WEB 管理手册

RG-NBR 系列出口网关

NBR_RGOS 11.9(4)B11P1

文档版本 ：V1.0

版权声明

免责声明

您所购买的产品、服务或特性等应受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，锐捷网络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。锐捷网络保留在没有任何通知或者提示的情况下对文档内容进行修改的权利。

本手册仅作为使用指导。锐捷网络在编写本手册时已尽力保证其内容准确可靠，但并不确保手册内容完全没有错误或遗漏，本手册中的所有信息也不构成任何明示或暗示的担保。

前　　言

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷睿易官方网站：http://www.ruijiery.com/
- 锐捷睿易在线客服：http://ocs.ruijie.com.cn/?p=smb
- 锐捷网络官方网站服务与支持版块：http://www.ruijie.com.cn/service.aspx
- 7 天无休技术服务热线：4001-000-078
- 锐捷睿易技术论坛：http://bbs.ruijiery.com/
- 常见问题搜索：http://www.ruijie.com.cn/service/know.aspx
- 锐捷睿易技术支持与反馈信箱：4001000078@ruijie.com.cn
- 锐捷网络服务公众号：【锐捷服务】扫码关注

本书约定

1. 命令行格式约定

命令行格式意义如下：

粗体：命令行关键字（命令中保持不变必须照输的部分）采用加粗字体表示。

斜体：命令行参数（命令中必须由实际值进行替代的部分）采用斜体表示

[ ] ：表示用[ ] 括起来的部分，在命令配置时是可选的。

{ x | y | ... }：表示从两个或多个选项中选取一个。

[x | y | ...]：表示从两个或多个选项中选取一个或者不选。

//：由双斜杠开始的行表示为注释行。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

□ □

□ □

□ □

□ □ /□ □

3. 说明

- 本手册举例说明部分的端口类型同实际可能不符，实际操作中需要按照各产品所支持的端口类型进行配置。
- 本手册部分举例的显示信息中可能含有其它产品系列的内容（如产品型号、描述等），具体显示信息请以实际使用的设备信息为准。
- 本手册中涉及的路由器及路由器产品图标，代表了一般意义下的路由器，以及运行了路由协议的三层交换机。

1 Web 配置指南

1.1 概述

本章节说明使用 Web 管理系统的方法，您可以使用这个 Web 管理系统来管理您的 NBR 路由器的常用功能。

用户使用浏览器（如 IE）访问 WEB 管理系统来管理 NBR 设备。

目前该文档仅适用于 NBR □ □ □ □ □ □

1.2 典型应用

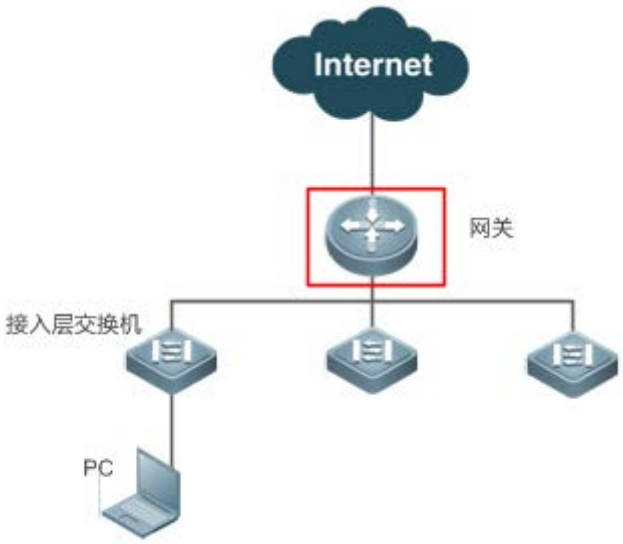
典型应用	场景描述
通过WEB管理设备	完成 NBR 设备相应配置后，用户可以通过浏览器访问 WEB 管理系统

1.2.1 通过 WEB 管理设备

应用场景

如下图所示，用户可通过 PC 浏览器访问 NBR 设备的 WEB 管理系统，对设备进行管理和配置。

图 1-1



【注释】 图中红框内设备为被访问的 NBR 设备，确保 PC 能够 ping 通该 NBR 设备就可以访问其 WEB 管理系统。

功能部属

↘ 配置环境要求

客户端的要求：

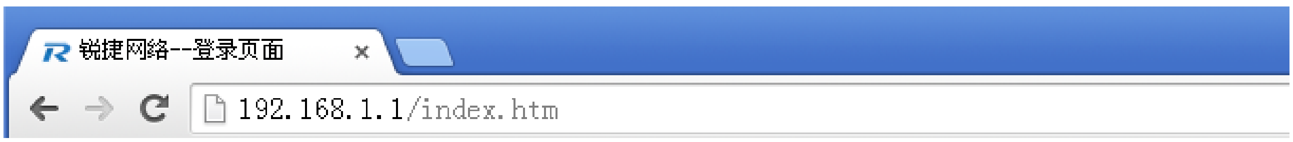
1. 网管使用客户端的浏览器登录到 WEB 管理界面对 NBR 进行管理。客户端通常是指 PC，也可能是一些其它的移动终端设备，如笔记本电脑等。
2. 浏览器：支持 Google chrome、IE8.0、IE9.0、IE10、IE11 以及部分基于 IE 内核的浏览器（如 360 浏览器）。使用其它浏览器登录 WEB 管理时，可能出现乱码或格式错误等异常。
3. 分辨率：建议分辨率设置为 1024*768、1280*1024、1440*960 及 1600*900，在其它分辨率下，页面字体和格式可能出现不对齐、不够美观等异常。

1.3 WEB 管理系统

本章节说明使用 Web 管理界面的方法，您可以使用这个 Web 管理界面来管理您的 NBR 的常用功能。

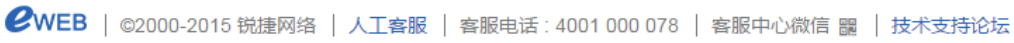
1.3.1 进入 WEB 管理界面

第一步：在您的浏览器地址栏中输入 NBR 路由器的【内网口\外网口\管理口】的 IP 地址。您的 PC 当前 IP 地址必须与 NBR 设备的 IP 地址处在同一网段。



- 在复位或初始情况下默认的 WEB □ □ □ □ □ □ http://192.168.1.1□
- □ □ □ □ https □ □ □ □ □ □ □ □ □ □ □ https://192.168.1.1:4430□
- □ admin□
- □ □ □ □ □ PC □ □ □ □ □ □ Gi0/0 □ □ □
- □ 1□ 2 □

第二步：进入系统登录界面，如下图所示：



1、 输入用户名和密码然后点击 登 录 按钮，进入设备管理的主界面。

2、 如果您忘记了用户名或密码，请点击 忘记密码？ 。

3、 如果需要客服帮助，请点击 人工客服 和客服进行在线交流。

4、 密码重置功能，如果你想重置默认密码，可以按长按 reset 按钮，然后在 web 上登录根据提示重置密码，是否需要保存配置，操作如下图。

5、防暴力破解登录，输入账号密码错误 5 次，会锁住 1 分钟，在锁住一分钟是无法尝试登录 eweb。

NBR路由器

以客户为中心·Ruijie|睿易

用户名或者密码不正确！您还有剩下4次尝试机会！

admin

登录

忘记密码?

要使用 web □□□□□□□□ NBR □□□□□ web □□□□□□□□□□□□ web.gz □□□□□□ web □□□ ngx □□□ □□□□□□□□□□□□□

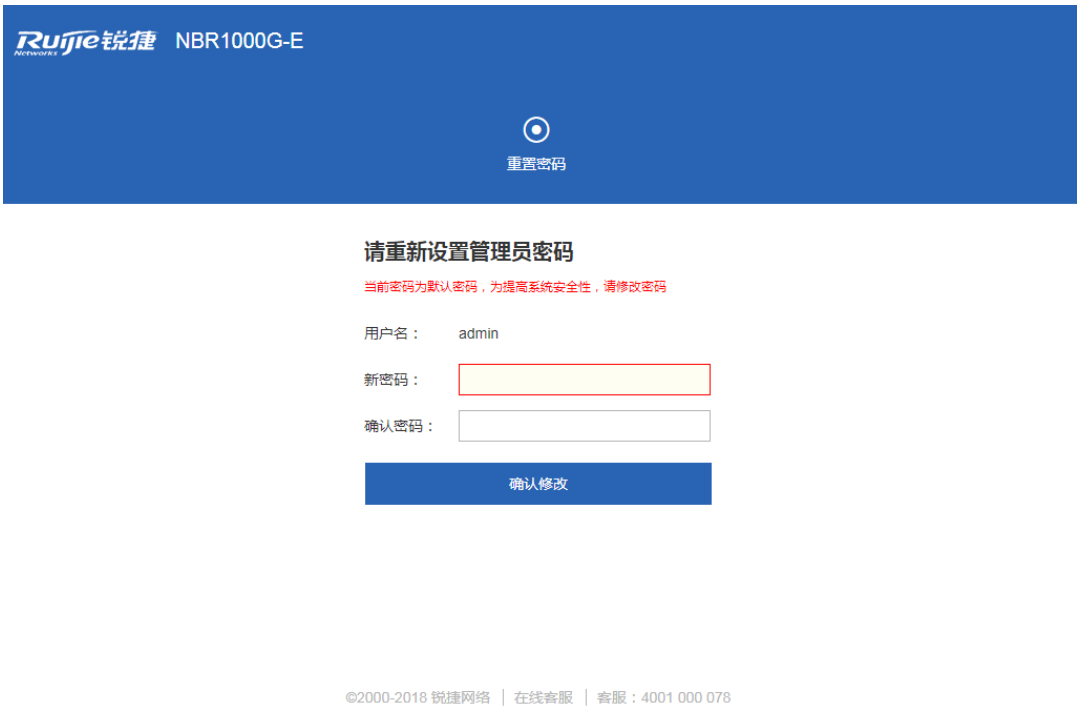
1.3.2 快速配置

首次登录 WEB 管理界面时设备处在空配置状态，为了简化您的配置工作，我们建议您使用“快速配置”向导来完成设备的常用功能设置。如果您不需要“快速配置”功能，请点击“转到首页”就可以直接进入，不过这个时候设备为空配置（不推荐；即使是旧设备升级到本版本，如果不走快速配置，有可能导致流控，默认路由等功能异常）。

□□□□□□ WEB □□□□□□□□□□□□□“ □□变更向导” □□□□□□□

1.3.2.1 快速配置

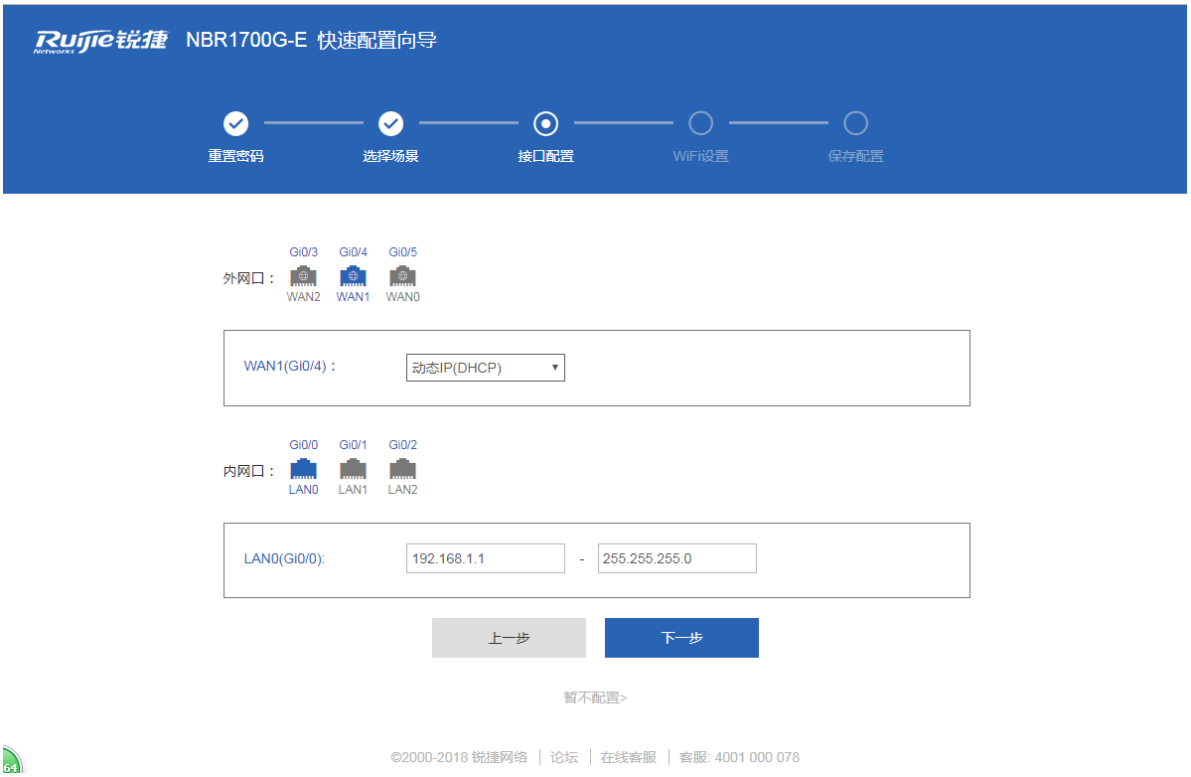
(1) 重置密码


NBR1000G-E
重置密码
请重新设置管理员密码
当前密码为默认密码，为提高系统安全性，请修改密码
用户名： admin
新密码：
确认密码：
确认修改
©2000-2018 锐捷网络 | 在线客服 | 客服：4001 000 078

(2) 场景选择


NBR1700G-E 快速配置向导
重置密码
选择场景
接口配置
保存配置
请选择您的网络场景
通用
配置全面，适用各种场景
中小企业
智能企业流控，办公无忧
别墅
别墅模式、家长控制、上网无忧
网吧
智能选路，游戏不卡
上一步
下一步
©2000-2018 锐捷网络 | 论坛 | 在线客服 | 客服: 4001 000 078

(3) 接口配置



(4) 智能流控

(5) WiFi 配置


Ruijie锐捷 NBR1700G-E 快速配置向导
重置密码
选择场景
接口配置
智能流控
WiFi设置
保存配置
用于管理其下连接的AP发射无线信号
WiFi名称：
1
WiFi密码：
显示密码
上一步
下一步
©2000-2018 锐捷网络 | 论坛 | 在线客服 | 客服: 4001 000 078

(6) 保存配置


Ruijie锐捷 EG2000K 快速配置向导
退出
选择场景
接口配置
智能流控
保存配置
正在下发配置，请勿做其它操作，请稍候...
34%
©2000-2018 锐捷网络 | 论坛 | 在线客服 | 客服：4008 111 000


Ruijie锐捷 EG2000K 快速配置向导
退出
选择场景
接口配置
智能流控
保存配置
恭喜您，配置成功~
外网连通性检测（请确认网络线路已接入后进行检测）
立即检测
如何使用手机进行远程管理？
配置清单
回首页
推荐配置
接口配置
©2000-2018 锐捷网络 | 论坛 | 在线客服 | 客服：4008 111 000

(7) 配置清单

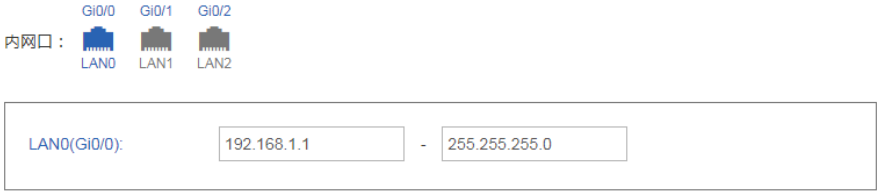
网络模式

快速配置只支持网关模式

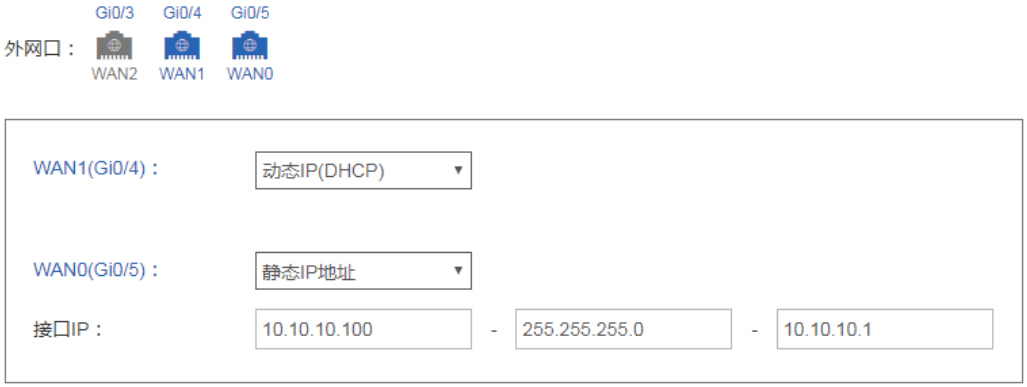
↘ 接口配置

接口配置：是实现内部上网的关键配置，这里的配置是否正确关系到内网是否可以正常上网。

1）内网口配置：选中您要配置的内网口，然后在下面的输入框中输入 IP 地址和子网掩码即可。如下图所示：



2）外网口配置：首先将您申请的外网线路与设备的外网口连接好，然后选中要配置的外网口。接着依次选择您的客户端 IP 分配方式、带宽信息和线路类型等。如下图所示：



当您的客户端上网方式选择“静态 IP 地址”时需要配置运营商分配给您的 IP 地址或您自己的内网 IP 及子网掩码和网关，如上图所示。要注意的是“下一跳地址”就是此外网口 IP 地址对应的网关。

如果您向运营商申请的是 ADSL 线路则请选择 “PPPoE(ADSL)”。配置如下图：。

如果您的上网方式选择“动态 IP(DHCP)”，则不需要其他额外配置。

线路带宽的缺省情况下是 10M 带宽，不过需要根据您向运营商申请的带宽实际数据填写，请务必准确填写该选项，以便设备能更好更智能的为您管理带宽。

配置完以上选项后您只需要点击 

按钮就可以完成配置，开始管理网络运行状况了！

1.3.2.2 全网智能快速配置

点击“连通网络”按钮，会下发相关配置。配置成功后提示用户跳转到全网智能配置，并且进入全网智能配置界面。

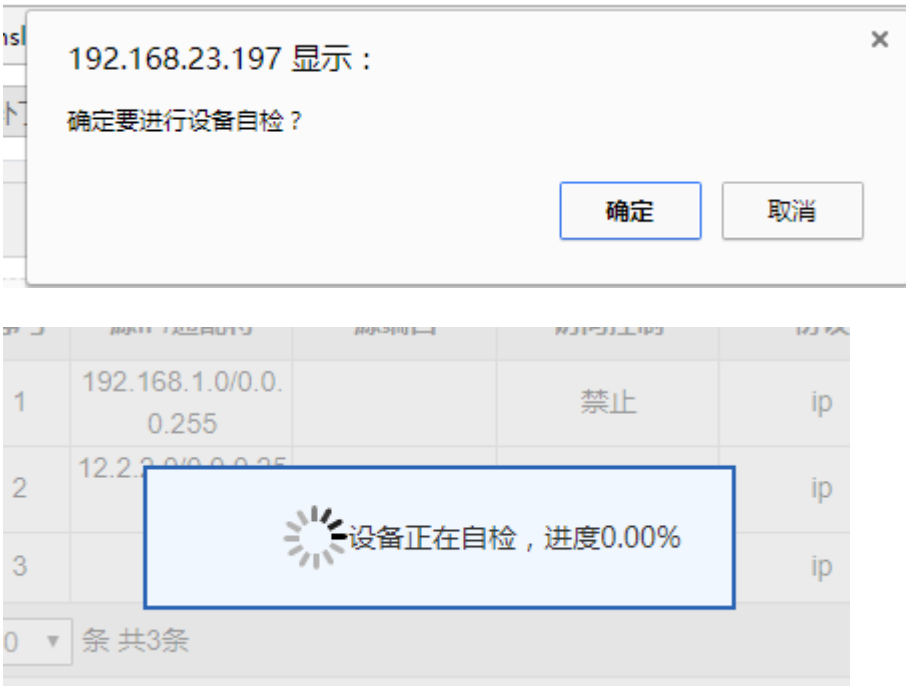

Ruijie锐捷 NBR3000D-E 全网智能配置向导
退出
已上电
未上电
已选中
外网口：
Gi0/6
Gi0/7
WAN1
WAN0
WAN0(Gi0/7)：
动态IP(DHCP)
路由器
互联网
内网口：
Gi0/0
Gi0/1
Gi0/2
LAN0
LAN1
LAN2
LAN3
LAN4
LAN5
LAN0(Gi0/0):
192.168.1.1
-
255.255.255.0
连通网络
©2000-2018 锐捷网络 | 在线客服 | 客服：4001 000 078


Ruijie锐捷 NBR3000D-E 全网智能配置向导
退出
已上电
未上电
已选中
Gi0/6
Gi0/7
外网口：
WAI
WAN0(GiC
Gi0
内网口：
LAI
LAN0(Gi0/0):
192.168.1.1
255.255.255.0
网络连接畅通！
接下来，将进行全网智能配置
自动跳转中...
连通网络
©2000-2018 锐捷网络 | 在线客服 | 客服：4001 000 078

如果您更改了接口 IP □□□□□□□□□□□□□□□□□□□□ IP □□□□□□ Web □□□□□

1.3.3 设备自检

点击设备自检

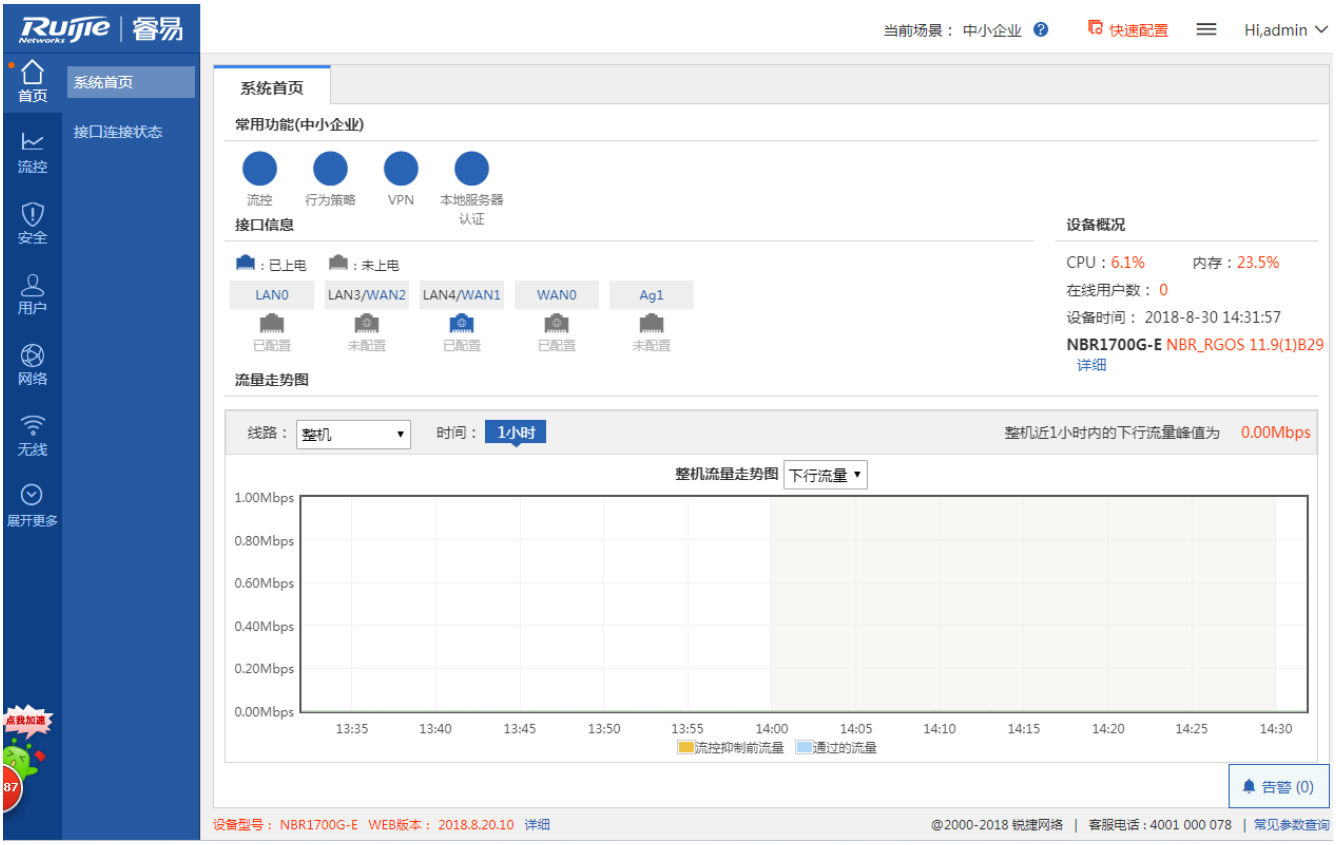


正常状态，如下图，增加有帮助和反馈的统计


设备自检
当前网络通畅
当前终端网络通畅，无需诊断无法上网问题。
重新检测
有帮助 | 反馈
设备检测正常
反馈设备自检意见
告诉我们你的建议或遇到的问题，允许输入100个字。
您的手机：
您的邮箱：
提交
更多高级诊断功能支持，请下载：信息收集诊断工具（捷哥的法杖）

上不了网的情况：

点击去修复，浏览器新窗口打开页面



1.3.4 Web 管理主界面说明

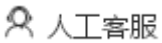
WEB 管理平台主页面下图所示：

1.3.4.1 标题区

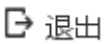
该区域为您提供了一些常用功能的链接，方便您快速定位到常用的功能设置页面。主要有“补丁版本”、“快速配置”、“智能客服”、“人工客服 ” 和“退出”。

客服

智能客服：点击  后将弹出本产品在线客服窗口，用户在此窗口页面填写访客信息后即可与智能客服对话咨询。

人工客服： 点击  后将弹出本产品在线客服窗口，用户在此窗口页面填写访客信息后即可与人工客服对话咨询。

退出

退出：当您完成本次设备管理后请单击  按钮，退出 NBR 的 Web 管理平台主页面，回到登录页面。

1.3.4.2 菜单导航区

在 Web 管理主界面的左侧设有“NBR 菜单导航”区域。该区域列出了 NBR 的所有功能菜单。当您点击相应菜单后在“主操作区”会打开详细的设置页面。

菜单的组织方式分为二级，当您点击一个功能大类时会展开相应的子菜单，如点击“流控/行为/安全”后将展开该功能大类的子菜单。如图所示：

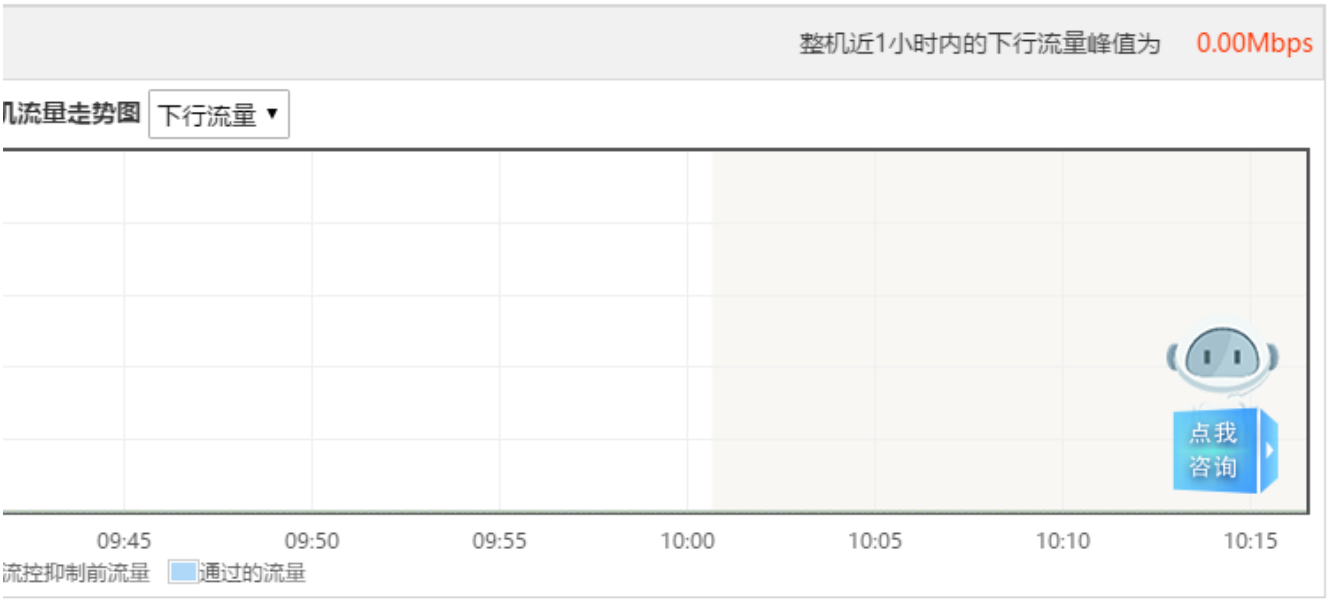
1.3.4.3 主操作区

主操作区是完成 NBR 功能设置的主要区域，当点击左边的导航菜单或顶部的快捷菜单，将会在主操作区打开详细的设置页面。

1.3.4.4 状态区

该区域左边显示设备的型号和版本号；右边显示技术论坛网址和技术支持联系方式，用户在使用中遇到问题可以通过这两个联系方式联系客服协助解决。

右下角增加闪电兔图标，可以拖拽，可以点击咨询


整机近1小时内的下行流量峰值为 0.00Mbps
机流量走势图
下行流量
点我
咨询
09:45
09:50
09:55
10:00
10:05
10:10
10:15
流控抑制前流量
通过的流量


小睿哥-有问必答
锐捷睿易
咨询非睿易产品，请点击这里跳转。
锐捷睿易
合作伙伴服务热线
今天 10:16
小睿哥-有问必答
大家好，我是小睿哥，汇集睿易5年经验精心打造出的最强知识库，涵盖万条知识，有问必答！
小睿哥-有问必答
【锐捷睿易热搜榜】
【易网络】易网络全套资料请点我！
【小睿期刊】易网络当周最热
【小睿视频】易网络自学视频 Hot!
【最全参数】 SMB产品全系列参数表（电脑请点我）
【最全参数】SMB产品全系列参数表（手机请点我）
【请您帮助】借用您2分钟，小睿哥虚心求指导
小睿哥使用小技巧（设备型号+问题关键字）：
【人工客服】小睿哥里找不到答案？点我获取协助
【保修查询】不知道设备保修期？点我查询
易网络【火爆】
版本获取
参数咨询
产品入门
自学视频
故障排查
请输入产品型号+问题关键字，如："RAC64 上网"
发送

1.3.4.5 导航栏告警

当有系统告警信息时，区域右上角会出现 

按钮，没有告警信息时则无提示信息。括号内的数字表示当前有哪几种告警。出现告警信息时，点击 

后会有系统告警弹窗出现，弹窗内只显示有告警的模块：

1. 流量攻击告警：

（1） 什么时候会出现告警提示？

当设备正在被攻击或曾经被攻击但是您未发觉或查看的攻击。

（2） 如何解决出现告警？

您可以在防攻击页面开启防流量攻击选项，如下图

（3） 点击【历史的攻击日志】可查看历史流量攻击信息。

2. 接口带宽不足告警：

（1） 什么时候会出现告警提示？

当设备接口带宽不足或曾经接口带宽不足但是您未发觉或查看的告警。

（2） 如何解决出现告警？

告警信息会有对应的解决措施方案。

（3） 点击‘带宽不足历史日志’可查看历史接口带宽不足信息。

3. 特征库审计告警：

特征库版本信息的告警，当前系统中不存在特征库，或者特征库升级后有配置丢失时，就会出现告警。点击

可查看所有特征库版本告警信息。

4. 硬盘告警：

硬盘有出现坏道，硬盘缺失，硬盘接触不良时出现告警。

5. 配置文件告警：

当配置文件超过 100KB 时将提示备份配置，超过 200KB 时出现告警。

6. 默认路由告警：

当设备未配置默认路由时会导致上网异常，建议配置默认路由，没有配置路由会出现告警。

7. 系统密码告警：

通常出厂密码为 admin，当进来 web 页面未修改密码会提示系统密码告警。

1.3.5 首页

1.3.5.1 系统首页

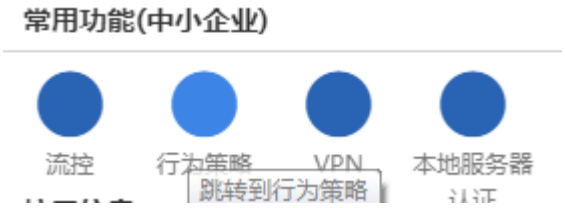
登录 WEB 管理界面后自动会转到系统首页，您也可以通过菜单区点击 

跳转到系统首页。

通过该页面，您可以方便地查看设备 CPU、内存、硬盘使用情况，在线用户数，系统版本及系统当前时间等信息。通过分析本日流量走势、本日应用流量 TOP10 和本日用户流量 TOP10 方便您全方位的查看内部网络流量的当前状态，您可以在该页面发现定位常见的网络问题，并快速解决问题。

1.3.5.1.1 常用功能

在系统首页页面上方，显示了常用功能，点击按钮可以进入对应菜单：

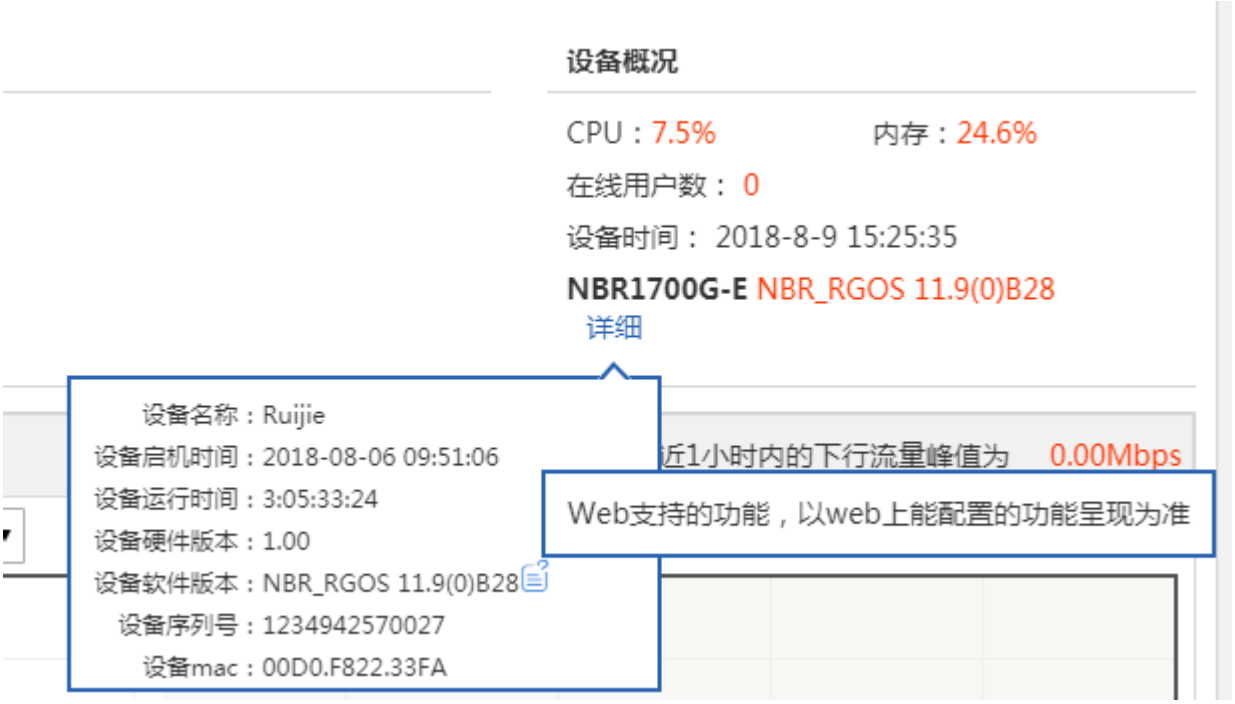


1.3.5.1.2 接口信息

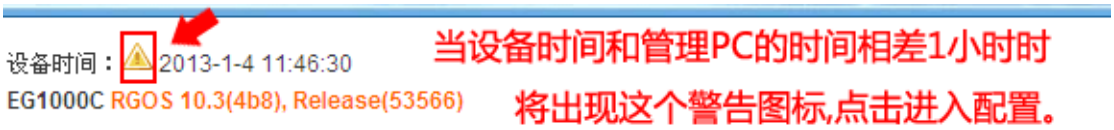
在系统首页页面上方，显示了接口信息，鼠标经过时可以显示接口配置的基本信息，如接口类型及 IP 地址，账号信息等：

1.3.5.1.3 设备概况

在系统首页页面上方，显示了当前设备的内存、CPU 使用情况，在线用户数及系统版本、系统时间等信息：



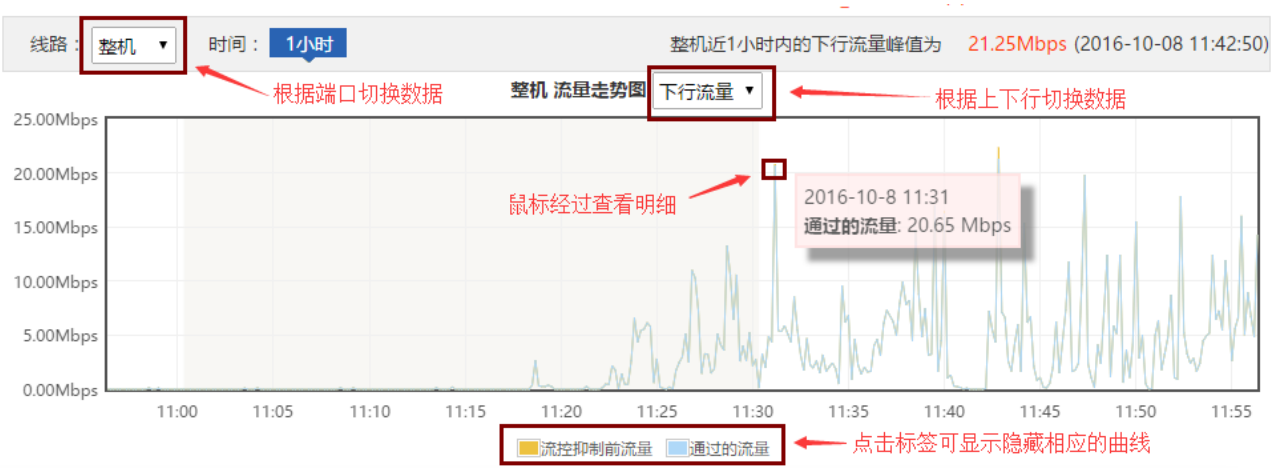
1. CPU：显示了当前设备的 CPU 使用率，您可以轻松的得知设备运行状况。
2. 内存：显示了当前设备的内存使用率，方便您得知设备的内存使用情况。
3. 硬盘：显示了当前设备的硬盘使用率，方便您得知设备的硬盘使用情况。
4. 在线用户数：显示了当前设备在线用户总数。
5. 设备时间：显示系统当前时间，如果您觉得当前系统时间有误，或因为某些需要而要重新设置系统时间，则可以到 高级选项 》 系统设置 》 系统时间 页面重新设置。



1.3.5.1.4 带宽状态

在系统首页页面，显示了系统带宽状态，在该功能页面您可以轻松地查看当前设备最近一小时的流量走势图、本日应用流量 TOP10 使用率、当前应用流量 TOP10、当前用户流量 TOP10 和用户会话数 TOP10。

- **最近一小时流量走势图：**

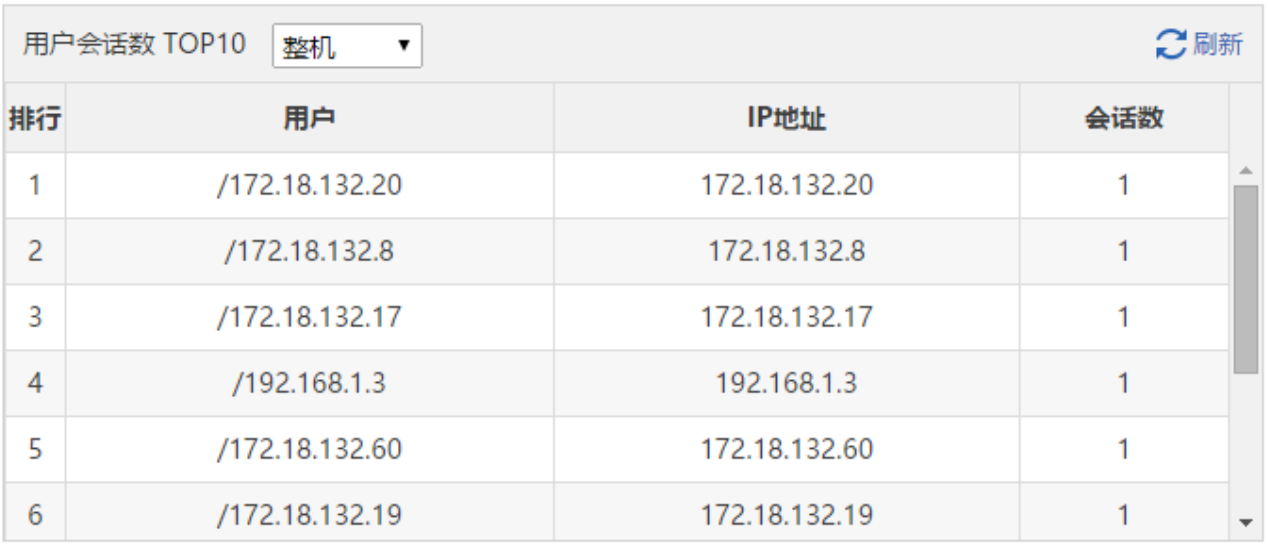


1. 如上图所示，黄色曲线显示的是“流控抑制前的流量”走势，蓝色曲线显示的是受流控抑制后实际通过的流量走势。
2. 您可以更改接口 整机 、及 下行流量 来查看各接口的本日流量走势；
3. 鼠标移上曲线点可以查看所在位置的“流控抑制前流量”和“通过的流量”。
4. 点击 流控抑制前流量 可以隐藏“流控抑制前流量”走势曲线，点击 通过的流量 可以隐藏通过的流量走向曲线。

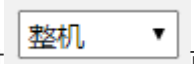
- **本日应用流量 TOP10**

1. 如上图所示，表格显示了流量 TOP10 的用户
2. 通过 下行 可根据不同上下行流量查看最近十分钟流量 TOP10；

- **本日用户会话数 TOP10**

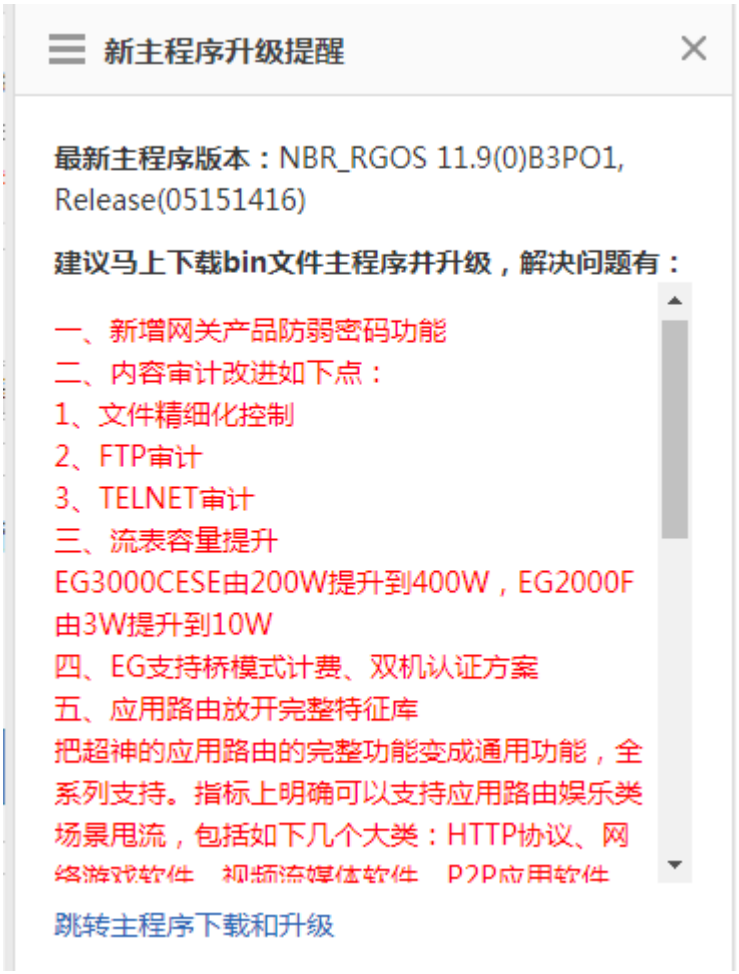


排行	用户	IP地址	会话数
1	/172.18.132.20	172.18.132.20	1
2	/172.18.132.8	172.18.132.8	1
3	/172.18.132.17	172.18.132.17	1
4	/192.168.1.3	192.168.1.3	1
5	/172.18.132.60	172.18.132.60	1
6	/172.18.132.19	172.18.132.19	1

1. 如上图所示，表格显示了流量 TOP10 的用户
2. 通过 

可根据不同端口查看用户会话数 TOP10；

1.3.5.1.5 主程序推送



1.3.5.2 接口连接状态

可以查看，各个接口的状态信息，ip 地址、速率、dns、是否连接等，当不支持 ipv6 字段，该字段会隐藏起来。

1.3.5.3 上网配置

请参考“1.3.2 快速配置”章节。

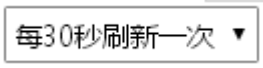
1.3.6 流控

1.3.6.1 流量监控

您可以通过 **流控/行为—>流量监控** 模块查看当前网络流量的使用情况，并对具体的应用进行智能分析。

1.3.6.1.1 实时流量

1. 实时流量页面上方显示实时流量导航菜单如下：

（1） 通过 

可以选择每隔 10 秒/30 秒/1 分钟自动刷新一次设备当前流量信息 ,也可以选择手动刷新设备当前流量信息。

（2） 通过 

可以选择根据线路、应用、用户来看看设备流量信息。

（3） 通过 

可以查看具体某条线路的流量信息，选择“整机”则显示所有线路的流量总和信息。

（4） 通过 

可以选择查看当前的流量信息，或者查看最近 1 个小时内或今天的整体流量走势。 

表示正在查看当前的流量信息。

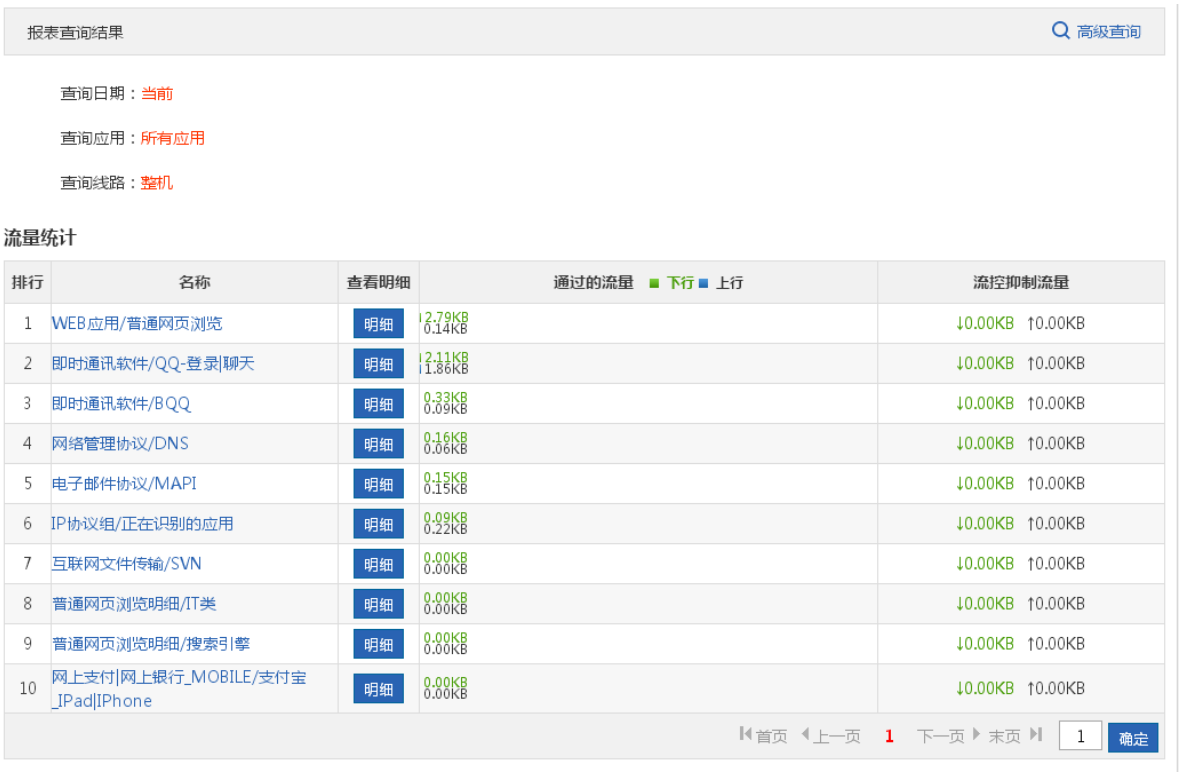
（5） 点击 

将弹出以下窗口，可以查看流量、在线用户数、会话数等明细：

流量明细：可以从用户、IP 或应用的角度查看某线路的当前流量或某个时间范围内的流量信息，如下图所示，点击名称后面的输入框，选择查看类型，点击右边输入框可以在弹出的应用树或用户树中选择需要查询的应用范围或用户范围：

选择接口，点击 

，将弹出查询结果如下：



在线用户数明细：通过以下窗口，可以查询某线路的当前在线用户数，或某个时间范围内的在线用户数：

点击 确定查询 ，将弹出查询结果如下：

会话数明细：通过以下窗口，可以查询某线路的当前会话数，或某个时间范围内的会话数

点击 

，将弹出查询结果如下：

- **接口流量分析**

该功能是把带宽的使用按不同的线路（接口）来统计，您可以对线路（接口）的流量进行控制和分析，以便提高流量的使用价值。点击实时流量页面导航菜单栏中的 

显示如下：

- 概况

概况：显示某条线路的流量信息。当线路选择“所有线路”时，将显示所有线路的流量总和信息，以及各条线路的流量信息。

当前流量信息：上图所示即线路当前的流量信息，通过上图的流量信息，也可以发现当前流量是否正常（有无出现告警），如果流量过高会出现黄色告警 告警，来帮助您快速定位带宽问题。

问题：什么时候会出现告警提示？

总流量达到了线路带宽（贵机构向电信等运营商申购的带宽）的 95%以上时。

问题：如何解决出现黄色告警？

1. □□□□□□□□□□□□□□□“□□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□

2. □□□□□□□□□□□□□“□□□□□”□□

□□□

- 应用

应用：应用区域显示了所选线路上各类应用（关键/保证类、普通/其他类、抑制类）占用的带宽比，总共有多少个应用正在使用、具体什么应用，以及各个应用占用的流量和因策略限速而被丢弃的流量等信息：

1) 该区域上方的两个饼图分别显示所选线路上行和下行流量为各应用类型占用的流量信息，鼠标经过饼图上方时将显示所选线路上行或下行流量中未被使用的流量大小：

关键/保证类：显示所有属于关键/保证类的应用在所选线路上/下行流量中占用的流量之和，与所选线路上/下行流量总和的百分比。

普通/其他类：显示所有属于普通/其他类的应用在所选线路上/下行流量中占用的流量之和，与所选线路上/下行的流量总和的百分比。

抑制类：显示所有属于抑制类的应用在所选线路上/下行流量中占用的流量之和，与所选线路上/下行的流量总和的百分比。

未使用：显示在所选线路上/下行流量中未被使用的流量，与所选线路上/下行的流量总和的百分比。

2) 该区域下方的表格显示所选线路上正在使用的具体应用的流量信息，包括各应用占用的上/下行流量，以及因策略限速而被丢弃的流量。

在表格左上方的导航菜单中选中 应用组 ，将显示所选线路上正在使用的应用组的流量信息：


应用 | 应用组

排行	名称	查看明细	通过的流量 ■ 下行 ■ 上行	流控抑制流量
1	HTTP协议	明细	0.96Kbps 0.23Kbps	↓0.00Kbps ↑0.00Kbps
2	即时通讯软件	明细	0.19Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps
3	IP协议组	明细	0.13Kbps 0.27Kbps	↓0.00Kbps ↑0.00Kbps
4	电子邮件协议	明细	0.02Kbps 0.02Kbps	↓0.00Kbps ↑0.00Kbps
5	P2P应用软件	明细	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps
6	网络管理协议	明细	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps
7	远程访问协议	明细	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps

显示: 10 首页 上一页 1 下一页 末页 1 确定

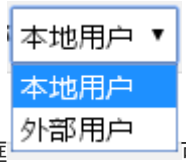
点击 明细 将弹出以下窗口：

该窗口显示了所选应用所属的应用组、类型信息，在所选线路上占用的上下行流量信息、因策略限速而被丢弃的流量信息，以及正在运行该应用的用户流量信息。

点击 阻断流量 按钮，可以对当前应用的流量进行阻断，阻断后，该应用后续的流量将被所选线路完全丢弃。

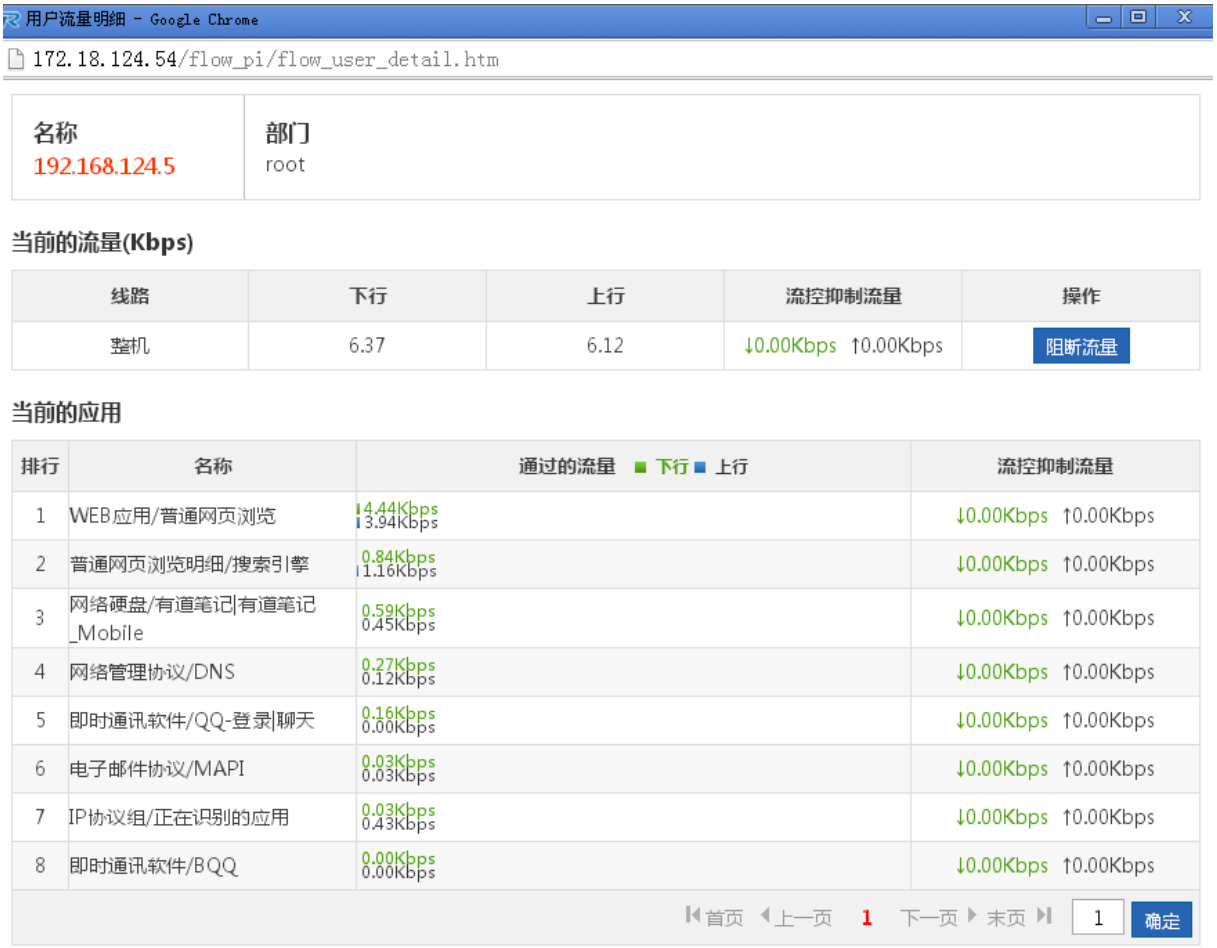
3) 用户

用户：用户区域显示了所选线路上的在线用户数、会话数，以及正在使用该线路的用户流量信息：



通过下拉框可以选择查看本地用户或认证用户的流量信息。

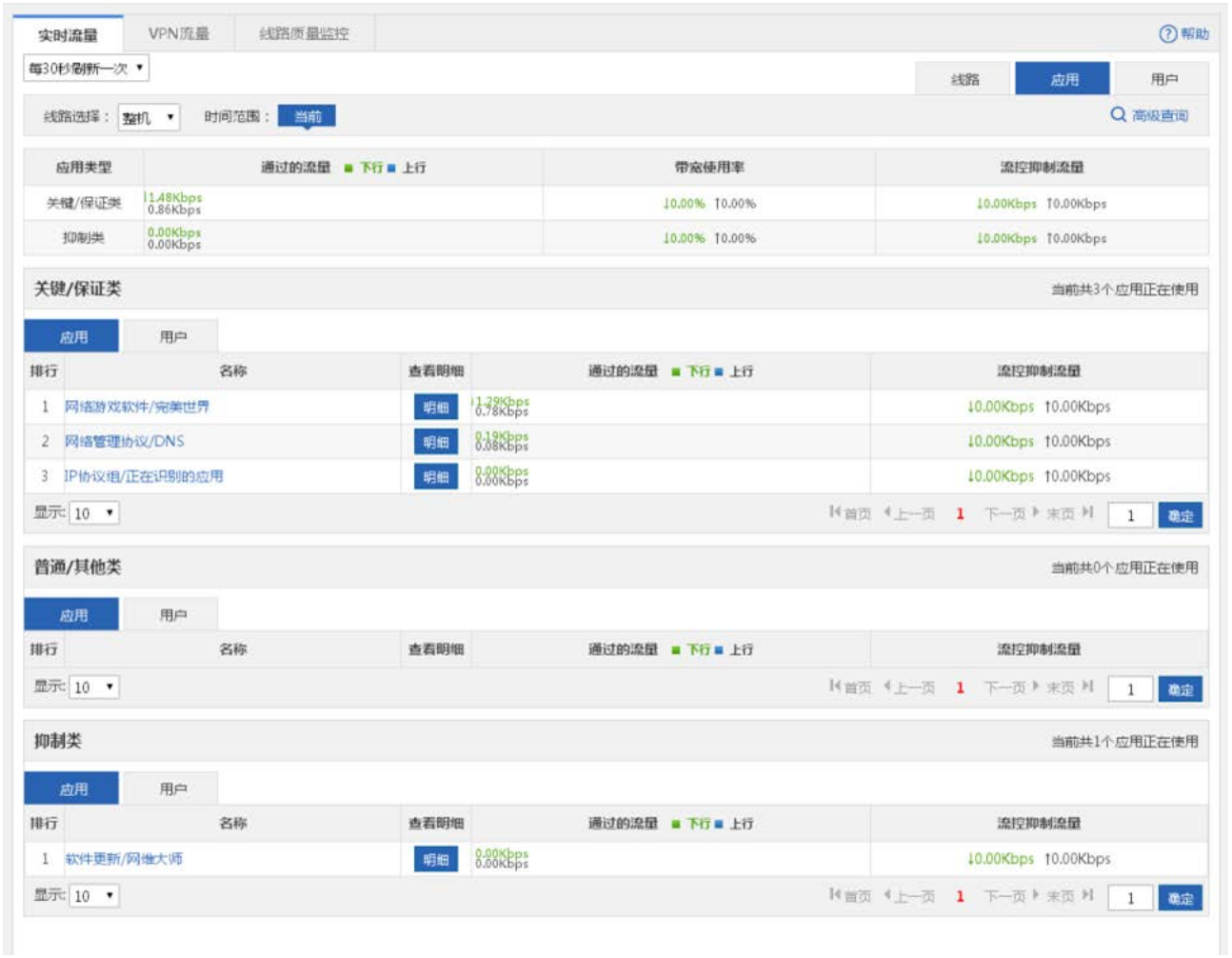
点击 明细 ，将弹出以下窗口，显示了所选用户在所选线路上的流量使用信息，以及所选用户正在运行的应用明细及各应用的流量信息：



点击 阻断流量 按钮，可以对当前用户的流量进行阻断，阻断后，该用户后续的流量将被所选线路完全丢弃。

- **应用流量分析**

该功能是把带宽的使用按不同的应用软件来统计，您可以对应用的流量进行控制和分析，以便提高流量的使用价值。点击实时流量页面导航菜单栏中的 应用 显示如下：



↘ 概况：页面第一区域显示了整机上，关键/保证类、普通/其他类、抑制类三种类型的应用的流量信息：

1) 当前流量信息：

如上图所示，显示了在所选线路上，关键/保证类、普通/其他类、抑制类三种类型的应用当前分别占用的流量、带宽使用率、以及因策略限速而被丢弃的流量。

1. 关键/保证类：该区域显示在所选线路上，属于关键/保证类的正在使用的应用明细、各应用占用的流量信息，以及正在运行关键/保证类应用的用户明细、各用户占用的流量信息。

点击 明细 将弹出应用流量明细窗口，详见“2.5.1.1 接口流量分析”章节中的应用流量明细窗口的分析。

上图显示的是关键/保证类应用的流量信息，点击

的“用户”将显示当前线路正在使用关键/保证类的用户流量信息：

点击 明细 将弹出用户流量明细窗口，详见“2.5.1.1 接口流量分析”章节中的用户流量明细窗口的分析。

2. 普通/其他类：该区域显示在所选线路上，属于普通/其他类的正在使用的应用明细、各应用占用的流量信息，以及正在运行普通/其他类应用的用户明细、各用户占用的流量信息。

点击 明细 将弹出应用流量明细窗口，详见“2.5.1.1 接口流量分析”章节中的应用流量明细窗口的分析。

上图显示的是普通/其他类应用的流量信息，点击  的“用户”将显示当前线路正在使用普通/其他类应用的用户流量信息：

点击 明细 将弹出用户流量明细窗口，详见“2.5.1.1 接口流量分析”章节中的用户流量明细窗口的分析。

3. 抑制类：该区域显示在所选线路上，属于抑制类的正在使用的应用明细、各应用占用的流量信息，以及正在运行抑制类应用的用户明细、各用户占用的流量信息。

点击 明细 将弹出应用流量明细窗口，详见“2.5.1.1 接口流量分析”章节中的应用流量明细窗口的分析。

上图显示的是抑制类应用的流量信息，点击 

的“用户”将显示当前线路正在使用抑制类应用的用户流量信息：

点击 

将弹出用户流量明细窗口，详见“2.5.1.1 接口流量分析”章节中的用户流量明细窗口的分析。

- **用户流量分析**

按照接口(线路)分析用户的流量，实时监控用户的当前流量状况和使用应用详情，支持对用户流量进行简易调整，从而达到快速限制流量过高的用户。如果您网络内的用户很多，你还可以通过用户名或 IP 地址段可对当前用户进行过滤。点击实时流量页面导航菜单栏中的 

显示如下：

该页面显示了所选线路的在线用户数、会话数、用户流量排行、用户组流量排行、VIP 用户流量排行及用户会话数排行信息。

点击 

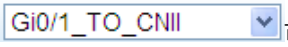
将弹出用户流量明细窗口，详见“2.5.1.1 接口流量分析”章节中的用户流量明细窗口的分析。

用户组流量：是指把用户划分成多个组（例如按班级、部门或楼层来划分），NBR 可以按照这个用户组来查看和管理流量。

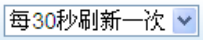
要配置“用户组”请在“用户管理 —□ □ □ □ □ —□ □ □ □ □ □ □ □”□ □ □ □

1.3.6.1.2 VPN 流量

1. 通过该页面可以查看某条线路上通过 VPN 拨号访问网络的用户明细及各 VPN 用户的流量信息。

2. 通过 

可以选择查看某条线路的 VPN 流量使用情况。

3. 通过 

可以选择每隔 10 秒、30 秒、1 分钟刷新一次设备的当前 VPN 流量信息，也可以选择手动刷新设备的当前 VPN 流量信息。

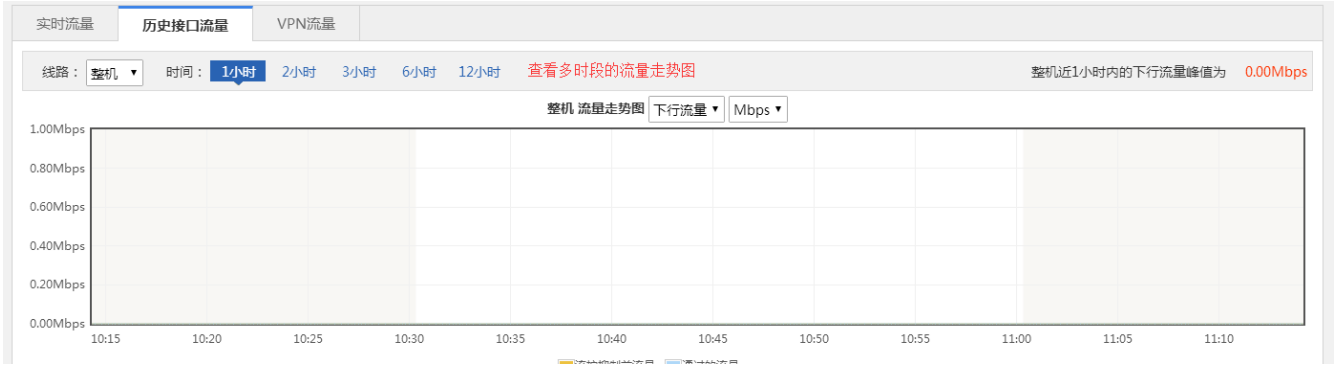
4. 通过 

可以查询某个 VPN 用户在某条线路上的流量使用信息：

输入名称或 IP，选择好接口后，点击 

：

1.3.6.1.3 历史接口流量

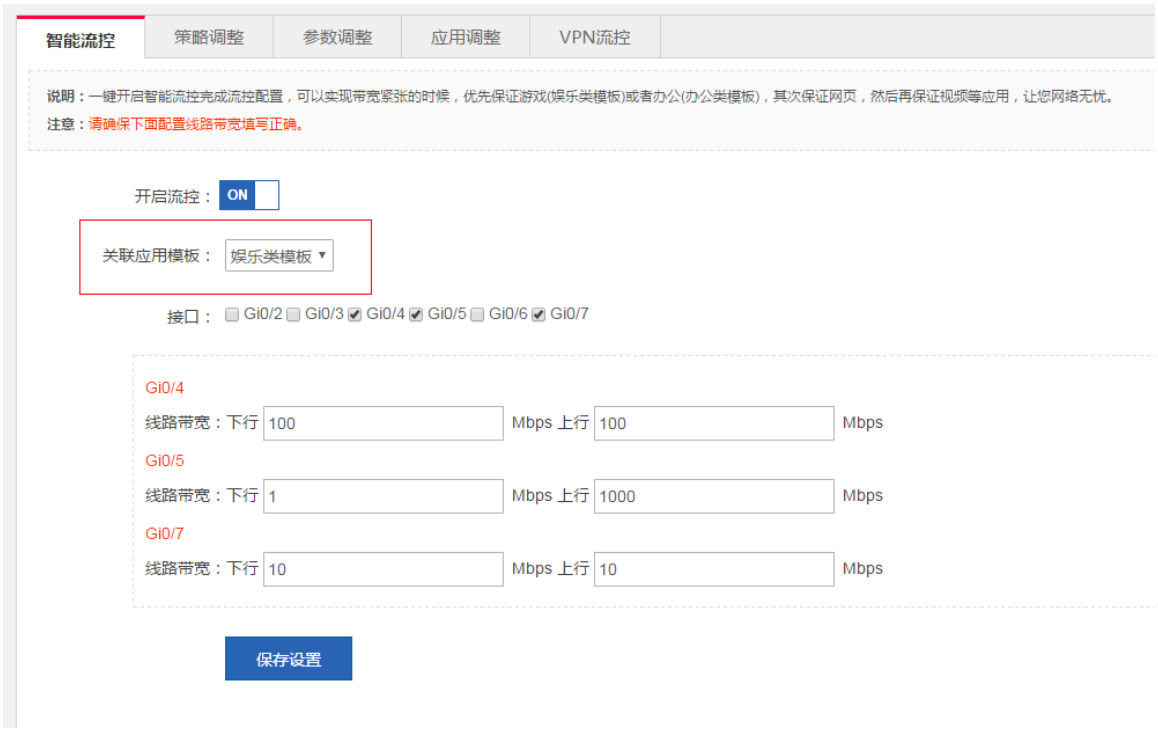


历史接口流量主要查看实时的接口流量和在单位时间的具体的实时曲线图，用户可以查看一天内的实时监测流量曲线

1.3.6.2 流控策略

1.3.6.2.1 智能流控

智能流控设置页面如下图所示：


智能流控
策略调整
参数调整
应用调整
VPN流控
说明：一键开启智能流控完成流控配置，可以实现带宽紧张的时候，优先保证游戏(娱乐类模板)或者办公(办公类模板)，其次保证网页，然后再保证视频等应用，让您网络无忧。
注意：请确保下面配置线路带宽填写正确。
开启流控：
ON
关联应用模板：
娱乐类模板
接口：
Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7
Gi0/4
线路带宽：下行 100 Mbps 上行 100 Mbps
Gi0/5
线路带宽：下行 1 Mbps 上行 1000 Mbps
Gi0/7
线路带宽：下行 10 Mbps 上行 10 Mbps
保存设置

添加了关联应用模块。


智能流控
策略调整
参数调整
应用调整
VPN流控
说明：优先保证游戏，其次保证网页，最后保证视频。
注意：请确保线路带宽填写正确。
开启流控：
ON
流控开关
接口：
Gi0/5 Di1 Di2 Di3 Di4(Gi0/7) Di5(Gi0/6)
选择接口
Gi0/5
线路带宽：下行 10 Mbps 上行 10 Mbps
保存设置

1.3.6.2.2 策略调整

- 新建策略

您可以根据贵公司的网络情况和公司需求，对公司内部网络进行规划管理，也可以对任意用户或应用进行规划管理。

点击 

将弹出“添加策略”的导航窗口

1. 策略名称：在“策略名称”输入框中输入能够标识该规则名称的意图或用途规则名称。

2. 选择应用组：下拉框中选择已有的应用，当不满足需求时可以点击【自定义应用分组】进行配置。

3. 流量限制：独立控制（保证网速、最大网速为策略所限制的某个具体用户在当前接口下使用某个具体应用的最低和最高网速，同时提供每个使用该通道的用户最低和最高网速），共享带宽，不限速。

4. 外网 IP 组：点击【选择IP组】进行选择 IP 组。

5. 生效时间：下拉框中可以选择已有的时间，当不满足需求时，点击【时间管理】自行配置

- 查看策略

新建策略后，将在页面表格中显示当前设备已配置的所有流控策略，并可以对现有策略进行修改和删除，如下图所示：

1. 点击“应用组”栏中的 按钮，可以查看某个应用组包含的应用信息。

2. 开启/关闭：支持针对全部规则或具体单条规则的开启和关闭。该功能影响规则的"当前状态"为生效或禁用。

3. 状态：包括"生效"、"不生效"、"禁用"三种状态，"生效"、"禁用"状态受规则的开启与否控制，若当前时间不在"生效时间"的时候，规则的当前状态显示为"不生效"状态。

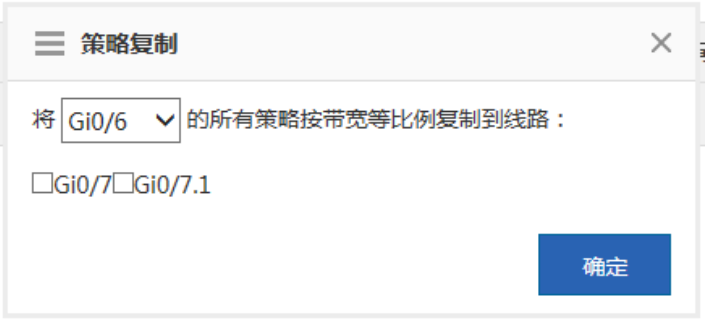
4. 匹配顺序：流控策略适应"后配先生效"原则，本列表按照第一条规则置顶的排序方式进行排列，可以直接点击 、 按钮对现有策略的优先级进行调整；

5. 点击 编辑 会弹出编辑对话框，可以会策略进行编辑修改。

6. 点击 删除 可以删除策略。

- 复制策略

点击 复制 按钮，可以将某个线路的流控策略复制到另一个线路：



1.3.6.2.3 参数调整

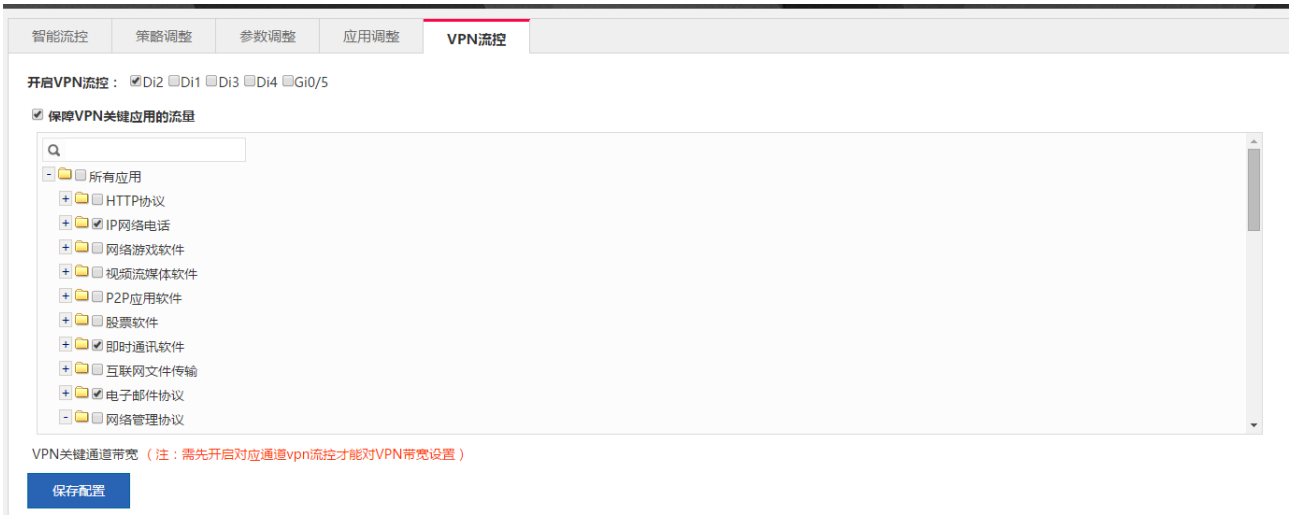
可根据具体情况进行各个接口参数调整。


智能流控
策略调整
参数调整
应用调整
VPN流控
提示：以下速率的单位统一为Kbps。优先级值越小，优先级越高
Gi0/6
Gi0/5
当前利用率：0%
紧张阈值：0%
范围（1%~99%）
预留带宽（范围：1%~80%）
上行（总带宽10M）：20%
下行（总带宽10M）：15%
修改
类型
优先级
速率（下行/上行）
上行承诺值
上行最大值
下行承诺值
下行最大值
上行每用户最小值
上行每用户最大值
下行每用户最小值
下行每用户最大值
操作
关键/保证类 0 0/0 6,000 10,000 6,000 10,000 -- 5,000 -- 5,000 编辑
普通/其他类 4 0/0 2,000 10,000 2,000 10,000 -- 3,000 -- 3,000 编辑
抑制类 7 0/0 1,000 10,000 1,000 9,000 -- 3,000 -- -- 编辑

