华御下一代防火墙

操作手册

北京华御科技有限公司

2017 年 11 月

目录

第一部分产品概述

1 图形界面格式约定

格式	描述
【 】	代表菜单或子菜单名称
>	代表 WEB 网管配置路径：如【系统对象】>【IP 组】，表示“系统对象”菜单下的“IP 组”菜单
<>	代表窗口中的选项或按钮名称

2 环境要求

设备系列产品可在如下环境使用：

- 输入电压： 220～240V
- 温度： -10～50 ℃
- 湿度： 5～90%
- 电源：交流电源 110V ～230V

为保证系统能长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求。

> **提示：**
> 1、 保证设备工作在建议的环境要求内，否则可能导致设备损坏或提早老化。
> 2、 设备良好的接地可以有效避免雷击。

3 接线方式

请按照如下步骤进行设备的接线：

1、 在后面板电源插座上插上电源线，打开电源开关，前面板的 Power 灯(绿色，电源指示灯)和 Alarm 灯(红色，告警灯)会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明设备正常工作。

2、 请用标准的 RJ-45 以太网线将 ETH0 口与内部局域网连接，对设备进行配置。

3、 透明模式：透明接口相当于普通的交换接口，不需要配置 IP 地址，不支持路由转发，根据 MAC 地址表转发数据。每个桥之间是独立通信的，桥之间不能传递数据。

4、 路由模式：可以接入多条出口线路，每个端口之间在策略允许的情况下可以通信。

5、 虚拟线路模式：虚拟网线接口也是普通的交换接口，不需要配置 IP 地址，不支持路由转发，转发数据时，直接从虚拟网线配对的接口转发。

6、 旁路镜像模式：连接到有镜像功能的交换机上，用于镜像流经交换机的数据。

提示：如果开机 5 分钟后，红灯还长亮，请关闭电源 5 分钟，然后重开。

4 登录设备

设备默认使用 ETH0 作为网管口，ETH0 出厂地址为 10.254.254.254/24。设备支持两种方式的 WEBUI 登录：

1、 安全的 HTTPS 登录，默认端口 9090。初始登录 URL 为：https:// 10.254.254.254:9090

2、 传统的 HTTP 登录，默认端口 9090。初始登录 URL 为：http://10.254.254.254:9090

系统默认使用 HTTPS 的登录方式，默认的管理员账号是 admin，密码是 admin*PWD。正确输入用户名和密码后，点击<登录>按钮即可进入管理界面。

提示：

1、 配置之前，必须保证用于网管的电脑与防火墙的网管口地址在同一个网段。如果第一次配置，请连接 EHT0 口，ETH0 出厂地址为 10.254.254.254/24，电脑的地址应配置为 10.254.254.0/24，但不允许为 10.254.254.254。

2、 连接后可以增加/修改物理端口的 IP 地址，设备的每一个 IP 地址都可以用于网管。

3、 首次进入设备请先升级到需要版本后，再恢复出厂设置。

5 刷新/保存/注销

在设备提供的 WEB 方式的管理界面中的最右上角有三个链接，分别是“刷新”、“保存”、“注销”。点击“刷新”可手动刷新当前页。点击“保存”并确认后，可将当前配置保存到系统硬盘中。点击“注销”

并确认后，即可成功退出系统。

6 密码恢复

如果管理员密码丢失，请按以下步骤恢复系统默认密码：

1. 进入 Console 连接，使用 root 用户（username：root，password：root*PWD）登录。
2. 选择 Reset WEBUI Password，进入密码恢复菜单，然后输入 yes，再回车。
3. 密码恢复成功，网管密码恢复到出厂设置（username：admin，password：admin*PWD）。

第二部分产品配置

7 设备状态

登录设备后，进入到设备首页，即设备状态页面。设备状态页面包含了设备版本信息、设备资源、实时网络流量、前十名服务实时速率分布、今日服务器安全排行前九、今日安全日志汇总、最近五次事件日志等七项内容。如下图：

图1. 首页

“设备版本信息”描述了系统固件的版本、应用特征的版本、URL 库的版本和授权类型的信息。授权类型有试用版和正式版两种。点击对应的<详细>按钮，可以连接到“系统升级”页面，查看到更详细的设备版本信息。

“设备资源”动态显示了 CPU 使用率、内存使用率、活跃会话数、在线用户数和在线认证用户数的信息。活跃会话数的显示格式为 N/M，N 表示当前活跃的并发会话数，M 表示设备最大并发会话数。当鼠标滑过某行时，会出现“显示最近一小时的趋势图”的提示，点击即可查看到最近一小时的趋势图。点击对应的<详细>按钮，可以连接到“设备资源”页面，查看到更详细的设备资源信息。

“实时网络流量”动态显示了当前 UP 的 WAN 口的速率。当鼠标滑过 WAN1、WAN2、……、WANm 时，会出现“显示最近一小时的趋势图”的提示，点击即可查看到最近一小时的速率趋势图。点击对应的<详细>按钮，可以连接到“物理接口”页面，查看到更详细的物理接口的统计信息。

“前十名服务实时流量分布”动态显示了以总速率排名的前十名服务。当鼠标滑过某服务名称时，会出现“显示在线用户”的提示，点击即可查看该服务的在线用户的信息。当鼠标滑过某服务后面的带宽值时，会出现“显

示最近一小时的趋势图”的提示，点击即可查看到该服务最近一小时的速率趋势图。点击对应的<详细>按钮，可以连接到“服务趋势图”页面，查看到前十名服务的速率叠加趋势。

“今日服务器安全排行前九”动态显示了发送攻击次数排列前九的服务器地址。

“ 今日安全日志汇总” 动态显示了各攻击类型被累计攻击的次数。

“最近五次事件日志”动态显示了最近五次的事件日志。点击<详细>按钮，可以连接到“事件日志”页面，查看和搜索更多的事件日志。

8 实时监控

实时监控部分用于查看设备实时的工作状态，包括设备资源、物理接口、服务监控、用户监控、在线用户、防共享上网、当前黑名单七大部分。

8.1设备资源

设备资源包括了 CPU 使用率、内存使用率、活跃会话数、在线用户数、在线认证用户数、磁盘信息等共六部分。如下图：

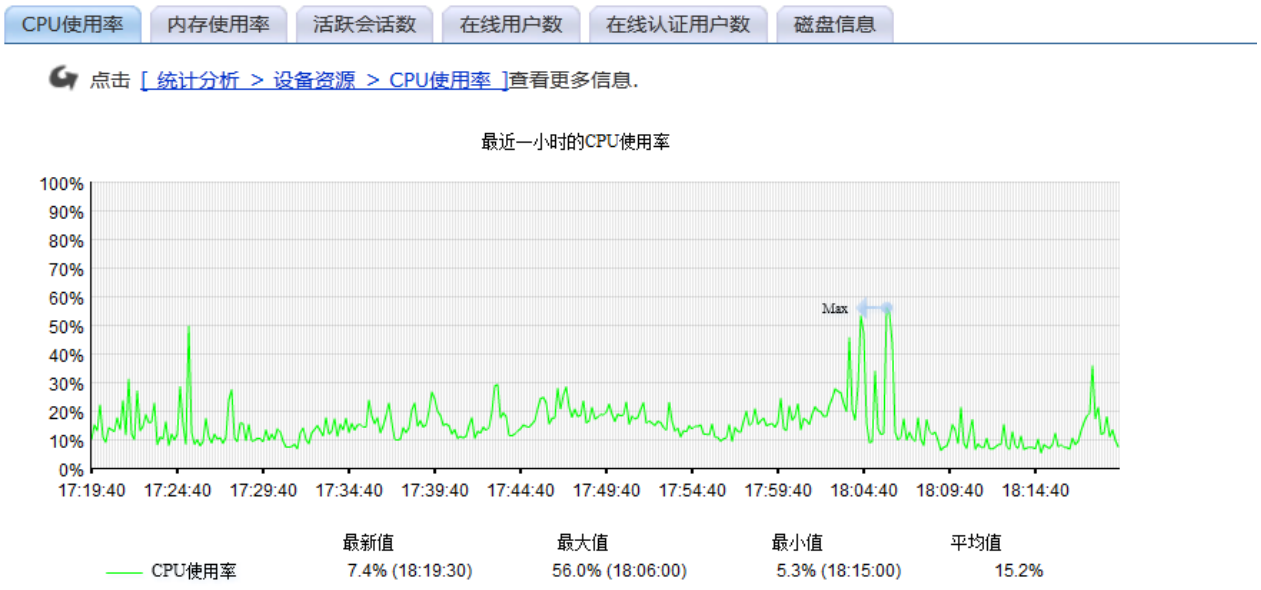


图2. 设置资源

各分页详细说明如下：

- CPU 使用率：查看最近一小时 CPU 使用率；
- 内存使用率：查看最近一小时内存使用率；
- 活跃会话数：查看最近一小时活跃会话数的统计趋势图；

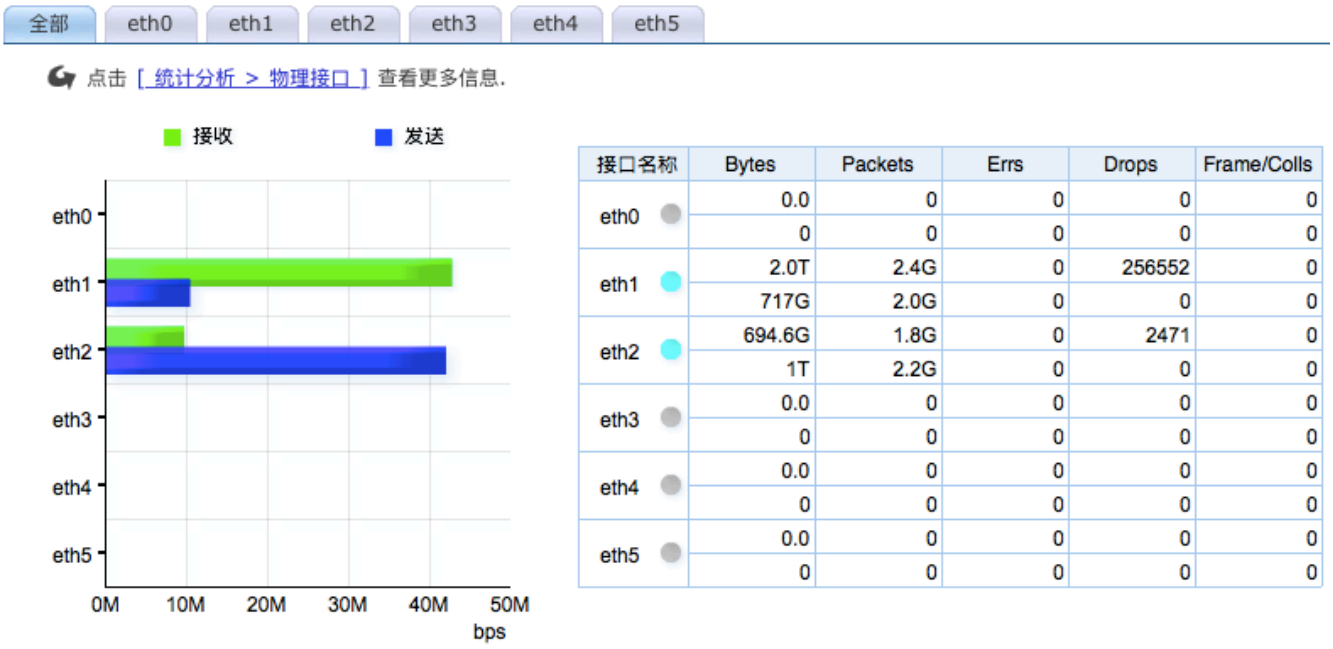
- 在线用户数：查看最近一小时在线用户数的统计趋势图；
- 在线认证用户数：查看最近一小时在线认证用户数的统计趋势图；

每个图的下方都显示了最新值(最近一个采样点的值)、最近一小时的最大值、最小值、平均值及每个值对应的时间点。图中还用箭头指明了最大值，如果这些值分布在多个时间点，则显示最后一个时间点。例如，最大值分布在 18:04:40 和 18:09:40 两个时间点，那么图中箭头指明的时间点和图下方最大值对应的括号中的时间点都是 18:06:00。

8.2物理接口

物理接口页面的内容含两部分：所有端口的全局信息、每个端口的速率趋势图。

第一：物理接口的全局信息，如下图：



接口名称	Bytes	Packets	Errs	Drops	Frame/Colls
eth0	0.0	0	0	0	0
	0	0	0	0	0
eth1	2.0T	2.4G	0	256552	0
	717G	2.0G	0	0	0
eth2	694.6G	1.8G	0	2471	0
	1T	2.2G	0	0	0
eth3	0.0	0	0	0	0
	0	0	0	0	0
eth4	0.0	0	0	0	0
	0	0	0	0	0
eth5	0.0	0	0	0	0
	0	0	0	0	0

图3. 物理接口统计图

全局信息包括了以下内容：

- 柱状图显示了每个物理接口收发速率。
- 表格显示了每个接口的收发数据的统计信息，每个物理接口上面一行对应该接口接收数据的统计信息，下面一行对应该接口发送数据的统计信息。
- 表格中的古蓝色圆饼代表该端口为连接状态，灰色圆饼代表该端口为未连接状态。

第二：单个物理接口的统计信息包括了总的速率、接收速率、发送速率，如下图：

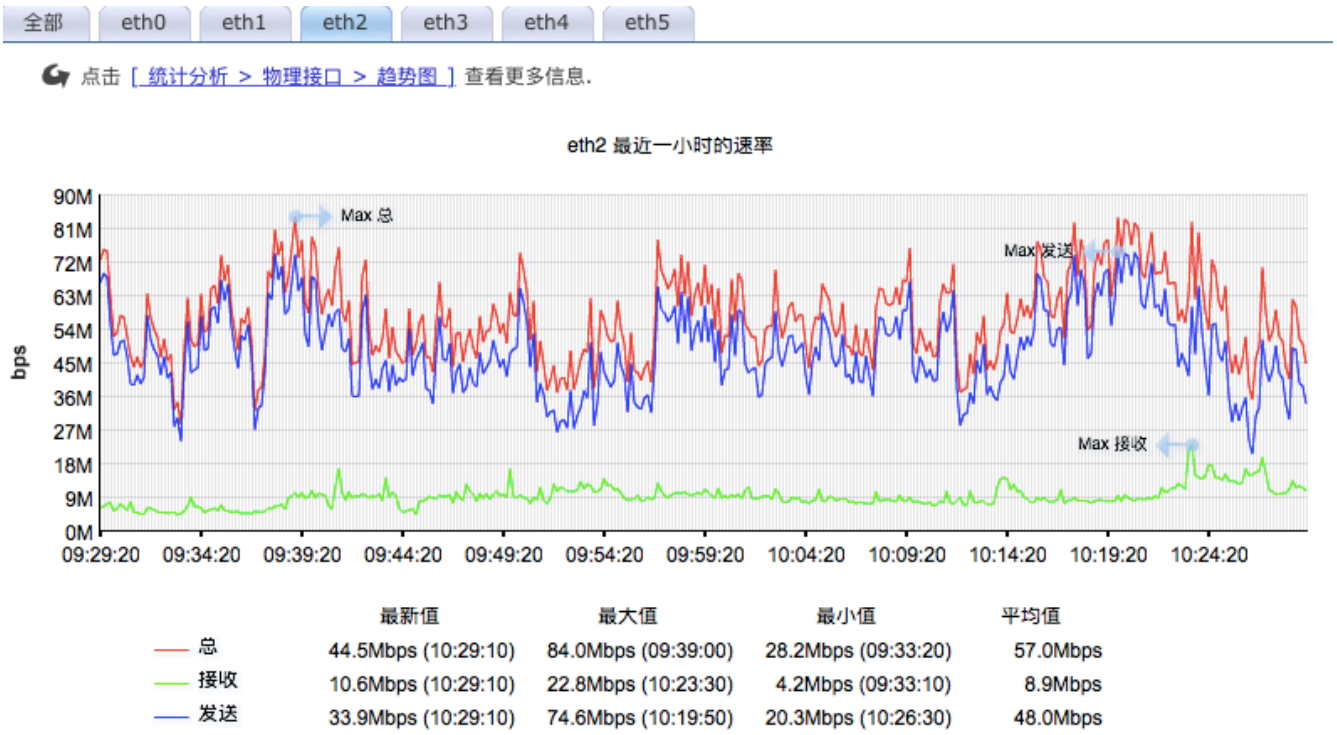


图4. ETH2 物理接口统计图

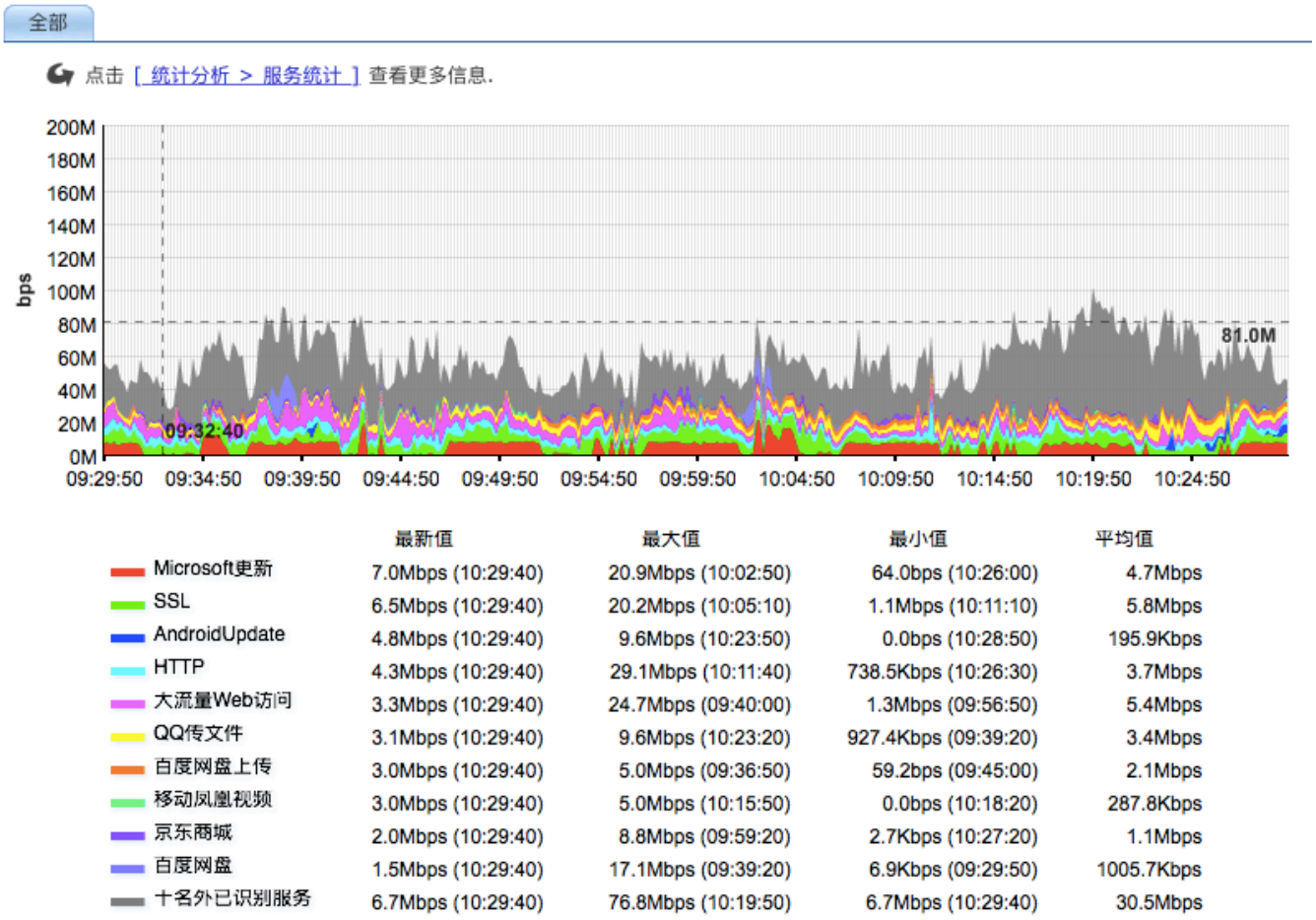
每个接口分页的下方都显示了最新值(最近一个采样点的值)、最近一小时的最大值、最小值、平均值及每个值对应的时间点。

8.3服务监控

服务监控页面显示了前十名服务趋叠加势图、服务组趋势图、活跃服务、所有服务四部分。

8.3.1 服务趋势叠加图

服务趋势叠加图如下：



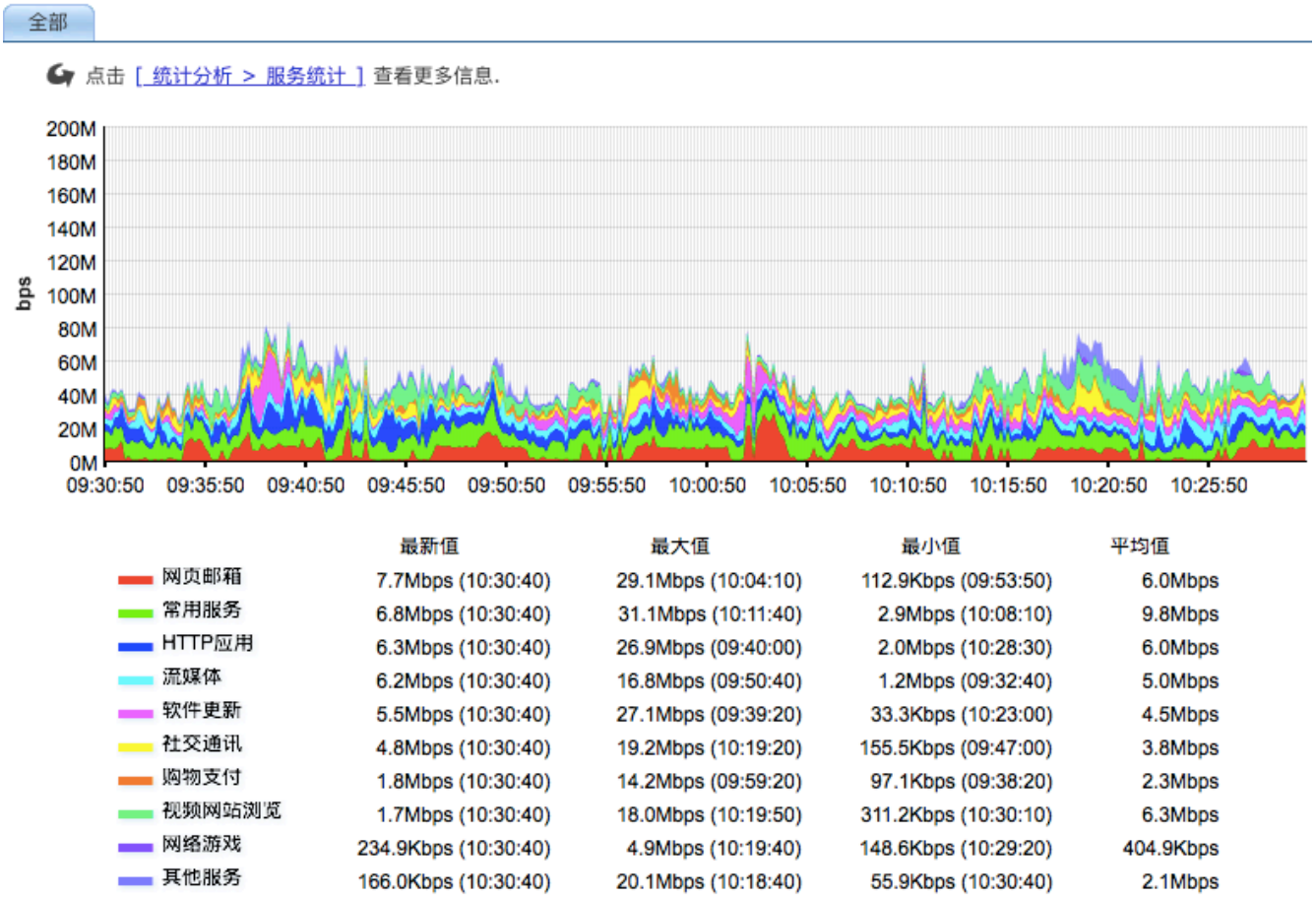
	最新值	最大值	最小值	平均值
Microsoft更新	7.0Mbps (10:29:40)	20.9Mbps (10:02:50)	64.0bps (10:26:00)	4.7Mbps
SSL	6.5Mbps (10:29:40)	20.2Mbps (10:05:10)	1.1Mbps (10:11:10)	5.8Mbps
AndroidUpdate	4.8Mbps (10:29:40)	9.6Mbps (10:23:50)	0.0bps (10:28:50)	195.9Kbps
HTTP	4.3Mbps (10:29:40)	29.1Mbps (10:11:40)	738.5Kbps (10:26:30)	3.7Mbps
大流量Web访问	3.3Mbps (10:29:40)	24.7Mbps (09:40:00)	1.3Mbps (09:56:50)	5.4Mbps
QQ传文件	3.1Mbps (10:29:40)	9.6Mbps (10:23:20)	927.4Kbps (09:39:20)	3.4Mbps
百度网盘上传	3.0Mbps (10:29:40)	5.0Mbps (09:36:50)	59.2bps (09:45:00)	2.1Mbps
移动凤凰视频	3.0Mbps (10:29:40)	5.0Mbps (10:15:50)	0.0bps (10:18:20)	287.8Kbps
京东商城	2.0Mbps (10:29:40)	8.8Mbps (09:59:20)	2.7Kbps (10:27:20)	1.1Mbps
百度网盘	1.5Mbps (10:29:40)	17.1Mbps (09:39:20)	6.9Kbps (09:29:50)	1005.7Kbps
十名外已识别服务	6.7Mbps (10:29:40)	76.8Mbps (10:19:50)	6.7Mbps (10:29:40)	30.5Mbps

图5. 服务监控统计图

这里显示了所有服务的叠加趋势图，其中列出了前十名的服务趋势图。

8.3.2 服务组趋势图

服务组趋势图如下：



	最新值	最大值	最小值	平均值
网页邮箱	7.7Mbps (10:30:40)	29.1Mbps (10:04:10)	112.9Kbps (09:53:50)	6.0Mbps
常用服务	6.8Mbps (10:30:40)	31.1Mbps (10:11:40)	2.9Mbps (10:08:10)	9.8Mbps
HTTP应用	6.3Mbps (10:30:40)	26.9Mbps (09:40:00)	2.0Mbps (10:28:30)	6.0Mbps
流媒体	6.2Mbps (10:30:40)	16.8Mbps (09:50:40)	1.2Mbps (09:32:40)	5.0Mbps
软件更新	5.5Mbps (10:30:40)	27.1Mbps (09:39:20)	33.3Kbps (10:23:00)	4.5Mbps
社交通讯	4.8Mbps (10:30:40)	19.2Mbps (10:19:20)	155.5Kbps (09:47:00)	3.8Mbps
购物支付	1.8Mbps (10:30:40)	14.2Mbps (09:59:20)	97.1Kbps (09:38:20)	2.3Mbps
视频网站浏览	1.7Mbps (10:30:40)	18.0Mbps (10:19:50)	311.2Kbps (10:30:10)	6.3Mbps
网络游戏	234.9Kbps (10:30:40)	4.9Mbps (10:19:40)	148.6Kbps (10:29:20)	404.9Kbps
其他服务	166.0Kbps (10:30:40)	20.1Mbps (10:18:40)	55.9Kbps (10:30:40)	2.1Mbps

图6. 服务组监控统计图

这里显示了所有服务组的叠加趋势图，一共有自定义普通服务、自定义特征识别、常用服务、HTTP 下载、P2P 下载、WEB 视频、流媒体、即时通讯、网络电话、网络游戏、股票交易、网上银行、其他服务等 13 种类型。

8.3.3 活跃服务统计

“活跃服务”将显示当前所有的活跃的服务，如下图：

全部

活跃服务

序号	服务名称	最新速率(bps)	最近一小时总流量(Byte)	最近一小时平均速率(bps)	操作
1	大流量Web访问	↑ 318.4K, ↓ 7.1M	↑ 332.2M, ↓ 2.0G	↑ 755.9K, ↓ 4.6M	趋势图 在线用户
2	Microsoft更新	↑ 97.8K, ↓ 7.3M	↑ 53.6M, ↓ 2.0G	↑ 122.0K, ↓ 4.6M	趋势图 在线用户
3	SSL	↑ 392.2K, ↓ 4.5M	↑ 250.6M, ↓ 2.3G	↑ 570.4K, ↓ 5.2M	趋势图 在线用户
4	QQ传文件	↑ 63.1K, ↓ 3.1M	↑ 151.8M, ↓ 1.3G	↑ 345.5K, ↓ 3.0M	趋势图 在线用户
5	百度网盘上传	↑ 3.0M, ↓168.3K	↑ 908.3M, ↓ 54.9M	↑ 2.0M, ↓124.9K	趋势图 在线用户
6	迅雷	↑ 1.1M, ↓ 1.9M	↑ 264.4M, ↓ 545.7M	↑ 601.7K, ↓ 1.2M	趋势图 在线用户
7	HTTP	↑ 771.9K, ↓ 1.2M	↑ 299.5M, ↓ 1.3G	↑ 681.5K, ↓ 3.0M	趋势图 在线用户
8	百度网盘下载	↑ 28.8K, ↓ 1.7M	↑ 10.1M, ↓ 484.5M	↑ 23.1K, ↓ 1.1M	趋势图 在线用户
9	天涯社区	↑ 23.5K, ↓ 1.4M	↑ 1.7M, ↓ 34.8M	↑ 3.8K, ↓79.2K	趋势图 在线用户
10	京东商城	↑ 294.5K, ↓727.5K	↑ 54.7M, ↓ 429.4M	↑ 124.4K, ↓977.1K	趋势图 在线用户
11	QQ/TM	↑ 195.3K, ↓392.5K	↑ 25.2M, ↓ 80.2M	↑ 57.4K, ↓182.4K	趋势图 在线用户
12	新浪论坛	↑ 20.3K, ↓530.8K	↑ 11.1M, ↓ 361.6M	↑ 25.2K, ↓822.8K	趋势图 在线用户

图7. 活跃服务监控统计图

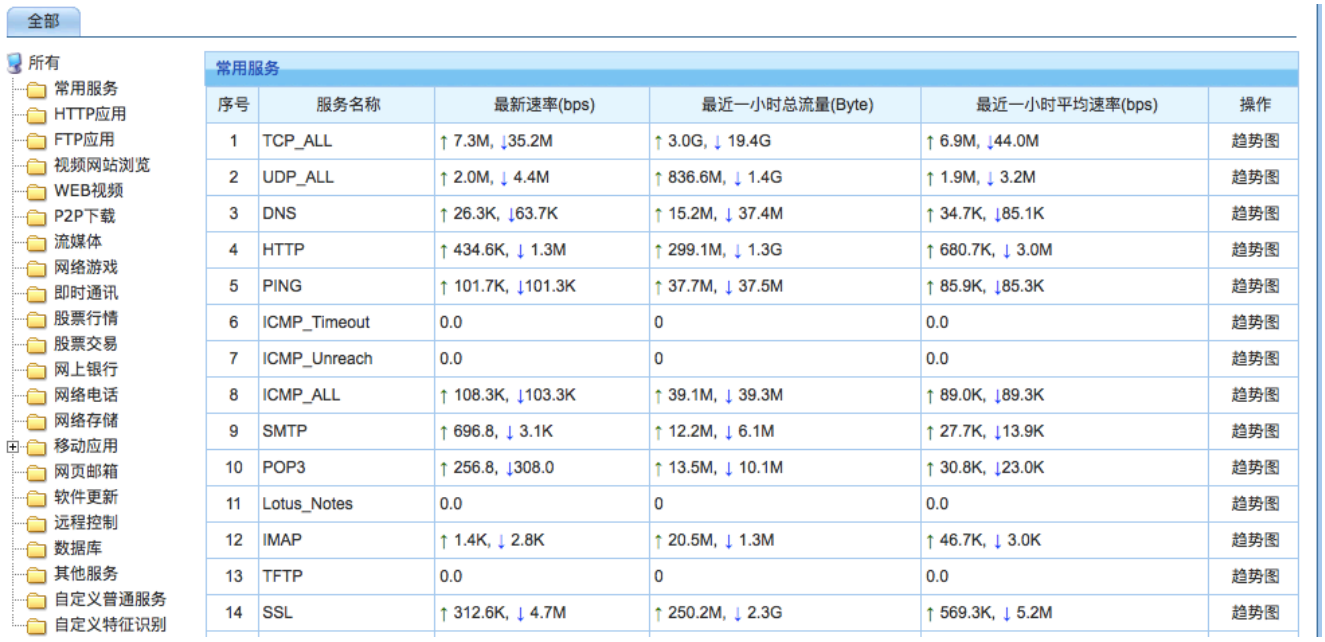
参数说明：

- 最新速率：表示某服务最后一个采样点的速率值。上箭头后面的值表示上行速率，下箭头后面的值表示下行速率。
- 最近一小时总流量：表示某服务最近一小时传输的流量叠加值。上箭头后面的值表示上行流量，下箭头后面的值表示下行流量。
- 最近一小时平均速率：表示某服务最近一小时的平均速率。上箭头后面的值表示上行速率，下箭头后面的值表示下行速率。

点击对应服务操作栏的<趋势图>按钮，查看该服务最近一小时的速率趋势图。点击<在线用户>，查看正在使用该服务的用户的信息。

8.3.4 所有服务统计

“所有服务”将分类显示所有的服务统计值，如下图：



序号	服务名称	最新速率(bps)	最近一小时总流量(Byte)	最近一小时平均速率(bps)	操作
1	TCP_ALL	↑ 7.3M, ↓35.2M	↑ 3.0G, ↓ 19.4G	↑ 6.9M, ↓44.0M	趋势图
2	UDP_ALL	↑ 2.0M, ↓ 4.4M	↑ 836.6M, ↓ 1.4G	↑ 1.9M, ↓ 3.2M	趋势图
3	DNS	↑ 26.3K, ↓63.7K	↑ 15.2M, ↓ 37.4M	↑ 34.7K, ↓85.1K	趋势图
4	HTTP	↑ 434.6K, ↓ 1.3M	↑ 299.1M, ↓ 1.3G	↑ 680.7K, ↓ 3.0M	趋势图
5	PING	↑ 101.7K, ↓101.3K	↑ 37.7M, ↓ 37.5M	↑ 85.9K, ↓85.3K	趋势图
6	ICMP_Timeout	0.0	0	0.0	趋势图
7	ICMP_Unreach	0.0	0	0.0	趋势图
8	ICMP_ALL	↑ 108.3K, ↓103.3K	↑ 39.1M, ↓ 39.3M	↑ 89.0K, ↓89.3K	趋势图
9	SMTP	↑ 696.8, ↓ 3.1K	↑ 12.2M, ↓ 6.1M	↑ 27.7K, ↓13.9K	趋势图
10	POP3	↑ 256.8, ↓308.0	↑ 13.5M, ↓ 10.1M	↑ 30.8K, ↓23.0K	趋势图
11	Lotus_Notes	0.0	0	0.0	趋势图
12	IMAP	↑ 1.4K, ↓ 2.8K	↑ 20.5M, ↓ 1.3M	↑ 46.7K, ↓ 3.0K	趋势图
13	TFTP	0.0	0	0.0	趋势图
14	SSL	↑ 312.6K, ↓ 4.7M	↑ 250.2M, ↓ 2.3G	↑ 569.3K, ↓ 5.2M	趋势图

图8. 所有服务监控统计

参数说明：

- 最新速率：表示某服务最后一个采样点的速率值。上箭头后面的值表示上行速率，下箭头后面的值表示下行速率。
- 最近一小时总流量：表示某服务最近一小时传输的流量叠加值。上箭头后面的值表示上行流量，下箭头后面的值表示下行流量。
- 最近一小时平均速率：表示某服务最近一小时的平均速率。上箭头后面的值表示上行速率，下箭头后面的值表示下行速率。
- 点击对应服务操作栏的<趋势图>按钮，查看该服务最近一小时的速率趋势图。点击<在线用户>，查看正在使用该服务的用户的信息。

8.4用户监控

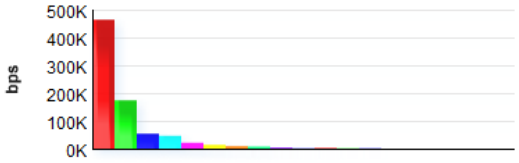
用户监控页面显示了前五十名用户的实时传输速率、新建会话速率和活跃会话数。

8.4.1 流量分析

前五十名用户的实时传输速率统计图如下：

全部

点击 [统计分析 > IP统计 > 流量统计] 查看更多信息.



序号	IP地址	用户名	用户组	总(bps)	上行(bps)	下行(bps)	操作
1	172.16.20.145	172.16.20.145	Root	463.4K	377.2K	86.3K	趋势图 活跃服务 黑名单 强制下线
2	172.16.99.2	172.16.99.2	Root	173.8K	161.9K	11.9K	趋势图 活跃服务 黑名单 强制下线
3	172.16.0.222	172.16.0.222	Root	54.1K	39.9K	14.2K	趋势图 活跃服务 黑名单 强制下线
4	172.16.20.30	172.16.20.30	Root	45.6K	24.0K	21.6K	趋势图 活跃服务 黑名单 强制下线
5	172.16.111.190	172.16.111.190	Root	21.4K	1.3K	20.1K	趋势图 活跃服务 黑名单 强制下线
6	172.16.16.99	172.16.16.99	Root	13.2K	9.4K	3.8K	趋势图 活跃服务 黑名单 强制下线
7	172.16.16.60	172.16.16.60	Root	8.3K	6.6K	1.7K	趋势图 活跃服务 黑名单 强制下线
8	172.16.17.7	172.16.17.7	Root	7.1K	2.6K	4.5K	趋势图 活跃服务 黑名单 强制下线
9	172.16.212.212	172.16.212.212	Root	3.1K	1.2K	2.0K	趋势图 活跃服务 黑名单 强制下线
10	172.16.161.248	172.16.161.248	Root	3.0K	805.6	2.2K	趋势图 活跃服务 黑名单 强制下线
11	172.16.16.221	172.16.16.221	Root	1.9K	776.0	1.1K	趋势图 活跃服务 黑名单 强制下线
12	172.16.111.206	172.16.111.206	Root	1.1K	157.6	976.0	趋势图 活跃服务 黑名单 强制下线
13	172.16.111.85	172.16.111.85	Root	963.2	428.8	534.4	趋势图 活跃服务 黑名单 强制下线
14	172.16.111.30	172.16.111.30	Root	441.6	288.8	152.8	趋势图 活跃服务 黑名单 强制下线
15	172.16.111.222	172.16.111.222	Root	216.0	88.8	127.2	趋势图 活跃服务 黑名单 强制下线
16	172.16.17.11	172.16.17.11	Root	204.8	92.0	112.8	趋势图 活跃服务 黑名单 强制下线
17	172.16.100.188	172.16.100.188	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
18	172.16.166.166	172.16.166.166	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
19	172.16.16.18	172.16.16.18	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线

图9. 流量分析

点击<趋势图>按钮，查看该用户最近一小时的速率趋势图。

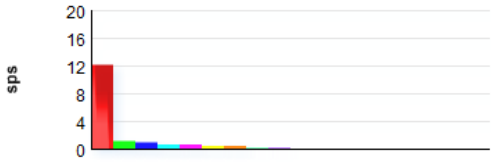
点击<活跃服务>按钮，查看该用户当前使用的服务的信息。

8.4.2 会话分析

前五十名用户的新建会话的统计图如下：

全部

点击 [统计分析 > IP统计 > 新建会话] 查看更多信息.



序号	IP地址	用户名	用户组	总(sps)	上行(sps)	下行(sps)	操作
1	172.16.0.222	172.16.0.222	Root	12.1	12.1	0.0	趋势图 活跃服务 黑名单 强制下线
2	172.16.16.99	172.16.16.99	Root	1.1	1.1	0.0	趋势图 活跃服务 黑名单 强制下线
3	172.16.16.221	172.16.16.221	Root	0.9	0.9	0.0	趋势图 活跃服务 黑名单 强制下线
4	172.16.20.145	172.16.20.145	Root	0.6	0.6	0.0	趋势图 活跃服务 黑名单 强制下线
5	172.16.16.60	172.16.16.60	Root	0.6	0.6	0.0	趋势图 活跃服务 黑名单 强制下线
6	172.16.20.30	172.16.20.30	Root	0.4	0.4	0.0	趋势图 活跃服务 黑名单 强制下线
7	172.16.99.2	172.16.99.2	Root	0.4	0.4	0.0	趋势图 活跃服务 黑名单 强制下线
8	172.16.17.11	172.16.17.11	Root	0.1	0.1	0.0	趋势图 活跃服务 黑名单 强制下线
9	172.16.111.85	172.16.111.85	Root	0.1	0.1	0.0	趋势图 活跃服务 黑名单 强制下线
10	172.16.16.90	172.16.16.90	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
11	172.16.111.206	172.16.111.206	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
12	172.16.166.166	172.16.166.166	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
13	172.16.111.222	172.16.111.222	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
14	172.16.0.177	172.16.0.177	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
15	172.16.16.18	172.16.16.18	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
16	172.16.111.30	172.16.111.30	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
17	172.16.111.186	172.16.111.186	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线
18	172.16.100.188	172.16.100.188	Root	0.0	0.0	0.0	趋势图 活跃服务 黑名单 强制下线

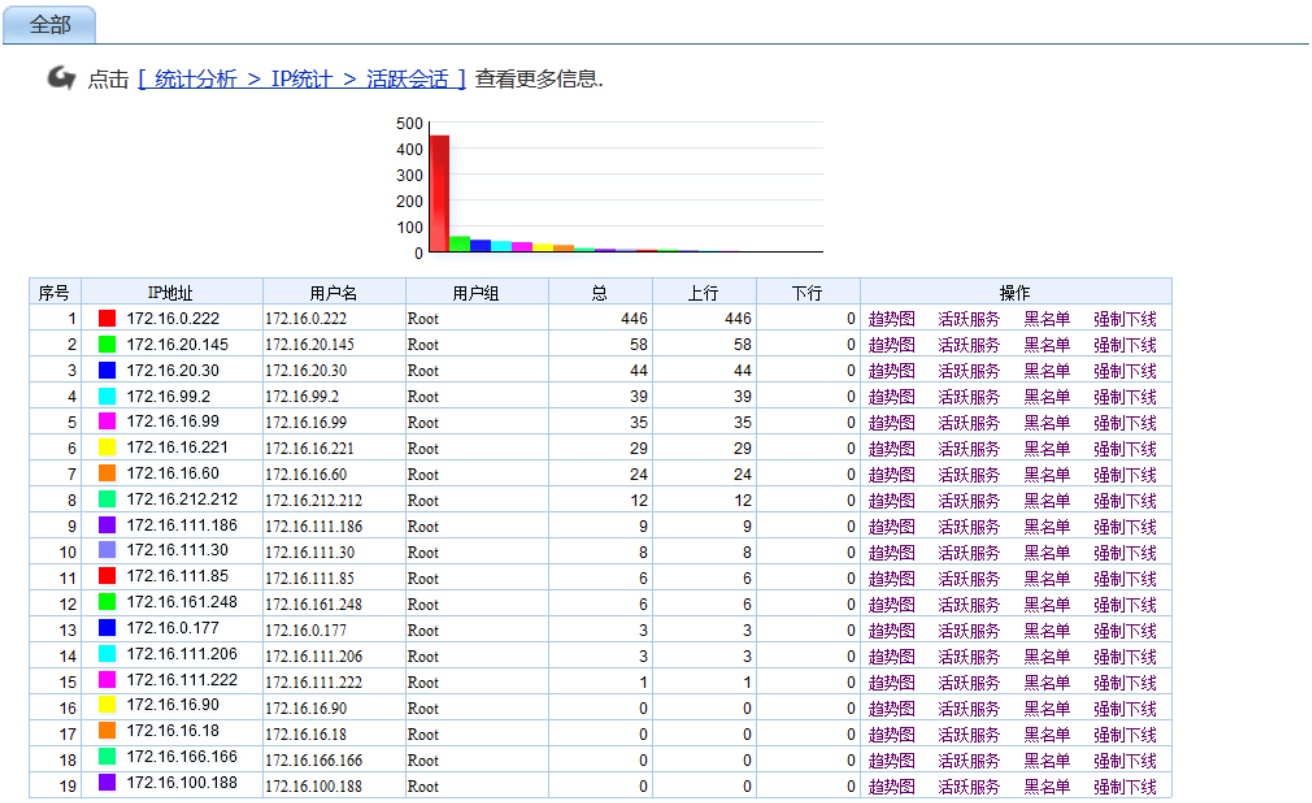
图10.会话分析

点击<趋势图>按钮，查看该用户最近一小时的速率趋势图。

点击<活跃服务>按钮，查看该用户当前使用的服务的信息。

8.4.3 活跃会话

前五十名用户的当前活跃会话统计图如下:



序号	IP地址	用户名	用户组	总	上行	下行	操作
1	172.16.0.222	172.16.0.222	Root	446	446	0	趋势图 活跃服务 黑名单 强制下线
2	172.16.20.145	172.16.20.145	Root	58	58	0	趋势图 活跃服务 黑名单 强制下线
3	172.16.20.30	172.16.20.30	Root	44	44	0	趋势图 活跃服务 黑名单 强制下线
4	172.16.99.2	172.16.99.2	Root	39	39	0	趋势图 活跃服务 黑名单 强制下线
5	172.16.16.99	172.16.16.99	Root	35	35	0	趋势图 活跃服务 黑名单 强制下线
6	172.16.16.221	172.16.16.221	Root	29	29	0	趋势图 活跃服务 黑名单 强制下线
7	172.16.16.60	172.16.16.60	Root	24	24	0	趋势图 活跃服务 黑名单 强制下线
8	172.16.212.212	172.16.212.212	Root	12	12	0	趋势图 活跃服务 黑名单 强制下线
9	172.16.111.186	172.16.111.186	Root	9	9	0	趋势图 活跃服务 黑名单 强制下线
10	172.16.111.30	172.16.111.30	Root	8	8	0	趋势图 活跃服务 黑名单 强制下线
11	172.16.111.85	172.16.111.85	Root	6	6	0	趋势图 活跃服务 黑名单 强制下线
12	172.16.161.248	172.16.161.248	Root	6	6	0	趋势图 活跃服务 黑名单 强制下线
13	172.16.0.177	172.16.0.177	Root	3	3	0	趋势图 活跃服务 黑名单 强制下线
14	172.16.111.206	172.16.111.206	Root	3	3	0	趋势图 活跃服务 黑名单 强制下线
15	172.16.111.222	172.16.111.222	Root	1	1	0	趋势图 活跃服务 黑名单 强制下线
16	172.16.16.90	172.16.16.90	Root	0	0	0	趋势图 活跃服务 黑名单 强制下线
17	172.16.16.18	172.16.16.18	Root	0	0	0	趋势图 活跃服务 黑名单 强制下线
18	172.16.166.166	172.16.166.166	Root	0	0	0	趋势图 活跃服务 黑名单 强制下线
19	172.16.100.188	172.16.100.188	Root	0	0	0	趋势图 活跃服务 黑名单 强制下线

图11.活跃会话

点击<趋势图>按钮，查看该用户最近一小时的速率趋势图。

点击<活跃服务>按钮，查看该用户当前使用的服务的信息。

8.5在线用户

功能描述：显示当前在线用户的统计信息。

配置路径：【实时监控】>【在线用户】

配置描述：进入【在线用户】配置页面，如下图：

图12.在线用户

查询条件：

- 用户名：根据用户名来查找。
- 所属组：根据用户组来查找，点击输入框后面的<选择>按钮，选择用户组。
- IP 地址：根据用户的 IP 地址来查找。
- MAC 地址：根据用户的 MAC 地址来查找。
- 时间范围：根据进入上线的时间范围来查找。

默认显示所有用户。输入查询条件后，点击<查询>按钮，显示满足查询条件的在线用户。

在线用户：显示当前在线的所有用户，共三种类型，如下：

- 已认证且在组织结构中：显示已经认证，并且已加入组织结构的在线用户。
- 已认证但不在组织结构中：显示已经认证，但未加入组织结构的在线用户。
- 未认证用户：显示未通过认证的在线用户。

参数说明：

- 用户名/用户组：显示用户名称和所属组。
- 地址：显示用户的 IP 地址和 MAC 地址。
- 物理接口：表示用户连接到设备的哪个物理接口。

- 上线时间：用户成为在线用户的时间点。

定制显示项（默认不显示，勾选后显示）：

- 累计在线流量：用户从上线到当前时刻的流量总和。上箭头后面的值表示上行流量的值，下箭头后面的值表示下行流量的值。当用户下线后，其对应的在线流量会被清零。
- 最新速率：用户最后一个采样点的速率值。上箭头后面的值表示上行速率的值，下箭头后面的值表示下行速率的值。
- 活跃会话：用户当前的活跃会话数。上箭头后面的值表示上行会话数，即用户主动发起的会话。下箭头后面的值表示下行会话数，即用户被别人连接时产生的会话。

操作按钮说明：

- 趋势图：链接到该用户的趋势图页面。
- 活跃服务：链接到该用户的活跃服务页面。
- 黑名单：链接到手动加入黑名单页面，可将该用户手动加入黑名单。
- 强制下线：将该用户强制下线。

8.6防共享上网

为解决发现移动终端的问题，部分客户需要对私接路由器、私接 360WiFi 的行为进行阻止，所以在企业的网络管理、在运营商代建的高校网络中出现了防共享上网的需求，即防代理、防一拖 N 的需求。设备支持将一个 IP 对应多个终端数的用户加入防共享上网的名单，以示惩罚。对进入防共享上网的用户可以采取惩罚机制，惩罚期限到了之后，该用户又可以正常使用网络。

功能描述：查看当前有共享行为的用户，需配合【流量控制 >黑名单策略】规则。

配置路径：【实时监控】>【防共享上网】

配置描述：进入【防共享上网】配置页面，如下图：

图13.防共享上网

查询条件：

- 用户名：根据用户名来查找。
- 所属组：根据用户组来查找，点击输入框后面的<选择>按钮，选择用户组。
- IP 地址：根据用户的 IP 地址来查找。
- MAC 地址：根据用户的 MAC 地址来查找。
- 时间范围：根据进入上线的时间范围来查找。

默认显示所有共享行为用户。输入查询条件后，点击<查询>按钮，显示满足查询条件的共享用户。

参数说明：

- 用户名/用户组：显示用户名称和所属组。
- 地址：显示用户的 IP 地址和 MAC 地址。
- 物理接口：表示用户连接到设备的哪个物理接口。
- 上线时间：用户成为在线用户的时间点。
- 内部终端数：进入防共享惩罚时识别出的终端数。
- 操作：查看进入防共享惩罚的详情，添加进黑名单，强制下线。

提示：进入防共享上网惩罚的条目，同时会进入当前黑名单的惩罚列表。

8.7当前黑名单

为了防止网络资源的滥用和方便管理员管理用户，设备支持将超量使用网络资源(流量、带宽、会话)的用户加入黑名单，以示惩罚。对进入黑名单的用户可以采取惩罚机制，惩罚期限到了之后，该用户又可以正常使用网络。需先定义黑名单规则，并在黑名单规则中选择适用用户组，有 IP 违规才会有当前黑名单列表。

功能描述：查看当前黑名单用户，以及手动添加和解除黑名单用户。该规则需配合【流量控制>黑名单策略】规则使用。

配置路径：【实时监控】>【当前黑名单】

配置描述：

第一：进入【当前黑名单】页面，如下图：

图14.当前黑名单

查询条件：

- 用户名：根据用户名来查找。
- IP 地址：根据进入黑名单的 IP 来查找。
- 所属组：根据所属组来查找进入黑名单的用户。
- 黑名单策略：根据用户引用的黑名单策略来查找。

默认显示所有黑名单用户。输入查询条件后，点击<查询>按钮，显示满足查询条件的当前黑名单。

当前黑名单：显示当前的黑名单，相关按钮说明如下：

- 手动添加：手动将某个用户加入黑名单。
- 删除所有：删除所有的当前黑名单用户，相当于接触所有黑名单用户。
- 解除：解除某个黑名单用户。
- 修改：只有手动添加的黑名单用户才有<修改>按钮，即修改手动添加的黑名单用户的配置。

第二：点击<手动添加>按钮，手动添加黑名单用户。如下图：

图15.手动添加黑名单用户

参数说明：

- 用户名：用户的名称。
- 惩罚方式：当用户进入黑名单时的惩罚方式。“强制下线”表示该用户不能上网，“修改带宽和会话”表示修

改用户的带宽和会话值。

- 惩罚时长：用户进入黑名单的时间。当惩罚时间到了，用户又可以正常上网。

9 网络配置

网络配置包括安全区域、接口配置、路由设置、DNS 配置、DDNS 配置、DHCP 配置、ARP 表等七部分。

9.1安全区域

功能描述：用于设置接口所属的区域，以提供内容安全、IPS、服务器保护、防火墙等模块调用。其中安全区域又分为二层区域、三层区域，虚拟网线区域三种类型，二层区域可以选择所有透明接口和旁路镜像接口，三层区域可以选择所有路由接口，包括子接口，虚网线区域可以选择所有虚拟网线接口。

配置路径：【网络配置】>【安全区域】

配置描述：

第一 ：进入【安全区域】页面，显示当前设备中所有的区域。如下图所示：

图16.安全区域

按钮说明：

点击<删除全部>，将删除所有没有被调用的安全区域 。

点击<新增>， 增加安全区域 。

点击<删除>，删除本条安全区域

点击<修改>，修改本条安全区域的参数，但不能修改本条安全区域的名称。

第二：进入点击<新增>按钮，添加安全区域。如下图：

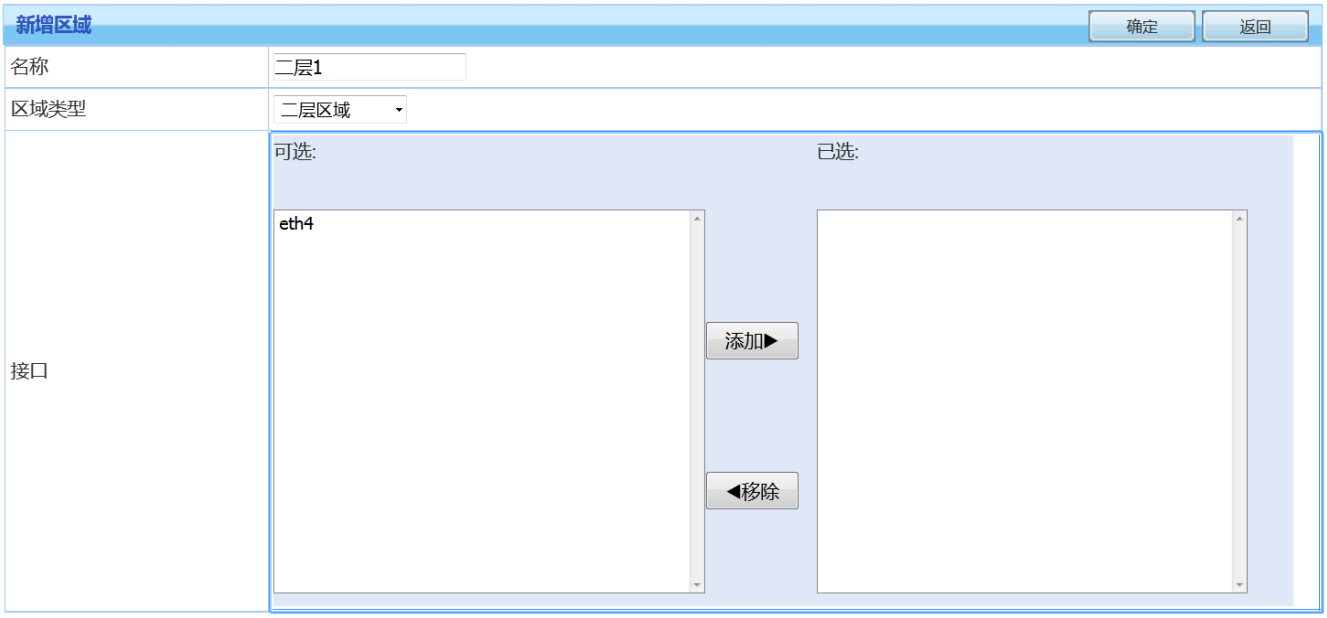


图17.新增安全区域

参数说明：

- 名称： 安全区域的名称。
- 区域类型：设置区域的类型。
  - 如果选择二层区域，接口列表会显示未被划到其他任何区域的剩余的透明接口和旁路镜像接口；
  - 如果选择三层区域，接口列表会显示未被划到其他任何区域的剩余的路由接口，包括子接口；
  - 如果选择虚拟网线区域，接口列表会显示未被划到其他任何区域的剩余的虚拟网线接口；
- 接口： 选择加入本安全区域的接口。选中某接口后，可通过<增加>，<移除>按钮来添加和删除接口；
- 确定： 点击<确定>按钮后，完成配置；
- 返回：点击<返回>按钮后，取消；

