



WEB

RG-NPE

RGOS 10.3(4b11)p4

V1.0

©2014



[] []

{x|y|...}

[x|y|...]

//

2)

⚡ i ∂ p i è r ¢
i i i ^ è r © ¢ r a ч ¢
^ ψ r ¢ ¤ © ¢ r a ч ¢

3)

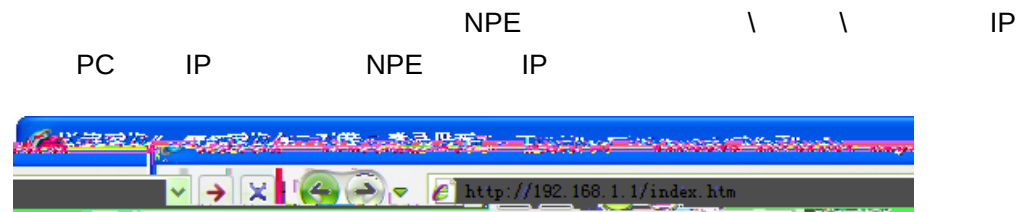
Web

Web

Web

NPE

2.1 Web



§

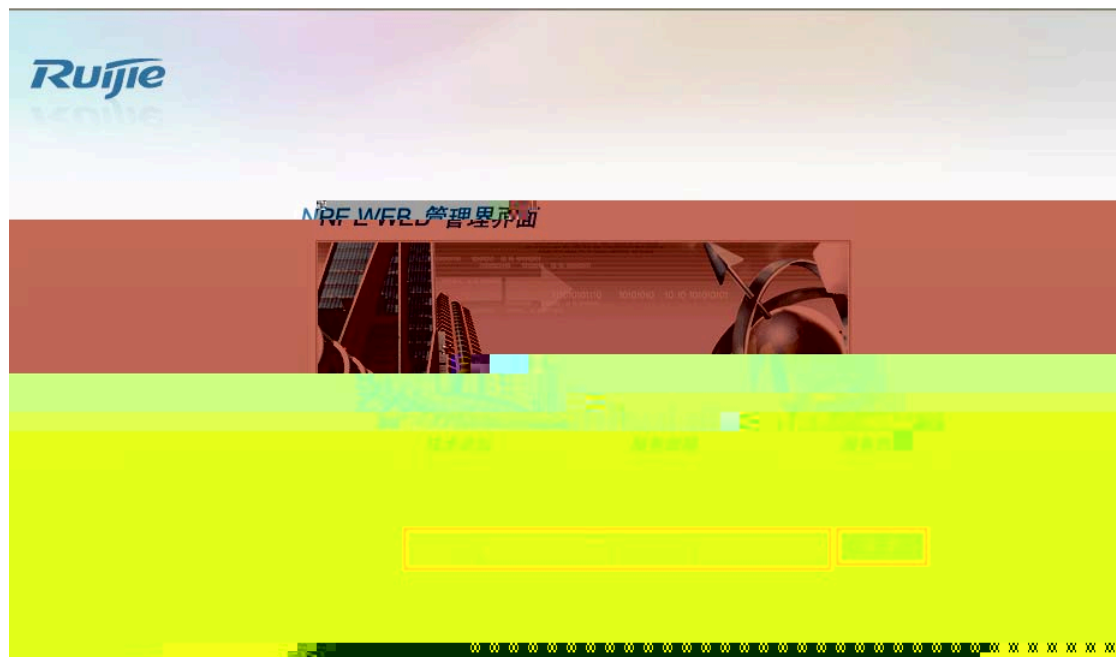
h h H X r WEB Ä ũ n § <http://192.168.1.1> ¢

h h H X r "I á o admin ¢

Ä PC "H" 5 9 r Gi0/0 ε i ¢

i 9 ' r o k y k o ố k ố ố z á y 1 a 2 j

r ¢ ố ~ j o "H T á y ` r ư



1

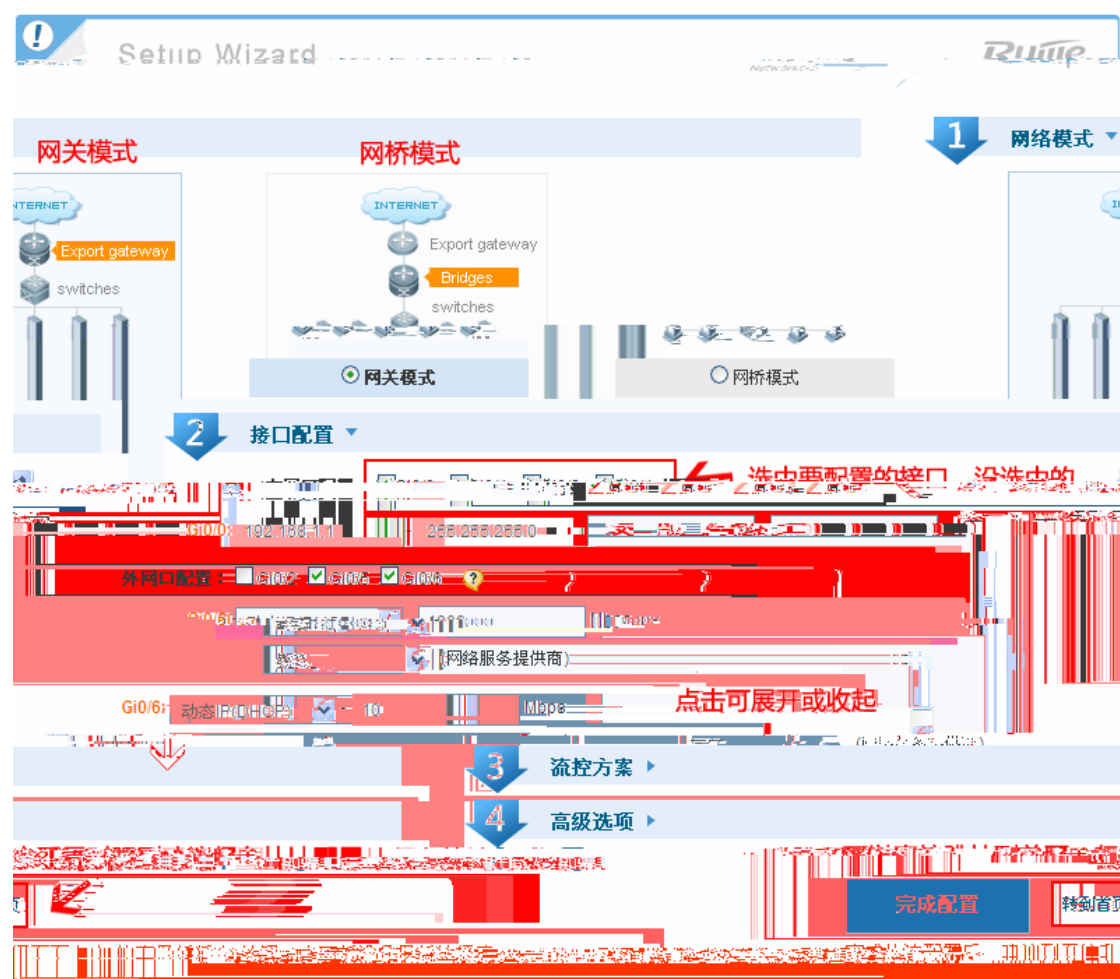
登 录

2



§

web 文件包 NPE 文件包 web 文件包
web_management_pack.upd 文件包 - 文件包 文件包 文件包



1 NPE

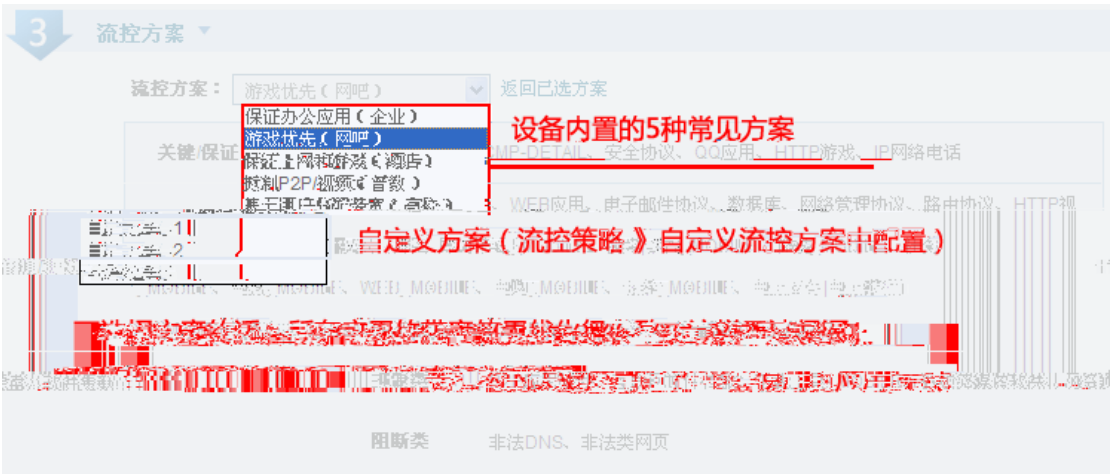
2

1

内网口配置: ☒ Gi0/0 ☐ Gi0/0/1 ☒ Gi0/1.1 ☐ Gi0/3 ☐ Gi0/4

Gi0/0: 100.100.30.1 - 255.255.255.0

Gi0/1.1: IP地址 - 掩码



A

NPE

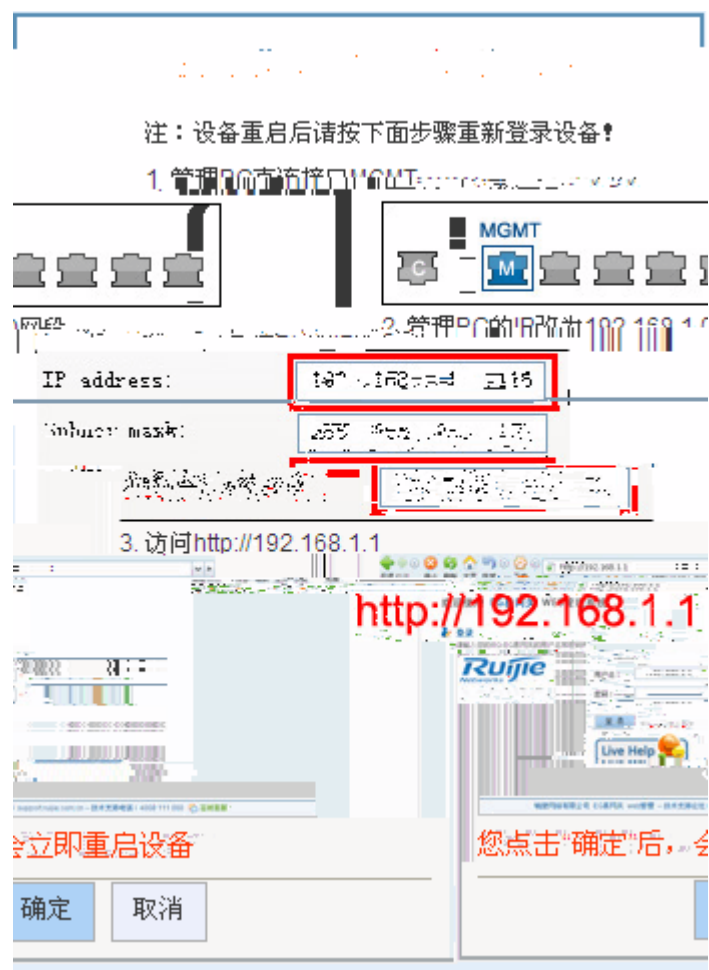
/

B

返回已选方案

完成配置

2.2.1.2





1 NPE

2

1 IP
Ip

管理口配置: 172.18.3.81 - 255.255.255.0 - 172.18.3.1
管理PC将通过该IP来访问设备的管理界面 管理口的网关地址

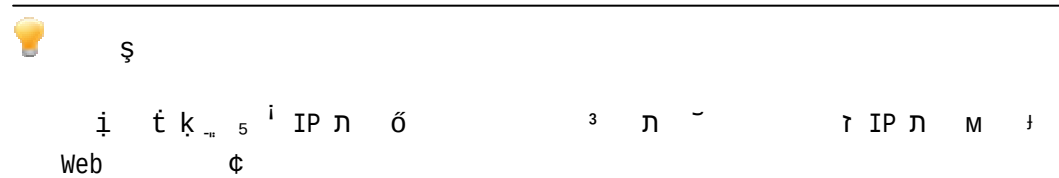
2

线路配置: 线路1 - GE0/24 - GE0/24 - 10 Mbps

3

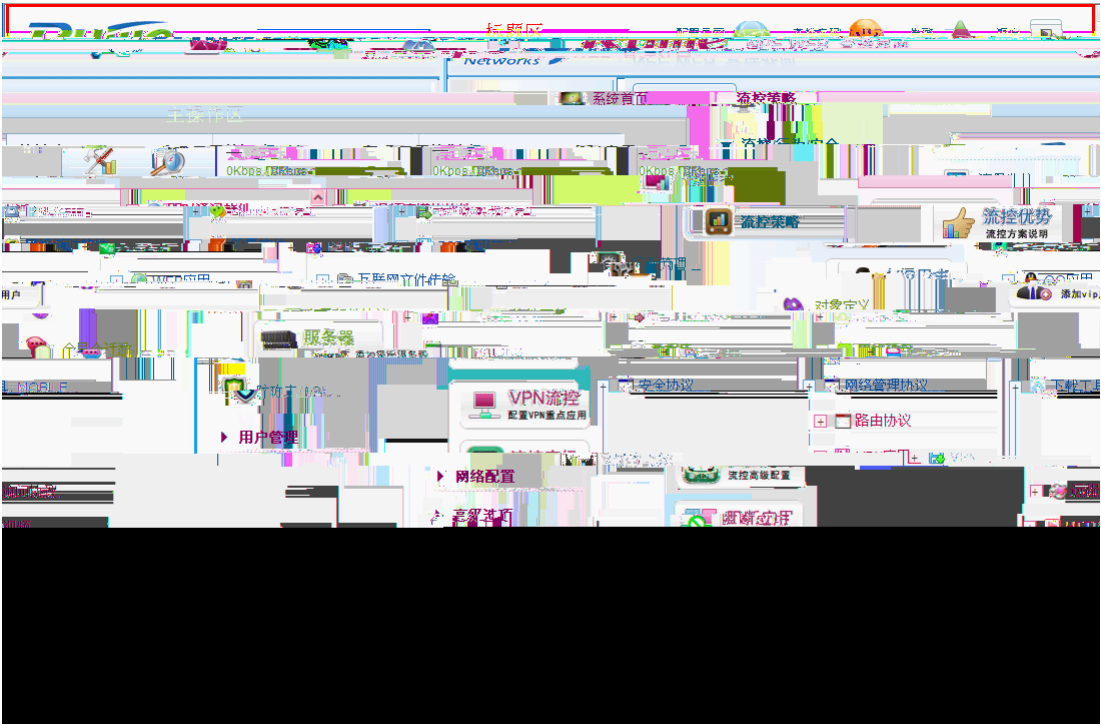


4



2.3 Web

WEB



2.3.1

1

(admin)





功能配置 系统操作 接口状态 常见问题

占丰进入接口配置页面

重新连接

接口名称	是否上电	IP地址	上行流量	下行流量
Gi0/5	已上电	172.18.3.14	0.81Kbps	1.45Kb
Gi0/2	未上电			

内网口状态

接口状态日志

IP地址	接口日志查询
	2013-08-08 13:55:00 接口GigabitEthernet 0/4, 链路协议状态改变为up。
192.168.1.1	2013-08-08 13:55:00 接口GigabitEthernet 0/4, 链路状态改变为up。
4.4.4.1	2013-08-08 13:53:18 接口GigabitEthernet 0/4, 链路协议状态改变为down。
	2013-08-08 13:53:18 接口GigabitEthernet 0/4, 链路状态改变为down。
5.5.5.8	2013-08-08 13:53:12 接口GigabitEthernet 0/4, 链路协议状态改变为up。

接口名称	是否上电
Gi0/0	已上电
Gi0/4	已上电
Gi0/1	未上电
Gi0/1.1	未上电

shutdown

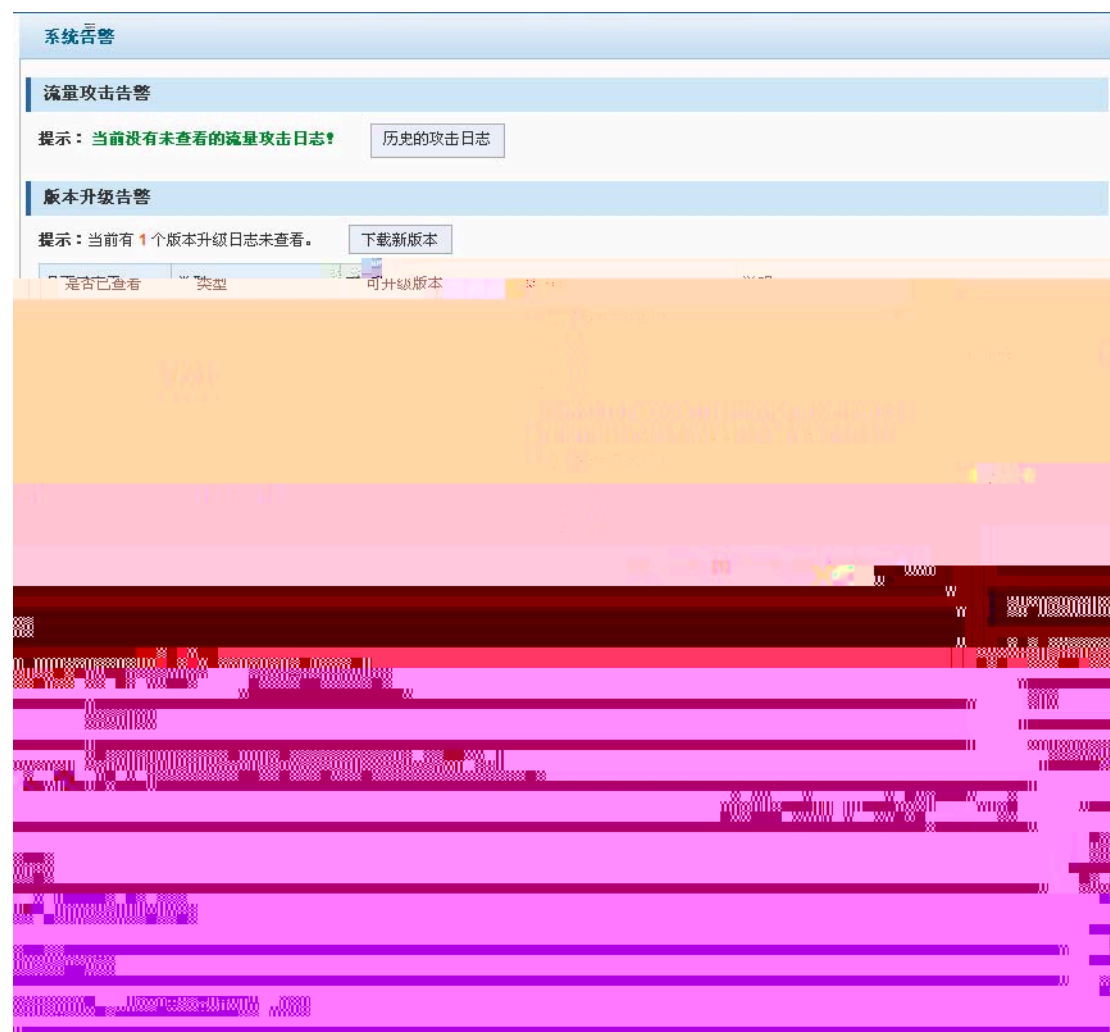
no shutdown

1



2

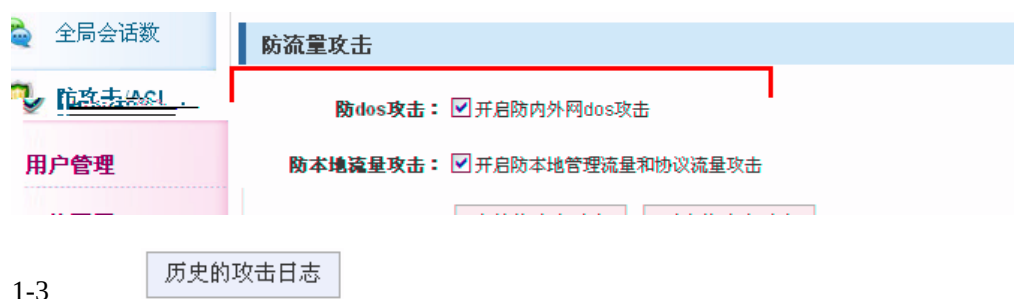




1

1-1

1-2



1-3

2

bin

web

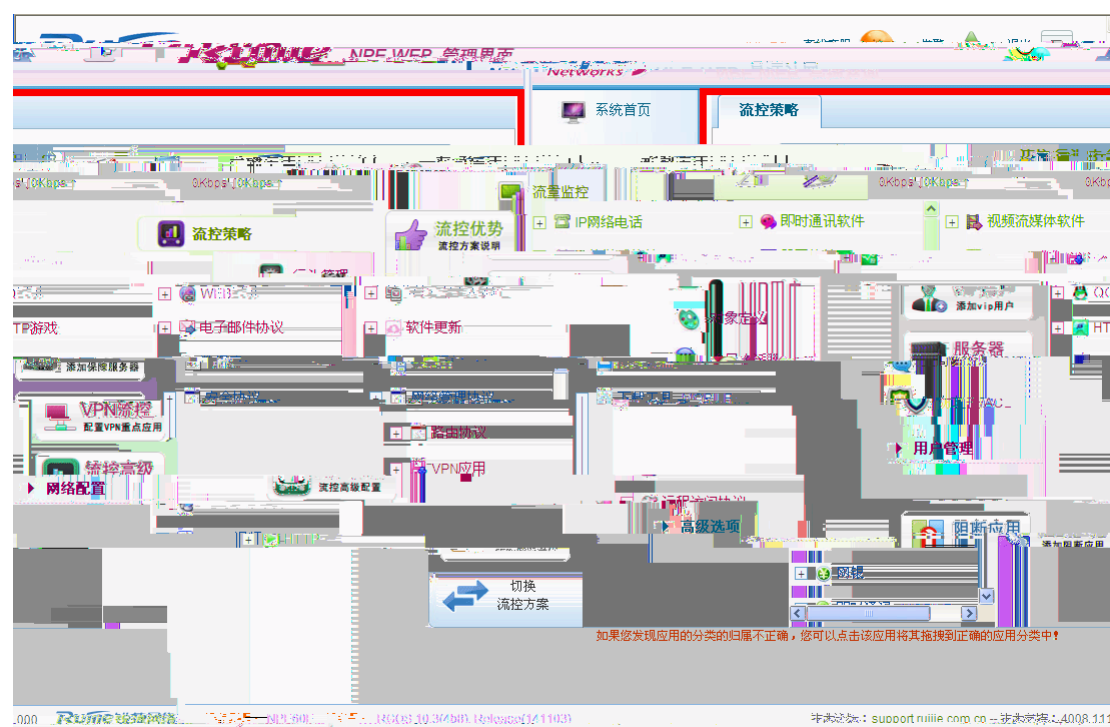
web

下载新版本



2.3.3

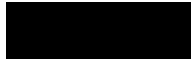
NPE



2.3.4

2.4

WEB



CPU

TOP10

TOP10

TOP10

2.4.1

CPU

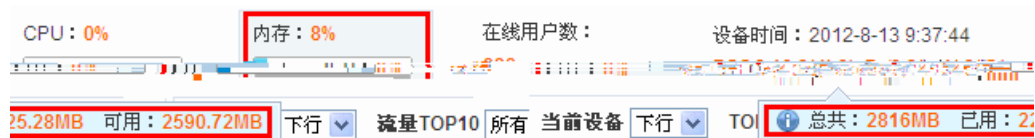
CPU: 0% 内存: 8% 在线用户数: 833 设备时间: 2012-8-13 9:36:28
 RGOS 10.3(4b8), Release(141642)