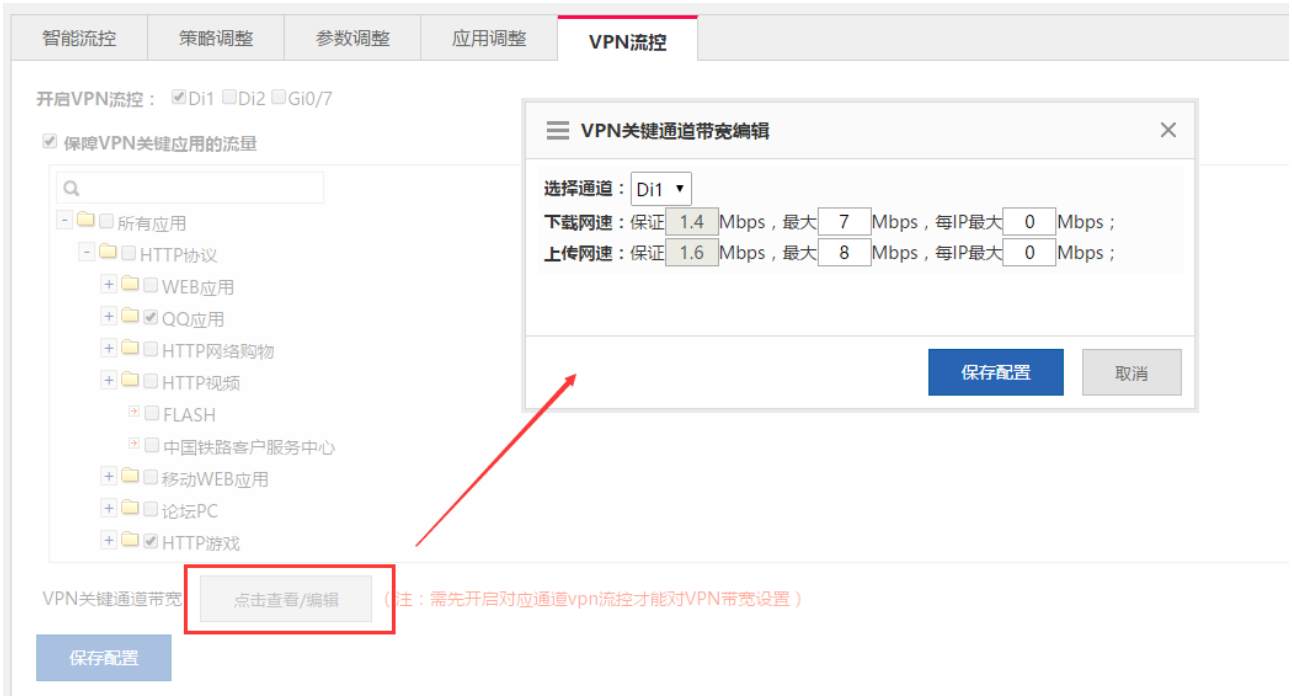
1.3.6.2.4 应用调整


智能流控
策略调整
参数调整
应用调整
VPN流控
说明："普通/其他类"属于默认分组，不能操作默认分组中的应用
重置办公应用模板
重置娱乐应用模板
应用分组名称
选择应用
管理
关键/保证类 即时通讯软件,IP网络电话,电子邮件协议,DNS,ICMP-DETAIL,VPN应用 编辑
网页类 HTTP协议,普通网页浏览明细,WEB_MOBILE 编辑
在线视频类 HTTP视频,视频|影音_MOBILE 编辑
影视娱乐类 视频流媒体软件 编辑
常用下载类 HTTP下载,下载工具_MOBILE,网络硬盘,FTP,快牙,TFTP,NNTP,IXIA,SVN,SMB,网盘_MOBILE 编辑
P2p下载类 P2P应用软件,软件更新 编辑
应用更新类 游戏更新,网吧游戏服务器 编辑
常用上传类 HTTP上传 编辑
抑制类 WEB应用,网络游戏软件,社交_MOBILE 编辑
阻断类 非法DNS 编辑
普通/其他类 股票软件,互联网文件传输,网络管理协议,路由协议,远程访问协议,网银,即时通讯_MOBILE,游戏_MOBILE,其他_MOBILE,证券_MOBILE,RFC,IP-RAW,IP协议组 默认组不能编辑
显示: 15
首页 上一页 1 下一页 末页 1 确定

1.3.6.2.5 VPN 流控



配置好接口后，可以点击查看编辑按钮



1.3.6.3 对象定义

对象定义配置页面：

1.3.6.3.1 自定义应用分组

该页面显示了当前系统已存在的所有应用分组以及每个应用分组包含的应用。其中关键/保证类、抑制类、阻断类、普通/其他类为系统定义的应用分组，其他为用户自定义的应用分组。

- **应用分组**

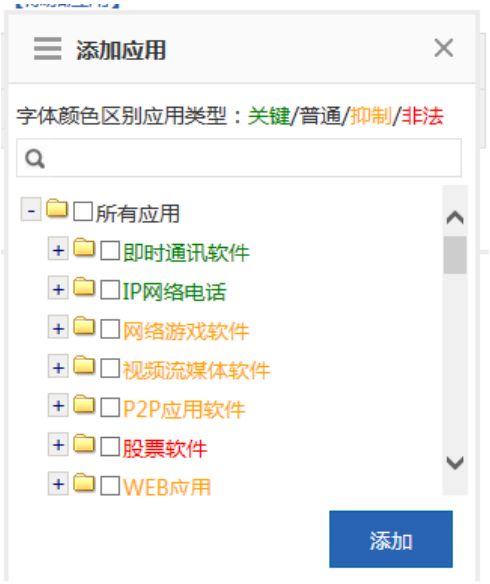
设置应用分组主要是方便用户统筹管理公司内部协议的使用情况，确保公司内部网络流畅且带宽不被浪费于无关的工作上。

1. 新增自定义应用分组：

点击 

按钮可以自定义应用分组：

在“应用组名”输入框中输入应用分组名称，点击【添加应用】按钮：



勾选要加入该自定义应用分组的应用，点击 添加 按钮，已勾选的应用将显示在下方的表格中：

点击 删除 按钮可以将某个应用从该应用分组中删除。

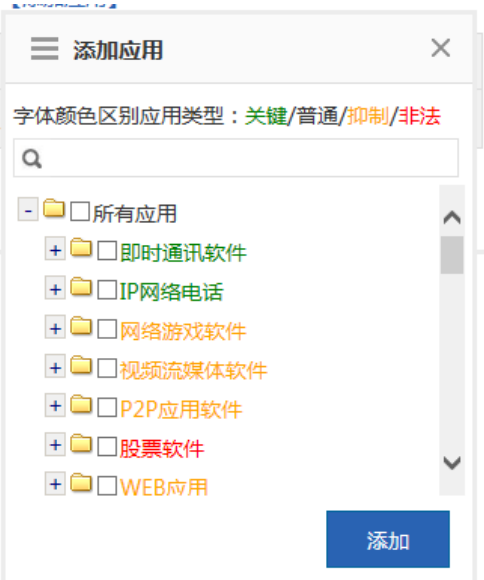
点击 保存 按钮即可完成自定义应用分组的配置，配置完成的应用分组信息将显示在自定义应用分组主页面的表格中：

2. 编辑应用分组：

点击自定义应用分组主页面表格中的 按钮可以重新分配某个应用分组包含的应用：

点击【添加应用】按钮可以往该应用分组中添加应用，点击 删除 可以将某个应用从该应用分组中删除。

点击【添加应用】按钮将弹出以下窗口：



其中绿色字体的说明已经被选择为关键/保证类应用，橙色字体的说明已经被选择为抑制类应用，红色字体的说明已经被选择为阻断类应用，黑色字体的则是被选择为普通/其他类应用组、或未被选择而统一归类到普通/其他类应用组的应用。

已被选择为关键/保证类或抑制类或阻断类的应用，不能加入到这三个应用分组中的另两个应用分组。

如果需要修改，假设需要将 抑制类应用 修改为 关键/保证类应用，那么需要先编辑抑制类应用分组，将要修改的应用从抑制类应用分组中删除，再编辑关键/保证类应用分组，将此应用添加至关键/保证类应用分组中。

3. 删除应用分组：

点击自定义应用分组主页面表格中的 

按钮可以删除某个自定义应用分组，系统应用分组（即关键/保证类、抑制类、阻断类、普通/其他类）不可删除。

- **自定义应用**

除了系统内建的网络应用协议，您还可以自己定义其他网络应用，如基于某个端口的应用，或基于某个目标服务器的应用。自定义协议和系统内建的其它协议一样，可用于策略中的网络应用控制、带宽管理，并可进行网络应用实时监控等。

注意：自定义协议优先级最高，即当自定义协议与系统内置协议冲突时（如端口相同），系统识别为用户自定义的网络应用协议。

点击自定义应用分组主页面的 

按钮将弹出自定义应用配置窗口：

创建自定义应用对象：输入自定义应用名称、选择协议类型、选择规则类型、应用所属分类（可以自己另外定义应用分类，也可以基于内建应用分类）、根据选择的规则类型输入源或目的端口、源或目的 IP，点击 添加设置 配置成功。

编辑自定义应用：选择需要修改的应用，点击 编辑 按钮即可修改。

删除自定义应用：选择需要删除的应用，点击 删除 即可。

- **反馈无法识别的应用**

如果您发现某个网络应用程序的流量无法被本设备正确识别，导致您无法对该应用进行有效控制，您可以点击 反馈无法识别的应用 按钮，根据弹出窗口中提供的方式反馈给我们，锐捷云中心将对您反馈过来的应用进行分析，并加入到特征库中，以满足您的使用需要！

1.3.6.3.2 时间对象

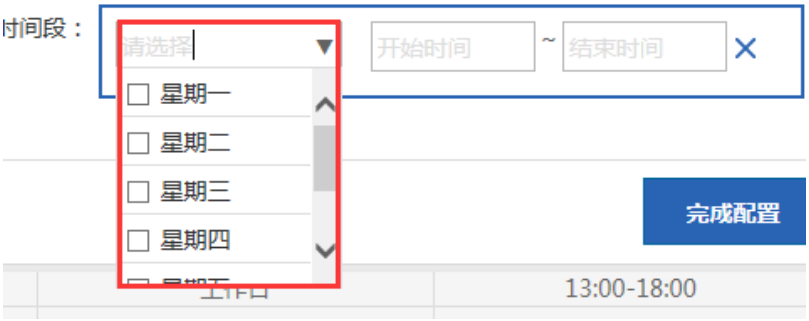
可以定义时间对象，用于策略设置时候使用。

1. 添加时间对象：点击 添加时间对象 ，在弹出窗中输入对象名称，选择时间段，支持设置多个时间段。

例如新建一个 工作时间 对象：

（1） 对象名称：在对象名称 对象名： * 输入时间对象名称；

（2） 时间段周期：选择时间段的周期，即选择每周从周一到周日



（3） 时间段：设置时间段

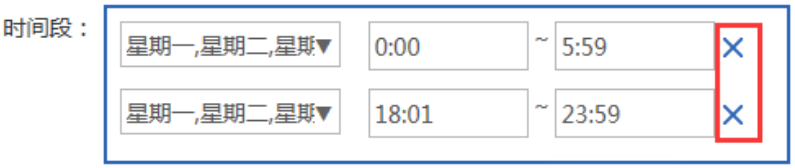
（4） 点击添加另一个时间段

完成后点击 完成配置 按钮生成一个时间对象：

2. 编辑时间对象：选择需要编辑的时间对象点击 编辑 按钮，在弹出窗中即可添加，删除，修改对应的时间段。

3. 删除时间对象：若需要某个时间对象，在列表中选择该时间对象，点击 删除 按钮即可。

4. 删除时间段：若需要删除某个时间对象的某个时间段，在列表中选择对应的时间对象，点击编辑在弹出窗中选择需要删除的时间段，点击 ✕ 按钮，可以删除某个时间段。



1.3.6.3.3 外网 IP 对象

外网 IP 对象是相对与您内部往来而言的外部服务器地址或其他 IP 地址。例如：贵公司的 OA 或业务系统的服务器不在内部是放在电信机房或托管中心 ;这个时候您为了保证内网用户访问这些服务器的网速那么您就可以将这个服务器地址配置为外网 IP 对象，然后在流控策略配置的时候对其带宽进行保底！

系统默认存在一个默认对象“/”，当启用二三层分类识别时，报文目的 ip 地址匹配不中其他任意一个网络对象则默认匹配中默认对象“/”。

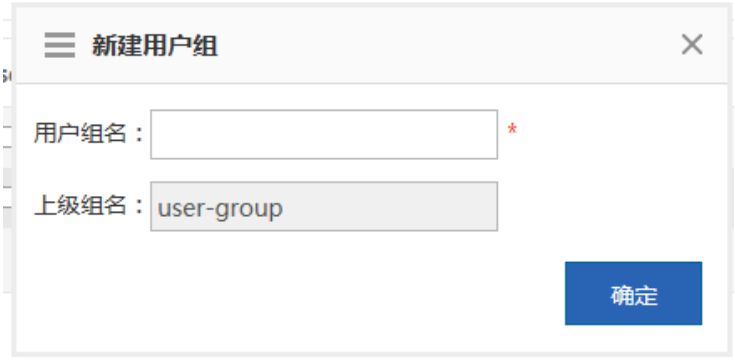
外网 IP 对象配置页面：

左侧的树状图是当前外网 IP 对象的组织结构，选中某个外网 IP 对象，会在右侧显示该对象的相关信息，并可以编辑、修改。

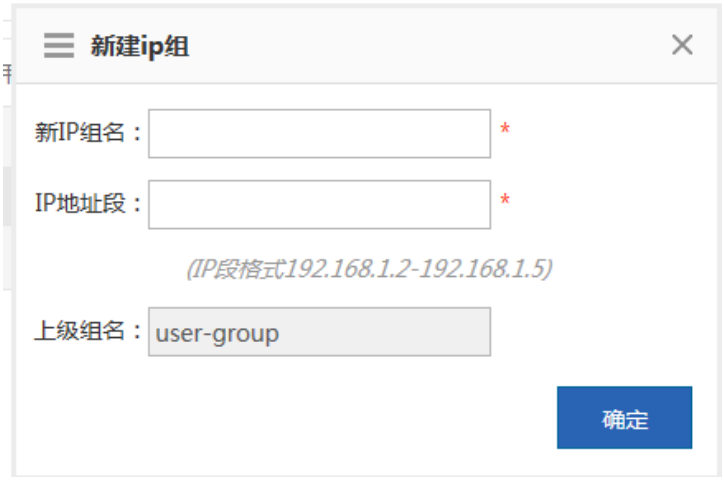
1. 点击 编辑组 按钮，可以对选中的外网用户组或外网 IP 组进行编辑，修改外网用户组或外网 IP 组名称：

2. 点击 删除组 按钮，会将选中的外网用户组或外网 IP 组从外网 IP 对象的组织结构中删除。

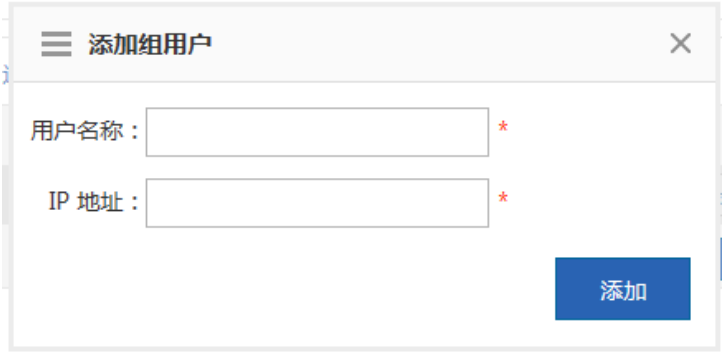
3. 点击 新建子组 按钮，可以在选中的外网用户组下新建子外网用户组：



4. 点击 新建IP子组 按钮，可以在选中的外网用户组下新建 IP 组：



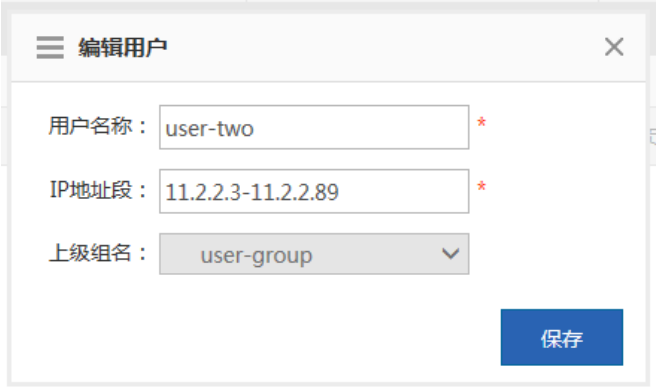
5. 点击 添加用户 按钮，可以为选中的外网用户组或外网 IP 组添加用户成员：



6. 外网用户组或外网 IP 组的用户列表：

以上表格列出了您在左侧选中的外网用户组或外网 IP 组底下的所有用户，你可以对用户进行编辑和删除操作。

点击 编辑 弹出编辑用户的对话框，支持修改用户名称、IP 范围和归属组（移动用户到其他外网用户组）：



点击 删除 即可将用户从选中的外网用户组或外网 IP 组中删除，也可以选择多个用户，点击 删除选中用户 删除。

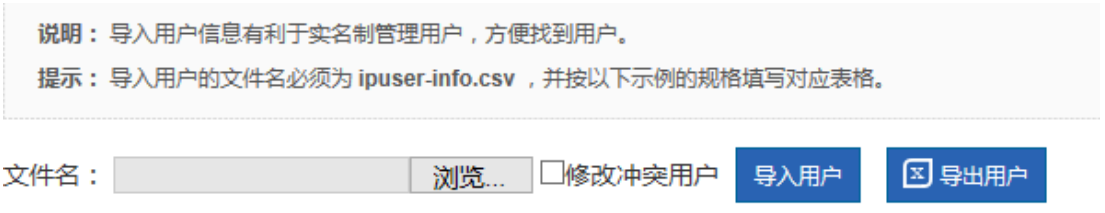
7. 导入导出

支持用户通过文件导入导出外网 IP，点击 批量导入导出外网ip 弹出以下窗口：

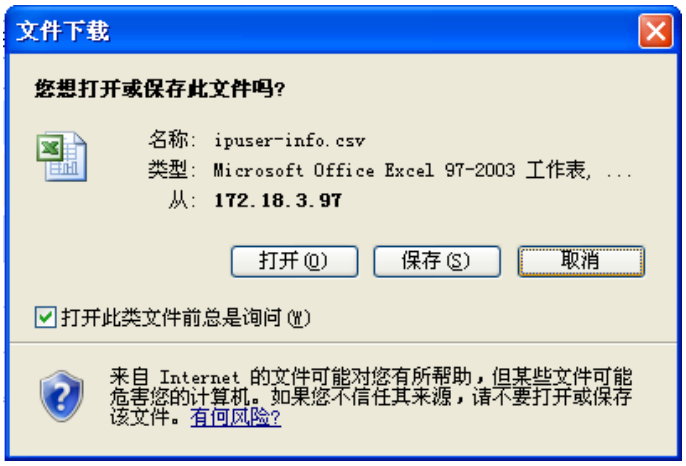
导入外网 IP：通过文件导入外网 IP，方便管理员一步完成外网 IP 的编辑。在本地新建一个表格 ipuser-info.csv，在表格内部按照以下格式输入外网 IP 的信息：

归属用户组	用户名称	IP地址
/人力资源部	张三	192.168.1.59
/财务部	李四	192.168.1.9
/研发部/研发5部	王五	192.168.1.29

点击 浏览... 按钮，找到文件 ipuser-info.csv，点击 导入用户 按钮，会出现文件导入进度条，待进度条加载完成说明文件已经上传成功。



导出外网 IP：点击 导出用户 按钮会弹出如下图对话框。点击 保存(S) 选择保存路径即可。



1.3.6.3.4 VLAN 对象

VLAN 对象之间的 VLAN ID 不能冲突，多个 VLAN ID 之间用逗号隔开，如需配置多个连续的 VLAN ID 属于同一个 VLAN 对象，可用“-”隔开起始 VLAN ID 和结束 VLAN ID 表示多个连续的 VLAN ID。

默认存在一个默认 VLAN 对象“any”，开启二三层分类识别功能时，在网关模式下所有数据流默认匹配中默认对象“any”，网桥模式下所有的数据流默认匹配中桥的 native VLAN 所对应的 VLAN 对象，若网桥的 native VLAN 没有对应的 VLAN 对象，则数据流匹配中默认对象“any”。

VLAN 配置页面如下图所示：

1. **新建 VLN 对象**：只需输入 VLAN 对象名称和 VLAN 对象 ID，点击 添加设置 按钮，就添加一个 VLAN 对象了：

2. **编辑 VLAN 对象：**只需选择需要编辑的 VLAN 对象点击 编辑 按钮即可修改。例如要编辑 vlan1 对象，点击 编辑 按钮后，修改 VLAN 对象名称或 VLAN 对象 ID 后，点击 保存编辑 按钮即可：

3. **删除 VLAN 对象：**只需选择需要删除的 VLAN 对象点击 删除 即可。例如：先要删除 vlan1 对象则主要点击后面的 删除 删除 即可。如果需要全部删除 VLAN 对象则点击 ✕删除全部 按钮。

1.3.6.3.5 IP 对象

添加了批量导入 IP 对象的功能。

4. **添加 IP 对象组：**在弹窗中输入对象组 ID，对象组描述，地址库，对象了吧等信息后，点击 确定 按钮完成配置。

5. **删除 IP 对象组：点击** 删除IP对象组 **按钮时，可以直接删除 IP 对象列表选中的对象组。**

6. **添加 IP 对象：点击** ＋添加IP对象 **，可以在该 IP 组下添加 IP 对象。**

7. **删除选中 IP 对象：点击** ✕删除选中IP对象 **，可以删除表格选中的 IP 对象。**

8. **编辑 IP 对象：点击** 编辑 **，对该行的 IP 对象进行编辑操作。**

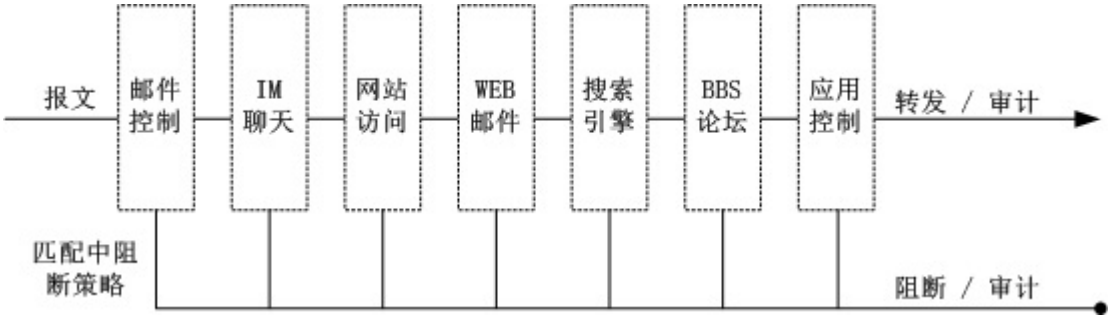
9. **删除 IP 对象：点击** 删除 **，对该行的 IP 对象进行单独删除操作。**

1.3.7 行为管理

1.3.7.1 行为策略

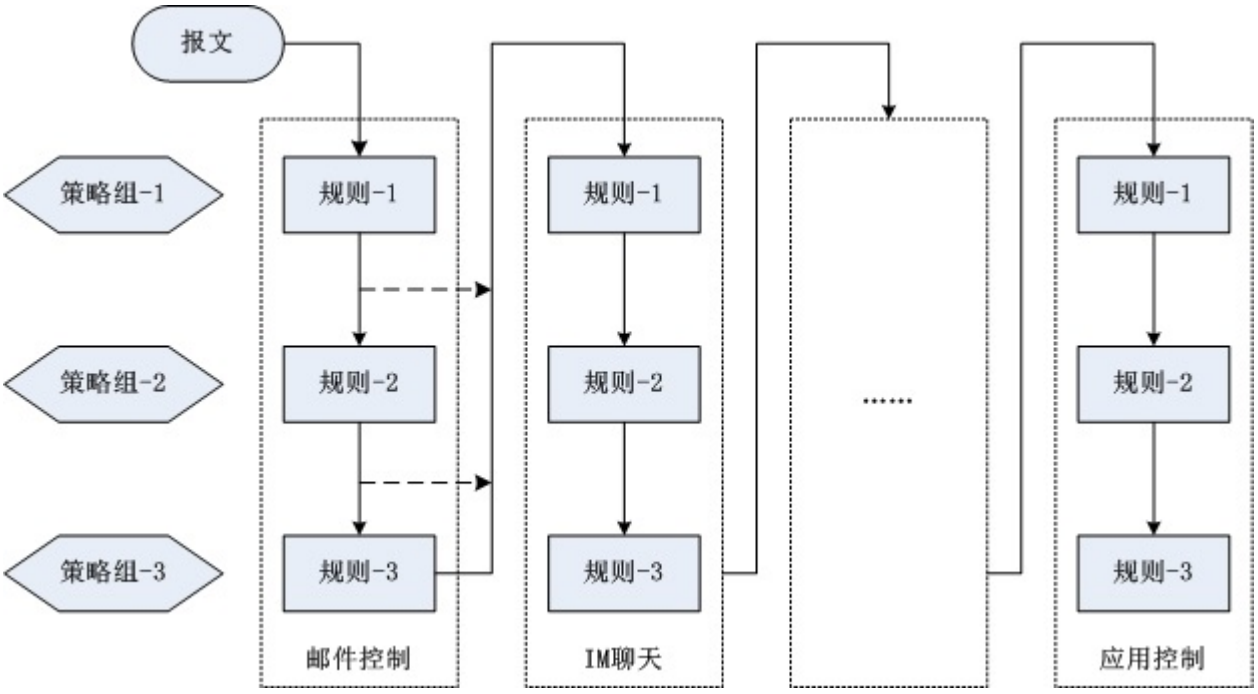
行为策略模块能够对用户行为进行访问审计、监控、配置策略等操作，不仅能够为用户提供所需的访问审计信息、同时提供管理员对用户行为进行管理的功能，引导用户正确的网络行为及时间分配，阻隔不良信息对于用户的影响。

行为管理各项功能的策略匹配是有顺序的。
如果第一种类型的行为管理业务没有对报文进行阻断，则报文会进入下一种行为管理业务继续处理；如果有一种行为管理业务对报文进行了阻断，则不再进入下一种行为管理业务处理。各行为管理业务的处理顺序如下：



图：各行为管理业务的处理顺序

行为策略的匹配顺序则按照策略组和规则的优先级顺序依次进行匹配：



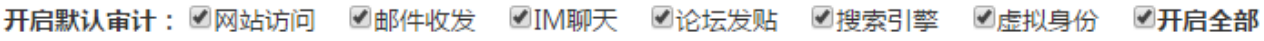
图：策略和规则的优先级匹配顺序

1.3.7.1.1 简易配置

在简易配置页面，您可以开启或关闭网站访问、邮件收发、IM 聊天、论坛发帖、搜索引擎等的默认审计功能，还可以对某些特定用户、特定应用、特定网站、特定文件类型进行特殊处理，如直接过滤或者免审计。

- **开启默认审计**

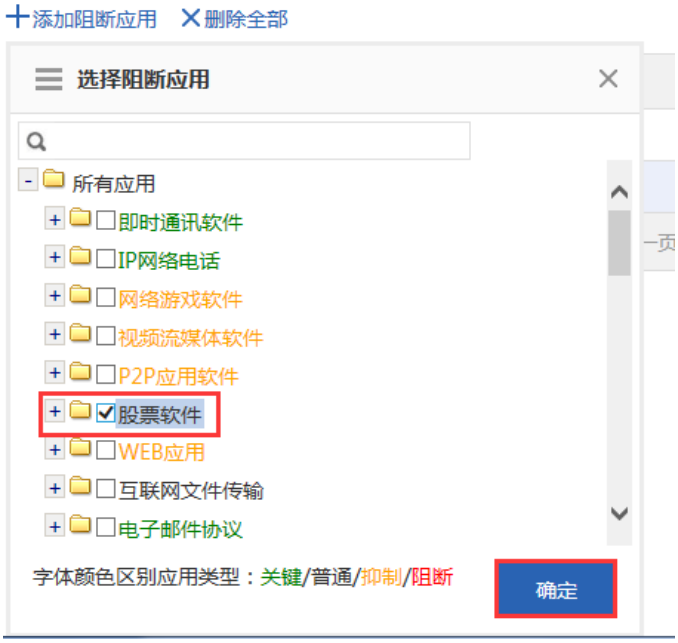
开启对应功能的默认审计后，设备将审计该类型的所有上网记录，如开启“搜索引擎”的默认审计，则用户所的有搜索记录都将被审计下来，反之只审计能匹配中行为策略的上网记录：



- **禁止应用**

点击 禁止应用 按钮将弹出以下窗口，通过这个窗口您可以查看当前哪些应用被禁止了，并可以添加或删除要禁止的应用：

点击 添加阻断应用 弹出以下窗口：



勾选需要禁止的应用，如“股票软件”， 点击 确定 按钮将选中的应用加入禁止应用列表：

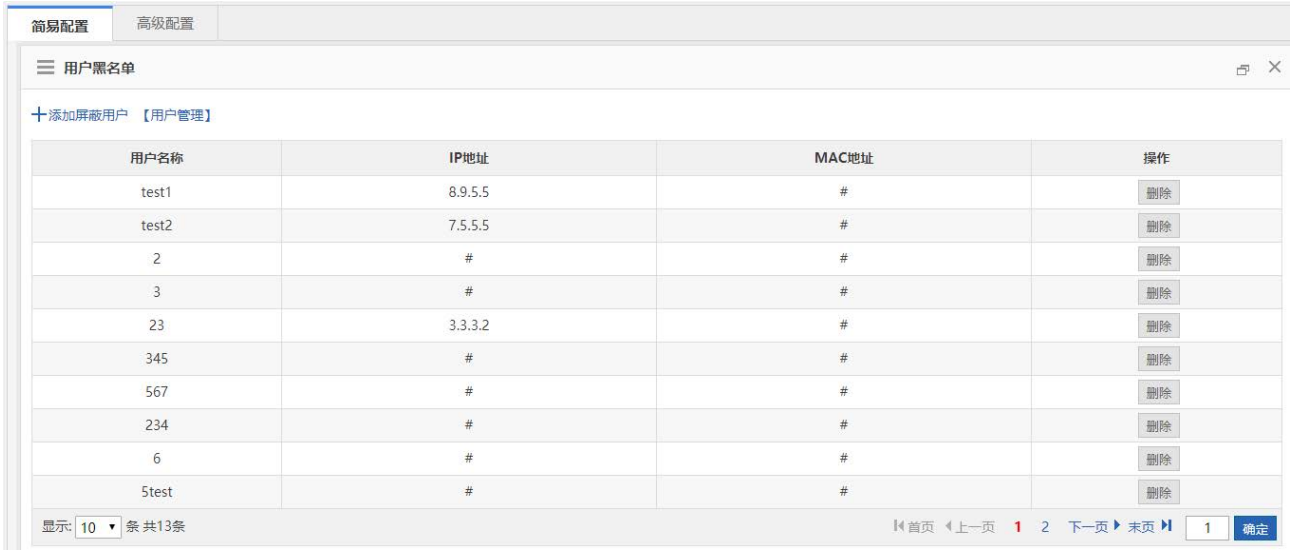
点击 按钮可以将单个应用从禁止应用列表中删除；

点击 删除全部 按钮可以将所有应用都从禁止应用列表中删除；

开启应用禁止功能后，设备禁止任何用户运行该列表中的应用软件。

- **禁止用户**

点击 按钮将弹出以下窗口，通过这个窗口您可以查看当前哪些用户被禁止了，并可以添加或删除要禁止的用户：



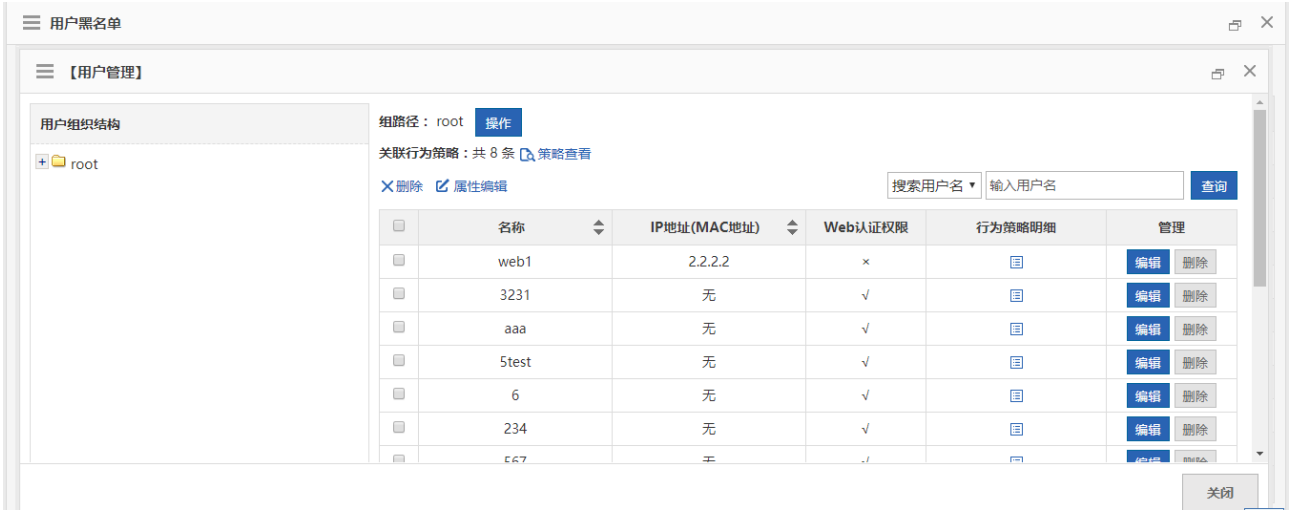
点击 添加屏蔽用户 按钮，将弹出以下窗口：

勾选需要禁止的用户，点击 确定，将选中的用户加入到屏蔽用户列表：

点击 删除 链接可以将某个用户从屏蔽用户列表中删除；

开启用户禁止功能后，设备将阻断屏蔽用户列表中的用户上网行为。

点击 【用户管理】，显示页面如下



- **免审计用户**

点击 免审计用户 按钮将弹出以下窗口，通过这个窗口您可以查看当前哪些用户设备不做审计，并可以添加或删除免审计的用户：

点击 添加免监控用户 按钮，将弹出以下窗口：

勾选需要免审计的用户，免审计用户默认免流控，若需要对所选用户进行流控，则只免审计不免流控 要打勾，点击 确定 添加到免监控用户列表：

“是否免监控”栏中，√ 表示该用户免流控，× 表示该用户需要流控；

点击 删除 可以将某个用户从免监控用户列表中删除；

免审计功能开启时，设备不会审计免监控用户的上网记录，如果勾选“只免审计不免流控”则流控策略中的限速规则还是会作用到免监控用户。

- **禁止网站**

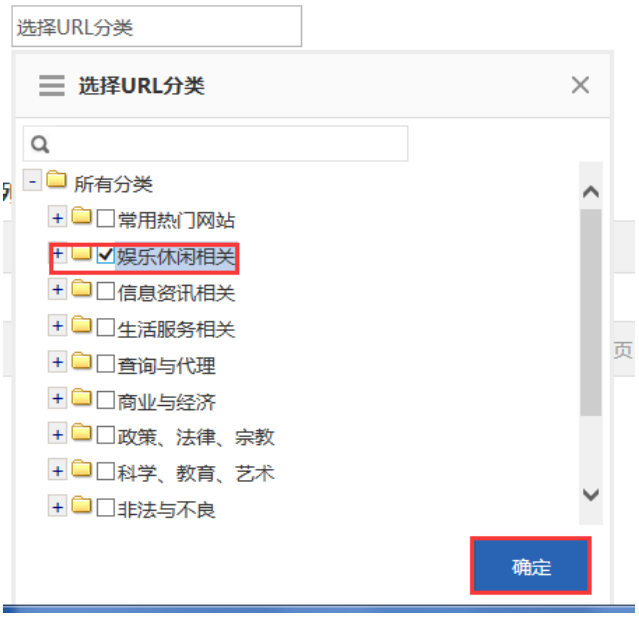
点击 禁止网站 按钮将弹出禁止网站配置窗口，通过该窗口您可以查看当前哪些网站会被设备阻断，并可以添加或删除需要禁止网站

该功能有两种模式：黑名单模式和白名单模式。

1. 黑名单模式：只有黑名单网站列表下的网站才会被设备阻断，其它网站全部放行：

（1） 添加禁止网站：有两种方式：选择已有的 URL 分类，或直接输入网址。

1) 选择已有的 URL 分类：如上图所示，点击“选择 URL 分类”后面的输入框，将弹出如下窗口，勾选需要禁止的 URL 分类，点击 确定 即可：



2) 直接输入网址：如下图所示，在“输入网址”输入框中输入需要禁止的网站地址，点击 添加设置 按钮即可。

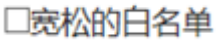
（2） 删除禁止网站：选择需要解除禁止的网站，点击 删除 按钮即可。

2. 白名单模式：只有白名单网站列表下的网站才能访问，其他网站将被设备阻断。

（1） 添加白名单网站：同样有两种方式，选择已有的 URL 分类，或直接输入网址。添加操作同添加黑名单网站，这里不再赘述。

（2） 删除白名单网站：选择需要禁止的网站，点击 

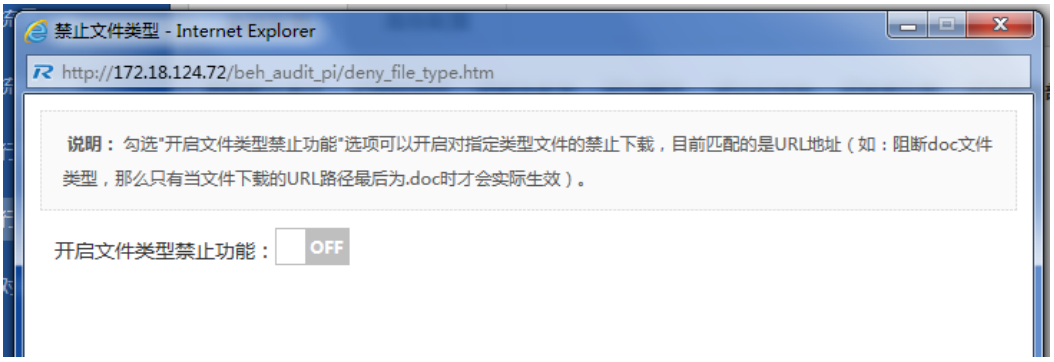
按钮即可。

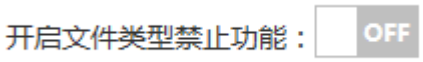
（3） 宽松的白名单：选中 

，则从“白名单网站”发起的相关 URL 请求都会被放行。如：www.ruijie.com.cn 是白名单网站，那么在该网站页面上的所有链接都会被允许访问。

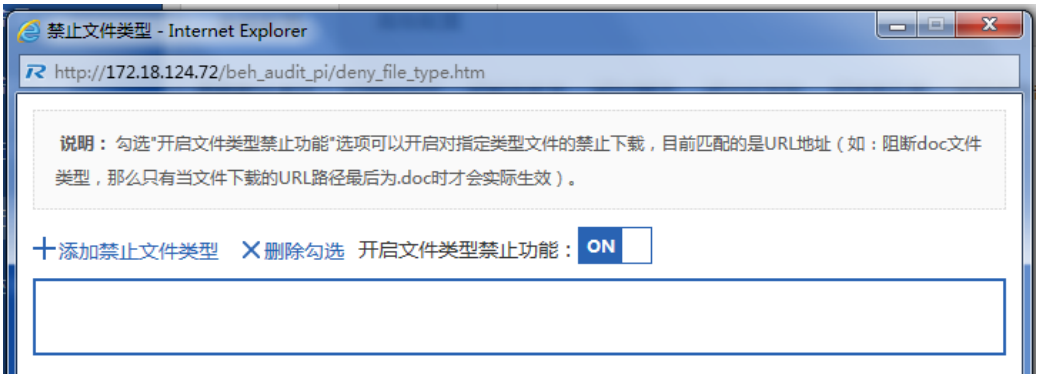
- **禁止的文件类型**

点击 禁止的文件类型 按钮将弹出以下窗口，通过这个窗口您可以查看当前哪些类型的文件资源会被设备阻断，并可以添加或删除需要禁止的文件类型：



勾选 

开启文件类型禁止功能：



点击 

，添加需要禁止的文件后缀名，多个后缀名以“，”分隔：

输入需要禁止的文件后缀名后，点击 

将后缀名添加到已禁止文件类型列表中：

点击 ✕删除勾选 按钮，可以将未勾选的文件类型从已禁止文件类型列表中删除。

开启文件类型禁止功能后，设备禁止对指定类型的文件上传下载。

- **不审计的网站**

点击 不审计的网站 按钮将弹出以下窗口，通过这个窗口您可以查看当前哪些网站不会被设备审计，并可以添加或删除不做审计的网站：

勾选 开启功能： ON 开启网站不审计功能：

点击 ＋添加不审计网址 在弹出窗中输入不做审计的网址，点击确定将网址加入到不审计网站列表中；

点击 删除 可以将某个网站从不审计网站列表中删除；

点击 ✕删除选中 可以将选中的网站批量从不审计网站列表中删除；

打开该功能后，这里配置的网站的访问不会被设备审计，也不会被阻断。

- **禁止客户端邮件**

点击禁止客户端邮箱，将弹出以下窗口，您可以通过该功能来添加一个禁止的邮箱帐号，配置完成后该邮箱帐号将无法发送接收邮件：

- **禁止 QQ 帐号**

点击 ，将弹出以下窗口，您可以通过该功能来添加一个禁止的 QQ 或 MSN 聊天帐号，配置完成后该帐号将无法发送接收消息：

1.3.7.1.2 高级配置

通过互联网传递信息已经成为企业（机关）的关键应用，然而信息的机密性、健康性、政治性等问题也随之而来。

锐捷网络的 NBR 设备全新为您制定了精细化的信息收发监控和审计，有效控制关键信息的传播范围，以及避免可能引起的法律风险。

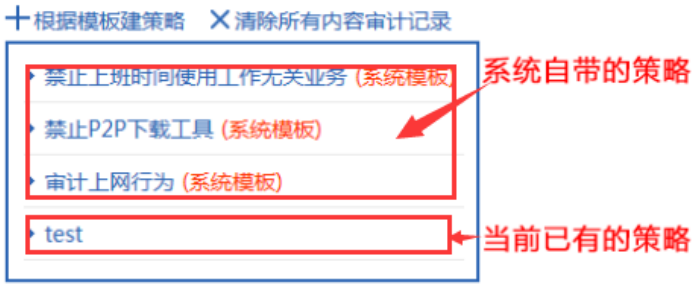
锐捷网络 NBR 设备支持对 Email、Webmail、BBS、IM、WEB-SEARCH、FTP、TELNET、WEB 页面内容等信息传递渠道的监控能力，例如可以对邮件内容、聊天内容、发贴内容等进行全面的审计。

高级配置页面如下：

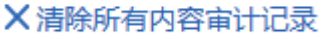
通过该页面，您可以管理和配置应用控制策略、网站访问策略、邮件审计策略、聊天审计策略、论坛发帖策略、搜索引擎策略。

其中点击 

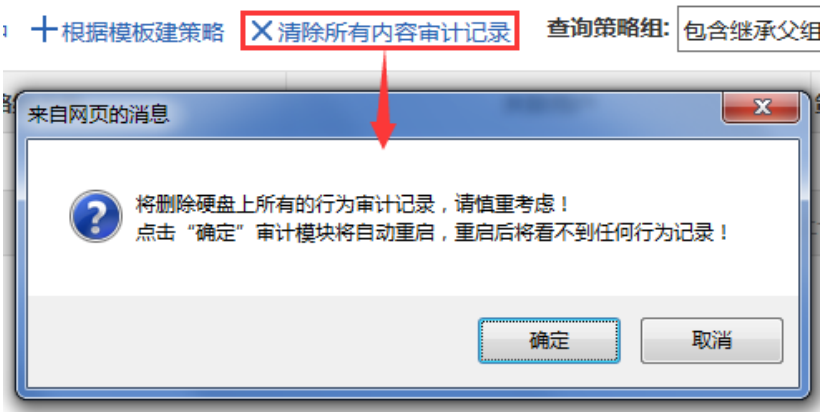
，可以基于现有的策略基础上创建新的策略。如下图所示：



选择现有策略后会弹出策略新建窗口，新策略中默认带有选中的策略规则。具体请参考下面章节。

点击 

将会清空设备上所有的行为审计记录。操作如下：



- **新建和编辑策略**

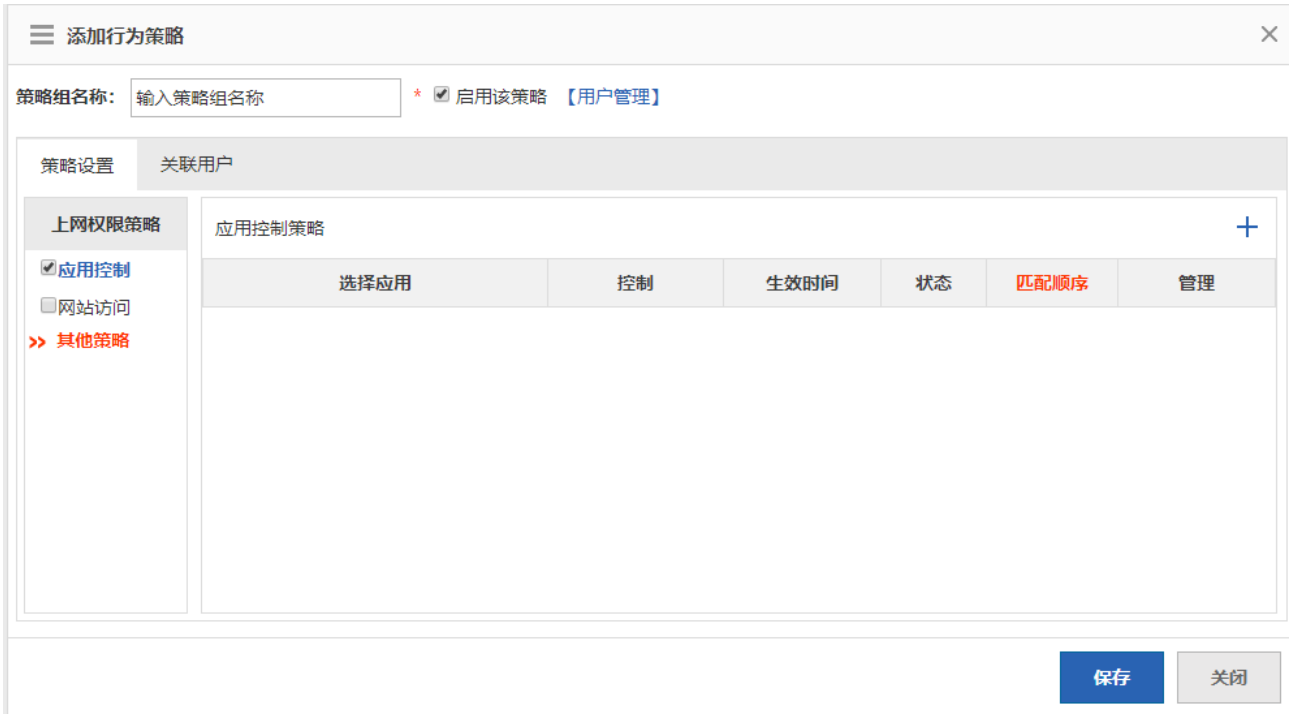
要创建行为策略请参考如下步骤：

1. 点击 

弹出“添加行为策略”配置向导窗口。

2. 策略组名：在“策略组名称”中输入能够标识该策略的规则或用途的名称；

3. 行为控制：选择要应用到该策略的行为规则，可以同时选择多个行为规则，界面如下图所示：



点击左侧的规则名称可以查看该类型下的所有规则，如果要编辑则要选中前面的复选框 

然后进行编辑、删除、添加操作。最后点击“完成”保存。各个类型的添加界面请参考下面章节。

控制规则说明：

允许并审计：不阻断选中用户的上网行为，但会记录上网信息。

允许但不审计：不阻断选中用户的上网行为，也不记录其上网信息。

阻断并审计：阻断选中用户的上网行为，同时记录下阻断信息。

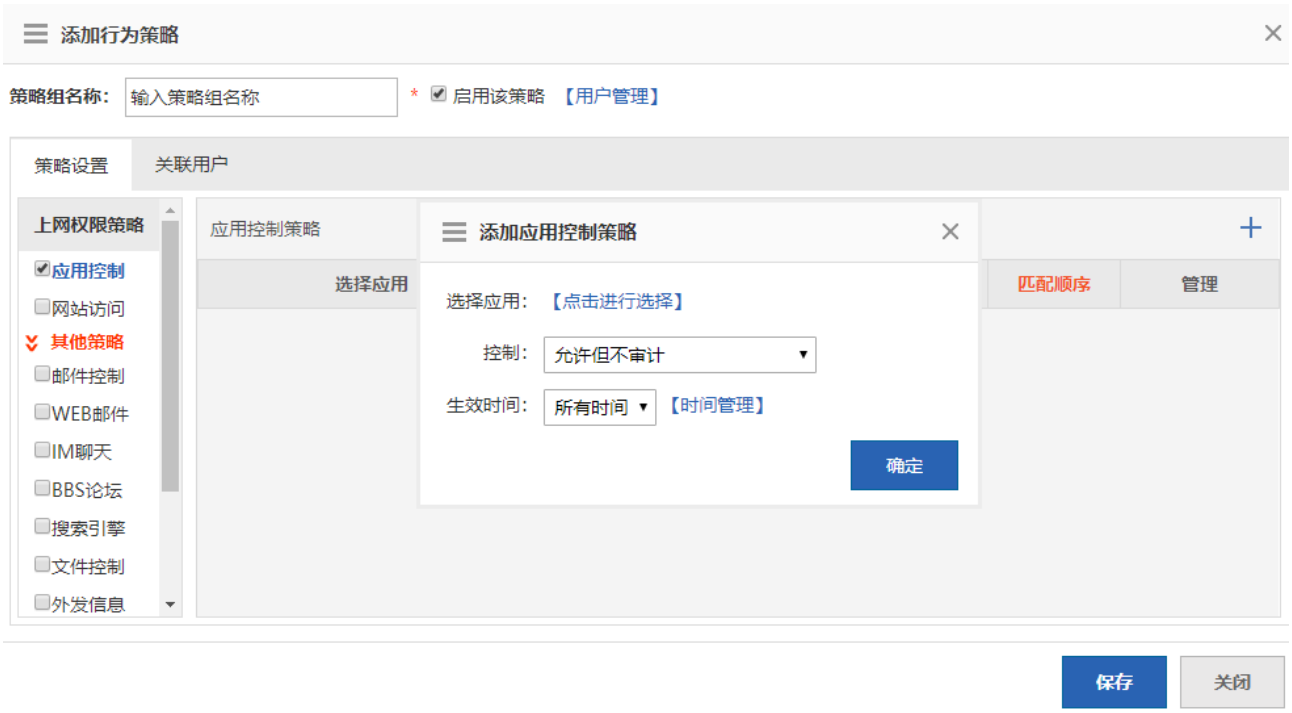
阻断但不审计：阻断选中用户的上网行为，但不记录其阻断信息。

生效时间：这条规则的生效时间，只有在生效时间内该规则才有作用。

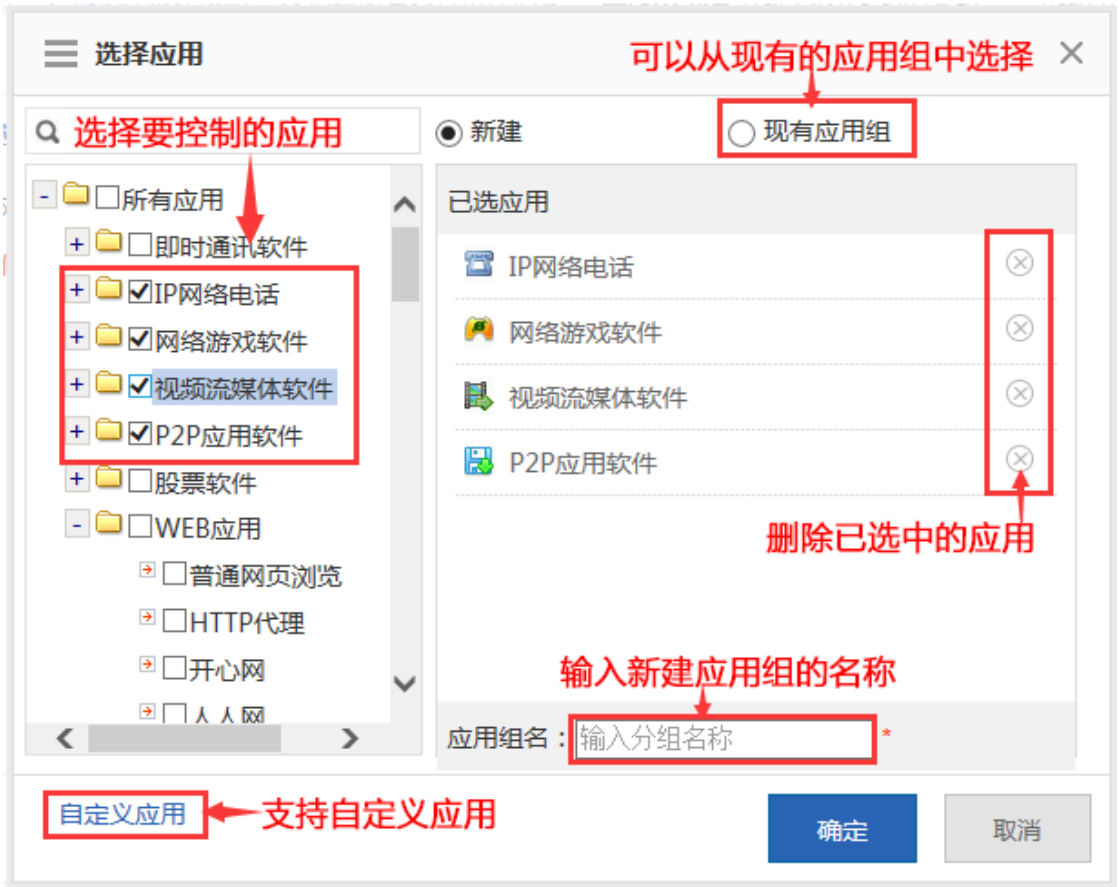
4. 关联用户：选择该策略要对哪些用户生效，可以是本地用户或外部用户，外部用户是指通过第三方认证登录进来的用户，如 VPN 和 WEB 认证用户。

- **应用控制**

应用控制主要针对各种应用的网络行为进行监控，根据需要放行或阻断相应的应用数据流，并对控制行为进行审计。要创建应用控制策略请参考如下步骤：



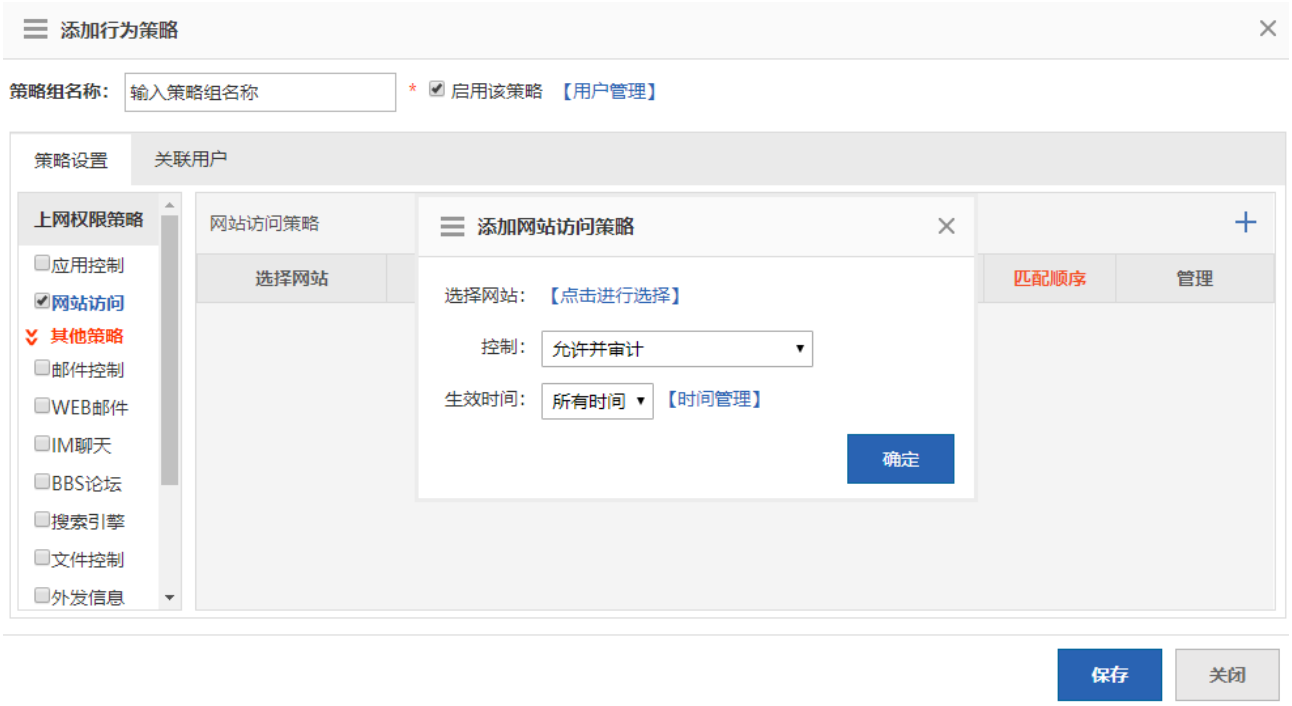
点击“选择应用”输入框将弹出如下界面：



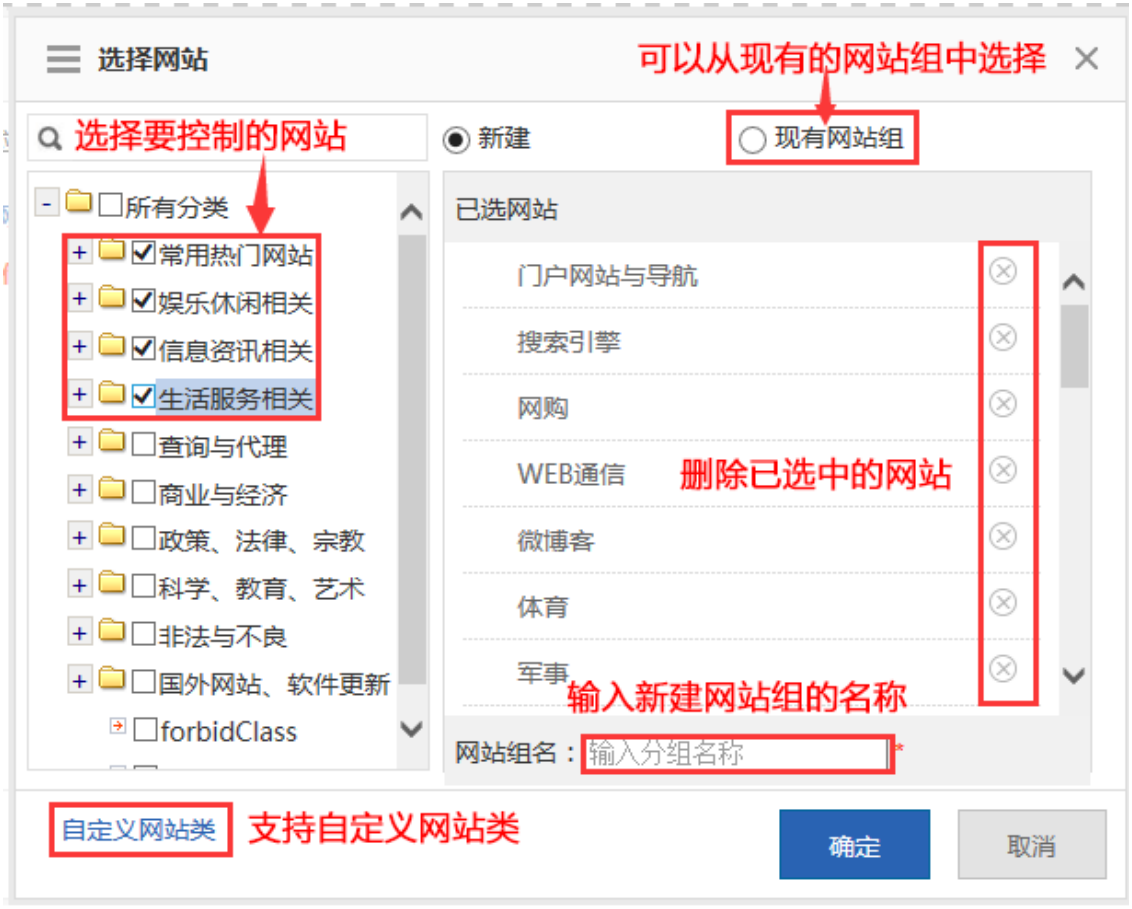
这里有可以选择新建应用组，或从现有的应用组中选择，如上图所示；需要新建应用组时，先选中要控制的应用，然后在“应用组名”中输入新创建的名称，最后点击“确定”。

- **网站访问策略**

主要针对 URL 访问进行监控，对内网发起的 URL 访问进行分类和审计，并根据需要对相应的 URL 访问进行阻断或放行。配置页面如下：



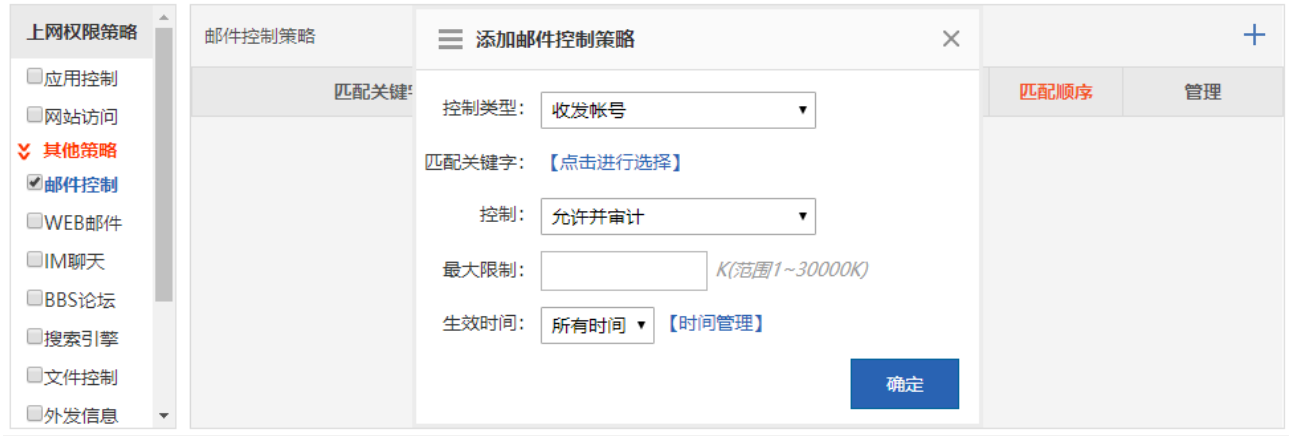
点击“选择网站”输入框将弹出如下界面：



左侧树状图是当前系统已配置的 URL 分类的组织结构，您可以在这里选择一个 URL 分类作为监控对象，如果您不选择的情况下系统默认是所有分类。

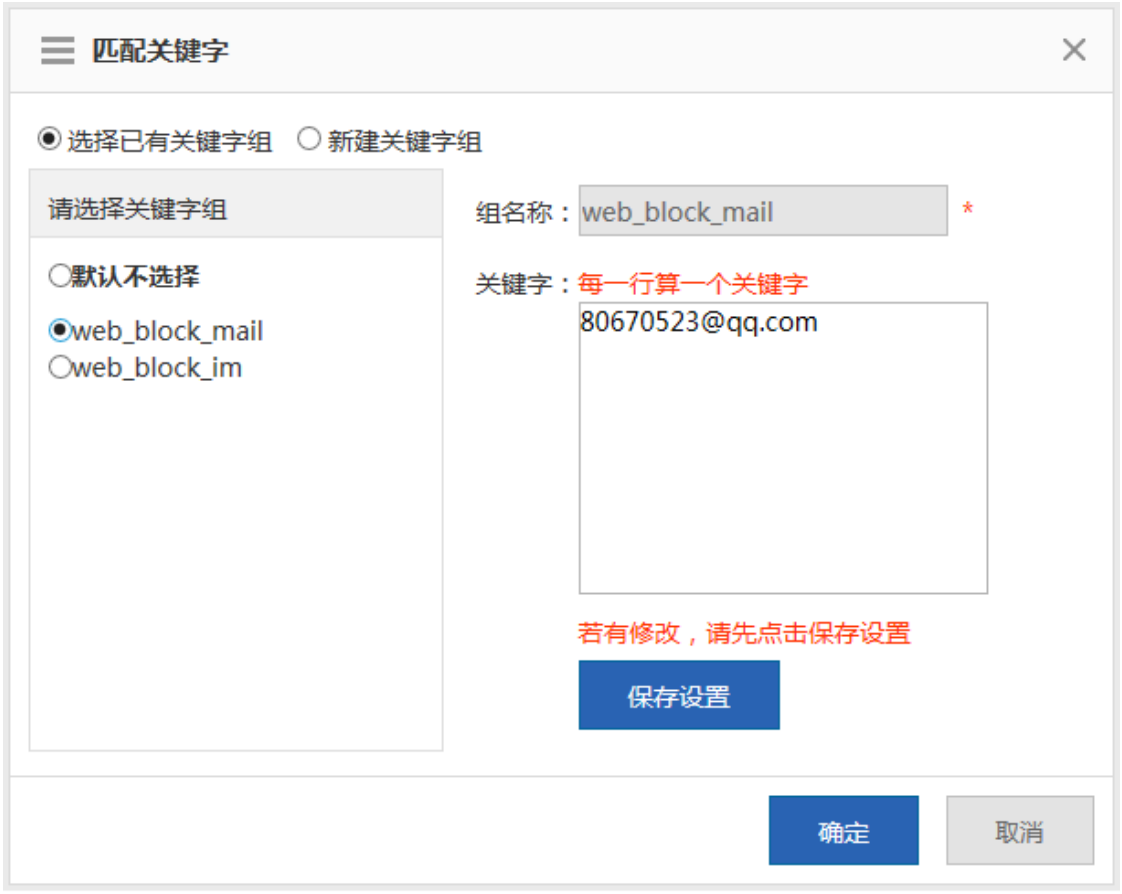
- **邮件控制策略**

邮件控制主要针对主流的邮件系统（如 OutLook，Foxmail）对邮件进行收发审计，信息过滤，并保存邮件的附件到设备硬盘上。配置页面如下：



控制类型是指，审计邮件时使用哪个字段来匹配关键字，比如控制类型选择“收发帐号”，匹配关键字输入“123456”，此时只有邮件帐号为“123456”的邮件才会被审计，而标题和邮件内容或附件中出现“123456”则不会被审计。

点击匹配关键字时弹出如下面窗口：



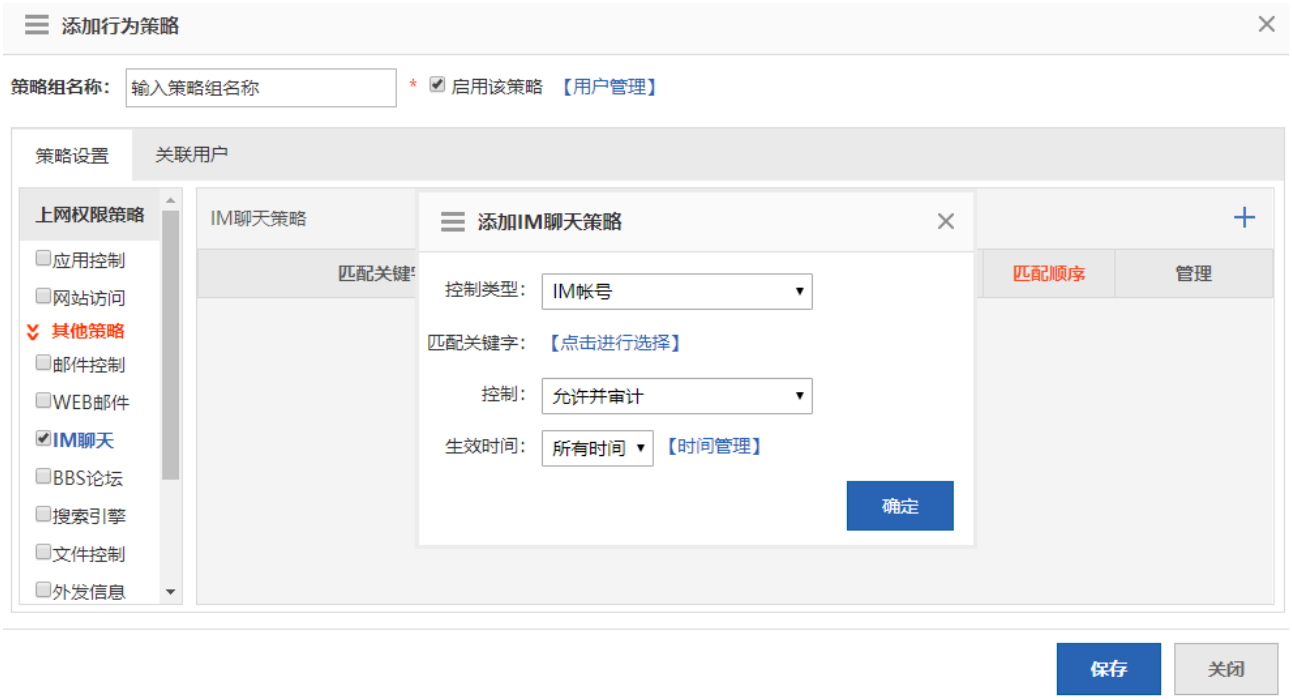
左侧列出了当前系统已配置的关键字组，您可以在这里选择一个关键字组作为监控对象，选择 默认不选择 ，设备将对客户端邮件的所有内容进行审计。选择其它关键字组后，可以在右侧查看、修改该关键字组包含的关键字内容。您也可以点击右侧的 新建关键字组 ，输入组名称和需要审计的关键字信息后保存，即可新建一个关键字组。

- **WEB 邮件策略**

WEB 邮件策略主要针对主流的 WEB 邮件系统（如新浪邮箱，网易邮箱，QQ 邮箱）对邮件进行发送审计，信息过滤，并保存邮件的附件至硬盘。WEB 邮件策略的配置和邮件控制策略一致，只是少了“最大限制”的配置。

- **IM 聊天审计策略**

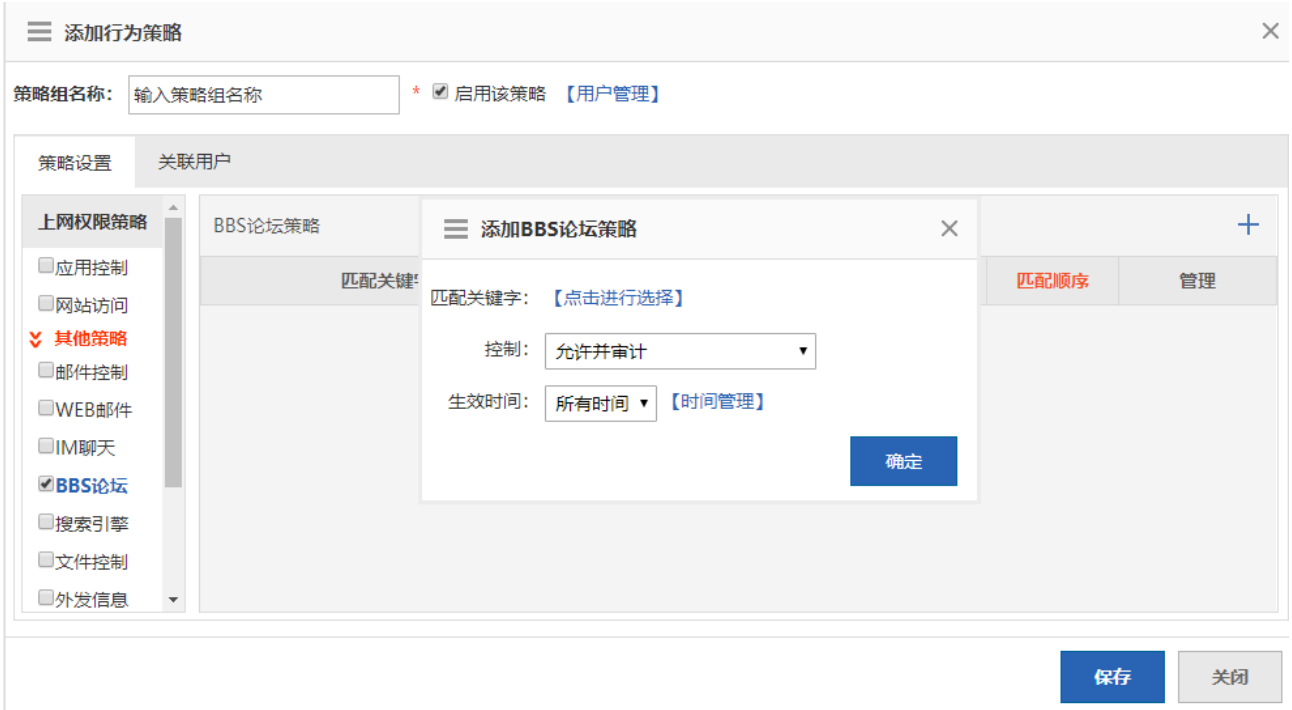
IM 聊天审计主要针对主流的 IM 聊天系统（如 QQ，MSN），对账号和聊天记录进行审计，并对账号进行过滤。配置页面如下：



目前 NBR 支持对 QQ 和 MSN 的聊天审计，如果是 QQ 的话只支持审计 IM 帐号，MSN 支持对帐号和聊天内容进行审计。

- **BBS 论坛策略**

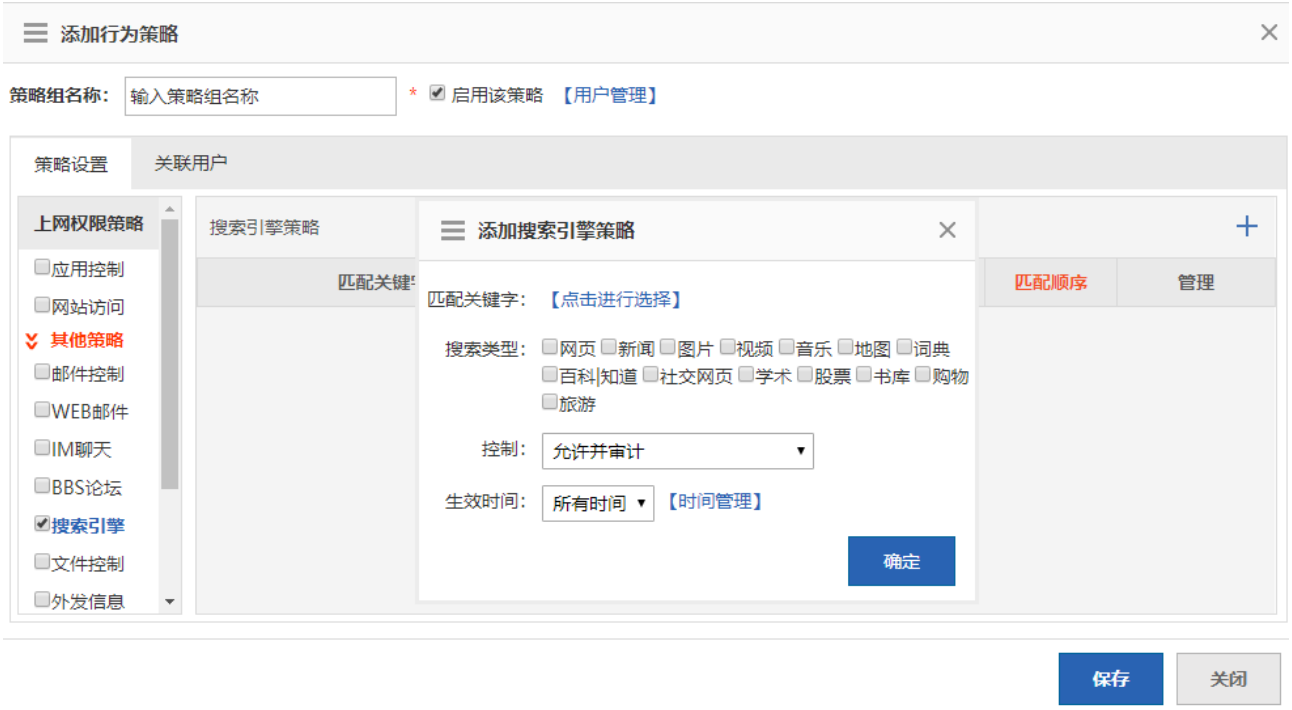
BBS 论坛主要针对主流 WEB BBS 站点(如天涯社区，猫扑社区)，对用户的发帖内容进行审计，并对用户的发帖内容进行过滤。配置页面如下：



