配置手册

RG-UAC6000 系列上网行为管理与审计系统

文档版本号：V1.0

版权声明

锐捷网络©2013

锐捷网络版权所有，并保留对本手册及本声明的一切权利。

未得到锐捷网络的书面许可，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。

、

、

、

、

、

、RGOS®、RGNOS®、

、

、

、锐捷®都是锐捷网络的注册商标，不得仿冒。

免责声明

1 本手册内容依据现有信息制作，由于产品版本升级或其他原因，其内容有可能变更。锐捷网络保留在没有任何通知或者提示的情况下对手册内容进行修改的权利。

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

前　言

版本说明

本手册对应的软件版本为：RG-UAC 6000　1.7.2

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷网络官方网站：http://www.ruijie.com.cn/ 。
- 锐捷网络在线客服：http://webchat.ruijie.com.cn。
- 锐捷网络远程技术支持中心：http://www.ruijie.com.cn/service.aspx 。
- 7×24 小时技术服务热线：4008-111-000
- 锐捷网络技术论坛：http://support.ruijie.com.cn
- 锐捷网络技术支持与反馈信箱：service@ruijie.com.cn

相关资料

手册名称	说明
产品 安装手册	本手册介绍了产品在功能和物理上的一些特性，提供了设备安装步骤、硬件故障排除、模块技术规格，以及电缆和连接器的规格和使用准则等。
产品 命令手册	本手册对产品支持的配置命令做了详细的描述。包括命令模式、参数说明和使用指南等，并配有具体的实例。
产品 WEB 管理手册	本手册对产品支持的各功能的 WEB 界面进行描述，并配有详细的配置实例。

本书约定

1)　命令行格式约定

命令行格式意义如下：

粗体：命令行关键字（命令中保持不变必须照输的部分）采用加粗字体表示。

斜体：命令行参数（命令中必须由实际值进行替代的部分）采用斜体表示

[ ] ：表示用[ ] 括起来的部分，在命令配置时是可选的。

{ x | y | ... }：表示从两个或多个选项中选取一个。

[x | y | ...]：表示从两个或多个选项中选取一个或者不选。

//：由双斜杠开始的行表示为注释行。

2)　图形界面格式约定

【】：表示用【】括起来的部分代表菜单或子菜单名称。

> ：代表 WEB 网管配置路径：如【系统对象】>【地址簿】，表示“系统对象”菜单下的“地址簿”菜单。

<>：代表窗口中的选项或按钮名称。

3)　各类标志

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

注意、警告、提醒操作中应注意的事项。

说明、提示、窍门、对操作内容的描述进行必要的补充。

对于产品支持情况进行必要的补充。

---

4)　说明

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

目录

1 本手册内容依据现有信息制作，由于产品版本升级或其他原因，其内容有可能变更。锐捷网络保留在没有任何通知或者提示的情况下对手册内容进行修改的权利。 2
目录 5
第一部分 产品概述 14
1 图形界面格式约定 14
2 WEB 管理概述 14
3 配置环境要求 15
3.1 客户端要求 15
3.2 服务器要求 15
3.3 接线方式 15
4 登陆 WEB 管理平台 16
第二部分 产品配置 18
5 系统配置 18
5.1 设备工作模式 18
5.1.1 网桥模式 18
5.1.2 路由模式 19
5.1.3 旁路模式 20
5.2 系统维护 22
5.2.1 系统升级 22
5.2.2 自动升级 23
5.2.3 备份与恢复 24
5.2.4 重启/关机 24
5.3 系统管理员 25
5.3.1 配置系统管理员 25
5.4 网管策略 27
5.5 网管参数 28
5.6 网络工具 29
5.6.1 Ping 29

5.6.2 TraceRoute 30
5.6.3 端口检测 31
5.7 日期/时间 32
5.8 系统信息 32
5.9 邮件配置 33
5.10 集中管理 34
6 设备状态 35
7 实时监控 36
7.1 设备资源 36
7.2 物理接口 37
7.3 服务监控 38
7.3.1 服务趋势叠加图 38
7.3.2 服务组趋势图 39
7.3.3 活跃服务统计 40
7.3.4 所有服务统计 41
7.4 用户监控 42
7.4.1 流量分析 42
7.4.2 会话分析 43
7.4.3 活跃会话 44
7.5 上网行为 44
7.6 在线用户 45
8 系统对象 46
8.1 地址簿 47
8.2 网络服务 47
8.2.1 自定义普通服务 47
8.2.2 自定义特征识别 49
8.2.3 自定义论坛/网评特征 50
8.2.4 协议剥离 51
8.3 时间计划 52
8.4 URL 库 54
8.5 关键字组 55
8.6 文件类型 56
8.7 证书管理 57
8.7.1 本地证书 57
9 网络配置 58

9.1 接口配置 58
9.1.1 物理接口 58
9.1.2 链路聚合 59
9.1.3 VLAN 接口 60
9.1.4 外网设置 61
9.1.5 GRE 隧道 62
9.1.6 网口模式 63
9.2 配置 IP 地址 64
9.3 静态路由 64
9.4 OSPF 路由 65
9.4.1 网络配置 65
9.4.2 接口配置 66
9.4.3 参数配置 67
9.4.4 虚链路配置 68
9.4.5 信息显示 69
9.5 策略路由 71
9.5.1 策略路由 71
9.5.2 均衡策略 73
9.5.3 持续路由 74
9.5.4 链路健康检查 75
9.6 DNS 配置 77
9.7 DDNS 配置 77
9.8 智能 DNS 78
9.8.1 全局配置 78
9.8.2 线路配置 79
9.8.3 均衡策略 80
9.8.4 DNS 策略 81
9.9 ARP 表 83
9.10 DHCP 配置 84
9.10.1 基本参数 84
9.10.2 DHCP 中继 86
9.10.3 已分配 IP 地址 87
9.11 SNMP 服务器 87
9.12 代理服务器列表 87
9.13 代理配置 88

10 防火墙 89
10.1 安全策略 89
10.2 NAT 规则 91
10.2.1 内网代理 92
10.2.2 一对一地址转换 93
10.2.3 端口映射 95
10.2.4 服务器池 97
10.3 防 DOS 攻击 98
10.4 ARP 欺骗防护 99
10.5 应用层网关 100
10.6 加速老化 100
10.7 移动终端管理 101
11 组织管理 102
11.1 组织结构 102
11.1.1 定位并选中当前操作对象 102
11.1.2 修改根组 103
11.1.3 新增子组 104
11.1.4 修改子组 105
11.1.5 新增普通用户 107
11.1.6 新增认证用户 108
11.1.7 修改用户 109
11.1.8 绑定检查 110
11.1.9 导出用户和组 115
11.1.10 移动用户和组 116
11.1.11 删除用户和组 117
11.1.12 查询用户和组 118
11.1.13 在线离线合并排序 118
11.1.14 清空当前组 119
11.1.15 策略列表 120
11.2 批量导入 120
11.3 LDAP/AD 导入 121
11.4 扫描内网主机 122
11.5 临时账号管理 124
11.5.1 临时账号设置 124
11.5.2 批量生成 125
11.5.3 申请临时账户 126
11.5.4 未审核账户列表 127
11.5.5 已审核账户列表 128
11.6 DKey 管理 129

12 流量管理 130
12.1 线路带宽配置 130
12.2 基于策略的流控 131
12.3 基于用户的流控 136
13 行为管理 138
13.1 认证策略 138
13.2 上网策略 141
13.2.1 上网权限策略 142
13.2.2 终端提醒策略 150
13.2.3 准入策略 150
13.2.4 应用限额策略 151
13.2.5 黑名单策略 152
13.2.6 上网审计策略 154
13.3 认证选项 155
13.3.1 跨三层 MAC 识别 155
13.3.2 认证参数 156
13.3.3 终端提示页面定制 157
13.3.4 未认证权限 157
13.3.5 SSO 159
13.3.6 短信认证 161
13.4 认证服务器 164
13.4.1 RADIUS 服务器 164
13.4.2 AD 服务器 165
13.4.3 LDAP 服务器 166
13.4.4 POP3 服务器 167
13.4.5 SMP 服务器 168
13.4.6 服务器测试 169
13.5 白名单管理 170
13.5.1 IP 白名单 170
13.5.2 URL 白名单 172
13.5.3 即时通讯白名单 173
13.6 黑名单管理 174

14 酒店管理 176
14.1 即插即用 176
15 VPN 配置 177
15.1 IPSec 177
15.1.1 IPSec 隧道 177
15.1.2 IPSec 规则 178
15.2 PPTP 179
15.3 L2TP 181
15.4 VPN 用户 182
16 HA 配置 183
17 系统日志 184
17.1 命令日志 184
17.2 事件日志 185
17.3 PPTP/L2TP 日志 186
17.4 IPSec 日志 187
17.5 日志服务器 188
17.6 短信配置 189
17.7 告警配置 190
18 故障排除 191
18.1 捕获数据包 191
18.2 查看数据包 192
18.3 调试信息下载 193
18.4 上网故障调试 193
19 报表中心 194
19.1 报表中心配置 194
19.2 内置报表中心 195
20 登录报表中心 197
20.1 登录内置报表中心 197
20.1.1 首页 197
21 统计分析 198

21.1.1 设备资源 198
21.1.2 物理接口 202
21.2 用户统计 203
21.2.1 流量统计 203
21.2.2 会话统计 204
21.2.3 活跃会话 206
21.3 用户组统计 208
21.3.1 流量统计 208
21.3.2 会话统计 209
21.3.3 活跃会话 211
21.4 服务统计 213
21.4.1 流量统计 213
21.4.2 会话统计 214
21.4.3 活跃会话 216
21.5 服务类型统计 218
21.5.1 流量统计 218
21.5.2 会话统计 220
21.5.3 活跃会话 222
21.6 URL 统计 223
21.6.1 流量统计 223
21.6.2 会话统计 225
21.6.3 活跃会话 227
21.7 URL 类型统计 229
21.7.1 流量统计 229
21.7.2 会话统计 231
21.7.3 活跃会话 233
21.8 线路统计 234
21.8.1 流量统计 234
21.8.2 会话统计 236
21.8.3 活跃会话 238
21.9 URL 访问量统计 239
21.9.1 基于 URL 统计 239
21.9.2 基于 URL 类型统计 240
21.9.3 基于用户统计 242
21.9.4 基于用户组统计 243
21.10 网页文件访问次数统计 245
21.10.1 基于文件类型统计 245
21.10.2 基于用户统计 246
21.10.3 基于用户组统计 248
21.10.4 上网时长统计 249

22 日志查询 251
22.1 上网行为 251
22.1.1 所有行为 251
22.1.2 网页标题 252
22.1.3 网页 URL 252
22.1.4 网页搜索 253
22.1.5 邮件收发 254
22.1.6 IM 聊天 255
22.1.7 论坛微博 256
22.1.8 账号登录 257
22.1.9 外发文件 257
22.1.10 外发信息 258
22.1.11 telnet 命令 259
22.1.12 阻断记录 260
22.2 会话记录 262
22.3 告警记录 263
23 系统日志 265
23.1 命令日志 265
23.2 事件日志 266
23.3 认证日志 267
23.4 PPTP 日志 268
23.5 黑名单日志 269
24 数据管理 270
24.1 数据列表 271
24.2 数据删除 271
25 报表管理 272
25.1 自动报表列表 272
25.2 自动报表配置 273
25.3 手动报表 275
26 系统配置 276
27 个人行为 276
27.1 综合记录 277

27.2 WEB 记录 279
27.2.1 网页标题 279
27.2.2 网页搜索 280
27.2.3 论坛微博记录 281
27.2.4 外发信息 282
27.2.5 URL 283
27.3 邮件收发 283
27.4 IM 聊天 285
27.4.1 QQ 通讯记录 285
27.4.2 MNS 通讯记录 286
27.4.3 Yahoo 通讯记录 286
27.4.4 SKYPE 通讯记录 286
27.4.5 Gtalk 通讯记录 286
27.4.6 阿里旺旺通讯记录 286
27.4.7 飞信通讯记录 286
27.5 账号登入 286
27.5.1 账号登入记录 286
27.6 外发文件 287
27.6.1 外发文件 287
27.7 Telnet 命令 288
27.7.1 Telnet 命令 288
27.8 导出个人行为记录 289

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】>【地址簿】，表示“系统对象”菜单下的“地址簿”菜单
<>	代表窗口中的选项或按钮名称

2　WEB 管理概述

WEB 管理通过使用浏览器如 IE 来管理网络设备，如统一上网行为管理与审计系统或路由器。

WEB 管理包括 WEB 服务器和 WEB 客户端两部分。WEB 服务器集成在设备上，用来接收和处理客户端发来的请求（读取 WEB 文件或执行命令请求），并把处理结果返回给客户端，WEB 客户端通常指网络浏览器，如 IE。

3 配置环境要求

3.1 客户端要求

- 网管使用 WEB 管理客户端的 WEB 浏览器登录到上网行为管理与审计系统 WEB 管理界面对上网行为管理与审计系统进行管理。客户端通常是指 PC，也可能是一些其它的移动终端设备，如笔记本电脑、IPAD 等
- 浏览器：支持 IE6.0、IE7.0、IE8.0 以及部分基于 IE 核心的浏览器，如傲游 maxthon 等。使用其它浏览器登录 WEB 管理时，可能出现乱码或格式错误等异常
- 分辨率：建议分辨率设置为 1024*768、1280*1024 及 1440*960，在其它分辨率下，页面字体和格式可能出现不对齐、不够美观等异常

3.2 服务器要求

- 上网行为管理与审计系统需要配置 WEB 管理登录认证信息
- 上网行为管理与审计系统需要配置管理 IP 地址

3.3 接线方式

请按照如下步骤进行设备的接线：

- 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。
- 用标准 RJ-45 以太网线将 LAN 口与内部局域网连接。
- 用标准 RJ-45 以太网线将 WAN 口与 Internet 接入设备相连接，如路由器、光纤收发器或 ADSL Modem 等。
- 桥接模式：LAN1 和 WAN1 为网桥 1，LAN2 和 WAN2 为网桥 2、……、LANm 和 WANm 为网桥 m（m≤9）。每个桥之间是独立通信的，桥之间不能传递数据。
- 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。

4 登陆 WEB 管理平台

设备默认使用 LAN1 作为网管口，LAN1 出厂地址为 192.168.1.200/24。设备 支持两种方式的 WEBUI 登录：

- 安全的 HTTPS 登录，默认端口 443。初始登录 URL 为：https:// 192.168.1.200
- 传统的 HTTP 登录，默认端口 80。初始登录 URL 为：http://192.168.1.200

系统默认支持 HTTPS 和 HTTP 的登录方式。输入登录 URL 后，按回车后将进入如下面页：

图 4-1 初始页面

选择好语言类型后，请在此对话框中输入用户名、密码。默认的管理员账号是 admin，密码是 firewall。正确输入用户名和密码后，点击<登录>按钮，认证成功后将进入 WEB 管理主页面，如下图：

图 4-2 WEB 管理平台主页面

当前管理员: admin
保存配置
在线客服
安全退出
设备状态
实时监控
系统配置
系统对象
网络配置
防 火 墙
组织管理
流量管理
行为管理
酒店管理
VPN配置
HA 配置
系统日志
故障排除
报表中心
设备版本信息 详细
系统版本 Test-8200-1.6.6
应用特征库 AIS-2.3.0.2
URL库 URL-2.3.0.2
授权类型 正式授权
设备资源 详细
CPU使用率 0.9%
内存使用率 24.2%
活跃会话数 232/524288
在线用户数 9
在线认证用户数 0
前十名服务实时速率分布 详细
SSL 28.7Kbps
Syslog 5.6Kbps
QQ/TM 2.3Kbps
HTTP 1.5Kbps
QQ邮箱 979.2bps
DNS 279.2bps
前十名站点排名
qq.com 23
mail.qq.com 10
show.qq.com 5
实时网络流量 详细
WAN1 Rx
WAN1 Tx
bps
20M
16M
12M
8M
4M
0M
20:41:00
20:44:20
20:47:40
前十名用户实时速率排名 详细
上行
下行
用户 上行 下行
172.16.160.120 3.9K 27.9K
172.16.161.3 1.7K 3.2K
172.16.162.254 332.0 244.8
172.16.0.167 389.6 115.2
172.16.166.166 254.4 0.0
172.16.162.220 48.0 0.0
0K 8K 16K 24K 32K 40K bps
最近五次事件日志 详细
时间 内容
2014-10-23 20:51:08 管理员登录成功, 用户名: admin, IP地址: 172.16.111.186
2014-10-23 20:51:06 管理员注销, 用户名: admin, IP地址: 172.16.111.186
2014-10-23 20:39:54 管理员登录成功, 用户名: admin, IP地址: 172.16.111.186
2014-10-23 20:22:20 管理员登录成功, 用户名: admin, IP地址: 172.16.166.166
2014-10-23 20:22:15 管理员登录失败, 用户名: , IP地址: 172.16.166.166
锐捷统一上网行为管理与审计系统 -- 技术支持论坛: support.ruijie.com.cn -- 技术支持电话: 4008 111 000

第二部分　产品配置

5　系统配置

“系统配置”主要包括设备工作模式、系统维护、系统管理员、网络配置、网管策略、重启操作、关机操作、网络工具、系统信息等。

5.1　设备工作模式

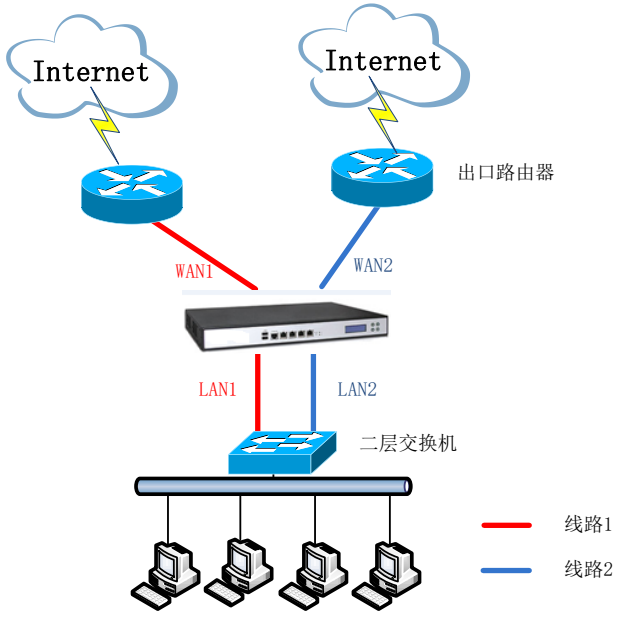
“设备工作模式”用来设置设备的工作模式，可以设定为网桥模式、路由模式和旁路模式，默认为网桥模式。用户可根据网络中的实际情况选择相应的接入模式。

5.1.1　网桥模式

功能描述：网桥模式是把“设备”视为一条带过滤功能的网线使用，把“设备”接在原有网关及内网用户之间，不用更改网络拓扑结构和配置，这种模式于用户可以做到完全“透明”。如下图所示：

