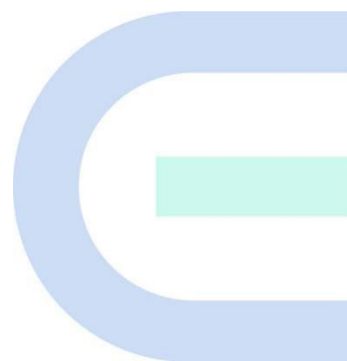


RG-NBR 系列出口网关

RGOS 11.9(6)B14 Web 管理手册



文档版本 V1.0

归档日期 2022-08-18

copyright © 2022 锐捷网络

版权声明

copyright © 2022 锐捷网络

保留对本文档及本声明的一切权利。

未得到锐捷网络的书面许可，任何单位和个人不得以任何方式或形式对本文档的部分或全部内容进行复制、摘录、备份、修改、传播、翻译成其他语言、将其部分或全部用于商业用途。

 和其他锐捷网络商标均为锐捷网络的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

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，本文档中描述的部分或全部产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，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：<https://www.ruijiery.com/>
- 锐捷睿易在线客服：<https://ocs.ruijie.com.cn/?p=smb>
- 锐捷网络官方网站服务与支持版块：<https://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：<https://www.ruijie.com.cn/service/know.aspx>
- 锐捷睿易技术支持与反馈信箱：4001000078@ruijie.com.cn
- 锐捷网络文档支持与反馈信箱：doc@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. 图形界面格式约定

界面图标	解释	举例
<>	按钮	<确定>
[]	菜单项，弹窗名称，页面名称，标签页的名称	菜单项“系统设置”可简化[系统设置]
>>	分级页面，子菜单项	选择[系统设置]>>[系统管理员]
""	配置项，提示信息，链接	如提示框提示“保存配置成功” 点击“开启”选项 点击“忘记密码”链接

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：



表示用户必须严格遵守的规则。如果忽视此类信息，可能导致数据丢失或设备损坏。

 注意

表示用户必须了解的重要信息。如果忽视此类信息，可能导致功能失效或性能降低。

 说明

用于提供补充、申明、提示等。如果忽视此类信息，不会导致严重后果。

 产品/版本支持情况

用于提供产品或版本支持情况的说明。

3. 说明

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

目 录

前 言.....	i
1 产品概述	1
2 登录设备	2
2.1 配置环境要求.....	2
2.2 缺省配置	2
2.3 使用PC登录Web	2
2.3.1 连接设备	2
2.3.2 配置管理客户端IP.....	3
2.3.3 登录Web.....	3
2.4 Web主界面说明.....	4
2.4.1 标题区.....	5
2.4.2 菜单导航区	7
2.4.3 主操作区	8
2.4.4 状态区.....	8
2.4.5 导航栏告警	10
3 快速配置	11
3.1 快速配置	11
3.2 睿易一体化配置	16
4 首页.....	19
4.1 系统首页.....	19
4.1.1 接口信息	19
4.1.2 设备概况.....	19
4.1.3 带宽状态.....	20
4.1.4 主程序推送	22
4.2 功能管理	23
4.3 接口连接状态.....	24
5 常用功能	25
6 行为管理	26
6.1 流量监控.....	26

6.1.1 功能简介	26
6.1.2 实时流量	26
6.1.3 历史接口流量	37
6.1.4 VPN流量	38
6.1.5 数据流明细	39
6.2 流控策略	40
6.2.1 智能流控	40
6.2.2 策略调整	42
6.2.3 参数调整	45
6.2.4 应用调整	46
6.2.5 VPN流控	47
6.3 对象定义	49
6.3.1 功能简介	49
6.3.2 自定义应用分组	49
6.3.3 自定义网站分组	53
6.3.4 时间对象	56
6.3.5 关键字组对象	58
6.3.6 外网IP对象	59
6.3.7 VLAN对象	63
6.3.8 IP对象	64
6.4 行为策略	67
6.4.1 功能简介	67
6.4.2 简易配置	67
6.4.3 高级配置	79
6.4.4 审计告警	98
6.4.5 告警信息查询	100
6.5 行为实时审计记录	100
6.6 行为阻断信息记录	101
6.7 行为审计日志查询	102
6.7.1 访问审计报表	102
6.7.2 内容审计报表	106

6.8 行为统计分析.....	109
6.8.1 功能简介.....	109
6.8.2 报表配置.....	110
6.8.3 自定义报表.....	110
6.8.4 客户端邮件.....	111
6.8.5 Web邮件.....	112
6.8.6 IM聊天.....	114
6.8.7 搜索引擎.....	115
6.8.8 论坛发帖.....	116
6.8.9 外发文件.....	118
6.8.10 网站分类.....	119
6.8.11 网站域名.....	120
6.8.12 虚拟身份.....	122
7 安全认证.....	124
7.1 用户组织.....	124
7.1.1 用户管理.....	124
7.1.2 导入导出用户.....	128
7.1.3 特殊用户管理.....	130
7.1.4 上网屏蔽模式.....	132
7.2 Web认证.....	133
7.2.1 Web认证.....	133
7.2.2 Web认证免认证.....	141
7.2.3 用户认证的高级设置.....	146
7.3 商业营销认证.....	147
7.3.1 商业营销认证.....	147
7.3.2 商业营销免认证.....	151
7.4 本地服务器认证.....	156
7.4.1 本地账号密码认证.....	156
7.4.2 短信认证.....	159
7.4.3 微信认证.....	162
7.4.4 二维码授权认证.....	165

7.4.5 二维码自助认证	168
7.4.6 AD域认证	171
7.4.7 认证策略管理	175
7.4.8 认证服务器管理	175
7.4.9 高级配置	175
7.4.10 免认证配置	178
7.4.11 单点登录	182
7.4.12 用户权限	183
7.4.13 在线信息	184
7.5 PPPoE Server	185
7.5.1 功能简介	185
7.5.2 服务器配置	185
7.5.3 账号管理	186
7.5.4 在线信息	189
7.6 本地防攻击	190
7.7 接口访问控制	192
7.8 ARP表项	193
7.8.1 功能简介	193
7.8.2 查看ARP表项	193
7.8.3 静态ARP绑定	193
7.8.4 设置ARP过滤	196
7.8.5 停止ARP学习	197
7.8.6 免费ARP请求	197
7.9 ACL访问列表	198
7.10 连接数限制	200
7.10.1 设备抗攻击配置	200
7.10.2 设置内网用户会话数限制	203
8 网络	208
8.1 接口配置	208
8.1.1 接口基本设置	208
8.1.2 一线多拨	213

8.1.3 多链路聚合	213
8.1.4 接口转换	214
8.1.5 链路检测	215
8.1.6 端口监控	215
8.1.7 接口基本设置IPv6	216
8.2 SUPER-VLAN	217
8.2.1 功能简介	217
8.2.2 SUPER-VLAN配置	217
8.2.3 在线SUPER-VLAN信息	218
8.3 路由/负载	218
8.3.1 功能简介	218
8.3.2 选路配置向导	219
8.3.3 策略路由	220
8.3.4 应用路由	221
8.3.5 普通路由	229
8.3.6 多链路负载均衡	232
8.4 DNS配置	233
8.4.1 功能简介	233
8.4.2 DNS服务器	233
8.4.3 正向DNS代理	233
8.5 VPN配置	235
8.5.1 功能简介	235
8.5.2 配置VPN服务端（总部）	235
8.5.3 配置VPN客户端（分支机构）	243
8.5.4 VPN配置	247
8.6 SSLVPN配置	251
8.6.1 功能介绍	251
8.6.2 配置向导	252
8.6.3 运行状态	260
8.6.4 基本设置	262
8.6.5 短信策略管理	269

8.6.6 隧道资源管理.....	270
8.6.7 用户授权.....	274
8.6.8 Site to Site管理	276
8.7 NAT/端口映射	278
8.7.1 功能介绍.....	278
8.7.2 端口映射	278
8.7.3 NAT转换规则.....	280
8.7.4 添加NAT地址池	281
8.8 NATPT配置.....	282
8.8.1 参数配置.....	283
8.8.2 V4V6规则	283
8.8.3 V6V4规则	284
8.8.4 地址池配置	285
8.9 DHCP配置.....	286
8.9.1 功能简介	286
8.9.2 服务端配置	286
8.9.3 静态地址分配.....	291
8.9.4 客户端列表	292
8.10 DHCP配置 (IPAM)	293
8.10.1 IPAM主页	293
8.10.2 IP智能管理	294
8.10.3 业务告警.....	295
8.10.4 DHCP配置管理	296
8.10.5 地址池使用情况.....	298
8.10.6 DHCP日志.....	300
8.10.7 DHCP黑名单	300
8.11 DHCP-V6配置.....	301
8.11.1 功能简介	301
8.11.2 服务端配置.....	301
8.11.3 客户端列表.....	303
8.12 线路逃生.....	303

8.12.1 功能简介	303
8.12.2 配置线路流量逃生	303
8.12.3 查看逃生日志	305
9 无线	306
9.1 无线开关	306
9.2 无线管理首页	306
9.3 用户信息	307
9.4 添加无线网络	307
9.4.1 功能介绍	307
9.4.2 无线网络[RGOS]	307
9.4.3 无线网络[Reyee OS]	311
9.5 AP管理	312
9.5.1 功能介绍	312
9.5.2 AP管理[RGOS]	312
9.5.3 AP管理[Reyee OS]	315
9.6 AP升级	317
9.6.1 AP升级[RGOS]	317
9.6.2 AP升级[Reyee OS]	318
9.7 DHCP安全	319
9.8 反制非法AP	320
9.9 黑白名单[RGOS]	321
9.10 黑白名单[Reyee OS]	323
9.10.1 全局黑白名单	323
9.10.2 基于SSID黑白名单	325
9.11 射频[Reyee OS]	327
9.12 禁止内网互访	328
9.13 WIS	329
9.14 负载均衡	329
9.15 整网管理	331
10 防火墙	333
10.1 防攻击配置	333

10.1.1	防攻击开关	333
10.1.2	全局防护	333
10.1.3	协议类策略	334
10.1.4	域策略	335
10.2	安全域配置	339
10.2.1	安全域开关	339
10.2.2	安全域	340
10.2.3	全局配置策略	343
10.2.4	域策略配置	343
10.3	防攻击域状态监控	350
10.3.1	域运行状态	350
10.3.2	当前攻击行为	351
10.3.3	防火墙流量查看	351
10.4	IP资源配置	352
10.4.1	主机地址	352
10.4.2	范围地址	353
10.4.3	子网地址	354
10.4.4	地址组配置	354
10.5	服务资源配置	355
10.5.1	自定义服务	355
10.5.2	服务组配置	356
10.5.3	预定义服务	357
11	运维	358
11.1	系统设置	358
11.1.1	修改密码	358
11.1.2	重启设备	359
11.1.3	恢复出厂设置	359
11.1.4	配置备份	359
11.1.5	系统时间	361
11.1.6	增强功能	363
11.1.7	SNMP	366

11.2	系统升级.....	367
11.3	一键收集.....	369
11.4	抓包工具.....	369
11.5	检测网络.....	371
11.5.1	ping检测	371
11.5.2	tracert检测	372
11.6	网络诊断.....	372
11.7	设备审计报表.....	373
12	高级.....	375
12.1	管理员权限	375
12.2	定时任务.....	376
12.3	License管理	377
12.4	云服务.....	377
12.4.1	功能介绍	377
12.4.2	云服务.....	378
12.4.3	云预注册	379
12.5	集中管理.....	379
12.6	第三方日志	380
12.6.1	配置第三方服务器	380
12.6.2	配置Elog	385
12.7	动态域名解析.....	386
12.8	系统日志.....	387
12.8.1	服务器日志	387
12.8.2	查看系统日志.....	387
12.8.3	SYSLOG服务器配置	388
12.9	日志策略.....	389
12.10	投屏服务.....	390
12.11	VRRP配置.....	393
12.11.1	功能介绍	393
12.11.2	VRRP配置	393
12.11.3	单地址VRRP配置	394

12.12 防共享接入	396
12.12.1 一键防共享	396
12.12.2 防共享策略	396
12.12.3 实时监测状态.....	397
12.13 启用防封杀	397
12.14 加速-应用缓存	398

1 产品概述

RG-NBR系列产品是锐捷睿易为办公、酒店、餐厅、娱乐、景区等综合场景量身打造的多业务综合网关（路由器）。RG-NBR系列产品支持业务加速通道、精准流控、上网行为管理、VPN总分互联、智能/应用选路等多个功能，并支持对接锐捷云平台（MACC免费云平台）实现远程云运维和集中管理，能够很好的满足办公、酒店、餐厅、娱乐、景区等场景的一体化网络需求。

RG-NBR系列出口网关支持Web GUI管理界面，可使用Web管理系统来配置和管理设备的常用功能。

2 登录设备

用户通过客户端（PC、移动终端设备等）访问NBR-E设备的管理IP地址，即可接入Web管理系统，对设备进行配置管理。

2.1 配置环境要求

用于登录Web管理系统的客户端（PC、移动终端设备等）需要满足如下环境要求：

- 浏览器：支持Google chrome、IE9.0、IE10.0、IE11.0以及部分基于谷歌/IE内核的浏览器（如360安全浏览器，推荐使用极速模式）。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。
- 分辨率：建议分辨率设置为1024*768、1280*1024、1440*960或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。

2.2 缺省配置

表2-1 缺省 Web 配置

功能特性	缺省值
设备IP	● 初始配置或恢复出厂设置后，默认的Web管理地址为：http://192.168.1.1。 ● 如果使用HTTPS协议，初始管理地址为：https://192.168.1.1:4430。
用户名/密码	admin/admin
端口	网关模式下PC机连接设备的Gi0/0端口，默认为网关模式。

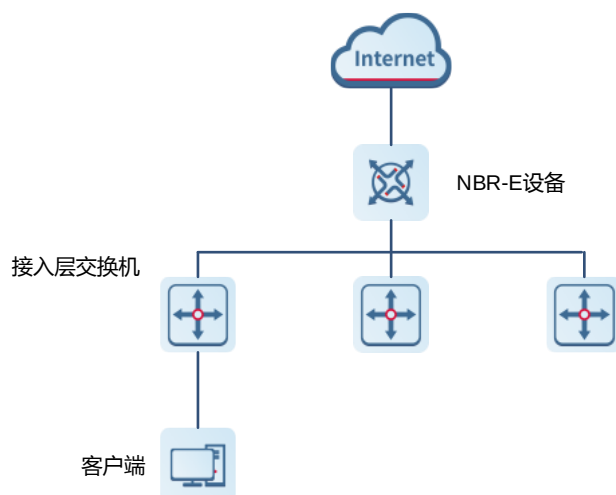
2.3 使用 PC 登录 Web

2.3.1 连接设备

将管理客户端与设备建立网络连接才能进入管理页面完成网关配置。

设备和客户端的连接关系如[图2-1](#)所示。

图2-1 连接关系示意



2.3.2 配置管理客户端 IP

为管理客户端配置一个与设备默认IP（设备默认IP地址：192.168.1.1，子网掩码：255.255.255.0）在同一网段的IP地址，使管理客户端能够访问设备。如设置管理客户端的IP地址为192.168.1.200。

2.3.3 登录 Web

【前置条件】

要使用Web管理，还必须确认NBR设备的存在Web页面升级包（设备里面存在web.gz这个文件）和Web运行的ngx环境，否则无法进入管理页面。Web管理所需的文件缺省已经安装在设备上，如果无法进入Web管理系统，请联系技术服务人员进行支持。

【操作步骤】

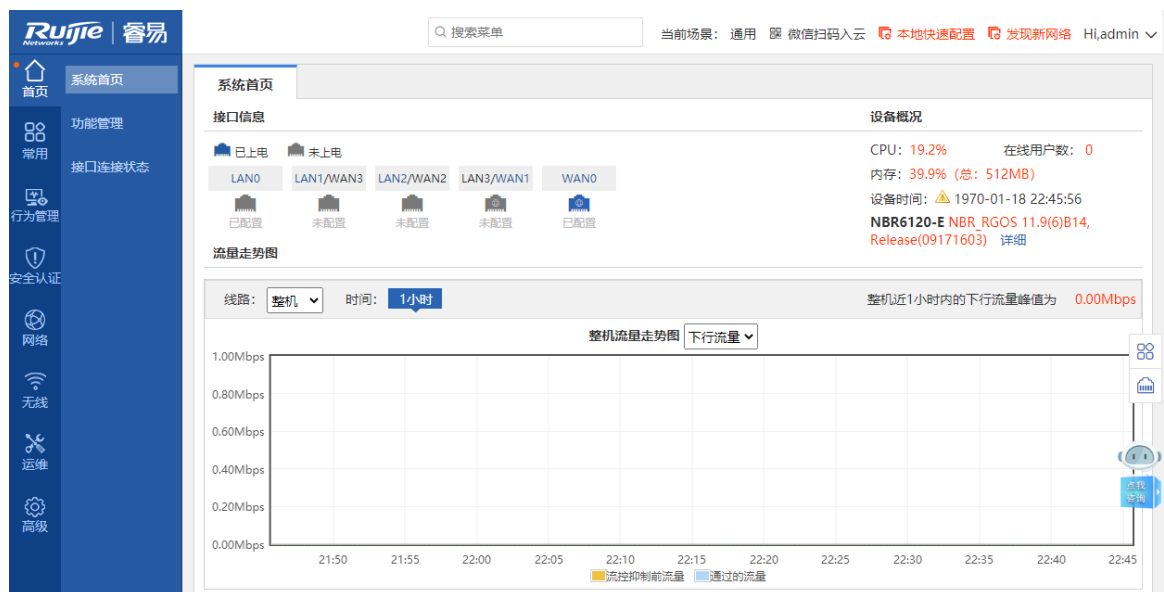
(1) 在浏览器地址栏中输入设备的IP地址（默认为192.168.1.1），进入登录页面。



登录界面提供了如下功能：

- 如果忘记了用户名或密码，请点击<忘记密码>。
- 如果需要客服帮助，请点击<在线客服>和客服进行在线交流。

(2) 输入用户名和密码后点击<登录>，进入Web管理系统首页。



【后续处理】

- 为了保障设备安全，建议在首次登录Web管理系统后修改默认密码。
- 若忘记IP或密码，可在设备接通电源的情况下，长按设备面板上的reset键5秒以上使设备恢复出厂设置，恢复后即可使用默认IP和密码登录。

⚠ 注意

恢复出厂设置将删除已有配置，再次登录需重新配置，请谨慎操作。

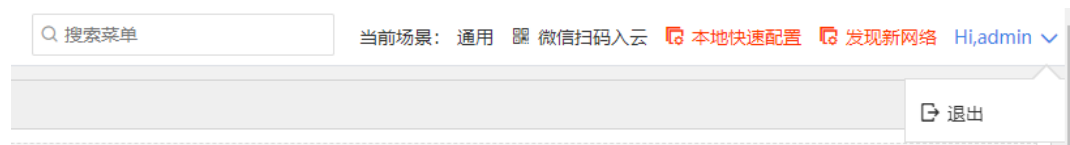
2.4 Web 主界面说明

Web管理平台主页面下图所示：



2.4.1 标题区

该区域为用户提供了一些常用功能的链接，方便用户快速定位到常用的功能设置页面。主要有“菜单搜索”、“微信扫码入云”、“本地快速配置”、“发现新网络”和“退出”。



功能项	说明	参考章节
本地快速配置	提供向导化的配置，实现设备快速接入网络。	3.1 快速配置
发现新网络	当组网环境中接入新的设备后，可以通过发现新网络功能完成一体化配置。	3.2 睿易一体化配置
菜单搜索	在输入框输入功能关键字，系统将自动搜索对应功能项，点击可直接跳转至配置页面，帮助用户快捷地找到功能入口。	无
微信扫码入云	通过扫描二维码，用户可以将设备绑定云端帐号，在云端随时随地对设备和网络进行配置管理。	无

- 本地快速配置
详见[3.1 快速配置](#)章节。
- 发现新网络
详见[3.2 睿易一体化配置](#)章节。
- 菜单搜索
点击搜索框，默认显示最近访问的菜单。



支持输入要查询的菜单名称，进行查询，点击菜单列表可以跳转至相应的菜单页面。



- 微信扫码入云

鼠标移动到该按钮，弹窗显示二维码。使用微信扫描二维码，可将设备绑定云端帐号，在云端进行配置管理。

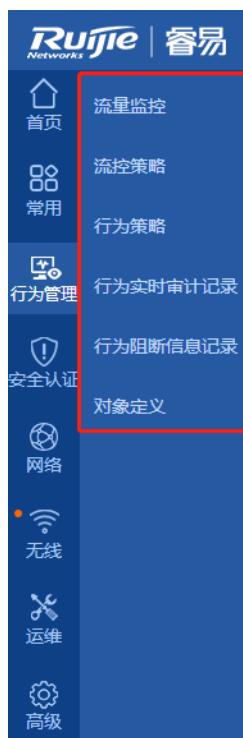


- 退出：当完成本次设备管理后，请单击  退出 按钮，退出NBR的Web管理平台主页面，回到登录页面。

2.4.2 菜单导航区

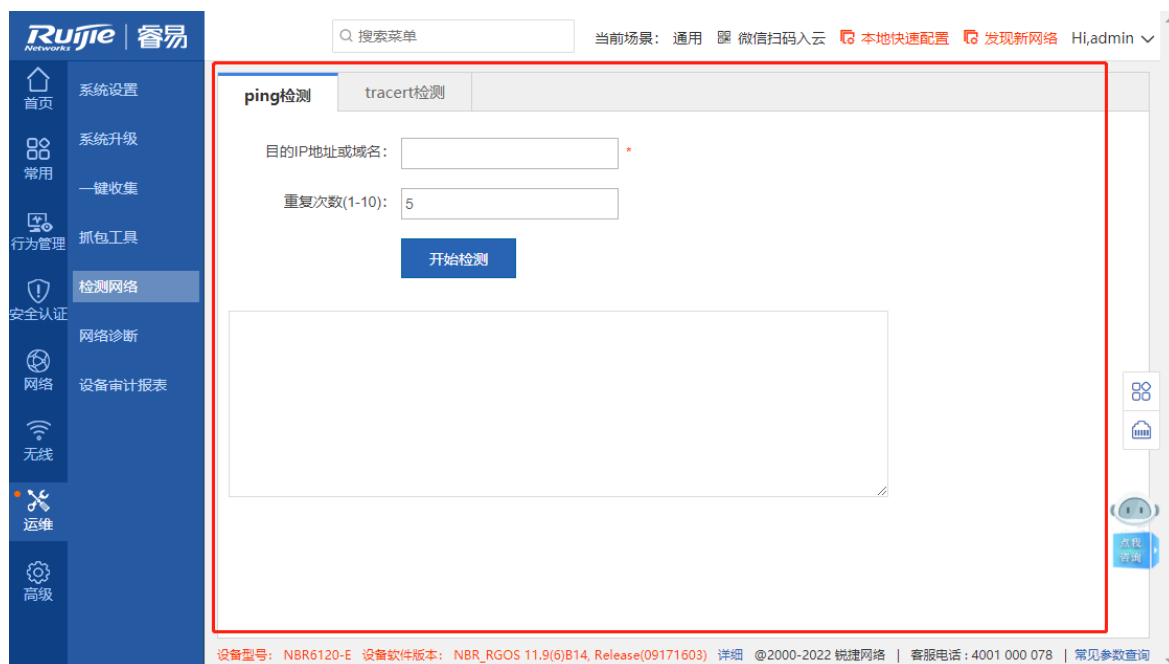
在Web管理主界面的左侧设有“功能菜单导航”区域。该区域列出了NBR的所有功能菜单。用户点击相应菜单后在“主操作区”会打开详细的设置页面。

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



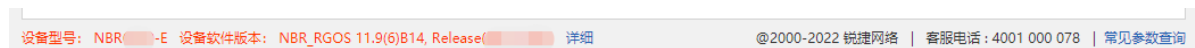
2.4.3 主操作区

主操作区是完成设备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。



2.4.4 状态区

- 页面底部左侧显示设备的型号和版本号；右侧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。



- 页面右下角增加闪电兔图标，可以点击进入咨询。





- 查看常用功能及配置样例：点击页面右侧  按钮，将显示设备的常用功能并给出部分配置案例，用户可点击功能名称跳转至各功能的配置页面，或点击“配置样例”查看配置指导文档。



- 查看接口信息：点击页面右侧  按钮，将显示接口的基本信息，包括是否上电和接口IP地址等。



2.4.5 导航栏告警

当前场景：通用  微信扫码入云  本地快速配置  发现新网络  告警 (1) Hi,admin ▾

当存在系统告警信息时，页面右上角标题区会出现  告警 (1) 按钮，括号内的数字表示系统当前存在的告警数量。点击该按钮，系统弹出“告警”提示框，显示有告警的模块：

说明

如果未产生告警，则系统无提示信息。

- 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

全部特征库告警日志

可查看所有特征库版本告警信息。

- 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。

- 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。

- 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。

- 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。

3 快速配置

3.1 快速配置

【应用场景】

首次登录Web管理界面时，设备处在空配置状态。为了简化配置工作，建议用户使用“快速配置”向导来完成设备的常用功能设置。

说明

- 如果用户不需要“快速配置”功能，请点击<转到首页>直接进入Web管理界面，此时设备为空配置。（不建议跳过“快速配置”，即使是旧设备升级到本版本，如果不走快速配置，也有可能流控、默认路由等功能异常）。
- 用户也可以通过Web管理主界面的右上角菜单中的“本地快速配置”来使用该功能。

【前置条件】

- 仅网关模式支持快速配置功能。
- 设备连接电源，用网线将设备WAN口与上级设备连接，或直接连接入户网线。
- 上网模式需根据当地网络运营商的要求进行配置，否则可能设置失败导致无法上网。建议先联系当地网络运营商确认上网方式为动态IP方式、宽带方式还是静态IP方式：
 - 如果是宽带上网（PPPoE），则需要宽带帐号和宽带密码。
 - 如果是静态IP，则需要IP地址、子网掩码、网关和DNS。

【操作步骤】

根据快速配置向导完成相关操作。

(1) 重置管理员密码。





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：

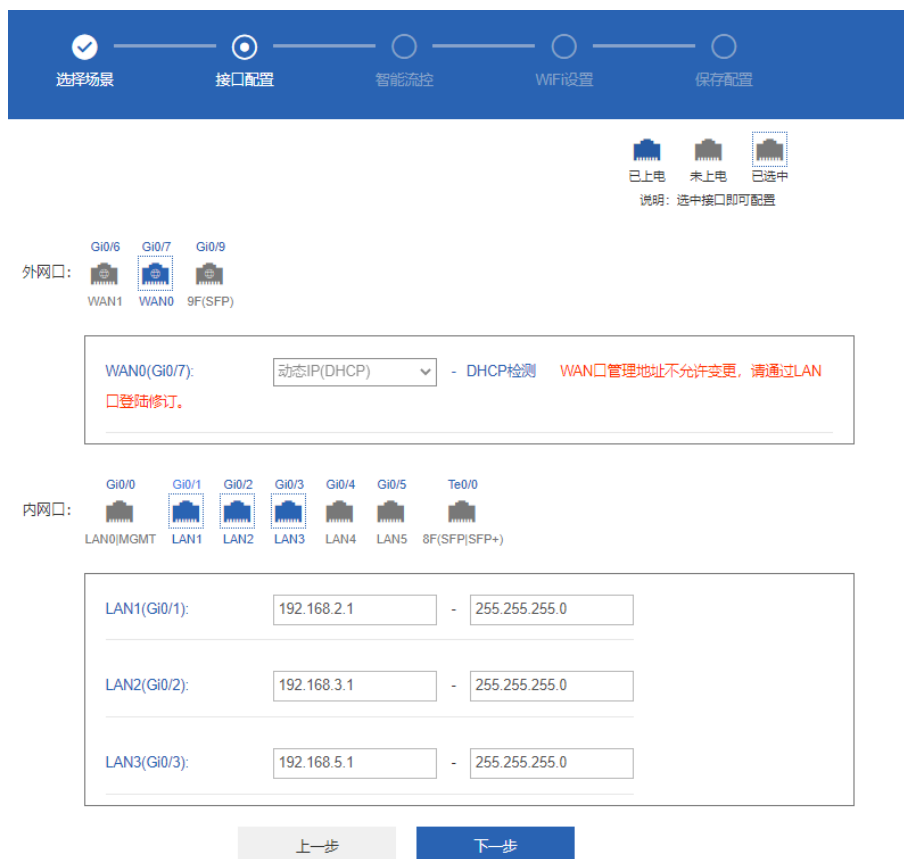
确认修改

- (2) 选择设备的应用场景，系统将根据不同的网络场景，生成适合的配置向导。下面以“中小企业”场景为例介绍快速配置功能。



- (3) 配置接口的IP地址。手动输入内网口的IP地址和掩码，外网口选择与运营商确认的上网方式：

- **动态IP (DHCP)**：设备检测DHCP能否获取地址上网，若成功联网，则无需输入帐号。
- **PPPoE (ADSL)**：宽带拨号上网，输入已准备好的宽带帐号和宽带密码。
- **静态IP地址**：输入已准备好的IP地址，掩码和网关IP地址。



- (4) 配置智能流控。在企业场景下，开启流控开关并填写线路带宽后，当带宽紧张时，将优先保证办公应用的流量。若用户的下行带宽超过100M或需要测速，则不建议开启流控。

 说明

线路带宽需要根据用户向运营商申请的实际带宽数据填写，请务必准确填写，以便设备能更智能地为用户管理带宽。



请填写线路带宽以配置智能流控，可以实现带宽紧张的时候，优先保证办公应用，让企业办公无忧。如果您的下行带宽超过100M或需要测速，不建议开启流控。

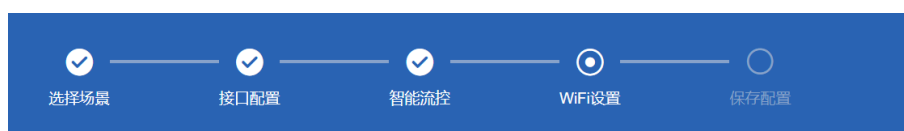
Gi0/6 WAN1	流控开关: ☐ OFF
Gi0/7 WAN0	流控开关: ☐ OFF
Gi0/9 9F(SFP)	流控开关: ☒ ON 下行: 上行: 100 - 100 Mbps

上一步 下一步

- (5) 配置Wi-Fi。输入Wi-Fi信号的名称和密码，该无线配置将下发至网关设备所管理的下联AP，使用户能够通过对应Wi-Fi名称和密码连接无线网络。

 说明

RG-NBR系列网关自身不支持发射无线Wi-Fi信号，Wi-Fi设置需下发至下联AP才能实际生效。



通过NBR管理内网AP，请设置WiFi名称和WiFi密码

WiFi名称: *

WiFi密码: ☐ 显示密码

上一步 下一步

暂不配置> 

- (6) 点击<下一步>，保存配置。配置下发需要一定时间，请耐心等待。



正在下发配置，请勿做其它操作，请稍候...



通过微信扫码或输入诺客账号，完成设备配置

微信扫一扫

诺客账号



刷新二维码



扫码进入小程序，开启云管之旅

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

配置清单



【后续处理】

根据界面提示，依次完成以下操作：

- (1) 微信扫码或输入诺客账号，可对接诺客云，对设备进行远程配置管理。

通过微信扫码或输入诺客账号，完成设备配置

微信扫一扫

诺客账号



Hello!

确认

(2) 点击<配置清单>，了解当前接口配置。

配置清单

▼

●接口配置

Gi0/4
WAN0

上网方式: 动态IP(DHCP)
办公模板流控: 开启 上行带宽: 100Mbps
下行带宽: 100Mbps

Gi0/0
LAN0

IP地址: 192.168.3.1 子网掩码: 255.255.255.0

说明:

当wan口配置为DHCP或PPPoE时，具体IP地址请至系统首页-接口信息中查看（如下图示）。

Dashboard

In

Static IP address:
192.168.20.1

0MGMT

1

2

Configured

Configured

Configured

(3) 点击<接口配置>，进行接口配置。

接口配置是实现内部上网的关键配置，正确配置接口信息才能确保内网可以正常上网。

- 内网口配置：选中用户要配置的内网口，然后在下面的输入框中输入IP地址和子网掩码即可。



LAN0(Gi0/0): 192.168.1.1 - 255.255.255.0

- 外网口配置：选中要配置的外网口，并依次设置客户端IP分配方式、带宽信息和线路类型等信息。
 - 当客户端上网方式选择“静态IP地址”时，需要设置运营商提供的IP地址、子网掩码和网关IP地址。



WAN1(Gi0/4): 动态IP(DHCP)

WAN0(Gi0/5): 静态IP地址

接口IP: 10.10.10.100 - 255.255.255.0 - 10.10.10.1

- 当客户端上网方式为向运营商申请的ADSL线路，则选择“PPPoE(ADSL拨号)”，并填写运营商提供的宽带帐号和密码。

WAN0(Gi0/5): PPPoE(ADSL拨号) - 获取账号

账号信息: 用户名 - 密码 ☐ 显示密码

- 当客户端上网方式选择“动态IP(DHCP)”，则接口自动获取IP地址，不需要其他额外配置。

下一步

- (4) 配置完以上选项后用户只需要点击 下一步 按钮就可以完成配置。此时，可以通过Web管理界面管理网络运行状况。

3.2 睿易一体化配置

【应用场景】

当组网环境中接入新的设备后，可以通过发现新网络功能完成一体化配置。

【操作步骤】

- (1) 点击状态区的<发现新网络>，系统弹出界面显示当前组网信息。





(2) 点击<开始配置>，按照界面提示输入网络项目名称并配置端口IP。



(3) 点击<创建项目并连通网络>，系统下发配置信息。

(4) 配置完成后，系统提示配置成功。可以扫码接入诺客云进行远程管理。

The image shows the Ruijie login interface. At the top, there is a blue header with the Ruijie logo and the text "锐捷 | 睿易". Below the header, the main content area is white. In the center, there is a prompt: "请微信扫码或输入账号, 继续下一步配置" (Please scan the WeChat QR code or enter the account number to continue the next step configuration). Below this prompt, there are two buttons: "微信扫一扫" (WeChat Scan) and "手机号登录" (Login with Phone Number). Below the buttons is a large QR code with the Ruijie logo in the center. At the bottom of the QR code, there is a small green circular icon with a white 'P' inside. Below the QR code, there is a small text prompt: "温馨提示: 支持微信扫一扫注册登录" (Warm reminder: Support WeChat scan registration and login). At the very bottom of the interface, there is a footer with the text: "©2008-2020 锐捷网络 | 在线客服 | 电话: 4001 600 078".

 说明

如果用户更改了接口IP地址，需要重新在浏览器地址栏中输入新的IP地址才能访问Web管理系统。

4 首页

4.1 系统首页



登录Web管理界面后会自动会转到系统首页，用户也可以通过菜单区点击 [系统首页](#) 跳转到系统首页。

在该页面，用户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。用户还可以通过查看本日流量走势、本日应用流量TOP10和本日用户流量TOP10等流量统计信息，全方位地监控和分析内部网络流量的当前状态，发现和定位常见的网络问题，并快速解决问题。

4.1.1 接口信息

系统首页左侧上方显示了接口的连接状态，点击接口图标可以查看该接口的基本信息，包括：接口类型、联网方式和IP地址等。



4.1.2 设备概况

系统首页页面右侧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、系统时间等概况信息。



表4-1 设备概况信息说明

信息	说明
CPU	当前设备的CPU使用率
内存	当前设备的内存使用率以及总内存大小
硬盘	当前设备的硬盘使用率。当设备安装了硬盘模块时会显示。
在线用户数	当前设备的下联在线用户总数
设备时间	显示系统当前时间 - 如果当前系统时间有误，或需要重新设置系统时间，可点击[运维]>>[系统设置]>>[系统时间]菜单项重新设置。 - 当设备时间和管理PC时间相差超过1小时时，“设备时间”旁会出现告警图标。点击告警图标，将进入系统时间配置界面。 设备时间:  1970-01-07 23:39:03 NBR6120-E NBR_RGOS 11.9(6)B14 详细
详细	单击<详细>，可以查看设备的启动时间、运行时间、硬件版本、软件版本等信息。

4.1.3 带宽状态

系统首页显示了系统带宽状态。在该功能页面用户可以通过图表查看到当前设备最近一小时的流量走势、本日应用流量TOP10的带宽使用率、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：

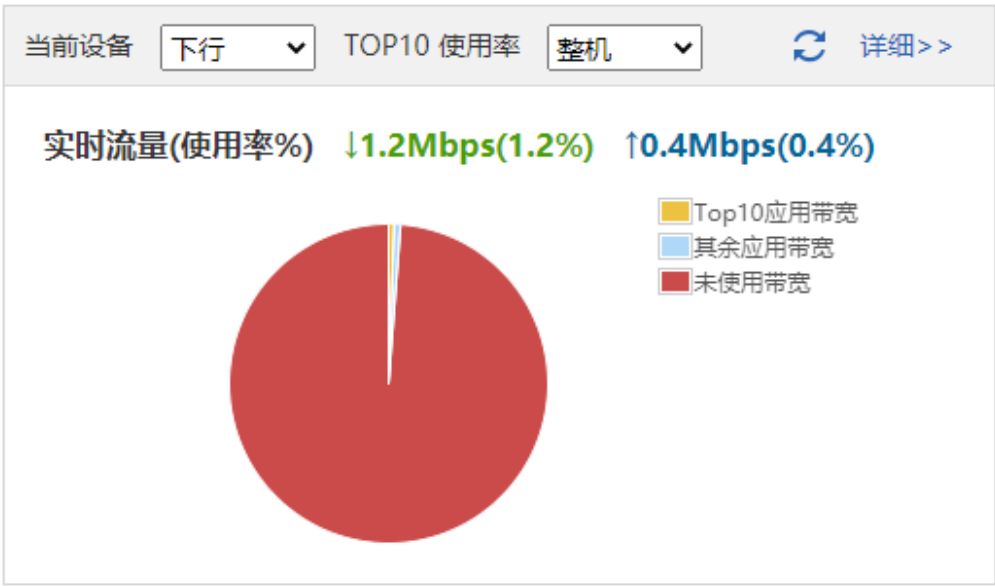


- 在流量走势图中，黄色曲线显示的是“流控抑制前的流量”走势，蓝色曲线显示的是受流控抑制后实际通过的流量走势。

- 用户可以更改接口 **整机** 及 **下行流量** 来查看各接口的流量走势。
- 鼠标移至走势曲线上的点可以查看所在位置的“流控抑制前流量”和“通过的流量”。
- 点击 **流量抑制前流量** 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势曲线。

● 本日应用流量TOP10的带宽使用率

以图表形式展现了实时流量TOP10的应用占总带宽的比例。



● 本日应用流量TOP10

当前应用 下行 最近10分钟的流量TOP10 刷新 详细>>

排行	应用程序	流量 Kb	应用类型
1	普通网页浏览	↓99.3Kb / 15.9Kb	普通/其他类
2	DNS	↓21.9Kb / 18.9Kb	关键/保证类
3	TCP交互应用	↓17.0Kb / 117.4Kb	普通/其他类
4	正在识别的应用	↓0.6Kb / 11.1Kb	关键/保证类
5	NETBIOS-DGM	↓0.0Kb / 11.5Kb	普通/其他类
6	NETBIOS-NS	↓0.0Kb / 13.0Kb	普通/其他类

○ 如上图所示，表格显示了流量TOP10的应用。点击<详细>可查看应用流量详情。

○ 通过修改 下行 下拉框中的选项，可分别查看最近十分钟的上/下行流量TOP10应用。

● 本日用户流量TOP10

表格显示了占用流量TOP10的用户。

当前用户 下行 流量 TOP10 整机 刷新 [详细>>](#)

排行	用户	IPv4地址	在线时长	流量 Kbps
1	/192.168.3.2	192.168.3.2	0小时0分4秒	↓553.1Kbps / ↑250.8Kbps

● 本日用户会话数TOP10

用户会话数 TOP10 整机 刷新

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

- 如上图所示，表格显示了流量TOP10的用户。
- 通过修改 整机 下拉框中的接口选项，可查看指定接口的会话数TOP10用户。

4.1.4 主程序推送

当设备联网且检测到最新版本时，会自动弹出“新主程序升级提醒”对话框。点击<跳转主程序下载和升级>下载最新的升级包并完成升级。

新主程序升级提醒

最新主程序版本：NBR_RGOS 11.9(0)B3PO1, Release(05151416)

建议马上下载bin文件主程序并升级，解决问题有：

一、新增网关产品防弱密码功能

二、内容审计改进如下点：
1、文件精细化控制
2、FTP审计
3、TELNET审计

三、流表容量提升
EG3000CESE由200W提升到400W，EG2000F由3W提升到10W

四、EG支持桥模式计费、双机认证方案

五、应用路由放开完整特征库
把超神的应用路由的完整功能变成通用功能，全系列支持。指标上明确可以支持应用路由娱乐类场景甩流，包括如下几个大类：HTTP协议、网络游戏软件、视频流媒体软件、P2P应用软件

跳转主程序下载和升级

4.2 功能管理

【应用场景】

本功能用于关闭设备不常使用的功能。
关闭后的功能不会在后台运行，也不会开机启动，相应的Web页面也不会显示。

 注意

部分情况下，启动和关闭功能需要重启设备才能生效。以页面提示信息为准。

【操作步骤】

(1) 点击[首页]>>[功能管理]菜单项。

功能管理

说明：这里可以关闭不常使用的功能服务。关闭后的功能不会在后台运行，也不会开机启动，相应的WEB页面也不会显示。
注意：部分情况下，启动和关闭功能需要重启设备才能生效。

功能名称	功能状态	功能描述	操作
缓存加速	停止	提供资源加速、应用缓存、悬浮窗广告等功能 注意：开关本功能要求重启设备 页面：【高级--加速-应用缓存】【高级--加速-资源加速】【高级--悬浮窗广告】	启动
SSLVPN	运行	SSLVPN是一种安全远程访问技术，能够通过WEB浏览器或者专用客户端与企业内部服务器建立安全的传输通道 页面：【网络--SSLVPN配置】	停止
集中管理	停止	支持RAC-SNC集中管理功能 页面：【高级--集中管理】	启动
服务器日志	停止	提供和SNC服务器、ELOG服务器对接的服务器日志功能 页面：【高级--系统日志--服务器日志】	启动
第三方日志	停止	提供第三方日志服务器配置和对接功能 页面：【高级--第三方日志】	启动

(2) 选择待关闭的功能，在“操作”列点击<停止>。

功能名称	功能状态	功能描述	操作
缓存加速	停止	提供资源加速、应用缓存、悬浮窗广告等功能 注意：开关本功能要求重启设备 页面：【高级--加速-应用缓存】【高级--加速-资源加速】【高级--悬浮窗广告】	启动
SSLVPN	运行	SSLVPN是一种安全远程访问技术，能够通过WEB浏览器或者专用客户端与企业内部服务器建立安全的传输通道 页面：【网络--SSLVPN配置】 本设备支持SSLVPN集中管理模式	停止

(3) 系统弹出提示信息，点击<确定>。

【后续处理】

点击<启动>可以重新开启对应的功能。

功能名称	功能状态	功能描述	操作
缓存加速	停止	提供资源加速、应用缓存、悬浮窗广告等功能 注意：开关本功能要求重启设备 页面：【高级--加速-应用缓存】【高级--加速-资源加速】【高级--悬浮窗广告】	启动

4.3 接口连接状态

【操作步骤】

选择[首页]>>[接口连接状态]，可以查看各个接口的状态信息，包括IP地址、速率、DNS、连接状态等。

 说明

若设备不支持IPv6特性，则不显示IPv6地址。

接口连接状态						
说明：可以查看协商后的双工速率及接口当前的状态。						
接口	IP地址/掩码	光电口	双工	速率	DNS	状态
GigabitEthernet 0/0	192.168.3.1/24	电口	自协商	自协商		未连接
GigabitEthernet 0/1		电口	自协商	自协商		未连接
GigabitEthernet 0/2		电口	自协商	自协商		未连接
GigabitEthernet 0/3		电口	自协商	自协商		未连接
GigabitEthernet 0/4	172.26.1.58/24	电口	双工	100M		连接
显示 10 条 共5条						
◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶ 1 确定						

5 常用功能

【应用场景】

通过本功能，用户可以了解设备的常用操作，并获取配置样例。

【操作步骤】

(1) 选择[常用]>>[常用功能]，进入常用功能页面。



(2) 选择需要了解的常用功能，点击<配置样例>获取相关功能的配置示例。点击功能名称，可直接跳转至对应设置页面。

6 行为管理

6.1 流量监控

6.1.1 功能简介

流量监控模块用于统计当前网络流量的使用情况，用户可以根据监控信息了解当前网络的运行状态，并对具体的应用进行智能分析。

6.1.2 实时流量

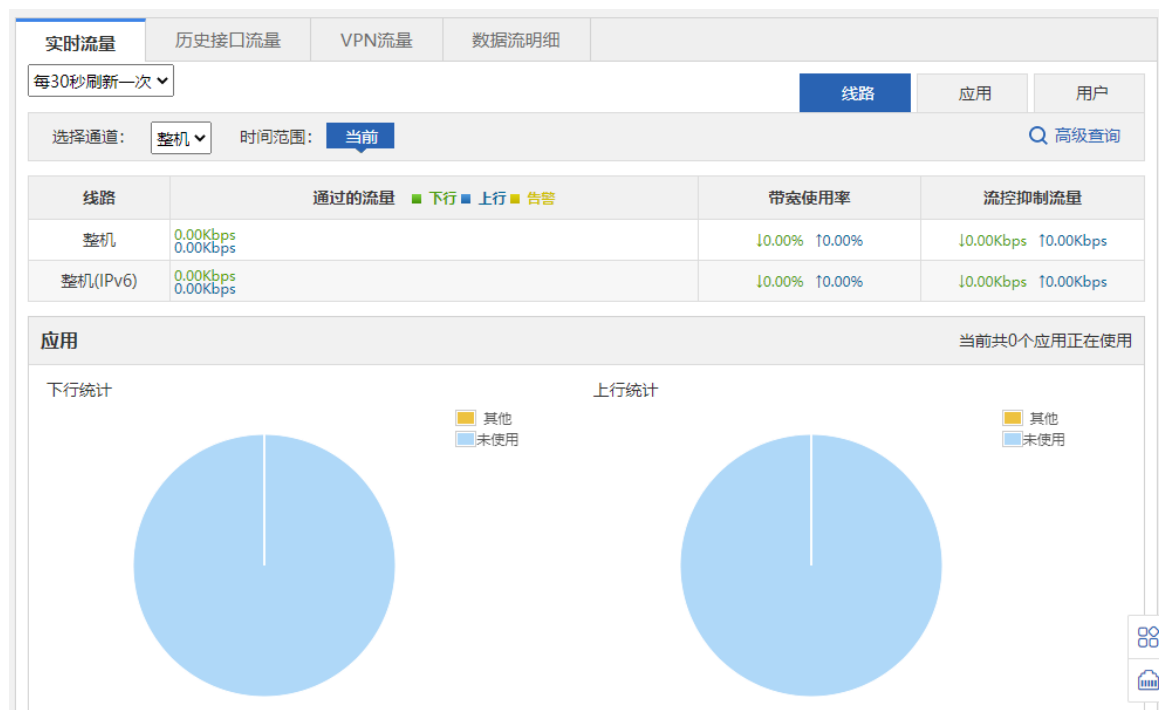
1. 功能概览

【应用场景】

管理员可以分别基于线路、应用和用户视角，查看实时的流量统计数据。

【操作步骤】

(1) 选择[行为管理]>>[流量监控]>>[实时流量]。



(2) 选择数据刷新频率。

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。



(3) 通过切换 **线路** **应用** **用户** 标签可以分别查看基于线路、应用或用户的设备流量统计信息。



(4) 通过在 **整机** 下拉框中选择接口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。



(5) 时间范围显示 **当前** 表示正在查看当前的流量信息。

(6) 点击 **高级查询** 将弹出高级查询功能窗口，可以查看流量、在线用户数、会话数等明细：



高级查询

流量 在线用户数 会话数

时间类型：☒ 当前 ☐ 日表 ☐ 周表 ☐ 月表

名称：应用

选择接口：整机

确定查询

- 查询流量明细：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。

a 选择<流量>，然后点击名称后方的下拉框，选择查询类型。选择好类型后，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：

高级查询

流量 在线用户数 会话数

时间类型：☒ 当前 ☐ 日表 ☐ 周表 ☐ 月表

名称：应用

选择接口：

应用
应用组
用户
用户组
外部用户
IP
应用类型

确定查询

b 选择接口，点击 ，将弹出查询结果。

高级查询

流量 在线用户数 会话数

名称：应用

选择接口：整机

确定查询

说明

若设备配置了硬盘，支持选择查询的时间区间。在“时间类型”中选择当前、日表、周表或月表，可查看对应的统计数据。

报表查询结果 高级查询

查询日期: 当前
 查询应用: 所有应用
 查询线路: 整机

当前在线数

排行	名称	查看明细	通过的流量 ■ 下行 ■ 上行	流控抑制流量
显示: 10 条 共0条	首页 上一页 1 下一页 末页 确定			

流量明细

排行	名称	ipv4地址	通过的流量 ■ 下行 ■ 上行	流控抑制流量
显示: 10 条 共0条	首页 上一页 1 下一页 末页 确定			

- 查询在线用户数明细：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。

a 选择<在线用户数>，并选择查询的线路。

高级查询

流量 **在线用户数** 会话数

时间类型: ☒ 当前 ☐ 日表 ☐ 周表 ☐ 月表

选择接口: 整机

确定查询

说明

若设备配置了硬盘，支持选择查询的时间区间。在“时间类型”中选择当前、日表、周表或月表，可查看对应的统计数据。

b 点击 **确定查询**，将弹出查询结果。

报表查询结果 高级查询

查询日期: 当前
 查询类型: 用户数
 查询线路: 整机

用户数统计

在线用户数
1

- 查询会话数明细：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。

a 选择<会话数>，并选择查询的线路。

说明

若设备配置了硬盘，支持选择查询的时间区间。在“时间类型”中选择当前、日表、周表或月表，可查看对应的统计数据。

b 点击 ，将弹出查询结果。

报表查询结果

高级查询

查询日期：当前

查询类型：会话数

查询线路：整机

会话数统计

会话数
17

2. 接口流量分析

该功能是把带宽的使用情况分别按不同的线路（接口）进行统计，用户可以对线路（接口）的流量进行控制和分析，以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：



【线路流量信息概况】

页面第一部分显示指定线路的流量信息。当线路选择“整机”时，将同时显示所有线路的流量总和的信息，以及各条线路的流量信息。



通过上图的流量信息，可以查看当前流量是否正常（有无出现告警），如果流量过高会出现黄色告警，来帮助用户快速定位带宽问题。

说明

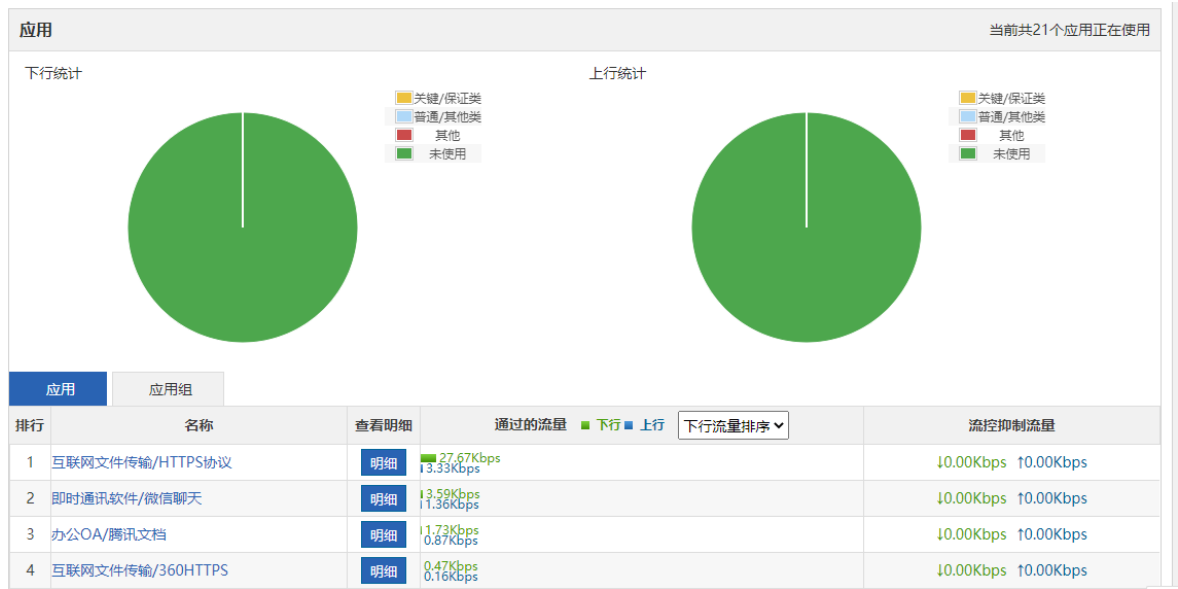
黄色告警出现的条件：总流量达到了线路带宽（用户向电信等运营商申购的带宽）的95%以上。

出现黄色告警后的解决办法：

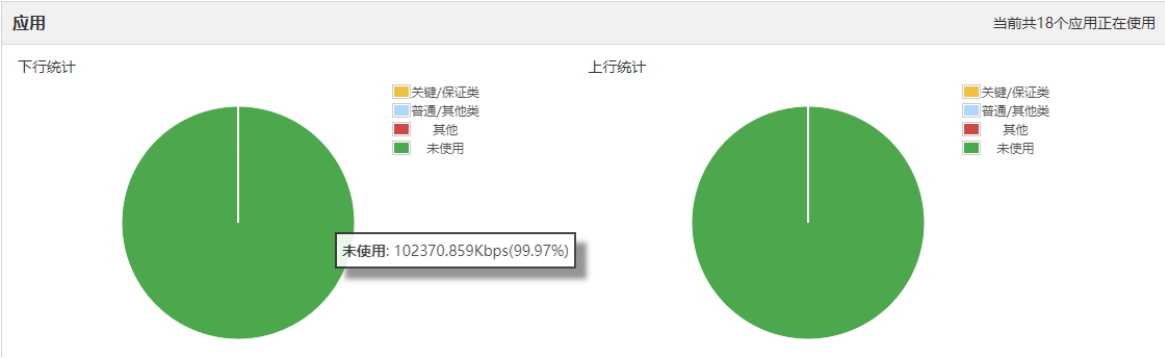
- 当只有总流量出现黄色告警，且“关键/保证类应用组”的流量与总流量相当，那么就到[行为管理]>>[流控策略]或[行为管理]>>[对象定义]>>[自定义应用分组]页面查看是否选择的应用都属于用户要保证的应用，如果确定都是需要保证的应用，那么说明当前带宽比较紧张，可以向运营商申请添加带宽，来解决问题，确保机构办公流畅。
- 当总流量出现黄色告警，且“抑制类应用组”带宽使用较大，那么此时可以先限制抑制应用组的流量，来解决流量过高的问题。
- 总流量出现告警，普通/其他类应用组的流量和抑制组的流量相当，那么用户可以依次限制抑制应用组、普通应用组的流量，来解决流量过高的问题。

【线路的应用流量信息】

页面中间部分显示了指定线路的应用流量信息，包括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流量、具体为哪些应用，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：



- 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，以及占据所选线路上/下行的流量总和的百分比。
- 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。

应用组

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	查看明细	通过的流量	下行流量排序	流控抑制流量
1	互联网文件传输	明细	28.08Kbps 13.30Kbps		↓0.00Kbps ↑0.00Kbps
2	办公OA	明细	13.13Kbps 11.15Kbps		↓0.00Kbps ↑0.00Kbps
3	即时通讯软件	明细	11.65Kbps 11.76Kbps		↓0.00Kbps ↑0.00Kbps
4	视频会议	明细	0.40Kbps 0.50Kbps		↓0.00Kbps ↑0.00Kbps
5	HTTP协议	明细	0.14Kbps 0.39Kbps		↓0.00Kbps ↑0.00Kbps

点击 明细 将弹出以下窗口：

应用组：

互联网文件传输

当前的流量(Kbps)

线路	下行	上行	流控抑制流量	操作
整机	26.33	2.36	↓0.00Kbps ↑0.00Kbps	阻断流量

用户

应用

排行	名称	本地用户	ipv4地址	通过的流量	下行	上行	流控抑制流量	操作
1	/192.168.3.2	192.168.3.2	26.96Kbps ↓2.42Kbps	↓0.00Kbps ↑0.00Kbps	明细			

显示:10条共1条

◀ 首页

◀ 上一页

1

下一页 ▶

末页 ▶

1

确定

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。

【线路的用户流量信息】

页面底端部分显示当前线路的用户流量使用情况，包括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：

用户

当前共1个用户在线

在线用户数

1

会话数

28

用户

用户组

排行	名称	本地用户	ipv4地址	在线时长	查看明细	通过的流量	下行	上行	流控抑制流量
1	/192.168.3.2	192.168.3.2	1小时21分42秒	明细	31.96Kbps ↓5.44Kbps	↓0.00Kbps	↑0.00Kbps		

显示: 10 条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶ 1 确定

通过在下拉框中选择用户类型，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：

名称 192.168.3.2	部门 root
-------------------	------------

当前的流量(Kbps)

线路	下行	上行	流控抑制流量	操作
整机	35.71	8.98	↓0.00Kbps ↑0.00Kbps	阻断流量

当前的应用

排行	名称	通过的流量 ■ 下行 ■ 上行	流控抑制流量
1	互联网文件传输/HTTPS协议	27.16Kbps 12.72Kbps	↓0.00Kbps ↑0.00Kbps
2	办公OA/腾讯文档	7.93Kbps 5.16Kbps	↓0.00Kbps ↑0.00Kbps
3	视频会议/Umeet	0.40Kbps 0.50Kbps	↓0.00Kbps ↑0.00Kbps
4	即时通讯软件/QQ协议相关	0.37Kbps 0.24Kbps	↓0.00Kbps ↑0.00Kbps

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。

3. 应用流量分析

该功能实现了分别根据不同的应用软件对带宽的使用情况进行统计，您可以对应用的流量进行控制和分析，以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：

实时流量	历史接口流量	VPN流量	数据流明细
每30秒刷新一次	选择通道：整机	时间范围：当前	线路 应用 用户
应用类型	通过的流量 ■ 下行 ■ 上行	带宽使用率	流控抑制流量
关键/保证类	1.67Kbps 1.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps
抑制类	0.04Kbps 0.04Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps
普通/其他类	27.44Kbps 3.01Kbps	↓0.03% ↑0.00%	↓0.00Kbps ↑0.00Kbps
关键/保证类 当前共10个应用正在使用			
应用	用户		
排行	名称	查看明细	通过的流量 ■ 下行 ■ 上行
1	办公OA/腾讯文档	明细	0.49Kbps 0.09Kbps
2	视频会议/Umeet	明细	0.40Kbps 0.50Kbps
3	即时通讯软件/QQ协议相关	明细	0.37Kbps 0.24Kbps
4	HTTP协议/普通网页浏览	明细	0.26Kbps 0.08Kbps
5	协议类/DNS	明细	0.11Kbps 0.04Kbps

页面由上至下分别显示了整机应用流量概览信息和关键/保证类、普通/其他类、抑制类三种类型的应用的流量信息。

● 应用流量概况

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。

实时流量	历史接口流量	VPN流量	数据流明细	
每30秒刷新一次				线路应用用户
选择通道: 整机	时间范围: 当前			高级查询
应用类型	通过的流量	下行	上行	带宽使用率
关键/保证类	9.26Kbps	7.18Kbps		↓0.01% ↑0.01%
抑制类	0.00Kbps	0.06Kbps		↓0.00% ↑0.00%
普通/其他类	27.48Kbps	13.24Kbps		↓0.03% ↑0.00%

- 关键/保证类应用流量分析：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。

关键/保证类					当前共10个应用正在使用
应用	用户				
排行	名称	查看明细	通过的流量	下行	上行
1	办公OA/腾讯文档	明细	↓6.37Kbps	↑4.64Kbps	
2	HTTP协议/普通网页浏览	明细	↓1.75Kbps	↑1.53Kbps	
3	视频会议/Umeet	明细	↓0.40Kbps	↓0.50Kbps	
4	即时通讯软件/QQ协议相关	明细	↓0.37Kbps	↓0.24Kbps	
5	协议类/DNS	明细	↓0.22Kbps	↓0.09Kbps	

点击 **明细** 将弹出应用流量明细窗口，详见“[接口流量分析](#)”章节中的应用流量明细窗口的分析。

关键/保证类				
应用	用户			

上图显示的是关键/保证类应用的流量信息，点击 **用户** 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：

关键/保证类					当前共11个应用正在使用
应用	用户				
排行	名称	本地用户	IPV4地址	查看明细	通过的流量
1	/192.168.3.2	192.168.3.2	明细	↓16.20Kbps	↓25.89Kbps
显示: 10 条 共1条					1 确定

点击 **明细** 将弹出用户流量明细窗口，详见“[接口流量分析](#)”章节中的用户流量明细窗口的分析。

- 普通/其他类应用流量分析：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。

普通/其他类					当前共8个应用正在使用
应用	用户				
排行	名称	查看明细	通过的流量	下行	上行
1	互联网文件传输/HTTPS协议	明细	↓32.00Kbps	↓4.69Kbps	
2	软件更新/360软件下载	明细	↓0.65Kbps	↓0.33Kbps	
3	软件更新/WINDOWSUPDATE	明细	↓0.40Kbps	↓0.07Kbps	
4	RFC/未知80端口	明细	↓0.37Kbps	↓0.02Kbps	

点击 **明细** 将弹出应用流量明细窗口，详见“[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 **用户** 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：

普通/其他类					
当前共9个应用正在使用					
应用		用户			
排行	名称	本地用户	IPV4地址	查看明细	通过的流量
1	/192.168.3.2		192.168.3.2	明细	30.15Kbps 4.02Kbps
					流控抑制流量
					↓0.00Kbps ↑0.00Kbps

点击 **明细** 将弹出用户流量明细窗口，详见“[接口流量分析](#)”章节中的用户流量明细窗口的分析。

- 抑制类应用流量分析：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。

抑制类					
当前共1个应用正在使用					
应用		用户			
排行	名称	本地用户	IPV4地址	查看明细	通过的流量
1	IP协议组/UDP交互应用			明细	0.00Kbps 0.04Kbps
					流控抑制流量
					↓0.00Kbps ↑0.00Kbps

显示: 10 条共1条

首页 < 上一页 1 下一页 > 末页

1 确定

点击 **明细** 将弹出应用流量明细窗口，详见“[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 **用户** 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：

抑制类					
当前共1个应用正在使用					
应用		用户			
排行	名称	本地用户	IPV4地址	查看明细	通过的流量
1	/192.168.3.2		192.168.3.2	明细	0.00Kbps 0.04Kbps
					流控抑制流量
					↓0.00Kbps ↑0.00Kbps

点击 **明细** 将弹出用户流量明细窗口，详见“[接口流量分析](#)”章节中的用户流量明细窗口的分析。

4. 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。如果网络内存在大量用户，用户数据过多，还可以通过用户名或IP地址

段对当前用户进行过滤。点击实时流量页面导航菜单栏中的 **用户** 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 **明细** 将弹出用户流量明细窗口，详见“[接口流量分析](#)”章节中的用户流量明细窗口的分析。
用户组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可以按照用户组来查看和管理流量。

说明
要配置“用户组”，请在[安全认证]>>[用户组织]>>[用户管理]中配置，参见[7.1.1 用户管理](#)章节。

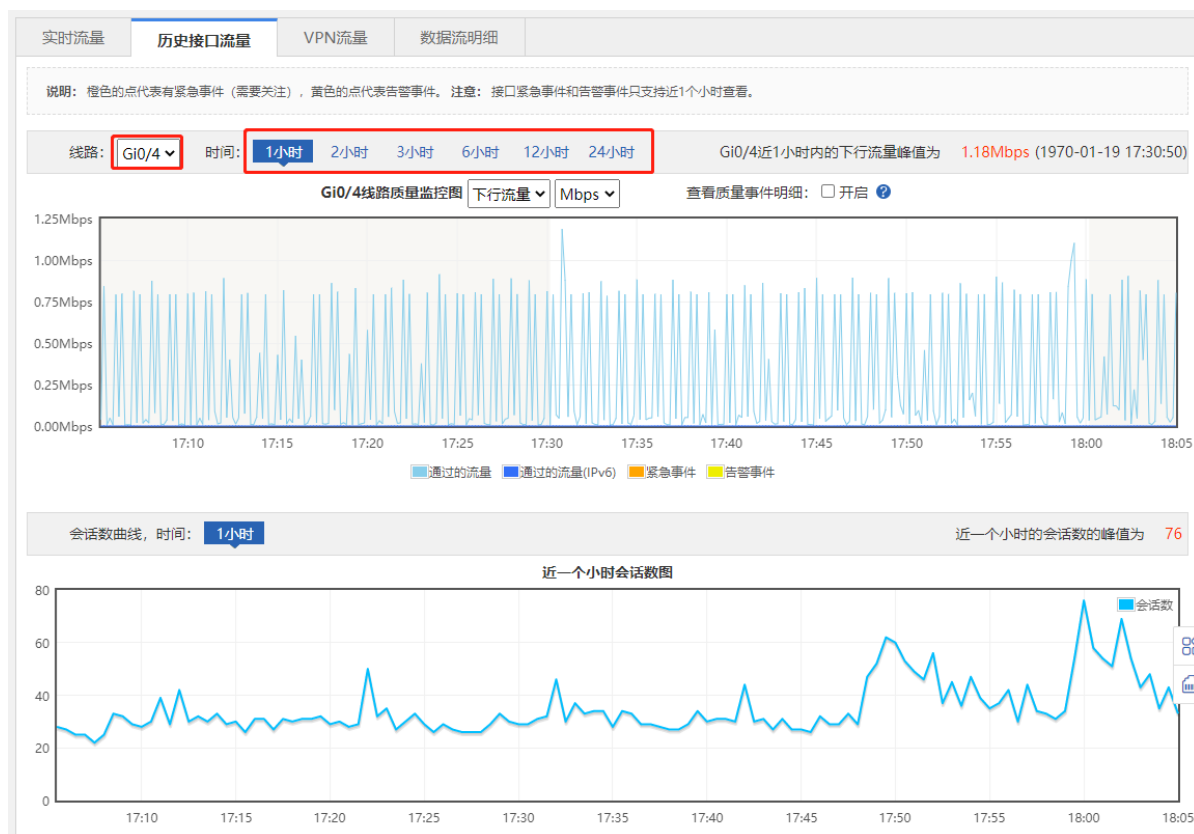
6.1.3 历史接口流量

【应用场景】

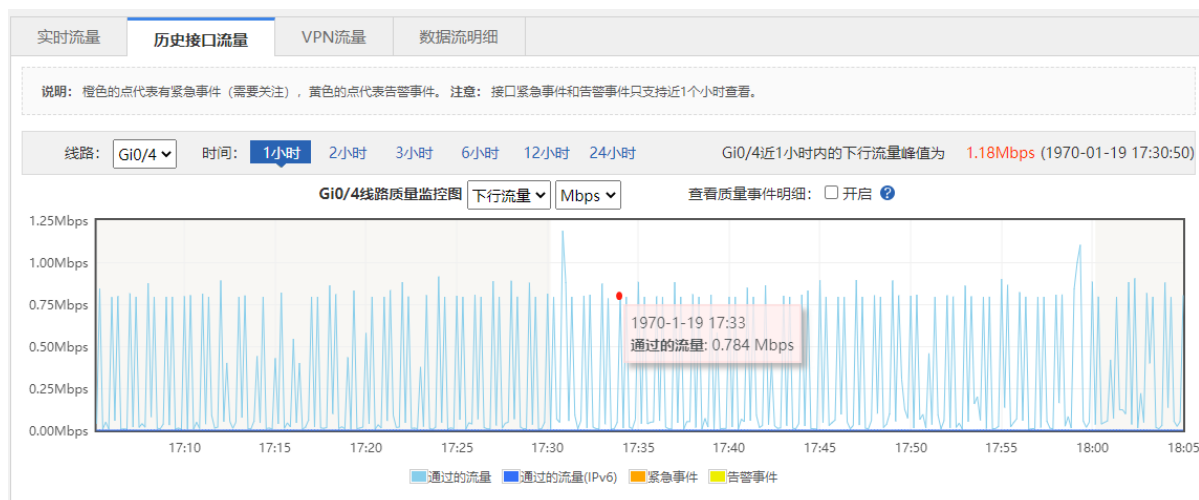
历史接口流量功能主要用于查看实时的接口流量和在单位时间的具体的实时曲线图。用户可以查看到一天内的实时监测流量曲线。

【操作步骤】

- (1) 点击[行为管理]>>[流量监控]>>[历史接口流量]菜单项。
- (2) 选择待监控的线路和监控的时间段。



(3) 鼠标移至监控曲线上的折点，可查看该时刻的流量或用户会话数。



6.1.4 VPN 流量

【应用场景】

用于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。

【操作步骤】

(1) 点击[行为管理]>>[流量监控]>>[VPN流量]菜单项。

实时流量

历史接口流量

VPN流量

数据流明细

选择通道:

Gi0/4

时间范围:

当前

每30秒刷新一次

审计对象:

基于外网IP

高级查询

排行

用户名

ipv4地址

查看明细

通过的流量

下行

上行

流控抑制流量

显示:

10

 条 共0条

首页

上一页

1

下一页

末页

1

确定

(2) 设置查询条件。

- 通过在

Gi0/4

 下拉框中选择接口，可以选择查看指定线路的VPN流量使用情况。
- 通过在

每30秒刷新一次

 中选择刷新频率，可以选择每隔10秒、30秒、1分钟自动刷新设备的当前VPN流量信息，也可以选择手动刷新设备的当前VPN流量信息。
- 通过

高级查询

 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

确定查询

。

说明

若设备配置了硬盘，支持选择查询的时间区间。在“时间类型”中选择当前、日表、周表或月表，可查看对应的统计数据。

高级查询

时间类型:

当前

日表

周表

月表

时间范围:

查看实时流量情况

名称或IP:

选择接口:

Gi0/6

确定查询

排行	用户名	基于外网IP查询	IP地址	查看明细	通过的流量 下行 上行	流控抑制流量
1	/192.168.1.2		192.168.1.2	明细	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps
2	/192.168.10.2		192.168.10.2	明细	172.00Kbps 359.55Kbps	↓0.00Kbps ↑0.00Kbps
3	/192.168.1.21		192.168.1.21	明细	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps
4	/192.168.1.25		192.168.1.25	明细	0.02Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps

首页

上一页

1

下一页

末页

1

确定

6.1.5 数据流明细

【应用场景】

用户在当前页面可以根据IP地址查看数据流信息。

【操作步骤】

- (1) 点击[行为管理]>>[流量监控]>>[数据流明细]菜单项。
- (2) 设置用户范围。可以选择显示所有用户的信息或只显示流量Top50或Top100的用户信息。

实时流量

历史接口流量

VPN流量

数据流明细

说明：可以根据IP地址查看流信息

用户范围：

Top50

Top100

所有

基于IP地址查询流信息：

查询

IP地址	上行流量	下行流量	流控抑制上行流量	流控抑制下行流量	操作
192.168.3.2	6.72 Kbps	33.89 Kbps	0.00 Kbps	0.00 Kbps	查看流信息

显示：

10

条 共1条

首页 < 上一页 1 下一页 > 末页

1

确定

- (3) 输入待查询的用户IP地址，点击<查询>。

用户范围：

Top50

Top100

所有

基于IP地址查询流信息：

查询

IP地址	上行流量	下行流量	流控抑制上行流量	流控抑制下行流量	操作
192.168.3.2	6.72 Kbps	33.89 Kbps	0.00 Kbps	0.00 Kbps	查看流信息

显示：

10

条 共1条

首页 < 上一页 1 下一页 > 末页

1

确定

- (4) 点击操作列的<查看流信息>，可查看用户数据流的具体信息，包括协议号、源/目的IP、源/目的端口、应用名称和收发报文字节数等。

用户范围：

Top50

Top100

所有

基于IP地址查询流信息：

查询

IP地址	上行流量	下行流量	流控抑制上行流量	流控抑制下行流量	操作
192.168.3.2	6.72 Kbps	33.89 Kbps	0.00 Kbps	0.00 Kbps	查看流信息

显示：

10

条 共1条

首页 < 上一页 1 下一页 > 末页

1

确定

IP 192.168.3.2 流信息

流ID	协议号	源IP	源端口	目的IP	目的端口	目的接口	应用名称	收到的字节数	发出的字节数
29990	TCP	192.168.3.2	59811	192.168.23.171	4430	Gi0/4	HTTPS协议	1770146	110662
29965	UDP	192.168.3.2	52936	114.114.114.114	53	Gi0/4	DNS	158	64
29955	TCP	192.168.3.2	52736	58.220.52.239	443	Gi0/4	HTTPS协议	6549	1734
29948	TCP	192.168.3.2	55623	112.49.10.97	443	Gi0/4	HTTPS协议	274655	511920
29937	UDP	192.168.3.2	53448	114.114.114.114	53	Gi0/4	DNS	164	67

6.2 流控策略

6.2.1 智能流控

【应用场景】

当用户需要对线路的上行流量和下行流量带宽进行合理控制时，可以选择开启智能流控功能。设置接口的线路带宽后，该接口下的流量将被限制在设置值范围内，同时将根据用户数量智能调整每个用户的带宽，保证每个用户

公平分享带宽。使用娱乐模板可以优先保证用户的游戏应用流量，使用办公模板可以优先保证用户的办公应用流量。

【操作步骤】

- (1) 点击[行为管理]>>[流量策略]>>[智能流控]菜单项。
- (2) 开启流控开关。

智能流控

说明：一键开启智能流量控制，娱乐模版可以优先保证您的游戏流量，办公模版可以优先保证您的办公流量。

注意：请确保下面配置线路带宽填写正确。

开启流控：☒ ON ☐

如需测试外网带宽的真实速度，可先暂时关闭流控功能

流控模板选择：

办公模板 ▾

接口：

☐ Gi0/3 ☐ Gi0/4

保存设置

- (3) 添加关联的应用模板。

开启流控：☒ ON ☐

如需测试外网带宽的真实速度，可先暂时关闭流控功能

流控模板选择：

办公模板 ▾

接口：

☒ Gi0/3 ☐ Gi0/4

保存设置

- (4) 选择接口并填写运营商分配的线路带宽。

开启流控: ☒ ON ☐ OFF 如需测试外网带宽的真实速度, 可先暂时关闭流控功能

流控模板选择: 办公模板 ▼

接口: ☒ Gi0/3 ☐ Gi0/4

Gi0/3

线路带宽: 下行	100	Mbps 上行	100	Mbps
----------	-----	---------	-----	------

保存设置

(5) 点击<保存设置>。

6.2.2 策略调整

【应用场景】

策略调整用于在智能流控功能的基础上进一步实现对特定用户或应用的流量限制, 从而满足网络规划或服务器的带宽需要。在创建流控策略时, 用户可以灵活配置受限的用户范围、用户的限制带宽值、受限的应用流量以及策略的生效时间等。

【操作步骤】

1. 新建流控策略

(1) 选择[行为管理]>>[流控策略]>>[策略调整]菜单项。

智能流控	策略调整	参数调整	应用调整	VPN流控																										
说明: 流量控制(Flow Control), 下面简称流控, 是一种区分不同用户、网段、应用的流量, 并进行有区别的转发和丢包的机制, 从而保证关键用户和应用流量, 抑制非关键应用的流量, 如P2P、网络游戏等。 注意: 由于流控功能升级, 以前版本配置的高级流控策略, 这个页面显示的策略可能不全, 需要重新配置, 建议先走快速配置/线路变更, 再到当前页面配置。 流控常见功能如何使用? + 添加策略 X 删除选中策略 选择接口线路: Gi0/4 ▼ <table border="1"><thead><tr><th>☐</th><th>策略名称</th><th>本地用户</th><th>外部用户</th><th>外网IP组</th><th>应用组</th><th>VPN</th><th>时间</th><th>流量管控</th><th>匹配顺序</th><th>启用</th><th>状态</th><th>管理</th></tr></thead><tbody><tr><td colspan="13">无记录信息</td></tr></tbody></table>					☐	策略名称	本地用户	外部用户	外网IP组	应用组	VPN	时间	流量管控	匹配顺序	启用	状态	管理	无记录信息												
☐	策略名称	本地用户	外部用户	外网IP组	应用组	VPN	时间	流量管控	匹配顺序	启用	状态	管理																		
无记录信息																														

(2) 点击 **+ 添加策略** 将弹出“添加策略”的设置窗口。

三 添加策略

策略名称:

选择用户:

所有用户

[【选择本地用户】](#)

所有用户

[【选择外部用户】](#)

选择应用组:

所有应用

[【自定义应用分组】](#)

流量限制:

☒ 限速 Kbps

(0表示不限制)

最大下载:

100000

保障下载:

0

每IP最大下载:

无限制

最大上传:

100000

保障上传:

0

每IP最大上传:

无限制

☐ 不限速

>> 高级选项

完成配置

取消

(3) 设置流控策略相关配置项。

- 策略名称：在“策略名称”输入框中输入能够标识该规则的名称。
- 选择用户：选择流控策略适用的用户，可以是本地用户或外部服务器用户。
- 选择应用组：在下拉框中选择已有的应用分组，若当前已有的应用分组不满足流控需求时可以点击[【自定义应用分组】](#)进行配置。

三 添加策略

策略名称:

选择用户:

所有用户

[【选择本地用户】](#)

所有用户

[【选择外部用户】](#)

选择应用组:

所有应用

[【自定义应用分组】](#)

自定义应用分组

+ 添加应用分组

应用分组名称	选择应用	操作
关键/保证类	DNS,即时通讯软件,IP网络电话,电子邮件协议,ICMP-DETAIL,VPN应用,办公OA,视频会议,即时通讯_MOBILE,WEB应用,QQ应用,网购_MOBILE,HTTP网络购物,微博,锐捷云,移动WEB应用,论坛PC,论坛-Mobile,旅行相关,旅行相关_Mobile,WEB邮箱,新闻资讯,新闻资讯_Mobile,WEB邮箱-Mobile,互联网金融,金融理财-Mobile,居家生活,阅读_MOBILE,阅读小说,教育相关,WEB_MOBILE,HTTP社交应用,社交_MOBILE,普通网页浏览明细	编辑
抑制类	其他TCP,其他UDP,TCP传输应用,UDP传输应用,TCP交互应用,UDP交互应用,网络游戏软件	编辑
阻断类	非法DNS	编辑
普通/其他类	HTTP协议,游戏_MOBILE,P2P应用软件,股票软件,视频类,协议类,数据库,物联网应用,远程访问协议,软件更新,网银 支付,电子邮件,互联网文件传输,网络硬盘,网盘_MOBILE,RFC,IP-RAW,IP协议组,网络管理协议,路由协议,网上支付 网上银行_MOBILE	默认组不能编辑

- 流量限制：可以选择“不限速”，所有用户共享带宽，不对单个用户限速；若开启限速，“保障上传/下载”、“最大上传/下载”分别为策略所限制的所有用户在当前接口下一共可使用的最低和最高带宽，“每用户最大上传/下载”为每个用户可使用的最大带宽。

点击 **>> 高级选项** 可展开更多高级设置。

高级选项

外网IP组: 所有外网IP **【选择IP组】**

生效时间: 所有时间 **【时间管理】**

VPN流控: ☐ 匹配VPN流量 (勾选后, 该条策略只对VPN用户生效)

- 外网IP组: 点击 **【选择IP组】** 进行选择IP组。
- 生效时间: 下拉框中可以选择已有的时间, 当已有时间段不满足流控需求时, 可点击 **【时间管理】** 手动配置。
- VPN流控: 勾选“匹配VPN流量”后, 该条流控策略只对VPN用户生效。

(4) 点击<完成配置>。

2. 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:

智能流控 **策略调整** 参数调整 应用调整 VPN流控

说明: 流量控制(Flow Control), 下面简称流控, 是一种区分不同用户、网段、应用的流量, 并进行有区别的转发和丢包的机制, 从而保证关键用户和应用流量, 抑制非关键应用的流量, 如P2P、网络游戏等。

注意: 由于流控功能升级, 以前版本配置的高级流控策略, 这个页面显示的策略可能不全, 需要重新配置, 建议先走快速配置/线路变更, 再到当前页面配置。 [流控常见功能如何使用?](#)

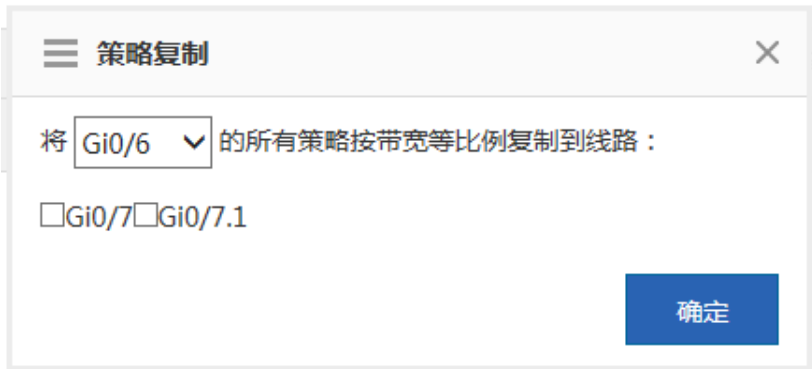
+ 添加策略 **× 删除选中策略** 选择接口线路: **GI0/4**

☐	策略名称	本地用户	外部用户	外网IP组	应用组	VPN	时间	流量管控	匹配顺序	启用	状态	管理
☐	test1	123	所有用户	所有外网IP	所有应用	否	所有时间	不限速		☒	生效	复制 编辑 删除
☐	test	所有用户	所有用户	所有外网IP	所有应用	否	所有时间	参数		☒	生效	复制 编辑 删除

显示: **10** 条 共2条 ◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶ **1** **确定**

- 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。
- 启用: 支持控制策略的启用和禁用。当策略被禁用时, 状态为“不生效”
- 状态: 包括“生效”和“不生效”两种状态, 若当前时间不在“生效时间”范围内, 或者策略被关闭, 则策略的状态显示为“不生效”。
- 匹配顺序: 流控策略适应“后配先生效”原则, 列表中自上而下排序靠前的策略优先匹配, 可以直接点击 、 按钮对现有策略的优先级进行调整。
- 点击 **编辑** 会弹出编辑对话框, 可以对策略进行编辑修改。
- 点击 **删除** 可以删除策略。

- 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。



6.2.3 参数调整

【应用场景】

在智能流控基础上，可根据具体情况调整总带宽的预留比例，以及各类型应用的带宽参数。

【操作步骤】

- (1) 点击[行为管理]>>[流控策略]>>[参数调整]。
- (2) 在左侧点击选择要修改的接口。



- (3) 如需修改当前线路的预留带宽比例，请点击<修改>；如需修改应用类型的承诺带宽和最大带宽，请点击对应行的<编辑>。修改完成后点击<完成>。速率的单位为Kbps。



6.2.4 应用调整

【应用场景】

在智能流控的基础上，可以根据实际需求调整应用模板包含的应用。

【操作步骤】

- (1) 点击[行为管理]>>[流控策略]>>[应用调整]。
- (2) 选择要修改的应用分组，点击<编辑>。在弹窗左侧勾选加入应用组的所有应用后，点击<保存>。



- (3) 点击<重置应用模板>可以将修改后的流控模板恢复至默认状态。

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

应用分组名称	选择应用	管理
关键/保证类	DNS,即时通讯软件,IP网络电话,电子邮件协议,ICMP-DETAIL,VPN应用,办公OA,视频会议,即时通讯_MOBILE,WEB应用,QQ应用,网购_MOBILE,HTTP网络购物,微博,锐捷云,移动WEB应用,论坛PC,论坛-Mobile,旅行相关,旅行相关_MOBILE,WEB邮箱,新闻资讯,新闻资讯_MOBILE,WEB邮箱-Mobile,互联网金融,金融理财-Mobile,居家生活,阅读_MOBILE,阅读小说,教育相关,WEB_MOBILE,HTTP社交应用,社交_MOBILE,普通网页浏览明细	编辑
抑制类	其他TCP,其他UDP,TCP传输应用,UDP传输应用,TCP交互应用,UDP交互应用,网络游戏软件	编辑
阻断类	非法DNS	编辑
普通/其他类	HTTP协议,游戏_MOBILE,P2P应用软件,股票软件,视频类,协议类,数据库,物联网应用,远程访问协议,软件更新,网银 支付,电子邮件,互联网文件传输,网络硬盘,网盘_MOBILE,RFC,IP-RAW,IP协议组,网络管理协议,路由协议,网上支付 网上银行_MOBILE	默认组不能编辑

显示15条共4条

首页上一页1下一页末页1确定

6.2.5 VPN 流控

【应用场景】

开启VPN流控后，可以保障VPN关键应用的流量，限制VPN用户带宽。

【操作步骤】

- (1) 点击[行为管理]>>[流控策略]>>[VPN流控]。
- (2) 选择要开启VPN流控的接口。

智能流控策略调整参数调整应用调整VPN流控

开启VPN流控：☐Gi0/4☒Gi0/3

☐保障VPN关键应用的流量

VPN关键通道带宽（注：需先开启对应通道vpn流控才能对VPN带宽设置）

保存配置

- (3) 如需保障VPN关键应用的流量，勾选“保障VPN关键应用的流量”，并选择VPN关键应用。

开启VPN流控: ☐ Gi0/4 ☒ Gi0/3

☒ 保障VPN关键应用的流量

-

所有应用

-

HTTP协议

+ WEB应用

+ QQ应用

+ 网购_MOBILE

+ HTTP网络购物

+ HTTP上传

+ HTTP下载

+ 移动WEB应用

+ 其他_MOBILE

+ 论坛PC

VPN关键通道带宽 (注: 需先开启对应通道vpn流控才能对VPN带宽设置)

保存配置

(4) 点击<保存配置>。

(5) 保存配置后, “VPN关键通道带宽” 旁出现<点击查看/编辑>按钮, 点击该按钮可查看和修改当前线路上VPN关键应用的可用带宽。

开启VPN流控: ☐ Gi0/4 ☒ Gi0/3

☒ 保障VPN关键应用的流量

-

所有应用

-

HTTP协议

+ WEB应用

+ QQ应用

+ 网购_MOBILE

+ HTTP网络购物

+ HTTP上传

+ HTTP下载

+ 移动WEB应用

+ 其他_MOBILE

+ 论坛PC

VPN关键通道带宽

点击查看/编辑

(注: 需先开启对应通道vpn流控才能对VPN带宽设置)

保存配置

VPN关键通道带宽编辑

选择通道

Gi0/3

下载网速: 保证 Mbps, 最大 Mbps, 每IP最大 Mbps;

上传网速: 保证 Mbps, 最大 Mbps, 每IP最大 Mbps;

保存配置

取消

(6) 完成修改后，点击<保存配置>。

6.3 对象定义

6.3.1 功能简介

为方便管理，可以将一些常用配置项抽象为对象，例如时间对象、应用组对象、VLAN对象等，用于设置流控或行为策略。

6.3.2 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。

自定义应用分组	自定义网站分组	时间对象	关键字组对象	外网IP对象	VLAN对象	IP对象	
+ 添加应用分组 + 自定义应用							
应用分组名称	选择应用						操作
关键/保证类	DNS,即时通讯软件,IP网络电话,电子邮件协议,ICMP-DETAIL,VPN应用,办公OA,视频会议,即时通讯_MOBILE,WEB应用,QQ应用,网购_MOBILE,HTTP网络购物,微博,锐捷云,移动WEB应用,论坛PC,论坛-Mobile,旅行相关,旅行相关_Mobile,WEB邮箱,新闻资讯,新闻资讯_Mobile,WEB邮箱-Mobile,互联网金融,金融理财-Mobile,居家生活,阅读_MOBILE,阅读小说,教育相关,WEB_MOBILE,HTTP社交应用,社交_MOBILE,普通网页浏览明细						编辑
抑制类	其他TCP,其他UDP,TCP传输应用,UDP传输应用,TCP交互应用,UDP交互应用,网络游戏软件						编辑
阻断类	非法DNS						编辑
普通/其他类	HTTP协议,游戏_MOBILE,P2P应用软件,股票软件,视频类,协议类,数据库,物联网应用,远程访问协议,软件更新,网银[支付,电子邮件,互联网文件传输,网络硬盘,网盘_MOBILE,RFC,IP-RAW,IP协议组,网络管理协议,路由协议,网上支付 网上银行_MOBILE						默认组不能编辑
常见网页应用	WEB应用,移动WEB应用,论坛PC,HTTP网络购物,HTTP游戏,WEB邮箱,腾讯网游WEB,普通网页浏览明细,腾讯游戏平台,腾讯游戏安全器,游戏更新,即时通讯软件,互联网文件传输,远程访问协议,即时通讯_MOBILE,社交_MOBILE,WEB_MOBILE,其他_MOBILE						编辑 删除

1. 设置应用分组

【应用场景】

将应用进行分组，便于针对不同优先级的应用生效不同的流量控制策略以及上网行为管理策略，使带宽合理分配。在企业场景下，设置应用分组能够方便管理员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。

【操作步骤】

- (2) 点击 **+ 添加应用分组** 按钮可以自定义应用分组。

自定义应用分组	自定义网站分组	时间对象	关键字组对象	外网IP对象	VLAN对象	IP对象
添加应用分组	自定义应用					
应用分组名称	选择应用	操作				
关键/保证类	DNS,即时通讯软件,IP网络电话,电子邮件协议,ICMP-DETAIL,VPN应用,办公OA,视频会议,即时通讯_MOBILE,WEB应用,QQ应用,网购_MOBILE,HTTP网络购物,微博,锐捷云,移动WEB应用,论坛PC,论坛-Mobile,旅行相关,旅行相关_MOBILE,WEB邮箱,新闻资讯,新闻资讯_MOBILE,WEB邮箱-Mobile,互联网金融,金融理财-Mobile,居家生活,阅读_MOBILE,阅读小说,教育相关,WEB_MOBILE,HTTP社交应用,社交_MOBILE,普通网页浏览明细	编辑				
抑制类	其他TCP,其他UDP,TCP传输应用,UDP传输应用,TCP交互应用,UDP交互应用,网络游戏软件	编辑				
阻断类	非法DNS	编辑				

添加自定义应用分组

应用组名:

Q

-

+

所有应用

+

HTTP协议

+

IP网络电话

+

网络游戏软件

+

游戏_MOBILE

+

P2P应用软件

+

股票软件

+

即时通讯软件

+

即时通讯_MOBILE

已选应用

删除全部

应用到行为策略

应用到流控策略

保存

取消

- (4) 已勾选的应用将显示在右侧。点击  按钮即可完成自定义应用分组的配置。

点击<应用到行为策略>将保存应用组配置并自动跳转至自定义行为策略页面，管理员可以在该页面基于应用组对用户上网行为进行管控，详见[6.4.3 高级配置](#)章节；

点击<应用到流控策略>将保存应用组配置并自动跳转至自定义流控策略页面，管理员可以在该页面基于应用组进行流量控制，详见[6.2.2 策略调整](#)章节。



(5) 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：

+

添加应用分组

+

自定义应用

🗉

反馈无法识别的应用

⏪

首页

⏪

上一页

1

下一页

⏩

末页

1

确定

【后续处理】

- 编辑应用分组：

点击自定义应用分组主页面表格中的

编辑

 按钮可以重新分配某个应用分组包含的应用。



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、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。

如果需要修改系统应用分组中的应用，例如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。

- 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。

2. 自定义应用

【应用场景】

除了系统内建的网络应用协议，用户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。

说明

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。

【操作步骤】

- (1) 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：

自定义应用分组

自定义网站分组

时间对象

+ 添加应用分组

+ 自定义应用

应用名称

应用规则

创建自定义应用

— □ ×

提示：名称长度不能超过27个字符(13个中文)。

自定义应用名称：

协议类型：

规则类型：

源IP+目的IP

应用所属分类：

☒ 自定义分类 ☐ 从已有分类选择：

源ip：

输入ip

?

