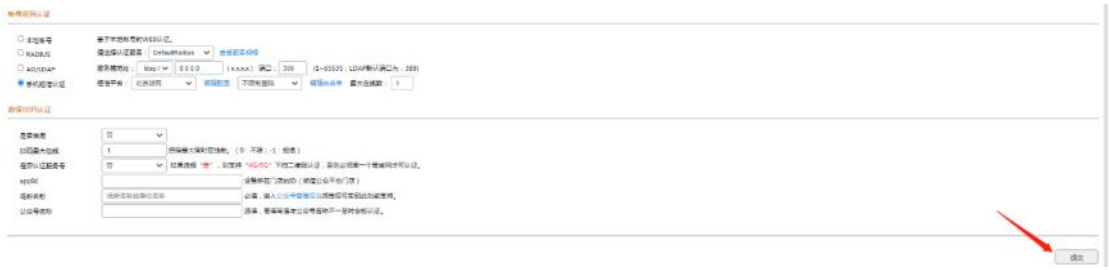
步骤 5 按照业务需要选择【短信平台】，选“北京派网”平台请联系派网工作人员或 400-773-3996 进行账号开通，其他短信平台参考平台说明文档进行开通。

参数名称	参数说明
短信平台	选择能够和上网行为管理设备对接的短信平台供应商。 
不限制登录	所有手机号都可以使用短信登录。
白名单登录	只有白名单内的手机号才能短信登录，非名单内的手机号无法收到短信信息。
最大在线数	同一手机验证码可以登录的数量。

步骤 6 单击短信平台后的【编辑配置】，弹出编辑页面。

步骤 7 输入平台账号、密码、用户 ID，设置内容模板，单击【保存】。

步骤 8 返回【基本配置】页面，单击【提交】。



——结束

4.8.6. 应用案例：微信认证

微信公众号消息认证上网。即用户向提供者的公众号发送消息“上网”来完成认证上网，主要目的是引流客户关注企业门店公众号。

4.8.6.1. 配置流程

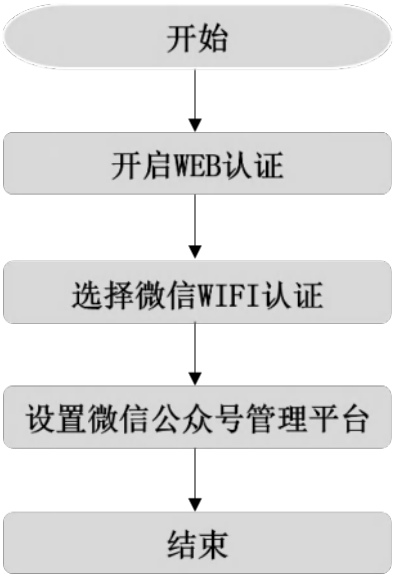


图 4-71 微信认证配置流程

4.8.6.2. 配置前提

- 设备已经以网关模式或网桥模式部署，参见网关部署、网桥部署。
- 已注册微信公众号，并登录微信公众平台。
  - 如何申请微信公众号：

    https://jingyan.baidu.com/article/597a06433af32f312a52436a.html
  - 微信公众平台地址：

    https://mp.weixin.qq.com/

4.8.6.3. 配置步骤

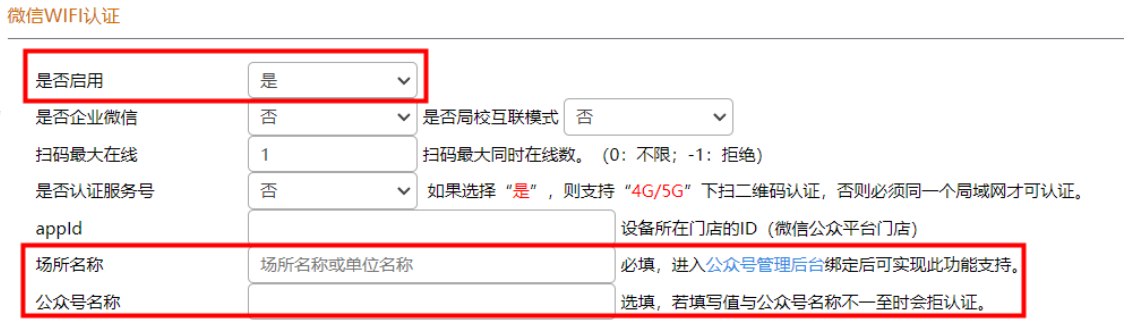
操作步骤

步骤 1 选择【流量概况】>【应用商店】>【我的应用】。

步骤 2 单击【WEB 认证】，弹出功能配置界面。

步骤 3 完成基本参数配置，其中免认证协议设置为“微信聊天”，具体请参见**基本配置**。

步骤 5 设置【微信 WIFI 认证】。



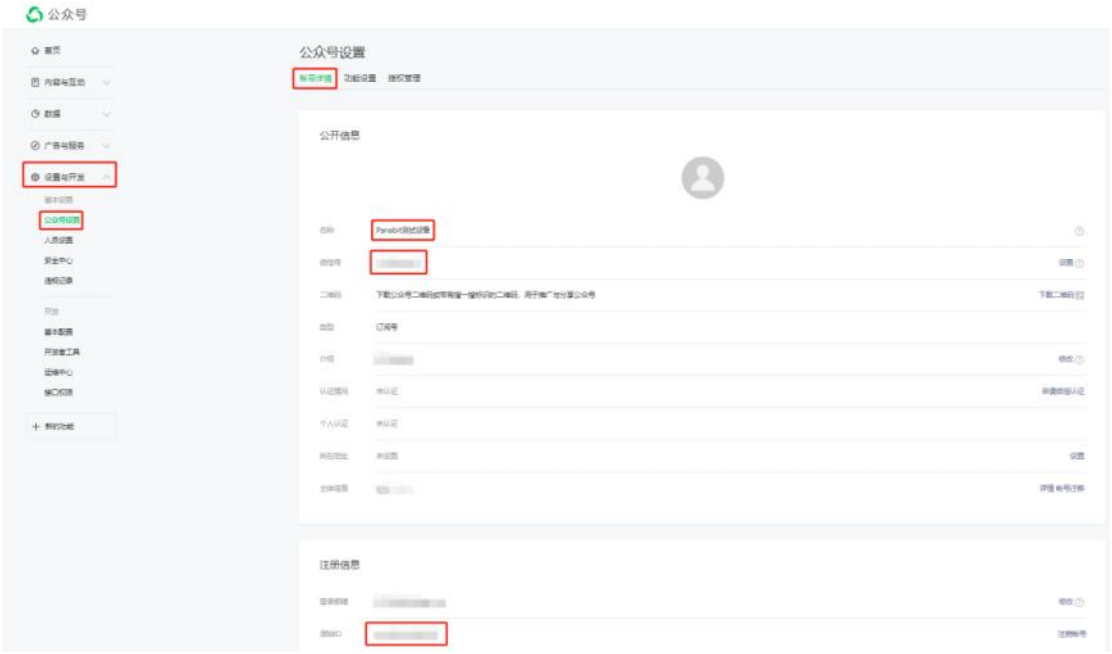
参数名称	参数说明
是否启用	是否启用微信认证功能，“是”启用微信认证，“否”不启用。
扫码最大在线	支持最大的在线用户数量，0 表示不限。
是否认证服务器号	建议选择“是”，选择“否”则在 4G/5G 下扫码无法认证
appid	微信公众平台产生，服务号门店 ID，必填
场所名称	Panabit 提供的管理平台的名称，必填
公众号名称	微信公众平台产生，公众号名称，选填

步骤 6 单击【提交】。

步骤 7 登录微信公众平台。

步骤 8 选择【设置与开发】>【公众号设置】>【账号详情】。

步骤 9 获取公众号名称、微信号、原始 ID。



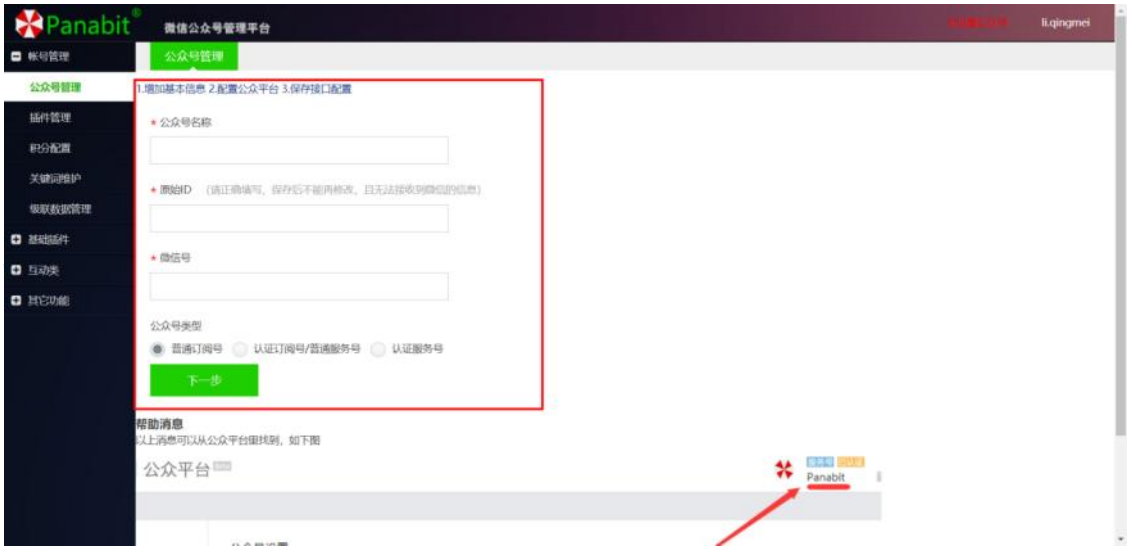
步骤 10 登录 Panabit 微信管理平台，可通过如下两种方式：

1. 单击场所名称后的“公众号管理平台”。

2. 访问 http://weixin.panabit.com/index.php?s=/home/user/login.html。

步骤 11 选择【公众号管理】>【新增】

步骤 12 填写“步骤 9”获取的公众号基本信息。



步骤 13 单击【下一步】，弹出服务器参数页面，复制参数信息。

步骤 14 返回微信公众平台首页。

步骤 15 选择【设置与开发】>【基本配置】>【服务器配置】。

步骤 16 单击【修改配置】，填入“步骤 13”已获取的服务器信息。

步骤 18 获取公众号的应用 ID、应用密钥、消息加解密密钥。

步骤 19 返回 Panabit 微信公众号管理后台，单击此页面的【下一步】。

步骤 20 填入“步骤 18”获取的公众号信息。

步骤 21 单击【保存】。

步骤 22 返回微信公众平台首页。

步骤 23 选择【设置与开发】>【基本配置】>【服务器配置】。

步骤 24 单击【查看】将 ping“weixin.panabit.com”获取的 IP“115.29.138.209”，加入白名单。

步骤 25 返回 Panabit 微信公众号管理后台。

步骤 26 默认回复“微信认证上网”即可做认证上网，如需自定义回复内容，请选择【账号管理】>【关键词维护】>【新增】进行设置。

步骤 27 单击【确定】。

——结束

4.8.7. 应用案例：对接 AD 域认证

在企业网络信息化建设中，通常会采用 AD 域控制手段，以实现对局域网中的 PC 终端的统一管理。PC 终端必须通过 AD 域的认证和鉴权才能访问内部资源。而另一方面，对于互联网访问的认证、鉴权和管控，通常需要额外部署独立的系统，这给网络运维和管理带来了不少麻烦。

因此，最佳的解决方案是将 AD 域控制与上网行为管理系统进行整合。这样，可以利用由 AD 域分配的账户和密码来进行互联网访问的认证和鉴权，并且能够对每个账户的上网行为进行精细管控。因此，基于这一需求，Panabit 实现了与 AD 域控制的联动功能。这使得管理互联网访问变得更加高效和方便。

4.8.7.1. 配置流程

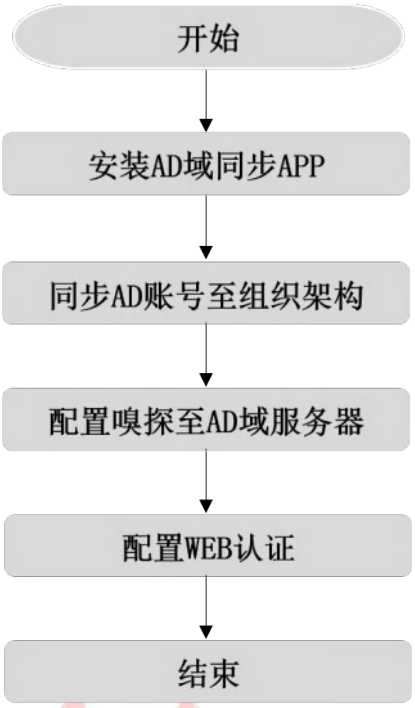


图 4-72 对接 AD 域认证配置流程

4.8.7.2. 配置前提

- 设备已经以网关模式或网桥模式部署，参见网关部署、网桥部署。
- Panabit 管理口与 AD 服务器能够正常通讯。

4.8.7.3. 配置步骤

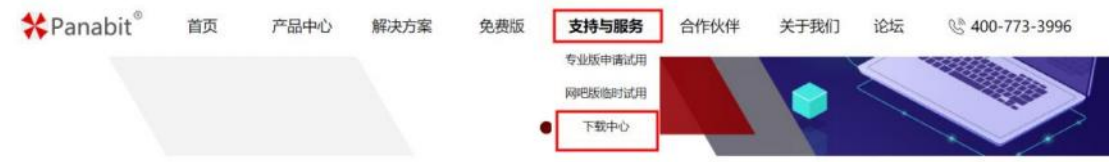
4.8.7.3.1. 安装 AD 域同步 APP

可通过 Panabit 官网或设备 WEB 控制台，安装“AD 域同步”APP。安装 APP 可通过如下两种方式：

1. 通过 Panabit 官网安装。

步骤 1 打开浏览器，前往官网 www.panabit.com。

步骤 2 选择【支持与服务】>【下载中心】，选择【APP】，在 APP 列表中找到“AD 域同步”。



步骤 3 单击【下载】，将 APP 安装文件下载至本地。

步骤 4 登录 WEB 控制台，进入【流量概况】>【应用商店】，点击页面右上方的 安装升级 ，找到本地已下载的 APP，按照提示完成安装。

——结束

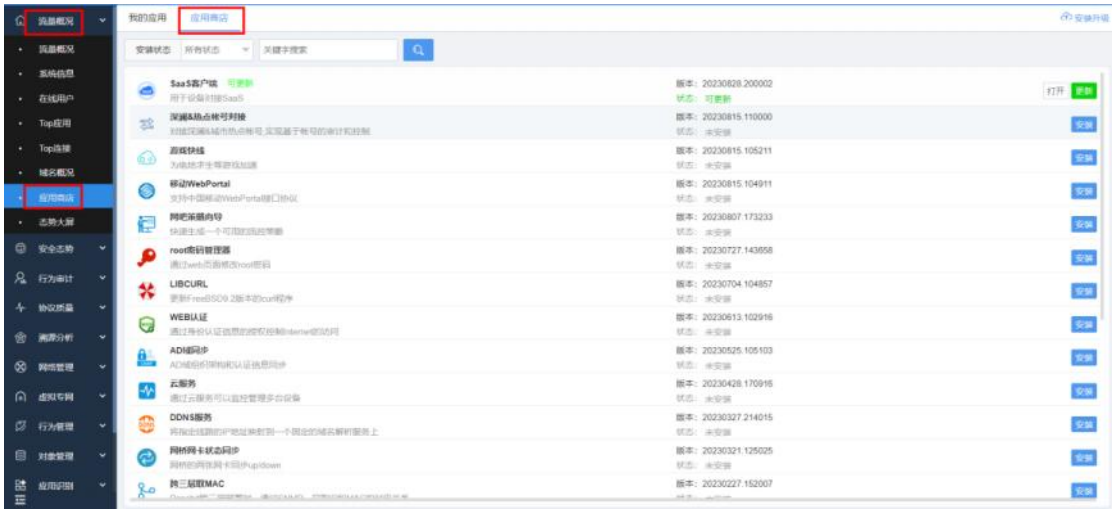
2. 通过 WEB 管理平台安装。

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名和密码，登录 WEB 控制台。

步骤 3 选择【流量概况】>【应用商店】>【应用商店】。

步骤 4 在 APP 列表找到“AD 域同步”APP，单击【安装】。



——结束

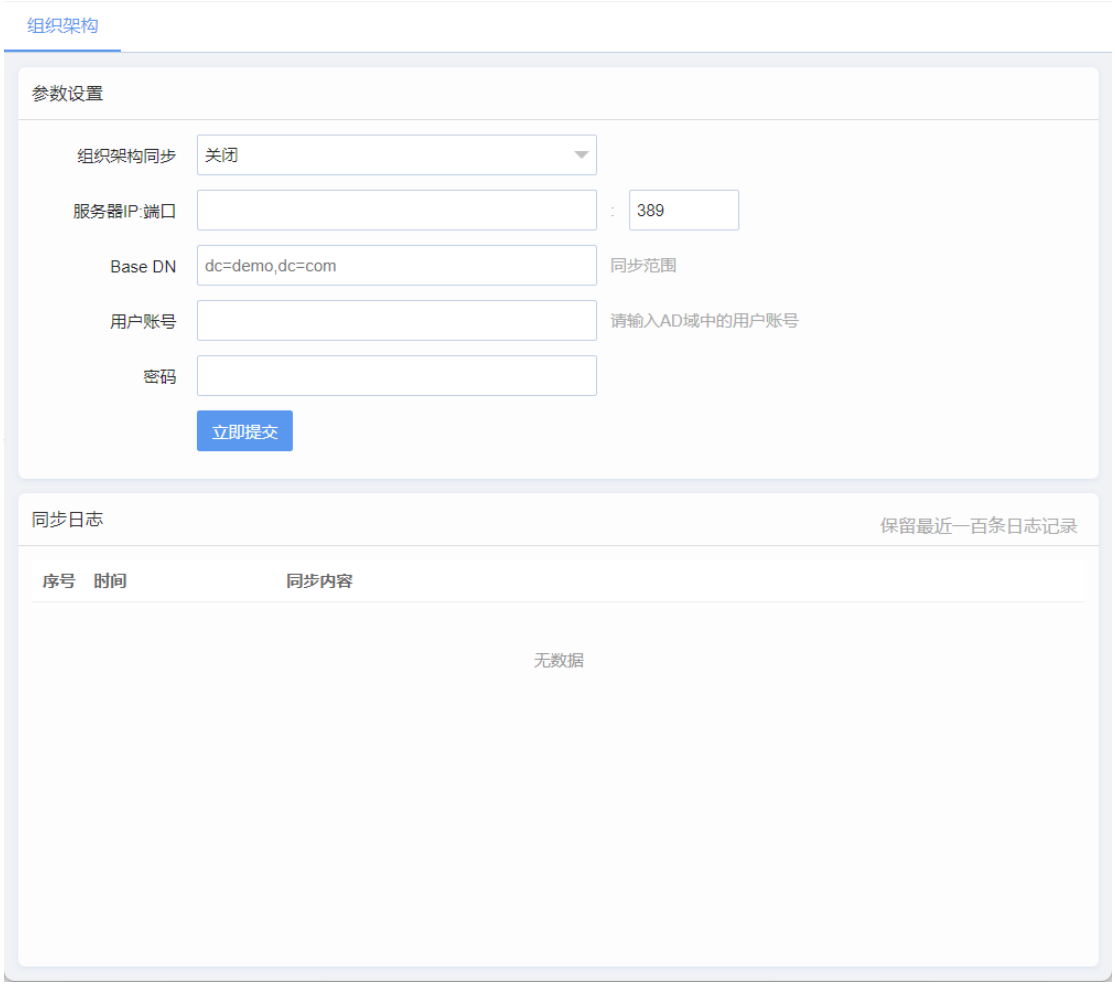
4.8.7.3.2. 同步 AD 账号至组织架构

将 AD 服务器上的组织单位和用户同步到 Panabit。组织单位即地址池名称，用户即为地址池的账号。

操作步骤

步骤 1 打开 AD 域同步 APP，选择【组织架构】。

步骤 2 填写 AD 域的对应参数，开启组织架构同步。



参数名称	参数说明
组织架构同步	是否启用同步功能。
服务器 IP:端口	AD 服务器的 IP 地址与服务端口，端口默认 389。
Base DN	设置同步范围。Base DN 通常是一个 LDAP 路径，表示搜索应从哪个节点或子树开始。通过设置 Base DN，您可以限定 LDAP 搜索的范围，以便只搜索特定的组织单位（OU）或容器。
用户账号	AD 域的用户账号。

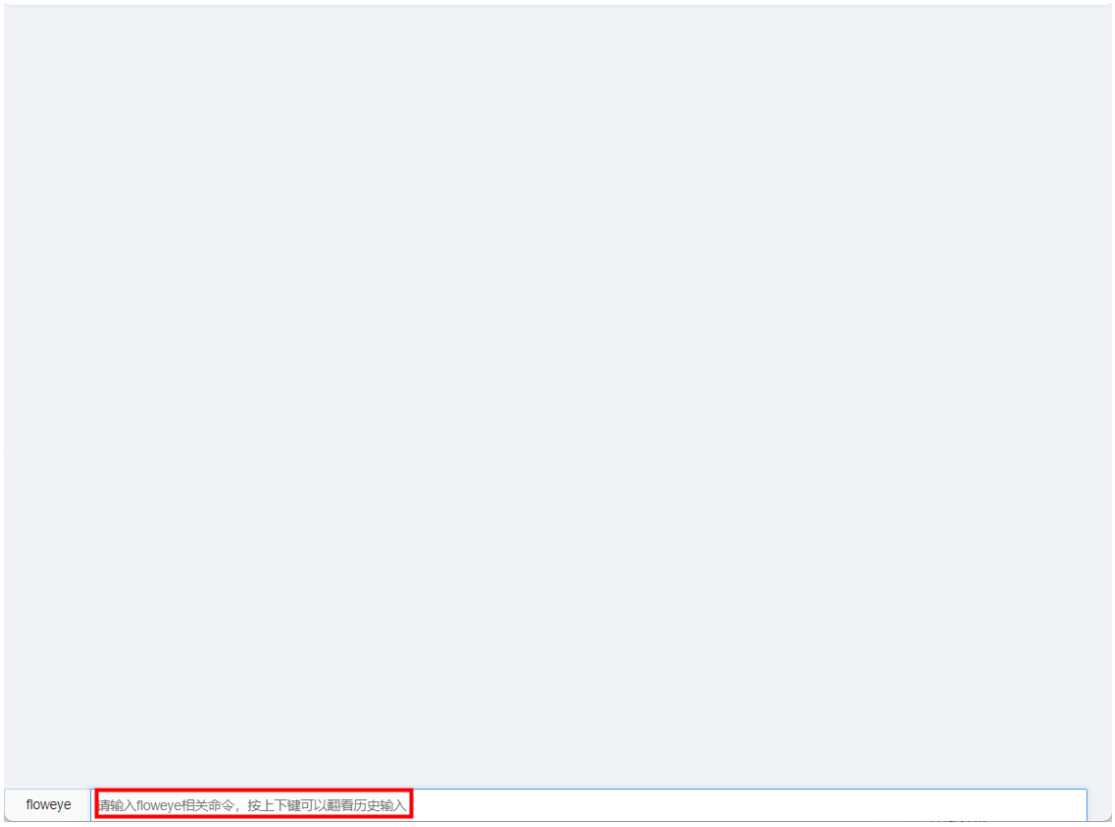
密码	账号对应的密码。

步骤 3 单击【立即提交】，完成设置。

步骤 4 单击工具栏</>，执行“floweye adauth config enable=<1|0> port=<x>”命令。

说明

- “enable”必须配置，开启或者关闭 Agent 登录功能，1 为开启，0 为关闭。这里选择“1”。
- “port”可选配置，配置报文端口号，默认端口 7777。



步骤 5 执行“floweye adauth stat”命令，查看运行状态。

```
# floweye adauth config enable=1

# floweye adauth stat
enable=1
debug=0
port=7777
count=0
login_count=0
logoff_count=0
panic_tag=0
panic_act=0
panic_namesz=0
panic_src=0
panic_ipconfict=0
panic_clntallocn=0
panic_ipobjalloc=0
panic_pxy=0
```

——结束

4.8.7.3.3. 配置嗅探至 AD 域服务器

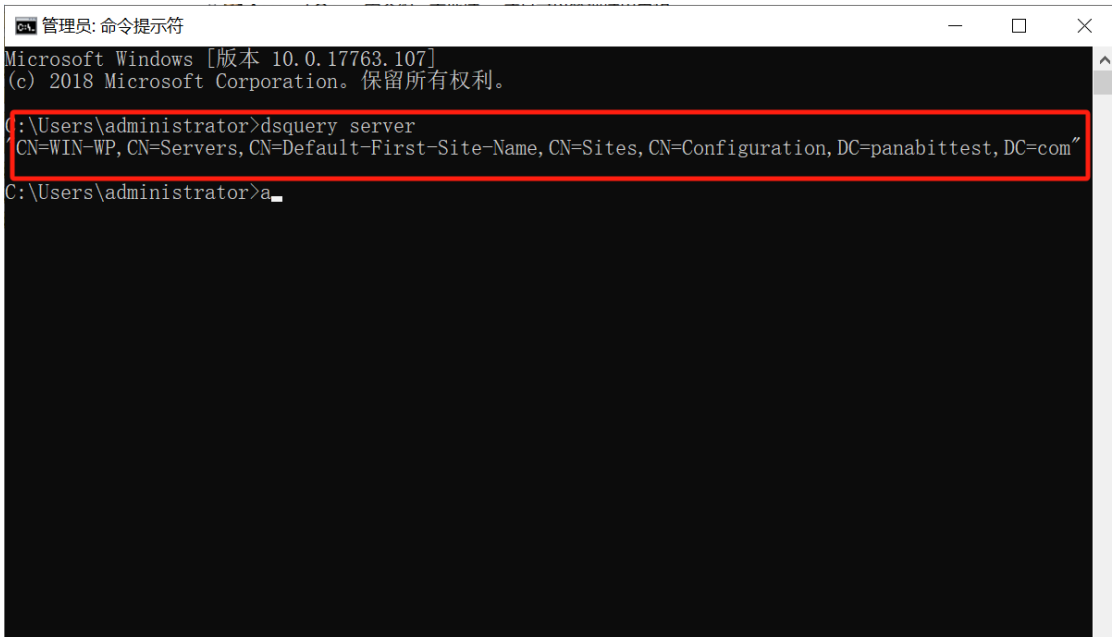
通过此操作，为 AD 域服务器安装嗅探，并完成与 Panabit 智能应用网关数据口的对接。

此操作在 AD 域服务器上进行。

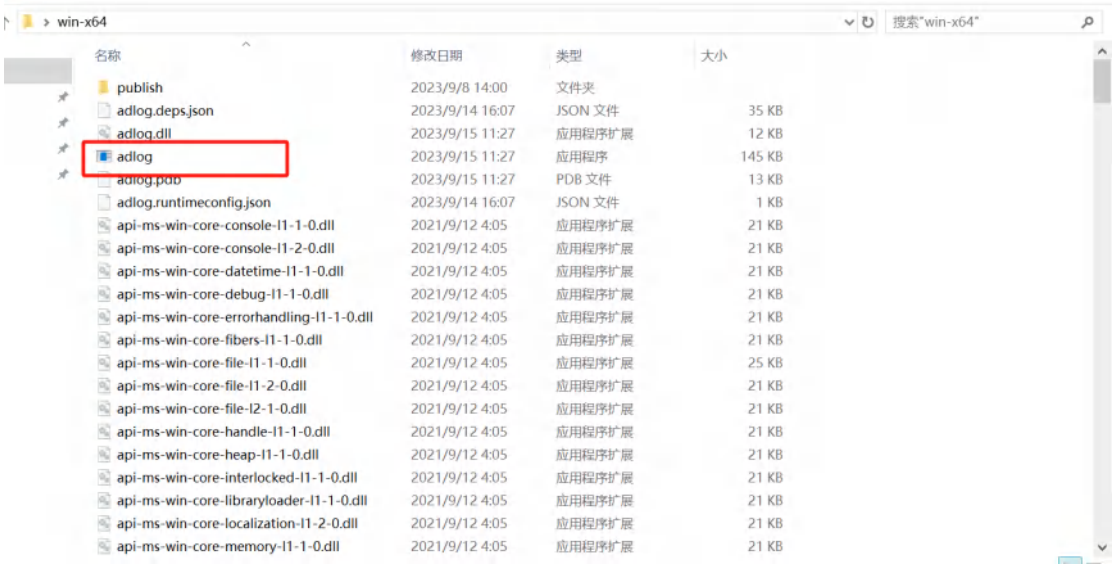
操作步骤

步骤 1 浏览器访问：https://www.kdocs.cn/view/l/cqbBHzIMMrfW，下载 WIN 嗅探安装包。

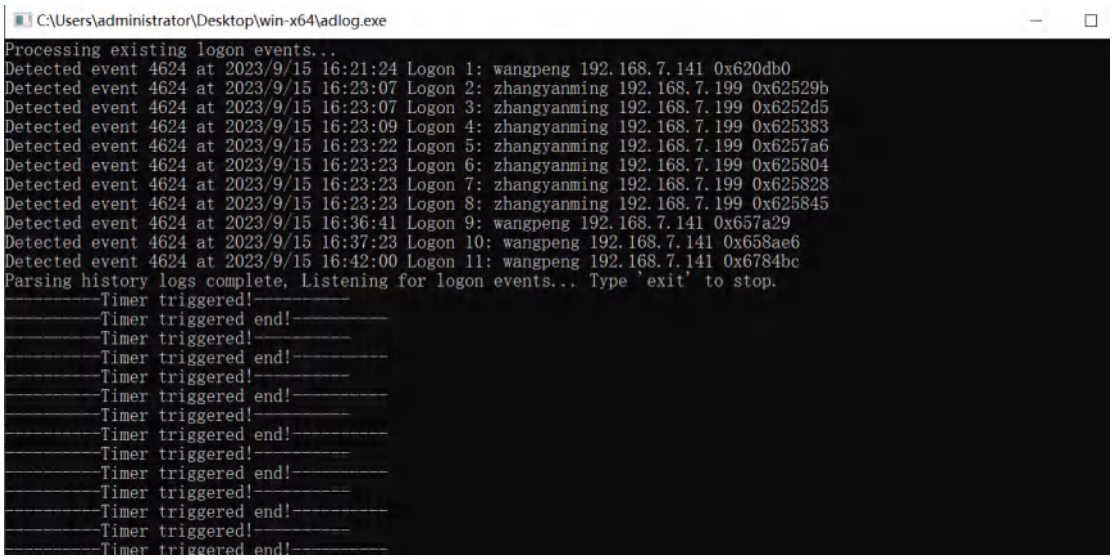
步骤 2 进入 CMD 界面，输入命令“dsquery server”。



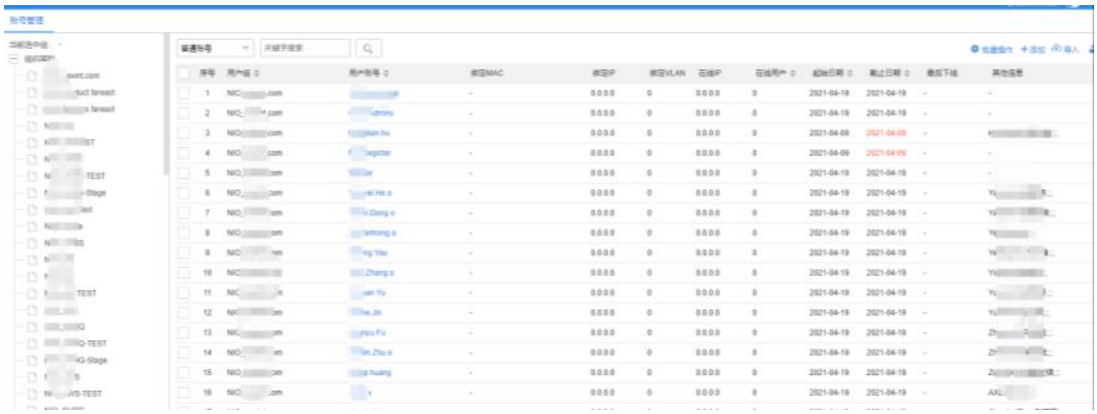
步骤 3 解压嗅探程序，双击运行程序。



步骤 4 进入 CMD 界面，输入 Panabit 数据口的 IP 地址，输入嗅探的端口号，默认为 7777



同步结果：



——结束

4.8.7.3.4. 配置 WEB 认证

操作步骤

步骤 1 选择【流量概况】>【应用商店】>【我的应用】。

步骤 2 单击【WEB 认证】名称，弹出功能配置界面。

步骤 3 完成基本参数配置，具体请参见基本配置。

步骤 5 账号密码认证栏目选择【AD/LDAP】。

参数名称	参数说明
服务器地址	AD 服务器的 IP 地址。
端口	AD 服务器的服务端口，默认 389。

步骤 6 单击【提交】。

——结束

4.9. 行为管理

4.9.1. 概述

Panabit 的行为管理功能，通过流量控制、数据通道、连接数、HTTP、DNS 等方式对用户上网行为进行管理控制。可以基于流量的源/目的 IP 地址、源/目的端口号、应用协议和报文传递方向等信息，对流量进行精准的允许、限速、阻断，以及应用级的管控操作。

Panabit 的行为管理功能，均通过配置策略（包含策略组及具体策略）来实现。

4.9.1.1. 策略组与策略

管理策略由 1 个或者多个策略组组成，每个策略组由 N 条具体策略组成。报文匹配到了策略才会被控制，行为管理模块默认没有任何策略。

图 4-73 策略组要素

图 4-74 策略要素

说明

1. 各个匹配条件之间是 “与” 的关系，报文的属性与各个条件必须全部匹配，才认为该报文匹配这条策略。也就是说报文中的信息要满足所有条件才能匹配。
2. 报文匹配策略条件后，就会执行相应的动作。执行动作后如果是停止，则不会继续

向下匹配策略。如果是执行动作是继续，那么会执行动作后继续向下匹配后面的策略。

4.9.1.2. 策略序号的设置原则

一个策略组中会有若干条策略，策略的匹配顺序由策略序号（范围 1~65535）决定，1 的优先级最高，65535 最低。在添加策略时，策略编号尽量不要连续或者间隔太小，否则后期需要添加策略时就会很不方便。

图 4-75 策略列表

4.9.1.3. 策略与对象

在策略的匹配条件中，可以选择调用的对象。可调用的对象，包括：用户组、IP 群组、域名群组及文件类型等。

- **用户组：**对本地用户进行归类的群组，每一个用户必须关联一个用户组（地址池）。参见组织架构。
- **IP 群组：**一个 IP 地址列表或范围，可以选择该列表或范围供策略使用。
- **域名群组：**一个域名列表或范围，可以选择该列表或范围供策略使用。
- **文件类型：**定义 HTTP 请求的文件后缀名，比如 exe、rar 等，用于 HTTP 管控。

4.9.2. 应用场景

Panabit 上网行为管理产品的行为管理功能是基于应用级别的流量、连接数及应用行为管控，适用于以下场景：

1. 防止网络中个别应用或用户使用带宽过高，影响其他用户正常上网。
2. 工作时间限制或阻止无关应用，如视频、购物、游戏等应用的访问，优先保障即时通信、视频会议等应用的访问。
3. 禁止用户访问违规应用或恶意网站。
4. 其他针对用户或应用的管控。

4.9.3. 流量控制

4.9.3.1. 概述

流量控制功能是基于数据包的控制，用户通过策略实现对指定条件数据包流量的统计、放行、阻断、DSCP 标记、限速、优先级、镜像、转发等操作。

- **统计：**对匹配策略条件的流量进行趋势统计和 IP 流量统计。
- **放行：**流量控制模块默认对所有流量放行。设置指定流量的放行策略是为了逻辑上能够更灵活多变。
- **阻断：**对指定条件的数据包进行丢弃。
- **DSCP 标记：**DSCP 是 IP 包头的一个通用字段，通常用于 QoS。通过对不同流量进行不同标记，可以配合第三方设备进行 QoS。
- **限速：**包含内网单 IP 限速和数据通道限速。数据通道是整体限速的手段，并且可以实现优先级。
- **镜像：**一种是传统的二层镜像，数据包被复制后从一个指定的物理口发出来。另一种是远程 SD-WAN 镜像，数据包被复制后，通过 iWAN 隧道传输到远端设备。镜像通常配合分析设备使用。
- **转发：**将匹配策略的流量直接从一个指定物理接口发出去。这个功能可以配合 IPS 这类的设备使用，将指定流量送给 IPS，降低 IPS 的负载压力。

4.9.3.2. 应用案例：流量的允许、阻断和限速

某用户内网有 50 个上网用户，出口带宽为 200M，具体需求如下：

1. 需要禁止员工在上班时间使用娱乐类软件和购物网站（上班时间为周一到周五 9:00-18:00）。
2. 员工需要在网上获取一些必要的资源，所以不能完全禁止 P2P 下载，但是下载不能占用太大带宽，每个用户的带宽占用限制在 3000kbits/s 以内。
3. 公司内部有需要不做限制的 IP ：192.168.3.200-192.168.3.210。

4.9.3.2.1. 配置流程

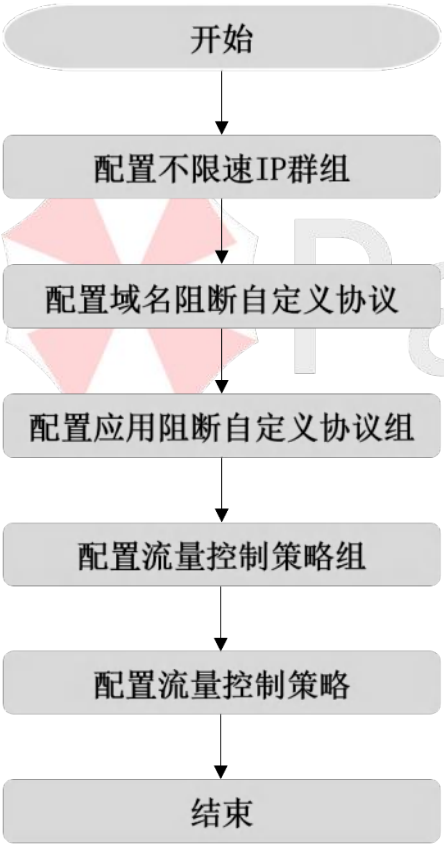


图 4-76 流量控制配置流程

4.9.3.2.2. 配置前提

Panabit 上网行为管理设备以网关模式或网桥模式部署在用户网络出口，开始配置前，已完成设备部署，具体操作请参见设备部署。

4.9.3.2.3. 配置步骤

4.9.3.2.3.1. 配置不限速 IP 群组

通过此操作，配置不限速 IP 群组，待后续策略调用。策略生效后，添加到群组的 IP 不再受其他控制策略影响。

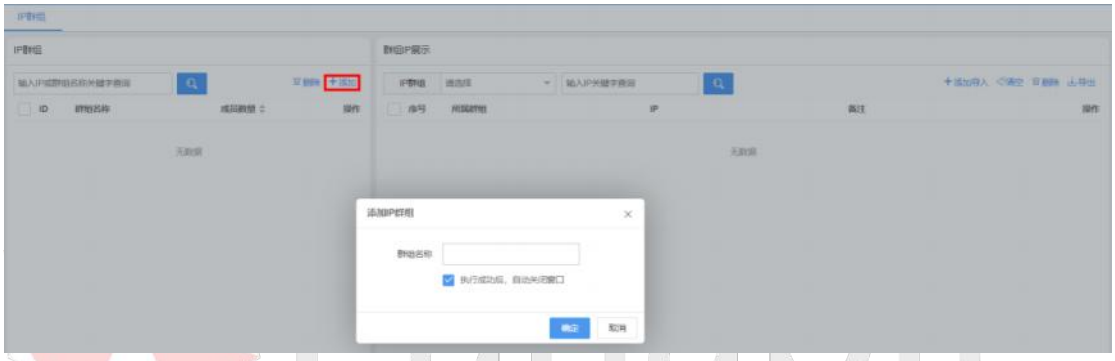
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【对象管理】>【IP 群组】。

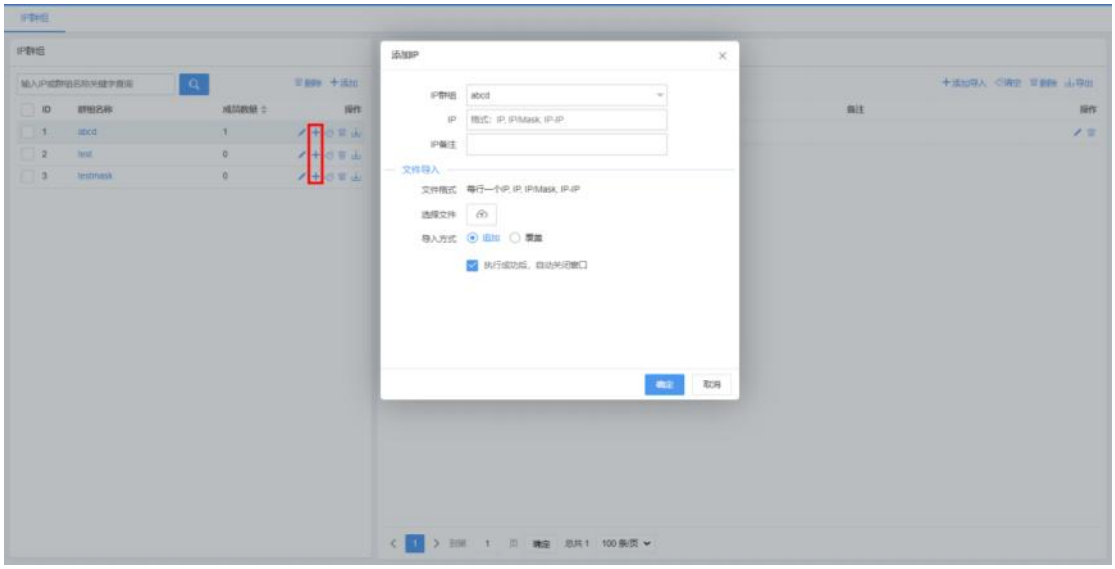
步骤 4 单击【添加】，弹出添加 IP 群组页面。



配置示例：输入群组名称为“不限速 IP 组”。

步骤 5 单击【确定】。

步骤 6 单击 IP 群组操作列的 ，弹出添加 IP 页面。



说明

添加 IP 时可单个添加，也可批量导入。

当需要添加多个 IP 时，不同 IP 之间用逗号隔开。

步骤 6 输入或导入 IP，单击【确定】。

配置示例：输入不限速 IP 地址段 :192.168.3.200-192.168.3.210。

——结束

4.9.3.2.3.2. 配置域名阻断自定义协议

通过此操作，可创建域名阻断自定义协议，添加需要阻断的域名，待协议组或策略调用。

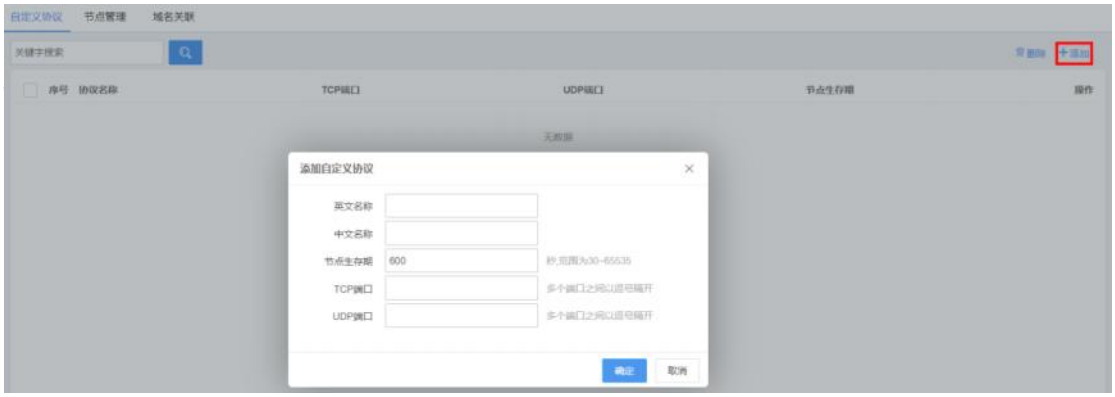
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【应用识别】>【自定义协议】>【自定义协议】。

步骤 4 单击【添加】，弹出添加自定义协议页面。



参数名称	参数说明
英文名称	自定义协议的英文名称。
中文名称	自定义协议的中文名称。
节点生存期	控制节点生效的时间长度。 单位：秒，取值：30~65535。 **说明** 数据包匹配该协议后，系统会将目的 IP 记录到节点，当节点在一定的时间段内没有被访问，系统就会把这个节点删除掉。
TCP 端口	为 TCP 协议通信提供服务的端口。 取值：0~65535，多个端口之间以逗号隔开。
UDP 端口	为 UDP 协议通信提供服务的端口。

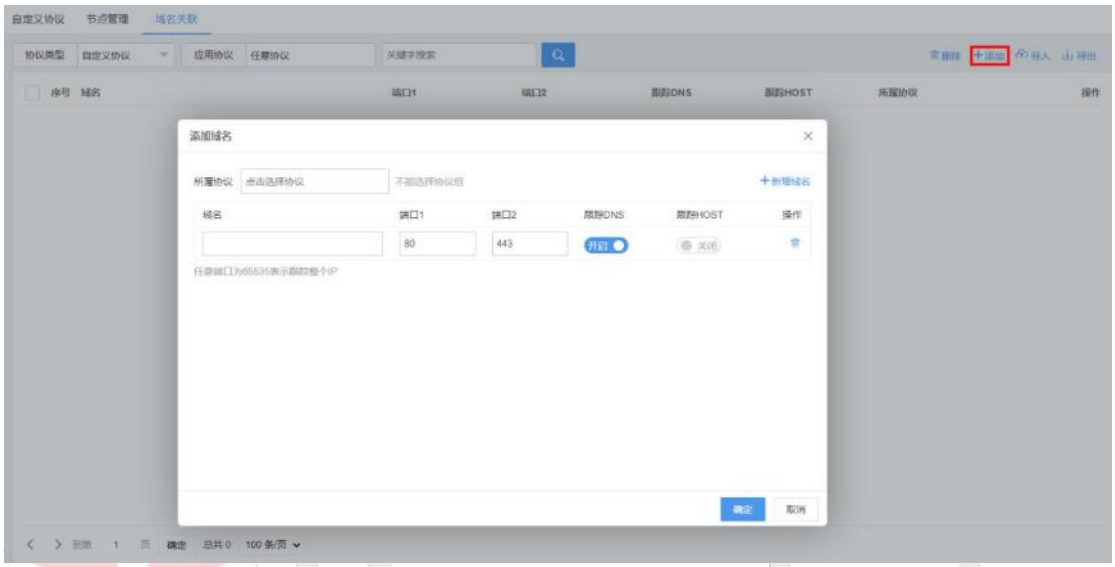
	取值：多个端口之间以逗号隔开。

步骤 3 配置自定义协议，单击【确定】。

配置示例：输入英文名称“zuduan”，输入中文名称“阻断域名”，其他参数可不做设置。

步骤 4 选择【应用识别】>【自定义协议】>【域名关联】。

步骤 5 单击【添加】，弹出添加域名页面。



步骤 6 在所属协议行，单击选择协议，新建阻断协议。

步骤 7 在域名列输入需要阻断的域名。单击【新增域名】，可添加其他需要阻断的域名。

步骤 8 单击【确定】。

配置示例：所属协议选择“阻断域名”，输入域名“www.taobao.com”，其他参数可不做设置。

——结束

4.9.3.2.3.3. 配置应用阻断自定义协议组

通过此操作，可创建基于域名或应用的阻断自定义协议组，待后续策略调用。协议组是应用协议的集合，其中可以添加特征库自带的应用协议或自定义协议。阻断策略生效后，协议组内所有的协议都不能再访问。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【应用识别】>【自定义协议组】。

步骤 4 单击【添加】，添加自定义协议组。

步骤 5 输入协议组中文名和英文名，单击【确定】。

配置示例：输入英文名称“zuduan”，输入中文名称“阻断协议组”，其他参数可不做设置。

步骤 6 单击协议组名称或操作列的  ，进入协议列表，搜索或勾选需要阻断的协议。

步骤 7 单击【确定】。

配置示例：搜索并勾选上一小节中自定义的“阻断域名”，以及其他需要阻断的应用，如网络游戏、抖音等，添加至阻断协议组。

——结束

4.9.3.2.3.4. 配置流量控制策略组

通过此操作，配置策略组，并设置生效周期及时间。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【行为管理】>【流量控制】。

步骤 4 单击页面右上角的【添加策略组】。

步骤 5 配置策略组，单击【确定】。

参数名称	参数说明
策略组名称	自定义策略组的名称。
内/外网地址	策略组管理的内网地址与外网地址。
调度日期	调度策略的时间段。
开始时刻	策略生效的开始时间。
结束时刻	策略生效的结束时间。
当	基于网卡下行流量的策略组调用条件。当指定网卡的下行流量大于等于特定数值时，调用策略组。
匹配后	继续匹配：这一组规则匹配后继续匹配后面的策略组。 停止匹配：不再匹配后面的策略组。
状态	可“启用”或“禁用”当前的策略组。

配置示例：策略组名称填入“工作流控组”，调度日期选择“每周、周一至周五”， 开始时刻设为“9:00:00”结束时刻设为“18:00:00”，状态为“启用”，其余参数暂不设置。

——结束

4.9.3.2.3.5. 配置流量控制策略

通过此操作，配置流量控制策略，对不同协议进行流量的允许、阻断、限速等操作。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【行为管理】>【流量控制】。

步骤 4 鼠标悬停已创建策略组名称，单击【添加策略】。

步骤 5 配置流量控制策略，单击【确定】。

参数名称	参数说明
策略序号	自定义策略的编号，系统将按照编号从小到大的方式依次执行策略表。 设置后，该编号不可编辑，也不可上下移动。 取值：1~65535。序号越小，优先级越高。
策略备注	对策略的补充说明。

线路及流向	匹配特定线路的数据报文，线路可选择 WAN 线路或网桥，流向可设置为“任意”、“上行”、“下行”。
首包接口	会话第一个数据包的源接口。
源接口	选择某个内网物理接口或逻辑 LAN 接口进行匹配。
协议	对应用进行匹配，该“应用协议”可以是特征库或者自定义协议，并且关联了域名特征，否则该策略无意义。
内/外地址	匹配报文中的内网/外网地址。
内/外端口	匹配报文中的内网/外网端口。
内网 MAC 组	MAC 加入该地址池后，可以基于 MAC 地址做控制。可以在【TOP 用户】或【IP/MAC 备注】中，将 MAC 加入指定地址池。
VLAN	匹配数据报文的 VLAN-Tag。
TTL	匹配数据包的 TTL 值。
共享用户>=	基于共享用户数的策略调用条件。
移动设备>=	基于移动设备连接数的策略调用条件。
QQ 用户数>=	基于 QQ 用户登录数的策略调用条件。
执行动作	允许:匹配策略的数据包允许通过。 ● 内网 IP 限速：单位 kbits/s，如 10 或 10-100，0 表示不限速。 ● 修改 DSCP：0~63，0 表示不修改。 ● 流量统计：关联统计对象，实现基于策略的流量统计。 阻断：匹配策略的数据包全部被丢弃。 通道限速：选择一个已经创建的数据通道，匹配策略的流量不能超过数据通道的大小。选择数据通道后，可以设置优先级，流量根据相应的优先级在数据通道内做队列。 ● 数据通道：对满足匹配条件的数据做整体的限速。 ● 通道优先级：0~16，数字越小越优先。0 表示不排队直接通过。 包转发：与策略路由的路由动作类似，区别在于包转发是基于数据包的，策略路由是基于会话的。选择一条已经创建的 LAN 或者 WAN 线路。 ● 转发线路：匹配策略的流量从所选接口转发出去。 iWAN 镜像：选择一条已经创建的 iWAN 线路，匹配策略的流量会被复制一份，并且通过 iWAN 线路转发到 iWAN SERVER 上。可以指定镜像会话的前 N 个报文，这样可以降低传输线路的带宽压力，又能保证业务识别的准确性。 ● iWAN 线路：选择镜像流量转发的 iWAN 线路。

	● 镜像包数：镜像会话前 N 个包，0 表示镜像所有包。 端口镜像：选择一个物理接口，匹配策略的流量会被复制一份，并通过物理接口发送出去。一般配合分析设备使用。可以指定镜像会话的前 N 个报文，这样可以降低分析设备的压力，又能保证业务识别的准确性。 ● 网络接口：选择发送镜像流量的物理接口。 端口转发：选择一个物理接口，将匹配策略的流量直接从指定物理接口发出去。这个功能可以配合 IPS 这类的设备使用，将指定流量送给 IPS，这样无关的流量就不会经过 IPS，可以降低 IPS 的负载压力。 ● 修改 VLAN：对匹配策略流量的 VLAN 进行修改。
继续匹配	这一组规则匹配后继续匹配后面的策略。
停止匹配	不再匹配后面的策略。

配置示例：

1. 单击【添加策略】，策略序号设为“1000”， 内网地址类型选择“IP 群组”，IP 选择“不限速 IP 组”。执行动作选为“允许”，内网 IP 限速输入“0”，执行动作过后选择“停止匹配”，单击确定。
2. 再次单击【添加策略】，策略序号设入“2000”，【协议】选择“阻断协议组”，执行动作选择“阻断”。
3. 再次单击【添加策略】，策略序号设为“3000”，协议选择“P2P 下载”， 执行动作选为“允许”，内网 IP 限速输入“3000”。

——结束

配置效果：

1. 策略序号为 1000 的策略，由于其序号最小，因此会被优先匹配，即，“不限速 IP 组”中的 IP 地址，系统会直接允许其通过；又因执行动作后为“停止匹配”，该 IP 群组不再受后面策略的影响。
2. 策略序号为 2000 的策略，会对“阻断协议组”内的所有应用协议进行阻断。
3. 策略序号为 3000 的策略，会对“P2P 下载”协议进行单 IP 限速，每个 IP 使用 P2P 下载的流量速率，不会超过 3000kbits/s（“不限速 IP 组”中的 IP 除外）。

说明

限速的原理实际是丢弃数据包，超过限速值的流量，会被流量控制模块丢弃。如果要对满足匹配条件的数据做整体的限速，请参见应用案例：通道限速。

4.9.3.3. 应用案例：用户组管控

某用户公司内有 5 台打印机，要求所有打印机都不能联网。

4.9.3.3.1. 配置流程

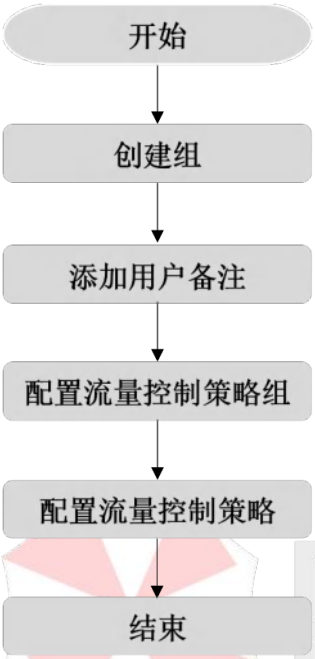


图 4-77 用户组管控配置流程

4.9.3.3.2. 配置前提

Panabit 上网行为管理设备以网关模式或网桥模式部署在用户网络出口，开始配置前，已完成设备部署，具体操作请参见设备部署。

4.9.3.3.3. 配置步骤

4.9.3.3.3.1. 创建组

通过此操作，配置用户组，待后续策略调用。策略生效后，添加到群组的用户将受到控制策略影响。

操作步骤

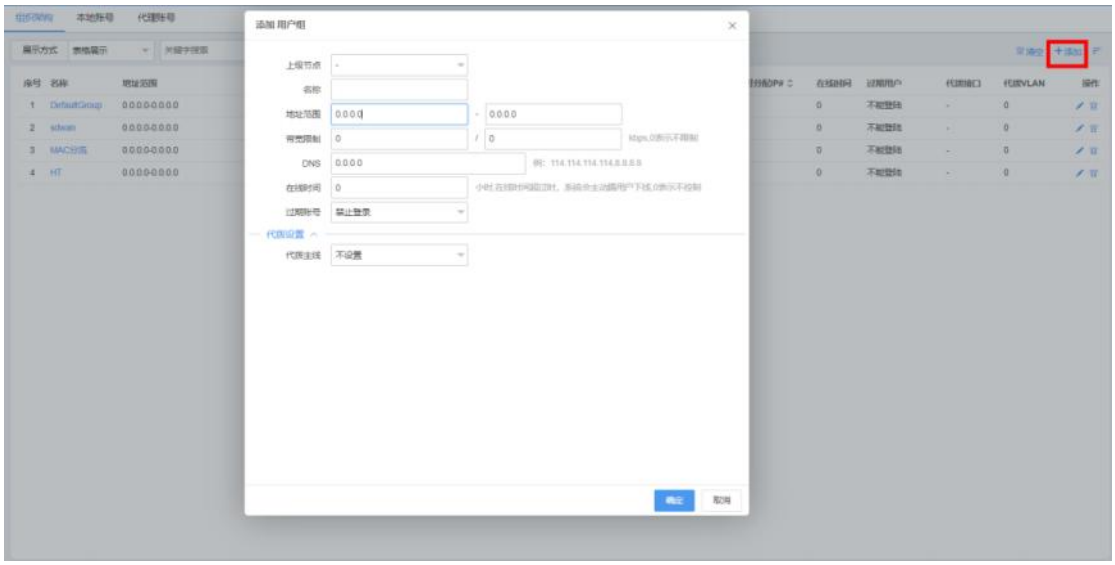
步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【对象管理】>【账号管理】>【组织架构】。

步骤 4 单击【添加】，弹出新增用户组页面。

步骤 5 设置用户组参数，单击【确定】。



参数名称	参数说明
上级节点	标识本用户组的上级组属，默认为空。
名称	自定义用户组的名称。
地址范围	该用户组的地址池范围。
带宽限制	单位 kbps，0 表示不限制
DNS	DNS 的 IP，格式为 0.0.0.0。
在线时间	单位小时，在线时间超过时，系统会主动让用户下线，0 表示不控制。
过期账号	可选择“禁止登录”、“允许登录，禁止上网”、“允许登录及上网”。

