

WEB 管理手册

RG-NBR 系列出口网关

NBR_RGOS 11.9(4)B11P1

文档版本 : V1.0

copyright © 2019 锐捷网络

版权声明

copyright © 2019 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内容或全部进行复制、摘录、备份、修改、 传播、翻译成其他语言、将其全部或部分用于商业用途。



以上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,本文档中描述的全部或部分产品、服务或特性可能不在您的购买 或使用范围之内。除非合同另有约定,锐捷网络对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因,本文档内容会不定期进行更新。锐捷网络保留在没有任何通知或者提示的情况下对文档内容进行修改的权利。

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

前 言

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

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



本书约定

1. 命令行格式约定

命令行格式意义如下:

粗体:命令行关键字(命令中保持不变必须照输的部分)采用加粗字体表示。

斜体:命令行参数(命令中必须由实际值进行替代的部分)采用斜体表示

[]:表示用[]括起来的部分,在命令配置时是可选的。

{ x | y | ... }:表示从两个或多个选项中选取一个。

- [x|y|...]:表示从两个或多个选项中选取一个或者不选。
- //:由双斜杠开始的行表示为注释行。
- 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:

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

1 Web 配置指南

1.1 概述

本章节说明使用 Web 管理系统的方法,您可以使用这个 Web 管理系统来管理您的 NBR 路由器的常用功能。 用户使用浏览器 (如 IE)访问 WEB 管理系统来管理 NBR 设备。

🥑 目前该文档仅适用于 NBR 🗆 🗆 🗆 🗆 🗆

1.2 典型应用

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

1.2.1 通过 WEB 管理设备

应用场景

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

图 1-1



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

功能部属

▶ 配置环境要求

客户端的要求:

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

1.3 WEB 管理系统

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

1.3.1 进入 WEB 管理界面

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

	┌ 锐捷网络	
	⊢⇒ C	🗋 192.168.1.1/index.htm
Û	在复位或初续	台情况下默认的 WEB □ □ □ □ □ □ □ http://192.168.1.1□
Û	□□□□ htt	ps 🗆 🗆 🗆 🗆 🗆 🗆 🗠 https://192.168.1.1:4430
Û		
Û		PC Gi0/0
i]

第二步:进入系统登录界面,如下图所示:



②WEB | ©2000-2015 锐捷网络 | 人工客服 | 客服电话: 4001 000 078 | 客服中心微信 闘 | 技术支持论坛

- 1、 输入用户名和密码然后点击 登录 按钮,进入设备管理的主界面。
- 2、 如果您忘记了用户名或密码 , 请点击 忘记密码 ?。
- 3、 如果需要客服帮助 , 请点击 人工客服 和客服进行在线交流。
- 4、 密码重置功能,如果你想重置默认密码,可以按长按 reset 按钮,然后在 web 上登录根据提示重置密码,是否需要保存配置,操作如下图。

没交	192.168.23.94 上的网页显示:	×	WEB前端开发-W	
	设备上存在备份文件,是否进行恢复?(注意恢复过程会重 启)			
	确定 取消]		
•	安持的近视器:IE8~IE11,容载,360近视器 admin ** ** 正在登录			
	忘记期码 ?			

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





用户名或者密码不正确!您还有剩下4次尝试机会!

admin

•

登录

忘记密码?



1.3.2 快速配置

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

① □□□□□ WEB □□□□□□□□□□□□ "□□ 变更向导"□□□□□□□□□

1.3.2.1 快速配置

(1) 重置密码

6

Ruffe税捷 NBR1000G-E	
	● 重置密码
	请重新设置管理员密码 当前密码为默认密码,为揭高系统安全性,请修改密码
	用户名: admin 新密码:
	确认密码: 确认修改

©2000-2018 锐捷网络 | 在线客服 | 客服:4001 000 078

(2) 场景选择



请选择您的网络场景



©2000-2018 锐捷网络 | 论坛 | 在线客服 | 客服: 4001 000 078

(3) 接口配置

Rujje 税捷 NBR1700G-E 作	
<u>車</u> 古 公 台	选择物景 接山配置 Win设置 保存配置
Gi0/3 外网口: IIIII WAN2	GI0/4 GI0/5 Control Control C
WAN1(GI0/4)	: 动态IP(DHCP) ▼
Gi0/0 内网口: 🛄 LANO	GiD/1 GiD/2
LAN0(Gi0/0):	192.168.1.1 - 255.255.255.0
	上—步 下—步
~	暂不配置>
64	©2000-2018 税捷网络 论坛 在线客服 客服: 4001 000 078
(4) 智能流控	
Ruíje 説捷 NBR1700G-E 作	快速配置向导
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	- 🌝 🕑 () () 选择场景 接口配置 智能流控 WIFi设置 保存配置
请填写线路	带宽以开启智能流控,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,建议不开启流控即可。
Gi0/3	GI04 GI05
WAN2	WAN1 WAND
WAN1(Gi0/4)): 下行: 10 - 上行: 10 Mbps
WAN0(Gi0/5)): 下行: 10 - 上行: 10 Mbps
	上一步下一步
	上一步 ©2000-2018 税捷网络 论坛 在线套服 套服: 4001 000 078

✓ —	🕗	😔		— o —	
<u>重置</u> 密码	选择场景	接口配置	智能流控	WiFi设置	
		用于管理其下连接	的AP发射无线信号	<u>1</u>	
	,	WiFi名称: 1	*		
		WiFi密码: ••••••		冯	
		上一步	下一步		

正在下发配置,请勿做其它操作,请稍候... 34% 34%

©2000-2018 锐捷网络 | 论坛 | 在线客服 | 客服: 4008 111 000

Rujje 税捷 EG2000K 快	速配置向导				日
	✓ → → → → → → → → → → → → → → → → → → →	🥪 接口配置	😔 智能流控	😔 保存配置	
		⊘ 恭喜您	、, 配置成功~		
	外网连通性检测	(请确认网络线路已接入局	5进行检测)	立即检测	
	如何使用手机进	行远程管理?		>	
	配置清单			>	
		目	首页		
		推荐	配置		

©2000-2018 锐捷网络 | 论坛 | 在线客服 | 客服: 4008 111 000

(7) 配置清单

如何使用手机进行远程管理?
1.关注"锐捷诺客MACC"微信公众号 2.扫描下方二维码,将该设备添加至诺客 MACC平台
配置清単
 ◆接口配置
Gi0/6
Gi0/0
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)。
系统首页
接口信息
动态IP(DHCP): 192.168.10.2
WAND LAN2-LAN7

网络模式

快速配置只支持网关模式

> 接口配置

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

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

内网口:	Gi0/0	Gi0/1	Gi0/2				
LAN0(Gi0/0):		192.168.1.1	-	255.255.255.0]	

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

Gi0/3 Gi0/4 G 外网口: 篇	3i0/5
WAN1(Gi0/4) :	动态IP(DHCP) T
WAN0(Gi0/5): 接囗IP:	静态IP地址 ▼ 10.10.10.100 - 255.255.255.0 - 10.10.10.1

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

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

WAN0(Gi0/5):	PPPoE(ADSL拨号) ▼		获取账号	
账号信息:	用户名	-	密码	□ 显示密码

如果您的上网方式选择"动态 IP(DHCP)",则不需要其他额外配置。

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

		下一步		
配置完以上选项后您只需要点击				按钮就可以完成配置,开始管理网络运行状况了!

1.3.2.2 全网智能快速配置

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

Rufe 税捷 NBR3000D-E 全网智能配置向导 Ð 退出 已上电 未上电 已选中 Gi0/6 Gi0/7 外网口: 💼 WAN1 WANO 动态IP(DHCP) WAN0(Gi0/7): ۷ Gi0/0 Gi0/1 Gi0/2 内网口: LAN1 LAN2 LAN3 LAN4 LAN5 LANO LAN0(Gi0/0): 192.168.1.1 255.255.255.0 -连通网络 ©2000-2018 锐捷网络 | 在线客服 | 客服:4001 000 078

Ruffee 税捷 NBR3000D-E 全网智能配置向导				日 退出
GI06 GI07 外网口: WANOCGIC MPI: GIO MPI: MI: MI: </td <td>EL®</td> <td>未上电</td> <td>Eže</td> <td></td>	EL®	未上电	Eže	
LAN0(Gi0/U): 192.168.1.1 - 255.255.0 连通网络 ©2000-2018 锐捷网络 在线客服 客服:4001 000 078				



1.3.3 设备自检

点击设备自检

当前场景:中小企业 💡	□ 快速配置 ■ Hi,admin ∨
	♀ 设备自检
	出 软件版本下载

nsl	192.168.23.197	显示:		×
۲.	确定要进行设备自检?	,		
			确定	取消
ב ת	1000 12 <u>00</u> 000	hileshil 🖂	CALTICALM	10 M
1	192.168.1.0/0.0. 0.255		禁止	ip



正常状态,如下图,增加有帮助和反馈的统计





上不了网的情况:

── 设备自检	×
✓ 设备自检已完成 共发现 1 个问题,请根据提示进行修复!	重新检测
0 网口状态配置	的加加。 1、请检查内网口是否有接线,线路
1. 所有内网囗均未上电	是否有接错,网线是否有松动可能导致无法上网 修复建议 ? 去修复
	首

点击去修复,浏览器新窗口打开页面

RL	jjīe│睿易	当前场景:中小企业 💡	C 快速配置
• <mark>()</mark> 前	系统首页	系统首页	
~	接口连接状态	常用功能(中小企业)	
流控			
① _{安全}		流控 行为策略 VPN 本地服务器 接口信息	设备概况
0		▲:已上电 ▲:未上电	CPU: 6.1% 内存: 23.5%
♪ 用户		LANO LAN3/WAN2 LAN4/WAN1 WAN0 Ag1	在线用户数: 0 设备时间: 2018-8-30 14:31:57
Ø		「「「「」」」「「」」」」「「」」」」「「」」」「「」」」「「」」」」「「」」」」	NBR1700G-E NBR_RGOS 11.9(1)B29
网络		流量走势图	и н ящ
() 无线		线路: 整机 ▼ 时间: 1小时 整机近1	小时内的下行流量峰值为 0.00Mbps
\odot		整机流量走势图 下行流量▼	
展开更多		Louindps	
		0.80Mbps	
		0.60Mbps	
		0.40Mbps	
		0.20Mbps	
点我加速		0.00Mbps	14-20 14-25 14-20
		13.35 13.40 13.45 13.50 13.55 14.05 14.05 14.15	14:20
87			▲ 告警 (0)
		设备型号: NBR1700G-E WEB版本: 2018.8.20.10 详细 @2000-2018 税建网络	A 客服电话:4001 000 078 常见参数查询

1.3.4 Web 管理主界面说明

WEB 管理平台主页面下图所示:

RL	「JIE 睿易	@WEB NBR管理	员:admin 补	丁版本:详细 补丁	「日志 标题格	ŧ.	快捷方式	R 快速配置/线路支更	🗏 实施一本通	占 软件版本下载	小告誓	◎ 人工客服	日週出
合颜	版图编校	智能流控	策略调整	学校调整	应用调整	VPN照控	三级菜单						
• 🗠	1242 0 16	说明:一使开启制	NERISAUCTOR	豊,可以 _失 現帯党派出	的时候,优先保证的	9%(原乐曲模板)或者(り公(の公乗機板), 其次保证阿切	1、然后再保证疫频等应用,让3	包网络无忧。				
協控	实时审计记录	注意:清神乐下言	國國法國帝國領導	EM.									
(N) 加速	行为策略	开	启流控: ON]									
(1) 安全	对象定义	关联应	用模板: の公明	純植板 *									
の節			接□: □G0	/4 😰 Gi0/5									
() () ()		e e	50/5 毛路带宽:下行	10	M	bps 上行 10	M	lbps					
? 斌			9	は存設者			Ŧ	操作区					
()) 高級													

1.3.4.1 标题区

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

当前场景:中小企业 😮 🛛 🕞 快速配置 🛛 💳 Hi,admin 🗸

> 客服

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

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

と 退出

退出:当您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。

1.3.4.2 菜单导航区

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

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



1.3.4.3 主操作区

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

1.3.4.4 状态区

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

右下角增加闪电兔图标,可以拖拽,可以点击咨询

F1 700





1.3.4.5 导航栏告警		
当有系统告警信息时,区域右上角会出现	⚠ 告警 (1)	按钮,没有告警信息时则无提示信息。括号内的数字表示当前
有哪几种告警。出现告警信息时 , 点击	⚠ 告警 (1)	后会有系统告警弹窗出现, 弹窗内只显示有告警的模块:
防攻击告警 提示: 非法网段过滤未配置 请到cli下进行配置 防新建连接攻击未配置! 新建会话数		

- 1. 流量攻击告警:
- (1) 什么时候会出现告警提示?

当设备正在被攻击或曾经被攻击但是您未发觉或查看的攻击。

(2) 如何解决出现告警?

您可以在防攻击页面开启防流量攻击选项,如下图

合颜	本地防攻击	本地防攻击							
k	接口访问控制	防ARP流量攻击: 🛛 开启防ARP流量攻击 (设备每秒处理的ARP报文不超过10个,多余ARP报文将被过滤掉)							
流控	ARP表项	防ARP欺骗: G防主机对整网ARP扫描							
不 加速	ACL访问列表	查看ARP嫌疑列表: 【ARP欺骗嫌疑列表】							
• 🔃	连接数限制	开启可信ARP: Gi0/0 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7 Ag1							
安全		防内网上行攻击: 【默认全局配置】 【对单个ip进行配置】 🛛 🕄							
と ^肺		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】 💡							
R		防流量攻击: 🔲 开启防流量攻击							
网络		攻击流日志: 【当前的攻击日志】 【历史的攻击日志】							
((元线		禁止web登录: 🗏 禁止内网登录设备web系统 🛛 禁止外网登录设备web系统							
~~~		禁止ping: 🗌 禁止内网ping设备 🛛 禁止外网ping设备							
{ <u>(</u> )} 高级		禁止ssh telnet: 🗏 禁止内网ssh telnet 🛛 禁止外网ssh telnet							
		禁止snmp管理: 🗏 禁止内网snmp管理 🛛 禁止外网snmp管理							
		web访问端口: 80 (80,1025-65535)默认为80							
		保存设置恢复默认设置							

(3) 点击 【历史的攻击日志】 可查看历史流量攻击信息。

2. 接口带宽不足告警:

- (1) 什么时候会出现告警提示?
- 当设备接口带宽不足或曾经接口带宽不足但是您未发觉或查看的告警。
- (2) 如何解决出现告警?
- 告警信息会有对应的解决措施方案。
- (3) 点击'带宽不足历史日志'可查看历史接口带宽不足信息。
- 3. 特征库审计告警:

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

全部特征库告警日志

可查看所有特征库版本告警信息。

4. 硬盘告警:

硬盘有出现坏道,硬盘缺失,硬盘接触不良时出现告警。

5. 配置文件告警:

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

6. 默认路由告警:

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

7. 系统密码告警:

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

- 1.3.5 首页
- 1.3.5.1 系统首页

登录 WEB 管理界面后自动会转到系统首页,您也可以通过菜单区点击 页。



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

# 1.3.5.1.1 常用功能

在系统首页页面上方,显示了常用功能,点击按钮可以进入对应菜单:

常用功能(中小企业)



# 1.3.5.1.2 接口信息

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



# 1.3.5.1.3 设备概况

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



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

设备时间: ▲ 2013-1-4 11:46:30
当设备时间和管理PC的时间相差1小时时
EG1000C RGOS 10.3(4b8), Release(53566)
将出现这个警告图标,点击进入配置。

# 1.3.5.1.4 带宽状态

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

• 最近一小时流量走势图:



1. 如上图所示,黄色曲线显示的是"流控抑制前的流量"走势,蓝色曲线显示的是受流控抑制后实际通过的流量走势。

- 2. 您可以更改接口 整机 ▼ 、及 下行流量 ▼ 来查看各接口的本日流量走势;
- 3. 鼠标移上曲线点可以查看所在位置的"流控抑制前流量"和"通过的流量"。
- 4. 点击 ^{■ 流控抑制前流量} 可以隐藏"流控抑制前流量"走势曲线,点击: 通过的流量 可以隐藏通过的流量走向 曲线。
- 本日应用流量 TOP10

当前	1110分钟的流	程TOP10	₿局新 详细>>
排行	应用程序	流量 Kb ▼	应用类型
1	🧭 普通网页浏览	<b>199.3Kb</b> / <b>15.9Kb</b>	普通/其他类
2	DNS	<b>↓21.9Kb</b> / ↑8.9Kb	关键/保证类
3	TCP交互应用	<b>↓17.0Kb</b> / ↑17.4Kb	普通/其他类
4	🗖 正在识别的应用	<b>↓0.6Kb</b> / ↑1.1Kb	关键/保证类
5	NETBIOS-DGM	<b>↓0.0Kb</b> / ↑1.5Kb	普通/其他类
6	NETBIOS-NS	<b>↓0.0Kb</b> / ↑3.0Kb	普通/其他类

- 1. 如上图所示, 表格显示了流量 TOP10 的用户
- 2. 通过

下行

▼」 可根据不同上下行流量查看最近十分钟流量 TOP10;

#### • 本日用户会话数 TOP10

用户	用户会话数 TOP10 整机 ▼							
排行	用户	IP地址	会话数					
1	/172.18.132.20	172.18.132.20	1	Â				
2	/172.18.132.8	172.18.132.8	1					
3	/172.18.132.17	172.18.132.17	1					
4	/192.168.1.3	192.168.1.3	1					
5	/172.18.132.60	172.18.132.60	1					
6	/172.18.132.19	172.18.132.19	1	-				

#### 1. 如上图所示, 表格显示了流量 TOP10 的用户

2. 通过 **整机 ▼** 可根据不同端□

」 可根据不同端口查看用户会话数 TOP10;

# 1.3.5.1.5 主程序推送

📃 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

#### 1.3.5.2 接口连接状态

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

接口连接状态								
<b>说明:</b> 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	光电口	双工	速率	DNS	状态		
Gi0/0	192.168.1.1	电口	自协商	自协商		未连接		
Gi0/1	100.111.111.1	电口	自协商	自协商		未连接		
Gi0/2		电口	自协商	自协商		未连接		
Gi0/3		电口	自协商	自协商		未连接		
Gi0/4		电口	自协商	自协商		未连接		
Gi0/5	192.168.23.248	电口	双工	100M		连接		
显示: 10 ▼ 条 共6条	显示 10 ▼ 条共6条							

1.3.5.3 上网配置

请参考"1.3.2 快速配置"章节。

1.3.6 流控

1.3.6.1 流量监控

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

# 1.3.6.1.1 实时流量



用户				当前共0个用户在线
	在线用户数 0			全活数 0
Шr	用户组			
排行	名称 本地用户 •	查看明细	通过的流星 ■ 下行 ■上行	流控抑制流量
			无记录信息	
显示 10 • 条				[4 首页 4 上一页 1 下一页 ▶ 来页 ) 1 <b>流</b> 症



#### 1. 实时流量页面上方显示实时流量导航菜单如下:

实时流量	VPN流量 线路质量监控			?帮助					
每30秒刷新一次	▼	线路    应用	用户						
线路选择: 整机 ▼ 时间范围: 当前									
线路	收到的流量 ■ 下行 ■ 上行 ■ 告警	流控抑制流量	流控抑制流量						
整机	1.49Kbps 0.91Kbps	10.00% t0.00%	10.00Kbps 10.00Kbps						
Gi0/6	1.49Kbps 0.91Kbps	↓0.01% ↑0.00%	10.00Kbps 10.00Kbps						







(4)	通过	时间	]范围:	当前	1小时	今天	可以选	泽查看当前的	的流量信息	、, 或者查看聶	最近 1 个小时
内耳	或今天的	P整体演	流量走势。	当前	表示正在查	查看当前的	沉量信息	l.			
(5)	点击	Qi	高级查询	将弹出以	以下窗口,可以	以查看流量	量、在线用	沪数、会话	数等明细	:	
				查询					×		
			流重	<u>1</u>	在线用户数	47	会话数				
	时间类型: ● 当前 ◎ 日表 ◎ 周表 ◎ 月表										
			í	名称: 应用	]						
			选择	宴口: 整机	ι •						
								确定查询			

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,点击名称后面的输入框,选择查看类型,点击右边输入框可以在弹出的应用树或用户树中选择需要查询的应用范围或用户范围:


报	表直询结果				Q 高级直询
	查询日期:当前				
	查询应用:所有应用				
	查询线路 : <mark>整机</mark>				
流量	充计				
排行	名称	查看明细	通过的流量 ■ 下行 ■ 上行	流控抑	制流量
1	WEB应用/普通网页浏览	明细	2.79KB 0.14KB	↓0.00KB	↑0.00KB
2	即时通讯软件/QQ-登录 聊天	明细	12.11KB 1.86KB	↓0.00KB	10.00KB
3	即时通讯软件/BQQ	明细	0.33KB	10.00KB	10.00KB
4	网络管理协议/DNS	明细	0.16KB	10.00KB	10.00KB
5	电子邮件协议/MAPI	明细	0.15KB	10.00KB	10.00KB
6	IP协议组/正在识别的应用	明细	0.09KB 0.22KB	10.00KB	↑0.00KB
7	互联网文件传输/SVN	明细	0.00KB	↓0.00KB	↑0.00KB
8	普通网页浏览明细/IT类	明细	0.00KB	10.00KB	10.00KB
9	普通网页浏览明细/搜索引擎	明细	0.00KB 0.00KB	↓0.00KB	↑0.00KB
10	网上支付 网上银行_MOBILE/支付宝 _IPad IPhone	明细	0.00KB	↓0.00KB	†0.00KB
			▼1000000000000000000000000000000000000	1 下一页 ▶ 末页	▶ 1 确定

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

📃 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 ▼		
			确定直询
点击	, 将弹出查询结果	如下:	

报表查询结果		Q 高级直询
直询日期:当前		
查询类型:用户数		
查询线路: <mark>整机</mark>		
用户数统计		
	在线用户数	
	1	

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

=	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
点击	确定直询 ,将弹出查询结果如下:	
报表	查询结果	
	查询日期:当 <del>前</del>	
	直间类型:会话数	
	查询线路: <mark>整机</mark>	
会话数	统计	
		会话数
		17

### • 接口流量分析

该功能是把带宽的使用按不同的线路(接口)来统计,您可以对线路(接口)的流量进行控制和分析,以便提高流量的使用



### 概况

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

每30秒刷新一次 🔻		线	路 应用 用户			
线路选择: 整机 ▼ 时间范围: 当前 1小时 今天 Q 高级营						
线路	通过的流量 🔳 下行 🖩 上行 🛢 告答	带宽使用率	流控抑制流量			
整机	■ 10.57Kbps 1.05Kbps	<b>↓0.01%</b> †0.00%	↓0.00Kbps			
Gi0/6	■ 10.57Kbps 1.05Kbps	<b>↓0.01%</b> ↑0.00%	<b>↓0.00Kbps</b> ↑0.00Kbps			

当前流量信息:上图所示即线路当前的流量信息,通过上图的流量信息,也可以发现当前流量是否正常(有无出现告警),如

果流量过高会出现黄色告警 - 告警, 来帮助您快速定位带宽问题。

问题:什么时候会出现告警提示?

总流量达到了线路带宽 (贵机构向电信等运营商申购的带宽)的 95%以上时。

问题:如何解决出现黄色告警?

- 2.

应用

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

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

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

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

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

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

应用组

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

在表	格左上方的导航菜单中选中		——————————————————————————————————————	Z用组的流量信息:
	应用 应用组			
排行	名称	查看明细	通过的流量 ■ 下行 ■ 上行	流控抑制流量
1	HTTP协议	明细	0.96Kbps 0.23Kbps	10.00Kbps
2	即时通讯软件	明细	0.19Kbps 0.00Kbps	10.00Kbps
3	IP协议组	明细	0.13Kbps 0.27Kbps	↓0.00Kbps
4	电子邮件协议	明细	0.02Kbps 0.02Kbps	10.00Kbps 10.00Kbps
5	P2P应用软件	明细	0.00Kbps 0.00Kbps	10.00Kbps
6	网络管理协议	明细	0.00Kbps 0.00Kbps	10.00Kbps
7	远程访问协议	明细	0.00Kbps 0.00Kbps	10.00Kbps
显示	10 •		「首の	〔《上一页 1 下一页》末页》 1 确定



1

确定

<u>⊾</u>	如用组: ITTP协议							
当前	当前的流量(Kbps)							
	线路		下行	上行	流控抑制流量		操作	
	整机	1	345.40	15.84	↓0.00Kbps	lbps ß	目断流量	
	用户应用							
排	· 石称 本地用户 ▼	IP地址		通过的流量 ■ 下行■ 」	LŦ	流控抑制流量	操作	
1	/172.18.18.238	172.18.18.238	∎ 15.84Kbps		845.40Kbps	↓0.00Kbps ↑0.0 0Kbps	明细	

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。

【●首页 ●上一页 1 下一页 ▶ 末页 ▶

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

3) 用户

显示: 10 🔻

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

用户										
在线用户数	会话数									
1	0						~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		0	
0										
14:40	14:45	14:50	14:55	15:00	15:05	15:10	15:15	15:20	15:25	15:30
	分类			峰值	直在线数			平均在线器	汝	
	在线用户数				1			1		
	会话数				44			22		
用户用户	□组									
排行 名称本	地用户 ▼	1	P地址		通过的	的流量 🔳 下行 🔳	上行		流控抑制流量	
1 /192.168.124.5		192	168.124.5	1.	56MB		18.79MB	19	7.76KB 10.00KB	
							◀首页 ◀上一页	<b>1</b> 下一页	▶ 末页 ▶ 1	确定

i	本地用户 ▼	
	本地用户	
海洋下拉框	外部用户	可以进场委委大地田户武计证田户的这是信息
通じいが低		り以匹拜旦自쑤地用厂以以业用厂的沉里后忌。

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

用的流量信息:

点击

○用户流量明细 - Google Chrome						
172.18.124.54/flow_pi/flow_user_detail.htm						
名称 192.168.124.5	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	6.37	6.12	↓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	WEB应用/普通网页浏览	14.44Kbps 13.94Kbps	↓0.00Kbps ↑0.00Kbps
2	普通网页浏览明细/搜索引擎	0.84Kbps 11.16Kbps	↓0.00Kbps ↑0.00Kbps
3	网络硬盘/有道笔记 有道笔记 _Mobile	0.59Kbps 0.45Kbps	↓ <b>0.00Kbps</b> ↑0.00Kbps
4	网络管理协议/DNS	0.27Kbps 0.12Kbps	↓0.00Kbps ↑0.00Kbps
5	即时通讯软件/QQ-登录 聊天	0.16Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps
6	电子邮件协议/MAPI	0.03Kbps 0.03Kbps	↓0.00Kbps ↑0.00Kbps
7	IP协议组/正在识别的应用	0.03Kbps 0.43Kbps	↓0.00Kbps ↑0.00Kbps
8	即时通讯软件/BQQ	0.00Kpps 0.00Kpps	↓0.00Kbps ↑0.00Kbps
		<首页 < <u>↓</u> —页 1 つ	下—页 ▶ 末页 ▶ 1 确定

点击 阻断流量

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

### • 应用流量分析

该功能是把带宽的使用按不同的应用软件来统计,您可以对应用的流量进行控制和分析,以便提高流量的使用价值。点击实

时流量页面导航菜单栏中的

显示如下:

应用

实时流量	VPN流量线路质量监	封空		(2) 報日
每30秒周新一次	•			线路 应用 用户
线路选择: 3	割し ・ 町间范園: 当前			Q 高级直询
应用类型	通过的流量	1 ■ 下行 ■ 上行	帶宽使用率	流控抑制流量
关键/保证类	1.48Kbps 0.86Kbps		10.00% 10.00%	10.00Kbps 10.00Kbps
抑制类	0.00Kbps 0.00Kbps		10.00% 10.00%	10.00Kbps 10.00Kbps
关键/保证类				当前共3个应用正在使用
应用	用户			
脚行	名称	查看明细	通过的流量 = 下行 = 上行	流控抑制流量
1 网络游戏软	《件/完美世界	明细 1.29Kbps 0.78Kbps		10.00Kbps 10.00Kbps
2 网络管理协	NX/DNS	明細 8.68885		10.00Kbps 10.00Kbps
3 IP协议组/I	正在识别的应用	明細 8:888855		10.00Kbps 10.00Kbps
显示 10 •				N 首页 《上一页 】 下一页 》 末页 N 1 改定
普通/其他类				当前共0个应用正在使用
应用	用户			
肺行	名称	查看明细	通过的流量 = 下行 = 上行	流控抑制流量
显示 10 •				▶(首页《上一页 1 下一页》来页 № 1 0±
抑制类				当前共1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	流控抑制流量
1 软件更新/0	网维大师	明細 0.00Kbps		10.00Kbps 10.00Kbps
显示:10 •				1音页 《上一页 1 下一页 》 末页 川 1 機定

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

每30秒刷新一次 🔻		线路	应用 用户		
総路选择: 翌初 ● 时间范围: 当前					
应用类型	通过的流星 🔳 下行 🖩 上行	带宽使用率	流控抑制流量		
关键/保证类	1.37Kbps 0.80Kbps	10.00% 10.00%	10.00	Kbps †0.00Kbps	

1) 当前流量信息:

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

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

关键	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	流控抑制流量				
1	即时通讯软件/BQQ	明细	5.48Kbps 2.37Kbps	↓0.00Kbps				
2	WEB应用/普通网页浏览	明细	2.58Kbps 2.08Kbps	<b>↓0.00Kbps</b> ↑0.00Kbps				
3	即时通讯软件/QQ-登录 聊天	明细	0.50Kbps 0.15Kbps	↓0.00Kbps				
4	普通网页浏览明细/搜索引擎	明细	0.17Kbps 0.23Kbps	↓ <b>0.00Kbps</b> ↑0.00Kbps				
5	IP协议组/正在识别的应用	明细	0.08Kbps 0.64Kbps	10.00Kbps				
6	网络管理协议/DNS	明细	0.08Kbps 0.04Kbps	10.00Kbps				
7	电子邮件协议/MAPI	明细	0.05Kbps 0.05Kbps	<b>↓0.00Kbps</b> ↑0.00Kbps				
8	互联网文件传输/HTTPS	明细	0.00Kbps 0.00Kbps	↓ <b>0.00Kbps</b> ↑0.00Kbps				
9	普通网页浏览明细/软件升级	明细	0.00Kbps 0.00Kbps	10.00Kbps 10.00Kbps				
10	ICMP-DETAIL/Echo-request	明细	0.00Kbps 0.00Kbps	↓0.00Kbps				
			▲ 首页 《 上一页	1 下─页 ▶ 末页 ▶ 1 确定				

点击明细

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



点击明细

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

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

普通	i/其他类			当前共2个应用正在使用
	立用 用户			
排行	名称	查看明细	通过的流量 📕 下行 🛯 上行	流控抑制流量
1	软件更新/金山毒霸-UP[	OATE 明细	0.00Kbps 0.00Kbps	↓ <b>0.00Kbps</b> ↑0.00Kbps
2	软件更新/搜狗-UPDATI	明细	0.00Kbps 0.00Kbps	↓0.00Kbps
			【★首页 《上一页	1 下─页 ▶ 末页 ▶ 1 确定

点击明细将	· 所述 · 和 · 和 · 和 · 和 · 和 · 和 · 和 · 和 · 和 ·	详见	"2.5.1.1	接口流量分析"	章节中的应用流量明细窗口的分析。
-------	--------------------------------------------	----	----------	---------	------------------

	普通/其他类		
上图显示的是普通/其他类应用的流量信息 , 点击	应用	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	当前共1个应用正在使用				
	应用 用户				
排行	名称 本地用户 ▼	IP地址	查看明细	通过的流量  ■ 下行  ■ 上行	流控抑制流量
1	/192.168.124.5	192.168.124.5	明细	3.52Kbps 0.70Kbps	<b>↓0.00Kbps</b> ↑0.00Kbps
				《首页 《上一页 <b>1</b> 下一页	▶ 末页 ▶ 1 确定