目的ip：

输入ip

?

添加设置

自定义应用名称	协议类型	所属分类	源端口	目的端口	源Ip	目的Ip	操作
显示: 10 条 共0条							
◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶							1 确定

(2) 设置自定义应用的相关配置项。

输入自定义应用名称，选择协议类型、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。

(3) 点击

添加设置

 完成配置。

【后续处理】

自定义应用名称	协议类型	所属分类	源端口	目的端口	源Ip	目的Ip	操作
test	udp	办公OA	所有端口	所有端口	任意ip	192.168.2.2	编辑 删除

显示: 10 条 共1条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶

1 确定

- **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。

6.3.3 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：

自定义应用分组

自定义网站分组

时间对象

外网IP对象

关键字组对象

VLAN对象

帮助

+ 添加网站分组

自定义网站类

系统网站类

查询网站所属分类

网站分组名称	选择网站	管理
ddd	病毒木马,赌博,暴力,犯罪技能,违反法律,成人,色情	编辑 删除
aaa	视频,音乐,游戏,文学小说,在线聊天,娱乐	编辑 删除
keyObject	keyUriClass,门户网站与导航,搜索引擎	编辑 删除
un_audit_object	软件升级,脚本未知,un_audit_class	编辑 删除
illegal	forbidClass,视频,音乐,游戏,文学小说,在线聊天,娱乐	编辑 删除

首页

上一页

1

下一页

末页

1

确定

1. 设置网站分组

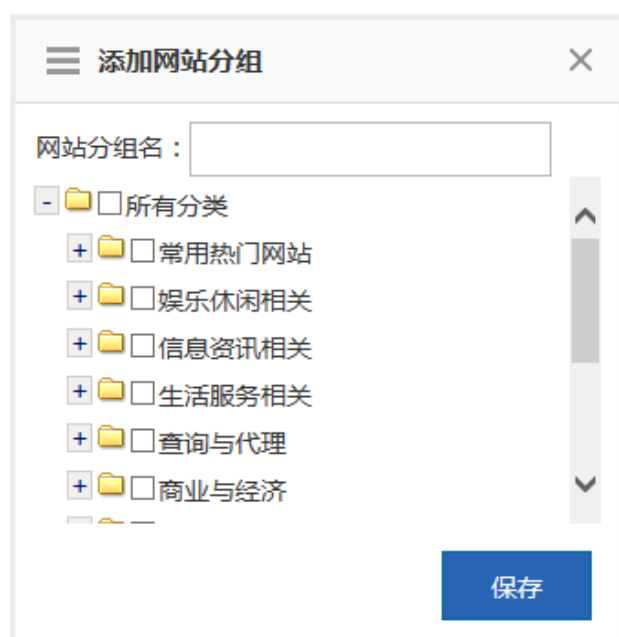
【应用场景】

将网站进行分组，便于限制不同类型网站的访问流量或禁止用户访问指定类型的网站，使带宽合理分配。配置的网站分组可应用于各种行为策略中，实现对网站访问流量进行限制。在企业场景下，设置网站分组能够帮助管理员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与工作无关的网站上。

【操作步骤】

(1) 点击[行为管理]>>[对象定义]>>[自定义网站分组]。

(2) 点击 [+ 添加网站分组](#) 按钮可以自定义网站分组。



(3) 输入网站分组名称，勾选该分组需要包含的网站类。

保存

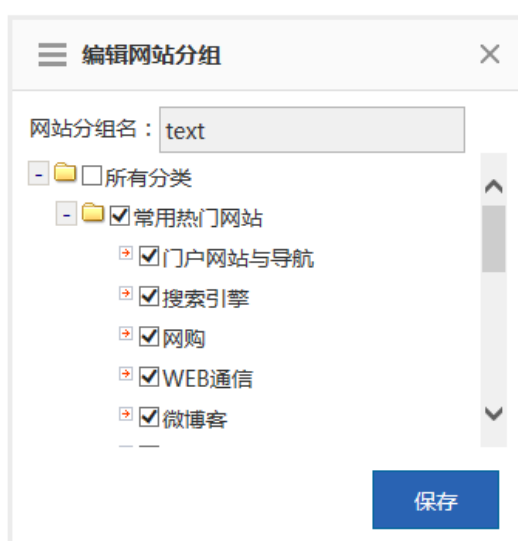
(4) 点击 即可新建一个网站分组。

【后续处理】



● 编辑网站分组：

点击自定义网站分组主页面表格中的 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 按钮即可。

● 删除网站分组：

点击自定义网站分组主页面表格中的 按钮可以删除选中的网站分组。

2. 自定义网站类

【应用场景】

除了系统内建的网站类，用户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。

【操作步骤】

(1) 点击[行为管理]>>[对象定义]>>[自定义网站分组]。

(2) 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。

自定义应用分组

自定义网站分组

时间对象

+ 添加网站分组

自定义网站类

查询网站所属分类

自定义网站分类

说明：用“回车或逗号”隔开可以输入多个网址,网址无需加http(s)://前缀

网站类名：

*

类型描述：

输入网址：域名最多支持二级目录，如www.ruijie.com.cn/about/summary.aspx

添加设置

自定义网站分类列表

网站类名	网址	类型描述	操作
显示: 10 条 共0条			
首页 上一页 1 下一页 末页 1 确定			

(3) 设置网站类的相关配置项。

创建自定义网站类：输入自定义网站类名称、能够标识该网站类的描述信息和需要包含的网站域名（多个域名以“,”隔开）。

(4) 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。

【后续处理】

- 编辑自定义网站类：选择需要修改的网站类，点击  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  即可。

6.3.4 时间对象

【应用场景】

定义时间对象，用于在配置流控或行为管理策略时作为配置选项，设置策略的生效时间。

【操作步骤】

(1) 点击[行为管理]>>[对象定义]>>[时间对象]。

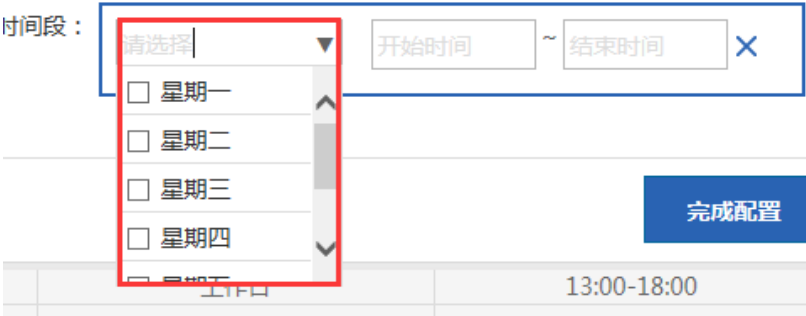


(2) 点击 **+ 添加时间对象**。

(3) 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：

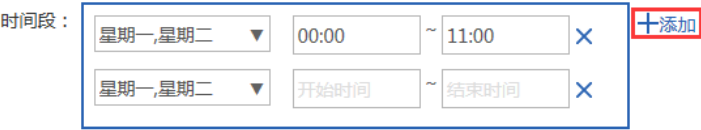
- a 对象名称：在对象名称 输入时间对象名称。
- b 时间段周期：选择时间段的周期，即选择每周的周一到周五。



c 时间段：设置时间段



d 点击添加另一个时间段



(4) 完成后点击 **完成配置** 按钮生成一个时间对象。

+ 添加时间对象

✕ 删除选中时间对象

☐	时间对象	时间周期	时间段	操作
☐	所有时间	每天	0:00-23:59	编辑删除
☐	白天	每天	6:00-18:00	编辑删除
☐	晚上	工作日	0:00-5:59	编辑删除
		每天	18:01-23:59	
☐	下班时间	工作日	0:00-7:59	编辑删除
		工作日	12:00-13:00	
		工作日	18:01-23:59	
☐	周末	周末	0:00-23:59	编辑删除
☐	上班时间	工作日	8:00-12:00	编辑删除
		工作日	13:00-18:00	
☐	工作日	工作日	0:00-23:59	编辑删除
☐	工作时间	工作日	9:00-12:00	编辑删除
		工作日	13:00-18:00	

【后续处理】

- 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。
- 删除时间对象：若需要删除某个时间对象，在列表中选择该时间对象，点击

删除

 按钮即可。
- 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。

时间段：

星期一,星期二,星期三▼

0:00

~

5:59

✕

星期一,星期二,星期三▼

18:01

~

23:59

✕

6.3.5 关键字组对象

【应用场景】

关键字组对象用于定义内容审计策略中审计的关键字，管理员可以在这里添加需要审计的内容的关键字，然后在策略配置中关联该对象。

【操作步骤】

(1) 点击[行为管理]>>[对象定义]>>[关键字对象]。

自定义应用分组	自定义网站分组	时间对象	外网IP对象	关键字组对象	VLAN对象	帮助
+ 新建关键字组						
关键字组名称		关键字			管理	
web_block_im		235345457			编辑	删除
web_block_mail		80670523@qq.com			编辑	删除
◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶						1 确定

(2) 点击

+ 新建关键字组

 。

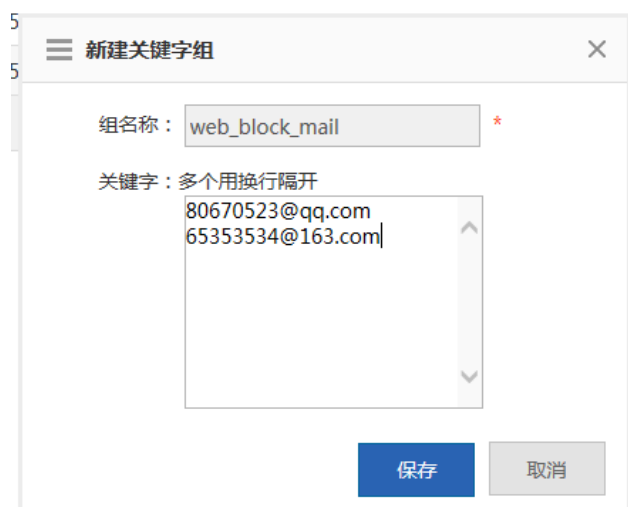


(3) 输入关键字组名称和该关键字组需要包含的关键字（多个关键字用换行隔开）。

(4) 点击 。

【后续处理】

- **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 ，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 。

6.3.6 外网 IP 对象

【应用场景】

外网IP对象是指相对于内部网络而言的外部服务器地址或其他IP地址。例如：企业的OA或业务系统的服务器未部署在内部网络，而是放在外网的电信机房或托管中心；此时为了保证内网用户访问外部服务器的网速，可以将外部服务器地址配置为外网IP对象，并设置流控策略对其带宽进行保障。

系统默认存在一个默认对象“/”，当启用二三层分类识别时，若报文目的IP地址不匹配其他任意一个网络对象，则默认匹配默认对象“/”。

【操作步骤】

(1) 点击[行为管理]>>[对象定义]>>[外网IP对象]菜单项。



(2) 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。

- 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：



- 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。
- 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：

新建用户组

用户组名：

*

上级组名：

user-group

确定

- 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：

新建ip组

新IP组名：

*

IP地址段：

*

(IP段格式192.168.1.2-192.168.1.5)

上级组名：

user-group

确定

- 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：

添加组用户

用户名称：

*

IP 地址：

*

添加

外网用户组或外网IP组的用户列表：

user-group 的用户列表 [X 删除选中用户](#)

☐	用户名称	IP 地址	管理	
☐	user-two	11.2.2.3-11.2.2.89	编辑	删除
☐	user-ui	2.2.2.2	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在左侧选中的外网用户组或外网IP组底下的所有用户，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）：

编辑用户

用户名称：

user-two

IP地址段：

11.2.2.3-11.2.2.89

上级组名：

user-group

保存

- 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。

(3) 从文件批量导入外网IP，或将导出设备上的外网IP设置导出为文件。

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：

e.WEB

说明：导入用户信息有利于实名制管理用户，方便找到用户。
提示：导入用户的文件名必须为 ipuser-info.csv，并按以下示例的规格填写对应表格。

文件名：

选择文件

 未选择任何文件 ☐修改冲突用户

导入用户

导出用户

导入文件信息规格示例：

提示：/表示根目录

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 2000::1
/研发部/研发6部	刘六	2000::1

- **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。
 - a 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

b 点击 **选择文件** 按钮，找到文件ipuser-info.csv。

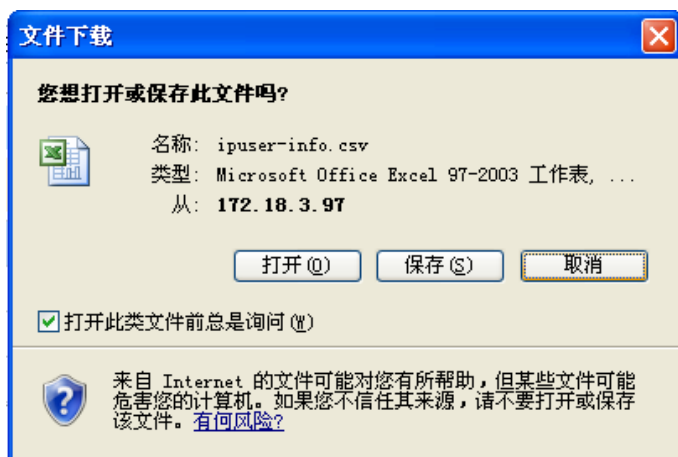
c 点击 **导入用户** 按钮，会出现文件导入进度条，待进度条加载完成说明文件已经上传成功。

说明：导入用户信息有利于实名制管理用户，方便找到用户。

提示：导入用户的文件名必须为 **ipuser-info.csv**，并按以下示例的规格填写对应表格。

文件名： **浏览...** ☐ 修改冲突用户 **导入用户** **导出用户**

- **导出外网IP：**点击 **导出用户** 按钮会弹出文件下载对话框，示例如下图所示。点击 **保存(S)** 选择保存路径即可。



6.3.7 VLAN 对象

【应用场景】

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”。

说明

目前NBR6135-E、NBR6205-E、NBR6205-Ev2、NBR6215-E、NBR6210-E、NBR6210-E V2支持网桥模式。

【操作步骤】

- (1) 点击[行为管理]>>[对象定义]>>[VLAN对象]菜单项。

自定义应用分组自定义网站分组时间对象外网IP对象关键字组对象VLAN对象帮助

说明：VLAN就是虚拟局域网，能够在逻辑上把一个广播域划分成多个广播域。

VLAN对象名称：*

VLAN对象ID：* 单个ID，或ID段（如：1-6），多个ID可以用逗号“，”隔开，ID范围(1~4094)

添加设置

删除全部

VLAN对象名称	VLAN对象ID	操作
vlan1	25	编辑 删除

首页 上一页 1 下一页 末页 1 确定

- (2) 输入VLAN对象名称和VLAN对象ID。
- 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来表示多个连续的VLAN ID。

(3) 点击添加设置按钮。

【后续处理】

- 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。

例如需要编辑“vlan1”对象，点击编辑按钮后，修改VLAN对象名称或VLAN对象ID，最后点击保存编辑按钮。

说明：VLAN就是虚拟局域网，能够在逻辑上把一个广播域划分成多个广播域。

VLAN对象名称：*vlan1

VLAN对象ID：* 2 单个ID，或ID段（如：1-6），多个ID可以用逗号“，”隔开，ID范围(1~4094)

保存编辑

取消编辑

删除全部

VLAN对象名称	VLAN对象ID	操作
vlan1	25	编辑 删除

首页 上一页 1 下一页 末页 1 确定

- 删除VLAN对象：只需选择需要删除的VLAN对象，点击删除按钮即可。

例如：需要删除“vlan1”对象则只要点击操作列的删除按钮即可。如果需要删除全部VLAN对象则点击删除全部按钮。

6.3.8 IP 对象

【应用场景】

定义IP地址对象用于配置应用路由等功能。数据转发至设备后，设备需要判断是否匹配设置的源目IP对象，若匹配，则按照对应功能进行选路或其他处理。

【操作步骤】

(1) 点击[行为管理]>>[对象定义]>>[IP对象]菜单项。

自定义应用分组 自定义网站分组 时间对象 关键字组对象 外网IP对象 VLAN对象 **IP对象**

IP对象列表: [添加IP对象组](#) [删除IP对象组](#) [+ 添加IP对象](#) [+ 批量导入IP对象](#) [X 删除选中IP对象](#)

☐	地址库	网段配置: 网段/掩码	范围配置: 起始IP/结束IP	操作
无记录信息				

显示: 条 共0条 首页 < 上一页 下一页 > 末页 1 确定

(2) 根据需要执行对应的操作：

- 点击 [+ 批量导入IP对象](#)，可通过配置文件批量添加多个IP对象。

文件名必须为ipgroup.txt，文件格式如下：

```
ip表项，每个表项一行；
ipv4的配置方式：
配置地址范围：2.2.2.2-2.2.2.3
配置单个地址：2.2.2.10
配置掩码：2.2.2.0/24
ipv6的配置方式：
配置地址范围：2a03:bbbb::cccc-
2a03:bbbb::ccde
配置单个地址：2a03:bbbb::cccc
配置掩码：aaaa:bb20::/55
```

- 添加IP对象组：点击 [添加IP对象组](#)，在弹窗中输入对象组ID，对象组描述，地址库，对象列表等信息后，点击 [确定](#) 按钮完成配置。

添加IP对象组

对象组ID:

*

1~1000

对象组描述:

*

地址库:

联通

▼

添加

IP对象列表:

每个单项格式可为 a.b.c.d 或 a.b.c.d/nn 或 a.b.c.d-e.f.g.h

确定

取消

- 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。
- 添加IP对象：点击 **添加IP对象**，可以在该IP组下添加IP对象。

添加IP对象

当前组名: 2-test

地址库:

联通

▼

添加

配置值:

每个单项格式可为 a.b.c.d 或 a.b.c.d/nn 或 a.b.c.d-e.f.g.h

*

确定

取消

- 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。
- 编辑IP对象：点击 **编辑**，对该行的IP对象进行编辑操作。
- 删除IP对象：点击 **删除**，对该行的IP对象进行单独删除操作

6.4 行为策略

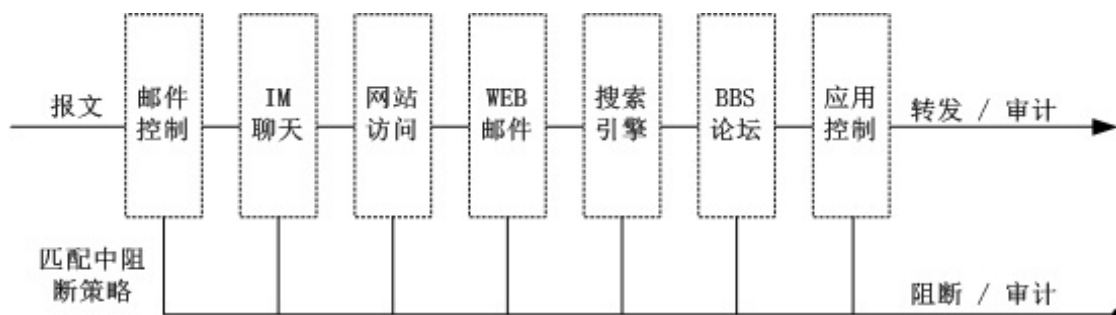
6.4.1 功能简介

行为策略用于管理用户的上网行为，能够对用户上网行为进行访问审计、监控和限制。适当的行为策略不仅能够帮助管理员对用户行为进行管理，还能帮助管理员分析用户上网行为趋势，引导用户进行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。

行为管理中各项功能的策略匹配是有顺序的。

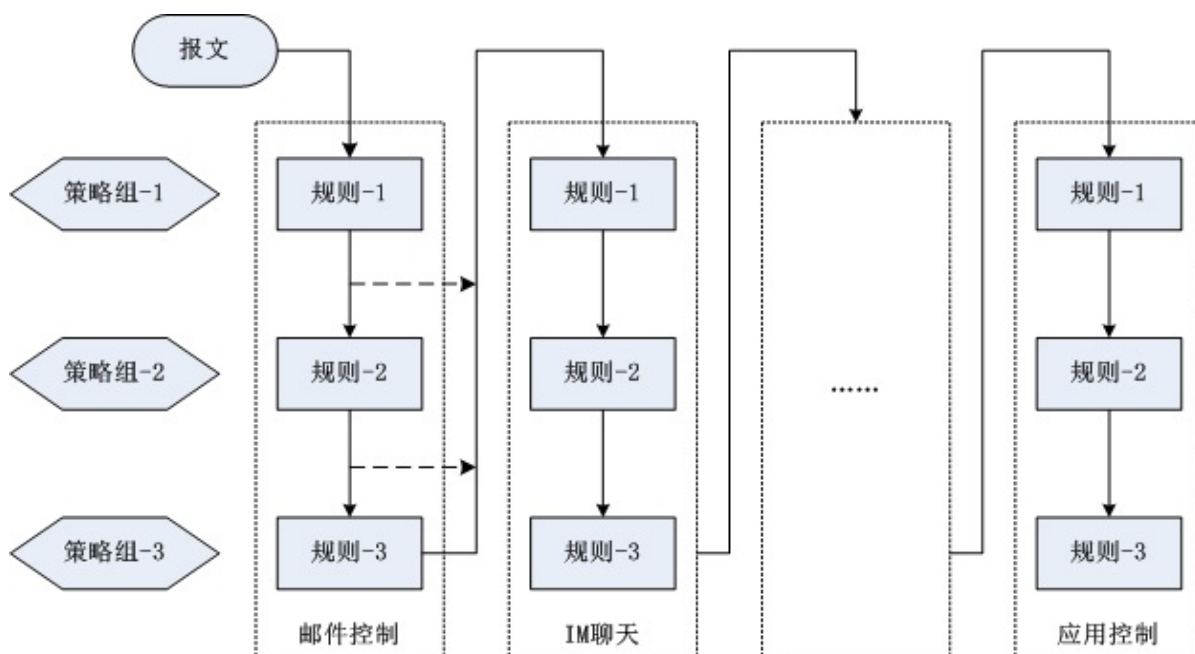
如果第一种类型的行为管理业务没有对报文进行阻断，则报文会进入下一种行为管理业务继续处理；如果有一种行为管理业务对报文进行了阻断，则不再进入下一种行为管理业务处理。各行为管理业务的处理顺序如下：

图6-1 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6-2 策略和规则的优先级匹配顺序



6.4.2 简易配置

【应用场景】

在简易配置页面，用户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。



1. 开启默认审计

【操作步骤】

- (1) 点击[行为管理]>>[行为策略]>>[简易配置]菜单项。
- (2) 勾选需要开启的默认审计项。

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，则用户的所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：

开启默认审计：☒ 网站审计 ☒ 邮件收发 ☒ IM聊天 ☒ 论坛发帖 ☒ 搜索引擎 ☒ 虚拟身份 ☒ FTP审计 ☒ TELNET审计 ☒ 开启全部

2. 设置禁止应用

将应用拉入黑名单，内网用户将不能使用被禁止的应用。

【操作步骤】

- (1) 点击[行为管理]>>[行为策略]>>[简易配置]菜单项。



- (2) 点击 **禁止应用**。
- (3) 在弹出的页面中，用户可以查看当前被禁止访问的应用了，点击<删除>可以取消对应用的禁用。
点击 **+ 添加阻断应用**，可以添加要禁止的应用。

禁止应用

提示：若应用（组）的上级应用组已配置在列表中，该应用（组）不重复显示！

+ 添加阻断应用

✕ 删除全部

阻断应用	删除
非法DNS	删除

显示: 10 条 共1条

◀ 首页

◀ 上一页

1

下一页 ▶

末页 ▶▶

1

确定

+ 添加阻断应用

✕ 删除全部

≡ 选择阻断应用

✕

Q

- 所有应用

+ 所有应用

+ HTTP协议

+ IP网络电话

+ 网络游戏软件

+ 游戏_MOBILE

+ P2P应用软件

+ 股票软件

+ 即时通讯软件

+ 即时通讯_MOBILE

+ 微博

字体颜色区别应用类型：关键/普通/抑制/阻断

确定

(4) 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：



(5) 添加完成后，可在禁止应用列表查看到对应表项。

提示：若应用（组）的上级应用组已配置在列表中，该应用（组）不重复显示！

+ 添加阻断应用 × 删除全部

阻断应用	删除
非法DNS	删除
股票软件	删除

显示: 10 条 共2条 << 首页 < 上一页 1 下一页 > 末页 >> 1 确定

- 点击  按钮可以将单个应用从禁止应用列表中删除。
- 点击  按钮可以将所有应用都从禁止应用列表中删除。

3. 设置用户黑名单

被拉入黑名单的内网用户将被禁止上网。



注意

- 用户黑名单配置可能会影响内网PC之间互访，如果需要允许PC之间互访，请在[流控策略]>>[策略调整]设置阻断策略来禁止用户上网，详见[6.2.2 策略调整](#)章节。
- 跨三层无法通过MAC地址禁止用户上网，例如终端PC的网卡所属的网关不在当前网关设备上，此时拉黑指定用户MAC无法生效。

【操作步骤】



用户黑名单

(1) 点击 用户黑名单 按钮。

(2) 弹出以下页面，用户可以查看到当前已被禁止上网的用户。点击<删除>可将用户移出黑名单。

简易配置

高级配置

三 用户黑名单

添加屏蔽用户 【用户管理】

用户名称	IP地址	MAC地址	操作
test1	8.9.5.5	#	删除
test2	7.5.5.5	#	删除
2	#	#	删除
3	#	#	删除
23	3.3.3.2	#	删除
345	#	#	删除
567	#	#	删除
234	#	#	删除
6	#	#	删除
5test	#	#	删除

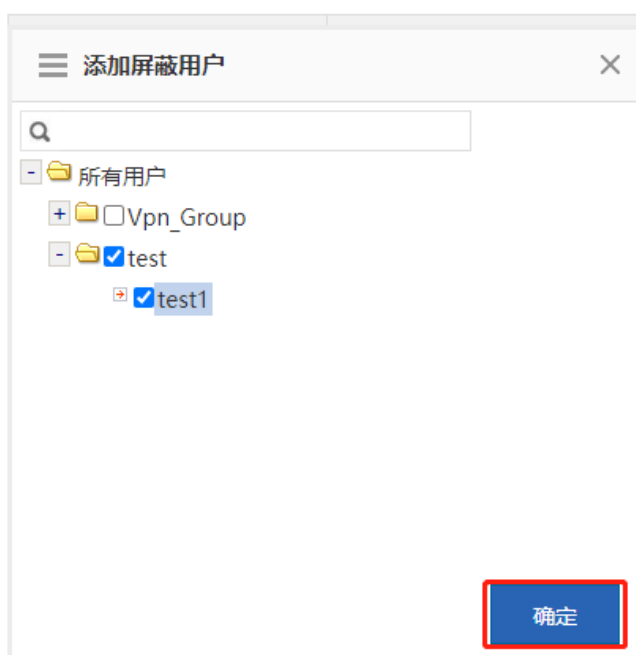
显示 10 条 共13条

首页 上一页 1 2 下一页 末页 1 确定

(3) 点击 + 添加屏蔽用户 按钮，将弹出用户列表窗口。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。

若当前用户列表找不到需要禁止的用户，点击 【用户管理】 可创建新的用户组 and 用户，配置详情见 [7.1 用户组织](#) 章节。

+ 添加屏蔽用户 【用户管理】



(4) 可以在屏蔽用户列表中查看到添加的屏蔽用户。



4. 设置免审计（免监控）用户

设备不会审计免监控用户的上网记录，且默认情况下流控策略也不对免监控用户生效；如果在配置免审计用户时，勾选了“只免审计不免流控”，则流控策略中的限速规则依然会对免监控用户生效。

【操作步骤】



- (1) 点击 **免审计用户** 按钮。
- (2) 弹出以下页面，用户可以在该页面查看当前不被审计的用户，点击<删除>可以将用户从免审计列表中移除，恢复对该用户的审计。

说明：免审计用户同时也不会进行防共享检测。

+ 添加免监控用户

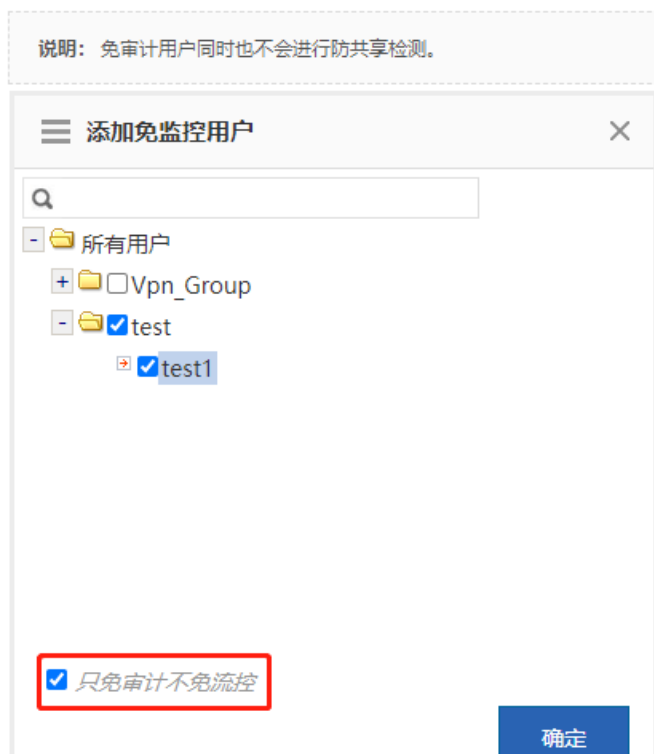
用户名称	IP地址	MAC地址	是否免流控	操作
test1	1.1.1.1	#	√	删除

显示: 10 条 共1条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶

1 确定

- (3) 点击 **+ 添加免监控用户** 按钮，将弹出用户列表窗口。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，则需要同时勾选 ☐ **只免审计不免流控**，点击 **确定** 添加到免监控用户列表



- (4) 可以在免监控用户列表中查看到添加的屏蔽用户。“是否免流控”栏中，√ 表示该用户不受流控策略限制，× 表示该用户依然受流控限制；



5. 设置禁止网站

分为黑名单和白名单两种模式：

网站黑名单模式：黑名单列表中的网站将被禁止访问，未加入名单的网站不受限制。

网站白名单模式：只有白名单列表中的网站能够被用户访问，未加入名单的网站都禁止。

【操作步骤】



- (1) 点击 **禁止网站** 按钮。
- (2) 点击选择要配置的网站过滤模式：黑名单模式或白名单模式。

(3) 在网站配置页面，用户可以查看并修改阻断或允许访问的网站。

- 黑名单模式：

☒ 黑名单模式

只有在黑名单网站列表下的网站才被阻断！

☐ 白名单模式

只有在白名单网站列表下的网站才能访问！

禁止网站： ☐ 选择URL分类 ☒ 输入网址

请输入单个网址

添加设置

黑名单网站列表

删除				删除
显示: 10	条 共0条	◀ 首页	◀ 上一页 1 下一页 ▶ 末页 ▶▶	1 确定

- 添加禁止网站：可以选择已有的URL分类，或直接手动输入网址。

选择URL分类：点击选择“禁止网站”类型为“选择URL分类”，然后点击“选择URL分类”下方的输入

框，在列表中勾选需要禁止的URL分类，点击 **确定**。最后点击 **添加设置** 将URL分类添加至黑名单中。

禁止网站： ☒ 选择URL分类 ☐ 输入网址

选择URL分类

黑名单网站列表

显示: 10

选择URL分类

所有分类

- ☒ 常用热门网站
- ☐ 信息资讯相关
- ☐ 商业与经济
- ☐ 非法与不良

确定

输入网址：点击选择“禁止网站”类型为“输入网址”，在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。

74

禁止网站： ☐ 选择URL分类 ☒ 输入网址

添加设置

○ 删除禁止网站：选择需要解除禁止的网站，点击  按钮即可。

● 白名单模式：

☐ 黑名单模式

只有在黑名单网站列表下的网站才被阻断！

☐ 白名单模式

只有在白名单网站列表下的网站才能访问！

白名单网站： ☐ 选择URL分类 ☒ 输入网址

添加设置

白名单网站列表 ☒ 宽松的白名单

白名单网站		删除
显示: 10 条 共0条	◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶▶	1 确定

○ 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。

○ 删除白名单网站：选择需要禁止的网站，点击  按钮即可。

○ 宽松的白名单：选中 ☐ 宽松的白名单，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。

6. 设置禁止的文件类型

设置后将禁止用户下载指定类型的文件，例如阻断doc文件类型，那么用户将无法下载以.doc为后缀的文件。

【操作步骤】



(1) 点击 **禁止的文件类型**。

(2) 在弹出的页面中点击开关开启文件类型禁止功能。

说明：勾选“开启文件类型禁止功能”选项可以开启对指定类型文件的禁止下载，目前匹配的是URL地址（如：阻断doc文件类型，那么只有当文件下载的URL路径最后为.doc时才会实际生效）。

开启文件类型禁止功能：



- (3) 点击 **+ 添加禁止文件类型**，输入需要禁止的文件后缀名，多个后缀名以“,”分隔。点击 **确定** 将后缀名添加到禁用文件类型列表中。

说明：勾选“开启文件类型禁止功能”选项可以开启对指定类型文件的禁止下载，目前匹配的是URL地址（如：阻断doc文件类型，那么只有当文件下载的URL路径最后为.doc时才会实际生效）。

+ 添加禁止文件类型

✕ 删除所选的项

开启文件类型禁止功能：

ON

≡ 添加禁用文件类型

✕

后缀名：

确定

取消

- (4) 添加的文件后缀名将显示在禁用文件类型列表中，点击 **✕ 删除勾选** 按钮，可以将勾选的文件类型从已禁止文件类型列表中删除。

+ 添加禁止文件类型

✕ 删除勾选

开启文件类型禁止功能：

ON

☒ .doc	☒ .txt	☒ .htm	☒ .jpg
--	--	--	--

7. 设置免监控网站

开启该功能后，在不审计网站列表中的网站不会被审计。

【操作步骤】



- (1) 点击 **不审计的网址（免监控）**。

- (2) 点击 **开启功能**：☐ **ON** ☐ 开启网站不审计功能。开启后，列表中网站的访问不会被设备审计，也不会被阻断。

说明：开启该功能后，在下表中的网址不会被审计。

+ 添加不审计的网址（免监控） **✕ 删除所选的项** 开启功能：☐ **ON** ☐

☐	不审计的网址（免监控）	操作
☐	ruijie.com.cn	删除
显示: 10 ▼ 条 共1条		
⏮ 首页 ⏪ 上一页 1 下一页 ⏩ 末页 1 确定		

- (3) 点击 **+ 添加不审计网址**，在弹窗中输入不受审计的网址，点击<确定>将网址加入到不审计网站列表中。

≡

添加不审计的网址（免监控）

✕

添加不审计的网址（免监控）

- (4) 添加的网址将在不审计网站列表中显示。

- 点击 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；

8. 设置禁止客户端邮箱

邮箱帐号被禁止后，将无法发送或接受邮件。

【操作步骤】



- 点击 **禁止客户端邮箱**。
- 在输入框中输入要禁用的邮箱帐号，点击<添加设置>，将要禁用的邮箱帐号添加至“禁用邮箱帐号列表”。

禁止邮箱帐号:

禁止邮箱帐号列表

禁止的邮箱帐号		删除
显示: 10 条 共0条	首页 上一页 1 下一页 末页	1 确定

(3) 点击 可将邮箱帐号恢复正常使用。

禁止邮箱帐号:

禁止邮箱帐号列表

禁止的邮箱帐号		删除
1213141516@qq.com		删除
显示: 10 条 共1条	首页 上一页 1 下一页 末页	1 确定

9. 设置禁止 QQ 帐号

被禁止的QQ帐号将无法发送或接收消息。本功能分为两种模式：

QQ黑名单模式：只有在QQ黑名单列表中的帐号才被阻断，其他帐号不受影响；

QQ白名单模式：只有在QQ白名单列表中的帐号能够正常使用，其他帐号都被禁用。

【操作步骤】



(1) 点击 **禁止QQ帐号**。

(2) 选择阻断模式：点击选择黑名单模式或白名单模式，在提示信息框内点击<确定>。

☒ 黑名单模式

只有在QQ黑名单列表下的帐号才被阻断！

☐ 白名单模式

只有在QQ白名单列表下的帐号才能访问！

禁止QQ帐号:

QQ黑名单列表

QQ帐号		删除
显示: 10 条 共0条	首页 上一页 1 下一页 末页	1 确定

- (3) 如果选择的是“黑名单模式”，则在输入框中输入需要禁用的QQ帐号；如果选择的是“白名单模式”，则在输入框中输入放行的QQ帐号。点击<添加设置>。
- (4) 添加的QQ帐号将显示在下方的列表中，点击<删除>可将QQ帐号移出黑/白名单。

QQ黑名单列表

QQ帐号	删除
123456789	删除
显示: 10 条 共1条	
首页 上一页 1 下一页 末页	
1	确定

6.4.3 高级配置

【应用场景】

行为策略的高级配置为用户提供了更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。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进行监控和限制，例如可以对邮件内容、聊天内容、发帖内容等进行全面的审计。

1. 基本步骤

- (1) 点击[行为管理]>>[行为策略]>>[高级配置]菜单项。

说明：URL重定向不支持对HTTPS加密的网站进行重定向。
 注意：我们不建议客户如下使用方式：只允许某些特定应用可以访问网络，其他所有应用都阻断。
 帮助：行为策略常见功能如何使用？

+ 添加行为策略 × 删除选中 + 根据模板建策略 + 设置HTTPS加密内容审计

查询策略组：包含继承父组的策略 输入用户名 查找

策略组名称	关联用户	策略开关	状态	匹配顺序	操作
显示: 10 条 共0条					

首页 上一页 1 下一页 末页 1 确定

在当前页面，用户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、搜索引擎策略等。

- (2) 点击 **+ 根据模板建策略**，可以基于现有的策略基础上创建新的策略。如下图所示：



选择现有策略模板后会弹出策略新建窗口，新建的策略默认包含模板中的策略规则。

- (3) 点击 **+ 添加行为策略** 弹出“添加行为策略”配置向导窗口。

a 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。

- b 策略设置：点击“策略设置”页签，设置当前策略组的行为规则。可以同时选择多种类型的上网权限策略，包括“应用控制”、“网站访问”等策略。点击 **>> 其他策略** 可选择更多策略类型。

点击左侧的策略类型名称可以查看该类型下的所有规则，如果要设置对应类型的规则则要选中前面的复

选框  **应用控制**，然后进行编辑、删除、添加操作。各个类型的具体添加操作请参考[策略设置详解](#)。

- c 设置关联用户：点击“关联用户”页签，选择该策略要对哪些用户生效。关联用户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。



d 点击<保存>。

(4) 设置HTTPS加密内容审计。

a 点击<设置HTTPS加密内容审计>，进入HTTPS加密内容审计功能的设置页面。



b 点击“开启加密内容审计”后的复选框，可开启或关闭加密内容审计功能。开启后可对SSL加密后的WEB邮件收发、论坛发帖、搜索引擎、虚拟身份等进行审计。

 注意

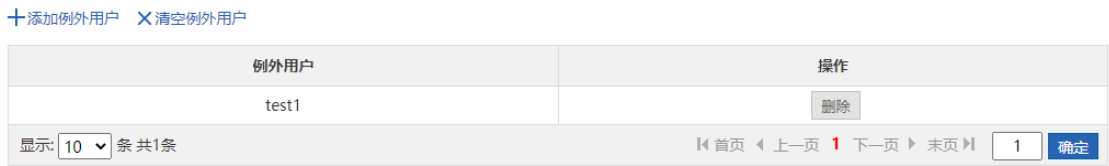
需要在终端电脑上导入SSL根证书，避免终端浏览器告警或应用使用异常。

(1) 终端PC访问当前页面并点击<下载SSL根证书>，将根证书保存到终端PC。

(2) 选择SSL根证书文件，点击鼠标右键选择“安装证书”，然后将证书安装到指定目录“受信任的根证书颁发机构”即可。



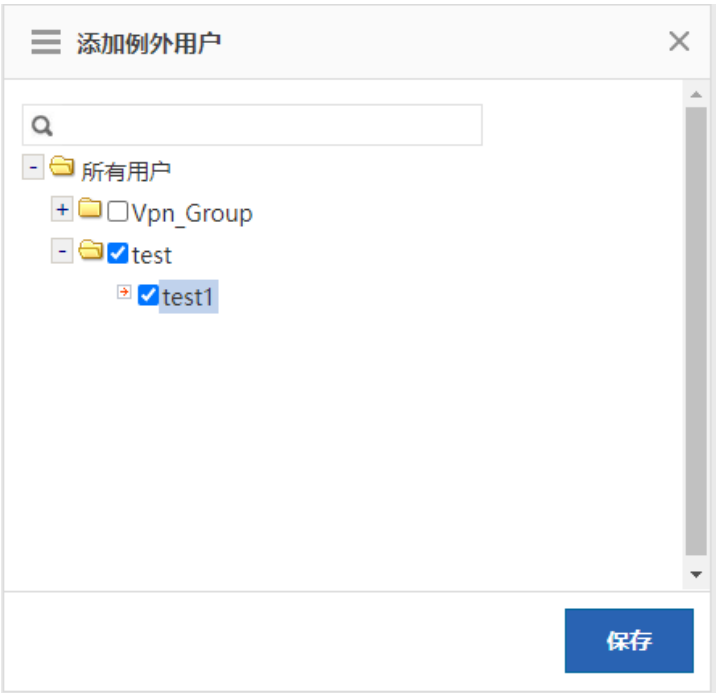
c 设置例外用户。



点击 **删除** , 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** , 可以添加用户为例外用户。选择要添加的用户, 点击<保存>。



2. 策略设置详解

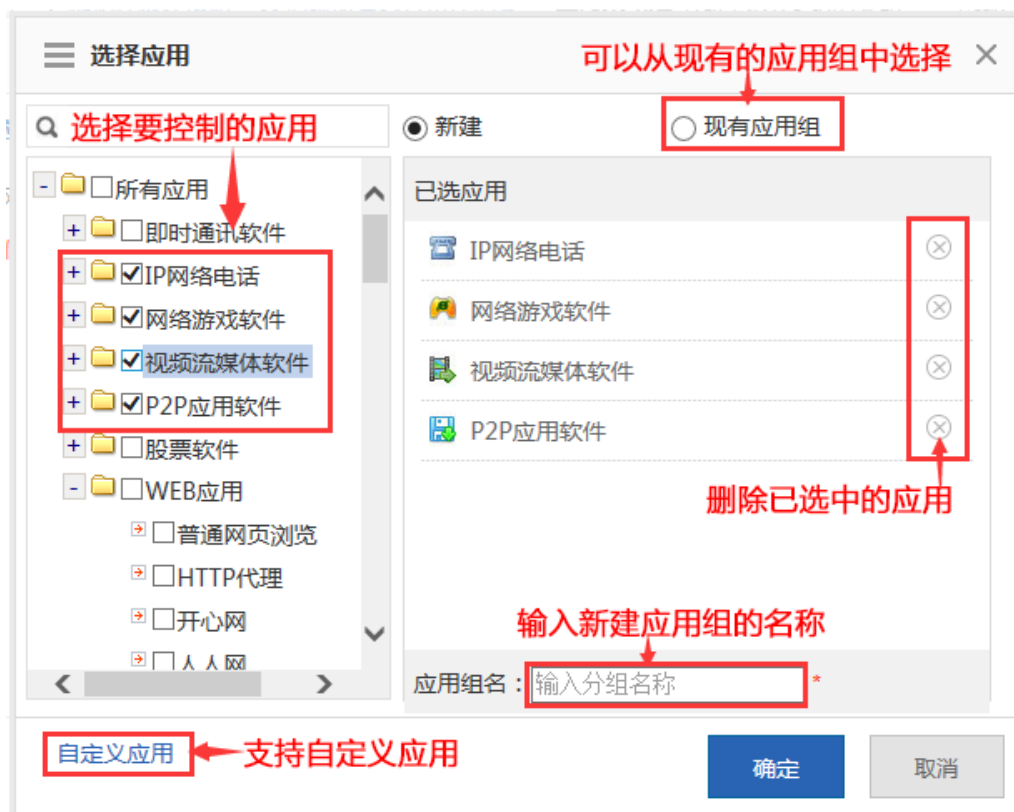
(1) 设置应用控制策略

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：

- a 在左侧“上网权限策略”中勾选“应用控制”，然后在右侧点击⁺添加规则。

- b 点击“选择应用”，将弹出如下页面。

可以从现有的应用组中选择，或新建用户组。需要新建应用组时，选择“新建”，在左侧先选中要控制的应用，然后在“应用组名”输入框中输入新建的应用组名称，最后点击<确定>。



- c 在下拉框中选择控制规则。控制规则说明：

允许但不审计：不阻断关联用户访问指定应用的上网行为，也不记录其上网信息。

阻断并审计：阻断关联用户访问指定应用的上网行为，同时记录下阻断信息。

阻断但不审计：阻断关联用户访问指定应用的上网行为，但不记录其阻断信息。

阻断并审计和告警：阻断关联用户访问指定应用的上网行为，同时记录下阻断信息，并给出告警。

- d 选择生效时间：设置规则的生效时间，只有在生效时间内该规则才起作用。

- e 点击<确定>。

(2) 设置网站访问策略

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。

添加行为策略

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

网站访问策略

选择网站

添加网站访问策略

选择网站: [【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

- a 在左侧“上网权限策略”中勾选“网站访问”，然后在右侧点击⁺添加规则。

添加网站访问策略

选择网站: [【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

- b 点击“选择网站”，将弹出如下页面。

左侧树状图是当前系统已配置的URL分类的组织结构，用户可以在这里选择一个URL分类作为监控对象。不选择的情况下系统默认对所有URL分类进行监控。选择完毕后点击<确定>。



- c 在下拉框中选择控制规则。控制规则说明：

允许并审计：不阻断关联用户访问指定网站的上网行为，但会记录上网信息。

允许但不审计：不阻断关联用户访问指定网站的上网行为，也不记录其上网信息。

阻断并审计：阻断关联用户访问指定网站的上网行为，同时记录下阻断信息。

阻断但不审计：阻断关联用户访问指定网站的上网行为，但不记录其阻断信息。

允许并审计和告警：不阻断关联用户访问指定网站的上网行为，但会记录下阻断信息，并给出告警。

阻断并审计和告警：阻断关联用户访问指定网站的上网行为，同时记录下阻断信息，并给出告警。

- d 选择生效时间：设置规则的生效时间，只有在生效时间内该规则才起作用。

- e 点击<确定>。

(3) 设置邮件控制策略

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。



- a 在左侧“上网权限策略”中点击 **>> 其他策略** 展开更多类型的策略，勾选“邮件控制”，然后在右侧点击 **+** 添加规则。



- b 在下拉框中选择控制类型。控制类型是指在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”，匹配关键字设为“123456”，则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。

控制类型分为“收发帐号”、“邮件标题”、“邮件正文”、“附件名称”和“全部”，“全部”表示同时匹配前面列举的所有字段。

- c 点击“匹配关键字”后方的 **【点击进行选择】**，设置审计邮件时匹配的关键字。

左侧列出了当前系统已配置的关键字组，用户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。用户也可以点击 ☐ **新建关键字组**，输入组名称和需要审计的关键字信息后点击<添加关键字>，即可新建一个关键字组。

d 在下拉框中选择控制规则。控制规则说明：

允许并审计：不阻断关联用户收发指定内容邮件的上网行为，但会记录对应上网信息。

允许但不审计：不阻断关联用户收发指定内容邮件的上网行为，也不记录其上网信息。

阻断并审计：阻断关联用户收发指定内容邮件的上网行为，同时记录下阻断信息。

阻断但不审计：阻断关联用户收发指定内容邮件的上网行为，但不记录其阻断信息。

允许并审计和告警：不阻断关联用户收发指定内容邮件的上网行为，但会记录下阻断信息，并给出告警。

阻断并审计和告警：阻断关联用户收发指定内容邮件的上网行为，同时记录下阻断信息，并给出告警。

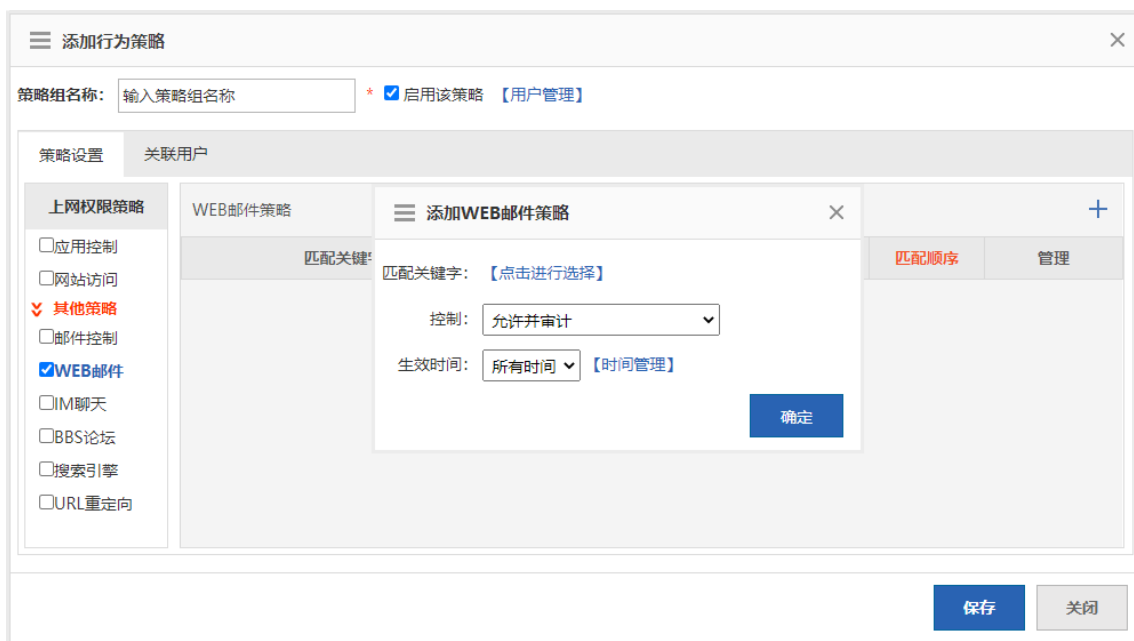
e 在“最大限制”后的输入框输入需要审计的整个邮件的最大限制大小，单位为K。设置后只能审计到比限制要小的邮件。

f 选择生效时间：设置规则的生效时间，只有在生效时间内该规则才起作用。

g 点击<确定>。

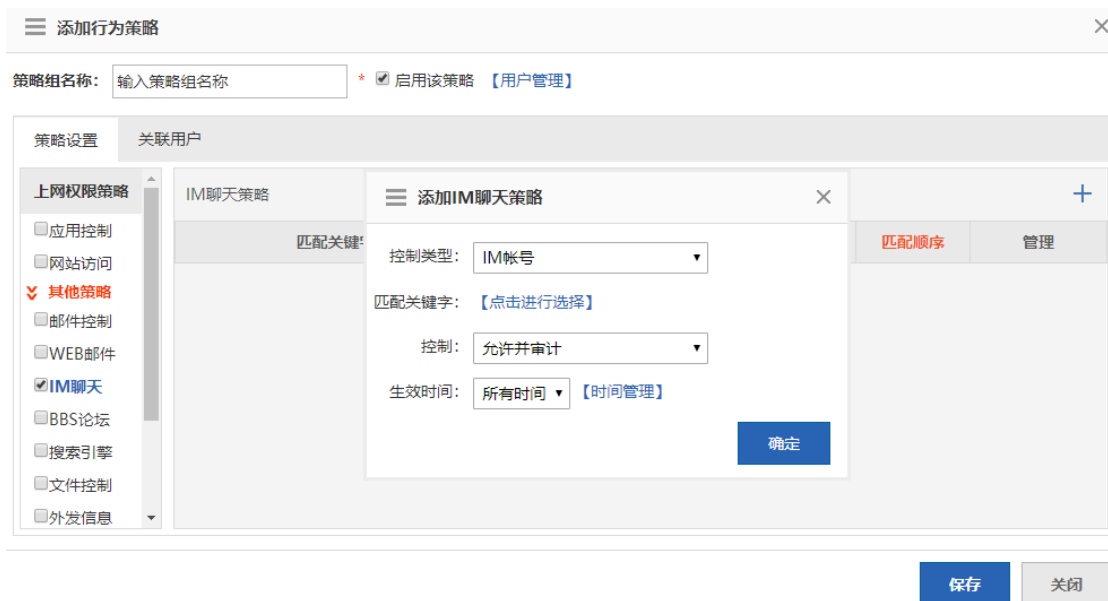
(4) 设置Web邮件策略

Web邮件策略主要针对主流的Web邮件系统（如新浪邮箱、网易邮箱和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相似，只是少了“控制类型”和“最大限制”的配置，请参考章节[\(3\)](#)。



(5) 设置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），对帐号和聊天内容进行审计，并对帐号进行过滤。目前设备支持对QQ和MSN的聊天进行审计，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。



- a 在左侧“上网权限策略”中点击 **>> 其他策略** 展开更多类型的策略，勾选“IM聊天”，然后在右侧点击 **+** 添加规则。

添加IM聊天策略

控制类型: IM帐号

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

- b 在下拉框中选择控制类型。选择“全部”表示同时对帐号和聊天内容进行审计。
- c 点击“匹配关键字”后方的[【点击进行选择】](#)，设置审计IM聊天时匹配的关键字。

匹配关键字

☒ 选择已有关键字组 ☐ 新建关键字组

请选择关键字组

☐ 默认不选择

☒ web_block_mail

☐ web_block_im

组名称: web_block_mail *

关键字: 每一行算一个关键字

80670523@qq.com

若有修改, 请先点击保存设置

保存设置

确定 取消

左侧列出了当前系统已配置的关键字组，用户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。用户也可以点击 **新建关键字组**，输入组名称和需要审计的关键字信息后点击<添加关键字>，即可新建一个关键字组。

- d 在下拉框中选择控制规则。控制规则说明：
- 允许并审计**：不阻断关联用户匹配该策略的上网行为，但会记录对应上网信息。
- 允许但不审计**：不阻断关联用户匹配该策略的上网行为，也不记录其上网信息。

阻断并审计：阻断关联用户匹配该策略的上网行为，同时记录下阻断信息。

阻断但不审计：阻断关联用户匹配该策略的上网行为，但不记录其阻断信息。

允许并审计和告警：不阻断关联用户匹配该策略的上网行为，但会记录下阻断信息，并给出告警。

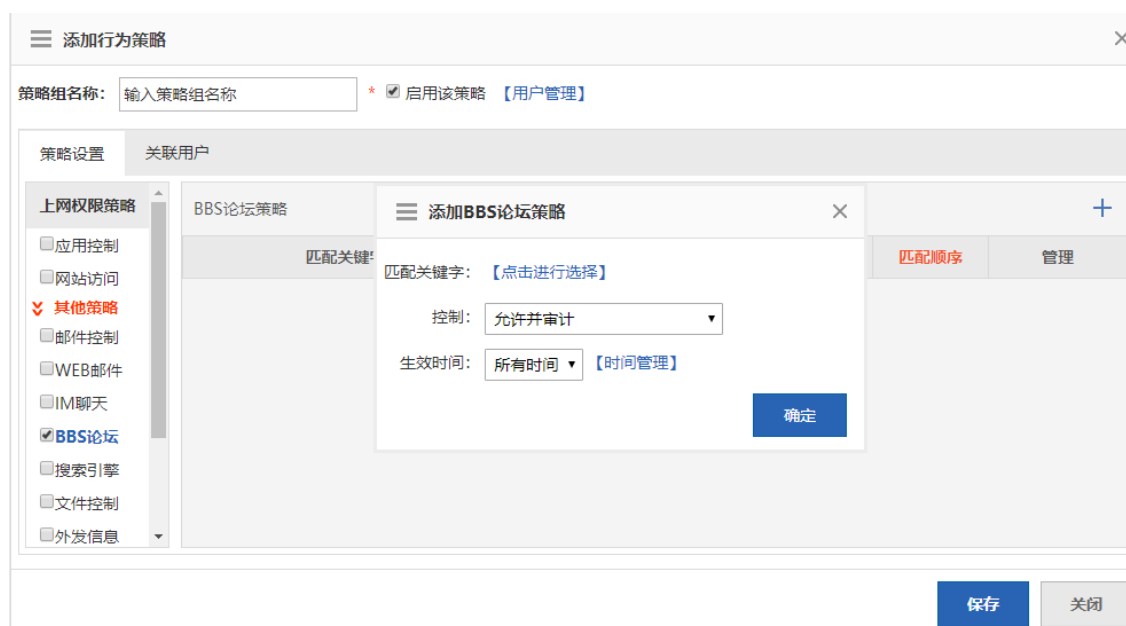
阻断并审计和告警：阻断关联用户匹配该策略的上网行为，同时记录下阻断信息，并给出告警。

e 选择生效时间：设置规则的生效时间，只有在生效时间内该规则才起作用。

f 点击<确定>。

(6) 设置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。当用户所发的帖子中包含“匹配关键字”时，设备将根据策略规则对帖子进行审计。



a 在左侧“上网权限策略”中点击 **>> 其他策略** 展开更多类型的策略，勾选“BBS论坛”，然后在右侧点击 **+** 添加规则。



b 点击“匹配关键字”后方的 **【点击进行选择】**，设置审计BBS论坛发帖内容时匹配的关键字。

左侧列出了当前系统已配置的关键字组，用户可以在这里选择一个关键字组作为审计对象。选择 **默认不选择**，设备将对所有内容进行审计。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。用户也可以点击 **新建关键字组**，输入组名称和需要审计的关键字信息后点击<添加关键字>，即可新建一个关键字组。

c 在下拉框中选择控制规则。控制规则说明：

允许并审计：不阻断关联用户匹配该策略的上网行为，但会记录对应上网信息。

允许但不审计：不阻断关联用户匹配该策略的上网行为，也不记录其上网信息。

阻断并审计：阻断关联用户匹配该策略的上网行为，同时记录下阻断信息。

阻断但不审计：阻断关联用户匹配该策略的上网行为，但不记录其阻断信息。

允许并审计和告警：不阻断关联用户匹配该策略的上网行为，但会记录下阻断信息，并给出告警。

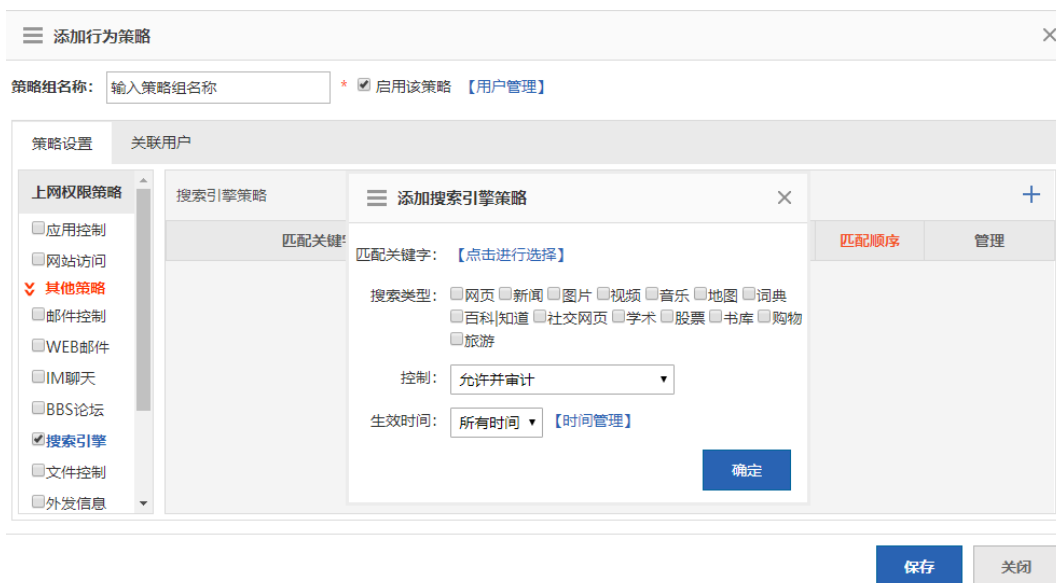
阻断并审计和告警：阻断关联用户匹配该策略的上网行为，同时记录下阻断信息，并给出告警。

d 选择生效时间：设置规则的生效时间，只有在生效时间内该规则才起作用。

e 点击<确定>。

(7) 设置搜索引擎策略

搜索引擎策略主要针对主流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：



- a 在左侧“上网权限策略”中点击 **>> 其他策略** 展开更多类型的策略，勾选“搜索引擎”，然后在右侧点击 **+** 添加规则。



- b 点击“匹配关键字”后方的 **【点击进行选择】**，设置审计搜索内容时匹配的关键词。

匹配关键字

☒ 选择已有关键字组 ☐ 新建关键字组

请选择关键字组

☐ 默认不选择

☒ web_block_mail

☐ web_block_im

组名称：web_block_mail *

关键字：每一行算一个关键字

80670523@qq.com

若有修改，请先点击保存设置

保存设置

确定 取消

c 选择需要审计的“搜索类型”。

d 在下拉框中选择控制规则。控制规则说明：

允许并审计：不阻断关联用户匹配该策略的上网行为，但会记录对应上网信息。

允许但不审计：不阻断关联用户匹配该策略的上网行为，也不记录其上网信息。

阻断并审计：阻断关联用户匹配该策略的上网行为，同时记录下阻断信息。

阻断但不审计：阻断关联用户匹配该策略的上网行为，但不记录其阻断信息。

允许并审计和告警：不阻断关联用户匹配该策略的上网行为，但会记录下阻断信息，并给出告警。

阻断并审计和告警：阻断关联用户匹配该策略的上网行为，同时记录下阻断信息，并给出告警。

e 选择生效时间：设置规则的生效时间，只有在生效时间内该规则才起作用。

f 点击<确定>。

(8) 设置文件控制策略

文件控制策略用于审计一些网盘应用的文件上传下载行为，可以限制用户所能上传和下载的文件。

控制类型：设置对文件的哪些属性进行审计。

其他配置步骤请参考章节[\(6\)](#)。

添加行为策略

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

匹配关键字

添加文件控制策略

控制类型:
匹配关键字: [【点击进行选择】](#)
控制:
生效时间: [【时间管理】](#)

确定

匹配顺序

管理

保存

关闭

(9) 设置外发信息审计策略

用于审计访问部分HTTP网站时发送的POST报文的内容。

请参考章节[\(6\)](#)进行设置。

添加行为策略

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

匹配关键字

添加外发信息策略

匹配关键字: [【点击进行选择】](#)
控制:
生效时间: [【时间管理】](#)

确定

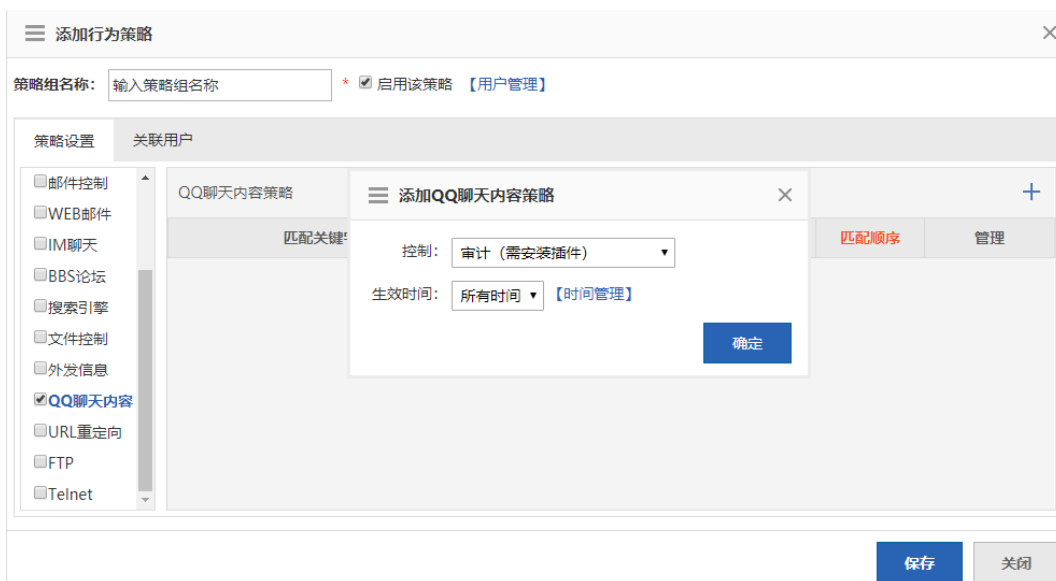
匹配顺序

管理

保存

关闭

(10) 设置QQ聊天内容审计策略



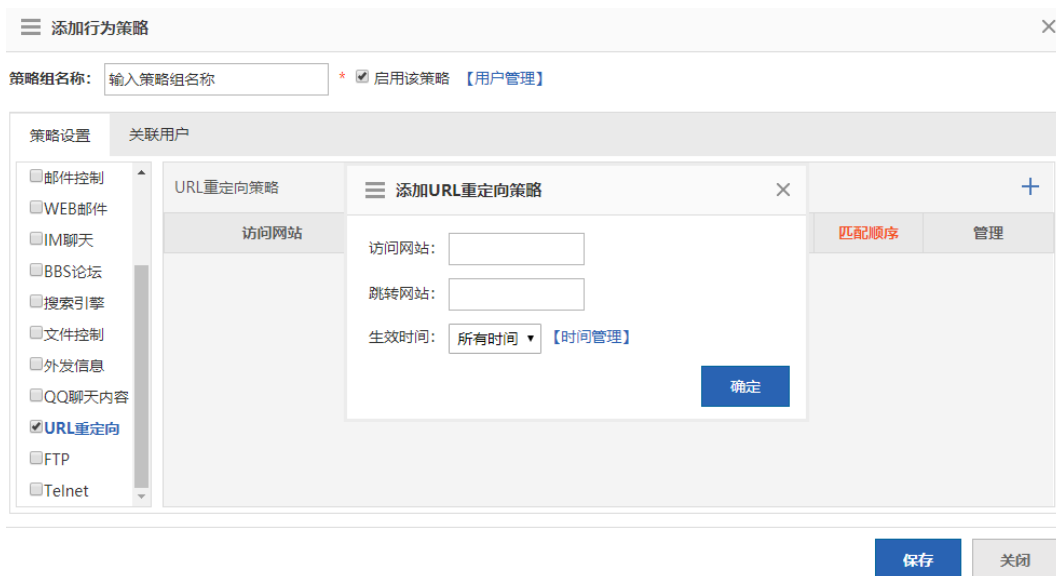
- 在左侧“上网权限策略”中点击 **>> 其他策略** 展开更多类型的策略，勾选“QQ聊天内容”，然后在右侧点击 **+** 添加规则。
- 在“控制”下拉框中选择控制类型（审计或不审计）。
- 在“生效时间”下拉框中设置规则的生效时间，只有在生效时间内该规则才起作用。
- 点击<确定>。

(11) 设置URL重定向策略

设置URL重定向策略后，当用户访问指定网站，将自动跳转至设置的另一个网站。

说明

URL重定向不支持对HTTPS加密的网站进行重定向。



- 在左侧“上网权限策略”中点击 **>> 其他策略** 展开更多类型的策略，勾选“URL重定向”，然后在右侧点击 **+** 添加规则。



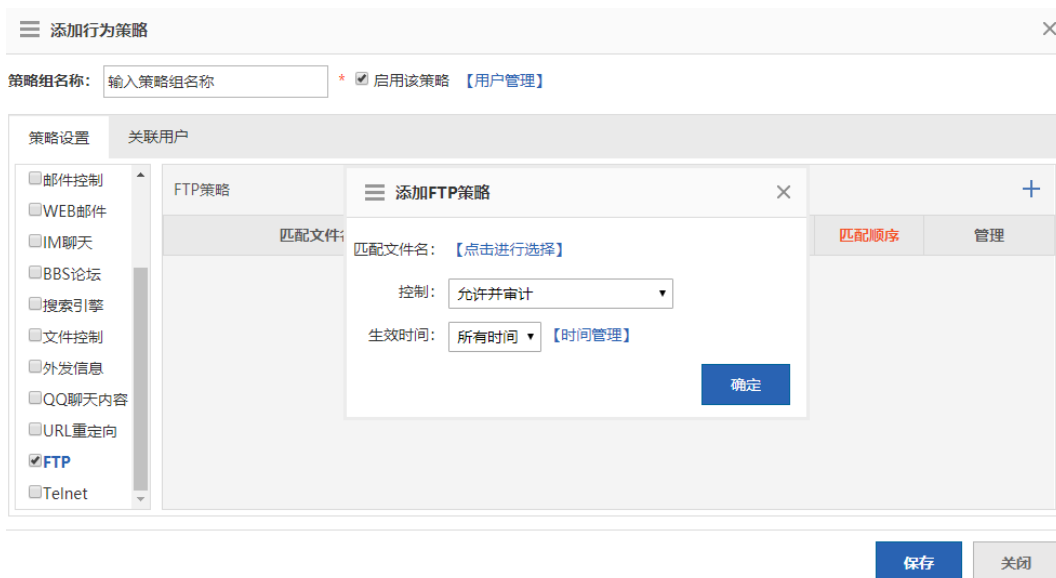
- b 输入访问网址以及重定向后的网站网址。
- c 在“生效时间”下拉框中设置规则的生效时间，只有在生效时间内该重定向规则才起作用。
- d 点击<确定>。

(12) 设置FTP策略

FTP服务提供了对文件的远程访问功能，通过FTP策略可以实现审计服务器IP、文件名、文件内容等，以及阻断指定文件名的上传下载。

匹配文件名：点击“匹配文件名”后方的【[点击进行选择](#)】，设置审计FTP文件时匹配的文件名关键字。

其他配置步骤请参考章节[\(6\)](#)。



(13) 设置Telnet策略

Telnet协议用于远程登录主机，Telnet策略用于审计基于Telnet协议建立的连接和会话。

配置步骤请参考章节[\(6\)](#)。

添加行为策略

策略组名称: * ☒ 启用该策略 [【用户管理】](#)

策略设置

关联用户

☐ 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

☐ QQ聊天内容

☐ URL重定向

☐ FTP

☒ Telnet

Telnet策略

匹配关键字

添加Telnet策略

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

6.4.4 审计告警

【应用场景】

开启审计告警后，当某一类上网行为被审计时，告警模块会判断该审计结果是否需要告警，并定期汇总，进行邮件告警。

 说明

在开启审计告警前，请先到[\[高级配置\]](#)添加告警的行为策略。

【操作步骤】

- (1) 点击[\[行为管理\]](#)>>[\[行为策略\]](#)>>[\[审计告警\]](#)菜单项。

简易配置

高级配置

审计告警

告警信息查询

说明：当某一类应用被审计时，告警模块判断该审计结果是否需要告警，并定期汇总，进行邮件告警，请先到高级配置添加告警策略。

审计告警：☒

发送告警邮件：☒

邮件主题：

收件人：

确定

前往配置发件邮件

告警周期设置

邮件告警

间隔时间： 分钟

确定

(2) 将“审计告警”设置为开启状态。

(3) 将“发送告警邮件”设置为开启状态，并点击 [前往配置发件邮件](#)，设置发件邮箱参数。

发件邮箱配置

— □ ×

邮件发送开关：☐ 开启

发送邮件服务器：

服务器端口：

邮件发送帐号：

帐号密码：

保存设置

验证配置：

(发送测试邮件前，请先保存配置！)

