



# 版本发行更新说明

核心代号：Panabit TANG(唐)r7

文档版本 V24.12.30

归档日期 2024-12-31

Copyright©2024 北京派网

## 版权声明

Copyright©2024 北京派网

保留对本文档及声明的一切权力。

未经北京派网的书面许可，任何单位和个人不得以任何方式或形式对本文档的部分或全部内容进行转印、影印、复制、摘要、修改、翻译成其他语言、将其部分或全部用于商业用途。

## 版本修订

北京派网保留不预先通知客户而修改本文档所含内容的权力。

## 责任限定

您所购买的产品、服务或特性等受商业合同和条款的约束，本文档中描述的部分或全部产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，北京派网对本文档内容不做任何明示或默示的声明或保证。北京派网对于您的使用或不能使用本产品或功能而发生的任何损害不负任何赔偿责任，包括但不限于直接、间接的、附加的个人损害或商业损失或任何其他损失。

由于产品版本升级或其他原因，本文档内容会不定期进行更新，北京派网在编写本手册时已尽力保证其内容准确可靠，但并确保手册内容完全没有错误或遗漏，本文档的所有信息也不构成任何明示或暗示的担保。

# 前言

## 读者对象

本文档适合下列人员阅读

- 网络工程师
- 网络维护管理人员
- 对本产品有兴趣的网络爱好者

## 技术支持

北京派网官方网站: <https://www.panabit.com/>

北京派网官方技术论坛: <https://bbs.panabit.com/forum.php>

北京派网技术服务热线: 400-773-3996






北京派网技术支持于反馈邮箱: [support@panabit.com](mailto:support@panabit.com)

## 文档约定

### 1. 图形界面符号约定

图标格式	解释	示例
【】	窗口名、菜单项、按钮和子模块名	【流量概况】
<注释 n>	对页面部分模块的说明与解释	<注释 6>显示提醒信息
>>	用于隔开多级菜单	【系统概况】>>【流量概况】

### 2. 标志符号约定

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

### 3. 说明

本文档中展示的部分信息（如产品型号、描述、软件界面等）仅供参考，具体信息请以实际使用的产品版本为准。

# 目 录

前 言 .....	3
目 录 .....	4
<b>1. 版本信息 .....</b>	<b>6</b>
<b>2. 新增功能 .....</b>	<b>8</b>
2.1. iWAN 二层交换 .....	8
2.2. iWAN 分段路由(SR 路由) .....	15
2.3. DHCPv6 有状态地址分配 .....	23
2.4. IDS 入侵检测 .....	24
2.5. 主动 DNS 域名解析 .....	32
<b>3. 功能优化 .....</b>	<b>33</b>
3.1. DNAT 功能优化 .....	33
3.2. 微信认证流程优化 .....	34
3.3. 共享限速模块优化 .....	35
3.4. 优化域名群组匹配 .....	35
3.5. 优化端口映射配置导入 .....	36
3.6. 用户地址池支持 IPV6 前缀 .....	36
3.7. 流媒体支持高码流超清频道 .....	37
3.8. 连接信息支持 IPv6 前缀查询 .....	37
3.9. 支持配置 IPv4 本地链路地址 .....	38
3.10. SLAAC 支持多 VLAN 下发 IPv6 .....	38
3.11. DHCPv4 WAN 线路支持 Option .....	40
3.12. 代拨场景内层 QinQ 支持 VLAN 范围 .....	41
3.13. iWAN 和 L2TP 客户端的域名解析优化 .....	42
3.14. 单个 SSID 最大接入终端数支持 254 个 .....	42
3.15. 携带 IPv6 本地链路地址时用户无感知上线失败 .....	42
<b>4. 界面优化 .....</b>	<b>43</b>
4.1. 支持 Panabit 系统日志导出 .....	43
4.2. 新增 WEB 应急恢复页面 .....	44

4.3.	LAN/WAN 接口导出优化 .....	44
4.4.	MAC 重复绑定提示 .....	45
4.5.	批量账号导入异常 .....	45
4.6.	删除重复引用 IP 群组时无提示 .....	46
<b>5.</b>	<b>BUG 修复 .....</b>	<b>47</b>
<b>6.</b>	<b>应用识别 .....</b>	<b>48</b>
6.1.	新增应用 .....	48
6.2.	更新应用 .....	49
<b>7.</b>	<b>升级说明 .....</b>	<b>51</b>
7.1.	支持说明 .....	51
7.2.	前置条件 .....	51
7.3.	注意事项 .....	51
7.4.	升级流程 .....	51

## 1. 版本信息

核心代号	TANG（唐）r7
版本类型	正式版本
适用产品	Panabit
适用客户	通用
发布日期	2024 年 12 月 30 日
新增功能	<ol style="list-style-type: none"><li>1. iWAN 二层交换</li><li>2. iWAN 分段路由(SR 路由)</li><li>3. DHCPv6 有状态地址分配</li><li>4. IDS 入侵检测</li><li>5. 主动 DNS 域名解析</li></ol>
功能优化	<ol style="list-style-type: none"><li>1. DNAT 功能优化</li><li>2. 微信认证流程优化</li><li>3. 共享限速模块优化</li><li>4. 优化域名群组匹配</li><li>5. 优化端口映射配置导入</li><li>6. 用户地址池支持 IPV6 前缀</li><li>7. 流媒体支持高码流超清频道</li><li>8. 连接信息支持 IPv6 前缀查询</li><li>9. 支持配置 IPv4 本地链路地址</li><li>10. SLAAC 支持多 VLAN 下发 IPv6</li><li>11. DHCPv4 WAN 线路支持 Option</li><li>12. 代拨场景内层 QinQ 支持 VLAN 范围</li><li>13. iWAN 和 L2TP 客户端的域名解析优化</li><li>14. 单个 SSID 最大接入终端数支持 254 个</li><li>15. 携带 IPv6 本地链路地址时用户无感知上线失败</li></ol>
界面优化	<ol style="list-style-type: none"><li>1. 支持 Panabit 系统日志导出</li><li>2. 新增 WEB 应急恢复页面</li><li>3. LAN/WAN 接口导出优化</li><li>4. MAC 重复绑定提示</li></ol>

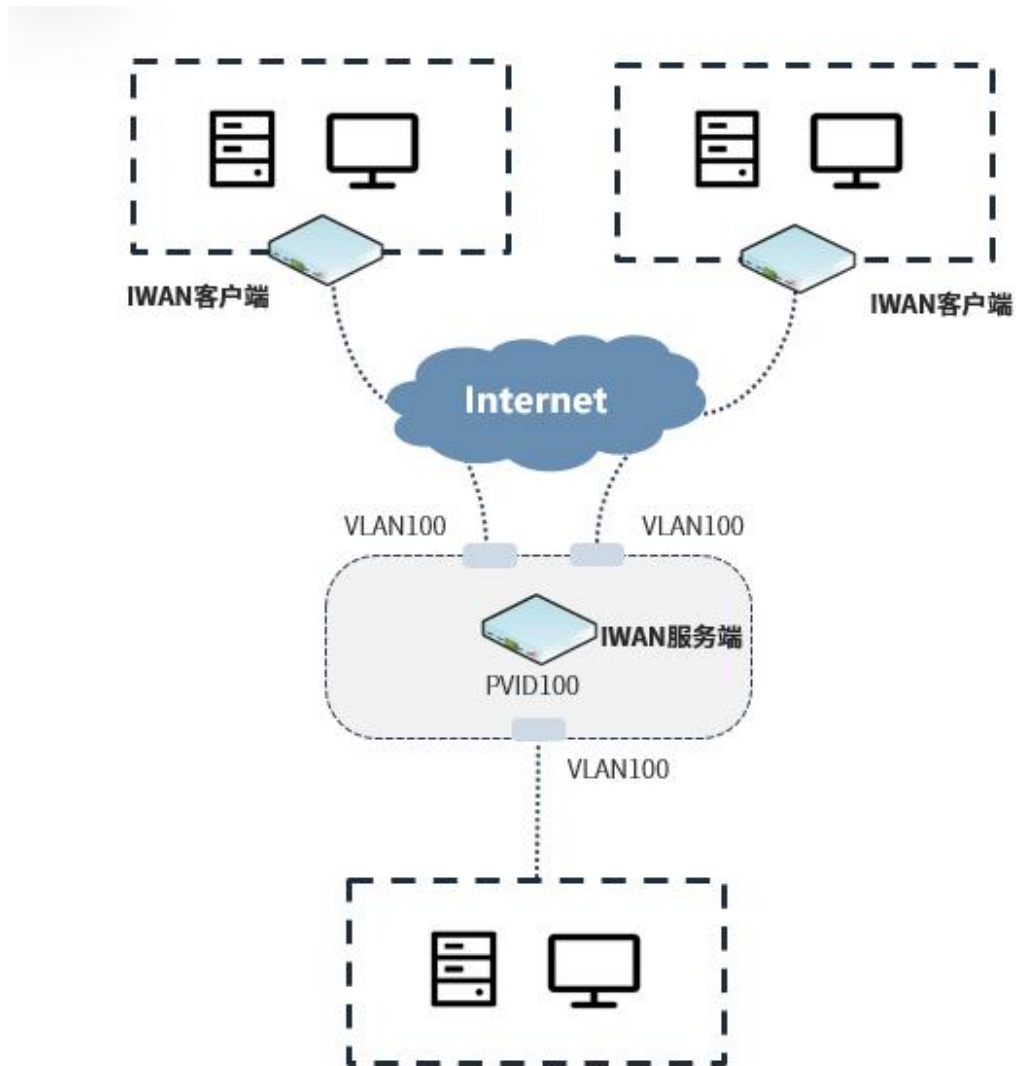
	5. 批量账号导入异常 6. 删除重复引用 IP 群组时无提示
BUG 修复	详见 BUG 修复
应用识别	详见应用识别