图 5-1 单网桥模式

图 5-2 双网桥模式



配置路径：【系统配置】>【工作模式】

配置描述：进入【工作模式】页面，工作模式选择[网桥模式]，并配置[网桥类型]、[端口配置]、[网关 IP]。如下图：

图 5-3 工作模式

参数说明：

网桥类型：根据组网情况，选择网桥数，并为其配置 IP 地址（网桥的 IP 地址的配置是可选的）。未配置为网桥的端口为独立端口，可用于网管或路由。

端口配置：根据需要对未配置为网桥的端口进行 IP 地址的配置。

网关 IP：默认路由(0/0)的的网关地址。若不在此处配置，可以在【网络配置>路由配置>静态路由】页面进行默认路由的配置。

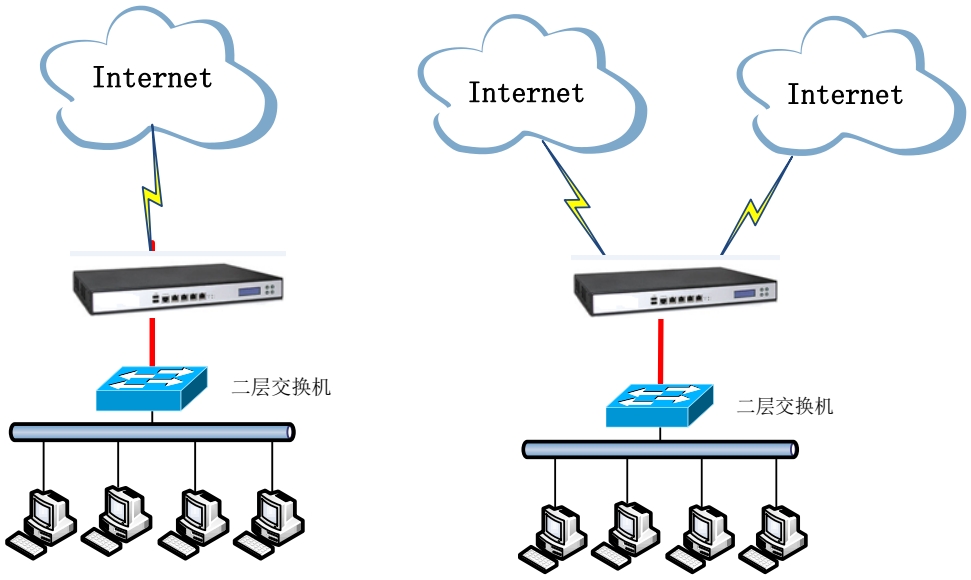
> 提示：
>
> 1、设备工作在网桥模式时，局域网内电脑的网关不需要改变。
>
> 2、设备工作在网桥模式时，必须保证原有上网数据穿透设备，即不能存在内网用户可绕过设备，到达原有网关的物理线路。
>
> 3、设备工作在网桥模式时，穿透数据时要保证 WAN 区接连接外网方向的路由设备，LAN 区接内网的交换机，不能接反。
>
> 4、设备的网桥模式是在数据链路层(OSI 第二层)上实现的透明，是通过把设备的两个网口桥接起来实现的。所以数据链路层及以上各层的数据均可穿透。
>
> 5、网桥模式时，设备支持 VLAN TRUNK 穿透，设备可以透明接在 VLAN TRUNK 的主干道

5.1.2 路由模式

功能描述：此模式下设备工作类似一个路由器，可以进行路由拓扑构造。每个物理接口可以工作在不同的子网中，使 LAN 与 Internet 之间建立一个安全网关。如下图所示：

图 5-4 单链路路由模式

图 5-5 双链路路由模式



配置路径：【系统配置】>【工作模式】

配置描述: 进入【工作模式】页面，工作模式选择[路由模式]，并配置[网桥类型]、[端口配置]、[网关 IP]。如下图：

图 5-6 路由模式

参数说明：

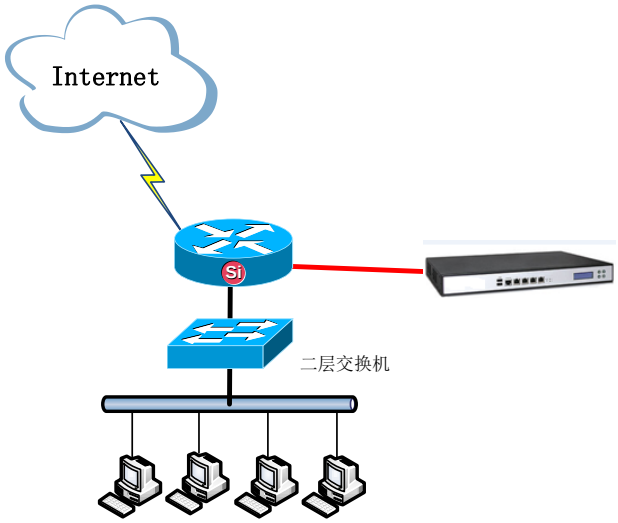
端口配置：根据需要对物理端口进行 IP 地址的配置。

网关 IP：默认路由(0/0)的的网关地址。若不在此处配置，可以在【网络配置>路由配置>静态路由】页面进行默认路由的配置。

5.1.3 旁路模式

功能描述：此模式下，设备只对网络中的数据进行记录和监控，不对网络中的数据进行过滤和控制。如下图所示：

图 5-7 旁路连接方式



配置路径：【系统配置】>【工作模式】

配置描述:进入【工作模式】页面，工作模式选择[旁路模式]，如下图：

图 5-4 旁路模式

参数说明：

端口配置：根据需要对物理端口进行 IP 地址的配置。

网关 IP：默认路由(0/0)的的网关地址。若不在此处配置，可以在【网络配置>路由配置>静态路由】页面进行默认路由的配置。

监控网段列表：被监控的内网 IP 地址。

5.2 系统维护

5.2.1 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：系统固件、应用特征库、URL 库、授权文件。

系统版本：设备软件程序

应用特征库：应用特征码的库文件

URL 库：内置 URL 库文件

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：

软件序列号：标示软件的唯一序列号。

硬件序列号：设备背板条形码，标识硬件唯一序列号

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 5-5 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<升级>按钮开始升级。如下图：

图 5-6 系统版本升级

提示：

1、未选中的文件类型后面显示当前的版本信息。

2、升级系统固件后，必须重启系统才能运行新的版本。

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

5.2.2 自动升级

功能描述：用户对“应用特征库”、“URL 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 5-7 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。

5.2.3 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 5-8 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.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>

5.2.4 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/关机】

配置描述：进入【重启/关机】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 5-9 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。

5.3 系统管理员

5.3.1 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】

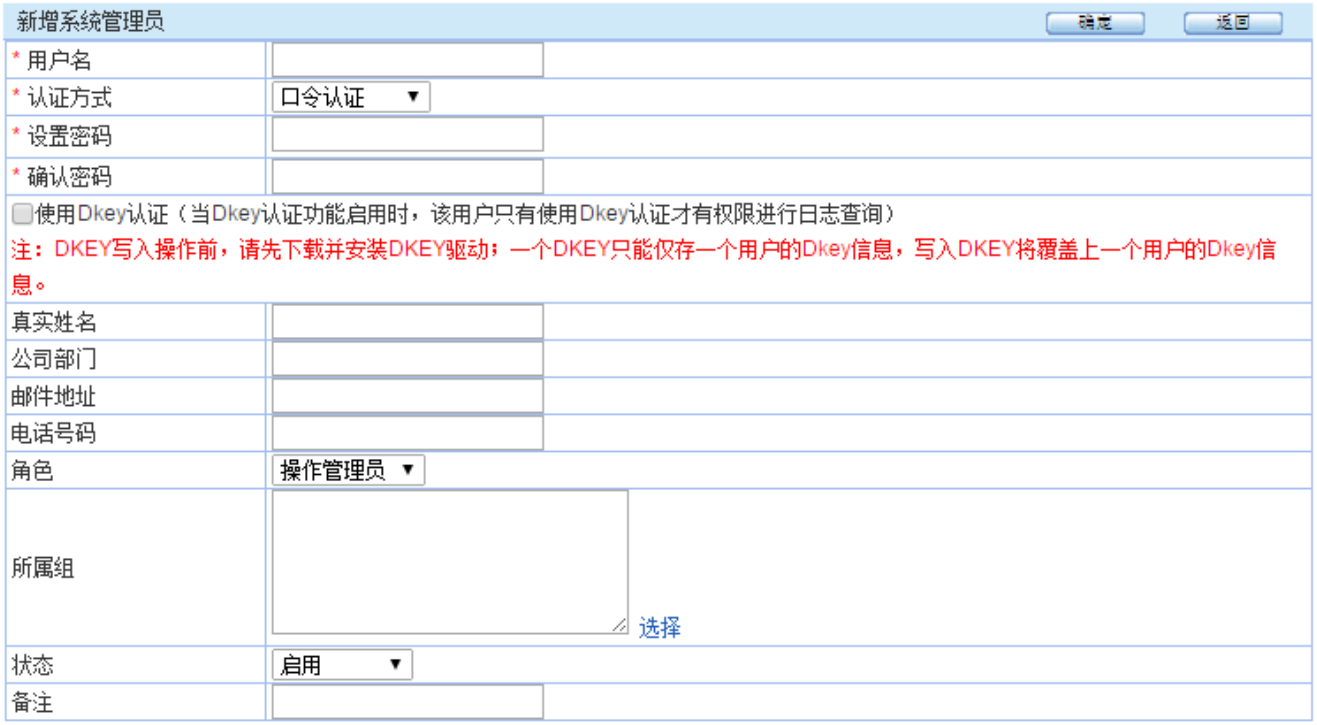
配置描述：

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 5-10 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 5-11 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：口令认证；

设置密码/确认密码：不限字符，但不能设置空格键；[必选项]

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：输入对应登录名的公司部门，不限字符；[可选项]

电话号码：即管理员的手机号码；[可选项]

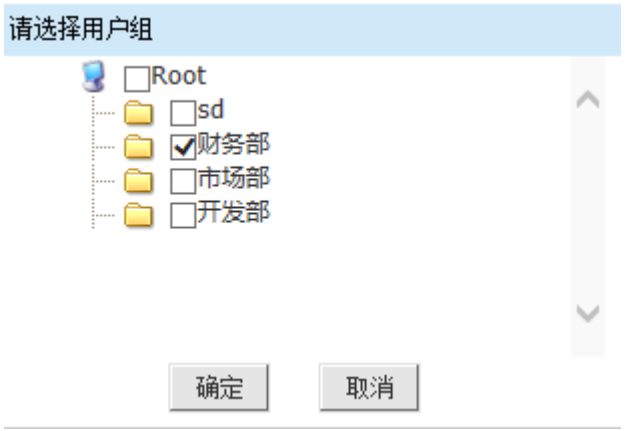
邮件地址：即管理员的邮箱地址，当管理员的配置信息有变更时，系统会通过邮件方式通知管理员；

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。

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/财务部”，那么 Mary 只能查看“根组(Root)”下的“财务部”组下的所有人的记录。点击<选择>按钮，可选择所属组，如下图：

图 5-12 权限分配



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]

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，默认密码为 firewall。
- guest：仅具有查看设备权限，默认密码为 guest123。默认不开启。
- audit：管理 Reporter，所属组为根组，默认密码为 audit123，该账号仅用于 reporter 界面登录，管理界面无登录权限。默认不开启。

2、 系统默认的管理员(admin、guest、audit)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、 新增的用户可以修改密码，可以被删除。

5、 具有管理 Reporter 权限的管理员 先登录了设备后 ,可以不用再次登录即可管理 Reporter。当先登录 Reporter，必须要再次登录才可以管理设备。

5.4 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：

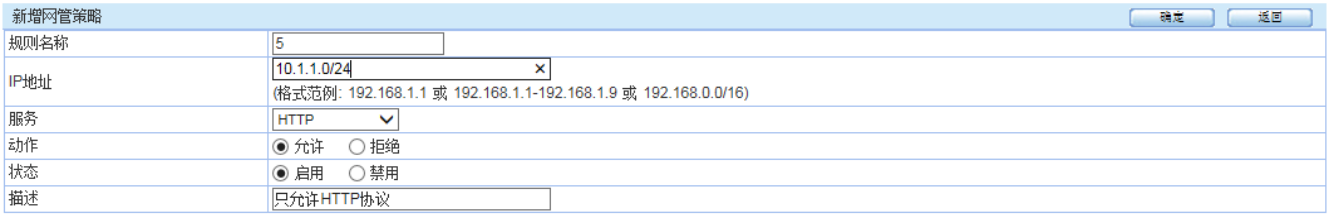
第一：进入【网管策略】页面，如下图：

图 5-13 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 5-14 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：
>
> 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。
>
> 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。
>
> 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

5.5 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 5-15 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，默认两种方式都可以登录设备 。

WEBUI 登录端口 :为安全起见 ,系统的 https WEB 网管默认采用 TCP 443 端口 ,可以改成 TCP 协议的其它端口，不能改成 80 端口。http WEB 网管默认采用 TCP 80 端口 ,可以改成 TCP 协议的其它端口 ,不能改成 443 端口。

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。

Telnet 登录端口：Telnet 端口默认为 2323，可以改成 TCP 协议的其他端口。

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。

5.6 网络工具

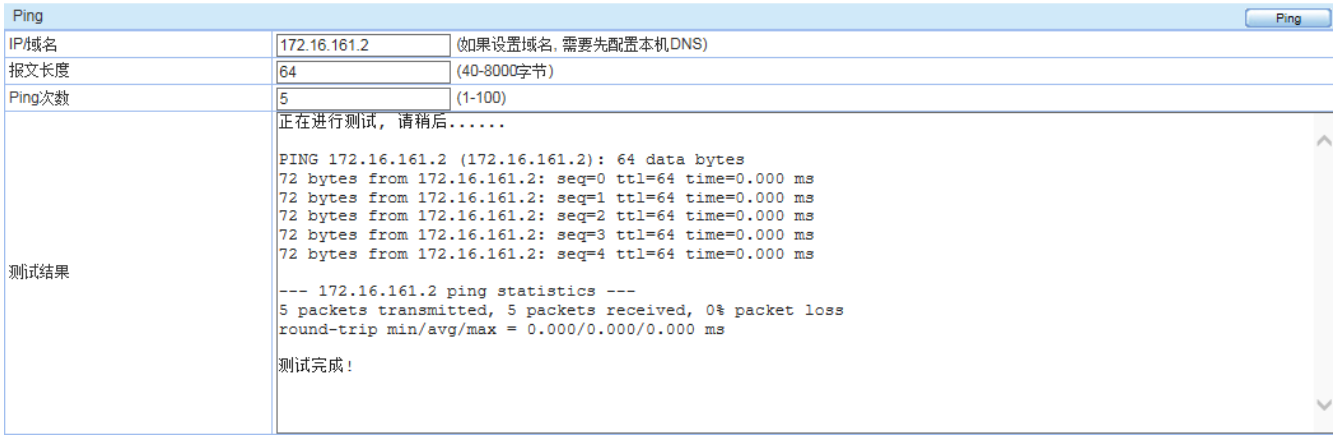
“网络工具”包括 Ping 和 TraceRoute 及端口检测。

5.6.1 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 5-16 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，40-8000 字节，默认 64 字节。

Ping 次数： 发送 Ping 报文的数量，1～100，默认 5 次。

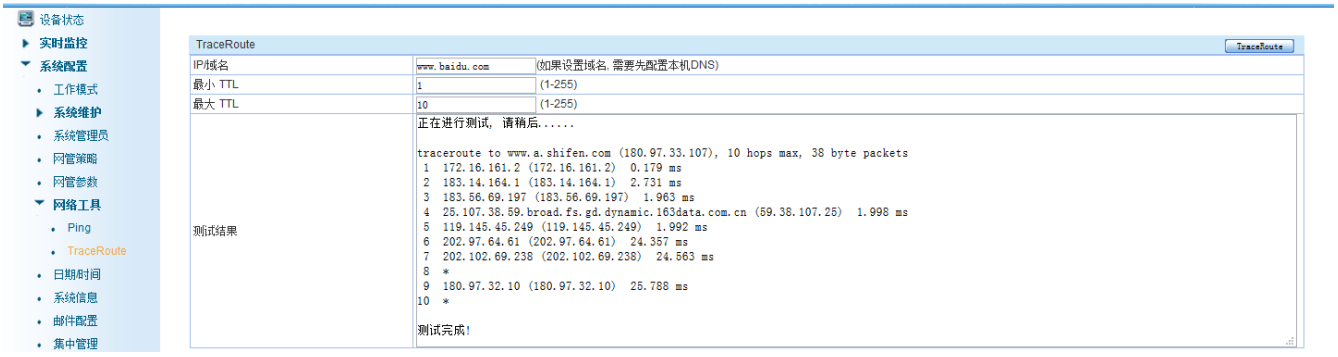
提示：如果输入域名，需要先配置本地 DNS 服务器，详见【网络配置>DNS 配置】。

5.6.2 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 5-17 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。

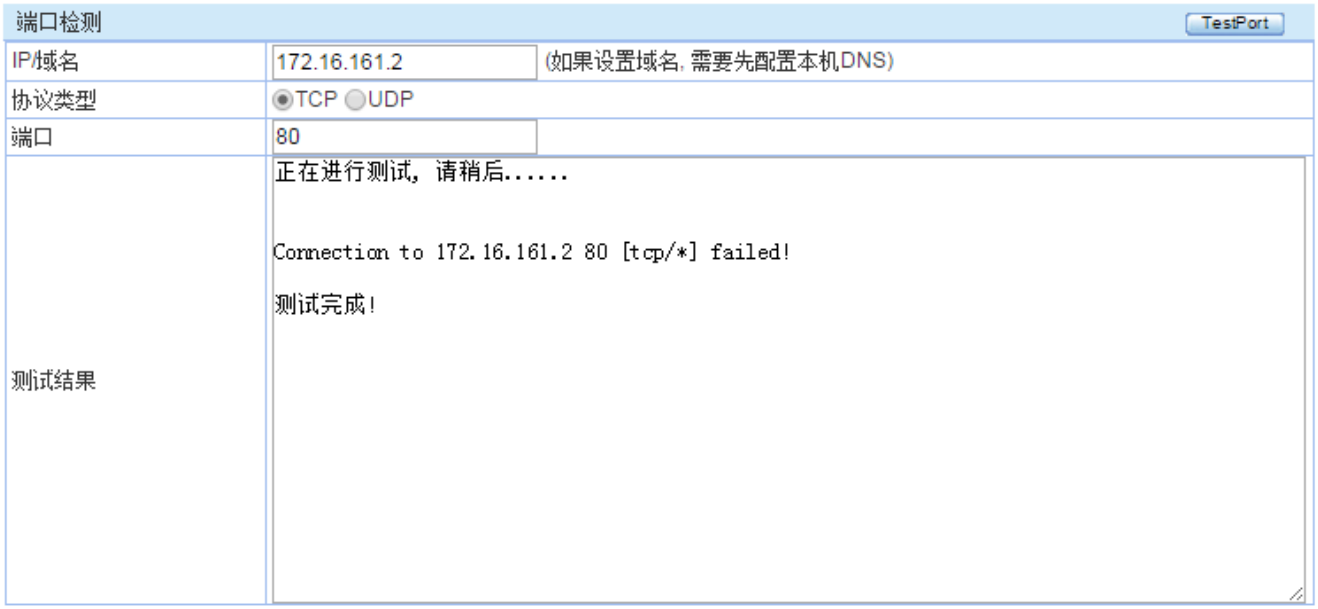
> **提示：**如果输入域名，需要先配置本地 DNS 服务器，详见【网络配置>DNS 配置】。

