深信服安智路由器 SDW-R
用户手册

产品版本	4.0.9
文档版本	01
发布日期	2021-06

深信服科技股份有限公司

注意

您购买的产品、服务或特性等应受深信服科技股份有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、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，深信服科技股份有限公司对本文档内容不做任何明示或默示的声明或保证。

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。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

前言

关于本文档

本文档针对深信服SDWAN安全智能路由器（简称：安智路由器或SDW-R）产品，介绍了SDW-R的特性、安装、功能配置和管理。

产品版本

本文档以下列产品版本为基准写作。

产品名称	版本
SDW-R	4.0.9

后续版本有配置内容变更时，本文档随之更新发布。

读者对象

本手册建议适用于以下对象：

- 网络设计工程师
- 运维人员
- 现场技术支持人员

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。

图形	文字	使用原则
危险	危险	若用户忽略危险标志，可能会因误操作发生危害人身安全、环境安全等严重后果。
警告	警告	该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。
小心	小心	若用户忽略警告标志，可能会因误操作发生严重事故（如损坏设备）或人身伤害。
注意	注意	提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。。
说明	说明	对操作内容的描述进行必要的补充和说明。

文字描述	代替符号	举例
窗口名、菜单名等	方括号“[ ]”	弹出[新建用户]窗口。
		选择[系统设置/接口配置]。
按钮名、键名	尖括号“< >”	单击<确定>按钮。

在本文中会出现图形界面格式，它们所代表的含义如下。

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本	发布时间	更新说明
01	2020-11	更新点： 1. SDW-R 云端易部署配置调整 2. 新增 sofast 功能配置 3. 新增 URL 控制策略配置 4. 应用/URL 控制策略新增对区域、IP 组、MAC 组生效 5. 对象设置新增 MAC 组设置 6. 新增 WIFI 802.1X 认证相关配置 7. 新增 4G 冷备配置 8. 新增标准 IPSec VPN 配置 9. 新增本地设备界面配置备份与恢复 10.支持在登录界面进行一键巡检 11.新增易部署配置界面，用于恢复出厂设置
02	2021-06	更新点： 1. 监控中心 UI 界面调整 2. 新增 VPN 多线路定制策略配置 3. 新增 SDWAN 智能选路策略模板界面 4. 新增流量管理配置界面 5. 新增单臂多线路的部署方式 6. 新增 VLAN 子接口的配置 7. 新增 OSPF 动态路由相关配置 8. 新增关于 VLAN 子接口的 DHCP 相关配置

资料获取

您可以通过深信服官方网站获取产品的最新资讯：

www.sangfor.com.cn

获取安装/配置资料、软件版本及升级包、常用工具地址如下：

bbs.sangfor.com.cn

深信服科技

深信服技术服务

技术支持

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

深信服科技服务商及服务有效期查询：

https://bbs.sangfor.com.cn/plugin.php?id=service:query

意见反馈

如果您在使用过程中发现任何产品资料的问题，可以通过以下方式联系我们。

- bbs.sangfor.com.cn
- 通过联系当地办事处电话反馈
- 售后服务电话 400-630-6430

目录

1. 产品说明

1.1. 产品简介

SD-WAN安智路由器（简称SDW-R或者安智路由器）是一体化IT设备，满足分支VPN、路由、交换等多种需求。VPN+SD-WAN：支持Sangfor VPN协议，并基于VPN隧道实现SD-WAN智能选路；路由交换一体：多网口型号设备，满足分支WAN/LAN及本地局域网数据交换需求；无线接入及WIFI：支持2.4G/5G双频WIFI，AP级品质；支持接入4G LTE线路，实现分支4G组网；边界安全防护：防DDOS、ARP攻击基于应用DPI的访问策略控制。

1.2. 产品关键特性

1.2.1. 线路成本和业务体验

内置SOFAST链路优化引擎：通过DPI库自动识别应用且划分为交互类、实时类、传输类，智能感知链路质量和匹配链路优化模型，保障在高丢包场景下，依然保障业务流畅访问体验。如针对高丢包音视频优化，在10%丢包环境可优化至无卡顿体验。应用访问体验可通过BBC统一管理平台查看，在线路质量丢包率偏高的场景下，应用体验还是优质的体验效果。

SD-WAN BEST选路引擎：以应用体验为核心，引入智能选路能力。通过实时感知应用流量行为特征和不同WAN线路的SLA状态，实现不同类型，不同优先级的应用实时匹配不同的线路。若线路状态发生改变如发生线路拥塞，劣化或者中断，BEST选路引擎可以自适应完成故障避免，为应用重新选择合适的线路，实现线路资源的最大化

使用和应用体验的高质量保障。

1.2.2. 部署运维效率

运维化繁为简零接触部署+业务可视化，分支设备分钟级上线，再复杂的网络拓扑也能整理得清清楚楚。

SDW-R基于云端易部署策略+集中可视化管理，足不出户就能实现分支零接触上线与集中可视运维。

云端易部署策略：采用全新云端易部署方案，SDW-R联动云端完成注册，实现分钟级部署上线，相对传统设备上线极大缩短上线周期和实施成本。

集中可视化管理：得益于每台SDW-R精准的DPI识别，联动集中管理平台可实现全网设备、应用流量可视化监控，解除传统专线运维应用流量“黑盒”之痛。

1.2.3. 安全防护能力

通过数据安全加密，边界多维防护，构建更加安全的合规广域网。

数据传输安全：基于VPN国际算法或国密算法加密数据，保障业务不“裸奔”，更安全。同时，针对不同业务流量可以匹配不同隧道，实现业务安全隔离。

应用访问控制：SDW-R本地内置防火墙、过滤规则等功能，且可以联动云端安全进行更完善的安全防护和安全审计，实现安全防护同时满足合规。

2. 安装部署

本部分主要介绍了SD-WAN安全智能路由器（简称SDW-R或者安智路由器）系列产品的硬件安装。硬件安装正确之后，您才可以进行配置和使用。

2.1. 安装前准备

本节主要写作安装前的准备工作，包括准备环境、软硬件材料等。

2.1.1. 环境要求

SDW-R设备可在如下的环境下使用。

输入电压： 110V~230V

温度：0～45℃

湿度：5～90％

为保证系统能长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

2.1.2. 电源要求

SDW-R系列产品使用交流110V到230V电源。在接通电源之前，请保证您的电源有良好的接地措施。

2.2. 产品外观

产品图片如下。

从接口和指示灯分别是：

- 4G 指示灯：4G 拨号过程中，该指示灯会闪烁；当设备通过 4G 拨号成功时，该指示灯会亮起。其他支持 4G 型号的设备（会在此信号灯标识 3G/4G），信号灯和 3G 共用；4G 网络差的时候会自动切换，但需要是该卡支持 3G 信号。
- POWER：SDW-R 设备电源指示灯。
- WIFI 指示灯：当设备启用 WIFI 功能时，该指示灯会亮起；有 WIFI 连接时，该指示灯会闪烁。
- ALARM：SDW-R 设备报警指示灯(设备启动时 1-2 分钟内长亮)。
- GE0：默认为设备的 LAN 接口。
- GE1：默认为设备的 LAN 接口。
- GE2：默认为设备的 DMZ 接口。
- GE3：默认为设备的 WAN1 接口。
- GE4：默认为设备的 WAN2 接口。
- 接口属性可在部署模式中进行修改。
- RESET：恢复出厂配置和恢复默认密码功能。SDW-R 设备通电状态下，按住 RESET 键 3 秒后松开，ALARM 红灯会开始闪烁，之后会红灯常亮，等红灯熄灭后即恢复默认配置成功。短按两次 RESET 用于恢复默认密码。
- SIM 卡插槽：用于插入 3G 或者 4G 上网卡。

🕮 说明：

图片仅供参考，不同型号的产品外观请以实物为准。

CONSOLE 口仅供开发和测试调试时使用，用户需从设备网口通过浏览器登录设备进行配置。

本节主要是在安装结束之后验证安装是否成功。安装验证可以是部分安装成功之后的验证，也可以是整体安装结束之后的验证。

2.3. 配置与管理

在配置SDW-R系列产品之前，您需要配备一台电脑，配置之前请确定该电脑的网页浏览器能正常使用（支持Internet Explorer、谷歌浏览器和火狐），然后把电脑与SDW-R连接在同一个局域网内，通过网络对设备进行配置。

接口	IP 地址
ge0	10.254.254.253/24
ge1	10.254.253.253/24

2.4. 设备接线方式

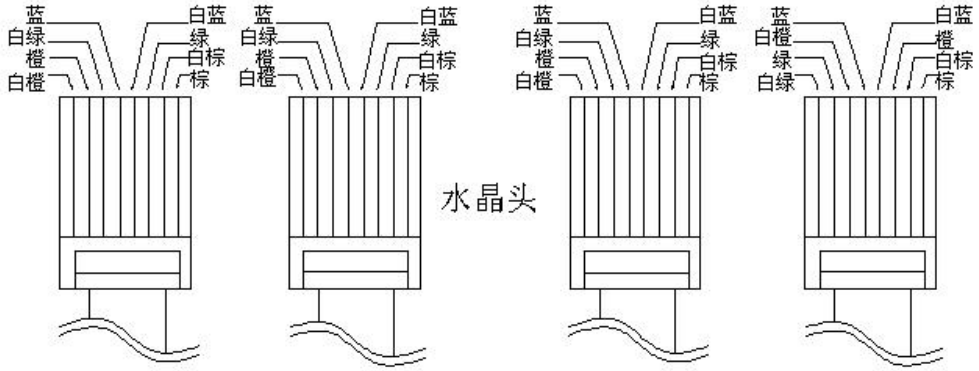
在背板上连接电源线，打开电源开关，用标准的RJ-45以太网线将LAN口与内部局域网连接，用标准的RJ-45以太网线将WAN口与Internet接入设备相连接，如路由器、光纤收发器或ADSL Modem等。

指示灯说明

1. 在背板上连接电源线，打开电源开关，此时前面板的Power灯(绿色，电源指示灯)和Alarm灯(红色，告警灯)会点亮。大约1-2分钟后Alarm灯熄灭，说明SDW-R正常工作。
2. SDW-R正常工作时POWER灯常亮，WAN口和LAN口LINK灯长亮，ACT灯在有数据流量时会不停闪烁。
3. ALARM红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在正常使用时，此红灯长亮，请将设备断电后加电重启，重启之后若红灯一直长亮不能熄灭，请与我们联系。

接线说明

- WAN 口直接连接 MODEM 应使用直通线、连接路由器应使用交叉线。
- LAN 口连接交换机应使用直通线、直接连接电脑网口应使用交叉线。
- 当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线序不同，线序如下图所示。



2.5. 结合 BBC 云端部署配置

操作场景

SDW-R结合BBC、云图实现分支的快速部署上线，减轻分支端设备的运维成本。

根据分支SDW-R上线获取内网地址段的方式分为两种场景：

1. 分支从全局地址池获取内网网段

客户划分分支内网时，全国分支内网从BBC中DHCP地址池中获取IP地址段。BBC对DHCP地址池中的IP地址段统一管理和下发，当分配出去DHCP地址池不再使用时，BBC可自动回收地址池，保证地址池的可持续使用性。适用于各分支内网用户数量差别不大的场景。

2. 分支从指定地址池获取内网网段

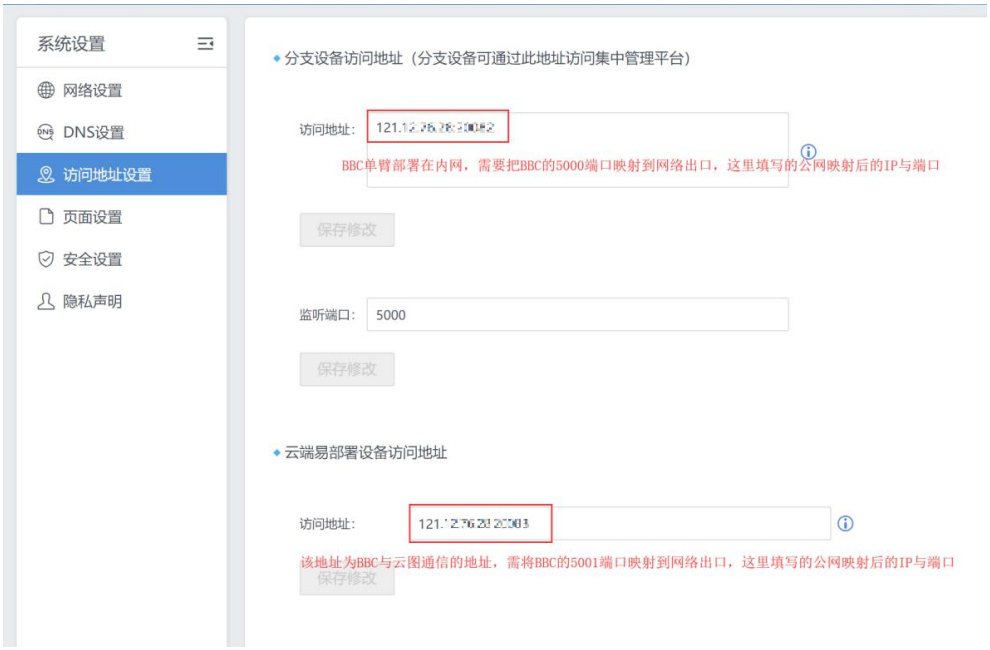
客户划分分支内网时，可指定区域获取指定的IP地址段。区域分支内网从BBC的区域DHCP地址池中获取IP地址段。BBC把全局DHCP地址池划分为各个小的区域DHCP地址池，最后区域中上线的分支从区域DHCP地址池中获取IP地址段。实现DHCP地址池合理分配，满足客户各分支内网IP数量不一致的问题。例如：北京区域中分支内网用户约为500，那么分支内网可设置获取的是10.1.0.x/22中的地址段，湖南省区域中分支内网用户约200个，那么分支内网可设置获取的是10.2.0.x/24中的地址段等。

前置条件

1. SDW-R设备需是出厂状态，如不是出厂状态请通过设备前面板的RESET键进行恢复出厂设置。
2. SDW-R4.0.5版本时，配合BBC版本必须在2.5.16及以上。
3. 中心端互联网出口网关映射TCP5000、TCP5001。
4. 测试云图账号的自注册，通过访问https://x.sangfor.com.cn实现云图账号自注册。
5. 需保证BBC可访问互联网，确保能与云图通信。

注意事项

1. 云端易部署需要确保设备访问地址是正确的，否则分支设备无法接入BBC。这里的地址必须是分支可以访问到的地址，BBC单臂部署在内网，通过出口网关映射进来的话，这里应该配置映射的公网IP。



2. BBC放置在纯内网环境时，无法使用云端易部署功能。

3. 云端易部署设备清单：需将SDW-R设备的SN码，网关序列号记录下来，可预配置分支的DHCP IP地址范围、分支名称，方便导入BBC中。设备清单信息如下图所示。

说明：

其中 SN 码与网关系列号为必填项设置，网关 ID、DHCP IP 地址范围、分支名称为可选项设置，如果配置了 DHCP IP 地址范围，则所有设备清单中的都要配置，且掩码一致。分支名称若不填写，SDW-R 会已 xxxx+SN 码的名称上线，后续修改 SDW-R 的分支名称步骤繁琐。

4. 分支设备通过4G方式进行云端易部署的时候，可以通过使用笔记本或者移动终端等设备连接SDW-R设备的WIFI，来确认分支设备是否部署成功。若WIFI名称已经修改为BBC端配置的WIFI名称，则说明分支设备已经通过4G完成易部署；若WIFI名称还是默认设备型号+网关ID，那么此时可通过WIFI方式继续进行完成分支设备的易部署配置。

5. 云端易部署时，可以对WIFI信息进行设置。当勾选策略模板时，BBC会自动下发策略模板中的WIFI配置到设备上，此时设备上的WIFI信息会与策略模板上的配置保持一致。若未关联策略模板，则使用云端易部署中设置的WIFI信息。

操作步骤

配置思路：

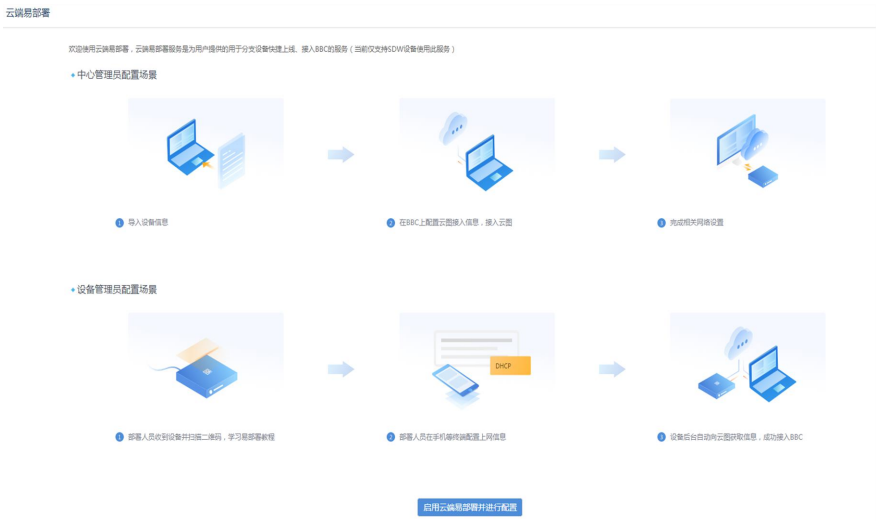
一、BBC端进行云端易部署配置向导。

二、分支端SDW-R配置互联网线路信息，完成上线。

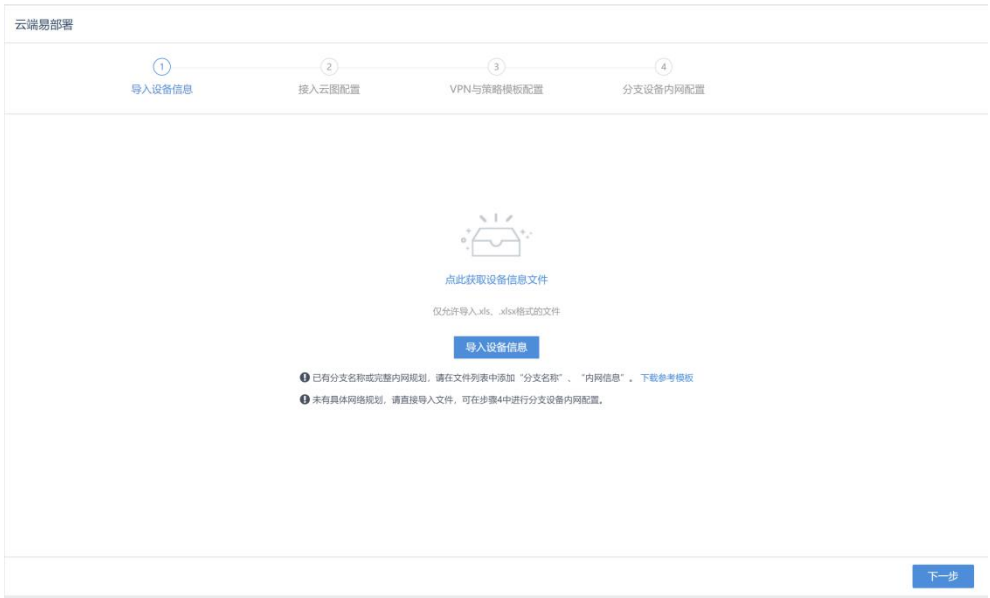
三、查看分支设备上线情况。

步骤1. BBC端开启云端易部署

1. 在[管理/云端易部署]页面下，点击<启用云端易部署并进行配置>。



2. 导入设备信息，点击<导入设备信息>。

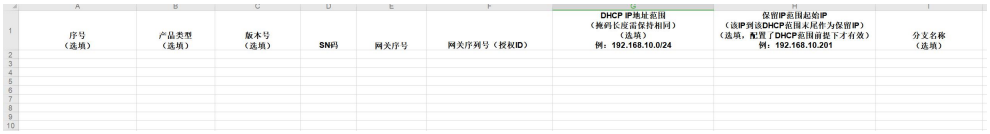


- 点击<浏览>，从本地选取设备信息文件，点击<开始导入>。

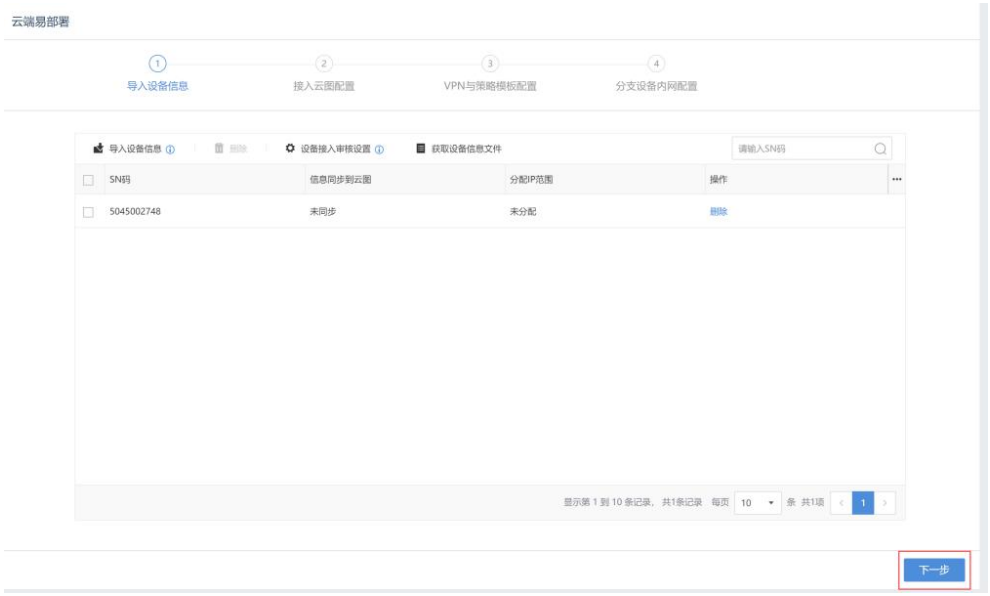
⚠ 注意：

测试设备需下载示例文件手动填写设备的 SN 码与网关序列号等信息。

- 示例文件如下图所示，其中 SN 码与网关序列号为必填项，若此处填写了 DHCP IP 地址范围，则分支设备不会将不会从 BBC[地址池集中管理]处获取 DHCP 地址池。



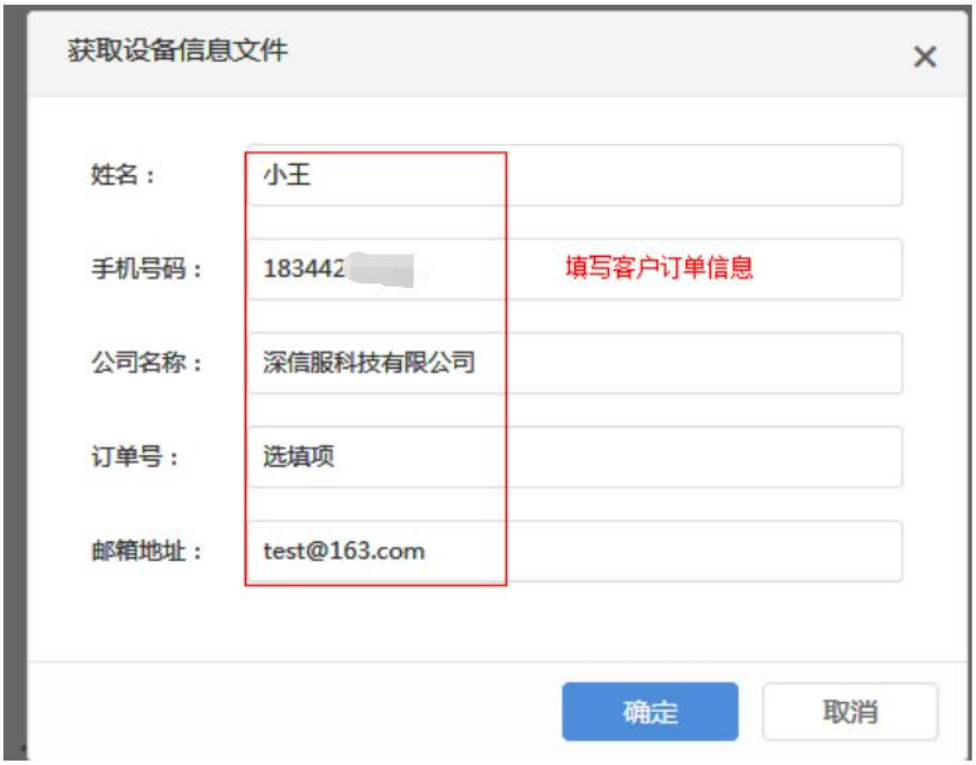
- 设备信息导入完毕后，点击<下一步>，进行接入云图配置。



设备信息列表获取

以上是针对客户已经有了部署SDW-R 设备的信息列表，如果客户还没有拿到信息列

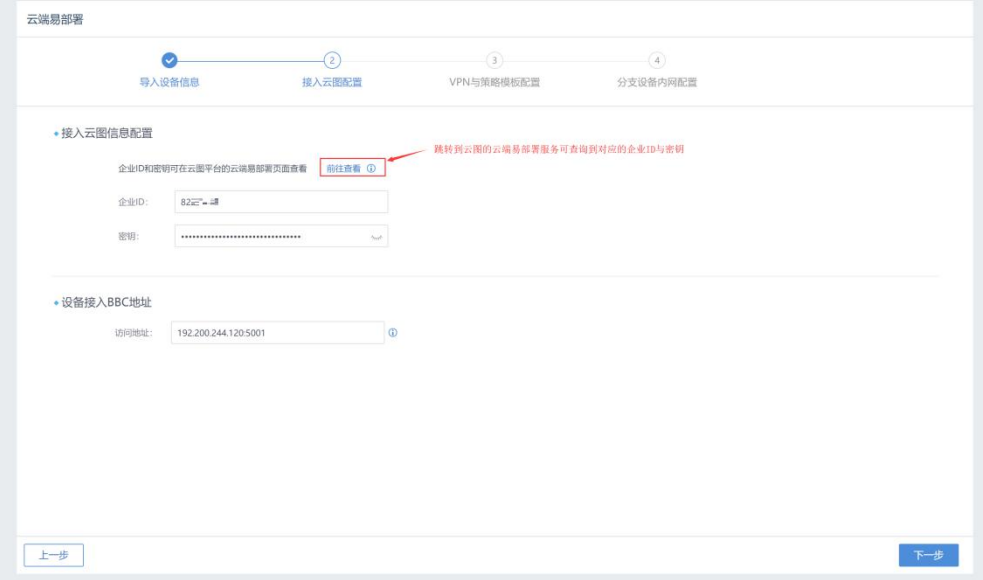
表，可以进行申请设备信息表，再导入，具体步骤如下。



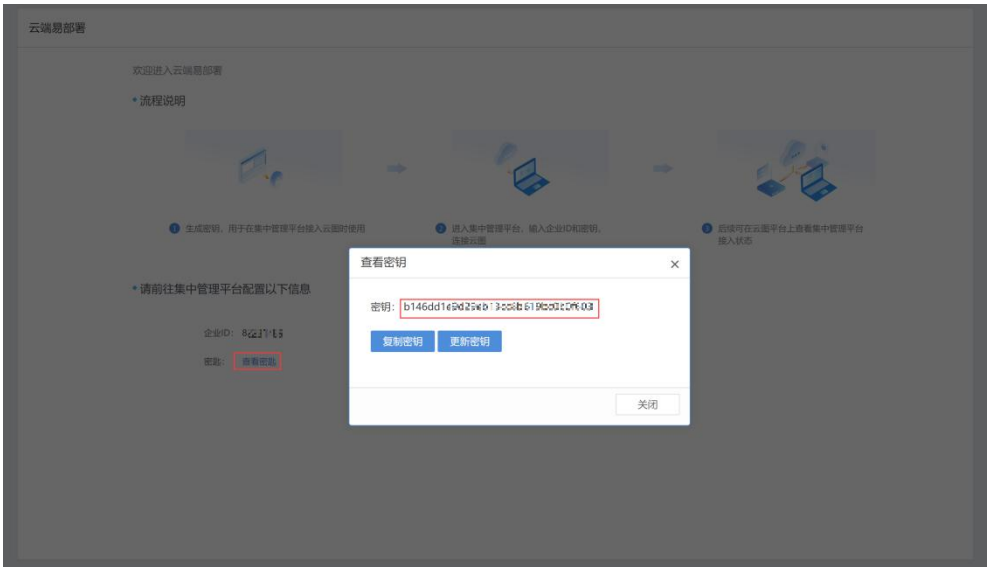
拿到设备信息列表后导入设备信息，继续下一步。

3. BBC接入云图。

- 填写接入云图信息配置：企业 ID 和密钥，可点击<前往页面>进入云图获取。



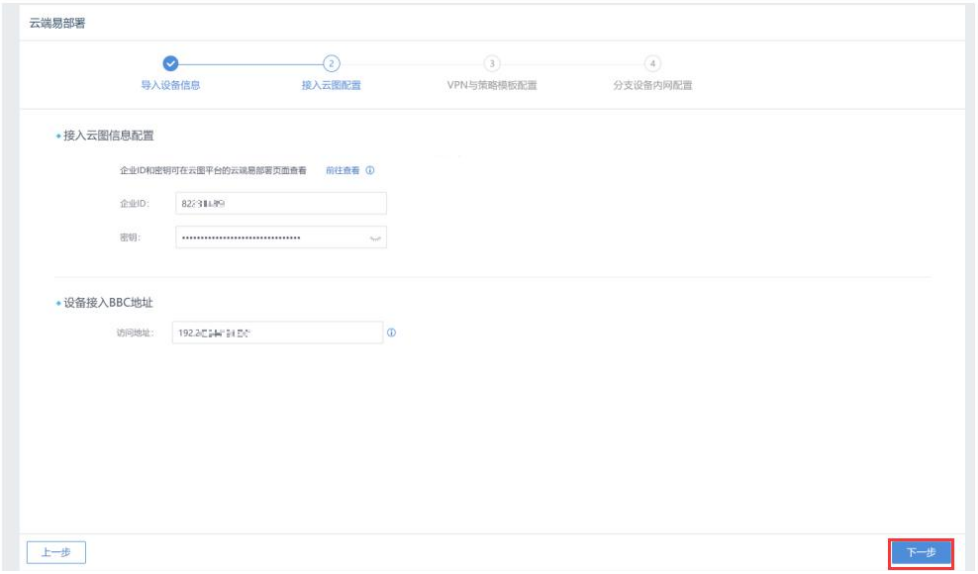
- 在云图界面复制企业 ID 和密钥，回到 BBC 云端易部署初始配置第二步填写。



- 接入云图信息配置填写完毕后，可选择修改设备接入 BBC 地址与端口。然后点击<下一步>。

⚠ 注意：

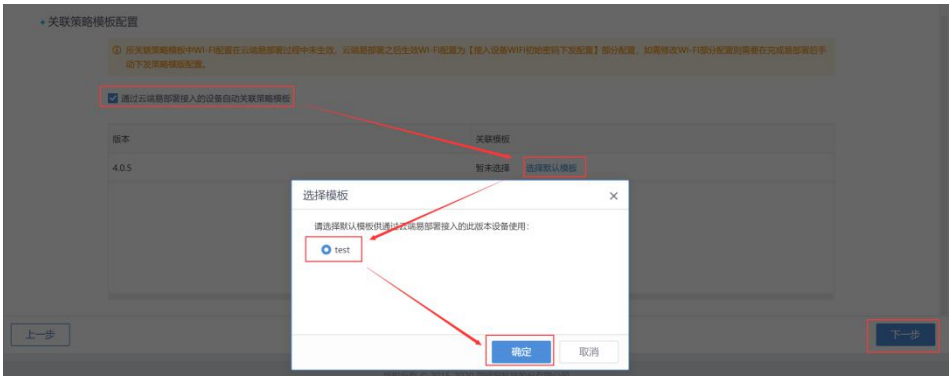
这里的地址必须是分支可以访问到的地址，BBC 单臂在内网，通过出口网关映射进来的话，这里应该配置映射的公网 IP。



4. VPN和策略模版配置。

- 勾选[通过云端易部署接入的设备自动加入默认 VPN 拓扑]，然后勾选已有的 VPN 拓扑或新增。

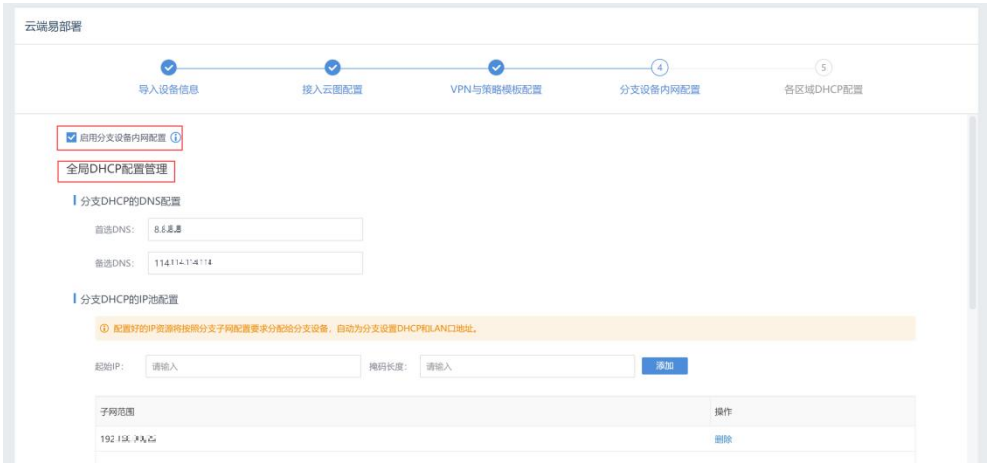
- 勾选[通过云端易部署接入的设备自动关联策略模板]，然后勾选已有的策略模板或创建。完成后点击<下一步>。



5. 分支设备内网设置。

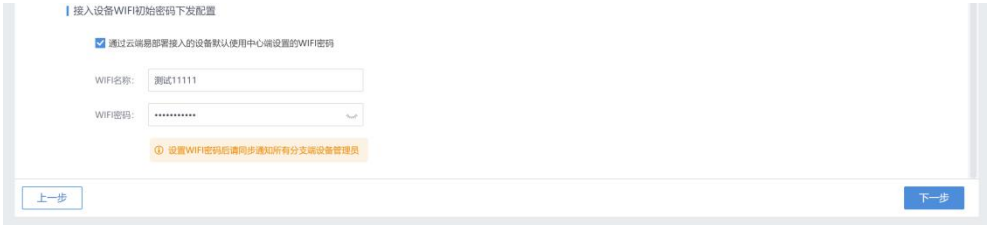
分支从全局地址池获取内网网段

A. 启用分支设备内网配置，并设置相应的全局DHCP的配置。



B. 可设置区域DHCP地址池的掩码长度与分支设备所获取到的DHCP地址池的掩码长度、设置子网自动回收的相关设置。

C. 设置WIFI相关的配置。

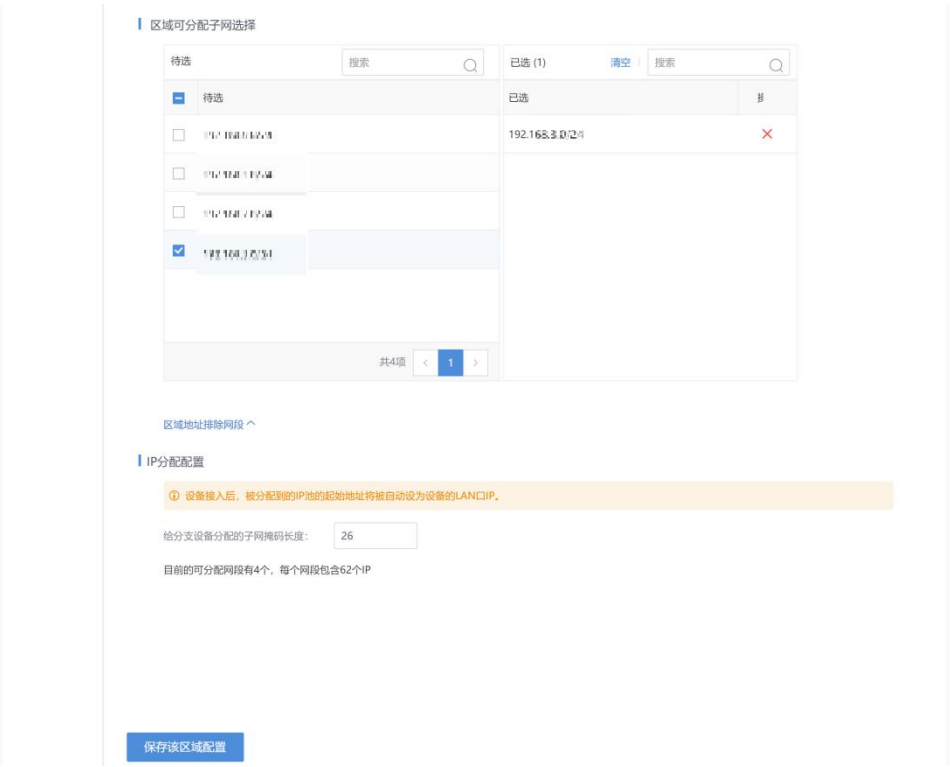


分支从指定地址池获取内网网段场景

A. 按上述方式配置完成全局DHCP地址池。

B. 设置区域DHCP地址池配置。

C. 配置完分支的DNS配置之后，选择区域可使用的子网，并设置区域中每个分支设备能分配到的地址池的掩码长度。最后保存该区域配置，点击<完成>即可。

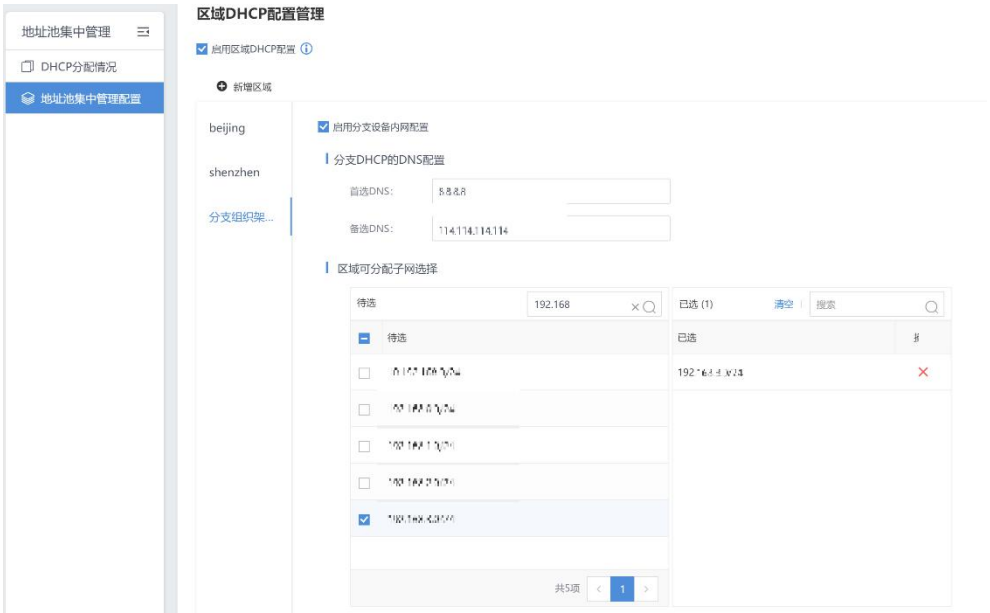


6. 确认配置信息。

A. 查看配置完成的相关配置项信息，包括云图接入配置、设备信息导入、关联策略模板配置等。

B. 查看配置完成的全局DHCP地址池相关配置，在BBC的[管理/地址池集中管理]配置处查看相关配置。

C. 查看配置完成的区域DHCP地址池相关配置，在BBC的[管理/地址池集中管理]配置处查看相关配置。



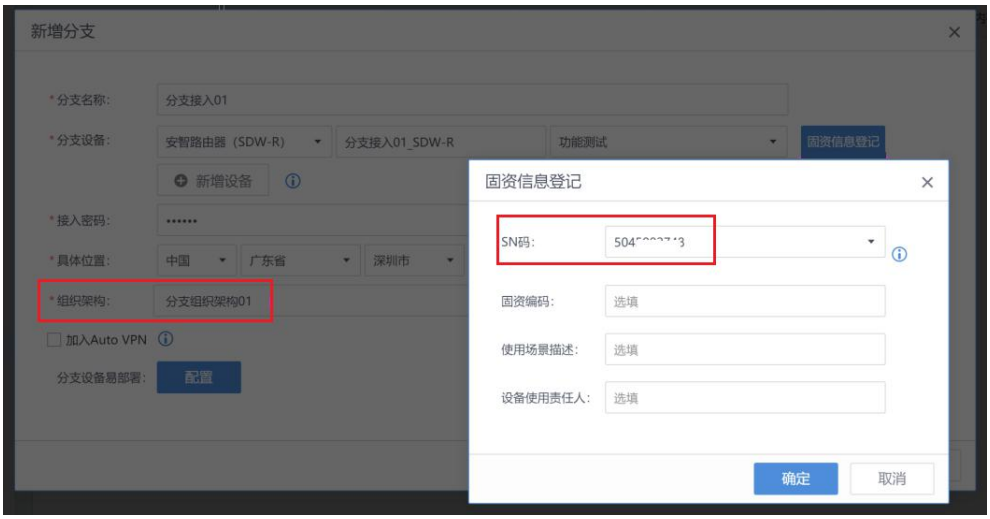
⚠ 注意：

分支从指定地址池获取内网网段场景还需要配置 SDW-R 的 SN 码关联分支信息，配置参考 7、8、9 步骤。

7. BBC上手动创建分支设备接入名称，关联对应SDW-R的SN码、策略模板、组织架构。配置与云端易部署设备清单中的设备SN码一致，并选择与DHCP地址池中配置的组织架构也保持一致。保证SDW-R通过云端易部署时，通过SN码绑定的分支名称进行接入。

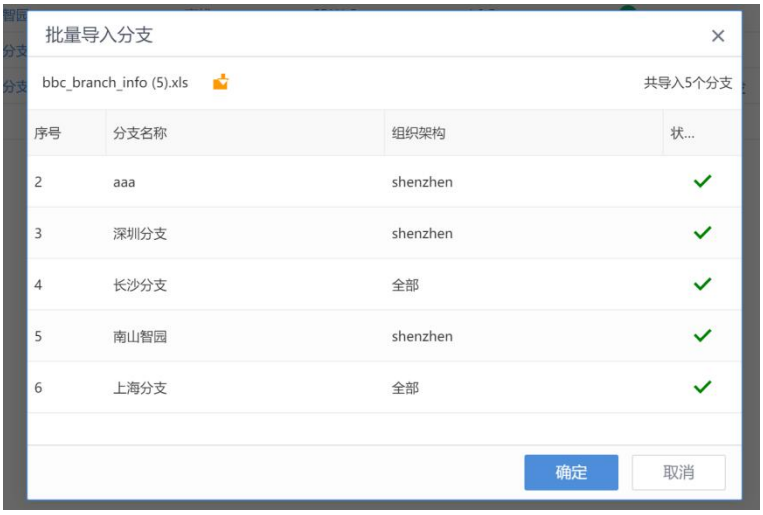
⚠ 注意：

该关联 SN 码的操作需要在导入设备信息之后再进行配置。



8. 若分支数量比较多，可在BBC上导入分支信息表格模板，在信息模板中填写对应的分支信息，比如分支名称、设备类型、设备名称、接入密码、SN码、组织架构的信息。填写完成之后选择上传文件，将对应的分支信息表格导入到BBC中，如下图。

9. 填写完成之后，将对应表格导入到BBC中，确认分支信息无误之后点击<确定>，导入分支信息。



10. SDW-R的SN码关联BBC的分支信息之后，分支端即可进行部署上线。

步骤2. 分支设备上线

分支部署人员通过扫描设备面板上二维码观看云端易部署教学视频，根据教学视频里面的操作步骤，给设备插电，接线。

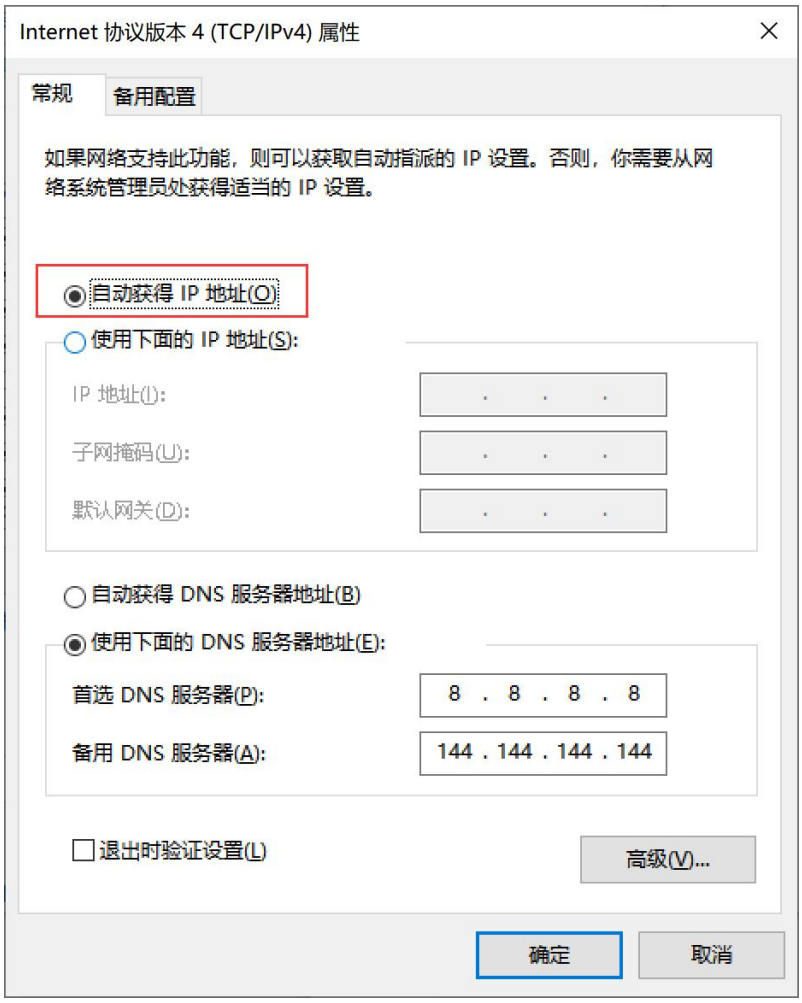
1. 将深信服设备接上电源线，如下图所示。

2. 将运营商网线插入深信服设备的 GE3 口（4G设备可插入4G卡），如下图所示。

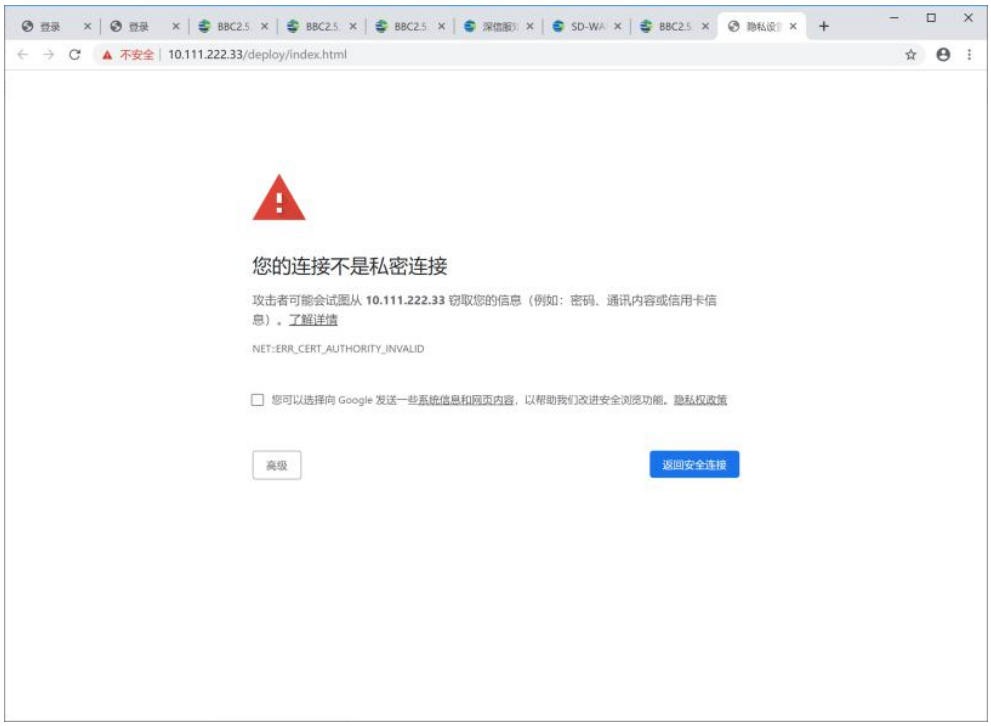
分支设备上线有三种方式，分别时标准版设备、WIFI版设备、4G版设备，下面一一进行介绍。