## 2. 新增功能

### 2.1. iWAN 二层交换

#### 应用场景

实现在三层网络的基础上建立二层以太网网络隧道，从而实现跨三层、跨地域的二层网络互连。



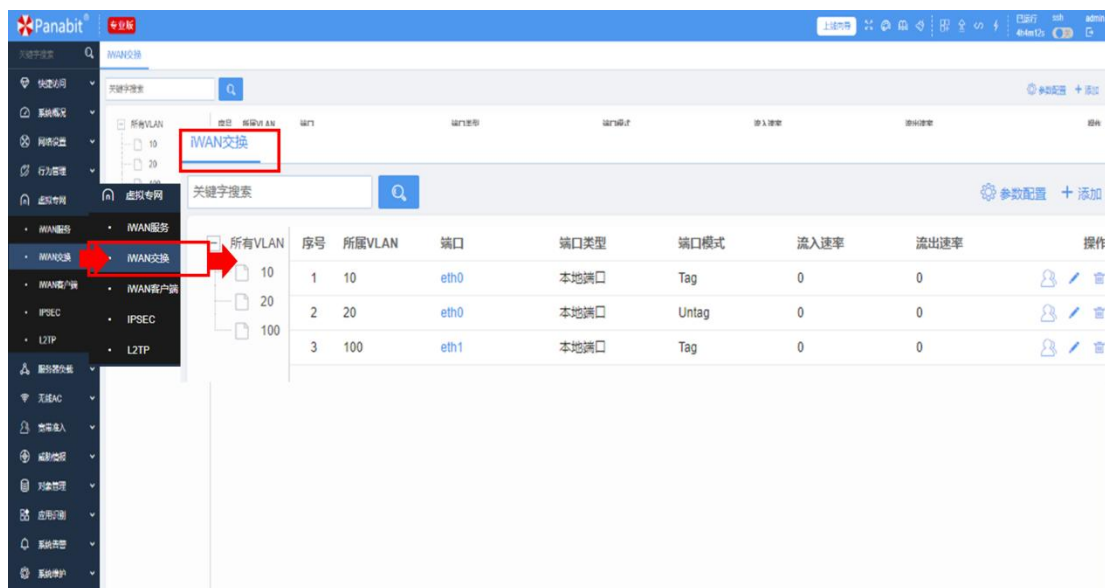
#### 说明

- 1、iWAN 内建立一台虚拟 L2 交换机，实现基于 MAC 地址的寻址转发
- 2、标准版不支持此功能，请升级 Panabit 版本至专业版。



## 实现原理

iWAN 服务端建立并维护接入客户端的 ARP 表项, 将服务端的本地物理端口与 iWAN 客户端组成虚拟二层局域网。



## 参数释义

序号	参数	备注
1	ID	策略序号
2	所属 VLAN	802.1Q VLAN 标签
3	端口类型	本地端口, iWAN server 端的物理端口; 远程端口, 接入 iWAN server 的 iWAN 客户端;
4	端口模式	TAG 模式, 从端口进入的数据包必须携带对应的 VLAN ID, 从端口出去的数据包也会打上对应的 VLAN ID。 UNTAG 模式, 从端口进入的数据包不能携带 VLAN, 从端口出去的数据包也不会携带 VLAN。
5	流入速率	当前端口流入速率
6	流出速率	当前端口流出速率
7	MAC	当前 VLAN 学习到且未老化的 MAC 地址

## 二层转发

在【网络配置】>>【LAN/WAN】>>【WAN 线路】>>iWAN 类型 WAN 线路中新增二层转发选项。

新增参数：功能开关、本地网卡、本地 VLAN、转发 VLAN。

添加

名称

线路类型

iWAN

网卡/承载线路

eth4

备注

IPv6

关闭

开启后，线路同时支持IPv4 和 IPv6

服务器IP/域名

服务器端口

8000

iWAN账号

iWAN密码

加密

● 关闭

二层转发

开启

分段标识

0

本地网卡

eth1

本地VLAN

0

① 范围：0-4095

转发VLAN

0

范围：0-4095，0表示不开启二层转发

高级

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

确定

取消

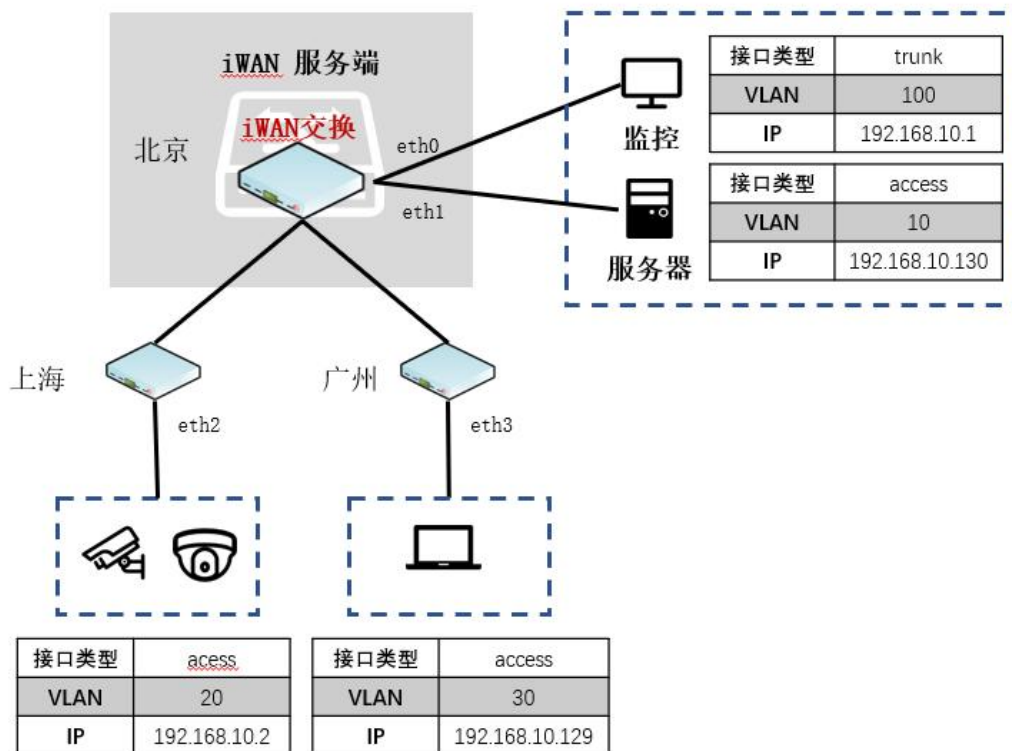
## 参数释义

序号	参数	备注
1	二层转发	开启/关闭客户端二层转发功能
2	本地网卡	选择客户端参与二层转发的本地物理网卡
3	本地 VLAN	配置 VLAN ID 【0-4095】 当本地网卡接收报文 VLAN 与【本地 VLAN】相同，且目标 MAC 与 LAN/WAN 线路 MAC 不重复时，匹配报文将被 iWAN 隧道转发到 iWAN 服务器端。
4	转发 VLAN	iWAN 服务端根据转发 VLAN，自动添加为对应 VLAN 的远

10

		<p>程端口。</p> <p>1) 当【本地 VLAN】=0, Panabit 将在数据包增加参数指定的值后从隧道发送至服务端;</p> <p>2) 当【本地 VLAN】≠0, Panabit 将数据包 VLAN TAG 改成【转发 VLAN】配置的 VLAN TAG 后从隧道发送至服务端</p>
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------

### 配置举例



### 业务需求

- ① 上海分公司视频监控需回传至总部监控系统
- ② 广州分公司 PC 需访问总部服务器资源
- ③ 监控业务与访问服务器二层 VLAN 隔离

### 配置思路

设备配置分为四个部分:

#### a) 转发 VLAN 规划

序号	名称	iWAN 转发 VLAN
1	监控业务	100
2	服务器业务	10

以服务端内网 VLAN 保持一致

## b) 北京服务端配置

序号	名称	步骤项	备注
1	北京服务端配置	互通性配置	WAN/LAN 线路
		iWAN 服务配置	配置 iWAN 服务 配置服务映射
		iWAN 用户	配置用户地址池 配置 iWAN 用户账号
		iWAN 交换	开启 iWAN 二层转发 【虚拟专网】>>【iWAN 交换】>>【参数配置】>>开启>>确定 添加监控 VLAN 【添加】>>【VLAN】100、【端口】eth0、【端口模式】Tag 模式 添加服务器 VLAN 【添加】>>【VLAN】10、【端口】eth1、【端口模式】Untag 模式

iWAN交换

关键字搜索

[参数配置](#) [+ 添加](#)

所有VLAN	序号	所属VLAN	端口	端口类型	端口模式	流入速率	流出速率	操作
<input checked="" type="checkbox"/> 100	1	100	eth0	本地端口	Tag	0	0	<a href="#">用户</a> <a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/> 10	2	10	eth1	本地端口	Untag	0	0	<a href="#">用户</a> <a href="#">编辑</a> <a href="#">删除</a>

< 1 > 到第 1 页 确定 共 2 条 100 条/页

## c) 上海客户端配置

序号	名称	步骤项	备注
2	上海客户端配置	互通性配置	WAN/LAN 线路
		iWAN 线路	添加 iWAN 线路 服务端 IP/端口、iWAN 账号/密码、开启二层转发、本地网卡【填写 eth2】、本地 VLAN【0】、转发 VLAN【100】
		策略路由	添加上网路由： 目的 IP【any】、线路【WAN 线路】、动作【NAT】的策略路由

参数设置    当前状态    TOP应用    实时流量    历史趋势    线路日志

名称

iWAN上海

线路类型

iWAN

网卡/承载线路

外网

备注

IPv6

关闭

开启后，线路同时支持IPv4 和 IPv6

服务器IP/域名

10.10.10.10

服务器端口

8000

iWAN账号

test

iWAN密码

test

加密

● 关闭

二层转发

开启

分段标识

1

本地网卡

eth2

本地VLAN

0

① 范围：0-4095

转发VLAN

100

范围：0-4095，0表示不开启二层转发

心跳服务器1

0.0.0.0

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

0.0.0.0

同上,任何一个IP通都表示心跳正常

最大时延

0

心跳时延连续 5 次超出则心跳失效; 0表示忽略

DNS代理

关闭

① 说明

MTU

1420

确定

## d) 广州客户端配置

序号	名称	步骤项	备注
3	广州客户端配置	互通性配置	WAN/LAN 线路
		iWAN 线路	添加 iWAN 线路 服务端 IP/端口、iWAN 账号/密码、开启二层转发、本地网卡【eth3】、本地 VLAN【30】、转发 VLAN【10】
		策略路由	添加上网路由： 目的 IP【any】、线路【WAN 线路】、动作【NAT】的策略路由

参数设置

当前状态

TOP应用

实时流量

历史趋势

线路日志

名称

iWAN广州

线路类型

iWAN

网卡/承载线路

外网

备注

iWAN参数

IPv6

关闭

开启后，线路同时支持IPv4 和 IPv6

服务器IP/域名

10.10.10.10

服务器端口

8000

iWAN账号

test

iWAN密码

test

加密

关闭

二层转发

开启

分段标识

1

本地网卡

eth3

本地VLAN

30

范围：0-4095

转发VLAN

10

范围：0-4095，0表示不开启二层转发

高级

心跳服务器1

0.0.0.0

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

0.0.0.0

同上,任何一个IP通都表示心跳正常

最大时延

0

心跳时延连续 5 次超出则心跳失效；0表示忽略

DNS代理

关闭

说明

MTU

1420

确定

## 2.2. iWAN 分段路由(SR 路由)

### 应用场景

iWAN 作为 Panabit SD-WAN 解决方案的关键技术，由于其高度的灵活性和超高的转发性能，越来越多的 SD-WAN 运营客户将其作为组网的核心技术方案。为了进一步提升如下应用需求：

#### ➤ 多租户

以 SD-WAN 运营为目的的网络内，分支节点的 IP 地址不可避免地会出现重复情况，无法以路由的方式转发数据。

#### ➤ 数据保密性

当前 CPE 接入到 POP 点后，POP 点需要对数据包进行解包处理，无法满足用户数据保密性需求。

### 实现原理

Panabit 在现有 iWAN 组网技术基础上引入了分段路由（Segment Routing，以下简称 SR）技术。SR 是一种根据事先设定好的转发路径（Path）来转发数据包的路由技术，SR 技术有以下特点：

1) **标签转发：**数据包的转发是基于事先设定好的路径，路径就是一段段（Segment）连接起来的有序的 Segment List，路径是全局唯一的。

2) **端到端加密：**中间转发节点（POP 点）只依据数据包中的路径来转发数据包，不对数据包做更深层次的解包处理，POP 点不关心数据包的任何 payload，payload 可以是传统的 IP 包，也可以是非 IP 包。