配置示例：输入用户组名称为“打印机”，其余参数可暂不设置。

——结束

4.9.3.3.3.2. 添加用户备注

添加用户备注分为两种方式：

IP 备注：将内网 IP 做备注标记，并且关联组。适用于内网 IP 固定分配的场景。

MAC 备注：将 MAC 做备注标记，并且关联组。适用于内网 IP 动态分配的场景。

当用户已上线时，可通过 IP 的账号备注，对当前用户添加备注。

操作步骤

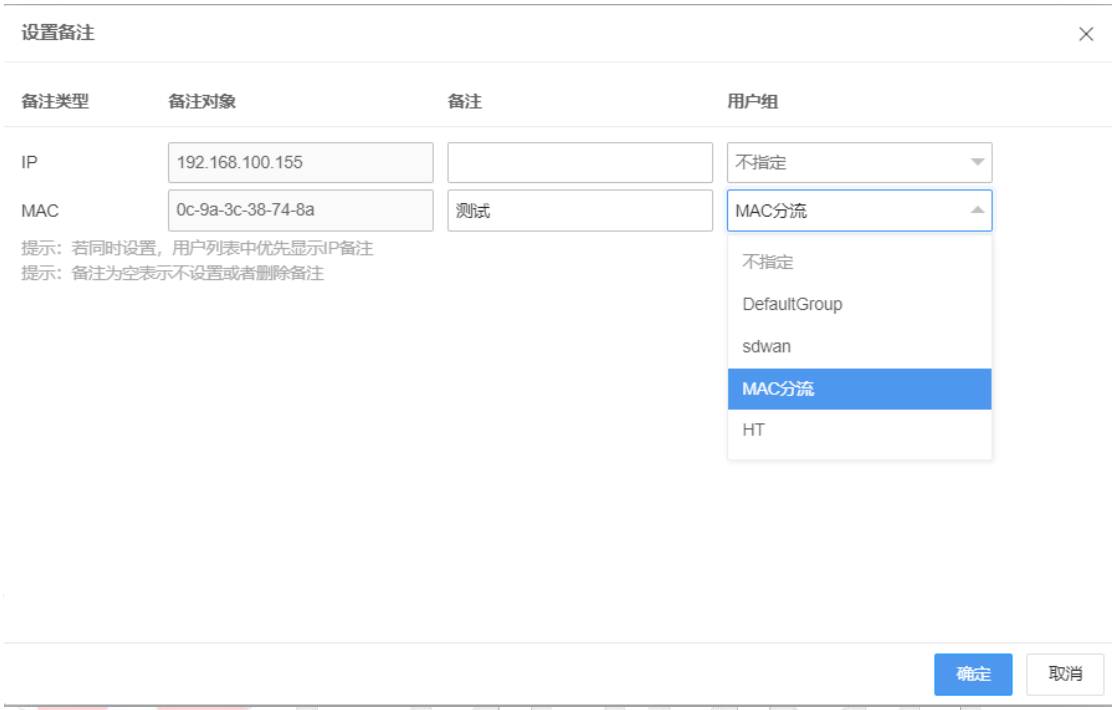
步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 如用户已上线

1. 选择【流量概况】>【在线用户】。

2. 单击当前 IP，账号备注列的 ，弹出用户备注页面。



步骤 4 单击【确定】。

——结束

当用户未上线时，可以通过手动添加和导入文件的方式添加用户备注。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【对象管理】>【IP/MAC 备注】。

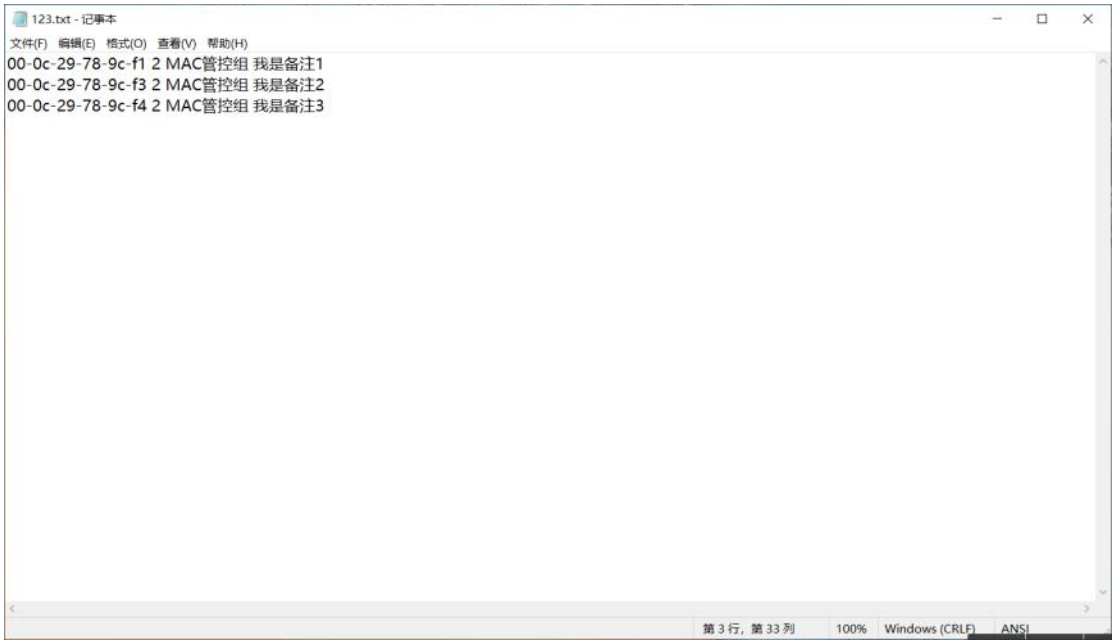
步骤 4 手动添加用户备注。

1. 单击页面右上方【添加】，进行用户备注。

2. 单击【确定】。

步骤 5 文本导入添加用户备注。

1. 创建 txt 文档，格式为：[MAC] [用户组 ID] [用户组名称] [备注内容]。



说明

每一个 MAC 对象单独为一行，用户组 ID 为组织架构中创建组时的序号，txt 文档格式也可选择编码格式为 ANSI。

2. 单击页面右上方【导入】，导入文件进行用户备注。
3. 单击【确定】，在备注对象列表，查看导入结果。

——结束

4.9.3.3.3.3. 配置流量控制策略组

通过此操作，配置策略组，并设置生效周期及时间，具体操作请参见配置流量控制策略组。

4.9.3.3.3.4. 配置流量控制策略

通过此操作，创建流量控制策略，对已创建的用户组进行管控。

操作步骤

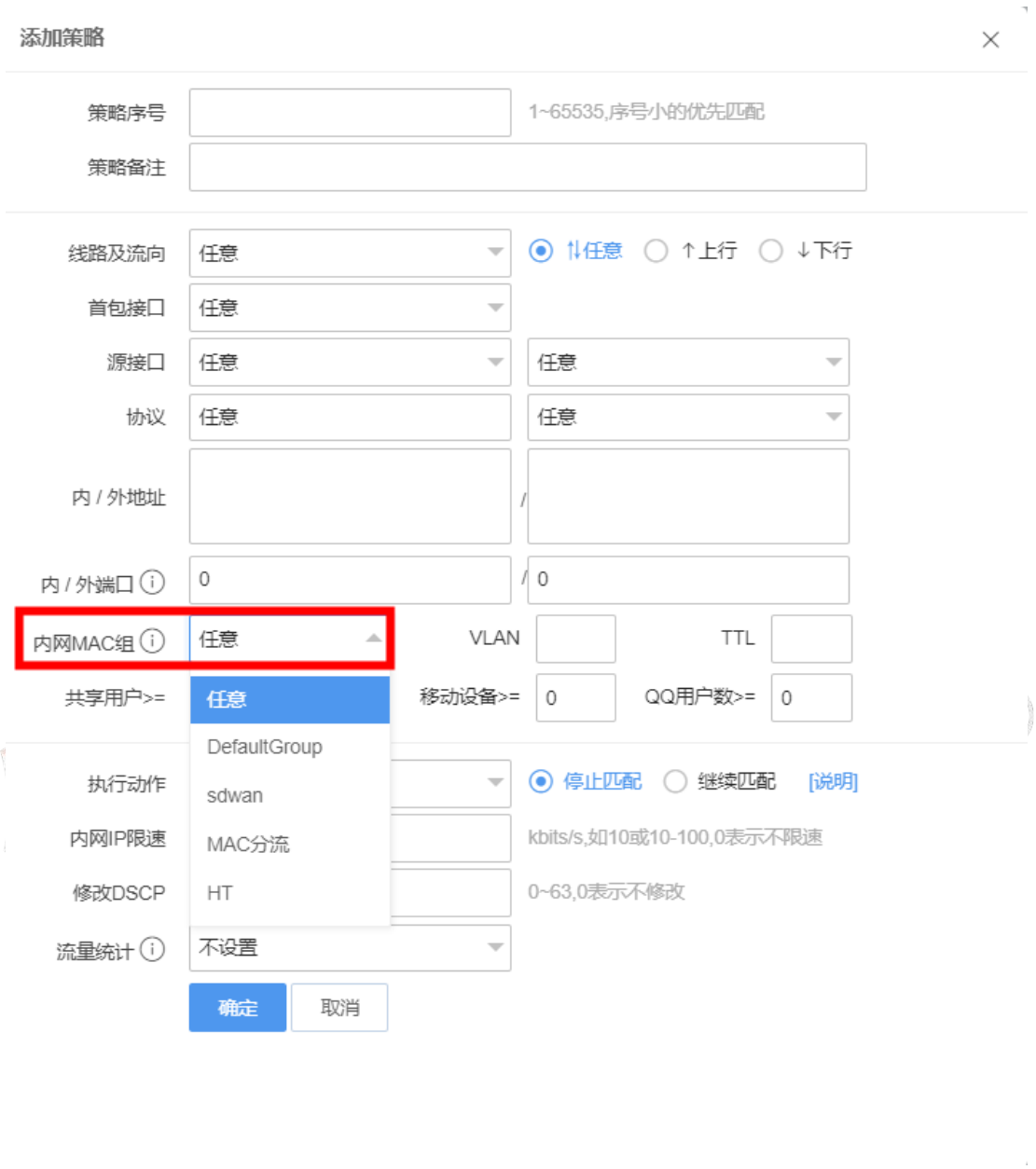
步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【行为管理】>【流量控制】。

步骤 4 鼠标悬停已创建策略组名称，单击【添加策略】。

步骤 5 配置流量控制策略，其中内网 MAC 组选择已创建的 MAC 组，单击【确定】。



配置示例：内网 MAC 组选择“打印机”，执行动作设置为“阻断”。

——结束

4.9.3.4. 应用案例：流量镜像

某用户需要旁路部署一台 WAF（WEB 应用防护系统）及一台 IDS（入侵检测系统），具体需求如下：

1. 内网核心交换机镜像口不足，需要由 Panabit 进行镜像。选取空闲的两个接口（例子中为 eth3/eth4），eth3 连接 WAF，eth4 连接 IDS，分别进行流量镜像。

2. WAF 与 IDS 需要的流量不同，需要将 HTTP/HTTPS 的流量镜像至 WAF，将全流量镜像至 IDS。

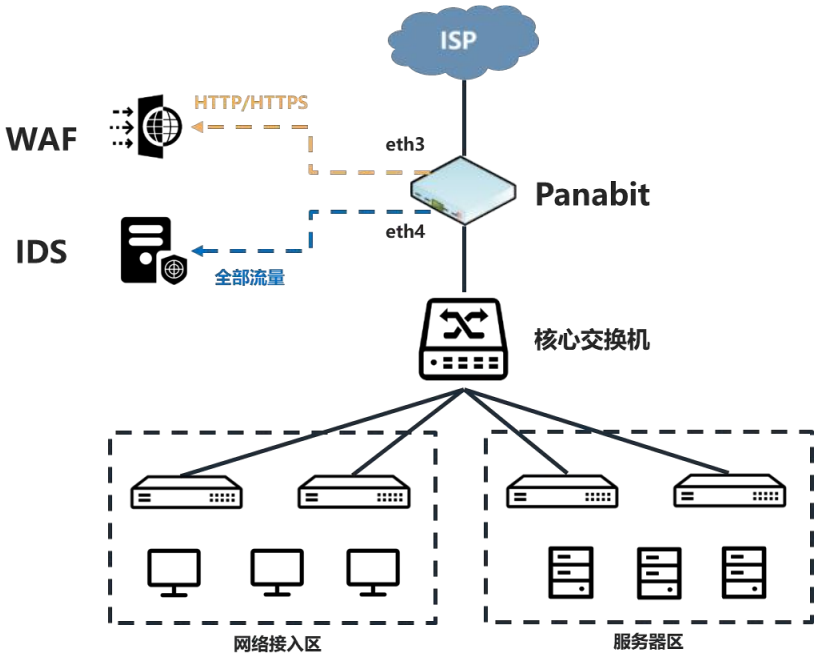


图 4-78 流量镜像拓扑

4.9.3.4.1. 配置流程

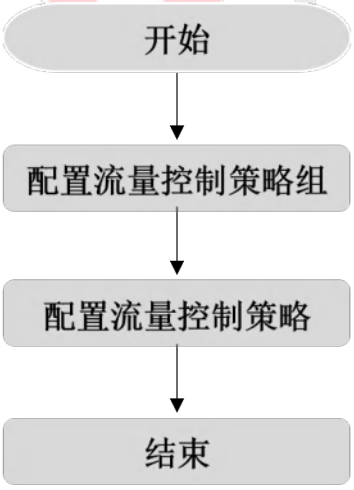


图 4-79 流量镜像配置流程

4.9.3.4.2. 配置前提

- Panabit 上网行为管理设备以网关模式或网桥模式部署在用户网络出口。
- Panabit 以旁路模式部署时，也能够支持流量镜像功能。

- 开始配置前，已完成设备部署，具体操作请参见设备部署。

4.9.3.4.3. 配置步骤

4.9.3.4.3.1. 配置流量控制策略组

通过此操作，配置策略组，并设置生效周期及时间，具体操作请参见配置流量控制策略组。

4.9.3.4.3.2. 配置流量控制策略

通过此操作，创建流量控制策略，对相应的流量进行镜像。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【行为管理】>【流量控制】。

步骤 4 鼠标悬停已创建策略组名称，单击【添加策略】。

步骤 5 配置流量控制策略，单击【确定】。

配置示例：

1. 单击【添加策略】，策略序号设为“1000”，协议选择“HTTP 协议”。执行动作选择“端口镜像”，执行动作过后选择“继续匹配”，网络接口选择 eth3，单击确定。
2. 再次单击【添加策略】，策略序号设入“2000”，其他条件默认，执行动作选择“端口镜像”，网络接口选择 eth4，单击确定。

——结束

配置效果：

1. 策略序号为 1000 的策略，由于其序号最小，因此会被优先匹配，即，所有被识别为“HTTP 协议”的流量，均会被复制一份，从 eth3 接口输出至对端的 WAF 设备。由于策略的执行动作后为“继续匹配”，因此 HTTP 协议的流量还是会继续匹配到下一条策略。
2. 策略序号为 2000 的策略，会对所有流量进行复制，并从 eth4 接口输出至对端的 IDS 设备。

说明

1. 在上面的案例中，序号 1000 的策略，执行动作后如果选择了“停止匹配”，则序号为 2000 的策略镜像的流量中，就不会包含 HTTP 协议的流量。

2. 序号为 2000 的策略，如果后面还需要添加其他的流量控制策略，则执行动作后也应该选择“继续匹配”，否则序号大于 2000 的策略就不会被匹配（选择“停止匹配”后，所有的流量已经匹配了序号 2000 的策略，就不再向下匹配）。

说明

Panabit 还支持一种特殊的流量镜像：iWAN 镜像。数据包被复制后，通过 iWAN 隧道传输到远端设备。

iWAN 线路的创建，请参见配置 iWAN 线路。

4.9.3.5. 应用案例：流量统计

流量统计具体配置操作请参见应用案例：基于流量统计的告警。

4.9.4. 数据通道

4.9.4.1. 概述

数据通道是对流量进行整体管控的手段，其目的是实现整体的流量限速。

优先级是在整体的流量限速基础上的一个扩展功能。当策略动作为“数据通道”时，可以设置优先级。

在数据通道内，可以对每个优先级设置保证带宽，这解决了优先级高的流量完全抢占数据通道，优先级低的流量完全抢占不到带宽的问题。

数据通道可以配置每日限额。用来控制每日经过数据通道的数据总量。当限额用完后，超过的数据将被丢弃。这个功能可以用来保护重要的数据服务器，防止数据被恶意访问或盗取。

4.9.4.2. 应用案例：通道限速

某用户内网有 100 个上网用户，出口带宽为 200M。员工经常使用 P2P 下载，占用大量带宽，但不能完全禁止，需要将 P2P 下载的下行整体带宽限制在 30M 以内。

4.9.4.2.1. 配置流程

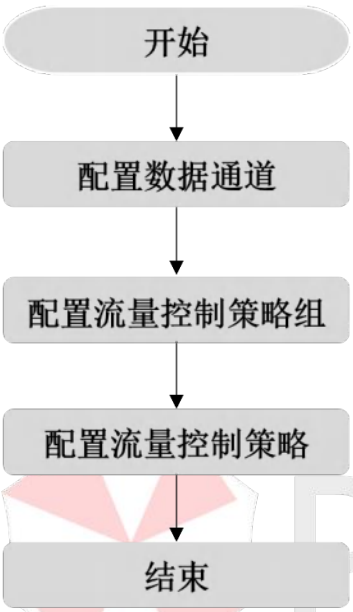


图 4-80 通道限速配置流程

4.9.4.2.2. 配置前提

Panabit 上网行为管理设备以网关模式或网桥模式部署在用户网络出口，开始配置前，已完成设备部署，具体操作请参见设备部署。

4.9.4.2.3. 配置步骤

4.9.4.2.3.1. 配置数据通道

通过此操作，配置数据通道，对需要管控的流量进行优先级排序或整体限速，待后续策略调用。策略生效后，匹配条件的流量将进入数据通道。

操作步骤

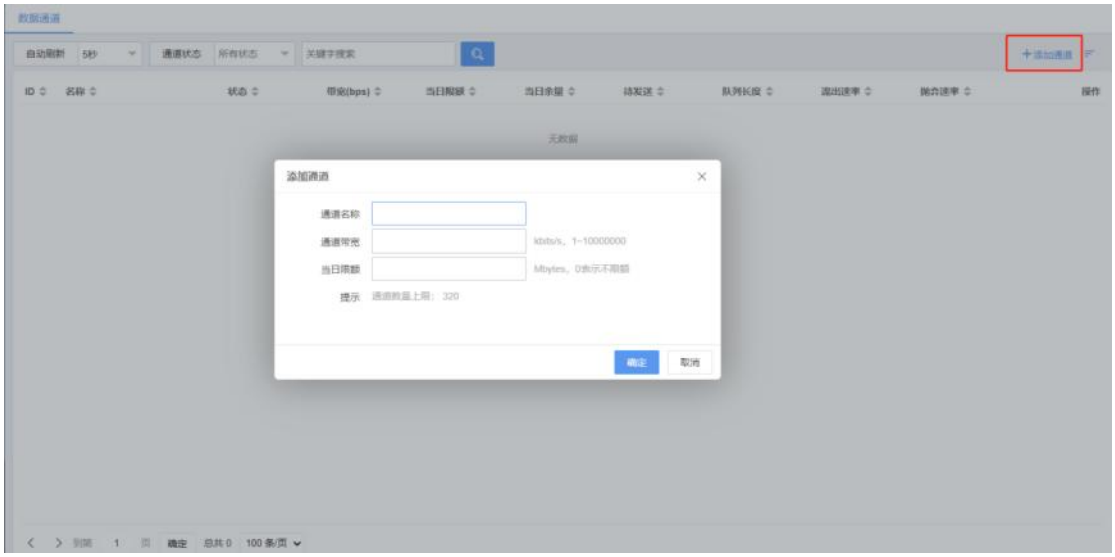
步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【行为管理】>【数据通道】。

步骤 4 单击【添加通道】，弹出添加通道页面。

步骤 5 配置数据通道，单击【确定】。



说明

最多可以添加 320 个数据通道，通道最大带宽为 10G。

参数名称	参数说明
通道名称	自定义数据通道的名称。
通道带宽	数据通道的整体带宽。 单位：kbits/s，取值：1~10000000
当日限额	当天流入该通道的数据超过这个限额后，后续进入通道的数据包都被丢弃。 单位：Mbytes，0 表示不限额。

配置示例：输入通道名称为“P2P 下载限速通道”，通道带宽为“30000”，当日限额为“0”。

——结束

4.9.4.2.3.2. 配置流量控制策略组

通过此操作，配置策略组，并设置生效周期及时间，具体操作请参见配置流量控制策略组。

4.9.4.2.3.3. 配置流量控制策略

通过此操作，配置流量控制策略，对不同协议进行流量的允许、阻断、限速等操作。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【行为管理】>【流量控制】。

步骤 4 鼠标悬停已创建策略组名称，单击【添加策略】。

步骤 5 配置流量控制策略，单击【确定】。

配置示例：

单击【添加策略】，策略序号设为“1000”，线路及流向选择“下行”，协议选择“P2P 下

载”， 执行动作选为“通道限速”，数据通道选择此前创建的“P2P 下载限速通道”。

策略生效后，P2P 下载类应用的下行速度之和，最终将不能超过“P2P 下载限速通道”的通道带宽大小，即 30000kbits/s。

——结束

说明

1. 限速是通过策略实现可控的数据包丢弃，防止有限的带宽资源耗尽，从而导致不可控的数据包丢弃。
2. 单 IP 限速和数据通道限速本质上都是限速，都是丢包。只是对于丢包的阈值统计方式不一样。
3. 对于 P2P 应用的限速，使用数据通道限制上行，比单 IP 限速效果要更好。
4. 对上行做限速也能影响下行的流入速率。当内网用户对带宽需求过大，导致出口线路的下行流量一直跑到峰值时，可以尝试使用上行限速来压制下行流量，保证重要业务。
5. 流量进入数据通道才能使用优先级，优先级是抢占数据通道带宽能力的体现，优先级的配置根据自己业务需求而定，不是必选项。需要 100%保障的业务，不需要放入数据通道内。
6. 动态限速是单 IP 限速的一种扩展，可以采用上行动态限速，下行不限速。这样能降低带宽浪费，但是对策略编写能力要求很高。

4.9.4.3. 应用案例：通道优先级

某用户内网有 100 个上网用户，出口带宽为 200M，具体需求如下：

1. 财务部的流量优先级最高，IP 地址范围：192.168.3.200-192.168.3.210。
2. 用户经常使用视频会议，需要保障在忙时，视频会议能够正常使用，带宽不得低于 50M，但最大不能超过 100M。

4.9.4.3.1. 配置流程

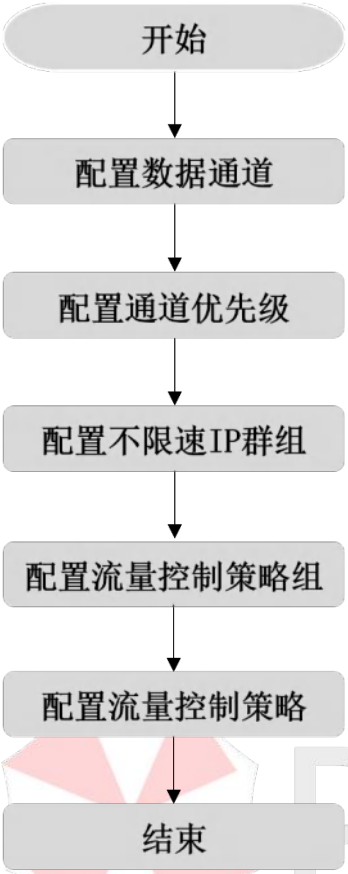


图 4-81 通道优先级配置流程

4.9.4.3.2. 配置前提

Panabit 上网行为管理设备以网关模式或网桥模式部署在用户网络出口，开始配置前，已完成设备部署，具体操作请参见设备部署。

4.9.4.3.3. 配置步骤

4.9.4.3.3.1. 配置数据通道

通过此操作，配置数据通道，对需要管控的流量进行优先级排序或整体限速，待后续策略调用。策略生效后，匹配条件的流量将进入数据通道，具体操作请参见配置数据通道。

配置示例：输入通道名称为“优先级通道”，通道带宽为“200000”，当日限额为“0”。

4.9.4.3.3.2. 配置通道优先级

操作步骤

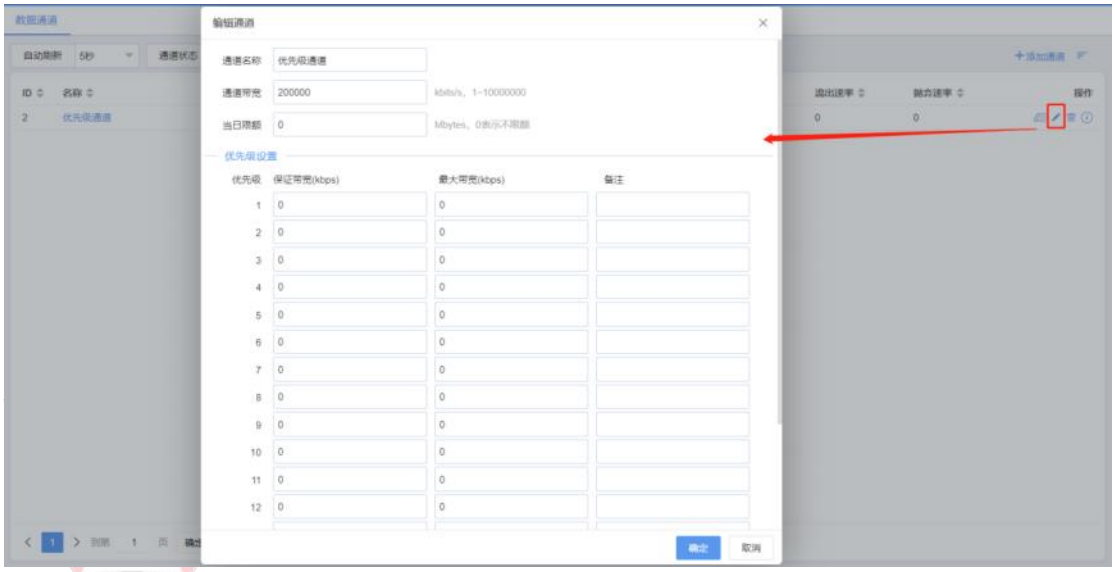
步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【行为管理】>【数据通道】。

步骤 4 单击当前数据通道操作列的 ，弹出编辑通道页面。

步骤 5 配置通道优先级，单击【确定】。



参数名称	参数说明
优先级	优先级有 1-16，十六个等级，1 优先级最高，16 优先级最低。 **说明** 优先级通过队列实现，流量控制模块会对匹配带有优先级策略的数据包进行优先级的标记。数据包根据自身优先级抢占队列。由于队列的长度是有限，因此在大流量的环境下不适宜用优先级。
保证带宽	在数据通道内可以对每个优先级设置保证带宽，用于保障（相对）低优先级的流量，使其至少能使用设置的带宽大小。各个优先级保证带宽的数值之和不能超过数据通道大小。 单位：kbps
最大带宽	为优先级设置最大可使用的带宽，用于限制（相对）高优先级的流量，使其不超过设置的带宽大小。 单位：kbps
备注	对优先级进行描述。

配置示例：

1. 优先级 1，备注输入“财务优先”。
2. 优先级 2，保证带宽输入“50000”，最大带宽输入“100000”，备注输入“视频会议”。
3. 优先级 3，备注输入“其他流量”。

——结束

4.9.4.3.3.3. 配置不限速 IP 群组

通过此操作，配置不限速 IP 群组，待后续策略调用。策略生效后，添加到群组的 IP 不再受其他控制策略影响，具体操作请参见配置不限速 IP 群组。

配置示例：输入群组名称为“财务部”，输入 IP 地址为“192.168.3.200-192.168.3.210”。

4.9.4.3.3.4. 配置流量控制策略组

通过此操作，配置策略组，并设置生效周期及时间，具体操作请参见配置流量控制策略组。

4.9.4.3.3.5. 配置流量控制策略

通过此操作，配置流量控制策略，对不同协议进行流量的允许、阻断、限速等操作。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【行为管理】>【流量控制】。

步骤 4 鼠标悬停已创建策略组名称，单击【添加策略】。

步骤 5 配置流量控制策略，单击【确定】。

配置示例：

1. 单击【添加策略】，策略序号设为“1000”，内网地址类型选择“IP 群组”，IP 选择“财务部”，执行动作选为“通道限速”，数据通道选择此前创建的“优先级通道”，通道优先级设置为 1，单击【确定】。
2. 单击【添加策略】，策略序号设为“2000”，协议选择“腾讯会议”，执行动作选为“通道限速”，数据通道选择此前创建的“优先级通道”，通道优先级设置为 2，单击【确定】。
3. 单击【添加策略】，策略序号设为“3000”，执行动作选为“通道限速”，数据通道选择此前创建的“优先级通道”，通道优先级设置为 3，单击【确定】。

配置效果：

1. 序号为 1000 的策略，财务部的流量适用优先级 1，其优先级最高，不会被其他流量抢占。
2. 序号为2000的策略，腾讯会议的流量适用优先级2，保证带宽为50M，最大带宽为100M。
3. 序号为 3000 的策略，表示其余流量适用优先级 3，优先级最低。

——结束

4.9.5. 连接控制

4.9.5.1. 概述

连接控制针对内网每一个 IP 的并发连接数进行控制，可单独针对内网某个 IP 下的 TCP 连接、UDP 连接或整体的连接数进行管控。

该功能适用于内网有主机中毒或木马， 爆发疑似攻击现象时的临时处理或预先处理。

4.9.5.2. 配置流程

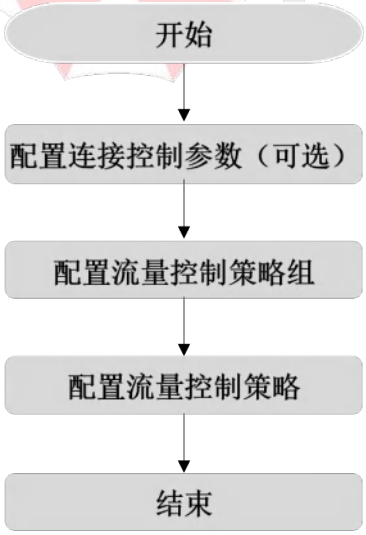


图 4-82 连接控制配置流程

4.9.5.3. 配置前提

Panabit 上网行为管理设备以网关模式或网桥模式部署在用户网络出口，开始配置前，已完成设备部署，具体操作请参见设备部署。

4.9.5.4. 配置步骤

4.9.5.4.1. 配置连接控制参数（可选）

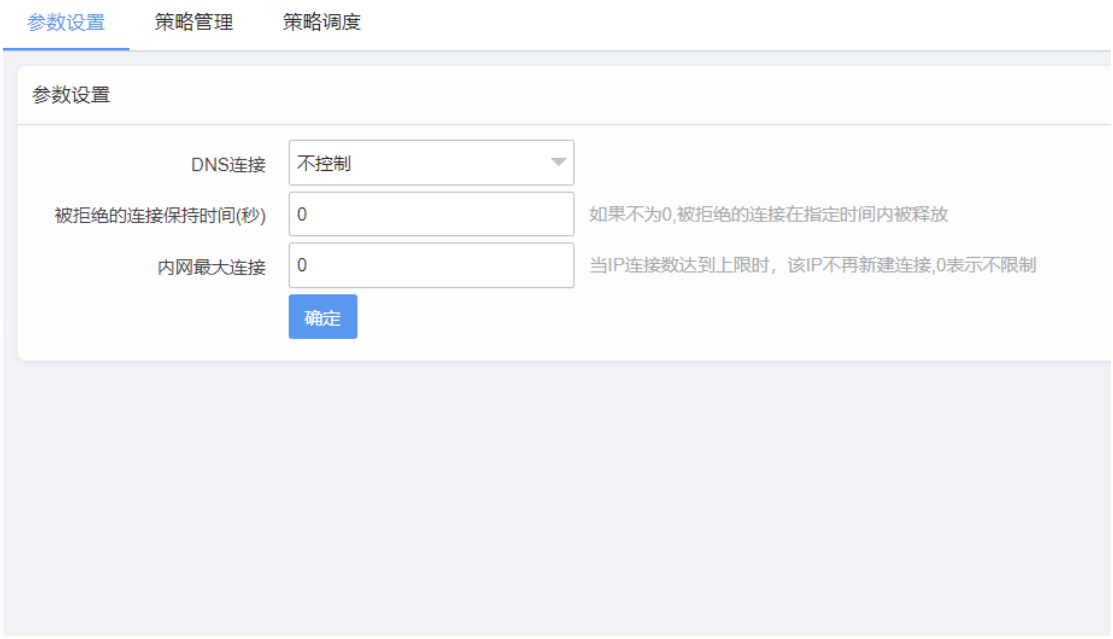
通过此操作，修改连接控制参数。一般情况下无需进行修改，使用默认设置即可。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【行为管理】>【连接控制】>【参数设置】。



参数名称	参数说明
DNS 连接	取值：控制/不控制。 如果选择不控制，即使在策略里做了对 DNS 的连接控制策略，系统也不会对 DNS 的连接做控制动作。
被拒绝的连接保持时间	单位：秒。 连接被策略拒绝后，Panabit 在设置的时间过后，对连接进行删除；如果该参数为 0，那么 Panabit 将按照默认的老化时间对连接进行删除。
内网最大连接	该参数为一个全局设置。 内网 IP 的连接数达到设定的值后，Panabit 不会再对该内网 IP 新建连接，如果为 0 不进行限制。

步骤 4 配置参数，单击【确定】。

——结束

4.9.5.4.2. 配置连接控制策略组

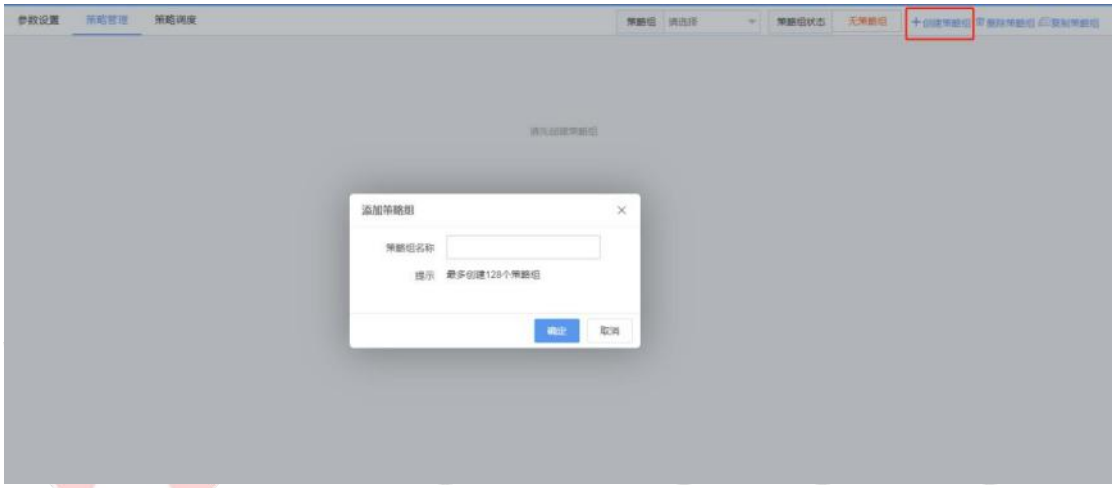
通过此操作，配置策略组，并设置生效周期及时间。

操作步骤

步骤 1 选择【行为管理】>【连接控制】>【策略管理】。

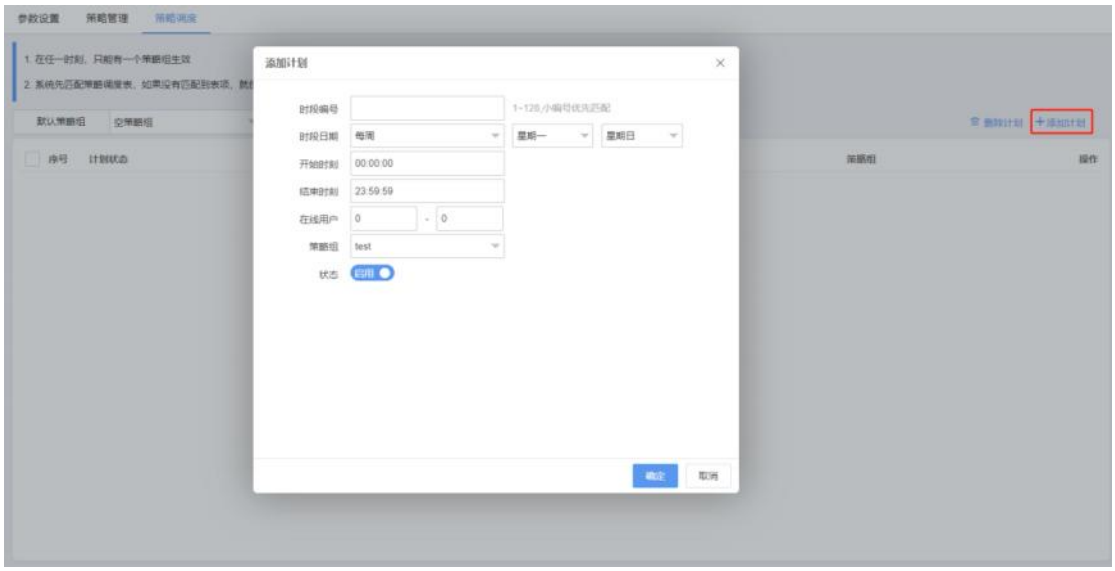
步骤 2 单击页面右上角的【创建策略组】。

步骤 3 自定义策略组名称，单击【确定】。



步骤 4 选择【行为管理】>【连接控制】>【策略调度】。

步骤 5 单击【添加计划】，配置计划中的参数。



参数名称	参数说明
时段编号	定义该计划时段的编号，序号越小，优先级越高。

时段日期	策略组生效的日期范围。
开始时刻	策略组生效的开始时间。
结束时刻	策略组生效的结束时间。
在线用户	设置策略组生效的在线用户范围。
策略组	选择需要生效的策略组。
状态	可“启用”或“禁用”该生效时段。

步骤 6 单击【确定】。

配置示例：时段编号填入“10”，策略组选择步骤 3 中创建的策略组，状态为“启用”，其余参数暂不设置。表示在所有时间段，步骤 3 中创建的策略组均生效。

——结束

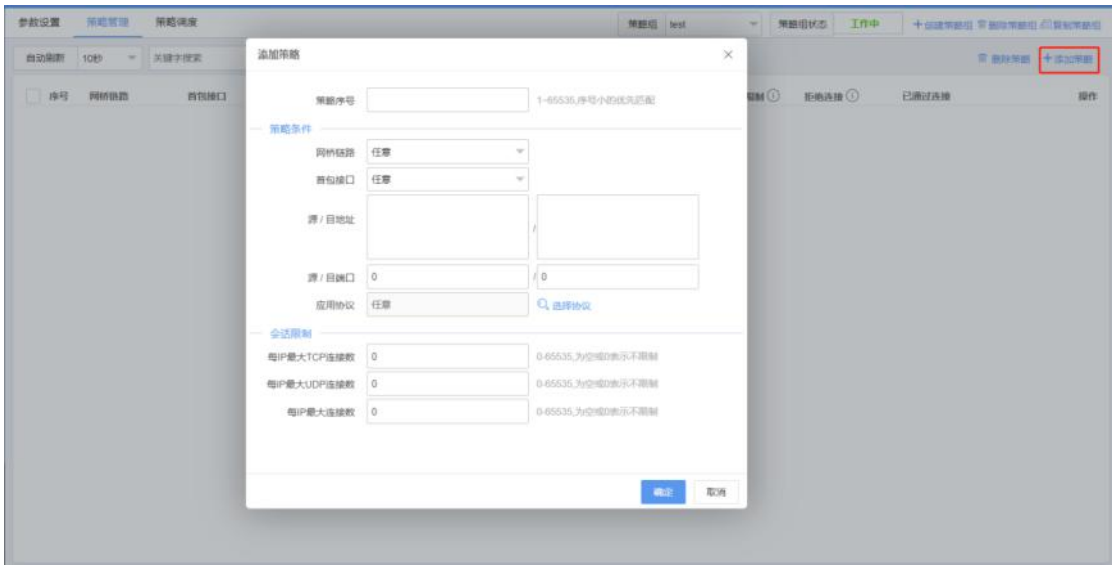
4.9.5.4.3. 配置连接控制策略

通过此操作，配置具体策略，对连接数进行控制。

操作步骤

步骤 1 选择【行为管理】>【连接控制】>【策略管理】，确定策略组状态为“工作中”。

步骤 2 单击页面右上方的【添加策略】。



参数名称	参数说明
策略序号	自定义策略的编号，系统将按照编号从小到大的方式依次执行策略表。

	设置后，该编号不可编辑，也不可上下移动。 取值：1~65535。序号越小，优先级越高。
网桥链路	匹配特定线路或网桥的数据报文。
首包接口	会话第一个数据包的源接口。
源/目地址	匹配报文中的源/目标地址。
源/目端口	匹配报文中的源/目标端口。
应用协议	对应用进行匹配，该“应用协议”可以是特征库或者自定义协议。
每 IP 最大 TCP 连接数	限制单个 IP 下的 TCP 连接总数。 取值：0-65535，为空或 0 表示不限制。
每 IP 最大 UDP 连接数	限制单个 IP 下的 UDP 连接总数。 取值：0-65535，为空或 0 表示不限制。
每 IP 最大连接数	限制单个 IP 下的所有连接总数。 取值：0-65535，为空或 0 表示不限制。

步骤 3 配置策略中的各项参数，点击【确定】提交。

配置示例：策略序号填入“10”，源地址填入“192.168.100.0/24”，每 IP 最大 TCP 连接数填入“2000”，每 IP 最大 UDP 连接数填入“2000”，每 IP 最大连接数填入“3000”，其余参数暂不设置。表示 192.168.100.0/24 地址范围内的所有单个 IP，每个 IP 最多能够通过 Panabit 的 TCP 并发连接数为 2000，UDP 并发为 2000，总并发为 3000，超过阈值的连接将会被拒绝。

——结束

4.9.6. HTTP 管控

4.9.6.1. HTTP 管控概述

超文本传输协议（HTTP，Hyper Text Transfer Protocol）是互联网上最广泛使用的网络协议之一。它由 HTTP 请求和 HTTP 响应两部分构成。当用户在浏览器中输入网址以访问某个网站时，浏览器会将这个请求封装成 HTTP 请求并发送给服务器站点。一旦服务器接收到请求，它会组织响应数据并将其封装成 HTTP 响应返回给浏览器。需要注意的是，没有请求就不会有响应。

Panabit 的 HTTP 管控功能正是基于 HTTP 的请求和响应进行运作。当用户在其终端设备上输入网址并发送请求，该请求经过 Panabit 时，Panabit 就可以对其进行管控和管理。

管控的条件有源地址、源端口、目标地址、目标端口、源接口、文件类型、访问域名等。

管控的手段有允许、阻断、信息提示、URL 跳转、报文镜像、TCP 重置等动作。

4.9.6.2. 配置流程

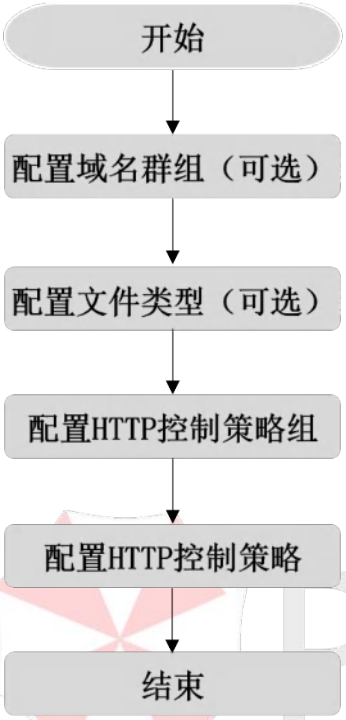


图 4-83 HTTP 管控配置流程

4.9.6.3. 配置前提

Panabit 上网行为管理设备以网关模式或网桥模式部署在用户网络出口，开始配置前，已完成设备部署，具体操作请参见设备部署。

4.9.6.4. 配置步骤

4.9.6.4.1. 配置域名群组（可选）

通过此操作，配置需要管控的域名群组，待后续策略调用。策略生效后，针对该群组中域名的请求将执行相应的动作。具体请参见域名群组。

4.9.6.4.2. 配置文件类型（可选）

通过此操作，配置需要管控的文件类型，待后续策略调用。具体请参见文件类型。

4.9.6.4.3. 配置 HTTP 管控策略组

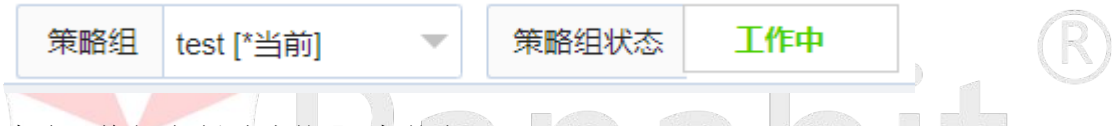
通过此操作，配置策略组，并设置生效周期及时间。HTTP 管控策略组的配置，与连接控制类似，参见配置连接控制策略组。

4.9.6.4.4. 配置 HTTP 管控策略

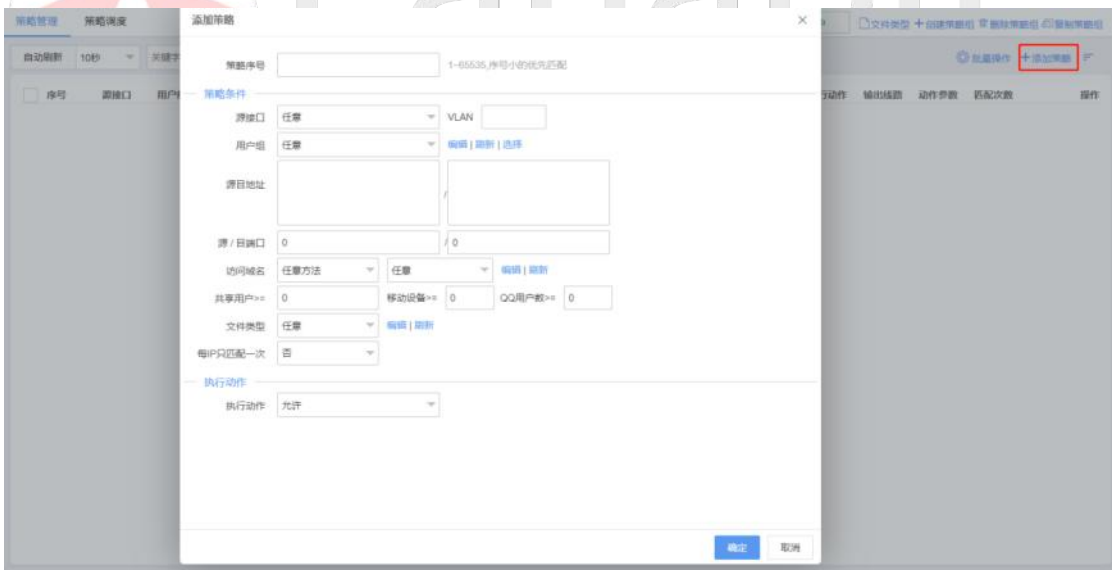
通过此操作，配置具体策略，对 HTTP/HTTPS 请求进行控制。

操作步骤

步骤 1 选择【行为管理】>【HTTP 管控】>【策略管理】，确定策略组状态为“工作中”。

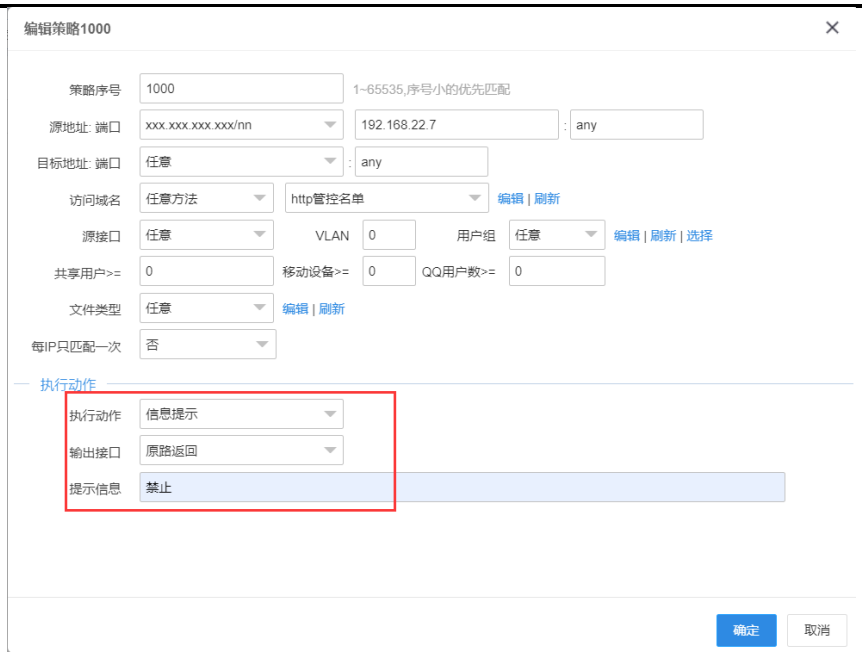


步骤 2 单击页面右上方的【添加策略】。

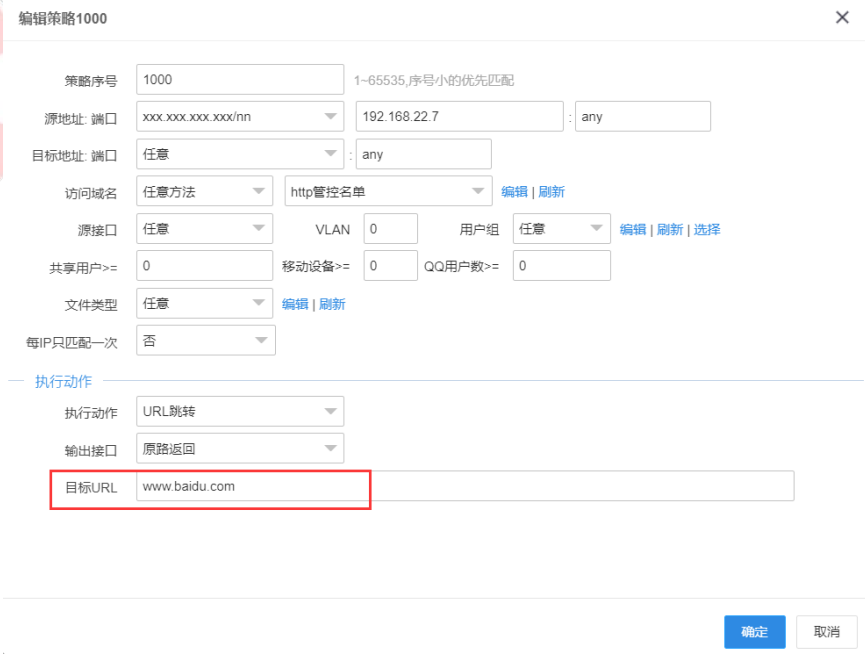


参数名称	参数说明
策略序号	自定义策略的编号，系统将按照编号从小到大的方式依次执行策略表。 设置后，该编号不可编辑，也不可上下移动。 取值：1~65535。序号越小，优先级越高。
源接口	选择某个内网物理接口或逻辑 LAN 接口进行匹配。

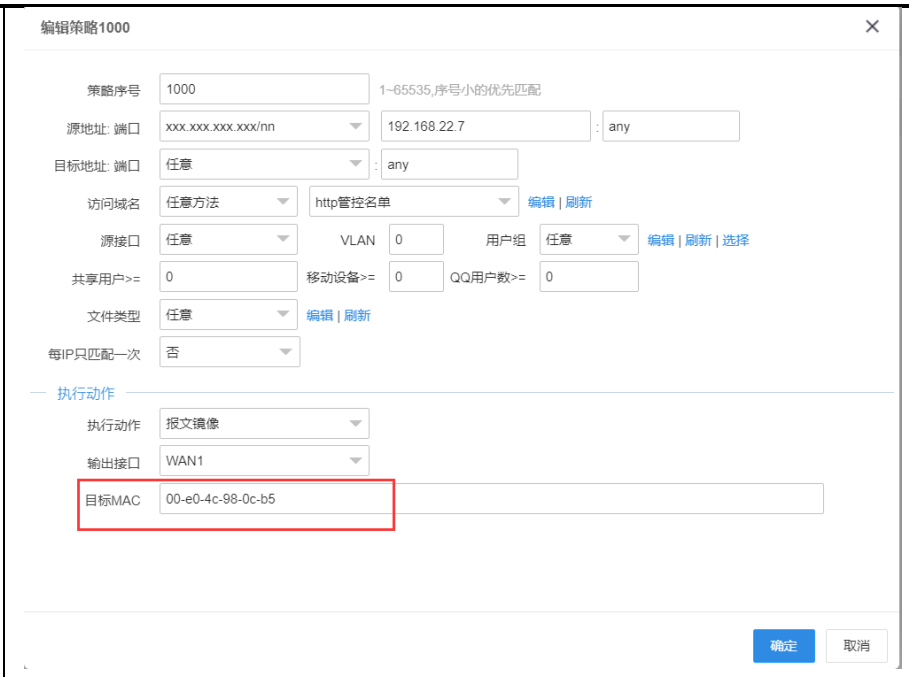
VLAN	匹配数据报文的 VLAN-Tag。
用户组	用户组织架构中的分组，详见组织架构。
源/目地址	匹配报文中的源/目标地址。
源/目端口	匹配报文中的源/目标端口。
访问域名	可以选择访问方式：GET 或者 POST，该选项只能和 HTTP 请求匹配。 可以选择一个域名群组，域名群组内的内容可以是域名，也可以是 URL，如果是 URL，则只有 HTTP 的请求才会匹配到，HTTPS 的请求只能匹配域名。
共享用户>=	基于共享用户数的策略调用条件。
移动设备>=	基于移动设备连接数的策略调用条件。
QQ 用户数>=	基于 QQ 用户登录数的策略调用条件。
文件类型	在【对象管理】>【文件类型】里定义 HTTP 请求的文件后缀名，比如 exe,rar 等。
每 IP 只匹配一次	可选择“是”或“否”。若选择“是”，则对匹配条件的流量，只匹配一次，意味着执行动作也就只执行一次；若选择“否”，则执行动作可重复执行多次。
执行动作	● 允许：即对匹配条件的数据不做任何处理，直接放行。 ● 阻断：即对匹配条件的数据进行阻断，不允许访问，阻断动作适用于 HTTP 的域名、HTTP 的 URL、HTTPS 的域名。 ● 信息提示：用户使用浏览器访问 HTTP 网页时，发送 HTTP 请求，Panabit 捕获 HTTP 请求，匹配条件后会走输出接口路径，在浏览器中返回所输入的提示信息界面。



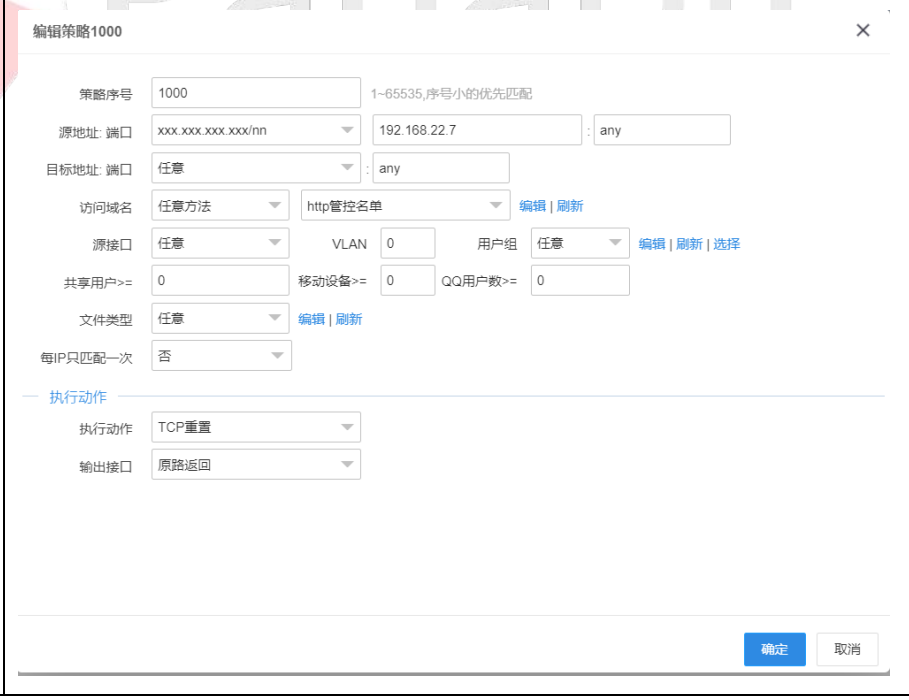
- URL 跳转：访问网页的基础是通过 URL，Panabit 在捕获 HTTP 请求后，将用户原本访问的 URL 重定向至我们输入的目标 URL 实现跳转的功能，同时 URL 跳转的目标也可以是 IP。



- 报文镜像：对于某些需要分析报文的情况，Panabit 可以将匹配条件的 URL 请求报文数据镜像至“输出接口”，并通过填写对端接收设备的 MAC 精确传输。



- TCP 重置：对于 HTTPS 的网页来说，由于 HTTPS 是加密传输的，导致目前所有的协议分析软件都只能捕获到 HTTPS 的通讯数据包，但不能分析并重组出它具体的访问信息，导致管控不力。在 Panabit 中，我们通过发送 RST 报文，用异常的关闭连接来阻断 HTTPS 网页的访问，使得终端电脑访问 HTTPS 网页时一样能被管控。