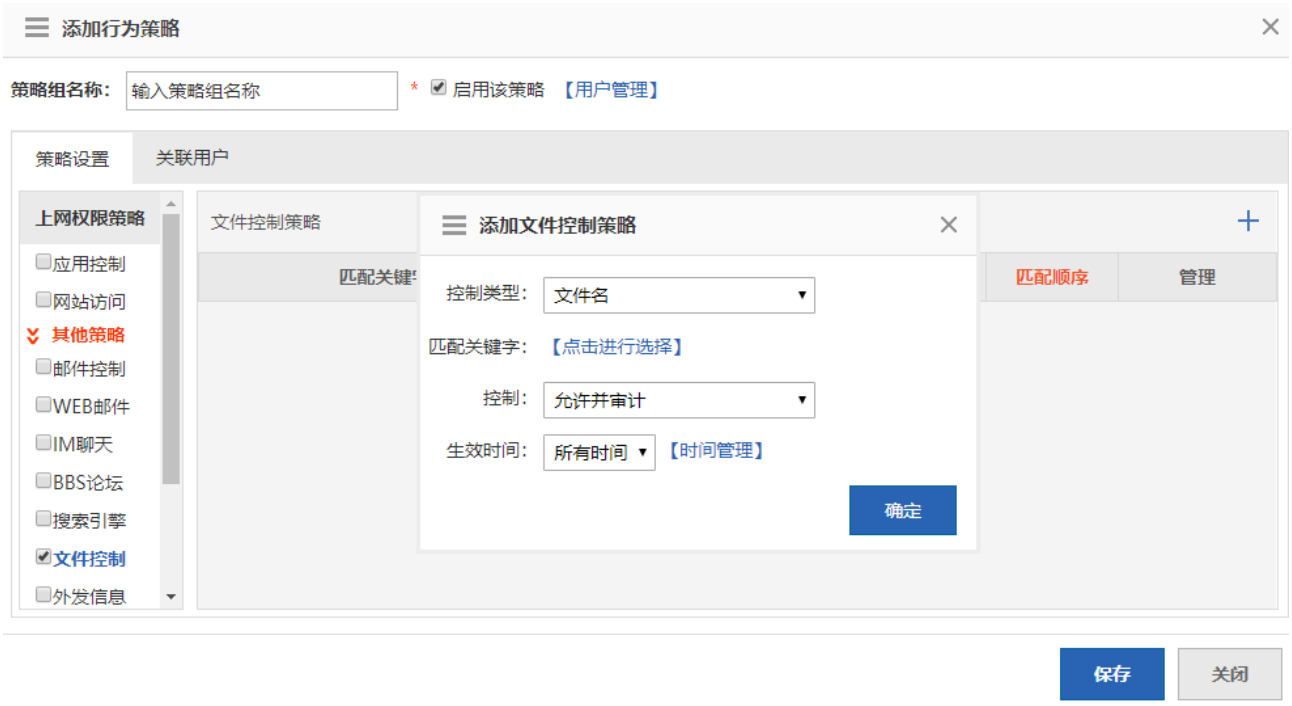
当用户所发的贴中包含“匹配关键字“时，设备将根据策略规则对贴子进行审计。

- **搜索引擎策略**

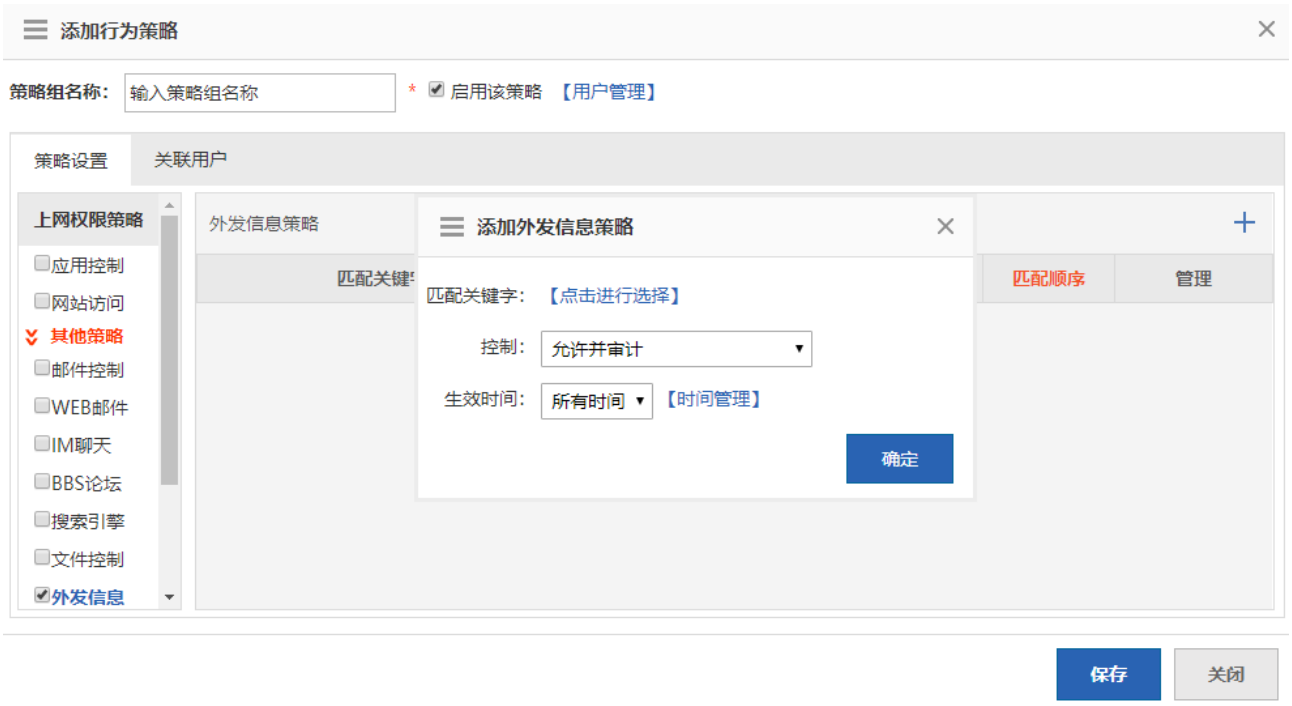
搜索引擎主要针对主流 WEB 搜索引擎站点(如百度，谷歌)，对用户的搜索引擎关键字进行审计，并对搜索引擎关键字进行过滤。配置页面如下：



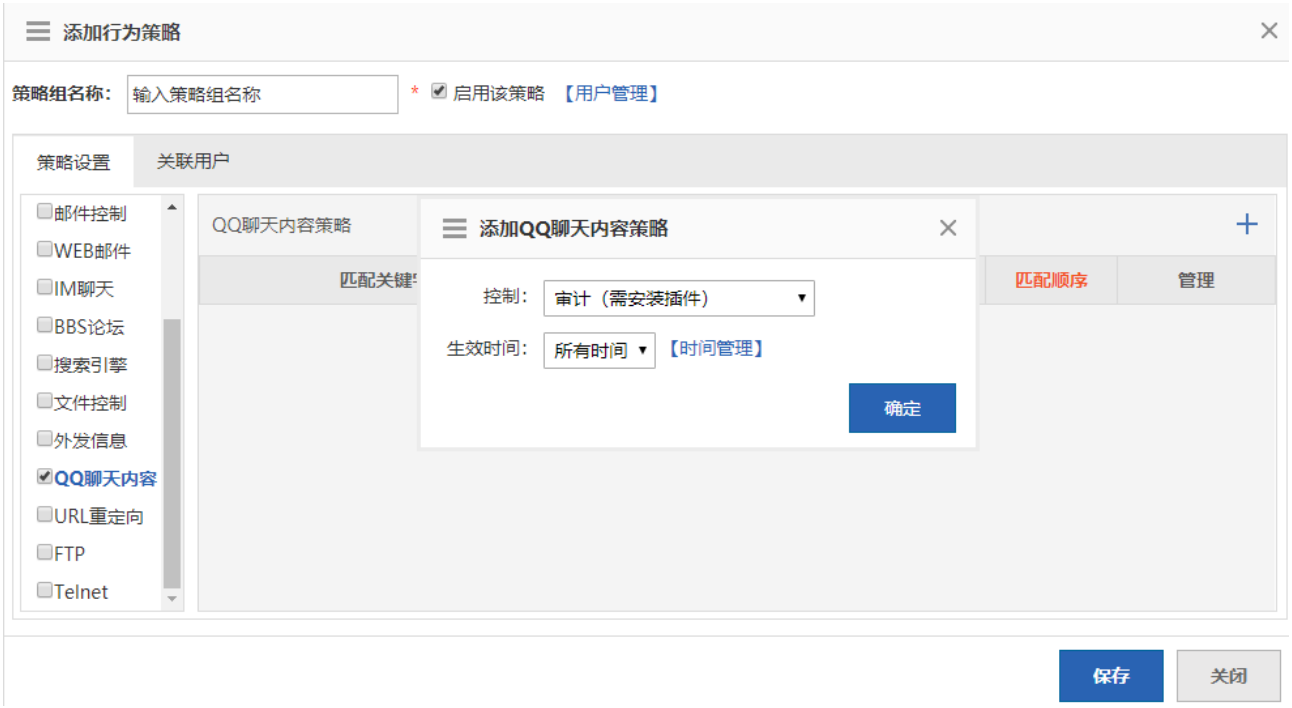
- **文件控制**


添加行为策略
策略组名称：
输入策略组名称
启用该策略
【用户管理】
策略设置
关联用户
上网权限策略
应用控制
网站访问
其他策略
邮件控制
WEB邮件
IM聊天
BBS论坛
搜索引擎
文件控制
外发信息
文件控制策略
添加文件控制策略
匹配关键字
控制类型：
文件名
匹配关键字：
【点击进行选择】
控制：
允许并审计
生效时间：
所有时间
【时间管理】
确定
匹配顺序
管理
保存
关闭

- **外发信息**

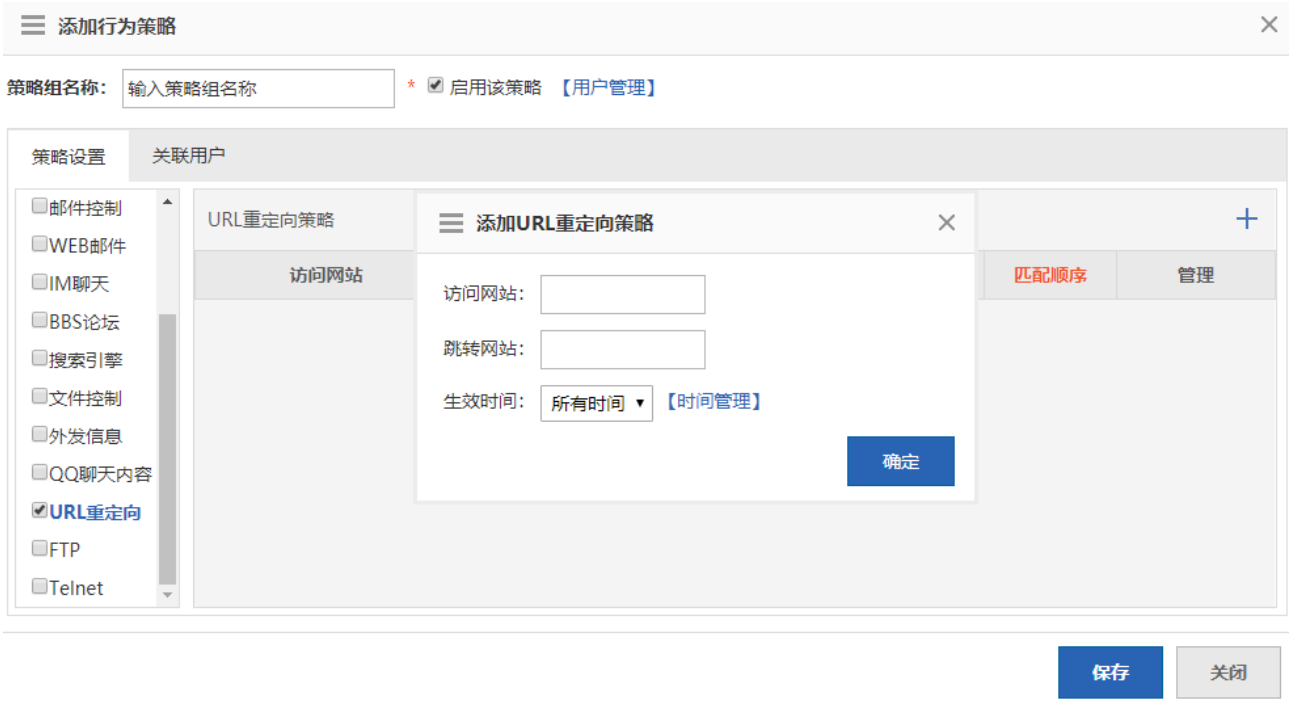

添加行为策略
策略组名称：
输入策略组名称
启用该策略
【用户管理】
策略设置
关联用户
上网权限策略
应用控制
网站访问
其他策略
邮件控制
WEB邮件
IM聊天
BBS论坛
搜索引擎
文件控制
外发信息
外发信息策略
添加外发信息策略
匹配关键字
匹配关键字：
【点击进行选择】
控制：
允许并审计
生效时间：
所有时间
【时间管理】
确定
匹配顺序
管理
保存
关闭

- **QQ 聊天内容**

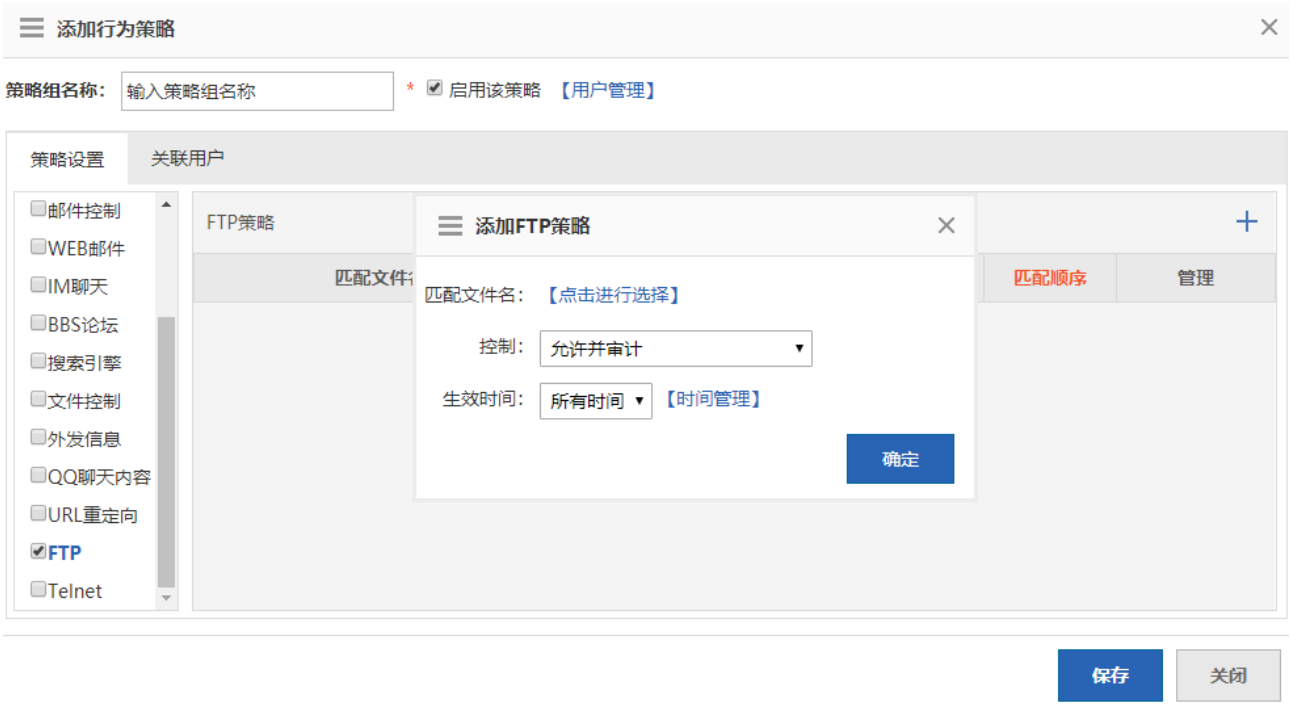


- **URL 重定向**

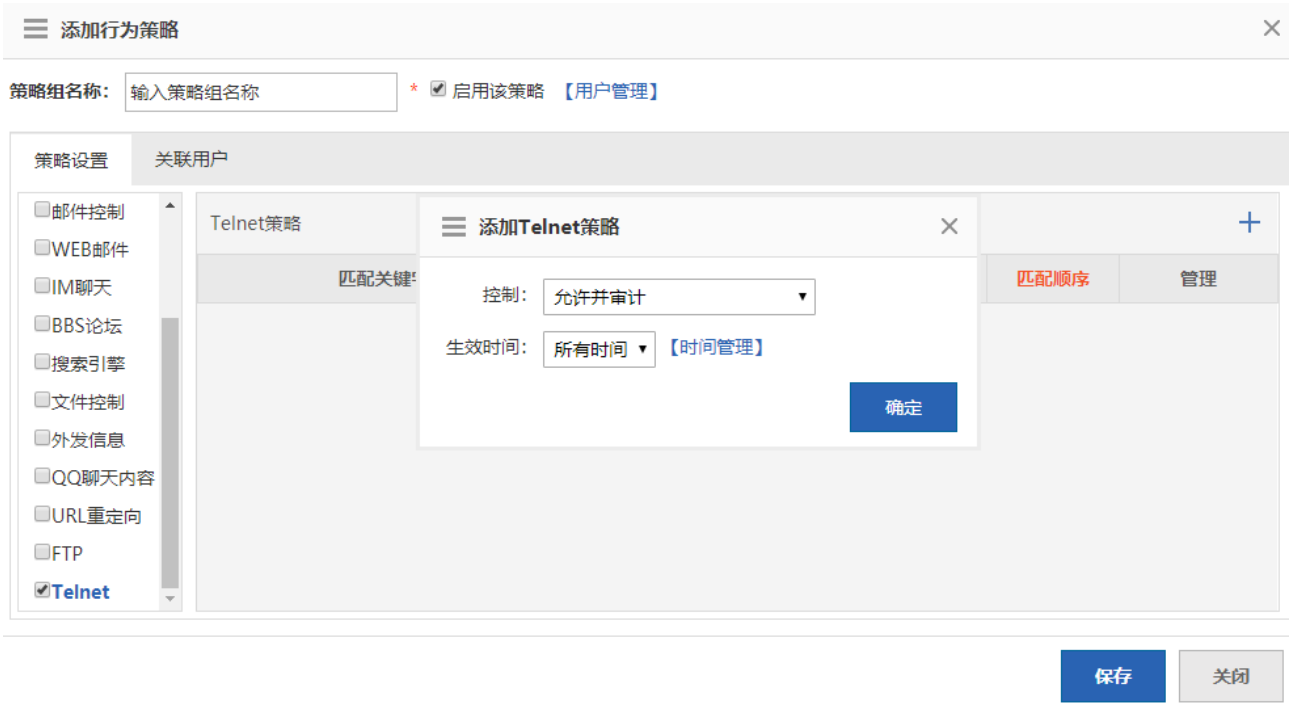
说明：URL 重定向不支持对 HTTPS 加密的网站进行重定向。配置页面如下：



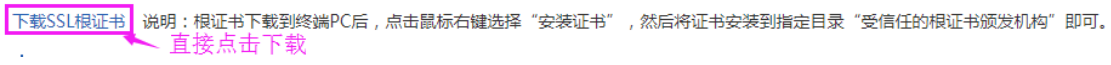
- **FTP**



- **TELNET**



- **设置 HTTPS 加密内容审计**



点击 

，可以删除该行的例外用户

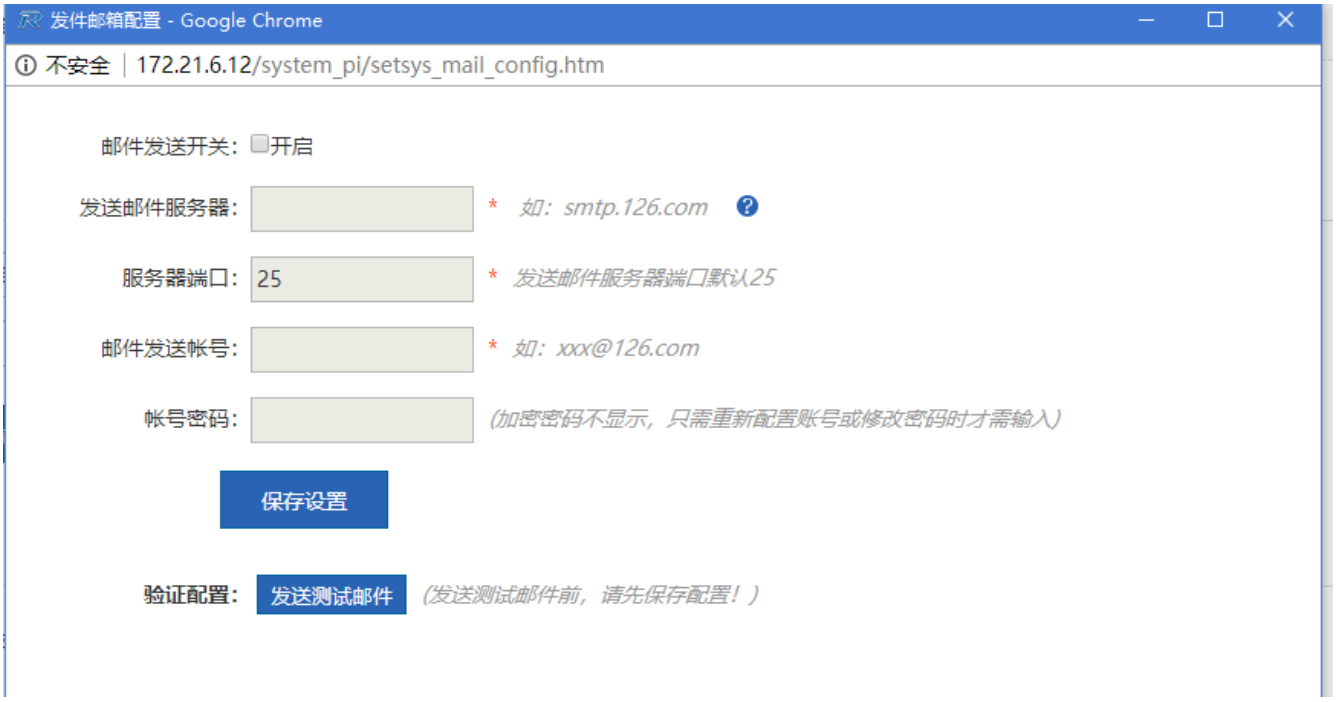
点击 ×清空例外用户 ，可以清除所有例外用户

点击 +添加例外用户


添加例外用户
所有用户
_a
3段
2段
1.1.241.10
testa
testb
选择要添加的用户，点击保存
保存

1.3.7.1.3 审计告警

点击 

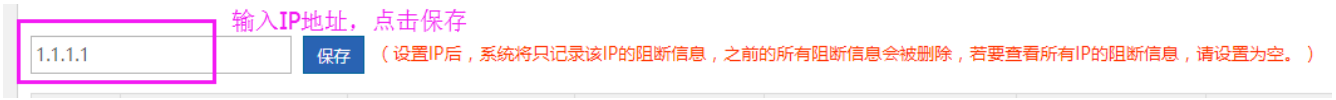


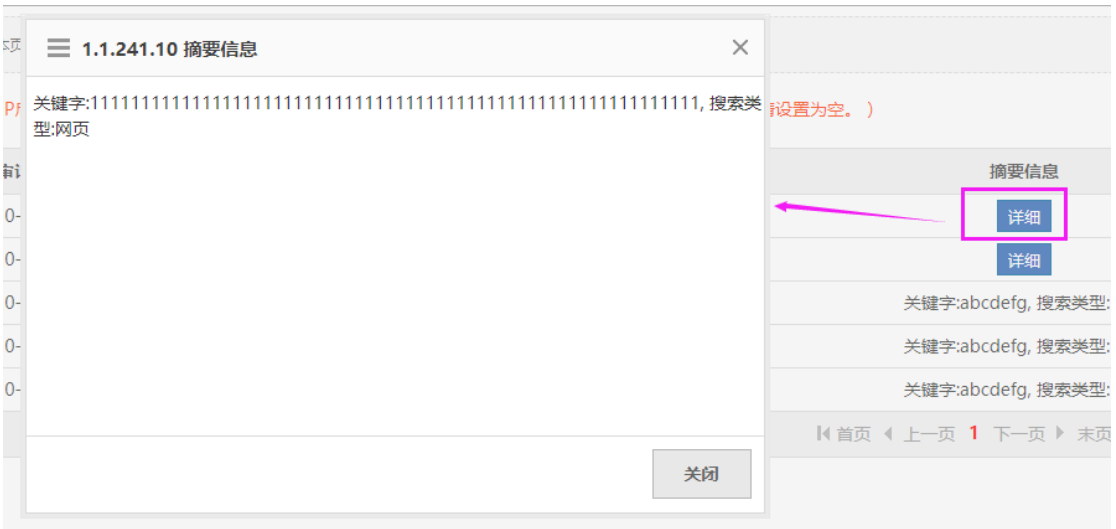
1.3.7.1.4 告警信息查询

1.3.7.2 实时审计记录

1.3.7.3 阻断信息记录

设置特定 IP





1.3.7.4 审计日志查询

1.3.7.4.1 访问审计报表

访问审计报表是用于查看与网页相关的访问记录，包括站点访问次数的排行，用户访问的网站数统计以及一些从浏览器页面审计的信息等。查看页面如下图所示：

点击 高级查询 会弹出高级查询的参数选择界面，具体请参考本章第 6 点。

点击 导出报表 可以将查询的报表结果导出保存到 PC 上。

1、 网站访问排行：

该表格显示网站访问次数排行，包括该网站的影响等级、网站分类、访问的次数。页面如下图所示：

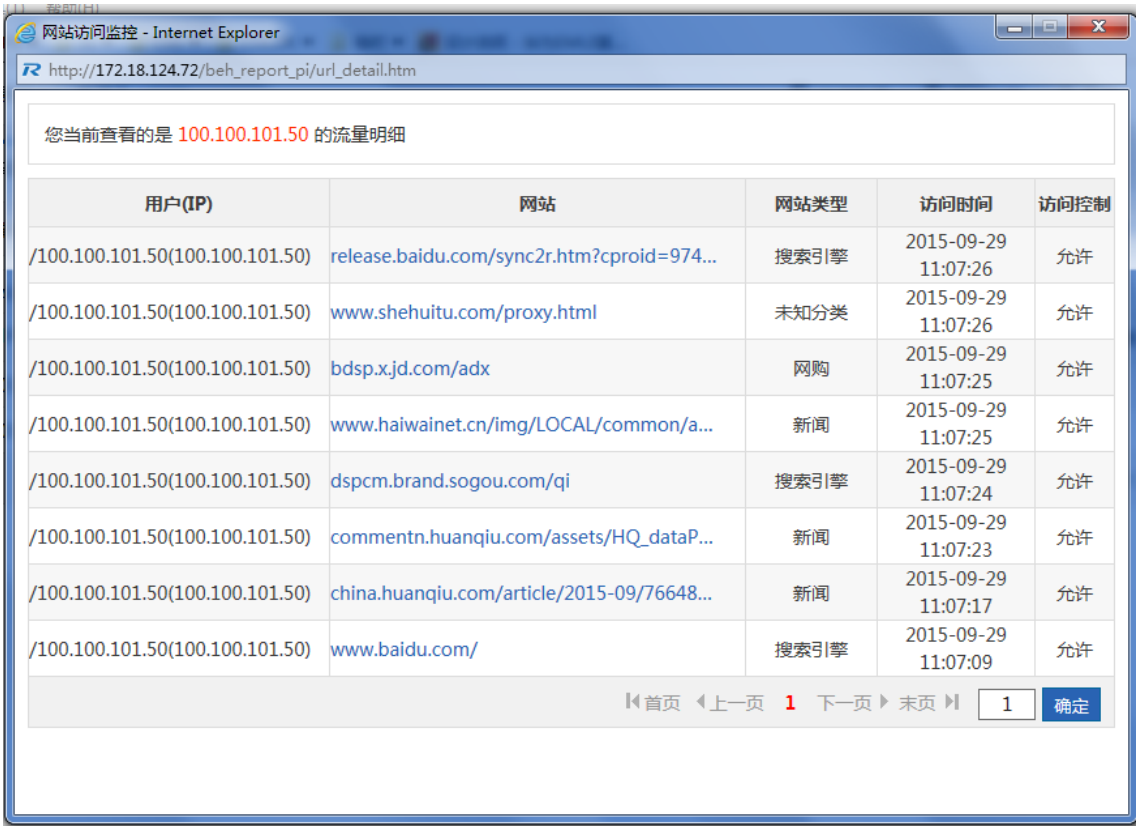
点击 明细 可以查看选中网站的流量明细，如都有哪些用户访问了该网站，在什么时间点访问的：

点击 阻断 可以对选中的网站进行阻断，一旦该网站被阻断，用户就无法访问该网站了。

2、 用户访问排行：

该表格显示了用户访问网站数目的排行，访问越多的用户排在越前面：

点击 明细 可以查看该用户都访问了哪些网站，哪个时间点访问的，以及这些网站所属的网站类型：



3、 网站访问明细：

该模块显示的是所有被访问的网站的一个明细 ,如果你想查看具体的某个网站 ,你可以通过 高级查询 输入网址然后查看。

4、 被阻断的网站：

该模块下也是一个表格，显示了所有被阻断的网站信息：

点击 明细 可以查看选中网站的流量明细：

5、 应用控制审计

应用控制访问审计，是用户在配置各种应用控制规则后，设备根据这些规则审计每个发生上网行为的应用，并记录在设备中供管理者查阅。要使用应用访问控制审计，必需先在行为策略中配置“应用控制”策略，只有策略审计到的记录才会在下方表格中显示。

“VPN 接入”是指审计到这条记录时，该用户是否是通过 VPN 连接上网。

6、 高级查询

点击 高级查询 可以查询某些用户在某个特定时间范围内访问某些网站的报表记录，查询界面如下图所示：

1.3.7.4.2 内容审计报表

内容审计报表是对用户上网访问的具体内容或行为进行审计的记录，内容审计包括对收发邮件、IM 聊天工具、论坛发贴、搜索引擎、WEB 页面、FTP、TELNET 的内容审计。

通过 高级查询 按钮可以查询各种内容审计信息。通过 导出报表 按钮可以导出各种内容审计报表。

1、 客户端邮件

NBR 支持对客户端邮件进行审计，如 foxmail、outlook 等。如下表所示，您可以通过该表格查看当前有哪些用户在使用客户端邮件，给谁发送邮件，邮件主要内容是什么等信息：

2、 WEB 端邮件

NBR 支持对 WEB 端邮件进行审计 ,如新浪、163、雅虎等。如下表所示 ,您可以通过该表格查看当前有哪些用户在使用 webmail，给谁发送邮件，邮件主要内容是什么等信息。

3、 IM 聊天

NBR 支持对 QQ、MSN 等的上下线记录和内容审计。审计信息如下表所示：

4、 论坛发贴

NBR 支持对 BBS 论坛内容审计，如天涯社区、猫扑、动网官方网站、PHPWIN 官方网站等。审计信息如下表所示：

5、 搜索引擎

NBR 支持对各种搜索引擎的审计，如百度、Google、雅虎等。如下表所示，您可以通过该表格查看哪些用户，在哪个时间段，用什么搜索引擎，搜索了什么内容等信息。

6、 虚拟身份

NBR 支持支持微信、QQ、新浪微博上线下线的，审计时间和账号信息，如下图。

7、 插件 QQ 聊天内容

8、 外发文件

9、 外发信息

10、 FTP

11、 TELNET

12、 高级查询

高级查询可以根据时间、类型、用户、关键字等信息对历史审计数据进行查询，并支持导出报表，查询界面如下所示：

查询结果如下图所示：

1.3.7.5 行为统计分析

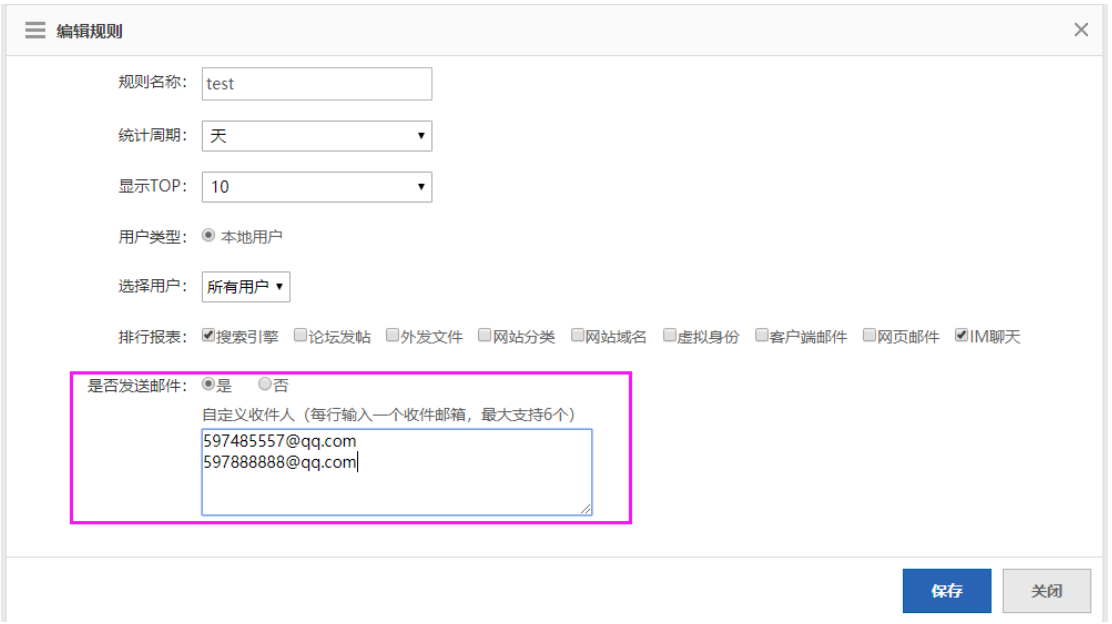
1.3.7.5.1 报表配置

1.3.7.5.2 自定义报表

点击添加规则

点击保存

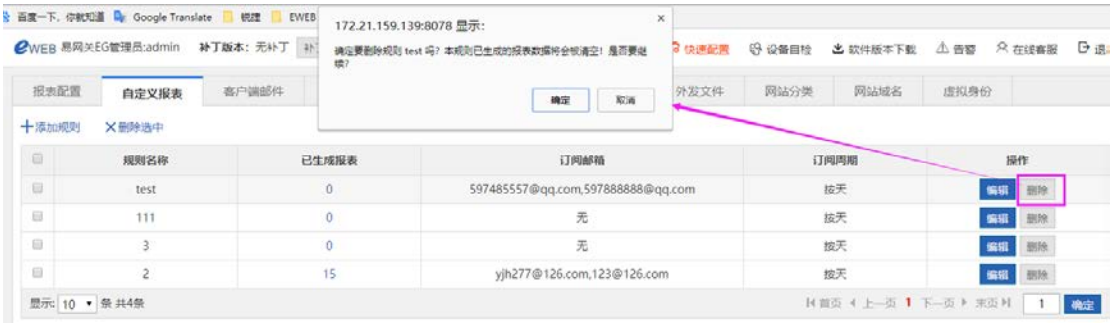
点击编辑



点击保存

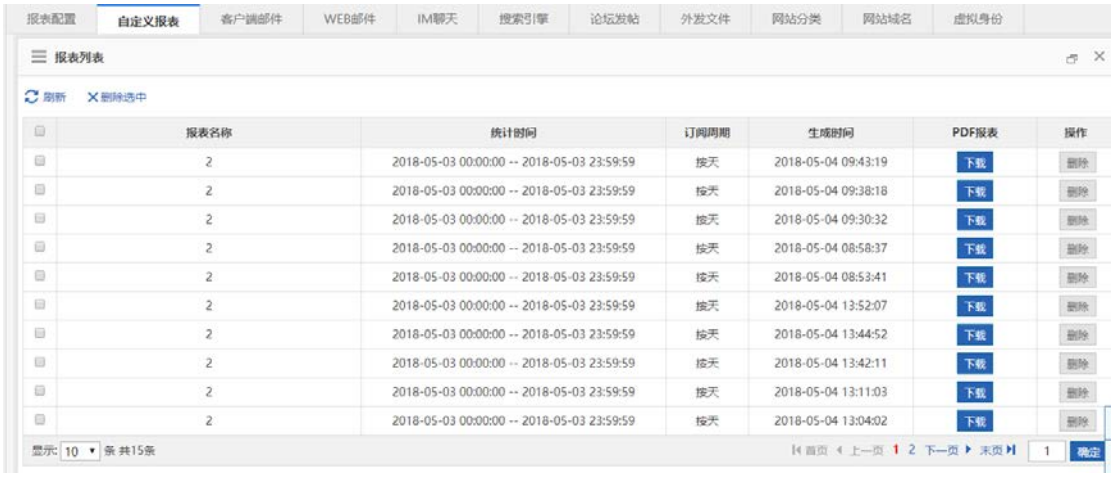
点击确定

点击删除



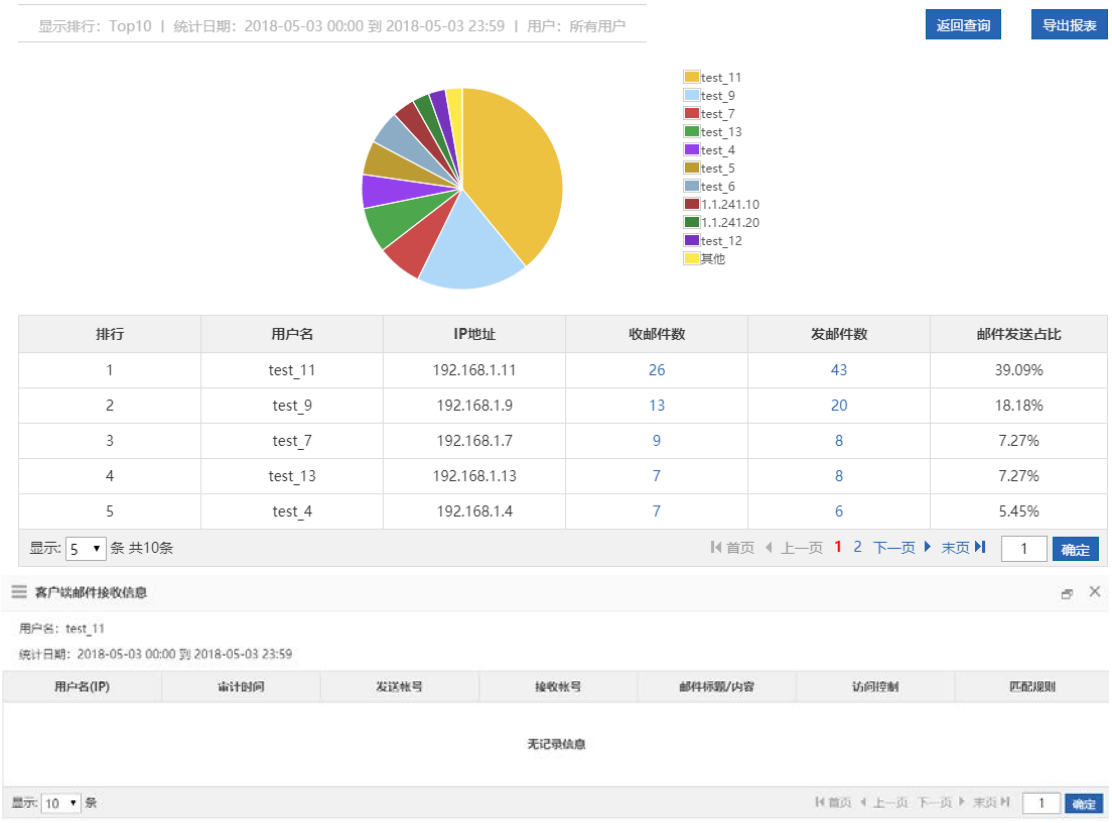
点击确定

点击已生成报表这一列



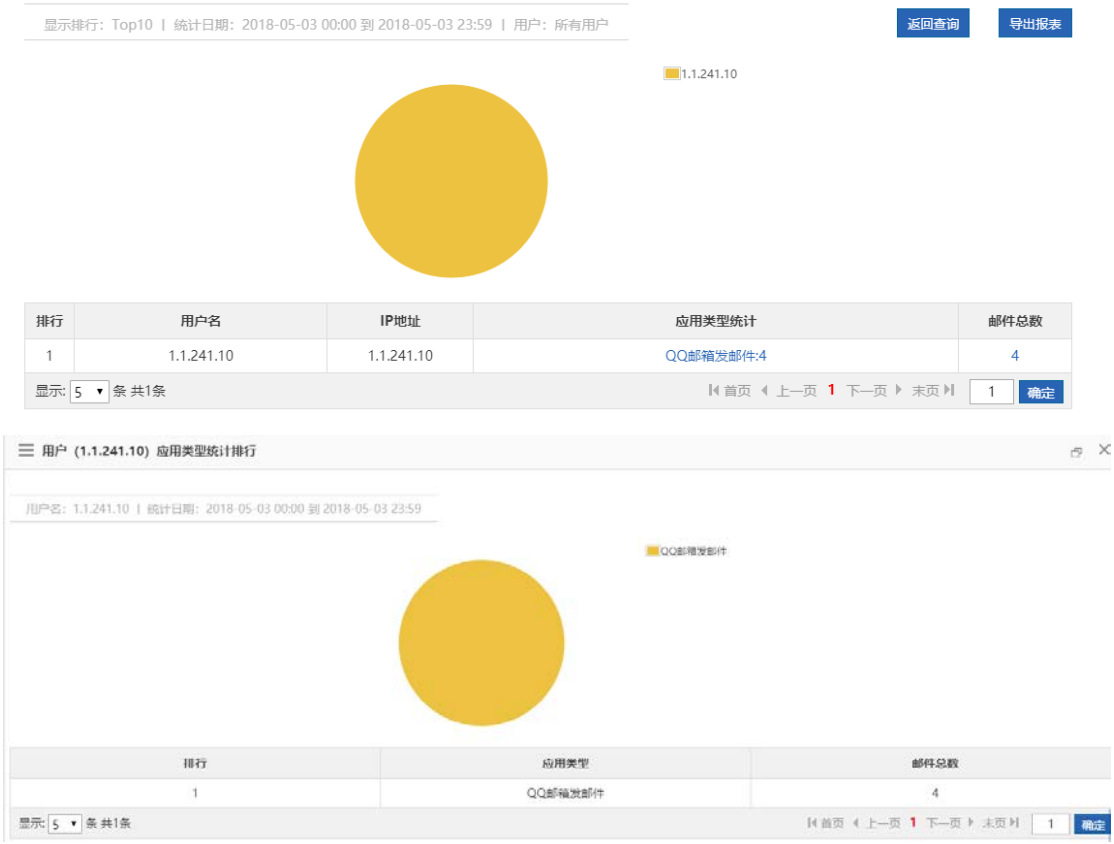
已生成的报表可进行下载、删除操作

1.3.7.5.3 客户端邮件


显示排行：Top10 | 统计日期：2018-05-03 00:00 到 2018-05-03 23:59 | 用户：所有用户
返回查询
导出报表
test_11
test_9
test_7
test_13
test_4
test_5
test_6
1.1.241.10
1.1.241.20
test_12
其他
排行 用户名 IP地址 收邮件数 发邮件数 邮件发送占比
1 test_11 192.168.1.11 26 43 39.09%
2 test_9 192.168.1.9 13 20 18.18%
3 test_7 192.168.1.7 9 8 7.27%
4 test_13 192.168.1.13 7 8 7.27%
5 test_4 192.168.1.4 7 6 5.45%
显示: 5 条 共10条
首页 上一页 1 2 下一页 末页
1
确定
客户端邮件接收信息
用户名：test_11
统计日期：2018-05-03 00:00 到 2018-05-03 23:59
用户名(IP) 审计时间 发送帐号 接收帐号 邮件标题/内容 访问控制 匹配规则
无记录信息
显示: 10 条
首页 上一页 下一页 末页
1
确定

1.3.7.5.4 WEB 邮件


报表配置
自定义报表
客户端邮件
WEB邮件
IM聊天
搜索引擎
统计维度：
用户排行
显示TOP：
10
用户类型：
本地用户
选择用户：
所有用户
统计周期：
天
选择时间：
2018-07-12
确定查询

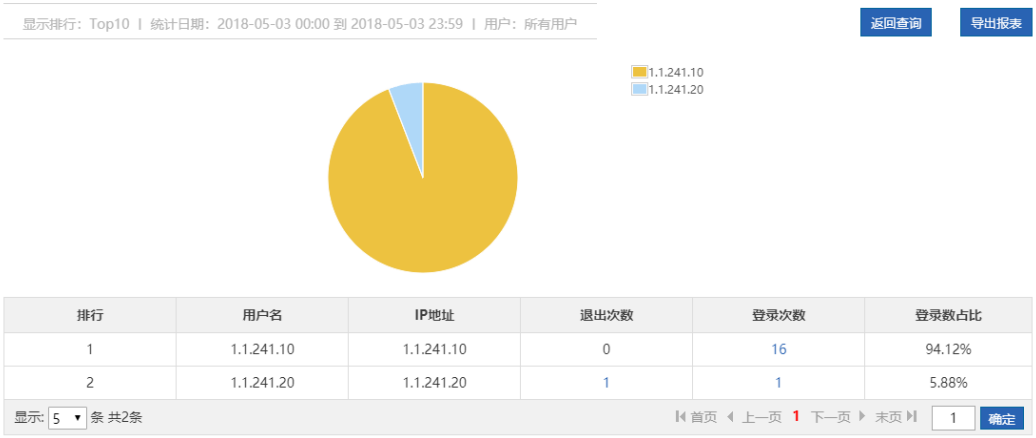

显示排行：Top10 | 统计日期：2018-05-03 00:00 到 2018-05-03 23:59 | 用户：所有用户
返回查询
导出报表
1.1.241.10
排行
用户名
IP地址
应用类型统计
邮件总数
1
1.1.241.10
1.1.241.10
QQ邮箱发邮件:4
4
显示: 5 条 共1条
首页 上一页 1 下一页 末页
1
确定

用户（1.1.241.10）应用类型统计排行
用户名：1.1.241.10 | 统计日期：2018-05-03 00:00 到 2018-05-03 23:59
QQ邮箱发邮件
排行
应用类型
邮件总数
1
QQ邮箱发邮件
4
显示: 5 条 共1条
首页 上一页 1 下一页 末页
1
确定


用户搜索信息
用户名：1.1.241.10
统计日期：2018-05-03 00:00 到 2018-05-03 23:59
用户名(IP)
审计时间
具体应用
发送帐号
接收帐号
邮件标题/内容
访问控制
匹配规则
无记录信息
显示: 10 条
首页 上一页 下一页 末页 1 确定

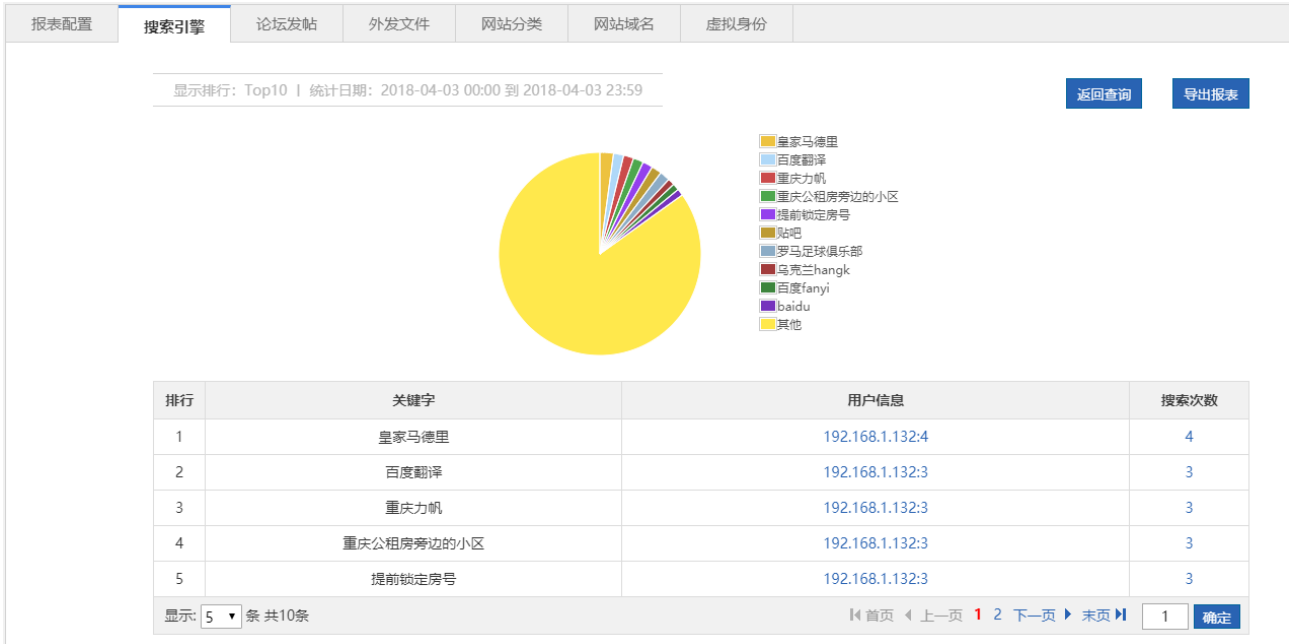
1.3.7.5.5 IM 聊天


报表配置
自定义报表
客户端邮件
WEB邮件
IM聊天
搜索引擎
统计维度：
登录数排行
显示TOP：
10
用户类型：
本地用户
选择用户：
所有用户
统计周期：
天
选择时间：
2018-07-12
确定查询

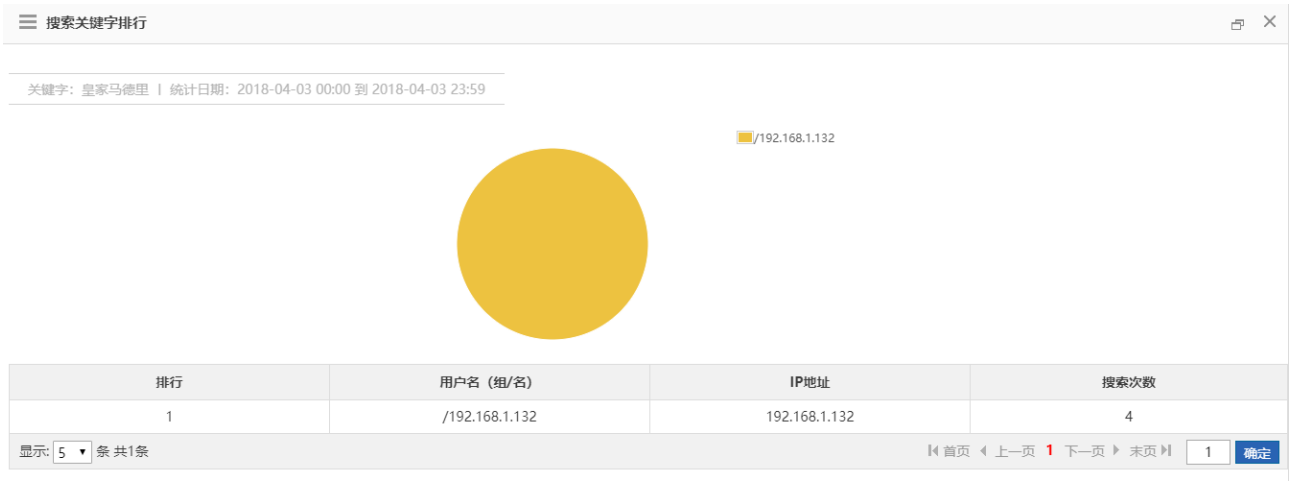

显示排行：Top10 | 统计日期：2018-05-03 00:00 到 2018-05-03 23:59 | 用户：所有用户
返回查询
导出报表
1.1.241.10
1.1.241.20
排行
用户名
IP地址
退出次数
登录次数
登录数占比
1
1.1.241.10
1.1.241.10
0
16
94.12%
2
1.1.241.20
1.1.241.20
1
1
5.88%
显示: 5 条 共2条
首页 上一页 1 下一页 末页 1 确定

1.3.7.5.6 搜索引擎

点击 



点击用户信息一列



排行	用户名（组/名）	IP地址	搜索次数
1	/192.168.1.132	192.168.1.132	4

显示: 5 条 共1条 首页 上一页 1 下一页 末页 1 确定

点击搜索次数一列

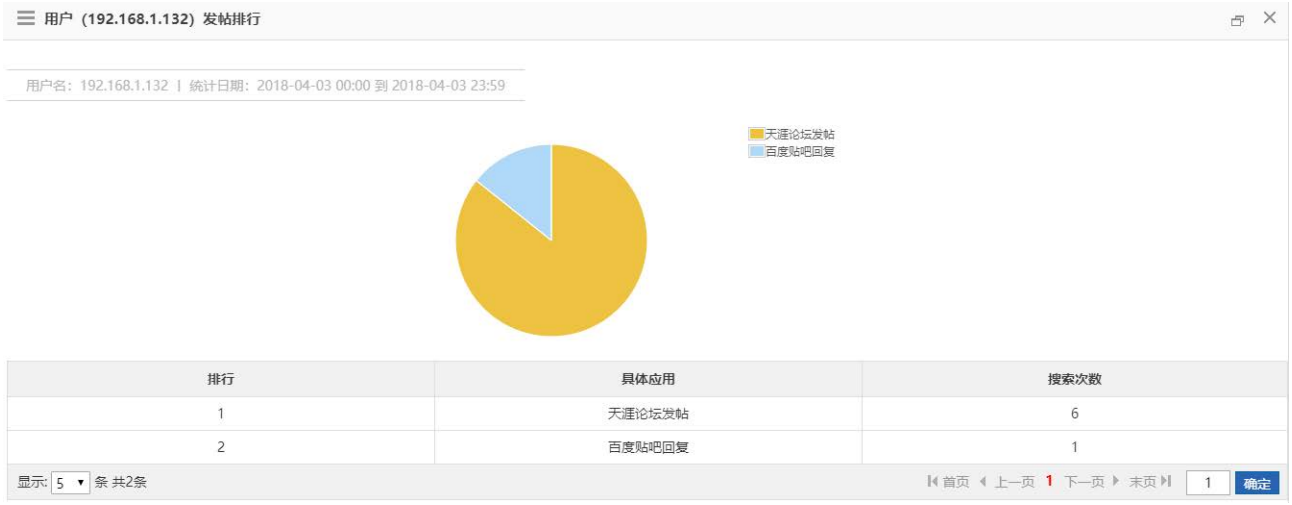
用户名(IP)	审计时间	网页地址	具体应用	搜索类别	搜索内容	访问控制	匹配规则
/192.168.1.132(192.168.1.132)	2018-04-03 14:42:44	tieba.baidu.com/f?k...	百度贴吧	社交网页	皇家马德里	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 14:42:47	tieba.baidu.com/f?k...	百度贴吧	社交网页	皇家马德里	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 15:29:07	tieba.baidu.com/f?k...	百度贴吧	社交网页	皇家马德里	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 15:29:26	tieba.baidu.com/f?k...	百度贴吧	社交网页	皇家马德里	允许	默认审计

显示: 10 条 首页 上一页 1 下一页 末页 1 确定

1.3.7.5.7 论坛发帖

点击 

点击发帖统计一列



排行	具体应用	搜索次数
1	天涯论坛发帖	6
2	百度贴吧回复	1

显示: 5 条 共2条 首页 上一页 1 下一页 末页 1 确定

点击发帖次数一列

用户名(IP)	审计时间	网页地址	具体应用	发送帐号	发贴标题/内容	访问控制	匹配规则
/192.168.1.132(192.168.1.132)	2018-04-03 15:28:44	https://tieba.baidu.c...	百度贴吧回复	192.168.1.132 024c3cdbdefdf807699d6afb	【详细】	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 15:59:29	http://bbs.tianya.cn/...	天涯论坛发帖	192.168.1.132	RR坐起慢慢听CC 【详细】	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 16:24:37	http://bbs.tianya.cn/...	天涯论坛发帖	192.168.1.132	幸好当时听了LZ的话，不然现在 【详细】	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 16:24:54	http://bbs.tianya.cn/...	天涯论坛发帖	192.168.1.132	幸好当时听了LZ的话，不然现在 【详细】	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 16:26:39	http://bbs.tianya.cn/...	天涯论坛发帖	192.168.1.132	个人觉得7分上下的样子 【详细】	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 16:26:53	http://bbs.tianya.cn/...	天涯论坛发帖	192.168.1.132	个人觉得7分上下的样子 【详细】	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 16:41:07	http://bbs.tianya.cn/...	天涯论坛发帖	192.168.1.132	WC的位置好突兀 WOW 【详细】	允许	默认审计

显示: 10 条 首页 上一页 1 下一页 末页 1 确定

1.3.7.5.8 外发文件

点击 

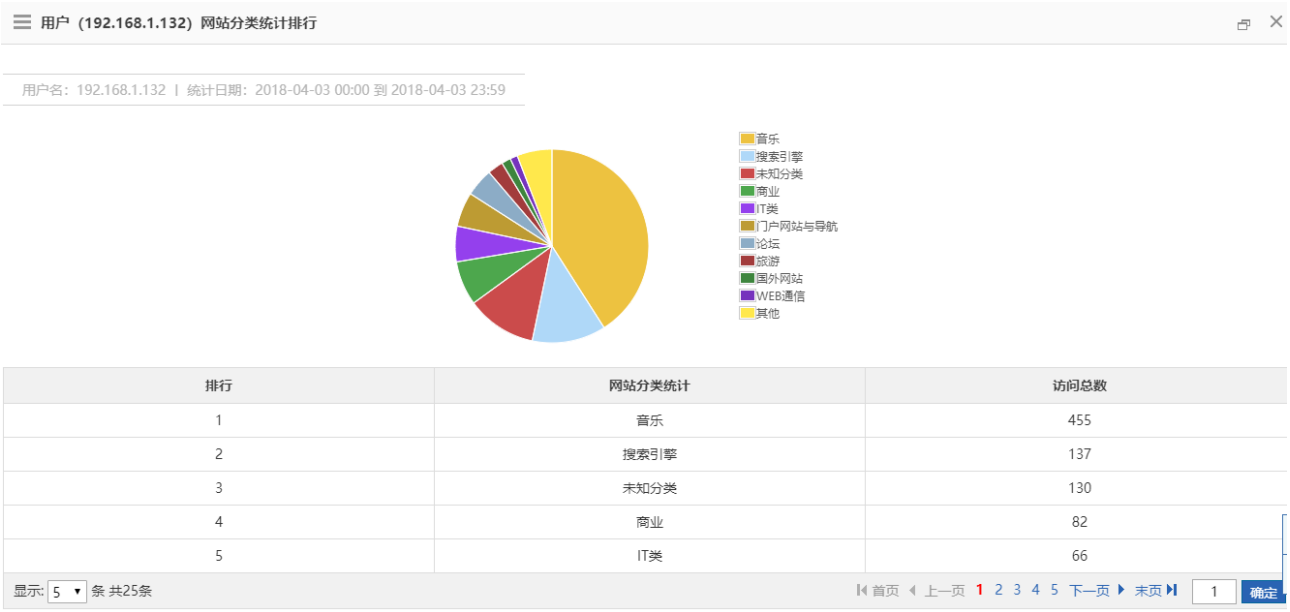
点击外发文件统计一列

点击外发次数一列

1.3.7.5.9 网站分类

点击 

点击网站分类统计一列

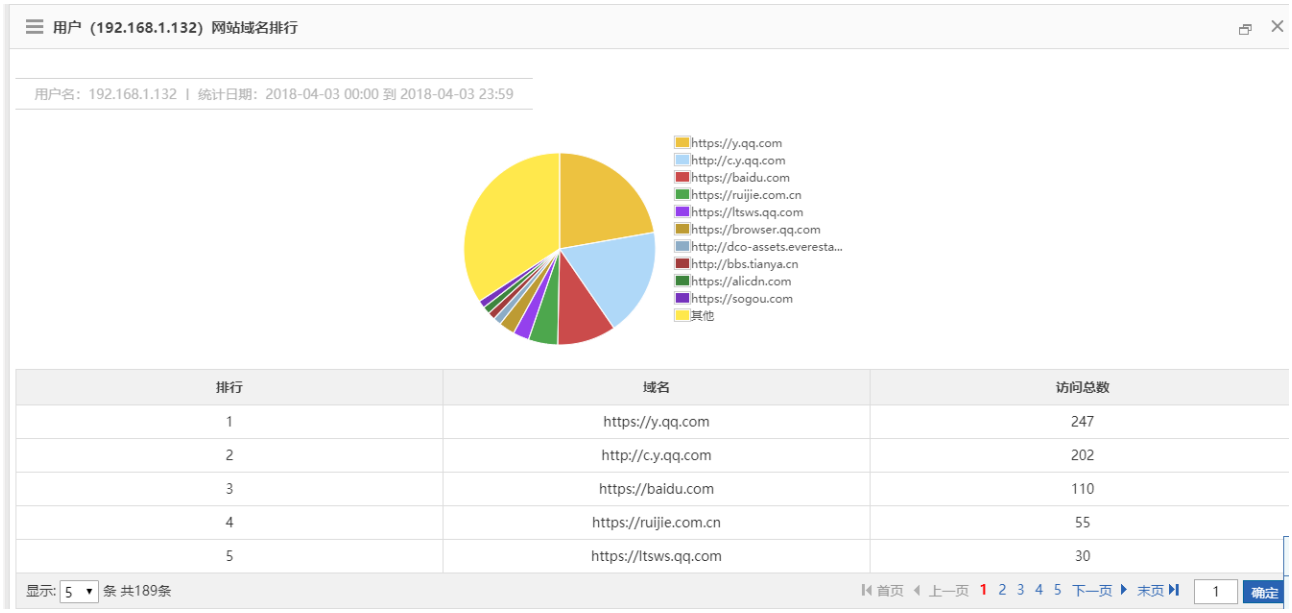


点击访问总数一列

1.3.7.5.10网站域名

点击 

点击域名统计一列

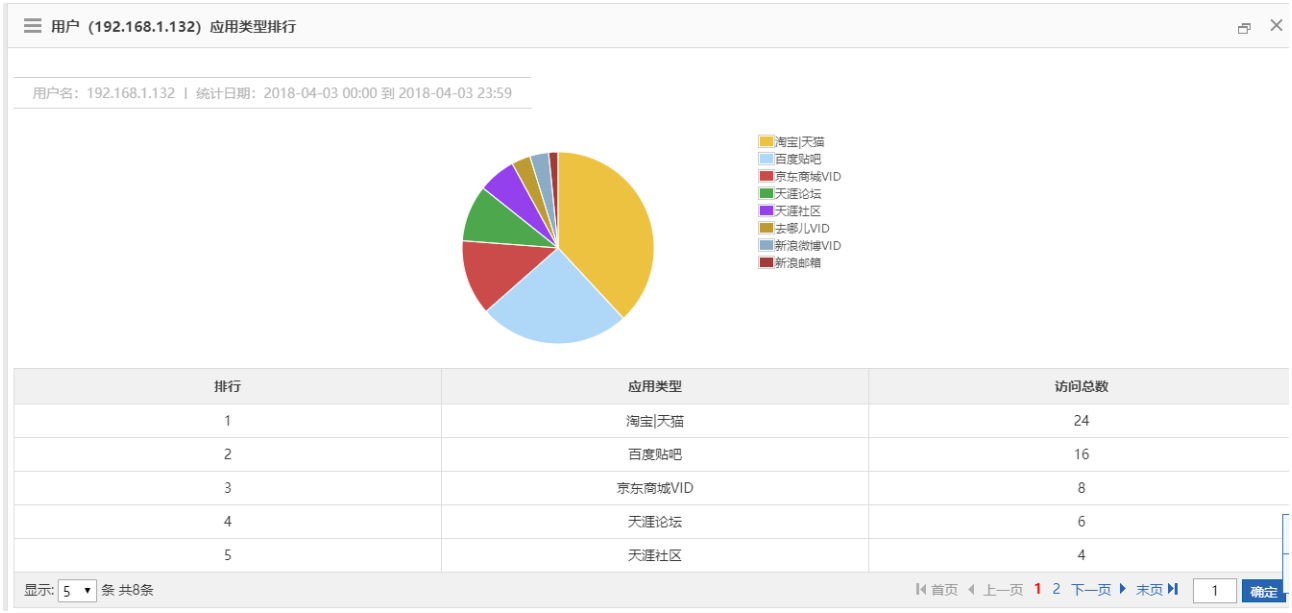


点击访问总数一列

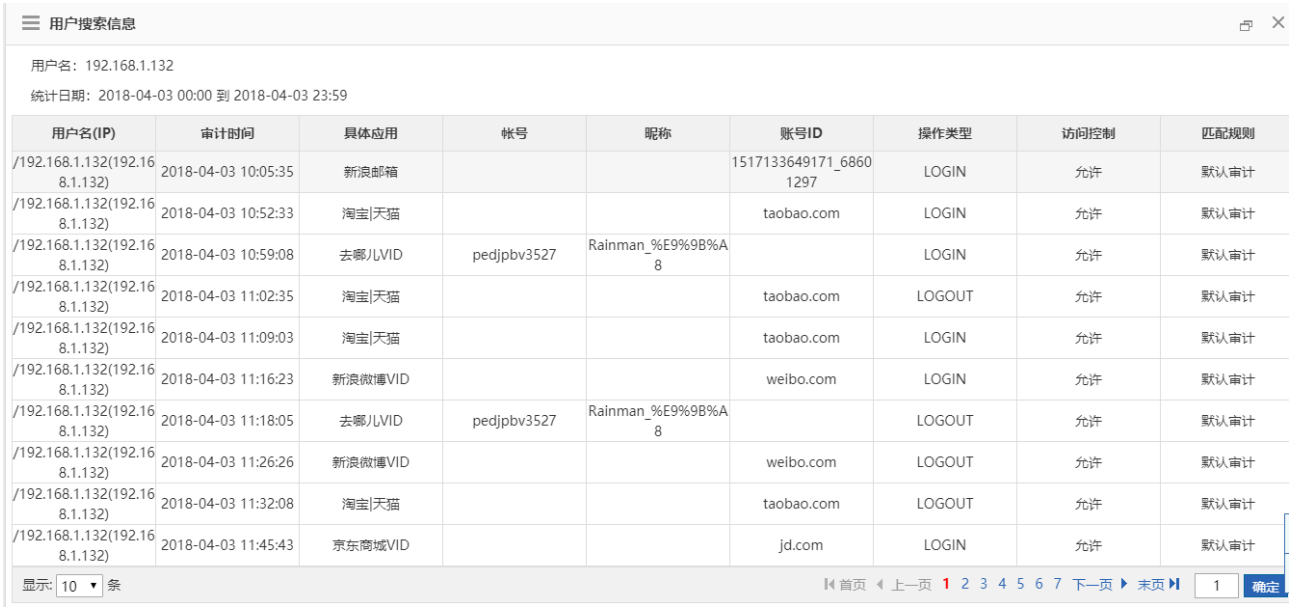
1.3.7.5.11虚拟身份

点击 

点击应用类型统计一列



点击访问总数一列



1.3.7.6 对象定义

对象定义配置页面：

1.3.7.6.1 自定义应用分组

该页面显示了当前系统已存在的所有应用分组以及每个应用分组包含的应用。其中关键/保证类、抑制类、阻断类、普通/其他类为系统定义的应用分组，其他为用户自定义的应用分组。

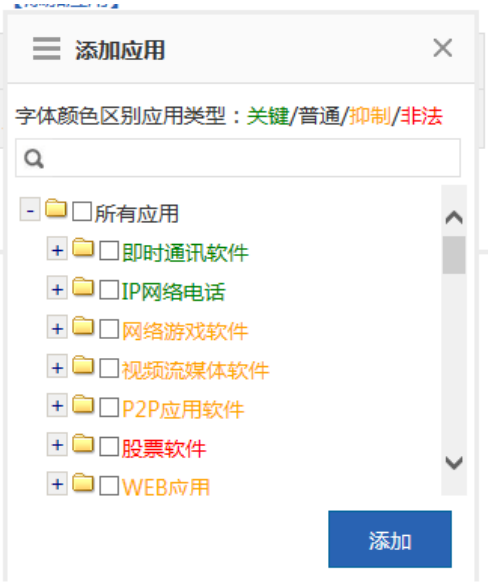
- **应用分组**

设置应用分组主要是方便用户统筹管理公司内部协议的使用情况，确保公司内部网络流畅且带宽不被浪费于无关的工作上。

4. 新增自定义应用分组：

点击 ＋添加应用分组 按钮可以自定义应用分组：

在“应用组名”输入框中输入应用分组名称，点击【添加应用】按钮：



勾选要加入该自定义应用分组的应用，点击 添加 按钮，已勾选的应用将显示在下方的表格中：

点击 删除 按钮可以将某个应用从该应用分组中删除。

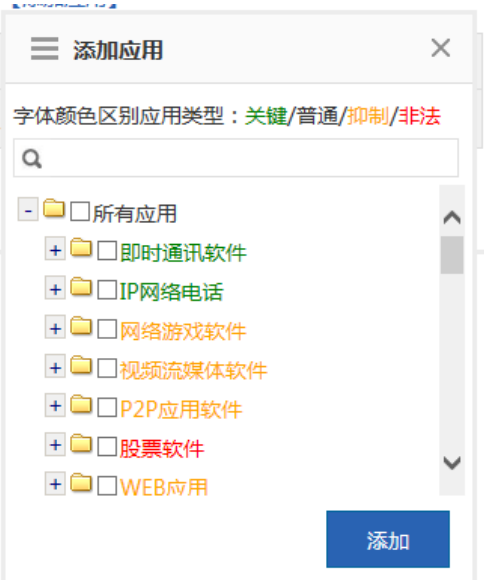
点击 保存 按钮即可完成自定义应用分组的配置，配置完成的应用分组信息将显示在自定义应用分组主页面的表格中：

5. 编辑应用分组：

点击自定义应用分组主页面表格中的 按钮可以重新分配某个应用分组包含的应用：

点击【添加应用】按钮可以往该应用分组中添加应用，点击 删除 可以将某个应用从该应用分组中删除。

点击【添加应用】按钮将弹出以下窗口：



其中绿色字体的说明已经被选择为关键/保证类应用，橙色字体的说明已经被选择为抑制类应用，红色字体的说明已经被选择为阻断类应用，黑色字体的则是被选择为普通/其他类应用组、或未被选择而统一归类到普通/其他类应用组的应用。

已被选择为关键/保证类或抑制类或阻断类的应用，不能加入到这三个应用分组中的另两个应用分组。

如果需要修改，假设需要将 抑制类应用 修改为 关键/保证类应用，那么需要先编辑抑制类应用分组，将要修改的应用从抑制类应用分组中删除，再编辑关键/保证类应用分组，将此应用添加至关键/保证类应用分组中。

6. 删除应用分组：

点击自定义应用分组主页面表格中的 删除 按钮可以删除某个自定义应用分组，系统应用分组（即关键/保证类、抑制类、阻断类、普通/其他类）不可删除。

- **自定义应用**

除了系统内建的网络应用协议，您还可以自己定义其他网络应用，如基于某个端口的应用，或基于某个目标服务器的应用。自定义协议和系统内建的其它协议一样，可用于策略中的网络应用控制、带宽管理，并可进行网络应用实时监控等。

注意：自定义协议优先级最高，即当自定义协议与系统内置协议冲突时（如端口相同），系统识别为用户自定义的网络应用协议。

点击自定义应用分组主页面的 +自定义应用 按钮将弹出自定义应用配置窗口：

创建自定义应用对象：输入自定义应用名称、选择协议类型、选择规则类型、应用所属分类（可以自己另外定义应用分类，也可以基于内建应用分类）、根据选择的规则类型输入源或目的端口、源或目的 IP，点击 添加设置 配置成功。

编辑自定义应用：选择需要修改的应用，点击 编辑 按钮即可修改。

删除自定义应用：选择需要删除的应用，点击 删除 即可。

- **反馈无法识别的应用**

如果您发现某个网络应用程序的流量无法被本设备正确识别，导致您无法对该应用进行有效控制，您可以点击 反馈无法识别的应用 按钮，根据弹出窗口中提供的方式反馈给我们，锐捷云中心将对您反馈过来的应用进行分析，并加入到特征库中，以满足您的使用需要！

1.3.7.6.2 自定义网站分组

自定义网站分组配置页面如下，该页面显示了当前系统已存在的所有网站分组以及每个网站分组包含的网站类：

- **网站分组**

设置网站分组主要是方便用户对公司内部员工访问的网站类型做统筹管理，确保公司内部网络流畅且带宽不被浪费于工作无关的网站上。

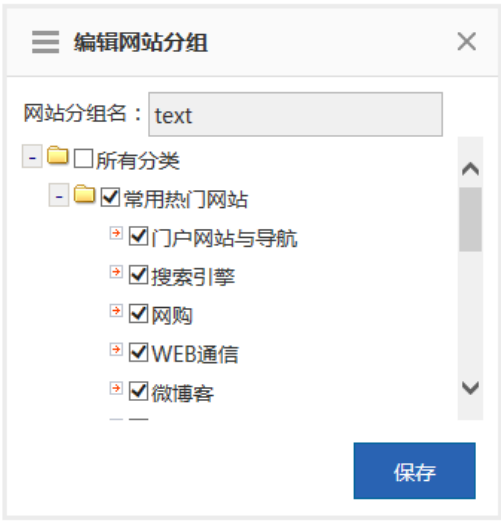
1. 新增自定义网站分组：

点击  按钮可以自定义网站分组：

输入网站分组名称、勾选该分组需要包含的网站类，点击  即可新建一个网站分组。

2. 编辑网站分组：

点击自定义网站分组主页面表格中的 编辑 按钮可以重新分配某个网站分组包含的网站类：



勾选需要包含的网站类，取消不需要包含的网站类，点击 保存 按钮即可。

3. 删除网站分组：

点击自定义网站分组主页面表格中的 删除 按钮可以删除选中的网站分组。

- **自定义网站类**

除了系统内建的网站类，您还可以自己定义其他网站类，如将某几个相似的网站划分到一个网络类中。自定义网站类和系统内建的网站类一样，可应用于各种行为策略中。

点击自定义网站分组主页面的 自定义网站类 按钮将弹出自定义网站类配置窗口：

创建自定义网站类：输入自定义网站类名称，输入能够标识该网站类的意图或用户的描述信息，输入该网站类需要包含的网站域名（多个域名以“，”隔开），点击 添加设置 配置成功。系统最多允许配置 100 个自定义网站类。

编辑自定义网站类：选择需要修改的网站类，点击 编辑 按钮即可修改。

删除自定义网站类：选择需要删除的网站类，点击 删除 即可。

1.3.7.6.3 时间对象

可以定义时间对象，用于策略设置时候使用。

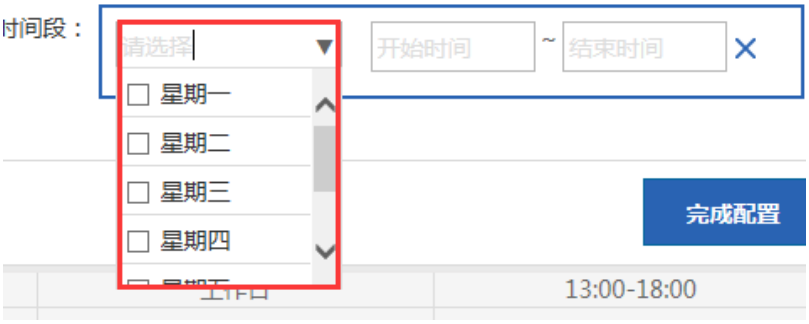
5. 添加时间对象：点击 添加时间对象 ，在弹出窗中输入对象名称，选择时间段，支持设置多个时间段。