设置完发件邮箱参数后，点击<保存配置>，然后点击<发送测试邮件>，验证当前发件邮箱设置是否正确。

(4) 填写邮件主题和接收告警信息邮件的邮箱账号，点击<确定>。

(5) 设置邮件告警周期，点击<确定>。

告警周期设置

邮件告警 间隔时间: 分钟

6.4.5 告警信息查询

【应用场景】

本功能用于查询审计告警信息。设备接入硬盘后，开启本地日志存储并重启设备后方可正常显示。

【操作步骤】

(1) 点击[行为管理]>>[行为策略]>>[告警信息查询]菜单项。

时间	用户	IP	策略名	审计类型	访问控制	详细信息
2018-03-27 10:36:57	/192.168.10.3	192.168.10.3	etst	网站访问	告警	网站访问: 访问网址[http://sug.baidu.com/su]
2018-03-27 10:35:35	/192.168.10.3	192.168.10.3	etst	网站访问	告警	网站访问: 访问网址[http://163.com/]
2018-03-27 10:35:35	/192.168.10.3	192.168.10.3	etst	网站访问	告警	网站访问: 访问网址[http://www.163.com/]

(2) 页面将显示所有审计产生的告警信息。选择开始时间、结束时间和审计类型，点击<查询>，可筛选出指定时间段内生成的、指定审计类型的告警信息。

6.5 行为实时审计记录

【应用场景】

本页面主要用于统计用户上网行为的实时审计记录。

说明

由于网站访问及外发信息的记录数通常比较多，本页面不显示这两类上网行为的审计记录。

【操作步骤】

(1) 点击[行为管理]>>[行为实时审计记录]菜单项。

(2) 查看各上网行为的实时审计记录。

说明

由于实时审计通常会产生较多记录数，Web只显示50条审计记录。

实时审计记录

说明：由于网站访问及外发信息的记录数通常比较多，本页面不显示这两个审计记录。

设备开机以来实时审计记录共产生 0 条记录

序号	用户名	审计时间	阻断/放行	应用分类	具体应用	摘要信息
无记录信息						

显示 10 条 共0条

首页 上一页 下一页 末页 1 确定

6.6 行为阻断信息记录

【应用场景】

本页面主要用于统计用户上网行为的阻断信息记录。

【操作步骤】

(1) 点击[行为管理]>>[行为实时审计记录]菜单项。

阻断信息记录

说明：由于网站访问及外发信息的记录数通常比较多，本页面不显示这两个审计记录。

请输入IP 保存 （设置IP后，系统将只记录该IP的阻断信息，之前的所有阻断信息会被删除，若要查看所有IP的阻断信息，请设置为空。）

序号	用户名	审计时间	应用分类	具体应用	匹配策略组	摘要信息
1	1.1.241.10	2017-10-31 10:24:29	search	BING搜索	搜索阻断	详细
2	1.1.241.10	2017-10-31 10:24:07	search	BING搜索	搜索阻断	详细
3	1.1.241.10	2017-10-31 10:16:03	search	BING搜索	搜索阻断	关键字:abcdefg, 搜索类型:网页
4	1.1.241.10	2017-10-31 10:15:41	search	BING搜索	搜索阻断	关键字:abcdefg, 搜索类型:网页
5	1.1.241.10	2017-10-31 10:15:19	search	BING搜索	搜索阻断	关键字:abcdefg, 搜索类型:网页

显示 10 条 共5条

首页 上一页 1 下一页 末页 1 确定

(2) 设置用户的IP地址，并单击<保存>。设置IP后，系统将只记录该IP的阻断信息，之前的所有阻断信息会被删除，若要查看所有IP的阻断信息，请设置为空。

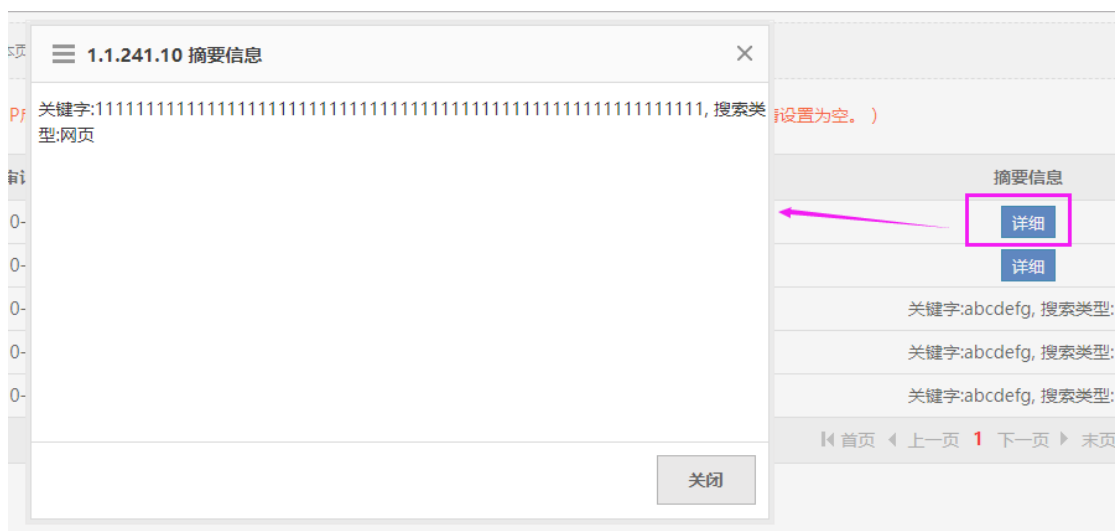
请输入IP

保存

 说明

如果需要查询所有IP的阻断记录，则无需设置IP地址。

(3) 页面显示所设置IP的阻断记录。在“摘要信息”区域，点击<详细>可以查看详细的信息。



6.7 行为审计日志查询

 说明

仅在设备安装硬盘模块后支持本功能。设备接入硬盘后，开启本地日志存储并重启设备后，方可在Web页面正常显示本功能。

6.7.1 访问审计报表

【应用场景】

访问审计报表用于统计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。

【操作步骤】

- (1) 点击[行为管理]>>[行为审计日志]>>[访问审计报告]菜单项。

访问审计报表

内容审计报表

今日审计报表

高级查询

导出报表

网站访问排行

用户访问排行

网站访问明细

被阻断网站

应用控制审计

排行	网站	请求次数	网站类型	操作
1	https://ruijie.com.cn	31	商业	明细 阻断
2	http://cloud.browser.360.cn	24	门户网站与导航	明细 阻断
3	http://www.msn.cn	22	未知分类	明细 阻断
4	https://medlav.com	10	未知分类	明细 阻断
5	http://img1.pcfg.cache.wpscdn.cn	10	未知分类	明细 阻断
6	https://baidu.com	7	百度	明细 阻断
7	https://fanqianbb.com	6	未知分类	明细 阻断
8	https://browser.qq.com	5	IT类	明细 阻断
9	http://l.y.qq.com	4	音乐	明细 阻断
10	http://bbs.csdn.net	4	论坛	明细 阻断

首页

上一页

1

2

3

4

5

下一页

末页

1

确定

(2) 页面显示访问网络的各项审计结果。

● 网站访问排行

“网站访问排行”页签下的表格显示了网站访问次数排行，包括该网站的影响等级、网站分类、访问的次数。

访问审计报表

内容审计报表

今日审计报表

高级查询

导出报表

网站访问排行

用户访问排行

网站访问明细

被阻断网站

应用控制审计

排行	网站	请求次数	网站类型	操作
1	https://ruijie.com.cn	31	商业	明细 阻断
2	http://cloud.browser.360.cn	24	门户网站与导航	明细 阻断
3	http://www.msn.cn	22	未知分类	明细 阻断
4	https://medlav.com	10	未知分类	明细 阻断
5	http://img1.pcfg.cache.wpscdn.cn	10	未知分类	明细 阻断
6	https://baidu.com	7	百度	明细 阻断
7	https://fanqianbb.com	6	未知分类	明细 阻断
8	https://browser.qq.com	5	IT类	明细 阻断
9	http://l.y.qq.com	4	音乐	明细 阻断
10	http://bbs.csdn.net	4	论坛	明细 阻断

首页

上一页

1

2

3

4

5

下一页

末页

1

确定

点击

明细

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

网站访问监控 - Internet Explorer

http://172.18.124.72/beh_report_pi/url_detail.htm

您当前查看的是 **www.baidu.com** 的流量明细

用户(IP)	网站	网站类型	访问时间	访问控制
/100.100.101.53(100.100.101.53)	www.baidu.com/	搜索引擎	2015-09-29 11:13:16	允许
/100.100.101.50(100.100.101.50)	www.baidu.com/	搜索引擎	2015-09-29 11:07:09	允许

首页

上一页

1

下一页

末页

1

确定

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。

● 用户访问排行

“用户访问排行” 页签下的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：

今日审计报表					高级查询	导出报表
网站访问排行	用户访问排行	网站访问明细	被阻断网站	应用控制审计		
排行	用户名	本地用户	网站数	操作		
1	MAC用户		186	明细		
2	1.1.241.10		3	明细		
3	2段		2	明细		
					1	确定

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：

您当前查看的是 100.100.101.50 的流量明细					
用户(IP)	网站	网站类型	访问时间	访问控制	
/100.100.101.50(100.100.101.50)	release.baidu.com/sync2r.htm?cproid=974...	搜索引擎	2015-09-29 11:07:26	允许	
/100.100.101.50(100.100.101.50)	www.shehuitu.com/proxy.html	未知分类	2015-09-29 11:07:26	允许	
/100.100.101.50(100.100.101.50)	bdsp.x.jd.com/adx	网购	2015-09-29 11:07:25	允许	
/100.100.101.50(100.100.101.50)	www.haiwainet.cn/img/LOCAL/common/a...	新闻	2015-09-29 11:07:25	允许	
/100.100.101.50(100.100.101.50)	dspcm.brand.sogou.com/qi	搜索引擎	2015-09-29 11:07:24	允许	
/100.100.101.50(100.100.101.50)	commentn.huanqiu.com/assets/HQ_dataP...	新闻	2015-09-29 11:07:23	允许	
/100.100.101.50(100.100.101.50)	china.huanqiu.com/article/2015-09/76648...	新闻	2015-09-29 11:07:17	允许	
/100.100.101.50(100.100.101.50)	www.baidu.com/	搜索引擎	2015-09-29 11:07:09	允许	
					1 确定

● 网站访问明细

“网站访问明细” 页签下的表格显示的是所有被访问的网站的明细信息，如果想查看具体的某个网站，可以

通过 **高级查询** 输入网址然后查询。

网站访问排行	用户访问排行	网站访问明细	被阻断网站	应用控制审计			
访问时间	用户/IP: 本地用户	网站	网页标题	网站类型	访问控制	匹配规则	
2018-04-04 10:39:52	/192.168.1.132(192.168.1.132)	https://y.qq.com		音乐	允许	默认审计	
2018-04-04 10:39:24	/192.168.1.132(192.168.1.132)	https://hupu.com		体育	允许	默认审计	
2018-04-04 10:38:59	/192.168.1.132(192.168.1.132)	https://baidu.com		搜索引擎	允许	默认审计	
2018-04-04 10:38:33	/192.168.1.132(192.168.1.132)	http://c.y.qq.com/qmmusic/fcgl-bl...		音乐	允许	默认审计	
2018-04-04 10:38:32	/192.168.1.132(192.168.1.132)	https://y.qq.com		音乐	允许	默认审计	
2018-04-04 10:36:41	/192.168.1.132(192.168.1.132)	https://baidu.com		搜索引擎	允许	默认审计	
2018-04-04 10:36:41	/192.168.1.132(192.168.1.132)	http://tieba.baidu.com/home/mai...		论坛	允许	默认审计	
2018-04-04 10:35:44	/192.168.1.132(192.168.1.132)	https://azurewebsites.net		未知分类	允许	默认审计	
2018-04-04 10:34:09	/192.168.1.132(192.168.1.132)	https://hupu.com		体育	允许	默认审计	
2018-04-04 10:33:36	/192.168.1.132(192.168.1.132)	https://rujile.com.cn		商业	允许	默认审计	
					1	确定	

- 被阻断的网站

以表格形式显示了所有被阻断的网站信息。

网站访问排行	用户访问排行	网站访问明细	被阻断网站	应用控制审计			
排行	网站			请求次数	网站类型	操作	
					⏪ 首页 ⏩ 上一页 1 下一页 ⏩ 末页 ⏪		
					1	确定	

点击 **明细** 可以查看选中网站的流量明细：

您当前查看的是 www.tudou.com 的流量明细				
用户(IP)	网站	网站类型	访问时间	访问控制
/100.100.101.50(100.100.101.50)	www.tudou.com/	阻断类	2015-09-29 11:26:15	阻断
首页 上一页 1 下一页 末页 1 确定				

- 应用控制审计

管理员在配置各种应用控制规则后，设备将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员查阅。要查看应用控制审计日志，必须先在行为策略中配置“应用控制”策略（详见[6.4 行为策略](#)），只有策略审计到的记录才会在“应用控制审计”页签下的表格中显示。

网站访问排行	用户访问排行	网站访问明细	被阻断网站	应用控制审计		
用户/IP： 本地用户		审计时间	应用名	VPN接入	访问控制	匹配规则
首页 上一页 1 下一页 末页 1 确定						

“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。

【后续处理】

- 点击 **高级查询** 可以查询指定用户在特定时间范围内访问指定网站的报表记录。

高级查询

×

选择类型：

网站访问明细 ▼

用户类型：

☒ 本地用户
 ☐ 外部用户

选择用户：

所有用户 ▼

时间范围：

2018-4-18

00 ▼ 时 00 ▼ 分 至 23 ▼ 时 00 ▼ 分

网站分类：

选择分类 ▼

【选择分类】 所有分类

网页标题：

确定查询

查询条件

选择类型：网站访问明细

选择用户：所有用户

查询时间：2018-04-04 0时0分至23时0分

查询网站：所有分类

返回报表

访问时间	用户/IP:	网站	网页标题	网站类型	访问控制	匹配规则
2018-04-04 10:40:36	/192.168.1.132(192.168.1.132)	https://itc.cn		未知分类	允许	默认审计
2018-04-04 10:40:35	/192.168.1.132(192.168.1.132)	https://www.sohu.com		门户网站与导航	允许	默认审计
2018-04-04 10:40:35	/192.168.1.132(192.168.1.132)	https://meiqia.com		未知分类	允许	默认审计
2018-04-04 10:40:34	/192.168.1.132(192.168.1.132)	http://www.ouougo.com/news/93...		未知分类	允许	默认审计
2018-04-04 10:40:34	/192.168.1.132(192.168.1.132)	https://alicdn.com		IT类	允许	默认审计
2018-04-04 10:40:33	/192.168.1.132(192.168.1.132)	https://baidu.com		搜索引擎	允许	默认审计
2018-04-04 10:40:10	/192.168.1.132(192.168.1.132)	https://gcp.gvt2.com		未知分类	允许	默认审计
2018-04-04 10:39:52	/192.168.1.132(192.168.1.132)	https://y.qq.com		音乐	允许	默认审计
2018-04-04 10:39:24	/192.168.1.132(192.168.1.132)	https://hupu.com		体育	允许	默认审计
2018-04-04 10:38:59	/192.168.1.132(192.168.1.132)	https://baidu.com		搜索引擎	允许	默认审计

14

首页

上一页

1

2

3

4

5

下一页

末页

1

确定

?

- 点击  导出报表 可以将查询的报表结果导出保存到本地PC上。

6.7.2 内容审计报表

【应用场景】

内容审计报表用于统计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、论坛发帖、搜索引擎、Web页面、FTP、Telnet的内容审计。

【操作步骤】

- (1) 点击[行为管理]>>[行为审计日志]>>[内容审计报表]菜单项。
- (2) 页面显示各项审计结果。

访问审计报表

内容审计报表

时间范围：

本日

本周

高级查询

导出报表

客户端邮件

WEB邮件

IM聊天

论坛发帖

搜索引擎

虚拟身份

插件QQ聊天内容

外发文件

外发信息

FTP

TELNET

用户名(IP)

本地用户

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

首页

上一页

1

下一页

末页

1

确定

● 客户端邮件

设备支持对客户端邮件进行审计，如foxmail、outlook等。用户可以通过“客户端邮件”页签下的表格查看当前有哪些用户在使用客户端邮件、邮件的接收者、邮件主要内容等信息：

客户端邮件	WEB邮件	IM聊天	论坛发帖	搜索引擎	虚拟身份	插件QQ聊天内容	外发文件	外发信息	FTP
TELNET									
用户名(IP)本地用户	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	
12345678910111213141516171819202122232425262728293031323334353637383940414243444546474849505152535455565758596061626364656667686970717273747576777879808182838485868788899091929394959697989910010110210310410510610710810911011111211311411511611711811912012112212312412512612712812913013113213313413513613713813914014114214314414514614714814915015115215315415515615715815916016116216316416516616716816917017117217317417517617717817918018118218318418518618718818919019119219319419519619719819920020120220320420520620720820921021121221321421521621721821922022122222322422522622722822923023123223323423523623723823924024124224324424524624724824925025125225325425525625725825926026126226326426526626726826927027127227327427527627727827928028128228328428528628728828929029129229329429529629729829930030130230330430530630730830931031131231331431531631731831932032132232332432532632732832933033133233333433533633733833934034134234334434534634734834935035135235335435535635735835936036136236336436536636736836937037137237337437537637737837938038138238338438538638738838939039139239339439539639739839940040140240340440540640740840941041141241341441541641741841942042142242342442542642742842943043143243343443543643743843944044144244344444544644744844945045145245345445545645745845946046146246346446546646746846947047147247347447547647747847948048148248348448548648748848949049149249349449549649749849950050150250350450550650750850951051151251351451551651751851952052152252352452552652752852953053153253353453553653753853954054154254354454554654754854955055155255355455555655755855956056156256356456556656756856957057157257357457557657757857958058158258358458558658758858959059159259359459559659759859960060160260360460560660760860961061161261361461561661761861962062162262362462562662762862963063163263363463563663763863964064164264364464564664764864965065165265365465565665765865966066166266366466566666766866967067167267367467567667767867968068168268368468568668768868969069169269369469569669769869970070170270370470570670770870971071171271371471571671771871972072172272372472572672772872973073173273373473573673773873974074174274374474574674774874975075175275375475575675775875976076176276376476576676776876977077177277377477577677777877978078178278378478578678778878979079179279379479579679779879980080180280380480580680780880981081181281381481581681781881982082182282382482582682782882983083183283383483583683783883984084184284384484584684784884985085185285385485585685785885986086186286386486586686786886987087187287387487587687787887988088188288388488588688788888989089189289389489589689789889990090190290390490590690790890991091191291391491591691791891992092192292392492592692792892993093193293393493593693793893994094194294394494594694794894995095195295395495595695795895996096196296396496596696796896997097197297397497597697797897998098198298398498598698798898999099199299399499599699799899910001001100210031004100510061007100810091010101110121013101410151016101710181019102010211022102310241025102610271028102910301031103210331034103510361037103810391040104110421043104410451046104710481049105010511052105310541055105610571058105910601061106210631064106510661067106810691070107110721073107410751076107710781079108010811082108310841085108610871088108910901091109210931094109510961097109810991100110111021103110411051106110711081109111011111112111311141115111611171118111911201121112211231124112511261127112811291130113111321133113411351136113711381139114011411142114311441145114611471148114911501151115211531154115511561157115811591160116111621163116411651166116711681169117011711172117311741175117611771178117911801181118211831184118511861187118811891190119111921193119411951196119711981199120012011202120312041205120612071208120912101211121212131214121512161217121812191220122112221223122412251226122712281229123012311232123312341235123612371238123912401241124212431244124512461247124812491250125112521253125412551256125712581259126012611262126312641265126612671268126912701271127212731274127512761277127812791280128112821283128412851286128712881289129012911292129312941295129612971298129913001301130213031304130513061307130813091310131113121313131413151316131713181319132013211322132313241325132613271328132913301331133213331334133513361337133813391340134113421343134413451346134713481349135013511352135313541355135613571358135913601361136213631364136513661367136813691370137113721373137413751376137713781379138013811382138313841385138613871388138913901391139213931394139513961397139813991400140114021403140414051406140714081409141014111412141314141415141614171418141914201421142214231424142514261427142814291430143114321433143414351436143714381439144014411442144314441445144614471448144914501451145214531454145514561457145814591460146114621463146414651466146714681469147014711472147314741475147614771478147914801481148214831484148514861487148814891490149114921493149414951496149714981499150015011502150315041505150615071508150915101511151215131514151515161517151815191520152115221523152415251526152715281529153015311532153315341535153615371538153915401541154215431544154515461547154815491550155115521553155415551556155715581559156015611562156315641565156615671568156915701571157215731574157515761577157815791580158115821583158415851586158715881589159015911592159315941595159615971598159916001601160216031604160516061607160816091610161116121613161416151616161716181619162016211622162316241625162616271628162916301631163216331634163516361637163816391640164116421643164416451646164716481649165016511652165316541655165616571658165916601661166216631664166516661667166816691670167116721673167416751676167716781679168016811682168316841685168616871688168916901691169216931694169516961697169816991700170117021703170417051706170717081709171017111712171317141715171617171718171917201721172217231724172517261727172817291730173117321733173417351736173717381739174017411742174317441745174617471748174917501751175217531754175517561757175817591760176117621763176417651766176717681769177017711772177317741775177617771778177917801781178217831784178517861787178817891790179117921793179417951796179717981799180018011802180318041805180618071808180918101811181218131814181518161817181818191820182118221823182418251826182718281829183018311832183318341835183618371838183918401841184218431844184518461847184818491850185118521853185418551856185718581859186018611862186318641865186618671868186918701871187218731874187518761877187818791880188118821883188418851886188718881889189018911892189318941895189618971898189919001901190219031904190519061907190819091910191119121913191419151916191719181919192019211922192319241925192619271928192919301931193219331934193519361937193819391940194119421943194419451946194719481949195019511952195319541955195619571958195919601961196219631964196519661967196819691970197119721973197419751976197719781979198019811982198319841985198619871988198919901991199219931994199519961997199819992000200120022003200420052006200720082009201020112012201320142015201620172018201920202021202220232024202520262027202820292030203120322033203420352036203720382039204020412042204320442045204620472048204920502051205220532054205520562057205820592060206120622063206420652066206720682069207020712072207320742075207620772078207920802081208220832084208520862087208820892090209120922093209420952096209720982099210021012102210321042105210621072108210921102111211221132114211521162117211821192120212121222123212421252126212721282129213021312132213321342135213621372138213921402141214221432144214521462147214821492150215121522153215421552156215721582159216021612162216321642165216621672168216921702171217221732174217521762177217821792180218121822183218421852186218721882189219021912192219321942195219621972198219922002201220222032204220522062207220822092210221122122213221422152216221722182219222022212222222322242225222622272228222922302231223222332234223522362237223822392240224122422243224422452246224722482249225022512252225322542255225622572258225922602261226222632264226522662267226822692270227122722273227422752276227722782279228022812282228322842285228622872288228922902291229222932294229522962297229822992300230123022303230423052306230723082309231023112312231323142315231623172318231923202321232223232324232523262327232823292330233123322333233423352336233723382339234023412342234323442345234623472348234923502351235223532354235523562357235823592360236123622363236423652366236723682369237023712372237323742375237623772378237923802381238223832384238523862387238823892390239123922393239423952396239723982399240024012402240324042405240624072408240924102411241224132414241524162417241824192420242124222423242424252426242724282429243024312432243324342435243624372438243924402441244224432444244524462447244824492450245124522453245424552456245724582459246024612462246324642465246624672468246924702471247224732474247524762477247824792480248124822483248424852486248724882489249024912492249324942495249624972498249925002501250225032504250525062507250825092510251125122513251425152516251725182519252025212522252325242525252625272528252925302531253225332534253525362537253825392540254125422543254425452546254725482549255025512552255325542555255625572558255925602561256225632564256525662567256825692570257125722573257425752576257725782579258025812582258325842585258625872588258925902591259225932594259525962597259825992600260126022603260426052606260726082609261026112612261326142615261626172618261926202621262226232624262526262627262826292630263126322633263426352636263726382639264026412642264326442645264626472648264926502651265226532654265526562657265826592660266126622663266426652666266726682669267026712672267326742675267626772678267926802681268226832684268526862687268826892690269126922693269426952696269726982699270027012702270327042705270627072708270927102711271227132714271527162717271827192720272127222723272427252726272727282729273027312732273327342735273627372738273927402741274227432744274527462747274827492750275127522753275427552756275727582759276027612762276327642765276627672768276927702771277227732774277527762777277827792780278127822783278427852786278727882789279027912792279327942795279627972798279928002801280228032804280528062807280828092810281128122813281428152816281728182819282028212822282328242825282628272828282928302831283228332834283528362837283828392840284128422843284428452846284728482849285028512852285328542855285628572858285928602861286228632864286528662867286828692870287128722873287428752876287728782879288028812882288328842885288628872888288928902891289228932894289528962897289828992900290129022903290429052906290729082909291029112912291329142915291629172918291929202921292229232924292529262927292829292930293129322933293429352936293729382939294029412942294329442945294629472948294929502951295229532954295529562957295829592960296129622963296429652966296729682969297029712972297329742975297629772978297929802981298229832984298529862987298829892990299129922993299429952996299729982999300030013002300330043005300630073008300930103011301230133014301530163017301830193020302130223023302430253026302730283029303030313032303330343035303630373038303930403041304230433044304530463047304830493050305130523053305430553056305730583059306030613062306330643065306630673068306930703071307230733074307530763077307830793080308130823083308430853086308730883089309030913092309330943095309630973098309931003101310231033104310531063107310831093110311131123113311431153116311731183119312031213122312331243125312631273128312931303131313231333134313531363137313831393140314131423143314431453146314731483149315031513152315331543155315631573158315931603161316231633164316531663167316831693170317131723173317431753176317731783179318031813182318331843185318631873188318931903191319231933194319531963197319831993200320132023203320432053206320732083209321032113212321332143215321632173218321932203221322232233223432253226322732283229323032313232323332343235323632373238323932403241324232433244324532463247324832493250325132523253325432553256325732583259326032613262326332643265326632673268326932703271327232733274327532763277327832793280328132823283328432853286328732883289329032913292329332943295329632973298329933003301330233033304330533063307330833093310331133123313331433153316331733183319332033213322332333243325332633273328332933303331									

● Web端邮件

设备支持对Web端邮件进行审计，如新浪、163、雅虎等。用户可以通过“WEB端邮件”页签下的表格查看当前有哪些用户在使用Webmail、邮件的接收者、邮件主要内容等信息。

时间范围： **本日** 本周 Q 高级查询 导出报表

客户端邮件 WEB邮件 IM聊天 论坛发帖 搜索引擎 虚拟身份 插件QQ聊天内容 外发文件 外发信息 FTP

TELNET

用户名(IP)	本地用户	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
首页 < 上一页 1 下一页 > 末页								

1 确定

● IM聊天

设备支持对QQ、MSN等聊天软件的上下线记录和内容进行审计。点击“IM聊天”页签，审计信息如下表所示：

客户端邮件 WEB邮件 IM聊天 论坛发帖 搜索引擎 虚拟身份 插件QQ聊天内容 外发文件 外发信息 FTP

TELNET

用户名(IP)	本地用户	审计时间	操作类型	信息内容	访问控制	匹配规则
首页 < 上一页 1 下一页 > 末页						

1 确定

● 论坛发帖

设备支持对BBS论坛内容进行审计，包括天涯社区、猫扑、动网官方网站、PHPWIN官方网站等。点击“论坛发帖”页签，审计信息如下表所示：

客户端邮件 WEB邮件 IM聊天 论坛发帖 搜索引擎 虚拟身份 插件QQ聊天内容 外发文件 外发信息 FTP

TELNET

用户名(IP)	本地用户	审计时间	网页地址	具体应用	发送帐号	发帖标题/内容	访问控制	匹配规则
首页 < 上一页 1 下一页 > 末页								

1 确定

● 搜索引擎

设备支持对各种搜索引擎进行审计，包括百度、Google、雅虎等搜索引擎。点击“论坛发帖”页签，管理员可以查看哪些用户、在哪个时间段、用什么搜索引擎、搜索了什么内容等信息。

客户端邮件 WEB邮件 IM聊天 论坛发帖 搜索引擎 虚拟身份 插件QQ聊天内容 外发文件 外发信息 FTP

TELNET

用户名(IP)	本地用户	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
首页 < 上一页 1 下一页 > 末页								

1 确定

● 虚拟身份

设备支持审计微信、QQ、新浪微博等应用中用户帐户上线下线的记录。点击“虚拟身份”页签，管理员可以查看具体的审计时间和帐号信息。

客户端邮件 WEB邮件 IM聊天 论坛发帖 搜索引擎 虚拟身份 插件QQ聊天内容 外发文件 外发信息 FTP

TELNET

用户名(IP)	本地用户	审计时间	具体应用	帐号	昵称	账号ID	操作类型	访问控制	匹配规则
首页 < 上一页 1 下一页 > 末页									

1 确定

● 插件QQ聊天内容

设备支持审计QQ聊天内容（终端需安装插件）。点击“插件QQ聊天内容”页签，查看QQ消息的发送方和接收方、消息内容等详细信息。

客户端邮件	WEB邮件	IM聊天	论坛发帖	搜索引擎	虚拟身份	插件QQ聊天内容	外发文件	外发信息	FTP
TELNET									
用户名(IP)	本地用户	审计时间	具体应用	发送类型	发送帐号	发送qq号	接收帐号	接收qq号	消息内容
首页 上一页 1 下一页 末页 1 确定									

- 外发文件

设备支持审计向外发送的文件信息。点击“外发文件”页签，可以查看发送文件的帐号、文件名、文件大小等审计信息。

客户端邮件	WEB邮件	IM聊天	论坛发帖	搜索引擎	虚拟身份	插件QQ聊天内容	外发文件	外发信息	FTP
TELNET									
用户名(IP)	本地用户	审计时间	具体应用	发送帐号	文件大小	文件名	访问控制	匹配规则	
首页 上一页 1 下一页 末页 1 确定									

- 外发信息

设备支持审计部分HTTP网站使用POST报文访问的信息。

客户端邮件	WEB邮件	IM聊天	论坛发帖	搜索引擎	虚拟身份	插件QQ聊天内容	外发文件	外发信息	FTP
TELNET									
用户名(IP)	本地用户	审计时间	具体应用	网页地址	发送内容	访问控制	匹配规则		
首页 上一页 1 下一页 末页 1 确定									

- FTP

设备支持审计FTP方式传输的文件。点击“FTP”页签，可以查看传输的目的IP地址、文件名、传输方向等详细信息。

客户端邮件	WEB邮件	IM聊天	论坛发帖	搜索引擎	虚拟身份	插件QQ聊天内容	外发文件	外发信息	FTP
TELNET									
用户名(IP)	本地用户	审计时间	目的ip	文件名	传输方向	访问控制	匹配规则		
首页 上一页 1 下一页 末页 1 确定									

- Telnet

设备支持审计基于Telnet协议建立的连接和会话。点击“TELNET”页签，可以查看对应审计信息。

客户端邮件	WEB邮件	IM聊天	论坛发帖	搜索引擎	虚拟身份	插件QQ聊天内容	外发文件	外发信息	FTP
TELNET									
用户名(IP)	本地用户	审计时间	目的ip	动作	访问控制	匹配规则			
首页 上一页 1 下一页 末页 1 确定									

【后续处理】

- 点击<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。

1、点击展开高级查询 [高级查询](#)

高级查询

2、选择查询类型

选择类型：全部

用户类型：☒本地用户 ☐外部用户

选择用户：所有用户

关键字：全部

时间范围：2015-9-29 00:00 至 2015-9-29 23:59

访问控制：默认

3、选择过滤参数

确定查询

4、点击确定查询

查询结果如下图所示：

查询条件 [高级查询](#) [导出报表](#)

选择类型：WEB端邮件

选择用户：所有用户

查询时间：2015-9-29 00时00分至 2015-9-29 23时59分

关键字：全部

[返回报表](#)

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
/周同学 (100.100.101.53)	2015-09-29 14:35:11	lanzhusiyu@foxmai...	445612727@qq.com	这是一封公司测试的邮件【详细】	允许	默认审计
/周同学 (100.100.101.53)	2015-09-29 14:34:37	lanzhusiyu@foxmai...	445612727@qq.com	test【详细】	允许	默认审计

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶ [1](#) [确定](#)

可以选择导出的数据

- 通过 [导出报表](#) 按钮可以导出各种内容审计报表。

6.8 行为统计分析

说明

仅在设备安装硬盘模块后支持本功能。设备接入硬盘后，开启本地日志存储并重启设备后，方可在Web页面正常显示本功能。

6.8.1 功能简介

显示各种行为的流量报表，以便更好地进行网络行为监控。

说明

使用该功能前，请确保设备已经正确安装硬盘模块。

6.8.2 报表配置

【应用场景】

通过开启报表预生成开关，实现统计数据能在后台自动生成和存储，便于查看审计报表。

【操作步骤】

- (1) 点击[行为管理]>>[行为统计分析]>>[报表配置]菜单项。
- (2) 开启<报表预生成>开关。

报表配置 | 搜索引擎 | 论坛发帖 | 外发文件 | 网站分类 | 网站域名 | 虚拟身份

注意:

- 1.为了减少审计报表查询等待的时间，我们采用数据后台预生成的方式，因此要想查询审计报表，必须先打开开关。
- 2.报表预生成开关打开后，凌晨（默认凌晨3点）设备会在后台生成审计报表数据，此时可能造成CPU短时间内升高，并且会消耗一定的硬盘存储空间。
- 3.报表预生成开关打开后，当天的数据可以在第二天（默认凌晨3点后）查询，在这之前的数据将无法查询，因此如果需要查询审计报表，建议提前开启本功能。

报表预生成: ☒ ON

6.8.3 自定义报表

【应用场景】

管理员可以自定义报表生成规则，定期获取所需的用户上网行为数据。

【操作步骤】

- (1) 点击[行为管理]>>[行为统计分析]>>[自定义报表]菜单项。

规则名称	已生成报表	订阅邮箱	订阅周期	操作
111	0	无	按天	编辑 删除
3	0	无	按天	编辑 删除
2	15	yjh277@126.com, 123@126.com	按天	编辑 删除

显示: 10 条 共3条

- (2) 点击<添加规则>。

添加规则

规则名称:

统计周期:

显示TOP:

用户类型: ☒ 本地用户

选择用户:

排行报表: ☒ 搜索引擎 ☐ 论坛发帖 ☐ 外发文件 ☐ 网站分类 ☐ 网站域名 ☐ 虚拟身份 ☐ 客户端邮件 ☐ 网页邮件 ☒ IM聊天

是否发送邮件: ☐ 是 ☒ 否

[保存](#) [关闭](#)

(3) 设置报表生成规则。

(4) 点击<保存>。

【后续处理】

- 选择待修改的报表规则项，点击<编辑>可以修改规则项的相关配置。

报表配置	自定义报表	客户端邮件	WEB邮件	IM聊天	搜索引擎	论坛发帖	外发文件	网站分类	网站域名	虚拟身份
+ 添加规则 X 删除选中										
☐	规则名称	已生成报表	订阅邮箱		订阅周期		操作			
☐	test	0	无		按天		编辑 删除			
☐	111	0	无		按天		编辑 删除			
☐	3	0	无		按天		编辑 删除			
☐	2	15	yjh277@126.com,123@126.com		按天		编辑 删除			
显示: 10 条 共4条										
[<] [首页] [上一] 1 [下一] [末页] [>]										1 确定

说明

修改规则项后，基于对应规则已生成的报表数据将会被清除。

- 选择待删除的报表规则项，点击<删除>可以删除该规则项。

1.1.1.3:4430 显示 确定要删除规则 test 吗？本规则已生成的报表数据将会被清空！是否需要继续？										
确定 取消										

- 点击<已生成报表>，可以查看已经生成的报表，并进行下载、删除操作。

报表配置

自定义报表

客户端邮件

WEB邮件

IM聊天

搜索引擎

论坛发帖

外发文件

网站分类

网站域名

虚拟身份

三 报表列表

✕

刷新

✕ 删除选中

☐	报表名称	统计时间	订阅周期	生成时间	PDF报表	操作
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 09:43:19	下载	删除
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 09:38:18	下载	删除
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 09:30:32	下载	删除
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 08:58:37	下载	删除
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 08:53:41	下载	删除
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 13:52:07	下载	删除
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 13:44:52	下载	删除
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 13:42:11	下载	删除
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 13:11:03	下载	删除
☐	2	2018-05-03 00:00:00 -- 2018-05-03 23:59:59	按天	2018-05-04 13:04:02	下载	删除

显示: 10 条 共15条

1 2

首页

上一页

下一页

末页

1

确定

6.8.4 客户端邮件

【应用场景】

管理员可以定义客户端邮件的行为统计规则，并获取与统计规则匹配的统计信息。

【操作步骤】

(1) 点击[行为管理]>>[行为统计分析]>>[客户端邮件]菜单项。

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:

发邮件数排行

显示TOP:

10

用户类型:

☒ 本地用户

选择用户:

所有用户

统计周期:

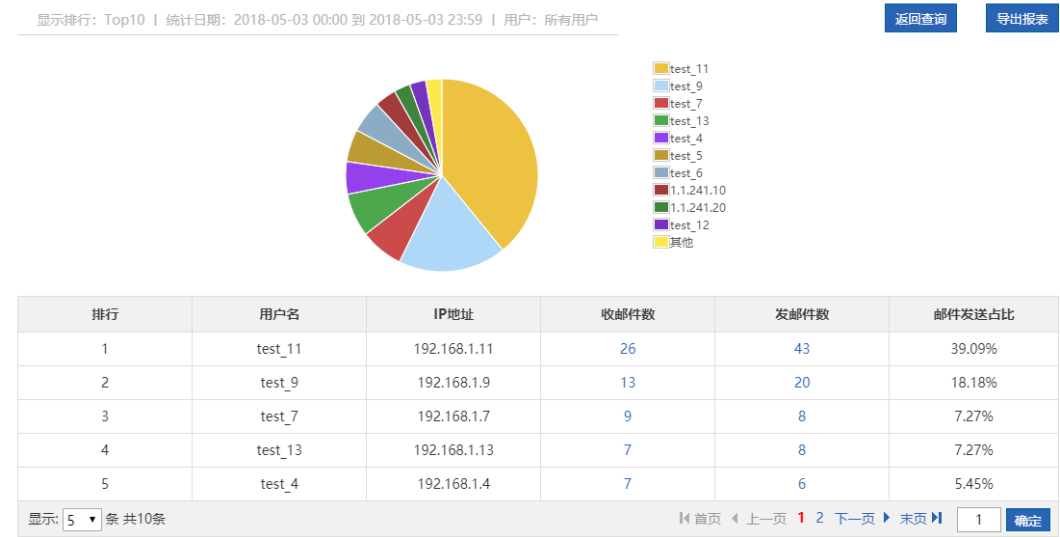
天

选择时间:

2018-07-12

确定查询

- (2) 设置统计规则，可指定统计维度、用户类型、统计周期、统计日期等条件。
- (3) 点击<确定查询>，系统显示查询结果。点击“收/发邮件数”的统计数字，可查看具体邮件信息。



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

6.8.5 Web 邮件

【应用场景】

管理员可以定义Web邮件的统计规则，并获取与统计规则匹配的统计信息。

【操作步骤】

(1) 点击[行为管理]>>[行为统计分析]>>[Web邮件]菜单项。

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

(2) 设置统计规则，可指定统计维度、用户类型、统计周期、统计日期等条件。

(3) 点击<确定查询>，系统显示查询结果。



- 点击查询结果表格中<应用类型统计>列的内容，可查看用户使用各类型应用发送邮件的次数以及邮件数排行。



- 点击查询结果表格中<邮件总数>列的内容，可查看用户收发邮件的详细信息，包括发件人帐号、收件人帐号和邮件内容等。

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							
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 9							

6.8.6 IM 聊天

【应用场景】

管理员可以定义对IM聊天行为的统计规则，并获取与统计规则匹配的统计信息。

【操作步骤】

- (1) 点击[行为管理]>>[行为统计分析]>>[IM聊天]菜单项。

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

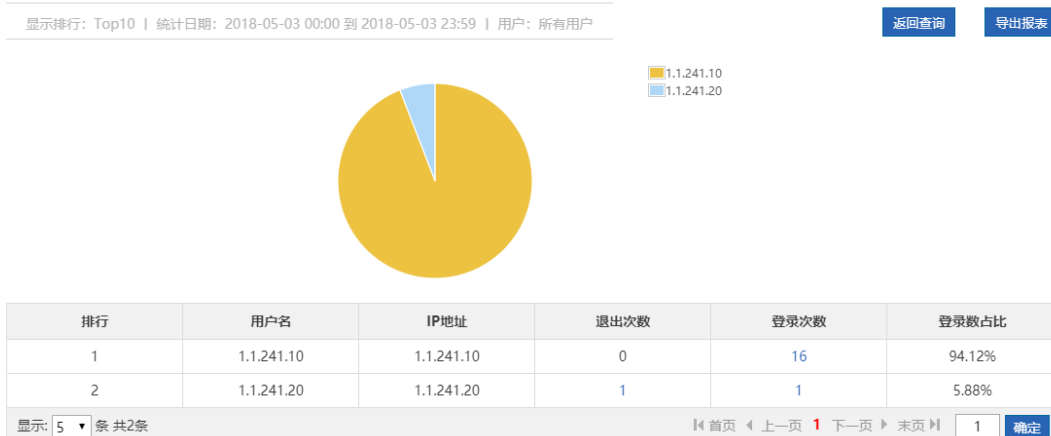
选择用户: 所有用户 ▼

统计周期: 天 ▼

选择时间: 2018-07-12

确定查询

- (2) 设置统计规则，可指定统计维度、用户类型、统计周期、统计日期等条件。
- (3) 点击<确定查询>，系统显示查询结果。



三 用户登录信息

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	操作类型	信息内容	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

6.8.7 搜索引擎

【应用场景】

管理员可以定义对使用搜索引擎行为的统计规则，并获取与统计规则匹配的统计信息。

【操作步骤】

(1) 点击[行为管理]>>[行为统计分析]>>[搜索引擎]菜单项。

报表配置 搜索引擎 论坛发帖 外发文件 网站分类 网站域名 虚拟身份

统计维度: 关键字排行

显示TOP: 10

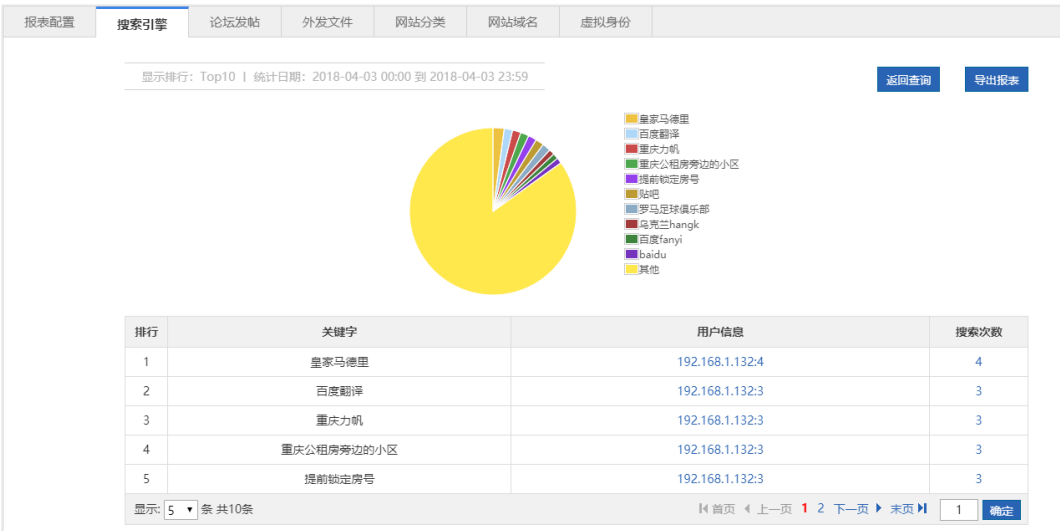
统计周期: 天

选择时间: 2018-04-03

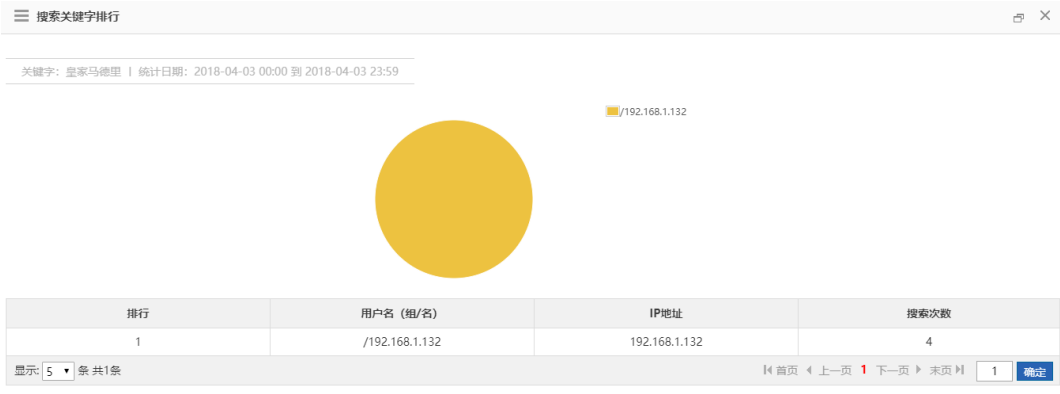
[确定查询](#)

(2) 设置统计规则，可以设置统计维度、统计周期、时间范围等条件。

(3) 点击<确定查询>，系统显示查询结果。



○ 点击查询结果表格中<用户信息>列的内容，可以查看详细的用户信息。



○ 点击查询结果表格中<搜索次数>列的数字，可以查看具体的搜索信息。

关键字搜索信息

关键字: 皇家马德里

统计日期: 2018-04-03 00:00 到 2018-04-03 23:59

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

6.8.8 论坛发帖

【应用场景】

管理员可以定义论坛发帖行为的统计规则，并获取与统计规则匹配的统计信息。

【操作步骤】

(1) 点击[行为管理]>>[行为统计分析]>>[论坛发帖]菜单项。

报表配置

搜索引擎

论坛发帖

外发文件

网站分类

网站域名

虚拟身份

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：

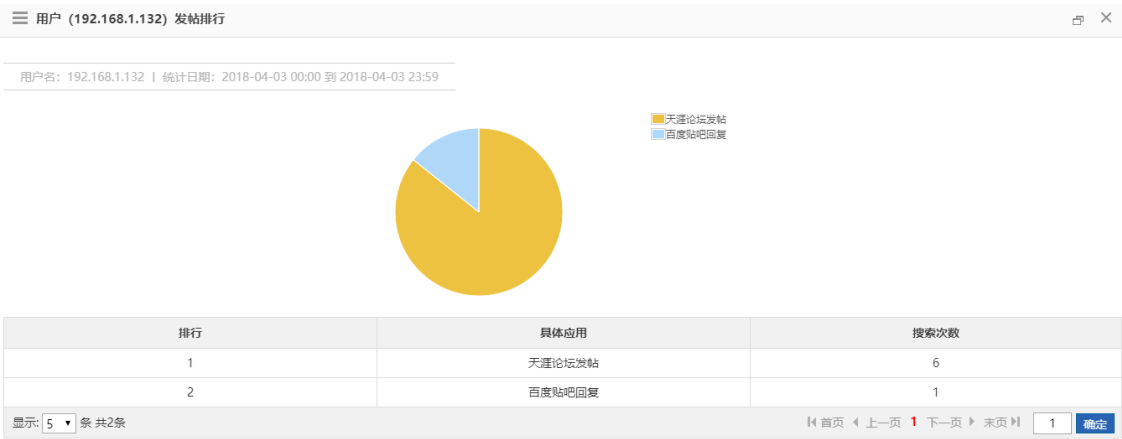
2018-04-03

确定查询

- (2) 设置统计规则，可指定统计维度、用户组、统计周期、时间范围等条件。
- (3) 点击<确定查询>，系统显示查询结果。



- 点击查询结果表格中<发帖统计>列的内容，可查看每个用户的发帖排行。



- 点击查询结果表格中<发帖次数>列的数字，可以查看每个用户的具体发帖信息。

三 用户发帖信息

用户名: 192.168.1.132
统计日期: 2018-04-03 00:00 到 2018-04-03 23:59

用户名(IP)	审计时间	网页地址	具体应用	发送帐号	发帖标题/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 024c3cdb-defdf807699d6afb	【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

6.8.9 外发文件

【应用场景】

管理员可以定义对于外发文件行为的统计规则，并获取与统计规则匹配的统计信息。

【操作步骤】

(1) 点击[行为管理]>>[行为统计分析]>>[外发文件]菜单项。

报表配置

搜索引擎

论坛发帖

外发文件

网站分类

网站域名

虚拟身份

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: 2018-04-03

确定查询

(2) 设置统计规则。

(3) 点击<确定查询>，系统显示查询结果。



- 点击查询结果表格中<外发文件统计>列的内容，可以查看用户进行外发文件的应用和次数。



- 点击查询结果表格中<外发次数>列的数字，可以获取用户外发文件的详细信息，包括发送文件的应用、发送帐号、文件名、文件大小等。

用户搜索信息

用户名: 192.168.1.132

统计日期: 2018-04-03 00:00 到 2018-04-03 23:59

用户名(IP)	审计时间	具体应用	发送帐号	文件大小	文件名	访问控制	匹配规则
/192.168.1.132(192.168.1.132)	2018-04-03 15:56:41	天涯论坛发图片	勿忘心雨	9455	QQ111.jpg	允许	默认审计

显示: 10 条

首页 < 上一页 1 下一页 > 末页 确定

6.8.10 网站分类

【应用场景】

管理员可以定义网站受访情况的统计规则，并获取基于网站分类的、与统计规则匹配的统计信息。

【操作步骤】

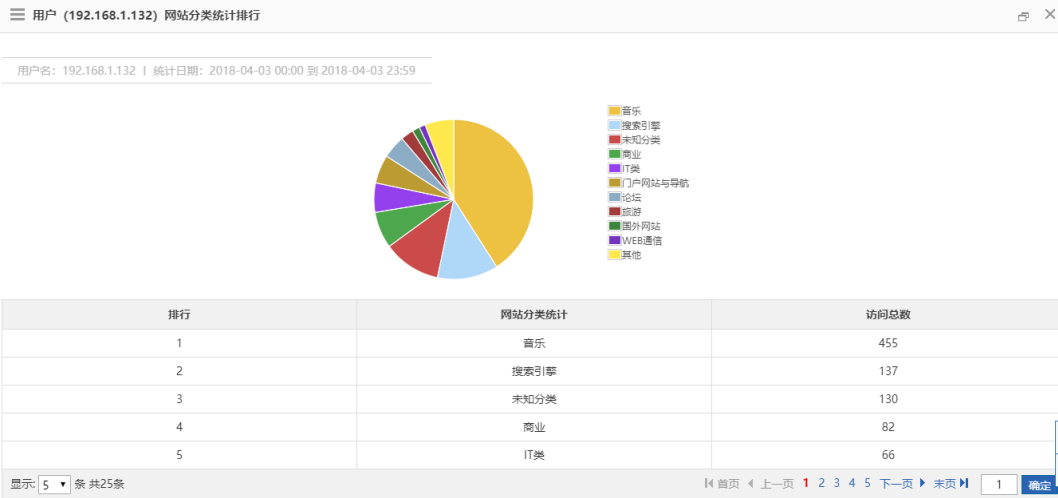
- (1) 点击[行为管理]>>[行为统计分析]>>[网站分类]菜单项。

报表配置	搜索引擎	论坛发帖	外发文件	网站分类	网站域名	虚拟身份
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: 2018-04-03 确定查询						

- (2) 设置统计规则。
- (3) 点击<确定查询>，系统显示查询结果。



○ 点击查询结果表格中<网站分类统计>列的内容，可以查看基于网站分类的访问次数排行。



○ 点击查询结果表格中<访问总数>列的数字，可以查看用户访问的具体网址信息。

三 用户搜索信息

用户名: 192.168.1.132

统计日期: 2018-04-03 00:00 到 2018-04-03 23:59

审计时间	用户名(IP)	网页地址	网站类型	访问控制
2018-04-03 10:04:56	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许
2018-04-03 10:04:56	/192.168.1.132(192.168.1.132)	http://c.y.qq.com/q...	音乐	允许
2018-04-03 10:07:22	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许
2018-04-03 10:08:58	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许
2018-04-03 10:08:58	/192.168.1.132(192.168.1.132)	http://c.y.qq.com/q...	音乐	允许
2018-04-03 10:11:25	/192.168.1.132(192.168.1.132)	https://ruijie.com.cn	商业	允许
2018-04-03 10:12:37	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许
2018-04-03 10:12:37	/192.168.1.132(192.168.1.132)	http://c.y.qq.com/q...	音乐	允许
2018-04-03 10:15:36	/192.168.1.132(192.168.1.132)	https://google.com	搜索引擎	允许
2018-04-03 10:15:42	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许

显示: 10 条

首页 < 上一页 1 2 3 4 5 6 7 8 9 10 下一页 > 末页

6.8.11 网站域名

【应用场景】

管理员可以定义网站域名受访情况的统计规则，并获取与统计规则匹配的统计信息。

【操作步骤】

(1) 点击[行为管理]>>[行为统计分析]>>[网站域名]菜单项。

报表配置

搜索引擎

论坛发帖

外发文件

网站分类

网站域名

虚拟身份

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:

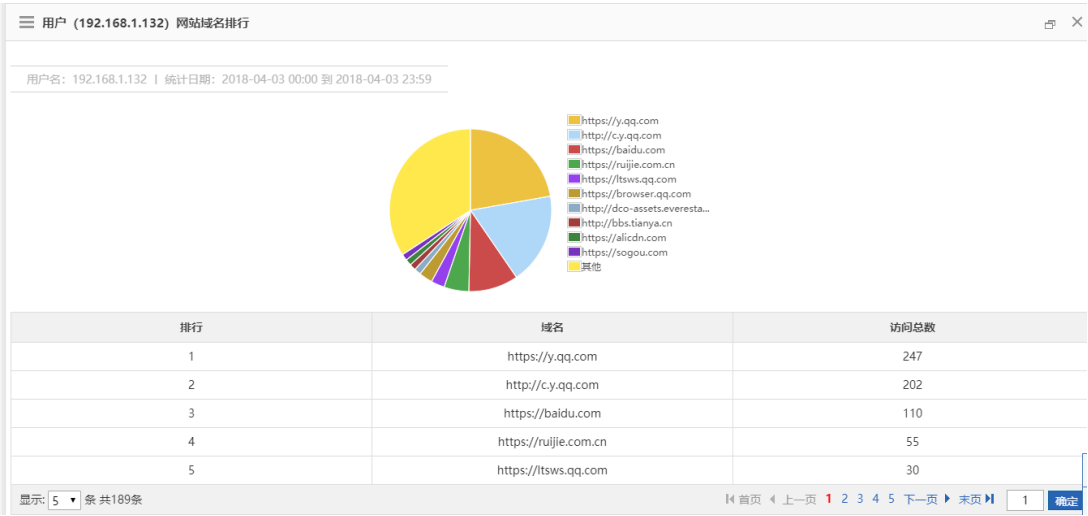
2018-04-03

确定查询

- (2) 设置统计规则。
- (3) 点击<确定查询>，系统显示查询结果。



- 点击查询结果表格中<域名统计>列的内容，可以查看每个用户访问各网站域名的总次数以及在各网站域名中的访问占比情况。



- 点击查询结果表格中<访问总数>列的数字，可以某个用户访问网站域名的信息。

三 用户搜索信息

用户名: 192.168.1.132

统计日期: 2018-04-03 00:00 到 2018-04-03 23:59

审计时间	用户名(IP)	网页地址	网站类型	访问控制
2018-04-03 10:04:56	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许
2018-04-03 10:04:56	/192.168.1.132(192.168.1.132)	http://c.y.qq.com/q...	音乐	允许
2018-04-03 10:07:22	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许
2018-04-03 10:08:58	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许
2018-04-03 10:08:58	/192.168.1.132(192.168.1.132)	http://c.y.qq.com/q...	音乐	允许
2018-04-03 10:11:25	/192.168.1.132(192.168.1.132)	https://rujie.com.cn	商业	允许
2018-04-03 10:12:37	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许
2018-04-03 10:12:37	/192.168.1.132(192.168.1.132)	http://c.y.qq.com/q...	音乐	允许
2018-04-03 10:15:36	/192.168.1.132(192.168.1.132)	https://google.com	搜索引擎	允许
2018-04-03 10:15:42	/192.168.1.132(192.168.1.132)	https://y.qq.com	音乐	允许

显示: 10 条

首页 < 上一页 1 2 3 4 5 6 7 8 9 10 下一页 > 末页 1 确定

6.8.12 虚拟身份

【应用场景】

虚拟身份是指用户在上网过程中，用于访问网页、软件应用所注册和使用的帐号。管理员可以定义对于用户上网过程中使用虚拟身份的行为的统计规则，并获取与统计规则匹配的统计信息。

【操作步骤】

- (1) 点击[行为管理]>>[行为统计分析]>>[虚拟身份]菜单项。

报表配置 搜索引擎 论坛发帖 外发文件 网站分类 网站域名 虚拟身份

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

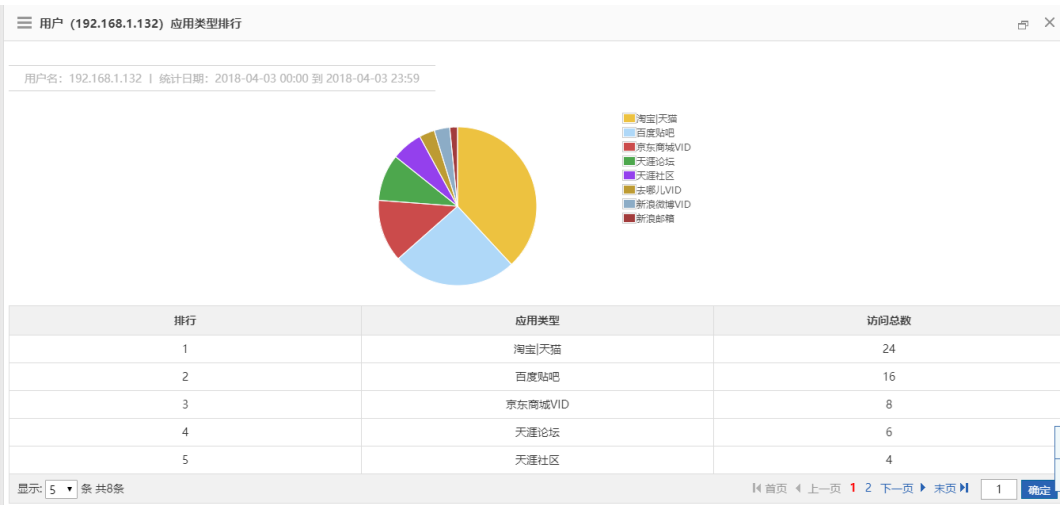
选择时间: 2018-04-03

确定查询

- (2) 设置统计规则。
- (3) 点击<确定查询>，系统显示查询结果。



○ 点击查询结果表格中<应用类型统计>列的内容，可以获取单个用户基于应用类型的访问次数统计结果。



○ 点击查询结果表格中<访问总数>列的数字，可以查询单个用户访问各类应用的具体行为信息，包括使用应用、帐号信息、操作类型（登录、登出）等。

三 用户搜索信息

用户名: 192.168.1.132

统计日期: 2018-04-03 00:00 到 2018-04-03 23:59

用户名(IP)	审计时间	具体应用	帐号	昵称	账号ID	操作类型	访问控制	匹配规则
/192.168.1.132(192.168.1.132)	2018-04-03 10:05:35	新浪邮箱			1517133649171_68601297	LOGIN	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 10:52:33	淘宝[天猫			taobao.com	LOGIN	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 10:59:08	去哪儿VID	pedjpbv3527	Rainman_ %E9%98%A8		LOGIN	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 11:02:35	淘宝[天猫			taobao.com	LOGOUT	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 11:09:03	淘宝[天猫			taobao.com	LOGIN	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 11:16:23	新浪微博VID			weibo.com	LOGIN	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 11:18:05	去哪儿VID	pedjpbv3527	Rainman_ %E9%98%A8		LOGOUT	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 11:26:26	新浪微博VID			weibo.com	LOGOUT	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 11:32:08	淘宝[天猫			taobao.com	LOGOUT	允许	默认审计
/192.168.1.132(192.168.1.132)	2018-04-03 11:45:43	京东商城VID			jd.com	LOGIN	允许	默认审计

显示: 10 条

1 确定

7 安全认证

7.1 用户组织

7.1.1 用户管理

【应用场景】

设备上的用户类型包括内网用户、Web认证用户和VPN用户等。

对于定义的用户，其用途并不受限于单一功能，一个用户既可以登录VPN，也可以进行Web认证。例如：在财务部配置一个用户叫“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。此时不仅李三在公司上网时，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。

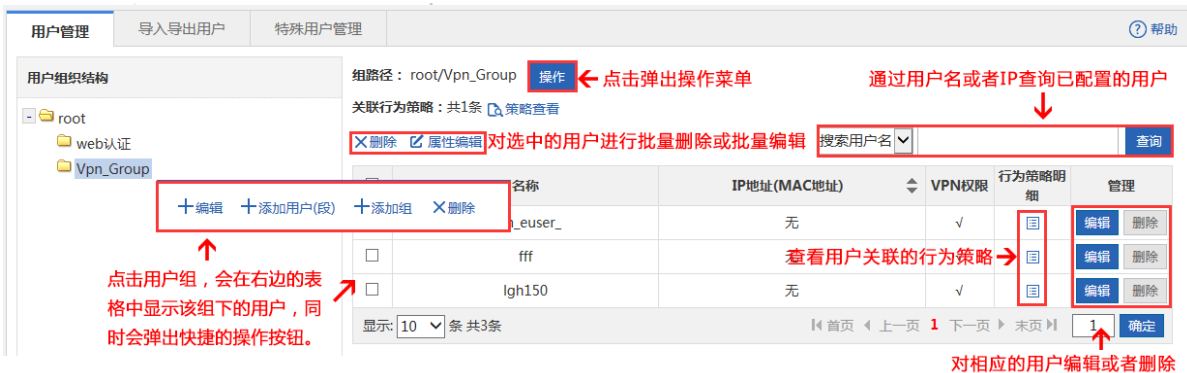


说明

上文中的VPN是指PPTP、L2TP或SSLVPN。

【操作步骤】

(1) 点击[安全认证]>>[用户组织]>>[用户管理]菜单项，进入[用户管理]页面。

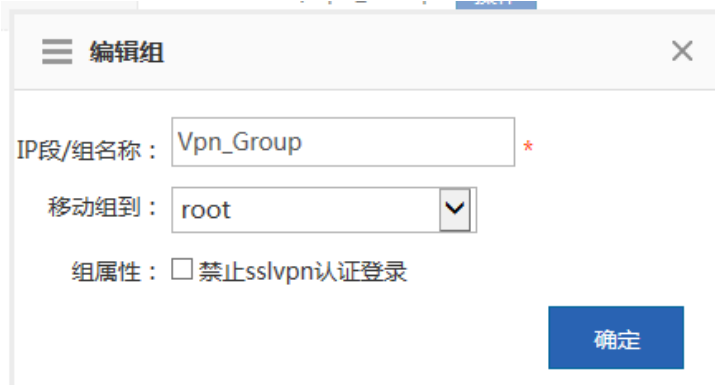


(2) 左侧的树状图是系统当前所有用户的组织结构，选中某个用户组，会在右侧显示该对象的相关信息，并可以对用户组信息进行编辑、修改。

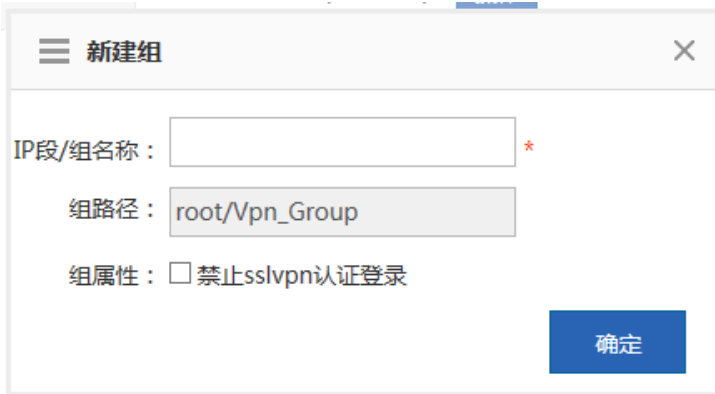
点击用户组后，显示信息如下图所示：



- 点击 **+ 编辑** 按钮，可以对选中的用户组进行编辑：可以修改用户组名称，以及把用户组移动到别的用户组下。



- 点击 **+ 添加组** 按钮，可以在选中的用户组下新建子用户组。用户组名称不能超过31个英文字符，一个中文字符相当于2个英文字符。



- 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。
- 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、本地服务器认证或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。
- **支持修改密码**：只有开启了“允许做Web认证用户”时才显示，当用户通过Web认证成功，是否允许该用户自行修改密码。



- **禁止WEB认证及本地服务器认证登录**：只有开启了“允许做Web认证用户”时才显示，勾选后用户Web认证成功也不能上外网，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。
- **禁止SSLVPN用户登录**：只有开启了“允许做VPN用户”时才显示，勾选后禁止使用当前用户登录SSLVPN。

- **SSLVPN使用Radius服务器进行身份认证**：只有开启了“允许做VPN用户”时才显示，勾选后SSLVPN登录时使用第三方的Radius服务器进行身份认证。

 说明

操作

点击 **操作** 按钮，同样可以增加组、删除组、添加用户。

(3) 对于用户组的用户列表，可执行的操作如下图所示。

关联行为策略：共1条 **策略查看** ← 查看该用户组关联的行为策略

删除 **属性编辑** 搜索用户名 **查询**

☐	名称	IP地址(MAC地址)	VPN权限	行为策略明细	管理
☐	123	无	√		编辑 删除
☐	3.3.3.3				编辑 删除

显示: 10 条 共2条 首页 上一页 1 下一页 末页 **确定**

勾选后可以批量删除或编辑 编辑或删除用户

以上表格列出了左侧选中的用户组包含的所有用户，可以在此处对用户信息进行编辑和删除操作。

- 点击 会弹出该用户（组）关联的行为策略情况，如下图所示：

查看 张三 的策略关联信息

+ 关联其它策略 **取消关联** ☐ 排除继承（该用户不使用父组的策略） **+ 行为策略管理**

☐	策略组名称	策略归属	状态	管理
☐	kk	继承所属组策略	未生效	不可删除

显示: 10 条 共1条 首页 上一页 1 下一页 末页 **确定**

- 点击 **+ 行为策略管理** 将跳转到[行为管理]>>[行为策略]>>[高级配置]页面。
- 点击 **+ 关联其它策略**，可设置当前用户关联到更多行为策略。
- 勾选策略表项，点击 **取消关联**，可取消行为策略与用户的关联。
- 勾选 ☐ **排除继承（该用户不使用父组的策略）**，则当前用户（组）不继承父组的策略。
- 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：

批量编辑属性

×

允许用途：☒允许做web认证及本地服务器认证用户☒允许做VPN用户

修改密码：☒支持修改密码

禁止登录：☐禁止WEB认证及本地服务器认证登陆

☐禁止sslvpn用户登录

sslvpn设置：☐SSLVPN使用Radius服务器进行身份认证

确定

- 点击 **编辑** 可以编辑相应的用户参数，各参数的介绍请参考“[新建用户](#)”步骤。

“移动到”表示将当前用户移动至下拉框中所选分组。

编辑用户

×

用户名称： *

IP&MAC：☒IP地址 ☐MAC地址 ☐IP和MAC ☐无IP

?

允许用途：☐允许做web认证用户 ☐允许做VPN用户

移动到： ▼

确定

- 在搜索区域，可输入的用户名或IP进行查询，查询的结果会显示到下方表格中。

×

删除

✎

属性编辑

查询参数

搜索用户名

张三

查询

搜索IP

☐	名称	IP地址(MAC地址)	VPN权限	行为策略明 细	管理
☐	张三 查询结果	无	×		编辑 删除

显示: 条 共1条

⏮

首页

◀

上一页

1

下一页

▶

末页

⏭

1

确定

7.1.2 导入导出用户

【应用场景】

通过本功能可以：

- 导出系统已有的用户配置。
- 通过模板，批量导入用户配置。

【操作步骤】

(1) 点击[安全认证]>>[用户组织]>>[导入导出用户]菜单项。

用户管理

导入导出用户

特殊用户管理

说明：导入用户信息有利于实名制管理用户，方便找到用户。

提示：导入用户的文件名必须为 **user-info.csv**，并按以下示例的规格填写对应表格。

文件名：

选择文件

未选择任何文件

☐ 修改冲突用户

导入用户

导出用户

导入文件信息规格示例

提示：其中“MAC地址”可以不填，但是在对应单元格中必须有一个空格。密码不能包含中文或者全角字符，否则可能出现错误。

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	192.168.1.9-192.168.1.12		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

(2) 导入或导出用户。

【导出用户】

点击

导出用户

按钮，将用户信息文件保存到本地。

用户管理

导入导出用户

特殊用户管理

上网屏蔽模式

说明：导入用户信息有利于实名制管理用户，方便找到用户。

提示：导入用户的文件名必须为 **user-info.csv**，并按以下示例的规格填写对应表格。

文件名：

选择文件

未选择任何文件

☐ 修改冲突用户

导入用户

导出用户

【导入用户】

通过文件批量导入用户，方便管理员快速完成用户的添加和管理。

- a 在本地新建一个表格user-info.csv，或者点击

导出用户

，导出文件名为user-info.csv的模板表格，在表格内部按照“导入文件信息规格示例”输入用户的信息。

导入文件信息规格示例

提示：其中“MAC地址”可以不填，但是在对应单元格中必须有一个空格。密码不能包含中文或者全角字符，否则可能出现错误。

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	手机号码
/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	189XXXXXXX
/财务部	李四	888	192.168.1.9-192.168.1.12	00-87-EF-22-2F-24	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	189XXXXXXX
/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	189XXXXXXX
/研发部/研发6部	刘六	888	2000::2	00-87-EF-12-4F-24	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	189XXXXXXX

- b 点击

选择文件

按钮，导入文件user-info.csv。

- c 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。

说明：导入用户信息有利于实名制管理用户，方便找到用户。

提示：导入用户的文件名必须为 **user-info.csv**，并按以下示例的规格填写对应表格。

文件名： user-info.csv

☐ 修改冲突用户

导入用户

导出用户

7.1.3 特殊用户管理

VIP/服务器用户：是指需要被保护的关键用户或内网服务器，该类用户上网速度将被优先保证。

禁止用户：是指黑名单用户，如果需要屏蔽某用户的一切上网行为，可以直接将该用户设置为黑名单用户。

免审计用户：是指免除内容审计、免除应用识别和免除流控限制的用户。例如：公司老板的上网行为不需要被审计，那么可以将老板设置为免审计用户。

对于以上几类特殊用户，可以通过[安全认证]>>[用户组织]>>[特殊用户管理]进行便捷管理。



- 设置VIP/服务器用户：



- a 点击 **VIP/服务器用户**，进入VIP用户或内网服务器设置页面。

+ 添加VIP用户或内网服务器 **✕ 删除选中用户**

☐	用户名称	IP地址	MAC地址	删除
显示: 10 条 共0条				
◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶▶ 1 确定				

- b 点击<添加VIP用户或内网服务器>，设置要添加的用户。

可以从用户组织中选择已创建的用户设置为VIP/服务器用户，点击<确定>；

或选择“添加VIP或内网服务器”，手动输入用户名和IP地址，创建用户，点击<添加>。

添加VIP用户或内网服务器

☒选择已有用户

☐添加 VIP 或内网服务器

Q

所有用户

☐

Vpn_Group

☒

test

☒

test1

带* 为VIP用户

确定

添加VIP用户或内网服务器

☐选择已有用户

☒添加 VIP 或内网服务器

用户名:

名称

*

IP地址:

IP或IP段

*

添加

c 如需删除配置，点击对应用户表项的<删除>，或勾选多条用户表项点击<删除选中用户>进行批量删除。

+ 添加VIP用户或内网服务器 X 删除选中用户

☐	用户名称	IP地址	MAC地址	删除
☒	1111	192.168.5.21	#	删除
显示: 10 条 共1条				
首页 < 上一页 1 下一页 > 末页 1 确定				

- **设置禁止用户：**点击  将弹出用户黑名单配置页面，管理员可以添加或删除黑名单用户。具体配置步骤请参考[6.4.2 3. 设置用户黑名单](#)。

- **免审计用户**：点击  将弹出配置页面，管理员可以添加或删除免审计用户。具体配置步骤请参考

免审计用户

[6.4.2 4. 设置免审计（免监控）用户。](#)

7.1.4 上网屏蔽模式

【应用场景】

开启上网屏蔽模式后，除了被设置为“排除屏蔽用户”的用户可以正常上网外，其余所有内网用户将不能通过设备上网。

【操作步骤】

- (1) 点击[安全认证]>>[用户组织]>>[上网模式屏蔽]菜单项。



上网屏蔽模式 ? 帮助

说明：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”；

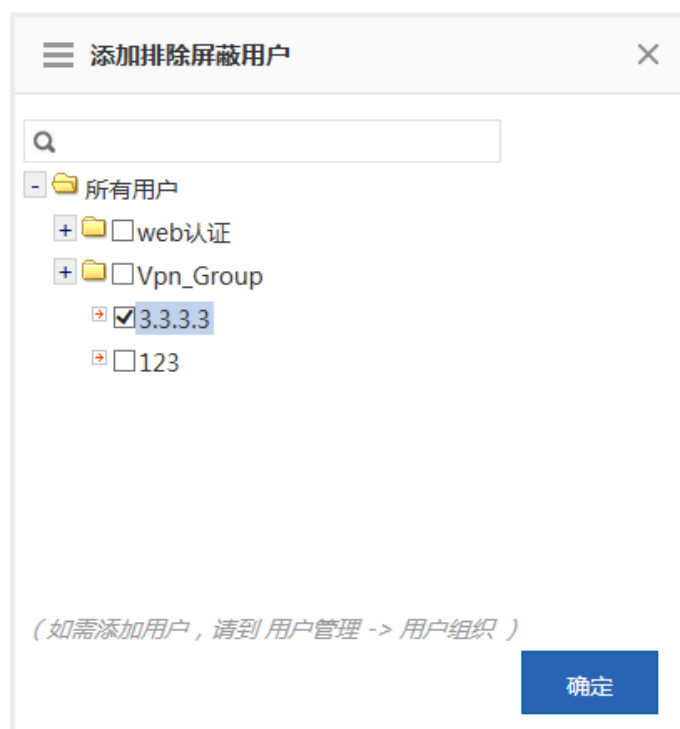
☐ 开启上网屏蔽模式

[+ 添加排除屏蔽用户](#) [X 删除选中用户](#)

☐	用户名称	IP地址	MAC地址	删除

首页 < 上一页 1 下一页 > 末页 1 确定

- (2) 点击 [+ 添加排除屏蔽用户](#)，添加至少一个排除屏蔽用户：勾选需要排除屏蔽的用户，点击<确定>。



添加排除屏蔽用户

Q

- 所有用户

- + ☐ web认证
- + ☐ Vpn_Group
 - ☒ 3.3.3.3
 - ☐ 123

(如需添加用户，请到 用户管理 -> 用户组织)

确定

- (3) 勾选 ☐ [开启上网屏蔽模式](#) 开启上网屏蔽模式。



【后续处理】

- 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。

7.2 Web 认证

7.2.1 Web 认证

Web认证是一种控制用户访问网络权限的身份认证方法。当未认证用户使用浏览器上网时，认证设备会强制浏览器访问特定站点（Portal服务器），用户无需认证即可访问Portal服务器上的服务。但若用户需要访问Portal服务器以外的其它网络资源时，则必须认证通过才行。

Web认证具有如下优点：

- 用户使用便利。用户不需要安装专用的客户端软件，只要拥有浏览器就可以完成身份认证。
- 可为用户提供个性化服务和拓展业务。利用用户浏览器与Portal服务器交互的特性，可以在Portal服务器页面定制广告、通知、业务链接等服务。

Web认证功能支持内置认证服务器和外置认证服务器两种实现方式。选择内置认证服务器则无需借助另外的服务器设备，本地需要配置认证用户；选择外置认证服务器则需要搭建好ePortal服务器与Radius服务器。

 注意

- 开启Web认证功能后如需使用Telnet管理，需要在[运维]>>[系统设置]>>[修改密码]页面重新配置Telnet密码。
- 本地服务器认证、商业营销认证、Web认证中任意两种认证功能不能同时开启。

1. 内置认证服务器场景

- (1) 点击[安全认证]>> [WEB认证]>>[WEB认证]菜单项。
- (2) 选择“认证选项”为“内置认证服务器”。

认证选项: ☒ 内置认证服务器 ☐ 广告推送服务 ☐ 外置认证服务器 ☐ 关闭web认证

认证方式: [【认证服务器】](#) [【SNMP配置】](#) [【查看在线用户】](#)

认证用户: [【管理配置认证用户】](#) (注意: 统一到用户组织时, 需把独立认证用户手动迁移到用户组织当中才能生效!)

SMP用户修改密码:

内置服务器端口: (1025 - 65535)

帐号共享开关: ☐

广告推送方式:

不保留下线页面: ☐ 认证成功后只推送广告不保留下线页面

广告地址: (需要配置设备的DNS)

无感知认证: ☐ 开启 ?

>> 高级设置

保存设置

(3) 设置Web认证参数。

- 认证方式: 如果使用设备内置的Portal服务器进行Web认证, 进行用户合法性认证时, 可以采用使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以及本地和Radius服务器并用的方式。
 - 优先服务器用户信息: 当配置了本地用户又添加了Radius服务器时, 优先到Radius服务器验证用户信息, 查找不到用户信息再到本地进行验证。
 - 优先本地用户信息: 先在本地设备查找用户验证, 找不到再到Radius服务器上验证。
 - 仅使用本地用户信息: 无Radius服务器时, 可选择仅使用本地用户信息, 提高认证的速度。
 - 仅使用服务器用户信息: 用户认证时, 在Radius服务器验证用户信息。

推荐使用“优先服务器用户信息”, 不过需要先搭建Radius服务器。

当需要通过服务器进行Web认证时, 需要设置Radius服务器参数, 包含“认证服务器”和“SNMP配置”。

说明

如何配置本地Web认证用户?

在[安全认证]>>[用户组织]>>[用户管理]页面添加用户, 设置用户名和密码, 并设置用途为“允许做web用户及本地服务器认证用户”。添加用户的详细步骤可参考[7.1.1 用户管理](#)。

新建用户

用户名称: **认证用户名** *

IP&MAC: ☐ IP地址 ☐ MAC地址 ☐ IP和MAC ☒ 无IP

允许用途: ☒ 允许做web认证及本地服务器认证用户
☐ 允许做VPN用户

密码: **认证密码**

绑定手机号: ?

☒ 支持修改密码 ?
☐ 禁止WEB认证及本地服务器认证登陆 ?

确定

- 点击【[认证服务器](#)】，填写认证服务器的IP和认证密码，以及认证端口，点击<保存设置>即可。

说明： 在设备转换网关或者网桥模式时，需要重新配置认证服务器才能生效；如果WEB认证模块、VPN或SSLVPN模块开启了Radius认证，那将共用此认证服务器列表。

提示： 如果认证端口设置为0，则该主机不进行身份认证。同样记帐端口如果设置为0，则该主机不进行记帐。

注意： 主备规则（先主后备），当主服务器不可达时，会使用备用服务器中第一个可达的服务器进行认证，探测用户名需到服务器上注册，密码默认为“ruijie”。开启无感知认证和逃生后，探测用户必配。有多台认证服务器时，将共用共享密码，超时时间和重传次数。对接锐捷smp作为portal，如下radius服务器超时时间建议配置2秒，重传次数3次。对接锐捷portal服务器超时时间为2s，重传次数1次。

共享密码：

* (有多台认证服务器时，将共用此密码)

超时时间：

(1-1000, 单位: 秒)

重传次数：

(0-100)

服务器IP：

* 认证端口：

(0-65535)

计费端口：

(0-65535)

探测用户名：

+添加

保存设置

清空配置

- 点击【[SNMP配置](#)】，配置认证设备与认证服务器之间的SNMP（简单网络管理协议）参数，通过SNMP实现认证服务器与认证设备之间的通讯。

SNMP配置

SNMP版本：☒ V2版本 ☐ V3版本

设备标识：

SNMP口令：

Trap口令：

SNMP目的主机：

Trap接收主机：

最多可配置9个Trap接收主机，IP之间请用“,”号隔开。

保存设置

清除设置

- SNMP版本：SNMP协议版本。目前设备支持V2和V3版本。V3版本提高了安全性设置，要求添加SNMP用户的加密密码和认证密码。
- 设备标识：设备的标识名称，可任意填写。
- SNMP口令：设置认证服务器（管理主机）对认证设备进行访问时使用的口令，设备上必须设置与认证服务器上相同的SNMP口令。对于SMP服务器，填写SMP服务器添加设备时配置的community名称。
- SNMP用户：SNMPv3版本的用户的用户名。
- 加密密码：SNMPv3版本的用户的加密口令。
- 认证密码：SNMPv3版本的用户的认证口令。

- Trap口令：设置认证设备向认证服务器（管理主机）发送Trap消息的认证口令。设备上必须设置与认证服务器上相同的Trap口令。对于SMP服务器，与SNMP口令相同。
- SNMP目的主机：Portal服务器的IP地址。
- Trap接收主机：接收设备告警信息的管理主机IP。一般同SNMP目的主机，为服务器IP地址。
- 点击【[查看在线用户](#)】按钮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，同时还支持查询在线用户：



- SMP用户修改密码：开启该功能后，需要输入修改密码的URL链接。SMP服务器用户可以通过该URL来修改认证密码。
- 内置服务器端口：设置内置Portal服务器的端口，取值范围为1025~65535，默认为8081。
- 帐号共享开关：一个帐号在同一时间只允许一个IP使用，通过开启帐号共享开关可以设置允许多个IP共享同一个帐号。可指定每帐号同时允许在线的IP个数。关闭帐号共享的情况下，后登录帐号的IP将抢占之前登录的IP，使先上线的IP下线。
- 广告推送方式：设定广告的显示方式，可以先认证后广告、先广告后认证或无广告。
- 广告地址：广告页面的URL地址。在设置广告地址前，需要先完成设备DNS的配置，配置步骤详见[8.4.2 DNS服务器](#)。
- 无感知认证：开启后用户上网只需输入一次用户名和密码，后续无需认证可直接上网。如果同时开启逃生功能，需要在认证服务器配置页面配置探测用户。

共享密码： * (有多台认证服务器时，将共用此密码)

超时时间： (1-1000, 单位: 秒) 重传次数： (0-100)

服务器IP： * 认证端口： (0-65535) 计费端口： (0-65535) 探测用户名： ?