标准版SDW-R设备上线（无WIFI无4G模块设备）

1. PC拿一根网线接入到SDW-R设备的GE0口，共享网络中心IP获取方式为DHCP方式。

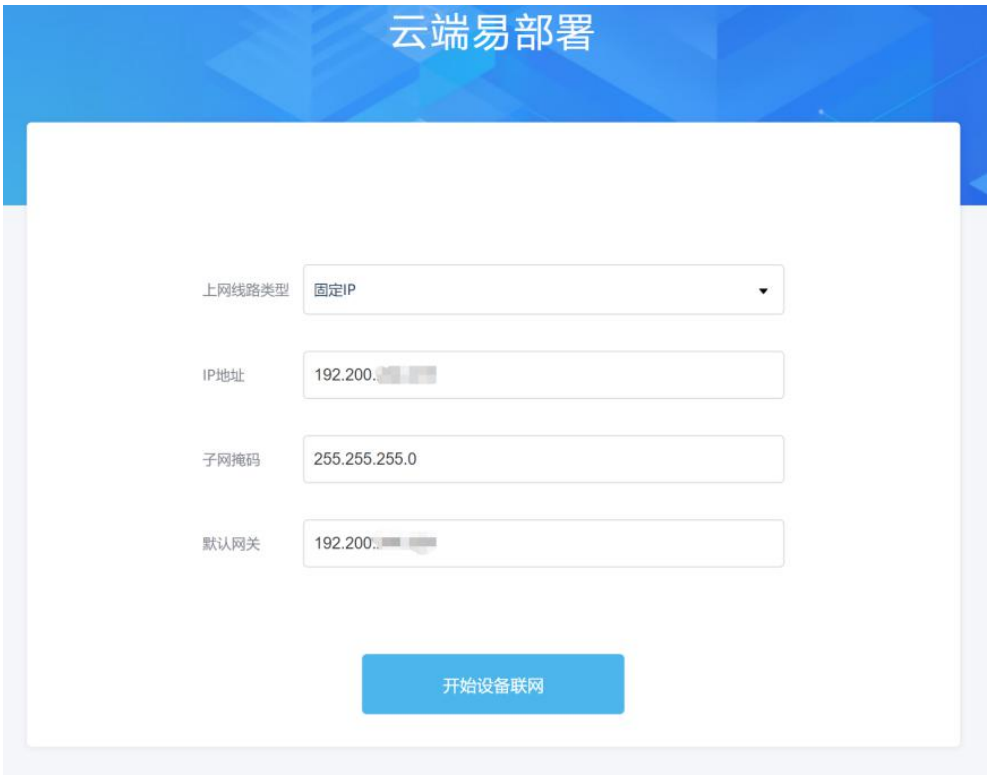


2. 设置成功之后输入https://ztp.sanfor.com或者输入10.111.222.33，进入易部署页面，如下图所示。



3. 点击<高级>，继续前往，进入到设备界面进行外网互联配置。

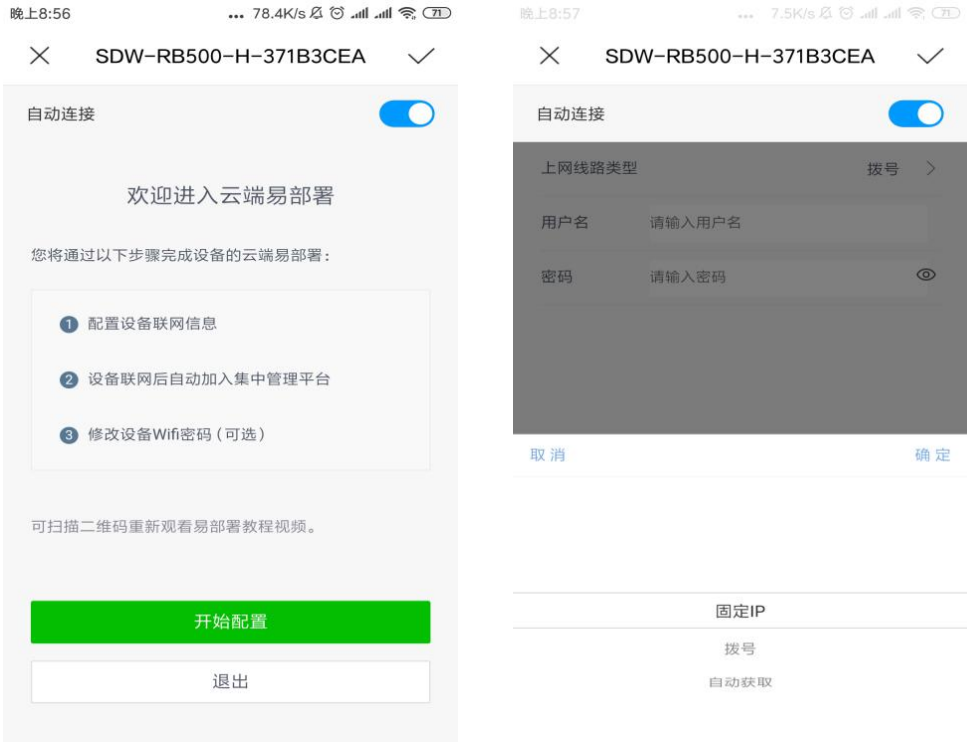
4. 点击<开始配置>，配置外网连接，选择上网线路类型，设置完成之后，点击<开始设备联网>，即可完成配置。



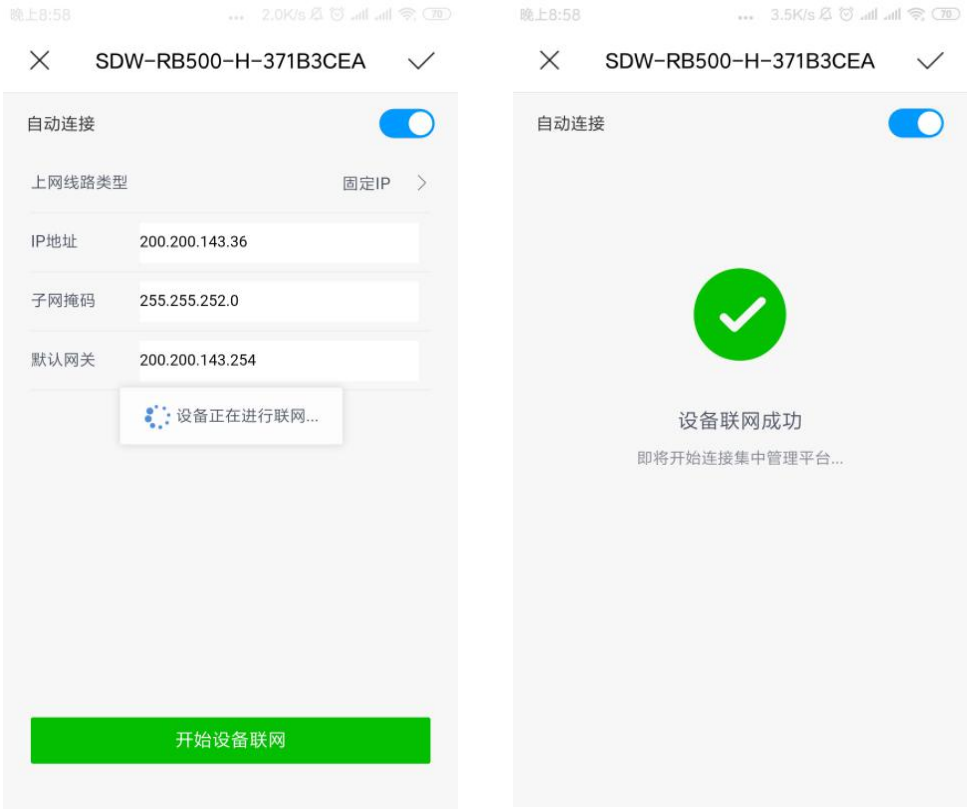
5. 等待SDW-R设备自动连接BBC，连接成功之后部署完成。

WIFI版SDW-R设备设置（有WIFI模块的设备）

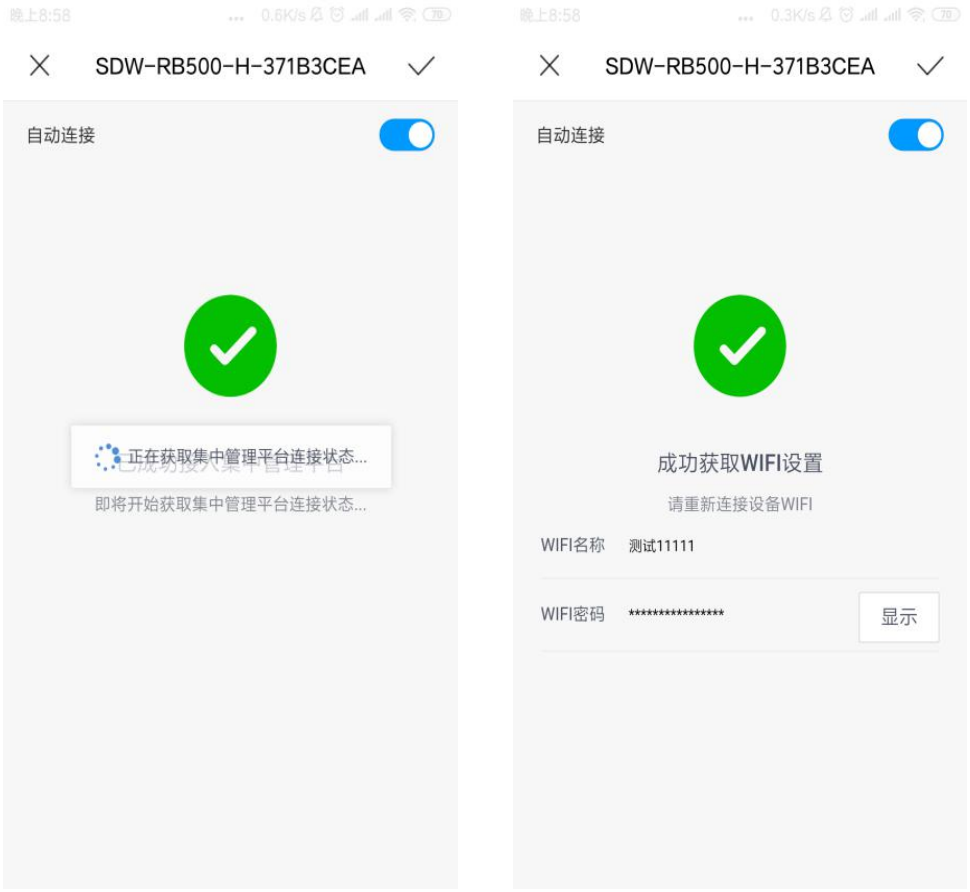
1. 连接SDW-R设备WIFI，默认WIFI名：SDW-R加上网关序列号。连接成功后，会自动弹出首页，点击<开始配置>，选择上网线路类型。



2. 配置SDW-R设备上网线路类型，分支设备联网访问BBC，接收BBC下发到分支的配置。



3. 等待1-2分钟同步完成BBC下发的配置之后，分支设备即可完成上线。注：需要查看该界面的WIFI名称与密码，易部署完成之后，WIFI相关的配置也会同步BBC上的配置。



4G版SDW-R设备设置

在设备的旁侧插入4G上网卡，设备自动组网上线并将自动接入集中管理平台。

设备自动组网上线，并自动接入集中管理平台，过程需1~2分钟，请耐心等待。

DHCP线路云端易部署设置

确认外网线路可以自动获取IP上网，将可以上网的外网线路接入SDW-R的GE3口，然后静等5-8分钟左右等待设备自动上线。

步骤3. 查看分支设备上线情况

1. 通过以上四种方式完成云端部署之后，分支设备自动加入BBC的集中管理。

4G易部署时插入4G卡之后等待3-5分钟之后，设备的4G指示灯正常闪烁，在BBC端可看到SDW-R正常上线。

DHCP线路云端易部署时约5-8分钟之后，总部端可以在BBC端查看SDW-R接入状态，分支端可以通过手机查看SDW-R对应的WiFi设置，确认分支SDW-R成功上线。

2. 分支端WIFI版设备部署完成之后，可以使用手机查找到相应的WiFi名称。通过笔记本或者其它移动终端开启WIFI搜索相关WIFI名称，检查WIFI名称已修改为BBC上配置的WIFI名称。


4:41
WLAN
WLAN
可用 WLAN 列表
已保存，加密 (可上网)
加密
加密
加密
测试11111
加密
加密
添加其他网络

3. 控制台的使用

3.1. 登录 WebUI 配置界面

设备出厂的默认IP见下表。

表1 设备出厂的默认IP对应表

接口	IP 地址
GE0/GE1	10.254.254.253/24
GE2	10.254.253.253/24

SDW-R支持WEB管理，使用443端口登录，如果使用初始地址登录LAN口，那么登录的URL地址为：https://10.254.254.253。

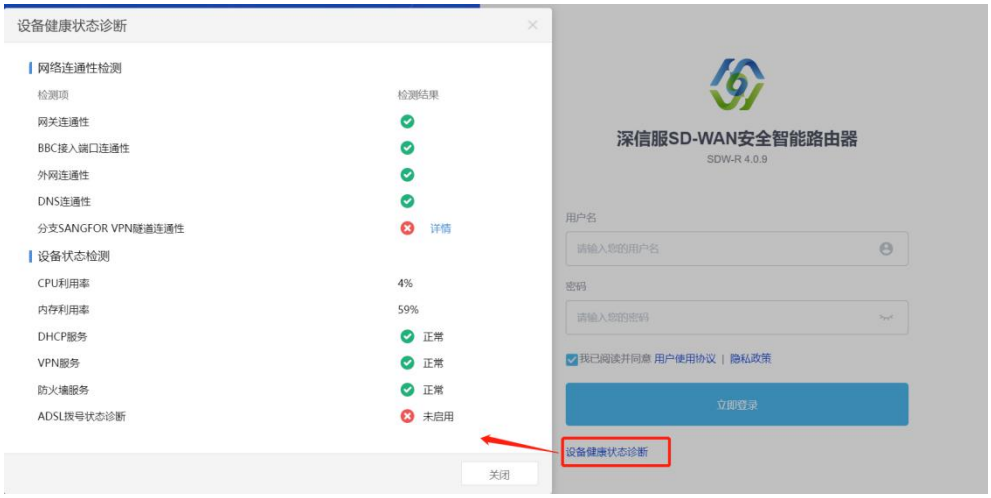
按照前面所示方法接好线后，通过Web界面来配置SDW-R硬件网关设备。方法如下：

1. 给本机配置一个10.254.254.X网段的IP（如配置10.254.254.100），掩码配置为255.255.255.0，然后在IE浏览器中输入网关的默认IP地址及端口，输入https://10.254.254.253，支持IE、谷歌浏览器和火狐浏览器。如下图。

2. 在登录框输入用户名和密码，勾选“我已阅读并同意 用户使用协议|隐私政策”，点击登录按钮即可登录SDW-R产品进行配置，默认情况下的用户名和密码均为：admin。如果需要查看当前设备的版本号，可在登录界面即可看到相应的版本号，

如下图。

3. 点击<设备健康状态诊断>，可查看到设备网络连通性检测、设备状态检测。其中网络连通性检测包括网关连通性、BBC接入端口连通性、外网连通性等；设备状态检测包括CPU利用率、内存利用率、DHCP服务等。



4. 登录控制台后，页面展示如下，由监控中心、VPN、安全管控、网络设置、系统几部分组成，在后续章节详细说明。

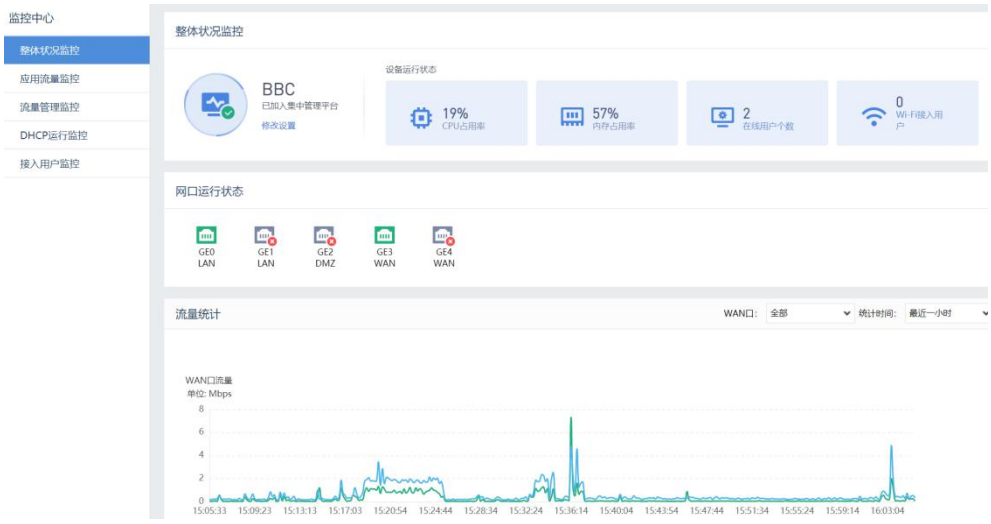
> ⚠ 注意：
>
> 所有配置界面中如果有确定或完成按钮，则配置完毕后，必须要点击该按钮才能使设置保存并生效，后面的文档不再赘述。

3.2. 监控中心

监控中心包含整体状态监控、应用流量监控、流量管理监控、DHCP运行监控和接入用户监控。

3.2.1. 整体状态监控

管理员登录控制台，在[监控中心/整体状态监控]页面下，可以查看本设备是否加入集中管理平台（BBC）、当前设备的运行状态、网口运行状态、流量状态等，便于管理员查看及运维管理。



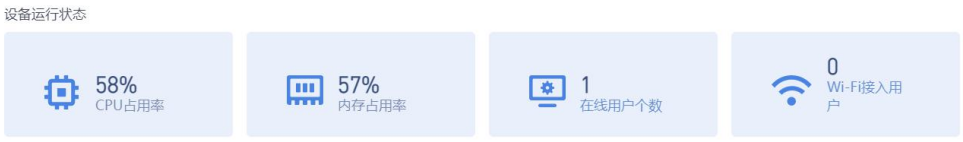
1. **BBC接入状态。**

- 若状态为已加入 BBC 平台，则可以实现在 BBC 平台上对设备的统一纳管。
- 若没有加入 BBC 平台，可以点击<去设置>，跳转到“加入集中管理设置”页面，配置 BBC 的 IP、接入设备名称等信息，详情可参考“加入集中管理”章节。

- 如需要修改 BBC 平台的信息，可以点击<修改设置>，跳转到“加入集中管理设置”，配置 BBC 的 IP 地址、接入的设备名称、密码等信息，修改配置前需要“解除集中管理”。

2. 设备运行状态

在设备运行状态栏下，可以查看当前设备CPU占用率、内存占用率、在线用户个数、WiFi接入用户，如下图所示，当CPU占用率和内存占用率过高时，管理员可以及时的对设备进行检查，避免影响设备的使用性能；同时能直观的显示当前设备的用户数量，包含在线用户个数和WiFi接入用户数量。



点击<在线用户个数>模块，可以跳转至“接入用户监控”页面，查看接入用户的详细信息。

点击<WIFI接入用户>模块，可以跳转至“WiFi设置”页面，查看WiFi的设置详情。

3. 网口运行状态

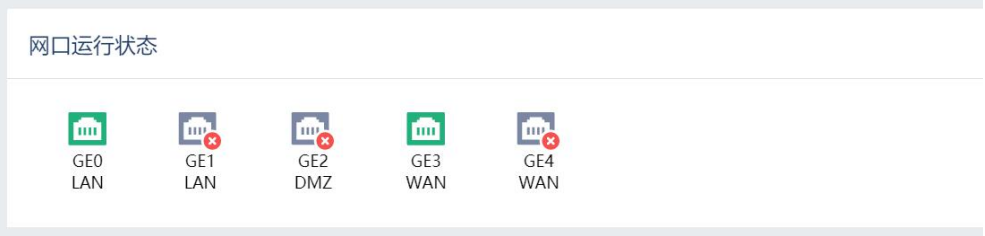
网口运行状态直观的展示当前设备物理网口数量、网口属性以及网口状态等信息。

网口状态主要有三中颜色区分。

状态	说明
网口显示为“绿色”	网口正常使用

网口显示为“灰色”	网口未使用
网口显示为“红色”	网口处于离线故障状态

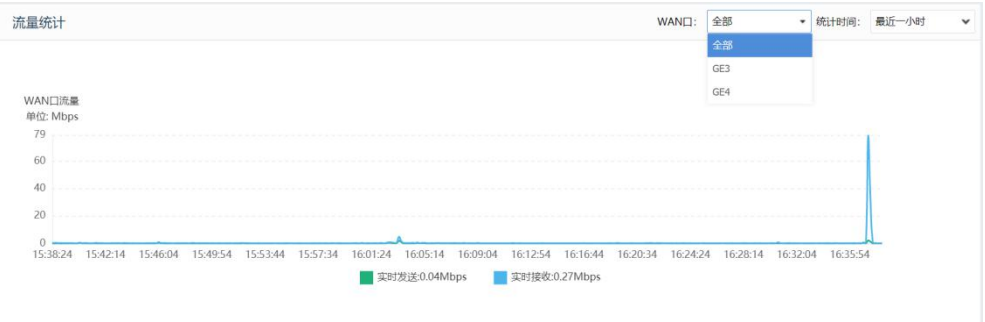
网口运行状态如下图所示。



名称	说明
LAN 口	局域网口，一般用于连接 PC 等终端设备
DMZ 口	隔离区接口
WAN 口	用于连接外网

4. 流量统计

可以查看WAN口的流量，也可以切换GE3/GE4视角，可设置查看最近一个小时或者最近一天的总体流量图，如下图。

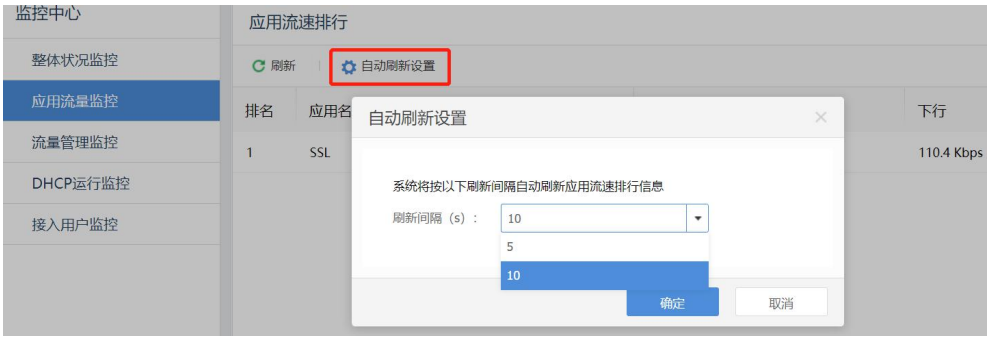


3.2.2. 应用流量监控

在应用流量页面，可以按指定刷新间隔自动刷新应用流速的排行，页面展示应用的排名、应用名称、上下行速率以及总流速。

点击<自动刷新设置>，可以设置刷新的间隔，刷新间隔为5秒/10秒，默认为5秒。可

以根据使用需求进行切换调整，如下图所示。



📖 **说明：**

应用流量监控排行，页面最多显示 15 个排名。

3.2.3. 流量管理监控

流量管理监控可以查看监控线路、线路流量监控图、通道实时信息等内容，监控线路包括：GE3\GE4\VPNTUN。此处以“GE3”为例，GE4\VPNTUN类似，此处不在详细说明。

1. 线路流量监控

线路流量监控实时展示通道的上行流速、下行流速、总流速，通道分为保证通道、限制通道和默认通道。点击“上行流速/下行流速/总流速”可以对流量趋势图进行筛选，如下图所示。

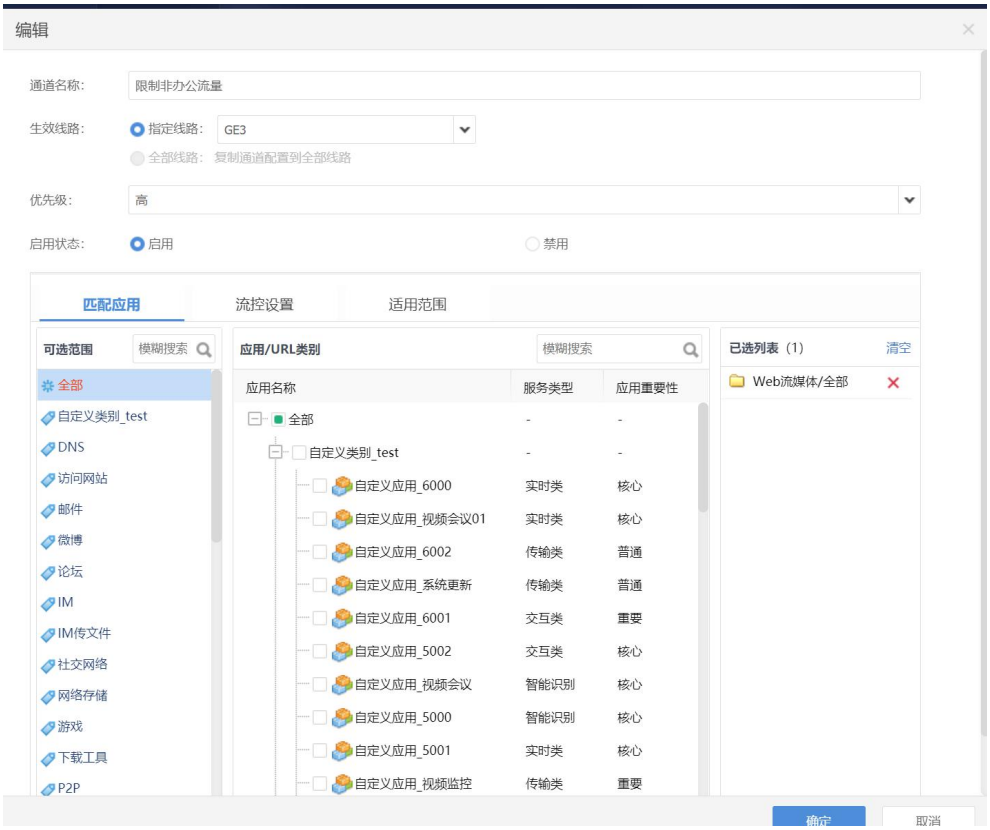
当鼠标移至线路流量图时，可以实时展示三种通道的流速。

2. 通道实时信息

实时展示不同通道的使用用户数、瞬时速率、状态等内容。

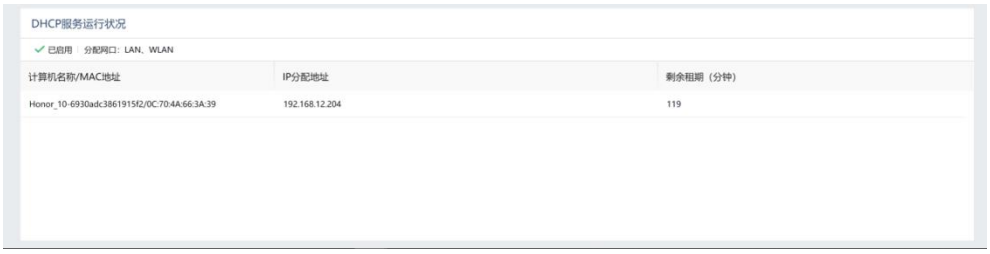
点击操作栏下的<查看详情>，可以查看流量状态详情，包含上行流速、下行流速、应用流速排名TOP10、用户流速排名TOP10。

点击<修改通道配置>，可以对通道配置进行编辑，包括修改通道名称、生效线路、优先级、启用状态、匹配应用、流控设置、适用范围等，如下图所示。



3.2.4. DHCP 运行监控

DHCP运行监控页面可以查看DHCP的运行状态和给其他计算机分配IP的情况，如下图。



3.2.5. 接入用户监控

在接入用户监控页面，可以查看接入用户的详情，包含终端名称、IP地址、MAC地址、接入时间、接入时长等信息。

点击操作栏下的<移入黑名单>，可以快捷将该用户强制下线并移入黑名单。

点击<管理接入用户>，可以跳转至“黑名单”页面，查看加入黑名单的用户，同时，支持对用户移出黑名单的操作。

支持通过IP地址、MAC地址、终端名称以及搜索的方式对接入用户进行筛选。

3.3. VPN

包括[VPN运行状态]、[基本设置]、[SD-WAN选路模板]、 [SOFAST优化设置]、[接入账号管理]、[连接管理]、[第三方对接管理]、[隧道间路由设置]、[证书管理]、[高级设置]等模块。

3.3.1. VPN 运行状态

1. [VPN运行状态]可以查看当前VPN连接和网络流量信息。如下图。

2. 勾选开启VPN服务，可以开启或关闭VPN服务。

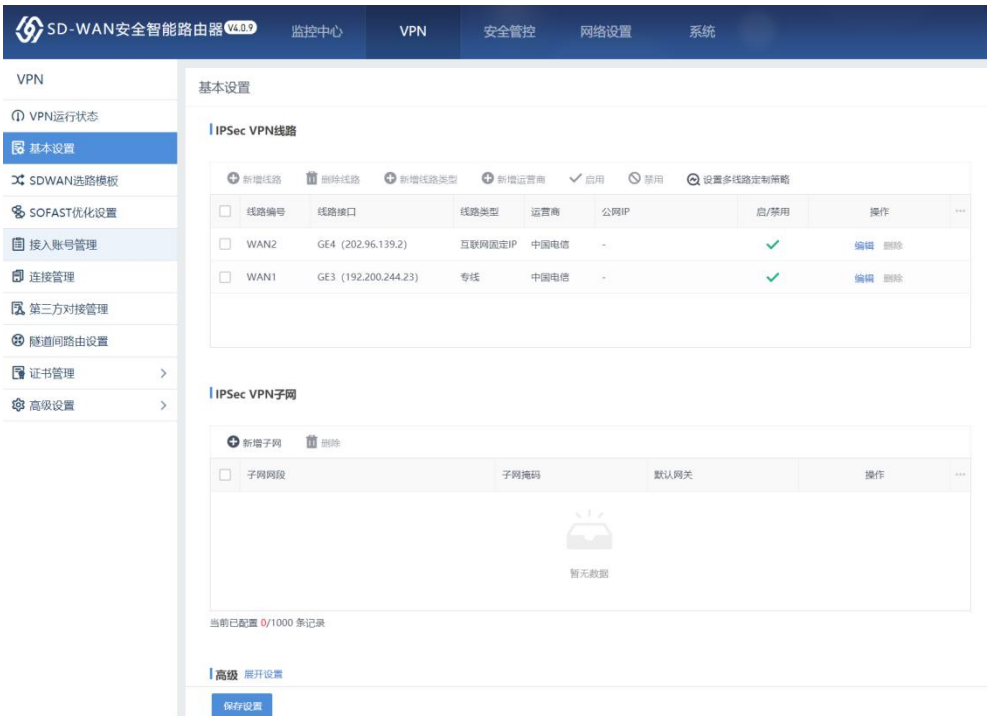
- [VPN 口流量]：可查看对应的 VPN 接口流量，可查询最近 1 小时、最近 24 小时的流量图。
- [隧道实时监控]：与首页“VPN 隧道监控”章节内容相同。

3. 连接告警阈值设置

可以查看隧道实时监控的信息，包含对端名称、设备类型、公网IP、发送流速、接收流速、发送丢包、接受丢包、时延、抖动。点击<连接告警阈值设置>，可以配置以下信息，如下图所示。

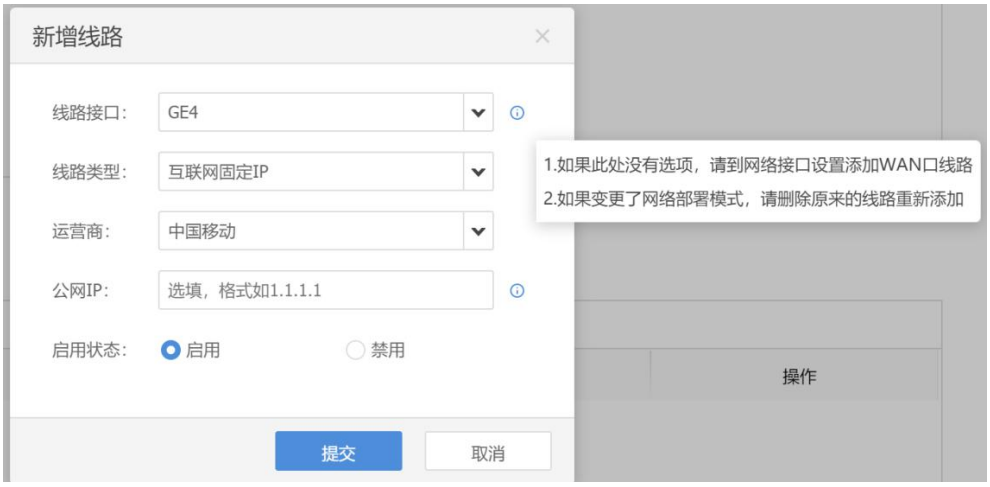
3. 3. 2. 基础设置

[基础设置]中包括[IPSec VPN线路]、[IPSec VPN子网]、[高级]等配置项，页面如下图。



3.3.2.1. IPSec VPN 线路

设备开启多线路授权的情况下，网络接口处配置了多个WAN接口，可以通过该配置项新增多条VPN线路，点击<新增线路>，对VPN线路进行配置，如图。



各配置项说明：

- [线路接口]：选择相应的 WAN 口作为线路接口。
- [线路类型]：可以选择设备预先设置好的类型，也可以点击添加进行自定义线路类型名称，页面如下图所示。

- [运营商]：可以选择设备预先设置好的运营商类型，也可以点击添加进行自定义运营商名称，页面如下。

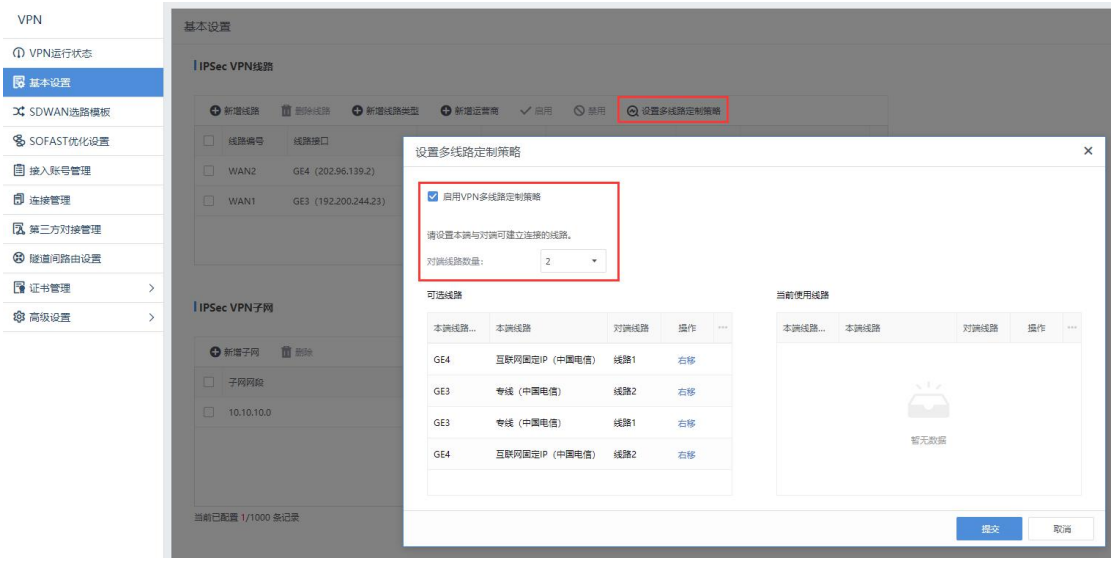
- [公网 IP]：填写相应的公网 IP，若设备网关模式部署可不需要填写该公网 IP，若设备单臂模式部署需要填写对应的公网映射 IP。

  配置完成之后，点击<提交>后，会保留在线路列表中，点击下方的<保存>配置，配置才会生效。

3.3.2.2. SANGFOR VPN 多线路定制策略

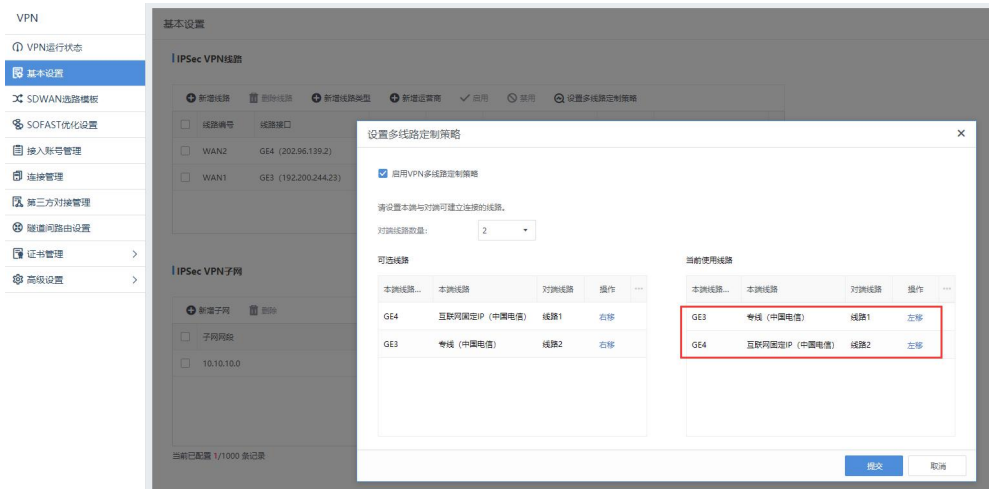
用于设置本端线路与对端指定线路建立SANGFOR VPN连接，未选中的线路不会建立SANGFOR VPN连接。防止跨运营商之间（或者跨线路类型之间）连接SANGFOR VPN连接。例如：总部端线路1为中国电信专线，线路2为中国电信互联网线路；分支端线路1为中国电信专线，线路2为中国电信互联网线路；此时要求总部与分支之间只存在两条SANGFOR VPN连接，分别是总部专线与分支专线之间的SANGFOR VPN

连接、总部互联网与分支互联网之间的SANGFOR VPN连接。此时配置如下图所示：



通过勾选[启用VPN多线路定制策略]启用该功能，根据实际线路情况，选择对端VPN线路数量。根据案例对端线路数量选择为2，通过[可选线路]中的[操作]来选择相应的VPN线路到[当前使用线路]中，设备通过[当前使用线路]中的VPN线路来建立SANGFOR VPN连接的。

本案例中将[可选线路]中的“GE3 专线（中国电信） 线路1”，“GE4 互联网固定IP（中国电信） 线路2”移动到[当前使用线路]。具体操作如下图所示：

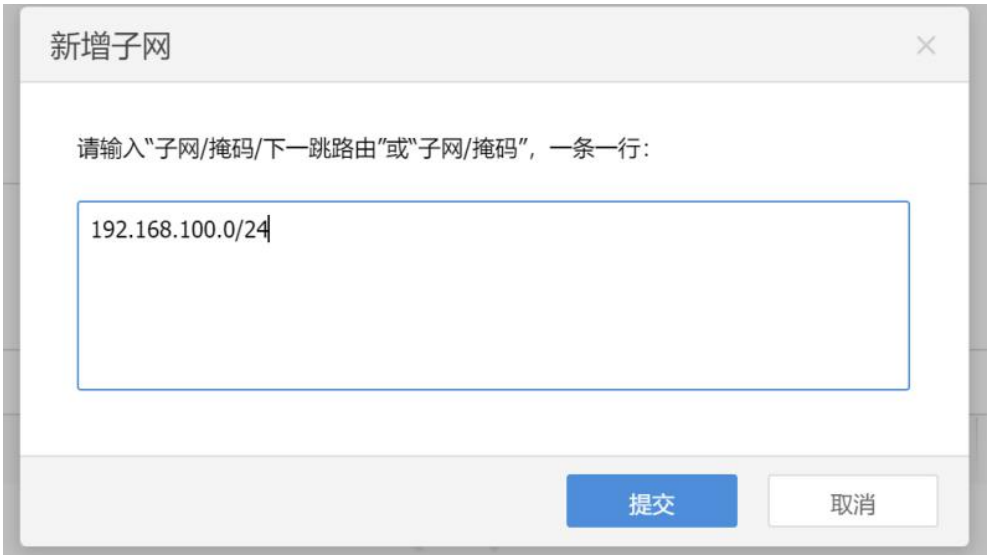


移动线路完成之后，点击[提交]并在基本设置界面[保存配置]配置才会生效。

3.3.2.3. IPSec VPN子网

1. 当设备所处内网有三层交换机或者路由器之类设备，划分了多个网段，则需要在这里将除设备LAN口所在网段之外的其他多个网段的信息给添加进去。

2. 点击<新增子网>，填入本端其他网段地址即可完成IPSec VPN子网列表的添加。页面如下。



注意：

设备 LAN 口和 DMZ 口所在网段，不需要添加到 IPSec VPN 子网列表。只有本地内网有多网段情况，才需要添加其他网段到 IPSec VPN 子网列表。

3. 3. 2. 4. 高级

1. 高级设置中，包括IPSec VPN内网接口、VPN接口、VPN监听端口等配置，页面如下。

各配置项说明：

- [IPSec VPN 内网接口]：包括 LAN 口和 DMZ 口，用于设置 VPN 网段，即属于 LAN 口或 DMZ 口网段范围之内的 IP 地址就认为是 VPN 数据，其他网段 IP 地址都为非 VPN 数据。
- [IPSec VPN 接口]：用于设置本端设备的 VPN 接口 IP 地址，可以自动分配或者手动定义 VPN 接口 IP。
- [IPSec VPN 监听端口]：用于设置 VPN 服务的监听端口，缺省为 4009，可根据需要设置。
- [MTU]：用于设置 VPN 数据的最大 MTU 值，默认为 1500。
- [MSS]：用于设置 UDP 传输模式下 VPN 数据的最大分片。

⚠ 注意：

MTU，MSS 一般情况下请保留默认值，如需设置，请在深信服技术支持工程师的指导下修改。

- [广播]：是否开启广播设置。
- [组播]：是否开启组播设置。

2. 配置完成之后，需点击<保存配置>，配置才可以生效。

3.3.3. SDWAN 智能选路策略

SDWAN选路策略设备本地端无法修改，SDWAN选路策略只可通过BBC下发到设备端，可查看总部端的选路策略或者查看分支端的选路策略。如下图所示。

作为总部时，查看SDWAN选路模板时可查看选路模板名称，模板所关联的分支设备数，以及可以查看选路模板所关联的具体分支设备，如下图所示。

点击[模板名称]时可跳转到SDWAN选路策略界面查看具体的SDWAN选路策略，如下图所示。

可查看BBC下发到总部和分支SDW-R设备的SDWAN选路策略。

点击[查看]可查看到SDWAN选路策略的详细信息。

作为分支时，可查看该设备所关联的总部设备的名称，如下图所示。

点击[模板名称]时，可以跳转到SDWAN选路策略界面查看具体的SDWAN选路策略信息，由于分支端与总部端的选路策略一致，这里就不再赘述了。

⚠ 注意：

1、VPN 池化流控与 SDWAN 智能选路（指定线路选路策略）结合使用时需要注意以下场景的问题：低优先级应用通过 VPN 流控设置了保障通道，同时低优先级应用配置指定线路选路策略，如果此时有高优先级应用也配置指定线路选路策略（与低优先级应用指定同一条线路），高优先级应用会抢占低优先级的应用带宽，会导致低优先级应用流控保障失效。

2、SDW-R4.0.9 及之后版本新增 SOFAST&BEST 选路序列号，该序列号关联 SDWAN 智能选路功能使用，当该授权过期时 SDWAN 智能选路功能将无法配置并保持默认智能选路策略。

3.3.4. SOFAST 优化设置

通过DPI库自动识别应用且划分为交互类、实时类、传输类，智能感知链路质量和匹配链路优化模型，保障在高丢包场景下，依然保障业务流畅访问体验。

1. 开启SOFAST优化功能，选择动态自适应或者自定义条件生效模式，如下图。

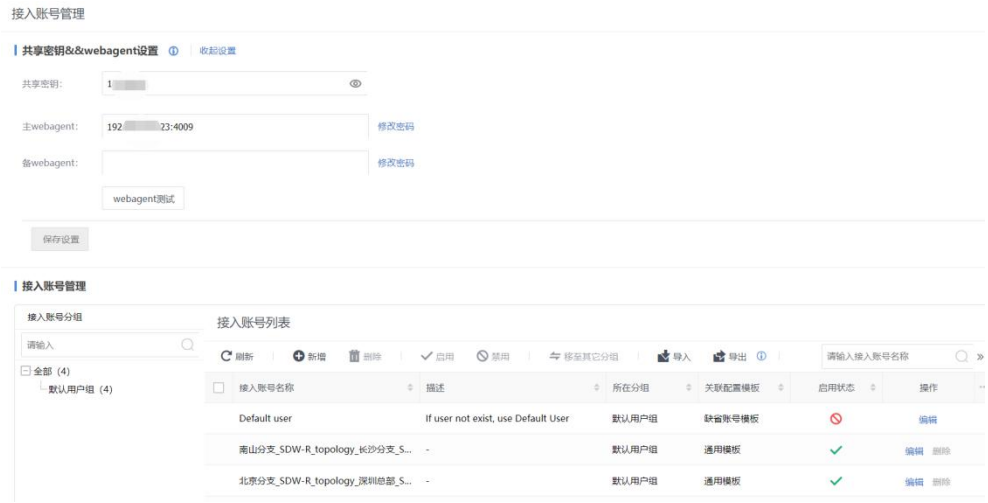
动态自适应是根据设备内置的应用丢包率启用SOFAST优化功能，动态自适应可自行设置SOFAST优化功能生效模式的丢包率阈值。

⚠ 注意：

SOFAST 优化功能必须结合 SANGFOR VPN 传输模式为 UDP 协议一起使用。

3.3.5. 接入账号管理

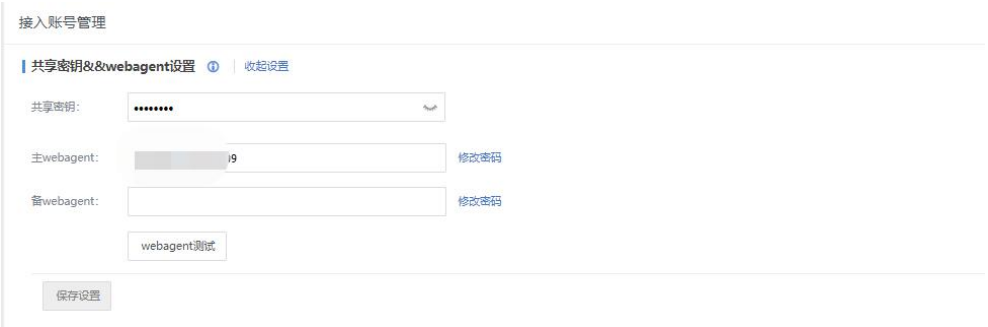
[接入账号管理]用于配置VPN的共享密钥、webagent、VPN分支接入账号，页面如下。



3.3.5.1. 共享密钥&webagent 设置

共享密钥的配置

可以设置共享密钥，防止非法设备接入。在[VPN/接入账号管理]的页面下，配置共享密钥，配置如图所示。



Webagent设置

webagent 设置包含支持的格式、匹配规则以及安全密码建议，如下图所示。

1. Webagent格式主要支持的格式有以下三种：

- 固定 IP：端口（其中固定 IP 支持单 IP 和多 IP，最多支持四个 IP，各 IP 之间以#号分隔，如：202.96.137.75#60.28.239.21:4009），此 IP 为总部网络出口 IP。

- 动态域名：端口（适用于总部已存在动态域名指向他们出口的公网 IP 的环境。如：www.sangfor.com.cn:4009）。
- 动态网页（适用于总部 VPN 设备没有固定公网 IP 的环境，如 ADSL 线路。如：www.sangfor.com/NG4.0/test.php、202.96.137.75/test.php）。

2. 主备webagent的匹配规则

主webagent的优先级高于备webagent，主webagent不可用时，备webagent才生效；分支连接时需要至少与本端配置的主或备webagent匹配上一条。

3. 安全密码设置建议

当webagent格式为动态网页时，可以根据要连接的webagent服务器的密码，在此次设置相同的密码。

4. 点击<修改密码>可以设置Webagent密码，以防止非法用户盗用Webagent更新虚假IP地址，只对页面地址有效。

其他注意事项：

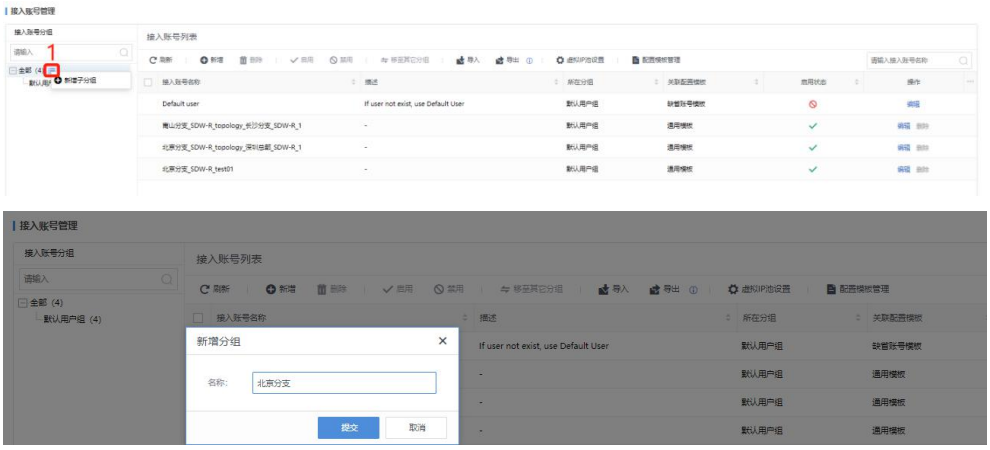
1. 如果设置[Webagent密码]，一旦遗失该密码则无法恢复，只能联系深信服科技客户服务中心，重新生成一个不包含“Webagent密码的文件”并替换原有文件。
2. 如果设置了[共享密钥]，则所有VPN网点都必须设置相同的[共享密钥]才能相互连接通信。
3. 如果是多线路且都是固定IP的情况下，可以采用“IP1#IP2:port”的方式来填写Webagent。