1 CPU
CPU

CPU



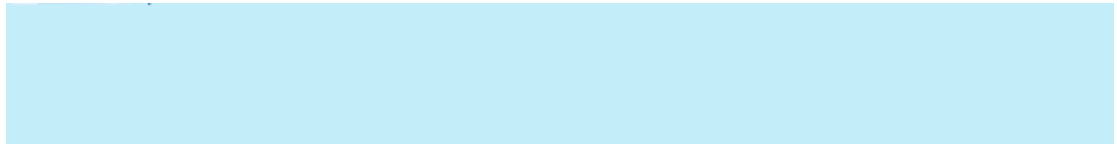
2



3



4



2.4.2

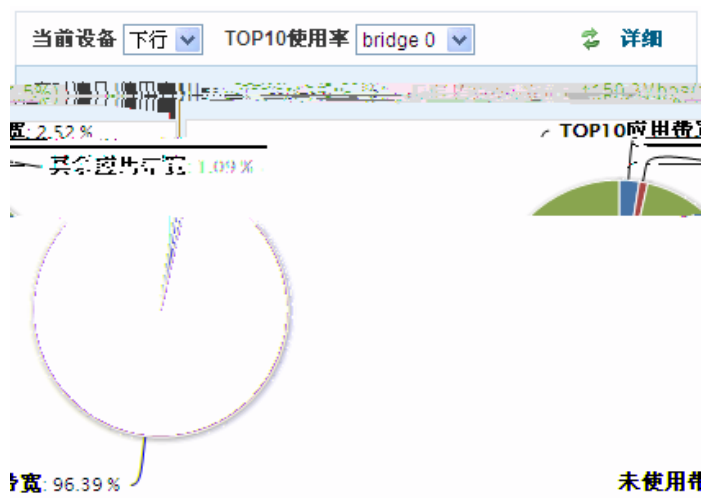
TOP10

TOP10

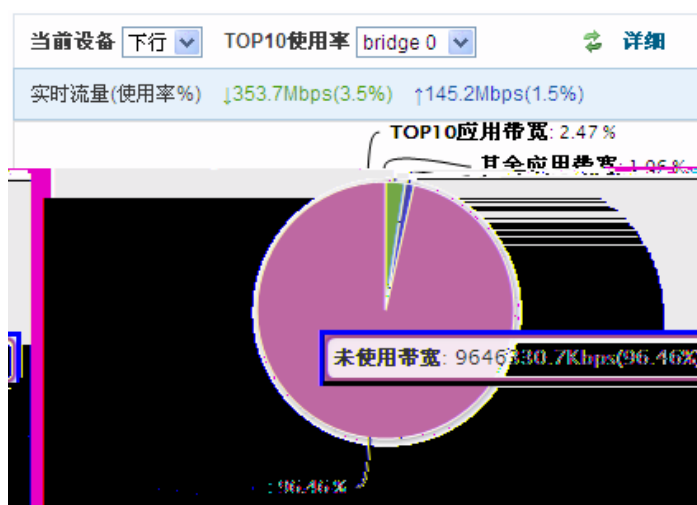
TOP10

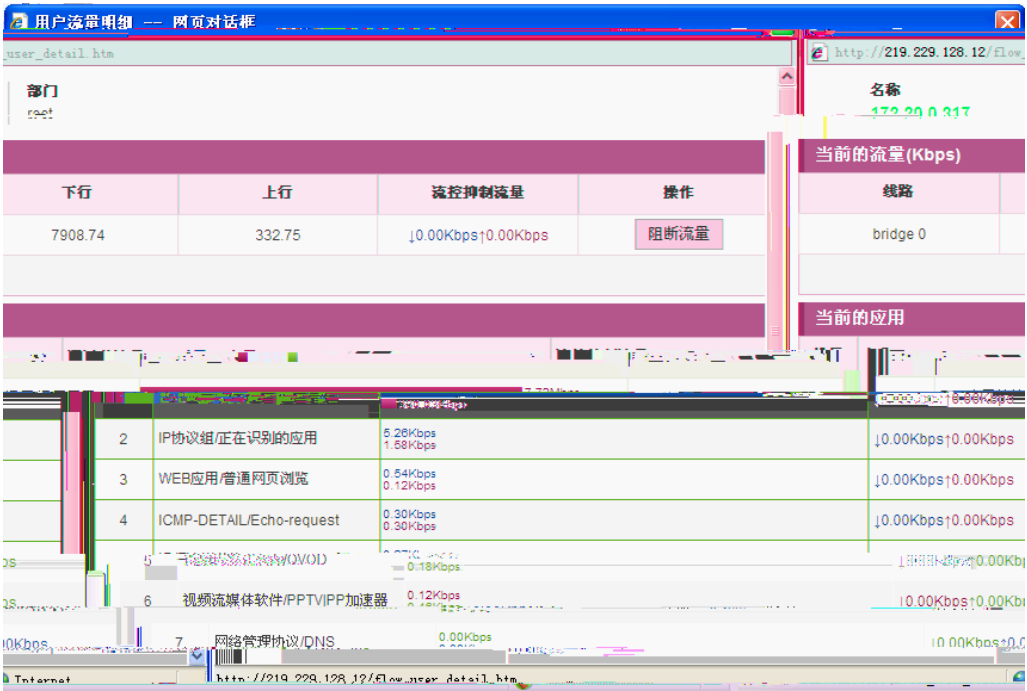


2.4.2.1



1	bridge 0		
TOP10	bridge 0	10	
	bridge 0		
	bridge 0	TOP10	
	bridge 0		
	bridge 0		bridge
0			
2	bridge 0	下行	TOP10
3			
4	详细	/	/
5		/	





1

2 阻断流量

2.4.2.3

4



TOP10

5

[详细](#)

/

/

2.4.2.4

TOP10

田口会社TOP10

話数	排行	用户	IP地址	会
100	1	/172.20.33.144	172.20.33.144	27
34	2	/172.20.32.102	172.20.32.102	24
16	3	/172.50.111.203	172.50.111.203	23
35	4	/172.50.100.5	172.50.100.5	21
21	5	/172.20.79.182	172.20.79.182	20
62	6	/172.50.113.17	172.50.113.17	17

1

bridge 0

TOP10

2



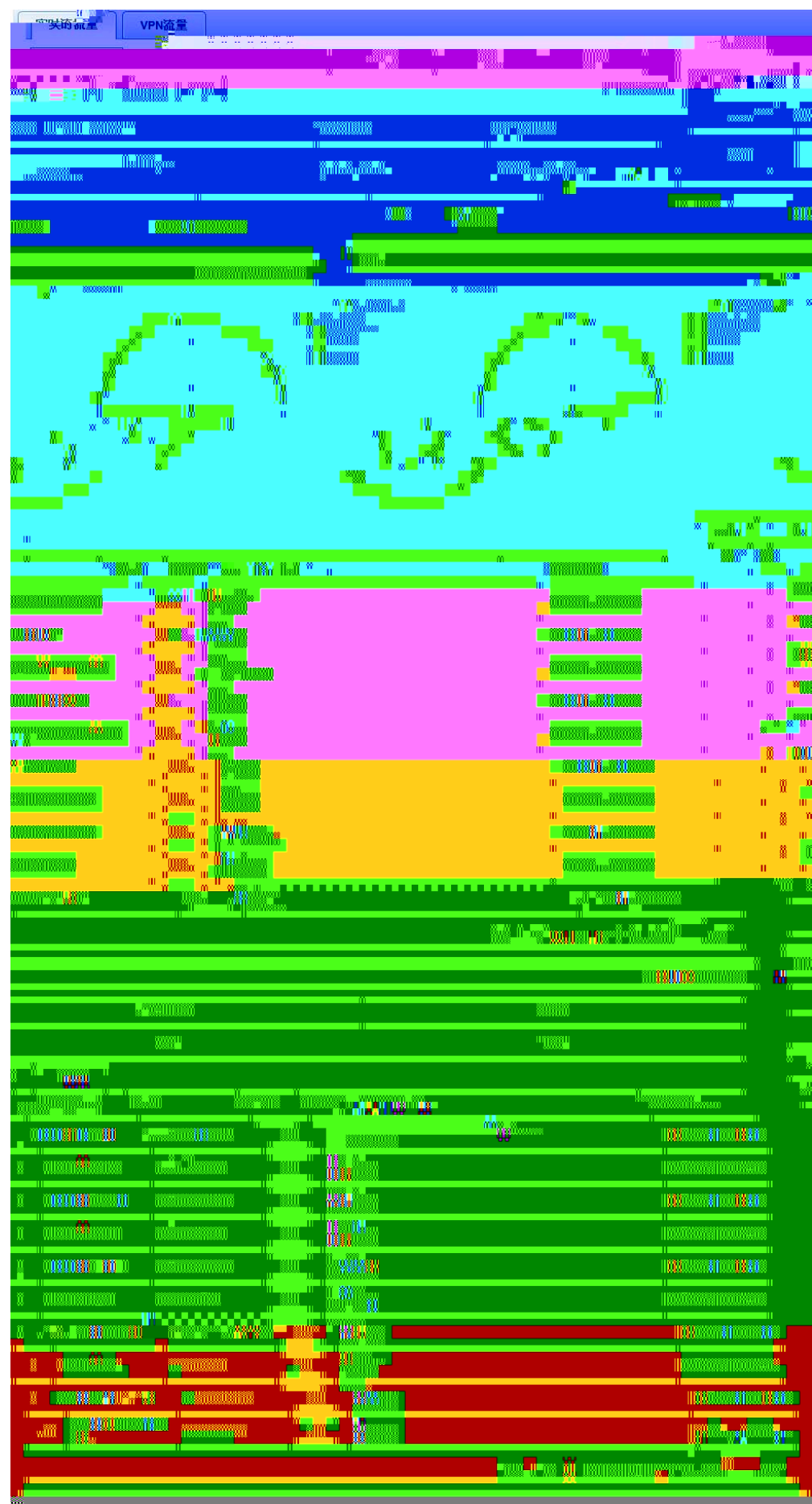
TOP10

2.5

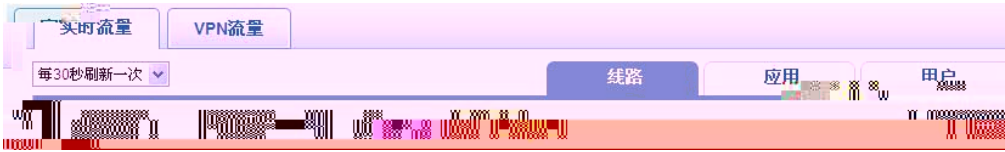
/

/

2.5.1



1



1

高级查询

[关闭]

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

确定查询

报表查询结果		高级查询
查询日期：当前		
查询类型：用户数		
查询线路：整机		
用户数统计		
在线用户数		
		1032

确定查询

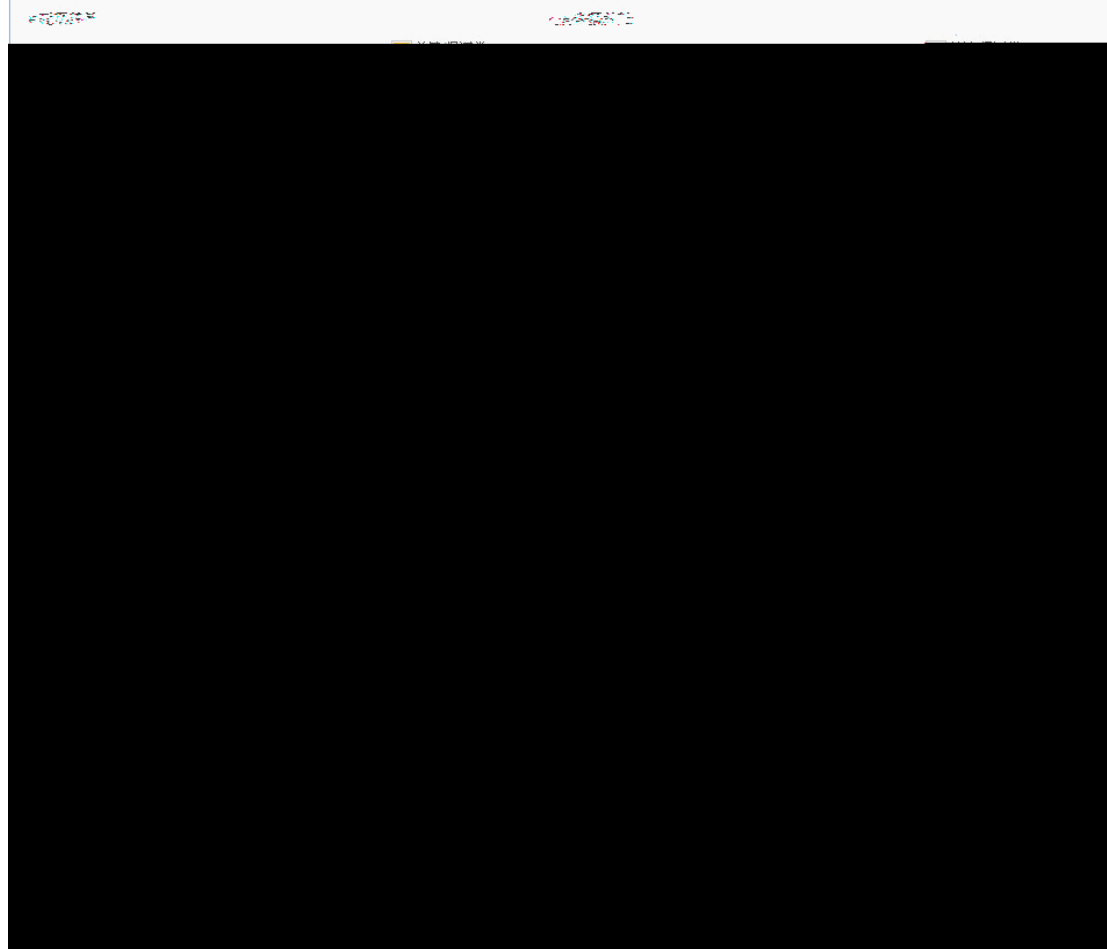
报表查询结果		会话查询	高级查询
		查询日期：当前	
		查询类型：会话数	
		查询线路：整机	
		会话数统计	
会话数			
138040			

2.5.1.1

线路



1



1

/

/

/

/

/

/

/

/

/

/

/

/

2

/

应用组

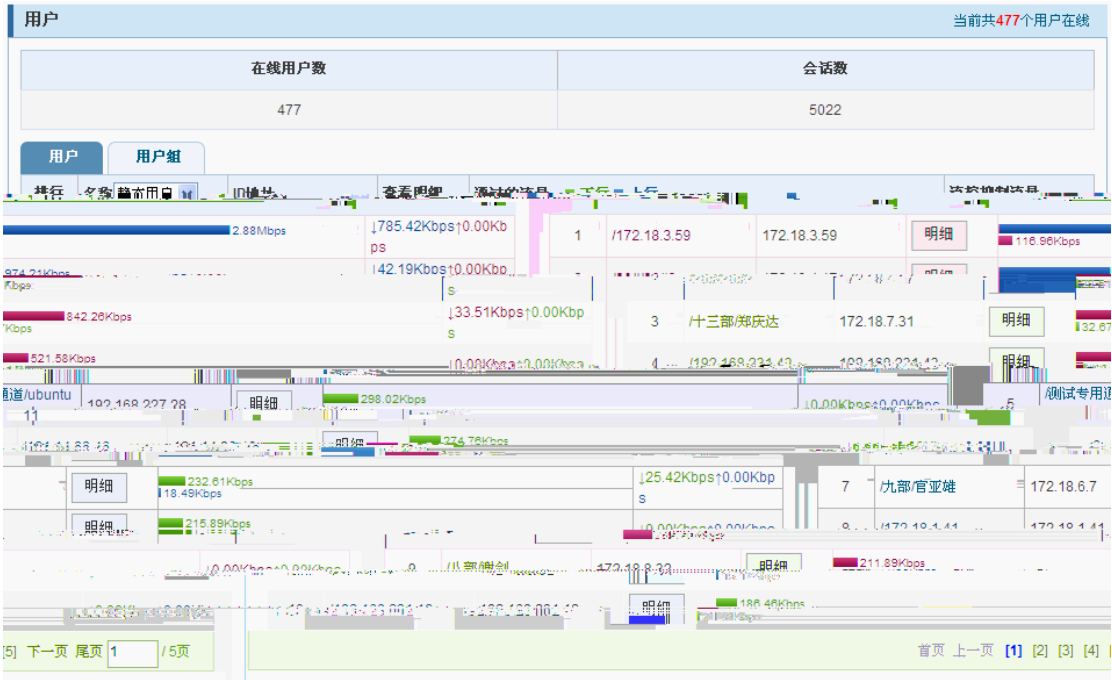


明细



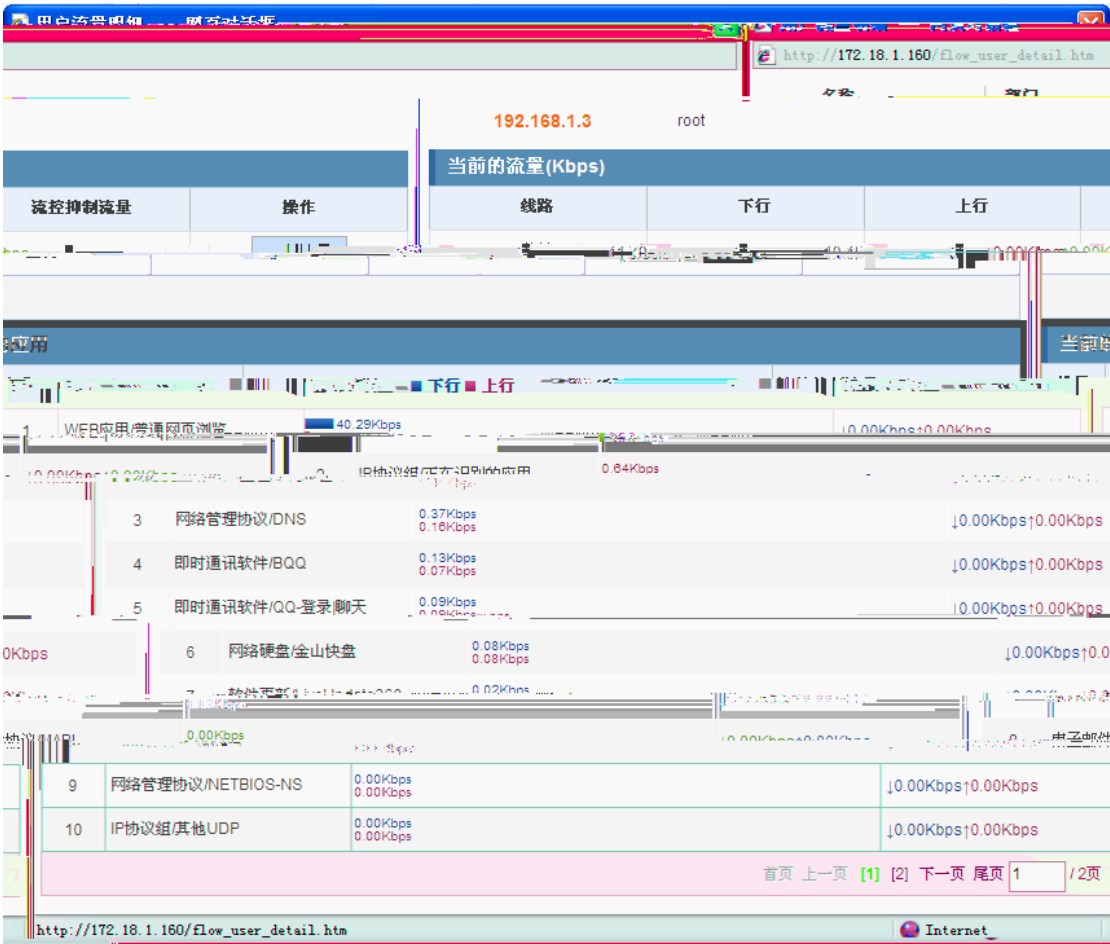
静态用户
静态用户
认证用户

3



静态用户
静态用户
认证用户

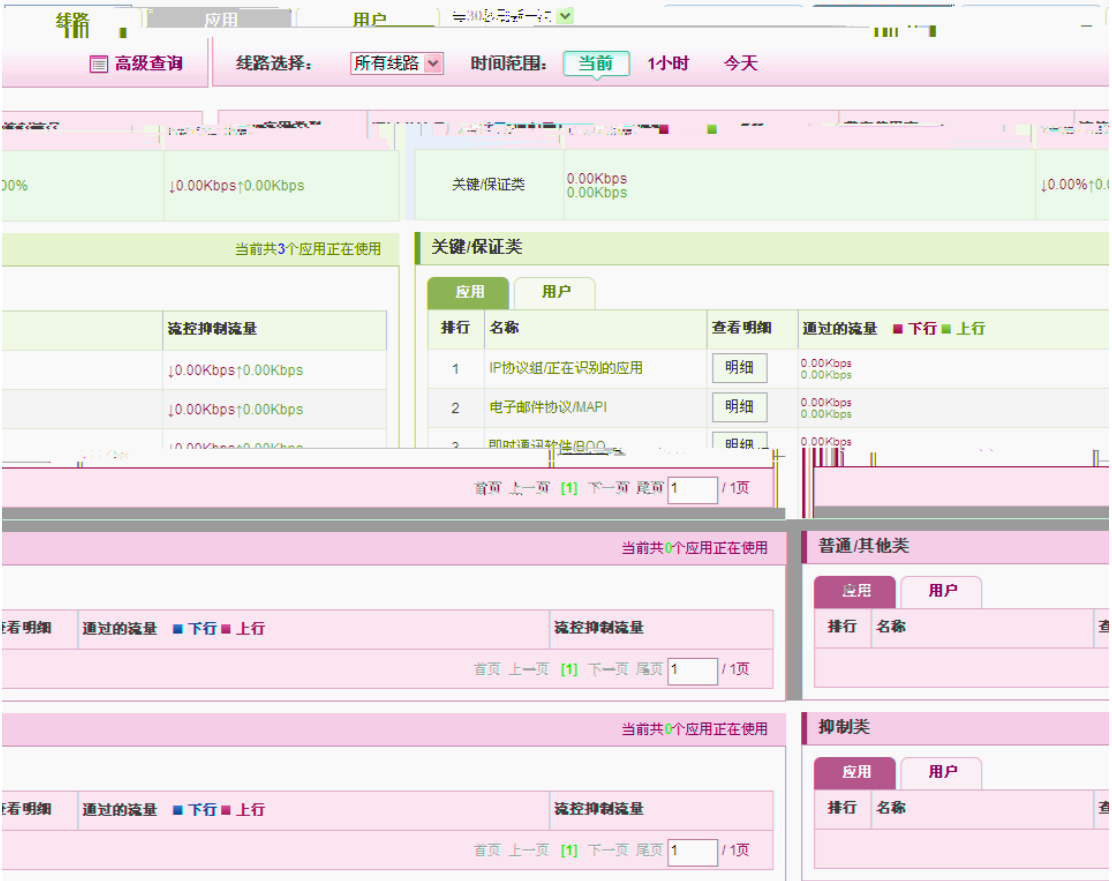
明细



阻断流量

2.5.1.2

应用



1 / /



/ /

2 / /

关键/保证类

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	IP协议组正在识别的应用	明细	433.56Kbps 1.31Mbps	↓0.00Kbps ↑0.00Kbps
首页 上一页 [1] 下一页 尾页 1 / 1页				

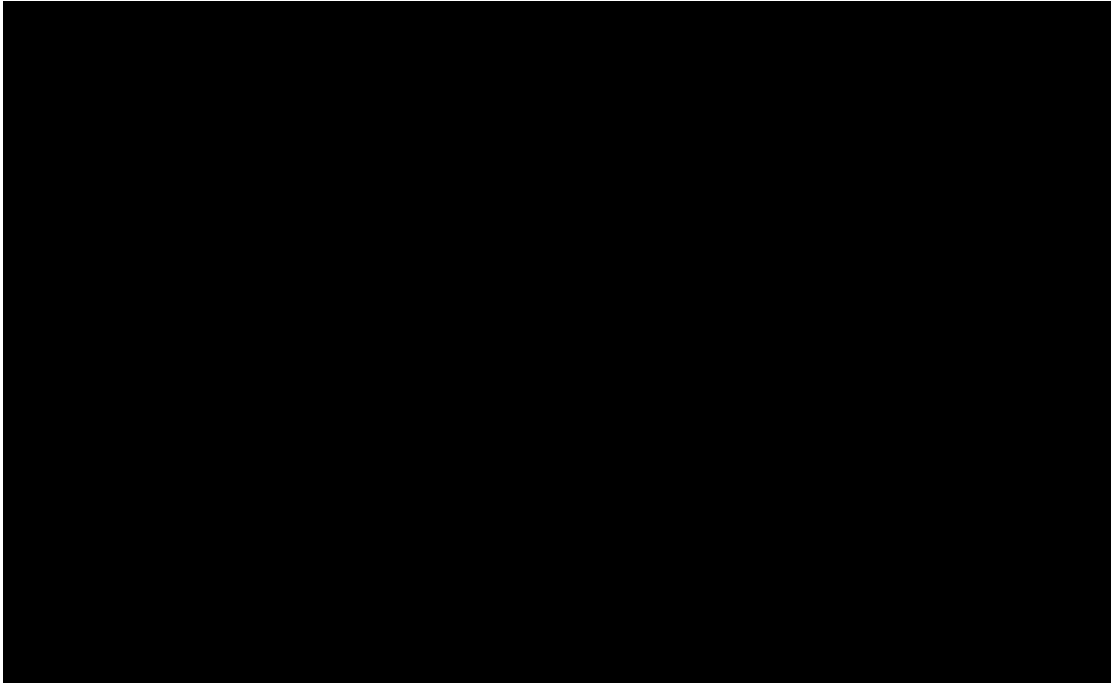
明细

2.5.1.1

/

/

关键/保证类	
应用	用户



明细

2.5.1.1

3 /

/



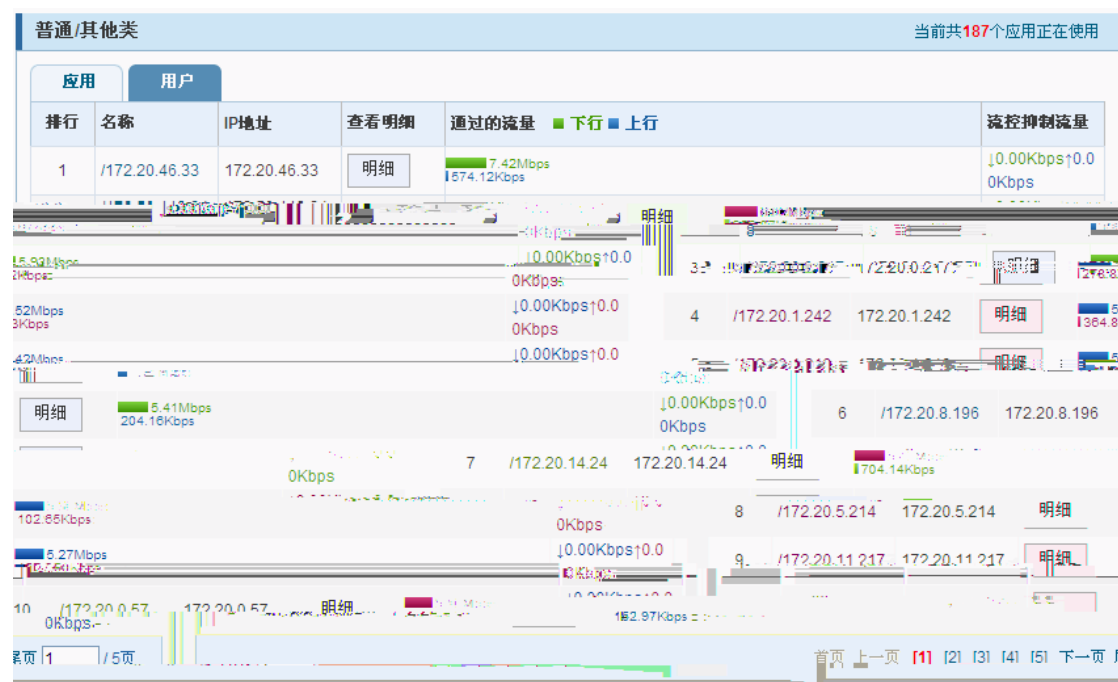
明细

2.5.1.1

普通/其他类

应用

用户



明细

2.5.1.1 4.1

@ELTuCPzE e2Ob@AA@ELTuCA

明细

2.5.1.1

2.5.1.3

()