说明

- 如需开启无感知认证功能，网关设备上需要开启DHCP服务，内网IP需要由网关动态分配。
- 对于具备无线功能的设备，请确认（1）[无线]>>[DHCP安全功能]，（2）[高级]>>[第三方日志]>>[ELOG]>>[无线日志功能]，这两个功能均已关闭，否则可能出现网络异常。

- 高级设置：点击 **>> 高级设置**，可以配置更多参数。配置详情请参考[7.2.3 用户认证的高级设置](#)。

高级设置

自定义登录LOGO：☐ 开启（开启为自定义LOGO，关闭为默认系统LOGO）

最大HTTP会话数： (1-255) 防止同一个未认证用户发起过多的HTTP连接请求，需要限制未认证用户的最大HTTP会话数。

重定向超时时间： (1-10秒) 设置维持重定向连接的超时时间，防止未认证用户不发GET/HEAD报文，而又长时间占用TCP连接。

重定向HTTP端口： 多个用“,”隔开（最多配10个）

在线信息更新时间： (30-3600秒) 设置在线用户信息的更新时间间隔。

下线检测模式：☒ 开启用户下线检测 在 (1 - 65535) 分钟内流量速率小于 (0 - 10)KB/s 的用户将被强制下线！

IP-MAC绑定模式：☐ 开启用户+IP+MAC三元素绑定（须在二层网络环境下，否则可能出现网络不通的情况。）

无需认证用户IP：☐ 开启无需认证用户推送广告 可配置IP段，例如：IP 192.168.1.0 掩码 255.255.255.0表示192.168.1.*的IP段；IP 0.0.0.0 掩码 0.0.0.0表示所有IP段；最大允许配置50条规则。

IP地址：

子网掩码：

×

+ 添加

保存设置

2. 外置认证服务器场景

【前置条件】

已完成外置认证服务器的搭建，包括ePortal服务器的部署以及在Radius服务器上配置合法用户。

【操作步骤】

(1) 点击[安全认证]>>[WEB认证]>>[WEB认证]菜单项。

(2) 选择“认证选项”为“外置认证服务器”。

说明：用户认证主要是指Web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。

重定向HTTP端口：拦截未认证用户访问指定端口的网络资源，并重定向到认证页面；最大允许配置10个。

注意：开启“内置认证”后如需使用Telnet管理，需要在“系统设置”修改密码”页面配置一下Telnet密码；

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。

认证选项：☐ 内置认证服务器 ☐ 广告推送服务 ☒ 外置认证服务器 ☐ 关闭web认证

主服务器IP：

重定向主页：

指定接入用户：

格式：192.168.1.0-255.255.255.255

[\[添加备用服务器\]](#) [?](#)

通讯密码：

 *

用户逃生功能：☐ 开启 [?](#)

服务器检测：☐ 开启 [?](#)

SNMP服务器：[\[SNMP配置\]](#) SNMP配置页面里的“SNMP目的主机”必须配置

高级设置

保存设置

(3) 设置Web认证参数。

- 主服务器IP：输入用户已经搭建好的外部ePortal服务器的IP地址。一般情况下，认证页面由认证ePortal服务器提供。

- 重定向主页：输入认证页面URL地址，当未认证的用户访问网络资源时会自动跳转到该页面，要求用户进行认证。
- 指定接入用户：配置需要在当前Portal服务器进行认证的用户网段。可选配置，如果当前环境中Portal服务器不唯一，要求不同用户在不同服务器上认证，则需要配置。配置后将根据用户所处网段选择不同的Portal服务器。
- 备用服务器：点击【[添加备用服务器](#)】添加备用服务器。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。最多可添加4个备用的Portal服务器。

说明：主备规则（先主后备），当主服务器不可达时，会使用备用服务器中第一个可达的服务器进行认证（需要开启服务器检测功能，指定接入用户除外），编辑服务器配置时会中断web认证业务。

备用服务器id: 1

备用服务器ip: *

重定向主页: *

指定接入用户: 格式: 192.168.1.0/255.255.255.255 ?

添加服务器

备用服务器id	备用服务器ip	重定向主页	指定接入用户	操作
显示: 10 条 共0条				1 确定

- 通讯密码：设置设备与认证服务器之间的通讯密码。该密码必须和认证服务器端的通讯密码一致否则无法生效。
- 用户逃生功能：开启后，当所有的Portal服务器都不可用时，新接入网络的用户无需认证即可访问网络资源。如果网络中有关键业务不允许中断，则可以开启此功能。当Portal服务器出现异常时，可以保证业务不受影响。
- 服务器检测：用于定时检测Portal服务器是否可用，并且在服务器不可用时自动切换到备用服务器。开启用户逃生功能或存在多个Portal服务器时，需要开启此功能。
- SNMP服务器：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目的主机等。点击【[SNMP配置](#)】进入配置页面。

SNMP配置

SNMP版本: ☒ V2版本 ☐ V3版本

设备标识: *

SNMP口令: *

Trap口令:

SNMP目的主机: ?

Trap接收主机: 最多可配置9个Trap接收主机, IP之间请用“,”号隔开。

- SNMP版本：SNMP协议版本。目前设备支持V2和V3版本。V3版本提高了安全性设置，要求添加SNMP用户的加密密码和认证密码。
 - 设备标识：设备的标识名称，可任意填写。
 - SNMP口令：设置认证服务器（管理主机）对认证设备进行访问时使用的口令，设备上必须设置与认证服务器上相同的SNMP口令。对于SMP服务器，填写SMP服务器添加设备时配置的community名称。
 - SNMP用户：SNMPv3版本的用户的用户名。
 - 加密密码：SNMPv3版本的用户的加密口令。
 - 认证密码：SNMPv3版本的用户的认证口令。
 - Trap口令：设置认证设备向认证服务器（管理主机）发送Trap消息的认证口令。设备上必须设置与认证服务器上相同的Trap口令。对于SMP服务器，与SNMP口令相同。
 - SNMP目的主机：Portal服务器的IP地址。
 - Trap接收主机：接收设备告警信息的管理主机IP。一般同SNMP目的主机，为服务器IP地址。
- 无感知认证：开启后用户上网只需输入一次用户名和密码，后续无需认证可直接上网。



说明

- 如需开启无感知认证功能，网关设备上需要开启DHCP服务，内网IP需要由网关动态分配。
 - 对于具备无线功能的设备，请确认（1）[无线]>>[DHCP安全功能]，（2）[高级]>>[第三方日志]>>[ELOG]>>[无线日志功能]，这两个功能均已关闭，否则可能出现网络异常。
- 高级配置：点击 [高级配置](#)，可以配置更多参数。配置详情请参考[7.2.3 用户认证的高级设置](#)。

高级设置

最大HTTP会话数： (1-255) 防止同一个未认证用户发起过多的HTTP连接请求，需要限制未认证用户的最大HTTP会话数。

重定向超时时间： (1-10秒) 设置维持重定向连接的超时时间，防止未认证用户不发GET/HEAD报文，而又长时间占用TCP连接。

重定向HTTP端口： 多个用“,”隔开（最多配10个）

在线信息更新时间： (30-3600秒) 设置在线用户信息的更新时间间隔。

下线检测模式：☒ 开启用户下线检测 在 (1 - 65535) 分钟内流量速率小于 (0 - 10)KB/s 的用户将被强制下线！

IP-MAC绑定模式：☐ 开启用户+IP+MAC三元素绑定（须在二层网络环境下，否则可能出现网络不通的情况。）

保存设置

(4) 点击<保存设置>。

3. 设置纯广告推送服务（无认证）

【前置条件】

已配置设备的DNS服务器地址，配置步骤详见[8.4.2 DNS服务器](#)。

【操作步骤】

(1) 点击[安全认证]>>[WEB认证]>>[WEB认证]菜单项。

(2) 选择“认证选项”为“广告推送服务”。

认证选项：☐ 内置认证服务器 ☒ 广告推送服务 ☐ 外置认证服务器 ☐ 关闭web认证

广告地址： (需要配置设备的DNS)

在线时长：☐ 开启

高级设置

保存设置

(3) 设置广告推送服务的相关参数。

- 广告地址：输入广告页面的URL地址。
- 在线时长：用户打开广告页面后，即可正常上网，在线时长即为允许用户上网的时长。
- 高级设置：点击高级设置，可以配置更多参数。配置详情请参考[7.2.3 用户认证的高级设置](#)。

高级设置

确保广告推送: ☐ 开启 (广告不被浏览器拦截)

重定向HTTP端口: 多个用 “,” 隔开 (最多配10个)

下线检测模式: ☒ 开启用户下线检测

在 (1 - 65535) 分钟内流量速率小于 (0 - 10)KB/s 的用户将被强制下线!

保存设置

(4) 点击<保存设置>。

开启广告推送服务后, 用户首次上网会弹出相应的广告页面。若开启后未弹出广告页面, 请设置浏览器 (internet选项--隐私--启用弹出窗口阻止程序, 选择不打勾) 或者在高级设置里开启 “确保广告推送” 选项。

确保广告推送: ☒ 开启 (广告不被浏览器拦截)

4. 关闭 Web 认证

保存设置

将认证选项置为 “关闭web认证” 并点击 **保存设置**, 即可关闭Web认证。

说明: 用户认证主要是指Web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。

重定向HTTP端口: 拦截未认证用户访问指定端口的网络资源, 并重定向到认证页面; 最大允许配置10个。

注意: 开启 “内置认证” 后如需使用Telnet管理, 需要在 “系统设置” 修改密码” 页面配置一下Telnet密码;

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。

认证选项: ☐ 内置认证服务器 ☐ 广告推送服务 ☐ 外置认证服务器 ☒ 关闭web认证

保存设置

7.2.2 Web 认证免认证

- 免认证网络资源: 用于设置允许未认证用户访问的网络资源。将网络资源服务器的IP地址或IP范围配置为免认证网络资源, 则所有用户 (包括未认证用户) 都可以访问该服务器资源。缺省情况下, 不存在免认证网络资源, 用户在访问任何网络资源前均需先通过Web认证。
- 免认证用户IP (IP范围): 该IP (范围) 的用户可以直接上网, 且不会推送广告。缺省情况下, 不存在免认证用户IP, 所有用户都必须先通过Web认证, 才能上网。
- 免认证用户MAC: 该MAC主机的用户可以直接上网, 且不会推送广告。缺省情况下, 不存在免认证用户MAC, 所有用户都必须先通过Web认证, 才能上网。

1. 设置免认证网络资源

- (1) 点击[安全认证]>>[Web认证]>>[Web认证免认证]菜单项。
- (2) 点击<添加免认证资源>。

WEB认证

WEB认证免认证

免认证网络资源：配置网络资源服务器的IP地址或IP范围，所有用户（包括未认证用户）都可以访问已配置，最大允许配置IP和IP范围各500条规则。

免认证用户IP(IP范围)：已配置用户可以直接上网，且不会推送广告，最大允许配置IP和IP范围各500条规则。

注意：本地服务器认证、商业营销认证、WEB认证任何两个不能同时开启。

免认证网络资源

+ 添加免认证资源

× 删除选中

查询资源ip:

基于IP或IP范围

查找

☐	IP地址	掩码地址	描述	操作
显示: 10 条 共0条				
1 首页 上一页 1 下一页 末页 1 确定				

(3) 填写免认证资源的信息。

用户可以按照如下格式添加免认证网络资源：

- 添加单个网络资源服务器：选择免认证类型为“IP地址”，填写IP地址和掩码地址。例如IP地址为192.168.1.1，掩码地址为255.255.255.255。
- 添加某个网段内的所有服务器：选择免认证类型为“IP地址”，填写网段IP和掩码。例如IP地址为192.168.1.0，掩码地址为255.255.255.0。
- 添加指定IP地址范围内的所有服务器：选择免认证类型为“IP范围”，按照“起始IP地址-结束IP地址”的格式填写IP范围，例如192.168.1.1-192.168.1.100。

添加免认证资源

×

免认证类型：

☒ IP地址
 ☐ IP范围

IP 地址：

格式：192.168.1.1

*

掩码地址：

*

描述：

保存

取消

(4) 点击<保存>。

【后续处理】

免认证网络资源

+ 添加免认证资源 X 删除选中

查询资源ip: 基于IP或IP范围 查找

☐	IP地址	掩码地址	描述	操作
☐	192.168.1.0	255.255.255.0		编辑 删除

显示: 10 条 共1条
 首页 上一页 1 下一页 末页
1 确定

- 点击<编辑>，可以修改网络资源配置。
- 点击<删除>，可以删除免认证网络资源。
- 在表格中勾选多条免认证资源表项，点击<删除选中>，可以批量删除多个免认证网络资源。
- 右上角搜索框支持根据资源IP或描述信息查找对应资源表项：在下拉框中选择查询的条件类型，在输入框里输入关键字，点击<查找>。

2. 设置免认证用户 IP

(1) 点击[安全认证]>>[Web认证]>>[Web认证免认证]菜单项。

(2) 点击<添加免认证用户>。

免认证用户IP

+ 添加免认证用户 X 删除选中

查询用户ip: 基于IP或IP范围 查找

☐	IP地址	掩码地址	描述	操作
--------------------------	------	------	----	----

显示: 10 条 共0条
 首页 上一页 1 下一页 末页
1 确定

(3) 填写免认证用户的信息。

用户可以按照如下格式添加免认证IP：

- 添加单个IP用户：选择免认证类型为“IP地址”，填写IP地址和掩码地址。例如IP地址为192.168.1.1，掩码地址为255.255.255.255。
- 添加某个网段内的所有用户：选择免认证类型为“IP地址”，填写网段IP和掩码。例如IP地址为192.168.1.0，掩码地址为255.255.255.0。
- 添加指定IP地址范围内的所有用户：选择免认证类型为“IP范围”，按照“起始IP地址-结束IP地址”的格式填写IP范围，例如192.168.1.1-192.168.1.100。

添加免认证用户IP

×

免认证类型：

☒ IP地址

☐ IP范围

IP 地址：

格式：192.168.1.1

*

掩码地址：

*

描述：

保存

取消

(4) 点击<保存>。

【后续处理】

免认证用户IP

[+ 添加免认证用户](#) [✕ 删除选中](#)

查询用户ip: 基于IP或IP范围

[查找](#)

☐	IP地址	掩码地址	描述	操作
☐	192.168.110.1-192.168.110.254	/		编辑 删除

显示: 10 条 共1条
首页 上一页 1 下一页 末页
1 [确定](#)

- 点击<编辑>，可以修改免认证IP配置。
- 点击<删除>，可以删除免认证IP。
- 在表格中勾选多条免认证IP表项，点击<删除选中>，可以批量删除多个IP。
- 右上角搜索框支持根据用户IP或描述信息查找对应表项：在下拉框中选择查询的条件类型，在输入框里输入关键字，点击<查找>。

3. 设置免认证用户 MAC

(1) 点击[安全认证]>>[Web认证] >>[Web认证免认证]菜单项。

(2) 点击<添加免认证用户MAC>。

免认证用户MAC

[+ 添加免认证用户MAC](#) [✕ 删除选中](#)

查询用户mac:

[查找](#)

☐	mac地址	操作
显示: 10 条 共0条		
首页 上一页 1 下一页 末页 1 确定		

(3) 在输入框中输入无需认证的主机MAC地址，点击<保存>。

添加免认证用户MAC

MAC地址:

格式: 0011.0022.0033 *

保存

取消

【后续处理】

免认证用户MAC

+ 添加免认证用户MAC × 删除选中

查询用户mac:

查找

☐	mac地址	操作
☐	0001.1111.1111	编辑 删除

显示: 10 条 共1条

首页

上一页

1

下一页

末页

1

确定

- 点击<编辑>，可以修改免认证MAC地址。
- 点击<删除>，可以删除免认证MAC配置。
- 在表格中勾选多条免认证用户MAC表项，点击<删除选中>，可以批量删除多条配置。
- 右上角搜索框支持根据用户MAC查找对应表项：在输入框里输入MAC地址，点击<查找>。

7.2.3 用户认证的高级设置

高级设置

自定义登录LOGO：☒ 开启 (开启为自定义LOGO，关闭为默认系统LOGO)

选择文件

未选择任何文件

上传

(注：LOGO图片的格式和命名必须为“free_login_logo.jpg”，建议尺寸为151*88像素)

最大HTTP会话数：

255

(1-255) 防止同一个未认证用户发起过多的HTTP连接请求，需要限制未认证用户的最大HTTP会话数。

重定向超时时间：

3

(1-10秒) 设置维持重定向连接的超时时间，防止未认证用户不发GET/HEAD报文，而又长时间占用TCP连接。

重定向HTTP端口：

80

多个用“,” 隔开 (最多配10个)

在线信息更新时间：

180

(30-3600秒) 设置在线用户信息的更新时间间隔。

下线检测模式：☒ 开启用户下线检测 在

15

(1 - 65535) 分钟内流量速率小于

0

(0 - 10)KB/s 的用户将被强制下线!

IP-MAC绑定模式：☐ 开启 (修订配置设备会强制清除在线用户)

无需认证用户IP：☐ 开启无需认证用户推送广告 可配置IP段，例如：IP 192.168.1.0 掩码 255.255.255.0表示192.168.1.*的IP段；IP 0.0.0.0 掩码 0.0.0.0表示所有IP段；最大允许配置50条规则。

IP地址：

子网掩码：

×

+添加

保存设置

- **自定义登录LOGO**：对于内置的认证服务器，支持修改Web认证页面的显示图标。开启本功能并上传LOGO图片文件后，登录页面将显示上传的自定义LOGO；若关闭本功能则Web认证页面显示默认系统LOGO。

The image shows a web login interface. At the top, there is a custom logo of a green apple with a leaf. Below the logo, there is a message "欢迎使用，请输入您的账号和密码！" (Welcome, please enter your account and password!). Underneath, there are two input fields: "用户名：" (Username) and "密码：" (Password). Below the password field, there is a checkbox labeled "记住用户名和密码" (Remember username and password). At the bottom, there are two buttons: "登录" (Login) and "重置" (Reset).

- **最大HTTP会话数**：支持设置每个未认证用户的最大HTTP会话数。开启Web认证后，未认证的用户在访问网络资源时，用户终端会发出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，造成设备的资源的浪费，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，所以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。

146

- **重定向超时时间**：支持设置维持重定向连接的超时时间。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，所以用户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。设置重定向超时限制时间可以防止用户不发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。
- **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。
- **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。例如：在线更新用户信息后，获取到用户的在线时间大于或等于在线时限，则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。
- **下线检测模式**：支持开启用户下线检测，设置基于流量来检测用户是否下线。如果在指定时间内，用户流量速率持续小于一定值，则认为用户下线。缺省情况下，如果在15分钟内，用户流量都没有增加，则认为用户下线。

 说明

- 下线检测功能仅用来辅助检测用户是否下线，会存在一些误检的风险。
 - 当前判断用户是否下线有以下两种方式：（1）用户点击认证页面上的“下线”按钮，则认为用户下线。（2）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。
-
- **IP-MAC绑定模式**：开启用户名与IP、MAC的绑定模式后，在Web认证时将验证用户的IP和MAC是否符合绑定关系，否则无法通过认证，从而防止终端篡改IP为已认证通过的IP来绕过认证。只能在二层网络下开启IP-MAC绑定，否则绑定后可能会出现网络不通的情况。
 - **无需认证用户IP**：该类用户IP无需认证可直接上网，与免认证用户IP的区别在于无需认证用户支持推送广告。

7.3 商业营销认证

7.3.1 商业营销认证

随着移动互联网的普及，“网络”成为商家的营销手段之一。顾客可以在观看广告、短信验证或者关注微信公众号后，连接商家提供的Wi-Fi或有线网络上网。对于商家而言，快捷实现用户认证上网功能并提升用户认证体验，以达到良好的营销效果，成为越来越迫切的需求。

设备支持对接云AC或者第三方服务器，能够实现多种认证功能，如短信认证、微信认证等。

 注意

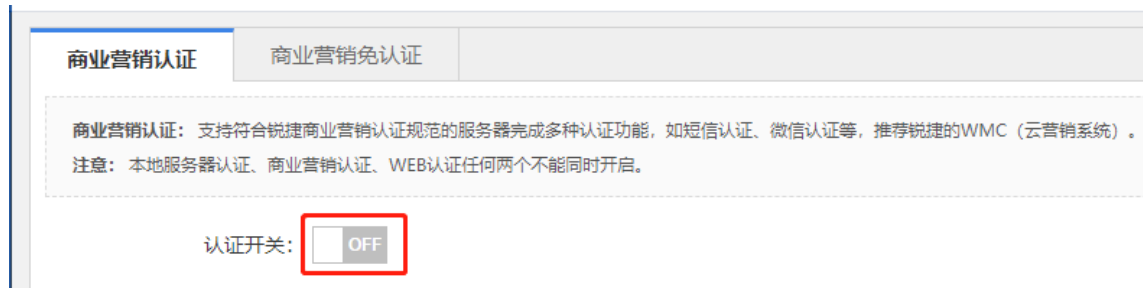
本地服务器认证、商业营销认证、Web认证中任意两种认证功能不能同时开启。

【前置条件】

- 商业营销认证需要与外部服务器（例如MCP）联动，需要先搭建和配置好外部服务器。
- 设备已经配置了DNS服务器地址。

【操作步骤】

- (1) 点击[安全认证]>>[商业营销认证]>>[商业营销认证]菜单项。
- (2) 如果认证开关处于OFF状态，点击开启认证开关。若已开启商业营销认证功能，则跳过本步骤。



- (3) 点击<认证快速配置>。通过此配置，可快速完成设备与MCP/WMC的联动认证。



服务器类型：根据认证服务器类型选择Wifidog或微信连Wifi(3.x)。

服务器地址：填入服务器的IP地址或域名。如使用WMC公有云方式，服务器地址填入112.124.31.88；若使用MCP私有云，则填入对应的MCP地址。

WiFi网络名称：用于认证的Wi-Fi名称。

≡ 微信认证配置引导

✕

1

微信服务器类型

服务器类型：

微信连Wifi(3.x) ▾

2

微信认证服务器

服务器地址：

格式：wmc.ruijieyun.com *

3

WiFi网络名称

WiFi网络名称：

*

完成

取消

(4) 点击<完成>。

(5) 点击 **>> 基本设置** 展开基本设置。可通过基本设置对设置参数进行调整。

认证方式：☒ 商业营销认证 ☐ 关闭商业营销认证

重定向主页：

*

通讯密码：

*

服务器类型：

Wifidog ▾

（如要变更服务器类型，请使用微信认证向导）

用户逃生功能：[【用户逃生功能配置】](#)

微信放行：

永久放行 ▾

认证信息：[【查看在线用户】](#)

保存设置

重定向主页：快速配置后，设备将根据选择的通信协议自动生成，通常不需要对该字段进行修订。

通讯密码：通常使用默认值ruijie，不建议修改。

服务器类型：支持Wifidog、微信连Wifi(3.x)和第三方类型。

用户逃生功能：Wifidog或微信连Wifi(3.x)协议都需要设置检测用户逃生的地址。点击<用户逃生功能配置>，可在弹出的页面中进行修改。可选择是否开启用户逃生功能，开启后，若服务器异常，用户可无需认证直接上网。

启用用户逃生功能: ☐ 勾选启用用户逃生功能

检测用户逃生的地址: *

保存设置

微信放行：设置是否在未认证的状态下放行微信应用的流量。可设置永久放行、临时放行或不放行。如果在WMC上开启了微信链接认证或者微信关注认证时必须设置放行；如不使用微信认证，可以根据需要修改为不放行。

WiFi网络名称：用于认证的Wi-Fi名称。

认证信息：点击<查看在线用户>，可以查看已通过认证、在线的用户信息，并可以将已认证用户剔下线。

第三方类型：支持定制第三方服务器对接，需要售后或者研发支持。

服务器类型： 第三方类型 （如要变更服务器类型，请使用微信认证向导，推荐使用Wifidog）

第三方类型： * 请与厂商联系，获取您的专属类型

第三方自定义信息： * 请与厂商联系，获取您的专属信息

(6) 配置完点击<保存设置>按钮完成基本设置。

(7) 点击 **>> 高级设置**，可以进行进一步设置。

高级设置

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 (添加/删除/修改此配置，对应进程会自动重启)

https重定向: ☐ 开启 访问https网页可以重定向。如使用微信认证，需要服务器支持微信临时放行
注意：由于缓存或者兼容性原因，某些浏览器或者APP的HTTPS无法正常重定向，这种情况下建议切换到HTTP的浏览器验证

mac-by-pass: ☐ 开启 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）

下线检测模式: ☒ 开启 开启用户下线检测，在 (1-65535) 分钟内流量速率小于 (0-10) Kb/s的用户将被强制下线！

网络类型: 二层网络

获取mac功能: ☐ 开启 功能开启时，需要下联设备dhcp relay到本设备上，该功能用于在三层网络场景下通过dhcp relay获取终端用户mac地址

IP范围ssid: [+添加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

网段	SSID
显示 10 条 共0条	

允许认证接入网段: 配置认证网段后，该网段内的用户需要进行认证，不在该网段内的用户则可以直接访问网络。单IP格式：如：192.168.1.2 IP范围：起始IP-结束IP，如：192.168.2.2-192.168.2.10。

[+添加](#)

保存设置

源IP地址：指定设备与认证服务器通讯的源IP地址。通常在IPSec VPN场景下使用，用于指定与VPN总部服务器通讯的私网地址。

https重定向：开启该功能后，终端访问https网页也可以重定向到认证页面。如使用微信认证，需要服务器支持微信临时放行

mac-by-pass：开启该功能后，终端在第一次连入网络时，由NBR设备向服务器通告终端接入，由服务器控制用户是否可直接上线。（只能在二层网络类型时使用）

下线检测模式：开启该功能后，终端在一定时间内的流量小于设定值时将被设备下线。

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（WMC/MCP上可以设置不同SSID调度不同的微信连WiFi规则）。未设置时，将默认使用基本设置中配置的Wi-Fi网络名称。

网络类型：包括二层网络和三层网络。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。如要变更网络类型配置，则在所有配置变更完成后需要关闭认证再重新开启（所有用户节点将被删除，即在线用户会强制下线）。

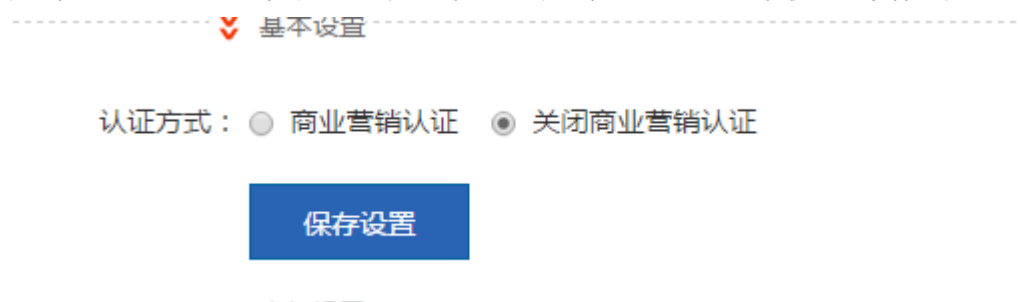
获取mac功能：该功能用于在三层网络场景下通过DHCP Relay获取终端用户mac地址。功能开启时，需要下联设备DHCP Relay到本设备上。

允许认证接入网段：默认所有接入用户都需要进行上网认证，配置网段后，只有该网段内的用户需要进行商业营销认证，其他网段直接放行。

(8) 配置完点击<保存设置>按钮完成高级设置。

【后续处理】

关闭商业营销认证：点击展开<基本设置>，选择“关闭商业营销认证”，最后点击<保存设置>。



7.3.2 商业营销免认证

配置为免认证的用户IP或者MAC，不需要认证可以直接上网。黑名单用户的流量会被全部拦截。

免认证用户IP：该用户可以直接上网，且不会推送广告。

免认证外网IP：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。

URL白名单：所有用户（包括未认证用户）都可以访问URL白名单中的网址。

用户MAC白名单：该MAC用户可以直接上网，且不会推送广告。

用户MAC黑名单：该MAC用户禁止上网。

临时黑白名单：免认证用户IP/免认证用户外网IP/用户MAC白名单/用户MAC黑名单可配置有效期，到期后相关配置将自动消失，已生效时间可在“已经生效时长”查看。

【操作步骤】

(1) 点击[安全认证]>>[商业营销认证]>>[商业营销免认证]菜单项。

商业营销认证商业营销免认证

免认证用户IP: 该用户可以直接上网,且不会推送广告,最大允许配置500条规则。单IP格式:如:192.168.1.2 IP范围:起始IP-结束IP,如:192.168.2.2-192.168.2.10。

免认证外网IP: 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50个地址条规则,单IP格式:如:192.168.1.2 IP范围:起始IP-结束IP,如:192.168.2.2-192.168.2.10。

URL白名单: URL白名单,所有用户(包括未认证用户)都可以访问该URL;支持通配,如配置ruijie.com,则允许访问www.ruijie.com,news.ruijie.com,最大允许配置100个网址。

用户MAC白名单: 该MAC用户可以直接上网,且不会推送广告,最大允许配置200条规则。MAC地址格式:如:0011.0022.0033。

用户MAC黑名单: 该MAC用户禁止上网,最大允许配置200条规则。MAC地址格式:如:0011.0022.0033。

临时黑白名单: 免认证用户IP/免认证用户外网IP/用户MAC白名单/用户MAC黑名单可配置有效期,到期后相关配置将自动消失,已生效时间可在已经生效时长查看。

注意: 本地服务器认证、商业营销认证、WEB认证任何两个不能同时开启。

免认证用户

+ 添加免认证用户 X 删除选中

☐	IP地址	有效期 (分钟)	已经生效时长 (分钟)	描述	操作
显示: 10 条 共0条					
					1 确定

免认证外网IP

+ 添加免认证外网IP X 删除选中

☐	IP地址	有效期 (分钟)	已经生效时长 (分钟)	描述	操作
显示: 10 条 共0条					
					1 确定

URL白名单

+ 添加URL白名单 X 删除选中

☐	免认证网址	操作
☐	mina.ruijieyun.com	编辑 删除
☐	wifi.weixin.qq.com	编辑 删除
☐	3gimg.qq.com/scan_wi-fi	编辑 删除
显示: 10 条 共3条		
		1 确定

(2) 设置免认证相关配置。

- 设置免认证IP用户。

点击 **+ 添加免认证用户**, 配置免认证用户的IP地址范围和免认证时长。可以输入单个IP (如192.168.110.2), 或者是IP地址范围 (如192.168.110.2-192.168.110.254)。

免认证用户

+ 添加免认证用户 X 删除选中

☐	IP地址	有效期 (分钟)	已经生效时长 (分钟)	描述	操作
显示: 10 条 共0条					
					1 确定

三 添加免认证用户

IP 地址:

格式: 192.168.1.1

*

?

有效期:

格式: 60, 范围60~655350

(分钟)

描述:

保存

取消

- 设置免认证外网IP。

点击 **+ 添加免认证外网IP**，输入用户可以无需认证直接访问的外网IP和免认证时长，点击 **保存**。

免认证外网IP

+ 添加免认证外网IP × 删除选中

☐	IP地址	有效期（分钟）	已经生效时长（分钟）	描述	操作
显示: 10 条 共0条					
首页 上一页 1 下一页 末页 1 确定					

三 添加免认证外网ip

IP 地址:

格式: 192.168.1.1

*

?

有效期:

格式: 60, 范围60~65535

(分钟)

描述:

保存

取消

- 设置URL白名单。

点击 **+ 添加URL白名单**，输入免认证的网址，点击 **保存**。当用户的目的URL在URL白名单中时，无论用户是否完成认证，流量都会被直接放行。

URL白名单

+ 添加URL白名单 **✕ 删除选中**

☐	免认证网址	操作
☐	mina.ruijieyun.com	编辑 删除

显示: **10** 条 共1条

◀ 首页 ◀ 上一页 **1** 下一页 ▶ 末页 ▶▶ **1** **确定**

≡ 添加URL白名单 **✕**

免认证网址: *

保存 **取消**

- 设置用户MAC白名单。

点击 **+ 添加用户MAC白名单**，输入免认证用户的MAC地址和免认证时长，点击 **保存**。

用户MAC白名单

+ 添加用户MAC白名单 **✕ 删除选中**

☐	MAC地址	有效期 (分钟)	已经生效时长 (分钟)	描述	操作
--------------------------	-------	----------	-------------	----	----

显示: **10** 条 共0条

◀ 首页 ◀ 上一页 **1** 下一页 ▶ 末页 ▶▶ **1** **确定**

三 添加用户MAC白名单

MAC地址:

格式: 0011.0022.0033 *

有效期:

格式: 60, 范围60~65535 (分钟)

描述:

保存

取消

- 设置用户MAC黑名单。

点击 [+ 添加用户MAC黑名单](#)，输入黑名单用户的MAC地址和限制时长，点击 [保存](#)。

用户MAC黑名单

[+ 添加用户MAC黑名单](#) [X 删除选中](#)

☐	MAC地址	有效期 (分钟)	已经生效时长 (分钟)	描述	操作
显示: 10 条 共0条					
首页 上一页 1 下一页 末页 1 确定					

三 添加用户MAC白名单

MAC地址:

格式: 0011.0022.0033 *

有效期:

格式: 60, 范围60~65535 (分钟)

描述:

保存

取消

- (3) 如需删除免认证配置，点击表项操作列的 [删除](#) 按钮。

免认证用户

[+ 添加免认证用户](#) [X 删除选中](#)

☐	IP地址	有效期 (分钟)	已经生效时长 (分钟)	描述	操作
☐	1.1.1.1	60		xxx	编辑 删除

显示: 10 条 共1条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶▶ 1 确定

7.4 本地服务器认证

本地服务器认证（简称本地认证）属于内置Web认证方式，由单台设备可以直接对接短信网关或AD域等服务器，支持以下几种认证方式：

- 本地账号密码认证：在上网认证页面，用户可以使用设备本地配置的账户认证上网。
- 短信认证：在上网认证页面，用户通过短信验证码的方式进行身份验证，认证通过后可上网。
- AD域认证：在上网认证页面，用户可以使用外部AD服务器上配置的账户认证上网。
- 微信认证：在上网认证页面，用户需要跳转到微信应用，关注指定微信公众号并根据公众号提示进行操作后可以正常上网。
- 二维码授权认证：上网认证页面显示二维码，需要由已通过认证的用户扫描二维码来为当前用户授权上网。
- 二维码自助扫码认证：二维码预先配置，并打印张贴在某处。终端直接扫描该二维码即可上网。对于PC等无法扫码的终端，将显示二维码授权认证界面。

注意

本地服务器认证、商业营销认证、Web认证中任意两个不能同时开启。

7.4.1 本地账号密码认证

本地账号密码认证属于系统自带的认证方法，与其他几种认证方法相比，不需要用户单独配置。在认证策略中可以直接关联账号密码认证。

1. 配置认证账号

- (1) 选择[安全认证]>>[用户组织]>>[用户管理]，进入用户配置页面。
- (2) 点击<操作>或点需要新增认证用户的用户组，在操作栏中点击“添加用户（段）”。



- (3) 选择“无IP”，输入用户名，勾选“允许做web认证及本地服务器认证用户”，并配置密码。

(4) 点击<确定>保存用户信息。在用户信息页面能够查看到添加的认证用户。

☐	名称	IP地址(MAC地址)	VPN权限	行为策略明细	管理
☐	web_user1	无	×		编辑 删除

2. 配置认证策略

(1) 点击[安全认证]>>[本地服务器认证]>>[认证策略]菜单项，进入本地服务器认证配置页面。

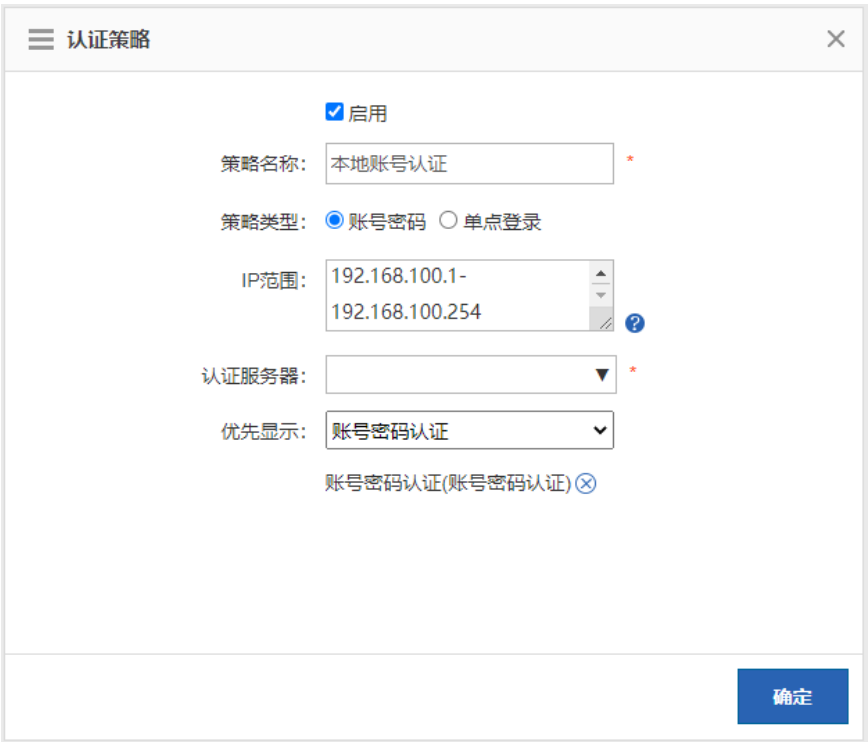
(2) 点击开启本地服务器认证功能开关。如果本地服务器认证功能已处于开启状态，请跳过本步骤。



(3) 在[认证策略]界面点击<添加认证策略>。



- (4) 配置本地认证策略。
- a 勾选“启用”开关。
 - b 填写策略名称。
 - c 指定匹配该策略的IP范围。可配置多个IP段，以换行符分隔。不配置IP范围则认为对所有内网IP网段都生效。
 - d 认证服务器选择“账号密码认证”。
 - e 优先显示：存在多个认证服务器时，选择在Portal认证页面上优先显示的认证方法。保持默认即可。
 - f 点击<确定>保存配置。



- (5) 配置的认证策略将显示在[认证策略]页面的列表中。策略支持按优先级匹配，排序在表格中越靠前的策略越优先匹配，通过“匹配顺序”中的和可调整策略的优先级。

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
☐	本地账号认证	192.168.100.1-192.168.100.254	账号密码认证	☒ 开启	生效		编辑 删除
☐	本地账号认证1	1.1.1.1-2.2.2.2	账号密码认证	☒ 开启	生效		编辑 删除

7.4.2 短信认证

1. 前置条件

在配置短信认证之前，需要先完成阿里云短信平台的注册和配置，包括获取Appkey和Secretkey、申请短信签名和短信模板以及购买短信资源包。

2. 配置认证服务器

(1) 点击[安全认证]>>[本地服务器认证]>>[认证服务器]菜单项。如果本地服务器认证功能处于关闭状态，需要先在[认证策略]页面开启本地服务器认证功能开关。



(2) 点击<添加认证服务器>，选择<短信认证>。



(3) 配置短信认证服务器对接参数。



- 填写名称，短信网关选择“阿里云通信”。
- 短信认证appkey，短信验证Secretkey：对应阿里云上申请的AccessKeyId和AccessKeySecret。
- 短信签名和模板：填入阿里云上申请的值，注意短信模板使用的是CODE ID。
- 预先输入手机号模式：启用本功能后，在发送短信校验码之前会先校验手机号是否已在设备端添加，不勾选则不进行检查。开启本功能则需要将本地认证用户绑定手机号，如下图所示。



(4) 点击<确定>。

3. 配置认证策略

- (1) 点击[安全认证]>>[本地服务器认证]>>[认证策略]菜单项。
- (2) 点击<添加认证策略>。

认证策略

认证服务器

高级配置

免认证配置

单点登录

用户权限

在线信息

说明：1.网桥模式支持本地服务器认证（需要配置BVI桥虚接口）。
2.WEB认证、商业营销认证、本地服务器认证任何两个不能同时开启。
3.账号密码信息通过“用户组织”菜单配置。
4.AD服务器导入的用户信息通过“用户组织”菜单查看。
5.单点登录失败用户会继续匹配其他策略。

+添加认证策略

✕删除选中

关闭本地服务器认证：

ON

配置示例

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
无记录信息							

显示：

10

条 共0条

⏪

首页

⏩

⏪

上一页

下一页

⏩

末页

⏪

1

确定

- (3) 配置短信认证策略。
 - a 勾选“启用”开关。
 - b 填写策略名称。
 - c 指定匹配该策略的IP范围。可配置多个IP段，以换行符分隔。不配置IP范围则认为对所有内网IP网段都生效。
 - d 认证服务器勾选在上一步骤中添加的短信认证服务器。
 - e 优先显示：存在多个认证服务器时，选择在Portal认证页面上优先显示的认证方法。保持默认即可。

≡ 认证策略

✕

☒ 启用

策略名称：

短信认证

策略类型：

☒ 账号密码

☐ 单点登录

IP范围：

192.168.111.1-192.168.111.254

认证服务器：

优先显示：

☐	认证服务器	服务器类型
☐	账号密码认证	账号密码认证
☒	短信认证测试	短信认证

确定

(4) 点击<确定>完成配置。配置的认证策略将显示在[认证策略]页面的列表中。策略支持按优先级匹配，排序在表格中越靠前的策略越优先匹配，通过“匹配顺序”中的和可调整策略的优先级。

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
☐	短信认证	192.168.111.1-192.168.111.254	短信认证测试	☒ 开启	生效		编辑 删除
☐	本地账号认证	192.168.100.1-192.168.100.254	账号密码认证	☒ 开启	生效		编辑 删除

显示:

10

 条 共2条

1

确定

7.4.3 微信认证

1. 前置条件

需要先在微信公众号平台完成认证URL的设置。认证URL示例：<http://11.11.11.11/wx?sign=ruijieAuthTest>，其中sign内容（即ruijieAuthTest）作为特征码，在设备端配置步骤中需要用到。

2. 配置认证服务器

(1) 点击[安全认证]>>[本地服务器认证]>>[认证服务器]菜单项。如果本地服务器认证功能处于关闭状态，需要先在认证策略页面开启本地服务器认证功能开关。



(2) 点击<添加认证服务器>，选择<微信认证>。



(3) 配置微信认证服务器对接参数。

- 名称：自定义服务器名称。
- sign：填写在公众号配置时所设置的认证URL中包含的特征码。设备端与公众号平台端所配置的sign应当一致。
- 提示语：在Portal页面上呈现的文字，用于指导用户如何操作。

(4) 点击<确定>。

3. 配置认证策略

(1) 点击[安全认证]>>[本地服务器认证]>>[认证策略]菜单项。

(2) 点击<添加认证策略>。

(3) 配置微信认证策略。

- 勾选“启用”开关。
- 填写策略名称。
- 指定匹配该策略的IP范围。可配置多个IP段，以换行符分隔。不配置IP范围则认为对所有内网IP网段都生效。
- 认证服务器勾选在上一步骤中添加的微信认证服务器。
- 优先显示：存在多个认证服务器时，选择在Portal认证页面上优先显示的认证方法。保持默认即可。

- (4) 点击<确定>完成配置。配置的认证策略将显示在[认证策略]页面的列表中。策略支持按优先级匹配，排序在表格中越靠前的策略越优先匹配，通过“匹配顺序”中的和可调整策略的优先级。

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
☐	本地账号认证	192.168.100.1-192.168.100.254	账号密码认证	☒ 开启	生效		编辑 删除
☐	微信认证	所有IP	微信认证测试	☒ 开启	生效		编辑 删除

显示: 10 条 共2条

首页 < 上一页 1 下一页 > 末页

7.4.4 二维码授权认证

二维码授权认证通常需要和其他认证方法配合使用，例如在企业场景下，开启二维码授权认证+账号密码认证，公司员工通过账号密码方式认证上网，访客则需要员工扫描二维码进行授权后才能够上网。

其他认证方法的配置步骤请参考相关章节，此处以二维码授权认证+本地账号密码认证为例。

1. 配置本地账号密码认证使用的账号

请参考[7.4.1 1. 配置认证账号](#)章节进行配置。

2. 配置认证服务器

- (1) 点击[安全认证]>>[本地服务器认证]>>[认证服务器]菜单项。如果本地服务器认证功能处于关闭状态，需要先在[认证策略]页面开启本地服务器认证功能开关。



- (2) 点击<添加认证服务器>，选择<二维码授权认证>。



(3) 配置二维码信息。



- 名称：自定义服务器名称。
- 二维码提示信息：填写二维码的提示信息，将在二维码显示页面呈现。建议将提示信息内容设置为用户实现上网的相关步骤。

(4) 点击<确定>。

3. 配置认证策略

- (1) 点击[安全认证]>>[本地服务器认证]>>[认证策略]菜单项。
- (2) 点击<添加认证策略>。

认证策略

认证服务器

高级配置

免认证配置

单点登录

用户权限

在线信息

说明：1.网桥模式支持本地服务器认证（需要配置BVI桥虚接口）。
2.WEB认证、商业营销认证、本地服务器认证任何两个不能同时开启。
3.账号密码信息通过“用户组织”菜单配置。
4.AD服务器导入的用户信息通过“用户组织”菜单查看。
5.单点登录失败用户会继续匹配其他策略。

+ 添加认证策略

✕ 删除选中

关闭本地服务器认证：

ON

配置示例

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
无记录信息							

显示：

10

条 共0条

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶

1

确定

- (3) 配置二维码授权认证策略。
 - a 勾选“启用”开关。
 - b 填写策略名称。
 - c 指定匹配该策略的IP范围。可配置多个IP段，以换行符分隔。不配置IP范围则认为对所有内网IP网段都生效。
 - d 认证服务器勾选在上一步骤中添加的二维码授权认证服务器以及需要配合使用的其他认证方法。
 - e 优先显示：存在多个认证服务器时，选择优先显示的认证方法为“二维码授权认证”。

≡ 认证策略

✕

☒ 启用

策略名称：

二维码授权认证

策略类型：

☒ 账号密码

☐ 单点登录

IP范围：

格式：1.1.1.1-2.2.2.2

认证服务器：

优先显示：

☐	认证服务器	服务器类型
☒	账号密码认证	账号密码认证
☐	微信认证测试	微信认证
☒	二维码授权测试	二维码授权认证

确定

(4) 点击<确定>完成配置。配置的认证策略将显示在[认证策略]页面的列表中。策略支持按优先级匹配，排序在表格中越靠前的策略越优先匹配，通过“匹配顺序”中的和可调整策略的优先级。

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
☐	本地账号认证	192.168.100.1-192.168.100.254	账号密码认证	☒ 开启	生效		编辑 删除
☐	二维码授权认证	所有IP	二维码授权测试 账号密码认证	☒ 开启	生效		编辑 删除

显示: 10 条 共2条

首页 上一页 1 下一页 末页

1 确定

7.4.5 二维码自助认证

1. 配置认证服务器

(1) 点击[安全认证]>>[本地服务器认证]>>[认证服务器]菜单项。如果本地服务器认证功能处于关闭状态，需要先在[认证策略]页面开启本地服务器认证功能开关。



(2) 点击<添加认证服务器>，选择<二维码自助认证>。



(3) 配置二维码信息。



- 名称：自定义服务器名称。
- 二维码IP：终端扫描二维码后实际访问的是该地址，因此需要配置成设备本机地址。因为微信扫描二维码时会对地址进行安全检测，所以该IP通常需要配置成私网地址，一般为设备LAN口地址。
- 二维码的动态码：修改二维码动态码后，二维码会随之发生变化，原有的二维码无法再使用。
- 二维码提示信息：未认证终端连接网络后如果不进行扫码而是直接打开浏览器，将看到该提示信息。
- 生成二维码：点击生成用于上网的二维码。可将生成的二维码打印张贴，供访客扫码上网。

(4) 点击<确定>。

2. 设置允许微信扫码

用户可使用微信或者其他扫码工具进行自助扫码，对于最常用的微信应用需要单独配置放行。

(1) 点击[安全认证]>>[本地服务器认证]>>[高级配置]菜单项。

(2) 设置“微信放行”为“永久放行”，点击<保存设置>。

认证策略

认证服务器

高级配置

免认证配置

单点登录

用户权限

在线信息

网络类型：☒ 二层网络 ☐ 三层网络

认证页面地址：

格式：192.168.1.1

非授权方式上线时长：

0

 分钟

授权方式上线时长：

0

 分钟

账号自动记录mac：☐ 开启

无感知认证功能：

关闭

注册用户空闲老化时间：

60

 天

通过DHCP SNOOPING获取mac功能：☐ 开启

无流量检测下线：☒ 开启

持续

60

 (1-65535)分钟内流量速率小于

0

 (0-10)KB/s的终端将被强制下线！

开启https重定向：☐ 开启

微信放行：

永久放行

 (配置自助扫码策略时，请选择微信永久放行)

授权管控：☐ 开启

终端管控功能：☐ 开启

文件名：

选择文件

 未选择任何文件

替换logo

恢复默认logo

保存设置

3. 配置认证策略

- (1) 点击[安全认证]>>[本地服务器认证]>>[认证策略]菜单项。
- (2) 点击<添加认证策略>。

认证策略

认证服务器

高级配置

免认证配置

单点登录

用户权限

在线信息

说明：1.网桥模式支持本地服务器认证（需要配置BVI桥虚接口）。
2.WEB认证、商业营销认证、本地服务器认证任何两个不能同时开启。
3.账号密码信息通过“用户组织”菜单配置。
4.AD服务器导入的用户信息通过“用户组织”菜单查看。
5.单点登录失败用户会继续匹配其他策略。

+ 添加认证策略

✕ 删除选中

关闭本地服务器认证：☒ ON ☐ OFF

配置示例

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
无记录信息							

显示:

10

 条 共0条

首页 上一页 下一页 末页

1

确定

- (3) 配置二维码自助认证策略。
- a 勾选“启用”开关。
- b 填写策略名称。

- c 指定匹配该策略的IP范围。可配置多个IP段，以换行符分隔。不配置IP范围则认为对所有内网IP网段都生效。
- d 认证服务器勾选在上一步骤中添加的二维码自助认证服务器。
- e 优先显示：存在多个认证服务器时，选择在Portal认证页面上优先显示的认证方法。保持默认即可。

- (4) 点击<确定>完成配置。配置的认证策略将显示在[认证策略]页面的列表中。策略支持按优先级匹配，排序在表格中越靠前的策略越优先匹配，通过“匹配顺序”中的↓和↑可调整策略的优先级。

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
☐	本地账号认证	192.168.100.1-192.168.100.254	账号密码认证	☒ 开启	生效	↓	编辑 删除
☐	二维码自助认证	所有IP	扫码上网	☒ 开启	生效	↑	编辑 删除

显示: 10 条 共2条

首页 < 上一页 1 下一页 > 末页

1 确定

7.4.6 AD 域认证

1. 前置条件

已完成LDAP服务器（即AD域控制器）的搭建和配置。

2. 配置认证服务器

- (1) 点击[安全认证]>>[本地服务器认证]>>[认证服务器]菜单项。如果本地服务器认证功能处于关闭状态，需要先在[认证策略]页面开启本地服务器认证功能开关。



(2) 点击<添加认证服务器>，选择<LDAP服务器>。



(3) 配置LDAP服务器参数。

LDAP服务器

服务器名称:

*

服务器地址:

格式: 1.1.1.1

*

?

源接口地址:

格式: 1.1.1.1

?

管理员名称:

@

*

?

管理员密码:

*

搜索入口:

格式:OU=test,DC=rj,DC=com

*

用户属性:

sAMAccountName

*

用户唯一属性:

distinguishedName

*

检测连通性

用户同步

确定

- 服务器名称：填写标识该服务器的名称。
- 服务器地址：填写服务器的IP地址。
- 源接口地址：如果认证设备同时作为VPN客户端，需要通过VPN隧道访问服务器时，需要配置该接口地址。
- 管理员名称：填写一个可以访问AD服务器的账号，推荐使用登录名。
- 管理员密码：账号的登录密码。
- 搜索入口：需要进行认证的AD域搜索路径。
- 用户属性：通常采用默认值即可。
- 用户唯一属性：通常采用默认值即可。

(4) 点击<检测连通性>测试配置是否正确。

(5) 点击<用户同步>，将搜索路径下的AD域用户组织结构同步到本地。同步完成后可在[安全认证]>>[用户组织]>>[用户管理]页面查看到AD域用户组织结构。

(6) 点击<确定>完成配置。

3. 配置认证策略

(1) 点击[安全认证]>>[本地服务器认证]>>[认证策略]菜单项。

(2) 点击<添加认证策略>。

认证策略

认证服务器

高级配置

免认证配置

单点登录

用户权限

在线信息

说明：1.网桥模式支持本地服务器认证（需要配置BVI桥虚接口）。
2.WEB认证、商业营销认证、本地服务器认证任何两个不能同时开启。
3.账号密码信息通过“用户组织”菜单配置。
4.AD服务器导入的用户信息通过“用户组织”菜单查看。
5.单点登录失败用户会继续匹配其他策略。

+ 添加认证策略

✕ 删除选中

关闭本地服务器认证：

ON

配置示例

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
无记录信息							

显示：

10

条 共0条

⏮ 首页

⏪ 上一页

下一页 ⏩

末页 ⏭

1

确定

- (3) 配置AD域认证策略。
- a 勾选“启用”开关。
 - b 填写策略名称。
 - c 若配置AD域SSO，则选择“单点登录”，否则选择“账号密码”即可。
 - d 指定匹配该策略的IP范围。可配置多个IP段，以换行符分隔。不配置IP范围则认为对所有内网IP网段都生效。
 - e 认证服务器勾选在上一步骤中添加的LDAP服务器。
 - f 优先显示：存在多个认证服务器时，选择在Portal认证页面上优先显示的认证方法。此处保持默认即可。

认证策略

✕

☒ 启用

策略名称：

AD域认证

*

策略类型：

☒ 账号密码

☐ 单点登录

IP范围：

192.168.111.1-
192.168.111.100

?

认证服务器：

*

优先显示：

LDAP服务器

▼

ladp112(LDAP服务器)

✕

确定

(4) 点击<确定>完成配置。

7.4.7 认证策略管理

[安全认证]>>[本地服务器认证]>>[认证策略]页面：

认证策略

认证服务器

高级配置

免认证配置

单点登录

用户权限

在线信息

说明：1. 网桥模式支持本地服务器认证（需要配置BVI桥虚接口）。
2. WEB认证、商业营销认证、本地服务器认证任何两个不能同时开启。
3. 账号密码信息通过“用户组织”菜单配置。
4. AD服务器导入的用户信息通过“用户组织”菜单查看。
5. 单点登录失败用户会继续匹配其他策略。

+ 添加认证策略

✕ 删除选中

关闭本地服务器认证：☒ ON

配置示例

☐	策略名称	认证范围	关联服务器	策略开关	状态	匹配顺序	操作
☐	本地账号认证	192.168.100.1-192.168.100.254	账号密码认证	☒ 开启	生效	↓	编辑 删除
☐	AD域认证	192.168.111.1-192.168.111.100	ladp112	☒ 开启	生效	⇅	编辑 删除
☐	二维码自助认证	所有IP	扫码上网	☒ 开启	生效	↑	编辑 删除

显示：10

共3条

◀ 首页

◀ 上一页

1

下一页 ▶

末页 ▶

1

确定

- 调整认证策略优先级：策略支持按优先级匹配，排序在表格中越靠前的策略越优先匹配，通过“匹配顺序”中的箭头↓和↑可调整策略的优先级。
- 点击<添加认证策略>，可以配置新的认证策略。
- 点击<编辑>，可以修改认证策略配置。
- 点击<删除>按钮，或者勾选多个认证策略，点击<删除选中>，可以删除认证策略。

7.4.8 认证服务器管理

[安全认证]>>[本地服务器认证]>>[认证服务器]页面：

认证策略

认证服务器

高级配置

免认证配置

单点登录

用户权限

在线信息

说明：1. 配置自助扫码时，如需使用微信进行扫码，请进入本地服务器认证-高级配置中选择微信放行。

+ 添加认证服务器

✕ 删除选中

☐	名称	认证类型	认证服务器	操作
☐	微信认证测试	微信认证	-	编辑 删除
☐	二维码授权测试	二维码授权认证	-	编辑 删除
☐	扫码上网	二维码自助认证	-	编辑 删除
☐	ladp112	LDAP服务器	1.1.1.1	编辑 删除

显示：10

共4条

◀ 首页

◀ 上一页

1

下一页 ▶

末页 ▶

1

确定

- 点击<添加认证服务器>，可以配置新的认证策略。各类型认证服务器的配置请参考前文对应章节。
- 点击<编辑>，可以修改认证策略配置。
- 点击<删除>按钮，或者勾选多个认证策略，点击<删除选中>，可以删除认证策略。

7.4.9 高级配置

[安全认证]>>[本地服务器认证]>>[高级配置]页面：

认证策略	认证服务器	高级配置	免认证配置	单点登录	用户权限	在线信息
网络类型: ☒ 二层网络 ☐ 三层网络 认证页面地址: 格式: 192.168.1.1 ? 非授权方式上线时长: 0 分钟 ? 授权方式上线时长: 0 分钟 ? 账号自动记录mac: ☐ 开启 ? 无感知认证功能: 关闭 ? 注册用户空闲老化时间: 60 天 ? 通过DHCP SNOOPING获取mac功能: ☐ 开启 ? 无流量检测下线: ☒ 开启 ? 持续 60 (1-65535)分钟内流量速率小于 0 (0-10)KB/s的终端将被强制下线! 开启https重定向: ☐ 开启 ? 微信放行: 永久放行 (配置自助扫码策略时, 请选择微信永久放行) 授权管控: ☐ 开启 ? 终端管控功能: ☐ 开启 ? 文件名: 选择文件 未选择任何文件 ? 替换logo 恢复默认logo 保存设置						

下面是各配置项的介绍：

- 网络类型：根据实际网络情况选择网络类型即可。
 - 二层网络时，在设备下联端通常不存在三层核心交换设备，整网的网关和DHCP Server都位于认证设备。
 - 三层网络时，在设备下联端通常存在三层核心交换设备，网关位于核心设备上。
- 认证页面地址：可选配置，可填写设备LAN口地址。使用微信扫描二维码时，如果认证页面非私网地址则会出现告警。可以在设备上增加一个环回口或配置Second IP作为认证页面地址。
- 非授权上网方式时长：指非授权用户本次通过认证后，允许在线的时长。0表示不限制。超过时长后用户将被踢下线并需要重新认证（开启无感知认证状态下也需要重新认证）。非授权上网方式包括账号密码认证、短信认证、AD域认证和微信认证。
- 授权上网方式时长：指授权用户本次通过认证后，允许在线的时长。0表示不限制。超过时长后用户将被踢下线。授权上网方式是指通过扫描二维码或者由他人协助扫描二维码获取上网权限的方式，包括二维码授权认证、二维码自助扫码认证和微信认证中的PC授权扫码。
- 账号自动记录mac：开启该功能后，通过账号密码认证、短信认证、AD域认证或微信认证的终端用户的MAC地址将被记录在设备上，并可通过[本地服务器认证]>>[用户权限]>>[注册用户]页面查看。

认证策略	认证服务器	高级配置	免认证配置	单点登录	用户权限	在线信息
------	-------	------	-------	------	-------------	------

说明：注册用户为用户上线后生成的表项。用户生成后可以点击“编辑”，在该账号下添加mac并指定终端类型。
注册用户和特权组中，对于AD域，都显示完整的DN。
特权组在授权管控开启时具有对其他用户进行授权上网的权限。

注册用户	特权组	✕ 删除选中	基于用户名 ▾		查询
☐	用户名		用户类型	mac地址（终端类型）	

无记录信息

- 每个账号自动记录mac限制个数：开启“账号自动记录mac”功能后可配置，用于限制每个账号允许被几个MAC地址（终端）使用。生效范围包括本地账号、手机号（未绑定到本地账号情况）、AD域账号。超过限制值后，新的MAC地址无法使用该账号进行认证。配置为0表示该账号不允许被任一MAC地址使用。

⚠ 注意

如果账号配置了特权权限，则不受MAC个数限制。特权权限通过[本地服务器认证]>>[用户权限]页面进行配置，详见[7.4.12 用户权限](#)。

- 无感知认证功能：开启后对于记录在[用户权限]>>[注册用户]列表中的用户可以体验无感知认证功能。无感知认证功能分为“macbypass无感知”和“WEB弹出方式无感知”。对于“macbypass无感知”，用户联网后无需任何操作即可上网；而对于“WEB弹出方式无感知”，联网后访问浏览器会弹出一个通告提示，然后即可上网。推荐使用macbypass方式。
- 注册用户空闲老化时间：被记录为注册用户的MAC地址在老化时间内未被使用，即该MAC终端未再次上线，则会被老化删除。若注册用户有被重新匹配（包括无感知方式认证上线），则刷新老化时间，开始新的统计周期。
- 通过DHCP SNOOPING获取mac功能：用于三层网络场景下，开启后设备能够通过DHCP Snooping方式获取到终端的mac信息。在配置该特性时，通常需要由核心设备（网关）开启DHCP Relay功能，并将DHCP Server部署到当前认证设备上（当前认证设备为DHCP Relay所指向的DHCP服务器）。
- 无流量检测下线：开启后，当认证用户在离开网络并持续一段时间未返回，即网络中该终端的流量持续小于一定值时，会将该终端强制下线。为了避免出现“终端A离开后，终端B拿到终端A的IP就能够绕过认证直接上网”的情况，无流量检测下线的持续时间条件通常要小于DHCP租期的一半。
- 开启https重定向：开启该功能后，终端访问https网页也可以进行重定向。https重定向对性能消耗较大，开启后可能导致CPU持续较高情况出现。

⚠ 注意

由于缓存或者兼容性问题，某些浏览器或APP的HTTPS无法正常重定向，这种情况下建议切换到HTTP的浏览器进行弹窗认证。

- 微信放行：用于配置未认证前是否需要放行微信，若开启了自助扫码认证方法，则需要设置微信“永久放行”，对于其他认证方法一般选择不放行。
- 授权管控：开启后，只有具有特权权限的用户才能进行授权上网。当无特权的认证终端进行授权时，会提示没有权限。

说明

特权权限通过[本地服务器认证]>>[用户权限]>>[特权组]页面配置。只有在用户管理中配置的账号或AD域中的账号才可以被授予特权，支持按组方式批量授予特权。

- 非特权用户可授权次数：在开启授权管控时可配置。设置后被特权用户授权上网的用户可以继续为其他用户授权一定次数，但由被授权用户继续授权（二次授权）的用户无法再进行授权操作。配置为0表示非特权用户无法为其他用户授权。常见的使用场景为“来宾用户由员工授权后，允许来宾用户继续进行授权上网”。例如来宾用户携带了手机和PC，手机由员工授权上网后，来宾PC可以自行授权上网。配置为0时，则来宾无法自行授权。
-

说明

开启该功能后，微信认证、自助扫码认证、未绑定账号的短信认证、二维码授权认证的上线用户授权次数都受此限制。

- 终端管控功能：该功能用于限定PC或移动终端只能在允许的时间段内（即例外时间）上网，其他时间则无法上网。但属于特权用户的终端类型不受该限制。
-

说明

终端类型可能存在误判，因此建议只在固定上网环境中使用。管理员可以在[安全认证]>>[本地服务器认证]>>[用户权限]>>[注册用户]页面中修改特定MAC的所属终端类型（前提是要开启自动记录MAC功能）。

- 自定义logo：允许用户自定义Portal页面的logo图标。
- <保存设置>用于保存高级配置。

7.4.10 免认证配置

配置为免认证的用户IP或者MAC，不需要认证可以直接上网。黑名单用户的流量会被全部拦截。

免认证用户IP：该用户可以直接上网，且不会推送广告。

免认证外网IP：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。

URL白名单：所有用户（包括未认证用户）都可以访问URL白名单中的网址。

用户MAC白名单：该MAC用户可以直接上网，且不会推送广告。

用户MAC黑名单：该MAC用户禁止上网。

临时黑白名单：免认证用户IP/免认证用户外网IP/用户MAC白名单/用户MAC黑名单可配置有效期，到期后相关配置将自动消失，已生效时间可在“已经生效时长”查看。

【操作步骤】

- (1) 点击[安全认证]>>[本地服务器认证]>>[免认证配置]菜单项。

认证策略

认证服务器

高级配置

免认证配置

单点登录

用户权限

在线信息

免认证用户IP: 该用户可以直接上网,且不会推送广告,最大允许配置500条规则。单IP格式:如:192.168.1.2 IP范围:起始IP-结束IP,如:192.168.2.2-192.168.2.10。

免认证外网IP: 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50个地址条规则,单IP格式:如:192.168.1.2 IP范围:起始IP-结束IP,如:192.168.2.2-192.168.2.10。

URL白名单: URL白名单,所有用户(包括未认证用户)都可以访问该URL;支持通配,如配置ruijie.com,则允许访问www.ruijie.com,news.ruijie.com。最大允许配置100个网址。

用户MAC白名单: 该MAC用户可以直接上网,且不会推送广告,最大允许配置200条规则。MAC地址格式:如:0011.0022.0033。

用户MAC黑名单: 该MAC用户禁止上网,最大允许配置200条规则。MAC地址格式:如:0011.0022.0033。

临时黑白名单: 免认证用户IP/免认证用户外网IP/用户MAC白名单/用户MAC黑名单可配置有效期,到期后相关配置将自动消失,已生效时间可在已经生效时长查看。

注意: 本地服务器认证、商业营销认证、WEB认证任何两个不能同时开启。

免认证用户

+添加免认证用户 X删除选中

☐	IP地址	有效期(分钟)	已经生效时长(分钟)	描述	操作
显示: 10 条 共0条					
1 确定					

免认证外网IP

+添加免认证外网IP X删除选中

☐	IP地址	有效期(分钟)	已经生效时长(分钟)	描述	操作
显示: 10 条 共0条					
1 确定					

(2) 设置免认证相关配置。

- 设置免认证IP用户。

点击 **+添加免认证用户**,配置免认证用户的IP地址范围和免认证时长。可以输入单个IP(如192.168.110.2),或者是IP地址范围(如192.168.110.2-192.168.110.254)。

免认证用户

+添加免认证用户 X删除选中

☐	IP地址	有效期(分钟)	已经生效时长(分钟)	描述	操作
显示: 10 条 共0条					
1 确定					

添加免认证用户

IP地址: 格式: 192.168.1.1 *

有效期: 格式: 60, 范围60~655350 (分钟)

描述:

保存 取消

- 设置免认证外网IP。

点击 [+ 添加免认证外网IP](#)，输入用户可以无需认证直接访问的外网IP和免认证时长，点击



免认证外网IP

[+ 添加免认证外网IP](#) [X 删除选中](#)

☐	IP地址	有效期（分钟）	已经生效时长（分钟）	描述	操作
显示: 10 条 共0条					
首页 上一页 1 下一页 末页 1 确定					

添加免认证外网ip

IP 地址:

格式: 192.168.1.1 *

有效期:

格式: 60, 范围60~65535 (分钟)

描述:

保存

取消

- 设置URL白名单。

点击 [+ 添加URL白名单](#)，输入免认证的网址，点击 [保存](#)。当用户的目的URL在URL白名单中时，无论用户是否完成认证，流量都会被直接放行。

URL白名单

[+ 添加URL白名单](#) [X 删除选中](#)

☐	免认证网址	操作
☐	mina.ruijieyun.com	编辑 删除
显示: 10 条 共1条		
首页 上一页 1 下一页 末页 1 确定		

添加URL白名单

×

免认证网址：

格式：如www.ruijie.com.cn *

保存

取消

- 设置用户MAC白名单。

点击 [+ 添加用户MAC白名单](#)，输入免认证用户的MAC地址和免认证时长，点击 [保存](#)。

用户MAC白名单

[+ 添加用户MAC白名单](#) [X 删除选中](#)

☐	MAC地址	有效期（分钟）	已经生效时长（分钟）	描述	操作
显示: 10	条 共0条	首页 上一页 1 下一页 末页			
					确定

添加用户MAC白名单

×

MAC地址：

格式：0011.0022.0033 *

有效期：

格式：60，范围60~65535（分钟）

描述：

保存

取消

- 设置用户MAC黑名单。

点击 [+ 添加用户MAC黑名单](#)，输入黑名单用户的MAC地址和限制时长，点击 [保存](#)。

用户MAC黑名单

+ 添加用户MAC黑名单

× 删除选中

☐	MAC地址	有效期 (分钟)	已经生效时长 (分钟)	描述	操作
显示: 10 条 共0条					
◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶					
					1 确定

添加用户MAC白名单

MAC地址: 格式: 0011.0022.0033 *

有效期: 格式: 60, 范围60~65535 (分钟)

描述:

保存

取消

(3) 如需删除免认证配置，点击表项操作列的

删除

 按钮。

免认证用户

+ 添加免认证用户

× 删除选中

☐	IP地址	有效期 (分钟)	已经生效时长 (分钟)	描述	操作
☐	1.1.1.1	60		xxx	编辑 删除
显示: 10 条 共1条					
◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶					
					1 确定

7.4.11 单点登录

【应用场景】

单点登录 (Single Sign On，简称为SSO) 是一种统一认证和授权机制，用于解决用户在多个站点之间跳转时需要频繁登录的问题。借助单点登录，用户只需要登录一次，即可访问同一服务器不同应用中的受保护资源；同理用户只需注销一次，就可以从多个应用系统退出登录。开启单点登录功能后，如果局域网系统已部署有认证服务器，局域网用户通过了该认证服务器的检查，成功接入网络之后，则认证设备自动认为该用户认证成功。认证后的用户后续访问外网时，不需要在认证设备上再做一次认证即可直接上网。

【操作步骤】

(1) 点击[安全认证]>>[本地服务器认证]>>[单点登录]菜单项。

启用域单点登录：☒ ON

☐ 通过域自动下发，执行指定的登录脚本，获取登录信息

[下载域单点登录程序](#)

共享秘钥： ☒ 显示密码

保存设置

(2) 设置“启用域单点登录”为启用状态。

说明

勾选“通过域自动下发，执行指定的登录脚本，获取登录信息”：管理员可以在AD域上配置一个用户登录脚本，用户登录域时会自动执行该脚本，发送登录数据包到本设备，完成上网身份识别。

(3) 设置共享秘钥。

(4) 点击<保存设置>。

7.4.12 用户权限

1. 设置注册用户

注册用户为用户上线后生成的表项，在当前页面可以设置注册用户的MAC地址和终端类型。

【操作步骤】

(1) 选择[安全认证]>>[本地服务器认证]>>[用户权限]，点击<注册用户>页签。

(2) 页面显示注册用户的相关信息。点击 ，可以在该账号下添加MAC地址并指定终端类型。

说明：注册用户为用户上线后生成的表项。用户生成后可以点击“编辑”，在该账号下添加mac并指定终端类型。
注册用户和组管理中，对于AD域，都显示完整的dn。

注册用户	组权限	
用户名	用户类型	mac地址（终端类型）
test	AD域用户	0011.0022.0033 操作

显示: 条 共1条

首页 上一页 1 下一页 末页

确定

2. 设置特权用户

设置用户权限，指定拥有特殊权限的用户。特权用户能够在开启授权管控的情况下为未认证用户授权，使其能够上网，并且自身不受终端管控功能限制。

说明

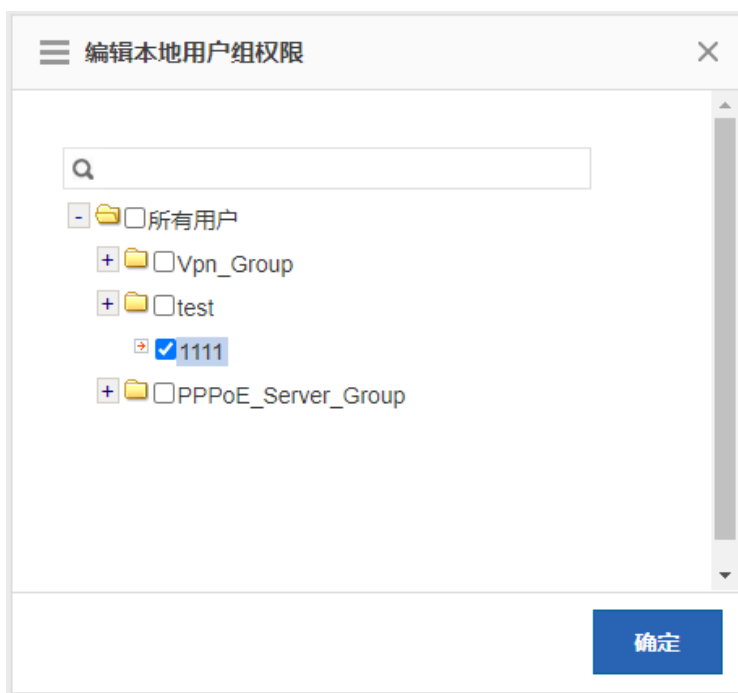
授权管控与终端管控功能均在[安全认证]>>[本地服务器认证]>>[高级配置]中配置。

【操作步骤】

(1) 选择[安全认证]>>[本地服务器认证]>>[用户权限]，点击<特权组>页签。



(2) 点击<编辑本地用户特权组>，可从本地用户中选择用户添加为特权用户；点击<编辑AD域用户特权组>，可从AD域用户中选择用户添加为特权用户。



7.4.13 在线信息

可以查看通过认证的在线用户的详细信息。

【操作步骤】

(1) 点击[安全认证]>>[本地服务器认证]>>[在线信息]菜单项。

(2) 系统显示在线用户相关信息。左上角搜索框可根据用户名或用户IP查找对应在线用户信息。



7.5 PPPoE Server

7.5.1 功能简介

PPPoE (Point-to-Point Protocol over Ethernet，以太网上的点对点协议) 是将点对点协议 (PPP) 封装在以太网框架中的一种网络隧道协议。作为PPPoE服务器的设备能够在局域网中向用户提供接入服务，并对用户提供带宽管理功能。

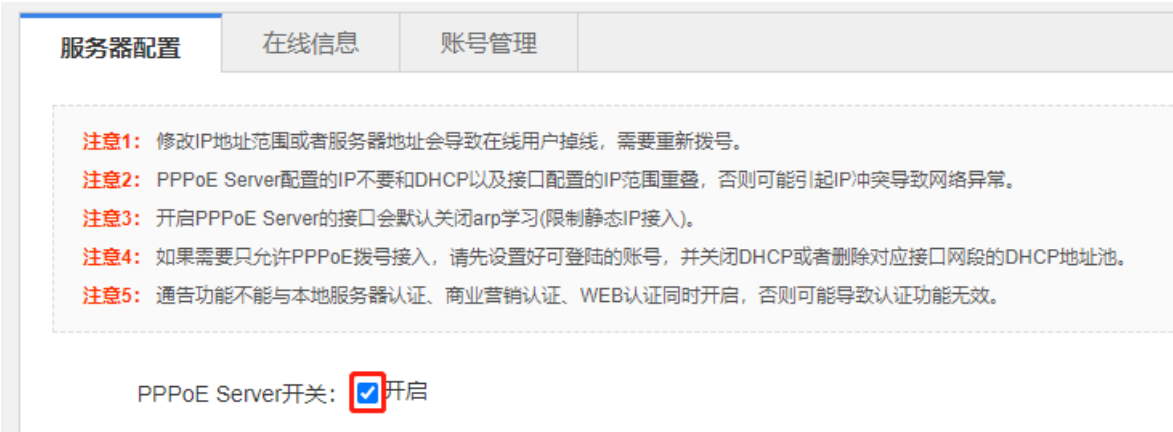
7.5.2 服务器配置

【前置条件】

已在[安全认证]>>[PPPoE Server]>>[账号管理]中配置了至少一个PPPoE账号（具体配置步骤请参考[7.5.3 账号管理](#)）。

【操作步骤】

- (1) 选择[安全认证]>>[PPPoE Server]>>[服务器配置]。
- (2) 点击复选框开启PPPoE Server功能开关。



- (3) 配置其他服务器参数。

内网接口：选择开启PPPoE Server功能的接口。

IP地址范围：PPPoE服务器分配给接入用户的地址范围，默认首个IP为服务器的本地隧道地址。

服务器地址：PPPoE拨号用户通过该地址访问服务器。配置IP地址范围后，默认首个IP为服务器地址。

首选/备选DNS：下发给接入用户的DNS服务器地址。

点击 **>> 高级设置**，展开更多配置项。

通告开关：开启后，账号快到期前会向用户推送通告页面，提醒用户续费。

注意

- 修改IP地址范围或者服务器地址会导致在线用户掉线，需要重新拨号。
- PPPoE Server配置的IP不要和DHCP以及接口配置的IP范围重叠，否则可能引起IP冲突导致网络异常。
- 开启PPPoE Server的接口会默认关闭ARP学习，从而限制静态IP接入。
- 如果需要接口只允许PPPoE拨号接入，请先设置好可登录的账号，并关闭DHCP服务或者删除对应接口网段的DHCP地址池。
- 通告功能不能与本地服务器认证、商业营销认证、WEB认证同时开启，否则可能导致认证功能无效。

服务器配置

在线信息

账号管理

注意1: 修改IP地址范围或者服务器地址会导致在线用户掉线，需要重新拨号。

注意2: PPPoE Server配置的IP不要和DHCP以及接口配置的IP范围重叠，否则可能引起IP冲突导致网络异常。

注意3: 开启PPPoE Server的接口会默认关闭arp学习(限制静态IP接入)。

注意4: 如果需要只允许PPPoE拨号接入，请先设置好可登陆的账号，并关闭DHCP或者删除对应接口网段的DHCP地址池。

注意5: 通告功能不能与本地服务器认证、商业营销认证、WEB认证同时开启，否则可能导致认证功能无效。

PPPoE Server开关: ☒ 开启

内网接口: ☐ Gi0/0 ☐ Gi0/1 ☐ Gi0/2

IP地址范围: - *

服务器地址: * ?

首选DNS: *

备选DNS:

高级设置

通告开关: ☐ 开启 ?