3.3.5.2. 接入账号管理

[接入账号管理]用于管理VPN接入账号信息，设置允许接入VPN的用户账号、密码、设置账号使用的配置模板、是否启用硬件捆绑鉴权、隧道内NAT、多线路选路策略等用户策略。如下图所示。

分组的新建

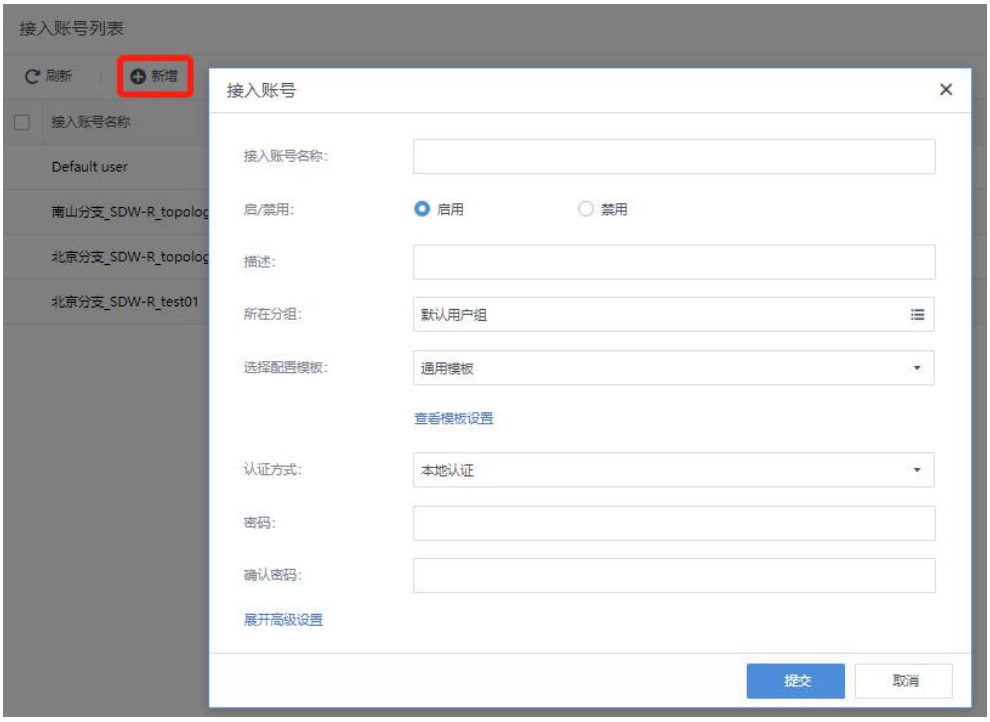
1. 点击[全部]后的“符号”可以新增分组，填写相应的名称，点击<提交>，完成分组的配置，如下图。



2. 配置新增的分组展示如下。

接入账号的新增

1. 在接入账号列表中点击<新增>，可以新增VPN接入账号，可依次设置[接入账号的名称]、[描述]、 [所在分组]等信息，如下图所示。



各配置项说明：

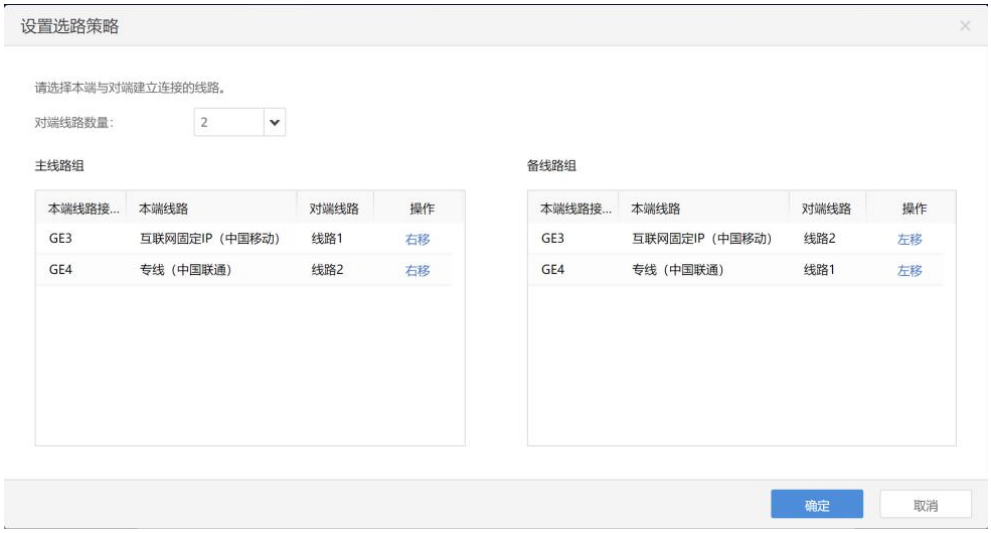
- [选择配置模板]：可查看模板设置，也可新增配置模板，以便修改其中的内容，模板中可配置模板名称、加密算法、是否启用多用户登录、用户的内网服务设置、组播服务、IPSec VPN 隧道超时时间等配置，如下图所示。

  通用模板设置如下图所示。

新增配置模板如下图所示。

- [认证方式]：选择用户的认证方式，包括本地认证、证书认证两种方式。
- [高级设置]：包括用户过期时间、硬件证书捆绑鉴定、隧道内 NAT、多线路选路策略等配置。

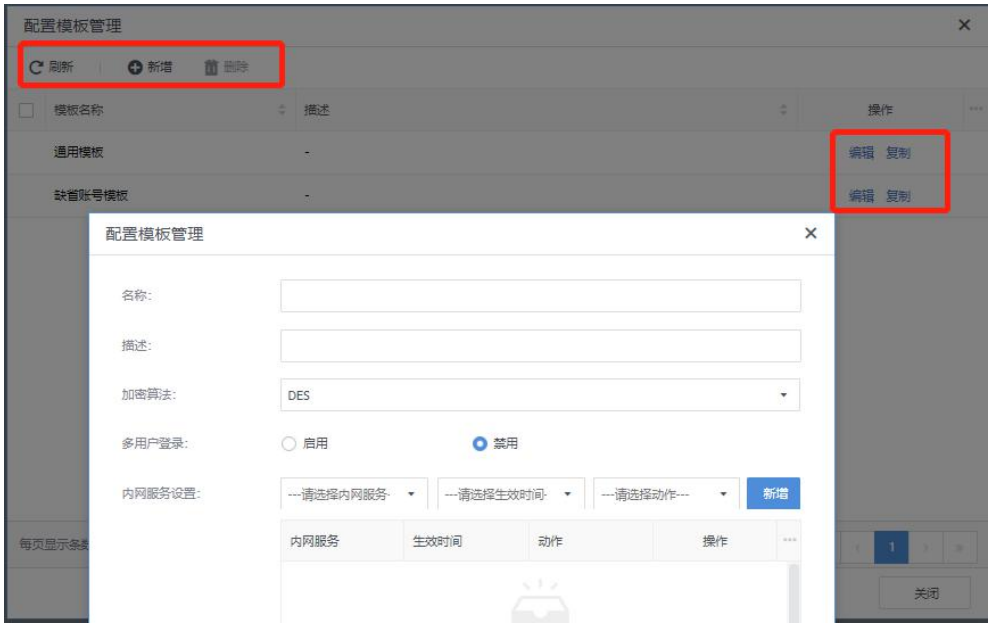
- [高级设置/多线路选路策略]：当智能选路不匹配时走多线路选路策略，根据实际情况选择建立 VPN 连接的两端线路数，然后选择主线路数和备线路数，如下图。



2. 配置完成之后，点击提交完成用户相关的配置。

配置模板管理

管理员在[VPN/接入账号管理]页面，点击<配置模板管理>，可以对当前的模板进行新增、编辑以及删除的操作。



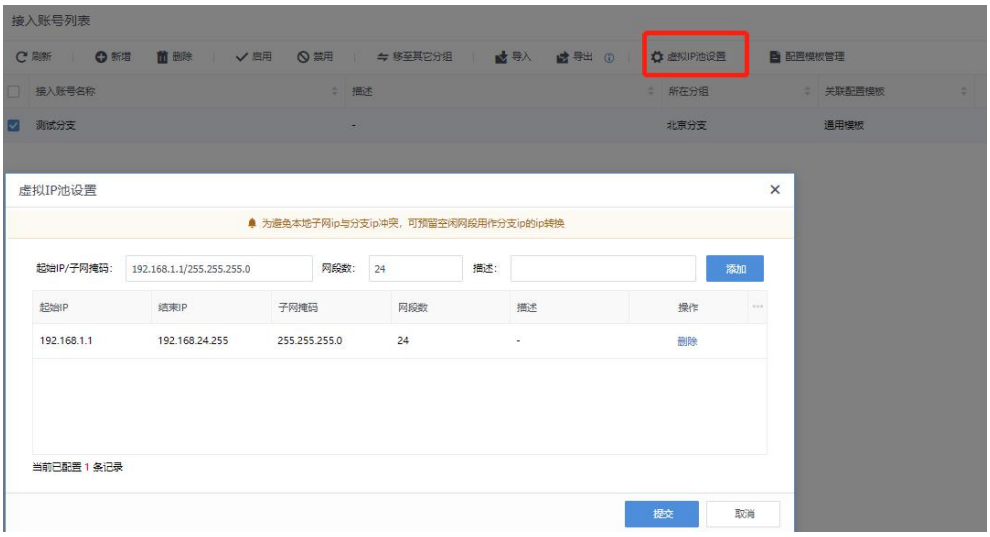
- 点击<新增>，可以进行配置模板中加密算法，内网服务设置、组播服务等进行配置。

配置完成点击<提交>，即可保存在配置模板列表中。

虚拟IP池设置

为避免本地子网IP与分支IP冲突，可预留空闲网段作为分支的IP地址转换。配置如下：

1. 点击<虚拟IP池设置>，创建分支虚拟IP池，分支虚拟IP池中的虚拟IP段提供给分支接入到总部时将分支的原网段替换成虚拟IP池中的一个网段，以解决当两个相同网段的分支同时接入到总部时的内网IP冲突问题。设置时设定虚拟IP的起始IP/子网掩码、网段数、描述，页面如下。



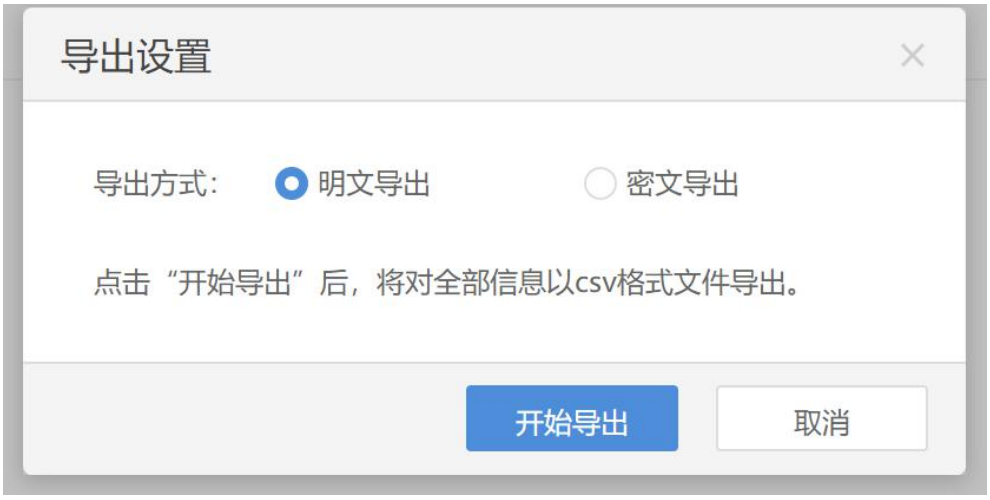
2. 点击<提交>，即可完成虚拟IP池的配置。

接入账号的管理

1. 接入账号列表中，可以对接入账号进行删除、启用、禁用、移动到其他分组等操作，页面如下图。

- 点击<导入>，可以从 CSV 文件中导入用户信息，导入后有相应的提示，如下图。

- 点击<导出>，可以从设备上将用户导出到本地进行保存，并可选择导出的用户密码是明文导出还是密文导出，页面如下。



⚠ 注意：

导入：仅允许导入 csv 和 txt 格式的文件；导出：当前不支持导出证书认证用户。

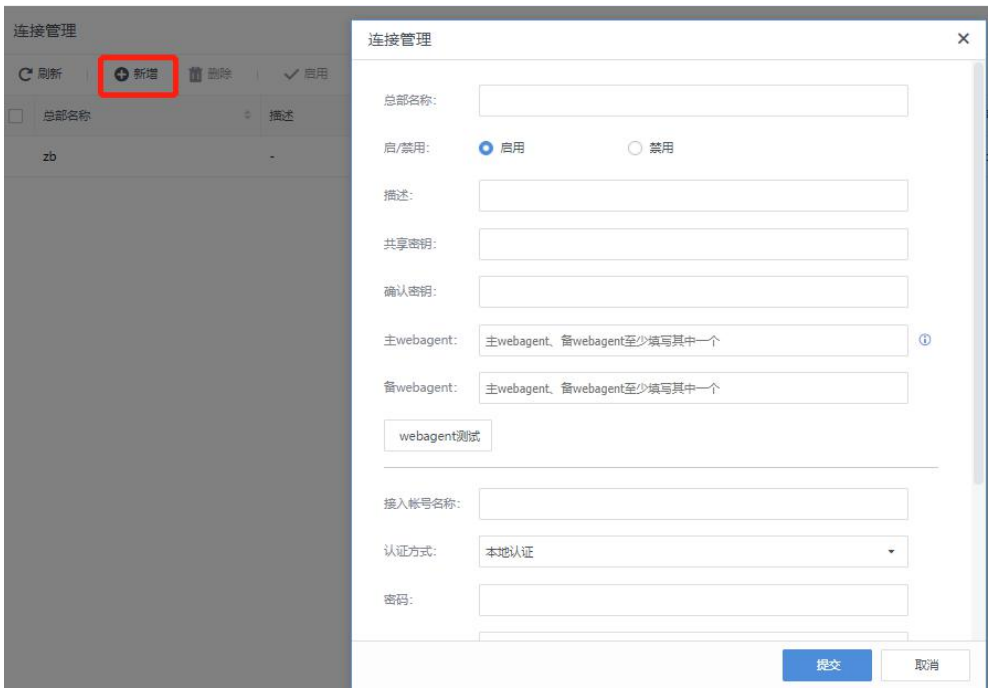
3.3.6. 连接管理

1. 为了实现多个网络节点的互联（组成“网状”网络），VPN硬件网关提供了对网络节点互联的自主管理和设置功能。可在[连接管理]中进行相关的设置。页面如下。

⚠ 注意：

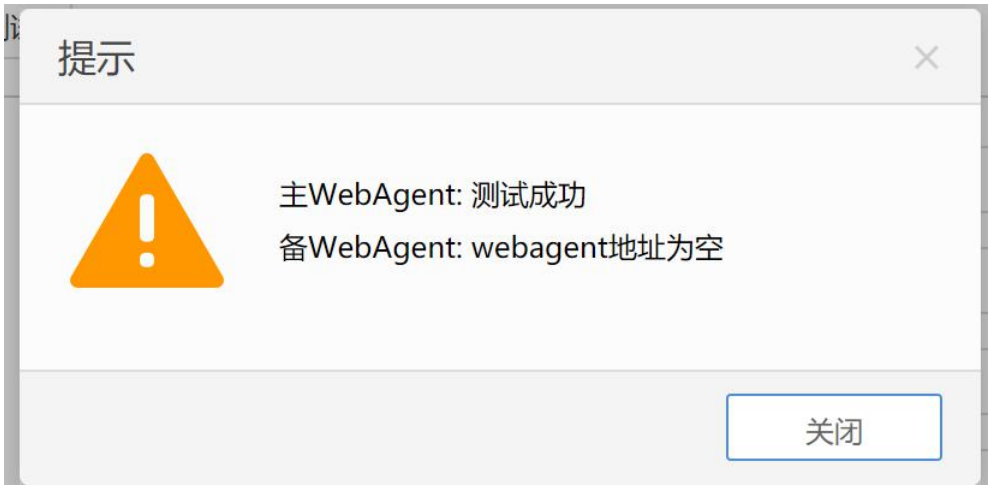
连接管理只有自设备当分支使用需要连接其他 SDW-R 设备时才需要启用，否则本端是 VPN 总部设备，不需要启用连接管理。

2. 点击<新增>，可以添加一个本设备到其他VPN总部的连接，页面如下图。



各配置项说明：

- [总部名称]和[描述]用于标记连接名称，可以自定义填写。
- [共享密钥]、[接入账号名称]、[密码]根据总部提供的接入账号信息来填写。
- [主/备 WebAagent]：用于填写需要连接的总部的对应 Webagent，点击<Webagent 测试按钮>可以测试 Webagent 是否工作正常，结果如下图所示。



说明：

测试请求均是从本机发起的而不是设备发起的。如果 Webagent 是用域名形式，测试成功代表该网页存在，否则网页不存在。如果 Webagent 采用固定 IP 方式，则测试成功代表填写的 IP:PORT 格式正确。该测试成功并不代表 VPN 就一定能连接成功。

- [传输类型]：可选[TCP]或[UDP]，用于决定传输 VPN 数据包的封装类型，默认为[UDP]传输模式。

- [封堵穿透]：使用 UDP 协议建立隧道有可能会被运营商封堵，这个时候可以启用封堵穿透，如下图。

其他说明：

针对TCP的封装穿透是在UDP的报文中加入TCP头部，让数据包从表面上看起来是TCP包，从而可以穿透封堵。但是TCP穿透并没有真正的TCP三次握手，还是有被运营商封堵的概率。

针对ESP的封装穿透是在UDP的报文中加入ESP头部，让数据包从表面上看起来是ESP包，从而可以穿透封堵。这种穿透也有可能被运营商识别从而穿透失败。

⚠ 注意：

如果使用了证书认证，用户名不需要填写，会自动获取证书中的颁发给字段。

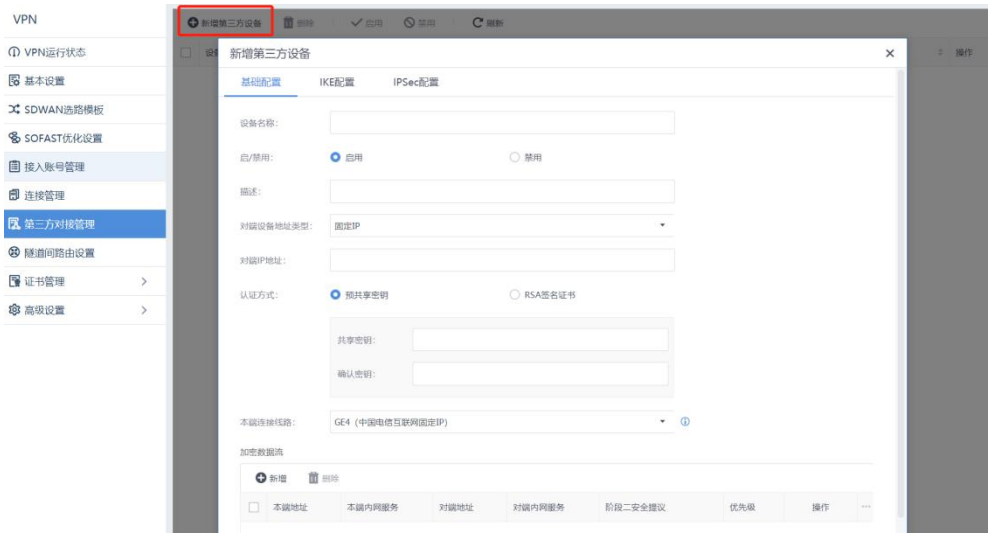
3. 点击[展开高级设置]，可以对VPN对端进行权限设置，即指定VPN对端只能访问本端的哪些服务，如下图所示。

4. 设置完以上信息后，勾选[添加]选项即完成内网服务的设置。最后点击<提交>即激活该连接，并保存设置信息。

3.3.7. 第三方对接管理

SDW-R支持与第三方设备之间建立标准IPSec VPN的对接。深信服的标准IPSEC遵循的是国际标准的IPSEC VPN协议，只要对端的VPN也是用的是标准的IPSEC协议，那本端设备就支持跟对端进行VPN对接。

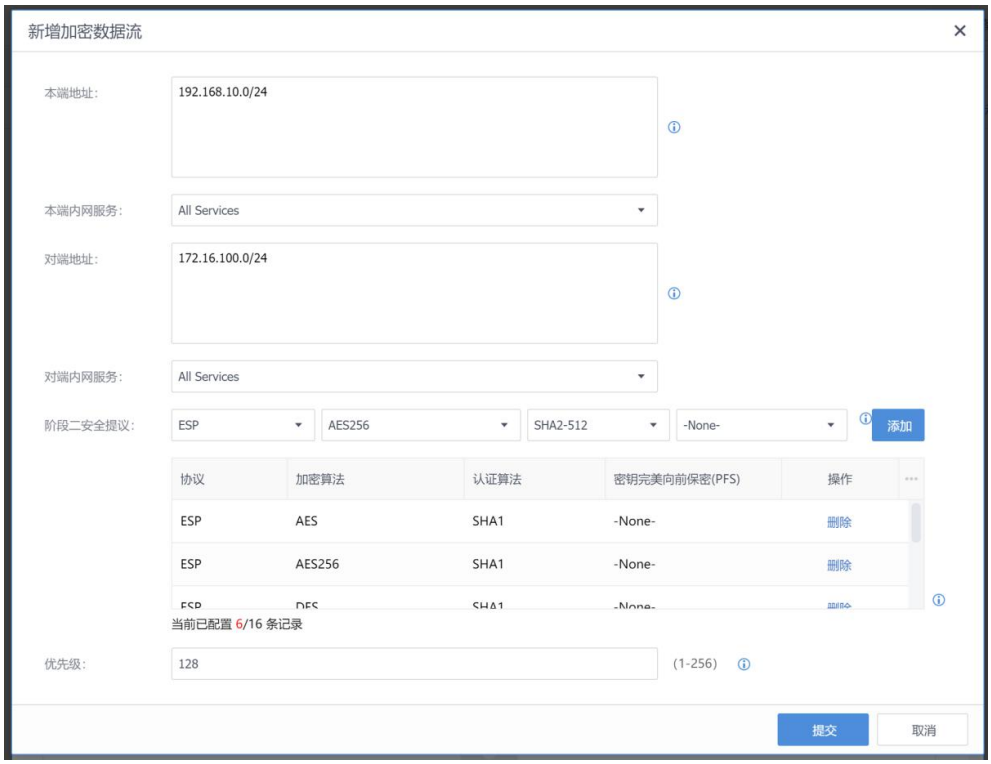
1. 在[VPN/第三方对接管理]页面，点击<新增第三方设备>，可新增标准IPSec VPN连接的配置，如下图。



[基础配置界面]各配置项目说明：

- [设备名称]：设置隧道名称。
- [启/禁用]：启用或者禁用该 VPN 连接。
- [描述]：用于标注隧道名称，可自定义填写。
- [对端设备地址类型]：包括固定 IP、动态 IP、动态域名三种，请根据实际情况选择：选择固定 IP，就填写上对端的 IP 地址；选择动态域名，就填写上对端外网绑定的域名。
- [认证方式]：包括预共享密钥和 RSA 签名证书两种，按需选择。
- [预共享密钥与确认密钥]：填入正确的预共享密钥，并确保连接双方采用的都是相同的预共享密钥。
- [本端连接线路]：根据实际线路情况选择对应的出口线路。
- [加密数据流]：选择设置标准 IPSec VPN 的感兴趣流以及第二阶段协商的参数。

2. 点击<新增加密数据流>可进行感兴趣流与协商参数的配置，如下图。



各配置项目说明：

- [本端地址]：设置标准 IPSec VPN 感兴趣流的源 IP 匹配规则，可填写单个 IP 或者 IP 网段。
- [本端内网服务]：设置标准 IPSec VPN 感兴趣流的源内网服务匹配规则，可选择 ALL Services、ALL TCP Services、ALL UDP Services、ALL ICMP Services 这四种服务类型的某一种，请按需选择。
- [对端地址]：设置标准 IPSec VPN 感兴趣流的目的 IP 匹配规则，可填写单个 IP 或者 IP 网段。
- [对端内网服务]：设置标准 IPSec VPN 感兴趣流的目的内网服务匹配规则，可选择 ALL Services、ALL TCP Services、ALL UDP Services、ALL ICMP Services 这四种服务类型的某一种，请按需选择。
- [阶段二安全提议]：选择阶段二协商时所使用的参数，包括所使用的协议、加密算法、认证算法、是否启用密钥完美向前保密（PFS）；其中数据包封装所使用的协议包括 AH、ESP 协议；数据加密所使用的加密算法包括 DES、3DES、AES、AES192、AES256、SANGFOR_DES；选择数据认证的认证算法包含 MD5、SHA1、SHA2-256、SHA2-384、SHA2-512。
- [优先级]：设置本端地址和对端地址优先级用于标识路由优先级。

3. 配置完<基础配置>界面中的配置之后，进入到<IKE配置>界面，如下图所示。

[IKE 配置界面]各配置项说明：

- [IKE 版本]：选择 IKEv1 或者 IKEv2 版本需要对端保持一致。
- [连接模式]：包括主模式和野蛮模式两种类型。主模式适用于双方均为固定 IP 或者一方固定 IP 一方动态域名方式，并且不支持 NAT 穿透；野蛮模式适用于其中一方为拨号的情况，并且支持 NAT 穿透；根据客户实际需求场景选择主模式或者野蛮模式。
- [主动连接]：用于控制设备是否主动发起建立 VPN 的连接。
- [本端身份类型]：设置本端身份类型，保证对端可以识别到本端设备。该类型包括：IP 地址（IPV4_ADDR）、域名字符串（FQDN）、用户字符串（USER_FQDN）三种类型。
- [本端身份 ID]：按照本端身份类型所选择的类型进行配置。
- [对端身份类型]：设置对端身份类型，保证本端可以识别到对端设备。该类型包括：IP 地址（IPV4_ADDR）、域名字符串（FQDN）、用户字符串（USER_FQDN）三种类型。
- [对端身份 ID]：按照本端身份类型所选择的类型进行配置。

- [IKE SA 超时时间]：标准 IPSEC 协商的第一阶段存活时间，只支持按秒计时方式。
- [D-H 群]：设置 Diffie-Hellman 密钥交换的群类型，包括 1、2、5、14、15、16、17、18 八种，请与对端设备配置保持一致。
- [DPD]：IPSEC 使用 DPD（Dead Peer Detection）功能来检测对端 Peer 是否存活。
- [NAT-T]：NAT-T 在野蛮模式下才会有，主要作用是避免有一方设备处于 NAT 之后导致标准 IPSEC 协商失败，NAT 穿透启用后数据会封装成 UDP 格式传输，而不是 ESP 封装，这样也可以避免内网没有放通 ESP 的情况。
- [检测间隔]：设置 DPD、NAT-T 的检测间隔。
- [超时次数]：设置 PDP、NAT-T 的检测超时次数，多次检测超时后，设备会认为对端失效而断开连接。
- [阶段一安全提议]：选择阶段一协商时所使用的参数，包括所加密算法、认证算法；其中数据加密所使用的加密算法包括 DES、3DES、AES、AES192、AES256、SANGFOR_DES、SANGFOR_NULL；选择数据认证的认证算法包含 MD5、SHA1、SHA2-256、SHA2-384、SHA2-512。

4. 配置完<IKE>界面中的配置之后，进入到<IPSec配置>界面。

<IPSec 配置界面>各配置项说明：

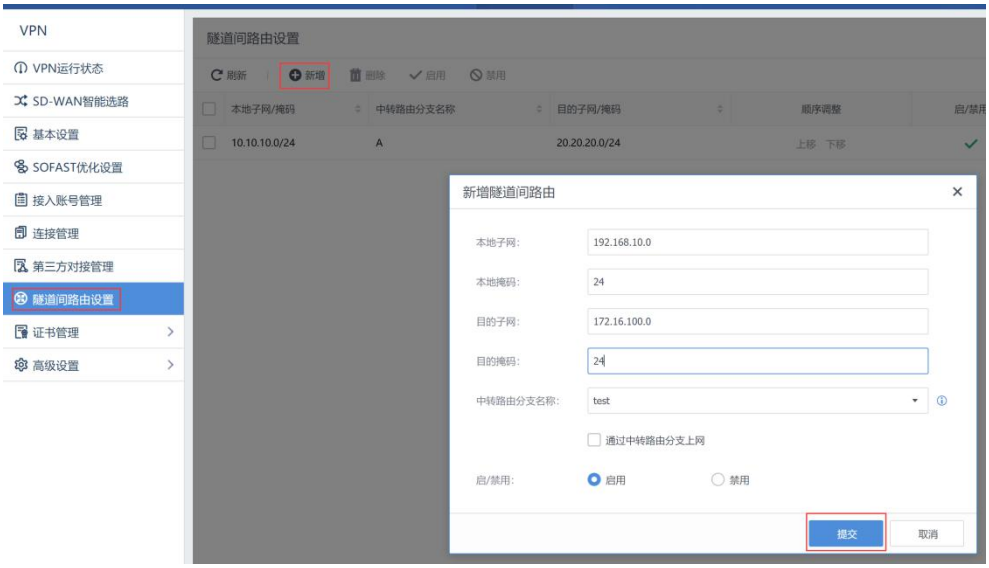
- [重试次数]：设置标准 IPSec VPN 的重试连接次数。
- [IPSec SA 超时时间]：设置 IPSec SA 对应的超时时间。
- [过期时间]：勾选启用或者禁用，来选择标准 IPSec VPN 隧道是否有过期时间。

5. 配置完成之后，点击<提交>即可保存配置。点击<编辑>可对VPN连接中的参数进行修改，点击<查看>显示加密数据流即可查看到对应的加密数据流的匹配规则。

3.3.8. 隧道间路由设置

SDW-R系列设备提供了强大的VPN隧道间路由功能，通过设置隧道间路由，可轻松实现多个VPN（软/硬件）之间的互联，真正实现“网状”VPN网络。

点击<新增>，可以添加一条隧道间路由，如下图。



各配置项目说明：

- [本地子网]：用来设置隧道间路由的源 IP 网络。
- [本地掩码]：用来设置隧道间路由的源子网网段的掩码。
- [目的子网]：用来设置隧道间路由的目的 IP 网络。
- [目的掩码]：用来设置隧道间路由的目的子网网段的掩码。
- [中转路由分支名称]：用来选择隧道间路由条目的 VPN 隧道（例如，A 跟 B 之间建立了 VPN 连接，使用的是用户“A”，现在 A 想通过 B 访问到 C，则对 A 设备而言，VPN 隧道为用户“A”）。
- 点击<启用>，则启用该隧道间路由条目，点击<提交>完成配置。

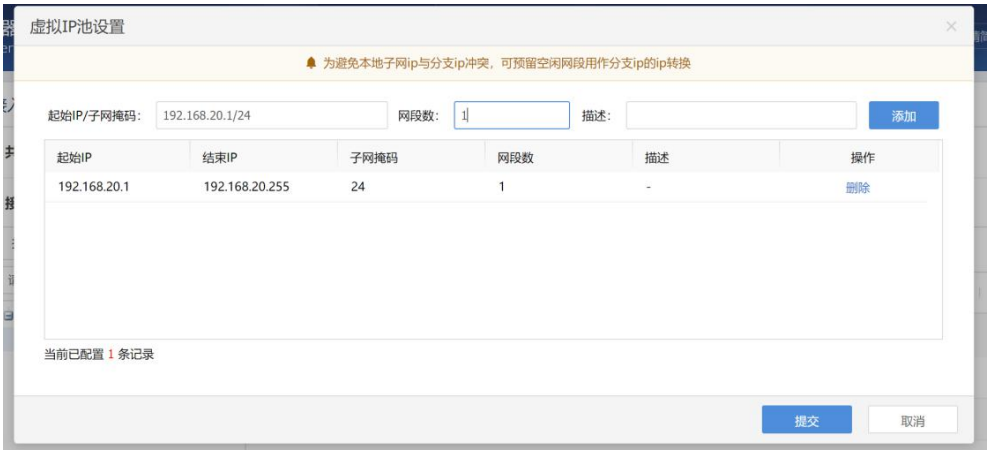
其他注意事项：

1. 启用通过中转路由分支上网功能时，VPN远程接入端设备必须部署为网关模式，本端设备网关、单臂部署均可。
2. 新建隧道间路由之前，需先确认在该VPN设备的[接入账号管理]中已经建好了用户或者[连接管理]中配置了连接管理，否则将无法创建隧道间路由。

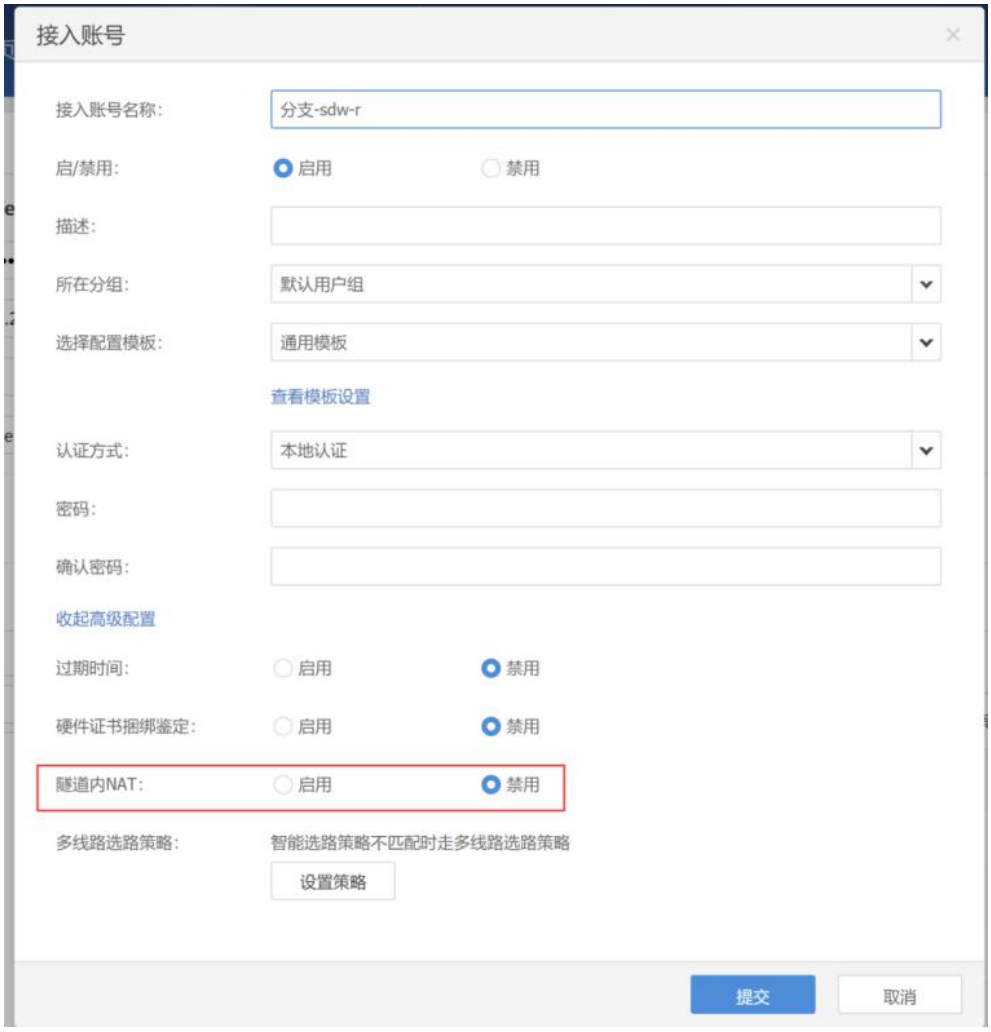
3. 其中中转路由分支名称是指：用户管理中未启用多用户登录选项的用户以及连接管理中配置了的用户（不包括二者重名或已禁用的用户）。

3.3.9. 隧道内 NAT

1. [隧道内NAT]主要用来解决分支之间内网网段冲突问题，通过在总部设备的[VPN/接入账号管理/虚拟IP池设置]的配置，如下图。



2. 在新增加入账号中可以看到是否启用隧道内NAT的功能，如下图。

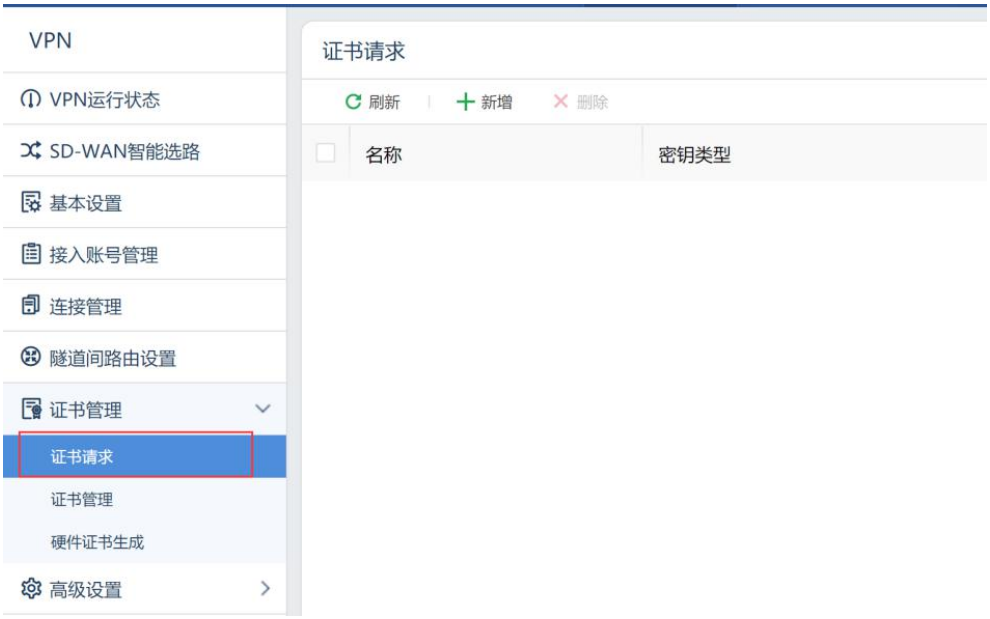


- 点击<启用>后，选择配置相应的原 IP 网段，系统就自动分支虚拟 IP 池给该网段，若虚拟 IP 池分配空了，可以到[VPN/接入账号管理/虚拟 IP 池设置]进行添加。

- 配置完成后，点击<提交>即可完成配置。

3.3.10. 证书管理

[证书管理]包含[证书请求]、[证书管理]和[生成硬件证书]，用来生成和导入RSA签名证书，配置如下图。



3.3.10.1. 证书请求

点击<新增请求证书>，如下图所示。

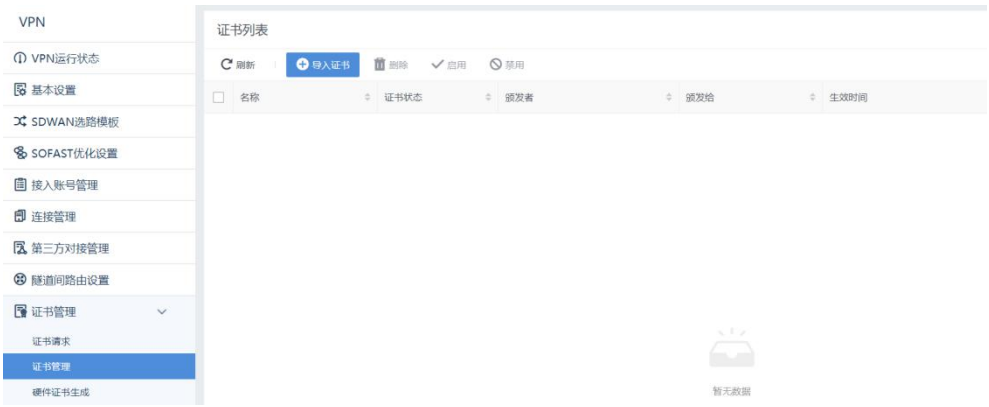
各配置项说明：

- [名称]和[主题]以及[拓展识别信息]模块的信息，根据实际情况来进行填写。
- [密码标准]：可以选国际商用密钥标准（RSA）。
- [RSA 密码长度]：可选 1024，2048，4096。
- [摘要算法]：可选 sha1，sha2。

新增申请后，会生成证书申请文件和密钥文件，点击<下载>可将申请文件下载下来。只支持离线证书申请，如下图。

3. 3. 10. 2. 证书管理

1. [证书管理]可以看到证书管理页面，显示如下图。



2. 点击<导入证书>，将离线申请的证书导入证书管理列表，显示如下图。

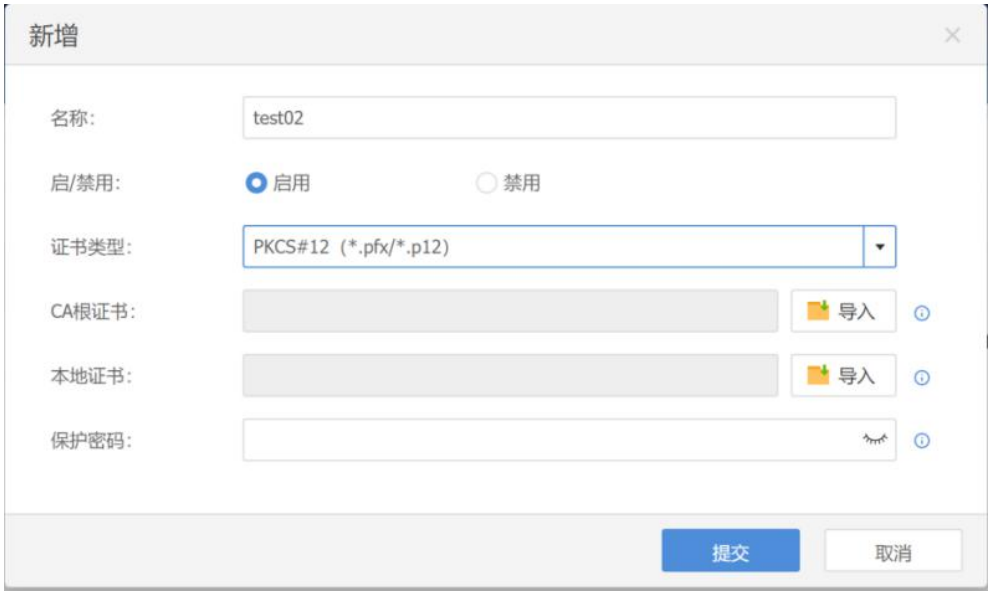
各配置项说明：

- [名称]：可根据实际情况自定义证书名称。
- [启/禁用]：可以启用或禁用该证书。
- [证书类型]：可选择：CER 本地证书（*.cer/*.crt）、CER 根证书（*.cer/*.crt）、PKCS#12 证书（*.pfx/.p12）、PKCS#7 证书（*.p7b）。

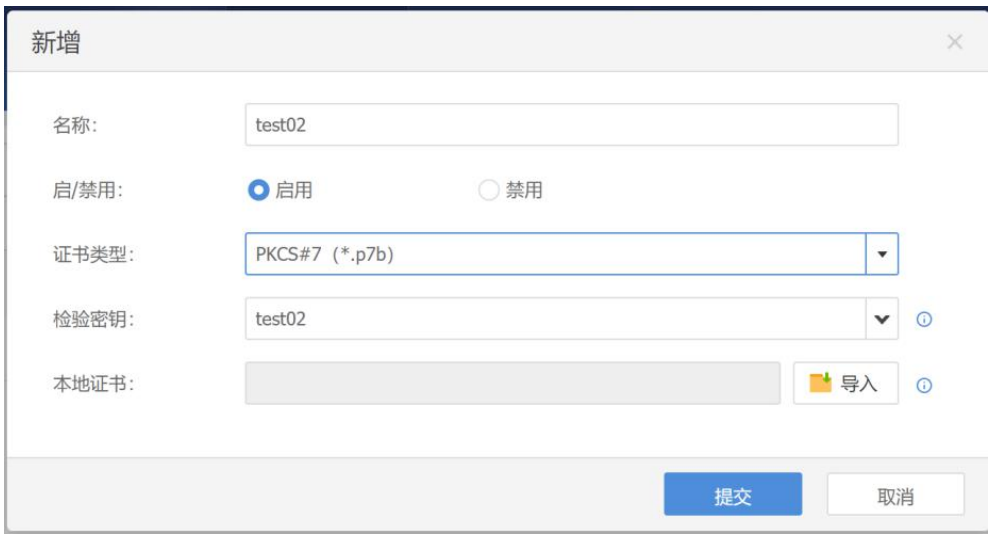
- 选择[证书类型]为 CER 本地证书导入时，校验密钥来自于申请信息列表，即选择即将导入的证书对应的申请信息。显示如下。

- 选择[证书类型]为 CER 根证书导入，显示如下。

- 选择[证书类型]为 PKCS#12 证书导入。保护密码为该证书导出/生成时的填写的保护密码，当根证书和保护密码正确时，证书才能导入成功。显示如下。



- 选择[证书类型]PKCS#7 证书导入。校验密钥来自于申请信息列表，即选择即将导入的证书对应的申请信息。如下图所示。



- 证书导入完毕后，可以在证书列表中看到证书信息，可以进行编辑和下载。如下图所示。

- 点击<编辑>，可查看证书详情，显示如下。

说明：

当该证书是根证书时，支持下载 CA 根证。当该证书是非根证时，支持下载 CA 根证或下载 PRCS#12 证书（*.pxf/*.p12）格式证书。

3.3.10.3. 生成硬件证书

基于硬件特性的证书认证系统是深信服公司的发明专利之一。SDW-R硬件设备也采用了该技术用于不同VPN节点之间的身份认证。该证书提取了SDW-R设备部分硬件特征生成加密的认证证书。由于硬件特性的唯一性，使得该证书也是唯一的、不可伪造的。通过对该硬件特性的验证，就保障了只有指定的硬件设备才能被授权接入网络，避免了安全隐患。

1. 点击<生成证书选择保存路径>即可生成硬件证书并保存到本地计算机上，页面如下图。

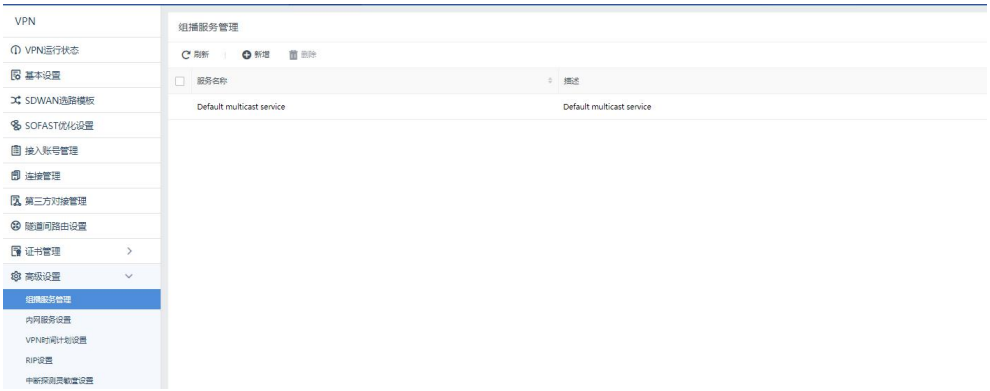
2. 将生成好的证书发给总部管理员，由总部管理员在新建VPN用户账号的时候选择硬件鉴权，将用户和对应的硬件证书进行绑定即可。

3.3.11. 高级设置

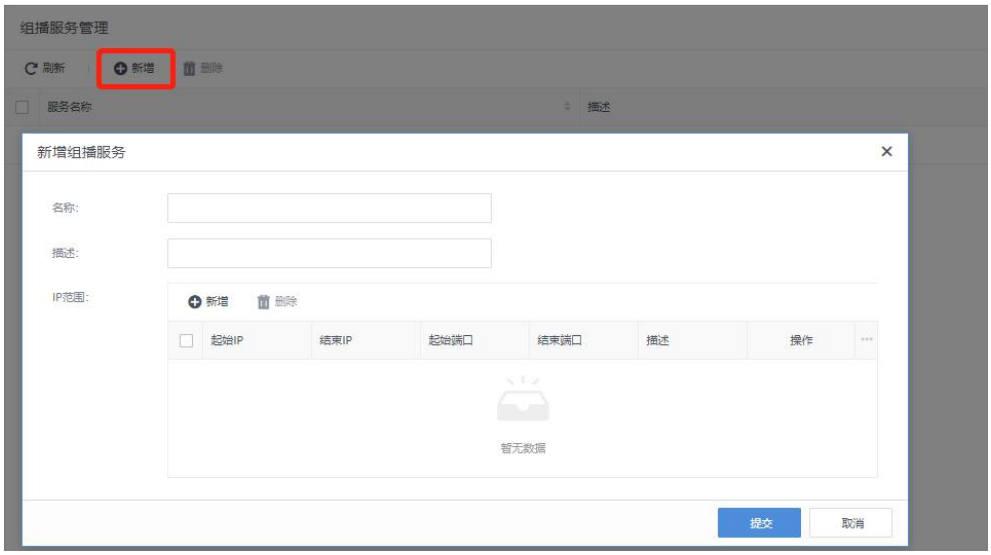
登录管理页面，点击[VPN/高级设置]，高级设置中包括[组播服务管理]、[内网服务管理]、[VPN时间计划设置]、[RIP设置]相应的界面如下。