IP

用户



VIP

明细

2.5.1.1

NPE



§

— “I ° — “I Â Ů >> “I >> “I £ W ° ¢

2.5.2 VPN



- 1

VPN

VPN
- 2

Gi0/1

VPN
- 3

10301

10301

VPN
- 4

高级查询

VPN

高级查询

关闭

时间范围：

查看实时流量情况

名称或ip：

选择接口：

Gi0/1

确定查询

IP

确定查询

排行	用户名	IP地址	通过的流量 下行上行	流控抑制流量
1	/59.56.177.93	59.56.177.93	615.92KB 610.68KB	20.17KB 20.25KB

首页 上一页 1 下一页 尾页 1 / 1页

2.6

关键应用 普通应用 抑制应用

Mbps 15% 1.5 Mbps

Mbps 0% 0 Mbps

Mbps 50% 5 Mbps 15% 1.5 Mbps

Mbps 70% 7 Mbps 20% 2 Mbps

Mbps 100% 10 Mbps 90% 9 Mbps

关闭

保存 关闭

复制方案 带宽升级

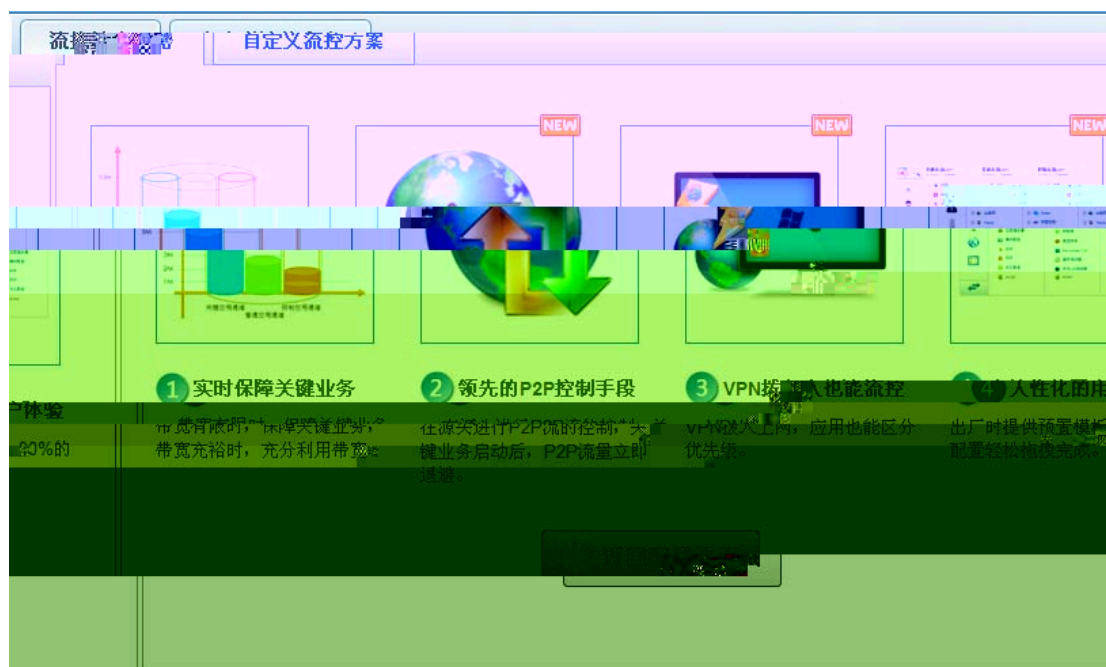
70% 7 Mbps

选中

点击“更多配置”展开下面选项

的接口

2.6.1



1



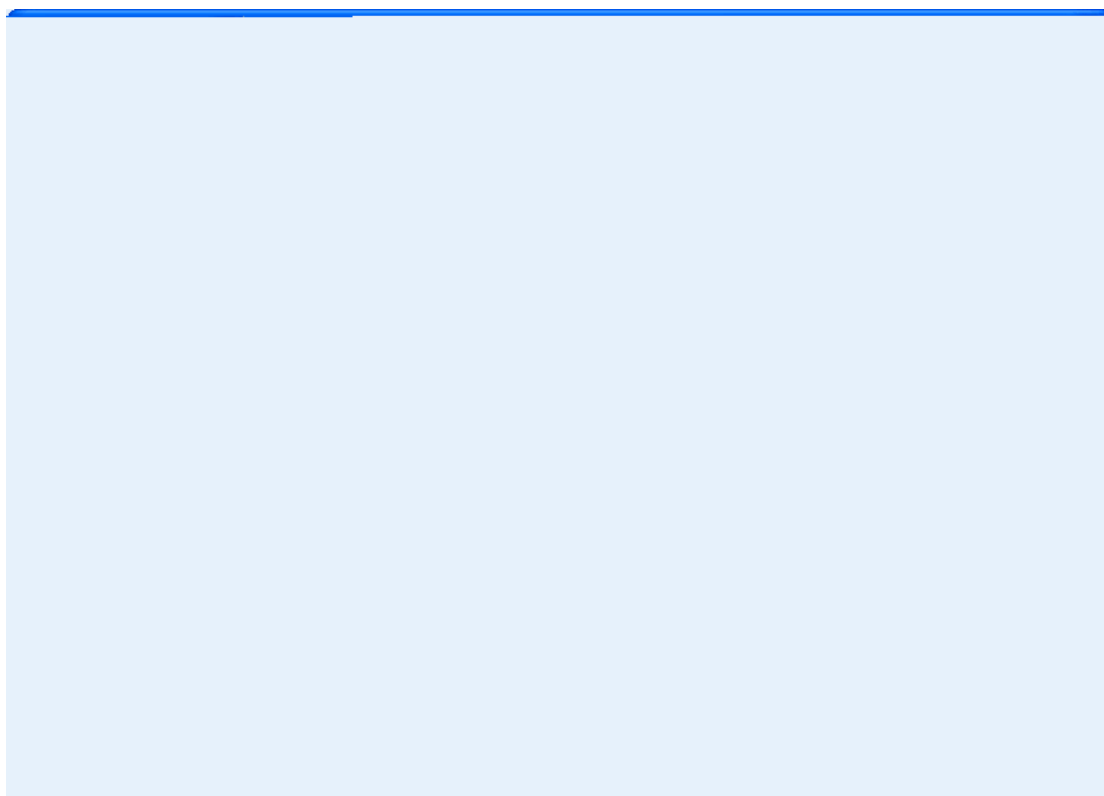
2.6.2 VIP

VIP

VIP



VIP



1 VIP 添加VIP用户或内网服务器



1

VIP

添加VIP用户或内网服务器 [关闭]

☐ 选择已有用户 ☒ 添加VIP或内网服务器

添加

VIP

IP IP

VIP

VIP

2

VIP

2

VIP

VIP

VIP

VIP

删除选中用户

VIP

3

☒ 已放行 ☐ VIP用户的阻断类应用 [指定放行范围](#)

☒ 已放行 ☐ VIP

☐ 已阻断 ☐ VIP

☒ 已放行 ☐ [指定放行范围](#)

[指定放行范围](#)

放行范围 [关闭]

☒ 放行非VPN流量

☒ 放行VPN流量

确定

VPN vpn

☒ 放行非VPN流量

VIP

vpn

VIP

vpn

2.6.3



内部服务器

外部服务器

1

IP IP IP ”

IP IP

添加外网服务器 [关闭]

名称	IP	端口
服务器1	192.168.1.1	8080

名称:

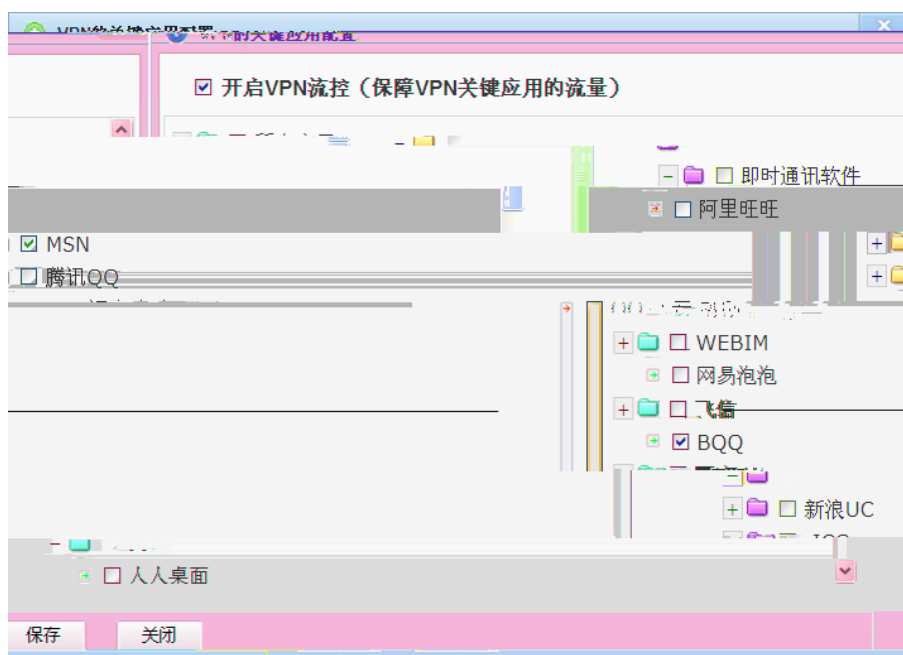
IP:

端口:

确定

IP

IP



VPN

VPN

VPN

2.6.5



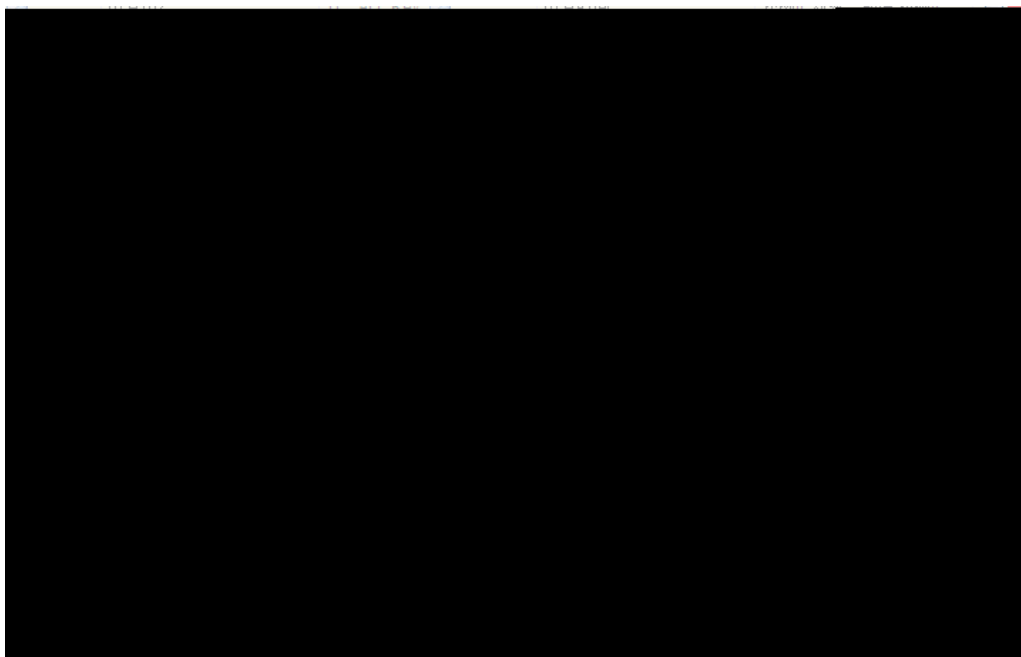
[返回主界面](#)

2.6.5.1

编辑

保存设置

IP



8

新建子通道

IP

IP

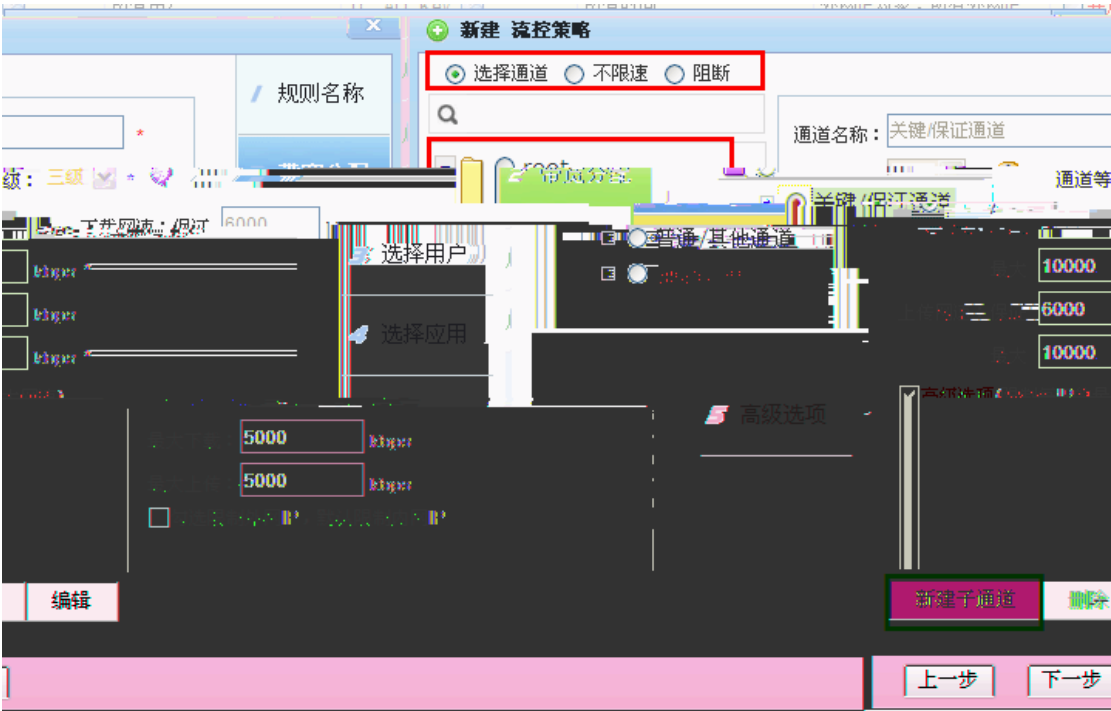
IP

IP

IP

☐ 勾选限制外网IP，默认限制内网IP

添加通道



删除

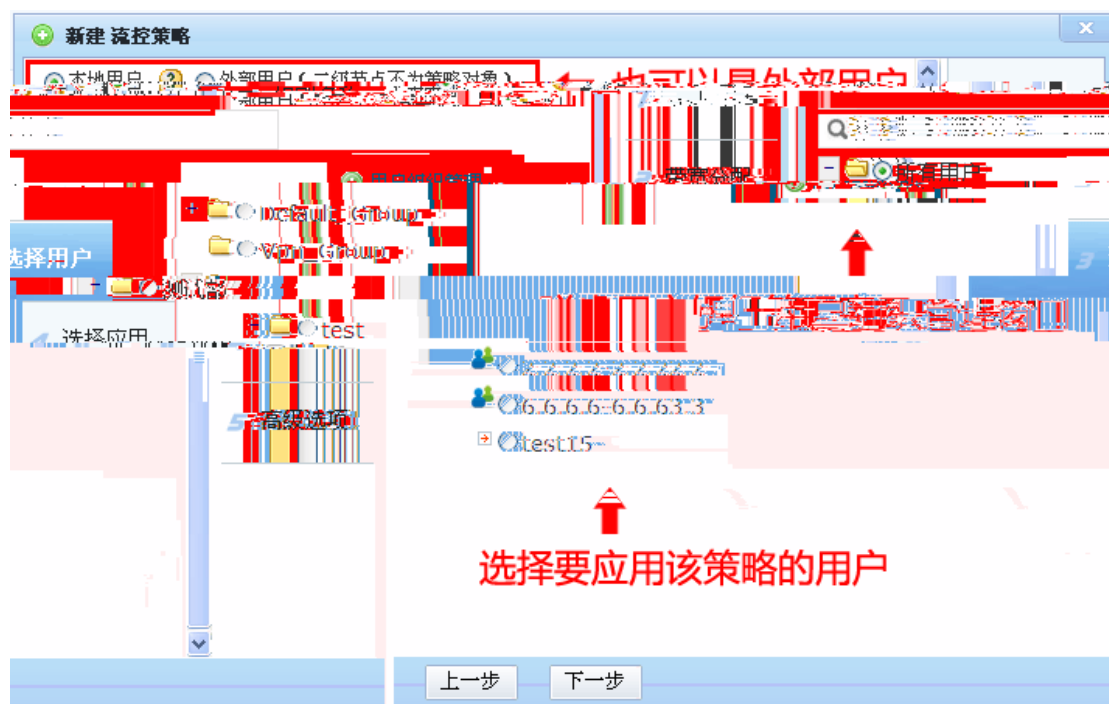
root /

/

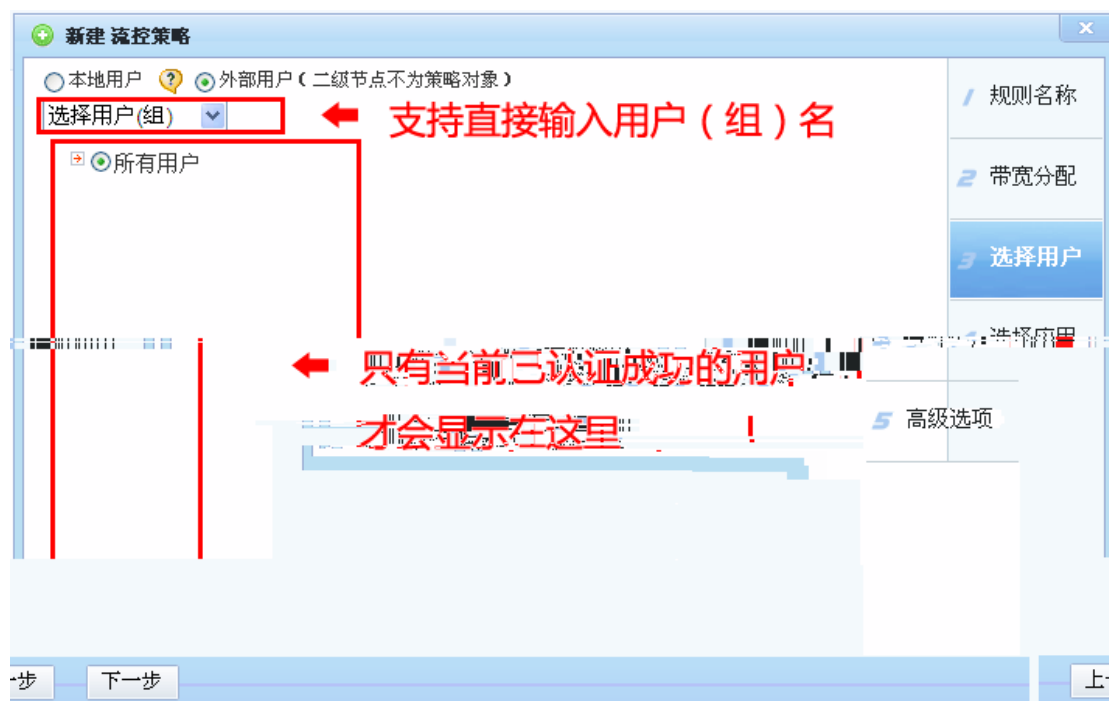
3

3

+ 用户组织管理



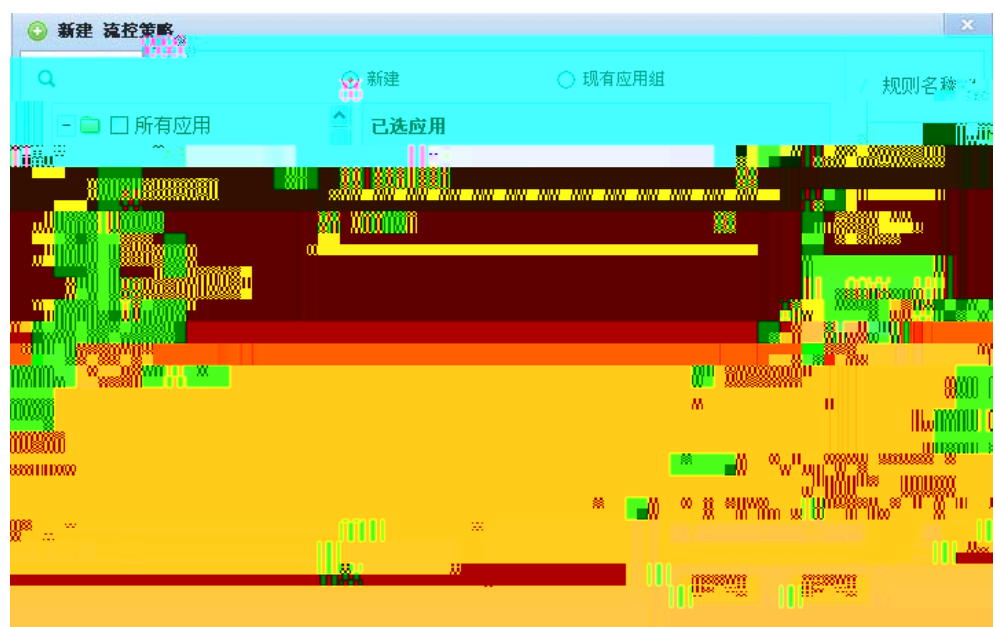
选择用户(组) ▼
 选择用户(组)
 输入用户(组)名





☒ 新建 ☐ 现有应用组

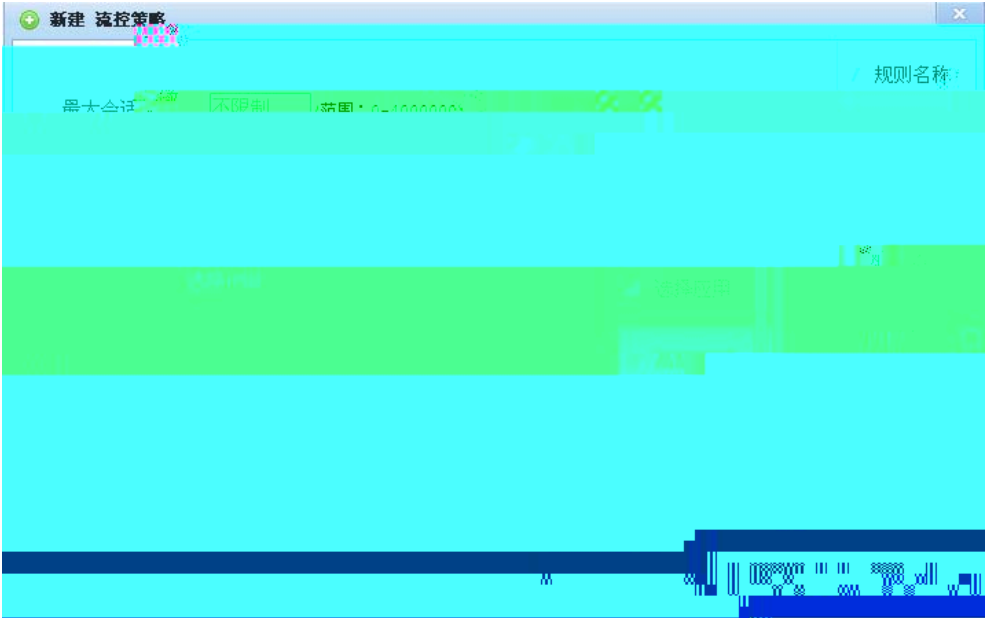
☒ 新建



☐ 现有应用组



2



0

0-4000000

所有时间

所有时间

白天

晚上

上班时间

下班时间

周末

工作日

时间管理

/

/

ip

218.25.36.6

VPN

VPN

2.6.5.2



1

2

3

4

“

”

IP

5 " " " " " " " " " "

 " " " "

6 " "

7 8 

9	策略查询
---	------

aaa

策略配置									
返回主界面		新建策略	复制策略	线路带宽和阈值	策略查询	选择线路或接口: Gi0/4			
策略名称	带宽通道	已选用户	已选应用	生效时间	高级选项	☒ 开启	状态	匹配顺序	管理
策略名称	普通/其他通道	所选用户	所选应用	生效时间	最大会话数: 无限制 所有外网IP	☒ 开启	生效		

1 / 1页

[首页](#)
[上一页](#)
[\[1\]](#)
[下一页](#)
[尾页](#)

2.6.5.3

复制策略

策略复制 [关闭]

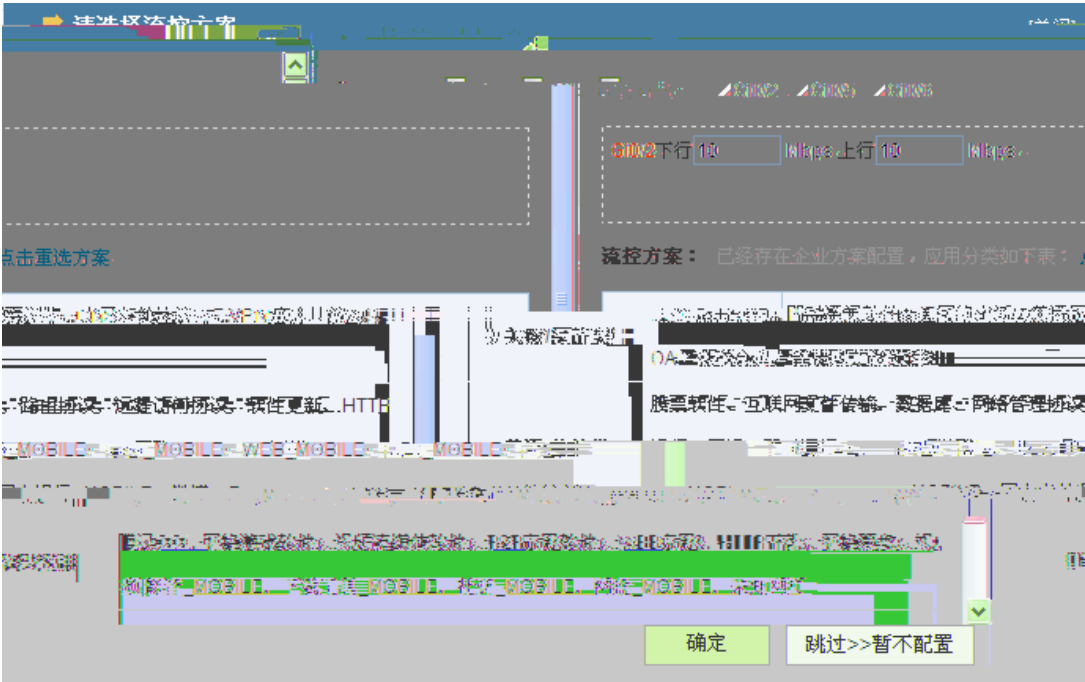
将线路 Gi0/4 ... 的策略复制到以下线路...