保存配置 清除配置

(4) 点击<保存配置>。

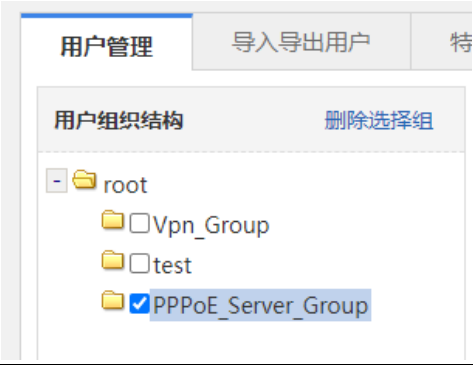
7.5.3 账号管理

说明

如需设置账号的限速，请在“[行为管理]>>[流控策略]”页面中进行流控策略设置并关联对应的用户账号。

注意

如果在“[安全认证]>>[用户组织]>>[用户管理]”中删除了“PPPoE_Server_Group”的用户账号信息，会导致PPPoE Server对应的账号状态变为“无效”。



1. 创建账号

- (1) 选择[安全认证]>>[PPPoE Server]>>[账号管理]。
- (2) 点击<创建账号>。



- (3) 输入设置的账号名称和密码，根据账号的有效期选择“计费方式”。“计费方式”设置为“不限制”，表示该账号永久有效；“计费方式”设置为“按日期”，表示该账号将在指定日期（到期时间）失效，失效后不能再用于PPPoE拨号上网。

(4) 点击 **高级设置**，可以设置账号绑定MAC地址，实现只有固定终端设备能使用账号拨号上网。

MAC地址：

- 不绑定：任意终端均可使用账号连接PPPoE服务器。
- 绑定：静态绑定一个MAC地址，只有该MAC地址的终端可以使用账号连接PPPoE服务器。
- 自动绑定：当终端使用该账号进行拨号时，自动将该账号与终端的MAC地址绑定，此后只有该终端能够使用该PPPoE账号。

备注：根据需求补充账号的备注信息。

(5) 点击<完成配置>。

2. 编辑和删除账号

- 点击操作列的<编辑>按钮可以修改账号的密码、到期时间、MAC绑定信息和备注信息。
- 点击操作列的<删除>按钮可以删除账号。
- 勾选多个账号，点击<删除选中>，可以批量删除账号。

 **注意**
修改账号密码、计费 and 绑定信息，可能导致用户离线。

3. 查询账号

在输入框中输入账号名称的关键字，点击<查询>，可以快速搜索出需要查看的账号信息。

服务器配置

在线信息

账号管理

说明：关于账号的限速，请在“流控-流控策略”页面中进行流控策略设置并关联对应的用户账号。修改账号密码，计费和绑定信息，可能导致用户离线。

注意：如果在“用户-用户组织-用户管理”中删除了“PPPoE_Server_Group”的用户账号信息，会导致PPPoE Server对应的账号状态变为“无效”。

创建账号

删除选中

账号

查询

☐	账号	MAC绑定	计费	状态	操作
☐	test_ppp	不绑定	未限制	有效	编辑 删除

显示: 10

条 共1条

◀ 首页

◀ 上一页

1

下一页 ▶

末页 ▶▶

1

确定

7.5.4 在线信息

查看当前通过PPPoE拨号接入的终端用户信息。查询功能支持分别根据用户账号、IP地址和MAC地址的关键字查询用户信息。

勾选需要强制下线的用户，点击<下线选中>可断开用户与PPPoE服务器的连接。

服务器配置

在线信息

账号管理

说明：显示在线用户信息。

刷新

下线选中

账号

查询

☐	账号	IP地址	MAC地址	上线时间	在线时长	操作
无记录信息						

显示: 10

条 共0条

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶▶

1

确定

表7-1 PPPoE 在线用户信息描述表

参数	说明
账号	接入的PPPoE账号
IP地址	接入终端的IP地址
MAC地址	接入终端的MAC地址
上线时间	用户接入的时间

参数	说明
在线时长	用户的连接时长

7.6 本地防攻击

【应用场景】

防攻击是指为达到保护控制层面的关键资源的目的，对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。

【操作步骤】

(1) 点击[安全认证]>>[本地防攻击]菜单项。

本地防攻击

注意：在配置ACL号时，由于web部分模块使用了特定的ACL号或ACL名，例如：VPN模块使用了110和199，本地防攻击使用了2397、2398，VWAN使用了198，CLI下配置时应该避开使用这几个号。特别是199号，禁止CLI下配置策略，否则会导致web页面VPN模块需要的ACE配置失败。

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

80、443端口限速：
☐开启本机80、443端口限速

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：
☐禁止内网ssh
☒禁止外网ssh

禁止telnet：
☐禁止内网telnet
☐禁止外网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

禁止vpn登录：
☐禁止VPN登录telnet、ssh、web

添加管理员IP：
[【更多】](#)

web访问端口：
(80, 1025-65535)默认为80

web(https)访问端口：
(1025-65535)默认为4430

保存设置

恢复默认设置

(2) 设置防ARP攻击策略。

- ARP欺骗检测：开启后会检测内网是否存在ARP攻击嫌疑，并将疑似存在攻击行为的主机记录在ARP嫌疑列表中，提供给管理员帮助判断嫌疑主机是否存在以及是否需要采取相应处理措施。
- 查看ARP嫌疑列表：点击[【ARP欺骗嫌疑列表】](#)可以查看系统当前存在ARP欺骗嫌疑的主机列表。

(3) 设置防流量攻击策略。

- 防流量攻击：开启后将网络中所有访问设备本身的流量进行限速，超出限速阈值的报文将被丢弃。开启后若设备遭受流量攻击，可以一定程度上减小攻击对设备CPU的压力。

- 80、443端口限速：开启后会对HTTP和HTTPS重定向报文以及访问设备Web的报文进行限速。开启80、443端口限速后可能会影响Web的访问速度，仅当设备开启了认证功能且性能消耗较大（如CPU超过80%）时建议开启。
- 攻击流日志：设备在被攻击的时候会生成对应的日志信息。点击【当前的攻击日志】可以查看系统当前遭受的攻击的日志信息；点击【历史的攻击日志】可以查看系统曾遭受的历史攻击的相关日志。

(4) 设置其他防攻击策略。

- 禁止ping：设备识别出发往本设备的流量中的Ping报文，将此类报文直接丢弃。通过启用 ☒ 禁止内网ping设备 禁止内网用户Ping本设备，通过启用 ☒ 禁止外网ping设备 禁止外网用户Ping本设备。
- 禁止ssh：设备识别出发往本设备的流量中的SSH报文，将此类报文直接丢弃。通过启用 ☒ 禁止内网ssh 禁止内网用户通过SSH方式登录设备，通过启用 ☒ 禁止外网ssh 禁止外网用户通过SSH方式登录设备。
- 禁止telnet：设备识别出发往本设备的流量中的Telnet报文，将此类报文直接丢弃。通过启用 ☒ 禁止内网telnet 禁止内网用户通过Telnet方式登录设备，通过启用 ☒ 禁止外网telnet 禁止外网用户通过Telnet方式登录设备。
- 禁止snmp管理：设备识别出发往本设备的流量中的SNMP管理报文，将此类报文直接丢弃。通过启用 ☒ 禁止内网snmp管理 禁止内网用户通过SNMP方式管理设备，通过启用 ☒ 禁止外网snmp管理 禁止外网用户通过SNMP方式管理设备。
- 禁止web登录：通过启用 ☒ 禁止内网登录设备web系统 禁止内网用户登录到本设备Web系统，启用 ☒ 禁止外网登录设备web系统 禁止外网用户登录到本设备Web系统。
- 禁止vpn登录：禁止VPN用户以Telnet、SSH或Web方式访问设备。
- 添加管理员IP：管理IP是指不受本地防攻击页面策略控制的IP，例如：配置了“禁止内网登录web”，然后配置内网IP“192.168.1.191”为管理IP，则此IP可以正常登录web。点击【更多】最多可添加32个管理IP。

说明：管理IP是指不受本地防攻击页面策略控制的IP，例如：配置了“禁止内网登录web”，然后配置内网IP“192.168.1.191”为管理IP，则此IP可以正常登录web，其他功能点也是类似。最多添加32个条目（IP如192.168.1.2或IP段如192.168.1.2-192.168.1.255）！

管理IP地址：		描述：		添加设置
---------	----------------------	-----	----------------------	-------------------------------------

管理IP地址	描述	操作
显示: 10 条 共0条		
◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶▶ 1 确定		

- web访问端口：通过HTTP协议访问Web时使用的端口号，默认为80端口。如果用户修改了端口号，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，即通过“http://设备IP地址:web访问端口”来访问设备。
- web(https)访问端口：通过HTTPS协议访问Web时使用的端口号，默认为4430端口。如果用户修改了端口号，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，即通过“https://设备IP地址:web(https)访问端口”来访问设备。

(5) 点击<保存设置>。

7.7 接口访问控制

【应用场景】

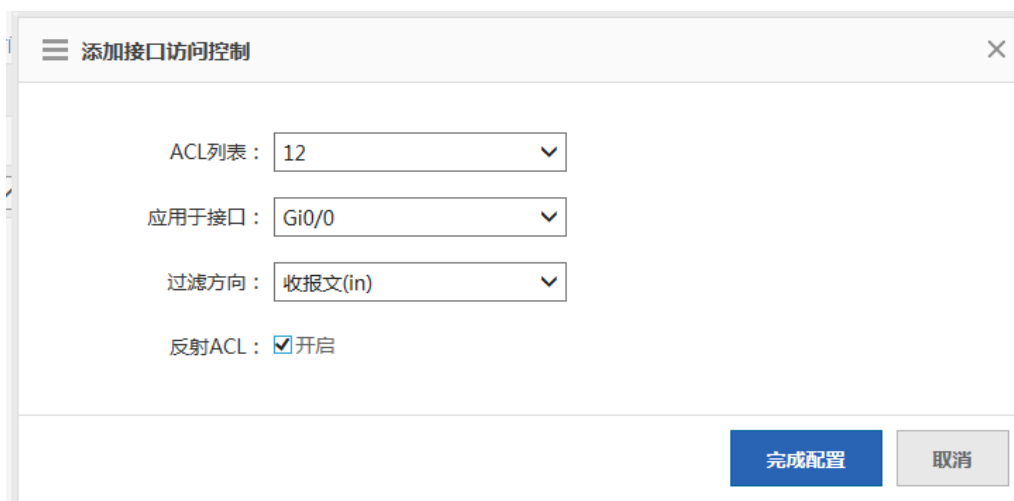
将ACL规则应用到设备接口上，对进出接口的数据包进行控制，从而提升网络设备的安全性。

【操作步骤】

(1) 点击[安全认证]>>[接口访问控制]菜单项。



(2) 点击 **+ 添加接口访问控制** 添加接口访问控制规则。



- a 选择应用的ACL列表号以及生效的接口。
- b 设置报文过滤方向，收报文(in)表示对接口接收到的报文进行过滤，发报文(out)表示对从接口发送出去的报文进行过滤。
- c 反射ACL：按照数据流状态进行检测过滤，开启该选项后，可以跟踪那些离开网络的连接，并允许这些连接的返回流量进入网络。
- d 点击 **完成配置**。

7.8 ARP 表项

7.8.1 功能简介

设备学习连接在设备各接口上的网络设备的IP地址与MAC地址，生成对应ARP表项。支持通过绑定ARP映射和停止ARP学习来限制局域网内主机访问外网，并可以通过免费ARP请求功能来防止ARP欺骗，提高网络安全性。

7.8.2 查看 ARP 表项

【操作步骤】

(1) 点击[安全认证]>>[ARP列表]菜单项。

ARP表项

注意：跨三层不支持ARP绑定（跨三层是指PC的网关不在设备上，请确认PC网关地址所对应的设备并在对应设备绑定ARP）。

说明：静态绑定的效果：一个MAC可以对应多个IP，但是一个IP只能对应一个MAC。如果修改为除静态表项里的其他IP可以正常上网，如果修改MAC则无法正常上网。

提示：导入的文件名必须为staticArp.csv，导入的静态ARP表内，如存在IP项重复的将会进行旧条目覆盖，不重复的不受影响。

[一键绑定](#) [动态>>静态绑定](#) [静态绑定](#) [解除静态绑定](#) ☐ 禁止未静态绑定的内网主机通过

总ARP表项：0 基于IP地址或MAC地址或备注查询: [查询](#)

[Choose File](#) No file chosen [导入静态绑定](#) [导出ARP表项](#)

(一次最多导入500条数据，[下载导入模板](#)，导入静态绑定，导出ARP所有表项。)

☐	IP地址	MAC地址	类型	备注	操作
无记录信息					

显示: 10 条 共0条

« 首页 « 上一页 下一页 » 末页 » 1 [确定](#)

ARP功能设置

停止ARP学习：将只允许静态绑定MAC的PC上网，但对应接口的源进源出功能需要关闭。

免费ARP请求：网关会定期向局域网PC通告自己的IP-MAC地址，避免内网PC被ARP欺骗，同时在被欺骗后仍能及时的学习到正确的网关地址。

停止ARP学习：☐ Gi0/0 ☐ Gi0/1 ☐ Gi0/2

开启免费ARP请求：☒ Gi0/0 ☐ Gi0/1 ☐ Gi0/2

[保存设置](#)

(2) 页面将显示设备学习到的ARP表项。点击<导出ARP表项>可以将表项数据导出到本地。右上角搜索框支持根据IP地址或MAC地址查找ARP表项。

7.8.3 静态 ARP 绑定

1. 手工绑定

【操作步骤】

(1) 点击[安全认证]>>[ARP列表]菜单项。

(2) 点击<静态绑定>。



- (3) 手工绑定分为两种模式：针对单用户一个一个手工配置，或通过整网扫描的方式批量绑定。
- 单用户绑定：输入要绑定的主机信息，包括IP地址、MAC地址和备注信息，点击<保存配置>。

单用户手工绑定

IP地址:

MAC地址:

(如: 00d0.f86b.dcb e)

备注:

保存设置

- 批量绑定：选择要扫描的接口，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。

批量用户手工绑定

说明: 1.如果电脑已经开机，只需输入IP地址范围，然后按扫描，设备会自动完成指定范围地址的电脑IP/MAC动态绑定。如果需要静态绑定，扫描完成后请到ARP表项页面点击一键绑定。
2.如果接口停止ARP学习，扫描功能将失效。

选择接口:

开始扫描

2. 动态表项转静态

【操作步骤】

- (1) 点击[安全认证]>>[ARP列表]菜单项。
- (2) 在ARP表项列表中勾选需要转换为静态表项的动态表项，点击<动态>>静态绑定>。

The screenshot shows the 'ARP Table' management interface. At the top, there are tabs for 'One-click Binding', 'Dynamic to Static Binding' (highlighted with a red box), 'Static Binding', 'Remove Static Binding', and 'Prohibit Internal Network Hosts from Accessing Static Binding'. Below the tabs, there are search and import/export buttons. A table lists ARP entries with columns for 'IP Address', 'MAC Address', 'Type', 'Remarks', and 'Operations'. The first entry has IP 192.168.3.2, MAC 00e0.4c36.0bea, and Type 'Dynamic Binding' (highlighted with a red box). The bottom status bar shows '1' entry and a 'Confirm' button.

- (3) 绑定后的表项显示为静态绑定类型。

This screenshot shows the same ARP Table interface after conversion. The 'Dynamic to Static Binding' tab is still selected. The entry with IP 192.168.3.2 now has a Type of 'Static Binding' (highlighted with a red box). The 'Operations' column now includes an 'Edit' button. The bottom status bar indicates '1' entry and a 'Confirm' button.

- (4) 点击<一键绑定>可以将设备上的所有动态ARP表项转为静态ARP表项。

This screenshot shows the 'One-click Binding' button (highlighted with a red box) being clicked. A confirmation dialog box appears in the center, asking 'Execute one-click binding will convert all dynamic ARP items to static ARP items. Do you want to execute one-click binding?'. The dialog has 'OK' and 'Cancel' buttons. A red arrow points from the 'One-click Binding' button to the dialog. The background interface shows the 'One-click Binding' tab is now active, and the table is empty.

3. 文件导入静态绑定表项

【操作步骤】

- (1) 点击[安全认证]>>[ARP列表]菜单项。
- (2) 点击<下载导入模板>，将导入模板下载到本地。

一键绑定

动态>>静态绑定

静态绑定

解除静态绑定

☐禁止未静态绑定的内网主机通过

总ARP表项: 1 基于IP地址或MAC地址或备注查询:

查询

Choose File

No file chosen

导入静态绑定

导出ARP表项

(一次最多导入500条数据, 下载导入模板, 导入静态绑定, 导出ARP所有表项。)

☐	IP地址	MAC地址	类型	备注	操作
☐	192.168.3.2	00e0.4c36.0bea	静态绑定		编辑

显示: 10 条 共1条

首页 上一页 1 下一页 末页 1 确定

(3) 修改模板文件，根据模板格式填入需要绑定的ARP表项。

	A	B	C
1	IP地址	MAC地址（格式要求xxxx.xxxx.xxxx，如12ab.23ab.34ab）	备注（长度不超过32个字符，中文占两个字符，不支持含换行符的字段）
2			
3			
4			
5			
6			

(4) 回到[ARP列表]页面，点击<选择文件>，选取上一步骤中修订的模板文件，点击<导入静态绑定>。

Choose File staticArp.csv 导入静态绑定 导出ARP表项

(一次最多导入500条数据, 下载导入模板, 导入静态绑定, 导出ARP所有表项。)

【后续处理】

解除静态绑定：勾选需要解除静态绑定的ARP表项，点击<解除静态绑定>。

一键绑定

动态>>静态绑定

静态绑定

解除静态绑定

☐禁止未静态绑定的内网主机通过

总ARP表项: 1 基于IP地址或MAC地址或备注查询:

查询

Choose File

No file chosen

导入静态绑定

导出ARP表项

(一次最多导入500条数据, 下载导入模板, 导入静态绑定, 导出ARP所有表项。)

☒	IP地址	MAC地址	类型	备注	操作
☒	192.168.3.2	00e0.4c36.0bea	静态绑定		编辑

显示: 10 条 共1条

首页 上一页 1 下一页 末页 1 确定

7.8.4 设置 ARP 过滤

开启后只有IP地址和MAC地址符合静态ARP绑定表项的主机才能上网。

【操作步骤】

- (1) 点击[安全认证]>>[ARP列表]菜单项。
- (2) 设置静态ARP绑定。参考7.8.3 静态ARP绑定章节。
- (3) 勾选开启“禁止未静态绑定的内网主机通过”选项。
设置该选项后，只有IP地址和MAC信息与静态绑定信息中一致，设备才会放行对应的流量。

ARP表项

注意：跨三层不支持ARP绑定（跨三层是指PC的网关不在设备上，请确认PC网关地址所对应的设备并在对应设备绑定ARP）。

说明：静态绑定的效果：一个MAC可以对应多个IP，但是一个IP只能对应一个MAC。如果修改或删除静态表项里的其他IP可以正常上网。如果修改MAC则无法正常上网。

提示：导入的文件名必须为staticArp.csv，导入的静态ARP表内，如存在IP项重复的将会进行旧条目覆盖，不重复的不会影响。

☐ 一键绑定
 ☐ 动态 >> 静态绑定
 ☐ 静态绑定
 ☐ 解除静态绑定
 ☐ 禁止未静态绑定的内网主机通过

总ARP表项：1 基于IP地址或MAC地址或备注查询：

No file chosen

(一次最多导入500条数据，下载导入模板，导入静态绑定，导出ARP所有表项。)

☐	IP地址	MAC地址	类型	备注	操作
☐	192.168.3.2	00e0.4c36.0bea	静态绑定		编辑

显示 条 共1条

7.8.5 停止 ARP 学习

停止接口的ARP学习功能后，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。

说明

需要同时关闭接口的源进源出功能（[网络]>>[接口配置]>>[接口基本设置]>>端口高级配置，详见[8.1.1](#) 章节），否则“停止ARP学习”功能可能不生效。

【操作步骤】

- 点击[安全认证]>>[ARP列表]菜单项。
- 在ARP功能设置部分，勾选需要停止ARP学习的内网接口，点击<保存设置>。

ARP功能设置

停止ARP学习：将只允许静态绑定MAC的PC上网，但对应接口的源进源出功能需要关闭。

免费ARP请求：网关会定期向局域网PC通告自己的IP-MAC地址，避免内网PC被ARP欺骗，同时在被欺骗后仍能及时地学习到正确的网关地址。

停止ARP学习：☒ Gi0/0 ☐ Gi0/1 ☐ Gi0/2

开启免费ARP请求：☐ Gi0/0 ☐ Gi0/1 ☐ Gi0/2

7.8.6 免费 ARP 请求

内网接口开启免费ARP请求功能后，当设备接口作为下联设备的网关时，接口将定时发送免费ARP请求来公告自己才是真正的网关，从而避免内网PC被ARP欺骗以及保证内网PC在被欺骗后仍能及时地学习到正确的网关地址。可以通过开启本功能来预防ARP网关欺骗类型的攻击行为。

【操作步骤】

- 点击[安全认证]>>[ARP列表]菜单项。
- 在ARP功能设置部分，勾选需要停止ARP学习的内网接口，点击<保存设置>。

ARP功能设置

停止ARP学习： 将只允许静态绑定MAC的PC上网，但对应接口的源进源出功能需要关闭。

免费ARP请求： 网关会定期向局域网PC通告自己的IP-MAC地址，避免内网PC被ARP欺骗，同时在被欺骗后仍能及时的学习到正确的网关地址。

停止ARP学习：☐Gi0/0 ☐Gi0/1 ☐Gi0/2

开启免费ARP请求：☒Gi0/0 ☐Gi0/1 ☐Gi0/2

保存设置

7.9 ACL 访问列表

【应用场景】

ACL（Access Control List，访问控制列表）也称为访问列表，有的文档中还称之为包过滤。ACL通过定义一系列包含“允许”或“拒绝”的规则语句，并将这些规则应用到设备接口上，对进出接口的数据包进行控制，从而提升网络设备的安全性。

【操作步骤】

(1) 点击[安全认证]>>[ACL访问列表]>>[ACL访问列表]菜单项。



(2) 点击 **添加** 按钮，添加ACL规则。

- 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。
- 点击<确定>。



(3) 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。

添加ACE规则

ACL类型：标准ACL（控制源地址） ← ACL类型

ACL列表：test ← ACL列表名称

... 规则设置

访问控制：
 ☒ 允许 ☐ 禁止 生效时间：晚上 [【生效时间管理】](#)

☐ 任意IP地址：（IP地址任意是对所有的IP应用该规则）

IP地址：12.12.5.5

确定 取消

- **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。

添加ACE规则

ACL类型：扩展ACL（细化控制数据流） ← ACL类型

ACL列表：test-ex ← ACL列表名称

... 规则设置

访问控制：
 ☐ 允许 ☒ 禁止

协议：IP 生效时间：白天 [【生效时间管理】](#)

☐ 源IP地址任意：（源IP地址任意是对所有的源IP应用该规则）

IP地址：12.2.25.7 掩码地址：255.255.255.255

☐ 目的IP地址任意：（目的IP地址任意是对所有的目的IP应用该规则）

IP地址：1.2.2.5

确定 取消

单IP地址

单IP地址

掩码设置

通配符

- 源地址和目的IP地址可以选择地址类型

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，通过掩码确定匹配的IP地址；

通配符：输入源或目的地址的IP地址段，通过通配符确定匹配的IP地址。



说明

- 其中源或目的IP地址和源或目的端口号 都可以设置为任意。
- 通配符掩码规定了当一个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”表示忽略IP地址中对应的位，而“0”则表示该位必须保留。如果忽略了通配符掩码，0.0.0.0将被认为是缺省的屏蔽字。

【后续处理】

- 系统生成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 [X 删除选中](#) 可以删除选中的ACL规则。

7.10 连接数限制

通过该功能可以限制通过设备总会话数，避免某一个用户消耗大量的新建连接，导致其他用户无法连接，出现上网卡顿等现象。

7.10.1 设备抗攻击配置

防内网上行攻击：用于限制内网用户每秒上行报文速率。

新建会话数限制：用于限制内网用户每秒会话数的新建速度。

【操作步骤】

- (1) 点击[安全认证]>>[连接数限制]菜单项。
- (2) 设置限制内网上行报文速率：可选择设置全局生效的默认配置，或对单个IP进行限制。
 - **全局设置**：设置默认每个IP每秒上行报文的限制个数。
 - a 点击<默认全局配置>。

全局会话数

设备抗攻击

说明：防止内网用户异常攻击行为导致设备转发异常。
 注意：在配置ACL号时，由于web部分模块使用了特定的ACL号或ACL名，例如：VPN模块使用了110和199，本地防攻击使用了2397、2398，VWAN使用了198，CLI下配置时应避开使用这几个号。特别是199号，禁止CLI下配置策略，否则会导致web页面VPN模块需要的ACE配置失败。

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】 ?

b 在弹出的页面中输入内网单个IP每秒上行报文的限制个数，0表示不限制。

防内网上行攻击配置

默认限制每个IP每秒上行报文的个数： pps (0 ~ 100000)

配置默认为关闭，0为关闭，非0为开启，开启建议配置 3000-5000

保存配置

c 点击<保存配置>。

- **设置单个IP**：设置指定IP每秒上行报文的限制个数。单IP的限制规则将优先于全局配置生效。

a 点击<对单个ip进行配置>。

全局会话数

设备抗攻击

说明：防止内网用户异常攻击行为导致设备转发异常。
 注意：在配置ACL号时，由于web部分模块使用了特定的ACL号或ACL名，例如：VPN模块使用了110和199，本地防攻击使用了2397、2398，VWAN使用了198，CLI下配置时应避开使用这几个号。特别是199号，禁止CLI下配置策略，否则会导致web页面VPN模块需要的ACE配置失败。

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】 ?

b 在弹出的页面中输入限制的IP地址和该IP每秒上行报文的限制个数，0表示不限制。

指定某个IP上行报文个数的限制，0是不限制，优先级比默认的限制规则高，匹配了这个就不会去匹配默认的规则
 如果某个IP被误识别成虚拟IP，可以使用该配置把该IP加入到真实IP中去

IP防上行流量攻击配置

IP:

上行报文个数: 个 (0 ~ 100000)

保存配置

c 点击<保存配置>。配置的规则将在页面下方表格显示，如需删除或修改，可点击<编辑>或<删除>。

IP	防上行流量 (pps)	管理
1.1.1.1	100	编辑 删除
显示: 10 条 共1条		
首页 上一页 1 下一页 末页 1 确定		

(3) 设置限制内网用户每秒可新建的会话数：可选择设置全局生效的默认配置，或对单个IP进行限制。

- **全局设置：**

a 点击<默认全局配置>。

全局会话数

设备抗攻击

说明：防止内网用户异常攻击行为导致设备转发异常。

注意：在配置ACL号时，由于web部分模块使用了特定的ACL号或ACL名，例如：VPN模块使用了110和199，本地防攻击使用了2397、2398，VWAN使用了198，CLI下配置时应避开使用这几个号，特别是199号，禁止CLI下配置策略，否则会导致web页面VPN模块需要的ACE配置失败。

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】](#) ?

b 在弹出的页面中输入每秒新建的连接数限制值，点击<保存配置>。

全局新建会话数限制配置

启机三分钟内，所有虚拟主机每秒新建的连接数限制： [↑ \(0 ~ 100000\)](#) [建议配置 1000-2000](#)

设备正常运行中，所有虚拟主机每秒新建的连接数限制： [↑ \(0 ~ 100000\)](#) [建议配置 500-800](#)

默认每个真实主机的每秒新建连接数限制： [↑ \(0 ~ 100000\)](#) [建议配置 100-150](#)

[保存配置](#)

- **设置单个IP：**单IP的限制规则将优先于全局配置生效。

a 点击<对单个ip进行配置>。

全局会话数

设备抗攻击

说明：防止内网用户异常攻击行为导致设备转发异常。

注意：在配置ACL号时，由于web部分模块使用了特定的ACL号或ACL名，例如：VPN模块使用了110和199，本地防攻击使用了2397、2398，VWAN使用了198，CLI下配置时应避开使用这几个号，特别是199号，禁止CLI下配置策略，否则会导致web页面VPN模块需要的ACE配置失败。

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】](#) ?

b 在弹出的页面中输入限制的IP地址和该IP的每秒新建连接数限制，0表示不限制。

指定某个真实主机的每秒新建连接数限制，0是不限制，优先级比默认的高，匹配了这个就不会去匹配默认的规则
如果某个IP被误识别成虚拟IP，可以使用该配置把该IP加入到真实IP中去

单IP每秒新建连接数限制配置

IP:

每秒新建连接数限制: ↑ (0 ~ 100000)

保存配置

c 点击<保存配置>。配置的规则将在页面下方表格显示，如需删除或修改，可点击<编辑>或<删除>。

IP	每秒新建连接数限制 (个)	管理
1.1.1.1	100	编辑 删除
显示: 10 条 共1条		
首页 上一页 1 下一页 末页 1 确定		

(4) 查看存在“通过新建大量会话攻击设备”的行为的嫌疑主机：点击<会话数攻击嫌疑列表>，查看具有攻击行为的主机信息。

全局会话数

设备抗攻击

说明：防止内网用户异常攻击行为导致设备转发异常。

注意：在配置ACL号时，由于web部分模块使用了特定的ACL号或ACL名，例如：VPN模块使用了110和199，本地防攻击使用了2397、2398，VWAN使用了198，CLI下配置时应该避开使用这几个号。特别是199号，禁止CLI下配置策略，否则会导致web页面VPN模块需要的ACE配置失败。

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】](#) ?

7.10.2 设置内网用户会话数限制

说明

如果存在特殊用途的IP（如服务器、外网口），请先将特殊用途的IP配置成用户（配置步骤见[7.1.1](#) 章节），再对该用户进行会话数配置。

1. 新建会话数策略

【操作步骤】

(1) 点击[安全认证]>>[连接数限制]菜单项。

(2) 新建会话数限制策略。

点击  [新建会话数策略](#) 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。

- 基于用户的会话数限制策略：

三 新建会话数限制策略

限制类型：☒ 基于用户 ☐ 基于ACL

选择用户：所有用户

选择用户

控制方式：

设置会话数

最大总会话数：

300000

 (0-600000, 0为不限制)推荐配置大于300000的值

每IP最大会话数：

500

 (0-600000, 0为不限制)推荐配置大于500的值

完成配置

取消

- a **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。

三 用户选择

所有用户

web认证

Vpn_Group

lgh150

fff

vpn_euser_

3.3.3.3

(如需添加用户请到 用户管理->用户组织)

确定

b **控制方式：**在下拉框

设置会话数

 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)。

c 点击<确定>。

- 基于ACL的会话数限制策略：

204

- a 选择ACL号：下拉框 中列出了系统已配置的ACL号，用户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。

- b 控制方式：在下拉框 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)。

- c 点击<完成配置>。

【后续处理】

- 会话数限制策略列表如下所示。

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

1

- 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 、 按钮可以调整现有策略的优先级。

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。

2. 限制内网 UDP 会话数比例

- (1) 点击[安全认证]>>[连接数限制]菜单项。
- (2) 点击<内网UDP会话数比例限制>。

内网用户会话数限制

说明：如果存在特殊用途的IP（如服务器、外网口），请先将特殊用途的IP【配置成用户】，再对该用户进行会话数配置。

+ 新建会话数策略 **内网UDP会话数比例限制** 查看每IP流会话数情况

(3) 输入内网UDP会话数占总会话数的比例，点击<保存>进行保存。

内网UDP会话数比例限制

说明：设置每用户最大总会话数的UDP比例上限，例如：配置某条基于用户的会话数策略，策略限制每IP最大会话数为2000，假如配置UDP会话数限制比例为50%，则每用户UDP的最大会话数不超过1000。比例配置为0表示不限制UDP会话数。

udp会话数限制比例： % (30~80, 0表示不限制udp , 推荐值50%)

保存

注意
限制比例范围为30-80，默认为0，即不限制UDP会话数比例。

3. 查看每 IP 流会话数情况

(1) 点击[安全认证]>>[连接数限制]菜单项。

内网用户会话数限制

说明：如果存在特殊用途的IP（如服务器、外网口），请先将特殊用途的IP【配置成用户】，再对该用户进行会话数配置。

+ 新建会话数策略 **内网UDP会话数比例限制** **查看每IP流会话数情况**

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
基于用户	所有用户	设置会话数	不限制	2000	生效		编辑 删除

显示 10 条 共1条

首页 上一页 1 下一页 末页 1 确定

(2) 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：

查看每IP流会话数情况

ip	用户	会话数
172.18.124.211	/172.18.124.211	2
10.10.10.105	/10.10.10.105	1
10.10.10.99	/10.10.10.99	0
3.3.3.6	/3.3.3.6	0
172.18.125.169	/172.18.125.169	0
192.168.119.233	/192.168.119.233	0
10.10.10.205	/10.10.10.205	0

首页

上一页

1

下一页

末页

1

确定

8 网络

8.1 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用户是否可以正常上网。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），显示为灰色  表示该接口未上电；如  图标上有小地球的接口表示外网口，没有的话为内网口。

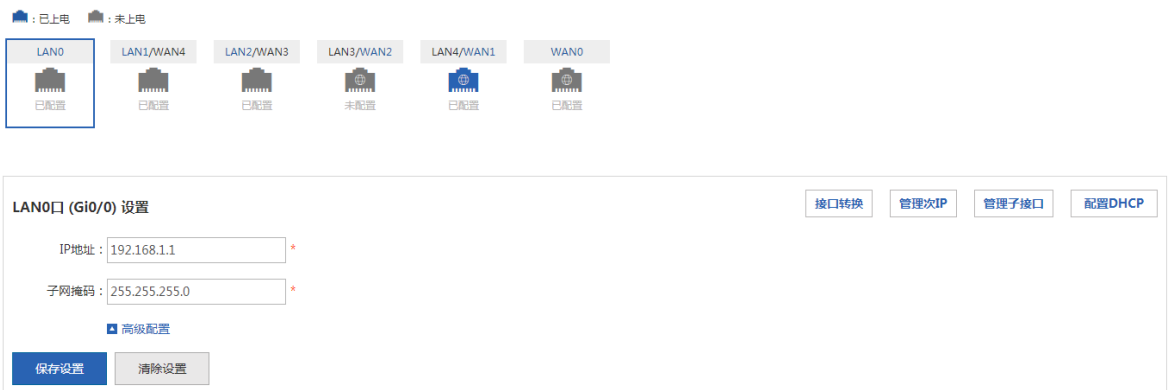
8.1.1 接口基本设置

【应用场景】

通过该操作，可以对设备的各类接口进行配置。

【操作步骤】

(1) 点击[网络]>>[接口配置]>>[接口基本设置]菜单项。



(2) 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  ：

LAN0口 (Gi0/0) 设置

IP地址：	192.168.1.1	*
子网掩码：	255.255.255.0	*
☒ 高级配置		
接口描述：		
MAC地址：	00d0.f822.33fa	(格式：00d0.f822.1234)
AnyIP配置：	☐ 勾选开启AnyIP功能	
开启源进源出：	☒ 勾选开启源进源出 ?	
保存设置 清除设置		

a 设置IP地址和子网掩码。

IP地址：输入内网口的IP地址，即内网网段的网关IP地址。

子网掩码：网段对应的掩码地址。

b 展开“高级选项”，设置LAN口的其他配置项。

MAC地址：接口的物理地址，为接口配置不同的MAC地址主要是为了防止内部物理地址冲突，通常情况下可以不配置。

AnyIP配置：开启AnyIP功能后，内网PC不配置或随意配置IP地址都能实现正常上网，也就是说开启该功能后可以避免部分PC配错IP地址导致无法上网的问题。

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。

c 设置次IP和子接口。

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

管理次IP

可以查看和管理选中接口下的次IP地址：

管理次IP

×

IP 地址：

*

子网掩码：

255.255.255.0

*

添加次IP

IP地址	子网掩码	操作
无记录信息		

显示: 10

条 共0条

首页

上一页

下一页

末页

1

确定

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：

接口配置 - 配置接口的逻辑子接口 - Internet Explorer

http://172.18.124.54/interface_pi/int_child.html

子接口名：

Gi0/4

1

*

(1至1023)

Vlan Id：

1

*

(1至4087)

IP地址：

*

掩码：

*

AnyIP配置：

☐

勾选开启AnyIP功能

开启源进源出：

☐

勾选开启源进源出

添加子接口

子接口列表

子接口名	Vlan Id	接口信息	线路带宽	网络服务商	操作
首页 上一页 1 下一页 末页 1 确定					

(3) 外网口配置

- a 首先将用户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。

LAN0
已配置

LAN1/WAN4
已配置

LAN2/WAN3
已配置

LAN3/WAN2
未配置

LAN4/WAN1
已配置

WAN0
已配置

WAN1口 (Gi0/4) 设置

动态IP(DHCP)

接口转换

管理子接口

IP地址 : 172.30.73.73

高级配置

接口描述 :

MAC地址 : 00d0.f822.33fe (格式 : 00d0.f822.1234)

下行带宽 : 10 Mbps(0.5~10000)

上行带宽 : 10 Mbps(0.5~10000)

MTU : 1500 (64-1500) 不配置时默认PPPoE为1488, 其他为1500 请勿随意修改, 可能导致网络异常

开启NAT配置 : ☒勾选开启线路NAT功能

开启源进源出 : ☒勾选开启源进源出

保存设置

清除设置

b 设置线路类型。

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：

当线路类型选择“静态IP地址”时需要配置运营商分配给用户的IP地址、子网掩码和网关地址。

WAN4口 (Gi0/3) 设置

静态IP地址

专线

IP地址:

子网掩码:

外网网关:

○ PPPoE（ADSL）

如果用户向运营商申请的是ADSL线路则请选择“PPPoE(ADSL)”，需要输入用户从网络运营商处申请的拨号帐号及密码。

外网口配置 **PPPoE(ADSL)** ▼

Gi0/6口-账号：*

密码：*

IP 地址：

接口描述：

MAC地址： (格式：00d0.f822.1234)

下行带宽： Mbps(0.5~10000)不配置时默认为4

上行带宽： Mbps(0.5~10000)不配置时默认为0.5

网络服务商：☐电信 ☐移动 ☐联通 ☐教育 ☒其它

开启缺省路由：☒勾选开启缺省路由

开启NAT配置：☒勾选开启线路NAT功能

开启源进源出：☒勾选开启源进源出

光电转换： ▼

○ 动态IP地址：

如果用户的上网方式选择“动态IP地址”，系统将动态获取IP地址。

外网口配置 **动态IP(DHCP)** ▼

IP 地址：

接口描述：

MAC地址： (格式：00d0.f822.1234)

下行带宽： Mbps(0.5~10000)不配置时默认为10

上行带宽： Mbps(0.5~10000)不配置时默认为10

开启NAT配置：☒勾选开启线路NAT功能

开启源进源出：☒勾选开启源进源出

光电转换： ▼

c 展开“高级配置”，设置外网口的其他配置信息。

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。

光电转换：选择接口作为光口还是作为电口使用，只有部分光电复用的外网口支持该配置项。

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

网络服务商：包括电信，移动，联通，教育，其他网络。

(4) 点击<保存设置>。

8.1.2 一线多拨

【应用场景】

开启一线多拨功能后，对接的接口可以添加拨号线路。

【操作步骤】

(1) 点击[网络]>>[接口配置]>>[一键多拨]。



(2) 开启一线多拨功能。

8.1.3 多链路聚合

【应用场景】

AP (Aggregate Port，链路聚合口) 可以将多个物理链接捆绑在一起形成一个逻辑链接，用于扩展链路带宽，提供更高的连接可靠性。当需要拓展链路带宽时，可以设置链路聚合。

【操作步骤】

(1) 点击[网络]>>[接口配置]>>[多链路聚合]菜单项。



(2) 点击 **+添加**。

三 添加内网多链路聚合

选择聚合口：Ag1

聚合接口：☐Gi0/0 ☐Gi0/1 ☐Gi0/2 ☐Gi0/3 ☐Gi0/4 ☐Gi0/5

IP地址：

掩码：

开启NAT配置：☒勾选开启线路NAT功能

确定

取消

- (3) 设置内网多路聚合相关配置项。
选择聚合口，聚合接口，输入IP地址和掩码
- (4) 点击 确定 完成配置。

8.1.4 接口转换

【应用场景】

对于支持LAN/WAN转换的接口，本页面提供内网口与外网口的转换功能。

【操作步骤】

- (1) 点击[网络]>>[接口配置]>>[接口转换]菜单项。

接口基本设置 一线多拨 多链路聚合 接入模式选择 接口转换 链路检测 接口基本配置IPv6

说明：该功能允许内外网口相互转换，详细对应关系见下面。
注意：第一个和最后一个接口不允许转换，在选择完毕并点击保存后，需要重启设备才能生效，生效后可以在接口配置页面进行对应的接口设置。
如有多条外网线情况下，至少留一个内网口。

LAN0 LAN1/WAN4 LAN2/WAN3 LAN3/WAN2 LAN4/WAN1 WAN0

内网口 内网口 外网口 内网口 外网口 外网口

接口转换保存

(2) 选择要进行接口转换的接口，点击下拉框选择接口属性，可将内网口转换为外网口，或将外网口转换为内网口。

214



(3) 点击  按钮重启设备，接口模式方可生效。

8.1.5 链路检测

【应用场景】

通过该操作可以检测设备外网口接口是否正常工作。

【操作步骤】

(1) 点击[网络]>>[接口配置]>>[链路检测]菜单项。



(2) 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：

ping地址： * 下一跳地址： * 探测间隔： 100 单位：毫秒

- 若要检测接口是否可连接，请输入可Ping通的IP地址。

⚠ 注意

请勿输入无法Ping通的IP地址，如果Ping失败，设备将关闭接口，使接口无法通信，从而导致设备断网。

- 输入下一跳地址，若为内网设备则输入网关地址。
- 输入探测间隔时间。

(3) 点击 ，如果符合上述配置可Ping通，则系统显示提示信息为“网络良好”，否则系统提示“网络不通”。

8.1.6 端口监控

【应用场景】

通过该操作，可以对端口接收和发送的数据进行监控，以便及时获取异常数据。

【操作步骤】

(1) 点击[网络]>>[接口配置]>>[端口监控]菜单项。



(2) 选择监控接口、被监控端口以及待监控数据。

(3) 点击<保存设置>。

8.1.7 接口基本设置 IPv6

说明

仅支持IPv6特性的设备支持配置本功能。支持IPv6的产品包括：NBR6205-E、NBR6205-E V2、NBR6135-E、NBR6210-E、NBR6210-E V2、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E。

【应用场景】

通过该操作，可以设置内网口和外网口的IPv6地址。

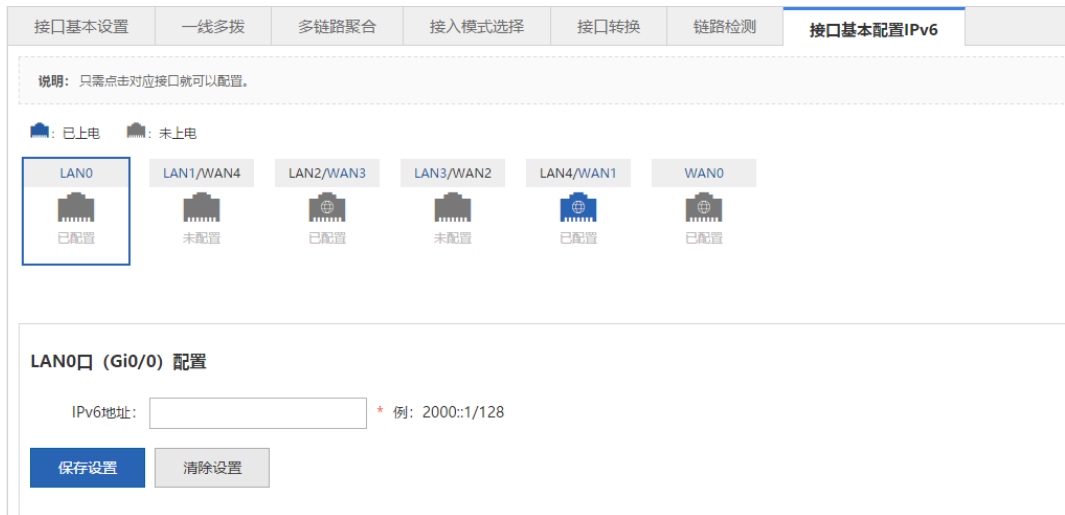
【前置条件】

需要在[运维]>>[系统设置]>>[增强功能]中开启IPv6大容量功能（配置后需要重启设备以生效）。



【操作步骤】

(1) 点击[网络]>>[接口配置]>>[接口基本配置IPv6]菜单项。



(2) 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 。

(3) 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 ：



8.2 SUPER-VLAN

8.2.1 功能简介

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。

8.2.2 SUPER-VLAN 配置

【应用场景】

通过该页面可以开启和配置SUPER-VLAN功能。

【操作步骤】

(1) 点击[网络]>>[SUPER-VLAN信息]>>[SUPER-VLAN配置]菜单项。

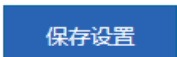
(2) 勾选“开启SUPER-VLAN”。

(3) 设置“每VID最大上线数”。

允许VLAN的最大上线数，取值范围为1到1000。

(4) 选择内网口配置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。

(5) 配置完后点  保存设置。

8.2.3 在线 SUPER-VLAN 信息

【操作步骤】

(1) 点击[网络]>>[SUPER-VLAN信息]>>[在线SUPER-VLAN信息]菜单项。

(2) 查看当前的在线的SUPER-VLAN信息，如下图所示。

8.3 路由/负载

8.3.1 功能简介

- 路由包括策略路由、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，例如校园网络的出口通常连接着教育网线路和电信/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。

8.3.2 选路配置向导

首次配置时，网吧场景下会增加选路配置向导菜单（[网络]>>[路由/负载]>>[选路配置向导]），如下图。



选路配置向导适用于多线路场景，向导可以根据当前设备出口的运营商以及带宽情况，自动识别线路好坏，生成较优的应用路由等选路方案，合理分配各线路的流量。

【操作步骤】

(1) 点击<开启检测>，系统将自动检测当前外网接口线路状态。



(2) 点击<生成选路配置>，确认主线路、线路运营商属性以及DNS服务器，点击<完成配置>便可一键生成较优配置方案。

接口信息

Gi0/4

运营商：

电信

DNS1：

192.168.58.110

主线路

DNS2：

完成配置

8.3.3 策略路由

【应用场景】

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，必须要创建并指定策略路由使用的路由图。一个路由图由很多条策略组成，每个策略都定义了一个或多个的匹配规则和对应该操作。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。

【操作步骤】

(1) 点击[网络]>>[路由/负载]>>[策略路由]菜单项。

策略路由

应用路由

普通路由

多链路负载均衡

路由优先级：策略路由、应用路由和普通路由都可以作为报文转发的依据。当策略路由同时存在的情况下，优先级为：策略路由 > 应用路由 > 普通路由（地址库）> 默认路由。
说明：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转发机制。以太网环境下需要配置下一跳地址，而PPPoE环境下需要配置接口。
注意：若存在不同内网网络互连，配置策略路由前需在关联的ACL中排除内网互连网络。
帮助：策略路由常见功能如何使用？

策略组匹配接口：

Gi0/0

策略优先级： * (0~65535)

匹配ACL列表：

1

[【新建ACL列表】](#)

出口/下一跳：

接口

指定接口

[【PPPoE环境】](#) PPPoE环境下需要配置接口

添加设置

策略路由列表

选择策略组匹配接口：

Gi0/0

删除全部

策略优先级	匹配ACL列表	接口	下一跳地址	操作
无记录信息				

显示 10 条 共 0 条

14 页 1 页 2 页 3 页 4 页 5 页 6 页 7 页 8 页 9 页 10 页 11 页 12 页 13 页 14 页 15 页 16 页 17 页 18 页 19 页 20 页 21 页 22 页 23 页 24 页 25 页 26 页 27 页 28 页 29 页 30 页 31 页 32 页 33 页 34 页 35 页 36 页 37 页 38 页 39 页 40 页 41 页 42 页 43 页 44 页 45 页 46 页 47 页 48 页 49 页 50 页 51 页 52 页 53 页 54 页 55 页 56 页 57 页 58 页 59 页 60 页 61 页 62 页 63 页 64 页 65 页 66 页 67 页 68 页 69 页 70 页 71 页 72 页 73 页 74 页 75 页 76 页 77 页 78 页 79 页 80 页 81 页 82 页 83 页 84 页 85 页 86 页 87 页 88 页 89 页 90 页 91 页 92 页 93 页 94 页 95 页 96 页 97 页 98 页 99 页 100 页 101 页 102 页 103 页 104 页 105 页 106 页 107 页 108 页 109 页 110 页 111 页 112 页 113 页 114 页 115 页 116 页 117 页 118 页 119 页 120 页 121 页 122 页 123 页 124 页 125 页 126 页 127 页 128 页 129 页 130 页 131 页 132 页 133 页 134 页 135 页 136 页 137 页 138 页 139 页 140 页 141 页 142 页 143 页 144 页 145 页 146 页 147 页 148 页 149 页 150 页 151 页 152 页 153 页 154 页 155 页 156 页 157 页 158 页 159 页 160 页 161 页 162 页 163 页 164 页 165 页 166 页 167 页 168 页 169 页 170 页 171 页 172 页 173 页 174 页 175 页 176 页 177 页 178 页 179 页 180 页 181 页 182 页 183 页 184 页 185 页 186 页 187 页 188 页 189 页 190 页 191 页 192 页 193 页 194 页 195 页 196 页 197 页 198 页 199 页 200 页 201 页 202 页 203 页 204 页 205 页 206 页 207 页 208 页 209 页 210 页 211 页 212 页 213 页 214 页 215 页 216 页 217 页 218 页 219 页 220 页 221 页 222 页 223 页 224 页 225 页 226 页 227 页 228 页 229 页 230 页 231 页 232 页 233 页 234 页 235 页 236 页 237 页 238 页 239 页 240 页 241 页 242 页 243 页 244 页 245 页 246 页 247 页 248 页 249 页 250 页 251 页 252 页 253 页 254 页 255 页 256 页 257 页 258 页 259 页 260 页 261 页 262 页 263 页 264 页 265 页 266 页 267 页 268 页 269 页 270 页 271 页 272 页 273 页 274 页 275 页 276 页 277 页 278 页 279 页 280 页 281 页 282 页 283 页 284 页 285 页 286 页 287 页 288 页 289 页 290 页 291 页 292 页 293 页 294 页 295 页 296 页 297 页 298 页 299 页 300 页 301 页 302 页 303 页 304 页 305 页 306 页 307 页 308 页 309 页 310 页 311 页 312 页 313 页 314 页 315 页 316 页 317 页 318 页 319 页 320 页 321 页 322 页 323 页 324 页 325 页 326 页 327 页 328 页 329 页 330 页 331 页 332 页 333 页 334 页 335 页 336 页 337 页 338 页 339 页 340 页 341 页 342 页 343 页 344 页 345 页 346 页 347 页 348 页 349 页 350 页 351 页 352 页 353 页 354 页 355 页 356 页 357 页 358 页 359 页 360 页 361 页 362 页 363 页 364 页 365 页 366 页 367 页 368 页 369 页 370 页 371 页 372 页 373 页 374 页 375 页 376 页 377 页 378 页 379 页 380 页 381 页 382 页 383 页 384 页 385 页 386 页 387 页 388 页 389 页 390 页 391 页 392 页 393 页 394 页 395 页 396 页 397 页 398 页 399 页 400 页 401 页 402 页 403 页 404 页 405 页 406 页 407 页 408 页 409 页 410 页 411 页 412 页 413 页 414 页 415 页 416 页 417 页 418 页 419 页 420 页 421 页 422 页 423 页 424 页 425 页 426 页 427 页 428 页 429 页 430 页 431 页 432 页 433 页 434 页 435 页 436 页 437 页 438 页 439 页 440 页 441 页 442 页 443 页 444 页 445 页 446 页 447 页 448 页 449 页 450 页 451 页 452 页 453 页 454 页 455 页 456 页 457 页 458 页 459 页 460 页 461 页 462 页 463 页 464 页 465 页 466 页 467 页 468 页 469 页 470 页 471 页 472 页 473 页 474 页 475 页 476 页 477 页 478 页 479 页 480 页 481 页 482 页 483 页 484 页 485 页 486 页 487 页 488 页 489 页 490 页 491 页 492 页 493 页 494 页 495 页 496 页 497 页 498 页 499 页 500 页 501 页 502 页 503 页 504 页 505 页 506 页 507 页 508 页 509 页 510 页 511 页 512 页 513 页 514 页 515 页 516 页 517 页 518 页 519 页 520 页 521 页 522 页 523 页 524 页 525 页 526 页 527 页 528 页 529 页 530 页 531 页 532 页 533 页 534 页 535 页 536 页 537 页 538 页 539 页 540 页 541 页 542 页 543 页 544 页 545 页 546 页 547 页 548 页 549 页 550 页 551 页 552 页 553 页 554 页 555 页 556 页 557 页 558 页 559 页 560 页 561 页 562 页 563 页 564 页 565 页 566 页 567 页 568 页 569 页 570 页 571 页 572 页 573 页 574 页 575 页 576 页 577 页 578 页 579 页 580 页 581 页 582 页 583 页 584 页 585 页 586 页 587 页 588 页 589 页 590 页 591 页 592 页 593 页 594 页 595 页 596 页 597 页 598 页 599 页 600 页 601 页 602 页 603 页 604 页 605 页 606 页 607 页 608 页 609 页 610 页 611 页 612 页 613 页 614 页 615 页 616 页 617 页 618 页 619 页 620 页 621 页 622 页 623 页 624 页 625 页 626 页 627 页 628 页 629 页 630 页 631 页 632 页 633 页 634 页 635 页 636 页 637 页 638 页 639 页 640 页 641 页 642 页 643 页 644 页 645 页 646 页 647 页 648 页 649 页 650 页 651 页 652 页 653 页 654 页 655 页 656 页 657 页 658 页 659 页 660 页 661 页 662 页 663 页 664 页 665 页 666 页 667 页 668 页 669 页 670 页 671 页 672 页 673 页 674 页 675 页 676 页 677 页 678 页 679 页 680 页 681 页 682 页 683 页 684 页 685 页 686 页 687 页 688 页 689 页 690 页 691 页 692 页 693 页 694 页 695 页 696 页 697 页 698 页 699 页 700 页 701 页 702 页 703 页 704 页 705 页 706 页 707 页 708 页 709 页 710 页 711 页 712 页 713 页 714 页 715 页 716 页 717 页 718 页 719 页 720 页 721 页 722 页 723 页 724 页 725 页 726 页 727 页 728 页 729 页 730 页 731 页 732 页 733 页 734 页 735 页 736 页 737 页 738 页 739 页 740 页 741 页 742 页 743 页 744 页 745 页 746 页 747 页 748 页 749 页 750 页 751 页 752 页 753 页 754 页 755 页 756 页 757 页 758 页 759 页 760 页 761 页 762 页 763 页 764 页 765 页 766 页 767 页 768 页 769 页 770 页 771 页 772 页 773 页 774 页 775 页 776 页 777 页 778 页 779 页 780 页 781 页 782 页 783 页 784 页 785 页 786 页 787 页 788 页 789 页 790 页 791 页 792 页 793 页 794 页 795 页 796 页 797 页 798 页 799 页 800 页 801 页 802 页 803 页 804 页 805 页 806 页 807 页 808 页 809 页 810 页 811 页 812 页 813 页 814 页 815 页 816 页 817 页 818 页 819 页 820 页 821 页 822 页 823 页 824 页 825 页 826 页 827 页 828 页 829 页 830 页 831 页 832 页 833 页 834 页 835 页 836 页 837 页 838 页 839 页 840 页 841 页 842 页 843 页 844 页 845 页 846 页 847 页 848 页 849 页 850 页 851 页 852 页 853 页 854 页 855 页 856 页 857 页 858 页 859 页 860 页 861 页 862 页 863 页 864 页 865 页 866 页 867 页 868 页 869 页 870 页 871 页 872 页 873 页 874 页 875 页 876 页 877 页 878 页 879 页 880 页 881 页 882 页 883 页 884 页 885 页 886 页 887 页 888 页 889 页 890 页 891 页 892 页 893 页 894 页 895 页 896 页 897 页 898 页 899 页 900 页 901 页 902 页 903 页 904 页 905 页 906 页 907 页 908 页 909 页 910 页 911 页 912 页 913 页 914 页 915 页 916 页 917 页 918 页 919 页 920 页 921 页 922 页 923 页 924 页 925 页 926 页 927 页 928 页 929 页 930 页 931 页 932 页 933 页 934 页 935 页 936 页 937 页 938 页 939 页 940 页 941 页 942 页 943 页 944 页 945 页 946 页 947 页 948 页 949 页 950 页 951 页 952 页 953 页 954 页 955 页 956 页 957 页 958 页 959 页 960 页 961 页 962 页 963 页 964 页 965 页 966 页 967 页 968 页 969 页 970 页 971 页 972 页 973 页 974 页 975 页 976 页 977 页 978 页 979 页 980 页 981 页 982 页 983 页 984 页 985 页 986 页 987 页 988 页 989 页 990 页 991 页 992 页 993 页 994 页 995 页 996 页 997 页 998 页 999 页 1000 页 1001 页 1002 页 1003 页 1004 页 1005 页 1006 页 1007 页 1008 页 1009 页 1010 页 1011 页 1012 页 1013 页 1014 页 1015 页 1016 页 1017 页 1018 页 1019 页 1020 页 1021 页 1022 页 1023 页 1024 页 1025 页 1026 页 1027 页 1028 页 1029 页 1030 页 1031 页 1032 页 1033 页 1034 页 1035 页 1036 页 1037 页 1038 页 1039 页 1040 页 1041 页 1042 页 1043 页 1044 页 1045 页 1046 页 1047 页 1048 页 1049 页 1050 页 1051 页 1052 页 1053 页 1054 页 1055 页 1056 页 1057 页 1058 页 1059 页 1060 页 1061 页 1062 页 1063 页 1064 页 1065 页 1066 页 1067 页 1068 页 1069 页 1070 页 1071 页 1072 页 1073 页 1074 页 1075 页 1076 页 1077 页 1078 页 1079 页 1080 页 1081 页 1082 页 1083 页 1084 页 1085 页 1086 页 1087 页 1088 页 1089 页 1090 页 1091 页 1092 页 1093 页 1094 页 1095 页 1096 页 1097 页 1098 页 1099 页 1100 页 1101 页 1102 页 1103 页 1104 页 1105 页 1106 页 1107 页 1108 页 1109 页 1110 页 1111 页 1112 页 1113 页 1114 页 1115 页 1116 页 1117 页 1118 页 1119 页 1120 页 1121 页 1122 页 1123 页 1124 页 1125 页 1126 页 1127 页 1128 页 1129 页 1130 页 1131 页 1132 页 1133 页 1134 页 1135 页 1136 页 1137 页 1138 页 1139 页 1140 页 1141 页 1142 页 1143 页 1144 页 1145 页 1146 页 1147 页 1148 页 1149 页 1150 页 1151 页 1152 页 1153 页 1154 页 1155 页 1156 页 1157 页 1158 页 1159 页 1160 页 1161 页 1162 页 1163 页 1164 页 1165 页 1166 页 1167 页 1168 页 1169 页 1170 页 1171 页 1172 页 1173 页 1174 页 1175 页 1176 页 1177 页 1178 页 1179 页 1180 页 1181 页 1182 页 1183 页 1184 页 1185 页 1186 页 1187 页 1188 页 1189 页 1190 页 1191 页 1192 页 1193 页 1194 页 1195 页 1196 页 1197 页 1198 页 1199 页 1200 页 1201 页 1202 页 1203 页 1204 页 1205 页 1206 页 1207 页 1208 页 1209 页 1210 页 1211 页 1212 页 1213 页 1214 页 1215 页 1216 页 1217 页 1218 页 1219 页 1220 页 1221 页 1222 页 1223 页 1224 页 1225 页 1226 页 1227 页 1228 页 1229 页 1230 页 1231 页 1232 页 1233 页 1234 页 1235 页 1236 页 1237 页 1238 页 1239 页 1240 页 1241 页 1242 页 1243 页 1244 页 1245 页 1246 页 1247 页 1248 页 1249 页 1250 页 1251 页 1252 页 1253 页 1254 页 1255 页 1256 页 1257 页 1258 页 1259 页 1260 页 1261 页 1262 页 1263 页 1264 页 1265 页 1266 页 1267 页 1268 页 1269 页 1270 页 1271 页 1272 页 1273 页 1274 页 1275 页 1276 页 1277 页 1278 页 1279 页 1280 页 1281 页 1282 页 1283 页 1284 页 1285 页 1286 页 1287 页 1288 页 1289 页 1290 页 1291 页 1292 页 1293 页 1294 页 1295 页 1296 页 1297 页 1298 页 1299 页 1300 页 1301 页 1302 页 1303 页 1304 页 1305 页 1306 页 1307 页 1308 页 1309 页 1310 页 1311 页 1312 页 1313 页 1314 页 1315 页 1316 页 1317 页 1318 页 1319 页 1320 页 1321 页 1322 页 1323 页 1324 页 1325 页 1326 页 1327 页 1328 页 1329 页 1330 页 1331 页 1332 页 1333 页 1334 页 1335 页 1336 页 1337 页 1338 页 1339 页 1340 页 1341 页 1342 页 1343 页 1344 页 1345 页 1346 页 1347 页 1348 页 1349 页 1350 页 1351 页 1352 页 1353 页 1354 页 1355 页 1356 页 1357 页 1358 页 1359 页 1360 页 1361 页 1362 页 1363 页 1364 页 1365 页 1366 页 1367 页 1368 页 1369 页 1370 页 1371 页 1372 页 1373 页 1374 页 1375 页 1376 页 1377 页 1378 页 1379 页 1380 页 1381 页 1382 页 1383 页 1384 页 1385 页 1386 页 1387 页 1388 页 1389 页 1390 页 1391 页 1392 页 1393 页 1394 页 1395 页 1396 页 1397 页 1398 页 1399 页 1400 页 1401 页 1402 页 1403 页 1404 页 1405 页 1406 页 1407 页 1408 页 1409 页 1410 页 1411 页 1412 页 1413 页 1414 页 1415 页 1416 页 1417 页 1418 页 1419 页 1420 页 1421 页 1422 页 1423 页 1424 页 1425 页 1426 页 1427 页 1428 页 1429 页 1430 页 1431 页 1432 页 1433 页 1434 页 1435 页 1436 页 1437 页 1438 页 1439 页 1440 页 1441 页 1442 页 1443 页 1444 页 1445 页 1446 页 1447 页 1448 页 1449 页 1450 页 1451 页 1452 页 1453 页 1454 页 1455 页 1456 页 1457 页 1458 页 1459 页 1460 页 1461 页 1462 页 1463 页 1464 页 1465 页 1466 页 1467 页 1468 页 1469 页 1470 页 1471 页 1472 页 1473 页 1474 页 1475 页 1476 页 1477 页 1478 页 1479 页 1480 页 1481 页 1482 页 1483 页 1484 页 1485 页 1486 页 1487 页 1488 页 1489 页 1490 页 1491 页 1492 页 1493 页 1494 页 1495 页 1496 页 1497 页 1498 页 1499 页 1500 页 1501 页 1502 页 1503 页 1504 页 1505 页 1506 页 1507 页 1508 页 1509 页 1510 页 1511 页 1512 页 1513 页 1514 页 1515 页 1516 页 1517 页 1518 页 1519 页 1520 页 1521 页 1522 页 1523 页 1524 页 1525 页 1526 页 1527 页 1528 页 1529 页 1530 页 1531 页 1532 页 1533 页 1534 页 1535 页 1536 页 1537 页 1538 页 1539 页 1540 页 1541 页 1542 页 1543 页 1544 页 1545 页 1546 页 1547 页 1548 页 1549 页 1550 页 1551 页 1552 页 1553 页 1554 页 1555 页 1556 页 1557 页 1558 页 1559 页 1560 页 1561 页 1562 页 1563 页 1564 页 1565 页 1566 页 1567 页 1568 页 1569 页 1570 页 1571 页 1572 页 1573 页 1574 页 1575 页 1576 页 1577 页 1578 页 1579 页 1580 页 1581 页 1582 页 1583 页 1584 页 1585 页 1586 页 1587 页 1588 页 1589 页 1590 页 1591 页 1592 页 1593 页 1594 页 1595 页 1596 页 1597 页 1598 页 1599 页 1600 页 1601 页 1602 页 1603 页 1604 页 1605 页 1606 页 1607 页 1608 页 1609 页 1610 页 1611 页 1612 页 1613 页 1614 页 1615 页 1616 页 1617 页 1618 页 1619 页 1620 页 1621 页 1622 页 1623 页 1624 页 1625 页 1626 页 1627 页 1628 页 1629 页 1630 页 1631 页 1632 页 1633 页 1634 页 1635 页 1636 页 1637 页 1638 页 1639 页 1640 页 1641 页 1642 页 1643 页 1644 页 1645 页 1646 页 1647 页 1648 页 1649 页 1650 页 1651 页 1652 页 1653 页 1654 页 1655 页 1656 页 1657 页 1658 页 1659 页 1660 页 1661 页 1662 页 1663 页 1664 页 1665 页 1666 页 1667 页 1668 页 1669 页 1670 页 1671 页 1672 页 1673 页 1674 页 1675 页 1676 页 1677 页 1678 页 1679 页 1680 页 1681 页 1682 页 1683 页 1684 页 1685 页 1686 页 1687 页 1688 页 1689 页 1690 页 1691 页 1692 页 1693 页 1694 页 1695 页 1696 页 1697 页 1698 页 1699 页 1700 页 1701 页 1702 页 1703 页 1704 页 1705 页 1706 页 1707 页 1708 页 1709 页 1710 页 1711 页 1712 页 1713 页 1714 页 1715 页 1716 页 1717 页 1718 页 1719 页 1720 页 1721 页 1722 页 1723 页 1724 页 1725 页 1726 页 1727 页 1728 页 1729 页 1730 页 1731 页 1732 页 1733 页 1734 页 1735 页 1736 页 1737 页 1738 页 1739 页 1740 页 1741 页 1742 页 1743 页 1744 页 1745 页 1746 页 1747 页 1748 页 1749 页 1750 页 1751 页 1752 页 1753 页 1754 页 1755 页 1756 页 1757 页 1758 页 1759 页 1760 页 1761 页 1762 页 1763 页 1764 页 1765 页 1766 页 1767 页 1768 页 1769 页 1770 页 1771 页 1772 页 1773 页 1774 页 1775 页 1776 页 1777 页

(2) 设置策略路由相关的配置项。

- a 选择需要策略的接口。
- b 输入策略优先级。
- c 选择匹配ACL列表，当报文命中ACL并且在ACL中定义为“允许转发”时，会按照策略路由进行转发。

点击 **【新建ACL列表】** 可以新增ACL列表，具体操作参考“7.9 ACL访问列表”章节。

- d 输入下一跳地址。

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。

- e 点击 **添加设置**。

【后续处理】

- 选择接口，在“策略路由列表”中查看生成的策略路由。

策略路由列表 选择策略组匹配接口： Gi0/0 ✕ 删除全部

策略优先级	匹配ACL列表	接口	下一跳地址	操作
2	1		12.2.25.2	编辑 删除

显示: 10 条 共1条 ◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶ 1 确定

- 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。

8.3.4 应用路由

1. 配置应用路由

【应用场景】

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。

i 说明

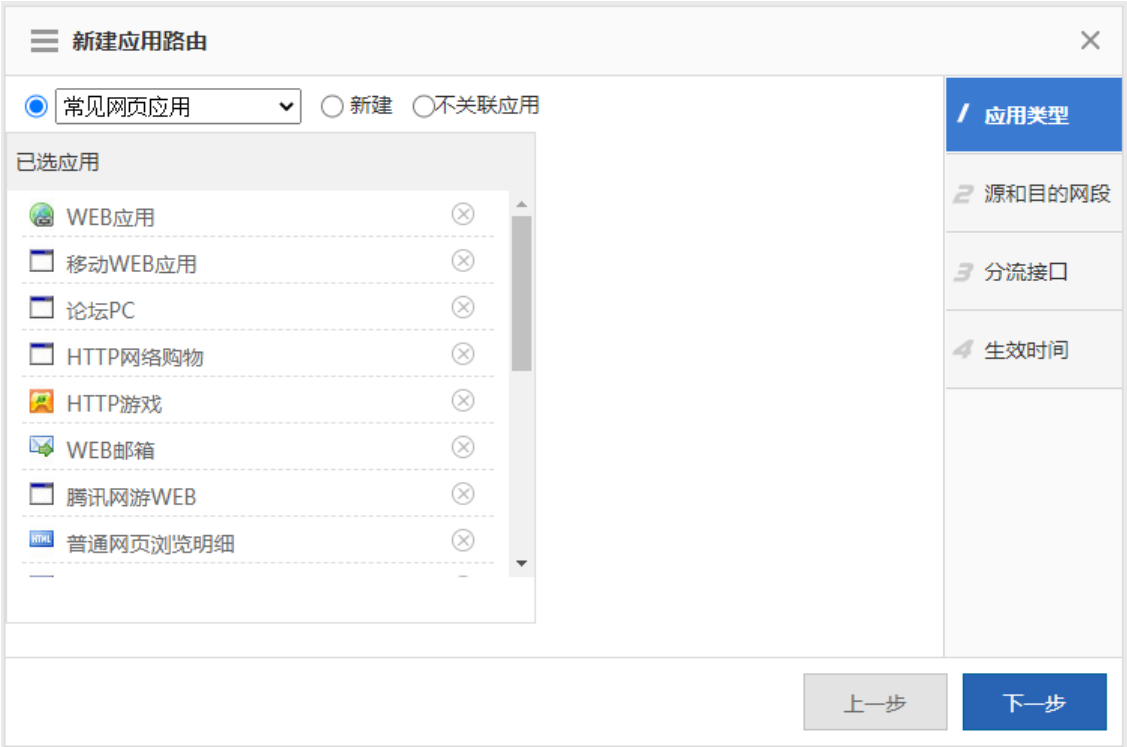
应用路由分流到指定接口后，各应用的流量依然由该指定接口的流控策略来管理。

【操作步骤】

- (1) 点击[网络]>>[路由/负载]>>[应用路由]菜单项。

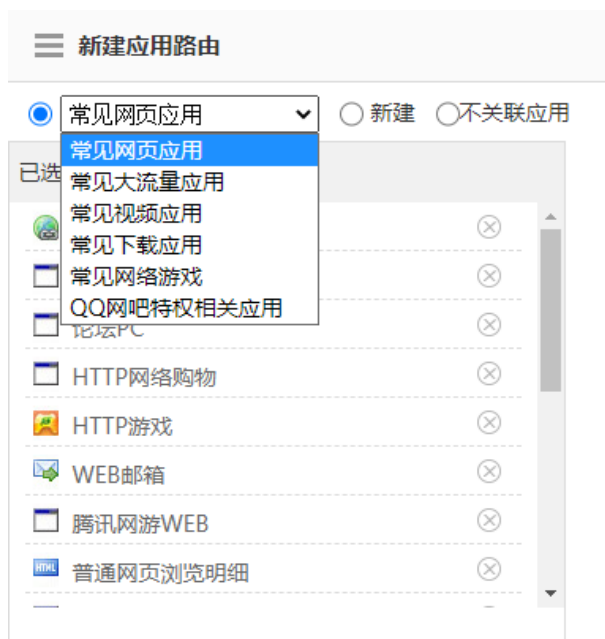


(2) 点击<+新建应用路由>。

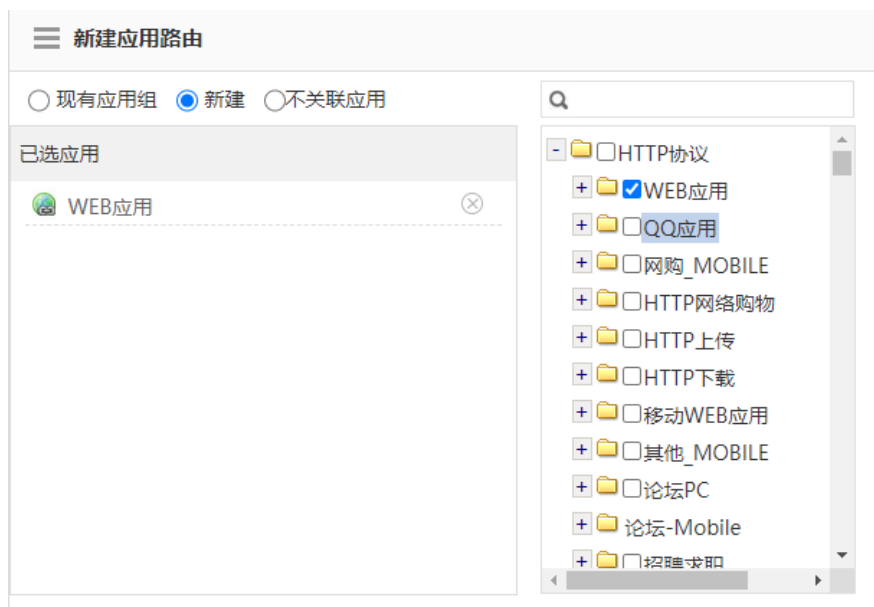


(3) 设置应用路由相关配置项。

- a 选择应用类型，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：
 - o 选择已有的应用分类作为策略关联的应用对象，此时策略将对选中应用分类下的所有应用进行匹配和分流：



- 点击选择“新建”，右侧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**，在应用树上选中多个应用或应用分类，此时左侧下方将出现“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：

说明

选择“现有应用组”，在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，点击 可以将不需要设置的应用从该应用组中删除。

b 设置源和目的网段，点击<下一步>。

应用路由支持指定报文协议、源IP与目的IP网段，以及目的URL组来进行引流。

优先级表示路由表项的匹配优先级，数值越大优先级越高。

源/目的网段可以是单个IP地址、IP地址范围或运营商地址库：

可以选择现有网段，即在下拉框中选择引用[行为管理]>>[对象定义]>>[IP对象]中定义的IP对象（可在当前页面通过点击<现有网段管理>配置）；或是在下拉框中选择运营商；也可以选择“新建”，新建IP网段。

指定源IP网段，如指定为内网的服务器IP地址，可以实现类似策略路由的效果。指定目的IP网段，如指定目的网段为电信地址库，可以实现类似根据地址库选路的效果。指定URL对象，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。

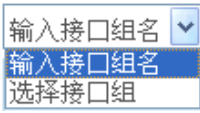
生成静态路由：根据URL路由生成静态路由。建议在需要将URL路由做路由重分发的时候开启，开启该功能后，设备会主动解析URL的域名，并且将解析出来的地址生成静态路由。开启前需要满足如下条件：上一步骤中的应用类型必须选择“不关联应用”；只配置URL路由参数，其他参数均为any；URL对象必须为自定义的。

c 设置分流接口。

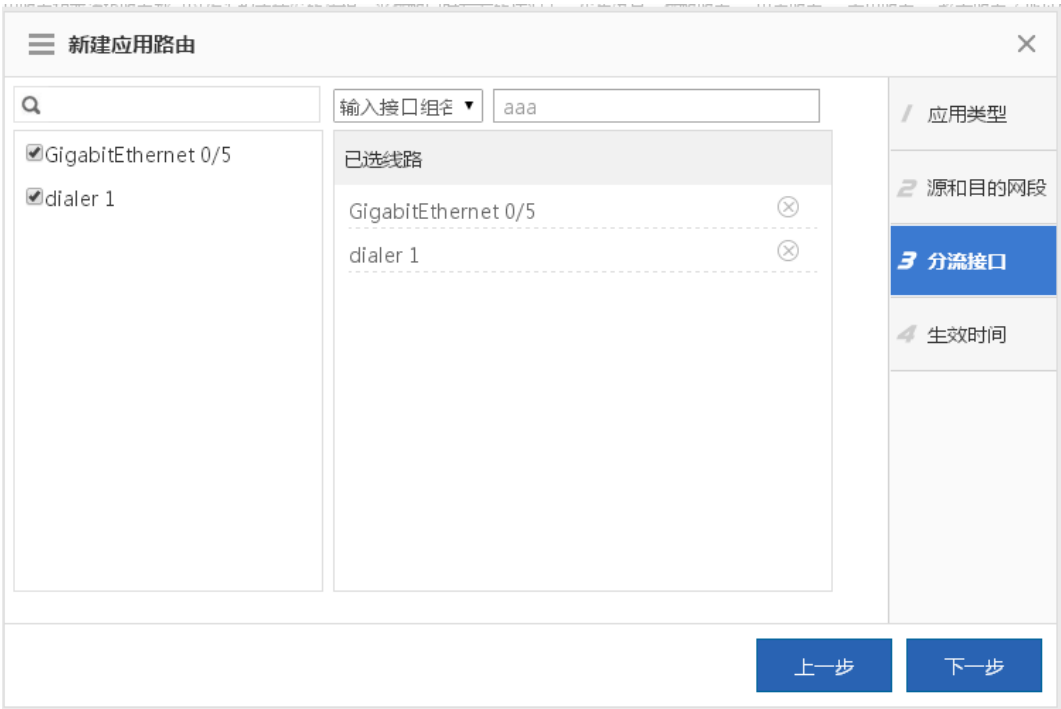
应用路由支持WAN口作为出接口。

接口组是指多个接口的组合。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。应用路由的出口可以指定为单个接口或接口组。

- 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  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：



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。

-  注意
- 不能让所有接口都做应用路由，请至少保留一条稳定线路，不做应用路由（走默认路由）。
 - 动态获取IP的接口，不支持配置应用路由。
 - 请提前确认选择的接口，已在接口配置或快速上网配置中完成基础配置（包括：接口类型，IP地址，下一跳地址等）。

d 设置生效时间。

新建应用路由

生效时间：

所有时间

【时间管理】

应用类型

源和目的网段

分流接口

生效时间

上一步

完成

在生效时间下拉框中列出了系统当前已配置的时间对象，用户可以选择一个合适的时间对象。

若没有满足用户要求的时间段，用户可以点击后面的【时间管理】新建时间对象。

e 点击<完成>。

【后续处理】

- 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：

+ 新建应用路由 + 指定主机走单线路

优先级	协议	源网段/源端口	目的网段/目的端口	应用	目的URL	分流接口名	生效时间	☒ 开启	状态	是否生成静态路由	匹配顺序	管理
1000		移动/	-/	常见网页应用	国外游戏DNS ~sys	Gi0/3	晚上	☒ 开启	未生效	未开启		编辑 删除
显示: 10 条 共1条												
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，各应用路由规则之间存在优先级关系，后配置的优先级高于先配置的。点击  和  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。
- 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:
◀ 首页
◀ 上一页
1
下一页 ▶
末页 ▶

应用类型名	分流接口名/接口组	命中连接数
test	dialer 1	0
P2P应用软件	dialer 1	0
test2	GigabitEthernet 0/6	0

2. 指定 IP 走单线路

【应用场景】

当存在多条外网线路，可以通过本功能实现IP主机从指定的某个线路走，保障关键流量。

【操作步骤】

(1) 点击[网络]>>[路由/负载]>>[应用路由]菜单项。

策略路由

应用路由

普通路由

多链路负载均衡

应用路由：根据数据流的应用类型、源目的IP地址、运营商等属性将流量分到不同的出口线路，从而保障关键应用的体验，并且合理充分利用各条线路的带宽。

注意：应用路由分流配置，建议采用基于大类的方向。由于应用特征的复杂性，避免出现有些应用无法分流或分流不干净的情况，建议配置之后测试下用户体验是否正常，如果不正常则需要调整配置。

url路由生成静态路由说明：该功能建议在需要将url路由做由重分发的时段开启，开启该功能后，设备会主动解析url的域名，并且将解析出来的地址生成静态路由。该功能仅在只配置url路由参数，其他参数均为any的情况下才生效。按照策略优先级，设备仅对至多100条url生成静态路由。该功能不支持接口组。

+新建应用路由

+指定主机走单线路

优先级	协议	源网段/源端口	目的网段/目的端口	应用	目的URL	分流接口名	生效时间	☐ 开启	状态	是否生成静态路由	匹配顺序	管理
显示:	10 ↓	条 共0条										
							1 < 首页 < 上一页 1 下一页 > 末页 >			1 确定		

(2) 点击<+指定主机走单线路>。

指定主机走单线路

优先级: 100 * (1-10000) ?

源网段: ☐ 现有网段 any ☒ 新建

自定义名称:

对象列表: 每个单项格式可为 a.b.c.d 或 a.b.c.d/nn 或 a.b.c.d-e.f.g.h

请选择线路: GigabitEthernet 0/3

确定

取消

(3) 配置路由优先级、主机IP地址（范围）以及出接口，配置完成后，点击<确定>。

8.3.5 普通路由

【应用场景】

普通IP路由使需要到达指定目标网络的数据包的传送，按照预定的路径进行。当设备无法学习到部分目标网络的路由时，配置静态路由就会显得十分重要。另外通常需要给所有没有确切路由的数据包配置一个默认路由。

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。

1. 配置静态路由

(1) 点击[网络]>>[路由/负载]>>[普通路由]菜单项。

应用路由 普通路由 多链路负载均衡 策略路由

路由优先级：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。

普通IP路由：使得得到指定目标网络的数据包的传送，按照预定的路径进行。当设备无法学习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。

+新建静态路由 +新建地址库 +新建默认路由

筛选条件： 全部

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		dialer 1	主路由	编辑 删除
0.0.0.0	0.0.0.0	192.168.23.1	GigabitEthernet 0/5	主路由	编辑 删除

显示: 10 条 共2条

首页

 < 上一页 1 下一页 > 末页

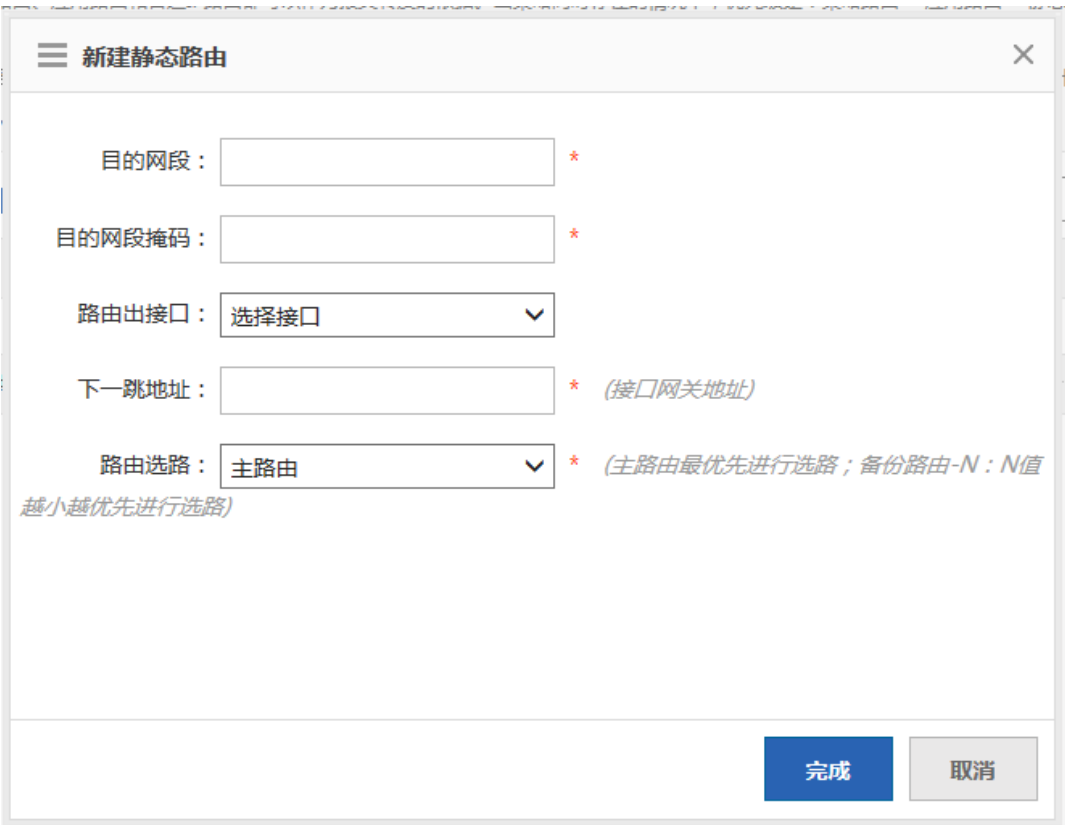
1 确定

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。

 说明

“路由选路”为“10”时，表示该表项为配置应用路由策略时自动生成的默认路由。

(2) 点击  **新建静态路由**。



The dialog box titled "新建静态路由" (New Static Route) contains the following fields and options:

- 目的网段 (Destination Network): Text input field with a red asterisk.
- 目的网段掩码 (Destination Network Mask): Text input field with a red asterisk.
- 路由出接口 (Route Out Interface): Dropdown menu with "选择接口" (Select Interface) and a downward arrow.
- 下一跳地址 (Next Hop Address): Text input field with a red asterisk and the label "(接口网关地址)" (Interface Gateway Address).
- 路由选路 (Route Selection): Dropdown menu with "主路由" (Main Route) and a downward arrow. A red asterisk is next to it, followed by the text "(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)" (Main route is selected first; backup route -N: N value越小越优先进行选路).