```
点击明细
```

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

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

抑制类				当前共0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	流控抑制流量
			<首页 <上─页	1 下一页 ▶ 末页 ▶ 1 确定



	抑制类		
上图显示的是抑制类应用的流量信息,点击 应用的用户资量信息:	应用	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0个应用正在使用
应用 用户				
排行 名称 本地用户 ▼	IP地址 重	查看明细 通过的	流量 🔳 下行 🔳 上行	流控抑制流量
			▶★首页 ◆上一页 <b>1</b> 下一页	▶ 末页 ▶ 1 确定

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

### 用户流量分析

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

流量	页面导航菜单	栏中的	用户	显示如下:						
每30	砂刷新──次 ▼							线路	应用	用户
线	线路选择: 整机 ▼ 时间范围: 当前 Q 高級查询									
	在线用户数 会话数									
			3				1			
	用户流量排行	用户组流量排	附 VIP用户流量	排行 用户领	会话数排行					
排行	名称 本地界	∄户 ▼	IP地址	查看明细		通过的流量	■ 下行 ■ 上行		流控抑制	訓流量
1	/172.18.132.48		172.18.132.48	明细	. <mark>05Kbps</mark> .70Kbps				↓0.00Kbps	†0.00Kbps
2	/172.18.135.1		172.18.135.1	明细	.12Kbps .00Kbps				↓0.00Kbps	†0.00Kbps
3	/172.18.132.40		172.18.132.40	明细	.00Kbps .00Kbps				↓0.00Kbps	†0.00Kbps
显示	10 🔻						▶★ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	页 1 下	一页▶ 末页 ▶	1 确定

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。

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

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

## 1.3.6.1.2 VPN 流量

实时	<b>防史流量报表</b>	VPN流量	历史接口	流量 当时间范围为1小时或者今天时,支持导出报表	? 帮助
线距	各选择: Gi0/6 ∨ 时	<b>间范围:</b> 当前	1小时 4	天 每30秒刷新一次 🗸	Q 高级查询
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	0.02Kbps 0.00Kbps	10.00Kbps 10.00Kbps
3	/192.168.1.21	192.168.1.21	明细	0.00Kbps 0.00Kbps	10.00Kbps 10.00Kbps
4	/192.168.1.25	192.168.1.25	明细	0.02Kbps 0.00Kbps	↓0.00Kbps
				《首页 《上一页 1 下一页》 末辺	页 ▶ 1 确定

- 1. 通过该页面可以查看某条线路上通过 VPN 拨号访问网络的用户明细及各 VPN 用户的流量信息。
- 2. 通过 Gi0/1_TO_CNII ▼ 可以选择查看某条线路的 VPN 流量使用情况。
- 3. 通过^{每30秒刷新一次 ▼}可以选择每隔 10 秒、30 秒、1 分钟刷新一次设备的当前 VPN 流量信息,也可以选择手动刷 新设备的当前 VPN 流量信息。
- 4. 通过 Q 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:

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
輸入名称或 IP ,选择好接口后 ,点击 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	10.00Kbps 10.00Kbps
2	/192.168.10.2	192.168.10.2	明细	172.08Kbps 359.55Kbps	10.00Kbps 10.00Kbps
3	/192.168.1.21	192.168.1.21	明细	0.00Kbps 0.00Kbps	10.00Kbps 10.00Kbps
4	/192.168.1.25	192.168.1.25	明细	0.02Kbps 0.00Kbps	↓0.00Kbps
				【●首页 ●上一页 1 下一页 ▶ 末辺	页 ▶ 1 确定

## 1.3.6.1.3 历史接口流量



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

### 1.3.6.2 流控策略

## 1.3.6.2.1 智能流控

智能流控设置页面如下图所示:

	开启流控: ON	]			
关职	送应用模板: 娱乐线	€模板 ▼			
	接口: 🗌 Gi0/	2 🔲 Gi0/3 🖉 Gi0/4	4 🕑 Gi0/5 🔲 Gi0/6 🕑	Gi0/7	
	Gi0/4				
	(18/4) 线路带宽:下行 1	100	Mbp	s 上行 100	Mbps
	Gi0/5				
	线路带宽:下行 1	1	Mbp	5 上行 1000	Mbps
	Gi0/7				
	线路带宽:下行 1	10	Mbp	s 上行 10	Mbps

### 添加了关联应用模块。

智能流控	策略调整	参数调整	应用调整	VPN流控		
<b>说明:</b> 优先保证 <b>注意:</b> 请确保线	游戏,其次保证网页 路带宽填写正确。	, 最后保证视频。				
Ŧ	T启流控: ON	] 🛶	_ 流控开关			
	接口: ✔ Gi0/	5 🔲 Di1 📄 Di2 🔤 [	Di3 🔲 Di4(Gi0/7) 🗌	] Di5(Gi0/6) 🔶	—— 选择接口	
	<mark>Gi0/5</mark> 线路带宽:下行 1	0	M	ops 上行 10		Mbps
	保	存设置				

## 1.3.6.2.2 策略调整

智能	流控 策略	周整 参数	数调整	应用调整	VPN流控						
说明:	流量控制(Flow Con	trol),下面简称流热	空,是一种区分不	司用户、网段、应用	的流量,并进行有图	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:		日本に見ばいる加東部			49.000 · Did -		74 台北十空午11			10 /6-1 6	
<b>T</b> /9		切尔主机萨风速束属	宿 入前床四中	東南 迈岸按口	dgamer. Di⊓ ▼		-90BE19711			操作灯边	⊻的東略
	策略名称	用白IP	应用组	外网IP组	时间	限速类型	<b>市</b> 來 限制	兀配顺皮	启田	开态	会団
	Store may.	100 C	ALL FOR ALL	ALL DO NOT AND		PRODUCT STATE	201-4-PK(#3	E-HOWK/S	10110	1/1/24	「「「」」「「」」「」」「「」」「」」「」」「」」「」」「」」「」」」
	例外主机限速策 略-1	IP-36.3.3.3	所有应用	所有外网IP	所有时间	共享带宽	上行 100Kbps 下行 100Kbps			不生效 ?	日理 复制 编辑 删除
	例外主机限速策 略-1 例外主机限速策 略-2	IP-36.3.3.3 IP-9.3.3.3	所有应用	所有外网IP	所有时间	共享带宽 共享带宽	上行 100Kbps 下行 100Kbps 上行 100Kbps 下行 100Kbps		e e	不生效 ? 不生效 ?	复制 编辑 删除           复制 编辑 删除           复制 编辑 删除

### • 新建策略

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

点击	十新建策略将弹出	出"添加策略"的导航窗口
$\equiv$	添加策略	×
	策略名称:	*
	用户IP:	*
	选择应用组:	普通/其他 ▼ 【自定义应用分组】
	流量限制:	● 独立控制 下行: Kbps * 上行: Kbps *
		<ul> <li>○ 共享带宽</li> <li>○ 不限速</li> </ul>
	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】
]	启用该策略的外网口:	Gi0/7     Gi0/7
		完成配置 取消

- 1. 策略名称:在"策略名称"输入框中输入能够标识该规则名称的意图或用途规则名称。
- 2. 选择应用组:下拉框中选择已有的应用,当不满足需求时可以点击 进行配置。

<ul><li>     荒控     新路(     </li></ul>	,是- 的操作 <b>≧ 添加策略</b>	· · · · · · · · · · · · · · · · · · ·	·、网	络游戏等。	
臣略	策略名称	•			
	<b>ビ</b> 新通/! 用户IP	*	状态	这 文	
		: 普通/其他 ▼ 【自定义应用分组】	生交	文	
	<ul> <li></li></ul>	ne ////////////////////////////////////			×
	应用分组名称	选择应用	ŧ	<b>雪理</b>	
	关键/保证类	DNS,QQ应用,HTTP游戏,HTTPS,网络游戏软件,ICMP-DETAIL,IP网络电话	勻	扁辑	
	网页类	HTTP协议,游戏_MOBILE,普通网页浏览明细,WEB_MOBILE	当	扁辑	
	在线视频类	HTTP视频,视频 影音_MOBILE	当	扁辑	
	影视娱乐类	视频流媒体软件	当	扁辑	
	常用下载类	HTTP下载,FTP,快牙,TFTP,NNTP,IXIA,SVN,SMB,下载工具_MOBILE,网络硬盘,网盘_ MOBILE	絹	扁辑	
	P2p下载类	P2P应用软件,软件更新	组	扁辑	
	应用更新类	游戏更新,网吧游戏服务器	勻	扁辑	
	常用上传类	HTTP上传	朝	扁辑	
9.3	抑制类	互联网文件传输	朝	扁辑	

- 3. 流量限制:独立控制(保证网速、最大网速为策略所限制的某个具体用户在当前接口下使用某个具体应用的最低和最高网速,同时提供每个使用该通道的用户最低和最高网速),共享带宽,不限速。
- 4. 外网 IP 组:点击 进行选择 IP 组。
- 5. 生效时间:下拉框中可以选择已有的时间,当不满足需求时,点击_______自行配置
- 查看策略

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

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 Con	trol),下面简称流	空,是一种区分不同	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	: 漆加服务器策略只想	是供便逮的添加策略	8的操作,万便网管	診添加服务器策略。									
1.37			A CONTRACTOR OF				-1 AV 12 Pm				S 11 11 11		
- <b>-</b> -/9	▲加東略 十 添加19	列外王机限速策	略 X 删除选中	中策略 选择接口的	践路: Di1 ▼		切能按钮			操作对应	应的策略 		
	▲加東略 十 ※加竹 策略名称	则外主机限速策 用户IP	略 X 删除选中 <b>应用组</b>	小策略 选择接口的	践踏: Di1 ▼ 时间	限速类型	山前 27 新社 連率限制	匹配顺序	启用	操作对近 <b>状态</b>	应的策略	管理	
	▲加東略 十/添加性 策略名称 例外主机限速策 略-1	列外主机限速策 用户IP IP-36.3.3.3	略 X 删除选中 应用组 所有应用	*策略 选择接口的 <b>外网IP组</b> 所有外网IP	66路: Di1 ▼ 时间 所有时间	<b>限速类型</b> 共享带宽	<u>切能按钮</u> 連率限制 上行 100Kbps 下行 100Kbps	匹配顺序	启用	操作对近 状态 不生效 <b>②</b>	应的策略 	管理	除
	例外主机限速策 略-1 例外主机限速策 略-2	明外王初時2里東市 用户IP IP-36.3.3.3 IP-9.3.3.3	略 X 删除选中 应用组 所有应用 所有应用	•策略 选择接口 <b>外网IP组</b> 所有外网IP 所有外网IP	(其語: Di1 ▼ 时间 所有时间 所有时间 所有时间	<b>限速类型</b> 共享带宽 共享带宽	<b>功能授祖</b> 速率限制 上行 100Kbps 下行 100Kbps 上行 100Kbps     下行 100Kbps     下行 100Kbps	匹配顺序 	启用 ✔	操作对! <b>状态</b> 不生效 ^② 不生效 ^③	应的策略           复制           复制	<ul> <li>管理</li> <li>编辑 (新)</li> <li>编辑 (新)</li> </ul>	除除

- 1. 点击"应用组"栏中的 🧮 按钮,可以查看某个应用组包含的应用信息。
- 2. 开启/关闭:支持针对全部规则或具体单条规则的开启和关闭。该功能影响规则的"当前状态"为生效或禁用。
- 3. 状态:包括"生效"、"不生效"、"禁用"三种状态,"生效"、"禁用"状态受规则的开启与否控制,若当前时间不在"生效时间"的时候,规则的当前状态显示为"不生效"状态。
- 匹配顺序:流控策略适应"后配先生效"原则,本列表按照第一条规则置顶的排序方式进行排列,可以直接点击¹
   按钮对现有策略的优先级进行调整;
- 6. 点击 可以删除策略。
- 复制策略



## 1.3.6.2.3 参数调整

可根据具体情况进行各个接口参数调整。

智能流控	策略调整	参数调整	应用调整	VPN流控								
<b>提示:</b> 以下速率的	单位统一为Kbps。优势	先级值越小,优	洗级越高									
 01010	当前利用率:0%	% 紧张阈值	直:0% 范围(1%	~99%)								
GIU/6	预留带宽(范围	:1%~80%)	) 上行 ( 总带宽10	M):20% T	▽行(总带宽10№	M):15%	修改					
Gi0/5	業型	优先级	速率	上行承诺值	上行最大值	下行承诺值	下行最大值	上行每用户	上行每用户	下行每用户	下行每用户	操作
	~		(下行/上行)	1.13-3-5-64.14		113.3.6444	1.13 467 (144	最小值	最大值	最小值	最大值	2001
	关键/保证类	0	0/0	6,000	10,000	6,000	10,000		5,000		5,000	编辑
	普通/其他类	4	0/0	2,000	10,000	2,000	10,000		3,000		3,000	编辑
	抑制类	7	0/0	1,000	10,000	1,000	9,000		3,000			编辑

## 1.3.6.2.4 应用调整

智能流控	策略调整	参数调整	应用调整	VPN流控		
说明: "普通/	其他类"属于默	认分组,不能操作默认分组	日中的応用			
重置办公应用	模板	重置娱乐应用模板				
应用分组	目名称				选择应用	管理
关键/保	证类	即时通讯软件,IP网络	电话 ,电子邮件协	议 ,DNS,ICMP-D	ETAIL,VPN应用	编辑
网页	类	HTTP协议,普通网页;	刘览明细 ,WEB_M	IOBILE		编辑
在线视	频类	HTTP视频,视频 影音	MOBILE			编辑
影视娱	乐类	视频流媒体软件				编辑
常用下	载类	HTTP下载,下载工具	MOBILE,网络硬	盘,FTP,快牙,TFTF	P,NNTP,IXIA,SVN,SMB,网盘_MOBILE	编辑
P2pT	载类	P2P应用软件,软件更	新			编辑
应用更	新类	游戏更新,网吧游戏服	务器			编辑
常用上	传类	HTTP上传				编辑
抑制	类	WEB应用,网络游戏转	r件,社交_MOBIL	E		编辑
阻断	类	非法DNS				编辑
普通/其	她类	股票软件,互联网文件	:传输 ,网络管理协	议,路由协议,远利	程访问协议,网银,即时通讯_MOBILE,游戏_MOBILE,其他_MOBILE,证券_MOBILE,RFC,IP-RAW,IP协议组	默认组不能编辑
显示: 15 🔻					(首页 《上一页 1 下一页 》末页	▶ 1 确定

# 1.3.6.2.5 VPN 流控

<b>官VPN</b> 流控	: 🗹 Di2 🗆 Di1 🗆	Di3 Di4 Gi0,	/5		
保障VPN	€键应用的流量				
Q					
- 🗀 🗆 所有	「应用				
+ 🗀 🗆	HTTP协议				
+ 🗀 🖌	P网络电话				
+ 🗀 🗆 ş	网络游戏软件				
+ 🗀 🗆 i	见频流媒体软件				
+ 🗀 🗆	P2P应用软件				
+ 🗀 🗆 į	投票软件				
+ 🗋 🖌	即时通讯软件				
+	互联网文件传输				
+ 🗀 🖌 🛛	电子邮件协议				
-	网络管理协议				

### 配置好接口后,可以点击查看编辑按钮

智能流控 策略调整	参数调整	应用调整	VPN流控	
<ul> <li>✓ 保障VPN法控: ●DIT ●DI2 ●GI</li> <li>✓ 保障VPN关键应用的流量</li> </ul>	0/7		WPN关键通道带宽编辑	×
Q 所有应用 HTTP协议		;	选择通道: Di1 ▼ 下载网速:保证 1.4 Mbps,最大 7 Mbps,每IP最大 0 Mbps 上传网速:保证 1.6 Mbps,最大 8 Mbps,每IP最大 0 Mbps	;
+ □ UKEB应用 + □ Ø QQ应用 + □ HTTP网络购物			保存配置	取消
<ul> <li>□ □ FLASH</li> <li>□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □</li></ul>	中心			
+ 🗀 □ 论坛PC + 🗀 🗹 HTTP游戏	/			
VPN关键通道带宽 点击查看/	编辑  (注:	需先开启对应通	i重vpn流控才能对VPN带宽设置)	

## 1.3.6.3 对象定义

对象定义配置页面:

合颜	流量监控	自定义应用分组自动	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		
• 🗠	流控策略	十添加应用分组 十 自定义应	+添加应用分组 + 自定义应用 ♥ 反馈无法识别的应用								
流控	行为审计报表	应用分组名称			选择应	闭		管	理		
<b>(</b> ) 加速	行为策略	关键/保证类	键/保证类 即时通讯软件,IP网络电话,电子邮件协议,普通网页浏览,普通网页浏览明细,DNS,ICMP-DETAIL,安全协议,VPN应用,办公OA,视频会议,HTTPS					安全协编	揖		
Û	对象定义	抑制类	网络游戏软件,初频 影音_MOBIL	3版流媒体软件,P2 E,下载工具_MOB	P应用软件,WEB应用 SILE,社交_MOBILE,即	目,HTTP下载,HTTP上位 网盘_MOBILE,未知网页	专,网络硬盘,HTTP社 5	观频 ,视 编辑	貫		
≫ 安全		阻断类	非法DNS,非法类	美网页,股票软件				编	貫		
と 馿		普通/其他类	HTTP游戏,互联 _MOBILE ,游戏_ 银行_MOBILE ,{	网文件传输,数据属 _MOBILE,WEB_N 微博,RFC,IP-RAV	두 ,网络管理协议 ,路日 10BILE ,其他_MOBII N ,IP协议组	由协议,远程访问协议,韩 LE,网购_MOBILE,证券	次件更新,网银,即时 _MOBILE,网上支付	通讯			
Ø						₹ 省页 ₹	—页 <b>1</b> 下—页	▶ 末页 ▶ 1	确定		

## 1.3.6.3.1 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	外网IP对象	文键字组对象         VLAN对象         IP对象         URL对象         自定		自定义内网用户对象			
+添加应用分组 +目定义应用 ,同反馈无法识别的应用									
应用分组名称		选择应用							
关键/保证类	DNS,QQ应用,H	DNS,QQ应用,HTTP游戏,HTTPS,网络游戏软件,ICMP-DETAIL,IP网络电话							
抑制类	HTTP视频P2P	应用软件 ,互联网文	件传输,下载工具_N	AOBILE,网络硬盘,软件	更新,视频流媒体软体	+		编辑	
阻断类	非同志DNS							编辑	
普通/其他类	HTTP协议,股票 OBILE ,游戏_M 明细 ,WEB应用	HTTP协议,股票软件,即时通讯软件,电子邮件协议,网络管理协议,路由协议,VPN应用,远程访问协议,网银,即时通讯_MOBILE,视频影音_M OBILE,游戏_MOBILE,社交_MOBILE,网盘_MOBILE,WEB_MOBILE,其他_MOBILE,证券_MOBILE,RFC,IP-RAW,IP协议组,普通网页浏览 明细,WEB应用,游戏更新							
显示:10 ▼							□ ▶ 末页 ▶ 1 确定		

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

• 应用分组

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

1. 新增自定义应用分组:

点击 十添加应用分组 按钮可以自定义应用分组:

➡ 添加自定义应用分组	×
应用组名: 已选应用:【添加应用】	
应用名称	操作
<b>应用名称</b> ▼ 首页	操作 1 确定

在"应用组名"输入框中输入应用分组名称,点击【添加应用】按钮:



➡ 添加自定义应用分组	×
应用组名:流量控制 ×	
已选应用:【添加应用】	
应用名称	操作
IP网络电话	删除
即时通讯软件	删除
《首页 《上─页 1 下─页 》末页 ▶ [	1 确定
	保存

点击

按钮可以将某个应用从该应用分组中删除。

点击 保存

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

### +添加应用分组 +自定义应用 ₽反馈无法识别的应用

应用分组名称	选择应用	管理
关键/保证类	即时通讯软件,IP网络电话,电子邮件协议,普通网页浏览,普通网页浏览明细,DNS,ICMP-DETAIL,安全协议,VPN应用,办公OA,视频会议,HTTPS	编辑
抑制类	网络游戏软件,视频流媒体软件,P2P应用软件,WEB应用,HTTP下载,HTTP上传,网络硬盘,HTTP视频,视频影音_MOBILE,下载工具_MOBILE,社交_MOBILE,网盘_MOBILE,未知网页	编辑
阻断类	非法DNS,非法类网页,股票软件	编辑
普通/其他类	HTTP游戏,互联网文件传输,数据库,网络管理协议,路由协议,远程访问协议,软件更新,网银,即时通讯 _MOBILE,游戏_MOBILE,WEB_MOBILE,其他_MOBILE,网购_MOBILE,证券_MOBILE,网上支付 网上 银行_MOBILE,微博,RFC,IP-RAW,IP协议组	编辑
流量控制	即时通讯软件,IP网络电话	编辑删除
		▶ 1 确定

### 2. 编辑应用分组:

点击自定义应用分组主页面表格中的 建铵钮可以重新分配某个应用分组包含的应用:

	CLUZZICHC
── 编辑自定义应用分组	×
应用组名: 流量控制	
已选应用:【添加应用】	
应用名称	操作
股票软件	删除
P2P应用软件	删除
视频流媒体软件	删除
IP网络电话	删除
即时通讯软件	删除
【●首页 ●上一页 1 下一页 ▶ 末页 ▶ [	1 确定
	保存

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

点击【添加应用】按钮将弹出以下窗口:



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

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

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

3. 删除应用分组:

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

#### 自定义应用

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

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

★ 自定义应用 按钮将弹出自定义应用配置窗口:

🥝 创建自定义应用	- Internet Explorer		-				- • ×		
R http://172.18.1	R http://172.18.124.72/object_pi/bw_setobj_appauto.htm								
提示:名称长度	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	≝: TCP ~	规则类型:源	IP+目的IP 、	•					
应用所属分类	第: ● 自定义分类	2 ○ 从已有分类	选择:						
源Ip	o: 輸入ip 🗸			0					
目的Ip	o: 輸入ip 🗸	•		0					
	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		
test	tcp	网络管理协议	所有端口	所有端口	1.2.4.4	20.2.0.47	编辑删除		
				◀首页 ◀.	上一页 1 下	一页▶ 末页 ▶	1 确定		

创建自定义应用对象:输入自定义应用名称、选择协议类型、选择规则类型、应用所属分类(可以自己另外定义应用分类, 也可以基于内建应用分类)、根据选择的规则类型输入源或目的端口、源或目的 IP,点击 添加设置 配置成功。 编辑自定义应用:选择需要修改的应用,点击 编辑 按钮即可修改。 删除自定义应用:选择需要删除的应用,点击 删除 即可。

• 反馈无法识别的应用

如果您发现某个网络应用程序的流量无法被本设备正确识别,导致您无法对该应用进行有效控制,您可以点击 一反馈无法识别的应用 按钮,根据弹出窗口中提供的方式反馈给我们,锐捷云中心将对您反馈过来的应用进行分析,并加 入到特征库中,以满足您的使用需要!

邀请您加入	"锐捷云-反馈	无法识别的应用	″ 计划	
如果您发现某	个网络应用程序的	的流量无法被本设	备正确识别,导致	您无法对该应
用进行有效控	制,您可以通过以	以下方式反馈给我们	门,锐捷云中心将	对您反馈过来
的应用进行分	析,并加入到特征	亚库中,以满足您的	的使用需要!	
受镭方式:请	用邮件的方式反复	#给我们!		
邮件内容/格式	式:应用程序名称	1,版本号,备注		
列如:网际快	车,flashGet 3.7	7,下载流量无法说	别	
发送到:feed	lback_gw@ruijie	e.com.cn		
发送到:feed	lback_gw@ruijie	e.com.cn		

## 1.3.6.3.2 时间对象

可以定义时间对象,用于策略设置时候使用。

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	v 象t	/LAN对象	IP对象	URL对象	自定义内网用户对象	
说明	说明:时间对象用于定义策略生效时间。									
十添加	十添加时间对象 X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 每天			0:00-5:59 18:01-23:59			编辑删除	
	下班时间		工作日 工作日 工作日			0:00-7:59 12:00-13:00 18:01-23:59			编辑删除	
	周末		周末			0:00-23:59			编辑删除	
	上班时间		工作日 工作日		8:00-12:00 13:00-18:00			编辑删除		
	工作日		工作日			0:00-23:59			编辑删除	
显示:	显示: 10 ▼ 条共7条 【 首页 ◀ 上一页 】 下一页 ▶ 末页 】 1 确定									

1. 添加时间对象:点击 十添加时间对象 ,在弹出窗中输入对象名称,选择时间段,支持设置多个时间段。

例如新建一个 工作时间 对象:

	5	付象名:	*	
(1)	对象名称:在对象名称	l	输	入时间对象名称;

(2) 时间段周期:选择时间段的周期,即选择每周从周一到周日



(3) 时间段:设置时间段



(4) 点击添加另一个时间段

时间	段: 星期一,星期二 ▼ 00 星期一,星期二 ▼ 77	0:00 ~ 11:00 × 始时间 ~ 结束时间 ×	十添加							
完成版	后点击 完成配置 按钮 按钮 按钮 计间对象 X删除选中时间对象	H生成一个时间对象:								
	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 18:01-23:59	编辑删除						
	test	星期一 星期二	0:00-11:00	编辑删除						
	test2	星期一 星期二	0:00-11:00	编辑删除						
	下班时间	工作日 工作日 工作日	0:00-7:59 12:00-13:00 18:01-23:59	编辑删除						
	周末	周末	0:00-23:59	编辑删除						
	上班时间	工作日 工作日	8:00-12:00 13:00-18:00	编辑删除						
	工作日	工作日	0:00-23:59	编辑删除						
显示	: 10 ∨ 条 共9条		€ 首页 《 上—页 1	下一页▶ 末页▶ 1 确定						
2. 3. 4.	<ul> <li>显示 10 √ &amp; 共9条</li> <li>K 首页 4 上→页 1 下→页 2 末页1 1 0 0000000000000000000000000000000</li></ul>									

时间段:	星期一,星期二,星期▼	0:00	~	5:59	×	
	星期一,星期二,星期▼	18:01	~	23:59	×	

## 1.3.6.3.3 外网 IP 对象

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

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

外网 IP 对象配置页面:

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	IP对象	URL对象	自定义内网用户对象
外网IP对象:是相对与您 个服务器地址面置为外网 注意:修改IP子组的地址	内部网络而言的外部服务器地 IP对象,然后在流控策略循 范围时,如果该组下用户的IP	地址或其他IP地址例如 品的时候对其带宽进行 9不在此地址范围内,	:贵公司的OA或业务系 保证! 那该用户将被自动删除。	统的服务器不在内部是放在	E电信机房或托管中心;i	这个时候您为了保	证内网用户访问这	些服务器的网速那么您就可以将这
- 😂 所有外网IP 🗀 Out_Server - 😂 fff	10 2	R可以对fff进行以 ^T S编辑组 X删除	下操作: 组 十新建子组 -	┞新建IP子组 ┼添咖	用户			
👤 test	ff	ff 的用户列表 🗙 🖁	删除选中用户					
			用户名称		IP	地址		管理
		🗆 test			12.3.3.3-	12.3.3.12		编辑 删除
	ᄪ	显示: 10 ▼				▲首页 《上-	一页 1 下一	-页▶末页▶ 1 确定
▲ 批量导入导出外网	ip							

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。

✓ 编辑组
 1. 点击 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:

── 编辑用户组	×
用户组名:user-group *	
上级组名: 所有外网IP	
	确定

- 2. 点击 X删除组 按钮 , 会将选中的外网用户组或外网 IP 组从外网 IP 对象的组织结构中删除。
- 3. 点击 十新建子组 按钮,可以在选中的外网用户组下新建子外网用户组:

54	➡ 新建用户组		×
	用户组名:	*	
-	上级组名: user-group		
			确定

4. 点击 按钮,可以在选中的外网用户组下新建 IP 组:

Ŧ	■ 新建i	p组	×
	新IP组名:		*
	IP地址段:		*
		(IP段榕式192.168.1.2-192.16	8.1.5)
	上级组名:	user-group	
			确定

▲ 添加用户
 5. 点击 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

6. 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

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

☰ 编辑用户	3	×
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 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 X删除选中用户 删除。

7. 导入导出

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

《外网ip对象用户导入导出 - Internet Explorer							
R http://172.18.124.72/object_pi/bw_setobj_ipfile.htm							
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 <b>□</b> 导出用户 <b>导入文件信息规格示例:</b>							
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					

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

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

说明: 提示:	导入用户信息有利于实名制导入用户的文件名必须为 i	管理用户,方便找到用户 puser-info.csv ,并按以 ⁻	³。 下示例的规格	1埴写对应表格。		
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	按钮会弹出如下图对话	框。点击	保存②  选择	译保存路径即可。	



## 1.3.6.3.4 VLAN 对象

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

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

VLAN	配置页面如	下图所示	
------	-------	------	--

Ē	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			
f	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I	D :	* 单	们D,或ID段(如:1-6	5),多个ID可以用逗号",	"隔开,ID范围(1~4094)	9			
		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─页▶末	项 ▶ 1 确定			
1.	新建 VLN 对	<b>象</b> :只需输入 V	LAN 对象名称	弥和 VLAN 对	象 ID , 点击	添加设置	按钮,就添加一个	VLAN 对复		
2.	编辑 VLAN	<b>对象 :</b> 只需选择需	需要编辑的 V	LAN 对象点击	编辑按钮图	即可修改。例如	要编辑 vlan1 对象	,点击 编		
	按钮后,修改	收 VLAN 对象名和	尔或 VLAN 对	據 ID 后 , 点	保存编辑 击	, 按钮即可:				

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 × 单个加	D,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						
3. <b>删除 VLAN 对象:</b> 只需选择需要删除的 VLAN	时家点击 即可。例如:先要删除 vlan1	对象则主要点击后面						
的 删除 即可。如果需要全部删除 \	/LAN 对象则点击×删除全部按钮。							

## 1.3.6.3.5 IP 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	IP对象		
IP対象列表:         添加IP対象组         計添加IP対象         十添加IP対象         十批量导入IP対象         X删除选中IP対象								
	地址库			置:网关/掩码		范围配置:起始IP/结束IP		
无记录信息								
显示: 10 ▼ 条 共0約	NK C					▲首页 《 上一页 下一页 》 末页	▶ 1 确定	



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	IP对象	URL对象	自定义内	,网用户对象
IP对象列表:	1-zidiying 🔻	添加IP对象组	删除IP对象组	动IP对象 ×删除选	中IP对象				
	地址库		网段配	置:网关/掩码		范围配置:	起始IP/结束IP		操作
	cnii			-			-		编辑删除
	-			-		192.168.25.2	~ 192.168.25.2		编辑删除
显示: 10 、	条共2条					◀ 首页 ◀ 上	页 <b>1</b> 下—页	▶ 末页 ▶	1 确定

4. 添加 IP 对象组:在弹窗中输入对象组 ID,对象组描述,地址库,对象了吧等信息后,点击

按钮完成配置。

确定

- 5. 删除 IP 对象组:点击 按钮时,可以直接删除 IP 对象列表选中的对象组。
- 6. 添加 IP 对象:点击 十添加 IP 对象,可以在该 IP 组下添加 IP 对象。
- 7. 删除选中 IP 对象:点击 米删除选中IP 对象,可以删除表格选中的 IP 对象。
- 8. 编辑 IP 对象:点击 编辑 / 对该行的 IP 对象进行编辑操作。
- 9. 删除 IP 对象:点击 删除 ,对该行的 IP 对象进行单独删除操作。
- 1.3.7 行为管理

### 1.3.7.1 行为策略

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

行为管理各项功能的策略匹配是有顺序的。

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



图:各行为管理业务的处理顺序

行为策略的匹配顺序则按照策略组和规则的优先级顺序依次进行匹配:



## 1.3.7.1.1 简易配置

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



### • 开启默认审计

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

开启默认审计: ☑ 网站访问 ☑ 邮件收发 ☑ IM聊天 ☑ 论坛发贴 ☑ 搜索引擎 ☑ 虚拟身份 ☑ 开启全部

● 禁止应用



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

🥑 咀断应用 - Internet Explorer	- 🗆 🗙
R http://172.18.124.72/beh_audit_pi/beh_dropapp.htm	
<b>提示:</b> 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
非法类网页	删除
【●首页 ●上一页 1 下一页 ▶ 末页 ▶	1 确定



### 十添加阻断应用 ×删除全部



3 阻断应用 - Internet Explorer - - X R http://172.18.124.72/beh_audit_pi/beh_dropapp.htm 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! 十添加阻断应用 X删除全部 阻断应用 删除 非法DNS 删除 非法类网页 删除 股票软件 删除 ┃ 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 米删除全部 按钮可以将所有应用都从禁止应用列表中删除;

开启应用禁止功能后,设备禁止任何用户运行该列表中的应用软件。

• 禁止用户


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

户黑名单			đ
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

# 点击 十添加屏蔽用户 按钮,将弹出以下窗口:

+添加屏蔽用户

➡ 添加屏蔽用户	×	I
Q		
- 🗁 所有用户	i	
<ul> <li>         14.2.2.2      </li> <li>         ✓ ■周同学     </li> </ul>		
	确定	

确定

勾选需要禁止的用户,点击

,将选中的用户加入到屏蔽用户列表:

开启用户禁止功能后,设备将阻断屏蔽用户列表中的用户上网行为。

【用户管理】 点击 ,显示页面如下

三 【用户管理】						đ
用户组织结构	组路径:	oot 操作				
+ 📮 root	关联行为第 ×删除(	3略:共8条 D 策略查看 2 属性编辑		搜索用	月户名 ▼ 輸入用户名	查询
		名称 🔷	IP地址(MAC地址) 🜲	Web认证权限	行为策略明细	管理
		web1	2.2.2.2	×	E	编辑删除
		3231	无	√	E	编辑删除
		aaa	无	√	E	编辑 删除
		5test	无	√	E	编辑删除
		6	无	√	E	编辑 删除
		234	无	√	E	编辑删除
		E67	エ	-1	-	

### • 免审计用户



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

◎ 添加免监控用户 - Internet Explorer					
R http://172.18.124.72/user_pi/user_passuser.htm					
十添加免监控用户					
用户名称	IP地址	MAC地址	是否免流控	操作	
14.2.2.2	14.2.2.2	#	$\checkmark$	删除	
《首页 《上一页 1 下一页 》末页 ▶ 1 确定					

点击 十添加免监控用户按钮,将弹出以下窗口:

#### ╋ → 添加免监控用户

■ 添加免监控用户	×	
Q		
- 🗇 所有用户		į
<ul> <li>□14.2.2.2</li> <li>□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □</li></ul>		
□ 只免审计不免流控	确定	

勾选需要免审计的用户,免审计用户默认免流控,若需要对所选用户进行流控,则□只免审计不免流控 要打勾,点击

确定		
TUAL	添加到免监控用户列表:	

② 添加免监控用户 - Internet Explorer					
http://172.18.124.72/user_pi/user_passuser.htm###					
十添加免监控用户					
用户名称	IP地址	MAC地址	是否免流控	操作	
14.2.2.2	14.2.2.2	#	$\checkmark$	删除	
周同学	100.100.101.53	#	$\checkmark$	删除	
【▲首页 ▲上一页 1 下一页 ▶ 末页 ▶ 1 确定					

"是否免监控"栏中,√表示该用户免流控,×表示该用户需要流控;

点击 删除 可以将某个用户从免监控用户列表中删除;

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

• 禁止网站



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

该功能有两种模式:黑名单模式和白名单模式。

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

♂行为策略简易配置-网站黑白名单模式 - Internet Explorer	
R http://172.18.124.72/beh_audit_pi/beh_dropurl.htm	
● 黑名单模式 只有在黑名单网站列表下的网站才被阻断!	〇 <b>白名单模式</b> 只有在白名单网站列表下的网站才能访问!
禁止网站: ⑧选择URL分类 〇翰入网址	
选择URL分类	
添加设置	
黑名单网站列表	
黑名单网纹	よ 删除
forbidClas	is 删除
I∢ĕ	顶 《上─页 <b>1</b> 下─页 ▶ 末页 ▶ 1 确定

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

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



<ul> <li>选择URL分类</li> <li>新有分类</li> <li>→ 「前有分类</li> </ul>		×					
→ 所有分类 + □□常用热门网站							
● 所有分类 + ● □ 常用热门网站							
+ 🗀 🗌 常用热门网站		^					
+							
+ 🗀 🗌 信息资讯相关							
+ 🗀 🗌 生活服务相关			-				
+ 🗀 🗌 查询与代理		5	-				
+ □□商业与经济							
+ □□政策、法律、宗教							
+□□科学、教育、艺术		~					
+□□非法与不良							
		确定					
				<i>44</i> — 31 141 14	L.	添加设置	
直接输入网址:如卜图	所示,在"输ん	入网址"输入框中	喻入需要禁止	的网站地址	, 点击		按钮即可。
征网站: ○远洋011万关	♥퀘八网址						
I							
添加设置							
10KOH EXTT							
<b>3单网站列表</b>							
	黑名	单网站			删除		
udou.com					删除		
ku.com					删除		
		◀首页 ◀上一页	1 下─页)	末页 🕨	1 确定		
udou.com ku.com	黑名	<b>单网站</b> ↓ 首页 ▲上一页	1 下一页 )	末页 🔰	删除 删除 删除 1 确定		
	<ul> <li>□ □ 查询与代理</li> <li>□ □ 商业与经济</li> <li>□ □ 政策、法律、宗教</li> <li>□ □ 和学、教育、艺术</li> <li>□ □ 和学、教育、艺术</li> <li>□ □ 司非法与不良</li> <li>□ 直接输入网址:如下图</li> <li>山内站: ○ 选择URL分类</li> <li>□ □ 加公司表</li> <li>□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □</li></ul>	<ul> <li>□ 自询与代理</li> <li>□ 商业与经济</li> <li>□ 政策、法律、宗教</li> <li>□ 副学、教育、艺术</li> <li>□ 副法与不良</li> <li>□ 国子、教育、艺术</li> <li>□ 副法与不良</li> <li>□ 国子、教育、艺术</li> <li>□ 国子、教育、艺术</li> <li>□ 国子、教育、学校、</li> <li>□ 国子、教育、学校、</li> <li>□ 国子、教育、学校、</li> <li>□ 国子、教育、学校、</li> <li>□ 国子、</li> <li>□</li></ul>	■ □ 查询与代理 ● □ 商业与经济 ● □ 政策、法律、宗教 ● □ 非法与不良 通程输入网址:如下图所示,在"输入网址"输入框中 此网站: ○选择URL分类 ● 输入网址 「 添加设置 <b>注 阿站列表</b> <b>建 阿站列表</b> 化dou.com ku.com	● □ 直询与代理     ● □ 商业与经济     ● □ 政策、法律、宗教     ● □ 和学、教育、艺术     ● □ 非法与不良	● □ 查询与代理     ● □ 命业与经济     ● □ 政策、法律、宗教     ● □ 非法与不良	■ 「「」 ● 「」商业与经济 ● 」」政策、法律、宗教 ● 二和学、教育、艺术 ● 二非法与不良 通定 直接输入网址:如下图所示,在"输入网址"输入框中输入需要禁止的网站地址,点击 此网站: ○选择URL分类 ● 输入网址 「 「 添加设置 * # # # # # # # # # # # # #	■ 画 頭与代理 ● □ 商业与经济 ● □ 和学、教育、艺术 ● □ 申 法与不良 ● □ 申 法与不良 ● 面接输入网址:如下图所示,在"输入网址"输入框中输入需要禁止的网站地址,点击 # 此网站: ○ 选择URL分类 ● 输入网址 ↓ 「 「 「 「 「 「 「 「 「 「 「 「 「 」 」 「 」 」 」 」 」 」 」 」 」 」 」 」 」

(2) 删除禁止网站:选择需要解除禁止的网站,点击

删除 按钮即可。

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

🥑 行为策略简易配置-网站黑白名单模式 - Internet Explorer		- • ×
R http://172.18.124.72/beh_audit_pi/beh_dropurl.htm		
〇 <b>黑名单模式</b> 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: ⑧ 选择URL分类 〇 输入网址		
选择URL分类		
添加设置		
<b>白名单网站列表</b> □宽松的白名单		
白名单网站		删除
keyUrlClass		删除
门户网站与导航	沆	删除
搜索引擎		删除
●首页	〔《上─页 1 下─页》末页》	1 确定

- (1) 添加白名单网站:同样有两种方式,选择已有的 URL 分类,或直接输入网址。添加操作同添加黑名单网站,这里不再赘述。
- (2) 删除白名单网站:选择需要禁止的网站,点击 按钮即可。
- 禁止的文件类型



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

が 🥝 禁止文件类型 - Internet Explorer	_ <b>D</b> X
A http://172.18.124.72/beh_audit_pi/deny_file_type.htm	
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 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)。	1:阻断doc文件
开启文件类型禁止功能: OFF	
开启文件类型禁止功能: OFF 勾选 开启文件类型禁止功能:	
一 禁止文件类型 - Internet Explorer	X
R http://172.18.124.72/beh_audit_pi/deny_file_type.htm	
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 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)。	: 阻断doc文件
+添加禁止文件类型 X删除勾选 开启文件类型禁止功能: ○N	
+添加禁止文件类型 ×删除勾选 开启文件类型禁止功能: ○▶	

★添加禁止文件类型 点击
,添加需要禁止的文件后缀名,多个后缀名以","分隔:

■ 添加禁用文件类型	×
后缀名: 添加多个后缀名可用","分隔	
确定	取消
输入需要禁止的文件后缀名后,点击	添加到已禁止文件类型列表中:
╋添加禁止文件类型 Ⅹ删除勾选 开启文件类型禁止功能:	ON
✓.doc ✓.txt	n ☑ .jg

点击 米删除勾选 按钮,可以将未勾选的文件类型从已禁止文件类型列表中删除。

开启文件类型禁止功能后,设备禁止对指定类型的文件上传下载。

• 不审计的网站



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

🥝 不审计的网站 - Internet Explorer					
http://172.18.124.72/beh_audit_pi/add_permit_url.htm					
说明:开启该功能后,在软件升级系统类和下表中的网址不会被审计。					
★添加不审计网址 ×删除选中 开启功能: OFF					
□ 不审计的网址	操作				
☐ jd.com	删除				
tmall.com	删除				
Daidu.com	删除				
▲ 首页 ▲ 上一页 1 下一页 ▶ 末页 ▶ 1	确定				

一开启网站不审计功能:

🦲 不审	计的网站 - Internet Explorer				
R http	p:// <b>172.18.124.72</b> /beh_audit_pi/add_permit_url.htm				
说明:开启该功能后,在软件升级系统类和下表中的网址不会被审计。					
十添加	加不审计网址 X删除选中开启功能: 이 🗌				
	不审计的	砌址		操作	
	jd.com			删除	
	tmall.com			删除	
	baidu.com			删除	
	「首)」	〔《上─页 1	下一页▶末页▶	1 确定	

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

■ 添加不审计网址		×
添加不审计的网址:		
	确定	取消



可以将某个网站从不审计网站列表中删除;

点击 ※删除选中可以将选中的网站批量从不审计网站列表中删除;

打开该功能后,这里配置的网站的访问不会被设备审计,也不会被阻断。

禁止客户端邮件 



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

② 行为策略简易配置-禁止邮箱帐号 - Internet Explorer					
<b>≈</b> http://172.18.1	24.72/beh_audit_pi/beh_dropmail.htm				
禁止邮箱帐号:	80670523@qq.com 添加设置				
禁止邮箱帐号	列表				
	禁止的邮箱帐号	删除			
80670523@qq	.com	删除			
	┃ ● 首页 ● 上一页   1   下一页 ● 末页 ▶ ┃	1 确定			

#### 禁止 QQ 帐号

点击



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

₽ QQ帐号(邮箱地址或数字帐号)不能为空,请重	新输入! - Google Chrome	
① 172.30.73.233/beh_audit_pi/beh_drop	pim.htm	
●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:	添加设置	
禁止QQ帐号:		
	QQ帐号	删除
	465465	删除
	594646	印度

### 1.3.7.1.2 高级配置

显示: 10 • 条共2条

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

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

↓ 首页 ↓ 上一页 1 下一页 ▶ 末页 ▶

1

确定

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

高级配置页面如下:

简易	高级配置	审计告警	告警信息查询					
说明 帮助	<b>説明:</b> URL重定向不支持対HTTPS加密的网站进行重定向。 帮助: Q 行力策略常见功能如何使用?							
+添加	上添加行为策略 X 删除选中 十 根据模板建策略 X 清除所有内容审计记录 十 设置HTTPS加密内容审计							
		策略组名称		关联用户	策略开关	状态	匹配顺序	操作
		bb 🔳		外部用户: root	☑ 开启	未生效 😮	\$	编辑删除
		aa 🔳		aa	☑ 开启	未生效 😮	۲	编辑删除

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

其中点击 十根据模板建策略 ,可以基于现有的策略基础上创建新的策略。如下图所示:

+根据模板建策略 × 清除所有内容审计记录	_
禁止上班时间使用工作无关业务(系统模板)	系统自带的策略
禁止P2P下载工具 (系统模板)	
• 审计上网行为 (系统模板)	
• test	当前已有的策略

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

点击 * 清除所有内容审计记录 将会清空设备上所有的行为审计记录。操作如下:

□ + 根据模板建策略 × 清除所有内	的容审计记录 查询策略组:包含继承父组
来自网页的消息	
移删除硬盘上所有的行为审计 点击"确定"审计模块将自动	十记录 , 请慎重考虑 ! 协重启 , 重启后将看不到任何行为记录 !
	确定取消

#### • 新建和编辑策略

要创建行为策略请参考如下步骤:

- 1. 点击 → 添加行为策略 弾出 "添加行为策略"配置向导窗口。
- 2. 策略组名:在"策略组名称"中输入能够标识该策略的规则或用途的名称;

■ 添加行为策略					
策略组名称	: 輸入策略组名称 * ☑ 启用该策略 【用户管理】				
策略设置	∃ 关联用户				

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

■ 添加行为策略 ×						
策略组名称: 输入策	離组名称 ★ ✔ 启用该策略	音 【用户管理】				
策略设置  关职	关用户					
上网权限策略	应用控制策略					+
	选择应用	控制	生效时间	状态	匹配顺序	管理
>> 其他策略					保在	天闭
点击左侧的规则名称可以查看该类型下的所有规则,如果要编辑则要选中前面的复选框 除、添加操作。最后点击"完成"保存。各个类型的添加界面请参考下面章节。 控制规则说明: 允许并审计:不阻断选中用户的上网行为,但会记录上网信息。						
允许但不审计:不	阳断选中用户的上网行为,也不证	己录其上网信息。				
阻断并审计:阻断	「选中用户的上网行为,同时记录]	下阻断信息。				

阻断但不审计:阻断选中用户的上网行为,但不记录其阻断信息。

生效时间:这条规则的生效时间,只有在生效时间内该规则才有作用。

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

≡	添加行为策略		×
策略	组名称: 输入策略	略组名称 ▲ ▲ 启用该策略 【用户管理】	
策	略设置 关联	用户	
	用户类型	٩	
	本地用户	<ul> <li>□□ 所有用户</li> <li>+□□ 用户组a</li> </ul>	
	外部用户	+ □ 用户组b	
		🤄 🔲 qqwe	
		注:勾选用户组后,该组下的所有用户将自动继承该策略("排除继承"的用户除外)。	
		保存	关闭

### • 应用控制

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

				×
策略组名称: 输入策略组名称	* 🗹 启用该策略 【用户管理】			
策略设置   关联用户				
<b>上网权限策略</b>	■ 添加应用控制策略	×		+
应用控制       选择应用           选择应用	选择应用: 【点击进行选择】 控制: 允许但不审计 ▼ 生效时间: 所有时间 ▼ 【时间管理】	确定	匹配顺序	管理
			保存	关闭

点击"选择应用"输入框将弹出如下界面:

■ 选择应用	可以从现有的应用	月组中选择 ×			
Q 选择要控制的应用	<ul> <li>新建</li> <li>切有应用组</li> </ul>	1			
- □ □ 所有应用	已选应用				
	IP网络电话	$\otimes$			
+ □ ☑ 网络游戏软件	网络游戏软件	$\otimes$			
+ 💭 🗹 视频流媒体软件	1. 视频流媒体软件	$\otimes$			
+ □ P2P应用软件 + □ □ 股票软件	B P2P应用软件	$\bigotimes$			
- ^〇 □ WEB应用	删除已进	选中的应用			
[●] □普通网页浏览 [●] □HTTP代理					
● □开心网	输入新建应用组的名称	Я			
<	应用组名: 输入分组名称	*			
自定义应用 ◆ 支持自定义应用 确定 取消					

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

### • 网站访问策略

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

三 添加行为策略					
策略组名称: 输入策略	路组名称	☑ 启用该策略 【用户管理】			