例如新建一个 工作时间 对象：

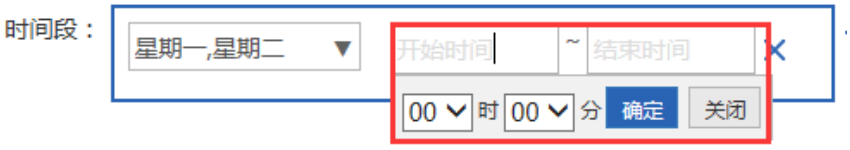
（5） 对象名称：在对象名称 

输入时间对象名称；

（6） 时间段周期：选择时间段的周期，即选择每周从周一到周日



（7） 时间段：设置时间段



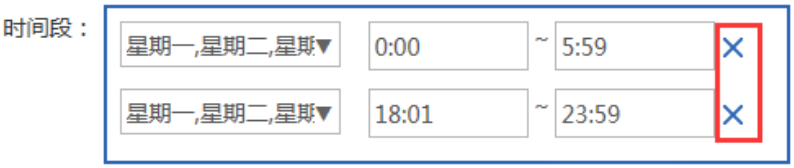
（8） 点击添加另一个时间段

完成后点击 完成配置 按钮生成一个时间对象：

6. 编辑时间对象：选择需要编辑的时间对象点击 编辑 按钮，在弹出窗中即可添加，删除，修改对应的时间段。

7. 删除时间对象：若需要某个时间对象，在列表中选择该时间对象，点击 删除 按钮即可。

8. 删除时间段：若需要删除某个时间对象的某个时间段，在列表中选择对应的时间对象，点击编辑在弹出窗中选择需要删除的时间段，点击 ✕ 按钮，可以删除某个时间段。

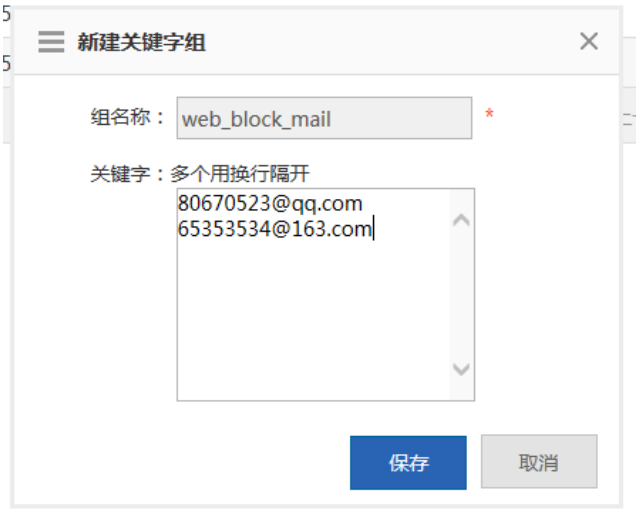


1.3.7.6.4 关键字组对象

关键字组对象是用于内容审计策略时使用的 ,你可以在这里添加你需要审计的内容的关键字 ,然后在策略配置中关联该对象。

新建关键字组：点击 新建关键字组 ，在弹出窗口中，输入关键字组名称和该关键字组需要包含的关键字（多个关键字用换行隔开），点击 保存 即可。

编辑关键字组：在关键字组对象主页面的表格中，选中需要编辑的关键字组，点击 编辑 ，在弹出窗口中，可以新增关键字，或者删除不需要的关键字。



删除关键字组：在关键字组对象主页面的表格中，选中需要编辑的关键字组，点击 删除 即可。

1.3.8 加速

1.3.8.1 线路捆绑

- **配置向导**

首次配置线路捆绑，配置页面如下图所示

点击“开始配置”按钮开始线路捆绑配置，进入如下页面：

可以根据实际情况(公司总部 or 分支机构)选择“总部”或者“分支机构”进行配置。下面将分别介绍总部和分支机构的配置。

- **总部配置**

在上图的“网络位置”配置页面中勾选“总部”类型的线路捆绑设置之后，点击左下角的 下一步 按钮，进入如下页面：

设置分支接入验证码，当分支通过线路捆绑接入总部时，需要输入该验证码进行验证

添加需要加速的业务资源，比如设置在总部内网的 OA 系统，填写业务资源服务器地址。可以添加多个业务资源。对已添加的业务资源可通过删除按钮删除

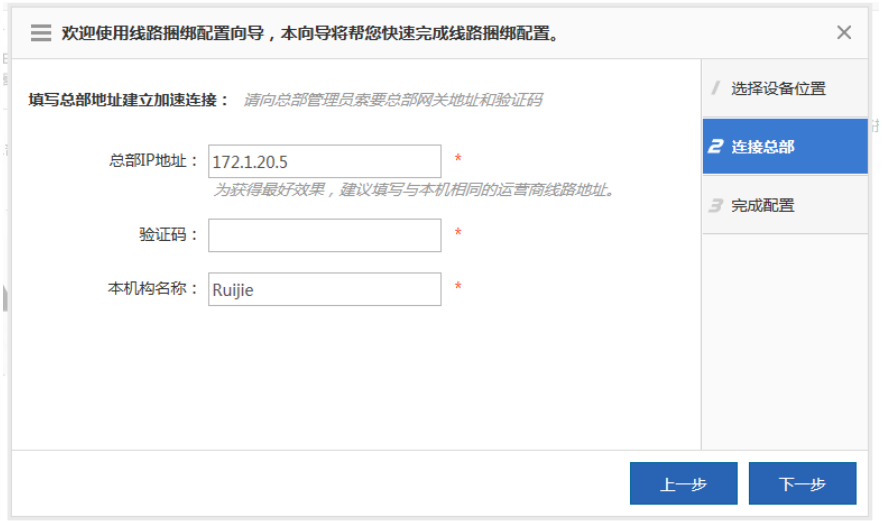
然后点击“下一步”，进入下一个配置界面

该页面显示了你已配置的相关信息，点击 另存到本地PC 可将相关配置信息保存到本地文本中，以后如果忘了配置信息，可通过查看保存的文本

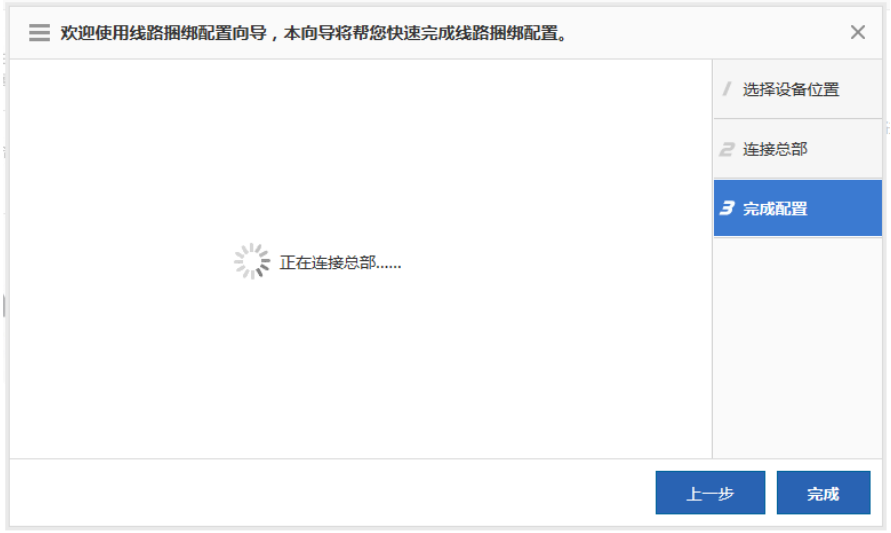
点击“完成”，完成线路捆绑配置

- **分支机构配置**

在上图的“网络位置”配置页面中勾选“分支”类型的线路捆绑设置之后，点击左下角的 下一步 按钮，进入如下页面：



填写要连接到总部的 IP 地址和验证码，总部 IP 地址和验证码可向总部管理员索要 IP 地址跟验证码。同时填写本机构名称，然后点击下一步，进入下一个配置页面

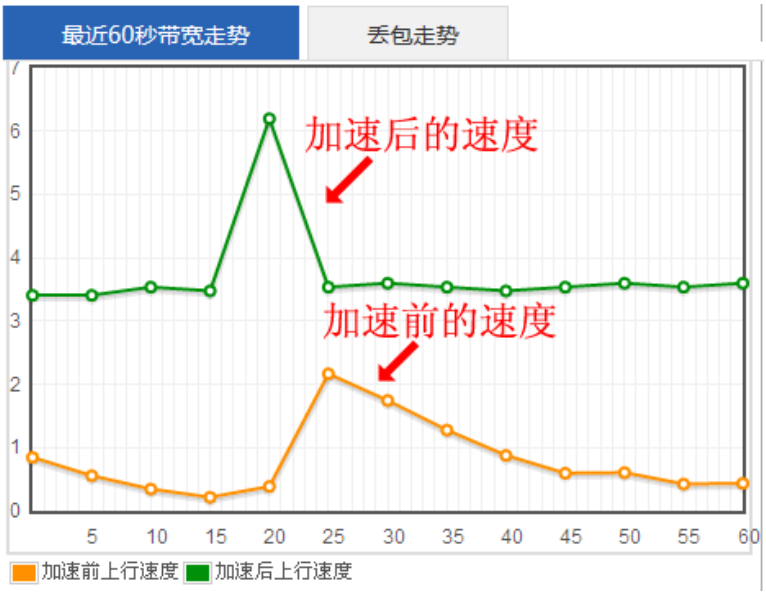


显示正在连接总部，连接成功后，点击“完成”完成线路捆绑配置。如果提示连接失败，返回上一步，检查下你填写总部 IP 地址跟验证码是否有误。

1.3.8.1.1 加速状态

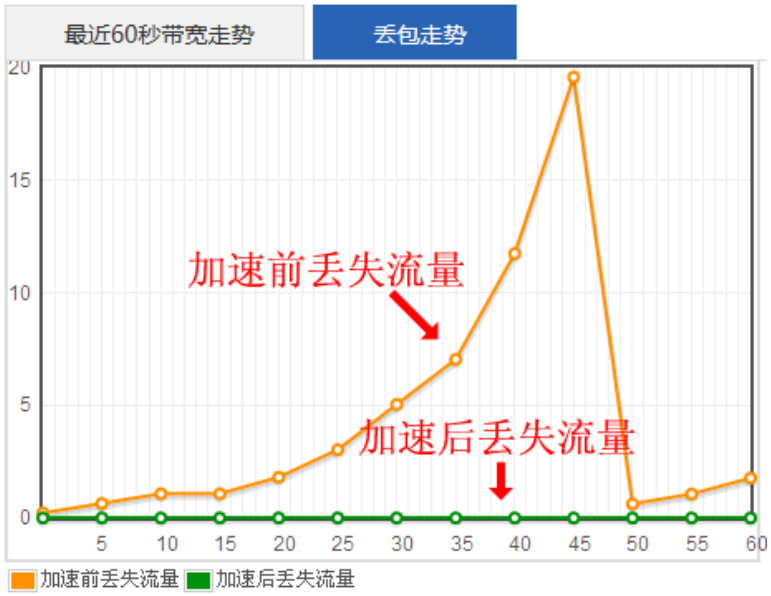
在总部模式下完成线路捆绑配置后，可看到如下页面

1. 当前加速实时情况



该页面显示当前加速上行实时加速情况：

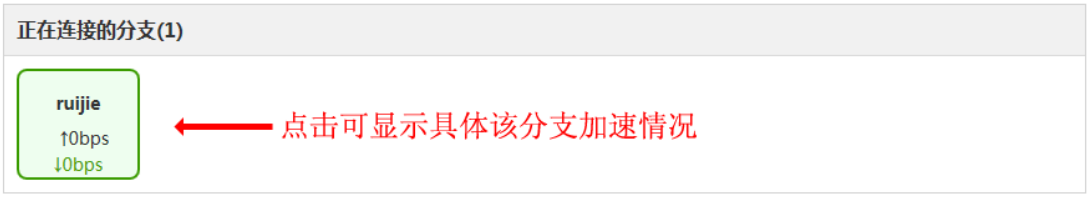
- 左边加速图显示了当前通过线路捆绑传输速度提高了多少，同时还显示了加速前速度跟加速后的速度
- 右边走势图显示了最近 60 秒加速的情况，其中橙色走势图显示是加速前的速度走势，绿色走势图显示的是加速后的速度走势
- 点击右图上的选项卡“丢包走势”可以查看最近 60 秒丢包走势情况如下图所示：



其中橙色走势图显示是加速前的丢包走势情况，绿色走势图显示的是加速后的丢包走势情况

- 你可以更改 上行加速状态 查看上下行的当前加速情况。

2. 正在连接的分支

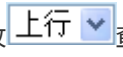


只有在总部模式下才会显示正在连接的分支，显示了目前连接到总部的分支，点击分支可查看该分支具体加速情况如下图：

左边加速图显示该分支当前通过加速提高了多少，以及加速前速度，加速后速度。后边走势图显示该分支最近 60 秒加速前的速度走势，加速后的速度走势。点击右图上方选项卡还可以查看丢包走势情况。

3. 正在加速的业务系统

该页面显示了目前正在加速的业务：

- 左边饼图显示各业务加速的占比情况，鼠标移到饼图上显示各业务的速度各占比
- 右边表格显示正在加速的各业务名称以及上下行流量
- 你可以更改 

查看上下行的各业务当前加速情况

1.3.8.1.2 加速设置

- **总部模式加速设置**

以下是当设备为总部模式时候下的设置页面

加速业务设置：设置你需要加速的业务资源地址，可以添加新业务资源地址和删除已加的业务资源地址

加速连接设置：可以开启或关闭用于加速的外网线路，开启时要填写相关的端口号，默认情况下可以使用默认值

加速状态：可以对于运行中的线路捆绑业务关闭，关闭后将影响接入总部的分支，关闭时候有两种模式可以选择，如下图：

一种是暂时关闭该功能，但在设备上还保留着配置，另一种是完全关闭，关闭后还会删除配置。可以设置新的分支连接总部验证码，修改完成后建议及时通知分支修改连接总部验的证码

高级配置：可以开启或关闭丢包恢复处理。

- **分支模式加速设置**

以下是当设备为分支模式时候下的设置页面

基本参数：可以对于运行中的线路捆绑业务关闭，关闭后将会使已建立的连接失败，关闭时候有两种模式可以选择，如下图：

一种是暂时关闭该功能，但在设备上还保留着配置，另一种是完全关闭，关闭后还会删除配置。当总部修改了分支接入验证码时，可以通过修改，填写新的验证码。还可以修改本机构名称

加速连接设置：可以开启或关闭用于加速的外网线路，开启时要填写相关的端口号，默认情况下可以使用默认值，同时还要填写要连接到总部的 IP 和端口

高级配置：可以开启或关闭丢包恢复处理。当总部没有配置服务资源时，可以添加加速网段配置：

首先要勾选“开启加速网段配置”，然后点击添加，填写本地要加速的网段，连接到总部要加速的网段，可实现在本地某些网段和本部某些网段的加速功能，可以添加多个对应关系。

1.3.8.2 应用缓存

Web 提供应用缓存的配置界面，如下图

1.3.9 安全

1.3.9.1 本地防攻击

防攻击就是对需要进入控制层面处理的数据报文进行分类、过滤、限速，实现对数据报文的控制，防止攻击行为，从而达到保护控制层面的关键资源的目的。

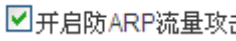
进入防攻击设置页面，如下图所示：


本地防攻击
ARP欺骗检测：检测内网ARP攻击
查看ARP嫌疑列表：【ARP欺骗嫌疑列表】
防流量攻击：开启防流量攻击
攻击流日志：【当前的攻击日志】【历史的攻击日志】
禁止ping：禁止内网ping设备 禁止外网ping设备
禁止ssh telnet：禁止内网ssh telnet 禁止外网ssh telnet
禁止snmp管理：禁止内网snmp管理 禁止外网snmp管理
禁止web登录：禁止内网登录设备web系统 禁止外网登录设备web系统
web访问端口：80 (80,1025-65535)默认为80
保存设置
恢复默认设置


本地防攻击
帮助
防ARP流量攻击：开启防ARP流量攻击 （设备每秒处理的ARP报文不超过10个，多余ARP报文将被过滤掉）
防ARP欺骗：防主机对整网ARP扫描
查看ARP嫌疑列表：【ARP欺骗嫌疑列表】
开启可信ARP：Gi0/0 Gi0/0.3 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7 Gi0/7.1 Ag1
防内网上行攻击：【默认全局配置】【对单个ip进行配置】
新建会话数限制：【默认全局配置】【对单个ip进行配置】【会话数攻击嫌疑列表】
防流量攻击：开启防流量攻击
攻击流日志：【当前的攻击日志】【历史的攻击日志】
禁止web登录：禁止内网登录设备web系统 禁止外网登录设备web系统
禁止ping：禁止内网ping设备 禁止外网ping设备
禁止ssh telnet：禁止内网ssh telnet 禁止外网ssh telnet
禁止snmp管理：禁止内网snmp管理 禁止外网snmp管理
web访问端口：80 (80,1025-65535)默认为80
保存设置
恢复默认设置

1. 防 ARP 攻击

ARP 攻击，是针对以太网地址解析协议（ARP）的一种攻击技术。此种攻击可让攻击者取得局域网上的数据封包甚至可篡改封包，且可让网络上特定计算机或所有计算机无法正常连接。

防 ARP 流量攻击：通过启用 

可以对到达本地的 ARP 流量配置限速，设备每秒处理的 ARP 报文不超过 10 个，多余 ARP 报文将被过滤掉。

防 ARP 欺骗：通过启用 

可以防止黑客窃听到网内所有的 (IP, MAC)地址，伪装成网内的某台 PC 进行 ARP 欺骗。

查看 ARP 嫌疑列表：点击 【ARP欺骗嫌疑列表】 可以查看系统当前有 ARP 欺骗嫌疑的主机列表。

开启可信任 ARP：选中的外网口会自动检测可信任的 ARP，防止 ARP 攻击。

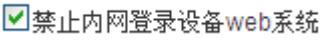
2. 防流量攻击

防流量攻击：启用 

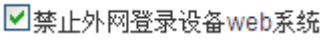
，防送进程的报文超过阀值就丢包，每秒平均 200 个，突发允许 300 个。

攻击流日志：点击 【当前的攻击日志】 可以查看系统当前受到的攻击日志，点击 【历史的攻击日志】 可以查看系统曾受到的历史攻击日志。

3. 其他防攻击

禁止 web 登录：通过启用 

禁止内网用户登录到本设备 web 系统，启用



禁止外网用户登录到本设备 web 系统。

添加管理 IP：这里输入的 Ip 地址 是管理员的 IP，也就是不受流量限速影响的 IP 地址，主要是为了提高管理员管理设备的效率。点击【更多】更方便查看和管理：

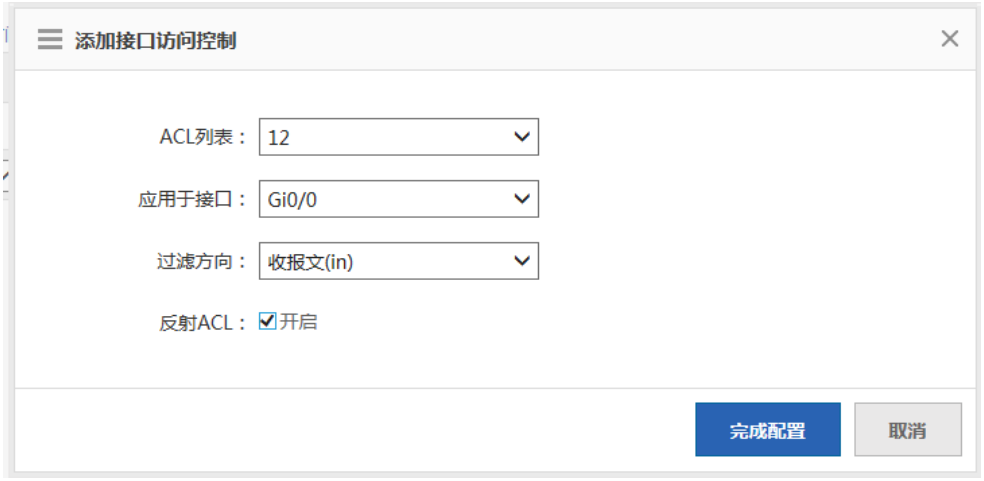
禁止 ping：勾选 禁止内网ping设备 、 禁止外网ping设备 可以禁止内网用户或外网用户 ping 同设备，禁止 ping 会防止掉一些不好的报文，因为一些报文发现 ping 不通就不再侵犯了。

web 访问端口：默认为 80 端口，如果您修改了端口号，那么管理设备的时候需要在地址栏后面添加端口号才能访问到设备，通过 http://ip 地址:访问端口来访问设备。

1.3.9.2 接口访问控制

点击 ＋添加接口访问控制 在弹出窗中选择 ACL 列表号匹配到一个接口，设置报文过滤方向（in or out）点击 完成配置 按钮就可以生成一条访问控制列表，起到防火墙的作用。

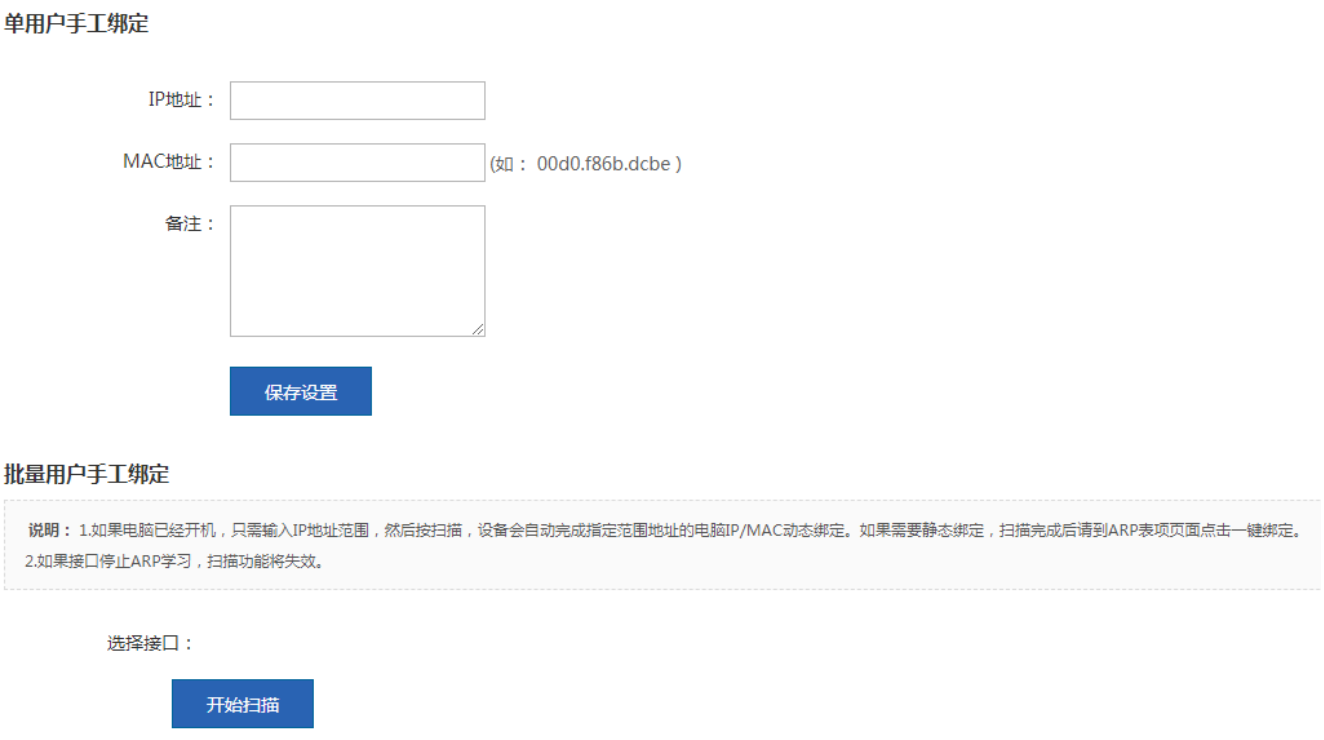
防火墙支持基于状态跟踪的 ACL。勾选反射ACL： ☑开启 支持反射 ACL 的配置。



1.3.9.3 ARP 表项

添加了禁止未静态绑定的内网主机通过选项。

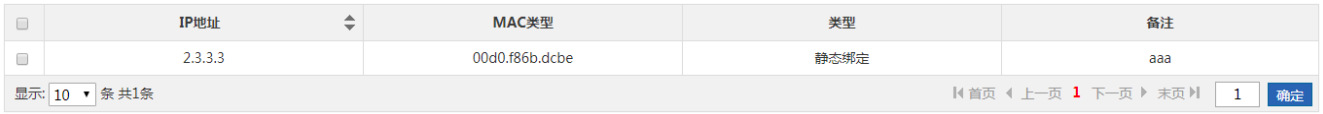
1. 静态绑定 IP/MAC：静态绑定 IP/MAC 有两种方式，一是针对单用户一个一个手工配置，二是通过整网扫描的方式批量绑定。点击 手工静态绑定 弹出窗口如下：



单用户手工绑定：只需输入 IP 地址和 MAC 地址，点击 保存设置 即可。

批量用户手工绑定：选择要扫描的外网口，指定扫描地址范围（若不指定地址范围则整网扫描），点击 开始扫描 ，设备会自动完成指定范围地址的电脑 IP/MAC 绑定。如果接口停止 ARP 学习，扫描功能将失效。

2. ARP 表项



以上表格显示了用户通过静态绑定或系统动态绑定的 IP/MAC 表项。

3. 删除静态绑定

在 ARP 表项中，选择需要删除的静态绑定的 IP/MAC 表项，点击 

即可。

4. 将动态绑定转为静态绑定

在 ARP 表项中，选择需要转为静态绑定的动态绑定的 IP/MAC 表项，点击 

即可。

5. ARP 功能设置

停止 ARP 学习：勾选需要停止 ARP 学习的接口，该接口上动态绑定的 PC 将不能上网，只允许静态绑定 MAC 的 PC 上网。

开启免费 ARP 请求：当设备的网络接口做为下联设备的网关时，如果下联设备中有冒充网关的行为，若该接口开启了开启免费 ARP 请求，则可以在此接口配置定时发送免费 ARP 请求，公告自己才是真正的网关。

1.3.9.4 ACL 访问列表

利用该功能可以配置 ACL 对象，用于提高网络安全配置时使用。如下图所示。

1. **添加 ACL**：

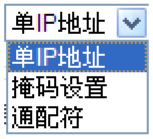
点击 添加 按钮会弹出添加 ACL 弹出窗，选择 ACL 的类型：标准 ACL（控制源地址）或者扩展 ACL（细化控制数据流），输入 ACL 列表的名称后点击 确定 。

2. 添加 ACL 规则

点击 添加ACE规则，在弹出窗中设置对应的访问控制规则。

标准 ACL（控制源地址）：选择访问动作和生效时间，输入 IP 地址，点击 确定 按钮，就可以生成一条标准 ACL 规则。

扩展 ACL（细化控制数据流）：选择访问动作、协议类型和生效时间，配置对应的源 IP 地址、目的 IP 地址、源端口和目的端口，点击 确定 按钮，就可以生成一条扩展 ACL 规则。

源地址和目的 Ip 地址中有一个地址类型选择 

：

单 IP 地址：输入源或目的地址的单个 IP 地址；

掩码设置：输入源或目的地址的 IP 地址段，以掩码方式的地址段；

通配符：输入源或目的地址的 IP 地址段，是以通配符的方式输入地址段的。

1 其中源或目的的 IP □□□□□□□□□□□□ □□□□□□□□□

2 通 符 码 定 当 □□□□ 一个 IP 地址与其他的 IP 地址进行比较时，该 IP 地址中哪些位应该被忽略。通配符掩码中的 “ 1” □□□□ IP □□□□□□□□□□“ 0” □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□0.0.0.0 □□□□□□□□□□□□

3. **ACL 访问控制列表**

□	序号	源IP/通配符	源端口	访问控制	协议	目的IP/通配符	目的端口	生效时间	状态	操作
□	1	任意		允许				所有时间	生效	编辑 | 移动
□	2	12.12.5.5/0.0.0.0		允许				晚上	生效	编辑 | 移动

显示: 10 条 共2条 首页 上一页 1 下一页 末页 1 确定

点击 移动 按钮可以调整 ACL 规则顺序。

点击 编辑 可以对选中的 ACL 规则进行编辑。

在列表中勾选需要删除的规则，点击 ✕删除选中 可以删除选中的 ACL 规则。

防共享接入

1.3.9.5 连接数限制

通过该功能可以限制通过设备总会话数。全局会话数配置页面如下图所示：

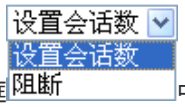
添加了设备抗攻击的设置。

1. **新建会话数限制策略**

点击  新建会话数限制策略，会话数限制有两种类型：基于用户和基于 ACL。

1) **基于用户的会话数限制策略**：

选择用户：点击 选择用户 ，在弹出的用户选择窗口上勾选需要限制会话数的用户，点击 确定 即可：



控制方式：在下拉框 中选择控制方式。选择“阻断”则所选用户将不允许访问外网；选择“设置会话数”则需要设置最大总会话数和每 IP 最大会话数，会话数范围 1~200000(会话数范围依产品型号不同而有所差别)。

2) **基于 ACL 的会话数限制策略**：

选择 ACL 号：下拉框 1 中列出了系统已配置的 ACL 号，您可以从中选择需要会话数限制的 ACL 号进行配置，也可以点击 【新建ACL访问控制列表】 新建一个 ACL 进行配置，新建 ACL 访问控制列表操作请参考 安全 》 ACL 访问列表 页面配置。

控制方式：在下拉框 设置会话数 / 设置会话数 / 阻断 中选择控制方式。选择“阻断”则所选 ACL 将不允许访问外网；选择“设置会话数”则需要设置最大总会话数，会话数范围 1~200000(会话数范围依产品型号不同而有所差别)。

2. 会话数限制策略列表

限制类型	选择用户/ACL号	控制方式	最大总会话数	每IP最大会话数	状态	匹配顺序	管理
基于ACL	12	设置会话数	100000	\	生效		编辑 删除
基于用户	fff	阻断	\	\	生效		编辑 删除
基于用户	所有用户	设置会话数	100000	100	生效		编辑 删除

首页 上一页 1 下一页 末页 1 确定

以上表格列出了用户配置的所有会话数限制策略。

限制类型：指出本策略是基于 ACL，还是基于用户。

状态：说明该策略当前是否生效。

会话数限制策略遵循“后配先生效”原则，点击“匹配顺序”栏的 、 按钮可以调整策略优先级，您可以对现有策略的优先级进行调整。

点击 编辑 按钮可以对策略进行修改；点击 删除 按钮可以删除策略。

3. 查看每 IP 流会话数情况

点击 查看每IP流会话数情况 可以查看设备当前需要进行每 IP 流会话数限制的 IP 的流会话数情况：

4、内网 UDP 会话数比例限制

增加内网 UDP 会话数比例限制的配置，点击弹窗进行保存，如下图

注意：限制比例范围为 30-80，默认为不配置，即 0 表示不限制 udp

1.3.9.6 防共享接入

1.3.9.6.1 一键防共享

说明：一键防共享开启后，会下发预定义的配置。

□□

1.3.9.6.2 防共享策略

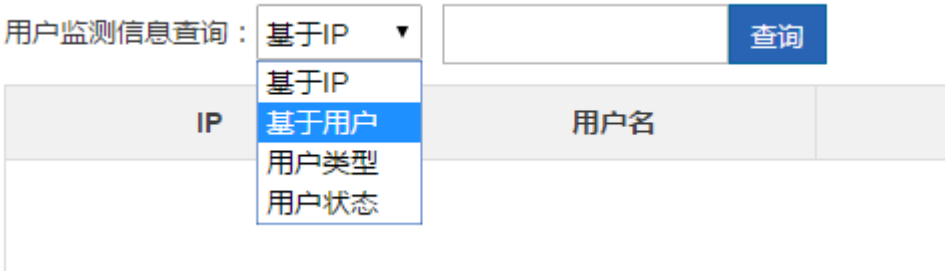
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□ 100 □□

可以添加，删除，编辑策略，还提供自定义放共享标准及白名单配置

1.3.9.6.3 实时监测状态

可以基于 IP 和用户等类型查询

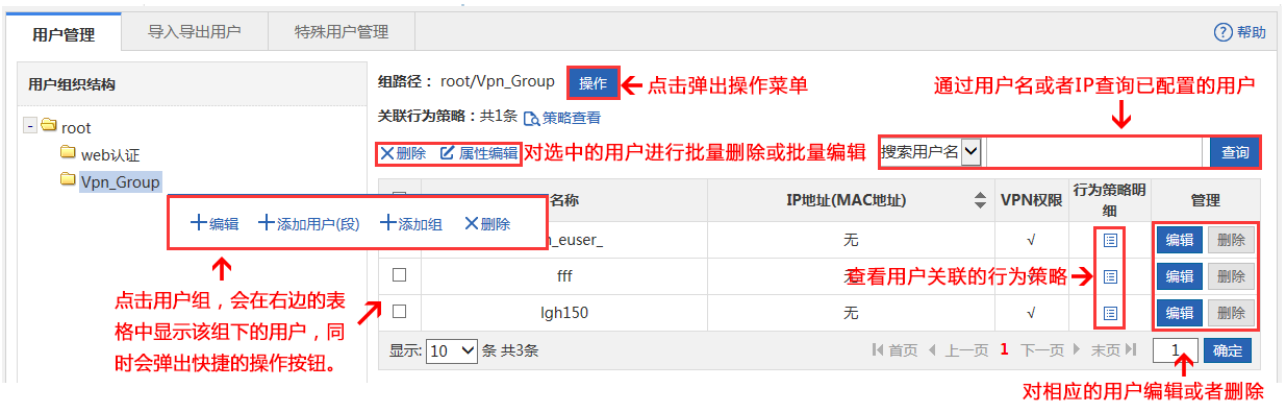


1.3.10 用户

1.3.10.1 用户组织

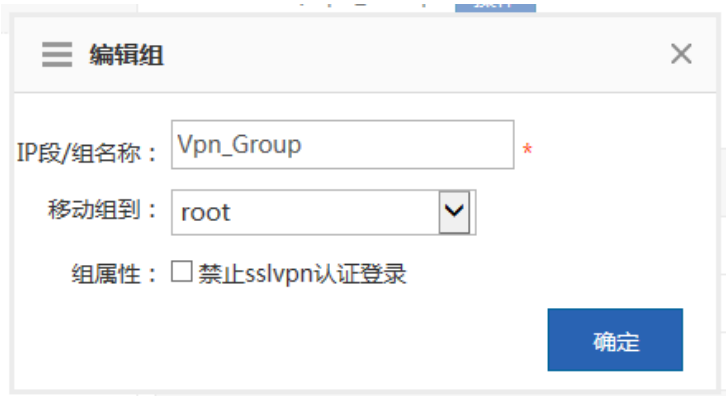
1.3.10.1.1用户管理

设备上的用户，可以是内网用户，也可以是 WEB 认证用户或 VPN 用户。此处是一个用户中心的概念，一个用户即可以登录 VPN，也可以进行 WEB 认证。例如：在财务部下配置一个用户叫“李三”并开启了 VPN 和 WEB 认证功能，同时绑定李三在公司里分配的电脑 IP。这时李三不仅在公司上网时，设备可以正常的审计和流控，李三通过 WEB 和 VPN 登录时同样可以做到审计和流控。这里的 VPN 是指 PPTP、L2TP 或 SSLVPN。



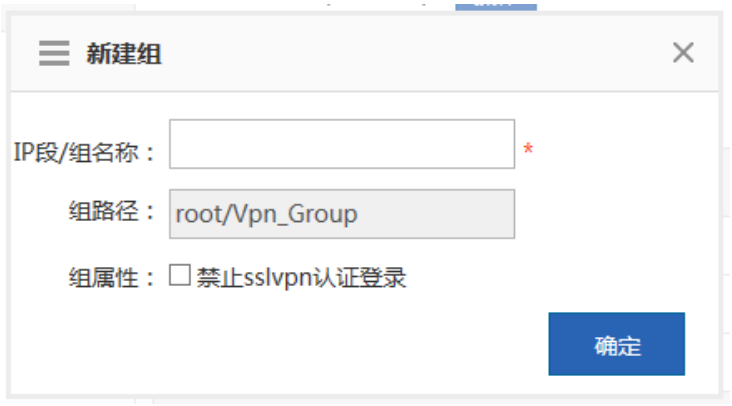
左侧的树状图是系统当前所有用户的组织结构，选中某个用户组，会在右侧显示该对象的相关信息，并可以编辑、修改。要修改用户（组）要先点击对应的用户组。点击后显示如下：

1. 点击 编辑 按钮，可以对选中的用户组进行编辑，如下图所示：



可以修改用户组名称，以及把用户组移动到别的用户组下。

2. 点击 添加组 按钮，可以在选中的用户组下新建子用户组，如下图所示：



用户组名称不能超过 31 个英文字符，一个中文算两个字符。

3. 点击 删除 按钮，会将选中的用户组从用户组织结构中删除。同时会删除掉该用户组下的所有用户。

4. 点击 添加用户(段) 按钮，可以在选中的用户组下新建用户或用户段：

用户名称：该用户的名称，同时也是登录 VPN 或 WEB 认证时的用户名。

允许用途：是否允许使用该用户名和密码进行 WEB 认证或 VPN 登录。如果允许，那密码不能为空，否则不能登录。

密码：进入 WEB 认证或 VPN 登录时使用的密码。

修改密码：只有允许做 WEB 认证用户时才显示，当用户通过 WEB 认证成功后，是否允许该用户自行修改密码。

禁止登录：只有允许做 WEB 认证用户时才显示，勾选后用户 WEB 认证成功后也不能上外网，只能访问内网资源。

IP 和 MAC 地址：该用户的 IP 地址或 MAC 地址，支持配置 IP 地址段，或 IP 和 MAC 地址同时配置。如果是 IP 地址段则要按“起始 IP-结束 IP”这种格式配置。

绑定方式：有单向绑定和双向绑定，只有开启 web 认证的时候才可配置。双向绑定是指上网实名认证时，该用户名只能使用指定的地址，指定的地址仅供该用户使用。单向绑定是指上网实名认证时，该用户名只能使用指定的地址，但其它用户也允许使用该地址！

5. 点击 操作 按钮，同样可以增加组、删除组、添加用户：

6. 用户组的用户列表：

以上表格列出了您在左侧选中的用户组底下的所有用户，你可以对用户进行编辑和删除操作。

7. 点击  会弹出该用户（组）关联的行为策略情况，如下图所示：

点击 行为策略管理 将跳转到“流控>行为策略>高级设置”页面。

8. 设备支持批量编辑用户；先勾选要操作的用户，再点击 删除 属性编辑 进行批量删除或编辑。编辑界面如下图所示：

9. 点击 编辑 可以编辑相应的用户参数，各参数的作用可以参考“添加用户”。

10. 通过 搜索用户名 查询 可以根据输入的用户名或 IP 进行查询，查询的结果会显示到下方表格中。

1.3.10.1.2导入导出用户

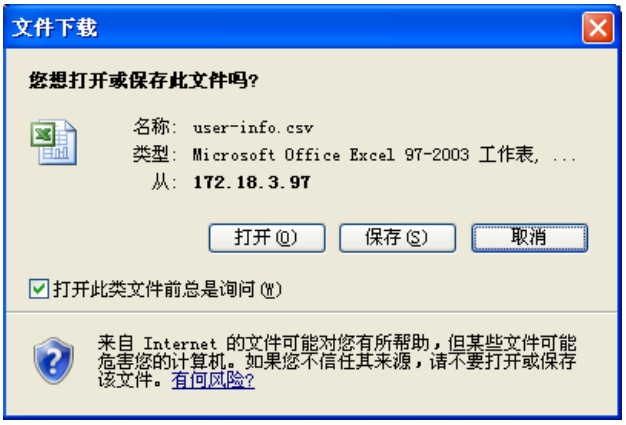
支持通过文件导入导出用户，导入导出用户配置页面如下：

导入用户：通过文件导入用户，方便管理员一步完成用户的编辑。在本地新建一个表格 user-info.csv，在表格内部按照以下格式输入用户的信息：

归属用户组	用户名称	密码	IP地址	MAC地址	是否双向绑定	是否免识别、审计	是否免流控	是否VIP用户	是否设置为白名单	是否禁止上网	是否允许修改密码	是否禁止认证登录	是否作为vpn分支机账号	是否允许web认证账号权限	是否允许vpn认证账号权限	是否禁止sslvpn认证登录
/人力资源部	张三	888	192.168.1.59	00-23-AE-86-B3-E9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
/财务部	李四	888	192.168.1.9-...		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
/研发部/研发5部	王五	888	192.168.1.29	00-87-EF-12-4F-24	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N

点击 浏览... 按钮，找到文件 user-info.csv，点击 导入用户 按钮，会出现文件导入进度条，待进度条加载完成说明文件已经上传成功。

导出用户：点击 导出用户 按钮会弹出如下图对话框。点击 保存(S) 选择保存路径即可。



1.3.10.1.3特殊用户管理

这里的特殊用户包括：VIP/服务器用户、禁止用户、免审计用户，配置页面如下图所示：

VIP/服务器用户：是指需要被保护的关键用户或内网服务器，这里的用户上网速度将被优先保证；点击 VIP/服务器用户将弹出 VIP/服务器用户配置窗口，您可以对 VIP/服务器用户进行添加、删除等操作。具体操作参考“2.6.2 VIP 用户”。

禁止用户：是指黑名单用户，如果您需要屏蔽某用户的上网一切行为，那么在这里直接将该用户设置为黑名单就可以了；点

击 禁止用户 将弹出用户屏蔽配置窗口，您可以对屏蔽用户进行添加、删除等操作。具体操作参考“2.8.1.3 禁止用户”。

免审计用户：是指免内容审计，免流量审计或免流控限制的用户，例如：老板的上网行为一般不希望被审计，那么就可以将

老板设置为免审计用户。点击 免审计用户 将弹出免审计用户配置窗口，您可以对免审计用户进行添加、删除等操作。具体操作参考“2.8.1.4 免审计用户”章节。

1.3.10.2 WEB 认证

WEB 认证包括 WEB 认证和 WEB 认证免认证。

1.3.10.2.1WEB 认证

WEB 认证，即用户认证。

用户认证是一种对用户访问网络的权限进行控制的认证方法，这种认证方式不需要用户安装专用的客户端认证软件，使用普通的浏览器软件就可以进行接入认证。未外部用户上网时，认证设备强制用户登录到特定站点，用户可以免费访问其中的服务。当用户需要使用互联网中的其它信息时，必须在 Web 认证服务器进行认证，只有认证通过后才可以使用互联网资源。如果用户试图通过 HTTP 访问其他外网，将被强制访问 Web 认证网站，从而开始 Web 认证过程，这种方式称作强制认证。认证可以为用户提供方便的管理功能，门户网站可以开展广告、社区服务、个性化的业务等。

设备支持内置认证服务器和外置认证服务器两种方式。选择内置认证服务器无需借助外面的服务器设备，设备本身就已经自带有相应的服务功能；选择外网认证服务器那么需要选搭建好 ePortal 服务器与 radius 服务器。

如果您不需要使用用户认证也可以关闭用户认证，只需选择 

，然后点击 

就可以了。

- **内置认证服务器**

1、 Web 认证信息，您可以根据指定的格式导入“认证用户信息”。

点击 【查看在线用户】 按钮会弹出以下窗口，您可以查看当前在线的认证用户，通过点击 强制下线 可以使选中用户下线,同时还支持对在线用户查询：

2、 认证方式：使用设备内置的 portal 服务器时，进行用户合法性认证时，可以采用本地用户信息的方式、从 radius 服务器上获取用户信息的方式、本地和 radius 服务器并用的方式。推荐使用“优先服务器用户信息”，不过需要先搭建 radius 服务器。

3、 内置服务器端口：是设置内置 portal 服务器的端口，1025 – 65535，默认 8081，在规定访问您可以对端口进行修改。

4、 帐号共享开关：一个账号在同一个时间只允许一个 IP 使用，通过开启 

可以设置允许多个 IP 共享同一个账号，关闭账号共享的情况下，后登陆的账号有效。

5、 SMP 用户修改密码：开启该功能后，需要输入修改密码的 url，这样 SMP 用户就可以通过这个 url 来修改密码。

6、 广告推送方式：设定广告的显示方式，可以先认证后广告或无广告等。

7、 推送广告时间间隔：通过开启推送广告时间间隔，可以设定在多长时间内用户重复登录不弹出广告。

8、 广告地址：广告页面的 URL 地址。

9、 无需认证：开启该功能后配置无需认证用户 ip 无需认证并且推送广告。

10、 记账更新：是配置记账更新检查时间的，主要是对应 SMP/ESS 服务器的配置。

11、 自定义登录 LOGO：开启为自定义 LOGO，关闭为默认系统 LOGO，用户可以自定义自己的内置认证 logo 如下图，

12、 高级设置：点击 

，可以配置更多信息，如下图所示，具体配置参考“2.13.3 用户认证的高级配置”章节：

- **外置认证服务器**

1、 服务器 IP：设置您已经搭建好的外部 ePortal 服务器的 IP 地址，一般情况下，认证页面是认证 ePortal 服务器所提供的。

2、 重定向主页：是在这里输入认证页面 URL 地址，当未认证的用户访问网络资源的时候会制动跳转到该页面，对用户进行认证后就会不跳转。

3、 允许用户接入网段：顾名思义即 ePortal 服务器允许认证的网段地址，不在该接入网段的不需要参加认证。

4、 备用服务器：当主服务器通信失败的时候，将自动切换到备用服务器，编辑服务器配置时候会中断 web 认证业务。如下图，web 可以添加至多 4 个备用 portal 服务器：

5、 通讯密码：设置设备与认证服务器之间的通讯密码。该密码必须认证服务器的通讯密码一致否则将不能生效。

6、 SNMP 团体名：是配置认证设备与认证服务器之间的 SNMP（简单网络管理协议）的参数，因为在外部认证服务器的情况，需要通过 SNMP 来做到与认证设备通讯，从而管理控制用户的上线或下线操作。

7、 SNMP 目的主机：是指认证服务器的主机地址。

8、 只有在存在外部认证服务器的情况下才支持 SNMP 的配置；要成功应用外部服务器的认证功能，必须设置认证设备与认证服务器之间的 SNMP 网管通信参数；包括设置 SNMP 通讯密码、SNMP 目的主机的配置。

9、 高级配置：点击 >> 高级设置 ，可以配置更多信息，如下图所示，具体配置参考“2.13.3 用户认证的高级配置”：

1.3.10.2.2Web 认证免认证

免认证网络资源：输入网络资源服务器的 IP 地址，所有用户（包括未认证用户）都可以访问该 IP，最大允许配置 1000 条规则。

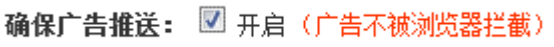
免认用户 IP：该用户可以直接上网，且不会推送广告，最大允许配置 1000 条规则。

10. 免认证网络资源：最多支持配置 50 条免认证网络资源，启动 Web 认证后，未认证用户需先通过 Web 认证，才能访问网络资源。如果允许未认证用户，也可以访问一些免认证的网络资源，需要使用此选项设置免认证的网络资源。设置了免认证的网络资源，如果某网站属于免认证的网络资源，那么所有用户（包括未认证用户）都可以访问该网站。缺省情况下，没有设置免认证的网络资源，未认证用户不能访问网络资源。（注意：这里您可以配置单个 IP 或 IP 段（IP+掩码 形式的 IP 段如：192.168..1.0 255.255.255.0），其中 IP 段也算是一条免认证资源）

11. **免认证用户 IP**：最多支持配置 50 条免认证用户，如果用户属于无需认证用户 IP 范围，那么该用户不需要通过 Web 认证，也能访问所有可达的网络资源。缺省时，没有设置无需认证用户，所有用户都必须先通过 Web 认证，才能访问网络资源。（注意：这里您可以配置单个 IP 或 IP 段（IP+掩码 形式的 IP 段如：192.168..1.0 255.255.255.0），其中 IP 段也算是一条免认证资源）

- **广告推送服务**

保存广告推送服务后，广告推送用户首次进行上网会弹出相应的广告链接地址页面；开启“广告推送服务”后，弹出广告没生效请设置浏览器（internet 选项--隐私--启用弹出窗口阻止程序，不打勾）或者在高级设置里配置“确保广告推送”开启选项。



- **用户认证的高级设置**

1、 **最大 HTTP 会话数**：支持设置每个为认证用户的最大 HTTP 会话数，未认证的用户在访问网络资源时，用户 PC 会发出 HTTP 会话连接请求，HTTP 报文会被设备拦截，并通过重定向要求用户进行 Web 认证。为了防止同一个未认证用户发起过多的 HTTP 连接请求，以节约设备的资源，需要在认证设备上限制未认证用户的最大 HTTP 会话数。由于用户在认证时，会占用一个 HTTP 会话，而用户的其他应用程序也可能占用着 HTTP 会话，因而不建议设置未认证用户的最大 HTTP 会话数为 1。缺省情况下，未认证用户的最大 HTTP 会话数为 255。

2、 **重定向超时时间**：支持设置维持重定向连接的超时时间，因为未认证的用户通过 HTTP 访问网络资源时，其 TCP 连接请求将被拦截，实际上是与认证设备建立起 TCP 连接。在连接建立后，认证设备需要等待用户发出的 HTTP 的 GET/HEAD 报文，然后回复 HTTP 重定向报文后才能关闭连接。设置这个限制可以防止用户不发 GET/HEAD 报文，而又长时间占用 TCP 连接。缺省情况下，维持重定向连接的超时时间为 3 秒。

3、 **重定向 HTTP 端口**：最大允许配置 10 个不同的目的端口号，当用户访问网络资源时（例如使用浏览器上网），此时用户会发出 HTTP 报文，认证设备通过拦截来自用户的 HTTP 报文，来判断用户是否在访问网络资源。当认证设备检测到未认证的用户在访问网络资源时，将阻止用户访问网络资源，并向用户弹出认证页面。缺省情况下，认证设备通过拦截用户发出的端口号为 80 的 HTTP 报文，来检测用户是否在访问网络资源。

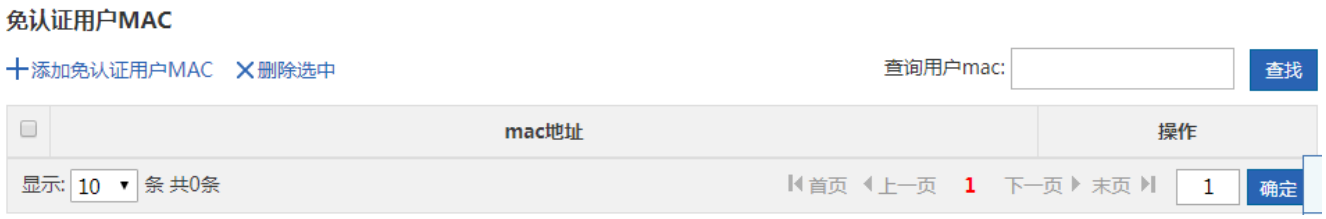
4、 **在线信息更新时间**：设置在线用户信息的更新时间间隔，认证设备维护着在线用户信息，认证设备需要定时地更新在线用户信息，包括在线时间等，以监控在线用户使用网络资源的情况，比如：用户的在线时间大于或等于在线时限，该用户会被停止使用网络。缺省情况下，认证设备每 60 秒更新一次在线用户的信息。

5、 **下线检测模式**：支持设置用户下线检测模式，设置可以基于流量来检测用户是否下线，如果在 15 分钟内，用户流量都没有增加，则认为用户下线。此命令仅用来辅助检测用户是否下线，会存在一些误检的风险。当前检测用户是否下线有以下二种方式：a、用户点击认证页面上的“下线”按钮；b、基于用户流量的检测模式，在 15 分钟内用户流量没有增加，则认为用户下线；默认情况下两种方式都开启。

6、 **IP-MAC 绑定模式**：设置用户 IP-MAC 绑定模式，设置根据 IP 或者 MAC、IP 绑定的模式，在二层网络中，可以选择用户名与 MAC、IP 绑定的模式，如果是三层网络结构，则只能选择用户名与 IP 绑定的模式，否则绑定后会出现网络不通的情况。

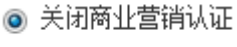
7、 **无需认证用户 IP**：与免认证用户 IP 的区别在于无需认证用户支持推送广告。

12. 免认证用户 MAC：可以针对用户 MAC 进行增删改查



1.3.10.3 商业营销认证

WEB 认证是用户连上网络，在浏览器页面填入用户名、密码后进行认证。用户在认证前无法使用任何 APP 应用访问网络。随着移动互联网的快速发展，尤其是如微信等 APP 的大量出现，如何通过 APP 应用进行认证上网并提升用户认证体验成为网络提供方越来越迫切的需求，并可以与云 AC 或者第三方服务器进行对接，实现微信营销功能。

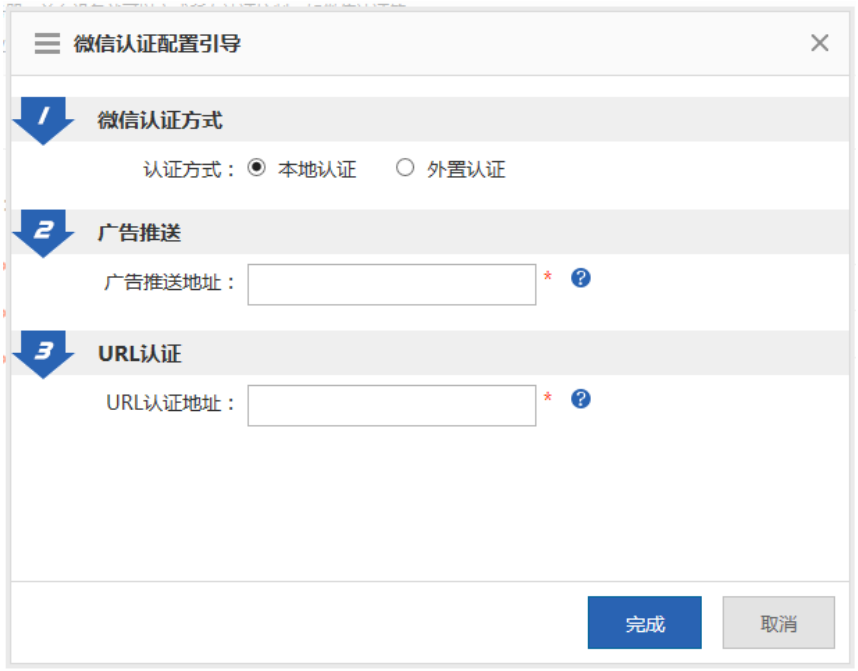
设备支持本地认证和与外置认证两种方式。选择单机内置认证，只要开启关联应用或者配置 URL 认证地址就可以使用；选择与 MCP 联动则需要选搭建好 mcp 服务器。如果你不需要应用认证，可以选择关闭按钮 

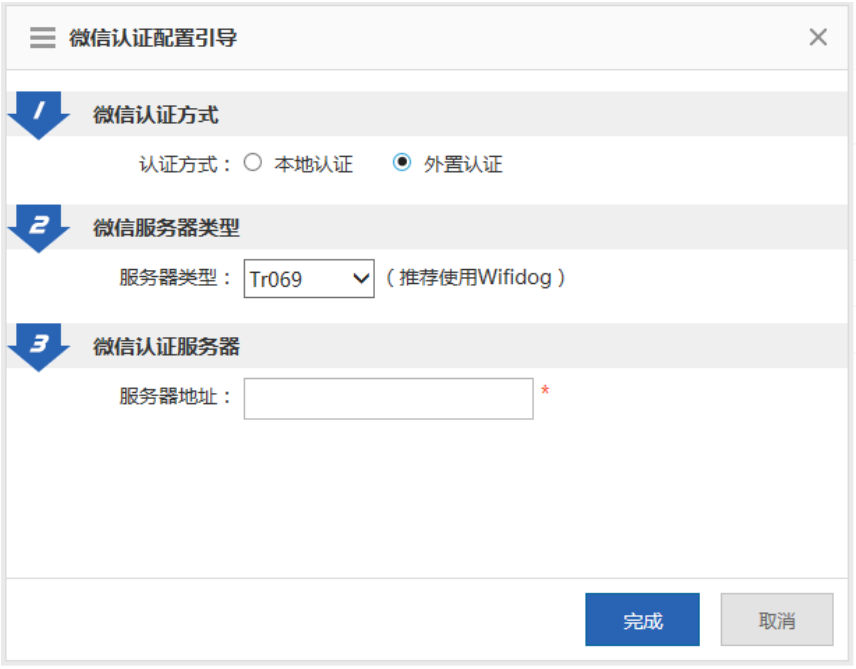
关闭商业营销认证，然后点击确定按钮即可 

。

商业营销认证配置分三个大块，1、基本设置；2、高级设置；3 免认证设置，如下图：

这里专门提供了一个微信认证快捷配置，方便一键开启使用微信认证，如下图：





具体参数功能如下基本设置、高级设置、免认证设置进行调整

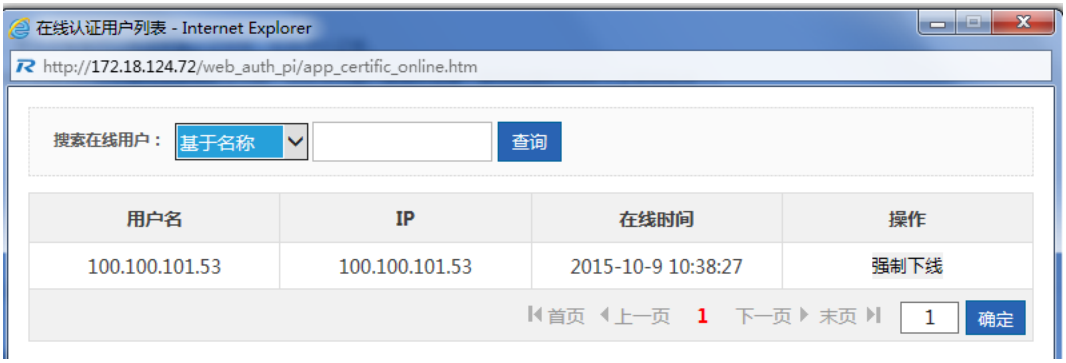
- **基本设置**

包括本地认证和与外置认证两种模式。

1. 本地认证

本地认证配置功能主要有微信关注功能、url 地址认证和推送广告页面，配置完信息点击保存设置即可。

查看在线用户：（可以查看用户名、ip、在线时间以及操作点击下线功能）



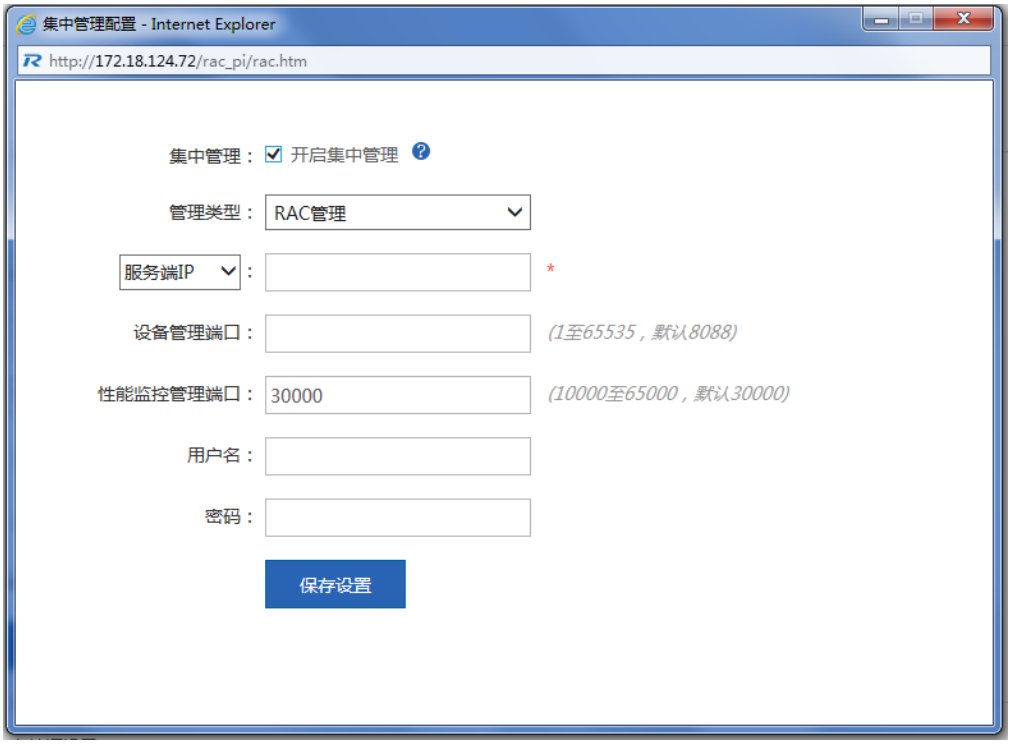
2. 外置认证

外置认证，需要配置对应的 MCP/WMC 服务的环境实现与 MCP/WMC 对接进行认证通过上网，实现功能是短信认证和微信认证等进行上网。

外置认证服务器分为以下几种类型：Tr069、Wifidog、微信连 Wifi 和自定义类型。

① Tr069 需要设置 MCP/WMC 服务器

MCP/WMC 服务器设置：（注意管理类型应该选择 MCP/WMC 管理）



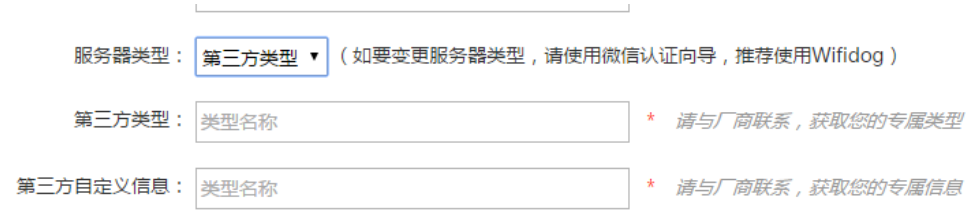
② Wifidog 需要设置检测用户逃生的地址

用户逃生功能配置如下：

③微信连 Wifi 需要设置检测用户逃生的地址和 wifi 网络名称

wifi 网络名称配置和逃生功能地址配置如下：

④自定义类型，支持定制第三方服务器对接，需要售后或者研发支持



其中 Portal 重定向主页和通讯密码是必填的选项。配置完点击外置认证的保存设置按钮 保存设置 即基本设置部署完毕。

3. 关闭商业营销认证

点击保存设置后关闭商业营销认证。

- **高级设置**

高级设置可以设置本地认证和与外置认证公共的配置，如源 IP 地址、mac-by-pass、下线检测模式、网络类型、IP 范围 ssid、允许认证接入网段。

源 IP 地址：指定设备与认证服务器通讯的源 IP 地址，在 ipsec vpn 场景下使用

mac-by-pass：开启该功能后，设备将向服务器发送新用户接入网络消息（只能在二层网络类型时使用）

IP 范围 ssid：可配置不同网段对应到不同的 SSID，用于外置认证服务器策略控制

网络类型：包括 2 层网络和 3 层网络，网络拓扑为三层网络，使用 ip 标示用户，网络拓扑为二层网络，使用 mac 标示用户；

允许认证接入网段：默认是所有用户都会进行认证上网，配置网段后只有该网段才会进行认证上网。

- **免认证设置**

免认证设置包括： URL 白名单、免认证域名、免认证用户 IP、用户 MAC 白名单、用户 MAC 黑名单、免认证外网 IP。

设置其他免认证配置，可以添加按钮 添加 ，如下图添加免认证 URL 白名单：

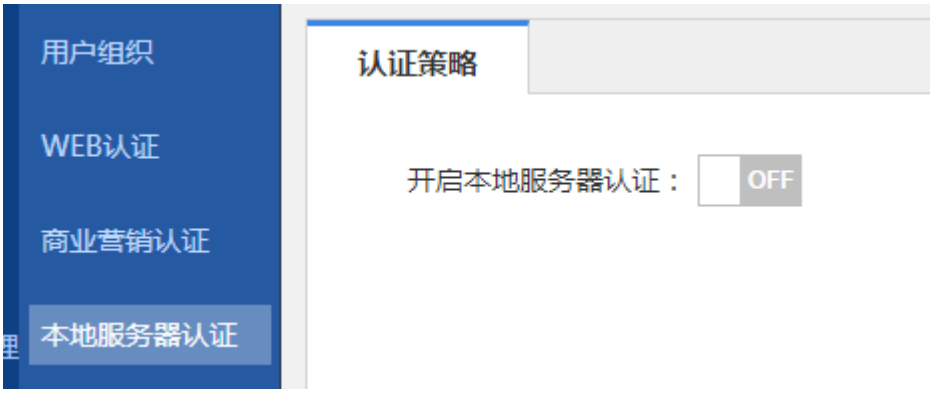
然后点击保存设置即可 保存设置 。

1.3.10.4 本地服务器认证

1.3.10.4.1认证策略

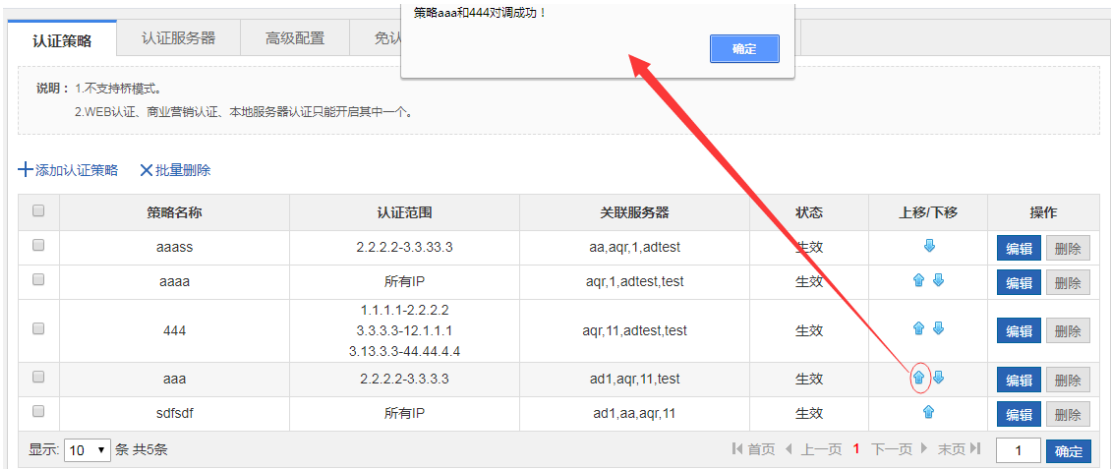
（1）本地服务器认证开关

进入【用户-本地服务器认证-认证策略】菜单后，判断本地服务器认证是否开启，可以进行开启操作。如果认证服务器是关闭状态，本地服务器认证子菜单只有认证策略。



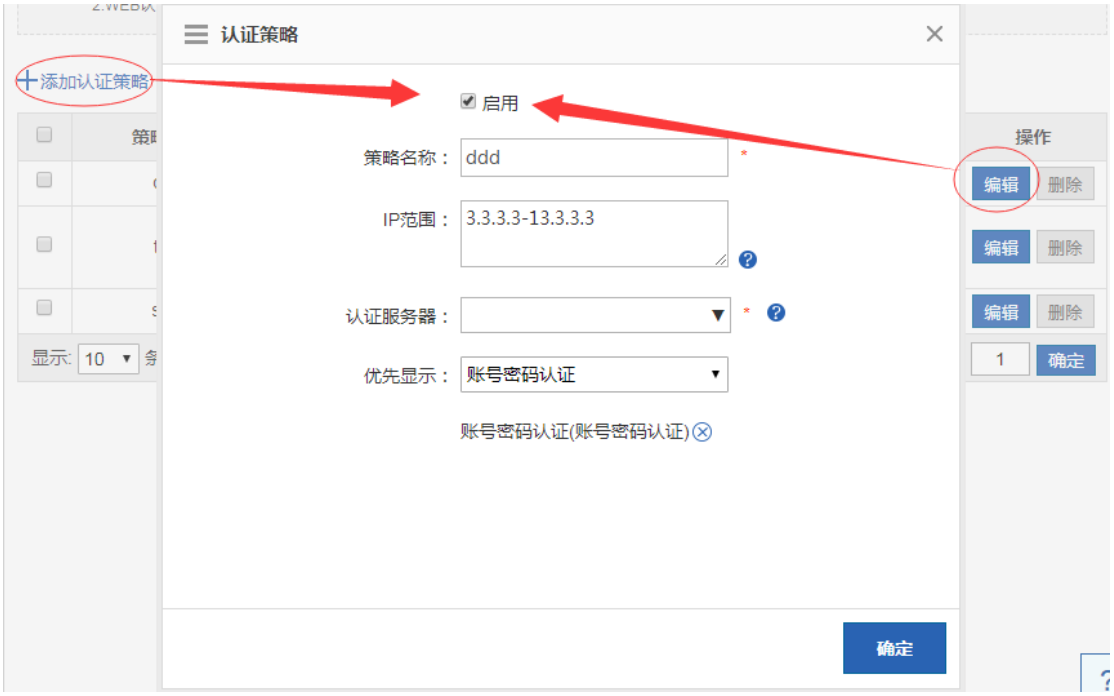
（2）调整认证策略优先级

认证策略表格中点击箭头进行优先级切换。



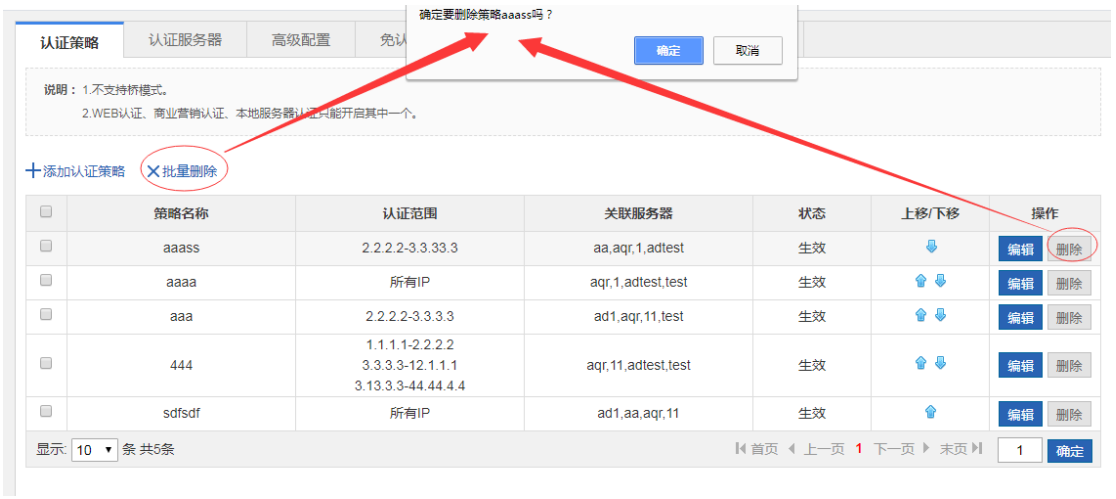
（3）添加/编辑认证策略

点击添加或者编辑，可以配置认证策略。需要点击启用才可以进行内容的编辑。认证服务器是通过【认证服务器】接口来获取。



（4）2.8.5 删除认证策略

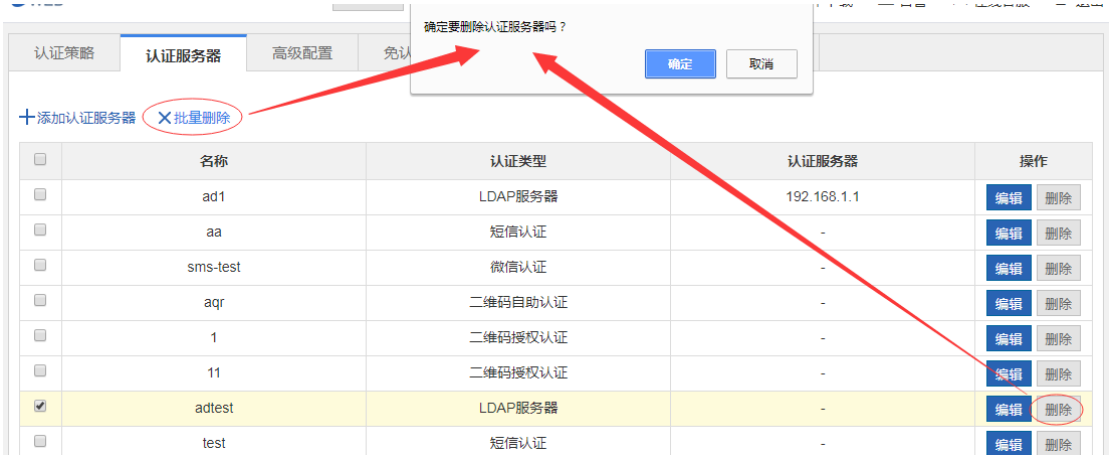
点击删除按钮或者点击批量删除，可以删除认证策略。



1.3.10.4.2认证服务器

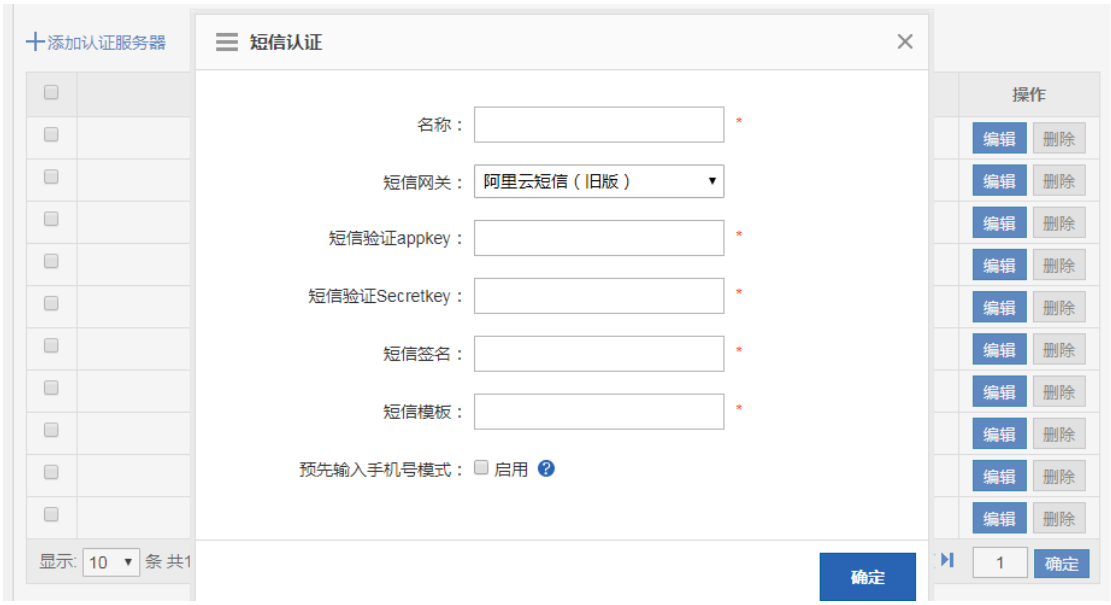
（1）删除认证服务器

点击删除按钮或者点击批量删除，可以删除认证服务器。



（2）添加/编辑短信认证

点击添加或者编辑，配置短信认证

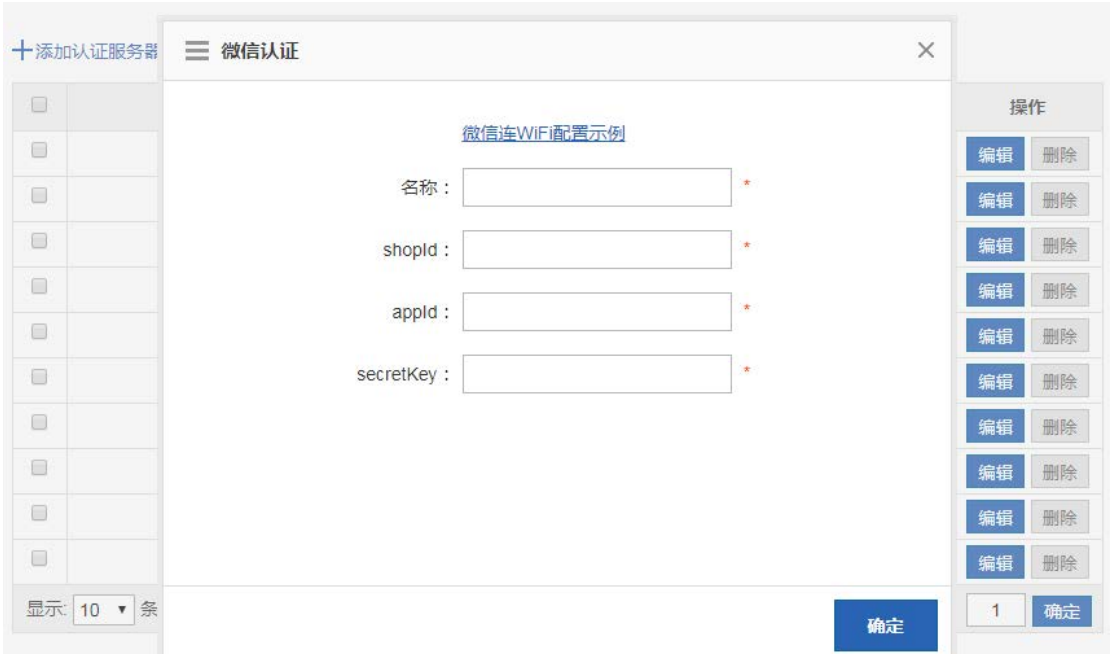


字段	说明
servername	认证服务器名称 名称不能是_PWD_AUTH 或者账号密码认证
servertype	sms：短信认证 qrcode-alone：二维码自助认证 qrcode-authorize：二维码授权认证 act-directory：LDAP 服务器 weixin：微信
isopen	未启用：值为 no；否则为空
smsserver	短信网关 aliyun-v1：阿里云短信（旧版） aliyun-v2：阿里云短信（新版）

keyid	短信验证 appkey
keysecret	短信验证 Secretkey
sign	短信签名
templet	短信模板

（3）添加/编辑微信认证

点击添加或者编辑，配置微信认证

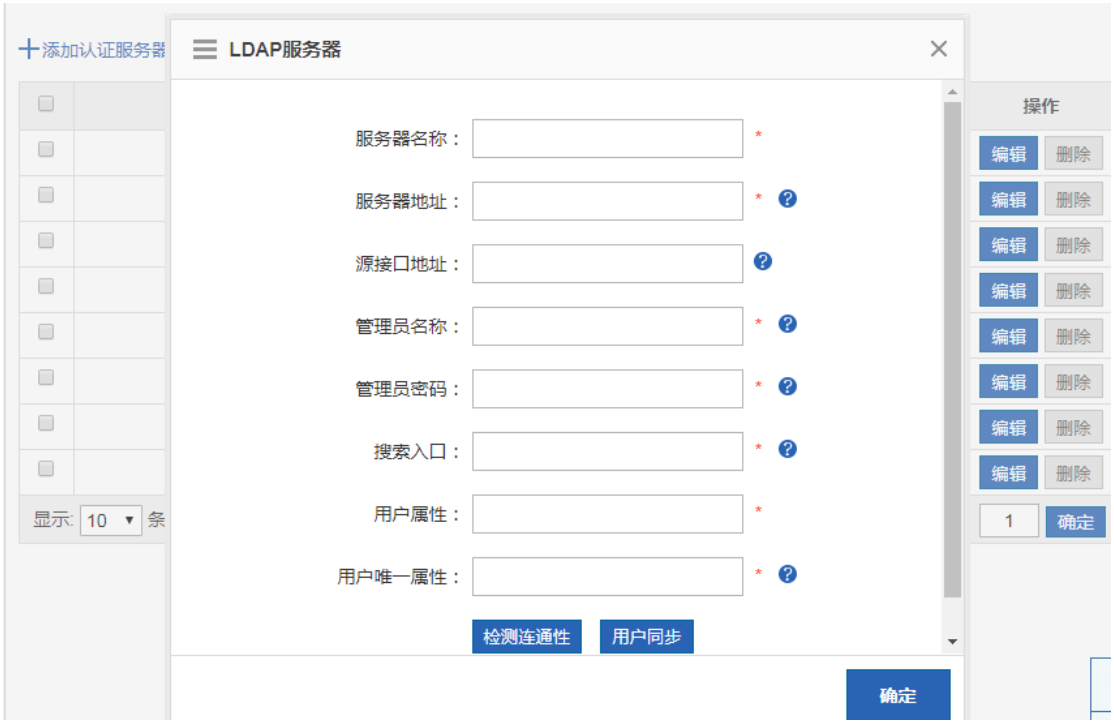


字段	说明
servername	认证服务器名称 名称不能是_PWD_AUTH 或者账号密码认证

servertype	sms：短信认证 qrcode-alone：二维码自助认证 qrcode-authorize：二维码授权认证 act-directory：LDAP 服务器 weixin：微信
ssid	ssid
shopid	shopid
appid	appid
secretkey	secretkey