☐ Gi0/1 ☐ di1(Gi0/3)

确定

2.6.5.4

线路带宽和阈值



1

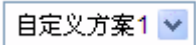
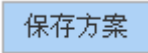
2

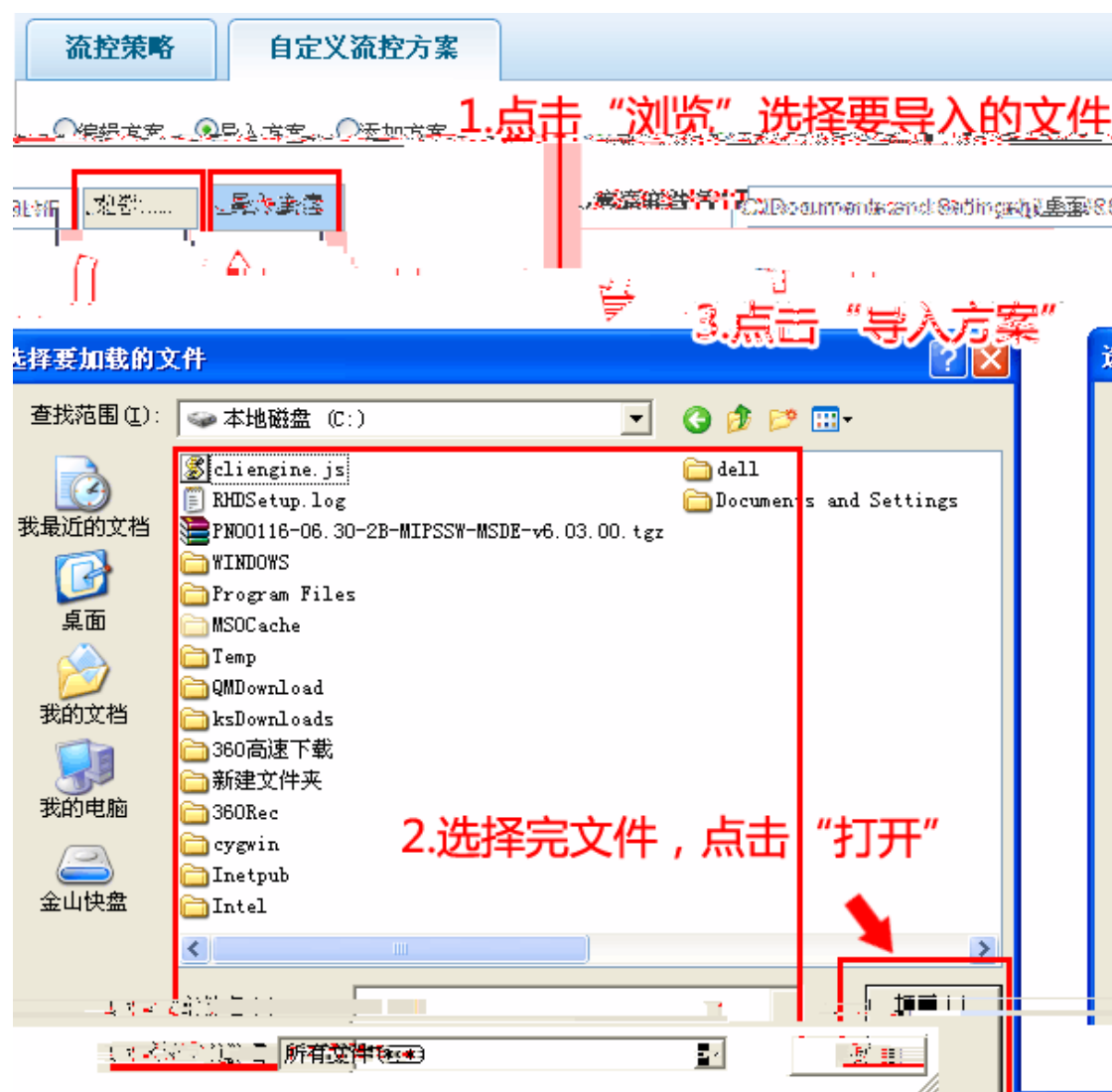
点击重选方案

2.6.8

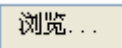
>

2.6.8.1

1.  编辑方案
2.  自定义方案1
3.  添加
4.  普通网页浏览 X
5.  保存方案



1.  导入方案

2. 

3. 

4.

2.6.8.3

2.7

2.7.1



2.7.1.1

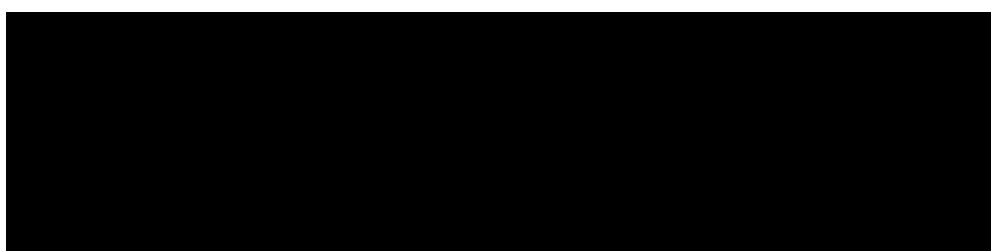




添加阻断应用



确定

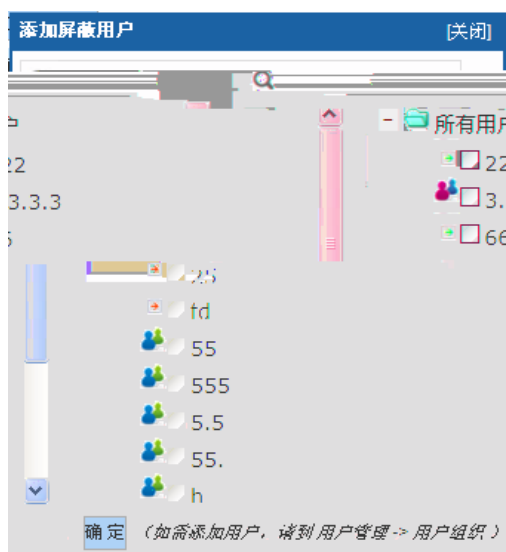


删除全部

2.7.1.2



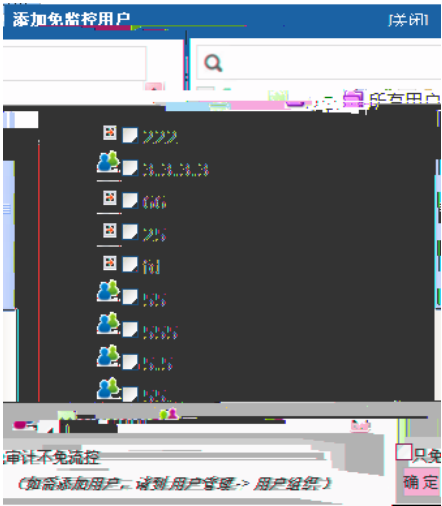
添加屏蔽用户



确定

屏蔽用户列表			
用户名称	IP地址	MAC地址	操作
bbb-1	2.2.2.2	#	删除
eee	9.9.9.9	#	删除
首页 上一页 [1] 下一页 尾页 1 / 1页			





☐ 只免审计不免流控

确定

免监控用户列表				
用户名称	IP地址	MAC地址	是否免流控	操作
删除	ddd	1.1.1.1 - 1.1.1.3	#	√
/1页		首页 上一页 [1] 下一页 尾页 1		

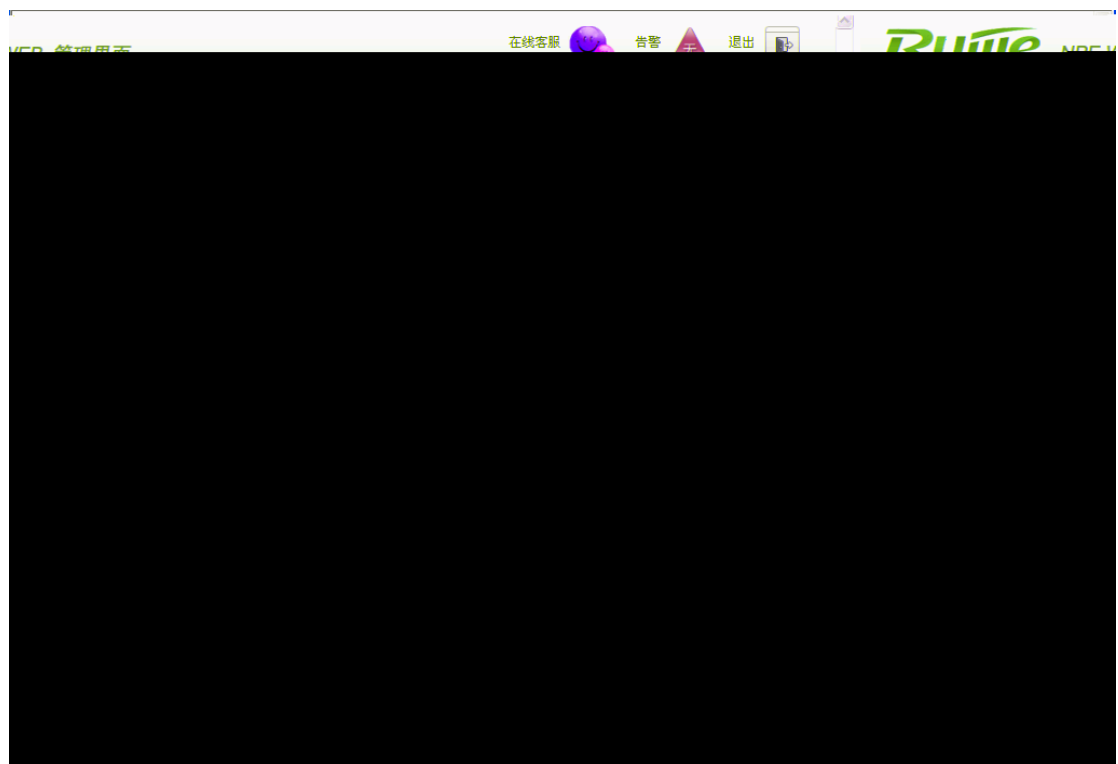
√

×

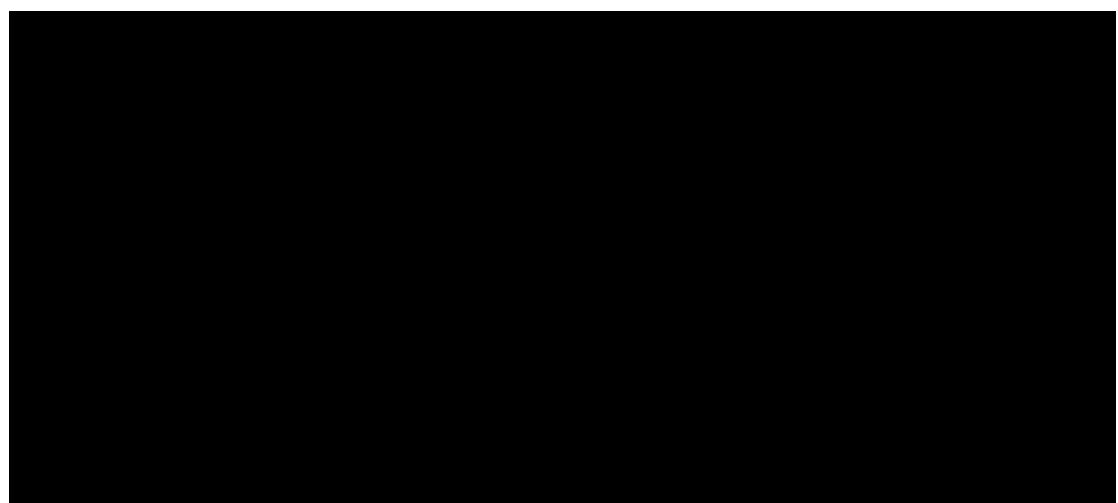
删除

选择用户





2.8.1



/

/

2.8.1.1

1

 [添加应用分组](#)

添加自定义应用分组

[关闭]

应用组名：

已选应用：

添加应用

应用名称	删除
首页 上一页 [1] 下一页 尾页 1 / 1页	

确定

添加应用

添加应用

[关闭]

Q

所有应用

+

☒ 即时通讯软件

+

☐ IP网络电话

+

☒ 网络游戏软件

+

☐ 视频流媒体软件

+

☐ P2P应用软件

+

☐ 股票软件

+

☐ 其他应用

互联网文件传输

+

电子邮件协议

▼

+

字体颜色区别应用类型：关键普通抑制非法

确定

确定

添加自定义应用分组

[关闭]

应用组名：

bbb

已选应用：

添加应用

应用名称	删除
网络游戏软件	删除

删除

删除

确定

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,普通网页浏览,DNS,安全协议,VPN应用	
抑制类	视频流媒体软件,P2P应用软件,互联网文件传输,网络硬盘,下载	
阻断类	非法DNS	
网络游戏软件,股票软件,WEB应用,电子邮件协议,数据库,网络		
管理化部署		
P2P应用软件,股票软件,WEB应用		
即时通讯软件,网络游戏软件		
		bbb
首页 上一页 [1] 下一页 尾页 1 / 1页		

2



编辑自定义应用分组 [关闭]

应用组名:

已选应用: 添加应用

应用名称	删除
即时通讯软件	删除
网络游戏软件	删除

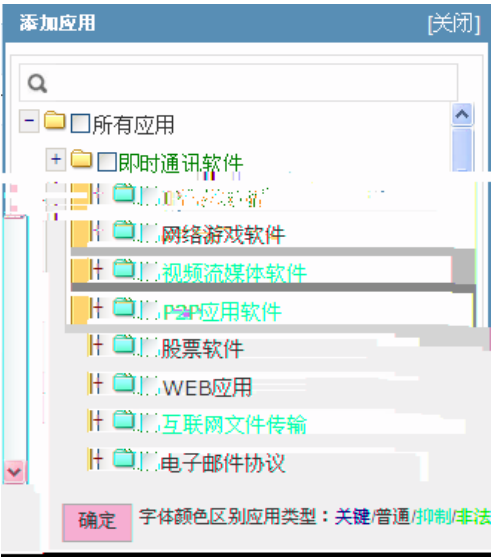
首页 上一页 [1] 下一页 尾页 1 / 1页

编辑

添加应用

删除

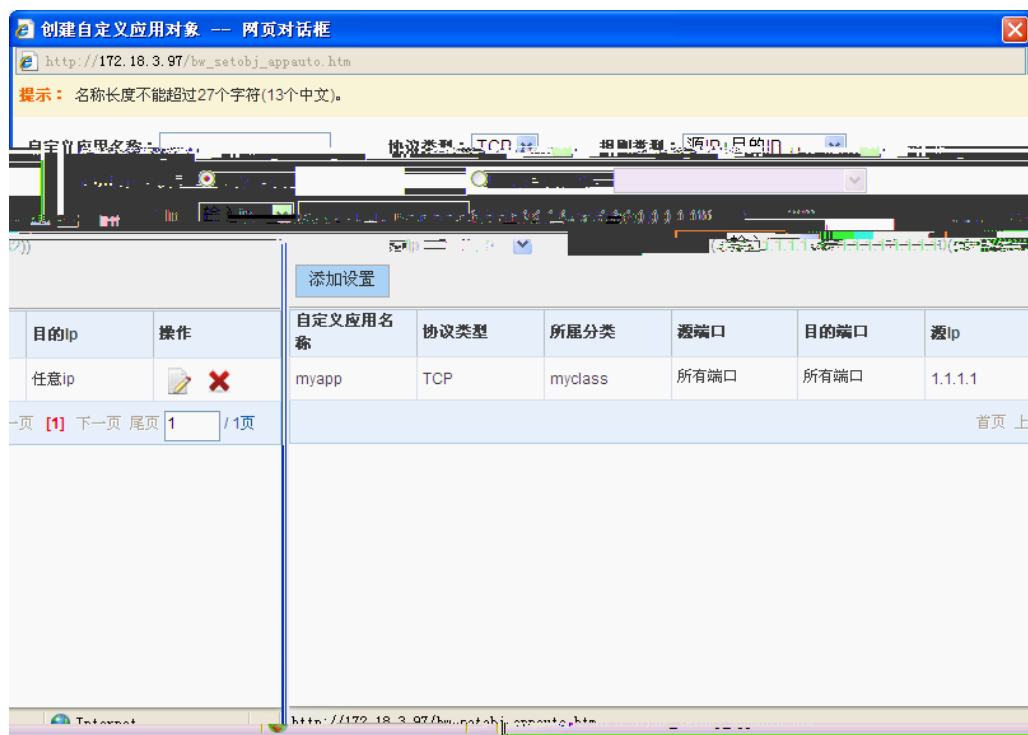
添加应用



3



2.8.1.2



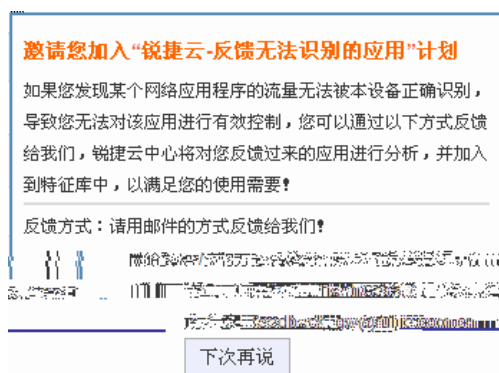
IP

添加设置



2.8.1.3

- 反馈无法识别的应用



2.8.2

说明：时间对象用于定义策略生效时间。

时间对象名称：

新对象名

选择已有对象

*

星期一

星期二

星期三

星期四

星期五

星期六

星期天

时间段1：

~

+

添加时间段

添加设置

时间对象列表：

所有时间

时间周	时间段	操作
每天	0:00 - 23:59	编辑 删除

查看全部

删除

1

1

2

☒ 星期一 ☒ 星期二 ☒ 星期三 ☒ 星期四 ☒ 星期五

3

1

时间段1：

08:00

~

12:00

+

添加时间段

2

4

添加设置

2

编辑

9:00~12:00 13:00~18:00

工作时间

71

编辑

9:00~12:00 13:00~18:00

保存编辑

时间对象名称：

新对象名

选择已有对象

工作时间

星期一

星期二

星期三

星期四

星期五星期六星期天

时间段1: 09:00 ~ 12:00

保存编辑 添加设置

3

删除

删除全部

2.8.3 IP



自定义应用分组

时间对象

外网IP对象

VLAN对象

删除组

新建子组

新建IP子组

添加用户

Out_Server

编辑组

	用户名称	IP 地址	管理
☐	out1	3.3.3.3	编辑 删除

批量导入导出外网ip

IP

IP

1

编辑组

IP

IP

编辑用户组

[关闭]

用户组名: Out_Server *

上级组名: 所有外网IP

确定

2

删除组

IP

IP

Out_Server 的用户列表 删除选中用户

☐	用户名称	IP 地址	管理
☐	aaa	3.3.3.3-3.3.3.7	编辑 删除

首页 上一页 1 下一页 尾页 / 1页

IP

编辑

IP

编辑用户 [关闭]

*

*

▼

保存

删除

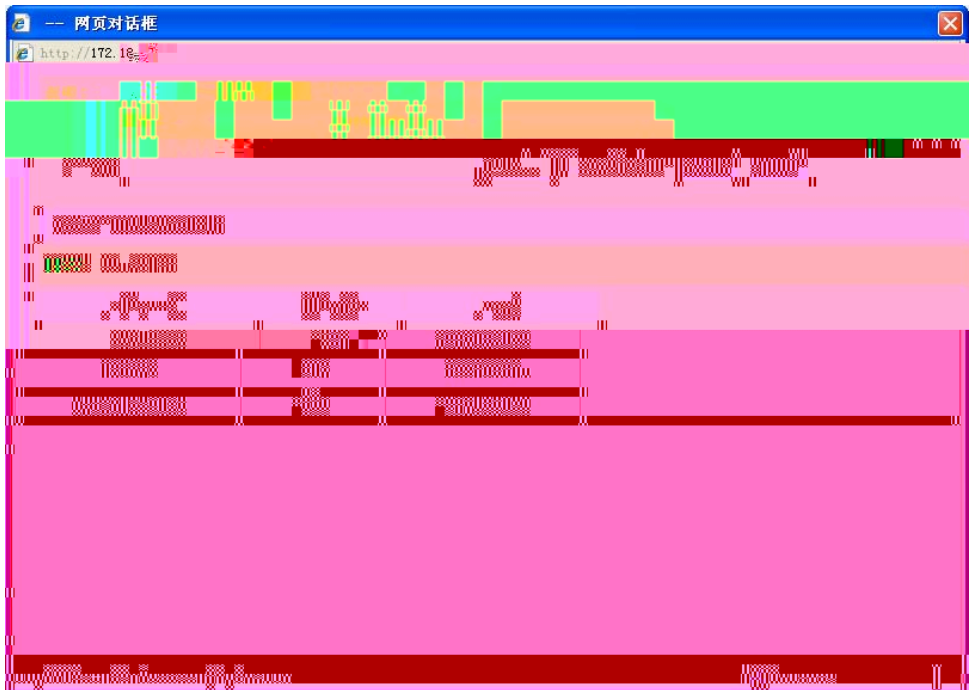
IP

删除选中用户

7

IP

批量导入导出外网ip



IP
ipuser-info.csv

IP

IP
IP

导入文件信息规格示例：

提示：/表示根目录

归属用户组	用户名称	IP地址
网络中心	网络中心	192.168.1.59
网络中心	网络中心	192.168.1.9
网络中心	网络中心	192.168.1.29

浏览...

ipuser-info.csv

导入用户

说明：导入用户信息有利于实名制管理用户，方便找到用户。

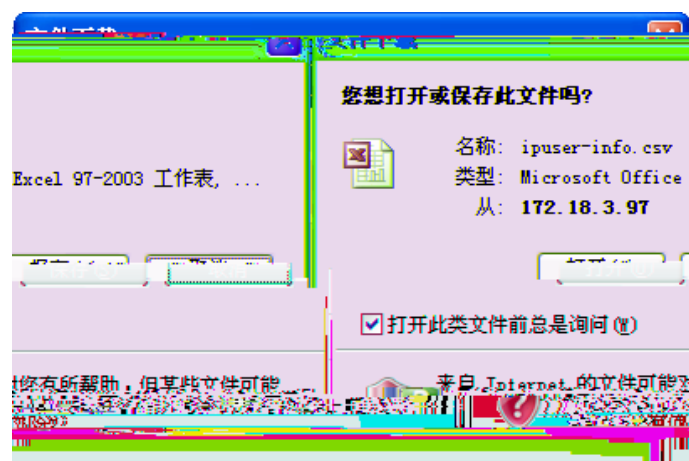
提示：导入用户的文件名必须为ipuser-info.csv，并按以下示例的格式填写对应表格

归属用户组	用户名称	IP地址
网络中心	网络中心	192.168.1.59
网络中心	网络中心	192.168.1.9
网络中心	网络中心	192.168.1.29