3.3.11.1. 组播服务管理

为满足VOIP和视频会议等应用，SDW-R设备支持组播服务在隧道间传输。在这里可以定义组播的服务，ip范围是224.0.0.1-239.255.255.255，端口范围是1-65535。页面如下。



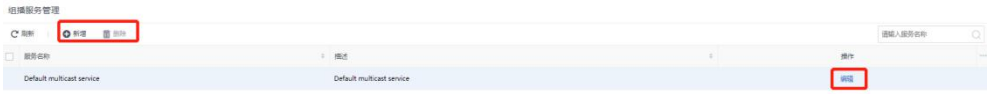
1. 点击<新增>出现组播服务编辑页面，在这里可以设置组播服务所用的组播地址和端口，页面如下。



2. 定义[名称]和[描述]，点击<新增>，可以设置组播服务所用的组播地址和端口。

3. 定义好组播服务后，在[VPN/入账号管理]上新增用户，然后在[选择配置模板/添加]新增配置模板中启用组播服务功能，然后在关联相应的组播服务，页面如下。

4. 对于组播服务器，管理员可以进行新增、编辑、删除等操作，如下图所示。



3. 3. 11. 2. 内网服务管理

SANGFOR系列硬件设备可以为接入的VPN用户指定相应的访问权限，可以限制分支用户内网的某个IP、某个分支用户只能访问内网的特定计算机和特定服务参数；其次

SDWAN智能选路策略也可以根据内网服务中五元组的定义来识别相应的应用，从而为SDWAN智能选路做应用识别。

操作场景

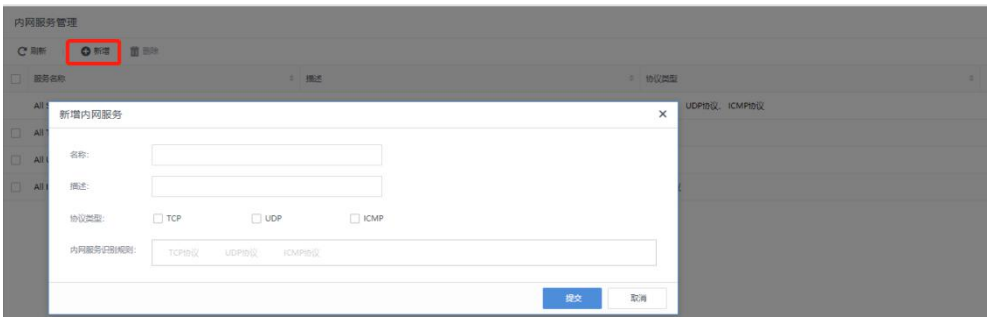
仅允许用户test访问总部的WEB服务器的WEB服务，对WEB服务器其它服务的访问请求都将被拒绝；分支内网其它IP的访问请求将被拒绝；SDWAN智能选路策略需要识别到某WEB服务器的WEB服务的五元组信息等等。

操作步骤

配置思路：

通过适当的内网服务设置，对服务进行访问授权和应用识别可以实现VPN隧道内的安全管理，也可以实现SDWAN智能选路中根据不同的应用做对应的选路策略。页面如下。

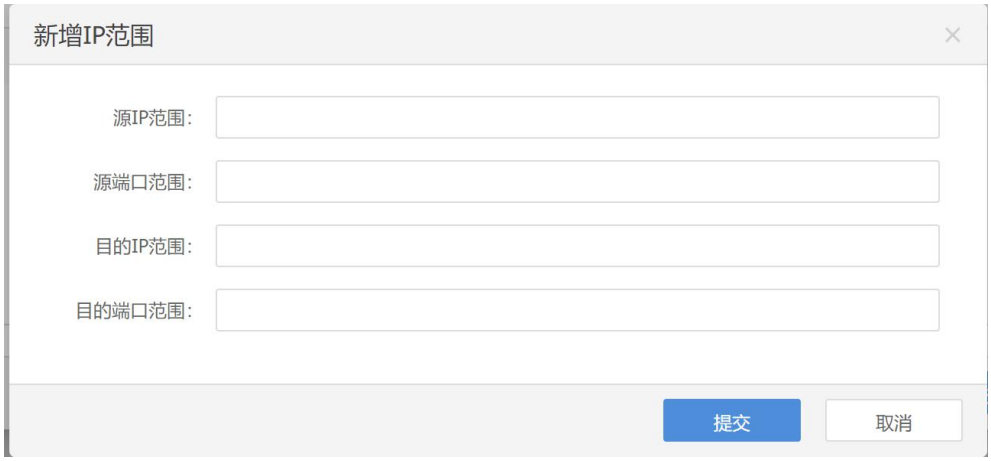
1. 在[VPN/高级设置/内网服务设置]页面下，点击<新增>，可以根据协议类型手动添加内网服务，如下图。



各配置项说明：

- [名称]和[描述]可自定义，方便管理即可。
- [协议类型]：选择定义的内网服务所使用的协议。

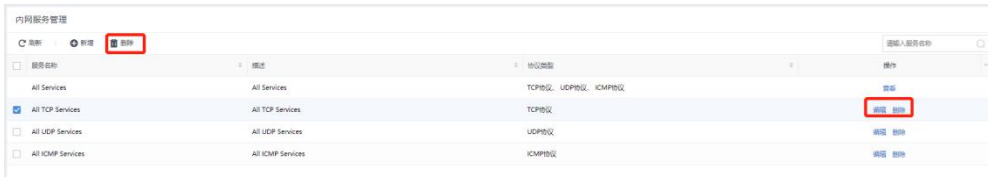
2. 选择[TCP]或[UDP]，还可以设置源IP范围、源端口范围、目标IP范围、目标端口范围等，点击<新增>，如下图。



3. 选择[ICMP]，可以设置源IP范围和目标IP范围，如下图。

4. 所有配置完成后，点击<提交>保存配置。

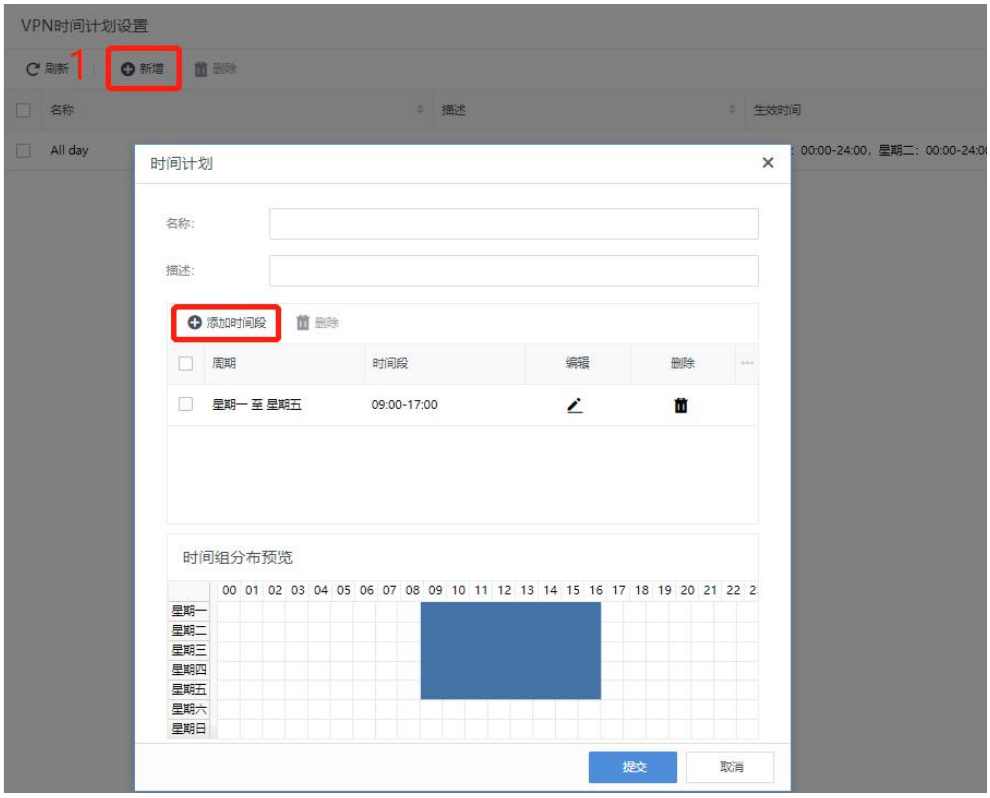
5. 对于新增的内网服务，管理员可以进行编辑、删除的操作，如下图所示。



3.3.11.3. VPN 时间计划设置

用于定义常用的时间段组合，这些时间组合可以在[VPN/接入账号管理/配置模板]模块中使用，以设置VPN内网服务的生/失效时间，该时间以设备上当前系统时间为准，页面如下图。

1. 在[VPN/高级设置/VPN时间计划设置]页面下，点击<新增>，出现时间计划配置页面，页面如下。

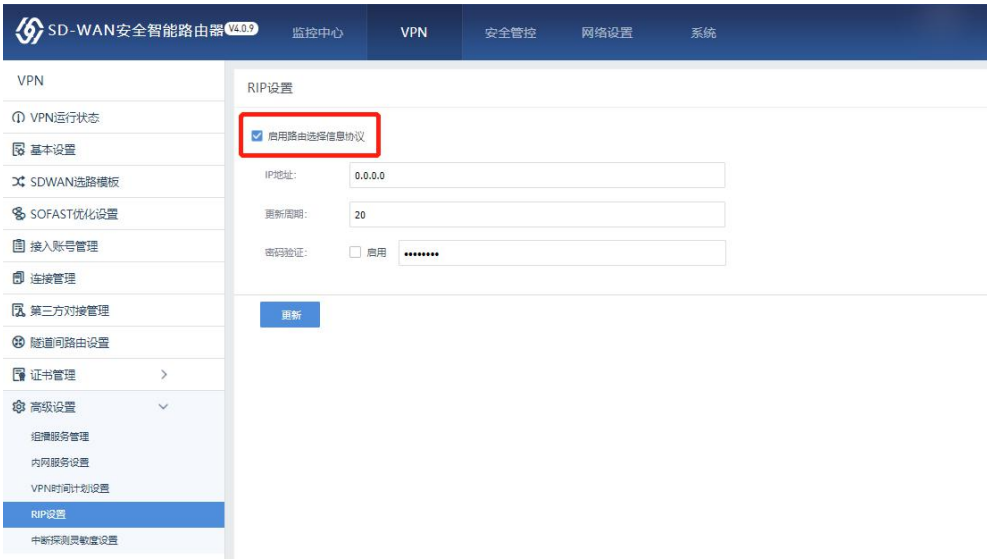


2. 定义一个名称为“test”的时间段，选取相应的时间段组合，宝蓝色为生效时段，白色为失效时段。点提交完成时间组的定义。

3. 定义完成时间段之后，对[VPN/接入账号管理/配置模板]中进行时间限定，如下图。

3.3.11.4. RIP 设置

[RIP设置]用于设置SDW-R设备通过RIP协议向其它路由设备通告路由信息，以实现内网路由设备RIP路由信息的动态更新，如下图。



各配置项说明：

- [启用路由选择信息协议]：整个 RIP 动态路由更新功能的开关，激活后，SDW-R 设备会向所设置的内网路由设备通告已与本端建立 VPN 连接的对端网络的信息（更新其他设备的路由表，添加到 VPN 对端的路由指向 SDW-R，VPN 连接断开后会通告路由设备删除该路由）。
- [IP 地址]：用于设置主动向哪个 IP（路由设备 IP）发布路由更新信息。
- [更新周期]：SDW-R 在路由信息有变化时会触发路由更新信息过程，这时下面设置的 RIP 更新周期参数失效。
- [启用密码验证]：用于设置交换 RIP 协议信息时需要验证的密码，可视具体情况进行设置。

3.3.11.5. 中断探测灵敏度设置

使用VPN业务时，如对线路切换速度要求非常高，可选择开启高灵敏度模式。

开启此模式后，线路中断切换速度最快可达200ms，未开启时预计在1s。

由于中断探测灵敏度高，当网络情况不稳定导致线路上200ms内没收到回包时，会被判断为线路中断，请谨慎操作。

在[VPN/高级设置/中断探测灵敏度设置]页面下，点击开启即可，如下图所示。

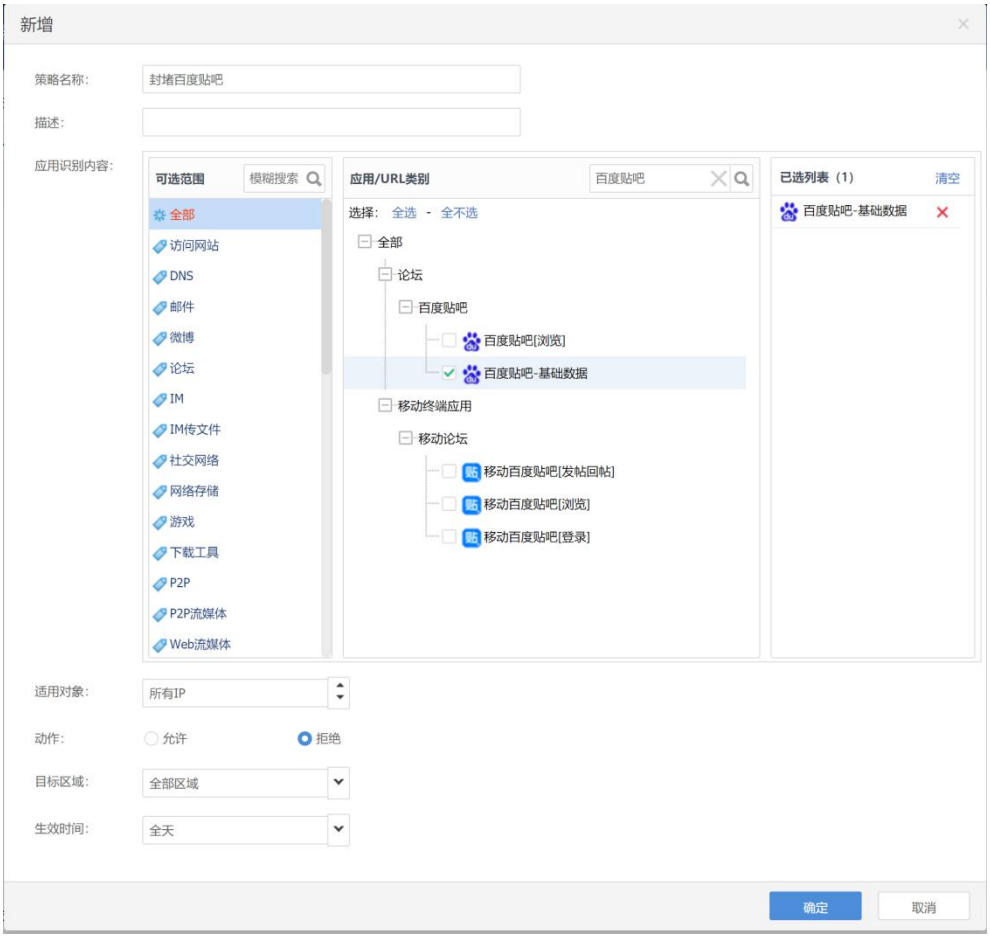
3.4. 安全管控

安全管控包括[访问控制策略]、[流量管理]、[防火墙]、[防DOS攻击]、[对象设置]模块。

3.4.1. 应用控制策略

3.4.1.1. 封堵应用和查看策略故障日志

1. 通过在[安全管控]页面的访问控制里，配置上网策略，对特定的或者所有的应用进行封堵。策略配置拒绝之后，用户即无法访问对应的应用。此处新增封堵策略，引用的应用是内置应用库中指定的应用。

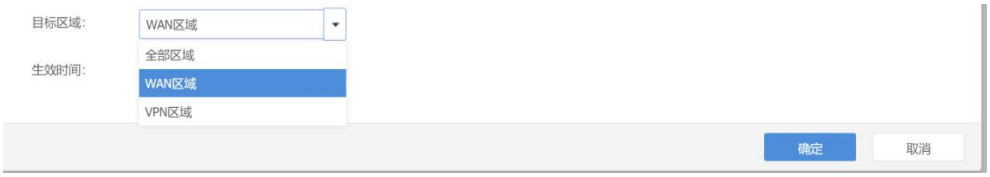


相关配置项说明：

[适用对象]：可选择相应的IP组或者MAC组，如下图所示。

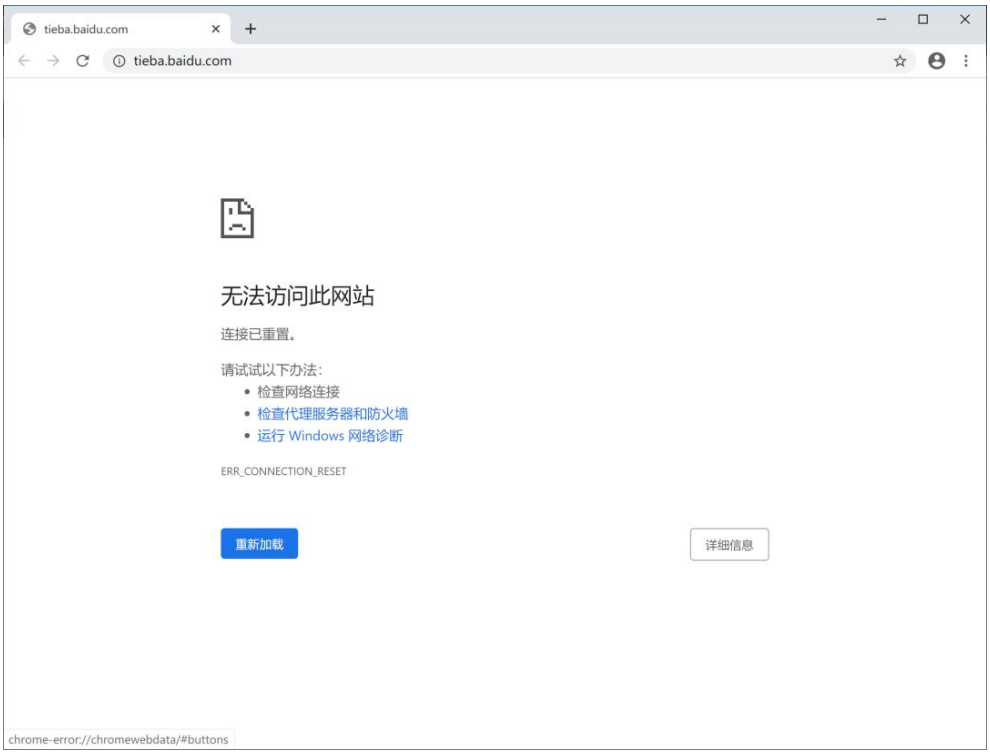
[动作]：选择策略匹配之后的动作是允许通过，还是拒绝通过。

[目标区域]：选择策略生效的目标区域为WAN区域还是VPN区域。

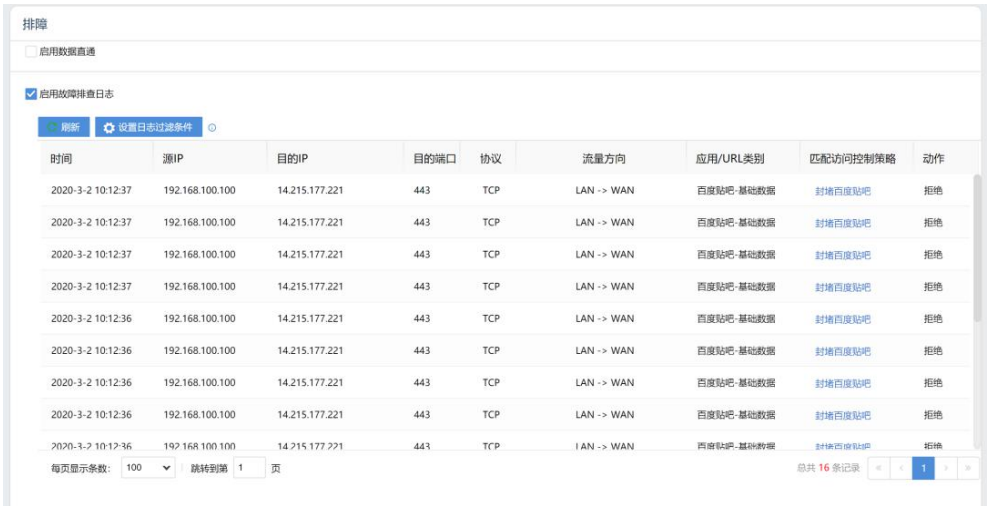


[生效时间]：选择策略生效的时间。

2. 配置完成封堵策略之后访问该应用，可以查看相应的访问动作无法执行。



3. 通过[系统/排障]查看策略故障日志时，可看到对应的拒绝信息。

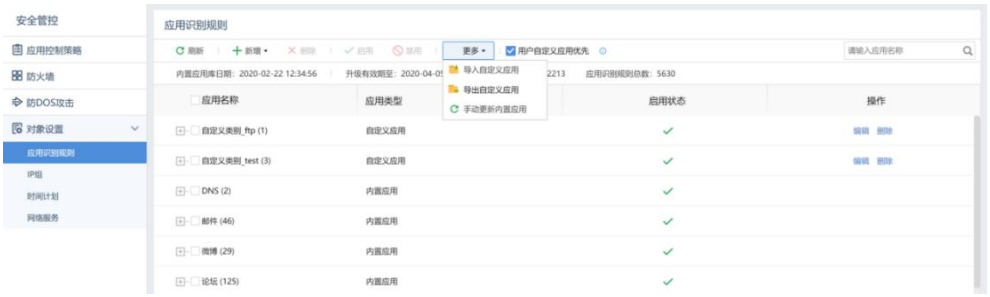


4. 通过日志记录可以发现流量被封堵了，想要放通的话就可以改变策略的动作为允

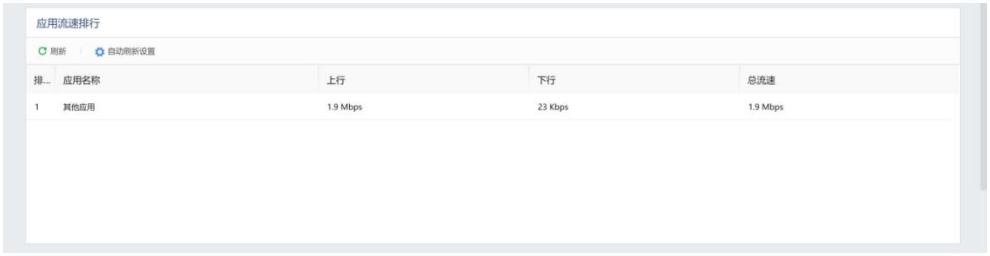
许，或者启用数据直通功能。

3.4.1.2. 应用的导入/导出和启/禁用

1. 为了更灵活的新增自定义应用，SDW-R还支持导入和导出自定义应用，可以将其它的SDW-R设备或者是BBC的自定义应用导入到自身设备里，或者将自身设备的自定义应用配置导入到别的SDW-R设备里，简化另一端的配置，前提是另一端的SDW-R版本一致。



2. 应用还支持启用/禁用，可以通过此方式选择被策略拒绝封堵。在上面的过程中，将自定义TCP:12000端口的流量（应用）给封堵掉。那么此时禁用这个应用，策略test就相当于没引用内容，封堵会失效。此时再次访问该应用时，查看PC2的接收情况和识别结果。发现PC2是可以接收到数据的，识别结果成为了其他应用。



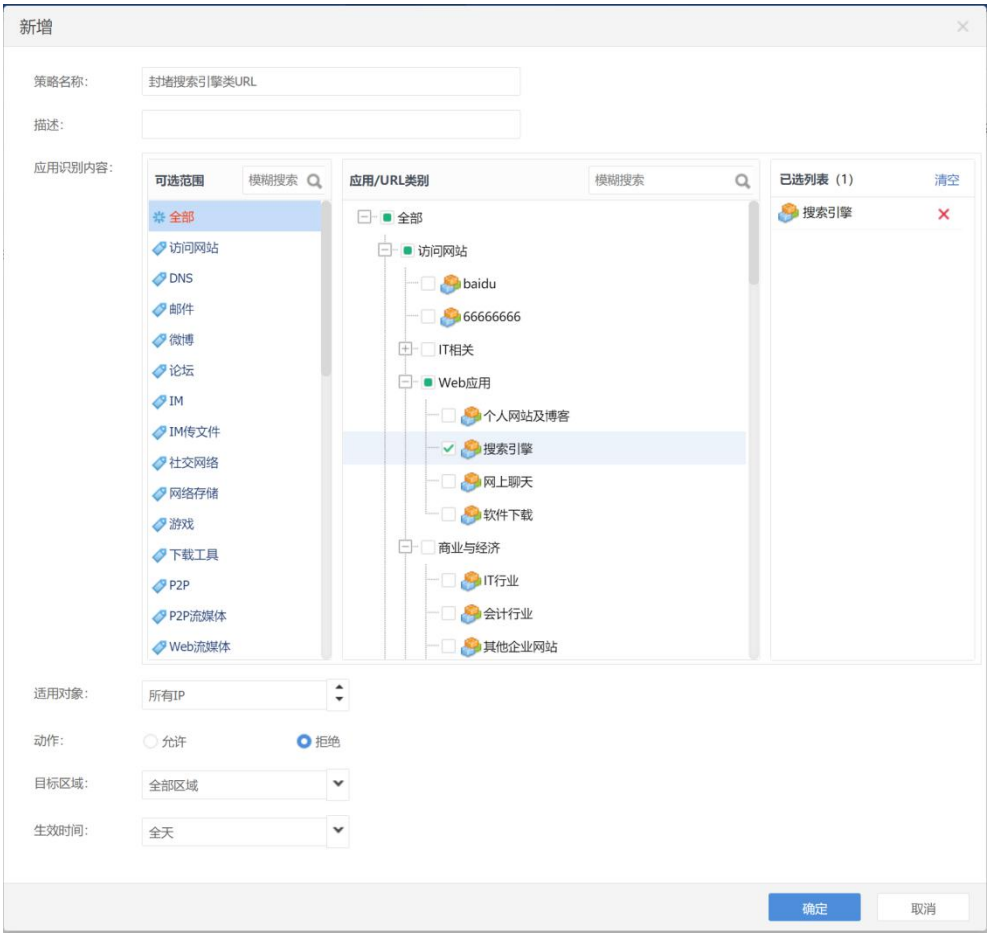
3. 此时如果再次启用引用的话，那么就依然是被封堵。

   有一些基础的协议是不允许被禁用的，如果禁用的话，可能上网功能就要受到影响了。比如说和一些ftp、pop3等协议。

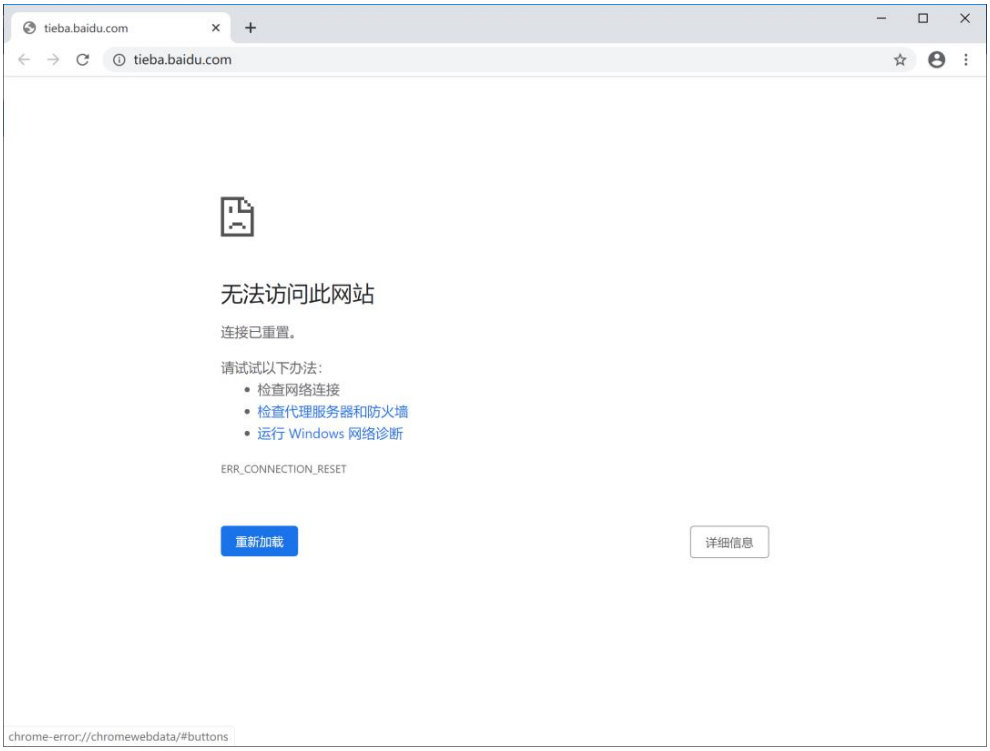
3.4.2. URL 控制策略

封堵URL和查看策略故障日志

1. 通过在[安全管控]页面的访问控制里，配置封堵URL策略，对特定的或者所有的URL进行封堵。策略配置拒绝之后，用户即无法访问对应的URL。此处新增封堵策略，引用的URL是通过与云端同步的云端URL类别。



2. 配置完成封堵策略之后访问该同类型的URL，可以查看相应的访问动作无法执行。



3.4.3. 流量管理

当开启流量管理，点击<高级设置>，可以启用线路繁忙保护，设置上下行繁忙阈值，可以更好的避免线路在流量高峰期时满载，以保证线路的可用性，并提高动态带宽保证的效果。

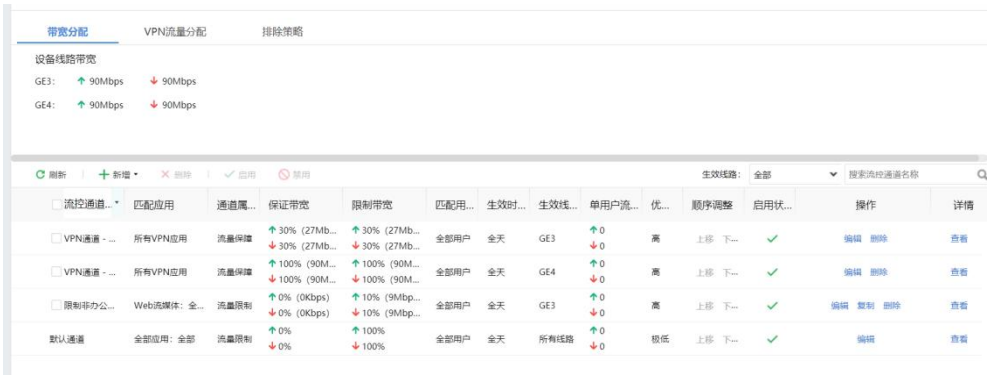
在实际线路使用过程，由于设备会尽可能的跑满线路带宽，为避免部分运营商可能存在带宽达不到标称值，链路满载后链路质量下降，业务体验不好的情况。建议在高级设置启用线路繁忙保护功能，保证流控保障策略的正常使用。

流量管理页面下，可以查看带宽分配、VPN流量分配、排除策略。

带宽分配

1. 总览

在带宽分配页面，可以查看设备线路带宽，在线路列表，可以查看流控通道、匹配应用、通道属性、限制带宽、生效时间、生效线路、优先级、启用状态等信息。

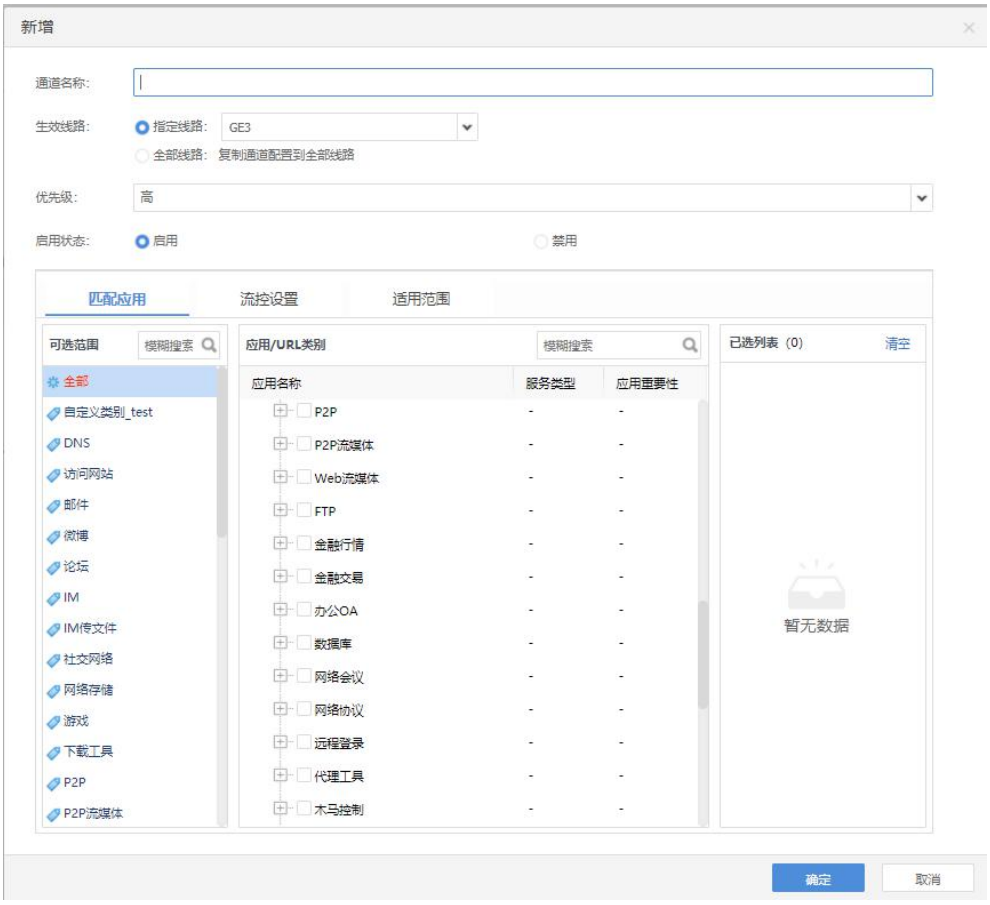


点击<详情>，跳转至“流量管理监控”页面，查看流量管理状态详情。

2. 在[安全管控/流量管理]页面下，点击<新增>，可以新增一级父级通道、新增子级通道、新增VPN通道三种类型。

以新增一级父级通道为例

- 点击<新增>，选择新增一级父级通道，页面如下，需配置通道名称、生效线路、优先级、启用状态、匹配应用详情、流控设置、适用范围等内容，配置完成后，点击<确认>即可。



匹配应用：指定需要匹配的应用，勾选即可。

流控设置：可配置通道的属性为流量保障、流量限制，当选择为流量保证时，可以设置上下行带宽，包含保证带宽和最大带宽；也可对单用户流量上限进行设置，如下图

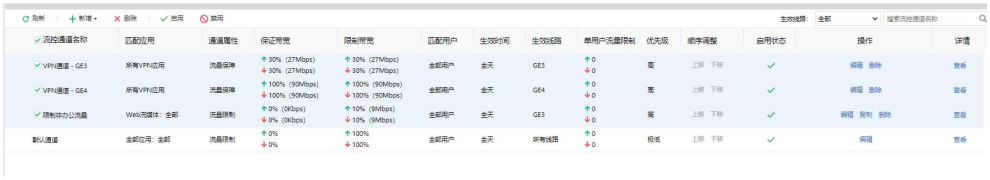
所示。

若通道属性为流量限制，需配置上下行最大带宽、支持单用户流量上限配置，如下图所示。

适用范围：可以配置适用用户以及时间计划，适用用户包含全部用户和指定用户，如下图所示。

- 配置完成后，点击<确定>即可。

3. 对新增配置的线路可以进行删除、启用、禁用等操作。对于默认通道，只能进行编辑和查看的操作。如下图所示。

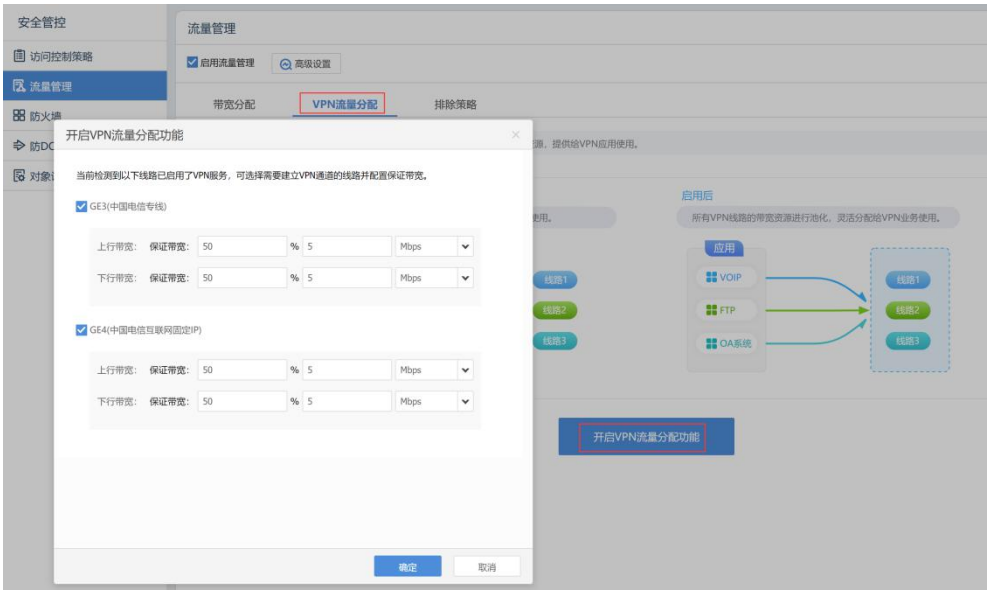


VPN流量分配

1. 总览

在VPN流量分配页面，可以查看VPN设备线路带宽，在线路列表，可以查看流控通道名称、匹配应用、通道属性、限制带宽、生效时间、优先级、启用状态等信息。

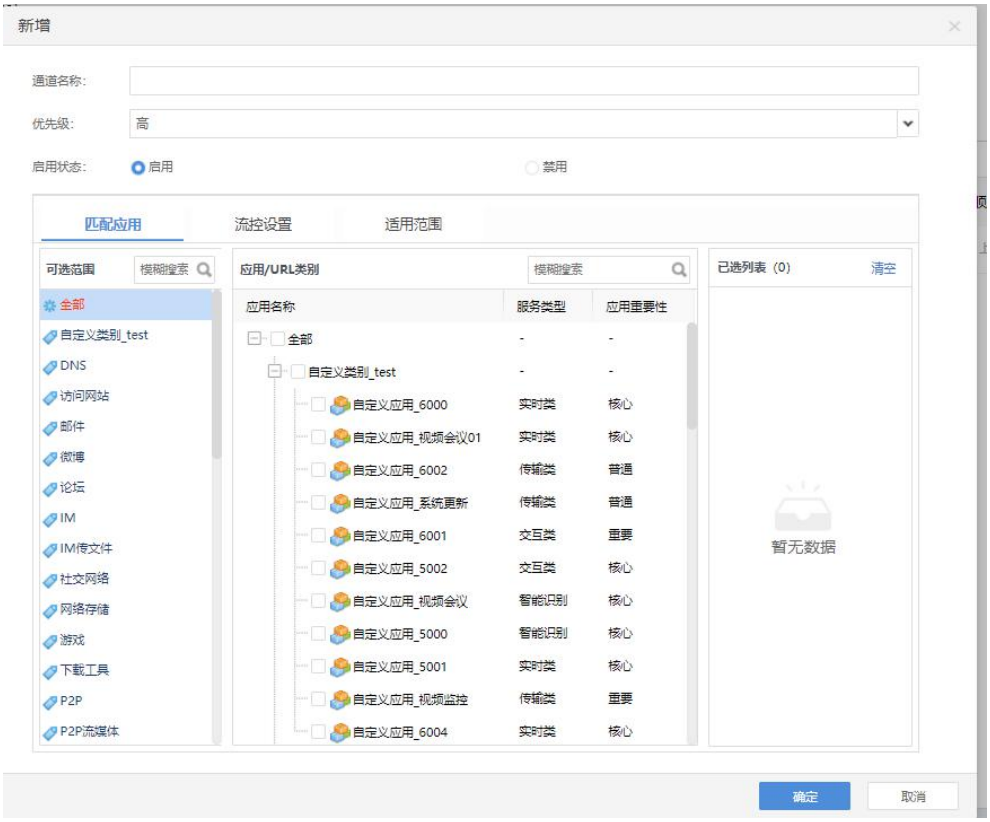
点击<VPN流量分配功能结束>，可以查看VPN流量详细的功能介绍，VPN流量分配功能可聚合VPN线路上的带宽资源，提供给VPN应用适用。启用后，所有的VPN线路的带宽资源进行池化，灵活分配给VPN业务使用。



2. 在[安全管控/流量管理]页面下，选择VPN流量分配页面，点击<新增>，可以新增一级父级通道、新增子级通道两种类型。

以新增一级父级通道为例

- 点击<新增>，选择新增一级父级通道，页面如下，需配置通道名称、生效线路、优先级、启用状态、匹配应用详情、流控设置、适用范围等内容，配置完成后，点击<确认>即可。



匹配应用：指定需要匹配的应用，勾选即可。

流控设置：可配置通道的属性为流量保障、流量限制，当选择为流量保证时，可以设置上下行带宽，包含保证带宽和最大带宽；也可对单用户流量上限进行设置，如下图所示。

若通道属性为流量限制，需配置上下行最大带宽、支持单用户流量上限配置，如下图所示。

适用范围：可以配置适用用户以及时间计划，适用用户包含全部用户和指定用户，如下图所示。

- 配置完成后，点击<确定>即可。

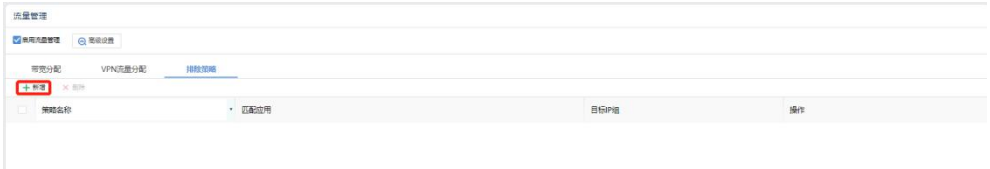
3. 对新增配置的线路可以进行删除、启用、禁用等操作。对于默认通道，只能进行编辑和查看的操作。如下图所示。

新增子级通道时，需先创建父级通道。

排除策略

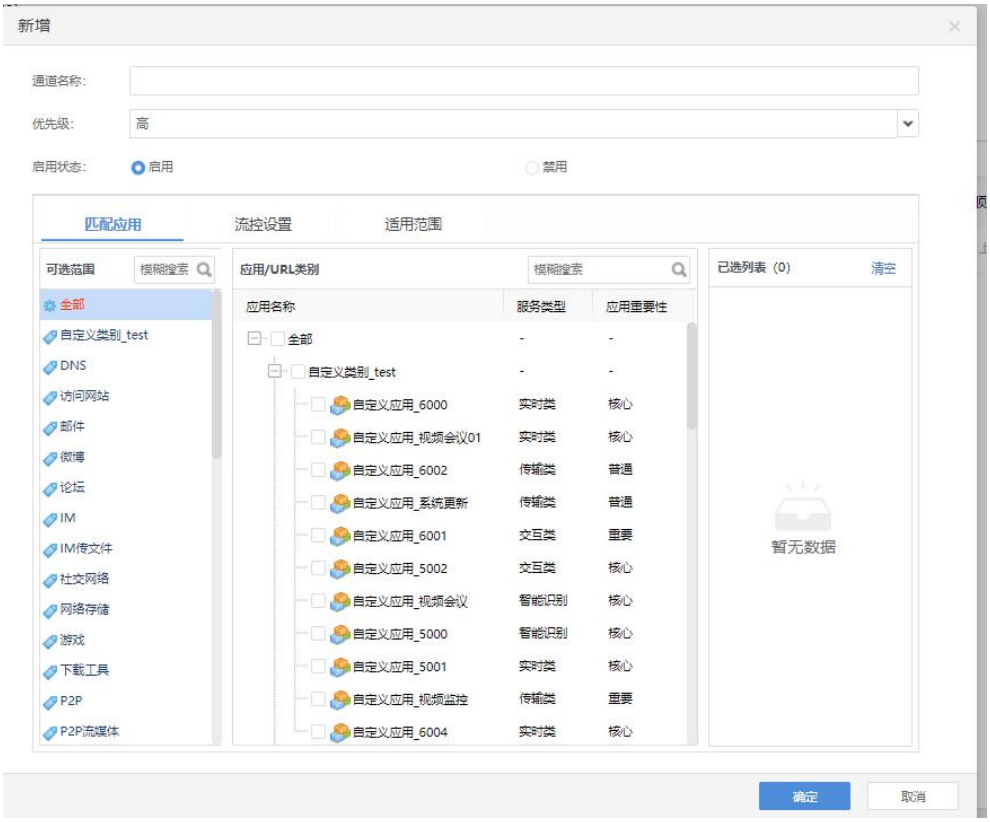
1. 总览

在排除策略页面，可以查看策略的名称、匹配的应用、目标IP组以及操作。

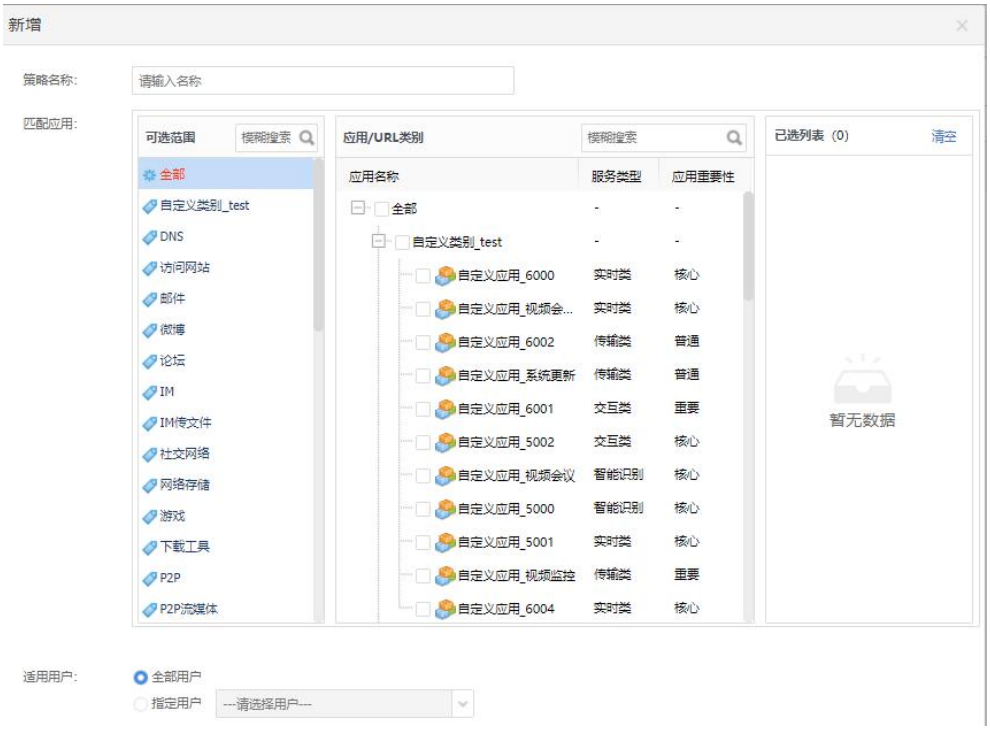


2. 在[安全管控/流量管理]页面下，选择排除策略页面，点击<新增>，可以新增策略。

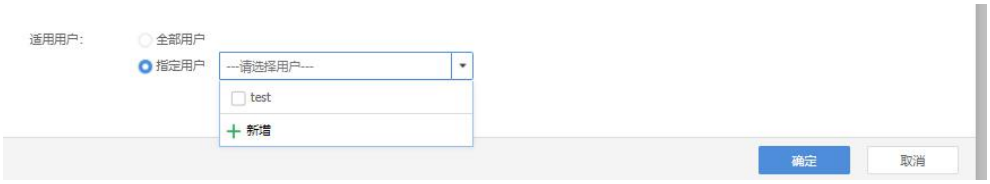
- 点击<新增>，页面如下，需配置策略称、匹配应用详情、适用范围等内容，配置完成后，点击<确认>即可。