（4）添加/编辑 LDAP 服务器

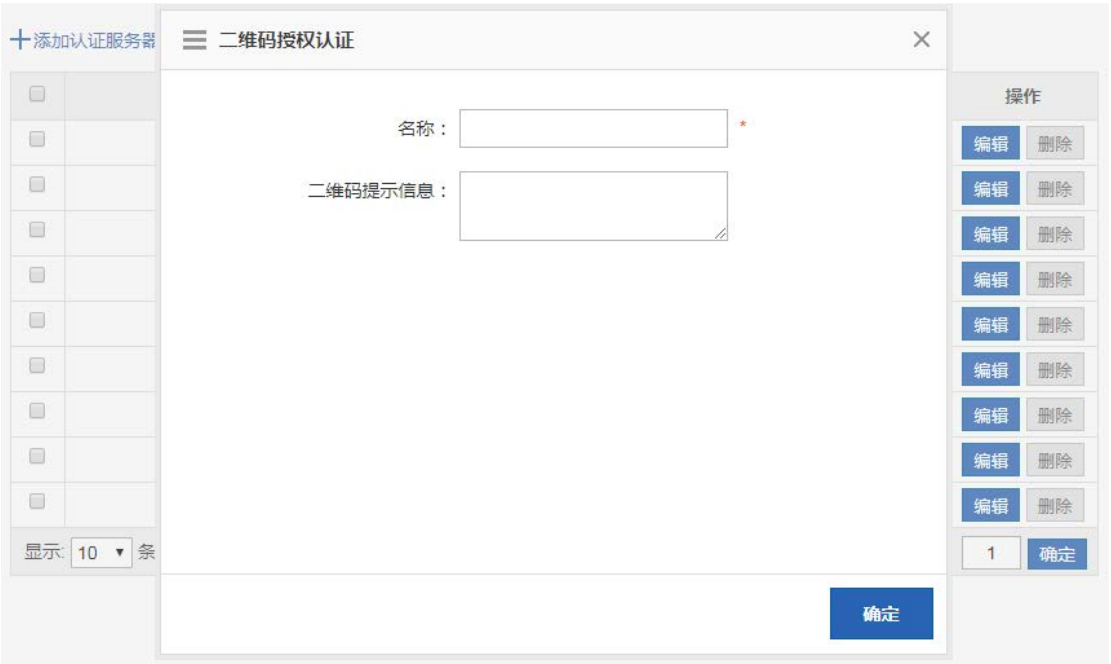
点击添加或者编辑，配置 LDAP 服务器



字段	说明
servername	认证服务器名称 名称不能是_PWD_AUTH 或者账号密码认证
servertype	sms：短信认证 qrcode-alone：二维码自助认证 qrcode-authorize：二维码授权认证 act-directory：LDAP 服务器 weixin：微信
serverip	服务器地址是 ip 格式
serverurl	服务器地址是 url 格式
user	管理员名称
password	管理员密码
searchkey	搜索入口
userattri	用户属性
uniqueattri	用户唯一属性
sourceip	源接口地址，可为空

（5）添加/编辑二维码授权认证

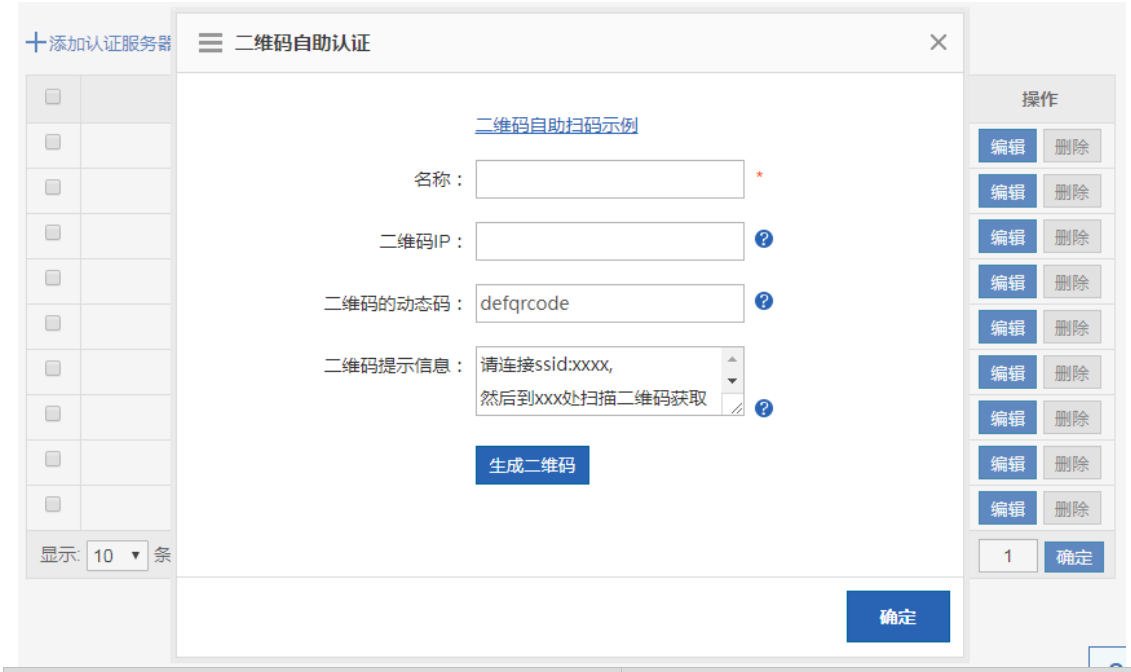
点击添加或者编辑，配置二维码授权认证



字段	说明
servername	认证服务器名称 名称不能是_PWD_AUTH 或者账号密码认证
servertype	sms：短信认证 qrcode-alone：二维码自助认证 qrcode-authorize：二维码授权认证 act-directory：LDAP 服务器 weixin：微信
authcomment	二维码提示信息，为空时下发 no 命令

（6）添加/编辑二维码自助认证

点击添加或者编辑，配置二维码自助认证



字段	说明
servername	认证服务器名称 名称不能是_PWD_AUTH 或者账号密码认证
servertype	sms：短信认证 qrcode-alone：二维码自助认证 qrcode-authorize：二维码授权认证 act-directory：LDAP 服务器 weixin：微信
alonecomment	二维码提示信息，为空时下发”请连接 ssid:xxxx,然后到 xxx 处扫描二维码获取上网权限”

qrcodeip	二维码 IP
qrcodekey	二维码的动态码，为空时下发 defqrcode

1.3.10.4.3高级配置

进入【用户-本地服务器认证-高级配置】菜单后，显示高级配置相关信息。

字段	说明
net-id	网络类型 1：二层网络 2：三层网络
authorize-time	非授权方式上线时长

online-time	授权方式上线时长
data-store.enable	是否开启账号自动记录 mac
user-mac-limit	每个账号自动记录 mac 限制个数
app-auth-inq	0：关闭 1：macbypass 无感知 2：看广告方式无感知
data-store.age-day	账号空闲老化时间
snoop-enable	是否开启通过 DHCP SNOOPIN 获取 mac 功能
flow-detect.enable	是否开启无流量检测下线
flow-detect.time-interval	持续多久
flow-detect.rate	流量小于多少
rdt-https	是否开启开启 https 重定向
wx-state	是否开启微信放行 wx-state 等于 direct 的时候是开启
authorize-chek	是否开启授权管控
restrict-times	被授权用户可继续授权次数
无	限制电脑上网和限制移动终端上网有一个开启 ,终端管控功能就开启
restrict.type==PC	
restrict.g_enable	是否开启限制电脑上网
restrict.time-range	限制电脑上网的例外时间 要有一个'无'的例外时间
restrict.type==MOBILE	
restrict.g_enable	是否开启限制移动终端上网
restrict,name	限制移动终端上网的例外时间 要有一个'无'的例外时间

1.3.10.4.4免认证配置

1.3.10.4.5单点登录

进入【用户-本地服务器认证-单点登录】菜单后，显示单点登录相关信息。

1.3.10.4.6用户权限

进入【用户-本地服务器认证-用户权限】菜单后，显示注册用户和组权限相关信息。

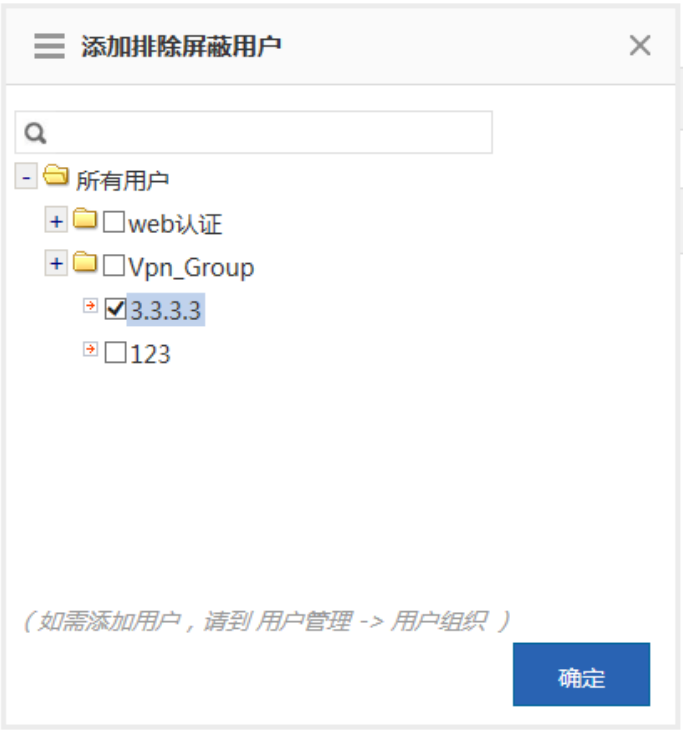
1.3.10.4.7在线信息

进入【用户-本地服务器认证-在线信息】菜单后，显示相关信息。

1.3.10.5 上网屏蔽模式

开启上网屏蔽模式后，所有内网用户将不能通过设备上网，除非将用户设置为“排除屏蔽用户”。上网屏蔽模式配置页面如下：

点击 添加排除屏蔽用户 至少添加一个排除屏蔽用户后，才能勾选 开启上网屏蔽模式 开启上网屏蔽模式。

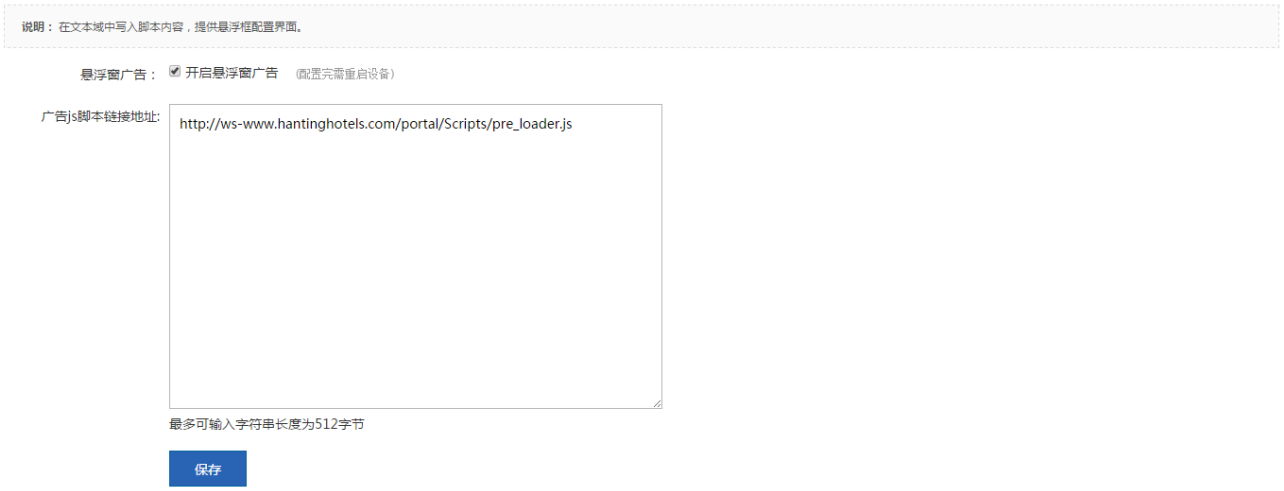


勾选需要排除屏蔽的用户，点击 确定 即可：

点击“删除”栏的 删除 按钮可以删除单个排除屏蔽用户，点击 删除选中用户 可以删除多个选中的排除屏蔽用户。

1.3.10.6 悬浮窗广告

首次开启该功能需要重启设备才能生效，悬浮窗广告的配置如下：



开启悬浮窗功能后，通过设备上网的 pc，浏览网页会弹出广告的效果如下，

1.3.11 网络

1.3.11.1 接口配置

接口配置是实现内部上网的关键配置，这里的配置是否正确关系到内网是否可以正常上网。接口配置页面如下图所示：

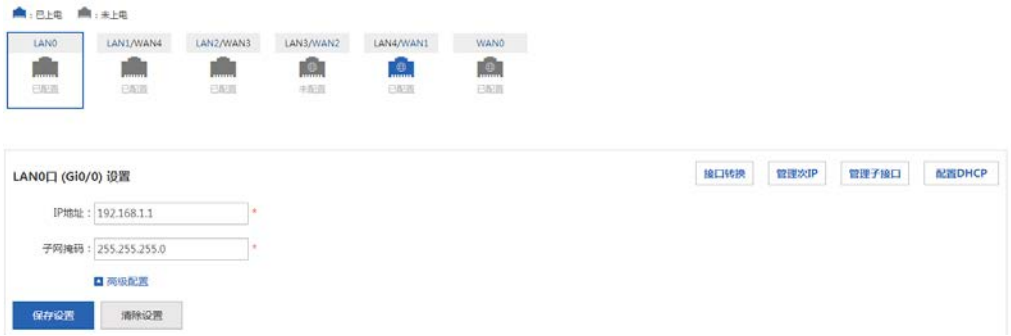
像这样  蓝色高亮显示的接口说明该接口处在上电状态（网线已接上），其中灰度  显示的接口说明该接口未上电，其中  有小地球的接口说明该接口是外网口，没有的话就是内网口。

接口配置在网关模式和网桥模式下的配置不同，接下来将分别为您介绍。

1.3.11.1.1接口基本设置

- **内网口配置**

点击需要配置的内网口即可对选中的内网口进行配置，如点击  ：



去掉了管理次 IP 和子接口管理。

IP 地址：这里输入内网口的 ip 地址，这个 ip 地址就是您内部规划好的网段 ip；

子网掩码：这个是网段对于的掩码地址；

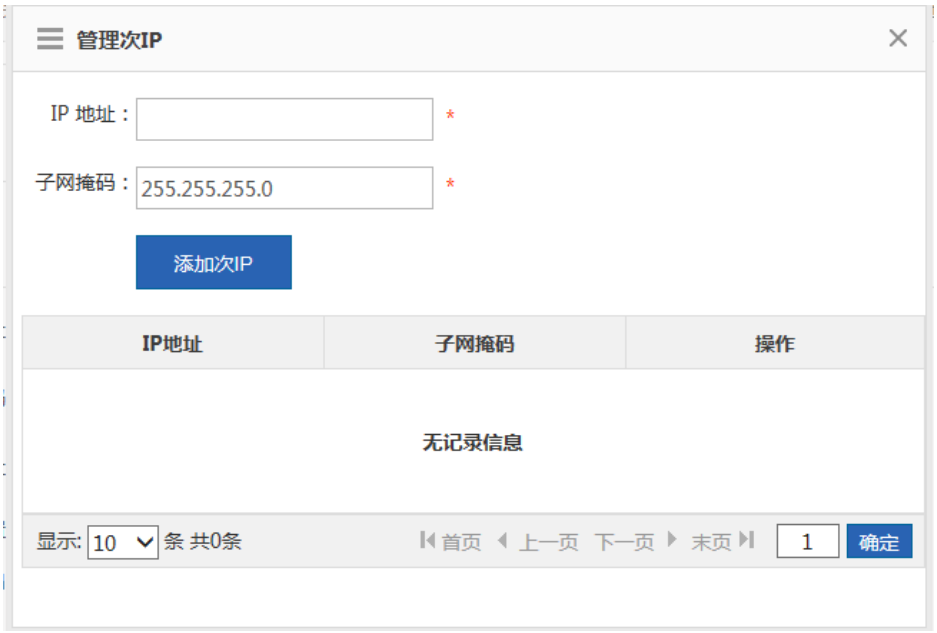
MAC 地址：是接口的物理地址，主要是为了防止内部物理地址冲突时使用的，通常情况下可以不配置。

AnyIp 配置：开启 AnyIp 功能后，内网 PC 可以不配置或随意配置 ip 地址都能达到正常上网的目的，也就是说开启这个功能后可以避免部分 PC 配错 ip 地址导致上不了网的问题。

源进源出：开启此功能后，从教育网接口进来的报文，还是从教育网接口出去，回报文时不再查找路由表，这样能防止如电信的用户的 DNS 请求报文从教育网接口进来，在回报文时去查看路由表发现要从电信接口出去，而运营商会做相应阻止导致丢包解析不成功的情况。

次 IP：以太网接口支持多个 IP 地址，次 IP 为除首次配置的 IP 地址之外的其它 IP 地址。点击 

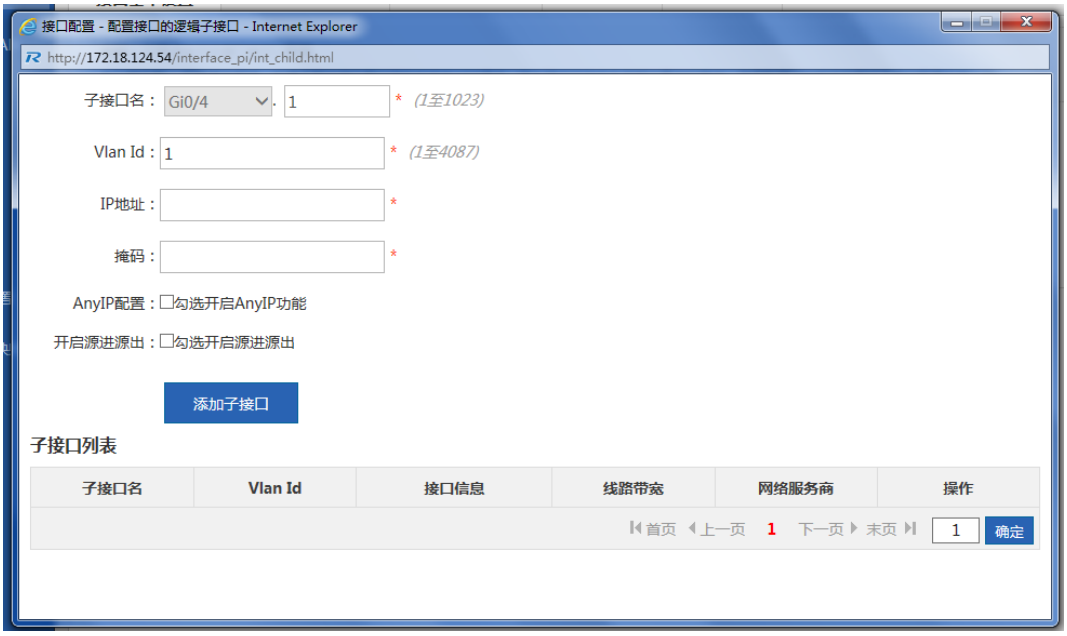
可以查看和管理选中接口下的次 IP 地址：



子接口：子接口是在一个物理接口上衍生出来的多个逻辑接口，即将多个逻辑接口与一个物理接口建立关联关系，同属于一个物理接口的若干个逻辑接口在工作时共用物理接口的物理配置参数，但又有各自的链路层与网络层配置参数。点击

子接口管理

可以查看和管理由选中接口衍生出的子接口：



- **外网口配置**

首先将您申请的外网线路与设备的外网口连接好，然后选择需要配置的外网口，将出现配置页面如下：

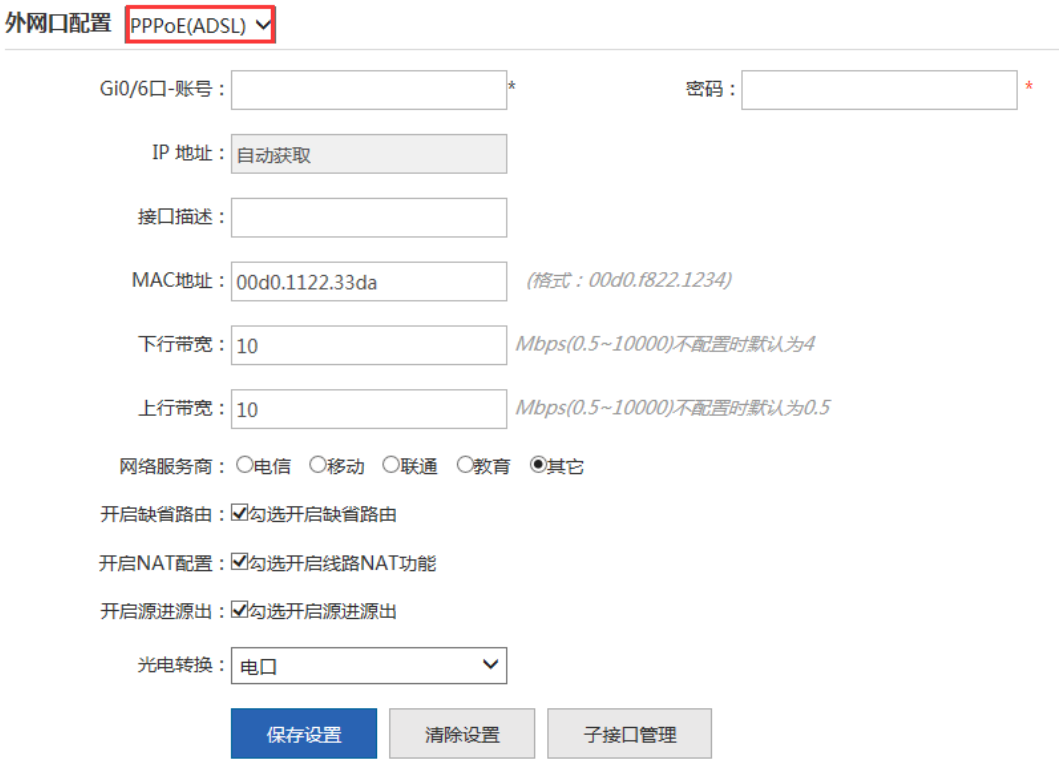
1. **线路类型**：外网口配置包括三种类型：静态 IP 地址，动态 IP 地址，PPPoE（ADSL）。

- 静态 IP 地址：

如上图所示，即为静态 IP 地址配置页面。当线路类型选择“静态 IP 地址”时需要配置运营商分配给您的 IP 地址以及子网掩码和下一跳地址（这里可以理解为网关）。

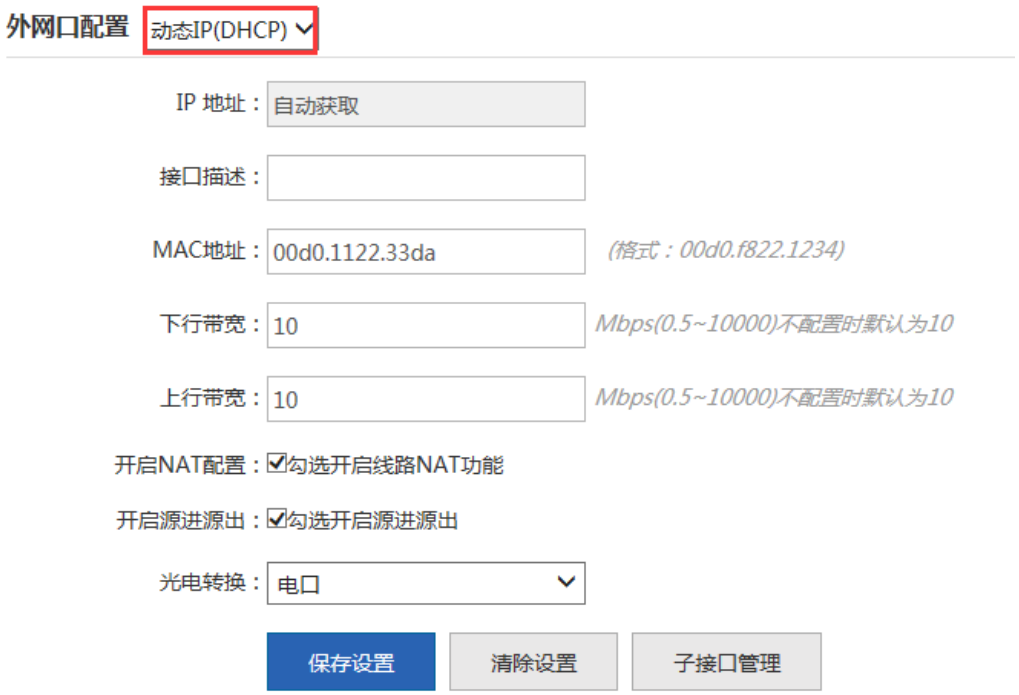
- PPPoE（ADSL）：

如果您向运营商申请的是 ADSL 线路则请选择 “PPPoE(ADSL)” ，需要输入您从网络运营商处申请到的拨号账号及密码，配置如下图：



- 动态 IP 地址：

如果您的上网方式选择“动态 IP 地址”，系统将动态获取 IP 地址。



2. **其它外网口配置信息**：

1) 接口描述：选择“静态 IP 地址”时的配置项，非必填项，用于描述接口的信息。

2) 光电转换：该接口可以作为光口也可以作为电口，一般只有部分外网口有这功能。

3) 上行带宽、下行带宽 :接口允许的最大带宽值，需要根据您向运营商申请的带宽实际数据填写，范围为 0.5~1000Mbps，默认 10Mbps。

4) 网络服务商：包括电信，移动，联通，教育，其他网络。

1.3.11.1.2一线多拨

1.3.11.1.3多链路聚合

点击 添加 在弹出窗中选择聚合口，聚合接口，输入 IP 地址和掩码，点击 确定 完成配置。

1.3.11.1.4接口转换

每个接口都支持内外网口模式的切换，本页面提供内网口与外网口的转换功能。配置页面如下图所示：

你可以选择点击下拉框 将内网口转换为外网口、或将外网口转换为内网口，点击 接口转换保存 按钮重启设备，接口模式方可生效。

一线多拨

1.3.11.1.5链路检测

链路检测：用于检测设备外网口接口是否正常工作，配置页面如下：

配置步骤：

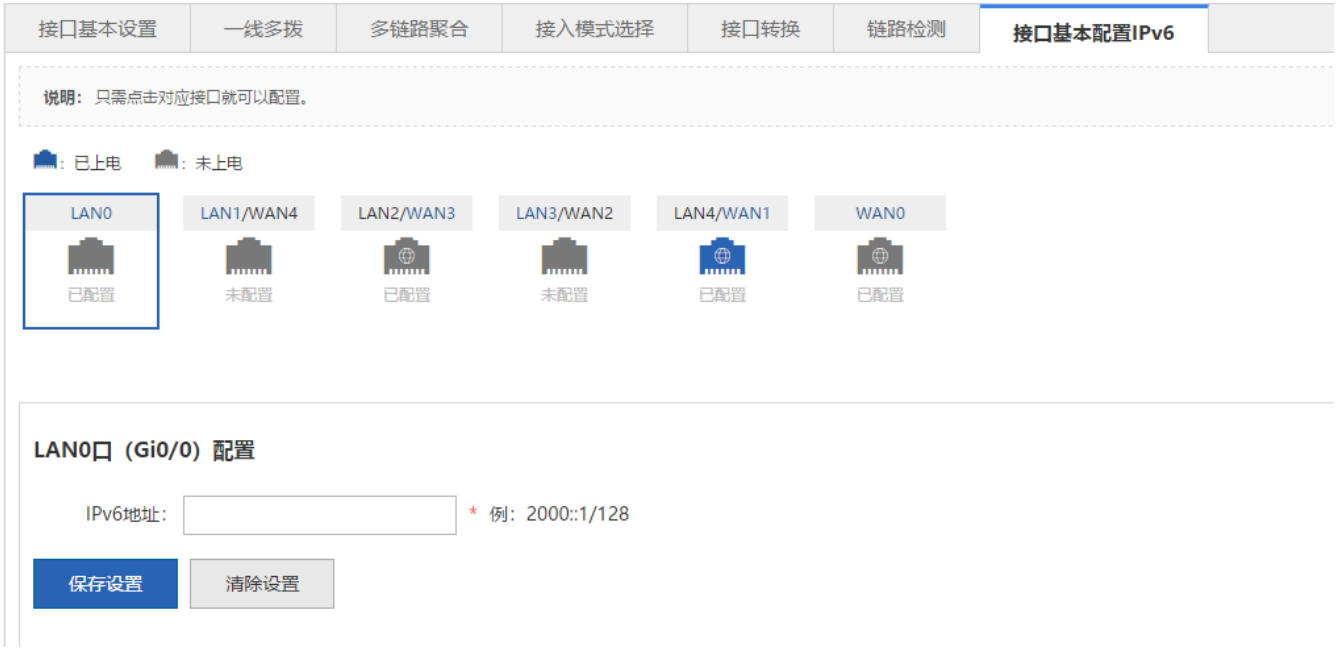
1. 勾选需要进行检测的接口，如勾选 开启Gi0/2口的多链路检测 ，将显示 Gi0/2 口的链路检测配置项：

2. 若要检测接口是否可连接，请输入可 ping 通地址，如百度 220.181.112.143。
3. 输入下一跳地址，若为内网设备则输入网关地址，若不配置，默认下一跳地址为 ping 地址。
4. 输入探测间隔时间，默认为 1s。
5. 点击 确定 ，如果符合上述配置可 ping 通，则显示提示信息为"网络良好"，否则为"网络不通"。

1.3.11.1.6接口基本设置 IPv6

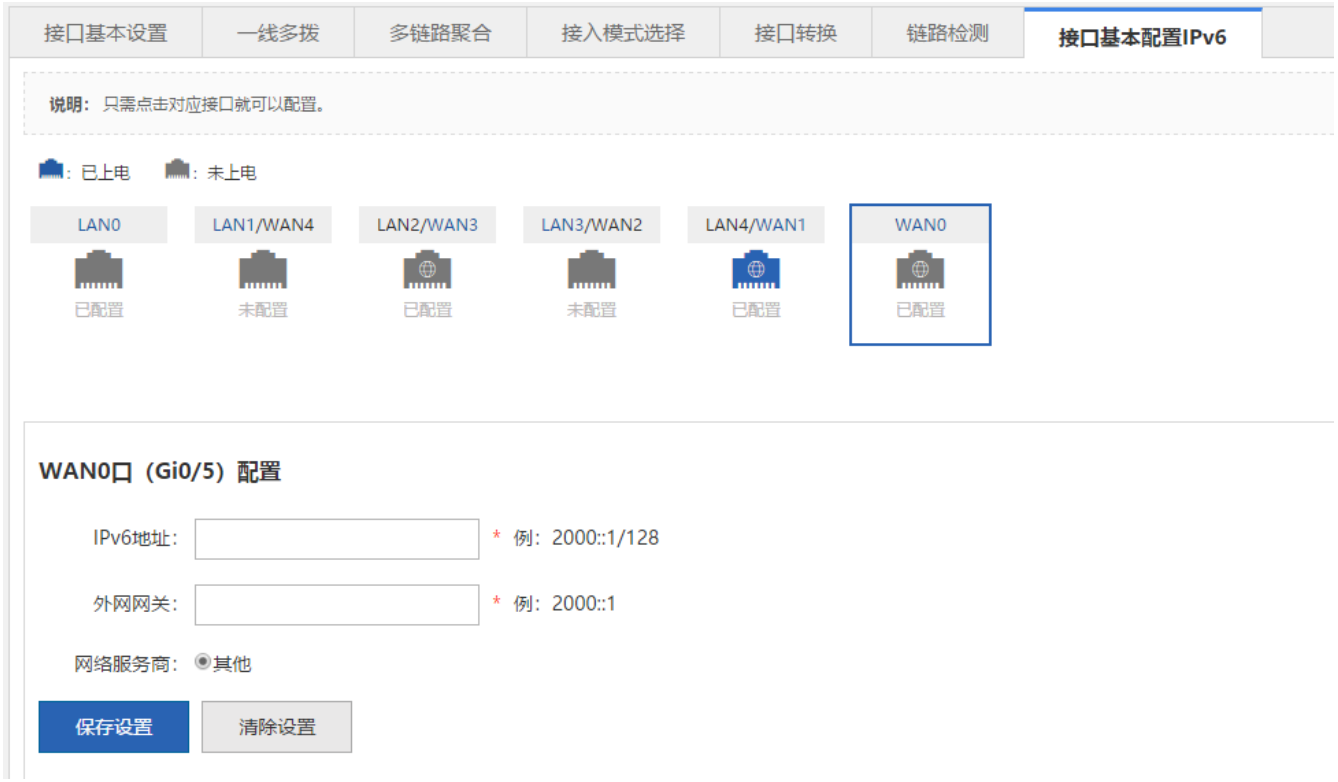
- **内网口配置**

点击需要配置的内网口即可对选中的内网口进行配置，如点击  ：



- **外网口配置**

点击需要配置的内网口即可对选中的内网口进行配置，如点击  ：



1.3.11.2 启用防封杀

1.3.11.3 SUPER-VLAN

SUPER-VLAN 就是实现单臂路由功能，通过 SUPER-VLAN 可以在不配置子接口的情况下，可以使每个 vlan 的流量都由指定的某一个内网口进出。

1.3.11.3.1SUPER-VLAN 配置

通过该页面可以开启和配置 SUPER-VLAN 功能，主要的界面如下：

开启 SUPER-VLAN：勾选后将开启 SUPER-VLAN 功能，要关闭的话请勾掉该选项。

VLAN 最大上线数：允许 VLAN 的最大上线数，取值范围为 1 到 1000。

内网口配置 VID：勾选要配置的内网口，下面会显示相应的配置选项。每个 VID 的取值范围为 1 到 4085。两个接口的 VID 不能重叠，如一个端口配置的 VID 为 1~1000，那么另一个端口就不能配 500~600 之类的，只能配 1~1000 范围之外的值。

配置完后点 保存设置 保存设置。

1.3.11.3.2在线 SUPER-VLAN 信息

查看当前的在线的 SUPER-VLAN 信息。界面如下图所示：

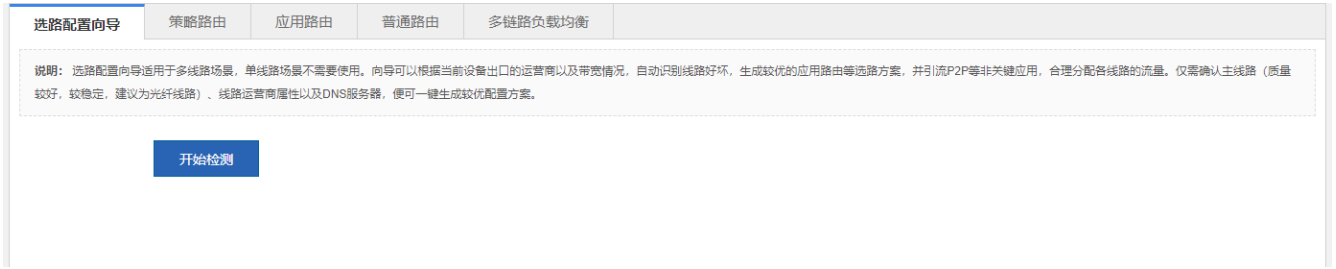
1.3.11.4 路由/负载

路由：策略路由、应用路由和普通 IP 路由都可以作为报文转发的依据。当策略同时存在的情况下，优先级是：策略路由 > 应用路由 > 静态路由（地址库） > 默认路由。

负载：网络出口通常会连接 2 条或 2 条以上的运营商链路，如在教育用户，会有教育网线路和电信/ 网通线路；在政府外网出口有电信、网通线路等。多条运营商链路按照一定策略分担流量或者作为备份，即所谓的多链路负载均衡。

1.3.11.4.1选路配置向导

网吧场景下，增加选路配置向导菜单，如下图



1.3.11.4.2策略路由

策略路由是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。应用了策略路由，设备将通过路由图决定如何对需要路由的数据包进行处理，路由图决定了一个数据包的下一跳转发设备。

应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。

策略路由配置页面如下图所示：

1. **策略路由设置：**选择需要策略的接口、输入策略优先级、选择匹配 ACL 列表（用于指定应用在哪个策略）、输入下一跳地址，点击 添加设置 即可。

ACL 列表：点击【新建ACL列表】可以新增 ACL 列表，具体操作参考“ACL 访问列表”章节。

下一跳地址：当“出口”下拉框中选中一个接口时，默认将此接口的网关地址作为路由的下一跳地址，若该接口未配置网关，可以在后面的“下一跳地址”输入框中输入一个 IP 地址作为它的网关地址；若“出口”下拉框中没有选中一个接口，则必须在“下一跳地址”输入框中输入一个 IP 地址。

2. **策略路由列表：**

编辑策略：在策略路由列表中点击 编辑 即可对对应项策略进行修改。

删除策略：在策略路由列表中点击 删除 即可删除对应项；点击配置页面右上角的 ✕删除全部 按钮可以删除对应策略组下的所有的路由策略。

1.3.11.4.3应用路由

1. **应用路由**：基于应用的路由，区别于传统的基于报文目的 IP 选路的 IP 路由技术，是一种根据数据流的应用类型进行路由转发的技术。基于这种技术，可以将不同应用类型的数据流分流到不同的出口，以达到关键业务与抑制业务各行其道，减少影响的目的。

注意：应用路由分流到指定接口后，各应用的流量依然由该指定接口的流控策略来管理。

应用路由配置页面如下图所示：

添加“优先级”列

新建应用路由：点击 ✚新建应用路由 弹出以下导航窗口：

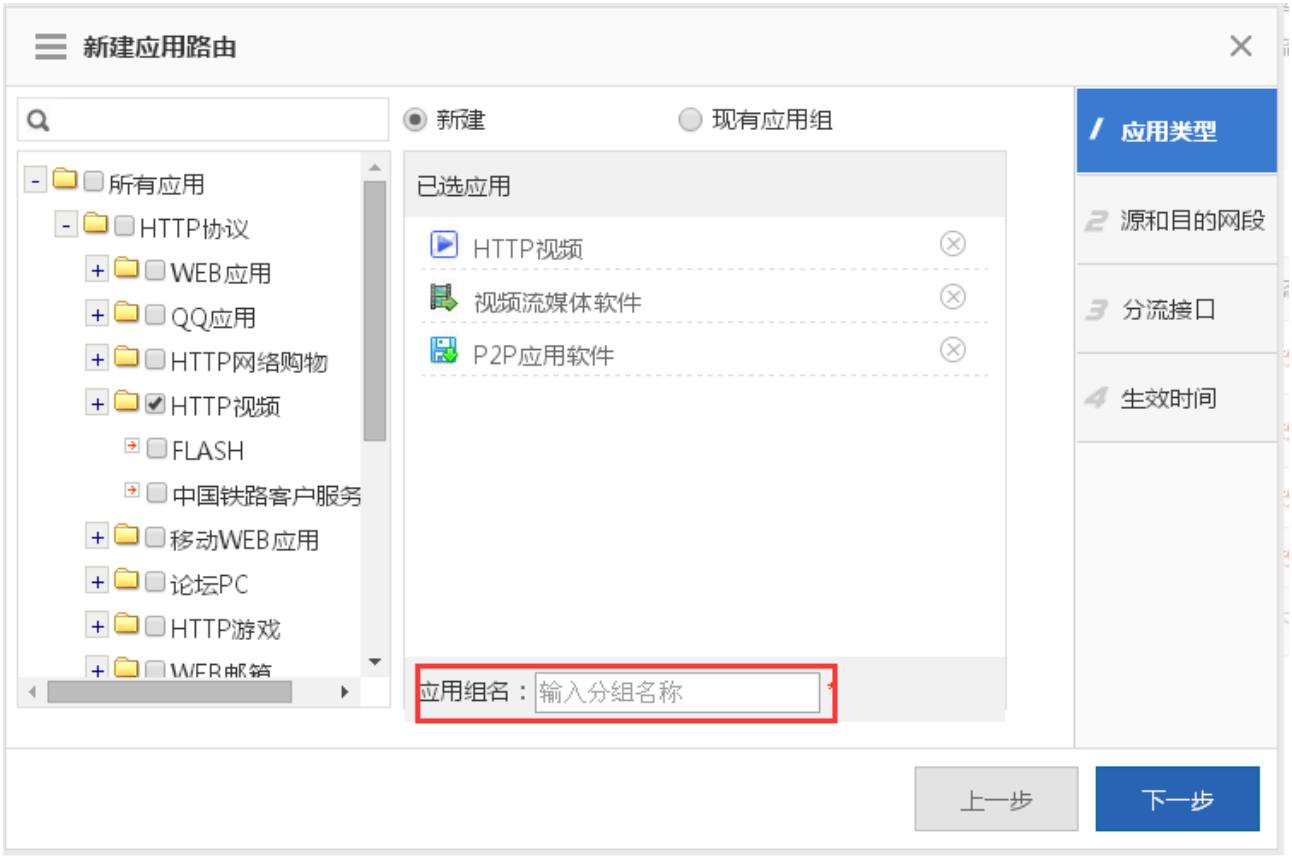
1) **应用类型**：应用路由根据配置的应用类型进行匹配和分流。这里可以选择需要应用路由的应用，有三种方式：

选择单个应用或应用分类作为策略关联的应用对象，此时策略将对选中的应用或应用分类下的所有应用进行匹配和分流：

左侧树状图列出了系统当前可应用路由的应用组织结构，可以直接在这里选择一个应用或应用分类作为策略关联的应用对象。

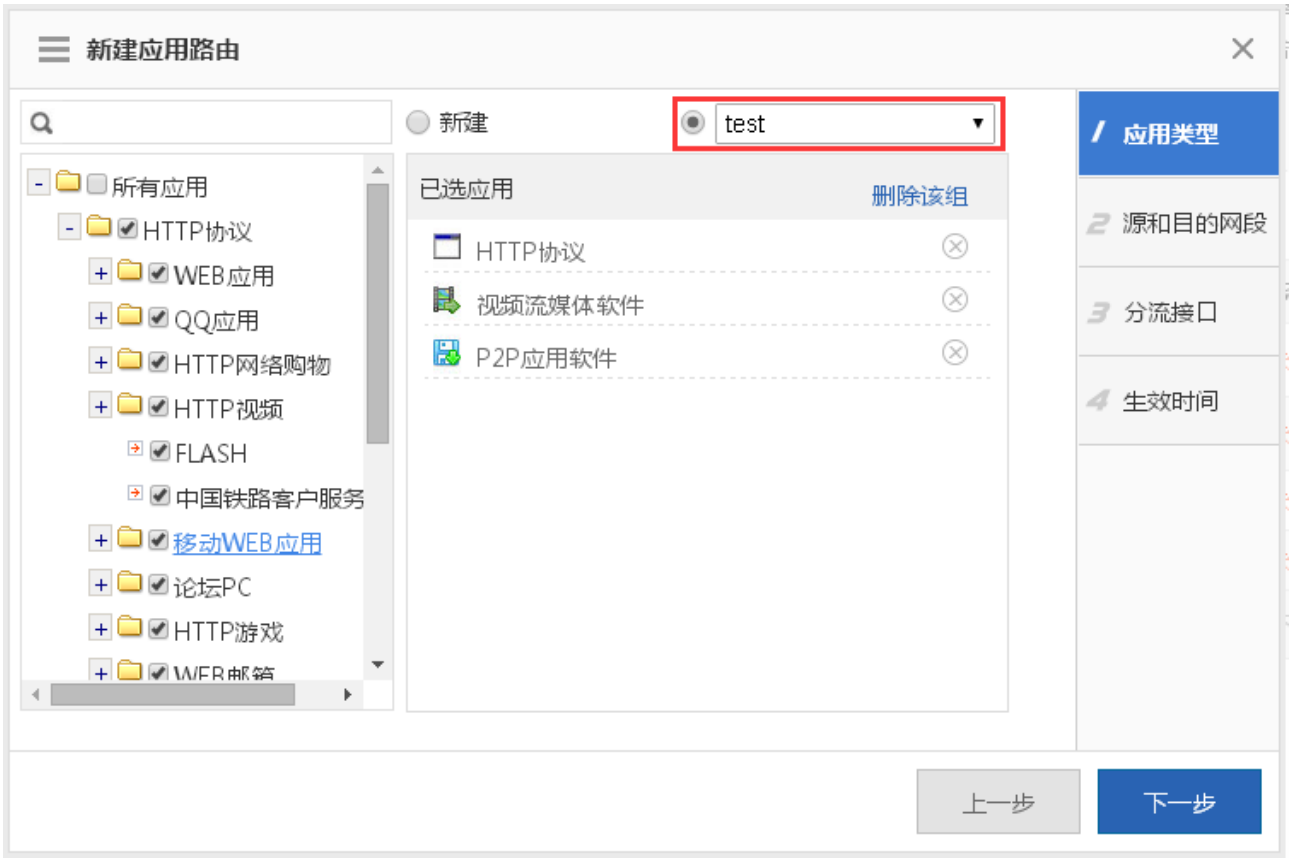
新建一个应用组作为策略关联的应用对象，此时策略将对该应用组包含的所有应用进行匹配和分流：

选中右侧的 新建 ，在左侧应用树上选中多个应用或应用分类，此时右侧下方将出现“应用组名”输入框，在输入框中输入应用组名，即可新建一个应用组，如下图所示：



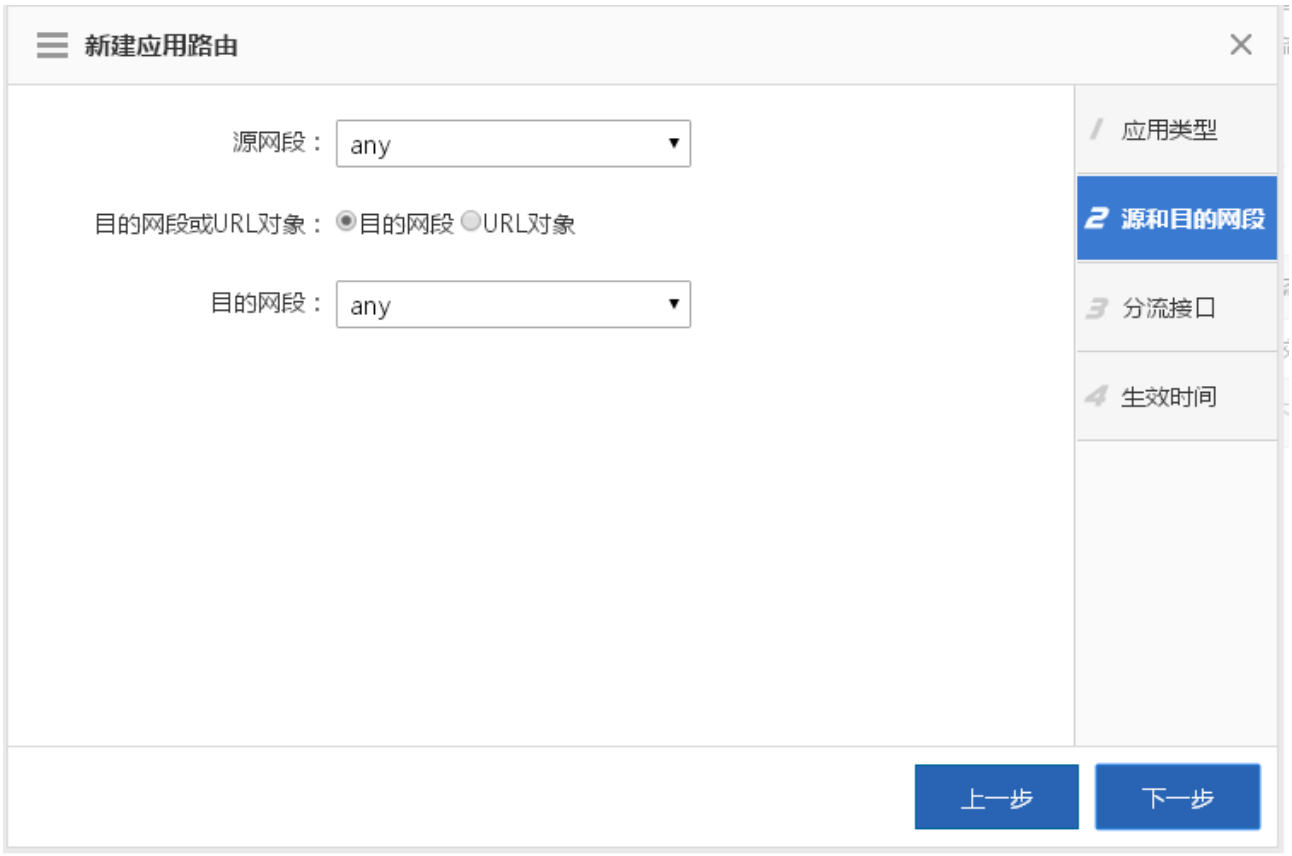
选择一个已存在的应用组作为策略关联的应用对象，此时策略将对该应用组包含的所有应用进行匹配和分流：

右侧选中 现有应用組 ，页面如下图所示：

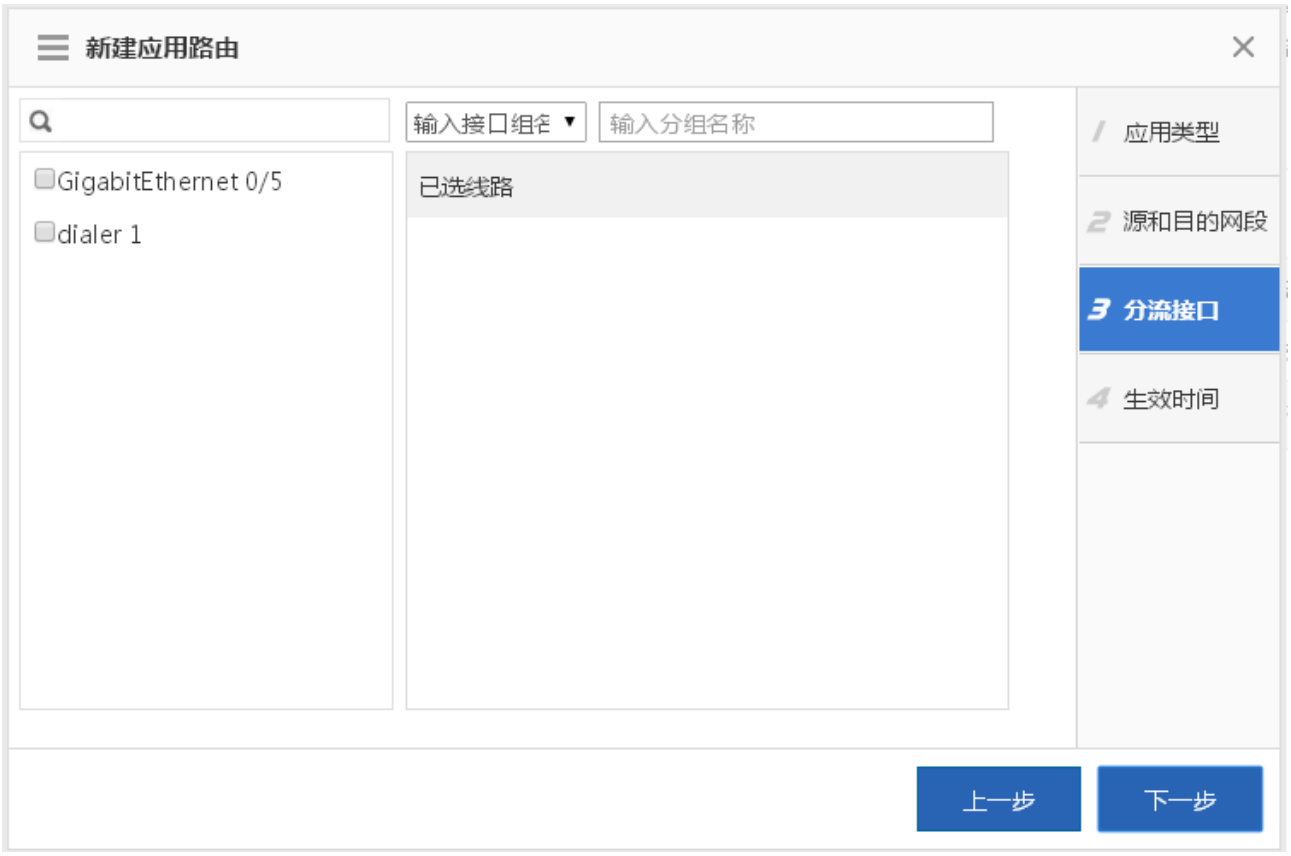


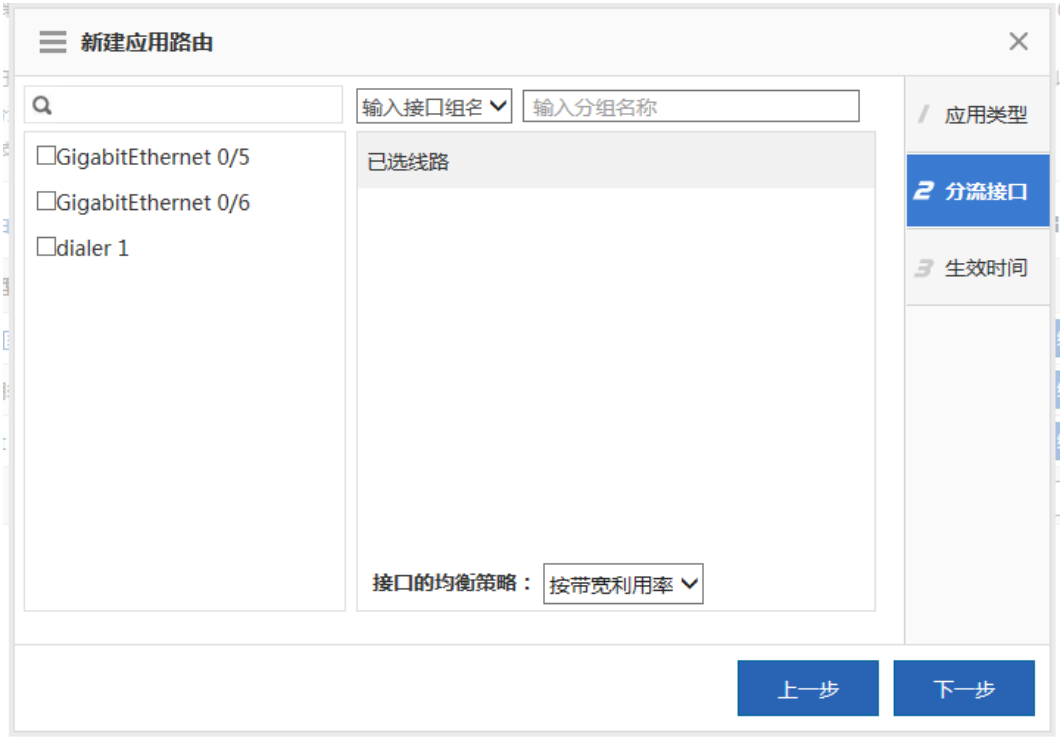
在右侧下拉框中选择一个已存在的应用组，将会在“已选应用”区域显示该应用组包含的应用成员，通过左侧树状图可以选择更多的应用添加到该应用组中，也可以点击 ⊗ 将不合适的应用从该应用组中删除：

2) **源和目的网段：**应用路由支持指定源 ip 与目的 ip 网段，以及目的 url 组来进行引流。ip 网段可以是单个 ip 地址，ip 地址范围，甚至地址库。指定源 ip 网段，如指定内网的服务器 ip 地址，可以实现类型策略路由的效果。指定目的 ip 网段，如指定目的网段是电信地址库，可以实现类似地址库的效果。指定目的 url 组，允许将指定的域名引流至指定的接口，包括 dns 的解析以及数据报文的引流。

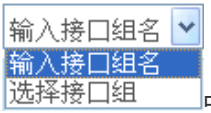


3) **分流接口：**应用路由支持 WAN 口作为出接口。接口组，是指一个 WAN 接口的组合。为了支持应用路由走多链路出口，并简化配置，抽象出一个接口组的概念。可以为接口组指定名称，包含的 WAN 接口，均衡策略。应用路由的出口可以指定为接口或接口组。


新建应用路由
输入接口组名
输入分组名称
GigabitEthernet 0/5
dialer 1
已选线路
1 应用类型
2 源和目的网段
3 分流接口
4 生效时间
上一步
下一步

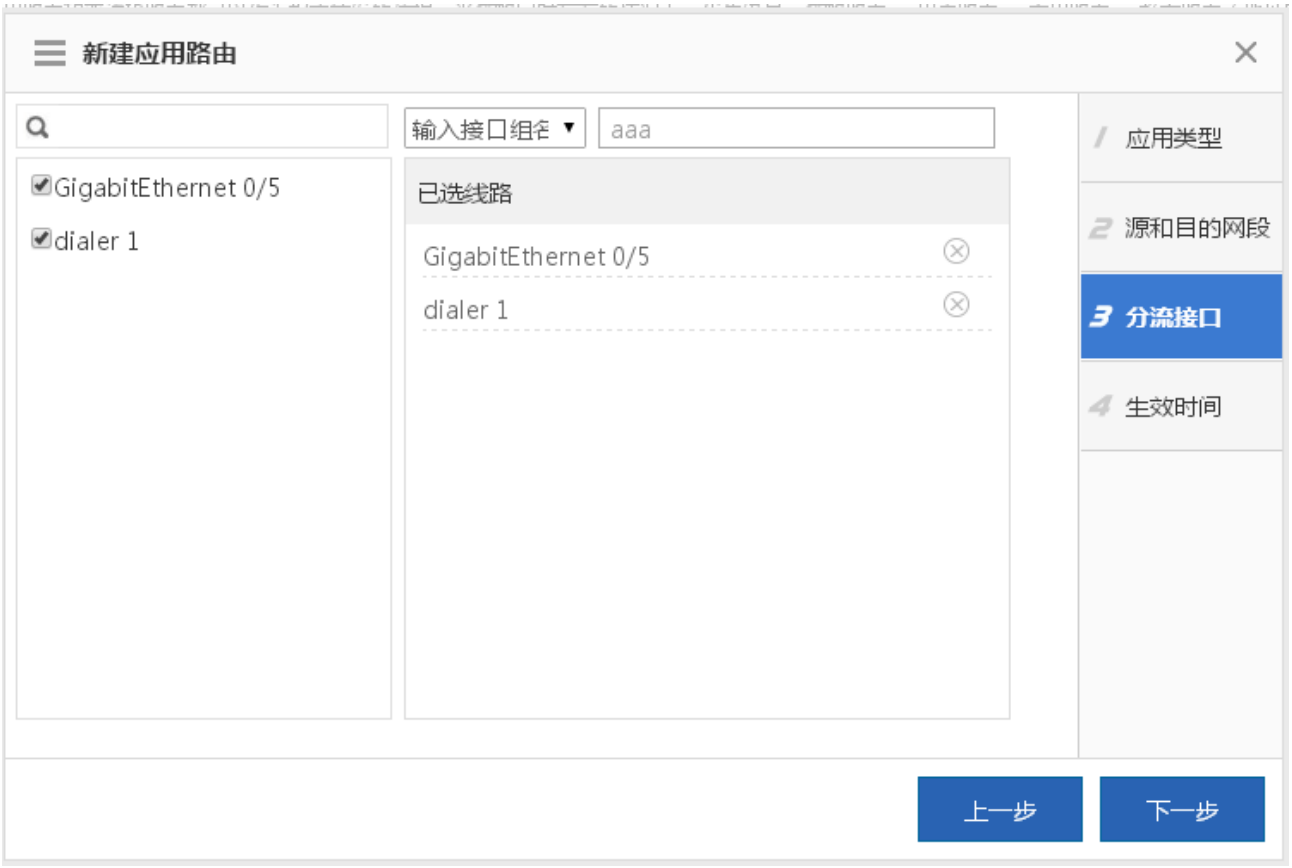

新建应用路由
输入接口组名
输入分组名称
GigabitEthernet 0/5
GigabitEthernet 0/6
dialer 1
已选线路
接口的均衡策略：
按带宽利用率
1 应用类型
2 分流接口
3 生效时间
上一步
下一步

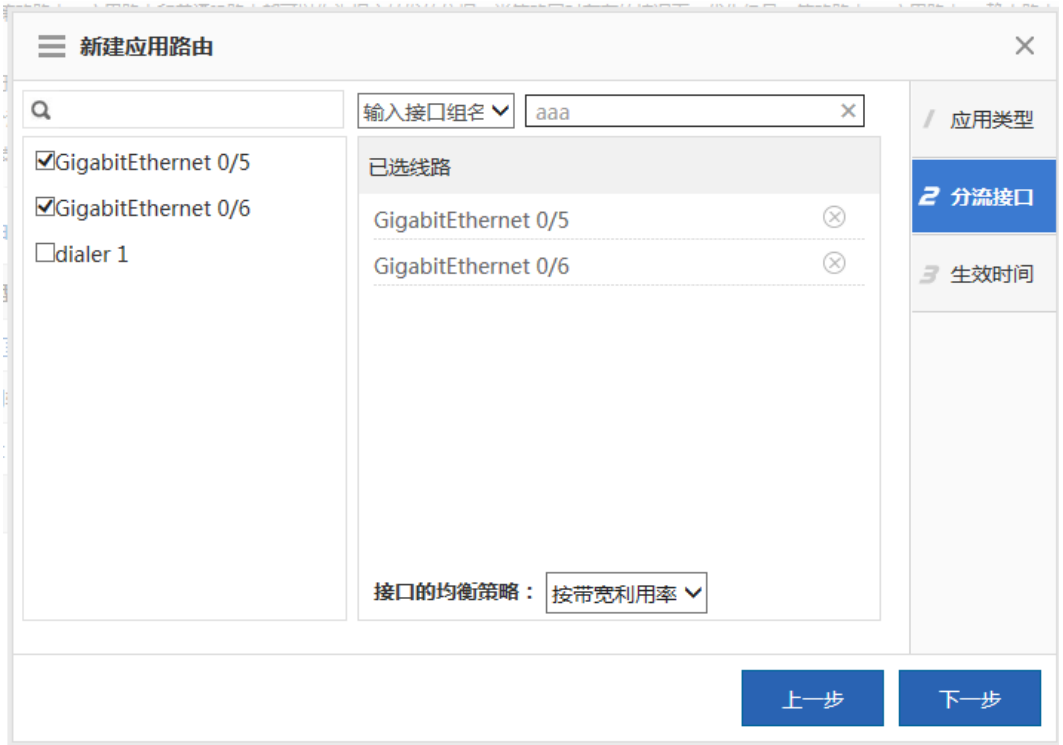
指定接口为应用路由出口：上图左侧列出了系统当前的线路，可以直接在这里选择一个 WAN 口作为应用路由的出口，点击 下一步 继续配置策略。

指定接口组为应用路由出口：可以在上图右侧的下拉框 

中选择“输入接口组名”或“选择接口组”。

选择“输入接口组名”则需要在后面的输入框中输入接口组名新建一个接口组，并从左边列出的线路中选择需要的线路加入该接口组，如下图所示，选中的线路将显示在右边的“已选线路”区，点击 ⊗ 可以将不需要的线路从该接口组中删除：


新建应用路由
输入接口组名
aaa
GigabitEthernet 0/5
dialer 1
已选线路
GigabitEthernet 0/5
dialer 1
1 应用类型
2 源和目的网段
3 分流接口
4 生效时间
上一步
下一步


新建应用路由
输入接口组名
aaa
GigabitEthernet 0/5
GigabitEthernet 0/6
dialer 1
已选线路
GigabitEthernet 0/5
GigabitEthernet 0/6
接口的均衡策略：
按带宽利用率
1 应用类型
2 分流接口
3 生效时间
上一步
下一步

选择“选择接口组”则后面的输入框为变为下拉选择框： 

，这里可以选择一个已存在的接口组，对该接口组进行编辑，接口添加、删除操作同上。

请注意：

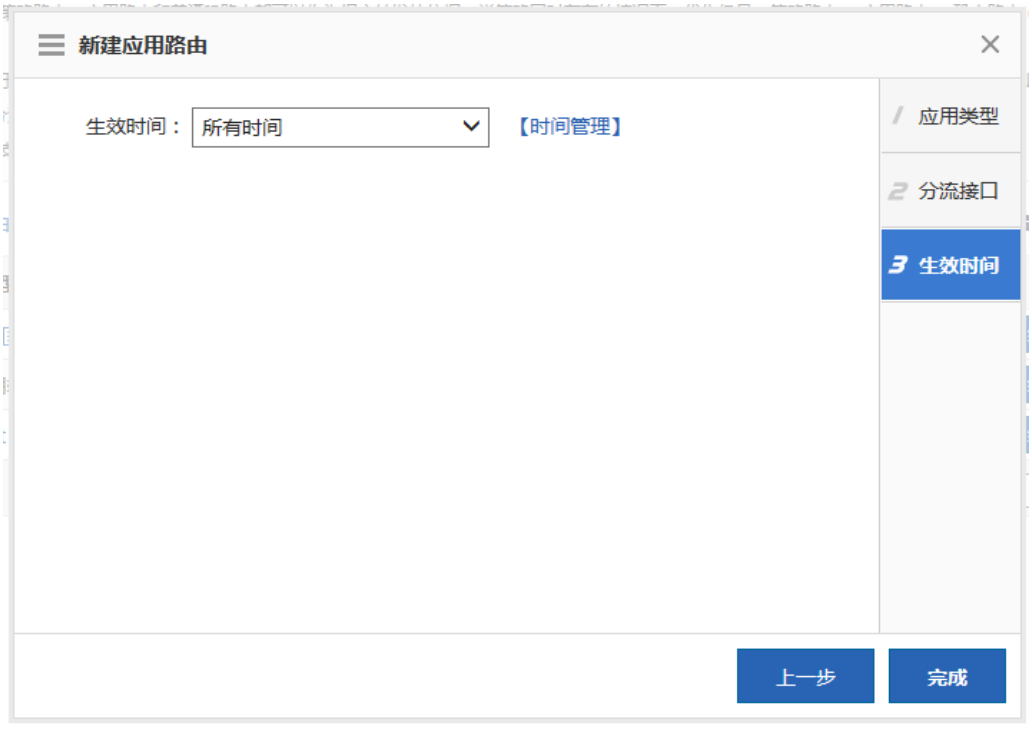
1) 不能让所有接口都做应用路由；请保留最少一条优质线路，不做应用路由（走默认路由）。
2) 动态获取 ip 的接口，不支持应用路由；
3) 请提前确认选择的接口，在接口配置 or 快速配置中，是配置好的（比如：接口类型，ip 地址，下一跳地址等）。

配置好接口组后，在 

这里选择接口均衡策略，选择“按带宽利用率”（推荐），则将根据出口链路的负载状况调整走向，使各出口的负载维持均衡；选择“按带宽值大小”，出口流量按照出口带宽比负载均衡。

3) **生效时间：**选择策略生效时间。在生效时间下拉框中列出了系统当前已配置的时间对象，您可以从中选择一个合适的时间对象，若没有满足您要求的时间段，您可以点击后面的【时间管理】新建时间对象。


新建应用路由
生效时间：
所有时间
【时间管理】
1 应用类型
2 源和目的网段
3 分流接口
4 生效时间
上一步
完成


新建应用路由
生效时间：
所有时间
【时间管理】
1 应用类型
2 分流接口
3 生效时间
上一步
完成

2. 应用路由列表：

根据以上导航窗口的步骤完成配置后，可以在下面的列表中查看已配置的应用路由策略：

应用类型名	源网段	目的网段	目的URL	分流接口名/接口组	生效时间	开启	状态	匹配顺序	管理
ffff	联通	-	P2P~sys(dns:1 2.3.3.3)	di1	下班时间	开启	未生效		编辑 删除
HTTP协议	教育	-	QQ特权~sys(dns:1 2.3.3.3)	Gi0/5	晚上	开启	未生效		编辑 删除
-	-	-	-	aaa(di1,Gi0/5)		开启	生效		编辑 删除

显示: 10 首页 上一页 1 下一页 末页 1 确定

点击 可以查看应用组或接口组包含的应用或接口成员。

点击 开启 可以开启或关闭某条应用路由。

状态：当前策略是否生效，对于未生效的策略，可以点击后面的 查看未生效原因。

匹配顺序：在配置了多条应用路由的情况下，各应用路由自身之间存在优先级关系，后配置的优先级高于先配置的。点击 可以调整策略优先级。

点击 明细 可以查看选中策略的命中情况。

点击 编辑 可以对策略进行编辑，点击 删除 可以删除一条策略。

3. 查看路由效果：

点击 查看路由效果 查看路由效果：

应用类型名	源网段	目的网段	目的URL	分流接口名/接口组	命中连接数
-	-	-	-	GigabitEthernet 0/5	0

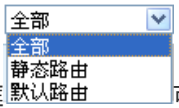
显示: 10 首页 上一页 1 下一页 末页 1 确定

1.3.11.4.4普通路由

普通 IP 路由：使得到指定目标网络的数据包的传送，按照预定的路径进行。当我司产品不能学到一些目标网络的路由时，配置静态路由就会显得十分重要。给所有没有确切路由的数据包配置一个默认路由，是通常的做法。

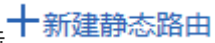
普通 IP 路由包括：静态路由、地址库和默认路由，其中默认路由的优先级是最低的。

普通路由配置页面如下图所示：

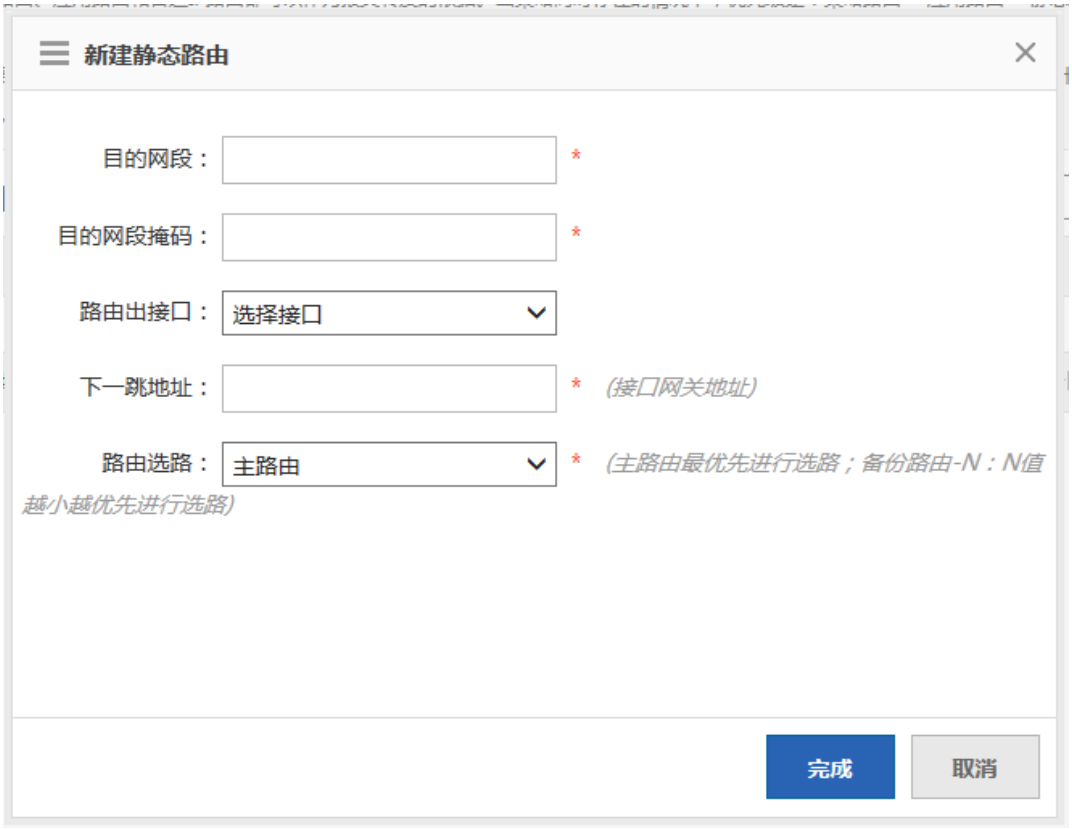
上图的表格列出了系统已配置的静态路由和默认路由，通过筛选条件输入框 

可以选择只显示静态路由或默认路由。

请注意：“路由选路”为“10”时，是配置应用路由策略时自动生成的默认路由策略。

1. **静态路由**：点击 

弹出以下窗口：



目的网段：路由要到达的网段。

目的网段掩码：目的网段的掩码。

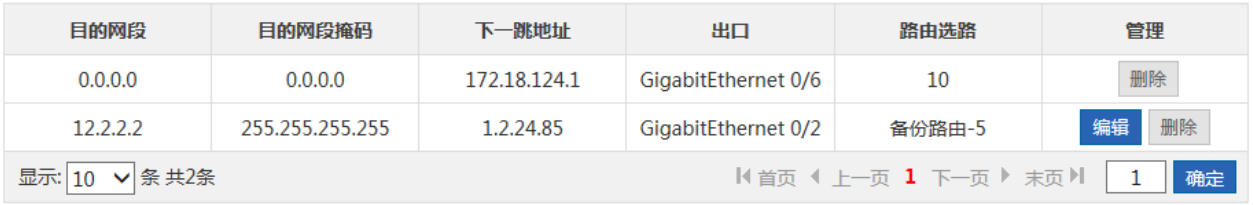
路由出接口：路由的出口。

下一跳地址：下一个路由（网关）的入口地址。

路由选路：指定路由选路的优先级。主路由最优先进行选路；备份路由-N：N 值越小越优先进行选路。

点击 

即可配置一条静态路由：



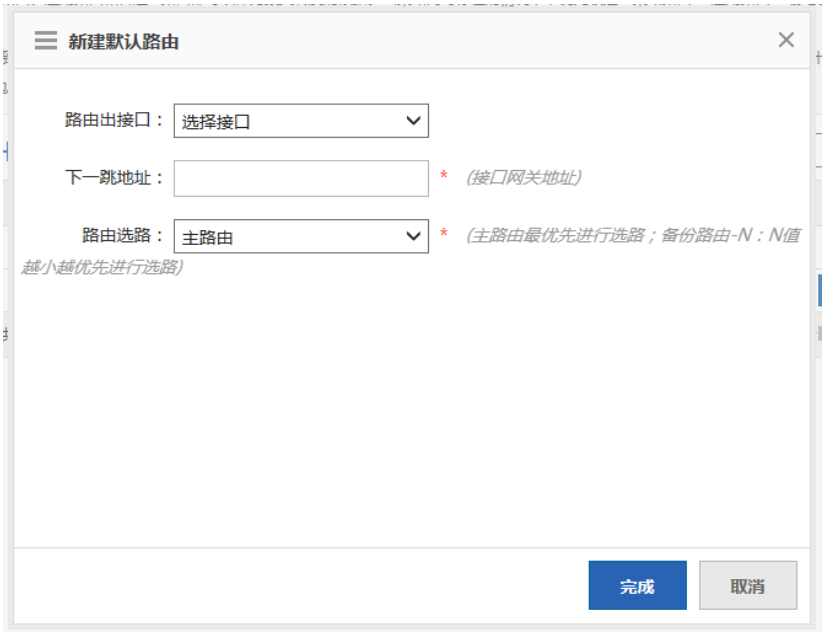
点击 删除 可以删除一条静态路由。

2. **地址库**：点击 +新建地址库 弹出以下窗口：

选择线路接口和网络服务商，点击 添加设置 即可完成某个接口的地址库配置；

点击表格中的 删除 即可删除某个接口的地址库配置。

3. **默认路由**：点击 +新建默认路由 弹出以下窗口：



选择路由出接口，输入下一跳地址，选择路由选路，点击 完成 即可配置一条默认路由：

目的网段	目的网段掩码	下一跳地址	出口	路由选路	管理
0.0.0.0	0.0.0.0	5.32.2.5	GigabitEthernet 0/3	备份路由-3	编辑 删除
0.0.0.0	0.0.0.0	172.18.124.1	GigabitEthernet 0/6	10	删除
12.2.2.2	255.255.255.255	1.2.24.85	GigabitEthernet 0/2	备份路由-5	编辑 删除

显示: 10 条 共3条 首页 上一页 1 下一页 末页 1 确定

点击 删除 可以删除一条默认路由。

1.3.11.4.5多链路负载均衡

多链路负载均衡是在多条链路上根据一定策略进行合理的流量分配，提高链路资源的利用效率。

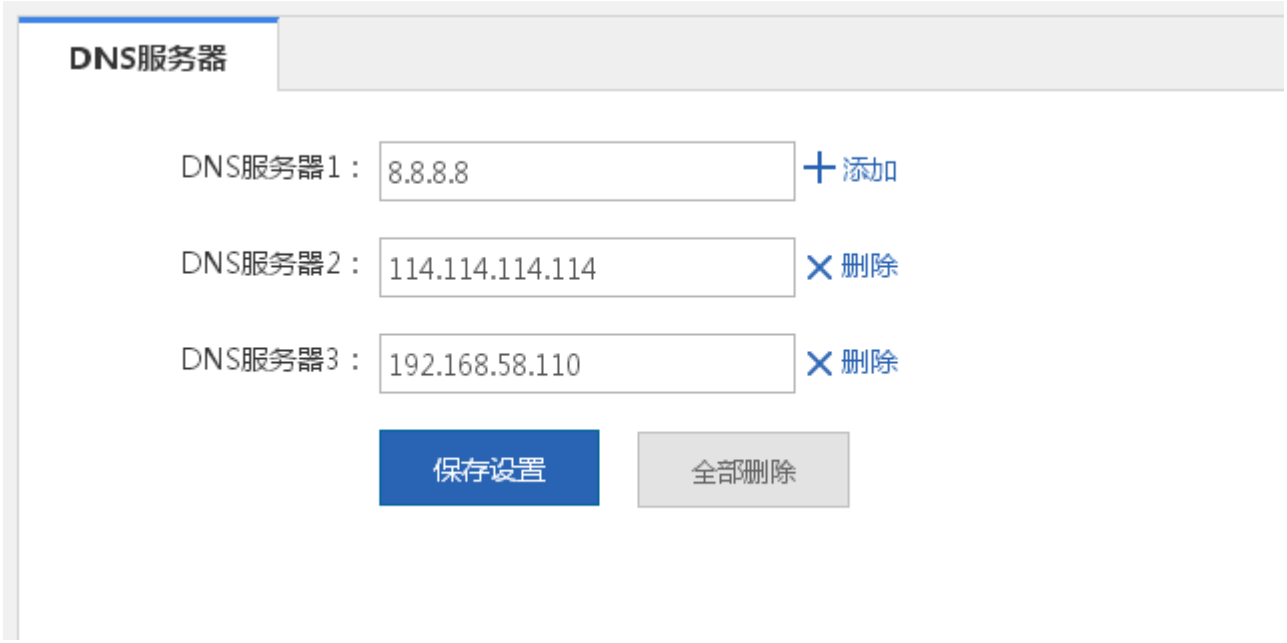
点击 【查看负载均衡结果】 可以查看负载均衡的效果：

1.3.11.5 DNS 配置

域名服务器等相关配置，包括 DNS 服务器的配置、正向 DNS 代理配置、智能 DNS 配置。

1.3.11.5.1DNS 服务器

配置设备的域名服务器地址，与 PC 的首选 DNS 服务器地址类似。最多可以配置两个 DNS 服务器的地址(点击 添加 可配置第二个 DNS 服务器的地址)，配置好之后点击 保存设置 即可。