提示：

1、一个接口只能属于一个安全区域，一个安全区域可以选择多个接口。一个区域可以同时选择 LAN 属性和 WAN 属性的接口。

2、如果安全区域被某模块调用，则不能被删除，若想删除，需将调用解除。

3、系统默认存在的一个“PPTP-VPN”安全区域，不能被删除和修改。进行 PPTP 拨号成功的用户默认加入该区域。

9.2接口配置

接口配置包括物理接口和子接口两部分。

9.2.1 物理接口

功能描述：物理接口页面可以查看各个接口的名称、描述、连接状态、接口类型 、所属区域、是否WAN、连接类型、IP地址、工作速率、MUT、PING、链路状态、接口UP或DOWN、MAC值等。

配置路径：【网络配置】>【 接口配置】>【物理接口】

配置描述：

第一 ：进入【物理接口】页面，显示当前各物理口的状态。如下图所示：

接口名称	连接状态	接口类型	所属区域	WAN	连接类型	IP地址	工作速率	MTU	PING	链路状态	状态	MAC	操作
eth0		路由	未选择区域	否	静态IPv4/静态IPv6	10.254.254.254/24		1500	允许	未检测	☑	1e:c5:6c:c0:00:9c	修改
eth1 WAN		路由	三层外网	是	静态IPv4/静态IPv6	/30 fe80::1cc5:6cff:fec0:9d/64	100Mb/s	1500	允许	未检测	☑	1e:c5:6c:c0:00:9d	修改
eth2 LAN		路由	三层内网	否	静态IPv4/静态IPv6	192.168.1.1/24 fe80::1cc5:6cff:fec0:9e/64	1000Mb/s	1500	允许	未检测	☑	1e:c5:6c:c0:00:9e	修改
eth3		路由	未选择区域	否	静态IPv4/静态IPv6			1500	不允许	未检测	☑	1e:c5:6c:c0:00:9f	修改
eth4		路由	未选择区域	否	静态IPv4/静态IPv6			1500	不允许	未检测	☑	1e:c5:6c:c0:00:a0	修改
eth5		路由	未选择区域	否	静态IPv4/静态IPv6			1500	不允许	未检测	☑	1e:c5:6c:c0:00:a1	修改

图18.物理接口

按钮说明：

点击<修改>,修改物理接口的参数；

点击<修改状态>，修改接口使用状态。在状态栏列表中，打√的复选框代表对应的接口 UP,未打√的复选框代表该接口 down；

参数说明：

- 接口名称：物理接口的名称，物理接口的名称不能修改。
- 描述：对接口的描述。如上图中eth0口，描述内容为“管理端口”。
- 连接状态：以图标颜色显示接口的链路状态， 表示接口已连接，处于UP状态， 表示接口未接线或者物理接口DOWN 掉。
- 接口类型：显示接口所属的类型。接口类型有路由模式、透明模式、虚拟网线模式和旁路镜像模式四种。
- 所属区域：接口所对应的安全区域。安全区域详见【网络配置 >安全区域】。
- WAN:显示接口是否为WAN口
- 连接类型：显示接口 IP 地址获取的类型。包括ADSL IPv4、静态 IPv4、DHCP IPv4、静态 IPv6、DHCP IPv6。
- IP地址：显示接口的IP地址。包括ipv6和ipv4。只要接口处于连接状态系统默认产生一个ipv6地址：fe80::6e62:6dff:fe4a:433d/64。
- 工作速率：显示接口的工作模式，如自动协商、全双工10M、全双工100M、全双工1G、全双工10G。

- PING:显示接口的IP是否允许PING。
- 链路状态：显示接口的链路工作状态。进行链路健康检测功能只使用于路由模式的接口。
- 状态：显示接口是否启用， 表示当前接口已启用。修改复选框内的当前状态，再点击<修改状态>，即能改变当前接口的状态。
- MAC：显示接口对应的 MAC。

9.2.1.1 路由模式

功能描述：选择为路由模式的接口需要配置IP地址，并且该接口具有路由转发功，像一个路由器一样部署在网络中。

配置路径：【网络配置】>【 接口配置】>【物理接口】

配置描述：进入点击【修改】页面，可查看路由模式下，接口各参数。如下图所示：

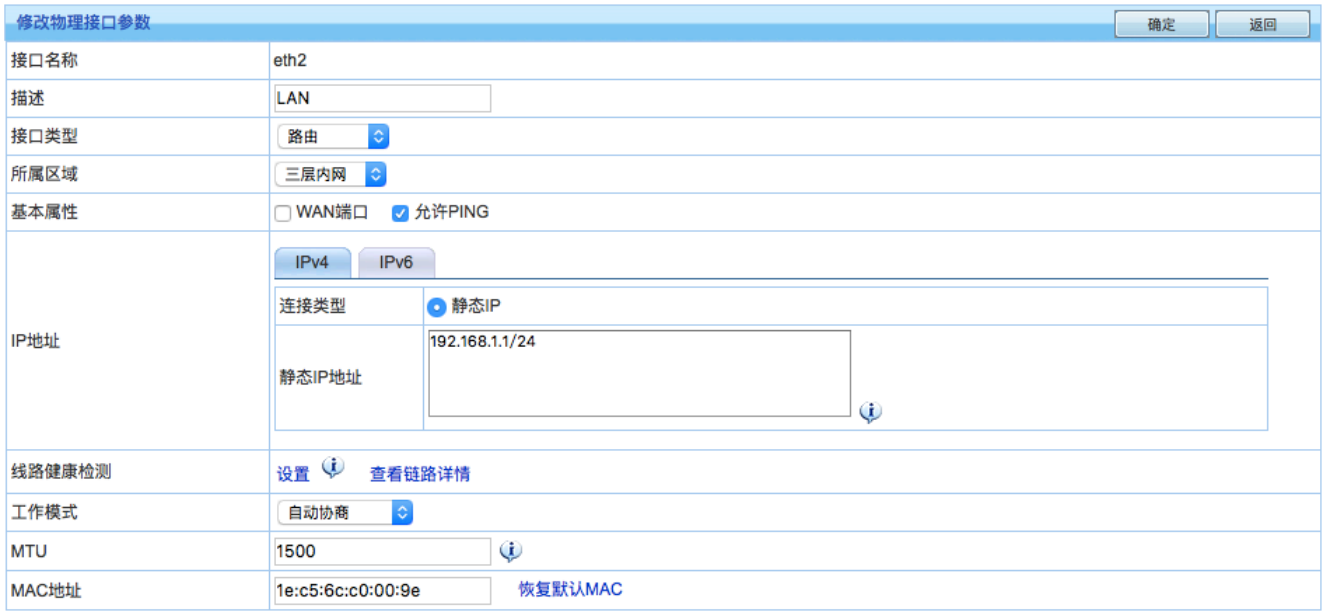


图19.修改物理接口-路由模式

参数说明：

- 接口类型：即决定了接口的模式，又决定了设备数据的转发功能。上图为“路由模式”，其中接口类型又分为：
  - ✧ 路由：此类型下的接口需要配置IP地址，并且该接口具有路由转发功能。
  - ✧ 透明：此接口相当于普通的交换接口，不需要配置 IP 地址，不支持路由转发，根据MAC 地址表转发数据。
  - ✧ 虚拟网线：此接口也是普通的交换接口，不需要配置 IP 地址，不支持路由转发，转发数据时，直接从虚拟网线配对的接口转发。
  - ✧ 旁路镜像：连接到有镜像功能的交换机上，用于镜像流经交换机的数据。

- 基本属性：用于设置是否为 WAN 口和允许 PING。接口为外网接口需要勾选WAN口。否则将统计不到任何过改接口的流量、会话和上网信息。
- 所属区域：选择接口所对应的区域。既可以在<所属区域>下拉框中新增，也可在【网络配置 >安全区域】中设置，上图为“三层内网”安全区域。
- IP地址：有静态 IP、DHCP、ADSL 拨号三种，根据该线路的需要进行配置。
  - ✧ 如果选择静态IP，要手动添加IP地址/掩码以及下一跳网关（如果不勾选WAN口，可以不添加）
  - ✧ 如果该接口是DHCP自动获得地址则设置DHCP参数；
  - ✧ 如果线路是 ADSL 拨号，则配置好拨号所需的用户名、密码和其他拨号参数。

  IPV6只支持静态IP和dhcp两种方式，配置方法和ipv4相同
- 上行带宽/下行带宽：设置链路的上下行带宽
- 链路健康检测：用于检测链路的连通性。配置详情查看【网络配置 >安全区域>物理接口>链路健康检测】。
- 工作模式：配置链路的工作模式。如：自动协商、全双工10M、全双工100M、全双工1G、全双工10G。
- MTU：设置数据包通过该接口的MTU值
- MAC地址：设置接口的MAC地址。

提示：

1、 ETH0 管理口的接口模式为路由口，不可更改接口模式，ETH0 口可以增加管理 IP 地址，但是默认的管理 IP 地址 10.254.254.254/24 不能删除。

2、 路由模式下，同一接口可以配置多个不同网段的 IP，且每个 IP 均生效。

3、 无论设备工作在何种模式下，建议将接口加入安全区域，否则可能影响其它模块的使用

9.2.1.2 透明模式

功能描述：选择为透明模式的接口相当于普通的交换接口，不需要配置 IP 地址，不支持路由转发，根据MAC地址表转发数据。

配置路径：【网络配置】>【 接口配置】>【物理接口】

配置描述：进入点击【修改】页面，可查看透明模式下，接口各参数。如下图所示：

图20.修改物理接口-透明模式

参数说明：

- 接口类型：即决定了接口的模式，又决定了设备数据的转发功能。上图为“透明模式”，其中接口类型又分为：
  - 路由：此类型下的接口需要配置IP地址，并且该接口具有路由转发功能。
  - 透明：此接口相当于普通的交换接口，不需要配置 IP 地址，不支持路由转发，根据MAC 地址表转发数据。
  - 虚拟网线：此接口也是普通的交换接口，不需要配置 IP 地址，不支持路由转发，转发数据时，直接从虚拟网线配对的接口转发。
  - 旁路镜像：连接到有镜像功能的交换机上，用于镜像流经交换机的数据。
- 基本属性：用于设置是否为WAN口。接口为外网接口需要勾选WAN口。否则将统计不到任何过改接口的流量、会话和上网信息。
- 所属区域：选择接口所对应的区域。既可以在<所属区域>下拉框中新增，也可在【网络配置 >安全区域】中设置，上图为“二层外网”安全区域。
- 连接类型：可以选择为 access 或者 trunk。，access 接口默认为vlan1，可以不修改，也可以设置成其它vlan；Ttrunk接口的Native ID在包转发过程中和access中的vlan ID一样，vlan范围可以根据需要适当修改。
- 上行带宽/下行带宽：设置链路的上下行带宽。
- 工作模式：配置链路的工作模式。如：自动协商、全双工10M、全双工100M、全双工1G、全双工10G
- MTU：设置数据包通过该接口的MTU值
- MAC地址：设置接口的MAC地址。

提示：

1、 ETH0 管理口的接口模式为路由口，不可更改接口模式，ETH0 口可以增加管理 IP 地址，但是默认的管理 IP 地址 10.254.254.254/24 不能删除。

2、 透明模式的组网中，连接内外网接口的连接类型有：access+access、access+trunk、trunk+trunk 三种方式，无论什么方式必须保证连接内外网的 VLAN ID 必须相同。

3、 无论设备工作在何种模式下，建议将接口加入安全区域，否则可能影响其它模块的使用

9.2.1.3 虚拟线路模式

功能描述：虚拟网线接口也是普通的交换接口，不需要配置 IP 地址，不支持路由转发，转发数据时，直接从虚拟网线配对的接口转发，虚拟网线对之间相当于一根网线。

配置路径：【网络配置】>【 接口配置】>【物理接口】

配置描述：进入点击【修改】页面，可查看虚拟线路模式下，接口各参数。如下图所示：

图21.修改物理接口-虚拟线路模式

参数说明：

- 接口类型：既决定了接口的模式，又决定了设备数据的转发功能。上图为“虚拟线路模式”，其中接口类型又分为：
  - 路由：此类型下的接口需要配置IP地址，并且该接口具有路由转发功能。
  - 透明：此接口相当于普通的交换接口，不需要配置 IP 地址，不支持路由转发，根据MAC 地址表转发数据。
  - 虚拟网线：此接口相当于普通的交换接口，不需要配置 IP 地址，不支持路由转发，转发数据时，直接从虚拟网线配对的接口转发。
  - 旁路镜像：连接到有镜像功能的交换机上，用于镜像流经交换机的数据。
- 基本属性：用于设置是否为WAN口。接口为外网接口需要勾选WAN口。否则将统计不到任何过改接口

的流量、会话和上网信息。

- 所属区域：选择接口所对应的区域。既可以在<所属区域>下拉框中新增，也可在【网络配置 >安全区域】中设置，上图为“虚拟外”安全区域。
- 接口二：选择形成一对虚拟网线的另外一个接口。如 eth1、eth3是一对虚拟网线接口，则接口二选择eth3，接口一就是当前接口。
- MTU：设置数据包通过该接口的MTU值。
- MAC地址：设置接口的MAC地址。

提示：

1、 ETH0 管理口的接口模式为路由口，不可更改接口模式，ETH0 口可以增加管理 IP 地址，但是默认的管理 IP 地址 10.254.254.254/24 不能删除。

2、 管理口不支持设置成虚拟网线接口，如果要设置 2 对或者 2 对以上虚拟网线，要求设备不少于 5 个接口，除了配置成虚拟网线接口，还必须预留一个专门的管理口。

3、 无论设备工作在何种模式下，建议将接口加入安全区域，否则可能影响其它模块的使用。

9.2.1.4 旁路镜像模式

功能描述：用于把设备接在交换机的镜像口或者接在 HUB 上，保证外网用户访问服务器的数据经过此交换机或者 HUB，并且设置镜像口的时候需要同时镜像上下行的数据，从而实现对服务器的保护。实现防护功能的同时，可以完全不需改变用户的网络环境，并且可以避免设备对用户网络造成中断的风险

配置路径：【网络配置】>【 接口配置】>【物理接口】

配置描述：进入点击【修改】页面，可查看旁路镜像模式下，接口各参数。如下图所示：

图22.修改物理接口-旁路镜像模式

参数说明：

- 接口类型：即决定了接口的模式，又决定了设备数据的转发功能。上图为“虚拟线路模式”，其中接口类型又分为：
  - 路由：此类型下的接口需要配置IP地址，并且该接口具有路由转发功能。
  - 透明：此接口相当于普通的交换接口，不需要配置 IP 地址，不支持路由转发，根据MAC 地址表转发数据。
  - 虚拟网线：此接口相当于普通的交换接口，不需要配置 IP 地址，不支持路由转发，转发数据时，直接从虚拟网线配对的接口转发。
  - 旁路镜像：连接到有镜像功能的交换机上，用于镜像流经交换机的数据。
- 基本属性：用于设置是否为WAN口。接口为外网接口需要勾选WAN口。否则将统计不到任何过改接口的流量、会话和上网信息。
- 所属区域：选择接口所对应的区域。既可以在<所属区域>下拉框中新增，也可在【网络配置 >安全区域】中设置，上图为“旁路镜像口”安全区域。
- 旁路流量统计：设置进行流量统计的参数。
- 工作模式：配置链路的工作模式。如：自动协商、全双工10M、全双工100M、全双工1G、全双工10G
- MTU：设置数据包通过该接口的MTU值
- MAC地址：设置接口的MAC地址。

提示：

1、 ETH0 管理口的接口模式为路由口，不可更改接口模式，ETH0 口可以增加管理 IP 地址，但是默认的管理 IP 地址 10.254.254.254/24 不能删除。

2、 无论设备工作在何种模式下，建议将接口加入安全区域，否则可能影响其它模块的使用。

9.2.1.5 链路健康检测

功能描述：检测链路的健康状态。

配置路径：【网络配置】>【接口配置】>【物理接口】

配置描述：

第一：进入【链路健康检查】页面，可以看到当前链路健康检测状态。如下图所示：

物理接口 修改状态

序号	接口名称	连接状态	接口类型	所属区域	WAN	连接类型	IP地址	工作速率	MTU	PING	链路状态	状态	MAC	操作
1	eth0 管理端口		路由	三层外网	是	静态IPv4/静态IPv6	172.16.16.18/16 10.254.254.254/24 fe80::290:fbff:fe50:2a3a/64	100Mb/s	1500	允许	正常	☑	00:90:fb:50:06:8c	修改
2	eth1		路由	未选择区域	否	静态IPv4/静态IPv6			1500	不允许	断开	☑	00:90:fb:50:06:8d	修改
3	eth2		路由	未选择区域	否	静态IPv4/静态IPv6	100.40.0.2/24		1500	允许	未检测	☑	00:90:fb:50:06:8e	修改
4	eth3		虚拟线路	未选择区域	否	---	---		1500	---	未检测	☑	00:90:fb:50:06:8f	修改
5	eth4		透明	二层内网	否	Access/access:2	---	1000Mb/s	1500	---	未检测	☑	00:90:fb:50:06:90	修改
6	eth5		透明	二层外网	是	Access/access:2	---	1000Mb/s	1500	---	未检测	☑	00:90:fb:50:2a:3f	修改

图23.链路健康检查

第二：进入点击【修改】>【设置】按钮，设置链路健康检测参数。如下图：

图24.设置链路健康检查

参数说明：

- 网关：ISP提供的网关IP地址。
- 侦测目标：侦测的目标对象。可使用 Ping、DNS、TCP 三种方式进行检测。
- 侦测间隔：向侦测目标发送侦测报文的时间间隔，默认为3s。
- 重试次数：当侦测目标没有回应时，需要重新发送侦测报文，重新发送的次数。如果每次都没有收到侦测目标的回应，则认为这条链路失效。在重试次数范围内收到了侦测目标的回应，则认为这条链路为健康状态。
- 状态：启用会禁用本条规则。

第三：进入点击【修改】>【查看链路详情】按钮，查看链路健康检测参数。如下图：

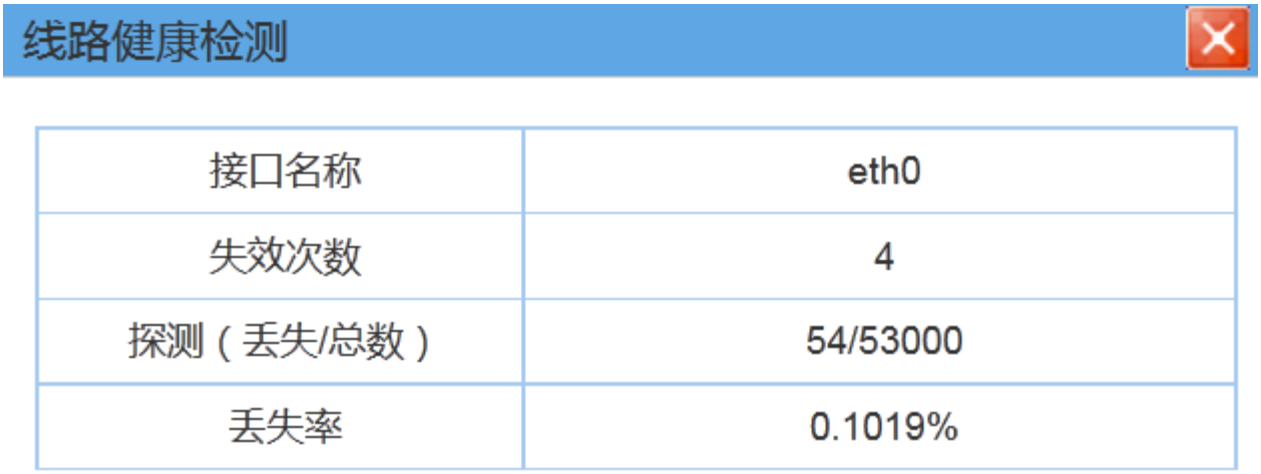


图25.线路健康检测详情

参数说明：

- 接口名称：进行链路健康检测的接口，如eth0。
- 失效次数：统计链路检测失败的次数。
- 探测： 统计“丢失/总数”的值。
- 丢失率： 根据“丢失/总数”的值，结算出链路检测过程中的丢失率。

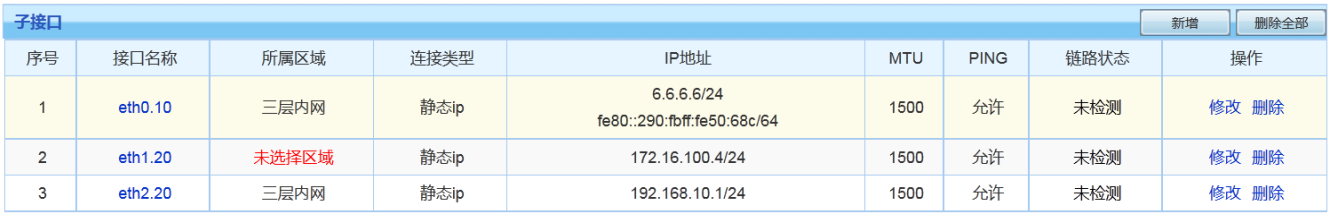
9.2.2 子接口

功能描述：子接口用于配置物理接口是路由接口，并且该路由接口需要启用 VLAN trunk 的场景，设备支持连接二层交换机的 TRUNK 口。

配置路径：【网络配置】>【 接口配置】>【子接口】

配置描述：

第一：点击进入【子接口】界面，可以看到当前已经建立的VLAN接口。如下图：



序号	接口名称	所属区域	连接类型	IP地址	MTU	PING	链路状态	操作
1	eth0.10	三层内网	静态ip	6.6.6.6/24 fe80::290:fbff:fe50:68c/64	1500	允许	未检测	修改 删除
2	eth1.20	未选择区域	静态ip	172.16.100.4/24	1500	允许	未检测	修改 删除
3	eth2.20	三层内网	静态ip	192.168.10.1/24	1500	允许	未检测	修改 删除

图26. 子接口

按钮说明：

点击<接口名称>，可以修改本子接口的参数，但不能修改物理接口和VLAN ID。接口名称是根据VLAN ID自动生成，且不可修改。

点击<删除全部>，将删除所有子接口。

点击<新增>， 增加子接口

点击<删除>，删除本子接口

点击<修改>，修改本子接口的参数，但不能修改物理接口和VLAN ID。

第二：点击进入<新增>界面，新增子接口，如下图所示：

图27.新增子接口

参数说明：

- 物理接口：选择添加子接口的物理接口，且物理接口只能是路由口。
- VLAN ID：设置VLAN ID。物理接口需要加入哪个 VLAN，就填写对应的 VLAN ID 即可。
- 所属区域：选择子接口所对应的区域。既可以在<所属区域>下拉框中新增，也可在【网络配置 >安全区域】。
- 基本属性：选择是否允许 PING 子接口。
- IP地址：有静态 IP、DHCP ，根据该线路的需要进行配置。
- 如果选择静态IP，要手动添加IP地址/掩码以及下一跳网关（ 可以不添加）
- 如果该接口是DHCP自动获得地址则设置DHCP参数；
- MTU: 设置数据包通过该接口的MTU值
- 链路健康检测：用于检测链路的连通性。配置详情查看【网络配置 >安全区域>物理接口>链路健康检测】。

第二：点击进入<修改>界面，修改子接口，如下图所示：

图28.修改子接口

新增子接口时由于子接口所在链路未确定，所以没有“链路健康检测”模块，要想检测子接口链路状态，修进入“修改子接口”设置相关参数。

9.3路由设置

路由设置包括静态路由和策略路由两部分。

9.3.1 静态路由

功能描述：根据组网需要合理添加静态路由。

配置路径：【网络配置】>【路由设置】>【静态路由】

配置描述：

第一：进入【静态路由】页面，如下图：

序号	目的网段	类型	网关	接口	状态	度量值	操作
1	10.254.254.0/24	直连	10.254.254.254	eth0	有效	0	修改 删除
2	100.40.0.0/24	直连	100.40.0.1	eth2	有效	0	修改 删除
3	172.16.0.0/16	直连	172.16.16.100	eth0	有效	0	修改 删除
4	0.0.0.0/0.0.0.0	静态	172.16.161.100	eth0	有效	0	修改 删除

图29.静态路由

按钮说明：

点击<删除全部>，将删除所有子接口。

点击<新增>， 增加子接口

点击<删除>，删除本子接口

点击<修改>，修改本子接口的参数，但不能修改物理接口和VLAN ID。

第二：进入点击<新增>按钮，增加静态路由。如下图：

图30.新增单个静态路由

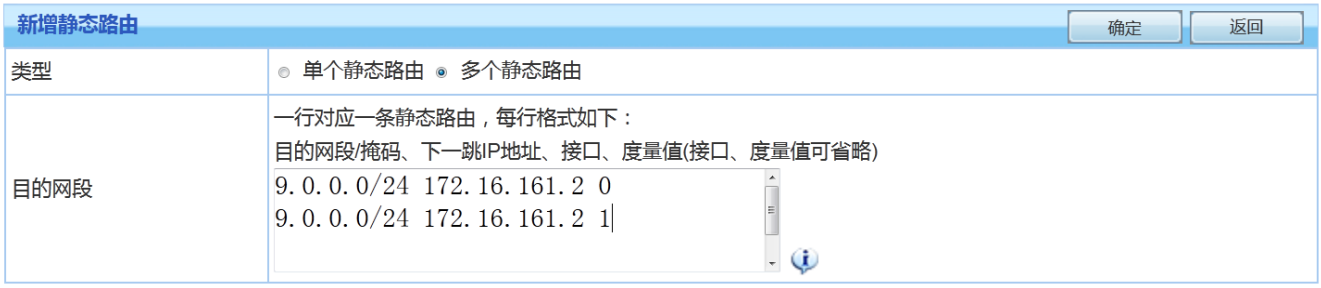


图31.新增多个静态路由

参数说明：

- 类型：选择新增静态路由的方式，即新增单个静态路由或新增多个静态路由。
- 目的网段：到达的目标网络号。
  - 如果选择单个静态路由，则配置格式为目的网段/掩码的方式，如：10.0.0.0/16或10.0.0.0/255.255.0.0。
  - 如果选择多个静态路由，则配置格式为：目的网段/掩码、下一跳IP地址、接口、度量值（接口、度量值可省略）的方式，如：9.0.0.0/24　172.16.161.2　eth0　0。
- 下一跳IP地址：达到目标网络的下一跳地址
- 接口：选择从设备哪个接口转发数据包的接口。
- 度量值：设置本条静态路由的度量值。

提示：

1、直连路由不可以修改和删除。

2、静态路由选择的接口，一般情况下建议设置“自动选择”。

9.3.2 策略路由

策略路由又包含策略路由、均衡策略、持续路由三部分

9.3.2.1 策略路由

功能描述：主要用于设备有多个外网口接多条外网线路时，根据源/目的 IP、源/目的端口、协议等条件进

行出接口和线路选择，以实现不同的数据走不同的外网线路的自动选路功能。

配置路径：【网络配置】>【路由设置】>【策略路由】>【策略路由】

配置描述：

第一：进入【策略路由】页面，可以看到当前配置的策略路由。如下图所示：

图32.策略路由

策略路由的优先级：序号越小的优先级越高，可通过<插入>和<移动>来改变路由的优先级。新增的策略路由放于最后。

按钮说明：

点击<新增>，增加策略路由

点击<修改状态>,在已策略路由列表里，改变“状态”列复选框的值，然后再点击“修改状态”按钮，则可改变某条(些) 表示本条策略路由是启用(有效)的；状态列对应的复选框如果为“不勾选”状态，则表示本条策略路由是禁用(无效)的。

点击<删除所有>,删除所有策略路由。

点击<计数清零>，将匹配计数栏中的计数归零。

点击<修改>,修改某条策略路由。

点击<插入>,在本条路由之前插入一条路由。

点击<移动>,移动某条路由到其他路由之前或之后，以改变路由的优先级。

点击<删除>,删除某条策略路由。

第二：进入点击<新增>按钮，增加策略路由。如下图：

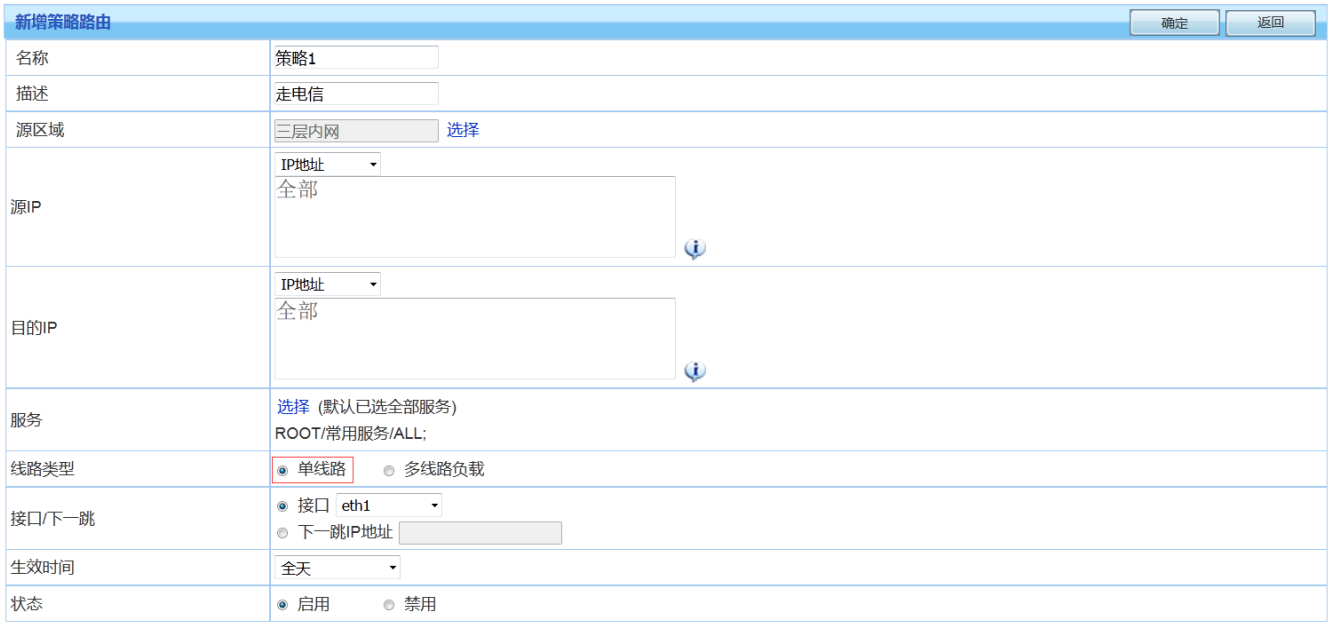


图33.新增策略路由-单线路

图34.新增策略路由-多线路

参数说明：

- 名称：设置策略路由的名称 。
- 描述：设置策略路由的描述信息。
- 源区域：选择源区域，须选择源区域。
- 源IP：匹配报文的源地址，可以选择为IP组或者输入IP地址。输入IP地址的格式范例：192.168.1.1、192.168.1.5-192.168.1.9、192.168.0.0/16 或 192.168.0.0/255.255.0.0。
- 目的IP：匹配报文的目的地址，可以输入多个地址。

- ✧ 如果类型为“IP“，则格式范例为：192.168.1.1、192.168.1.5-192.168.1.9、192.168.0.0/16 或 192.168.0.0/255.255.0.0。
- ✧ 如果类型选择为“ISP自动地址表”，表示自动根据各 ISP 厂商的地址表来选路，后面会出现一个下拉框，下拉框的值为：电信、移动、联通、铁通、网通。
- ✧ 若果类型选择为“IP组”, 既可以在IP组快速链接中新增，也可以在【系统对象>IP组】中添加。

- 服务：选择匹配报文的四层服务。有常用服务和自定义普通服务。
- 链路类型：选择单线路或多线路负载。
  - ✧ 单线路：用于固定指派某条链路，选路规则并不参考均衡策略。如：用户需要访问一个网上银行，地址是 127.8.66.42，访问协议是 HTTPS，网上银行会校验连入的 IP 地址， 如果同一连接中的源 IP 发生了改变， 网上银行会断开链接，导致无法访问。因此，可以设置一条测略路由，指定访问到这个目标地址的数据固定走WAN1的线路出去。
  - ✧ 多线路：参考均衡策略的选路规则，选择报文走哪条链路。如：某用户有 2 条外网线路，分别是 2M 和 10M 的电信线路，用户希望实现内网用户访问公网的时候自动选择流量最小的链路。

    因此可以添加一条限制流量的均衡策略，在策略路由中引用。
- 均衡策略 ：择均衡策略；均衡策略的详细配置和说明见“均衡策略”一节。
- 接口/下一跳：选择符合条件的数据报从哪个接口或者下一跳进行转发。
- 生效时间：默认全天，也可在【系统对象>时间计划】自定义时间计划。
- 状态：启用或禁用。启用后表示此条路由有效，禁用后表示此条路由无效。

提示：

1、 策略路由只能选择 WAN 口属性的路由接口

2、 只有静态路由中有缺省路由存在，策略路由才生效

9.3.2.2 均衡策略

功能描述：配置均衡策略。

配置路径：【网络配置】>【路由设置】>【策略路由】>【策略路由】

配置描述：

第一：进入【均衡策略】页面，可以看到当前配置的均衡策略。如下图所示：

图35.均衡策略

按钮说明：

点击<删除全部>，将删除所有未被策略路由调用的均衡策略 。

点击<计数清零>，将把所有生效策略的匹配计数归零。

点击<新增>， 增加均衡策略

点击<删除>，删除本挑均衡策略

点击<修改>，修改本均衡策略的相关参数

第二：进入点击<新增>按钮，增加策略路由。如下图：

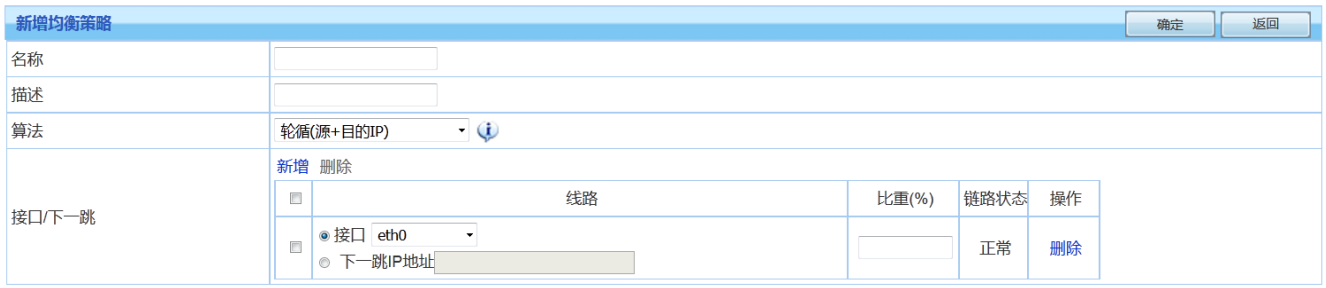


图36. 新增均衡策略

参数说明：

- 名称：均衡策略名称。
- 算法：均衡策略算法，共 7种算法，分别如下：
  - 轮询（源IP+目的IP）：按照源IP+目的IP的组合和比重值进行轮询。
  - 轮询（源IP）：按照源IP和比重值进行轮询。
  - 上行流量：根据链路的上行流量所占的比重，进行计算选路。
  - 下行流量：根据链路的下行流量所占的比重，进行计算选路。
  - 总流量(上行+下行)：根据链路的上行+下行流量之和所占的比重，进行计算选路。
  - 最佳路径：根据对端设备响应时间，进行选路，对端设备响应时间最小者为最佳路径

- ✧ 优先使用前面的线路：用于线路需要做主备的场景，则所有连接均分配到第一条线路，如果第一条线路故障，才把连接切换到第二条选择的可用线路。

➢ 接口/下一跳：出口网关地址。可以点击“新增”按钮，新增接口/下一跳，最多可增加八条。算法不同，对应的接口/下一跳的配置页面不同。

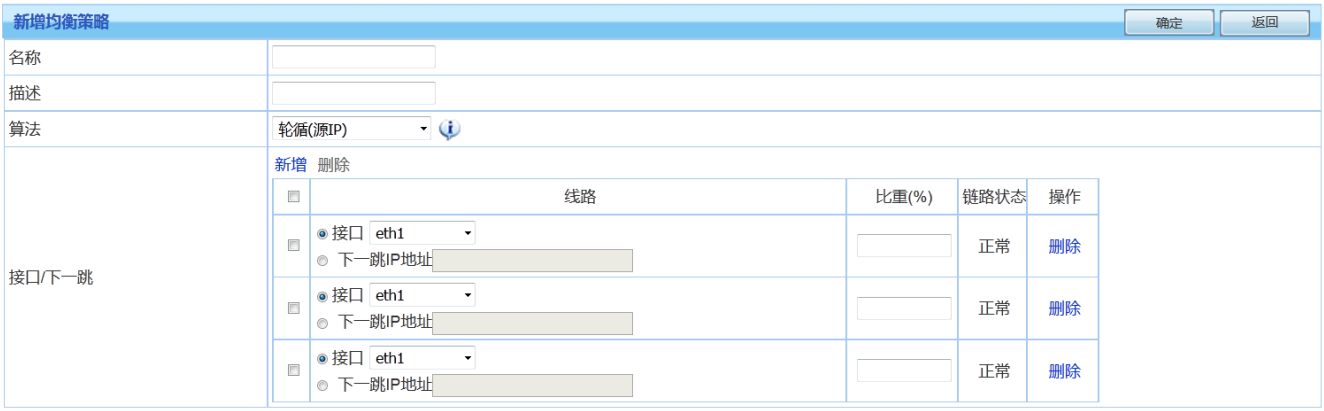


图37.新增均衡策略-轮询(源 IP)

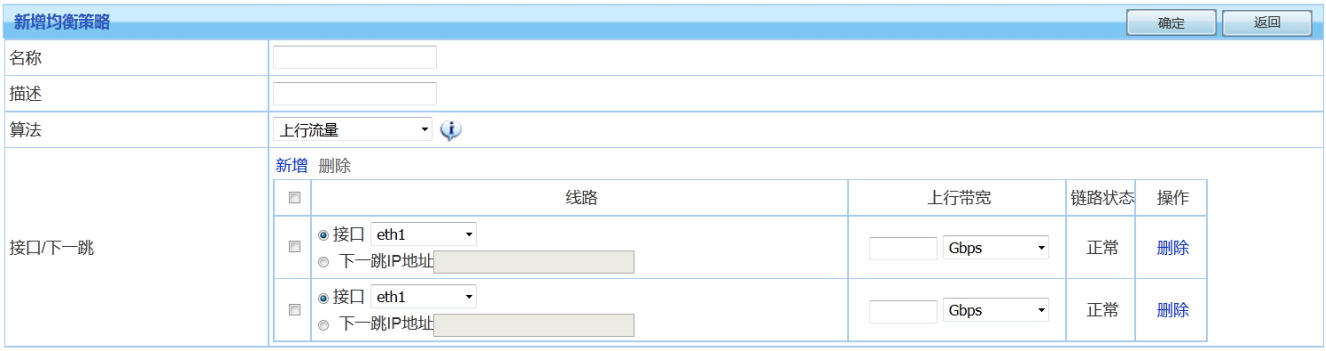


图38.新增均衡策略-上行流量

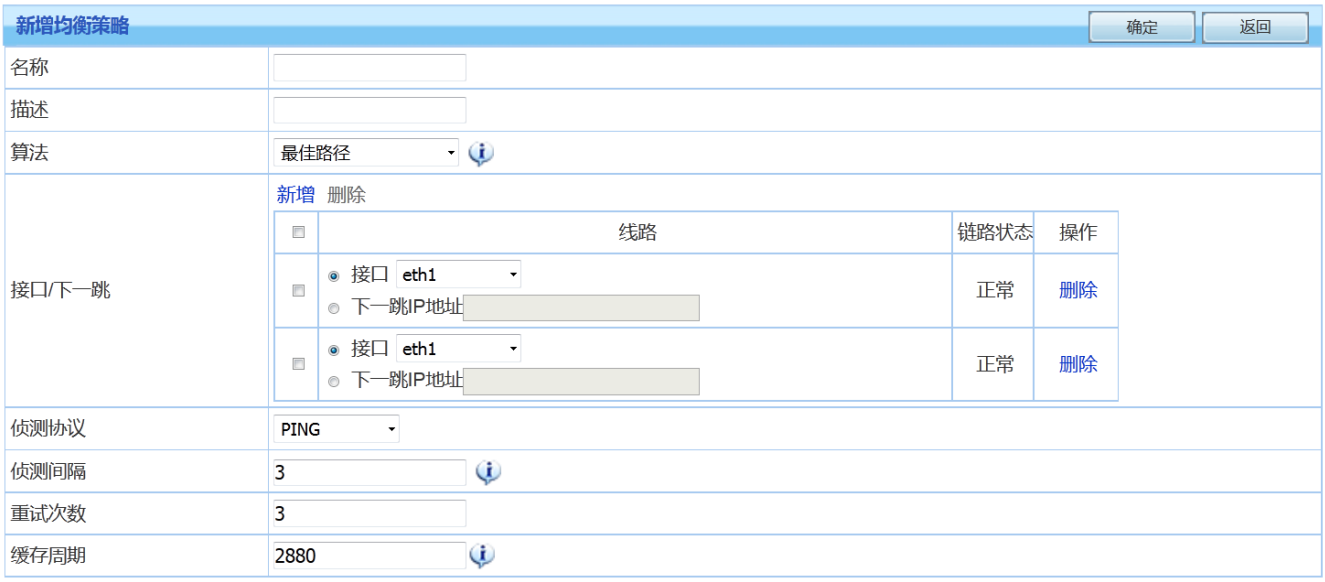


图39.新增均衡策略-最佳路径

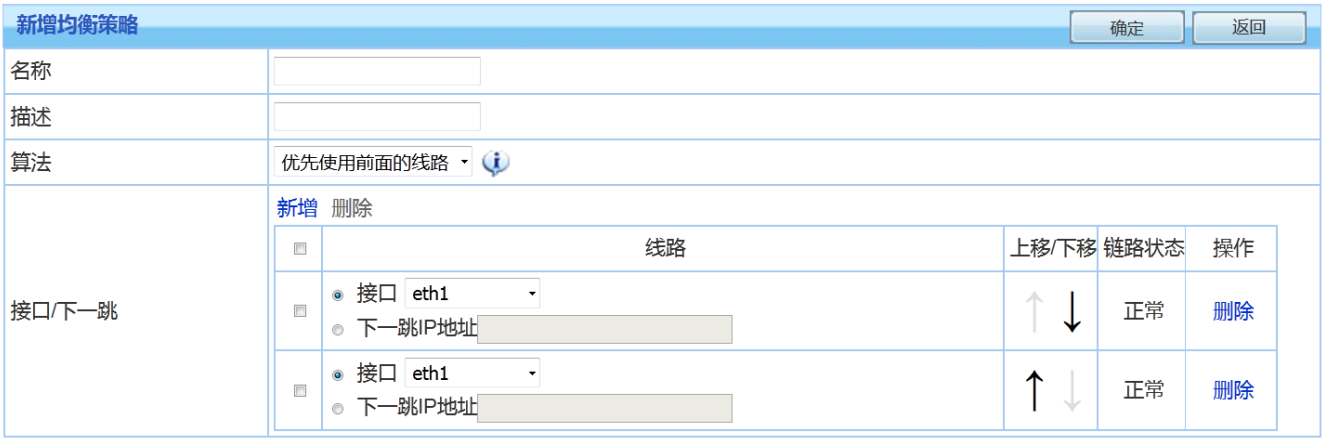


图40.新增均衡策略-优先使用前面的线路

9.3.2.3 持续路由

功能描述：指当要建立连接时，首先依照“均衡策略”设定的算法进行选路。当决定使用某条链路后，再参考“持续路由”设定的规则，决定是否固定使用这条链路。

配置路径：【网络配置】>【路由设置】>【策略路由】>【持续路由】

配置描述：

第一：进入【持续路由】页面，可以看到当前配置的持续路由规则。如下图所示：

图41.持续路由

超时时间：固定使用某条链路的最大等待时间，默认为 60 秒。根据“均衡策略”选定使用某条链路后，并且“持续路由”规则决定要固定使用这条链路，但在 60 秒内都没有报文再次使用这条“持续路由”规则进行选路，则新的报文再次选路时，需要首先依照“均衡策略”设定的算法进行重新选路，再参考“持续路由”设定的规则决定是否固定使用那条链路。

第二：进入点击<新增>按钮，增加持续路由规则。如下图：

图42. 新增持续路由

参数说明：

- 名称：持续路由规则的名称。
- 源地址：匹配报文的源地址，可以选择为IP组或者输入IP地址。输入IP地址的格式范例：192.168.1.1、192.168.1.5-192.168.1.9、192.168.0.0/16 或 192.168.0.0/255.255.0.0。
- 目的地址：匹配报文的目的地址，可以选择为IP组入IP地址。输入IP地址的格式范例：192.168.1.1、192.168.1.5-192.168.1.9、192.168.0.0/16 或 192.168.0.0/255.255.0.0。
- 动作：选择为“使用持续路由”或“不使用持续路由”。
- 状态：选择“启用”或“禁用”该条策略

9.4DNS 配置

功能描述：配置设备的 DNS 服务器、DNS 代理、DNS 缓存。

配置路径：【网络配置】>【DNS 配置】

配置描述：进入【DNS 配置】页面，配置 DNS 服务器。如下图所示：

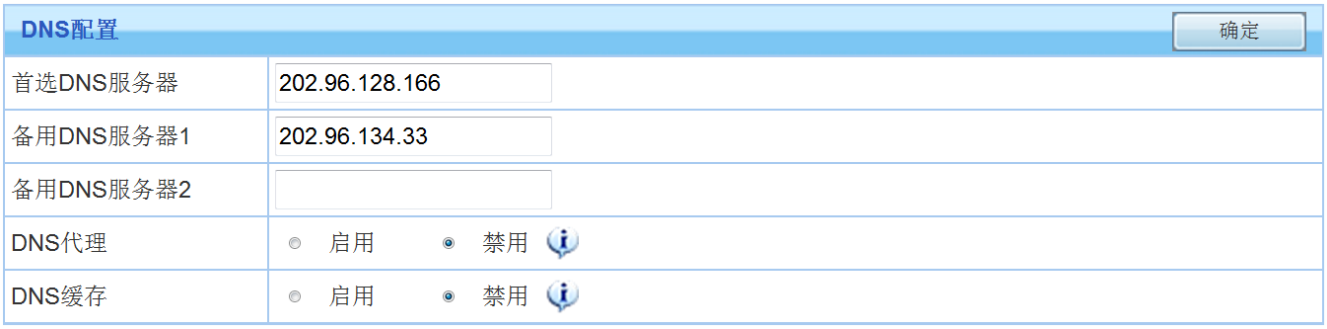


图43.DNS 配置

参数说明：

- 首选 DNS 服务器/备份 DNS 服务1/备份 DNS 服务2：配置设备的 DNS 服务器的 IP 地址。

- DNS 代理：内网的 DNS 代理功能。内网主机的 DNS 服务器必须配置为设备连接内网的 LAN 口的 IP 地址。
- DNS 缓存：内网的 DNS 缓存器。内网主机无需修改 DNS 服务器的配置，设备作为 DNS 透明代理，缓存 DNS 记录。比如，当第一个用户请求 Google 的 DNS 解析，设备将 Google 的 DNS 记录缓存到设备，第二个用户再请求 Google 的 DNS 解析时，设备直接返回给用户，不必再到 DNS服务器去请求。

9.5DDNS 配置

功能描述：DDNS可以捕获用户每次变化的IP地址，然后将其与域名相对应，这样其他上网用户就可以通过域名来访问。

配置路径：【网络配置】>【DDNS 配置】

配置描述：进入【DDNS 配置】页面，配置 DNS 服务器。如下图所示：

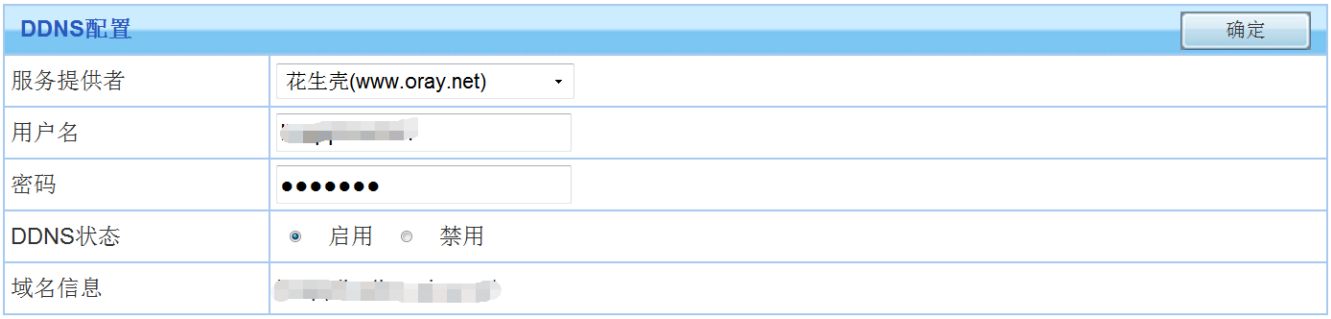


图44.DDNS 配置

参数说明：

- 服务提供者：提供 DDNS 服务的服务器域名，可选择为[花生壳(www.oray.net)] 或 [DynDns(www.dyndns.com)]。
- 用户名：在 DDNS 服务商那里注册的用户名。
- 密码：在 DDNS 服务商那里注册的用户名对应的密码。
- DDNS 状态：当前 DDNS 的工作状态。
- 域名信息：为本用户名分配的域名，以后不论 IP 地址如何变化，则会自动对应到该域名信息。

提示：首先需要在 DDNS 服务商那里注册一个可用的用户名，然后 DDNS 服务就会为该用户名分配一个域名。当启用 DDNS 功能后，DDNS 服务会将动态变化的 IP 对应到该域名。

9.6DHCP 配置

9.6.1 基本参数

功能描述：配置DHCP基本参数。

配置路径：【网络配置】>【DHCP配置】>【基本参数】

配置描述：

第一：进入【基本参数】页面，可以看到当前已建立的 DHCP 配置。如下图：

基本参数 新增

序号	接口名称	网关/子网掩码	IP地址池	DNS服务器	租用期限	状态	操作
1	eth3	172.16.161.2/255.255.0.0 192.168.100.1/255.255.255.0	172.16.0.10-172.16.0.50 192.168.100.4- 192.168.100.50	202.96.134.133, 8.8.8.8 8.8.8.8	3日 3日	启用	修改 删除

图45.DHCP 基本参数

第二：进入点击<新增>按钮，增加 DHCP 配置。如下图：

新增DHCP基本参数 确定 返回

接口名称	eth3		
组1	网关IP	172.16.161.2	（第一组必须与接口首IP同网段,一般为接口IP,其它组可以为DHCP中继服务）
	子网掩码	16	(必填，格式范例: 24或255.255.255.0)
	首选DNS服务器	202.96.134.133	(必填)
	备用DNS服务器	8.8.8.87	
	IP地址池	172. 16. 161. 20-172. 16. 161. 40	(必填)
	固定IP		
	租用期限	永不过期 3 日 0 时 0 分	

新增组

图46.新增 DHCP 参数

参数说明：

- 接口名称：选择启用 DHCP 服务的接口名称。
- 网关IP：第一组必须为接口同网段IP,一般为接口IP,其它组可以为DHCP中继服务。
- 子网掩码：配置 DHCP 客户端所获得的 IP 地址的掩码。
- 首选 DNS 服务器/备用 DNS 服务器：配置 DHCP 客户端所获得的 DNS 配置信息。
- IP 地址池：配置 DHCP 客户端所获得的 IP 地址的范围。一行一个地址，格式范例：192.168.2.2 或 192.16.2.2-192.168.2.253。地址范围必须与接口地址同网段，多个范围间地址不能重叠。
- 固定 IP ：可根据 MAC 绑定 IP， 即根据 MAC 地址把固定的 IP 地址分配给对应的客户端。一行一个固定 IP，固定 IP 的地址不能在 IP 地址池范围内，名称不能为中文。格式范例：名称/IP/MAC, 如 :Tom/192.168.1.1/00:19:21:3f:a1:11。
- 租用期限：设置 DHCP 获得的 IP 地址的有效期，默认为永远有效。
- 新增组：和第一组配置完全一致，用于跨网段获得IP，即FW下有开启DHCP中继的三层设备。

提示：

1、 配置 IP 地址池时，一行一个地址范围，起始地址与结束地址间以英文中线(-)隔开。

2、 地址范围必须与网关接口地址同网段，不要包含网络地址及网段广播地址、网关 IP 地址，多个范围间地址不能重叠。

3、 固定 IP 地址不能包含在 IP 地址池中。

4、 只有路由模式的接口可以启用 DHCP。

9.6.2 DHCP 中继

功能描述：用于 DHCP 服务器与 DHCP 客户端 IP 在不同 IP 网段的应用场景,FW作为连接DHCP服务器和DHCP客户端中间的设备。

配置路径：【网络配置】>【DHCP配置】>【基本参数】

配置描述：进入【DHCP中继】页面，可以看到配置页面，如下图：

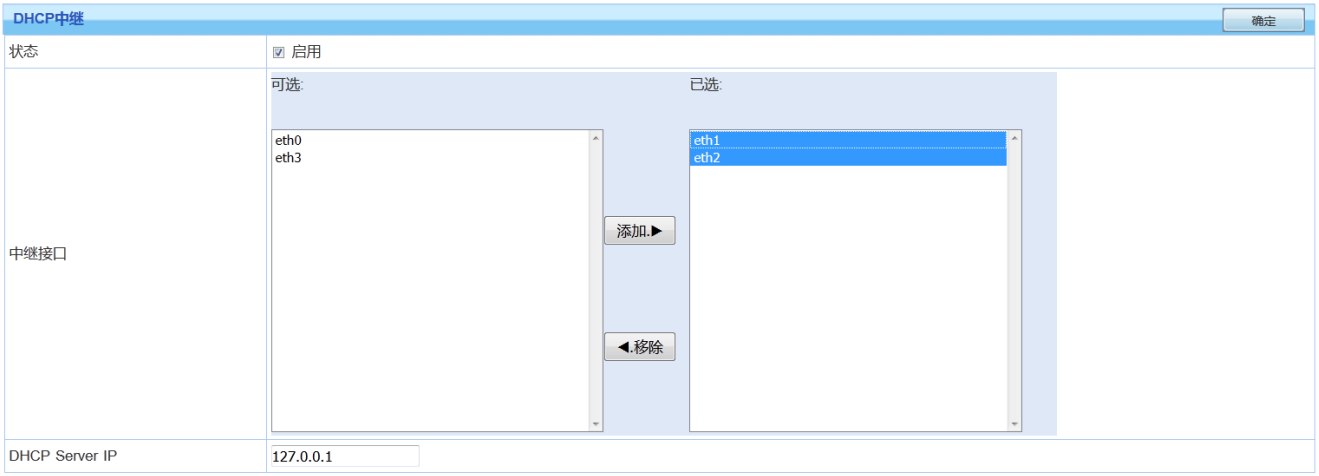


图47.DHCP 中继

参数说明：

- 状态：选择启用或禁用DHCP中继， 代表启用。
- 中继接口：选择开启DHCP中继的接口，可通过<添加>,<移除>按钮添加和删除接口。
- DHCP 服务器：配置DHCP服务器的IP地址。