路径的全局唯一性和 POP 点不解包特性，完美地解决了多租户及用户数据泄密担忧问题。



注意

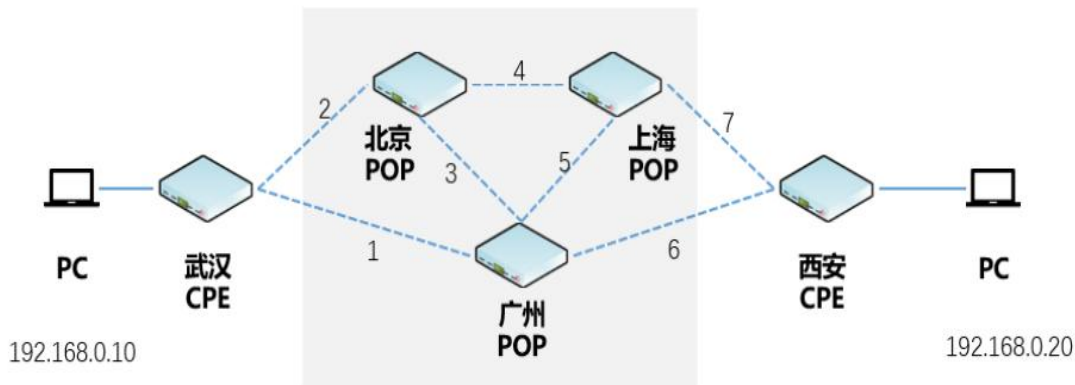
标准版不支持此功能，请升级 Panabit 版本至专业版。

---

## 分段路由特性

### ➤ 分段标识

CPE 和 POP，POP 和 POP 之间的连接称为分段（Segment），为了标识该分段，给每个分段赋予一个唯一的标识，这个标识称之为分段 ID。



 **注意** 分段标识在运营网络内的 Panabit 不能重复，分段标识字段设置范围为【1-2<sup>32</sup>】

添加 ×

名称: iWAN北京

线路类型: iWAN

网卡/承载线路: 外网

备注:

**iWAN参数**

IPv6: 关闭 开启后，线路同时支持IPv4 和 IPv6

服务器IP/域名:

服务器端口: 8000

iWAN账号:

iWAN密码:

加密: ☒ 关闭

二层转发: 关闭

**分段标识: 1**

**高级**

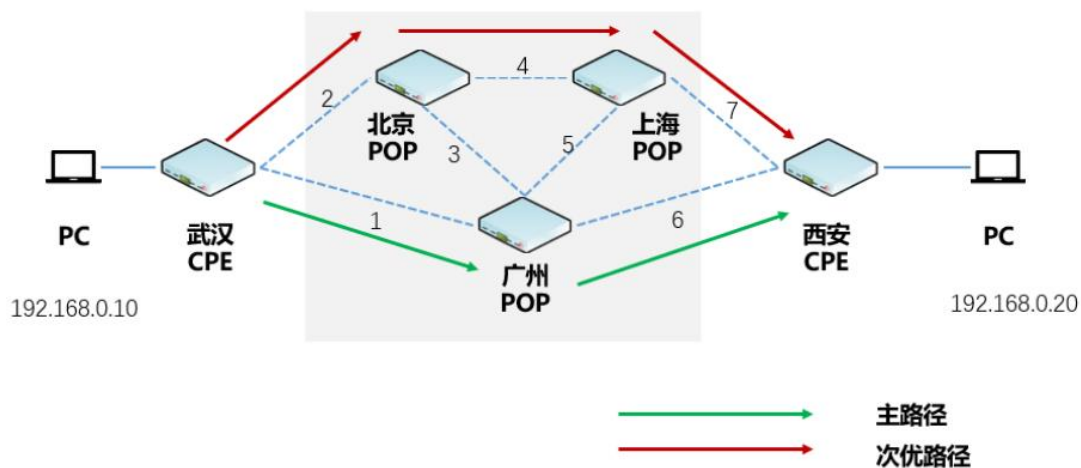
心跳服务器1:  通过ping此IP来对线路做健康检查,为空表示关闭

心跳服务器2:  同上,任何一个IP通都表示心跳正常



➤ 转发路径（Routing Path）。

转发路径就是由若干个分段标识组成的一个有序的分段标识列表，按照列表数值的排列顺序不同而不同，所以“2，4，7”和“7，4，2”是两条不同的转发路径。



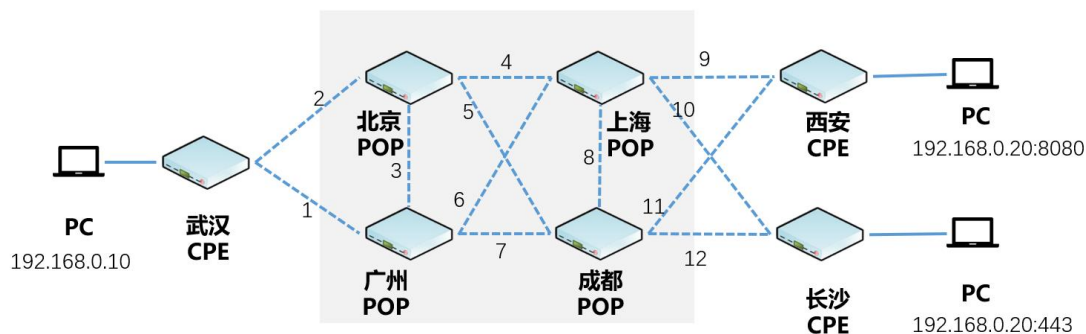
注意

- 1、目前 Panabit 支持的最长 SR 转发路径为 6 跳
- 2、Panabit 的 SR 会话数据基于分段标识转发，为保证数据私密性，SR 数据经过的中间 Panabit 节点内无法在 TOP 用户内查看 SR 会话。

## 配置举例

内容服务商通过 Panabit 设备搭建 SD-WAN 网络，为接入的用户业务加速、异地互联等业务。

对有异地互联业务需求的用户提供最近的接入 POP 点信息和分配的【线路标签】，各分支和总部通过 iWAN 接入 SD-WAN 网络。通过配置分段路由实现异地互联。



### (1) 业务需求

- ① 北京上海广州建设 POP 运营网络
- ② 武汉客户 PC 需要访问西安客户 PC
- ③ 武汉客户 PC 需要访问长沙客户 PC
- ④ 任意 POP 节点故障一台不影响客户业务

### (2) SR 路由规划

业务名称	优先级	业务路径	分段路由转发路径
武汉-西安	主链路	武汉-广州-成都-西安	1-7-11
	备用链路	武汉-北京-上海-西安	2-4-9
武汉-长沙	主链路	武汉-广州-成都-长沙	1-7-12
	备用链路	武汉-北京-上海-长沙	2-4-10

### (3) 配置思路

配置主要分为两个部分：POP 点（4 台），CPE（2 台）

## 服务端配置

POP 节点配置数据类似，下文以北京 POP 节点配置为例进行说明

序号	名称	配置类别	配置项	备注
1	北京 POP	基础配置	连通性配置	WAN/LAN 线路
		iWAN 服务	iWAN 服务配置	iWAN 服务、服务映射
			iWAN 用户	用户地址池、武汉 iWAN 用户账号
		iWAN 互联	POP 互联-上海	【网络设置】>>【WAN/LAN】>>添加上海 iWAN 线路>>分段标识设置为 4
			POP 互联-广州	【网络设置】>>【WAN/LAN】>>添加广州 iWAN 线路>>分段标识设置为 3
			POP 互联-成都	【网络设置】>>【WAN/LAN】>>添加广州 iWAN 线路>>分段标识设置为 5
		结果验证	互联检查	【系统概况】>>【在线用户】中确认互联 Panabit 的 iWAN 账号是否在线。

## 客户端配置

序号	名称	配置类别	配置项	备注
1	武汉 CPE	基础配置	连通性配置	WAN/LAN 线路
		iWAN 互联	POP 互联-北京	【网络设置】>>【WAN/LAN】>>添加上海 iWAN 线路>>分段标识设置为 2
			POP 互联-广州	【网络设置】>>【WAN/LAN】>>添加广州 iWAN 线路>>分段标识设置为 1
		iWAN SR 转发路径	SR 转发路径-西安主	【网络设置】>>【WAN/LAN】>>添加线路>>【线路类型】iWAN-SR>>【转发路径】2, 4, 9
			SR 转发路径-西安备	【网络设置】>>【WAN/LAN】>>添加线路>>【线路类型】iWAN-SR>>【转发路径】1, 7, 11
			SR 转发路径-长沙主	【网络设置】>>【WAN/LAN】>>添加线路>>【线路类型】iWAN-SR>>【转发路径】1, 7, 12
			SR 转发路径-长沙备	【网络设置】>>【WAN/LAN】>>添加线路>>【线路类型】iWAN-SR>>【转发路径】2, 4, 10
		SR 路由	武汉-西安主	【网络设置】>>【路由/NAT】>>【IPv4】添加策略>>【匹配条件】192.168.0.20: 8080>>【执行动作】路由>>【路由线路】
			武汉-西安备	【网络设置】>>【路由/NAT】>>【IPv4】添加策略>>【匹配条件】192.168.0.20: 8080>>【执行动作】路由>>【路由线路】
			武汉-长沙主	【网络设置】>>【路由/NAT】>>【IPv4】添加策略>>【匹配条件】192.168.0.20: 443>>【执行动作】路由>>【路由线路】
			武汉-长沙备	【网络设置】>>【路由/NAT】>>【IPv4】添加策略>>【匹配条件】192.168.0.20: 443>>【执行动作】路由>>【路由线路】
			结果验证	数据转发验证 策略路由顺序检查

## 西安客户端配置

序号	名称	配置类别	配置项	备注
1	西安 CPE	基础配置	连通性配置	WAN/LAN 线路
		iWAN 互联	POP 互联-上海	【网络设置】>>【WAN/LAN】>>添加上海 iWAN 线路>>分段标识设置为 9
			POP 互联-成都	【网络设置】>>【WAN/LAN】>>添加成都 iWAN 线路>>分段标识设置为 11
		iWAN SR 转发路径	SR 转发路径-武汉主	【网络设置】>>【WAN/LAN】>>添加线路>>【线路名称】SR 武汉主>>【线路类型】iWAN-SR>>【转发路径】9, 4, 2
			SR 转发路径-武汉备	【网络设置】>>【WAN/LAN】>>添加线路>>【线路名称】SR 武汉备>>【线路类型】iWAN-SR>>【转发路径】11, 7, 1
		SR 路由	武汉-西安回指路由主	【网络设置】>>【路由/NAT】>>【IPv4】添加策略>>【匹配条件】192.168.0.10>>【执行动作】路由>>【路由线路】SR 武汉主
			武汉-西安回指备	【网络设置】>>【路由/NAT】>>【IPv4】添加策略>>【匹配条件】192.168.0.10>>【执行动作】路由>>【路由线路】SR 武汉备
			结果验证	数据转发验证 策略路由顺序检查