在没有配置 DNS 服务器地址时，用设备 ping www.baidu.com 是 ping 不通的，因为设备无法解析 www.baidu.com 这个域名。只有配置了可用的 DNS 服务器地址，ping www.baidu.com 才能 ping 通。(这里 ping www.baidu.com 只是举例说明。)

1.3.11.5.2正向 DNS 代理

1.3.11.6 VPN 配置

VPN 的英文全称是“Virtual Private Network”即“虚拟专用网络”。它并不是真实存在的物理链路，而是通过技术手段模拟出来的虚拟线路。互联网上的两个节点通过 VPN，可以建立一条虚拟的专用数据传输通道，在这个专用通道中相互传递资料不会被外界干扰或窃听。

1.3.11.6.1配置向导

首次配置 VPN，配置页面如下图所示：

可以根据实际情况(公司总部 or 分支机构)选择“总部”或者“分支机构”进行配置。下面将分别介绍总部和分支机构的配置。

- **总部配置**

点击右侧的“开始配置”按钮开始总部 VPN 配置，并进入如下页面：

根据公司的需求，推荐 VPN 类型，如下图


VPN配置向导
VPN类型选择 → 完成
请选择您的需求【多选】，为您推荐最合适的VPN类型：
隧道需加密
支持IOS终端
支持安卓终端
支持WIN使用
推荐VPN类型：L2TP IPSec
使用VPN类型：
IPSec
对传输数据进行加密防止数据被窃取、篡改和破坏。适合端到端接入，设备与设备之间使用。
L2TP
支持入网身份认证没有对传输数据进行加密。可以终端拨入，也可以设备与设备之间使用，终端适用PC与安卓手机
L2TP IPSec
不仅支持入网身份认证还能对传输数据进行加密防止数据被窃取、篡改和破坏。可以终端拨入，也可以设备与设备之间使用，终端适用PC、安卓与苹果手机。
PPTP
支持入网身份认证没有对传输数据进行加密。只能终端拨入，只能PC和安卓手机接入。
上一步
下一步

请根据具体需要勾选需要支持的协议类型，此时向导将根据您选择的协议类型，增加相应的配置步骤，如选择 PPTP 或 L2TP，将多出“配置基本信息”和“管理用户帐户”两个步骤。然后点击“下一步”按钮进入下一个配置页面。

下图所示为“配置基本信息”页面，这个页面可以配置 PPTP 和 L2TP VPN 总部相关参数：

客户端地址范围：给 vpn 客户端分配的隧道 ip，有多少个 ip 就只能有多少个 VPN 客户端连进来；
DNS 服务器：如果 vpn 客户端需要通过域名来访问本局域网中的系统，则需要配置 DNS 服务器地址，这个地址一般和本局域网中使用的 DNS 服务器地址是一致的；

点击“高级设置”旁边的 » 按钮，将有更多的配置信息：

本机隧道 IP：远程客户端通过 PPTP 或 L2TP 协议与本机建立起 VPN 隧道时本机使用的隧道 ip，默认取客户端地址范围中的第一个 ip 地址。

PPTP 隧道状态检测：设置此参数，表示在持续此时间间隔没有收到隧道对端的任何合法报文后，本机将主动探测隧道状态。建议采用默认值 60 秒。

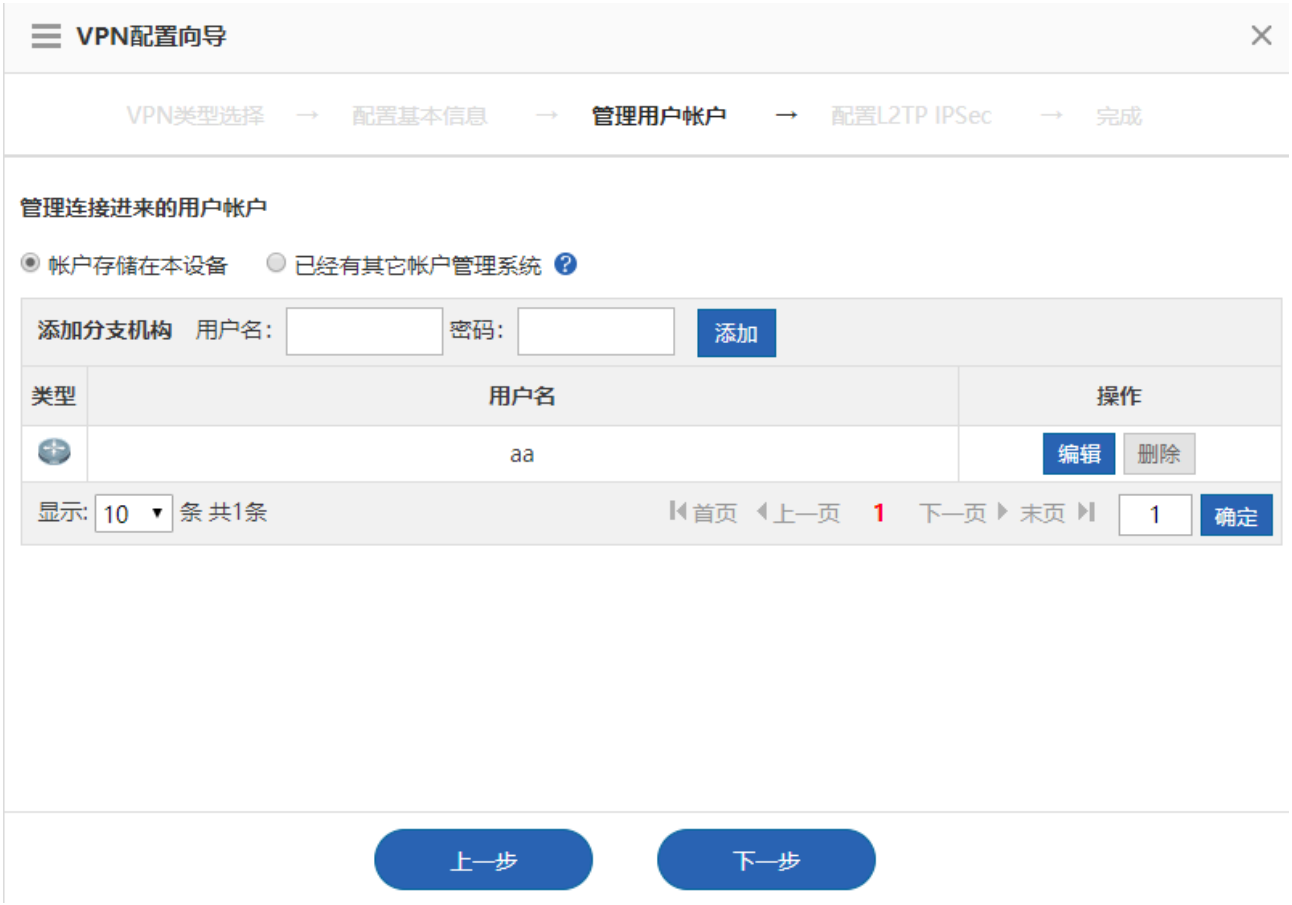
L2TP 隧道超时检测：设置隧道控制消息重传参数，超过指定时间间隔内无会话将自动清除隧道。建议采用默认值 600 秒。

L2TP 隧道验证密码：在默认情况下，L2TP 隧道的建立不要求通道验证，如果要求进行 L2TP 通道验证，L2TP 通道的两端必须配置相同的验证密码。

允许总部访问分支内网：若希望总部能够访问分支机构内网，您必须事先规划好各分支机构拨入总部的隧道 IP 和各个分支机构的内网网段，在这里点击 ☑ 开启 后，填写表格。 如果鼠标经过 按钮时，会显示配置指导：

填写完基本信息后，点击“下一步”按钮，进入下一个配置页面。

下图所示为“管理用户帐户”配置页面，您可以在此页面配置用户信息，对试图远程 PPTP 或 L2TP 接入本地的客户端进行用户身份验证。 您可以选择“帐户存储在本设备”或者“已经有其它账户管理系统”。下图所示为选择“帐户存储在本设备”的配置页面，表格中列出了本设备已配置的用户名和密码信息，您可以通过表格“操作”列中的 编辑 和 删除 按钮对已有的用户名和密码信息进行修改或删除，也可以在 添加分支机构 用户名： 密码： 添加 这里新增用户名和密码。



选择“已经有其它账户管理系统”，将通过第三方服务器来管理用户信息，如下图所示，选择“已经有其它账户管理系统”之后，点击【管理认证服务器】，在弹出窗中共享密码和服务器 IP 即可。

L2TP over IPSec 为 L2TP 和 IPSec 协议的结合，选择 L2TP over IPSec 协议类型的 VPN 总部，除了要在前面所示的“配置基本信息”和“管理用户帐户”页面中配置 L2TP 相关参数，还需要在下图所示的配置页面中配置 IPSec 相关参数：

预共享密钥：移动用户和分支机构必需输入正确的密钥才能成功拨入；

应用到接口： 对于 IPSec 通信将要途经的每个接口，都需要为它配置一个加密映射集合（加密映射集合将转换集和数据流联系起来，并描述了对端的地址以及通讯必要参数，它完整地描述了与远端对等体的 IPSec 通讯所需要的内容。通过加密映射条目，才能建立 IPSec 安全联盟）。这里列出了本设备已配置的外网口，并默认都为选中状态。

IKE 策略：选择 IKE 协议使用的参数加密算法、散列算法、Diffie-Hellman 组标识。参与 IKE 协商的双方至少拥有一套一致的 IKE 策略，这是 IKE 协商成功的必要条件。

转换集：是特定安全协议和算法的组合。在 IPSec 安全联盟协商期间，对等体一致使用一个特定的变换集合来保护特定的数据流。IPSec 隧道生命周期：当隧道建立时间到达生命周期后，双方将自动重新协商建立隧道，这样可以有效的防止隧道被破解，建议采用默认值 1 小时；

下图所示为 IPSec VPN 总部相关参数的配置页面：

基本参数与前面所示的 L2TP over IPSec 配置页面基本一致，只是多了“需经隧道访问的网络”的配置，您可以在这里的表格中配置总部和分支机构间需要通过 IPSec 隧道加密互访的网段。

完成各种协议类型的 VPN 参数后，点击“下一步”就完成配置了，下图所示为“完成”页面。

到了这里，只需要点击左下方的“完成”按钮即可完成总部的 VPN 配置。在点击“完成”按钮之前，记得先点击 配置指南 图标，可查看此处配置的全部内容。如下图所示，

移动用户 PPTP VPN	
服务器公网IP：	172.18.124.72
配置步骤：	+ Windows XP配置参考 + Windows 7配置参考

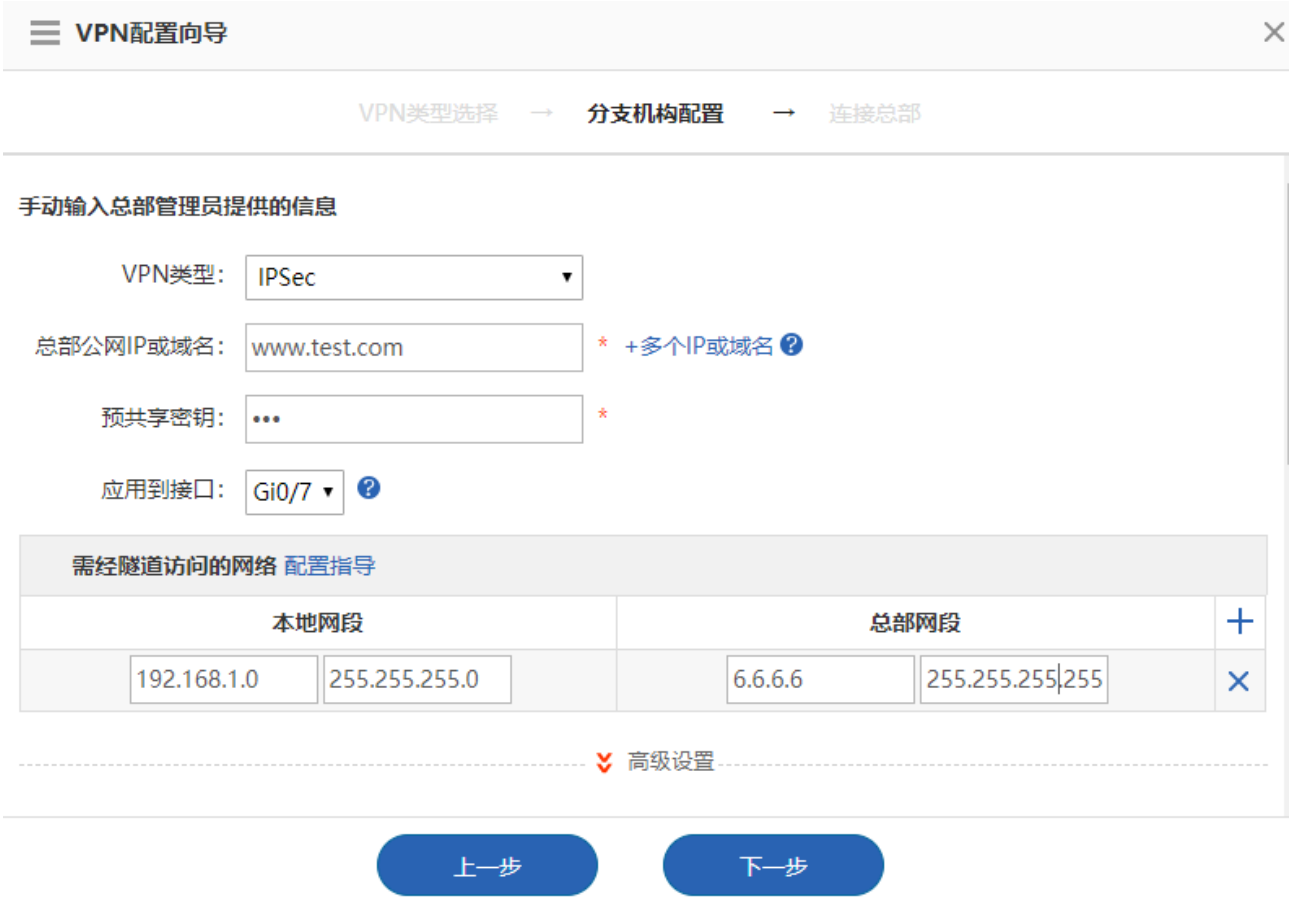
分支机构 L2TP IPSec VPN	
服务器公网IP：	172.18.124.72
预共享密钥：	023
总部网络：	网段：100.100.101.0 掩码：255.255.255.0
转换集1：	esp-des esp-sha-hmac
转换集2：	esp-3des esp-md5-hmac
IKE策略：	序号 加密算法 散列算法 DH组 1 3DES SHA group1 2 DES SHA group1 3 3DES SHA group2 4 DES MD5 group1 5 DES SHA group1
L2TP隧道验证密码：	未开启
允许总部访问分支：	开启
本机隧道IP：	手动配置(192.168.1.2~192.168.1.254)
配置步骤：	+ Windows XP配置参考 + Windows 7配置参考

还可以点击展开“配置参考”，将可以看到有关移动用户 PC 如何连接到本总部 VPN 服务器的参考指南。

- **分支机构配置**

点击左下角的  按钮，进入如下页面，


VPN配置向导
VPN类型选择 → 分支机构配置 → 连接总部
请您登录至总部端设备查看相关信息或总部网络管理员获取相关信息已完成本端配置
分支机构的VPN类型（需跟总部相同）：
IPSec
对传输数据进行加密防止数据被窃取、篡改和破坏。适合端到端接入，设备与设备之间使用。
L2TP
支持入网身份认证没有对传输数据进行加密。可以终端拨入，也可以设备与设备之间使用，终端适用PC与安卓手机
L2TP IPSec
不仅支持入网身份认证还能对传输数据进行加密防止数据被窃取、篡改和破坏。可以终端拨入，也可以设备与设备之间使用，终端适用PC、安卓与苹果手机。
上一步
下一步



VPN 类型：根据实际情况，选择 L2TP IPSec、L2TP 或者 IPSec 隧道协议；

总部公网 IP：总部 VPN 服务器的公网 IP 地址；

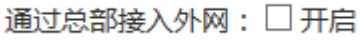
预共享密钥：需要与总部 VPN 服务器保存一致，可向总部 VPN 服务器管理员获取；

用户名、密码：可登陆 VPN 网络的用户名、密码；

总部网络：想访问的总部的内网网段；

本机名称显示：选择 IPSec 或 L2TP IPSec 协议时才需要的配置，开启本机名称显示后，可使总部获知分支机构的名称，便于 VPN 管理。

高级设置：包括 IKE 策略、转换集、允许总部访问分支内网等设置，需要与总部 VPN 设置保持一致。需要特别说明的是：



，这里如果勾选的话，分支机构正常上外网会全部走 VPN 再通过总部连接到外网，如果不勾选的话，只有要访问那些总部内网网段的时候才走 VPN，其余流量则按照分支机构的网络出口直接连接到外网的。

设置好之后，点击“下一步”按钮，即可看到如下页面，


VPN配置向导
VPN类型选择 → 分支机构配置 → 连接总部
分支机构端配置成功
接下来建议您进行（需对端设备在线）：
VPN线路联通性检测
立即检测
上一步
完成

点击立即检测

等待一段时间后就会有连接成功或失败的提示信息。等连接成功之后，点击左下方的“完成”按钮，即可完成分支机构的 VPN 配置。

1.3.11.6.2VPN 配置

- **拓扑图显示页面**

完成 VPN 配置后，可以看到如下配置页面：

您可以在拓扑图区域中查看本机在 VPN 环境中的位置，其中有显示“（本机）”字样的设备便是您当前正在配置的设备，

如上图所示的 图标。点击此图标可以查看、修改本机的 VPN 配置信息。拓扑图中灰色线条、设备表示连接失败，绿色线条、设备、蓝色设备表示连接成功。

本机上方的设备，表示本机作为 VPN 分支机构时，连接的总部。点击 添加接入总部 图标，可以设置本机作为 VPN 分支机构，接入到其他设备中，并可以多次配置，使本机接入到多个 VPN 总部，最多允许接入 9 个 VPN 总部。配置步骤参见 2.16.1.2 章节。

本机下方的设备，表示本机作为 VPN 总部时，与本机连接的设备。若本机为 L2TP 或 L2TP IPSec VPN 总部时，将会有

添加分支机构 图标，点击此图标可新增一个帐户。

若当前设备只配置作为 VPN 分支机构，如下图所示，您可以点击 让分支接入总部 图标，配置本机作为 VPN 总部，配置步骤参见 1.3.21.1.2 章节。

表格显示页面

如上图所示，第一个表格列出了本机作为 VPN 分支机构时，接入的总部信息；第二个表格列出了本机作为 VPN 总部时，与本机连接的分支机构信息。

点击 管理本机配置 按钮，可以查看、修改本机的 VPN 配置信息。点击 添加接入总部 按钮，可以配置本机作为 VPN 分支机构，接入到多个总部。点击 添加分支机构 按钮，可以添加用户信息。点击表格“操作”列中的 查看 修改 删除，可以对选中的用户进行查看、修改、删除。

- **查看本机的 VPN 配置信息**

可以通过拓扑图页面点击本机设备图标，或表格页面点击“管理本机设备”来查看本机的 VPN 配置信息，如下图所示：

查看作为总部的配置 按钮为灰色状态时，表示当前查看的是本机作为 VPN 总部的配置信息，此时点击 查看作为分支的配置 按钮，将切换到本机作为 VPN 分支机构的配置信息查看页面，如下图所示：

若本机作为 VPN 分支机构，接入到多个总部，VPN 参数上方将有多个选项卡如 接入总部1 接入总部2，此时表示当前显示的是接入到总部 1 的 VPN 配置信息，点击 接入总部2 将会显示本机接入到总部 2 的 VPN 配置信息。

点击 修改配置 按钮，可以对当前选中的 VPN 配置进行修改，如下图所示：

修改完成后，点击 保存 即可。

点击 清空配置 按钮可以清空当前选中的 VPN 配置。如当前选中的是本机作为分支机构中的“接入总部 2”，则本机将与总部 2 断开连接。

- **移动用户信息**

本机配置作为 VPN 总部时，您可以在 VPN 监控页面看到移动用户配置信息，如下图所示：

点击 这里 将弹出移动用户管理页面，如下图所示，您可以在此页面查看、修改、删除某个移动用户信息，也可以点击【用户组织管理】按钮管理移动用户。

1.3.11.7 SSLVPN 配置

SSLVPN 服务为用户提供安全远程接入功能，相对其他类型 VPN，SSLVPN 具有“随时、随地、任何设备”都能安全接入到企业内网的特点，强大的易用性使其在 VPN 市场中优势越来越大，兼具保护企业网络安全和提供远程接入办公功能，在政府、金融、学校、企业、运营商中都有应用。

SSLVPN 使用安全的加密算法和摘要算法，有效保证数据在传输过程中不被窃取及篡改。

SSLVPN 提供细粒的资源访问控制功能，控制用户只能访问管理员授权的内网服务器资源，解决非授权用户大肆访问并修改内网服务器的重要数据。

SSLVPN 有三种接入方式，WEB 接入、安全隧道接入。

WEB 接入：用户登录成功后，可以使用 WEB 浏览器直接访问内网基于 WEB 的应用系统。

安全隧道接入：用户登录成功后可以像局域网一样使用内网资源，包括 TCP/UDP/ICMP 类型的应用。

SSLVPN 可以根据用户授予不同的资源访问权限，用户将无法访问没有授权的资源，具体功能如下：

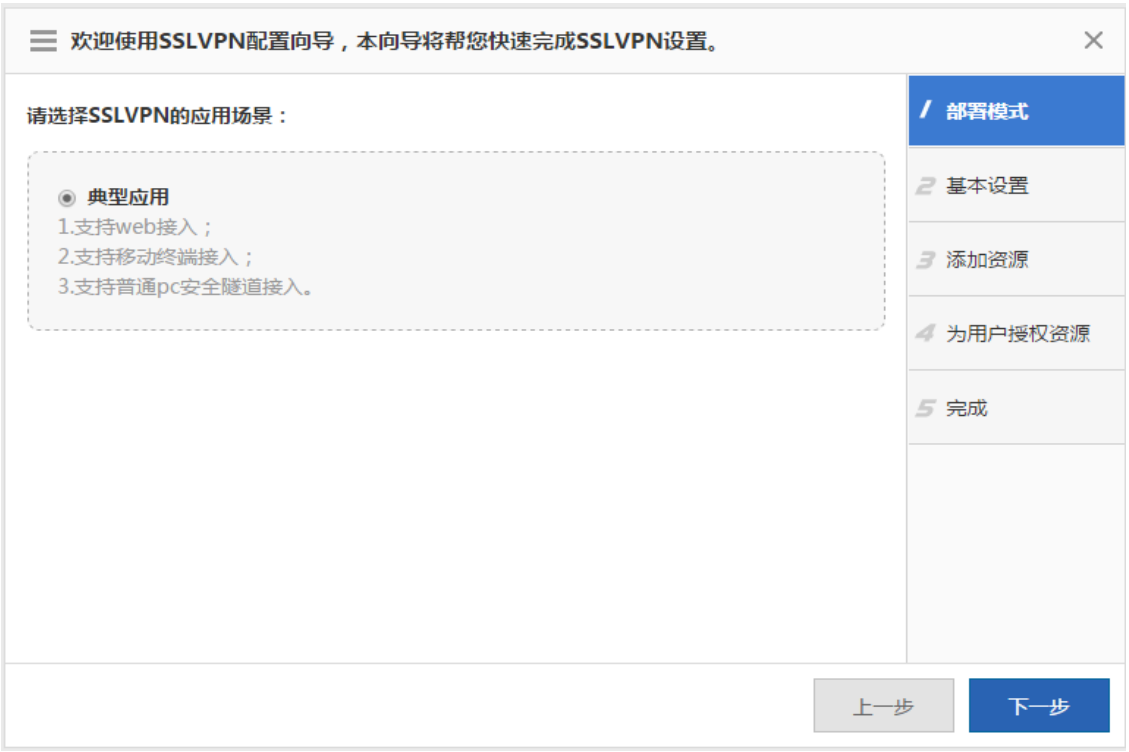
- **对用户/用户组进行授权**：管理员“用户授权”对指定的用户组或用户进行资源授权。
- **资源继承**：用户/用户组会继承其‘父组’的授权的资源；针对指定用户/用户组可以关闭继承。

采用 Radius 认证时，Radius 认证用户默认只继承了“所有用户”已授权的资源，若要授权特定资源，需要在“用户组织”中创建对应的用户或用户组并对其授权。

1.3.11.7.1配置向导

当设备从未配置过 SSLVPN 时，点击“SSLVPN 配置“菜单会打开 SSLVPN 简介和配置向导页面，如下图所示：

点击“开始配置“打开 SSLVPN 配置向导窗口，如下图所示：



下面是典型应用应用的向导配置：

SSLVPN 服务器端口：默认为 https 协议的缺省端口 443，所以当客户端使用 https 访问 SSLVPN 服务时，可以不用输入端口号。如无特殊情况，建议这里保持缺省配置。

SSLVPN DNS：默认使用设备的 DNS，客户端接入时将使用该 DNS 服务器解析域名，如果不配置，则只能通过 IP 访问资源。

用户认证方式：客户端登录 SSLVPN 服务时，使用的认证类型。本地认证是指使用“用户管理>用户组织>用户管理”页面中配置的用户名和密码进行认证。Radius 认证是指使用第三方的 Radius 服务器进行认证。Radius 的配置界面如下：

填上认证服务器的 IP 和密码，以及认证端口即可。同时支持添加多个备用服务器。

配置后 SSLVPN 的基本参数后，点击下一步进入“添加资源”配置，界面如下：

隧道接入资源配置：如何配置见 1.3.23.4 章节

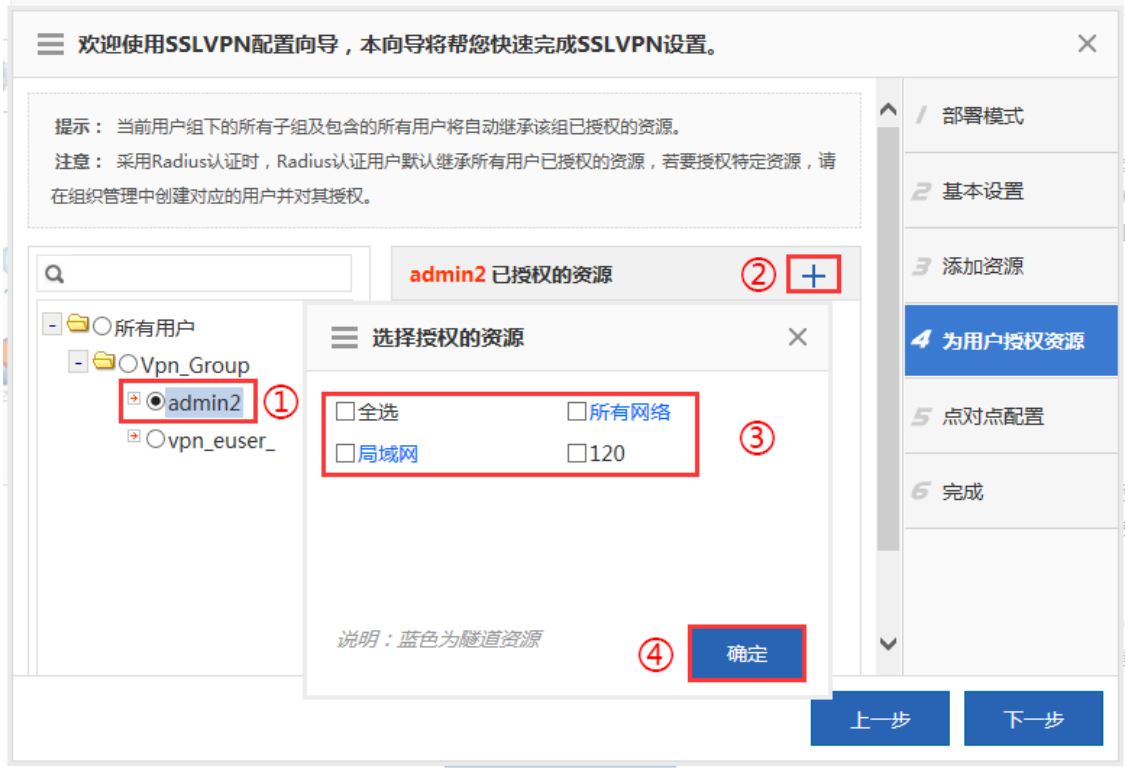
客户端网段：配置 WEB 接入资源：

1. .要启用 WEB 接入资源，请勾选 ☑配置SSLVPN提供的WEB资源
2. 资源名称：用于标识该 WEB 资源的名称。客户端登录成功后将显示该名称。
3. 网址：该 WEB 资源的 URL 地址。必需以 http://或 https://开头。
4. 最多可以配置 127 个 WEB 资源。

为用户授权：

这一步是为用户进行授权，只有授权的用户才可以访问 SSLVPN 提供的服务。具体可参考“2.19.6 用户授权”章节。用户授权的界面如下图所示：

授权步骤如下：



1. 选中要授权的用户或用户组 

2. 点击  将弹出未授权的资源列表。

3. 勾选要授权的资源，这里只列出未授权的资源。

4. 点击  完成对用户（组）新增资源。

5. 要取消资源授权，请点击  。

6. 如果要管理用户请点击  ，会弹出用户管理窗口。

授权完成点击下一步完成 SSLVPN 配置

注意：进入“为用户授权”前建议把要创建的资源配置好，如果从“为用户授权”跳回“添加资源”将清空掉当前的授权□ □ □□ □ □ □ □ □ □ □ □ □ □ □ □□ □ □ □ □ □ □ SSLVPN □ □ □ □□ □ CLI □ □ □ □ □ □ □ □ □ □“ no sslvpn gateway sslvpn “ □ SSLVPN □□ □ □ □ SSLVPN □

1.3.11.7.2运行状态

当设备已启动 SSLVPN 服务，则点击 

时会进入“运行状态“页面。这里显示当前的 SSLVPN 服务的运行状态，包括在线用户、用户名锁定、IP 锁定等信息，同时提供日志查看，用户搜索功能。

SSLVPN 服务正常时：

当 SSLVPN 服务暂停时：

SSLVPN 服务正常时的说明如下：

1. 点击 查看日志 可以查看 SSLVPN 运行中生成的日志记录，界面如下：

日志类型分别有：系统日志、管理员日志、用户日志；日志等级分为：错误、警告、信息。

当设备上的日志文件超过 1M 时，设备将根据时间顺序自动删除掉早期的日志。

2. 通过 用户状态查询： 查询 可以查询用户的在线状态。输入用户名后，点击“查询”。界面如下图所示：

当用户在线时，还可以进行“强制下线”操作。如果用户被锁定，这里也可以解锁。

3. 点击 刷新 会立即刷新相应的显示数据。系统默认每 15 秒会自动刷新一次。

4. 点击 强制下线 会把该用户强制下线，当设备的最大并发用户数有限时，可以通过该功能来确保重要的用户优先上线。

5. 点击 解锁 可以对锁定的 IP 或用户进行解锁。

1.3.11.7.3基本设置

这里提供 SSLVPN 服务的基本参数配置，界面如下图所示：

当 SSLVPN 服务正常运行时，客户端可以通过设备的任意 IP 来访问 SSLVPN 服务。例如设备的外网 IP 为 172.6.6.6，那客户端可以在浏览器中输入 https://172.6.6.6 来访问，如果 SSLVPN 的服务端口不是为 443，那还要加上端口号。设备的所有接口 IP 都可以访问到 SSLVPN 服务。

参数说明：

SSLVPN 服务端口：客户端必需通过该端口访问 SSLVPN 服务。如设备外网 IP 为 172.6.6.6，SSLVPN 服务端口为：3658。那客户端需要在浏览器中输入 https://172.6.6.6:3658 来访问 SSLVPN 服务。当端口为 443 时客户端可以不输入端口号访问。如无特殊情况，建议这里保持缺省配置。

SSLVPN 服务 DNS：默认使用设备的 DNS，客户端接入时将使用该 DNS 服务器解析域名，如果不配置，则只能通过 IP 访问资源。

用户认证方式：客户端登录 SSLVPN 服务时，使用的认证类型。本地认证是指使用“用户管理>用户组织>用户管理”页面中配置的用户名和密码进行认证。Radius 认证是指使用第三方的 Radius 服务器进行认证。

DNS 查询优先级：

启用用户锁定：开启后，当同名用户登录连续出错达到指定次数(默认 5 次)后，该用户名将被锁定，同时可以配置锁定时间，在锁定时间内该用户无法登录，0 为不自动解锁。该功能主要为了防止客户端被爆力破解。

启用用户锁定：开启该功能后，当相同用户名登录连续出错达到指定次数(默认 5 次)后，该用户名将被锁定，同时可以配置锁定时间，在锁定时间内该用户无法登录，0 为不自动解锁。该功能主要为了防止客户端被爆力破解。

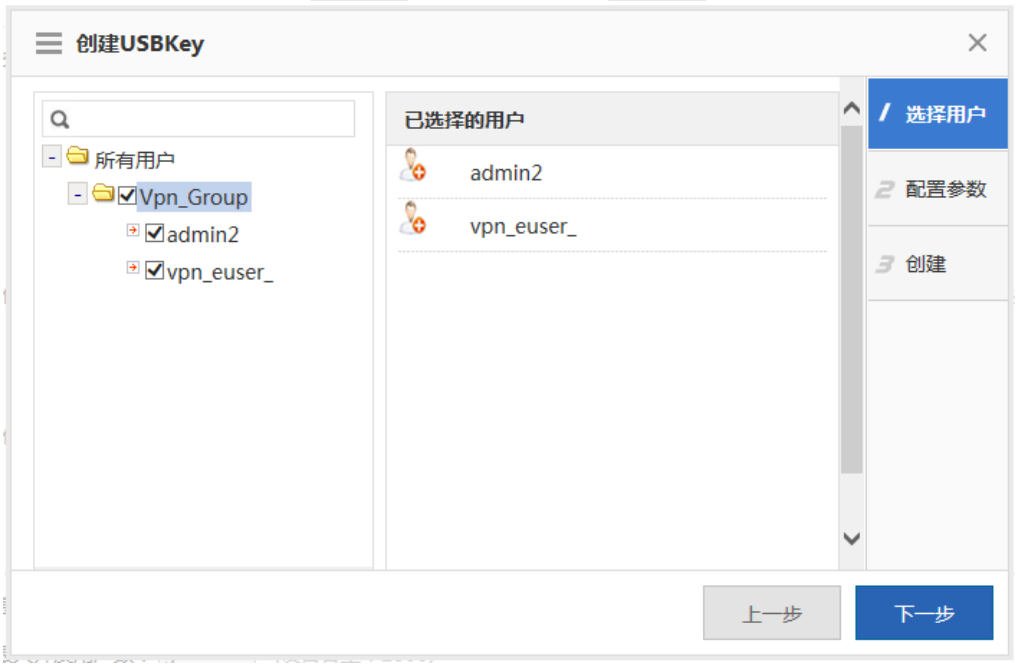
启用 IP 锁定：开启后，同 IP 用户登录连续出错达到指定次数（默认 64 次）后，该 IP 地址将被锁定。

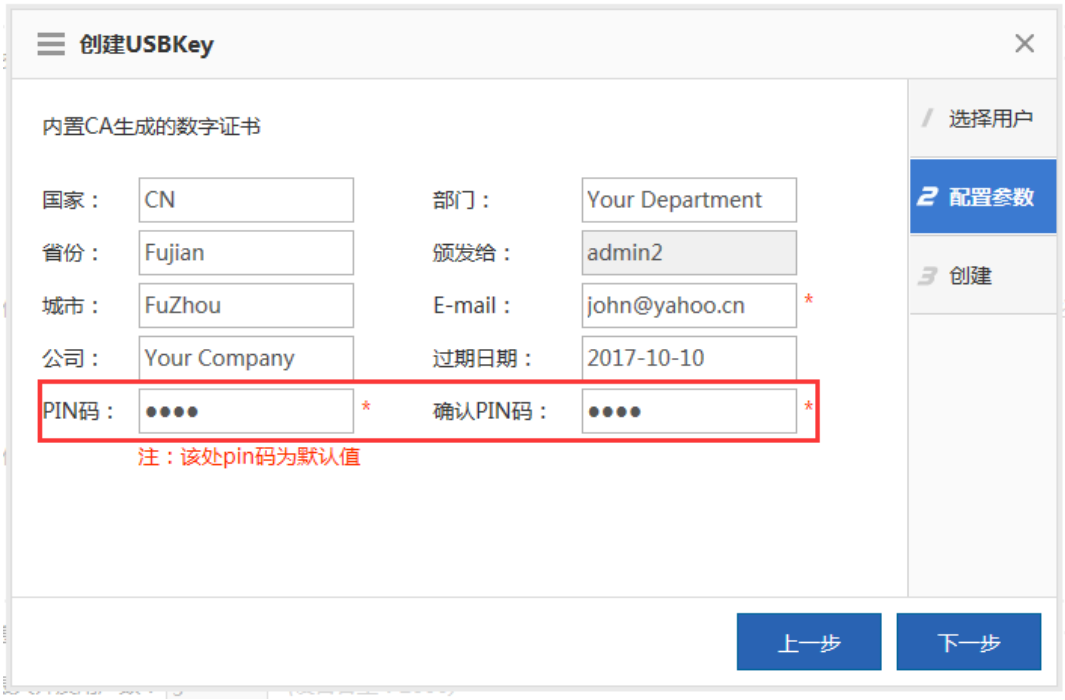
启用图形验证码：开启图形验证码功能，用户使用 WEB 浏览器登录必须先输入图形验证码，可以有效的防止暴力破解用户密码，开启后，可以选择图形验证码来登录，如下：

启用 USBKey **认证：**若开启 USBKey 认证，用户可以选择 USBKey 认证方式进行访问 SSLVPN 服务。启用 USBKey 认证后，若所有接入用户均分发了 USBKey，为了安全考虑，可以禁止账号方式从 PC 登录，只允许用户通过 USBKey 登录。由于无法在移动终端上使用 USBKey，因此在移动终端上依然可以使用账号方式登录。开启 USBKey 认证后，可以选择 USBKey 来登录 sslvpn 客户端如下图：

创建 USBKey：创建前需要下载 USBKey 控件和驱动，根据你的 pc 安装 32 位或者 64 位控件 USBKey导入控件和驱动安装包下载，然后点击创建按钮【创建USBKey】，如下图创建页面

可以选择你想创建的用户：





默认的 pin 码为 1234,

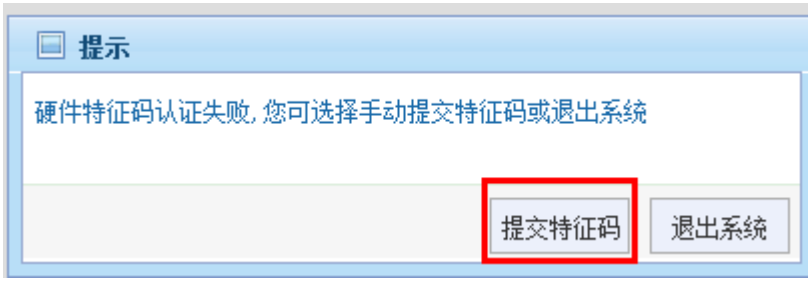
创建一个用户成功后，会跳到下一个用户继续创建直到结束，如果你不想创建当然用户你可以选择跳过下一个创建。

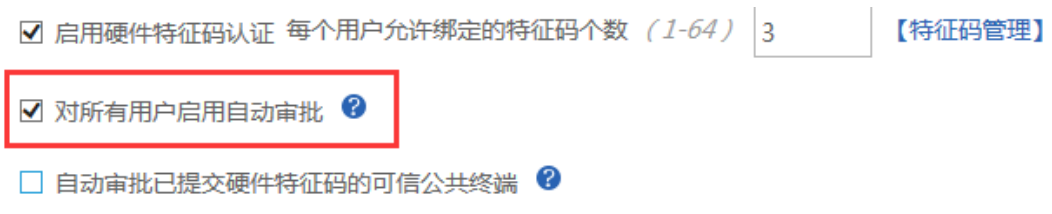
启用硬件特征码：

硬件特征码是根据接入终端硬件特性，如 CPU、硬盘序列号、网卡等计算出来的一串硬件代码，其唯一性可以标识一台特定的终端。

SSLVPN 利用该特性进行账号与终端进行捆绑，限制账号只能在已审批的终端进行登录，防止非法黑客盗取用户账号后在其他终端上登录使用，从而进一步的保护 SSLVPN 用户账号的安全。

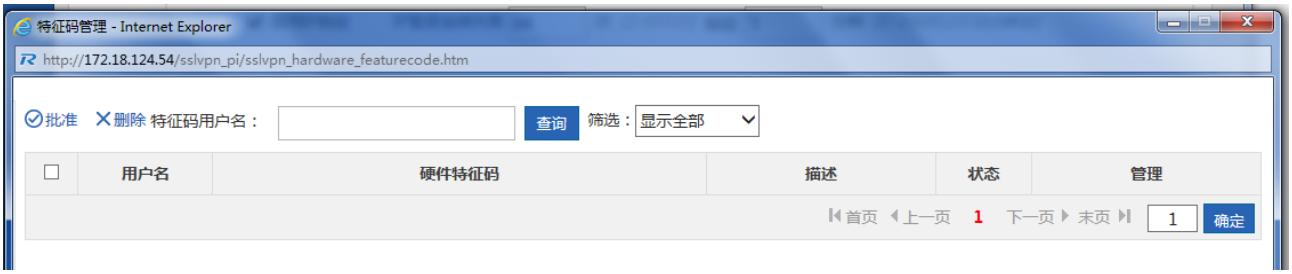
收集硬件特征码





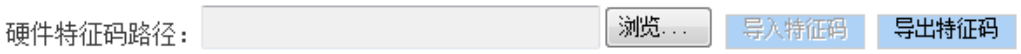
开启对所有用户

自动审批后，只要提交特征码就能自动审批，也可以手动在特征码管理 【特征码管理】 手动审批：



特征码管理还可以对硬件特征码做批量的审批和删除操作。

硬件特征码的导入和导出：



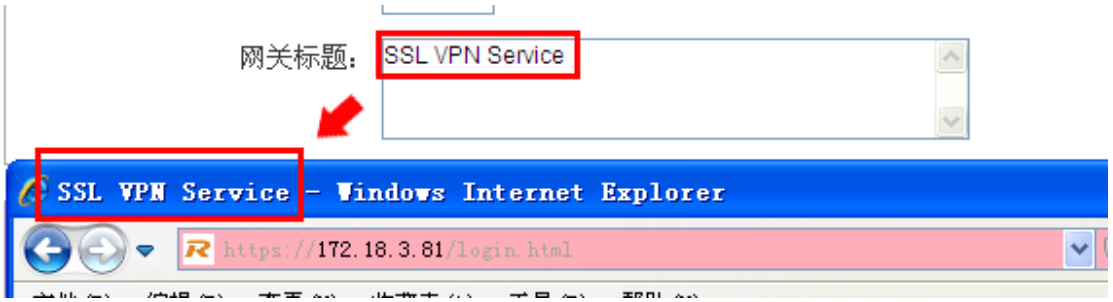
可以对设备的硬件特征码进行备份，以及导入方便网管的操作。

启用软键盘：开启该功能后，客户端 WEB 登录页面可以使用虚拟的图形软键盘进行输入密码，有效防止木马进行键盘记录窃取用户密码，当开启后，客户端的登录页面会显示软键盘，如下图所示：

最大并发用户数：允许同时在线的用户数，设备出厂赠送 5 个并发用户数。如果需要更多并发用户数，可以通过购买 License 获得，License 在‘高级选项’ → ‘License 管理’进行导入。

单用户并发最大连接数：一个用户登录后允许使用的最大连接数，0 为不限制，设备默认为不限制。该功能可以防止单用户创建过多的连接数，如开启 P2P 软件致内网网速变慢。

网关标题：客户端使用 SSLVPN 服务时网页显示的标题，如下图所示：



启用超时自动退出：当客户端登录 SSLVPN 服务后，空闲超过一定的时间后，设备将自动把该用户强制下线，释放设备资源同时保证安全。

启用 SSLVPN 专线：开启后，当用户成功登陆 SSLVPN 后将不能访问互联网，形成一个只能访问 SSLVPN 的专线环境。

显示 URL 地址栏：开启后，则在客户端显示 URL 地址栏，并允许访问内网任意 WEB 资源。客户端界面如下图所示：

SSLVPN 网关证书导入：导入.pfx 格式的网关证书及证书密码。导入证书后，用户在登录 SSLVPN 之前，设备使用网关证书向用户浏览器进行认证，用户浏览器可以通过证书信任链来验证该网关证书的合法性。

可信客户端证书导入和导出：
导入功能：导入本设备先前导出的可信客户端CA证书用于恢复先前分发USBkey的认证，同时导入其他设备可信客户端CA证书后，其他设备生成的USBKey也可在本设备进行验证。导入可信客户端CA证书不会覆盖设备原有的证书，到时在原有证书的基础上叠加，可导入多张可信客户端证书。

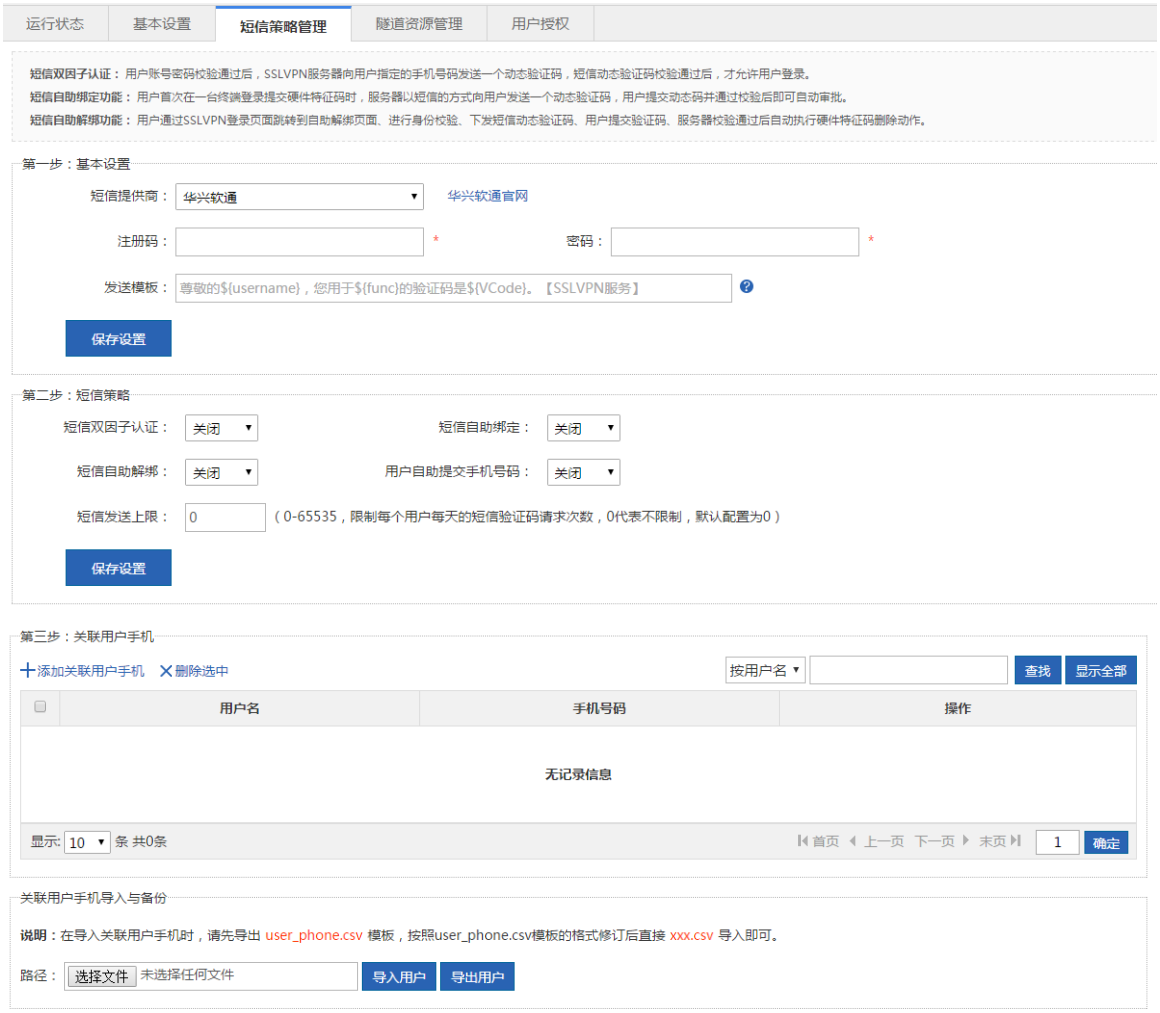
导出功能：主要用于可信客户端 CA 证书的备份。可信客户端 CA 用于验证 USBKey 认证用户，当生成 USBKey 并分发给用户使用后 建议导出可信客户端 CA 证书 避免因出现意外 如设备被格式化、设备恢复出厂设置导致分发给用户的 USBKey 无法被正常验证。

LOGO 文件配置：上传 logo 文件，在用户登录页面及用户登录后的页面将显示你上传的 logo

暂停服务：可以暂时关闭 SSLVPN 服务，SSLVPN 相关的配置还会保留。服务暂停后客户端将无法使用 SSLVPN 功能。

关闭服务：彻底关闭 SSLVPN 服务，彻底关闭 SSLVPN 服务后会清空 SSLVPN 相关的配置信息。

1.3.11.7.4短信策略管理



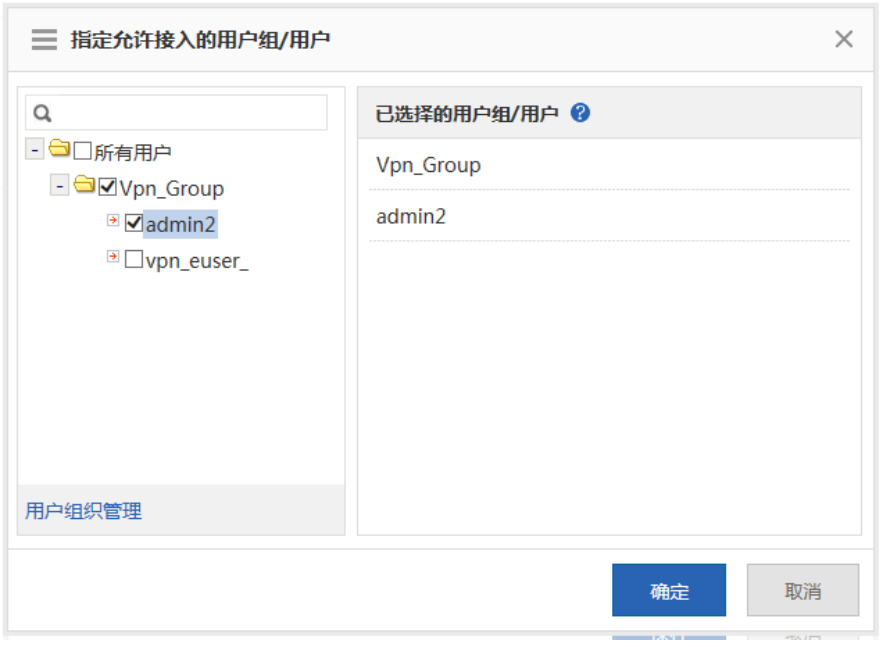
1.3.11.7.5隧道资源管理

通过本页面可以管理 SSLVPN 服务提供的隧道资源。通过管理隧道资源管理，可以控制哪些 SSLVPN 用户可以使用内网的哪些资源。

- **所有网络资源管理**

所有网络资源管理是默认存在的，通过添加相关用户，用户可以像局域网一样使用内网资源，点击后弹出如下弹出框：

点击设置按钮，添加可以使用该资源的用户，弹出添加用户弹出框如下



点击确定后就可以添加相关的用户，然后返回上一个弹出框点击保存，就可以添加成功

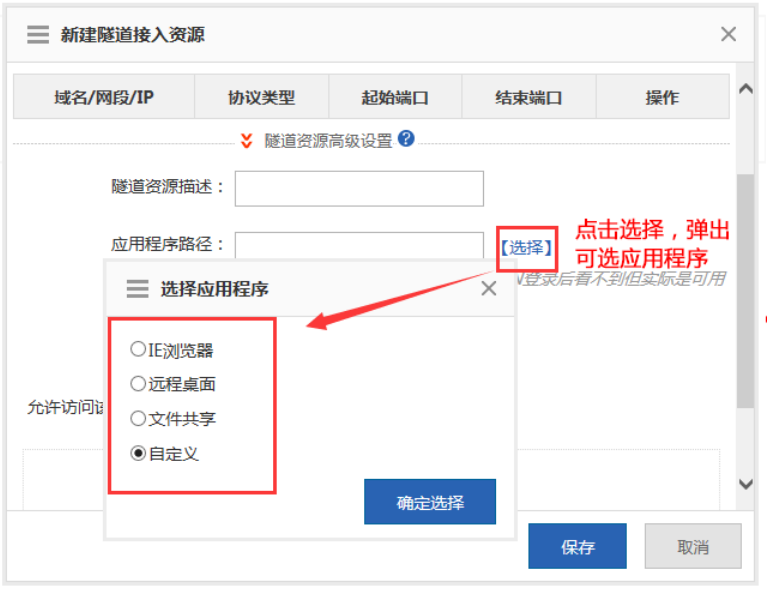
- **添加新隧道资源**

点击 添加新的隧道资源，弹出添加框如下：

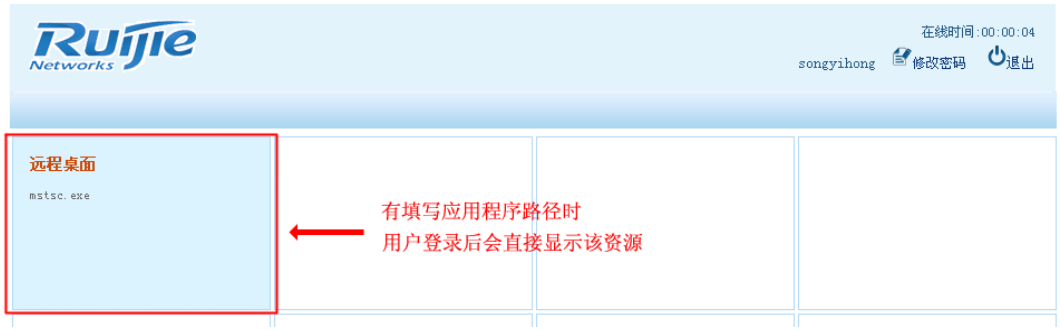
1. 当客户端通过隧道接入后，设备将为该客户端分配一个内网 IP 地址，此处就是配置可分配的 IP 地址池。所以必需要保证这些 IP 不和内网其它 IP 段冲突，如果存在冲突客户端将无法正常使用。
2. DNS 查询优先级：这里优先级只对没有授予“所有网络”隧道资源用户生效，选择内网 DNS 优先，用户将使用上一步中配置的 DNS 解析地址，选择客户端 DNS 优先，用户将使用自己电脑上配置的 DNS 解析地址
3. 新建隧道资源：点击  添加隧道资源，弹出如下弹出框：

填写资源的地址，可以选择网段、IP、域名，当资源地址使用的是内网域名时候，最好要填写内网的 DNS 解析地址，并采用内网 DNS 优先。点击“高级选项”展开可以选择更细致信息，资源使用的协议包括 ANY、TCP、UDP，资源使用的端口号。可以同时添加多个控制规则，形成一个资源组。

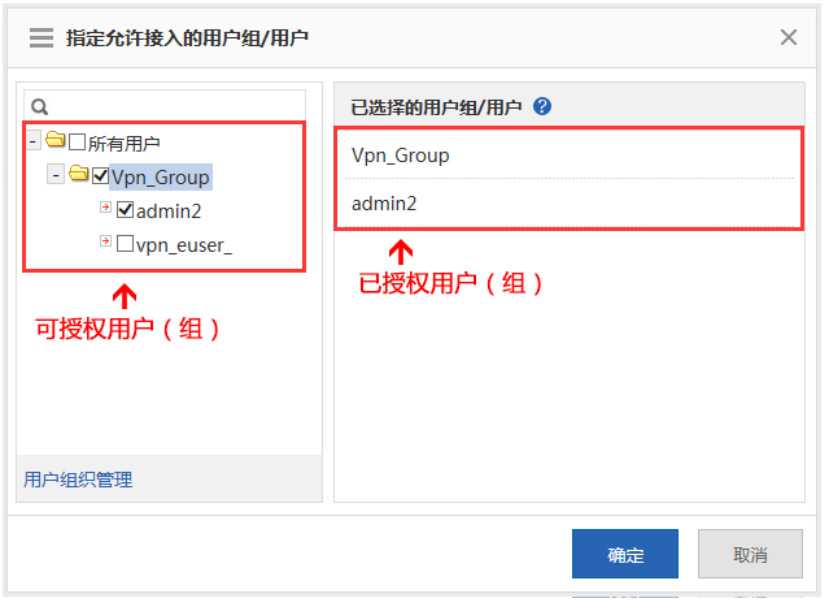
点击“隧道资源高级设置”展开更多信息，可对该资源组进行描述，可以选择应用程序的路径，点击选择有 IE 浏览器、远程桌面、文件共享三个已知路径的可供选择，当然还可以自定义应用程序路径，有时候启动应用程序的还需要参数的，可以填写启动该程序的参数。



当有填写应用程序路径的时候，会在用户登录后列出该资源列表，用户直接点击就可以打开使用，如果没有填写用户程序时候，用户登录后将看不到该资源列表，其实该资源是可以使用的。



4. 允许访问该资源的用户组：可以设置哪些用户有权使用当前资源，点击 +设置 添加可以访问该资源的用户：



选择完要授权的用户后，点击“确定”。返回添加页面点击“保存”之后就可以完成新资源添加

对已有的隧道资源，鼠标移上，点击 X 可直接删除。

1.3.11.7.6WEB 资源配置

点击 添加新的 web 资源地址，弹出添加框如下：

1. 资源名称：用于标识该 WEB 资源的名称。客户端登录成功后将显示该名称。
2. 网址：该 WEB 资源的 URL 地址。必需以 http://或 https://开头。
3. 允许访问页面的子链接：有时一个 WEB 接入资源只是一个门户，通常它可能会有很多不同域站点的超链接也同样需要访问，这时可以开启该功能，而不用分别为这些不同域资源授权。
4. 开启 URL 改写：内网 WEB 服务通过 SSLVPN 访问时，需要对网页内容，特别是网页中的超链接进行自动改写，以达到用户如在内网访问一样的效果，这是可以开启该功能
5. 允许访问该资源的用户组：可以设置哪些用户有权使用当前资源。

对已有的 web 资源可以鼠标移上，点击 X 可进行删除。

1.3.11.7.7用户授权

通过这页面可以对用户（组）进行授权。这里的用户树列出的是本地用户，也就是用户管理中配置的用户。S3760E-24(EL)的 SSLVPN 采用认证和授权分离的机制，就是认证可以是本地用户或 Raduis 服务器认证，但授权只能对本地用户授权，要对 Raduis 服务器上的用户授权，需要在本地用户中创建一个同名用户，如果没有同名用户，那 Raduis 认证进来的用户默认继承“所有用户”组的资源。

如果在用户管理中关闭了“允许做 VPN 用户”的功能，采用本地用户认证时，该用户将无法登录成功，如果是使用 raduis 认证，同时又有同名用户，那只有开启“允许做 VPN 用户”后才能对该用户进行细致地授权，否则只继承“所有用户”的资源。

资源的授权有继承关系，如果对用户组授权，那该组下的所有用户或用户组都将自动继承到该组的资源。用户授权的页面如下：

授权步骤如下：

1. 选中要授权的用户或用户组 

2. 点击  将弹出未授权的资源列表。

3. 勾选要授权的资源，这里只列出未授权的资源。

4. 点击 

完成对用户（组）新增资源。

5. 要取消资源授权，请点击 ✕。带有（继）的资源是从父用户组继承来的。

6. 如果要管理用户请点击 用户组织管理，会弹出用户管理窗口。

1.3.11.8 NAT/端口映射

NAT 英文全称是“Network Address Translation”,即“网络地址转换”,它允许一个整体机构以一个公用 IP 地址出现在 Internet 上。顾名思义，它是一种把内部私有网络地址（IP 地址）翻译成合法网络 IP 地址的技术。

1.3.11.8.1端口映射

端口映射包含两个映射关系，端口映射和整机映射（DMZ 主机）；

端口映射如图：

点击“添加”，在弹出窗中进行端口映射配置。

内网 IP：要映射到外网的内网 IP，通常是您的服务器 IP 地址。

内网端口：要映射到外网的端口。

外网 IP：广域网的 IP 地址。如果选择接口，则该外网接口上所有的 IP 都会映射。

外网端口：广域网上的端口，取值范围为 1 至 65535。

协议类型：请根据需要选择 TCP 或 UDP。

描述：端口映射的描述信息。

设置完毕后点击 确定 按钮。

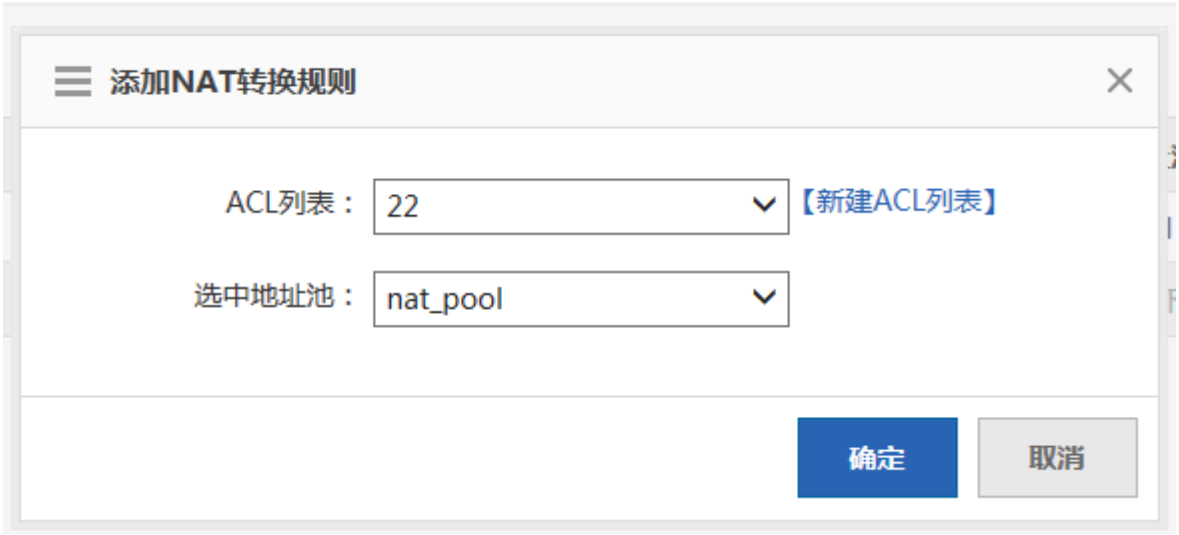
Ps：可根据示例进行配置。

1.3.11.8.2NAT 转换规则

该功能是将 ACL 应用于 NAT 地址池，只有匹配该 ACL 的地址才进行转换。

ACL 列表：选择您要应用到该规则的 ACL 序号或名称。

应用于地址池：选择要作用到的地址池。

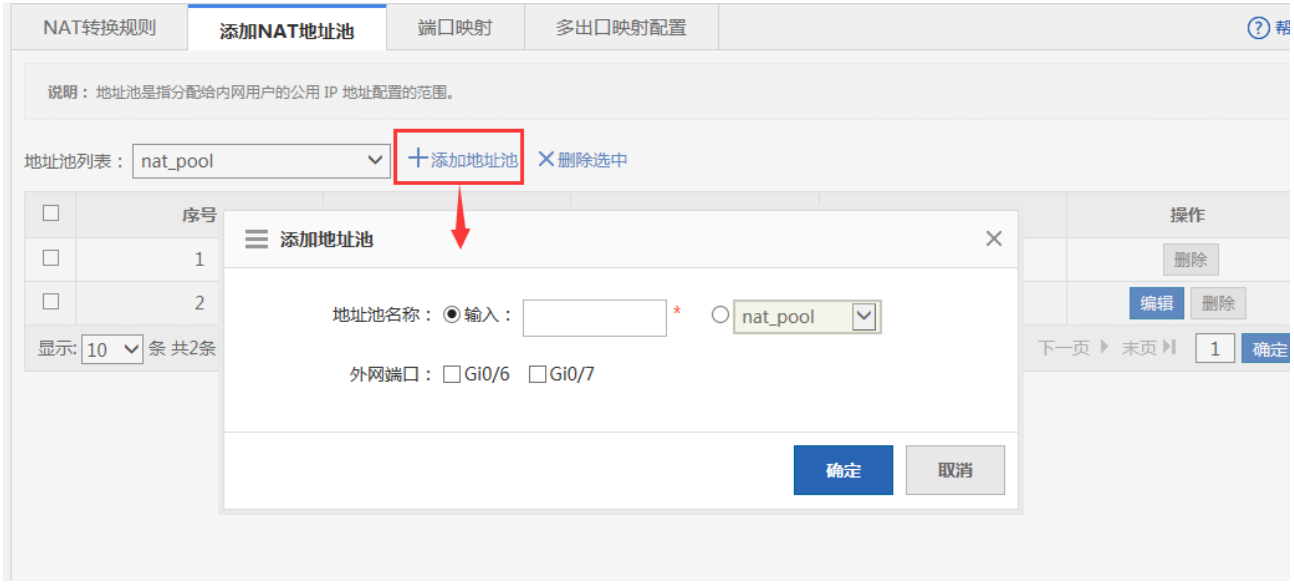


选择完毕后点击“确定”按钮来新增一条地址转换规则。

1.3.11.8.3添加 NAT 地址池

当您有多个外网 IP 时，您可以通过添加地址池让内网 IP 自动选择地址池中的外网 IP 进行转换。

点击“添加地址池”，在弹出窗中进行地址池的配置。



地址池名称：该地址池的名称，如果要在现有的地址池上添加地址，请选择  选择现有的地址池。

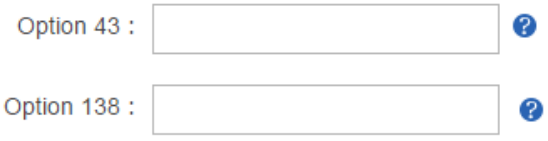
选择外网口：选择您要添加的外网口，此时下方会出现如下图所示选项：

输入起始 IP 地址和结束 IP 地址，如果只有一个 IP 地址，那结束 IP 和起始 IP 输入一致即可。可以为一个地址池配置多个 IP 段，IP 段之间不可以重叠。配置完后点击  进行保存。

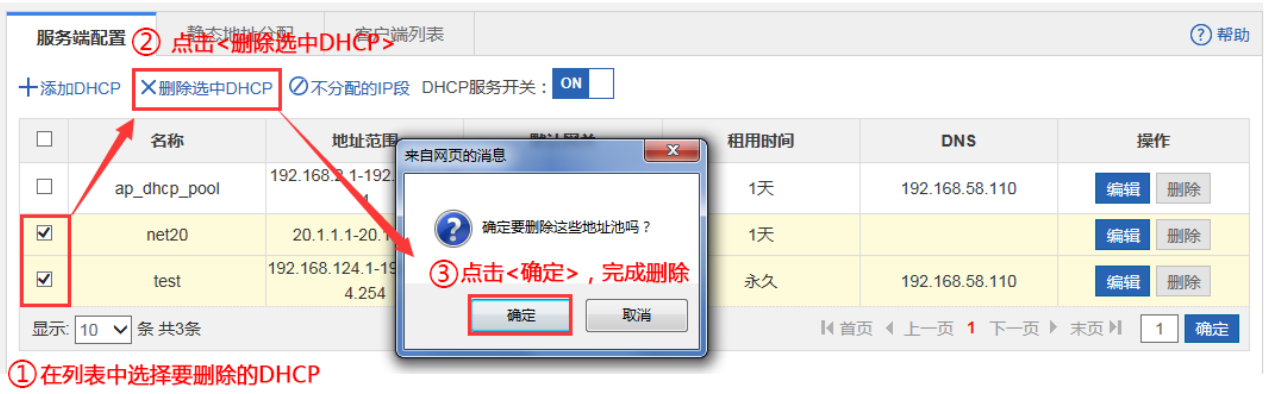
1.3.11.9 DHCP 配置

1.3.11.9.1服务端配置

- 添加 DHCP

- 

- 批量删除 DHCP

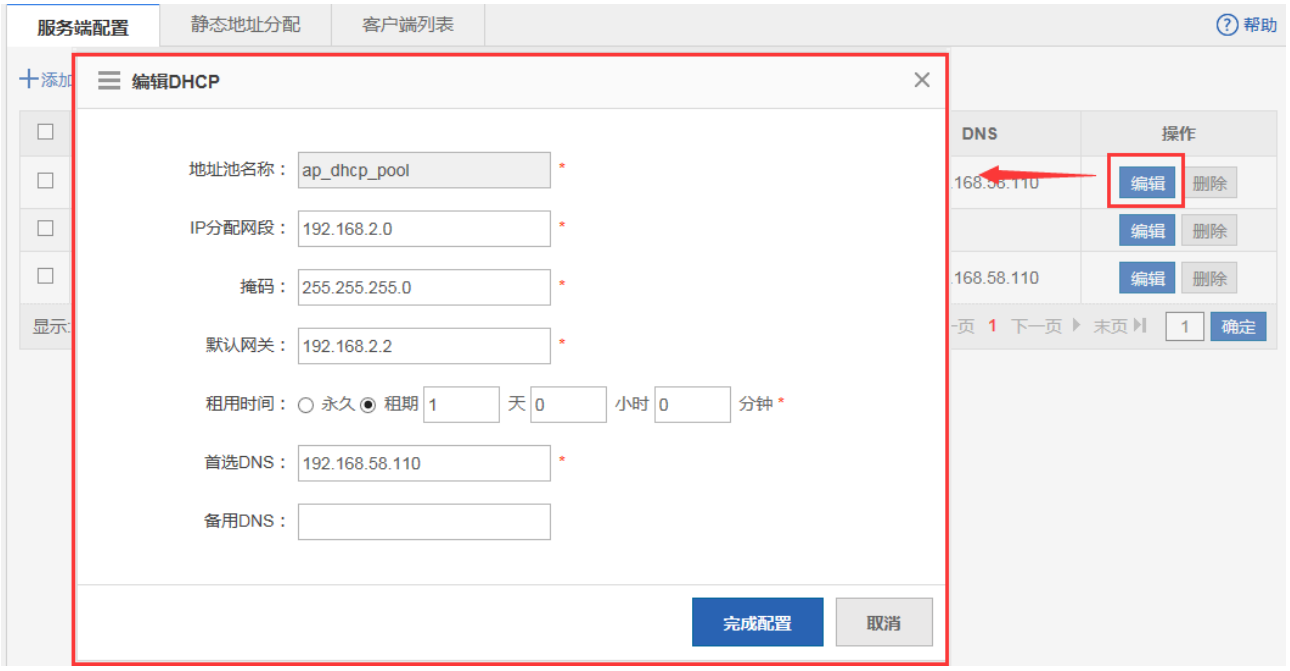


- 配置不分配的 IP 段

不分配的 IP 段：可以配置若干个 IP 段，IP 段内的 IP 将不会分配给用户。

- DHCP 服务开关

- 编辑 DHCP



在 DHCP 列表中，点击<编辑>按钮，在弹出窗中可以对该条 DHCP 信息进行编辑。

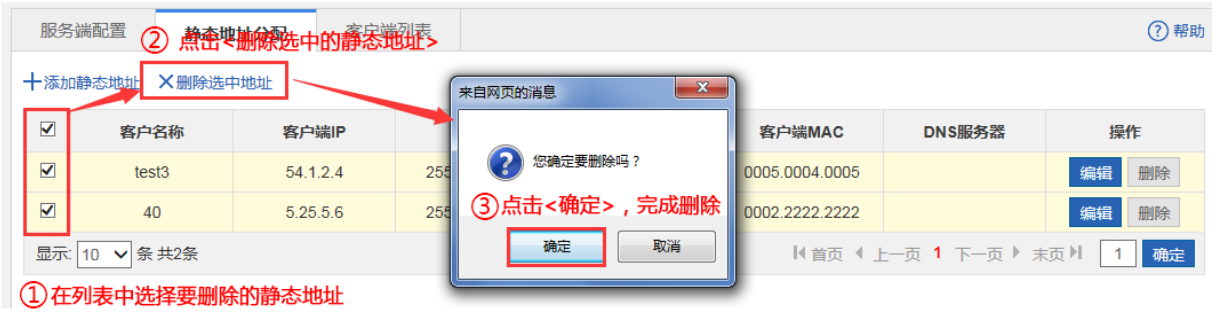
- 删除 DCHP

在 DHCP 列表中，点击<删除>按钮，在弹出窗确认窗口中，点击<确定>后可以删除该条 DHCP 信息。

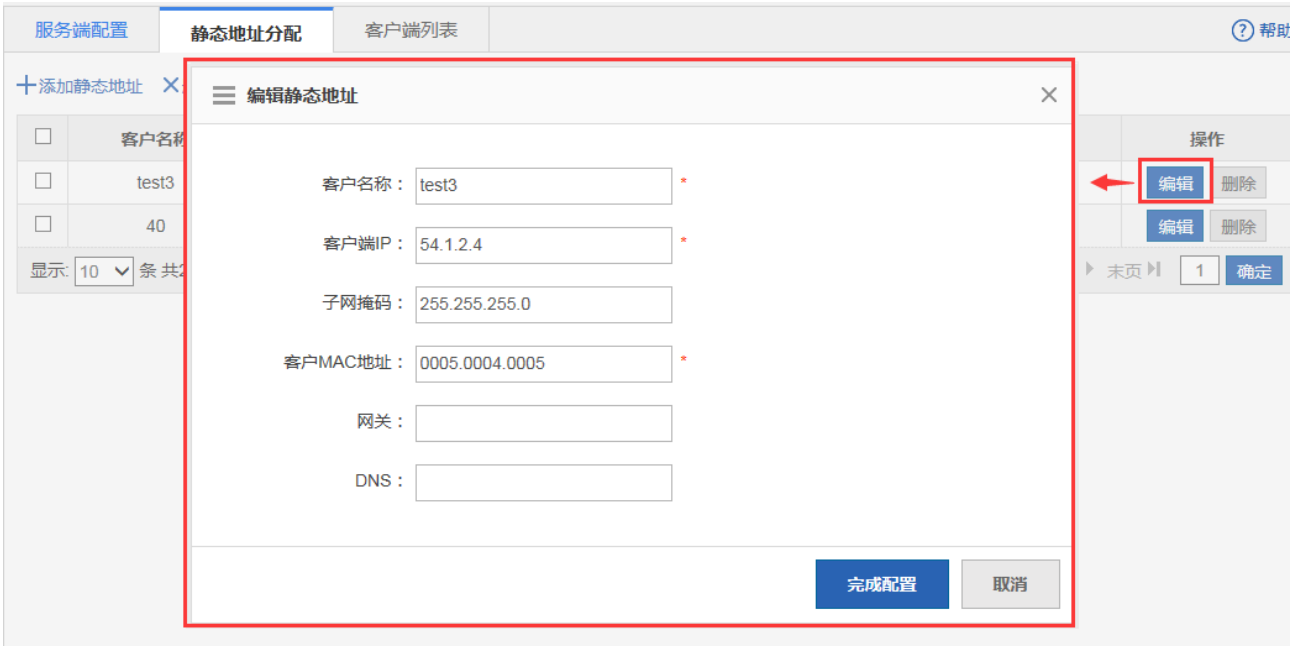
1.3.11.9.2静态地址分配

- 添加静态地址

- 批量删除静态地址



- 编辑静态地址



在静态地址列表中，点击<编辑>按钮，在弹出窗中可以对该条静态地址信息进行编辑。

- 删除静态地址

在静态地址列表中，点击<删除>按钮，在弹出窗确认窗口中，点击<确定>后可以删除该条静态地址信息。

1.3.11.9.3客户端列表

- 绑定 MAC 地址到动态获取的 IP 上

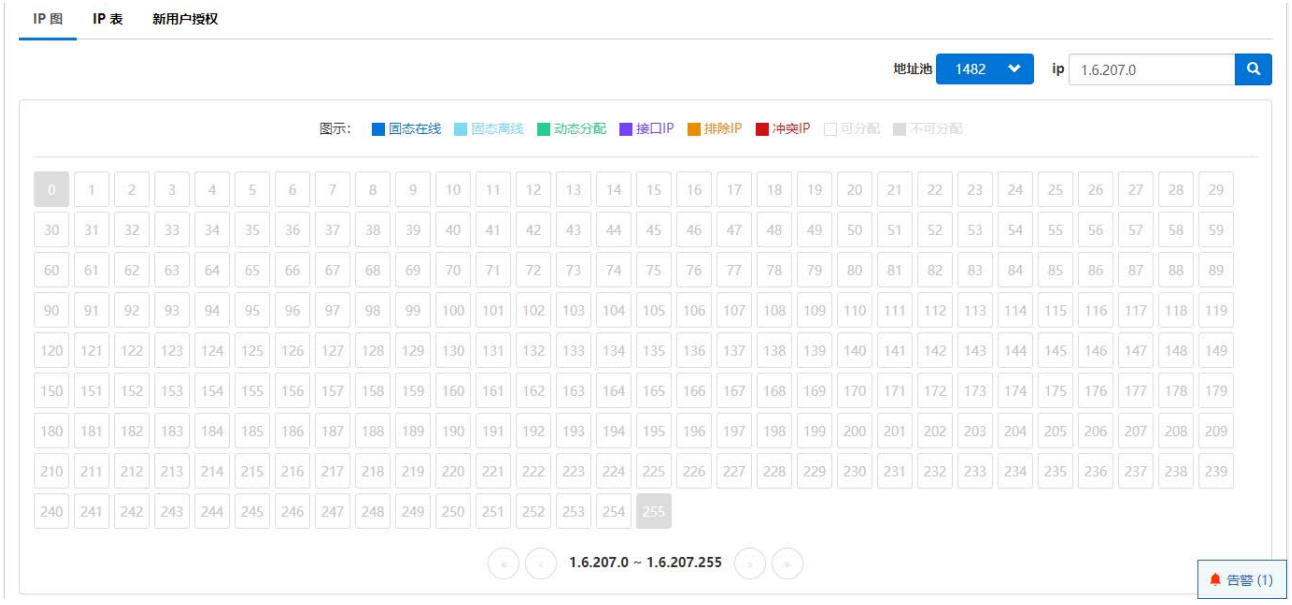
在列表中，选择要绑定记录，点击<把 MAC 地址绑定到动态获取的 IP 上>，即可完成绑定。