IP

导出用户

保存(S)



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。

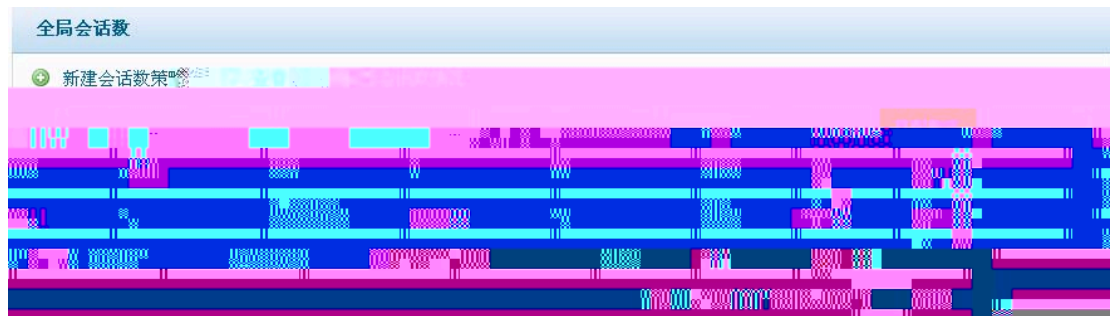
VLAN对象名称：

IP范围： ~ VLAN对象ID： 单个IP，或IP段（如：1.1.1.1），多个IP可以用逗号“,”隔开

3 VLAN VLAN 删除 VLAN

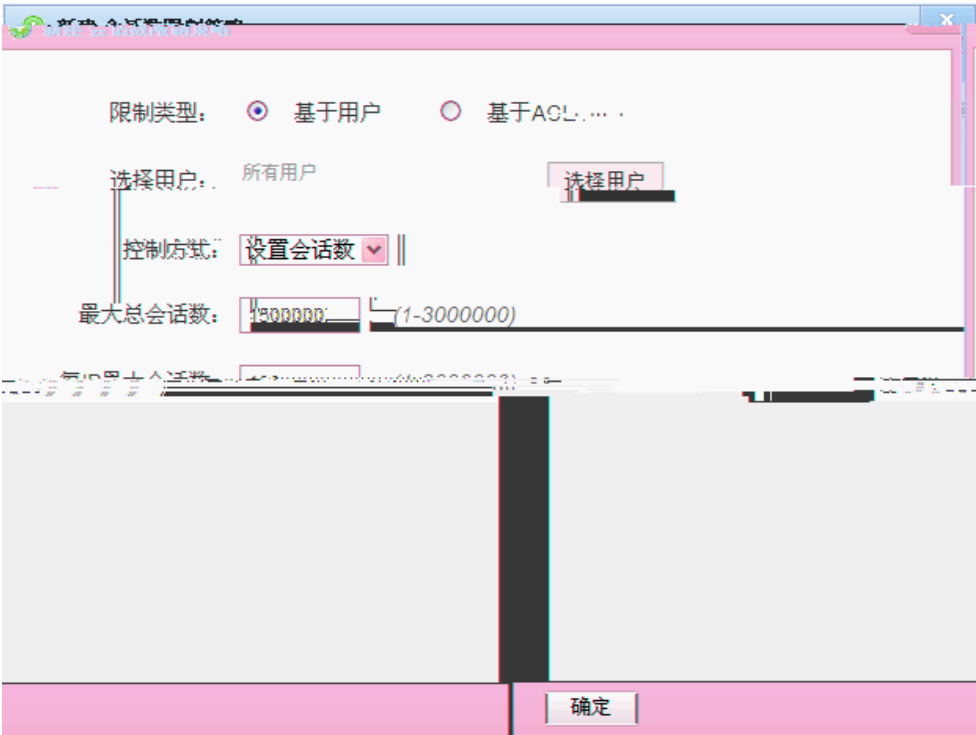
vlan1 删除

2.9



2.9.1

1



选择用户

确定

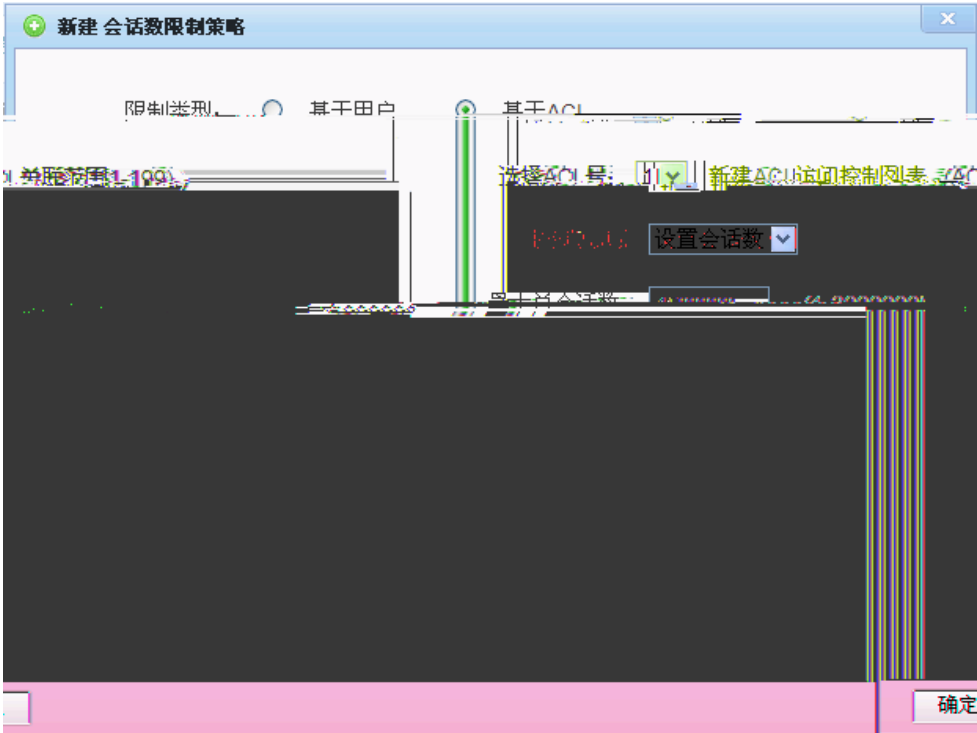


设置会话数
设置会话数
阻断

IP

1~3000000

2 ACL



ACL 1 ACL

ACL 新建ACL访问控制列表 ACL

ACL / / /ACL ACL

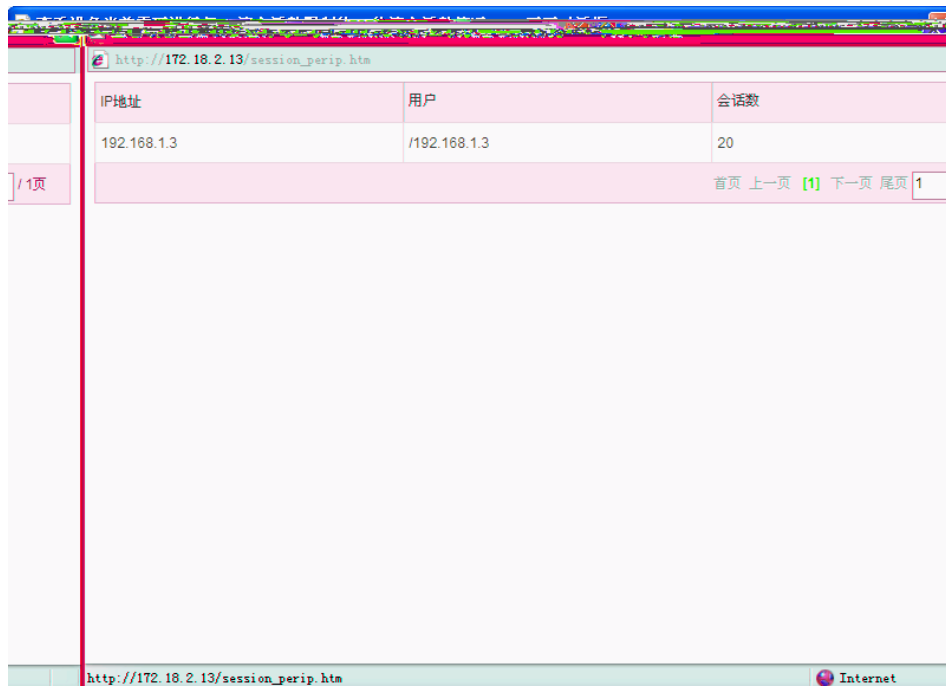


2.9.2 IP

 查看每IP流会话数情况

IP

IP



The screenshot shows a web browser window with the address bar displaying `http://172.18.2.13/session_perip.htm`. The main content area contains a table with three columns: IP地址, 用户, and 会话数. The table has one data row showing IP 192.168.1.3 with user /192.168.1.3 and 20 sessions. The browser's status bar at the bottom shows `http://172.18.2.13/session_perip.htm` and an Internet icon.

IP地址	用户	会话数
192.168.1.3	/192.168.1.3	20

Page navigation: 1 / 1页, 首页, 上一页, [1], 下一页, 尾页, 1

2.10 /ACL

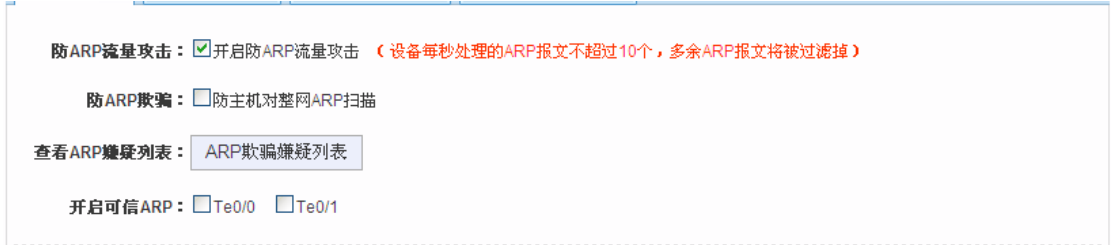
2.10.1



1 ARP

ARP

ARP



ARP

ARP

ARP

10

ARP

ARP



WEB

2.10.2 ARP

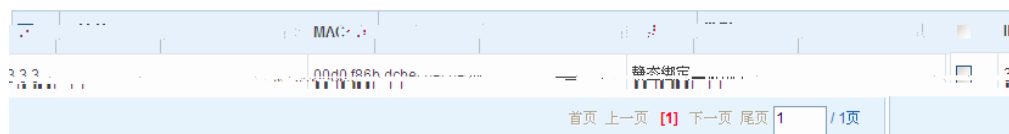


1 IP/MAC IP/MAC 手工静态绑定



IP MAC 保存设置 开始扫描 IP/MAC ARP

2 ARP



IP/MAC

3

ARP

IP/MAC

删除静态绑定

4

ARP

IP/MAC

动态>>静态绑定

5 ARP

ARP

ARP

PC

MAC

PC

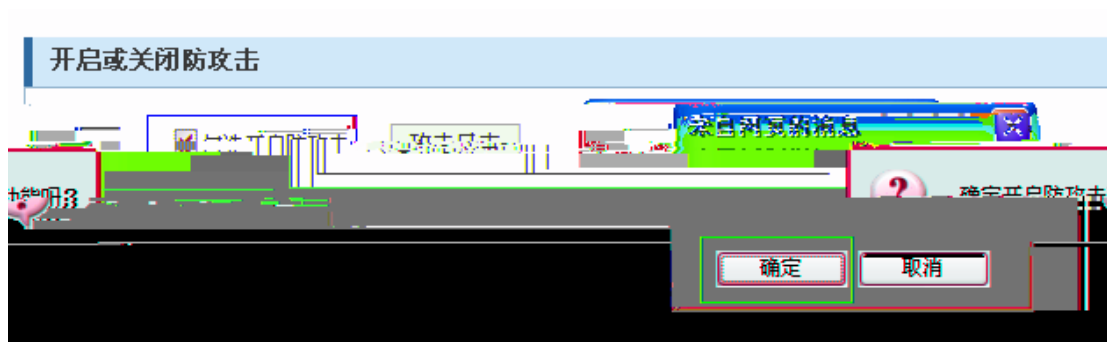
ARP

ARP

ARP

2.10.3

☐ 勾选开启防攻击



2.10.3.1

IP
Ping of Death Teardrop



LAND IP
Land
UNIX TCP SYN
Windows NT
ICMP
ICMP
IP
Winnuke
WinNuke
Windows
NetBIOS 139 OOB out-of-band NetBIOS
IP
IP
IP



2.10.3.3

要关联的源IP或IP段：

8.8.8.8
6.6.6.0/255.255.255.0
7.7.0.0/255.255.0.0
9.9.9.9|

IP

"/"

192.168.0.0/255.255.255.0

☐ 检测所有报文 ☒ 检测特定报文

☐ 检测TCP、UDP和ICMP报文 ☒ 不检测TCP报文

☒ 检测UDP报文 ☐ 不检测UDP报文

☒ 检测ICMP报文 ☐ 不检测ICMP报文

IP

IP

IP

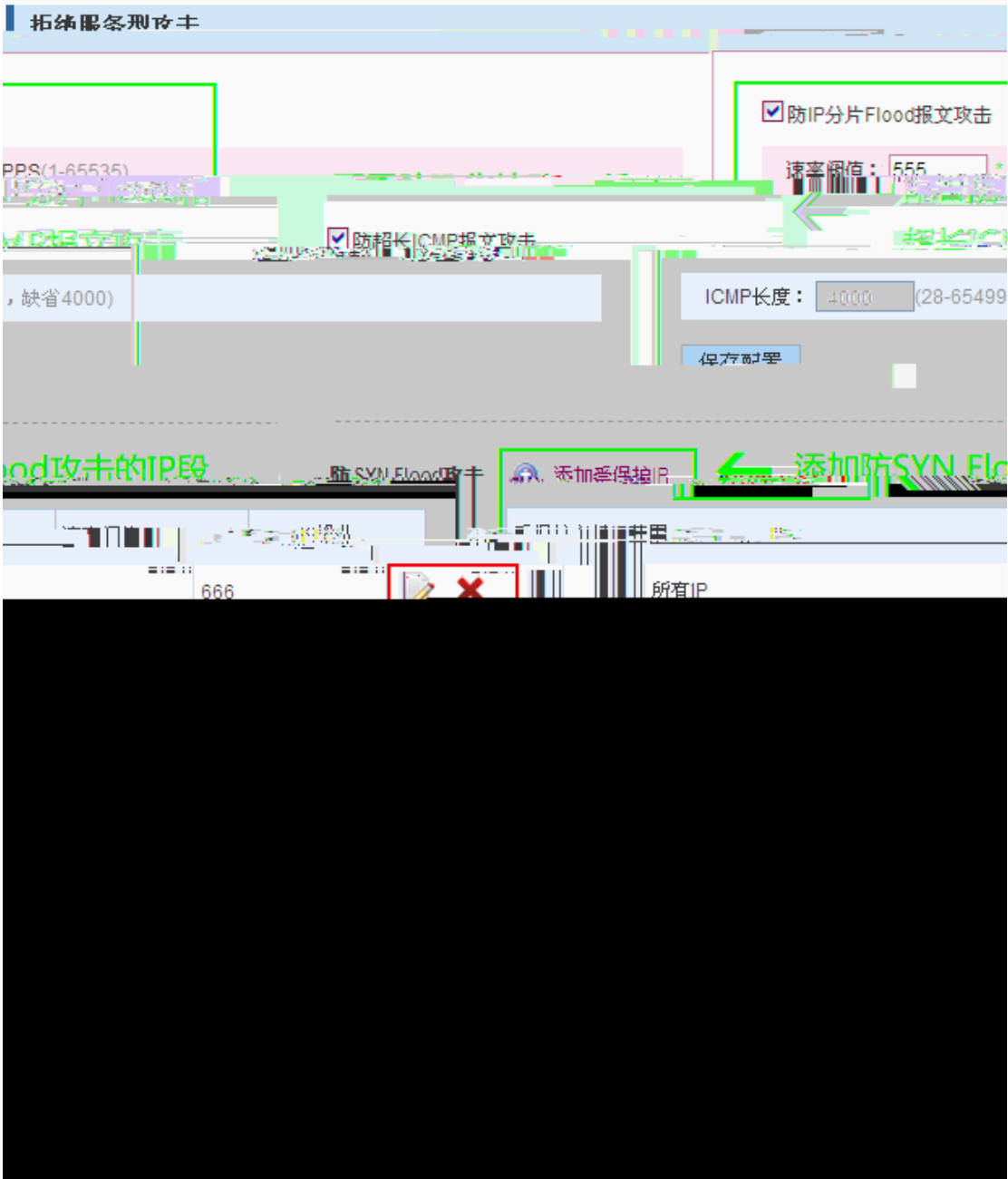
2.10.3.4

DoS Denial of Service

DoS

SYN

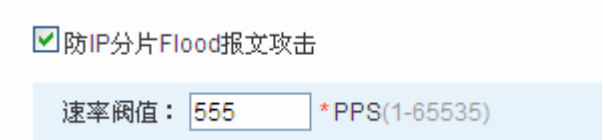
Flood Fraggle



IP Flood teardrop jolt2

flood

CPU



ICMP

ICMP

IP Flood攻击

添加受保护IP

防ICMP

主机IP范围	速率阈值(PPS)	操作	受保护
800 2.2.2.0/255.255.255.0	5000000		

第一页

1

下一页

尾页

1

/ 1页

GO

首页

上一步

IP

SYN Flood

UDP Flood

UDP



IP

IP



2.10.5



ACL

in or out

添加设置

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。

特殊协议跟踪：目前支持FTP特殊协议跟踪，确保开启反射ACL后，数据通道能够建立临时的通行访问机制。

ACL

ACL访问控制列表：

作	ACL号	应用于接口	过滤方向	反射ACL	操作
---	------	-------	------	-------	----

2.10.6 ACL

ACL

ACL

说明：ACL即访问控制列表（Access Control Lists），通过配置一系列匹配规则，对指定数据流（如限定的源IP地址、端口号等）执行允许或禁止通过，达到对网络接口数据的过滤。

新建ACL访问控制列表

请选择欲查看的 ACL 访问控制列表 110 的规则列表

生效时间对象	状态	规则顺序	操作	动作	协议	源IP通配符掩码	源端口	目的IP通配符掩码	目的端口	生效
所有时间	生效	↓	编辑 删除	禁止	ip	192.168.188.4 / 0.0.0.0		7.7.7.7 / 0.0.0.0		
任意	所有时间	生效	↑	编辑 删除	允许	ip	任意			

删除全部

1 ACL

ACL访问控制列表 新建

ACL

ACL



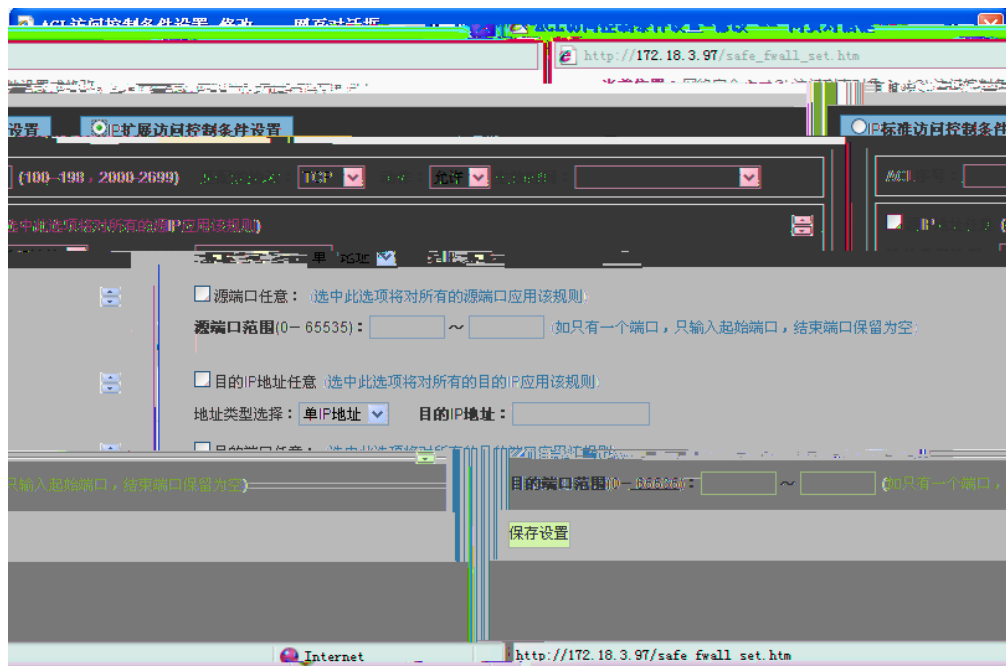
IP

ACL

IP

IP

IP



ACL

TCP ▾

TCP

UDP

IP

ICMP

TCP UDP

IP ICMP



单IP地址 ▾

Ip

IP

IP

IP

IP

保存设置

IP



§

1 ĩ ĩ ĩ IP ĩ á ĩ ĩ ĩ ε ĩ ÿ 0 z ¢

2 Ð Ä ĩ ĩ Š IP ĩ ĩ IP ĩ © ĩ 1 ÓK IP ĩ

 K ŸH ¢ Ð ĩ 1° I ĩH IP ĩ ĩ ĩ Ó ĩ 0° I K Q

 λ ¢ ĩ ĩH Ð Ó 0.0.0.0 " Ÿ ĩ 9 ¢

2 ACL

请选择欲查看的 ACL 访问控制列表 110 的规则列表									
7.7.7.7 / 0.0.0.0		所有时间	生效	↓	编辑 删除	禁止	ip	192.168.188.4 / 0.0.0.0	
任意		所有时间	生效	↑	编辑 删除	允许	ip	任意	

110

ACL

ACL



ACL

编辑

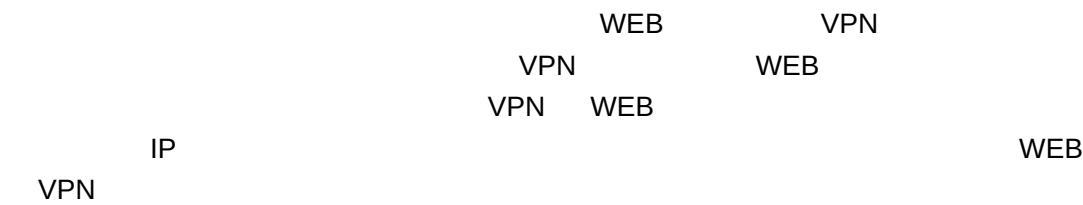
ACL

删除

ACL

2.11

2.11.1



1  编辑组

2 添加组



31

3 删除组

4 添加用户(段)

IP

新建用户 [关闭]

用户名称： *

IP&MAC： ☒ IP地址 ☐ MAC地址 ☐ IP和MAC ☐ 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)

认证上网方式：

确定

VPN WEB

WEB

VPN

WEB

VPN

WEB

WEB



WEB

WEB

IP MAC

MAC

IP MAC

IP

IP

IP-

IP

web

5

操作

操作

+添加用户(段)

+添加组

6

1. 单击“策略管理”按钮，进入策略管理页面。

56

7

本系统的策略管理信息

关联其它策略...