步骤 3 配置策略中的各项参数，点击【确定】提交。

配置示例：策略序号填入“10”，访问域名选择一个包含了“taobao.com”的域名群组“test”，执行动作选择“TCP 重置”，其余参数暂不设置。表示所有通过 Panabit，针对

taobao.com 的 HTTP/HTTPS 网页访问，均会被阻断，效果如下图：

——结束

4.9.7. DNS 管控

4.9.7.1. DNS 管控概述

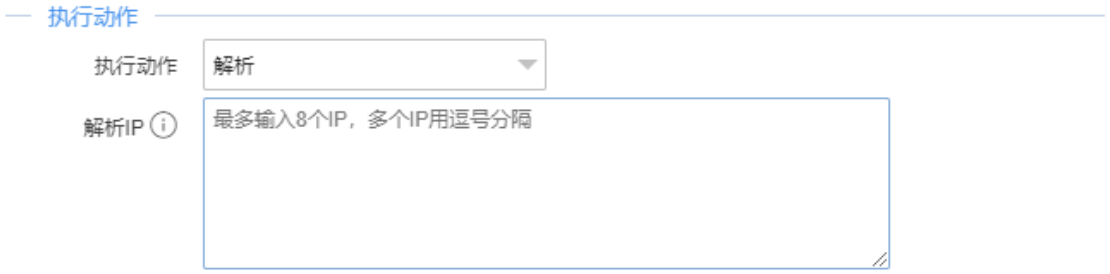
Panabit 上网行为管理能够针对 DNS 数据报文进行特殊控制，对 DNS 数据报文进行丢弃，牵引，解析，QPS 限速等操作。

- 放行：对匹配策略的 DNS 数据报文不经过任何改变，直接放行。
- 丢弃：对匹配策略的 DNS 数据报文直接丢弃。
- 牵引：对匹配策略的 DNS 数据报文，将目标 DNS 地址转换成所设置的 IP，该设置优先 WAN 线路 DNS 设置。

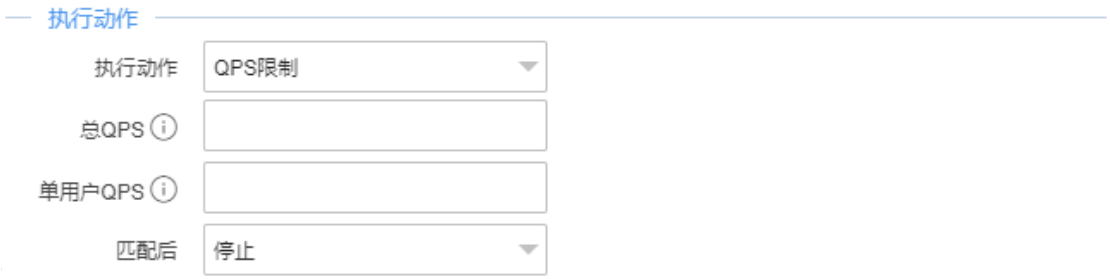
  - 牵引线路：选择牵引动作的 WAN 线路。
  - 牵引 DNS：默认使用牵引线路的 DNS，如果输入则使用输入的 IP，最多输入 4 个

IP，多个 IP 用逗号分隔。

- 解析：对匹配策略的 DNS 数据报文，直接返回的域名解析结果，返回的解析结果为所填 IP 地址。最多输入 8 个 IP，多个 IP 用逗号分隔。



- QPS 限制：对匹配策略的 DNS 的 QPS（每秒最大请求数）做限制。



  - 总 QPS：对整体每秒最大请求数的限制。
  - 单用户 QPS：对单个 IP 每秒最大请求数的限制

4.9.7.2. 应用案例：DNS 丢弃与控制

某用户内网有 100 个上网用户，出口带宽为 200M。具体需求如下：

1. 禁止员工在上班时间使用购物网站，如淘宝，京东等（上班时间为周一到周五 9:00-18:00）。
2. 为防止内/外网发起大量 DNS 请求的 DDoS 攻击，需要对每秒流经设备的 DNS 请求数进行限制，总 QPS 限制为 1000，单用户的 QPS 限制为 100。

4.9.7.2.1. 配置流程

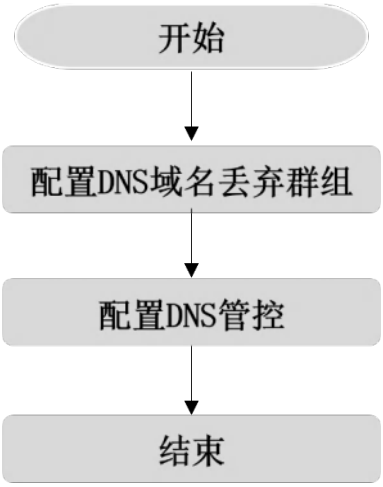


图 4-84 DNS 丢弃与控制配置流程

4.9.7.2.2. 配置前提

Panabit 上网行为管理设备以网关模式或网桥模式部署在用户网络出口，开始配置前，已完成设备部署，具体操作请参见设备部署。

4.9.7.2.3. 配置步骤

4.9.7.2.3.1. 配置域名群组

通过此操作，配置 DNS 域名丢弃群组，待后续策略调用。策略生效后，针对该群组中域名的 DNS 请求将被丢弃。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【对象管理】>【域名群组】。

步骤 4 单击【添加】，弹出添加域名群组页面

步骤 5 输入域名，单击【确定】。

配置示例：输入域名为“DNS 丢弃域名”。

步骤 6 单击当前域名操作列的 ，选择域名群组，添加域名。

步骤 7 单击【确定】。

配置示例：选择域名群组为“DNS 丢弃域名”，输入域名“www.taobao.com”。

——结束

4.9.7.2.3.2. 配置 DNS 管控

通过此操作，配置 DNS 管控，可针对 DNS 数据报文进行特殊控制，对 DNS 数据报文进行放行、丢弃等操作。

操作步骤

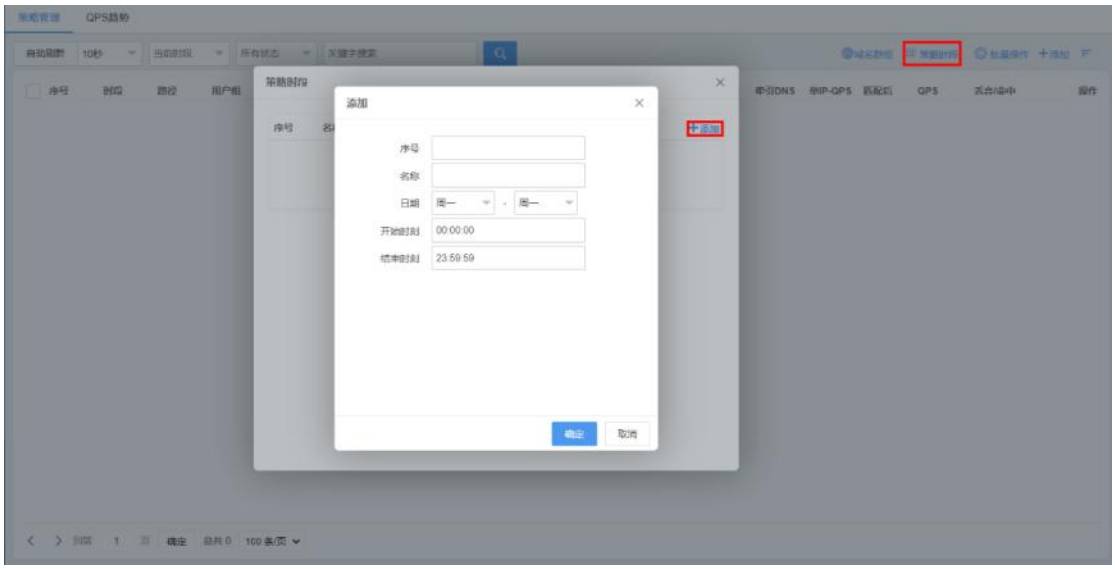
步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【DNS 管控】>【策略管理】。

步骤 4 选择页面右侧的【策略时段】，单击【添加】。

步骤 5 配置策略时段，单击【确定】。



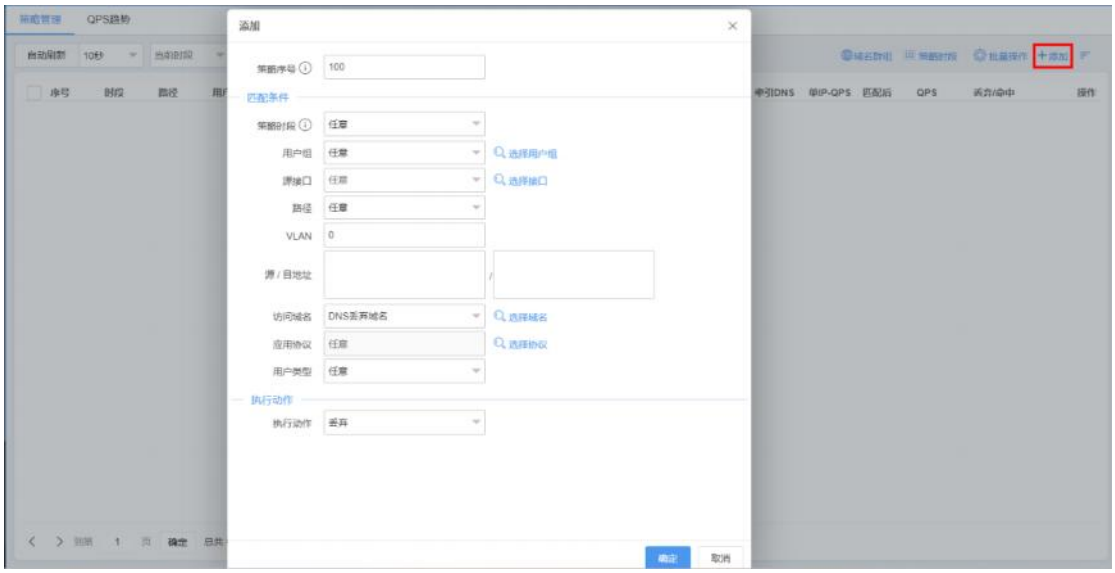
参数名称	参数说明
序号	策略时段的编号，用于标识不同的策略时段。
名称	策略的名称。
日期	策略生效的日期。
开始时刻	策略生效的开始时间。
结束时刻	策略生效的结束时间。

配置示例：

1. 序号设为“10”，名称设为“工作时段”，日期选择“周一到周五”，开始时刻设为“9:00:00”结束时刻设为“18:00:00”，点击【确定】。
2. 序号设为“20”，名称设为“全部时段”，直接点击【确定】。

步骤 6 选择【网络管理】>【DNS 管控】>【策略管理】。

步骤 7 单击页面右上角的【添加】，配置 DNS 管控。



参数名称	参数说明
策略序号	策略的编号，系统将按照编号从小到大的方式依次执行策略表，该编号不可编辑，也不可上下移动。 取值：1~65535。编号越小，优先级越高。
策略时段	策略只在该时间段内生效。
用户组	用户组织架构中的分组，详见组织架构。
源接口	选择某个内网物理接口或逻辑 LAN 接口进行匹配。
路径	可选择某个网桥或全部路径内的数据进行匹配。
VLAN	匹配数据报文的 VLAN-Tag。
源/目地址	匹配源/目的 IP 地址，该地址为 XXX.XXX.XXX.XXX/NN 或 n.n.n.n-m.m.m.m 或是一个 IP 群组。
访问域名	匹配用户侧的 DNS 报文所含的域名，可指定一个域名列表。
应用协议	对应用进行匹配，该“应用协议”可以是特征库或者自定义协议，并且关联了域名特征，否则该策略无意义。
用户类型	可设为代拨用户、非代拨用户，或者任意。
执行动作	当数据报文与上述的策略条件相匹配后所执行的动作。

步骤 8 单击【确定】。

配置示例：

1. 策略序号设为“100”，策略时段设为“工作时段”， 访问域名设为“DNS 丢弃域名”，执行动作设为“丢弃”。
2. 策略序号设为“200”，策略时段设为“全部时段”，执行动作设为“QPS 限制”，总 QPS 设为“1000”，单用户 QPS 设为“100”。

配置效果：

1. 序号为100的策略，由于其序号最小，因此会被优先匹配，即，在工作时间内，访问淘宝的DNS请求均会被丢弃，用户无法访问淘宝网页。
2. 序号为200的策略，能够在全部时间段，对其他所有DNS请求的QPS进行限制，总QPS限制为1000，单用户限制为100，超过阈值的DNS请求会被丢弃。

——结束

4.9.7.3. 应用案例：DNS牵引

某用户内网中，很多 PC 的 DNS 遭受篡改，导致网站访问缓慢。需要在出口进行 DNS 重定向，将所有向外的DNS请求牵引至223.5.5.5及114.114.114.114。

4.9.7.3.1. 配置流程

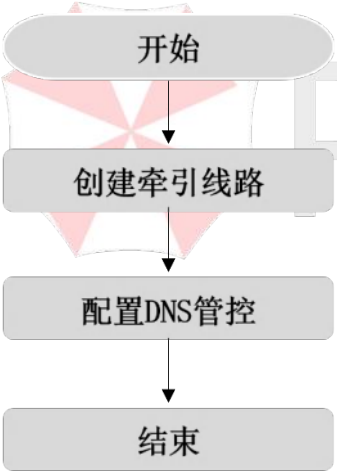


图 4-85 DNS牵引配置流程

4.9.7.3.2. 配置前提

Panabit 上网行为管理设备以网关模式或网桥模式部署在用户网络出口，开始配置前，已完成设备部署，具体操作请参见设备部署。

4.9.7.3.3. 配置步骤

4.9.7.3.3.1. 创建牵引线路

在 Panabit 上设置一个 WAN 线路（可以新建线路，或利用已有的线路），通过这条 WAN 线路，我们把 DNS 的流量牵引到指定的 DNS 服务器上。

参见配置 WAN 线路。

4.9.7.3.3.2. 配置 DNS 管控

通过此操作，配置 DNS 管控，针对 DNS 数据报文进行牵引控制，对出网的 DNS 数据报文进行重定向。

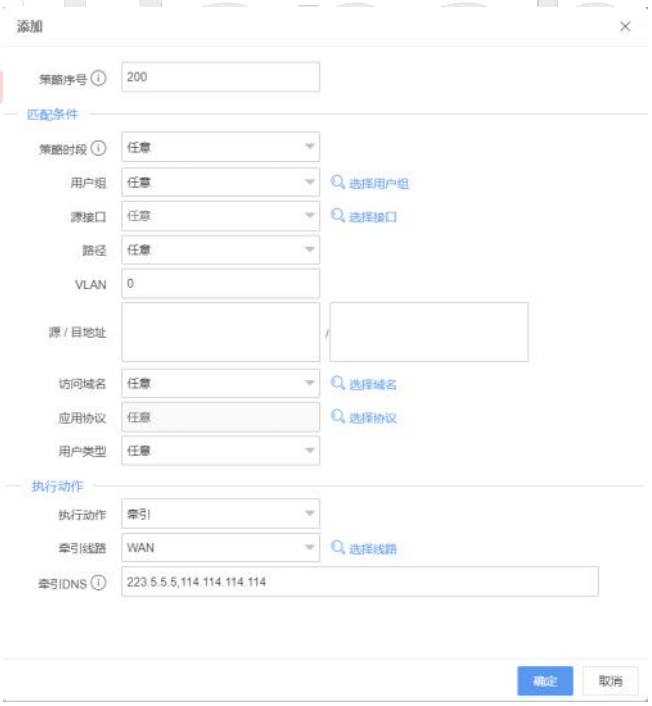
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【DNS 管控】>【策略管理】。

步骤 4 单击页面右上角的【添加】，配置 DNS 管控，点击确定。



配置示例：

策略序号设为“200”，执行动作设为“牵引”，牵引线路选择上面步骤创建的 WAN 线路，牵引 DNS 填写“223.5.5.5,114.114.114.114”。

——结束

说明

1. 牵引 DNS 一栏，如果为空，则默认会使用牵引线路中设置的 DNS。

2. 牵引时，需要确保牵引的 WAN 线路与牵引的 DNS 地址可达。

4.9.8. 常见问题

1. 如何用一条策略同时管控几个不同的应用？

答：匹配的应用支持自定义协议组，在【应用识别】、【自定义协议组】中将要选择的协议创建为协议组。然后在策略中选择新创建的协议组即可。

2. 为什么策略前/后速率有数值标红？

答：策略前/后速率表示匹配中该条策略前后符合条件流量的速率变化情况，数值标红表示该流量被此条策略的限速或阻断规则成功限制。

4.10. 链路负载

4.10.1. 概述

Panabit 上网行为管理支持传统基于网络层的链路负载均衡，还支持基于域名、应用协议的负载。同时，可设置调度通道和调度时间的组合策略，实现高级负载均衡。

Panabit 上网行为管理的链路负载功能，需要通过配置线路（逻辑接口）与策略路由来实现。

4.10.2. 应用场景

Panabit 上网行为管理在链路负载方面的应用场景相当广泛，特别是解决多出口的有限带宽场景下，通过基于应用、域名、IP 和端口等对象的调度，完成对业务路径优化，以及对重要业务正常传输进行有效保障。

4.10.3. 应用案例

某用户公司办公网络投资费用有限，出口选择了多条不同资费的线路（一条运营商专线和两条的 ADSL 拨号线路），但由于无法提供基于业务级的精细化的负载分担，导致重要业务无法使用优质的线路达到好的体验。

Panabit 上网行为管理作为出口网关进行负载，接在核心交换机和运营商光猫之间，有一条运营商专线和两条 ADSL 拨号线路。要求公司关键业务（OA、腾讯会议、常用网站）走运营商专线。其他的普通上网业务（视频、游戏、下载）负载到拨号线路。当运营商专线线路异常后，重要业务能自动负载到 ADSL 线路上。

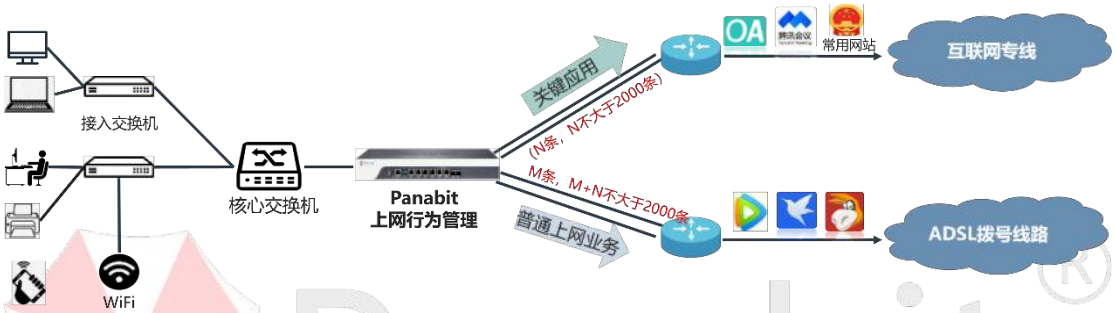


图 4-86 链路负载详情

4.10.4. 配置流程

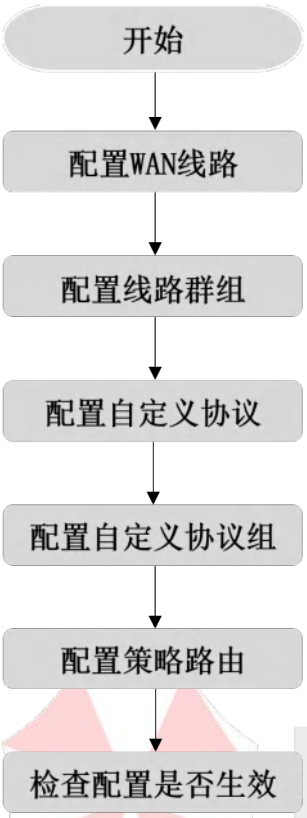


图 4-87 链路负载配置流程

4.10.5. 配置前提

Panabit 上网行为管理设备以网关模式部署在用户网络出口，开始配置前，已完成设备部署，具体操作请参见设备部署。

4.10.6. 配置步骤

4.10.6.1. 配置 WAN 线路

通过此操作，配置 WAN 线路，可设置线路的接入模式、接入方向及线路类型。

操作步骤

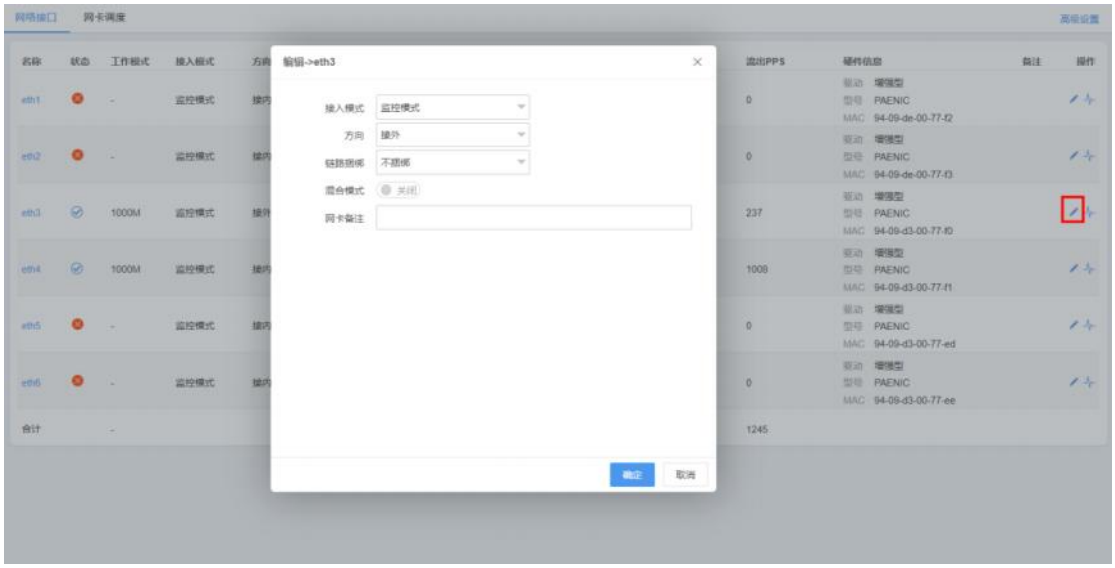
步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【网卡设置】>【网络接口】。

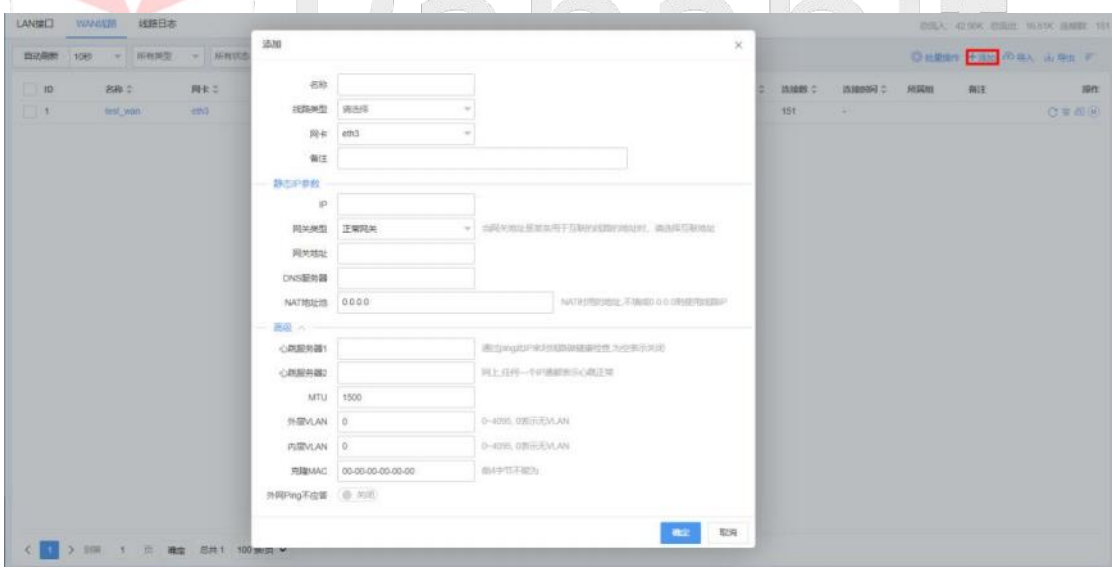
步骤 4 任选两个接口，单击操作列 ，弹出接口编辑页面，此处以 eth3、eth4 为例。

步骤 5 接入模式选择“监控模式”，方向选择“接外”，单击确定。



步骤 6 选择【网络管理】>【LAN/WAN】>【WAN 线路】。

步骤 7 单击页面右上角【添加】，弹出添加 WAN 线路页面。



参数名称	参数说明
名称	自定义 WAN 线路名称。
线路类型	WAN 线路类型，可选择“静态 IPv6”、“静态 IPv4”、“DHCP IPv4”、“PPPoE”、“iWAN”、“L2TP”、“IPsec”、“GREWAN”。
网卡	选择承载该 WAN 线路的物理网卡，网卡需提前设置为“接外网”
备注	对 WAN 线路的补充说明。

IPv6 线路参数	IPv6 IP：IPv6 的 IP。 网关地址:线路对端的网关地址。 网关类型: ● 正常网关：一般的网关类型。 ● 互联网关：当网关地址是某条用于互联的线路的地址时，请选择互联网关。 DNS 服务器：当设置 DNS 管控策略的时候， 这个选项才会起作用。
静态 IP 参数	IP：IPv4 的 IP。 网关地址:线路对端的网关地址。 网关类型: ● 正常网关：一般的网关类型。 ● 互联网关：当网关地址是某条用于互联的线路的地址时，请选择互联地址。 DNS 服务器：当设置 DNS 管控策略的时候， 这个选项才会起作用。 NAT 地址池：NAT 时用的地址，不填或 0.0.0.0 则使用线路 IP。
PPPoE 参数	PPPoE 账号/密码：输入 PPPoE 账号/密码 BRAS 名称：如果填写，只接受同名的 BRAS 服务。 Service 名称 ：如果填写，只接受同名的服务。 重拨等待时间：单位秒，避免频繁拨号而被运营商封线。
iWAN 参数	具体请参见配置 iWAN 线路。
L2TP 参数	具体请参见配置 L2TP 线路。
IPsec 参数	具体请参见配置 IPsec 线路。
GRE WAN	IP：指定本地网络的 IP 地址。 对端地址：另一个网络的 IP 地址，该网络与本地网络之间将建立隧道。 心跳间隔：隧道设备之间周期性发送心跳消息的时间间隔。这些心跳消息用于确认隧道的活动状态。0~255，0 表示关闭. 隧道校验：通过验证机制来确认隧道的状态和可用性。通过发送测试数据包或心跳消息来检查隧道是否正常工作。可“开启”或“关闭”。 隧道关键字： 在配置隧道时使用的标识符，以便在设备之间唯一标

	识隧道。取值为 0-4294967295。
心跳服务器 1	通过 ping 此 IP 来对线路做健康检查，为空表示关闭。
心跳服务器 2	通过 ping 此 IP 来对线路做健康检查，为空表示关闭。与心跳服务器 1 任何一个 IP 通都表示心跳正常。
MTU	定义数据的最大传输单元。
外层 VLAN	定义从该接口出去的数据报文所携带的外层 VLAN 标记，0 表示外出的数据不带修改 VLAN 标记，与进入接口时的 VLAN 保持一致。 取值：0~4095，0 表示无 VLAN
内层 VLAN	定义从该接口出去的数据报文所携带的内层 VLAN 标记，0 表示外出的数据不带修改 VLAN 标记，与进入接口时的 VLAN 保持一致。 取值：0~4095，0 表示无 VLAN
克隆 MAC	不使用自身携带的 MAC 地址，而是使用自定义手工输入的 MAC 地址。 格式：00-00-00-00-00-00，前 4 字节不能为空。
外网 Ping 不应答	可选择“开启”或“关闭”。

说明

- 线路类型请根据现网实际选择。当网络出口不是固定 IP，只有 PPPoE 拨号线路时，线路类型请选择“PPPoE”，然后填入 PPPoE 的账号密码；同理，线路类型也可选择 DHCP 等方式。其他的 VPN 线路类型，如 iWAN、IPsec 等，请参见虚拟专网。
- 当有多条线路时，需多次进行添加。

步骤 8 配置线路参数，单击【确定】。

配置示例：

1. 线路名称为“运营商专线”，线路类型选择静态 IPv4，网卡选择 eth3，IP 地址为 1.1.1.1，网关为 1.1.1.2。
2. 线路名称为“线路 1”（线路 1 带宽 100M），线路类型选择静态 PPPoE，网卡选择 eth4，输入账号 test1，密码 pass123456。
3. 线路名称为“线路 2”（线路 2 带宽 200M），线路类型选择静态 PPPoE，网卡选择 eth4，输入账号 test2，密码 pass123456。

——结束

4.10.6.2. 配置 WAN 线路群组

通过此操作，创建 WAN 线路群组，并把线路添加至群组内。

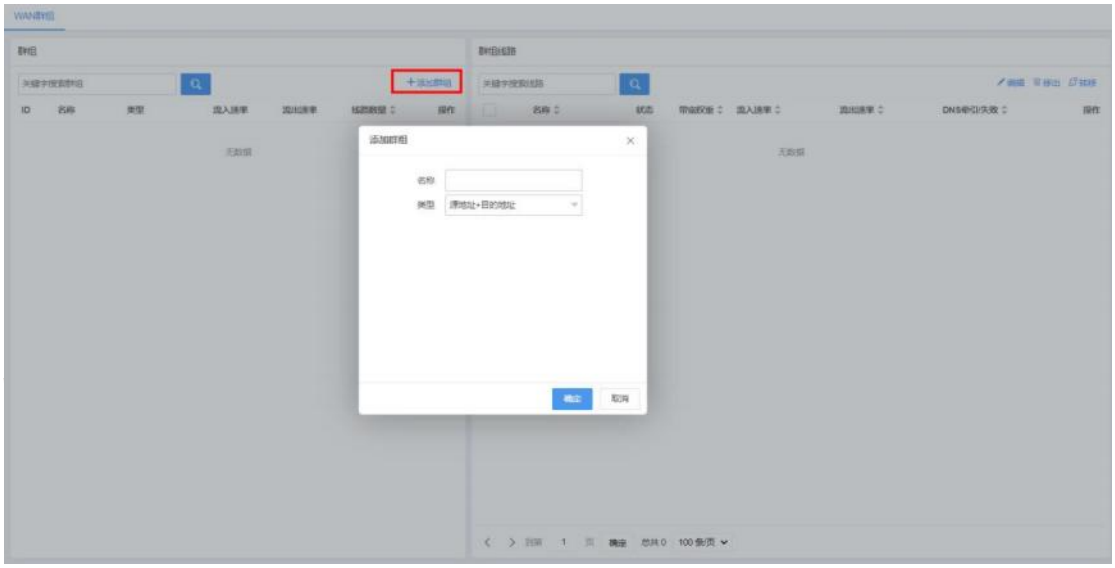
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【WAN 群组】。

步骤 4 单击【添加】，弹出添加群组页面。

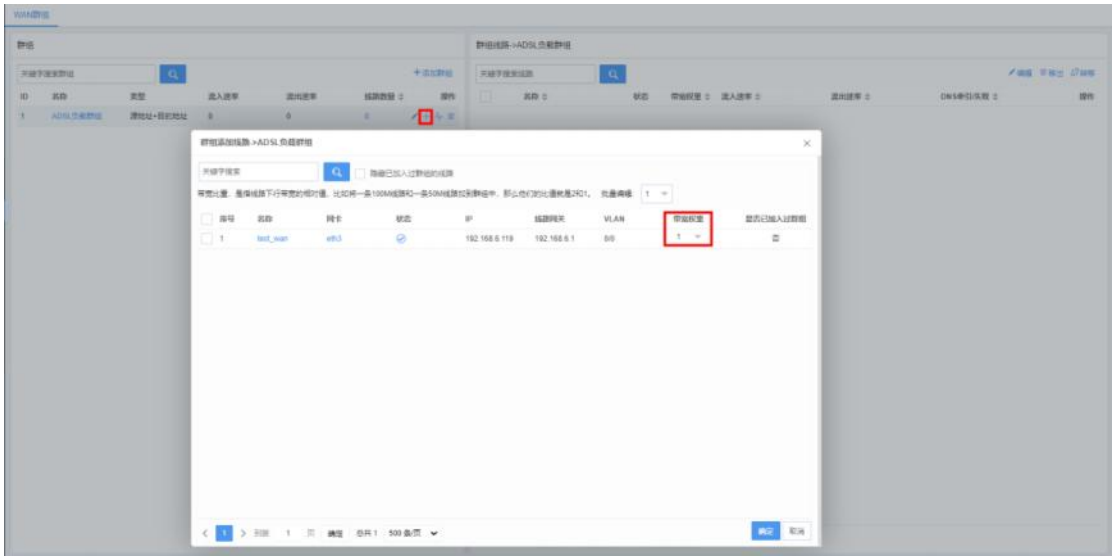


参数名称	参数说明
名称	自定义 WAN 群组名称。
类型	根据所选负载类型，决定负载均衡的算法。 源地址+目的地址：以会话的源地址和目的地址为条件进行计算。 源目地址+源目端口：以会话的源端口、目的地址、源端口、目的端为条件进行计算。 源地址：以会话的源地址为条件进行计算。 源地址+源端口：以会话的源地址和源端口为条件进行计算。 目的地址：以会话的目的地址为条件进行计算。 目的地址+目的端口：以会话的目的地址和目的端口为条件进行计算。 最大空闲带宽：在线路群组里，线路的权重可以设置为线路的最大下行带宽值（以 Mbps 为单位），这种负载方式会将连接（源目 IP+源目端口）优先分配给空闲带宽最大（最大下行带宽-当前下行带宽=空闲带宽）的线路，避免带宽的浪费。

步骤 5 设置群组名称及类型，单击【确定】。

配置示例：名称设置为“ADSL 负载群组”，负载类型选择“源地址+目的地址”。

步骤 6 单击当前群组操作列的 ＋，添加线路。



步骤 7 勾选已创建的线路，并设置带宽权重，单击【确定】

说明

带宽权重：是线路下行带宽的相对值，比如将一条 100M 线路和一条 50M 线路加到群组中，那么他们的比值就是 2 和 1。

配置示例：线路 1 的带宽:线路 2 的带宽=100M:200M=1:2，则线路 1 带宽权重设置为 1，线路 2 带宽权重设置为 2。

——结束

4.10.6.3. 配置自定义协议

通过此操作，可帮助用户创建当前特征库中没有的协议，主要用于内部应用的识别和分流操作。

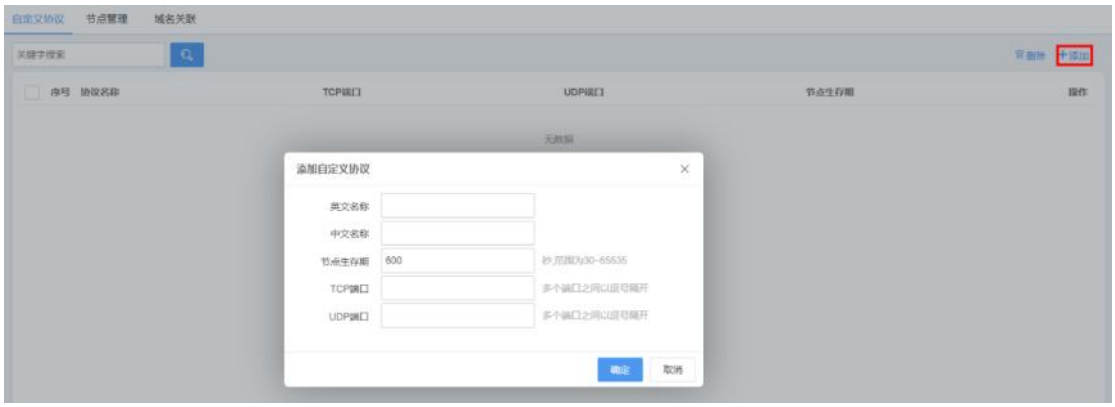
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【应用识别】>【自定义协议】>【自定义协议】。

步骤 4 单击【添加】，添加自定义协议。

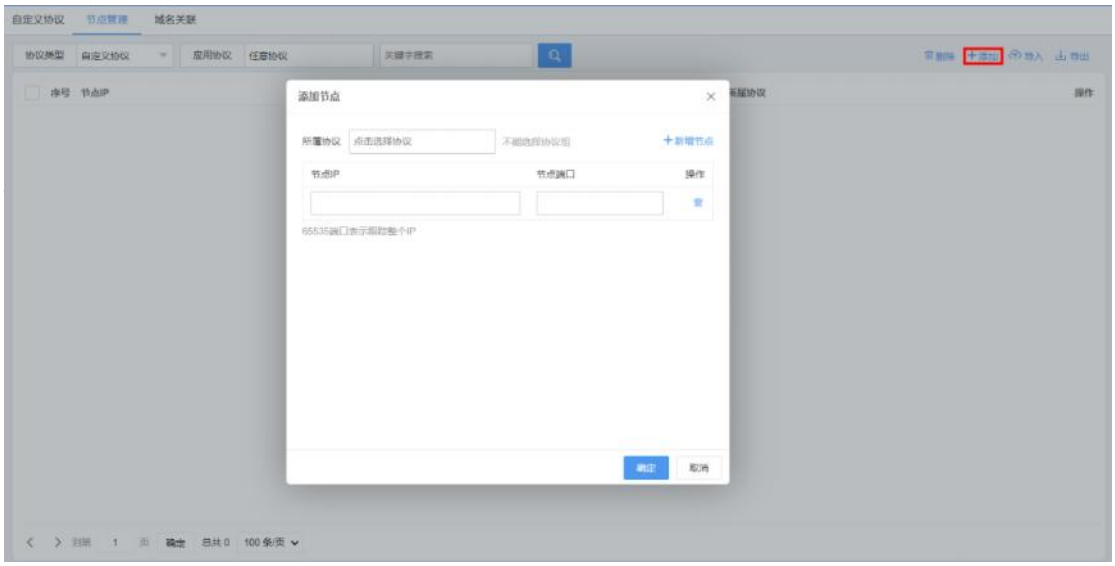


步骤 5 输入英文名称和中文名称，单击【确定】。

配置示例：中文名称设置为“OA”，中文名称设置为“OA 系统”。

步骤 6 选择【应用识别】>【自定义协议】>【节点管理】。

步骤 7 单击页面右上角【添加】，添加节点。

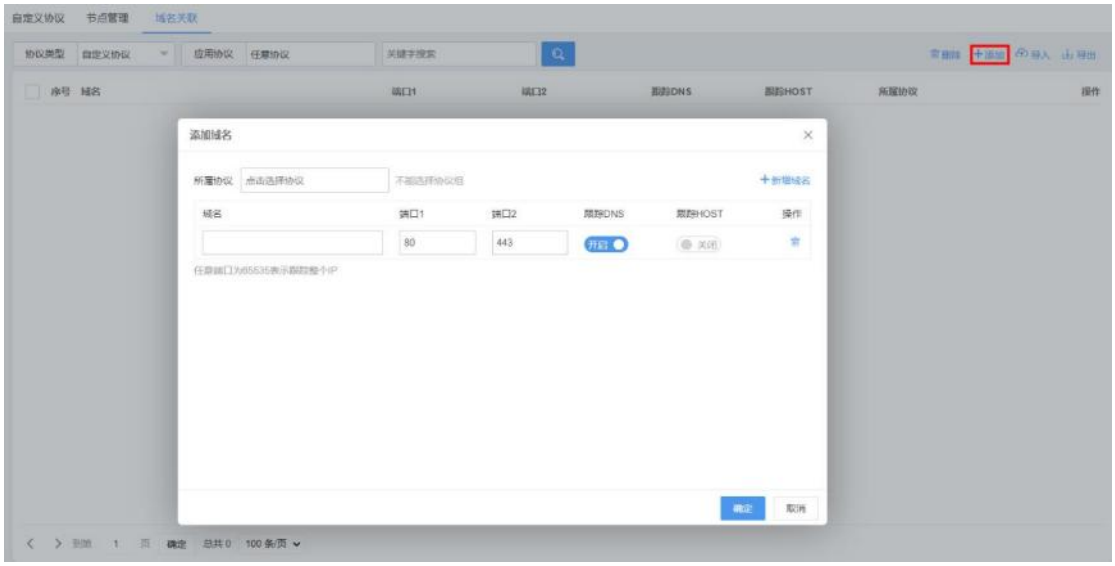


步骤 8 单击选择或搜索所属协议，输入节点 IP 及端口，单击【确定】。

配置示例：所属协议选择为“OA 系统”，节点 IP 设置为 11.1.11.1，节点端口设置为 8080。

步骤 9 选择【应用识别】>【自定义协议】>【域名关联】。

步骤 10 单击页面右上角【添加】，添加域名。



步骤 11 单击选择或搜索所属协议，输入域名、端口，开启“跟踪 HOST”，单击【确定】。

配置示例：所属协议选择为“OA 系统”，输入域名 www.OA.com，节点端口设置为 8080。

——结束

4.10.6.4. 配置自定义协议组

通过此操作，创建自定义协议组，可应用于策略路由、DNS 管控、流量管理和其他有应用协议选项的多个功能中。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

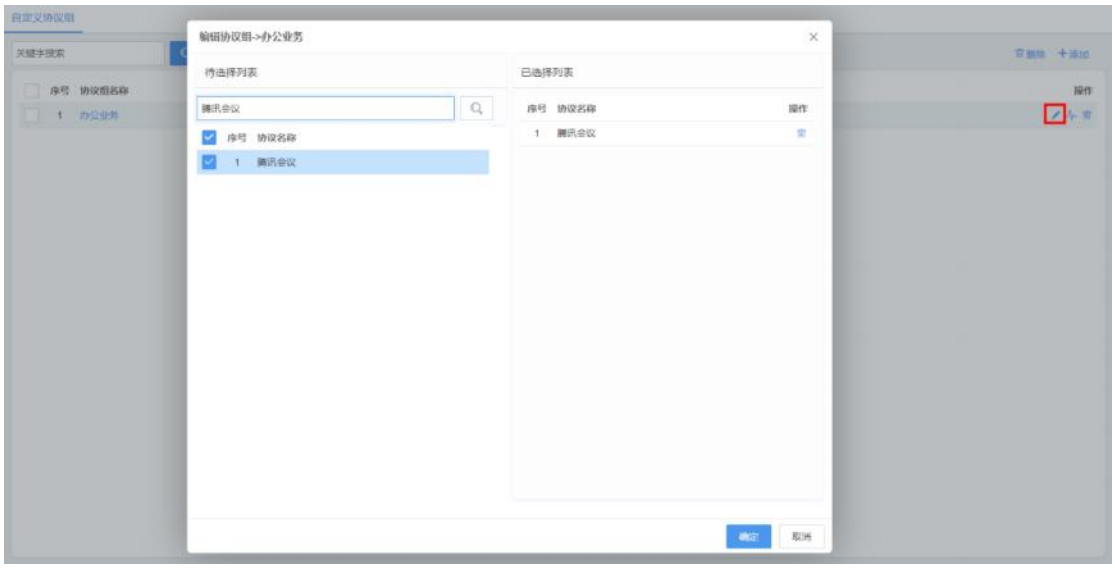
步骤 3 选择【应用识别】>【自定义协议组】。

步骤 4 单击【添加】，添加自定义协议组。

步骤 5 设置协议组的英文名称和中文名称，单击【确定】。

配置示例：设置协议组的英文名称为 office，中文名称为办公业务。

步骤 6 单击当前协议组操作列的 ，添加协议。



步骤 7 搜索并勾选需要添加的协议，单击【确定】。

配置示例：添加 OA 系统、腾讯会议等，到“办公业务”协议组。

——结束

4.10.6.5. 配置策略路由

通过此操作，添加策略路由，为不同协议及协议组设置负载策略。

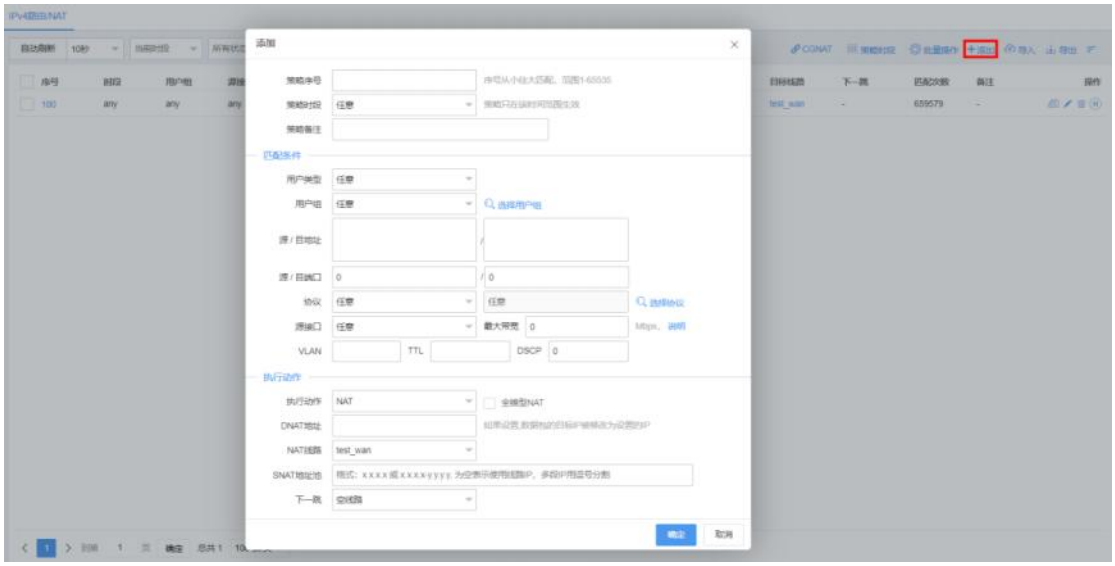
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【网络管理】>【IPv4 路由/NAT】。

步骤 4 单击【添加】，添加策略路由。



参数名称	参数说明
策略序号	策略的编号，系统将按照编号从小到大的方式依次执行策略表，该编号不可编辑，也不可上下移动。 取值：1~65535。编号越小，优先级越高。
策略时段	策略只在该时间范围生效。
策略备注	对该策略的补充说明。
用户类型	可设为代拨用户、非代拨用户，或者任意。
用户组	用户组织架构中的分组，详见【用户认证】
源/目的地址	源地址：匹配用户侧 IP 地址，该地址为 xxx.xxx.xxx.xxx/nn 或 n.n.n.n-m.m.m.m 或是 IP 群组、用户组、用户账号。 目的地址：对匹配访问目标服务的 IP 地址，该地址为 xxx.xxx.xxx.xxx/nn 或 n.n.n.n-m.m.m.m 或是 IP 群组。
源/目的端口	源端口：匹配用户侧的端口号。 目的端口：匹配访问目标服务的端口号。
协议	传输协议：对使用服务的传输层协议进行匹配，可选择 TCP、UDP、ICMP； 应用协议：对应用进行匹配，该 “应用协议”为 Panabit 自身携带的应用特征库，可以选择协议库的某一个应用或某一个分类。
源接口	选择某个内网物理接口或逻辑 LAN 接口进行匹配。
最大带宽	如果参数不为 0，表示当目标线路下行流量超过设定的最大带宽参数时该策略路由自动失效，会继续匹配下一条路由策略。
VLAN	匹配数据报文的 VLAN-Tag，0 表示对任意 VLAN 均有效。

TTL	匹配数据包的 TTL 值。
DSCP	匹配 DSCP 值。
执行动作	当数据报文与上述的策略条件相匹配后所执行的动作。匹配策略路由的会话，会做 NAT、DNAT、CGNAT、路由、走代拨其中一种动作。 NAT：指对匹配会话的数据包进行源地址转换，并从指定的线路进行数据转发。 ● 全锥型 NAT：从内网的｛IP:端口｝发送出来的请求，NAT 设备会为之分配一个固定的公网｛IP:端口｝，同时产生一个内网主机的内网｛IP:端口｝与公网｛IP:端口｝映射关系，任何一个外网主机都可以通过这个公网｛IP:端口｝，实现访问位于内网的主机设备功能。 **说明** Panabit 的全锥型 NAT 特性如下： 6. 目标端口为 1024 以下的会话，不会触发全锥型 NAT 动作，即便策略里指定了也不生效。 7. 针对一些知名目标端口，如 5353，1900，也会忽略。 8. 如果会话触发了全锥形 NAT 策略，Panabit 在做 SNAT 的同时，将外网 IP 和 NAT 端口动态映射到内网 IP 和内网端口上，这个映射在这条触发映射的会话周期内一直存在，可通过命令 **floweye dynpm config ttl=xxx** 调整映射老化时间。 9. 动态端口映射条目有限制，与设备型号有关系。使用 floweye dynpm stat 可以查看当前已经分配条目（count）和支持的最大条目（pool_size）； 10. 如果内存允许，可以在/etc/PG.conf 里通过设置 DYNPM_POOLSZ 变量来扩大最大可支持的动态端口映射条目。 ● NAT 线路：可以选择 WAN 线路、WAN 线路群组 、“空线路”，选择“空线路”表示数据从网桥转发 。 ● SNAT 地址池：x.x.x.x 或 x.x.x.x-y.y.y.y，为空则表示使用线路 IP，多段 IP 用逗号隔开。 ● 下一跳：指定数据转发的下一跳。下一跳为空，动作后的数据报文则向路由线路的网关地址转发。如果不为空，数据报文则向所选择线路的网关转发。 DNAT：源地址被转换为 WAN 线路的地址，并且目标地址被转换成 DNAT 地

	址选项框内的地址，DNAT 地址选项框如果不填目标地址则被转换成 WAN 线路网关地址。 ● DNAT 地址：如果设置，数据包的目标 IP 被修改为设置的 IP。 CGNAT：源地址和源端口按照 CGNAT 设置规则进行转换。 路由：对匹配会话的数据包不改变其源地址，并从指定的线路进行数据转发。 ● 路由线路：可以选择 WAN 线路，或者一个 LAN 接口。 ● 下一跳：指定数据转发的下一跳 。LAN 线路是没有网关的，所以要填写 LAN 对端的互联地址。 **说明** 1. CGNAT 主要应用于运营商级的网络地址转换。因为 CGNAT 在实现 NAT 的同时可以大大降低日志量，提升日志溯源的效率。 2. CGNAT 在将私网地址（源地址）转换为指定的公网地址后，源端口也要在一段固定且连续的端口范围内进行转换。 3. CGNAT 有静态和动态两种。静态 CGNAT，手动指定内网 IP 与公网 IP+端口范围的对应关系；动态 CGNAT，自动分配内网 IP 与公网 IP+端口范围的对应关系。 走代拨：匹配了代拨策略的用户进行源地址转换，并从相应的代拨线路做数据转发。

步骤 5 配置策略路由，单击【确定】。

说明

当有多条线路时，需要多次进行添加，策略序号越小，优先级越高。每条策略基于优先级的不同，构成了分流策略冗余功能。

配置示例：

1. 策略序号设为“600”、协议为“办公业务”、执行动作为“NAT”、NAT 线路为“运营商专线”，其余默认。
2. 策略序号设为“700”、执行动作为“NAT”、NAT 线路为“ADSL 负载群组”其余默认。
3. 策略序号设为“800”、执行动作为“NAT”、NAT 线路为“ADSL 负载群组”其余默认。

——结束

4.10.6.6. 检查配置是否生效

选择【网络管理】>【IPv4 路由/NAT】，查看匹配次数，有则代表策略生效。

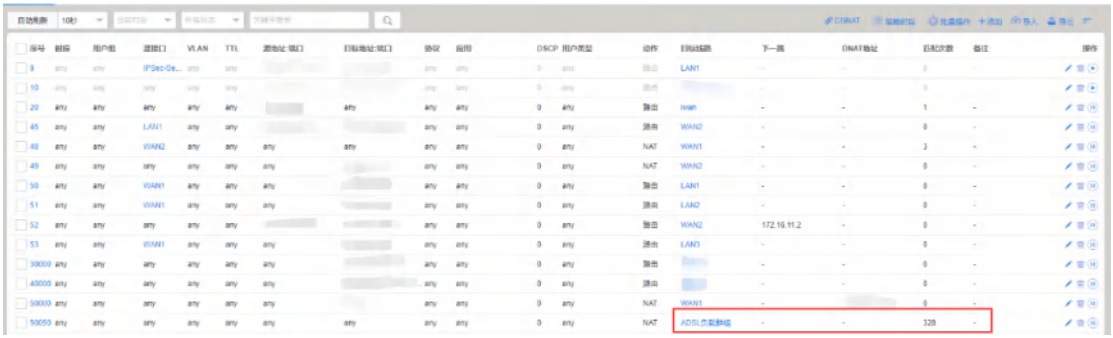


图 4-88 IPv4 路由/NAT 界面

选择【流量概况】>【在线用户】，单击想要查看的 IP，单击连接信息，查看分流的策略和线路。

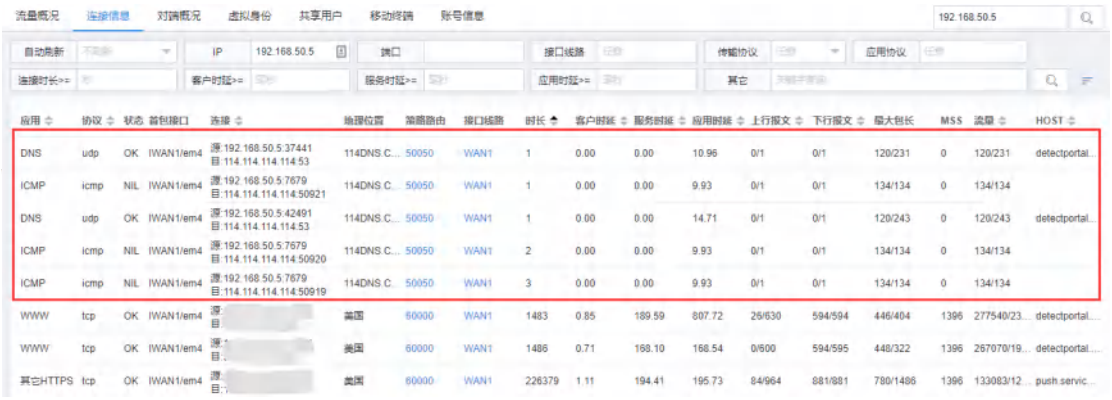


图 4-89 在线用户界面

4.10.7. 常见问题

1. 内网流量负载条件较多，上网行为管理有哪些负载方式？

支持基于五元组、应用协议、域名、VLAN、网络接口、用户类型等多种参数匹配实现流量科学负载，合理使用每一条接入链路。

2. 最高吞吐流量是多少？用户比较多，线路也多，而且杂。

根据不同的网络环境可以合理选择设备，最高支持 1G 吞吐与 30 万的并发连接数。支持全场景接入。支持 DHCP、静态地址、L2TP，最高支持多达 32 条的线路负载汇聚。

3. 线路群组上有很多负载方式可以选择，源地址+目的地址之类的，具体是怎么负载的呢？

如：【源地址+目的地址】以会话的源地址和目的地址为条件进行计算。当选定负载均衡方式后，设备会对接入设备的流量，根据设置的负载模式进行 HASH 计算，根据 HASH 值分配流量到出口的线路上进行转发。

4.11. 虚拟专网

4.11.1. 概述

虚拟专网并非真的专用网络，但却能够实现专用网络的功能。

虚拟专网又称 VPN（Virtual Private Network）专网，指的是依靠 ISP （Internet Service Provider 服务提供商）和其他 NSP（Network Service Provider 网络服务提供商），在公用网络中建立专用的数据通信网络的技术。

在虚拟专网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公网的物理链路资源动态组成。虚拟专网通过使用加密和隧道技术来创建一个安全的通信通道，使用户能够在不受外部干扰的情况下传输数据。

4.11.1.1. 虚拟专网的角色

虚拟专网通常由 VPN 客户端和 VPN 服务器组成。客户端通过连接到服务器来建立安全通信通道。VPN 技术有多种实现方式，选择合适的 VPN 协议取决于您的需求和安全要求。Panabit 上网行为管理支持的虚拟专网隧道协议，包含 L2TP、IPsec，以及派网的自研协议 iWAN 等。

4.11.1.2. 虚拟专网的线路

当虚拟专网的隧道建立成功后，隧道将作为一种逻辑上的出口链路，可以被其他业务进行调度，进而实现如：总部与分支之间业务互联、重要业务带宽保障，特定应用业务加速等能力。

虚拟专网的隧道都需要使用一条 WAN 线路来做承载线路，所以我们需要先建立一条 WAN 线路，然后再在 WAN 线路上建立隧道。这里需要注意的是，通常情况下，iWAN 和 IPsec 服务端需要具有固定的公网 IP，iWAN 客户端、L2TP、IPSEC 客户端则不需要固定公网 IP，只需

要互联网线路即可。

WAN 线路的创建，具体请参见 WAN 线路。进入界面后通过【网络管理】->【LAN/WAN】->【WAN 线路】点击添加按钮进行承载线路添加，承载线路类型支持，PPPoE、静态 IPV4、动态 DHCP 等。

4.11.2. 应用场景

虚拟专网可以在各种不同的情景中发挥作用，提供安全、隐私和灵活性。以下是一些常见的应用场景：

1. 远程办公：随着越来越多的员工需要在远程工作，虚拟专网可以提供安全远程访问公司内部网络的方式，防止未经授权的访问。
2. 分支机构互联：大型组织通常有多个分支机构，虚拟专网可以用于连接这些分支机构，实现安全的数据共享和通信。
3. 远程支持和维护：IT 团队可以使用虚拟专网连接到远程服务器和设备，以进行支持、维护和故障排除。

4.11.3. iWAN

4.11.3.1. iWAN 简介

在云计算、移动应用和企业全球化成为大背景的环境下，越来越多的实时应用（如异地办公、视频会议、远程桌面、支付交易系统和远程医疗）需要在多个节点之间进行高效传输。当前，常见的专线隧道技术，如 IPsec VPN、SSL VPN、L2TP VPN 和 MPLS VPN，虽然已经非常成熟，但随着带宽需求的不断增长，用户的期望也在不断演进，传统隧道技术开始显露出一些问题。

在市场需求不断变化的背景下，传统的隧道技术面临以下主要问题：

1. 服务开放性不足，缺乏灵活性。
2. 专线的运维成本相对较高。
3. 关键业务的可靠性较差，难以实现业务差异化。

随着常见问题如断线和访问缓慢的出现，用户不满程度增加，甚至造成业务的损失。因此，需要引入一种更优质的隧道技术，以解决互联网不稳定，专线成本又昂贵的问题，同时满

足即时性和实时性应用的要求。

在此背景下，Panabit 的 iWAN 应运而生，它被设计为一种新型隧道技术，专为提高性能而生，同时解决了传统 VPN 隧道技术无法解决的稳定性和快速重连等问题。