匹配应用：指定需要匹配的应用，勾选即可。



适用范围：可以配置适用用户以及时间计划，适用用户包含全部用户和指定用户，如下图所示。



- 配置完成后，点击<确定>即可。

3. 对新增的策略可以进行删除等操作。

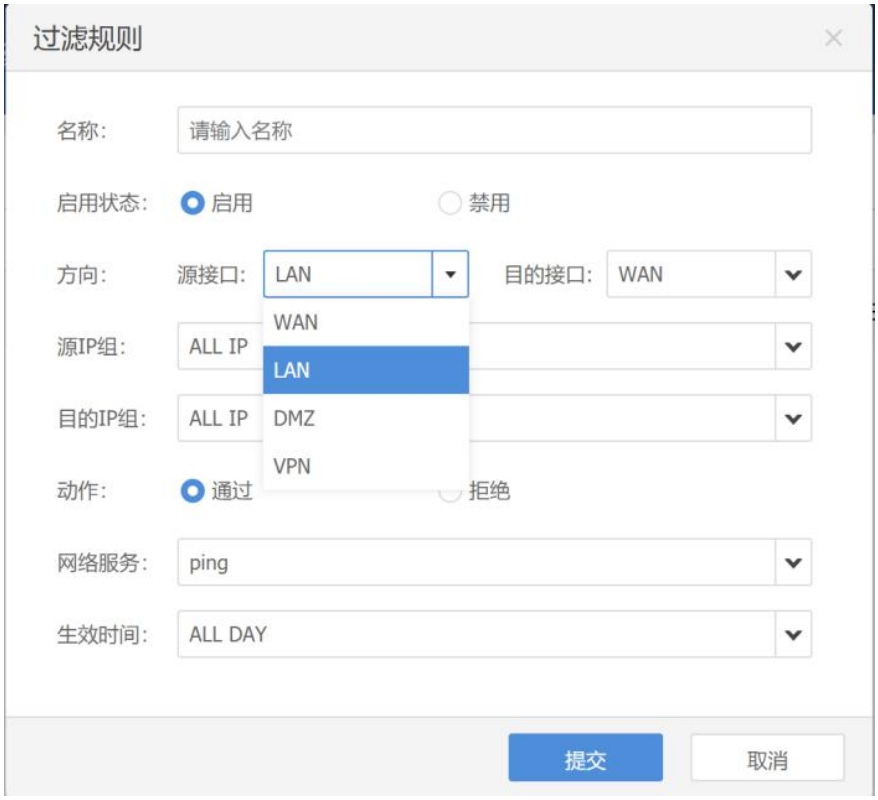
⚠ 注意：

1、VPN 池化流控与 SDWAN 智能选路（指定线路选路策略）结合使用时需要注意以下场景的问题：低优先级应用通过 VPN 流控设置了保障通道，同时低优先级应用配置指定线路选路策略，如果此时有高优先级应用也配置指定线路选路策略（与低优先级应用指定同一条线路），高优先级应用会抢占低优先级的应用带宽，会导致低优先级应用流控保障失效。

3.4.4. 防火墙

3.4.4.1. 新增过滤规则

SDW-R硬件网关防火墙采用状态检测包过滤技术，可在多个数据传输方向上结合时间计划实现基于协议类型、源IP、目的IP的数据包过滤。配置页面如下图。



各配置项说明：

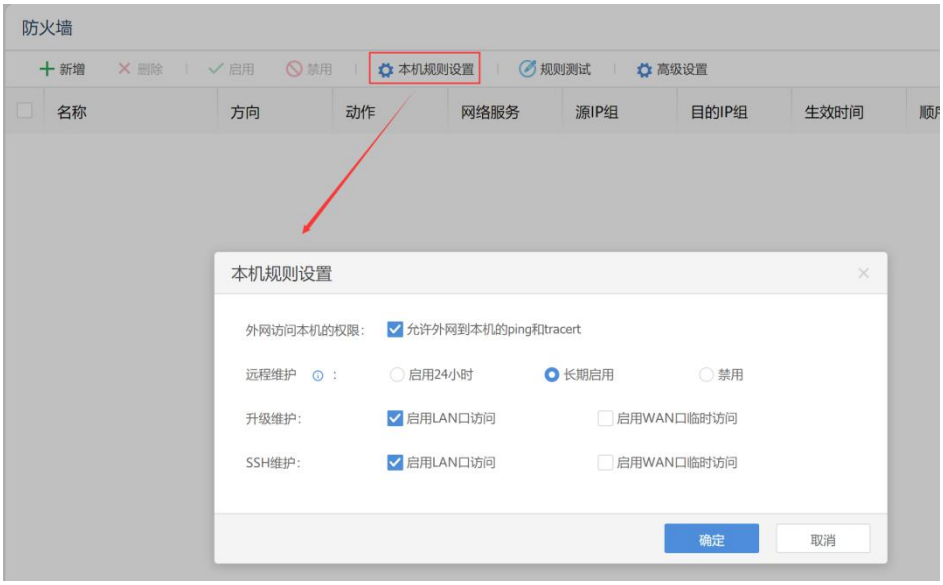
- [名称]：输入规则名称，用于标识。
- [方向]：源接口可选择 LAN、WAN、DMZ、VPN，目的接口可选择 WAN、DMZ、VPN，接口类型总共有 4 种、数据方向分为十二个方向的规则设置。
- [源 IP 组]：选择规则要匹配的源 IP 地址。
- [目的 IP 组]：选择规则要匹配的 IP 地址。
- [动作]：设置规则匹配后所需要执行的动作。
- [网络服务]：设置规则要匹配的服务类型。
- [生效时间]：设置规则生效的时间。

其他注意事项：

1. 所有的VPN数据都会经由VPN接口传输（例如：本端设备LAN接口下的计算机与VPN对端计算机的数据通信是经由设备LAN接口与VPN接口传输），因此可以通过防火墙的过滤规则对VPN数据进行控制。
2. [方向]选择VPN接口与WAN接口之间双向数据传输的防火墙过滤规则时，需关注如果VPN连接对端在[隧道间路由设置]中设置了以本端作为[中转路由分支名称]并启用[通过中转路由分支名称上网]，则在本端可通过设置VPN<->WAN的双向过滤规则实现对分支上网数据的控制）。

3.4.4.2. 本机规则设置

此页面用于设置外网用户通过公网IP配置、管理、维护等权限，页面如下。



各配置项说明：

- [外网访问本机的权限]：勾选允许外网到本机的 ping 和 tracert，允许外网用户直接 ping 设备的 wan 口，主要用于测试网络的联通性等。
- [启用远程维护]：用于厂商人员的维护，可选择启用 24 小时或者长期启用或者禁用。
- [升级维护]：用于厂商人员的维护，可设置内网或者外网通过升级客户端连接设备进行升级、调试等操作。
- [SSH 维护]：用于厂商人员的维护，可设置启用 LAN 口访问、WAN 口临时访问。

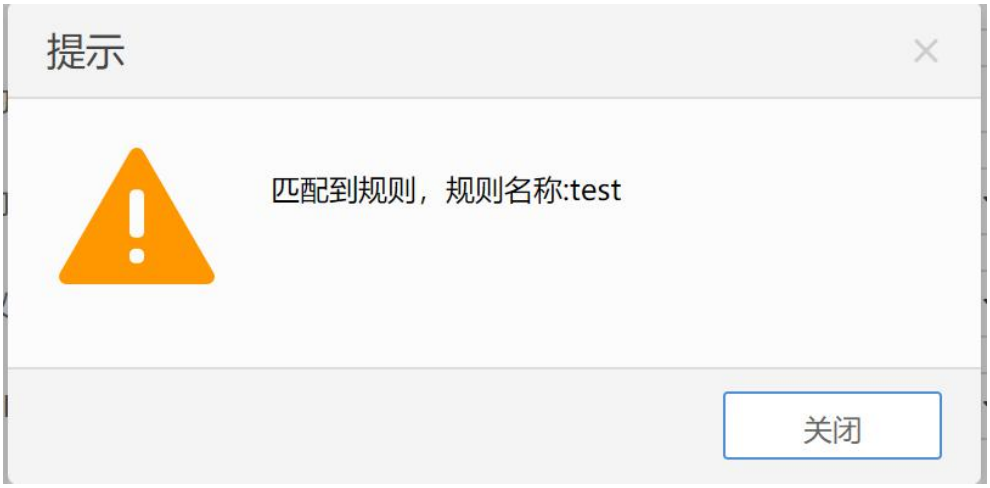
3.4.4.3. 规则测试

1. 可模拟生成数据包查看过滤规则匹配是否错误，可以降低由于规则配置错误导致的网络问题，具体配置如下图所示。

各配置说明：

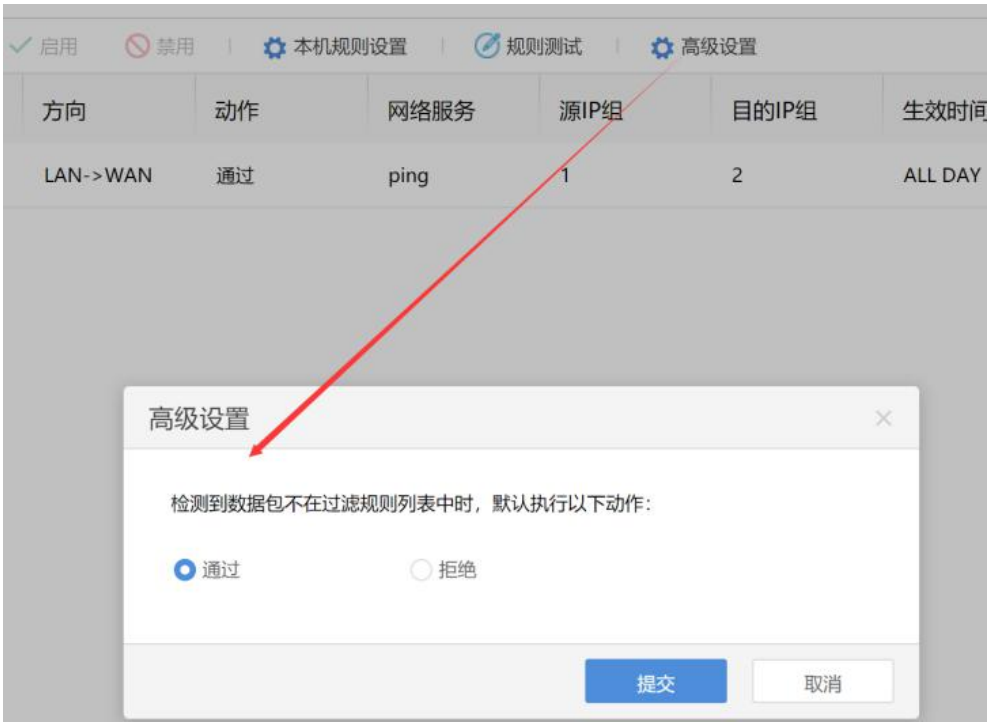
- [源 IP]：模拟数据包的源 IP 地址。
- [目的 IP]：模拟数据包的目的 IP 地址。
- [方向]：选择模拟数据包的方向。
- [协议]：可选择的协议为 TCP 或者 UDP 或者 ICMP。
- [目的端口]：填写相应的目的端口。
- [模拟数据包发出时间]：选择立刻发出或者自定义一个时间段。

2. 配置完成之后，点击<开始测试>，即开始匹配规则，匹配到规则后即可显示相应的规则名称。



3.4.4.4. 高级设置

选择检测到数据包不在过滤规则表中时，默认执行的动作，用于做防火墙的黑名单列表或者白名单列表，如下图。



3.4.4.5. 案例学习

某公司总部只允许接入总部的SDW-R分支（172.16.1.0/24）的其中一部分IP地址（172.16.1.100-172.16.1.200）访问总部内网服务器（192.168.10.20）的WEB服务，但禁用这一部分IP访问系统总部内网服务器的SQL SERVER服务。

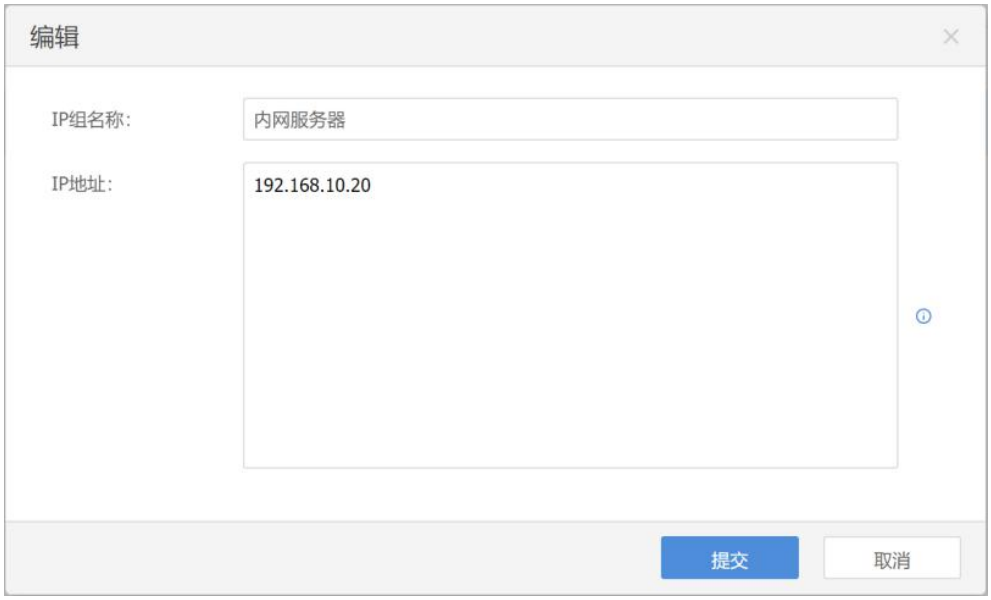
设置步骤如下：

1. 进行[IP组设置]，在[对象设置/IP组设置]中进行配置。SDW-R分支配置页面如下图。

各配置项说明：

- [IP 组名称]：给需要定义的 IP 或 IP 段进行命名，可自定义。
- [IP 组定义]：使用 IP 范围，填入分支允许访问的 IP 地址段：172.16.1.100-172.16.1.200 之后，点击<提交>，则完成“SDW-R 分支”IP 组的设置。

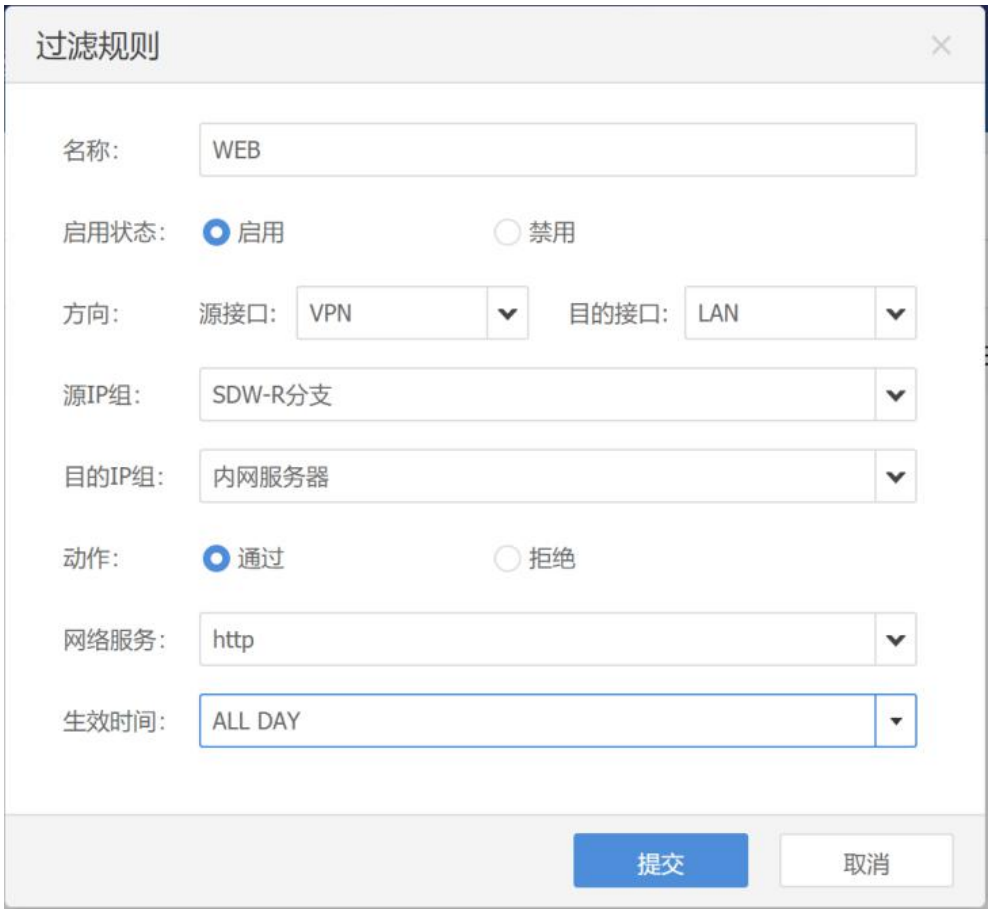
2. 内网服务器配置界面如下图。



各配置项说明：

- [IP 组名称]：给需要定义的 IP 或 IP 段进行命名，可自定义。
- [IP 组定义]：使用单个 IP 192.168.10.20，填入分支允许访问的 IP 地址段：172.16.1.100-172.16.1.200 之后，点击<提交>，则添加到[对象设置/IP 组设置]列表中。

3. 新建WEB服务过滤规则，通过[防火墙设置/过滤规则设置]进行配置，配置页面如下。



各配置项说明：

- [规则名称]：自定义规则名称。
- [规则方向]：设置为 VPN->LAN。
- [规则动作]：设置为对此类数据通过。
- [服务对象]：设置为 http。
- [源 IP 组]：选择设置好的 IP 组“SDW-R 分支”。
- [目的 IP 组]：选择设置好的 IP 组“内网服务器”。
- [时间组]：设置规则生效的时间。

4. 选择启用状态选项，点击<提交>完成配置。

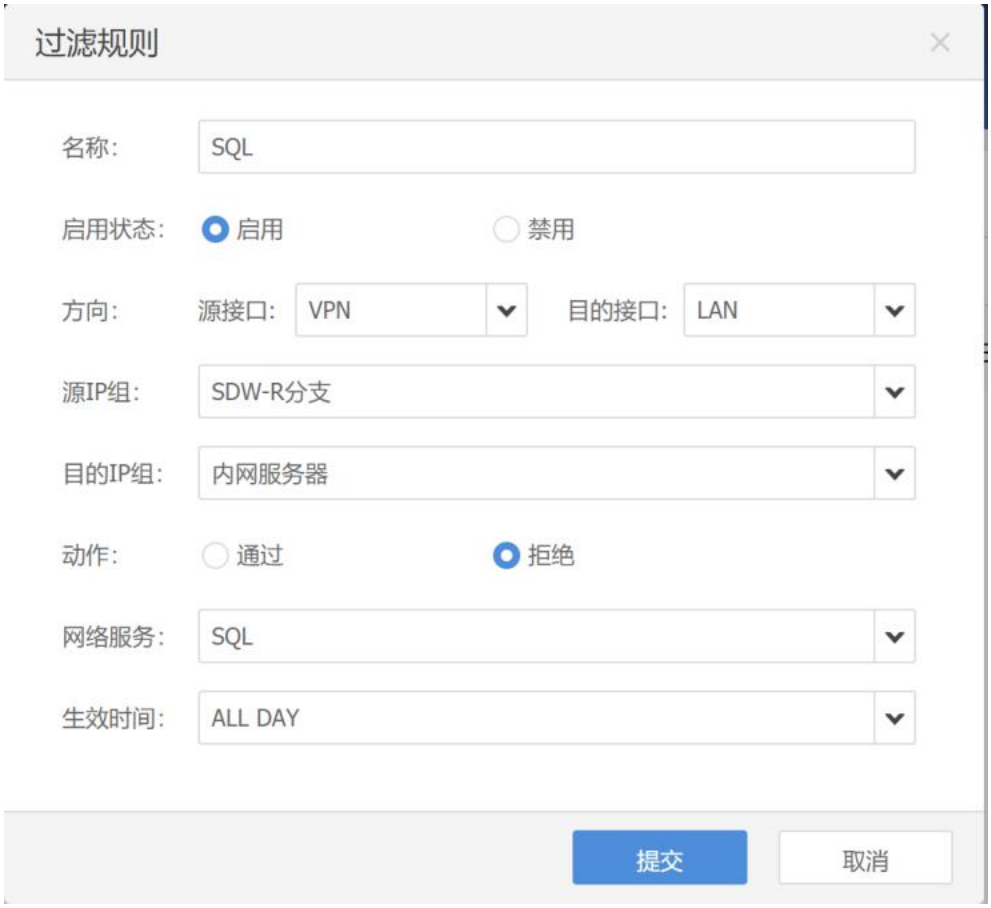
5. 接下来设置SQL SERVER服务过滤规则，首先进行服务定义，页面如下图。

各配置项说明：

- [服务名称]：可自定义（本例中可设置为 SQL）。
- [服务信息]：选择 TCP。
- [端口号]：填写 1433。

6. 点击<提交>，将该服务添加到[对象设置/网络服务设置]列表中。

7. 设置SQL SERVER服务过滤规则，页面如下图。



与WEB服务过滤相似，区别在于案例中对于SQL的服务是拒绝的，因此在[动作]处选择拒绝。

📖 说明：

其他如限制总部访问分支服务、限制分支通过总部上网的数据等需求都可以通过在相应接口之间设置过滤规则实现。

3.4.5. 防 DOS 攻击

防火墙功能模块不仅肩负着阻隔Internet上的用户对局域网非法攻击的任务，很多时候由于局域网内有电脑中毒，会向网关发送大量的数据包，这样有可能会造成带宽阻塞或者网关死机。SDW-R系列硬件设备内部集成了[防DOS攻击]功能，可以监测单位时间内某个IP向网关发送了多少数据量，当超过一定值时则SDW-R系列硬件设备会认为受到此IP的DOS攻击，并会阻断此IP一段时间从而保护自己，页面如下。

选择启用防DOS攻击后，可根据情况对相应阈值进行设置，包括[每个IP地址在一分钟内可发起的最大TCP连接数]、[每台主机在一秒钟内可发送的最大SYN包次数]、[检测到攻击后对攻击主机的封锁时间]。

[同时检测来自内网网段的IP地址（未勾选时，仅检测内网网段外的IP地址）]：勾选该选项时，表示检测外部网段IP地址的同时也检测内部网段的IP地址，防止来自内网DOS攻击。

3.4.6. 对象设置

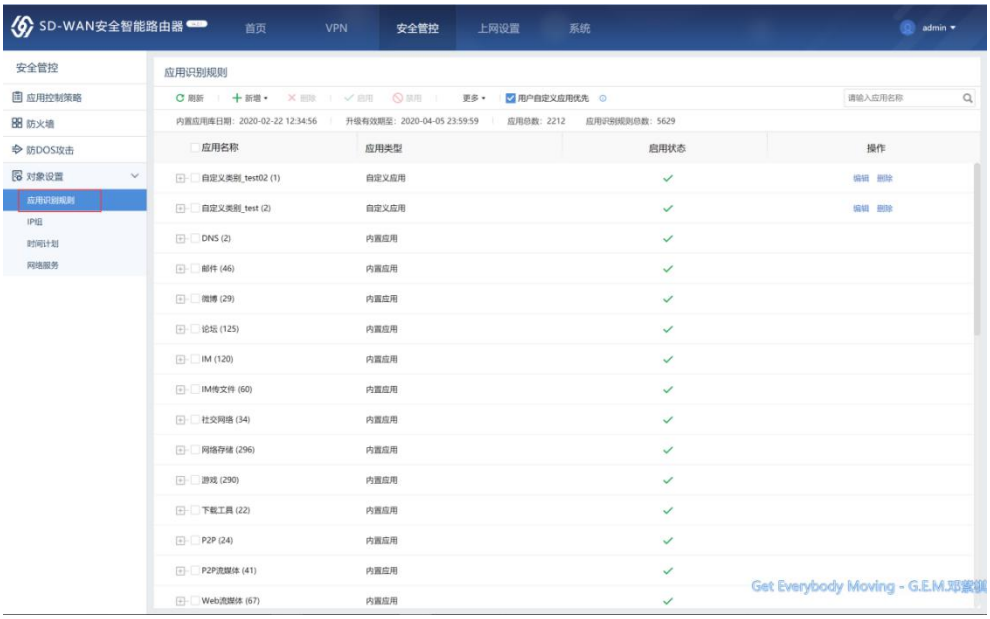
对象设置包括[应用识别规则]、[IP组]、[时间计划]、[网络服务]、[Radius认证服务器设置]，如下图。

3.4.6.1. 应用识别规则

该应用识别功能的内置识别库包含了2200多条应用，5600多条的规则，涵盖了主流的应用，可以对绝大多数的用户流量进行识别。

内置应用库

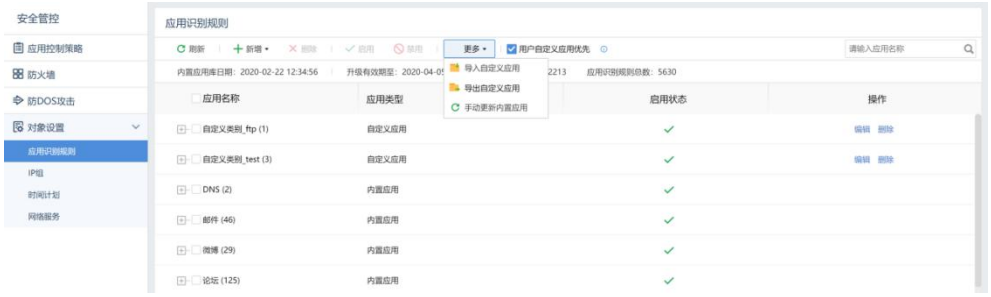
内置库中的应用为系统本身内置，无法进行删除。



部分基础网络行为在禁用应用的同时，会提示不允许禁用基础网络协议。

其他说明：

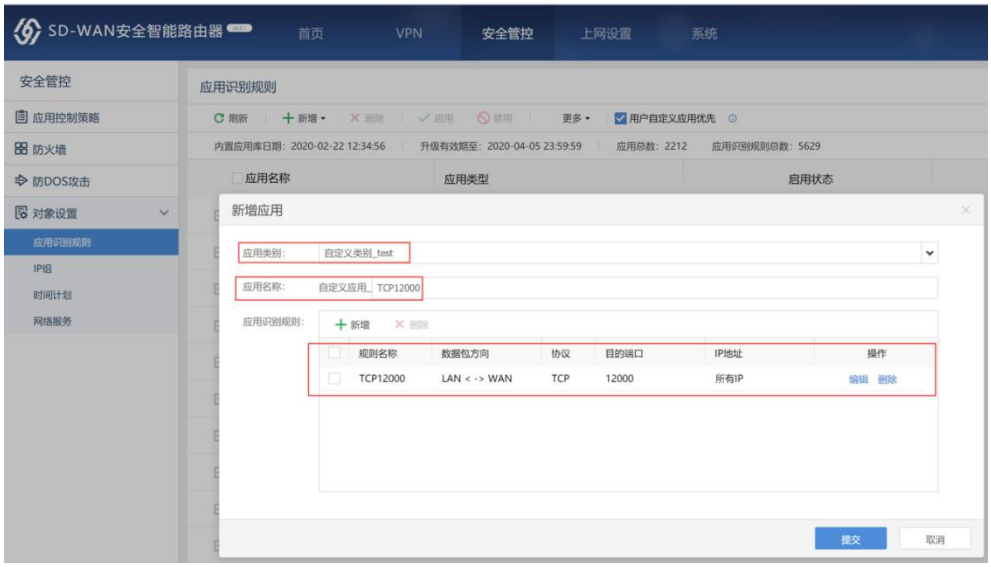
SDW-R的内置应用库一般是在线自动更新到最新版本，或者可以通过离线的方式手动更新内置应用。



自定义应用

SDW-R支持自定义应用，具体操作如下：

1. 点击<新增>，配置界面如下图。



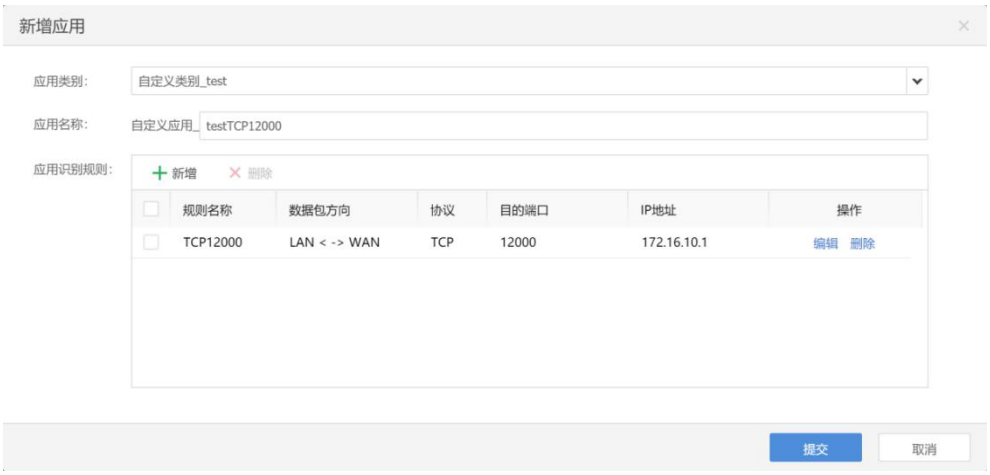
2. 新增应用识别规则，根据应用类型特征进行相应的配置。

例如：该客户内网的服务器地址段172.16.10.0/24，现需要SDW-R可识别172.16.10.1端口12000的流量。根据该例子配置应用识别规则时，如下图所示。

各配置项说明：

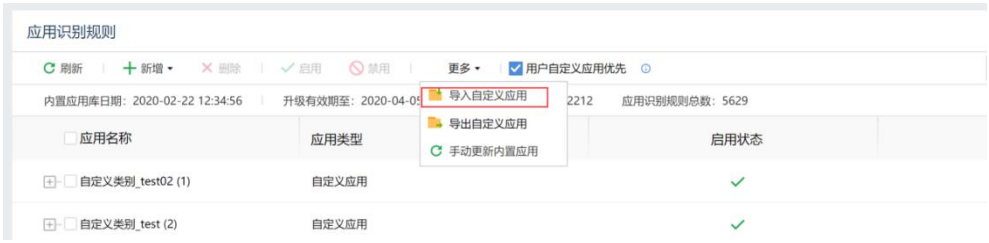
- [规则名称]：自定义规则名称。
- [数据包方向]：可选择 LAN<->WAN，LAN->WAN，WAN->LAN 三个方向，根据实际情况选择，本例子中选择 LAN<->WAN。
- [协议类型]：选择相应的协议类型。
- [目的端口]：选择相应的端口。
- [IP 地址]：选择相应的 IP 地址。

3. 配置完成之后，点击<确定>，点击<提交>之后，即可保存配置。

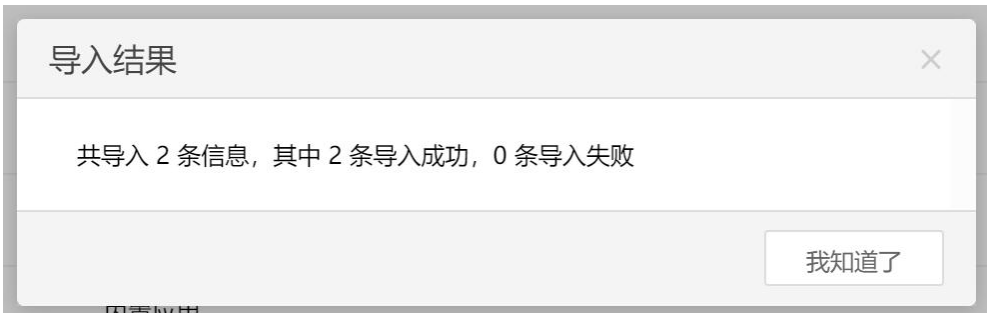


其他配置说明：

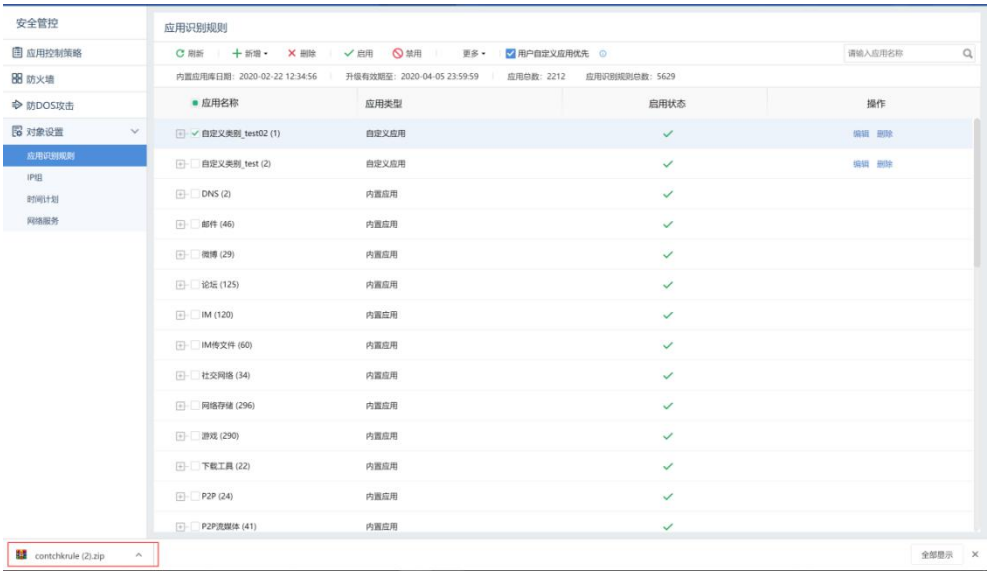
1. 当前自定义应用较多时，支持一键导入通过[更多/导入自定义应用]。



导入完成之后，提示导入成功。



2. 也可将设备上的自定义应用导出存放在本地。



导出完成之后为“contchkrule”的压缩包文件。

3. 当勾选了用户自定义应用优先时， 则识别应用时优先会匹配自定义应用规则。

注意：

设备接入 BBC 且和策略模板相关联后，设备端自己的自定义应用会消失，因为要和 BBC 的策略模板保持一致。而且在设备上，除了升级内置库的操作外，其余操作全被禁用。接入 BBC 之后需要现将自定义的应用先导出放本地保存。

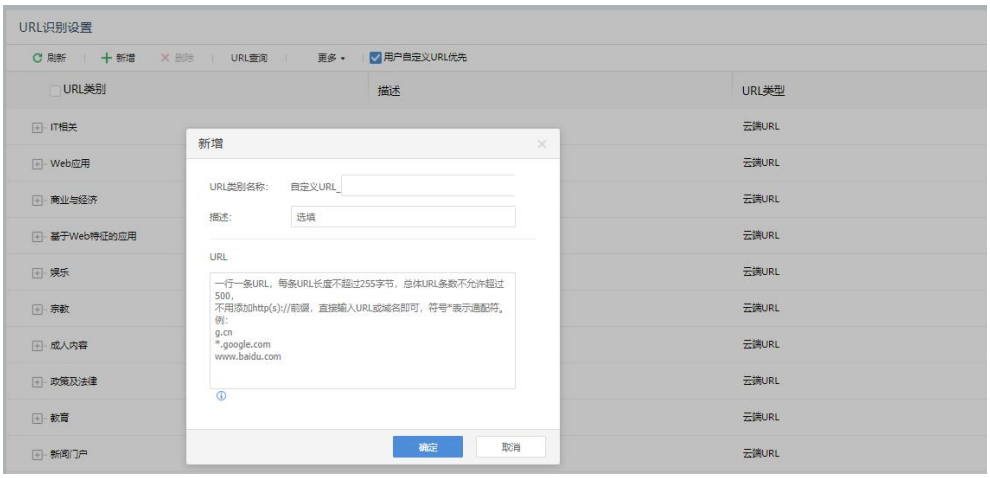
3.4.6.2. URL 识别设置

URL功能的内置多条URL识别规则，涵盖了主流的URL。在URL识别设置，可以查看内置的URL的详情，如下图所示。

管理员也可也点击<URL查询>，通过输入URL进行搜索，如下图所示。

URL的新增

在[安全管控/对象设置/URL识别设置]的页面下，点击<新增>，配置URL类型名称、描述以及URL，如下图所示。



配置完成后，点击<确定>即可。

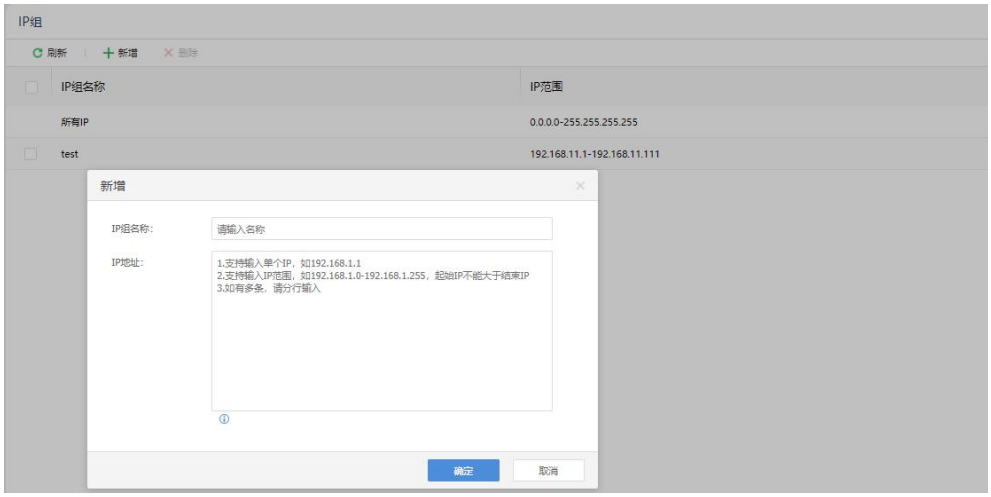
URL的管理

对于新增的URL识别规则，点击<删除>，可对新增的规则进行删除以及编辑。

勾选“用户自定义URL优先”，则自定义的URL规则展示在默认URI设置的规则前。

3.4.6.3. IP 组设置

1. 内网有不同的IP段拥有不同的上网权限，在这里可以根据IP地址进行IP组的定义，页面如下图。



例如：该客户内网有两个地址段192.168.1.0/24和192.168.2.0/24，那在这里可以进行IP组的定义，可以定义单个IP也可以定义一段IP，点击新增，出现[新增页面]进行配置。

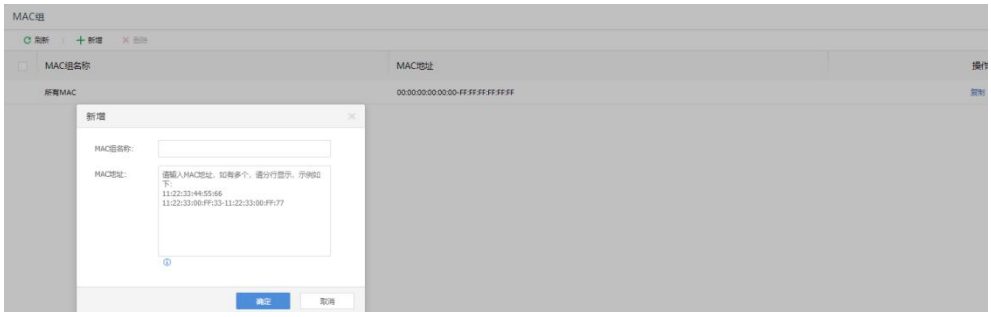
各配置项说明：

- [IP 组名称]：给需要定义的 IP 或 IP 段进行命名，可自定义。
- [IP 地址]：可以输入单个 IP 或者 IP 范围。

2. 点击该页面的<提交>保存配置。

3.4.6.4. MAC 组设置

针对内网不同的MAC拥有不同的上网权限，在这里可以根据MAC地址进行MAC组的定义，页面如下图。



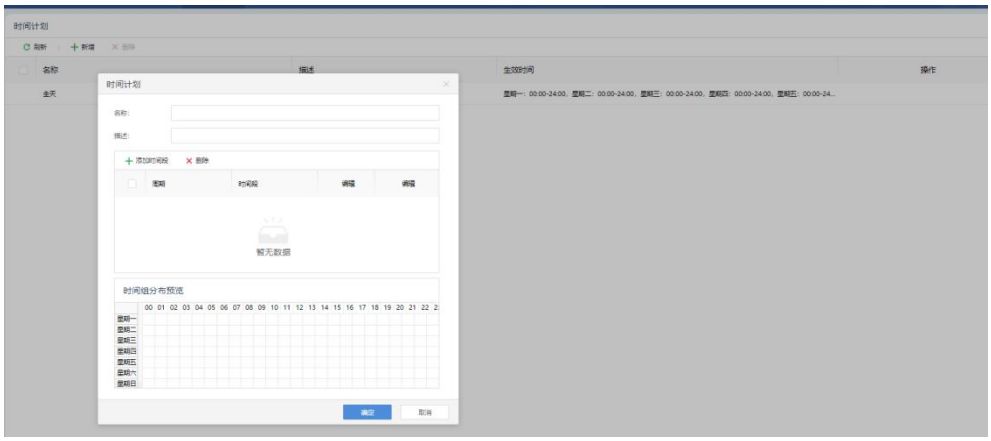
点击新增，出现[新增页面]进行配置。

各配置项说明：

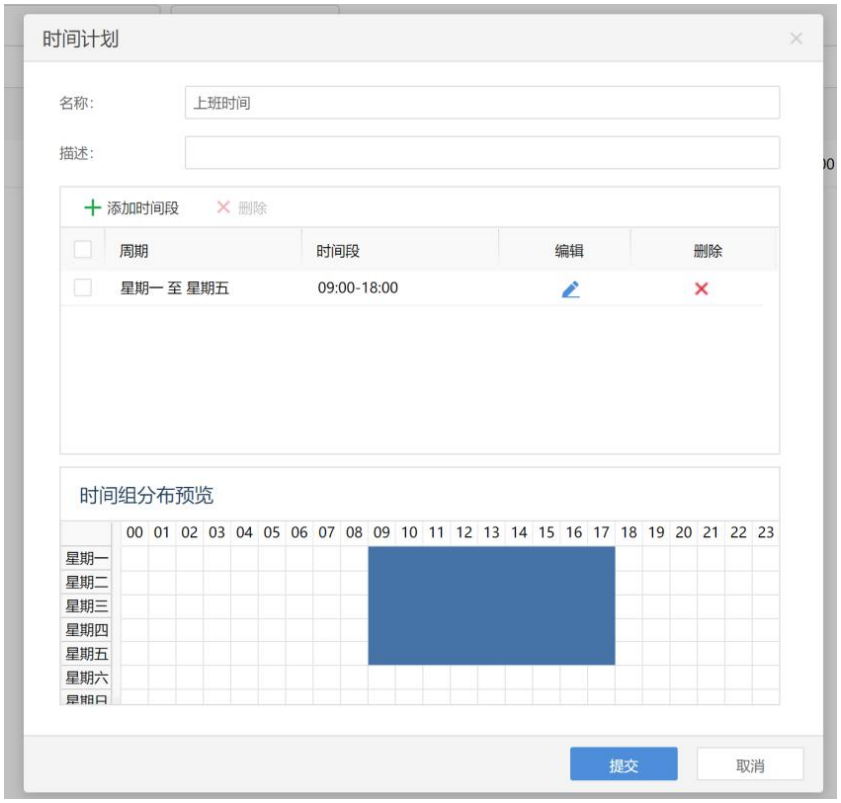
- [MAC 组名称]：给需要定义的 MAC 组进行命名，可自定义。
- [MAC 地址]：可以输入单个 MAC 或者 MAC 范围。

3.4.6.5. 时间计划设置

1. 用于定义常用的时间段组合，这些时间组合可以在[防火墙设置]模块中使用，以设置相应的规则生/失效时间，该时间以设备上当前系统时间为准，页面如下图。

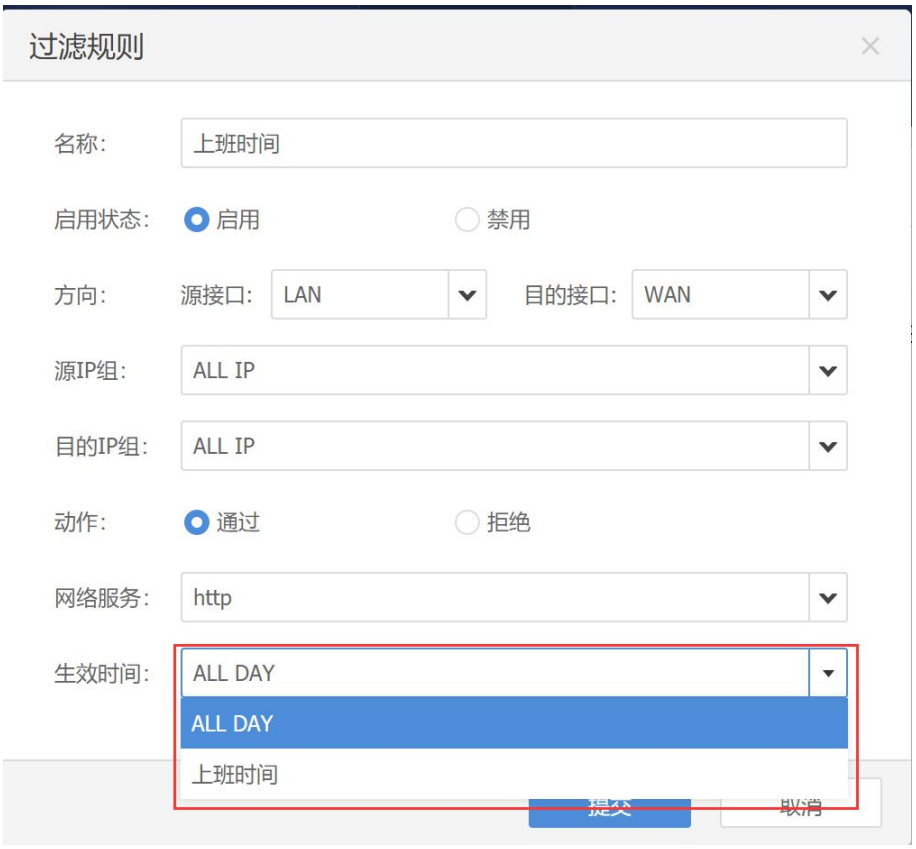


2. 点击<新增>，出现时间计划配置页面，页面如下。



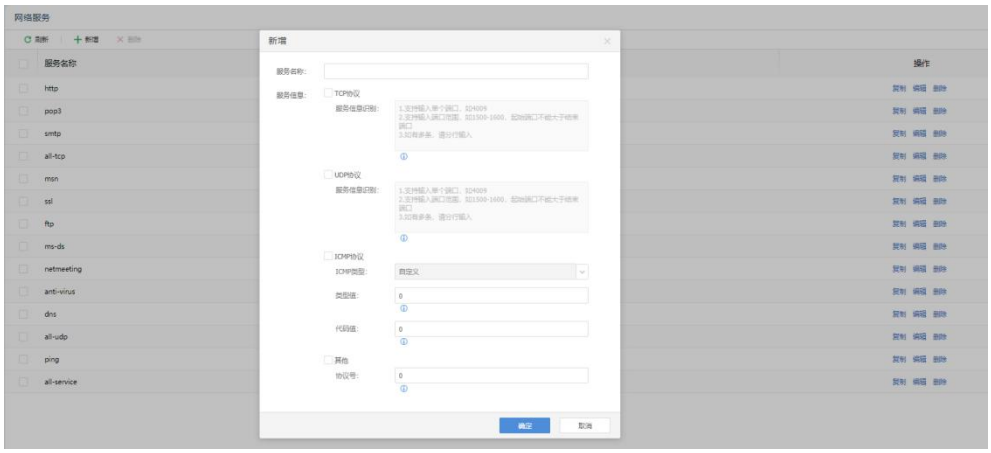
3. 定义一个名称为“上班时间”的时间段，选取相应的时间段组合，宝蓝色为生效时段，白色为失效时段。点<提交>完成时间组的定义。