取消关联

☐ 排除继承 (该用户不使用父组的策略)

行为策略管理

状态	管理	☐ 策略组名称	策略归属
未生效	不可删除	☐ 23	继承所属组策略

首页 上一页 [1] 下一页 尾页 1 / 1页 GO

关闭

(继)

+ 行为策略管理

/ / > >

8

✕ 删除 ↻ 编辑

批量编辑属性 [关闭]

允许用途：☒ 允许做web认证用户 ☒ 允许做VPN用户

修改密码：☒ 认证成功后支持修改密码

禁止登录：☐ 禁止登录(不允许上网)

确定

9



编辑用户 [关闭]

用户名称：

允许用途：☐ 允许做web认证用户 ☐ 允许做VPN用户

移动到：

确定

10

 搜索用户名 查询

IP

✕ 删除 ↻ 编辑 **查询参数**

搜索用户名 查询

☐	名称	IP地址(MA	行为策略数	管理
☐	韩伟业 查询结果	无		✕

首页 上一页 [1] 下一页 尾页 1 / 1页

2.11.2

用户管理

导入导出用户

特殊用户管理

说明：导入用户信息有利于实名制管理用户，方便找到用户。

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

文件名称：

浏览

导出用户

导出用户

导入文件信息规格示例：

提示：其中“MAC地址”可以不填，但是在对应单元格中必须有一个空格。

归属用户组	用户名称	密码	IP地址	MAC地址	是否双向绑定
人力资源部	张三	888	192.168.1.59	00-23-AE-86-B3-E9	Y
财务部	李四	888	192.168.1.9-192.168.1.12	Y	Y
研发部/研发5部	王五	888	192.168.1.29	00-87-EF-12-4F-24	N

user-info.csv

导入文件信息规格示例：

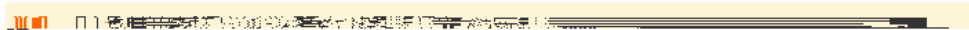
提示：其中“MAC地址”可以不填，但是在对应单元格中必须有一个空格。

归属用户组	用户名称	密码	IP地址	MAC地址	是否双向绑定
人力资源部	张三	888	192.168.1.59	00-23-AE-86-B3-E9	Y
财务部	李四	888	192.168.1.9-192.168.1.12	Y	Y
研发部/研发5部	王五	888	192.168.1.29	00-87-EF-12-4F-24	N

浏览...

user-info.csv

导入用户



导出用户

保存(S)



WEB

上网屏蔽模式

说明： 开启上网屏蔽模式后所有内网用户将不能通过设备上网，除非将用户设置为“排除屏蔽用户”；

☒ 开启上网屏蔽模式

排除屏蔽用户列表  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
--------------------------	------	------	-------	----

首页 上一页 **[1]** 下一页 尾页 / 1页

 添加排除屏蔽用户

添加排除屏蔽用户 [关闭]

所有用户

☐ 222

☒ 3.3.3.3

☒ 66

☒ 333

td

55

555

5.5

jjjj

> 用户组

确定 (如需添加用户，请到用户管理-组织)

确定

排除屏蔽用户列表  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
☐	3.3.3.3-3.3.3.33	#	 ☐ 3.3.3.3	
☐	6.6.6.6	#	 ☐ 66	
☐	3.3.3.35	#	 ☐ 25	

首页 上一页 **[1]** 下一页 尾页 / 1页



 删除选中用户

2.13



2.13.1

2.13.1.1



IP ip ip ip

MAC

AnyIp

AnyIp

PC

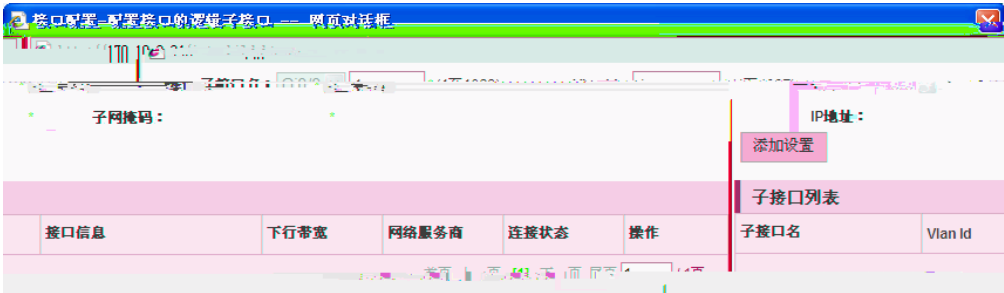
PC

ip

ip

DNS

子接口管理



2.13.1.2

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

说明：只需点击对应接口就可以配置。

接口已上电

内网口 外网口 万兆口

内网口 内网口 万兆口

管理口 内网口 内网口

Gi0/0 口 ip地址：10.22.2.32 * 接口描述：

子网掩码：255.255.255.0 * 下一跳地址：10.22.2.1 *

光电转换：电口

下行带宽：10 Mbps(0.5~1000)不配置时默认为10

上行带宽：10 Mbps(0.5~1000)不配置时默认为10

网络服务商：☐ 电信 ☐ 移动 ☒ 联通 ☐ 教育 ☐ 其它

开启缺省路由：☒ 勾选开启缺省路由

开启NAT配置：☒ 勾选开启线路NAT功能

开启源进源出：☐ 勾选开启源进源出

保存设置 清空设置 子接口管理

1

IP

IP

PPPoE ADSL

IP

IP

IP

IP

PPPoE ADSL

ADSL

PPPoE(ADSL)

外网口配置 PPPoE(ADSL)

Gi0/0 口 账号：13321231244 * 密码：***** *

ip地址：自动获取 光电转换：电口

下行带宽：10 Mbps(0.5~1000)不配置时默认为4

上行带宽：10 Mbps(0.5~1000)不配置时默认为0.5

网络服务商：☐ 电信 ☐ 移动 ☒ 联通 ☐ 教育 ☐ 其它

开启缺省路由：☒ 勾选开启缺省路由

开启NAT配置：☒ 勾选开启线路NAT功能

保存设置 清空设置 子接口管理

IP

IP

IP

外网口配置 动态IP(DHCP)

光电转换：电口

下行带宽：10 Mbps(0.5~1000)不配置时默认为10

上行带宽：10 Mbps(0.5~1000)不配置时默认为10

网络服务商：☐ 电信 ☐ 移动 ☒ 联通 ☐ 教育 ☐ 其它

其它NAT配置：☒ 勾选并启用线路NAT功能

2

1 IP

2

NPE40

3

0.5~1000Mbps 10Mbps

4

5

6 nat ANT

NAT

7

DNS

2.13.2

接口模式选择

接口模式选择

接口模式选择

说明：管理口用户管理设备使用的

但不做流量控制。

直接转发。

只接收报文，不转发报文要求配置内网网段

子网掩码：255.255.255.0

线路4

外口线路：G10/2 电口

保存设置

管理口配置

管理口-ip地址：172.18.2.13

网关：172.18.2.1

保存设置

网桥模式下的接口配置

☒ 带宽线路1 ☐ 带宽线路2 ☐ 带宽线路3 ☐ 带宽

带宽线路1

工作模式：网桥转发

内口线路：G10/1 电口

IP

保存设置

☐ 带宽线路2 ☐ 带宽线路3 ☐ 带宽线路4

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

IP地址：192.168.1.3

掩码：255.255.255.0

开启NAT配置：☒勾选开启链路NAT功能

保存设置

是否开启NAT	操作
开启	编辑 删除

一页 1 下一页 尾页 1/1页 共 1 条

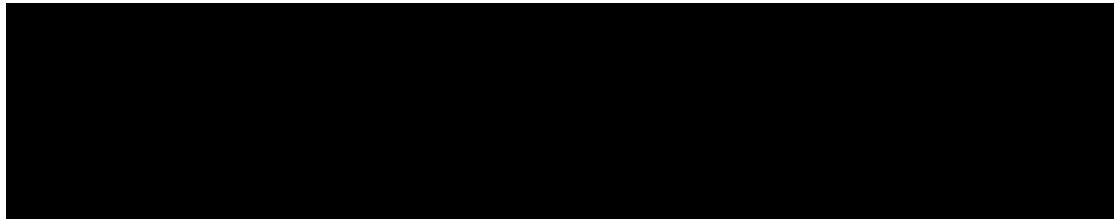
内网多链路聚合口 流量平衡：源IP+目的IP

聚合接口名	聚合接口	接口信息
AggregatePort 1	Gi0/0, Gi0/2	IP地址：192.168.1.3 子网掩码：255.255.255.0

首页 上

IP

保存设置



保存设置

2.13.5

NPE



☒ 开启G10/1口的多链路检测

ping地址: * 下一跳地址: * 探测间隔: (单位: 秒)

2 ping 220.181.112.143

3

ping

4 0.5s

5 DNS IP

6 TCP

7 TCP 80 1~65535

8 ping " "

" "

2.14 /

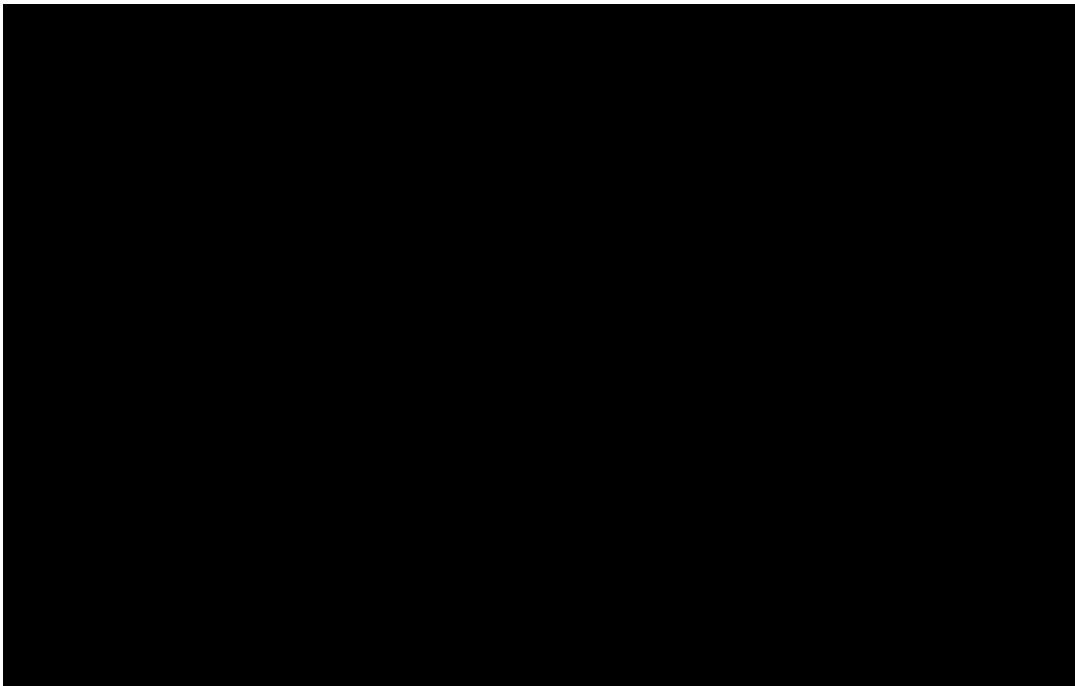
IP
> > > >

2 2

/

2.14.1

1



1 ACL

添加设置

ACL 新建ACL列表 ACL 2.11.4 ACL

IP

IP

2

策略路由列表 选择策略组匹配接口： Gi0/0				
策略优先级	匹配ACL列表	出口地址	下一跳地址	操作
1	1	Gi0/0.1		编辑 删除
2	11	192.168.1.1		编辑 删除

[编辑](#)

[删除](#)

[删除全部](#)

2.14.2

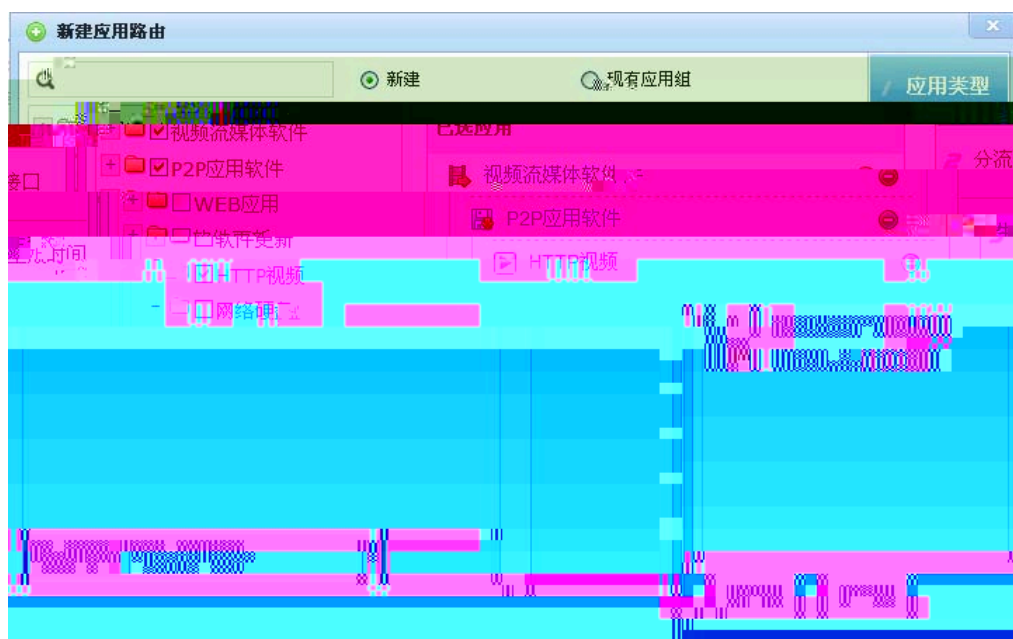


2.14.3

IP

IP

● 新建



● 现有应用组





2

WAN

WAN

WAN

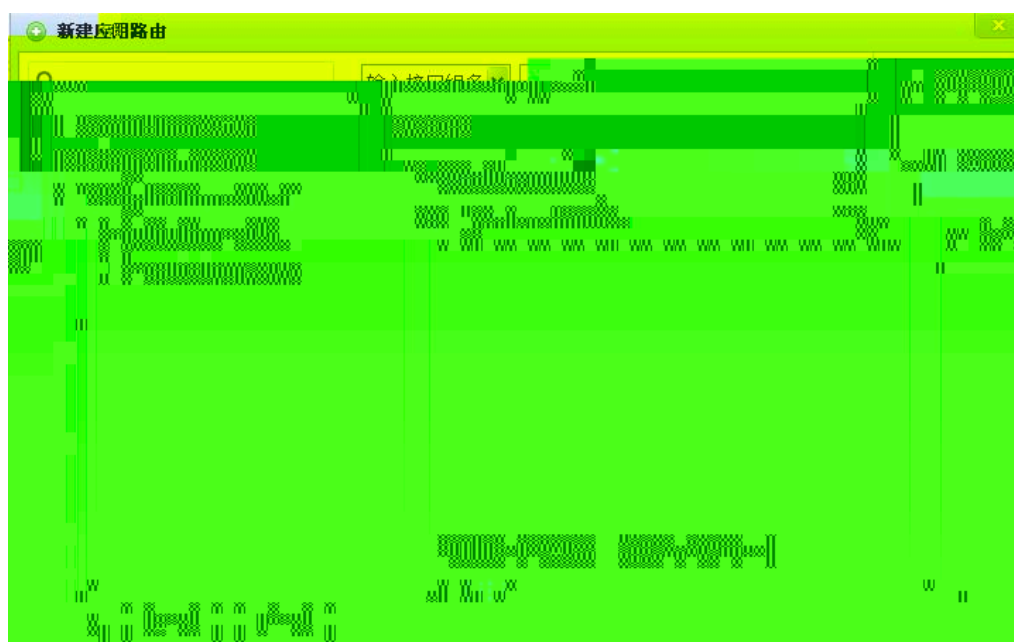


WAN

下一步

输入接口组名	▼
输入接口组名	
选择接口组	





选择应用组  aaa 

接口的均衡策略: 
按线路负载均衡
按线路负载均衡
按线路带宽均衡

3

 时间管理

新建应用路由

生效时间: 所有时间 时间管理

应用类型

分流接口

生效时间

上一步

完成

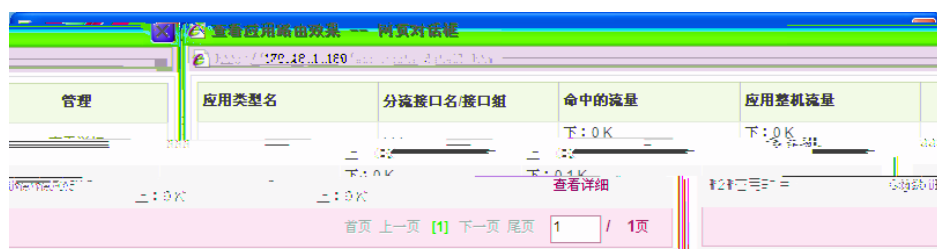
2

应用类型名	分流接口名/接口组	生效时间	☒ 开启	状态	应用顺序	路由效果	管理
aaa	bbb	所有时间	☒ 开启	未生效		明细	
P2P应用软件	GigabitEthernet 0/5	所有时间	☒ 开启	生效		明细	

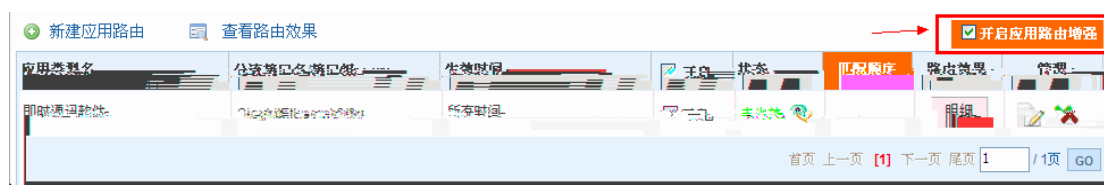
首页 上一页 1 下一页 尾页 1 / 1页



☒ 开启

[查看详细](#)

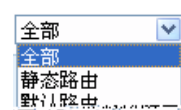
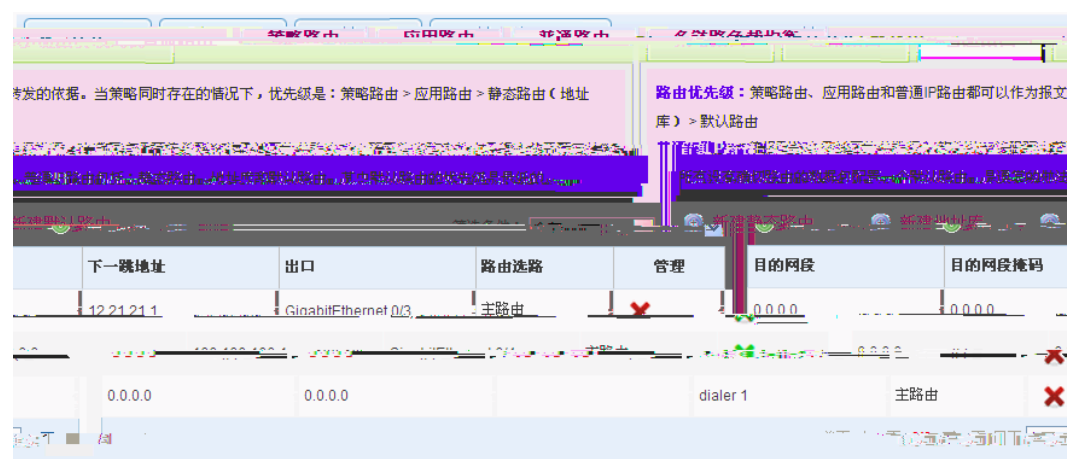
4



2.14.4

IP

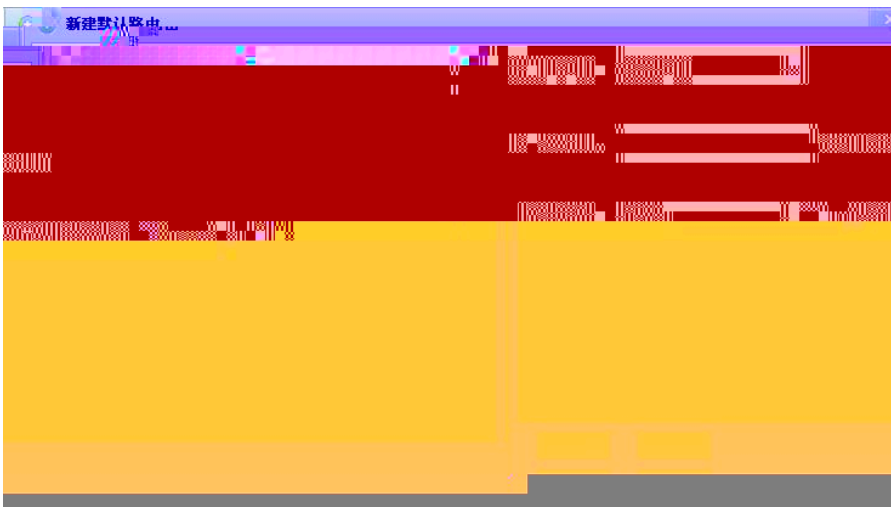
IP





3

新建默认路由



完成

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	100.100.100.1	GigabitEthernet 0/6	主路由	✖

首页 上一页 1 下一页 尾页 1 / 1页



2.14.5



1

☐ 开启多链路负载均衡

关联接口组：

关闭

接口组名：

选择接口：

☐ Gi0/5

☐ Gi0/6

保存设置

IP

2.15.5

10

2.15 DNS

DNS

DNS

DNS

2.15.1 DNS

PC

DNS

DNS

(

+ 添加

 DNS)

保存设置

DNS服务器

正向DNS代理

智能DNS

DNS服务器1：

192.168.5.3

+ 添加

保存设置

全部删除

DNS

ping www.baidu.com ping

www.baidu.com

DNS

ping

www.baidu.com ping (ping www.baidu.com)

2.15.2 DNS

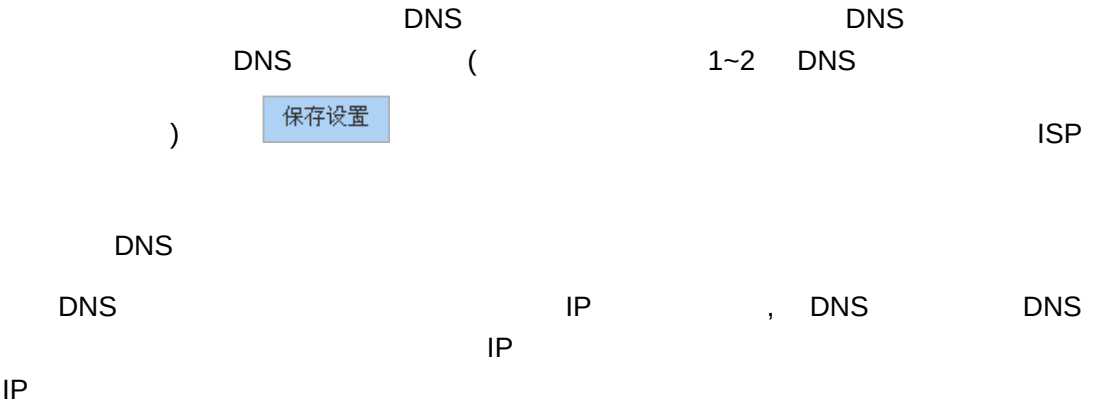
DNS

DNS

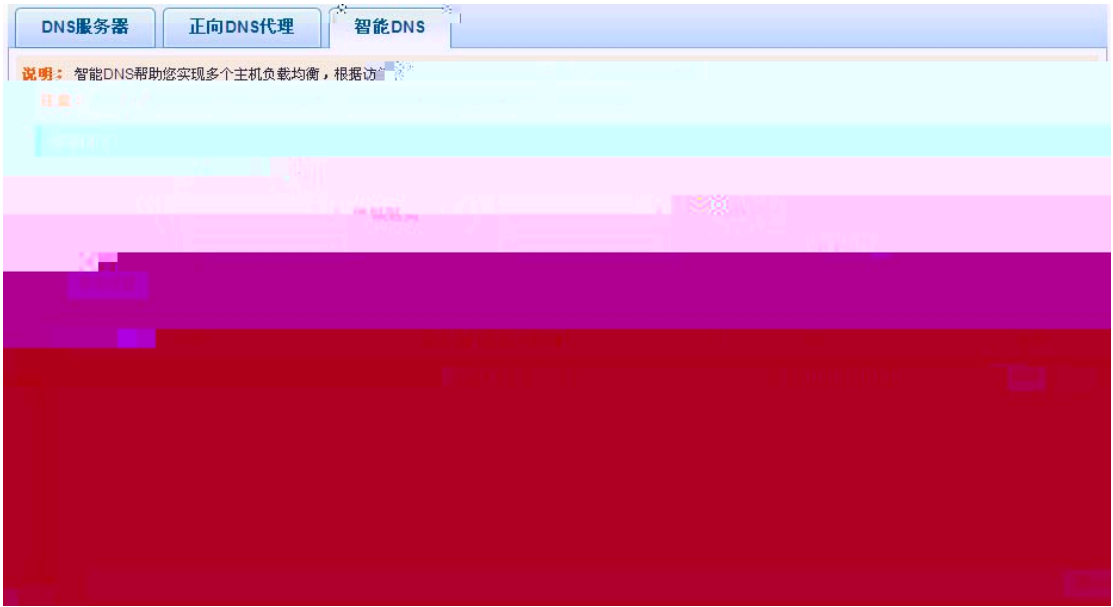
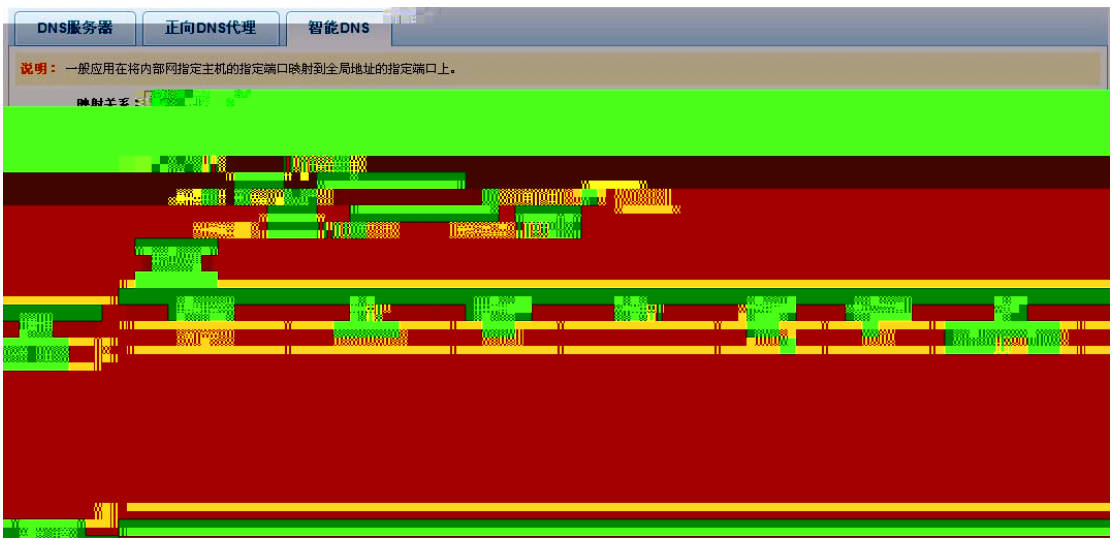
PC