提示：

1、 配置 DHCP 中继时，必须保证 dhcp 中继和 dhcp 服务器互通。

2、 必须将连接 DHCP 客户端和连接 DHCP 服务器的接口都添加到中继接口中，若上图 eth1 和 eth2。

3、 只有路由模式的接口可以启用 DHCP 中继。

9.6.3 已分配 IP

显示当前 DHCP 分配的 IP 总数，所分配的 IP 地址、计算机名称、MAC 地址及分配的 IP 地址到期时间。

9.7ARP 表

功能描述：查看ARP表，配置静态ARP。

配置路径：【网络配置】>【ARP表】

配置描述：

第一：进入【ARP表】页面，可查看到当前ARP。如下图：

ARP表

转为静态 | 新增 | 删除所有

序号	IP地址	MAC地址	物理接口	类型	静态	操作
1	172.16.7.20	8c:89:a5:74:0a:74	eth3	动态		删除
2	172.16.16.18	00:90:fb:50:06:8c	eth3	动态		删除
3	172.16.0.177	f0:92:1c:55:b2:fb	eth3	动态		删除
4	172.16.161.65	28:80:23:c0:a7:ee	eth3	动态		删除

图48.ARP 表

类型为“动态”代表自动学习到的 ARP 条目；为“静态”代表将固定的 IP 和 MAC 绑定在一起。

第二：当选“静态”列的复选框，再点击<转为静态>，可以将动态学习到的 ARP转换为静态ARP。当类型为“静态”时，对应ARP条目的“静态”列的复选框消失。勾选表头的“静态”复选框，可以选中所有的动态ARP条目。

第三：点击<新增>按钮，可添加静态ARP条目，如下图：

新增静态ARP

确定 | 返回

IP地址	192.168.0.3
MAC地址	00:00:DB:1a:23:2A

图49.新增静态 ARP

10 防火墙

防火墙包括安全策略、NAT 规则、DOS/DDOS 防护、ARP 欺骗防护、应用层网关、加速老化等六部分。

10.1 安全策略

功能描述：安全策略定义了对数据流的控制规则；可以通过指定报文的源地址、目的地址、服务、时间段等

参数来控制信息流。安全策略的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，所以同一组策略中，序号小的优先级高。

配置路径：【防火墙】>【安全策略】

配置描述：

第一：进入【防火墙】页面，可以查看当前安全策略，如下图：

图50.安全策略

按钮说明：

点击<新增>，新增安全策略。

点击<计数清零>，将策略列表中的所有匹配计数归零。

点击<删除所有>，将删除所有的安全策略。

点击<删除本组>，将删除本组的安全策略，如删除 ALL→ALL 的所有安全策略。

点击<删除>，删除本条安全策略。

点击<修改>，修改本条安全策略的参数，但不能修改本条安全策略的方向。

点击<插入>，在当前位置之前插入一条安全策略。

点击<移动>，改变对应安全策略的序号，从而改变安全策略的优先级。

改变状态栏复选框的值，再点击<修改状态>，可修改安全策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有安全策略的状态。

第二：点击<新增>按钮，新增安全策略，如下图：

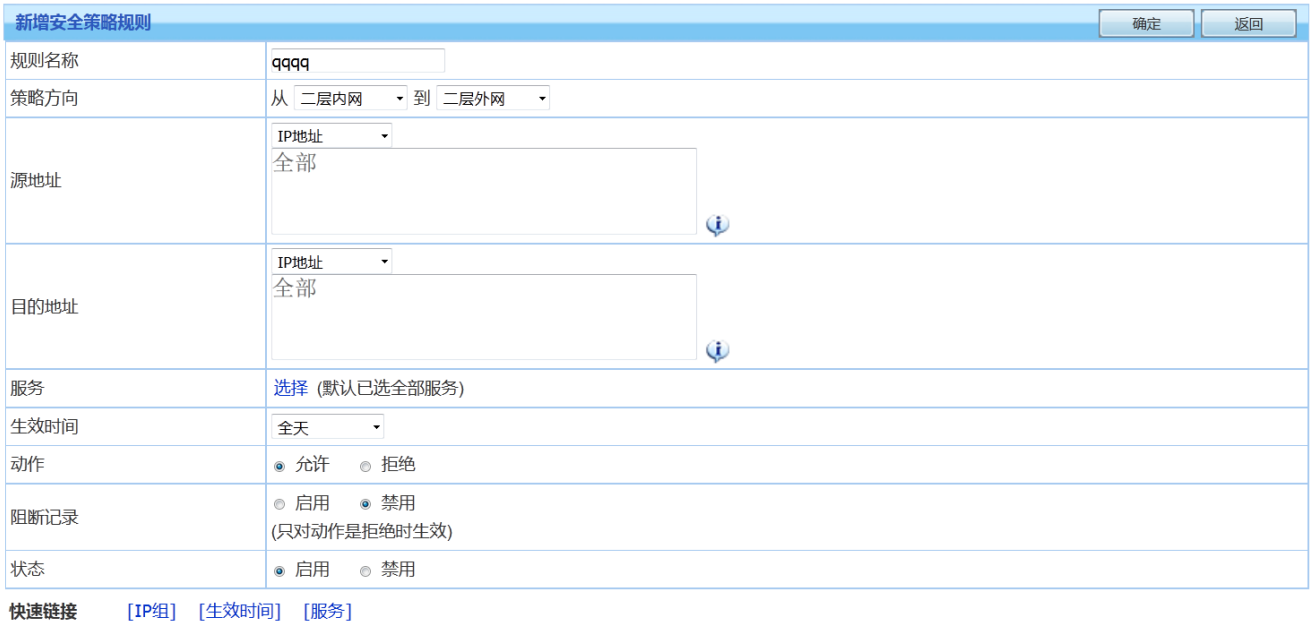


图51.新增安全策略

参数说明：

- 规则名称：设置安全策略的名称。
- 策略方向：代表数据流的方向。如从二层内网区域到二层外网区域。
- 源地址：数据流的源地址，可输入IP地址、选择IP组或选择用户及用户组。IP组可以快速连接中设置IP组，也可在【系统对象>IP组】中配置。
- 目的地址：数据流的目的地址，可输入IP地址、选择IP组或选择用户及用户组。
- 服务：数据流的服务类型。默认选择全部。
- 生效时间：默认为全天，可在快速链接中自定义时间，也可在【系统对象>时间计划】自定义时间计划。
- 动作：安全策略允许、拒绝服务的动作。
- 阻挡记录：启用后可将阻挡信息以日志的形式，记录在阻挡记录中。
- 状态：启用或禁用本规则，默认启用。

提示：

1、 策略规则遵循从按顺序从前往后匹配的原则，如果一个规则匹配了，就不会再向下匹配，所以序号小的规则优先级高。请注意规则的先后顺序，先定义的规则，位置排在前面，可通过<插入>或<移动>来改变规则的先后顺序。

2、 系统默认添加了一条**拒绝**所有的安全策略，以保证网络的安全性，且不能修改、移动和删除。因此，无论客户端以什么模式连接外网，需放通区域间的流量，否则将影响彼此间的通信。

10.2 NAT 规则

功能描述：“NAT 规则”有三种 NAT 转换方式，包括：源地址转换、目的地址转换、双向地址装换。用于路

由模式下的组网环境中，在透明模式、虚拟线路、旁路镜像模式下均不可适用。

配置路径：【防火墙】>【NAT规则】

配置描述：进入【NAT规则】页面，可以查看当前NAT规则策略，如下图：

NAT规则　　新增　修改状态　删除全部　计数清零

序号	名称	转换类型	原始数据包							转换后数据包			匹配计数	状态	操作
			源区域	目的区域/接口	源IP	目的IP	协议	源端口	目的端口	源IP	目的IP	目的端口			
1	内网代理	源地址转换	三层内网	三层外网	全部	全部	所有协议	所有端口	所有端口	出接口地址	-	不转换	1339386	☑	修改 复制 插入 移动 删除
2	vpn代理	源地址转换	PPTP-VPN	三层外网	全部	全部	所有协议	所有端口	所有端口	出接口地址	-	不转换	327	☑	修改 复制 插入 移动 删除
3	.18	目的地址转换	三层外网	/	全部	接口地址	TCP	所有端口	9090	-	172.16.16.18	不转换	6	☑	修改 复制 插入 移动 删除
4	pptp	源地址转换	PPTP-VPN	三层外网	全部	全部	所有协议	所有端口	所有端口	出接口地址	-	不转换	0	☑	修改 复制 插入 移动 删除

图52.NAT 规则

按钮说明：

点击<新增>，新增NAT规则。

点击<计数清零>，将NAT规则列表中的所有匹配计数归零。

点击<删除所有>，将删除所有的NAT规则。

点击<删除>，删除本条NAT规则。

点击<复制>，在本策略前产生一条策略。

点击<修改>，修改本条安全策略的参数，但不能修改本条安全策略的方向。

点击<插入>，在当前位置之前插入一条安全策略。

点击<移动>，改变对应安全策略的序号，从而改变安全策略的优先级。

改变状态栏复选框的值，再点击<修改状态>，可修改安全策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有安全策略的状态。

NAT规则的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，所以序号小的优先级高。

10.2.1 源地址转换

功能描述：用于将符合条件的数据进行源 IP 地址转换，最常用的是设备部署在公网出口时，代理内网用户上网，需要设置源地址转换规则进行源地址转换。内部网络的所有主机均可共享一个或者多个合法外部 IP 地址实现对 Internet 的访问。

配置路径：【防火墙】>【NAT规则】> 【新增】

配置描述：

第一：进入新增进入【NAT规则】页面，如下图：

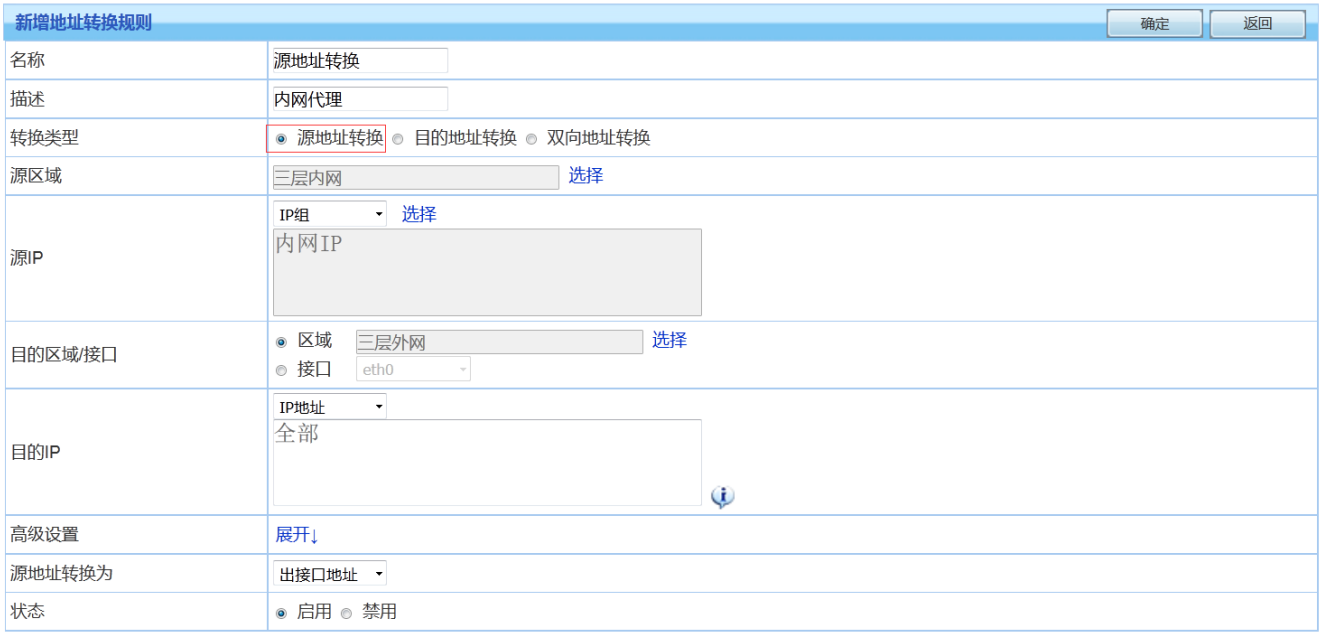


图53.新增 NAT 规则-源地址转换

参数说明：

- 名称：设置设置NAT转换的名称。
- 描述：设置规则的描述信息。
- 转换类型： 选择规则的转换类型。此处为源地址转换。
- 源区域或源IP： 用于设置需要进行源地址转换时匹配此条规则的源 IP 条件， 只有来自指定的源区域和指定 IP或IP 组的数据才会匹配该规则、进行源地址转换。如路由接口代理内网上网，则一般配置源区域为内网、源 IP 组为内网 IP 网段，或者全部。
- 目的区域/接口：用于设置匹配条件的数据，数据到哪个目标区域或者从哪个接口出去的数据才匹配该规则。如路由接口代理内网上网， 则一般配置目标区域为公网、若选择接口即为连接公网的接口。
- 目的IP: 用于设置匹配条件的数据，数据到哪个目标区域、访问哪些目标IP或IP组才匹配该规则。如路由接口代理内网上网，则一般配置目标IP或IP组为全部
- 高级设置：用于设置需要符合指定的协议、源端口、目标端口的数据才进行源地址转换，则可以定义这部分。
- 源地址转换为：设置当源地址、目标地址、协议等条件都匹配的数据，进行 IP 地址转换时，将源 IP 转换为哪个IP 地址。可以选择防火墙接口的出接口地址、某一段或单个IP地址、IP组或不转换。
- 状态：设置该策略启用或禁用。

提示：

1、 源地址转换只能用于路由模式下的组网环境。

2、 当源地址转换为的接口有多个IP时，不能选择出接口地址，否则转换不成功。

3、 IP 组除了在对象定义中添加外，还可以直接在转换规则的选择框中新增。

10.2.2 目的地址转换

功能描述：用于对经过设备的数据做目标地址转换。相当于端口映射、IP地址映射，通过将内网服务器的服务映射到公网，使 Internet 用户通过访问防火墙上的公网IP 访问到内网服务器。如：客户内网有一台 WEB 服务器 172.16.1.100 的 80 端口提供服务 。客户希望外网用户输入 http://1.2.1.1:666 访问到内网 172.16.1.100 服务器。此处就需要使用目的地址转换规则来实现。

配置路径：【防火墙】>【NAT规则】> 【新增】

配置描述：

第一：进入新增 NAT规则】页面，如下图：

图54.新增 NAT 规则-目的地址转换

参数说明：

- 名称：设置设置NAT转换的名称。
- 描述：设置规则的描述信息。
- 转换类型： 选择规则的转换类型。此处为目的地址转换。
- 源区域：指明从哪个区域进入的数据才进行目标地址转换，如上图：发布内网服务器到公网时，允许来自公网的用户对内网服务器（172.6.1.100）的访问，设置源区域为“三层外网”。
- 目的IP: 指明公网用户访问哪个地址的时候，才进行目标地址转换。目的IP 是数据包目的地址转换之前用户访问的地址，一般是设备自身接口的公网 IP。 如上图IP：1.2.1.1。
- 协议及端口：设置进行目的地址转换的协议以及目的端口。如：上图中协议类型需要选择TCP，因为 HTTP 服务 80 端口属于 TCP 协议。目的端口指定为666。
- 高级设置：用于设置需要符合指定的协议、源端口、目标端口的数据才进行源地址转换，则可以定义这部分。

- 目的地址转换为：指明将目的地址转换为什么地址。如：上图中真正提供 TCP 80 端口服务的内网服务器 IP 为 172.16.1.100，
- 目的端口转换为：指明将目的端口转为什么端口，如将666端口转换为80端口。
- 数据放行： 若启动，NAT转换后，将不受安全策略的限制；否则，将受安全策略的限制。
- 状态：设置该策略启用或禁用。

提示：

1、目的地址转换只能用于路由模式下的组网环境。

2、 若不启动数据放行，需在安全策略中放通外网区域和内网区域间的数据。

10.2.3 双向地址转换

功能描述：指在一条地址转换规则中，同时包含源地址和目标地址的转换，匹配规则的数据流将被同时转换源 IP 地址和目标 IP 地址，常用于内网用户通过公网 IP 或者域名访问内网的服务器。

配置路径：【防火墙】>【NAT规则】> 【新增】

配置描述：

第一： 进入新增【NAT规则】页面，如下图：

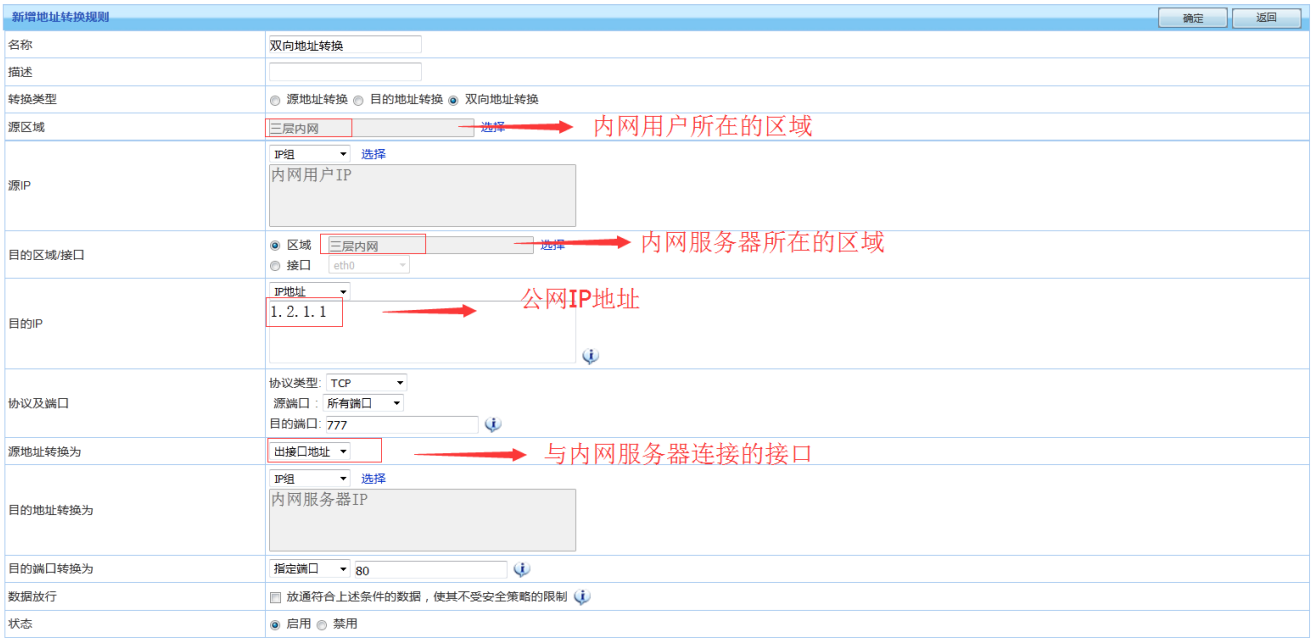


图55.新增 NAT 规则-双向地址转换

参数说明：

- 名称：设置 NAT转换的名称。
- 描述：设置规则的描述信息。
- 转换类型： 选择规则的转换类型。此处为双向地址转换。

- 源区域：指明从哪个区域进入的数据才进行匹配该策略，如图55：内网用户通过外网地址或域名访问内网服务器，且内网用户对应三层内网区域，所以，源区域为三层内网。
- 源IP: 指明从某区域进入哪些IP才能匹配该该策略。IP可以通过IP地址或IP组设置。如图55：所有的内网用户的IP。
- 目的区域/接口：设置数据最终从哪个区域或接口发送出去。如图55:内网用户访问的服务器在三层内网区，数据最终需要从设备定义的三层内网区转发出去，所以目的区域选择“ 三层内网区”。
- 目的IP: 指明内网用户访问哪个地址的时候，才进行双向地址转换。目的 IP 是数据包目的地址转换之前用户访问的地址，一般是设备自身接口的公网 IP。 如上图IP：1.2.1.1。
- 协议及端口：设置进行双向地址转换的协议以及端口。如图55：协议类型需要选择TCP， 源端口为所有，目的端口为777。
- 源地址转换为：设置当源地址、目标地址、协议等条件都匹配的数据，进行 IP 地址转换时，将源 IP 转换为哪个IP 地址。可以选择防火墙接口的出接口地址、某一段或单个IP地址、IP组或不转换。如上图：连接内网服务器接口的地址，一般是设备本身。
- 目的地址转换为：指明将目的地址转换为什么地址。
- 目的地址转换为：指明将目的地址转换为什么地址，以及是否进行目的端口的转换。如：上图中真正提供 TCP 80 端口服务的内网服务器 IP 为 172.16.1.100。
- 目的端口转换为：指明将目的端口转为什么端口，如将666端口转换为80端口。
- 数据放行： 若启动，NAT转换后，将不受安全策略的限制；否则，将受安全策略的限制。
- 状态：设置该策略启用或禁用。

提示：

1、 双向地址转换只能用于路由模式下的组网环境。

2、若禁用数据放行，需在安全策略中放通内网用户和内网服务器间的数据。

10.3 DOS/DDOS 防护

DOS 攻击/DDoS 攻击（拒绝服务攻击/分布式拒绝服务攻击），通常是以消耗服务器端资源、迫使服务停止响应为目标，通过伪造超过服务器处理能力的请求数据造成服务器响应阻塞，从而使正常的用户请求得不到应答，以实现其攻击目的。 DOS/DDOS 防护分成外网防护和内网防护两个部分，既可以防止外网对内网的 DOS 攻击，也可以阻止内网的机器中毒或使用攻击工具发起的 DOS 攻击。

10.3.1 外网防护

功能描述： 用于防止外网对内网的DOS攻击。

配置路径：【防火墙】>【DOS/DDOS防护】> 【外网防护】

配置描述：

第一：进入 【外网防护】页面，可以查看当前外网防护策略列表。如下图：

外网防护

新增 修改状态 删除全部 计数清零

序号	名称	描述	策略类型	攻击源区域	匹配计数	状态	操作
1	1	1	ARP洪水攻击防护:开启 扫描防护:开启 DOS/DDOS攻击防护:开启 基于数据包攻击:开启 异常报文侦测:开启	三层外网	1110	☑	修改 删除
2	外网防护		ARP洪水攻击防护:开启 扫描防护:开启 DOS/DDOS攻击防护:关闭 基于数据包攻击:关闭 异常报文侦测:关闭	三层外网	0	☑	修改 删除
3	外网防护2	保护内网用户	ARP洪水攻击防护:关闭 扫描防护:部分开启 DOS/DDOS攻击防护:关闭 基于数据包攻击:开启 异常报文侦测:关闭	三层外网	0	☑	修改 删除

图56. 外网防护

按钮说明：

点击<新增>，新增外网防护策略。

点击<计数清零>，将外网防护策略中的所有匹配计数归零。

点击<删除全部>，将删除所有的外网防护策略。

点击<删除>，删除本条外网防护策略。

点击<修改>，修改本条外网防护策略的参数 。

改变状态栏复选框的值，再点击<修改状态>，可修改外网防护策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有外网防护策略的状态。

外网防护策略的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，所以序号小的优先级高。

第二：点击进入<新增>页面，如下图：

图57.　新增外网防护策略

图58.　DOS/DDOS 防护攻击

参数说明：

- 名称：设置外网防护策略的名称。
- 描述：设置策略的描述信息。
- 源区域：设置需要防护的源区域。外网防护的源区域一般是外部区域。
- ARP洪水攻击：设置每源区域阀值的参数。若勾选<开启>，则只要在每秒该区域的接口收到超过阀值的ARP包，则会被认为是攻击。如果检测攻击后操作为阻断，则检测到攻击后，会丢弃超过阀值的ARP包。
- 扫描防护：选择扫描防护的类型。包括IP地址扫描防护和端口扫描防护。
  - IP地址扫描防护：设置IP地址扫描防护阈值参数，若开启，则每秒内如果收到来自源区域的IP地址扫描包的个数超过阀值，则会被认为是攻击。如果检测攻击后操作为阻断，则检测到攻击后，5分钟之内会阻断该源IP的所有数据。5分钟后解锁，再次计算该 IP的扫描次数。
  - 端口扫描防护：设置端口扫描阈值参数，若开启，则每秒单位内如果收到来自源区域的端口

扫描包个数超过阀值，则会被认为是攻击。如果检测攻击后的操作为阻断，则检测到攻击后，5 分钟之内会阻断源IP的所有数据。5分钟后解锁，再次计算该IP的端口扫描次数

- DOS/DDOS攻击防护：点击<请选择防护类型>后，进入进入 DoS/DDoS 攻击防护设置页面，如图58。主要参数解释如下：
  - 目的IP: 配置要保护的目标服务器的IP。表示从源区域来访问该目的IP数据才会匹配下面设置的阀值进行 DOS/DDOS 防护。
  - ICMP洪水攻击：设置每目的IP阈值的参数。若开启，则每秒内如果收到来自源区域访问单个目的IP的ICMP包个数超过阀值，则会被认为是攻击，如果检测攻击后操作为阻断，则检测到攻击后，会丢弃超过阀值的ICMP包。
  - UDP洪水攻击：设置每目的IP阈值的参数。若开启，则在每秒内如果收到来自源区域访问单个目的IP的UDP包的个数超过阀值，则会被认为是攻击。如果检测攻击后操作为阻断，则检测到攻击后，会丢弃超过阀值的UDP 包。
  - SYN洪水攻击防护：设置每目的IP阈值的参数。若开启，则在每秒内若果收到来自源区域访问单个目的IP的SYN包个数超过阈值时，则会被认为是攻击。如果检测攻击后操作为阻断，则检测到攻击后，会丢弃超过阀值的SYN包。
  - DNS洪水攻击防护：设置每目的IP阈值的参数。若开启，则在每秒如果收到来自源区域访问单个目的 IP 的 DNS 包个数超过阀值，则会被认为是攻击。如果检测攻击后操作为阻断，则检测到攻击后，所有发往该目标IP的DNS包进行丢弃。
- 基于数据包攻击：点击<请选择防护类型>，进入基于数据包攻击设置页面，选择需要防护的数据包攻击如下图：

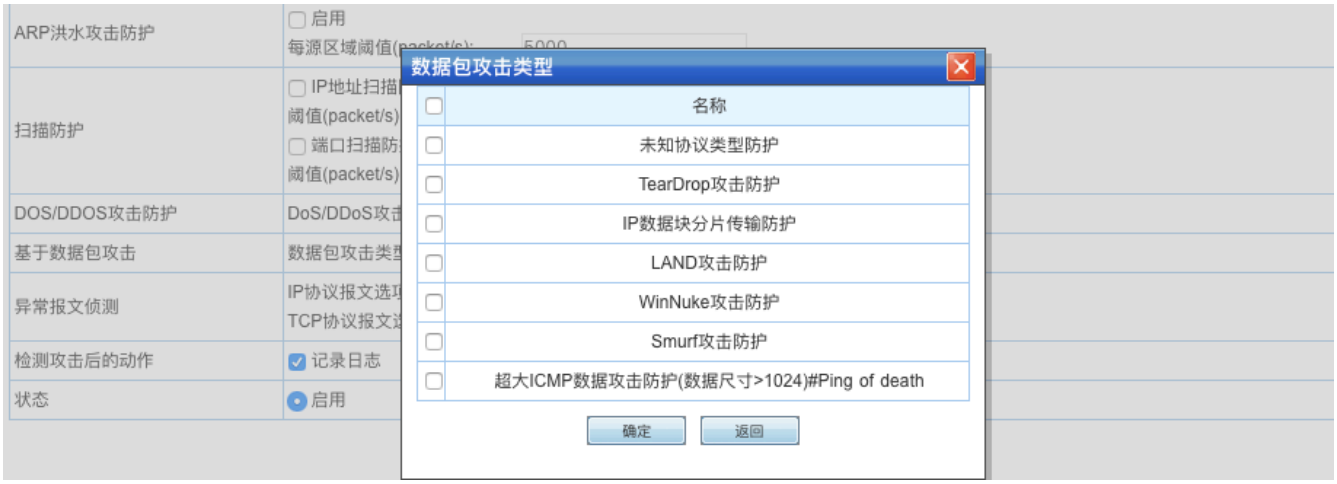


图59. 数据包攻击类型

- 未知协议类型防护：当协议ID大于137时会被认为是未知协议类型。
- TearDrop 攻击防护：TearDrop攻击防御主要是严格控制 IP 头的分片偏移的长度，当 IP 头分片偏移不符合规范时，则认为是 TearDrop 攻击。
- IP 数据块分片传输防护：勾选后，则表示不允IP数据块分片传输，若有分片传输则认为是攻击。非特殊情况下，建议不要勾选此项，可能会引起网络中断。

- ✧ LAND 攻击防护：当设备发现数据报文的源地址和目标地址相同时，则认为此报文为 LAND攻击。
- ✧ WinNuke 攻击防护：当 TCP头部标识 URG 位置为 1，且目标端口是 TCP139、TCP445 等，则此报文为 WinNuke 攻击。
- ✧ Smurf 攻击防护：当设备发现数据包的回复地址为网络的广播地址的 ICMP 应答请求包，则认为是 Smurf 攻击。
- ✧ 超大 ICMP 数据攻击防护：当 ICMP 报文大于 1024时，被认为是攻击。

➢ 异常报文侦测：设置对异常数据报文的侦测，包括侦测 IP 协议报文和 TCP 协议报文

- ✧ IP 协议报文：将带有 IP 时间戳选项、IP 安全选项、IP 数据流选项、IP 记录路由选项、IP 宽松源路由选项、IP 严格源路由选项等的普通报文认为是带有攻击性的，如果不允许数据报文携带这些选项，则勾选对应的选项即可进行防护。
- ✧ TCP 协议报文选项：包括 SYN 数据分片传输防护、TCP 报头标志位全为 0 防护、SYN 和 FIN 标志位同时为 1 防护、仅 FIN 标志位为 1 防护。正常的 TCP 报文标识不可能存在这些特征，目标主机可能因无法正常处理这些 TCP 报文而出现异常，勾选对应的选项即可进行保护。

➢ 检测攻击后的动作：根据需要选择是否产生日志或将阻挡攻击包。

➢ 状态：选择禁用或启用该策略。

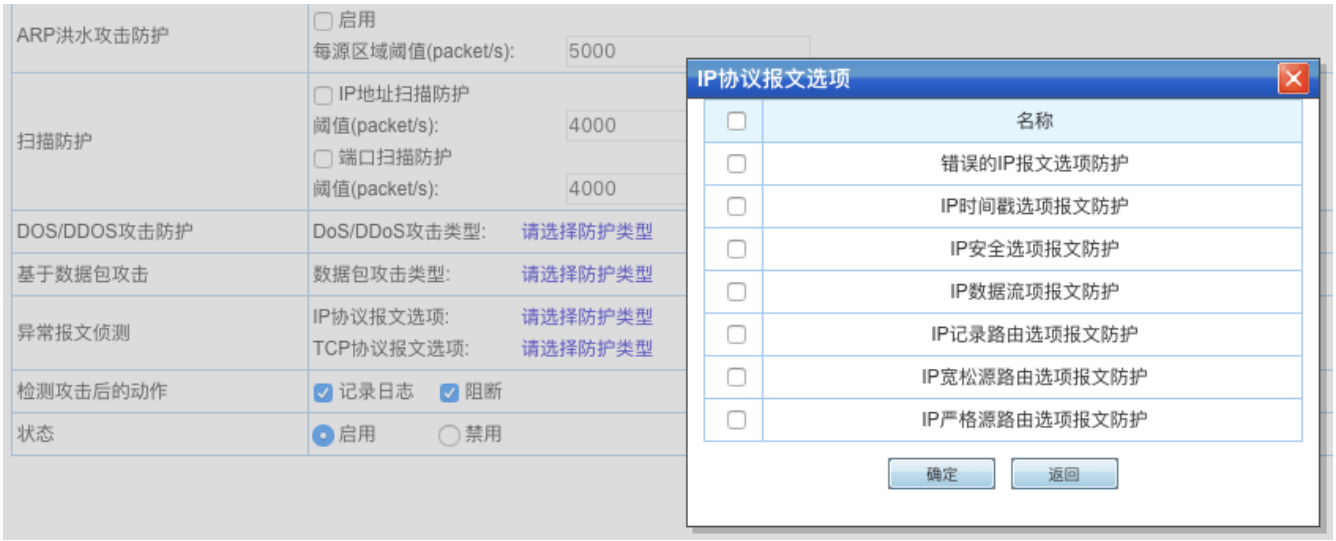


图60.IP 协议报文选择项

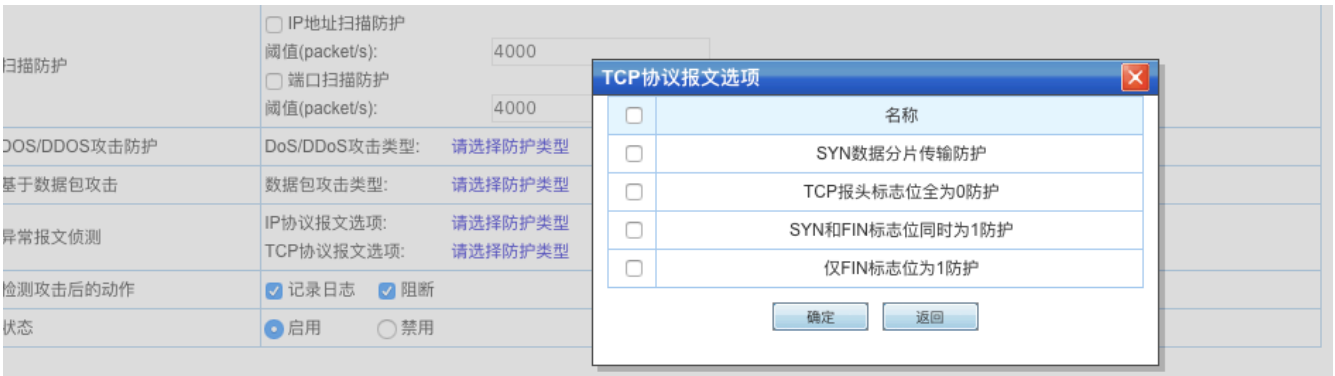


图61.协议报文选项

提示：

1、 数据包匹配是由上往下匹配的，当匹配到任何一个攻击行为被丢弃之后，都不会往下匹配。如果数据包没有匹配到前面的攻击，则会继续匹配下面设置的攻击行为是否符合。

2、 为有效地防范攻击行为设置了扫描防护后，建议再设置 DoS/DDoS 攻击防护里的 ICMP 攻击防护等信息。

10.3.2 内网防护

功能描述：防止内网设备因中毒或使用攻击工具发起的DOS攻击。

配置路径：【防火墙】>【DOS/DDOS防护】>【内网防护】

配置描述：

第一：点击进入【内网防护】页面，如下图：

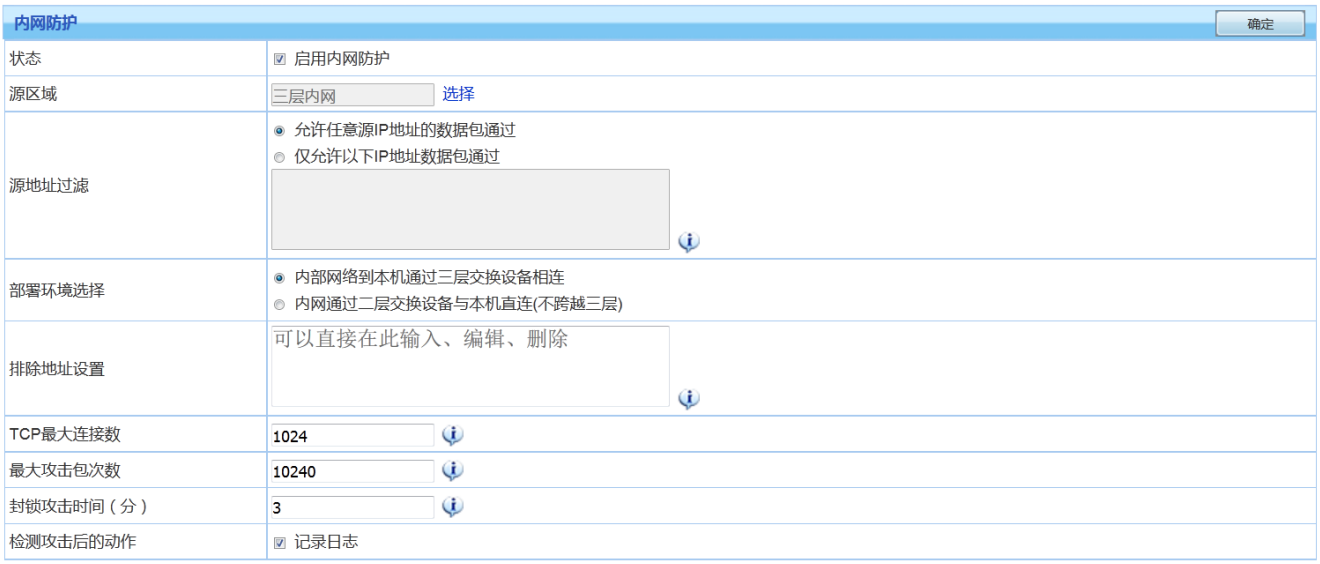


图62.内网防护

参数说明：

- 状态：设置内网防护的状态， 此状态为开启。
- 源区域：设置内网防护的源区域。一般为内网区域。
- 源地址过滤：设置哪些IP可以经过防火墙。若勾选<允许任意源IP地址的数据包通过>，将不对过源区域的IP做限制。若勾选<仅允许以下IP地址的数据包通过>，则只有设置的IP才能经过防火墙，其余的IP包将被丢弃。
- 部署环境选择：选择防火墙与内网的部署环境。若设备和内网之间是通过二层交换机直接相连，没有过任何三层设备或者路由器，则勾选<内网通过二层设备与本机直接相连>或<内部网络到本机通过三层交换设备相连>均可；若设备和内网之间是通过三层设备直接相连，则勾选<内部网络到本机通过三层交换设

备相连>。

- 排除地址设置：配置不进行DOS防护的IP地址或域名。
- TCP最大链接数：限制同一IP地址在一分钟内向同意目标IP地址的同一端口发起的最大TCP链接数，若超过设定的值则把源IP封锁特定的时间。
- 最大攻击包次数：限制每个IP在每分钟内发起的最大攻击包次数（攻击包包括SYN、ICMP、TCP/UDP等小包），若超过设定的值则把该IP或MAC封锁特定的时间
- 封锁攻击时间：设置设备在检测到攻击以后对攻击主机的封锁时间，以分钟为单位，默认3min。
- 检测攻击后的动作：设置是否对检测到攻击的数据包产生日志记录。

提示：在部署环境选择时，建议选择<内部网络到本机通过三层交换设备相连>，该选是基于 IP 地配策略的，而<内部网络到本机通过二层交换设备相连>选项是基于 MAC 匹配策略。若选择后者，设备部署在三层环境，有内网攻击时，造成连接三层设备的所用用户均不能上网。

10.4 ARP 欺骗防护

功能描述：防止设备本身或指定 IP不受 ARP 欺骗。

配置路径：【防火墙】>【启用 ARP 欺骗防护】

配置描述：

第一：进入【启用 ARP 欺骗防护】页面，如下图：

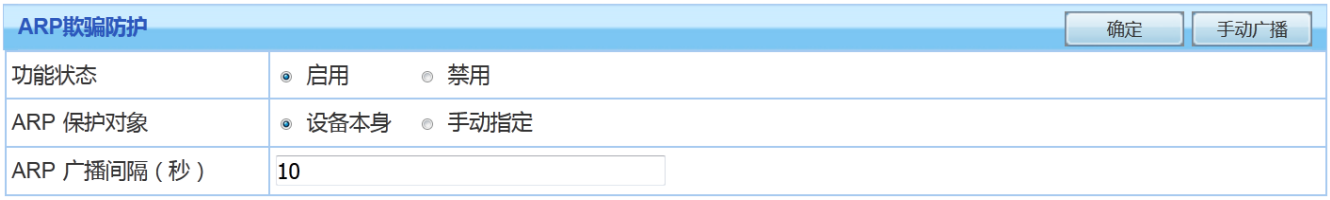


图63.ARP 欺骗防护 1

参数说明：

- 功能状态：启用或禁用 ARP 欺骗防护功能。
- ARP 保护对象：防止被ARP 风暴攻击的对象。
- ARP 广播间隔：发送 ARP 请求的时间间隔。设备定时向外发送 ARP 请求，以便网络中其他设备（如内网 PC、邻近交换或路由设备）的 ARP 表能定时更新，防止被 ARP 风暴攻击。广播的 ARP 请求有以下两种情况：
  - ✧ 若[ARP 保护对象]设置为[设备本身]，则从每个 UP 的接口广播 ARP 请求（源 IP 和 MAC 为设备的接口 IP 和 MAC）。
  - ✧ 若[ARP 保护对象]设置为[手动指定]，则根据设置的发送IP 和发送 MAC 和发送接口向外广播 ARP 请求。设置界面如下图：

图64.ARP 欺骗防护 2

- 发送 IP：ARP 请求的 源 IP。
- 发送 MAC：ARP 请求的 源 MAC。
- 发送接口：发送 ARP 请求的接口号，可选择多个接口。

10.5 应用层网关

功能描述：启用或禁用应用层网关。

配置路径：【防火墙】>【应用层网关】

配置描述：

第一：进入【应用层网关】页面，如下图：

图65.应用层网关

参数说明：

- h323:若视频会议使用 h323，则启用。
- sip:若视频会议使用 sip，则启用。

10.6 加速老化

功能描述：设置会话的超时时间，当并发会话量大时，可以加快会话的老化速度。

配置路径：【防火墙】>【加速老化】

第一：进入【加速老化】页面，如下图：

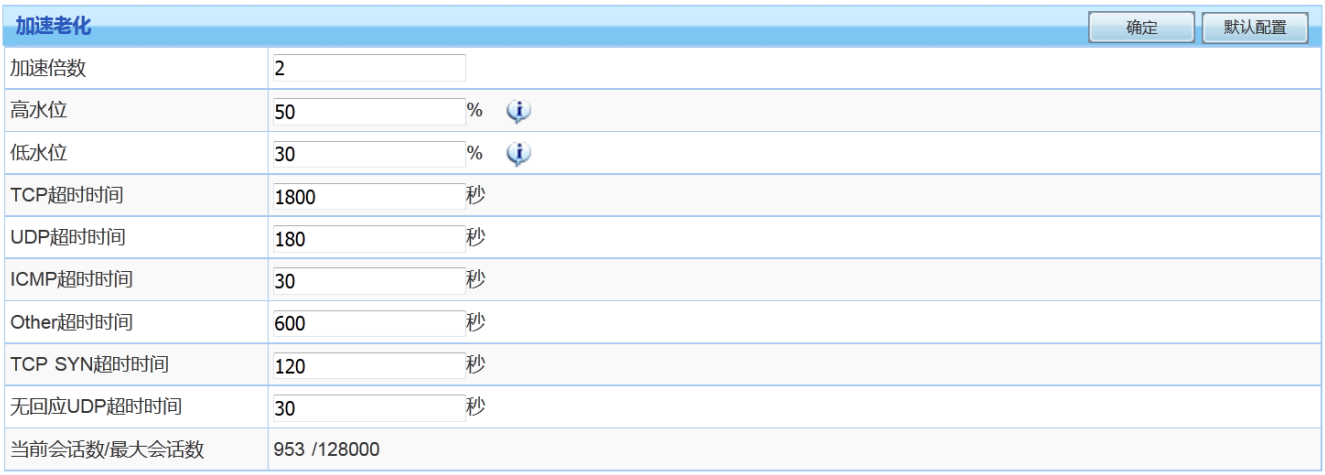


图66.加速老化

参数说明：

- 加速倍数：当需要加速老化时，以默认的几倍加速老化现有会话。
- 高水位：当前会话数与总会话数容量的比例，从低升至高水位时，开始加速老化。
- 低水位：当前会话数与总会话数容量的比例，从高水位下降至低水位时，恢复正常老化速度。
- TCP 超时时间：可设定 TCP 会话的超时时间。默认为 1800s。
- UDP 超时时间：可设定 UDP 会话的超时时间。默认为 180s。
- ICMP 超时时间：可设定 ICMP 会话的超时时间。默认是 30s。
- Other 超时时间：可设定其它会话的超时时间。默认是 600s。
- TCP SYN 超时时间：可自定义 tcp-syn 报文老化时间，默认为 120s。
- 无回应 UDP 超时时间：可自定义无回应的 UDP 会话的超时时间，默认是 30s。
- 当前会话数/最大会话数：可查看当前会话数跟最大会话数。

11 内容安全

内容安全包括应用控制策略、应用内容过滤、防病毒策略四部分。

11.1 应用控制策略

功能描述： 应用控制策略根据报文的源地址、目的地址、服务类型、时间段等参数组合成各种流量，可对这些流量进行阻断或放通，策略规则的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，所以同一组策略中，序号小的优先级高。

配置路径：【内容安全】>【应用控制策略】

配置描述：

第一：进入【应用控制策略】页面，如下图：

图67.应用控制策略

按钮说明：

点击<新增>,新增应用控制策略。

点击<删除所有>，删除所有的应用控制策略

点击<计数清零>，将应用控制略列表中的所有匹配计数归零。

点击<删除本组>，删除某线路中所有的控制策略，如：二层内网→二层外网。

点击<修改>，修改本条应用控制策略，但规则名称和生效线路不能修改。

点击<插入>，在当前位置插入一条应用控制策略。

点击<移动>，改变应用控制策略的序号，从而改变该规则的优先级。

点击<删除>，删除某条应用控制策略。

改变状态栏复选框的值，再点击<修改状态>，可修改应用控制策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有应用控制策略的状态。

第二：点击<新增>按钮，增加应用控制策略，如下图：

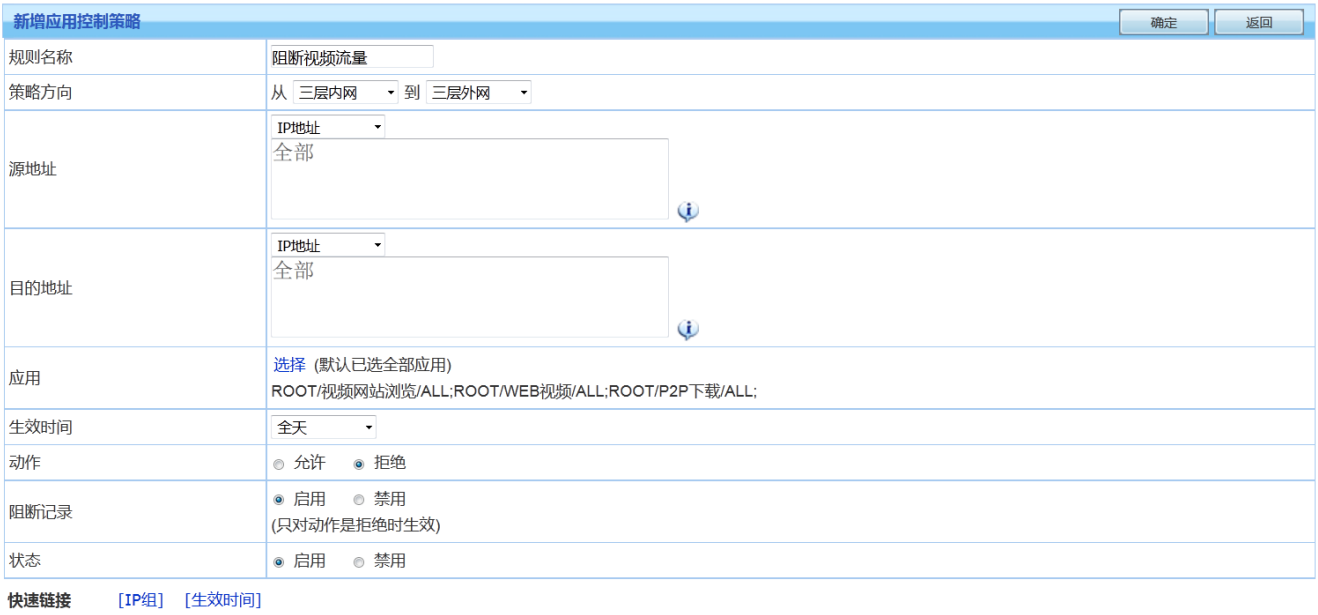


图68.新增应用控制策略

参数说明：

- 规则名称：设置应用控制策略的名称。
- 策略方向：代表数据流的方向。如从二层内网区域到二层外网区域。
- 源地址：设置匹配该策略的源地址。可输入 IP 地址、选择 IP 组或用户及用户组。IP 组在【系统对象>IP 组】中配置，用户及用户组在【用户认证>组织结构】中配置。
- 目的地址：设置匹配该策略的目的地址，可输入 IP 地址、选择 IP 组或用户及用户组。IP 组在【系统对象>IP 组】中配置，用户及用户组在【用户认证>组织结构】中配置。
- 应用：选择匹配该策略的服务。默认选择“所有”，点击<选择>按钮，进入选择服务页面，可以根据组网需要选择相关服务。如下图：

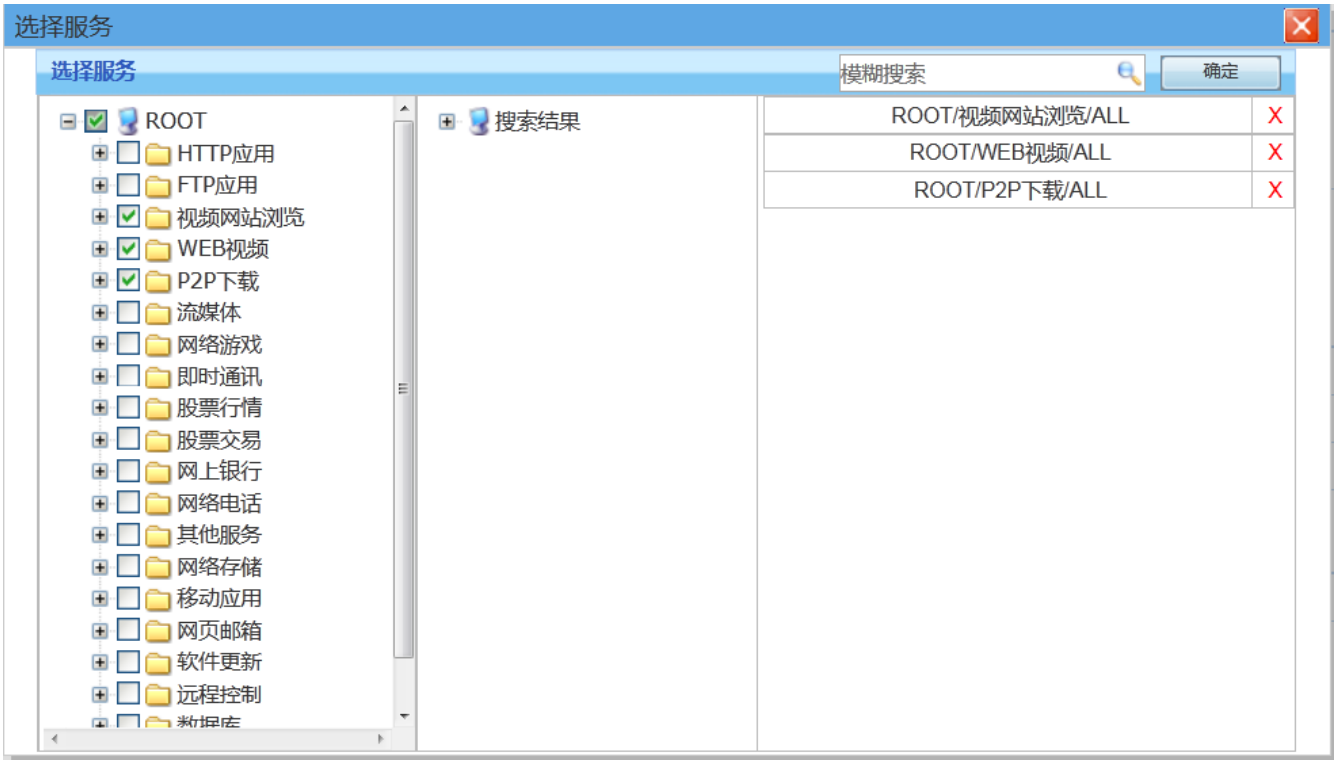


图69.选择服务

- 生效时间：设置本策略的有效时间段，可分时段控制数据流，比如 9：00～12：00 和 14：00～18：00，不允许员工用 QQ。生效时间可在快速链接中的“生效时间”中配置，也可在【系统对象>时间计划】中配置。
- 动作：设置当有数据流匹配该策略时的动作。勾选“允许”则数据流允许通过，勾选“拒绝”则数据流被阻断。
- 阻断记录： 选择启用或禁用阻断记录，该规则只对动作是拒绝时生效。
- 状态：选择启用或禁用本策略。

11.2 应用内容过滤

功能描述：用于设置内网用户的上网策略，上网策略对象可以同时被多个用户组或用户引用，从而对内网用户进行上网行为的控制。应用内容过滤包括：URL 过滤、关键字过滤、文件传输过滤、邮件过滤、SSL 管理。每个策略对象可以同时设置这 5 部分的内容。

配置路径：【内容安全】>【应用内容过滤】

配置描述：

第一：点击进入【应用内容过滤】页面，如下图：

图70.上网权限策略

按钮说明：

点击<新增>,新增内容过滤策略。

点击<删除所有>，删除所有的内容过滤策略

点击<计数清零>，将内容过滤策略列表中的所有匹配计数归零。

点击<修改>，修改本条内容过滤策略，但规则名称。

点击<插入>，在当前位置插入一条应用内容过滤策略。

点击<移动>，改变内容过滤策略的序号，从而改变该策略的优先级。

点击<删除>，删除某条内容过滤策略。

改变状态栏复选框的值，再点击<修改状态>，可修改内容过滤策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有内容过滤策略的状态。

第二：点击新增按钮，添加策略。策略类型包括 URL 过滤、关键字过滤、文件传输过滤、邮件过滤，SSL 管理 5 种类型。下面详细说明：

11.2.1 URL 过滤

功能描述：对 URL 的 HTTP Get 进行过滤。

配置路径：【内容安全】>【应用内容过滤】

配置描述：

第一：进入【应用内容过滤】页面，点击<新增>按钮，增加应用内容过滤策略。

第二：选择“URL 过滤>内置 URL 库”选项卡。首选勾选需要进行控制的 URL 条目的“选定”复选框，再次是对选定的条目进行“动作”和“生效时间”的选择。若需要对选定的条目进行“动作”和“生效时间”的批量配置，则在“批量操作”后面的选择相应的“动作”与“生效时间”。若需要单独配置某条目，则在相应的条目后面选择“动作”和“生效时间”。“动作”包括“拒绝”和“允许”两项。所有的条目是按照顺序从上往下匹配。配置界面如下图：