4. 定义完成时间段之后，对防火墙设置中的规则进行时间限定，如下图。



3.4.6.6. 网络服务设置

通过网络运行的软件和通信程序使用不同的传输协议和端口，在设定针对这些数据的防火墙规则之前需要先定义其传输协议和端口，页面如下。



操作案例

需要在SDW-R设备上对SQL SERVER服务数据的传输设置规则。

操作步骤

1. 首先需要对SQL SERVER服务所使用的协议和端口进行定义，点击<新增>，出

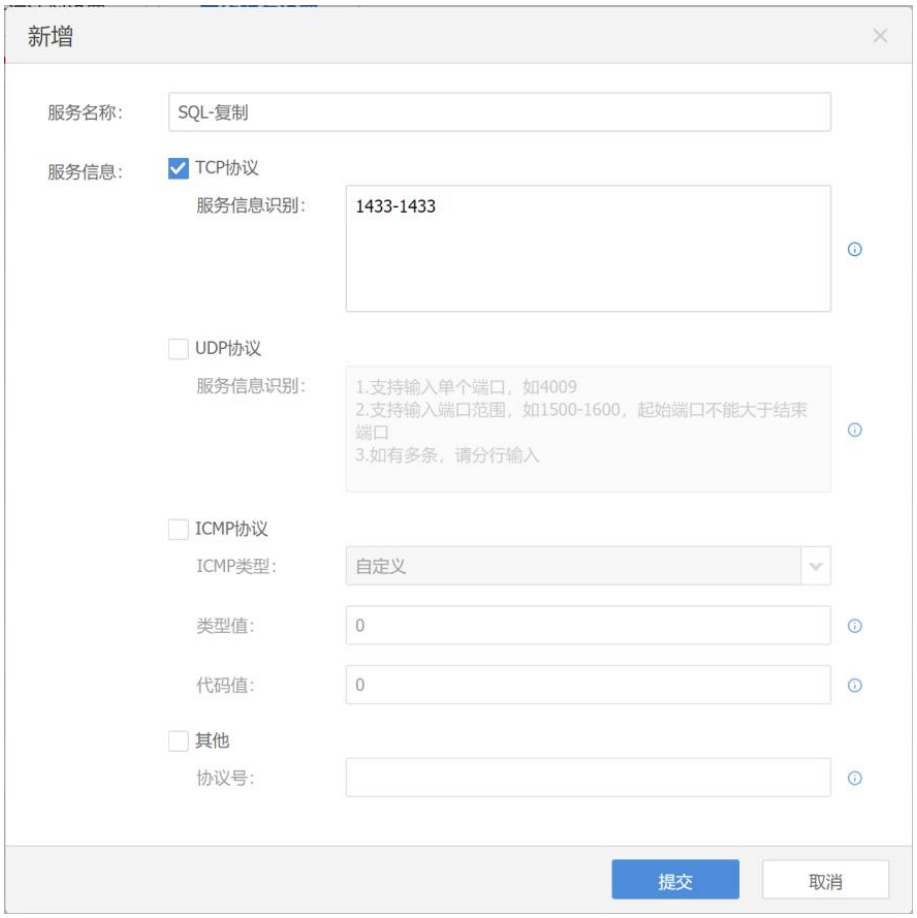
现[网络服务]配置对话框，页面如下图。

各配置项说明：

- [服务名称]：可以自定义（本例中可以设置为：SQL）。
- [服务信息]：选择 TCP 协议。
- [服务信息识别]：填写 1433。

2. 点击<提交>，将该服务添加到网络服务设置定义列表中，完成SQL SERVER服务的定义。

3. 在此新增复制功能，可以直接复制该服务规则，点击<复制>，则出现如下页面。

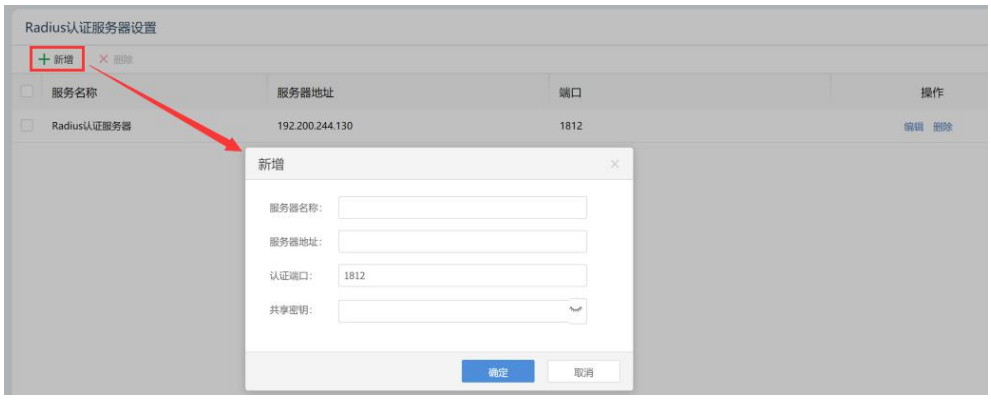


其他说明：

[服务名称]：可以进行修改，添加端口的方式同上。如果客户有个ERP系统，要用到SQL的服务端口，同时还需要80等服务端口，可以添加到这个表里面，放通规则的时候只要放通这一个服务就可以了。

3.4.6.7. Radius 认证服务器设置

新增Radius认证服务器，用于WIFI接入时，提供用户名密码认证方式。配置界面如下。



各配置项说明：

- [服务器名称]：可以自定义设置。
- [服务器地址]：填写 Radius 服务器的地址。
- [认证端口]：Radius 服务器认证默认使用 1812 端口，如 Radius 服务器有修改则需要修改为对应的端口。
- [共享密钥]：Radius 服务器处所设置的密钥，配置时需保持一致。

3.5. 上网设置

上网设置包括[接口设置]、[WLAN设置]、[路由设置]、[NAT地址转换]、[DHCP设置]模块，如下图所示。

3.5.1. 接口设置

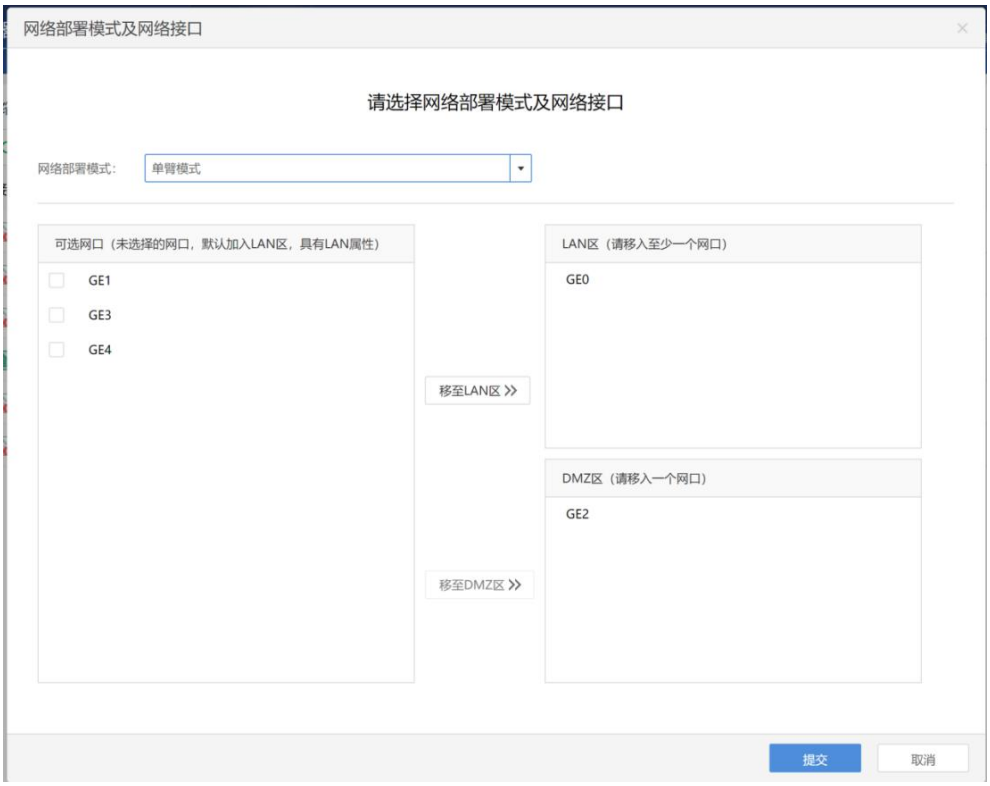
用于配置设备的部署模式，有两种网络部署模式可供选择：单臂模式和网关模式。

3.5.1.1. 部署模式

单臂单线路

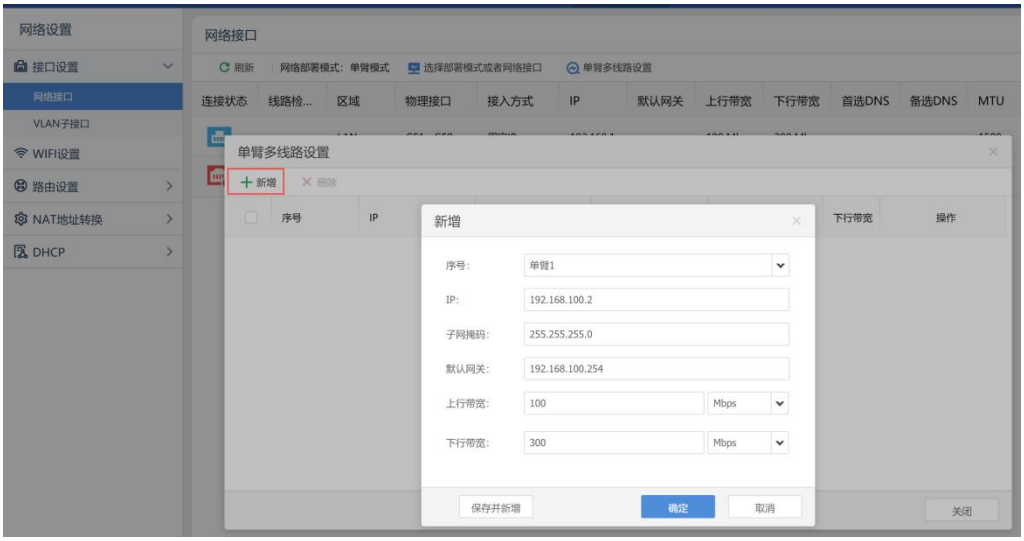
用于用户总部或者分支环境只有一条出口线路的场景中，对用户的网络环境改动较小。

1. 选择单臂模式时，需要选择相应的物理接口移动至内网区域（LAN区）、DMZ区，如下图。



单臂多线路

用于用户总部或者分支环境有两条出口线路的场景中，对用户的网络环境改动较小。选择[网络部署模式/单臂多线路设置]，具体配置界面如下图所示。



各配置项说明：

- [序号]：设置单臂多线路中的第一条线路信息（单臂 1）、第二条线路信息（单臂 2）等；
- [IP]：设置单臂线路的 IP 地址，该 IP 地址必须与 LAN 口同网段；
- [子网掩码]：设置单臂线路 IP 地址的子网掩码；
- [默认网关]：设置单臂线路 IP 地址的默认网关地址；
- [上下行带宽]：根据实际网络环境进行带宽值设置。

⚠ 注意：

1、多线路 IP 要求跟 LAN 口 IP 同网段，线路数最大支持 4 条。

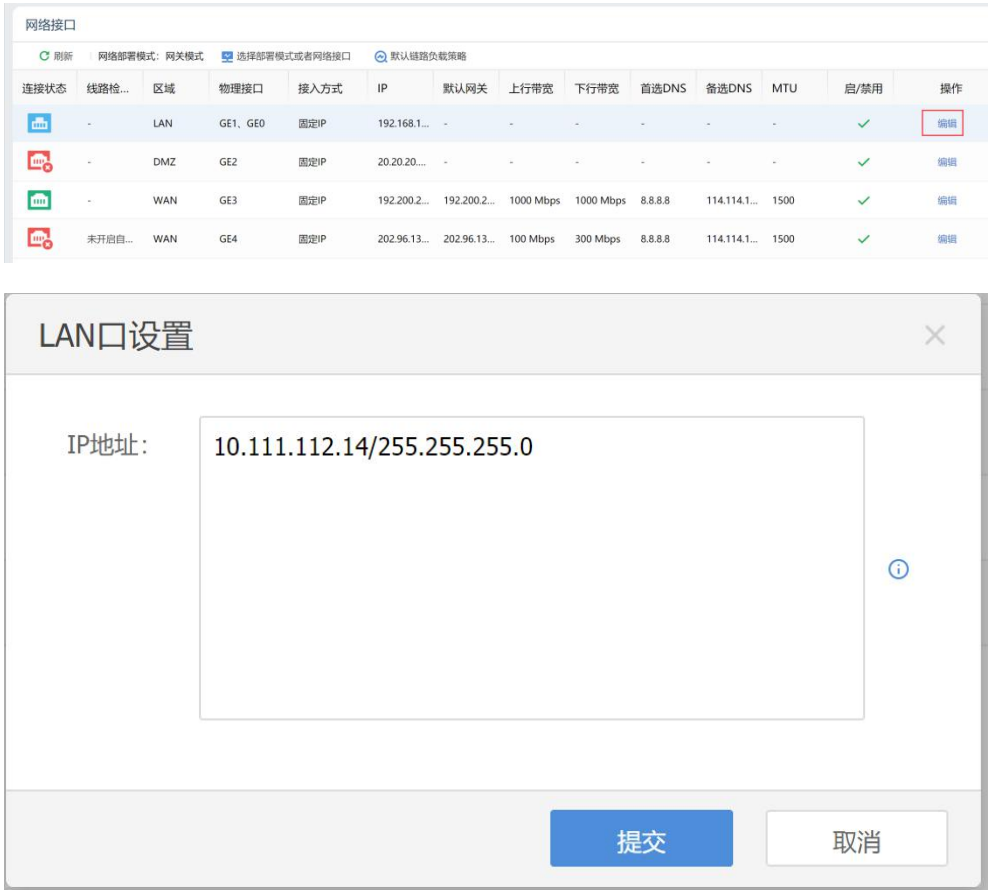
2、配置单臂 VPN 多线路后，VPN 监听端口改成对应的多线路 IP。

网关单线路/网关多线路

2. 选择网关模式时，不仅需要选择相应的物理接口到内网区域（LAN区），同时也必须选择相应的外网线路至WAN区。如下图。

3.5.1.2. 区域接口配置

1. 将物理接口分配完区域之后，对内网（LAN区）、DMZ区进行IP地址的配置，如下图。



2. 外网线路（WAN区）选择接入方式、是否启用线路配置、上下行带宽、MTU值、MAC设置，如下图所示。

[GE1配置]：点击<编辑>，选择接入方式，包括“ADSL拨号”，“DHCP”，“固定IP”三种方式，界面如下图。

A. ADSL拨号配置

GE1线路为ADSL拨号时，填写完[用户名]和[密码]信息后，点击<开始拨号>，点击<查看详情>可查看当前拨号成功之后获取到的IP地址、默认网关的基础信息的详情。可以设置是否开启自动拨号，可以设置掉线检测条件。

点击<线路故障检测>对线路故障检测进行修改，如下图所示。

勾选启用线路故障自动检测，可以启用线路故障自动检测功能。

各配置项说明：

- [检测方法]：DNS 解析、PING、ARP，DNS 解析方式输入正常情况下设备可以解析到的域名，PING 方式输入正常情况下设备可以 PING 通 的目标 IP，ARP 方式输入正常情况下设备可以通过 ARP 请求获取到 MAC 地址的 IP 地址。通过以上方式来判断线路工作是否正常。
- [检测间隔]：设置自动检测的时间间隔。
- [失败阈值]：检测间隔间隔内出现数据包请求出现失败的次数阈值，超过该值就认为线路故障。

点击<高级设置>对设备上下行带宽、MTU、MAC设置等进行修改，如下图所示。

各配置项说明：

- [上下行带宽]：根据实际带宽值进行配置。
- [MTU 值]：一般使用默认值即可。
- [MAC 设置]：默认使用物理网口的 MAC 地址。

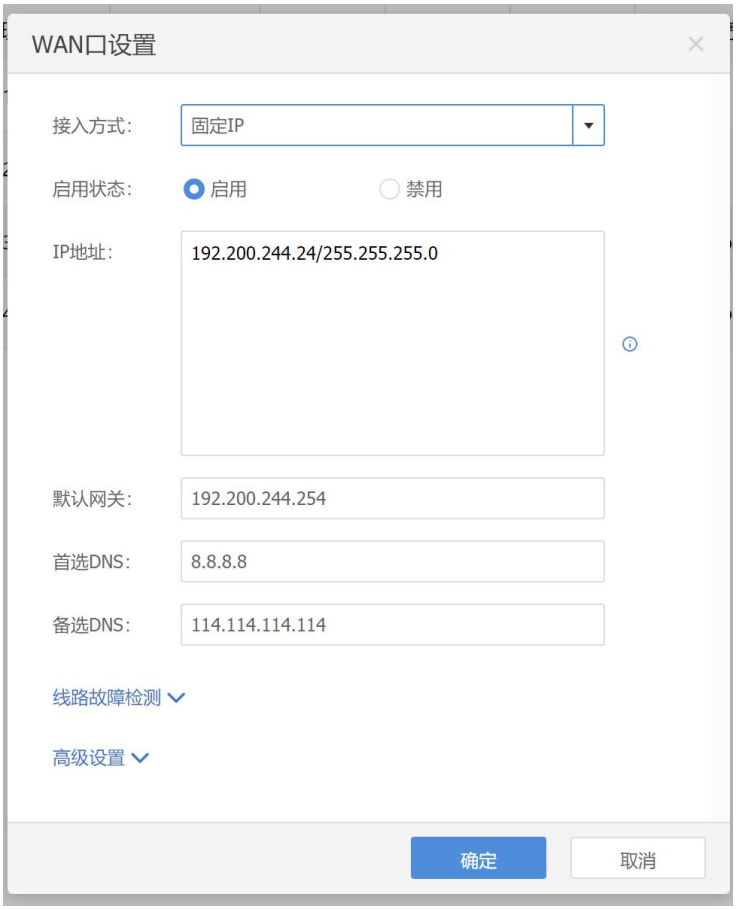
B. DHCP配置

外网接口线路选择接入方式为DHCP方式时，只需启用该线路，设备会向相应的DHCP服务器请求地址。

线路故障检测与高级设置与ADSL拨号中的设置类似，这里不再赘述。

C. 固定IP配置

外网接口线路选择接入方式为固定IP时，需要启用该线路，配置相应的公网IP、掩码、默认网关、首选DNS、备选DNS的信息。



线路故障检测与高级设置与ADSL拨号中的设置类似，这里不再赘述。

D. 4G线路配置：

支持4G拨号功能的设备，在网络接口设置处会一条4G线路，如下图所示。

点击<编辑>，可以对4G线路进行配置，如下图所示。

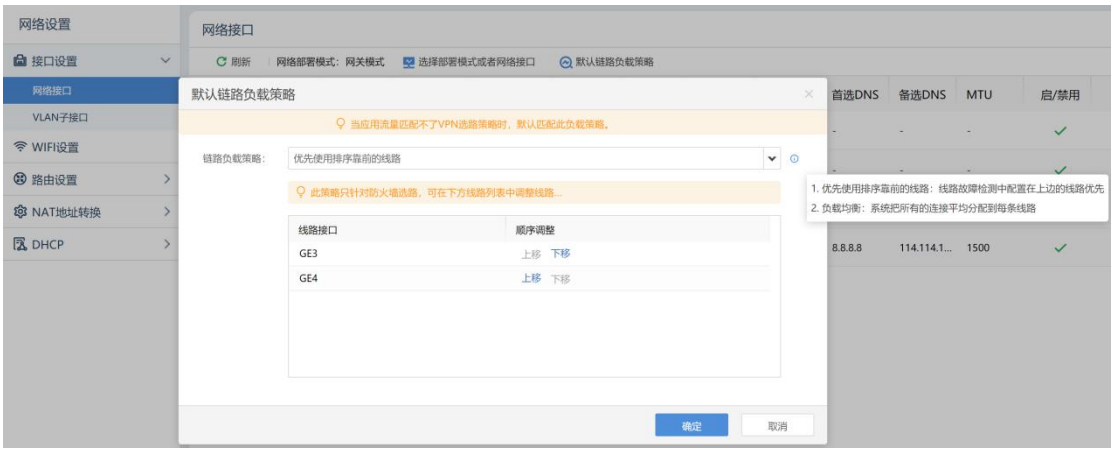
各配置项说明：

- [启用状态]：线路是否启用。
- [当前状态]：查看 4G 线路当前状态。
- [查看详情]：查看 4G 线路的 IP 地址、默认网关的情况。
- [开始拨号]：填写完 APN 码、用户名、密码之后，点击开始拨号，4G 线路开始进行拨号。
- [自动拨号]：是否开启自动拨号功能。
- [上下行带宽]：根据实际的带宽值进行配置。
- [MTU 值]：一般保持默认的 MTU 值。
- [模式]：可以选择 4G 优先、仅 4G 两种模式。
- [认证方式]：可选择自动选择或使用 PAP 认证、使用 CHAP 认证。
- [绑定 SIM 卡]：选择是时，只能使用绑定的 SIM 卡进行拨号，提供安全性；选择否时，不绑定 SIM 卡，可使用任意 SIM 卡进行拨号访问互联网。

3.5.1.3. 默认链路负载策略

线路分配策略

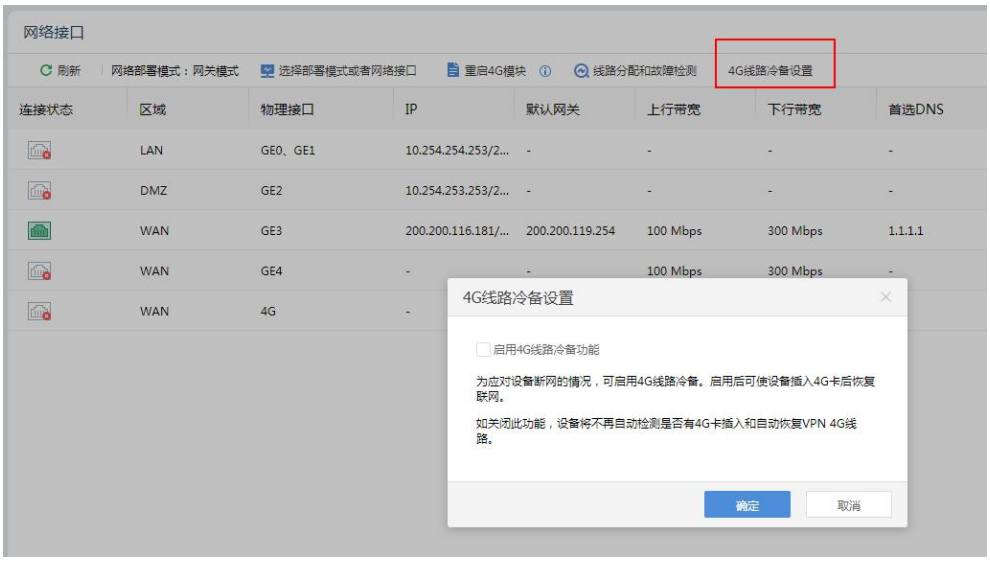
设备开启多线路授权的情况下，需要通过[线路分配与故障检测]来检测两条线路的健康状况，同时需要实现SDW-R中针对防火墙选路功能，也必须设置该选项。其中线路分配策略分别为：优先使用排序靠前的线路，线路负载均衡两种方式，如下图所示。



此策略针对SDW-R作为网络出口时，代理内网PC访问互联网时，所有的上网流量是走排序靠前的线路，还是通过负载均衡调度到各个线路上。

3.5.1.4. 4G 线路冷备设置

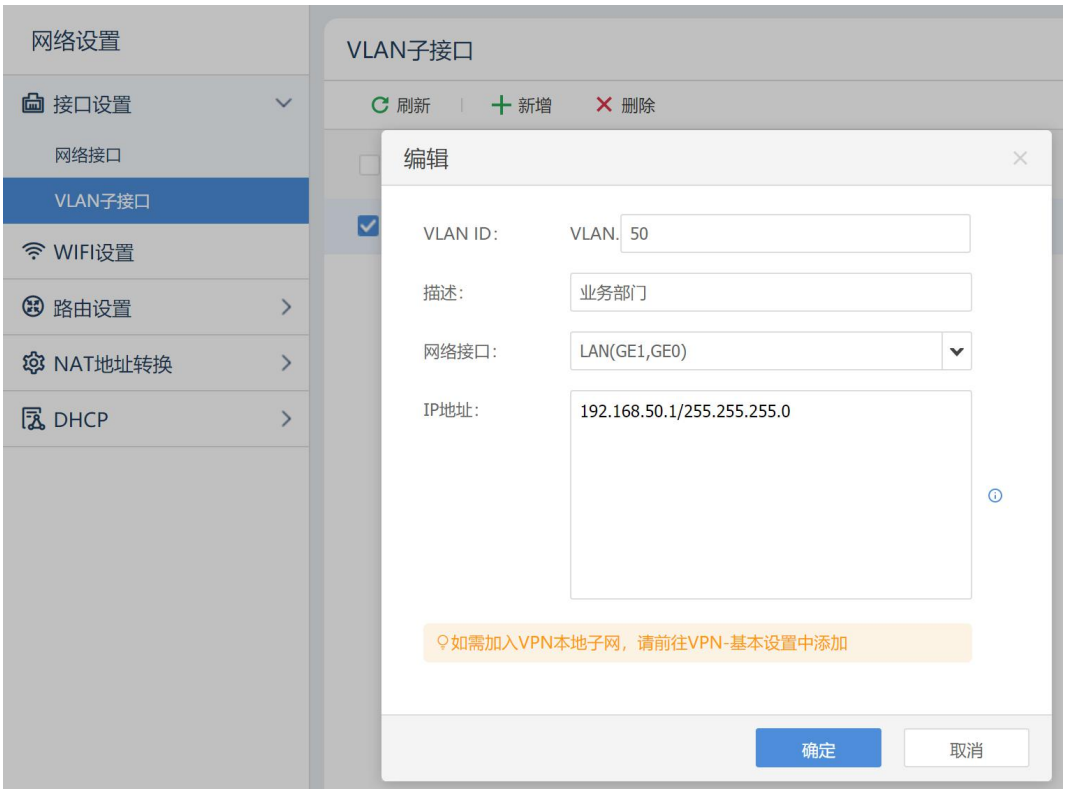
4G卡可以作为冷备灾备线路，平常只用有线，没有插4G卡，当有线故障的时候插入4G卡的情况下可以实现外网业务和VPN业务自动恢复。



启用该功能需要配合线路探测一起使用，相关配置请参考“线路故障检测”章节配置。

3.5.2. VLAN 子接口

SDW-R设备提供vlan子接口功能，提高设备网口扩展性；设备与vlan交换机连接使用，划分网口区域（广播域），配置如下图所示。



点击<新增>可进行VLAN接口相关的配置，配置项说明如下：

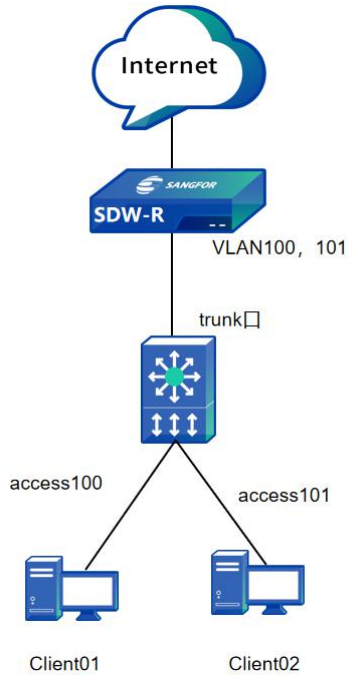
- [VLAN ID]：设置 VLAN 的序列号；
- [描述]：设置 VLAN 的描述信息，可自行定义；
- [网络接口]：设置 VLAN 所关联的区域接口，可以选择 LAN 或者 DMZ；
- [IP 地址]：设置 VLAN 的 IP 地址。

注意：

VLAN 子接口归属于 LAN 或 DMZ 区域，所以如果其他功能配置生效区域为 LAN，则包含 LAN 下的 VLAN；VLAN 网段如果需要加入 VPN 本地子网，请前往 VPN-基本设置中添加对应 VLAN 网段。

3.5.2.1. VLAN 子接口配置案例

分支内网存在采购部门与财务部门，现在需要财务部门无法访问互联网，采购部门正常访问互联网。相关拓扑如下图所示。



⚠ 注意：

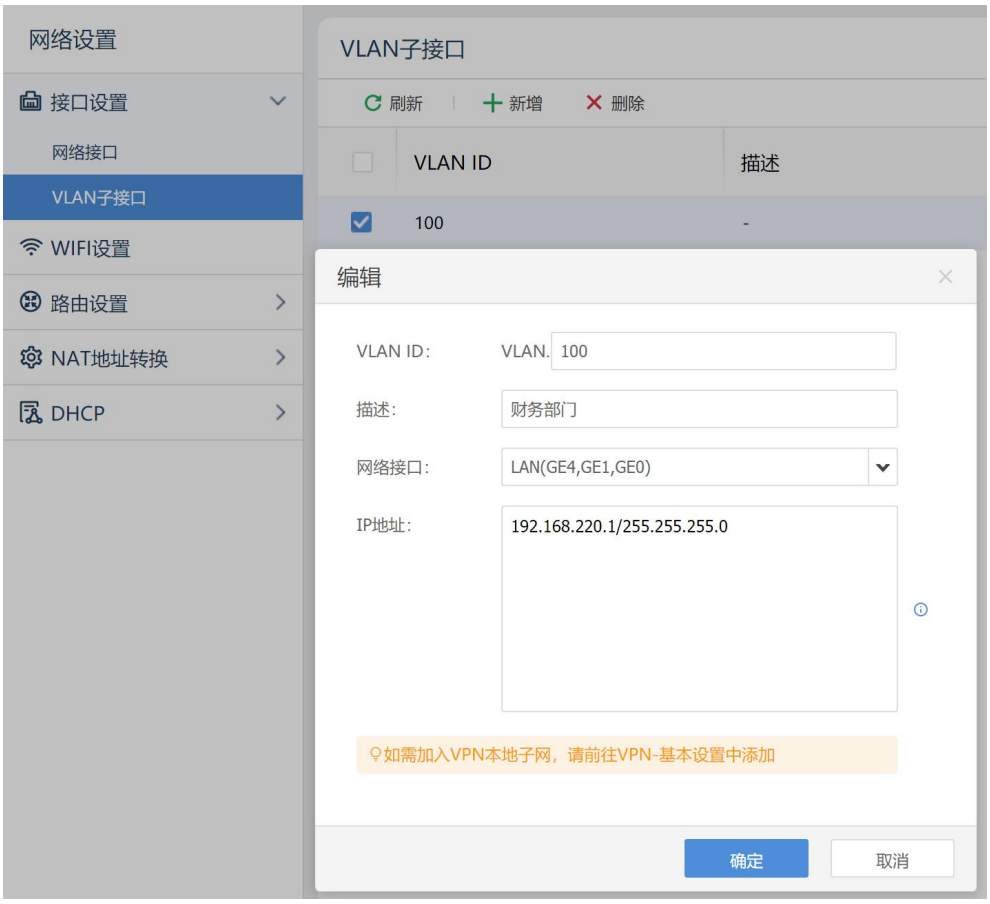
1.设备的 VLAN 子接口对应网口要与 VLAN 交换机的 trunk 口相连。

2.VLAN 子接口的 DHCP 是单独的功能，如果要使用 DHCP 功能，要在 DHCP 服务中启用。

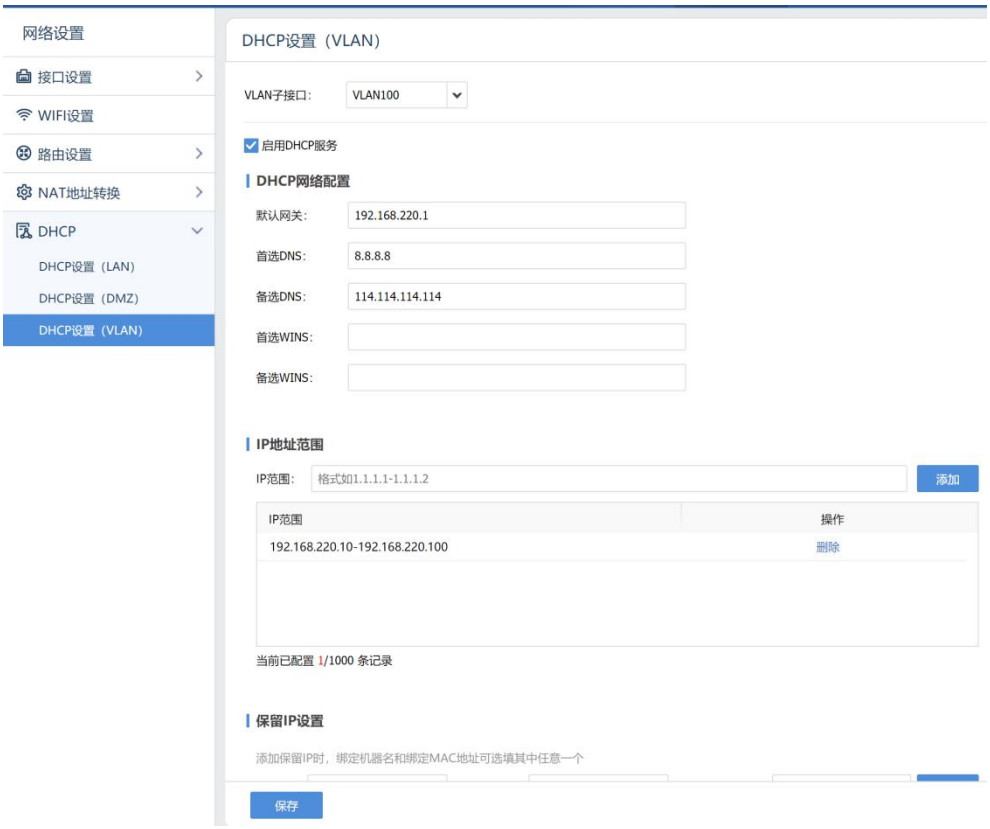
3.VLAN 子接口归属于 LAN 或 DMZ 区域，所以如果其他功能模块生效区域为 LAN，则包含 LAN 下的 VLAN。

4.VLAN 子接口下的内网如果要加入 SANGFOR VPN，需要在 VPN 基本设置-本地子网上加对应网段。

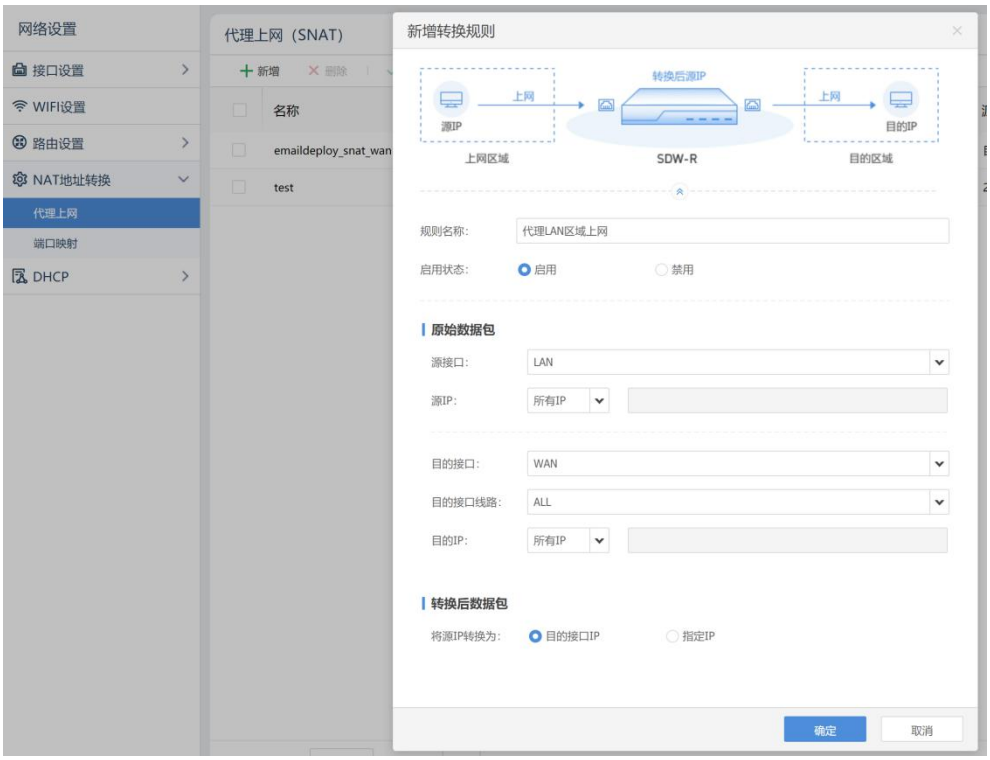
1. SDW-R设备控制台，打开[网络设置/接口设置/VLAN子接口]，设置VLAN接口配置。新增VLAN子接口VLAN100，网络接口选择“LAN”（或者DMZ），配置相应的IP地址。



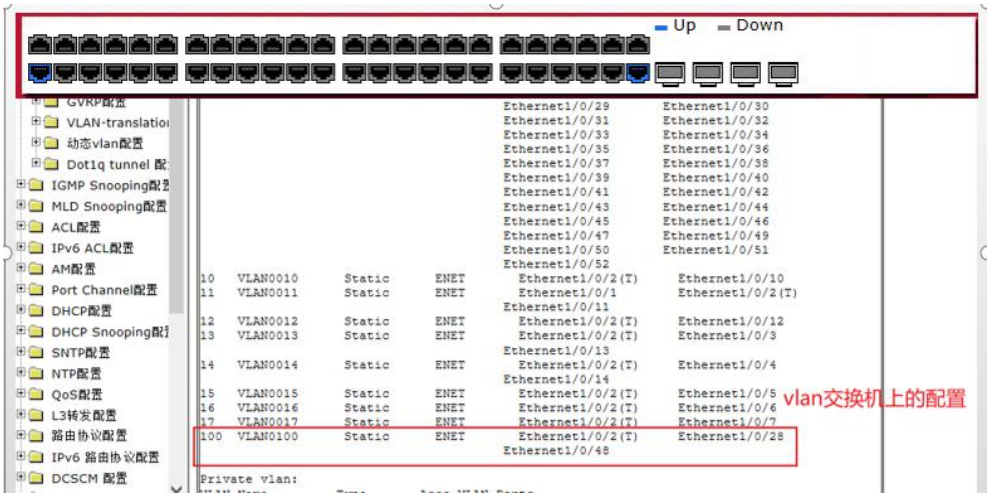
2. 在SDW-R控制台[网络设置/DHCP/DHCP设置(VLAN)]开启VLAN子接口的DHCP功能。



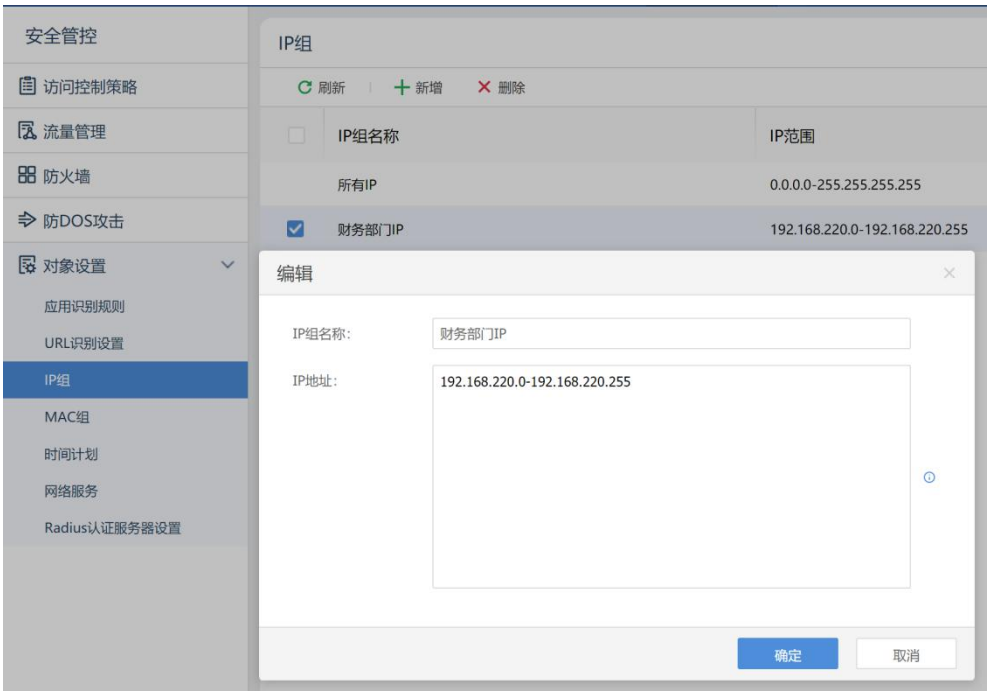
3. 在SDW-R控制台[网络设置/NAT地址转换/代理上网]，开启SNAT代理上网，代理LAN（如果步骤1中的VLAN子接口选择的网口为DMZ，则用DMZ口）上网。



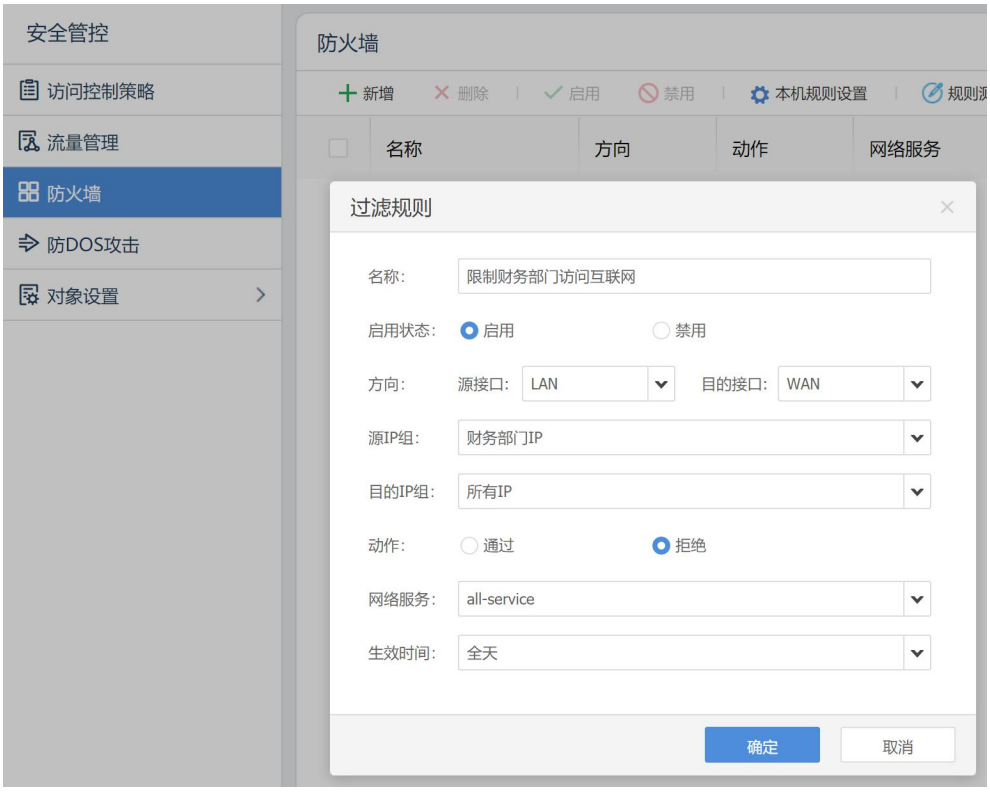
4. 设备的LAN口连接VLAN交换机的trunk口（下图中的交换机2口），Client连接VLAN交换机的access口（下图中的交换机28或48口）



5. 在在SDW-R控制台[安全管控/对象设置]设置对应的财务部门IP组。



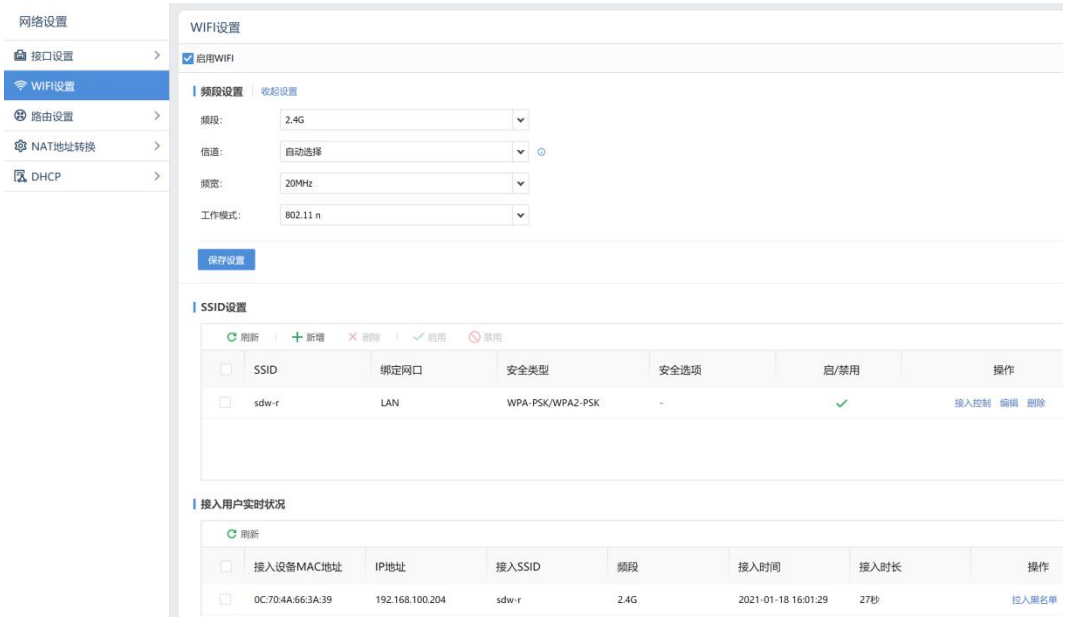
6. 在SDW-R控制台[安全管控/防火墙]新增过滤规则，禁用LAN-WAN的all-service服务；则属于LAN区域的VLAN 100下的财务部门Client访问外网时----会被防火墙封堵无法访问。



3.5.3. WLAN 设置

3.5.3.1. 频段设置

1. SDW-R设备WIFI版本支持局域网使用无线WIFI方式接入，在SDW-R设备的配置界面可以看到WIFI相关的配置选项，如下图。



2. 勾选[启用WLAN]，表示在设备上开启WIFI功能。

各配置项说明：

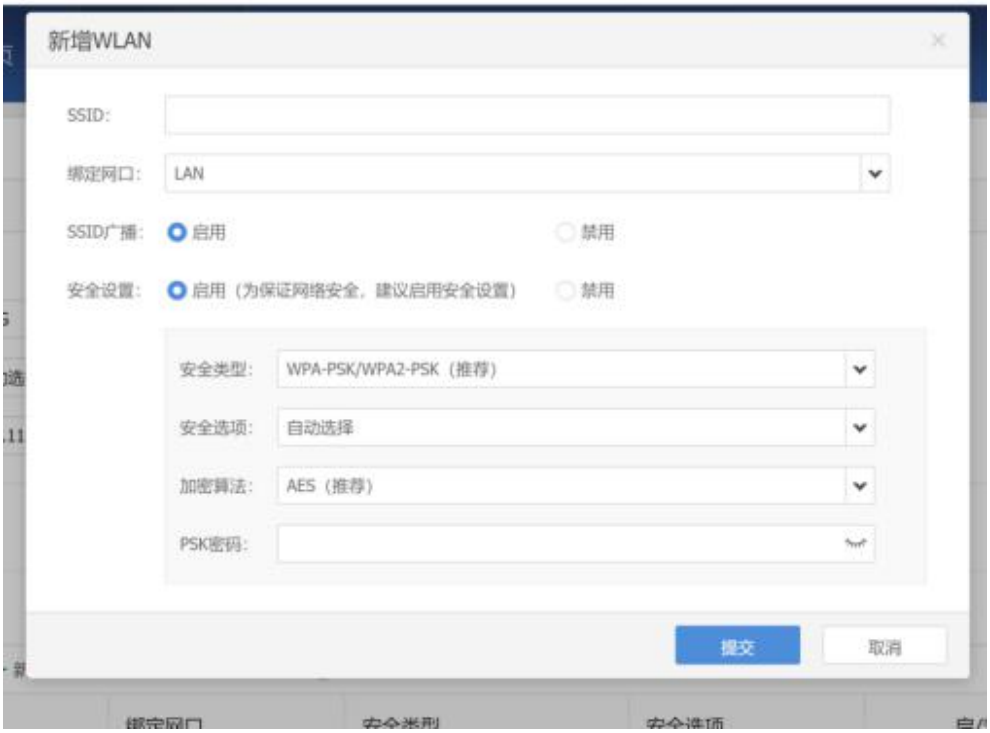
- [频段设置]：频段可以选择 2.4G 或者 5G；信道可从信道 1 至信道 13 中选路一个信道进行传输，推荐使用的默认信道可避免无线信道冲突造成的传输速率下降；2.4G 频段工作模式可以选择 802.11n，802.11b，802.11g 中的一种，5G 频段工作模式可以选择 802.11a，80211.ac 中的一种。