DNS

DNS



WEB



IP

IP

ip

添加设置

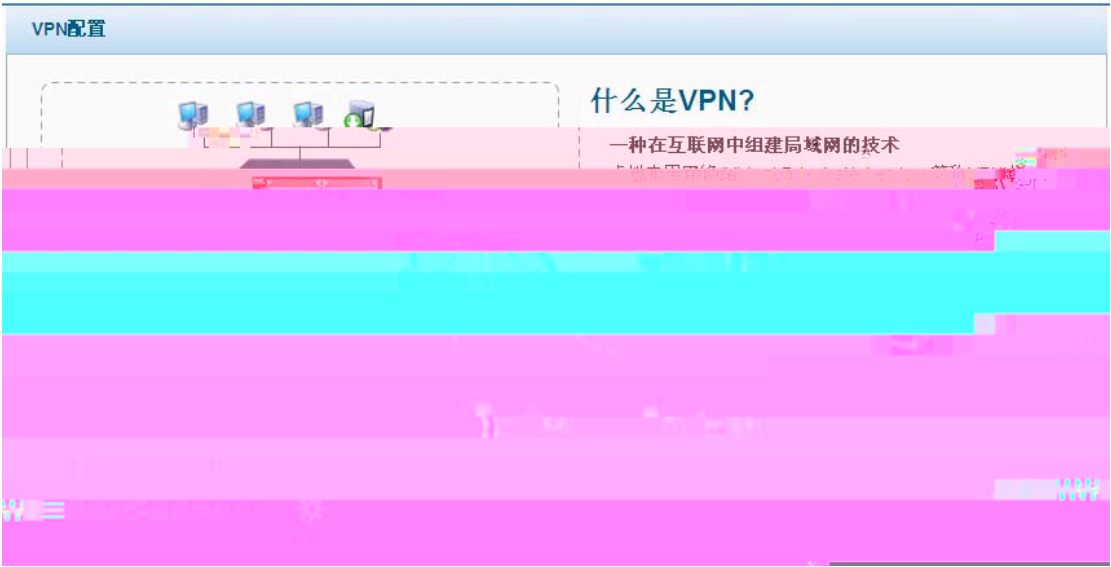
TCP or UDP

2.16 VPN

VPN

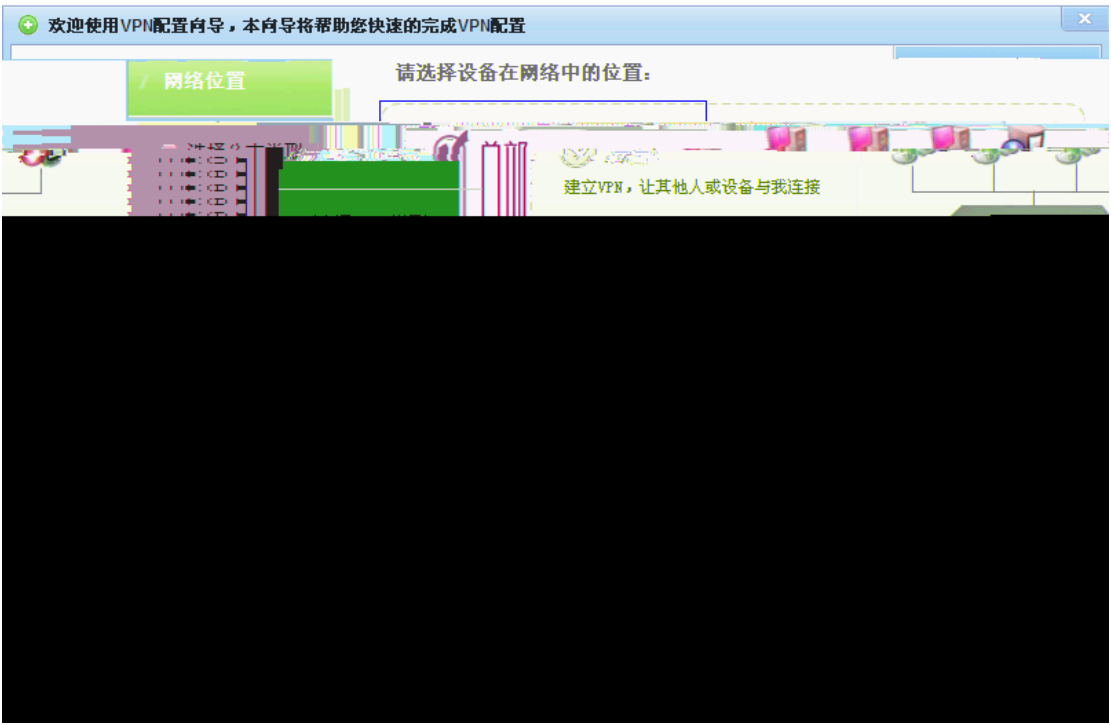
Virtual Private Network

VPN



 开始配置

VPN



(or)

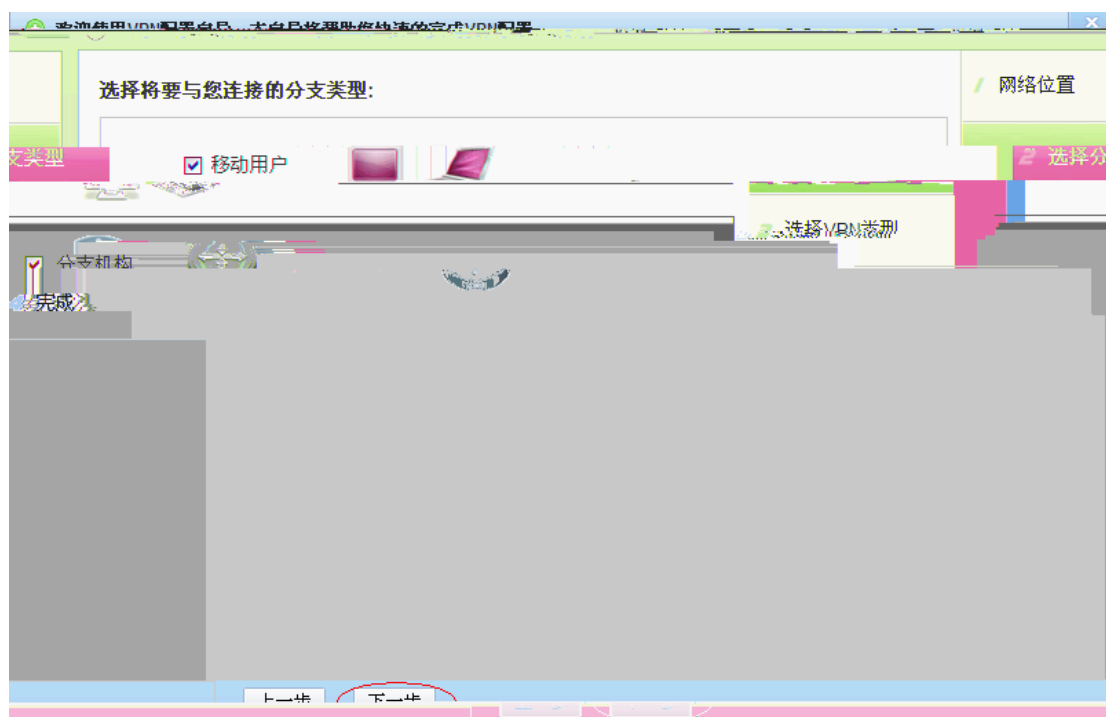
2.16.1

1

VPN

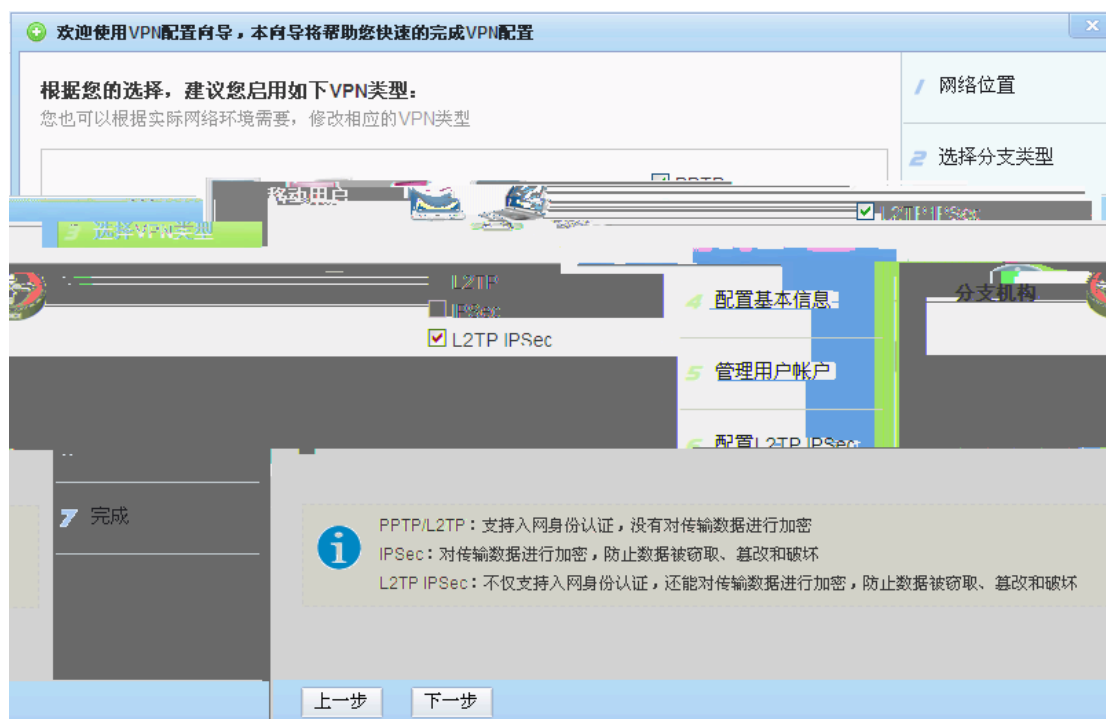
下一步

2



VPN

3 VPN



PPTP/L2TP

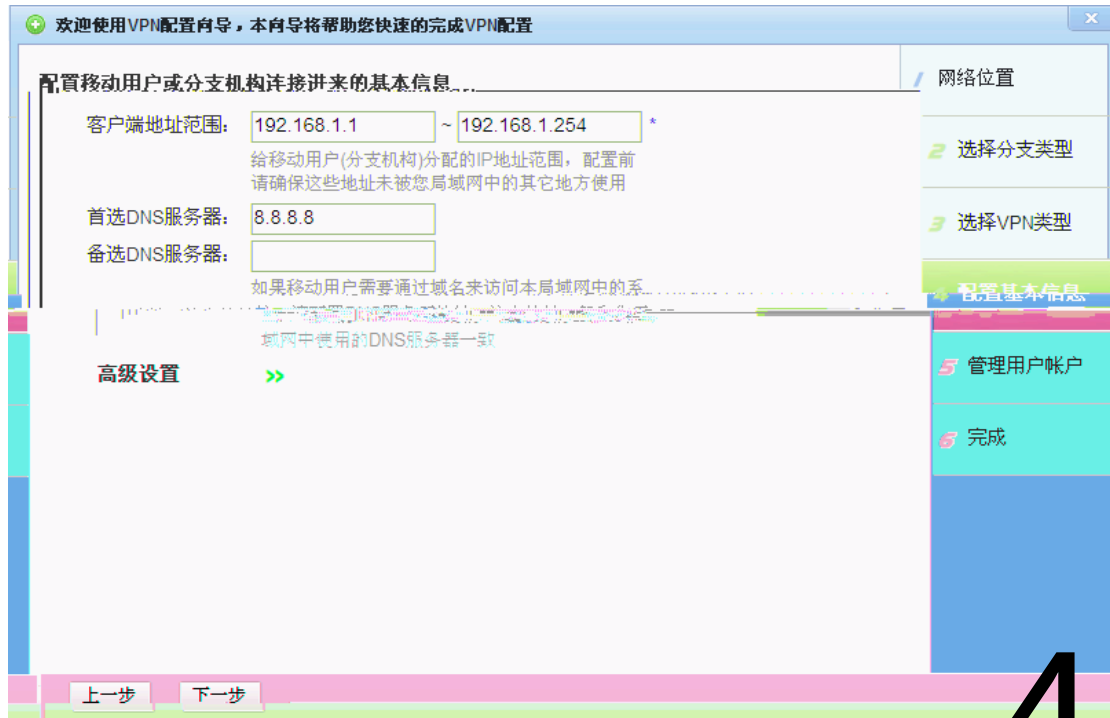
IPSec

IPSec

L2TP IPSec

L2TP IPSec

4



vpn

ip

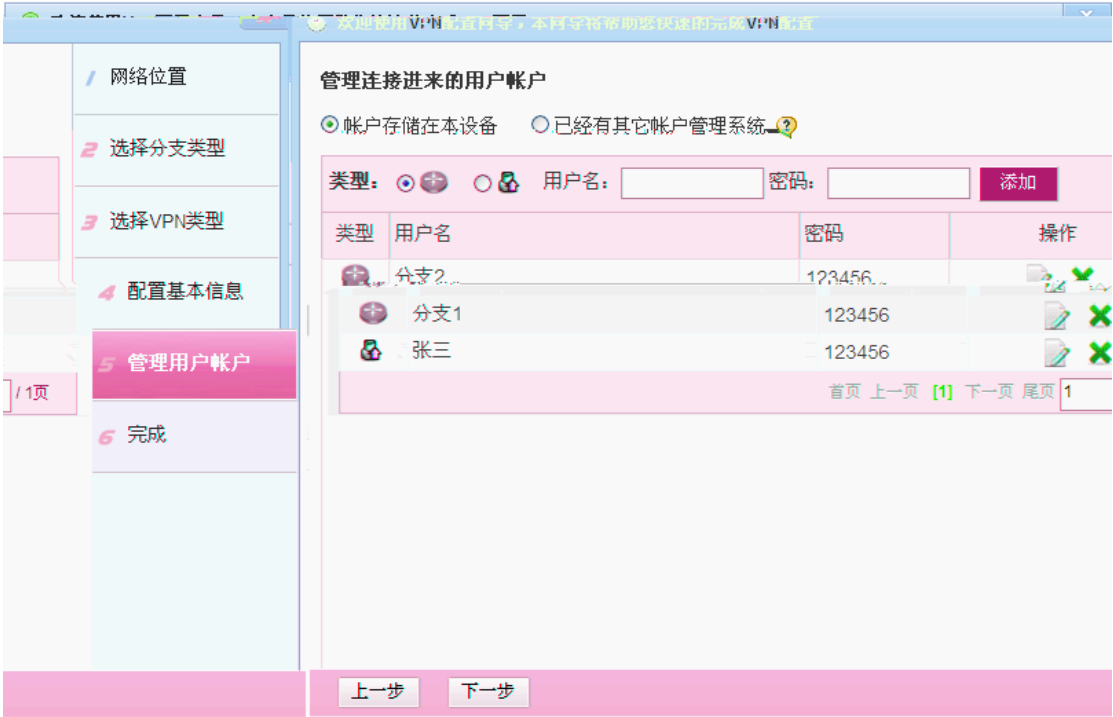
ip

ip

4

IP

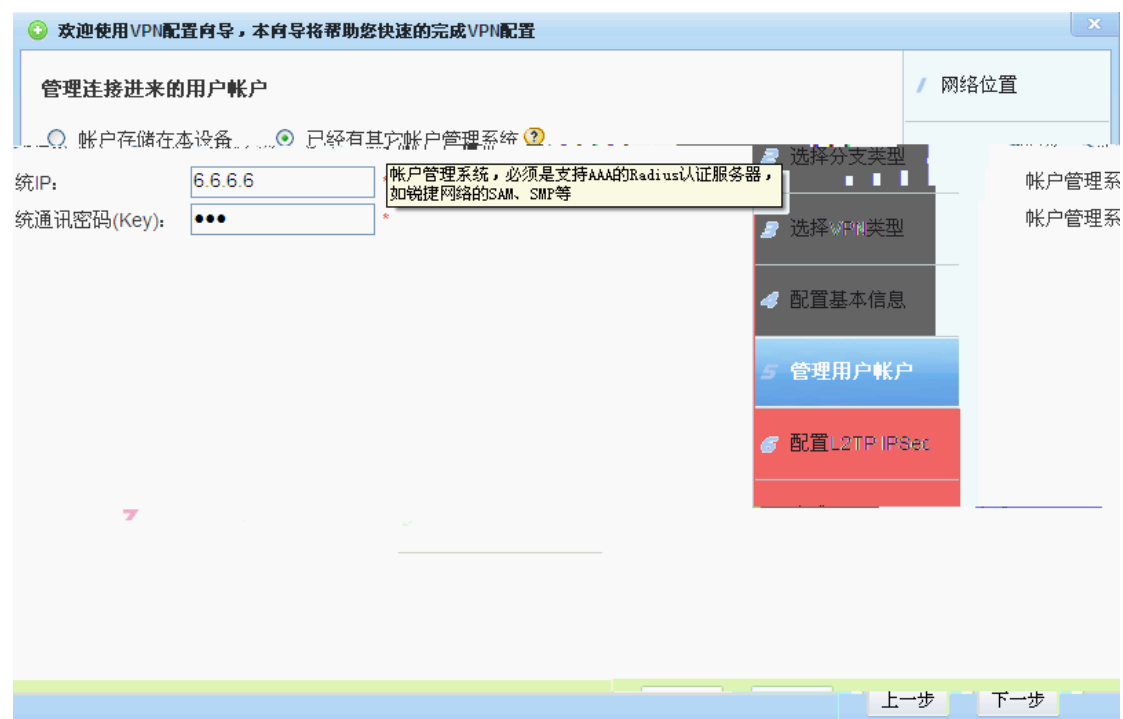
5



添加

AAA Radius
IP

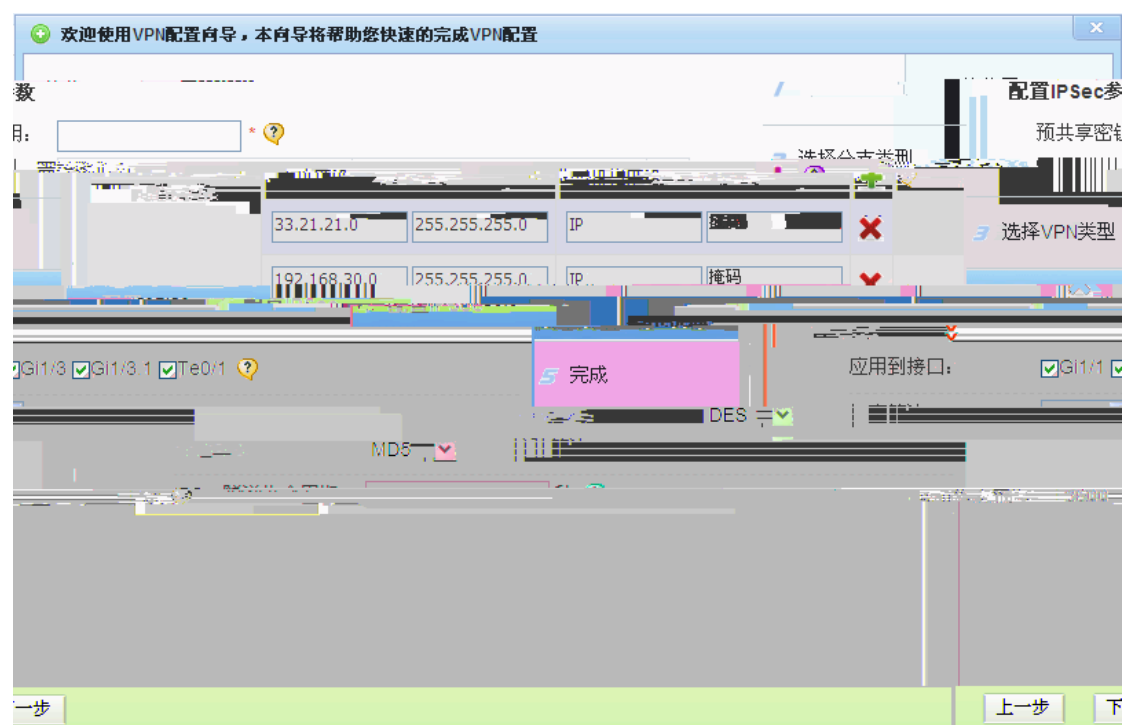
SAM SMP



6 IPSec

IPSec

Internet



IPSEC

配置指导

请在表格中配置总部和分支机构间需要通过IPSec隧道加密互访的网段。

配置举例1：希望总部的192.168.1.1和分支的172.18.58.1网段可以加密互访

本地网段		分支机构网段		
192.168.1.1	255.255.255.0	172.18.58.1	255.255.255.0	✖

7 L2TP IPSec

欢迎使用VPN配置向导，本向导将帮助您快速的完成VPN配置

配置L2TP IPSec参数

预共享密钥：

高级设置

应用至接口：

☒Gi1/1

☒Gi1/3

☒Gi1/3.1

☒Te0/1

加密算法：

DES

校验算法：

MD5

IPSec隧道生命周期：

3600

秒

网络位置

选择分支类型

选择VPN类型

配置基本信息

配置L2TP IPSec

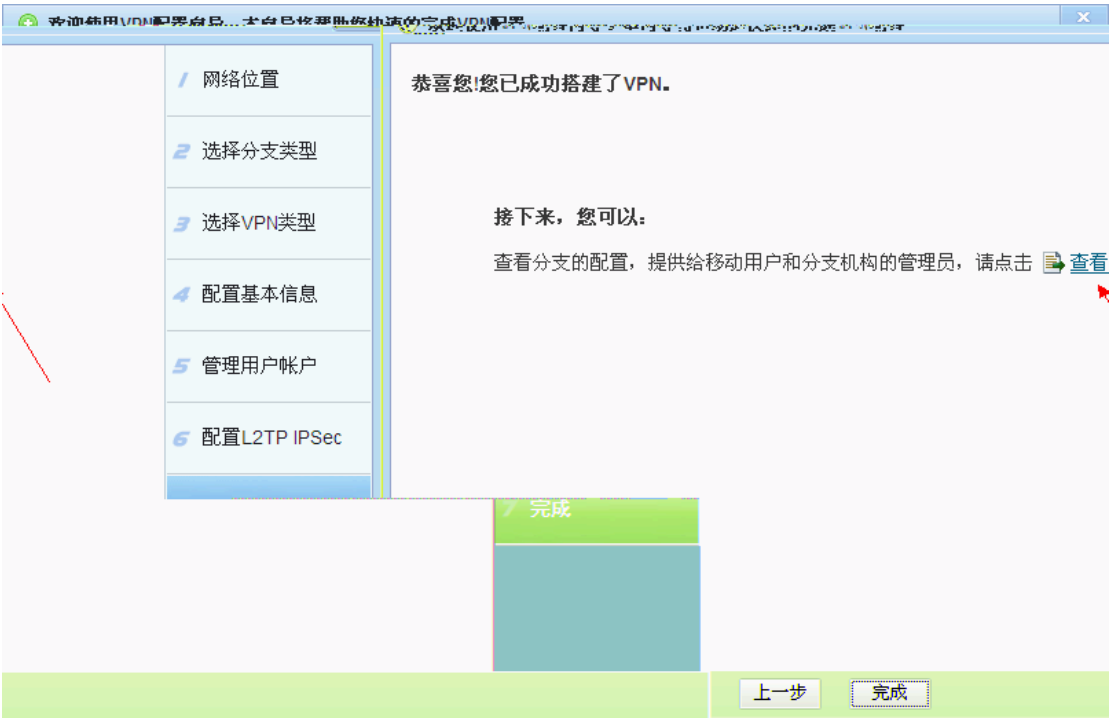
完成

上一步

下一步

L2TP IPSec

8



... 完成 ...