4.11.3.1.1. iWAN 的作用

1. 在多台 Panabit 设备间进行 VPN 组网。
2. 为用户提供快速稳定的隧道，以部署海外加速和内网互联等服务。

4.11.3.1.2. iWAN 的优势

1. 重连速度快：IPsec 要重连，需要有几十次交互，而 iWAN 只需要一次即可。
2. 客户端不受底层承载线路 IP 变化影响：当底层承载线路（比如 PPPoE 拨号线路）的 IP 地址发生变化时，iWAN 隧道不会中断，能保证通信正常进行。现有的会话可以照常使用，不需要做任何改变。
3. 传输效率高：iWAN 的包头很小，只有 8 个字节，所以能大幅度提升传输效率。
4. 抗干扰：使用 L2TP 时，中间人可以直接发包 TERMINATE。但是 iWAN 控制命令有完整性检查，可以避免中间人攻击。
5. 全局监控：云平台监控，集中资源下发，集中大数据分析。

4.11.3.2. 应用案例：异地分支互联

企业内部研发部门和管理部门需要频繁地使用隧道服务访问分部/总部内网资源，之前使用的专网线路费用比较昂贵，管理部门大文件传输速率不理想，现使用 iWAN 方案解决。总部 Panabit 作为 iWAN 服务端（LAN：172.16.0.1/24 网段），分部 Panabit 作为 iWAN 客户端（LAN：192.168.0.1/24 网段）。两个不同的内网环境，通过 iWAN 服务提供一个高效的传输通道，实现两边内网互通与资源共享。

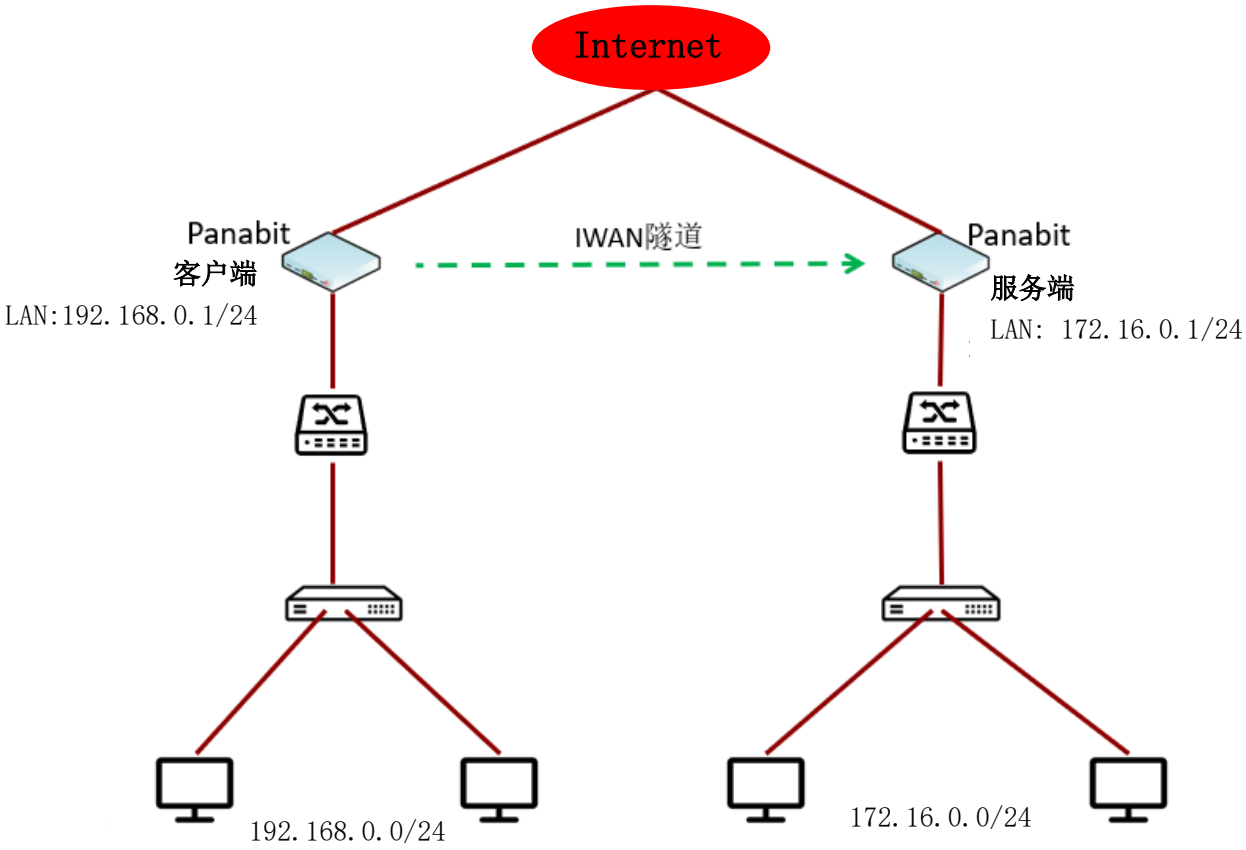

Internet
Panabit
客户端
LAN:192.168.0.1/24
IWAN隧道
Panabit
服务端
LAN: 172.16.0.1/24
192.168.0.0/24
172.16.0.0/24

图 4-90 iWAN 拓扑

4.11.3.2.1. 配置流程

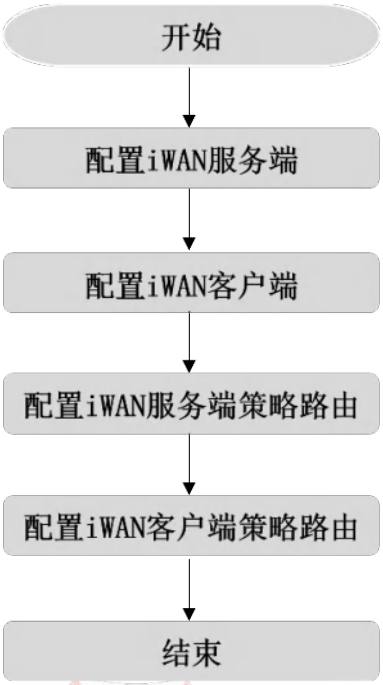


图 4-91 iWAN 配置流程

4.11.3.2.2. 配置前提

1. 客户端与服务端的 Panabit 均以网关模式进行部署。
2. 无论是客户端还是服务端，都需要有一条能够正常用于与服务端/客户端通信的 WAN 线路。
3. 服务端的网络中，需要有一个固定的公网 IP 地址（或域名）。

4.11.3.2.3. 配置 iWAN 服务端

- iWAN 服务端需要设置一个地址池，用于给 iWAN 客户端分配账号、IP 地址、DNS，限制 iWAN 客户端带宽等。
- iWAN 服务目前有本地认证、Radius 认证和免认证三种方式，在此案例中，采用本地认证。
- iWAN 服务端创建的服务，需要将其映射到公网，以便客户端进行连接。

4.11.3.2.3.1. 配置 WAN 线路

创建 WAN 线路时，建议选择静态 IPv4，具体操作请参见配置 WAN 线路。

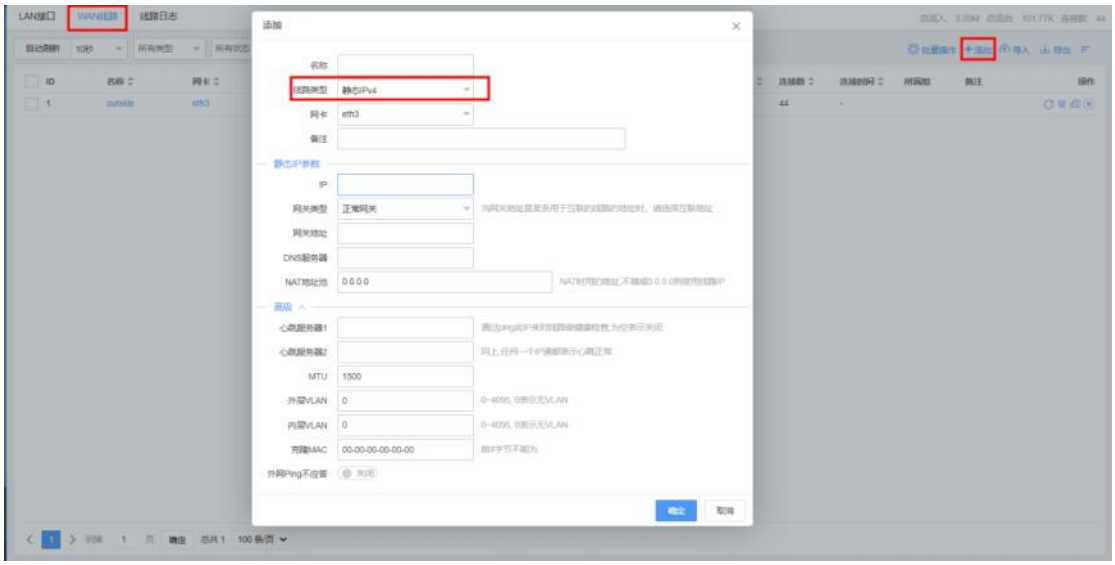


图 4-92 WAN 线路详情

4.11.3.2.3.2. 创建地址池

这里应使用一个不会产生冲突的私网地址，并分配 DNS，如 114.114.114.114。具体操作请参见组织架构。

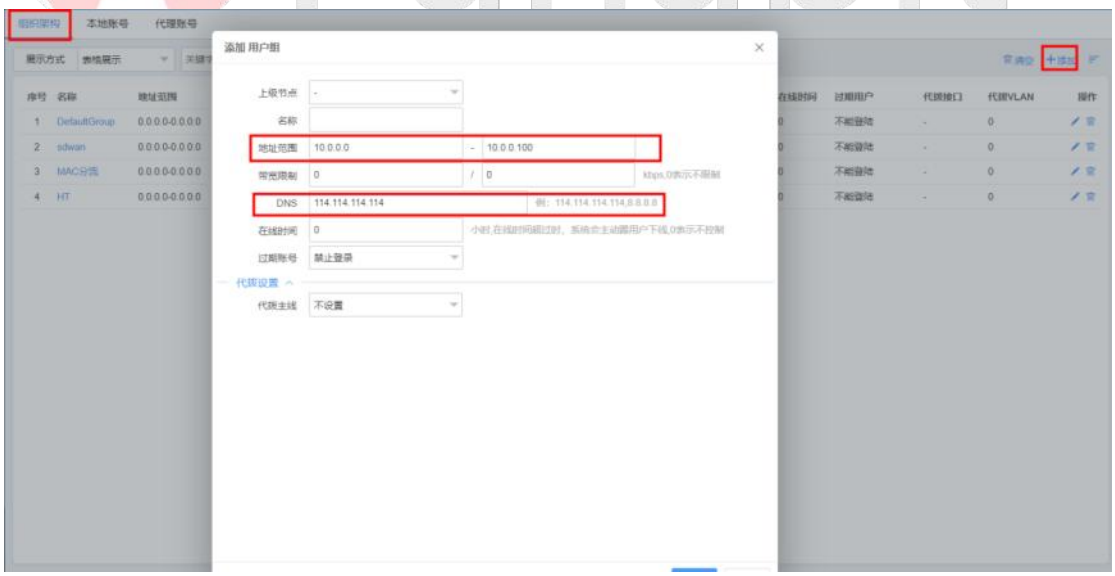


图 4-93 组织架构详情

为能够正常使用认证功能，在已创建的地址池中添加账号，并为此账号绑定一个 IP，具体操作请参见本地账号。

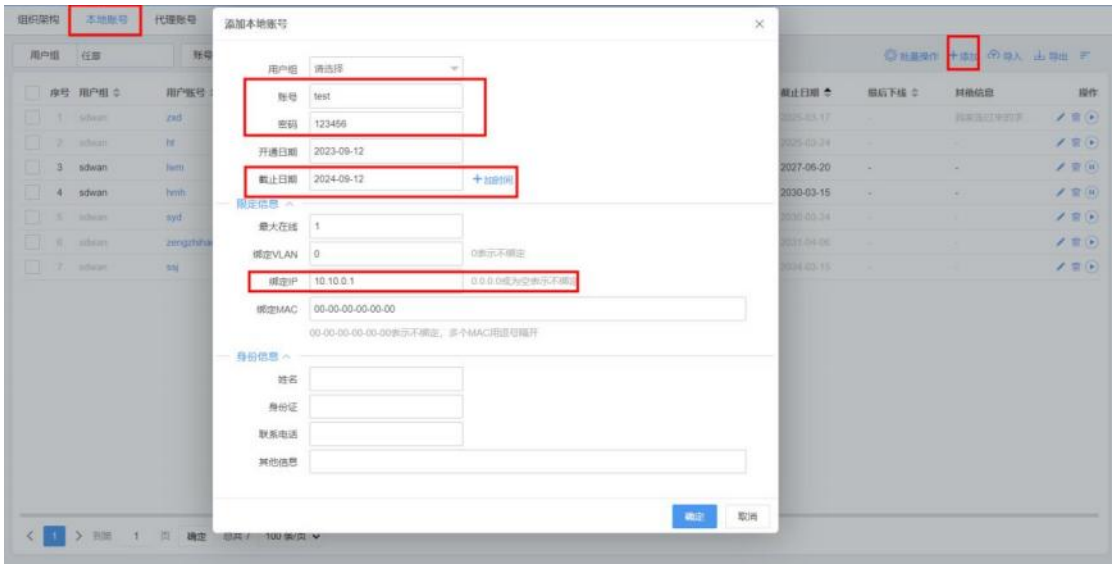


图 4-94 本地账号详情

配置示例：用户组选择上一步中创建的地址池名，账号填写“test”，密码填写“123456”，截止日期选择“加一年”，绑定 IP 填写“10.0.0.1”。

说明

这里的账号，即为 iWAN 客户端连接服务端时的认证凭据。

绑定 IP 地址，当 iWAN 客户端重拨后，服务端为其分配的 IP 地址也不会变。

案例中之所以要绑定 IP 地址，是为了在配置服务端访问客户端的路由时，下一跳为固定的 IP。

4.11.3.2.3.3. 创建 iWAN 服务

通过此操作，创建 iWAN 服务，用于与 iWAN 客户端形成连接。

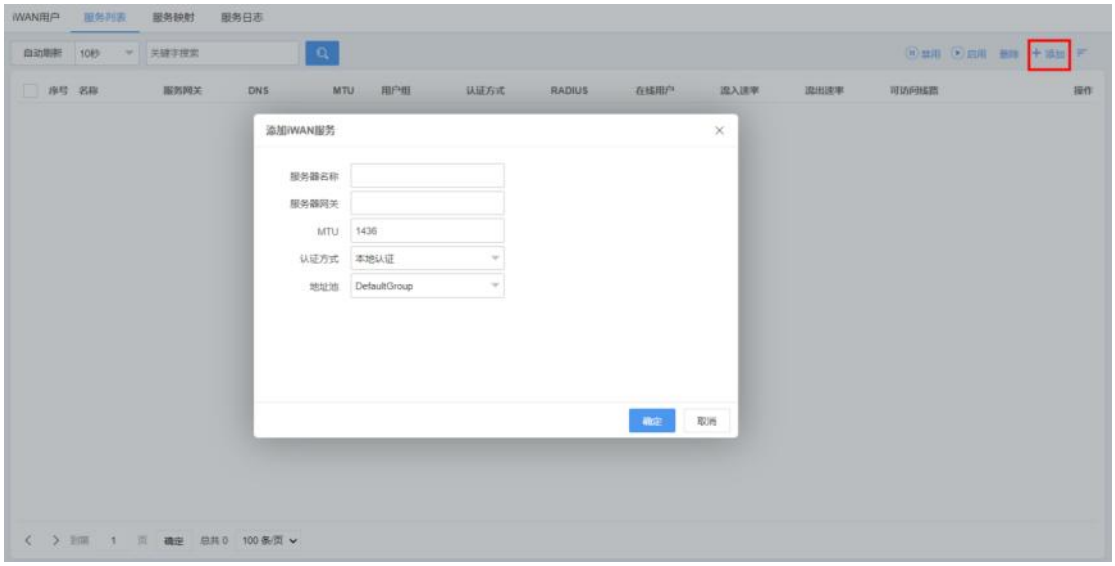
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【虚拟专网】>【iWAN 服务】>【服务列表】。

步骤 4 单击页面右上角【添加】，创建 iWAN 服务。



参数名称	参数说明
服务器名称	自定义服务器名称。
服务器网关	自定义 iWAN 服务的网关，建议使用一个不会产生冲突的私网地址。
MTU	定义数据的最大传输单元。
认证方式	目前有“本地认证”、“Radius 认证”和“免认证”三种方式。
地址池	选择用于分配地址的地址池。

配置示例：设置服务器名称为“iWAN 服务端”，设置服务器网关为“10.0.0.100”，MTU 默认，认证方式选择“本地认证”，地址池选择创建地址池步骤中创建的地址池。

步骤 5 单击【确定】。

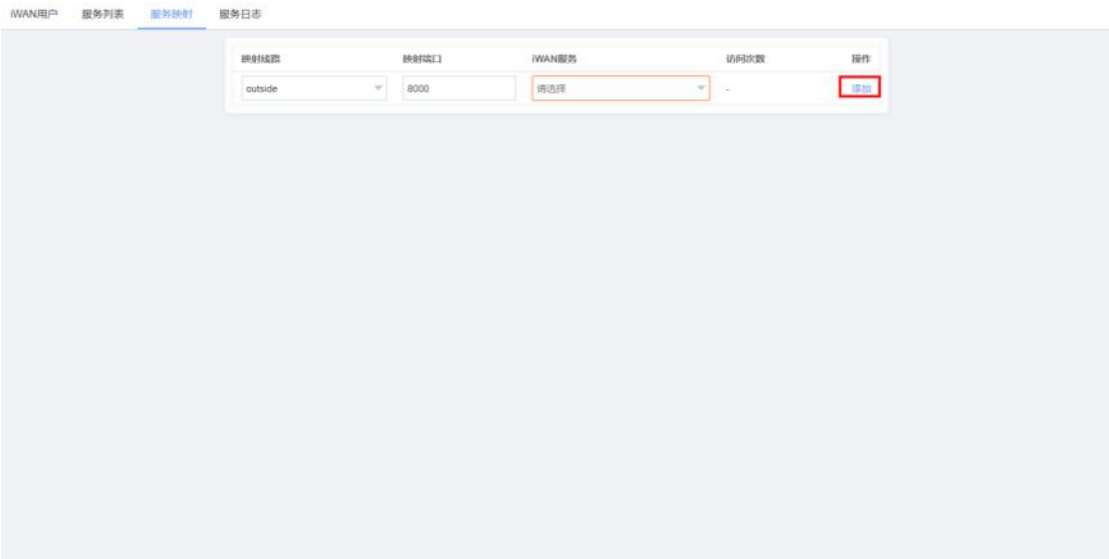
——结束

4.11.3.2.3.4. 映射 iWAN 服务

操作步骤

步骤 1 选择【虚拟专网】>【iWAN 服务】>【服务映射】。

步骤 2 选择 iWAN 服务，及其绑定的线路和端口，单击操作列的【添加】。



参数名称	参数说明
映射线路	选择一条 iWAN 服务的映射线路。
映射端口	设置 iWAN 服务的映射端口，可自定义，默认为 8000（UDP）。
iWAN 服务	选择已创建好的 iWAN 服务。

配置示例：映射线路选择配置 WAN 线路步骤中创建的 WAN 线路，映射端口默认，iWAN 服务选择上一步骤中创建的 iWAN 服务“iWAN 服务端”。

说明

如果服务端侧的固定公网 IP 地址不在 Panabit 的 WAN 线路上，则还需要在出口设备上进行配置，将[iWAN 服务映射线路地址]+[iWAN 服务映射端口]映射到公网固定 IP 上。

——结束

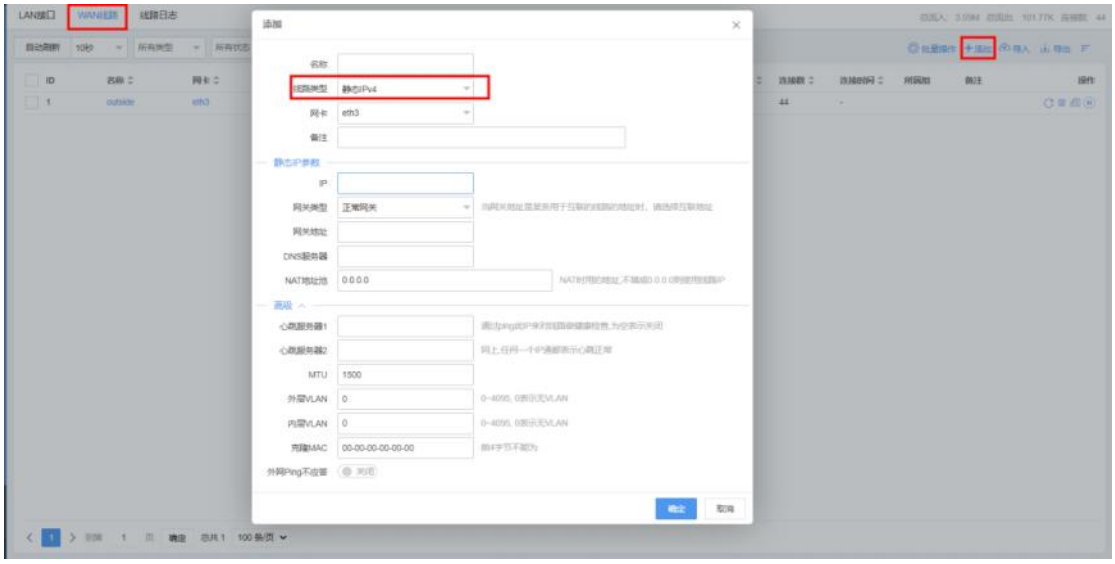
4.11.3.2.4. 配置 iWAN 客户端

创建 iWAN 客户端，连接 iWAN 服务，打通隧道。

- iWAN 客户端在 Panabit 上表现为一条 WAN 线路，这条线路的类型就是 iWAN。
- iWAN 线路需要承载在一条 WAN 线路之上，因此需要事先创建好一条 WAN 线路。

4.11.3.2.4.1. 配置 WAN 线路

创建 WAN 线路时，线路类型可选择静态 IPv4/DHCP IPv4/PPPoE，并确保该 WAN 线路能够连通 iWAN 服务端映射到公网的地址+端口。具体操作请参见配置 WAN 线路。



4.11.3.2.4.2. 配置 iWAN 线路

需要选择一条 WAN 线路来承载 iWAN 线路，实现客户端与服务端互通。

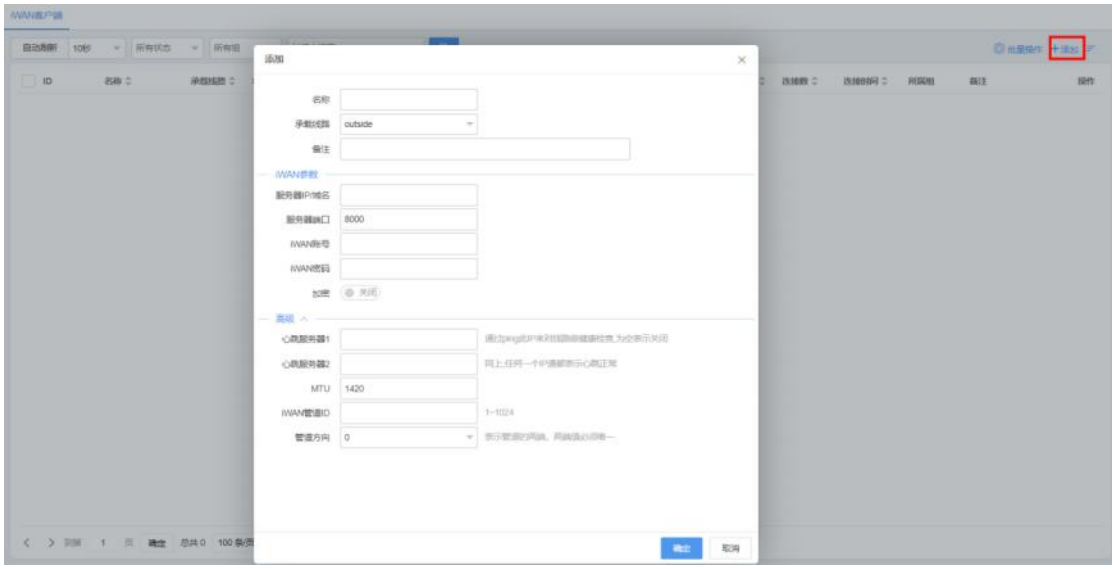
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【虚拟专网】>【iWAN 客户端】。

步骤 4 单击页面右上角【添加】，弹出添加 iWAN 客户端。



参数名称	参数说明
名称	自定义 iWAN 客户端名称。
承载线路	选择 iWAN 客户端所要使用的 WAN 线路。

备注	可为 iWAN 客户端添加备注。
服务器 IP/域名	iWAN 服务端的 IP 地址或域名。
服务器端口	iWAN 服务端开放的端口。
iWAN 账号/密码	输入 iWAN 账号/密码。
加密	可选择“开启”或“关闭”。
心跳服务器 1	通过 ping 此 IP 来对线路做健康检查，为空表示关闭。
心跳服务器 2	通过 ping 此 IP 来对线路做健康检查，为空表示关闭。与心跳服务器 1 任何一个 IP 通都表示心跳正常。
MTU	定义数据的最大传输单元。
iWAN 管道 ID	取值 1~1024。
管道方向	表示管道的两端，两端值必须唯一。

配置示例：

1. 设置名称为“iWAN 客户端”，承载线路选择上一步骤中的 WAN 线路。
2. 服务器 IP/域名、服务器端口填写映射 iWAN 服务步骤中映射的公网 IP+端口。
3. iWAN 账号/密码填写创建地址池步骤中创建的账号信息。
4. 其余默认即可。

客户端成功添加后效果如下：

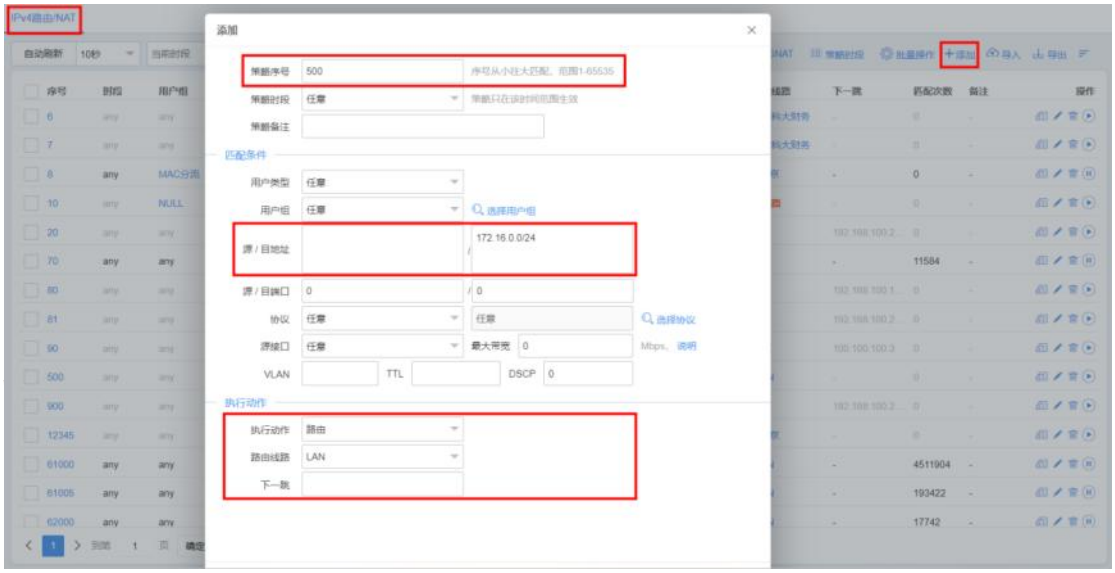
服务端 Panabit，【虚拟专网】-【iWAN 服务】-【iWAN 用户】中也可以查看连接情况。

4.11.3.2.5. 配置 iWAN 服务端策略路由

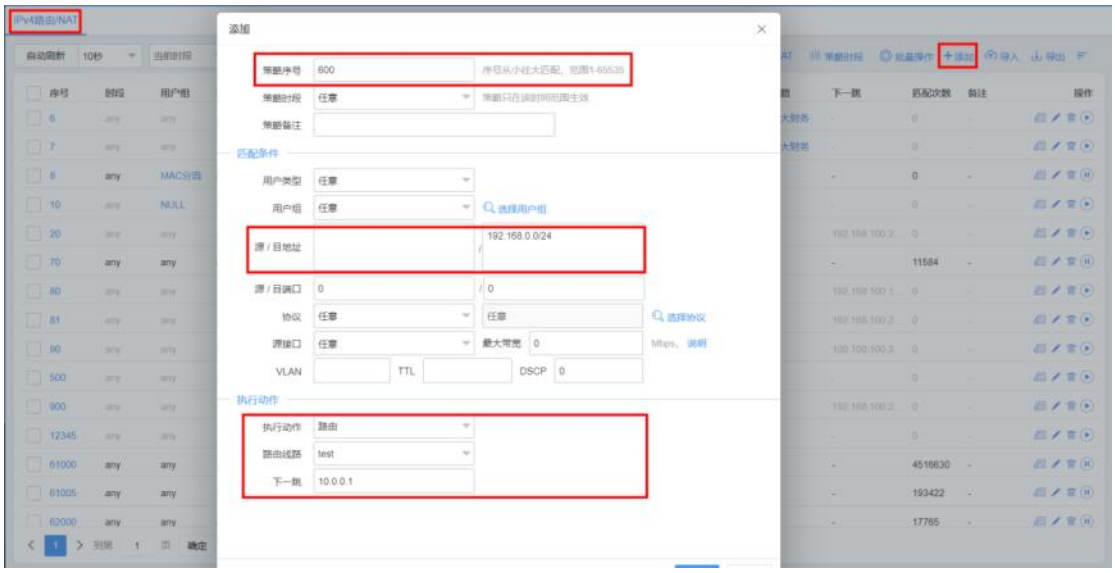
添加策略路由具体操作请参见配置策略路由，此处需要创建两条策略路由，以保证服务端与客户端能互相访问。

配置示例：

策略路由 1（到内网的路由）：目标地址设置为总部的内网地址段即“172.16.0.0/24”，执行动作设置为“路由”，路由线路为服务端 Panabit 的 LAN 接口，由于内网与 LAN 口在同一网段，下一跳可不填。



策略路由 2（到 iWAN 客户端的路由）：目标地址设置为分部 Panabit 的内网地址段，即“192.168.0.0/24”，执行动作设置为“路由”，路由线路为创建 iWAN 服务步骤中创建的 iWAN 服务，下一跳地址为创建地址池步骤中，创建账号时为其绑定的 IP 地址。



须知

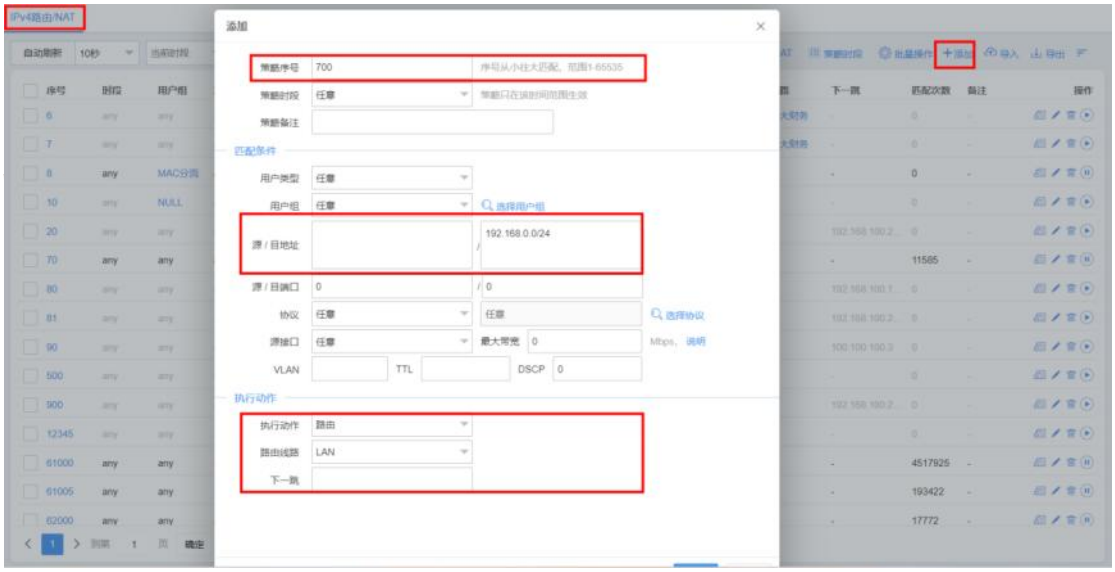
由于策略路由序号从小到大的匹配顺序，上面创建的两条策略路由，其策略序号需要小于服务端侧自身出网的默认路由，例如：匹配条件为任意，执行动作为 NAT 至出网 WAN 线路。

4.11.3.2.6. 配置 iWAN 客户端策略路由

添加策略路由具体操作请参见配置策略路由，此处需要创建两条策略路由，以保证服务端与客户端能互相访问。

配置示例：

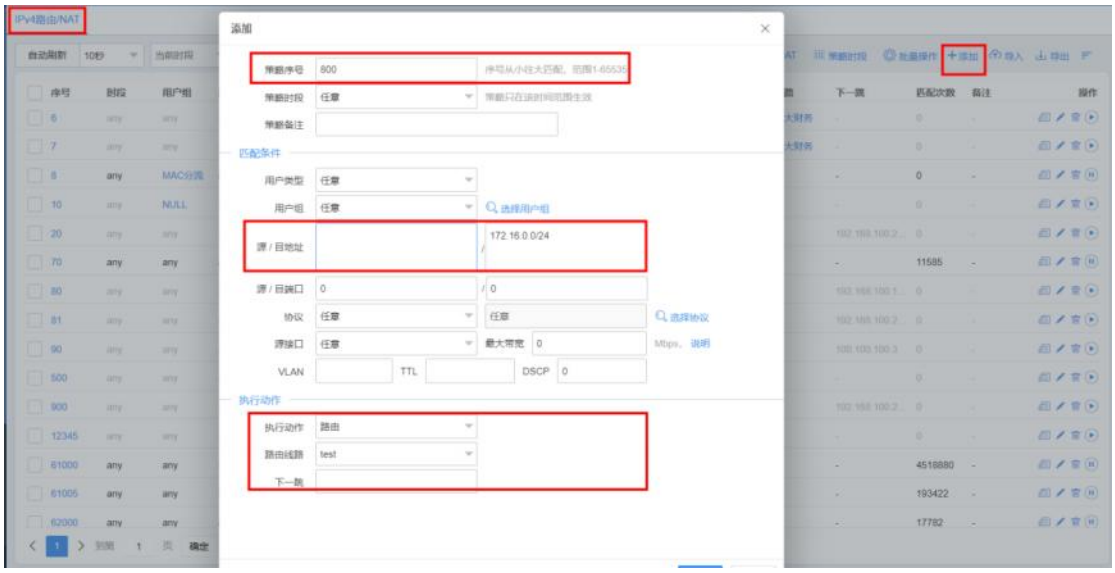
策略路由 1（到内网的路由）：目标地址设置为分部 Panabit 的 LAN 线路地址段即“192.168.0.0/24”，执行动作设置为“路由”，路由线路为分部 Panabit 的 LAN 线路。



策略路由 2（到 iWAN 服务端的路由）：目标地址设置为总部的内网地址段即“172.16.0.0/24”，执行动作设置为“路由”，路由线路为 iWAN 客户端上创建的 iWAN 线路。

说明

由于在创建 iWAN 服务步骤中，已经设置了服务网关，因此到 iWAN 服务端的路由无须设置下一跳。



须知

与服务端的路由类似，由于策略路由序号从小到大的匹配顺序，上面创建的两条策略路由，其策略序号需要小于客户端侧自身出网的默认路由，例如：匹配条件为任意，执行动作为 NAT 至出网 WAN 线路。

以上步骤完成后，即可通过总部与分部间的 iWAN 隧道完成私网互联。

4.11.4. IPsec

4.11.4.1. IPsec 简介

IPsec（ IP Security）是 IETF 制定的一系列协议，为 Internet 上传输的数据提供了高质量的、可互操作的、基于密码学的安全保护。特定的通信方通过在 IP 层加密与数据源认证等操作，来保证数据包在网络上传输的机密性、完整性、真实性和防重放。

IPsec 协议由 AH（Authentication Header 认证头）协议、ESP（Encapsulating Security Payload 封装安全载荷）协议、IKE（Internet Key Exchange 因特网密钥交换）协议、认证与加密算法等组成。其中，AH 协议与 ESP 协议用于提供安全服务，IKE 协议用于密钥交换。

IPsec VPN 模块实现了 IKEv1、IKEv2、ESP 等协议，其中 IKEv1 协议支持主模式（Main Mode）与野蛮模式（Aggressive Mode）。

IPsec VPN 一般用于局域网互连，如企业总部与分支机构之间的办公网互连。当 IPsec 隧道建立后，两地办公网内的计算机可以相互访问，安全地共享内网资源等。

Panabit 上网行为管理 IPsec 模块支持作为发起方（客户端）和应答方（服务端），并仅支持使用共享密钥（Pre-Shared Key）作为认证方式。在上网行为管理中，IPsec VPN 模块将作为“WAN 线路”，并结合“策略路由”，为符合 IPsec 安全策略的数据包提供加解密服务。

4.11.4.2. 应用案例

现有两台 Panabit 上网行为管理设备，设备 1 为服务端，设备 2 为客户端，现需要实现两端设备下的局域网地址互通。

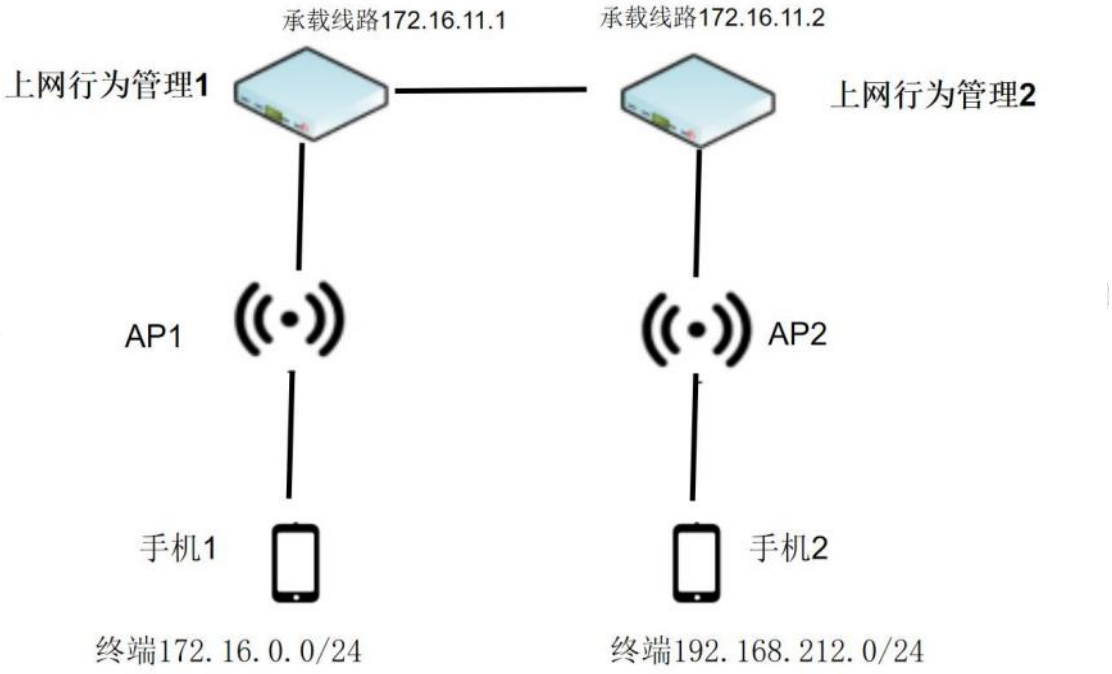


图 4-95 IPsec 拓扑

4.11.4.2.1. 配置流程

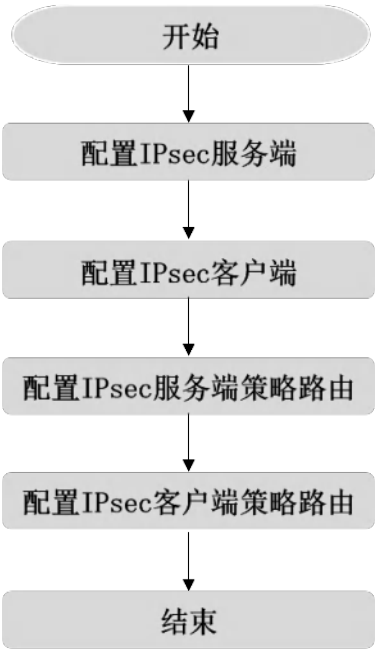


图 4-96 IPsec 配置流程

4.11.4.2.2. 配置前提

1. 客户端与服务端的 Panabit 均以网关模式进行部署。
2. 无论是客户端还是服务端，都需要有一条能够正常用于与服务端/客户端通信的 WAN 线路。

4.11.4.2.3. 配置 IPsec 服务端

4.11.4.2.3.1. 配置 WAN 线路

创建 WAN 线路，选择静态 IPv4，设置地址为 172.16.11.1，网关地址为 172.16.11.2。具体操作请参见配置 WAN 线路。

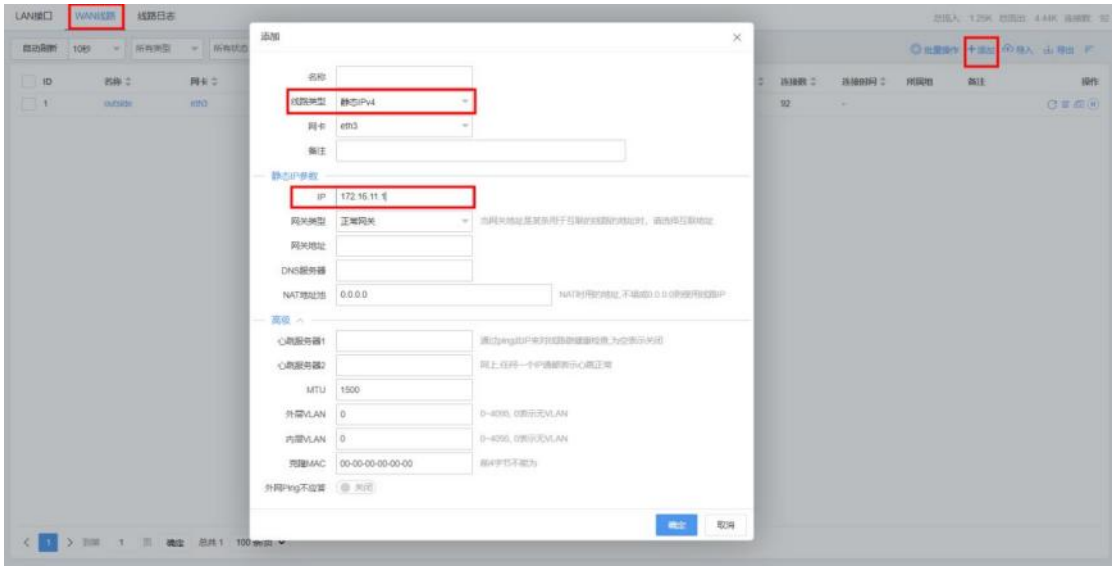


图 4-97 WAN 线路详情

4.11.4.2.3.2. 配置 IPsec 线路

需要在服务端选择一条 WAN 线路来承载 IPsec 线路，实现客户端与服务端互通。这里选择上一步骤中创建的 WAN 线路。

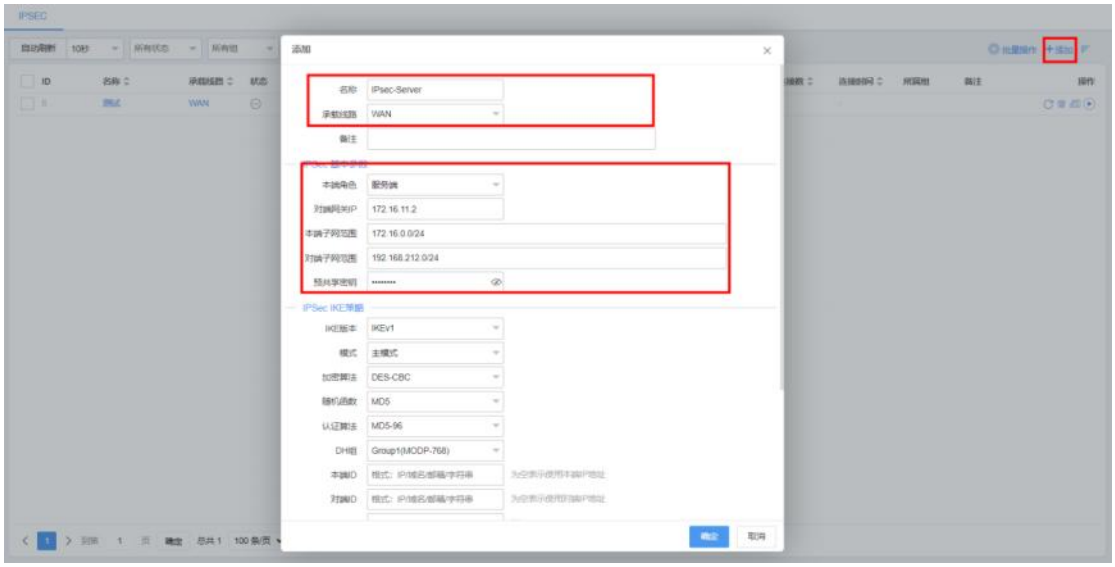
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【虚拟专网】>【IPsec】。

步骤 4 单击页面右上角【添加】，弹出添加 IPsec 线路页面。



参数名称	参数说明

名称	自定义线路名称。
承载线路	选择 IPsec 所要使用的 WAN 线路。
备注	可为线路添加备注。
IPsec 参数	本端角色：指定当前设备在 IPsec 连接中的角色，可选择“客户端”或“服务端”。此处请选择“服务端”。 对端网关 IP：对端网关是与本设备建立 IPsec 连接的另一个设备的 IP 地址。用于确定要与之建立连接的远程设备。 本端子网范围：格式为 x.x.x.x/24 或 x.x.x.x/255.255.255.0 或 x.x.x.x-y.y.y.y，多段用逗号分隔。 对端子网范围：格式为 x.x.x.x/24 或 x.x.x.x/255.255.255.0 或 x.x.x.x-y.y.y.y，多段用逗号分隔。 **说明** 本端子网范围与对端子网范围作为 IKE 协商时进行身份认证的标识，其格式支持字符串（如 panabit）、IP 地址（如 1.2.3.4）、FQDN（如 panabit.com）、User FQDN（如 IPsec@panabit.com）等。 预共享密钥：在建立 IPsec 连接之前双方共享的密钥。这个密钥用于进行认证和加密操作，确保通信的机密性和完整性。这个密钥必须在本地和对端设备之间保持保密。
IPsec IKE 策略	IKEv1/IKEv2 模式：可选择“主模式”、“野蛮模式”。 **说明** 当使用 IKEv1 协议时，若本端与对端之间存在 NAT 设备，则推荐使 用“野蛮模式”。当使用“主模式”且需要设置“本端 ID”或“对端 ID”时，“本端 ID”或“对端 ID”应设置为本端或对端的 IP 地址。 加密算法：加密算法确定用于保护数据机密性的加密方法，如 AES、3DES 等。 随机函数：在密钥协商过程中使用的随机数生成函数，用于生成加密和认证所需的随机值。 认证算法：认证算法用于验证数据的完整性和真实性。常见的算法包括 HMAC（Hash-based Message Authentication Code）等。 DH 组：DH（Diffie-Hellman）组定义了在密钥交换中使用的素数和

	基本参数。不同的 DH 组提供不同的安全级别。 本端 ID：本端标识是用于标识本地设备的信息，通常是 IP 地址或域名。 对端 ID：对端标识是用于标识远程设备的信息，通常是 IP 地址或域名。 生存时间：生存时间定义了 IPsec 安全关联的持续时间，可以是时间间隔或数据传输量。一旦超过生存时间，IPsec 连接将重新协商或终止。 DPD 检测频率：DPD（Dead Peer Detection）用于检测对端设备是否仍然在线。这个参数定义了发送 DPD 检测消息的频率。当连续 5 次心跳检测失败时，表示到“对端网关 IP”的连接已经丢失，会重新发起 IKE 协商。
IPsec ESP 策略	加密算法：加密算法用于将传输的数据进行加密，以确保数据在传输过程中不会被未经授权的人访问。常见的加密算法包括 AES（Advanced Encryption Standard）、3DES（Triple Data Encryption Algorithm）等。选择强大的加密算法有助于保护数据免受窃听和解密攻击。 认证算法：认证算法用于验证传输的数据的完整性和真实性，以防止数据被篡改。认证算法通常使用 HMAC（Hash-based Message Authentication Code）等方法来生成数据的摘要，并将其与预期摘要进行比较。这样可以检测出数据是否被篡改过。 生存时间：生存时间定义了 ESP 安全关联的持续时间。它可以根据时间间隔或数据传输量来定义。一旦 ESP 安全关联的生存时间到期，设备将重新协商安全参数或终止连接。这有助于确保安全参数的更新，以及防止不断保持相同参数而可能导致的安全风险。
MTU	定义数据的最大传输单元。

配置示例：

1. 名称设置为“IPsec-Server”，承载线路选择配置 WAN 线路步骤中创建的 WAN 线路。
2. IPsec 基本参数：本端角色选择“服务端”，对端网关 IP 为“172.16.11.2”，本端子网范围：“172.16.0.0/24”，对端子网范围：“192.168.212.0/24”，预共享密钥填写“ASCD1234”。
3. IKE 策略：如无特殊需求，默认即可。

4. ESP 策略：如无特殊需求，默认即可。

说明

在配置时，需注意两端的预共享密钥、IKE 策略（本端 ID 与对端 ID 除外）与 ESP 策略中的参数均保持一致，否则可能导致协商失败。

步骤 5 单击【确定】。

——结束

4.11.4.2.4. 配置 IPsec 客户端

4.11.4.2.4.1. 配置 WAN 线路

创建 WAN 线路，选择静态 IPv4，设置地址为 172.16.11.2，网关地址为 172.16.11.1。具体操作请参见配置 WAN 线路。

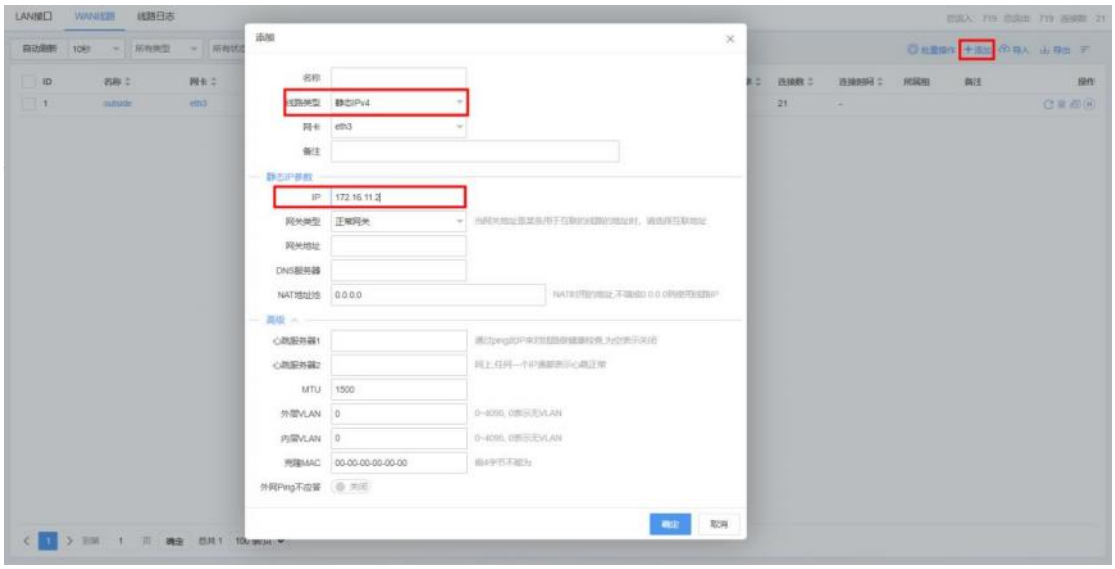


图 4-98 WAN 线路详情

4.11.4.2.4.2. 配置 IPsec 线路

客户端需要选择一条 WAN 线路来承载 IPsec 线路，实现客户端与服务端互通。

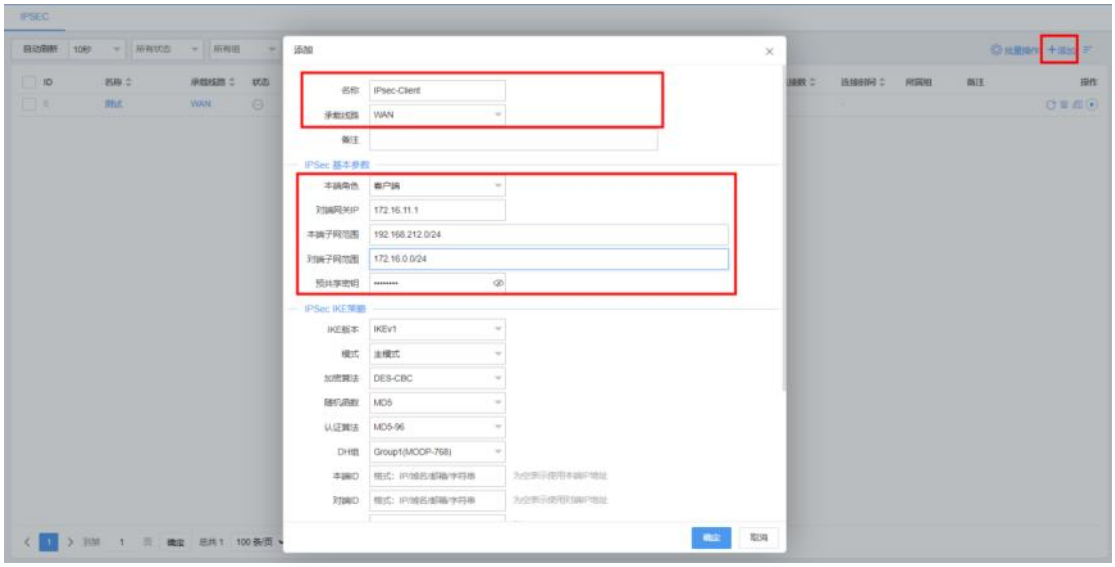
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【虚拟专网】>【IPsec】。

步骤 4 单击页面右上角【添加】，弹出添加 IPsec 线路页面。



配置示例：

1. 名称设置为“IPsec-Client”，承载线路选择配置 WAN 线路步骤中创建的 WAN 线路。
2. IPsec 基本参数：本端角色选择“客户端”，对端网关 IP 为“172.16.11.1”，本端子网范围：“192.168.212.0/24”，对端子网范围：“172.16.0.0/24”，预共享密钥填写“ASCD1234”。
3. IKE 策略：如无特殊需求，默认即可。
4. ESP 策略：如无特殊需求，默认即可。

说明

在配置时，需注意两端的预共享密钥、IKE 策略（本端 ID 与对端 ID 除外）与 ESP 策略中的参数均保持一致，否则可能导致协商失败。

步骤 5 单击【确定】。

——结束

4.11.4.2.5. 配置 IPsec 服务端策略路由

添加策略路由具体操作请参见配置策略路由，此处需要创建两条策略路由，以保证服务端与客户端能互相访问。

配置示例：

策略路由 1（到内网的路由）：目标地址设置为“172.16.0.0/24”，执行动作设置为“路由”，路由线路为需要访问的 LAN 线路。

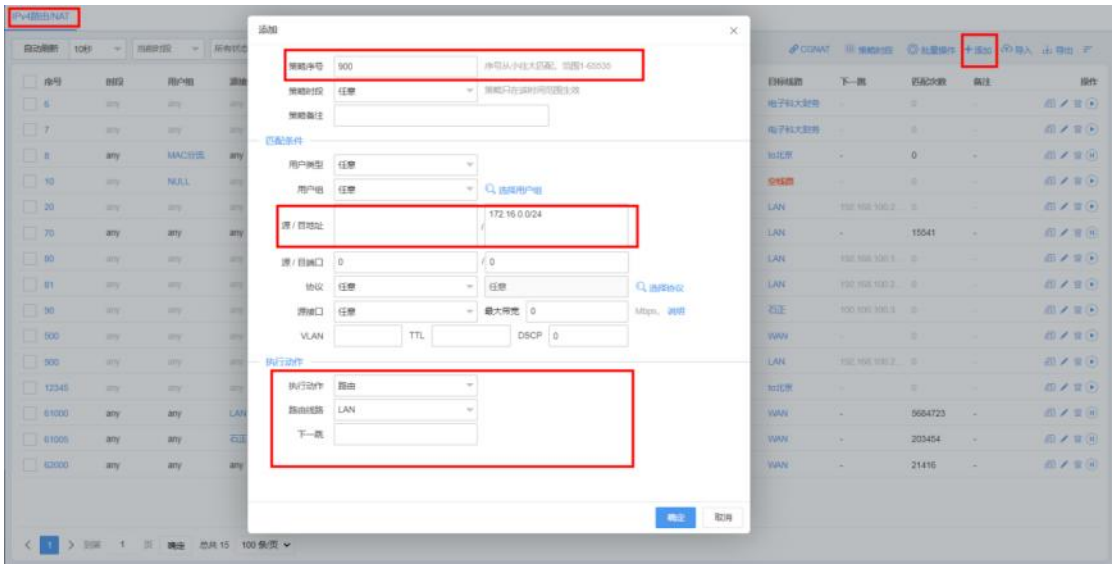


图 4-99 IPv4 路由/NAT 详情

策略路由 2（到 IPsec 客户端的路由）：目标地址设置为“192.168.212.0/24”，执行动作设置为“路由”，路由线路为已创建的 IPsec 线路。

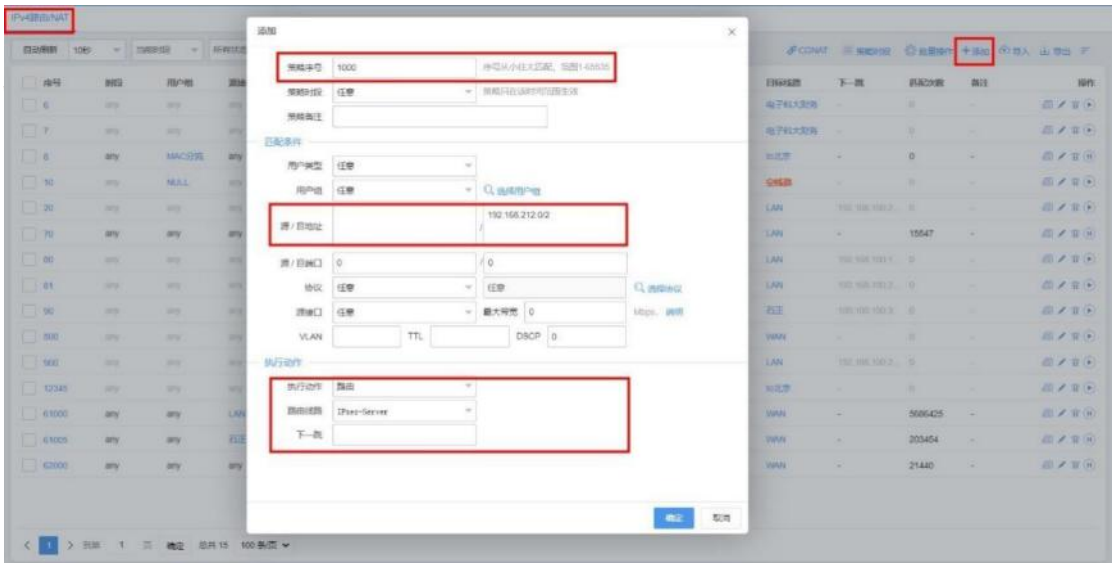


图 4-100 IPv4 路由/NAT 详情

须知

由于策略路由序号从小到大的匹配顺序，上面创建的两条策略路由，其策略序号需要小于服务端侧自身出网的默认路由，例如：匹配条件为任意，执行动作为 NAT 至出网 WAN 线路。