3. 点击<保存设置>，即可保存频段相应的设置。点击<收起设置>可以隐藏频段相应的设置。

3.5.3.2. SSID 设置

WLAN设置支持双SSID。允许双SSID，SSID的启用、绑定网口、SSID广播、安全认证等单独配置。

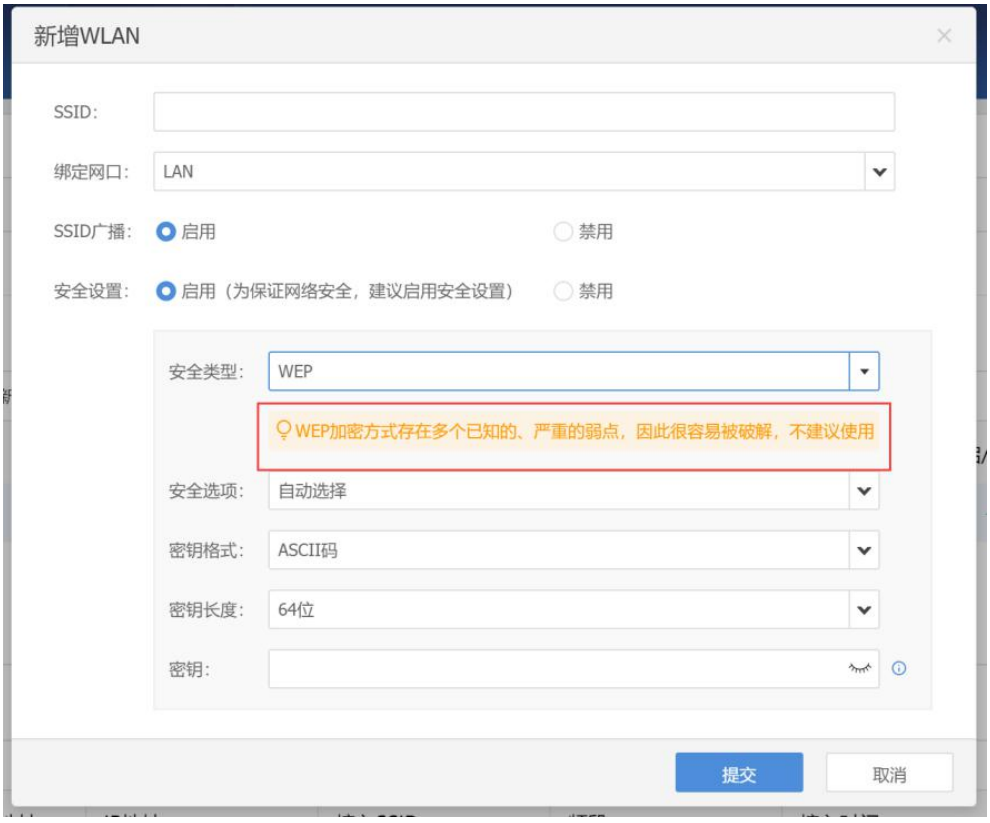
1. 点击<新增>如下图。



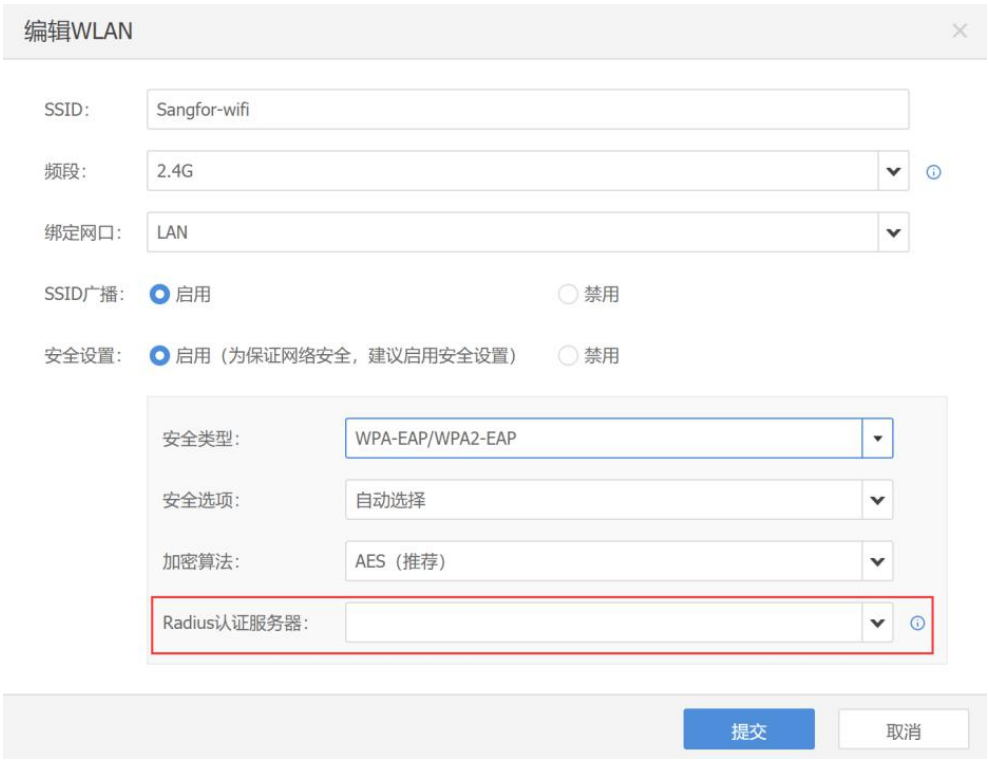
各配置项说明：

- [SSID]：用于设置 WIFI 的名称，无线 WIFI 客户端将显示对应的 SSID 名称。
- [绑定网口]：可以选择 LAN 口。

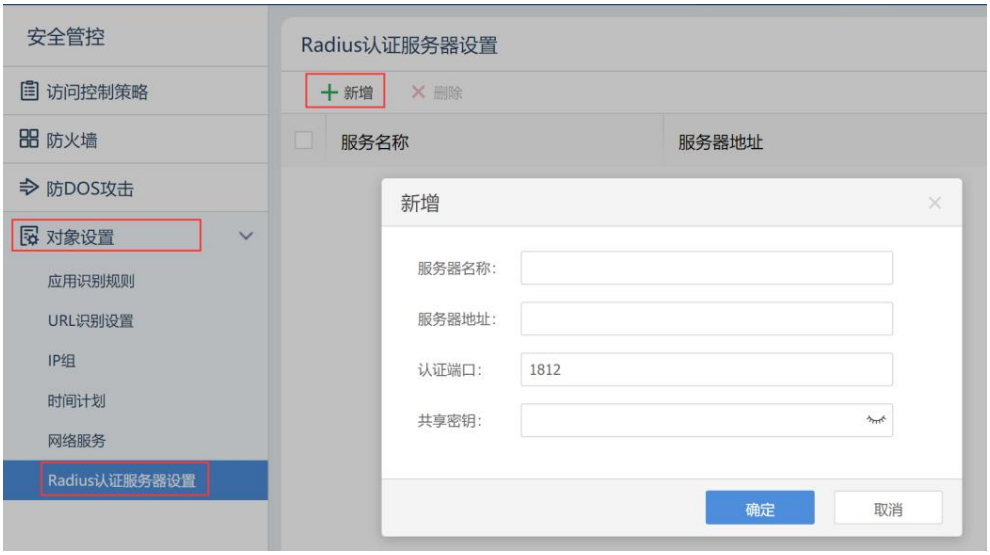
- [启用 SSID 广播]：用于设置是否广播 SSID，如果广播 SSID，则所有处于设备无线信号范围内的无线设备均能发现这个 WIFI 网络，默认该选项启用，如果需要较高的 WIFI 安全性则可以取消勾选该功能。
- [启用安全设置]：表示对 WIFI 网络进行加密保护，防止未经授权的无线用户擅自接入 WIFI 网络。
- [安全类型]：用于选择 WIFI 网络的加密协议，包括 WPA-PSK/WPA2-PSK、WEP、WPA-EAP/WPA2-EAP 三种加密方式，默认为 WPA-PSK/WPA2-PSK。WEP 加密协议因为容易遭到破解，除非有无线设备不支持 WPA-PSK/WPA2-PSK，否则不建议使用 WEP，在切换到 WEP 方式时，设备也会有对应的提示，如下图。



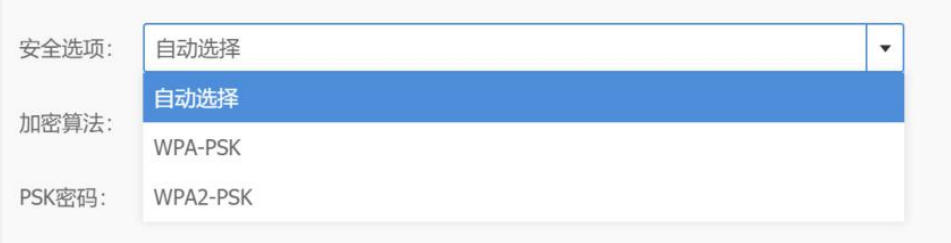
安全类型WPA-EAP/WPA2-EAP是结合Radius认证服务器实现的，支持使用账号密码认证。



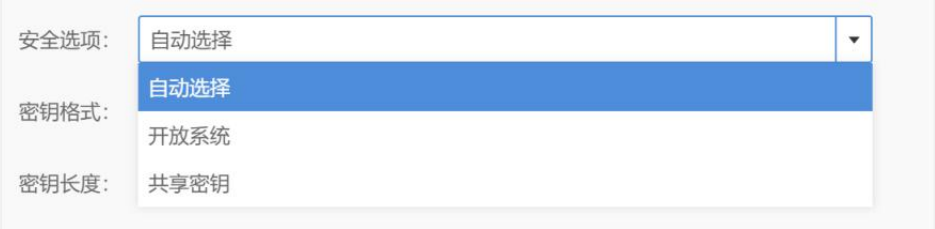
2. 需要在[对象设置]中提前预设置好Radius认证服务器的相关信息，具体如下图所示。



- [安全选项]：用来选择具体的加密协议，如果[安全类型]选择的是WPA-PSK/WPA2-PSK 方式，则[安全选项]包括自动选择、WPA-PSK 和 WPA2-PSK 三种方式，如下图。

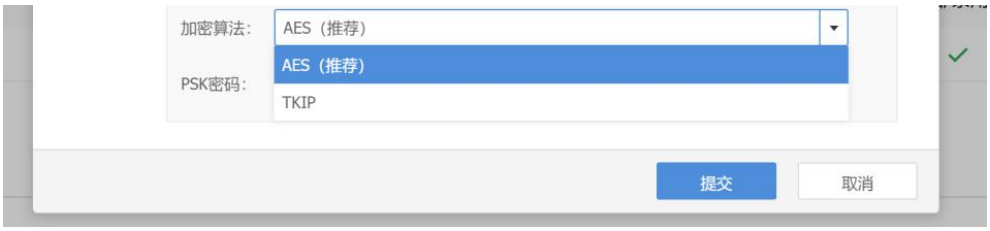


如果[安全类型]选择的是WEP方式，则[安全选项]包括自动选择、开放系统和共享密钥三种方式，如下图。



其中开放系统意味着不需要认证，任何无线客户端都可以接入WIFI网络。共享密钥则需要无线客户端接入的时候输入跟设备配置相符的共享密钥才能接入WIFI网络。

- [加密算法]：用来选择对应的加密算法，包括 AES 和 TKIP 两种，如下图。



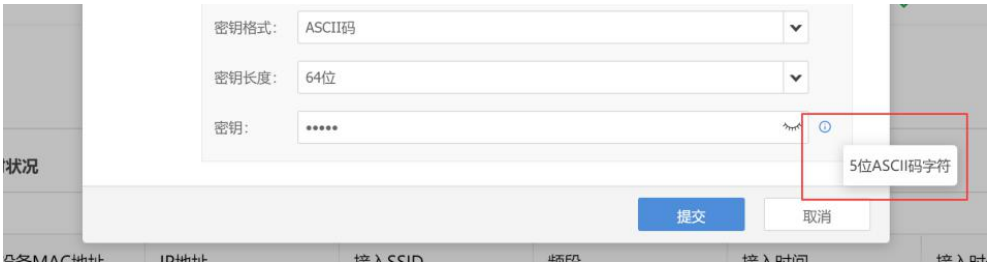
默认为AES算法，TKIP加密算法会导致WIFI 802.11n工作在较低的传输速率，因此除非无线终端不支持AES算法，否则建议使用默认的AES算法。

- [PSK 密码]：用来设置 WIFI 网络密码，无线终端接入 WIFI 网络时需要输入正确的密码才能接入 WIFI 网络，如下图。

如果安全类型选择为WEP方式，则没有加密算法和PSK密码设置选项，而是密钥格式、密钥长度及密钥选项，如下图。

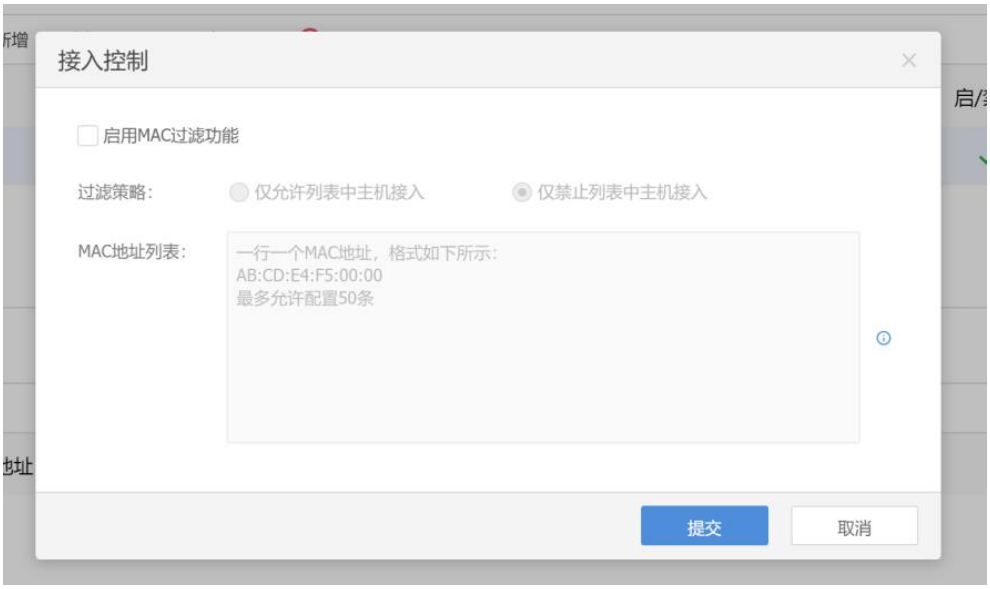
- [密钥格式]：用来设置 WEP 加密的密钥格式，包括 ASCII 码和十六进制两种方式，密钥长度包括 64 位和 128 位两种，如下图。

- [密钥]：用来设置 WEP 方式的密钥，ASCII 码情况下长度为 5-13 个字符，十六进制情况下长度为 10-26 个十六进制字符，如下图。



3. 点击<提交>，保存WIFI设置。

4. 点击<接入控制>，可对无线用户接入进行限制，如下图。

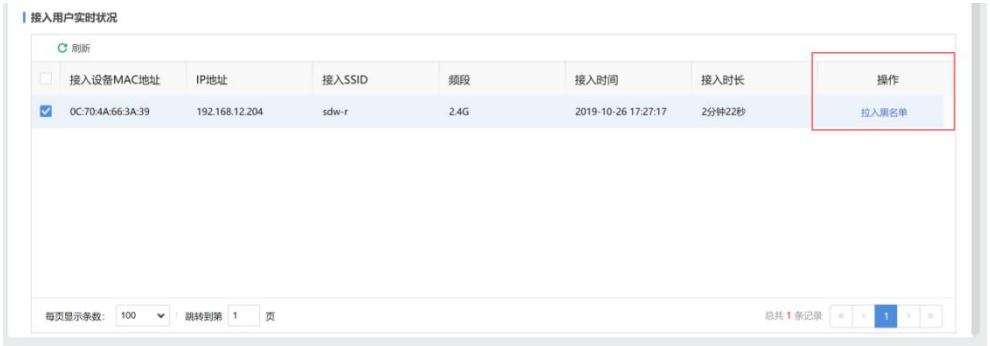


5. 勾选启用MAC过滤功能。

- [过滤策略]：仅允许列表中主机接入：只允许 MAC 地址列表中的主机进行接入、不在列表中的主机无法接入无线网络，用于做白名单；仅禁止列表中主机接入：只禁止 MAC 地址列表中的主机接入无线网络，用于做黑名单。

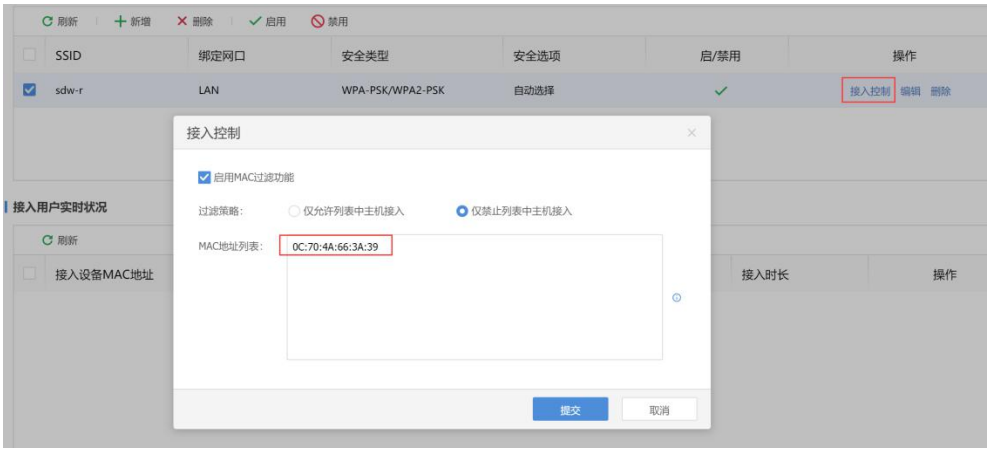
3.5.3.3. 接入用户实时状况

1. [接入用户实时状况]页面详情如下图所示。



2. 点击<拉入黑名单>，可以将非法接入无线网络的用户进行加入黑名单处理，提高安全性。如下图所示。

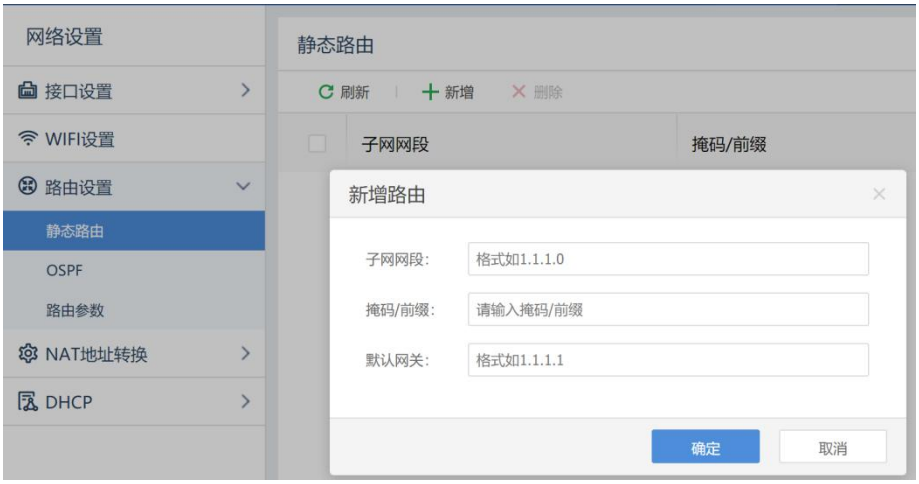
3. 点击<是>，即可将对应的用户加入黑名单，加入黑名单之后，可以在对应的SSID名称的接入控制中查看到对应的黑名单信息。



3.5.4. 路由设置

3.5.4.1. 静态路由设置

用于设置SDW-R设备的静态路由，[静态路由设置]页面详情为下图所示。



1. 点击<新增>进行静态路由设置，需要填写相应的子网网段、掩码或者掩码前缀、默认网关，配置完成点击<提交>，即可完成配置。

2. 点击相应的路由选项，可以进行编辑和删除操作。

3.5.4.2. OSPF 动态路由设置

OSPF是由IETF组织开发的链路状态路由协议，是目前比较常见的内网动态路由协议，若客户内部网络使用OSPF协议时进行OSPF相关配置即可。在OSPF配置界面勾选[启用OSPF服务]来开启设备的OSPF服务。

全局配置

用于设置OSPF的路由器ID、发布区域内网运行网段、路由重分发相关配置内容。

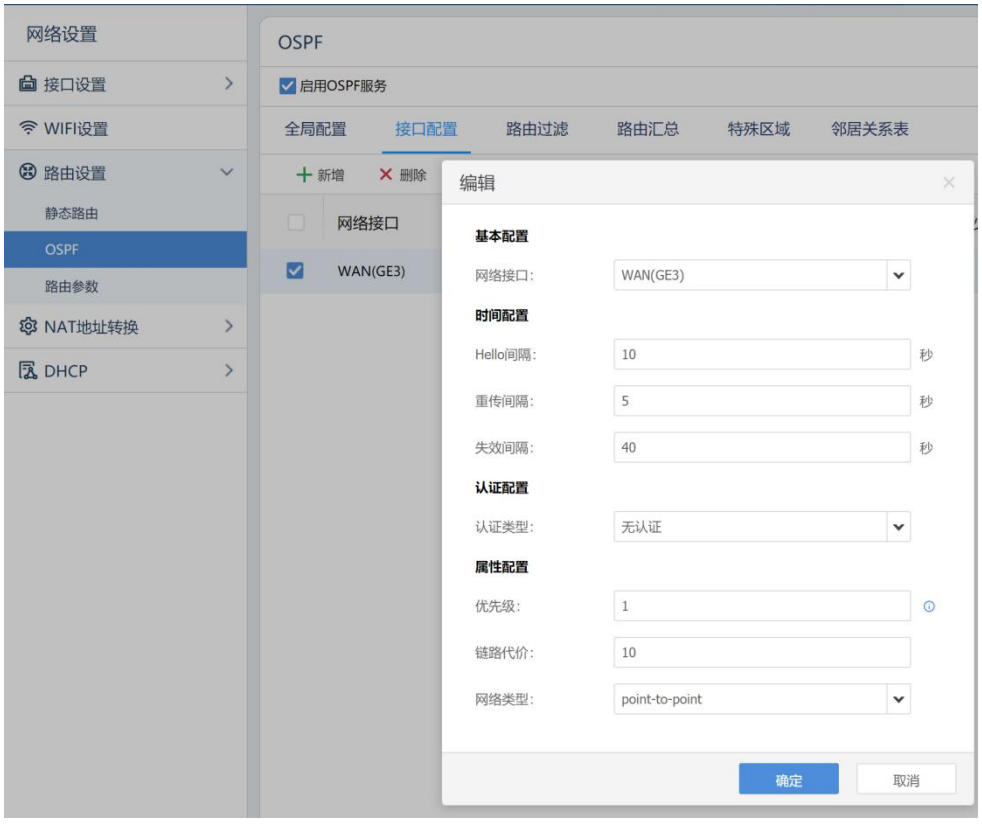
各配置项说明：

- [路由器 ID]：用于作为路由器（网关设备）的唯一标识，可以用于 DR、BDR 选举。

- [区域配置]：设备内网所运行的网段，需要通告对端设备的网段，设置运行网段的区域 ID。
- [区域 ID]：标识协议中各个区域，区域 0 默认表示骨干区域。
- 点击<高级设置>可查看到路由重分发配置。
- 通过勾选相应<启用>可将非 OSPF 协议路由（直连路由、默认路由、静态路由、BGP 路由）重分布进入到 OSPF 区域中，让区域中路由器学习到相关的路由。
- [Metric-type]为：OSPF 引入外部路由时，其他路由器计算到达外部路由的花费的一个概念，默认是 type2 的。
- [度量值]：设置路由的 cost 值。

接口配置

用于设置OSPF接口相关的配置，主要包括OSPF关联的网络接口、hello包时间间隔、重传间隔、失效间隔、接口认证、网络类型的配置。



各配置项说明：

- [网络接口]：选择相应的网络接口。
- [hello 间隔]：修改 OSPF 发送 hello 包的时间间隔，其中该时间间隔数值与失效间隔数值、认证类型需要总部和分支保持一致，否则邻居关系无法建立。
- [重传间隔]：OSPF 的 hello 包进行重新传送的时间间隔。
- [失效间隔]：OSPF 的 hello 包在该时间内没有被响应，则视为对端无邻居。
- [认证类型]：OSPF 邻居之间可选择认证方式：无认证、明文认证、MD5 认证。

- [优先级]：用于 OSPF 的 DR 与 BDR 的选举。
- [链路代价]：链路的开销值。
- [网络类型]：可选择 OSPF 协议的网络类型为：广播类型还是点对点类型。

路由过滤

用于设置OSPF模块的路由过滤规则，可设置分发列表过滤或者3类LSA过滤两种方式，分发列表过滤用于过滤通过重分发的方式进OSPF中的路由表项。配置如下图所示。

分发列表过滤点击<新增>时，各配置项说明如下：

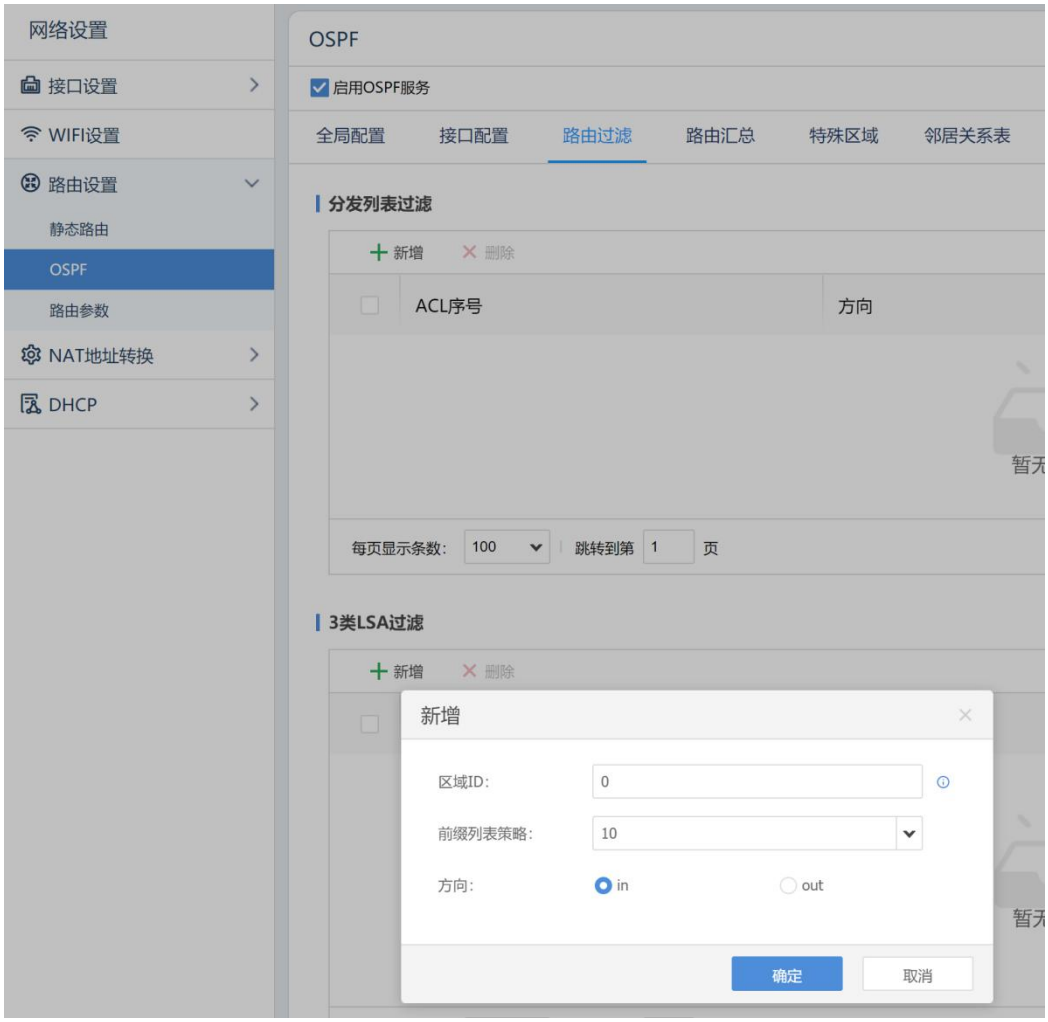
- [ACL 序号]：支持选择[路由参数]中配置的 ACL 访问列表，即具体的路由过滤对象；
- [路由类型]：可选择 VPN、Direct、static 三种类型，即对重分发的 VPN、直连、静态的路由做过滤；
- [方向]：当前只可选择 out 方向。

该规则的整体含义为：在该SDW-R上重分发直连路由进入OSPF后，用out方向（数据发送方向）的分发列表可过滤掉ACL序号10中的网段。例如：在SDW-R1通过直连路由重分发将192.168.1.0，192.168.2.0，192.168.3.0引入OSPF，SDW-R1上设置了out方向的分发列表过滤，out方向的分发列表过滤内容为过滤掉ACL序号10中192.168.3.0网段。那么此时SDW-R1的下游路由器SDW-R2就无法接收到192.168.3.0网段的路由。

⚠ 注意：

分发列表过滤中的方向目前只支持 out 方向的过滤，不支持 in 方向的过滤。

3类LSA过滤用于过滤某一区域的3类LSA进入到其它区域，配置如下图所示。



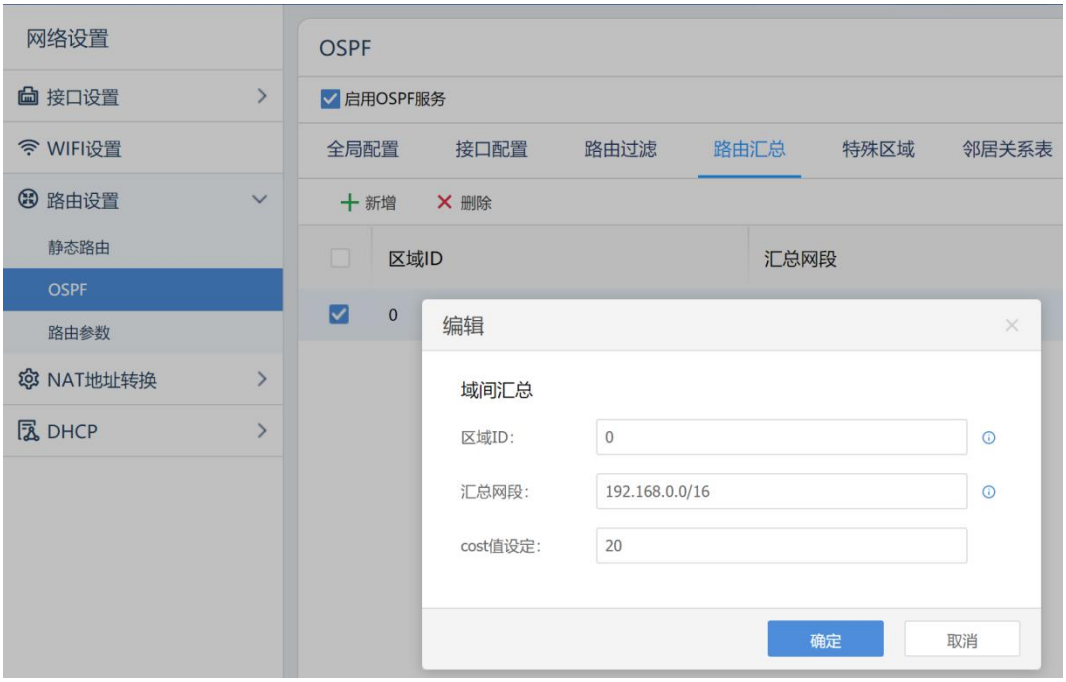
3类LSA列表过滤点击<新增>时，各配置项说明如下：

- [区域 ID]：设置对应的区域 ID 号，即路由过滤策略生效的区域；
- [前缀列表策略]：选择关联对应的前缀列表策略，即需要过滤的网段；
- [方向]：选择过滤策略是从数据的接收方向（in 方向）还是数据的发送方向（out 方向）

该规则的整体含义为：在SDW-R（该SDW-R为ABR时）上由其它区域进入区域0的LSA，进行前缀列表策略10中的网段过滤。

路由汇总

用于区域间路由汇总，详情配置界面如下图所示。



各配置项说明如下：

- [区域 ID]：设置对应的区域 ID 号，即路由汇总策略生效的区域；
- [汇总网段]：设置需要汇总的网段；
- [cost 值设定]：设置汇总后网段路由的 cost 值。

特殊区域

用于OSPF的特殊区域设置，主要可以设置stub、完全stub、两种特殊区域的设置。详细配置界面如下图所示。

各配置项说明如下：

- [区域 ID]：设置响应的区域 ID；

- [stub 域]：设置该区域为 stub 域，stub 区域的具体含义为：不允许发布自治系统外部路由，只允许发布区域内路由和区域间路由。在 stub 区域中，路由器的路由表规模和路由信息传递的数量都会大大减少。为了保证到自治系统外的路由可达，由该区域的 ABR 发布 Type3 缺省路由传播到区域内，所有到自治系统外部的路由都必须通过 ABR 才能发布；
- [完全 stub 域]：勾选 no-summary 时，该区域就成为完全 stub 区域，该区域内不允许发布自治系统外部路由和区域间的路由，只允许发布区域内路由。在完全 stub 区域中，路由器的路由表规模和路由信息传递的数量都会大大减少。为了保证到自治系统外的路由可达，由该区域的 ABR 发布 Type3 缺省路由传播到区域内，所有到自治系统外部的路由都必须通过 ABR 才能发布；

邻居关系表

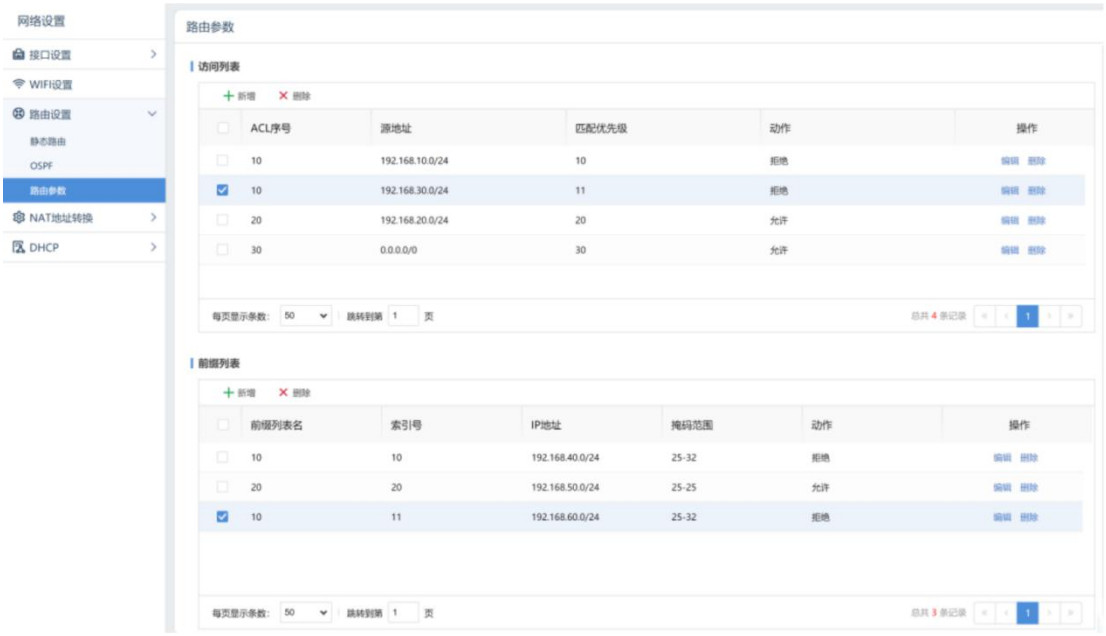
用于查看OSPF邻居关系信息，界面详情如下图所示。

各配置项说明如下：

- [邻居路由器 ID]：查看相应的邻居路由器 ID；
- [优先级]：查看邻居路由器的优先级；
- [邻接状态]：查看与邻居的邻接状态与 DR/BDR 的信息；
- [超时时间]：查看邻居 hello 包发送检测时间，当超时时间超过失效间隔时认为该邻居已经失效；
- [邻居邻接 IP]：查看邻接邻接的 IP 地址；
- [邻接网口]：查看邻居的邻接网口信息。

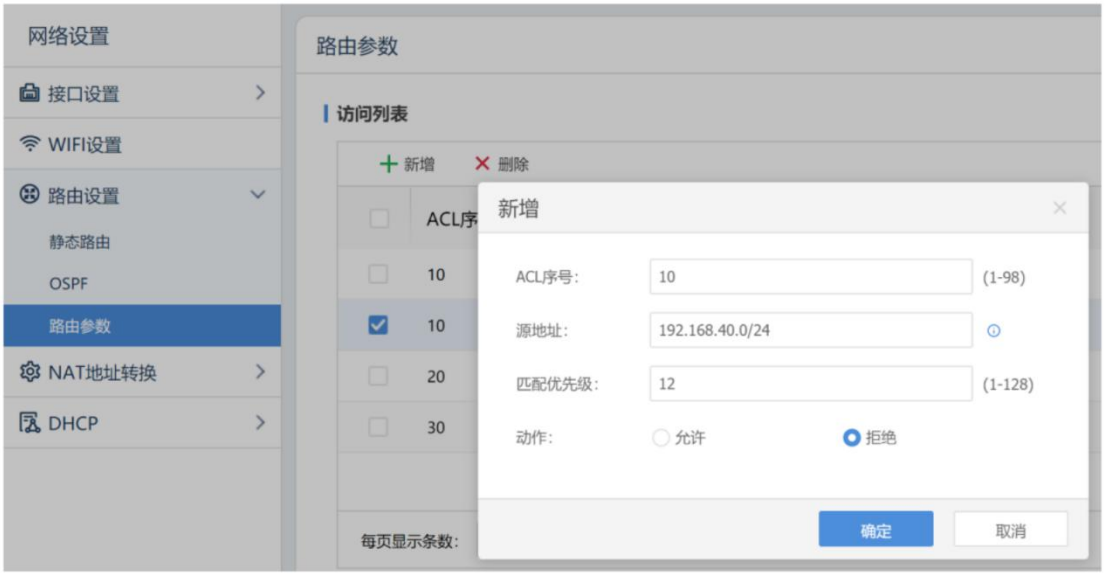
3.5.4.3. 路由参数设置

用于设置OSPF路由过滤规则中的ACL访问列表和前缀列表，详情配置界面如下图所示。



ACL访问列表

用于设置ACLf访问列表，详情配置界面如下图所示。

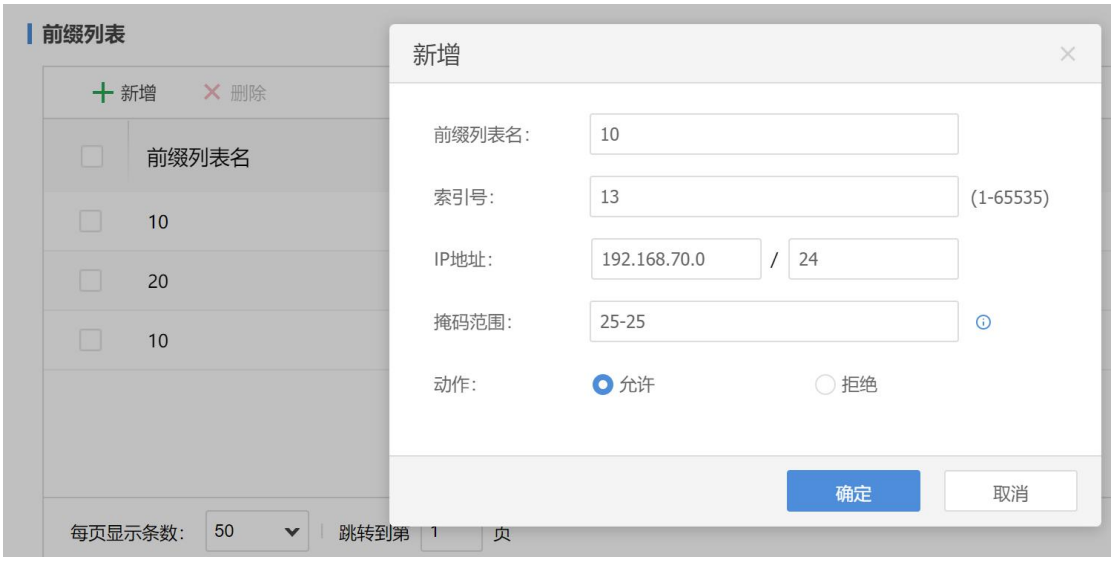


各配置项说明如下：

- [ACL 序号]：设置对应的 ACL序号，多个 ACL 规则可设置同一个 ACL 序号；
- [源地址]：设置 ACL 规则中的源 IP 地址，可设置单个 IP 地址或者 IP 网段；
- [匹配优先级]：设置 ACL 规则的匹配优先级；
- [动作]：设置 ACL 规则匹配之后的动作，是允许还是拒绝。

前缀列表

用于设置OSPF中3类LSA过滤时所关联的前缀列表的设置，配置界面如下图所示。



各配置项说明如下：

- [前缀列表名]：设置对应的前缀列表名，多个前缀列表规则可设置同一个前缀列表名；
- [索引号]：设置前缀列表的优先级；
- [IP 地址]：用于设置前缀列表的 IP 地址段；
- [掩码范围]：用于设置 IP 地址中的掩码范围，可用于匹配某个大网段中的小网段。比如：上面策略的 IP 地址和掩码长度为 192.168.70.0/24，掩码范围填写 25-25 时，它表明网段 192.168.70.0 的前 24 位必须匹配，同时子网掩码还需要在 25 位。

3.5.5. NAT 地址转换

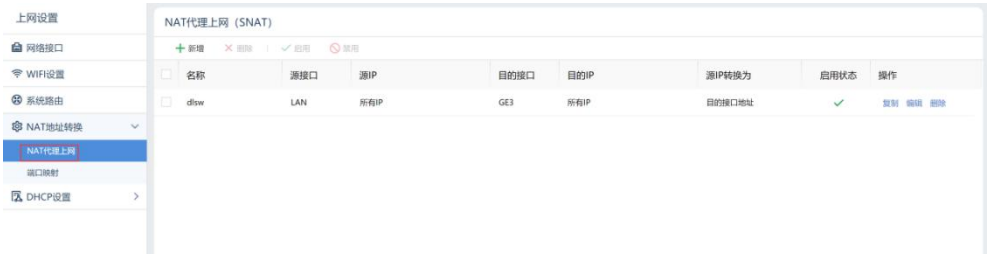
NAT地址转换包括[NAT代理上网]、[端口映射]模块。

3.5.5.1. NAT 代理上网

[NAT代理上网]即内网地址向外访问时，发起访问的内网IP地址转换成指定的IP地址。

典型场景

用于设置代理局域网上网的规则，SDW-R硬件网关不仅通过[NAT代理上网]的NAT代理上网功能，还可通过与过滤规则进行配合对内网的上网服务进行控制，在页面中的SNAT设置中可以看到有[名称]、[源接口]、[源IP]、[目的接口]、[目的IP]、[源IP转化为]、[启用状态]、[操作]等配置信息，如下图所示。



1. 设备缺省设置中不包含SNAT规则设置，需要云端易部署或者手动添加，点击<新增>，页面如下所示。

各配置项说明：

- [名称]：用于自定义规则名称。
- [启用状态]：选择启用或者禁用该规则。
- [原始数据包/源接口/源 IP]：源接口用于设置数据包的源接口地址，表示从该接入过来的数据包会继续往下匹配，可以选择 LAN、DMZ、VPN 三种。勾选代理本区域所有网段可以代理选择区域的所有网段，或者在源 IP 处写上指定的源 IP 网段。
- [目的接口]：目的接口用于设置数据包的出接口，可选择 WAN，VPN 两种。

- [目的接口线路]：目的接口线路用于设置数据的出接口所选择的线路，表示数据从出接口中的那一条线路出去，可选择 ALL、或者出口线路中一条。
- [目的 IP]：目的 IP 表示原来数据包的目的 IP 在设置的范围内，则继续往下匹配。
- [转换后数据包/将源 IP 转换为]：用于设置符合指定条件的数据包转换源地址为“目的接口 IP”或者“指定 IP”。选择目的接口 IP，则会将数据包源地址转换为“目的接口”选择的接口 IP 地址。选择“指定地址”则需要手动设置一个 IP 地址。

2. 配置完成，点击<提交>，即可完成SNAT规则的配置。

常用代理上网设置示例一

某客户出口是一台SDW-R设备，WAN口为ADSL拨号，LAN口地址IP地址为192.168.0.1，内网PC都是192.168.0.0/24网段，网关指向192.168.0.1。部署SDW-R设备后，需要保证内网PC可以访问公网。

操作步骤

1. 配置设备接口IP地址，IP地址配置请参考“网络接口设置”章节，此处不赘述。
2. 配置代理上网，源接口选择LAN，子网网段填写LAN口网段，出接口为上公网的WAN口，目的IP地址为所有IP地址，将源地址转换为WAN口IP，界面如下图。

常用代理上网设置示例二

某客户总与分支用SANGFOR VPN对接，连上了VPN隧道，总部与分支使用SDW-R设备，分支内网网段为192.168.0.0/24。客户希望分支的用户全部通过总部上网，而不通过分支的网络上网。

操作步骤

1. 在分支端的SDW-R设备配置隧道间路由，并且勾选“通过中转路由分支上网”，详情请参考“隧道间路由设置”章节。
2. 在总部端的SDW-R设备配置代理上网规则，源接口选择VPN接口（因为是从VPN对端过来的数据），源地址填写192.168.0.0/24，目的接入选择WAN，界面如下

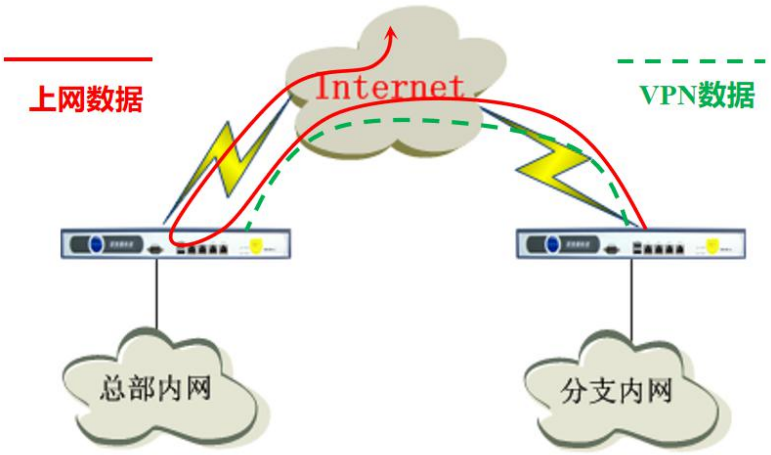
图。

📖 **说明：**

关于源接口选择 VPN 的高级应用场景及案例请参考下面“案例学习”。

案例学习

总部SANGFOR 设备采用网关模式部署，分支（172.16.10.0/24）需要通过VPN接入总部后上网，拓扑图如下图。



操作步骤

1. 在VPN正常连接的情况下，分支SANGFOR设备需要添加隧道间路由（详见“隧道间路由设置 ”小节）。
2. 总部SANGFOR设备需添加[内网接口]为VPN的代理规则并添加分支的内网网段，页面如下图。

3. 防火墙规则是会自动放通，无需手动去放通。点击[防火墙/过滤规则设置/高级设置]，可以看到数据包不在过滤规则列表中时，默认执行允许动作，页面如下图。

3.5.5.2. 端口映射

[端口映射]用于设置SDW-R网关设备的端口映射规则，如果局域网内的服务器需要向外网提供服务，则需要添加[端口映射]，在DNAT设置页面中可以看到有[名称]、[源接口]、[源IP]、[目的IP]、[目的端口]、[协议]、[目的IP转换为]、[目的端口转换为]、[启

用状态]、[操作]等配置信息，如下图。

点击<新增>，用来增加一条DNAT规则，页面如下图。

各配置项说明：

- [名称]：用于自定义规则名称。
- [启用状态]：选择启用则规则生效，防火墙会自动对应过滤规则。
- [原始数据包/源接口/源接口线路/源 IP]：源接口用于设置数据包的源接口地址，表示从该接口进来的数据会继续往下匹配，可以选择 LAN、DMZ、WAN 三种；选择 WAN 口在双线路情况下还需要选择对应的线路；源 IP 选择所有 IP 或者自定义 IP 网段/掩码，该源 IP 用于设置源地址匹配条件，表示数据包的源 IP 地址在设置的范围内，则可以往下匹配。
- [目的 IP/转换协议/目的端口]：用于设置转换条件。
  目的 IP：表示数据包的目的 IP 符合设定的条件，则继续往下匹配；
  转换协议：表示数据包所使用的协议符合设定的条件，则继续往下匹配；
  目的端口：表示数据包的目的端口符合设定的条件，则继续往下匹配。
- [转换后数据包/目的 IP/目的端口]：用于设置转换的数据包目的 IP、端口，表示符合上述所有条件的数据包，将该数据包的目的地址和目的端口转换成设置的值。

端口映射设置示例

某客户出口部署SDW-R ，一条电信线路接到设备的线路1，WAN口IP地址为202.96.137.75，LAN口IP地址为192.168.0.1，内网有一台WEB服务器（80端口提供服务）IP地址为192.168.0.100，现在客户希望公网的用户也能访问到192.168.1.100这台服务器。