5.6.3 端口检测

功能描述：用于测试端口的连通性

配置路径：【系统配置】>【网络工具】>【端口检测】，设置界面如下图：

图 5-18 端口检测工具



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。

协议类型：端口的类型，可选择 TCP 或者 UDP。

端口号：需要检测的端口号。

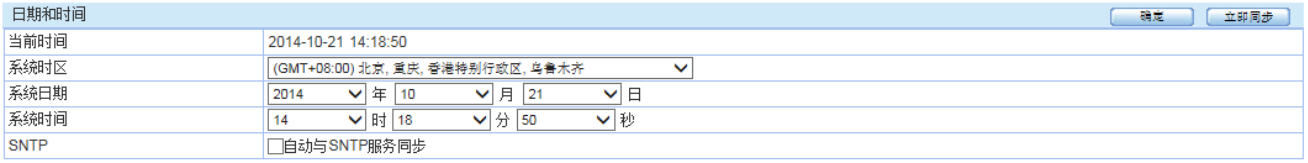
> **提示：**如果输入域名，需要先配置本地 DNS 服务器，详见【网络配置>DNS 配置】。

5.7 日期/时间

功能描述：用于设定设备的系统时间。

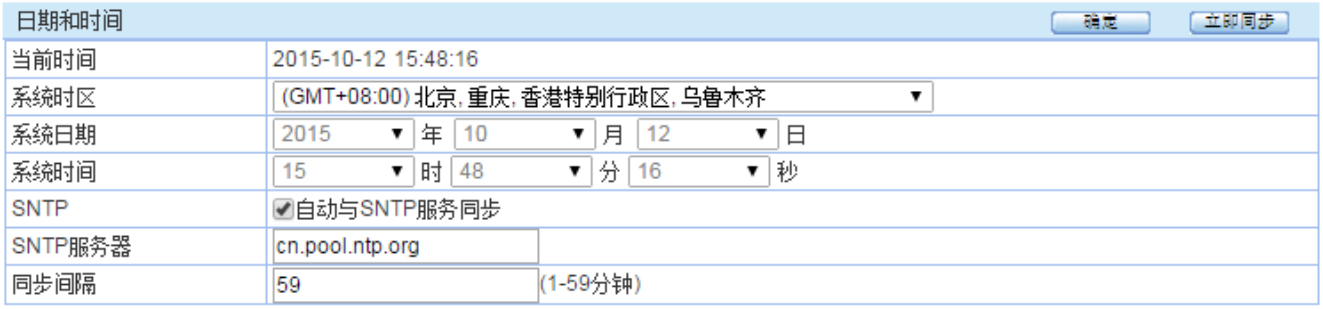
配置路径：【系统配置】>【日期时间】，设置界面如下图：

图 5-19 设置系统时间



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]。默认的 SNTP 服务器为 cn.pool.ntp.org，默认的同步间隔为 59 分钟。如下图：

图 5-20 SNTP 服务器同步



提示：SNTP服务器填写服务器地址，如IP：192.168.1.1 域名cn.pool.ntp.org，tick.stdtime.gov.tw

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。

5.8 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：

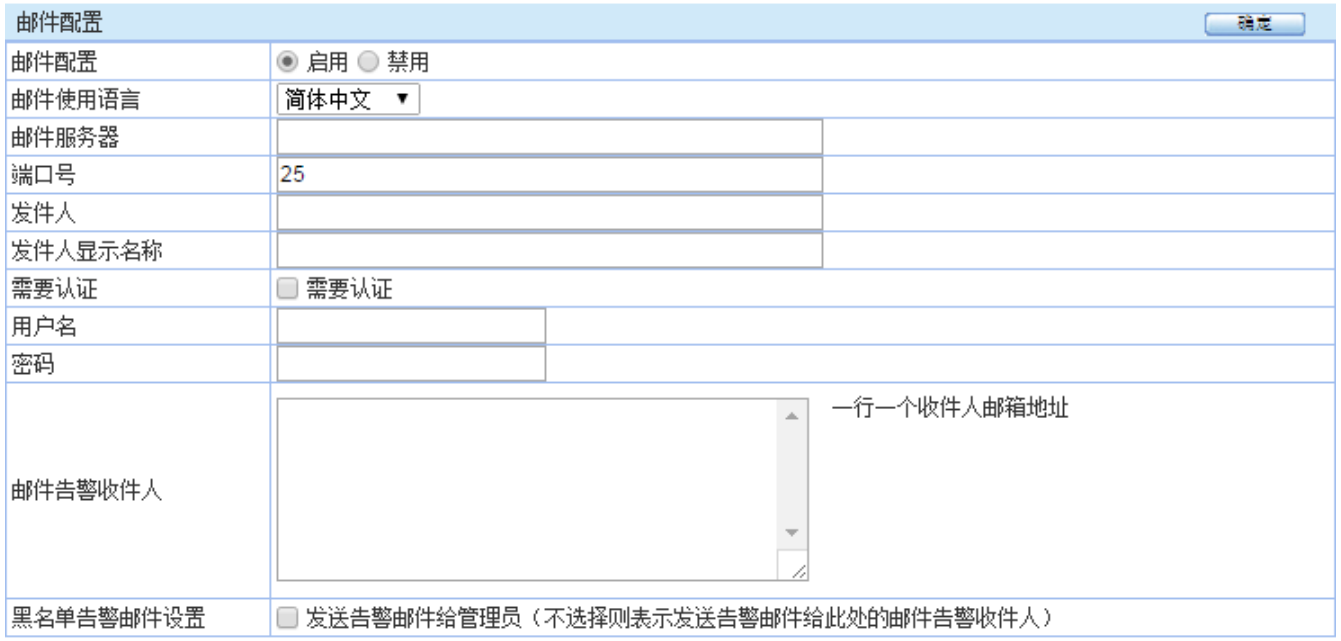
图 5-21 系统信息

5.9 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 5-22 邮件配置



说明：申请临时账户需要启用此功能。

参数说明：

邮件使用语言：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。

加密方法：对邮件进行加密操作，加密方式有不加密，SSL 加密，TLS 加密三种。

端口号：设置邮件端口号。当加密方式为无时，端口号默认为 25；当加密方式为 SSL 时，端口号为 465,当加密方式为 TLS 时，端口号为 25 或是 587。

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。

邮件告警收件人：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。

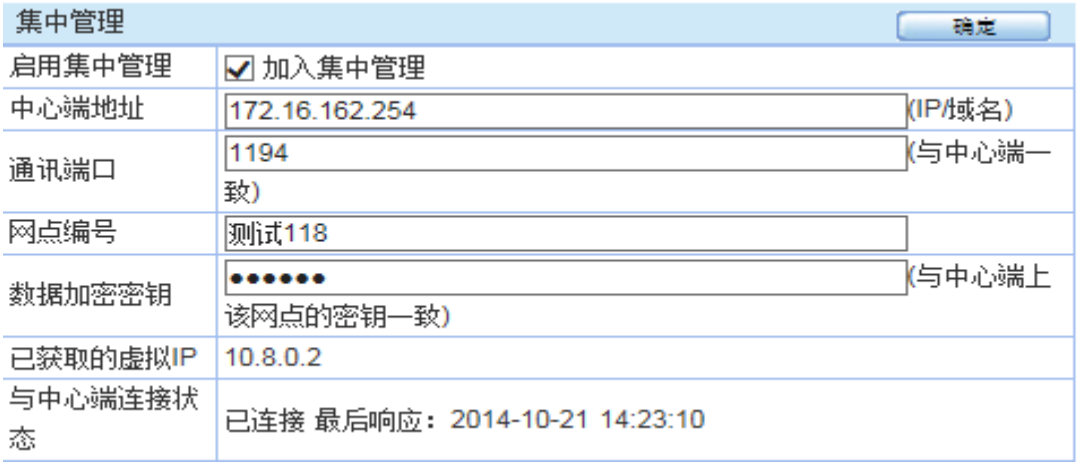
黑名单告警邮件设置：发送告警邮件给管理员（不选择则表示发送告警邮件给此处的邮件告警收件人）

5.10集中管理

功能描述：配置设备是否加入集中管理平台。

配置路径：【系统配置】>【集中管理】，配置页面如下：

图 5-23 集中管理



参数说明：

启用集中管理：配置设备是否加入集中管理，加入后即成为集中管理的客户端或网点。

中心端 IP 地址：配置集中管理的中心端的 IP 地址。

通讯端口：配置与中心端通信的端口号，默认是 1194。须与中心端配置的通讯端口一致。

网点名称：配置设备在中心端的区域结构中显示的设备名称。

数据加密密钥：与中心端通信时的数据是加密的，此处配置的密钥与中心端上该网点密钥一致。

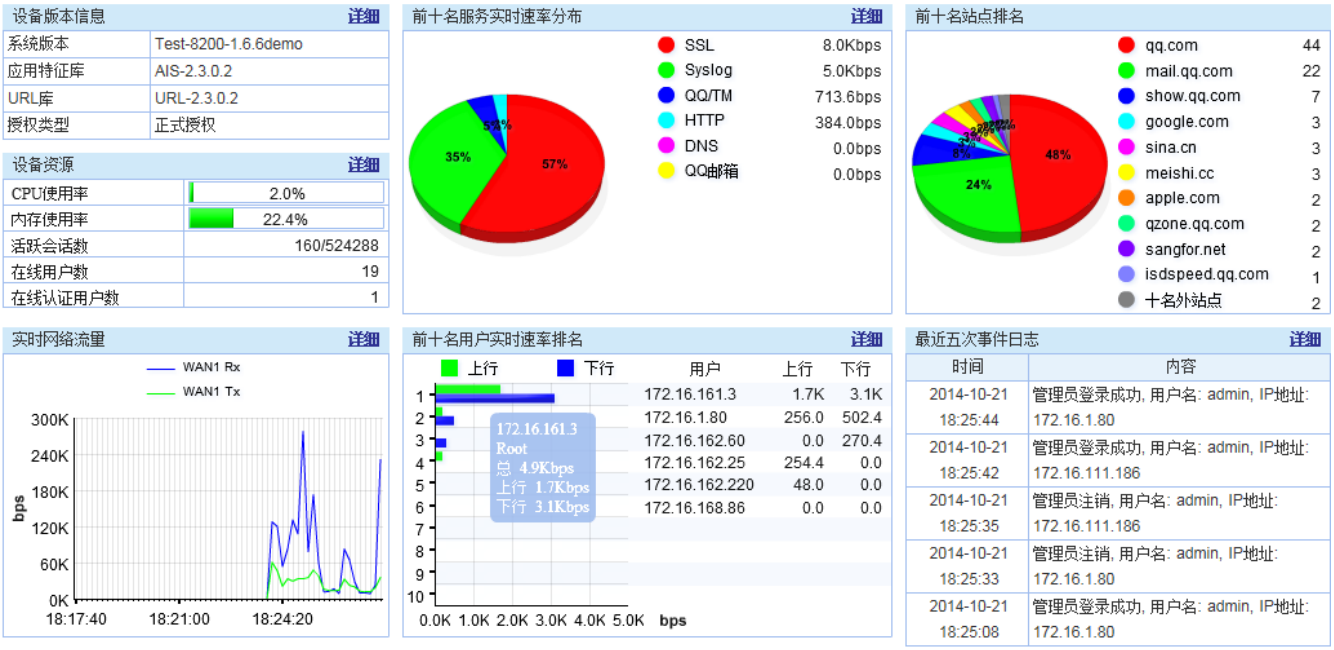
已获取的虚拟 IP：中心端分配给设备的虚拟 IP 地址。

与中心端连接状态：显示与中心端的连接状态。“连接”表示与中心端的数据通道连接正常，“断开”表示与中心端的数据通道连接已断开。“最后响应时间”表示最后一次与中心端通信的时间。

6 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、前十名用户实时速率排名、前十名站点排名、最近五次事件日志等七项内容。如下图：

图 6-1 设备状态



“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图。

“前十名用户实时流量排名”动态显示了以总速率排名的前十名用户。当鼠标滑过某用户时，会出现“显示活跃服务”的提示，点击即可查看该用户正在使用的服务的信息。当鼠标滑过某用户后面的带宽值时，会出现“显示最近一小时的趋势图”的提示，点击即可查看到该用户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“用户流量分析”页面，查看到前五十名用户的速率排名统计信息。

“前十名站点排名”动态显示了以被访问次数排名的前十名网站。

“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。

7 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、用户监控四大部分。

7.1 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 7-1 设备资源

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；

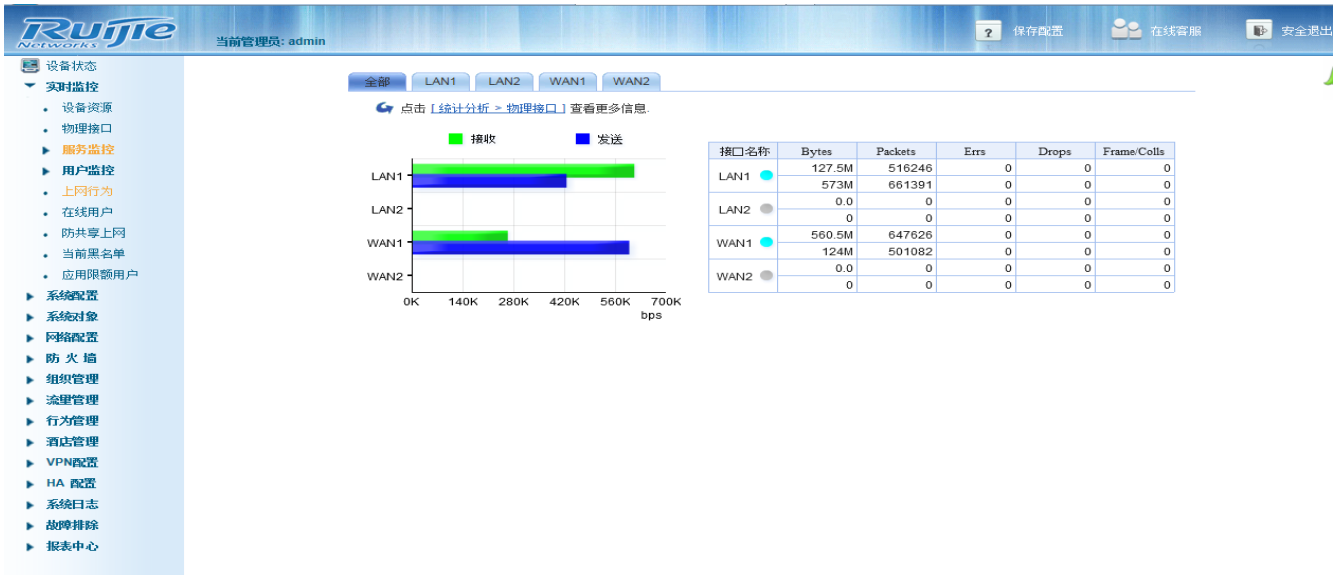
每个图的下方都显示了最新值(最近一个采样点的值)、最近一小时的最大值、最小值、平均值及每个值对应的时间点。图中还用箭头指明了最大值，如果这些值分布在多个时间点，则显示最后一个时间点。例如，最大值分布在 15:09:11 和 15:45:23 两个时间点，那么图中箭头指明的时间点和图下方最大值对应的括号中的时间点都是最后一个点 15:45:23。

7.2 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：

图 7-2 物理接口统计图



全局信息包括了以下内容：

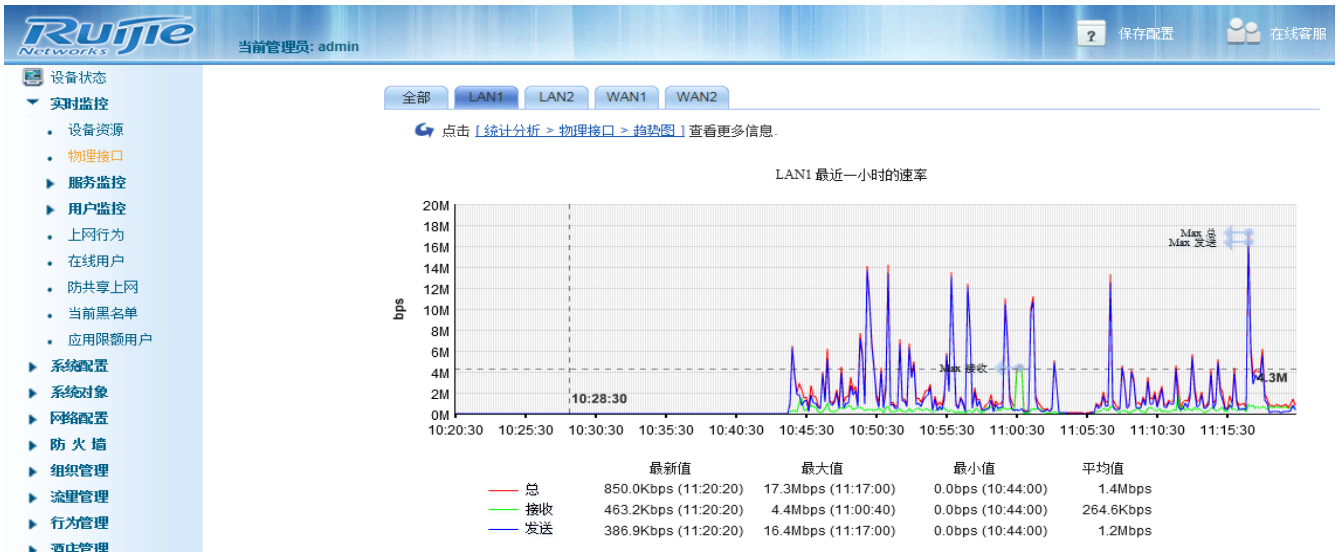
柱状图显示了每个物理接口收发速率。

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 7-3 LAN1 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。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 15:09:11 和 15:45:23 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最后一个点 15:45:23。