- 基于 IP 地址查询客户端

在输入框内输入要查询的 IP 地址。点击<搜索>按钮，列表中显示符合条件的搜寻结果。

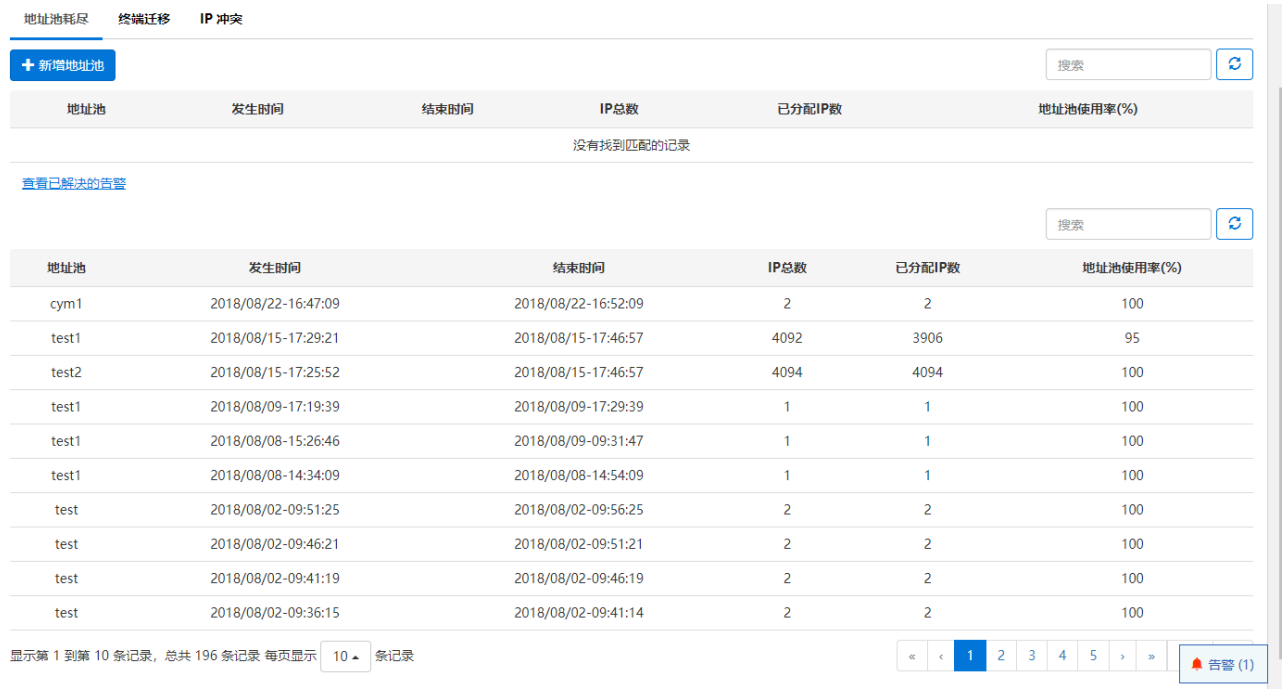
1.3.11.9.4IPAM 主页

1.3.11.9.5IP 智能管理

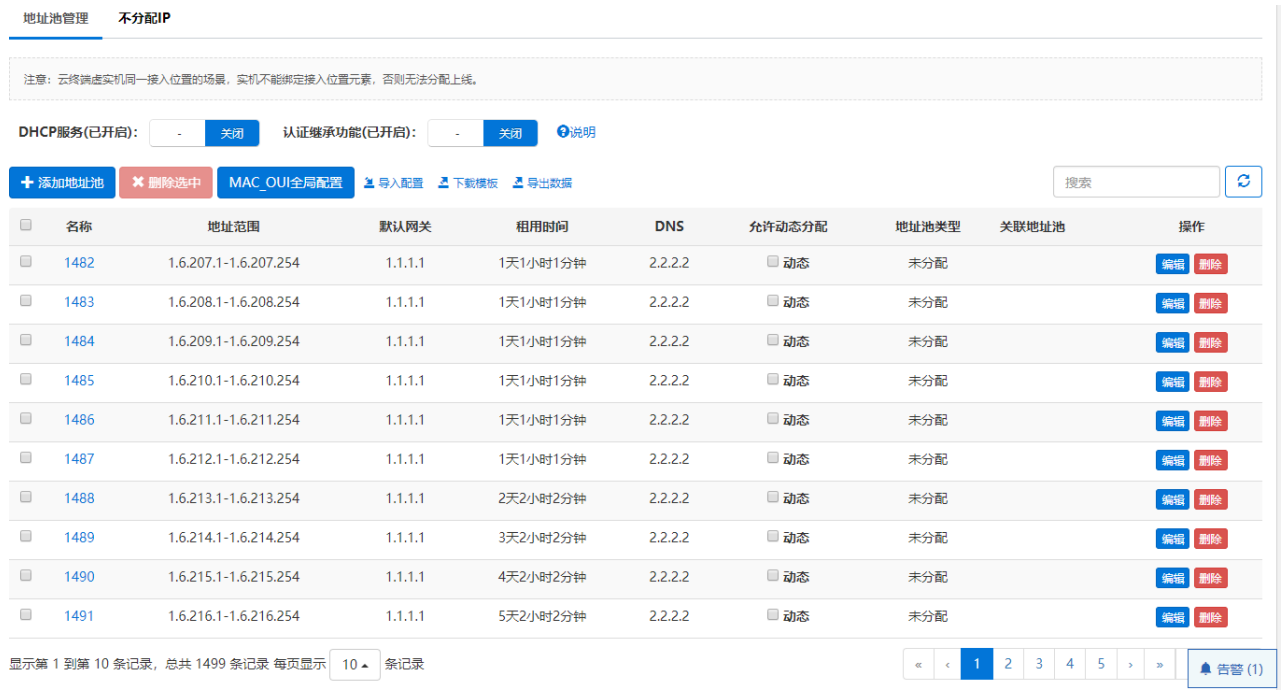


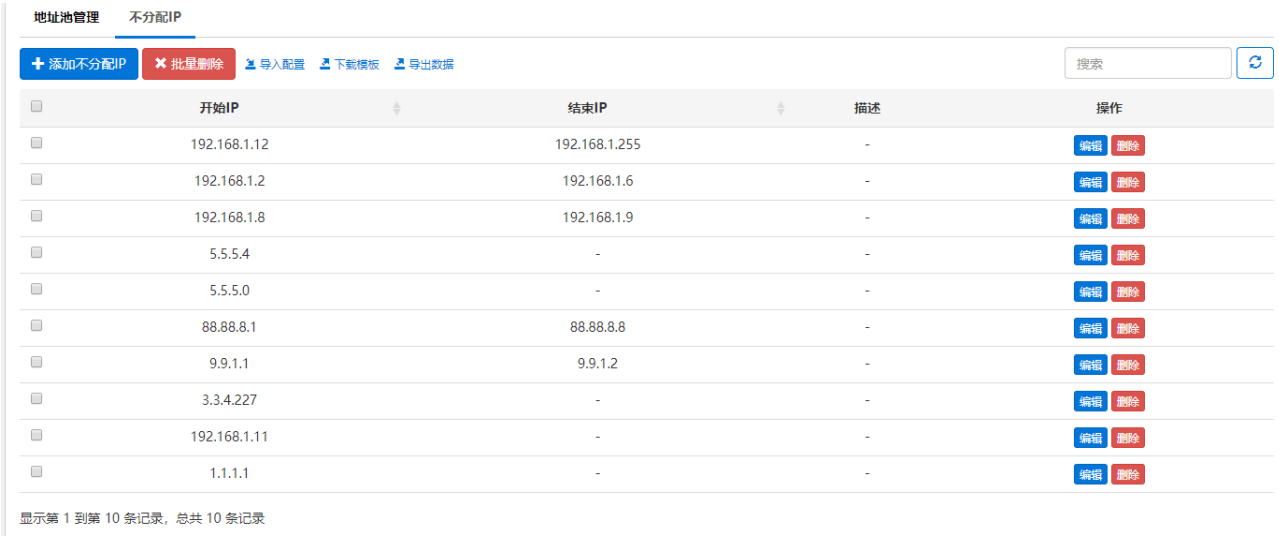

IP 图
IP 表
新用户授权
自定义显示
新增固态用户
批量绑定
删除选中
批量加入mac黑名单
导入配置
下载模板
导出数据
搜索地址池:
所有地址池
搜索字段
搜索字段值
搜索
清空搜索
MAC
IP
所有用户
地址租期
接入设备
主机名
所有状态
所有绑定类型
操作
0000.0000.0001 1.3.151.1 普通用户 0天0小时0分钟 固态离线 IP+MAC
0000.0000.0002 1.1.212.190 普通用户 0天0小时0分钟 固态离线 IP+MAC
0000.0000.0003 1.1.212.191 普通用户 0天0小时0分钟 固态离线 IP+MAC
0000.0000.0004 1.1.212.192 普通用户 0天0小时0分钟 固态离线 IP+MAC
0000.0000.0005 1.1.212.193 普通用户 0天0小时0分钟 固态离线 IP+MAC
0000.0000.0006 1.1.212.194 普通用户 0天0小时0分钟 固态离线 IP+MAC
0000.0000.0007 1.1.212.195 普通用户 0天0小时0分钟 固态离线 IP+MAC
编辑
加入mac黑名单
删除
IP 图
IP 表
新用户授权
批量授权
全部授权
批量删除
全部删除
搜索
MAC地址
所属地址池
接入设备信息
VLAN
端口索引
主机名
失败时间点
上线失败次数
授权建议
操作
没有找到匹配的记录

1.3.11.9.6业务告警


地址池耗尽
终端迁移
IP 冲突
新增地址池
搜索
地址池
发生时间
结束时间
IP总数
已分配IP数
地址池使用率(%)
没有找到匹配的记录
查看已解决的告警
cym1 2018/08/22-16:47:09 2018/08/22-16:52:09 2 2 100
test1 2018/08/15-17:29:21 2018/08/15-17:46:57 4092 3906 95
test2 2018/08/15-17:25:52 2018/08/15-17:46:57 4094 4094 100
test1 2018/08/09-17:19:39 2018/08/09-17:29:39 1 1 100
test1 2018/08/08-15:26:46 2018/08/09-09:31:47 1 1 100
test1 2018/08/08-14:34:09 2018/08/08-14:54:09 1 1 100
test 2018/08/02-09:51:25 2018/08/02-09:56:25 2 2 100
test 2018/08/02-09:46:21 2018/08/02-09:51:21 2 2 100
test 2018/08/02-09:41:19 2018/08/02-09:46:19 2 2 100
test 2018/08/02-09:36:15 2018/08/02-09:41:14 2 2 100
显示第 1 到第 10 条记录，总共 196 条记录 每页显示 10 条记录
告警 (1)

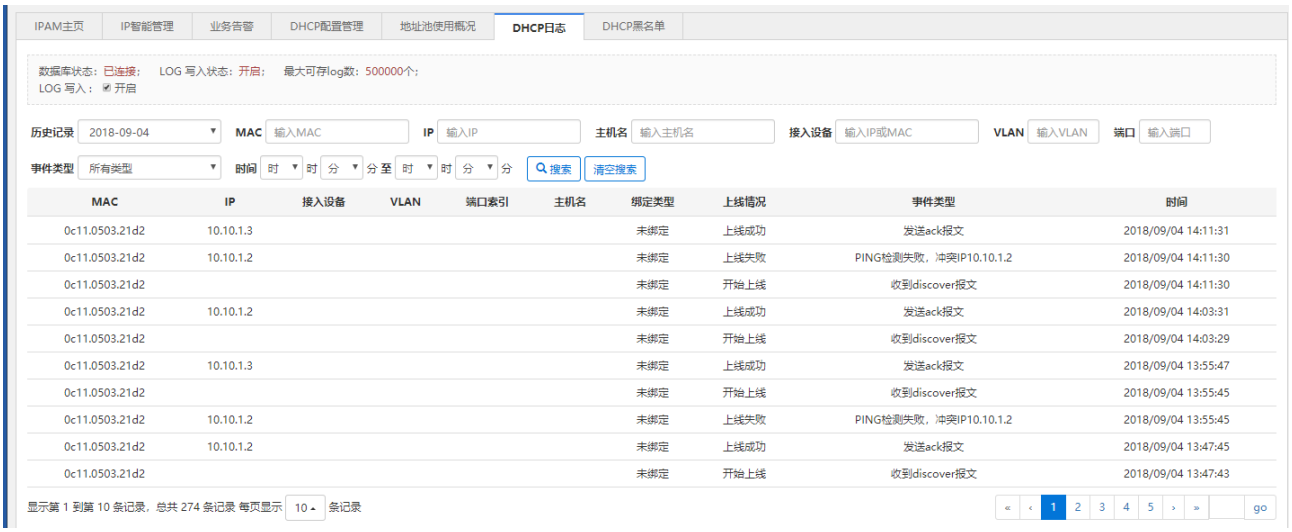
1.3.11.9.7DHCP 配置管理





1.3.11.9.8地址池使用情况

1.3.11.9.9DHCP 日志



1.3.11.9.10 DHCP 黑名单

1.3.11.10 线路逃生

分三个菜单，线路流量逃生、路由流量逃生和逃生日志

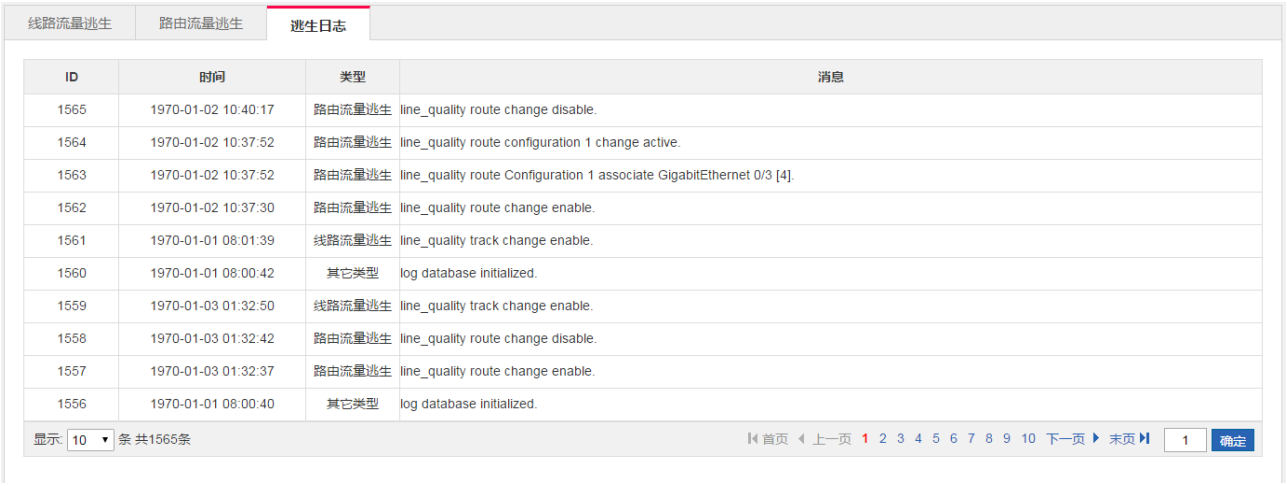
1.3.11.10.1 线路流量逃生

可以一键开启，如下图配置。

支持高级选项配置：

- 该配置属于高危操作，**注意：**检查线路是否正常，探测到线路异常时，可能导致断网。
- 对接口进行 UP、DOWN 操作为高危操作，请谨慎操作。

1.3.11.10.2 逃生日志

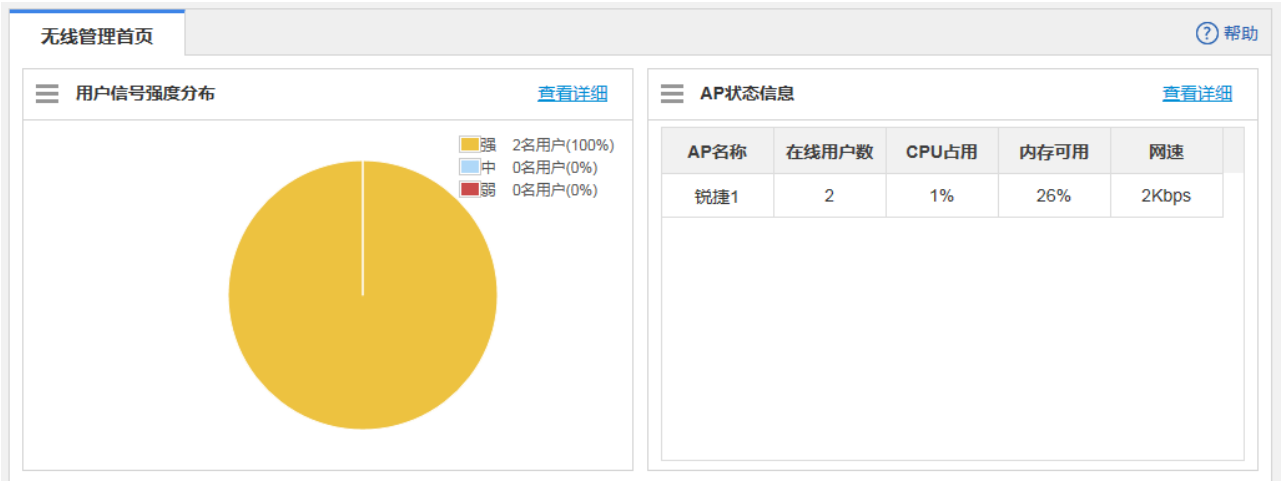


可以查看近期的逃生日志

1.3.12 无线

1.3.12.1 无线管理首页

无线管理首页包含用户信号强度分布和 AP 状态信息。

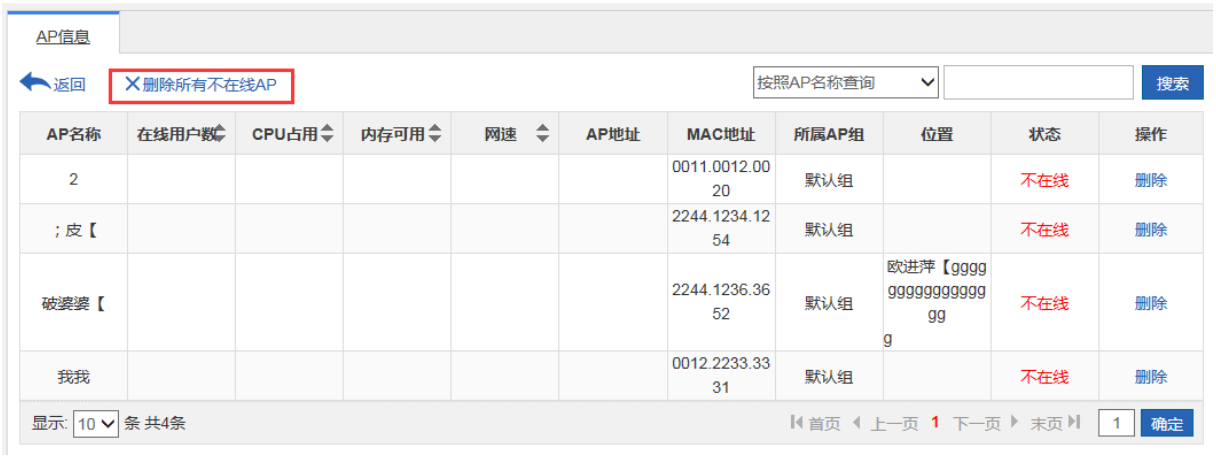


- 用户信号强度分布

  点击“查看详细”可以查看详细的用户信息和历史记录，点击“返回”即可回到无线管理首页。

- AP 状态信息

  点击“查看详细”可以查看详细的 AP 信息，删除不在线 AP，点击“返回”即可回到无线管理首页。

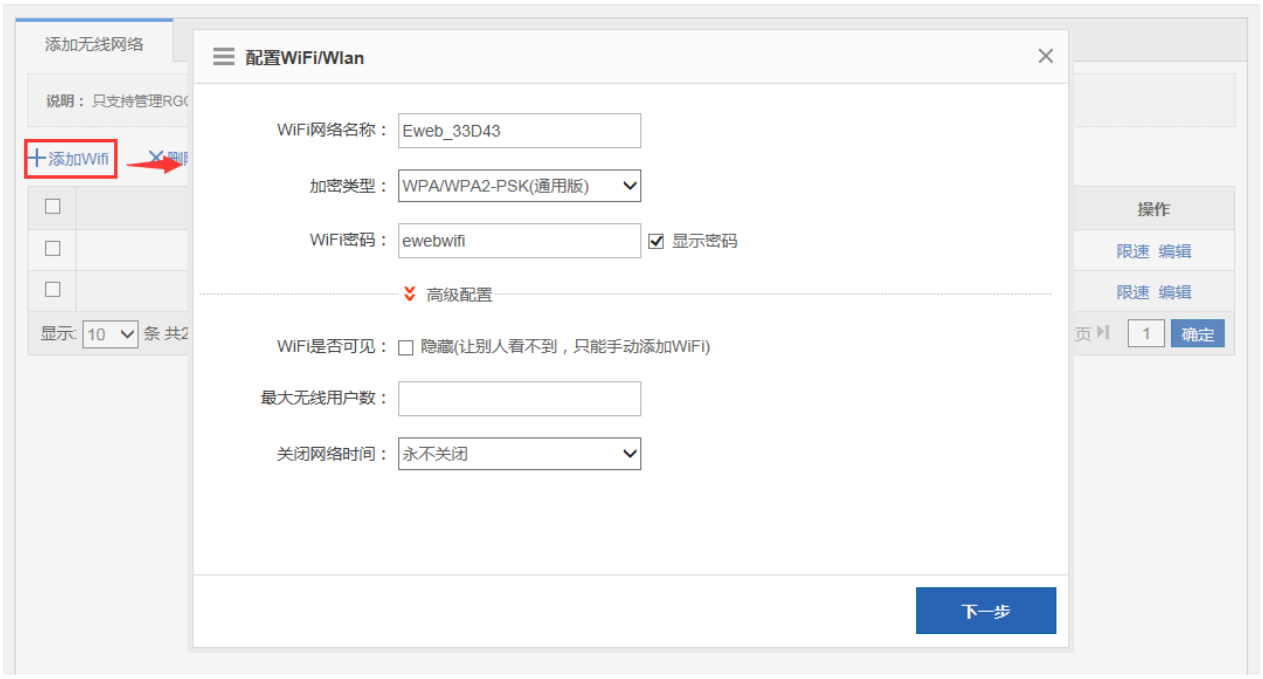


1.3.12.2 添加无线网络

无线网络是为了让无线终端用户能够通过 wifi 接入 AP 进行上网。可以添加多个无线网络，最多配置 4094 个。

- 添加 WIFI

点击<添加 wifi>，在弹出窗中配置相关的信息。



加密类型

WPA/WPA2-PSK（通用版）：基于共享密钥的 WPA 模式，安全性很高，设置比较简单，适合普通家庭用户和小型企业使用。

WPA/WPA2-802.1x（专业版）：采用 Radius 服务器进行身份认证并得到密钥的 WPA 或 WPA2 安全模式。由于要架设一台专用的认证服务器，代价比较昂贵且维护也很复杂，所以不推荐普通用户使用此安全类型。

网络类型切换

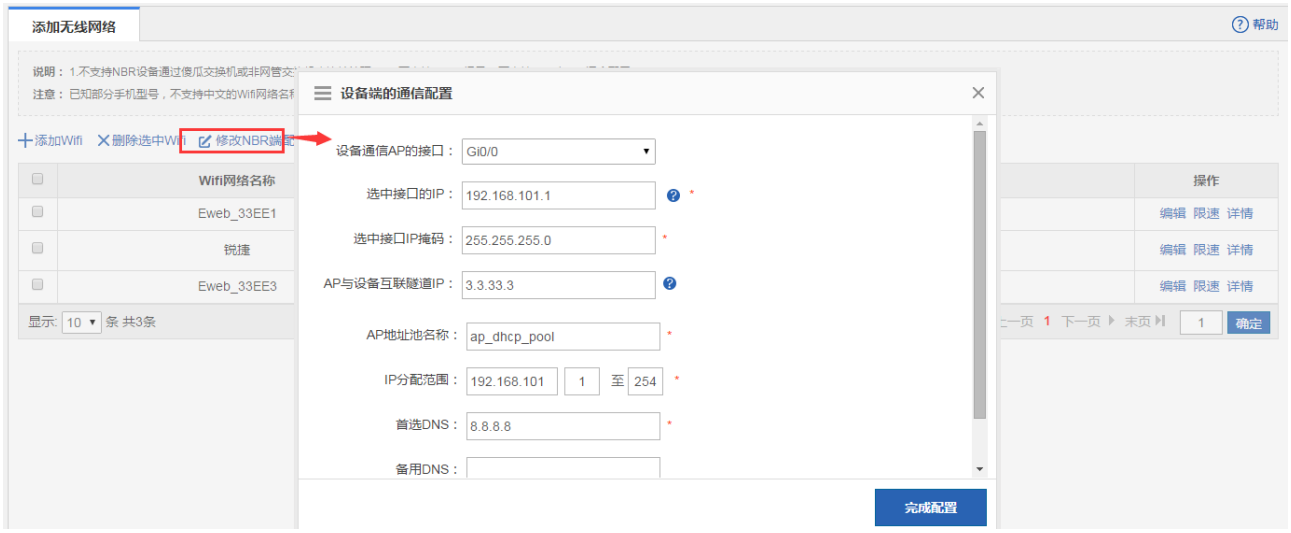
分为 2.4G,2.5G 网络都支持、仅支持 2.4G 网络、仅支持 5G 网络。旧版本升级上来默认为 2.4G,2.5G 网络都支持。

- 删除 WIFI：

在列表中选中一条或多条记录，点击<删除选中 WIFI>，在弹出的确认窗口中点击<确认>完成删除操作。

- 修改 NBR 段配置：

点击<修改 NBR 端配置>，在弹出窗中配置 NBR 端的通讯配置。



AP 与 NBR 互联隧道 IP

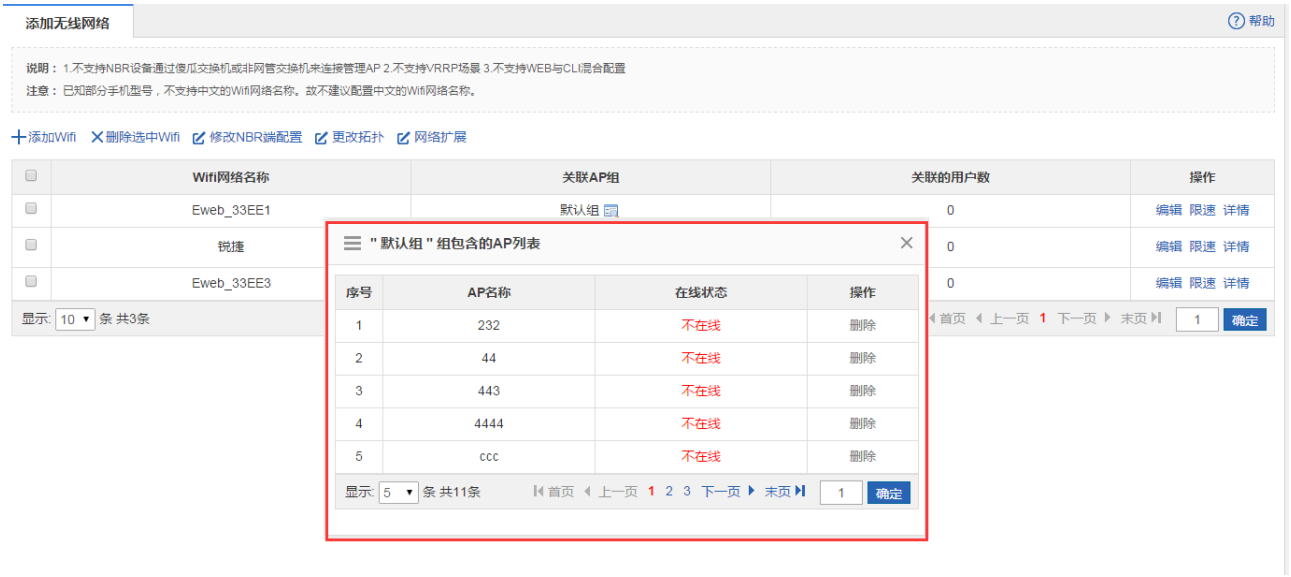
隧道 IP 也即回环口(loopback)地址，这个地址可以配置任意值，这个是建立 NBR 与 AP 互联隧道的标识地址，配置该地址的用途是让 NBR 更好的管理 AP。

- 更改拓扑图：

  点击<更改拓扑图>，在弹出窗中选中拓扑，点击确定修改拓扑图后会删除所有关于 WIFI 的配置。

- 查看关联 AP 组

点击“关联 AP 组”的 图标，可查看和删除该 AP 组下属的 AP。

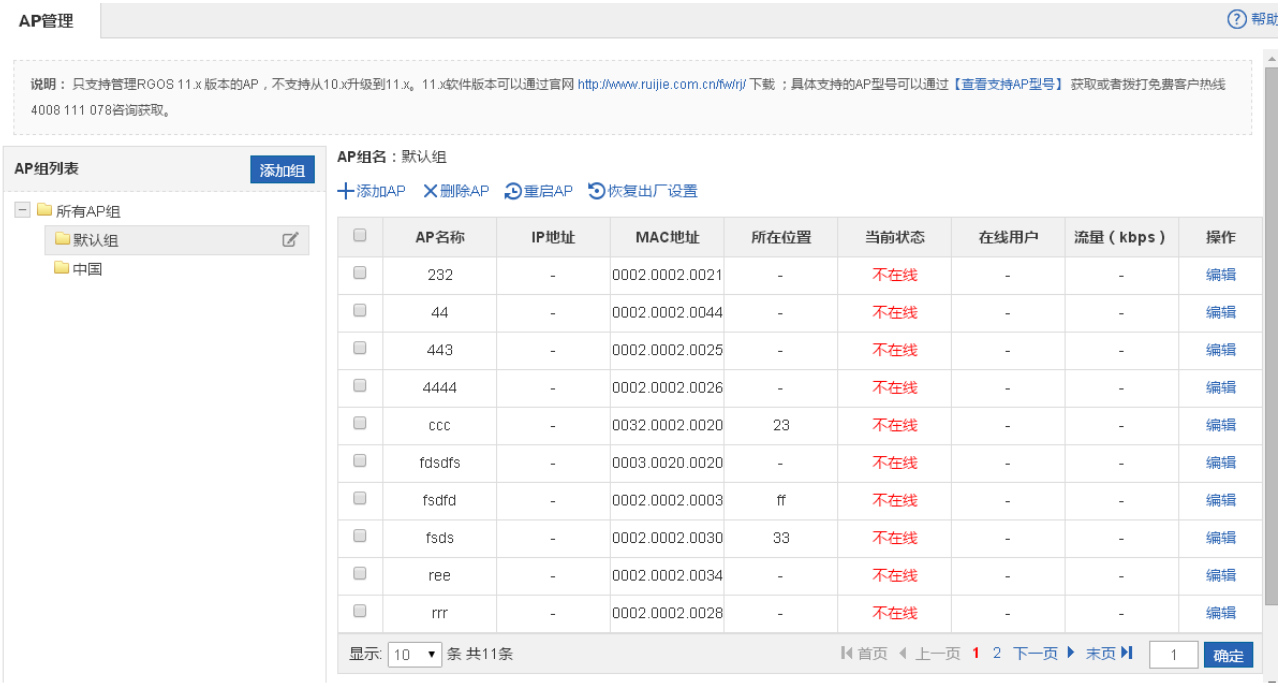


- 限速：

点击“操作”列中的<限速>链接，弹窗页配置无线网络限速值，点击<保存>提示“设置成功”即可。

1.3.12.3 AP 管理

AP在WLAN 网络中要能为无线用户提供服务，必需与某个AC建立连接，并且需要加入一个AP组。所有新加入的AP都属于默认AP组：default。



- AP 组

在左边 AP 组列表中，可以添加、编辑和删除 AP 组。

- 添加 AP

点击左边列表中的<添加 AP>，在弹出窗中填写配置项，点击<完成配置>。

- 删除 AP

在列表中选择一条或多条记录，点击<删除 AP>，在弹出的确认窗口中点击<确认>完成删除操作。

- 重启 AP

在“AP 列表”中选择一条或多条记录，点击<重启 AP>链接，批量重启 AP，弹出确认窗口，点击<确定>按钮，完成重启操作。

- 恢复出厂设置

在“AP 列表”中选择一条或多条记录，点击<重启 AP>链接，批量恢复 AP 设置，弹出确认窗口，点击<确定>按钮，完成恢复出厂设置操作。

- 支持的 ap 型号列表

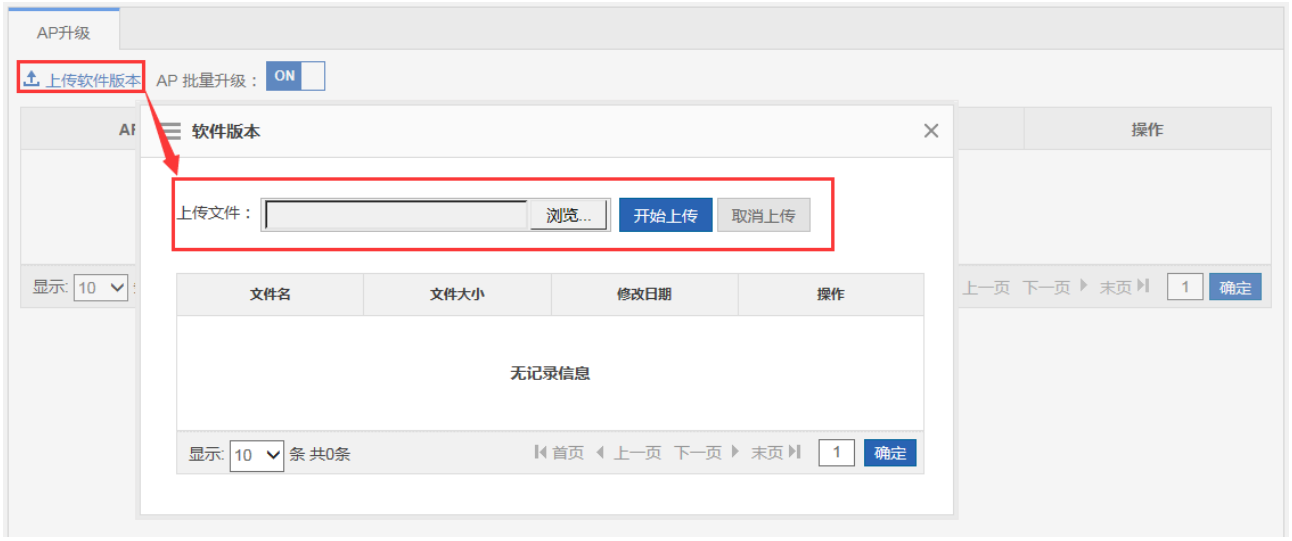
1.3.12.4 AP 升级

- 单个 AP 升级

选定列表中需要升级的 AP，点击 升级 ，在弹出窗中上传软件版本，点击 开始升级 ，完成单个 AP 的升级配置。

- 批量 AP 升级

点击 AP 批量升级： ON 开启 AP 批量升级，然后点击 上传软件版本 ，在弹出窗中上传软件版本，点击 开始上传 ，可以同时升级多台 AP 设备，方便快捷。



1.3.12.5 DHCP 安全

开启该功能，将只允许信任端口的 DHCP 响应，避免非法架设 DHCP Server，扰乱 IP 地址的分配和管理，影响用户的正常上网的行为；同时还可以有效防范 DHCP 动态分配 IP 环境下的 ARP 主机欺骗和源 IP 地址的欺骗。

1.3.12.6 反制非法 AP

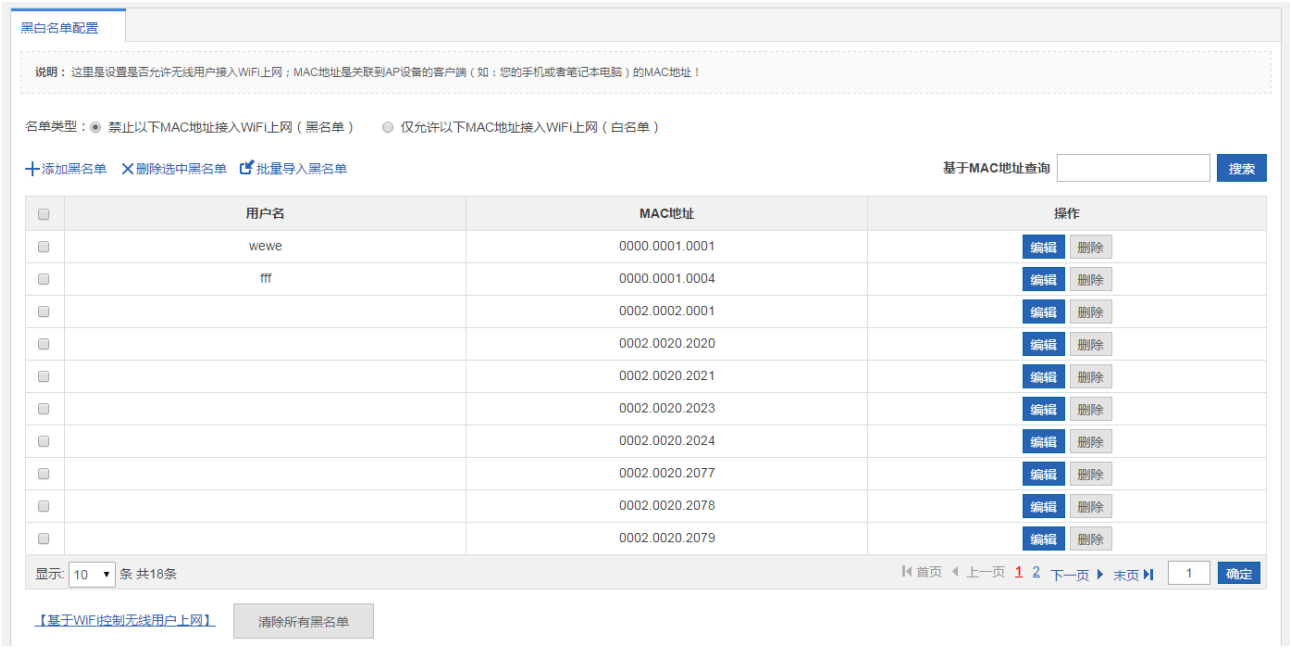
说明：主动发现网络中未经授权或存在恶意的 AP(如：私自接入的非法 AP,未经配置的 AP,攻击者控制的 AP,非法的桥接或未经授权的 Ad-hoc 设备)对这些非法设备进行反制，避免用户接入到非法 AP！配置界面如下：

查看被反制的非法 AP 列表，

添加信任设备列表

1.3.12.7 黑白名单

说明： 这里是设置是否允许无线用户接入 WiFi 上网；MAC 地址是关联到 AP 设备的客户端（如：您的手机或者笔记本电脑）的 MAC 地址！



1.3.12.8 禁止内网互访

说明： 在不影响用户正常上网的情况下对用户进行隔离，使之不能互访，保证了用户业务的安全。配置如下图。

1.3.12.9 WIS

接入 WIS 云，即可拥有一键诊断，一键网优和移动运维服务 。 web 可以支持一键开启关闭。

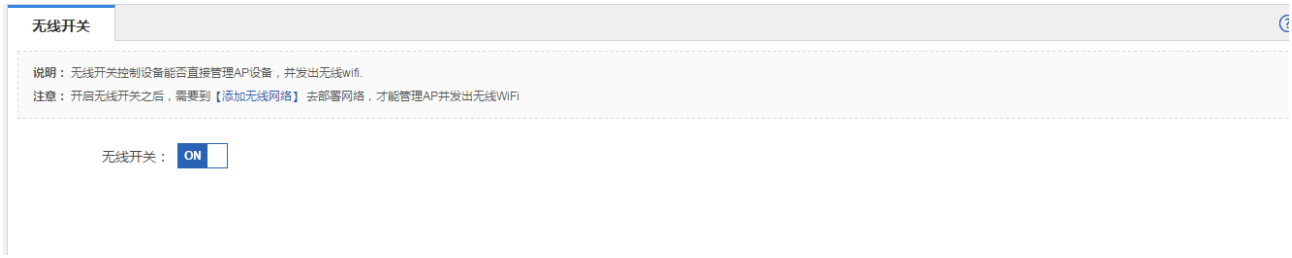
1.3.12.10 负载均衡

说明：在无线网络中，如果有多台 AP，并且信号相互覆盖。由于无线用户接入都是随机的，因此有可能会出现某台 AP 负载较重的、网络利用率较差的情况。通过将同一区域的 AP 都划到同一个负载均衡组，协同控制无线用户的接入，可以起到负载均衡的作用。 配置如下图。

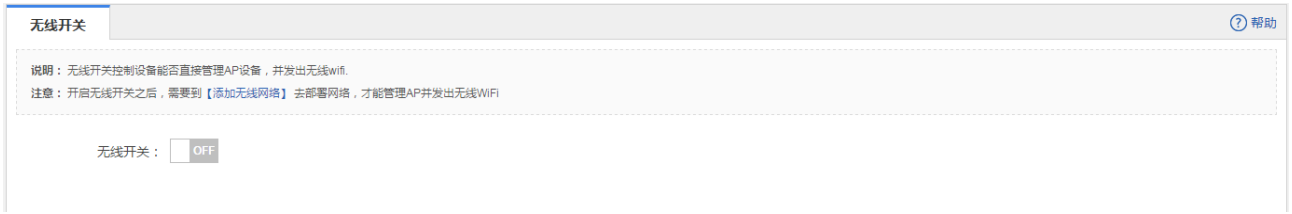
1.3.12.11 无线开关

说明： 无线开关控制 NBR 设备能否直接管理 AP 设备，并发出无线 wifi.

注意： 开启无线开关之后，需要到【添加无线网络】 去部署网络，才能管理 AP 并发出无线 WiFi



只有开启无线开关的时候才可以管理无线的菜单，而关闭的时候是不显示无线相关的菜单选项的如下图：



1.3.13 防火墙

1.3.13.1 防攻击配置

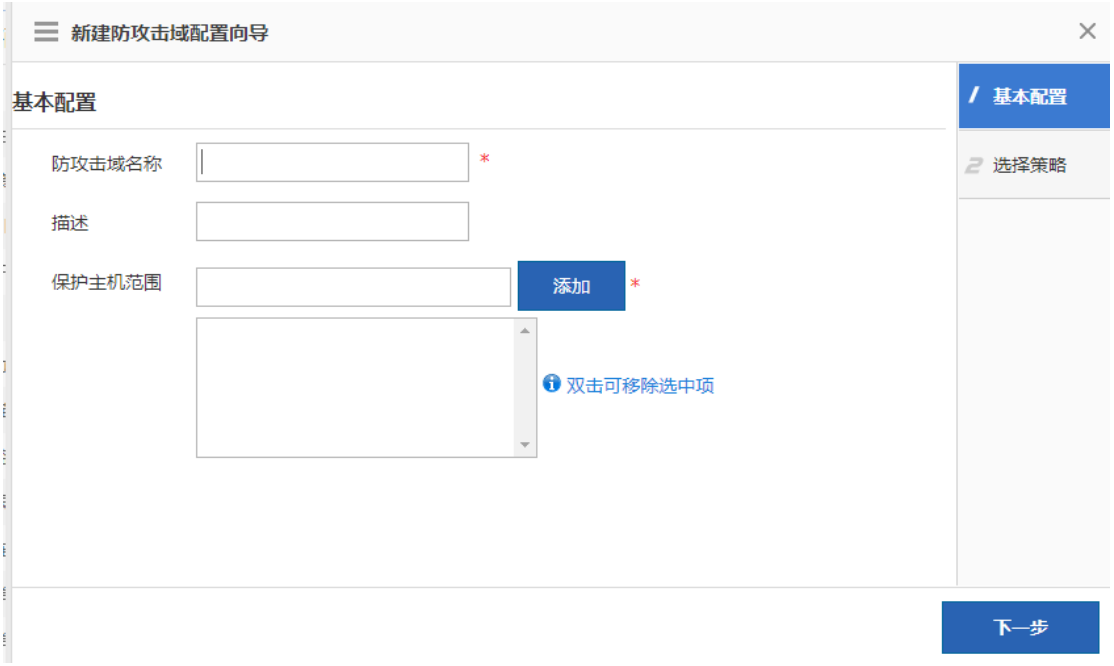
1.3.13.1.1防攻击开关

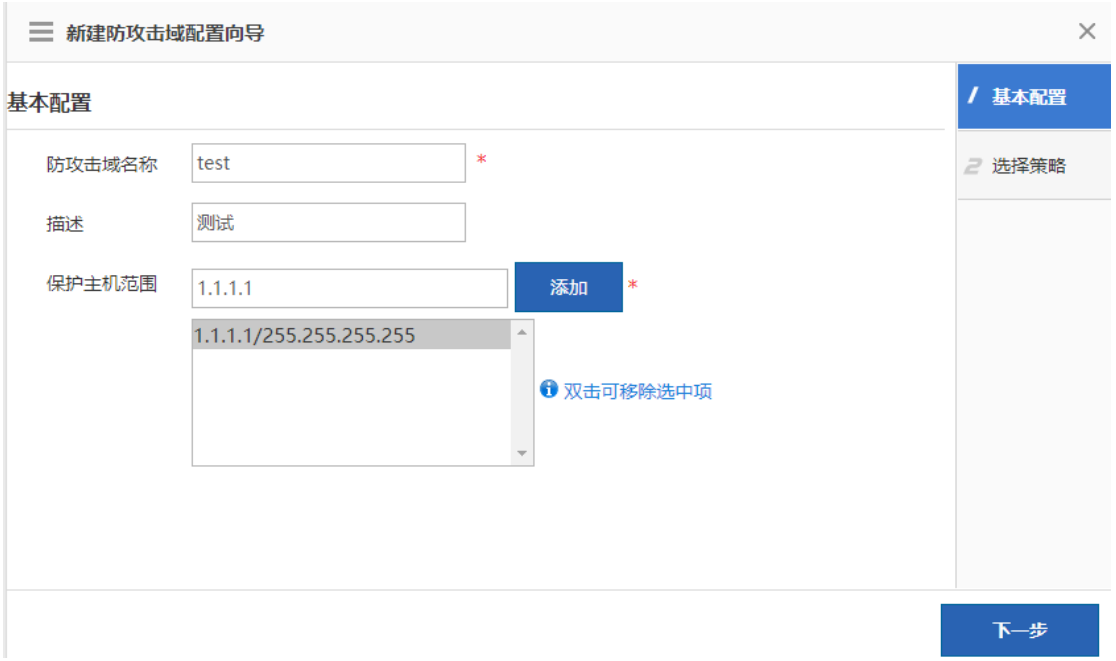
1.3.13.1.2全局防护

1.3.13.1.3协议类策略

1.3.13.1.4域策略

点击 新建域





点击下一步

点击完成配置


防攻击开关
全局防护
协议类策略
域策略
说明：每个防攻击域运行各自独立的域策略。这些策略包括：防洪水攻击，防扫描，流量限制，流量监控，流
防攻击域列表
新建域
删除选中域
859
aaa
test
域策略配置
描述
测试
保护主机范围
1.1.1.1
防护策略自学习
域运行故障（原因：ace co
TCP Flood 防护
未配置
UDP Flood 防护
未配置


防攻击域列表
域策略配置
点击配置可以进行相关参数配置

点击 
删除选中域
，可以删除选中的域

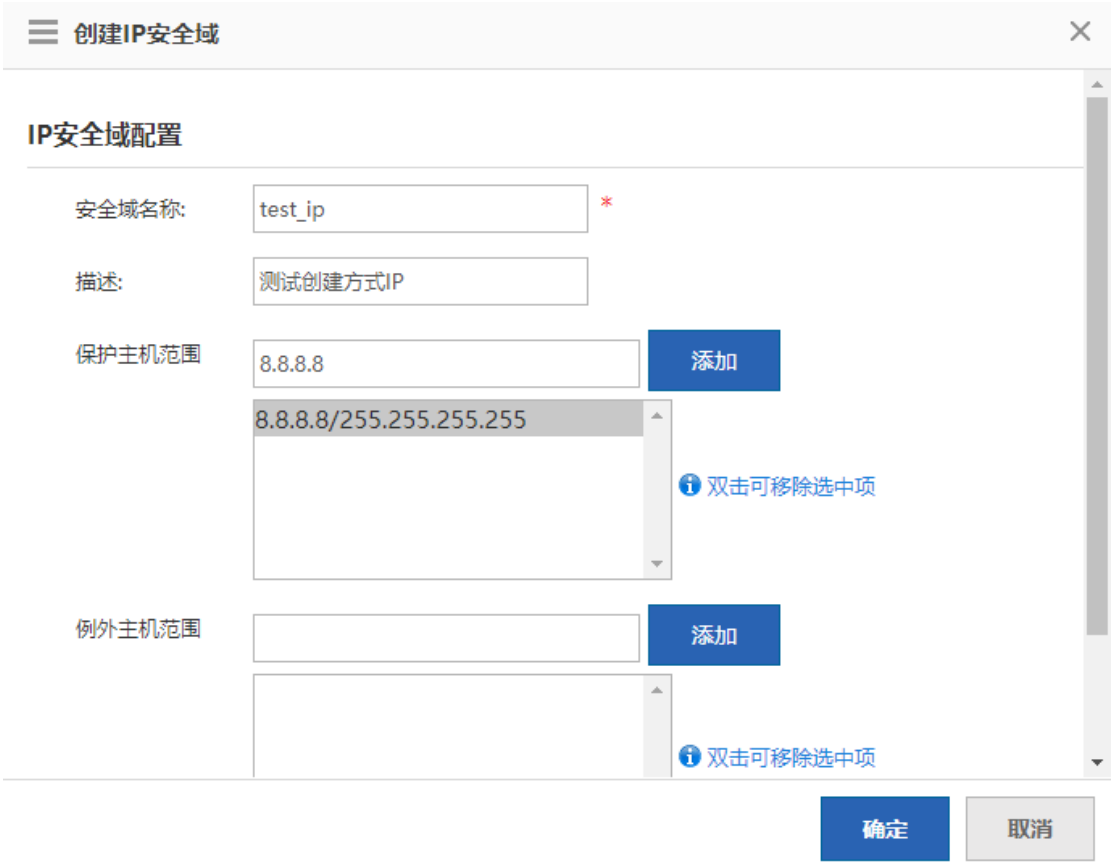
1.3.13.2 安全域配置

1.3.13.2.1安全域开关

1.3.13.2.2安全域

基于 IP 创建方式

点击 



可以进行编辑、删除操作

点击 切换创建方式


切换安全域创建方式
请选择安全域建创方式
IP地址
接口
确定
取消

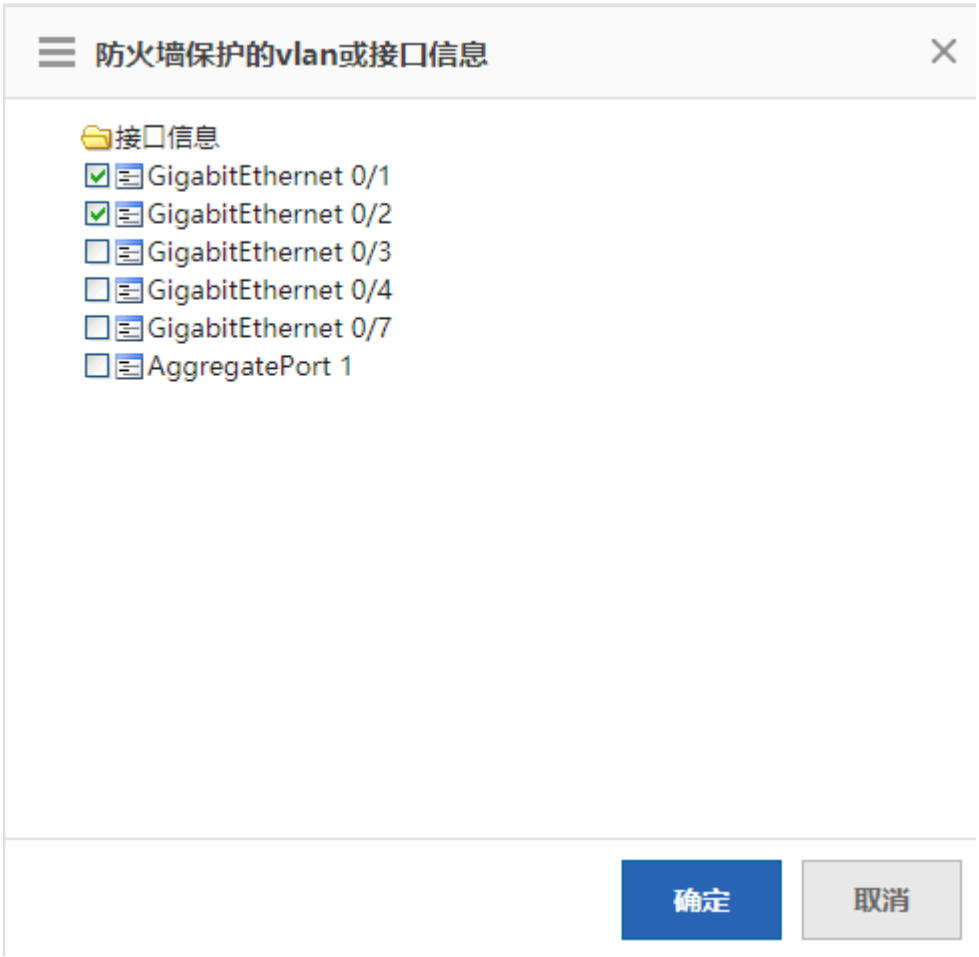
基于接口创建方式


安全域开关
安全域
全局策略配置
域策略配置
安全域管理
当前安全域创建方式：接口
切换创建方式
安全域名称:
安全域等级:
查询...
刷新 提示:default 安全域不能删除
+添加
安全域名称
保护等级
保护VLAN范围
允许区间内互访?
描述
操作
default
GigabitEthernet 0/1,GigabitEthernet 0/2,GigabitEthernet 0/3,GigabitEthernet 0/4,GigabitEthernet 0/5,GigabitEthernet 0/6,GigabitEthernet 0/7,AggregatePort 1
否
编辑
显示: 10 条 共1条
首页 上一页 1 下一页 末页
1
确定

点击 
+添加


创建接口安全域
接口安全域配置
安全域名称:
test_接口
*
描述:
测试基于接口创建方式
配置接口:
请选择
双击可移除选中项
安全域等级:
(1-100)
确定
取消

点击 请选择


防火墙保护的vlan或接口信息
接口信息
GigabitEthernet 0/1
GigabitEthernet 0/2
GigabitEthernet 0/3
GigabitEthernet 0/4
GigabitEthernet 0/7
AggregatePort 1
确定
取消


创建接口安全域
接口安全域配置
安全域名称:
test_接口
描述:
测试基于接口创建方式
配置接口:
GigabitEthernet 0/1
GigabitEthernet 0/2
请选择
双击可移除选中项
安全域等级:
88
(1-100)
点击确定
确定
取消


安全域开关
安全域
全局策略配置
域策略配置
安全域管理
当前安全域创建方式：接口
切换创建方式
安全域名称:
安全域等级:
查询...
刷新 提示:default 安全域不能删除
添加
安全域名称
保护等级
保护VLAN范围
允许区间内互访?
描述
操作
default
GigabitEthernet 0/3,GigabitEthernet 0/4,GigabitEthernet 0/5,GigabitEthernet 0/6,GigabitEthernet 0/7,AggregatePort 1
否
编辑
test_接口
88
GigabitEthernet 0/1,GigabitEthernet 0/2
否
测试基于接口创建方式
编辑 删除
显示: 10 条 共2条
首页 上一页 1 下一页 末页
确定

可以进行编辑、删除操作

1.3.13.2.3全局配置策略

1.3.13.2.4域策略配置

基于 ACL 配置域间策略

点击 


创建安全域策略
策略基本配置
源安全域: default *
目的安全域: default *
描述: 测试：基于ACL (不能为以%&?+<|,\ " 等非法字符)
提示：序号默认不填,系统会自动生成
规则序列号: 111 (1到2147483647) 自定义序列号
提示：1、IP范围策略：通过指定IP范围和协议的简单策略； 2、ACL策略：通过引用acl来实现更复杂的控制策略。
配置策略方式 IP范围策略 引用ACL策略
策略基本配置
2 IP范围策略
下一步

点击下一步

点击完成配置

可对安全域策略修改、删除、激活/不激活、复制操作

基于对象配置域间策略

点击 添加

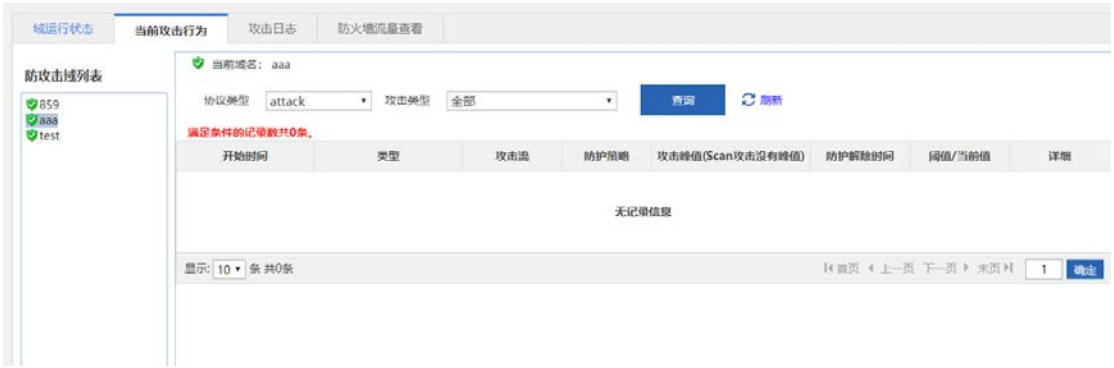
点击确定

可对域策略进行修改、复制、删除操作

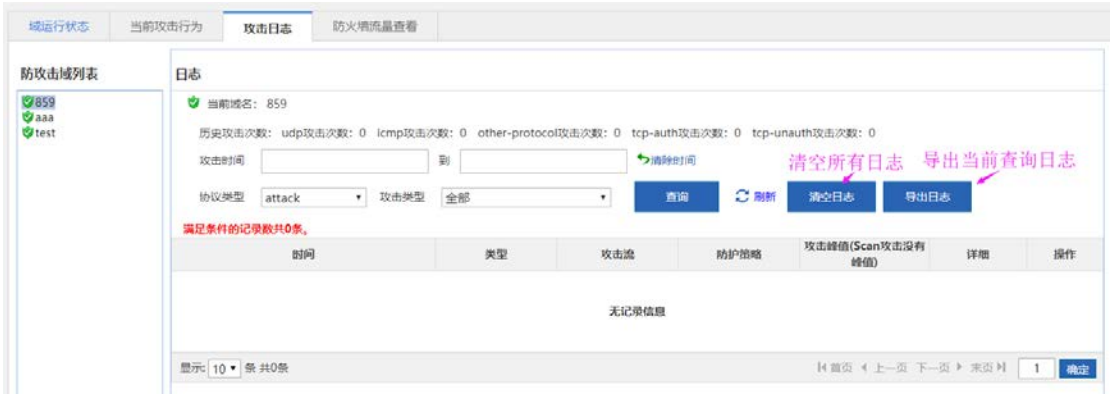
1.3.13.3 防攻击域状态监控

1.3.13.3.1域运行状态

1.3.13.3.2当前攻击行为



1.3.13.3.3攻击日志



1.3.13.3.4防火墙流量查看

1.3.13.4 安全域状态监控

1.3.13.4.1安全域运行日志

默认显示当天数据

点击 清空日志 可以清空所有日志

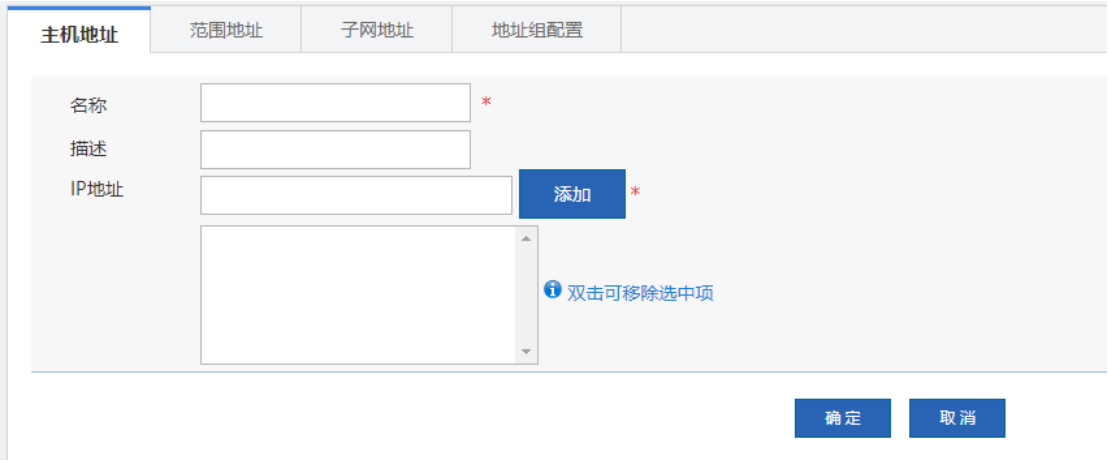
点击 导出数据 可以导出当前显示的数据

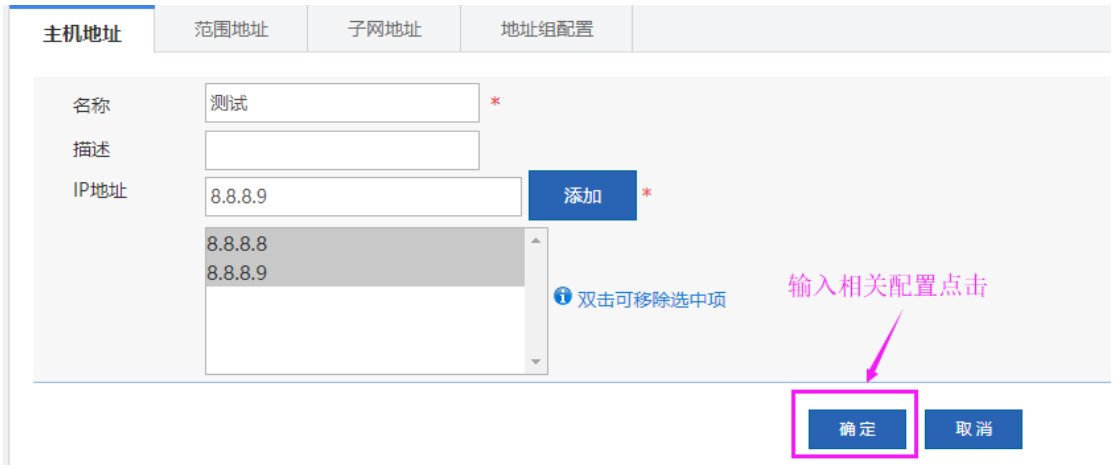
1.3.13.5 IP 资源

1.3.13.5.1主机地址

可进行添加、修改、删除、查询、刷新操作

点击 添加




主机地址
范围地址
子网地址
地址组配置
名称
测试
描述
IP地址
8.8.8.9
添加
8.8.8.8
8.8.8.9
双击可移除选中项
输入相关配置点击
确定
取消


主机地址
范围地址
子网地址
地址组配置
查询项:
名称
关键字:
查询
刷新
添加
删除所选
名称
IP地址
描述
状态
操作
kkkk
4.5.6.7
未使用
修改
删除
wqeqwe
5.8.8.8
测试
8.8.8.8,8.8.8.9
显示:
15
条 共3条
首页
上一页
下一页
末页
确定

点击修改


主机地址
范围地址
子网地址
地址组配置
名称
测试
描述
我修改了描述信息
IP地址
添加
8.8.8.8
8.8.8.9
双击可移除选中项
确定
取消


主机地址
范围地址
子网地址
地址组配置
查询项:
名称
关键字:
查询
刷新
添加
删除所选
名称
IP地址
描述
状态
操作
kkkk
4.5.6.7
未使用
修改
删除
wqeqwe
5.8.8.8
测试
8.8.8.8,8.8.8.9
我修改了描述信息
显示:
15
条 共3条
首页
上一页
下一页
末页
确定

点击删除

1.3.13.5.2范围地址

可进行添加、修改、删除、查询、刷新操作，操作方法与主机地址类似

1.3.13.5.3子网地址

可进行添加、修改、删除、查询、刷新操作，操作方法与主机地址类似

1.3.13.5.4地址组配置

可进行添加、修改、删除、查询、刷新操作，操作方法与主机地址类似

1.3.13.6 服务资源配置

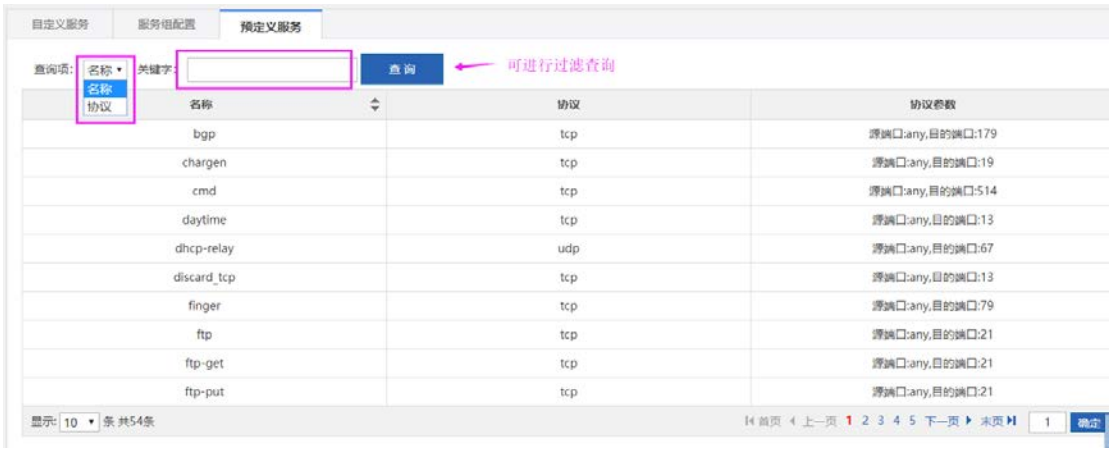
1.3.13.6.1自定义服务

可进行添加、修改、删除、查询、刷新操作，操作方法与主机地址类似

1.3.13.6.2服务组配置

可进行添加、修改、删除、查询、刷新操作，操作方法与主机地址类似

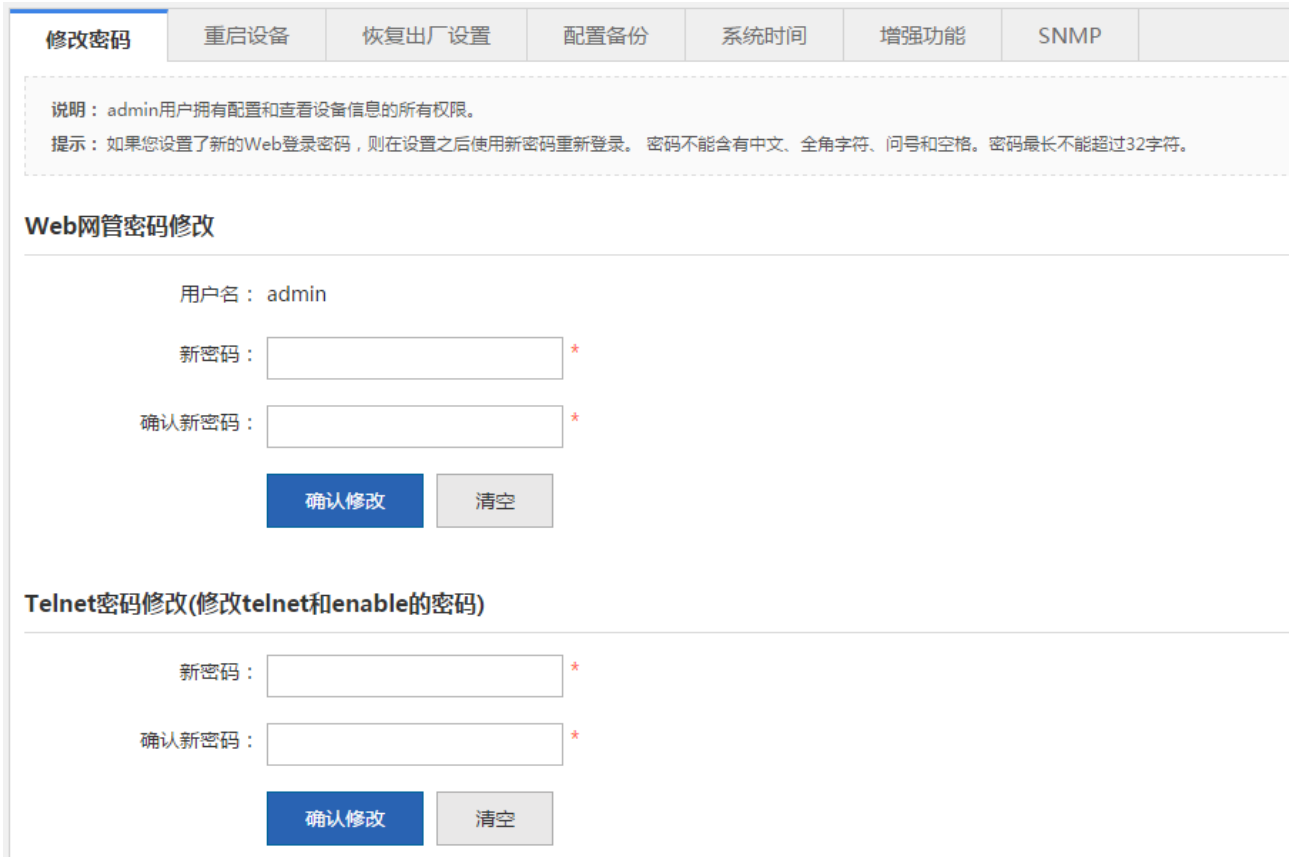
1.3.13.6.3预定义服务



1.3.14 高级

1.3.14.1 系统设置

1.3.14.1.1修改密码



Web 配置密码：当使用 WEB 界面配置设备时，必需使用该密码登录。 这个页面只有超级管理才能配置，也就是只有 admin 用户可见！这里可以修改 admin 管理员的管理密码！

Telnet 配置密码：用 Telnet 配置设备时，必需使用该密码登录。

注意：修改后的密码请务必牢记，以免下次登录时无法进入。

1.3.14.1.2重启设备

点击“立即重启设备”将使设备重新启动。重新启动需要 1 分钟左右的时间，该期间不要做其它任何操作。当设备重启成功后将自动刷新当前页面。

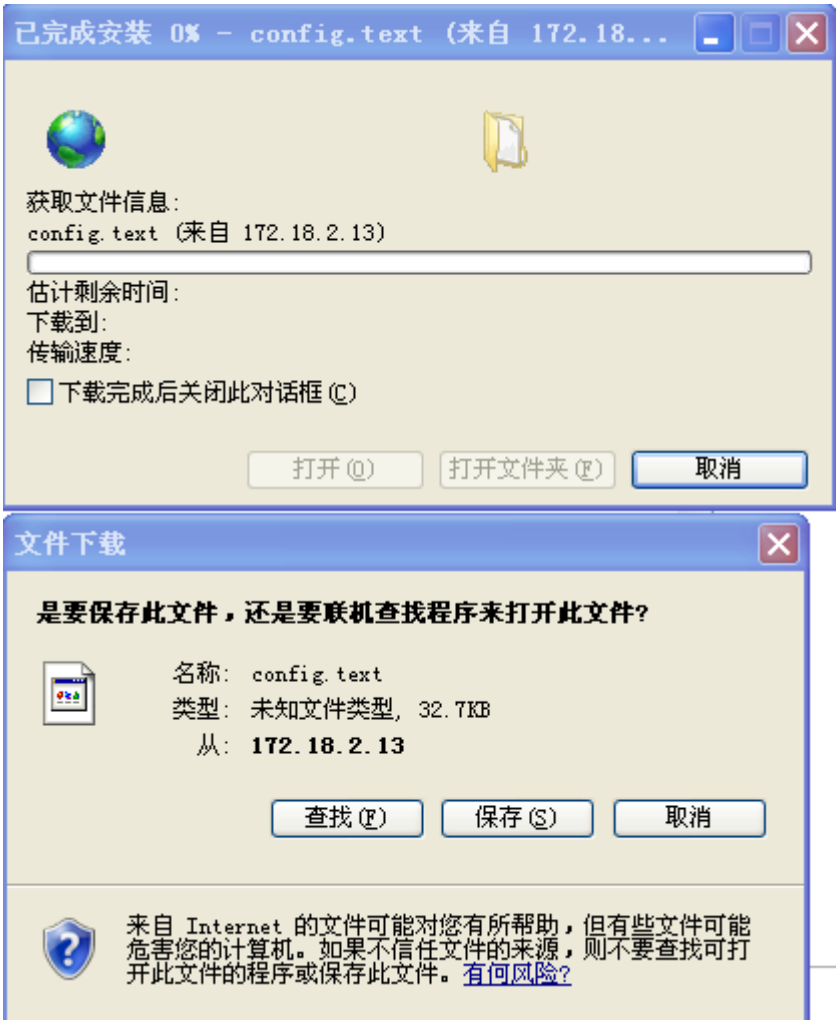
1.3.14.1.3恢复出厂设置

“恢复出厂设置”功能会删除当前设备的所有配置，设备将恢复到出厂时的默认配置状态。如需保留现有配置，建议先通过“配置备份”导出当前配置。

1.3.14.1.4配置备份

配置导出：该功能可以将设备的当前配置导出到本地电脑进行备份。

点击“导出当前配置”按钮，系统会弹出文件保存对话框，然后选择文件的保存位置即可。



配置备份：将本地电脑上的配置备份文件上传到设备上进行还原。

点击“浏览”，然后选择本地电脑上的备份文件（文件名必需是“config.text”）。选择完毕后，点击“导入配置”进行导入。

要使导入的配置生效，请重新启设备。若发现导入的配置有问题，在没有重启生效之前，可以通过点击“取消导入”按钮来进行恢复。

配置查看：点击“查看详细配置内容”可以查看当前设备的所有配置命令。

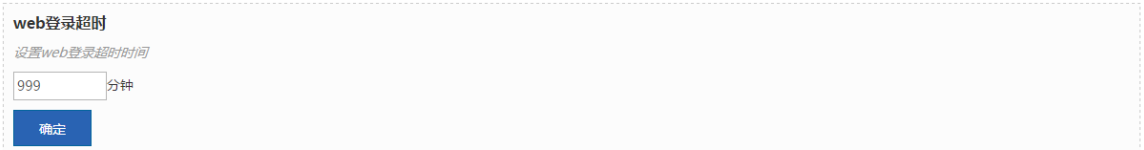
1.3.14.1.5系统时间

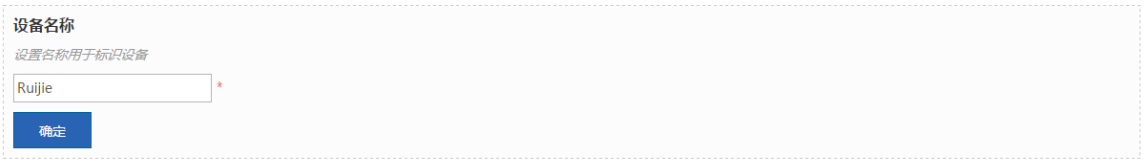
系统日期和时间：通过该功能可以设置设备的当前时间。

您也可以开启“自动与 Internet 时间服务器同步”时间，也就是设备的时间会始终保持跟互联网上的时间一致；不过这个功能依赖于是否配置了正确的 DNS 服务，如果您还未配置 DNS 服务器，请到“**网络配置》DNS 配置**”界面配置 DNS 服务器。