### 长沙客户端配置

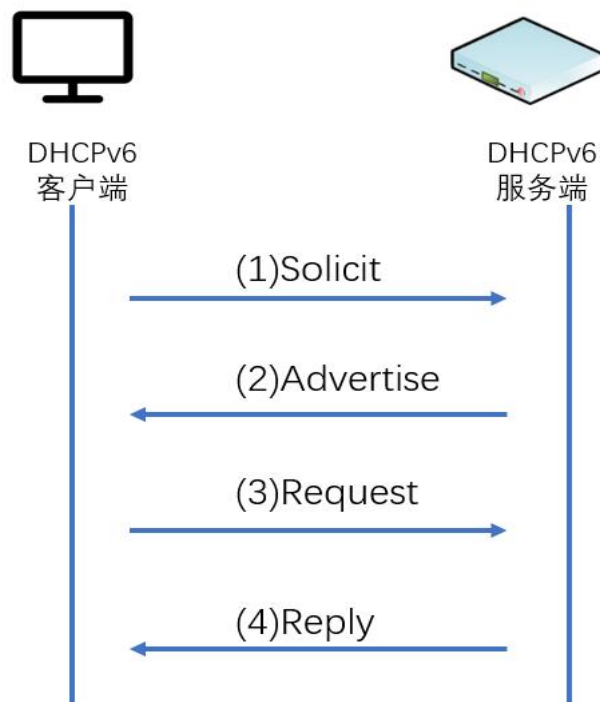
序号	名称	配置类别	配置项	备注
1	长沙 CPE	基础配置	连通性配置	WAN/LAN 线路
		iWAN 互联	POP 互联 - 上海	【网络设置】>>【WAN/LAN】>>添加上海 iWAN 线路>>分段标识设置为 10
			POP 互联 - 成都	【网络设置】>>【WAN/LAN】>>添加成都 iWAN 线路>>分段标识设置为 12
		iWAN SR 转发路径	SR 转发路径-武汉主	【网络设置】>>【WAN/LAN】>>添加线路>>【线路名称】SR 武汉主>>【线路类型】iWAN-SR>>【转发路径】12, 7, 1
			SR 转发路径-武汉备	【网络设置】>>【WAN/LAN】>>添加线路>>【线路名称】SR 武汉备>>【线路类型】iWAN-SR>>【转发路径】10, 4, 2
		SR 路由	武汉-西安回指路由主	【网络设置】>>【路由/NAT】>>【IPv4】添加策略>>【匹配条件】192.168.0.10>>【执行动作】路由>>【路由线路】SR 武汉主
			武汉-西安回指备	【网络设置】>>【路由/NAT】>>【IPv4】添加策略>>【匹配条件】192.168.0.10>>【执行动作】路由>>【路由线路】SR 武汉备
			结果验证	数据转发验证 策略路由顺序检查

## 2.3. DHCPv6 有状态地址分配

### 应用场景

DHCPv6 客户端向 DHCPv6 服务器发送配置申请报文(申请包括 IPv6 地址、DNS 服务器地址等参数)，服务器根据策略返回携带相应配置信息的报文。

### 解决方案



DHCPv6 交互地址分配过程如下：

1) DHCPv6 客户端发送 Solicit 报文，请求 DHCPv6 服务器为其分配 IPv6 地址和网络配置参数。

2) DHCPv6 服务器回复 Advertise 报文，通知客户端可以为其分配的地址和网络配置参数。

3) 如果 DHCPv6 客户端接收到多个服务器回复的 Advertise 报文，则根据 Advertise 报文中的服务器优先级等参数，选择优先级最高的一台服务器，并向所有的服务器发送 Request 组播报文，该报文中携带已选择的 DHCPv6 服务器的 DUID。

4) DHCPv6 服务器回复 Reply 报文，确认将地址和网络配置参数分配给客户端使用。

### IPv6 地址分配相关功能

IPv6 配置方式	功能描述	应用场景
-----------	------	------

手动配置	手动配置 IPv6 地址/前缀及其他如 DNS 等网络配置参数。	配置静态 IPv6
DHCPv6 中继	客户端使用 Solicit 报文确定 DHCPv6 服务端的位置，并使用 Request 报文请求 IPv6 地址/前缀和其他网络配置信息。	DHCPv6 服务中继
DHCPv6 PD 前缀代理	DHCPv6 PD 允许网络设备（如路由器）向上游网络设备请求一个较大的 IPv6 地址前缀，然后将这个前缀划分为更小的前缀分配给下游设备	内网未部署 DHCPv6 服务器时常用的 IPv6 地址获取方式
DHCPv6 有状态自动分配	DHCPv6 服务器自动分配 IPv6 地址/前缀以及其他如 DNS 服务地址等其他网络配置参数。	集中式内网纯 PC 管理场景

### 配置举例

【网络管理】>>【LAN/WAN】>>【LAN 线路】中点击已添加的 V6 LAN 线路：

- 1) 配置【DHCPv6 地址范围】，填写可用的 IPV6 客户端地址范围即可。
- 2) 【地址分配】修改为开启状态。
- 3) 如需指定 VLAN 分配 DHCPv6，在【分配 VLAN】中输入指定的 VLAN ID。



注意

本文中提到的所有 IPv6 相关的功能，均需 IPV6 识别功能为开启状态。

开启方式为【应用识别】>>【引擎参数】>>【参数设置】>>【IPv6 流量识别】

## 2.4. IDS 入侵检测

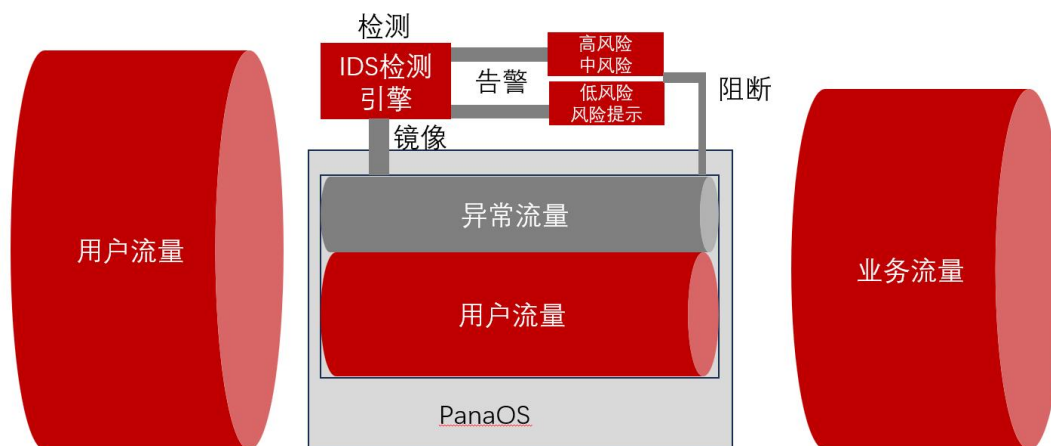
入侵检测系统（Intrusion Detection System，简称“IDS”）是一种网络安全技术，主要用于监测网络或系统中可能存在的入侵行为，帮助用户检测网络



中的异常行为，如攻击、病毒、蠕虫等，并及时发出告警或阻断。

### 实现原理

IDS 入侵检测引擎根据内置规则库对 PanaOS 预选流量进行检测，对匹配的异常会话生成日志告警或阻断指令到 PanaOS 进行流量阻断。



### 支持型号

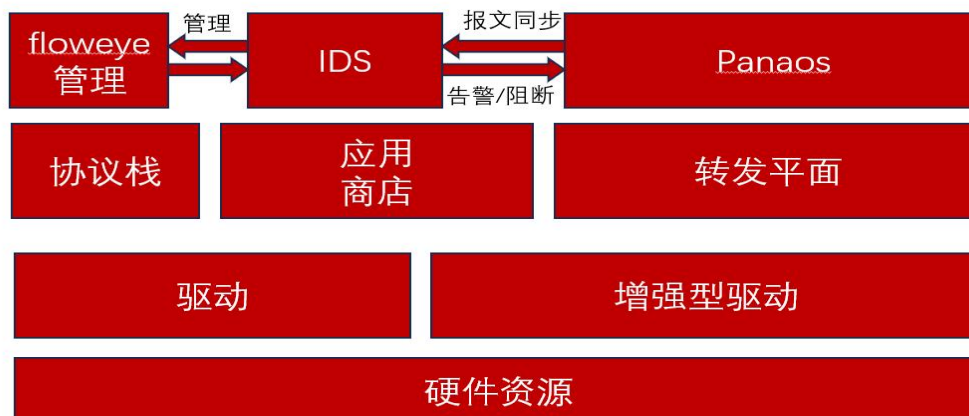
开启 IDS 功能需要消耗较多内存及单独的处理单元，目前支持以下硬件型号：

IDS 支持型号	AX40、AX120、AX10K
	PX7C、PX30C
	PX6Z、PX7S

### 功能特点

#### ➤ 业务数据转发无延迟

IDS 检测引擎为旁路并行处理架构，在解决网络安全需求的同时，降低业务数据转发延迟。





- 1、Panabit IDS 使用独立管理平面运行，不影响正常业务数据转发
- 2、标准版不支持此功能，请升级 Panabit 版本至专业版。

#### ➤ 七层应用 DPI+入侵检测 IDS

利用 Panabit 七层应用识别优势，对经由 Panabit 识别为正常的流量，无需 IDS 二次检测，在提高 IDS 检测效率的同时降低对系统性能消耗。

名称	参数
查看过滤白名单	floweye paids list
添加白名单应用	floweye paids config appenable=[appname]
删除白名单应	floweye paids config appdisable=[appname]

#### ➤ 安全强大的实时监控和防御能力

内置 15 大类常见的网络威胁特征，快速发现异常行为，及时发出警报，使组织能够迅速采取措施应对可能存在的信息泄露或攻击风险。

类型	内容
漏洞 (Vulnerability)	指信息系统中存在的、可被利用的安全缺陷。攻击者可以通过这些漏洞获得未经授权的访问权限，或造成其他损害。
木马 (Trojan Horse)	一种恶意软件，通常伪装成合法程序诱骗用户安装。一旦激活，它可以窃取信息、破坏数据或允许攻击者远程控制受感染的计算机。
Web 攻击 (Web Attack)	指针对网站或 Web 应用的安全威胁，如 SQL 注入、跨站脚本 (XSS)、文件上传漏洞等，目的是盗取敏感数据、篡改网页内容或中断服务。
恶意攻击 (Malicious Attack)	泛指所有出于恶意目的而实施的攻击行为，包括但不限于病毒传播、数据盗窃、服务中断等。
扫描 (Scanning)	攻击者使用自动化工具探测目标系统的开放端口、服务及存在的漏洞，为后续的攻击做准备。
非法访问 (Unauthorized Access)	指未经授权擅自进入计算机系统或网络的行为，常通过利用漏洞或猜测密码等方式实现。
病毒 (Virus)	一种寄生型的恶意软件，附着于正常程序之中，当宿主程序运行时激活，可自我复制并传播到其他程序或文件中，造成破坏或信息泄露。
蠕虫 (Worm)	一种能够独立运行并通过网络传播的恶意软件，不需要附着在其他程序上，常用于消耗带宽、破坏系统或传播其他恶意软件。