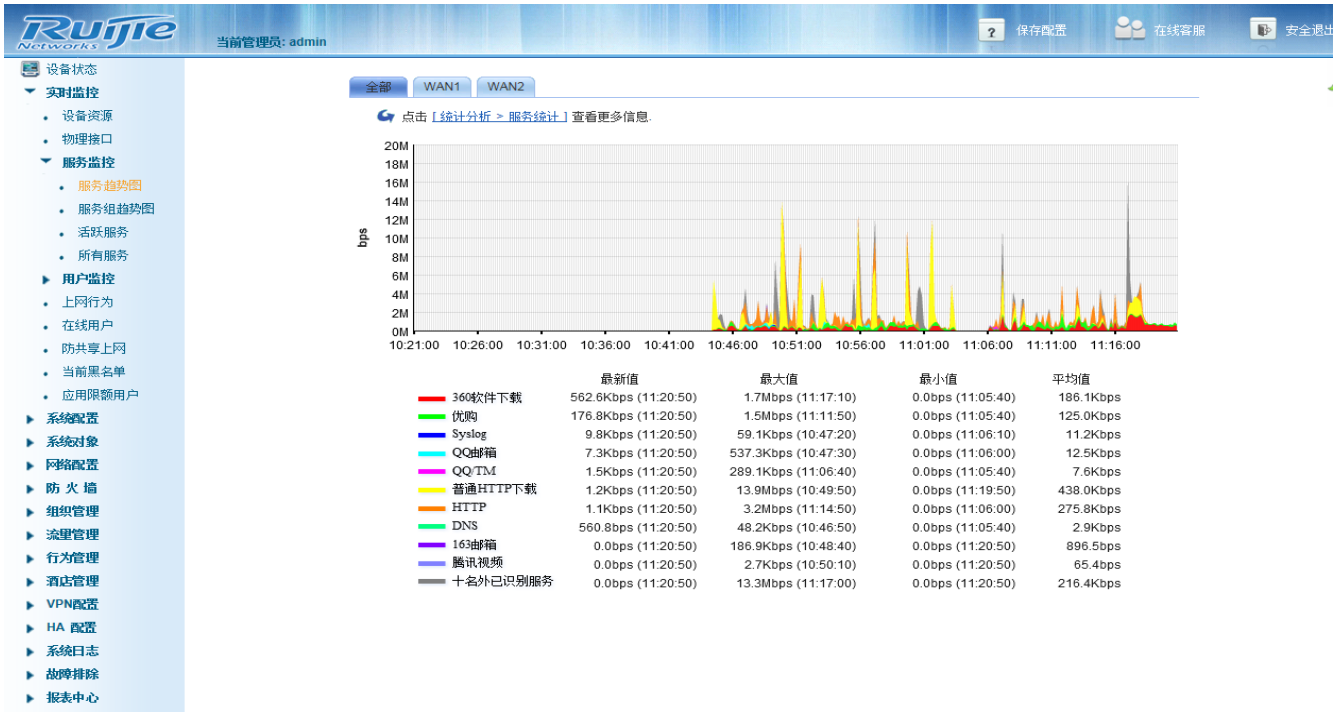
7.3 服务监控

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。

7.3.1 服务趋势叠加图

服务趋势叠加图如下：

图 7-4 服务监控统计图

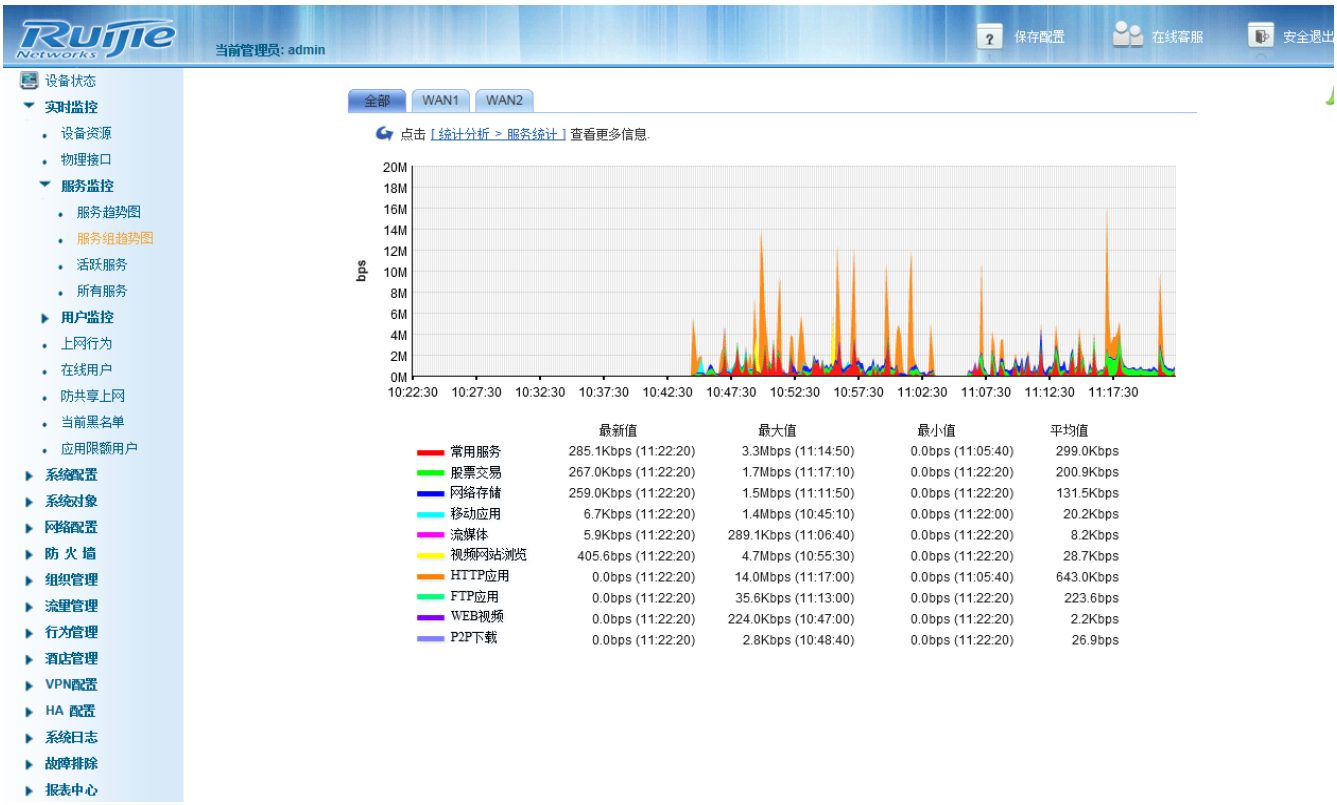


这里显示了所有服务的叠加趋势图，其中列出了前十名和 Other。Other 表示网络中除了前十名以外的其它服务的速率值。

7.3.2 服务组趋势图

服务组趋势图如下：

图 7-5 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。

7.3.3 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：

图 7-6 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。

7.3.4 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：

图 7-7 所有服务监控统计图

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	↑ 47.0K, ↓176.7K	↑ 76.3M, ↓ 562.5M	↑ 173.6K, ↓ 1.3M	趋势图
2	UDP_ALL	↑ 15.7K, ↓12.2K	↑ 72.7M, ↓ 36.1M	↑ 165.5K, ↓82.1K	趋势图
3	DNS	↑ 244.8, ↓332.0	↑ 584.3K, ↓ 880.6K	↑ 1.3K, ↓ 2.0K	趋势图
4	HTTP	↑ 5.4K, ↓ 2.6K	↑ 9.2M, ↓ 135.3M	↑ 20.9K, ↓307.9K	趋势图
5	PING	0.0	↑ 73.7K, ↓ 65.1K	↑ 167.7, ↓148.2	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	↑ 2.2K	↑ 883.7K, ↓ 143.4K	↑ 2.0K, ↓326.3	趋势图
9	SMTP	0.0	0	0.0	趋势图
10	POP3	0.0	0	0.0	趋势图
11	Lotus_Notes	0.0	0	0.0	趋势图
12	IMAP	0.0	0	0.0	趋势图
13	TFTP	0.0	0	0.0	趋势图
14	SSL	0.0	0	0.0	趋势图
15	SNMP	0.0	0	0.0	趋势图
16	SQL	0.0	0	0.0	趋势图
17	MySQL	0.0	0	0.0	趋势图
18	NTP	0.0	0	0.0	趋势图
19	NetBIOS	0.0	0	0.0	趋势图
20	DHCP	0.0	0	0.0	趋势图
21	Syslog	↑ 2.2K, ↓ 6.6K	↑ 804.1K, ↓ 5.2M	↑ 1.8K, ↓11.9K	趋势图
22	UPNP	0.0	0	0.0	趋势图
23	SOCKS	0.0	0	0.0	趋势图
24	PING_v6	0.0	0	0.0	趋势图
25	BGP	0.0	0	0.0	趋势图
26	AH	0.0	0	0.0	趋势图
27	ESP	0.0	0	0.0	趋势图
28	GRE	0.0	0	0.0	趋势图
29	HSRP	0.0	0	0.0	趋势图

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。

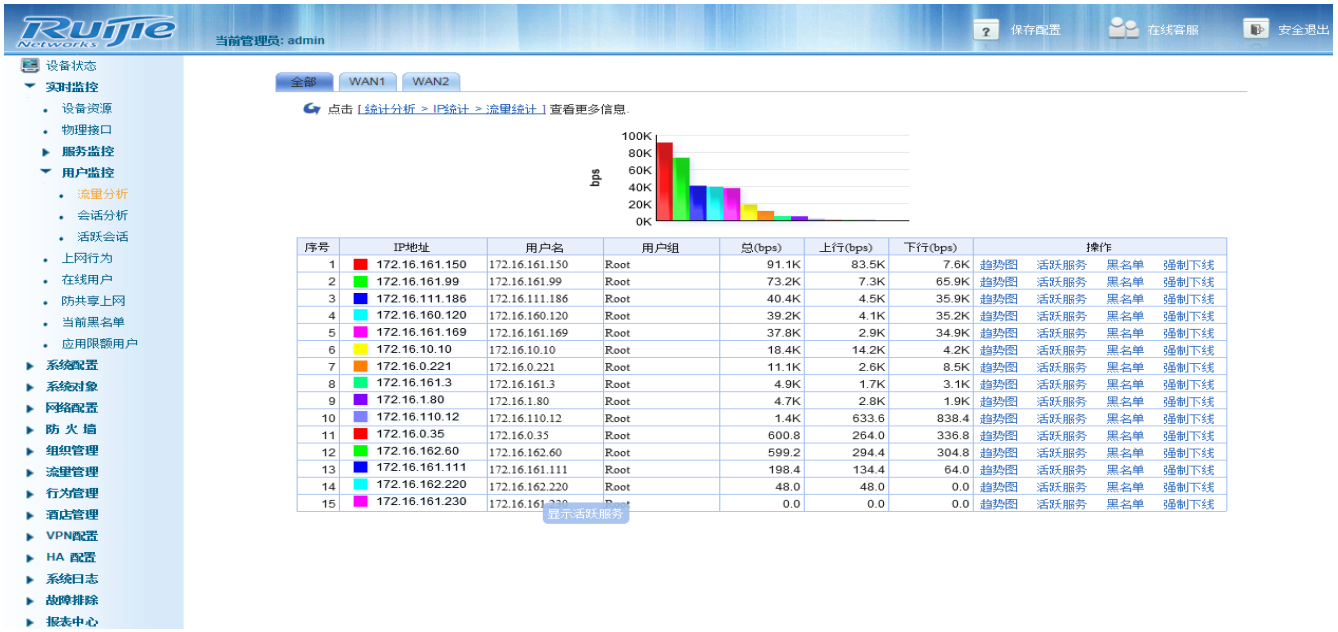
7.4 用户监控

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。

7.4.1 流量分析

前五十名用户的实时传输速率统计图如下：

图 7-8 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。

7.4.2 会话分析

前五十名用户的新建会话的统计图如下：

图 7-9 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。

7.4.3 活跃会话

前五十名用户的当前活跃会话统计图如下:

图 7-10 活跃会话

序号	IP地址	用户名	用户组	总	上行	下行	操作
1	172.16.161.150	172.16.161.150	Root	198	197	1	趋势图 活跃服务 黑名单 强制下线
2	172.16.162.60	172.16.162.60	Root	61	61	0	趋势图 活跃服务 黑名单 强制下线
3	172.16.111.186	172.16.111.186	Root	45	45	0	趋势图 活跃服务 黑名单 强制下线
4	172.16.1.80	172.16.1.80	Root	32	32	0	趋势图 活跃服务 黑名单 强制下线
5	172.16.161.169	172.16.161.169	Root	26	26	0	趋势图 活跃服务 黑名单 强制下线
6	172.16.161.3	172.16.161.3	Root	11	10	1	趋势图 活跃服务 黑名单 强制下线
7	172.16.160.120	172.16.160.120	Root	7	7	0	趋势图 活跃服务 黑名单 强制下线
8	172.16.0.221	172.16.0.221	Root	4	3	1	趋势图 活跃服务 黑名单 强制下线
9	172.16.161.230	172.16.161.230	Root	1	1	0	趋势图 活跃服务 黑名单 强制下线
10	172.16.162.220	172.16.162.220	Root	1	1	0	趋势图 活跃服务 黑名单 强制下线

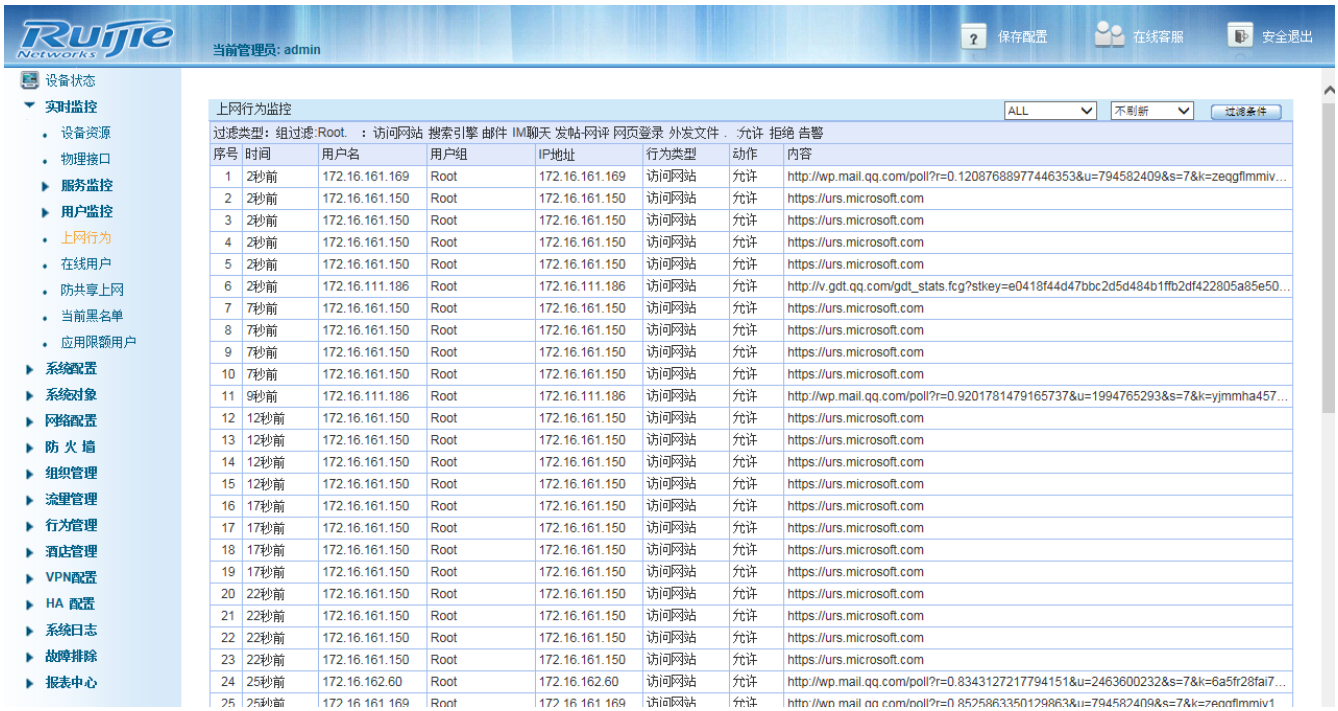
点击<趋势图>按钮，查看该用户最近一小时的速率趋势图。

点击<活跃服务>按钮，查看该用户当前使用的服务的信息。

7.5 上网行为

本页面显示了用户上网行为的实时状况，内容包括访问的网站、搜索引擎（关键字搜索）、发帖内容（含网页评论）、网页文件上传、WEB 网页账户登录、邮件收发、即时通讯、FTP 传输、Telnet 传输。本页面是自动刷新，刷新间隔可设置为：5 秒、10 秒、20 秒、30 秒和 60 秒。网页如下：

图 7-11 上网行为分析



7.6 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 7-12 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。

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。

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 系统对象

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

8.1 地址簿

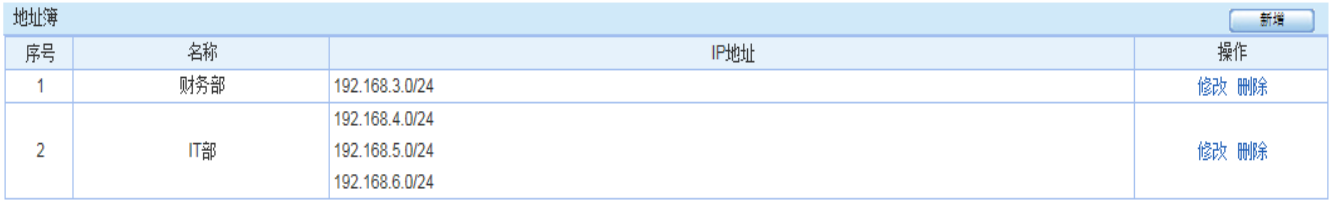
功能描述：用于定义一个包含某些 IP 地址的 IP 地址组，这个 IP 组可以是任意的一个 IP、一段 IP 或者 IP 范围的任意组合。“地址簿”将被【防火墙>安全策略】、【防火墙>NAT 规则】、【行为管理】及【流量管理】中定义的规则时引用。

配置路径：【系统对象】>【地址簿】

配置描述：

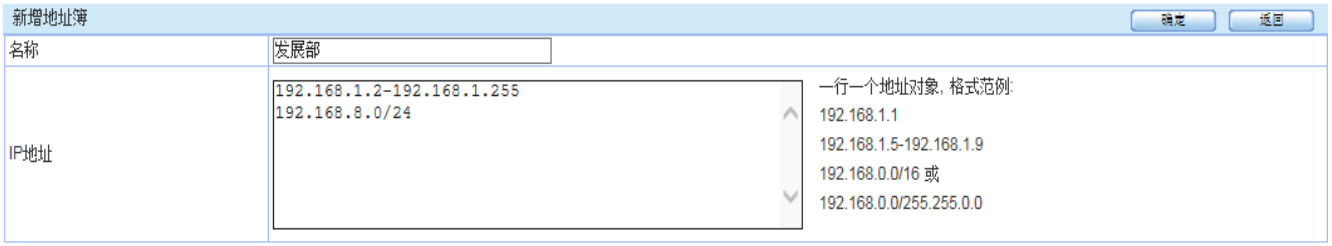
第一：进入【地址簿】页面，如下图：

图 8-1 地址簿



第二：点击<新增>按钮，增加地址簿，如下图：

图 8-2 新增地址簿



。

8.2 网络服务

网络服务共分为：内置服务、自定义普通服务、自定义特征识别、自定义论坛/网评、协议剥离，其中内置服务又包括常用服务、HTTP 应用、WEB 视频、P2P 下载、流媒体、网络游戏、即时通讯、股票交易、网上银行、网络电话、其他服务等。[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；内置服务是基于内容识别的服务，在【流量管理】中将被引用。