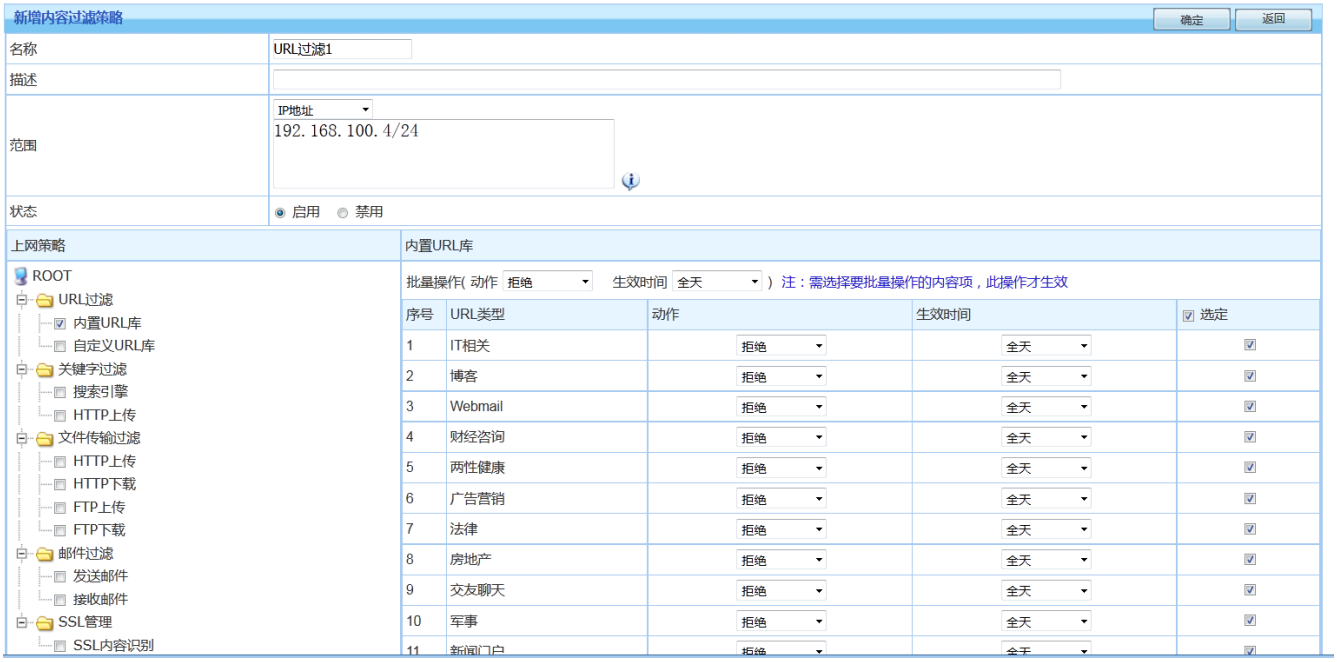


图71.上网策略-增加上网策略 URL 过滤

第三：选择生效适用用户组或者终端类型，两者可同时勾选。用户分为：用户及用户组、IP、IP 组，可勾选组织结构用户、用户组。

提示：

1、URL 条目遵循从按顺序从前往后匹配的原则，如果一个条目匹配了，就不会再向下匹配，所以序号小的条目优先级高。

2、“自定义 URL”的优先级高于“内置 URL 库”的优先级。

3、对于“自定义 URL”的优先顺序是在【系统对象>关键字组】页面定义的，可以通过<移动>和<插入>来调整 URL 条目的顺序。

关

11.2.2 关键字过滤

功能描述：针对对在搜索引擎中搜索的关键字进行过滤，即阻止某些关键字的搜索。2对论坛发帖的内容进行关键字进行过滤，即阻止包括某些关键字的帖子发送。

配置路径：【内容安全】>【应用内容过滤】

配置描述：

第一：进入【应用内容过滤】页面，点击<新增>按钮，增加上网策略。或者继续前面新增“办公室组”策略对象的基础上配置关键字过滤。

第二：选择“关键字过滤>引擎搜索”选项卡。首选勾选需要进行控制的关键字组条目的“选定”复选框，再次是对选定的条目进行“动作”和“生效时间”的选择。若需要对选定的条目进行“动作”和“生效时间”的批量配置，则在“批量操作”后面的选择相应的“动作”与“生效时间”。若需要单独配置某条目，则在相应的条目后面选择“动作”和“生效时间”。“动作”包括“拒绝”和“允许”两项。所有的条目是按照顺序从上往下匹配。配置界面如下图：

上网策略-关键字过滤-搜索引擎

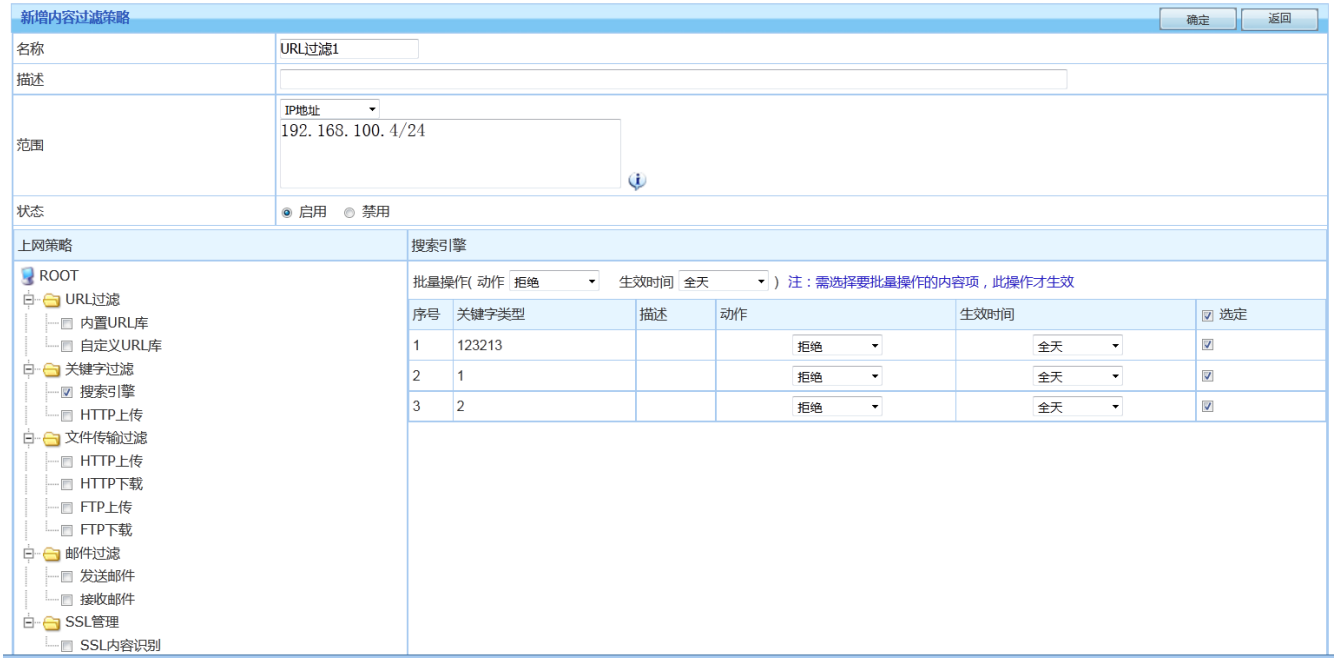


图72.添加上网策略-搜索引擎过滤

设置完成选择生效适用用户组

第三：选择“关键字过滤>发帖内容（HTTP 上传）”选项卡，配置方法与“搜索引擎”相同。如下图：

上网策略-关键字过滤-发帖内容

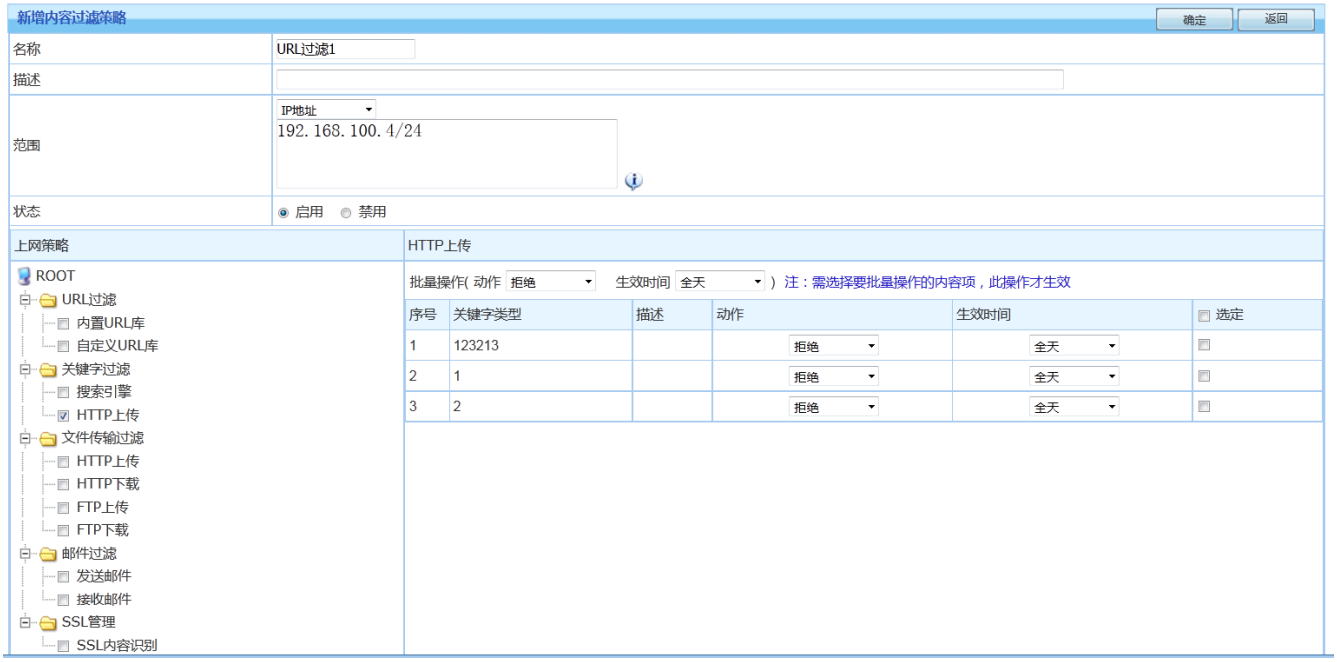


图73.添加上网权限策略-上网策略发帖过滤

设置完成选择生效适用用户组

配置关键字过滤前需要先配置关键字组，详见【系统对象>关键字组】的配置。

第四：选择生效适用用户组 。用户分为：用户及用户组、IP、IP 组，可勾选组织结构用户、用户组。

提示：

1、 关键字条目遵循从按顺序从前往后匹配的原则，如果一个条目匹配了，就不会再向下匹配，所以序号小的条目优先级高。

2、 关键字组之间的优先顺序是在【系统对象>关键字组】页面定义的，可以通过<移动>和<插入>来调整关键字组条目的顺序。

11.2.3 文件传输过滤

功能描述：通过文件后缀名的方式对 HTTP/FTP 文件的上传和下载进行过滤

配置路径：【内容安全】>【应用内容过滤】

配置描述：

第一：进入【应用内容过滤】页面，点击<新增>按钮，增加应用内容过滤策略。或者继续前面新增“办公室组”策略对象的基础上配置文件传输过滤。

第二：选择“文件传输过滤>HTTP 上传” 选项卡。首选勾选需要进行控制的文件类型条目的“选定”复选框，再次是对选定的条目进行“动作”和“生效时间”的选择。若需要对选定的条目进行“动作”和“生效时间”的批量配置，则在“批量操作”后面的选择相应的“动作”与“生效时间”。若需要单独配置某条目，则在相应的条目后面选择“动作”和“生效时间”。“动作”包括“拒绝”和“允许”两项。所有的条目是按照顺序从上往下匹配。配置界面如下图：

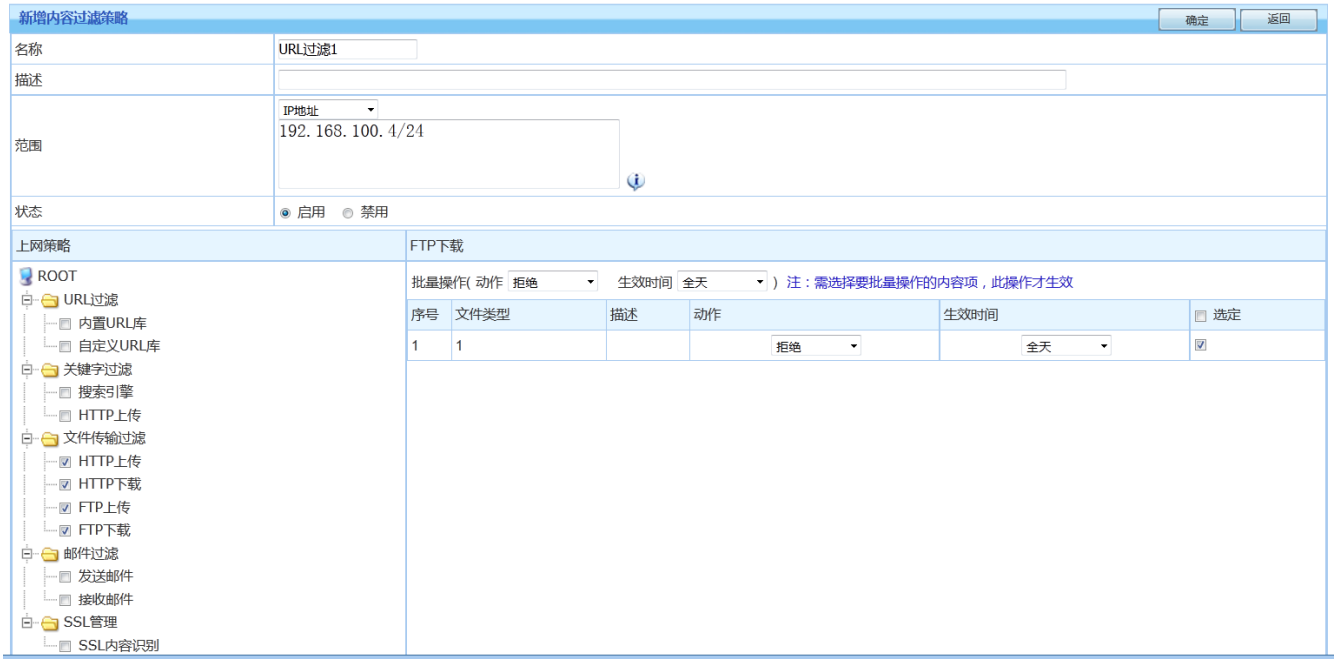


图74.添加上网策略-文件传输过滤

第三：选择生效适用用户组。 用户分为：用户及用户组、IP、IP 组，可勾选组织结构用户、用户组。

<HTTP 下载>、<FTP 上传>、<FTP 下载>的配置方法与 <HTTP 上传>相同。

配置文件过滤前需要先配置文件类型，详见【系统对象>文件类型】的配置。

提示：

1、 文件类型条目遵循从按顺序从前往后匹配的原则，如果一个条目匹配了，就不会再向下匹配，所以序号小的条目优先级高。

2、 文件类型条目之间的优先顺序是在【系统对象>文件类型】页面定义的，可以通过<移动>和<插入>来调整文件类型条目的顺序。

11.2.4 邮件过滤

☆ 发送邮件过滤

功能描述：用于对内网用户使用邮件客户端(SMTP/WebMail)协议发送邮件时，对发送的邮件地址、邮件主题、邮件内容及附件进行检查，对符合过滤条件的邮件进行过滤。

配置路径：【内容安全】>【应用内容过滤】

配置描述：

第一：进入【应用内容过滤】页面，点击<新增>按钮，增加应用内容过滤策略。选择“发送邮件过滤”选项卡，配置过滤条件。如下图：

图75.添加上网策略-发送邮件过滤

第二：选择生效适用用户组。用户分为：用户及用户组、IP、IP 组，可勾选组织结构用户、用户组。

参数说明：

- 发件人过滤：可选择<不允许发件人的邮件地址包含以下后缀>或<仅允许发件人的邮件地址包含以下后缀>。比如：只允许后缀为 yahoo.com.cn 的人发邮件，则选择<仅允许发件人的邮件地址包含以下后缀>，

在后面的文本框中进入“yahoo.com.cn”

- 主题和内容关键字过滤：对发送邮件的主题及内容的关键字进行过滤。
- 附件过滤：对邮件附件的文件类型进行过滤。比如：过滤文件类型为“exe”的附件，则在文本框中输入“*.exe”。
- 邮件内容大小过滤：配置邮件内容容量的最大值，超过该大小的邮件将不允许发送。容量大小的单位有“KB”和“MB”，可以根据需要来选择单位。
- 附件大小过滤：配置邮件附件的最大值，超过该大小的邮件将不允许发送。附件大小的单位有“KB”和“MB”，可以根据需要来选择单位。

提示：

1、 如某个过滤条件未配置任何值，则不检查此项内容。

2、 <发件人过滤>、<主题和内容关键字过滤>、<附件过滤>、<邮件内容大小过滤>、<附件大小过滤>中任何一个条件满足，就会被过滤。

☆ 邮件过滤--接收邮件过滤

功能描述：用于对内网用户使用邮件客户端(*POP3* /WebMail)协议接受邮件时，对接受的邮件地址、邮件主题、邮件内容及附件进行检查，对符合过滤条件的邮件进行过滤。

配置路径：【内容安全】>【应用内容过滤】

配置描述：

第一：进入【应用内容过滤】页面，点击<新增>按钮，选择“接受邮件过滤”选项卡，配置过滤条件。如下图：

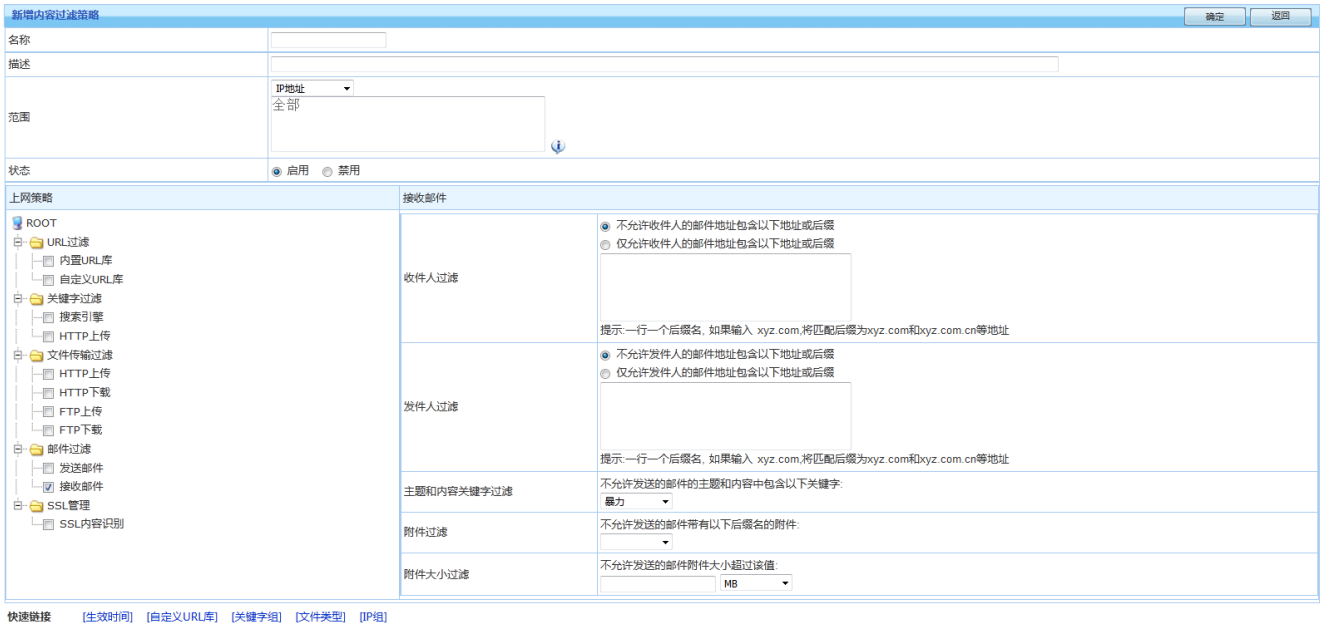


图76.添加上网策略-接受邮件过滤

第二：选择生效适用用户组 。用户分为：用户及用户组、IP、IP 组，可勾选组织结构用户、用户组。

参数说明：

- 收件人过滤：可选择<不允许收件人的邮件地址包含以下后缀>或<仅允许收件人的邮件地址包含以下后缀>。比如：只允许后缀为 yahoo.com.cn 的人收邮件，则选择<仅允许收件人的邮件地址包含以下后缀>，在后面的文本框中进入“yahoo.com.cn”
- 发件人过滤：可选择<不允许发件人的邮件地址包含以下后缀>或<仅允许发件人的邮件地址包含以下后缀>。比如：只允许后缀为 yahoo.com.cn 的人发邮件，则选择<仅允许发件人的邮件地址包含以下后缀>，在后面的文本框中进入“yahoo.com.cn”
- 主题和内容关键字过滤：对发送邮件的主题及内容的关键字进行过滤。
- 附件过滤：对邮件附件的文件类型进行过滤。比如：过滤文件类型为“exe”的附件，则在文本框中输入“*.exe”
- 附件大小过滤：配置邮件附件的最大值，超过该大小的邮件将不允许发送。附件大小的单位有“KB”和“MB”，可以根据需要来选择单位。

提示：

1、 如某个过滤条件未配置任何值，则不检查此项内容。

2、 <收件人过滤>、<发件人过滤>、<主题和内容关键字过滤>、<附件过滤>、<附件大小过滤>中任何一个条件满足，就会被过滤。

11.2.5 SSL 管理

功能描述：针对加密的 WEB 应用内容和加密的邮件内容进行识别和审计。

配置路径：【内容安全】>【应用内容过滤】

配置描述：进入【应用内容过滤】页面，点击<新增>按钮，选择“SSL 内容识别”选项卡，配置过滤条件。如下图：

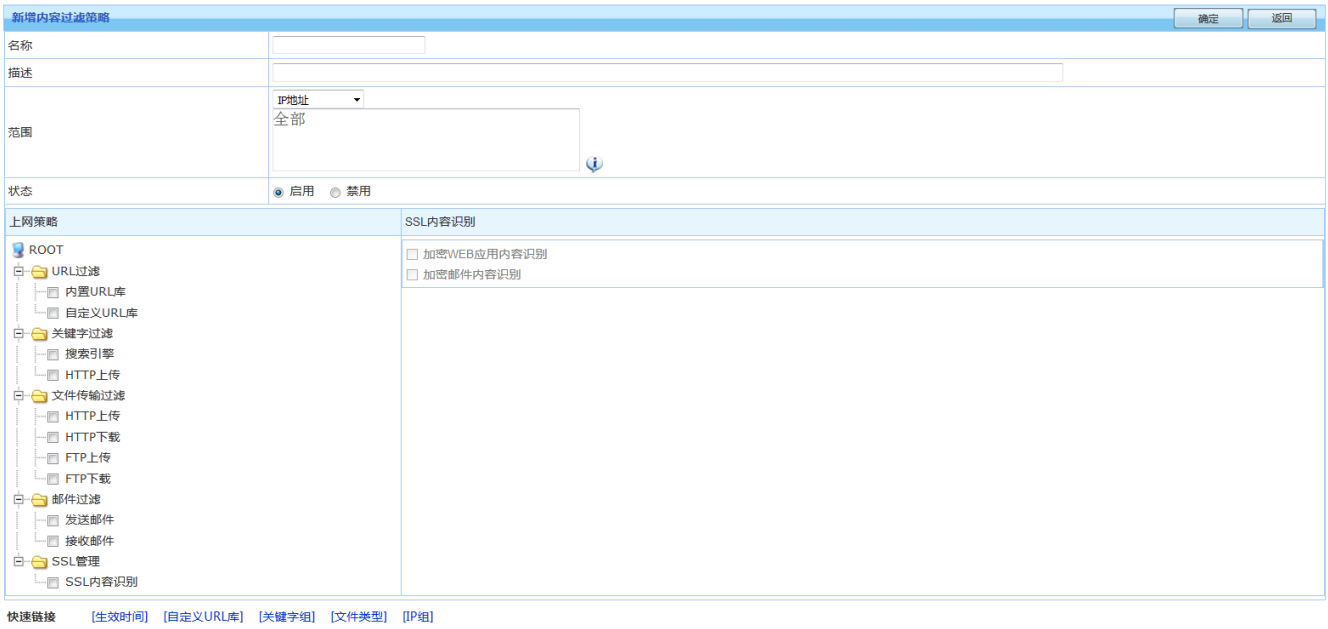


图77.添加上网策略-SSL 内容识别

选择生效适用用户组 。用户分为：用户及用户组、IP、IP 组。

参数说明：

- 加密 WEB 应用内容识别：识别加密的 WEB 网站内容，比如：https://www.yahoo.com/
- 加密邮件内容识别：识别加密的邮件内容。

11.3 防病毒策略

功能描述：针对 HTTP、FTP、POP3 和 SMTP 这四种常用协议进行杀毒，来保护经过设备数据的安全。 一般用于保护内网用户不被病毒入侵。

配置路径：【内容安全】>【防病毒策略】

配置描述：

第一：点击进入<防病毒策略>,可查看当前所有的防病毒策略，如下图：

防病毒策略 [新增] [修改状态] [删除全部] [计数清零]

序号	名称	源区域	源IP/用户	目的区域	目的IP	文件类型	排除域名/IP	匹配计数	状态	操作
1	邮件查杀	三层内网	内网用户IP	三层外网	全部	exe com	www.baidu.com	0	☑	修改 上移 下移 移动 删除
2	HTTP查杀	三层内网	全部	三层外网	全部	txt com exe		0	☑	修改 上移 下移 移动 删除

图78.防病毒策略

按钮说明：

点击<新增>，新增防病毒策略。

点击<计数清零>，将防病毒策略列表中的所有匹配计数归零。

点击<删除全部>，将删除所有的防病毒策略。

点击<删除>，删除本条防病毒策略。

点击<修改>，修改本条防病毒策略的参数，但不能修改本条策略的名称。

点击<上移>， 当前策略的序列号减少一，从而升高了本条策略的优先级。

点击<下移>，当前策略的序列号增加一，从而减低了本条策略的优先级。

改变状态栏复选框的值，再点击<修改状态>，可修改防病毒策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有防病毒策略的状态。

策略规则的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，序号小的优先级高。

第二：点击<新增>按钮，增加防病毒策略，如下图：

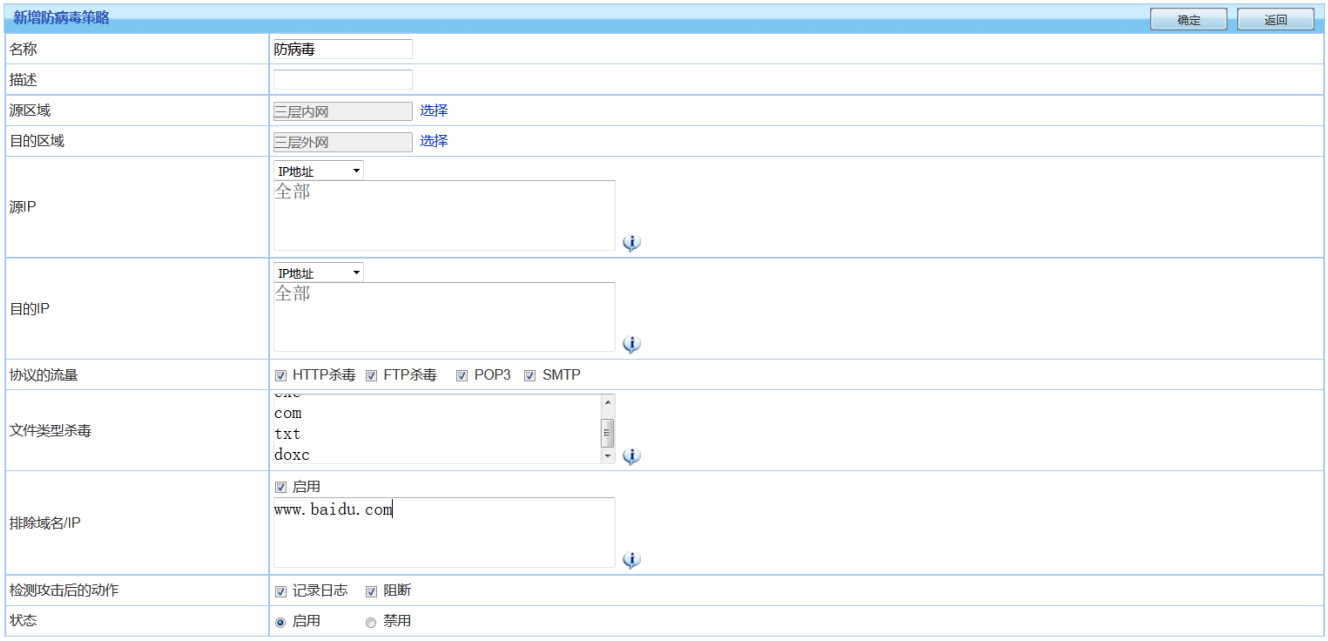


图79.新增防病毒策略

参数说明：

- 名称：设置防病毒策略的名称。
- 描述：设置策略的描述信息。
- 源区域：设置需要保护的源区域，如保护内网区域的所有用户不被感染病毒。
- 目的区域：设置源区域用户访问哪些目标区域地址时才进行病毒防御。
- 源 IP：设置需要防护的源 IP。只有从源区域进入的匹配源 IP 的数据，才匹配该策略。IP 的设置可以用 IP 地址或 IP 组，IP 组即可以在快速栏中添加，也可在【系统对象>IP 组】中配置。
- 目的 IP:设置需要防护的目的 IP。配置同源 IP。
- 协议的流量：设置需要进行病毒防御的应用类型，有 HTTP 杀毒、FTP 杀毒、邮件杀毒（POP3 收邮件/SMTP 发邮件）四种。
- 文件类型杀毒：设置用于杀毒的文件扩展名。仅适用于 HTTP 杀毒和 FTP 杀毒。
- 排除域名/IP：勾选“启用”复选框，启用排除域名/IP，可设置某些特殊网站的数据不需要杀毒，仅适用于 HTTP 杀毒。
- 检测攻击后的动作：设置检测到带有病毒的数据时，设备处理的动作，有<日志记录>和<阻断>两种。
- 状态：设置启用或禁用该策略。

12 IPS

入侵防御系统（Intrusion Prevention System）依靠对数据包的检测来发现对内网系统的潜在威胁。IPS 将检查入网的数据包，确定这种数据包的真正用途，然后根据用户配置决定是否允许这种数据包进入目标区域网络。

12.1 IPS

功能描述：通过对进入设备的数据包进行检测，来保护内网的完全。

配置路径：【IPS】>【IPS】

配置描述：

第一：点击进入<IPS>,可查看当前 IPS 策略，如下图：

IPS　　新增　修改状态　删除全部　计数清零

序号	名称	源区域	源IP	目的区域	目的IP	漏洞列表	匹配计数	状态	操作
1	保护服务器	三层外网	全部	三层内网	内网服务器IP	保护服务器 dns漏洞攻击...	0	☑	修改 上移 下移 移动 删除
2	保护客户端	三层内网	内网用户IP	三层外网	全部	保护客户端 telnet漏洞攻击...	0	☑	修改 上移 下移 移动 删除

图80.IPS

按钮说明：

点击<新增>，新增IPS策略。

点击<计数清零>，将IPS策略列表中的所有匹配计数归零。

点击<删除全部>，将删除所有的IPS策略。

点击<删除>，删除本条IPS策略。

点击<修改>，修改本条IPS策略的参数，但不能修改本条策略的名称。

点击<上移>， 当前策略的序列号减少一，从而升高了本条策略的优先级。

点击<下移>，当前策略的序列号增加一，从而减低了本条策略的优先级。

改变状态栏复选框的值，再点击<修改状态>，可修改IPS策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有IPS策略的状态。

策略规则的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，序号小的优先级高。

第一：点击<新增>按钮，增加 IPS 策略，如下图：

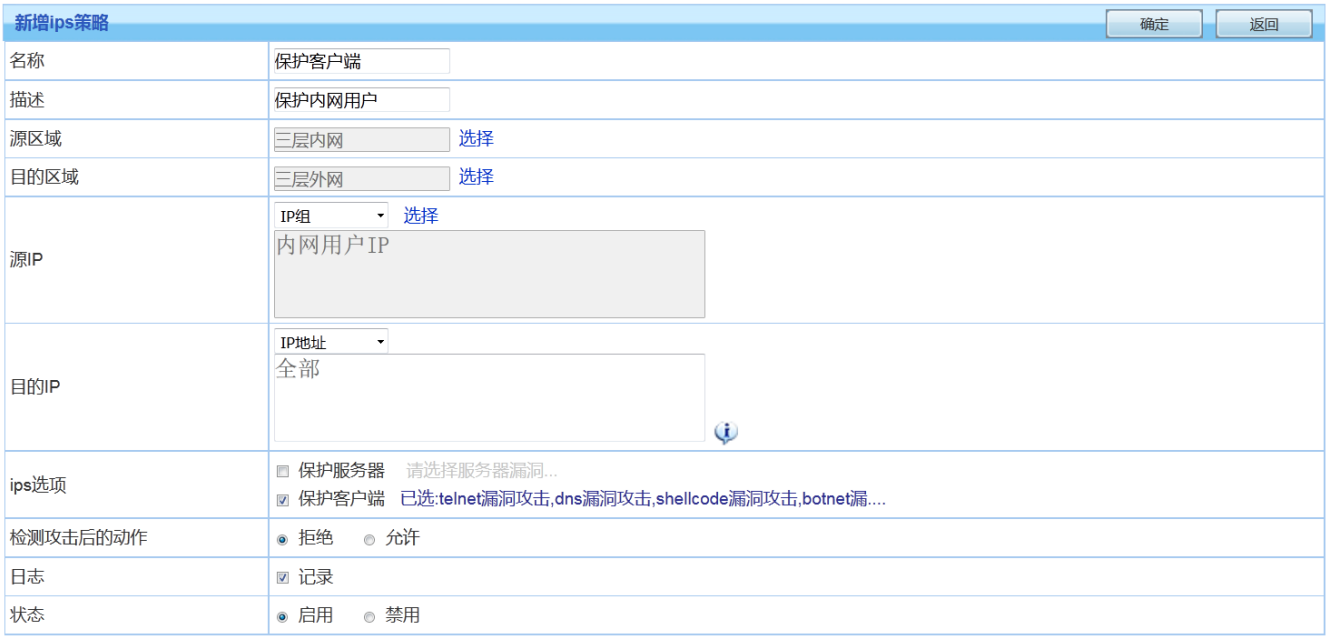


图81.新增 IPS 策略

参数说明：

- 名称：设置 IPS 策略的名称。
- 描述：设置策略的描述信息。
- 源区域：设置需要防护的源区域。保护客户端的源区域一般为内网区域，保护服务器的源区域一般为外网区域。
- 目的区域：设置访问的目标区域。保护客户端的目的区域一般为外网区域，保护服务器的目的区域一般为内网区域。
- 源 IP：设置需要防护的源 IP。只有从源区域进入的匹配源 IP 的数据，才匹配该策略。IP 的设置可以用 IP 地址或 IP 组，IP 组即可以在快速栏中添加，也可在【系统对象>IP 组】中配置。
- 目的 IP:设置需要防护的目的 IP。配置同源 IP。
- IPS 选项：设置需要保护的内容，包括保护客户端和保护服务器两部分。
  - 保护客户端：用于保护内网用户的网络安全。包括telnet、dns、shellcode、botnet、web-browse、system等漏洞攻击。点击<请选择客户端漏洞>后，可根据需要选择需要防护的漏洞。如下图：

图82.客户端漏洞

✧ 保护服务器：用于保护内网服务器的网络安全。包括ftp、worm、web、rpc等漏洞攻击。点击<请选择服务器漏洞>后，可根据需要选择需要防护的漏洞。如下图：

图83.服务器漏洞

➢ 检测攻击后的动作：用于设置当发现保护的目标对象出现 IPS 攻击后，该数据包是放行还是拒绝。若勾选

“允许”，则放行该数据包；若勾选“拒绝”，则丢弃数据包。

- 日志：用于设置当发现保护的目标对象出 IPS 攻击后，是否记录到 IPS 日志中，勾选“启用”，则会记录 IPS 攻击包的攻击行为。可在【报表中心>内置报表中心>日志查询>IPS 日志】中查看。
- 状态：选择启用或禁用该策略。

提示：一般情况下保护服务器源区域需要选择外网接口所属区域，目的区域选择内网接口所属区域。保护客户端源区域选择内网接口所属区域，目的选择外网接口所属区域。建议在添加保护客户端和保护服务器的策略时分开配置。

13 服务器保护

13.1 WEB 应用防护

功能描述：专门用于保护内网的 WEB 服务器，可以有效防止跨站请求伪造、SQL 注入、XSS 攻击、会话劫持、目录遍历等各种针对 WEB 应用的攻击行为。

配置路径：【服务器保护】>【WEB 应用防护】

配置描述：

第一：点击进入<WEB 应用防护页面>,可查看当前 IPS 策略，如下图：

WEB应用防护　　新增　修改状态　删除全部　计数清零

序号	名称	源区域	源IP	目的区域	目的IP	网站攻击防护	动作	匹配计数	状态	操作
1	保护WEB服务器	三层外网	全部	三层内网	内网服务器IP	SQL注入,XSS攻击,网站扫描	拒绝	0	☑	修改 上移 下移 移动 删除

图84.WEB 应用防护

按钮说明：

点击<新增>，新增WEB应用防护策略。

点击<计数清零>，将WEB应用防护策略列表中的所有匹配计数归零。

点击<删除全部>，将删除所有的WEB应用防护策略。

点击<删除>，删除本条WEB应用防护策略。

点击<修改>，修改本条WEB应用防护策略的参数，但不能修改本条策略的名称。

点击<上移>， 当前策略的序列号减少一，从而升高了本条策略的优先级。

点击<下移>，当前策略的序列号增加一，从而减低了本条策略的优先级。

改变状态栏复选框的值，再点击<修改状态>，可修改WEB应用防护策略的状态(“勾选”表示启用，“不勾选”表

示禁用)。点击表头的“状态”复选框，可以改变所有IPS策略的状态。

策略规则的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，序号小的优先级高。

第一：点击<新增>按钮，增加 WEB 应用防护策略，如下图：

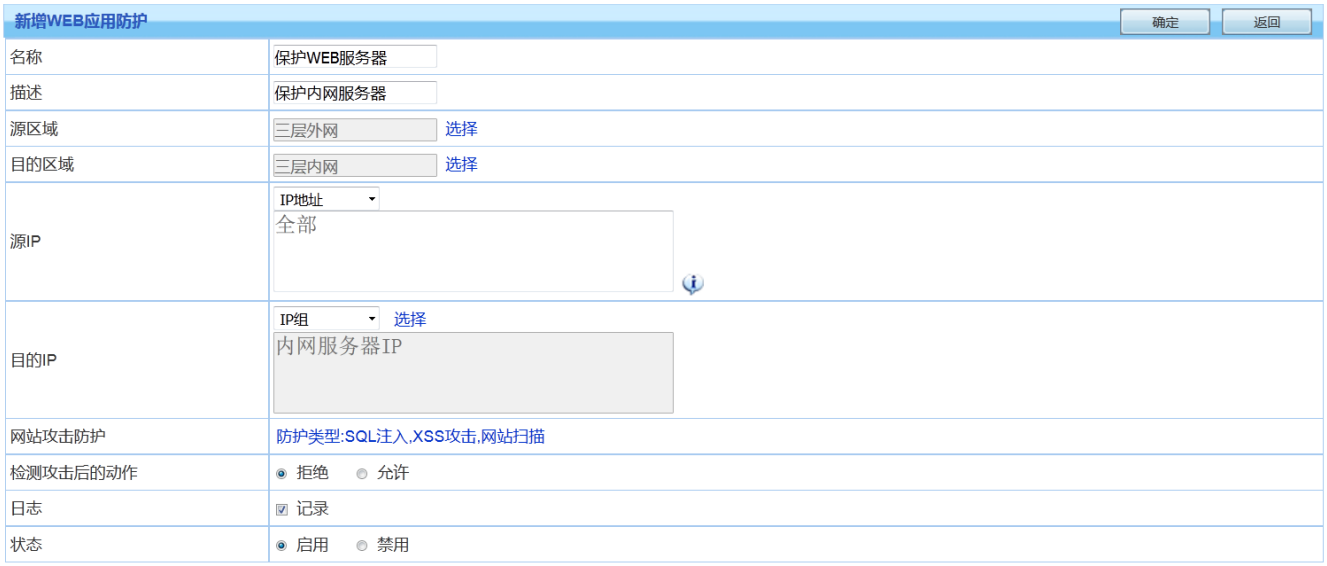


图85.新增 IPS 策略

参数说明：

- 名称：设置 WEB 应用防护策略的名称。
- 描述：设置策略的描述信息。
- 源区域：设置匹配该策略的源区域。如选择外网区，则可以检测来自公网用户针对内网服务器的漏洞攻击。
- 目的区域：设置访问的目标区域。一般选择防御的保护对象。 如内网服务器所在的区域。
- 源 IP：设置需要防护的源 IP。只有从源区域进入的匹配源 IP 的数据，才匹配该策略。IP 的设置可以用 IP 地址或 IP 组，IP 组即可以在快速栏中添加，也可在【系统对象>IP 组】中配置。
- 目的 IP:设置需要防护的目的 IP。配置同源 IP。
- 网站攻击防护：设置需要保护的攻击行为。点击<请选择网站攻击防护>后，可根据需要选择需要防护的漏洞。如下图：

图86.WEB 应用防护类型

- ✧ SQL注入：即攻击者通过设计上的安全漏洞，把SQL代码黏贴在网页形式的输入框内，获取网络资源或改变数据。
- ✧ XSS攻击：即跨脚本攻击。它允许代码植入到提供给其他用户使用的页面中，攻击者可利用 XSS 漏洞绕过访问控制，获取数据，例如盗取账号等。
- ✧ 网站扫描：对 WEB 网站扫描，对 WEB 网站的结构、漏洞进行扫描。
- ✧ WEBSHELL: WEBSHELL 是 WEB 入侵的一种脚本工具，通常情况下，是一个 ASP、PHP 或者 JSP 程序页面，也叫做网站后面木马，在入侵一个网站后，常常将这些木马放置在服务器 WEB 目录中，与正常网页混在一起。通过 WEHSHELL，长期操纵和控制受害者网站。
- ✧ 跨站请求伪造：通过伪装来自受信任用户的请求来利用受信任的网站。
- ✧ 普通攻击：常见的攻击例如命令执行，代码执行，注入，文件包含，敏感信息泄漏，会话固定，HTTP响应拆分等相关规则。
- ✧ 目录遍历攻击：通过浏览器向web服务器任意目录附加“../”，或者是在有特殊意义的目录附加“../”，或者是附加“../”的一些变形，编码，访问WEB服务器根目录之外的目录。
- ✧ 会话劫持攻击：攻击者可以通过破坏已建立的数据流而实现劫持，冒充合法用户进行破坏活动。

- ➢ 检测攻击后的动作：用于设置当发现保护的目标对象出现 击后，该数据包是放行还是拒绝。若勾选“允许”，则只会检测攻击行为，检测出来后仍然会放行攻击包；若勾选“拒绝”则上述各种攻击检测出来后进行阻断。
- ➢ 日志：用于设置当发现保护的目标对象出击后，是否记录到 WEB 应用防护日志中，勾选“启用”，则会记录 IPS 攻击包的攻击行为。可在【报表中心>内置报表中心>日志查询>WEB 应用防护】中查看。
- ➢ 状态：选择启用或禁用该策略。

14 VPN

14.1 IPSec

14.1.1 IPSec 隧道

功能描述：配置 IPSec 隧道。

配置路径：【VPN】>【IPSec】>【IPSec隧道】

配置描述：

第一：进入【IPSec 隧道】页面，可以看到当前已建立的 IPSec 隧道配置。如下图：

图87.IPSec 隧道配置

第二：进入点击<新增>按钮，增加 IPSec 隧道。如下图：

图88.新增 IPSec 隧道

参数说明：

- 本地网关：指防火墙 WAN 端下一跳 IP 地址或本地 ID。
- 对端网关：指对端 VPN 设备连接 IP 或域名或对端为 VPN 拨号用户，必须有一端为为固定 IP。

- 协商模式: 配置 VPN 协商模式，两端协商模式必须一致。
- 预共享密钥：配置 VPN 连接的预共享密钥，两端预共享密钥必须一致。
- 点击<高级>按钮，可配置 IPSec 连接的更多详细参数，两端必须一致。

14.1.2 IPSec 规则

功能描述：配置 IPSec 规则。

配置描述：

第一：进入【IPSec 规则】页面，可以看到当前已建立的 IPSec 规则配置。如下图：

图89.配置 IPSec 规则

第二：进入点击<新增>按钮，增加IPSec规则。如下图：

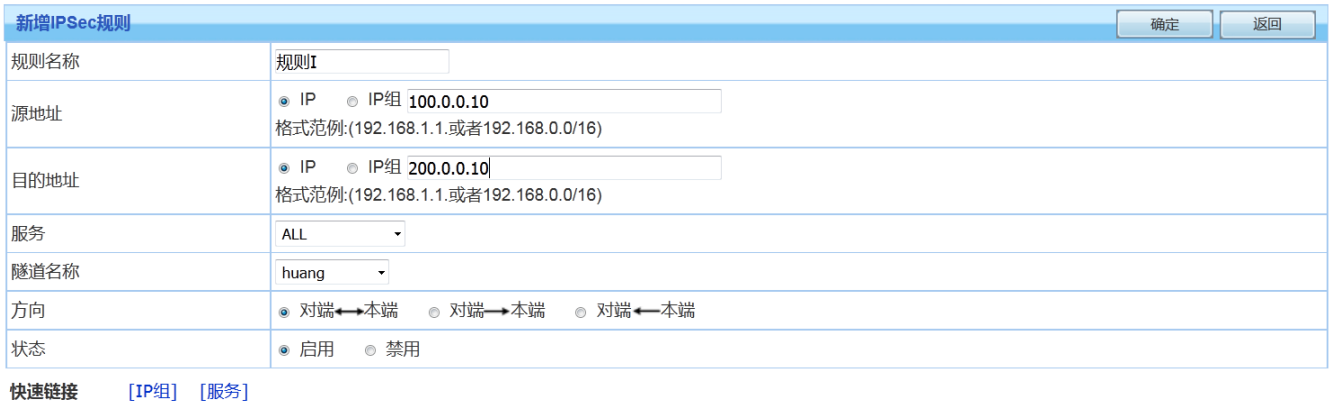


图90.新增 IPSec 规则

参数说明：

- 源地址：指需要匹配 VPN 规则的行为管理设备 LAN 端地址。
- 目标地址：指与哪些目标地址通讯时使用 VPN 隧道。
- 服务：被指定的服务将使用 VPN 隧道。
- 隧道名称：将此规则应用在合适的 VPN 隧道上。
- 方向：指规则应用的数据流方向。
- 状态：启用或禁用该规则。

提示：

1. IPSec 规则配置完成，需点击<应用>按钮，触发 ipsec 协商。
2. IPSec 协商成功，IPSec 规则的状态灯为绿色，不成功则为红色。
3. IPSec 协商日志，在【系统日志>IPSec 日志】详细查看。

14.2 PPTP

功能描述：配置 PPTP VPN

配置路径：【VPN】>【PPTP】

配置描述：

第一：进入【PPTP】页面，开始设置 PPTP 的相关参数。如下图：

图91.配置 PPTP

参数说明：

- PPTP 状态：启用或禁用 PPTP 服务器功能。
- 服务器 IP：本机作为 PPTP 服务器的接口 IP 地址。
- 首选 DNS 服务器：分配给 PPTP 客户端的首选 DNS 服务器。
- 备用 DNS 服务器：分配给 PPTP 客户端的备用 DNS 服务器。
- 认证方式：Radius 认证和本地认证，默认本地认证。

第二：进入点击<新增>按钮，增加 PPTP IP 池。如下图：

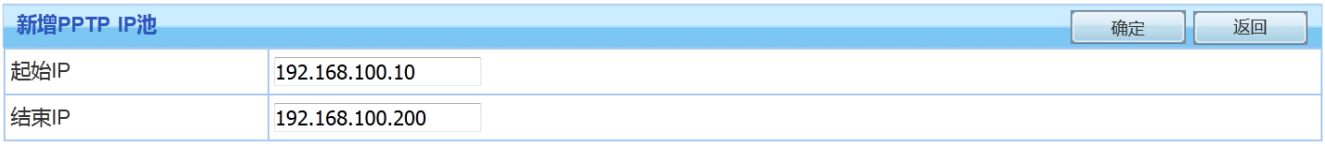


图92.新增 PPTP IP 池

参数说明：

- 起始 IP：分配给 PPTP 客户端的 IP 地址段的起始地址。
- 结束 IP：分配给 PPTP 客户端的 IP 地址段的结束地址。

提示：当 PPTP 客户端连接 PPTP 服务器时，设备就将 DNS 服务器和 PPTP IP 池里面的地址随机分配给 PPTP 客户端。

14.3 VPN 用户

功能描述：配置 VPN 的用户，该用户可应用于 PPTP VPN。

配置路径：【VPN】>【VPN 用户】

配置描述：

第一：进入【VPN 用户】页面，可以看到当前已配置好的 VPN 用户。如下图：

VPN用户 [新增] [删除所有]

序号	用户名	接入模式	操作
1	zhoudan	PPTP	修改 删除
2	test	PPTP	修改 删除
3	james	PPTP	修改 删除
4	123	PPTP	修改 删除
5	huang	PPTP	修改 删除

图93.配置 VPN 用户

第二：进入点击<新增>按钮，增加 PPTP 用户。如下图：

新增VPN用户 [确定] [返回]

用户名	zhangsan
密 码	●●●●●● (6-16位)
确认密码	●●●●●●
接入模式	☑ PPTP

图94.配置 VPN 用户

参数说明：

- 用户名：VPN 用户的名称。
- 密码：VPN 用户的密码。
- 确认密码：VPN 用户的确认密码
- 接入模式：选择该用户可以应用于 PPTP VPN 协议。

提示：VPN 用户可应用于 PPTP VPN 拨号用户。

15 用户认证

“用户认证”包括认证策略、组织结构、认证选项、认证服务器、组织管理、临时账号设置等六部分。

15.1 认证策略

功能描述：定义认证的条件、认证方式及使用的认证服务器。策略规则的匹配原则是按顺序从前往后匹配，即从第一条规则开始顺序匹配，一旦遇到一条匹配的规则就停止，所以序号越小的规则优先级越高。

配置路径：【用户认证】>【认证策略】

配置描述：

第一：进入【认证策略】配置页面，如下图：

图95.认证策略列表

按钮说明：

点击<新增>，新增认证策略。

点击<删除所有>，删除所有的认证策略。

点击<删除>，删除本条认证策略。

点击<修改>，修改本条认证策略。

点击<插入>，在当前位置插入一条认证策略。

点击<移动>，改变认证策略的序号。

改变状态栏复选框的值，再点击<修改状态>，可修改认证策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有认证策略的状态。

提示：没有配置任何策略的情况下，系统默认以 IP 地址作为新用户名，自动加入到根组(Root)，并自动绑定 IP 地址。

第二：点击<新增>，新增认证策略，如下图：

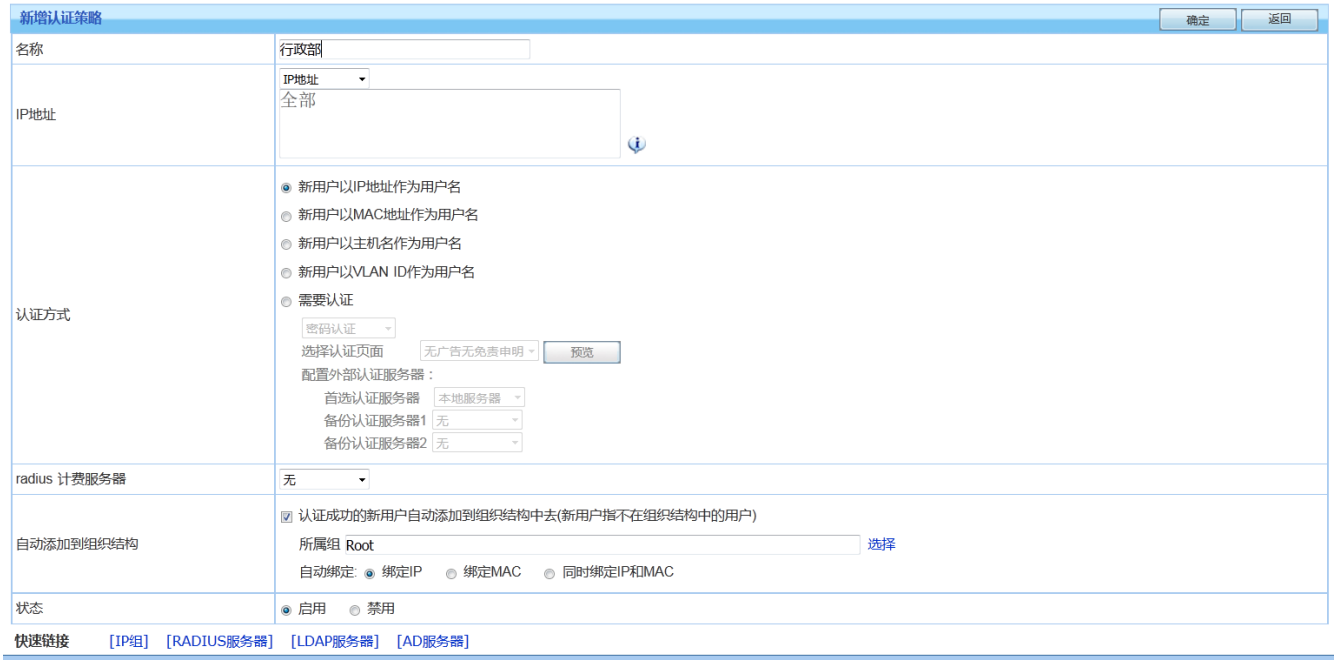


图96.新增认证策略 1

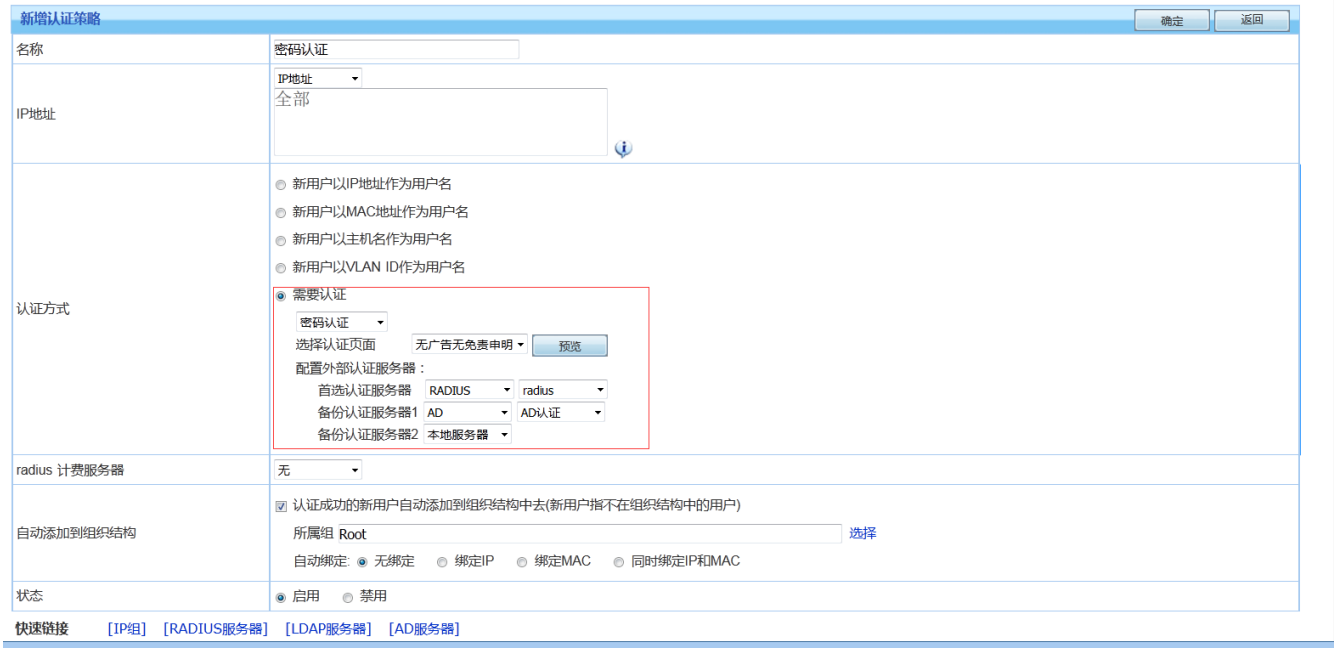


图97.新增认证策略 2

参数说明：

- 名称：认证策略的名称。
- IP 地址：匹配认证条件的内网地址。
- 认证方式： 根据内网地址的 IP 地址来判断用户采取的认证方式，共有如下五种：
  - 新用户以 IP 地址作为用户名：内网用户不需要密码认证，并且当该用户不在组织结构中时，自动以用户的 IP 地址为用户名。
  - 新用户以 MAC 地址作为用户名：内网用户不需要密码认证，并且当该用户不在组织结构中时，

自动以用户的 MAC 地址为用户名。

- ✧ 新用户以主机名作为用户名：内网用户不需要密码认证，并且当该用户不在组织结构中时，自动以用户的主机名。
- ✧ 新用户以 VLAN ID 作为用户名：内网用户不需要密码认证，并且当该用户不在组织结构中时，自动以用户的 VLAN ID 地址为用户名。
- ✧ 需要认证：内网用户需要用户名和密码认证，并选择认证服务器，一共可以选择三个服务器。首先去[首选认证服务器]进行认证；若未返回认证结果，再去[备份认证服务器1]进行认证；若仍未返回认证结果，再去[备份认证服务器2]进行认证。