VPN

[查看](#)

移动用户 PPTP VPN	
服务器公网IP:	172.18.2.13(其他)
配置步骤:	+ 配置参考
分支机构 L2TP VPN	
服务器公网IP:	172.18.2.13(其他)
L2TP隧道验证密码:	未开启

[+ 配置参考](#)

PC

VPN

2.16.2

1

VPN



2



1 VPN

L2TP IPSec

L2TP

IPSec

L2TP IPSec

L2TP

VPN类型:

L2TP

:

+多个IP

总部公网IP

用户名:

密码:

总部网络:

IP

掩码

添加

IPSec

VPN类型:

IPSec

总部公网IP:

*

预共享密钥:

*

需经隧道访问的网络:

本地网段		总部网段		
33.21.21.0	255.255.255.0	IP	掩码	✗
192.168.30.0	255.255.255.0	IP	掩码	✗

2

IP

VPN

IP

3

4

VPN

5

+添加

6

IPSec



VPN

VPN

2.16.3 VPN

VPN



WEB

VPN

1

移动用户信息

当前共1个移动用户，其中有0个移动用户接入专网。点击 [这里](#) 管理移动用户。

NAT转换规则

添加NAT地址池

端口映射

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。

保存设置

NAT地址池列表：

pool

IP地址	操作	序号	接口	起始IP地址	结束
/	编辑 删除	1	Gi0/5	/	

选择：

pool

Gi0/5-起始IP地址：

结束IP地址：

IP

IP

IP

IP

IP

保存设置

2.17.3

DMZ

说明：一般应用在该市域网指定主机指定端口映射到公网地址指定端口上。

映射关系：

端口映射

内网IP：

*

内网端口：

*(1-65535)

外网IP：

输入地址：

使用接口地址：

Gi0/3

外网端口：

*(1-65535)

协议类型：

TCP

添加设置

端口映射	内网IP	内网端口	外网IP	外网端口	协议类型	接口	操作
端口映射	100.100.1.2	2220	100.100.1.2	2220	TCP	Gi0/5	编辑

IP

IP

IP

IP

IP

IP

1

65535

TCP

UDP

添加设置

2.17.4 DMZ

DMZ

DMZ

说明：一般应用在将内部网指定主机的指定端口映射到全局地址的指定端口上。

映射关系：整机映射(DMZ主机)

内网IP：

外网IP：☐ 输入地址： ☒ 使用接口地址：G10/3

添加设置

映射关系	内网IP	内网端口	外网IP	外网端口	协议类型	接口	操作
192.168.1.20					GigabitEthernet 0/5	编辑 删除	整机映射
192.168.1.3	3389		40001	TCP	GigabitEthernet 0/5	编辑 删除	端口映射

IP

DMZ

IP

IP

IP

添加设置

DMZ

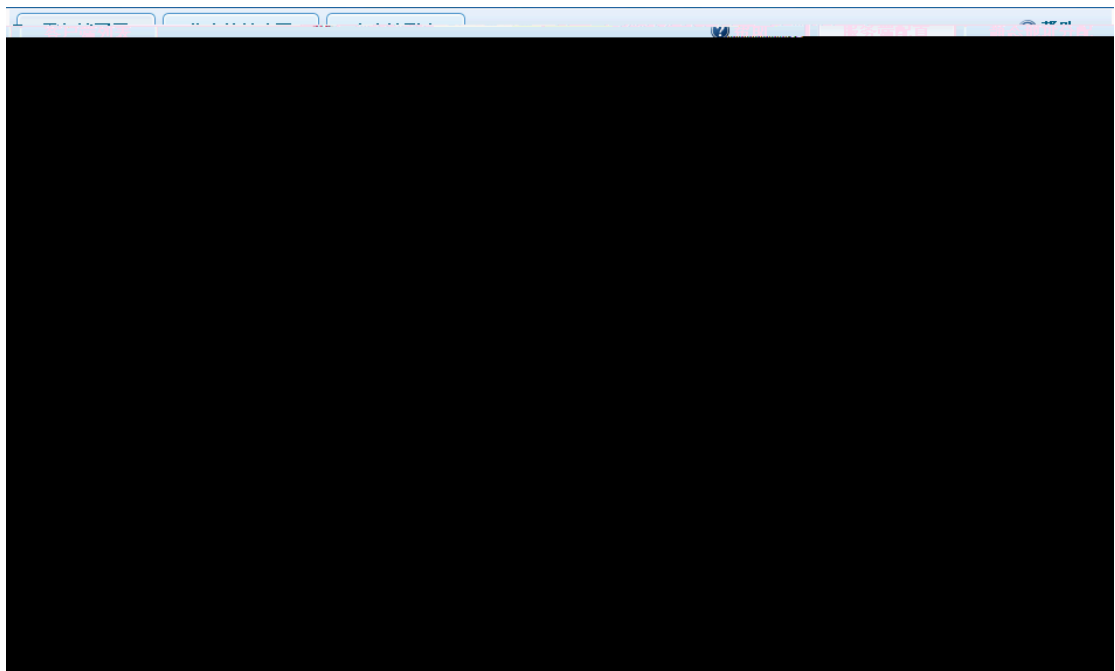
2.18 DHCP

Dynamic Host Configuration Protocol, DHCP

UDP

IP

2.18.1



DHCP

☒ 勾选启用DHCP服务

DHCP

IP

IP

DNS

DNS

IP

增加地址池

DHCP

配置不分配的IP段,

IP

IP

配置不分配的IP段

IP段格式如：

不分配的IP段：不分配的IP段将不会分配给客户。如果不需要，请留空。不分配的IP段格式如：1.1.1.1-1.1.1.30 或者只填1.1.1.1代表单个IP。

不分配的IP段1：

192.168.2.4

-

192.168.2.8

不分配的IP段2：

192.168.2.245

-

192.168.3.230

-

192.168.3.250

保存

关闭

DHCPDHCP

2.18.2

DHCPIPMACIPDHCPDHCP

本页配置DHCP静态IP分配: 如果在增加时发现客户名称出现重复，原有的那条静态IP绑定将会被新的静态IP绑定取代，不同的MAC地址不能同时绑定到同一个IP地址。

客户名称：

*

(用来区分每一条IP/MAC绑定)

客户端IP：

*

子网掩码：

指定MAC地址：

*

给定的MAC地址必须有效的

网关：

DNS：

1.5	255.255.255.0	2a22.3332.3366	172.18.1.1	0.0.0.0	张三	192.168.
-----	---------------	----------------	------------	---------	----	----------

全选

删除

IPIP

IP

MAC

MAC

()

DNS

DNS

()

增加

"

"

IP

MAC

2.18.3

服务端配置

静态地址分配

客户端列表

帮助

IP地址	掩码	MAC地址	地址租期	IP分配方式
192.168.1.3.2	255.255.255.0	6666.6666.6666	闲置	静态绑定

把MAC地址绑定到动态获取的IP上

首页 上一页 [1] 下一页 尾页 1 / 1页 GO

IP

把MAC地址绑定到动态获取的IP上

IP

MAC

2.19

2.19.1

2.19.1.1

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 配置

说明： admin用户拥有配置和查看设备信息的所有权限。

提示： 如果你设置了新的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。

修改web超级管理员密码

用户名： admin

新密码： *

确认新密码： *

确定修改 清空

修改telnet登录密码

新密码： *

确认新密码： *

确定修改 清空

Web

admin

Telnet

Telnet

admin

admin

2.19.1.2

立即重启设备

说明: 单击此按钮将使路由器重新启动。

提示: 重启过程需要1分钟左右的时间, 请耐心等待, 设备重启后将会自动刷新页面。

立即重启设备

1

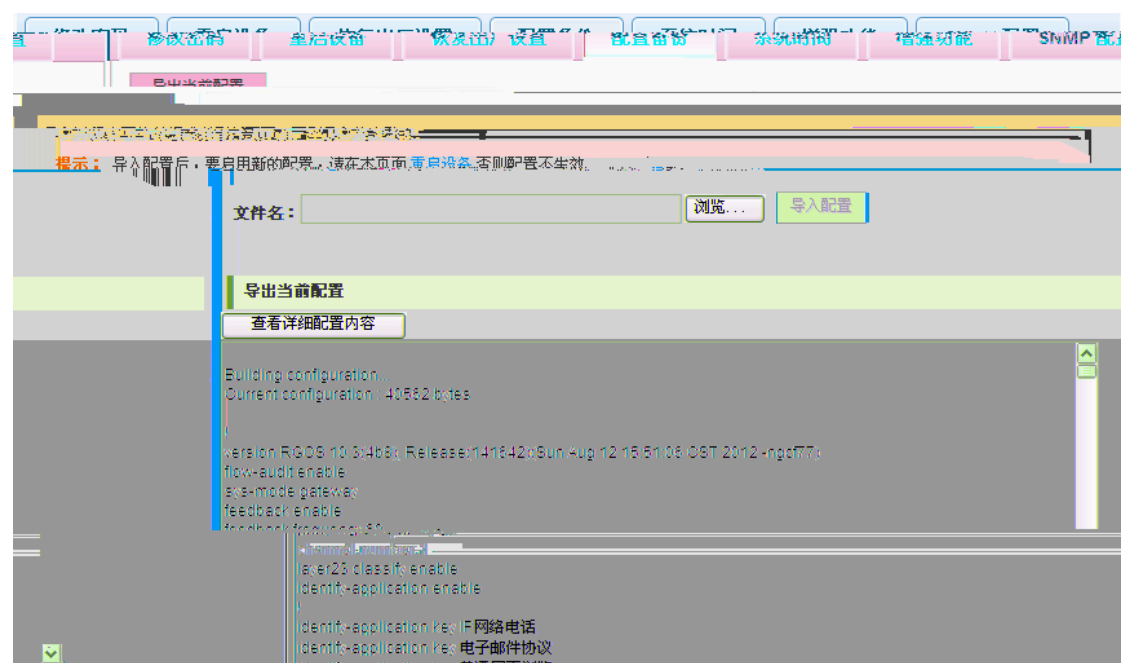
2.19.1.3

恢复出厂设置

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

2.19.1.4



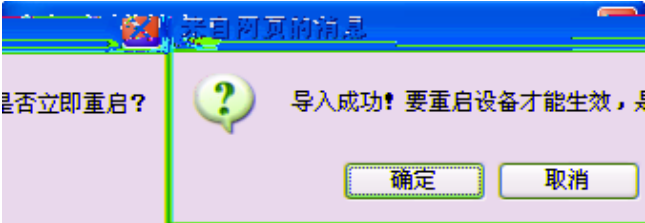
导出当前配置



浏览...

config.text

导入配置



取消

查看详细配置内容

2.19.1.5

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 配置

说明：该功能修改设备时间。

提示：开启“自动与Internet时间服务器同步”后请检查是否已经配置了正确的DNS服务器，否则将不能生效！

重新设置时间：

0

时

0

分

☐ 自动与Internet时间服务器同步

☐ 通过管理口自动与Internet时间服务器同步

确定修改

Internet
DNS
DNS
DNS
DNS

2.19.1.6

系统时间

增强功能

SNMP 配置

修改密码

重启设备

恢复出厂设置

配置备份

网络不通过网络安全设备的系统，而直接物理上导通。

，目前支持邮件方式反馈！

硬件ByPass

就是旁路功能，也就是说可以通过特定的触发状态（断电或死机）让两个网

马上配置硬件Bypass

反馈用户信息

配置反馈用户信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

马上配置用户信息

配置模板下载和导入

下载

导入

流量审计实时数据生成频率

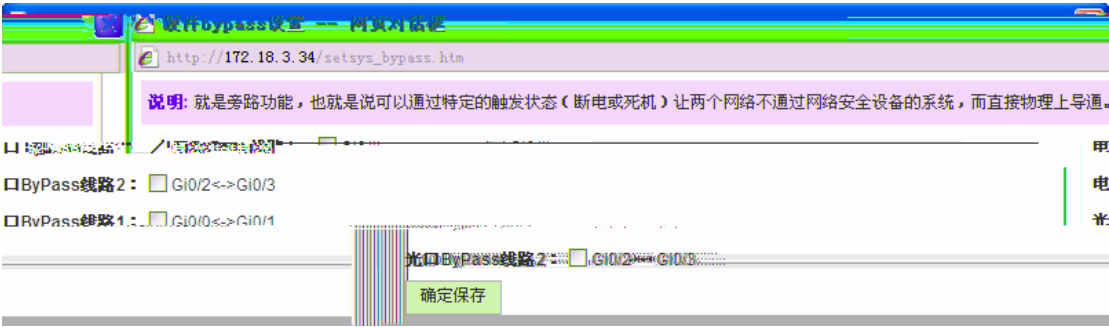
10

30秒

停止

ByPass

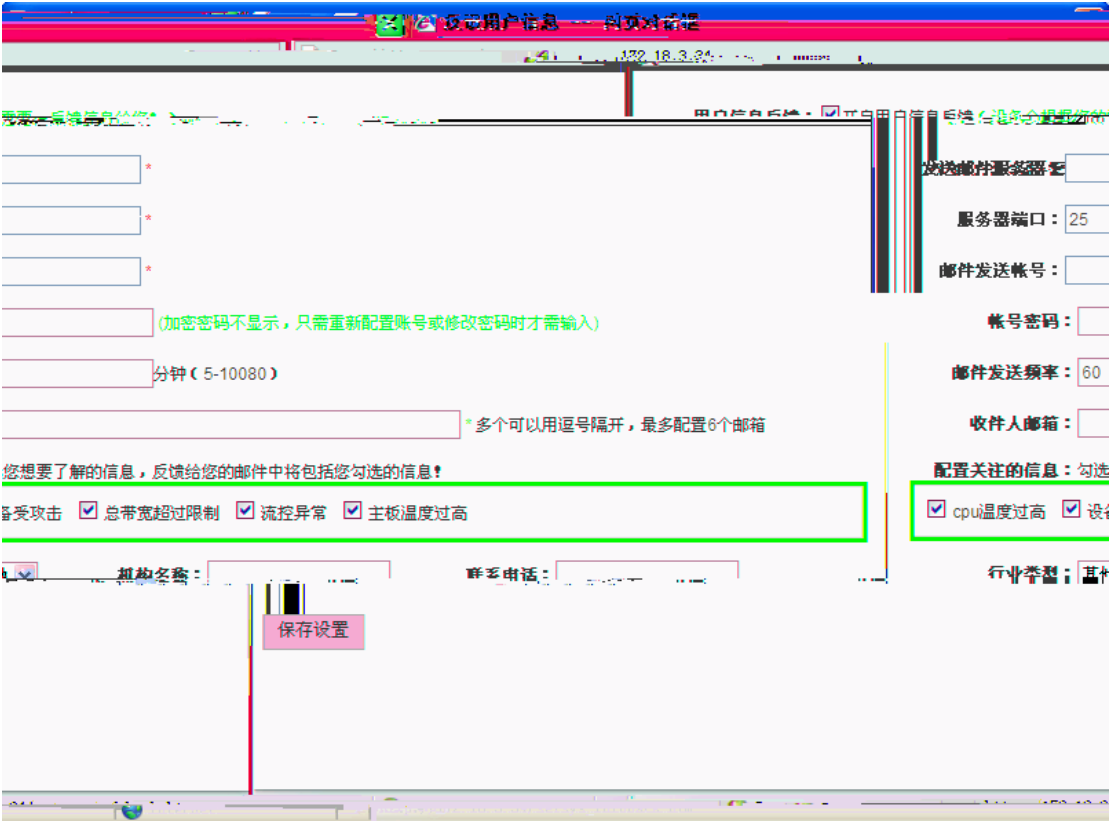
马上配置硬件Bypass



ByPass

确定保存

马上配置用户信息



1

☒ 开启用户信息反馈 (设备会根据您的需要, 反馈信息给您!)

2

serv@163.com

pop.163.com | SMTP

smtp.163.com | IMAP

imap.163.com)

3

163

(POP3

4

serv@163.com

5

serv@163.com

6

60



2.19.1.7 SNMP/SAM

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

数据库导出

SNMP/SAM

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

SAM : 锐捷自主研发的RADIUS认证计费服务器

SNMP配置

SNMP版本：☒ V2版本 ☐ V3版本

设备标识：

SNMP口令：

Trap口令：

Trap接收主机：

用",号隔开。

最多可配置10个Trap接收主机，IP之间用",号隔开。

保存设置

清除设置

SAM配置

IP:

端口:

认证:

计费:

设置

保存

SNMP

- 1
- SMNP
- V2
- V3
- V2
- 2
-
- SMNP
- 3
- SNMP
- 4
- Trap
- 5
- Trap

V3

配置10个Trap接收主机，IP之间请用“,”号隔开。

SNMP版本：☐ V2版本 ☒ V3版本

设备标识： *

SNMP用户： *

加密密码： *

认证密码： *

Trap口令：

Trap接收主机：

最多可

保存设置

清除设置

V3

SNMP

SAM

SAM

RADIUS

SAM配置

开启SAM联动：☒ 勾选开启SAM联动

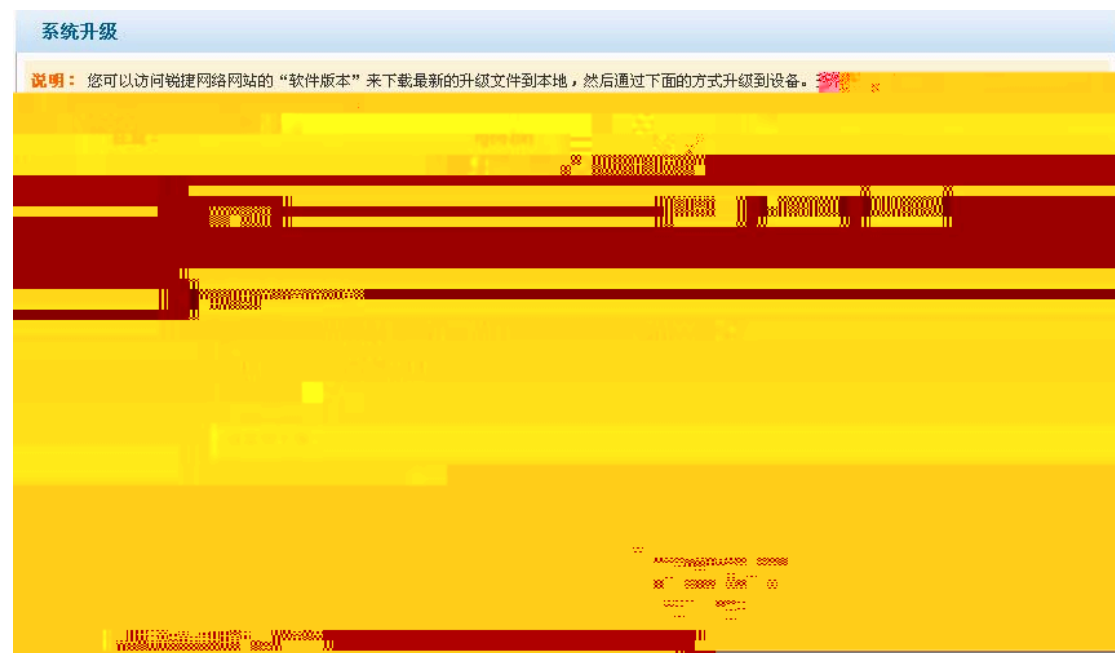
TCP

已链接的SAM：192.168.25.120

保存设置

- 1 SAM ☒ 勾选开启SAM联动
- 2 TCP SAM TCP
- 3 SAM
- 4 SAM SAM IP

2.19.2



§

з і € ã ° і "NPE - 0 ж" \ і á - , ж л ѓ "H о
 К á , ѓ ѓ á о к в А ↑ ѓ ж ѓ ч á К у і ѓ В
á л á Е ѓ á о к ° К Ї 50 і ѓ ѓ



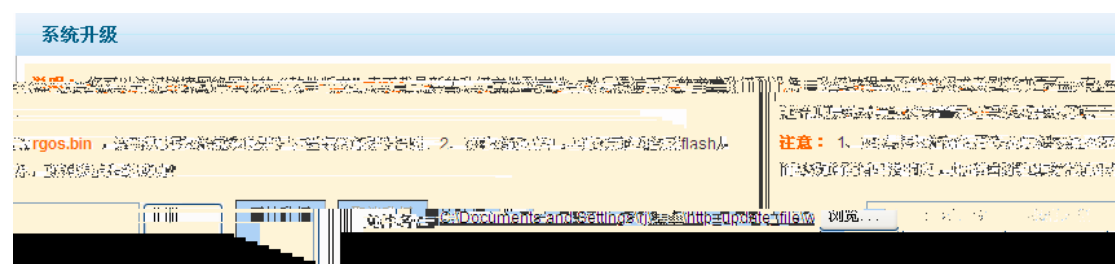
§

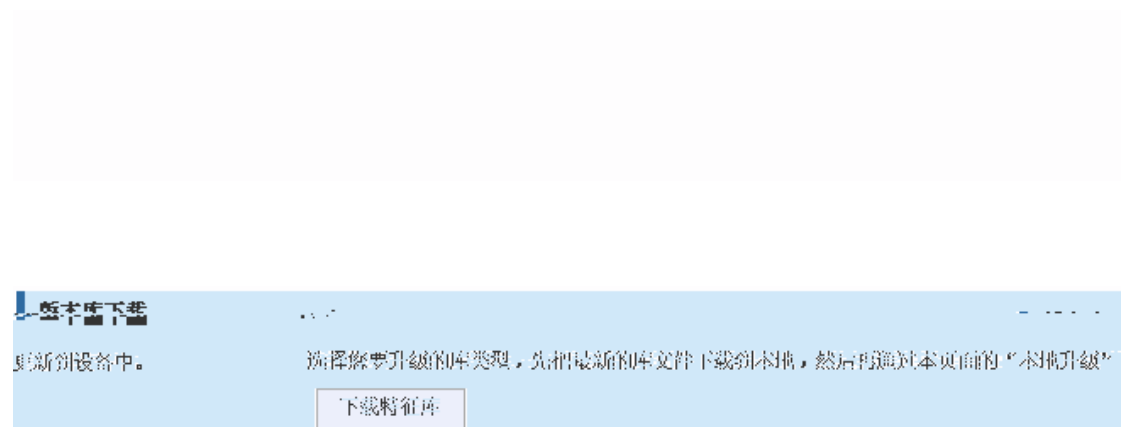
1 і і á - к р " - "rgos.bin" ѓ á і 0 ж ý ж
ѓ і ý ѓ

2 і á о к ѓ з á , ѓ flash з ° л ѓ ж в к т ѓ
ѓ ѓ á К у ѓ

开始升级

50





下载特征库



设置自动更新

☒ 启动自动更新

17 6 分 ☒ 特征库 ☒ 地址库 ☐ 反馈文件 ☐ web网管升级包 ☐ 通过管理口升级

☒ 启动自动更新

确定

DNS

DNS

2.19.3

管理员权限

说明：本页面添加的设备管理员可以管理该设备并设置设备密码，但不该设备可以运行命令，该设备用户不能删除。

用户名：

登录密码：

添加管理员

操作

编辑

编辑

下一頁 尾页 1 / 1 页

删除选中

前一頁 上一頁 [1]

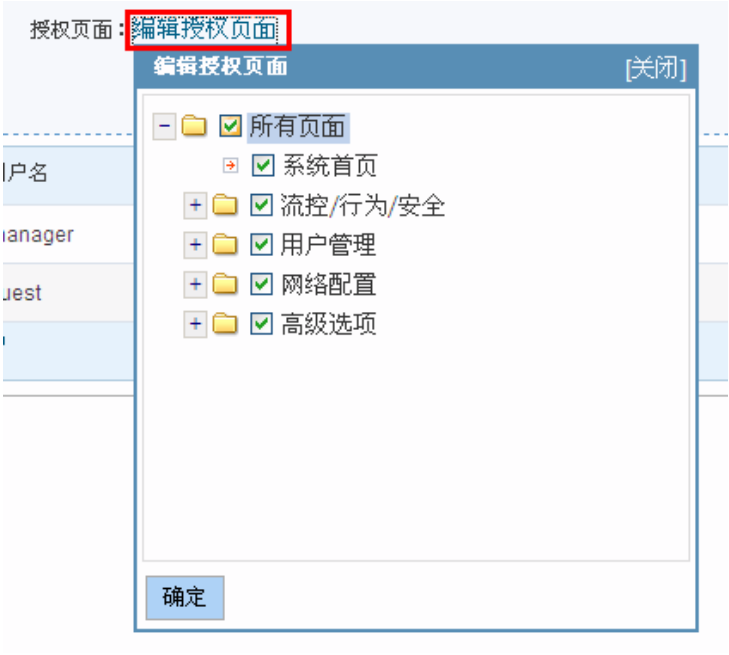
Web

```
Telnet
admin
```

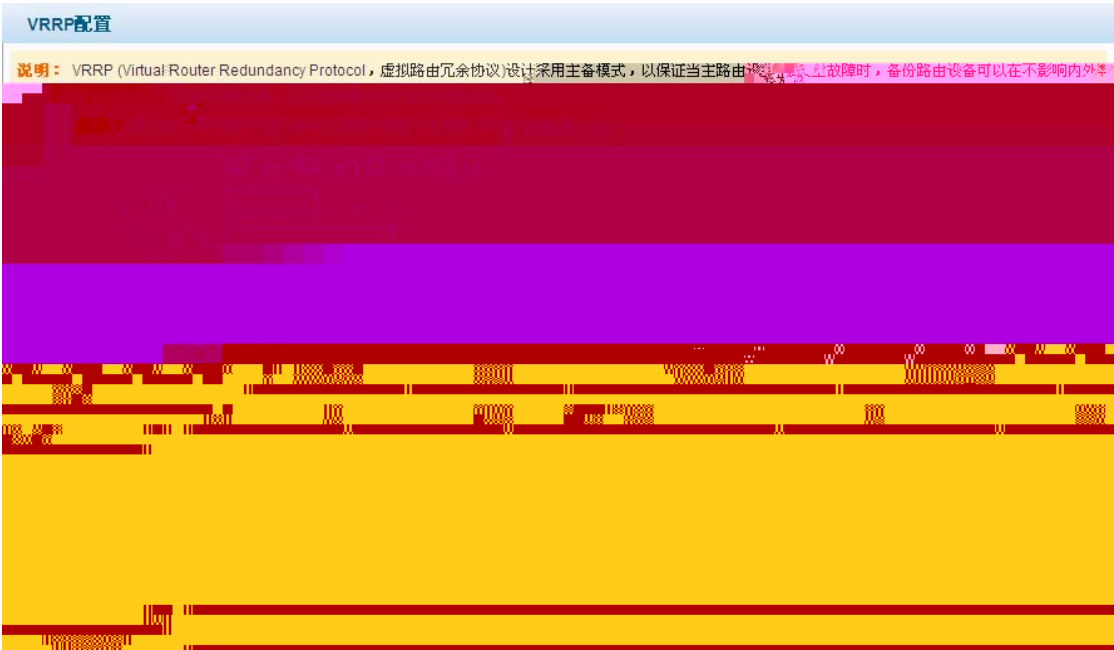
manager guest

zhangs;

web



2.19.4 VRRP



VRRP (Virtual Router Redundancy Protocol)

VRRP		VRRP		VRRP	
VRRP	IP	VRRP	IP	IP	IP
	VRRP		255.		

VRRP

VRRP

2.19.5

动态域名解析

动态域名解析： 功能是实现固定域名到动态IP地址之间的解析。

服务提供者：花生壳 (www.oray.net) 没有帐号请先注册

用户名：*

密 码：*

登 录

链接状态：未链接

IP

☐ 开启流日志	4	☐ CPU、内存使用率日志	4
☐ 硬盘使用日志	4	☐ 设备审计日志	4
☐ 开启URL审计	4	☐ 接口会话数审计	4
☐ IP应用流量审计	4	☐ IP会话数审计	4
☐ 设备流量审计	4	☐ 设备流量审计	4
☐ IP在线时长审计日志			

1	ip	ip			
2			20000	E-LOG	
20000	SNC	E-LOG	URL	SNC	

2.19.7

2.2

2.19.8 NPE

NPE