8.2.1 自定义普通服务

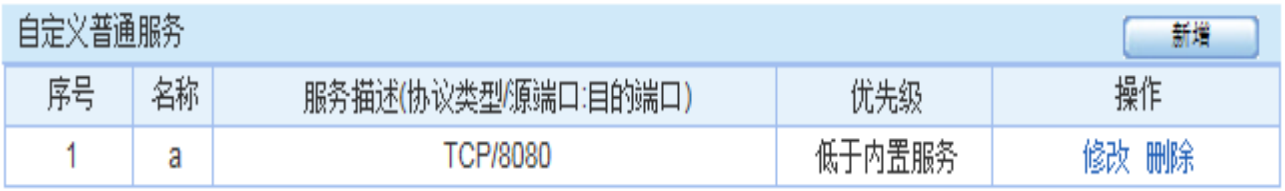
功能描述：自定义基于端口的四层服务

配置路径：【系统对象】>【网络服务】>【自定义普通服务】

配置描述：

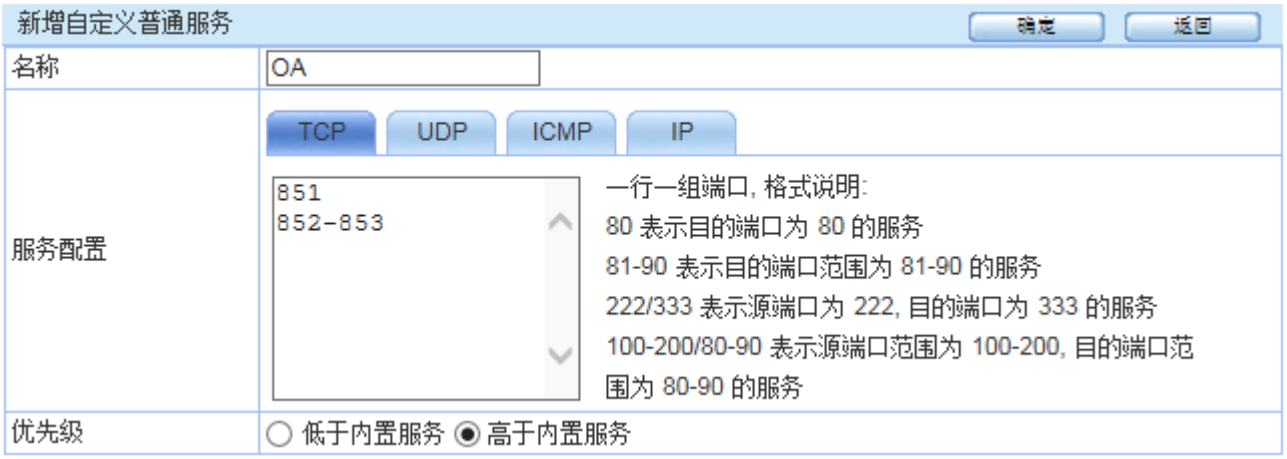
第一：进入【自定义普通服务】页面，可看到当前已定义的服务，如下图：

图 8-3 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：

图 8-4 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。

8.2.2 自定义特征识别

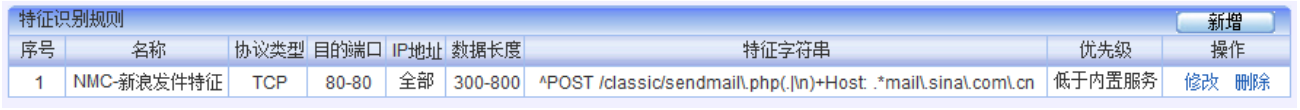
功能描述：自定义基于特征识别的 7 层服务

配置路径：【系统对象】>【网络服务】>【自定义特征识别】

配置描述：

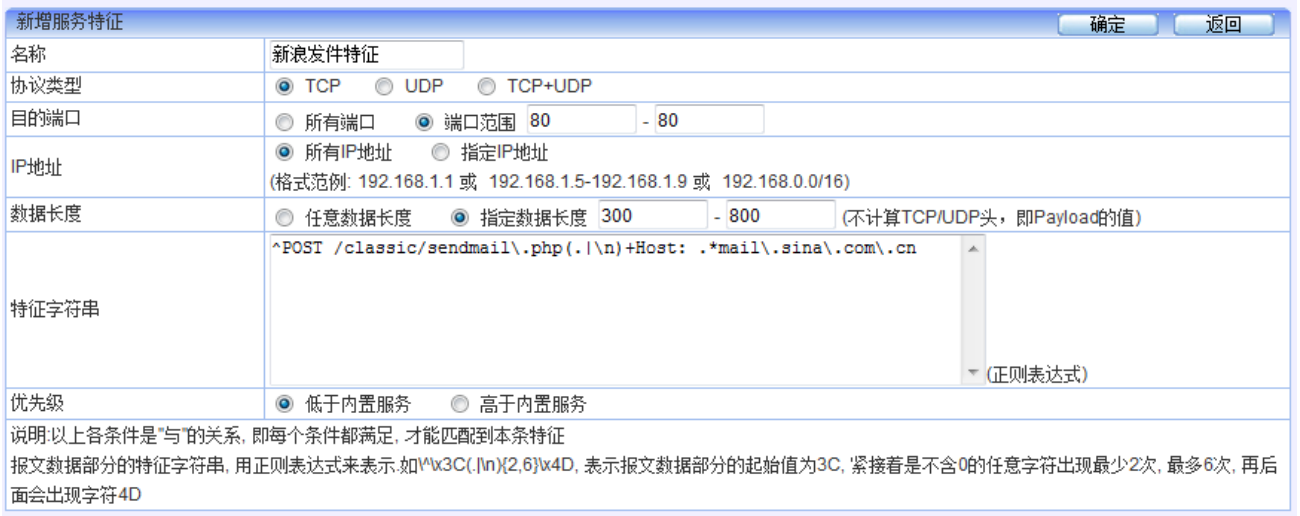
第一：进入【自定义特征识别】页面，可看到当前已定义的服务，如下图：

图 8-5 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：

图 8-6 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。

8.2.3 自定义论坛/网评特征

功能描述：自定义 HTTP 论坛或者网页评论页面的特征。

配置路径：【系统对象】>【网络服务】>【自定义论坛/网评特征】

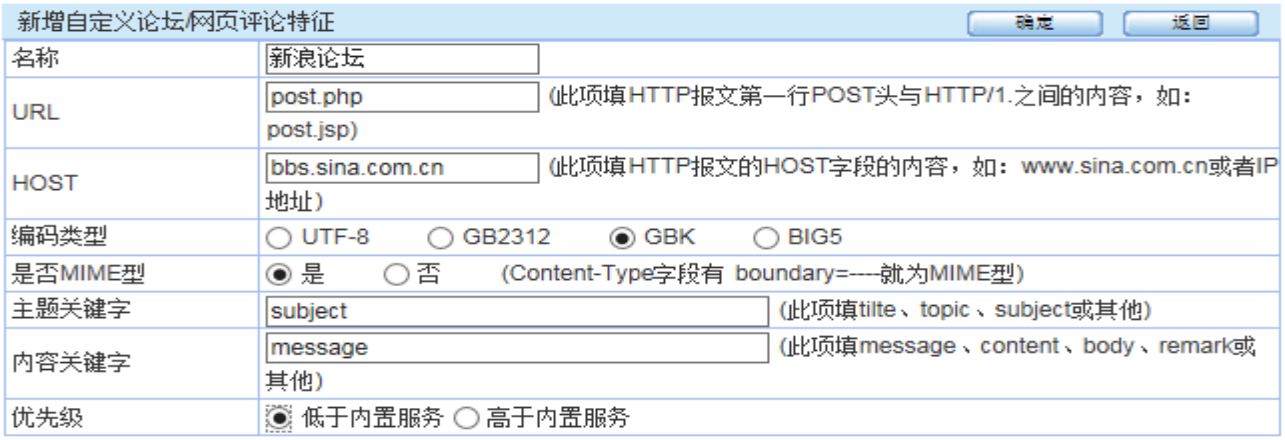
配置描述：

第一：进入【自定义论坛/网评特征】页面，可看到当前已经定义好的[自定义论坛/网评特征]列表，如下图：

图 8-7 自定义论坛/网评特征

第二：点击表格右上角的<新增>按钮，新增[论坛/网评特征]，配置页面如下：

图 8-8 新增自定义论坛/网评特征



参数说明：

URL：HTTP 报文第一行 POST 头与 HTTP/1.之间的内容，如：post.jsp。

HOST：HTTP 报文的 HOST 字段的内容，如：www.sina.com.cn 或者 IP 地址。

编码类型：网页的编码类型。

是否 MIME 型：选择[是]或[否]，当 Content-Type 字段含有“boundary=----”时，即为 MIME 型。

主题关键字：tilte、topic、subject 或其他。即下面“发表帖子”和“回复帖子”两个图例中①所指的部分所包含的关键字。

内容关键字：message、content、body、remark 或其他。即下面“发表帖子”和“回复帖子”两个图例中②所指的部分包含的关键字。

图 8-9 发表帖子

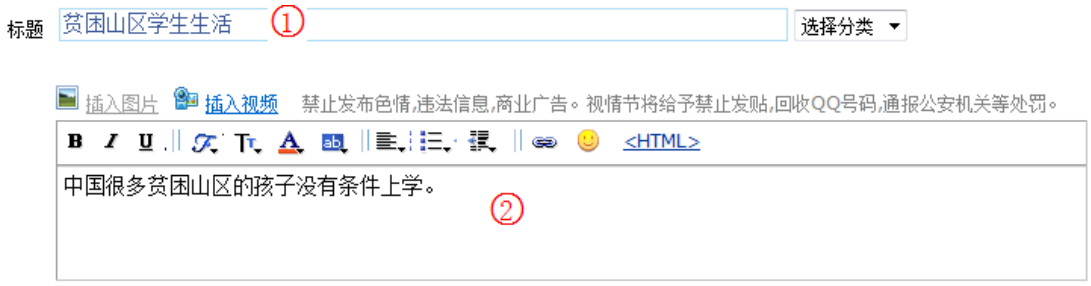
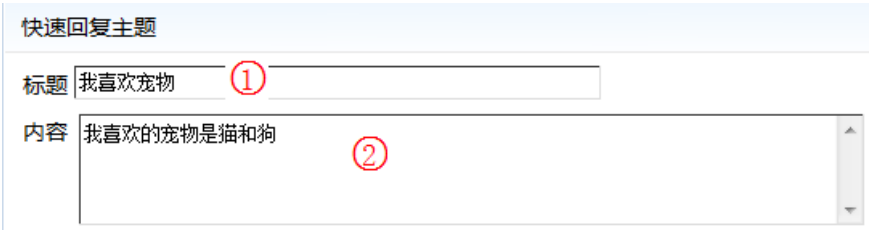


图 8-10 回复帖子



优先级：默认低于系统定义的特征。

提示：

1. 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。
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。

8.2.4 协议剥离

在某些网络环境中，通讯数据包经过了一些特殊协议类型的封装（PPPoE、MPLS 等），这些协议数据包在普通 IP 包的基础上添加了各自协议特有的头部标识，使得一般带有协议分析功能的设备也无法正常分析。

本设备通过协议剥离功能，分析出这些特殊协议数据包的特点，并与内置特殊协议规则匹配，在设备内部剥离掉特殊协议的协议头，这样可以支持对特殊协议封装内的原始数据进行认证、审计和控制。

设备内部目前内置了[VLAN（Q-in-Q）协议的剥离] 和 [PPPoE 协议的剥离]，并且支持[自定义协议的剥离]。

如果网络环境中存在非普通 IP 报文的其他特殊协议，但该协议不在内置的协议剥离列表，在可以设置自定义的协议剥离。配置方法如下：

配置路径：【系统对象】>【网络服务】>【协议剥离】

配置描述：进入【协议剥离】页面，如下图：

图 8-11 自定义协议剥离

参数说明：

协议剥离：启用或禁用协议剥离功能。

匹配协议头特征：指明需要做协议剥离的特殊协议的协议头在整个数据包中（含以太头）的起始位址和协议头特征值。

IP 头起始位址：指明经过此特殊协议封装后 IP 头的起始位址。

提示：

1、 路由模式不支持协议剥离。

2、 网桥模式下支持协议剥离，可对协议剥离后的数据进行自动认证、应用审计和控制，但特殊环境下部分功能不生效，如 Web 认证、准入认证、SSL 内容识别，MSN 传文件控制等等。

3、 旁路模式下支持协议剥离，协议剥离环境下仅支持自动认证和审计，不支持控制功能。

4、 协议剥离环境下，不支持以计算机名作为用户名、不支持以 MAC 地址作为用户名、不支持用户绑定 MAC 地址。

5、 某些数据经特殊协议封装后，会有 2 个 IP 头部，如 L2TP，协议剥离后最外层的 IP 头（底层）已经剥离，所以最终认证、审计、控制是根据最里层（上层）的 IP 来控制的，同时设备策略不应该组织外层 IP 通讯。

6、 设备默认支持单层的 802.1Q VLAN 剥离、Q-in-Q VLAN 剥离、PPPoE 剥离、VLAN+PPPoE 剥离 ,Q-in-Q+PPPoE 支持，以及对 PPPoE SSO 支持。对这些协议的支持，不必开启协议剥离功能，就能自动运行。

7、 协议剥离均不支持协议以压缩、加密的方式通讯。

8.3 时间计划

功能描述：用于定义时间段，然后可在【防火墙>安全策略】、【流量管理】、【行为管理】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】

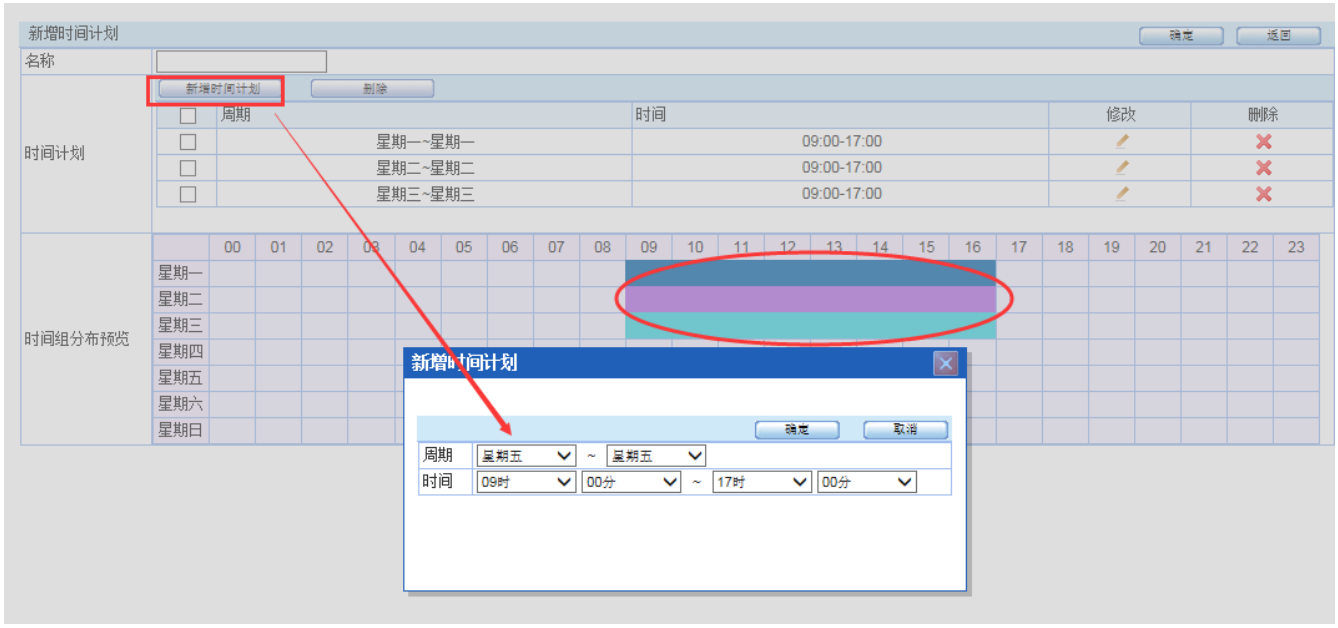
配置描述：

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 8-12 时间计划

第二：点击<新增>按钮，增加时间计划，如下图：

图 8-13 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，只有格子为绿色时，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。

8.4 URL 库

功能描述：

包括内置和自定义的 URL 库。URL 库可用于【行为管理>上网策略>URL 过滤】，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：

图 8-14 内置 URL 库

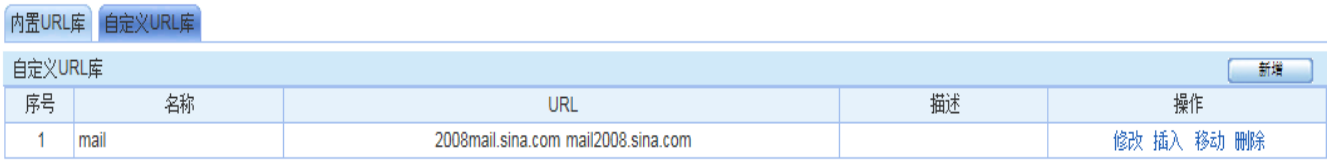
内置URL库 自定义URL库

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
20	电子银行	电子银行网站

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

图 8-15 自定义 URL 库


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	mail	2008mail.sina.com mail2008.sina.com		修改 插入 移动 删除

操作说明：

- 【上网策略>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【上网策略>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 8-16 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。

8.5 关键字组

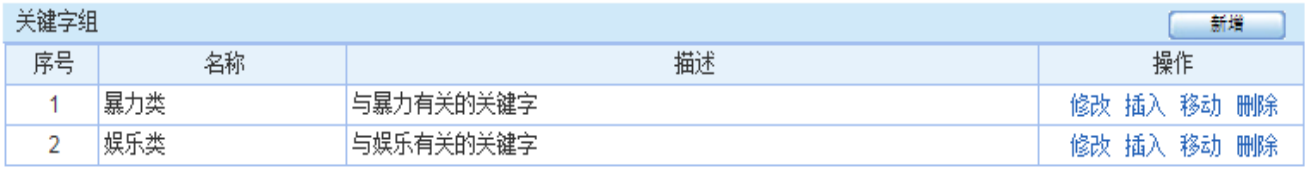
功能描述：用于设置关键字，并把关键字分组，这些关键字组可用于【上网策略>关键字过滤】中限制某些关键字的搜索和上传。

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 8-17 关键字组



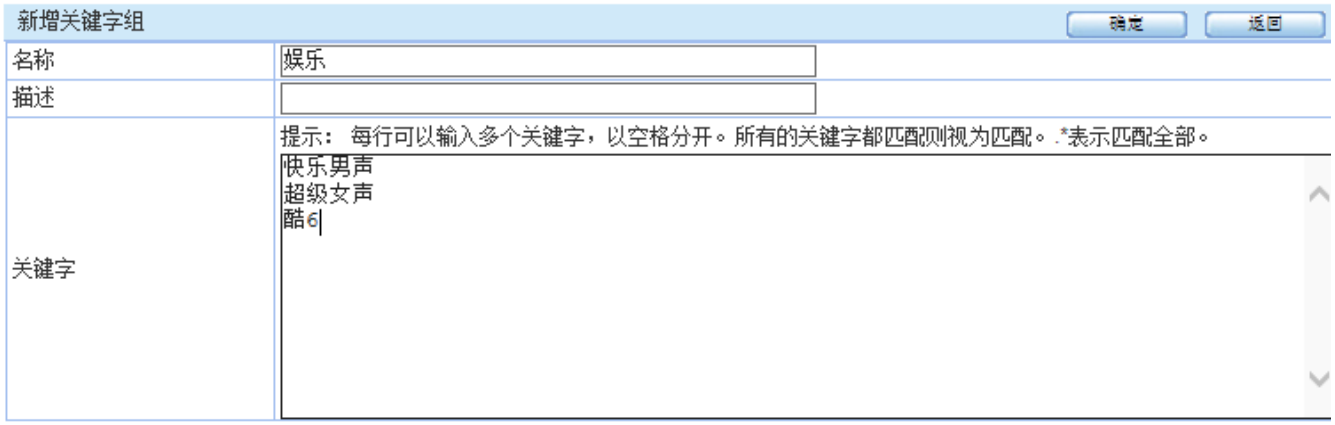
操作说明：

【上网策略>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【上网策略>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 8-19 新增关键字组