后门 (Backdoor)	攻击者在系统中留下的秘密入口，以便日后未经正式授权再次进入系统。有时开发者也会故意设置后门以便维护。
拒绝服务攻击 (Denial of Service, DoS)	通过大量无效请求使目标服务器过载，导致合法用户无法访问服务。分布式拒绝服务攻击（DDoS）则是由多台被控制的计算机同时发起攻击。
跨站脚本攻击 (Cross-Site Scripting, XSS)	攻击者通过在 Web 页面中插入恶意脚本代码，当用户浏览该页面时，恶意脚本将在用户的浏览器中执行，可能导致敏感信息泄露或会话劫持。
恶意软件 (Malware)	泛指所有设计用来损害计算机系统、收集敏感信息或未经用户同意执行操作的软件，包括病毒、木马、蠕虫等。
设备安全 (Device Security)	指保护硬件设备及其操作系统免受物理损坏、未经授权访问和其他安全威胁的技术和策略。
缓冲区溢出 (Buffer Overflow)	当程序试图向缓冲区写入超出其容量的数据时发生的一种编程错误。攻击者可以利用这种漏洞执行任意代码、篡改数据或导致程序崩溃。
注入攻击 (Injection Attack)	攻击者将恶意代码插入到程序的输入数据中，当程序处理这些输入时，恶意代码被执行。常见的类型有 SQL 注入、命令注入等。

### ➤ 用户自定义 IDS 规则库编排

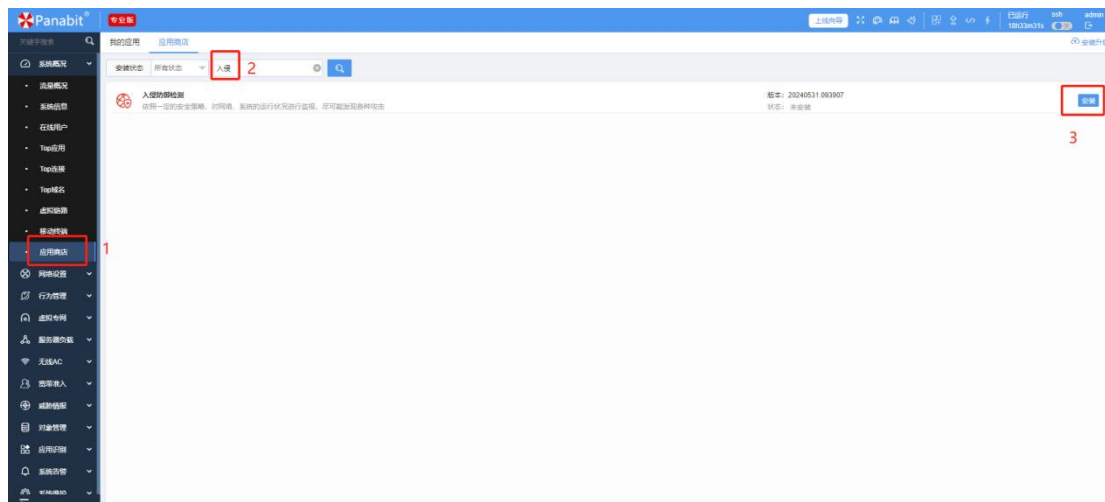
设备默认对全部流量进行全量规则匹配，支持用户自定义规则组对特定五元组流量进行筛选检查，提高 IDS 威胁检测效率，降低设备性能消耗。

### ➤ 自动绑定空闲处理单元

开启 IDS APP 时，优先使用设备空闲处理单元，如无空闲单元则绑定管理单元。

## 下载安装

### 应用商店在线安装



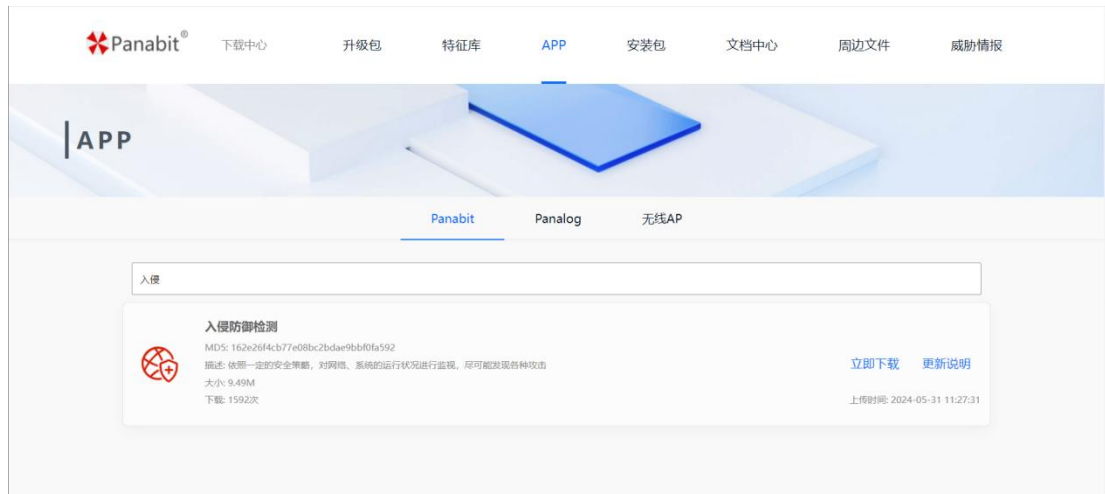


注意

- 1、需要管理口（MGT）支持访问互联网。
- 2、管理口配置可用的 DNS 服务器。

## 离线安装

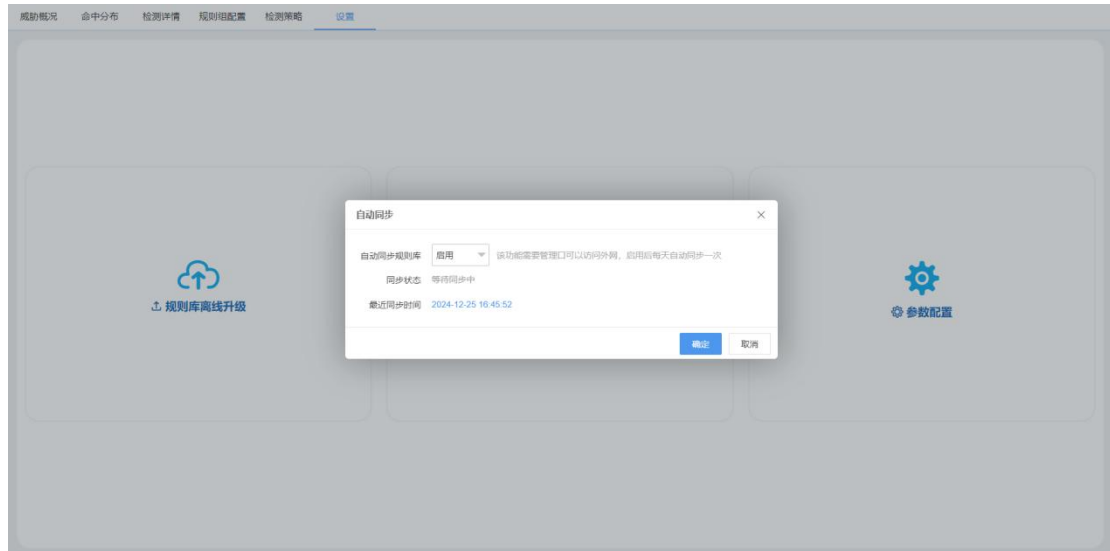
官网下载：<https://download.panabit.com:9443/app.php>