  认证方式有：密码认证、短信认证、短信/密码认证。

提示：

1、 密码认证-本地认证，需手动创建本地用户名及密码，如果初始密码为 000000 或者 111111 这种情况，使用这种密码登录，系统会提示“修改密码太过简单，请先修改密码”。在弹出的认证窗口点击[修改密码]，密码修改完成，使用新的密码方可完成认证。
2、 密码认证-外部服务器认证，需在【用户认证>认证服务器】完成服务器相关参数设定。
3、 短信认证需在【用户认证>认证选项】完成相关参数设定。
4、 认证页面可使用系统内置页面，也可在【用户认证>认证选项>终端提示页面定制】自定义。

- ➢ 自动添加到组织结构：认证成功的新用户自动添加到组织结构中去，新用户指不在组织结构中的用户。“所属组”表示自动添加到那个组，点击输入框后面的<选择>按钮，可选择组。
- ➢ 自动绑定：在自动添加用户时，是否要配置绑定检查。随着选择认证方式不同，自动绑定选项也稍微有区别，具体如下：
  - ✧ 新用户以 IP 地址作为用户名：可以选择为“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“绑定 IP”。
  - ✧ 新用户以 MAC 地址作为用户名：可以选择为“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“绑定 MAC”。
  - ✧ 新用户以主机名作为用户名：可以选择为“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“绑定 IP”。
  - ✧ 新用户以 VLAN ID 作为用户名：只能且必须选择为“绑定 VLAN”。
  - ✧ 到服务器去认证：可以选择为“无绑定”、“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“无绑定”。
  - ✧ 状态：启用或禁用本策略，默认启用。

15.2 组织结构

通过设备提供的 Web 管理界面，可以输入、维护用户和组的信息，从而建立起和本单位实际组织结构相

一致的组织信息。用户和组的维护功能包括新建、删除、更新、改变所属关系、绑定 MAC 地址等。

15.2.1 定位并选中当前操作对象

功能描述：在针对用户和组操作时，应首先浏览、定位、选中当前要操作的用户或组。

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，在下图中，点击左边的组织结构中的节点，右边的列表中将显示该组织的成员，可以通过右面列表中的复选框选择要操作的用户或组。如下图：

图98.定位当前操作对象

左边是当前所有用户组的树型结构，默认有一个 Root 根组，所有建立的组和用户都在根组之下。右边是左边已定为的组所包含的所有直属用户和子组。名称列图标为两个人的表示子组，图标为一个人且颜色为彩色的表示在线用户，图标为一个人且颜色为黑白的表示离线用户。

第二：若想查看或编辑当前组下面的用户和子组，点击右边列表中名称列子组或用户应的链接。

15.2.2 修改根组

功能描述：修改根组的名称、上网策略、黑名单控制

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，点击顶部的<修改根组>按钮，弹出“修改根组”页面，如下图：

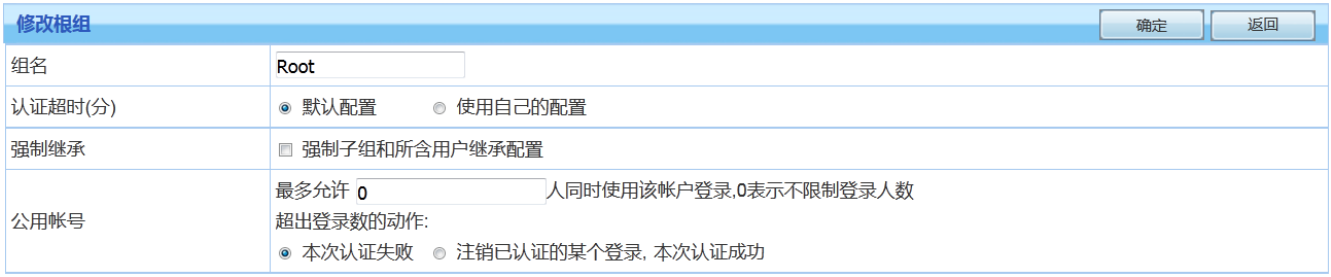


图99.修改根组

参数说明：

- 组名：根组的名称，默认 Root，可填入需要修改的名称。
- 强制继承：强制子组和所含用户继承上网策略和黑名单控制的配置，默认未启用。启用后，所有的用户和子组的上网策略和黑名单控制都被修改为根组的配置。
- 公用账号：多个人同时使用同一个认证账号即为公用账号，默认不限制登录人数。超出登录数的动作：本次认证失败/注销当前最早登录的账号，本次认证成功。

15.2.3 新增子组

功能描述：新增子组，并设置子组的上网策略和黑名单控制

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，点击顶部的<新增子组>按钮，弹出“新增子组”页面，如下图：

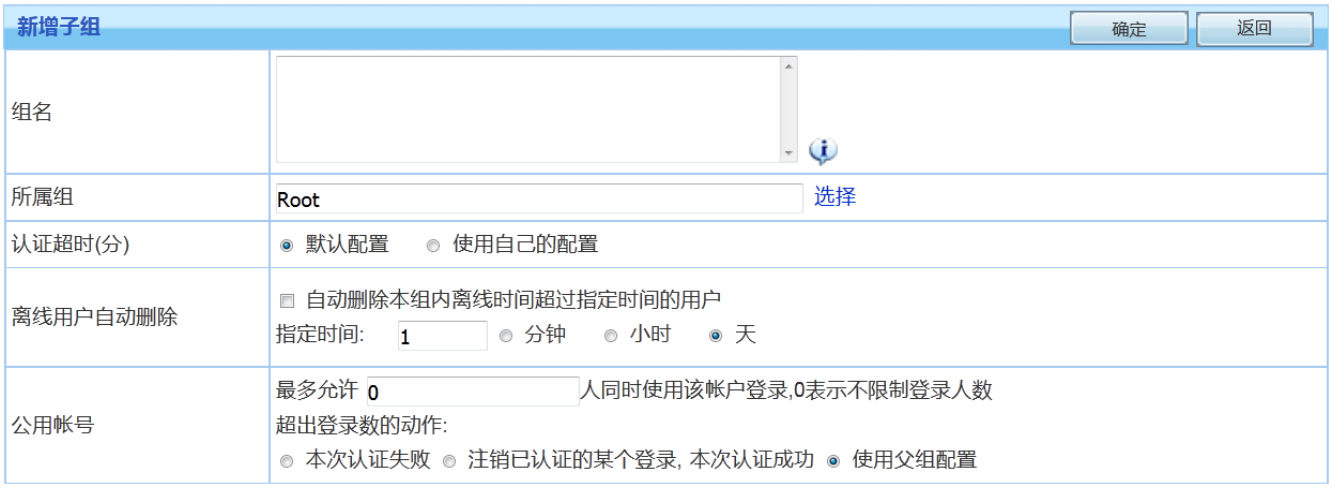


图100.　　新增子组

参数说明：

- 组名：子组的名称，一次可以创建多个子组，一行一个组名，支持汉字、数字、字母、下划线、中划线。
- 所属组：默认已经填好刚才进入新增页面时的父组，也可以点击后面的<选择>，就出现选择用户组的框，可改变父组。

- 所属组：父组，当前组隶属的父组。
- 认证超时（分）：默认配置(默认 10 分钟，十分钟内该用户没有任何流量经过上网行为管理，即为超时，系统置为离线用户)；使用自己的配置（0-100000,0 表示不限制）。
- 离线用户自动删除：自动删除本组内离线时间超过指定时间的用户（默认不启用）。
- 公用账号：多个人同时使用同一个认证账号即为公用账号，默认不限制登录人数。超出登录数的动作：本次认证失败/注销当前最早登录的账号，本次认证成功。

15.2.4 修改子组

功能描述：修改子组的配置上网策略和黑名单控制

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，点击右边列表中名称列对应的子组的链接。比如要修改 Root 下面的[临时用户组]。先定位到 Root，然后点击名称列的 [临时用户组]，如下图：

图101.　修改子组 1

第二：进入子组的修改页面，填入需要修改的值。如下图：

图102.　　修改子组 2

参数说明：

- 组名：不可修改。
- 所属组：父组，当前组隶属的父组。也可以点击后面的<选择>，就出现选择用户组的框，可改变父组。
- 认证超时（分）：默认配置(默认 10 分钟，十分钟内该用户没有任何流量经过上网行为管理，即为超时，系统置为离线用户)；使用自己的配置（0-100000,0 表示不限制）。
- 离线用户自动删除：自动删除本组内离线时间超过指定时间的用户（默认不启用）。
- 公用账号：多个人同时使用同一个认证账号即为公用账号，默认不限制登录人数。超出登录数的动作：本次认证失败/注销当前最早登录的账号，本次认证成功。

15.2.5 新增普通用户

功能描述：新增普通用户，并设置子组的上网策略和黑名单控制

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，点击顶部的<新增用户>按钮，弹出“新增用户”页面，用户类型选择“普通用户”。如下图：

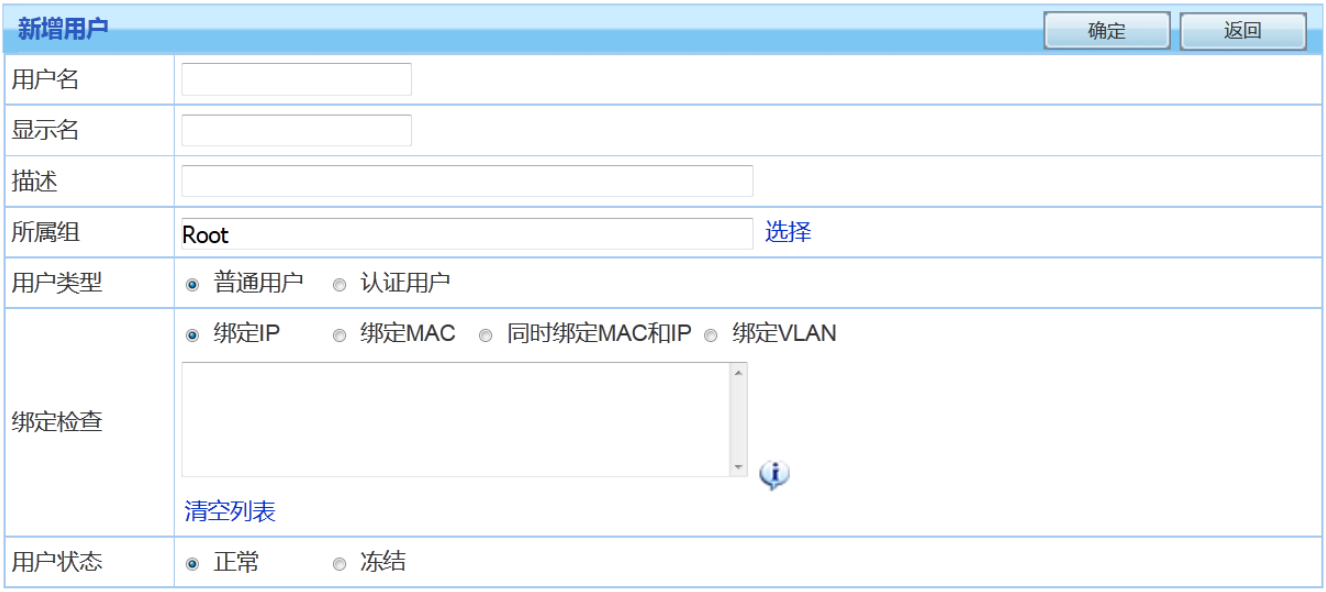


图103.　新增普通用户

参数说明：

- 用户名：用户名称。
- 显示名：用户的别名，如果是以用户的 IP、MAC、主机名等为用户名，在显示名处可填入用户真实的姓名，在统计的时候就会看到真实的姓名，方便记忆。
- 描述：对该用户的一个简单的描述。
- 所属组：默认已经填好刚才进入新增页面时的父组，也可以点击后面的<选择>，就出现选择用户组的框，可改变父组。
- 用户类型：普通用户表示不需密码认证的用户，认证用户表示在上网之前需要输入用户名和密码认证的用户。
- 绑定检查：用来绑定 IP、MAC、IP+MAC 和 VLAN ID，以保证过滤策略的准确有效。普通用户和认证用户的绑定含义不尽相同，将在绑定检查章节详细描述。
- 状态：正常或冻结。正常表示该用户可用，冻结表示暂时不可用。

15.2.6 新增认证用户

功能描述：新增普通用户，并设置子组的上网策略和黑名单控制。

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，点击顶部的<新增用户>按钮，弹出“新增用户”页面，“用户类型”选择“认证用户”。如下图：

图104. 新增认证用户

参数说明：

- 用户名：用户名称。
- 显示名：用户的别名，如果是以用户的 IP、MAC、主机名等为用户名，在显示名处可填入用户真实的姓名，在统计的时候就会看到真实的姓名，方便记忆。
- 所属组：默认已经填好刚才进入新增页面时的父组，也可以点击后面的<选择>，就出现选择用户组的框，可改变父组。
- 用户类型：普通用户表示不需密码认证的用户。认证用户表示在上网之前需要输入用户名和密码认证的用户。
- 绑定检查：用来绑定 IP、MAC、IP+MAC 和 VLAN ID，以保证过滤策略的准确有效。认证用户默认无绑定。普通用户和认证用户的绑定含义不尽相同，将在绑定检查章节详细描述。
- 认证方式：包括本地认证、到外部服务器去认证。本地认证表示在账号放于设备本地，这时候需要为用户设置密码。到服务器去认证，表示到外部服务器去认证，不用设置密码。外部服务器包括：Radius 服务器、LDAP 服务器、AD 服务器。
- 公用账号：表示可以多人同时使用同一账号登录，0 表示不限制登录人数。当超出登录人数时，处理方法包括：本次登录失败/注销已认证的某个登录，本次认证成功。
- 有效期：认证账号的有效使用时间范围。用户有效期，当有效期到了，该账号显示[已过期]，即为不可用。
- 状态：正常或冻结。正常表示该用户可用，冻结表示暂时不可用。

15.2.7 修改用户

功能描述：修改用户的配置

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，点击右边列表中名称列对应的用户的链接。比如要修改 Root/临时用户组下面的 test 用户。先定位到 Root/临时用户组，然后点击名称列的 test 用户的链接，如下图：

图105.　　修改用户 1

第二：进入用户的修改页面，填入需要修改的值。如下图：

图106. 修改用户 2

参数说明：

- 用户名：用户名称，不可修改。
- 显示名：用户的别名，如果是以用户的 IP、MAC、主机名等为用户名，在显示名处可填入用户真实的姓名，在统计的时候就会看到真实的姓名，方便记忆。
- 描述：对该用户的一个简单的描述。
- 所属组：默认已经填好刚才进入新增页面时的父组，也可以点击后面的<选择>，就出现选择用户组的框，可改变父组。
- 用户类型：普通用户表示不需密码认证的用户，认证用户表示在上网之前需要输入用户名和密码认证的用户。
- 绑定检查：用来绑定 IP、MAC、IP+MAC 和 VLAN ID，以保证过滤策略的准确有效。普通用户和认证用户的绑定含义不尽相同，将在绑定检查章节详细描述。
- 状态：正常或冻结。正常表示该用户可用，冻结表示暂时不可用。

15.2.8 绑定检查

绑定检查用来绑定 IP、MAC、IP+MAC 和 VLAN ID，以保证过滤策略的准确有效。普通用户和认证用户的绑定含义不尽相同，以下为详细描述。

- 普通用户：必须要选择一个绑定检查条件，即在IP、MAC、IP+MAC 和 VLAN ID 的绑定检查条件中选择一个，默认选择了“绑定IP”。当绑定IP、或绑定MAC、或绑定 VLAN ID 时，表示符合绑定条件的流量会被统计到该用户名上。当绑定IP+MAC 时，表示符合绑定条件的流量会被统计到该用

户名上的同时，还会对IP和MAC进行绑定检查，如果IP和MAC地址不相符，就不能上网。

- 认证用户：默认选择“不绑定”，即没有绑定任何条件。也可在IP、MAC、IP+MAC 和 VLAN ID 的绑定检查条件中选择一个。当绑定了任何条件，认证时，用户名必须要和绑定条件一致，才能认证成功，否则认证失败，主要是为了防止用户名被盗用。比如，用户名为Tom的用户绑定了IP为172.16.5.3，那么只有从IP地址为172.16.5.3的机器上用“Tom”的用户名进行认证才能认证成功。

15.2.8.1 绑定 IP

功能描述：绑定用户的 IP 地址

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，然后进入新增或修改用户页面，进行 IP 绑定。下面以新增用户页面来说明，如下图：

图107. 绑定 IP

第二：在绑定检查一行，选择“绑定 IP”，输入需要绑定的 IP 地址。一个用户可以绑定一个或多个 IP 地址。IP 地址格式范例为：192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/255.255.0.0 或 192.168.0.0/16 。

<清空列表>按钮可以清空输入框内已填入的 IP 地址。

15.2.8.2 绑定 MAC

功能描述：绑定用户的 MAC 地址

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，然后进入新增或修改用户页面，进行 MAC 绑定。下面以新增用户页面来说明，如下图：

图108.　　绑定 MAC

第二：在绑定检查一行，选择“绑定 MAC”，输入需要绑定的 MAC 地址。一个用户可以绑定一个或多个 MAC 地址。MAC 地址格式范例为：00:45:AD:CC:D1:67 或 00:45:AD:CC:D1:BC#(192.168.100.20)，括号里面的 IP 地址是对 MAC 的注释。

<清空列表>按钮可以清空输入框内已填入的 MAC 地址。

<扫描 MAC 地址>按钮可以扫描某个（些）IP 的 MAC 地址。点击<扫描 MAC 地址>，然后在“扫描起始 IP”和“扫描结束 IP”里面填入要扫描的 IP 地址，再点击<立即扫描>按钮，即可扫描出对应 IP 的 MAC 地址。如下图：

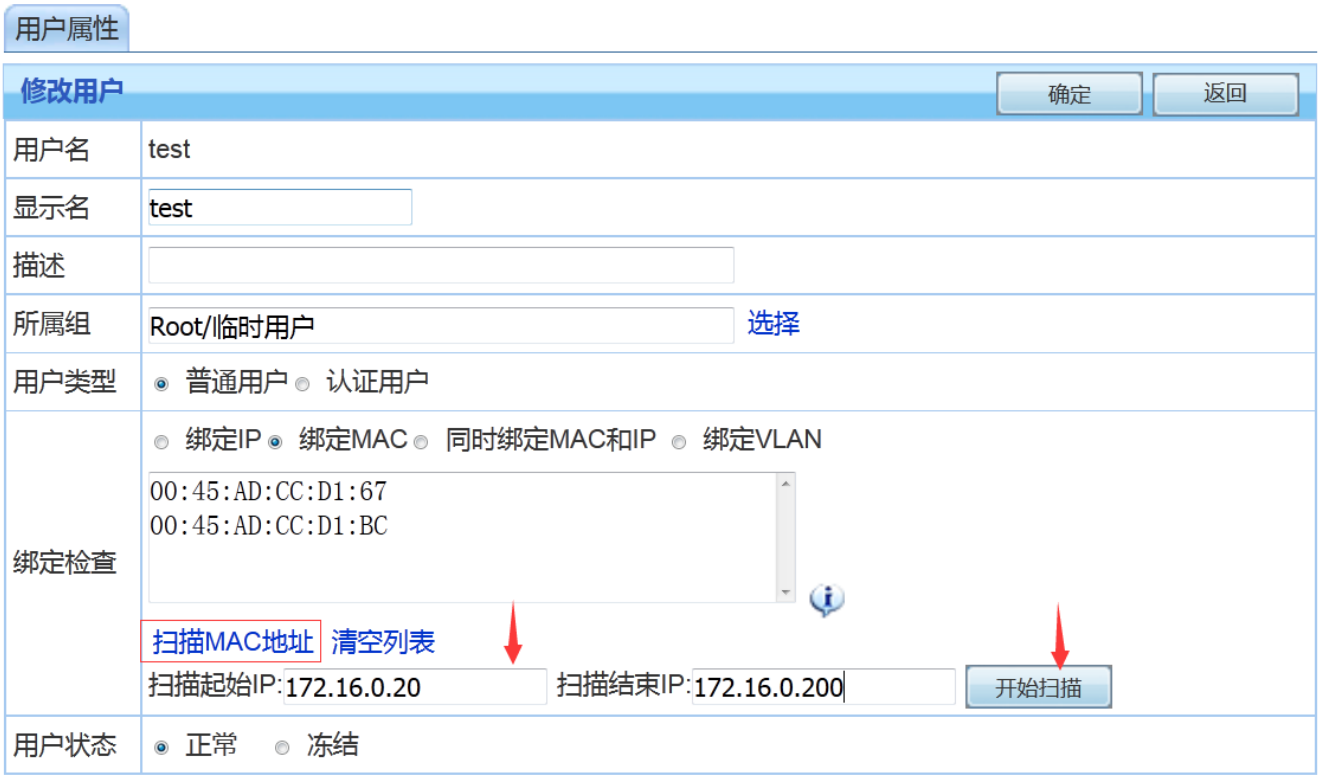


图109. 绑定 MAC-扫描 MAC

图110. 绑定 Mac-扫描 Mac 结果

扫描的结果会自动填入输入框内，MAC 地址后面的 IP 是表示改 MAC 当前对应的 IP 地址，是对 MAC 扫描完成的一种注释。新增完成，点击修改，查看注释已经去掉。

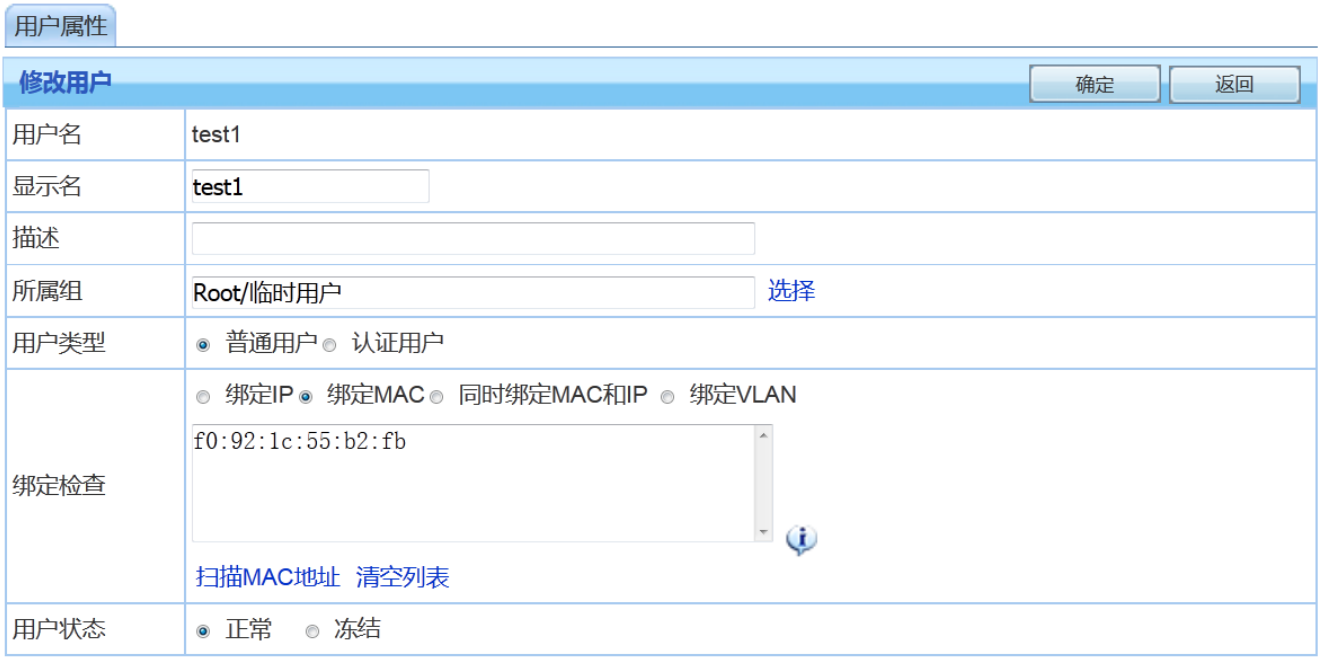


图111.　绑定 Mac-扫描 Mac 完成后查看该用户

提示：

1、此处的扫描 MAC 地址是设备通过 NetBIOS 协议去扫描的，而不是依靠的 SNMP 协议去三层交换机上获取，所以此处的扫描需要内网计算机支持并启用了 NetBIOS 协议，且三层交换机没有对 NetBIOS 协议做限制。

2、当跨三层交换机的网络需要绑定 MAC 地址时，必须开启 SNMP 选项功能。具体配置详见【用户认证>认证选项> 跨三层 MAC 识别】

15.2.8.3　绑定 IP+MAC

功能描述：绑定用户的 IP 和 MAC 地址

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，然后进入新增或修改用户页面，进行 IP+MAC 绑定。下面以新增用户页面来说明，如下图：

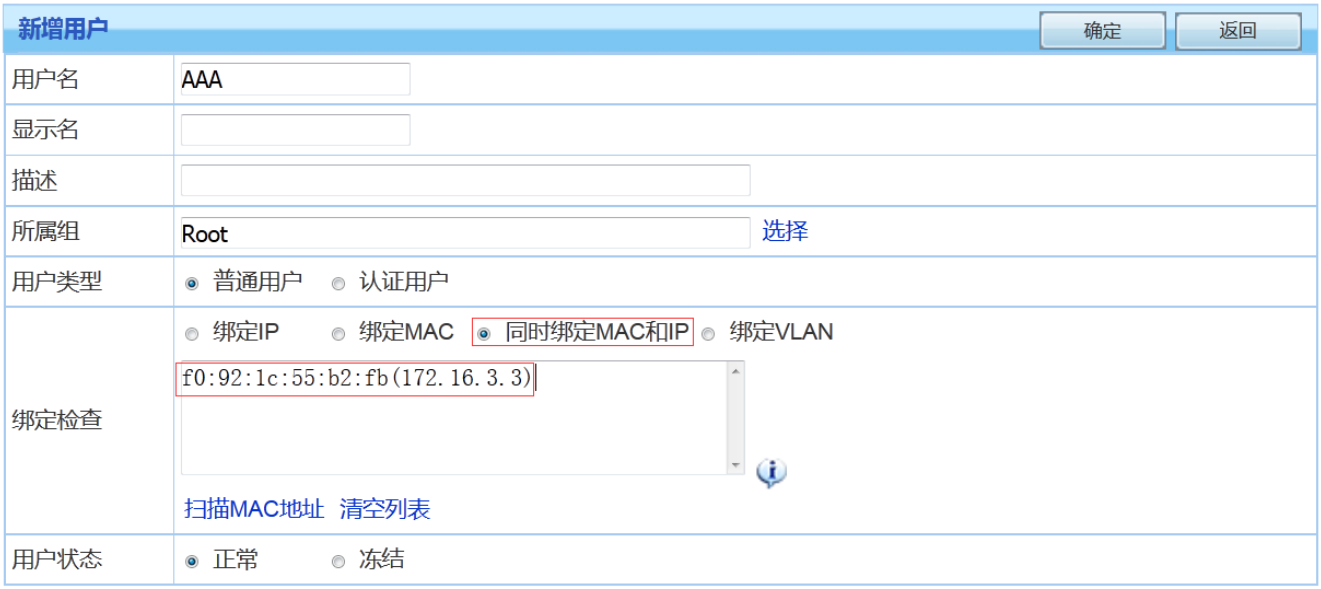


图112.　　绑定 IP+MAC

第二：在绑定检查一行，选择“同时绑定 IP 和 MAC”，输入需要绑定的 IP 和 MAC 地址。一个用户可以绑定一个或多个 IP+MAC。格式范例为 172.16.3.3(00:24:8C:51:24:23)。

<清空列表>按钮可以清空输入框内已填入的 IP+MAC 地址。

<扫描 MAC 地址>按钮可以扫描某个（些）IP 的 MAC 地址。点击<扫描 MAC 地址>，然后在“扫描起始 IP”和“扫描结束 IP”里面填入要扫描的 IP 地址，再点击<开始扫描>按钮，即可扫描出对应 IP 的 MAC 地址。如下图：

图113.　　绑定 IP+MAC-扫描 MAC

提示：

1、 此处的扫描 MAC 地址是设备通过 NetBIOS 协议去扫描的，而不是依靠的 SNMP 协议去三层交换机上获取，所以此处的扫描需要内网计算机支持并启用了 NetBIOS 协议，且三层交换机没有对 NetBIOS 协议做限制。

2、 当跨三层交换机的网络需要绑定 MAC 地址时，必须开启 SNMP 选项功能。具体配置详见【用户认证> 认证选项> 跨三层 MAC 识别】

15.2.8.4 绑定 VLAN

功能描述：绑定用户的 VLAN ID

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，然后进入新增或修改用户页面，进行 VLAN 绑定。下面以新增用户页面来说明，如下图：

图114. 绑定 VLAN

第二：在绑定检查一行，选择“绑定 VLAN”，输入需要绑定的 VLAN ID。一个用户可以绑定一个或多个 VALN。格式范例：108 或 121-123。

<清空列表>按钮可以清空输入框内已填入的 VLAN ID。

当报文里携带的 VLAN Tag 与绑定的 VLAN ID 不一致时，表示绑定检查失败。

15.2.9 导出用户和组

功能描述：导出用户和组的配置

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，勾选要导出的组和用户，然后点击<导出>按钮，如下图：

图115.　　导出用户和组

第二：将选中的用户和组保存到 PC。如下图：

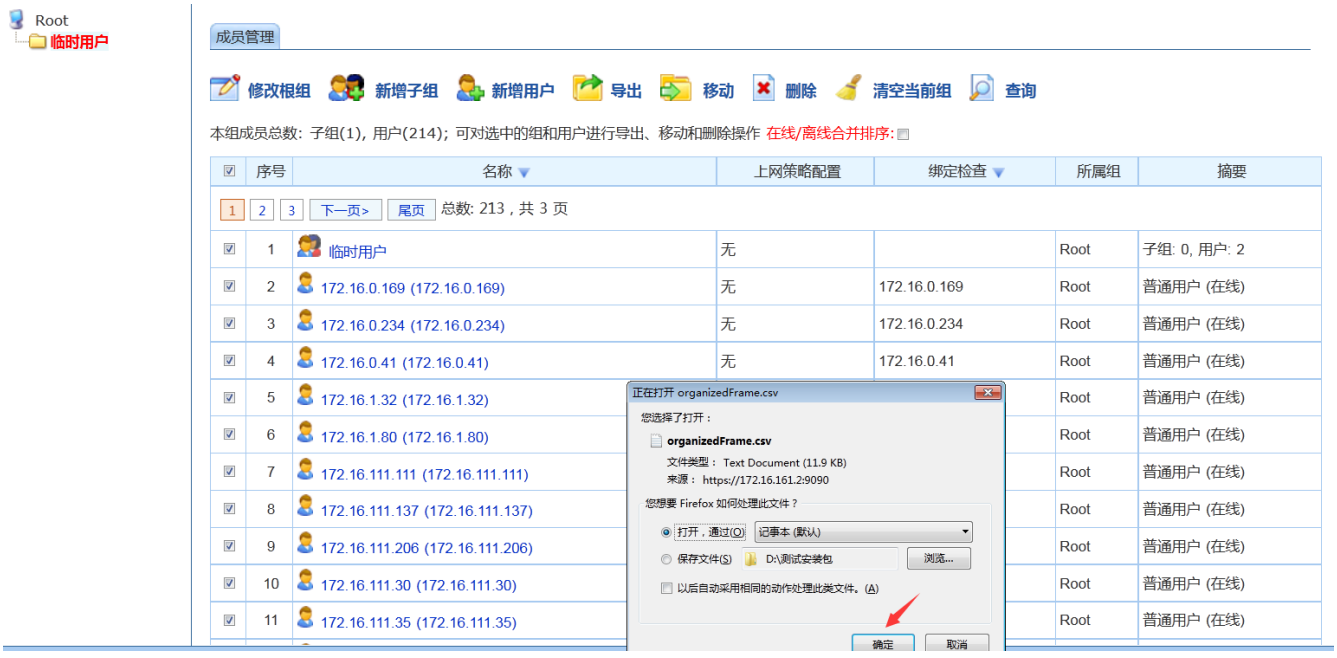


图116.　　组织结构-导出用户和组 2

15.2.10 移动用户和组

功能描述：移动用户和子组从 A 组移动到 B 组。

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，勾选要移动的组和用户，然后点击<移动>按钮，如下图：

图117. 组织结构-移动用户和组 1

第二：弹出移动框，然后输入将被移动到的目的组的路径。也可以点击输入框后面的<选择>按钮，选择目的组。如下图：

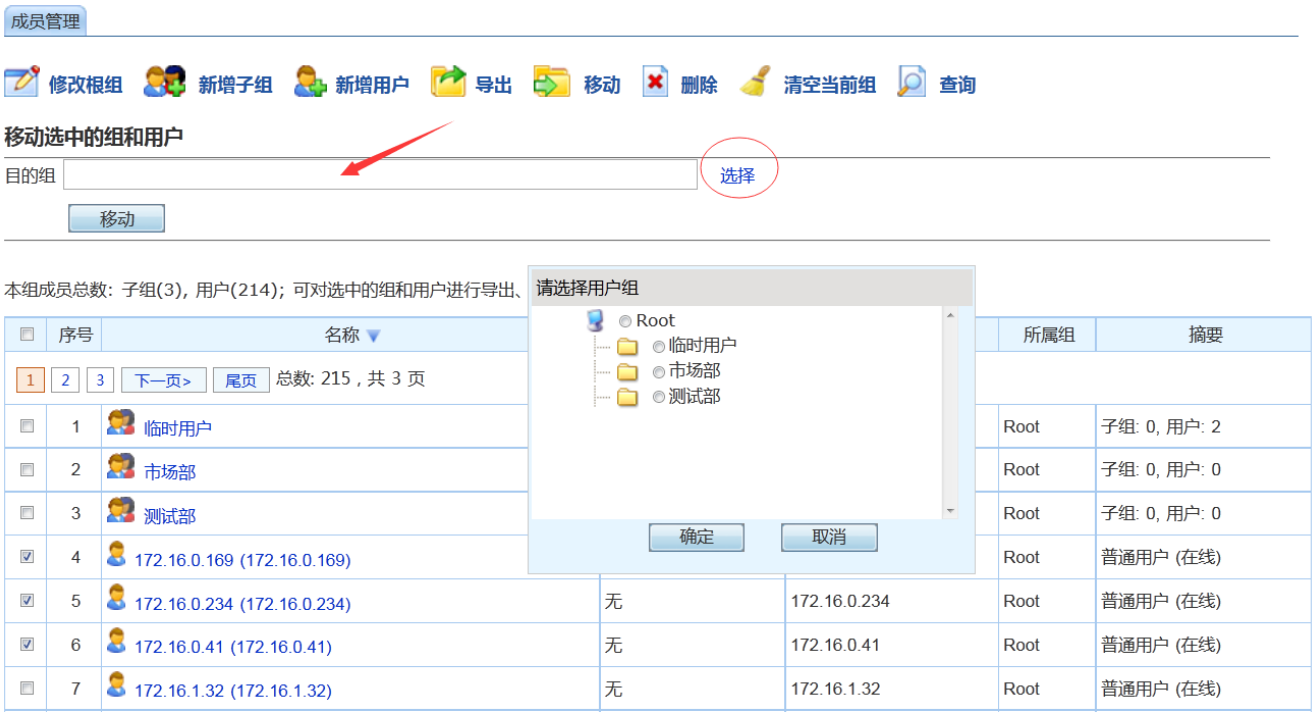


图118.　组织结构-移动用户和组 2

第三：选择好目的组后，点击目的组下面的<移动>按钮，移动已选中的用户和组。

15.2.11　删除用户和组

功能描述：删除用户和组。

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，浏览定位相应的组，勾选要删除的组和用户，然后点击<删除>按钮，如下图：

图119.　　组织结构-删除用户和组

第二：弹出询问框“确定要删除吗？”，点击<确定>即删除选中的用户和组，点击<取消>回到原来页面。

15.2.12　查询用户和组

功能描述：查询用户和组

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，然后点击<查询>按钮，弹出查询框。如下图：

图120.　　组织结构-查询用户和组

第二：输入查询条件，然后点击<查询>按钮，查询整个组织结构中符合条件的用户或组。

15.2.13 在线离线合并排序

功能描述：在线离线合并排序

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面，然后勾选<在线离线合并排序>。如下图：

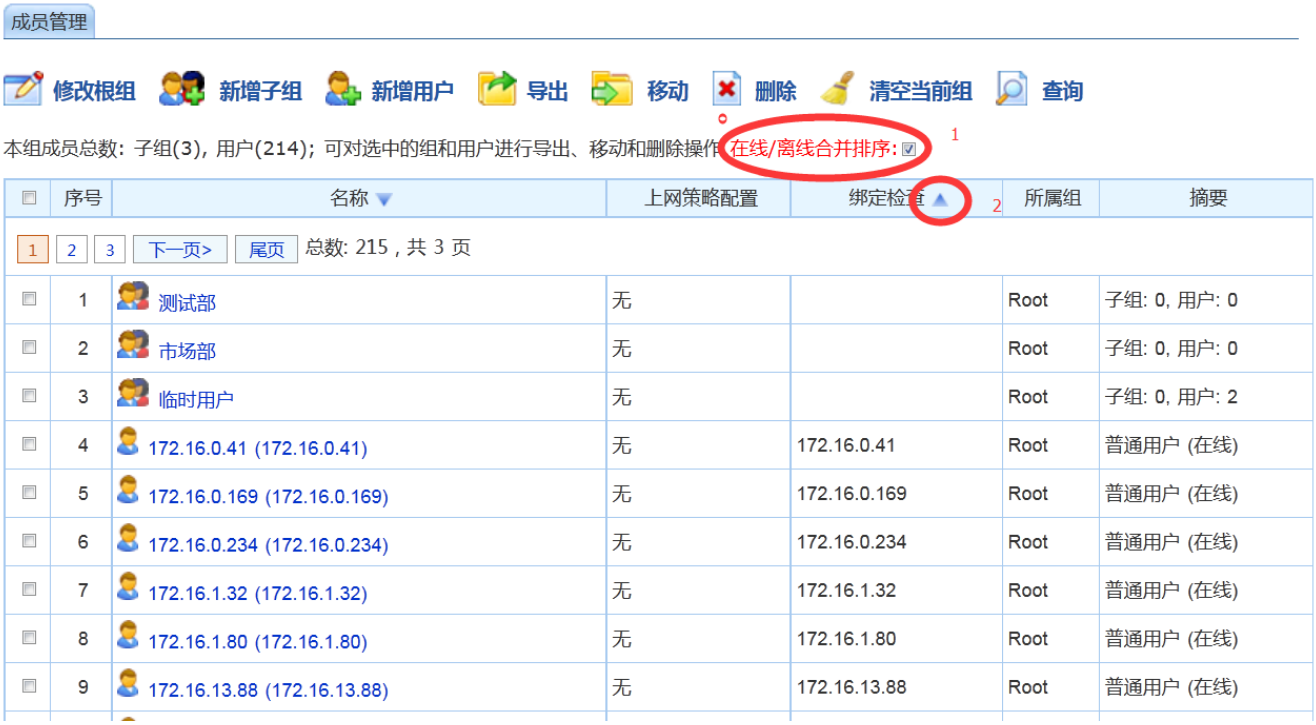


图121. 组织结构-在线离线合并排序

第二：点击<绑定检查>，根据升序/降序的方式进行在线离线用户排序。

15.2.14 清空当前组

功能描述：清空当前组

配置路径：【用户认证】>【组织结构】

配置描述：

第一：进入【组织结构】页面。如下图：

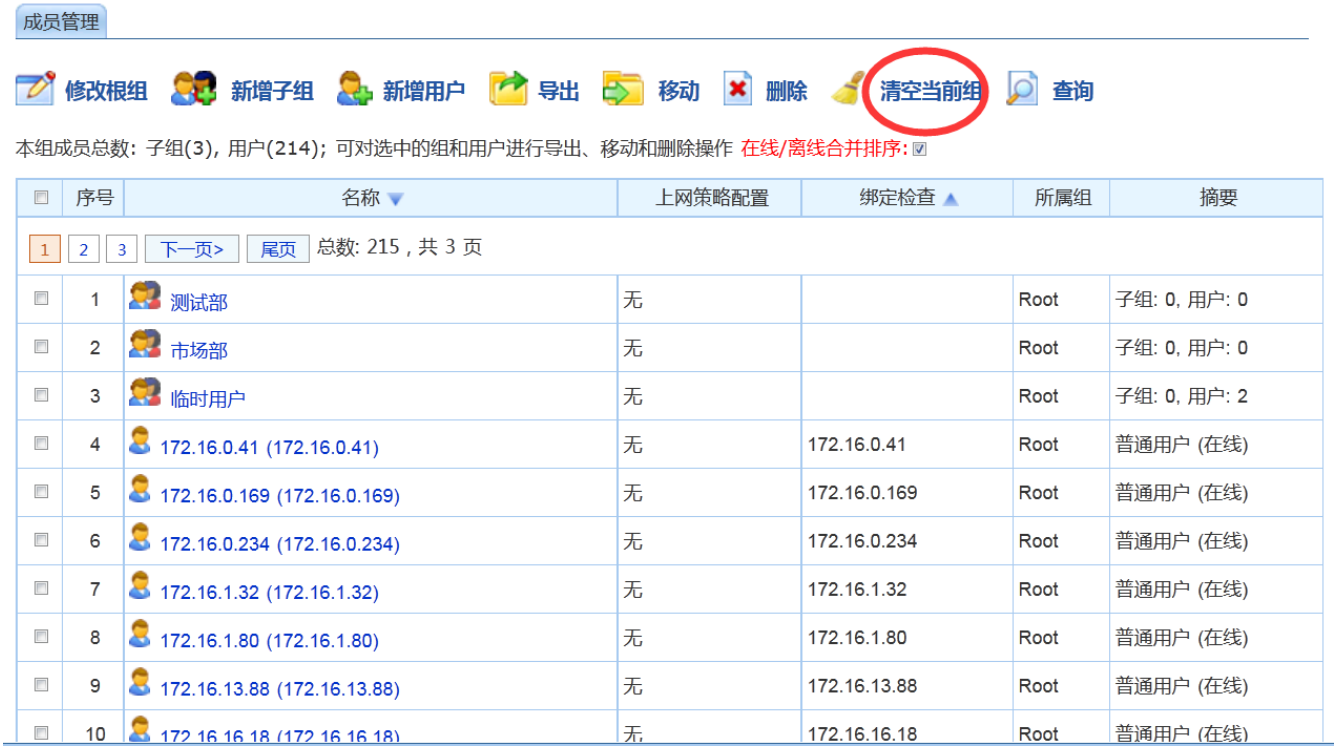


图122.　　组织结构-清空当前组

第二：点击 Root 下面任意一组，点击清空当前组按钮，所选择的组中的用户即被清空。

15.3 认证选项

认证选项包含跨三层 MAC 识别、认证参数、终端提示页面定制、未认证权限和短信认证的配置。

15.3.1 跨三层 MAC 识别

功能描述：用在三层环境下绑定 MAC 或绑定 IP+MAC 进行上网认证的实现方式。设备将主动去读取三层交换机上的内网主机的 MAC 地址。

配置路径：【用户认证】>【认证选项】>【跨三层 MAC 识别】，配置页面如下：

图123. 跨三层 MAC 识别

参数说明：

- 功能状态：选择<启用>或<禁用>开启或关闭“跨三层MAC识别”功能。当跨三层的交换机的网络需要绑定MAC地址时, 必须开启此功能。
- SNMP服务器列表：三层交换机的 IP 地址、MAC 地址、SNMP 的 Oid 和三层交换机的 community。一行一个服务器, 最多支持64个。格式为：IP/MAC/Oid/Community，IP 和 MAC 为三层交换机离设备最近的接口的 IP 和 MAC 地址。Oid一般为 .1.3.6.1.2.1.4.22.1.2 和 .1.3.6.1.2.1.3.1.1.2， 例如：192.168.2.1/00:01:03:0A:EF:03/.1.3.6.1.2.1.4.22.1.2/public
- 超时设置：访问三层交换机的超时时间。保持默认值即可。
- 访问间隔：访问三层交换机的间隔，用于配置设备多久去三层交换机上取一次内网用户的 MAC 地址表。保持默认值即可。

> **提示：**
>
> 1、 如果启用“SNMP 选项”功能，三层交换机必须支持 SNMP 服务，并正确配置三层交换机的 Community 和 SNMP 版本（版本为 v2）
>
> 2、 比如，在实例中内网有 3 台三层交换机，其中一台为核心交换机，另外两台分别为连接到核心交换机的三层交换机 A 和 B，A 和 B 分别连接到内网的两个部门。则三台交换机的 IP/MAC/Oid/Community 都必须填入到 SNMP 服务器列表中。核心交换机不要求一定能支持 SNMP，但是设置 SNMP 选项时必须要把核心交换机的 IP、MAC 填写进去，在不支持 SNMP 时，oid 和 community 可以随便设置。

15.3.2 认证参数

功能描述：设置 WEB 认证客户端相关的参数。

配置路径：【用户认证】>【认证选项】>【认证参数】，配置页面如下：

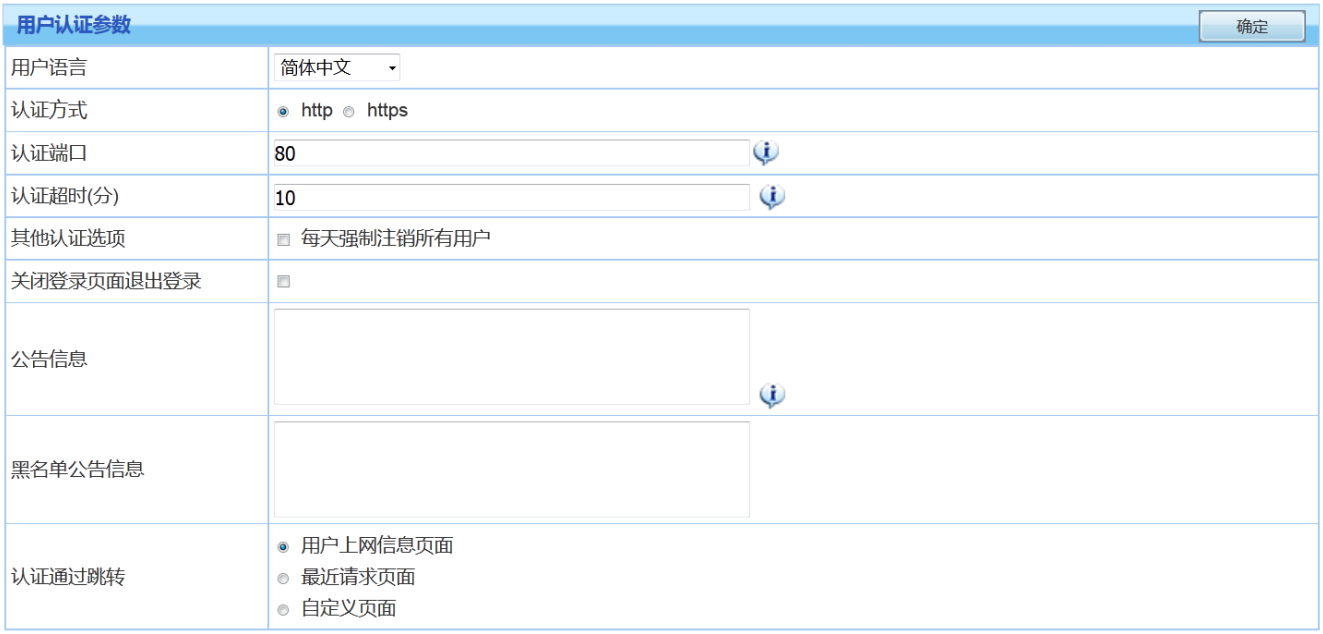


图124.　　配置认证参数

参数说明：

- 用户语言：选择认证界面显示的语言
- 认证方式：现在认证过程使用的协议，有[HTTPS]和[HTTP]两种，默认[HTTP]。
- 认证端口：[HTTP]认证方式的认证端口，默认80。[HTTPS]认证方式的端口固定为443，如果网管端口为443，则不能将认证端口设置为[HTTPS]的方式。
- 认证超时：认证成功后，在设定的时间内用户没有上网流量，认证用户自动下线。
- 其他认证选项：每天24:00注销所有用户，默认不启用。
- 关闭登录页面退出登录：关闭认证通过的页面，强制注销当前认证，默认不启用。
- 认证成功页面：认证成功后浏览器自动跳转到此处配置的网页。
- 公告信息：管理员可以设置一些信息公告给每个用户，将在认证客户端页面显示。
- 黑名公告信息：管理员可以设置一些信息公告给每个用户，将在用户进入黑名单时显示到客户端。
- 认证通过跳转：认证成功后的跳转页面。
  - 用户上网页面信息：用户认证成功的页面，系统内置。主要包含上下线时间、在线时长、今日流量使用情况、当前活跃服务、最近一月流量、公告信息。
  - 最近请求页面：如访问www.baidu.com 弹出认证界面，认证通过后自动跳转到www.baidu.com 。
  - 自定义页面：认证通过后自动跳转到该自定义网站。

15.3.3 终端提示页面定制

功能描述：自定义 WEB 认证客户端登录界面的风格与参数

配置路径：【用户认证】>【认证选项】>【终端提示页面定制】，配置页面如下：

图125.　　自定义终端页面

15.3.3.1　认证页面

功能描述：自定义 WEB 认证客户端登录界面的风格与参数

配置路径：【用户认证】>【认证选项】>【终端提示页面定制】>【认证页面】，配置页面如下：

图126.　　系统内置认证页面

参数说明：

- 预览：可分别预览电脑、手机上的认证效果图。
- 修改：可直接修改系统内置的页面，修改的内容包括认证页面网页标题、logo图片、页面内容、背景颜色、免责声明、广告图片。
- 复制：可直接复制系统内置的模板，生成新的认证界面，可在此模板修改成新的认证界面。
- 恢复初始页面：恢复为系统内置的认证页面。
- 上传页面：新增自定义页面，效果图如下：

图127.　　自定义认证页面

- ✧ 页面名称：认证页面名称。
- ✧ 描述：认证页面备注信息。
- ✧ 页面文件：通过界面[下载示例]，下载模板，自定义生成的页面文件（zip压缩文件）。

  密码认证、短信认证需勾选[短信认证页面]，否则认证策略选择相应的认证方式，找不到对应的认证页面。

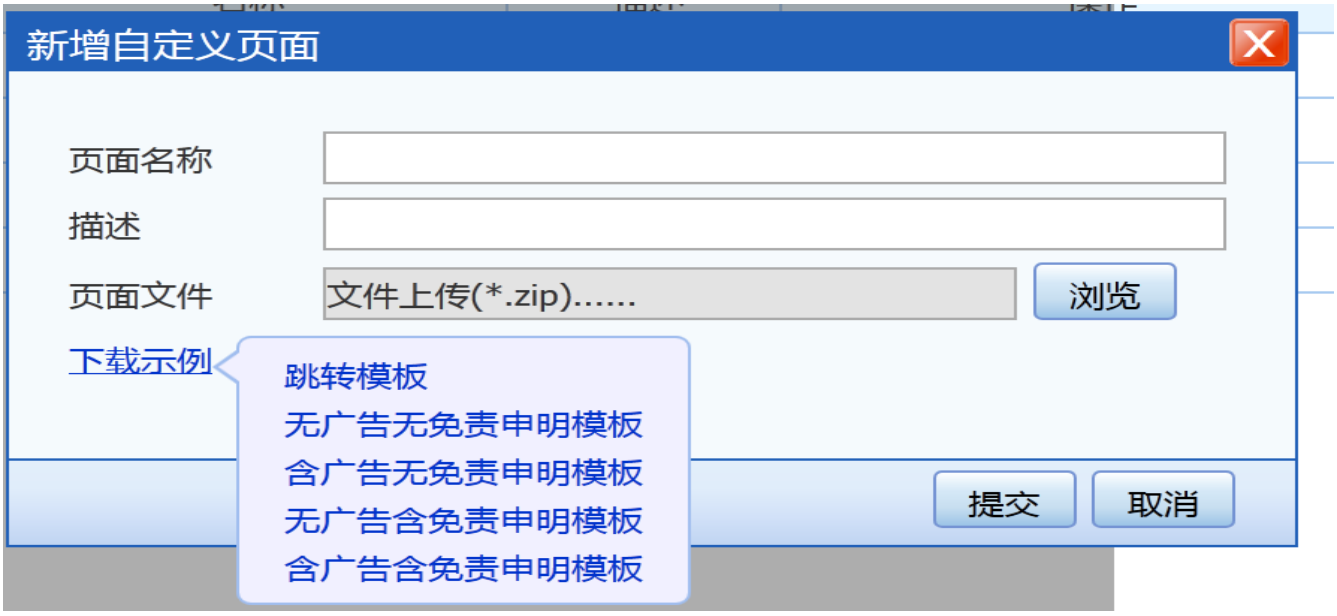


图128.　　自定义认证页面-模板

15.3.3.2 认证成功

功能描述：自定义 WEB 认证客户端认证成功的风格与参数

配置路径：【用户认证】>【认证选项】>【终端提示页面定制】>【认证成功】，配置页面如下：

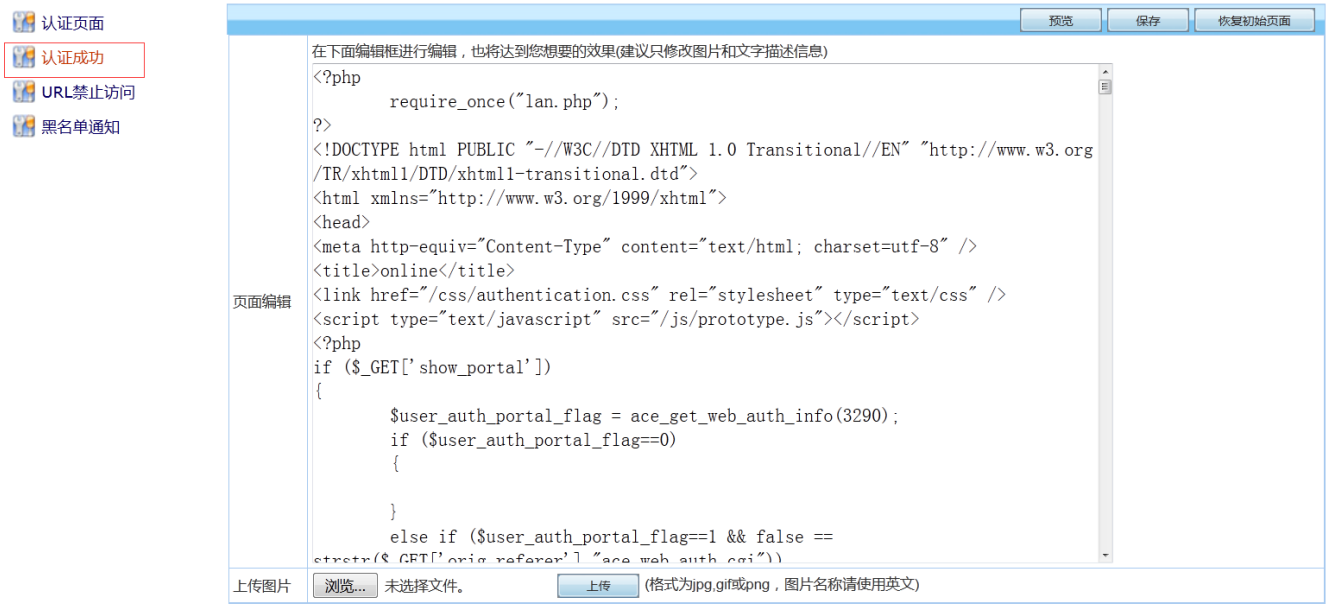


图129. 认证成功页面

参数说明：

- 预览：预览当前客户认证成功的页面。
- 保存：保存客户当前认证成功的页面。
- 恢复初始页面：恢复到设备初始认证成功的页面。
- 上传图片：上传页面需要显示的图片，格式为jpg、gif或png，图片名称必须使用英文。