At the bottom right, there are two buttons: "完成" (Finish) in a blue box and "取消" (Cancel) in a grey box.

(3) 设置静态路由相关配置项。

- 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。

(4) 点击 。

【后续处理】

- 查看生成的路由。

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	172.18.124.1	GigabitEthernet 0/6	10	<button>删除</button>
12.2.2.2	255.255.255.255	1.2.24.85	GigabitEthernet 0/2	备份路由-5	<button>编辑</button> <button>删除</button>

显示: 10 条 共2条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶ 1 确定

- 点击 删除 可以删除静态路由。

2. 配置默认路由

(1) 点击[网络]>>[路由/负载]>>[普通路由]菜单项。

(2) 点击  **新建默认路由**，弹出以下窗口：

新建默认路由

路由出接口:

选择接口

下一跳地址: * (接口网关地址)

路由选路:

主路由

 * (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)

完成

取消

(3) 选择路由出接口，输入下一跳地址，选择路由选路，点击  即可生成一条默认路由：

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	<button>编辑</button> <button>删除</button>
0.0.0.0	0.0.0.0	172.18.124.1	GigabitEthernet 0/6	10	<button>删除</button>
12.2.2.2	255.255.255.255	1.2.24.85	GigabitEthernet 0/2	备份路由-5	<button>编辑</button> <button>删除</button>

显示: 10 条 共3条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶ 1 确定

【后续处理】

点击  可以删除默认路由。

3. 配置地址库

(1) 点击[网络]>>[路由/负载]>>[普通路由]菜单项。

(2) 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。

8.3.6 多链路负载均衡

【应用场景】

多链路负载均衡是指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。一键开启，无需手动调整策略，便能自动进行合理的流量分配。

说明

多链路负载均衡只生效于普通路由的线路，对策略路由或应用路由线路不起作用。

【操作步骤】

(1) 点击[网络]>>[路由/负载]>>[多链路负载均衡]菜单项。



(2) 勾选“开启多链路负载均衡”。

(3) 点击<保存设置>。

【后续处理】

点击 **[查看负载均衡结果]** 可以查看负载均衡的效果：



8.4 DNS 配置

8.4.1 功能简介

在一个TCP/IP架构的网络环境中，DNS（Domain Name System，域名系统）是一个重要且常用的系统。DNS主要的功能是将易于记忆的域名与不容易记忆的IP地址作转换。通过域名（或主机名）得到对应IP地址的过程叫做域名解析（或主机名解析）。

DNS配置功能包括配置本机DNS服务器和正向DNS代理。

8.4.2 DNS 服务器

【应用场景】

配置设备的DNS服务器地址，当用户使用某些应用进行域名操作时，系统DNS解析器查询外部的DNS服务器，获取到域名对应的IP。

【操作步骤】

(1) 点击[网络]>>[DNS配置]>>[DNS服务器]菜单项。

(2) 设置DNS服务器1的IP地址。

说明

DNS服务器IP支持设置为IPv4或IPv6地址。

(3) （可选）如果需要配置多个服务器，点击  即可配置第二个DNS服务器的地址。

(4) 配置好之后点击  即可。

【配置验证】

以ping www.baidu.com举例说明DNS的服务器配置效果：

- 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。

8.4.3 正向 DNS 代理

【应用场景】

正向DNS代理一般部署于DNS服务器和用户PC中间，代理DNS服务器处理用户的域名解析请求。

【配置步骤】

(1) 点击[网络]>>[DNS配置]>>[正向DNS代理]菜单项。

(2) 选择“基础配置”页签，设置DNS代理基础配置。

DNS服务器 正向DNS代理

基础配置：是“正向DNS代理”功能生效的前提配置，需要实现DNS管控，排除DNS代理，应用路由联动等功能必须先在对应线路配置DNS服务器IP地址；

DNS管控：开启DNS管控后内网客户机可以任意配置DNS，设备将智能做到DNS透明纠错，从而不影响客户机正常上网！您开启了DNS管控后，请记得在接口配置指定线路的“网络服务商”。

排除DNS代理：是设置一些特殊的不需要受正向DNS代理功能影响的资源（包括：IP地址、DNS服务器）。

IP段 格式如：192.168.1.1-192.168.1.150

注意：填写运营商给您的DNS地址，若不确定地址，可直接填写114.114.114.114。

基础配置 排除DNS代理

内网口开启正向DNS代理：☐ Gi0/0 ☐ Gi0/1 ☐ Gi0/2

外网口配置DNS信息：☐ Gi0/3 ☐ Gi0/4

保存设置

DNS代理统计信息

拦截到的所有DNS请求：0

拦截到的所有DNS应答：0

命中DNS黑名单的有：0 命中排除DNS代理的有：0

命中用户路由的有：0 命中负载均衡的有：0

a 勾选需要开启DNS代理功能的内网口。

基础配置 排除DNS代理

内网口开启正向DNS代理：☒ Gi0/0 ☐ Gi0/1 ☐ Gi0/2

外网口配置DNS信息：☐ Gi0/3 ☐ Gi0/4

保存设置

b 勾选连接DNS服务器的外网口，并配置对应线路的DNS服务器地址。

基础配置 排除DNS代理

内网口开启正向DNS代理：☒ Gi0/0 ☐ Gi0/1 ☐ Gi0/2

外网口配置DNS信息：☒ Gi0/3 ☐ Gi0/4

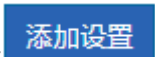
☒ 配置Gi0/3线路 接口上的DNS:

保存设置

- c 点击 。
- d 在下方可以查看到DNS代理的统计信息。

DNS代理统计信息

拦截到的所有DNS请求:	0
拦截到的所有DNS应答:	0
命中DNS黑名单的有:	0
命中排除DNS代理的有:	0
命中用户路由的有:	0
命中负载均衡的有:	0

- (3) 选择“排除DNS代理”页签，设置排除DNS代理相关配置项。
- 排除DNS代理功能用于设置一些特殊的不需要受DNS代理功能影响的资源（包括：IP地址、DNS服务器）。
- 选择资源类型为“IP或IP段”或“DNS服务器”，在输入框输入对应IP地址，点击 。
- 配置将在下方表格中显示。

DNS服务器

正向DNS代理

基础配置：是“正向DNS代理”功能生效的前提配置，需要实现DNS管控，排除DNS代理，应用路由联动等功能必须先在该对应线路配置DNS服务器IP地址；

DNS管控：开启DNS管控后内网客户机可以任意配置DNS，设备将智能做到DNS透明纠错，从而不影响客户机正常上网！您开启了DNS管控后，请记得在接口配置指定线路的‘网络服务商’。

排除DNS代理：是设置一些特殊的不需要受正向DNS代理功能影响的资源（包括：IP地址、DNS服务器）。

IP段 格式如：192.168.1.1-192.168.1.150

注意：填写运营商给您的DNS地址，若不确定地址，可直接填写114.114.114.114。

基础配置

排除DNS代理

选择类型：

IP或IP段

*

指定IP或IP段：

*

添加设置

类型	排除DNS代理资源	管理
显示: 10	条共0条	1 确定

8.5 VPN 配置

8.5.1 功能简介

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。

 注意

开启VPN功能后如需使用Telnet管理，需要在[运维]>>[系统设置]>>[修改密码]页面重新配置Telnet密码。

8.5.2 配置 VPN 服务端（总部）

【应用场景】

在企业总部部署VPN服务器，使出差员工和分支机构能够接入到总部VPN，访问总部内网资源，实现公司信息平台、资源、数据的共享。

【操作步骤】

(1) 选择[网络]>>[VPN配置]。

(2) 首次配置VPN，配置页面如下图所示。选择“我在总部”，点击<开始配置>，使用配置向导快速完成配置。



(3) 在配置向导页面中，点击选择VPN需求，向导将根据需求推荐VPN类型。在下方“使用VPN类型”中勾选要配置的VPN类型，点击<下一步>。VPN配置向导将根据选择的VPN类型自动生成相应配置步骤，首次配置只需根据向导指示逐步操作即可完成配置。

VPN配置向导

VPN类型选择 → 配置基本信息 → 管理用户帐户 → 配置L2TP IPsec → 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

(4) 进入“配置基本信息”页面，配置PPTP或L2TP VPN总部相关参数。若仅配置IPsec VPN，则跳过此步骤。

VPN配置向导

VPN类型选择 → 配置基本信息 → 管理用户帐户 → 配置L2TP IPsec → 完成

配置移动用户或分支机构连接进来的基本信息

客户端地址范围： ~ *

给移动用户(分支机构)分配的IP地址范围配置
前请确保这些地址未被您局域网中的其它地方使用

总部域名：

首选DNS服务器：

备选DNS服务器：

如果移动用户需要通过域名来访问本局域网中的系统请配置DNS服务器地址这个地址一般和您局域网中使用的DNS服务器一致

上一步

下一步

客户端地址范围：给VPN客户端分配的隧道IP，IP地址个数即为允许接入的VPN客户端数量。

总部域名：配置后VPN客户端可通过域名来访问总部内网。

DNS服务器：如果VPN客户端需要通过域名来访问总部局域网中的系统，则需要配置DNS服务器地址，该地址一般和总部局域网中使用的DNS服务器地址是一致的。

填写完基本信息后，点击<下一步>按钮，进入下一个配置页面。

(5) 进入“管理用户帐户”配置页面，管理员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。对于连接用户，可以选择“帐户存储在本设备”或者“已经有其它帐户管理系统”。若仅配置IPSec VPN，则跳过此步骤。

- 选择“帐户存储在本设备”，表格中列出了本设备已配置的用户名和密码信息，用户可以通过表格“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： **新建** 中新增用户名和密码。

VPN配置向导

VPN类型选择

→

配置基本信息

→

管理用户帐户

→

配置L2TP IPSec

→

完成

管理连接进来的用户帐户

● 帐户存储在本设备

● 已经有其它帐户管理系统 ?

添加分支机构

用户名：

密码：

添加

类型	用户名	操作
	aa	编辑 删除

显示: 10

条 共1条

首页

上一页

1

下一页

末页

1

确定

上一步

下一步

- 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。选择“已经有其它账户管理系统”之后，点击 **【管理认证服务器】**，在弹出的页面中共享密码和服务器IP即可。

VPN配置向导

VPN类型选择 → 配置基本信息 → 管理用户帐户 → 配置L2TP IPsec → 完成

管理连接进来的用户帐户

☐ 帐户存储在本设备

☒ 已经有其它帐户管理系统 ?

帐户管理系统，必须是支持AAA的Radius认证服务器，如锐捷网络的SAM、SMP等

【管理认证服务器】

上一步

下一步

(6) L2TP IPsec即L2TP over IPsec，为L2TP和IPsec协议的结合。选择IPsec或L2TP IPsec协议类型的VPN总部，接下来还需要配置IPsec相关参数。

○ 设置L2TP IPsec VPN参数：

VPN配置向导

VPN类型选择 → 配置基本信息 → 管理用户帐户 → 配置L2TP IPsec → 完成

配置L2TP IPsec参数

预共享密钥：

*

?

确认预共享密钥：

*

总部本机ID ?：

☐ 勾选开启 ?

上一步

下一步

预共享密钥：移动用户和分支机构必须输入正确的密钥才能成功拨入。

总部本机ID：勾选开启后需要设置总部ID。如果分支是通过域名连接总部，则总部必须配置总部本机ID。总部开启本功能后，分支在连接总部时必须输入总部ID，即分支设备的“对端ID”必须和本设备的“本机ID”一致，否则将连接失败。

○ 设置IPSec VPN参数：

VPN配置向导

VPN类型选择 → 配置基本信息 → 管理用户帐户 → 配置IPSec → 完成

配置IPSec参数

预共享密钥：

*

?

确认预共享密钥：

*

总部本机ID

?

：☐ 勾选开启

?

需经隧道访问的网络 配置指导

本地网段		分支机构网段		出口	
192.168.3.0	255.255.255.0	IP	掩码	请选择出口	+ ×

IKE策略：加密算法

DES

 散列算法

SHA

 DH组

group1

 生命周期

86400

?

上一步

下一步

预共享密钥：移动用户和分支机构必须输入正确的密钥才能成功拨入。

总部本机ID：勾选开启后需要设置总部ID。如果分支是通过域名连接总部的，则总部必须配置总部本机ID。总部开启本功能后，分支在连接总部时必须输入总部ID，即分支设备的“对端ID”必须和本设备的“本机ID”一致，否则将连接失败。

需经隧道访问的网络：在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。

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。

完美向前加密：设置IPsec隧道封装的使用Diffie-Hellman组标识，group1、group2和group5分别为768比特、1024比特和1536比特的Diffie-Hellman组。可以选择“不启用”。

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。

DPD探测类型和探测周期：目前DPD实现上采用了两种机制：

on-demand机制：有流量的情况才探测，在隧道闲置时间超过探测周期后，如果有报文发送，会触发发送DPD探测消息。

periodic机制：周期性探测，在超过探测周期后就会主动发送DPD探测消息。

on-demand机制可以减少额外开销，periodic机制时间反应较快，需要根据实际网络情况选择使用。

(7) 完成各种协议类型的VPN参数配置后，点击<下一步>完成配置。下图为“总部配置完成”页面。

VPN配置向导

VPN类型选择 → 配置IPSec → 完成

总部端配置成功

接下来建议您进行：

对端设备配置：

对端设备
可根据本端配置参数进行对端设备配置

配置指南

终端接入：

WINXP
本端当前配置支持 WINXP 系统

接入指南

IOS/安卓
本端当前配置支持 IOS/安卓 系统

接入指南

WIN7/WIN10
本端当前配置支持 WIN7/WIN10 系统

接入指南

一键下载所有接入指南

上一步

完成

点击下方的“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，查看并记录客户端（分支）所需的对应配置。

点击终端设备的“接入指南”，可以查看各类型的终端连接到本总部VPN服务器的操作步骤。

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			

【后续处理】

241

(1) 回到[VPN配置]页面，显示“(本机)”字样的图标表示当前正在配置的总部设备，点击图标可以查看和修改当前VPN配置。

i 说明

- 配置向导包含VPN总部的必要功能配置，根据向导完成配置后当前设备已经可以作为VPN总部服务器正常工作。如需配置更多功能，可按照当前步骤进行后续操作。
- 修改总部配置后，分支配置也应同步修改，否则可能导致VPN连接失败。

分支机构信息



☰ 本机VPN配置信息

✕

基本参数

修改配置清空配置

启用的VPN类型：☐ PPTP ☐ L2TP ☐ IPSec ☒ L2TP IPSec

客户端地址范围： 至 *

总部域名：

首选DNS服务器： 备选DNS服务器：

本机隧道IP： * 本机隧道掩码： *

其它帐户管理系统：☐ 开启

L2TP隧道超时检测： 秒

L2TP隧道认证方式：☐ 开启

取消

(2) 点击<修改配置>，可修改在配置向导中已配置的参数，并在配置向导基础上配置更多VPN参数。

 说明

对于L2TP over IPSec类型的VPN，除配置向导中设置的“预共享密钥”与“是否开启总部本机ID”外，还可按照当前步骤设置更多IPSec加密参数，具体参数说明请参考“[设置IPSec VPN参数](#)”。

对于在配置向导中已配置的参数，可参见相关步骤说明，这里不再赘述。下面介绍可配置的其他参数：

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：检测PPTP隧道的时间间隔。超过该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的时间间隔。超过该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隧道验证密码功能处于关闭状态，L2TP隧道的建立不要求通道验证；如果开启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，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，然后在当前页面勾选 ☒ 开启 后，并填写下方表格。

☒ 开启 

允许总部访问分支内网：

分支机构隧道IP	分支机构网段		+
IP	IP	掩码	×

鼠标移至  按钮时，将显示配置指导信息，可根据该信息进行规划配置：

配置指导

1、开启本功能前，需事先规划好全网网段以及分配给各分支机构的隧道IP，并在分支机构设备上相应开启“允许总部访问分支内网”功能。

2、下表中的“分支隧道IP”推荐从“客户端地址范围”的末尾IP开始规划配置，如客户端地址范围是192.168.3.2 ~ 192.168.3.254，那么这里就从192.168.3.254开始依次向下规划配置！

注意：如果一个分支机构有多个内网网段，请按以下格式填写

分支机构隧道IP	分支机构网段		+
192.168.3.254	172.18.102.0	255.255.255.0	×
192.168.3.254	172.18.103.0	255.255.255.0	×

8.5.3 配置 VPN 客户端（分支机构）

【操作步骤】

- (1) 选择[网络]>>[VPN配置]。
- (2) 首次配置VPN，配置页面如下图所示。选择“我在分支机构”，点击<开始配置>，使用配置向导快速完成配置。



- (3) 根据总部的VPN配置，勾选与总部相同的VPN类型，点击<下一步>。



- (4) 在当前页面输入总部管理员提供的VPN参数，配置分支机构作为VPN客户端向服务端发起连接请求。

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服务器保持一致，可向总部VPN服务器管理员获取。

用户名、密码：用于身份验证的用户名和密码，由VPN服务端配置和提供。

总部网络：分支机构需要访问的总部的内网网段。

身份验证：选择IPSec或L2TP IPSec协议时的可选配置，默认关闭。开启后，可使总部获知分支机构名称，便于VPN管理。但开启身份验证后总部的“本机ID”必须和本设备的“对端ID”一致，否则可能连接失败。

心跳(Hello)报文发送周期：设置Hello消息发送间隔，以定时检测L2TP通道是否依然可用。

本机隧道IP：本机与远程服务端通过PPTP或L2TP协议建立起VPN隧道时本机使用的隧道IP，默认由服务端自动分配。开启“手动配置”后，可手动指定一个在服务端的地址池范围内的隧道IP。

说明

若开启“允许总部访问分支内网”功能，则必须手动配置本机隧道IP为服务端规划分配的IP，详见“[允许总部访问分支内网（服务端配置）](#)”。

IKE策略、转换集、完美向前加密、IPSec隧道生命周期、DPD探测功能、是否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。各配置项的详细介绍可参考[8.5.2](#) 章节。

注意

如果勾选了 **允许总部访问分支内网**：☐ **开启（总部需同时开启才能生效）**，分支机构访问互联网的流量会全部走VPN，再通过总部连接到外网；如果不勾选的话，只有当访问总部内网网段时才走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。

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

(5) 完成参数设置后，点击<下一步>按钮，向总部发起连接请求。

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>可检测VPN隧道是否成功建立，VPN线路是否联通。等待一段时间后就会有连接成功或失败的提示信息。等待提示连接成功之后，点击下方的<完成>按钮，完成分支机构的VPN配置。

VPN配置向导

VPN类型选择 → 分支机构配置 → 连接总部

正在连接中.....

上一步

完成

8.5.4 VPN 配置

1. 拓扑图显示页面

完成VPN配置后，[VPN配置]页面将以拓扑形式显示当前VPN连接状态。



通过拓扑图可以了解本机当前在VPN网络环境中的位置，其中显示“(本机)”字样的设备



表示当前正在配置的设备。点击此图标可以查看和修改本机的VPN配置信息。

拓扑图中灰色设备表示未连接的用户或设备，灰色线条表示未成功建立连接的VPN通道，灰色设备表示未连接的用户或设备，蓝色设备和蓝色线条表示连接成功的VPN设备和通道。



添加接入总部

位于本机上方的设备，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VPN总部中；可以多次配置，使本机同时接入多个VPN总部。最多允许接入9个VPN总部。详细配置步骤请参见[8.5.3 配置VPN客户端（分支机构）](#)章节。

位于本机下方的设备，表示本机作为VPN总部时，与本机连接的分支设备或用户帐户。若本机为L2TP或L2TP



添加分支机构

IPSec VPN总部时，拓扑图左上角将会有添加分支机构图标，点击此图标可新增一个帐户。



让分支接入总部

若当前设备只配置作为VPN分支机构，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[8.5.2 配置VPN服务端（总部）](#)章节。

分支机构信息



2. 表格显示页面

点击“表格”页签，切换至表格形式的配置页面。



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，可以新增用于VPN验证的用户帐号。

点击表格“操作”列中的 [查看](#) [修改](#) [删除](#) ，可以分别对选中的用户帐户进行查看、修改和删除。

3. 查看本机的 VPN 配置信息

在拓扑图页面点击本机设备图标，或在表格页面点击“管理本机配置”可以查看本机的VPN配置信息，如下图所示：

本机VPN配置信息

查看作为总部的配置

查看作为分支的配置

基本参数

修改配置

清空配置

启用的VPN类型：☐ PPTP ☐ L2TP ☐ IPSec ☒ L2TP IPSec

客户端地址范围： 至 *

总部域名：

首选DNS服务器： 备选DNS服务器：

本机隧道IP： * 本机隧道掩码： *

其它帐户管理系统：☐ 开启

取消

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，将切换到显示本机作为VPN分支机构的配置信息，如下图所示：

本机VPN配置信息

查看作为总部的配置

查看作为分支的配置

VPN参数

修改配置

清空配置

VPN类型：

L2TP IPSec

☐ 开启身份验证 ?

总部公网IP或域名： * +多个IP或域名

预共享密钥： * IPSec隧道生命周期： 秒

用户名： * 密码： *

总部网络： -

取消

若本机作为VPN分支机构，接入到多个总部，VPN参数上方将多个选项卡。例如

接入总部1 **接入总部2** 表示当前显示的是接入到总部1的VPN分支配置信息，点击 **接入总部2** 将会显示本机接入到总部2的VPN分支配置信息。

点击 **修改配置** 按钮，可以对当前VPN配置进行修改，如下图所示。

本机VPN配置信息

查看作为总部的配置

查看作为分支的配置

接入总部1

接入总部2

VPN参数

修改配置

清空配置

VPN类型：

L2TP IPSec

☐ 开启身份验证 ?

总部公网IP或域名：

192.168.23.171

 * +多个IP或域名

预共享密钥：

.....

 *

IPSec隧道生命周期：

3600

 秒

用户名：

123

 *

密码：

...

 *

保存

取消

修改完成后，点击 **保存** 保存配置。

点击 **清空配置** 按钮可以清空当前VPN配置并断开VPN连接。例如当前清空了本机作为分支机构接入总部2的配置，则本机将与总部2断开连接。

4. 查看移动用户信息

本机配置作为VPN总部时，管理员可以在VPN监控页面看到终端用户的接入信息，如下图所示：

移动用户信息

当前共 有0个移动用户接入专网。点击 [这里](#) 管理移动用户。

点击 [这里](#) 将弹出移动用户管理页面，可以在此页面查看、修改或删除某个移动用户信息；点击 **【用户组织管理】** 可以对VPN用户的组织结构、所属用户组进行管理。

移动用户管理

×

【用户组织管理】

接入筛选: 查询

当前共 有1个移动用户接入专网

用户名	是否接入	接入时间	内网IP	互联网IP	操作
NA		1970-01-01 05:56:19	192.168.12.1	192.168.23.171	查看

显示: 条 共1条

◀ 首页
◀ 上一页
1
下一页 ▶
末页 ▶▶

确定

取消

8.6 SSLVPN 配置

8.6.1 功能介绍

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。

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提供细粒度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、安全隧道接入和点对点接入。

- **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。
- **点对点接入**：将带SSLVPN功能的设备当作接入客户端（称为分支）连接到SSLVPN服务器（称为总部），由分支与总部建立安全隧道；与分支连接的局域网内所有终端用户登录成功后，都能通过该安全隧道安全地与总部或其它分支进行通信。

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。

SSLVPN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。

注意

开启SSLVPN功能后如需使用Telnet管理，需要在[运维]>>[系统设置]>>[修改密码]页面重新配置Telnet密码。

8.6.2 配置向导

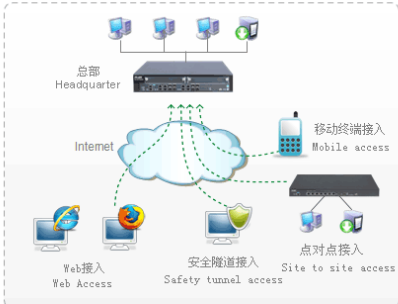
【应用场景】

当设备从未配置过SSLVPN时，可以使用配置向导快速完成配置。

【操作步骤】

(1) 点击[网络]>>[SSLVPN]，进入SSLVPN配置向导页面。

SSLVPN配置



总部 Headquarter

Internet

Web接入 Web Access

安全隧道接入 Safety tunnel access

移动终端接入 Mobile access

点对点接入 Site to site access

什么是SSLVPN?

一项新兴的安全远程访问技术

SSLVPN是Secure Sockets Layer Virtual Private Network（安全套接字层虚拟专用网络）的缩写，是一项新兴的安全远程访问技术。SSL是一个成熟的安全协议，在所有WEB浏览器上均可支持，同时WEB浏览器又是操作系统预装软件之一，从而使得SSLVPN可以真正实现零客户端的安全接入。

WEB接入

不需要安装任何客户端软件就能够直接访问内网基于WEB的应用，包括手机、平板、PC等终端使用浏览器接入。

安全隧道接入

安全隧道接入实现远程主机与内网服务器在网络层之上的安全通信，实现了远程主机与内网服务器之间所有基于IP的互通。SSLVPN登录成功后，用户可以像在办公室一样使用内网资源。

Site to Site接入

将带SSLVPN功能的设备当作接入客户端（称为分支）连接到SSLVPN服务器（称为总部），由分支与总部建立安全隧道；与分支连接的局域网内所有终端都能通过该安全隧道安全地与总部或其它分支进行通信。

开始配置

(2) 点击<开始配置>，弹出SSLVPN配置向导窗口，如下图所示。

欢迎使用SSLVPN配置向导，本向导将帮您快速完成SSLVPN设置。

典型应用

1.支持web接入；
2.支持移动终端接入；
3.支持普通pc安全隧道接入。

典型应用 + 点对点应用

1.支持web接入；
2.支持移动终端接入；
3.支持普通pc安全隧道接入。
4.支持其它SSLVPN设备作为分支接入。

总部

部署模式

基本设置

添加资源

为用户授权资源

完成

上一步

下一步

(3) 选择SSLVPN的部署模式。“典型应用”支持Web接入、移动终端接入和普通PC安全隧道接入；在“典型应用”基础上还可增加“点对点应用”，使设备能够作为VPN总部接受其他SSLVPN设备接入，或是作为VPN分支接入SSLVPN总部。可选的点对点应用模式如下：

- 总部：设备作为SSLVPN服务器，支持其他SSLVPN设备作为分支接入，共享内网资源。
- 分支：设备作为SSLVPN客户端（分支），能够接入总部的SSLVPN服务器，访问授权资源。
- 既是总部又是分支：设备能够同时作为SSLVPN服务器和客户端，既接入其他SSLVPN服务器，又接受其他SSLVPN设备的接入。
- 仅做分支，不允许普通PC接入：设备仅作为SSLVPN客户端，接入其他SSLVPN服务器，访问资源，但不接受其他终端的接入，不允许非内网设备访问内网资源。

下面以“典型应用+点对点应用：既是总部又是分支”模式为例对配置步骤进行说明，不同部署模式的配置步骤不同，可根据实际情况忽略不涉及的配置步骤。

欢迎使用SSLVPN配置向导，本向导将帮您快速完成SSLVPN设置。

☐ 典型应用

1.支持web接入;
2.支持移动终端接入;
3.支持普通pc安全隧道接入。

☒ 典型应用 + 点对点应用

1.支持web接入;
2.支持移动终端接入;
3.支持普通pc安全隧道接入。
4.支持其它SSLVPN设备作为

总部
总部
分支
既是总部又是分支
仅做分支，不允许普通PC接入

1 部署模式
2 基本设置
3 添加资源
4 为用户授权资源
5 点对点配置
6 完成

上一步 下一步

(4) 点击<下一步>，设置基本配置相关配置项。

三

欢迎使用SSLVPN配置向导，本向导将帮您快速完成SSLVPN设置。

×

SSLVPN服务端口：

443

*

(1-65535)

如果设备不是部署在出口，请在出口设备配置TCP及UDP的端口映射。

内网DNS：

114.114.114.114

*

?

用户认证方式：

☒

本地认证

☐

Radius认证

☐

优先本地认证

【添加本地认证用户】

本地认证 使用本设备用户组织结构中的用户名和密码进行认证。

Radius认证 使用第三方的RADIUS服务器认证。

优先本地认证 优先使用本设备用户组织结构中的用户名和密码进行认证，若查找不到用户名时，通过Radius服务器认证。

部署模式

2 基本设置

3 添加资源

4 为用户授权资源

5 点对点配置

6 完成

上一步

下一步

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。

内网DNS：用于解析内部域名，存在域名资源时必须配置。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[安全认证]>>[用户组组织]>>[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；优先本地认证是指优先使用本地用户进行身份认证，若查找不到用户名，再通过Radius服务器进行认证。

Radius服务器管理：当选择“用户认证方式”为“Radius认证”时，可以对使用的第三方Radius服务器进行管理。点击<管理认证服务器>，Radius的配置界面如下图所示。填写认证服务器的IP和密码，以及认证端口，点击<保存设置>即可。支持点击<添加>添加多个备用服务器。

说明：在设备转换网关或旁网桥模式时，需要重新配置认证服务器才能生效；如果WEB认证模块、VPN或SSLVPN模块开启了Radius认证，那将共用此认证服务器列表。

提示：如果认证端口设置为0，则该主机不进行身份认证，同样接口端如果设置为0，则该主机不进行计费。

注意：主备规则（先主后备），当主服务器不可达时，会使用备用服务器中第一个可达的服务器进行认证，探测用户名需到服务器上注册，密码默认为“rujie”，开启无感知认证和逃生后，探测用户时必须，有多台认证服务器时，将共用共享密码，超时时间和重传次数。对接锐捷smp作为portal，如radius服务器超时时间建议配置2秒，重传次数3次。对接锐捷portal服务器超时时间为2s，重传次数1次。

共享密码:

*

(有多台认证服务器时, 将用此密码)

超时时间:

(1-1000, 单位: 秒)

重传次数:

(0-100)

服务器IP:

*

认证端口:

(0-65535)

计费端口:

(0-65535)

探测用户名:

?

+

添加

保存设置

清空配置

(5) 配置SSLVPN的基本参数后，点击<下一步>进入[添加资源]配置。本页面用于配置分配给用户的资源，用户接入成功后可以使用这些资源。

三 欢迎使用SSLVPN配置向导，本向导将帮您快速完成SSLVPN设置。

配置隧道接入资源 ?

客户端网段: 子网 / 掩码 * + 1

分配给隧道接入用户的IP地址网段，配置前请确认这些地址未在您局域网中的其它地方使用。

DNS查询优先级: ☒ 内网DNS优先 ☐ 客户端DNS优先

用于隧道接入时指定优先查询的DNS，只对未授予“所有网络”隧道资源的用户生效。

新建隧道资源: + 添加 2

部署模式

基本设置

3 添加资源

4 为用户授权资源

5 完成

上一步

下一步 3

客户端网段：分配给隧道接入用户的IP地址网段，配置前请确认这些地址未在局域网中的其它地方使用。

DNS查询优先级：用于隧道接入时指定优先查询的DNS，可指定优先使用服务端内网的DNS服务器地址，或是优先使用客户端自身的DNS服务器地址。只对未授予“所有网络”隧道资源的用户生效。

新建隧道资源：

- a 点击<+添加>，进入隧道资源配置页面，添加可授权用户使用的资源，包括IP、网段或域名。

三 新建隧道接入资源

隧道资源名称: *

访问控制规则: + 添加

域名/网段/IP	协议类型	起始端口	结束端口	操作
>> 隧道资源高级设置 ?				

保存

取消

- b 输入隧道资源的名称，用于标识资源。
- c 点击<+添加>，添加可访问资源的匹配规则。选择匹配的目标类型（IP/网段/域名），并输入相应参数。在“高级选项”中还可以配置匹配协议和端口号。



新建访问控制规则

目标类型: IP

单IP: *

注意: IP地址不允许为组播、广播、本地环回地址

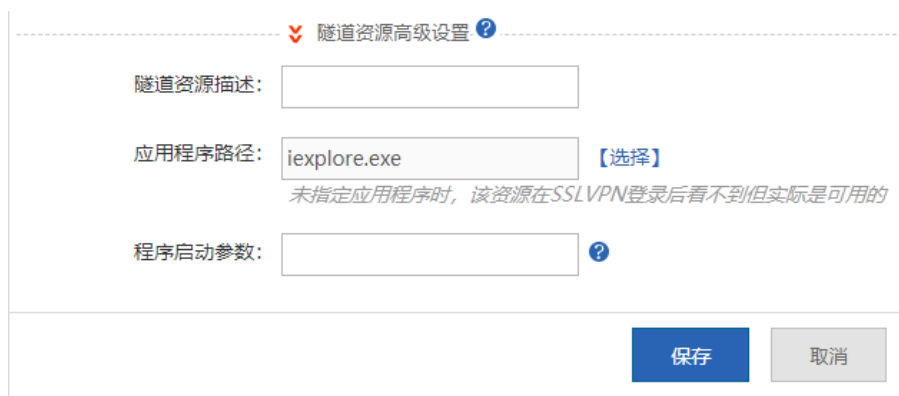
高级选项

协议: ANY

端口: 1 - 65535 (1-65535)

继续添加 保存 取消

- d 点击<保存>完成访问控制规则配置。回到[新建隧道接入资源]页面，点击“隧道资源高级设置”可为隧道资源添加描述，并设置访问资源的应用路径，例如“IE浏览器”、“远程桌面”、“文件共享”或自定义其他应用。未指定应用程序时，该资源在SSLVPN登录后看不到但实际是可用的。最后点击<保存>完成隧道资源设置。



隧道资源高级设置 ?

隧道资源描述:

应用程序路径: iexplore.exe [选择]

未指定应用程序时，该资源在SSLVPN登录后看不到但实际是可用的

程序启动参数: ?

保存 取消

(6) 添加资源后，点击<下一步>进行用户授权。

说明

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配置。为了防止用户误操作，如果想彻底关闭SSLVPN服务，请在CLI下的配置模式下执行：no sslvpn gateway sslvpn 或在SSLVPN配置完成后到基本设置页面的高级选项里勾选关闭服务。彻底关闭SSLVPN服务后会删除掉所有的资源以及用户授权信息。

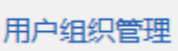
只有授权的用户才可以访问SSLVPN提供的服务。用户授权的界面如下图所示。详细功能介绍可参考[8.6.7](#) 章节。



具体授权步骤如下：



- a 选中要授权的用户或用户组。
- b 点击  将弹出未授权的资源列表。
- c 勾选要授权的资源，这里只列出未授权的资源。

- d 点击  完成对用户（组）新增资源。
- e 要取消资源授权，请点击 。
- f 如果要管理用户请点击 ，会弹出用户管理窗口。

(7) 授权完成，点击<下一步>进入点对点配置页面。

欢迎使用SSLVPN配置向导，本向导将帮您快速完成SSLVPN设置。

Site to Site接入方式： 将带SSLVPN功能的设备当作接入客户端（称为分支）连接到SSLVPN服务器（称为总部），由分支与总部建立安全隧道；与分支连接的局域网内所有终端都能通过该安全隧道安全的与总部或其它分支进行通信。

总部配置

添加分支
 批量添加资源
 管理访问资源
 删除选中

☐	分支用户	分支网段	允许访问的资源	是否禁用	连接状态	操作
显示: 10 条 共0条 1						

分支配置

用户名: *

密码: *

部署模式

基本设置

添加资源

为用户授权资源

点对点配置

完成

点对点配置分为总部配置和分支配置，根据SSLVPN部署模式提供相应配置项。

【总部配置】

总部配置

添加分支
 批量添加资源
 管理访问资源
 删除选中

☐	分支用户	分支网段	允许访问的资源	是否禁用	连接状态	操作
显示: 10 条 共0条 1						

- 点击 添加分支，添加分支的接入信息。完成设置后点击<保存>。

分支名称：接入分支的名称，即登录用户名，不能与本地用户或Radius用户的名称重复。

登录密码：分支内终端连接SSLVPN时需要验证的密码。

分支网段：分配给分支终端的IP网段，不能与服务端内网网段重合。

访问的资源：勾选允许分支终端访问的内网资源。

 说明

访问资源中存在域名资源时，请将分支内PC的首选DNS设置为SSLVPN的内网DNS地址。

新增分支

×

分支名称:

*

与本地用户或Radius用户不能相同

登录密码:

*

分支网段:

*

+

请使用尚未在您网络部署的局域网网段

访问的资源:

存在域名资源时, 请将分支内PC的首选DNS设置为SSLVPN的内网DNS地址

☐ 全选

☐ ★ 局域网

- 勾选列表中已添加的分支表项，点击 **批量添加资源**，可对多个分支批量授权可访问的资源。

总部配置

[+ 添加分支](#) [+ 批量添加资源](#) [⚙ 管理访问资源](#) [✕ 删除选中](#)

☒	分支用户	分支网段	允许访问的资源	是否禁用	连接状态	操作
☒	testxxx	192.168.11.0/255.255.255.0	局域网	已启用 禁用	未连接	删除

显示: 10 条 共1条
 ◀ 首页
◀ 上一页
1
下一页 ▶
末页 ▶
1
确定

- 点击  **管理访问资源** 可对隧道资源进行管理，详见[8.6.6](#) 章节。
- 勾选列表中已添加的分支表项，点击  **删除选中** ，可以批量删除分支信息。
- 点击  **禁用** ，可以一键禁用对应分支。点击  **开启** ，可以重新启用分支。

【分支配置】

分支配置

用户名:		*
密码:		*
服务器:	IP ▼	端口: (范围1-65535) +

- **用户名和密码**：输入总部设置的验证用户名和密码。
- **服务器**：输入需要连接的SSLVPN服务器的IP地址或域名以及端口号。点击+可添加多个服务器作为备份。

(8) 点击<下一步>完成SSLVPN配置



8.6.3 运行状态

【应用场景】

当设备已启动SSLVPN服务，可以查看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。

【操作步骤】

点击[网络]>>[SSLVPN]>>[运行状态]进入页面：

- 当SSLVPN服务暂停时：



SSLVPN服务暂停时，除了Site to Site配置中的允许设备作为分支接入总部外，其他SSLVPN功能均会失效。可以点击 [启动服务](#) 重新启动SSLVPN服务，恢复正常使用。

- SSLVPN服务正常时：

运行状态

基本设置

短信策略管理

隧道资源管理

用户授权

Site to Site管理

用户状态查询： [查找](#) | [硬件特征码管理](#) | [查看日志](#)

当前在线用户：[刷新](#)

用户名	登录IP	登录时间	在线时长	上行流量：	下行流量：	操作
显示: 8 条 共0条 首页 上一页 1 下一页 末页 1 确定						

作为Site to Site总部：接入的分支列表（共0个分支在线）[刷新](#)

用户名	登录IP	登录时间	在线时长	上行流量：	下行流量：	操作
显示: 8 条 共0条 首页 上一页 1 下一页 末页 1 确定						

作为Site to Site分支的接入情况：☐ OFF [刷新](#)

允许访问资源列表：

允许访问的网络号	掩码	端口范围	协议
显示: 8 条 共0条 首页 上一页 1 下一页 末页 1 确定			

路由列表（分支内的PC必须处于该列表范围）：

IP地址	MASK地址
显示: 8 条 共0条 首页 上一页 1 下一页 末页 1 确定	

当前锁定信息 [刷新](#)

锁定用户：同名用户登录连续出错达到指定次数后，该用户名将被锁定

锁定IP地址：同IP用户登录连续出错达到指定次数后，该IP地址将锁定

锁定用户名	解锁剩余时间	操作
显示: 8 条 共0条 首页 上一页 1 下一页 末页 1 确定		

锁定IP地址	解锁剩余时间	操作
显示: 8 条 共0条 首页 上一页 1 下一页 末页 1 确定		

SSLVPN服务正常时的说明如下：

- (1) 点击页面右上角的 [查看日志](#) 可以查看SSLVPN运行中生成的日志记录，界面如下：

查看sslvpn日志

日志类型：[用户日志](#) 日志等级：[错误](#) 关键字： [查询](#) [导出全部日志](#)

日志类型	日志等级	时间	内容
首页 上一页 1 下一页 末页 1 确定			

取消

日志类型分别有：系统日志、管理员日志和用户日志；日志等级分为：错误、警告和信息。可以通过日志类型、日志等级以及手动输入的关键字来筛选日志信息。

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。

- 用户状态查询： [查询](#)
- (2) 通过 [用户状态查询](#) 可以查询用户的在线状态。输入用户名后，点击“查找”。界面如下图所示：



- 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。
- 当用户在线时，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。
- 点击 [解锁](#) 可以对锁定的IP或用户进行解锁。

8.6.4 基本设置

【应用场景】

本功能用于设置SSLVPN服务的基本参数。

【操作步骤】

- (1) 点击[网络]>>[SSLVPN配置]>>[基本设置]菜单项。

运行状态	基本设置	短信策略管理	隧道资源管理	用户授权	Site to Site管理
说明： SSLVPN客户端支持主流操作系统，包含Windows PC及笔记本、MAC苹果电脑、Android、IOS（不支持linux操作系统） SSLVPN访问方式： 用户启动Web浏览器(推荐用IE)或客户端，输入https://服务器地址:端口，其中服务器地址为设备的外网IP地址或域名，端口为本页面配置的SSLVPN服务端口 SSLVPN客户端下载地址： http://www.ruijie.com.cn/fw/wt/82396。					
SSLVPN服务端口: 443 * (1-65535)如果设备不是部署在出口，请在出口设备配置TCP及UDP的端口映射。 内网DNS: 114.114.114.114 用于解析内部域名，存在域名资源时必须配置。 用户认证方式: ☒ 本地认证 【添加本地认证用户】 ☐ Radius认证 ☐ 优先本地认证 ? 客户端网段: 2.1.2.0 / 255.255.255.0 * + 分配给隧道接入用户的IP地址网段，配置前请确认这些地址未在您的局域网中的其它地方使用。 ? DNS查询优先级: ☒ 内网DNS优先 ☐ 客户端DNS优先 用于隧道接入时指定优先查询的DNS，只对未授予“所有网络”隧道资源的用户生效。 >> SSLVPN高级设置 保存配置 暂停服务 关闭服务					

(2) 设置SSLVPN基本配置项。

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。

- 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。
- 内网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 “[安全认证]>>[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**：用于隧道接入时指定优先查询的DNS，可指定优先使用服务端内网的DNS服务器地址，或是优先使用客户端自身的DNS服务器地址。

(3) 展开“SSLVPN高级配置”，设置SSLVPN高级选项。

a 设置防爆破配置选项。

防爆破配置选项			
☒ 启用用户锁定	用户登录连续失败	5 次 (1-65535)	锁定 5 分钟 (0-10080,0不自动解锁)
☒ 启用IP锁定	IP登录连续失败	64 次 (1-65535)	锁定 5 分钟 (0-10080,0不自动解锁)

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暴力破解。

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。

b 设置用户登录时校验选项。

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：



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，可以禁止帐号方式从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帐号方式登录。

☐ [【创建USBKey】](#) [【黑名单管理】](#) [↓ USBKey导入控件和驱动安装包下载](#)

开启USBKey认证后，可以选择USBKey来登录SSLVPN客户端，如下图：



[设为首页](#) [收藏本页](#)

[客户端软件下载](#)

[登录](#) [SSLVPN](#)

登录类型: U-KEY登录

用户名登录

用户名: U-KEY登录 *

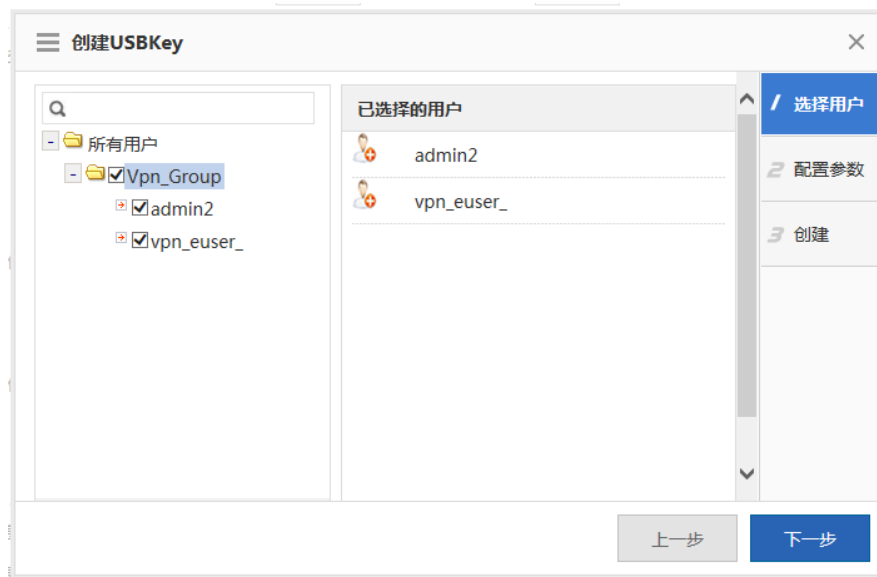
密 码: *

[登录](#)

[说明](#)

启用USBKey前需要**创建USBKey**:

- (1) 创建前需要下载USBKey控件和驱动，点击 [USBKey导入控件和驱动安装包下载](#) 根据PC终端系统安装32位或者64位控件，然后点击创建按钮 [【创建USBKey】](#)，进入创建USBKey页面。
- (2) 选择需要创建USBKey的用户，点击<下一步>。



- (3) 配置相关参数，点击<下一步>。默认的PIN码为1234。

- (4) 点击<开始创建>即可创建用户的USBKey。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，如果不想创建当前用户可以点击<跳过>选择跳过，创建下一个。

可信客户端证书导入和导出：

可信客户端CA路径： 未选择任何文件 (证书文件格式必须为.pem)

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。

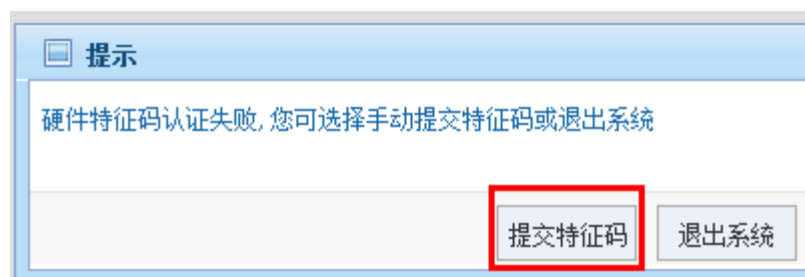
启用硬件特征码认证：

☐ 启用硬件特征码认证 [【特征码管理】](#)

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

开启硬件特征码认证后，当用户认证失败，系统将向用户收集硬件特征码。



对所有用户自动审批：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。

☒ 启用硬件特征码认证 每个用户允许绑定的特征码个数 (1-64) [【特征码管理】](#)

☒ 对所有用户启用自动审批 [?](#)

☐ 自动审批已提交硬件特征码的可信公共终端 [?](#)

特征码管理：除了开启自动审批，管理员也可以点击 [【特征码管理】](#) 在特征码管理页面进行手动审批：



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。

自动审批已提交硬件特征码的可信公共终端：如果某个终端已经存在于特征码管理列表中，则该终端的任何特征码用户均可自动通过审批。

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。

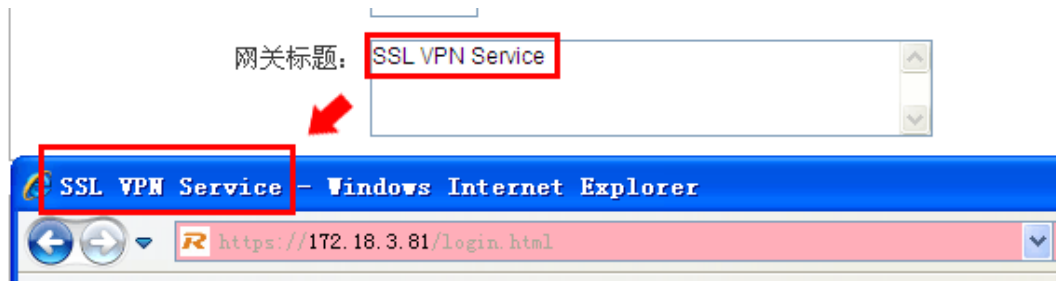
硬件特征码路径： 未选择任何文件

启用HTTP地址访问：开启后客户端可以通过HTTP协议访问服务。

- c 设置网关定制信息配置。

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：



LOGO文件配置路径：用来设置用户登录时和登录后页面左上角显示的LOGO。

- d 设置网关策略配置。

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

- e 设置SSLVPN网关证书。

SSLVPN网关证书导入

证书路径： 未选择任何文件

证书密码：

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。

- (4) 点击<保存配置>。

【后续处理】



页面底部提供<暂停服务>和<关闭服务>按钮：

- **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。

8.6.5 短信策略管理

【应用场景】

通过配置短信策略，在SSLVPN登录验证、硬件特征码绑定与解绑等环节对接短信服务器，从而实现登录的双重验证（用户名密码+短信验证）和绑定解绑操作的自动审批。

【操作步骤】

(1) 点击[网络]>>[SSLVPN配置]>>[短信策略管理]菜单项。

(2) 设置短信策略基本信息，并点击<保存设置>。

短信提供商：短信服务的运营商，要想实现短信验证码的发送，需要从短信运营商那购买短信包并获取相应对接参数。

注册码、密码、发送模板、APP ID等参数：根据选择的短信提供商，输入对应的对接参数进行绑定。如果不确定各参数值，请咨询短信服务商官网客服。

第一步：基本设置

短信提供商：	华兴软通	华兴软通官网
注册码：		密码：
发送模板：	尊敬的\${username}，您用于\${func}的验证码是\${VCode}。【SSLVPN服务】	
保存设置		

(3) 设置短信策略，并点击<保存设置>。

短信双因子认证：开启后，用户账号密码校验通过后，SSLVPN服务器会向用户指定的手机号码发送一个动态验证码，短信动态验证码校验通过后，才允许用户登录。默认关闭。

短信自助绑定：开启后，用户首次在一台终端登录提交硬件特征码时，服务器会以短信的方式向用户发送一个动态验证码，用户提交动态码并通过校验后即可自动审批。默认关闭。

短信自助解绑：开启后，用户能够通过SSLVPN登录页面跳转到自助解绑页面，通过身份校验、下发短信动态验证码、用户提交验证码、服务器校验通过后自动执行硬件特征码删除动作。默认关闭。

用户自助提交手机号码：开启后，用户在进行短信验证操作时可以手动输入接收短信的手机号码。默认关闭，即用户只能使用用户名所关联的手机号进行短信验证。

短信发送上限：限制每个用户每天的短信验证码请求次数，0代表不限制，默认配置为0。

第二步：短信策略

短信双因子认证：	关闭	短信自助绑定：	关闭
短信自助解绑：	关闭	用户自助提交手机号码：	关闭
短信发送上限：	0	(0-65535，限制每个用户每天的短信验证码请求次数，0代表不限制，默认配置为0)	
保存设置			

(4) 点击<添加关联用户手机>，设置用户名与手机号的关联。

输入用户名和手机号码，点击<添加>。当“用户自助提交手机号码”功能处于关闭状态时，验证短信只能发送到用户名所关联的手机号上。

三

添加关联用户手机

×

用户名:

*

手机号码:

*

添加

(5) 批量导入与备份关联用户手机。

关联用户手机导入与备份

说明: 在导入关联用户手机时, 请先导出 **user_phone.csv** 模板, 按照user_phone.csv模板的格式修订后直接 **xxx.csv** 导入即可。

路径:

选择文件

未选择任何文件

导入用户

导出用户

备份: 点击 **导出用户**, 将关联用户手机信息文件保存到本地。

批量导入:

- a 点击 **导出用户**, 导出user_phone.csv模板。
- b 按照user_phone.csv模板的格式, 填入需要导入的关联用户手机信息, 保存文件。
- c 点击<选择文件>, 选取上一步中保存的.csv格式文件, 再点击 **导入用户**。

8.6.6 隧道资源管理

【应用场景】

本功能用于管理SSLVPN服务提供的隧道资源, 控制哪些SSLVPN用户可以使用内网的哪些资源。

【操作步骤】

(1) 点击[网络]>>[SSLVPN配置]>>[隧道资源管理]菜单项。

运行状态

基本设置

隧道资源管理

WEB资源管理

用户授权

Site to Site管理

帮助

+

添加新的资源

所有网络

默认的全网资源

局域网

(2) 管理所有网络资源。

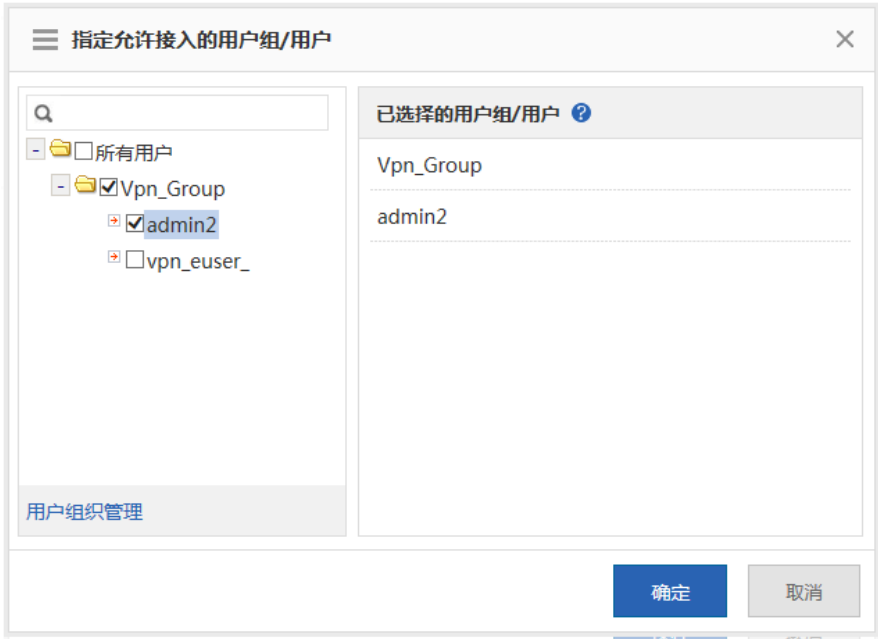
所有网络资源管理是默认存在的, 通过添加相关用户, 用户可以像局域网一样使用内网资源。

- a 点击“所有网络”资源图标, 进入授权页面:

270

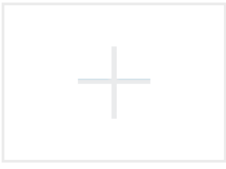


- b 点击<设置>，添加可以使用该资源的用户。在左侧用户组织结构中勾选允许使用资源的用户，点击<确定>。如需修改用户组织结构，可点击“用户组织管理”。



- c 返回授权页面后点击<保存>，完成资源授权操作。

(3) 添加新隧道资源。

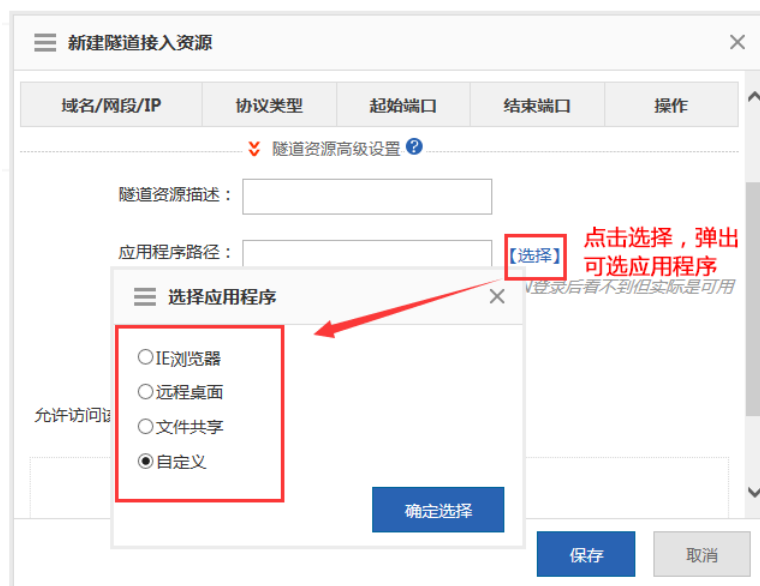


- a 点击 添加新的隧道资源，弹出添加框如下：

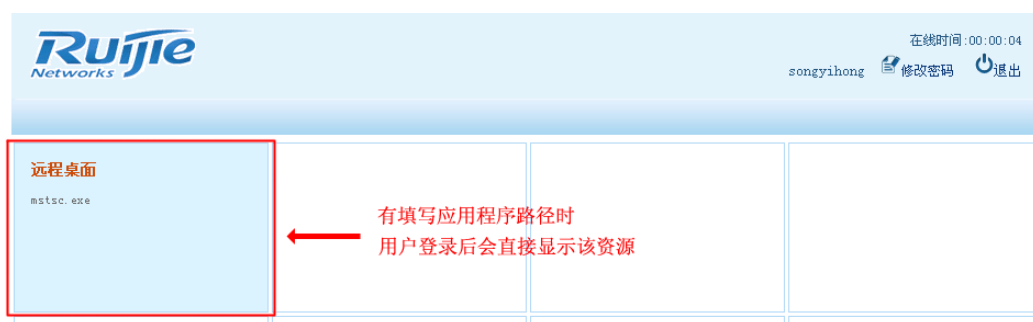
- b 输入隧道资源的名称，用于标识资源。
- c 点击<+添加>，添加可访问资源的匹配规则。选择匹配的目标类型（IP/网段/域名），并输入相应参数。在“高级选项”中还可以配置匹配协议和端口号。可以同时添加多个访问控制规则，形成一个资源组。

- d 点击<保存>完成访问控制规则配置。回到[新建隧道接入资源]页面，点击“隧道资源高级设置”可为隧道资源添加描述，并设置访问资源的应用路径，例如选择已有的“IE浏览器”、“远程桌面”、“文件共享”应用路径，或自定义其他应用程序路径。若启动应用程序需要参数，可以填写“程序启动参数”。

最后点击<保存>完成隧道资源设置。



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；如果没有设置应用程序路径，用户登录后将看不到该资源列表，但实际该资源是可以使用的。



e 设置允许访问该资源的用户组。

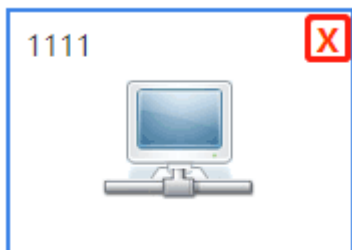
点击 **+ 设置** 添加可以访问该资源的用户。



(4) 选择完要授权的用户后，点击<确定>。返回添加页面点击<保存>，完成新资源的添加。

【后续处理】

对已有的隧道资源，鼠标移至图标，点击  可直接删除。



8.6.7 用户授权

【应用场景】

本功能用于对用户（组）授权隧道资源。这里的用户树列出的是本地用户，也就是[安全认证]>>[用户组织]>>[用户管理]中配置的用户。设备的SSLVPN采用认证和授权分离的机制，就是认证方式上可以使用本地用户或Radius服务器进行认证，但授权只能对本地用户授权；要对Radius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Radius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，那么SSLVPN使用本地用户认证时，该用户将无法登录成功；如果使用Radius认证，同时本地用户中又有同名用户，那么只有当该用户开启了“允许做VPN用户”，才能对该用户授权特定资源，否则默认继承“所有用户”已授权的资源。

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：



【操作步骤】

- (1) 点击[网络]>>[SSLVPN配置]>>[用户授权]菜单项。
- (2) 按如下步骤进行用户授权。



- a 在左侧用户组织中选中要授权的用户或用户组。
- b 点击  将弹出未授权的资源列表。
- c 勾选要授权的资源，这里只列出未授权的资源。
- d 点击  完成对用户（组）新增资源。

【后续处理】

- 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。
- 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。

8.6.8 Site to Site 管理

【应用场景】

用于配置设备作为VPN总部接受其他SSLVPN设备接入，或是作为VPN分支接入SSLVPN总部，实现点对点接入场景。可选的应用模式如下：

- 总部：设备作为SSLVPN服务器，支持其他SSLVPN设备作为分支接入，共享内网资源。
- 分支：设备作为SSLVPN客户端（分支），能够接入总部的SSLVPN服务器，访问授权资源。与分支连接的局域网内所有终端都能通过安全隧道安全地与总部或其它分支进行通信。
- 既是总部又是分支：设备能够同时作为SSLVPN服务器和客户端，既接入其他SSLVPN服务器，又接受其他SSLVPN设备的接入。

【操作步骤】

- (1) 点击[网络]>>[SSLVPN配置]>>[Site to Site管理]菜单项。
- (2) 选择本设备的部署模式。

本设备为：分支

- (3) 设置站点相关配置项。

【总部配置】

总部配置

[+ 添加分支](#) [+ 批量添加资源](#) [@ 管理访问资源](#) [X 删除选中](#)

☐	分支用户	分支网段	允许访问的资源	是否禁用	连接状态	操作
☐	testxxx	192.10.10.0/255.255.255.0	局域网	已启用 禁用	未连接	配置同步 编辑 删除

显示: 10 条 共1条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶

1 [确定](#)

- 点击[+ 添加分支](#)，添加分支的接入信息。完成设置后点击<保存>。

分支名称：接入分支的名称，即登录用户名，不能与本地用户或Radius用户的名称重复。

登录密码：分支内终端连接SSLVPN时需要验证的密码。

分支网段：分配给分支终端的IP网段，不能与服务端内网网段重合。

访问的资源：勾选允许分支终端访问的内网资源。

说明

访问资源中存在域名资源时，请将分支内PC的首选DNS设置为SSLVPN的内网DNS地址。

三 新增分支

×

分支名称:

*

与本地用户或Radius用户不能相同

登录密码:

*

分支网段:

子网

掩码

*

+

请使用尚未在您网络部署的局域网网段

访问的资源: 存在域名资源时, 请将分支内PC的首选DNS设置为SSLVPN的内网DNS地址

☐ 全选

☐ ★ 局域网

保存

取消

- 勾选列表中已添加的分支表项，点击 [+ 批量添加资源](#)，可对多个分支批量授权可访问的资源。

总部配置

[+ 添加分支](#) [+ 批量添加资源](#) [管理访问资源](#) [× 删除选中](#)

☒	分支用户	分支网段	允许访问的资源	是否禁用	连接状态	操作
☒	testxxx	192.10.10.0/255.255.255.0	局域网	已启用 禁用	未连接	配置同步 编辑 删除

显示: 10 条 共1条

首页 上一页 1 下一页 末页 1 确定

- 点击 [管理访问资源](#) 可对隧道资源进行管理，详见[8.6.6 隧道资源管理](#)章节。
- 勾选列表中已添加的分支表项，点击 [× 删除选中](#)，可以批量删除分支信息。
- 点击 [禁用](#)，可以一键禁用对应分支。点击 [开启](#)，可以重新启用分支。

【分支配置】

分支配置

用户名:

*

密码:

*

服务器:

IP

端口:

(范围1-65535)

+

- 用户名和密码**：输入总部设置的验证用户名和密码。
- 服务器**：输入需要连接的SSLVPN服务器的IP地址或域名以及端口号。点击 [+](#) 可添加多个服务器作为备份。

8.7 NAT/端口映射

8.7.1 功能介绍

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。

8.7.2 端口映射

端口映射包含两种映射关系，端口映射和整机映射（DMZ主机）；

1. 设置端口映射

【操作步骤】

(1) 点击[网络]>>[NAT/端口映射]>>[端口映射]菜单项。

端口映射

NAT转换规则

添加NAT地址池

说明：一般应用在将内网指定主机的指定端口映射到全局地址的指定端口上。设备性能限制建议端口映射数量不超过500条。

注意：若存在多出口场景，当存在整机服务器映射时，要配置这个服务器只能从某个特定的出口出去。

帮助：[端口映射常见功能如何使用?](#)

FTP服务器端口：

保存

(如果映射的是FTP服务器，则映射的外网端口要包含在FTP端口中，多个端口用逗号“,”隔开，FTP服务器端口最多只能配8个)

+添加

×删除选中

基于 查询映射：

查找

☐	映射关系	内网IP	内网端口范围	外网IP	外网端口	协议类型	接口	描述	操作
无记录信息									

显示： 条 共0条

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶

确定

(2) 点击<添加>，选择映射关系为“端口映射”，并设置端口映射相关配置项，设置完成后点击<确定>。

添加端口映射

映射关系：

端口映射

?

 参看示例

内网IP：

*

内网端口范围：

*

 ~ (1-65535)

外网IP：

输入地址：

*

?

使用接口地址：

Gi0/3

外网端口范围：

*

 ~ (1-65535)

协议类型：

TCP

描述：

确定

取消

- **内网IP**：要映射到外网的内网IP，通常是您的服务器IP地址。
- **内网端口范围**：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。
- **外网端口范围**：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。

点击<参看示例>，可以根据示例进行配置。

?

 参看示例

将内网WEB服务器IP: 192.168.1.200, 端口: 80
或80~8080
映射到设备公网IP: 200.10.10.10, 端口: 80或
80~8080
示例填写说明:
映射关系: 端口映射
内网IP:192.168.1.200
内网端口: 80或80~8080
外网IP->输入地址: 200.10.10.10
外网端口: 80或80~8080
协议类型: TCP

2. 设置整机映射 (DMZ 主机)

【操作步骤】

(1) 点击[网络]>>[NAT/端口映射]>>[端口映射]菜单项。

端口映射

NAT转换规则

添加NAT地址池

说明：一般应用在将内网指定主机的指定端口映射到全局地址的指定端口上，设备性能限制建议端口映射数量不超过500条。
注意：若存在多出口场景，当存在整机服务器映射时，要配置这个服务器只能从某个特定的出口出去。
帮助：[端口映射常见功能如何使用？](#)

FTP服务器端口：

21

保存

(如果映射的是FTP服务器，则映射的外网端口要包含在FTP端口中，多个端口用逗号“,”隔开，FTP服务器端口最多只能配8个)

+ 添加

✕ 删除选中

基于

内网IP

 查询映射：

查找

☐	映射关系	内网IP	内网端口范围	外网IP	外网端口	协议类型	接口	描述	操作
无记录信息									

显示：

10

条 共0条

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶

1

确定

(2) 点击<添加>，选择映射关系为“整机映射(DMZ主机)”，输入内部服务器IP地址和规则生效的外网IP或外网口，设置完成后点击<确定>。当外来的数据包没有命中任何端口映射时，DMZ规则可将该数据包重定向到内网服务器中，即所有从Internet主动发往设备的数据报文都将转发给指定的DMZ主机。

≡ 添加端口映射

✕

映射关系：

整机映射(DMZ主机)

?

[参看示例](#)

内网IP：

*

外网IP：

●

输入地址：

*

?

○

使用接口地址：

Gi0/3

▼

描述：

确定

取消

8.7.3 NAT 转换规则

【应用场景】

将ACL应用于NAT地址池，实现只对匹配ACL规则的地址进行NAT转换。

【操作步骤】

(1) 点击[网络]>>[NAT端口映射]>>[NAT转换规则]菜单项。

	ACL列表	应用于地址池
☐	110 [编辑]	nat_pool
☐	1 [编辑]	nat_pool

显示: 10 条 共2条

首页 < 上一页 1 下一页 > 末页

(2) 点击<添加>。

ACL列表: 1 [\[新建ACL列表\]](#)

选中地址池: nat_pool

确定 取消

(3) 设置NAT转换规则相关的配置项。

- ACL列表：选择要应用的ACL序号或名称。下拉框中为当前设备上已配置的ACL，点击[【新建ACL列表】](#)可新建ACL列表，具体配置步骤请参考[7.9 ACL访问列表](#)章节。
- 选中地址池：选择要应用到的NAT地址池。添加NAT地址池请参考[8.7.4 添加NAT地址池](#)章节。

(4) 点击<确定>。

8.7.4 添加 NAT 地址池

【应用场景】

当用户有多个外网IP时，用户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。

【操作步骤】

(1) 点击[网络]>>[NAT端口映射]>>[添加NAT地址池]菜单项。

端口映射

NAT转换规则

添加NAT地址池

说明：地址池是指分配给内网用户的公用 IP 地址配置的范围，设备性能限制建议地址池数量不超过500条。

地址池列表： nat_pool + 添加地址池 × 删除选中

☐	序号	接口	起始IP地址	结束IP地址	操作
☐	1	Gi0/4	/	/	编辑 删除

显示: 10 条 共1条

首页
 上一页
 1
 下一页
 末页

1 确定

(2) 点击<添加地址池>。

添加地址池

×

地址池名称: ☒ 输入: * ☐ nat_pool

外网端口: ☐ Gi0/3 ☐ Gi0/6 ☐ Gi0/7 ☐ Gi0/9 ☐ Di1 ☐ Di2 ☐ Di3

确定

取消

(3) 设置地址池相关配置项。

- 地址池名称：输入地址池的名称。

如果要在现有的地址池上添加地址，请在下拉框 ☒ nat_pool 中选择现有的地址池。

- 选择外网端口：选择用户要添加的外网口，此时下方会出现地址池起始与结束IP地址的输入框：

Gi0/6-起始IP地址: 结束IP地址:

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。

(4) 点击<确定>保存配置。

8.8 NATPT 配置

说明

支持本功能的产品包括：NBR6205-E、NBR6205-E V2、NBR6135-E、NBR6210-E、NBR6210-E V2、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E。

NAT-PT(Network Address Translator - Protocol Translator，附带协议转换的网络地址转换)，是一种纯IPv6节点和IPv4节点间的互通方式，该过程中所有包括地址、协议在内的转换工作都由设备来完成。

【前置条件】

需要在[运维]>>[系统设置]>>[增强功能]中开启IPv6大容量功能（配置后需要重启设备以生效）。



8.8.1 参数配置

【应用场景】

配置NATPT功能的基本参数。

【操作步骤】

(1) 点击[网络]>>[NATPT配置]>>[参数配置]菜单项。



(2) 设置对应的参数。

- **NATPT前缀**：IPv6发往IPv4的报文，匹配该前缀的，交由NATPT处理；IPv4发往IPv6的报文，源IPv4地址未匹配地址映射的情况下，使用该前缀生成新的IPv6源地址。
- **DNS-ALG**：DNS应用层网关，用于支持DNS报文跨IPv4/IPv6的传输。
- **FTP-ALG**：FTP应用层网关，用于支持FTP报文跨IPv4/IPv6的传输。

8.8.2 V4V6 规则

【应用场景】

本功能可以将IPv6地址池应用于ACL，以实现NATPT动态规则转换；或者将静态IPv4地址映射到IPv6地址，实现NATPT静态规则转换。在从IPv4向IPv6域中转发数据包时使用。

【操作步骤】

(1) 点击[网络]>>[NATPT配置]>>[V4V6规则]菜单项。

(2) 点击<添加规则>。

(3) 设置V4V6规则相关配置项。

静态规则是指手工建立IPv4地址和IPv6地址的一对一永久映射，需要输入匹配的IPv4地址和映射的IPv6地址。

动态规则是指建立IPv4地址和IPv6地址池的临时映射关系。IPv6地址池中的地址用来将IPv4报文中的源地址转换为IPv6地址，ACL访问列表用于实现对NATPT转换网段的匹配。

(4) 点击<保存>。

8.8.3 V6V4 规则

【应用场景】

本功能可以将IPv4地址池应用于ACL，以实现NATPT动态规则转换；或者将静态IPv6地址映射到IPv4地址，实现NATPT静态规则转换。在从IPv6向IPv4域中转发数据包时使用。

【操作步骤】

(1) 点击[网络]>>[NATPT配置]>>[V6V4规则]菜单项。

参数配置

V4V6规则

V6V4规则

地址池配置

说明： 此功能用于将IPv4地址池应用于ACL，实现NATPT动态规则转换；或者将静态IPv6地址映射到IPv4地址，实现NATPT静态规则转换。 由于已有

+ 添加规则

× 删除选中

☐	类型	ACL

无记

显示: 10 条 共0条

(2) 点击<添加规则>。

添加规则

×

类型：

☒ 静态规则

☐ 动态规则

匹配IP：

* 填写IPv6地址

映射IP：

* 填写IPv4地址

保存

关闭

(3) 设置V4V6规则相关配置项。

静态规则是指手工建立IPv4地址和IPv6地址的一对一永久映射，需要输入匹配的IPv6地址和映射的IPv4地址。

动态规则是指建立IPv6地址和IPv4地址池的临时映射关系。IPv4地址池中的地址用来将IPv6报文中的源地址转换为IPv4地址，ACL访问列表用于实现对NATPT转换网段的匹配。

(4) 点击<保存>。

8.8.4 地址池配置

【应用场景】

地址池是指在NATPT过程中分配给内网用户的IP地址范围，设备性能限制建议地址池数量不超过500条。

【操作步骤】

- (1) 点击[网络]>>[NATPT配置]>>[地址池配置]菜单项。
- (2) 点击<添加地址池>。

添加地址池

类型：☒ v4v6 ☐ v6v4

地址池名称：

开始IP： * 填写IPv6地址

结束IP： * 填写IPv6地址

前缀长度： * 范围：0-128

保存

关闭

(3) 设置地址池相关配置项。

类型：选择地址池类型，v4v6表示需要将IPv4地址转换为IPv6地址，即设置IPv6地址池；v6v4表示需要将IPv6地址转换为IPv4地址，即设置IPv4地址池。

开始IP：地址池起始IP。

结束IP：地址池结束IP，“开始IP-结束IP”为可分配的IP地址范围。

前缀长度/子网掩码：IPv6地址池的地址前缀长度或IPv4地址池的网络掩码。

(4) 点击<保存>。

8.9 DHCP 配置

8.9.1 功能简介

DHCP (Dynamic Host Configuration Protocol, 动态主机设置协议) 是一个局域网的网络协议，使用UDP协议工作，被广泛用来动态分配可重用的网络资源，如IP地址。规模较小的网络，通过DHCP可以使后续增加网络设备变得简单快捷。

使用DHCP，可以带来以下受益：

- 降低客户端的配置和维护成本

DHCP易配置部署，对于非技术用户，DHCP能够将客户端与配置相关的操作降至最低，并能够降低远程部署和维护成本。

- 集中管理

DHCP服务器可以管理多个网段的配置信息，当某个网段的配置发生变化时，管理员只需要更新DHCP服务器上的相关配置即可。

NBR网关设备可以作为DHCP服务器，为内网用户提供IP地址。

8.9.2 服务端配置

点击[网络]>>[DHCP配置]>>[服务端配置]菜单项：

服务端配置

静态地址分配

客户端列表

?

帮助

+ 添加DHCP

✕ 删除选中DHCP

🔗 不分配的IP段

DHCP服务开关：

ON

☐	名称	地址范围	默认网关	租用时间	DNS	操作
☐	ap_dhcp_pool	192.168.2.1-192.168.2.254	192.168.2.2	1天	192.168.58.110	编辑 删除
☐	net20	20.1.1.1-20.1.1.254		1天		编辑 删除
☐	test	192.168.124.1-192.168.124.254	192.168.124.1	永久	192.168.58.110	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

若DHCP服务处于OFF状态，请点击开启：



1. 添加 DHCP

(1) 点击<添加DHCP>。

服务端配置		静态地址分配	客户端列表							
+ 添加DHCP		添加DHCP								
① 点击<添加DHCP>		② 在弹出窗中填写配置项								
☐ ap_dhcp_pool		地址池名称：								
☐ net20		IP分配网段：								
☐ test		掩码：								
显示: 10 条 共3条		默认网关：								
		租用时间：	● 永久 ○ 租期 天 小时 分钟 *							
		首选DNS：								
		备用DNS：								
		③ 点击<完成配置>提示成功后，内容会显示在列表中								
		完成配置 取消								

(2) 在弹窗中填写配置项。点击<高级配置>，可配置DHCP Option以及地址租期。

添加DHCP

地址池名称:

* ? 参考示例

IP分配网段:

* 格式: 192.168.1.0

掩码:

* 格式: 255.255.255.0

IP分配范围:

至

默认网关:

* 格式: 192.168.1.1

首选DNS:

* 格式: 114.114.114.114

备用DNS:

完成配置

取消

高级配置

Option 43:

ip

?

Option 138:

?