策略设置 关联	用户				
上网权限策略	网站访问策略	■ 添加网站访问策略	×		+
<ul> <li>□应用控制</li> <li>② 网站访问</li> <li>&gt; 其他策略</li> <li>□邮件控制</li> <li>□WEB邮件</li> <li>□IM聊天</li> <li>□BBS论坛</li> <li>□搜索引擎</li> <li>□文件控制</li> <li>□外发信息</li> </ul>	选择网站	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

点击"选择网站"输入框将弹出如下界面:

		可以从现有的网站组中	选择	× ۲	
Q 选择要控制的网站	● 新建	○ 现有网站组			
	已选网站				
+□□□常用热门网站	门户网站	与导航	$\otimes$	^	
+ □ ☑信息资讯相关	搜索引擎		$\otimes$		
	网购		$\otimes$		
土 □ □ 鱼询与代理 + □ □ 商业与经济	WEB通信	删除已选中的网站	$\otimes$		
+ □□政策、法律、宗教	微博客		$\otimes$		
	体育		$\otimes$		
+ □□国外网站、软件更新	军事	新建网站组的名称	$\otimes$	~	
	网站组名:输				
自定义网站类 <b>支持自定义网站类</b>					

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

### • 邮件控制策略

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

上网权限策略	邮件控制策略	☰ 添加邮	件控制策略	×		+
□应用控制	匹配关键				兀配顺序	管理
□网站访问		控制类型:	收发帐号    ▼			
¥ 其他策略		匹配关键字:	【点击进行选择】			
✔邮件控制						
■WEB邮件		控制:	允许并审计    ▼			
□IM聊天		最大限制:	K(范围1~30000K)			
BBS论坛						
□搜索引擎		主效时间:	所有时间▼【时间管理】			
□文件控制			确定			
□外发信息 ▼						

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

点击匹配关键字时弹出如下面窗口:

三 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	组名称:web_block_mail    *	
○默认不选择 ●web_block_mail ○web_block_im	关键字: <mark>每一行算一个关键字</mark> 80670523@qq.com 若有修改,请先点击保存设置 保存设置	
	确定取消	肖

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

### • WEB 邮件策略

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

### • IM 聊天审计策略

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

				×
<b>策略组名称:</b> 输入策略组名称 *	☑ 启用该策略 【用户管理】			
策略设置  关联用户				
上网权限策略 IM聊天策略	── 添加IM聊天策略	×		+
<ul> <li>□应用控制</li> <li>□网站访问</li> <li>□ 四站访问</li> </ul>	控制类型: IM帐号	•	匹配顺序	管理
	匹配关键字: 【点击进行选择】			
□ WEB曲β件	控制: 允许并审计	•		
	生效时间: 所有时间 ▼ 【时间管理】			
		确定		
			保存	关闭

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

### • BBS 论坛策略

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

→ 添加行为策略					
策略组名称: 输入策	略组名称 *	☑ 启用该策略 【用户管理】			
策略设置 关联	美用户				
上网权限策略	BBS论坛策略	── 添加BBS论坛策略	×		+
<ul> <li>□应用控制</li> <li>□网站访问</li> <li>&gt; 其他策略</li> <li>□邮件控制</li> <li>□WEB邮件</li> <li>□IM聊天</li> <li>&gt; BBS论坛</li> <li>□搜索引擎</li> <li>□文件控制</li> <li>□外发信息</li> </ul>	匹配关键:	匹配关键字: 【点击进行选择】 控制: 允许并审计 、 生效时间: 所有时间 、【时间管理】	确定	匹配顺序	管理
				保存	关闭

当用户所发的贴中包含"匹配关键字"时,设备将根据策略规则对贴子进行审计。

### ● 搜索引擎策略

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

📃 添加行为策略					×
策略组名称: 输入策略组织	名称 * 🖉	☑ 启用该策略 【用户管理】			
策略设置 关联用户	1				
上网权限策略 搜	索引擎策略	■ 添加捜索引擎策略	×		+
<ul> <li>应用控制</li> <li>网站访问</li> <li>¥ 其他策略</li> <li>邮件控制</li> <li>WEB邮件</li> <li>IM聊天</li> <li>BBS论坛</li> <li>✓ 捜索引擎</li> <li>文件控制</li> <li>小发信息</li> </ul>	匹配关键:	<ul> <li>□配关键字: 【点击进行选择】</li> <li>搜索类型: □网页 □新闻 □图片 □视频 □音乐 □地图</li> <li>□百科 知道 □社交网页 □学术 □股票 □ =</li> <li>□旅游</li> <li>控制: 允许并审计 ▼</li> <li>生效时间: 所有时间 ▼ 【时间管理】</li> </ul>	图 同 词 典 书 库 一 购物 物 一 、 、 、 、 、 、 、 、 、 、 、 、 、	匹配顺序	管理
				保存	关闭

• 文件控制

				×
策略组名称: 输入策略组名称	* 🗹 启用该策略 【用户管理】			
策略设置  关联用户				
上网权限策略 文件控制策略	■ 添加文件控制策略	×		+
回应用控制 匹配关键 四站访问	" 控制类型: 文件名	•	匹配顺序	管理
► 其他策略	匹配关键字: 【点击进行选择】			
□WEB邮件	控制: 允许并审计	T		
	生效时间: 所有时间 ▼ 【时间管理】			
□搜索引擎		确定		
			保存	关闭

### • 外发信息

📃 添加行为策略					×
策略组名称: 输入策	略组名称 *	☑ 启用该策略 【用户管理】			
策略设置 关联	用户				
上网权限策略	外发信息策略	── 添加外发信息策略	×		+
<ul> <li>□应用控制</li> <li>□网站访问</li> <li>¥ 其他策略</li> </ul>	匹配关键		1	匹配顺序	管理
□邮件控制 □WEB邮件		12前· 九井井車订 ▼ 生效时间: 所有时间 ▼ 【时间管理】			
□IM聊天 □BBS论坛			确定		
<ul> <li>□1000 Jup</li> <li>□1000 J</li></ul>					
				保存	关闭

• QQ 聊天内容

保存

关闭

■ 添加行为策略						
策略组名称: 输入策	略组名称 *	☑ 启用该策略 【用户管理】				
策略设置 关联	用户					
<ul> <li>邮件控制</li> <li>WEB邮件</li> </ul>	QQ聊天内容策略	── 添加QQ聊天内容策略	×		+	
□IM聊天	匹配关键:	控制: 审计 (需安装插件)	•	匹配顺序	管理	
□BBS论坛		牛效时间: 〔近右时间 ▼ 【时间管理】				
□搜索引擎						
□文件控制			确定			
□外发信息						
✓QQ聊天内容						
■URL重定向						
FTP						
Telnet						
				保存	<b>荞 关闭</b>	

### • URL 重定向

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

📃 添加行为策略					×
策略组名称: 输入策	略组名称,	🗹 启用该策略 【用户管理】			
策略设置 关联	用户				
<ul><li>■邮件控制</li><li>■WEB邮件</li></ul>	URL重定向策略		×		+
□IM聊天	访问网站	访问网站:		匹配顺序	管理
□BBS论坛		跳转网站:			
		生效时间: 所有时间 ▼ 【时间管理】			
			确定		
□QQ聊大内容 <b>IRL重定向</b>					
□FTP					
Telnet					

• FTP

■ 添加行为策略				×
<b>策略组名称:</b> 输入策略组名称	☑ 启用该策略 【用户管理】			
策略设置  关联用户				
□邮件控制 [▲] ■WEB邮件	═ 添加FTP策略	×		+
□IM聊天 匹配文件	, 「 匹配文件名: 【点击进行选择】		匹配顺序	管理
BBS论坛 授索引擎 文件控制	控制: 允许并审计 ▼ 生效时间: 所有时间 ▼ 【时间管理】			
■		确定		
□URL重定向 <b>☑FTP</b> □Telnet _▼				
			保存	关闭

#### • TELNET

				×
<b>策略组名称:</b> 输入策略组名称 *	☑ 启用该策略 【用户管理】			
策略设置  关联用户				
□邮件控制 [▲] Telnet策略	■ 添加Telnet策略	×		+
□IM聊天 匹配关键 [。]	控制: 允许并审计 ▼		匹配顺序	管理
□BBS论坛				
□搜索引擎	至双时间, 所有时间 ▼ 【时间管理】			
□文件控制		确定		
□外发信息				
□QQ聊天内容				
□URL重定向				
FTP				
✓Telnet -				
			保存	关闭

### • 设置 HTTPS 加密内容审计

说明: URL重定	向不支持对HTTPS加密的网站进行	重定向。
帮助: bl 行为	唐略常见功能如何使用?	点击进入HTTPS加密内容审计页页
十添加行为策略	X删除选中 十根据模板部	畫策略 × 清除所有内容审计记录 +设置HTTPS加密内容审计
■ 开启QQ群聯天	「内容审计(需要先通过局级看	2置开启QQ聊天内容审计策略)
高級配置 高级配置		
Ξ 设置HTTPS加索内容审	it	s ×
- 逐加例外用户 × 清空例外	(19)5-19)5-19 (19)5-19)5-19	現作
	testa	Hote
显示 10 • 条共1条		H前面 + 上一页 1 下一页 ▶ 未页 H 1 (ma)
E信加密内容审计: ☑ (可	₽₩IH 点击可开启/关闭加密内容审计功 IXMSSL加密后的邮件收发、论坛发帖、搜索引擎	能 3、外发文件、虚拟身份等进行审计。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。)
周加麥內容审计: 2 (可 载SSL根证书 说明 添加例外用户 ×清空例	₩ 点击可开启/关闭加密内容审计功 IMSSL加密后的邮件收发、论坛发帖、搜索引厚 :根证书下载到终端PC后,点击鼠标 直接点击下载	能 8、外发文件、虚拟身份等进行审计。需要在终端电脑上导入SSL根证书,避免终端浏览器告誓或应用使用异常。)   7. 方键选择 "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。
日加坡内容审计: 2 (可 载SSL根证书 说明 承加例外用户 ×清空例	##i+ 点击可开启/关闭加密内容审计功 顶SSL加密后的邮件收发、论坛发帖、搜索引擎 :根证书下载到终端PC后,点击鼠标 直接点击下载 例外用户 例外用户	能 低、外发文件、虚拟身份等进行审计,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。) 示右键选择"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。 最作
周加寒内察审计: 2 (回 载SSL根证书 说明 添加例外用户 ×清空例	##i+ 点击可开启/关闭加密内容审计功 IXJSSL加密后的邮件收发、论坛发帖、搜索引导 ::根证书下载到终端PC后,点击副标 直接点击下载 例外用户 testa	能 低、外发文件、虚拟身份等进行审计。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。) 示右键选择"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。 操作 删除
Gamma Jake 9 日 Halmson容审计: ⑦ (可 载SSL根证书 说明 添加例外用户 × 清空例 読示 10 ▼ 条 共1条	Amit 点击可开启/关闭加密内容审计功 IXIJSSL加密后的邮件收发、论坛发帖、搜索引擎 :根证书下载到终端PC后,点击副板 直接点击下载 例外用户 例外用户 testa	部 数、外发文件、虚拟身份等进行审计。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。) 或右键选择"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。 操作 服除 以首页《上一页 1 下一
	##it 」点击可开启/关闭加密内容审计功 [XJSSL加密后的邮件收发、论坛发帖、搜索引导 ::根证书下载到终端PC后,点击最极 直接点击下载 例外用户 testa ,可以删除该行的例外用」	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
	##it 」点击可开启/关闭加密内容审计功 IXJSSL加密后的邮件收发、论坛发帖、搜索引导 : 根证书下载到终端PC后,点击副校 直接点击下载 例外用户 使sta ,可以删除该行的例外用, 小可以删除,该行的例外用,	能 本、外发文件、虚拟身份等进行审计、需要在终端电路上导入SSL根证书,递免终端浏览器苦警或应用使用异常、)   示石键选择"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。   《 加爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾爾



## 1.3.7.1.3 审计告警

简易配置	高级配置 审计	<b>告警</b> 告警信息查	询	
说明: 当某一参	屹应用被审计时, 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,请先到高级酮	已置添加告警策略。
审计告警: 이				
发送告警邮件:	ON			
ŧ	附主题: 内容审计告警	* 😢		
	收件人:	* 多个	→可以用逗号隔开,最多配置6个邮络	箱
确定	前往配置发件	曲阳牛		
告警周期设置				
邮件告警	<b>计 间隔时间:</b> 5	分钟		
确定				
前往配置发	文件邮件			

深 发件邮箱配置 - Google	Chrome	—	×
③ 不安全   172.21.6.12	2/system_pi/setsys_mail_config.htm		
邮件发送开关:	□开启		
发送邮件服务器:	* 如: smtp.126.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:	* 女[]: xxx@126.com		
帐号密码:	(加密密码不显示,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!)		

## 1.3.7.1.4 告警信息查询

简易配置	高级配置	审计告警告警	結息查询				
开始时间: 2018-03-26 10:48 结束时间: 2018-03-29 10:48 审计类型: 所有类型 • 查询							
时间	I	用户 本地用户 ▼	IP	策略名	审计类型	访问控制	详细信息
2018-03-27	7 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://su g.m.baidu.com/su]
2018-03-27	7 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://16 3.com/]
2018-03-27	7 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://ww w.163.com/]

### 1.3.7.2 实时审计记录

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	实时审计记录总共产生 0 务	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	显示 10 · 条共0条 【首页 《 上一页 下一页 》 末页 】									

### 1.3.7.3 阻断信息记录

<b>卿:</b> 由于	网站访问及外发信息的记录数通	<b>第七较多,本页面不显示这两个审计</b>	记录。			
输入IP	977	(设置IP后,系统将只记录)	giP的阻断信息,之前的	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	<b>网络哈尔马马</b>	擒要位度
1	1.1.241.10	2017-10-31 10:24:29	search	BING搜索	搜索阻断	<b>注</b> 4回
2	1.1.241.10	2017-10-31 10:24:07	search	BING搜索	複素這新	1749
3	1.1.241.10	2017-10-31 10:16:03	search	BING搜索	搜索组断	关键字:abcdefg, 搜索关型: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, 提索类型:网页

### 设置特定 IP





ŢZ		
₽ŗ	关键字:111111111111111111111111111111111111	<b>設置为空。</b> )
<b>a</b> i		摘要信息
0-		¥ 详细
0-		详细
0-		关键字:abcdefg, 搜索类型:
0-		关键字:abcdefg, 搜索类型:
0-		关键字:abcdefg, 搜索类型:
		( 首页 《 上─页 1 下─页 》 末页
	关闭	

### 1.3.7.4 审计日志查询

### 1.3.7.4.1 访问审计报表

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

访问	<b>] 审计报表</b> 内容审计报表									
\$	今日审计报表 Q 高级查询 び 号出报表									
	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	明細 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://mediav.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://i.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	★页 1 确定						



Q 高级查询 会弹出高级查询的参数选择界面,具体请参考本章第6点。

点击 GHH 与出报表 可以将查询的报表结果导出保存到 PC 上。

1、 网站访问排行:

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

访问	可审计报表	内容审计报表							
\$	今日南计报表 Q 高级查询 C 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.co	om.cn					31	商业	明细 阻断
2	http://cloud.br	owser.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://mediav	.com					10	未知分类	明细 阻断
5	http://img1.pc	fg.cache.wpscdn.cn					10	未知分类	明细 阻断
6	https://baidu.c	om					7	百度	明细 阻断
7	https://fanqiar	bb.com					6	未知分类	明细 阻断
8	https://browse	r.qq.com					5	IT类	明细 阻断
9	http://i.y.qq.co	m					4	音乐	明细 阻断
10	http://bbs.csdi	n.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,如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									
R 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) 本地用户 V	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─页 】 下─页 》末页 ) 1 確定									

### 2、 用户访问排行:

该表格显示了用户访问网站数目的排行,访问越多的用户排在越前面:

4	日审计报表	Q 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	用户者 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
	《 首页 《 上一页 1	下一页 🕨 末页	▶ 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:

网站访问监控 - Internet Explorer R http://172.18.124.72/beh report pi/u	url detail.htm			
您当前查看的是 100.100.101.50 自				
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
	【▲首页 《上一	-页 <b>1</b> 下一页	▶ 末页 ▶ 1	确定

### 3、 网站访问明细:

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

网站访问排行 用户说	5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/qqmusic/fcgi-bi		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://ruijie.com.cn		商业	允许	默认审计
			▲首页 《上—3	<b>1</b> 2 3 4 5	下─页▶末	页】 1 确定

### 4、 被阻断的网站:

### 该模块下也是一个表格,显示了所有被阻断的网站信息:

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:

🥝 网站访问监控 - Internet Explorer	-			
R http://172.18.124.72/beh_report_pi/u	rl_detail.htm			
您当前查看的是 www.tudou.com	的流量明细			
用户(IP) 本地用户 🗸	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
	Ĭ₹	顷 《上─页 <b>1</b> 下─页	▶ 末页 ▶ 1	确定

### 5、 应用控制审计

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

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
					I	首页 《上─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。

6、 高级查询

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

默认审计

默认审计

默认审计

1

音乐

体育

搜索引整

允许

允许

允许



### 1.3.7.4.2 内容审计报表

/192.168.1.132(192.168.1.132)

/192.168.1.132(192.168.1.132)

/192.168.1.132(192.168.1.132)

https://y.qq.com

https://hupu.com

https://baidu.com

2018-04-04 10:39:52

2018-04-04 10:39:24

2018-04-04 10:38:59

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

访问审计报表	内容审计报表								
时间范围: 本	本周							Q高级	直询 🖸 导出报表
客户端邮件	WEB邮件	IM聊天	论坛发贴	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	8	发送帐号	接收	2145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
0		-							
通过	同级宣闻	」 按钮可以查	间各种内	容审计信息。	。通过 🖸	导出报表	按钮可以导出	各种内容审	计报表。

1、 客户端邮件

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

客户端邮件	WEB邮件	IM聊天	论坛发贴	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) 本均	b用户▼	审计时间	发	送帐号	接收	女帐号	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

2、 WEB 端邮件

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

时间范围:本日本周							Q 高約	吸查询 🕻 导出报表
客户端邮件 WEB邮件 TELNET	IM聊天	论坛发贴	搜索引擎	虚拟身份	插件QQ聊天内容	外发文件	外发信息	FTP
用户名(IP) 本地用户▼ 审论	十时间	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─页 ▶ 末3	፤ ▶ 1 确定

### 3、 IM 聊天

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

客户端邮件	WEB 曲 附件	IM聊天	论坛发贴	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	匹置	己规则
							▲ 首页 ▲ 上一页	1 下─页▶ 末	5 M 1 7

4、 论坛发贴

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

客户端邮件	WEB邮件	IM聊天	论坛发贴	搜索引擎	虚拟身份	插件QQ聊天内容	外发文件	外发信息	F	TP
TELNET										
用户名(IP)本地用	户▼ 审	计时间	网页地址	ļ	具体应用	发送帐号	发贴标题	/内容 ;	方问控制	匹配规
								• <b>- - - -</b>	+ T N	4

### 5、 搜索引擎

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

客户端邮件	WEB邮件	IM聊天	论坛发贴	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									
田白冬(IP) 大地田白	• + ++++++++++++++++++++++++++++++++++	9	No 25 Hittel	目体应用			-		
10/ 10/ 14/8/日/一	• • • • • • • • • • • • • • • • • • •	6)	网贝地址	景种应用	授案失)	別	약 1	万问控制	「「「「「」」」「「」」「「」」「」」「「」」「」」「」」「」」「」」「」」「

### 6、 虚拟身份

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

客户端邮件	WEB邮件	IM聊天	论坛发贴	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

### 7、 插件 QQ 聊天内容

客户端邮件	WEB邮件	IM聊天	论坛发贴	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	用装	送类型	发送帐号	发送qq号	接收帐号	接收qq号	消息内容	
									-	

### 8、 外发文件

客户端邮件	WEB邮件	IM聊天	论坛发贴	搜索引擎	虚拟身份	插件QQ聊天内容	外发文件	外发信息	F	TP
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	8	访问控制	匹配规则
							▲首页  ▲上一页	1 下一页▶	末页▶	1 确定

### 9、 外发信息

客户端邮件	WEB邮件	IM聊天	论坛发贴	论坛发贴 搜索引擎		虚拟身份 插件QQ聊天内容		外发信息	F	TP
TELNET										
用户名(IP)本	地用户▼	审计时间	ļ	具体应用	pi	顶地址	发送内容	i	方问控制	匹配规则
							●首页 ●上一页	1 下一页 ▶	末页 🕨 🗍	1 确:

### 10、 FTP

客户端邮件	WEB邮件	IM聊天	论坛发贴	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「	自计时间	目的lp		文件名	传输方向	访问控	制	匹配规则

### 11、TELNET

客户端邮件	WEB邮件	IM聊天	论坛发贴	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lp		动作	访问控制		匹配规则	
							◀首页 ◀上一页	1 下一页 ▶ 末3	হ ▶ 1	确定

### 12、高级查询

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

	1、点击展开高级查询 Q 高级查询
;	<u>型</u> ×
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	0
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	<b>文</b> 确定查询
	4、点击确定查询

查询结果如下图所示:

查询条件					Q 高级查	间 🕻 导出报表
选择类型:WEB端邮件	ŧ				可以选	译导出的数据
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
WEB端邮件						
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
			▲ 崔	页 《上—页 1 下—	页▶ 末页 ▶	1 确定

1.3.7.5 行为统计分析

## 1.3.7.5.1 报表配置

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: 2.报表预生成开 3.报表预生成开	报表查询等待的时间, 关打开后,凌晨(默) 关打开后,当天的数	我们采用数据后台预 人凌晨3点)设备会在 居可以在第二天(默认	项生成的方式,因此要 后台生成审计报表数3 入凌晨3点后)查询,荷	想查询审计报表,必 据,此时可能造成CPI 在这之前的数据将无法	须先打开开关。 U短时间内升高,并且 去查询,因此如果需要	会消耗一定的硬盘存 ]查询审计报表,建议	储空间。 提前开启本功能。
报	表预生成: ON						

## 1.3.7.5.2 自定义报表

报表配置	自定义报表	客户端部件	WEB 由 时件	IM聊天	搜索引擎	论坛发帖	外发文件	网站分类	网站域名	虚拟导份	
爆加规则	×删除选中										
8	规则名称		已生成报表		i	Triasta		រោល	UM ANI	擾	n
8	111		0			无		按	天	18458	删除
0	3		0			无		拉	天	sasa	翻除
	2		15		vih277@126	.com.123@126.co	m	10	天	10100	8814

点击添加规则
☰ 添加规则			×
规则名称:	test		
统计周期:	र र		
显示TOP:	10 •		
用户类型:	◉ 本地用户		
选择用户:	所有用户 ▼		
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
			200

# 点击保存

报表配置	自定义报表	客户调邮件	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	
一添加规则	×删除选中										
0	规则名称		已生成报表			订阅邮箱		订例	問期	採	t)e
	test		0			无		15	庆	9658	翻除
0	111		0			无		扬	天	编辑	删除
8	3		0			无		核	天	988i	删除
0	2		15		yjh277@126	.com,123@126.ci	om	12	天	6655	删除

# 点击编辑

── 编辑规则	$\times$
规则名称: test	
統计周期: 天 🔻	
显示TOP: 10 •	
用户类型: ⑧ 本地用户	
选择用户: 所有用户▼	
排行报表: 國搜索引擎 圖论坛发帖 圖外发文件 圖网站分类 圖网站域名 圖虛拟身份 圖客戶端邮件 圖网页邮件 圖IM聊天	
是否发送邮件: ●是 ◎否 自定义收件人 (每行输入一个收件邮箱,最大支持6个) 597485557@qq.com 597888888@qq.com	
<b>保存</b> 关闭	Ð

#### 点击保存

jle Translate 📙 锐捷 📙 EW	EB 172.21.159.139:8078 显示: ×	
── 编辑规则	本规则已生成的报表数据将会被请空! 是否要继续?	×
规则名称:	<b>确定</b> 取消	
统计周期:	χ. τ	
显示TOP:	10 •	
用户类型:	<ul> <li>●本地用户</li> </ul>	
选择用户:	所有用户 ▼	
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:	<ul> <li>● 査</li> <li>自定义收件人(每行输入一个收件邮箱,最大支持6个)</li> <li>597485557@qq.com</li> <li>597888888@qq.com</li> </ul>	
	保存 关键	স

### 点击确定

报表配置 ·添加规则	自定义报表 ×删除选中	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	
	规则名称		已生成报表		1	丁间邮箱		ija	UMUNU	授	作
8	test		0	5	97485557@qq.c	om,5978888888@	qq.com	ţ5	沃	<b>S</b> (6	<b>B</b> (19:
	111		0	1.0		无	1. A.	10	庆	-	翻除
0	3		0			无		16	沃	196-197	删除
8	2		15		yjh277@126	.com,123@126.co	om	18	沃	1941	删除

# 点击删除

百度一下, 你就 @WEB 易网	和道 🗣 Google Tran 实EG管理员:admin	slate <mark>] 税證  </mark> EWEB <b>补丁版本:</b> 无补丁   补	172.21.159.13 确定要删除规则 ter	9:8078 显示: × 8:678 最示: 8:078 最示: 盘恋要递	3 (A.B.B.B.	♀ 役备目校	<b>出</b> 软件版本下载	1. 22	☆ 在线客服	₿
报表配置	自定义报表	客户谱邮件		Main Rom	外发文件	网站分类	网站成名	虚拟身份		
	规则名称	Ea	成报表	1.J MARAG		ជ	间周期		操作	
	test		0	597485557@qq.com,5978888888@q	ą.com		按天	5	191 Billio	
	111		0	无			按天	5	111 BER	
	3		0	无			按天	5	iiii Blik	
8	2		15	yjh277@126.com,123@126.com	1		按天	5	1511 BB100	
显示: 10	▼ 景 共4祭					H	雨 《上一页 1	下页 🖡 末回	EH 1	确定

### 点击确定

很非配置	自定义报表	客户调邮件	WEB胡科牛	IM聊天	搜索引擎	10153286	外发文件	网站分类	网站域名	虚拟身份	
十個加规则	X删除选中			test规则已删	189:						
0	规则名称		已生成报表		i	丁间邮箱		订阅	间期	操	作
8	111		0			无		15	沃	96197	10179:
	3		0			无		挖	沃	编辑	删除
8	2		15		yjh277@126	.com,123@126.co	mc	18	沃	16151	删除
显示: 10 •	条 共3条							14 (0)	司《上一页 1	下一页 ▶ 末页 Ħ	1 201:

# 点击已生成报表这一列

☰ 报表列表							a 1
	зФ						
0	报表名称		统计时间	订阅周期	生成时间	PDF报表	操作
0	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 09:43:19	FR	删除
8	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 09:38:18	下級	8599
8	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 09:30:32	<b>TF82</b>	855A
0	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 08:58:37	下蛇	删印
0	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 08:53:41	下報	删除
8	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 13:52:07	THE	删除
0	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 13:44:52	下载	809
	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 13:42:11	下载	影吟
0	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 13:11:03	TSR	删除
0	2	2018-05-03	00:00:00 2018-05-03 23:59:5	9 按天	2018-05-04 13:04:02	下载	册99

已生成的报表可进行下载、删除操作

# 1.3.7.5.3 客户端邮件

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:	◉ 本地序	用户			
	选择用户:	所有用户	⊐ ▼			
	统计周期:	天		¥		
	选择时间:	2018-07	7-12			
		确定	查询			

显示排行: Top10   统计	十日期:2018-05-03 00:00 至	9 2018-05-03 23	:59   用户: 所有用	户	l	返回查询 导出报表
				test_11 test_9 test_7 test_13 test_4 test_5 test_6 1.1.241. 1.1.241. test_12 test_12	10 20	
排行	用户名	IP地	bl:	收邮件数	发邮件数	邮件发送占比
1	test_11	192.168	.1.11	26	43	39.09%
2	test_9	192.168	3.1.9	13	20	18.18%
3	test_7	192.168	3.1.7	9	8	7.27%
4	test_13	192.168	.1.13	7	8	7.27%
5	test_4	192.168	3.1.4	7	6	5.45%
显示: 5 ▼ 条 共10条				▲ 首引	页 《 上─页 1 2 下─页)	末页▶ 1 确定
三 客户端邮件接收信息						s ×
用户名: test_11 统计日期: 2018-05-03 00:00 到。	2018-05-03 23:59					
用户者(IP)	审计时间	发送帐号	接收帐号	邮件标题/内容	3 访问控制	匹配规则
			无记录信息			
显示 10 ▼ 祭					目前页 4 上一页 下	一页▶ 末页月 1 确定

1.3.7.5.4 WEB邮件

	报表配置	自定义	报表	客户端邮件	WEB邮件	IM聊天	搜索引擎
		统计维度:	用户排行	ī	T		
		显示TOP:	10		T		
		用户类型:	◉ 本地用	户			
		选择用户:	所有用户	1 🔻			
		统计周期:	天		T		
		选择时间:	2018-07	/-12			
			765.000				
			4用大王.	旦问			
	显示排行: Top10   统计日	王期:2018-05-03 00:00	到 2018-05-03 2	3:59   用户: 所有用户		返回查询 导出报表	
					1.1.241.10		
	推行 用户谷	名	IP地址		应用类型统计	邮件总数	
	1 1.1.241	1.10	1.1.241.10		QQ邮箱发邮件:4	4	
	显示: 5 ▼ 条 共1条				( 首页	▶ 萩) 1 确定	
=	用户 (1.1.241.10) 应用类型组	统计排行				6	×
	户名: 1.1.241.10   统计日期: 2	2018-05-03-00:00 🗐 2018-	05-03-23:59				
			122	-	QQ邮箱发邮件		
	1077			应用类型		邮件总数	
	1			QQ由FR最发用F/中		4	
靈疗	元 5 ▼ 条 共1条				H 苗页 4 上一	页 1 下页 1 未页 1 1	雕定

戶名: 1.1.241.10							
計日期: 2018-05-03	8 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
			无记载	設備度			

# 1.3.7.5.5 IM 聊天

报表配置	自定义	报表	客户端邮件	WEB曲附牛	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/	<b>当</b>			
	选择用户:	所有用户	•			
	统计周期:	天		•		
	选择时间:	2018-07-	12			
		确定查	询			
显示排行: Top10   參	钻日期:2018-05-03 00:00	) 到 2018-05-03 23:5	9   用户: 所有用户		返回查询 导出报表	
				1.1.241.10 1.1.241.20		
排行	用户名	IP地址	退出次数	登录次数	登录数占比	
5015						
1	1.1.241.10	1.1.241.1	0 0	16	94.12%	

三 用户登录信息					8 ×
用户名: 1.1.241.10 统计日期: 2018-05-03 00:00 到	9 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	区配规则
		无记录	發信應		
显示 10 • 祭				H 普页 4 上一页 下	

# 1.3.7.5.6 搜索引擎

报表配置	<b>王</b>	搜索引擎	论坛发帖	外发文件	网站分类	网站域名	虚拟身份
	42	充计维度: 关键	建字排行	•			
	티	显示TOP: 10		T			
	48	充计周期: 天		T			
	ž	选择时间: 201	8-04-03				
			确定查询				
点击 确定	直询						
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		
	·	腓行: Top10   統计日其	B: 2018-04-03 00:00 到 201	8-04-03 23:59	<ul> <li>         ・皇家马德里         <ul> <li>百度罰達</li> <li>重点力峭</li> <li>重点力峭</li> <li>重点大小峭</li> <li>重点大小峭</li> <li>重点大小峭</li> <li>重点大小峭</li> <li>三方公石房旁边的小区</li> <li>現着物助定房号</li> <li>必吧</li> <li>野马足球県乐部</li> <li>乌克兰hangk</li> <li>百度fanyi</li> <li>baidu</li> <li>其他</li> </ul> </li> </ul>	:	返回查询 导出报表
	排行		关键字		用户信息	đ.	搜索次数
	1		皇家马德里		192.168.1.1	32:4	4
	2		百度翻译		192.168.1.1	32:3	3
	3		重庆力帆		192.168.1.1	32:3	3
	4	重	夫公租房旁边的小区		192.168.1.1	32:3	3
	5		提前锁定房号		192.168.1.1	32:3	3
	显示:	5 ▼ 条 共10条			▲ 首页	《上─页 1 2 下─页 ▶	末页▶ 1 确定

æ ×

匹配规则

默认审计

默认审计

默认审计

默认审计

访问控制

允许

允许

允许

允许

|< 首页 ◀ 上--页 1 下--页 ▶ 末页 ▶ 1 确定

# 点击用户信息一列

点击搜索次数一列 Ξ 关键字搜索信息

关键字: 皇家马德里

用户名(IP)

1.132) /192.168.1.132(192.168.

1.132) /192.168.1.132(192.168. 1.132)

/192.168.1.132(192.168. 1.132)

显示: 10 ▼ 条

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

审计时间

2018-04-03 14:42:47 tieba.baidu.com/f?k...

2018-04-03 15:29:07 tieba.baidu.com/f?k...

2018-04-03 15:29:26 tieba.baidu.com/f?k...

/192.168.1.132(192.168. 2018-04-03 14:42:44 tieba.baidu.com/f?k...

网页地址

具体应用

百度贴吧

百度贴吧

百度贴吧

百度贴吧

搜索类别

社交网页

社交网页

社交网页

社交网页

搜索内容

皇家马德里

皇家马德里

皇家马德里

皇家马德里

			r ×
关键字: 皇家马德里   统计日期: 2018-04-03 00	2:00 到 2018-04-03 23:59	/192.168.1.132	
排行	用户名 (组/名)	IP地址	捜索次数
1	/192.168.1.132	192.168.1.132	4
显示: 5 ▼ 条 共1条		【 首页	《上→页 1 下→页 ▶ 末页 ▶ 1 确定

# 1.3.7.5.7 论坛发帖

	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	T			
	显示TOP: 10		T			
	用户类型: 🖲 本	地用户				
	选择用户: 所有	用户 ▼				
	统计周期: 天		T			
	选择时间: 2018	-04-03				
	ক	靛查询				
200-00	查询					
누 위원자들	And Page					
点击 44.00 显示排行: 1	Top10   统计日期: 2018-04-	03 00:00 到 2018-04-03	23:59   用户: 所有用	≐ ■ 192.168.1.132		返回查询 导出报表
点击 ————————————————————————————————————	Top10   統计日期: 2018-04-	03 00:00 到 2018-04-03	23:59   用户: 所有用	는 		返回查询 导出报表
	Top10   统计日期: 2018-04-	03 00:00 到 2018-04-03	23:59   用户: 所有用	≐ ■192.168.1.132		返回查询 导出报表
点击 州北	Top10   统计日期: 2018-04-	03 00:00 到 2018-04-03	23:59   用户: 所有用	≐ ■192.168.1.132		<u>返回查询</u> 导出报表
点击 *****	Top10   统计日期: 2018-04-	03 00:00 到 2018-04-03	23:59   用户: 所有用	 		返回查询 导出报表
点击 出た 显示排行: 1	Top10   统计日期: 2018-04- 用户名 192168.1.132	03 00:00 到 2018-04-03	23:59   用户: 所有用	□ □ □ □ □ 192.168.1.132 发帖统计 天涯论坛发融:6 百度	味吧回复:1	<u>返回査询</u> 导出报表 <u> 友帖次数</u> 7

## 点击发帖统计一列



### 点击发帖次数一列

|--|--|

r ×

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	发贴标题/内容	访问控制	匹配规则
/192.168.1.132(192.168. 1.132)	2018-04-03 15:28:44	https://tieba.baidu.c	百度贴吧回复	192.168.1.132 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─页 1 下─页 》	萩♪▶ 1 确

# 1.3.7.5.8 外发文件

报表配置	搜索引载	肇 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				
点击		确定查询				
显示形行: lop10	统计日期: 2013	8-04-03 00:00 到 2018-04-03 2:	3:59   用户: 所有用户	192.168.1.132	赵	回查询 寻出报表
排行	用户名	IP地址		外发文件统计		外发次数
1	192.168.1.132	192.168.1.132		天涯论坛发图片:1		1
显示: 5 ▼ 条 共1約	N.			▲ 首页 《	上—页 1 下—页 ▶ 末	须▶ 1 确定

点击外发文件统计一列



### 点击外发次数一列

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	匹西起见则
/192.168.1.132(192.168.     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							默认审计
显示 10 · 余 Ⅰ(首页 《上页 1 下页 》 末页 Ⅰ 1 4							

# 1.3.7.5.9 网站分类

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		T			
	选择时间: 2018	3-04-03				
	ą	<del>〕 角定直</del> 询				

朝	定查询								
因表配置	搜索引擎	论坛发帖	外发文件	网站分类	网站域名	虚拟身份			
	显示排行	テ: Top10   统计	日期: 2018-04-03	3 00:00 到 2018-0	4-03 23:59   月	沪: 所有用户		返回查询	导出报表
							192.168.1.132		
	排行	用户	名	IP地址			网站分类统计		访问总数
	1	192.168	.1.132	192.168.1.	132	音乐:455,	搜索引擎:137,未知分类:130,其他:389		1111
	显示: 5	▼ 条 共1条					《 首页 《 上—页 1 下—	页▶ 末页▶	1 确定

### 点击网站分类统计一列



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



排行	网站分类统计	访问总数
1	音乐	455
2	搜索引擎	137
3	未知分类	130
4	裔业	82
5	IT类	66
显示: 5 ▼ 条 共25条	ŀ	(首页 《 上—页 1 2 3 4 5 下—页 ▶ 末页 ▶ 1 确定

点击访问总数一列

用户名: 192.168.1.132

r ×

统计日期: 2018-04-03 00:00 到 2018-04-0	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			I《首页 《 上─页 <b>1</b> 2 3 4 5 6 7 8	3 9 10 下—页 ▶ 末页 ▶ 1 确定

# 1.3.7.5.10网站域名

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: ④	》本地用户				
	选择用户: 月	所有用户 ▼				
	统计周期:	天	¥			
	选择时间: 2	2018-04-03				
	_ 1	确定查询				
<u>确定</u> 查询 点击						

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		
	显示排行	<del>ī</del> : Top10   统计	日期: 2018-04-03	3 00:00 到 2018-0	4-03 23:59   用	户: 所有用户	返回查询 192.168.1.132	导出报表
	排行	用户	名	IP地址			域名统计	访问总数
	1	192.168	3.1.132	192.168.1.	132 https://	y.qq.com:247,htt	p://c.y.qq.com:202,https://baidu.com:110,其他:552	1111
	显示: 5	▼ 条 共1条					《首页 《 上─页 1 下─页 》 末页	1 确定

### 点击域名统计一列

■ 用户 (192.168.1.132) 网站域名排行		~ ×
用户名: 192.168.1.132   统计日期: 2018-04-03 00:00 到 2018-0	04-03 23:59	
排行	域名	访问总数
1	https://y.qq.com	247
2	http://c.y.qq.com	202
3	https://baidu.com	110
4	https://ruijie.com.cn	55
5	https://ltsws.qq.com	30
显示: 5 ▼ 条 共189条		【《首页 《 上—页 1 2 3 4 5 下—页 ▶ 末页 ▶ 1 确定

点击访问总数一列

#### 📃 用户捜索信息

r ×

Ħ	护名:1	92.168.1.132			
纺	钻计日期:	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			I∜ 首页 ◀ 上─页 <b>1</b> 2 3 4 5 6 7 8	9 10 下页 ▶ 末页 ▶ 1 确定

# 1.3.7.5.11 虚拟身份

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	
	統计维度: 用户	排行	•				
	显示TOP: 10		T				
	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: 201	8-04-03					
	4	角定查询					
<u>确定者</u>	询						



### 点击应用类型统计一列

■ 用户 (192.168.1.132) 应用类型排行		e ×
用户名: 192.168.1.132   统计日期: 2018-04-03 00:00 到 2018-	04-03 23:59 - 海里天猫 - 百度始吧 - 方东南城VID - 天涯社区 - 去鄉J,VID - 新浪做埠VID - 新浪做埠VID - 新浪做埠VID	
排行	应用类型	访问总数
1	淘宝 天猫	24
2	百度贴吧	16
3	京东商城VID	8
4	天涯论坛	6
5	天涯社区	4
显示 5 • 条 共8条		〈 首页 《 上─页 】 2 下─页 ▶ 末页 ▶ 1 <b>确定</b> ·

点击访问总数一列

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(192.16 8.1.132)	2018-04-03 10:05:35	新浪邮箱			1517133649171_6860 1297	LOGIN	允许	默认审计
/192.168.1.132(192.16 8.1.132)	2018-04-03 10:52:33	淘宝 天猫			taobao.com	LOGIN	允许	默认审计
/192.168.1.132(192.16 8.1.132)	2018-04-03 10:59:08	去哪儿VID	pedjpbv3527	Rainman_%E9%9B%A 8		LOGIN	允许	默认审计
/192.168.1.132(192.16 8.1.132)	2018-04-03 11:02:35	淘宝 天猫			taobao.com	LOGOUT	允许	默认审计
/192.168.1.132(192.16 8.1.132)	2018-04-03 11:09:03	淘宝 天猫			taobao.com	LOGIN	允许	默认审计
/192.168.1.132(192.16 8.1.132)	2018-04-03 11:16:23	新浪微博VID			weibo.com	LOGIN	允许	默认审计
/192.168.1.132(192.16 8.1.132)	2018-04-03 11:18:05	去哪儿VID	pedjpbv3527	Rainman_%E9%9B%A 8		LOGOUT	允许	默认审计
/192.168.1.132(192.16 8.1.132)	2018-04-03 11:26:26	新浪微博VID			weibo.com	LOGOUT	允许	默认审计
/192.168.1.132(192.16 8.1.132)	2018-04-03 11:32:08	淘宝 天猫			taobao.com	LOGOUT	允许	默认审计
/192.168.1.132(192.16 8.1.132)	2018-04-03 11:45:43	京东商城VID			jd.com	LOGIN	允许	默认审计
显示: 10 ▼ 条					∢ 首页	▲ 上—页 1 2 3 4	5 6 7 下—页 🕨 末页	[】 1 确定

### 1.3.7.6 对象定义

### 对象定义配置页面:

流量监控	自定义应用分组	自定义网站分组	时间对象	外网IP对象	关键李组对象	VLAN对象	IP对象		(?) 帮助
流注策增	十添加应用分组 十目定》	2应用 🔛 反馈无法	尼别的应用						
行为审计报表	应用分组名称					选择应用			管理
1-1-1-1	关键/保证类	普通网页浏览,D	NS,HTTPS,即时通	用软件,IP网络电话	电子邮件协议,普通网	页浏览明细,ICMP-D	NETAIL,安全协议,VF	N应用,办公OA,視频会议	編編
132034048	抑制类	WEB应用,HTTP _MOBILE,网盘	下载,HTTP上传,H MOBILE	ITTP视话,未知网页	网络游戏软件,视频流动	集体软件,P2P应用载	(件,网络硬盘,视须属	影音_MOBILE,下载工具_MOBILE,社交	编辑
均衡定义	阻断类	ali法DNS,ali法9	的页						編輯
	普通/其他类	HTTP协议,股票 _MOBILE,网购	软件,互联网文件很 _MOBILE,证券_M	轴,数据库,网络管理 OBILE,网上支付[网	動议,路由协议,远程。 上银行_MOBILE,阅读_	方间协议,软件更新, MOBILE,RFC,IP-R	网银,即时通讯_MOI AW,IP协议组,微博	BILE ,游戏_MOBILE ,WEB_MOBILE ,姚伯	1918
	堂示 10 •							1(前页 (上一页 1 下一页) 末页	1 and

# 1.3.7.6.1 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	外网IP对象	关键字组对象	VLAN对象	IP对象		? 帮助
十添加应用分组 十自	目定义应用 📮 反馈无法	识别的应用						
应用分组名称					选择应用			管理
关键/保证类	普通网页浏览,[	ONS,HTTPS,即时通	讯软件 ,IP网络电话	电子邮件协议 ,普通网	页浏览明细 ,ICMP-[	)ETAIL,安全协i	义,VPN应用,办公OA,视频会议	编辑
抑制类	WEB应用,HTTI _MOBILE ,网盘	P下载 ,HTTP上传 ,I _MOBILE	HTTP视频 ,未知网页,	网络游戏软件 ,视频流	媒体软件 ,P2P应用转	吹件,网络硬盘,褚	见频 影音_MOBILE,下载工具_MOBILE,社交	编辑
阻断类	非法DNS,非法	类网页						编辑