15.3.3.3 URL 禁止访问

功能描述：当设备开启了URL过滤功能，用户访问被设备拒绝的网站的时候，会弹出URL禁止访问提示页面，URL过滤配置详见。【内容安全>应用内容过滤>上网策略>URL过滤】

配置路径：【用户认证】>【认证选项】>【终端提示页面定制】>【URL 禁止访问】，配置页面如下：

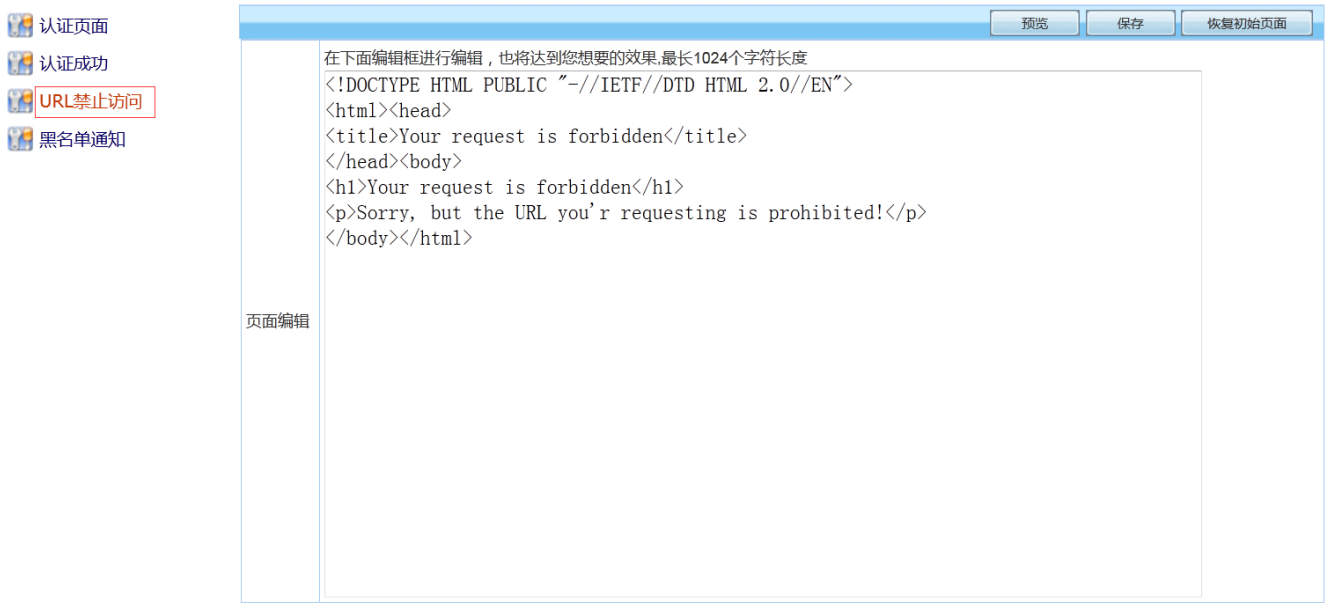


图130.　　URL 禁止访问页面

参数说明：

- 预览：预览当前客户认证成功的页面。
- 保存：保存客户当前认证成功的页面。
- 恢复初始页面：恢复到设备初始认证成功的页面。

案例 1：修改提示信息为“对不起，您访问的网站不合法”，修改完成后，点击**保存**

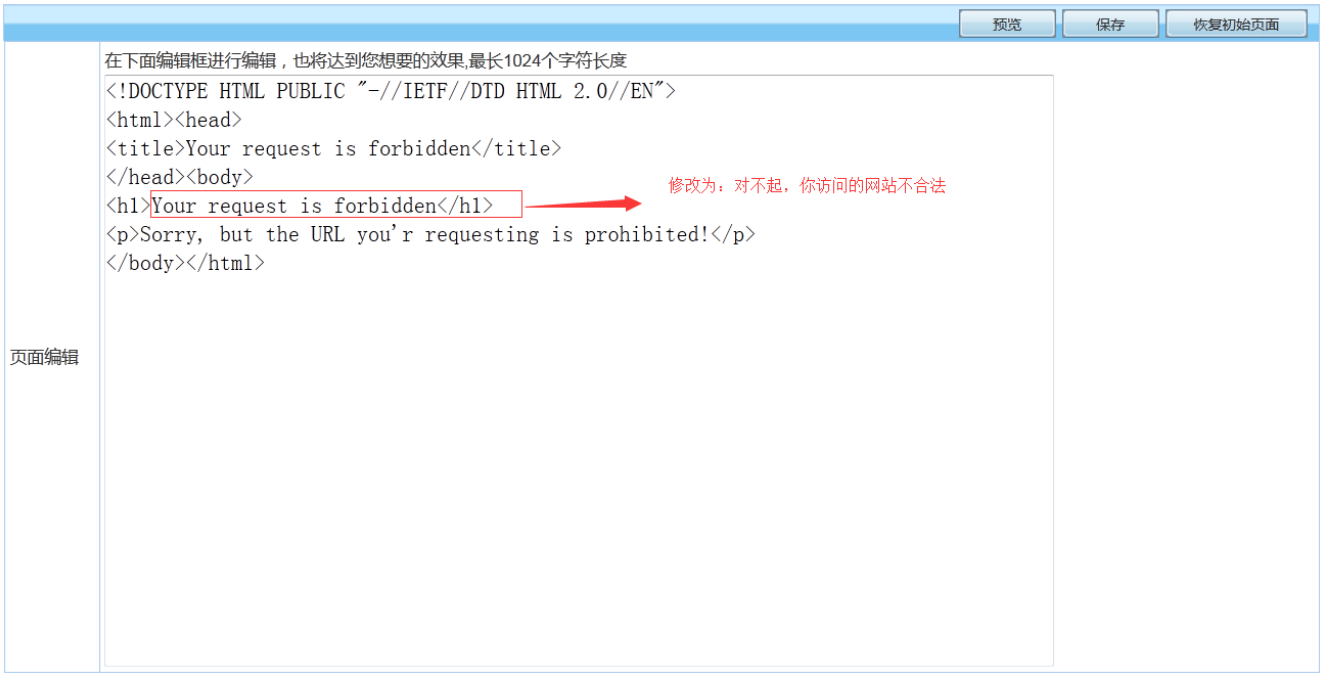


图131.　　URL 禁止访问页面-修改后

修改后，可点击预览查看效果：

图132.　效果对比

15.3.3.4　黑名单通知

功能描述：用户加入黑名单后，访问网站会弹出黑名单通知页面，黑名单策略配置详见【策略流控>黑名单策略】。

配置路径：【用户认证】>【认证选项】>【终端提示页面定制】>【黑名单通知】，配置页面如下：

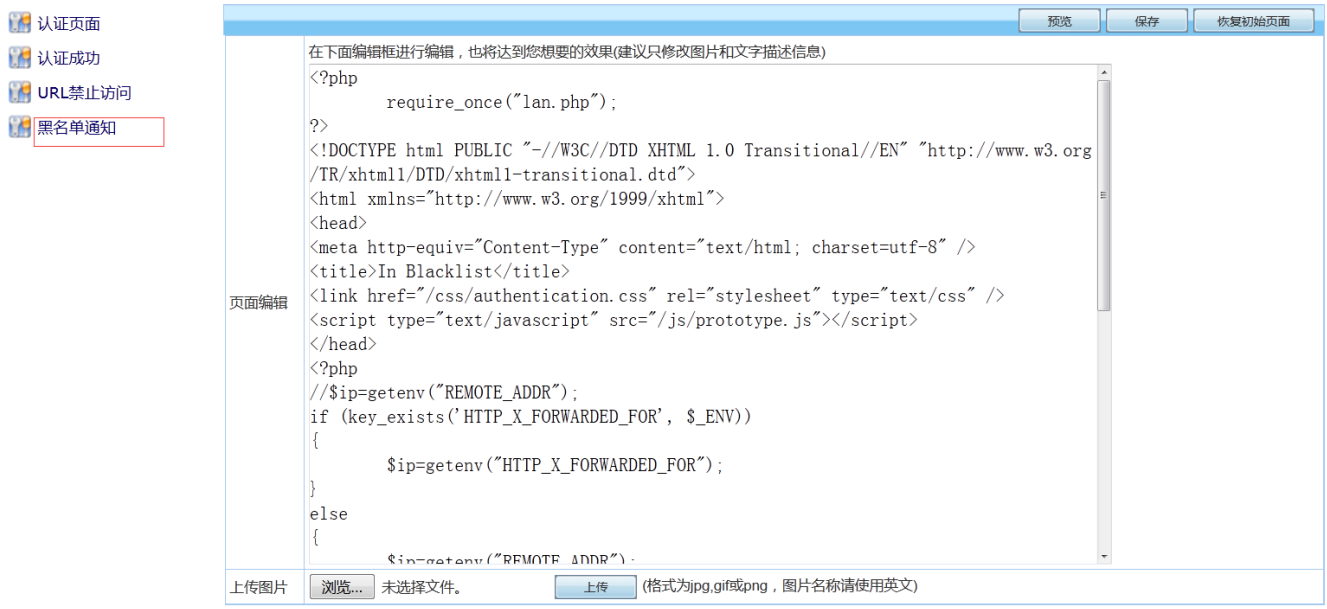


图133.　黑名单通知页面

参数说明：

- 预览：预览当前客户认证成功的页面。
- 保存：保存客户当前认证成功的页面。
- 恢复初始页面：恢复到设备初始认证成功的页面。
- 上传图片：上传页面需要显示的图片，格式为jpg、gif或png，图片名称必须使用英文。

案例1：

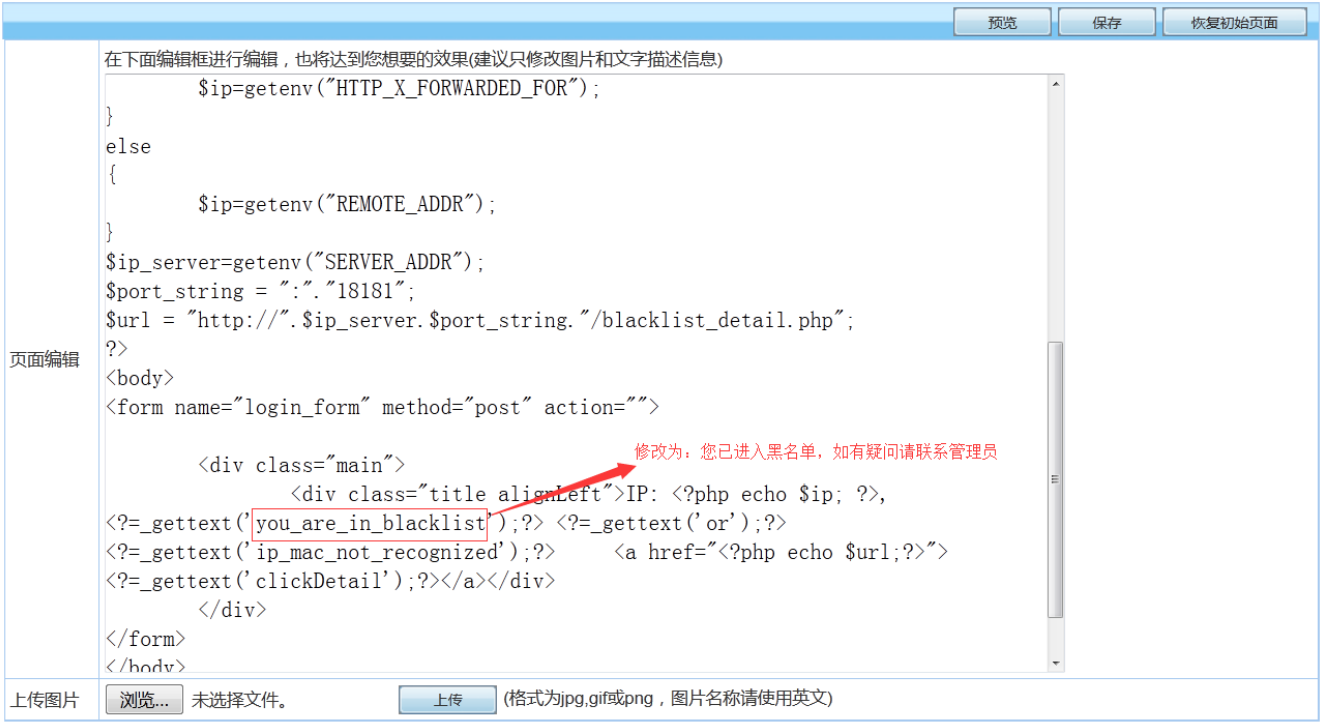


图134.　　黑名单通知-修改后

可点击预览查看修改效果图：

图135.　　修改后效果图

15.3.4 未认证权限

配置描述：进入【未认证权限】页面，[当用户未通过认证时可以访问 DNS 和 Ping 服务]默认已勾选，即未通过认证的用户可以访问 DNS 和 Ping 服务。其它服务禁止访问，若未认证用户需要访问更多的服务，可要在[未认证权限策略]处添加策略。配置页面如下：

配置路径：【用户认证】>【认证选项】>【未认证权限】，配置页面如下：

图136.　　未认证权限

点击<删除所有>，将删除所有的策略。

点击<计数清零>，将清除匹配计数数值为0，重新统计匹配数。

改变状态栏复选框的值，再点击<修改状态>，可修改策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有策略的状态。

点击<修改>，修改本条策略的参数，但不能修改本条策略的方向。

点击<插入>，在当前位置之前插入一条策略。

点击<移动>，改变对应策略的序号，从而改变策略的优先级。

点击<删除>，删除本条策略。

点击<新增>，新增策略，如下图：

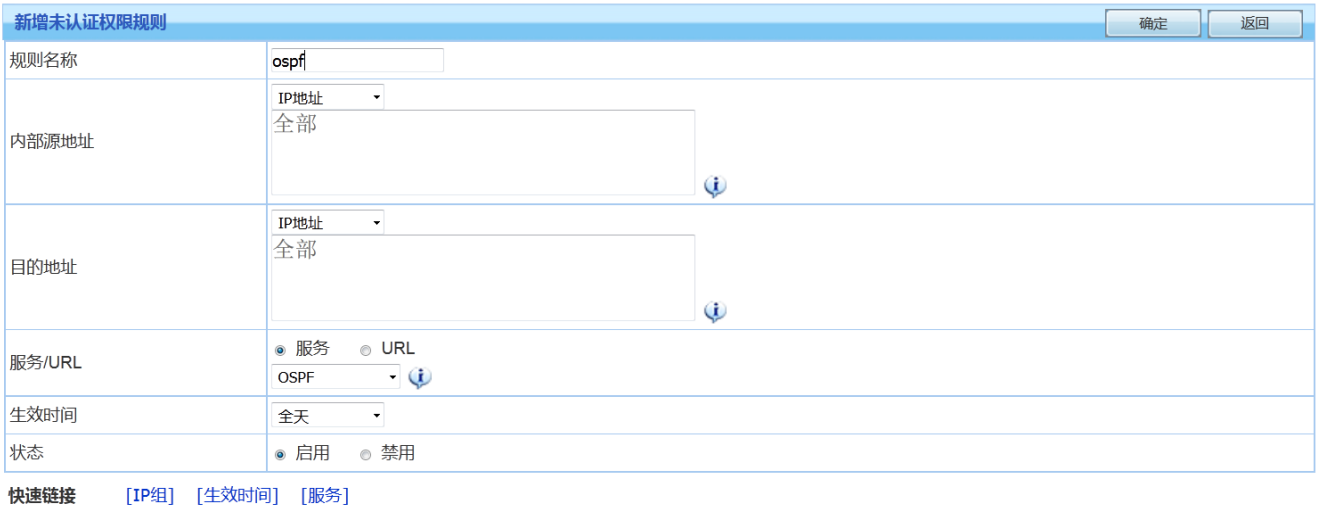


图137.　　新增策略 1

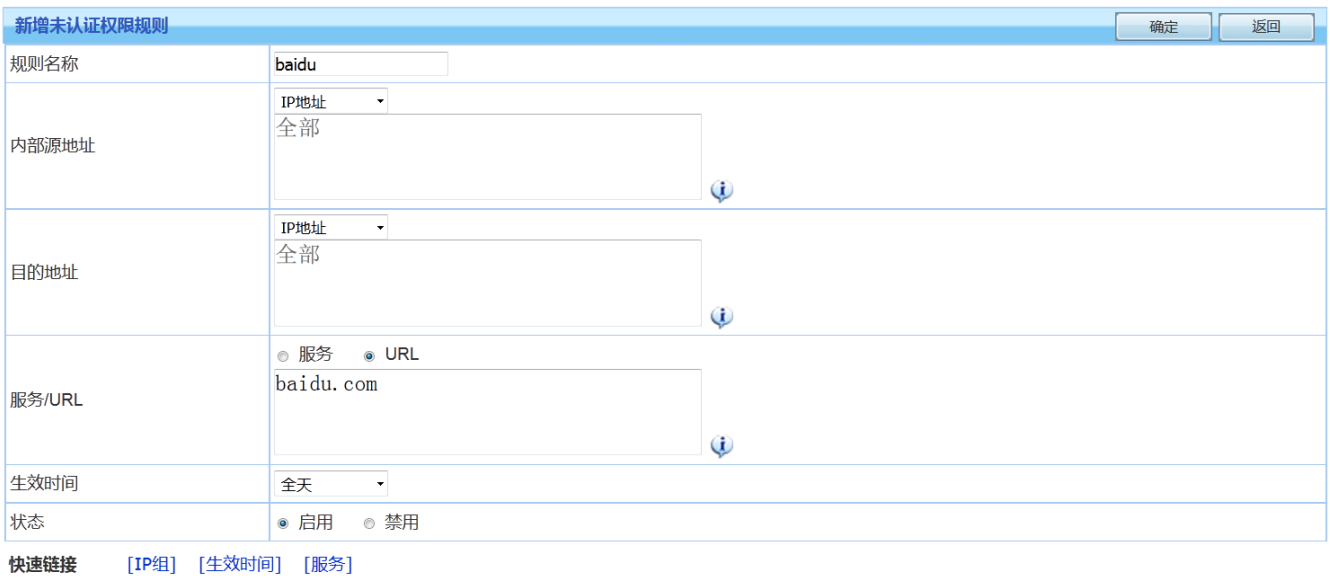


图138.　　新增策略 2

参数说明：

- 内部源地址：数据流的源地址（内网主机地址），可输入 IP 地址或选择地址簿。地址簿在【系统对象>IP组】中配置。
- 目的地址：数据流的目的地址，可输入 IP 地址或选择地址簿。
- 服务/URL：数据流的服务类型/目的网站域名。
- 生效时间：本策略的有效时间段。
- 状态：启用或禁用本规则，默认启用。

15.3.5 短信认证

配置描述：用于设置通过短信认证方式进行认证的相关参数。

配置路径：【用户认证】>【认证选项】>【短信认证】，如下图：

图139. 短信认证

参数说明：

- 功能状态：勾选“启用短信认证功能”即可开启短信认证功能。
- 短信内容：可根据自己的需求，对短信内容进行编辑。点击“恢复初始内容”，就可以将自定义短信的内容恢复为默认值。
- 免认证设置：勾选“已通过短信认证的用户启用以下免认证信息”则可以根据下面的设置对用户进行免认证。不勾选“已通过短信认证的用户启用以下免认证信息”，则终端每次上线都需获取验证码，输入手机号+验证码认证通过才能上网。
- 有效时长：用户认证通过后的有效时长。可选择“分钟”、“小时”、“天”。如设置成1小时，则手机获取到验证码，使用手机号+验证码认证通过后，一个小时之内反复上下线都无需认证，可直接上线。

- 免认证类型：有“基于浏览器的COOKIE”和“基于mac地址”两种。如果选择“基于浏览器的COOKIE”，则在有效时长内只要浏览器 Flash cookie 值相同就不需要再次进行认证，否则需要重新认证；如果选择“基于mac地址”，则在有效时长内只要用户的mac值相同就不需要再次进行认证，否则需要进行重新认证。
- 认证后跳转：可选择“最近访问页面”和“认证成功页面”。如选择“最近访问页面”，则在认证成功后，就会跳转至最近打开的页面；如果选择“认证成功页面”，认证成功后则会跳转至设备的认证成功页面。
- 参数设定：用来定义短信认证的参数。
- 网关类型：可选择“GSM短信猫”、“CDMA短信猫”、“HTTP协议”、“电信运营商”、及“自定义的服务器”
  - 选择“GSM 短信猫”及“CDMA 短信猫“，需要准备短信猫和电话卡，将短信猫连接在设备的 usb 接口即可。如下图所示：

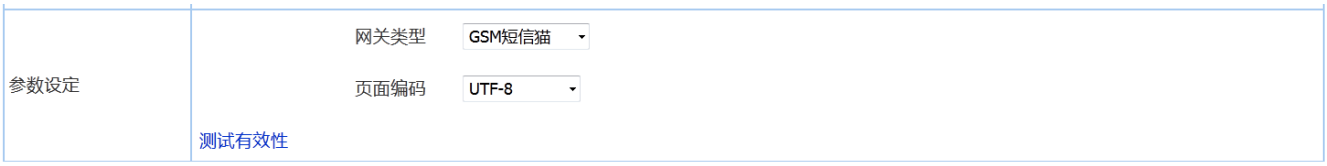


图140.　　网关类型－GSM 短信猫

选择“HTTP 协议”，则还需要填写以下参数，如下图所示：

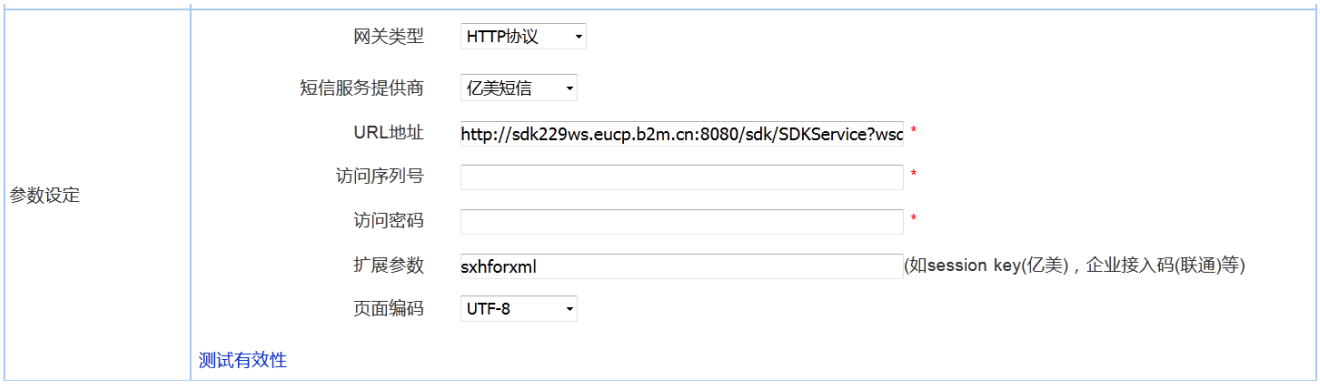


图141.　　网关类型－HTTP 协议

短信提供商现在支持以下几种：亿美短信、互亿无线、Lousimao、浙江联通、浙江移动、国宇短信等。如下图所示：

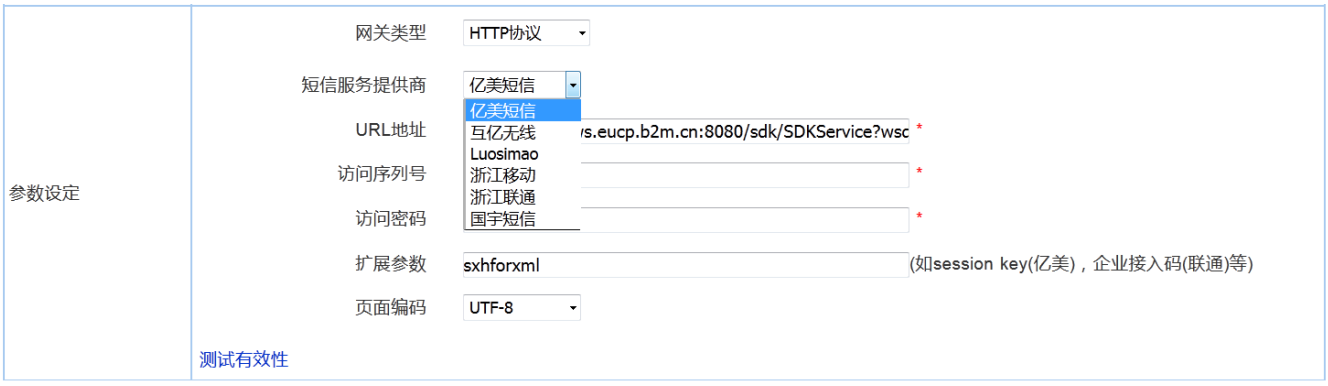


图142.　　设备支持的短信网关类型

- URL地址：填写由短信提供商提供的URL地址即可。
- 访问序列号：填写由短信提供商提供的访问序列号即可。
- 访问密码：填写由短信提供商提供的密码即可。
- 扩展参数：可选，可以为空，如果有的话，请向短信提供商销售人员获取。
- 页面编码：支持UTF-8和GBK。
    - ✧ 选择电信运营商，现在只支持北京移动。需要填写以下参数，如下图所示：

图143. 网关类型－电信运营商

- 服务器地址：电信运营商提供的服务器地址。
- 服务器端口：电信运营商提供的服务器端口地址。
- 企业代码： 申请的时候用的企业代码。
- 业务代码：电信运营商提供的业务代码。
- Sp接入号：电信运营提供的SP接入号。
- 网关编号：电信运营商提供的网关编号。
- 登录账号：电信运营商提供的登录账号。
- 登录口令：电信运营商提供的登录密码。

选择“自定义服务器”，配置页面如下：

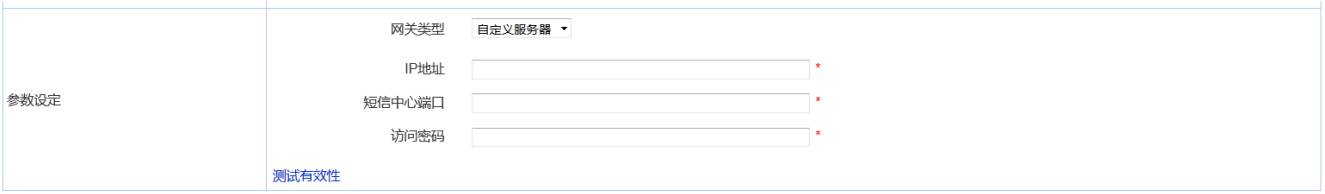


图144. 网关类型－自定义服务器

- IP地址：自定义服务器的IP地址。
- 短信中心端口：服务器与设备通信的端口。
- 访问密码：访问自定义服务器的密码。

- 页面编码：有“GBK” 和“UTF-8”。

在配置完成后，点击测试有效性可能配置进行测试。如下图：

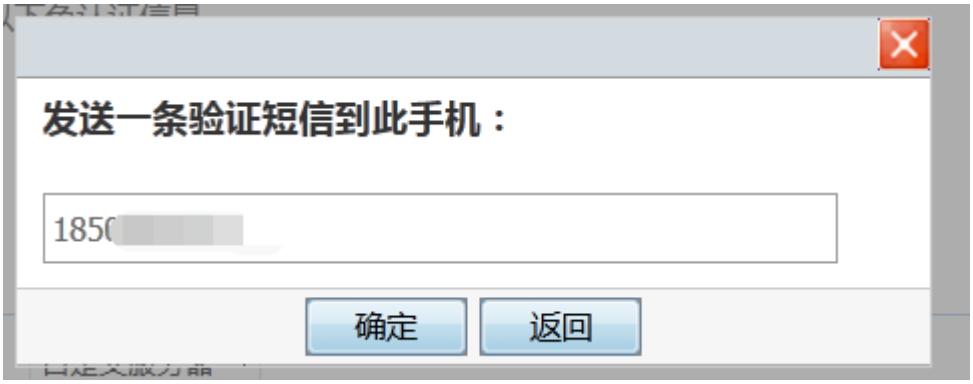


图145. 测试有效性

提示：

1. 手机获取到验证码后，十分钟之内没有使用，该验证码无效，需重新获取验证码。

2. 如选择的短信网关类型为短信猫的时候，使用 usb 口相连与行为管理设备相连时，对于有两个 usb 口的行为管理建议使用下面的 USB 口与短信猫相链接，一般购买短信猫会有延长线，这样的话不影响接口使用。

3. 使用第三方短信认证服务商的短信服务时，**目前仅支持 webservice 方式!!!**

15.4 认证服务器

认证服务器包括 RADIUS 服务器、AD 服务器、LDAP 服务器。

15.4.1 RADIUS 服务器

功能描述：配置 RADIUS 认证服务器。

配置路径：【用户认证】>【认证服务器】>【RADIUS 服务器】

配置描述：

第一：进入【RADIUS 服务器】页面，如下图：

RADIUS认证服务器 新增

序号	名称	IP地址	认证端口	计费端口	间隔传送时间	操作
1	radius	172.16.161.100	1812	1813	30	修改 删除
2	radius1	192.168.0.10	1812	1813	30	修改 删除
3	bao	172.16.0.10	1812	1813	30	修改 删除

图146. RADIUS 服务器配置列表

第二：点击<新增>按钮，配置 RADIUS 认证服务器，如下图：

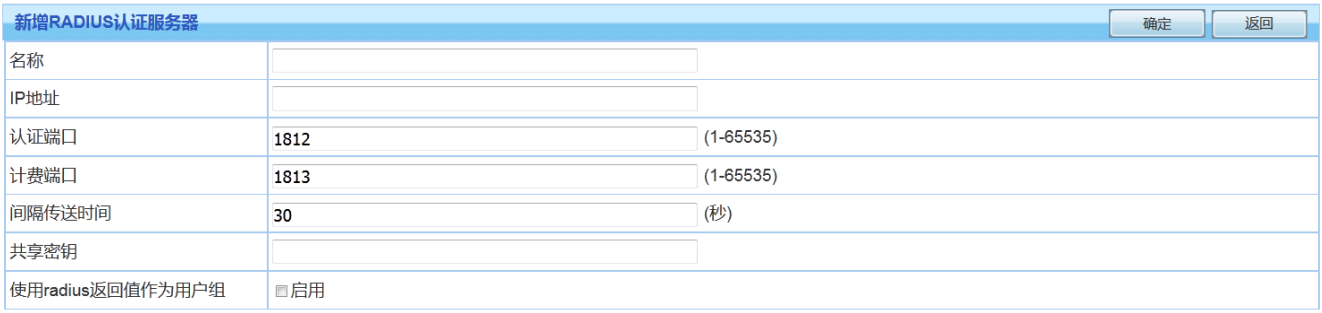


图147.　　新增 RADIUS 服务器

参数说明：

- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP地址：RADUIS服务器IP地址。
- 认证端口：服务器中用于认证的端口号，缺省 1812。
- 计费端口：服务器中用于计费的端口号，缺省 1813。
- 共享密钥：与RADUIS服务器交换数据时进行加密的密钥。

15.4.2 AD 服务器

功能描述：配置 AD 认证服务器

配置路径：【用户认证】>【认证服务器】>【AD 服务器】

配置描述：

第一：进入【AD 服务器】页面，如下图：

图148.　　AD 服务器配置列表

第二：点击<新增>按钮，配置 AD 认证服务器，如下图：

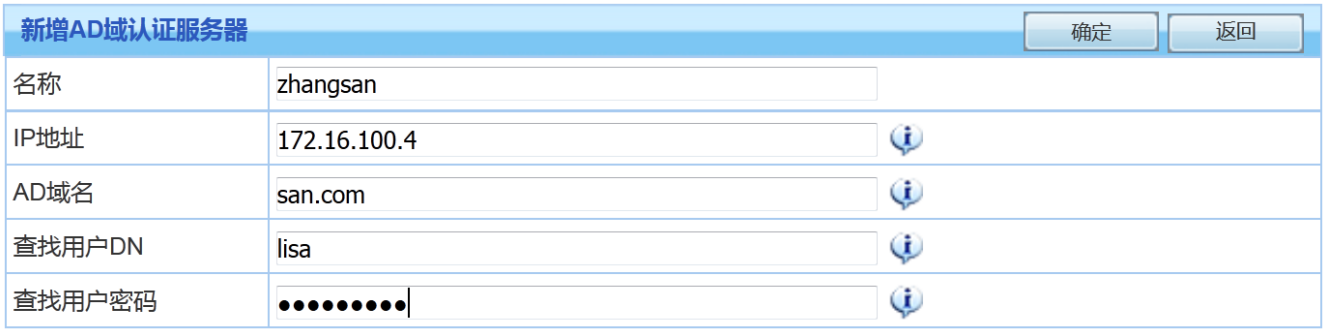


图149. 新增 AD 服务器

参数说明：

- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP地址：AD服务器IP地址。
- AD域名：域控制器域名，例如 abc.com。
- 查找用户DN：AD 服务器中的用户认证是基于用户 DN 完成的，为了完成认证用户名到 AD域 用户 DN 的转换，需要根据用户输入的用户名在 AD 服务器中执行查找操作。一般来说填写查找用户名即可。如果不知道用户的 DN，可以在 AD 服务器的 Doc 界面执行 dsquery user 命令，即可显示 AD 服务器中用户的 DN。
- 查找用户名密码：查找用户在 AD 服务器中的密码。

15.4.3 LDAP 服务器

功能描述：配置 LDAP 认证服务器。

配置路径：【用户认证】>【认证服务器】>【LDAP 服务器】

配置描述：

第一：进入【LDAP 服务器】页面，如下图：

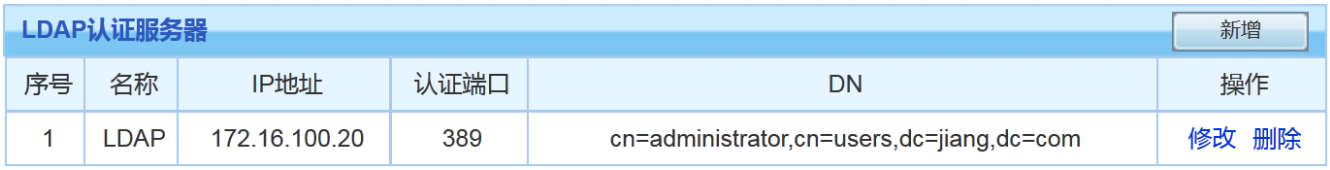


图150. LDAP 服务器配置列表

第二：点击<新增>按钮，配置 LDAP 认证服务器，如下图：

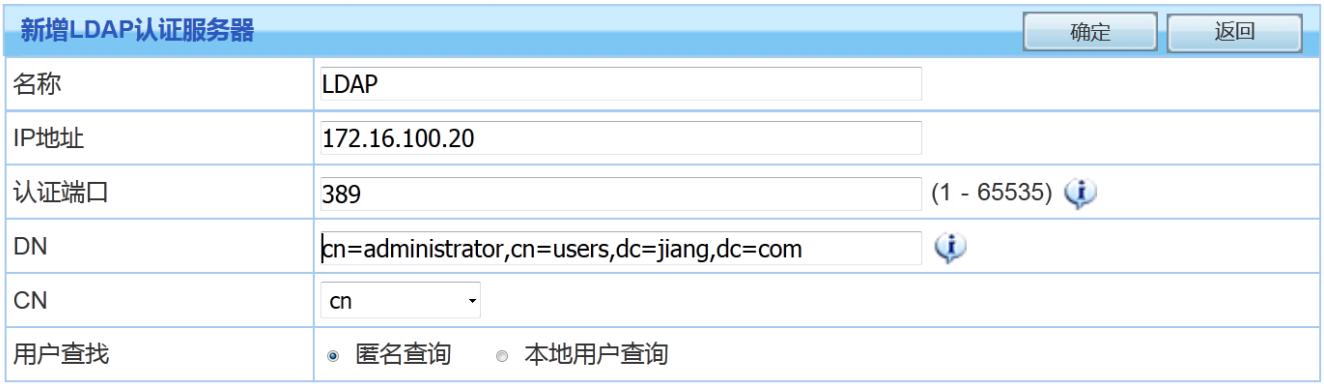


图151. 新增 LDAP 服务器

参数说明：

- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP地址：LDAP服务器IP地址。
- 认证端口：服务器中用于认证的端口号，缺省为 389。
- DN：LDAP 服务器用通用名称标识符搜索具体条目时所使用的路径，如 cn=searcher,cn=software,dc=abc,dc=com。
- CN：LDAP用户，分为cn和uid两种方式。
- 用户查找：分为匿名查询和本地用户查询。
- 查找用户DN: 所查找用户的路径，如cn=searcher,ou=group1,dc=abc,dc=com。
- 查找用户密码：LDAP服务器上用来查找的用户对应的密码。

15.4.1 服务器测试

功能描述：测试认证服务器是否可达，是否正常工作。

配置路径：【用户认证】>【认证服务器】>【服务器测试】

配置描述：

第一：测试[Raduis 服务器]，如下图：

图152.　Raduis 服务器测试

参数说明：

- 认证服务器类型：选择测试的服务器类型。
- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP地址：RADUIS服务器IP地址。
- 认证端口：服务器中用于认证的端口号，缺省 1812。
- 共享密钥：与RADUIS服务器交换数据时进行加密的密钥。
- 用户名/密码：用于测试的 Raduis 用户名和密码。

第二：测试[LDAP 服务器]，如下图：

图153.　LDAP 服务器测试

参数说明：

- 认证服务器类型：选择测试的服务器类型。
- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP地址：LDAP服务器IP地址。
- DN：LDAP 服务器用通用名称标识符搜索具体条目时所使用的路径，如 cn=searcher,cn=software,dc=abc,dc=com。
- 查找用户DN: 所查找用户的路径，如cn=searcher,ou=group1,dc=abc,dc=com。
- 查找用户密码：所查找用户的密码。

15.5 组织管理

“组织管理”包括批量导入、LDAP/AD 导入、扫描内网主机

15.5.1 批量导入

功能描述：手动将已导出的组织结构文件，或者自定义的文件批量导入。

配置路径：【用户认证】>【组织管理】>【批量导入】

配置描述：进入【批量导入】页面，如下图：

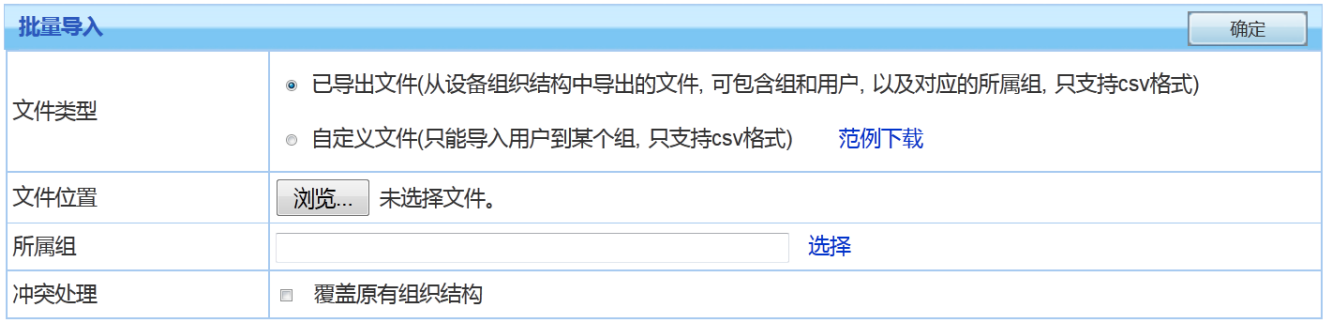


图154.　　组织结构-批量导入

参数说明：

- 文件类型：包括“已导出文件”和“自定义文件”两种类型。已导出文件表示从设备组织结构中导出的文件，文件类型：可包含组和用户，以及对应的所属组。自定义文件表示自定义格式，只能导入用户到某个组，支持 xls 格式。点击<范例>按钮，可以查看文件范例。
- 文件位置：点击<浏览>按钮，选择要导入的文件。
- 所属组：点击<选择>按钮，选择将要导入的子组和用户放于哪个父组下面。

15.5.2 LDAP/AD 导入

功能描述：通过 LDAP/AD 服务器导入和更新用户信息

配置路径：【用户认证】>【组织管理】>【LDAP/AD 导入】

配置描述：

第一：进入【LDAP/AD 导入】页面，如下图：

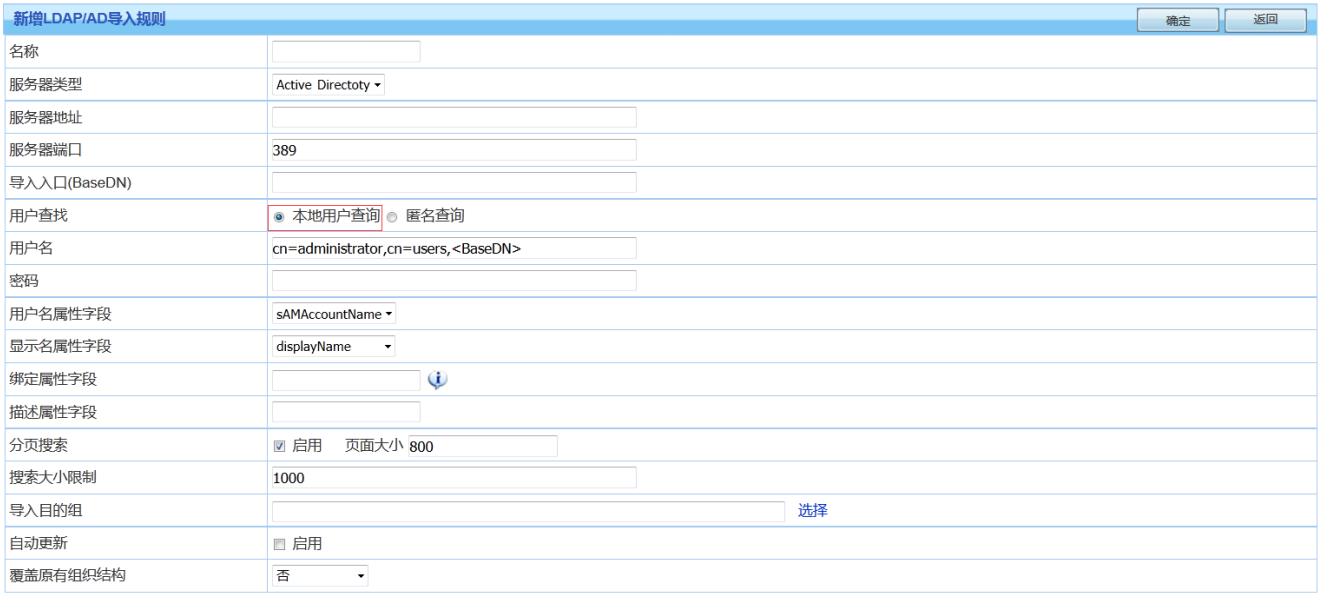


图155.　　LDAP/AD 导入-本地用户查询

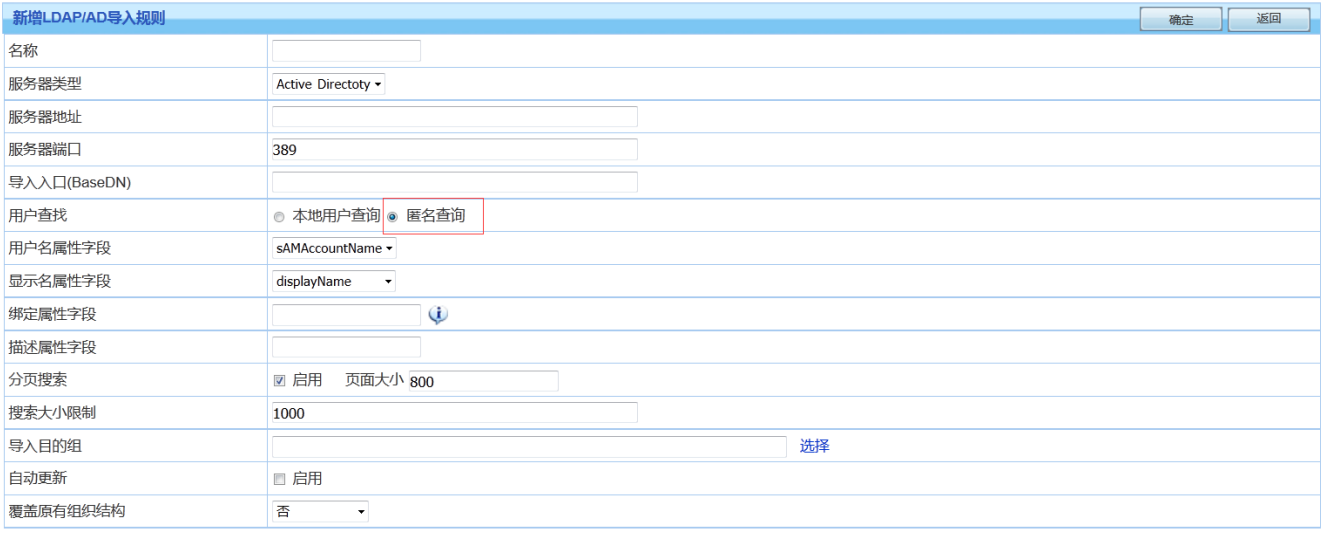


图156. LDAP/AD 导入-匿名查询

第二：配置各个参数，参数说明如下：

- 用户查找： [匿名查询]指不需要进行认证，即可进行用户导入；[本地用户查询]必须要输入LDAP/AD域里的任何一个用户名及密码，并成功进行认证后，才能进行用户导入。
- 服务器地址：运行 LDAP/AD 服务的服务器 IP 地址
- 服务器端口：LDAP/AD 服务的端口，默认值389。
- 导入入口：确定导入用户数据的导入点，由域名和用户组名组成。格式为：[ou=2 级用户组，ou=1级用户组，dc=N 级域名，……，dc=2 级域名，dc=1 级域名]。
- 用户名：LDAP/AD 中任何一个用户的名称。
- 密码：对应上面输入的用户名的密码。
- 用户名属性字段：对应LADP/AD服务器上面用户名属性。
- 显示名属性字段：对应LADP/AD服务器上面显示名属性。
- 绑定属性字段：对应LADP/AD服务器上面绑定属性，根据需要填写，绑定格式同组织结构中的绑定格式,多条用","号分开。
- 描述属性字段：对应LADP/AD服务器上面描述属性，根据需要填写。
- 用户组过滤：支持导入LDAP/AD服务器上指定用户组，即导入指定用户组，也可导入除指定用户组之外的其他用户组，通过“与或非”逻辑实现。如只需导入finance组，只需填写ou=finance，无需完整路径；如需导入除finance之外的任何组，则填写ou!=finance。
- 分页搜索：LDAP/AD服务器的用户/用户组数目庞大的情况下需启用分页搜索，否则会导致用户无法导入或者用户/用户组信息导入不完整。页面大小推荐值为800个。
- 搜索大小限制：与[分页搜索]配合使用，推荐值为1000。
- 导入目的组：将LDAP/AD服务器上的用户组导入的本地组，可点击[选择]按钮选择某个本地组作为目的组。
- 自动更新：定时自动同步LDAP/AD 服务器上的用户和组信息，默认未启用。点击<启用>按钮，选择自动

更新的时间。更新时间选择的是时间计划里配置的时间对象，以时间对象配置的起始时间作为更新时间。自动更新对设备与AD服务器资源都有比较大的资源消耗，建议更新时间设置6小时以上，且避开业务高峰期，以免影响在线用户上网。

- 覆盖原有组织结构：不推荐使用，默认不启用，除非必须使用才启用该功能会清空整个用户组，只保留导入的LDAP/AD用户组信息。
- 公用账号：一个LDAP/AD账号多个人同时使用，0表示不限制账号的同时使用人数。

第三：点击<更新配置>按钮，以上参数配置成功。

第四：点击<导入>按钮后，如果成功连接到服务器后，会出现“导入时将删除原有组织结构信息，确定要导入吗？”的提示。点击<确定>，则将删除原有组织结构信息并导入 LDAP 服务器上的用户和组信息。

15.5.3 扫描内网主机

功能描述：通过 NetbIOS 协议扫描内网的主机信息。

配置路径：【用户认证】>【组织管理】>【扫描内网主机】

配置描述：

第一：进入【扫描内网主机】页面，如下图：

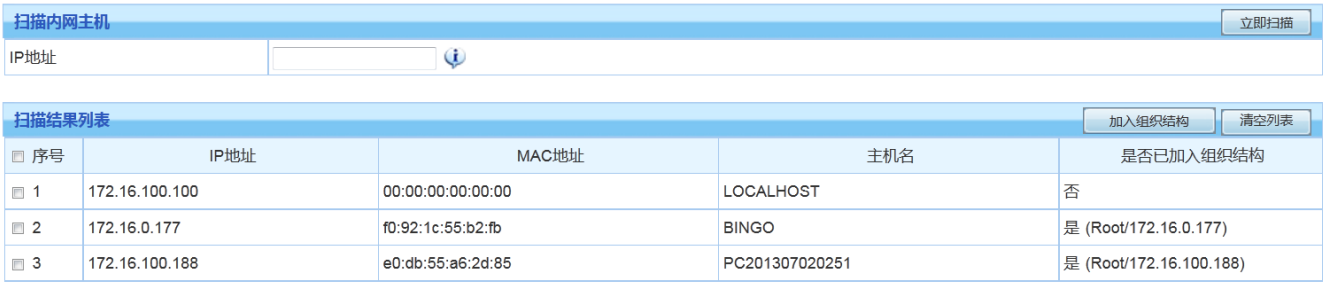


图157. 扫描内网主机 1

第二：在“IP 地址”输入框内输入要扫描的 IP 地址，格式范例为：192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.1.200/24。最大只能输入 C 类地址。

第三：点击<立即扫描>按钮，扫描当前开机的主机。然后在“扫描结果列表”将列出扫描到的主机。如上图，扫描结果将列出每个主机的 IP 地址、MAC 地址和主机名，以及“是否已加入组织结构”。“是否已加入组织结构”一列有显示扫描到的用户是否已经在组织结构中。“否”表示不在组织结构中，“是”表示已经在组织结构中，括号后面表示所属组路径及用户名。

第四：点击<清空列表>按钮，可清空当前扫描结果列表。

第五：勾选扫描到的主机，再点击<加入组织结构>按钮，弹出将扫描到的主机加入组织结构的界面，如下图：

图158. 扫描内网主机 2

参数说明：

- 用户名：通过单选框可以选择以IP、MAC或者主机名为用户名，默认以IP地址作为用户名。
- 显示名：用户的别名，如果是以用户的IP、MAC、主机名等为用户名，在显示名处可填入用户真实的姓名，在统计的时候就会看到真实的姓名，方便记忆。
- 绑定IP：主机的IP地址。勾选“绑定IP”前的复选框，表示添加用户时自动绑定IP地址。
- 绑定MAC：主机的MAC地址。勾选“绑定MAC”前的复选框，表示添加用户时自动绑定MAC地址。
- 主机名：主机名称。
- 所属组：将用户添加到哪个组下。点击表头的<选择所有用户的组>，批量添加扫描用户到组织结构。单个用户则点击每个条目后面对应的<选择>按钮。
- 冲突处理：默认禁用，若组织结构存在于当前用户信息相同的信息（用户名、绑定信息），启用该功能可覆盖之前的用户，使用当前的用户信息加入组织结构。

提示：

1、 此处的扫描 MAC 地址是设备通过 NetBIOS 协议去扫描的，而不是依靠的 SNMP 协议去三层交换机上获取，所以此处的扫描需要内网计算机支持并启用了 NetBIOS 协议，且三层交换机没有对 NetBIOS 协议做限制。

2、 当跨三层交换机的网络需要绑定 MAC 地址时，必须开启 SNMP 选项功能。具体配置详见【用户认证>认证选项> 跨三层 MAC 识别】

3、 组织结构绑定 MAC 信息，操作[扫描 MAC]，如果有扫描结果，也会在[扫描结果列表]产生扫描结果。具体操作详见【用户认证>组织结构>绑定检查】

15.6 临时账号设置

支持临时用户自主申请临时账户，主要提供给外来的临时用户使用。支持自动审核和管理员手动审核的核定方法将临时帐户加入到组织结构中。减少管理员对临时账户的频繁配置，统一临时账户的上网权限和使用期限的管理。

15.6.1 临时账号基本设置

15.6.1.1 手动审核

功能描述：设置临时账户的审核类型、用户组、使用期限。

配置路径：【用户认证】>【临时账号设置】>【基本配置】

配置描述：进入【临时账号设置】配置页面，如下图：

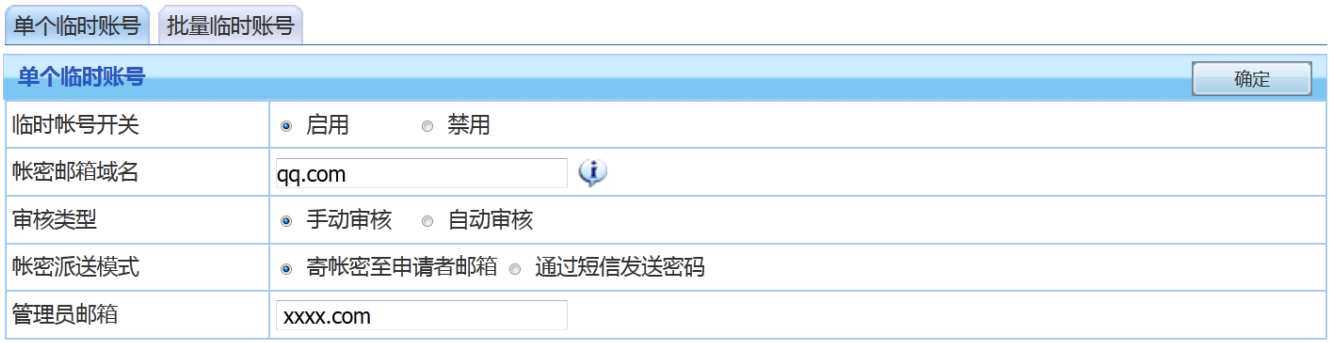


图159. 临时账号设置-手动审核

参数说明：

- 临时账号开关：[开启]或[禁用]临时账户功能。
- 账密邮箱域名：如果在这个地方规定了邮箱的类型，则用户申请临时账号的邮箱（接收临时账户信息的邮箱）只能用这里规定的邮箱类型。若不指定邮箱域名则允许临时账户申请者输入任何类型邮箱地址。
- 审核类型：自动审核表示系统自动审核临时账户的申请信息，审核通过后，用户名和密码立即返回到申请窗口；手动审核表示需要管理员手动核定临时账户的申请信息，申请的用户名和密码将发到账户申请时指定的邮箱里。
- 账密派送模式：手动审核支持将密码发送至用户邮箱或通过短信发送到手机两种方式；
- 管理员邮箱：将临时账号的申请信息发送给管理员邮箱，通过邮件的方式提醒管理员去审核未通过的临时账号。