租用时间:

☐ 永久 (可能导致地址池可分配IP数量不足)

☒ 租期

1

天

0

小时

0

分钟 *

完成配置

取消

表8-1 DHCP 地址池配置说明

参数	说明
地址池名称	地址池的名称
IP分配网段	用于分配的IP地址网段
掩码	IP地址网络掩码
IP分配范围	分配网段中可用于分配的IP地址范围
默认网关	分配IP的网关地址
DNS	运营商提供的DNS服务器地址，可分别设置首选DNS和备用DNS，当首选DNS不可

参数	说明
	用时，将使用备用DNS进行域名解析
Option 43	用在无线网络管理中，当AC（无线控制器）与AP不在同一局域网，AP通过DHCP服务器获取IP地址后，无法通过广播方式发现AC，因此需要在DHCP服务器上配置DHCP响应报文中携带的Option 43信息，通告AP使AP能够发现AC。 不同AP设备对于Option支持情况不一样，需要根据被管理AP设备，选择Option 43还是Option 138
Option 138	用在无线网络管理中，填入AC的IP地址。与Option 43类似，当AC与AP不在同一局域网时，可通过设置Option 138选项使AP获取AC的IPv4地址。 不同AP设备对于Option支持情况不一样，需要根据被管理AP设备，选择Option 43还是Option 138
租用时间	分配的IP地址的可用租期，默认为1天。到期后将收回IP地址，需要终端重新获取进行续租。

(3) 点击<完成配置>。

【后续处理】

● 批量删除DHCP

② 点击<删除选中DHCP>

③ 点击<确定>, 完成删除

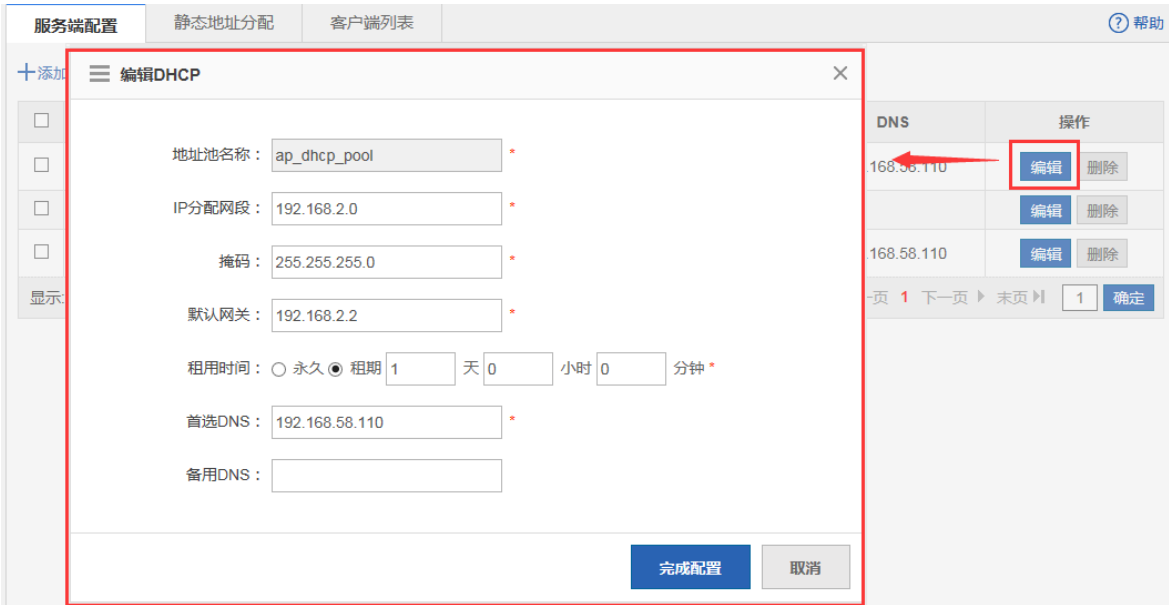
① 在列表中选择要删除的DHCP

a 选择需要删除的地址池，点击<删除DHCP>。

b 在弹出的确认框中点击<确定>。

- 删除DHCP：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。

- 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。



2. 配置不分配的 IP 段



- (1) 点击<不分配的IP段>。
- (2) 在弹窗中设置不分配的IP段。可以配置若干个IP段，IP段内的IP将不会分配给用户。
- (3) 点击<完成配置>。

3. DHCP 服务开关



8.9.3 静态地址分配

(1) 点击[网络]>>[DHCP配置]>>[静态地址分配]菜单项。



(2) 点击<添加静态地址>。



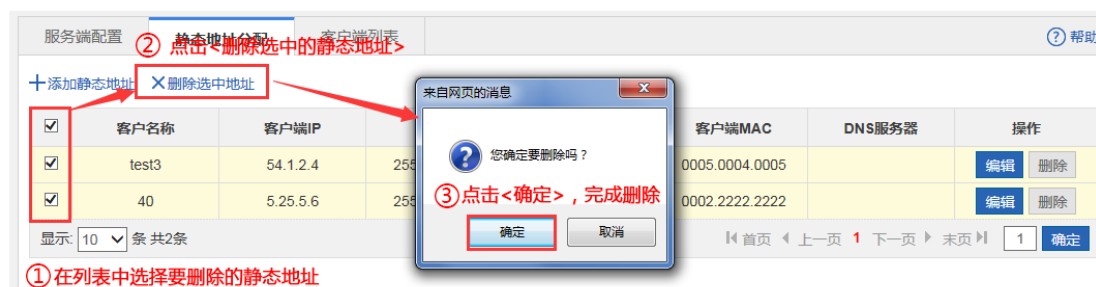
(3) 在弹窗中填写配置项。

- 客户名称：客户端主机名称或标识。
- 客户端IP：分配给客户端的固定IP地址。
- 子网掩码：IP地址的掩码。
- 客户MAC地址：客户终端的MAC地址。配置后，该MAC地址每次联网都将获取到固定IP。
- 网关：分配给客户端的网关地址。
- DNS：分配给客户端的DNS服务器。
- 更多配置项介绍可参考[表8-1](#)。

(4) 点击<完成配置>。

【后续处理】

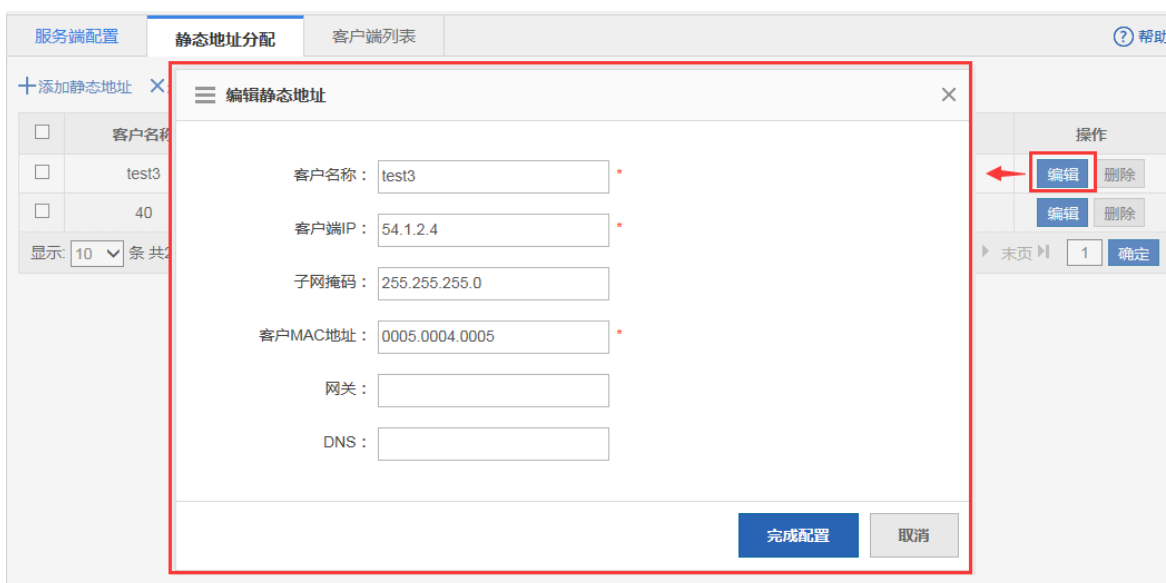
- 批量删除静态地址



a 勾选需要删除的静态地址表项，点击<删除选中地址>。

b 在确认框中点击<确定>。

- 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。



8.9.4 客户端列表

点击[网络]>>[DHCP配置]>>[客户端列表]，可查看当前获取到IP的客户端信息。

服务端配置

静态地址分配

客户端列表

帮助

把MAC地址绑定到动态获取的IP上

基于IP地址查询：

搜索

☐	已分配的IP地址	MAC地址	地址租期	IP分配方式
☐	20.1.1.134	6c62.6dd2.f4f3	0天3小时22分钟	动态获取

显示: 20 条 共1条

首页 上一页 1 下一页 末页

1 确定

- 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。

基于IP地址查询：

搜索

8.10 DHCP 配置 (IPAM)

说明

支持配置DHCP IPAM（DHCP高级模式）功能的产品：NBR2500D-E、NBR3000D-E、NBR6135-E、NBR6210-E、NBR6210-E V2、NBR6205-E、NBR6205-E V2、NBR6215-E。

8.10.1 IPAM 主页

【应用场景】

通过该操作，可以获取地址池使用情况、地址池使用率Top10、IP安全绑定情况等信息。

【操作步骤】

(1) 点击[网络]>>[DHCP配置]>>[IPAM主页]菜单项。

(2) 获取对应的信息。

IPAM主页

IP智能管理

业务告警

DHCP配置管理

地址池使用情况

DHCP日志

DHCP黑名单

地址池使用情况

手动刷新

当前系统告警: 地址池耗尽 (0条), 终端迁移 (0条), 地址冲突 (0条), 待授权用户 (0个), 每5分钟刷新一次

地址池数

1499个

地址总数

380745个

已分配地址数

0个

使用率

0%

地址池使用率top10

更多

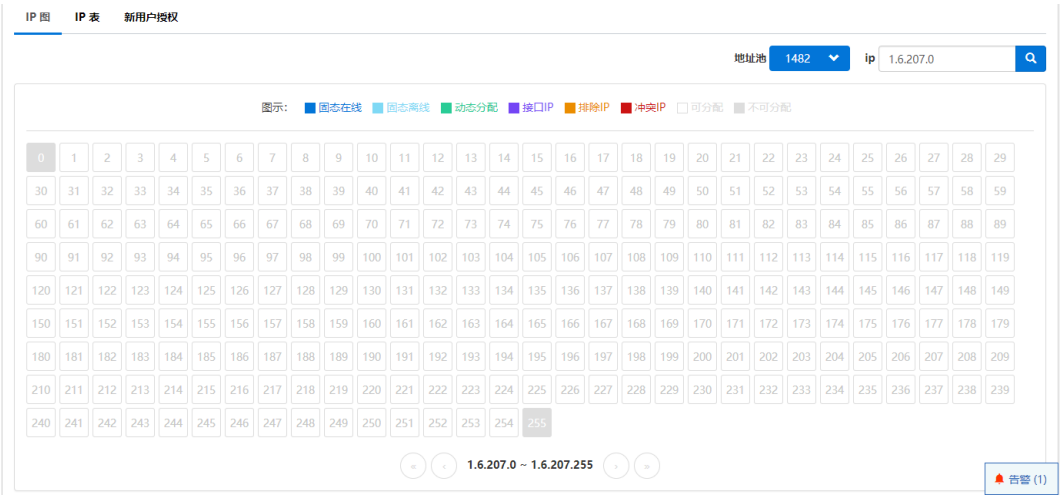
地址池名称	总数	已用个数	利用率
1480	254	0	0%
1478	254	0	0%
1481	254	0	0%
1476	254	0	0%
1479	254	0	0%
1474	254	0	0%
1477	254	0	0%
1472	254	0	0%
1475	254	0	0%
1470	254	0	0%



8.10.2 IP 智能管理

【操作步骤】

- (1) 点击[网络]>>[DHCP配置]>>[IP智能管理]菜单项。
- (2) 在[IP图]页面，显示地址池的使用情况和IP地址详细信息，包括显示地址池网段的IP使用情况、搜索目标地址网段、单个IP地址的详细信息。



- (3) 在[IP表]页面，以表格形式显示获取IP地址的用户信息，包括用户类型、用户状态、绑定类型等。可以点击<加入mac黑名单>，禁止用户获取IP地址。

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	编辑 加入mac黑名单 删除
+	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	编辑 加入mac黑名单 删除
+	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	编辑 加入mac黑名单 删除
+	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	编辑 加入mac黑名单 删除
+	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	编辑 加入mac黑名单 删除
+	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	编辑 加入mac黑名单 删除
+	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

- (4) 针对部分不允许动态分配IP地址的场景，在[新用户授权]页面配置授权用户后，只有授权过的用户才可正常获取到地址。

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	上次失败次数	授权建议	操作
没有找到匹配的记录									

8.10.3 业务告警

【操作步骤】

- 点击[网络]>>[DHCP配置]>>[业务告警]菜单项。
- 在[地址池耗尽]页签，查看地址池耗尽告警：
 - 定时每5分钟检测地址池当前已分配数量是否达到告警阈值，若达到则打印地址池耗尽的系统日志，同时生成地址耗尽告警信息。当定时检测地址池的已分配数量未超过告警阈值或用户手动清除告警信息时，将地址池地址耗尽的当前告警节点加入到历史告警信息中。
 - 终端获取地址过程中，若匹配地址池发现地址池耗尽也会生成地址池耗尽告警信息。

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 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(%)
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					
< 1 2 3 4 5 > 告警 (1)					

- 点击[终端迁移]，查看终端迁移告警。

只检测静态绑定MAC的终端，记录终端首次接入位置信息，当该终端后续DHCP报文的接入位置信息和首次接入位置信息不相同，生成终端迁移告警信息。当该终端后续DHCP报文的接入位置信息和首次接入位置信息相同或用户手动清除当前告警节点时，将终端迁移告警信息加入历史告警信息中。

地址池耗尽

终端迁移

IP 冲突

✓ 批量确认

搜索

☐	IP地址	MAC地址	所属地址池	发生时间	接入设备IP (迁移前 / 迁移后)	接入设备MAC (迁移前 / 迁移后)	VLAN号 (迁移前 / 迁移后)	端口索引 (迁移前 / 迁移后)	操作
没有找到匹配的记录									

[查看已解决的告警](#)

- 点击[IP冲突]，查看IP冲突告警。

- DHCP服务器收到DHCP客户端的discover广播报文后，选择空闲IP地址响应offer报文。响应offer报文之前，会使用该IP地址进行PING检测，若检测可以PING通则认为该IP地址冲突，此时需要添加地址冲突告警节点。
- DHCP客户端收到DHCP服务器的服务端offer报文后，会发送ARP请求检测该IP地址是否对应其他的终端MAC地址，若存在则发送给DHCP Server端Decline报文。DHCP服务器接收到decline报文后时需要添加地址冲突告警节点。

地址池耗尽		终端迁移	IP 冲突
✕ 清除选中		✕ 清除所有	搜索
☐	冲突IP	发生时间	结束时间
	接入设备IP	接入设备MAC	VLAN号
	端口索引	操作	
没有找到匹配的记录			
查看已解决的告警			

8.10.4 DHCP 配置管理

【应用场景】

通过该操作，可以设置DHCP相关配置。

【操作步骤】

- (1) 点击[网络]>>[DHCP配置]>>[DHCP配置管理]菜单项。
- (2) 在[地址池管理]页面，开启DHCP服务并添加DHCP地址池。
 - a 开启DHCP服务。

IPAM主页

IP智能管理

DHCP配置管理

地址池使用情况

DHCP黑名单

地址池管理

不分配IP

注意：云终端虚拟同一接入位置的场景，实体不能绑定接入位置元素，否则无法分配上线。

DHCP服务(已开启): 关闭 认证继承功能(已关闭): 开启 说明

+ 添加地址池

✕ 清除选中

MAC_OUI批量配置

导入配置

下载模板

导出数据

搜索

↺

☐	名称	地址范围	默认网关	租用时间	DNS	允许动态分配	地址池类型	关联地址池	操作
☐	pool_gi0/1	192.168.2.10-192.168.2.200	192.168.2.1	1天	114.114.114.114	☒ 动态	未分配		编辑删除
☐	pool_gi0/3	2.1.1.1-2.1.1.254	2.1.1.1	8小时	114.114.114.114	☒ 动态	未分配		编辑删除
☐	pool_gi0/1.7	192.168.7.1-192.168.7.254	192.168.7.1	8小时	114.114.114.114	☒ 动态	未分配		编辑删除
☐	pool_gi0/1.1	10.0.0.1-10.0.0.254	10.0.0.1	8小时	114.114.114.114	☒ 动态	未分配		编辑删除
☐	pool_gi0/2	133.133.11.1-133.133.11.254	133.133.11.21	8小时	114.114.114.114	☒ 动态	未分配		编辑删除
☐	pool_gi0/4	192.168.144.1-192.168.144.254	192.168.144.1	8小时	114.114.114.114	☒ 动态	未分配		编辑删除
☐	test	192.168.200.1-192.168.200.30	192.168.200.1	5分钟	192.168.58.110	☒ 动态	未分配		编辑删除
☐	pool_gi0/0	192.168.1.1-192.168.1.254	192.168.1.1	8小时	114.114.114.114	☒ 动态	未分配		编辑删除
☐	pool_gi0/5	192.168.22.1-192.168.22.254	192.168.22.1	8小时	114.114.114.114	☒ 动态	未分配		编辑删除

显示第 1 到第 9 条记录，总共 9 条记录

- b 点击<添加地址池>，设置DHCP地址池相关配置项，并点击<完成配置>。

说明

- 虚拟地址池配置项用于配置为虚拟机分配IP的虚拟地址池，可应用于云办公场景。云终端包含物理机和虚拟机两个IP地址且接入网络位置相同，物理机IP地址用于与云主机建立隧道，虚拟机用于实际的云桌面呈现及操作。通过分别设置实机地址池并关联实机MAC-OUI以及设置虚机地址池并关联虚机MAC-OUI，可以实现为云终端同时分配所需的两个IP地址。
- 匹配mac-oui用于设置地址池OUI信息。

新增DHCP

* 地址池名称

地址池名称必填

允许动态分配

☒ 动态

* IP分配网段

192.168.1.0

* 掩码

255.255.255.0

网段起始IP

192.168.1.1

网段结束IP

192.168.1.254

* 默认网关

默认网关

* 租用时间

☐ 永久（可能导致地址池可分配IP数量不足）

☒ 租期

1

天

0

时

0

分

* 首选DNS

首选DNS必填

备用DNS

备用DNS

(虚拟) 地址池

☒ 普通地址池 ☐ 虚拟地址池

匹配mac-oui

mac前6位（例：525400），一行一个

☒ 完成配置

切换到高级设置

(3) 点击<MAC_OUI全局配置>，设置匹配的全局MAC-OUI信息。

MAC地址的前3字节特征简称为MAC-OUI，MAC-OUI分为全局OUI和地址池OUI信息，其中全局OUI信息仅对未配置地址池OUI的虚地址池生效。当地址池关联MAC-OUI信息后，仅当终端的MAC-OUI信息和地址池的MAC-OUI匹配时才允许从该地址池分配地址。当地址池（普通、实地址池）不配置MAC-OUI信息时，不对终端MAC-OUI进行校验，当其他条件比如接口与地址池网段匹配满足后，都允许从该地址池中获取地址。

通过设置全局MAC-OUI，可以实现根据终端的MAC-OUI分配不同的IP地址段。

a 设置“认证继承模式”。

根据实际匹配情况进行选择即可，可以只匹配MAC，也可只匹配接入位置，或二者同时匹配。

b 设置“全局MAC_OUI”，最大可设置16个。

c 点击<保存>。

(4) 在[不分配IP]管理页面，设置地址池中不用于分配的IP地址。

a 点击<添加不分配IP>。

添加不分配IP

* 开始IP

输入IP地址

结束IP

输入IP地址

描述

输入的字符不能包含字符 \ ? , 中间不能包含空格

保存

- b 设置“开始IP”和“结束IP”。
- c 点击<保存>。

8.10.5 地址池使用情况

【应用场景】

通过该操作可以创建DHCP地址池，并了解各地址池的使用情况。

【操作步骤】

- (1) 点击[网络]>>[DHCP配置]>>[地址池使用概况]菜单项。
- (2) 点击<新增地址池>。

新增DHCP

* 地址池名称

地址池名称必填

允许动态分配

☒ 动态

* IP分配网段

192.168.1.0

* 掩码

255.255.255.0

网段起始IP

192.168.1.1

网段结束IP

192.168.1.254

* 默认网关

默认网关

* 租用时间

☐ 永久（可能导致地址池可分配IP数量不足）

☒ 租期

1

天

0

时

0

分

* 首选DNS

首选DNS必填

备用DNS

备用DNS

(虚拟) 地址池

☒ 普通地址池 ☐ 虚拟地址池

匹配mac-oui

mac前6位（例：525400），一行一个

完成配置

切换到高级设置

- (3) 设置DHCP地址池相关配置项。
- (4) 点击<切换到高级配置>，设置高级选项。
- (5) 点击<完成配置>。

【后续处理】

在[DHCP使用概况]页面，可以查询地址池的使用情况，包括总IP数、已分配IP数、未使用IP数和IP使用率。

IPAM主页IP智能管理业务告警DHCP配置管理地址池使用概况DHCP日志DHCP黑名单

+ 新增地址池

搜索

地址池	总IP数	已分配IP数	未使用IP数	IP使用率
test1	253	0	253	0%
lin1	244	0	244	0%
lin2	253	0	253	0%
lin3	253	0	253	0%
lin4	253	0	253	0%
2	254	0	254	0%
3	254	0	254	0%
4	254	0	254	0%
5	254	0	254	0%
6	254	0	254	0%

显示第 1 到第 10 条记录，总共 501 条记录 每页显示 10 条记录

<

<

1

2

3

4

5

>

>

告警 (1)

8.10.6 DHCP 日志



DHCP日志将保存在硬盘中，对于无硬盘的设备，无法正常记录和查看DHCP日志。

【操作步骤】

(1) 点击[网络]>>[DHCP配置]>>[DHCP日志]菜单项。

IPAM主页

IP智能管理

业务告警

DHCP配置管理

地址池使用概况

DHCP日志

DHCP黑名单

数据源状态: 已连接

LOG写入状态: 开启

最大可存日志: 500000个;

LOG写入: 开启

历史记录

2018-09-04

MAC

IP

主机名

接入设备

VLAN

端口

事件类型

所有类型

时间

时

分

分

时

分

分

分

搜索

清空搜索

MAC	IP	接入设备	VLAN	端口索引	主机名	绑定类型	上线情况	事件类型	时间
0c11.0503.21d2	10.10.1.3				未绑定	上线成功		发送ack报文	2018/09/04 14:11:31
0c11.0503.21d2	10.10.1.2				未绑定	上线失败	PING检测失败。冲突IP10.10.1.2		2018/09/04 14:11:30
0c11.0503.21d2					未绑定	开始上线		收到discover报文	2018/09/04 14:11:30
0c11.0503.21d2	10.10.1.2				未绑定	上线成功		发送ack报文	2018/09/04 14:03:31
0c11.0503.21d2					未绑定	开始上线		收到discover报文	2018/09/04 14:03:29
0c11.0503.21d2	10.10.1.3				未绑定	上线成功		发送ack报文	2018/09/04 13:55:47
0c11.0503.21d2					未绑定	开始上线		收到discover报文	2018/09/04 13:55:45
0c11.0503.21d2	10.10.1.2				未绑定	上线失败	PING检测失败。冲突IP10.10.1.2		2018/09/04 13:55:45
0c11.0503.21d2	10.10.1.2				未绑定	上线成功		发送ack报文	2018/09/04 13:47:45
0c11.0503.21d2					未绑定	开始上线		收到discover报文	2018/09/04 13:47:43

显示第 1 到第 10 条记录, 总共 274 条记录 每页显示

10

条记录

<

1

2

3

4

5

>

go

(2) 上方搜索栏支持根据记录时间、终端IP、终端MAC、主机名、接入设备的IP/MAC、日志事件类型等条件筛选需要查看的日志。

8.10.7 DHCP 黑名单

【应用场景】

基于MAC地址添加黑名单，加入黑名单的客户端无法通过DHCP自动获取IP地址。

【操作步骤】

(1) 点击[网络]>>[DHCP配置]>>[DHCP黑名单]菜单项。

IPAM主页

IP智能管理

业务告警

DHCP配置管理

地址池使用概况

DHCP日志

DHCP黑名单

说明：基于MAC地址添加黑名单，清空详情会删除过滤的相关信息；过滤次数和过滤时间，不会删除对应的mac和备注信息。

✓ 选中删除

MAC地址

MAC必填，af09.af09.af09

备注

备注信息，可为空

添加

📄 导入配置

📄 下载模板

📄 导出数据

搜索

🔄

☐	MAC地址	过滤次数	主机名	接入设备IP	接入设备MAC	端口索引	最近过滤时间	VLAN	备注	操作
☐	2222.2312.4587	0		0.0.0.0	0000.0000.0000	0		0	大师傅士大夫	清空详情 删除
☐	1111.1111.1111	0		0.0.0.0	0000.0000.0000	0		0	哈哈	清空详情 删除
☐	6666.9999.2222	0		0.0.0.0	0000.0000.0000	0		0	test	清空详情 删除
☐	8888.3333.6666	0		0.0.0.0	0000.0000.0000	0		0	hehe	清空详情 删除

显示第 1 到第 4 条记录，总共 4 条记录

(2) 添加DHCP黑名单。

可通过以下几种方式添加DHCP黑名单：

- 输入MAC地址，点击<添加>。
- 点击<下载模板>，下载模板后填写对应的信息，并点击<导入配置>导入配置信息。

【后续处理】

- 点击<导出数据>可以导出已经配置的DHCP黑名单信息。
- 选择需要删除DHCP黑名单，点击<选中删除>可以删除对应的信息。

8.11 DHCP-V6 配置

说明

- 支持本功能的产品包括：NBR6205-E、NBR6205-E V2、NBR6135-E、NBR6210-E、NBR6210-E V2、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E。
- 前置条件：需要在[运维]>>[系统设置]>>[增强功能]中开启IPv6大容量功能（配置后需要重启设备以生效），Web页面才会显示DHCP-V6配置项。



8.11.1 功能简介

DHCPv6 (Dynamic Host Configuration Protocol for IPv6, IPv6动态主机配置协议) 是一种允许DHCPv6服务器将配置信息（如IPv6网络地址、DNS、NIS和SNTP服务器地址等参数）传递给IPv6节点的协议。

NBR网关设备可以作为DHCPv6服务器，为内网用户提供IPv6地址。

8.11.2 服务端配置

【操作步骤】

- (1) 点击[网络]>>[DHCP-V6配置]>>[服务端配置]菜单项。



(2) 点击<添加DHCP>。

三 添加DHCP

地址池名称：

*

IP分配网段：

* 格式：2000::1

前缀长度：

*

租用时间：

8

小时

*

首选DNS：

格式：3000::1

备用DNS：

关联接口：

☐ Gi0/0

☐ Gi0/5

☐ Te0/0

完成配置

取消

(3) 设置DHCPv6服务端配置项。

地址池名称： DHCPv6地址池名称。

IP分配网段： 网关设备作为DHCPv6服务端分配给内网用户的IPv6地址网段。

前缀长度： 用来确定分配的地址前缀范围。

租用时间： 在租用时间内，内网用户可通过网关设备自动获取IP地址，且IP地址不变。

首选DNS： DHCPv6服务首选使用的DNS服务器。

备选DNS： DHCPv6服务备选使用的DNS服务器。

关联接口：选择开启DHCPv6服务器功能的接口。

(4) 点击<完成配置>。

8.11.3 客户端列表

【应用场景】

通过该操作，可以查询已分配客户端的IP地址及客户端DUID的关系。

【操作步骤】

(1) 点击[网络]>>[DHCP-V6配置]>>[客户端列表]菜单项。

(2) 查询相关的信息。



已分配IP地址	客户端DUID	租期
无记录信息		

8.12 线路逃生

8.12.1 功能简介

可以设置定时探测线路是否正常，并在线路异常时，及时将该线路DOWN掉，使得应用流量能够从正常线路出去。

8.12.2 配置线路流量逃生

【注意事项】

- 该配置属于高危操作。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。
- 流量逃生与链路检测不能同时配置，请确认需要开启线路流量逃生的接口未开启链路检测后，再配置流量逃生。
- DHCP接口不支持线路逃生。

【操作步骤】

(1) 点击[网络]>>[线路逃生]>>[线路流量逃生]菜单项。

(2) 将“线路探测”设置为“开启”状态，一键开启线路流量逃生功能。

线路流量逃生

逃生日志

说明： 定时探测线路是否正常。在线路异常时，及时将该线路DOWN掉，使得应用能够从正常线路出去。
建议优先配置PING探测。开启PING检测时，当PING探测正常，则不会进行DNS和TCP探测。
同时开启DNS和TCP探测时，2个探测成功一个则视为线路正常，2个都失败，则视为线路异常。
配置探测目标为URL时，必须先在‘网络-DNS配置’页面中配置好DNS服务器。
TCP探测只针对80端口。

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。
配置流量逃生的接口，不能配置链路检测，请确认链路检测没有配置后，再配置流量逃生。
DHCP接口不支持线路逃生。

线路探测：☒ 开启

当线路探测失败时：☐ 只记录日志 ☒ 关闭接口并记录日志

开启探测接口：☐ Gi0/3 ☐ Gi0/6 ☐ Gi0/7 ☐ Gi0/9 ☐ di1 ☐ di2 ☐ di3

>> 高级设置

完成配置

- (3) 选择线路探测失败时的处理动作：默认当线路探测失败时，将会关闭接口并记录日志，可修改为“只记录日志”。
- (4) 勾选需要开启探测的接口，并配置各探测类型的目标地址。支持分别设置PING探测、DNS探测和TCP探测的目标地址。开启PING检测时，当PING探测正常，则不会进行DNS和TCP探测。同时开启DNS和TCP探测时，两类探测中成功一个则视为线路正常，DNS探测和TCP探测都失败，则视为线路异常。

i

说明

- 建议优先配置PING探测。
- 当探测目标配置为URL网址时，必须先在[网络]>>[DNS配置]>>[DNS服务器]页面中配置好DNS服务器（详见[8.4.2](#) 章节介绍），否则可能导致探测失败。

开启探测接口：☒ Gi0/3 ☐ Gi0/4

Gi0/3口 状态：未配置

PING探测：

DNS探测：

TCP探测：

?

- (5) 展开“高级设置”，设置高级选项。

高级设置

下行流量大于

50

%时不探测

接口UP时：探测频率

10

秒

探测确认时间

12

秒

接口UP，且探测失败时，探测频率会自动切换到接口DOWN时的探测频率。探测确认时间不变。

接口DOWN时：探测频率

3

秒

探测确认时间

60

秒

完成配置

(6) 点击<完成配置>。

8.12.3 查看逃生日志

【应用场景】

通过该操作，可以查看近期的逃生日志。

【操作步骤】

- (1) 点击[网络]>>[线路逃生]>>[逃生日志]菜单项。
- (2) 查看逃生日志的详细信息，包括：ID、时间、类型及具体消息。

线路流量逃生

逃生日志

高级查询

ID	时间	类型	消息
100	1970-01-01 00:01:26	关键事件	log database initialized.
99	1970-01-01 00:01:24	关键事件	log database initialized.
98	1970-01-01 00:01:14	关键事件	log database initialized.
97	1970-01-01 00:01:13	关键事件	log database initialized.
96	1970-01-01 00:01:09	关键事件	log database initialized.
95	1970-01-01 00:01:14	关键事件	log database initialized.

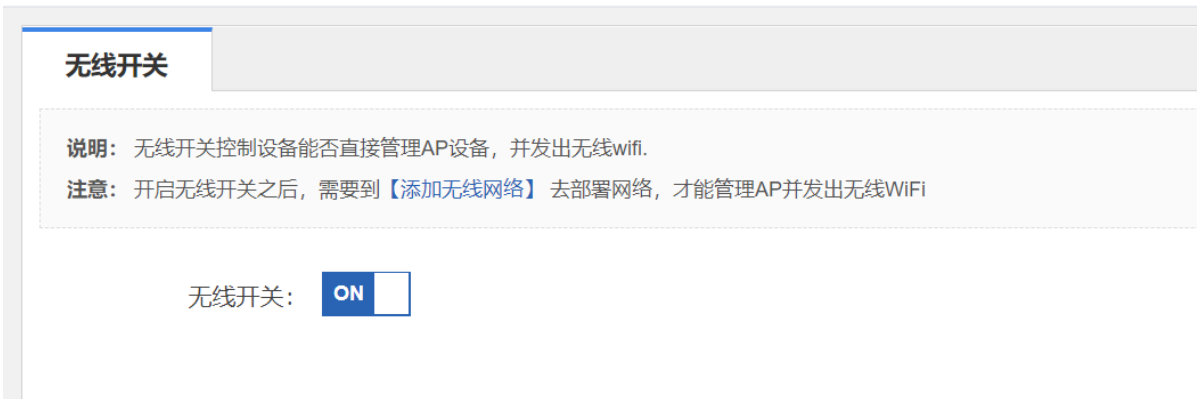
9 无线

9.1 无线开关

无线开关用于控制无线功能菜单的显示及配置，只有打开无线开关才能查看并配置无线功能。开启无线开关后，设备将会作为AC（Access Control）无线控制器通过有线网络与AP相连，对下联AP进行集中管理控制。

【操作步骤】

- (1) 选择[无线]>>[用户信息]。
- (2) 点击“无线开关”，将其置于ON状态，左侧导航菜单自动展示其他无线功能菜单。

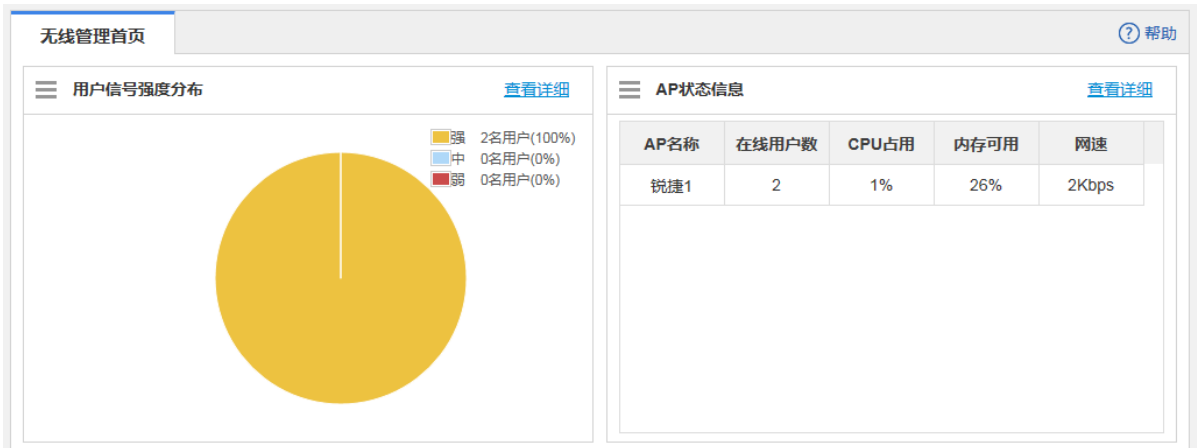


9.2 无线管理首页

本功能用于展示用户信号强度分布和关联AP状态信息。

【操作步骤】

- (1) 选择[无线]>>[无线管理首页]。



- (2) 在“用户信号强度分布”区域，点击<查看详细>进入[用户信息]页面，可以查看详细的用户信息和历史记录，点击<返回>可回到无线管理首页。

用户信息

历史记录

返回

输入MAC地址:

搜索

☐	客户端类型	用户名称	MAC地址	IP地址	IPv4网速	IPv6网速	连接AP	序列号	信号强度	在线时长	所在网络	操作
☐	XIAOMI Phone Android		3cbd 3e35 51f3	192.168.6.26	上行: 0Kbps 下行: 0Kbps	上行: 0Kbps 下行: 0Kbps	8005 8800 12e3	CAM70U7001564	强	0天00时09分34秒	aaa	详细 限速 加入黑名单
☐		??V40???-79eccb87ff4a80dd	e2 b5 b8 6d da 1c	192.168.6.23			Ruijie	CANL2R00146A	中	0天00时08分36秒	test	加入黑名单

显示

10

条 共2条

14

首页

<

上一页

1

下一页

>

末页

1

确定

(3) 在“AP状态信息”区域，点击<查看详细>进入[AP信息]页面，可以查看所有AP的详细信息或删除不在线AP，点击“返回”即可回到无线管理首页。

AP信息										
← 返回 X 删除所有不在线AP										
按照AP名称查询										搜索
AP名称	在线用户数	CPU占用	内存可用	网速(Kbps)	AP地址	MAC地址	所属AP组	位置	状态	操作
AP1						0011.0022.0033	默认组	教室1	不在线	删除
AP2						0011.0022.0044	默认组	教室2	不在线	删除
显示 10 条 共2条										
14 首页 < 上一页 1 下一页 > 末页 1 确定										

9.3 用户信息

本页面用于展示通过本设备提供的无线网络上网的用户信息。

【操作步骤】

- (1) 选择[无线]>>[用户信息]。
- (2) 点击操作列的<限速>或<加入黑名单>，您可以对这些用户执行限速或加入黑名单操作。

用户信息

← 返回

输入MAC地址：

搜索

☐	客户端类型	用户名	MAC地址	IP地址	IPv4网速	IPv6网速	连接AP	序列号	信号强度	在线时长	所在网络	操作
☐	XIAOMI Phone Android		3cbd.3e35.51f3	192.168.6.26	上行：0Kbps 下行：0.1Kbps	上行：0Kbps 下行：0Kbps	8005.8800.12e3	CAM70U7001564	强	0天00时01分55秒	aaa	详细 限速 加入黑名单
☐			e29f.9380.5439		上行：0Kbps 下行：0Kbps	上行：0Kbps 下行：0Kbps	8005.8800.12e3	CAM70U7001564	强	0天00时01分56秒	aaa	详细 限速 加入黑名单
☐		??V40???-79eccb87ff4a80dd	12.5a.b3.11.a0.83	192.168.6.22			Ruijie	CANL2R00146A	强	1天47时26分39秒	@Ruijie-s7FFE	加入黑名单

显示

10

条

共3条

14

首页

<

上一页

1

下一页

>

末页

1

确定

9.4 添加无线网络

9.4.1 功能介绍

配置无线网络并将其部署到AP后，无线终端用户能够通过AP释放的Wi-Fi信号上网。

9.4.2 无线网络[RGOS]

【应用场景】

本功能用于配置无线网络并将其部署到集成AC的AP。

【操作步骤】

- (1) 选择[无线]>>[添加无线网络]>>[无线网络[RGOS]]。
- (2) 在自动弹出的[确定您的拓扑]弹窗中，根据实际情况选择组网场景后，点击<下一步>。

确定您的拓扑

AP和用户的地址池在三层设备上

AP和用户地址池在NBR设备上

该拓扑上的三层交换机必须支持option 138

该拓扑只支持下联二层交换机

下一步

(3) 在[设备端的通信配置]页面，根据实际情况修改配置参数，点击<下一步>。

说明

AP与设备互联隧道IP即回环口（loopback）IP地址，是建立NBR网关设备与AP互联隧道的标识地址，可以配置为任意值。配置该地址的作用是让NBR网关设备更好的管理AP。

拓扑选择“AP和用户的地址池在三层设备上”，配置参数如下：

设备端的通信配置

设备通信AP的接口:

Gi0/0

选中接口的IP:

192.168.1.1

选中接口IP掩码:

255.255.255.0

AP与设备互联隧道IP:

3.3.33.3

上一步

下一步

拓扑选择“AP和用户的地址池在NBR设备上”时，需要配置AP地址池，具体配置参数如下：

308

设备端的通信配置

设备通信AP的接口:

Gi0/0

选中接口的IP:

192.168.1.1

选中接口IP掩码:

255.255.255.0

AP与设备互联隧道IP:

3.3.33.3

AP地址池名称:

pool_Gi0/0

IP分配范围:

至

首选DNS:

8.8.8.8

备用DNS:

上一步

下一步

(4) 在[配置WiFi/Wlan]页面，根据实际情况修改Wi-Fi参数，点击<下一步>。

 说明

加密类型支持以下两种：

- 1. WPA/WPA2-PSK（通用版）：基于共享密钥的WPA模式，安全性高，设置比较简单，适合普通家庭用户和小型企业使用。
- 2. 不加密：无需密码即可连接上Wi-Fi。

设置最大无线用户数后，超过数量的用户不能连接该Wi-Fi。

配置WiFi/Wlan

WiFi网络名称:

Eweb_33F61

加密类型:

WPA/WPA2-PSK(通用版)

WiFi密码:

ewebwifi

☒ 显示密码

高级配置

WiFi是否可见:

☐ 隐藏(让别人看不到，只能手动添加WiFi)

最大无线用户数:

关闭网络时间:

永不关闭

优先接入5G网络:

☐ OFF

上一步

下一步

(5) 选择关联AP组、DHCP服务配置位置及支持的网络类型，并输入VLAN ID，点击<完成配置>。

 说明

点击操作列的<添加>按钮，可以新增一条上网配置。

三 无线用户的上网配置

关联AP组

无线用户VLAN ID

无线用户DHCP服务

支持网络类型

操作

默认组

1

配在三层交换机上

2.4G,5G网络都支持

✕ + 添加

上一步

完成配置

(6) 点击关联AP组列的图标，可查看或删除该AP组下的AP。

三 “默认组”组包含的AP列表

序号	AP名称	在线状态	操作
1	8005.8800.12e3	不在线	删除

显示: 5 条共1条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶

1 确定

(7) 点击操作列的<限速>链接，可以设置无线网络限速值。配置完成点击<保存>即可。

☐	Wifi网络名称	关联AP组	关联的用户数	操作
☐	Eweb_33F61	默认组 	0	编辑 限速 详情

显示: 10 条共1条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶

1 确定

限制下载: 不限速 ×8kb/s

限制上传: 不限速 ×8kb/s

保存 不限速

(8) （可选）无线网络添加完成后，如需修改NBR设备端的通信配置，可以点击<修改NBR端配置>进行修改。

无线网络[RGOS]

说明: 1.不支持VRRP场景 2.不支持WEB与CLI混合配置

注意: 1、已知部分手机型号，不支持中文的Wifi网络名称。故不建议配置中文的Wifi网络名称。
2、无线网络的认证方式选择WPA/WPA2-802.1X(企业版)，会导致WEB认证无感知、商业营销认证获取MAC地址、本地服务器认证获取MAC地址功能失效。

+ 添加Wifi

✕ 删除选中Wifi

修改NBR端配置

更改拓扑

☐	Wifi网络名称	关联AP组	关联的用户数	操作
☐	Eweb_33F61	默认组 	0	编辑 限速 详情

显示: 10 条共1条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶

1 确定

(9) （可选）无线网络添加完成后，如需修改拓扑（AP和地址池的配置位置），可以点击<更改拓扑>进行修改。

 **注意**
更改拓扑会删除删除所有WiFi，请谨慎操作。

无线网络[RGOS]

说明：1.不支持VRRP场景 2.不支持WEB与CLI混合配置

注意：1、已知部分手机型号，不支持中文的Wifi网络名称。故不建议配置中文的Wifi网络名称。
2、无线网络的认证方式选择WPA/WPA2-802.1X(企业版)，会导致WEB认证无感知、商业营销认证获取MAC地址、本地服务器认证获取MAC地址功能失效。

+ 添加Wifi

✕ 删除选中Wifi

✎ 修改NBR端配置

✎ 更改拓扑

☐	Wifi网络名称	关联AP组	关联的用户数	操作
☐	Eweb_33F61	默认组 	0	编辑 限速 详情

显示: 10 ▾ 条 共1条

⏪ 首页

⏴ 上一页

1

⏵ 下一页

⏩ 末页

1

确定



9.4.3 无线网络[Reyee OS]

【应用场景】

本功能用于配置无线网络并将其部署到睿易AP。

【前置条件】

您已配置“发现新网络”功能，并且接入了睿易AP设备。有关“发现新网络”功能的详细介绍请参见[3.2 睿易一体化配置](#)。

【操作步骤】

- (1) 选择[无线]>>[添加无线网络]>>[无线网络[Reyee OS]]。
- (2) 选择无线网络所属分组，点击<添加WiFi>，进入[添加WiFi]页面。

无线网络[RGOS]

无线网络[Reyee OS]

提示：修改配置会重启无线配置，可能导致当前连接的终端掉线。

说明：每个分组最大支持配置8个Wi-Fi。

1

2

分组: 默认组 ▾

+ 添加Wifi

Wifi网络名称	应用频段	加密类型	是否隐藏	VLAN ID	操作
@Ruijie-s7FFE	2.4G + 5G	OPEN	否	与AP同VLAN	编辑

显示: 10 ▾ 条 共1条

⏪ 首页

⏴ 上一页

1

⏵ 下一页

⏩ 末页

1

确定



- (3) 输入WiFi名称，根据实际情况选择WiFi网络名称编码、频段及加密类型。

-  说明

 - WiFi网络名称编码默认为UTF-8，若WiFi名称显示为乱码请切换到其他编码格式。
 - 加密类型设置为WPA-PSK/WPA2-PSK表示：基于共享密钥的WPA模式，安全性高，设置比较简单，适合普通家庭用户和小型企业使用。
 - 加密类型设置为不加密表示：无需密码即可连接上Wi-Fi。

添加WiFi

WiFi网络名称:

WiFi网络名称编码: UTF-8

应用频段: 2.4G + 5G

加密类型: 不加密

高级配置

确定 取消

(4) 点击“高级配置”设置WiFi高级属性。



说明

- 选择时段表示选择WiFi生效时间段。
- VLAN字段可以设置通过该WiFi上网的用户是否与部署该WiFi的AP处于同一个VLAN。

添加WiFi

高级配置

选择时段: 所有时段

VLAN: 用户与AP同VLAN

隐藏Wi-Fi: ☐ (让别人看不到WiFi热点, 只能手动添加)

用户隔离: ☐ (隔离接入该WiFi的用户)

5G优先: ☐ (支持5G的终端优先关联到5G)

竞速模式: ☐ (开启后体验更快的上网速度)

三层漫游: ☐ (支持5G的终端优先关联到5G)

确定 取消

(5) 确认配置无误, 点击<确定>即可。

9.5 AP 管理

9.5.1 功能介绍

在WLAN网络中, AP必需与某个AC建立连接, 并且加入一个AP组, 才能正常为无线用户提供服务。在本功能中, NBR设备相当于一个AC设备, 用于与AP建立连接并管理AP。

AP上线以后将会被NBR设备自动识别并加入默认组。

9.5.2 AP 管理[RGOS]

【应用场景】

本功能用于远程管理集成AC的AP。

【操作步骤】

(1) 选择[无线]>>[AP管理]>>[AP管理[RGOS]]。

(2) 添加AP组：

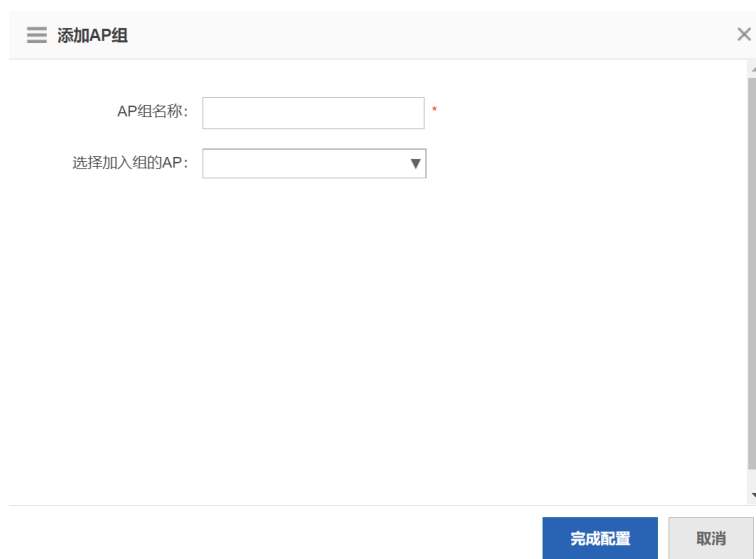
说明

设备提供默认组，你也可以将AP加入“默认组”进行管理。

a 点击<添加组>，进入[添加AP页面]。



b 输入AP组名称，并选择要加入该组的AP，点击<完成配置>。



(3) 添加AP：

a 选择一个AP组，点击<添加AP>，进入[添加AP]页面。



b 输入AP信，点击<完成配置>

三

添加AP

×

AP名称:

*

MAC地址:

*

所在位置:

(不支持多个中文标点符号)

高级设置

归属组:

test

▼

Telnet管理AP账号:

Telnet管理密码:

□ 显示密码

完成配置

取消

(4) 管理AP，您可以根据需求对选中的AP执行以下操作：

○ 删除AP：

在AP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<确定>，可批量删除AP。



○ 重启AP

在AP列表中选择一条或多条记录，点击<重启AP>，在弹出的确认窗口中点击<确定>，可批量重启AP。

i 说明

重启功能只对在线的AP生效。



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>，在弹出的确认窗口中点击<确定>，可批量对AP进行恢复出厂设置操作。

说明

恢复出厂设置功能只对在线的AP生效，恢复出厂设置将会清空AP中现有配置，请谨慎操作。



9.5.3 AP 管理[Reyee OS]

【应用场景】

本功能用于远程管理睿易AP。

【前置条件】

您已配置“发现新网络”功能，并且接入了睿易AP设备。有关“发现新网络”功能的详细介绍请参见[3.2 睿易一体化配置](#)。

【操作步骤】

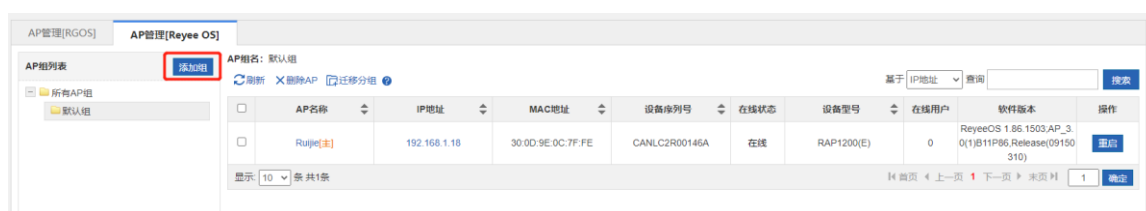
(1) 选择[无线]>>[添加无线网络]>>[无线网络[Reyee OS]]。

(2) 添加AP组：

说明

设备提供默认组，通过“发现新网络”功能发现的AP都会被加入“默认组”。您可以新建AP组后，将其迁移到新的AP组中，也可以通过默认组对其进行管理。

a 点击<添加组>，进入[添加AP页面]。



b 输入AP组名称，点击<完成配置>。

添加AP组

×

AP组名称:

完成配置

取消

(3) 为新建的AP添加AP :

a 选中默认组，勾选要迁移的AP，点击<迁移分组>。

说明

不在线的AP被迁移到新AP组后，必须等该AP重新上线后，才能在新AP组查看到该AP信息。



b 选择新建的AP组名称，点击<完成配置>。

迁移分组

×

归属组:

完成配置

取消

(4) 管理AP，您可以根据需求对选中的AP执行以下操作：

○ 修改AP名称：

点击AP名称，可以修改AP名称。



○ 登录AP Web管理页面：

点击AP的IP地址，可以跳转到AP的web登录页面。



○ 删除AP：

在AP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<确定>，可批量删除AP。



○ 重启AP：

找到目标AP，点击操作列的<重启>按钮，在弹出的确认窗口中点击<确定>，即可重启AP。



9.6 AP 升级

9.6.1 AP 升级[RGOS]

【应用场景】

本功能用于对集成AC的AP进行远程版本升级，支持单个AP升级和批量升级两种方式。

【前置条件】

您已通过锐捷官网获取对应的AP的最新软件版本文件。

【操作步骤】

- (1) 选择[无线]>>[AP升级]>>[AP升级[RGOS]]。
- (2) 根据需要选择以下任意一种升级方式：

○ 单个AP升级

选择目标AP，点击操作列<升级>按钮，进入[升级AP]页面。

AP名称	产品型号	mac地址	当前版本信息	操作
锐捷1	AP330-I	00d0.f822.340a	AP_RGOS 11.1(5)B7	升级

显示: 10 条 共1条

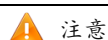
首页 < 上一页 1 下一页 > 末页

点击<浏览>，选择上传最新软件版本，点击<开始升级>，等待升级即可。



- 批量升级

将AP批量升级开关置于ON状态，然后点击<上传软件版本>。



注意

批量升级时，请确保所选的版本文件适用于所有AP，否则会导致AP异常。



在[软件版本]弹窗中，点击<选择文件>，选择上传最新的软件版本文件，点击<开始升级>即可同时升级多台AP设备。



9.6.2 AP 升级[Reyee OS]

【应用场景】

本功能用于对睿易AP进行远程升级软件版本，支持在线升级和本地升级两种升级方式。

【前置条件】

您已配置“发现新网络”功能，并且接入了睿易AP设备。有关“发现新网络”功能的详细介绍请参见[3.2 睿易一体化配置](#)。

进行本地升级前，请确保您已通过锐捷官网获取对应的AP的最新软件版本文件。

【操作步骤】

(1) 选择[无线]>>[AP升级]>>[AP升级[Reyee OS]]。

(2) 根据实际情况选择在线升级或本地升级：

○ 在线升级：

选择软件版本带“new”标志的AP，点击<在线升级>，即可在线升级AP的软件版本。



AP名称	IP地址	MAC地址	设备序列号	软件版本	在线状态	本地升级	设备型号	在线用户	所在分组
Ruijie [主]	192.168.6.18	30 0D 5E 0C 7F FE	CANLC2R00146A	AP_3.0(1)B11P50.Release(08133002)	在线	本地升级	RAP1200(E)	0	默认组

○ 本地升级：

选择软件版本带“new”标志的AP，点击<本地升级>将会跳转到AP的Web登录页面，登录后可在AP上进行升级操作。



AP名称	IP地址	MAC地址	设备序列号	软件版本	在线状态	本地升级	设备型号	在线用户	所在分组
Ruijie [主]	192.168.6.18	30 0D 5E 0C 7F FE	CANLC2R00146A	AP_3.0(1)B11P50.Release(08133002)	在线	本地升级	RAP1200(E)	0	默认组

9.7 DHCP 安全

开启DHCP安全功能后，设备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。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。

【操作步骤】

(1) 选择[无线]>>[DHCP安全]。

(2) 点击“DHCP安全”开关，将其置于ON状态。

(3) （可选）在“防止WiFi下IP冲突”后面的下拉列表中选择WiFi网络，可以防止所选WiFi下的终端出现IP地址冲突的情况。



说明

点击“无线管理”可以查看和编辑WiFi配置。



DHCP安全

说明： 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。

注意： 开启该功能，会导致WEB认证无感知、商业营销认证获取MAC地址、本地服务器认证获取MAC地址功能失效。

DHCP安全： ☒ ON

防止WiFi下IP冲突： [【无线管理】](#)

信息列表： [【查看DHCP安全信息】](#) [【查看合法用户信息】](#)

[保存设置](#)

(4) 点击<保存配置>。

9.8 反制非法 AP

非法AP是指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设备等。开启反制非法AP功能可以阻止这些非法AP设备继续工作，避免用户接入到非法AP。

【操作步骤】

- (1) 选择[无线]>>[反制非法AP]。
- (2) 点击“反制非法AP”开关，将其置于ON状态。

反制非法AP配置

要被反制的非法AP列表

信任设备列表

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！

反制非法AP：☒

[【扫描到所有的相邻AP】](#)

反制模式：☐ 发现非同一AC下的无线设备发出的相同wifi名称信号,然后对其反制

☐ 属于非AP模拟出来的信号（如：笔记本或手机等设备模拟发出的信号）

☐ 根据信号强度

☐ 手动添加需要反制的无线设备MAC

反制范围：☒ 只对本设备同一信道下的进行扫描/反制

☐ 对所有信道下设备都进行扫描/反制（会消耗较大的设备性能）

保存设置

- (3) 选择反制模式和反制范围，点击<保存配置>。
- (4) （可选）点击进入[要被反制的非法AP列表]页签，可以查看被反制的非法AP列表。点击<清空非法AP>按钮可以删除非法AP信息。

⚠ 注意

清空非法AP列表只是在本页面删除了数据，原来添加的AP依旧会被反制，如需解除反制，请将其添加到信任设备列表。

反制非法AP配置

要被反制的非法AP列表

信任设备列表

反制模式：

检测到非同一AC设备的AP设备

每一分钟刷新一次

清空非法AP

基于WiFi名称查询：

搜索

WIFI名称	MAC地址	信道	速率(Mbps)	信号强度
无记录信息				

显示：

10

条 共0条

◀ 首页 ◀ 上一页 下一页 ▶ 末页 ▶ 1 确定

- (5) （可选）点击进入[信任设备列表]页签，可以添加信任设备。添加到信任设备列表的AP不会被认为是非法AP。输入设备MAC地址或厂商MAC地址，点击<保存设置>即可添加信任设备。

 说明

若只配置厂商唯一标识符，则该厂商的设备都是可信任设备；若同时配置了厂商唯一标识符和对应的WiFi，则同时满足厂商唯一标识符和WiFi名称才是可信任设备。

反制非法AP配置

要被反制的非法AP列表

信任设备列表

说明：以下配置的MAC地址对应的设备将不会被认为是非法AP,是不会被反制的AP设备,是信任设备

信任设备MAC地址：

+ 增加 MAC 地址

信任厂商列表

厂商唯一标识符：

+ 增加 MAC 地址

多对多关系

厂商唯一标识符对应的WiFi名称：

+ 增加 WiFi

保存设置

点我咨询

9.9 黑白名单[RGOS]

黑白名单用于设置是否允许无线用户通过Wi-Fi上网。通过禁止或允许MAC地址对应的客户端（如您的手机、笔记本电脑等）连接WiFi网络来实现用户上网控制：

- 黑名单：名单中的MAC地址对应的用户将被禁止上网，未加入名单的设备不限制。
- 白名单：只有名单中的MAC地址对应的用户能够上网，未加入名单的设备都禁止。

【应用场景】

本功能针对通过集成AC的AP上网的用户进行联网控制。

【操作步骤】

- (1) 选择[无线]>>[黑白名单RGOS]>>[黑白名单配置]。
- (2) 根据需求选择添加黑名单或白名单：

 注意

从黑名单模式切换到白名单模式时，原有的黑名单配置会被清空；从白名单模式切换到黑名单模式时，原有的白名单配置会被清空，请谨慎操作。

○ 添加黑名单

名单类型选择 “禁止以下MAC地址接入WiFi上网（黑名单）”

黑白名单配置

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！

名单类型：☒ 禁止以下MAC地址接入WiFi上网（黑名单） ☐ 仅允许以下MAC地址接入WiFi上网（白名单）

[+ 添加黑名单](#) [批量导入黑名单](#) 基于MAC地址查询 [搜索](#)

☐	MAC地址	操作
无记录信息		

显示: 条 共0条 ◀ 首页 ◀ 上一页 下一页 ▶ 末页 ▶ [确定](#)

点击<添加黑名单>，输入MAC地址。如需添加多个MAC地址，点击<添加>按钮可以继续添加。

添加黑名单 ×

MAC地址: ✕ [+ 添加](#)

[确定](#) [取消](#)

配置完成后，点击<确定>即可将所有输入的MAC加入黑名单。

○ 添加白名单

名单类型选择 “仅允许以下MAC地址接入WiFi上网（白名单）”

黑白名单配置

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！

名单类型：☐ 禁止以下MAC地址接入WiFi上网（黑名单） ☒ 仅允许以下MAC地址接入WiFi上网（白名单）

[+ 添加白名单](#) [批量导入白名单](#) 基于MAC地址查询 [搜索](#)

☐	MAC地址	操作
无记录信息		

显示: 条 共0条 ◀ 首页 ◀ 上一页 下一页 ▶ 末页 ▶ [确定](#)

点击<添加白名单>，输入MAC地址。如需添加多个MAC地址，点击<添加>按钮可以继续添加。

添加白名单 ×

MAC地址: ✕ [+ 添加](#)

[确定](#) [取消](#)

配置完成后，点击<确定>即可将所有输入的MAC加入白名单。

9.10 黑白名单[Reyee OS]

9.10.1 全局黑白名单

全局黑白名单用于设置是否允许无线用户通过WiFi上网。通过禁止或允许MAC地址对应的客户端（如您的手机、笔记本电脑等）连接WiFi网络来实现用户上网控制：

- 黑名单：名单中的MAC地址对应的用户将被禁止上网，未加入名单的设备不限制。
- 白名单：只有名单中的MAC地址对应的用户能够上网，未加入名单的设备都禁止。

【应用场景】

本功能针对通过睿易AP上网的用户进行联网控制。

【前置条件】

您已配置“发现新网络”功能，并且接入了睿易AP设备。有关“发现新网络”功能的详细介绍请参见[3.2 睿易一体化配置](#)。

【操作步骤】

- (1) 选择[无线]>>[黑白名单Reyee OS]>>[全局黑白名单]。
- (2) 根据需求选择添加黑名单或白名单：

⚠ 注意

从黑名单模式切换到白名单模式时，原有的黑名单配置会被清空；从白名单模式切换到黑名单模式时，原有的白名单配置会被清空，请谨慎操作。

○ 添加黑名单

名单类型选择“禁止以下MAC地址接入WiFi上网（黑名单）”

全局黑白名单 基于SSID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！
提示：切换模式后，请到 无线—黑白名单[RGOS]—黑白名单配置 页面同步模式。

名单类型：☒ 禁止以下MAC地址接入WiFi上网（黑名单） ☐ 仅允许以下MAC地址接入WiFi上网（白名单）

+ 添加黑名单 × 删除选中黑名单 提示：最大支持配置30个名单。 基于MAC地址查询 搜索

☐	MAC地址	备注	操作
无记录信息			

显示: 10 条 共0条

首页 上一页 下一页 末页 1 确定

点击<添加黑名单>，选择匹配规则，输入MAC地址或MAC地址前缀以及备注信息。

添加黑名单

×

规则：☒ 完全匹配 ☐ 匹配前缀(OUI)

MAC地址：

格式：00:11:22:33:44:55

*

备注：

确定

取消

点击<确定>即可将指定MAC地址加入黑名单。

○ 添加白名单

名单类型选择“仅允许以下MAC地址接入WiFi上网（白名单）”

全局黑白名单

基于SSID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！

提示：切换模式后，请到 无线—黑白名单[RGOS]—黑白名单配置 页面同步模式。

名单类型：☐ 禁止以下MAC地址接入WiFi上网（黑名单） ☒ 仅允许以下MAC地址接入WiFi上网（白名单）

+ 添加白名单

✕ 删除选中白名单

提示：最大支持配置30个名单。白名单列表为空不生效，即所有MAC均可接入。

基于MAC地址查询

搜索

☐	MAC地址	备注	操作
无记录信息			

显示：10 条 共0条

首页

上一页

下一页

末页

1

确定

点击<添加白名单>，选择匹配规则，输入MAC地址或MAC地址前缀以及备注信息。

添加白名单

×

规则：☒ 完全匹配 ☐ 匹配前缀(OUI)

MAC地址：

格式：00:11:22:33:44:55

*

备注：

确定

取消

点击<确定>即可将指定MAC地址加入白名单。

324

9.10.2 基于 SSID 黑白名单

SSID即Wi-Fi名称，无线用户使用无线网卡搜索SSID发现网络并接入。通过设置基于SSID的黑白名单，可以控制用户是否能接入某个Wi-Fi网络进行联网：

- 黑名单：名单中的MAC地址对应的用户将被禁止接入指定Wi-Fi，未加入名单的设备不限制。
- 白名单：只有名单中的MAC地址对应的用户能够接入指定Wi-Fi，未加入名单的设备都禁止。

【应用场景】

本功能针对通过睿易AP上网的用户进行联网控制。

【前置条件】

您已配置“发现新网络”功能，并且接入了睿易AP设备。有关“发现新网络”功能的详细介绍请参见[3.2 睿易一体化配置](#)。

【操作步骤】

- (1) 选择[无线]>>[黑白名单Reyee OS]>>[基于SSID黑白名单]。
- (2) 选择无线网络所属分组，点击选中网络名称。

全局黑白名单

基于SSID黑白名单

说明：无线黑白名单的作用是拒绝/允许无线用户接入Wi-Fi联网。

注意：“OUI匹配规则”和“基于SSID”的黑白名单仅睿易网络且P32及以上版本支持。

规则：1、黑名单模式下，添加到黑名单列表里的终端无法连接Wi-Fi。2、白名单模式下且列表不为空时，未添加到白名单列表里的终端无法连接Wi-Fi。

分组：

默认组

1

@Ruijie-s7FFE2

名单类型：☒ 禁止以下MAC地址接入WiFi上网（黑名单）☐ 仅允许以下MAC地址接入WiFi上网（白名单）

+ 添加黑名单

✕ 删除选中黑名单

提示：最大支持配置30个名单。

☐	MAC地址	备注	操作
无记录信息			

显示：

10

条 共0条

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶

1

确定

- (3) 根据需求选择添加黑名单或白名单：

⚠ 注意

从黑名单模式切换到白名单模式时，原有的黑名单配置会被清空；从白名单模式切换到黑名单模式时，原有的白名单配置会被清空，请谨慎操作。

○ 添加黑名单

名单类型选择“禁止以下MAC地址接入WiFi上网（黑名单）”

全局黑白名单

基于SSID黑白名单

说明：无线黑白名单的作用是拒绝/允许无线用户接入Wi-Fi联网。

注意：“OUI匹配规则”和“基于SSID”的黑白名单仅支持网络自P32及以上版本支持。

规则：1、黑名单模式下，添加到黑名单列表里的终端无法连接Wi-Fi。2、白名单模式下且列表不为空时，未添加到白名单列表里的终端无法连接Wi-Fi。

分组：

默认组

@Ruijie-s7FFE

名单类型：

禁止以下MAC地址接入WiFi上网（黑名单）

仅允许以下MAC地址接入WiFi上网（白名单）

+添加黑名单

×删除选中黑名单

提示：最大支持配置30个名单。

☐	MAC地址	备注	操作
无记录信息			

显示：

10

条 共0条

◀ 首页 ◀ 上一页 下一页 ▶ 末页 ▶

1

确定

点击<添加黑名单>，选择匹配规则，输入MAC地址或MAC地址前缀以及备注信息。

添加黑名单

×

规则：

完全匹配

匹配前缀(OUI)

MAC地址：

格式：00:11:22:33:44:55

*

备注：

确定

取消

点击<确定>即可将指定MAC地址加入黑名单。

○ 添加白名单

名单类型选择 “仅允许以下MAC地址接入WiFi上网（白名单）”



点击<添加白名单>，选择匹配规则，输入MAC地址或MAC地址前缀以及备注信息。



(4) 点击<确定>即可将指定MAC地址加入白名单。

9.11 射频[Reyee OS]

睿易AP设备在开机时能够检测周围无线环境并选择合适的配置。但无法避免无线环境变化而引起的网络卡顿。用户可以分析AP和路由器周围的无线环境，手动选择合适的参数。

【前置条件】

您已配置“发现新网络”功能，并且接入了睿易AP设备。有关“发现新网络”功能的详细介绍请参见[3.2 睿易一体化配置](#)。

【操作步骤】

- (1) 选择[无线]>>[射频Reyee OS]>>[射频设置]。
- (2) 选择无线网络所属分组。

⚠ 注意

修改配置会重启无线配置，可能导致当前连接的终端掉线。请谨慎操作。

射频设置

提示：修改配置会重启无线配置，可能导致当前连接的终端掉线。

分组：

默认组

国家码

中国(CN)

2.4G 频宽

自动

5G 频宽

自动

最大用户数

64

最大用户数

128

保存设置

表9-1 射频配置信息描述表

参数	说明
国家码	各国规定的Wi-Fi信道有可能不同。为防止终端搜索不到Wi-Fi，请选择实际所在的国家或地区
2.4G/5G频宽	频宽小网络较稳定，频宽大易受干扰。若干扰较严重，选择较低的频宽能够一定程度上避免网络卡顿。2.4GHz频段支持20MHz和40MHz的频宽，5GHz频段支持20MHz、40MHz和80MHz的频宽。 默认为“自动”，表示自动根据环境选择频宽
最大用户数	大量用户接入AP或路由器上，可能导致无线网络性能下降，影响用户上网体验。设置最大用户数后，当接入用户达到阈值，将禁止新用户接入。若接入终端带宽需求较高，可调低最大用户数。无特殊情况建议保持默认

 说明

- 可选无线信道与国家码有关，请正确选择所在的国家或地区的国家码。
- 信道、功率和漫游灵敏度不支持全局设置，需要在对应设备上单独设置。

9.12 禁止内网互访

配置禁止内网互访功能，可以在不影响用户正常上网的情况下，对用户进行隔离，使内网用户之间不能互相访问，从而保证用户业务的安全。目前仅支持二层隔离。

【操作步骤】

- (1) 选择[无线]>>[禁止内网互访]。
- (2) 点击“禁止内网用户互访”开关，将其置于ON状态。

(3) 选择用户类型，并输入允许互访的用户MAC。

说明

允许互访的用户MAC即例外MAC地址，这些MAC地址对应的用户不受限制，可以互相访问。点击<添加>按钮可以添加多个MAC。

(4) 配置完成后，点击<保存配置>。

9.13 WIS

设备支持接入WIS云，通过WIS云对设备进行一键诊断、一键网优和移动运维等操作。有关WIS云的详细介绍，请参考其配套的用户手册。

【前置条件】

您已购买并部署WIS云。

设备与WIS云之间网络互通。

【操作步骤】

- (1) 选择[无线]>>[禁止内网互访]。
- (2) 点击“网优功能”开关，将其置于ON状态。

(3) 登录[WIS官网](http://wispi.ruijie.com.cn)，完成WIS云账号注册，并根据提示完成设备接入。

9.14 负载均衡

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，因此可能会出现某台AP负载较重、网络利用率较差的情况。通过配置负载均衡组，将同一区域的AP都划到同一个组内，协同控制无线用户的接入，实现资源的有效利用。

【操作步骤】

- (1) 选择[无线]>>[负载均衡]。
- (2) 点击<添加均衡组>，进入[添加均衡组]页面。

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。

举例：AP1当前已关联用户15个，AP2关联10个，当前配置阈值2个。这两个AP间用户数差5个，大于阈值，因此后续用户会关联到AP2上。

+ 添加均衡组

✕ 删除选中均衡组

☐	均衡组名	类型	阈值	组内AP成员	操作
无记录信息					

显示: 10 条 共0条

◀ 首页 ◀ 上一页 下一页 ▶ 末页 ▶ 1 确定

- (3) 输入均衡组信息。

添加均衡组

均衡组名:

*

均衡类型:

按照关联用户数均衡

▼

用户数门限值:

3

?

关联用户数差值达到:

3

个时实现均衡

组内AP成员:

▼

*

完成配置

取消

配置项	说明
均衡组名	负载均衡组的唯一标识

配置项	说明
均衡类型	- 按照关联用户数均衡 需要设置用户数门限值和关联用户数差值 当组内所有AP关联的用户数超过设置的用户数门限值，并且AP之间的关联用户数差值大于设置关联用户数差值时进行负载均衡，将后续上网的用户关联到用户较少的AP上 - 按照AP上流量均衡 需要设置流量门限值和流量差值 当组内所有AP流量超过设置的流量门限值，并且AP之间的流量差值大于设置流量差值时进行负载均衡，将后续上网的用户关联到流量较少的AP上
组内AP成员	属于同一个组的AP之间进行负载均衡

(4) 确认配置无误，点击<完成配置>。

9.15 整网管理

Master设备是通过SMB自发现协议，在整个网络中选举出来的一台设备，用来管理整个网络的其他设备。通过整网管理功能可以跳转到master设备的登录页面。

【前置条件】

您已配置“发现新网络”功能，并且接入了睿易AP设备。有关“发现新网络”功能的详细介绍请参见[3.2 睿易一体化配置](#)。

【操作步骤】

- (1) 选择[无线]>>[整网管理]。
- (2) 浏览器会新建一个窗口跳转到master设备登录页面。



你好, EAP201

 请输入设备密码...

登录

[忘记密码?](#)

10 防火墙

防火墙功能能够检测出多种类型的网络层攻击，并根据配置的策略采取相应的措施，避免内部网络遭受恶意攻击，从而保证内部网络的正常运行。

说明

- NBR6205-E、NBR6205-E V2、NBR6135-E、NBR6210-E、NBR6210-E V2、NBR6215-E支持防火墙功能。
- NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G不支持防火墙功能。

10.1 防攻击配置

网关设备通常部署在内网出口位置，经过网关的流量有正常的业务流量，也有恶意攻击流量。在网关上开启防攻击功能并配置相应策略后，可以对流经网关的攻击流量进行检测和阻断，保障内网安全。

防攻击配置支持全局防护策略、协议类策略和域策略，它们的优先级从大到小为：协议类策略> 域策略 > 全局防护策略。

10.1.1 防攻击开关

防攻击开关用于控制防攻击功能菜单的显示及配置，只有打开防攻击开关才能查看并配置防攻击功能。开启防攻击开关后，设备按预定义的防护策略对设备本身和内网进行防护，您也可以根据实际需求新增防护策略。

【操作步骤】

- (1) 选择[防火墙]>>[防攻击配置]>>[防攻击开关]。
- (2) 勾选开启防攻击功能，点击<保存>。



10.1.2 全局防护

全局防护是针对网关设备本身实施的防护。全局防护的工作原理是通过限制会话的建立速率来确保设备自身资源的有效使用，可以有效预防资源消耗类攻击，避免设备产生拒绝服务。

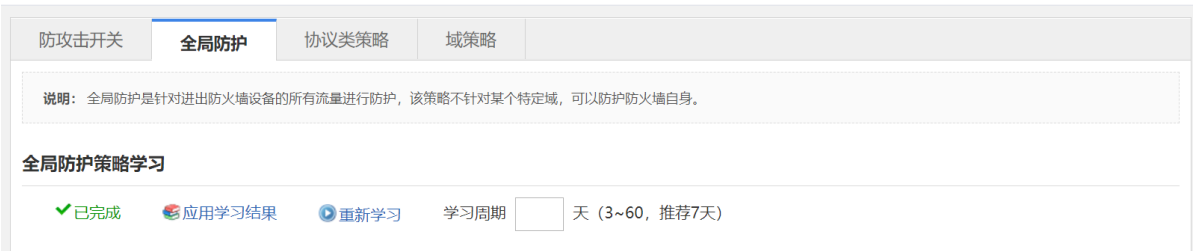
【操作步骤】

- (1) 选择[防火墙]>>[防攻击配置]>>[全局防护]。
- (2) 点击<开始学习>，设备将会通过自学习的方式获取适合当前网络环境的最优防护阈值。

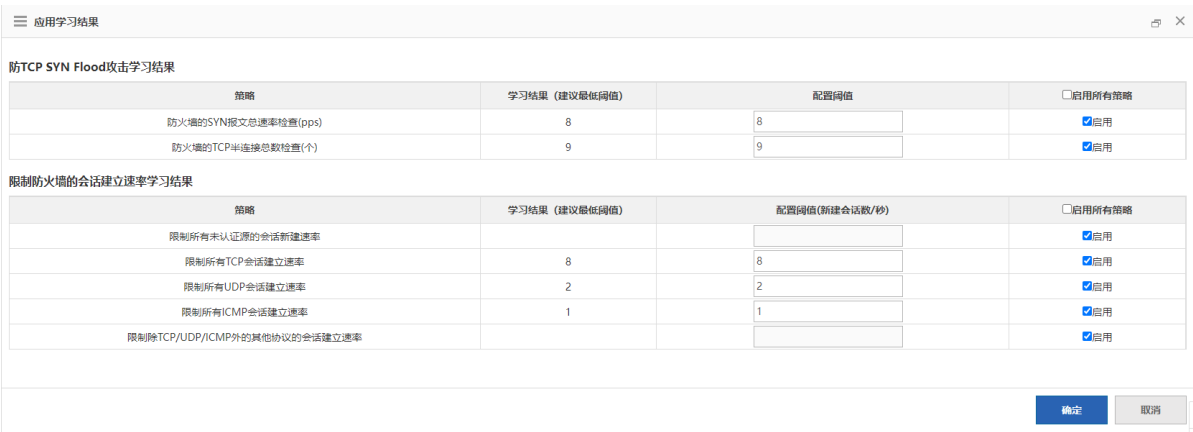
注意

- 为保证学习到的策略效果更好，请确保自学习周期内包含流量高峰期。
- 学习时长默认为7天，您也可以根据实际情况中断学习或设置新的学习时长。

- 当网络规模发生变化后，建议重新学习并应用新的学习结果。



(3) 学习完成后，点击<应用学习结果>，参考学习结果，结合当前网络实际情况调整配置阈值。



(4) 配置完成后，点击<确定>。

10.1.3 协议类策略

协议类攻击主要是针对协议运行机制的漏洞发起的攻击，开启对应协议开关，设备将会过滤符合攻击特征的协议报文。

【操作步骤】

- (1) 选择[防火墙]>>[防攻击配置]>>[协议类策略]。
- (2) 根据实际需求点击开启对应的开关，即可生效指定类型的防攻击策略。

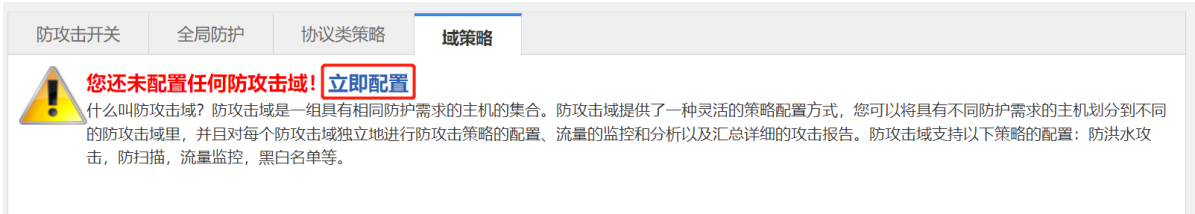


10.1.4 域策略

防攻击域是具有相同防护需求的主机的集合。您可以根据实际情况将具有不同防护需求的主机划分到不同的域，进行分类保护，独立管理。针对不同的域配置不同的防护策略，从而实现精准防护。

【操作步骤】

- (1) 选择[防火墙]>>[防攻击配置]>>[域策略]。
- (2) 点击<立即配置>，进入[新建防攻击域配置向导]页面。



- (3) 输入防攻击域名称、描述和保护主机范围，点击<下一步>。

说明

保护主机范围支持单个IP地址（如1.1.1.1）、子网/掩码长度（如1.1.1.0/24）、子网/掩码（如1.1.1.0/255.255.255.0）等三种输入形式，输入后点击<添加>按钮后，可以继续输入。

- (4) 根据实际情况选择策略配置方式，点击<完成配置>。

新建防攻击域配置向导

选择策略配置方式

策略配置方式

自动学习策略

学习周期

天 (3~60, 推荐7天)

手动配置策略

配置建议: 为保证学习到的策略效果更好, 请保证自动学习时间包含流量高峰期。

自动学习策略: 设备通过一段时间的学习, 可以给出针对此网络防攻击域较为合理的策略配置建议。

手动配置策略: 直接手动配置防御策略。如果您对域内流量已有充分了解, 您可以选择手动配置策略。

基本配置

选择策略

上一步

完成配置

(5) 策略配置方式选择“自动学习策略”时按本步骤执行，选择“手动配置策略”则跳过本步骤：

a 等学习完成后，点击<应用学习结果>，进入[应用学习结果]页面。

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, 流量监控, 黑白名单等。

防攻击域列表

域策略配置

描述	防护服务器网段	
保护主机范围	1.1.1.0/255.255.255.0, 1.1.2.0/255.255.255.0	配置
防护策略自学习	已完成 学习周期 天	应用学习结果 重新学习
TCP Flood 防护	未配置	配置
UDP Flood 防护	未配置	配置
ICMP Flood 防护	未配置	配置
其他协议 Flood 防护	未配置	配置
防扫描	未配置	配置
流量监控	未配置	配置
白名单	已添加0条	配置
黑名单	已添加0条	配置
攻击日志	未配置	配置

b 参考学习结果，结合当前防护域的实际情况调整配置阈值。

说明

因为流量监控功能会消耗部分设备性能，建议在安全策略工作顺畅之后，关闭流量监控，以确保设备能够达到最大的业务处理能力。

应用学习结果

TCP FLOOD策略

策略	学习结果 (建议最低阈值)	配置阈值	☐ 启用所有策略
域外可信源主机发送的SYN报文速率检查(pps)	-	(1倍)	☐ 启用
域外可信源主机发送的TCP半连接数检查(个)	-	(1倍)	☐ 启用
域外可信源主机发送的TCP连接数检查(个)	-	(1倍)	☐ 启用

UDP FLOOD策略

策略	学习结果 (建议最低阈值)	配置阈值	☐ 启用所有策略
整域接收的未经认证的UDP报文速率检查(pps)	-	(1倍)	☐ 启用
域外可信源主机发送的UDP报文速率检查(pps)	-	(1倍)	☐ 启用
限制域内主机的UDP报文速率(pps)	-	(1倍)	☐ 启用
限制整域的UDP报文速率(pps)	-	(1倍)	☐ 启用
域内每主机接受的未经认证的UDP报文速率检查	-	(1倍)	☐ 启用

确定

取消

c 配置完成后，点击<确定>。

(6) 策略配置方式选择“手动配置策略”时按本步骤执行，选择“自动学习策略”则跳过本步骤。

说明

因为流量监控功能会消耗部分设备性能，建议在安全策略工作顺畅之后，关闭流量监控，以确保设备能够达到最大的业务处理能力。

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，流量监控，黑白名单等。

防攻击域列表

域策略配置

描述		配置
保护主机范围	1.1.1.0/255.255.255.0, 1.1.2.0/255.255.255.0	配置
防护策略自学习	未开启 (建议您先进行自学习后再配置策略!) 学习周期 天	启动学习
TCP Flood 防护	未配置	配置
UDP Flood 防护	未配置	配置
ICMP Flood 防护	未配置	配置
其他协议 Flood 防护	未配置	配置
防扫描	未配置	配置
流量监控	未配置	配置
白名单	已添加0条	配置
黑名单	已添加0条	配置
攻击日志	未配置	配置

(7) (可选) 对于可信的源IP，可以将其添加到白名单，从而绕开设备的检测，使该源IP的流量不受影响。点击白名单对应的<配置>进入[配置白名单]页面，输入源IP地址、子网掩码，并选择协议类型和端口号，点击<添加>即可。

说明

- 白名单只对在本防护域生效。

- 白名单优先级大于黑名单。若同一个IP同时被添加到白名单和黑名单，则白名单生效。

配置白名单

说明：白名单里定义的流量可以绕开防火墙体系，不会受到防攻击策略和限速的影响，也不进行流量监控。该配置仅对当前防攻击域有效。

源IP地址

*

子网掩码

协议类型

所有协议

目的端口范围

☒ 所有端口

☐ 指定端口

添加

源IP地址/子网掩码	协议类型	目的端口	操作
无记录信息			

显示: 10 条 共0条

首页

上一页

下一页

末页

1

确定

关闭

(8) （可选）对于非可信的源IP，可以将其添加到黑名单，设备将阻断该IP与本防护域之间的双向流量。点击黑名单对应的<配置>进入[配置黑名单]页面，输入主机IP地址，点击<添加>即可。

 说明

- 黑名单只对在本防护域生效。
- 白名单优先级大于黑名单。若同一个IP同时被添加到白名单和黑名单，则白名单生效。

配置黑名单

说明：黑名单中的主机流量将被防火墙直接阻断，无法通过防火墙。该配置仅对当前防攻击域有效。

主机IP

*

添加

主机IP	操作
无记录信息	

显示: 10 条 共0条

首页

上一页

下一页

末页

1

确定

关闭

- (9) (可选) 点击攻击日志对应的<配置>，可以开启指定类型策略的日志记录和打印功能。根据需要勾选对应类型日志前面的复选框，点击<确定>即可。

配置攻击日志

☒ 记录由真实源产生的TCP攻击日志
 ☒ 记录由伪造源产生的TCP攻击日志
 ☒ 记录所有的UDP攻击日志

☒ 记录所有的ICMP攻击日志
 ☒ 记录所有的其他协议的攻击日志
 ☒ 记录扫描攻击日志

全选

全不选

确定

取消

10.2 安全域配置

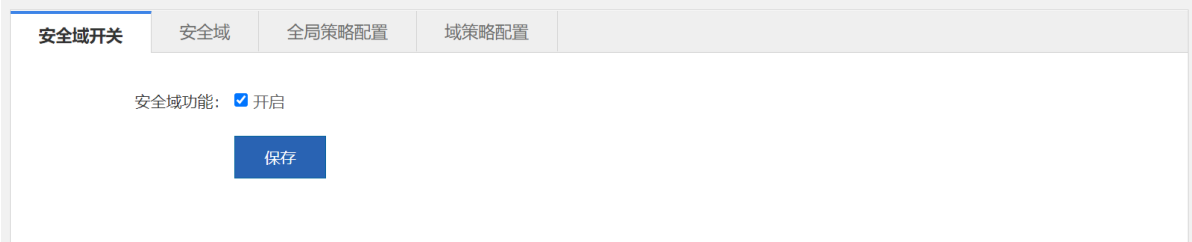
安全域是一个逻辑概念，同一个安全域的中对象具有相同的安全保护需求、安全访问控制和边界控制策略。您可以将设备上具有相同安全防护需求的多个接口或IP地址划分到同一个安全域，实现策略的分层管理，精准防护。例如，子网A连接到网关设备接口1（属于安全域1），子网B连接到网关设备接口2（属于安全域2），您只需配置安全域1和安全域2之间的访问策略，即可对子网A和子网B进行访问控制。

10.2.1 安全域开关

安全域开关用于控制安全域功能菜单的显示及配置，只有打开安全域开关才能查看并配置安全域及策略。

【操作步骤】

- 选择[防火墙]>>[安全域配置]>>[安全域开关]。
- 勾选安全域功能，点击<保存>。



10.2.2 安全域

设备支持基于IP地址（仅支持IPv4）和设备自身接口两种方式划分安全域。两种安全域不能同时使用，切换安全域创建方式后，原有的安全域及域策略将会被删除。缺省情况下使用基于接口方式划分安全域。

缺省情况下，不同安全域之间的访问规则如下：

- 同一个安全域内的IP或端口之间不能互访。
- 高优先级安全域可以访问低优先级安全域，低优先级安全域不能访问高优先级安全域。
- 相同优先级的安全域间不允许互相访问。

若配置了域策略和全局策略，则按域策略和全局策略设置的访问规则进行报文处理，否则按照缺省访问规则进行处理。

1. 接口安全域

将接口划分到安全域后，当报文到达设备时，设备将会识别出报文的源接口和目的接口，并将报文的接口和安全域关联的接口进行匹配，确定报文所属的源安全域和目的安全域，然后按照安全域间策略或缺省访问规则进行报文转发或阻断。

设备预定义了default安全域，不能删除，未配置所属安全域的接口将被划入default安全域。

【操作步骤】

- (1) 选择[防火墙]>>[安全域配置]>>[安全域]。
- (2) 点击<添加>，进入[创建接口安全域]页面。

说明

缺省情况下，设备展示接口安全域页面，若当前非接口安全域页面，你可以点击<切换创建方式>进入接口安全域页面。



- (3) 输入安全域名称和描述，点击<请选择>选择属于该安全域的接口，输入安全域等级，选择是否允许域内互访，点击<确定>即可。



说明

安全域等级即优先级，数值越大优先级越高。缺省情况下，高优先级的安全域可以访问低优先级的安全域，而低优先级的安全域不能访问高优先级的安全域；相同优先级的安全域之间不能互访。