4.11.4.2.6. 配置 IPsec 客户端策略路由

添加策略路由具体操作请参见配置策略路由，此处需要创建两条策略路由，以保证服务端

与客户端能互相访问。

配置示例：

策略路由 1（到内网的路由）：目标地址设置为“192.168.212.0/24”，执行动作设置为“路由”，路由线路为需要访问的 LAN 线路。

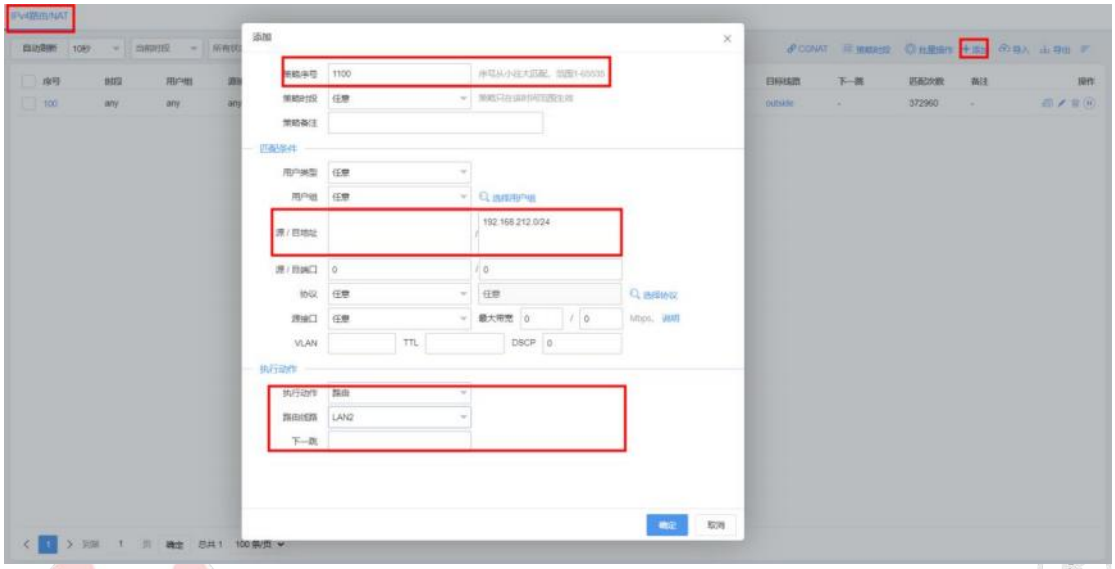


图 4-101 IPv4 路由/NAT 详情

策略路由 2（到 IPsec 服务端的路由）：目标地址设置为“172.16.0.0/24”，执行动作设置为“路由”，路由线路为已创建的 IPsec 线路。

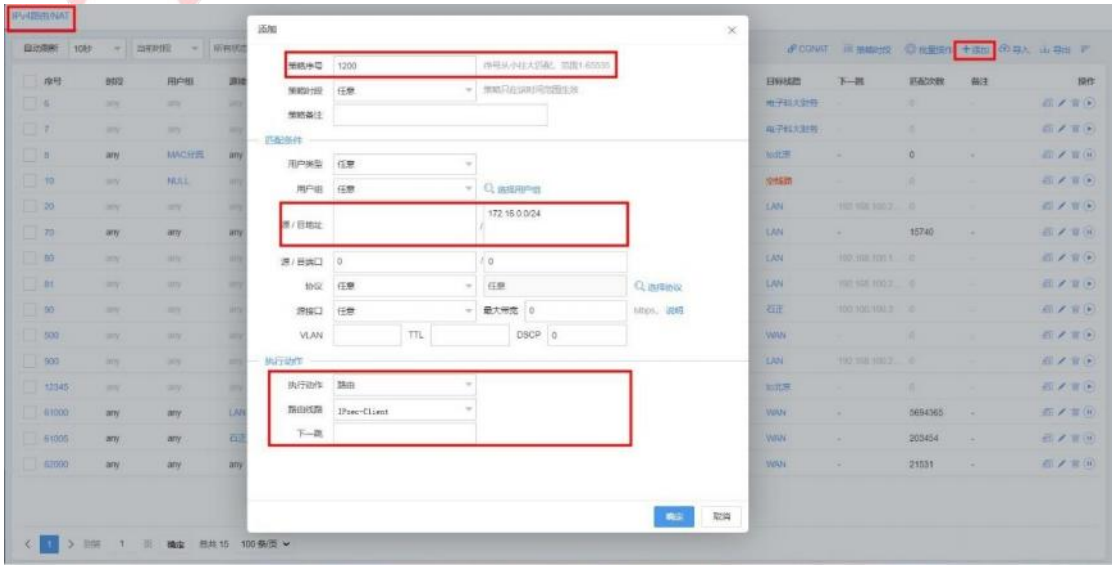


图 4-102 IPv4 路由/NAT 详情

须知

由于策略路由序号从小到大的匹配顺序，上面创建的两条策略路由，其策略序号需要小于客户端侧自身出网的默认路由，例如：匹配条件为任意，执行动作为 NAT 至出网 WAN

线路。

4.11.5. L2TP 客户端

4.11.5.1. L2TP 简介

Panabit 上网行为管理只支持 L2TP 客户端。L2TP 是标准的 Internet 隧道协议，L2TP 使用多隧道，提供包头压缩、隧道验证，并要求建立面向数据包的点对点连接。

4.11.5.2. 配置 L2TP 客户端

4.11.5.2.1. 配置 WAN 线路

创建 WAN 线路时，线路类型可选择静态 IPv4/DHCP IPv4/PPPoE，具体操作请参见配置 WAN 线路。

4.11.5.2.2. 配置 L2TP 线路

需要选择一条 WAN 线路来承载 L2TP 线路，来与 L2TP 客户端互通。

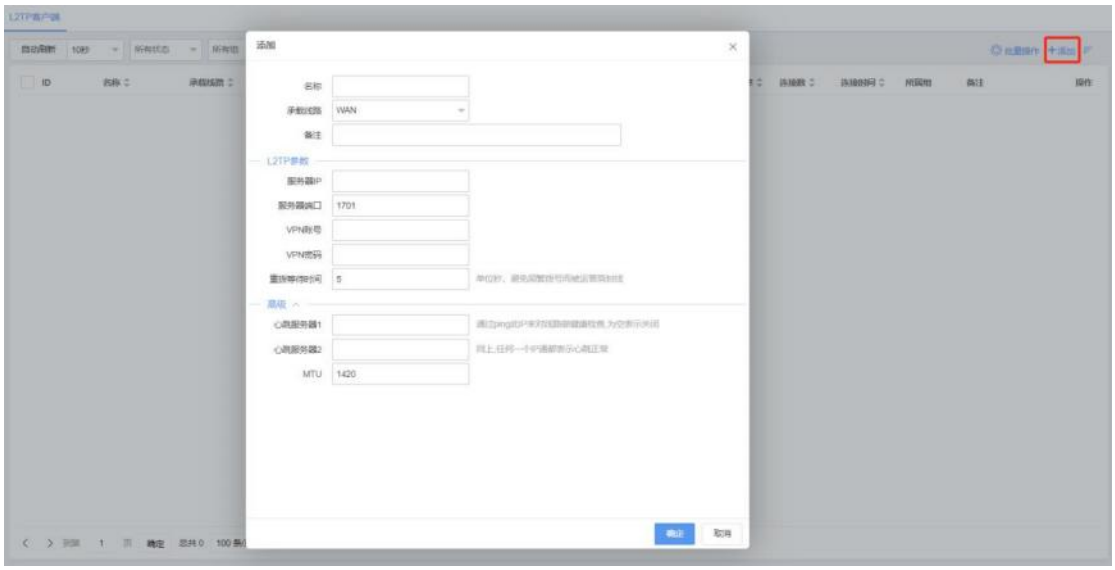
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【虚拟专网】>【L2TP 客户端】。

步骤 4 单击页面右上角【添加】，弹出添加 L2TP 线路页面。



参数名称	参数说明
名称	自定义 L2TP 线路名称。
承载线路	选择承载该 L2TP 线路的 WAN 线路。
备注	对 L2TP 线路的补充说明。
服务器 IP	L2TP 服务端的 IP 地址。
服务器端口	L2TP 服务端开放的端口。
VPN 账号/密码	输入 VPN 账号/密码。
重拨等待时间	单位秒，避免频繁拨号而被运营商封线。
心跳服务器 1	通过 ping 此 IP 来对线路做健康检查，为空表示关闭。
心跳服务器 2	通过 ping 此 IP 来对线路做健康检查，为空表示关闭。与心跳服务器 1 任何一个 IP 通都表示心跳正常。
MTU	定义数据的最大传输单元。

步骤 5 单击【确定】。

——结束

4.11.6. 常见问题

1. iWAN 客户端无法正常与服务端连接。

1）检查两端线路的公网地址能否互通。

2）检查网络出口是否有防火墙等设备屏蔽了 iWAN 绑定的端口（默认为 UDP 8000）。

3）检查 1,2 确认无问题且 iWAN 错误提示为“认证超时”，请在 iWAN 服务端中将认证模式改为“免认证”，如果“免认证”模式能正常连接，可以尝试重新创建账号或者 iWAN

服务。

2. 已按照“异地分支互联”场景步骤设置好了 iWAN 的双端和策略，但无法正常访问到目标内网。

1）确认路由策略设置正确。

2）使用客户端/服务端的 ping 功能，对 iWAN 网关进行 ping 检测。

3）如果确认状态 2 正常，则尝试 ping 对端的 LAN 线路地址。

4）确认 2,3 正常，但只能 ping 到 LAN 线路，往下则不通。如果对端是三层交换机接口，就需要在【策略路由】中，对“访问内网”的策略添加一个下一跳，下一跳为对端接口的 IP 地址。

4.12. 无线 AC

4.12.1. 概述

Panabit 上网行为管理的无线 AC 功能，配合自有品牌的 AP，能够适用于政企、酒店、商场、学校等场所无线网络环境。Panabit 上网行为管理系统自带高性能无线控制器，可以统一管理 Panabit 所有型号的 AP 设备，支持管理的 AP 数目高达 2048，提供 AP 运行状态监控 、统一固件升级、零配置、射频信道 SSID、VLAN 等设置的集中管理。

4.12.2. 应用案例：无线 AC 开局配置

某用户已经上线了上网行为管理设备，现需要新安装 20 个小派 AP，由上网行为管理设备进行统一管理，为所有 AP 统一下发“ABC 公司”的 SSID。

4.12.2.1. 配置流程

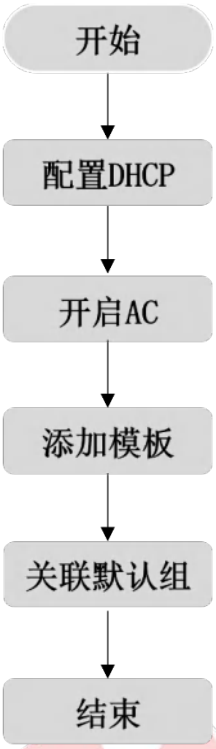


图 4-103 无线 AC 配置流程

4.12.2.2. 配置前提

Panabit 上网行为管理设备在开始配置前，已完成设备部署，具体操作请参见设备部署。

4.12.2.3. 配置步骤

4.12.2.3.1. 配置 DHCP

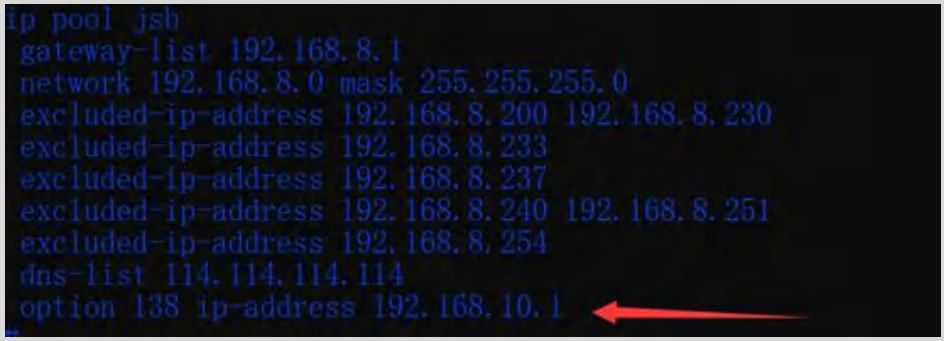
开启 AC 功能前，请完成 DHCP 功能的配置，为 AP 下发无线 AC 的地址。

具体操作请参见 DHCP 服务。

说明

1. 当上网行为管理提供 DHCP 服务时，需设置“无线控制器”参数，填写 LAN 线路地址。

2. 当其他设备提供 DHCP 服务时，需要配置 opt138 字段为 Panabit 的 LAN 线路地址，并且 AP 地址和 opt138 配置的地址能够互通。



其他设备配置 DHCP 示例

4.12.2.3.2. 开启 AC

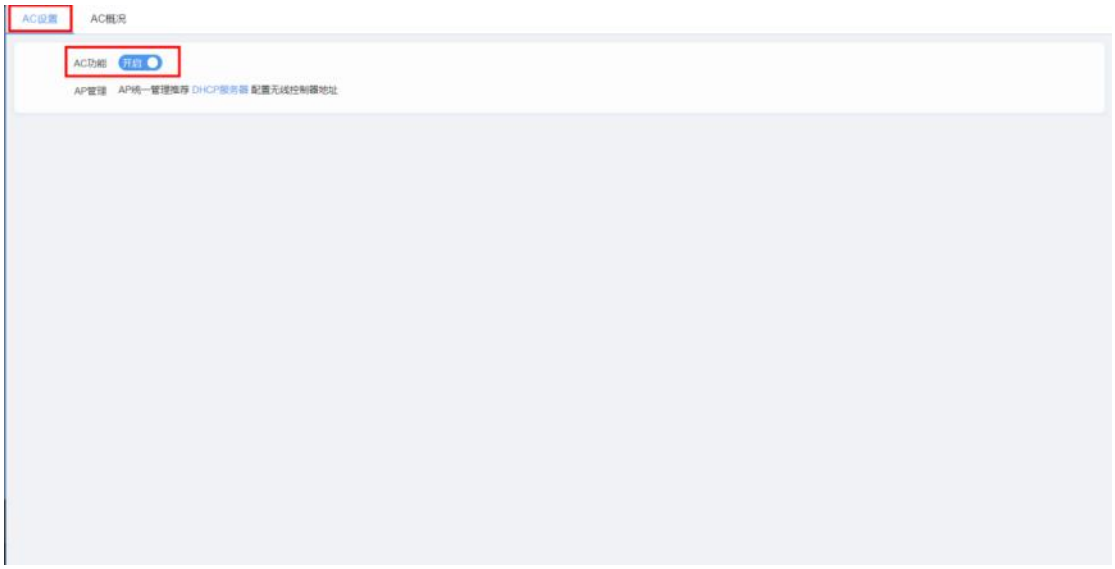
通过此操作，开启设备的 AC 功能。

操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【无线 AC】>【AC 概况】>【AC 设置】。



步骤 4 单击 开启，开启 AC 功能。

——结束

4.12.2.3.3. 添加模板

上网行为管理的无线 AC 模块，能够根据预先设置的模板，向小派 AP 批量下发配置。

说明

以下三种情况，会触发模板下发配置：

1. 新设备上线。
2. 设备更换 AP 组。
3. 修改模板配置。

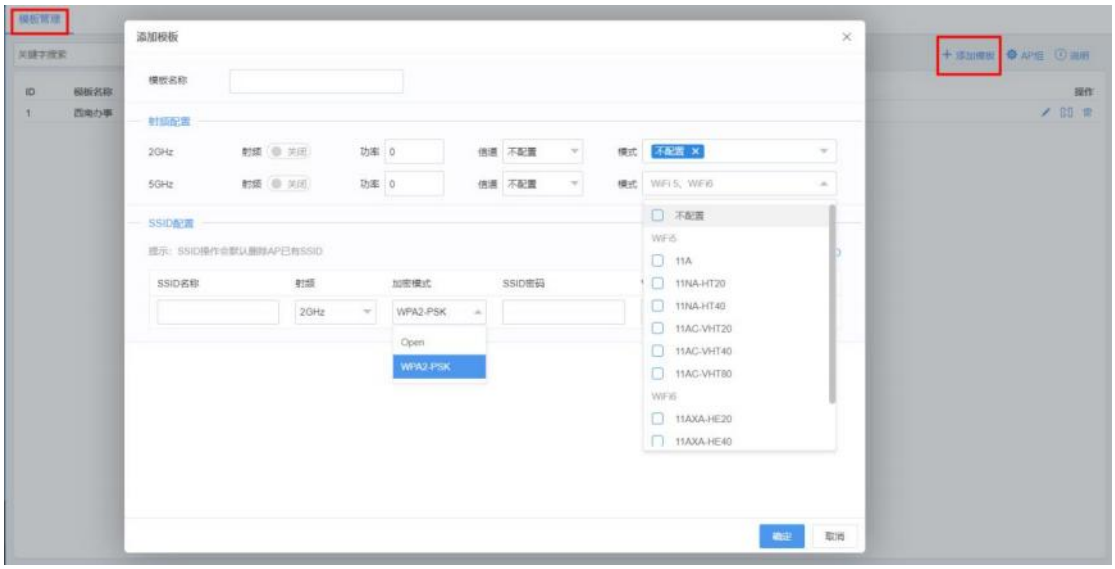
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【无线 AC】>【模板管理】。

步骤 4 单击页面右上角【添加模板】，弹出新增模板页面。



参数名称	参数说明
模板名称	自定义模板名称。
射频配置	对 2GHz、5GHz 的射频分别进行配置，可配置开启/关闭、功率、信道及模式。
SSID 配置	配置下发的 SSID，可以在此新增 SSID。 或选择已创建的 SSID，参见 SSID 管理。

配置示例：

1. 射频配置中分别开启 2GHz、5GHz 的射频。

2. SSID 配置中，点击两次 +新增SSID，添加两个 SSID。

   a) 填写 SSID 名称为“ABC 公司”，射频选择“2GHz”，SSID 密码填写“Panabit123”。

   b) 填写 SSID 名称为“ABC 公司”，射频选择“5GHz”，SSID 密码填写“Panabit123”。

步骤 5 单击【确定】。

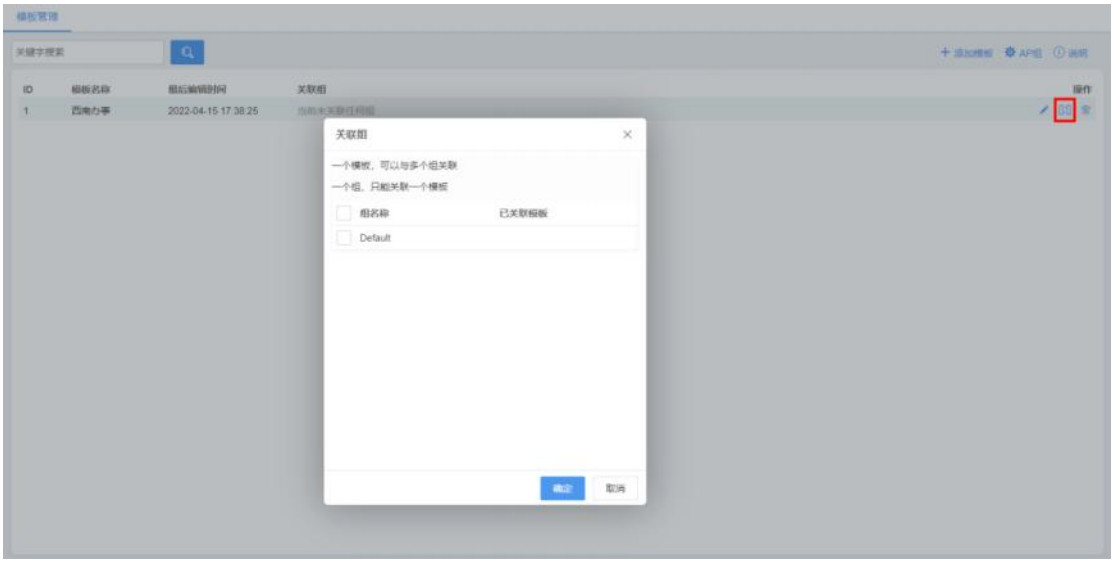
——结束

4.12.2.3.4. 关联默认组

模板配置完毕后，可以将其关联到 AP 组。AP 上线后直接通过模板可下发射频、功率、频宽、SSID 名称、密码、VLAN 的配置信息到 AP。

操作步骤

步骤 1 单击已创建模板操作列的，可进行模板关联。



步骤 2 勾选默认组“Default”，单击【确定】。

——结束

上述设置完毕后，模板中的配置都会对新接入的小派 AP 生效。

4.12.3. AC 概况

通过该模块，可以查看无线 AC 的整体运行情况。

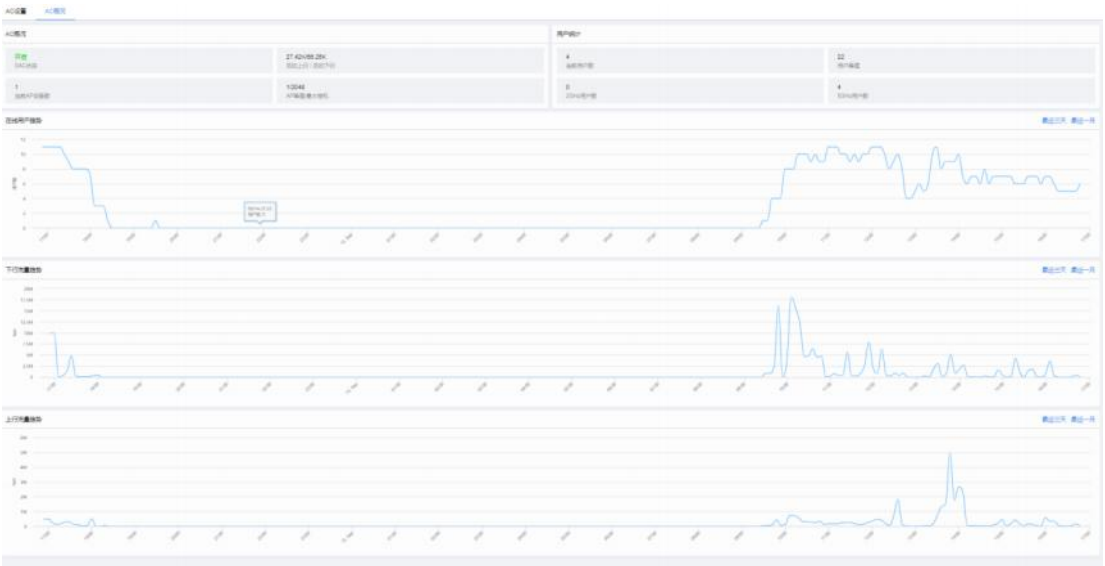


图 4-104 AC 概况详情

参数名称	参数说明

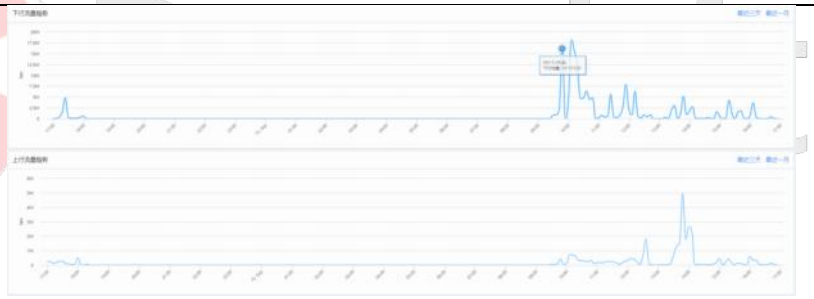
AC 概况	 显示 AC 的基本情况，如 AC 的开启状态、总的上行/总的下行、当前 AP 设备数、AP 峰值/最大带机。
用户统计	 显示 AP 的无线用户情况，如当前用户数、用户峰值、2GHz 用户数、5GHz 用户数。
在线用户趋势	 显示近 24 小时内无线在线用户数统计趋势图，可查看最近三天与最近一月的统计。
下行/上行流量趋势	 显示近 24 小时内无线用户的上下行流量趋势，可查看最近三天与最近一月的统计。

表 4-58 AC 概况参数说明

4.12.4. 无线用户

在此模块下，可以查看当前无线用户的详细情况。

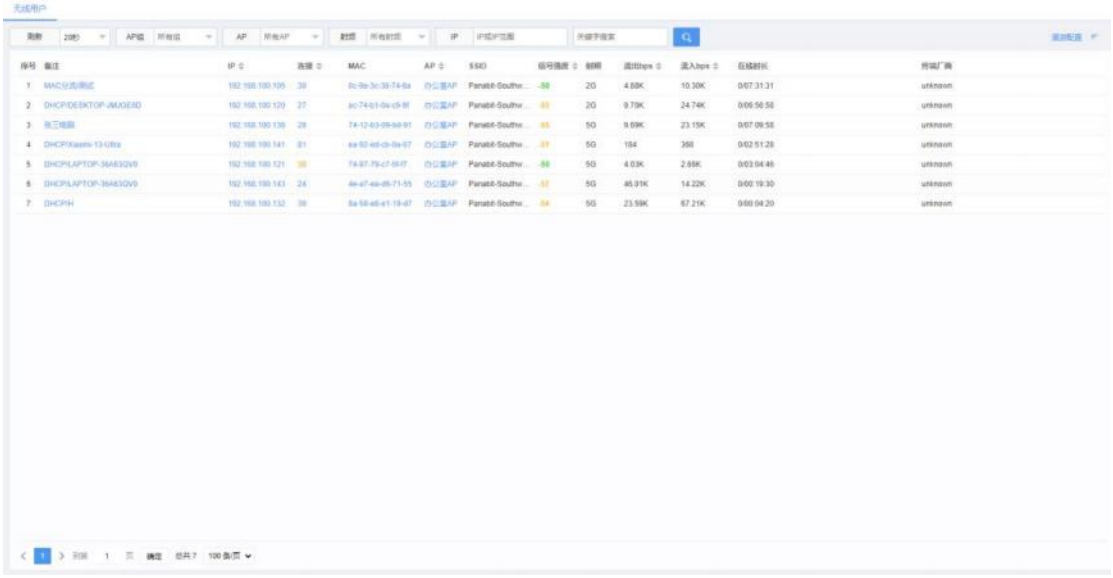


图 4-105 无线用户详情

参数名称	参数说明
序号	在线无线用户的序号
备注	显示在线用户的备注，点击具体的备注名，可对该用户进行 IP/MAC 的备注，并指定用户组。 
IP	无线用户的 IP 地址，点击可查看 IP 档案。  IP 档案中的详细参数，参见所有用户。
连接	无线用户当前的连接数，点击可查看 IP 档案。

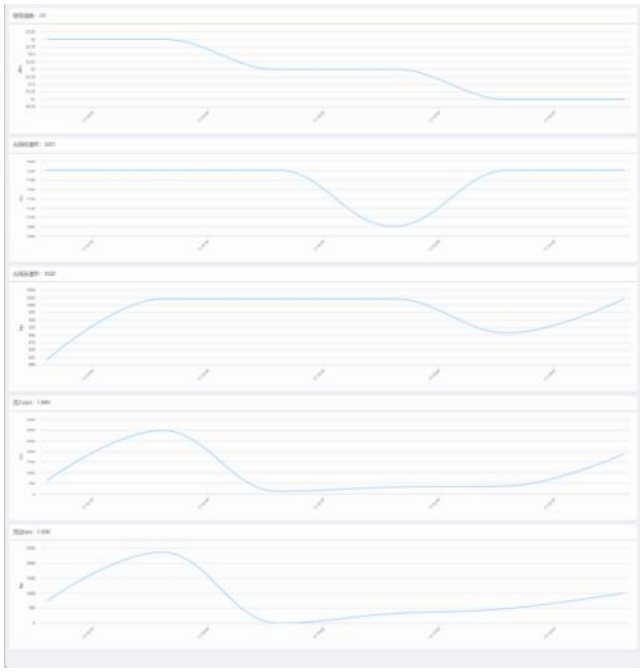
MAC	无线用户的 MAC 地址，点击可查看其实时连接的重点参数。 
AP	无线用户所连接的无线 AP，点击可查看 AP 详情。 
SSID	无线用户所连接的无线 SSID。
信号强度	无线用户当前连接的信号强度，单位 dBm。
射频	无线用户所连接的无线射频。
流出 bps	无线用户当前的流出速率。
流入 bps	无线用户当前的流入速率。
在线时长	无线用户连接 AP 后的在线时间。
终端厂商	无线用户的终端厂商标识。
漫游配置	对无线用户的漫游进行配置。

表 4-59 无线用户参数说明

4.12.5. AP 管理

通过该模块，设置 AP 的属性、射频、信道，并能对 AP 执行开/关灯、重启、重置、升级、迁移至云、导入、导出等操作。

4.12.5.1. 创建 AP 组

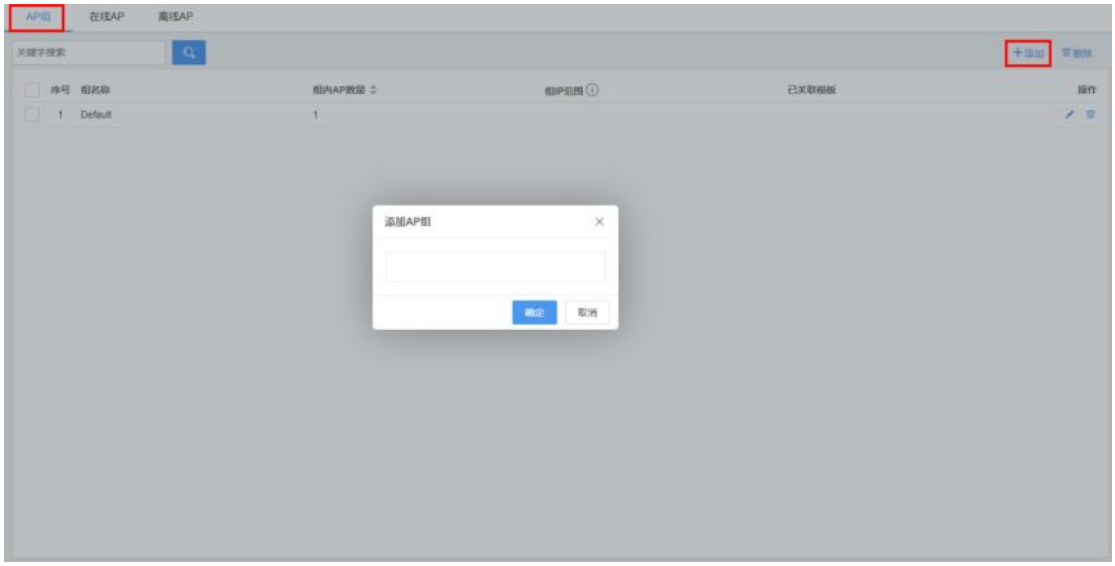
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【无线 AC】>【AP 管理】>【AP 组】。

步骤 4 单击【添加】，新增 AP 组。



步骤 5 输入 AP 组名称，单击【确定】。

——结束

4.12.5.2. 属性配置

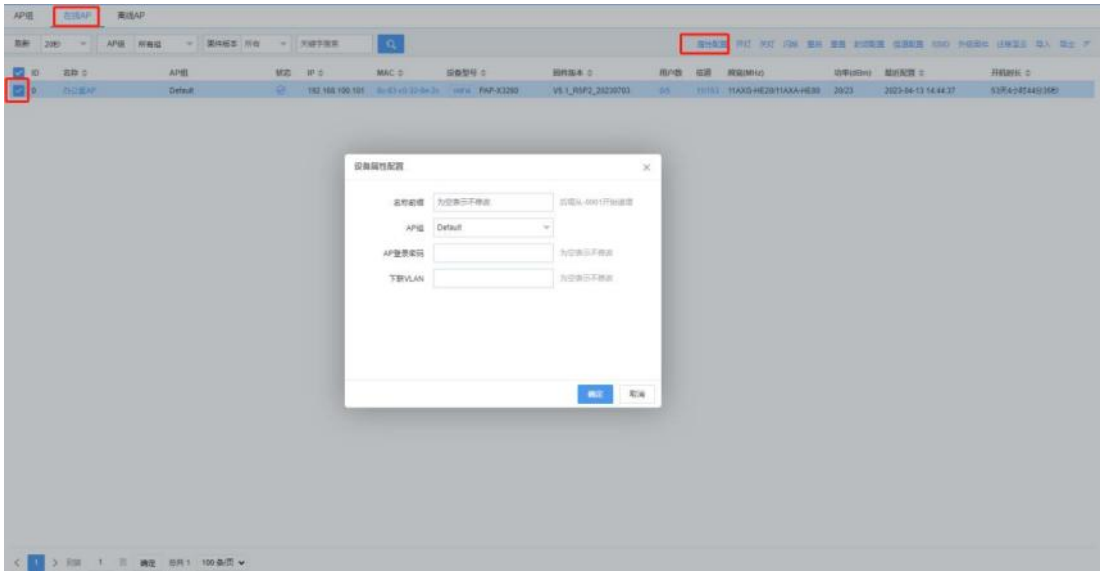
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【无线 AC】>【AP 管理】>【在线 AP】。

步骤 4 勾选需要配置的 AP，单击【属性配置】，配置 AP 属性。



参数名称	参数说明

名称前缀	对 AP 进行批量命名时使用，如设置前缀为“公司”，则 AP 的名称将配置为“公司-0001”、“公司-0002”，以此类推。
AP 组	将 AP 加入选择的 AP 组之中。
AP 登录密码	修改 AP 管理页面的登录密码。
下联 VLAN	为 AP 的有线接口配置 VLAN。

步骤 5 单击【确定】。

4.12.5.3. 射频配置

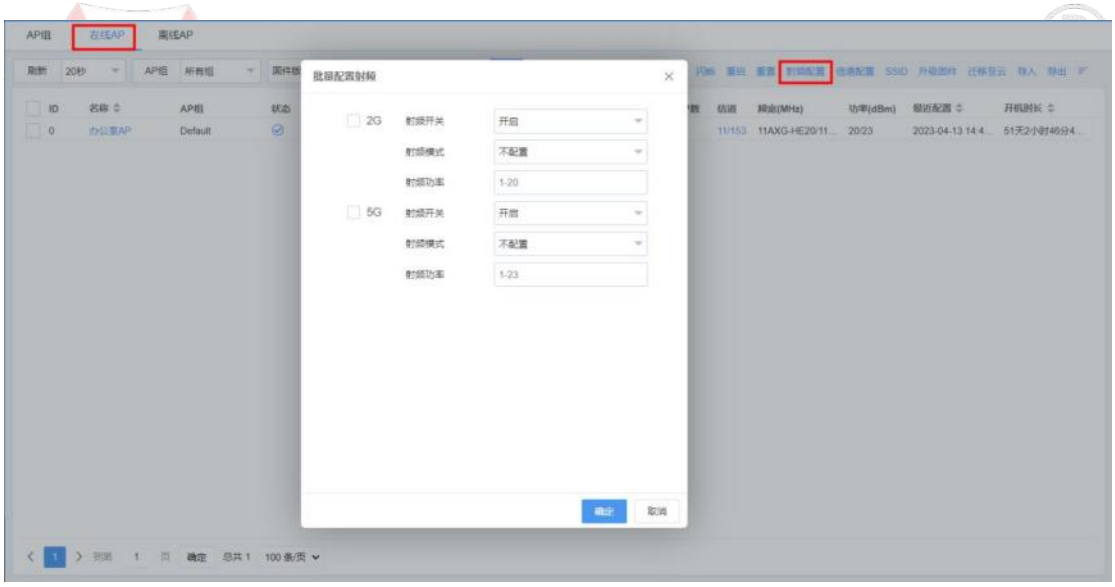
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

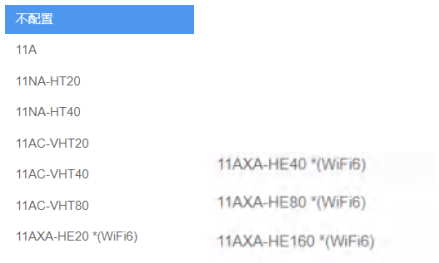
步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【无线 AC】>【AP 管理】>【在线 AP】。

步骤 4 勾选需要配置的 AP，单击【射频配置】，配置 AP 射频。



参数名称	参数说明
2G	射频开关：可设为“开启”或“关闭”。 射频模式：可选择如下射频模式。 不配置 11B 11G 11NG-HT20 11NG-HT40 11AXG-HE20 *(WiFi6) 11AXG-HE40 *(WiFi6) 射频功率：取值 1~20。

5G	射频开关：可设为“开启”或“关闭”。 射频模式：可选择如下射频模式。  射频功率：取值 1~23.

步骤 5 单击【确定】

——结束

4.12.5.4. 信道配置

无线 AP 的信道是指用于在无线局域网络（WLAN）中传输数据的特定频段或频率范围。这些信道被用于在无线网络中传输数据，以确保不同设备之间的通信不会干扰彼此。

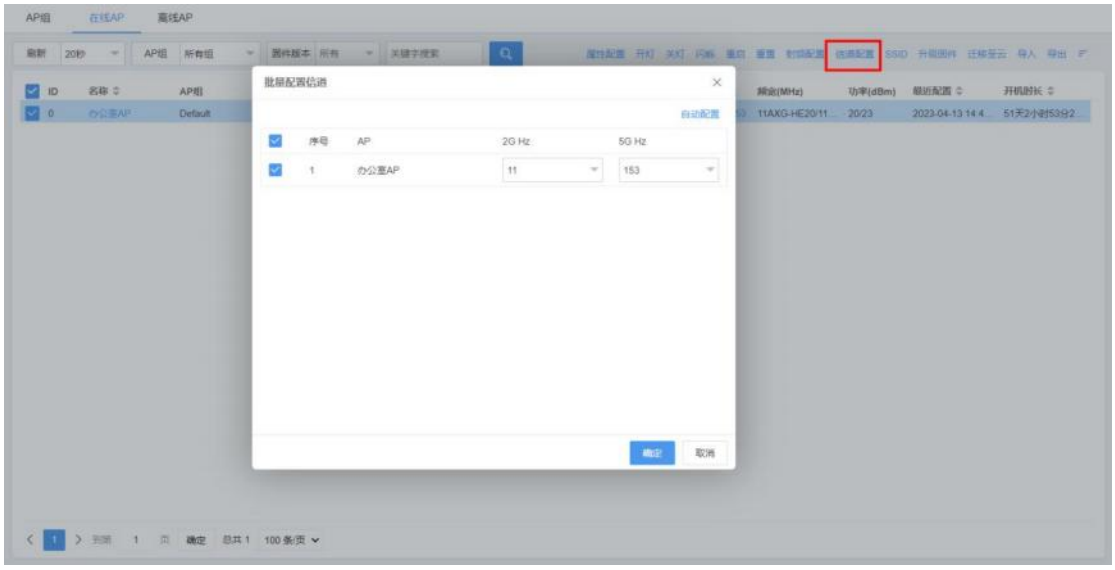
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【无线 AC】>【AP 管理】>【在线 AP】。

步骤 4 勾选需要配置的 AP，单击【信道配置】，配置 AP 信道。



参数名称	参数说明

2G Hz	选择 2G Hz 的信道。
5G Hz	选择 5G Hz 的信道。
自动配置	点击后，自动为所选 AP 分配信道。

步骤 5 单击【确定】。

——结束

4.12.5.5. 升级固件

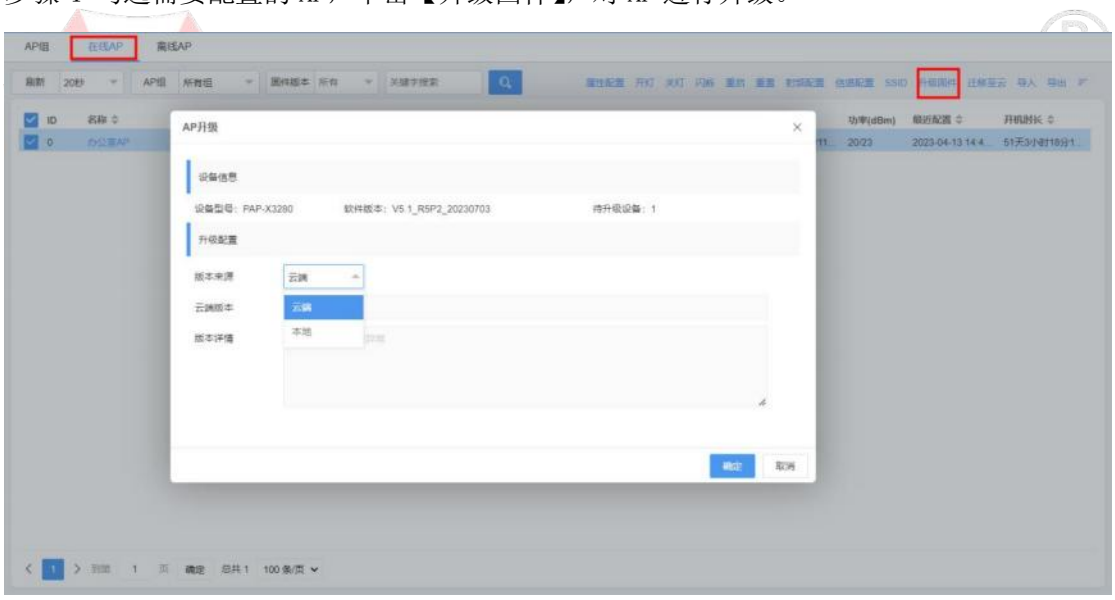
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【无线 AC】>【AP 管理】>【在线 AP】。

步骤 4 勾选需要配置的 AP，单击【升级固件】，对 AP 进行升级。



参数名称	参数说明
设备信息	当前设备的固件信息。
版本来源	云端 ● 云端版本：云端的固件版本号。 ● 版本详情：版本的详细更新内容描述。 本地：

	● 版本链接：固件版本所在的 URL。

步骤 5 单击【确定】。

——结束

4.12.6. SSID 管理

通过此操作，在 SSID 管理页面配置 WiFi 名字，可调整参数是否加密，以及生效的 AP、生效射频等信息，并能设置和修改不同 SSID 生效的 VLAN。

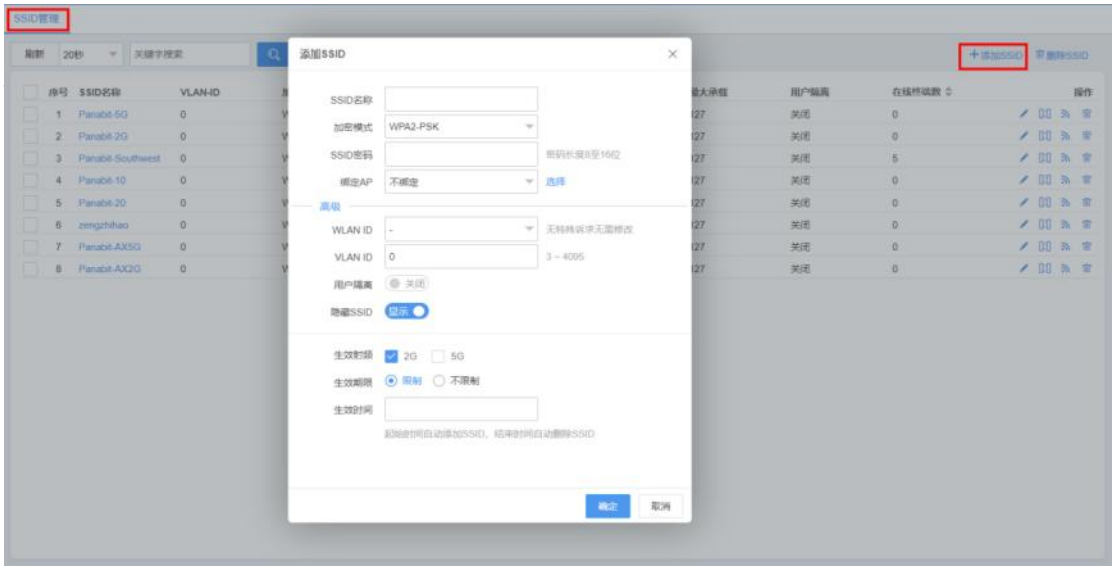
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【无线 AC】>【SSID 管理】。

步骤 4 单击右上角的【添加 SSID】，弹出新增 SSID 页面。

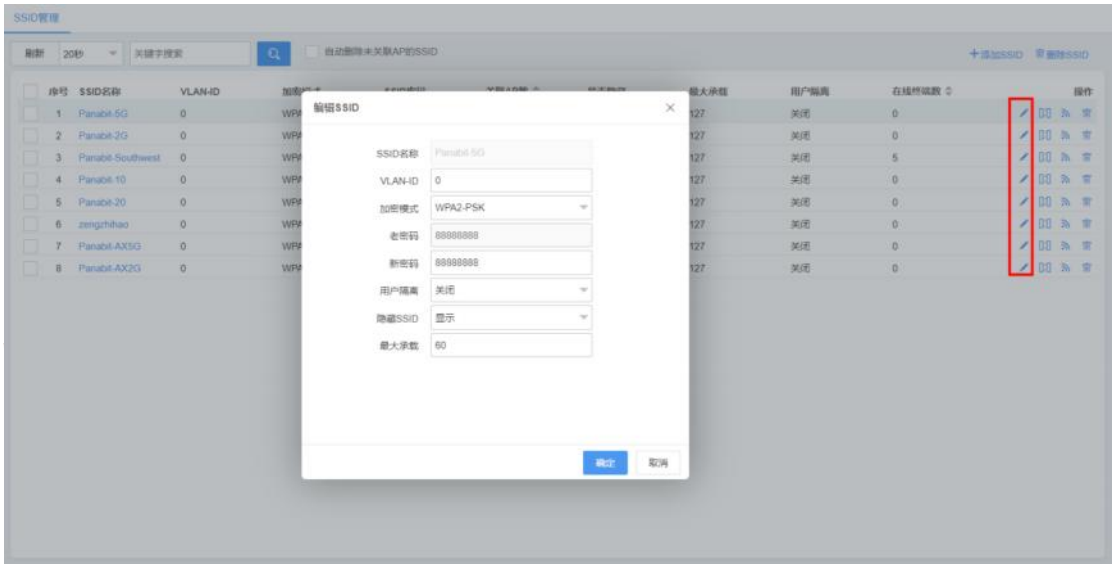


参数名称	参数说明
SSID 名称	设置 SSID 的名称。
加密模式	选择加密的模式，如设为“WPA2-PSK”或“Open”。
SSID 密码	密码长度 8 至 16 位。
绑定 AP	将该 SSID 绑定至选择的无线 AP 上。
WLAN IN	用于识别和区分不同的无线局域网络（WLAN）的唯一标识符。无特殊诉求无需修改。
VLAN ID	3 ~ 4095

用户隔离	如果启用了用户隔离，连接到同一 SSID 的设备将无法直接相互通信。可设为“开启”或“关闭”。
隐藏 SSID	是否隐藏该 SSID。可设为“显示”或“隐藏”
生效射频	可选择“2G”或“5G”。
生效期限	可选择“限制”或“不限制”。 选择限制时需要设置生效时间，起始时间自动添加 SSID，结束时间自动删除 SSID。

步骤 5 单击【确定】。

步骤 6 单击 SSID 名称后的 ，可编辑 SSID。



步骤 7 单击【确定】。

——结束

4.12.7. 模板管理

参见添加模板。模板添加完成后，单击已创建模板操作列的 ，可进行模板关联。

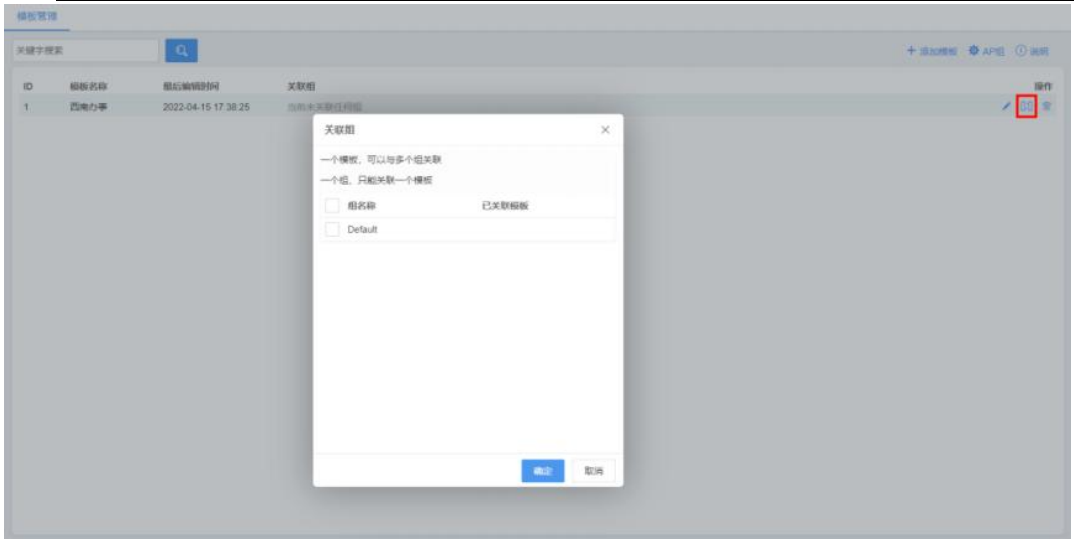


图 4-106 模板管理详情

勾选需要关联的 AP 组，单击【确定】即可下发模板配置。

4.12.8. 计划任务

通过此模块，添加计划可设置某些 AP 定时开关灯、重启、添加删除 SSID 操作。

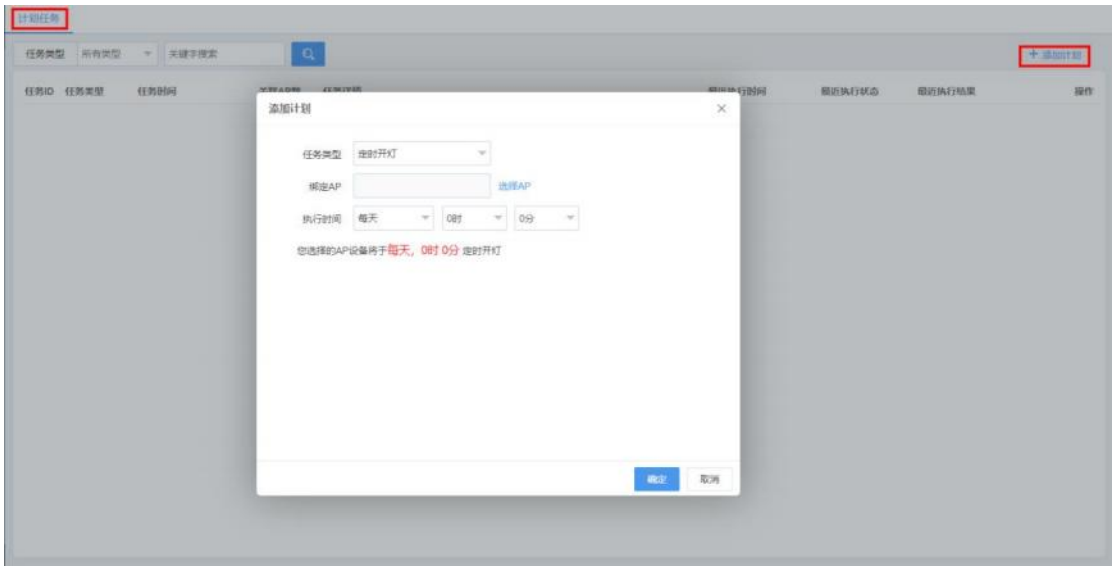
操作步骤

步骤 1 打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2 输入用户名 admin 并校验密码，登录 WEB 控制台。

步骤 3 选择【无线 AC】>【计划任务】。

步骤 4 单击页面右上角【添加计划】，对 AP 进行升级。



参数名称	参数说明

任务类型	可执行“定时开灯”、“定时关灯”、“定时重启”等任务。
绑定 AP	选择需要绑定的 AP。
执行时间	设置任务执行时间。

步骤 5 单击【确定】。

——结束

4.12.9. AC 日志

通过此模块，查看 AC 管理下的无线 AP 的历史事件记录。可记录的事件包含：添加 SSID、删除 SSID、修改 SSID、修改射频、AP 升级、重启、重置、关灯、开灯、上线、超时离线等。点击右上角的导出，可将日志文件导出至本地。

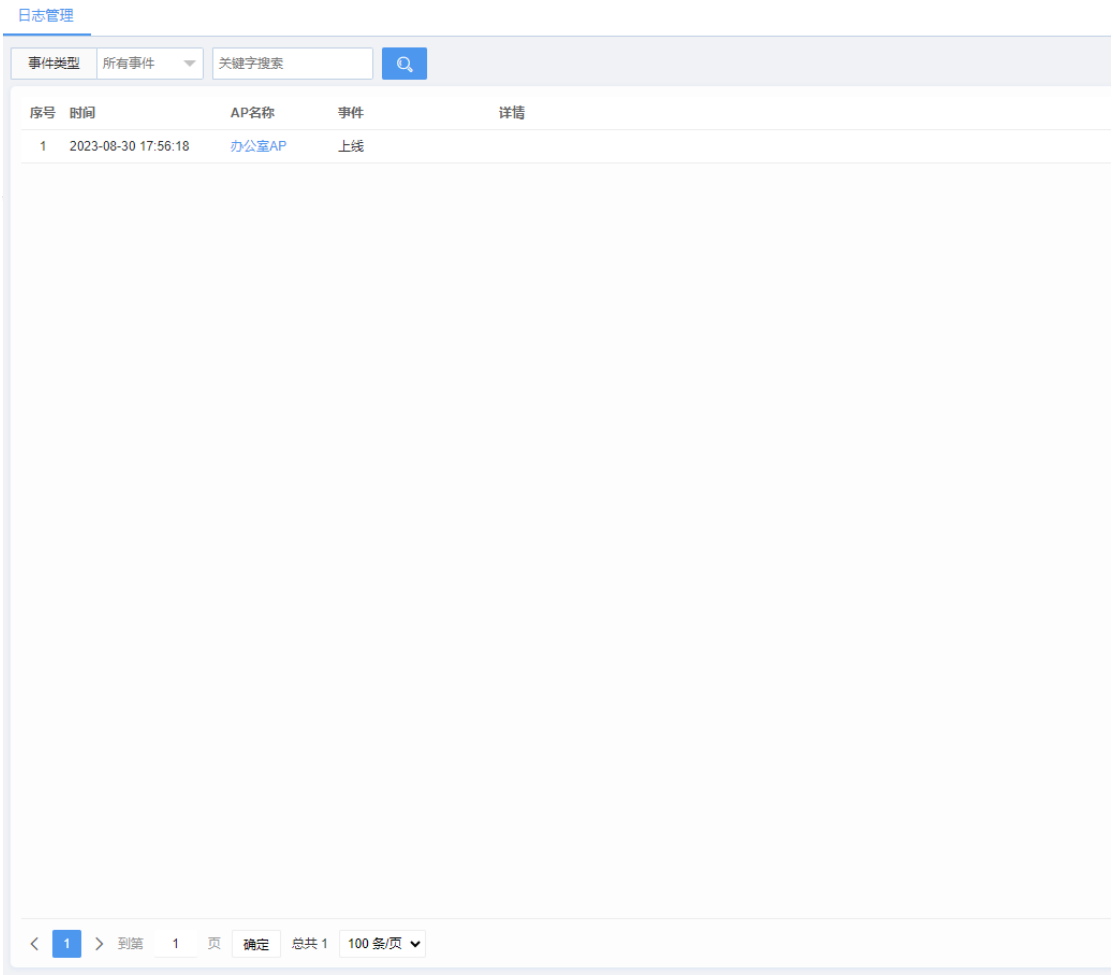


图 4-107 AC 日志详情

4.13. 对接公安网监：公共无线上网管理平台

4.13.1. 概述

随着社会的不断发展和进步，互联网在创造巨大商业价值的同时，色情、反动、暴力等网络犯罪行为也严重干扰大家的正常生活，给社会带来了极大危害。

国家公安部于 2006 年 3 月 1 日正式实施的 82 号令，即《互联网安全保护技术措施规定》中提到：“公安机关应当根据网络安全防范需要和网络安全风险隐患的具体情况，对提供公共上网服务的单位开展监督检查”，“未采取记录并留存用户注册信息和上网日志信息措施的，依照《中华人民共和国网络安全法》，第五十九条第一款的规定予以处罚”。