8.6 文件类型

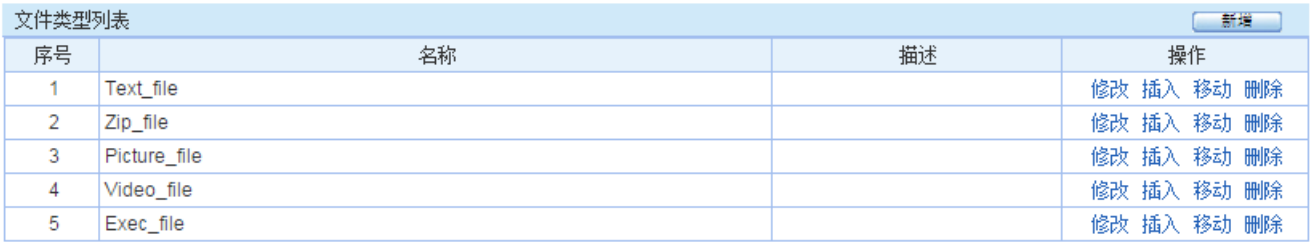
功能描述：用于定义文件类型，并把文件类型分组。这些文件类型可用于【上网策略>文件传输过滤】中限制这些类型的文件的上传和下载。

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，可以看到当前默认定义的文件类型分组。如下图：

图 8-17 文件类型



序号	名称	描述	操作
1	Text_file		修改 插入 移动 删除
2	Zip_file		修改 插入 移动 删除
3	Picture_file		修改 插入 移动 删除
4	Video_file		修改 插入 移动 删除
5	Exec_file		修改 插入 移动 删除

操作说明：

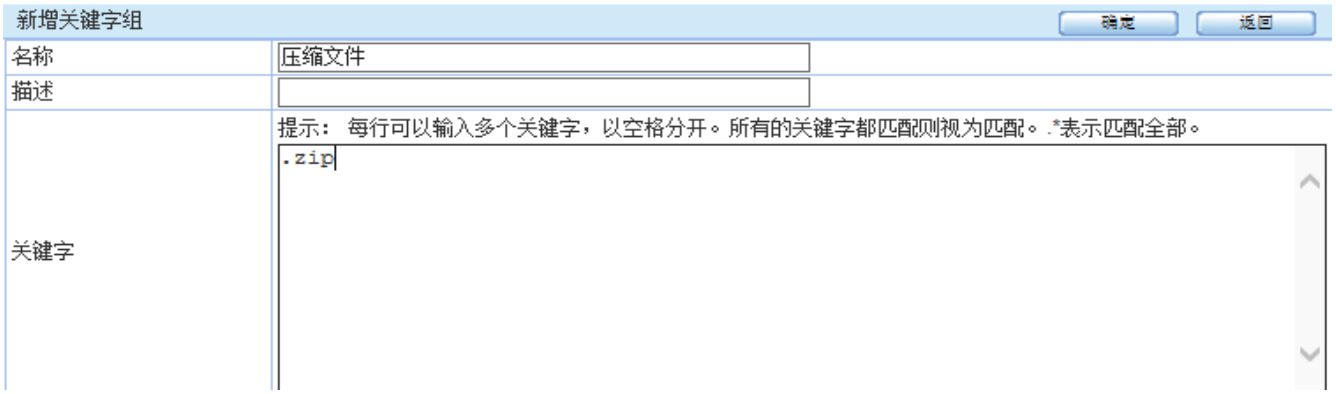
设备默认定义了 5 种常见的文件类型列表，如 Text_file，Zip_file 等。可以通过<修改>按纽对默认的文件类型进行修改。也可以直接使用<删除>按纽将默认文件类型进行删除。

【上网策略>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【上网策略>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 8-21 新增文件类型



8.7 证书管理

证书管理包括本地证书，可直接将本地证书导入系统。

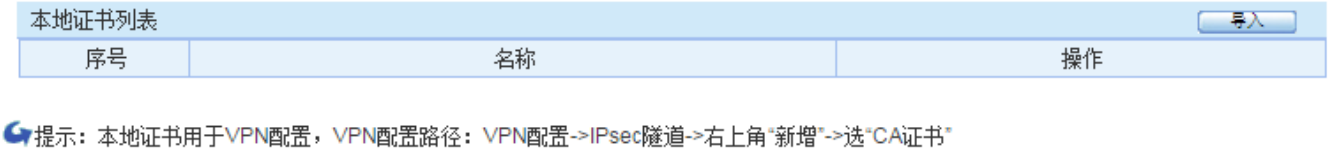
8.7.1 本地证书

功能描述：用于作 IPSEC VPN 的共享密钥

配置路径：【系统对象】>【证书管理】>【本地证书】

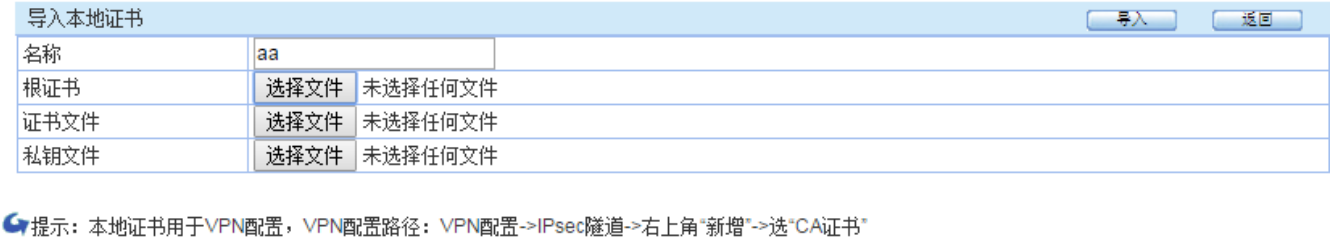
配置描述：

第一：进入【文件类型】页面，可以看到当前的本地证书。如下图：



第二：点击<导入>按钮，导入本地证书。如下图：

图 8-21 导入本地证书



参数说明：

名称：导入的本地证书的名称

根证书：选择需要导入的根证书

证书文件：选择需要导入的证书文件

私钥证书：选择需要导入的私钥文件。

9 网络配置

“网络配置”包括：物理接口、配置 IP 地址、路由配置、DNS 配置、ARP 表、GRE 隧道、PPPOE 和 DHCP 配置。

9.1 接口配置

包括物理接口、VLAN 接口、PPPoE、GRE 隧道 四部分。

9.1.1 物理接口

功能描述：物理接口指在设备的面板上看到的数据接口，不同产品型号接口数目不一样。

配置路径：【网络配置】>【接口配置】>【物理接口】，配置页面如下图所示：

配置描述：

第一：进入【物理接口】页面，如下图：

图 9-1 物理接口

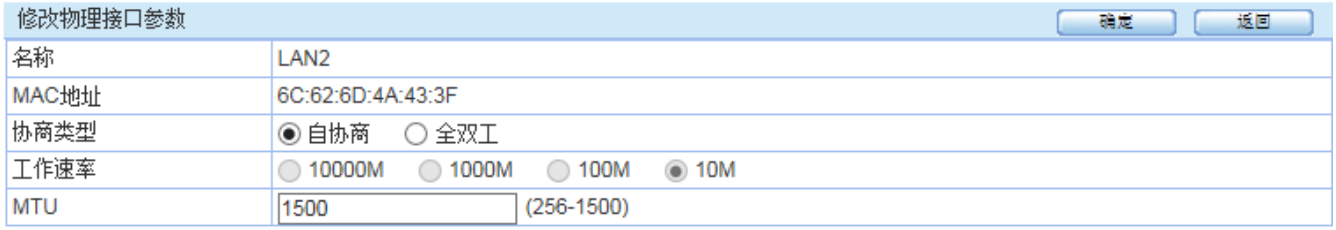
物理接口

名称	MAC地址	工作速率	协商类型	MTU	状态	操作
LAN1	6C:62:6D:4A:43:3D	100M	自协商	1500	连接	修改
LAN2	6C:62:6D:4A:43:3F	0M	自协商	1500	未连接	修改
WAN1	6C:62:6D:4A:43:3E	1000M	自协商	1500	连接	修改
WAN2	6C:62:6D:4A:43:40	0M	自协商	1500	未连接	修改

4、用。

第二：点击操作栏的<修改>按钮，对物理接口的参数进行配置，如下图所示：

图 9-2 修改物理接口参数



提示：当协商类型为自协商时，工作速率不可配置。

9.1.2 链路聚合

链路聚合是将多个以太网物理端口捆绑成一条逻辑端口(即将多个端口捆绑成一个逻辑的端口以增加带宽 ,同时增加链路备份)。链路聚合通道最多可以捆绑 10 个物理端口。

链路聚合遵循的规则：

参与捆绑的物理端口必须属于同一个 VLAN。

参与捆绑的物理端口必须属于 LAN 口或同属于 WAN 口。

参与捆绑的物理端口的物理参数设置必须相同，应该有相同的速度和全/半双工模式设置。

配置路径：【网络配置】>【接口配置】>【链路聚合】

第一：进入【链路聚合】界面，可以看到当前已经建立的链路聚合接口。如下图：

图 9-3 链路聚合

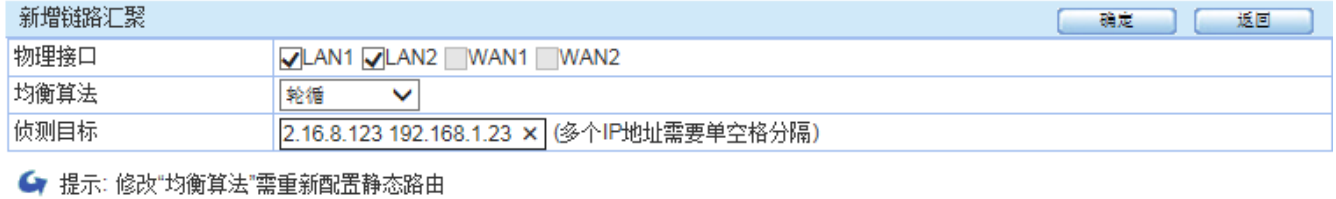
链路聚合接口名称的命名规则是：

LAN 口的聚合：名称为 LCG，编号为第一个 LAN 口的编号。例如：LAN2 和 LAN4 聚合，则接口名称为 LCG2。

WAN 口的聚合：名称为 WCG，编号为第一个 LAN 口的编号。例如：WAN1 和 WAN3 聚合，则接口名称为 WCG1。

第二：点击<新增>按钮，增加 VLAN 接口。如下图：

图 9-4 新增链路聚合



参数说明：

物理接口：选择需要绑定的物理接口，要么都选择 LAN 口，要么都选择 WAN 口。

均衡算法：流量在多个物理接口之间的负载均衡算法，共 7 种，如下：

轮询：所有链路处于负载均衡状态，轮询方式往每条链路发送报文，基于 per packet 方式发送。这模式的特点增加了带宽，同时支持容错能力，当有链路出问题，会把流量切换到正常的链路上。默认此算法。

主备：一个端口处于主状态，一个处于从状态，所有流量都在主链路上处理，从不会有任何流量。当主端口 Down 掉时，从端口接手主状态。

哈希：该模式将限定流量，以保证到达特定对端的流量总是从同一个接口上发出。如果所有流量是通过单个路由器（比如只有一个网关时，源和目标 MAC 都固定了，此时算出的线路就一直是同一条，那么这种模式就没有多少意义了），那该模式就不是最好的选择。这模式是通过源和目标 MAC 做 hash 因子来做 XOR 算法来选路的。

广播：这种模式的特点是一个报文会复制多份，往所有绑定的物理接口分别发送出去,当有对端交换机失效时，感觉不到任何 Downtime，但此法过于浪费资源；不过这种模式有很好的容错机制。此模式适用于金融行业，因为他们需要高可靠性的网络，不允许出现任何问题。

802.3d：此模式是 IEEE 标准，因此所有实现了 802.3ad 的对端都可以很好的互操作。802.3ad 标准要求帧按顺序（一定程度上）传递，因此通常单个连接不会看到包的乱序。802.3ad 实现通过对端来分发流量（通过 MAC 地址的 XOR 值）。

发送自适应：通过对端均衡外出（Outgoing）流量。

双向自适应：该模式包含了发送自适应模式，同时加上针对 IPV4 流量的接收负载均衡。

侦测目标：填写与被绑定后的汇聚接口的同一网段的 IP 地址，多个 IP 地址需要以单空格分隔。

> **提示：**在被绑定为汇聚接口之前，物理接口已经配置了 IP 地址的，IP 地址将会被 Disable，但会保留配置，在被结束绑定后，IP 地址变为可用。

9.1.3 VLAN 接口

功能描述：通过配置 802.1Q 的 VLAN 接口地址，来实现 VLAN 间的数据转发，设备产品支持连接二层交换机的 TRUNK 口。

配置路径：【网络配置】>【接口配置】>【VLAN 接口】

第一：进入【VLAN 接口】界面，可以看到当前已经建立的 VLAN 接口。如下图：

图 9-5 VLAN 接口

VLAN接口 新增

序号	接口名称	物理接口	VLAN ID	操作
1	LAN2.2	LAN2	2	删除
2	LAN2.8	LAN2	8	删除

接口名称是物理接口和 VLAN ID 的组合。例如，LAN2.2 表示物理接口为 LAN2，VLAN ID 为 2 的 VLAN 接口。然后在【网络配置>配置 IP 地址】处，可以查看 VLAN 接口配置 IP 地址。