操作步骤

1. 基础网络配置，配置接口IP地址信息，请参考“网络接口配置”章节，此处不赘述。
2. 配置端口映射，本案例中的配置信息如图所示。

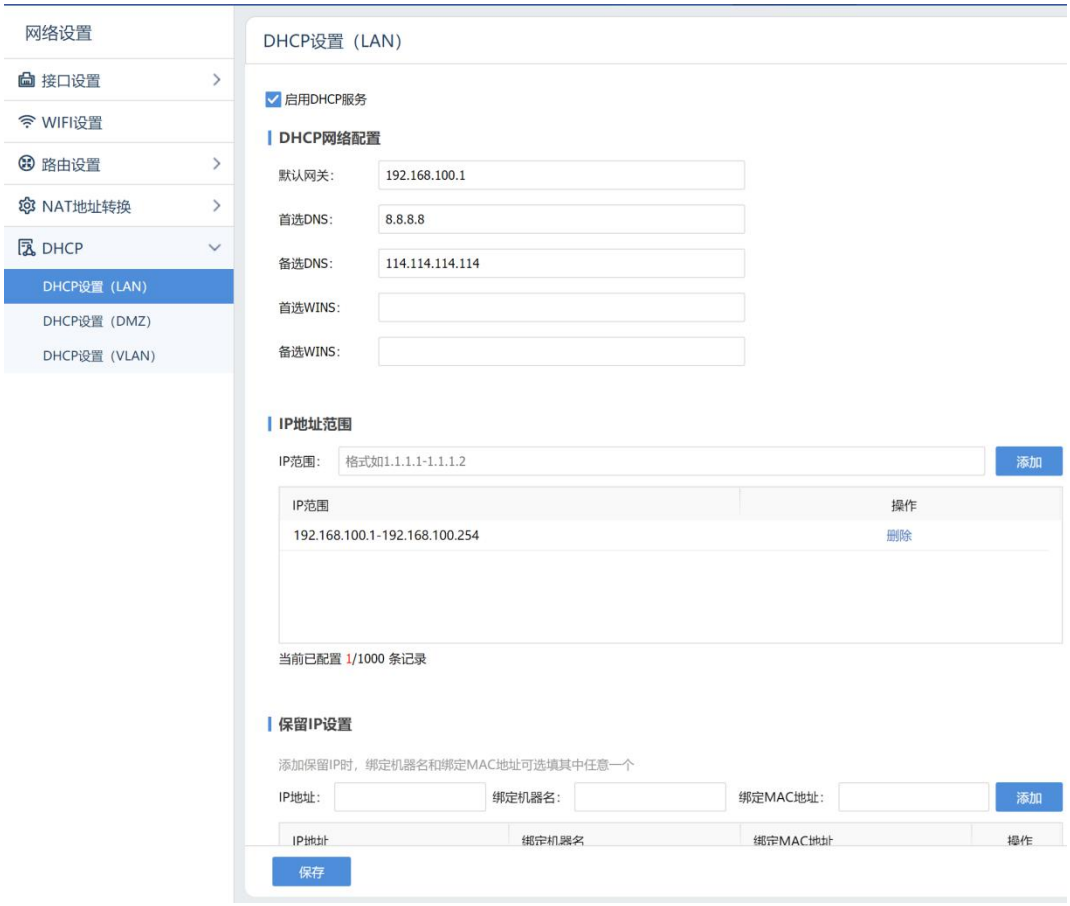
注意：

通过 SANGFOR VPN 硬件设备设置端口映射向外网提供服务的内网服务器，必须是以 VPN 硬件设备作为 NAT 代理上网（网关指向 VPN 或上网路由最终指向 VPN），否则端口映射将无法生效。

3.5.6. DHCP 设置

3.5.6.1. DHCP 设置（LAN）

1. DHCP设置主要用于设置DHCP服务的一些参数，页面如下图所示。



2. 勾选LAN口启用DHCP服务（同时启用在WLAN上），才可进行DHCP相应的配置。

3. 在[DHCP网络配置]中设置适当的网关IP和有效的DNS服务器IP，一般情况下[默认网关]填写的是SDW-R设备的“LAN口IP”，[DNS]则填写当地ISP所提供的DNS服务器IP。[WINS]服务器可根据自己的具体应用判断是否需要填写。

4. [IP地址范围]：在IP范围对话框中输入起始IP-结束IP，可以设定DHCP所分配的IP地址范围。输入完成后，点击<添加>后，在页面底部点击<更新>，即可保存配置。

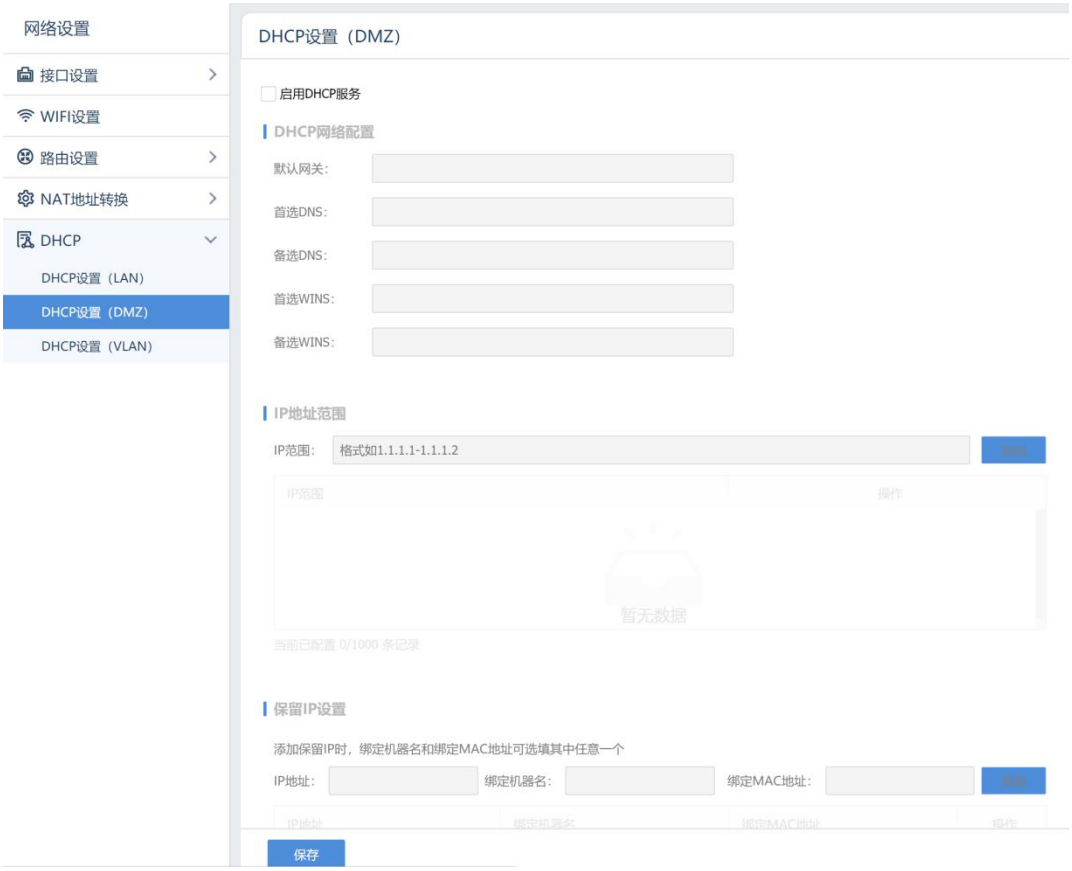
5. [保留IP设置]：用于设置为某些计算机保留分配固定的IP，IP地址填写需要保留分配给该用户的特定内网IP；DHCP保留的条件可以根据用户电脑的“MAC地址”或者“机器名”来绑定，填写绑定机器名、绑定MAC地址的两种方式中选择一种即可，配置完成后，点击<添加>后，在页面底部点击<更新>，即可保存配置。

6. [高级]：选项用于设置DHCP的租约时间，可自行修改，默认为120分钟。

7. 所有配置完成之后，需要点击<更新>才可保存配置。

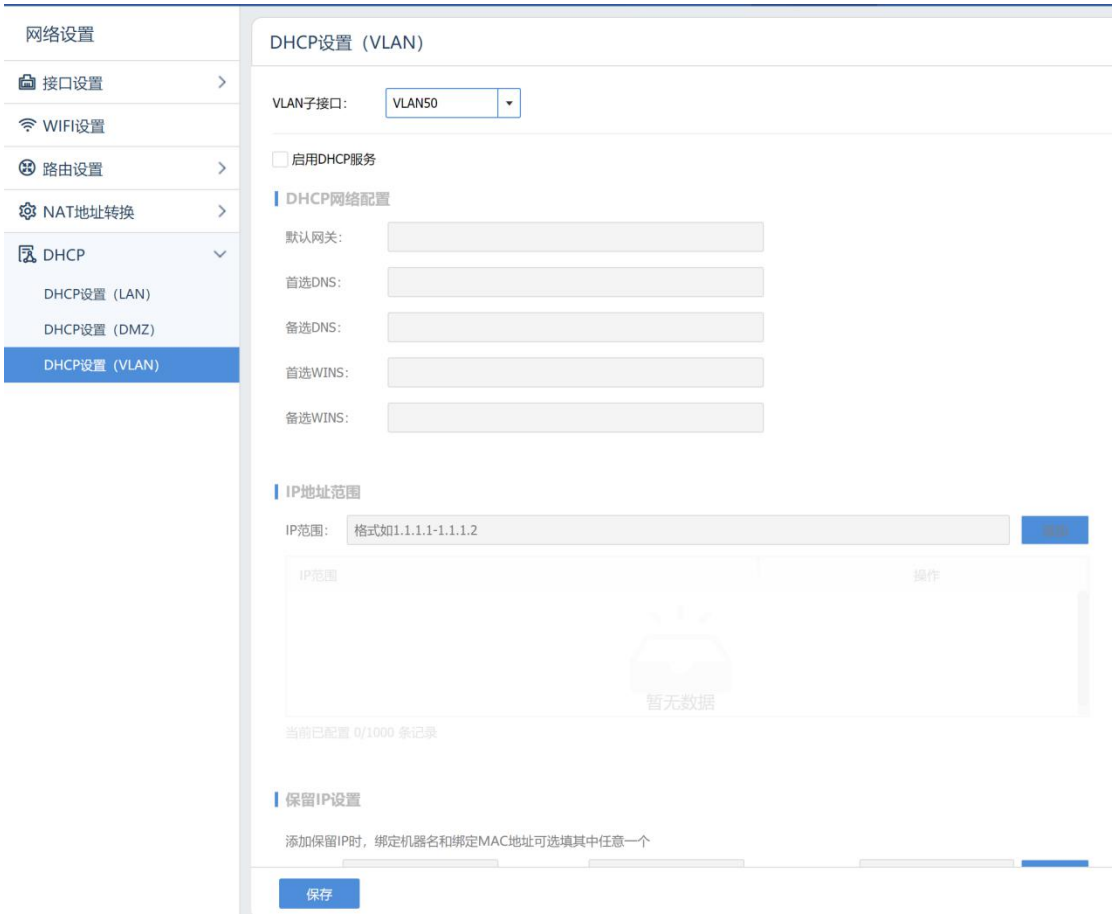
3.5.6.2. DHCP 设置（DMZ）

DHCP设置（DMZ）相应与DHCP设置（LAN）章节相似，区别在于默认网关处需要填写DMZ口的IP，如下图所示。



3.5.6.3. DHCP 设置（VLAN）

DHCP设置（VLAN）相应与DHCP设置（LAN）章节相似，区别在于默认网关处需要填写VLAN口的IP，需要选择DHCP生效时对应的VLAN子接口如下图所示。



3.6. 系统

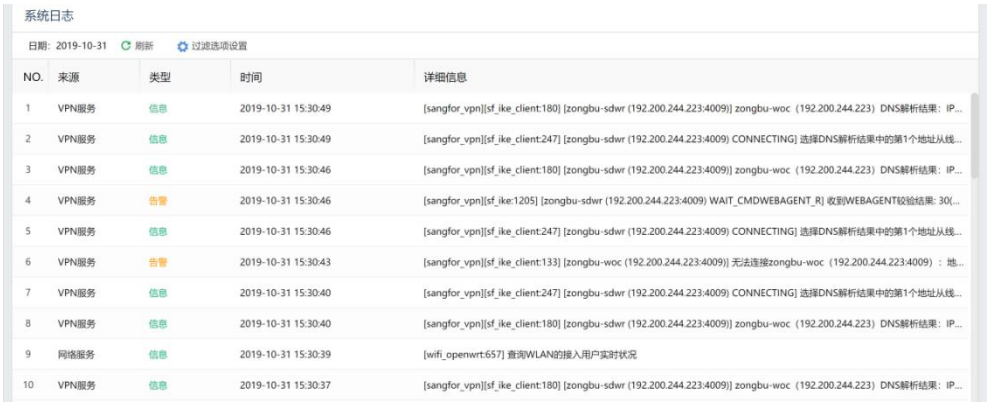
系统包括[系统诊断]、[接入用户管理]、[加入集中管理]、[管理员账号]、[系统配置]模块，如下图所示。

3.6.1. 系统诊断

系统诊断包括[系统日志]、[操作日志]、[排障]、[重启操作]功能配置，如下图所示。

3.6.1.1. 系统日志

[系统日志]可以查看当前设备的系统日志信息，选择要查看的日期，会显示相应时间下的日志记录，页面如下图。



点击<过滤选项设置>时， 可以设置指定查看系统日志范围，页面如下。

3.6.1.2. 操作日志

[操作日志]可以查看当前设备管理员对设备进行的操作日志信息，选择要查看的日期，会显示相应时间下的日志记录，页面如下图。

点击<过滤选项设置>，可以设置指定查看操作日志范围，页面如下图。

3.6.1.3. 排障

可在排障中开启数据直通与启用故障排查日志，数据直通可设置全局放通与局部放通，

全局放通时可设置数据是否经过流控，用于排查是否为流控策略的影响。

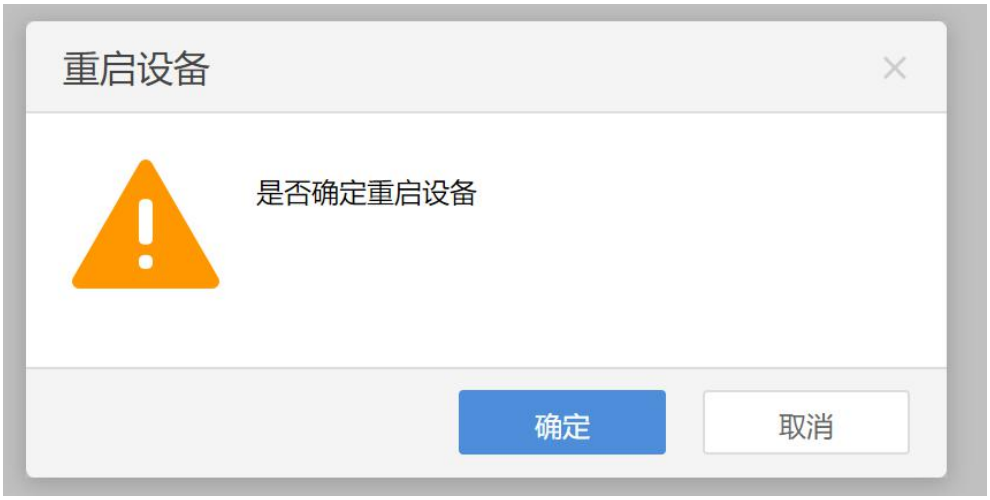
局部放通可设置相关的IP地址与协议类型。

一般数据直通与启用故障排查日志配合使用，当开启数据直通时可优先保障网络的联通性；然后再开启故障排查日志检查是由于那条应用控制策略拦截的数据，根据故障排查日志显示的内容对应用控制策略进行调整。如下图所示：

3.6.1.4. 重启操作

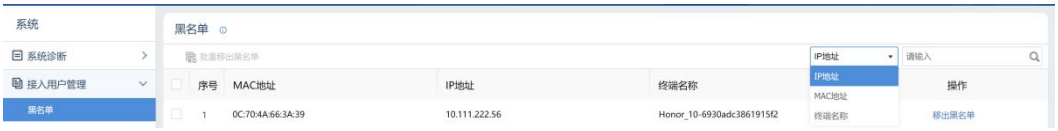
1. 控制台界面进行设备重启操作，注意该操作可能会到内网设备断网，请谨慎操作。

2. 点击<重启设备>时，会提示是否确定重启设备。

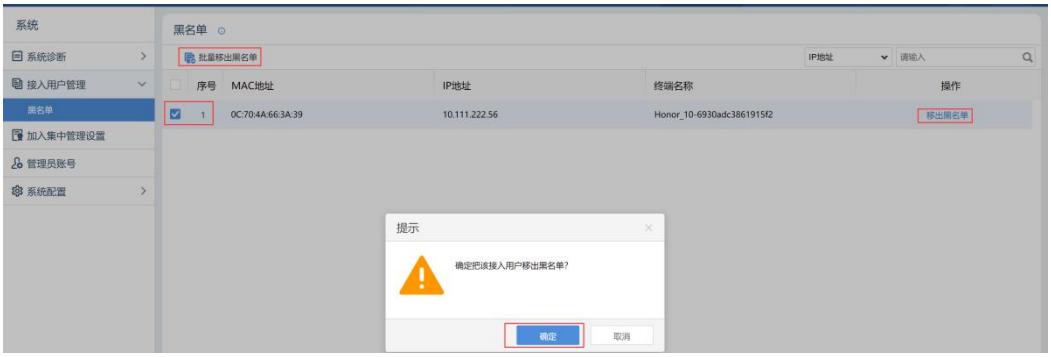


3.6.2. 接入用户管理

可以查看与管理被管理员移入黑名单的接入用户，可根据IP地址、MAC地址、终端名称来搜索对应的用户名称。



管理员可进行移出黑名单的操作，选择对应的用户，针对单个用户移出黑名单、也可选择多个应用进行批量移出黑名单。确定之后，该用户的网络连接即可恢复正常。



3.6.3. 加入集中管理设置

[加入集中管理]可以配置接入BBC，达到分支业务由BBC中心进行管控。加入BBC之后，部分模块无法在SDW-R段配置，这些模块都由BBC管控设置。页面如下图。

各配置项说明：

- [中心端接入地址]：填写 BBC 的 IP 加端口。
- [接入设备名称]：填写 BBC 上配置的分支设备的这个名称。
- [接入密码]：填写 BBC 上配置的接入密码。
- [共享密钥]：填写在 BBC 上门配置的共享密钥，如果 BBC 未配置，SDW-R 端也不用配置。
- [测试有效性]：点击可测试与 BBC 中心端接入地址是否格式有误。

点击<更新>，保存配置。

- [解除集中管理]：点击可以退出 BBC 管理，解除的密码是在总部 BBC 上配置的密码。

⚠ 注意：

加入 BBC 集中管理后，设备上部分配置需从 BBC 中心端统一下发，本机将不可配置。加入 BBC 会重启 SDW-R 所有服务，请在业务空闲时期操作，避免业务影响。

3.6.3.1. BBC 配置下发

SDW-R分支接入BBC后，可以在BBC中心端统一配置策略模板，批量下发给SDW-R受控端。可以下发[系统设置/对象设置]，[防火墙/过滤规则设置]等。BBC处对SDW-R下发配置的界面如图。

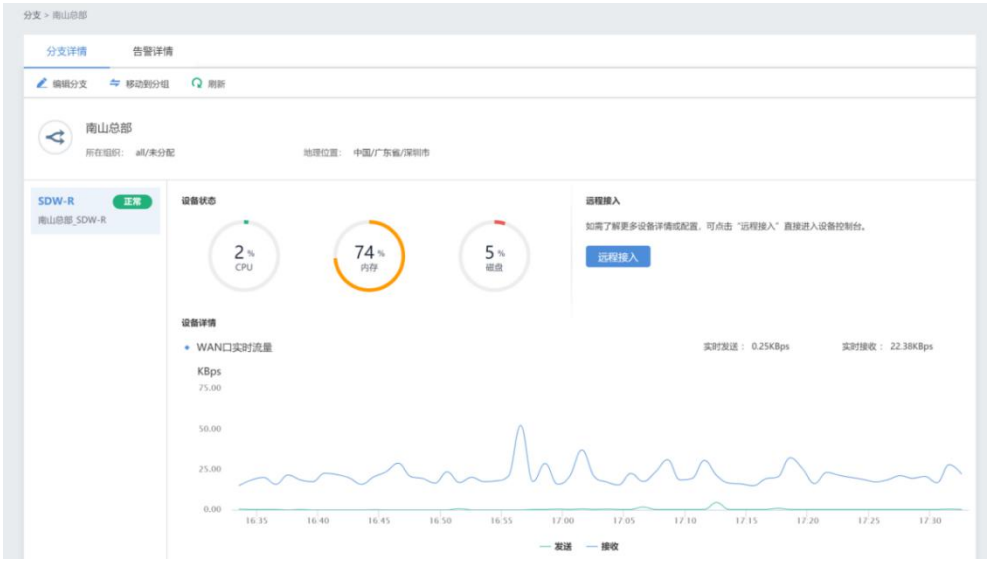
3.6.3.2. BBC 查看设备使用状态和状态告警

SDW-R接入BBC后，可以在BBC中心端看到设备使用状态以及状态告警，支持内容如下：

1. 支持CPU、内存、磁盘设置告警阈值，超过阈值后会产生告警。
2. 支持VPN离线和VPN授权不足告警。
3. 支持SDW-R带宽利用率超过阈值、出现错误日志、出现告警日志时告警。

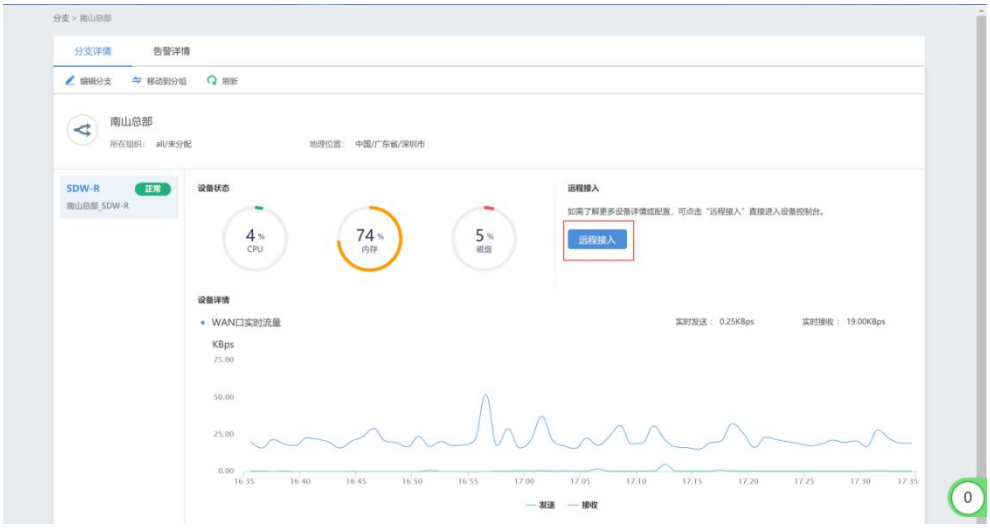
3.6.3.3. 系统状态上报给 BBC

SDW-R加入BBC后，可以在BBC分支详情查看SDW-R受控端的CPU、内存、磁盘使用率，另外也支持查看分支最近一小时流速，如下图。



3.6.3.4. 从 BBC 单点登录到 SDW-R

通过[分支详情]可免密单点登录到SDW-R设备，也可以通过分支概览网络设备名进行单点登录到SDW-R设备。在BBC页面[设备]选择SDW-R分支，在[分支详情]中点击<远程接入>，即可实现单点登录设备，如下图。



3.6.4. 管理员账号

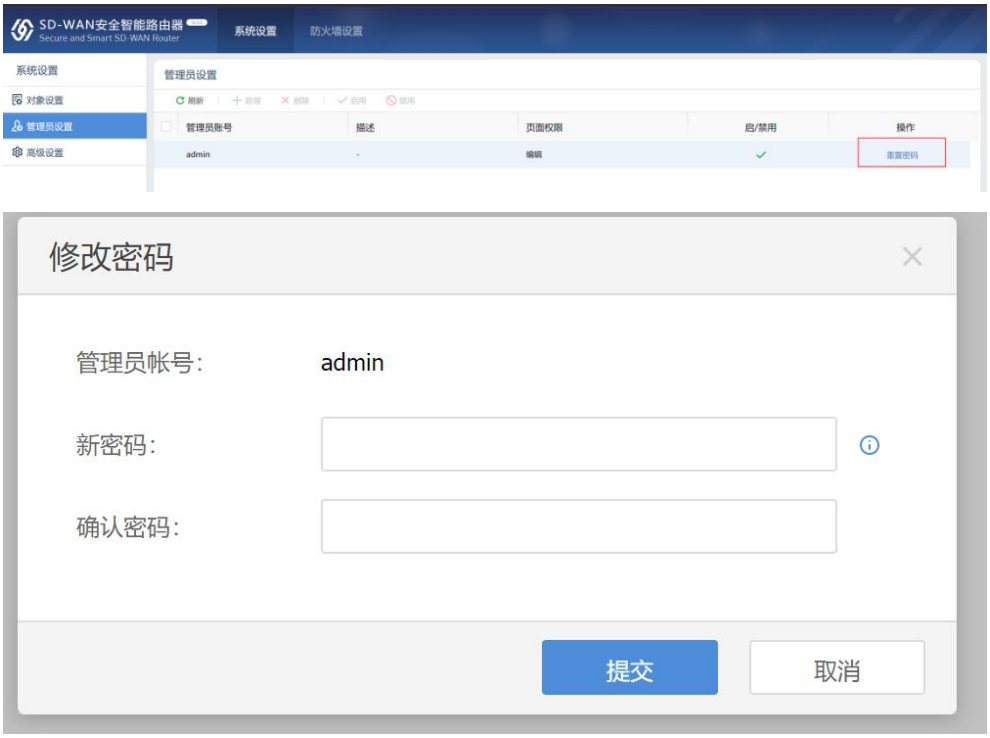
[管理员账号]用于设置可登录网关控制台的管理账号。

1. 点击<新增>弹出新增用户对话框，设置管理员账号、密码、权限，设置界面如下

图。

2. 配置完成之后，点击<提交>即可完成配置。

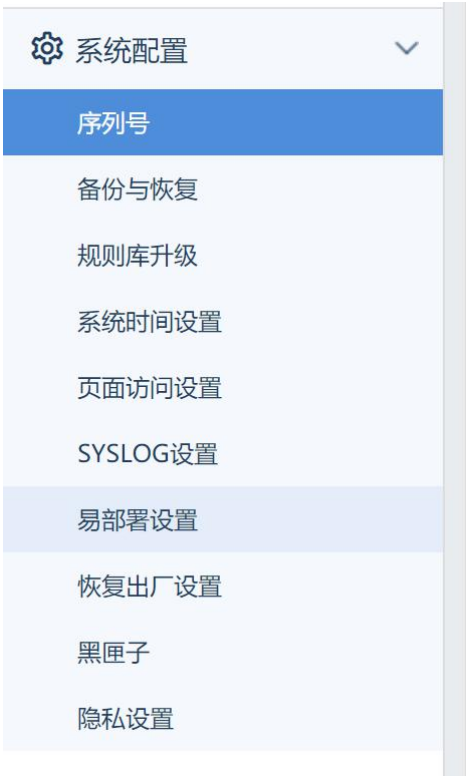
3. 点击<重置密码>时，可以修改管理员账号的密码，如下图。



4. 输入对应的新密码和确认密码，点击<提交>就可完成管理员账号的密码修改。

3.6.5. 系统设置

登录控制台，点击[系统/系统设置]，系统设置包括[序列号]、[备份与恢复]、[规则库升级][系统时间设置]、[页面访问设置]、[SYSLOG设置]、[易部署设置]、[恢复出厂设置]、[黑匣子]、[隐私设置]，相应的页面如下图所示。



3.6.5.1. 序列号

[序列号]用于填写SDW-R设备的授权信息，该授权信息控制SDW-R设备的分支数、外网线路数，不同的序列号对应着不同线路数量和接入分支数，激活授权ID时，这些授权数会自动生成，如下图所示。

各配置项说明：

- [授权 ID]：由深信服提供，用于识别授权信息。点击<更新授权 ID>时，激活步骤如下：

- [网关 ID]：设备的软件标识 ID，出厂默认，不可修改。
- [授权用户]：用户的授权信息。
- [SN 码]：设备的硬件 ID，出厂默认，不可修改。
- [设备版本]：显示设备的当前版本。
- [授权状态]：说明设备是否完成授权，有两种状态一种是“未激活”另一种是“已激活”。
- [激活时间]：显示设备授权激活成功的时间。
- [设备信息文件]：设备硬件信息文件，出厂默认，不可修改。

⚠ 注意：

SDW-R4.0.9 及之后版本新增 SOFAST&BEST 选路序列号，该序列号关联 SDWAN 智能选路功能使用，当该授权过期时 SDWAN 智能选路功能将无法配置并保持默认智能选路策略。

3.6.5.2. 备份与恢复

可下载设备当前的配置信息，保存在本地。

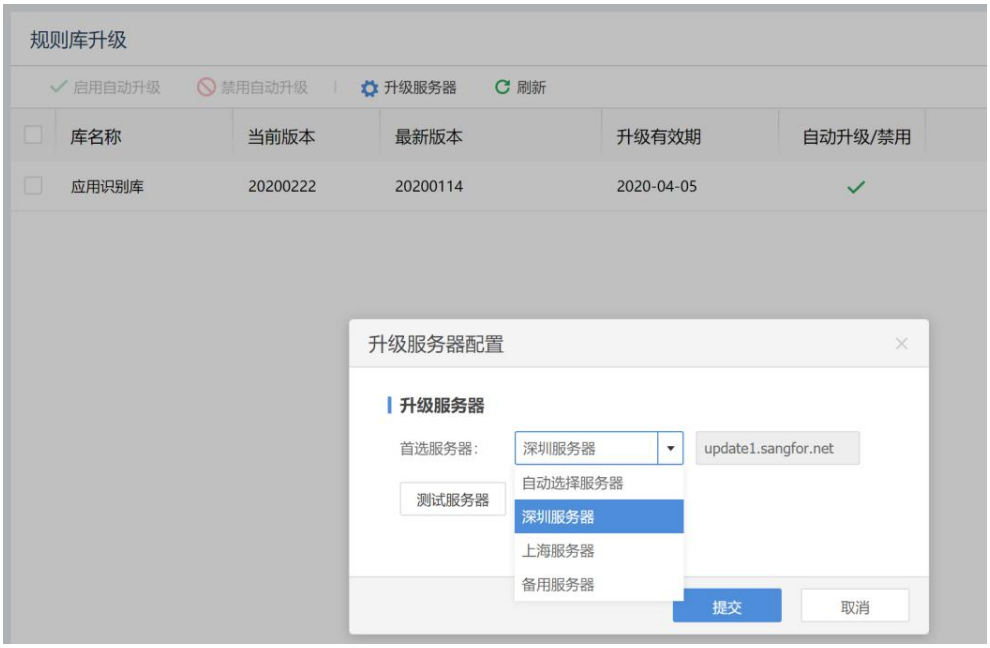
也可以选择本地备份文件进行恢复。

注意：

不同版本设备之间的配置文件不支持恢复。

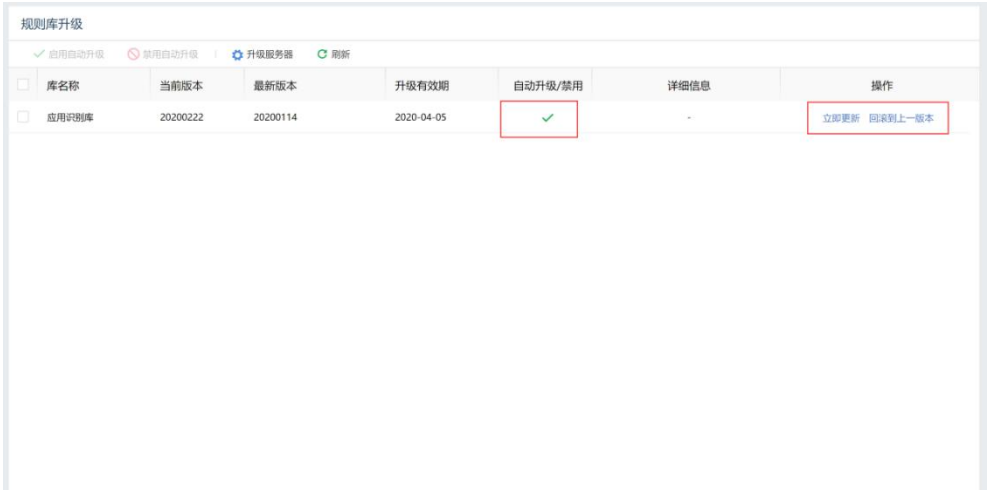
3.6.5.3. 规则库升级

应用识别内置库升级服务器配置，支持手动升级，自动升级，回滚到上一版本。



规则库手动升级

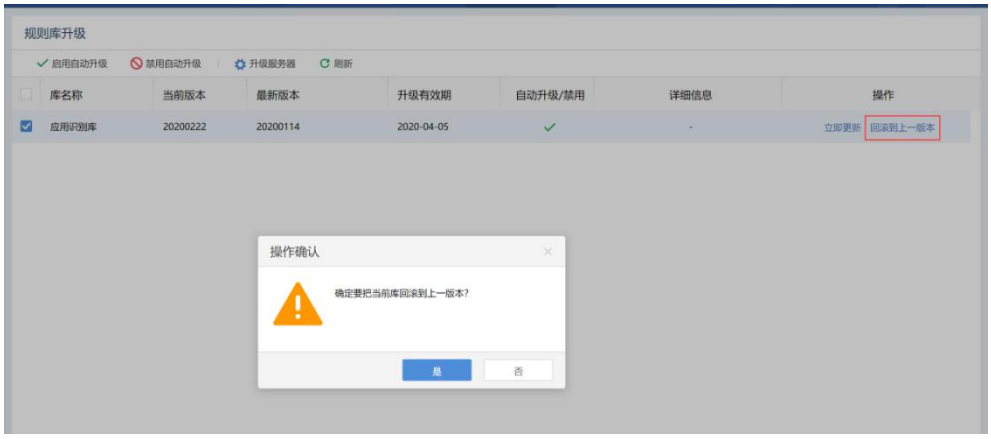
也可进行手动更新，如下图所示。



点击<立即更新>时，需要选择对应的离线版本的内置规则库进行更新。

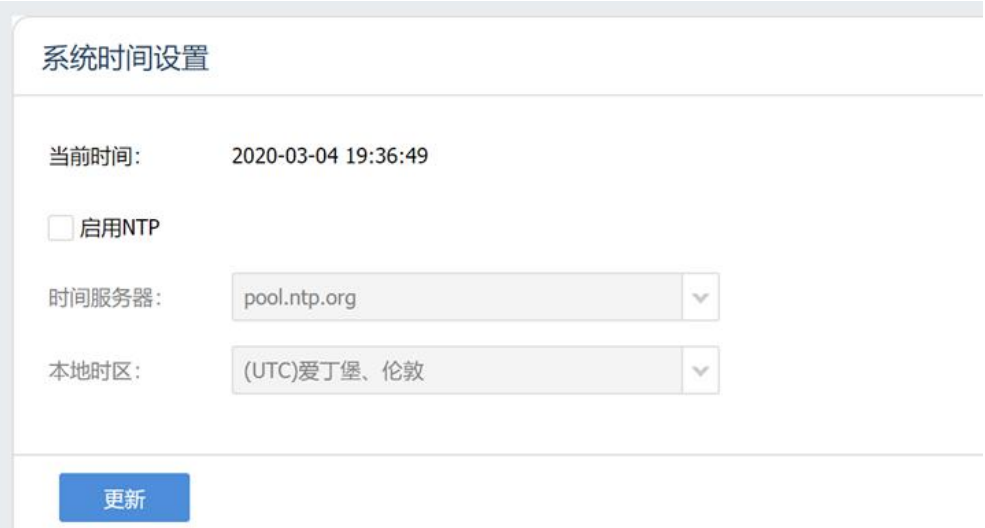
规则库版本回滚

选择回滚到上一版本时，会提示是否回滚到上一版本，如下图。



3.6.5.4. 系统时间设置

[系统时间设置]可以查看设备当前的系统时间，可以勾选[启用NTP]，选择相应的时间服务器，本地时区，点击<更新>即可获取到相应的设备当前时间。



3.6.5.5. 页面访问设置

[页面访问设置]用于设置网关控制台的https服务端口（默认443端口）和用户登录设备控制台的超时时间，如修改了服务端口，下次登录需通过修改后的端口登录网关控制台，页面如下图。

3.6.5.6. SYSLOG 设置

SYSLOG设置用于设置syslog服务器的IP地址和端口号，可以把SDW-R设备产生的上网行为记录日志和管理员日志以及系统日志发送到其他第三方的syslog服务器上，页面如下图。

各配置项说明：

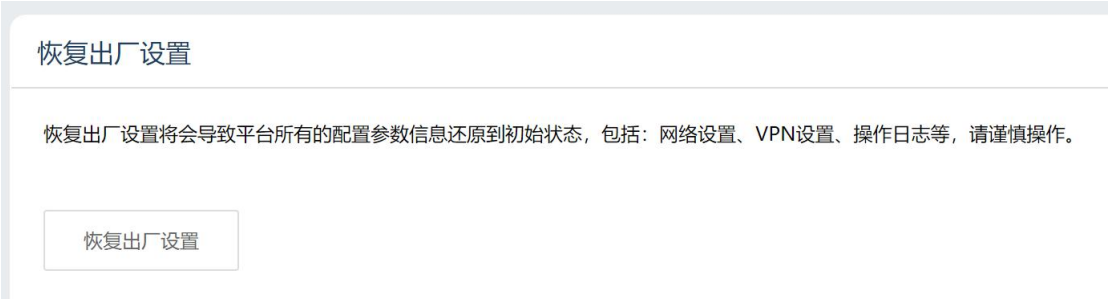
- [启用 SYSLOG 服务器]：启用于 syslog 服务器通讯的功能。
- [服务器 IP]：syslog 服务器的 ip 地址。
- [服务器端口]：syslog 服务器开放的同步端口。
- [输出到 SYSLOG 服务器的日志设置]：可以选择操作日志、系统日志。

3.6.5.7. 易部署设置

用于将云端易部署设置中的平台配置参数还原到初始状态，包括：网络设置、VPN设置等，请谨慎操作。

3.6.5.8. 恢复出厂设置

支持界面恢复出厂设置，恢复出厂设置将会导致平台所有的配置参数信息还原到初始状态，包括网络设置、VPN设置、操作日志等。请谨慎操作。



⚠ 注意：

恢复出厂设置将会恢复设备出厂状态，所有配置就还原到初始状态，请谨慎操作。

3.6.5.9. 黑匣子

支持界面下载设备当前黑匣子信息，用于在设备发现异常时，排查和定位问题原因。

3.6.5.10. 隐私设置

隐私设置用于用户是否参与用户体验改进计划，页面如下图。

4. BBC 管控 SDW-R 介绍

4.1. AUTO VPN

AutoVPN可在BBC端创建SANGFOR VPN拓扑，配置VPN总部的基础信息，选择对应的分支设备，其它信息由BBC自动生成。

在VPN设备接入BBC后，组建SANGFOR VPN网络就由BBC来配置完成，分支不用做其他的配置。

首先是BBC自动识别设备，然后在BBC配置好总部和分支的VPN对接信息，分支连接总部的用户和密码也同时由BBC自动生成。

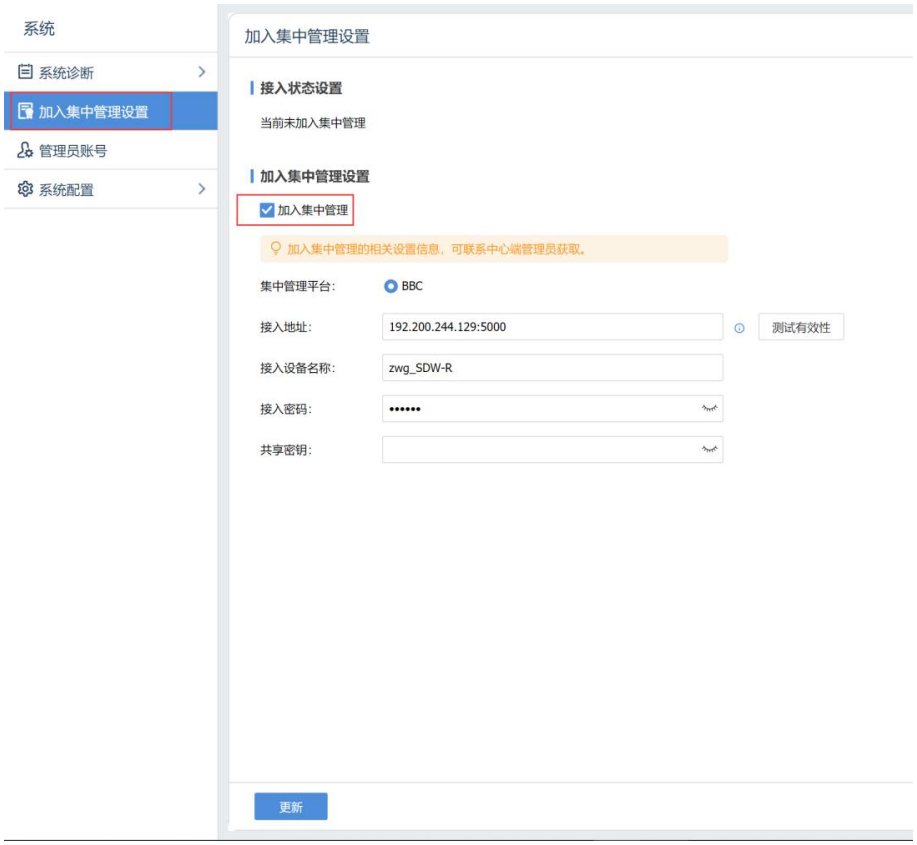
最后，下发SANGFOR VPN配置，接入BBC的设备就可以得到对应的配置。分支设备再向VPN总部设备发起SANGFOR VPN连接，最后组建起SANGFOR VPN网络。整个过程实现了优于传统VPN组网需要在总部和分支两端设备配置的方案。

接入BBC后，一切组建SANGFOR VPN网络的配置，都掌握在BBC端，更加有大体的规划视觉。维护人员只需要在BBC配置即可，避免了之前版本可能分支对接VPN总部误配的可能情况，同时也减轻了分支的配置维护成本。

4.1.1. SANGFOR VPN 建立

总部和分支先加入BBC，在BBC上面分别配置总部和分支的SANGFOR VPN配置，总部和分支后续都从BBC获取配置。

1. VPN总部和分支分别配置设备加入BBC，如下图。



2. 再在BBC上面创建组建VPN拓扑，分别设置总部和分支的配置。

- 总部 VPN 设备配置：在 BBC 上[VPN/VPN 拓扑管理/新增 VPN 拓扑]中选择已接入 BBC 的总部端设备（只有接入 BBC 的设备，才可以被选中用于组建 VPN 网络）。配置 VPN 相关配置，包含 webagent、VPN 端口、共享密钥、本地子网等。如下图。

- 分支 VPN 设备配置：在上图配置好总部设备后，在[VPN 分支设备]选择对应的分支网点即可，无需再像传统方案那样配置分支的连接管理。此处，只需要选择分支设备即可，如下图。

3. 配置好之后，可以选择下发配置到VPN硬件设备上面，分支根据自己得到的配置向总部发起VPN连接，最后组建起VPN网络。

⚠ 注意：

选择下发 VPN 配置，可以立即将 VPN 的相关配置下发到设备上，若不点击下发 VPN 配置，默认 10 分钟之内将会进行 VPN 配置的下发。

4.1.2. VPN 拓扑上报

已有的VPN连接拓扑可自动上报BBC。受控端在第一次接入BBC时，会上报已有的VPN连接配置，BBC会根据上报的VPN连接，自动识别VPN拓扑。如下图。

4.1.3. VPN 状态可视-拓扑大屏

VPN识别拓扑后，可大屏展示，在BBC端，路径：[大屏/VPN运维大屏]处可以显示拓扑大屏。可以直观查看VPN链路的状态、业务流量构成等信息。如下图。

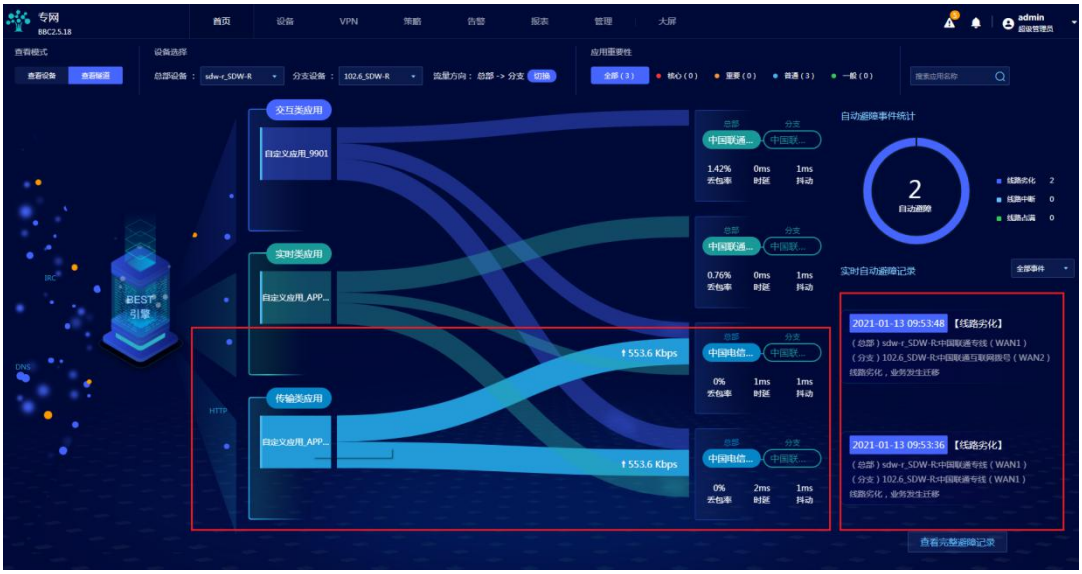
4.1.4. VPN 状态可视-设备列表

BBC可以通过列表展示全网VPN网点状态，点击具体的VPN设备,可以查看此VPN设备上和哪些VPN设备连接了VPN连接,以及相应的连接状态。如图。

4.1.5. VPN 状态可视-SDWAN 选路可视

点击[大屏/VPN业务选路大屏]，以大屏形式展示总部与分支VPN业务流量选路详情，已经流量自动避障事件情况，如下图所示。

设备自身会由于线路劣化、线路中断或者线路占满时VPN业务流量会自动发生切换，此时自动避障事件会记录当天由于线路质量发生变化并且VPN业务流量发生切换的事件。

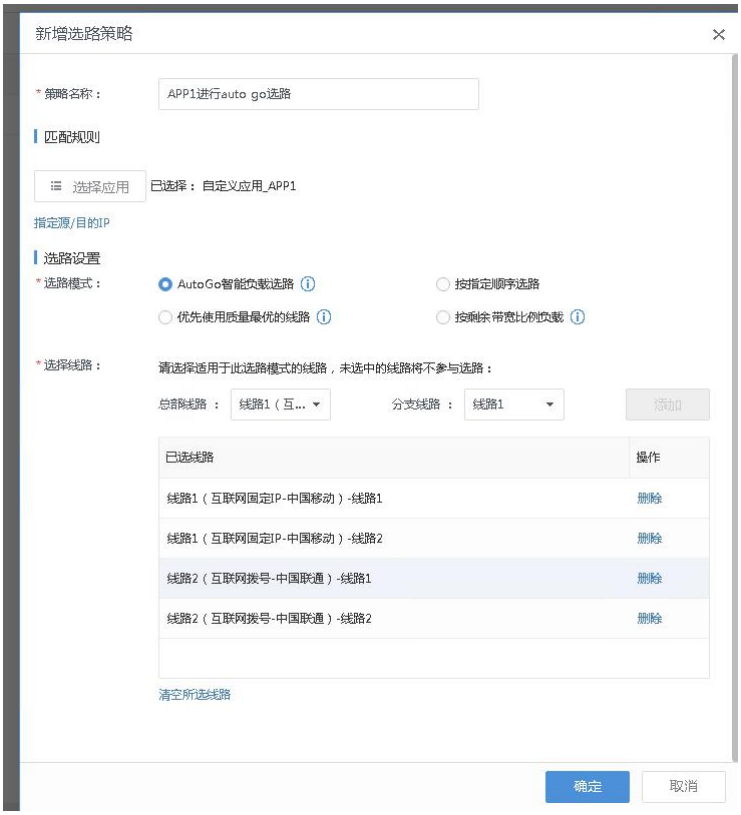


4.2. SDWAN 智能选路策略模板下发

在BBC中[VPN/SD-WAN智能选路模板]可以将BBC上的SD-WAN选路策略模板下发至SDW-R分支上。界面如下。

1. 点击<新增>，界面如下。

2. 创建SDWAN策略“APP1进行auto go选路”，匹配规则选择APP1，选路模式选择auto go智能负载选路，线路选择所有线路，将不存在的线路清空。



其他说明：

- Auto Go 智能负载选路是根据业务特性（实时类、传输类、交互类）将应用流量自动负载到最佳链路；
- 按指定顺序选路是将业务根据所选择的线路来进行选路，常用于核心业务走指定的线路；
- 剩余带宽比例负载是根据剩余带宽的比例选择最优的线路；
- 线路质量选路是根据线路的丢包率、延时和抖动计算一条质量最优的线路进行选路。

3. 配置完成之后选择下发模板配置，将配置下发到分支上。

注意：

SD-WAN 配置如果不点击立即下发，需要等 10 分钟以后才会自动下发。

SD-WAN 的选路策略除了 Auto Go 智能负载外，还可以选择按顺序选路、按线路剩余带宽比例、优先使用质量最好的线路进行选路。

5. 附录

通过RESET键恢复默认配置和密码。

1. SDW-R设备通电状态下，连续按RESET键两次，用于恢复密码为默认值，不会将设备恢复为出厂设置状态。
2. SDW-R设备通电状态下，按住RESET键不放，3秒钟以后ALARM红灯会开始闪烁，此时松开RESET键，之后ALARM红色告警灯会常亮，等ALARM灯熄灭后即恢复默认配置成功，此时可通过设备LAN/DMZ口使用默认出厂IP地址登录设备，登录用户名密码也恢复到默认值。

⚠ 注意：

通过 RESET 键恢复默认配置时，会导致设备恢复到出厂状态，请在 BBC 上确认是否有保留备份配置，防止配置丢失。