## 首次使用

### 规则库升级

入侵防御 APP>>【设置】>>【规则库自动升级】>>【自动同步规则库】>>【启用】



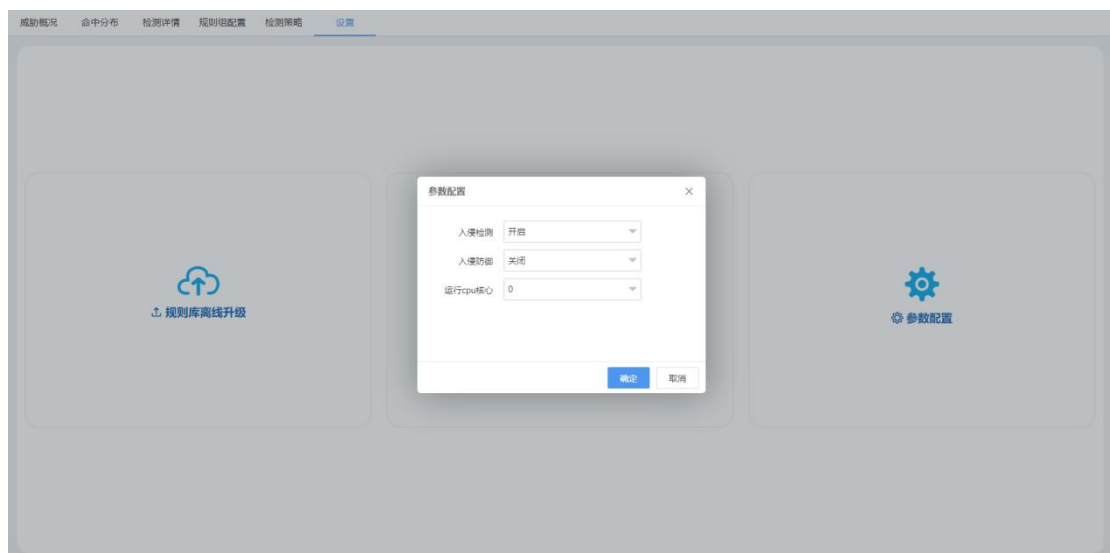
### 说明

1、同步成功后显示最后一次同步时间

### 绑定 IDS 处理单元后开启 IDS 功能

入侵防御 APP>>【设置】>>【参数设置】>>【运行 CPU 核心】>>【2】

入侵防御 APP>>【设置】>>【参数设置】>>【入侵防御】>>【开启】

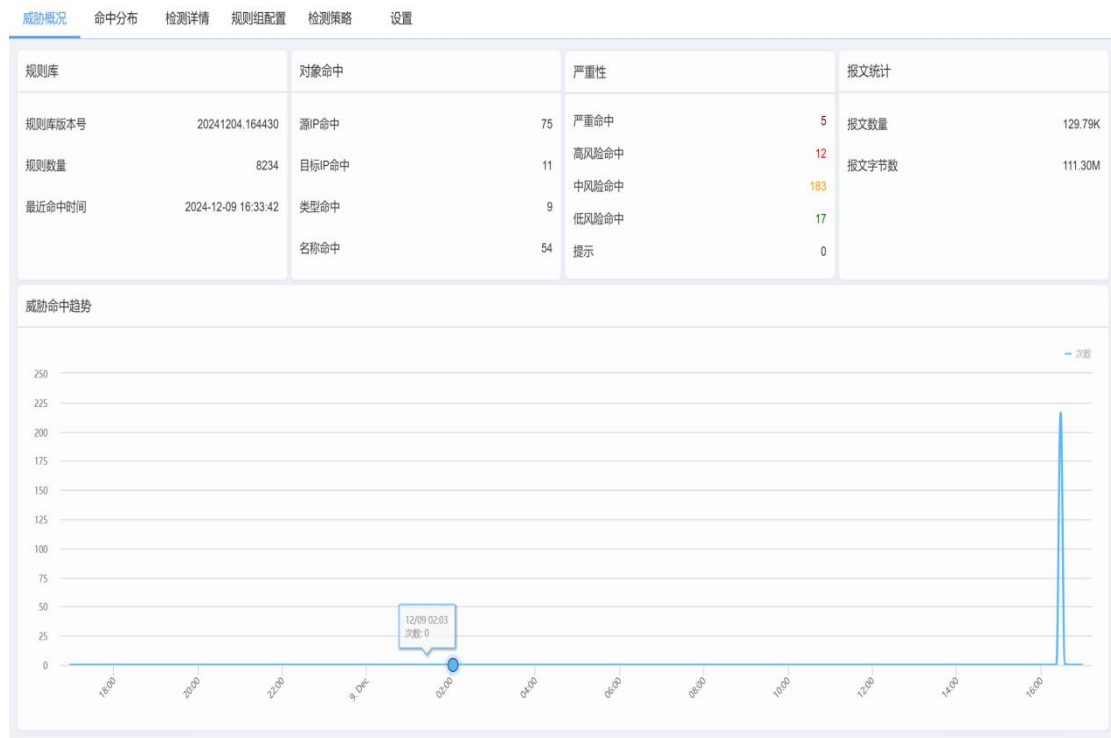


### 注意

- 1、当设备有当前空闲可用核心时，IDS 自动运行在空闲核心。
- 2、无空闲核心时复用管理单元 0 时，设备访问 WEB 页面管理可能较慢。

## 功能界面

“威胁概况”页面显示当前 IDS 运行情况

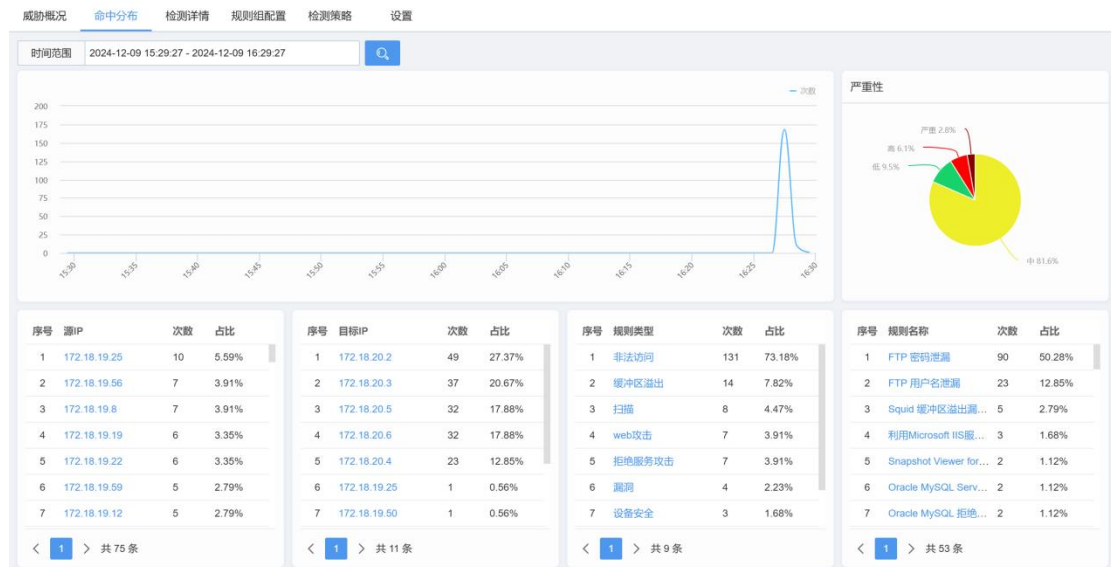


注意

- 1、IDS 处于关闭状态，在“报文统计”中会显示“入侵防御检测关闭”
- 2、设备可用内存少于 1024M 时，可能导致 IDS App 启动失败，“报文统计”中会显示为“内存不足，入侵防御模块无法启动”

## 命中分布

“命中分布”页面用于显示日志的分布情况，分别基于“源 ip”、“目的 ip”、“规则类型”、“规则名称”、“严重性”进行统计



## 检测详情

“检测详情”页面用于显示日志的详细信息，可以基于“时间”、“源 IP”、“源 IP”、“目的端口”、“目的 IP”、“传输协议”、“规则名称”、“规则类型”、“严重性”进行过滤查看

威胁概况 命中分布 检测详情 规则组配置 检测策略 设置

源IP	源端口	目标IP	目标端口	规则类型	所有类型	传输协议	任意
规则名称	严重性	任意	时间范围	2024-12-09 15:54:54 - 2024-12-09 16:54:54	Q		

序号	时间	源IP	目标IP	传输协议	威胁类型	威胁名称	威胁详情	严重性	上行流量	下行流量	上行包数	下行包数
1	2024-12-09 16:...	172.18.19.49.51...	172.18.20.2.21	tcp	非法访问	FTP 密码泄露	1300645	中	814 B	974 B	12	11
2	2024-12-09 16:...	172.18.19.60.50...	172.18.20.6.21	tcp	非法访问	FTP 密码泄露	1300645	中	752 B	970 B	11	11
3	2024-12-09 16:...	172.18.19.71.31...	172.18.20.3.21	tcp	非法访问	FTP 用户名泄露	1300644	中	383 B	2.85 K	6	7
4	2024-12-09 16:...	172.18.19.3.520...	172.18.20.6.21	tcp	非法访问	FTP 用户名泄露	1300644	中	1.00 K	1.03 K	10	10

“威胁详情”可以查看该规则的描述信息

规则编号:1300645

×

规则名称: FTP 密码泄露

规则类型: 非法访问

严重性: 中

规则描述: 检测到 FTP 密码泄露。

规则措施: 1、加强设备的访问控制，比如配置复杂密码。

## 2.5. 主动 DNS 域名解析

### 应用场景

过往版本中，Panabit 需要使用管理口对系统内配置的域名进行解析，存在以下问题：

- 1) 管理口无法访问 DNS 服务器时，无法解析域名为 IP
- 2) 无法指定特定线路实现域名解析；
- 3) iWAN 服务端使用动态公网 IP 线路时：服务端线路重播(服务端 IP 变更)，iWAN 客户端未及时更新服务端 IP 导致客户端无法上线问题。

### 解决方案

新增 miniDNS 模块，解决 Panabit 内配置域名时无法解析或非预期线路解析问题。

名称	参数
从指定 WAN 线路解析域名	<code>floweye minidns add name=域名 proxy=wan 线路名称</code>
查询 minidns 模块域名解析结果	<code>floweye minidns get name=域名 proxy=wan 线路名称</code>
查看 minidns 所有域名解析结果	<code>floweye minidns list</code>
修改 minidns 域名解析的缓存时间	<code>floweye minidns config ttl=xxx</code>



### 说明

- 1、mini DNS 为独立解析模块，不更新域名路由等 DNS 缓存



## 3. 功能优化

### 3.1. DNAT 功能优化

#### 客户场景

某互联网数据中心客户使用 Panabit 作为网络集中调度设备，为满足溯源要求，需 Panabit 配置 DNAT 时仅对目的 IP 地址进行修改，保持源 IP 地址不变。

#### 解决方案

【策略路由】>>【DNAT】>>新增“不改变源地址”参数。

添加 ×

策略序号  序号从小往大匹配，范围1-65535

策略时段  策略只在该时间范围生效

策略备注

匹配条件

用户类型

用户组  [选择用户组](#)

源 / 目地址  /

源 / 目端口  /

协议   [选择协议](#)

源接口  最大带宽  /  Mbps, [说明](#)

VLAN  TTL  DSCP

执行动作

执行动作  ☐ 不改变源地址

DNAT地址  如果设置,数据包的目标IP被修改为设置的IP

NAT线路

SNAT地址池

线路

确定 取消

## 3.2. 微信认证流程优化

### 客户场景

Panabit 网桥模式部署时微信认证无法正常使用

### 解决方案

在 webauth 功能中增加 noack 选项，当 noack=1 时，panaos 不对 80 端口的 TCP 握手报文应答，而是放行 TCP 握手的报文，让目标服务器进行应答。

---



#### 说明

Panabit 网桥部署微信认证时，需要开启 noack 选项  
floweye webauth config noack=1

---

### 3.3. 共享限速模块优化

#### 客户场景

某高校项目网络分为办公及宿舍区，师生在办公区上网时提供上网计费策略（20M 带宽、免费），宿舍区为计费策略（200M 带宽、收费）。为客户使用便利性，同一账号支持 3 个终端登录。

可能存在账号同时在办公区及宿舍区在线的情况，需要 Panabit 根据用户 IP 地址+计费组+用户账号为条件创建不同计费属性的限速策略。

#### 解决方案

Panabit 接收认证系统计费报文后，将用户 IP 地址+计费组信息+账号信息进行关联，实现不同计费属性的单用户差异限速策略。

Panabit 接收到计费组信息后，在【在线用户】的【账号备注】显示信息为“账号@classid”

### 3.4. 优化域名群组匹配

#### 应用场景

客户使用 Panabit 域名路由时，需要配置单个域名群组内导入 10 万+条域名，出现以下问题：

- 导入域名条目较多时可能出现超时无法导入问题
- 精确匹配后缀域名时需要重复添加两次后缀

#### 解决方案

- 优化域名群组匹配算法，避免短域名导致的冲突问题。
- 在域名里引入“@”字符，@panabit.com 可以匹配 www.panabit.com 和 panabit.com



说明 1、域名群组匹配为后缀匹配原则

#### 域名群组标识符

示例	字符类型	备注
1	无字符	.panabit.com 时匹配 pa.panabit.com、pb.panabit.com 等
2	无字符	panabit.com 时匹配 www.apanabit.com、www.bpanabit.com 等
3	^字符	^pa.panabit.com 时精确匹配 pa.panabit.com，pb.panabit.com 则不能匹配
4	@字符	效果等同于^panabit.com”与”.panabit.com”

### 3.5. 优化端口映射配置导入

#### 客户场景

在某 IDC 场景中，用户需要一次性导入 10 万条端口映射配置，导入端口映射策略时超时失败。



#### 解决方案

针对端口映射策略导入逻辑进行优化：

- 1) 支持文件方式导入端口映射配置；
- 2) 支持端口映射导入失败时配置自动回滚：当加载导入映射配置出现错误时，自动回滚至原配置。

### 3.6. 用户地址池支持 IPV6 前缀

#### 应用场景

某高校客户根据需要在 TOP 用户内实现基于 IPV6 地址前缀关联用户组属性

#### 解决方案

Panabit 用户组属性中新增：IPv6 地址字段

在【对象管理】>>【账号管理】>>【组织架构】>>【添加用户组】>>【IPv6 地址】支持配置 IPv6 前缀地址、前缀长度

添加用户组 ×

上级节点	-	
名称	办公	
IPv4地址范围	0.0.0.0	- 0.0.0.0
IPv6地址	前缀地址	/ 前缀长度
v4账号带宽限制	0	/ 0 kbps,0表示不限制
v6账号带宽限制	0	/ 0 kbps,0表示不限制
DNS	0.0.0.0	例: 114.114.114.114,8.8.8.8
在线时间	0	小时,在线时间超过时,系统会自动踢用户下线,0表示不控制
过期账号	禁止登录	