普通/其他类	HTTP协议,股票 _MOBILE ,网购	软件 ,互联网文件( I_MOBILE ,证券_M	特新,数据库,网络管理 OBILE,网上支付 网.	里协议 ,路由协议 ,远程 上银行_MOBILE ,阅读_	访问协议 ,软件更新 , _MOBILE ,RFC ,IP-R	网银 ,即时通讯, AW ,IP协议组 ,	_MOBILE ,游戏_MOBILE ,WEB_MOBILE ,其他 微博	编辑
显示: 10 🔻							▶ 首页 《上一页 <b>1</b> 下一页 》 末页	▶ 1 确定

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。

r ×

### • 应用分组

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

4. 新增自定义应用分组:

点击 十添加应用分组 按钮可以自定义应用分组:

── 添加自定义应用分组	×
应用组名:	
已选应用:【添加应用】	
应用名称	操作
<b>应用名称</b> 【▲首页 ▲上一页 <b>1</b> 下一页 ▶ 末页 】	操作 1 确定

在"应用组名"输入框中输入应用分组名称,点击【添加应用】按钮:



➡ 添加自定义应用分组	×
应用组名:流量控制 ×	
已选应用:【添加应用】	
应用名称	操作
IP网络电话	删除
即时通讯软件	删除
《首页 《上─页 1 下─页 》末页 ▶ [	1 确定
	保存

点击

按钮可以将某个应用从该应用分组中删除。

点击 保存

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

### +添加应用分组 +自定义应用 ₽反馈无法识别的应用

应用分组名称	选择应用	管理
关键/保证类	即时通讯软件,IP网络电话,电子邮件协议,普通网页浏览,普通网页浏览明细,DNS,ICMP-DETAIL,安全协议,VPN应用,办公OA,视频会议,HTTPS	编辑
抑制类	网络游戏软件,视频流媒体软件,P2P应用软件,WEB应用,HTTP下载,HTTP上传,网络硬盘,HTTP视频,视频影音_MOBILE,下载工具_MOBILE,社交_MOBILE,网盘_MOBILE,未知网页	编辑
阻断类	非法DNS,非法类网页,股票软件	编辑
普通/其他类	HTTP游戏,互联网文件传输,数据库,网络管理协议,路由协议,远程访问协议,软件更新,网银,即时通讯, _MOBILE,游戏_MOBILE,WEB_MOBILE,其他_MOBILE,网购_MOBILE,证券_MOBILE,网上支付 网上 银行_MOBILE,微博,RFC,IP-RAW,IP协议组	编辑
流量控制	即时通讯软件,IP网络电话	编辑删除
	【首页 《上─页 1 下─页》末页	▶ 1 确定

### 5. 编辑应用分组:

点击自定义应用分组主页面表格中的 建铵钮可以重新分配某个应用分组包含的应用:

ר ובנונאנינאאגזוטיגאנאן 🦇 רו בניאבאר   דא געוו בניאואנאאן							
── 编辑自定义应用分组	×						
应用组名: 流量控制							
已选应用:【添加应用】							
应用名称	操作						
股票软件	删除						
P2P应用软件	删除						
视频流媒体软件	删除						
IP网络电话	删除						
即时通讯软件	删除						
【●首页 ●上一页 1 下一页 ▶ 末页 ▶ [	1 确定						
	保存						

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

点击【添加应用】按钮将弹出以下窗口:



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

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

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

6. 删除应用分组:

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

#### 自定义应用

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

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

★ 自定义应用 按钮将弹出自定义应用配置窗口:

🥝 创建自定义应用 -	Internet Explorer		-				_ <b>_</b> ×	
R http://172.18.12	http://172.18.124.72/object_pi/bw_setobj_appauto.htm							
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	R :							
协议类型	协议类型: TCP → 规则类型: 源IP+目的IP →							
应用所属分类	应用所属分类: ⑧ 自定义分类 ○ 从已有分类选择:							
源Ip	): 輸入ip 🗸	•		8				
目的Ip	): 輸入ip 🗸	•		0				
	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	
test	tcp	网络管理协议	所有端口	所有端口	1.2.4.4	20.2.0.47	编辑删除	
				▲首页 ▲_	上一页 1 下	一页 ▶ 末页 ▶	1 确定	

创建自定义应用对象:输入自定义应用名称、选择协议类型、选择规则类型、应用所属分类(可以自己另外定义应用分类, 也可以基于内建应用分类)、根据选择的规则类型输入源或目的端口、源或目的 IP,点击 添加设置 配置成功。 编辑自定义应用:选择需要修改的应用,点击 编辑 按钮即可修改。 删除自定义应用:选择需要删除的应用,点击 即可。

• 反馈无法识别的应用

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



# 1.3.7.6.2 自定义网站分组

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

自定义应用分组 自定义网站分组 时间	司对象	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			管理						
ddd	病毒木马,赌博,暴力	编辑删除							
aaa	礼	视频,音乐,游戏,文学	编辑删除						
keyObject	k	keyUrlClass,门户区	编辑删除						
un_audit_object	笔	软件升级,脚本未知	编辑删除						
illegal	f	forbidClass,视频,音乐,游戏,文学小说,在线聊天,娱乐 编辑 删							
★ 首页 《 上一页 <b>1</b> 下一页 》 末页 ) <b>1</b> 确定									

#### ● 网站分组

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

1. 新增自定义网站分组:

点击 十添加网站分组 按钮可以自定义网站分组:



Я	点击自定义网站分组主页面表格中的	₽ 按	冠田可以重新分配某个网站分组包含的网站类:
	── 编辑网站分组	×	
	网站分组名: text		
	- 🗀 🗌 所有分类	~	
	- 🗀 🗹 常用热门网站		
	▶ ☑ 门户网站与导航		
	⑦ 2 搜索引擎		
	▶ 🗹 网络		
	Image: Web Image:		
	≥☑微博客	$\sim$	
	 保存	1	
2	勾选需要包含的网站类,取消不需要包含的	]网站	类 , 点击 保存 按钮即可。
3	3. 删除网站分组:		
万	点击自定义网站分组主页面表格中的	余按	钮可以删除选中的网站分组。

### • 自定义网站类

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

点击自定义网站分组主页面的 ⁽²⁾ 自定义网站类 按钮将弹出自定义网站类配置窗口:

🥑 创建自定义网站类 - 1	Internet Explorer		
R http://172.18.124.7	72/object_pi/action_class_web1.htm		
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/summ	ary.aspx	
			×
	添加设置		
自定义网站分类列	山表		
网站类名	网址	类型描述	操作
un_audit_class	baidu.com, tmall.com, jd.com	unaudit	编辑删除
forbidClass	ui.tudou.com, youku.com		编辑删除
	▲首页 《上一页	〔1 下─页▶	末页 ▶ 1 确定
建自定义网站类:	输入自定义网站类名称,输入能够标识该网站类的意图	或用户的描述信息	
域名 (多个域名)	人","隔开),点击	多允许配置 100 ·	个自定义网站类。



# 1.3.7.6.3 时间对象

可以定义时间对象,用于策略设置时候使用。

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	: 时间对象用于定	义策略生效时间。						
十添加	十添加时间对象 X删除选中时间对象							
	By	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E 毎天	3	0:00-5:59 18:01-23:59		编辑删除	
	न	班时间	工作日 工作日 工作日	3 3 3	0:00-7:59 12:00-13:00 18:01-23:59		编辑删除	
		周末	周末		0:00-23:59		编辑删除	
	F	班时间	工作E 工作E	3	8:00-12:00 13:00-18:00		编辑删除	
	]	E作日	工作日		0:00-23:59		编辑删除	
显示:	10 ▶ 条 共7会	<u>k</u>			▲首页 ◀	上—页 <b>1</b> 下—页	▶ 末页 ▶ 1	确定

5. 添加时间对象:点击 十添加时间对象,在弹出窗中输入对象名称,选择时间段,支持设置多个时间段。

例如新建一个 工作时间 对象:

(5)	对象名称:在对象名称	对象名:	* 输入时间对象名称;
(6)	时间段周期:选择时间	段的周期,即选择每周从周一到周日	
时间段:	<ul> <li>清选择</li> <li>↓ 星期一</li> <li>▲ 里期二</li> <li>↓ 星期三</li> <li>↓ 星期四</li> </ul>	开始时间 ~ 结束时间 X 完成配置	
		13:00-18:00	
(7)	时间段:设置时间段		

时间段:	星期一,星期二	开始时间	~	结束时间		k
		 00~时00~	23	分确定	关闭	

(8) 点击添加另一个时间段

时间	一 単 単 一 , 星 期 二 ▼ 00 星 期 一 , 星 期 二 ▼ 00 星 期 一 , 星 期 二 ▼ 开 テ 成 配 置 古 土      ☆ 次 1	11:00 ~ 11:00 × 始时间 ~ 结束时间 ×	十添加						
フロルメル		1110月111111111111111111111111111111111							
十添加	如时间对象 X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 毎天	0:00-5:59 18:01-23:59	编辑删除					
	test	星期一 星期二	0:00-11:00	编辑删除					
	test2	星期一 星期二	0:00-11:00	编辑删除					
	下班时间	工作日 工作日 工作日	0:00-7:59 12:00-13:00 18:01-23:59	编辑删除					
	周末	周末	0:00-23:59	编辑删除					
	上班时间	工作日 工作日	8:00-12:00 13:00-18:00	编辑删除					
	工作日	工作日	0:00-23:59	编辑删除					
显示	☆10 ∨ 条 共9条		《 首页 《 上—页 1	下一页 ▶ 末页 ▶ 1 确定					
6. 7. 8.	显示 10 ▼ 条 共9条       N 首页 4 上→页 1 下→页 ▶ 末页 N 1 毫定         6. 编辑时间对象:选择需要编辑的时间对象点击       编辑         按钮,在弹出窗中即可添加,删除,修改对应的时间段。         7. 删除时间对象:若需要某个时间对象,在列表中选择该时间对象,点击       按钮即可。         8. 删除时间段:若需要删除某个时间对象的某个时间段,在列表中选择对应的时间对象,点击编辑在弹出窗中选择需要删除的时间段,点击 × 按钮,可以删除某个时间段。								

时间段:	星期一,星期二,星期▼	0:00	~	5:59	×	
	星期一,星期二,星期▼	18:01	~	23:59	×	

# 1.3.7.6.4 关键字组对象

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

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
十新建关键字组						
关键字组名称			关键	Ż		管理
web_block_im	235345457					编辑 删除
web_block_mail	80670523@qq.c	om				编辑删除
				▲首页 ▲上		▶ 末页 ▶ 1 确定





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



删除关键字组:在关键字组对象主页面的表格中,选中需要编辑的关键字组,点击

# 1.3.8 加速

### 1.3.8.1 线路捆绑

#### • 配置向导

首次配置线路捆绑,配置页面如下图所示



点击"开始配置"按钮开始线路捆绑配置,进入如下页面:

📃 欢迎使用线路捆绑配置向导 , 本向导将	帮您快速完成线路捆绑配置。	×
青选择设备在网络中的位置:		/ 选择设备位置
		2 配置总部资源
<ul> <li>总部(服务器所在网络)</li> <li>建立加速的业务资源,供连接使用。</li> </ul>		3 完成配置
<ul> <li>小又</li> <li>需要访问服务资源的网络。</li> </ul>		
	±–	步下一步

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

● 总部配置

在上图的"网络位置"配置	置页面中勾选"总部"类型的线路捆绑设置之后,点音	志左下角的 <mark>下一步</mark>	安钮 , 进入如下页面:
📃 欢迎使用线路捆绑配置	置向导,本向导将帮您快速完成线路捆绑配置。	×	
。 设置分支接入的验证码:	*	/ 选择设备位置	
	请输入31位内的字符(中文占两个字符),且不能包含空格。	2 配置总部资源	
需加速的业务资源:	地址:     ×     +添加       地址:     ×     ×	3 完成配置	
h			
		┟──步    下──步	

设置分支接入验证码,当分支通过线路捆绑接入总部时,需要输入该验证码进行验证

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

然后点击"下一步",进入下一个配置界面

📃 欢迎使用线路捆绑配置向导,本向导将帮您快速完成线路捆绑配置。	×
总部的加速部署配置完成,请使用以下地址指导分支进行配置:	/ 选择设备位置
分支连接总部的验证码为:ruijie	2 配置总部资源
总部地址(使用任意一个即可): 其它运营商	3 完成配置
^{地址1:172.18.124.54} <del>月存到本地PC</del> ← 可以将以上 本地信息保存到本地文本中 忘记配置信息时,可以查看保存的文本	
Ŀ	步 完成

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

点击"完成",完成线路捆绑配置

• 分支机构配置

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

☰ 欢迎@	使用线路捆绑面	2置向导,本向导将帮您快速完成	成线路捆绑配置。		×
填写总部地	址建立加速连持	<b>妾:</b> 请向总部管理员索要总部网头	关地址和验证码		/ 选择设备位置
	总部IP地址:	172.1.20.5	*		2 连接总部
	验证码:	为获得最好效果,建议填写与本情	机相同的运营商线路地址。		3 完成配置
	本机构名称:	Ruijie	*		
			1		
				F1E	T-45

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

📃 欢迎使用线路捆绑配置向导,本向导将帮您快速完成线路捆绑配置。	×
	/ 选择设备位置
	2 连接总部
	3 完成配置
学长 正在连接总部	
Ŀ	步完成

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

# 1.3.8.1.1 加速状态

在总部模式下完成线路捆绑配置后,可看到如下页面



1. 当前加速实时情况



该页面显示当前加速上行实时加速情况:

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



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

- 你可以更改 上行加速状态 ❤ _{查看上下行的当前加速情况。}
- 2. 正在连接的分支



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

🧉 线路排	困绑 - Internet Explore	r							_ <b>_</b> ×	
R http:	://172.18.124.54/vwar	n_pi/vwan_state.htm								_
ruij	jie / 上行累计传输	流量: OB / 下行累	计传输流量: 0	В						^
1	最近60秒带宽走势	丢包走势								
1.0										
0.8										
0.6										
0.4										
0.2										
0.0	5	10 15	20	25 30 ■上行速度 ■	35 下行速度	40	45	50 55	60	
									``	~

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

3. 正在加速的业务系统

正在加速的业务系统(0) 上行 >						
📒 普通网页浏览	业务名称	上行流量	下行流量			
	普通网页浏览	2.23KB	0.23KB			
<b>金玉田高大時時</b> , 2017/500/1						
百進門央网亮. 3.04K8pS(100%)						

该页面显示了目前正在加速的业务:

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

# 1.3.8.1.2 加速设置

### • 总部模式加速设置

### 以下是当设备为总部模式时候下的设置页面

加速状态加速配置							
加速业务设置							
业务资源地址: 172.18.124.0		×	十添加				
业务资源地址: 192.168.1.0	业务资源地址: 192.168.1.0						
加速连接设置							
用于加速的外网线路		端口	状态	操作			
✓ Gi0/6(其它 100M 已上	☑ Gi0/6(其它 100M 已上电)		连接已建立,加速中	1/2-74			
Gi0/7(其它 1000M 不可	用)		未开启	19 DX			
注意:建议不要使用拨号口做加速线	锴,拨号口望	重连后外网IP会改多	变,从而分支必需更改连接起	总部的IP,否则无法成功接入。			
加速状态							
当前状态:	运行中			关闭			
分支连接总部的验证码:			修改				
高级配置	高级配置						
丢包恢复处理:	<b>丢包恢复处理:</b> ▼开启丢包恢复处理 修改						

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

**加速连接设置**:可以开启或关闭用于加速的外网线路,开启时要填写相关的端口号,默认情况下可以使用默认值 **加速状态**:可以对于运行中的线路捆绑业务关闭,关闭后将影响接入总部的分支,关闭时候有两种模式可以选择,如下图:

🧮 请选择当前配置处理方式。	×
在设备上保留配置,暂时关闭该功能	
清空配置,关闭功能	
	取消
一种是暂时关闭该功能,但在设备上还保留着配置,另一种是完全关闭,关闭后还会删除配置。可以设置新的分支连接总部 验证码,修改完成后建议及时通知分支修改连接总部验的证码

高级配置:可以开启或关闭丢包恢复处理。

#### • 分支模式加速设置

以下是当设备为分支模式时候下的设置页面

加速状态加速配置						
基本参数						
当前〉	状态:	加速	中			关闭
连接总部的验证码:			e	*		修改
本机构	名称:	ruiji	e	*		修改
加速连接设置						
用于加速的外网线路	媏		要连接的总部IP和	端口	连接状态	操作
☑ Gi0/1(其它 10M 已上电)	123	315	172.18.124.54 : 1	12315	连接已建立,加速中	
☑ Gi0/1.1(其它 10M 已上电)	123	315	172.18.124.54	12315	主动连接,正在协商	1/42-21/7
☑ Di1(其它 1000M 已上电)	123	315	172.18.124.54	12315	空闲,初始状态	19 LX
Gi0/3(其它 1000M 不可用)			未开启			
高级配置						
<b>丢包恢复处理:</b> 开启丢包恢复处理 🎯						1427br
加速网段	配置:	□ 开	后加速网段配置 🖓			修改

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

📃 请进	战争当前配置处理方式。	×
	在设备上保留配置,暂时关闭该功能	
	清空配置,关闭功能	
re e		取消

一种是暂时关闭该功能,但在设备上还保留着配置,另一种是完全关闭,关闭后还会删除配置。当总部修改了分支接入验证 码时,可以通过修改,填写新的验证码。还可以修改本机构名称 加速连接设置:可以开启或关闭用于加速的外网线路,开启时要填写相关的端口号,默认情况下可以使用默认值,同时还要 填写要连接到总部的 IP 和端口

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

#### 高级配置

丢包恢复处理:	□开	启丢包恢复处理	0	
加速网段配置:	☑开	启加速网段配置	0	
本地网段			总部网段	+
1.22.2.2 255.255.255	255	12.2.22.2	255.255.255.255	删除
5.2.2.2 255.255.255	255	12.2.22.3	255.255.255.255	删除

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

### 1.3.8.2 应用缓存

Web 提供应用缓存的配置界面,如下图

应用缓存							
<b>说明:</b> 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	援存: ON		【最近缓存详情】				
应用缓存容量	き (已使用: <i>08</i> , 总容量	量: <i>100.00GB</i> )	硬盘容量 (未使用: <b>4</b> 4	<i>13469.57MB</i> , 总容量:	469452.20MB)		
应用选择							
手机应用:	✔ 苹果应用	☑ 安卓应用					
办公应用:	☑ 微软补丁	☑ 360安全卫:	土系统补丁	腾讯电脑管家			
自定义类型:			多个请用" "号隔开	F, 例: ipa apk			
自定义特征:			多个请用" "号隔开	F, 例: windowsup	odate 360safe		
文件类型:	ipa apk exe msi n	nsu cab zip					
URL特征:	windowsupdate	Windows micros	oft 360safe				
		保存设置	删除全部				

## 应用服务器地址

	□ 全部HTTP (端口)	]80)	
	地址1:	* × 删除	十添加
		保存设置删除全部	
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:	* ×删除	十添加
		保存设置 删除全部	
缓存指定	应用-时间窗 💡		
	地址1:	* ×删除	十添加
		保存设置删除全部	

# 1.3.9 安全

# 1.3.9.1 本地防攻击

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

进入防攻击设置页面,如下图所示:

本地防攻击
ARP欺骗检测:□检测内网ARP攻击 ^②
查看ARP嫌疑列表: 【ARP欺骗嫌疑列表】
防流量攻击:□开启防流量攻击 ?
攻击流日志: 【当前的攻击日志】 【历史的攻击日志】
禁止ping:□禁止內网ping设备 □禁止外网ping设备
禁止ssh telnet: 🗏 禁止内网ssh telnet 🛛 🗏 禁止外网ssh telnet
禁止snmp管理: ■禁止内网snmp管理 ■禁止外网snmp管理
禁止web登录:■禁止内网登录设备web系统  ■禁止外网登录设备web系统
web访问端口: 80 (80,1025-65535)默认为80
<b>保存设置</b> 恢复默认设置

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

1. 防 ARP 攻击

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

防 ARP 流量攻击:通过启用 IFF 后防ARP流量攻击 可以对到达本地的 ARP 流量配置限速,设备每秒处理的 ARP 报文不超过 10 个,多余 ARP 报文将被过滤掉。

防 ARP 欺骗:通过启用 ^{IIII}防主机对整网ARP扫描 可以防止黑客窃听到网内所有的 (IP, MAC)地址, 伪装成网内的某台 PC 进行 ARP 欺骗。

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

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

2. 防流量攻击

防流量攻击: 启用 🗹 开启防流量攻击 , 防送进程的报文超过阀值就丢包 , 每秒平均 200 个 , 突发允许 300 个。

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

3. 其他防攻击

禁止 web 登录:通过启用 🗹 禁止内网登录设备 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。

添加管理 IP:这里输入的 Ip 地址 是管理员的 IP,也就是不受流量限速影响的 IP 地址,主要是为了提高管理员管理设备的

(更多) 效率。点击 更方便查看和管理:

🥝 防攻击-配置管理	IP - Internet Explorer	
R http://172.18.1	24.54/anti_attack_pi/safe_att_user.htm	
<b>说明: 管理IP</b> 類 则此IP可以正常到	書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"; 登录web,其他功能点也是类似。最多添加32个条目(IP或IP段)!	为管理IP,
管理IP地址:	添加设置	
	管理IP地址	操作
	125.36.36.5	
	▲首页 《上一页 1 下一页》 末页 >	1 确定

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

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

# 1.3.9.2 接口访问控制

接口	接口访问控制 ? 帮助								
说明 反射。	说明:此功能是将ACL应用于接口,以实现防火墙的功能。 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回来进入网络。 ╋ 添加接口访问控制 ★删除选中策略								
	ACL号         应用于接口         过滤方向         反射ACL         操作								
	□ 12 II Gi0/0 收报文(in) 关闭 删除								
显示:	显示: 10 ♥ 条共1条								

点击 十添加接口访问控制 在弹出窗中选择 ACL 列表号匹配到一个接口,设置报文过滤方向(in or out)点击

完成配置

按钮就可以生成一条访问控制列表,起到防火墙的作用。

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

Í	📃 添加接口访问控制		×
	ACL列表:	12 ~	
-	应用于接口:	Gi0/0 ~	
	过滤方向:	收报文(in)	
	反射ACL:	☑开启	
			完成配置 取消

# 1.3.9.3 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EG设备上面,请确认PC网关地址所对应的设备并在对应设备绑定ARP)。 <b>说明:</b> 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。								
<b>唱</b> 一键绑定	由一键绑定 點 动态>>静态绑定 \$ 静态绑定 \$ 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地址查询: 查询							
	IP地址	\$	MAC类型	类型	备注			
			无记录值	息				
显示: 10 •	条 共0条			「首	顶 《 上─页 下─页 》 末页 № 1 <b>确定</b>			

添加了禁止未静态绑定的内网主机通过选项。

ARP表项					
<b>注意: 跨三层</b> <b>说明: 静</b> 态绑	邵支持ARP绑定(跨三层是指PC的P 定的效果:一个MAC可以对应多个I	网关不在EG设备上面,请确认PC IP,但是一个IP只能对应一个MA(	网关地址所对应的设备并在对应设备绑定ARP C,如果修改为除静态表项里的其他IP可以正常	)。 3上网,如果修改MAC则无法正常上网。	
a一键绑定 品动态>>静态绑定 【 静态绑定 】 静态绑定 目 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地址查询:					
	IP地址	*	MAC类型	类型	备注
			无记录信	₿.	
显示: 10 🔹	条 共0条			[4 首	顶 《上一页 下一页》 末页》 1 确定
RP功能设置	2				
停止ARP学习 免费ARP请求	: 将只允许静态绑定MAC的PC上网 : 网关会定期向局域网PC通告自己的	,但对应接口的源进源出功能需要 的IP-MAC地址,避免内网PC被AB	要关闭。 RP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ARF	2学习:┏ Gi0/0 🔲 Ag1				
开启免费ARF	⊃请求: 🗹 Gi0/0 🔲 Ag1				
	保存设置				

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

绑定。点击 5 手工静态绑定 弹出窗口如下:

单用户手工绑定

IP地址:			
MAC地址:		(女	: 00d0.f86b.dcbe)
备注:			
		//	
	保存设置		

#### 批量用户手工绑定

	<b>说明:</b> 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。	e
	选择接口:	
	开始扫描	
单	引户手工绑定:只需输入 IP 地址和 MAC 地址,点击  保存设置  即可。	

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

2. ARP 表项

	IP地址 🌲	MAC类型	类型	备注	
	2.3.3.3	00d0.f86b.dcbe	静态绑定	aaa	
显示	〒10 ▼ 条 共1条		∢ 首页	《上一页 1 下一页 ▶ 末页 ▶ 1 确定	

即可。

以上表格显示了用户通过静态绑定或系统动态绑定的 IP/MAC 表项。

3. 删除静态绑定

在 ARP 表项中,选择需要删除的静态绑定的 IP/MAC 表项,点击

4. 将动态绑定转为静态绑定

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

5. ARP 功能设置

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

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

#### 1.3.9.4 ACL 访问列表

利用该功能可以配置 ACL 对象,用于提高网络安全配置时使用。如下图所示。

确定

ACL访问列表											
注意: 在配置ACL号时,由于web部分模块使用了特定的ACL号,例如:VPN模块使用了110和199,本地防攻击使用了2397、2388,VWAN使用了198,CLI下配置射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。											
ACL列表 添加 删除	ACL列表 添加 删除 十添加ACE规则 X 删除选中										
1		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
110		1	任意		允许				所有时间	生效	编辑 移动
2397 显示 10 ▼ 条共1条 K首页 《 上一页 1 下一页 》 末页 N 1 确定											

1. 添加 ACL:

375.60

点击	TORNU	按钮会弹出添加 ACL	弹出窗 , 选择 AC	L 的类型 :标准 ACL	(控制源地址)	或者扩展 ACL(	细化控制数据流),	
----	-------	-------------	-------------	---------------	---------	-----------	-----------	--

输入 ACL 列表的名称后点击

☰ 添加ACL	×
ACL类型:  ◎ 标准ACL (控制源	馳址 ) ── 扩展ACL(细化控制数据流 )
ACL列表:	* 支持中英文名称 数字 范围为(1-99, 1300-1999)
	确定取消

#### 2. 添加 ACL 规则

• 点击

╋ 小本市本部では「本本学生の中での「本本学生の中でのです」 → 本学出の中でので、 → 本学出の中でので、 → 本述ので、 → 本

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 梅定 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	访问控制规则 <b>小</b>
访问	控制: ⑧ 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P应用该规则) 单IP地址 ✓ 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	访问控制规则
访问控制: ○ 允许 ④ 禁止 协议: IP   ✔   生效时间: 白天     ✔	
□ 源IP地址任意:( ^{源P地址任意是对所有的源P应用该规则} )	: 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 単IP地址   IP地址: 1.2.2.5	0)
	确定取消



源地址和目的 lp 地址中有一个地址类型选择

单 IP 地址: 输入源或目的地址的单个 IP 地址;

掩码设置: 输入源或目的地址的 IP 地址段, 以掩码方式的地址段;

通配符: 输入源或目的地址的 IP 地址段, 是以通配符的方式输入地址段的。

## 3. ACL 访问控制列表

	序号	源IP/通配符	源端口	访问控制	协议	目的IP/通配符	目的端口	生效时间	状态	操作	
	1	任意		允许				所有时间	生效	编辑 移动	
	2	12.12.5.5/0.0.0. 0		允许				晚上	生效	编辑 移动	
显示	显示: 10 ♥ 条共2条										

点击 移动 按钮可以调整 ACL 规则顺序。

点击 编辑 可以对选中的 ACL 规则进行编辑。

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

### 防共享接入

一键防共享	防共享策略	实时监测状态					
说明:一键防共享	开启后,会下发预定)	义的配置。					
注意: 开启一键防	5共享后,配置共享的	1所有本地用户不能上网。 🗄	关闭一键防共享后,防共享策时	婚都会被清空。 			
开启一键	1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 1115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115 - 115	关闭					
_							
键防共享	防共享策略	实时监测状态					
<b>说明:</b> 对指定的用户	与进行检测,发现用户	有共享行为后阻断用户上际	ଗ୍.				
注意: 防共享策略	最多配置100条。						
▶ 添加防共享策略	<b>X删</b> 除选中	🗹 自定义防共享标准	■ 防共享白名单				
	用户/用户组		认证用户	惩罚方式		状态	操作
				无记录信息			
記示: 10 ▼ 条 #	+0条				【▲首页 ▲ ト		1
							WALL
-键防共享	防共享策略	定时些测状态					
-键防共享	防共享策略	实时监测状态					
键防共享 中监测信息直询:	防共享策略 基于IP ▼	实时监测状态	查询				
键防共享 中监测信息查询: IP	防共享策略 基于IP ▼	实时监测状态 1 用户名	查询 认证用户	状态	间闭	终端信息	操作
·键防共享 户监测信息直询: IP	防共享策略 基于IP ▼	实时监测状态           1           用户名	前	状态	时间	终端信息	操作
-键防共享 户监测信息直询: IP	防共享策略 <b>基于iP</b> ▼	实时监测状态 用户名	新 <mark>新</mark> 认证用户	状态	时间	终端信息	操作

## 1.3.9.5 连接数限制

通过该功能可以限制通过设备总会话数。全局会话数配置页面如下图所示:

全局会话数												
设备抗攻击												
<b>说明</b> : 防止内网用户异常攻击行为导致设备转发异常。												
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】【会话数攻击嫌疑歹	刊表】 ?									
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。									
十新建会话数策略 🔍 直看	冒每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	1000	生效		编辑删除					
显示: 10 ▼ 条 共1条				▲首页 《上一页	<b>1</b> 下-	─页 ▶ 末页	▶ 1 确定					

#### 添加了设备抗攻击的设置。

全局会话数	全局会话数												
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	十新建会话数策略 Ca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	1000	生效		编辑删除						
	▲首页 《上一页 1 下一页 》 末页 ▶ 1 确定												

#### 1. 新建会话数限制策略

点击 十新建会话数策略 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。

## 1) 基于用户的会话数限制策略:

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300	000的值
毎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
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	送话数的用户,点击 确定 周
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 ×	法数的用户,点击 确定 限
用户:点击 曲户选择 ■ ● 所有用户	, 在弹出的用户选择窗口上勾选需要限制会	会话数的用户,点击 确定 即
用户:点击 选择用户 ■ 用户选择 ■ ● 所有用户 ■ ● ○ weeb认证	, 在弹出的用户选择窗口上勾选需要限制会	法数的用户,点击 确定 即
用户:点击 选择用户 用户选择 ●●所有用户 ● ● ○web认证 ■ ● ○Vpn_Group	, 在弹出的用户选择窗口上勾选需要限制会	会话数的用户,点击 确定 即
第月户:点击 选择用户 ● 前行用户 ● ○ いからしいです。 ● ○ いからいです。 ● ○ いないのの ● ○ いないののの ● ○ いないのののののののののののののののののののののののののののののののののの	, 在弹出的用户选择窗口上勾选需要限制会	法数的用户 , 点击 确定 _即
用户:点击 选择用户 用户选择 ◎所有用户 + ○ ○web认证 - ○ Vpn_Group ◎ ○ lgh150 ◎ ○ fff	, 在弹出的用户选择窗口上勾选需要限制会	会话数的用户,点击 确定 即
第月户:点击 选择用户 ● 前方用户 ● ○ 所有用户 ● ○ web认证 ● ○ lgh150 ● ○ lgh150 ● ○ fff ● ○ vpn_euser_ ● ○ 22222	, 在弹出的用户选择窗口上勾选需要限制会	法透数的用户 , 点击 确定 _即
第月户:点击 选择用户 第月户选择 ● 所有用户 + ● ○ web认证 ● ○ lgh150 ● ○ lgh	, 在弹出的用户选择窗口上勾选需要限制会	法 一
使用户:点击 法择用户 ● 用户选择 ● ● 所有用户 ● ● いweb认证 ● ● Okpn_Group ● ● Okp150 ● ● ● Okp150 ● ● ● Okp150 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	,在弹出的用户选择窗口上勾选需要限制会	徐话数的用户 , 点击 确定 [

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

2) 基于 ACL 的会话数限制策略:

	制策略	$\times$				
限制类型: 〇 基于用户 ) ④ 基于ACL						
选择ACL号:	12 ¥ 【新建ACL访问控制列表】 (ACL关联范围1-199)					
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					
	完成配置					

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

#### 设置会话数 ≥ 设置会话数

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

#### 2. 会话数限制策略列表

限制类型	选择用户/ACL号	控制方式	最大总会话数	每IP最大会话数	状态	匹配顺序	管理
基于ACL	12 🔳	设置会话数	100000	λ	生效	-	编辑删除
基于用户	fff	阻断	λ	λ	生效	∲ 😽	编辑删除
基于用户	所有用户	设置会话数	100000	100	生效	Ŷ	编辑删除
				▲首页 ◆上一页	<b>1</b> 下-	─页▶ 末页	▶ 1 确定

以上表格列出了用户配置的所有会话数限制策略。

限制类型:指出本策略是基于 ACL, 还是基于用户。

状态:说明该策略当前是否生效。

会话数限制策略遵循"后配先生效"原则,点击"匹配顺序"栏的⁴、¹按钮可以调整策略优先级,您可以对现有策略的优先级进行调整。



3. 查看每 IP 流会话数情况

点击 合查看每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:

Ξ 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				
10.10.105	/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 <b>1</b> 下一页 ▶ 末页 ▶	1 确定				

#### 4、内网 UDP 会话数比例限制

.

+新建会话数策略 ፟
[●] 内网UDP会话数比例限制 L 查看每IP流会话数情况

:	一 内网UDP会话数比例限制	×
	<b>说明:</b> 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: 0 %( <i>30~80,0表示不限制udp</i> ,推荐值50%) 保存	

增加内网 UDP 会话数比例限制的配置,点击弹窗进行保存,如下图

注意:限制比例范围为 30-80,默认为不配置,即 0 表示不限制 udp

1.3.9.6 防共享接入

# 1.3.9.6.1 一键防共享

() 说明:一键防共享开启后,会下发预定义的配置。

# 1.3.9.6.2 防共享策略

#### $\mathbf{i}$

## 

一键防共享	防共享策略 实时监测状:	态历史检测日志				
<b>说明</b> :对指定的用户进行检测,发现用户有共享行为后阻断用户上网。						
上法加防共享	· · · · · · · · · · · · · · · · · · ·	客标准 国际共享白经单				
╋ 添加防共享	策略 X删除选中 C 自定义防共 用户/用户组	字标准 国防共享白名单	征留方式	状态	擾作	
	策略 X 删除选中 C 目定义防共 用户/用户组 所有用户	字标准 目 防共享白名单 认证用户 否	惩罚方式 限速上网	状态	操作	

#### 可以添加,删除,编辑策略,还提供自定义放共享标准及白名单配置

_ ------

名称	限制数量	状态	操作
微信	不限制	生效	清除
示: 10 ▼ 条 共1条	K	首页 《上一页 1 下一页 》 末页 》	1 确定

# 1.3.9.6.3 实时监测状态

一键防共享 防共享	策略 实时监测状态	历史检测日志					
用户监测信息查询: 基于IP ▼							
IP	用户名	认证用户	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	

## 可以基于 IP 和用户等类型查询

用户监测信息查询:	基于IP ▼	查询
	基于IP	
IP	基于用户	用户名
	用户类型	
	用户状态	

# 1.3.10 用户

1.3.10.1 用户组织

# 1.3.10.1.1用户管理

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

用户管理 导入导出用	白 特殊用户管理	理						
用户组织结构	组路行 关联行 ×删	<ul> <li>組路径: root 提作</li> <li>关联行为策略: 共1条 ① 策略直看</li> <li>X 删除 ピ 属性编辑</li> </ul>				搜索用户名 <b>v</b> 輸入用户名		
		名称	÷	IP地址(MAC地址) 无记	◆	VPN权限	行为策略明细	管理
	显示	: 10 ▼ 条 共0条				▲首页  ▲	上─页 下─页 ▶ 末页 ▶	1 确定

用户管理导入	入导出用户	特殊用户管	理							?帮助
用户组织结构 组路径: root/Vpn_Group				ᄱ 操作 ← 点击弹	出操作菜单	通过用	户名或者	TP查询已	配置的用户	
- 😂 root		关联行为策略:共1条 金策略查看							↓ ↓	
📮 web认证			×删	余 🗹 属性编辑 对	选中的用户进行批	量删除或批量编辑	搜索用户名 🗸			查询
Vpn_Group					名称	IP地址(MAC	地址) 🜲	VPN权限	行为策略明細	管理
	┿编辑 -	╋添加用户(段)	十添	加组 ×删除	i_euser_	无		√		编辑删除
	1				fff	查礼	看用户关联的	行为策略	→ 🗉	编辑删除
点击用	户组,会在  二:汝织玉秋	E右边的表			lgh150	无		√	<b></b>	编辑删除
旧中亚	格中显示该组下的用户,同 时会弹出快捷的操作按钮			:10 🗸 条 共3条		I	∢首页 《 上一页	<b>1</b> 下一页	▶ 末页 ▶	确定
								对相应	立的用户编	扁辑或者删除

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

用户组织结构	组路径: root/Vpn_Group 操作
- 😂 root	关联行为策略:共1条 、策略查看
🗀 web认证	★删除 ピ属性编辑
Vpn_Group	名称
十编辑 十添加用户(段) 十	添加组 X删除 vpn euser
<u>↑</u>	
点击用尸组,显示快捷采申	<b>组下的用户→</b> lgh150
	显示: 10 🗸 条 共3条

1. 点击 十编辑 按钮,可以对选中的用户组进行编辑,如下图所示:

☰ 编辑组		20101		×
IP段/组名称:	Vpn_Group		*	
移动组到:	root	~		
组属性:	□ 禁止sslvpn认证登录			
				确定

可以修改用户组名称,以及把用户组移动到别的用户组下。

2. 点击 十添加组 按钮,可以在选中的用户组下新建子用户组,如下图所示:

		>	<
IP段/组名称:		*	
组路径:	root/Vpn_Group		
组属性:	□禁止sslvpn认证登录		
		确定	

用户组名称不能超过 31 个英文字符,一个中文算两个字符。

- 3. 点击 米删除 按钮 , 会将选中的用户组从用户组织结构中删除。同时会删除掉该用户组下的所有用户。
- 4. 点击 *添加用户(段) 按钮,可以在选中的用户组下新建用户或用户段:

☰ 新建	用户	×
用户名称	: 输入用户名 *	
IP&MAC	: ●IP地址 OMAC地址 OIP和MAC O无IP	
	格式:单IP或起始IP-结束IP 🕜	
允许用途	: 🗹 允许做web认证用户 🗌 允许做VPN用户	
	密码:	
	☑支持web认证和SSLVPN用户修改密码	
	□禁止web认证登录(不允许上网)	
	确定	

用户名称:该用户的名称,同时也是登录 VPN 或 WEB 认证时的用户名。

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

密码:进入WEB认证或VPN登录时使用的密码。

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

✤ 恭喜您,登录成 注:请您添加收 线时请打开此链	<b>功! 您可以上</b> <u>藏本链接</u> ,当: 接进行手动下!	网 <b>了</b> 您要下 线 <b>!</b>
用户名: 李	靖	允许时这里才
IP地址: 189 用户权限: 允;	5.36.6.35 许上网	显示修改密码
可用时间:不	限时 🦊	
下线	修改密码	

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

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

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

- 5. 点击 操作 按钮,同样可以增加组、删除组、添加用户: +添加用户(段) +添加组
- 6. 用户组的用户列表:

## 关联行为策略: 共1斜 □、策略查看 ← 查看该用户组关联的行为策略

	×删附	注 区 属性编辑	搜索用户名 🗸					查询
		名称	IP地址(MAC地址) 🌲	VPN权限	行	b策略明 细	管	理
		123	无	√		∷≣	编辑	删除
		3.3.3.3	查看该用户的	]行为策略	÷	≣	编辑	删除
	<b>4</b> 77:	10 🗸 条 共2条	◀ 首页 ◀ 上一页	<b>1</b> 下一页	•	末页▶		确定
1	勾选质	后可以批量删除或编辑				编	辑或册	除用户

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

7. 点击 🗐 会弹出该用户(组)关联的行为策略情况,如下图所示:

	查看 张三 的策略关联信息 ×										
3	┿ 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) 十行为策略管理										
		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 】 1 确定										

▲ 十行为策略管理 将跳转到"流控>行为策略>高级设置"页面。

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



9. 点击

编辑 可以编辑相应的用户参数,各参数的作用可以参考"添加用户"。

📄 编辑用	户	×
用户名称:	\$.3.3.3	
IP&MAC :	●IP地址 ○MAC地址 ○IP和MAC ○无IP	
	3.3.3.3	
允许用途:	□允许做web认证用户 □允许做VPN用户	
移动到 :	root 🗸	
	确定	

10. 通过 搜索用户名 🗸

可以根据输入的用户名或 IP 进行查询,查询

的结果会显示到下方表格中。

Ⅹ删除	: 🕑 属性编辑	查	查询参数		搜索用户名 搜索ID			查询		
				授案IP						
	名称		IP地址	业(MAC地址)		VPN权限	1) 刃東哨明 细	管	理	
	张三	查询结果		无		×	⊞	编辑	删除	
显示:	10 🖌 条 共1条			▲首页 ▲ 上	一页	<b>1</b> 下一页	▶ 末页 ▶	1	确定	

查询

# 1.3.10.1.2导入导出用户

支持通过文件导入导出用户,导入导出用户配置页面如下:

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																
入文件條	言息规格	示例	Ø													
提示:其	中"MAC地	8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	2合中文或者	全角字符,召	5则可能出现	观错误。							
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 sslvpni, 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	192.168.1.9-19 2.168.1.12		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

#### 导入文件信息规格示例 💡

文件名:

提示:	<b>提示:</b> 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	蜜码	IP地址	MAC地址	是否 <b>双</b> 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 <del>允</del> 许web 认证账 号权限	是否 <del>允</del> 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	γ	Y	Y	Y	γ	Y	Y	Y	Y
<b>/</b> 财务 部	李四	888	192.168.1.9		Y	Y	Y	γ	Y	Y	Y	Y	Υ	Y	Y	N
/研发 部/研 发5部	王五	888	192.168.1.29	00-87-EF-12-4F-24	Ν	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N

浏览... □修改冲突用户 导入用户 导出用户

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

归属用 户组	用户名 称	密码	IP地址	MAC地址	是否双 向绑定	是否免 识别、 审计	是否免 流控	是否 VIP用 户	是否设 置为白 名单	是否禁 止上网	是否允 许修改 密码	是否禁 止认证 登录	是否作 为vpn 分支机 账号	是否 <del>允</del> 许web 认证账 号权限	是否 <del>允</del> 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	Υ	Y	Y	Y	Υ	γ	Y	Υ	Y	Υ	Y	Y
/财务 部	李四	888	192.168.1.9		Y	Y	Y	Y	Υ	Υ	Y	Υ	Y	Y	Y	Ν
/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	Ν

点击 浏览 按钮 , 找到文件	user-info.csv,点击导入用户按钮,会出现文件导入进度条,待进度条加载完成说明文
件已经上传成功。	
说明: 导入用户信息有利于实名制 提示: 导入用户的文件名必须为 u	管理用户,方便找到用户。 ser-info.csv ,并按以下示例的规格填写对应表格。
文件名: C:\Documents and S	tettings\user-info.csv 浏览 □修改冲突用户 导入用户 导出用户
<b>导出用户</b> :点击	钮会弹出如下图对话框。点击 保存 © 选择保存路径即可。
	文件下载 🛛 🔀
	您想打开或保存此文件吗?
	名称: user-info.csv 类型: Microsoft Office Excel 97-2003 工作表, 从: 172.18.3.97
	打开 (1) 保存 (2) 取消
	☑打开此类文件前总是询问(₩)
	来自 Internet 的文件可能对您有所帮助,但某些文件可能 危害您的计算机。如果您不信任其来源,请不要打开或保存 该文件。 <u>有何风险?</u>

# 1.3.10.1.3特殊用户管理

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





VIP/服务器用户:是指需要被保护的关键用户或内网服务器,这里的用户上网速度将被优先保证;点击 VIP/服务器用户将 弹出 VIP/服务器用户配置窗口,您可以对 VIP/服务器用户进行添加、删除等操作。具体操作参考 "2.6.2 VIP 用户"。 禁止用户:是指黑名单用户,如果您需要屏蔽某用户的上网一切行为,那么在这里直接将该用户设置为黑名单就可以了;点



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

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



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

1.3.10.2 WEB 认证

WEB 认证包括 WEB 认证和 WEB 认证免认证。

# 1.3.10.2.1WEB 认证

WEB 认证,即用户认证。

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

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



内置认证服务器

<ul> <li>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。</li> <li>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。</li> <li>注章: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;</li> <li>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。</li> </ul>		
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	
内置portal包:	浏览… 导入 【查看在线用户】	
认证方式:	仅使用本地用户信息.	
认证用户: <i>当中才能生效!)</i>	统─到用户组织  【管理配置认证用户】 (注意:統─到用户组织时,需把独立认证用户手动迁移到用户组织	
内置服务器端口:	8081 (1025 - 65535)	
帐号共享开关:		
广告推送方式:	先认证后广告 🖌	
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:	http://www.ruijie.com.cn (需要配置设备的DNS)	
推送广告时间间隔:		
	>> 高级设置	
	保存设置	

1、 Web 认证信息,您可以根据指定的格式导入"认证用户信息"。

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

在线认证用户列表 - Internet Explorer			