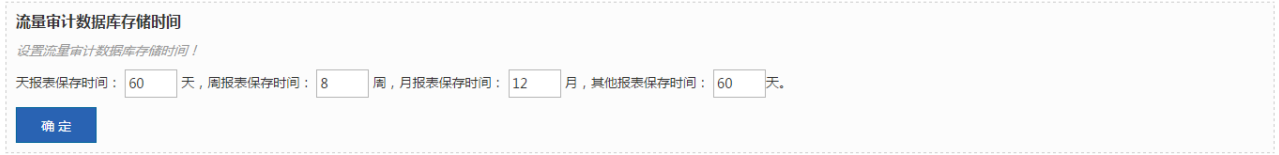
1.3.14.1.6增强功能


流量审计实时数据生成频率
通过这里设置可以提高设备实时生成流量数据的频率，最高可以设置每隔10秒生成一次流量数据！
设置生成频率为：30秒
确定


web登录超时
设置web登录超时时间
999
分钟
确定


设备名称
设置名称用于标识设备
Ruijie
*
确定


流量审计实时数据生成频率
通过这里设置可以提高设备实时生成流量数据的频率，最高可以设置每隔10秒生成一次流量数据！
设置生成频率为：30秒
确定


流量审计数据库存储时间
设置流量审计数据库存储时间！
天报表保存时间：60 天，周报表保存时间：8 周，月报表保存时间：12 月，其他报表保存时间：60 天。
确 定

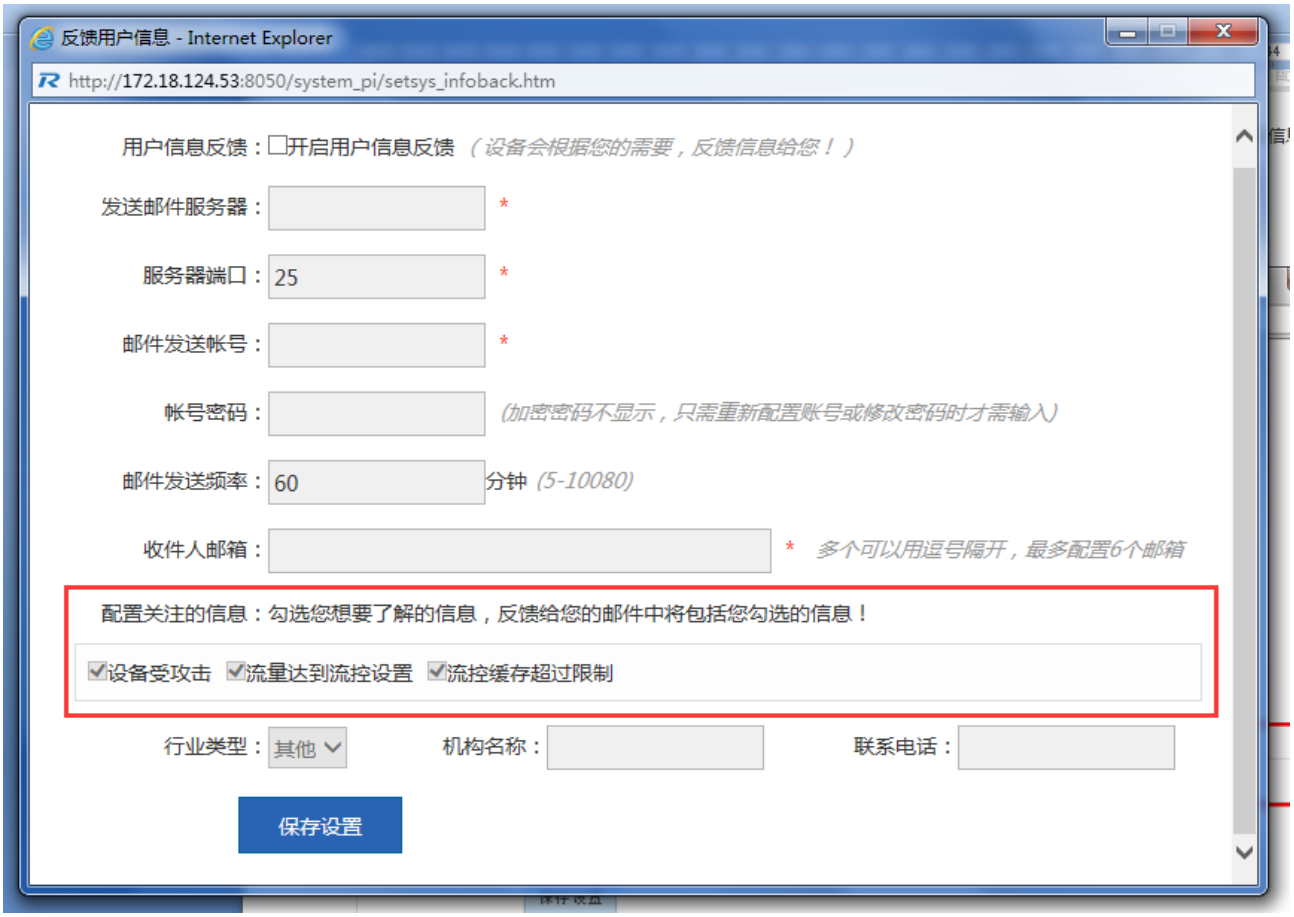

内容审计数据库存储时间
设置内容审计数据库存储时间！
内容审计数据保存时间：60 天
确 定


严格应用选路配置
开启严格的应用选路后，应用路由功能将会更优越！
开启严格的应用选路
确定

这个功能主要是设备的一些增强型的功能。

反馈用户信息：该功能是用来配置您想让设备将一些警告信息通过邮件的方式及时的通知到您，并提醒处理这些告警信息，以保证设备的正常稳定。点击 

按钮会弹出如下窗口。



开启用户信息反馈：您要配置该功能前需要先勾选 

发送邮件服务器：是指您用来做主发送邮箱的服务器，例如您有一个 163 的邮箱是 serv@163.com，您想将这个邮箱作为主发送邮箱，那么这里要填写的服务器就是(POP3 服务器：pop.163.com | SMTP 服务器：smtp.163.com | IMAP 服务器：imap.163.com)您可以根据您的需要在这三个任意选择一个！

服务器端口：这里填写的您主发送邮箱服务器的端口，如果没有特殊，采用缺省就可以了，除非您的服务器有特别的说明。

邮件发送帐号：这里填写的主发送邮件帐号，如第二点举例的 serv@163.com。

帐号密码：这里输入主发送邮箱的密码，也就是 serv@163.com 的密码。

邮件发送平率：这个是设置设备告警信息发送到您指定邮箱的平率，缺省情况下是每 60 分支发送一次通知，如：设备存在内存不足的告警，那么设备会每 1 个小时就会给您发送一份告警邮件。

收件人邮箱：这个是设置您自己通常使用的工作邮箱或经常打开的邮箱，主要是为了接受设备发送过来的告警信息的邮箱。

配置关注的信息：这里有列出了系统当前支持的所有告警信息，你可以根据你的需要选择；选择后如果设备有出现告警那么就会将告警信息发送到您指定的收件人邮箱；

行业类型、机构名称、联系电话：这个三个是填写您自身信息的，官方建议您如实填写，以方便我们为您提供更好的服务。

网站访问被阻断后的反馈信息 配置：

这里是配置阻断网站后反馈给用户的信息，例如：您在 “行为管理》禁止网站”页面禁止了“www.xxx.com”网站，员工（或内网用户）访问了这个网站会看到提示信息，就是您在这里配置的信息！我们缺省的提示信息为“你被禁止访问这个网站，请联系网站管理员！”效果如下图

以及其他一些不常用的功能配置。

1.3.14.1.7SNMP

SMNP 配置：

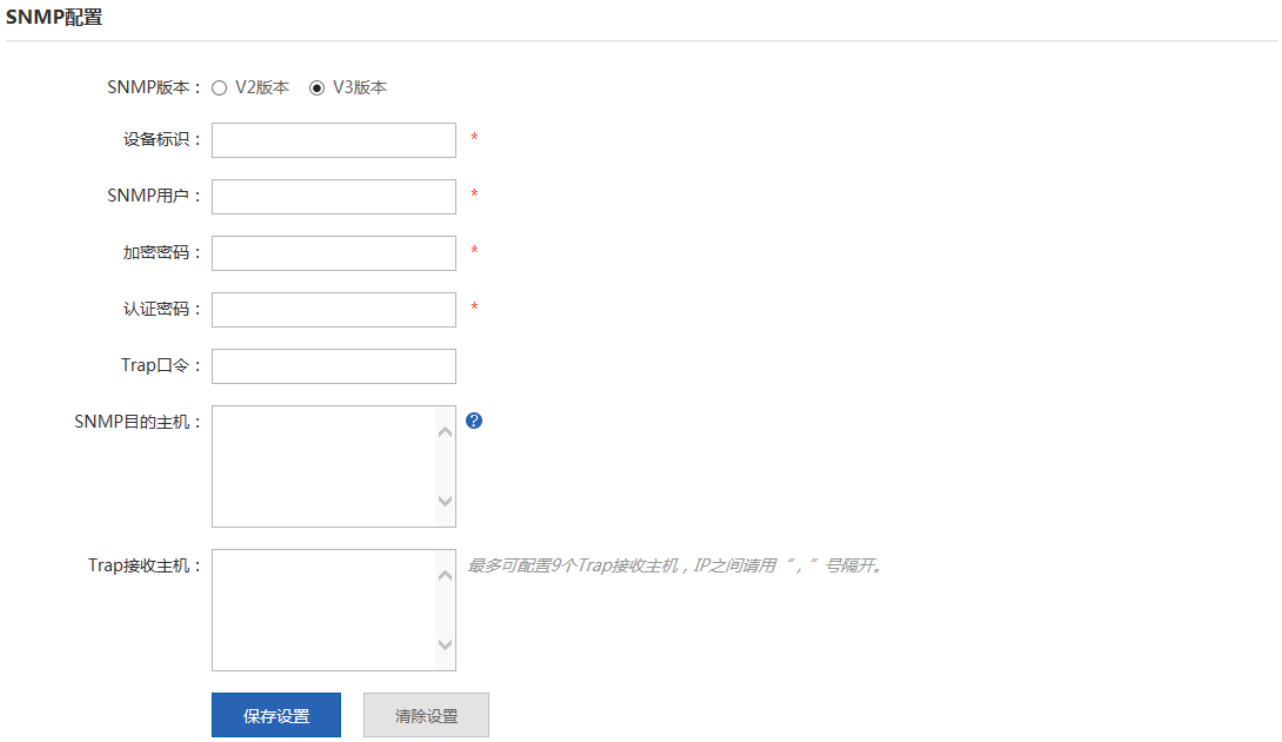
简单网络管理协议，配置 SNMP 管理员可轻松进行对网络上的节点进行监控和管理。

1. SMNP 版本：目前设备支持 V2 和 V3 版本；上图是配置 V2 版本的示意。
2. 设备标识：这里是为了标识您 SMNP 服务的名称；
3. SNMP 口令：管理主机可以通过该口令连接当前设备。

4. Trap 口令：连接管理主机的口令。设备发生告警，也会主动向管理主机发送告警信息。

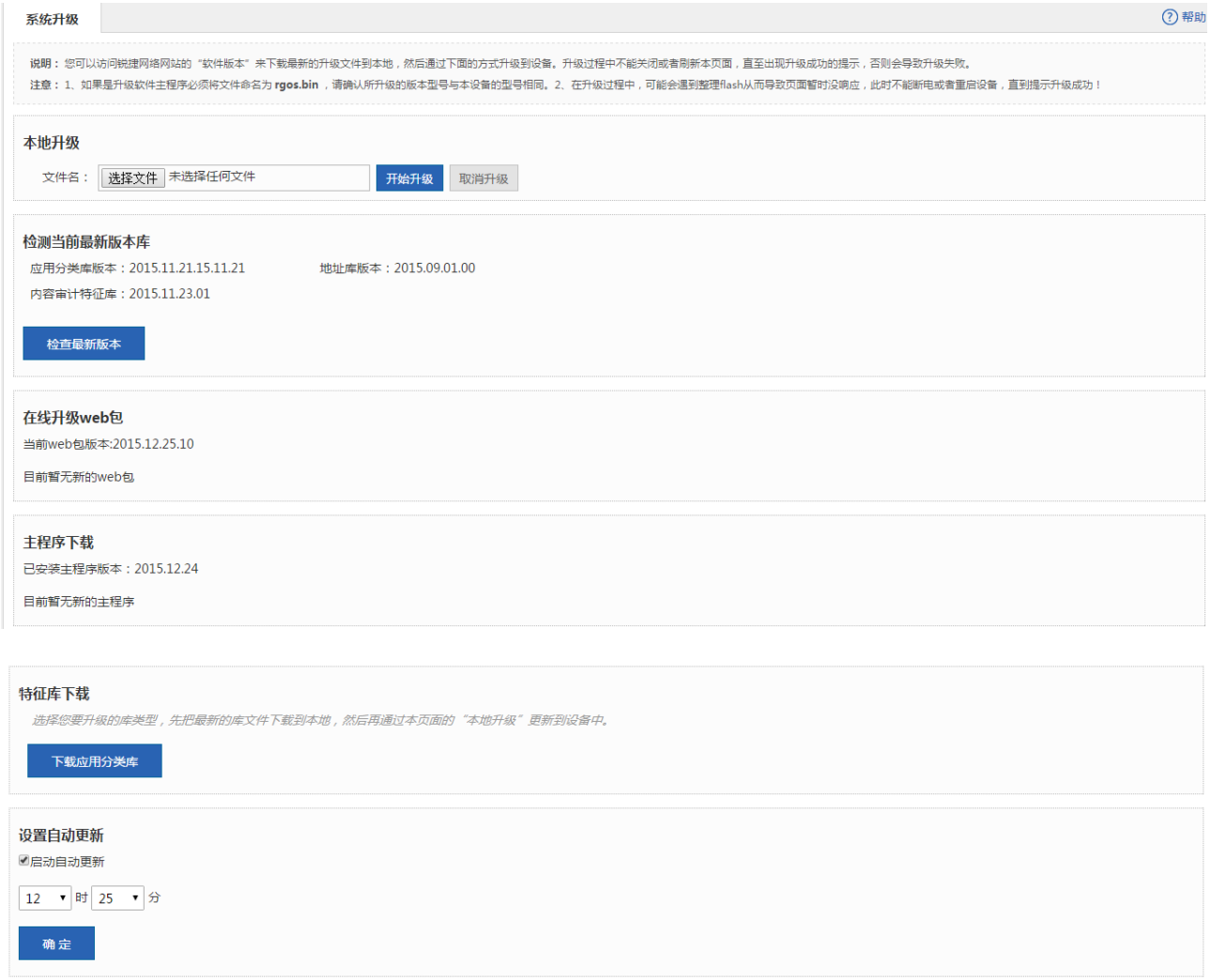
5. Trap 接收主机：要接收设备告警信息的管理主机列表。最多可以配置 10 台主机。

配置 V3 版本的示意图：



V3 版本提高了安全性设置，这里要求添加 SMNP 用户的 加密密码和认证密码。

1.3.14.2 系统升级



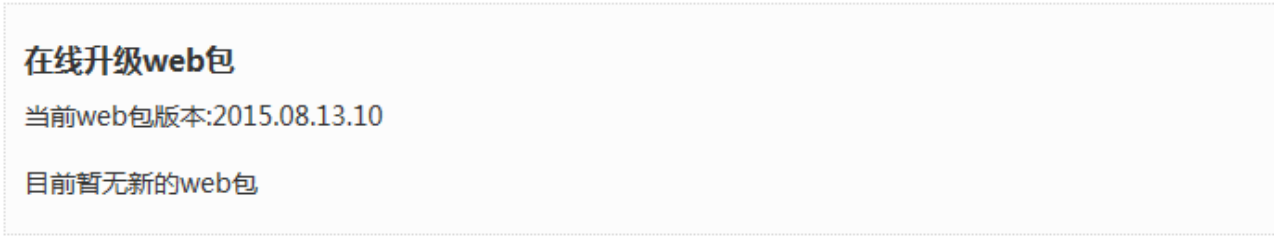
您可以访问锐捷网络官方网站的"软件版本"来下载最新的升级文件到本地，然后通过该页面升级到设备。升级过程中不能关闭或者刷新本页面，直至出现升级成功的提示，否则会导致升级失败。升级过程大概需要花您 50 秒左右的时间！

如果是升级软件主程序必须将文件命名为”rgos.bin”□ □

本地升级：点击“浏览”按钮，选择你下载到本地电脑上的升级包文件。然后点击“开始升级”，界面会出现“正在升级”的进度条，此时请耐心等待，不能进行任何操作。大约等待 50 秒左右设备会提示升级成功，您点击确定即可。

主程序下载：如果有新版本会提示更新，点击确认升级按钮即可完成升级。

在线升级 web 包：如果有新版本会提示更新，点击确认升级按钮即可完成升级。

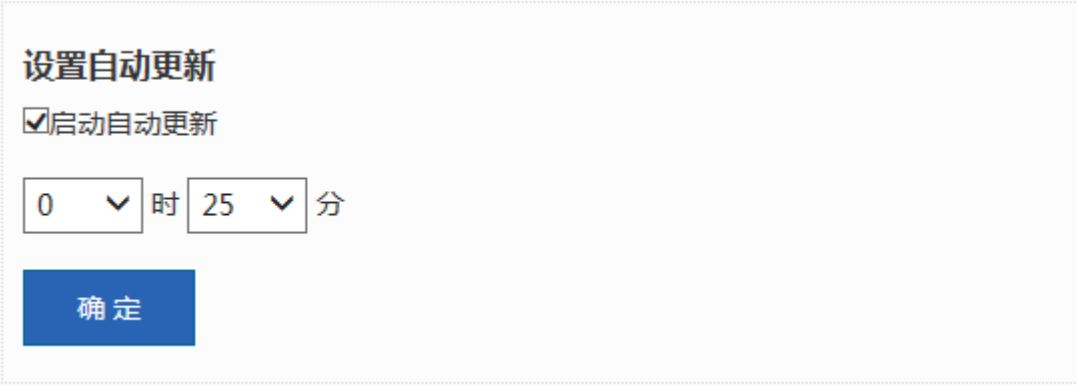


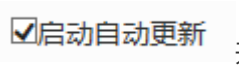
检测当前最新版本：显示当前设备的版本信息。点击“检查最新版本”按钮将自动检测当前发布的最新版本。如果当前设备不是最新版本则会出现“立即更新”按钮，点击该按钮将自动下载“协议特征库”和“URL 数据库”文件到设备进行升级。

版本库下载：您可以通过这里下载到最新的 URL 库或应用特征库版本。

点击 下载URL库 或 下载应用分类库 ，系统会弹出下载窗口，选择一个下载地址，先把最新的库下载到本地，然后通过本页面的“本地升级”更新到设备中。下载窗口如下图所示：

设置自动更新：该功能可以设置设备按指定的时间，对指定的文件进行检测版本并自动更新。



选中  开启自动更新功能。

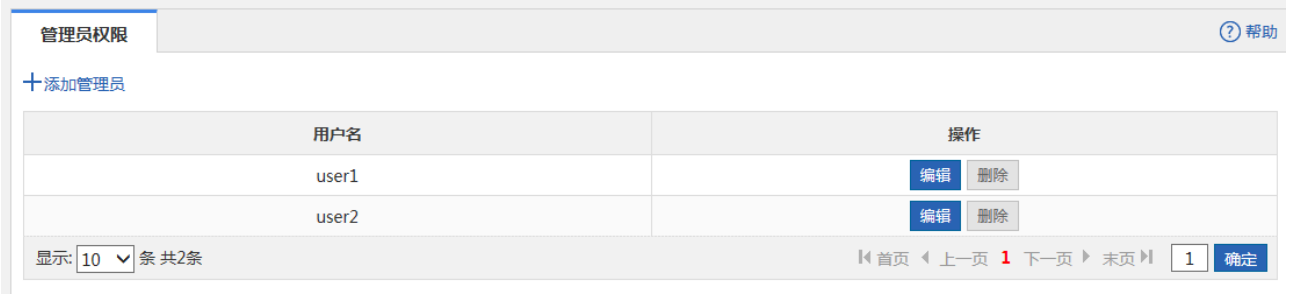
选择设备自动更新的时间，系统将在每天的这个时间检测最新版本。

选择需要自定升级的文件，系统将只对选中的文件自动更新。

配置完毕后，点击  。

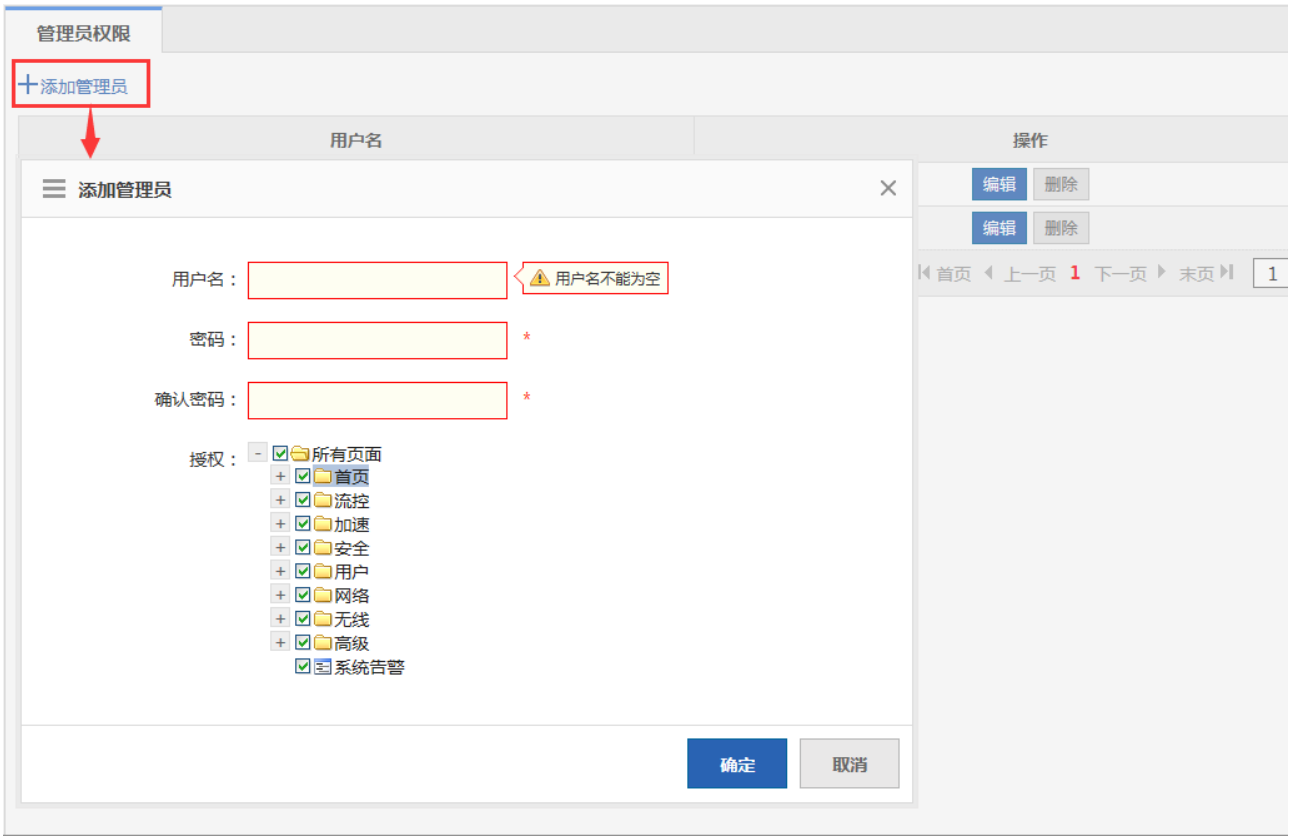
注：自动更新依赖于设备是否配置了可用的 DNS 服务器，您可以到 **网络配置 》DNS 配置**。

1.3.14.3 管理员权限



管理员权限 本页面添加的设备管理员 新增的管理员可以登录Web管理系统对设备进行日常维护或管理 ,但无法通过Telnet执行命令；保留用户 manager 和 guest 不能删除。为了安全起见该功能页面有且只有 admin 用户可以查看并编辑！

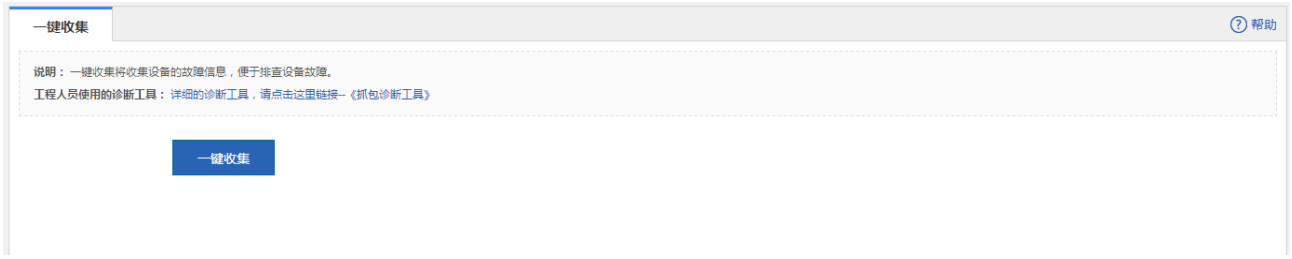
点击“添加管理员”，可以添加新的管理员账户信息，注意用户名，密码及确认密码不能为空。



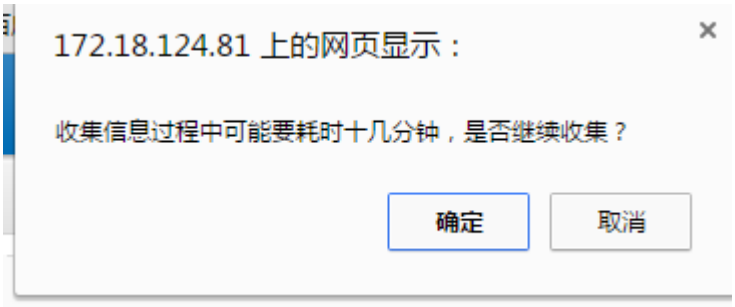
用户名：这里可以任意输入您想要的管理员名称，推荐使用英文避免使用中文；例如：zhangs;
登录密码：是管理员登录设备 web 网管的密码；
授权页面：您可以对该管理员指派管理功能的权限；

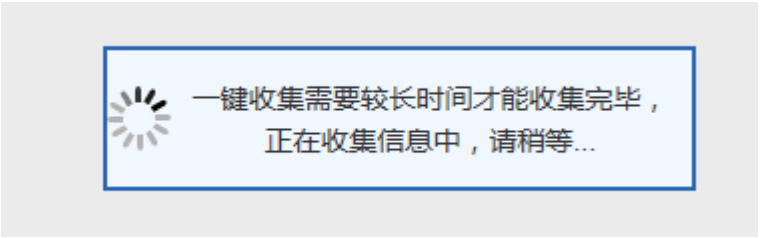
1.3.14.4 一键收集

一键收集将收集设备的故障信息，便于排查设备故障。



点击确定后，会有等待的时间





执行完后，点击 下载 会生成一个包，如 tech_vsd0_20150727172504.tar.gz，便于工程师分析故障。

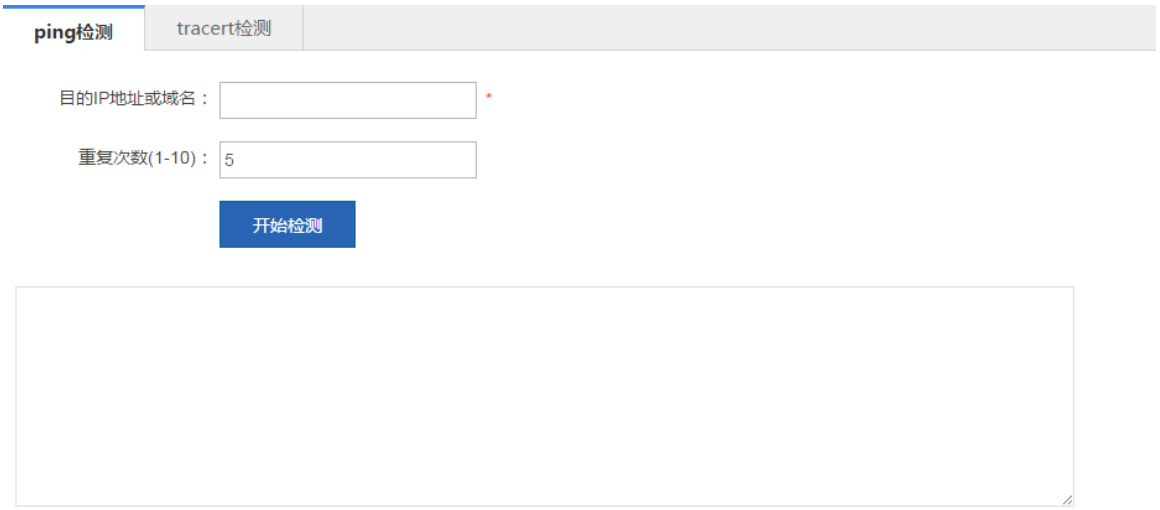
1.3.14.5 抓包工具

抓包诊断工具：设备抓包功能详细请点击链接。收集抓包如下图，

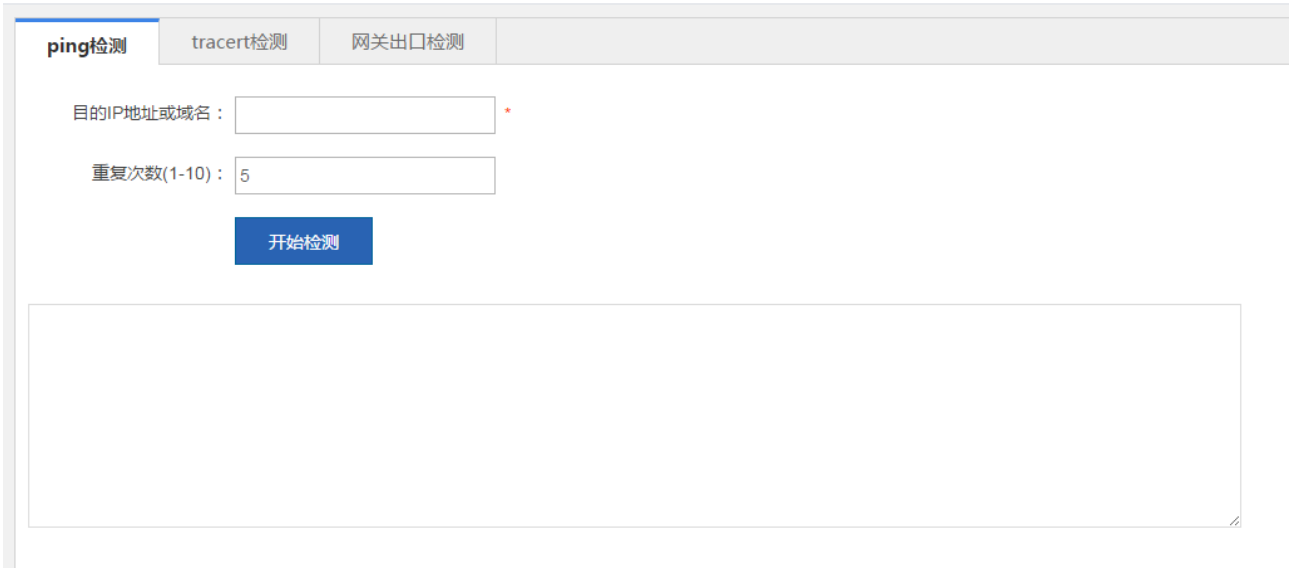
注意：该功能是给工程人员定位故障使用的，切莫乱用，以免导致影响网络正常。

1.3.14.6 检测网络

分为 ping 检测和 tracert 检测。



去掉了网关出口检测。

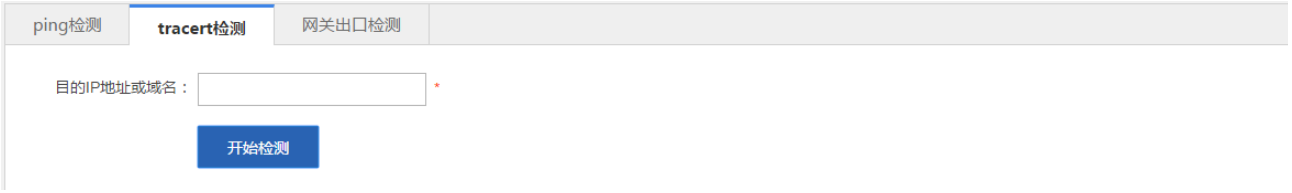


Ping 检测如下图：

输入“目的 IP 地址或域名”点击开始检测后会生成如下信息：

```
Translating "www.baidu.com"...[OK]
Sending 5, 100-byte ICMP Echoes to 14.215.177.37, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 33/34/35 ms.
```

tracert 检测如下图：



输入“目的 IP 地址或域名”点击开始检测后可以查看 tracert 的结果。

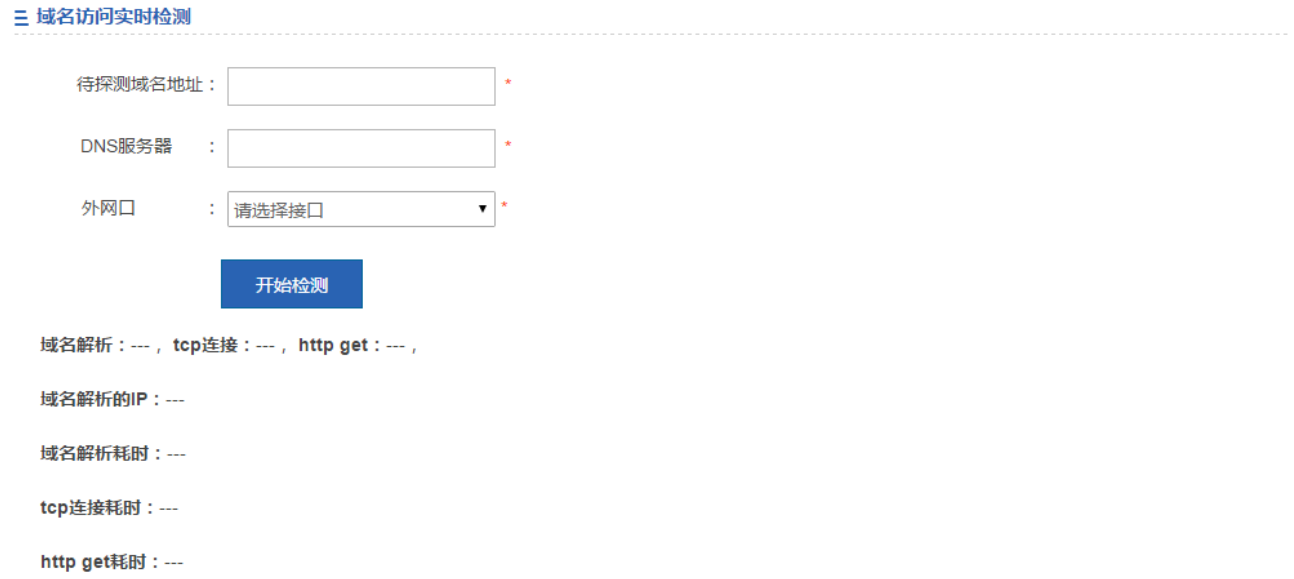
```
  < press Ctrl+C to break >
Tracing the route to 192.168.23.1

 1       192.168.23.1     <1 msec   <1 msec   <1 msec
```

网关出口检测，分为接口时延检测和域名实时访问检测。

接口时延检测，如下图

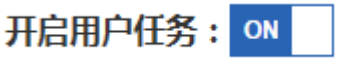
域名实时访问检测，如下图



1.3.14.7 定时任务

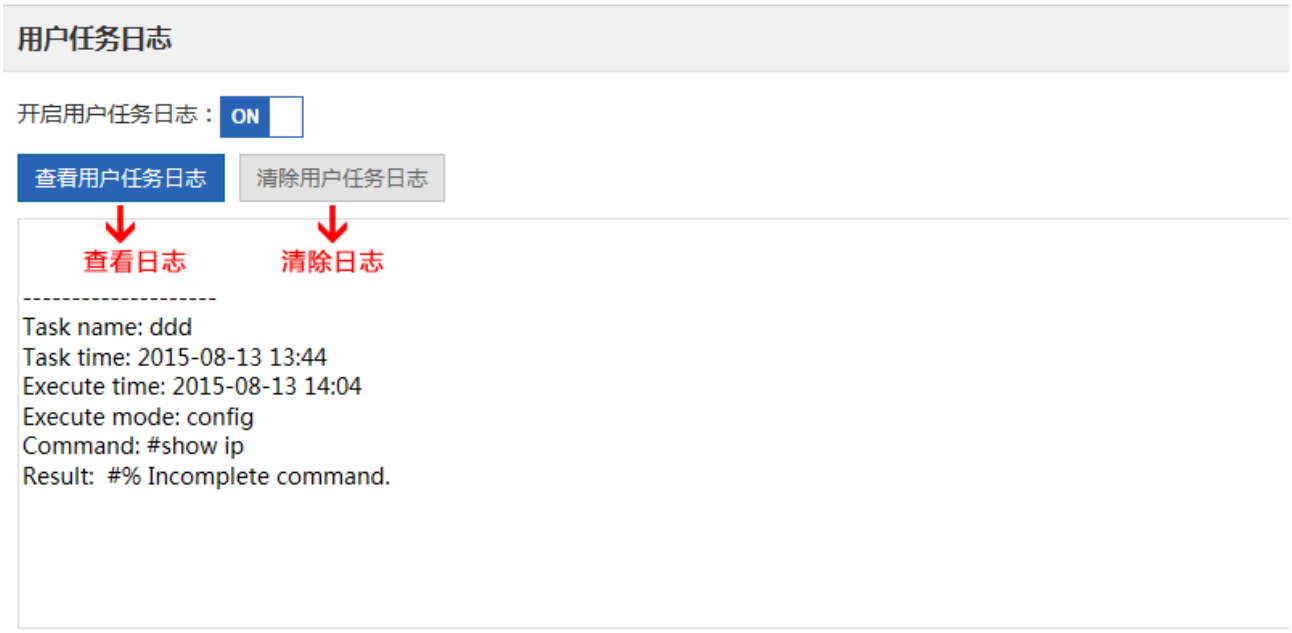
定时任务：是用于定时在设备上执行指定的 CLI 命令。工作原理是通过配置添加需要执行的 CLI 命令，到达配置的执行时间后，设备自动地执行该命令，达到无人值守的目的。

命令模式：分为特权模式与全局配置模式，配置为特权模式的时候执行权限为特权模式权限（即登录设备后的 Ruijie#，通常用于执行 show 命令）；全局配置模式则是执行权限为配置模式权限（即输入 config 后进入的 Ruijie(config)#，通常用于配置一些命令）。

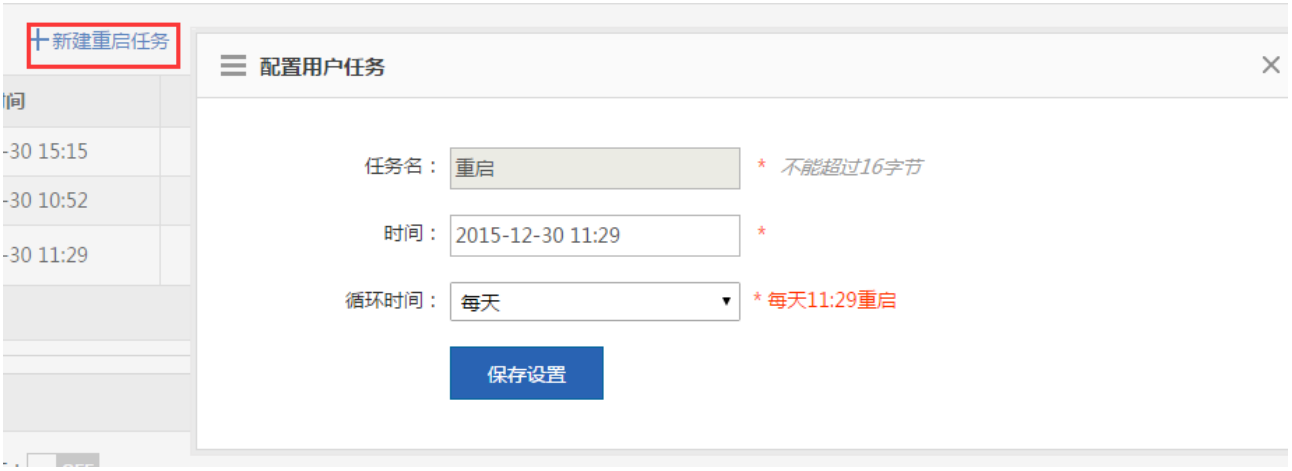
开启用户任务点击开启按钮 

后才能配置用户任务，新建用户任务如下弹出窗口：

对执行完任务可以查看用户任务日志，在开启日志模块后可查看如下



另外增加每日/每周重启场景的配置。如下图：



1.3.14.8 云服务

1.3.14.8.1云服务

账号绑定：


云服务
Online
状态：用账号进行管理网关设备。云网地址链接为：http://cloud.ruijie.com.cn/
注意：连接云服务需要配置DNS，请检查是否已经配置了正确的【DNS服务器】，否则将不能生效！
云服务配置与集中管理配置冲突，只能二选一。
绑定方式：
账号绑定
扫码绑定
网络名称
绑定账号：
手机尾号四位数：
阅读并同意<<隐私政策和用户协议>>
开启云服务并绑定账号
立即注册

扫码绑定：

成功绑定账号后。显示如下图

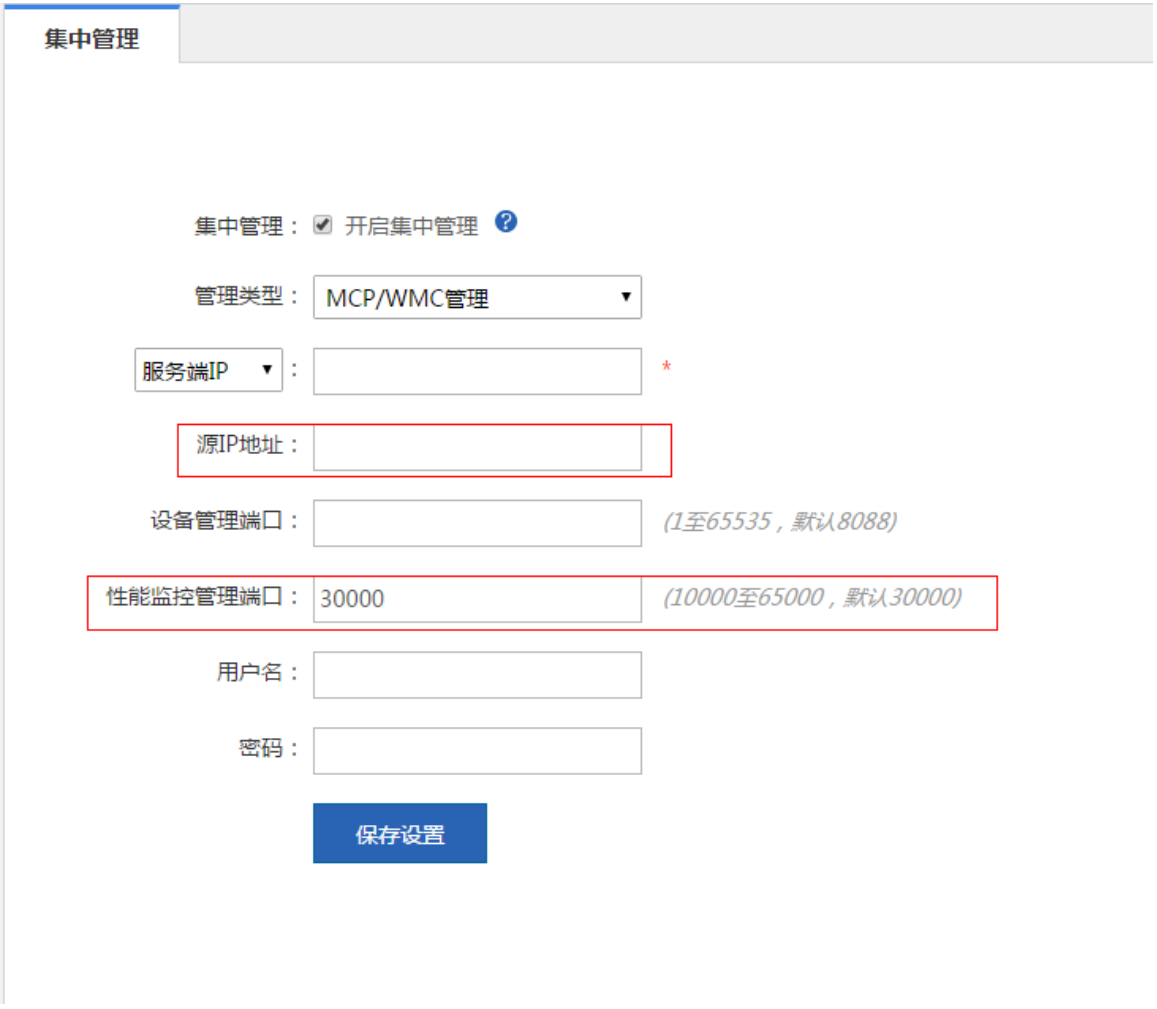
1.3.14.8.2Online

online 为云服务管理平台，设备提供与之对接的开关按钮，打开时候同意我们的隐私政策和用户协议！

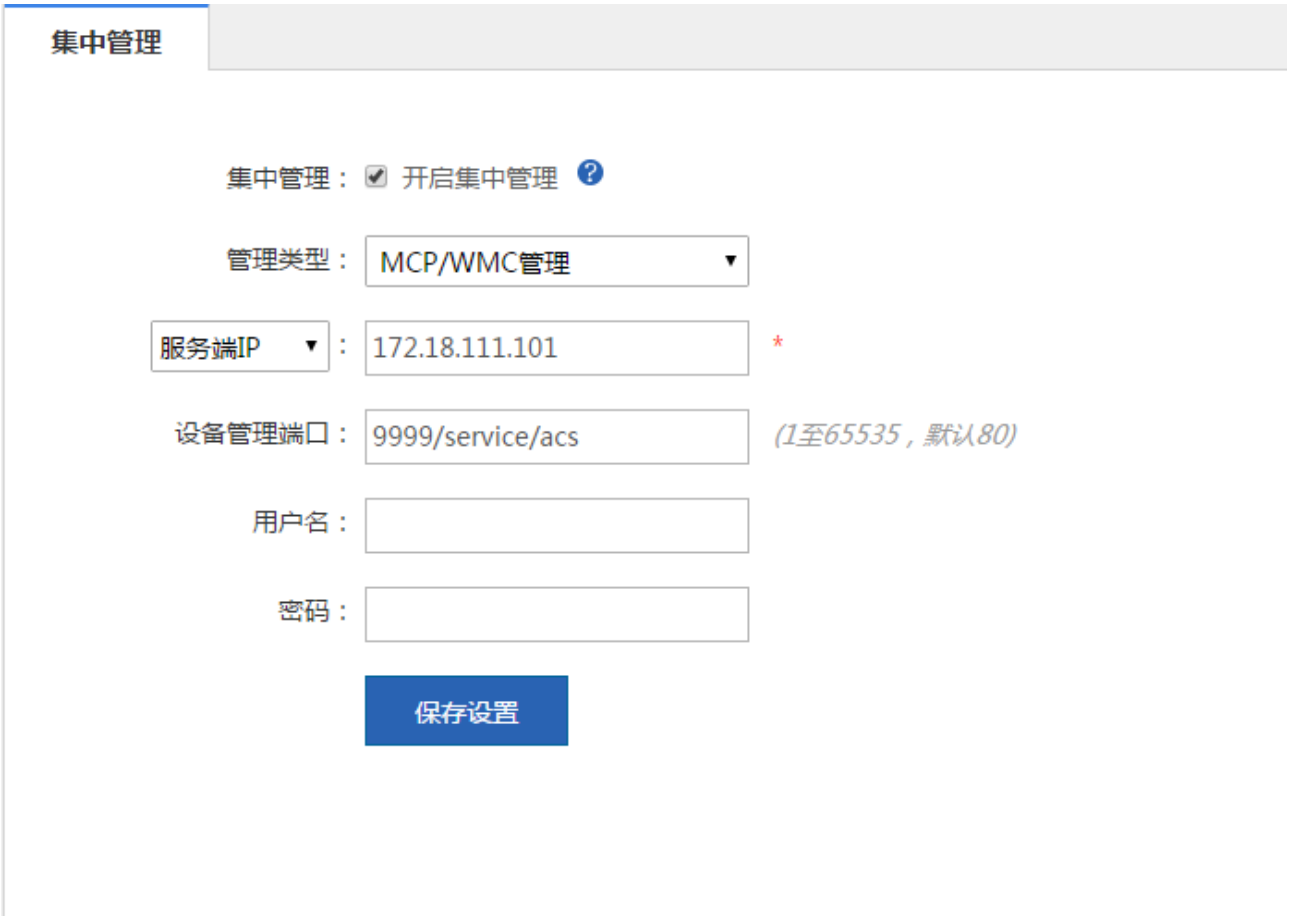
配置如下图，


开启Online：
OFF
Online 用户协议隐私政策
On-Line智慧门店云平台用户协议
《用户协议》（以下简称"本协议"）是您（或称"用户"，指注册、登录、使用、浏览本服务的个人或组织）与锐捷网络股份有限公司及其关联公司（以下简称"锐捷"）及其运营合作单位（以下简称"合作单位"）之间关于锐捷设备与锐捷On-Line智慧门店云平台网站（http://On-Line智慧门店云平台1.ruijie.com.cn，简称本网站）、锐捷睿易APP软件所订立的协议。
锐捷在此特别提醒用户认真阅读、充分理解---本协议中各条款，包括免除或者限制锐捷责任的免责条款及对用户的权利限制条款。请您审慎阅读并选择接受或不接受本协议(未成年人应在法定监护人陪同下阅读）。除非您接受本协议所有条款，否则您无权注册、登录或使用本协议所涉相关服务。您的注册、登录、使用等行为将视为对本协议的接受，并同意接受本协议各项条款的约束。
1.用户使用规则
1)在使用On-Line智慧门店云平台时，您必须承诺和保证：
您了解并同意，用户须对注册信息的真实性、合法性、有效性承担全部责任；用户不得冒充他人，不得利用他人的名义发布任何信息；不得恶意使用注册帐户导致其他用户误认；否则我们有权立即停止提供服务，您独自承担由此而产生的一切法律责任。 您使用On-Line智慧门店云平台的行为必须合
同意并开启
不同意

1.3.14.9 集中管理



添加了源 IP 地址和性能监控管理端口。



集中管理包括两种种类型 MCP 管理、RAC-SNC 管理、RCN 管理。

1.3.14.10 第三方日志

1.3.14.10.1 第三方服务器配置

配置第三方服务器：

选择 ELOG

选择第三方日志服务器

点击 添加

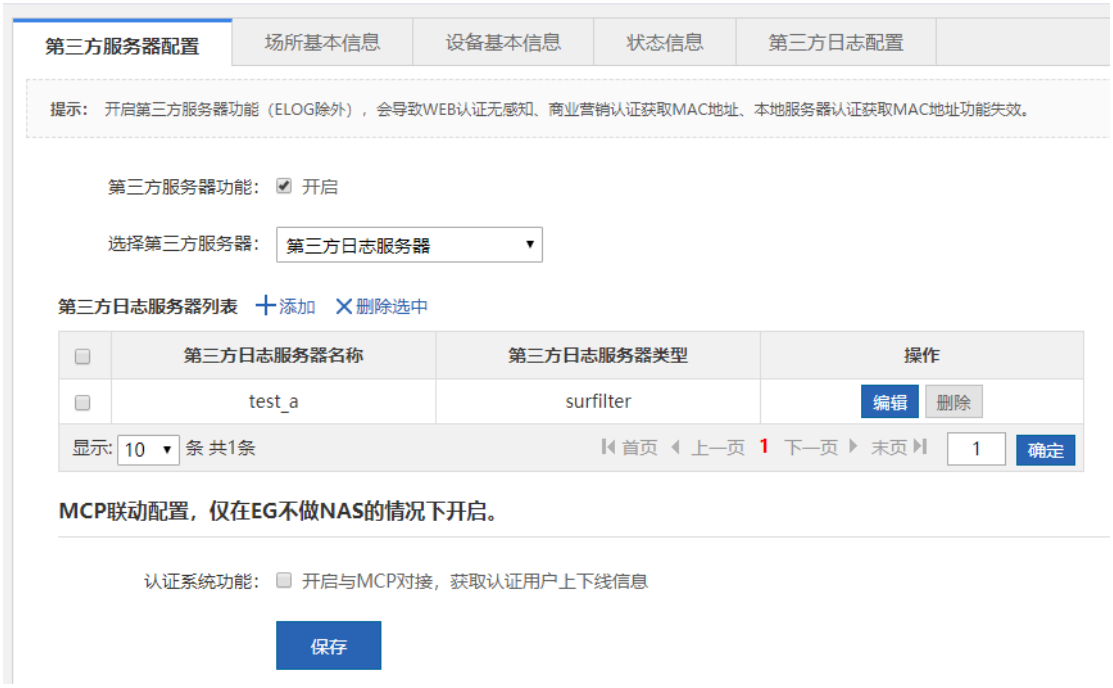

添加第三方日志服务器
第三方日志服务器类型:
任子行
第三方日志服务器名称:
*
服务器参数
服务器IP:
* IP地址
服务器端口(FTP):
21
* (1-65535，默认21)
FTP用户名:
*
FTP密码:
*
数据采集参数
保存
关闭

输入相关参数

点击弹窗中的 

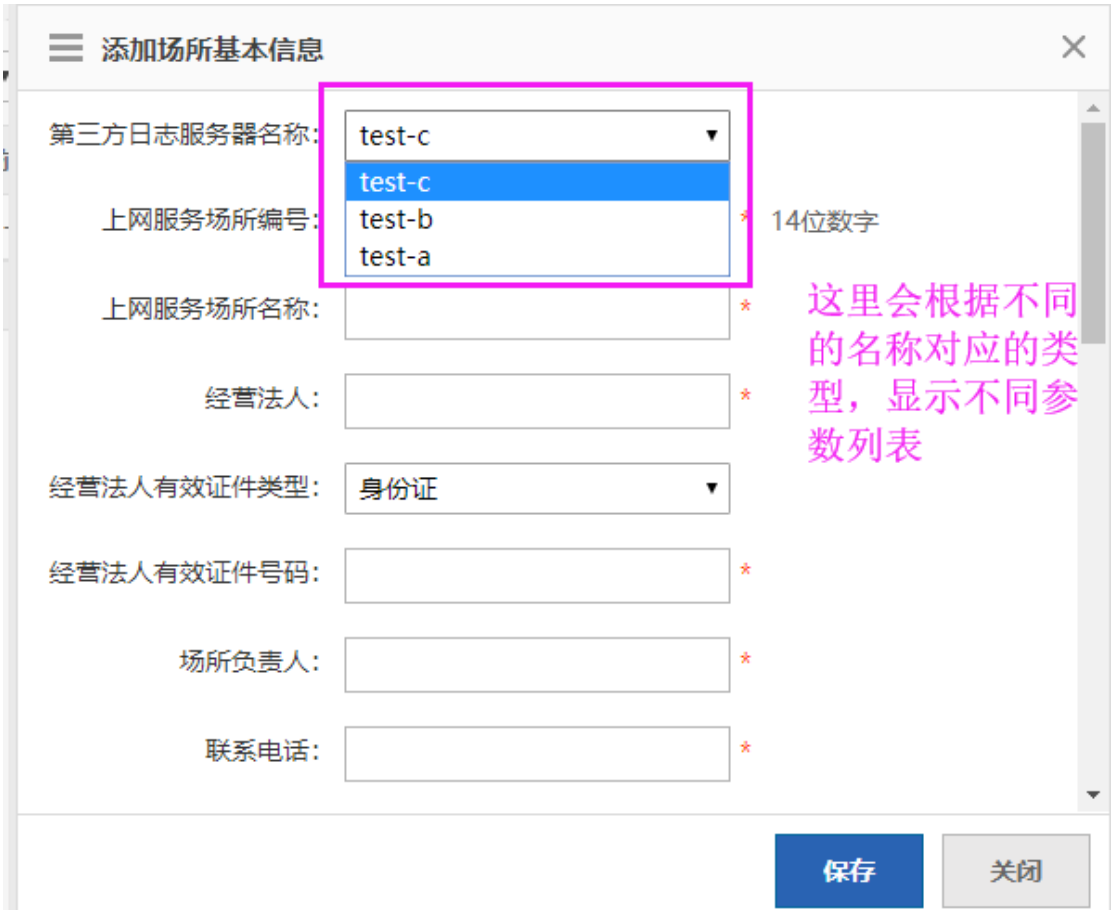
可进行编辑、删除操作

点击页面底下的保存按钮，显示如下

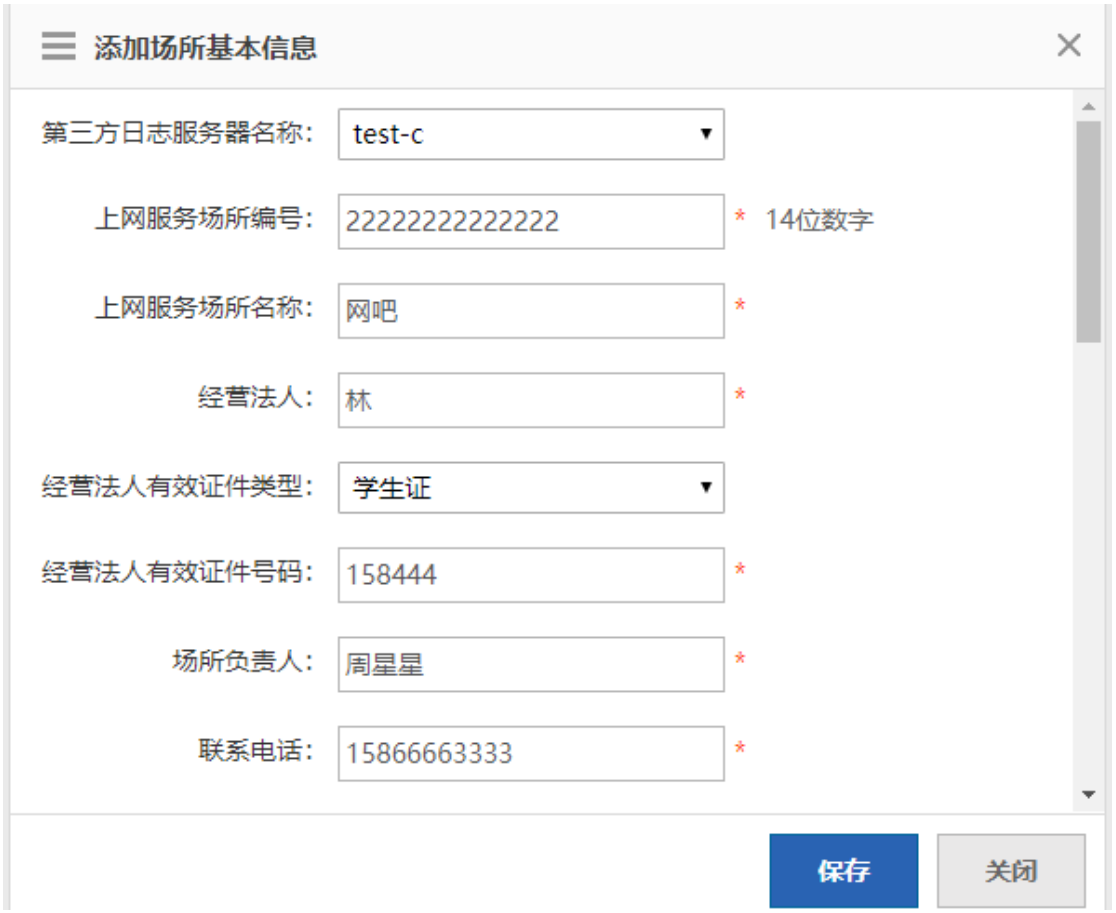


1.3.14.10.2 场所基本信息

点击 添加场所基本信息


添加场所基本信息
第三方日志服务器名称:
test-c
test-c
test-b
test-a
上网服务场所编号:
14位数字
上网服务场所名称:
经营法人:
这里会根据不同的名称对应的类型，显示不同参数列表
经营法人有效证件类型:
身份证
经营法人有效证件号码:
场所负责人:
联系电话:
保存
关闭

输入参数



点击 

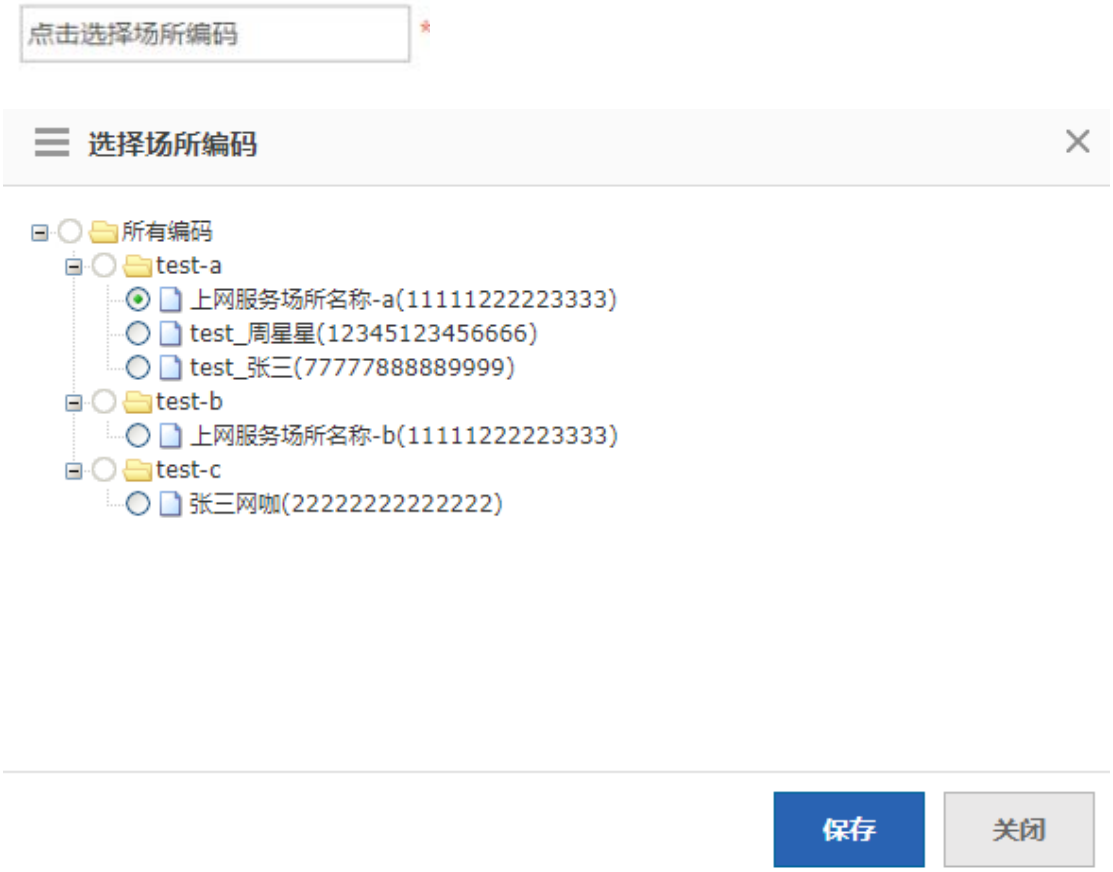
表格数据可以进行删除、编辑

查找、导出导入数据（必须先选择服务器名称）

1.3.14.10.3 设备基本信息

点击 ＋添加AP基本信息

点击


点击选择场所编码
选择场所编码
所有编码
test-a
上网服务场所名称-a(11111222223333)
test_周星星(12345123456666)
test_张三(77777888889999)
test-b
上网服务场所名称-b(11111222223333)
test-c
张三网咖(22222222222222)
保存
关闭

点击 
保存

再点击弹窗中的 

表格数据可进行编辑、删除操作

查找、导入导出数据

1.3.14.10.4 状态信息

点击 

可以清空日志跟发送记录

1.3.14.10.5 第三方日志配置

可以直接点击全部开启/关闭，单独勾选 NAT 审计日志、BBS 审计日志、虚拟身份审计日志、搜索审计日志、MAIL 审计日志、HTTP/URL 审计日志后。点击 保存配置 按钮完成配置。

1.3.14.11 SDN 配置

1.3.14.12 VRRP 配置

VRRP (Virtual Router Redundancy Protocol，虚拟路由冗余协议)设计采用主备模式，以保证当主路由设备发生故障时，备份路由设备可以在不影响内外数据通信的前提下进行功能切换，且不需要再修改内部网络的参数。

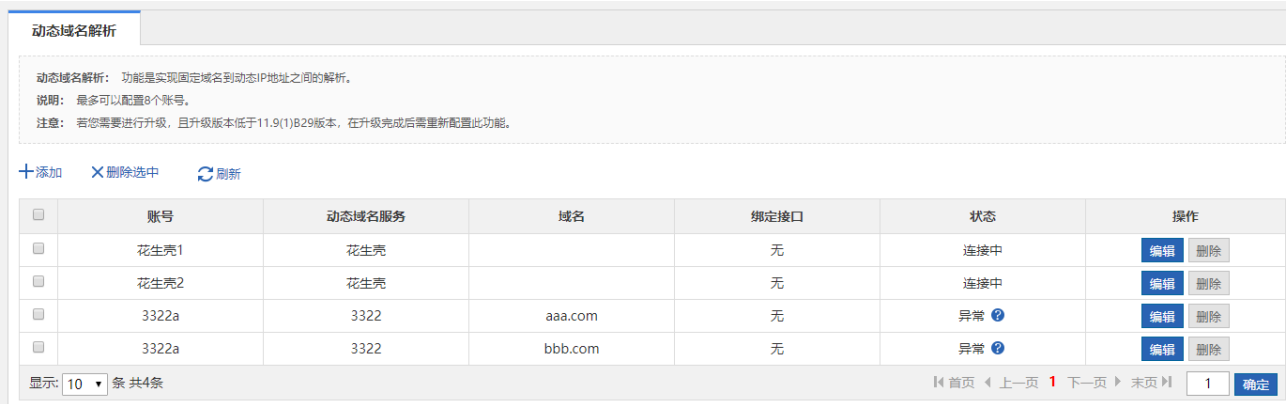
指定接口：这里会将设备当前所有内网口都展示出来，您可以选择一个要配置的接口；

VRRP 组号：这个好比是 VRRP 名称，是用户标记 VRRP 策略的；

VRRP 组 IP：这里输入 VRRP 组 IP，要特别注意的是，当您输入的 IP 跟选择的接口 IP 相同的时，那么 VRRP 优先级会自动设置为 255.不可以修改。

VRRP 优先级：同一接口的 VRRP 匹配优先顺序。

1.3.14.13 动态域名解析



动态域名解析是是实现固定域名到动态 IP 地址之间的解析。

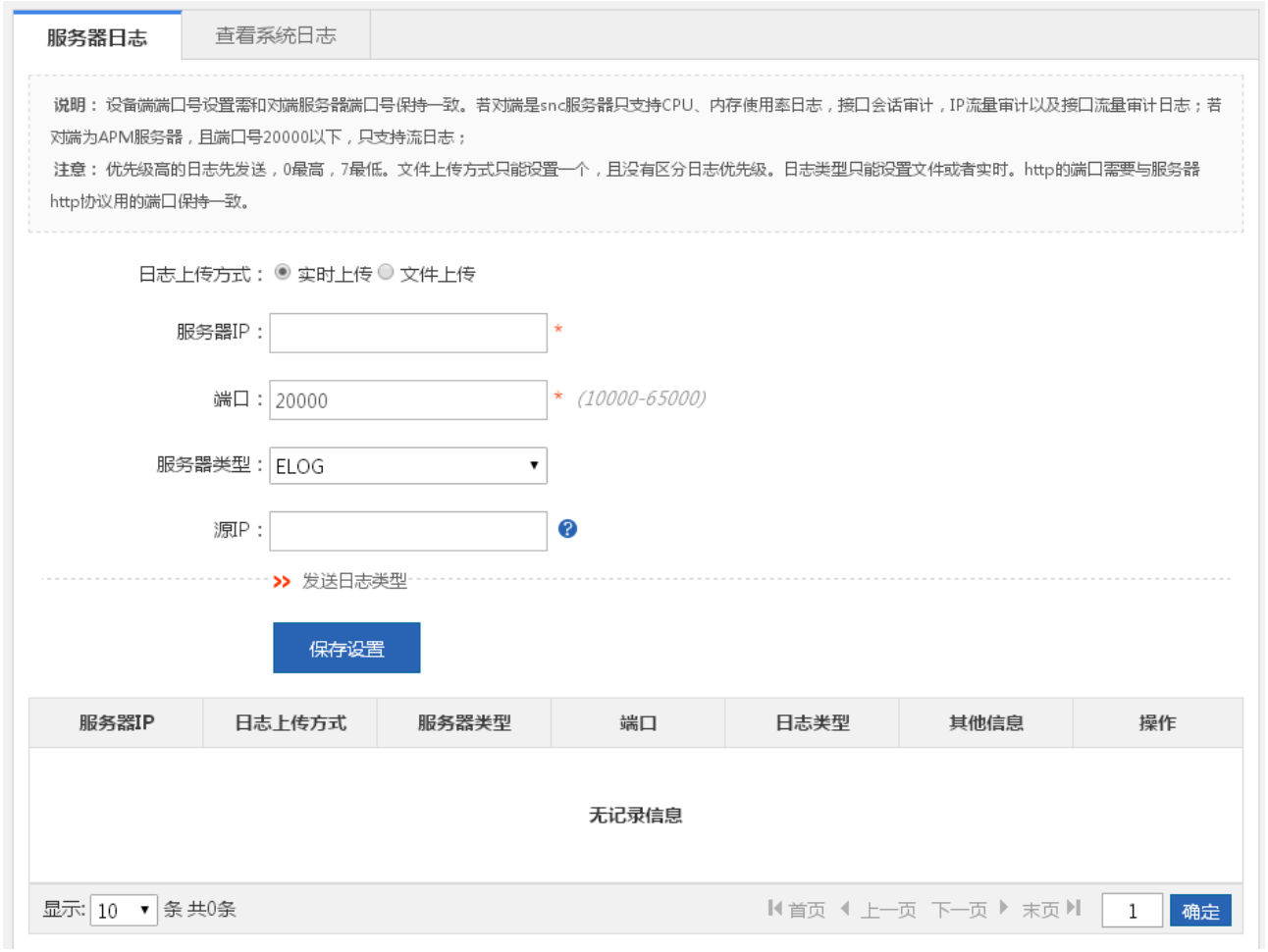
目前设备支持 花生壳、3322 服务提供商；如果您没有帐号可以点击【没有帐号请先注册】 这里注册帐号；

用户名和密码：这里输入您在花生壳用户名和密码；

1.3.14.14 系统日志

1.3.14.14.1 服务器日志

是指将设备审计下来的日志发生给指定的日志服务器。目前 NBR 设备支持的日志类型如下图所示，您可以根据您的需要配置日志类型发送到指定的服务器。



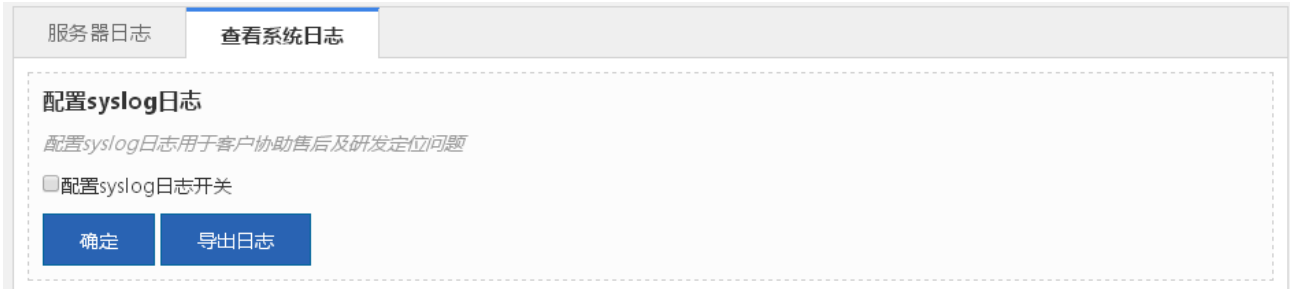
输入服务器 ip 地址：这里输入接收日志的服务器的 ip 地址；

1. 端口 特别注意了 ,端口范围是有含义的 ,端口号小于 20000 的为 E-LOG 服务器 ,20000 及以上为 SNC 服务器 ,E-LOG 只支持 URL 和流日志，SNC 支持所有日志。

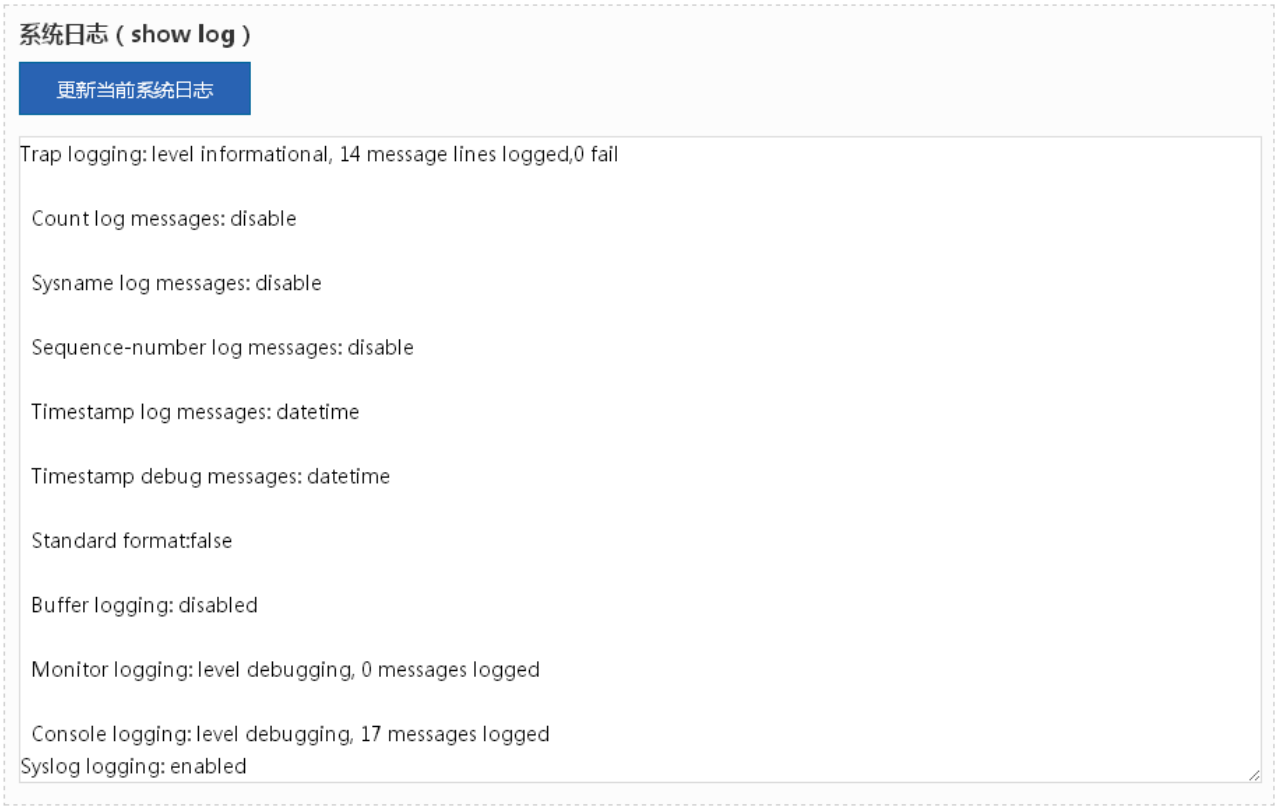
1.3.14.14.2 查看系统日志

包括配置 syslog 日志和查看系统日志 。

配置 syslog 日志，开启日志的时候才可以导出 syslog。



点击更新当前系统日志按钮，可刷新当前系统日志信息如下图所示：



1.3.14.14.3 SYSLOG 服务器配置

1.3.14.15 日志策略

1.3.14.16 投屏服务

说明： 投屏服务能在内网跨网段支持苹果和安卓投屏功能，终端通过认证加入到某一房间号，终端的房间号与电视 IP 绑定的房间号需要一致才能在对应房间号下使用投屏，避免了投射到其它房间的电视上；每个房间最多能添加 8 台电视映射。

该功能默认不开启，配置界面如下：

开启后的状态：

导入模板示例：

	A	B
1	房间号	电视IP/MAC（多个用“,”隔开，最多配置8个）
2	101	192.168.101.1
3		
4		

1.3.14.17 设备审计报表

1.3.14.17.1 WEB 操作日志

系统操作日志查看操作设备的情况