提示：

开启临时账号功能后，还有如下注意事项：

1、 配置一条相关的本地认证策略，参考【用户认证>认证策略】。

2、 【用户认证>认证选项>未认证权限】放开申请者邮箱域名。

3、 检查设备静态路由和 DNS 设置。

4、 设定邮件配置，以便设备作为邮件客户端发送相应邮件信息。

15.6.1.2 自动审核

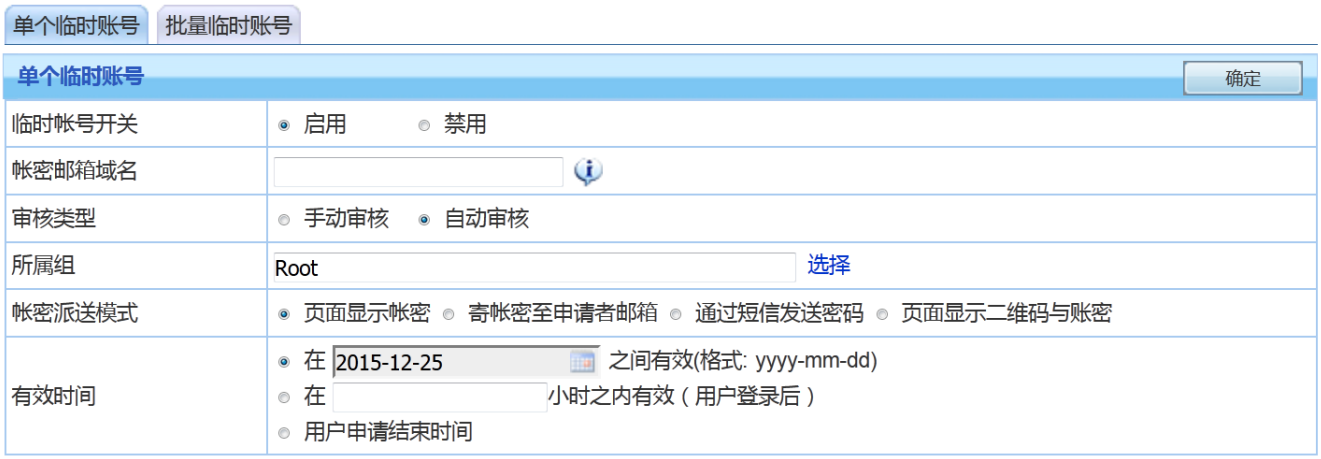


图160. 临时账号设置-自动审核

参数说明：

- 临时账号开关：[开启]或[禁用]临时账户功能。
- 审核类型：自动审核表示系统自动审核临时账户的申请信息，审核通过后，用户名和密码立即返回到申请窗口；手动审核表示需要管理员手动核定临时账户的申请信息，申请的用户名和密码将发到账户申请时指定的邮箱里。
- 所属组：选择将临时账户加入哪个用户组中。
- 账密派送模式：手动审核支持将密码发送至用户邮箱或通过短信发送到手机两种方式；自动审核支持密码发送至用户邮箱、短信接收、页面显示二维码与账密、认证页面直接显示四种方式。
- 有效时间：临时账户的使用期限，超过有效时间，临时账户不可用。

提示：

开启临时账号功能后，还有如下注意事项：

1、 配置一条相关的本地认证策略，参考【用户认证>认证策略】。

2、 【用户认证>认证选项>未认证权限】放开申请者邮箱域名。

3、 检查设备静态路由和 DNS 设置。

4、 设定邮件配置，以便设备作为邮件客户端发送相应邮件信息。

15.6.2 批量生成

功能描述：批量生产临时帐号。

配置路径：【用户认证】>【临时账号设置】>【批量生成】

配置描述：进入【批量生成】页面，如下图：

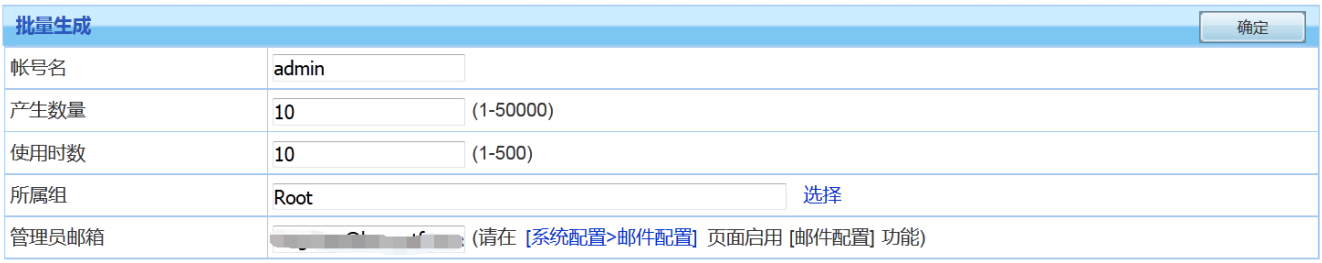


图161.　临时账号设置-批量生成

参数说明：

- 账号名：临时帐号基数名，例如test。
- 生产数量：生产临时帐号的个数，配置为5，则在组织结构里面自动生成的用户分别为test1,test2,test3,test4,test5。
- 使用时数：临时帐号被生成后，在组织结构里面的有效时间（单位小时）。
- 所属组：临时帐号将在指定组里被生产出来。
- 邮件：填写网络管理者邮箱，用来接收包含临时帐号用户名和密码的Excel表格的邮件。

15.6.3 申请临时账户

功能描述：临时用户自主申请临时账户信息。

配置路径：用户上网认证页面

配置描述：

第一、进入【用户认证】页面，如下图：

图162.　新增临时用户的认证策略

第二、点击【申请临时帐号】按钮，开始申请临时帐户，如下图：

图163.　　临时账号申请

自动审核方式：

- ✧ 页面显示帐密：在在申请参数填写完毕，点击[确定]后，界面会弹出包含有用户名/密码的提示框，使用该用户名密码即可完成认证。
- ✧ 帐密寄至申请者邮箱：在申请参数填写完毕，点击[确定]后，界面弹出的提示信息为“帐密将发送至您填写的邮箱：xxxxxx@xxx.xxx，使用该邮箱的账号密码完成认证。
- ✧ 通过短信发送密码：在申请参数填写完毕，点击[确定]后，会提示密码发送至 xxxx，使用短信用户名密码完成认证。
- ✧ 二维码与帐密：扫描接待者认证完成的页面生成的二维码，即可上网。

手动核定方式：

- ✧ 帐密发送至申请者邮箱：管理员审核通过后，帐密才会派送至申请者邮箱。
- ✧ 通过短信发送密码，管理员审核通过后，帐密才会派送至申请者手机。

15.6.4 未审核账户列表

功能描述：查看当前未审核的临时账户，并进行手动审核。

配置路径：【用户认证】>【临时账号设置】>【未审核账户列表】

配置描述：进入【未审核账户列表】配置页面，如下图：

图164.　　未审核账户列表-单个未审核账户

管理员点击[手动审核]，指定所属组，有效时间，之后点击[批准]完成审核。

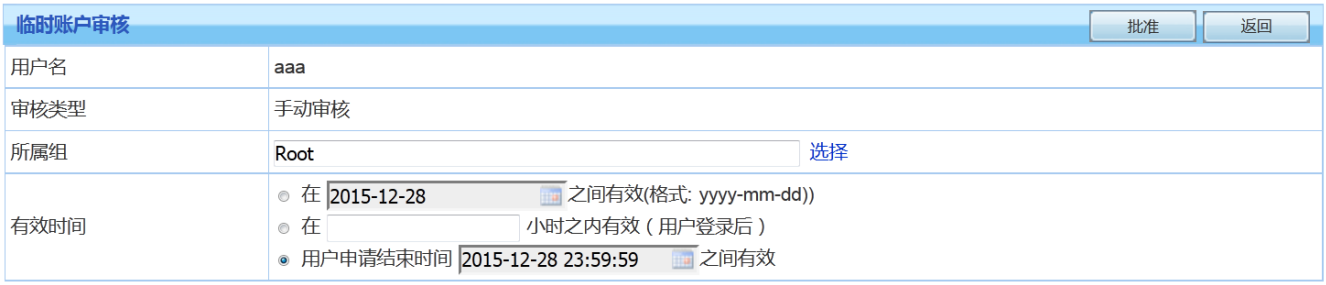


图165.　　单个未审核账户-手动审核

图166.　　未审核账户列表-批量未审核账户

管理员点击[手动审核]，指定所属组，有效时间，之后点击[批准]、[拒绝]完成审核。

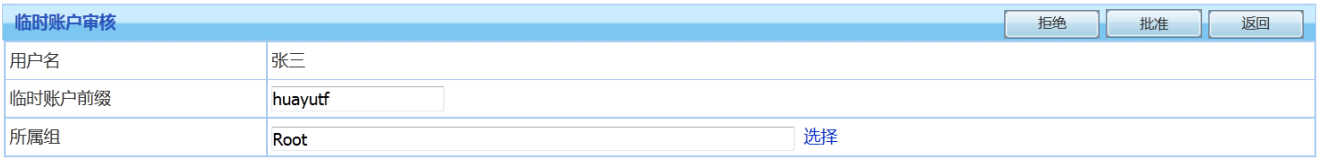


图167.　　批量未审核账户-手动审核

批量临时账号审核后的用户名为【临时账户前缀+当天年月日】组合的形式：

	序号	名称	上网策略配置	绑定检查	所属组	摘要
	1	huayutf20160108001 (huayutf20160108001)	无		Root	认证用户 (离线)
	2	huayutf20160108002 (huayutf20160108002)	无		Root	认证用户 (离线)
	3	huayutf20160108003 (huayutf20160108003)	无		Root	认证用户 (离线)
	4	huayutf20160108004 (huayutf20160108004)	无		Root	认证用户 (离线)
	5	huayutf20160108005 (huayutf20160108005)	无		Root	认证用户 (离线)
	6	huayutf20160108006 (huayutf20160108006)	无		Root	认证用户 (离线)
	7	huayutf20160108007 (huayutf20160108007)	无		Root	认证用户 (离线)
	8	huayutf20160108008 (huayutf20160108008)	无		Root	认证用户 (离线)
	9	huayutf20160108009 (huayutf20160108009)	无		Root	认证用户 (离线)
	10	huayutf20160108010 (huayutf20160108010)	无		Root	认证用户 (离线)

图168.　　批量未审核账户-手动审核通过后的用户

15.6.5 已审核账户列表

功能描述：查看当前已审核的临时账户。

配置路径：【组织管理】>【临时账号设置】>【已审核账户】

配置描述：进入【已审核账户】配置页面，如下图：

申请人	身份证	申请时间	用途	联络电话	联络email	上网所在位置	审核类型	密　码	核定时间	操作
aaa	372924199001091546	2015-12-28 18:30:55	测试专用	18508486501	1968140343@qq.com@qq.com	深圳市	手动	unpquk	2015-12-28 18:35:18	删除

图169.　单个已审核账户列表

申请人	申请单位	申请时间	起始时间	结束时间	申请数量	联络电话	联络email	使用用途	上网所在位置	核定时间	操作
张三	huayutf	2016-01-08 16:55:06	2016-01-08 16:55:06	2016-01-08 23:59:59	10	18508486506	19681440@163.com	临时客户	深圳	2016-01-08 16:59:02	删除

图170.　批量已审核账户列表：

按钮说明：

- 清空：清空当前已审核的所有临时账户。
- 删除：删除某个已审核的临时账户。

16　流量控制

“流量管理”包括线路带宽配置、策略流控、用户流控、黑名单策略、白名单策略。

- 线路带宽配置：用于限制出口(WAN 口)线路的总带宽，如限制 WAN1 口为 100M、WAN2口为 300M。
- 策略流控：根据报文的源地址、目的地址、服务类型、时间段等参数组合成各种流量，可对这些流量提供最大带宽限制、保障带宽、预留带宽的功能。
- 基于用户的流控：对单个主机进行带宽限制、会话控制、分类服务限制以及分时段管理。
- 黑名单策略：对超量使用网络资源(流量、带宽、会话)的用户加入黑名单，并进行惩罚。
- 白名单策略：对源地址加入白名单的用户包含的流量全部放行，不受任何策略的控制，也不被审计。

提示：三种流量控制方式同时生效，所以控制的结果是数字小的优先级高。

16.1 线路带宽配置

功能描述：用于限制出口(WAN 口)线路的总带宽。

配置路径：【流量管理】>【线路带宽配置】，配置页面如下图：

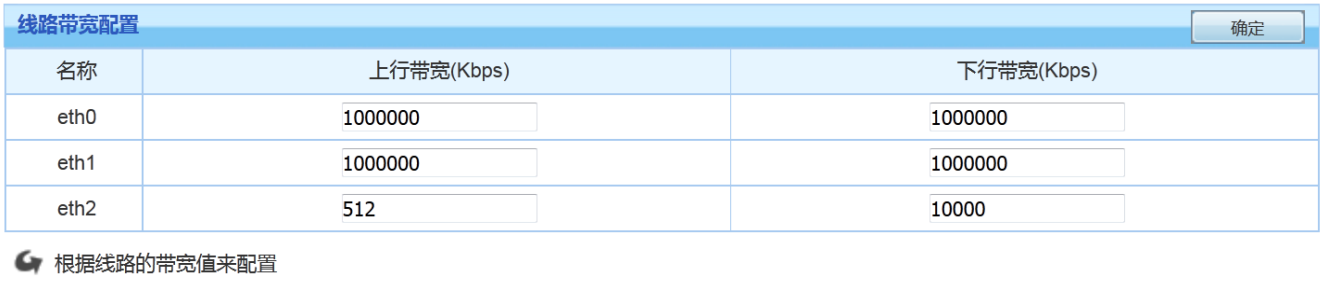


图171. 线路带宽配置

WAN0：WAN0（eth0）线路的带宽限制，配置范围在 8～1000000， 单位 kb/s

WAN1：WAN1(eth1)线路的带宽限制，配置范围在 8～1000000， 单位 kb/s

WAN2：WAN2(eth2)线路的带宽限制，配置范围在 8～1000000， 单位 kb/s

提示：要使用“策略流控”，必须在【网络配置>接口配置>物理接口】页面勾选”WAN”复选框,然后再配置相应的出口线路的带宽。

16.2 策略流控

功能描述：设备提供强大的流量带宽管理功能，可以根据报文的源地址、目的地址、服务类型、时间段等参数组合成各种流量，可对这些流量提供保障通道、限制通道功能。既能保证重要应用的访问带宽，又能限制总上下行带宽，还能针对服务类型、用户组、IP地址等建立带宽保证和带宽限制。

策略规则的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，所以同一组策略中，序号小的优先级高。

配置路径：【流量管理】>【策略流控】

配置描述：

第一：进入【策略流控】页面，如下图：

图172.　　策略流控

按钮说明：

点击<删除所有>，删除所有的流控规则

点击<删除本组>，删除某线路所有的流控规则。

点击<删除>，删除某条流控规则。

点击<修改>，修改本条流控规则，但规则名称和生效线路不能修改

点击<插入>，在当前位置插入一条流控规则

点击<移动>，改变对应流控规则的序号，从而改变该规则的优先级。

改变状态栏复选框的值，再点击<修改状态>，可修改流控规则的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有规则的状态。注意：若父通道状态为禁用状态，就算是子通道为启用状态也是不生效的。

第二：点击<新增>按钮，增加策略流控规则，如下图：

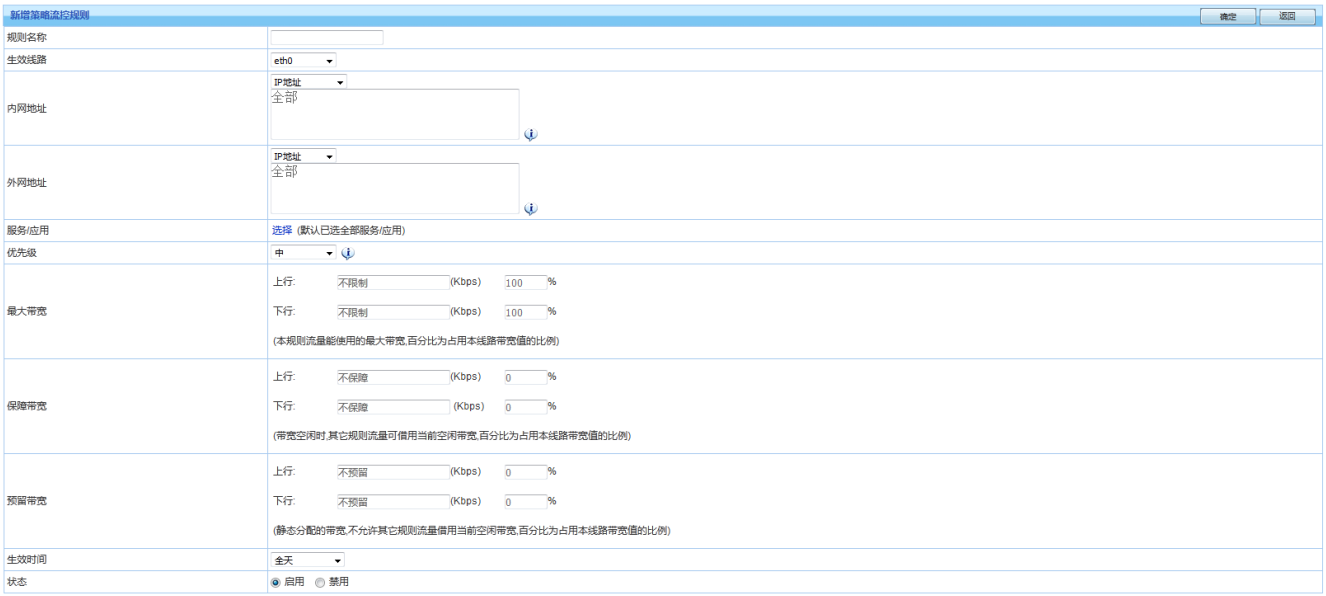


图173.　　新增策略流控规则

参数说明：

- 规则名称：设置流控策略的名称。
- 生效线路：流控规则的生效线路
- 内网地址：内网用户的主机地址或者用户组名称，可输入IP地址、选择IP组或用户组。IP组在【系统对象>IP组】中配置，用户组在【用户认证>组织结构】中配置。
- 外网地址：数据流的目的地址，可输入IP地址、选择IP组或用户组。
- 优先级：在对通道进行带宽保障时，优先级较高的报文优先传送。（在多条流控策略规则下有效）为保证重要业务优先传送，在实现流量控制时，可将核心业务应用、时延要求高的应用、以及重要人物的流量配置为高优先级，同时将 P2P、网络电视、WEB视频等非核心的、占用带宽资源较多的应用配置为低优先级。
- 最大带宽：限制该通道最大带宽，百分比为占用本线路带宽值的比例。
- 保障带宽：结合最大带宽和优先级，根据需要为某些关键应用或者VIP客户保障一定带宽。当网络繁忙时，这些关键应用或者VIP客户至少可以得到设定的保障带宽，并还可以租借空闲的或低优先级流量的带宽；当网络空闲时，低优先级的流量亦可使用当前空闲带宽。从而保证了带宽的合理、高效的使用。百分比为占用本线路带宽值的比例。
- 生效时间：本规则的有效时间段，可分时段控制数据流，比如9：00～12：00和14：00～18：00，不允许员工用 QQ；下拉框内容为事先定义好的“时间计划”名称
- 状态：启用或禁用本规则
- 服务/应用：默认选择“所有”，如要控制一种或多种服务，请点击“选择”按钮。如下图：

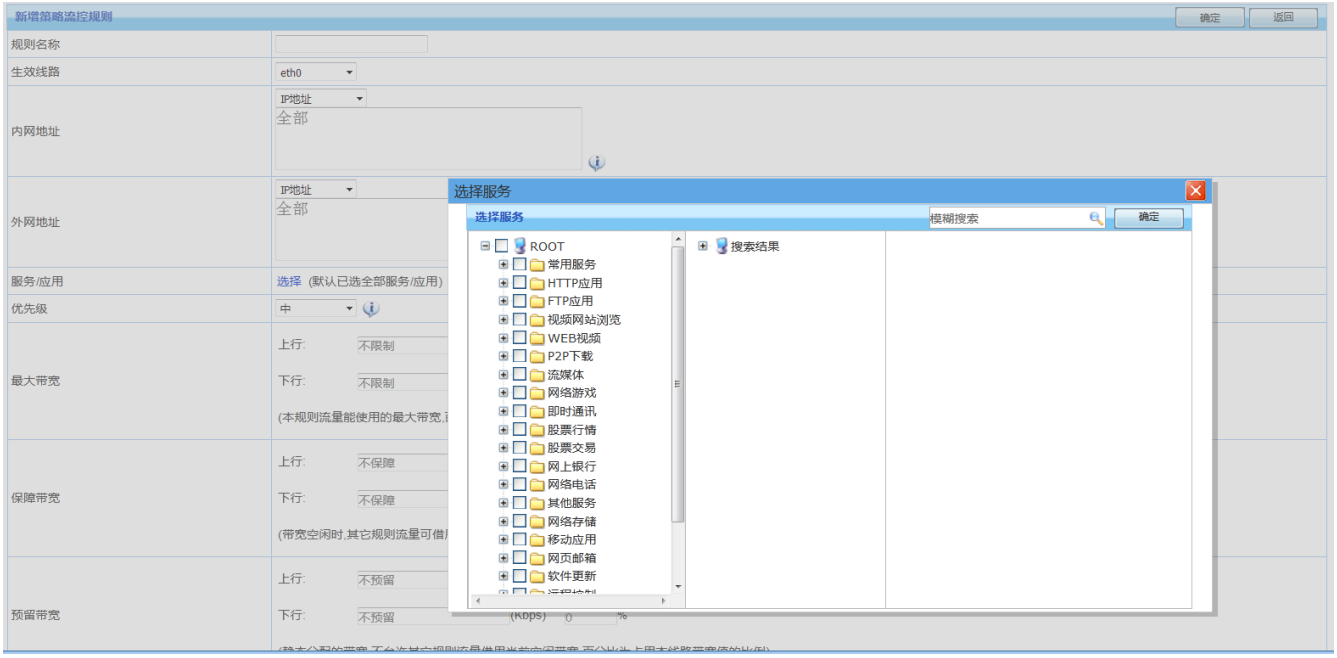


图174.　　自选服务配置页面

此配置页面可以选择需要进行流量控制或者阻断流量的服务，每种类型的服务用一个分页列出，一次可以选择多个服务类型，每个类型可以选择多种服务。

页面支持模糊搜索，可通过搜索需要选择的服务。

选中想要的服务后，点击<确定>按钮，返回新增“ 策略流控”配置页面，如下图：

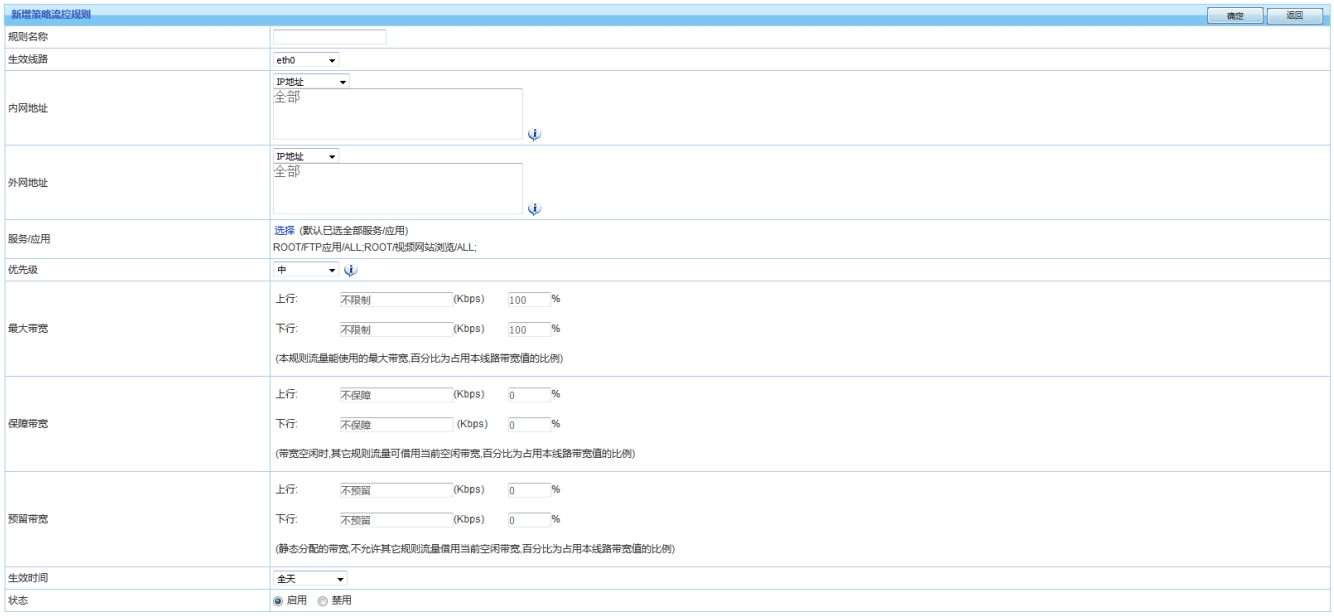


图175.　　配置自选服务

提示：

1、 “预留带宽”不能大于“保障带宽”，“保障带宽”不能大于“最大带宽”。

2、 当所有规则的保障带宽总和小于或等于线路带宽时，根据配置值分配保障带宽。

3、 当所有规则的保障带宽总和大于线路带宽时，优先保障优先级高的流量的带宽。

4、 某一优先级的保障带宽总和大于线路带宽时，根据每条规则配置的值大小按比例分配保障带宽。

5、 策略规则遵循从按顺序从前往后匹配的原则，如果一个规则匹配了，就不会再向下匹配，所以序号小的规则优先级高。请注意规则的先后顺序，先定义的规则，位置排在前面，可通过<插入>或<移动>来改变规则的先后顺序。

16.3 用户流控

功能描述：可以对单个主机进行带宽限制、会话控制、分类服务限制以及分时段管理。策略规则的匹配原则是按顺序从前往后匹配，即从第一条规则开始顺序匹配，一旦遇到一条匹配的规则就停止，所以序号越小的规则优先级越高。

配置路径：【流量管理】>【 用户流控】

配置描述：

第一：进入【 用户流控】页面，如下图：

图176.　　基于 IP 的流控

按钮说明：

“最大带宽”显示值的“↑”表示上行，“↓”表示下行。

“会话数”显示值的“↑”表示上行，“↓”表示下行。

“匹配计数”表示本条策略被匹配的次数。

点击<删除所有>，删除所有的流控规则

点击<删除>，删除某条流控规则。

点击<修改>，修改本条流控规则

点击<插入>，在当前位置插入一条流控规则

点击<移动>，改变对应流控规则的序号，从而改变该规则的优先级。

改变状态栏复选框的值，再点击<修改状态>，可修改流控规则的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有规则的状态。

第二：点击<新增>按钮，增加基于用户的流控规则，如下图：

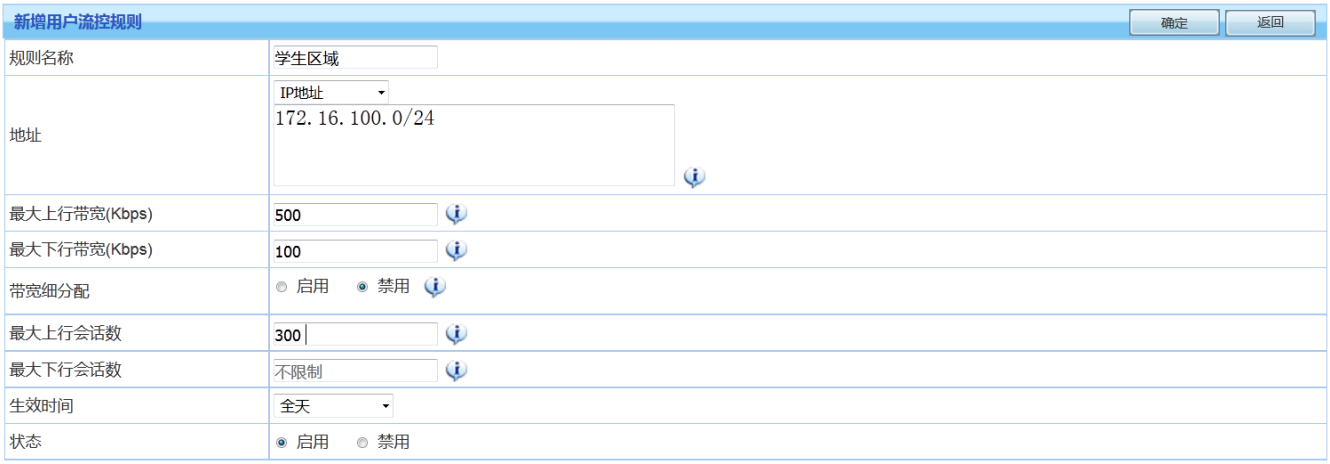


图177.　　新增流控规则

参数说明：

- 规则名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- 地址：内网用户主机地址或者用户组名称，可输入IP地址、选择IP组或用户组。IP组在【系统对象>IP组】

中配置，用户组在【用户认证>组织结构】中配置。

- 最大上行带宽：限制单个IP/用户的上行总带宽，包含特定服务带宽值。
- 最大下行带宽：限制单个IP/用户的下行总带宽，包含特定服务带宽值。
- 源会话数：限制单个IP/用户的源会话数。
- 目的会话数：限制单个IP/用户的目的会话数。
- 生效时间：选择此规则的生效时间，在“系统对象”中预先配置时间计划。
- 状态：启用或禁用本规则，默认启用。

带宽细分配：默认为“禁用”；当“启用”时，将显示“带宽细分配”配置页面。“带宽细分配”是指限制某个主机的最大带宽的同时，可以再对这个主机的某些服务限制一定带宽，可以配置三组，每组可以包含多个服务。如下图：

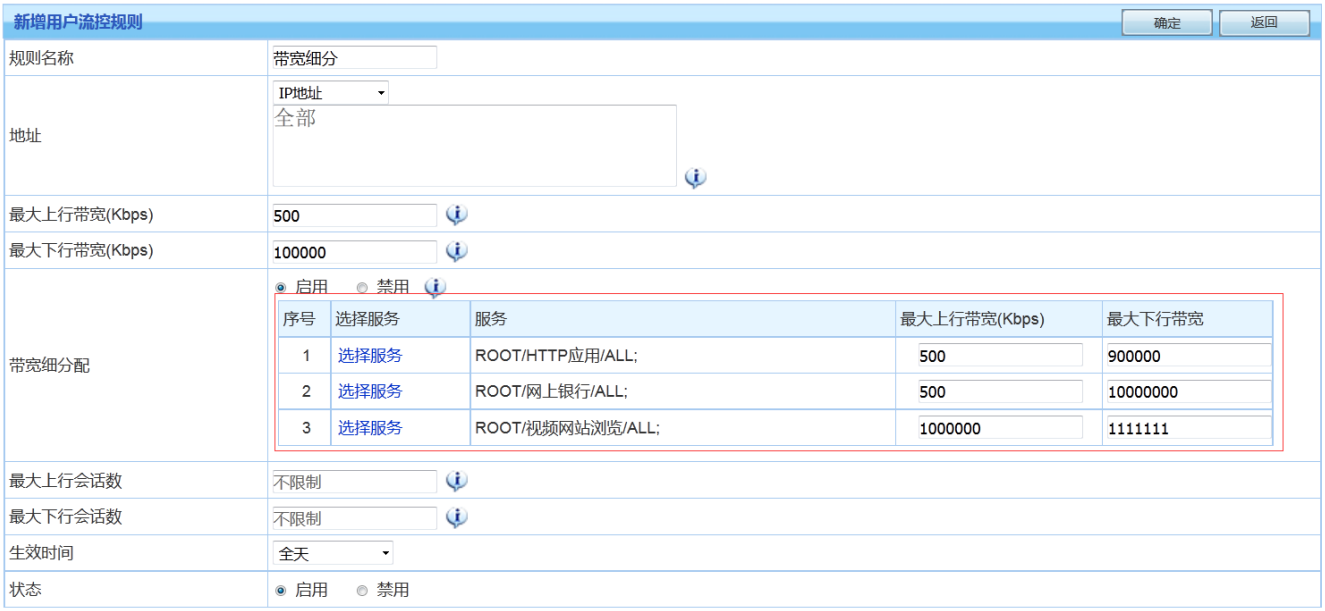


图178.　　带宽细分配

提示：

1、 “带宽细分配”中的最大带宽应小于或等于本规则的最大带宽。

2、 策略规则遵循从按顺序从前往后匹配的原则，如果一个规则匹配了，就不会再向下匹配，所以序号小的规则优先级高。请注意规则的先后顺序，先定义的规则，位置排在前面，可通过<插入>或<移动>来改变规则的先后顺序。

16.4 黑名单策略

功能描述：将超量使用网络资源(流量、带宽、会话)的用户加入黑名单，并进行惩罚。

配置路径：【流量控制】>【黑名单策略】

配置描述：

第一：进入【黑名单策略】页面，点击<新增>按钮，增加黑名单策略。

第二：对用户进行相应的策略配置，设置用户的上网流量、时长以及最大速率和最大会话数，当用户超过所设置的额度时，所应该接受的惩罚方式和惩罚时长。再次是对选定的条目进行 “生效时间”的选择。若需要对选定的条目进行“生效时间”的批量配置，则在“批量操作”后面的“生效时间”选择相应的配置。配置界面如下图：

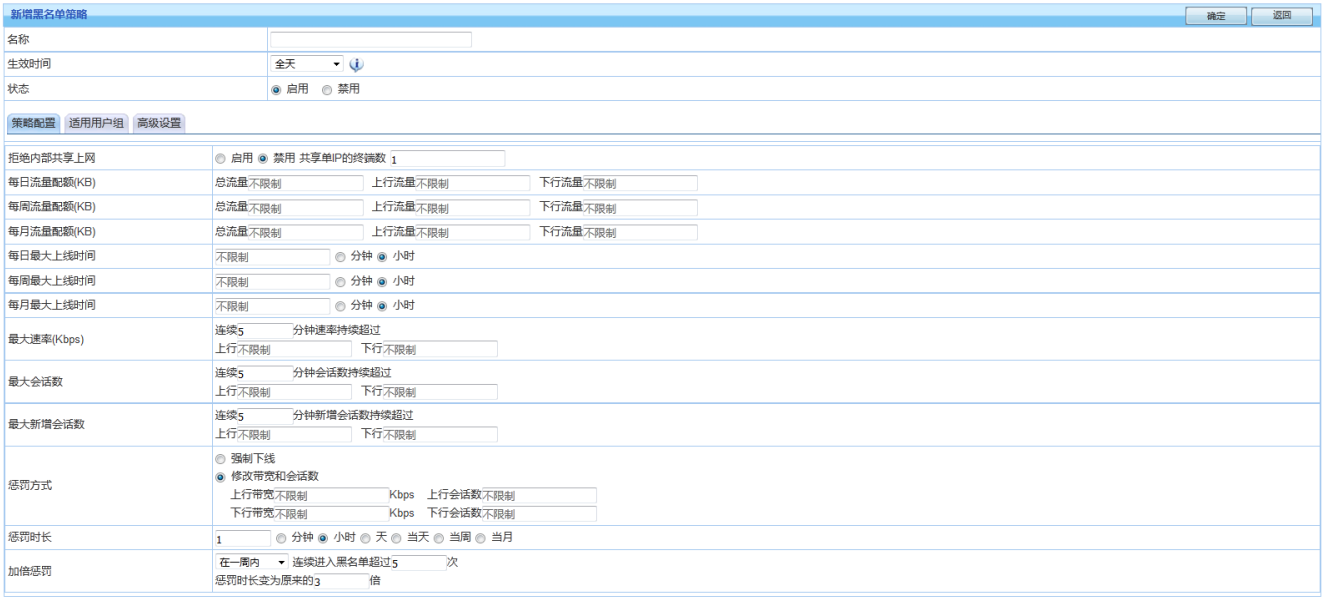


图179. 新增黑名单策略

第三：选择生效适用用户组，两者可同时勾选。用户包括用户及用户组、IP、IP 组，可勾选组织结构用户、用户组。

参数说明：

- 拒绝内部共享上网：不允许内部通过共享上网。
- 每日流量配额：每天允许使用的流量值，总流量、上行流量、下行流量三个值独立计算。
- 每周流量配额：每天允许使用的流量值，总流量、上行流量、下行流量三个值独立计算。
- 每月流量配额：每天允许使用的流量值，总流量、上行流量、下行流量三个值独立计算。
- 每日最大上线时间：每天允许的上网时长。
- 每周最大上线时间：每周允许的上网时长。
- 每月最大上线时间：每月允许的上网时长。
- 最大速率：连续多少分钟内，速率超过一定阀值，上行和下行分开计算。

- 最大会话数：连续多少分钟内，会话数超过一定阀值，上行和下行分开计算。
- 最大新增会话数：连续多少分钟内，新增会话数超过一定阀值，上行和下行分开计算。
- 惩罚方式：当用户进入黑名单时的惩罚方式，包括：强制下线、修改带宽和会话。强制下线表示该用户不能上网，修改带宽和会话表示修改用户的带宽和会话值。
- 惩罚时长：用户进入黑名单的时间。当惩罚时间到了，用户又可以正常上网。
- 加倍惩罚：当用户在一段时间内(包括：在一周内、在一月内、在一季度内) 连续进入黑名单的次数超过预设阀值后，将被加倍惩罚。比如，惩罚时间将变为原来的3倍。

提示：

1、 流量配额、最大速率、最大会话数等里面的每个阀值是或的关系，只有一个值达到阀值，则都会进入黑名单。

2、 查看用户是否违反黑名单规则，在【实时监控>当前黑名单】中查看。

16.5 白名单策略

对于公司领导或者重要的用户，他们的上网不希望受到各种控制策略的限制，也不希望上网的内容被记录。设备的白名单功能可以很好的满足这些需求。符合白名单规则的流量，将不受“防火墙规则、流控规则、认证策略规则、应用内容过滤规则、黑名单规则”的控制；上网的流量值以及会话记录将被统计；但统计的流量将不计入黑名单规则的流量统计中；应用内容过滤的内容（如发送的邮件、发送的帖子、访问的网页、即时通讯记录等）将全部不记录。

功能描述：将特殊的流量加入白名单规则中，使其不受“防火墙规则、流控规则、认证策略规则、应用内容过滤规则、黑名单规则”的限制。

配置路径：【策略流控】>【白名单策略】

配置描述：

第一：进入【白名单策略】配置页面，如下图：

白名单策略　　新增　删除所有

序号	名称	内网地址	控制白名单	生效时间	操作
1	产品经理	192.168.0.100-192.168.0.110	全部	全天	修改 删除
2	销售总监	172.16.0.10	全部	全天	修改 删除
3	特殊外网地址	外网地址组	全部	全天	修改 删除

提示：IP 白名单策略包含的流量全部放行，不受任何策略的控制，也不被审计。

图180.　IP 白名单规则

第二：点击<新增>按钮，增加白名单规则，如下图：

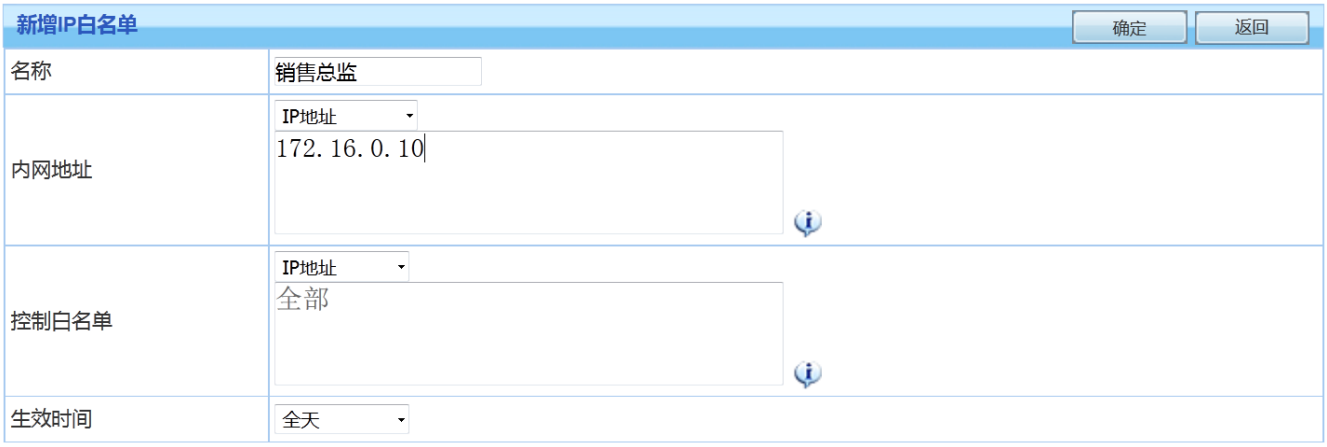


图181.　　新增 IP 白名单规则

参数说明：

- 名称：IP 白名单规则的名称。
- 内网地址：不受控的用户的地址,有三种输入方式，详细说明如下：
  - IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；
  - IP 组：引用已定义好的 IP 组；
  - 用户组：引用组织结构中定义的用户组
- 控制白名单：不受控的外网地址,有两种输入方式，详细说明如下：
  - IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；
  - IP 组：引用已定义好的 IP 组；
- 生效时间：白名单规则的生效时间。生效时间以外，该规则不起作用。

17　系统对象

“系统对象”包括 IP 组、网络服务、时间计划、URL 库、关键字、文件类型等。

17.1 IP 组

功能描述：用于定义一个包含某些 IP 地址的 IP 地址组，这个 IP 组可以是任意的一个 IP、一段 IP 或者 IP 范围的任意组合。

配置路径：【系统对象】>【IP 组】

配置描述：

第一：进入【IP 组】页面，如下图：

图182. IP 组

第二：点击<新增>按钮，增加 IP 组，如下图：

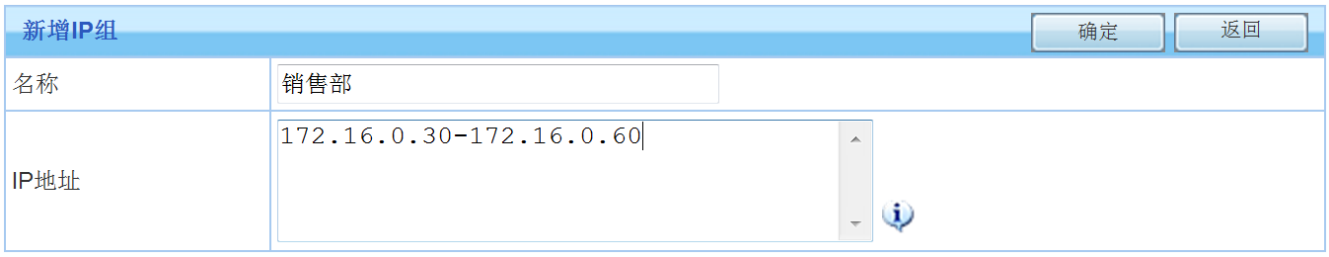


图183. 新增 IP 组

提示：如果某 IP 组已经被引用，则不能被删除。删除前必须先解除引用。

17.2 网络服务

网络服务共分为：自定义普通服务、自定义特征识别、内置服务。内置服务包含常用服务、HTTP 服务、FTP 应用、视频网站浏览、WEB 视频、P2P 下载、流媒体、网络游戏、即时通信和其他服务等。其中[自定义普通服务]与[常用服务]是基于端口的服务，在【防火墙>安全策略】中被引用；其他服务都是基于内容识别的服务，在【流量控制>策略流控】、【内容安全>应用控制策略】中将被引

17.2.1 自定义普通服务

功能描述：自定义基于端口的四层服务

配置路径：【系统对象】>【网络服务】>【自定义普通服务】

配置描述：

第一：进入【自定义普通服务】页面，可看到当前已定义的服务，如下图：

自定义普通服务 新增

序号	名称	服务描述(协议类型/源端口:目的端口)	优先级	操作
1	HTTP协议	TCP/80 TCP/90 TCP/9090	低于内置服务	修改 删除
2	连通性	ICMP/type:3 code:0 ICMP/type:4 code:0	低于内置服务	修改 删除

图184. 自定义普通服务

第二：点击表格右上角的<新增>按钮，增加服务，配置页面如下：

新增自定义普通服务 确定 返回

名称	OA
服务配置	TCP UDP ICMP IP 222 3333
优先级	低于内置服务 高于内置服务

图185. 新增自定义普通服务

点击<TCP>、<UDP>、<ICMP>或<IP>选项卡，可选择协议类型。如果选择 TCP 或 UDP，则需要填写目的端口和源端口。如果选择 ICMP，需要填写类型值和代码值。如果选择 IP，则只需要填写协议号即可。

优先级：默认低于系统定义的常用服务。

提示：

1、 某一种服务，可同时包含 TCP、UDP、ICMP、IP 类型的子服务。

2、 如果某服务已经被引用，则不能被删除。要删除某服务，必须先解除引用。

17.2.2 自定义特征识别

功能描述：自定义基于特征识别的 7 层服务

配置路径：【系统对象】>【网络服务】>【自定义特征识别】

配置描述：

第一：进入【自定义特征识别】页面，可看到当前已定义的服务，如下图：

特征识别规则 新增

序号	名称	服务组	协议类型	源地址	目的地址	数据长度	特征字符串	优先级	操作
1	新浪发件特征	自定义特征识别	TCP	全部 ：10-30	全部 ：0-20	全部	432432	低于内置服务	修改 删除

图186. 自定义特征识别规则

第二：点击表格右上角的<新增>按钮，增加服务，配置页面如下：

新增服务特征 确定 返回

名称	腾讯发件特征		
服务组	自定义特征识别		
协议类型	TCP UDP		
方向	会话建立方向 会话应答方向		
源端口	所有端口 端口范围		
源地址	所有IP地址 指定IP地址		
目的端口	所有端口 端口范围		
目的地址	所有IP地址 指定IP地址		
数据长度	任意数据长度 指定数据长度		
特征字符串1	位置234324324	内容23432432	位置0表示任意位置
特征字符串2	位置234234	内容111111	位置0表示任意位置
特征字符串3	位置24324	内容3534534	位置0表示任意位置
特征字符串4	位置	内容	位置0表示任意位置
优先级	低于内置服务 高于内置服务		
说明:以上各条件是"与"的关系, 即每个条件都满足, 才能匹配到本条特征			

图187. 新增自定义特征识别规则

参数说明：

- 协议类型：选择本条规则的协议类型，可选择 TCP、UDP 或者 TCP+UDP
- 目的端口：可选择[所有端口]或者[端口范围]
- IP地址：可选择[所有 IP 地址]或者[指定的 IP 地址]
- 数据长度：可选择[任意数据长度]或者[指定数据长度]；该长度不计算 TCP/UDP 的头部，仅是 Payload 的长度。符合设定长度的报文才会被匹配。
- 特征字符串：报文的特征，用正则表达式来表示。
- 优先级：默认低于系统定义的特征。

> **提示：**如果某服务已经被引用，则不能被删除。要删除某服务，必须先解除引用。

17.3 时间计划

功能描述：用于定义时间段，然后可在【网络配置>策略路由】、【防火墙>安全策略】、【内容安全】、【流量控制】等中引用，以控制这些策略生效或失效的时间，从而可对各种策略分时间段管理。

配置路径：【系统对象】>【时间计划】

配置描述：

第一：进入【时间计划】页面，可以看到当前已配置的时间计划，如下图：

图188. 时间计划

第二：点击<新增>按钮，增加时间计划，如下图：

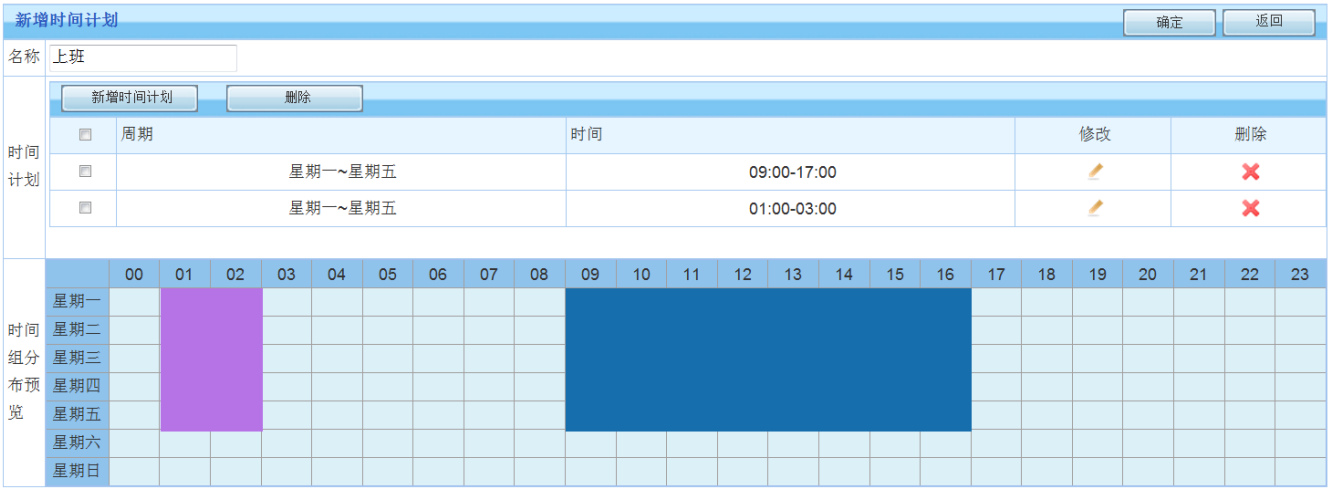


图189. 新增时间计划

按钮说明：

<选定>：选中横坐标和纵坐标对应的时间格子，当格子为黑色时，点击<选定>，格子颜色变为绿色，即选中了时间。

<取消选定>：选中横坐标和纵坐标对应的时间格子，当格子为黑色时，点击<取消选定>，格子颜色变为灰色，即取消了选中的时间。

<重置>：取消所有选中的时间。

第三：选中时间后，点击<确定>按钮，配置成功。

提示：

1、 每个格子代表半小时，只有格子为彩色时，才是已经选定的时间。

2、 如果某时间计划已经被引用，则不能被删除。要删除某时间计划，必须先解除引用。

17.4 URL 库

功能描述：

包括内置和自定义的 URL 库。URL 库可用于【防火墙>安全策略】、【内容安全>应用内容过滤】和【内容安全>应用控制策略】，实现对 URL 的过滤。

配置路径：【系统对象】>【URL 库】

配置描述：

第一：进入【URL 库】页面，可以看到当前的[内置 URL 库]，如下图：

内置URL库 | 自定义URL库

内置URL库

序号	名称	描述
1	IT相关	IT咨询、编程设计类网站
2	博客	网络博客类网站
3	Webmail	使用网页浏览器来阅读和发送邮件
4	财经咨询	财经咨询网站
5	两性健康	两性健康、成人话题等网站
6	广告营销	广告营销
7	法律	法律法规
8	房地产	房地产网站
9	交友聊天	交友,聊天
10	军事	军事国防,军事论坛,军旅生活,军史纪念,军事院校
11	新闻门户	门户网站，新闻类网站
12	人才招聘	人才招聘,简历,行业人才,地方人才网
13	少年儿童	少年儿童网站
14	生活休闲	生活休闲、生活服务咨询类网站
15	视频	视频网站
16	搜索引擎	搜索引擎网站
17	体育	体育运动网站
18	网络硬盘	网络硬盘
19	网上购物	网上购物网站

图190.　　内置 URL 库

第二：点击<自定义 URL 库>选项卡，进入自定义 URL 库页面，如下图：

内置URL库 | 自定义URL库

自定义URL库　　新增

序号	名称	URL	描述	操作
1	内容阻挡	www.baidu.com	ZUBAIDU	修改 插入 移动 删除
2	流量控制	sina.com	控制sina.com	修改 插入 移动 删除

图191.　　自定义 URL 库

操作说明：

- 【内容安全>应用内容过滤>URL 过滤】页面进行 URL 过滤时，遵循从按顺序从前往后匹配的原则，如果一个条目匹配了，就不会再向下匹配，所以序号小的条目优先级高。
- 此处的 URL 条目的顺序决定了【内容安全>应用内容过滤>URL 过滤】页面的关键字条目的匹配顺序，可以通过<移动>和<插入>来调整关键字组条目的顺序。

第三：点击<新增>按钮，可以很方便的自定义 URL 库。如下图：

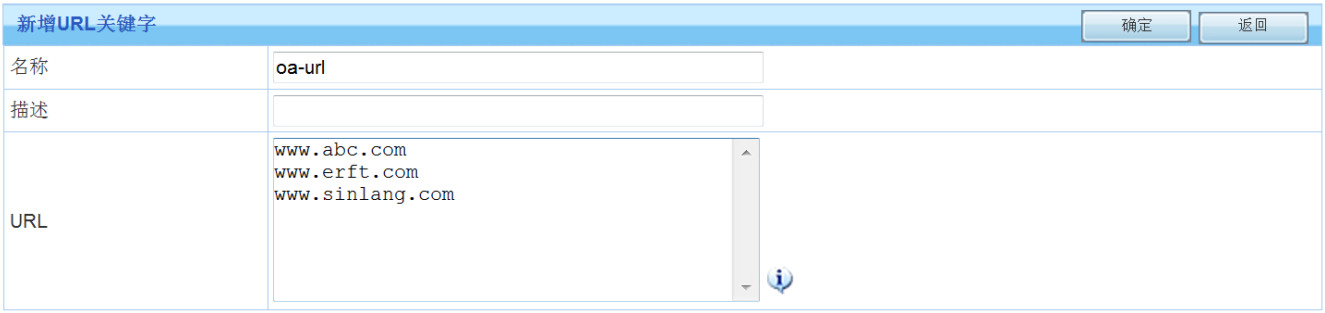


图192.　新增自定义 URL

在“URL”输入框内填写 URL，一行一个 URL 关键字(或 URL 全名)。采用子串匹配方式，如配置 xyz.com，将匹配 www.xyz.com、www.xyz.com.cn、www.xyz.com/hardware 等。

17.5 关键字组

功能描述：用于设置关键字，并把关键字分组，这些关键字组可用于【内容安全>应用内容过滤>关键字过滤】中限制某些关键字的搜索和上传。

配置路径：【系统对象】>【关键字组】

配置描述：

第一：进入【关键字组】页面，可以看到当前已定义的关键字组，如下图：

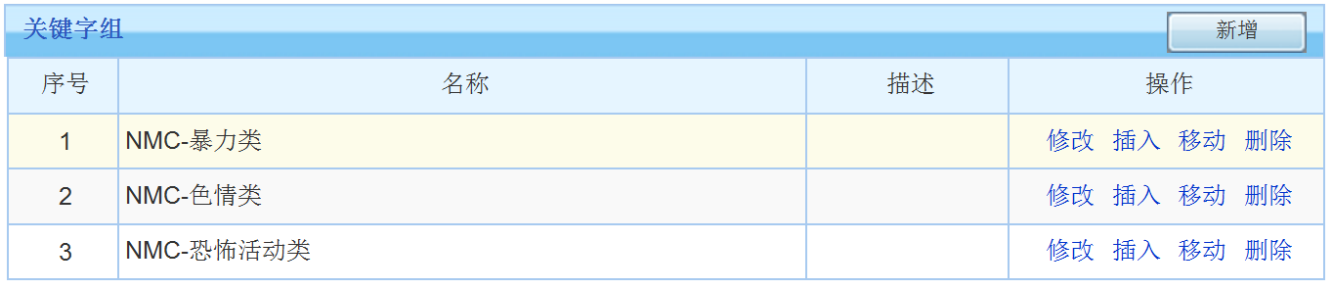


图193.　关键字组

操作说明：

- 【内容安全>应用内容过滤>关键字过滤】页面进行关键字过滤时，遵循从按顺序从前往后匹配的原则，如果一个条目匹配了，就不会再向下匹配，所以序号小的条目优先级高。
- 此处的关键字条目的顺序决定了【内容安全>应用内容过滤>关键字过滤】页面的关键字条目的匹配顺序，可以通过<移动>和<插入>来调整关键字组条目的顺序。