— 代拨设置 ^

代拨主线	不设置
------	-----

### 3.7. 流媒体支持高码流超清频道

#### 客户场景

随着对视频清晰度要求的提升,当前视频码流存在多种规格(标清 4M、高清 8M、超清 12M),播放超清频道时可能存在马赛克、花屏、卡顿问题。

#### 解决方案

为满足客户对超清视频节目的需求,适配不同码率的视频。新增 IPTV\_BITRATE 参数默认参数为 1024(表示 8Mbps 码率)。

默认为 8M 码率时,配置单个输入频道占用 Panabit 设备 16M 内存。

配置码流为 16M 时,配置单个输入频道将占用 Panabit 设备 32M 内存。



注意

内存消耗超出可用内存时可能导致 PanaOS 系统无法启动。

### 3.8. 连接信息支持 IPv6 前缀查询

#### 应用场景

某客户校园网使用 Panabit 对接 IPv6 用户认证设备,认证系统在认证报文中仅同步用户 v6 前缀地址。导致在 Panabit 【TOP 用户】中无法直接查看当前 v6 地址对应网络连接。

#### 解决方案

【TOP 用户】>>【连接信息】页面中的 IP 选项框支持 IPv6 地址前缀模糊查

询。

### 3.9. 支持配置 IPv4 本地链路地址

#### 应用场景

某运营商客户设备，需要在 LAN/WAN 添加 169.254.1.1 的 IP 地址，添加该地址时 Panabit 提示错误 IP。

##### ➤ 地址段定义与用途

根据 RFC3927 定义，169.254.0.0/16 地址段被定义为本地链路地址（Link-local address），用于在没有 DHCP 服务器或 DHCP 获取失败时，主机自动配置 IP 地址进行本地通信。

#### 解决方案

【网络设置】>>【LAN/WAN】>>支持配置 169.254.0.0 的 IP 地址

### 3.10. SLAAC 支持多 VLAN 下发 IPv6

#### 应用场景

客户存在多个内网 VLAN 需要使用 SLAAC 地址分配 IPV6 地址时，之前版本需要每个内网 VLAN 创建一个 LAN 口，当内网 VLAN 比较多时需要创建较多 LAN 接口，配置较为烦琐。

#### 解决方案

优化 SLAAC 主动发送 RA 报文的机制。如果无状态地分配（【WAN 线路】>>外网线路）中配置一段 VLAN 范围，Panabit 将对配置的所有内网 VLAN 的都发送一次 RA 报文。

添加
×

名称

办公V6\_LAN

线路类型

IPv6

网卡

eth0

在“系统概况->网络接口”中，将网卡设置为接内网

IPv6 IP

线路掩码

DHCPv6

地址范围

-

提示

更多参数，复用“无状态地址分配”配置

无状态地址分配

委派线路

V6上网

子网前缀

子网长度

0表示不开启

地址分配

开启

分配VLAN

0-0

若配置，则只给指定VLAN分配地址

DNS1

240c::6666

确定

取消

### 3.11. DHCPv4 WAN 线路支持 Option

#### 应用场景

IPOE 接入业务是一种接入认证业务，通常利用 DHCP+OPTION 扩展字段方式作为终端鉴权使用，也被称为 DHCP+认证。

#### 解决方案

DHCP v4 类型 WAN 线路支持 Option12、Option61、Option60 选项

添加

名称

IPTV01

线路类型

DHCP-v4

网卡/承载线路

eth1

备注

DHCP

option12

android-d20ebc7a994bad58

字符串

HostName

option61

fc5703fe4cdc

字符串

Vendor class ID

option60

3c4500001f410148b9893892fd41

16进制

Client ID

高级

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

同上,任何一个IP通都表示心跳正常

最大时延

0

心跳时延连续 5 次超出则心跳失效; 0表示忽略

MTU

1500

外层/内层VLAN

0

/

0

0~4095, 0表示无VLAN

克隆MAC

00-00-00-00-00-00

前4字节不能为

外网Ping不应答

☒ 关闭



#### 说明

1、获取 IPOE 认证数据方式：Panabit 网桥部署在光猫与机顶盒之间，利用网卡抓包方式获取 DHCP 报文。

2、查看 DHCP discover 报文中对应的 Option 字段



## 3.12. 代拨场景内层 QinQ 支持 VLAN 范围

### 客户场景

客户某运营商代拨项目要求 PPPoE 客户端接入时需携带 QinQ 双层 VLAN，创建代拨线路时外层标签为固定值，内层 VLAN 在特定范围（800-4000）随机使用。

### 解决方案

- 1) 代拨地址 VLAN 选项支持 10/100-1000（内层 VLAN 区间为 800-4000）格式
- 2) 当内层 VLAN 配置为 VLAN 区间时，Panabit 代拨在选择内层 VLAN 时会根据账号选择区间内的某个 VLAN TAG，
- 3) 为了确保内网 VLAN 与账号的一致性，相同代拨账号将固定绑定到相同内层 VLAN。



### 3.13. iWAN 和 L2TP 客户端的域名解析优化

#### 客户场景

iWAN 客户端和 L2TP 客户端的服务器地址支持配置为域名,当前版本 Panabit 域名解析需要利用管理口对域名进行解析,存在以下问题:

- 1) 如果管理口无法访问 DNS 服务器时,无法完成域名解析;
- 2) 无法指定特定线路实现域名解析;

3) 服务端使用动态公网 IP 线路时:服务端线路重播(服务端 IP 变更),iWAN 客户端使用原 IP 拨号导致 iWAN 无法上线问题。

#### 解决方案

支持 iWAN 客户端和 L2TP 客户端内配置的域名由当前承载线路进行解析。

### 3.14. 单个 SSID 最大接入终端数支持 254 个

单个 SSID 最大 STA 数由 127 提升至 254.

### 3.15. 携带 IPv6 本地链路地址时用户无感知上线失败

#### 客户场景

客户网络为 IPv4 环境,用户终端默认启用 IPv6,终端自动生成 fe80 本地链路地址,当使用 IPv6 本地链路地址认证时无感知上线失败,使用 IPv4 地址时正常上线。