R http://172.18.124.72/web_auth_pi/user_certific_online.htm			
搜索在线用户: 基于名称 基于IP地址	查询  显示全部		
用户名	IP	操作	
wzhy	100.100.101.50	强制下线	
周同学	100.100.101.53	强制下线	
	【●首页 ●上一页	1 下─页 ▶ 末页 ▶ 1 确定	

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

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

4、 帐号共享开关:一个账号在同一个时间只允许一个 IP 使用,通过开启 □ 允许账号共享 可以设置允许多个 IP 共享 同一个账号,关闭账号共享的情况下,后登陆的账号有效。

- 5、 SMP 用户修改密码:开启该功能后,需要输入修改密码的 url,这样 SMP 用户就可以通过这个 url 来修改密码。
- 6、 广告推送方式:设定广告的显示方式,可以先认证后广告或无广告等。
- 7、 推送广告时间间隔:通过开启推送广告时间间隔,可以设定在多长时间内用户重复登录不弹出广告。
- 8、 广告地址:广告页面的 URL 地址。
- 9、 无需认证:开启该功能后配置无需认证用户 ip 无需认证并且推送广告。
- 10、 记账更新:是配置记账更新检查时间的,主要是对应 SMP/ESS 服务器的配置。
- 11、 自定义登录 LOGO:开启为自定义 LOGO,关闭为默认系统 LOGO,用户可以自定义自己的内置认证 logo 如下图,

4	1		
🧞 欢迎使	用,请输入	您的账号和密	码!
用户名:			]
密码:			]
	□ 记住用户	名和密码	
	登录	重置	

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

	▶ 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:	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
1.0.0.0表示所有IP段;量	<i>大允许配置50条规则。</i>
	IP地址:     子网掩码:     ×
初日:用户认证主要是指W 接入认证。 記定向HTTP端口: 拦截未 注意: 开启 "内置认证"后 信 "广告推送服务"后, 3 认证选项:	◆eb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 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。 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; 单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。 ○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:192.168.1.0-255.255.25! 【添加备用服务器】 🛛
通讯密码:	*
用户逃生功能:	
服务器检测:	
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
	<i>但</i> <b>扫</b> 一

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

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

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

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

🥑 添加/管理备用服务器	울 - Internet Explorer		
R http://172.18.124.	54/web_auth_pi/user_certific_portal.htm		
<b>说明:</b> 主备规则(5 用户除外) , 编辑服	E主后备),当主服务器不可达时,会使用 员务器配置时会中断web认证业务。	备用服务器中第一个可达的服务器进行	亍认证(需要开启服务器检测功能,指定接入
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	/255.255.25! 😵
	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
		【▲首页 ▲上一页	1 下一页 ▶ 末页 ▶ 1 确定

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

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

7、 SNMP 目的主机:是指认证服务器的主机地址。

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

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

	▶ 高级设置
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

# 1.3.10.2.2Web 认证免认证

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

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

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

#### 免认证网络资源(共有2条)

十添加	免认证资源 X删除选中		查询资源ip: 查询
	IP地址	掩码地址	操作
	1.2.2.2	255.255.255.255	编辑 删除
	12.2.5.5	255.255.255.255	编辑删除
		【▲首页 ▲」	

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

#### 免认用户IP(共有3条)

十添加免证	以证用户 X删除选中		查询用户ip: 查询
	IP地址	掩码地址	操作
	1.2.25.5	255.255.255.255	编辑删除
	4.55.55.2	255.255.255.255	编辑 删除
	54.5.55.2	255.255.255.255	编辑删除
		【▲首页 ▲」	上一页 1 下一页 ▶ 末页 ▶ 1 确定

#### • 广告推送服务

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:〇内置认证服务器 ③广告推送服务 〇外置认证服务器 〇关闭web认证
广告地址: http://www.ruijie.com.cn (需要配置设备的DNS)
推送广告时间间隔: 🗌 开启
>>> 高级设置 保存设置

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

确保广告推送: 🗹 开启(广告不被浏览器拦截)

#### • 用户认证的高级设置

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

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

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

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

5、 **下线检测模式**:支持设置用户下线检测模式,设置可以基于流量来检测用户是否下线,如果在15分钟内,用户流量 都没有增加,则认为用户下线。此命令仅用来辅助检测用户是否下线,会存在一些误检的风险。当前检测用户是否下线有以下 二种方式:a、用户点击认证页面上的"下线"按钮;b、基于用户流量的检测模式,在15分钟内用户流量没有增加,则认为 用户下线;默认情况下两种方式都开启。 6、 IP-MAC 绑定模式:设置用户 IP-MAC 绑定模式,设置根据 IP 或者 MAC、IP 绑定的模式,在二层网络中,可以选择用户名与 MAC、IP 绑定的模式,如果是三层网络结构,则只能选择用户名与 IP 绑定的模式,否则绑定后会出现网络不通的情况。

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

12. 免认证用户 MAC:可以针对用户 MAC 进行增删改查

#### 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
n	nac地址	操作
显示: 10 ▼ 条 共0条	【▲首页 《上—页 <b>1</b> 下	一页▶末页▶ 1 确定

## 1.3.10.3 商业营销认证

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

设备支持本地认证和与外置认证两种方式。选择单机内置认证,只要开启关联应用或者配置 URL 认证地址就可以使用;选

			◙ 关闭商业营销认证	
择与 MCP 联动则需要选搭建好 mcp 服务器。	如果你不需要应用认证	,可以选择关闭按钮	-	关闭商业

营销认证,然后点击确定按钮即可

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

保存设置

商业营销认证	
<b>商业营销认证:</b> 支持符合	\$税捷商业营销认证规范的服务器完成多种认证功能,如短信认证、微信认证等,推荐锐捷的WMC(云营销系统)。
商业营销认证	
商业营销认证向	回导: 【认证快速配置】 🕜
	▶ 基本设置
	≫ 高级设置
	▶ 免认证设置

这里专门提供了一个微信认证快捷配置,方便一键开启使用微信认证,如下图:

	微信认证配置引导	×
<b>V</b>	/ 微信认证方式	
	认证方式: 🖲 本地认证 🛛 外置认证	
2	广告推送	
	广告推送地址: * ?	
3	· URL认证	
	URL认证地址: *	
	完成	取消

── 微信认证配置引导	$\times$
微信认证方式	
认证方式:○本地认证 ◎ 外置认证	
2 微信服务器类型	
服务器类型: Tr069 ✔ (推荐使用Wifidog)	
→ 微信认证服务器	
服 <del>务器</del> 地址:	
完成取消	

具体参数功能如下基本设置、高级设置、免认证设置进行调整

#### ● 基本设置

包括本地认证和与外置认证两种模式。

1. 本地认证

✔ 基本设置			
认证方式: 🖲 本地认证 🔘 外置认证 🔘	关闭商业营销认证		
认证信息: 【查看在线用户】			
微信关注功能: 🗆 开启 ( 微信关注后用户认证上线 ) 🗲 微信认证后上网			
URL认证:	设备匹配到该URL后用户认证通过	← 点击URL链接上网	
推送广告地址:	需要配置设备的DNS	← 推送广告页面	
保存设置			

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

🧉 在线认证用户列表 - Internet Expl	orer		_ <b>_</b> X
http://172.18.124.72/web_auth_pi/app_certific_online.htm			
搜索在线用户: 基于名称		管间	
用户名	IP	在线时间	操作
100.100.101.53	100.100.101.53	2015-10-9 10:38:27	强制下线
【▲首页 ▲上一页 1 下一页 ▶ 末页 ▶ 1 确定			

查看在线用户:(可以查看用户名、ip、在线时间以及操作点击下线功能)

2. 外置认证

	认证方式:	○ 本地认证 (	◉ 外置认证	○ 关闭商	业营销认证
	重定向主页:	http://www.b	aidu.com	*	
	通讯密码:			*	
	服务器类型:	Tr069 🗸	(推荐使用W	/ifidog)	← 推荐使用Wifidog
MCI	P/WMC服务器:	[MCP/WMC]	配置】		
	认证信息:	【查看在线用户	ני		
	微信关注功能:	🖌 开启 ( 微信:	关注后用户认识	正上线)	【 ← 微信关注后上网
		保存设置			

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

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

① Tr069 需要设置 MCP/WMC 服务器

MCP/WMC 服务器设置:(注意管理类型应该选择 MCP/WMC 管理)

🤗 集中管理配置 - Internet Explorer					
R http://172.18.124.72/rac_pi/rac.htm					
集中管理:	☑ 开启集中管理 😮				
管理类型:	RAC管理 V				
服务端IP V:		*			
设备管理端口:		(1至65535 , 默认8088)			
性能监控管理端口:	30000	(10000至65000 , 默认30000)			
用户名:					
密码:					
	保存设置				

② Wifidog 需要设置检测用户逃生的地址


用户逃生功能:	【用户逃生功能配置】	
WiFi网络名称:	eweb	*
启用用户逃生功能	2: 🔲 勾选启用用户逃生功能	
检测用户逃生的地址	E: http://wmc.ruijieyun.com	*
	保存设置	
④自定义类型,支	持定制第三方服务器对接,需要售后或	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:	类型名称	* 请与厂商联系,获取您的专属类型
第三方自定义信息:	类型名称	* 请与厂商联系,获取您的专属信息
其中 Portal 重定向	]主页和通讯密码是必填的选项。配置完	高击外置认证的保存设置按钮 即基本设置部署完毕。
3. 关闭商业营销	肖认证	
认证方式:(	🔾 本地认证 🛛 外置认证 💿	关闭商业营销认证
	保存设置	
点击保存设置后关	闭商业营销认证。	

● 高级设置

*	高级设置					
源IP地址:	输入源ip 指定设备与认证服务器通讯的源IP地址,在ipsec vpn场景下使用					
mac-by-pass :	: 🛛 开启 开启读功能后,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:	: 図 开启用户下线检测 ,在 60 (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 !					
网络类型:	: 二层网络					
IP范围ssid:	十添加IP范围ssid 可配置不同网段对应到不同的SS	ID,用于外置认证服务器策略控制				
	IP地址	WIFI网络名称	操作			
	显示: 10 •		【●首页 ●上一页 1 下一页 ▶ 末页 ▶ 1 确定			
		十添加				

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

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

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

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

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

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

#### • 免认证设置

•••••	免认证设置
URL白名单:	URL白名单,所有用户(包括未认证用户)都可以访问读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。
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50条规则。单IP格式:如:192.168.1.2 IP范围:起始IP-括束IP,如:192.168.2.2-192.168.2.10。 ┃ ┃ ┃ ┃ ┃ ┃ ┃ ┃ ┃ ┃
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100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100条规则。MAC地址格式:如:0011.0022.0033。 ╋ → 添加
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。   <b>十</b> 添加

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

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

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ww					
	免认证网址: 格式:如www.ruijie.com.cn					
然后点击保存设置	即可保存设置。					

1.3.10.4 本地服务器认证

## 1.3.10.4.1认证策略

(1)本地服务器认证开关

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

用户组织	认证策略
WEB认证	开启本地服务器认证: OFF
商业营销认证	
里 本地服务器认证	

(2)调整认证策略优先级

认证策略表格中点击箭头进行优先级切换。

	策略aaa和444对调成功!						
认证策略         认证服务器         高级配置         免认							
说明:	说明:1不支持桥模式。 2.WEB认证、商业营销认证、本地服务器认证只能开启其中一个。						
十添加认证策略 ×批量删除							
	策略名称	认证范围	关联服务器	状态	上移/下移	操作	
	aaass	2.2.2.3.3.33.3	aa,aqr,1,adtest	集效	-	编辑删除	
	aaaa	所有IP	aqr,1,adtest,test	生效	€ &	编辑删除	
	444	1.1.1.1-2.2.2.2 3.3.3.3-12.1.1.1 3.13.3.3-44.44.4.4	aqr,11,adtest,test	生效	88	编辑删除	
	aaa	2.2.2-3.3.3.3	ad1,aqr,11,test	生效		编辑删除	
	sdfsdf	所有IP	ad1,aa,aqr,11	生效	۲	编辑删除	
显示: 10 ▼ 条共5条							

#### (3)添加/编辑认证策略

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

	2.0000	📃 认证策略		$\times$	
一添加	山认证策略		☑ 启用		
	策	策略名称:	ddd *		操作
	(	IP范围:	3.3.313.3.3.3	(	编辑删除
	1		// <b>?</b>		编辑删除
	ę	认证服务器:	* ?		编辑删除
显示	10 ▼ 务	优先显示:	账号密码认证    ▼		1 确定
			账号密码认证(账号密码认证) 🛞		
			确定		

(4) 2.8.5 删除认证策略

点击删除按钮或者点击批量删除,可以删除认证策略。

认证策略	8 认证服务器 高级	确定要删除策略aaas           配置         免认	ss吗? <b>晚</b> 定 取	Ă		
<b>说明:</b> 1.2 2.1	不支持桥模式。 WEB认证、商业营销认证、本地服务器	山江只能开启其中一个。				
十添加认证	E策略 ×批量删除					
	策略名称	认证范围	关联服务器	状态	上移/下移	操作
	aaass	2.2.2-3.3.33.3	aa,aqr,1,adtest	生效		编辑删除
	aaaa	所有IP	aqr,1,adtest,test	生效	€	编辑删除
	aaa	2.2.2.3.3.3.3	ad1,aqr,11,test	生效	€ -	编辑删除
	444	1.1.1.1-2.2.2.2 3.3.3.3-12.1.1.1 3.13.3.3-44.44.4.4	aqr,11,adtest,test	生效	€ 8	编辑删除
	sdfsdf	所有IP	ad1,aa,aqr,11	生效	•	编辑删除
显示: 10	▼ 条 共5条		н	首页 ◀ 上一页 1	下一页 ▶ 末页 ▶	1 确定

# 1.3.10.4.2认证服务器

#### (1)删除认证服务器

点击删除按钮或者点击批量删除,可以删除认证服务器。

认证	策略 认证服务器 高级配置	确定要删除认证服务器吗? 免认		· · · • • • • • • • • • • • • • • • • •
<b>十</b> 添加	以证服务器 ×批星删除 × 批星删除 × 名称	认证类型	认证服务器	操作
	ad1	LDAP服务器	192.168.1.1	编辑删除
	aa	短信认证		编辑删除
	sms-test	微信认证	-	编辑删除
	aqr	二维码自助认证	-	编辑删除
	1	二维码授权认证	-	编辑删除
	11	二维码授权认证	-	<b>编辑</b> 删除
	adtest	LDAP服务器	-	编辑删除
	test	短信认证	-	编辑删除

(2)添加/编辑短信认证

点击添加或者编辑,配置短信认证

一添加	认证服务器 ×批量删除	余			
			认证类型	认证服务器	操作
	微信认证		LDAP服务器	192.168.1.1	编辑删除
+	二维码授权认证		短信认证	- 	编辑删除
+	二维码自助认证 st		御国外。		编辑删除
+	LDAP服务器		二维码自助认证		编辑删除
	1		二维码授权认证		编辑删除
	11		二维码授权认证	-	编辑删除
	adtest		LDAP服务器	-	编辑删除
	test		短信认证	-	编辑删除
	aaa		短信认证	-	编辑删除
	123456		短信认证	-	编辑删除
显示:	10 ▼ 条 共12条		H	首页 《 上─页 1 2 下─页 》 末页 》	1 确定

十添加认证服务器	l 短信认证 ×	<
		操作
	名称: *	编辑删除
	短信网关: 阿里云短信(旧版) 🔹	编辑删除
	短信验证appkey:	编辑删除
		编辑删除
	短信验证Secretkey:          *	编辑删除
	短信签名:	编辑删除
	短信模板:	编辑删除
		编辑删除
	预先输入手机号模式: 🗌 启用 😢	编辑删除
		编辑删除
显示: 10 ▼ 条共1	确定	1 确定

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

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

(3)添加/编辑微信认证

#### 点击添加或者编辑,配置微信认证

#### ★添加认证服务器 ×批量删除

		认证类型	认证服务器	操作
	微信认证	LDAP服务器	192.168.1.1	编辑删除
+	二维码授权认证	短信认证	-	编辑删除
+	二维码自助认证	微信认证 弹出微化	言认证配置框	编辑删除
+	LDAP服务器	二维码自助认证	-	编辑删除
	1	二维码授权认证	-	编辑删除
	11	二维码授权认证	-	编辑删除
	adtest	LDAP服务器	-	编辑删除
	test	短信认证	-	编辑删除
	aaa	短信认证	-	编辑删除
	123456	短信认证	-	编辑删除
显示:	10 ▼ 条共12条	【 首页	《 上─页 1 2 下─页 ▶ 末页 ▶	1 确定

十添加认证服务器	── 微信认证	×	
			操作
•	微信连WiFi面	<u> 置示例</u>	编辑删除
	名称:	*	编辑删除
	shopId :	2*	编辑删除
		*	编辑删除
	арріа :		编辑删除
0	secretKey :	*	编辑删除
			编辑删除
显示: 10 🔻 条		确定	1 确定
段		说明	
ervername		认证服务器名称	
		名称不能是_PWD_AUTH 或者	账号密码认证

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

### (4) 添加/编辑 LDAP 服务器

### 点击添加或者编辑,配置 LDAP 服务器

十添加认证服务器 ×批量删除							
			认证类型		认证服务器	操	作
	··微信认证		LDAP服务器		192.168.1.1	编辑	删除
+	十二年码授权认证		短信认证	弾出	LDAP服务器配置框	编辑	删除
+	十二年月自助认证		维码自助认证		-	编辑	删除
+	LDAP服务器		二维码授权认证		-	编辑	删除
	aaa		二维码授权认证		-	编辑	删除
	wexin-test		微信认证		-	编辑	删除
	sms-bbb		短信认证		-	编辑	删除
	ldap-ssss		LDAP服务器		192.168.1.1	编辑	删除
显示	10 ▼ 条 共8条			∢ 首	页 ◀ 上一页 1 下一页 ▶ 末页 ▶	1	确定



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

(5)添加/编辑二维码授权认证

点击添加或者编辑,配置二维码授权认证

~ 添加认证服务器	X批量	删除				
			认证类型	认证服务器	操作	
			LDAP服务器	192.168.1.1	编辑删除	
十二维码授权	人证 LiF		短信认证	-	编辑删除	
十二维码自助证	人证		二维码自助认证	-	编辑删除	
╋LDAP服务器	2 T		二维码授权认证 弹出	二维码授权认证配置框 🔶	(编辑)删除	
	aaa		二维码授权认证	-	编辑删除	
	wexin-te	st	微信认证	-	编辑删除	
	sms-bbt	þ	短信认证	-	编辑删除	
	Idap-sss	s	LDAP服务器	192.168.1.1	编辑删除	
	Idap-tes	t	LDAP服务器	1.1.1.1	编辑删除	
显示: 10 ▼ 条 #	共9条		ŀ	首页 《 上─页 1 下─页 》 末页	[】 1 确定	
添加认证服务器	<u> </u>	推码授权认证			×	
					操作	
			名称:	*	编辑删除	
		二维码	提示信息:		编辑删除	
					编辑删除	
					编辑删除	
					编辑删除	
					编辑删除	
					编辑删除	
					编辑删除	
0					编辑删除	
显示: 10 ▼ 条					1 确定	
				确定		
段			ì	兑明		
rvername			ì	人证服务器名称		
			Ĩ	名称不能是_PWD_AUTH 或	诸账号密码认证	
rvertype			S	ms:短信认证		
			c	ɪrcode-alone : 二维码自助ù	人证	
			c	qrcode-authorize:二维码授权认证		
				act-directory:LDAP 服务器		
			ν	veixin:微信		
authcomment				二维码提示信息,为空时下发	发 no 命令	

(6)添加/编辑二维码自助认证

#### 点击添加或者编辑,配置二维码自助认证

「添加认证服务器 ×批量删除							
	十 关 信 认 证 十 微 盲 认 证 十 二 单 码 授 权 认 证		认证类型	认证服务器	操作		
			LDAP服务器	192.168.1.1	编辑删除		
+			短信认证	-	编辑删除		
十二维码自助认证		二维码自助认证 弹出二维码	自助认证配置框	编辑》删除			
+	十LDAP服务器		二维码授权认证	-	编辑删除		
	aaa		二维码授权认证	-	编辑删除		
	wexin-te	st	微信认证	-	编辑删除		
	sms-bbb	D	短信认证	-	编辑删除		
	ldap-sss	s	LDAP服务器	192.168.1.1	编辑删除		
	Idap-tes	t	LDAP服务器	1.1.1.1	编辑删除		
显示:	10 ▼ 条共9条		▼	页 《 上─页 1 下─页 》 末页 》	1 确定		



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

		ш		-	
四r.	首	Ŧi	ΞI	主	
ΠU		JI			

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

# 1.3.10.4.3高级配置

进入【用户-本地服务器认证-高级配置】菜单后,显示高级配置相关信息。

网络类型:	◎二层网络 ◎三层网络		
非授权方式上线时长:	11	•	
授权方式上线时长:	33		
账号自动记录mac :	≥ 开启 🔮		
	每个账号自动记录mac限制个	数: 22	
	无感知认证功能: 看广告方	式无! ▼ 🧧	
账号空闲老化时间:	44	•	
通过DHCP SNOOPIN获取mac功能:	☞ 开启 💿		
无流量检测下线:	≥ 开启 🔮		
	持续 55	流量小于 66	终端将被下线
开启https重定向:	≥ 开启 🔮		
微信放行:	☞ 开启 ( 如有配置自助扫码)	<del>6</del> 略,则建议开启微信放行功能)	
授权管控:	2 0		
被授权用户可继续授权次数:	88	9	
终端管控功能:	≥ 开启 🔮		
限制电脑上网:	≥ 开启 例外时间: offic	e ▼	
限制移动终端上网:	≥开启 例外时间:晚上	T	
	【时间管理】		
文件名:	选择文件未选择任何文件	督 接 logo 恢 复	t认logo
	保存设置		
字段		说明	
net-id		网络类型	
		1:二层网络	
		2:三层网络	
authorize-time		非授权方式上线时长	

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

# 1.3.10.4.4免认证配置

免认证用户IP: 该用户可以直接上网,且不会推送 免认证外网IP: 输入网络资源服务器的IP地址,所和 URL白名单: URL白名单,所有用户(包括未认证月 用户MAC白名单: 该MAC用户可以直接上网,且不 用户MAC属名单: 该MAC用户禁止上网,最大允许 施时黑白名单: 免认证用户IP/免认证用户外网IP/用 注章: 本地服务器认证、商业营销认证、WEB认证使	告,最大允许配置50条规则。单IP格式;如:192. 用户(包括未认证用户)都可以访问该P:最大方 引)都可以访问该URL;支持通配,如配置ruijie.c 会推送广告,最大允许配置100条规则。MAC地址 配置100条规则。MAC地址模式;如:0011.002; 户MAC白名单/用户MAC黑名单可配置有效期,到 印两个不能同时开启。	168.1.2 IP范围:起始IP-结束IP,如:192.16 均希置50个地址条规则,单IP格式:如:192 om,则允许访问www.ruijie.com, news.ruijie. 格式:如:0011.0022.0033。 2.0033。 期后相关配置将自动消失,已生效时间可在已	8.2.2-192.168.2.10, 8.168.1.2 [P范围:記始IP-结束IP , 如:192.168.2.2- com,最大允许配置100个网址。 经生效时长查看。	192.168.2.10,
免认证用户				
十添加兔认证用户 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			▲首页 《上一页	1 下─页 ▶ 末页 ▶ 1 确定
免认证外网IP				
╋ 十添加免认证外网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
URL白名单				[
十添加URL白名单 X删除选中				-
	免认证网址		操作	L
显示: 10 ▼ 条 共0条			(首页 《上一页	1 下─页 ▶ 末页 ▶ 1 确定

## 1.3.10.4.5单点登录

进入【用户-本地服务器认证-单点登录】菜单后,显示单点登录相关信息。

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:	ruijie111	☑ 显示密码
	保存设置	

## 1.3.10.4.6用户权限

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

说明:注册用户为用户上线后生成的新 注册用户和组管理中,对于AD	项。用户生成后可以点击"编辑", 在该账号下添 成,都显示完整的dn。	homac并指定终端类型。	
注册用户 组权限			
用户名	用户类型	mac地址(终端类型)	操作
test	AD域用户	0011.0022.0033	编辑
显示: 10 ▼ 条共1条	н	首页 《 上─页 1 下─页 》 末页 》	1 确定

注册用户	组权限	十编辑组权限		
	用户名		用户类型	操作
D	omain-Controllers	;	AD域用户	删除
	综合网关事业部		AD域用户	删除
	特权组		本地用户	删除
	mygrp		本地用户	删除
显示: 10 ▼ 条共	4条		◀首页 ◀ 上一页 1 下一页 ▶ 末页 ▶	1 确定

## 1.3.10.4.7在线信息

进入【用户-本地服务器认证-在线信息】菜单后,显示相关信息。

认证策略	认证服务器	高级配置	免认证配置	用户权限	在线信	息		
<b>说明:</b> 短信认道	E时手机号已绑定账号,	用户名显示为账号。						
基于用户名 ▼		查询	<b>×</b> 下线选中					
	用户名			IP		类型	在线时间	操作
						无记录信息		
显示: 10 ▼ 务	ŧ						【●首页 ● 上一页 下一页 ▶ 末页】	1 确定

### 1.3.10.5 上网屏蔽模式

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

上网屏蔽模式				?帮助
<b>说明:</b> 开启上网屏蔽	模式后所有内网用户将不能通过设计	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 十添加排除屏蔽用户	℃ - ★删除选中用户			
	用户名称	IP地址	MAC地址	删除
		н	首页 《上─页 1 下─页 ▶ 末页 ▶	1 确定

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

■ 添加排除屏蔽用户	$\times$
Q	
- 🔁 所有用户	
+ 🗀 🗆 web认证	
+ 🗀 🗆 Vpn_Group	
€ 3.3.3.3	
€ 123	
(如斋添加用户,请到 用户管理 -> 用户组织 )	
确定	
勾选需要排除屏蔽的用户,点击 明可:	

上网屏蔽模式				?帮助
<b>说明:</b> 开启上网屏蔽	旋模式后所有内网用户将不能通过设备	备上网,除非将用户设置为"排除屏蔽用户" ;		
<ul> <li>☑ 开启上网屏蔽模式</li> <li>十添加排除屏蔽用户</li> </ul>	∜ ■ X删除选中用户			
	用户名称	IP地址	MAC地址	删除
3.3.3.3		3.3.3.3	#	删除
		ю	首页 《上─页 1 下─页 》 末页 》 □	l 确定

删除 点击"删除"栏的

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

### 1.3.10.6 悬浮窗广告

首次开启该功能需要重启设备才能生效,悬浮窗广告的配置如下:

悬浮窗广告		
注意:本模块使用了tcp代t	里,悬浮窗功能会跟上网屏蔽模式冲突,请确认已关闭上网屏蔽模式。	
<b>悬</b> 浮窗广告:	☑ 开启悬浮窗广告 (面) 置完需重启设备)	
广告链接地址:	请输入url(如:http://www.ruijieyun.com/xx.js)	
		1
[	最多可输入字符串长度为255字节	
基于IP过滤广告:		1
		十添加
甘工術を対慮亡生		-
		十添加
		1
	保存 删除全部过滤IP 删除全部过滤域名	



开启悬浮窗功能后,通过设备上网的 pc,浏览网页会弹出广告的效果如下,



### 1.3.11 网络

### 1.3.11.1 接口配置

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

Г	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	
	说明: 只需点击 AnyIP功能: 设计	对应接口就可以配置。 产 备冒充网关,代理应答非	品的光电口分布请查看 妾口直连网段的所有AR	<mark>帮助中心 。 DHCP接l</mark> P请求 , 并为用户IP动态	□不支持线路逃生和链路 注此相应直连的路由,	<mark>路检测。</mark> 使得配置IP和网关的用	月户不修改配置也能上网。
	💼 : 已上电 🛛 🗯	: 未上电					
	LAN0	LAN1/WAN4	LAN2/WAN3	LAN3/WAN2	LAN4/WAN1	WAN0	
				$\oplus$	•	$\oplus$	
	已配置	已配置	已配置	未配置	已配置	已配置	
像这		蓝色高亮显示的接口	口说明该接口处在。	上电状态(网线已	接上 ), 其中灰度	显示的	时接口说明该接口
上未	主电,其中,更有	与小地球的接口说明	该接口是外网口	, 没有的话就是内	网口。		
接Ľ	口配置在网关模	試和网桥模式下的	配置不同 , 接下来	将分别为您介绍。			

:

# 1.3.11.1.1接口基本设置

#### • 内网口配置

点击需要配置的内网口即可对选中的内网口进行配置 , 如点击

and the second se	LAN1/WAN4	LAN2/WAN3	LAN3/WAN2	LAN4/WAN1	WANO			
				•				
-Melli	CAIR	ENDI	中的目	CALIE	Entili			
N0口 (Gi0/	0) 设置					接口转换	管理次IP	管理子接口
IP地址:	192.168.1.1	*						
	255.255.255.0	•						
于阿强制:								
于阿雅的	■ 两级配置							

去掉了管理次 IP 和子接口管理。

### LAN0口 (Gi0/0) 设置



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

子网掩码:这个是网段对于的掩码地址;

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

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

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

次 IP:以太网接口支持多个 IP 地址,次 IP 为除首次配置的 IP 地址之外的其它 IP 地址。点击 可以查看 和管理选中接口下的次 IP 地址:

Ξ 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-	-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 Explore	er		X
R http://172.18.124.	54/interface_pi/int_child.html			
子接口名:	Gi0/4 V. 1	* <i>(1至1023)</i>		
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 <del>了接</del> 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─页 1 下─页》末页	1 确定

#### • 外网口配置

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

LAN0	LAN1/WAN4	LAN2/WAN3	LAN3/WAN2	LAN4/WAN1	WAN0		
			$\oplus$	•	$\oplus$		
已配置	已配置	已配置	未配置	已配置	已配置		
WAN1[] (Gi0	/4) 设置 动态IP	(DHCP) V				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	(1	格式:00d0.f822.123	34)			
下行带宽:	10	M	bps(0.5~10000)				
上行带宽:	10	M	bps(0.5~10000)				
MTU :	1500	(1	64-1500)不配置时黑	默认PPPoE为1488	<i>, 其他为1500</i> 请勿随	意修改,可能导致	如络异常
开启NAT配置:	☑勾选开启线路NA	T功能					
开启源进源出:	☑勾选开启源进源出	4 🕜					
保存设置	清除设置						

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

● 静态 IP 地址:

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

• PPPoE (ADSL) :

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

外网口配置 PPPoE(ADS	SL) 🗸		
Gi0/6口-账号:		* 踏码: *	
IP 地址:	自动获取		
接口描述:			
MAC地址:	00d0.1122.33da	(指式:00d0.f822.1234)	
下行带宽:	10	Mbps(0.5~10000)不配置时默认为4	
上行带宽:	10	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	◎ 美它	
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:	电口 >		
	保存设置清除设置	子接口管理	

● 动态 IP 地址:

如果您的上网方式选择"动态 IP 地址",系统将动态获取 IP 地址。

外网口配置 动态IP(DHC	(P) 🗸	
IP 地址:	自动获取	
接口描述:		
MAC地址:	00d0.1122.33da	(格式:00d0.f822.1234)
下行带宽:	10	Mbps(0.5~10000)不配置时默认为10
上行带宽:	10	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:	电口 ~	
	保存设置 清除设置	子接口管理

2. 其它外网口配置信息:

- 1) 接口描述:选择"静态 IP 地址"时的配置项,非必填项,用于描述接口的信息。
- 2) 光电转换:该接口可以作为光口也可以作为电口,一般只有部分外网口有这功能。
- 3) 上行带宽、下行带宽:接口允许的最大带宽值,需要根据您向运营商申请的带宽实际数据填写,范围为 0.5~1000Mbps, 默认 10Mbps。
- 4) 网络服务商:包括电信,移动,联通,教育,其他网络。

### 1.3.11.1.2一线多拨

接口基本设置	一线多拨	多链路聚合	接口转换	链路检测	
<b>说明:</b> 开启一线多拨 <b>注意:</b> 关闭该功能,	后,请到接口基本设 会将已配置的拨号口:	置界面对应接口下添加拨 全部删除掉。	5号线路。		
开启一线	多拨:	关闭			

## 1.3.11.1.3多链路聚合

接口基本设置内网络	多链路聚合	接入模式选择	接口转换	链路检测		? 帮助
流量平衡: 源IP+目的IP		▶ +添	bo			
聚合接口名	聚合接口		接口信息	是	否开启NAT	操作
AggregatePort 1	Gi0	/1	5.5.5.5/255.255.255.	0	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

确定 完成配置。

	三 添加内网多链	格聚合	×
[	选择聚合口:	Ag1 🗸	<u>a</u>
	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	<b>正</b> 取消

## 1.3.11.1.4接口转换

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



一线多拨

接口基本设置	一线多拨	接口转换 链路检测					
<b>说明:</b> 开启一线多拨后,请到接口基本设置界面对应接口下添加拨号线路。 <b>注意:</b> 关闭该功能,会将已配置的拨号口全部删除掉。							
开启一线	多拨:	关闭					

## 1.3.11.1.5链路检测

链路检测:用于检测设备外网口接口是否正常工作,配置页面如下:

接口基本设置	内网多链路聚合	接入模式选择	接口转换	链路检测	(?) 帮助				
<b>说明:</b> 检查设备接口工作是否正常,是否链接 <mark>。当ping的IP地址不通时会导致断网!</mark> 当对端IP不可达,那么设备认为该链路有问题,对应接口协议状态变成down,该接口无法继续通信;当对端IP可达的时候接口协议状态UP,通信恢复正常。配置本功 能时请确保对端IP稳定。									
□开启Gi0/6口的多	链路检测								
□开启Gi0/7口的多	链路检测								
确定									

配置步骤:

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

ping地址:	*	下一跳地址:	*	探测间隔:	100	单位:毫秒

2. 若要检测接口是否可连接,请输入可 ping 通地址,如百度 220.181.112.143。

- 3. 输入下一跳地址,若为内网设备则输入网关地址,若不配置,默认下一跳地址为 ping 地址。
- 4. 输入探测间隔时间,默认为1s。
- 5. 点击^{确定},如果符合上述配置可 ping 通,则显示提示信息为"网络良好",否则为"网络不通"。

## 1.3.11.1.6接口基本设置 IPv6

• 内网口配置

点击需要配置的内	内网口即可对选	中的内网口进行	冠置 , 如点击				
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	
<b>说明:</b> 只需点击对应	过接口就可以配置。						
💼: Ele 🛤	: 未上电						
LAN0	LAN1/WAN4	LAN2/WAN3	LAN3/WAN2	LAN4/WAN1	WAN0		
		$\oplus$		•			
已配置	未配置	已配置	未配置	已配置	已配置		
LAN0口 (Gi0/	0) 配置						
IPv6地址:		* 13	희: 2000::1/128				
保存设置	清除设置						
● 外网口配置							

点击需要配置的内网口即可对选中的内网口进行配置,如点击



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
<b>说明:</b> 只需点击对	应接口就可以配置。					
💼: Ele 🛤	: 未上电					
LAN0	LAN1/WAN4	LAN2/WAN3	LAN3/WAN2	LAN4/WAN1	WAN0	
		$\oplus$			$\oplus$	
已配置	未配置	已配置	未配置	已配置	已配置	
WANOD (Gio	0/5) 配置	* 4	헤: 2000::1/128			
II TOMENT !						
外网网关:		* f	列:2000::1			
网络服务商:	◉其他					
保存设置	清除设置					

### 1.3.11.2 启用防封杀

启用防封杀	
说明:端口启用此功能 注意:ADSL线路通常等	,可以尽量避免ISP封杀共享,主要用于ADSL线路。 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 Gi0/5 Gi0/6 Gi0/7
	保存设置

### 1.3.11.3 SUPER-VLAN

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

## 1.3.11.3.1SUPER-VLAN 配置

通过该页面可以开启和配置 SUPER-VLAN 功能,主要的界面如下:

SUPER-VLAN配置	在线SUPER-VLAN信息	(?)帮助
<b>什么是SUPER-VLAN:</b> SU 出。	PER-VLAN就是实现单臂路由功能,近	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
开启SUPER-VLAN:	☑ 勾选开启SUPER-VLAN ←	·开启SUPER-VLAN
每VID最大上线数:	100	(1-1000)
勾选内网口配置VID:	□Gi0/0 □Gi0/2 □Gi0/3	Gi0/4 Gi0/5 (VID的配置范围为1-4085,格式如:10,20,40-100)
	保存设置	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●

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

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

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

配置完后点 保存设置 保存设置。

## 1.3.11.3.2在线 SUPER-VLAN 信息

查看当前的在线的 SUPER-VLAN 信息。界面如下图所示:

SUPER-VLAN配置	在线SUPER-VLAN信息	() 帮助
说明: 每VID允许最大上线 注意: 如果下面信息有多多	澂为100,其它VLAN无用户上线,不显 _杀 相同的ip信息,那么内网中可能存在ip)	示在表格中 中突,请排查
		暂无SUPER-VLAN信息!

#### 1.3.11.4 路由/负载

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

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

点我 咨询

# 1.3.11.4.1选路配置向导

### 网吧场景下,增加选路配置向导菜单,如下图

选路配置向导	策略路由  应	用路由	普通路由	多链路负载均衡						
<b>说明:</b> 选路配置向导锁 较好,较稳定,建议为	适用于多线路场景,单线路场 5光纤线路)、线路运营商属(	景不需要使用。「 性以及DNS服务者	向导可以根据当前ù 条,便可一键生成转	设备出口的运营商以及带宽情况 较优配置方案。	,自动识别线路好坏,	生成较优的应用路由等选路方案	并引流P2P等非关键应用,	合理分配各线路的流量。	仅需确认主线路(周	睡
	开始检测									
选路配置向导	策略路由 应	用路由	普通路由	多链路负载均衡						
说明:选路配置向导过 较好,较稳定,建议为	适用于多线路场景,单线路场 5光纤线路)、线路运营商属	i景不需要使用。 性以及DNS服务	向导可以根据当前 器,便可一键生成	前设备出口的运营商以及带宽情》 较优配置方案。	兄, 自动识别线路好坏	,生成较优的应用路由等选路方;	髦,并引流P2P等非关键应	用, 合理分配各线路的流	量。仅需确认主线路	(质量
选路配置与网络使用	目情况 2 重新检测									
接囗: Gi0/4	下行宽带及使用率: 上行宽带及使用率: 线路: 运营商:	1000.0Mbit 1000.0Mbit 主线路 电信	↓0.0% ↑0.0%							
应用路由	是否开启:	🛿 未开启								
应用路由 多链路负载均衡	是否开启: 是否开启:	<ul> <li>未开启</li> <li>未开启</li> </ul>								

📃 接口信息						×
Gi0/4	运营商: DNS1:	电信 ▼ 192.168.58.110	*	主线路 DNS2:		
						完成配置

### 1.3.11.4.2策略路由

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

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

策略路由配置页面如下图所示:

应用路由	普通路由	多链路负载均衡	策略路由			
<b>路由优先级:</b> 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。 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路由转发机制,以太网环境下需要面置下一跳地址,而PPOE环境下需要面置接口。						
策略组	匹配接口:	Gi0/0	T			
策	略优先级:		* (0~65535)			
匹酉	ACL列表:	1	▼【新建ACL列表】			
L	日口/下一跳[	接口	▼ 请选择接口	▼【PPOE环境】 PPOE	不填下需要配置接口	
		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			▶★ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	▶ 末页 ▶ 1 确定	

1. 策略路由设置:选择需要策略的接口、输入策略优先级、选择匹配 ACL 列表(用于指定应用在哪个策略)、输入下一

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

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

#### 2. 策略路由列表:

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		н	首页 《 上─页 1 下─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 即可删除对应项;点击配置页面右上角的 光删除全部 按钮可以删除对应策略 组下的所有的路由策略。

## 1.3.11.4.3应用路由

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

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

#### 应用路由配置页面如下图所示:

策略路由	应用路由	普通路由	多链路负载均衡							
<b>应用踏由</b> :根据	器数据流的应用类型、 	源目的IP地址、运营	商等属性将流量分到不同的	的出口线路,	从而保障关键应用的(	本验,并且合理充分	利用各条线路的有	带宽。		
十新建应用路由	十指定主机走单	线路								
十 新建应用路由 优先级	十指定主机走单	线路 源网段/源端口	目的网段/目的端 口	应用	分流接口名	生效时间	□开启	状态	匹配顺序	管理

#### 添加"优先级"列

应用路由	<b>应用路由</b> 普通路由 多链路负载均衡 策略路由									
路由优先级: 第 应用路由: 基于 业务各行其道, 》 温馨提示: 不建	<b>路由优先级</b> : 新略路由、用户路由、应用路由和普通P路由都可以作为报文转发的依据。当新略同时存在的修况下,优先级是:新略路由 > 用户路由 > 应用路由 > 静态路由(地址库) > 默认路由。 应用器由: 基于应用的路由,区别于传统的基于报文目的IP选路的IP路由技术,是一种根据数据流的应用类型进行路由转发的技术。基于这种技术,可以将不同应用类型的数据流分流到不同的出口,以达关键业务与抑制 业务各行其道,减少影响的目的。 温馨提示: 不建议对关键应用做应用路由,建议对客户需求中抑制的应用做应用路由。									
十新建应用路由	▲ 直看路由效果	₽.						1	查看未生 /	之效原因
应用类型名	源于日代中田	网段	目的网段	目的URL	分流接口名/接口组	生效时间	☑ 开启	状态	匹配顺序	管理
test 🗐	有具体应用 zid	liying	-	P2P~sys(dns:192.16 8.58.110)	Gi0/6	下班时间	☞ 开启	未生效 💈	-	编辑删除
视频流媒体转	14	-	-	QQ特权~sys(dns:19 2.168.58.110)	Gi0/6		☞ 开启	未生效 😮	۰ 🕹	编辑删除
HTTP协议	÷	文育	电信	-	Gi0/6	晚上	☑ 开启	未生效 😮	۰ 🌡	编辑删除
-		-	-	-	di 1		☑ 开启	未生效 😮	<b>^</b>	编辑删除
显示: 10 🔻						▲東 ◆	上一页	1 下一页 调整	▲ 末页) 】 を优先级	1 确定

新建应用路由:点击 十新建应用路由 弹出以下导航窗口:

■ 新建应用路由				×
۹	● 新建	○ 现有应用组		/ 应用类型
- □ □ <mark>所有应用</mark> + □ □ HTTP协议	已选应用			2 源和目的网段
				3 分流接口
				4 生效时间
+				
		L	步	下一步

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

选择单个应用或应用分类作为策略关联的应用对象,此时策略将对选中的应用或应用分类下的所有应用进行匹配和分流: 左侧树状图列出了系统当前可应用路由的应用组织结构,可以直接在这里选择一个应用或应用分类作为策略关联的应用对象。 新建一个应用组作为策略关联的应用对象,此时策略将对该应用组包含的所有应用进行匹配和分流:

➡ 新建应用路由				×
Q	• 新建	◎ 现有应用组		/ 应用类型
- □ □ 所有应用 - □ □ HTTP协议 + □ □ WFB应用	已选应用 HTTP视频		$\otimes$	2 源和目的网段
+ □ QQ应用	▶ 视频流媒体	<b>本软件</b>	⊗	3 分流接口
+ → HTTP网络购物 + → HTTP视频 → FLASH → 中国铁路客户服务 + → 移动WEB应用 + → 论坛PC + → HTTP游戏 + → WFR邮箱	▶ P2P应用载 ★ D2P应用载	分组名称		4 生效时间
			上一步	下一步

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

右侧选中 🔍 现有应用组 ,页面如下图所示:

■ 新建应用路由			×
Q		● test •	/ 应用类型
- □ 所有应用 - □ ● HTTP协议 + □ ● WEB应用 + □ ● QQ应用 + □ ● HTTP网络购物 + □ ● HTTP视频	<ul> <li>已选应用</li> <li>□ HTTP协议</li> <li>■ 视频流媒体软件</li> <li>□ P2P应用软件</li> </ul>	删除该组 ⊗ ⊗	<ol> <li>2 源和目的网段</li> <li>3 分流接口</li> <li>4 生效时间</li> </ol>
<ul> <li>♥ ● FLASH</li> <li>♥ ● 中国铁路客户服务</li> <li>+ ● ♥ <u>移动WEB应用</u></li> <li>+ ● ♥ 论坛PC</li> <li>+ ● ♥ HTTP游戏</li> <li>+ ● ♥ WEB邮箱</li> </ul>			
		上	<del>த</del> ⊥⊤

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

2) 源和目的网段:应用路由支持指定源 ip 与目的 ip 网段,以及目的 url 组来进行引流。ip 网段可以是单个 ip 地址, ip 地址范围,甚至地址库。指定源 ip 网段,如指定内网的服务器 ip 地址,可以实现类型策略路由的效果。指定目的 ip 网段,如指定目的网段是电信地址库,可以实现类似地址库的效果。指定目的 url 组,允许将指定的域名引流至指定的接口,包括 dns 的解析以及数据报文的引流。
| ■ 新建应用路由    |              | ×        |
|-------------|--------------|----------|
| 源网段:        | any 🔻        | / 应用类型   |
| 目的网段或URL对象: | ●目的网段 ●URL对象 | 2 源和目的网段 |
| 目的网段:       | any 🔻        | 3 分流接口   |
|             |              | 4 生效时间   |
|             |              |          |
|             |              |          |
|             |              |          |
|             |              |          |
|             | 上一步          | 下一步      |

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

	■ 新建应用路由												$\times$
Q			输入接口	]组名 ▼	输入分	组名称					7	应用类型	Ī
□GigabitEt	□GigabitEthernet 0/5 □dialer 1			各							_		
🗆 dialer 1											2	源和目的	]网段
											3	分流接口	1
											4	生效时间	]
									上-	-步		下一步	
新建应用路由	I								×	1			
Q		输入接口	组名 🗸 🗍	入分组名	称			∕应	用类型				
□GigabitEthernet □GigabitEthernet	: 0/5 : 0/6	已选线路	ł					<b>2</b>	流接口				
□dialer 1								3 生	效时间				
		接口的均	的衡策略:	按带宽利	用率 ✔								