第二：点击<新增>按钮，定义关键字组。一行一个关键字，支持通配符匹配，如输入 snow*n,，将匹配 snowman 或 snowmn 等。如下图：

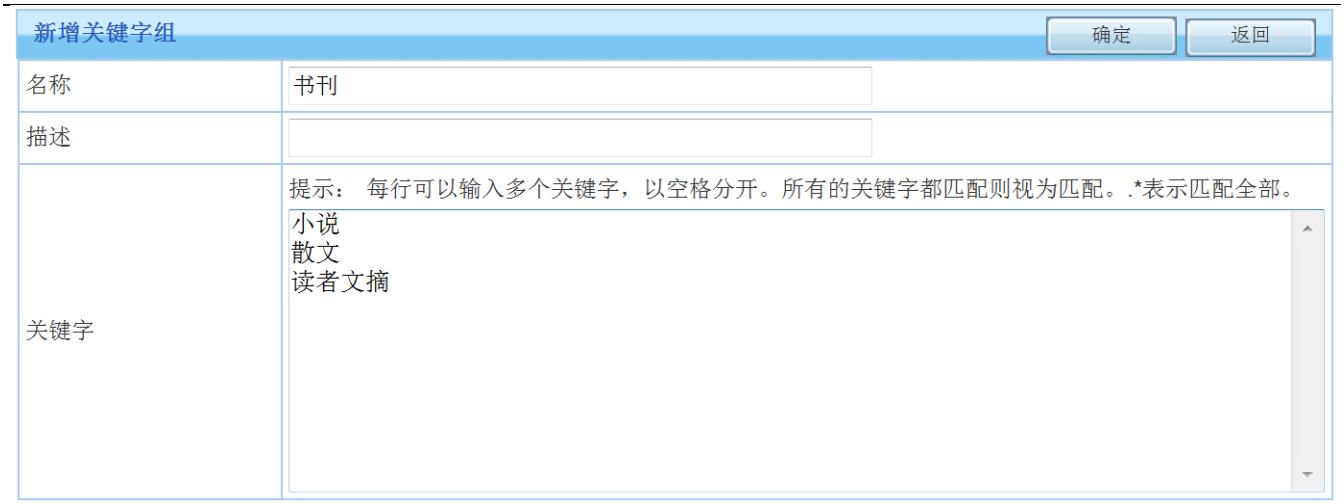


图194. 新增关键字组

17.6 文件类型

功能描述：用于定义文件类型，并把文件类型分组。这些文件类型可用于【内容安全>应用内容过滤>文件输过滤】中限制这些类型的文件的上传和下载。

配置路径：【系统对象】>【文件类型】

配置描述：

第一：进入【文件类型】页面，可以看到当前已定义的文件类型分组。如下图：

图195. 文件类型

操作说明：

- 【内容安全>应用内容过滤>文件传输过滤】页面进行文件传输过滤时，遵循从按顺序从前往后匹配的原则，如果一个条目匹配了，就不会再向下匹配，所以序号小的条目优先级高。
- 此处的文件类型条目的顺序决定了【内容安全>应用内容过滤>文件传输过滤】页面的文件类型条目的匹配顺序，可以通过<移动>和<插入>来调整文件类型组条目的顺序。

第二：点击<新增>按钮，定义文件类型分组。一行一个文件类型，格式为“.后缀名”，如 .zip。如下图：

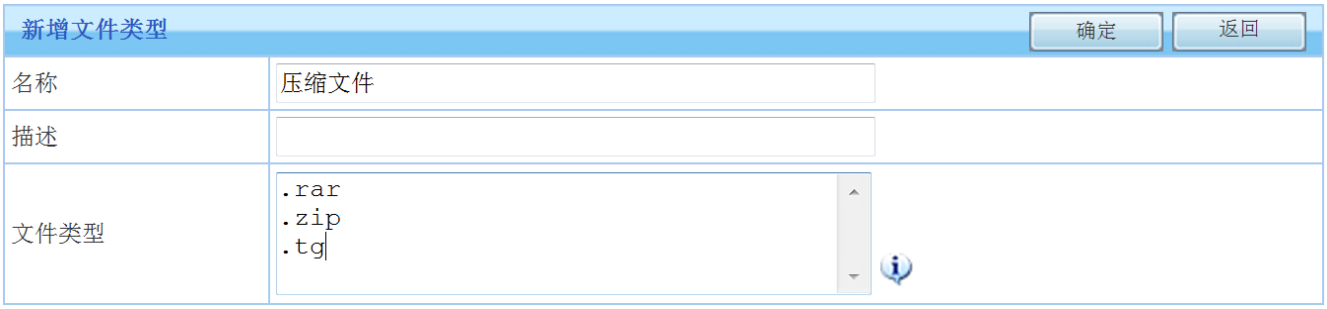


图196. 新增文件类型

18 系统配置

“系统配置”主要包括设备系统维护、系统管理员、网管策略、SNMP 服务器、网络工具、日期/时间、系统信息、邮件配置等。

18.1 系统维护

18.1.1 系统升级

功能描述：升级设备的系统文件，可以升级的系统文件包括：系统版本、IPS 特征库、应用特征库、URL 库、病毒库、ISP 自动地址表、授权文件。

- 系统版本：设备软件程序
- IPS特征库：IPS特征码的库文件
- 应用特征库：应用特征码的库文件
- URL库：内置URL库文件
- 病毒库：带有病毒特征码的库文件
- ISP自动地址表：内置运营商地址集合。
- 授权文件：给设备进行授权的文件。当前授权文件包括以下信息：
  - 设备序列号：标示设备的唯一序列号。
  - 授权类型：试用版/正式版；试用版是指给客户试用的版本，正式版是指正式销售的版本。
  - 授权有效期: 授权文件的有效期限。
  - 升级服务有效期: 正式版的升级服务有效期，在有效期之前可升级系统固件、应用特征库、URL 库，过期则不能升级。

配置路径：【系统配置】>【系统维护】>【系统升级】

配置描述：

第一：进入【系统升级】页面，可以查看设备的各种系统文件信息。如下图：

图197. **系统升级**

第二：选择需要升级的文件类型，点击<浏览>，找到文件的位置，再点击<确定>按钮开始升级。如下图：

图198. 系统升级

提示：

1、 未选中的文件类型后面显示当前的版本信息。

2、 升级系统版本后，必须重启系统才能运行新的版本。

3、 升级 IPS 特征库、应用特征库、URL 库文件、病毒库、ISP 自动地址表和授权文件后，不需要重启系统即可生效。

18.1.2 自动升级

功能描述：用户对“应用特征库”、“URL 库”、“病毒库”的自动升级。

配置路径：【系统配置】>【系统维护】>【自动升级】

配置描述：进入【自动升级】页面，可自动升级系统文件。如下图：

图199. 自动升级

参数说明：

- 启用自动升级：勾选后，即启用了对应库的自动升级功能，设备会定期去服务器检查是否有新版本，若有就会自动升级新的库文件；
- 立即升级：点击此按钮，则立即去获取最新的版本并升级；
- 回滚：将库文件回滚到上一次升级的版本；
- 服务器：自动去该服务器上获取新版本，可配置IP或者域名。配置域名，则需要在【网络配置>DNS配置】页面设置DNS服务器；
- 延迟升级：当有新版本时，是否延迟升级。选择“不延迟”，则立即升级；选择“延迟…”，则延迟一段时间再升级。

18.1.3 备份与恢复

功能描述：设备支持配置文件备份与恢复功能。

配置路径：【系统配置】>【系统维护】>【备份与恢复】

配置描述：

第一：进入【备份与恢复】页面，如下图：

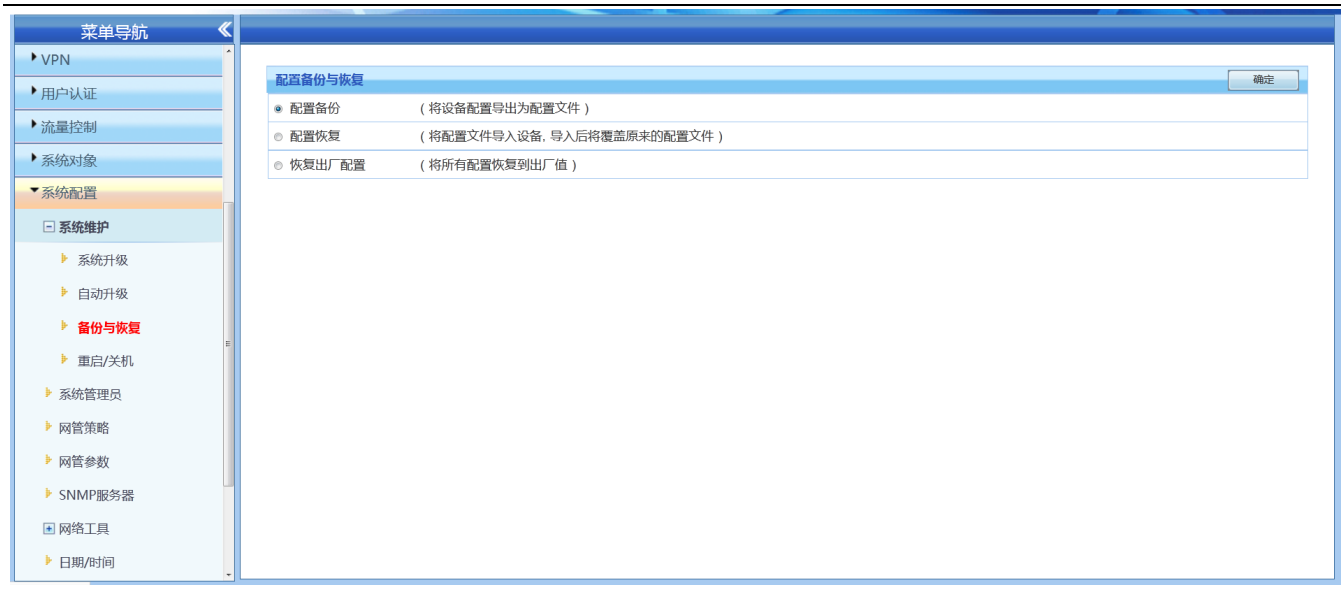


图200.　　配置备份与恢复

- 备份：系统会将所有的配置以文件的形式存储，然后可将这个配置文件导出到PC。
- 恢复：导入一个配置文件（备份到PC的.conf的压缩文件），导入后会覆盖原来的配置文件，设备将自动重启。
- 恢复出厂配置：将设备的配置恢复到出厂值，设备将自动重启。

第二：选择备份或恢复，点击<确定>

18.1.4 重启/关机

功能描述：重启或关闭设备

配置路径：【系统配置】>【系统维护】>【重启/关闭】

配置描述：进入【重启/关闭】页面，选择重启或关机，再点击<确定>按钮，可重启或关闭设备。如下图：

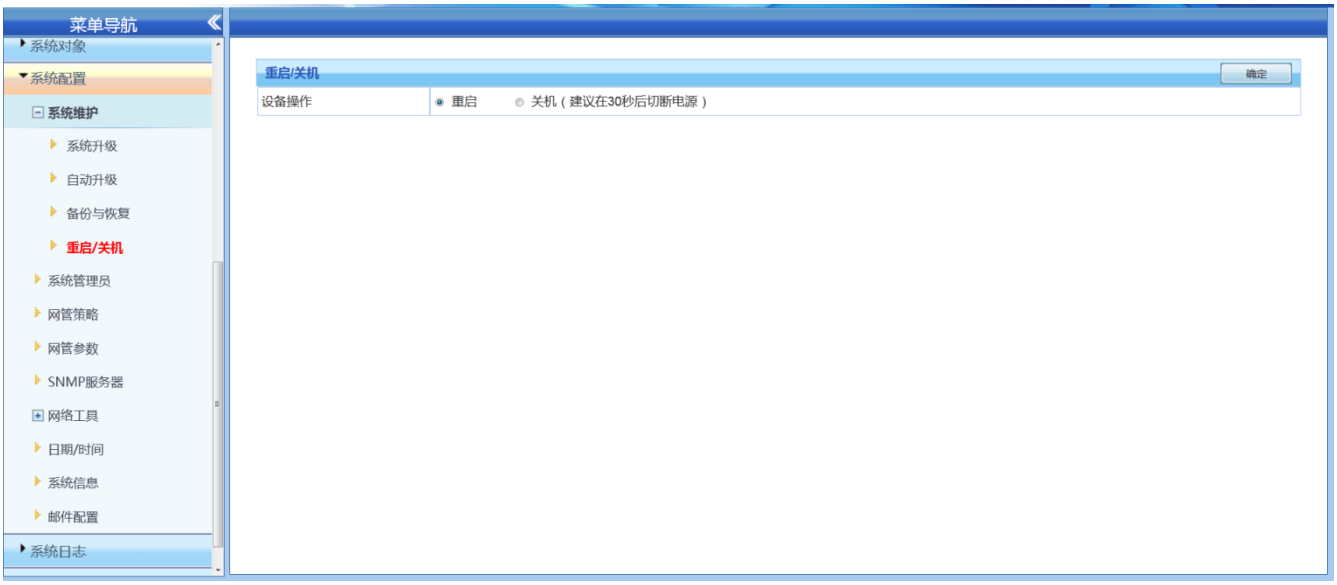


图201.　　重启/关机

提示：移动设备或切换电源时，最好先关机，30 秒后再切断电源。

18.2 系统管理员

18.2.1 配置系统管理员

功能描述：配置系统管理员。

配置路径：【系统配置】>【系统管理员】

配置描述：

第一：进入【系统管理员】页面，可以看到当前的管理员列表，如下图：

图202. 系统管理员

第二：点击<新增>，进入新增管理员的界面，填写各项参数，然后点击<确定>。如下图：

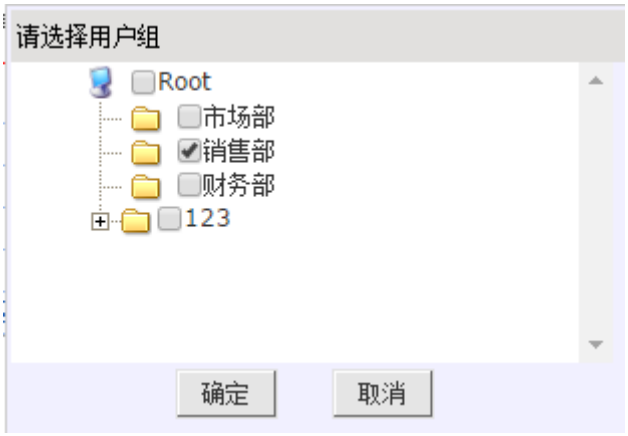
图203. 新增系统管理员

参数说明：

- 用户名：输入用户名称，由数字、英文、下划线、中杠线、点组成，开头必须为字母或数字，且长度为1-16个字符。[必选项]
- 认证方式：口令策略、Radius认证。[必选项]
  - 口令策略：手工配置密码。系统会根据密码强度规则自动检测用户输入密码的安全强度。

- ✧ Radius 认证：需指定 radius 服务器，配置参考【用户认证>认证服务器>RADIUS 服务器】。

- 使用Dkey认证：默认不启用；启用时，只有使用Dkey登录的管理员才有权限查询他的所属组日志。
- 注：DKEY写入操作前，请先下载并安装DKEY驱动；一个DKEY只能仅存一个用户的Dkey信息，写入DKEY将覆盖上一个用户的Dkey信息。
- 真实姓名：输入对应登录名的真实姓名，不限字符。[可选项]
- 公司部门：输入对应登录名的所属部门，不限字符。[可选项]
- 手机号码：即管理员的手机号码。[可选项]
- 邮箱地址：即管理员的邮箱地址，当管理员的配置信息有变更时，系统会通过邮件方式通知管理员。
- 角色：将定义的用户分配一个角色。[必选项]。
- 系统默认配置了三个角色（超级管理员、Guest、审计员），您可以根据准备工作中确定的用户权限来灵活自定义分配的角色。如果要自定义角色，请参见本文【角色管理】章节。
- 所属组：报表中心（Reporter）的权限。例如，一个名为Mary的管理员，“所属组”配置为“Root/销售部”，那么Mary只能查看“根组(Root)”下的“销售部”组下的所有人的记录。点击<选择>按钮，可选择所属组，如下图：



- 状态：启用或禁用该用户，默认启用。
- 备注：主要是作为描述该用户的附加注释信息。[可选项]

18.2.2 角色管理

功能描述：配置系统管理员的角色分类，即管理权限。

配置路径：【系统配置】>【系统管理员】

配置描述：

第一：进入管理员新增页面，点击<角色配置>按钮，进入下图：

序号	用户名	角色	认证方式	所属组	状态	操作
1	admin	超级管理员	口令认证		☑	修改 删除 写入key
2	guest	Guest	口令认证		☑	修改 删除 写入key
3	reporter	审计管理员	口令认证		☑	修改 删除 写入key

图204.　　系统管理员

第二：点击<新增>，进入新增系统角色的界面，填写各项参数，然后点击<确定>。如下图：

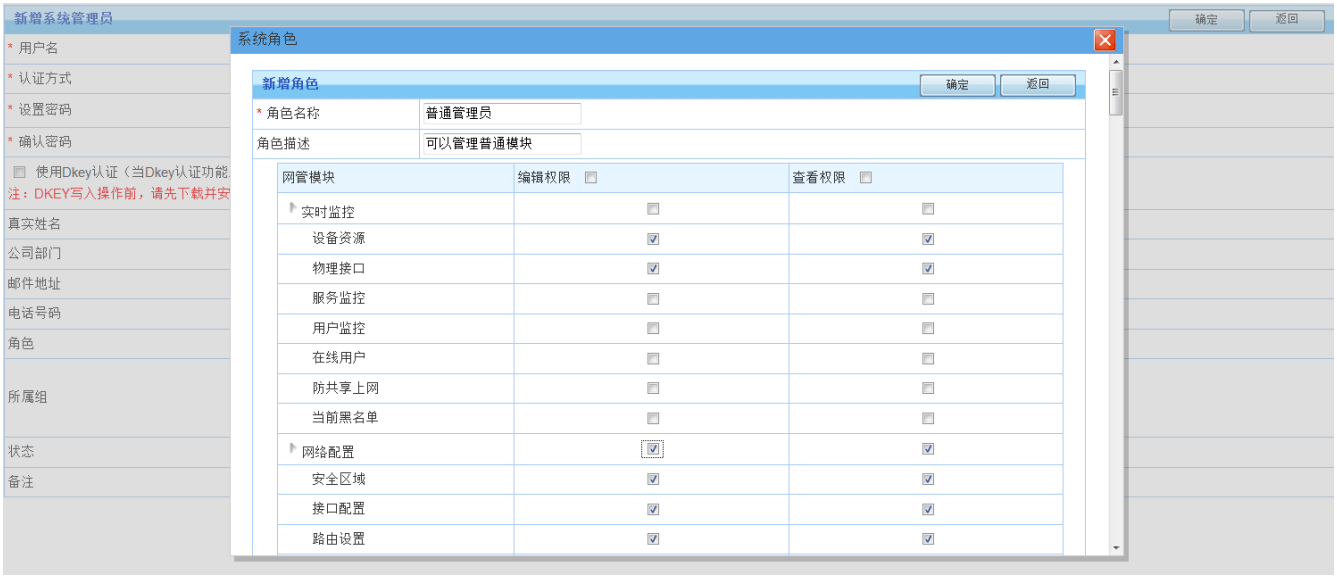


图205.　　新增系统角色

参数说明：

- 角色名称：输入管理员的角色名称。[必选项]
- 角色描述：可以输入描述该角色的注释等。[可选项]
- 权限列表：选择为该角色分配的权限。[编辑权限]表示可以对设备进行读写操作。[查看权限]表示对设备仅有读操作权限。[必选项]

提示：

1、 系统默认配置了三个管理员：
   - admin：具有所有权限，可以配置设备、查看设备、管理 Reporter。
   - guest：仅具有查看设备权限，默认密码为 guest*PWD。
   - reporter：管理 Reporter，所属组为根组，默认密码为 reporter*PWD。
2、 系统默认的管理员(admin、guest、reporter)不能删除，可修改密码。
3、 超级管理员可以修改其它管理员的属性，其它管理员只能修改自己的密码。
4、 新增的管理员可以修改密码，可以被删除。
5、 具有管理 Reporter 权限的管理员，先登录了设备管理界面，可在[报表中心>内置报表中心]菜单快速访问 Reporter。当先登录 Reporter，必须要再次登录才可以管理设备。

18.3 网管策略

功能描述：设置网管策略，可允许部分 IP 能网管设备，以限制非法用户访问设备。

配置路径：【系统配置】>【网管策略】

配置描述：

第一：进入【网管策略】页面，如下图：

图206. 网管策略

第二：选择策略类型，再点击右上角的<确定>。

第三：点击<新增>按钮，增加“允许网管设备的策略”。

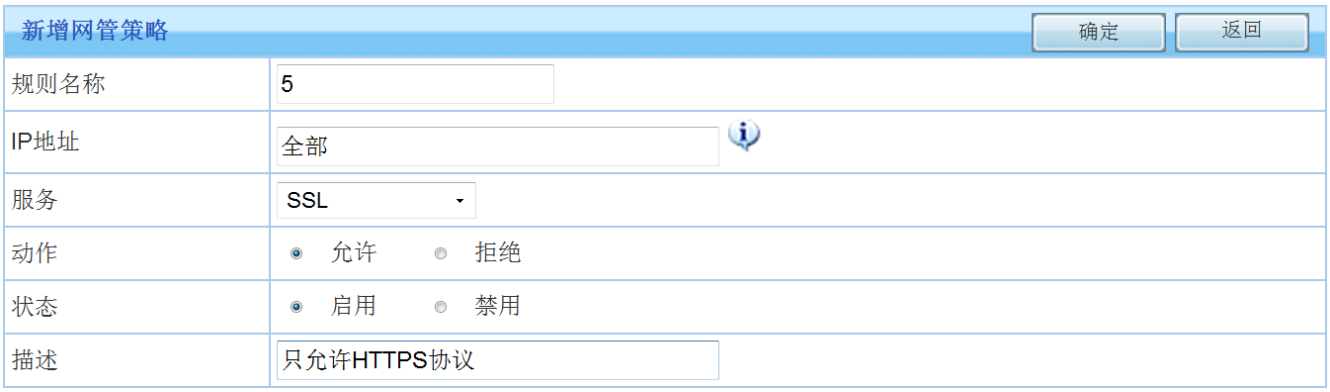


图207. 新增网管策略

第四：改变“状态”栏的值，再点击<修改状态>可以改变配置条目的状态。

提示：

1、 策略类型：默认为“允许所有 IP 网管”，这时所有 IP 都可以网管设备。

2、 策略类型选择为“根据下面策略进行控制”时，如果网管策略里没有配置任何策略，则所有 IP 都可以网管设备；如果配置了策略，则只有符合这些策略的才可以网管设备。

3、 状态复选框：勾选，表示此条配置的状态为“启用”。不勾选，即此条配置的状态为“禁用”，即此策略未生效。

18.4 网管参数

功能描述：对网管参数的设置，包括 WEBUI 及 SSH 网管参数的设置。

配置路径：【系统配置】>【网管参数】

图208.　网管参数

参数说明：

- WEBUI网管方式：支持安全的 HTTPS 方式和传统的 HTTP 方式，默认为HTTPS方式 。
- WEBUI登录端口：为安全起见，系统的 WEB 网管默认采用 TCP 9090 端口，可以改成 TCP 协议的其它端口，不能改成正在使用的端口，如 80 端口、9091端口、2222端口等。
- WEBUI超时：WEBUI未操作超时时间，默认 10 分钟。
- REPORTER登录端口：为安全起见，系统的 WEB 网管默认采用 TCP 9091 端口，可以改成 TCP 协议的其它端口，不能改成 80 端口。
- REPORTER超时：REPORTER的WEBUI未操作超时时间，默认 10 分钟。
- SSH登录端口：为了安全性，系统的 SSH 网管默认采用 TCP 2222 端口，可以改成 TCP 协议的其它端口。
- 管理员最大登录次数：管理员账号登录WEB 管理设备，允许连续输错密码的最大次数。
- 管理员超出登录次数惩罚时间：管理员输错密码的次数超过最大限制次数后，加入惩罚的时间，惩罚时间过后，才允许输入正确的用户名、密码。

18.5 SNMP 服务器

功能描述：当设备作为 SNMP 服务器时，配置允许访问该SNMP 服务器的 SNMP 客户端 IP 地址。

配置路径：【系统配置】>【SNMP服务器】

配置描述：进入【SNMP服务器】页面，配置允许访问该SNMP 服务器的 SNMP 客户端 IP 地址。如下图：

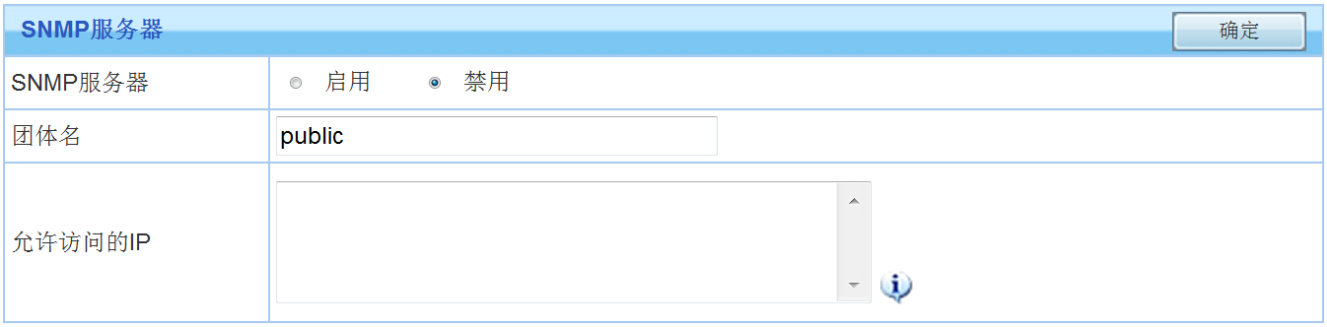


图 28. SNMP 服务器

18.6 网络工具

“网络工具”包括 Ping 、TraceRoute、捕获数据包、查看数据包、上网故障调试五部分。

18.6.1 Ping

功能描述：用于测试网络的连通性。

配置路径：【系统配置】>【网络工具】>【Ping】，设置界面如下图：

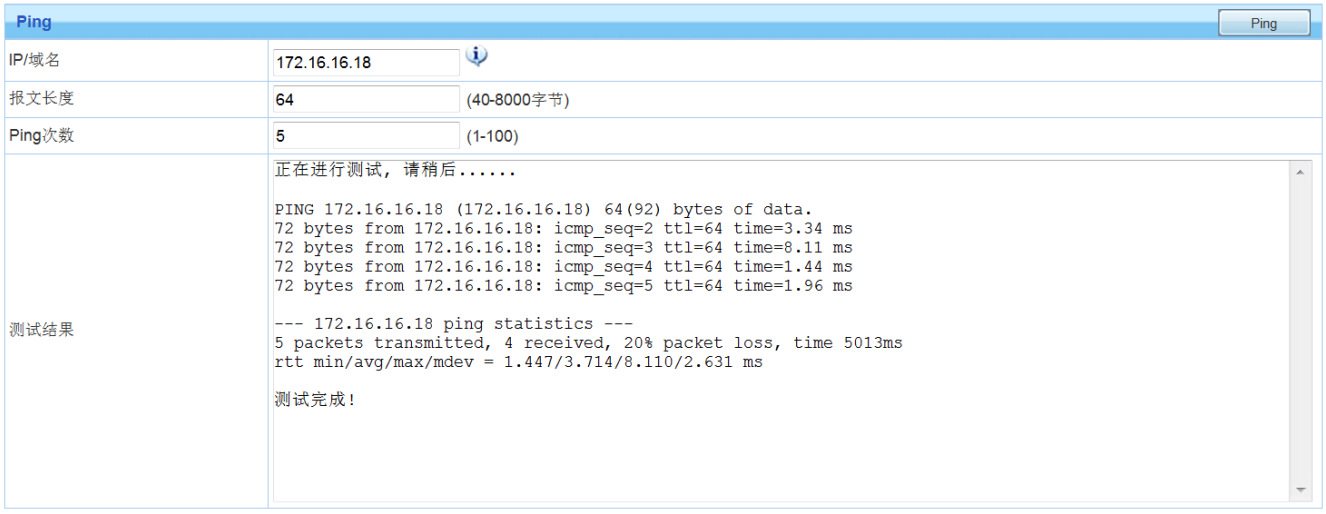


图209.　　PING 工具

参数说明：

- IP/域名：目的 IP 地址或者域名，如果设置域名，需要先配置本机DNS。
- 报文长度：Ping报文的长度，20-8000 字节，默认64字节。
- Ping次数： 发送Ping报文的数量，1～2000000000，默认 5次。

> **提示：**如果输入域名，需要先配置本地 DNS 服务器，详见【网络配置>DNS 配置】。

18.6.2 TraceRoute

功能描述：用于确定 IP 数据访问目标所采取的路径。

配置路径：【系统配置】>【网络工具】>【TraceRoute】，设置界面如下图：

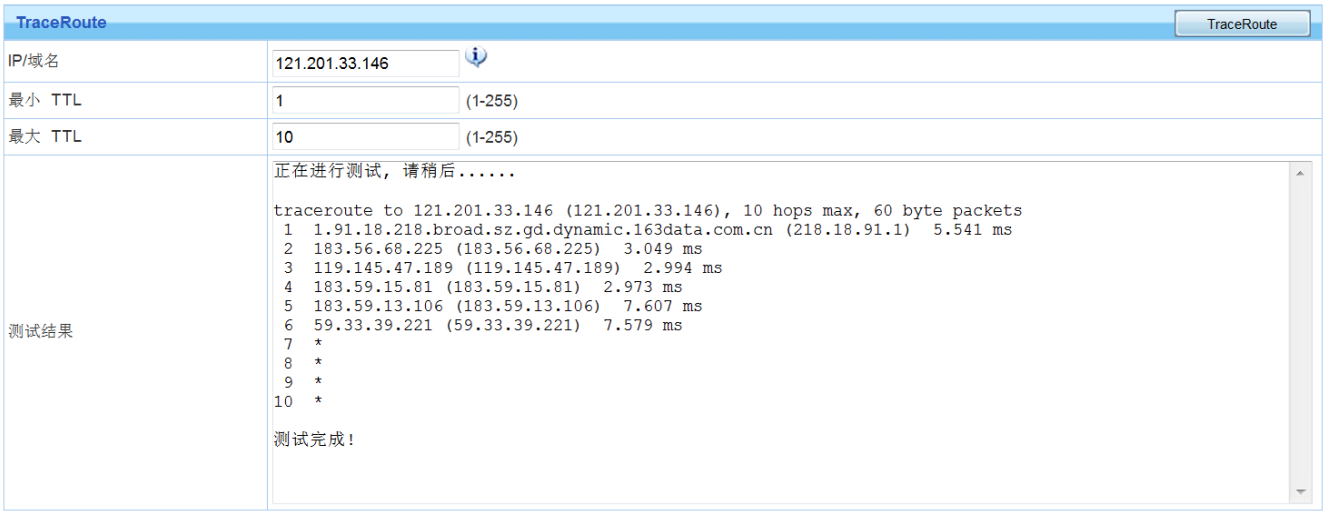


图210. TraceRoute 工具

参数说明：

- IP/域名：目的 IP 地址或者域名，如果设置域名，需要先配置本机DNS。
- 超时设置：1-10秒，缺省 10秒。
- 最小 TTL：1-255，缺省 1。
- 最大 TTL：1-255，缺省 10。

> **提示：**如果输入域名，需要先配置本地 DNS 服务器，详见【网络配置>DNS 配置】。

18.6.3 捕获数据包

功能描述：配置捕获数据报文的规则，然后可以捕获数据报文，进行故障排除分析。

配置路径：【系统配置】>【网络工具】>【捕获数据包】

配置描述：进入【捕获数据包】页面，如下图：

图211. 捕获数据包 1

图212. 捕获数据包 2

参数说明：

- 捕获报文个数：捕获报文的总个数。
- 物理接口：捕获在此接口收到的报文，“全部”代表设备所有的物理接口。
- 简易配置：根据报文源 IP、目的 IP、源端口、目的端口和协议类型来捕获报文。
- 高级配置：根据过滤正则表达式来进行报文的捕获。如要抓取单个 IP 地址的所有 TCP 包，则输入：host 1.1.1.1 and tcp。

配置好捕获规则后，点击<开始捕获>按钮，开始报文的捕获。点击<停止捕获>，停止报文的捕获。然后到【系统配置>网络工具>查看数据包】页面去查看捕获到的数据包文件。

18.6.4 查看数据包

功能描述：查看已捕获的数据报文。

配置路径：【系统配置】>【网络工具】>【查看数据包】

配置描述：进入【查看数据包】页面，如下图：

图213. 查看数据包

点击<下载>按钮后，即下载已捕获的的文件，然后可通过 Sniffer 或 Ethereal 等软件进行报文分析。

18.6.5 上网故障调试

功能描述：下载调试信息。

配置路径：【系统配置】>【网络工具】>【上网故障调试】

配置描述：进入【上网故障调试】页面，如下图：

图214. 上网故障调试

参数说明：

- 状态：启动或关闭【上网故障调试】。
- IP地址：输入单个IP地址，双向IP不能同时设置成全部。
- 端口：输入单个端口，当协议选择全部、TCP或UDP时，双向端口不能同时设置成全部。
- 协议类型：有全部、TCP、UDP、ICMP、ARP五个选项。

上网故障调试过程较耗费设备资源，慎用。

18.7 日期/时间

功能描述：用于设定设备的系统时间和日期。

配置路径：【系统配置】>【日期/时间】，设置界面如下图：

图215. 设置系统时间/日期

如需启用 SNTP 功能，则勾选[自动与 SNTP 服务器同步]，然后可配置[SNTP 服务器]和[同步间隔]。如下图：

图216. 设置系统时间/日期

点击<立即同步>按钮，可立即与所配置的服务器进行时间的同步。

提示：启用 [自动与SNTP服务器同步]后，系统日期和系统时间两项不可配置。

18.8 系统信息

功能描述：设备基本信息描述。

配置路径：【系统配置】>【系统信息】，配置页面如下：

图217. 系统信息

18.9 邮件配置

功能描述：配置设备发送告警邮件的参数。

配置路径：【系统配置】>【邮件配置】，配置页面如下：

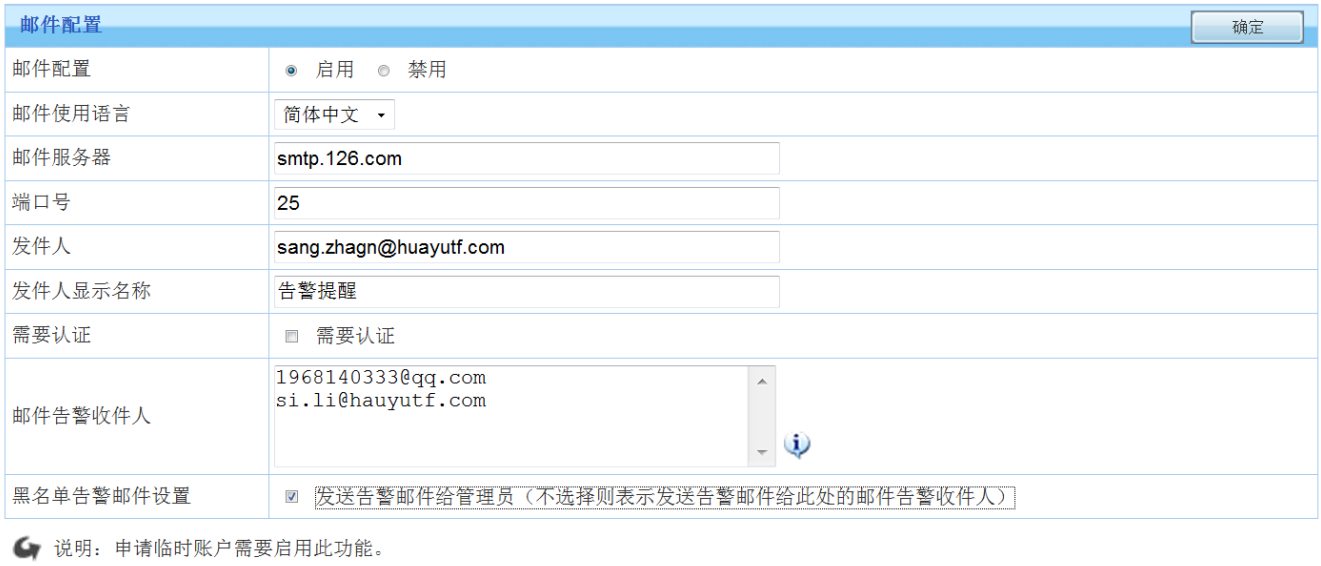


图218.　　邮件配置

参数说明：

- 邮件使用语音：发送邮件时使用的语言。
- 邮件服务器：设置邮件发服务器地址。
- 端口号：设置邮件端口号，端口对应加密方法相应端口号。
- 发件人：设置告警邮件的发送者。
- 发件人显示名：设置告警邮件发送者显示的姓名。
- 需要认证：选择是否需要进行密码安全认证。
- 用户名：需要安全认证时，必须填入用户名。
- 密码：需要安全认证时，必须填入用户密码。
- 收件人：设置告警邮件的收件人邮箱地址，可以设置多个，一行一个收件人地址。
- 黑名单告警邮件设置：选择是否将告警邮件发送给管理员。

19　系统日志

“系统日志”包含：命令日志、事件日志、PPTP 日志、IPSEC 日志、日志服务器、告警配置、系统调试信息。

19.1 命令日志

功能描述：将管理员对设备配置的命令记录下来，以便查询。

配置路径：【系统日志】>【命令日志】

配置描述：进入【命令日志】页面，如下图：

图219. 查看命令日志

查询条件：

- 管理员：根据配置设备的管理员名称来查找。
- IP地址：根据配置设备的管理员使用的 IP 地址来查找
- 命令内容：根据配置的命令的内容来查找
- 执行结果：根据配置的结果(失败/成功)来查找
- 时间范围：根据管理员配置设备时的时间范围来查找

默认显示所有命令日志。输入查询条件后，点击<查询>按钮，显示满足查询条件的命令日志。

点击<清空>按钮，清空所有的命令日志。

19.2 事件日志

功能描述：设备提供事件日志，用于监视系统事件的发生。

配置路径：【系统日志】>【事件日志】

配置描述：进入【事件日志】页面，如下图：

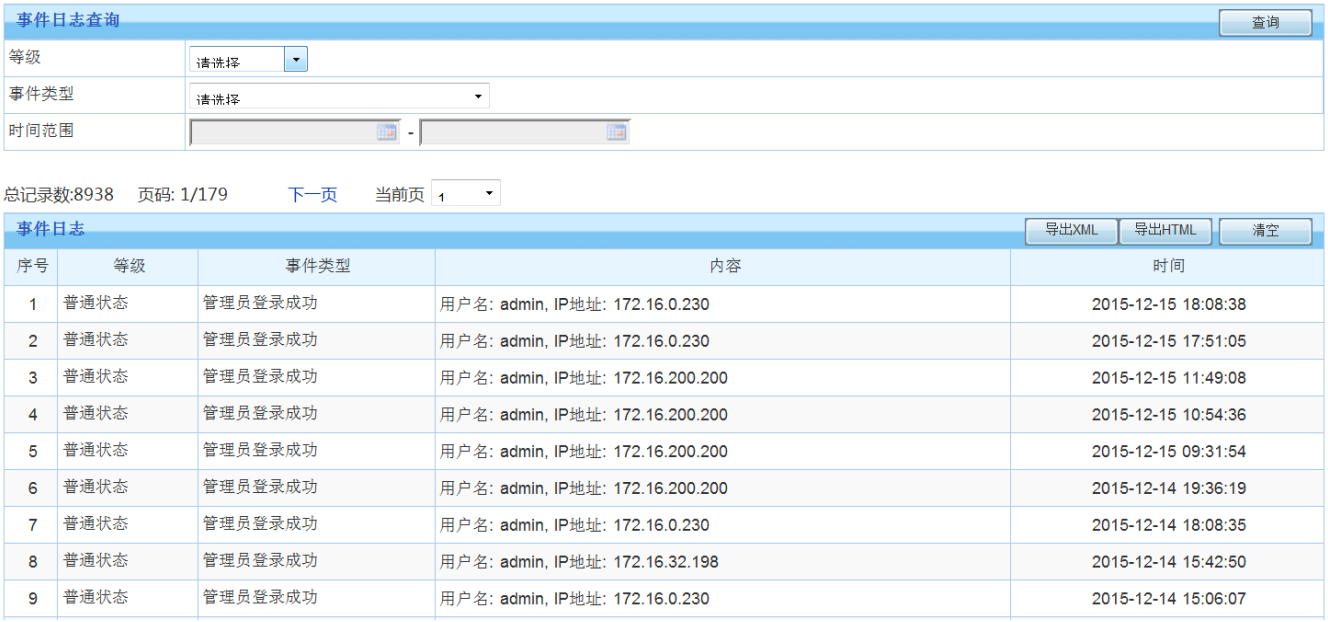


图220. 查看命令日志

事件日志的内容包括：管理员登录设备成功/失败、物理接口 UP/Down、设备启动成功、ARP 冲突、线路健康结果等等信息。

点击<清空>按钮，清空所有的命令日志。

19.3 PPTP 日志

功能描述：记录 PPTP 拨号的日志。

配置路径：【系统日志】>【PPTP 日志】

配置描述：

第一：进入【PPTP 日志】页面，如下图：

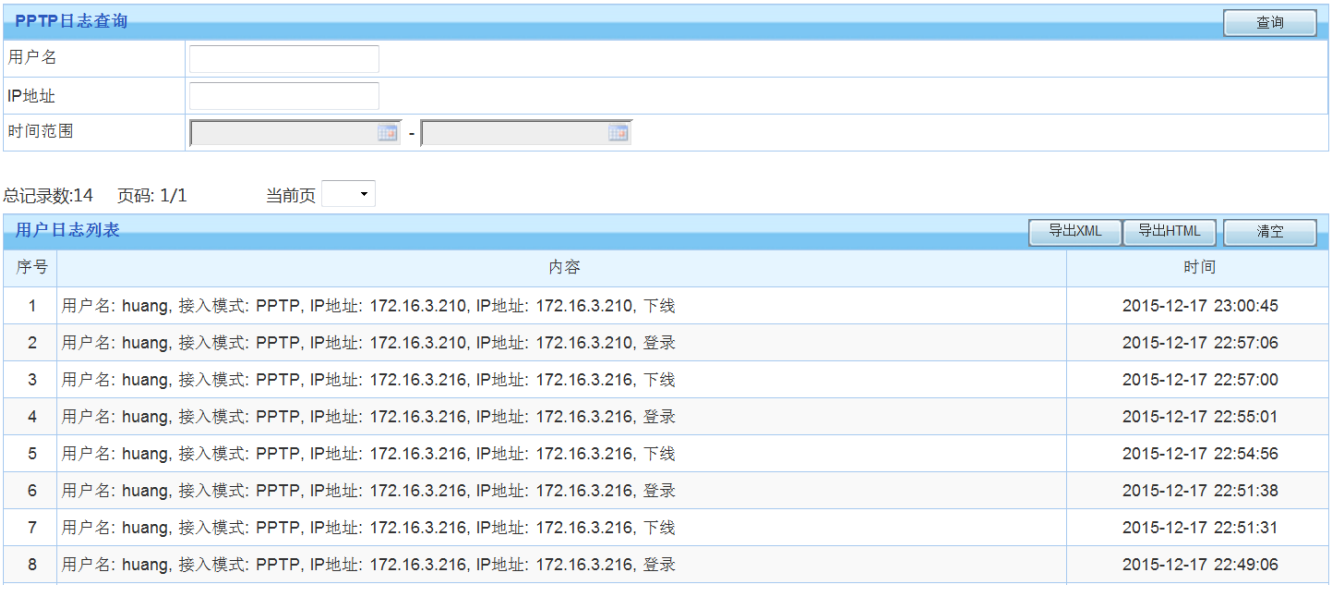


图221.　查看 PPTP 日志

查询条件：

- 用户名：根据用户名称来查找。
- IP地址：根据用户的 IP 地址来查找
- 时间范围：根据用户登录、认证、下线的时间范围来查找

默认显示所有 PPTP 日志。输入查询条件后，点击<查询>按钮，显示满足查询条件的用户日志。

点击<清空>按钮，清空所有的用户日志。

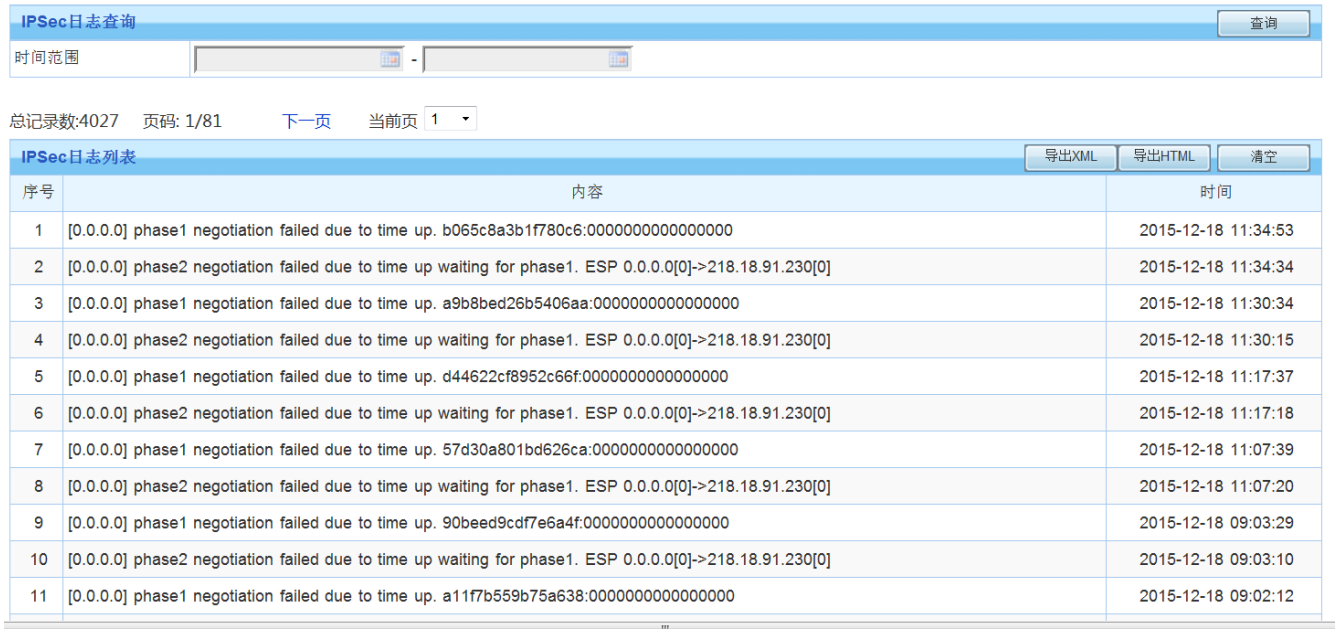
19.4 IPSEC 日志

功能描述：记录 IPSec VPN 连接的日志。

配置路径：【系统日志】>【IPSec 日志】

配置描述：

第一：进入【IPSec 日志】页面，如下图：



序号	内容	时间
1	[0.0.0.0] phase1 negotiation failed due to time up. b065c8a3b1f780c6:0000000000000000	2015-12-18 11:34:53
2	[0.0.0.0] phase2 negotiation failed due to time up waiting for phase1. ESP 0.0.0.0[0]->218.18.91.230[0]	2015-12-18 11:34:34
3	[0.0.0.0] phase1 negotiation failed due to time up. a9b8bed26b5406aa:0000000000000000	2015-12-18 11:30:34
4	[0.0.0.0] phase2 negotiation failed due to time up waiting for phase1. ESP 0.0.0.0[0]->218.18.91.230[0]	2015-12-18 11:30:15
5	[0.0.0.0] phase1 negotiation failed due to time up. d44622cf8952c66f:0000000000000000	2015-12-18 11:17:37
6	[0.0.0.0] phase2 negotiation failed due to time up waiting for phase1. ESP 0.0.0.0[0]->218.18.91.230[0]	2015-12-18 11:17:18
7	[0.0.0.0] phase1 negotiation failed due to time up. 57d30a801bd626ca:0000000000000000	2015-12-18 11:07:39
8	[0.0.0.0] phase2 negotiation failed due to time up waiting for phase1. ESP 0.0.0.0[0]->218.18.91.230[0]	2015-12-18 11:07:20
9	[0.0.0.0] phase1 negotiation failed due to time up. 90beed9cdf7e6a4f:0000000000000000	2015-12-18 09:03:29
10	[0.0.0.0] phase2 negotiation failed due to time up waiting for phase1. ESP 0.0.0.0[0]->218.18.91.230[0]	2015-12-18 09:03:10
11	[0.0.0.0] phase1 negotiation failed due to time up. a11f7b559b75a638:0000000000000000	2015-12-18 09:02:12

图222.　查看 IPSec 日志

时间范围：根据 IPSec VPN 连接时间范围来查找

默认显示所有 IPSec VPN 日志。输入查询条件后，点击<查询>按钮，显示满足查询条件的用户日志。

点击<清空>按钮，清空所有的 IPSec VPN 日志；点击<导出>按钮，可以将 IPSec VPN 日志以 HTML、XML 的格式导出。

19.5 日志服务器

功能描述：配置 Syslog 服务器。

配置路径：【系统日志】>【日志服务器】

配置描述：进入【日志服务器】页面，如下图：

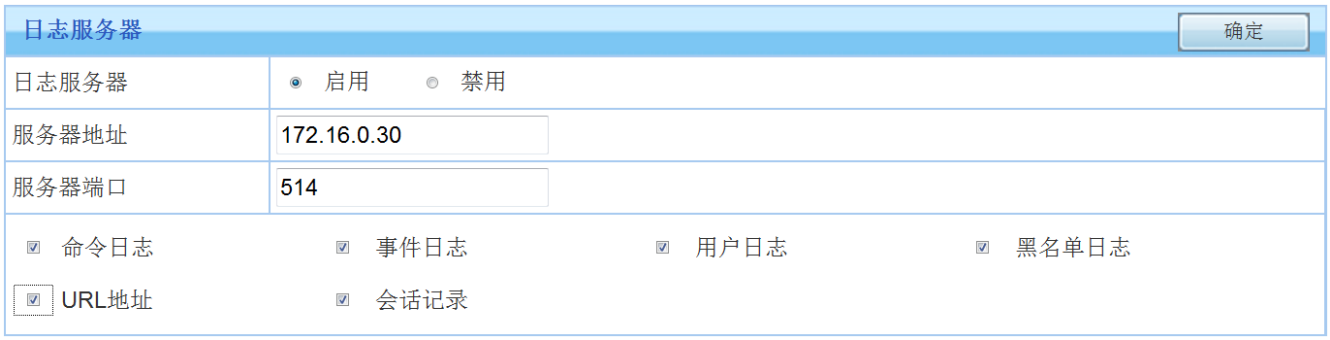


图223.　Syslog 服务器配置

参数说明：

- 日志服务器：启用或禁用 Syslog 服务器，启用后设备将会向 Syslog 服务器发送日志消息；
- 服务器地址：Syslog 服务器的IP地址；
- 服务器端口：与Syslog 服务器通信的端口号，默认是514。

19.6 告警配置

功能描述：配置设备发送告警邮件的参数。

配置路径：【系统配置】>【告警配置】，配置页面如下：

图224.　告警配置

参数说明：

告警功能有四种级别：普通状态、预警状态、严重状态、紧急状态；

告警策略：日志记录、邮件告警、syslog 服务器接收告警信息，及其组合方式产生告警的信息。

- 日志记录，即本地告警日志，详见内置报表中心【日志查询>告警记录】菜单。

- ✧ 邮件告警，即以邮件的方式将告警信息发送到指定邮箱。邮箱参数的设置详见【网络配置>邮件配置】。
- ✧ Syslog，即以标准的 syslog 格式将告警信息发送到指定 Syslog 服务器。Syslog 参数详见【系统日志>日志服务器】。
- ➢ 事件告警：系统级别的事件日志将产生告警，如接口UP/Down、系统重启等。
- ➢ 黑名单告警：用户进出黑名单的产生告警。
- ➢ 监控告警：当CPU和内存使用率，以及活跃会话数大于预设阈值时，产生告警。
- ➢ 违规网站：当内网终端访问指定网站时，产生告警。需在【系统对象>URL库】预先自定义URL。

19.7 调试信息下载

功能描述：下载调试信息。

配置路径：【系统日志】>【调试信息下载】

配置描述：进入【调试信息下载】页面，如下图：

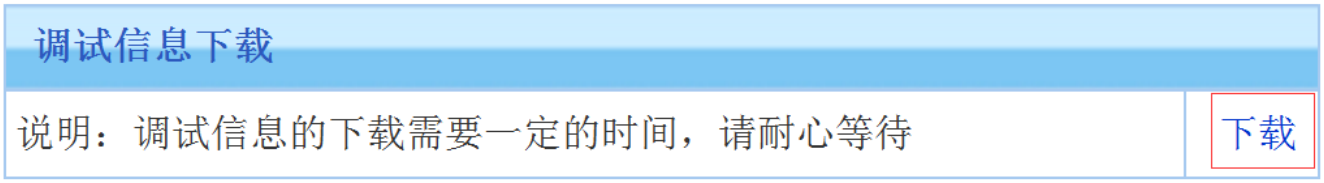


图225. 调试信息下载

点击<下载>按钮后，即下载调试信息的文件，文件是加密的，需要提供给研发。

20 报表中心

报表中心包括日志审计策略和内置报表中心两部分。其中设备提供的内置报表中心，无需另外安装外置报表中心即可实现对实时监控、统计分析、行为分析的记录与查询功能。在内置报表中心，默认已开启对流量的实时监控、统计分析，应用内容过滤等所有的记录。

20.1 日志审计策略

功能描述：针对用户的上网行为进行审计。

配置路径：【报表中心】>【日志审计策略】

配置描述：

第一：进入【日志审计策略】页面，如下图：

图226.　日志审计策略

图227.　审计选项

参数说明：

- 审计策略：　系统管理员可以通过新增按钮选择需要 审计的用户信息，如：WEB记录、会话记录等。
- 审计选项：默认情况下，审计方式为全部审计，系统管理员可以通过修改审计方式访问网站日志记录选项等更改需要审计的用户信息。

第二：点击<新增>按钮，增加日志审计策略。选择“日志审计策略”选项卡。勾选需要进行审计的上网行为记录的“选定”复选框，包括 WEB 记录、会话记录、统计记录和告警记录。再次是对选定的条目进行 “生效时间”的选择。若需要对选定的条目进行“生效时间”的批量配置，则在“快速链接”后面的“IP 组”选择相应的配置。配置界面如下图：

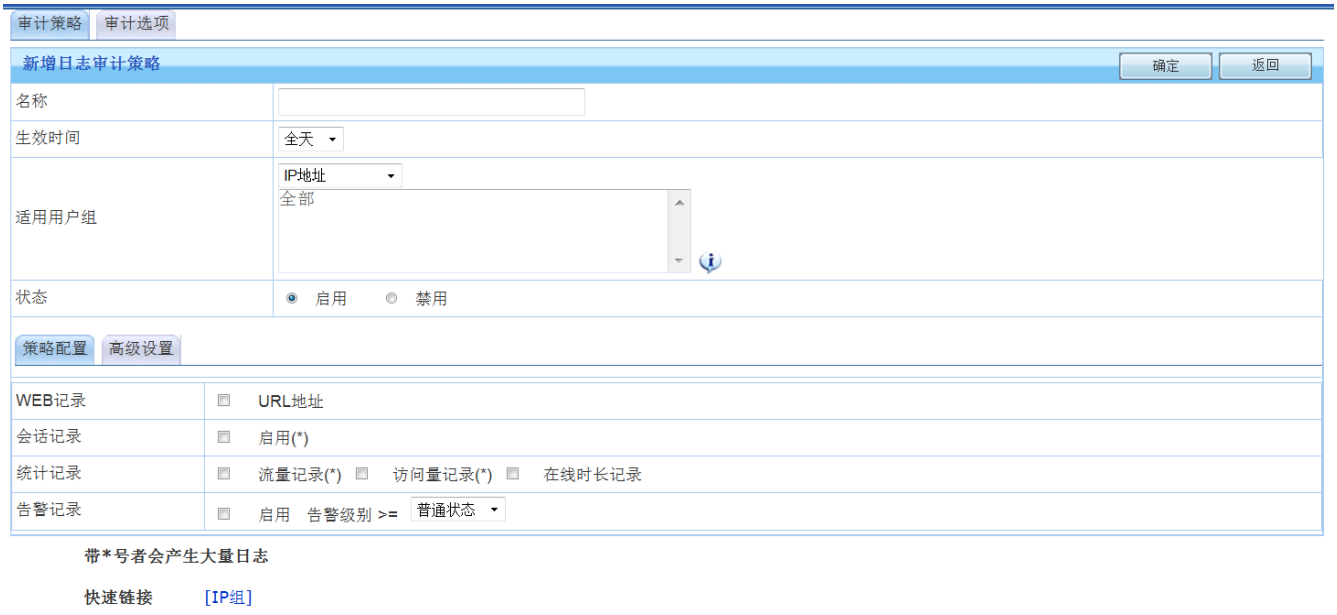


图228.　　新增上网策略-上网审计策略

第三：选择生效适用用户组 ，用户分为：用户及用户组、IP、IP 组，可勾选组织结构用户、用户组。

20.2 内置报表中心

功能描述：进入内置报表中心查看统计记录。

配置路径：【报表中心】>【内置报表中心】

配置描述：点击【内置报表中心】，进入内置报表中心首页。如下图：

图229.　　内置报表中心首页