第二：点击<新增>按钮，增加 VLAN 接口。如下图：

图 9-6 新增 VLAN 接口，并设置 vlan 接口 IP 地址

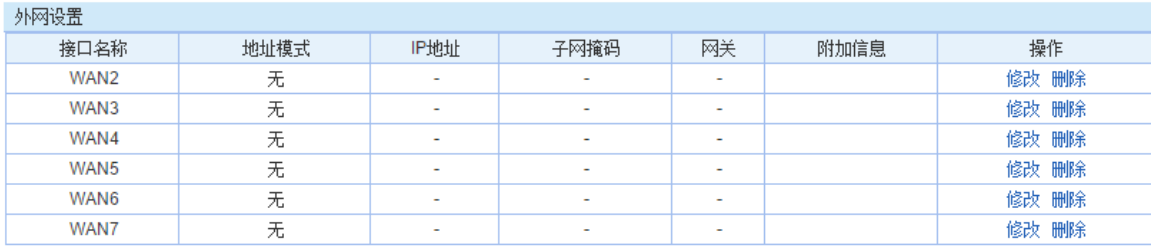
9.1.4 外网设置

功能描述：配置外网口为静态 IP、PPPoE、DHCP 模式，并完成相关设置。

配置路径：【网络配置】>【接口配置】>【外网设置】

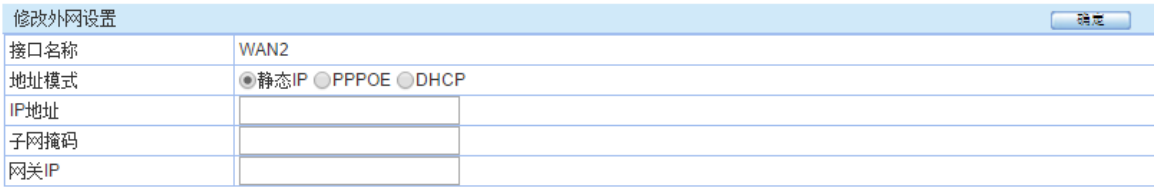
第一：进入【外网设置】界面，可以看到当前已经建立的配置。如下图：

图 9-7 外网设置

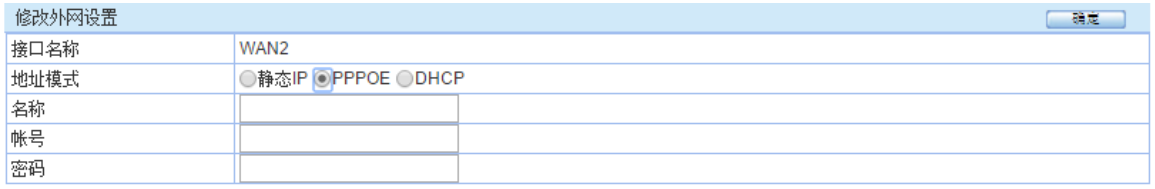


静态 IP 地址模式：点击<修改>按钮，地址模式选中静态 IP，设定 IP 地址、子网掩码、网关 IP。如下图：

图 9-8 修改接口配置为静态 IP



PPPOE 地址模式：点击<修改>按钮，地址模式选中 PPPOE，设定 pppoe 账号名称，对应的 pppoe 账号及密码。如下图：



参数说明：

名称：为 PPPoE 拨号配置取的名字

外网口：拨号链路连接的外网物理端口，即 WAN 口。一个 WAN 口只能连接一个拨号。

帐号：PPPoE 的帐号

IP 地址：拨号成功后，获得的 IP 地址；未成功时，IP 地址为空。

子网掩码：拨号成功后，获得的 IP 地址对应的掩码；未成功时，掩码为空。

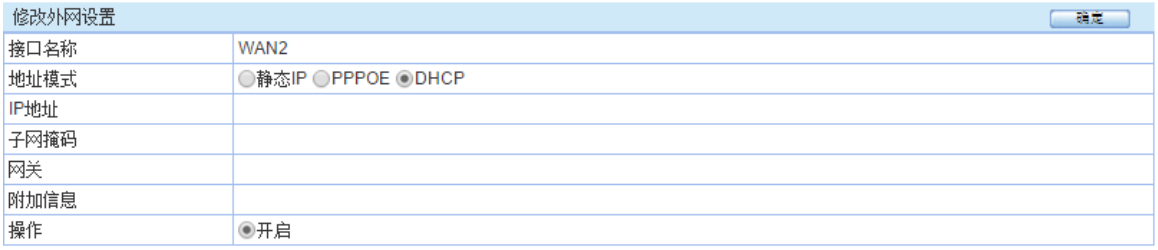
网关：拨号成功后，获得的网关地址；未成功时，网关地址为空。

连接状态：拨号成功后，状态为“正常”；未成功时，状态为“断线”。

DHCP 地址模式：点击<修改>按钮，地址模式选中 DHCP。如下图：

此接口启用 DHCP 客户端后，就会自动去获取 IP 设置。点击<更新>按钮，更新接口的 IP 设置。点击<释放>，取消接口的 IP 设置。

图 9-10 配置外网接口为 DHCP 客户端模式



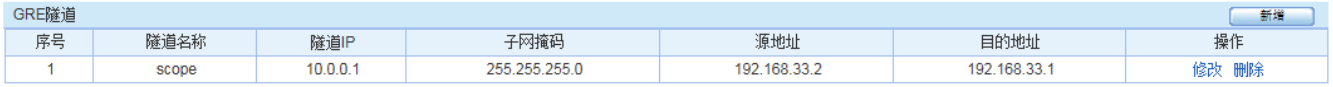
9.1.5 GRE 隧道

功能描述：配置 GRE 隧道。

配置路径：【网络配置】>【接口配置】>【GRE】

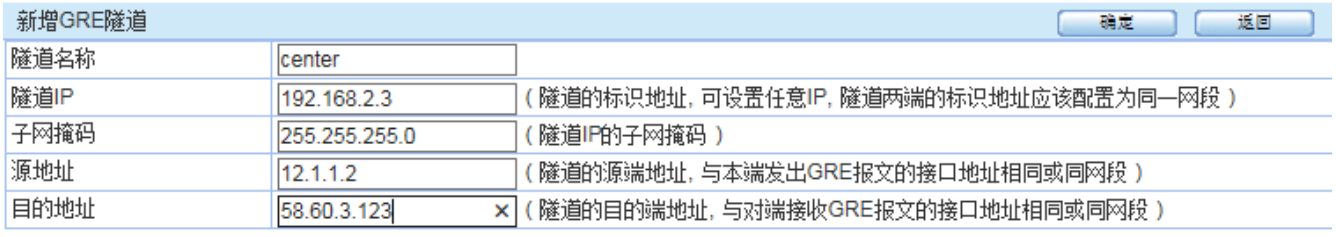
第一：进入【GRE】界面，可以看到当前已经建立的 GRE 配置。如下图：

图 9-11 GRE



第二：点击<新增>按钮，增加 GRE 配置。如下图：

图 9-12 新增 GRE



参数说明：

隧道名称：为 GRE 隧道取的名字。

隧道 IP：隧道的标识地址，可设置任意 IP，隧道两端的标识地址应该配置为同一网段。

子网掩码：隧道 IP 的子网掩码

源地址：隧道的源端地址，与本端发出 GRE 报文的接口地址相同或同网段

目的地址：隧道的目的端地址，与对端接收 GRE 报文的接口地址相同或同网段

提示：配置完 GRE 隧道后，在【网络配置>路由配置】添加路由，选择 GRE 隧道。

9.1.6 网口模式

功能描述：配置网口位置。

配置路径：【网络配置】>【接口配置】>【网口模式】

第一：进入【网口模式】界面，可以看到当前的网口的位置。如下图：

图 9-11 网口设置

网口设置 确定 恢复出厂配置

序号	网口位置(槽位-序号/数量)	名称
1	1-1/2	LAN1
2	1-2/2	WAN1
3	2-1/8	LAN2
4	2-2/8	WAN2
5	2-3/8	LAN3
6	2-4/8	WAN3
7	2-5/8	LAN4
8	2-6/8	WAN4
9	2-7/8	LAN5
10	2-8/8	WAN5
11	3-1/8	LAN6
12	3-2/8	WAN6
13	3-3/8	LAN7
14	3-4/8	WAN7
15	3-5/8	LAN8
16	3-6/8	WAN8
17	3-7/8	LAN9
18	3-8/8	WAN9

对于多插槽的硬件平台，系统缺省从插槽1网口1开始排列，支持手动配置物理接口，重启后方能生效；一旦手动配置，如果需要更换插槽或增加插卡，请事先点击该页面上“恢复出厂配置”，再务必断电后更换或增加插卡。

提示：网口设置功能模块只适用于X系列型号

9.2 配置 IP 地址

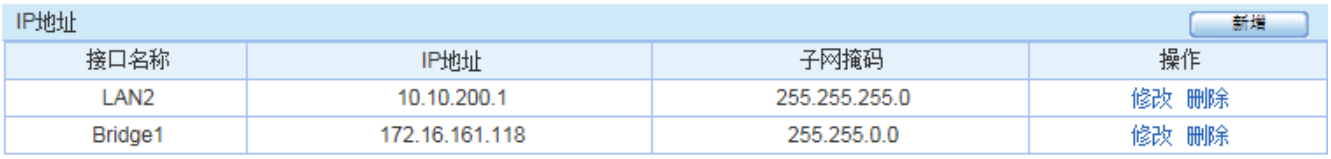
功能描述：用于给设备的接口或网桥配置 IP 地址。在单网桥模式下，可对网桥和其它独立的网口配置 IP 地址；在路由模式下可为每个接口配置 IP 地址。

配置路径：【网络配置】>【配置 IP 地址】

配置描述：

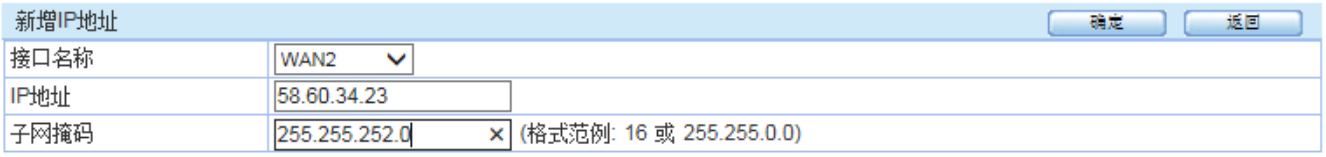
第一：进入【配置 IP 地址】页面，如下图所示：

图 9-13 配置 IP 地址



第二：点击<新增>按钮，为接口增加 IP 地址。新增页面的物理接口名称随工作模式的改变而不同，单网桥时物理接口名称为 Bridge1、LAN2、WAN2，……；双网桥时物理接口名称为：Bridge1 和 Bridge1，……；路由模式时时物理接口名称为 LAN1、LAN2、WAN1、WAN2，……。下图是四个网口，单网桥模式下新增 IP 地址的页面：

图 9-14 新增 IP 地址



提示：

1、 可对物理接口、VLAN 接口、网桥配置 IP 地址。

2、 不同的接口不能配置相同网段的 IP 地址。

3、 每个接口可配置多个不同网段的 IP 地址。

9.3 静态路由

功能描述：配置静态路由。

配置路径：【网络配置】>【静态路由】

配置描述：

第一：进入【静态路由】页面，如下图所示：

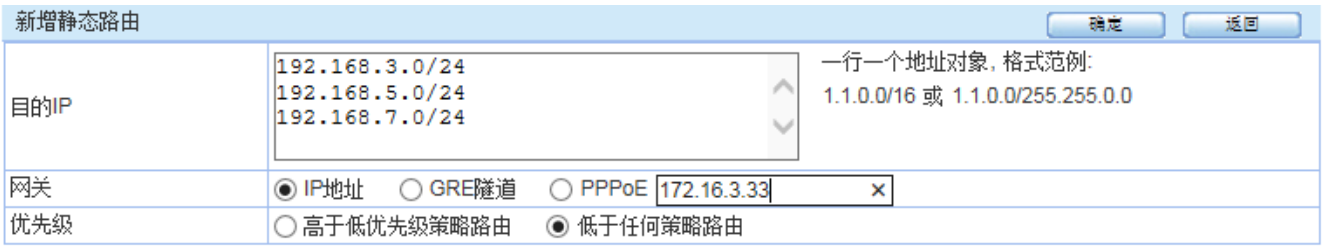
图 9-15 静态路由

静态路由表 新增 删除所有

序号	目的网段	类型	网关	物理接口	优先级	操作
1	0.0.0.0/0	静态	172.16.161.2	Bridge1	低	修改 删除
2	10.0.0.0/24	直连	10.0.0.1	scope	高	修改 删除
3	10.8.0.0/24	直连	10.8.0.2	tun0	高	修改 删除
4	10.10.100.0/24	静态	scope	scope	低	修改 删除
5	10.10.200.0/24	直连	10.10.200.1	LAN2	高	修改 删除
6	172.16.0.0/16	直连	172.16.161.118	Bridge1	高	修改 删除

第二：点击<新增>按钮，增加静态路由。如下图：

图 9-16 新增静态路由



网关可以选择为“IP 地址”、“GRE 隧道”或者“PPPoE”。选择 GRE 隧道和 PPPoE，需先分别到【网络配置>GRE 隧道】和【网络配置>PPPoE 】页面配置 GRE 隧道 PPPoE 拨号。

提示：

1、 直连路由不可以修改和删除。

2、 <删除所有>按钮表示删除所有静态路由。

3、 子网掩码可以输入掩码长度或者点分十进制的格式，如 16 或者 255.255.0.0。

9.4 OSPF 路由

开启和设置 OSPF 动态路由协议，包括网络配置、接口配置、参数配置、信息显示等内容。

9.4.1 网络配置

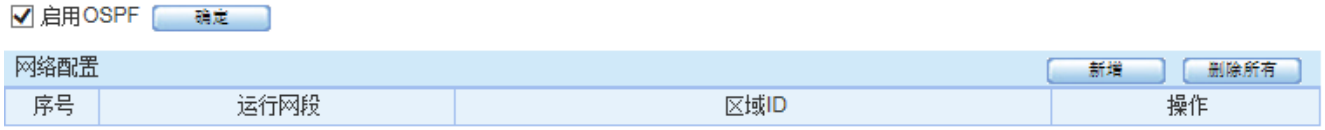
功能描述：开启或关闭 OSPF 路由功能，配置运行 OSPF 的网段。

配置路径：【网络配置】>【OSPF 路由】>【网络配置】

配置描述：

第一：进入【网络配置】页面，可以看到当前配置。如下图所示：

图 9-17 网络配置



参数说明：

启用 OSPF：勾选或不勾选后再点击<确定>按钮，即开启或关闭 OSPF 功能。

新增：增加运行网段。

删除所有：删除所有运行网段。

修改：修改某条已设定的运行网段。

删除：删除某条已设定的运行网段。

第二：进入点击<新增>按钮，增加 OSPF 运行网段。如下图：

图 9-18 新增 OSPF 运行网段

参数说明：

运行网段：设置需要发布的网段地址，填写格式为：IP/掩码。

区域 ID：设置讲该网段引入到那个区域，一般填写骨干区域的 ID。

9.4.2 接口配置

功能描述：显示【OSPF 路由>网络配置】中发布的网段。

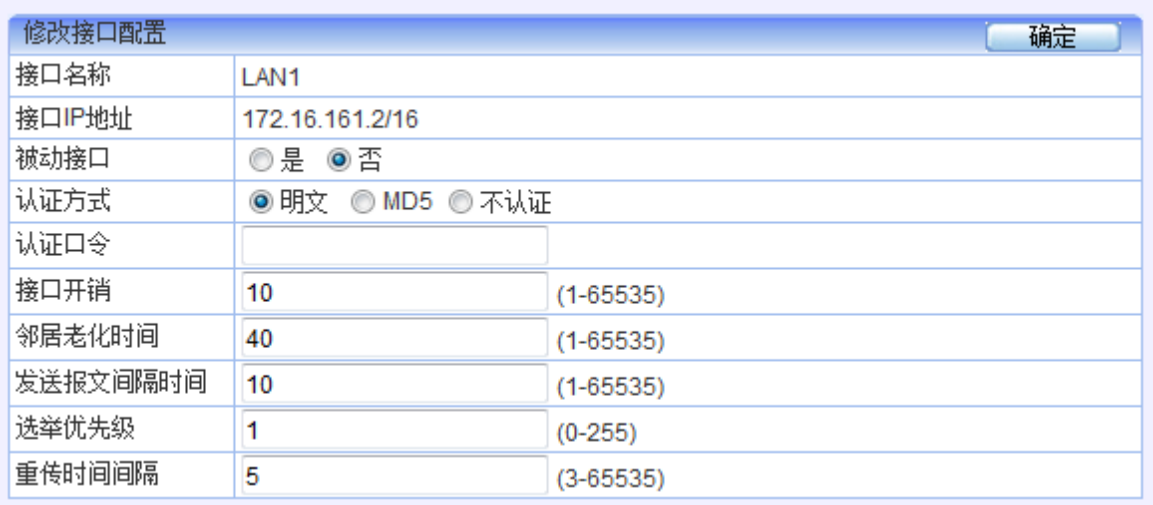
配置路径：【网络配置】>【OSPF 路由】>【接口配置】

配置描述：进入【接口配置】页面，可以看到当前的运行 OSPF 的接口信息。当在【OSPF 路由>网络配置】发布了某网段后，会在此处自动生成接口信息，然后可以对接口的其它参数进行修改。如下图所示：

图 9-19 接口信息

点击<修改>按钮，修改接口信息，如下图所示：

图 9-20 修改接口配置



参数说明：

接口名称：【OSPF 路由>网络配置】中发布的网段对应的接口名称，不可修改。

接口 IP 地址：运行 OSPF 的接口 IP 地址，不可修改。

被动接口：被动接口不发送 OSPF 链路状态，配置为被动接口后，直连路由可以发布，但接口的 OSPF 报文将会被阻塞，邻居无法建立。被动接口默认为[否]。

认证方式：可以选择明文、MD5、不认证，默认是明文认证。

认证口令：设置明文或 MD5 认证方式的口令。

接口开销 :指定从某条链路发送报文的开销。接口开销会影响到 LSA 的 Metric ,直接影响 OSPF 的选路结果 ,范围为 1-65535，默认为 1.

邻居老化时间：默认失效时间是 40s

发送报文间隔时间：Hello 报文的间隔时间，默认为 10s

选举优先级：优先级为 0 的路由器不会被选举成 DR 或者 BDR。DR 由本网段路由器通过 Hello 报文共同选举，设备将自己选出的 DR 写入 Hello 报文中，发网段上其他路由器。当同一网段的两台路由器都宣布自己是 DR 时，优先级高的胜出；如果优先级也相同，Router ID 大的设备胜出。选举优先级默认是 1。

重传时间间隔：缺省情况下，相邻路由重传 LSA 的时间间隔值为 5s。

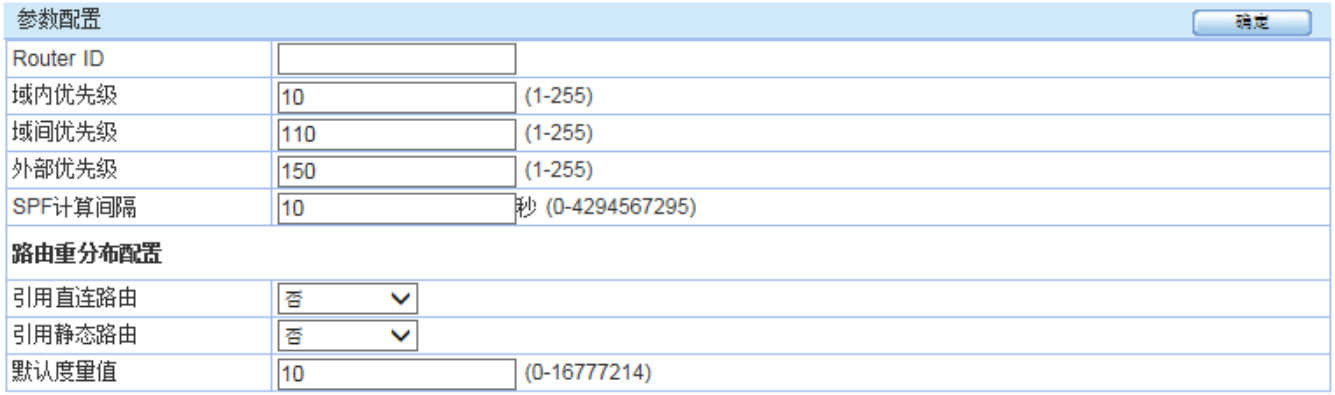
9.4.3 参数配置

功能描述：开启或关闭 OSPF 路由功能，配置运行 OSPF 的网段。

配置路径：【网络配置】>【OSPF 路由】>【参数配置】

配置描述：进入【参数配置】页面，可以看到当前配置的网段。如下图所示：

图 9-21 参数配置



参数说明：

Router ID:设置设备的 Router ID。

域内优先级：域内的 LSA 在计算后输出到路由表时，所携带的优先级（Cisco 设备中成为管理距离 AD），默认为 10。.

域间优先级：域间 LSA 计算后输出到路由表中的优先级，默认值为 110。.