						Ŀ	步	<u></u> ጉ-	步				

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

下一步

继续配置策略。

输入接口组名 💙 输入接口组

指定接口组为应用路由出口:可以在上图右侧的下拉框 选择接口组 中选择"输入接口组名"或"选择接口组"。

选择"输入接口组名"则需要在后面的输入框中输入接口组名新建一个接口组,并从左边列出的线路中选择需要的线路加入该

接口组,如下图所示,选中的线路将显示在右边的"已选线路"区,点击 🖄 可以将不需要的线路从该接口组中删除:

📃 新建应用路由		×
Q	输入接口组名 ▼ aaa	/ 应用类型
GigabitEthernet 0/5     Ødialer 1	已选线路	2 源和目的网段
	dialer 1	3 分流接口
		4 生效时间
	上一步	5 下一步
■ 新建应用路由	×	
Q	輸入接口组名 ✓ aaa × / 应用类型	
☑GigabitEthernet 0/5	已洗线路	
✓GigabitEthernet 0/6	GigabitEthernet 0/5	
	GigabitEthernet 0/6 ② 3 生效时间	
	接口的时間策略: 按帝党利用率 >	
	上一步下一步	

选择"选择接口组"则后面的输入框为变为下拉选择框: 输入接口组名 🗸 aaa X , 这里可以选择 一个已存在的接口组, 对该接口组进行编辑, 接口添加、删除操作同上。

#### 请注意:

1) 不能让所有接口都做应用路由;请保留最少一条优质线路,不做应用路由(走默认路由)。

2) 动态获取 ip 的接口,不支持应用路由;

3) 请提前确认选择的接口,在接口配置 or 快速配置中,是配置好的(比如:接口类型, ip 地址,下一跳地址等)。

按带宽利用率 按带宽值大小

接口的均衡策略:

配置好接口组后,在

━┛ 这里选择接口均衡策略,选择"按带宽利用率"(推荐),

则将根据出口链路的负载状况调整走向,使各出口的负载维持均衡;选择"按带宽值大小",出口流量按照出口带宽比负载均衡。

3) **生效时间**:选择策略生效时间。在生效时间下拉框中列出了系统当前已配置的时间对象,您可以从中选择一个合适的时间

对象,若没有满足您要求的时间段,您可以点击后面的【时间管理】新建时间对象。

新建应用路由			×
生效时间: 所有时间 🔹 🔻	【时间管理】		/ 应用类型
			2 源和目的网段
			3 分流接口
			4 生效时间
		上一步	完成
☰ 新建应用路由	. /	×	
生效时间:所有时间 > 【时间管理】		/ 应用类型	
- -		2 分流接口	
		3 生效时间	
	上一步	完成	

#### 2. 应用路由列表:

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

应用类型名	源网段	目的网段	目的URL	分流接口名/接口组	生效时间	☑ 开启	状态	匹配顺序	管理
ffff 🔳	联通	-	P2P~sys(dns:1 2.3.3.3)	di 1	下班时间	☑ 开启	未生效 😮		编辑删除
HTTP协议	教育	-	QQ特权~sys(dns:1 2.3.3.3)	Gi0/5	晚上	☑ 开启	未生效 😮	۵ 🌡	编辑删除
-	-	-	-	aaa(di1,Gi0/5)		☑ 开启	生效	٢	编辑删除
显示: 10 🔻					▲ 首页  ▲	上一页	<b>1</b> 下一页	▶ 末页 ▶	1 确定

点击 🗐 可以查看应用组或接口组包含的应用或接口成员。

点击 ♥ 开启 可以开启或关闭某条应用路由。

状态:当前策略是否生效,对于未生效的策略,可以点击后面的 ? 查看未生效原因。

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

會 可以调整策略优先级。





3. 查看路由效果:

点击 ① 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	1名/接口组	命中连接数		
-	-	-	-	GigabitE	thernet 0/5	0		
显示: 10 🔻			ŀ	(首页 《上─页	1 下一页 ▶ 末页	1 确定		
查看应用路由效果 - Ir R http://172.18.124.72	nternet Explorer	oute detail.htm						
		ouce_occanintant			A 1 44 14			
<u>赵</u> 用类3	2名		<b>分流接口省/接L</b>	山田	命中连接	5X		
test			dialer 1		0			
P2P应用	软件		dialer 1		0			
test?	)		GigabitEthernet	0/6	0			
	<u>-</u>		OlgabitEthernet		°			

## 1.3.11.4.4普通路由

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

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

普通路由配置页面如下图所示:

应用路由	普通路由	多链路负载均衡	策略路由					
路由优先级: 第略路由、应用路由和普通IP路由都可以作为报文转发的依据。当第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: 使得到指定目标网络的数据包的传送,按照预定的路径进行。当我可产品不能学到一些目标网络的路由时,配置静态路由就会显得十分重要。给所有没有确切路由的数据包配置一个默认路由,是通常的做法。普通IP路由包括:静态路由、地址库和默认路由,其中默认路由的优先级是最低的。 十新建静态路由 十新建地址库 十新建默认路由								
目的网段	目的	的网段掩码	下一跳地址	出口	路由选路	管理		
0.0.0		0.0.0		dialer 1	主路由	编辑删除		
0.0.0.0		0.0.0.0 19	92.168.23.1	GigabitEthernet 0/5	主路由	编辑删除		
显示: 10 ▼ 条	共2条			【▲首页 ▲	上─页 1 下─页 ▶ я	惊天▶ 1 确定		

全部 全部 全部 静态路由 赴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 默认路由

可以选择只显示静态路由或默认路

由。

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

## 1. 静态路由:点击 十新建静态路由 弹出以下窗口:

■ 新建静态路由	1		×	ł
目的网段:		*		-
目的网段掩码:		*		-
路由出接口:	选择接口 🗸			
下一跳地址:		*	(接口网关地址)	•
路由选路: 越小越优先进行选路	主路由	*	(主路由最优先进行选路;备份路由-N:N值	
			完成取消	
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。

**完成** 点击________即可配置一条静态路由:

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 0.0.0.0		GigabitEthernet 0/6	10	删除
12.2.2.2	12.2.2.2 255.255.255		GigabitEthernet 0/2	备份路由-5	编辑删除
显示: 10 🗸 条 共2条	2		▲首页 ▲	上─页 1 下─页 🕨 未	页▶ 1 确定

点击

删除可以删除一条静态路由。

2.	地址库:	点击	工新建地址库	弹出以下窗口:

-	晋通IP路由-地址库配置		×	2
-	线路接口: 选择接口 💙 网络服务商		146	
	线路接口	网络服务商	删除	
i	Gi0/6	联通	删除	
		【▲首页 《上一页	1 下一页 ▶ 末页 ▶ 1 确定	

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。

**┼新建默认路由 默认路由**:点击 3.

MCI		3		>	<	t
1	路由出接口:	选择接口 🗸 🗸	]			
1	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:Nd	直	
	越小越优先进行选择	<del>9</del> )				l
ţ						
				完成 取消		

目的网段	目的网段掩码	下一跳地址	出口	路由选路	管理
0.0.0.0	0.0.0.0	5.32.2.5	GigabitEthernet 0/3	备份路由-3	编辑删除
0.0.0.0	0.0.0.0	172.18.124.1	GigabitEthernet 0/6	10	删除
12.2.2.2	255.255.255.255	1.2.24.85	GigabitEthernet 0/2	备份路由-5	编辑删除
显示: 10 🗸 条 共3条	Z,		∢ 首页 《	上─页 1 下─页 ▶ 末	□ 确定

完成

即可配置一条默认路由:

点击 可以删除一条默认路由。

## 1.3.11.4.5多链路负载均衡

选择路由出接口,输入下一跳地址,选择路由选路,点击

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

策略路由	应用路由	普通路由	多链路负载均衡		?帮助
线路负载均衡	设置				
多链路负载均衡	j: 是在多条链路上标	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(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)。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。	
Ŧ	千启/关闭: 🗹 开启	1多链路负载均衡			
	<u>【</u> 查看	负载均衡结果】			
	保	存设置			
		TRE			

点击 【查看负载均衡结果】 可以查看负载均衡的效果:

2 查看负载均衡结果 - Internet Explorer	
R http://172.18.124.54/route_pi/fast_are_view.htm	
说明:这里查看负载均衡的效果。	
远时队列的汗细后态	
出口线路	成功流数
	↓首页 《上一页 1 下一页 ▶ 末页 ▶ 1 确定

### 1.3.11.5 DNS 配置

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

## 1.3.11.5.1DNS 服务器

配置设备的域名服务器地址 , 与 PC 的首选 DNS 服务器地址类似。最多可以配置两个 DNS 服务器的地址(点击 十添加 可



保存设置 配置第二个 DNS 服务器的地址),配置好之后点击 即可。

NS服务器		
DNS服务器1:	8.8.8.8	十添加
DNS服务器2:	114.114.114.114	★删除
DNS服务器3:	192.168.58.110	★删除
	保存设置	全部删除

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

## 1.3.11.5.2正向 DNS 代理

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黑名单、排除DNS代理等功能必须先开启对应或线路的DNS代理功能; 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	
基础而置 排除DNS代理	
说明:开启DNS代理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!您开启了正向DNS代	理后,请记得在接口配置指定线路的'网络服务商'。
内网口开启正向DNS代理: Gi0/0 Gi0/1 Gi0/2 Gi0/3 外网口配置DNS信息: Gi0/4 Gi0/5	
◎配置Gi0/4线路 接口上的DNS:	
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	
<b>命中DNS</b> 黑名单的有:0 命中排除DNS代理的有:0	
命中用戶證曲的有: 命中攻載均衡的有: U	
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黑名单、排除DNS代理等功能必须先开启对应或线路的DNS代理功能 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	8;
基础配置 排除DNS代理	
选择类型: IP或IP段 * 指定IP或IP段: * 活加设置	
关型	排除DNS代理资源 管理
显示 10 ▼ 条 共0条	《首页 《上一页 】 下一页 》 末页 ) 1 确定

#### 1.3.11.6 VPN 配置

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

## 1.3.11.6.1配置向导

首次配置 VPN,配置页面如下图所示:

vpn配置			
VPN简介: 虚拟	专用网络(Virtual Private Network 简称VPN)指的是在互联网上	建立专用网络的技术。互联网上的两个节点通过VPN可以建立一条虚	認知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。
常用场景:小同 -分支 -需分	域网 <b>组成大局域网</b> 机构接入到总部VPN实现公司信息平台、资源、数据的共享 别配置:总部及分支机构的网关设备	移动用户 <b>远程办公</b> -员工回家或出差在外通过计算机接入公司VPN进行办公 -需分别配置:总部的网关设备及接入的个人终端	
帮助: 🔍 旁路音	I署VPN常见功能如何使用?		
请您根据需要使用	的场景及这台网关所处的位置进行配置: 我在分支机构 连接至总部的网络设备/服务器	現在总部         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●      <	乗援入进来

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

• 总部配置

点击右侧的"开始配置"按钮开始总部 VPN 配置,并进入如下页面:



根据公司的需求,推荐 VPN 类型,如下图





请根据具体需要勾选需要支持的协议类型,此时向导将根据您选择的协议类型,增加相应的配置步骤,如选择 PPTP 或 L2TP, 将多出"配置基本信息"和"管理用户帐户"两个步骤。然后点击"下一步"按钮进入下一个配置页面。 下图所示为"配置基本信息"页面,这个页面可以配置 PPTP 和 L2TP VPN 总部相关参数:

UPN 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建	生接进来的基本信息
客户端地址范围:	192.168.1.2 ~ 192.168.1.254 *
	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:	192.168.33.3
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
	> 高级设置
	上一步下一步

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

点击"高级设置"旁边的 🂛 按钮,将有更多的配置信息:

I 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	
本机隧道IP:	192.168.1.2 *	
本机隧道掩码:	255.255.255.0 *	
PPTP隧道状态检测:	每隔 60 秒检测—次	
L2TP隧道超时检测:	超过 600 秒无会话自动清除隧道	
L2TP隧道验证密码:	□ 开启	
允许总部访问分支内网:	☑ 开启 🕜	
分支机构隧道IP	分支机构网段	+
IP	IP 掩码	×
	F#	

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

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

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

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

允许总部访问分支内网:若希望总部能够访问分支机构内网,您必须事先规划好各分支机构拨入总部的隧道 IP 和各个分支机

构的内网网段,在这里点击 🗹 开启后,填写表格。 如果鼠标经过 😢 按钮时,会显示配置指导:

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 2. 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	<b>友机构网段</b>	+			
192.168.3.254	172.18.102.0	255.255.255.0	×			
192.168.3.254	172.18.103.0	255.255.255.0	×			

#### 填写完基本信息后,点击"下一步"按钮,进入下一个配置页面。

下图所示为"管理用户帐户"配置页面,您可以在此页面配置用户信息,对试图远程 PPTP 或 L2TP 接入本地的客户端进行用 户身份验证。 您可以选择"帐户存储在本设备"或者"已经有其它账户管理系统"。下图所示为选择"帐户存储在本设备"

的配置页面,表格中列出了本设备已配置的用户名	和密码信息,	您可以通过表格"	操作"列中的	^{無額} 和 删除	按钮对已有
的用户名和密码信息进行修改或删除,也可以在	添加分支机构	用户名:	密码:	添加	这里新增用户

名和密码。

三 VPN配置向导			×
VPN类型选择 →	配置基本信息 → 管理	閉户帐户 → 配置L2TP	IPSec → 完成
言理连接进来的用户帐户			
●帐户存储在本设备   ○ 已经补	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
٩	aa		编辑删除
显示: 10 ▼ 条 共1条		I<1 首页 <1 下	—页▶末页▶ 1 确定
	上一步	下一步	
译"已经有其它账户管理系统"	,将通过第三方服务器来管	管理用户信息,如下图所示,	选择"已经有其它账户管理系统"
点击【管理认证服务器】	,在弹出窗中共享密码和明	资务器 IP 即可。	

I VPN配置向导		×
VPN类型选择 → 面		配置L2TP IPSec → 完成
管理连接进来的用户帐户	Radius认证服务器,如税捷网络的 SAM、SMP等	
◎ 帐户存储在本设备 <ul><li>● 已经有其</li></ul>	真它帐户管理系统 😮	
【管理认证服务器】		
	上一步	

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

■ VPN配置向导						×
VPN类型进	择 → 配置基	本信息 → 管理用所	[〕] 帐户 →	配置L2TP IPSec	→ 完成	
配置L2TP IPSec参数	[					
预共享密钥:		* 😮				
总部本机ID 💡 :	🗌 勾选开启					
		🕇 高级	设置			
应用到接口:	𝖉 Gi0/4𝕊 Gi0/6	🗹 Gi0/7 💡				
IKE策略:	加密算法 DES V	飲列算法 DH组	生命周期 86400	0		
		SHA • group1 •				
转换集1:	esp-aes-128 esp	o-sha-hmac	•			
<u>*</u> ≠t染佳)•	2 dec	上—步	下步			

预共享密钥:移动用户和分支机构必需输入正确的密钥才能成功拨入;

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

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

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

下图所示为 IPSec VPN 总部相关参数的配置页面:

<b>■ VPN</b> 配	置向导						×	
		VPNš		→ 配置	PSec → 完成			
配置IPSec参	数							
预共	享密钥:			* ?				
总部本机	UD 😮 : 🛛	□勾选开启						
需经隧道	首访问的网	络配置指导						
	本地	地网段		分支机构网段		出口	+	
192.16	8.1.0	255.255.255.0		IP	掩码	请选择出口	×	
192.16	58.2.0	255.255.255.0		IP	掩码	请选择出口	×	
	→							
Ik	KE策略:加		」算法	DH组	生命周期			
			上一步		下—步			

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

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



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

移动用户 PPTP VPN					
服务器公网IP:	172.18	172.18.124.72			
配置步骤:	+ Wind	dows XP配置参	考 + Windo	ws 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:255.255.2	255.0	
转换集1:	esp-de	s esp-sha-hm	iac		
转换集2:	esp-3d	les esp-md5-l	nmac		
	序号	加密算法	散列算法	DH组	
	1	3DES	SHA	group1	
TV Faarmar .	2	DES	SHA	group1	
IKE東哈:	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:	+ Wind	dows XP配置参	参考 + Window	ws 7配置参考	

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

#### • 分支机构配置

vpn配置		
VPN简介:	虚拟专用网络(Virtual Private Network 简称VPN)指的是在互联网上建	立专用网络的技术、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
常用场景:	小局域网 <b>组成大局域网</b> -分支机构接入到总部VPN实现公司信息平台、资源、数据的共享 -需分别配置:总部及分支机构的网关设备	移动用户 远程办公 -员工回家或出单在外通过计算机接入公司VPN进行办公 -需分别配置:总部的网关设备及接入的个人终端
帮助: 😡	旁路部署VPN常见功能如何使用?	
请您根据需要	要使用的场景及这台网关所处的位置进行配置:	
	我在分支机构 達接至急部的网络设备/服务器	我在总部         使分支机构/个人终端接入进来
	开始配置	开始配置
ā击左下#	开始配置 角的 按钮 , 进入	\如下页面 ,

■ VPN配置向导				×
	VPN类型选择	$\rightarrow$	$\rightarrow$	

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 🛛	L2TP	L2TP IPSec 🔲
对传輸数据进行加密 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。	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	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。



■ VPN配置向导			×
	VPN类型选择 →	<b>分支机构配置</b> → 连接总部	
手动输入总部管理员损	供的信息		
VPN类型:	IPSec	]	
总部公网IP或域名:	www.test.com	* +多个IP或域名 🕜	
预共享密钥:		*	
应用到接口:	Gi0/7 🔻 😮		
需经隧道访问的阶	网络配置指导		
	本地网段	总部网段	+
192.168.1	.0 255.255.255.0	6.6.6.6 255.2	5.255 ×
		- ✔ 高级设置	
	上一步	下一步	

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

总部公网 IP:总部 VPN 服务器的公网 IP 地址;

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

用户名、密码:可登陆 VPN 网络的用户名、密码;

总部网络:想访问的总部的内网网段;

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

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

通过总部接入外网: 开启 ,这里如果勾选的话,分支机构正常上外网会全部走 VPN 再通过总部连接到外网, 如果不勾选的话,只有要访问那些总部内网网段的时候才走 VPN,其余流量则按照分支机构的网络出口直接连接到外网的。 设置好之后,点击"下一步"按钮,即可看到如下页面,





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

## 1.3.11.6.2VPN 配置

#### • 拓扑图显示页面

完成 VPN 配置后,可以看到如下配置页面:

vpn配置			
VPN简介:	虚拟专用网络(Virtual Private Network 简称VPN)指的是在互联网上	建立专用网络的技术。互联网上的两个节点通过VPN可以建立一条卤	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。
常用场景:	小局域网 <b>组成大局域网</b> -分支机构接入到台部VPN实现公司信息平台、资源、数据的共享 -需分别配置:总部及分支机构的网关设备	移动用户 远程办公 -员工回家或出壁在外通过计算机接入公司VPN进行办公 -需分别配置:总部的网关设备及接入的个人终端	
帮助: 😡	旁路部署VPN常见功能如何使用?		
分支机构信	息		
拓扑图	表格 所有分支机构 ▼		及指南下载 及查看vpn日志
- <b>0-</b> 添加接入总	(王)		■ 已接入 ■ 未接入
		参部1 www.test.com Ruijie (本却) IP: 172:30.73.	233

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



如上图所示的

图标。点击此图标可以查看、修改本机的 VPN 配置信

息。拓扑图中灰色线条、设备表示连接失败,绿色线条、设备、蓝色设备表示连接成功。

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

0

+

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

添加分支机构 图标,点击此图标可新增一个帐户。

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

#### 表格显示页面

vpn配置						?帮助
分支机构信息						
拓扑图 表格	所有分支机构 🗸					Ca音看vpn日志
②管理本机配置 十添加	接入总部					
当前设备共接入 0 台VP	N总部。					
设备名	是否接入	接入时间		内网IP	互联网IP	操作
总部1	6				192.168.1.2	查看
				Kĕ	页 《上一页 1 下一页 ▶ オ	転▶ 1 确定
十添加分支机构						
当前共2个分支机构,其	中有0个机构接入专网					
用户名	设备名	是否接入	接入时间	内网IP	互联网IP	操作
test		6				查看修改删除
admin2		6				查看 修改 删除
				▼▲	页《上─页 1 下─页》 я	雨▶ 1 确定
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。						

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 ②管理本机配置 按钮,可以查看、修改本机的 VPN 配置信息。点击 十添加接入总部 按钮,可以配置本机作为 VPN 分支机构,接入到多个总部。点击 十添加分支机构 按钮,可以添加用户信息。点击表格"操作"列中的 查看 修改 删除 ,可以对选中的用户进行查看、修改、删除。

• 查看本机的 VPN 配置信息

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

➡本机VPN配置信息					×
查看作为总部的配置	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:	1.2.2.2 至 1.2.2	*.254			1
总部域名:	1.2.2.2				
首选DNS服务器:	1.25.2.25	备选DNS服务器:			
本机隧道IP:	1.2.2.2 *	本机隧道掩码:	255.255.255.0	*	
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,将切换到本机作为 VPN 分支机构的配置信息查看页面,如下图所示:

						×
查看作为总部的配置	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:	12.3.3.3	* +多个IP或域名				
预共享密钥:	•••••	*				
用户名:	dd	*	密码:	••	*	~
					取消	
	不按八					

接入总部1 接入总部2 若本机作为 VPN 分支机构, 接入到多个总部, VPN 参数上方将有多个选项卡如 ,此时表示当

接入总部2 前显示的是接入到总部 1 的 VPN 配置信息,点击 将会显示本机接入到总部 2 的 VPN 配置信息。

按钮,可以对当前选中的 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	至看作为分支的配置					^
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 V					
	□开启身份验证 ?					
总部公网IP或域名:	12.3.3.35	* +多个IP或域名				
预共享密钥:	•••••	*				
用户名:	gg	*	密码:	••	*	~
		I _ I		保存	取消	
	1 THE ALL A 1					

修改完成后,点击

清空配置

保存

即可。

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

#### 移动用户信息

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

## 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。

修改配置 点击

点击 这里 将弹出移动用户管理页面,如下图所示,您可以在此页面查看、修改、删除某个移动用户信息,也可以点击

# 【用户组织管理】按钮管理移动用户。

	理				×	
【用户组织管理】			接入筛选:	用户名或IP	查询	
当前共有0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	
		ŀ	「首页 《上─页 ]	▶ 下一页 ▶ 末页	1 确定	
					取消	

#### 1.3.11.7 SSLVPN 配置

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

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

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

SSLVPN 有三种接入方式, WEB 接入、安全隧道接入。

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

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

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

> 对用户/用户组进行授权:管理员"用户授权"对指定的用户组或用户进行资源授权。

> 资源继承:用户/用户组会继承其'父组'的授权的资源;针对指定用户/用户组可以关闭继承。

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

## 1.3.11.7.1配置向导

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

SSLVPN配置	() 帮助
	什么是SSLVPN?
总部 Headquarter	<b>一项新兴的安全远程访问技术</b> 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。
Internet	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。
</td <td>开始配置</td>	开始配置

点击"开始配置"打开 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。	×
请选择SSLVPN的应用场景:	/ 部署模式
◉ 典型应用	2 基本设置
<ol> <li>1.支持web接入;</li> <li>2.支持移动终端接入;</li> <li>3.支持普诵nc安全隧道接入。</li> </ol>	3 添加资源
	4 为用户授权资源
	<b>5</b> 完成
Ŀ	步下一步

下面是典型应用应用的向导配置:
■ 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	/ 部署模式						
	射。	2 基本设置						
内网DNS:	内网DNS: 192.168.58.110 8							
用户认证方式:	用户认证方式: ◎ 本地认证 ⑨ RADIUS认证 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昵名哭管理,	Radius认证:使用第三方的RADIUS服务器认证。	5 完成						
	【自注於证版力情】							
	上一步	₺ 下─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。

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

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

🥝 认证服务器配置 - Internet Explore	er 📃 🔤 🗙
R http://172.18.124.54/web_auth_	pi/user_certific_server.htm
注意: 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Raduis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0.0	1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。
土亨宓四・	* (右冬会:);证明冬恩时,烧土田(/)廖琛)
х <del>э</del> щи.	
服务器IP:	* 认证端口: 1812 (0-65535) 计费端口: 1813 (0-65535) 十添加
保存设置	清空配置
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
服务器IP: 保存设置	* 认证端口: 1812 (0-65535) 计费端口: 1813 (0-65535) 十添加 清空配置 済空配置 ん击可添加多 个备用服务器

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

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

■ 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 😮	/ 部署模式						
客户端网段: 子网 / 掩码 * 十 1	2 基本设置						
网中的其它地方使用。	3 添加资源						
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。	4 为用户授权资源						
新建隧道资源: 🕂 添加	5 完成						
✓配置SSLVPN提供的WEB资源							
资源名称: 网址: 例如: http://xxx 或 ht 🔀 2							
	3						
上一步	步 下一步						

隧道接入资源配置:如何配置见 <u>1.3.23.4 章节</u>

客户端网段:配置WEB接入资源:

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

✓配置SSLVPN提供的WEB资源

资源名称:	网址: 例如: http://xxx 或 ht 🗙	十添加
资源名称:	网址: 例如: http://xxx 或 ht 🗙	

为用户授权:

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

	本向导将帮您快速完成SSLVPN设置	Lo		×					
提示: 当前用户组下的所有子组及包含	提示: 当前用户组下的所有子组及包含的所有用户将自动继承该组已授权的资源。								
注意:采用Radius认证时,Radius认 在组织管理中创建对应的用户并对其授	注意:采用Radius认证时,Radius认证用户默认继承所有用户已授权的资源,若要授权特定资源,请 在组织管理中创建对应的用户并对其授权。 添加或者删除选择用户(组)授权资源								
٩	admin2 已授权的资源	+		3 添加资源					
- 〇 所有用户	所有网络	×		4 为用户授权资源					
	120	×	Ľ	5 点对点配置					
● Ovpn_euser_ 个 可授权用户	▲ 当前用户(组)授权情况			6 完成					
			~						
上一步 下一步									

授权步骤如下:

★ 次迎使用SSLVPN配置的 提示:当前用户组下的所有子组 注意:采用Radius认证时,Rad 在组织管理中创建对应的用户并对。	× 1 部署模式 2 基本设置		
	admin2 已授权的资源	2+	3 添加资源
- ⊖Улаль⊢ - ⊖OVpn_Group	🧮 选择授权的资源	×	4 为用户授权资源
 eadmin2 	□全选 □目は図 □目120	3	5 点对点配置
		-	6 完成
	说明:蓝色为隧道资源	确定	~
		Ŀ	一步 下一步

- 1. 选中要授权的用户或用户组
- 2. 点击 + 将弹出未授权的资源列表。
- 3. 勾选要授权的资源,这里只列出未授权的资源。
- 5. 要取消资源授权 ,请点击 🗙。
- 6. 如果要管理用户请点击用户组织管理, 会弹出用户管理窗口。

授权完成点击下一步完成 SSLVPN 配置

■ 欢迎使用SSLVPN配置向导,本向导将帮您快速完成SSLVPN设置。	×
恭喜您,您已经成功搭建了SSLVPN!	/ 部署模式
	2 基本设置
✓ 访问SSLVPN,请点击以下链接: https://172.30.73.63	3 添加资源
	4 为用户授权资源
✔ SSLVPN客户端下载,请点击以下链接: 💈	5 完成
下载SSLVPN客户端	
Ŀ	一步 完成

1.3.11.7.2运行状态

当设备已启动 SSLVPN 服务,则点击 SSLVPN配置 时会进入"运行状态"页面。这里显示当前的 SSLVPN 服务的 运行状态,包括在线用户、用户名锁定、IP 锁定等信息,同时提供日志查看,用户搜索功能。 SSLVPN 服务正常时:

运行状态	基本设置	隧道资源管理	WEB资源管理	用户授权							? 帮助
						用户状态查询	:	查询	硬件特征码	管理 查	看日志
当前在线用户: 2刷新										€刷新	
用	户名	登录IP	登家	时间	i	在线时长	上行流量	下行	流量	操作	
显示: 8 🔻								▲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	司名用户登录连续出	1错达到指定次数后,该用	户名将被锁定			锁定IP地址:同I	9用户登录连续出错达到	指定次数后,该IP地址将	炭定		
	锁定用户名	解	锁剩余时间	操	ſſĘ	锁题	全IP地址	解锁剩余时间	1	操作	
显示: 8	•	▲ 页 番 ♪	页 1 下页	▶ 末页 ▶ 1	确定	显示: 8 🔻		《首页 《上一页 1	下一页 ▶ 末	页 № 1	确定

当 SSLVPN 服务暂停时:

运行状态	基本设置	隧道资源管理	WEB资源管理	用户授权				?帮助
			SSL	VPN服务:已暂停	启动服务	查看日志		

SSLVPN 服务正常时的说明如下:

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

	查看	sslvpn日志	i								×
E	志类型:	用户日志	▶ 日志等级	: 错误 ✔	关键字:			查询	び 号	出全部	日志
	日志类型	日志等级	时间				内容	!			
					H	「首页 ◀	上一页 1	下一页▶	末页 ▶	1	确定
1											
										1	取消

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

当设备上的日志文件超过 1M 时,设备将根据时间顺序自动删除掉早期的日志。

2	用户状态查询:	查询	可以本沟田白的左绊坐太	检》田中夕后	上十
∠.	通过		可以旦问用厂的任线状态。	11八円「白口 ,)	三日

"查询"。界面如下图所示:

	查看用户test信息	×	
	用户状态:离线	^	-
	上行流量:无		1
	下行流量:无		
	已授权的资源:无		
	硬件特征码认证: ^{关闭}	~	1
		取消	

当用户在线时,还可以进行"强制下线"操作。如果用户被锁定,这里也可以解锁。

3. 点击 2刷新 会立即刷新相应的显示数据。系统默认每 15 秒会自动刷新一次。

- 4. 点击 ^{强制下线} 会把该用户强制下线,当设备的最大并发用户数有限时,可以通过该功能来确保重要的用户优先上 线。
- 5. 点击 解锁 可以对锁定的 IP 或用户进行解锁。

1.3.11.7.3基本设置

这里提供 SSLVPN 服务的基本参数配置, 界面如下图所示:

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名 SSLVPN访问方式 SSLVPN客户端下	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 。									
SSLVP	N服务端口:	443	* (1-6553)	5)如果设备不是部署	辞在出口,请在出口设备配置	置TCP及UDP的端口映射。				
	内网DNS:	114.114.114.114	用于解析内	1部域名,存在域名:	资源时必须配置。					
用	户认证方式: ④ ((本地认证【添加本地认证用户】 Radius认证 优先本地认证 ³ 								
7	客户端网段:	2.1.2.0 / 分配给隧道接入用户的IF	255.255.255.0 2地址网段,配置前请朝	】* + 确认 <i>这些地址末在</i> 怨	汤局域网中的其它地方使用。	Ø				
DNS <u>a</u>	查询优先级: ①	• 内网DNS优先 常户端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						

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

参数说明:

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

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

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

DNS 查询优先级:

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

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

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

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

	♣ 登录 SSLVPN	
KUJJ	用户名: *	
设为首页 收藏本页	密码: *[è
客户端软件下载	验证码: RFK k 换一	张
	登录	

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

Networks	登录类型: U-KEY登录 ▼ 田户名登录
设为首页 收藏本页	用户名: U-KEY登录 *
客户端软件下载	密码: * 🖮
	登录

创建 USBKey:创建前需要下载 USBKey 控件和驱动,根据你的 pc 安装 32 位或者 64 位控件

▲ USBKey导入控件和驱动安装包下载,然后点击创建按钮【创建USBKey】,如下图创建页面

可以选择你想创建的用户:

Q		已选择的用户		^	/ 选择用户	
- 🖼 所有	5用户	log admin2	admin2			
- 🖂	^I Vpn_Group [●] I admin2	b vpn_euse	r_			
					3 创建	
				~		
			Ŀ-	步	下一步	
_						
∃ 创建	USBKey					
内置CA生	E成的数字证书				/ 选择用	
ヨ宏・	CN	血につい	Vour Department		2 記習参	
	Eulian		admin?			
	FuZhou		iohn@vahoo.cn	*	3 创建	
	Fuzhou		John@yanoo.cn			
公司:	Your Company	过期日期:	2017-10-10			
·IN码:		】* 确认PIN码:	••••	~		
	注:该处pin码为默认(

默认的 pin 码为 1234,

── 创建USBKey	×
请点击"开始创建"按钮,将用户信息写到目标USBKey中!	▲ / 选择用户
要跳过该用户请点击"跳过"按钮!	2 配置参数
当前创建用户:admin2	3 创建
PIN码: •••• 开始创建 跳过 ← 可以选择跳过该	
本次创建总数为:2个 点击开始创建	
已经创建USBKey为:0个。	
0%	~
上一步	▶ 完成

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

启用硬件特征码:

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

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

收集硬件特征码

硬件特征码认证失败,您可选择手动提交特征码或退出系统	
提父特征码」题出系统	
☑ 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) 3 【特征码管理】	
☑ 对所有用户启用自动审批 3	
	开启对所有用户
自动审批后,只要提交特征码就能自动审批,也可以手动在特征码管理【符征的管理】手动审批:	

🥖 特征码管	管理 - Internet Explo	orer	PERSONAL INC.	A CONTRACTOR OF MILES					
R http://	R http://172.18.124.54/sslvpn_pi/sslvpn_hardware_featurecode.htm								
⊘批准	X删除 特征码用	1户名:	查询	筛选:显示全部 💙					
	用户名		硬件特征码		描述	状态	管理		
					▲首页 《上一引	ī 1 下-	-页▶末页▶ 1 确定		

特征码管理还可以对硬件特征码做批量的审批和删除操作。

硬件特征码的导入和导出:

硬件特征码路径:	浏览	导入特征码	导出特征码

可以对设备的硬件特征码进行备份,以及导入方便网管的操作。

启用软键盘:开启该功能后,客户端WEB登录页面可以使用虚拟的图形软健盘进行输入密码,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健盘,如下图所示:



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

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

网关标题:客户端使用 SSLVPN 服务时网页显示的标题,如下图所示:

网关标题: SSL	VPN Service
🖉 SSL VPN Service - Window	s Internet Explorer
💽 🗢 🗷 https://172.18.3.8	11/login. html

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

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

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



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

可信客户端证书导入和导出:

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

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

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

登	录页显示你上传的logo
Duíto	▲ 登录 SSLVPN
Networks	用户名: *
设为首页 收藏本页	密码: * 📷
移动客户端下载	登录
Rujje ← 登录	在機时间:00:03:13 と后页面顶部显示你上传的logo songyihong 留修改密码 Ů選出
内丽 http://ruijie.com.cn/	

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

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

1.3.11.7.4短信策略管理

运行状态 基	本设置	短信策略管理	隧道资源管理	用户授权		
短信双因子认证: 用户 短信自助绑定功能: 月 短信自助解绑功能: 月	□账号密码校期 用户首次在一↑ 用户通过SSLV	俭通过后,SSLVPN服务看 台终端登录提交硬件特征码 PN登录页面跳转到自助制	静向用户指定的手机号码发送 吗时,服务器以短信的方式向月 跳页面、进行身份校验、下发	个动态验证码,短信动态验证码 用户发送一个动态验证码,用户提 短信动态验证码、用户提交验证	校验通过后,才允许用户登录。 交动态码并通过校验后即可自动 码、服务器校验通过后自动执行/	审批。 硬件特征码删除动作。
第一步:基本设置						
短信提供	滴: 华兴	软通	▼ 华兴软	通官网		
注册	码:		*	密码:		*
发送模	版:尊敬的	的\${username},您用]于\${func}的验证码是\${V	Code}。【SSLVPN服务】	0	
保存设置	i					
第二步:短信策略						
短信双因子认	证: 关	团 ▼	短信自助	绑定: 关闭 ▼		
短信自助解	鄉: 关(团 •	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(言验证码请求次数,0代表不	限制,默认配置为0)	
保存设置	È					
意三步:关联用户手	机					
┣ 添加关联用户手机	, X删除遗	世中			按用户名 ▼	查找 显示全部
		用户名		手机号码		操作
				无记录信息		
显示: 10 条 共	\$0条				€ 1	插页 ◀ 上一页 下一页 ▶ 末页 № 1 确定
€联用户手机导入与行	备份					
说明: 在导入关联用/	户手机时,i	请先导出 user_phone	. <mark>.csv</mark> 模板,按照user_pho	one.csv模板的格式修订后直接	接 XXX.CSV 导入即可。	
経: 选择文件 5	未选择任何	文件	导入用户 导出用	- c		

1.3.11.7.5隧道资源管理

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

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	② 帮助
	-		所有网络	局域	g 		
	添加	新的资源	默认的全网	资源			

• 所有网络资源管理

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

── 所有网络资源授权	×
说明:全网资源,用户SSLVPN登录后,所有的网络访问都经过SSLVPN转发。	
允许访问该资源的用户组 + 设置 添加用户	
Svpn_euser_ Sadmin2	
保存取消	

点击设置按钮,添加可以使用该资源的用户,弹出添加用户弹出框如下

■ 指定允许接入的用户组/用户	×
Q	已选择的用户组/用户 😵
- ➡ □ 所有用户 - ➡ ♥ Vpn_Group ● ♥ admin2 ● □ vpn_euser_	Vpn_Group
	admin2
用户组织管理	
	确定取消

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

• 添加新隧道资源



新建隧道接入资源				:	×
访问控制规则		하미호드바이에			^
		*刀口动口为3293			ľ
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 🕜 🔥 点	击展开高级设	<u>置</u>	
隧道资源描述	:				
应用程序路径	:		【选择】		
	<i>未指定应用</i> 的	程序时,该资源在。	SSLVPN登录后看	不到但实际是可用	'
程序启动参数	(:				
允许访问该资源的用户组	十设置 🔭	加授权用户			~
			保存	取消	

- 1. 当客户端通过隧道接入后,设备将为该客户端分配一个内网 IP 地址,此处就是配置可分配的 IP 地址池。所以必需要 保证这些 IP 不和内网其它 IP 段冲突,如果存在冲突客户端将无法正常使用。
- 2. DNS 查询优先级:这里优先级只对没有授予"所有网络"隧道资源用户生效,选择内网 DNS 优先,用户将使用上一步中配置的 DNS 解析地址,选择客户端 DNS 优先,用户将使用自己电脑上配置的 DNS 解析地址
- 3. 新建隧道资源:点击 十添加 添加隧道资源,弹出如下弹出框:

📄 新建访问控制	规则	×
目标类型:	网段 🗸	^
IP网段:	/ 掩码 * 注意:IP网段不允许为组播、广播、本地环回地址	
协议:	¥ 高级选项 ANY ✓	
端口:	1 - 65535 (1-65535)	~
	继续添加 保存 取消	

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

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



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

Ruffe		在线时间:00:00:04 songyihong 留修改密码 也 選出
<mark>远程桌面</mark> mstsc.exe	▲ 有填写应用程序路径时 ● 用户登录后会直接显示该资源	

4. 允许访问该资源的用户组:可以设置哪些用户有权使用当前资源,点击 十设置 添加可以访问该资源的用户:

指定允许接入的用户组/用户						
Q ● ③ □ 所有用户 ● ④ ☑ Vpn_Group ● ☑ admin2 ● □ vpn_euser_ 可授权用户(组)	已选择的用户组/用户 ❷ Vpn_Group admin2 ↑ 已授权用户(组)					
用户组织管理	确定取消					

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

对已有的隧道资源,鼠标移上,点击 × 可直接删除。

1.3.11.7.6WEB 资源配置

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	(?) 养
建议: 仅当该资	意源为允许移动接入的	网页或提供导航服务的网	顶时配置。			
		120	X			
-			2			
占土沃加\	₩ 20 20 20 20 20 20 20 20 20 20 20 20 20	占土则除汝	次酒抽北			
点 古 珍加V	WED页源地址	点 古 删 际 区	页 源地址			
_		\			-+	
山 · — — · · · · ·		添加新	的 Web 资源地	J址,理出汤	SUU11年9日 下:	
☰ 新建	web资源					×
						^
	资源访问	方式: WEB》	刘览器			
	资源	名称:			*	
	资源	网址: 例如:	http://xxx 或 h	nttps://xxx	*	
		☑ 弁:	许访问页面中的	子链接		
			1.4.2 million (1.4.2	J KLISC		
		☑ 开	启URL改写			
允许访问]该资源的用	户组:十设	置			
						•
					保存	取消

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

对已有的 web 资源可以鼠标移上,点击 × 可进行删除。

1.3.11.7.7用户授权

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

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

☰ 编辑	用户	\times
用户名称	* vpn_euser_	
IP&MAC	: OIP地址 OMAC地址 OIP和MAC ④无IP	
允许用途	: □允许做web认证用户	
	密码: •••••	
	□支持web认证和SSLVPN用户修改密码	
	□禁止sslvpn用户登录	
	确定	

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:

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	
提示: 当前用/ 注意: 采用Ra	户组下的所有子组及包 dius认证时,Radius	2含的所有用户将自动继承 认证用户默认继承所有用户	该组已授权的资源。 9已授权的资源,若要授权将	定资源,请在组织管	理中创建对应的用户并对其授	反.		
Q		vpn_euser_ E	已授权的资源			已继承	+	1
]户 p. Group	所有网络					×	
	admin2	120					×	
• •						增加和計	删除	
	212(继)							
12121		120(继)						
		已授权的	资源					
用户组织管理		带"(继)"为	9继承上级得到的资源,	不允许删除。				

授权步骤如下:

Q	Vpn_Group 已授权的资源		-
- つの所有用户 - つのVpn_Group ① つadmin2	局域网(继)	■ 选择授权的资源 ×	
	212(继)		
	120(继)		
		光明,市在头上影响次派	
四六次次常期			
用户租款官理	帝 (题) 为瑶承上级得到的资源,不允许删除。		

- 1. 选中要授权的用户或用户组 🕂 🗀 💿 五部
- 2. 点击 + 将弹出未授权的资源列表。
- 3. 勾选要授权的资源,这里只列出未授权的资源。
- 4. 点击^{确定}完成对用户(组)新增资源。

- 5. 要取消资源授权,请点击 ×。带有^(继)的资源是从父用户组继承来的。
- 6. 如果要管理用户请点击^{用户组织管理},会弹出用户管理窗口。

1.3.11.8 NAT/端口映射

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

1.3.11.8.1端口映射

端口映射包含两个映射关系,端口映射和整机映射(DMZ 主机);

端口映射如图:

说明 注意 帮助	:一般应用在將内网指定主 :若存在多出口场景,当有 : 😡 端口映射常见功能	E机的指定端口映射到全局; 存在整机服务器映射时,要翻 口何使用?	也址的指定满口上,设备性能 配置这个服务器只能从某个特涉	限制建议端口映射数量不超 定的出口出去。	过500条。				
FTP服务 十添加	☆ 開除选中		保存(如果映射的是	EFTP服务器,则映射的	外网端口要包含在FTP端	口中,多个端口用逗著	号","隔开,FTP服务器端口 基于 内网IP▼ 查询映射]最多只能配8个) :	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