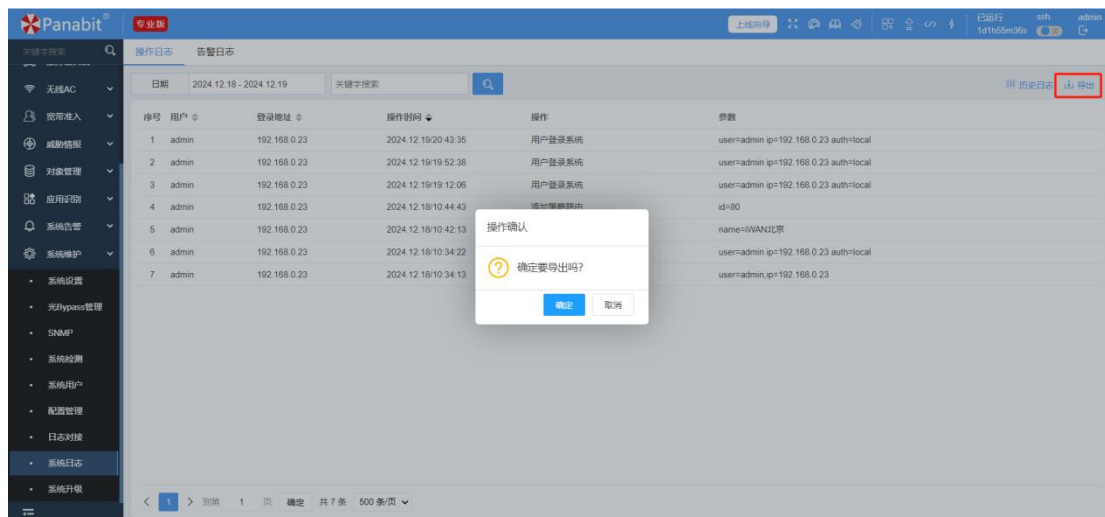
#### 解决方案

Panabit 创建内网 IP 对象忽略 IPv6 本地链路地址

## 4. 界面优化

### 4.1. 支持 Panabit 系统日志导出

检索特定周期日志后点击导出按钮，可以导出特定日期内 Panabit 生成的系统日志。



## 4.2. 新增 WEB 应急恢复页面

### 应用场景

为满足行业标准并提升设备安全性，升级 Panabit 系统后会自动关闭 SSH 功能，导致设备出现异常情况时难以远程维护。

### 解决方案

当 WEB 管理界面加载失败时自动打开 WEB 应急恢复页面，利用应急恢复页面开启 SSH 进行 Panabit 设备维护。



**说明** Panabit 为转发、管理双平面架构，WEB 管理页面打开失败不影响业务数据转发。



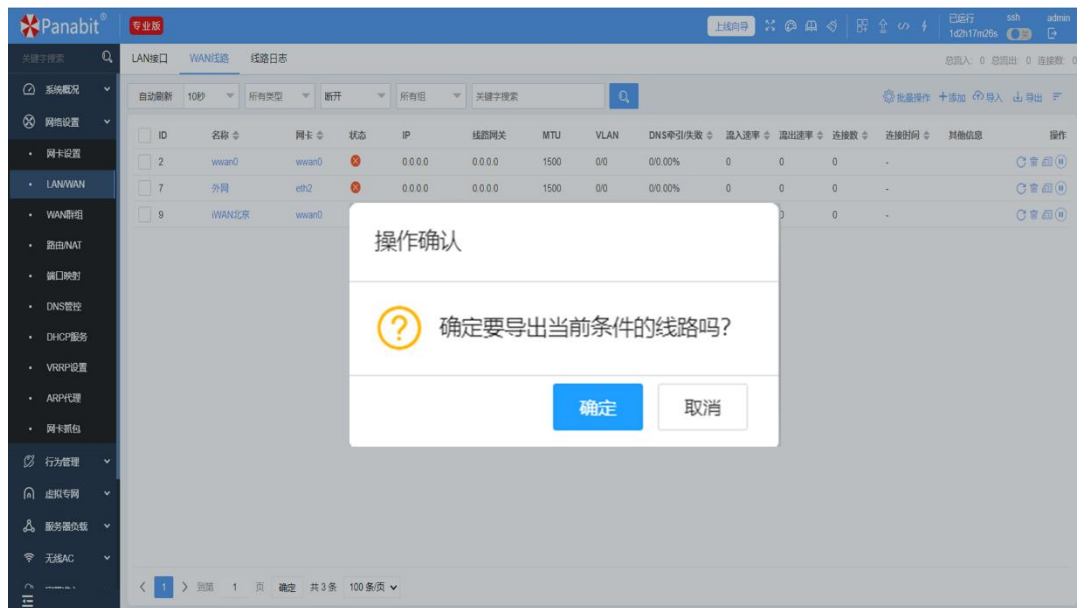
## 4.3. LAN/WAN 接口导出优化

### 应用场景

Panabit 设备最大支持 4000+条 WAN/LAN 线路，当出现较多线路中断时，运维人员无法快速导出中断线路。

### 解决方案

为解决运维便利性问题，在 Panabit LAN/WAN 菜单支持导出当前筛选条件的线路。



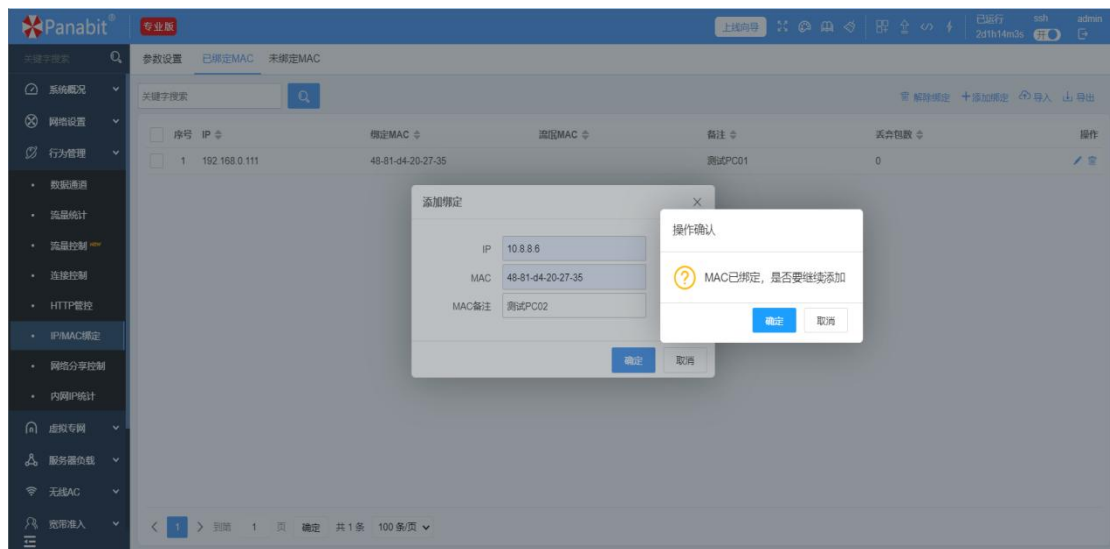
## 4.4. MAC 重复绑定提示

### 应用场景

用户设置对 MAC 对 IP 进行绑定时，相同 MAC 绑定多个 IP 不能提示“MAC 已绑定”。

### 解决方案

新增 MAC 地址如在【行为管理】>>【IP/MAC 绑定】>【已绑定 MAC】中存在时，提示“MAC 已绑定，是否继续添加”



## 4.5. 批量账号导入异常

### 应用场景

在【账号管理】>>【本地账号】批量添加本地账号时，可能导致身份信息字段丢失。

### 解决方案

问题已修复。

## 4.6. 删除重复引用 IP 群组时无提示

### 应用场景

如果某 IP 群组中被引用多次引用，【对象管理】>>【IP 群组】中删除此群组无提示“已引用策略删除操作确认”

### 解决方案

问题已修复。

## 5. BUG 修复

序号	模块	修复
1	告警模块	告警模块将对“AuthTimeout”事件不做告警
2	LAN/WAN	DNS 代理配置丢失
3	告警模块	告警超过 2048 后不告警
4	告警模块	线路名称带()特殊字符导致不告警问题
5	威胁情报	配置多个白名单对象，重启 panaos，只有 id 为 1 的白名单对象会被保存，其余均丢失
6	ipobj 模块	在 BSD 版本中，ipobj list 中的会话连接数和 get ip 中的数量不一致
7	iWAN	iWAN 服务端回包的 BUG
8	流量控制	行为管理--流量控制的 v4 条件匹配异常
9	OS	AX10K 设备导入配置时 PanaOS 无法正常启动
10	会话管理	在线用户不支持删除 ipv6 会话
11	WEB UI	用户密码使用特殊字符导致登录白名单失效
12	radsnif	radsnif 模块 port 参数配置加载异常
13	域名负载	修改域名负载线路时域名负载策略丢失
14	域名跟踪	域名跟踪策略引用主线路中断时，备线路未生效
15	NAT6 模块	未配置 66 NAT 策略时，66 端口映射策略不生效
16	mbuf 模块	DNS 回复的域名部分为字符串（非偏移 ptr）时，域名跟踪模块不能正确解析数据包

## 6. 应用识别

### 6.1. 新增应用

一级分类	二级分类	应用	备注
应用协议	蜻蜓 FM	蜻蜓 FM	国内首家网络音频应用，汇聚广播电台、版权内容、人格主播等优质音频 IP。
HTTP 协议	Web 视频	全民 K 歌	全民 K 歌基于用户需求打造的线上 K 歌工具
HTTP 协议	Web 视频	联想视频	联想手机内置的优质视频播放器 APP，具备丰富的资源整合，拥有丰富多样的视频资源库，
HTTP 协议	云服务	Filez 网盘	联想 Filez 企业网盘是业界领先的企业级文件管理与协同办公平台。
网络游戏	移动游戏	无限暖暖	《无限暖暖》是由叠纸游戏开发的开放世界换装冒险游戏
网络游戏	完美时空	诛仙世界	《诛仙世界》是一款由完美世界游戏开发的仙侠题材网络游戏
网络游戏	网易游戏	漫威争锋	《漫威争锋》是一款由漫威正版授权，网易游戏运营的多平台第三人称射击游戏
移动应用	手机应用	瓜子二手车	二手车交易平台
HTTP 协议	云服务	UC 网盘	UC 浏览器推出的一款云服务产品
HTTP 协议	常用网站	电信 189	中国电信
HTTP 协议	Web 视频	Dramabox	海外短剧平台
常用协议	电子邮件	阿里邮箱	阿里邮箱
HTTP 协议	云服务	阿里云服务	阿里巴巴集团旗下
常用协议	电子邮件	新浪邮箱	新浪网邮箱产品
金融财经	股票交易	苹果股市	苹果股票服务
HTTP 协议	云服务	奶牛快传	一款无需注册即可使用的大文件临时传输服务
网络游戏	STEAM 游戏	王权与自由	于老牌 MMORPG 开发商 NCSOFT 的新作《王权与自由》



## 6.2. 更新应用

一级分类	二级分类	应用	备注
常用协议	虚拟货币	虚拟货币	更新协议特征
常用协议	游戏维护	其它游戏更新	更新协议特征
网络游戏	网易游戏	永劫无间	更新协议特征
网络游戏	移动游戏	斗罗大陆	更新协议特征
网络游戏	移动游戏	神雕侠侣	更新协议特征
网络游戏	移动游戏	实况足球	更新协议特征
HTTP 协议	Web 视频	微信直播	更新协议特征
HTTP 协议	Web 视频	其它 WEB 视频	悟空浏览器是一个视频聚合应用，合并到“其它 WEB 视频”
网络游戏	其他游戏	坦克世界	更新协议特征
网络游戏	STEAM 游戏	Brawlhalla	更新协议特征
网络游戏	盛大网络	传奇系列	更新协议特征
网络游戏	盛大网络	三国杀	更新协议特征
网络游戏	腾讯游戏	穿越火线	更新协议特征
网络游戏	网易游戏	逆水寒	更新协议特征
HTTP 协议	Web 视频	韩剧 TV	更新协议特征
商业系统	商业系统	闲鱼	更新协议特征
常用协议	常用协议	QUIC	网易会议使用 STUN 和 QUIC 协议
HTTP 协议	Web 视频	斗鱼 TV	更新协议特征
HTTP 协议	Web 视频	快直播	更新协议特征
HTTP 协议	Web 视频	龙珠直播	更新协议特征
HTTP 协议	Web 视频	腾讯视频	更新协议特征
网络游戏	移动游戏	少年三国志	更新协议特征
HTTP 协议	Web 视频	AfreecaTV	更新协议特征
HTTP 协议	WebMail	189 邮箱	更新协议特征
HTTP 协议	Web 视频	新蓝网	中国蓝 TV 改名新蓝网
HTTP 协议	带宽测速	SpeedTest	更新协议特征

网络游戏	STEAM 游戏	Steam 登录	更新协议特征
网络游戏	其它游戏	完美电竞	更新协议特征
网络游戏	腾讯游戏	英雄联盟	改进首包识别
HTTP 协议	云服务	123 云盘	更新协议特征
常用协议	网络广告	UMENG	更新协议特征
HTTP 协议	云服务	蓝奏云	更新协议特征
HTTP 协议	云服务	腾讯微云	腾讯微云和腾讯下载的特征重叠
HTTP 协议	Web 视频	河马剧场	更新协议特征
HTTP 协议	Web 视频	影视大全	合并入 funshion
网络游戏	移动游戏	全民奇迹	更新协议特征
HTTP 协议	带宽测速	泰尔网测	更新协议特征
HTTP 协议	Web 视频	新浪视频	更新协议特征
常见协议	电子邮件	SMTP	更新协议特征
常见协议	电子邮件	POP3	更新协议特征
常见协议	游戏维护	Wegame 下载	更新协议特征
网络游戏	腾讯游戏	FIFAOnline	更新协议特征
网络游戏	腾讯游戏	腾讯云游戏	更新协议特征
网络游戏	腾讯游戏	逆战	更新协议特征
网络游戏	移动游戏	全民主公	更新协议特征
社交	即时通讯	企业微信	更新协议特征
网络游戏	STEAM 游戏	大逃杀登录	更新协议特征
常见协议	终端控制	AnyDesk	更新协议特征
P2P 下载	迅雷系列协议	迅雷	更新协议特征

## 7. 升级说明

### 7.1. 支持说明

Panabit 各版本软件升级包区分硬件架构和操作系统，需要根据所使用的产品进行相应的选择。

类型	说明	升级包格式
x86/Linux	x86 硬件架构，基于 Linux 操作系统	Panabit**_**_Linux3.*
x86/FreeBSD	x86 硬件架构，基于 FreeBSD 操作系统	Panabit**_**_.FreeBSD9.*
arm/Linux	ARM 硬件架构，基于 Linux 操作系统	Panabit**_**_.arm64.*

### 7.2. 前置条件

- 本文档针对已经使用 Panabit 的设备进行升级说明
- 对于全新安装 Panabit 请参考官方论坛或技术支持服务热线
- 授权许可在有效期内

### 7.3. 注意事项

- 需参照对应硬件产品平台选择对应关键词标识的升级包
- 需参照对应商用版本标识选择对应的升级包
- 升级过程中可能网络中断

### 7.4. 升级流程

① 请于官方下载中心 <https://www.panabit.com/download> 下载对应 Panabit 版本



② 访问 Panabit 设备【升级中心】



### ③ 【升级系统】选择下载的升级包

升级中心

操作系统: Linux 4.19

软件版本: R8.52[TANG(大唐)r5p2], Build date 2023-07-24 16:25:04

DPI特征库: 20230724.162418

升级系统

升级特征库

系统授权

授权编号: PE303VV-25BM

### ④ 【确定】升级，等待升级完成即可

升级确认

升级包上传成功!

当前版本: 专业版, R8.52[TANG(大唐)r5p2], Build date 2023-07-24 16:25:04

上传版本: 专业版, R8.57[TANG(大唐)r5p7], Build date 2023-12-27 18:48:53

升级提示: 升级过程网络会中断!

确定要继续升级吗?

确定

取消