公安部门正逐步加大对公共网络接入和上网的监管力度，以共同构建绿色上网环境，保障公共利益，组织网络犯罪。对接公安网监平台，成为公共网络接入的基本要求。

Panabit 上网行为管理支持对接公安网监：公共无线上网管理平台，该功能通过安审对接 APP 实现。

4.13.2. 应用场景

Panabit 上网行为管理支持与全国公安网监的无线非经营场所的监管平台对接，满足非经营性互联网信息服务提供用户的“合规审计”需求。

适用于非经营类公共场所：交通枢纽场所、娱乐场所、旅店宾馆场所、餐饮服务场所、金融服务场所、购物场所、公共服务场所、公共休闲场所，以及教育机构场所等。

4.13.3. 业务流程

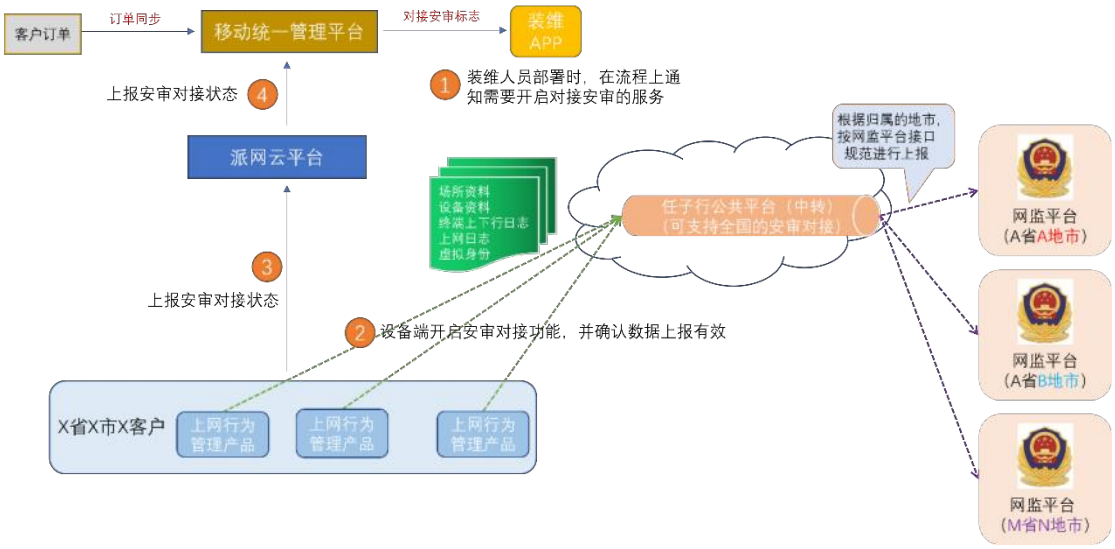


图 4-108 对接公安网监流程

1. 在客户侧已部署的 Panabit 上网行为管理设备上安装与配置“安审对接 APP”。
2. 对接完成后，Panabit 上网行为管理将连接用户信息数据以私有协议方式传输给任子行公共平台中转节点服务器（可支持全国）。上报数据包括场所资料、设备资料、终端上下行日志、上网日志、虚拟身份。
3. 对接完成后，客户侧需在安审对接 APP 上将填报数据导出一份 Excel 提交给任子行进行备案。
4. 任子行公共平台中转节点服务器收到上报数据后根据归属地市，将数据按公安部门传输规范上报给该地市的公安网监平台。

4.13.4. 配置步骤

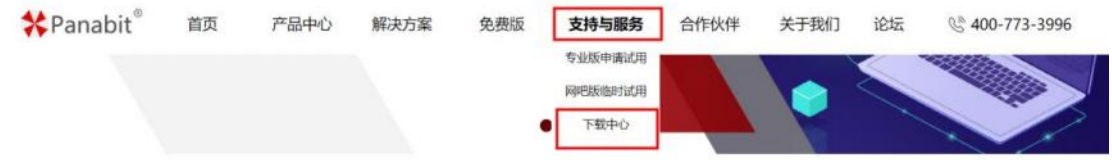
4.13.4.1. 安装安审对接 APP

可通过 Panabit 官网或设备 WEB 控制台，安装安审对接 APP，为后续对接安全审计信息提供平台。安装“安审对接”APP 可通过如下两种方式：

1. 通过 Panabit 官网安装“安审对接”APP。

步骤 1 打开浏览器，前往官网 www.panabit.com。

步骤 2 选择【支持与服务】>【下载中心】，选择【APP】，在 APP 列表中找到“安审对接 APP”。



步骤 3　单击【下载】，将 APP 安装文件下载至本地。

步骤 4　登录 WEB 控制台，进入【流量概况】>【应用商店】，点击页面右上方的 安装升级 ，找到本地已下载的安审对接 APP，按照提示完成安装。

——结束

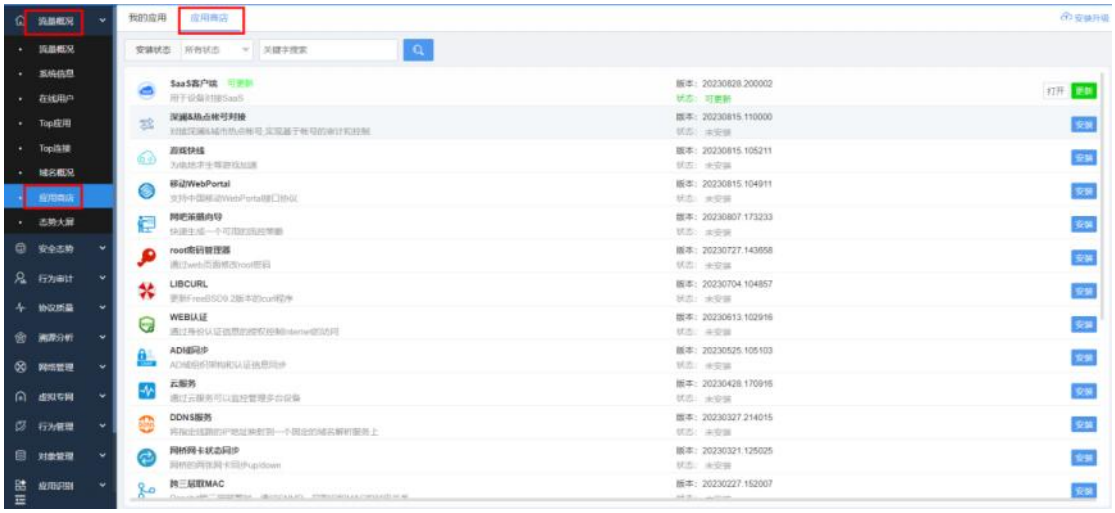
2. 通过 WEB 管理平台安装“安审对接”APP。

步骤 1　打开浏览器，输入设备管理口地址，进入登录页面。

步骤 2　输入用户名和密码，登录 WEB 控制台。

步骤 3　选择【流量概况】>【应用商店】>【应用商店】。

步骤 4　在 APP 列表找到“安审对接”APP，单击【安装】。



——结束

4.13.4.2. 开启安审对接

通过此操作，打开安审对接功能。

操作步骤

步骤 1 登录安审对接 APP，选择【参数配置】。

步骤 2 安审对接设置为“开启”，其他参数默认。

参数名称 *参数为必填	参数说明
服务器状态	已连接：表示与任子行对接服务器对接成功。 未连接：表示与任子行对接服务器对接失败。 **说明** 如连接失败需要检查服务器 IP 与端口号是否正确或与任子行服务器网络是否可达。
*安审对接	开启：允许与任子行对接服务器建立连接。 关闭：不允许与任子行对接服务器建立连接。
*服务器 IP 地址	由任子行分配。
*服务器端口号	由任子行分配。
*认证方式	认证：终端接入设备时，会接收到运营商发来的认证信息。 不认证：终端接入设备时，不进行认证。

——结束

4.13.4.3. 填报场所信息

场所信息请提前使用以下表模板向客户收集：

数据项名称 *数据为必填	长度 单位：字符	说明	示例
场所编码后六位	6	导入场所是否需要定制化。 1：定制化场所后以定制化为主，此时填写无效。 2：非定制化时，若填写编码，则以填写的编码为准，否则自动生成新的场所编码	258636
*场所名称	100	场所名称必须唯一	XX 酒店
*场所地址	100	场所地址用来确定经纬度	广东-深圳-南山-XX 路 XXX 号
*场所类型	100	下拉选择场所类型	
*省代码（省份）	6	/	440000
*市代码（城市）	6	必须为所选省下的市代码	440300
*区代码（地区）	6	必须为所选市下的区县代码	440305
*服务状态	100	下拉选择服务状态	/
*经营性质	30	下拉选择经营性质	/
*采集类型	30	下来选择采集类型	/
*合作厂商	100	对照合作厂商选择合适厂商	/
*安全厂商	100	对照填写安全厂商	/
网监厂商	100	对照填写网监厂商	/
网监平台	30	填写对应厂商下的网监平台	/
派出所	30	填写所选省市区下的派出所编码	4403050
备注	100		/

场所网络接入服务商	30	下拉选择服务商	/
接入方式	30	下拉选择接入方式	/
网络接入账号或固定 IP 地址	30	运营商账号信息或 IP	192.168.53.85
法定代表人姓名	30		张三
法定代表人身份证	20		440303XXXXXXXX3356
法定代表人联系电话	20		138XXXX5432
营业开始时间	20	格式：hh:mm	08:00
营业结束时间	20	格式：hh:mm	21:00
场所负责人	20		
负责人联系电话	20		
信息安全员	8		
安全员联系电话	14		
统一社会信用代码	30		
上级场所编码	300	注意确认场所编码是否存在	
上级场所名称	300	注意确认场所名称是否存在	

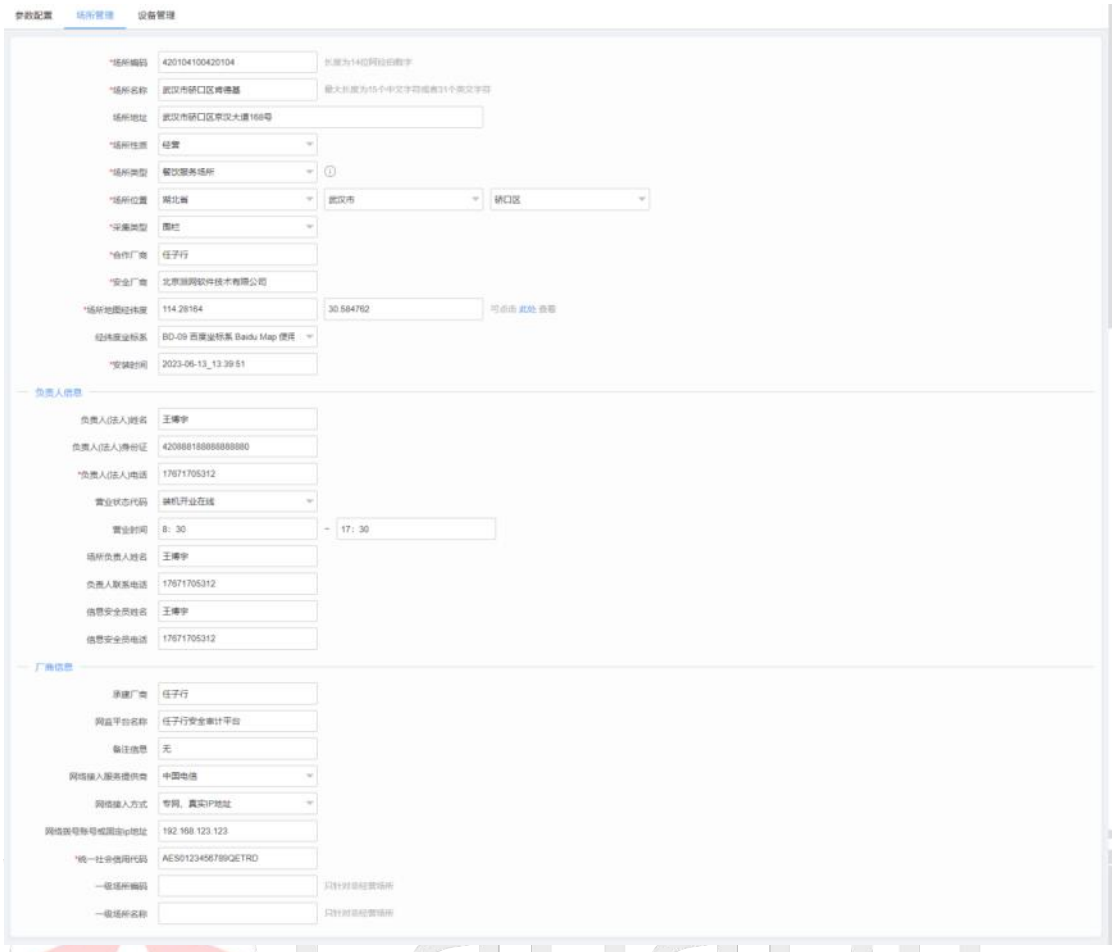
说明

涉及的区域代码（省、市、区）及派出所代码，请联系派网技术人员获取。

操作步骤

步骤 1 登录安审对接 APP。

步骤 2 选择【场所管理】，设置场所信息。



参数名称 *参数为必填	参数说明
场所编码	场所编码由 14 位阿拉伯数字组成。 代码从左至右的含义是： ● 第 1 至第 6 位表示上网营业场所所在省（自治区、直辖市）、市（地区、盟）、区（县、 旗），按 GB/T 2260 规定的行政区划代码生成，作为标识代码使用，该标识代码生成后不随当地行政区划代码变更而改变。 ● 经营性上网服务场所，第 7、第 8 ，第 9 位取值为“100”。 ● 非经营性上网服务场所， 第 7 固定为 2，表示属于互联网公共上网服务场所，第 8 位表示上网服务场所类型。 ● WIFI 无线采集前端，第 7 固定为 3，表示属于 WIFI 无线采集前端， 第 8 位表示上 网服务场所类型。 ● 电子围栏前端， 第 7 位固定为 8，表示属于电子围栏前端， 第 8 位表示上网服务场所类型。

	● 车辆卡口前端， 第 7 为固定为 7，表示车辆卡口前端，第 8 为表示上网服务场所类型。 ● 视频探头， 第 7 为固定为 6，表示视频探头，第 8 为表示上网服务场所类型。 ● 第 9 至第 14 位用 6 位阿拉伯数字表示序列号， 该序列号由该单位或场所管辖地公安机关网安部门定义。
场所名称	客户设备所在场所名称（最大长度为 15 个中文字符或者 31 个英文字符）。
场所地址	如要填写，填写客户设备所在场所地址即可。
场所性质	客户设备所在场所经营性质，根据实际情况填写即可。
场所类型	● 客户经营场所所属类型，可按下列分类选择： ● 旅店宾馆类 （住宿服务场所）：宾馆酒店、招待所、度假村、旅店。 ● 图书馆阅览室：图书馆。 ● 电脑培训中心类：电脑培训中心类。 ● 娱乐场所类：KTV、酒吧、咖啡厅、棋牌室、茶楼、录像厅（室）、 桑拿洗浴、足浴、理发店、美容院、 游戏厅等。 ● 交通枢纽：飞机场、火车站、轮船码头、公交枢纽站、交通要道、城市出入口等。 ● 公共交通工具：地铁、公交车、轮船、 火车、高铁、客运大巴、 出 租营运车辆等。 ● 餐饮服务场所：餐饮连锁。 ● 金融服务场所：银行、证券公司、保险公司、银行网点等。 ● 购物场所：大型商场、普通商店、超市、 书店、汽车销售场所等。 ● 公共服务场所：政府机构办事大厅、 学校、 加油站、 医院、邮局、 社区服务中心等。 ● 文化服务场所： 展览馆、博物馆、美术馆、电影院、音乐厅、剧场等。 ● 公共休闲场所： 体育场（馆）、游泳场（馆）、 广场、公园、街 道、小区休闲广场、浴室等。
场所位置	根据客户设备实际所处的省，市，区填写即可。

采集类型	● 围栏：数据从围栏设备采集。 ● WIFI：数据从 WIFI 设备采集。 ● 车载：数据从车载设备采集。
合作厂商与安全厂商	● 目前合作厂商指定为任子行网络技术有限公司。 ● 目前安全厂商指定为北京派网软件有限公司。
场所地图经纬度与经纬度坐标系	场所所在经纬度可根据选择的坐标系中查询获得，复制填入即可
安装时间	以客户设备实际安装时间填写
负责人（法人）姓名，省负责	如实填写设备所在该场所负责人（法人）姓名，省负责人姓名。
负责人（法人）电话	如实填写设备所处该场所负责人（法人）11 位手机号码或 8 位座机号码。
营业状态代码	如实填写当前设备营业状态即可。
营业时间	如实填写营业开始时间与结束时间即可。
场所负责人姓名，电话	如实填写设备所处场所负责人姓名，手机或座机号码即可。
信息安全员姓名，电话	如实填写设备所处场所信息安全员姓名，手机或座机号码即可。
承建厂商	目前承建厂商指定为任子行网络技术有限公司。
网监平台名称	承建厂商建立的网监平台系统名称。
网络接入服务商	网络接入服务商选择接入的相应运营商即可。
网络接入方式	接入方式按照真实的网络接入环境选择。
网络拨号账号或固定 IP 地址	客户设备网络拨号账号或固定的 IP 地址。
统一社会信用代码	设备厂商的 9 位厂商编码。
一级场所编码	安审对接 APP 所在设备的场所编码（只针对非经营性场所）。
一级场所编码名称	安审对接 APP 所在设备的场所名称（只针对非经营性场所）。

步骤 3 单击【立即提交】。

——结束

4.13.4.4. 填报设备信息

设备信息提前使用以下模板向客户收集：

设备 MAC 地址	二选一即可，若两个都有值，以场所编码为准		0 表示无则新增，有也不覆盖 1 表示无则新增，有则覆盖	设备所在楼层号 非必填项
*设备 MAC	*场所编码	*场所名称	*更新标识	设备楼层或房号

操作步骤

步骤 1 登录安审对接 APP。

步骤 2 选择【设备管理】，设置设备信息。

参数名称 ***参数为必填**	**参数说明**
*设备 MAC	设备网卡 MAC 地址。
*场所编码	请参照填报场所信息步骤中填写的内容。
*场所名称	请参照填报场所信息步骤中填写的内容。
*更新标识	根据需求填写。
楼层号或房号	设备所在楼层号或房号。

步骤 2 单击【立即提交】。

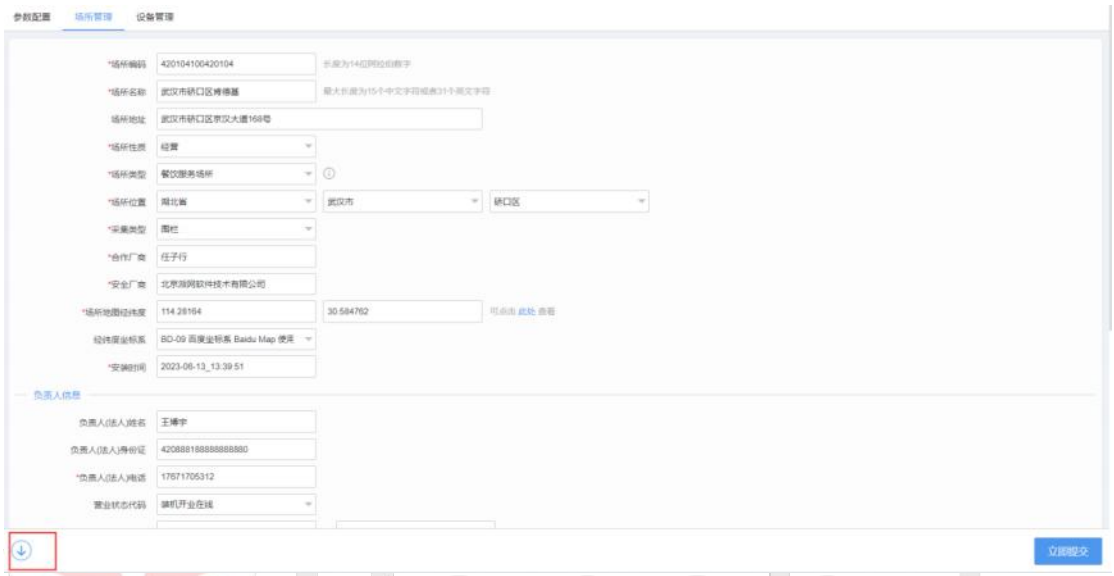
——结束

4.13.4.5. 上报信息至任子行平台

提供信息到任子行平台做接入备案，并验证上报信息是否有效。

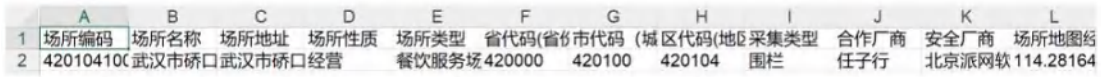
操作步骤

步骤 1 选择【场所管理】，单击，导出场所信息到本地。

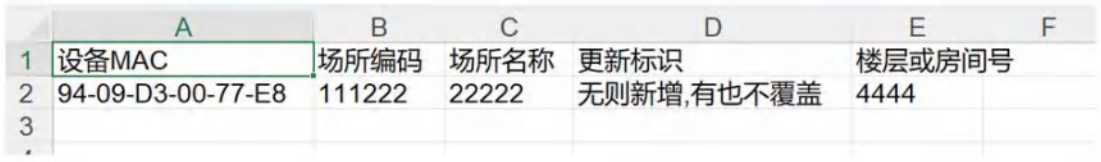


步骤 2 选择【设备管理】，单击【导出】，导出设备信息到本地。

步骤 3 将导出的【场所管理】和【设备管理】的 Excel 表格提供至任子行平台。



	A	B	C	D	E	F	G	H	I	J	K	L
1	场所编码	场所名称	场所地址	场所性质	场所类型	省代码(省份	市代码（城	区代码(地区	采集类型	合作厂商	安全厂商	场所地图经
2	42010410(	武汉市硚口	武汉市硚口	经营	餐饮服务场	420000	420100	420104	围栏	任子行	北京派网软	114.28164



	A	B	C	D	E	F
1	设备MAC	场所编码	场所名称	更新标识	楼层或房间号	
2	94-09-D3-00-77-E8	111222	22222	无则新增,有也不覆盖	4444	
3						

步骤 4 由派网技术人员联系任子行平台技术人员，确认上报数据的有效性。

——结束

5. 系统管理

本章节涵盖对象管理、应用识别、系统告警和系统维护四部分。对象管理可定义其他模块所调用的对象；应用识别可针对系统的 DPI 引擎进行设置；系统告警监控系统状态和流量，提前发现问题并采取措施；系统维护涵盖基础设置，确保上网行为管理的稳定运行。

5.1. 对象管理

本章主要介绍了对象管理模块的各项功能，以及基本的使用与操作配置方法。其中，“对象”表示在配置其他模块时可以调用的部分，例如“用户组/账号”、“文件类型”、“域名群组”、“IP 群组”等。

5.1.1. 账号管理

账号管理用于认证账号的管理，以及 IP 与账号的对应关系管理。

5.1.1.1. 组织架构

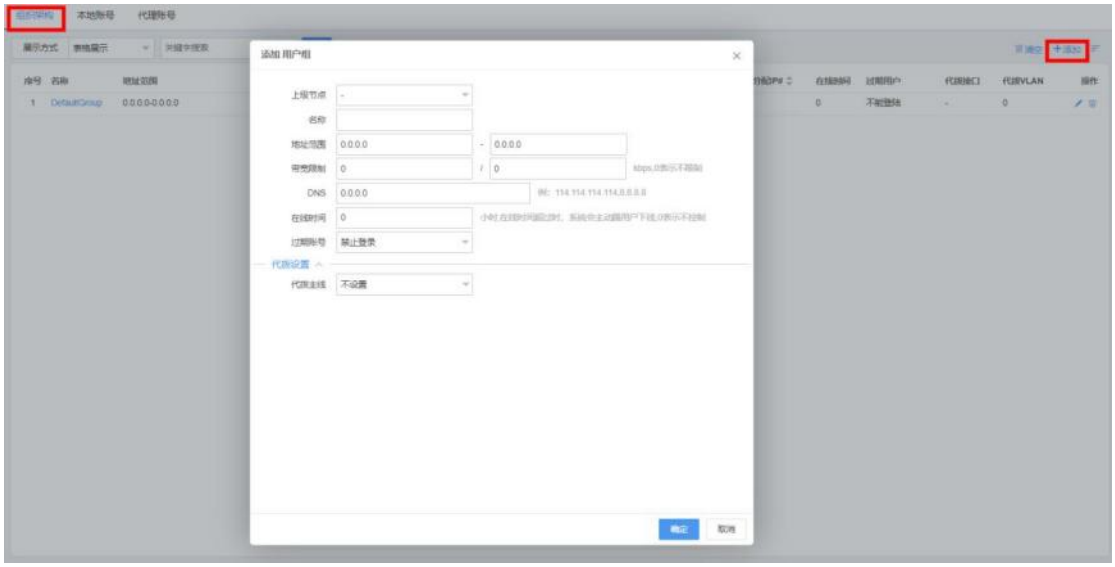
通过此操作，配置用户组，待后续策略调用。策略生效后，添加到群组的用户不再受其他控制策略影响。

操作步骤

步骤 1 选择【对象管理】>【账号管理】>【组织架构】。

步骤 2 点击页面右上角的【添加】。主要设置用户组的“名称”与“地址范围”。

步骤 3 单击【确定】。



参数名称	参数说明
上级节点	标识本用户组的上级组属，默认为空。
名称	定义用户组的名称。
地址范围	该用户组的地址池范围。
带宽限制	单位 kbps，0 表示不限制
DNS	DNS 的 IP，格式为 0.0.0.0。
在线时间	单位小时，在线时间超过时，系统会主动让用户下线，0 表示不控制。
过期账号	可选择“禁止登录”、“允许登录，禁止上网”、“允许登录及上网”。

——结束

5.1.1.2. 本地账号

通过本地账号，选择在地址池中添加本地用户，用于 PPPOE 认证、WEB 认证、iWAN 客户端认证。

操作步骤

步骤 1 选择【对象管理】>【账号管理】>【本地账号】。

步骤 2 单击页面右上角的【添加】，弹出添加本地账号页面。

步骤 3 设置账号信息，单击【确定】。

参数名称	参数说明
用户组	选择一个地址池（用户组）。
账号	自定义账号名称。 取值：不超过 30 个英文字符或者 15 个中文字符。
密码	自定义账号密码。 取值：不超过 30 个英文字符。
开通日期	用户生成时间。
截止日期	用户到期时间。
最大在线	单位小时，在线时间超过时，系统会主动让用户下线，0 表示不控制。
绑定 VLAN	默认不绑定 ，绑定后不仅认证用户名和密码 ，还会认证用户的 VLAN。
绑定 IP	为账号分配地址池内的固定 IP 地址。
绑定 MAC	默认不绑定 ，绑定后不仅认证用户名和密码 ，还会认证用户的 MAC 地址。
身份信息	用户的身份信息，包含姓名、身份证、联系电话等。

——结束

5.1.2. 临时账号

5.1.2.1. 临时账号

该模块账号用于 WEB 认证，在一定时间后账号会被删除 。

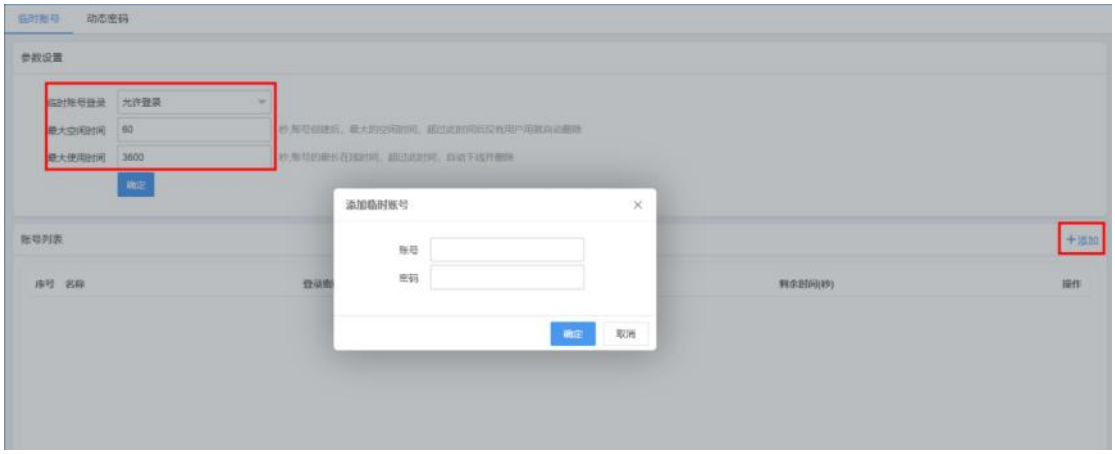


图 5-1 临时账号详情

参数名称	参数说明
临时账号登录	可设置允许登录、禁止登录。
最大空闲时间	账号创建后，最大的空闲时间，超过此时间后没有用户用就自动删除，单位“秒”。
最大使用时间	账号的最长在线时间，超过此时间，自动下线并删除，单位“秒”。
账号	自定义账号名称。
密码	设置账号登录密码。

表 5-1 临时账号参数说明

5.1.2.2. 动态密码

1. 动态密码可以用于网吧等经营场所的 WIFI 防蹭网。
2. 动态密码只能通过 PC 机访问产生，用手机或 iPad 等移动终端无效。
3. 在 PC 机上访问链接 http://192.168.100.100:8010/cgi-bin/webauth/wifitoken 获取动态账号和密码。
4. 本功能需要开启 WEB 认证才可以用，请在应用商店里安装并开启 WEB 认证。

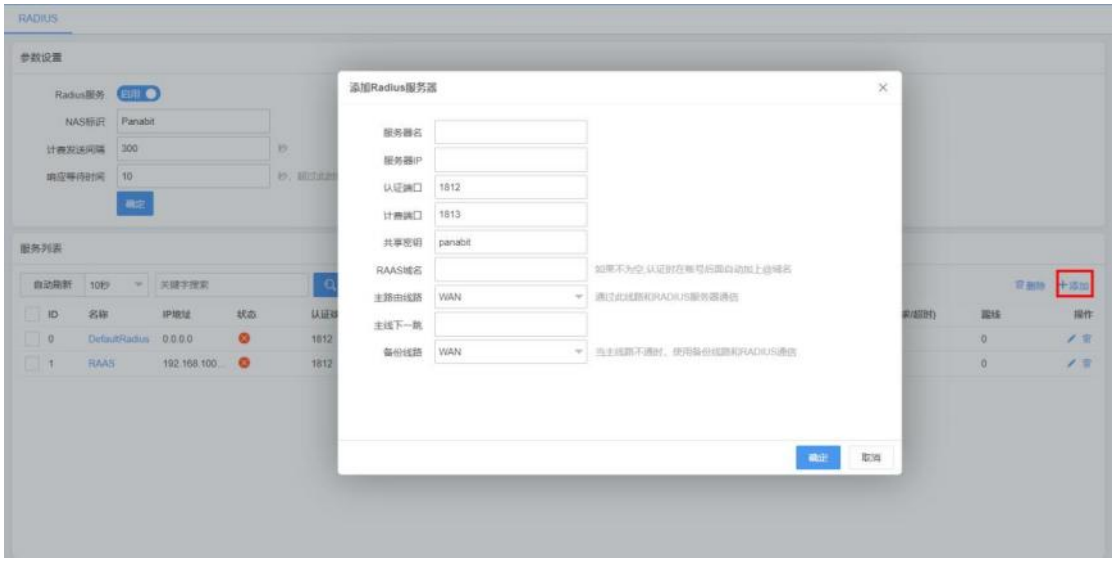
5.1.3. RADIUS

当 Panabit 提供接入服务时，该模块可对接 Panabit RAAS 认证计费系统，或第三方 Radius 软件完成认证与计费。

操作步骤

步骤 1 选择【对象管理】>【RADIUS】。

步骤 2 单击服务列表的【添加】，可新增 Radius 服务器。



参数名称	参数说明
Radius 服务	控制 Radius 服务的开关，默认不启用，选择启用后可以与第三方 Radius 对接。
NAS 标识	与 Radius 通讯时所带的标识，Radius 可以通过这个标识识别数据是否合法。
计算发送间隔	向 Radius 服务器发送计费包的时间间隔。
响应等待时间	向 Radius 服务器发送认证或者计费包后，在设定时间内没有回应，即认为超时，超过此时间的 Radius 应答将被丢弃。
服务器名	定义 Radius 服务的名称。
服务器 IP	第三方 Radius 服务器的 IP。
认证端口	发送认证数据报文的端口，默认 1812。
计费端口	发送计费数据报文的端口，默认 1813。
共享密钥	用于验证 Radius 报文合法性，与 Radius 服务器相应的设置一致
RAAS 域名	与派网 RAAS 产品对接时使用。
主路由线路	发送认证与计费报文的逻辑接口，逻辑接口必须与 Radius 服务器 IP 能够互相通讯。
主线下一跳	当 Radius 服务器在内网，使用 LAN 口与内网 Radius 服务器对接，并且跨路由访问时填写。
备份线路	当主路由线路断开时，使用备份线路与 Radius 服务器进行通讯。

说明

在配置 WEB 认证时，认证方式选择“Radius 认证”，即可调用 Radius。具体操作请参见 WEB 认证。

5.1.4. 文件类型

文件类型用于自定义 URL 中的文件名后缀，在【HTTP 管控】时可以调用文件类型。

操作步骤

步骤 1 选择【对象管理】>【文件类型】。

步骤 2 单击页面右上方【添加】，添加文件类型。

步骤 3 单击【确定】。

参数说明	参数名称
群组名称	自定义群组名称。
文件类型列表	如 zip,txt,rar 等，多个类型用逗号隔开。

——结束

5.1.5. 域名群组

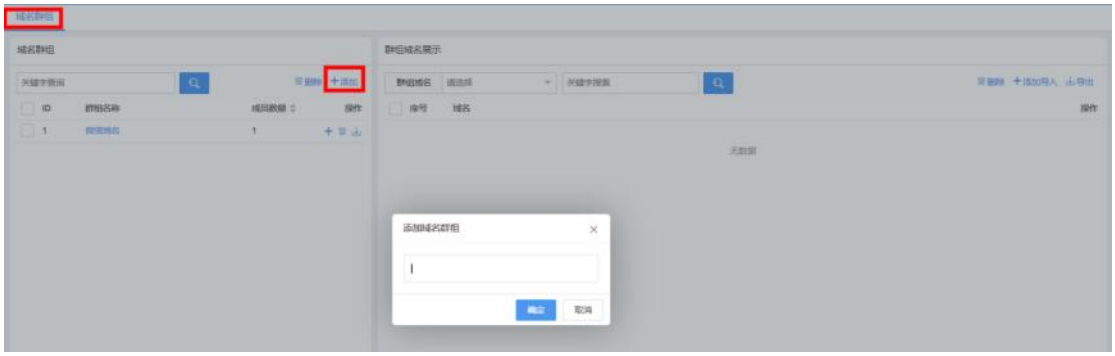
域名群组以域名为维度，对域名进行归类，方便策略调用。在【HTTP 管控】与【DNS 管控】中可以调用域名群组。

操作步骤

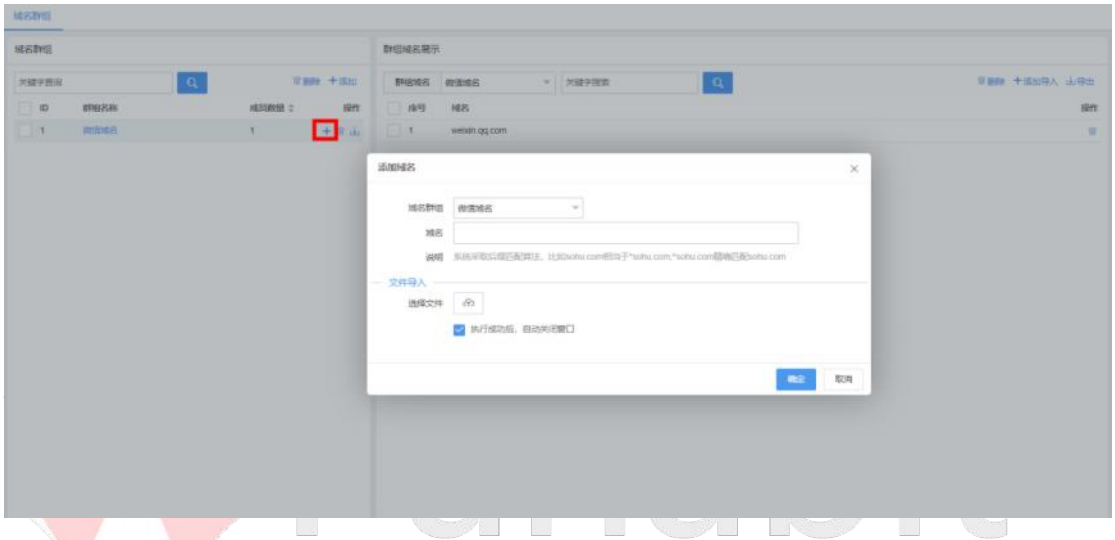
步骤 1 选择【对象管理】>【域名群组】。

步骤 2 单击【添加】，弹出添加域名群组页面。

步骤 3 输入域名，单击【确定】。



步骤 4 单击当前域名操作列的 ，选择域名群组，添加域名。



步骤 5 单击【确定】。

说明

系统采用后缀匹配算法，比如添加的域名是“sohu.com”，那么 www.sohu.com、news.sohu.com、www.woaisohu.com 等都会匹配到。

——结束

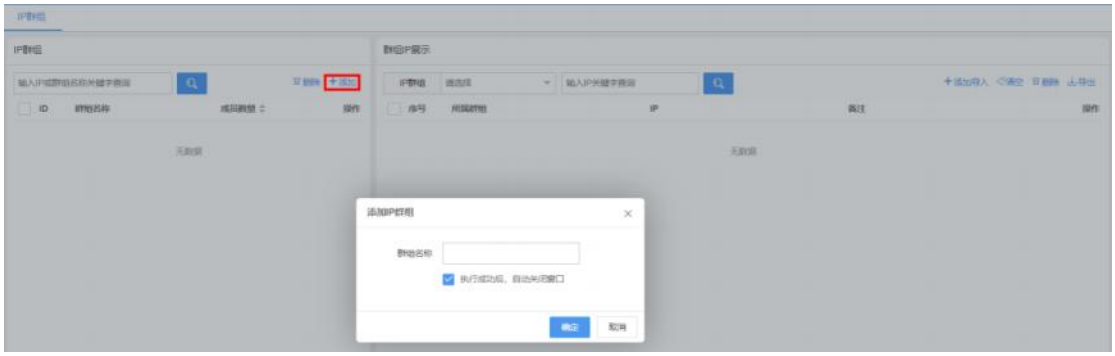
5.1.6. IP 群组

该模块以 IP 为维度，可以将 IP 地址进行归类，方便策略调用。凡是有 IP 条件的策略，都可以调用 IP 群组。

操作步骤

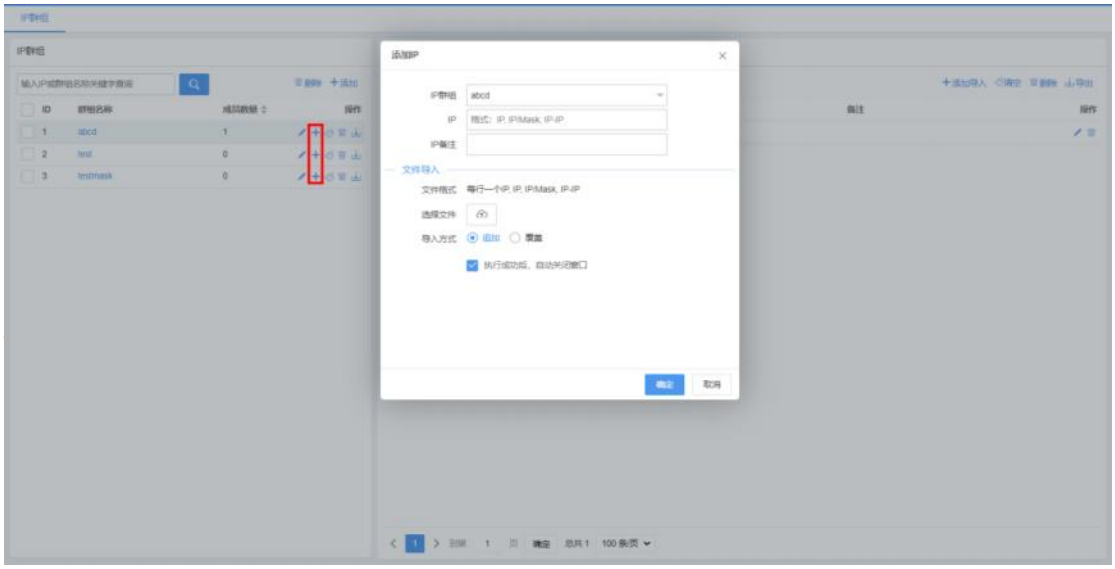
步骤 1 选择【对象管理】>【IP 群组】。

步骤 2 单击【添加】，弹出添加 IP 群组页面。



步骤 3 单击【确定】。

步骤 4 单击 IP 群组操作列的 + 或【群组 IP 展示】>【添加导入】，弹出添加 IP 页面。



步骤 5 输入或导入 IP，单击【确定】。

说明

添加 IP 时可单个添加，也可批量导入。

当需要添加多个 IP 时，不同 IP 之间用逗号隔开。

——结束

5.1.7. 白名单 IP

选择一个 IP 群组作为白名单后，不在群组内的 IP 都为非法 IP。

5.1.7.1. 参数设置

参数设置主要用于设置白名单 IP 群组，并对群组内的 IP 进行添加、删除、导入、导出等

操作。

步骤 1 选择【对象管理】>【白名单 IP】。

步骤 2 选择页面上方的【参数设置】。

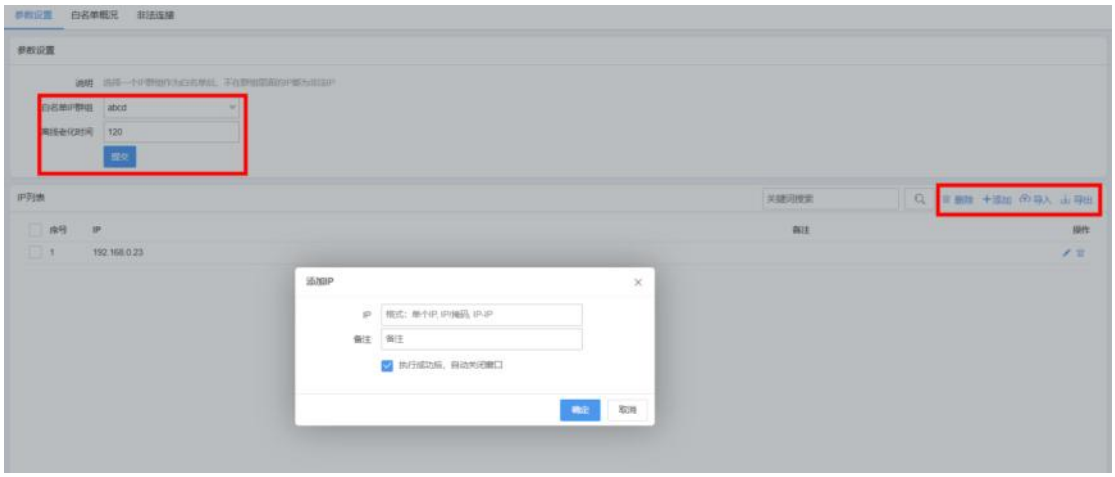


图 5-2 参数设置详情

参数名称	参数说明
白名单 IP 群组	选择某个 IP 群组，将其设置为白名单。
离线老化时间	对没有流量的空闲 IP 设置离线时间，单位：秒。
添加	单击 +，添加白名单，格式为“单个 IP”、“IP/掩码”、“IP-IP”。
删除	删除选中的 IP。
导入	手动导入白名单 IP 文件。
导出	将配置好的白名单 IP 导出至本地。

表 5-2 参数设置参数说明

5.1.7.2. 白名单概况

白名单概况主要展示白名单内的合法 IP 数、非法 IP 数、合法 IP 在线趋势以及合法/非法 IP 的连接数、在线时间等。

步骤 1 选择【对象管理】>【白名单 IP】。

步骤 2 选择页面上方的【白名单概况】。

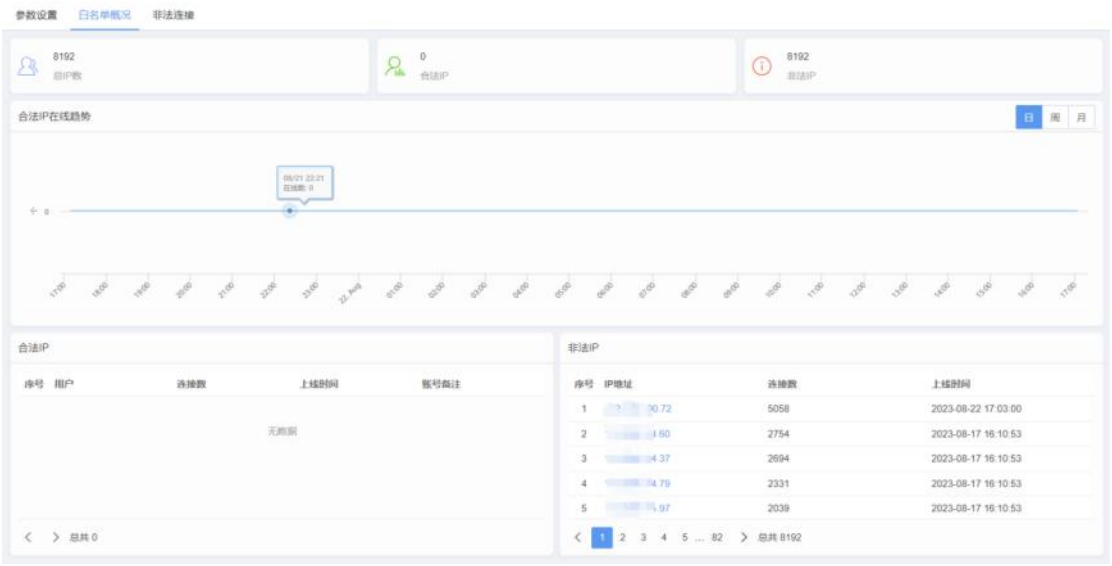


图 5-3 白名单概况详情

参数名称	参数说明
合法 IP 在线趋势	展示合法 IP 日/周/月的在线趋势。
合法 IP	展示合法 IP 的连接数、上线时间及账号备注。
非法 IP	展示非法 IP 的 IP 地址、连接数、上线时间。

表 5-3 白名单概况参数说明

5.1.7.3. 非法连接

非法连接主要展示非法 IP 的源 MAC、源/目标 IP、协议等信息。

步骤 1 选择【对象管理】>【白名单 IP】。

步骤 2 选择页面上方的【非法连接】。

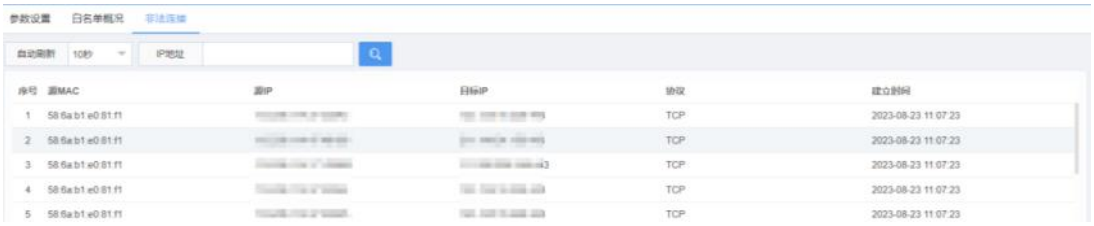


图 5-4 非法连接详情

参数名称	参数说明
自动刷新	非法连接详情的刷新频率，可选择不刷新或以 5s/10s/20s/60s 为周期刷新。
IP 地址	输入需要查询的 IP 地址进行搜索。

源 MAC	会话源 MAC。
源 IP	会话源 IP。
目标 IP	会话源目标 IP。
协议	会话涉及的协议。
建立时间	会话建立的时间。

表 5-4 非法连接参数说明

5.1.8. IP/MAC 备注

IP/MAC 备注可以将 IP 或者 MAC 与用户名关联，关联后可以在在线用户中显示。

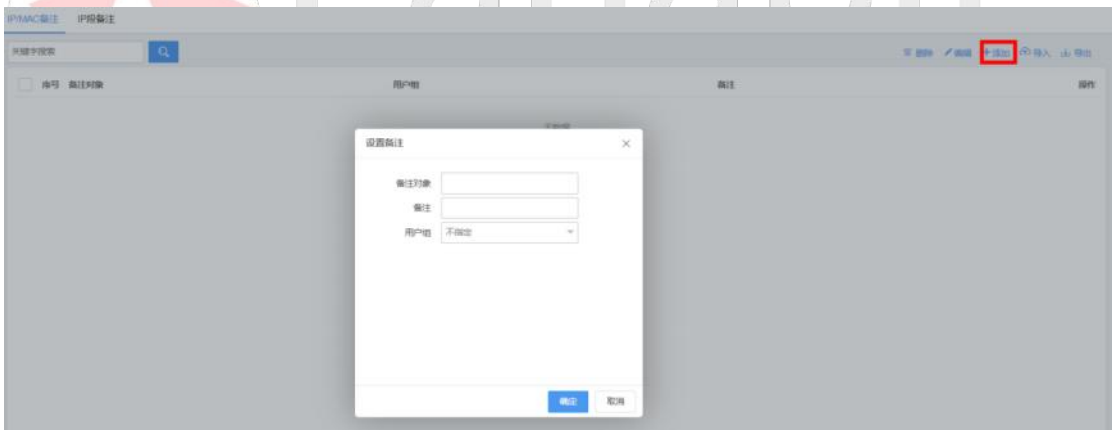
5.1.8.1. IP/MAC 备注

操作步骤

步骤 1 选择【对象管理】>【IP/MAC 备注】。

步骤 2 手动添加用户备注。

1. 单击页面右上方【添加】，进行用户备注。



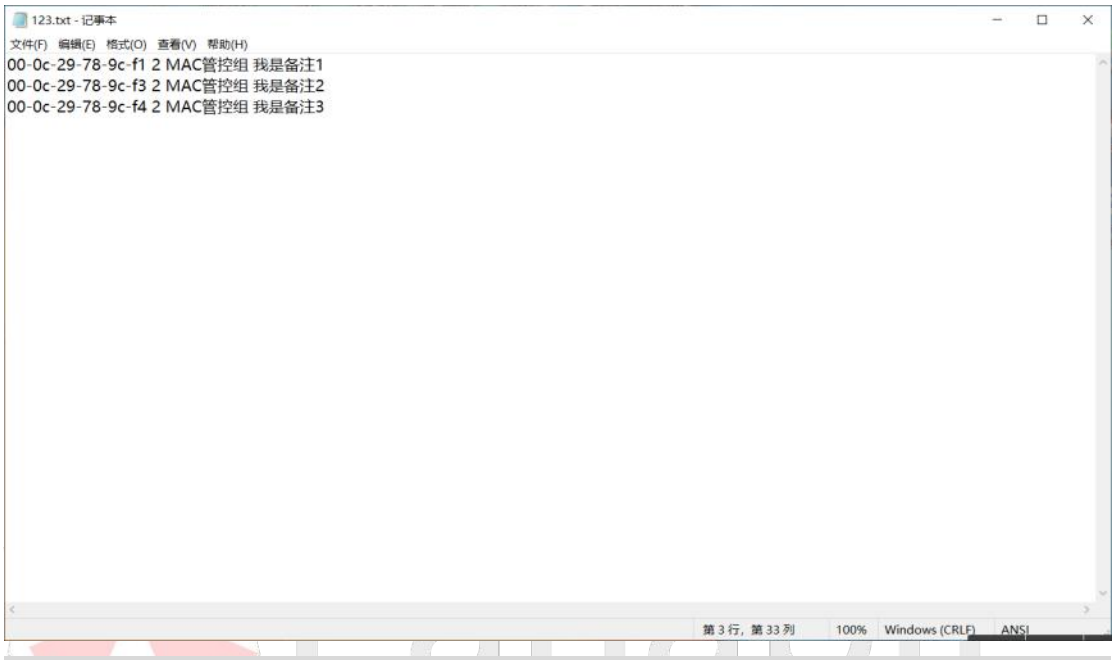
参数名称	参数说明
添加	添加备注信息。 ● 备注对象：输入需要备注的 IP/MAC。 ● 备注：输入备注信息。 ● 用户组：将备注对象加入已创建的组。
导入	批量导入备注信息。
导出	批量导出备注信息。

删除	单个/批量删除备注信息。

2. 单击【确定】。

步骤 3 文本导入添加用户备注。

1. 创建 txt 文档，中文编码中文参数必须为 GB2312 编码。格式为：[MAC/IP] [用户组 ID] [用户组名称] [备注内容]。



说明

每一个 MAC 对象单独为一行，用户组 ID 为组织架构中创建组时的序号，txt 文档格式也可选择编码格式为 ANSI。

2. 单击页面右上方【导入】，导入文件进行用户备注。

3. 单击【确定】，在备注对象列表，查看导入结果。

——结束

5.1.8.2. IP 段备注

查询数据，IP 地理位置信息时，会匹配系统地址库，以及自定义的 IP 备注。

步骤 1 选择【对象管理】>【IP/MAC 备注】。

步骤 2 选择页面上方【IP 段备注】。

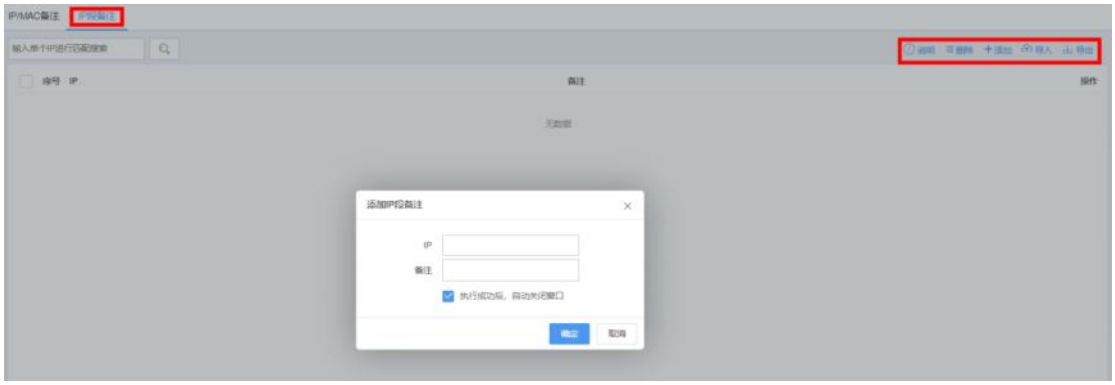


图 5-5 IP 段备注详情

参数名称	参数说明
删除	单个/批量删除备注信息。
添加	单个/批量添加备注信息。 ● IP：输入需要进行备注的 IP。 ● 备注：输入当前 IP 的备注信息。
导入	批量导入备注信息。
导出	批量导出备注信息。

表 5-5 IP 段备注参数说明

5.2. 应用识别

本章主要介绍了应用识别模块的各项功能，以及基本的使用与操作配置方法。在该模块中，您可以对 Panabit 上网行为管理识别的应用协议进行搜索查询，并对应用识别的一些配置进行编辑。

5.2.1. 引擎参数

通过该模块能够设置应用识别 DPI 引擎的相关参数，增加合法 IP 并设置 IP 备注。

5.2.1.1. 引擎参数

通过引擎参数能够设置应用识别引擎部分功能。

步骤 1 选择【应用识别】>【引擎参数】。

步骤 2 选择页面上方【引擎参数】。

图 5-6 引擎参数详情

参数名称	参数说明
IPv6 流量识别	可选择“开启”或“关闭”。 未开启时，所有 IPv6 的流量均会被 DPI 引擎匹配识别为【IPv6】这个特征标签。开启后能够对 IPv6 的流量进行深度识别，IPv6 的流量将被 DPI 引擎匹配识别为特征库的各个特征标签。开启后 IPv6 的路由配置才会生效。
NPM 时延分析	可选择“开启”或“关闭”。 开启后，能够对每一条会话的客户时延、服务时延、应用时延等进行分析。
GRE 隧道分析	可选择“开启”或“关闭”。
智能 P2P 识别	可选择“开启”或“关闭”。当流量不完整或网络内 P2P 加密流量较多时，开启智能 P2P 识别引擎能提升识别率，但是会消耗更多资源。
迅雷增强识别	可选择“开启”或“关闭”。开启迅雷增强识别引擎可以更好地识别迅雷的加密流量。
WWW 加强代理	可选择“开启”或“关闭”。单独分流 WWW 协议时，需要开启此选项。
伪 IP 防护功能	可选择“开启”或“关闭”。启用伪 IP 防护后，请填写“合法 IP 列表”，不在列表里的 IP 的流量识别成“内网 IP 伪装”。 伪 IP 防护设置，主要用于在旁路部署时，通过设置内网合法 IP，区分哪些是内网 IP、哪些是外网 IP。

表 5-6 引擎参数说明

5.2.1.2. 合法 IP 列表

合法 IP 主要用于添加或导入新的合法 IP，并能对已有的 IP 进行删除、导出操作。

步骤 1 选择【应用识别】>【引擎参数】。

步骤 2 选择页面上方【合法 IP 列表】。

图 5-7 合法 IP 列表详情

参数名称	参数说明
删除	单个/批量删除列表中的 IP。
添加	添加合法 IP。 ● IP：输入添加的 IP。 ● 备注：输入当前 IP 的备注信息。
导入	批量导入合法 IP 列表，导入方式可选择“追加”或“覆盖”。 
导出	将列表中的 IP 导出到本地。