	端口映射	1.1.1.1	111		111	ТСР	GigabitEthernet 0/3		编辑删除
	整机映射	1.1.1.1		2.2.2.2					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"添加",在弹出窗中进行端口映射配置。

十添加 X删除选中	添加端口映射	×	
□ 映射关系	映射关系:	端□映射 ▼ ? 参看示例	1
	内网IP:	*	
显示: 10 ▼ 条 共0条	内网端口范围:	* ~ (1-65535)	
	外网IP:	● 输入地址: *	
		 ● 使用接口地址: Gi0/5 ▼ 	
	外网端口范围:	* ~ (1-65535)	
	协议类型:	ТСР •	
		本会日の総	
		WHALE AXIFI	



内网 IP:要映射到外网的内网 IP,通常是您的服务器 IP 地址。

内网端口:要映射到外网的端口。

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

外网端口:广域网上的端口,取值范围为1至65535。

协议类型:请根据需要选择 TCP 或 UDP。

描述:端口映射的描述信息。

设置完毕后点击	确定	按钮。

Ps:可根据示例进行配置。

1.3.11.8.2NAT 转换规则

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

NAT转换规则	添加NAT地址池	端口映射	多出口映射配置	민		? 帮助			
说明:此功能是将ACL应用于NAT地址池,以实现NAT转换规则的功能。									
十添加 ×删除选中	+添加 ×删除选中								
	ACL	川表			应用于地址池				
	110	=			nat_pool				
显示: 10 ▼ 条 共1条 I 下一页 ▶ 末页 ▶ 末页 ▶ 1 确定									

ACL 列表:选择您要应用到该规则的 ACL 序号或名称。

应用于地址池:选择要作用到的地址池。

═ 添加NAT转换规则		×	
ACL列表:	22 🗸	【新建ACL列表】	
选中地址池:	nat_pool V		
		确定取消	

选择完毕后点击"确定"按钮来新增一条地址转换规则。

1.3.11.8.3添加 NAT 地址池

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

NA	T转换规则 添加NAT	也址池 端口映射	多出口映射配置		?帮助					
说明	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。									
地址池	地址池列表: nat_pool									
	序号	接口	起始IP地址	结束IP地址	操作					
	1	Gi0/1	/	/	编辑删除					
	□ 2 Virtual-ppp1 / / 删除									
显示	显示: 10 ♥ 条共2条 【《首页 《 上一页 1 下一页 》 末页 】 1 确定									

点击"添加地址池",在弹出窗中进行地址池的配置。

NAT转换规则	添加NAT地址池	端口映射	多出口映射配置				?帮
说明:地址池是指分配。	合内网用户的公用 IP 地址配	置的范围。					
地址池列表: nat_poo		十添加地址池 ×	《删除选中				
	号 → 添加地址池	+			×	操作	
□ 1 □ 2 显示: 10 V 条 共2会	地址池	名称: ④ 输入:	* Gi0/7	O nat_pool		5000000000000000000000000000000000000	确定
				确定	取消		
地址池名称 :该地址	出的名称 ,如果要	要在现有的地址》	也上添加地址 ,ü	● nat	t_pool	➤ 选择现有的地址	上池。
选择外网口:选择您	您要添加的外网口	, 此时下方会出	现如下图所示道	5项:			
Gi0/6-起始IP	'地址:		结束IPt	也址:			
输入起始 IP 地址和	结束 IP 地址 , 如	果只有一个 IP i	地址 , 那结束 IF	,和起始 IP 输入	一致即可。可	J以为一个地址池配置;	多个
IP段,IP段之间不	可以重叠。配置完	确定 記点击	进行保存。				

1.3.11.9 DHCP 配置

1.3.11.9.1服务端配置

服务	服务端配置 静态地址分配 客户端列表 ? 帮									
十添加	+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	192.168.2.1-192.168.2.25 4	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 192.168.124.1-192.168.12 4.254 192.168.124.1 永久 192.168.58.110 编辑 删除										
显示:	显示: 10 ▼ 条共3条 【▲首页 ▲ 上一页 1 下一页 ▶ 末页 】 1 确定									

● 添加 DHCP

■ 添加DHCP		×
		•
地址池名称:	* 3 参看示例	
IP分配网段:	*格式:192.168.1.0	
掩码:	* 格式: 255.255.255.0	
默认网关:	*格式:192.168.1.1	
租用时间:	 ● 永久 ◎ 租期 天 小时 分钟 * 	
首选DNS:	* 格式: 114.114.114.114	ł
备用DNS:		
Option 43 :	?	
Option 138 :	0	

服务端配置静	态地址分配 客户端列表			?帮助
+添加DHCP ¥₩₩₩	■ 添加DHCP		×	
① 点击<添加的PCF	>			操作
ap_dhcp_pc	地址池名称:	* (2)在弹出窗中填写配置项		编辑删除
net20	IP分配网段:	*		编辑删除
□ test	掩码:	*		编辑删除
显示: 10 🗸 条 共3条	默认网关:	*	末页	▶ 1 确定
	租用时间: ④	永久 () 租期 天 小时 分钟*		
	首选DNS:	*		
	备用DNS:			
	③点击<完成配置	置>提示成功后,内容会显示在列表中 完成配置 取	【消	

• 批量删除 DHCP

服务	服务端配置 ② 点音交蹦除强中DH 含它端列表 ③ 帮助										
十添加	+添加DHCP × 删除选中DHCP ②不分配的IP段 DHCP服务开关: ◎ ●										
	ap_dhcp_pool	192.168.2 1-192.		1天	192.168.58.110	编辑删除					
	net20	20.1.1.1-20.1	@ 确定要删除这些地址池吗?	1天		编辑删除					
	☑ 192.168.124.1-19 ③点击<确定>,完成删除 永久 192.168.58.110 编辑										
显示	10 🗸 条 共3条		确定取消	Ĭ∮首	页 ◀ 上一页 1 下一页 ▶	末页▶ 1 确定					
①在3	列表中选择要删除的	DHCP									

• 配置不分配的 IP 段

服务	5端配置 青	^{争态地} 也一就击<不分能的和	没>			? 帮助
十添加	DHCP X删除	选中DHCP 0不分配的IP段 DHC	P服务开关: ON			
	名称	田市谷田	野江网头	田田町石	DMS	操作
	ap_dhcp_j	三 不分配的IP段			×	编辑删除
	net20			2 在弹出窗中填写面	置项	编辑删除
	test	不分配的IP段:设置的	IIP地址将不会分配给客户。	格式如:1.1.1.1-1.1.1.30,	只填1.1.1.1代表单个IP。	编辑删除
显示	:10 🗸 条共3氪	不分配的IP段1:	-	+		・ 末页り 1 确定
		③ 点击 <完成配置 > 损	記示成功后 , 内容会显	記示该窗口中 完成	副置 取消	

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

• DHCP 服务开关

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 ②不分配的IP段 DHCP服务开关: ○N 点击 < DHCP服务开关 > 可以开启或者关闭DHCP服务									
	名称	ñ	地址范围	默认网关	租用时间	DNS	操作		
	ap_dhcp	_pool 192.10	68.2.1-192.168.2.25 4	192.168.2.2	1天	192.168.58.110	编辑删除		
	net2	0 20.	1.1.1-20.1.1.254		1天		编辑删除		
□ test 192.168.124.1-192.168.12 4.254 192.168.124.1 永久 192.168.58.110 编辑 删除							编辑删除		
显示:	显示 10 ♥ 条共3条 【▲首页 ▲ 上一页 1 下一页 ▶ 末页 ▶ 1 确定								

● 编辑 DHCP

服务	端配置静态地址分配	客户端列表						?帮助
十添加	═ 编辑DHCP					×		
							DNS	操作
	地址池名称:	ap_dhcp_pool	*				168.55.110	编辑删除
	IP分配网段:	192.168.2.0	*					编辑删除
	掩码:	255.255.255.0	*				.168.58.110	编辑删除
显示:	默认网关:	192.168.2.2	*				-页 1 下一页)	末页▶ 1 确定
	租用时间:	○ 永久 ④ 租期 1	天 0	小时 0	分钟 *			
	首选DNS:	192.168.58.110	*					
	备用DNS:							
					完成配置	取消		

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

• 删除 DCHP

服务	端配置 静态地址	分配 客户端列表			? 帮助
十添加	DHCP X删除选中DHC	P 🖉 不分配的 IP段 DHCF	服务开关: 00		
	名称	地址范围	默认网关	来自网页的消息	操作
	ap_dhcp_pool	192.168.2.1-192.168.2.25 4	192.168.2.2	58	3.110 编辑 删除
	net20	20.1.1.1-20.1.1.254		WHALSO MINATING ADALI (DIA) :	编辑删除
	test	192.168.124.1-192.168.12 4.254	192.168.124.1	· · · · · · · · · · · · · · · · · · ·	3.110 编辑 删除
显示	10 🗸 条 共3条				下一页 ▶ 末页 ▶ 1 确定

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

1.3.11.9.2静态地址分配

服务端配置 静态地址分配 客户端列表 ② 帮													
+添加静态地址 ★删除选中地址													
	客户名称	客户端IP	掩码	网关	客户端MAC	DNS服务器	操作						
	test3	54.1.2.4	255.255.255.0		0005.0004.0005		编辑删除						
	40	5.25.5.6	255.255.255.0		0002.2222.2222		编辑删除						
显示: 10 ♥ 条共2条													

● 添加静态地址

服务端配置 静态地	也址分配 客户端列	表			? 帮助
十添加静态地址×删除	·····			~	
① 点击<添加静态地址	☆川静念地址 >			X	操作
Image: block state test3 Image: block state 40	客户名称:		* ② 在弹出窗中填写配置项		编辑 删除 编辑 删除
显示: 10 🗸 条 共2条	客户端IP:		*		末页▶ 1 确定
	子网掩码:				
	客户MAC地址:		ż		
	网关:				
	DNS :				
	③ 点击<完成	配置>提示成功后,内容	会显示列表中 完成配置	取消	

• 批量删除静态地址

服务		勘除选中的静态进	⊶				? 帮助
十添加		中地址	ſ	来自网页的消息	1		
	客户名称	客户端IP			客户端MAC	DNS服务器	操作
	test3	54.1.2.4	255	② 您确定要删除吗?	0005.0004.0005		编辑删除
	40	5.25.5.6	255	③点击<确定>,完成删除	0002.2222.2222		编辑删除
显示	: 10 ∨ 条共2条			确定取消	∢首页 ∢ _	E—页 1 下—页 ▶ я	际 ▶ 1 确定
①在	列表中选择要删除	的静态地址	l				

• 编辑静态地址

服务	端配置	静态地址分配	客户端	② 帮助				
十添加	·静态地址 X		趾				×	
	客户名称	R				操作		
	test3	睿	客户名称:	test3	*			← 编辑 删除
	- 40		≷户端IP:	54 1 2 4	*			编辑删除
显示	10 ∨ 条共	2	47 Shorn .	04.1.2.4				▶ 末页 ▶ 1 确定
		子	² 网掩码:	255.255.255.0				
		客户M	AC地址:	0005.0004.0005	*			
			网关:					
			DNS:					
						完成配置	取消	

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

● 删除静态地址

服务	端配置 静态地	址分配 客户端	颍表				? 帮助
十添加	动静态地址 X删除选中	中地址			来自网页的消息	N	
	客户名称	客户端IP	掩码	网关		务器	操作
	test3	54.1.2.4	54.1.2.4 255.255.255.0		@ 确定要删除该静态地址吗?		编辑删除
	40	5.25.5.6	255.255.255.0				编辑删除
显示:	10 🗸 条 共2条				确定取消	页▶ ォ	雨▶ 1 确定
						J	

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

1.3.11.9.3客户端列表

服务	端配置 静态地址分配	客户端列表								
₽ <mark>し</mark> 把M/	AC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 20 < 条 共1条		▲ 首页 《 上一页	1 下─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。

1.3.11.9.4IPAM 主页

地址池使用情况					€ 手动刷
▲ 当前系统告答: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	地址总数	已分配地	址数		使用率
1499 ↑	380745 ↑	0 个			0%
地址池使用率top10					→ 更
	*	地址池名称	总数	已用个数	利用率
		1480	254	0	0%
1480		1478	254	0	0%
1475 1478		1481	254	0	0%
		1476	254	0	0%
1672		1479	254	0	0%
100		1474	254	0	0%
July Into		1477	254	0	0%
14/4 14/9		1472	254	0	0%
		1475	254	0	0%

11定情况								檀
9.8*	0.0%	0.0%	0.1*	0.0%	0.0%	0.1% 2↑	0.0%	0.0%
単MAC	IP+主机名	IP+主机名+接入设备	IP+MAC	IP+MAC+主机名	IP+MAC+接入设备	IP+MAC+主机名+接 入设备	IP+接入设备	动态地址 (未绑定)
沥史情况								
						±		
1.4								
0.6.4								
0.4人-								
2224								
0.2.5								

1.3.11.9.5IP 智能管理

																					地切	L池	1482	*	ip	1.6.20	07.0		
							图示:		司态在约	浅 📕	固态离	线 📕	动态分	配	接口IP	j∎ j	⊧除IP	📕 冲手	eiP		8								
0	1	2	3	4	5	δ	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	-22	23	24	25	26	27	28	29
	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		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		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		226	227	228	229	230	231	232	233	234	235	236		238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255														

IP 图 IP 表 新用户授权

自	定义显示	〒 ★ 新増固态用户	▲ 批星绑定	★删除选中	★批量加入mac黑	名单 💄 导/	和置 💆 下!	戦模板 🗳 导出数援	24				
搜索	地址池:	所有地址池	T						搜索字段 ▼ 搜索	字段值	搜索	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	۲	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+MA	2	编辑 加入mac黑名	副除	
+		0000.0000.0002	1.1.212.190	普通用户	0天0小时0分钟			固态离线	IP+MA0	2	编辑 加入mac黑名	副除	
+		0000.0000.0003	1.1.212.191	普通用户	0天0小时0分钟			固态离线	IP+MA0	2	编辑 加入mac黑名	創除	
+		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+MA0	2	编辑 加入mac黑名	創除	
+		0000.0000.0006	1.1.212.194	普通用户	0天0小时0分钟			固态离线	IP+MA0	2	编辑 加入mac黑名	離嚴	
+		0000.0000.0007	1.1.212.195	普通用户	0天0小时0分钟			固态离线	IP+MA0	2	编辑 加入mac黑名	創除	
	• 图 • 批量授	IP 表 新用户授权 权 ✓ 全部授权	✓批星删除 (2 全部删除							搜索	S	
		MAC地址	所属地址池	接入设计	备信息 VL	AN 🕯	端口索引	主机名	失败时间点	上线失败次数	授权建议	操作	
						没有找	到匹配的记录	₹.					

1.3.11.9.6业务告警

地址池耗尽	Night State							
+ 新增地址池						捜索		
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	a. K				
查看已解决的肯整								
						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 10 ▲ 条记录 10 ▲ 条记录 10 ▲ 余容 (1)								

地址池耗尽	终端迁移	IP 冲突								
✔ 批量确认								搜索	S	
□ IP地	at \$	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									
<u>青著已解决的音警</u> 地址 违耗尽 终端迁移 IP 冲突										
★ 清除选中	★ 清除月	所有						搜索	C	
. ,	中突IP	♦ 发	生时间	结束时间	接入设备IP	∲ 接入设备M	AC VLAN号	端口索引	操作	
没有找到匹配的记录										
查看已解决的	的告警									

1.3.11.9.7DHCP 配置管理

地址池管理 不分配IP										
注意:云终靖虚实机间一接入位置的场景,实机不能绑定接入位置元素,否则无法分配上线。										
DHCP服务(已开启): -										
+添加地址池 × 删除选中 MAC_OUI全局配置 ≥导入配置 圣下载模板 圣导出数据								搜索	S	
	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	
	1482	1.6.207.1-1.6.207.254	1.1.1.1	1天1小时1分钟	2.2.2.2	□ 动态	未分配		编辑删除	
	1483	1.6.208.1-1.6.208.254	1.1.1.1	1天1小时1分钟	2.2.2.2	□ 动态	未分配		编辑删除	
	1484	1.6.209.1-1.6.209.254	1.1.1.1	1天1小时1分钟	2.2.2.2	□ 动态	未分配		編輯 删除	
	1485	1.6.210.1-1.6.210.254	1.1.1.1	1天1小时1分钟	2.2.2.2	□ 动态	未分配		编辑 删除	
	1486	1.6.211.1-1.6.211.254	1.1.1.1	1天1小时1分钟	2.2.2.2	□ 动态	未分配		编辑】删除	
	1487	1.6.212.1-1.6.212.254	1.1.1.1	1天1小时1分钟	2.2.2.2	□ 动态	未分配		編輯 删除	
	1488	1.6.213.1-1.6.213.254	1.1.1.1	2天2小时2分钟	2.2.2.2	□ 动态	未分配		編輯 劃除	
	1489	1.6.214.1-1.6.214.254	1.1.1.1	3天2小时2分钟	2.2.2.2	□ 动态	未分配		编辑 删除	
	1490	1.6.215.1-1.6.215.254	1.1.1.1	4天2小时2分钟	2.2.2.2	□ 动态	未分配		编辑】删除	
	1491	1.6.216.1-1.6.216.254	1.1.1.1	5天2小时2分钟	2.2.2.2	□ 动态	未分配		编辑删除	
显示第	1 到第 10 翁	紀录,总共 1499 条记录 每页显示	10▲ 条记录				« < 1	2 3 4 5	> » 🌲 告警 (1)	
地址池管理	不分配IP									
-----------	-----------------	---------------------------------	---------------	------	-------					
+ 添加不分配IP	★ 批量删除 2 导入配置 2	下载模板 🛛 💆 导出数据			捜索					
	开始IP	$\frac{\mathbb{A}}{\mathbb{V}}$	结束IP	⇒ 描述	操作					
	192.168.1.12		192.168.1.255	-	編輯 圖除					
	192.168.1.2		192.168.1.6	-	編辑』删除					
	192.168.1.8		192.168.1.9	-	編輯 圖除					
	5.5.5.4		-	-	編輯 删除					
	5.5.5.0			-	編輯 圖除					
	88.88.8.1		88.88.8.8	-	編輯 删除					
	9.9.1.1		9.9.1.2	-	編輯 圖除					
	3.3.4.227		-	-	編輯圖除					
	192.168.1.11		-	-	編輯 删除					
	1.1.1.1		-	-	編輯圖除					

显示第 1 到第 10 条记录,总共 10 条记录

1.3.11.9.8地址池使用情况

IPAM主页	IP智能管理 业务告望	管 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	S
地址》	的 总IP援	λ.	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 >	»

1.3.11.9.9DHCP 日志

IPAM主页 IP智能管理	业务告警 DHCP配置管理	地址池使用概况 DHCF	日志 DHCP黑名单			
数据库状态: 已连接 ; LOG LOG 写入: ◎ 开启	写入状态:开启; 最大可存log数: 5/	00000个;				
历史记录 2018-09-04	▼ MAC 输入MAC	IP 输入IP	主机名 输入主机名		接入设备 输入IP或MAC VLAN 输入VLAN	靖口
事件类型 所有类型	▼ 时间 时 ▼ 时 分 ▼ 分	至时ず时分ず分(複素			
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 2	274 条记录 每页显示 10 🖌 条记录				« < <mark>1</mark> 2	3 4 5 > » go

1.3.11.9.10 DHCP 黑名单

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	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					
◆ 选	中删除 MAC地址	MAC必填, af09.af	i09.af09 备注 备注信息	,可为空	动 2 导入配置	乙下載模板 互 导出数数	ž	搜索	G
	MAC地址	过滤次数	主机名 接入设备IF	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		0	test	清空详情』删除
	8888.3333.6666	0	0.0.0.0	0000.0000.0000	0 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							

1.3.11.10 线路逃生

分三个菜单,线路流量逃生、路由流量逃生和逃生日志

1.3.11.10.1 线路流量逃生

可以一键开启,如下图配置。

.

线路流量逃生	路由流量逃生 逃生日志									
说明: 定时探测线 开启PING热 同时开启DI 配置探测目 TCP探测只 注意: 检查线路是 对接口进行	 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。 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。 									
2	线路探测: ☑ 开启									
当线路探测	则失败时: ◎ 只记录日志 ④ 关闭接口并记录日志									
开启排	开启探测接口: Gi0/3 Gi0/4									
	>>> 高级设置									
	完成配置									
支持高级选项配置:	:									
	▶ 高级设置									
行行	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DC	WN时:探测频率 3 秒 探测确认时间 60 秒									
	完成配置									

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

1.3.11.10.2 逃生日志

线路流量逃生	路由流量逃生	逃生日志	
ID	时间	类型	消息
1565	1970-01-02 10:40:17	路由流量逃生	line_quality route change disable.
1564	1970-01-02 10:37:52	路由流量逃生	line_quality route configuration 1 change active.
1563	1970-01-02 10:37:52	路由流量逃生	line_quality route Configuration 1 associate GigabitEthernet 0/3 [4].
1562	1970-01-02 10:37:30	路由流量逃生	line_quality route change enable.
1561	1970-01-01 08:01:39	线路流量逃生	line_quality track change enable.
1560	1970-01-01 08:00:42	其它类型	log database initialized.
1559	1970-01-03 01:32:50	线路流量逃生	line_quality track change enable.
1558	1970-01-03 01:32:42	路由流量逃生	line_quality route change disable.
1557	1970-01-03 01:32:37	路由流量逃生	line_quality route change enable.
1556	1970-01-01 08:00:40	其它类型	log database initialized.
显示: 10 ▼ 身	专共1565条		↓ 首页 ↓ 上一页 1 2 3 4 5 6 7 8 9 10 下一页 ▶ 末页 ▶ 1 確定

可以查看近期的逃生日志

1.3.12 无线

1.3.12.1 无线管理首页

无线管理首页包含用户信号强度分布和 AP 状态信息。



• 用户信号强度分布

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

用户信	息	历史记录	₹									
へ 返	Э	输入MAC地址: 搜									搜索	
用户	名 客户	端类型	MAC地址	IPv4地址	IPv4网速	IPv6地址	IPv6网速	连接AP	信号强度	在线时长	所在网络	操作
			38bc.1a94.d 491		上行: 17.3Kbps 下行: 304.4Kbps		上行: OKbps 下行: OKbps	锐捷1	强	0天00时03分 54秒	wzhywifi	详细 限速
			90b6.86c2.9 1d0		上行: 7.7Kbps 下行: 95.1Kbps		上行: OKbps 下行: OKbps	锐捷1	强	0天00时02分 15秒	wzhywifi	详细 限速
显示:[显示: 10 √ 条共2条 【▲首页 ▲ 上一页 1 下一页 ▶ 末页 № 1 确定											

AP 状态信息

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

<u>AP信息</u>										
←返回	X 删除所有不在	E线AP			按	按照AP名称查询 V 搜				
AP名称	在线用户数	CPU占用令	内存可用 🔷	网速 🌲	AP地址	MAC地址	所属AP组	位置	状态	操作
2						0011.0012.00 20	默认组		不在线	删除
;皮【						2244.1234.12 54	默认组		不在线	删除
破婆婆【						2244.1236.36 52	默认组	欧进萍【gggg gggggggggggg gg g	不在线	删除
我我						0012.2233.33 31	默认组		不在线	删除
显示: 10 🗸	条共4条						◀ 首页 ◀ 」	上一页 1 下一页	↓ 末页 ▶	1 确定

1.3.12.2 添加无线网络

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

● 添加 WIFI

点击<添加 wifi>, 在弹出窗中配置相关的信息。

添加无线网络		×
 説明:只支持管理RG(十添加Wifi 一 二 二 	WiFi网络名称: Eweb_33D43 加密类型: WPA/WPA2-PSK(通用版) ↓ WiFi密码: ewebwifi ☑ 显示密码 ¥ 高级配置	操作 限速 编辑 限速 编辑
显示: 10 🗸 条 共2	WiFi是否可见: 🗌 隐藏(让别人看不到,只能手动添加WiFi)	页月 1 确定
	最大无线用户数:	
	关闭网络时间: 永不关闭 🗸	
	下一步	

添加Wifi X删	除选中Wifi 🔽 修		上网配置				×			
	Wifip	关联AP组	1 🕜	无线用户VLAN ID 🕜	无线用户DHCP服务 😮	支持网络类型	操作		操作	
	Eweb	默认组	Ŧ	1	pool_Gi0/1,pool_Gi0/2,pool_(V	2.4G,5G网络都支持 ▼	× 十添加	编辑	限速	详情
1	Eweb							编辑	限速	详
						▶—#	京成配置			

加密类型

WPA/WPA2-PSK (通用版):基于共享密钥的 WPA 模式,安全性很高,设置比较简单,适合普通家庭用户和小型企业使用。 WPA/WPA2-802.1x (专业版):采用 Radius 服务器进行身份认证并得到密钥的 WPA 或 WPA2 安全模式。由于要架设一台 专用的认证服务器,代价比较昂贵且维护也很复杂,所以不推荐普通用户使用此安全类型。

网络类型切换

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

检测当前最新特征库
应用分类库版本: 2018.07.20.18.07.20(V2.0) 地址库版本: 2018.06.10.00
URL库版本: 内容审计特征库: 2018.03.14.00
QQ插件库版本: 2017.11.10.02 内容审计特征库2: 2018.07.09.01
检查特征库最新版
性征库工书
行任牛下站
下载URL库 下载应用分类库
设置自动更新
☑启动自动更新
更新时间:每天的 1 ▼ 时 5 ▼ 分
· · · · · · · · · · · · · · · · · · ·

● 删除 WIFI:

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

添加无线网络	添加无线网络 27 帮助										
说明: 1 不支持NBR设备通过便瓜交换机或非网管交换机来连接管理AP 2.不支持VRRP场景 3 不支持WEB与CLI混合配置 注意: 巳和部分手机型号,不支持中文的Win网络名称。故不建议配置中文的Win网络名称。											
+添加Wifi X豐寧选中Wifi ℃%改NBR編配置 ℃ 更改拓扑 ℃ 网络扩展											
	Wifi网络名称	关联AP组	关联的用户数	操作							
	Eweb_33EE1 默认组 圖 0 限速 编辑										
显示: 10 ▼ 券	显示 10 ▼ 条共1条 【首页 《 上一页 1 下一页 》 末页 】 1 确定										

• 修改 NBR 段配置:

点击<修改 NBR 端配置> , 在弹出窗中配置 NBR 端的通讯配置。

添加无线网络						(?)帮助
说明: 1.不支持NB 注意: 已知部分手	BR设备通过傻瓜交换机或非网管交 机型号,不支持中文的Wifi网络名称				×	
添加Wifi X册	I除选中Wii 🕑 修改NBR端配	➡ 设备通信AP的接口:	Gi0/0	•	Í.	
	Wifi网络名称	选由接口的IP·	192 168 101 1			操作
	Eweb_33EE1	2211304430	132.100.101.1	•		编辑 限速 详情
	锐捷	选中接口IP掩码:	255.255.255.0	*		编辑 限速 详情
	Eweb_33EE3	AP与设备互联隧道IP:	3.3.33.3	0		编辑 限速 详情
显示: 10 ▼ 条	共3条	AP地址池名称:	ap_dhcp_pool	*		页 1 下页 ▶ 末页 ▶ 1 确定
		IP分配范围:	192.168.101 1 至 25	*		
		首选DNS:	8.8.8.8	*		
		备用DNS:			•	

AP 与 NBR 互联隧道 IP

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

• 更改拓扑图:

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



• 查看关联 AP 组

点击"关联 AP 组"的 📴 图标 , 可查看和删除该 AP 组下属的 AP。

添加无	线网络							?帮助
说明: 1 注意: E	1.不支持NBR 已知部分手机	设备通过傻瓜交换机或非网管交换机来 型号,不支持中文的Wifi网络名称。故7	连接管理AP 2.不 不建议配置中文的	支持VRRP场暴 3.不支持WEB与CLI混)Wifi网络名称。	合配置			
十添加W	/ffi X删除	选中Wifi 🕑 修改NBR 端配置 🛛	29 更改拓扑 2	3 网络扩展				
		Wifi网络名称		关联科	P组	×	联的用户数	操作
		Eweb_33EE1		默认组	1 📷		0	编辑 限速 详情
		锐捷	☰ " 默认				0	编辑 限速 详情
		Eweb_33EE3	序号	AP名称	在线状态	操作	0	编辑 限速 详情
显示: 1	10 ▼ 条共	3条	1	232	不在线	删除	《首页 《 上─页 1 下─页 》 >	抹页 ▶ 1 确定
			2	44	不在线	删除		
			3	443	不在线	删除		
			4	4444	不在线	删除		
			5	ccc	不在线	删除		
			显示: 5	▼ 条 共11条 【 首页 《	上─页 1 2 3 下─页 ▶ オ	両】 1 确定		

限速:

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

91-	'\$X		J#TF			
			限速	编辑		
	限制下载:	12	×8kb/s	编辑		
E-	限制上传:	74	×8kb/s	确		
	保存	不限	速	-		

1.3.12.3 AP 管理

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

? 帮助

AP管理

说明:只支持管理RGOS 11 x版本的AP / 不支持从10 x升级到11 x。11 x软件版本可以通过官网 http://www.rujjie.com.cn/fw/r//下载;具体支持的AP型号可以通过【查查支持AP型号】获取或者拨打免费客户热线
4008 111 078咨询获取。

AP组列表	添加组	AP组名										
🖃 📄 所有AP组		1 7de/de										
🗋 默认组	Ø		AP名称	IP地址	MAC地址	所在位置	当前状态	在线用户	流量(kbps)	操作		
━ 中国			232	-	0002.0002.0021	-	不在线	-	-	编辑		
			44	-	0002.0002.0044	-	不在线	-	-	编辑		
			443	-	0002.0002.0025	-	不在线	-	-	编辑		
			4444	-	0002.0002.0026	-	不在线	-	-	编辑		
			CCC	-	0032.0002.0020	23	不在线	-	-	编辑		
			fdsdfs	-	0003.0020.0020	-	不在线	-	-	编辑		
			fsdfd	-	0002.0002.0003	ff	不在线	-	-	编辑		
			fsds	-	0002.0002.0030	33	不在线	-	-	编辑		
			ree	-	0002.0002.0034	-	不在线	-	-	编辑		
			rrr	-	0002.0002.0028	-	不在线	-	-	编辑		
		显示:	10 ▼ 条共11	条			▲ 首页 《 上一页	页 1 2 下一页	▶ 末页 ▶ 1	确定		

● AP组

在左边 AP 组列表中,可以添加、编辑和删除 AP 组。

AP管理	添加AP组									
AP组列表	添加组	AP组名 十添加	i:tesxt IAP <mark>X</mark> 删除AF	。 ②重启AP	③ 恢复出厂设置	8				
■ M有AP组 ■ 默认组			AP名称	IP地址	MAC地址	所在位置	当前状态	在线用户	流量 (kbps)	操作
🗀 tesxt 编辑	IAP组 ← 🗹 × J		2	-	0011.0012.002	-	不在线	-	-	编辑
	删除AP组		; 皮【	-	2244.1234.125 4	-	不在线	-	-	编辑
		显示: 10 ♥ 条共2条							确定	

● 添加 AP

点击左边列表中的<添加 AP> , 在弹出窗中填写配置项 , 点击<完成配置>。

AP管理 AP组列表	添加组	AP组名:tesxt	
 ■ 所有AP组 ■ 默认组 ■ tesxt 	C ×	★添加AP ※動除AP ②重启AP ③恢复出厂设置 添加AP ※ 添加AP ※ 本書目の ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	編編
		完成配置 取消	

• 删除 AP

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

AP管理										
	添加组	AP组名 十添加	:tesxt IAP X删除AI	▷ ②重启AP	③ 恢复出厂设置	1				
□ □ M ¶ A P 组 □ 默认组			AP名称	IP地址	MAC地址	所在位置	当前状态	在线用户	流量 (kbps)	操作
iesxt	ĭ×		2	-	0011.0012.002 0	-	不在线	-	-	编辑
			; 皮【	-	2244.1234.125 4	-	不在线	-	-	编辑
	显示 10 ▼ 条 共2条 【 首页 《 上一页 1 下一页 》 末页 1 3 确定									

• 重启 AP

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

AP管理				
AP组列表 添加组	AP组名:tesxt			
- 🗀 所有AP组	+添加AP ★删除AP シ重启AP	シ恢复出厂设置		
📄 默认组	☑ AP名称 IP地址	MAC地址 所在位置	当前状态在线用户	流量 (kbps) 操作
⊑ tesxt ℤ ×	2	0011.0012.002	不在线 -	- 编辑
	☑ ;皮【	2244.1234.125 4	不在线 -	- 编辑
	显示: 10 V 条 #2条 来自网页的消息			页▶末页▶ 1 确定
	2 是否确认3	更重启选中的AP?(不在线的AP,重启 确定	环生效) 取消	

• 恢复出厂设置

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

AP管理	
AP组列表 添加组 □ □ 所有AP组	AP组名:tesxt 十添加AP X删除AP ②重字 ②恢复出厂设置
□	☑ AP名称 IP地址 MAC地址 所在位置 当前状态 在线用户 流量(kbps) 操作
Etesst 🗹 🗙	☑ 2 - 0011.001 .002 - 不在线 编辑
	★自网页的消息 显示 10 2 是否确认要恢复选中的AP?(不在线的AP,恢复出厂设置不生效) 1 下一页 ▶ 末页 ▶ 1 确定
	強定 取消

• 支持的 ap 型号列表

支持的AP型号列表			×
AP型号	硬件版本	支持软件版本	
RG-RAP120	V1.00	1	1
RG-RAP220	V1.00	1	1
RG-RAP220(E)	V1.00	1	1
显示: 10 ▼ 条共3条	◀ 首页 ◀ 上一页 1	下一页 ▶ 末页 ▶ 1 确定	1
			1
			1
			1
			-

1.3.12.4 AP 升级

● 单个 AP 升级

	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─页 1 下─	页 ▶ 末页 ▶ 1 确定
选定列	l表中需要升级的 A	.P , 点击 <mark>升级</mark> , ィ	王弹出窗中上传软件版本 ,	开始升级 ,	完成单个 AP 的升级配置。
P名称		产品型号	mac地址	当前版本信息	操作
脱捷 [·] ♪ 子				级取消升级	X <u>升级</u> 页
	文件名	文件大!	修改日期	操作	
	显示: 10 🗸 务	€ 共0条	(首页 《 上一页 下-	─页 ▶ 末页 ▶ 1	确定

● 批量 AP 升级

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

AP升级									
▲ 上传软件版本 AF	○批量升级: ○N								
AF	软件版本				×	操作			
	上传文件:		浏览 开始上传 1	取消上传					
显示: 10 🗸 :	文件名	文件大小	修改日期	操作	上一页	下一页 》 末页 》 1 确定			
无记录信息									
	显示: 10 🗸 条 共0条	Į	(首页 《 上一页 下一页)	▼ 末页 ▶ 1 确定					

1.3.12.5 DHCP 安全

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

DHCP安全	
说明:开启该功能,将只允许值任端口的DHCP调应,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DH	CP动态分配IP环境下的ARP主机欺骗和源IP地址的欺骗。
DHCP安全: ON	
防止WIFI下IP冲突:	
信息列表: 【查看DHCP安全信息】 【查看合法用户信息】	
保存设置	

1.3.12.6 反制非法 AP

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

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: 主动发现网络中未线	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:	ON [1] 【扫描到所有的相邻AP】 [1]
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

查看被反制的非法 AP 列表,

~ 100	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2				<u> </u>
反制模式: 检测到非同一AC设备	备的AP设1 ▼ 每一分钟刷新一次	▼ 清空非法AP	基于WiFi名称重	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 🛚 🔤	确定

添加信任设备列表

反制非法AP配置	要被反制的非法AP列表	信任设备列表	
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(原任役者
信任设备MAC地址:			
	十增加MAC地址		
	▶ 信任厂商列表		
保存设置			

1.3.12.7 黑白名单

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

黑白名单		後 / fn , 信息时间, 1994年11月1日187 , 1991 A / 494 A /	
17549.		אראייאטאיידער (אפא-אראפין אראיינער אראפיידער איזער אראנער אראנער איז אין און און און איז אין איז און און און א איז איז איז איז איז איז איז איז איז איז	
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)	
十添加	黑名单 🗙 删除选中黑名单 🗹 批量导入黑名单		基于MAC地址查询 搜索
	用户名	MAC地址	操作
	wewe	0000.0001.0001	编辑 删除
	fff	0000.0001.0004	编辑 删除
		0002.0002.0001	编辑 删除
		0002.0020.2020	编辑 删除
		0002.0020.2021	编辑 删除
		0002.0020.2023	编辑 删除
		0002.0020.2024	编辑 删除
		0002.0020.2077	编辑 删除
		0002.0020.2078	编辑 删除
		0002.0020.2079	编辑 删除
显示:	10 ▼ 条共18条		< 首页 < 上一页 1 2 下一页 ▶ 末页 ▶ 1 确定
【基	TWIFI控制无线用户上网】 清除所有黑名单		

1.3.12.8 禁止内网互访

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

禁止内网用户互访	
说明: 在不影响用户正常上	_网的情况下对用户进行隔离,使之不能互访,保证了用户业务的安全。
禁止内网用户互访:	ON
用户类型:	☑连接同个AP的用户 ☑连接同个AP相同Wifi的用户
允许互访的用户MAC:	用户名: MAC地址: 0002.0220.0002 × +添加
	保存设置 清除设置

1.3.12.9 WIS

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

说明: 接入WIS云,即可拥有- 项目接入流程只要点击登录 【 WIST市访问地址: http://wispi.n	一键诊断,一键网优和 WIS官网】 到wis注册 uijie.com.cn	移动运维服务 。 帐号界面即可实现	┨──步步引导式完全	全自助接入wis,	10分钟内搞定!		
网优功能:	OFF						
WIS π 项目接	该 入流程						
く 注册WIS账号	本地接入 本地接入 で ご 読 授入	ジ 项目信息补充	添加AC MAC	於 AC上配置	学会 绑定微信账号	or 使用wis n	
wis.ruijie.com.cn			r	设备上操作	微信 锐捷无线百科	WIS Π 访问地址 /微信查看网络	

1.3.12.10 负载均衡

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

负载	均衡				② 帮助	
说明: 衡的作 举例:	说明:在无线网络中,如果有多台AP,并且偏号相互覆盖。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,当前配置词值2个。这两个AP间用户数差5个,大于词值,因此后续用户会关联到AP2上。					
十添加	均衡组 X删除选中均衡组					
	均衡组名	类型	阀值	组内AP成员	操作	
	3223	按照关联用户数均衡	3 个	2323	编辑删除	
	3223e	按照AP流量均衡	500 kbps	sfdsdf,ccc,fsdfd,232,44,443,4444,fdsdfs,f sds,ree	编辑 删除	
显示:	10 ▼ 条 共2条			《首页 《 上一页	1 下─页 ▶ 末页 № 1 确定	

1.3.12.11 无线开关

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

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

无线管理首页	无线开关
添加无线网络	说明:无线开关控制设备能否直接管理AP设备,并发出无线wifi.
AP管理	注意: 升启尤线升天之后,需要到【漆加尤线网络】 去部署网络,才能管理AP开发出尤线WiFi
AP升级	无线开关:
DHCP安全	
反制非法AP	
黑白名单	
禁止内网互访	
负载均衡	
无线开关	

无线开关	
说明:无线开) 注意:开启无线	关控制设备能否直接管理AP设备,并发出无线wifi. 线开关之后,器要到【添加无线网络】去部署网络,才能管理AP并发出无线WiFi
Я	无线开关: ON

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

无线开关	(? 帮助
说明: 无线开关控制设备能否直接管理AP设备,并发出无线wifi. 注意:开启无线开关之后,需要到【 <mark>添加无线网络】</mark> 去部署网络,才能管理AP并发出无线WiFi	
无线开关:	

1.3.13 防火墙

1.3.13.1 防攻击配置

1.3.13.1.1防攻击开关

防攻击开关 全局防护 协议类策略 域策略 防攻击功能: <td< th=""><th></th></td<>	
防攻击功能: ☑ 开启 防攻击功能模式: NAT ▼	
保存	

1.3.13.1.2全局防护

防攻击开关	全局防护	协议类策略	域策略		
说明: 全局防护等	師用于保护防火墙自	身免受外部攻击, 该策	略对当前虚拟防火墙有多	效。	
全局防护策略学	3				
● 未开启(建	议您先进行自学 习	后再配置策略!)	◎启动学习	学习周期 天 (3~60, 默认73	F)
防TCP SYN Flo	od攻击				
☑ 防火墙的S ¹ 阈值 防护策	YN报文总速率检查 信用syn-c	ookie	pps *		
□ 防火墙的TO 限制防火墙的会	CP半连接总数检查 话建立速率				
 限制所有T(CP会话建立速率				
🗌 限制所有U	DP会话建立速率				
🗌 限制所有IC	MP会话建立速率				
📄 限制除TCP	/UDP/ICMP外的非	其他协议的会话建立	速率		
确定	刷新				

1.3.13.1.3协议类策略



1.3.13.1.4域策略

说明:每个防攻击城运行各!	自独立的城镇略,这些策略包括:防洪	火攻击,防扫描,流量探刺,流量深刻,合适连接强速,黑白名单等。	
攻击域列表	域策略配置		
新建城 其前除远中城	描述		1 配置
859	保护主机范围	1.1.1.1	プ配置
	防护策略目学习	① 未开启(建议您先进行自学习后可配置策略!) 学习周期 天	◎ 启动学习
	TCP Flood 防护	0 ≭ 8. <u>8</u>	》配置
	UDP Flood 訪評	θ ≠£cm	产配置
	ICMP Flood 防护	0 +8. <u>∎</u>	PER
	其他协议 Flood 防护	●未起置	が配置
	防扫描	9 未配置	PER
	流量监控	●未記表	が配置
	流量限制	θ ≠£ <u>π</u>	》配置
	会话连接限速	④未配置	命配置
	白名单	✓已添加0条	》 配要
	黑名单	✓已添加0余	》配置
	攻击日志	✓已开启所有日志	产配置

点击



■ 新建防攻击域	配置向导		×
基本配置			/ 基本配置
防攻击域名称	test	*	2选择策略
描述	测试		
保护主机范围	1.1.1.1	添加 *	
	1.1.1.1/255.255.255.255	A	
		⑦ 双击可移除选中项	
		Ŧ	
点击下一步			下一步
	配置向导		×
选择策略配置方式			/ 基本配置
策略配置方式	 自动学习策略 学习周期 	天 (3~60, 默认7天)	2选择策略
	◎ 手动配置策略		
◆自动学习策略: ◆手动配置策略:	设备通过一段时间的学习,可 直接手动配置防御策略。如果	以给出针对此网络防攻击域较为合理的策略配置建议。 您对域内流量已有充分了解,您可以选择手动配置策略。	
		上一步	完成配置

点击完成配置

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

防攻击域列表	域策略配置			
◆新建城 ¥删除选中城	描述	测试		₽配置
10 859 10 aaa	保护主机范围	1.1.1.1		/ RE
1 test	防护策略自学习	· 感运行故障(原因:ace conflict - 85	91.)	
	TCP Flood 助护	0 *RE		PRE
	UDP Flood 855P	0未配置		が配置
	ICMP Flood \$539	●未配置	点击配置可以进行相关参数配置	が配置
	其他协议 Flood 防护	④未配置		₽ 配置
	防扫描	日末配置		PRE
	流量监控	● 未配置		产配用
	洗量限制	◎未配置		が配置
	会话连接限速	日 末配置		●配置
	白名単	✓已添加0条		/ 配置
	黑名单	✓ 己添加0条		学配置
	攻击日志	● 未配置		PRE

✖删除选中域

点击

, 可以删除选中的域

1.3.13.2 安全域配置

1.3.13.2.1安全域开关

安全域开关	安全域	全局策略配置	域策略配置				
安全域功能: 🗹 开启							
		保存					

1.3.13.2.2安全域

				-						
友全域名称 :		安全城等级		11 iii	≷ 間新 登示:default	定全域不能删除				
安全域名称	保护等级		保护IP范围	根据参数	查询	透明IP范围	允许区的	司内互访?	描述	擾
default								F.		
显示: 10 • 条共	1余						「「前面」(」	一页 1	下页) 末页)	1
F IP 创建	方式 _{安全域}	全局策略能置	城策略配置							
	方式 _{安全域} 前安全域的群	 全局策略配置 方式: IP 初期後 安全域数85: 	城策略配置 融方式	青海	♪ 製紙 提示:default €	全國大統領領				
F IP 创建 全域开关 全域管理 当 の 全域管理 全域管理 全域管理 全域管理 全域管理 全域管理 全域管理 全域管理 全域	方式 _{安全域} 前安全域の間	全局策略配置 功方式: IP 切换命 安全域等级:	城策略配置 離方式	查询	② 期新 提示cdefault 委	全成不能删除	A14210			*
于 IP 创建 ^{全域招供} ^{全域招聘} ^{全域名時}	方式 _{安全域} 前安全域的群 保护等级	全局策略配置 方式: IP 安全線等度:	城市部配置 Mac方式 保护IP范围	查询	② 期款 提示cdefault 受	全國不能開除 这卷明界和國	九件区向	内互访?	描述	+ 1911



📄 创建IP安全域		×
IP安全域配置		
安全域名称:	test_ip *	
描述:	测试创建方式IP	
保护主机范围	8.8.8.8 添加	
	8.8.8/255.255.255.255	
	⑦ 双击可移除进行	时 项
	Ψ	
例外主机范围	添加	
	1 双击可移除进	钟项 🔹
		确定取消
安全城开关 安全域 全局	第曲記畫 域界動記畫	
安全感管理 当前安全感创建方式:	IP UNRABILISSC	
安全域名称: 5	安全線等級: 査询 💦 🥏 刷新 提示:default 安全域不能影响	◆添加

安全域名称	保护等级	保护IP范围	违例IP范围	允许区间内互访?	描述	操作
default				否		
test_ip		8.8.8/255.255.255.255	50 24 56 35 A 1.0	香	例试创建方式IP	编辑 删除
元 10 • 条共	2条		新建的安全域	目前页 4 上一页 1	下页 ▶ 末页 月 [1 2

可以进行编辑、删除操作



📃 切换安全域创建	建方式	×
	请选择安全域建创方式	
	◎ IP地址	
	◉ 接口	
	确定取消	肖
基于接口创建方式		

文主國自定	当前安全域创	建方式:接口 切線	Jr. eC(1819)			
安全域名称:		安全域等级:	查询 🧟 剧新 提示cdefault 安全域不	45893A		+ 添加
安全域名称	保护等级		保护VLAN范围	允许区间内互访?	描述	湿作
	Gigabi	tEthernet 0/1,GigabitE	thernet 0/2,GigabitEthernet 0/3,GigabitEthernet 0/4,GigabitEth	hernet 0/5,GigabitEthern		1015



接口安全域配置			
安全域名称:	test_接口	*	
描述:	测试基于接口创建方式		
配置接口:		A	
		请选择 ————————————————————————————————————	
		-	
① 双击可移除选	沖项		
安全域等级:	(1-100)		
		協会	田澤
		WHAL	4X/F

▶ 防火墙保护的vlan或接口信息 ● 按□信息 ● GigabitEthernet 0/1 ● GigabitEthernet 0/2 ● GigabitEthernet 0/3 ● GigabitEthernet 0/4 ● GigabitEthernet 0/7 ● AggregatePort 1 ● MagregatePort 1

📃 创建接口安全地	或			×
接口安全域配置				
安全域名称:	test_接口 *			
描述:	测试基于接口创建方式			
配置接口:	GigabitEthernet 0/1 GigabitEthernet 0/2	▲ 请选打	¥	
① 双击可移除进 安全域等级:	中项 88(1-100)	点击社	确定	双消
交全域开关 安全域 全局策略 安全域管理 当前安全域创建方式:接口 安全域 安全域名称: 安全域 安全域	2回			◆ 7≅∆⊓
安全域名称 保护等极 default GigabitEthernet 0/3 test_接口 88	保护VLAN改图 GigabitEthernet 0/4,GigabitEthernet 0/5,GigabitEthernet 0/6,GigabitEthernet 0/7,Agg t 1 GigabitEthernet 0/1,GigabitEthernet 0/2	大许区间内互访? gregatePor 否 否	描述 詞试基于接口创建方式	操作 编辑 網辑 删除

可以进行编辑、删除操作

1.3.13.2.3全局配置策略



1.3.13.2.4域策略配置

基于 ACL 配置域间策略

BC-910 default											
upper uerault	• 目的安全域: 。	iefault 🔻	査約 27日	INT						◆向导添加	× 1919/97/2
□ 序号	源安全域	目的安全域	引用的ACL撤赠	源IP范围	目的IP范围	传输协议	源城口	目的城口	生效时间	設活状态	操作
					无记录信息						
显示 10 • 条共	0祭								「村前页()」	L-፬ 下-፬ ኦ ቋ፬ ነ	1 动动

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

点击下一步

📃 创建安全域策略	Š.				×
安全域IP范围策略西	記置			*	/ 策略基本配置
源IP范围:	5.5.5.5		添加	I	2 IP范围策略
	5.5.5.5/255.255.255.255	*		L	
			⑦ 双击可移除选中项	L	
		Ŧ		L	
目的IP范围:	6.6.6.6		添加	I	
	6.6.6.6/255.255.255.255	*		L	
			⑦ 双击可移除选中项	L	
		Ŧ		l	
传输层协议:	icmp •			l	
选择生效时间:	所有时间 ▼ 时间段管	理		-	
			上一步	ЦУ	完成配置