创建接口安全域

安全域名称

*

描述

配置接口

请选择

双击可移除选中项

安全域等级

(1-100)

允许域内互访

☐ 否 ☒ 是

确定

取消

2. IP 安全域

将IP地址划分到安全域后，当报文到达设备时，设备将会识别出报文的源IP地址和目的IP地址，并将IP地址和安全域关联的ACL规则进行匹配，确定报文所属的源安全域和目的安全域，然后按照安全域间策略或缺省访问规则进行报文转发或阻断。

设备预定义了default安全域，不能删除，未配置所属安全域的IP地址将被划入default安全域。

- (1) 选择[防火墙]>>[安全域配置]>>[安全域]。
- (2) 点击<切换创建方式>，进入[切换安全域创建方式]页面。

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	保护的接口范围	允许区间内互访?	描述	操作
default		GigabitEthernet 0/0,GigabitEthernet 0/3,GigabitEthernet 0/5,GigabitEthernet 0/6,GigabitEthernet 0/7,GigabitEthernet 0/9,TenGigabitEthernet 0/0,dialer 1,dialer 2,dialer 3	否		编辑

显示: 10 条 共1条

首页 上一页 1 下一页 末页

1

确定

- (3) 选择“IP地址”，点击<确定>。

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

(4) 点击<添加>，进入[创建IP安全域]页面。

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: IP

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IP范围	例外主机IP范围	允许区间内互访?	描述	操作
default				否		

显示: 10 条 共1条

首页 上一页 1 下一页 末页

1

确定

(5) 输入IP安全域参数，点击<确定>即可。

创建IP安全域

IP安全域配置

安全域名称:

*

描述:

保护主机范围

添加

双击可移除选中项

例外主机范围

添加

双击可移除选中项

安全域等级:

(1-100)

允许域内互访:

☒ 否 ☐ 是

确定

取消

参数	说明
安全域名称	安全域唯一标识。
描述	安全域的描述信息。

保护主机范围	加入该安全域的主机IP范围，支持单个IP地址（如1.1.1.1）、子网/掩码长度（如1.1.1.0/24）、子网/掩码（如1.1.1.0/255.255.255.0）和any四种输入形式，输入后点击<添加>按钮后，可以继续输入。
例外主机范围	不属于该安全域的IP地址。例如将子网1.1.1.0/24加入某个安全域，但是其中IP地址1.1.1.1不需要加入该安全域，可将其添加到例外主机范围。
安全等级	安全域优先级，数值越大优先级越高。缺省情况下，高优先级的安全域可以访问低优先级的安全域，而低优先级的安全域不能访问高优先级的安全域；相同优先级的安全域之间不能互访。
允许域内互访	选择是否允许该安全域内的IP地址之间互相访问。

10.2.3 全局配置策略

全局访问策略用于控制域内是否允许访问、相同优先级的安全域间是否允许访问，以及匹配安全域策略后，在连接建立和撤销时是否需要产生日志、违反安全域访问策略而丢弃报文时是否需要产生日志。

全局访问策略优先级高于缺省访问规则。

【操作步骤】

- (1) 选择[防火墙]>>[安全域配置]>>[全局策略配置]。
- (2) 根据需要勾选对应的选项，点击<保存>即可。

10.2.4 域策略配置

域策略用于控制不同安全域之间是否能互相访问。报文到达设备后，设备将会根据报文特征识别出报文所属的源安全域和目的安全域，若源安全域不等于目的安全域则为域间访问，按照域策略进行报文的转发控制，未配置域策略时则按全局策略或缺省访问规则处理；若源安全域等于目的安全域则为域内互访，按照安全域配置是否允许域内互访进行处理。

域策略随安全域创建方式联动变化，即从接口安全域切换到IP安全域时，域策略页面也将会切换到IP安全域安全域策略配置页面，原有的域策略随之失效删除，反之同理。

域策略的优先级高于全局策略，全局策略优先级高于缺省访问规则。

1. 创建基于接口安全域的域策略

缺省情况下未配置基于接口的安全域域策略。

【前置条件】

安全域配置方式选择基于接口的安全域。

【操作步骤】

(1) 选择[防火墙]>>[安全域配置]>>[域策略配置]。

(2) 点击<添加>，进入[新增策略]页面。

安全域开关

安全域

全局策略配置

域策略配置

安全域策略配置

查询项: 源域

关键字:

查询

刷新

+添加

删除所选

☐	移动	序号	源域	目的域	源IP地址	目的IP地址	服务	时间段	动作	描述	状态	操作
无记录信息												

显示: 10 条 共0条

首页 上一页 下一页 末页

1

确定

(3) 根据以下信息配置策略参数，点击<确定>即可。

新增策略

策略配置

同步安全域 | 重置配置数据

源安全域: --请选择源安全域--

目的安全域: --请选择目的安全域--

序号: *

描述:

源IP地址: any_address IP资源配置

目的IP地址: any_address IP资源配置

选择服务: any_service 服务资源配置

过滤动作: ☒ Permit ☐ Deny

时间段: ---选择生效时间--- 时间段管理

启用策略: ☒ 启用

确定

取消

配置项	参数
源安全域	对所选源安全域和目的安全域之间进行访问控制
目的安全域	对所选源安全域和目的安全域之间进行访问控制
序号	策略的优先级，数值越小优先级越高。配置了多个域策略时，优先级高的策略优先进行匹配
描述	域策略的描述信息
源IP地址	对指定源IP地址的报文进行访问控制。点击<IP资源配置>可以新增IP地址对象。有关IP资源的详细介绍请参见 10.4 IP资源配置

目的IP地址	对指定目的IP地址的报文进行访问控制。点击<IP资源配置>可以新增IP地址对象。有关IP资源的详细介绍请参见 10.4 IP资源配置
选择服务	对所选服务类型的报文进行访问控制。点击<服务资源配置>可以新增服务对象。有关IP资源的详细介绍请参见 10.5 服务资源配置
过滤动作	对匹配域策略的报文执行的动作
时间段	策略生效的时间段
启用策略	是否启用策略，只有启用状态的域策略才会对报文进行匹配

2. 创建基于 IP 安全域的域策略

缺省情况下未配置基于接口的安全域策略。

【前置条件】

安全域配置方式选择基于IP的安全域。

【操作步骤】

- (1) 选择[防火墙]>>[安全域配置]>>[域策略配置]。
- (2) 点击<向导添加>，进入[创建安全域策略]页面。



- (3) 根据以下信息完成策略基本配置，点击<下一步>。

创建安全域策略

策略基本配置

策略基本配置

IP范围策略

源安全域: default *

目的安全域: default *

描述: (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: (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

下一步

配置项	参数
源安全域	对所选源安全域和目的安全域之间进行访问控制
目的安全域	对所选源安全域和目的安全域之间进行访问控制
描述	域策略的描述信息
序号	策略的优先级，数值越小优先级越高。配置了多个域策略时，优先级高的策略优先进行匹配
配置策略方式	匹配报文的方式，支持根据IP范围和ACL规则两种方式匹配报文

(4) 根据以下信息配置IP范围策略，点击<完成配置>。策略方式选择“引用ACL策略”时请跳过本步骤，进行下一步。

 说明

配置IP范围后，根据IP范围匹配到的ACL策略中设置的动作（允许或阻断）进行访问控制。

创建安全域策略

安全域IP范围策略配置

源IP范围:

添加

双击可移除选中项

目的IP范围:

添加

双击可移除选中项

传输层协议:

---请选择协议(默认IP)---

选择生效时间:

---选择生效时间---

时间段管理

上一步

完成配置

策略基本配置

2 IP范围策略

配置项	参数
源IP地址	对指定源IP地址的报文进行访问控制。支持单个IP地址（如1.1.1.1）、子网/掩码长度（如1.1.1.0/24）、子网/掩码（如1.1.1.0/255.255.255.0）和any四种输入形式，输入后点击<添加>按钮后，可以继续输入。
目的IP地址	对指定目的IP地址的报文进行访问控制。支持单个IP地址（如1.1.1.1）、子网/掩码长度（如1.1.1.0/24）、子网/掩码（如1.1.1.0/255.255.255.0）和any四种输入形式，输入后点击<添加>按钮后，可以继续输入。
传输层协议	对所选协议类型的报文进行访问控制。
请选择生效时间	策略生效的时间段。点击<时间段管理>可以新增时间段。

(5) 根据以下信息配置ACL策略，点击<完成配置>。策略方式选择“IP范围策略”时请忽略本步骤。

a 点击<请选择>可以选择引用已配置的ACL策略，若无可用ACL，点击<管理ACL>创建ACL策略。

创建安全域策略

选择ACL策略配置

*应用ACL策略:

请选择

+管理ACL

上一步

完成配置

策略基本配置

2 引用ACL策略

b 点击<添加>按钮，进入[添加ACL]页面。



c 选择ACL类型，并输入ACL列表名称或编号，点击<确定>。



d 选中刚刚创建的ACL列表，点击<添加ACE规则>，进入[添加ACE规则]页面。



e 根据以下信息配置ACE规则参数，点击<确定>。

添加ACE规则

ACL类型: 标准ACL (控制源地址)

ACL列表: 1301

规则设置

访问控制: ☒ 允许 ☐ 禁止 生效时间:

请选择生效时间

[【生效时间管理】](#)

☐ 任意IP地址: (IP地址任意是对所有的IP应用该规则)

单IP地址

 IP 地址:

确定

取消

配置项	参数
访问控制	对匹配本规则的报文执行的动作
生效时间	本规则生效的时间段。点击<时间段管理>可以新增时间段。
IP地址	对指定IP地址的报文进行访问控制。支持单个IP地址（如1.1.1.1）、掩码设置（如1.1.1.0/255.255.255.0）、通配符（如1.1.1.0/0.0.0.255）三种输入形式 勾选“任意IP地址”则所有报文都会匹配本规则

f 配置规则配置完成后，关闭[管理ACL]页面。在[创建安全域策略]页面点击<请选择>进入[选择ACL策略]页面。

创建安全域策略

选择ACL策略配置

* 应用ACL策略:

请选择

+管理ACL

策略基本配置

引用ACL策略

上一步

完成配置

g 点击<刷新>，然后选择刚刚创建的ACL策略，点击<确定>。

选择ACL策略

ACL策略信息

acl策略名称:

查询

刷新

选择	acl策略名称	策略条目(ace)信息
☐	1	共有: 1条策略条目(ace) 详细
☐	110	共有: 1条策略条目(ace) 详细
☒	1301	共有: 1条策略条目(ace) 详细
☐	2397	共有: 7条策略条目(ace) 详细

显示:

8

 条 共4条

首页

上一页

1

下一页

末页

1

确定

确定

取消

h 点击<完成配置>即可。

创建安全域策略

选择ACL策略配置

* 应用ACL策略:

请选择

+管理ACL

策略基本配置

引用ACL策略

上一步

完成配置

10.3 防攻击域状态监控

10.3.1 域运行状态

本功能用于展示各防护域的基本信息和流量统计。

【前置条件】

您已配置防攻击域策。有关防攻击域的详细介绍请参见[10.1.4 域策略](#)。

【操作步骤】

- (1) 选择[防火墙]>>[防攻击域状态监控]>>[域运行状态]。
- (2) 选中防攻击域，页面右侧将会展示该域的基本信息、运行状态和流量统计信息。



10.3.2 当前攻击行为

本功能用于展示各防攻击域当前正在发生的攻击，支持按照攻击类型和协议类型筛选攻击行为信息。

【前置条件】

您已配置防攻击域策。有关防攻击域的详细介绍请参见[10.1.4 域策略](#)。

【操作步骤】

- (1) 选择[防火墙]>>[防攻击域状态监控]>>[当前攻击行为]。
- (2) 选中防攻击域，页面右侧默认将会按攻击类型展示所选防攻击域当前正在发生的攻击行为。
- (3) （可选）点击“协议类型”后面的下拉列表选择其他协议，点击<查询>即可按协议类型查看攻击信息。



10.3.3 防火墙流量查看

本功能用于展示全局防护情况。

【前置条件】

您已配置全局防护。有关全局防护的详细介绍请参见[10.1.2 全局防护](#)。

【操作步骤】

- (1) 选择[防火墙]>>[防攻击域状态监控]>>[防火墙流量查看]。

- (2) 点击“全局防护统计”可以查看防护流量统计。
- (3) 点击“整体丢弃统计”可以查看防攻击丢包统计。



10.4 IP 资源配置

IP资源主要用于配合其他功能模块使用，不单独使用。例如，配置安全域间策略时，可以对源安全域中指定源IP地址的报文进行访问控制。

10.4.1 主机地址

主机地址即单个IP地址，为单个IP地址配置合适的名称，管理员可以快速识别该IP地址对应的设备。

【操作步骤】

- (1) 选择[防火墙]>>[IP资源配置]>>[主机地址]。
- (2) 点击<添加>按钮。

- (3) 输入名称、描述，输入IP地址，点击<添加>。如需添加多个IP，可以继续输入并点击<添加>。

(4) 配置完成，点击<确定>。

10.4.2 范围地址

范围地址，如1.1.1.1~1.1.1.10。为IP地址范围配置合适的名称，管理员可以快速识别该IP范围对应的设备。

【操作步骤】

(1) 选择[防火墙]>>[IP资源配置]>>[范围地址]。

(2) 点击<添加>按钮。

(3) 输入名称、描述和IP地址范围。如有排除地址，输入排除地址（仅支持输入单IP），点击<添加>。如需添加多个排除地址IP，可以继续输入并点击<添加>。

(4) 配置完成，点击<确定>。

10.4.3 子网地址

子网地址，如1.1.1.0/255.255.255.0。为子网配置合适的名称，管理员可以快速识别该子网。

【操作步骤】

(1) 选择[防火墙]>>[IP资源配置]>>[子网地址]。

(2) 点击<添加>按钮。

(3) 输入名称、描述和IP地址/掩码。如有排除地址，输入排除地址（仅支持输入单IP），点击<添加>。如需添加多个排除地址IP，可以继续输入并点击<添加>。

(4) 配置完成，点击<确定>。

10.4.4 地址组配置

地址组是多个IP地址的集合。您可以将具有相同安全防护需求的主机地址、范围地址或子网加入同一个地址组，方便管理。

【前置条件】

您已配置主机地址、范围地址或子网地址。

【操作步骤】

(1) 选择[防火墙]>>[IP资源配置]>>[地址组配置]。

(2) 点击<添加>按钮。

(3) 输入名称、描述，按照实际需求选择地址组成员，点击<增加>。

(4) 配置完成，点击<确定>。

10.5 服务资源配置

服务资源是通过协议类型以及协议的特性来呈现，协议特性如TCP、UDP的源端口和目的端口、ICMP的消息类型/消息码等，用于匹配报文中的可承载的上层协议。

服务资源主要用于配合其他功能模块使用，不单独使用。例如，配置安全域间策略时，可以对指定服务的报文进行访问控制。

10.5.1 自定义服务

设备预定义了常用的服务，您可以在[预定义服务]页面查看。若预定义服务中没有您需要的服务，您可以自行配置服务资源。

【操作步骤】

- (1) 选择[防火墙]>>[服务资源配置]>>[自定义服务]。
- (2) 点击<添加>按钮。

自定义服务

服务组配置

预定义服务

查询项: 名称

关键字:

查询

刷新

+添加

删除所选

☐	名称	协议	协议参数	描述	状态	操作
无记录信息						

显示: 15

条 共0条

首页

上一页

下一页

末页

1

确定

(3) 输入名称、描述，选择相应的协议类型并配置对应的协议参数，点击<确定>。

说明

不同的类型的协议配置参数不同，请以页面实际情况为准。

自定义服务

服务组配置

预定义服务

名称

*

描述

协议

TCP

源端口

-

*

目的端口

-

*

确定

取消

10.5.2 服务组配置

服务组是多个服务的集合。您可以将具有相同安全防护需求的自定义服务或预定义加入同一个服务组，方便管理。

【操作步骤】

(1) 选择[防火墙]>>[服务资源配置]>>[服务组配置]。

(2) 点击<添加>按钮。

自定义服务

服务组配置

预定义服务

查询项: 名称

关键字:

查询

刷新

+添加

删除所选

☐	名称	成员	描述	状态	操作
无记录信息					

显示: 15

条 共0条

首页

上一页

下一页

末页

1

确定

(3) 输入名称、描述，按照实际需求选择服务组成员，点击<增加>。

自定义服务

服务组配置

预定义服务

名称

服务组1

*

描述

测试

成员

-----可用的服务组成员-----

自定义服务1

bgp

chargen

cmd

daytime

dhcp-relay

discard_tcp

finger

ftp

ftp-get

ftp-put

gopher

-----已选的服务组成员-----

增加->

<-移除

确定

取消

(4) 配置完成，点击<确定>。

10.5.3 预定义服务

本功能用于展示设备预定义的服务。

【操作步骤】

- (1) 选择[防火墙]>>[服务资源配置]>>[预定义服务]。
- (2) （可选）选择查询项或输入关键字，点击<查询>按钮可搜索需要的服务信息。

自定义服务

服务组配置

预定义服务

查询项:

名称

关键字:

查询

名称	协议	协议参数
bgp	tcp	源端口:any,目的端口:179
chargen	tcp	源端口:any,目的端口:19
cmd	tcp	源端口:any,目的端口:514
daytime	tcp	源端口:any,目的端口:13
dhcp-relay	udp	源端口:any,目的端口:67
discard_tcp	tcp	源端口:any,目的端口:13
finger	tcp	源端口:any,目的端口:79
ftp	tcp	源端口:any,目的端口:21
ftp-get	tcp	源端口:any,目的端口:21
ftp-put	tcp	源端口:any,目的端口:21

显示:

10

条 共54条

首页

上一页

1

2

3

4

5

下一页

末页

1

确定

11 运维

11.1 系统设置

11.1.1 修改密码

Web网管密码：当用户通过Web页面配置设备时，必需使用该密码登录设备。通过本页面可修改admin用户的登录密码，设置新的Web网管密码后，需要使用新密码重新登录。

Telnet密码：用户通过Telnet登录和配置设备时，必须使用该密码登录。

 注意

- 修改后的密码请务必牢记，以免下次登录时无法进入。
- 本页面仅超级管理有配置权限，即本页面只对admin用户可见。

【应用场景】

出于设备安全性考虑，首次登录设备后，建议尽快修改设备初始密码。

【操作步骤】

- (1) 选择[运维]>>[系统设置]>>[修改密码]。
- (2) 根据实际需求，输入Web网管密码或Telnet密码，点击<确认修改>。

修改密码	重启设备	恢复出厂设置	配置备份	系统时间	增强功能	SNMP
说明： admin用户拥有配置和查看设备信息的所有权限。 提示： 如果您设置了新的Web登录密码，则在设置之后使用新密码重新登录。密码不能含有中文、全角字符、问号和空格。密码最长不能超过32字符。						
Web网管密码修改 用户名： admin 新密码： * 确认新密码： * 确认修改 清空						
认证Telnet密码配置(修改telnet和enable的密码) ? 用户名： admin 新密码： * 确认新密码： * 确认修改 清空						

11.1.2 重启设备

设备重新启动需要1分钟左右，期间请勿做其它任何操作，设备重启成功后将自动刷新页面。

【前置条件】

重启前，所有配置均已保存，否则重启后将会丢失未保存的配置信息。

【配置步骤】

- (1) 选择[运维]>>[系统设置]>>[重启设备]。
- (2) 点击<立即重启设备>。



11.1.3 恢复出厂设置

恢复出厂设置将会清除设备当前所有配置，并恢复设备出厂时的默认配置。如需保留现有配置，请先通过“配置备份”导出当前配置。

【配置步骤】

- (1) 选择[运维]>>[系统设置]>>[恢复出厂设置]。
- (2) 点击<恢复出厂设置>。



11.1.4 配置备份

1. 导出当前配置

该功能可以将设备的当前配置导出到本地电脑进行备份。

【配置步骤】

- (1) 选择[运维]>>[系统设置]>>[配置备份]。
- (2) 点击<导出当前配置>。

修改密码	重启设备	恢复出厂设置	配置备份	系统时间	增强功能	SNMP
------	------	--------	------	------	------	------

说明： 导入过程中不能关闭或者刷新页面，否则导入将失败！

提示： 导入配置后，要启用新的配置，请在本页面 [【重启设备】](#) 否则配置不生效。

导出当前配置

文件名：

选择文件 未选择任何文件

导入配置

查看当前配置

查看当前配置

(3) 选择配置文件保存路径，点击<保存>。

2. 导入配置

该功能可以将本地电脑上的配置备份文件上传到设备上还原。

【配置步骤】

(1) 选择[运维]>>[系统设置]>>[配置备份]。

(2) 点击<选择文件>，选择本地电脑上的配置文件（文件名必需是“config.text”），然后点击<导入配置>。

修改密码	重启设备	恢复出厂设置	配置备份	系统时间	增强功能	SNMP
------	------	--------	------	------	------	------

说明： 导入过程中不能关闭或者刷新页面，否则导入将失败！

提示： 导入配置后，要启用新的配置，请在本页面 [【重启设备】](#) 否则配置不生效。

导出当前配置

文件名：

选择文件 未选择任何文件

导入配置

查看当前配置

查看当前配置

(3) 进入[重启设备]页面，点击<立即重启设备>。设备重启成功后，导入的配置才能生效。



说明

若发现导入的配置有问题，可在没有重启之前，点击“取消导入”按钮来恢复原有配置。

3. 查看当前配置

该功能用于查看当前设备的所有配置命令。

- (1) 选择[运维]>>[系统设置]>>[配置备份]。
- (2) 点击<查看当前配置>。

修改密码

重启设备

恢复出厂设置

配置备份

系统时间

增强功能

SNMP

说明：导入过程中不能关闭或者刷新页面，否则导入将失败！

提示：导入配置后，要启用新的配置，请在本页面【重启设备】否则配置不生效。

导出当前配置

文件名：

选择文件

未选择任何文件

导入配置

查看当前配置

查看当前配置

Building configuration...

Current configuration: 5705 bytes

version NBR_RGOS 11.9(6)B14, Release(09171603)

!

11.1.5 系统时间

该功能用于设置设备系统时间。设备支持手动修改和从时间服务器同步两种方式修改系统时间。选择从Internet时间服务器同步时间时，必须先在[网络配置]>>[DNS配置]页面配置正确的DNS服务器，确保设备与时间服务器之间网络互通。

【操作步骤】

- (1) 选择[运维]>>[系统设置]>>[系统时间]。
- (2) 手动修改系统时间：
 - a 取消勾选“自动与Internet时间服务器同步”和“通过管理口自动与Internet时间服务器同步”，点击“重新设置时间”后面的输入框，设置日期和时间。

修改密码	重启设备	恢复出厂设置	配置备份	系统时间	增强功能	SNMP
------	------	--------	------	-------------	------	------

温馨提醒： 修改设备时间可能导致历史流量报表的审计时间出错。

提示： 开启“自动与Internet 时间服务器同步”后请检查是否已经配置了正确的【DNS服务器】，否则将不能生效！

系统日期和时间

当前系统时间： 2022年5月30日上午8:59:38

重新设置时间：

时间服务器： (系统自带：ntp.ntsc.ac.cn、ntp1.aliyun.com)

时区：

☐ 自动与Internet 时间服务器同步

☐ 通过管理口自动与Internet 时间服务器同步

b 选择时区，点击<确认修改>。

(3) 从时间服务器地址同步时间：

a 勾选“自动与Internet时间服务器同步”或“通过管理口自动与Internet时间服务器同步”，在“时间服务器”后面的输入框中输入服务器URL。

说明

- 设备处于网桥模式或网关模式，并且只能通过管理口连接外网时，必须勾选“通过管理口自动与Internet 时间服务器同步”。
- 时间服务器配置为系统自带的服务器地址时，不需要额外的DNS配置。

修改密码	重启设备	恢复出厂设置	配置备份	系统时间	增强功能	SNMP
------	------	--------	------	-------------	------	------

温馨提醒： 修改设备时间可能导致历史流量报表的审计时间出错。

提示： 开启“自动与Internet 时间服务器同步”后请检查是否已经配置了正确的【DNS服务器】，否则将不能生效！

系统日期和时间

当前系统时间： 2022年5月30日上午8:57:59

重新设置时间：

时间服务器： (系统自带：ntp.ntsc.ac.cn、ntp1.aliyun.com)

时区：

☒ 自动与Internet 时间服务器同步

☐ 通过管理口自动与Internet 时间服务器同步

- b 选择时区，点击<确认修改>。

11.1.6 增强功能

本页面集中提供了多个功能配置入口，各个功能之间互不影响。

- Web登录超时：用于设置登录超时时长。默认超时时长为60分钟，即登录账号超过60分钟无Web操作将会强制登出。
- 设备名称：用于设置设备名称，修改设备名称后，可在[首页]>>[系统首页]查看更新设备名称。
- 反馈用户信息：通过本功能可以配置设备将警告信息通过邮件的方式及时通知给相关责任人时，从而提醒责任人处理告警信息，以保证设备的正常稳定。
- 发送邮箱配置：配置发送用户反馈信息和审计告警信息的邮箱信息。
- 网站访问被阻断后的反馈信息配置：配置阻断网站访问后反馈给用户的信息，例如，在[行为管理]>>[禁止网站]页面配置了禁止访问“www.xxx.com”网站，用户访问这个网站后看到的提示信息，就是在本页面配置的信息。
- 流量审计实时数据生成频率：设置设备实时生成流量审计数据的时间周期。
- WiFi6特性：开启该功能后，AC将会下发配置到对应AP，告知AP支持11AX用户接入。

【操作步骤】

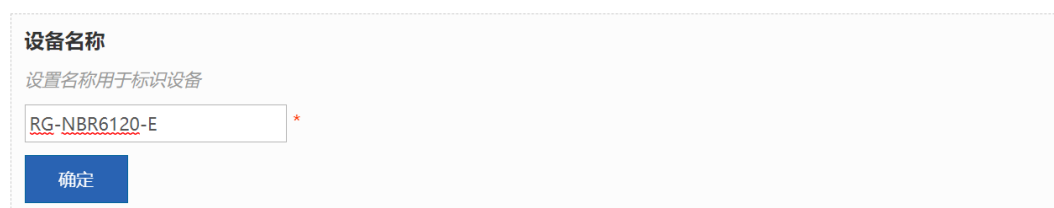
- (1) 选择[运维]>>[系统设置]>>[增强功能]。

- (2) 根据需要设置以下一种或多种功能：

- 配置Web登录超时时长：输入时长，点击<确定>。确定后配置立即生效。



- 配置设备名称：输入名称，点击<确定>。确定后配置立即生效。



- 配置反馈用户信息：

点击<马上配置用户信息>，进入[反馈用户信息]弹窗。



勾选“开启用户信息反馈”，输入邮件服务器、收件人邮箱等信息。

反馈用户信息 - Google Chrome

不安全 | https://192.168.23.93:4430/system_pi/setsys_infoback.htm

用户信息反馈：☒开启用户信息反馈（设备会根据您的需要，反馈信息给您！）

发送邮件服务器： * 如：smtp.sina.com

服务器端口： * 发送邮件服务器端口默认25

邮件发送帐号： * 如：xxx@sina.com.cn

帐号密码： (加密码不显示，只需重新配置账号或修改密码时才需输入)

邮件发送频率： 分钟 (5-10080)

收件人邮箱： * 多个可以用逗号隔开，最多配置6个邮箱

验证配置：

配置关注的信息：勾选您想要了解的信息，反馈给您的邮件中将包括您勾选的信息！

☒设备受攻击 ☒流量达到流控设置 ☒流控缓存超过限制

行业类型： 机构名称： 联系电话：

配置项	说明
发送邮件服务器	发送告警邮件的服务器地址，例如smtp.sina.com等
服务器端口	邮箱服务器的端口，若无特殊要求，采用缺省配置即可
邮件发送帐号	发送告警邮件的邮件账号，如serv@sina.com
帐号密码	发送邮箱的密码，即上例中serv@sina.com的密码
邮件发送频率	设备告警信息发送到指定邮箱的频率，缺省情况下每60分钟发送一次。例如，设备发生内存不足的告警时，则每隔1个小时就会给指定邮箱发送一份告警邮件
收件人邮箱	接收告警信息的邮箱
验证配置	点击<发送测试邮件>可以测试配置的邮箱服务器是否可用。若不可用请按界面提示信息进行故障排查处理
配置关注的信息	根据实际需求选择关注的告警信息，选择后，当设备出现告警时将会发送告警邮件到收件人邮箱
行业类型	填写您所属的行业类型，建议您如实填写，以方便我们为您提供更好的服务
机构名称	填写您所在的机构名称，建议您如实填写，以方便我们为您提供更好的服务
联系电话	填写您的联系电话，建议您如实填写，以方便我们为您提供更好的服务

确认配置无误，点击<保存设置>。

- 发送邮箱配置：

点击<马上配置>，进入[发送邮箱配置]弹窗。

发件邮箱配置

发件邮箱用于发送用户反馈信息和审计告警信息。

马上配置

勾选“开启”，输入邮件服务器、收件人邮箱等信息。

发件邮箱配置 - Google Chrome

不安全 | https://192.168.23.93:4430/system_pi/setsys_mail_config.htm

邮件发送开关：☒ 开启

发送邮件服务器： * 如：smtp.sina.com ?

服务器端口： 25 * 发送邮件服务器端口默认25

邮件发送帐号： * 如：xxx@sina.com.cn

帐号密码： (加密码不显示，只需重新配置账号或修改密码时才需输入)

保存设置

验证配置：

发送测试邮件

 (发送测试邮件前，请先保存配置！)

配置项	说明
发送邮件服务器	发送告警邮件的服务器地址，例如smtp.sina.com等
服务器端口	邮箱服务器的端口，若无特殊要求，采用缺省配置即可
邮件发送帐号	发送告警邮件的邮件账号，如serv@sina.com
帐号密码	发送邮箱的密码，即上例中serv@sina.com的密码
验证配置	点击<发送测试邮件>可以测试配置的邮箱服务器是否可用。若不可用请按界面提示信息进行故障排查处理

确认配置无误，点击<保存设置>。

- 网站访问被阻断后的反馈信息配置：输入提示信息，点击<保存设置>。

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“行为策略》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！

保存设置

- 设置流量审计实时数据生成频率：选择频率，点击<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

- 管理WiFi6特性：根据实际需求选择开启或关闭WiFi6特性。

WiFi6特性

管理wifi6特性，是否支持wifi6功能以AP功能规格为准。RAP目前都不支持wifi6。

开启

关闭

11.1.7 SNMP

通过SNMP（Simple Network Management Protocol，简单网络管理协议）协议，网络管理员可以对网络上的节点进行信息查询、网络配置、故障定位、容量规划等，轻松管理网络节点。

【操作步骤】

- (1) 选择[运维]>>[系统设置]>>[SNMP]。
- (2) 输入SNMP配置参数，点击<保存设置>。

修改密码

重启设备

恢复出厂设置

配置备份

系统时间

增强功能

SNMP

SNMP：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；注意：在设备转换网关或者网桥模式时，需要重新配置SNMP配置才能生效。
提示：任子行只支持V2版本。

SNMP配置

SNMP版本：

☒ V2版本

☐ V3版本

设备标识： *

SNMP口令： *

Trap口令：

SNMP目的主机： ?

Trap接收主机： 最多可配置9个Trap接收主机，IP之间请用“，”号隔开。

保存设置

清除设置

配置项	说明
SMNP版本	目前设备支持V2和V3版本。V3版本提高了安全性设置，要求添加SMNP用户的加密密码和认证密码。

配置项	说明
设备标识	用于标识您的SMNP服务的名称
SNMP口令	管理主机可以通过该口令连接当前设备
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
Trap接收主机	接收设备告警信息的管理主机IP，多个IP之间用英文逗号隔开

11.2 系统升级

本功能用于升级系统软件、Web包、特征库等新版本，您可以根据需求更新对应的版本。升级过程需要约50秒，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。

【前置条件】

使用在线等级、自动更新等功能前，请确认您已配置了可用的DNS服务器。

【操作步骤】

- (1) 选择[运维]>>[系统升级]。
- (2) 请根据实际需求选择以下一项或多项进行配置：

- 本地升级：

您可以在锐捷网络官方网站下载最新的升级文件到本地，然后通过本功能升级设备软件版本。

点击<选择文件>，选择您从官网下载到本地电脑上的升级包文件。然后点击<开始升级>。升级过程中不能进行任何操作，约50秒，设备会提示升级成功，点击<确定>即可。

系统升级

说明： 您可以访问锐捷网络的“软件版本”来下载最新的升级文件到本地，然后通过下面的方式升级到设备。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。

注意： 主程序文件名不能包含中文和全角字符，升级更新完后设备会自动重启，请确认所升级的版本型号与本设备的型号相同。2、在升级过程中，请勿做其他操作！

本地升级

文件名：

选择文件

未选择任何文件

开始升级

取消升级

- 最新软件版本下载：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。

最新软件版本下载

已安装软件版本： NBR_RGOS 11.9(6)B14, Release(09171603)

目前暂无新的软件版本

- 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。

在线升级web包

当前web包版本：

目前暂无新的web包

- 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。

检测当前最新特征库
应用分类库版本: 2019.06.15.19.06.15(V2.0S) 地址库版本: 2019.07.21.00
URL库版本: 2022-2-22 内容审计特征库: 2020.11.10.00
内容审计特征库2: 2022.05.05.01

检查特征库最新版

- 特征库下载：

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>，进入[特征库下载]弹窗。

特征库下载
选择您要升级的库类型，先把最新的库文件下载到本地，然后再通过本页面的“本地升级”更新到设备中。

下载URL库 下载应用分类库

点击下载地址，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。

URL库下载 - Google Chrome
不安全 | rgos.ruijie.com.cn/url/download/DownWeb/library_download.htm?model=NBR6120-E&version=NBR_R...



URL库下载

URL Library Download

更新说明
版本:5.5.9
数量:62w
更新时间:2022-2-22

为了能提供精准的URL库和特征库，希望您留下贵机构的联系方式!
机构名称:
联系电话:
提交

URL库下载: http://rgos.ruijie.com.cn/url/download/all_class/url_XNBRs.rar

- 设置自动更新：

设置设备按指定的时间对软件版本、特征库版本等进行版本检测并自动更新。

勾选“启动自动更新”，设置更新时间，点击<确定>。

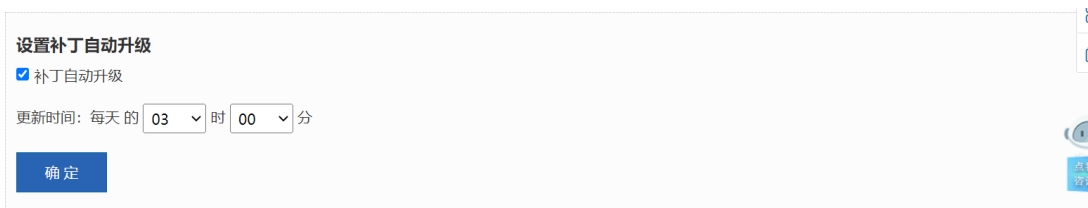
设置自动更新
☒ 启动自动更新
更新时间: 每天的 时 分

确定

- 设置补丁自动升级：

设置设备按照指定的时间对补丁版本进行检测并自动更新。

勾选“补丁自动升级”，设置更新时间，点击<确定>。

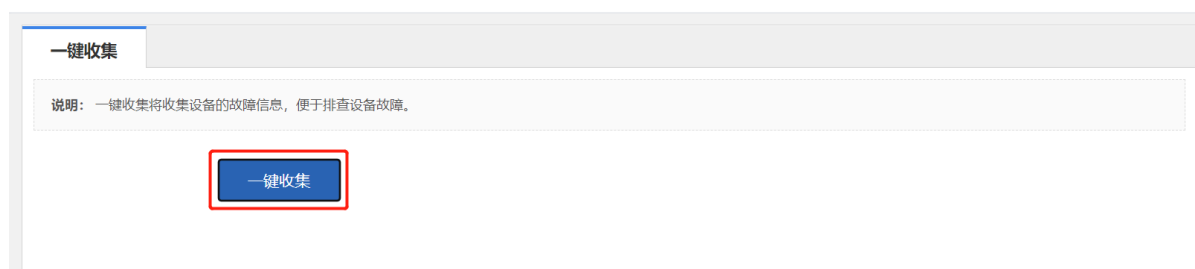


11.3 一键收集

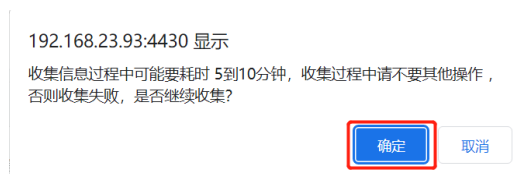
一键收集将收集设备的故障信息，便于排查设备故障。

【操作步骤】

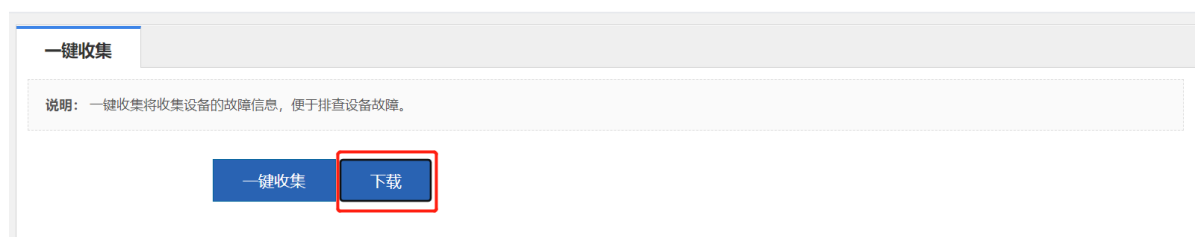
- (1) 选择[运维]>>[一键收集]。
- (2) 点击<一键收集>。



- (3) 页面弹出如下提示框，点击<确定>。



- (4) 收集完成后，点击<下载>按钮下载生成的文件包，便于工程师进行故障分析。



11.4 抓包工具

抓包工具可以对指定的协议报文进行抓包，方便技术人员进行故障定位。设备正常运行时，请勿使用本功能，以免影响网络流畅。

【操作步骤】

- (1) 选择[运维]>>[抓包工具]。
- (2) 点击<点击添加抓包规则>，进入[添加规则]页面。



(3) 输入抓包点名称，选择协议并配置对应的参数。不同协议需要配置的参数不同，请以界面实际情况为准。

三

添加规则

×

抓包点名称:

请输入抓包点名称

二层协议:

any

▼

目的MAC:

格式: 1272.1218.1241

源MAC:

格式: 1272.1218.1241

保存

(4) 配置完成后，点击<保存>。

(5) 点击<添加抓包点>，进入[添加抓包点]页面。



(6) 输入抓包名称，选择抓包接口及抓包规则，点击<保存>。

三 添加抓包点

×

抓包点名称

请输入抓包点名称

接口:

Gi0/0

▼

抓包规则

test

▼

保存

(7) 点击<开始抓包>。

Packet Capture

Ruijie

抓包诊断工具

+ 添加抓包点

+ 添加抓包规则

+ 编辑抓包规则

抓包点	规则名	接口	操作
test	test	Gi0/0	编辑 删除

抓包已结束，请下载文件

开始抓包

下载文件

清除文件

说明

抓包过程中，您可以根据需要随时停止抓包。

(8) 抓包结束后，点击<下载文件>按钮可下载生成的抓包文件到本地进行分析。

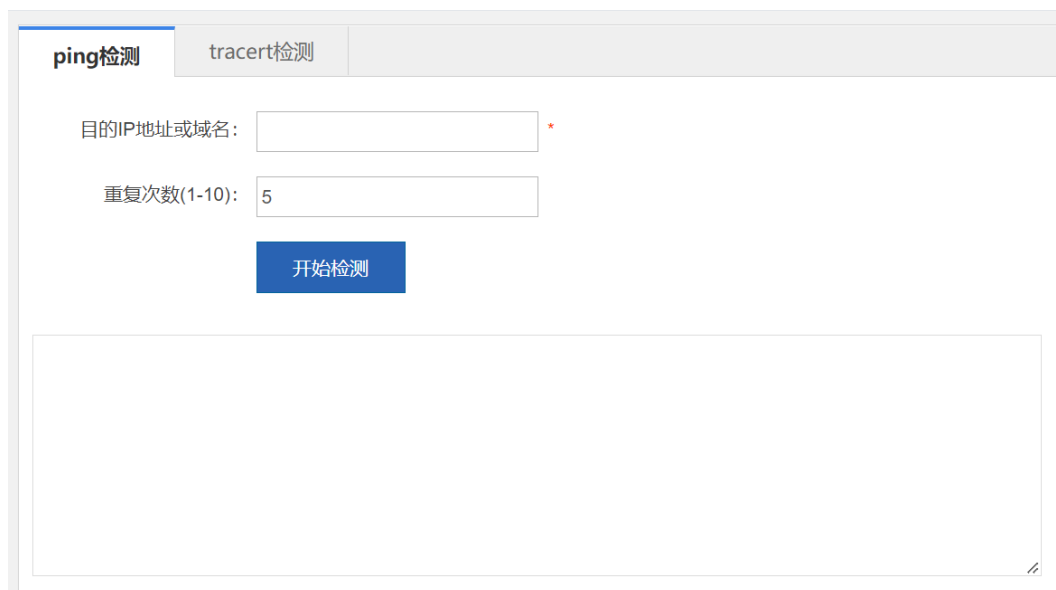
11.5 检测网络

11.5.1 ping 检测

ping检测用于测试本设备与目标IP或域名之间的网络连通性。

【操作步骤】

- (1) 选择[运维]>>[检测网络]>>[ping检测]。
- (2) 输入目的IP地址或域名及重复次数，点击<开始检测>。



(3) 检测完成后，页面下方将会展示检测结果。

11.5.2 tracert 检测

tracert检测用于查看本设备到目标IP或域名所经过的网络路径。

【操作步骤】

- (1) 选择[运维]>>[检测网络]>>[ping检测]。
- (2) 输入目的IP地址或域名，点击<开始检测>。

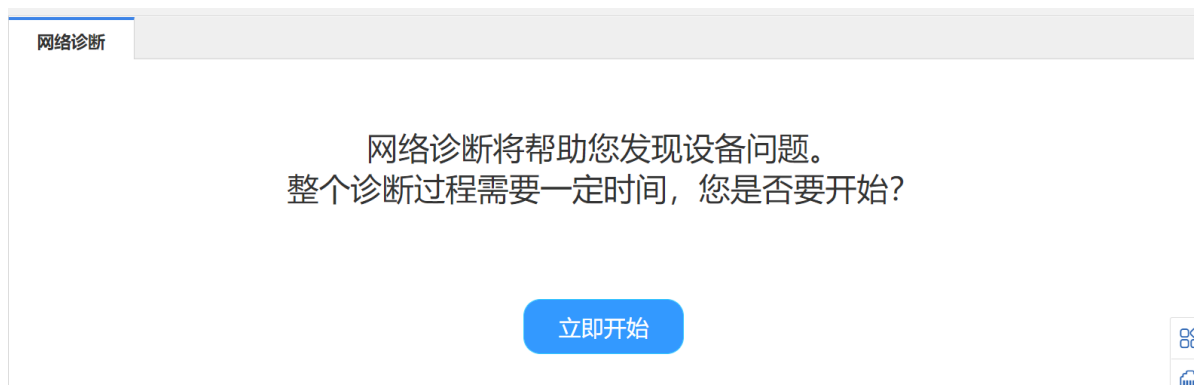


11.6 网络诊断

当设备出现网络问题时，通过本功能可以检测设备配置，并提供处理建议。

【操作步骤】

- (1) 选择[运维]>>[网络诊断]。
- (2) 点击<立即开始>。



(3) 诊断完成后，您可以建议进行配置优化。



11.7 设备审计报告

本功能用于查看设备Web操作日志，并支持导出为报表到本地进行查看。

【操作步骤】

(1) 选择[运维]>>[设备审计报告]。

(2) 选择查询日期，页面下方将展示指定日期当天Web操作记录。

WEB操作日志

请选择需要查看的操作日志: 2022-5-30

导出报表

最近一次删除日志记录: (删除时间) 2022-3-25 06-45-43 , (删除操作ip) 172.26.30.144 , (删除内容) "2022-3-25 14-01-24, 172.26.30.144, admin(配置), 配置认证策略"

时间	操作员的IP	描述	操作
无记录信息			

显示: 10 条 共0条

首页 上一页 下一页 末页 1 确定

(3) 点击<导出报表>，可将Web操作日志导出为报表并下载到本地。

12 高级



说明

不同型号的设备对本章节所介绍的功能的支持情况不同，请以界面实际情况为准。

12.1 管理员权限

本功能用于添加的设备管理员，新增的管理员可以通过Web登录设备进行日常维护或管理，但不能通过Telnet登录设备执行命令。



注意

本页面仅admin用户可以查看和编辑。

【操作步骤】

- (1) 选择[高级]>>[管理员权限]。
- (2) 点击<添加管理员>，进入[添加管理员]页面。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。

管理员权限

说明： 1、旧版本升级上来仍然兼容以前分级分权账号，不影响使用；2、该版本暂不支持对用户web页面授权，新增账号都为超级用户权限。

+ 添加管理员

用户名	操作
无记录信息	

显示: 10 条 共0条

◀ 首页 ◀ 上一页 下一页 ▶ 末页 ▶ 1 确定

- (3) 输入用户名、密码，并确认密码，点击<确定>。

添加管理员

用户名:

密码:

确认密码:

确定 取消

12.2 定时任务

定时任务用于定时在设备上执行指定的CLI命令。通过Console口或Telnet等方式登录设备，并配置添加需要定时执行的CLI命令，然后在本页面添加定时任务，到达指定的执行时间后，设备自动地执行该命令，达到无人值守的目的。有关CLI命令的介绍请参考设备配套的配置命令手册。

目前仅支持创建定时重启任务。

【操作步骤】

- (1) 选择[高级]>>[管理员权限]。
- (2) 将“开启定时任务”开关置于ON状态。

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。

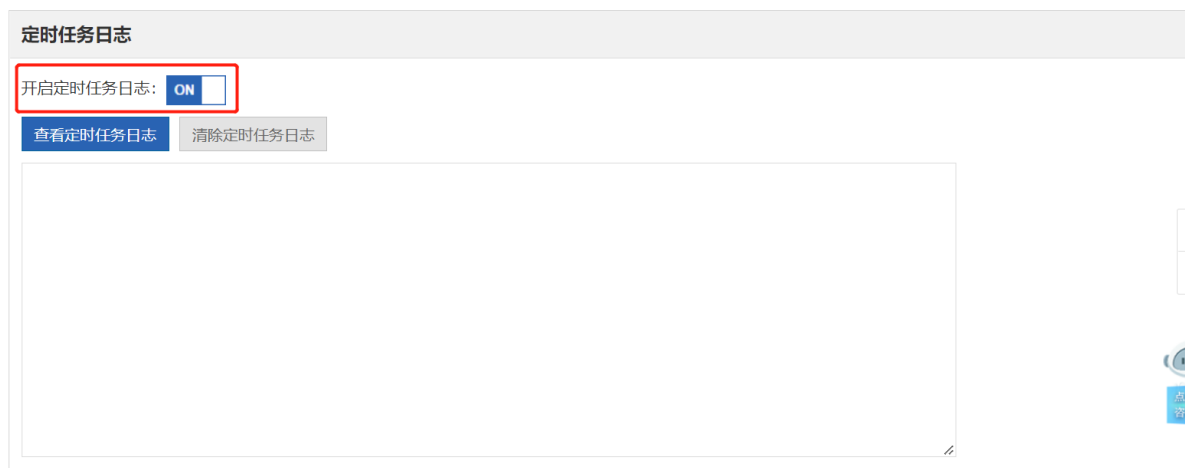
命令模式：分为特权模式与全局配置模式。配置为特权模式的时候执行权限为特权模式权限（即登录设备后的Ruijie#，通常用于执行show命令）；全局配置模式则是执行权限为配置模式权限（即输入config后进入的Ruijie(config)#，通常用于配置一些命令）。

开启定时任务：☒ ON

任务配置

+ 新建重启任务

时间	任务名	命令模式	循环时间	命令	管理
显示: 10 条 共0条					
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495 2496 2497 2498 2499 2500 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 2511 2512 2513 2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524 2525 2526 2527 2528 2529 2530 2531 2532 2533 2534 2535 2536 2537 2538 2539 2540 254					



12.3 License 管理

某些扩展功能（AP支持的用户数量、SSLVPN支持的并发用户数量）需要购买并安装License后才能使用或扩展其数量。本功能用于升级License文件，并展示已经安装的License信息。

【前置条件】

您已通过License授权服务系统购买了正确的License文件。

【操作步骤】

- (1) 选择[高级]>>[License管理]。
- (2) 点击<浏览>，选择您已购买的License文件并上传到设备，点击<开始升级>。



- (3) 升级成功后，页面下方将会展示License信息。

12.4 云服务

12.4.1 功能介绍

NBR设备支持通过诺客云服务（网址为：<http://cloud.ruijie.com.cn/>）进行统一管理，使设备管理更加方便高效。

12.4.2 云服务

该功能用于配置设备与诺客云服务的绑定参数，配置绑定参数后，诺客云服务才能纳管本设备。

⚠ 注意

云服务配置与集中管理功能配置冲突，只能选择配置其中一种功能。

【应用场景】

总分型企业、连锁酒店等需要同时管理多台网关设备的场景。

【前置条件】

设备与诺客云服务之间网络互通。

【操作步骤】

(1) 选择[高级]>>[云服务]>>[云服务]。

(2) 选择绑定方式：

- 账号绑定：输入绑定参数，勾选“阅读并同意<<隐私政策和用户协议>>”，点击<开启云服务并绑定账号>。

ℹ 说明

若无账号点击“立即注册”先注册账号再绑定。

云服务

云预注册

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：

☐ 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：



(3) 成功绑定账号后, 可前往诺客云服务查看并管理设备。

12.4.3 云预注册

开启云预注册功能后, 可以在诺客云服务上直接添加设备序列号绑定设备, 从而对设备进行管理。

设备默认开启云预注册功能, 无需手动开启。



12.5 集中管理

锐捷RAC (Remote Auto-management Center , 远程运维中心)、Ruijie Cloud平台等系统可以对NBR系列网关设备进行集中管理, 并基于全局进行设备性能、VPN、流量、业务情况的监控, 大大提高网管的工作效率。



注意

云服务配置与集中管理功能配置冲突, 只能选择配置其中一种功能。

【应用场景】

总分型企业、连锁酒店等需要同时管理多台网关设备的场景。

【前置条件】

您已部署锐捷RAC或Ruijie Cloud, 并且RAC或Ruijie Cloud平台上已完成相关配置。

【操作步骤】

- (1) 选择[高级]>>[集中管理]。
- (2) 勾选开启集中管理功能, 选择管理类型并配置对接参数:

- 管理类型选择“MCP/WMC管理”、“RCN/WIS管理”时，配置参数如下：

集中管理

集中管理：☒ 开启集中管理 ?

管理类型：

服务端域名： *

设备管理端口： (1至65535, 默认80)

用户名：

密码：

保存设置

- 管理类型选择“RAC-SNC管理”时，配置参数如下：

集中管理

集中管理：☒ 开启集中管理 ?

管理类型：

服务端IP： *

源IP地址：

设备管理端口： (1至65535, 默认8088)

性能监控管理端口： (10000至65000, 默认30000)

用户名：

密码：

保存设置

(3) 配置完成后，点击<保存设置>即可。

12.6 第三方日志

本功能用于设备生成的日志信息（如无线终端上下线信息、审计日志等）并发送到第三方日志服务器或Elog日志系统。

⚠ 注意

设备与第三方日志服务器或Elog日志系统之间必须网络互通，否则会导致日志上传失败。

12.6.1 配置第三方服务器

- 选择[高级]>>[第三方日志]>>[第三方服务器配置]。
- 勾选开启第三方服务器功能，并选择第三方日志服务器。

第三方服务器配置

ELOG

第三方日志配置

提示：开启第三方服务器功能（ELOG除外），会导致WEB认证无感知、商业营销认证获取MAC地址、本地服务器认证获取MAC地址功能失效。

第三方服务器功能：☒ 开启

选择第三方服务器：

第三方日志服务器

无线终端信息收集：☒ AP厂商锐捷，通过【SNMP】收集信息 ☐ AP厂商，通过SYSLOG收集信息

第三方日志服务器列表

+

添加

×

删除选中

☐	第三方日志服务器名称	第三方日志服务器类型	操作
无记录信息			

显示

10

条 共0条

首页

上一页

下一页

末页

1

确定

MCP联动配置，仅在网关设备不做NAS的情况下开启。

认证系统功能：☐ 开启与MCP对接，获取认证用户上下线信息

保存

(3) 根据实际情况选择无线终端信息收集场景，AP厂商是锐捷时，设备通过SNMP协议收集AP上下线信息；AP厂商不是锐捷时，设备通过Syslog方式收集AP上下线信息。

第三方服务器配置

ELOG

第三方日志配置

提示：开启第三方服务器功能（ELOG除外），会导致WEB认证无感知、商业营销认证获取MAC地址、本地服务器认证获取MAC地址功能失效。

第三方服务器功能：☒ 开启

选择第三方服务器：

第三方日志服务器

无线终端信息收集：☒ AP厂商锐捷，通过【SNMP】收集信息 ☐ AP厂商，通过SYSLOG收集信息

第三方日志服务器列表

+

添加

×

删除选中

☐	第三方日志服务器名称	第三方日志服务器类型	操作
无记录信息			

显示

10

条 共0条

首页

上一页

下一页

末页

1

确定

MCP联动配置，仅在网关设备不做NAS的情况下开启。

认证系统功能：☐ 开启与MCP对接，获取认证用户上下线信息

保存

(4) 点击<添加>按钮，进入[添加第三方日志服务器]页面，配置服务器参数和数据采集参数。

 说明

服务器类型不同，需要配置的服务器参数和数据采集参数不同，请以界面实际情况为准。

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

(5) 确认配置无误，点击<保存>，页面上方将显示第三方服务器的相关配置菜单。

第三方服务器配置

场所基本信息 设备基本信息 状态信息 第三方日志配置

提示： 开启第三方服务器功能（ELOG除外），会导致WEB认证无感知、商业营销认证获取MAC地址、本地服务器认证获取MAC地址功能失效。

第三方服务器功能：☒ 开启

选择第三方服务器：

第三方日志服务器

无线终端信息收集：☒ AP厂商锐捷，通过【SNMP】收集信息 ☐ AP厂商，通过SYSLOG收集信息

第三方日志服务器列表

添加 删除选中

☐	第三方日志服务器名称	第三方日志服务器类型	操作
☐	服务器1	任子行	编辑 删除

显示:

10

 条 共1条

首页 上一页 1 下一页 末页

1

确定

MCP联动配置，仅在网关设备不做NAS的情况下开启。

认证系统功能：☐ 开启与MCP对接，获取认证用户上下线信息

保存

(6) 配置第三方日志服务器所在场所的信息：

a 点击进入[场所基本信息]页面，点击<添加场所基本信息>。

第三方服务器配置

场所基本信息 设备基本信息 状态信息 第三方日志配置

说明： 导入场所基本信息的文件名必须以.csv为后缀。

添加场所基本信息 删除选中

请选择服务器名称

导出场所基本信息

Choose File No file chosen

导入场所基本信息

☐	上网服务场所编码	上网服务场所名称	第三方日志服务器名称	所属省	所属城市	所属分区	操作
无记录信息							

显示:

10

 条 共0条

首页 上一页 1 下一页 末页

1

确定

b 输入场所所在地理位置、负责人等详细信息，点击<保存>。

添加场所基本信息

第三方日志服务器名称：

服务器1

上网服务场所编号： * 14位数字

上网服务场所名称： *

经营法人： *

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： *

负责人联系电话： *

保存

关闭

(7) 配置第三方日志服务器所在场所中的AP信息：

a 点击进入[设备基本信息]页面，点击<添加AP基本信息>。

第三方服务器配置

场所基本信息

设备基本信息

状态信息

第三方日志配置

说明： 导入AP基本信息的文件名必须以 .csv为后缀。

Choose File

No file chosen

导入AP基本信息

+ 添加AP基本信息

× 删除选中

请选择服务器名称

场所名称：

导出AP基本信息

☐	上网服务场所编码	上网服务场所名称	MAC地址	名称	创建时间	操作
无记录信息						

显示：

10

 条 共0条

首页 上一页 下一页 末页

1

确定

b 选择AP所属的服务场所，点击<保存>。

添加AP基本信息

上网服务场所编号：

点击选择场所编码

 *

保存

关闭

c 输入AP信息，点击<保存>。

(8) 点击进入[第三方日志配置]页面，选择要收集的日志类型，然后点击<保存设置>。

(9) (可选) 配置完成后，点击进入[状态信息]页面，可查看日志发送结果。

序号	文件	时间	失败原因
1	/tmp/plog/服务器1/NETSITE16/20220706185559_211_123_320000_754961764_008.log	2022-07-06 18:58:59	无法连接到远程主机
2	/tmp/plog/服务器1/NETSITE16/20220706185059_736_123_320000_754961764_008.log	2022-07-06 18:53:59	无法连接到远程主机

12.6.2 配置 Elog

- (1) 选择[高级]>>[第三方日志]>>[第三方服务器配置]。
- (2) 勾选开启第三方服务器功能，第三方日志服务器选择“ELOG”。

第三方服务器配置 ELOG 第三方日志配置

提示：开启第三方服务器功能（ELOG除外），会导致WEB认证无感知、商业营销认证获取MAC地址、本地服务器认证获取MAC地址功能失效。

第三方服务器功能：☒ 开启

选择第三方服务器：ELOG

MCP联动配置，仅在网关设备不做NAS的情况下开启。

认证系统功能：☐ 开启与MCP对接，获取认证用户上下线信息

保存

- (3) 点击<保存>，页面上方将显示ELOG服务器的相关配置菜单。

第三方服务器配置 ELOG 第三方日志配置

提示：开启第三方服务器功能（ELOG除外），会导致WEB认证无感知、商业营销认证获取MAC地址、本地服务器认证获取MAC地址功能失效。

第三方服务器功能：☒ 开启

选择第三方服务器：ELOG

MCP联动配置，仅在网关设备不做NAS的情况下开启。

认证系统功能：☐ 开启与MCP对接，获取认证用户上下线信息

保存

- (4) 点击进入[ELOG]页面，输入ELOG服务器地址，并选择认证账号类型及是否开启日志压缩和无线日志功能。

第三方服务器配置 ELOG 第三方日志配置

提示：
1、如需使用双ELOG功能传送无线终端的上下线日志，需要配备单独硬件AC；
2、网关设备本身开启的无线功能，其无线终端上下线日志仅支持发给第一台ELOG；

服务器地址： * 格式：http://ruijie.com

服务器地址1： 格式：http://ruijie.com

源IP： ? 格式：192.168.23.14

认证账号类型：手机号

日志压缩功能：☐ 开启日志压缩 对生成的日志使用压缩的形式发送到服务器，开启该功能前请确认服务器支持解压缩。

无线日志功能：☐ 开启无线终端上下线信息上传 开启后，会导致WEB认证无感知、商业营销认证获取MAC地址、本地服务器认证获取MAC地址功能失效。

保存设置

- (5) 配置完成后，点击<保存设置>。
- (6) 点击进入[第三方日志配置]页面，选择要收集的日志类型。

第三方服务器配置

ELOG

第三方日志配置

开启第三方日志：☐全部开启

☐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

保存配置

(7) 配置完成后，点击<保存设置>。

12.7 动态域名解析

动态域名解析功能用于实现固定域名到动态IP地址之间的解析。

【操作步骤】

- (1) 选择[高级]>>[动态域名解析]。
- (2) 点击<添加>，进入[添加账号]页面。

动态域名解析

动态域名解析： 功能是实现固定域名到动态IP地址之间的解析。
说明： 最多可以配置8个账号。
注意： 若您需要进行升级，且升级版本低于11.9(1)B29版本，在升级完成后需重新配置此功能。

+添加 X删除选中 刷新

☐	账号	动态域名服务	域名	绑定接口	状态	操作
☐	花生壳1	花生壳		无	连接中	编辑 删除
☐	花生壳2	花生壳		无	连接中	编辑 删除
☐	3322a	3322	aaa.com	无	异常	编辑 删除
☐	3322a	3322	bbb.com	无	异常	编辑 删除

显示 10 条 共4条

首页 上一页 1 下一页 末页 1 确定

(3) 选择服务提供者、接口，并输入您的花生壳或3322服务的用户名和密码。若无账号请先注册账号。

添加账号

服务提供者：

花生壳（www.oray.net）

[【没有帐号请先注册】](#)

接口：

请选择接口

用户名：*

密码：*

保存 关闭

(4) 点击<保存>。

12.8 系统日志

12.8.1 服务器日志

本功能用于配置Elog日志系统信息，设备对接Elog日志系统后，可将指定类型的日志发送Elog日志系统。

【前置条件】

设备与Elog日志系统之间网络互通。

您已在[首页]>>[服务]页面开启“服务器日志”功能。

【操作步骤】

- (1) 选择[高级]>>[系统日志]>>[服务器日志]。
- (2) 选择日志上传方式，并输入Elog日志系统服务器IP、端口，并选择要上报的日志类型。

服务器日志

查看系统日志

SYSLOG服务器配置

说明：设备端口号设置需和对端服务器端口号保持一致。若对端是snc服务器则支持CPU、内存使用率日志，硬盘使用日志，接口会话审计，IP流量审计以及接口流量审计日志；若对端是ELOG服务器则支持流日志，URL审计，IM审计日志，BBS审计日志，邮件审计日志，端口号需设置20000及以上；

注意：优先级高的日志先发送，0最高，7最低。文件上传方式只能设置一个，且没有区分日志优先级，日志类型只能设置文件或实时。http的端口需要与服务器http协议用的端口保持一致。

日志上传方式：☒ 实时上传 ☐ 文件上传

服务器IP：

端口： (10000-65000)

服务器类型：

源IP：

☒ 发送日志类型

☐ 开启流日志

☐ CPU、内存使用率日志

☐ 硬盘使用日志

☐ 开启URL审计

☐ 接口会话数审计

☐ IP应用流量审计

☐ IP会话数审计

☐ 通道流量审计

☐ 接口流量审计

☐ IP在线时长审计日志

☐ 邮件审计日志

☐ 搜索引擎审计日志

☐ BBS审计日志

☐ IM审计日志

☐ 应用在线时长审计日志

☐ 缓存资源点击统计

保存设置

服务器IP	日志上传方式	服务器类型	端口	日志类型	其他信息	操作
无记录信息						

显示： 条 共0条

首页 上一页 下一页 末页

1 确定

- (3) 配置完成，点击<保存设置>即可。

12.8.2 查看系统日志

本功能用于查看和导出系统日志。

【操作步骤】

- (1) 选择[高级]>>[系统日志]>>[查看系统日志]。
- (2) 点击<更新当前系统日志>按钮，可刷新日志信息，如下图所示。

查看系统日志 SYSLOG服务器配置

配置syslog日志
配置syslog日志用于客户协助售后及研发定位问题

☒ 配置syslog日志开关

确定 导出日志

系统日志 (show log)

更新当前系统日志

*Jun 1 04:39:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/3, changed state to up.

*Jun 1 04:39:13: %LINK-3-UPDOWN: Interface GigabitEthernet 0/3, changed state to up.

*Jun 1 04:37:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/3, changed state to down.

*Jun 1 04:37:20: %LINK-3-UPDOWN: Interface GigabitEthernet 0/3, changed state to down.

*Jun 1 01:16:47: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host 192.168.23.33

*Jun 1 01:16:47: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host 192.168.23.33

(3) 勾选“配置syslog日志开关”，点击<确定>。然后点击<导出日志>按钮，可将系统日志导出并下载到本地。

注意

必须勾选“配置syslog日志开关”并确定才能导出日志。

查看系统日志 SYSLOG服务器配置

配置syslog日志
配置syslog日志用于客户协助售后及研发定位问题

☒ 配置syslog日志开关

确定 导出日志

12.8.3 SYSLOG 服务器配置

配置SYSLOG服务器后，设备将会定时向指定服务器发送Syslog格式日志。

【前置条件】

设备与SYSLOG服务器之间网络互通。

SYSLOG服务器上已经完成日志接收的相关配置。

【操作步骤】

(1) 选择[高级]>>[系统日志]>>[SYSLOG服务器]。

(2) 输入Syslog服务器IP地址及端口号，点击<保存配置>。

说明

若设备只能通过管理口与服务器进行网络通讯时，请勾选“通过管理口发送日志”。

查看系统日志

SYSLOG服务器配置

Syslog服务器IP:

* 格式: 192.168.23.14

端口:

514

* (1-65535, 默认514, 小于1024的端口确保没有被其他UDP使用)

通过管理口发送:

☐ 通过管理口发送日志

保存设置

清除设置

12.9 日志策略

通过日志策略，可以控制指定用户、IP或IP段是否将日志上报给第三方服务器或Elog日志系统，以及上报的日志类型。

【操作步骤】

(1) 选择[高级]>>[日志策略]。

(2) 点击<添加日志策略>。

日志策略

+ 添加日志策略

× 删除选中

查询策略:

查找

☐	策略名	管理用户	日志类型	匹配顺序	操作
无记录信息					

显示:

10

 条 共0条

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶▶

1

确定

(3) 在页面上方弹出的提示框中点击<确定>。

192.168.21.16:14430 显示

如需配置第三方日志请到首页-功能管理菜单开启相应日志类型

确定

(4) 在[添加策略]页面，输入策略名称，选择要上报的日志类型，并设置关联的用户或IP，点击<保存>即可。

⚠ 注意

- 日志类型选择“第三方日志”或“82号令日志”时，必须先在[首页]>>[功能管理]页面启动“第三方日志”或“服务器日志”功能模块。
- 日志类型选择“第三方日志”表示该类日志将会被发送到第三方日志服务器，有关第三方日志服务器的介绍请参见[12.6.1 配置第三方服务器](#)。
- 日志类型选择“82号令日志”表示该类日志将会被发送到Elog日志系统，有关Elog日志系统的配置请参见。
- 日志类型选择“关闭日志”表示不发送指定用户或IP的日志。

添加策略

策略名称: *

日志类型: ☒ 第三方日志 ☐ 82号令日志 ☐ 关闭日志

关联类型: ☒ IP ☐ 用户

单IP : * 例: 192.168.1.1

保存

关闭

12.10 投屏服务

投屏功能是指将手机屏幕投放到电视机上。在酒店行业，每个酒店的每个房间几乎都标配一台电视机，通常情况下，酒店内电视和移动终端在同一局域网内，导致在酒店内会产生电视错投、乱投的情况。对于客户来说，酒店的电视只是一个摆设，体验也不好。

锐捷睿易NBR系列网关所支持的定点投屏功能，可以解决上述问题，通过网络规划隔离电视和移动终端后，NBR系列网关作为投屏代理，可以将不在同一局域网内的电视和移动终端进行一对一的绑定，从而实现酒店内定点投屏的效果。

【应用场景】

针对酒店投屏场景而设计，一些简单的跨VLAN拓扑也可以使用本功能。

【操作步骤】

(1) 网段配置：

a 选择[高级]>>[投屏服务]>>[网段配置]。

投屏配置

高级配置

网段配置

状态信息

说明：使用投屏功能必须进行网段配置，对客户终端和酒店投屏设备进行互访限制，消除客户终端应用绕过映射管理直接投屏的隐患。配置后的电视网段和终端网段在扫码配对前无法通信。

添加

删除选中

☐	网段类型	网段范围	操作
无记录信息			

显示: 10 条 共0条

首页

上一页

下一页

末页

1

确定

b 点击<添加>，配置隔离网段，设置酒店电视网段。

390

网段配置

网段类型：

酒店电视网段

网段范围： -

格式如：1.1.1.1-1.1.1.2.30 ,填1.1.1.1-1.1.1.1代表单个IP

保存

关闭

- c 配置完成，点击<保存>。
- d 并按同样的方法设置客户终端网段，配置完成页面显示如下（下图仅作参考）。

投屏配置

高级配置

网段配置

状态信息

说明：使用投屏功能必须进行网段配置，对客户终端和酒店投屏设备进行互访限制，消除客户终端应用绕过映射管理直接投屏的隐患。配置后的电视网段和终端网段在扫码配对前无法通信。

添加

删除选中

☐	网段类型	网段范围	操作
☐	酒店电视网段	192.168.1.1 - 192.168.1.100	编辑 删除
☐	客户终端网段	192.168.2.1 - 192.168.2.100	编辑 删除

显示：

10

 条 共2条

首页

上一页

1

下一页

末页

1

确定

(2) 投屏配置：

- a 选择[高级]>>[投屏服务]>>[投屏配置]。
- b 点击开启投屏功能开关，将其置于ON状态。

投屏配置

高级配置

网段配置

状态信息

说明：投屏服务能在内网跨网段支持苹果和安卓投屏功能，终端入网后通过扫码绑定某一房间后，可以在房间号相同的设备上使用投屏。投屏服务支持的使用范围包括苹果设备的镜像、苹果和安卓应用程序的投屏功能，不支持安卓手机自带的手机镜像功能（部分手机上为“无线显示”）。

帮助：[定点投屏如何配置？](#)

开启投屏功能：

ON

当前匹配模式：☒ IP模式（电视用IP地址进行映射匹配） ☐ MAC模式（电视用MAC地址进行映射匹配）

添加

删除选中

手工绑定

选择文件

未选择任何文件

导入

帮助

下载导入模板

导出二维码

导出选中

导出所有

基于

房间号

 查询映射：

查找

☐	房间号	电视IP	操作
无记录信息			

显示：

10

 条 共0条

首页

上一页

下一页

末页

1

确定

- c 根据实际情况选择匹配模式，点击<添加>按钮，将房间号和电视IP地址或电视MAC地址绑定。

说明

- 切换匹配模式会清空原有配置，请谨慎操作。
- 一个房间号只能绑定一个IP地址或一个MAC地址。

当前匹配模式: ☐ IP模式 (电视用IP地址进行映射匹配) ☒ MAC模式 (电视用MAC地址进行映射匹配)

添加 **删除选中** **手工绑定** 未选择任何文件 **导入** **帮助: ?** [下载导入模板](#) 导出二维码: **导出选中** **导出所有**

基于 查询映射: **查找**

☐	房间号	电视MAC	操作
无记录信息			

显示: 条 共0条 ◀ 首页 ◀ 上一页 下一页 ▶ 末页 ▶ **确定**

d 配置完成点击<完成配置>即可。

创建映射

房间号:

电视IP:

格式: 192.168.1.1, 只能配置1个IP!

完成配置

取消

创建映射

房间号:

电视MAC:

格式: 2222.2222.2222, 只能配置1个MAC!

完成配置

取消

(3) (可选) 高级配置：

- a 选择[高级]>>[投屏服务]>>[高级配置]。
- b 根据需要选择是否开启投屏认证功能及其他投屏参数。



注意

每一项配置完成都需要点击后面的<保存>按钮，否则配置不生效。

投屏配置

高级配置

网段配置

状态信息

联动认证组件：

☒ 需要开启认证功能，认证在线才能使用投屏功能
 ☐ 不需要开启认证功能，即可使用投屏功能

保存联动认证组件配置

定时下线时间：

关闭

保存

开启电视自动注册：

OFF

开启终端授权模式：

OFF

(待授权电脑终端的系统仅支持macOS)

电视通讯密钥：

保存

(用于电视请求url)

电视投屏url密钥：

保存

(电视投屏url/二维码生成时使用的密钥，修改后原有url/二维码失效)

投屏二维码有效时间：

480

分钟

保存

(范围：1 - 43200)

(4) (可选) 查看投屏情况：

- 选择[高级]>>[投屏服务]>>[状态信息]。
- 查看各个房间的投屏情况，支持基于房间号、电视IP、终端IP/账号三种方式查找投屏数据。

投屏配置

高级配置

网段配置

状态信息

基于

房间号

▼

查询映射：

查找

房间号	电视IP	终端IP / 账号	绑定方式	操作
无记录信息				

显示：

10

▼

条 共0条

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶

1

确定

12.11 VRRP 配置

12.11.1 功能介绍

VRRP (Virtual Router Redundancy Protocol，虚拟路由冗余协议) 是一种路由容错协议。VRRP功能将可以承担网关功能的一组设备加入到备份组中，形成一台虚拟路由器，并为该虚拟路由器指定虚拟IP地址，然后过选举机制决定哪台路由器作为主设备，承担转发任务。局域网内的主机仅需要知道这台虚拟路由器的虚拟IP地址，并将其设置为网关的IP地址即可通过这台虚拟路由器与外部网络进行通信。

VRRP采用主备模式，一般情况下，由主设备承担报文转发任务，若主设备发生故障，则处于备份状态的设备将会代替原来的主设备转发报文，确保业务流量能正常转发，大大提高了链路的可靠性。

 注意

VRRP配置页面配置的指定接口、组号不能与单地址VRRP配置的指定接口、组号冲突

12.11.2 VRRP 配置

【应用场景】

在连接局域网的设备上可以配置多个备份组，局域网中的主机分别以各备份组的虚拟IP作为网关，备份组中的路由设备互相作为主路由设备和备份路由设备。

【操作步骤】

- (1) 选择[高级]>>[VRRP配置]>>[VRRP配置]。
- (2) 输入VRRP组号、组IP及优先级，点击<添加设置>。

VRRP配置

单地址VRRP配置

说明：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。

提示：输入的VRRP组IP和接口IP地址相同的情况下会设置VRRP优先级为 255。

指定接口：☒ Gi0/0 ☐ Gi0/1 ☐ Gi0/2 ☐ Gi0/3

VRRP组号： * (1-255)

VRRP组IP： *

VRRP优先级： (1-254)

添加设置

删除全部

VRRP组号	接口	VRRP组IP	VRRP优先级	操作
无记录信息				

显示: 10 条 共0条

首页 上一页 下一页 末页 1 确定

配置项	说明
指定接口	在指定接口上启用VRRP功能
VRRP组号	取值范围为1~255
VRRP组IP	即虚拟路由器的IP地址，局域网中的主机以该IP为默认网关
VRRP优先级	数值越大优先级越高，优先级高的备份组将会作为主路由设备承担转发报文工作。不同优先级的VRRP组之间互为主备关系

- (3) （可选）根据需求可以继续添加VRRP组。

12.11.3 单地址 VRRP 配置

【应用场景】

单外网地址的场景下的双机冗余备份。

【操作步骤】

- (1) 选择[高级]>>[VRRP配置]>>[单地址VRRP配置]。
- (2) 根据以下信息配置单地址VRRP功能。

VRRP配置

单地址VRRP配置

说明：为了实现单外网地址的场景下的双机冗余备份，我们推出VRRP单地址方案。该方案除了满足冗余备份，还支持多种形式的外网IP配置，满足控制器远程管理设备。这个方案具体支持功能如下：1、在单个外网IP地址的条件下通过两台设备实现冗余备份。2、外网线路类型支持静态、DHCP或者拨号。3、双机设备都可以同时连接到控制器进行远程管理。

注意：使用单外网地址VRRP方案，跟踪的外网口IP地址必须配置成mac地址一致。

提示：目前不支持多拨，指定接口的IP不能与VRRP组IP相同。

指定接口：☒ Gi0/0 ☐ Gi0/1 ☐ Gi0/2 ☐ Gi0/3

VRRP组号： * (1-255)

VRRP组IP： *

VRRP优先级：☒ 主设备 ☐ 从设备

通讯内网口：☐ Gi0/0 ☐ Gi0/1 ☐ Gi0/2 ☐ Gi0/3

通讯外网口：☐ Gi0/4 ☐ Gi0/5

跟踪外网口：☐ Gi0/4 ☐ Gi0/5

保存设置

清除设置

配置项	说明
指定接口	在指定接口上启用VRRP功能
VRRP组号	取值范围为1~255
VRRP组IP	即虚拟路由器的IP地址，局域网中的主机以该IP为默认网关
VRRP优先级	设置本设备角色，主设备将承担转发报文工作。主设备故障后，会从备设备中选举一个新的主设备承担转发工作。
通讯内网接口	● 必须配置1个通讯内网接口 ● 通讯内网接口不能和通讯外网接口相同 ● 不支持聚合口
通讯外网接口	● 不支持聚合口 ● 通讯外网接口的IP地址必须设置静态IP地址，且已配置了IP地址和下一跳（不支持拨号口）
跟踪外网接口	跟踪外网接口用于探测通讯外网口链路是否正常 注意： ● 不支持聚合口 ● 若跟踪外网口的IP设置为静态IP类型，则必须配置接口IP地址 ● 跟踪外网口可选1-3个，但不能与通讯外网口相同 ● 切换跟踪外网接口时，会清空原跟踪口的配置

(3) 确认配置无误，点击<保存设置>即可。

12.12 防共享接入

12.12.1 一键防共享

开启一键防共享后，会按照预定义的防共享策略下发配置。您可以在防共享策略页面添加或修改防共享策略。

开启一键防共享后，对于共享接入的用户，设备将按照防共享策略中设置的惩罚方式对用户进行只检测不阻断、阻断或限速等操作。关闭一键防共享后，防共享策略都会被清空。

【操作步骤】

- (1) 选择[高级]>>[防共享接入]>>[一键防共享]。
- (2) 将“开启一键防共享”的开关置于开启状态。



12.12.2 防共享策略

通过防共享策略可以对指定的用户进行检测，对共享接入的用户进行只检测、阻断或限速。

【操作步骤】

- (1) 选择[高级]>>[防共享接入]>>[防共享策略]。
- (2) 点击<添加防共享策略>，进入[添加防共享策略]页面。



- (3) 选择用户和惩罚方式。其中，选择“只检测”则会只检测用户是否存在共享接入行为，不进行任何限制；选择“不允许上网”将会阻断共享接入的用户的网络；选择“限速上网”将会对共享接入的用户的网络进行限速。

三 添加防共享策略

×

选择用户：所有用户 本地用户 ▾ 【选择用户】

惩罚方式： ☐ 只检测 ☐ 不允许上网 ☒ 限速上网

限速带宽： 上行 Kbps 下行 Kbps

阻断时长： 10 分钟

确定

取消

- (4) 配置完成后，点击<确定>。
- (5) （可选）对于不需要监测的用户，点击<配置免监控用户>可以将其添加到白名单中，设备不会对白名单中用户进行检测。
- (6) （可选）点击<自定义防共享标准>可以设置共享行为。

12.12.3 实时监测状态

本功能用户展示检测结果，并支持基于IP、用户、用户类型、用户状态等条件查询检测信息。

【操作步骤】

- (1) 选择[高级]>>[防共享接入]>>[实时监测状态]。
- (2) 选择查询条件，点击<查询>按钮即可查看满足条件的监测结果。

一键防共享

防共享策略

实时监测状态

用户监测信息查询：

用户类型 ▾

☒ 本地用户 ☐ 认证用户

查询

IP	用户名	用户类型	状态	时间	终端信息	操作
无记录信息						

显示： 10 条 共0条

◀ 首页 ◀ 上一页 下一页 ▶ 末页 ▶▶

1

确定

12.13 启用防封杀

ADSL线路通常会限制一条线路上的上网终端个数，超出的终端将无法上网，开启本功能后可尽量绕开该限制，实现上网终端数不受限。

【操作步骤】

- (1) 选择[高级]>>[启用防封杀]。
- (2) 选择要启用防封杀的接口，点击<保存配置>。

启用防封杀

说明：端口启用此功能，可以尽量避免ISP封杀共享，主要用于ADSL线路。

注意：ADSL线路通常会限制一条线路最多上网终端个数（超出的终端将无法上网），开启功能后可尽量绕开此限制，实现上网终端数不受限！

启用防封杀接口：☐ Gi0/3 ☐ Gi0/4

保存设置

12.14 加速-应用缓存

应用缓存是一种针对手机应用的缓存功能，可以缓存所有安卓和苹果的应用文件，也可以只缓存指定厂家的应用文件。用户可以直接从本设备下载应用文件，可以大大提高下载速率，提升用户体验。

应用缓存的工作原理是手机用户通过HTTP协议下载应用安装文件，第一次下载时，设备识别出URL中含有的apk或ipa文件的下载链接，并对应答的报文进行缓存。再有用户下载相同应用文件时，网关设备会直接构造应答报文并反馈给手机用户。

【操作步骤】

- (1) 选择[高级]>>[加速-应用缓存]。
- (2) 点击应用缓存开关，将其置于ON状态。
- (3) 根据实际情况勾选应用类型，包括安卓应用和苹果应用，并点击<保存设置>。

加速-应用缓存

说明：当地址为域名时，需要先 [【配置dns】](#)。不支持以https开头的域名！本模块使用了tcp代理，会跟上网屏蔽模式冲突，请确认已关闭上网屏蔽模式

注意：Apple应用商店的下载服务器域名为'iosapps.itunes.apple.com'，建议配置

应用缓存：☒ ON [【最近缓存详情】](#)

应用缓存容量（已使用：0B，总容量：100.00MB） 硬盘容量（未使用：132.05MB，总容量：139.22MB）

应用选择

手机应用：☒ 苹果应用 ☒ 安卓应用

保存设置 删除全部

- (4) 设置存储原始应用文件的服务器IP地址或域名，并点击<保存设置>。

说明

单击<添加>可以继续添加服务器。

应用服务器地址

☐ 全部HTTP（端口80）

地址1: * [X 删除](#) [+ 添加](#)

保存设置 删除全部

(5) 设置要缓存到网关设备本地的应用文件名，并点击<保存设置>。

 说明

单击<添加>可以继续添加应用名。

缓存指定应用-应用名  (本功能只适用于安卓与苹果应用)

应用名1: * 

 添加

保存设置

删除全部



(6) 对于指定下载地址的应用，用户访问该地址后10分钟内下载的应用才被缓存。

 说明

单击<添加>可以继续添加地址。

缓存指定应用-时间窗 

地址1: * 

 添加

保存设置

删除全部