表 5-7 合法 IP 列表参数说明

须知

一般情况下，该功能仅在旁路部署时启用。

5.2.2. 应用协议

应用协议呈现了上网行为管理的应用特征库列表，展示了当前已有协议库概览、流量、连接趋势，并支持对具体协议进行配置。

步骤 1 选择【应用识别】>【应用协议】。

步骤 2 选择页面左侧的应用协议树。

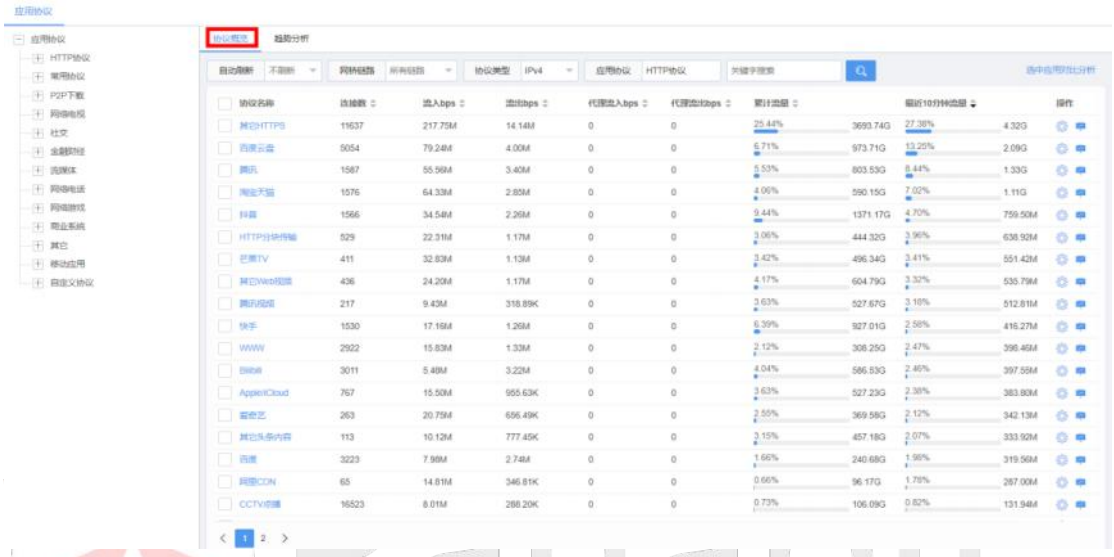


图 5-8 应用协议概览详情

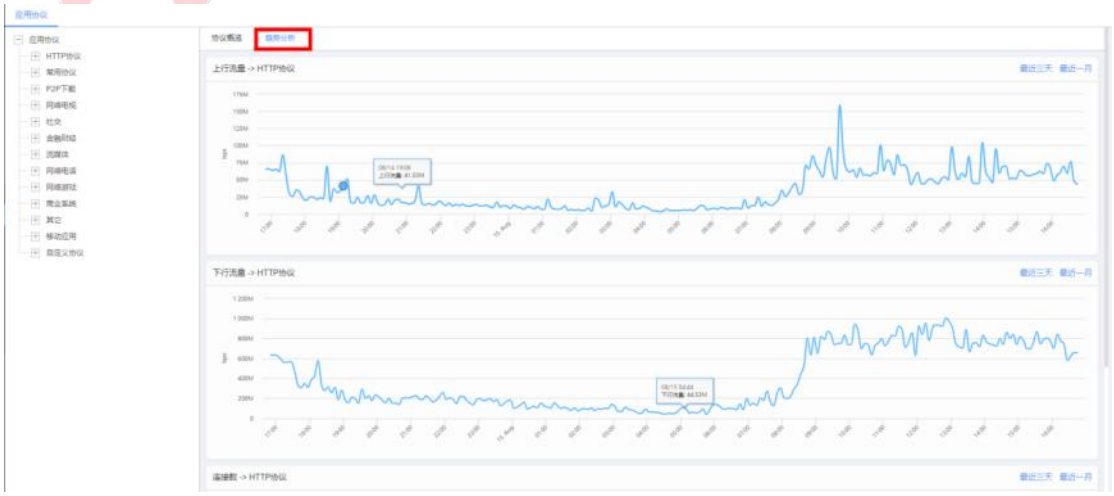


图 5-9 应用协议趋势分析详情

参数名称	参数名称
协议概览	某种协议分类下的所有应用，可查看其连接数及流量详情。
趋势分析	展示某种协议类型最近 24 小时/最近三天/最近一周/最近一月的下/行流量、连接数趋势。

表 5-8 应用协议参数说明

单击某个具体协议名称或操作列的⚙，可以查看协议档案。

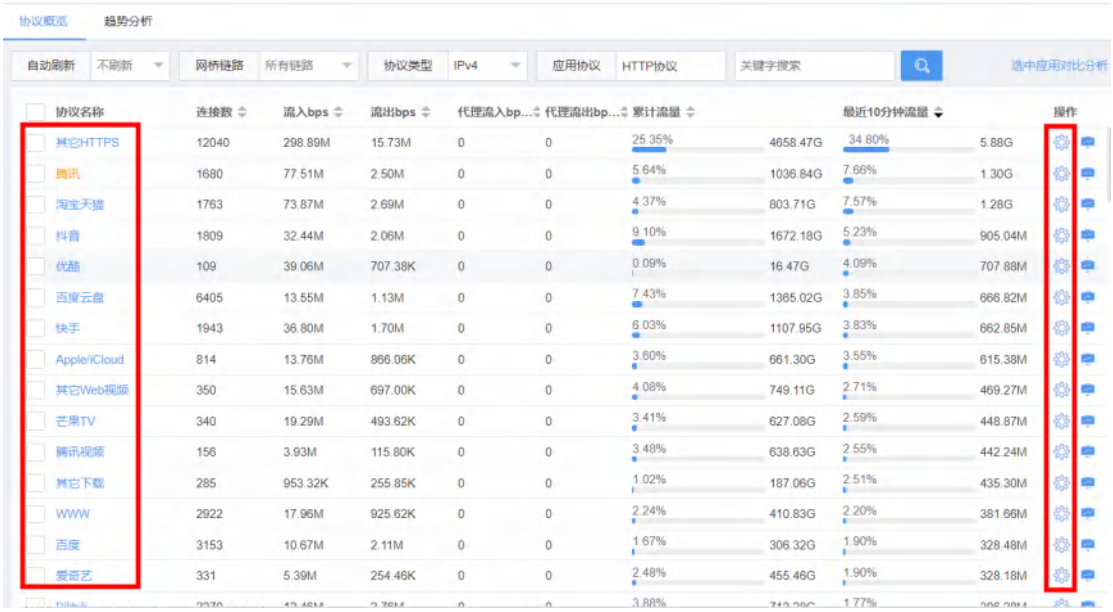
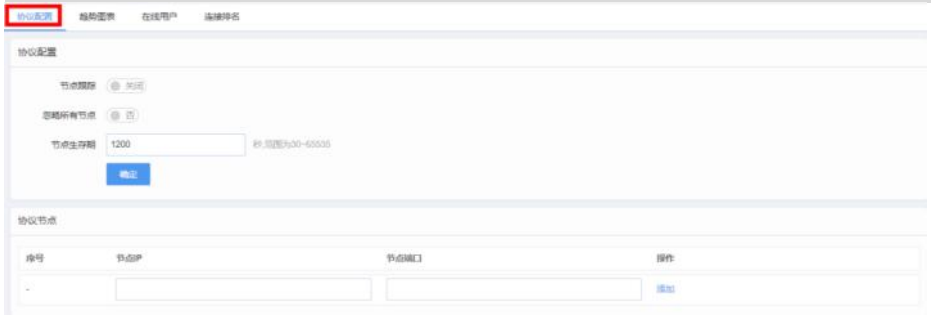


图 5-10 协议档案详情

参数名称	参数说明
协议配置	可配置该协议的节点参数，添加 IP+端口特征。 **说明** IP+端口指的是目标 IP+目标端口。当会话的目标 IP+目标端口被命中，就会被识别成对应的协议。  ● 节点跟踪：每个协议都有节点跟踪的选项，当节点跟踪选项开启时，数据包匹配过特征库后就会将目的 IP 记录到节点，这样可以大大地提高识别效率。 ● 节点生存期：每个节点被记录后不是永久存在的，当节点在一定的时间段内没有被访问，系统就会把这个节点删除掉，节点生存期就是控制这个时间。 ● 忽略节点：该选项默认关闭，当开启后，该应用下的节点不会被使用。

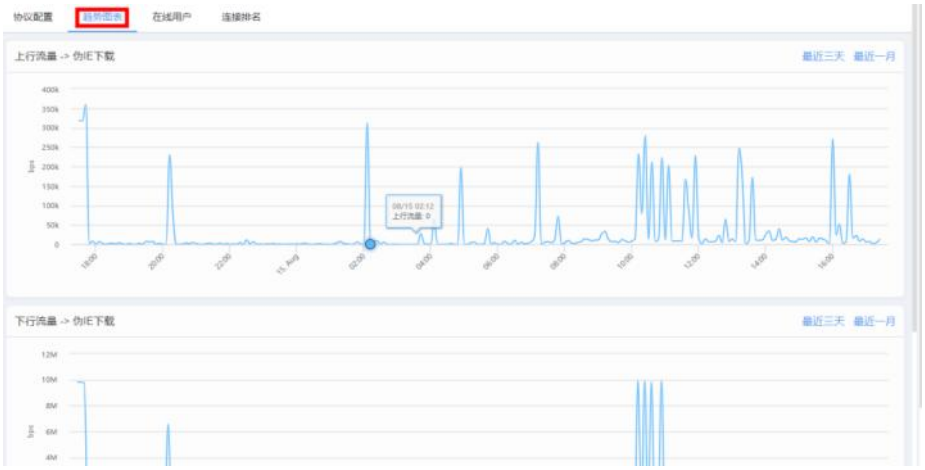
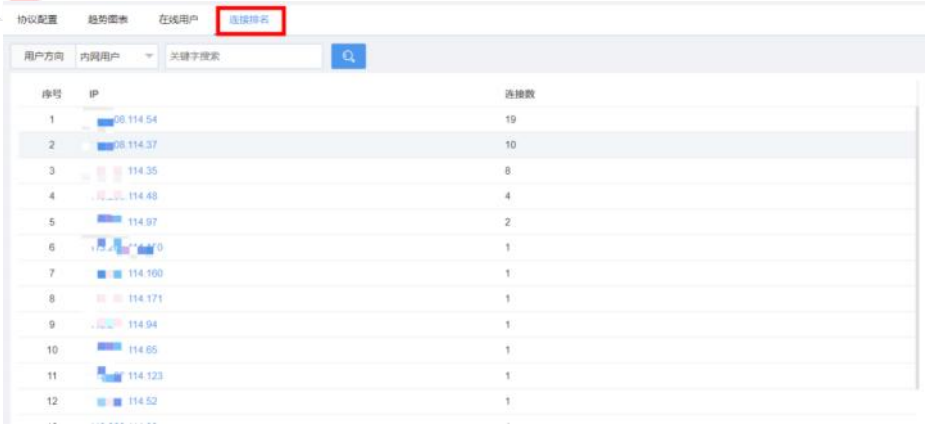
	● 协议节点：可以自行添加 IP+端口，作为应用的节点。
趋势图表	展示当前协议的上/下行流量及连接数趋势。 
在线用户	展示当前协议在线用户的 IP、账号及流量速率。 
连接排名	展示当前协议所有 IP 的连接次数排名。 

表 5-9 协议档案参数说明

5.2.3. 节点管理

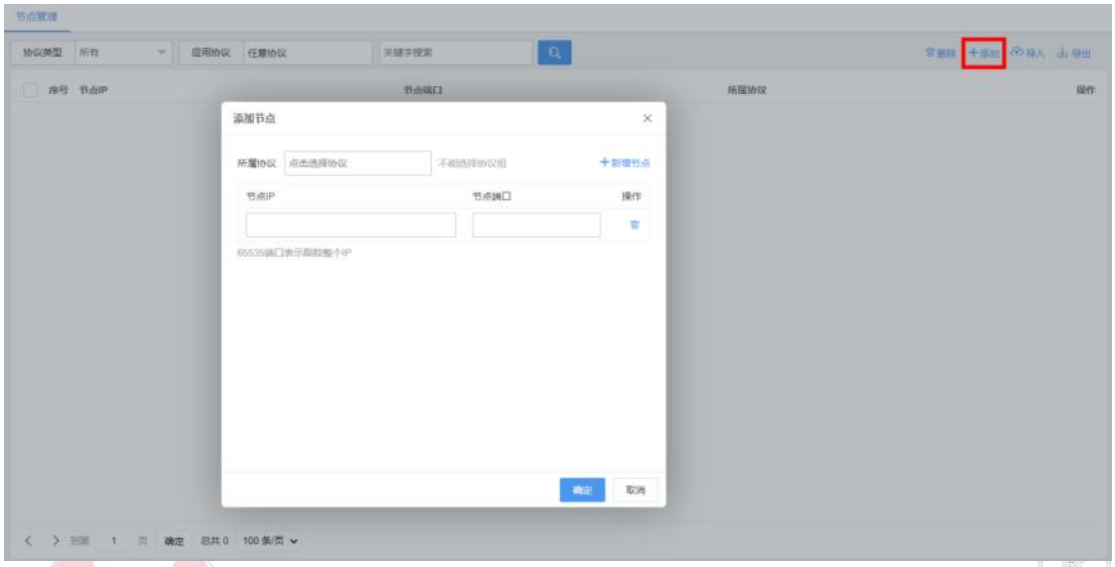
通过节点管理，可添加 IP+端口特征。这里的 IP+端口指的是目标 IP+目标端口。当会话的目标 IP+目标端口被命中，就会被识别成对应的协议。

操作步骤

步骤 1 选择【应用识别】>【节点管理】。

步骤 2 单击页面右上方【添加】，添加节点。

步骤 3 单击选择或搜索对应协议，输入节点 IP 及端口，单击【确定】。



步骤 4 当节点较多时，单击【导入】，批量增加节点。

——结束

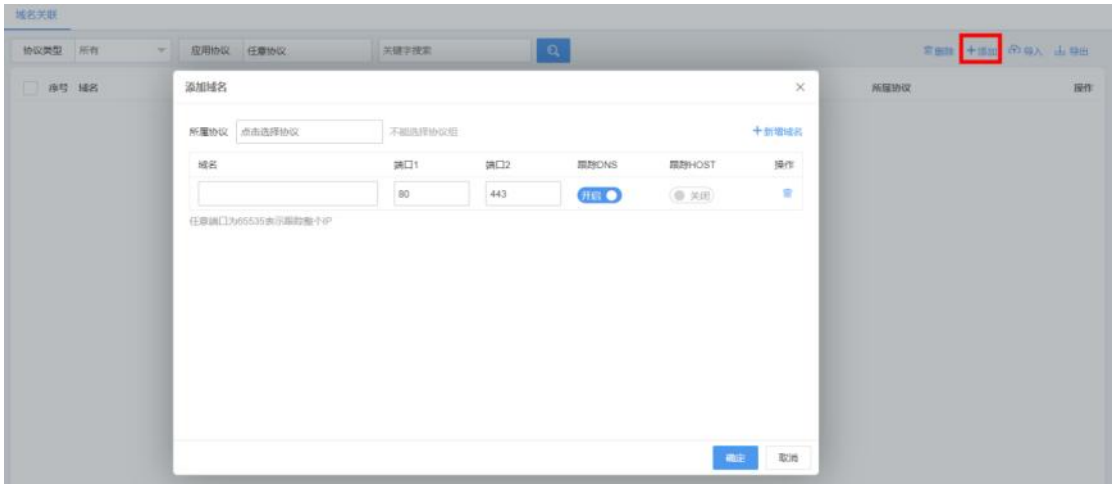
5.2.4. 域名关联

通过域名关联，可添加域名特征。域名特征的原理是将域名与 IP 做关联。“跟踪 DNS”和“跟踪 HOST”就是获取会话中域名与 IP 对应关系的手段。因此在添加域名特征时，建议“跟踪 DNS”和“跟踪 HOST”都选择“开启”。当会话中的域名命中了域名特征，就会被识别成对应的协议。

操作步骤

步骤 1 选择【应用识别】>【域名关联】。

步骤 2 单击页面右上角【添加】，添加域名。



步骤 3 单击选择或搜索所属协议，输入域名、端口。

步骤 4 （可选）开启“跟踪 DNS”、“跟踪 HOST”。

步骤 5 单击【确定】。

步骤 6 当需要添加的域名较多时，可单击【导入】，批量添加域名特性。

——结束

5.2.5. 自定义协议

在该模块中，可以添加自定义协议，每个自定义协议可以添加自定义特征。自定义协议能够作为系统特征库的补充。

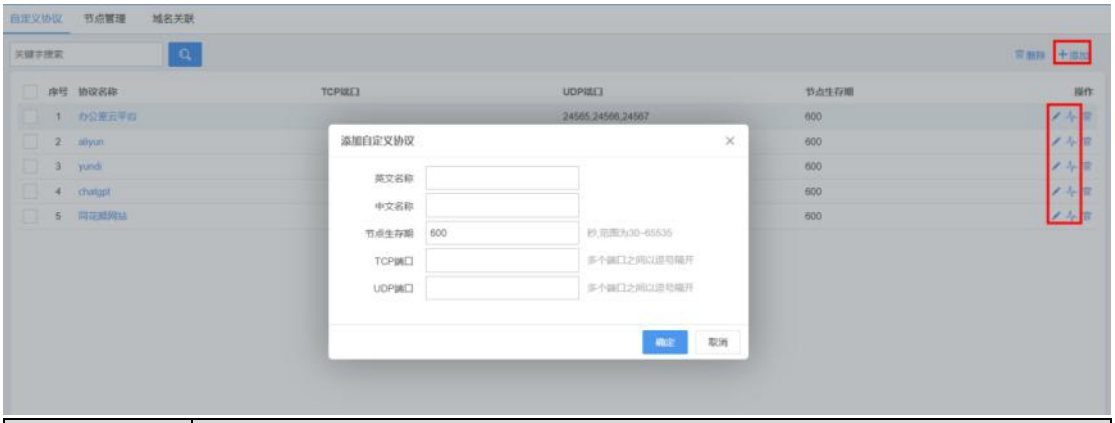
自定义特征分为三类：端口特征，IP+端口特征，域名特征。每个自定义协议可以同时添加这三种特征，会话命中其中任何一种特征，就会被识别为该自定义协议。

5.2.5.1. 添加端口特征

操作步骤

步骤 1 选择【应用识别】>【自定义协议】>【自定义协议】。

步骤 2 单击【添加】，弹出添加自定义协议页面。

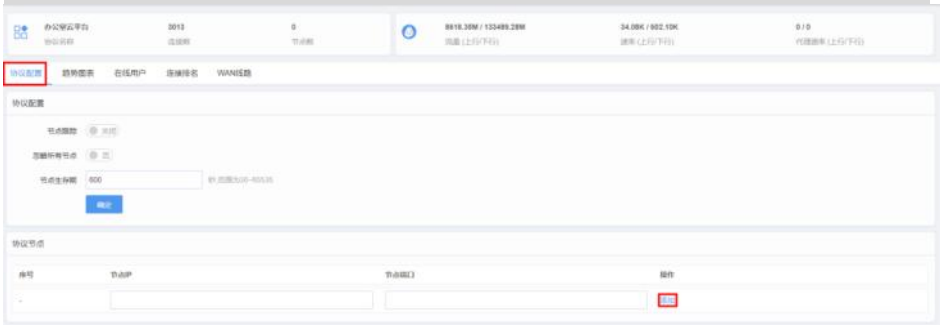
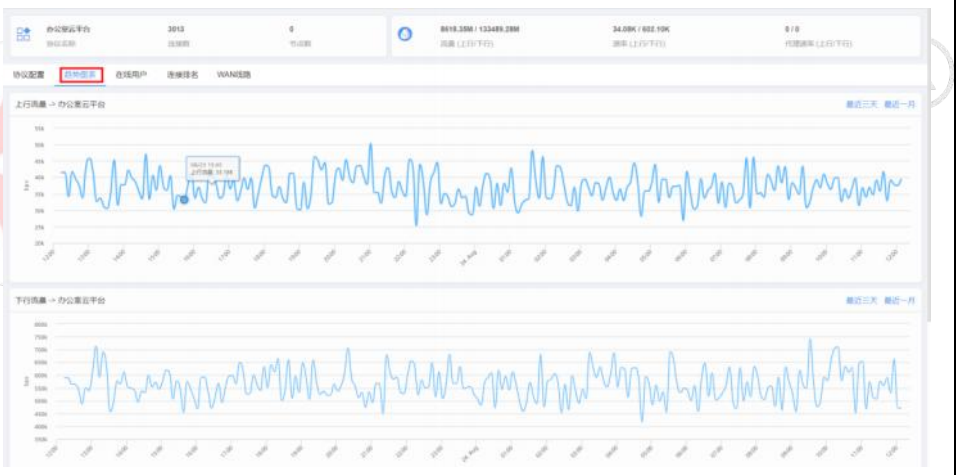
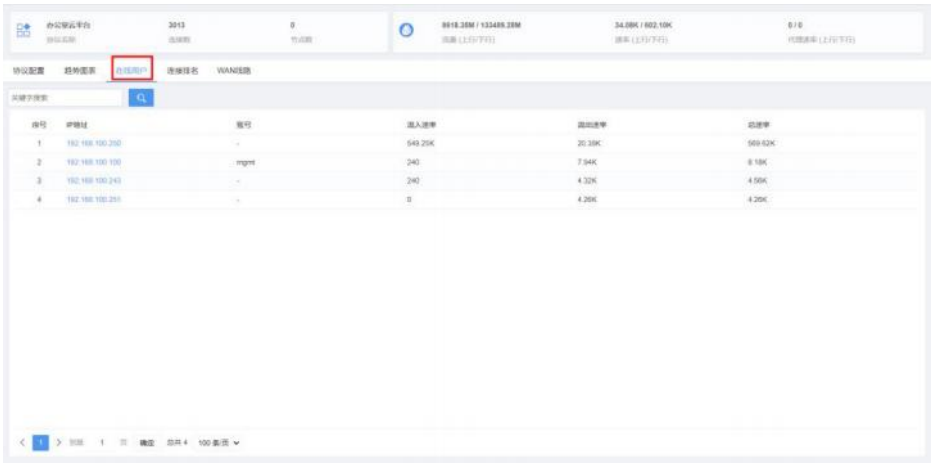


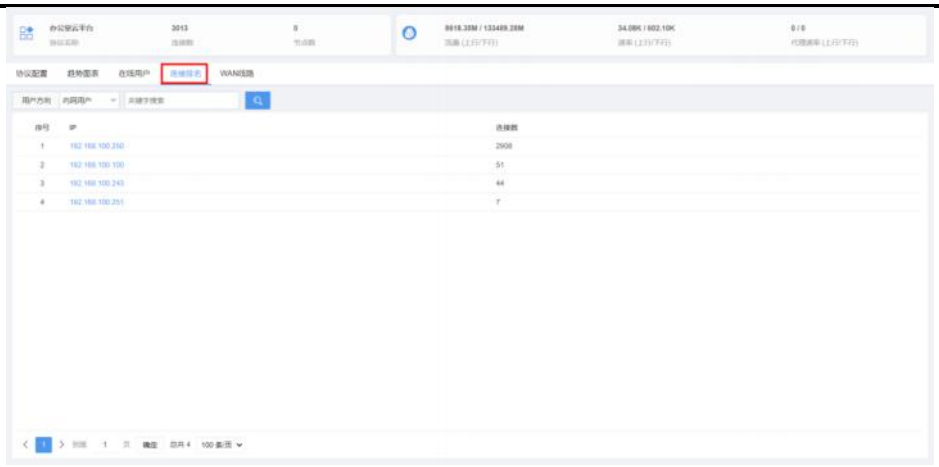
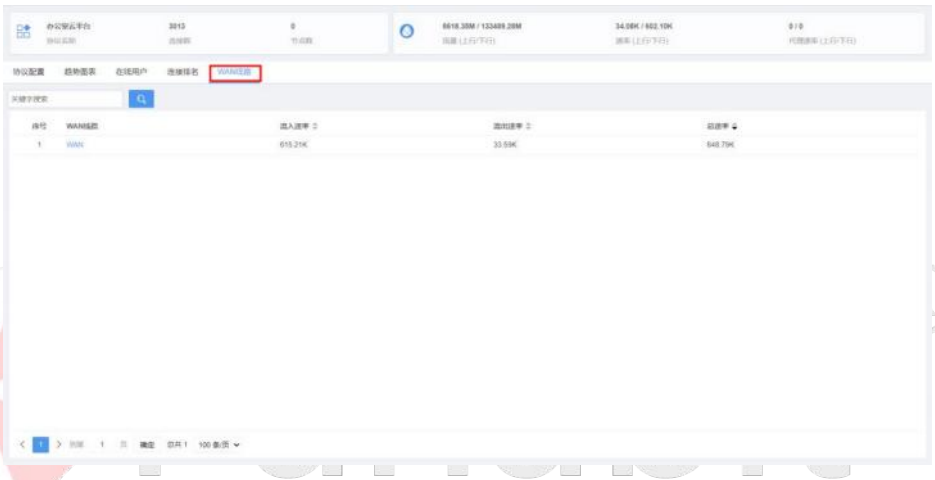
参数名称	参数说明
英文名称	自定义协议的英文名称。
中文名称	自定义协议的中文名称。
节点生存期	控制节点生效的时间长度。 单位：秒，取值：30~65535。 **说明** 数据包匹配该协议后，系统会将目的 IP 记录到节点，当节点在一定的时间段内没有被访问，系统就会把这个节点删除掉。
TCP 端口	为 TCP 协议通信提供服务的端口。 取值：0~65535，多个端口之间以逗号隔开。
UDP 端口	为 UDP 协议通信提供服务的端口。 取值：多个端口之间以逗号隔开。

步骤 3 配置自定义协议，单击【确定】。

步骤 4 单击协议名称或操作列的，可对当前协议进行编辑。

步骤 5 单击操作列的，可查看协议档案。

参数名称	参数说明
协议配置	可配置该协议的节点参数，添加 IP+端口特征。 **说明** IP+端口指的是目标 IP+目标端口。当会话的目标 IP+目标端口被命中，就会被识别成对应的协议。 
趋势图表	展示当前协议的上/下行流量及连接数趋势。 
在线用户	展示当前协议在线用户的 IP、账号及流量速率。 
连接排名	展示当前协议所有 IP 的连接次数排名。

	
WAN 线路	展示当前协议已有的 WAN 线路。 

——结束

5.2.5.2. 添加 IP+端口特征

进入【应用识别】>【自定义协议】>【节点管理】，根据数据包的目标 IP+端口进行识别，在“所属协议”处，可以选择我们之前创建的自定义协议进行目标 IP 及端口来定义识别协议，也可以选择对系统自带特征库名称进行 IP 端口的协议补充。详细操作请参考节点管理。

5.2.5.3. 添加域名特征

进入【应用识别】>【自定义协议】>【域名关联】，添加域名特征，可以选中我们之前创建的自定义协议，通过域名特征来定义识别协议，也可以选择对系统自带特征库进行补充。域名特征的匹配逻辑是后缀匹配，详细操作请参考域名关联。

说明

- 节点管理端口填写 65535 表示跟踪整个 IP。
- 域名关联端口填写 65535 表示跟踪所有端口。
- 需通过命令“floweye dpi config gametrack_enable=1”开启识别。

5.2.6. 自定义协议组

通过此操作，可以将系统所有特征库中的应用协议（包括自定义协议）重新进行自定义分组。协议组是应用协议的集合，其中可以添加特征库自带的应用协议或自定义协议。

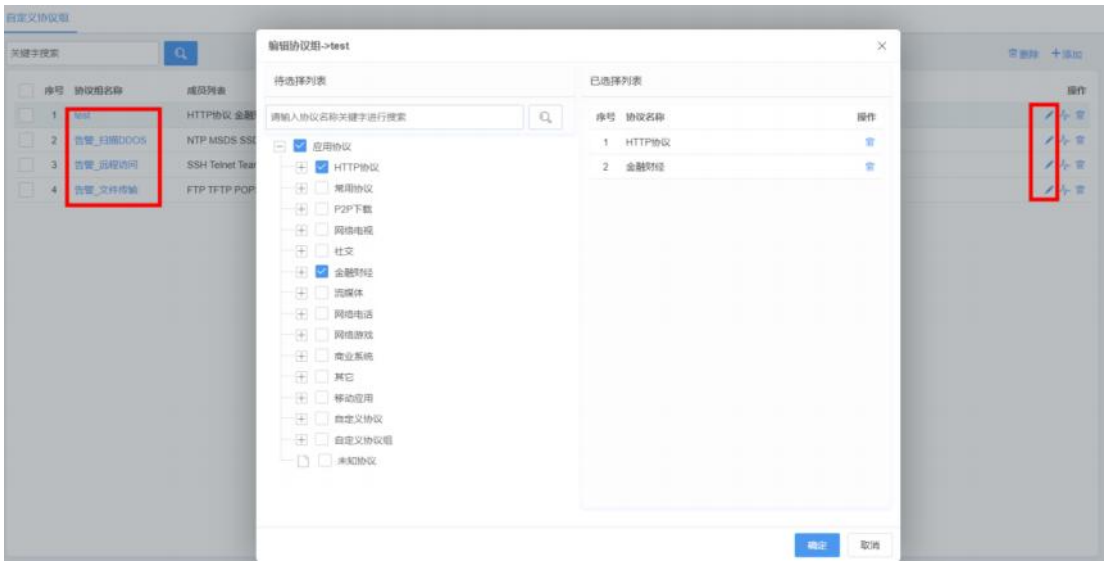
操作步骤

步骤 1 选择【应用识别】>【自定义协议组】。

步骤 2 单击【添加】，添加自定义协议组。

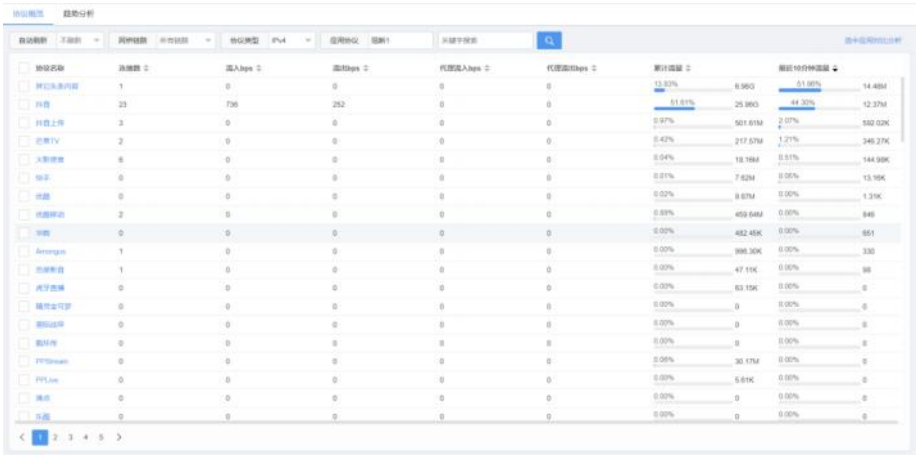
步骤 3 输入协议组中文名和英文名，单击【确定】。

步骤 4 单击协议组名称或操作列的  ，进入协议列表，添加协议组成员。



步骤 5 单击【确定】。

步骤 6 单击操作列的，可查看自定义协议组档案。

参数名称	参数说明
协议概览	某种协议分类下的所有应用，可查看其连接数及流量详情。 
趋势分析	展示某种协议类型最近 24 小时/最近三天/最近一周/最近一月的下/行流量、连接数趋势。 

——结束

5.2.7. 协议搜索定位

在该模块中，可通过关键字搜索，查找某个应用协议所在的位置。

步骤 1 选择【应用识别】>【协议搜索定位】。

图 5-11 协议搜索定位详情

5.3. 系统告警

本节主要介绍了系统告警模块的各项功能，以及典型场景下的配置实例。

系统告警模块监控系统的核心指标、性能数据以及流量情况，及时识别潜在的风险和异常。通过设置智能的告警规则，您可以在问题发生时及时得到通知，从而能够迅速采取措施来防止系统中断或性能下降。

5.3.1. 告警策略

Panabit 上网行为管理的告警功能建立在策略的基础上，用户可以自定义策略，指定需要告警监控的对象。监控的对象可以是上网行为管理系统本身，也可以针对内网 IP、应用协议以及威胁情报进行监控。

步骤 1 选择【系统告警】>【告警策略】。

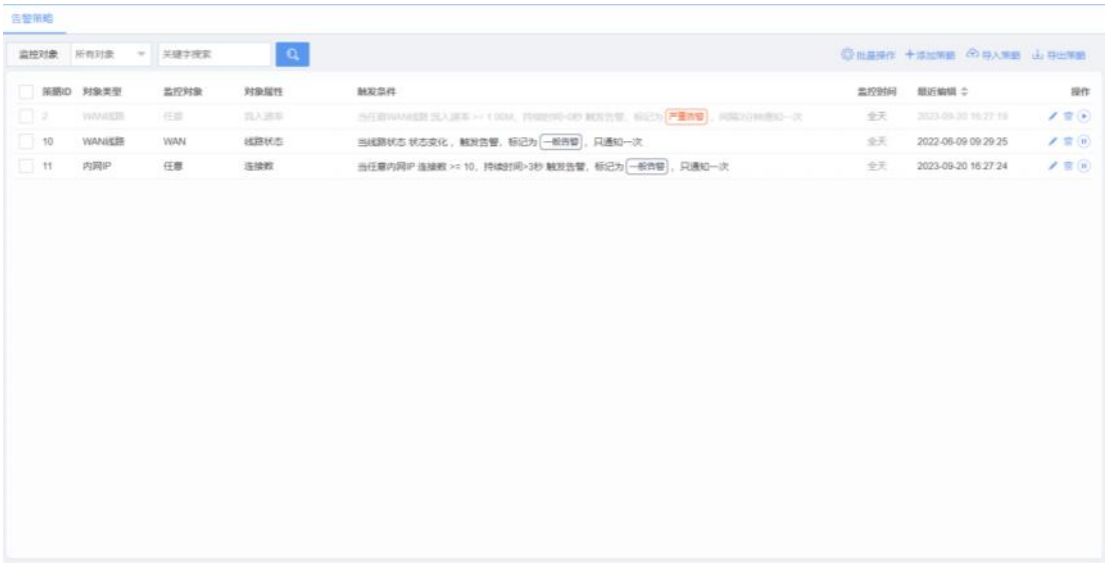


图 5-12 告警策略详情

参数名称	参数说明
监控对象	根据监控对象筛选告警策略，监控对象包括：系统、网卡、WAN 线路、内网 IP、应用协议、流量统计对象。
关键字搜索	可根据配置策略的关键字搜索相应告警策略。
批量操作	针对选中的策略，进行批量禁用、启用、删除操作。
添加策略	添加一条新的策略。
恢复默认策略	点击后，恢复至系统默认的策略。
导入策略	手动导入策略文件。
导出策略	将配置好的策略导出至本地。

表 5-10 告警策略参数说明

每一条告警策略，均由以下要素组成：

图 5-13 添加告警策略

1. **策略 ID**：策略的编号，系统将按照编号从小到大的方式依次执行策略表。设置后，该编号不可编辑，也不可上下移动。

2. **策略对象**：告警需要监控的对象，具体分类见下表。

对象类型	监控对象	对象属性
系统	CPU	CPU 温度
		CPU 使用率
	授权	授权剩余天数
	SYN	SYN PPS
		SYN PPS 与 SYN ACK PPS 的比值
	SYNACK	SYNACK PPS
	连接数	总连接数
		总连接数使用率
	IP 数	总 IP 数使用率
		总 IP 数
网卡	任意网卡	流入速率
		流出速率
		网卡状态
		网卡流入带宽使用率
		网卡流出带宽使用率
		网卡总带宽使用率
	具体网卡（网卡 a、网卡 b）	同“任意网卡”

WAN 线路	任意 WAN 线路	流入速率
		流出速率
		心跳时延
		线路状态
	具体 WAN 线路（线路 a、线路 b）	同“任意 WAN 线路”
内网 IP	任意内网 IP	连接数
		会话应用
应用协议	应用协议特征库	上行速率
		下行速率
		连接数
流量统计对象	任意流量统计对象	上行速率
		下行速率
		上行流量
		下行流量
	具体流量统计对象（对象 a、对象 b）	同“任意流量统计对象”

表 5-11 策略对象参数说明

说明

除上述监控对象外，系统还支持 Ping 监测告警，请参见 Ping 检测。

3. **触发条件**：设置告警生效的阈值条件，用于标志一次事件。如：上行速率大于等于 100Mbps，持续时间超过 5 秒。
4. **策略动作**：在事件发生时，设置是否通知，以及通知的次数与间隔。
5. **监测时间**：告警策略的生效时间，0:00 ~ 0:00 表示全天。
6. **告警等级**：定义告警的级别，分为：一般告警、次要告警、主要告警、严重告警。

5.3.2. 进行中的事件

系统当前正在匹配告警策略的事件，展示其详情。

步骤 1 选择【系统告警】>【进行中的事件】

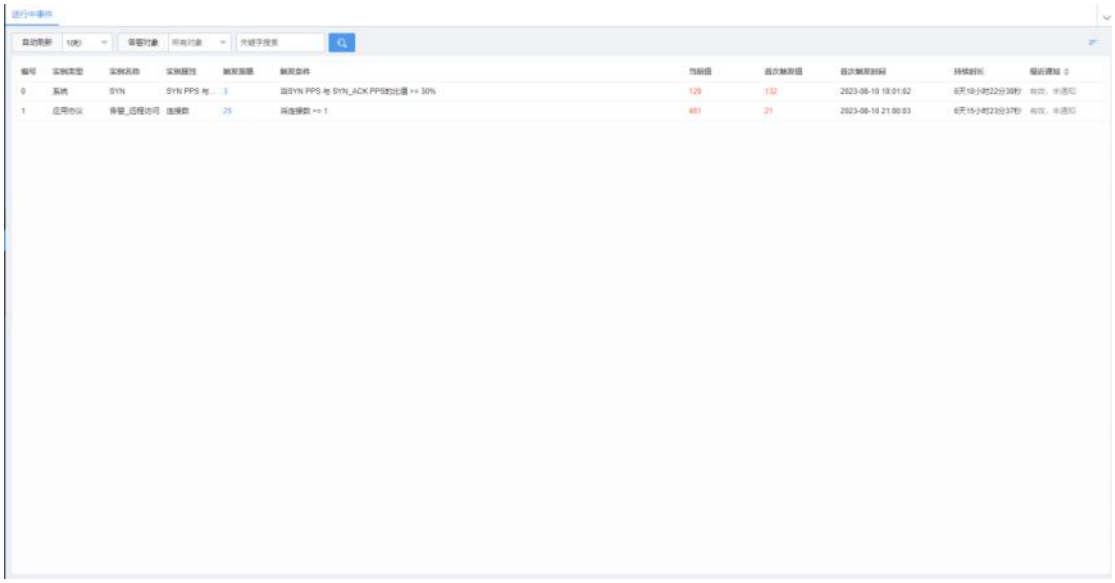


图 5-14 进行中的事件详情

参数名称	参数说明
自动刷新	进行中事件统计结果刷新时间，可选择不刷新或以 5s/10s/20s/60s 为周期进行刷新。
告警对象	根据监控对象筛选告警策略，监控对象包括：系统、网卡、WAN 线路、内网 IP、应用协议、流量统计对象、威胁情报。
关键字搜索	可根据配置策略的关键字搜索相应告警策略。
编号	进行中事件的编号，用于标识一次事件。
实例类型	告警监控的对象分类，同“告警对象”。
实例名称	告警监控的具体对象，如具体的应用协议，内网 IP 等。
实例属性	告警监控对象的属性，如上下行速率、连接数等。
触发策略	该进行中事件所对应的策略 ID，点击数字可查看策略。
触发条件	告警策略中设置的触发条件。
当前值	进行中事件当前触发告警条件时的具体数值。
首次触发值	进行中事件首次触发告警条件时的具体数值。
首次触发时间	事件首次发生的时间。
持续时长	首次触发时间至当前的持续时间。
最近通知	进行中事件的通知情况：告警是否为有效可通知事件，是否进行了通知。

表 5-12 进行中的事件参数说明

5.3.3. 已结束的事件

系统匹配告警策略的历史事件，展示其详情。

步骤 1 选择【系统告警】>【已结束的事件】

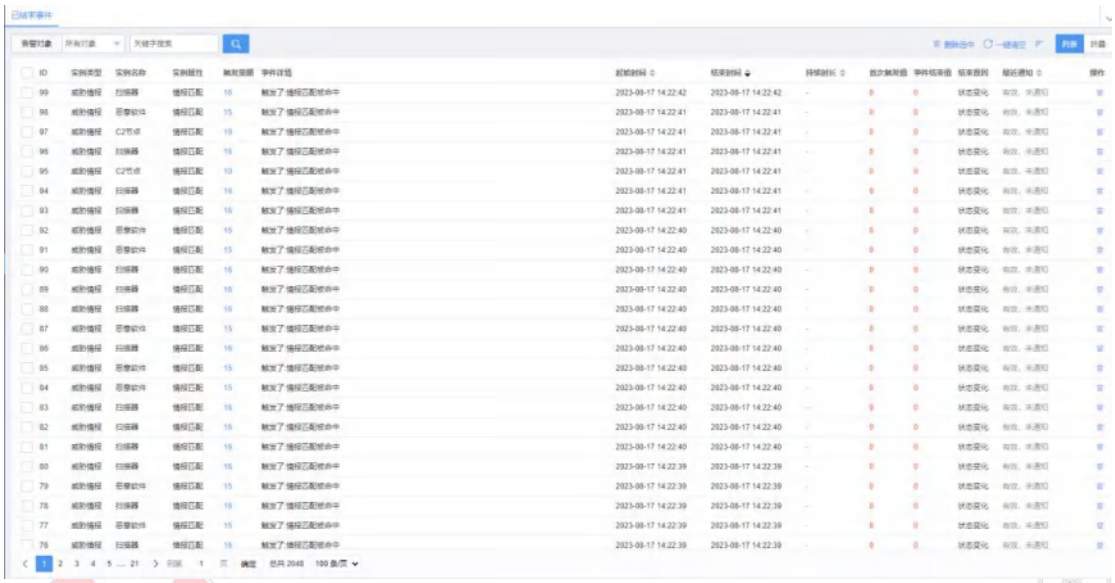


图 5-15 已结束的事件详情

参数名称	参数说明
告警对象	根据监控对象筛选告警策略，监控对象包括：系统、网卡、WAN 线路、内网 IP、应用协议、流量统计对象、威胁情报。
关键字搜索	可根据配置策略的关键字搜索相应告警策略。
删除选中	针对选中的事件，进行批量删除。
一键清空	点击后可删除全部事件。
ID	事件的编号，用于标识一次事件。
实例类型	告警监控的对象分类，同“告警对象”。
实例名称	告警监控的具体对象，如具体的应用协议，内网 IP 等。
实例属性	告警监控对象的属性，如上下行速率、连接数等。
触发策略	该事件所对应的策略 ID，点击数字可查看策略。
事件详情	事件的具体描述，触发的具体条件。
起始时间	事件首次发生的时间。
结束时间	事件结束的时间。
持续时长	事件起始至结束的持续时间。
首次触发值	事件首次触发告警条件时的具体数值。
事件结束值	事件不再触发告警条件时的具体数值。

结束原因	事件为何结束的描述，如低于阈值、状态变化等。
最近通知	进行中事件的通知情况：告警是否为有效可通知事件，是否进行了通知。
操作	点击 可删除该事件。

表 5-13 已结束的事件参数说明

5.3.4. 告警通知

告警事件发生后，可以通过该页面，对事件的通知进行设置，如通知的日期时间等。

步骤 1 选择【系统告警】>【告警通知】

图 5-16 告警通知详情

参数名称	参数说明
告警通知	设置是否开启通知， 关闭 为关闭， 开启 为开启。
通知时间	设置告警通知发送的时间段，默认为全天。
通知日期	设置告警通知发送的日期（星期一-星期日）。
通知方式	参见通知方式。

表 5-14 告警通知参数说明

5.3.5. 通知方式

告警的内容需要通知给接收端，该页面中，可以设置具体的通知方式。通知方式包括微信、企业微信、钉钉、飞书、邮箱、Panabit SaaS。

5.3.5.1. 微信

操作步骤

步骤 1 选择【系统告警】>【通知方式】。

步骤 2 选择页面上方【微信】。

步骤 3 关注“Panabit”公众号，点击 查看公众号二维码 查看。

步骤 4 用手机扫描二维码，绑定设备，点击 查看设备二维码。查看。

步骤 5 开启微信通知。

步骤 6 单击【提交】。

微信接收到的告警示例：

——结束

5.3.5.2. 企业微信

操作步骤

步骤 1 选择【系统告警】>【通知方式】。

步骤 2 选择页面上方【企业微信】。

步骤 3 在企业微信群中，创建机器人。

步骤 4 输入机器人 Webhook 地址。

步骤 5 开启企业微信通知。

步骤 6 单击【提交】。

——结束

5.3.5.3. 钉钉

操作步骤

步骤 1 选择【系统告警】>【通知方式】。

步骤 2 选择页面上方【钉钉】。

步骤 3 在钉钉中，创建自定义群聊机器人，安全设置选择“自定义关键字”。

步骤 4 输入机器人 Webhook 地址。

步骤 5 输入钉钉中设置的安全关键字。

步骤 6 开启钉钉通知。

步骤 7 单击【提交】。

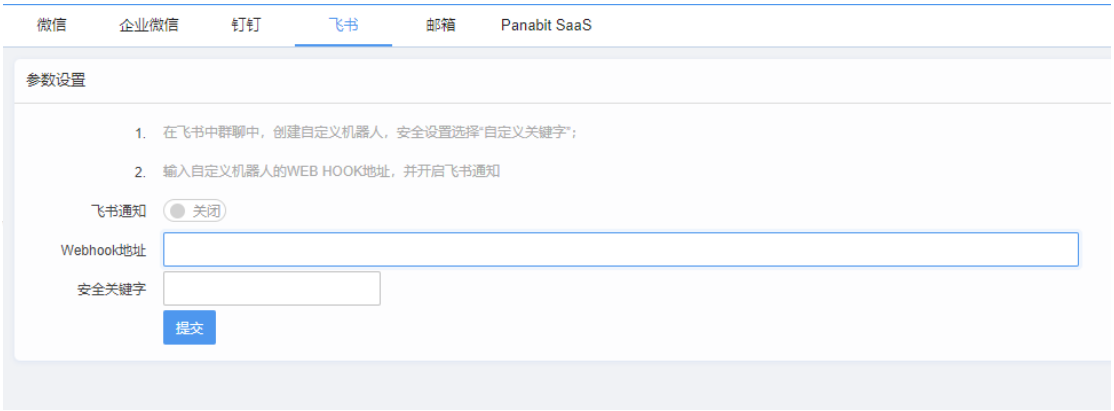
——结束

5.3.5.4. 飞书

操作步骤

步骤 1 选择【系统告警】>【通知方式】。

步骤 2 选择页面上方【飞书】。



步骤 3 在飞书中，创建自定义机器人，安全设置选择“自定义关键字”。

步骤 4 输入机器人 Webhook 地址。

步骤 5 输入飞书中设置的安全关键字。

步骤 6 开启飞书通知。

步骤 7 单击【提交】。

——结束

5.3.5.5. 邮箱

操作步骤

步骤 1 选择【系统告警】>【通知方式】。

步骤 2 选择页面上方【邮箱】。

参数名称	参数说明
SMTP 服务器地址（SMTP Server Address）	用于发送邮件的服务器的地址。
SMTP 服务器端口（SMTP Server Port）	SMTP 服务器监听的端口号。
发件人邮箱地址（Sender Email Address）	用于发送邮件的邮箱地址，即邮件的发件人。
发件人邮箱密码（Sender Email Password）	与发件人邮箱地址相对应的邮箱密码。
收件人邮箱地址（Recipient Email Address）	想要将邮件发送到的邮箱地址，即邮件的收件人。

步骤 2 开启邮件通知。

步骤 3 单击【提交】。

——结束

5.3.5.6. Panabit SaaS

操作步骤

将告警通知发送至 Panabit SaaS 平台：https://saas.panabit.com。

步骤 1 选择【系统告警】>【通知方式】。

步骤 2 选择页面上方【Panabit SaaS】。

步骤 3 填写邮箱相关设置。

参数名称	参数说明
服务器地址	saas.panabit.com
端口	8090

步骤 3 开启 SaaS 通知。

步骤 4 单击【提交】。

——结束

5.3.6. 应用案例：基于应用协议的告警

5.3.6.1. 应用场景

某企业对于其网络数据的保密性要求较高，禁止使用远程访问类应用，如 TeamViewer，向日葵等。一旦发现网络中存在远程访问类应用，需要及时告警，通知到网络管理员的微信。

5.3.6.2. 配置流程

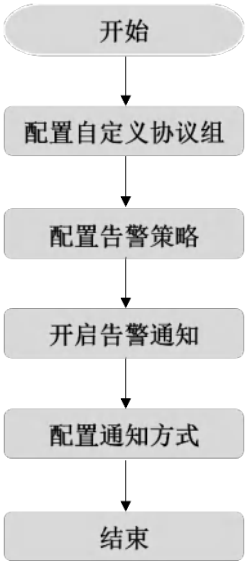


图 5-17 应用协议告警配置流程

5.3.6.3. 配置步骤

5.3.6.3.1. 配置自定义协议组

配置自定义协议组，具体操作请参见自定义协议组。

配置示例：添加自定义协议组，命名为“告警_远程访问”，选择 SSH、Telnet、TeamViewer、向日葵远控、PCAnywhere，添加至协议组中。

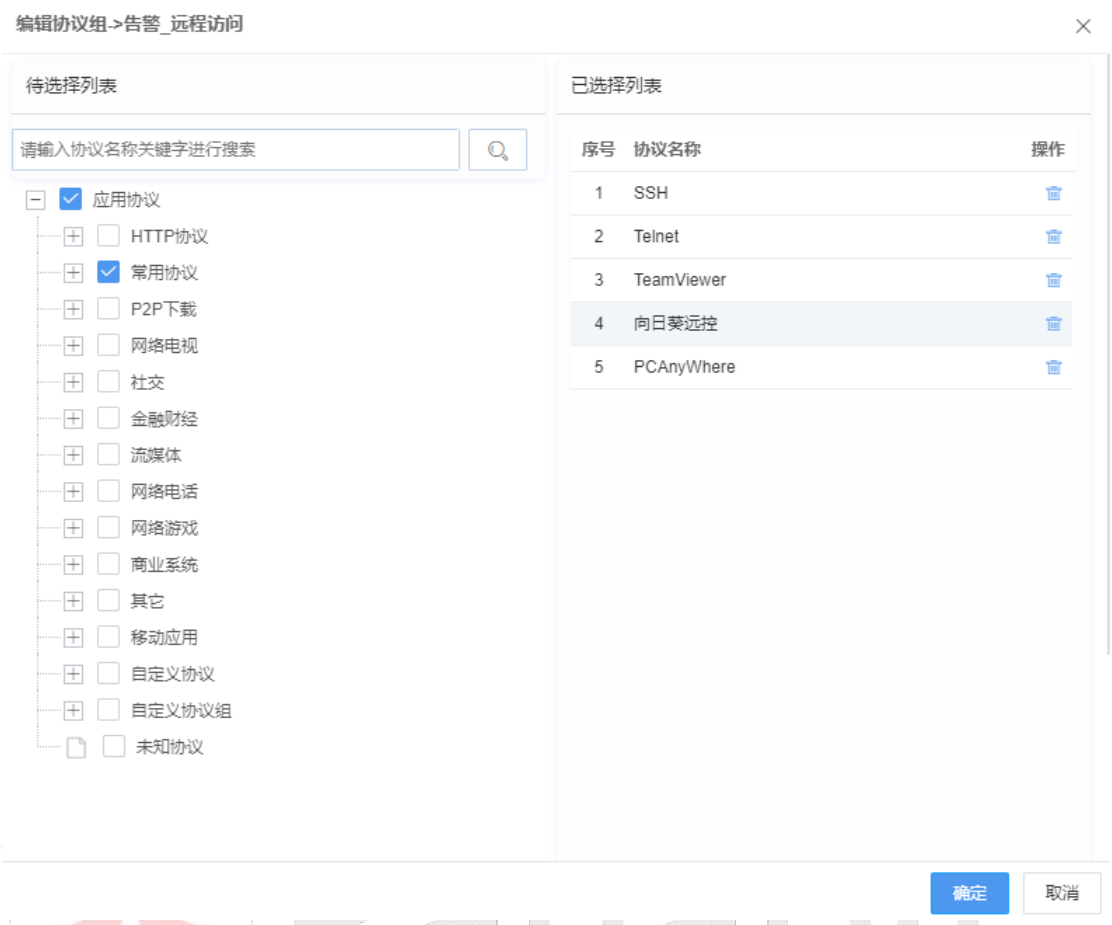


图 5-18 添加协议至协议组

5.3.6.3.2. 配置告警策略

步骤 1 选择【系统告警】>【告警策略】，添加告警策略。

步骤 2 设置策略 ID、策略条件、监测时间、告警等级，具体操作请参见告警策略。

配置示例：策略 ID 设置为“100”，策略条件选择“应用协议”，选择上一步配置的策略组：“告警_远程访问”，对象属性为“连接数”，触发条件为“大于等于”，阈值为“1”，将告警等级设置为“严重告警”。

含义为：当网络中出现了“告警_远程访问”应用组中的任何应用，且连接数 >=1，持续时间>0 秒，则触发告警，标记为严重告警，每隔 5 分钟通知一次，系统将全天对其进行监控。

步骤 3 点击【确定】。

——结束

5.3.6.3.3. 开启告警通知

开启告警通知，具体操作请参见告警通知。

图 5-19 开启告警通知详情

配置示例：开启告警通知，通知时间 0:00-23:59，通知日期全选。表示所有时间均可发送通知。

5.3.6.3.4. 配置通知方式

微信通知的配置，具体操作请参见微信。

5.3.7. 应用案例：基于流量统计的告警

我们可以通过流量控制策略中的流量统计功能，灵活自定义需要监控的流量，再结合告警模块进行监控与提醒。这个功能的组合，可以在很多监控场景下发挥作用，比如监控某个服务器的流量异常，或者摄像头终端的流量异常等。

5.3.7.1. 应用场景

某煤矿企业，为保证煤矿生产安全，会在煤矿下面部署多个监控服务器，这些服务器实时与集团总部传输数据，上报煤矿下的信息（人员，瓦斯等数据），当数据传输为 0，就需要判定为数据传输异常，需发出告警信息通知到信息中心人员排查原因。

5.3.7.2. 配置流程

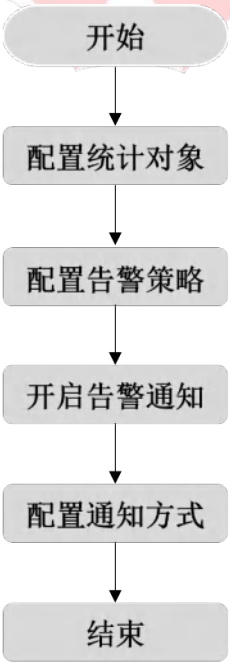


图 5-20 流量统计告警配置流程

5.3.7.3. 配置步骤

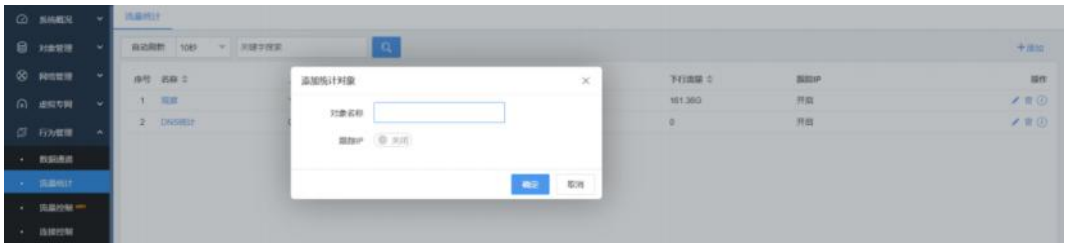
5.3.7.3.1. 配置统计对象

通过此操作，添加流量统计对象并配置流量控制策略。

操作步骤

步骤 1 选择【行为管理】>【流量统计】。

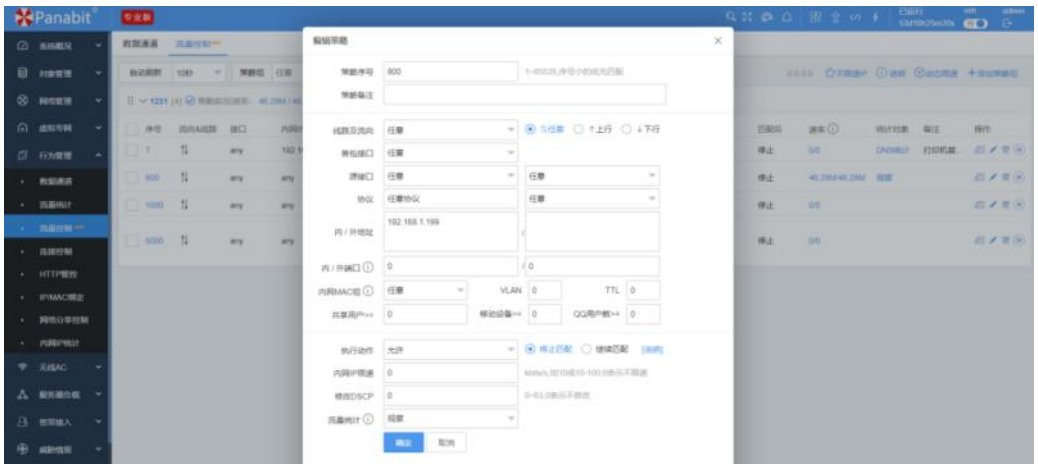
步骤 2 单击【添加】，添加统计对象。



步骤 3 选择【行为管理】>【流量控制】>【流量控制】。

步骤 4 鼠标悬停已创建策略组名称，单击【添加策略】。

步骤 5 配置流量控制策略，单击【确定】。



配置示例：在流量控制策略中，根据需要监控的内外网 IP 设置策略条件，内网地址设置为 192.168.1.199，执行动作为“允许”，流量统计选择“步骤 2”创建的对象。这个策略可以统计内网 192.168.1.199 的流量。