点击完成配置					

安全域策略积害

原安全如	R: default	• 目的安全域	l: default •	童術 4	「用的行						+	的导体加 🗶 删除所行
	序号	源安全域	目的安全域	引用的ACL策略	源IP范围	目的IP范围	传输协议	源端口	目的端口	生效时间	激活状态	操作
•	111	default	default		5.5.5.5/255.255.255. 255	6.6.6.6/255.255.255. 255	icmp			any	激活	2 2 2 新 不敢活 修改 删除

可对安全域策略修改、删除、激活/不激活、复制操作 基于对象配置域间策略

当前域策略配置方式 每于ACL起量地用 安全域策略配置 	刀换: 截略 ⑧ 墨于对象起	量地间策略								
查询项: 源域	▼ 关键字:		查询						◆添加	★ 删除所选
□ 移动 攻号	; 281d	日的城	源IP地址	日的IP地址	服务	时间的	动作	描述	\$\$ \$\$	操作
				无记录	信息					
显示 10 • 条共09	ŧ						I	() 页首)	七一页 下一页 🕨	初日 1 初日



策略配置 同步	安全域 重置配置数据	客	
源安全域:	test_接口	T	
目的安全域:	default	v	
序号:	123		
描述:	基于对象配置		
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 Open	y	
时间段:	白天	•	时间段管理
启用策略:	✔ 启用		

点击确定

0 8	FACLE	置成的策略	· #FX#R	臺城司策略								
全域策	略配置	R										
查询项:	源均	z •	关键字:		血的	2° 18185					+添加	×删除所选
8	助	序号令	源域	目的域	源IP地址	目的IP地址	服务	时间段	动作	描述	秋恋 \$	操作
9		123	test_接口	default	any_address	any_address	any_service	day_time	permit	基于对象配 营	◎禁止	修改 心复制 删除

可对域策略进行修改、	复制、	删除操作

1.3.13.3 防攻击域状态监控

1.3.13.3.1域运行状态

2 自动刷新 2 刷	WT				
攻击域列表	基本状态				
859	城省	859			
aaa	描述				
test	状态	✓ Running			
	保护主机范围	1.1.1.1			
	保护主机数	0 个			
	监视外部主机数	0 个			
	流量统计	清空流服统计			
		流量分布圈		异常流量分布圈	
			■ 转发流量 回应管流量 ■ 降常流量		■ 黒谷单舌包 流量現制舌包 ■ 減策報舌包

1.3.13.3.2当前攻击行为

AND TO THE PARTY OF	当期攻击打对		CUI LINE?	1037C-1001Late.201418							
防攻击域列表	ې	当前域名:	: aaa								
859	t/	议类型	attack	 攻击关型 	全部		音词	の思新			
2 aaa 2 test	满足	条件的记录	戰戰共0条。					10			
		开始时间	ด	类型	攻击蛊	防护策略	攻击峰值(Se	can攻击没有单值)	防护解除时间	网络/当前值	详细
						无记	發值息				
	显示:	10 * 余	. 共0条						4首页 4 上一到	5 下一页 1 末页 1	1 确
	量示。	10 * 余	: 共0余						N 前页 4 上一部	5 下一页 1 末页 1	1

1.3.13.3.3攻击日志

攻击域列表	日志						
Ø859 Øaaa Øtest	当前域名: 859 历史攻击次数: udp攻击次数: 0 icmp攻击次	数: 0 other-protocol政	击次取:0 tcp-auth政击;	政: 0 tcp-un	auth政击次数: 0	مور الدرين الم	V. C
	攻击时间	到	▶清除則间	_ 8	清空所有日志 与	出当时食	间日志
	协议类型 attack • 攻击类型	全部	• <u>1</u> 10		精空日志 导出日	志	
	满足条件的记录数共0条。						
	830-7	类型	攻击流	防护措略	攻击峰值(Scan攻击没有 峰值)	详细	操

1.3.13.3.4防火墙流量查看

运行状态 当前现	攻击行为 攻击日志	防火墙流量查看	
i ilizhanari 📿 anari			
村列表	全局防护统计参数	清空波星统计	
全局防护统计	流量信息:		
會体态开境计	接收数	0	
	丢弃流数	0	
	具体策略丢弃信息:		
	原认证失败会话限速		
	UDP协议会话限速	0	
	其他协议会话限速	0	
	具体策略应答信息:		
	TCP防伤策略syn报文限速	0	
	TCP防伤策略会话总数限制	0	

1.3.13.4 安全域状态监控

1.3.13.4.1安全域运行日志

默认显示当天数据

域行为统计信息(近 自确访问次数:1050	30天): udp拒绝访问次数:	1245540 icmp#	编访问次数: 3760	08 減低的収容	#香酒编访问次数:(
允许访问次数:0	udp允许访问次数:0	lcmp允许访问次数	: 0 其他协议类	重允许访问次数	: 0					
时间: 2018-06-12	2 00:00 结束时间:	2018-06-12 24:0	0 清空时间	协议类型: 3	新选择协议 · 谭	P:				
P:	2	R2M⊡: (0	-65535) EBDan		(0-65535)	词 清空日表	5 9 3380	55		
开始时间	结束时间	协议	201P	目的IP	源端口	目的端口	源安全域	目的安全域	动作	操作
					无论获得思					



1.3.13.5 IP 资源

1.3.13.5.1主机地址

161ā: 28	ς ▼ 关键字:	查询 名制新		+2	あわれ 米田秋月
1	名称	IP III LL	描述	状态 章	操作
9	kkkk	4.5.6.7		未使用	修改 脑神
wqeqwe		5.8.8.8		未使用	1822 Bile

可进行添加、修改、删除、查询、刷新操作

点击 🕂	家力口						
主机地址	范围地址	子网地址	地址组配置				
名称 描述 IP地址			* 添加	* 5可移除选中项			
					确定	取消	




点击删除

査慮項: 名称 ・	关键字:	1		即国家	+:8	10 米田(時余
8	名称		IPI8址	描述	秋香辛	操作
8	kkkk		4.5.6.7		未使用	修改 删除
•	wqeqwe		5.8.8.8		未使用	修改 删除
	例成 8.8.8.8,8.8.8.9			我修改了描述信息	未使用	修改 删除
机地址 范围地	址 子网地址	地址相配置				
机地址 范围地 普询项: 名称 • 关	址 子闷地址 罐字:	地址由起版	ध्य दिक्षा	己删除选中项	+10	加 米删除好
机地址 范围地 和词项: 名称 • #	12 子向地址 12 子向地址 12 存 名称	地址用起版	199 マ 和明 IP地社	己酮除选中项	+:5 #8≎	100 ×田田分 接作
Пара: 287 • э	址 子岡地址 電手: 名称 wqeqwe		19日 で 第8時日 19地址 5.8.8.8	己删除选中项 描述	◆添 状态◆ 未使用	(カロ) 米 世(1995年 最大作 4年2次 世(1995年
6.1 6.1 6.1 7.1 </td <td>地 子网地址 出す: 名称 wqeqwe 遊試</td> <td>104:06E</td> <td>19日 で 第8時日 19地址 5.8.8.8 8.8.8.8.8.8.9</td> <td>已剩除选中项 施述 我终议7编述信息</td> <td>◆/& 秋恋令 未使用 未使用</td> <td>加 ¥田時刊 操作 修改 部時 修改 部時</td>	地 子网地址 出す: 名称 wqeqwe 遊試	104:06E	19日 で 第8時日 19地址 5.8.8.8 8.8.8.8.8.8.9	已剩除选中项 施述 我终议7编述信息	◆/& 秋恋令 未使用 未使用	加 ¥田時刊 操作 修改 部時 修改 部時
机地址 范围地 師順语: 名称 ▼ ∮ 〕 〕 元 15 ▼ 衆 共2祭	批 子网地址 翻字: 名称 wqeqwe 游戏	#2#86度 章	19日 で 第8時日 19地址 5.8.8.8 8.8.8.8.8.8.9	已删除选中项 施述 我嫁改7强遗信意 14首页 4 上一页 1	◆添 秋志◆ 未使用 未使用 1 下一员 > 末页	加米田(約) 操作 修改 田(約) 修改 田(約) 利 1 2
九地址	批 子网地址 翻字: 名称 wqeqwe 游戏	加加的範疇	19日 で 第8時日 19地址 5.8.88 8.8.8.8.8.8.9	已删除选中项 施述 我嫁衣7强遗信息 注言页 《上一页 1	◆28 秋む◆ 来使用 来使用 1 下一页 > 来页	加 業期時期 様式 新聞 ド 1

查询项:	名称 ▼ 名称	关键字			I	查询	≈ 刷新	点击刷新数据
	IP地址 描述	Ê	3称	输入关键字可	过滤查试	旬	IP地址	
	畑坯	wqe	eqwe				5.8.8.8	1
		沨	则试				8.8.8.8,8.8	.8.9
显示: 15	▼ 条 共2翁	R						

1.3.13.5.2范围地址

to sub-st	RENACTE	1 Manager	AD-IL-CONVER				
1) 1) 1) 1) 1) 1) 1) 1) 1) 1) 1) 1) 1) 1			2 IG (2 10)			◆源加	★删除所选
1	名称	\$	地址范围	得餘地址	描述	状态令	操作
8	测试1		7.7.7.7.7.33		房试描述	未使用	修改 删除

可进行添加、修改、删除、查询、刷新操作,操作方法与主机地址类似

1.3.13.5.3子网地址

eruste	范围地址	子网地址	地址组配置				
1 陶項: 名8	尔 ▼ 关键字:		査询 ご 刷新			◆添加	× 删除所选
1	名称	\$	子网	排除地址	描述	状态令	操作
3	子网地址测试		9.9.9/9.9.9.99			未使用	修改 删除

可进行添加、修改、删除、查询、刷新操作,操作方法与主机地址类似

1.3.13.5.4地址组配置

主机地址	范围地址	子网地址	地址组配置				
查询项: 名	称▼ 关键字:		重询	≥ Rist		◆添加	X图除所选
8	i	各称	\$	成员	描述	状态令	操作
8	地站	上组刻试		测试,测试1		未使用	修改 删除
显示: 15 •	条 共1条				H 首页 4 上一页 1 下一	◎ F 末茂月	1 執法

可进行添加、修改、删除、查询、刷新操作,操作方法与主机地址类似

1.3.13.6 服务资源配置

1.3.13.6.1自定义服务

查询项:名	称* 关键字:	查询 🕫	時行		◆添加	X 删除所
B)	名称	\$ 协议	协议参数	描述	秋恋 \$	操作
9	ok	tcp	源靖口:1-2,目的靖口:3-4	ok	未便用	修改 删
8	test1	tcp	源纳口:2-3,目的纳口:2-3	描述aa	未使用	修改 删
B), .	test3	tcp	漂跳口:4-77,目的跳口:4-77		未使用	修改副
	测试1	tcp	源端口:33-77,目的端口:33-77		未使用	修改 删

可进行添加、修改、删除、查询、刷新操作,操作方法与主机地址类似

1.3.13.6.2服务组配置

	MADE STREET						
查词项: 名称·	关键字:	查访	S RIM		+15.h0	* 885	後所謂
	名称	\$	成员	描述	状态令	採	ff:
0	测试1		bgp		未使用	修改	删料
	周星星	dł	cp-relay,discard_tcp,ftp,ftp-get,ftp-put	星令	未使用	修改	删时
8	9999		chargen, http	描述文字	未使用	修改	删除
显示: 15 · 亲:	共3条			目前页 (上一页 1	下一页 > 東页 > 1	1	and

可进行添加、修改、删除、查询、刷新操作,操作方法与主机地址类似

1.3.13.6.3预定义服务

海项: 名称 • 关键字:	直询 可进行过滤查询			
24% 协议 名称 令	NO SKI	协议卷数		
bgp	tcp	源端口:any,目的端口:179		
chargen	tcp	源编口:any,目的编口:19		
cmd	tcp	源讷口:any,目的讷口:514		
daytime	tcp	源靖口:any,目的靖口:13		
dhcp-relay	udp	漂涛□:any,目的端□:67		
discard_tcp	tcp	源迪口: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	源論口:any,目的論口:21		
ftp-put	tcp	源端口:any.目的端口:21		

1.3.14 高级

1.3.14.1 系统设置

1.3.14.1.1修改密码

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 提示: 如果您认	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ì	认新密码:		*								
	确	认修改 清空									
Telnet密码修	改(修改telnet和	lenable的密码)									
	新密码:		*								
确ì	认新密码:		*								
	确认修改 清空										

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

Telnet 配置密码:用 Telnet 配置设备时,必需使用该密码登录。

1 注意:修改后的密码请务必牢记,以免下次登录时无法进入。

1.3.14.1.2重启设备

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	② 帮助			
说明: 单击此排 提示: 重启过程	說明:单击此按钮将使路由器重新启动。 握示:重启过程需要1分种左右的时间,请耐心等待,设备重启后将会自动跳转到登录页,需要重新登录。									
立即重启设行	畜									

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

1.3.14.1.3恢复出厂设置

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	(2) 帮助				
说明:恢复出/	说明: 恢复出厂设置,将删除当前所有配置。如果当前系统有有用的配置,可先【导出当前配置】后再恢复出厂设置。										
恢复出厂设	置										

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

1.3.14.1.4配置备份

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		? 帮助
说明: 导入过程中不能关闭或者创新页面,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					
				Î	
Building configuration					
Current configuration: 13267 bytes					
version 11.1(6)B2					
1					
wlan-config 1 Eweb_33EE1				•	

配置导出:该功能可以将设备的当前配置导出到本地电脑进行备份。

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

已完成安裝 0% - config.text(来自 172.18 🔳 🔲 🗙					
获取文件信息: config.text (来自 172.18.2.13)					
[] 估计剩余时间: 下载到: 传输速度: □ 下載完成 ∈ 关闭此对话框 (c)					
打开 (2) 打开文件夹 (2) 取消					
文件下载 🔀					
是要保存此文件,还是要联机查找程序来打开此文件?					
名称: config.text 类型: 未知文件类型, 32.7KB 从: 172.18.2.13					
查找 (r) 保存 (s) 取消					
来自 Internet 的文件可能对您有所帮助,但有些文件可能 危害您的计算机。如果不信任文件的来源,则不要查找可打 开此文件的程序或保存此文件。 <u>有何风险?</u>					

配置备份:将本地电脑上的配置备份文件上传到设备上进行还原。

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

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

配置查看:点击"查看详细配置内容"可以查看当前设备的所有配置命令。

1.3.14.1.5系统时间

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	⑦ 帮助	
溫馨提醒:修改设备时间可能导致历史流量报表的审计时间出错。 握示: 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	0							
当前系	当前系统时间: 2016年2月2日下午2:36:23							
重新设	置时间:							
	时区: UTC	+8	•					
	目目	动与Internet 时间服务器	洞步					
	□ 通过管理□自动与Internet 时间服务器同步							
	70	认修改						

系统日期和时间:通过该功能可以设置设备的当前时间。

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

1.3.14.1.6增强功能

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	⑦ 帮助	
反馈用户信息								
配置反馈用户价	言息后系统会自动。	将您所关注的信息或一	些告警信息反馈给	您,目前支持邮件。	方式反馈!			
马上配置用	沪信息							
网站访问被阻	断后的反馈信息	息配置						
这里是配置阻碍	这里是配置阻断网站后反馈始用户的信息,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!							
You are forbidden to visit the website, please contact webmaster!								
保存设置								

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秒生成一次流星数据! 设置生成频率为: 30秒 ▼ 確定	
web登录超时 设置web登录超时时间 999 分钟 确定	
<mark>设备名称</mark> 设置名称用于标识设备 Ruijie * 確定	
流量审计实时数据生成频率 通过这里设置可以提高设备实时生成流量数据的频率,最高可以设置每隔10秒生成一次流量数据! 设置生成频率为: 30秒 ▼ 确定	
流量审计数据库存储时间 设置流星审计数据库存储时间! 天报表保存时间: 60 天,周报表保存时间: 8 周,月报表保存时间: 12 月,其他报表保存时间: 60 天。 确定	
内容审计数据库存储时间 <i>设置内容审计数据库存储时间</i> / 内容审计数据保存时间: 60 天 确定	
严格应用选路記置 <i>开启严格的应用选路后,应用路由功能将会更优越!</i> ●开启严格的应用选路 <	

云维护巡检
开启云维护巡检,可以将设备运行状态上传到脱捷云维护中心进行分析,就捷云维护团队将在第一时间分析并提供对应的解决方案,这将有助于提升网络稳定性。 隐私声明:我们只会上传设备运行状态相关信息,不会收集任何个人隐私信息。所有上传的信息将仅用于脱捷云维护中心分析使用,不会透露给任何第三方组织或个人。
◎开启云维护巡检
确定
web登录超时
设置web登录超时时间
30 分钟
确定
设备名称
设置名称用于标识设备
Ruijie *
确定
配置syslog异常日志
配置syslog异常日志用于客户协助售后及研发定位问题
☑配置syslog异常日志开关
確定 号出异常日志
这个功能主要是设备的一些增强型的功能。

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

以保证设备的正常稳定。点击

马上配置用户信息

按钮会弹出如下窗口。

G 质用户信息 - Internet Explorer G 质用户信息 - Internet Explorer G 成 用户信息 - Internet Explorer G 成 用 户 信息 G 成 用 户 信息 - Internet Explorer G 成 用 户 信息 G 成 用 户 信息 G 成 用 户 信息 - Internet Explorer G 成 用 户 信息 G 成 用 G 成 用 G 成 用 G 成 用 G 成 G 成	Ŋ					
R http://172.18.124.53:8050/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: *						
服务器端口: 25 *						
邮件发送帐号: *						
帐号密码: (加密密码不显示,只需重新配置账号或修改密码时才需输入)						
邮件发送频率: 60 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						
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: 其他 ∨ 机构名称: 联系电话:						
保存设置						
ikit old	2					

开启用户信息反馈:您要配置该功能前需要先勾选 · F店用户信息反馈 (设备会根据您的需要 , 反馈信息给您 !)

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

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

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

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

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

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

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

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

网站访问被阻断后的反馈信息 配置:

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



你被禁止访问这个网站,请联系网站管理员!

以及其他一些不常用的功能配置。

1.3.14.1.7**SNMP**

NMP: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。
MP配置	
SNMP版本:	 ● V2版本 ○ V3版本
设备标识:	*
SNMP□令 :	*
Trap□令 :	
SNMP目的主机:	0
Trap接收主机:	最多可獻置9个Trap接收主机,IP之间適用","号稿开。
	保存设置 清除设置

SMNP 配置:

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

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

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

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

配置 V3 版本的示意图:

SNMP配置



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

1.3.14.2 系统升级

系统升级	? 帮助
<mark>说明</mark> : 您可以访问税捷网络网站的"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: 1、如果是升级软件主程序必须特文件命名为 rgos.bin ,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,可能会遇到整理flash从而导致页面暂时没响应,此时不能所电或者重启设备,直到提示升级成功!	
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	
检测当前最新版本库 应用分类库斯本:2015.11.21.15.11.21 地址库斯本:2015.09.01.00	
內容审计将征库:2015.11.23.01	
检查最新版本	
在线升级web包	
当前web包版本:2015.12.25.10	
日前周之祖功死亡日子	
主程序下载 已安等主程序版本: 2015.12.24	
目前解无新的主程序	
还体影要并就即库夹型,光比顺新的库义件下载到本地,然后用通过本贝面的 本地并微 更新到设备年。 下载内用分类库	
确定	

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

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

系统升级	() 帮助
说明: 您可以 失败。 注意:1、如 者重启设备,	以访问锐捷网络网站的"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 课是升级软件主程序必须将文件命名为 rgos.bin ,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,可能会遇到整理flash从而导致页面暂时没响应,此时不能断电或 直到提示升级成功!
本地升级 _{文件名} :	C:\Users\Lycol\Desktop\web.gz 浏览] 开始升级 取消升级

主程序下载:如果有新版本会提示更新,点击确认升级按钮即可完成升级。

在线升级web包
当前web包版本:2015.12.25.10
目前暂无新的web包

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:2015.08.13.10

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。



版本库下载:您可以通过这里下载到最新的 URL 库或应用特征库版本。

特征库 选择總	、载 要升级的库类型, 或URL库	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"。 下载应用分类库	更新到设备中。
点击 下载到本地	F 载URL库 或 然后通过本页面的	下载应用分类库 ,系统会弹出下载窗口,选择一个下载。 "本地升级"更新到设备中。下载窗口如下图所示:	也址 , 先把最新的库
2 存在片下数 更新说明 特征库下载	, 四贝对诺維	特征库下载 Agreement feature library 为了能提供更精准的URL库和特征库,希望忽留下贵机构的联系方式 机构名称: 锁捷网络1 联系电话: 87426983	
	官方下载地址:	http://rgos.ruijie.com.cn:8800/url/download/all_class/feature.rar http://www.newhua.com/soft/115898.htm	

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



☑启动自动更新 选中 开启自动更新功能。

选择设备自动更新的时间,系统将在每天的这个时间检测最新版本。

选择需要自定升级的文件,系统将只对选中的文件自动更新。



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

1.3.14.3 管理员权限

管理员权限	(?) 帮助
十添加管理员	
用户名	操作
user1	编辑 删除
user2	编辑 删除
显示: 10 🗸 条 共2条	(首页 《 上─页 1 下─页 》 末页 》 1 确定

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

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

管理员权限					
十添加管理员					
+	用户名				操作
➡ 添加管理员				×	编辑删除
					编辑删除
用户名:		▲ 用户名不能为空			▲ 首页 ▲ 上一页 1 下一页 ▶ 末页 ▶ 1
密码:		*			
确认密码:		*			
授权 :	 Image: Second system Image: Second system Image: Second system<th></th><th></th><th></th><th></th>				
			确定	取消	

用户名:这里可以任意输入您想要的管理员名称,推荐使用英文避免使用中文;例如:zhangs;

登录密码:是管理员登录设备 web 网管的密码;

授权页面:您可以对该管理员指派管理功能的权限;

1.3.14.4 一键收集

一键收集将收集设备的故障信息,便于排查设备故障。





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

1.3.14.5 抓包工具

- -

抓包诊断工具:设备抓包功能详细请点击链接。收集抓包如下图,

Pa	acket Capture))			,	Ruíje
	抓包诊断工具	Ļ				
	十添加抓包点 十添加	山抓包规则 十级	扁辑抓包规则			
	抓包点	规则名	接口	状态	操作	
			无记录信息			
	开始抓包 停	止抓包				

注意: 该功能是给工程人员定位故障使用的, 切莫乱用, 以免导致影响网络正常。

1.3.14.6 检测网络

分为 ping 检测和 tracert 检测。

ping检测	tracert检测	
目的IP地址	上或域名: *	
重复次数	欸(1-10): 5	
	开始检测	
		<i>i</i>

去掉了网关出口检测。

ing检测	tracert检测	网关出口检测
目的IP地址或	成域名:	
重复次数((1-10): 5	
	开始检	: 5页
	71×413	

Ping 检测如下图:

目的IP地址或域名:	www.baidu.com] *
重复次数(1-10):	5]
	开始检测	

输入"目的 IP 地址或域名"点击开始检测后会生成如下信息:

Translating "wome baidu com" [OK]
Sending 5, 100-byte ICMP Echoes to 14,215,177,37, timeout is 2 seconds:
<pre>< press Ctrl+C to break ></pre>
Success rate is 100 percent (5/5), round-trip min/avg/max = 33/34/35 ms.

tracert 检测如下图:

ping检测	tracert检测	网关出口检测	
目的IP地址	或域名:		•
	开始检	测	

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



网关出口检测,分为接口时延检测和域名实时访问检测。

接口时延检测 , 如下图

ping检测	tracert检测	网关出口检测		
三 接口时延检测	1			
检	测方式: 🖲 全部接[] ○ 指定接口 ○ 源利	目的IP	
	开始检查	则		
半开连接数信 无	息:			
延迟信息: 无				
选路模块作用 无	流量信息:			

域名实时访问检测 , 如下图

三 域名访问实时检测

<mark>待探测域名地址</mark>	:	*
DNS服务器	:	*
外网口	: 请选择接口 ▼	*
	开始检测	
域名解析:, tcp)	连接:, http get:,	
域名解析的IP:		
域名解析耗时:		
tcp连接耗时:		
http get耗时:		

1.3.14.7 定时任务

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

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

用户任务					? 帮助
用户任务:是用于定时在设备上执行指 命令模式:分为特权模式与全局配置模式 一些命令)。	宝的CLI命令。工作原理是通过配置添加需要 式,配置为特权模式的时候执行权限为特权	耽折行的CLI命令,到达配置的执行时间后 模式权限(即登录设备后的Ruijie#,通常	,设备目动地执行该命令,达到无人值守的 用于执行show命令);全局配置模式则是	目的。 执行权限为配置模式权限(即输入config后	5进入的Ruijie(config)#,通常用于配置
开启用户任务: 이					
任务配置					
十新建用户任务 十新建重启任约	<u>5</u>				
时间	任务名	命令模式	循环时间	命令	管理
2015-12-30 15:15	1	特权模式	24h	show version	编辑删除
2015-12-30 10:52	123	特权模式	20h	show run	编辑删除
2015-12-30 11:29	重启	特权模式	每天	reload y	编辑删除
显示: 10 ▼				《首页 《上一页 1	下一页 ▶ 末页 ▶ 1 确定
用户任务日志 开启用户任务日志: 0FF					

开启用户任务点击开启按钮

开启用户任务: 이

后才能配置用户任务,新建用户任务如下弹出窗口:



对执行完任务可以查看用户任务日志,在开启日志模块后可查看如下

用户任务日志	ā
开启用户任务日常	3志: ом
查看用户任务日	日志清除用户任务日志
● 査看日志	● 志 清除日志
Task name: dd Task time: 201 Execute time: 2 Execute mode: Command: #sk Result: #% Inc	dd 15-08-13 13:44 2015-08-13 14:04 e: config show ip ncomplete command.

另外增加每日/每周重启场景的配置。如下图:

╋新建重启任务	三 配置用户任务		×
(F)			
-30 15:15	任务名:	重启	* 不能超过16字节
-30 10:52			
-20 11.20	时间:	2015-12-30 11:29	*
-50 11.29			
	循环时间:	每天 •	* 每天11:29重启
		保存设置	

1.3.14.8 云服务

1.3.14.8.1云服务

账号绑定:

云服务	Online				
状态 :用账 ⁵ 注意:连接 云服约	号进行管理网关设备 G服务需要配置DN 各配置与集中管理商	音。云网地址 S , 请检查是 3置冲突 , 只	链接为:http:// 哈巴经配置了I 能二选一。	/cloud.ruij 正确的【[ije.com.cn/ DNS服务器】,否则将不能生效!
	绑定方式: 💿	账号绑定	○ 扫码绑定	ΤĒ	
	网络名称				0
	绑定账号:				×
手机尾	号四位数:				*
		阅读并同意	<<隐私政策和月	用户协议>	~
		开启云服	务并绑定账号	3	
			立即注	主册,	

扫码绑定:





1.3.14.8.20nline

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

开启Online:	OFF	
		×
	0n-Line智慧门店云平台用户协议	
	《用户协议》(以下简称"本协议")是您(或称"用户",指注册、登录、使用、浏览本服务的个人或组织)与税捷网络股份有限公司及其关联公司(以 下简称"税捷")及其运营合作单位(以下简称"合作单位")之间关于税捷设备与税捷On-Line智慧门店云平台网站(http://On-Line智慧门店云平台 1.ruijie.com.cn,简称本网站)、税捷睿易APP软件所订立的协议。	
	锐捷在此特别提醒用户认真阅读、充分理解本协议中各条款,包括免除或者限制锐捷责任的免责条款及对用户的权利限制条款。请您审慎阅读并选择 接受或不接受本协议(未成年人应在法定监护人陪同下阅读)。除非您接受本协议所有条款,否则您无权注册、登录或使用本协议所涉相关服务。您的 注册、登录、使用等行为将视为对本协议的接受,并同意接受本协议各项条款的约束。	
	1.用户使用规则	
	1)在使用On-Line智慧门店云平台时,您必须承诺和保证:	
	您了解并同意,用户须对注册信息的真实性、合法性、有效性承担全部责任;用户不得冒充他人,不得利用他人的名义发布任何信息;不得恶意使用注 册帐户导致其他用户误认;否则我们有权立即停止提供服务,您独自承担由此而产生的一切法律责任。 您使用On-Line智慧门店云平台的行为必须合 注.你必须为自己注册帐户下的一切行为份责,句括你所发表的任何内容以及由此产生的任何结果。田户应对其由的内容自行加以判断,并承担因使用	•
	同意并开启不同意	t

1.3.14.9 集中管理

集中	2管理		
	集中管理:	☑ 开启集中管理 😮	
	管理类型:	MCP/WMC管理 ▼	
	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:	30000	(10000至65000,默认30000)
	用户名:		
	密码:		
		保存设置	

添加了源 IP 地址和性能监控管理端口。

集中管理		
集中管理:	🗹 开启集中管理 😵	
管理类型:	MCP/WMC管理 ▼]
服务端IP ▼:	172.18.111.101	*
设备管理端口:	9999/service/acs	(1至65535 , 默认80)
用户名:]
密码:		
	保存设置	

集中管理包括两种种类型 MCP 管理、RAC-SNC 管理、RCN 管理。

1.3.14.10 第三方日志

1.3.14.10.1 第三方服务器配置

第三方服务器配置				
提示: 开启第三方服务器功能	(ELOG除外) , 会导致V	WEB认证无感知、商业	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	T		
第三方日志服务器列表	╋ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶			
第三方日言	志服务器名称	第三方日	志服务器类型	操作
t	est_a	S	urfilter	编辑 删除
显示: 10 ▼ 条 共1条			◀首页 ◀ 上一页	1 下页 ▶ 末页 ▶ 1 确定
MCP联动配置,仅在E	G不做NAS的情况	下开启。 ŧ,获取认证用户上	下线信息	
服务器IP地址:	192.168.1 <mark>1</mark> 0.1	* ;	格式: 192.168.110.1	
源IP:		ħ	函式: 192.168.23.14(通	过IPSEC VPN隧道与MCP通信)
服务器登录用户名:	test	*	服务器管理员账户名,	支持最大32个英文字符
连接状态:	断开已连接状态	下如无法同步上下约	线用户信息, 请检查服务	s器ip和登录用户名是否准确
ſ	保存	这个按钮	田保存下发的命	令只不包括日志服务器列表

配置第三方服务器:

第三方服务器配置				
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	き: 🗌 开启			
	保存			

选择 ELOG

第三方服务器配置	
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EG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	
选择第三方日志服务器	
第三方服务器配置	
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 ▼	
第三方日志服务器列表 十添加 X 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EG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	

🔜 添加第三方日志服务	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)	1
FTP用户名:		×	
FTP密码:		*	
数据采集参数			
		7	-
		保存关闭	I

输入相关参数

📃 添加第三方日志服务	3器	2	×
第三方日志服务器类型:	任子行 •		•
第三方日志服务器名称:	test_a	*	I
服务器参数			I
服务器IP:	1.1.1.1	* IP地址	I
服务器端口(FTP):	21	* (1-65535, 默认21)	l
FTP用户名:	aa	*	
FTP密码:	••	*	
数据采集参数			
	[1	*
		保存关闭	
保存 点击弹窗中的			

第三方日志服务器列表 十添加 X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	
	test_a	surfilter	编辑 删除	
显示	: 10 ▼ 条共1条	▲ 首页 《 上—页	1 下—页 ▶ 末页 ▶ 1 确定	

可进行编辑、删除操作

点击页面底下的保存按钮,显示如下

第三方服	济器配置	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	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。								
Э	第三方服务器功能: 🖻 开启								
送	选择第三方服务	器: 第三方日志服务							
第三方E	日志服务器列表	€ 十 添加 Ⅹ删除选	Þ						
	第三方	方日志服务器名称	第三方日志	服务器类型	操作	E			
		test_a	sur	filter	编辑	删除			
显示:	10 ▼ 条共	1条		▲首页 《 上一页	〔 1 下─页 ▶ 末页 ▶	1 确定			
MCP助	送动配置,仅	在EG不做NAS的情况	祝下开启 。						
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							

1.3.14.10.2 场所基本信息

· 日本	REENTERASU with	1.42					
▶ 漆加场新基本信息	· ×删除选中 清选的		线 导出场所基本信息		选择文件	任何文件	Q入场听越本信息
	界场所编码 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
					1000000000		BIRDER 0000000

┣添加场所基本信息 点击

➡ 添加场所基本信息		×
第三方日志服务器名称:	test-c 🔹	A
. 上网服务场所编号:	test-c test-b test-a	* 14位数字
上网服务场所名称:		这里会根据不同的名称对应的类型。
经营法人:		* 型,显示不同参 数 列表
经营法人有效证件类型:	身份证 🔹	x1/11
经营法人有效证件号码:		*
场所负责人:		*
联系电话:		*
		保存关闭

输入参数
📃 添加场所基本信息					×
第三方日志服务器名称:	test-c		T		A
上网服务场所编号:	22222222222222	22	* 14	一数字	
上网服务场所名称:	國吧	*		- 1	
经营法人:	林		*		
经营法人有效证件类型:	学生证		T		
经营法人有效证件号码:	158444		*		
场所负责人:	周星星		×		
联系电话:	15866663333		*		
保存				保存	关闭
·击					
法 第三方服务器配置 協所基本信息 役益基本 関約: 島)、路行基本信息がなけるの感じ、いわざ信	信息 秋本信息 第三方	日本配置			
第三方限务器配置 協所基本信息 (公告基本 規制: 号入场所基本信息的文件名か成以 exy为成唱。 十次加场所基本信息 X 勤労造中 満近保密分響名称 ・	信息 状态信息 第三方	日志配置	选择文件 未进择	任何文件	导入场件基本信息
 第三方訳务様配置 路所基本信息 (公告基本 規約: 導入5所基本信息的文件名の意以、のつな6編。 十派加塔所基本信息 X 副時息中 満進塔級会員名名称 ・ 上周期客场所協約 ト同期客は所名曲 	信息 秋志信息 第三方日 查找 号出场所基本信息 第三方日 第二方日本屬外國本信息 第二方日 第二方日	日本記室	透探文件 未透择 所属城市	任何文件	导入场听题本语思 提代:
第三方服务標配置 场所基本信息 设备基本 规制:导入场所基本信息的文件名必须以.cvv为后端。 计规加场所基本信息 X 勤労选中 查选择服务器名称。 上网服务场所编码 上网服务场所名称。 11111222223333 上网服务场所名称。	 (信息 状态信息 第三方) 登送 号出送将加本信息 第三方日本服务器名称 1051-3 	日志配置 所属省 111222	[透释文件] 未透择 所属城市 333444	任何文件 所属分区 44444	 · 日本
 第三方服务福配置	 (信息 秋志信息 第三方) (信息 報志保護本信息) (第三方日本服务器名称 1 [est-a] (est-b) 	日志配置 所属省 111222 111111	透耀文件 / 水透描 / 所属城市 333444 111111	任何文件 所属分区 444444 111111	 令入私所営本信息 提作 契約 契約 第時 報告 報告

表格数据可以进行删除、编辑

查找、导出导入数据(必须先选择服务器名称)

.

说明:	导入场所基本信息的文件名必须	以.csv为后缀。	根据服务器名称过滤查打	线、导出数据、导	入数据		
+ 添加水	杨所基本信息 X 删除选中	请选择服务器名称 •	13% 导出场所基本信息		选择文件 未选择	任何文件	导入场所基本
	上网服务场所编码	test-c	第三方日志服务器名称	所属省	所属城市	所属分区	腺性
8	11111222223333	test-a	test-a	111222	333444	444444	编辑 删除
8	11111222223333	上网服务场所名称-b	test-b	111111	111111	111111	\$16 #10
8	22222222222222222	网吧	test-c	333444	555666	777888	编辑 副徐

1.3.14.10.3 设备基本信息

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	的文件名必须以 Lew为后的	ä.				
上添加AP基本信息 X	删除造中 请选择制	股务器名称 ▼ 场所名称:	直线 导线	EAP基本信息	發展文件 未选择任何文件	导入AP基本信息
□ 上网服务:	汤所编码	上网服务场所名称	MACIEL	名称	entersion	操作
			无记录信息	13		

点击 十添加AP基本信息

■ 添加AP基本信息			×
上网服务场所编号:	点击选择场所编码	* 14位数字	
		保存	关闭

保存关闭



■ 添加AP基本	信息					×
上网服务场所	编号: 1111	1222223333		*		
MAC	2222	.2222.2222		* 例	: 2222.222	22.2222
AF	の名称: 测试-	а		*		
AF)类型: 固定	AP	•	•		
AP所在	E楼层: 7楼			*		
AP创建	时间: 2018	-11-06		*		
再点击弹窗中的	呆存				保存	关闭
第三方服务器配置 场所基本信息	!! 设备基本信息 ^状	ふ信息 第三方日志配置				
第二方服务器配置 场所基本信息 設局:导入AP基本信息的文件名必须以 zev为b	2 设备基本信息 ³⁾ 后载.	活信思 第三方日志配置				
第三方服务器配置 场所基本信息 股票:导入AP基本信息的文件名必须以 cm/知 十语加AP基本信息 X 删除选中 通选择	 设备基本信息 近后端。 案服务器名称 • 场所名称: 	这倍思 第二方日本配置 查线 - 933/	中基本信息	选择文件 未进	握任何文件	ВХАРШИДС
 第二方服务器配置 场所基本信息 取用:导入AP基本信息的文件名必须以 cm/和 十流加AP基本信息 X部除选中 清选择 上网服务场所编码 	 2 没备基本信息 3 (2) 各基本信息 4 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	这信息 第二方日志配置 直线 9世/ MAC地址	P基本信息 名称	选择文件 未透	操任何文件 创建时间	ə)APBBB的 操作
第三方服务器配置 场所基本信息 説明: 导入AP基本信息的文件名必须以 zev/bi + 添加AP基本信息 X 新除选中 清选計 - 上門服务场所编码 - 11111222223333	设备基本信息 対 価値、 運搬完課名称・ 场所名称: 上周顧券通所名称 上周顧券通所名称・	法信息 第二方日志配置 取残 日出 MAC地址 2222.2222.2222	P基本信息 名称 激试-3	选择文件 未透	總任何文件 的助助问 2018-11-06	日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日

查找、导入导出数据

			- Hange		LY J HAVE HOUR			
说明: 导入AP器	本信息的文件名必须	Lowhill。 可根据服务器分	乙称、 场 所	名称讲行讨谢		根据	服务器名称进行导入导	争出数据
十添加AP基本信息	· 大田除透中	う 100 MF/100 57 1111 清选择服务器名称 ・	场所名称:	1110-22-11 22-06	查找 导出AP基本信息	选择文件	未选择任何文件	Ģ入AP基本信息
E Fi	网服务场所编码	test-a	6 所名称	MAC	tht e	5称	entren	操作
111	111222223333	test-b test-c	ilfr名称-a	2222.2222	2.2222 例	हिं,-a	2018-11-06	编辑 删除

1.3.14.10.4 状态信息

第三方	服务器配置	场所基本信	B 8	备基本信息	状态信息		第三方日志教	置						
	第三方日志 test-a	● 未连接	1	ē三方日志 est-b	● 未连接	1	第三方日志 test-c	 未当 	e					
55 34	服务器状态: ● 未進續 第三方日志对接库版本: 2018.10.19.01													
E	志続计:												(W28	R)
	网络虚拟身 0个	粉轨迹	搜索关键字 0个	上网	行为日志	终端 0个	止下线日志	STA	特征采集日志	采集後	各基础信息	场所资料 0个		
成 (共	成功发送记录 (O个) 失败发送记录 (O个)													
点击	清空	记录	可以	清空日	志跟发送	<u>É</u> 记:	录							
第	三方服务	器配置	场	所基本信	息	设备	番基本信息	١. ال	状态信	息	第三方	日志配置		
	第 te	三方日志 est-a	ŧ,			第 tes	三方日志 st-b	•	未连接		第三方 test-(5日志 c	未连接	
				点	击可切	换月	服务器	, 显;	示相应	的配置	I.			

1.3.14.10.5 第三方日志配置

第三方服务器配置	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

以直接点击全部开启/关闭,单独勾选 NAT 审计日志、BBS 审计日志、虚拟身份审计日志、搜索审计日志、MAIL 审计日志、

HTTP/URL 审计日志后。点击

按钮完成配置。

1.3.14.11 SDN 配置

OPENFLOW配置		
说明: 通过openflow协议连 控制器地址是远程服	接SDN控制器,提供全局的网络性能监测 务器地址。控制器默认端口是6633。	则度量功能。
设备出接口:	◯ Gi0/6	
控制器地址:		*
控制器端口:	6633 *	
连接状态:	未配置	
	保存设置 清除设置	

1.3.14.12 VRRP 配置

VRRP配置				? 帮助						
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: ④ 🤇	指定接口:									
VRRP组号:	VRRP组号: * (1-255)									
VRRP组IP:	YP组IP: *									
VRRP优先级:	(1	1-254)								
	添加设置									
★删除全部										
VRRP组号	接口	VRRP组IP	VRRP优先级	操作						
54	Gi0/1	66.25.57.5	2	编辑删除						
显示: 10 🗸 条 共1条			▲首页 ◆上一页 1 下-	-页▶ 末页▶ 1 确定						

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

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

VRRP 组号:这个好比是 VRRP 名称,是用户标记 VRRP 策略的;

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

VRRP优先级:同一接口的 VRRP 匹配优先顺序。

1.3.14.13 动态域名解析

动态域	动态域名解析										
动态固 说明: 注意:	动态域名解析: 功能是实现固定域名到动态P地址之间的解析。 说明: 最多可以配置0个账号。 注意: 若您需要进行升级,且升级版本低于11.9(1)829版本,在升级完成后需重新配置此功能。										
十添加											
	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─页 1 下-	-页 ▶ 末页 ▶ 1 确定					

动态域名解析是是实现固定域名到动态 IP 地址之间的解析。

目前设备支持 花生壳、3322 服务提供商;如果您没有帐号可以点击 【没有帐号请先注册】 这里注册帐号; 用户名和密码:这里输入您在花生壳用户名和密码;

1.3.14.14 系统日志

1.3.14.14.1 服务器日志

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

服务器日志	查看系统日志					
说明: 设备端端口 对端为APM服务器 注意: 优先级高的 http协议用的端口(1号设置需和对端服务器端口 ,且端口号20000以下,只 1日志先发送,0最高,7最低 料寺一致。	号保持一致。若对端是。 支持流日志 ; 。文件上传方式只能设	inc服务體只支持CPU、内 置一个,且没有区分日志(存使用率日志 , 接口会读 优先级。日志类型只能没	5审计,IP流量审计以及接 置文件或者实时。http的迹	口流量审计日志;若 前口需要与服务器
日志	上传方式: 🖲 实时上传	◎ 文件上传				
E	服务器IP:		*			
	端口: 20000		* (10000-65000)			
服雪	务器类型: ELOG	•				
	源P:		0			
	>>> 发送日志	<u>美型</u>				
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: 10 ▼ 条	.共0条			◀首页 ◀ 上一	页 下─页 ▶ 末页 ▶	1 确定

♥ 发送日志类型		
□开启流日志 4 ∨	□CPU、内存使用率日志 4 V	□硬盘使用日志 4 ∨
□开启URL审计 4 V	□接口会话数审计 4 ∨	□IP应用流量审计 4 V
□IP会话数审计 4 ∨	□通道流量审计 4 ∨	□接口流量审计 4 ∨
□IP在线时长审计日志 4 V	□邮件审计日志 4 ~	□ 搜索引擎审计日志 4 ∨
□BBS审计审计日志 4 V	□IM审计日志 4 ∨	
保存设置		

输入服务器 ip 地址:这里输入接收日志的服务器的 ip 地址;

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

1.3.14.14.2 查看系统日志

包括配置 syslog 日志和查看系统日志 。

配置 syslog 日志,开启日志的时候才可以导出 syslog。

服务器日志	查看系统日志	
配置syslog日	志	
配置syslog日志用	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	

点击更新当前系统日志按钮,可刷新当前系统日志信息如下图所示:

系统日志(show log)
更新当前系统日志
Trap logging: level informational, 14 message lines logged,0 fail
Count log messages: disable
Sysname log messages: disable
Sequence-number log messages: disable
Timestamp log messages: datetime
Timestamp debug messages: datetime
Standard format:false
Buffer logging: disabled
Monitor logging: level debugging, 0 messages logged
Console logging: level debugging, 17 messages logged Syslog logging: enabled

1.3.14.14.3 SYSLOG 服务器配置

	服务器日志	本地日志	ŧ	查看系统日志	s	SYSLOG服务器配置	
	Syslog	g服务器IP:	6.6.6	i.6		】* 格式: 192.168.23.14	ł
		端口:	55			】 * (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							
			ť	保存设置			

1.3.14.15 日志策略

日志	日志策略					
十添加	十添加日志策略 X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	
	aaa	1.2.3.4	82号令日志		编辑 删除	
	外部用户-所有用户	外部用户: 所有用户	82号令日志	€ 4	编辑删除	
	bendi	本地用户: b&aa	网监日志	€ 4	编辑 删除	
	本地-所有用户	本地用户: 所有用户	82号令日志	€ 8	编辑 删除	
	AD域用户	外部用户: ad域用户-a	网监日志	Ŷ	编辑 删除	
显示:	显示: 10 ▼ 条共5条 II 首页 《 上一页 1 下一页 》 末页 II 确定					

1.3.14.16 投屏服务

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

该功能默认不开启,配置界面如下:

投屏面	X态信息
说明: 提示:	: 投屏服务能在内网跨网段支持苹果和安卓投屏功能,终确通过认证加入到某一房间号,终端的房间号与电视IP绑定的房间号需要一致才能在对应房间号下使用投屏,避免了投射到其它房间的电视上;每个房间最多能添加8台电视映射。 : 号入的文件名必须为screen.csv,匹配模式如果是IP,只能导入IP,如果是MAC,只能导入MAC。 下载导入模板
开启投剧	屏功能: OFF
开启后	的状态:
说明: 提示:	投屏服务能在内网跨网段支持苹果和安卓投屏功能,终端通过认证加入到某一房间号,终端的房间号与电视IP绑定的房间号需要一致才能在对应房间号下使用投屏,运免了投射到其它房间的电视上;每个房间最多能添加8台电视映射。 导入的文件名必须为screen.csv,匹配模式如果是IP,只能导入IP,如果是MAC,只能导入MAC。 下载导入模板

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 基于 房间号 ▼ 查询映射: 查找	选择文件 未选择任何文件 导入 导出二维码: 导出	选中 导出所有
	房间号	电视IP	操作
	1110	10.101.10.100	编辑删除
显示	10 ▼ 条共1条	〈首页 《 上─页 1 下─页 》 末页	1 确定

投屏配置状态信息			
基于 房间号 ▼ 查询映射: 查找			
房间号	电视IP	终端IP / 账号	
1110	10.101.10.100	无	
显示: 10 ▼ 条共1条		I 首页 ◀ 上→页 1 下→页 ▶ 末页 ▶ 1 确定	

导入模板示例:

	А	В
1	房间号	电视IP/MAC(多个用","隔开,最多配置8个)
2	101	192.168.101.1
3		
4		

1.3.14.17 设备审计报表

1.3.14.17.1 WEB 操作日志

WEB操作日志					
请选择需要查看的操作日志: 2017-10-16 ▼ 【 导出报表					
时间	操作员的IP	描述			
2017-10-16 10-58-20	192.168.23.23	admin(配置), admin用户登录			
2017-10-16 10-08-17	192.168.23.201	admin(配置) , admin用户登录			
2017-10-16 10-03-24	192.168.23.196	admin(配置) , admin用户登录			
2017-10-16 10-03-15	192.168.23.196	admin(配置),系统升级页面,升级web包			
2017-10-16 10-02-54	192.168.23.196	admin(配置),admin用户登录			
显示: 10 ▼ 条 共5条	【●首页 ● 上一引	瓦 1 下一页 ▶ 末页 ▶ 1 确定			

系统操作日志查看操作设备的情况