步骤 6 选择【行为管理】>【流量统计】。

步骤 7 单击操作对操作列的 ，查看统计结果。

——结束

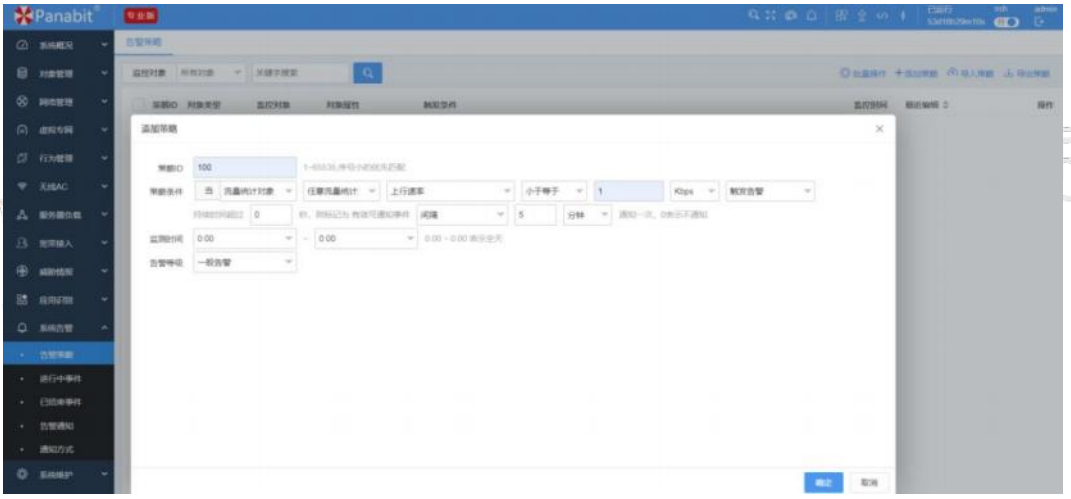
5.3.7.3.2. 配置告警策略

通过此操作，添加流量统计对象配置告警策略。

操作步骤

步骤 1 选择【系统告警】>【告警策略】，添加告警策略。

步骤 2 设置策略 ID、策略条件、监测时间、告警等级，具体操作请参见告警策略。



配置示例：在告警策略中，策略条件选择“流量统计对象”，流量统计选择上一步骤创建的对象，选择“上行速率”、“小于等于”，阈值填写“1”。表示当流量统计对象的上行速率小于等于 1Kbps 时，触发告警。

——结束

5.3.7.3.3. 开启告警通知

开启告警通知，具体操作请参见告警通知。

图 5-21 开启告警通知详情

配置示例：开启告警通知，通知时间 0:00-23:59，通知日期全选。表示所有时间均可发送通知。

5.3.7.3.4. 配置通知方式

选择适用于自己的告警通知方式，具体操作请参见通知方式。

图 5-22 配置通知方式详情

5.4. 系统维护

本章主要介绍了系统维护模块的各项功能，以及基本的使用与操作配置方法。在该模块中，您可以对上网行为管理系统本身进行一些基础的配置维护。

5.4.1. 系统设置

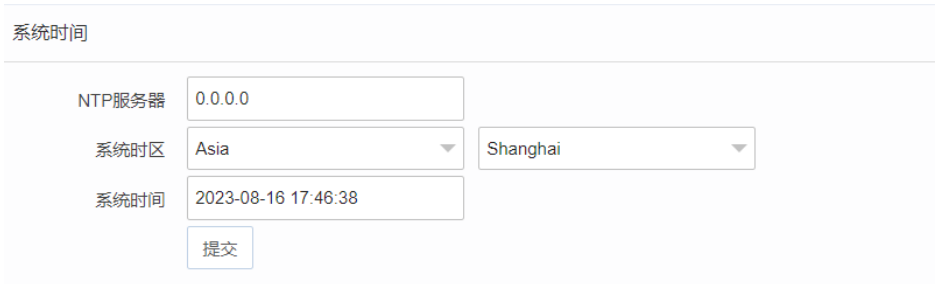
系统设置支持对当前设备进行基本的配置。

5.4.1.1. 基础设置

基础设置能对系统名称、管理接口、系统名称进行编辑。

步骤 1 选择【系统维护】>【系统设置】。

步骤 2 选择页面上方的【基础设置】。

参数名称	参数说明
系统名称	自定义设备名称，在自定义设备名称时请不要使用特殊符号。 
管理接口	可对当前设备的管理接口 IP、掩码、网关、DNS 做配置修改。 
系统时间	可对当前设备的系统时间做修改。可添加 NTP 服务，自动与 NTP 服务器同步时间。 

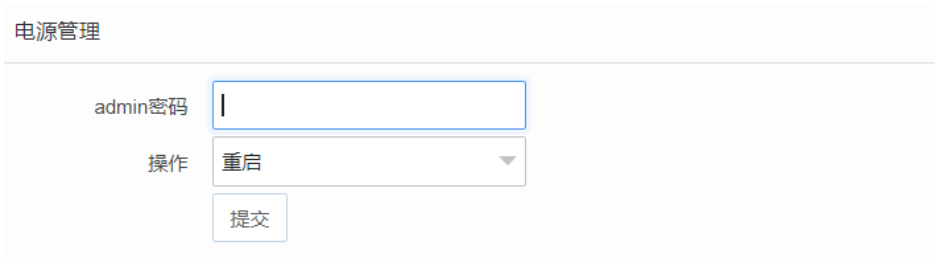
电源管理	校验 admin 账号密码后，可“重启”或“关机”设备。 

表 5-15 基础设置参数说明

5.4.1.2. WEB 设置

WEB 设置可以设置 WEB 访问的安全防护功能。

步骤 1 选择【系统维护】>【系统设置】。

步骤 2 选择页面上方的【WEB 设置】。

参数名称	参数说明
WEB 访问	界面闲置退出时间：登录设备无操作一段时间后，账号自动退出。 界面全屏后不退出：设置全屏系统是否退出。 首次登录显示验证码：用户首次登录界面时，是否需要显示验证码。 登录失败次数：设置登录失败的锁定次数； 登录页面锁定时间：页面被锁定后的持续时间。 WEB API 接口：可设置为“开启”或“关闭”WEB API 接口。 XSS 过滤：可设置为“开启”或“关闭”XSS 过滤。 最近访问页面：可设置为“开启”或“关闭”最近访问页面。 
WEB 服务器	WEB 端口：取值 1 ~ 65535 HTTP 读取超时时间：默认 60 秒，用于应对“缓慢 HTTP 拒绝服务攻击”。

	一般不建议修改。 

表 5-16 WEB 设置参数说明

5.4.2. 存储概况

存储概况是对系统存储的情况展示，包括存储池情况、读写速率、硬盘概况等。

步骤 1 选择【系统维护】>【存储概况】。

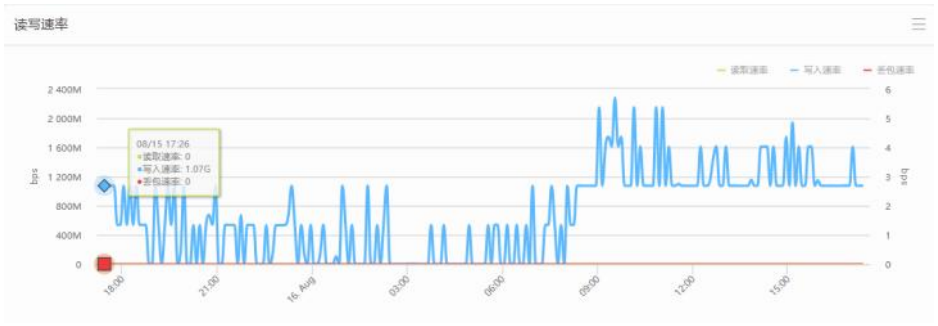
参数名称	参数说明
存储概况	展示所有磁盘存储可用总量，蓝色表示已使用空间，灰色表示剩余空间。 
读写速率	展示最近 24 小时/最近三天/最近一月磁盘的读写速率。 
存储池	展示存储池信息。 

表 5-17 存储概况参数说明

5.4.3. SNMP 服务

SNMP（简单网络管理协议）是一种广泛应用于 TCP/IP 网络的网络管理标准协议（应用层协议），广泛应用于网络交换机、路由器、打印机等网络设备上。

步骤 1 选择【系统维护】>【SNMP 服务】。

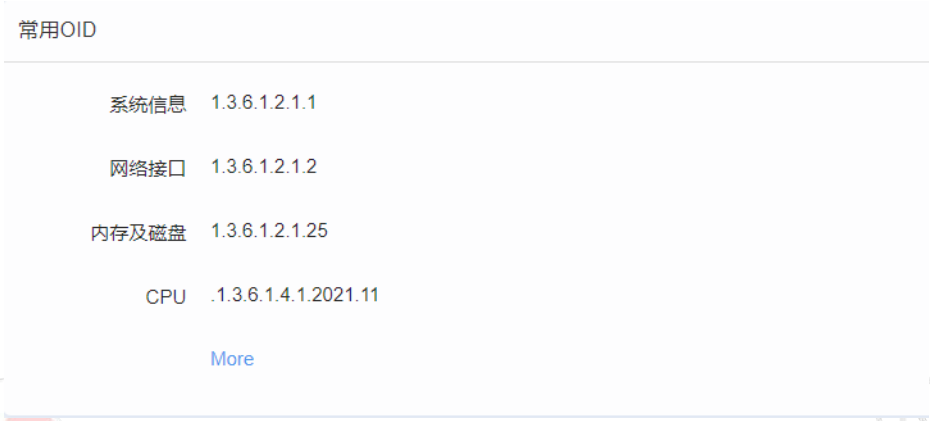
参数名称	参数说明
常用 OID	展示 SNMP 服务的系统、网络、硬件等信息。 
参数设置	SNMP 服务：是否开启系统的 SNMP 服务。 SNMP 端口：定义 SNMP 的服务端口 服务团体名：定义 SNMP 团体名。 服务白名单：格式为 x.x.x.x 或 x.x.x.x/y，多个 IP 用逗号分隔，为空表示任意 IP 都可以来获取数据。 

表 5-18 SNMP 服务参数说明

5.4.4. 系统用户

系统用户支持对当前设备的 WEB 用户进行管理。

5.4.4.1. 用户账号

对 WEB 用户的账号进行管理，可进行添加、删除、编辑操作。

步骤 1 选择【系统维护】>【系统用户】。

步骤 2 选择页面上方的【用户账号】。

图 5-23 用户账号详情

说明

用户账号分为三大类型：

- 超级管理员：访问编辑不受限制，页面部分内容只能由超管操作。
- 普通管理员：访问编辑受限，能够对系统进行基本配置。
- 只读用户：只能查看系统配置。

5.4.4.2. 认证方式

定义 WEB 账号的认证方式，默认为本地认证。可在本页面中将认证方式更改为 RADIUS 认证或 LDAP 认证。

步骤 1 选择【系统维护】>【系统用户】。

步骤 2 选择页面上方的【认证方式】。

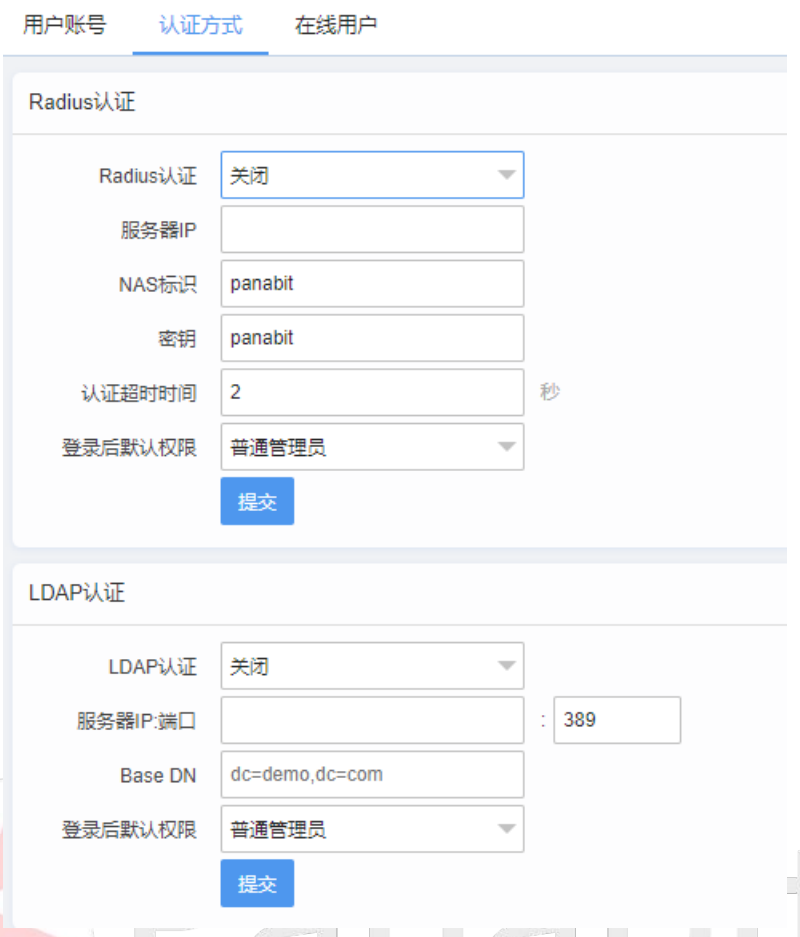


图 5-24 认证方式详情

5.4.4.3. 在线用户

展示当前已登录，在线的 WEB 账号相关信息，包括用户名、登录地址、登录时间等，超级管理员点击 强制下线 可将对应的用户强制登出。

步骤 1 选择【系统维护】>【系统用户】。

步骤 2 选择页面上方的【在线用户】。

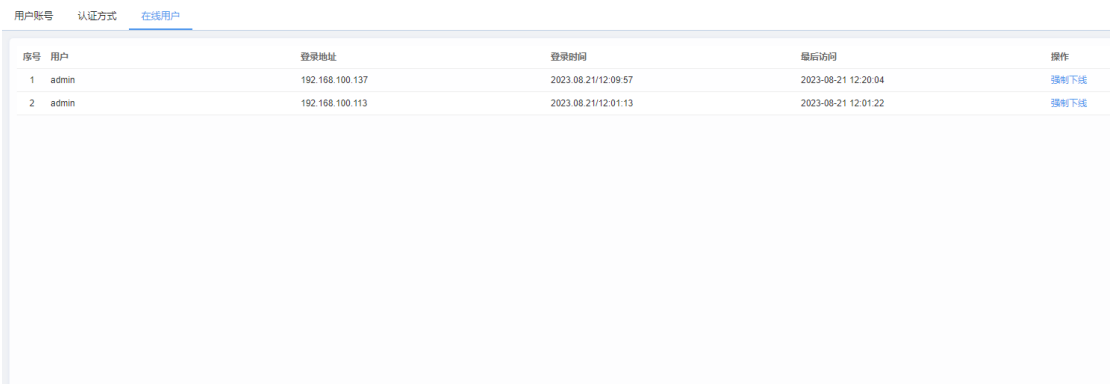


图 5-25 在线用户详情

5.4.5. 系统检测

系统检测支持对系统的系统硬件和软件进行检查，也支持添加Ping对象，进行Ping监测。

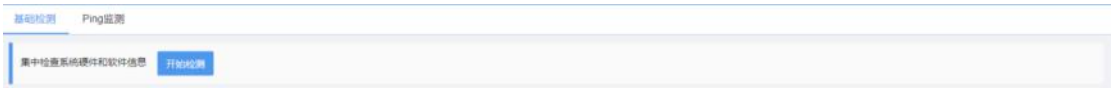
5.4.5.1. 基础检测

基础检测用于集中检查系统硬件和软件信息。

步骤 1 选择【系统维护】>【系统检测】。

步骤 2 选择页面上方的【基础检测】。

步骤 3 单击【开始检测】，开始进行系统检测。



检测结果示例：

5.4.5.2. Ping 检测

Ping 监测可选择不同接口线路，针对目标 IP 地址持续 Ping 监测，以确定不同线路或网络的质量，并可以设置告警。

步骤 1 选择【系统维护】>【系统检测】。

步骤 2 选择页面上方的【Ping 检测】。

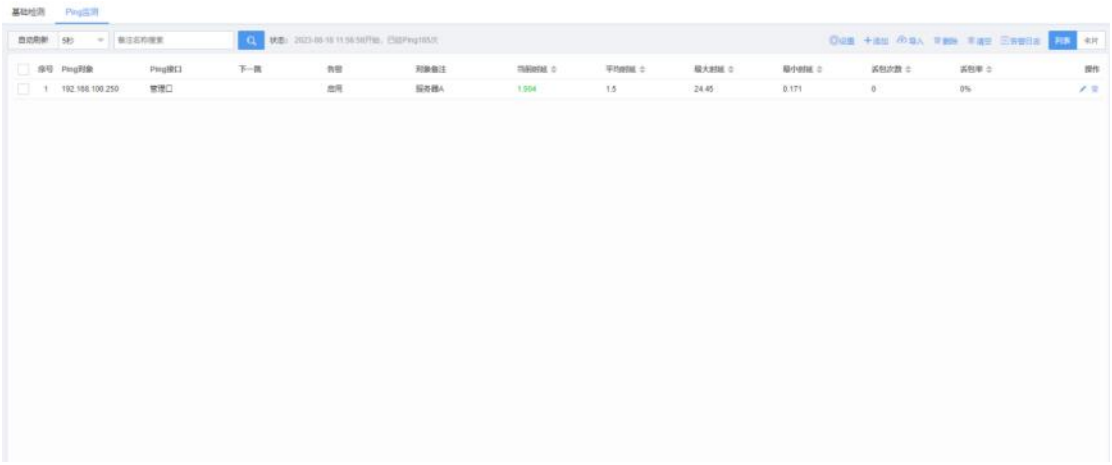
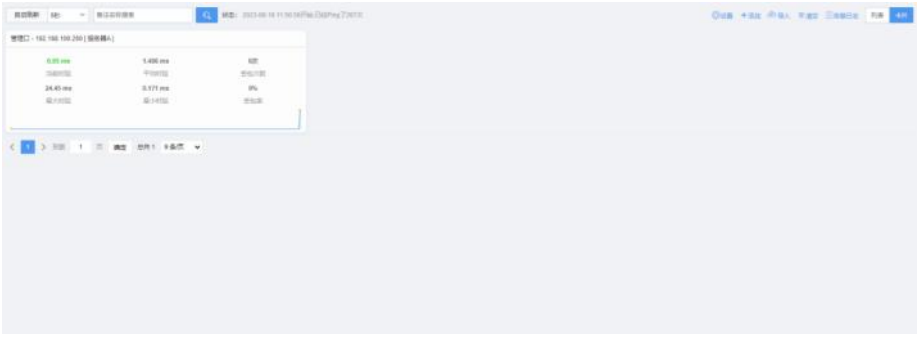


图 5-26 Ping 监测详情

参数名称	参数说明
自动刷新	统计结果刷新时间，可选择不刷新或以 5s/10s/20s/60s 为周期进行刷新。
备注名称搜索	针对 Ping 对象的备注名，进行搜索筛选。
状态	Ping 测的开始时间，测试次数。
设置	对 Ping 监测的功能进行配置。
添加	添加 Ping 监测的对象。
导入	从文本导入 Ping 监测的对象。
删除	删除选定的 Ping 监测对象。
清空	一键清空所有 Ping 监测对象。
告警日志	记录告警通知的历史日志。
列表/卡片	选择检测数据的呈现方式，上图为列表。 卡片形式如下所示： 
Ping 对象	监测对象的 IP 地址。
Ping 接口	Ping 监测的源接口。
下一跳	Ping 接口的下一跳地址。

告警	告警状态是否启用。
对象备注	针对 Ping 监测对象的描述。
当前时延	最近一次 Ping 测的时延数值，单位：ms。
平均时延	从 Ping 测开始，到最近一次 Ping 测期间的平均时延数值，单位：ms。
最大时延	从 Ping 测开始，到最近一次 Ping 测期间的最大时延数值，单位：ms。
最小时延	从 Ping 测开始，到最近一次 Ping 测期间的最小时延数值，单位：ms。
丢包次数	从 Ping 测开始，到最近一次 Ping 测期间的总丢包数。
丢包率	从 Ping 测开始，到最近一次 Ping 测期间的总丢包数/总 Ping 测包数。
操作	表示对 Ping 监测对象进行编辑操作。 表示对 Ping 监测对象进行删除操作。

表 5-19 Ping 监测参数说明

5.4.5.2.1. 配置实例

公司内部的某台服务器，需要时刻监测其是否在线，并监测从内部访问服务器的时延情况，当 ping 不可达，或时延大于 100ms 时，需产生告警，通过微信通知给网络管理员。

5.4.5.2.2. 配置流程

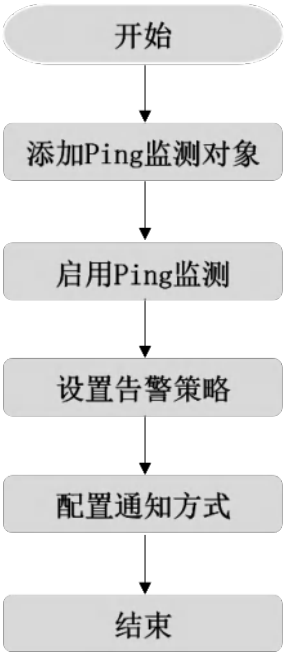


图 5-27 Ping 监测配置流程

说明

在无需进行告警，仅实现监控的情况下，步骤为：添加 Ping 监测对象-启用 Ping 监测

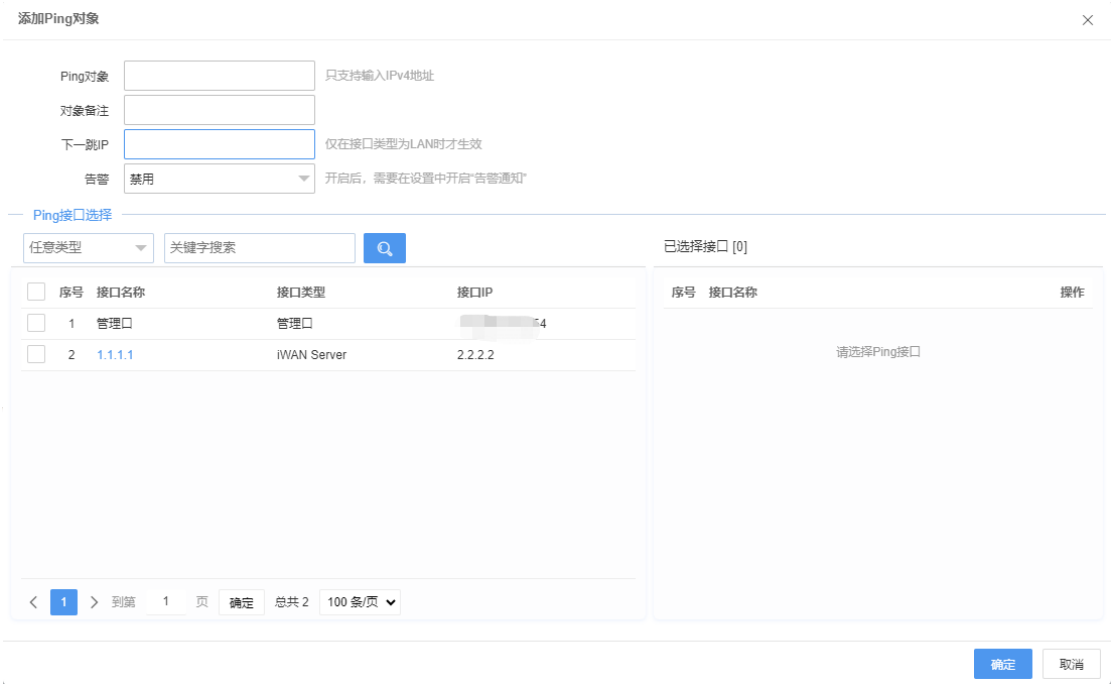
5.4.5.2.3. 配置步骤

操作步骤

步骤 1 选择【系统维护】>【系统检测】。

步骤 2 选择页面上方的【Ping 监测】。

步骤 3 单击【添加】，添加 Ping 监测对象。



参数名称	参数说明
Ping 对象	Ping 监测的目标地址，格式：IPv4 地址（x.x.x.x）。
对象备注	针对 Ping 对象的描述。
下一跳 IP	仅在接口类型为 LAN 时才生效
告警	选择是否启用告警。启用后，需要在 设置 中开启“告警通知”。
Ping 接口选择	勾选并指定 Ping 监测的源接口，可多选。

配置示例：

1. Ping 对象填写服务器的 IP 地址，如“192.168.100.250”。
2. 对象备注填写“服务器 A”。
3. Ping 接口选择“管理口”。

步骤 4 单击【设置】，启用 Ping 监测。

参数名称	参数说明
Ping 监测	选择是否启用检测功能。
Ping 测间隔	设定每两次 Ping 间的间隔时长，单位：秒。
最大 Ping 测次数	达到最大次数后重置统计数据

步骤 5 在步骤 4 的页面中，设置告警策略。

参数名称	参数说明
告警通知	选择是否启用告警功能。
告警条件	设定告警的触发规则。
告警频率	设置告警触发后，事件的通知频率。

配置示例：

1. Ping 通知选择“启用”。
2. 告警条件设置：“开启告警的对象”连续“5”次，时延大于“100”毫秒时，产生告警事件。
3. 告警频率设置：每个告警事件“间隔”“10”分钟通知一次。

步骤 6 在步骤 4 的页面中，点击【系统通知】，配置告警的通知方式。

配置示例：微信通知的配置，具体操作请参见微信。

下图为微信接收到的告警示例。

——结束

5.4.6. 配置管理

配置管理支持配置文件的导入/导出。

步骤 1 选择【系统维护】>【配置管理】。

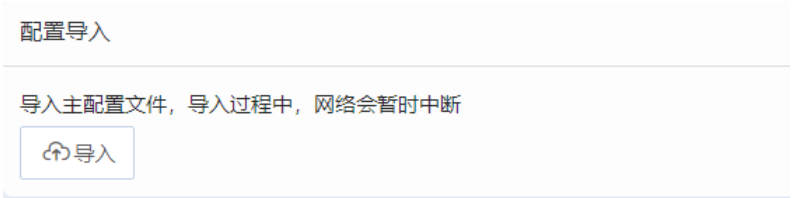
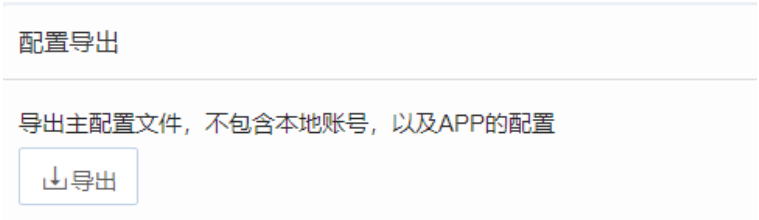
参数名称	参数说明
配置导入	单击【导入】，导入本地的配置文件。 
配置导出	单击【导出】，将当前配置导出至本地。 
重置配置	可以通过校验 admin 密码，将导入的配置重置，恢复出厂设置。

表 5-20 配置管理参数说明

5.4.7. 系统日志

系统日志主要记录 WEB 管理的操作日志及告警日志，可查看历史日志，并支持导出日志到本地。

5.4.7.1. 操作日志

操作日志记录 WEB 管理的登录日志、操作日志等信息，可以按日期与关键字进行查询。

步骤 1 选择【系统维护】>【系统日志】。

步骤 2 选择页面上方的【操作日志】。

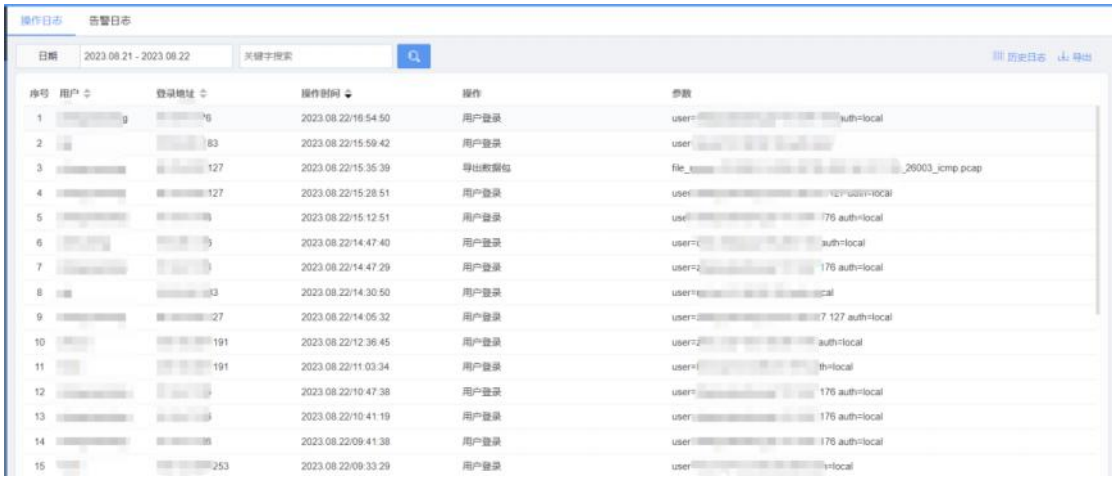


图 5-28 操作日志详情

参数名称	参数说明
历史日志	单击【历史日志】，弹出历史操作文件页面。

	 ● 单击操作列的，可查看每个文件下的操作详情。 ● 单击操作列的，可将每个文件下载到本地。
导出	单击【导出】，可将操作日志下载到本地。

表 5-21 操作日志参数说明

5.4.7.2. 告警日志

告警日志记录 WEB 管理的登录日志、登录状态、数据接口的 UP/DOWN 状态等信息，可以按照日期与关键字进行查询。

步骤 1 选择【系统维护】>【系统日志】。

步骤 2 选择页面上方的【告警日志】。

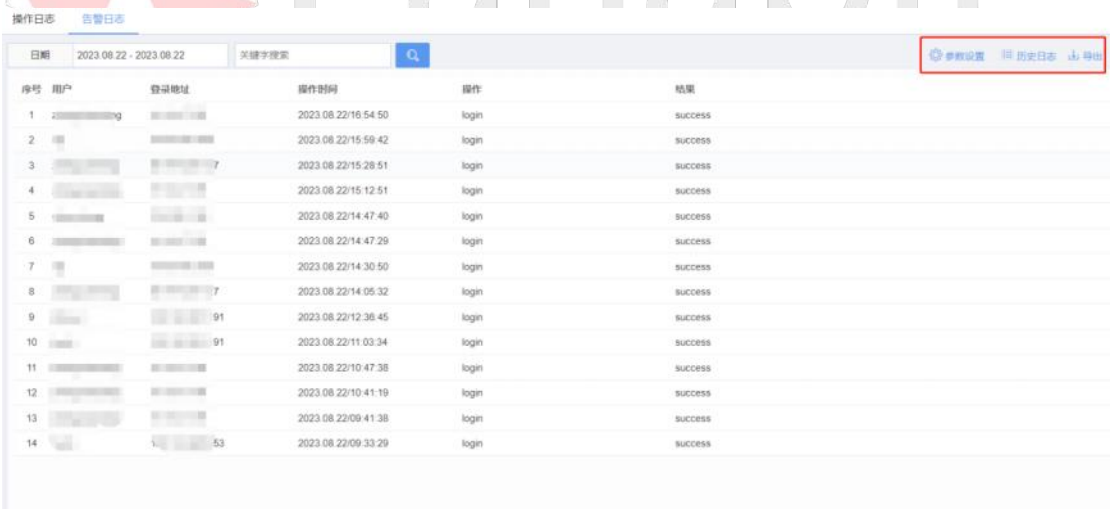


图 5-29 告警日志详情

参数名称	参数说明
参数设置	单击【参数设置】，弹出发送告警日志到服务器的设置页面。

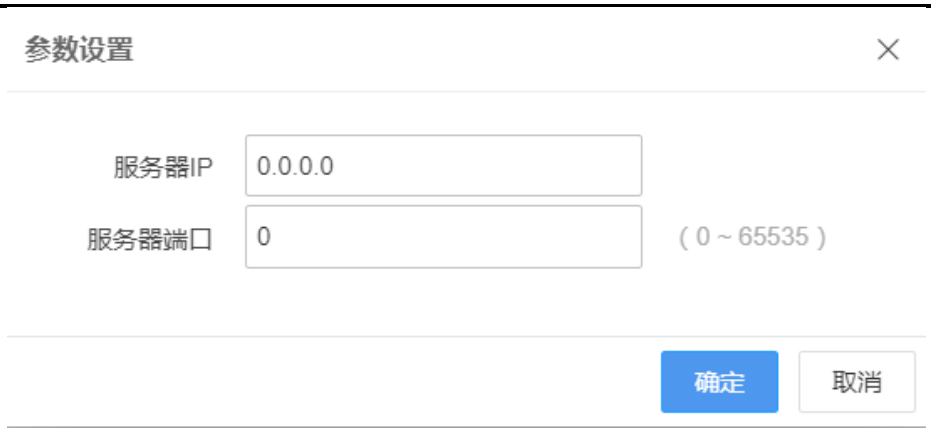
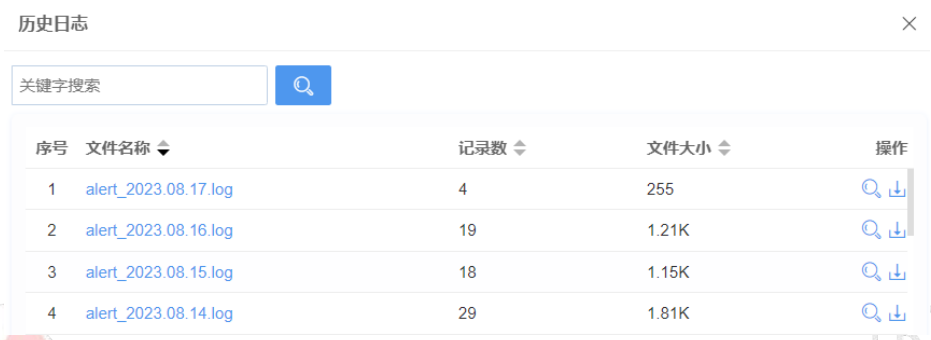
	
历史日志	单击【历史日志】，弹出历史日志文件页面。  ● 单击操作列的，可查看文件下的操作详情。 ● 单击操作列的，可将文件下载到本地。
导出	单击【导出】，可将告警日志下载到本地。

表 5-22 告警日志参数说明

5.4.8. 系统升级

5.4.8.1. 系统升级

本页面中，可进行系统升级与授权导入与导出操作，请参见系统升级与 License 导入。

图 5-30 系统升级详情

5.4.8.2. 升级日志

本页面可查看系统的历史升级记录。

图 5-31 升级日志详情

6. 附录

6.1. 常见术语表

名词	英文全称	解释
AAA	Authentication（认证）、Authorization（授权）、Accounting（计费/审计）	一种网络和信息安全体系结构，用于管理用户对网络资源的访问。AAA 服务器起到核心作用，用于验证用户身份、授权用户访问资源，并记录用户的网络活动以进行计费和审计。
AC	Access Control	一种用于管理和控制无线访问点（AP）的网络设备。主要功能是集中管理和协调多个 AP，以确保无线网络的可靠性、性能和安全性。
AD	Active Directory	一种目录服务，用于在网络中存储和组织有关用户、计算机、打印机、文件共享和其他网络资源的信息。它是 Windows 网络环境中的关键组件，旨在提供集中的身份管理、访问控制和资源管理。
AP	Access Point	用于将无线设备连接到有线网络的设备。它允许无线设备（如笔记本电脑、智能手机、平板电脑）通过 Wi-Fi 连接到有线局域网（LAN），从而实现无线网络接入。
API	Application Programming Interface	应用程序编程接口。API 是一组定义了不同软件组件之间如何互相交互和通信的规则和协议的集合。它允许不同的软件系统、应用程序或服务之间共享功能和数据，以实现特定的任务或目标。
ARP	Address Resolution Protocol	地址解析协议。用于将 IP 地址映射到 MAC 地址或物理硬件地址，以便在局域网（LAN）中正确地路由数据帧。
CGNAT	Carrier-Grade Network Address Translation	一种网络技术，用于处理 IPv4 地址枯竭问题（IPv4 地址短缺）。CGNAT 允许多个用户共享单个公共 IPv4 地址，同时维护网络通信的完整性

		和安全性。
DDOS	Distributed Denial of Service	分布式拒绝服务。DDoS 攻击是一种网络安全攻击，旨在通过使目标系统或网络不可用来剥夺合法用户的服务。这种攻击是通过向目标系统发送大量伪造的流量或请求来实施的，以超负荷地消耗目标系统的资源，导致它无法正常运行。
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议，通常用于自动分配 IP 地址和其他网络配置参数给网络上的设备。DHCP 常常在家庭和办公室网络中使用，以简化 IP 地址的设置和管理过程。
DNAT	Destination Network Address Translation	目标网络地址转换。DNAT 是一种网络技术，通常用于网络地址转换（NAT）的一部分，用于修改数据包的目标 IP 地址。DNAT 可以将传入的数据包的目标 IP 地址替换为内部网络中的某个设备的 IP 地址，从而将数据包传送到正确的内部设备。
DNS	Domain Name System	一种用于将人类可读的域名转换为计算机网络中使用的 IP 地址的分布式命名系统。
DPI	Deep Packet Inspection	深度数据包检测。DPI 是一种网络分析技术，用于详细检查传输在计算机网络中的数据包，以便了解数据包的内容、结构和特征。这项技术可以用于网络管理、安全监控、流量分析和应用程序识别等领域。
FTP	File Transfer Protocol	文件传输协议。它是一种用于在计算机网络上传输文件的标准协议。FTP 允许用户从一个计算机（通常是称为 FTP 服务器的计算机）向另一个计算机（通常是称为 FTP 客户端的计算机）传输文件，以便在这些计算机之间共享和管理文件。
GRE	Generic Routing Encapsulation	通用路由封装。一种用于在 IP 网络中封装和传输其他协议数据包的协议。GRE 通常用于构建虚

		拟专用网络（VPN）和在不同网络之间隧道传输数据。
HTTP	Hypertext Transfer Protocol	超文本传输协议。它是一种用于在互联网上传输和交换超文本（即包含文本、图像、链接等多媒体元素的文档）的应用层协议。HTTP 是互联网上最常用的协议之一，用于支持和驱动万维网（World Wide Web）的运作。
HTTPS	Hypertext Transfer Protocol Secure	它是 HTTP 协议的安全版本，用于在互联网上安全传输数据。HTTPS 通过使用加密机制来保护数据的完整性和隐私，使得数据在传输过程中更难以被窃听或篡改。
ICMP	Internet Control Message Protocol	Internet 控制报文协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。
IMAP	Internet Message Access Protocol	互联网消息访问协议。IMAP 是一种用于电子邮件客户端和邮件服务器之间的通信的标准协议。与 POP3（邮局协议版本 3）不同，IMAP 允许用户在多个设备上访问和管理他们的电子邮件，同时保留邮件服务器上的副本，以便在任何时间和地点都可以同步查看邮件。
IPsec	Internet Protocol Security	它是一组网络协议和技术，用于提供互联网通信的安全性和隐私保护。IPsec 的主要目标是确保数据在互联网上的传输过程中保持机密性、完整性和身份验证，以防止数据被未经授权的访问、窃听或篡改。
ISP	Internet Service Provider	互联网服务提供商。是一种提供互联网连接和相关服务的公司或组织。它们通过各种技术（如拨号、DSL、光纤、电缆、卫星等）将用户连接到互联网，使用户能够访问网络、发送电子邮件、浏览网页、下载文件等。
iWAN	N/A	一种派网自研的隧道协议，区别于传统的 VPN 隧道技术，它是一种高连通性的隧道协议。

		iWAN 专门为 SD-WAN 的高效、加速场景而设计，具备传输效率高，重连速度快的特点，不受 IP 变化影响，抗沿途干扰能力强。
L2TP	Layer 2 Tunneling Protocol	它是一种网络协议，通常用于创建虚拟私有网络（VPN）连接。L2TP 是一个跨平台协议，允许远程用户通过公共互联网连接到私有网络，以便安全地访问内部资源。
LAN	Local Area Network	局域网。局域网是一种网络拓扑结构，通常用于连接位于相对较近的地理位置的计算机和网络设备，以实现它们之间的通信和资源共享。
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议。一种用于在网络中访问和查询目录服务信息的开放标准协议。LDAP 协议旨在提供一种标准的方式来查询和管理这些目录信息。
MSDS	Microsoft Domain Sharing	微软局域网共享协议，利用 445 端口通信的一种协议，该协议允许计算机上的应用程序读取文件和向服务器请求服务。
MTU	Maximum Transmission Unit	最大传输单元。MTU 是网络通信中的一个重要参数，它指示了在网络中可以传输的数据包的最大大小。具体来说，MTU 定义了一条网络链路上可以发送的数据包的最大字节数。
NAT	Network Address Translation	网络地址转换。它是一种网络协议和技术，用于在计算机网络中管理和映射 IP 地址。NAT 允许多个局域网中的设备共享一个或多个公共 IP 地址，同时将这些设备的私有 IP 地址映射到公共 IP 地址上，以实现在内部网络和外部网络之间进行通信。
NetBIOS	Network Basic Input/Output System	网络基本输入/输出系统协议，它提供了 OSI 模型中的会话层服务，让在不同计算机上运行的不同程序，可以在局域网中，互相连线，以及分享数据。
NPM	Network Performance Management	网络性能管理，用于监测、测量、分析和优化网络的性能。

NTP	Network Time Protocol	网络时间协议，是用来使计算机时间同步化的一种协议，它可以使计算机对其服务器或时钟源（如石英钟，GPS 等等）做同步化。
PanaOS	N/A	派网自研的专用数据面操作系统，在 DPDK 之前就解决了 x86 吞吐问题，在打开七层功能情况下，可以顺畅工作在 100G 网络环境。
POP3	Post Office Protocol version 3	邮件协议第三版。POP3 是一种用于检索电子邮件的标准协议，它允许电子邮件客户端从邮件服务器上下载和存储电子邮件消息，以便用户可以阅读和管理它们。
PPPoE	Point-to-Point Protocol over Ethernet	以太网上的点对点协议。PPPoE 通常用于在以太网上建立点对点连接，以提供广域网（WAN）接入服务，尤其在宽带互联网连接中常见。
PPS	Packets Per Second	每秒数据包数。用于描述网络通信中的数据包传输速率，即每秒传输的数据包数量。PPS 是衡量网络设备、路由器、交换机、防火墙和其他网络设备性能的一种常用指标之一。
RAAS	RADIUS as a Service	Panabit RAAS 是一套基于标准 Radius 的认证、计费和管理的软件服务系统，适用于学校、企业、政府、酒店以及其他 WiFi 覆盖场所等场景。
RADIUS	Remote Authentication Dial-In User Service	远程身份验证拨号用户服务。它是一种网络协议和客户端/服务器系统，用于进行用户身份验证、授权和账户管理。RADIUS 通常用于在计算机网络中提供安全的远程访问服务，如虚拟专用网络（VPN）、无线局域网（Wi-Fi）、拨号接入等。
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议。SMTP 是一种用于发送和传递电子邮件的标准协议，它规定了电子邮件如何从发送者的电子邮件客户端（例如，电子邮件应用程序或电子邮件服务器）发送到接收者的电子邮件服务器，然后再传送到接收者的电子邮件客户端。

SNAT	Source Network Address Translation	源网络地址转换。SNAT 是一种网络技术，通常用于网络地址转换（NAT）的一部分，用于修改数据包的源 IP 地址。SNAT 在网络中的主要作用是隐藏内部网络的真实 IP 地址，以保护内部网络的安全性和隐私，并允许多个内部设备共享单个公共 IP 地址来访问互联网。
Socks4/5	Socks: Protocol for sessions traversal across firewall securely	Socks 是一种网络传输协议，主要用于客户端与外网服务器之间通讯的中间传递，分为 v4 版本和 v5 版本。
SSDP	Simple Service Discovery Protocol	简单服务发现协议，是一种应用层协议，是构成通用即插即用（UPnP）技术的核心协议之一。
SSH	Secure Shell	安全外壳协议，为建立在应用层和传输层基础上的安全协议。是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。
SSID	Service Set Identifier	一种用于识别无线局域网（WLAN）的名称，通常也称为无线网络名称。SSID 是用于区分不同无线网络的标识符，使用户能够选择并连接到他们想要的特定无线网络。
SYN	Synchronize Sequence Numbers	TCP/IP 建立连接时使用的握手信号，TCP 连接的第一个包。
TCP	Transmission Control Protocol	传输控制协议。TCP 是互联网通信协议的一种，用于在计算机和网络设备之间建立可靠的连接，以确保数据的可靠传输。它是 OSI 模型中的传输层协议之一，用于在应用层之间提供端到端的数据传输服务。
Telnet	N/A	是 Internet 远程登录服务的一种标准协议，为用户提供了在本地计算机上完成远程主机工作的能力
UDP	User Datagram Protocol	用户数据报协议。UDP 是一种互联网通信协议，属于 OSI 模型中的传输层协议之一，用于在计算机和网络设备之间传输数据。与 TCP

		（传输控制协议）不同，UDP 是一种不可靠的协议，它主要用于传输数据时对数据传输的可靠性要求较低的情况。
URL	Uniform Resource Locator	统一资源定位符。URL 是用于在互联网上标识和定位资源的一种标准化方式。URL 包括了描述资源位置、访问资源的协议以及资源在特定位置的路径和文件名等信息。
VLAN	Virtual Local Area Network″	虚拟局域网。VLAN 是一种在物理网络基础设施上创建逻辑网络的技术，允许将多个网络设备划分为不同的虚拟网络，即虚拟局域网，而不受物理位置的限制。这有助于提高网络的灵活性、安全性和管理性，并允许有效地组织和隔离不同的网络流量。
VRRP	Virtual Router Redundancy Protocol	虚拟路由器冗余协议。它是一种网络协议，用于提供网络冗余和高可用性，确保在一个网络中存在多个路由器时，如果其中一个路由器发生故障，其他路由器可以自动接管其工作，以保持网络的连通性和可用性。
VRRP	Virtual Router Redundancy Protocol	虚拟路由器冗余协议。它是一种网络协议，用于提供网络冗余和高可用性，确保在一个网络中存在多个路由器时，如果其中一个路由器发生故障，其他路由器可以自动接管其工作，以保持网络的连通性和可用性。
WAN	Wide Area Network	广域网。是一种网络拓扑结构，用于连接位于较远地理位置的计算机和网络设备，以实现它们之间的通信和数据传输。与局域网（LAN）不同，广域网跨越较大的地理区域，通常覆盖城市、国家，甚至跨越全球范围。
Web 认证	Web Authentication	一种用于验证用户身份的技术，通常用于保护 Web 应用程序和在线服务的安全性。它是确保只有经过授权的用户可以访问受保护资源的关键组成部分。

服务时延	Server Network Delay	TCP 三次握手中，Panabit 上[SYN_ACK 包记录的时间]-[SYN 包记录的时间]，约等于运营商侧的时延。
客户时延	Client Network Delay	TCP 三次握手中，Panabit 上[ACK 包记录的时间]-[SYN_ACK 包记录的时间]，约等于用户侧的时延。
派网 SaaS	N/A	一种基于 SaaS 模式的云管平台，能够对分散在各地的 Panabit 设备实现集中监控和远程管理。用户无需单独安装管理平台，只需通过 Web 访问即可监控管理所有 Panabit 设备。
应用时延	Application Network Delay	Panabit 上[服务端首回包记录的时间]-[客户端首包记录的时间]，约等于服务提供者自身的响应时延。

6.2. 应用商店 APP

应用名称	应用简介
SaaS 客户端	用于设备对接 SaaS。 派网 SaaS 云管平台地址：https://saas.panabit.com
深澜&热点账号对接	对接深澜&城市热点账号，实现基于账号的审计和控制。
游戏快线	为绝地求生等游戏加速。
移动 WebPortal	支持中国移动 WebPortal 接口协议。
网吧策略向导	快速生成一个可用的流控策略。
root 密码管理器	通过 Web 页面修改 root 密码。
LIBCURL	更新 FreeBSD9.2 版本的 curl 程序。
WEB 认证	通过身份认证信息的授权控制 Internet 的访问。
AD 域同步	AD 域组织架构和认证信息同步。
云服务	通过云服务可以监控管理多台设备。
DDNS 服务	将指定线路的 IP 地址映射到一个固定的域名解析服务上。
网桥网卡状态同步	网桥的两张网卡同步 up/down。
跨三层取 MAC	Panabit 跨三层部署时，通过 SNMP，获取 IP 和 MAC 的对应关系。
ADSL 定时重拨	定时重拨应用路由的动态 WAN 线路。
威胁情报 IOCs 同步	同步威胁情报 IOCs 数据。

赛博谛听安全云服务	赛博谛听安全云服务。
MAC 黑白名单	MAC 黑白名单管理。
服务快线	为您的网络借线加速。
会话共享检测	通过特定会话检测共享
系统时区文件库	系统时区文件库。
时间设置页面补丁	时间设置页面补丁。
BYPASS 控制器	Bypass 交换机控制器。

6.3. 威胁情报列表

名词	解释
数字货币	数字货币是一种基于节点网络和数字加密算法的虚拟货币。包括全球千余种数字货币的相关信息，具体包括矿池地址、矿池域名和 IP 信息，挖矿软件的 hash 值等。
C2 节点	C2 节点是感染或传播木马病毒等其他类型恶意软件的网络设备的节点地址，通常用来和控制终端进行通信，包括各种恶意软件回连的命令&控制端 IP 地址等信息。
APT 攻击	APT 指高级持续性威胁，通常指利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。APT 情报指全球范围内黑客组织进行 APT 攻击活动相关的情报。可包括组织名称，攻击目标，攻击方式，利用工具等其他信息。
网站后门	黑客植入的后门，它可以帮助黑客控制网站。
钓鱼网站	钓鱼网址指为了窃取金融账号、密码等敏感信息而伪装成合法的商业网站进行欺诈活动的网站。
僵尸网络	僵尸网络指由多个被某种恶意软件感染和控制的主机设备组成的被控网络。包括组成僵尸网络的被控主机的 IP 地址等信息。
恶意软件	恶意软件是指在未经用户许可的情况下，在计算机或其他终端上安装运行、损害服务器或客户端的系统和网络、对用户造成危害的软件。恶意软件包含故意在计算机系统上执行恶意任务的后门、间谍软件、欺诈软件等其他形式的各种恶意软件。
扫描器	扫描器节点主要指未经授权进行的网络扫描行为的 IP 地址。
TOR 节点	Tor（The Onion Router）是洋葱路由器的缩写，是实现匿名通信的软件套

	件。Tor 节点指匿名网络通信系统分散在全世界的服务器节点信息。
代理和隧道	Proxy 代理可用于访问因地理位置或其他原因而被阻止的网站。Proxy 代理由于可隐藏主机的源地址信息，可被攻击者利用进行恶意活动，具有一定的潜在风险。
网络广告	在各种互联网平台上投放的广告。
恶意网站	恶意网站指被植入恶意代码以实现攻击者目标的网站。包括植入各种恶意代码的欺诈类网站，漏洞利用网站、攻击链上的跳转、传输网站等。
色情网站	色情网站指提供、展示、传播色情及相关内容的网站。
赌博网站	赌博网站指提供赌博信息或者支持在线赌博的各类网站。
垃圾邮件	垃圾邮件一般指未经用户许可就强行发送到用户邮箱中的各种电子邮件。包括垃圾邮件的发送方、邮件内容里的 spam 链接，邮件服务器及其中转服务器的 IP 信息等，也包括黑客组织注册或利用的邮箱信息。
可疑行为	攻击程序或者病毒常用的一些网络访问，例如：获取外网 IP 地址，单次的可疑行为并不意味着已经被恶意程序感染控制，因为正常程序偶尔也会有这类访问，但是持续不断地使用则需要引起用户重视。

6.4. SNMP OID 列表

分类	详情
Panabit 设备专有信息	.1.3.6.1.4.1.58819.1.2.1 CPU 温度 .1.3.6.1.4.1.58819.2.2.1 License 起始时间 .1.3.6.1.4.1.58819.2.2.2 License 结束时间 .1.3.6.1.4.1.58819.2.2.3 License 剩余天数 .1.3.6.1.4.1.58819.2.2.4 License 并发连接数 .1.3.6.1.4.1.58819.2.2.5 License 并发 IP 数 .1.3.6.1.4.1.58819.3.2.1 最高在线用户数 .1.3.6.1.4.1.58819.3.2.2 当前在线用户数 .1.3.6.1.4.1.58819.4.2.1 最高 PPS .1.3.6.1.4.1.58819.4.2.2 当前 PPS
系统信息	.1.3.6.1.2.1.1.1.0 sysDescr .1.3.6.1.2.1.1.2.0 sysObjectID .1.3.6.1.2.1.1.3.0 sysUpTimeInstance

	.1.3.6.1.2.1.1.4.0 sysContact .1.3.6.1.2.1.1.5.0 sysName .1.3.6.1.2.1.1.6.0 sysLocation .1.3.6.1.2.1.1.7.0 sysServices
网络接口数（物理口+虚线路）	.1.3.6.1.2.1.2.1.0 ifNumber
网络接口信息（x 为网卡编号或线路 ID）	.1.3.6.1.2.1.2.2.1.1.x ifIndex .1.3.6.1.2.1.2.2.1.2.x ifDescr .1.3.6.1.2.1.2.2.1.3.x ifType .1.3.6.1.2.1.2.2.1.4.x ifMtu .1.3.6.1.2.1.2.2.1.5.x ifSpeed .1.3.6.1.2.1.2.2.1.6.x ifPhysAddress .1.3.6.1.2.1.2.2.1.7.x ifAdminStatus .1.3.6.1.2.1.2.2.1.8.x ifOperStatus .1.3.6.1.2.1.2.2.1.9.x ifLastChange .1.3.6.1.2.1.2.2.1.10.x ifInOctets .1.3.6.1.2.1.2.2.1.11.x ifInUcastPkts .1.3.6.1.2.1.2.2.1.14.x ifInErrors .1.3.6.1.2.1.2.2.1.16.x ifOutOctets .1.3.6.1.2.1.2.2.1.17.x ifOutUcastPkts .1.3.6.1.2.1.2.2.1.19.x ifOutDiscards .1.3.6.1.2.1.2.2.1.20.x ifOutErrors
系统运行时间	.1.3.6.1.2.1.25.1.1.0 hrSystemUptime
网络接口信息（扩展，x 为网卡编号或线路 ID）	.1.3.6.1.2.1.31.1.1.1.1.x ifName .1.3.6.1.2.1.31.1.1.1.2.x ifInMulticastPkts .1.3.6.1.2.1.31.1.1.1.3.x ifInBroadcastPkts .1.3.6.1.2.1.31.1.1.1.4.x ifOutMulticastPkts .1.3.6.1.2.1.31.1.1.1.5.x ifOutBroadcastPkts .1.3.6.1.2.1.31.1.1.1.6.x ifHCInOctets .1.3.6.1.2.1.31.1.1.1.7.x ifHCInUcastPkts .1.3.6.1.2.1.31.1.1.1.8.x ifHCInMulticastPkts .1.3.6.1.2.1.31.1.1.1.9.x ifHCInBroadcastPkts .1.3.6.1.2.1.31.1.1.1.10.x ifHCOutOctets

	.1.3.6.1.2.1.31.1.1.1.11.x ifHCOutUcastPkts .1.3.6.1.2.1.31.1.1.1.12.x ifHCOutMulticastPkts .1.3.6.1.2.1.31.1.1.1.13.x ifHCOutBroadcastPkts .1.3.6.1.2.1.31.1.1.1.15.x ifHighSpeed
内存信息	.1.3.6.1.4.1.2021.4.5.0 memTotalReal .1.3.6.1.4.1.2021.4.6.0 memAvailReal .1.3.6.1.4.1.2021.4.13.0 memShared .1.3.6.1.4.1.2021.4.14.0 memBuffer .1.3.6.1.4.1.2021.4.15.0 memCached
磁盘信息（x 为分区编号）	.1.3.6.1.4.1.2021.9.1.1.x dskIndex .1.3.6.1.4.1.2021.9.1.2.x dskPath .1.3.6.1.4.1.2021.9.1.6.x dskTotal .1.3.6.1.4.1.2021.9.1.7.x dskAvail .1.3.6.1.4.1.2021.9.1.8.x dskUsed .1.3.6.1.4.1.2021.9.1.9.x dskPercent .1.3.6.1.4.1.2021.9.1.10.x dskPercentNode
系统负载	.1.3.6.1.4.1.2021.10.1.1.1 laIndex Load-1 .1.3.6.1.4.1.2021.10.1.1.2 laIndex Load-5 .1.3.6.1.4.1.2021.10.1.1.3 laIndex Load-15 .1.3.6.1.4.1.2021.10.1.2.1 laNames Load-1 .1.3.6.1.4.1.2021.10.1.2.2 laNames Load-5 .1.3.6.1.4.1.2021.10.1.2.3 laNames Load-15 .1.3.6.1.4.1.2021.10.1.3.1 laLoad Load-1 .1.3.6.1.4.1.2021.10.1.3.2 laLoad Load-5 .1.3.6.1.4.1.2021.10.1.3.3 laLoad Load-15 .1.3.6.1.4.1.2021.10.1.4.1 laConfig Load-1 .1.3.6.1.4.1.2021.10.1.4.2 laConfig Load-5 .1.3.6.1.4.1.2021.10.1.4.3 laConfig Load-15 .1.3.6.1.4.1.2021.10.1.5.1 laLoadInt Load-1 .1.3.6.1.4.1.2021.10.1.5.2 laLoadInt Load-5 .1.3.6.1.4.1.2021.10.1.5.3 laLoadInt Load-15
CPU 占用信息	.1.3.6.1.4.1.2021.11.50.0 ssCpuRawUser .1.3.6.1.4.1.2021.11.51.0 ssCpuRawNice

	.1.3.6.1.4.1.2021.11.52.0 ssCpuRawSystem .1.3.6.1.4.1.2021.11.53.0 ssCpuRawIdle .1.3.6.1.4.1.2021.11.59.0 ssRawInterrupts .1.3.6.1.4.1.2021.11.60.0 ssRawContexts
CPU 使用率	.1.3.6.1.4.1.2021.11.9.0 ssCpuUser

6.5. 告警对象列表

对象类型	监控对象	对象属性
系统	CPU	CPU 温度
		CPU 使用率
	授权	授权剩余天数
	SYN	SYN PPS
		SYN PPS 与 SYN ACK PPS 的比值
	SYNACK	SYNACK PPS
	连接数	总连接数
		总连接数使用率
	IP 数	总 IP 数使用率
		总 IP 数
网卡	任意网卡	流入速率
		流出速率
		网卡状态
		网卡流入带宽使用率
		网卡流出带宽使用率
		网卡总带宽使用率
	具体网卡（网卡 a、网卡 b）	同“任意网卡”
WAN 线路	任意 WAN 线路	流入速率
		流出速率
		心跳时延
		线路状态
	具体 WAN 线路（线路 a、线路 b）	同“任意 WAN 线路”
内网 IP	任意内网 IP	连接数

		会话应用
应用协议	应用协议特征库	上行速率
		下行速率
		连接数
流量统计对象	任意流量统计对象	上行速率
		下行速率
		上行流量
		下行流量
	具体流量统计对象（对象 a、对象 b）	同“任意流量统计对象”