外部优先级：外部路由经过 SPF 计算后，输出到路由表时所赋予的优先级，默认为 150。

SPF 计算间隔：当链路状态数据库 LSDB 发生变化时，需要重新就是最短路径，默认值为 5s。

路由重发布配置 算在是否需要讲直连路由、静态路由引入 OSPF 路由中作为外部路由信息 ,并可设置路由引入后的 Metric 值。

引用直连路由 选择是否需要讲直连路由引入 OSPF 路由中作为外部路由信息 ,并可设置路由引入后的 Metric 值 ,默认为 10。

引用静态路由 选择是否需要讲静态路由引入 OSPF 路由中作为外部路由信息 ,并可设置路由引入后的 Metric 值 ,默认为 10。

默认度量值：默认引入路由的条数，在引入路由时，如果不分别指定各类型路由的 Metric 参数，则使用该度量值作为路由引入后的跳数。度量值默认为 10。

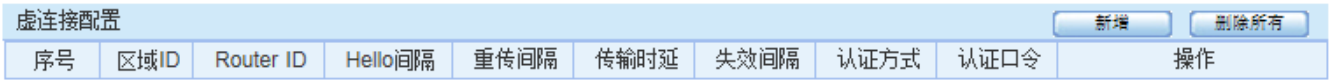
9.4.4 虚链路配置

功能描述：当设备所在的区域与 OSPF 的骨干区域不相邻时。需要启用和配置虚连接。

配置路径：【网络配置】>【OSPF 路由】>【虚连接配置】

配置描述：进入【虚链路配置】页面，可以看到当前虚连接的配置。如下图所示：

图 9-22 虚链路配置



进入点击<新增>按钮，增加 OSPF 运行网段。如下图：

图 9-23 新增 OSPF 运行网段

参数说明：

区域 ID：填写骨干区域的 ID。

Router ID：填写建立虚连接的对端路由器 ID，指明与哪一台路由器建立虚连接。

Hello 间隔：设置发送 Hello 报文的间隔，默认 10s。

重传时间：与接口相邻的连接状态报文重发时间，默认 10s。

传输时延：传输一个链路状态更新数据包的估计时间，默认 5s。

失效间隔：如果超过失效间隔时间还未收到 Hello 报文，则认为该 OSPF 邻居不可达，一般设置为 Hello 间隔的 4 倍，默认是 40s。

认证口令：报文加密使用的口令。

9.4.5 信息显示

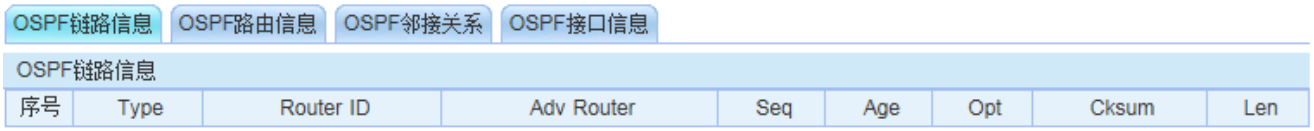
9.4.5.1 OSPF 链路信息

功能描述：显示 OSPF 链路信息。

配置路径：【网络配置】>【OSPF 路由】>【信息显示】

配置描述：进入【信息显示>OSPF 链路信息】页面，查看当前 OSPF 链路信息。如下图所示：

图 9-24 OSPF 链路信息



参数说明：

Type：LSA 的类型。

Router ID：LSA 所在的 Router ID，* 代表设备自己产生的 LSA。

Adv Router：表示有哪个设备通告的这条 LSA 给本设备。

Seq：这条 LSA 的序号。

Age：表示收到该 LSA 已有多长时间。超时时间到了之后，该 LSA 将被老化。

Opt：表示 Hello 报文中携带的选项信息。如果邻居与本设备的 Option 字段一致，可以拒绝接受该邻居的消息。

Cksum：LSA 的校验和。

Len：LSA 的长度。

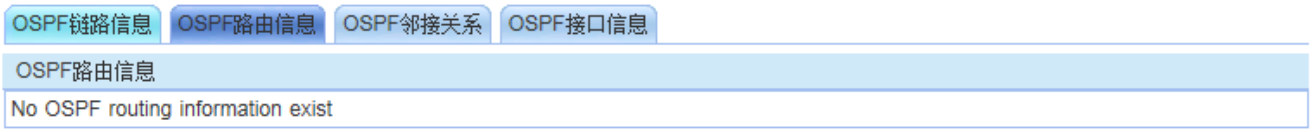
9.4.5.2 OSPF 路由信息

功能描述：显示 OSPF 路由信息。

配置路径：【网络配置】>【OSPF 路由】>【信息显示】

配置描述：进入【信息显示>OSPF 路由信息】页面，查看当前 OSPF 路由信息。如下图所示：

图 9-25 OSPF 路由信息



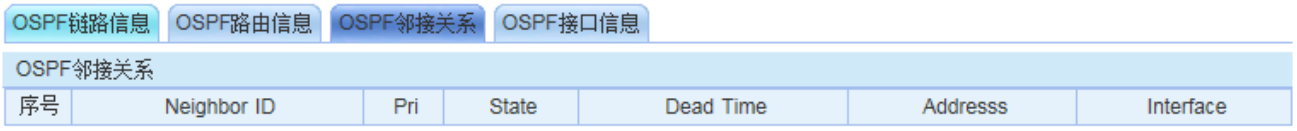
9.4.5.3 OSPF 邻接关系

功能描述：显示 OSPF 邻接关系。

配置路径：【网络配置】>【OSPF 路由】>【信息显示】

配置描述：进入【信息显示>OSPF 邻接关系】页面，查看当前 OSPF 邻接关系。如下图所示：

图 9-26 OSPF 邻接关系



参数说明：

Neighbor ID：邻接路由器的 Router ID。

Pri：邻接路由器的优先级。

State：邻接路由器的功能状态。

Dead Time：如果邻居不发 Hello 报文，还有多长时间该路由器变为 Dead。

Address：邻居与本设备相连接口的 IP 地址。当 OSPF 信息包被传输到邻居，此地址将是下一跳 IP 地址。OSPF_VL1 是虚连接标识。

Interface：邻居与本设备相连的接口。

9.4.5.4 OSPF 接口信息

功能描述：显示 OSPF 接口信息。

配置路径：【网络配置】>【OSPF 路由】>【信息显示】

配置描述：进入【信息显示>OSPF 接口信息】页面，查看当前 OSPF 接口信息。如下图所示：

图 9-27 OSPF 接口信息

参数说明：

Interface：接口名称。

IP：接口的 IP 地址。

Area：该接口所属区域。

State：该接口的角色。

DR：该区域的 DR 地址。

BDR：该区域的候选 BDR 地址。

9.5 策略路由

9.5.1 策略路由

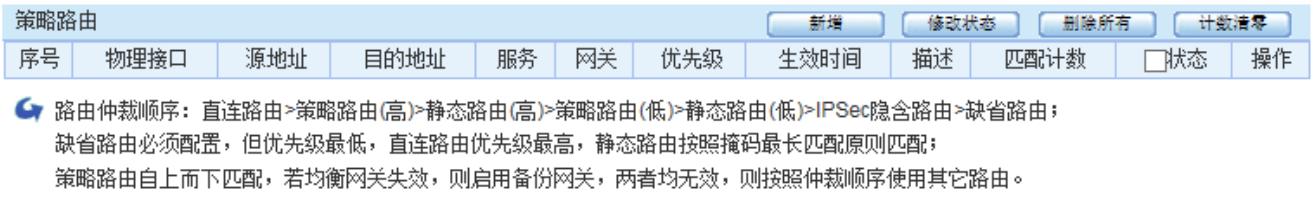
功能描述：配置策略路由。

配置路径：【网络配置】>【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 9-28 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：

新增：增加策略路由

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)策略路由的状态。状态列对应的复选框如果为“勾选”状态，则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。

删除所有：删除所有策略路由。

修改：修改某条策略路由。

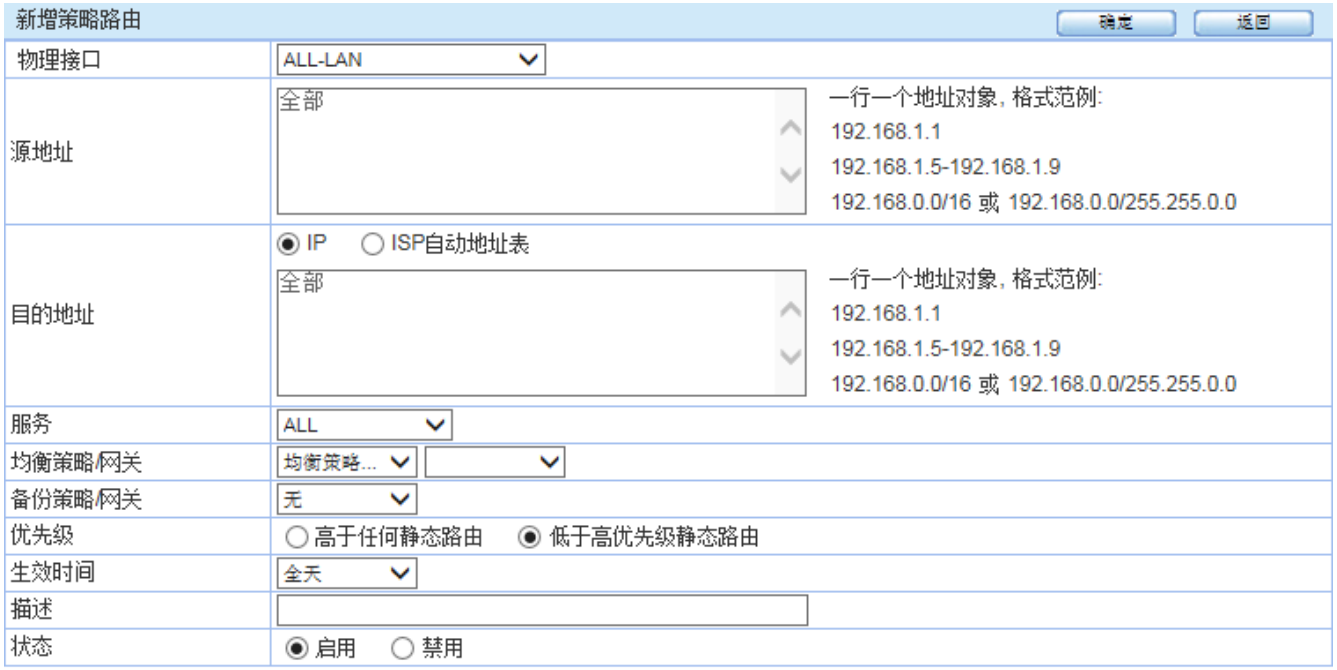
插入：在本条路由之前插入一条路由。

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。

删除：删除某条路由。

第二：进入点击<新增>按钮，增加策略路由。如下图：

图 9-29 新增策略路由



参数说明：

LAN 接口：连接内网的物理端口，ALL-LAN 表示所有 LAN 口。

源地址：匹配报文的源地址，可以输入多个地址。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、网通、铁通。

服务：匹配报文的四层服务。

均衡策略/网关：选择均衡策略；均衡策略的详细配置和说明见“均衡策略”一节。

备份策略/网关：选择备份均衡策略；系统首选按照“均衡策略/网关”的算法策略进行选路，若“均衡策略/网关”失效，则按照“备份策略/网关”的算法策略进行选路。

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。

9.5.2 均衡策略

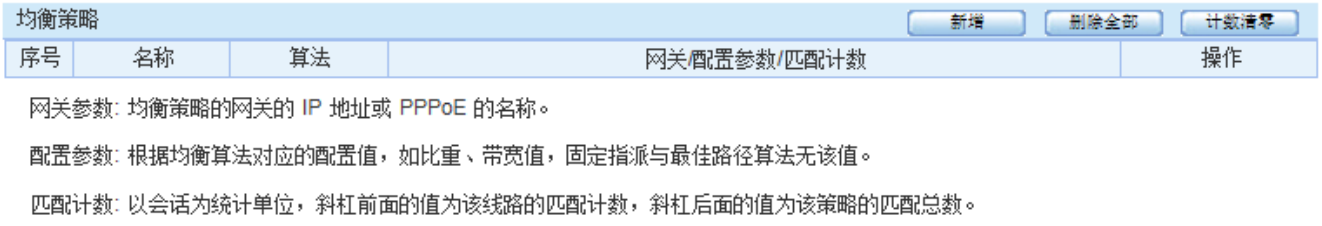
功能描述：配置均衡策略。

配置路径：【网络配置】>【策略路由】>【均衡策略】

配置描述：

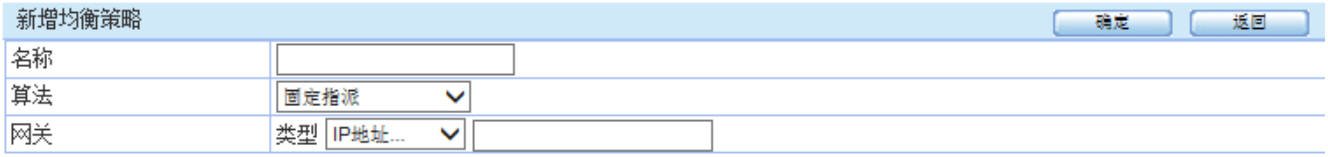
第一：进入【均衡策略】页面，可以看到当前配置。如下图所示：

图 9-30 均衡策略



第二：进入点击<新增>按钮，增加均衡策略。如下图：

图 9-31 新增均衡策略-固定指派



参数说明：

名称：均衡策略名称。

算法：均衡策略算法，共 5 种算法，分别如下：

固定指派：固定指派某条链路。

轮询（源 IP）：按照源 IP 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。

上行流量：根据链路的下行流量所占的比重，进行计算选路。

网关：出口网关地址。网关类型可选择为“IP”或“PPPoE”。如果选择“IP”，则直接在后面的输入框内填入网关 IP 地址即可。如果选择“PPPoE”，在直接在后面的下拉框里选择之前配置好的 PPPoE 拨号的名称即可。

图 9-32 新增均衡策略-轮询(源 IP)

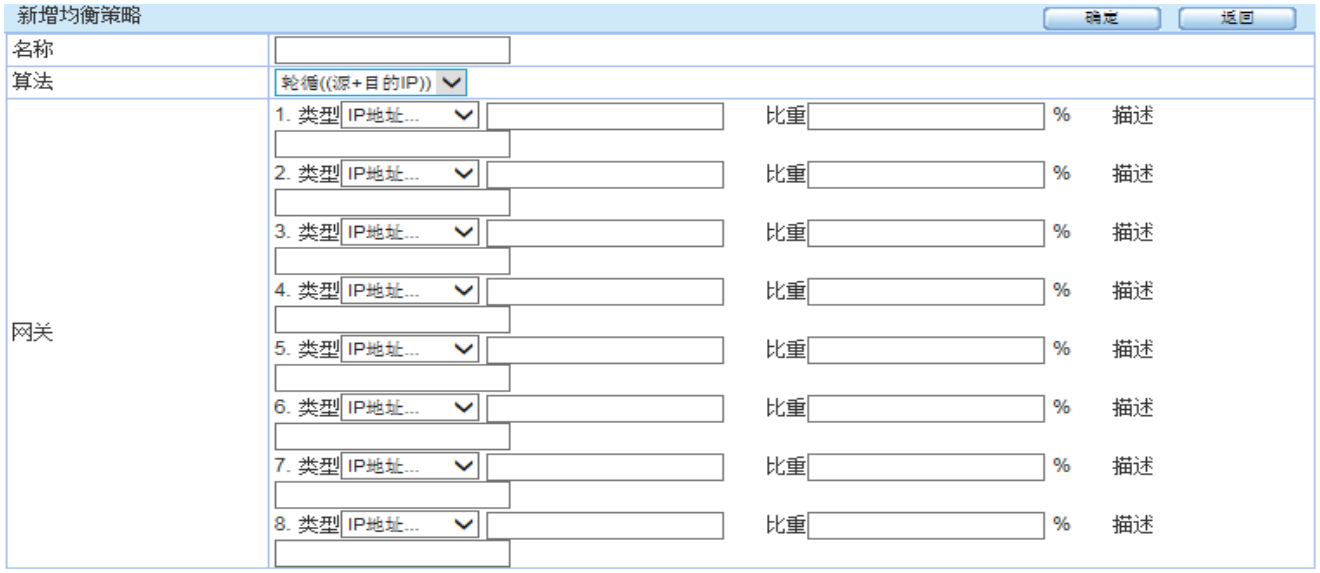
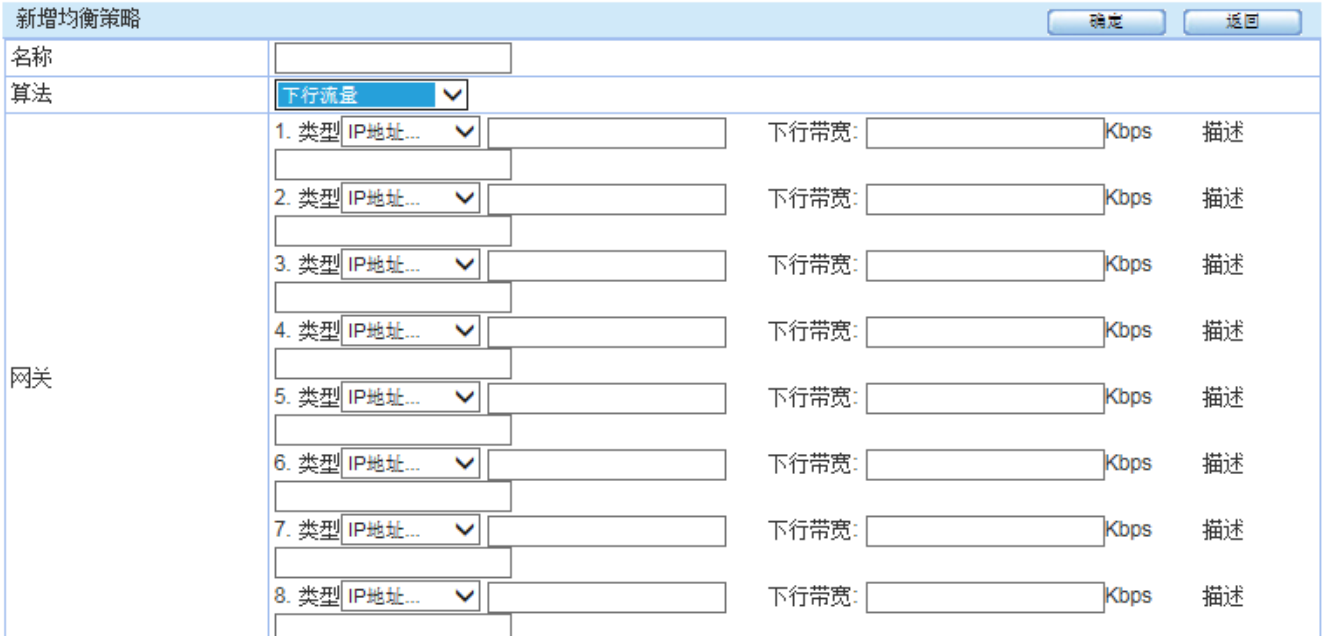


图 9-33 新增均衡策略-下行流量



9.5.3 持续路由

持续路由是指当要建立连接时，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。

功能描述：配置持续路由策略规则。

配置路径：【网络配置】>【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 9-34 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 9-35 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，可以选择为地址簿或者输入 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，可以选择为地址簿或者输入 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。

动作：选择为“使用持续路由”或“不使用持续路由”。

9.5.4 链路健康检查

功能描述：检测链路的健康状态。

配置路径：【网络配置】>【策略路由】>【链路健康检查】

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规则。如下图所示：

图 9-36 链路健康检查

链路健康检查 新增 修改状态 删除全部 计数清零

序号	名称	网关	侦测间隔（秒）	重试次数	失效次数	探测（丢失/总数）	丢失率	静态路由检查	静态路由切换	链路状态	□状态	操作
1	wan	192.168.1.1	3	3	0	0/0	0.0000%	禁用	禁用	正常	☑	修改 删除

第二：进入点击<新增>按钮，增加联络健康检查规则。如下图：

图 9-37 新增链路健康检查

新增链路健康检查 确定 返回

名称	
网关	类型 IP地址 （ISP提供的网关IP地址）
侦测目标	一行一个侦测对象，格式： ping/目标IP地址 或 dns/DNS服务器IP地址/目标域名 或 tcp/目标IP地址/端口，例如： ping/1.1.1.1 dns/202.96.154.8/www.google.cn tcp/2.2.2.2/65
侦测间隔	3 (1-600秒)
重试次数	3 (1-20)
状态	◉ 启用 ○ 禁用
静态路由检查	○ 启用 ◉ 禁用
静态路由切换	○ 启用 ◉ 禁用

参数说明：

名称：链路健康检查规则的名称。

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。

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。

静态路由检查 :开启静态路由检查 ,当前网关失效后 ,可以实现静态路由的备份。比如 ,配置了 3 条路由 :ip route add 0.0.0.0/1 via 1.1.1.1、ip route add 128.0.0.0/1 via 1.1.1.1 和 ip route add 0.0.0.0/0 via 2.2.2.2。启用对 1.1.1.1 的健康检查，并开启“静态路由检查”。假设目的 IP 是 202.96.134.133，因静态路由查找本身是最长匹配的，所以先查 128.0.0.0/1，再查 0.0.0.0/0。目的 IP 202.96.134.133 本来应该匹配 128.0.0.0/1，由于 1.1.1.1 失效，则路由 128.0.0.0/1 via 1.1.1.1 不参与查找，所以继续查找 0.0.0.0/0，从而 202.96.134.133 匹配到 2.2.2.2，达到了路由备份功能。

静态路由切换：如果检查到该网关失效，那么“目的子网”内配置的网段将被切换到“备份网关”上。比如，在网关 1.1.1.1 上启用 “静态路由切换”，“目的子网”配置为 121.1.2.0/24，“备份网关”配置为 2.2.2.2。如果链路 1.1.1.1 失效，目的网段 121.1.2.0/24 将被切换到备份网关 2.2.2.2，从而实现了链路备份功能。

备份网关：当主网关失效后，“目的子网”内配置的网段将被切换到“备份网关”上。

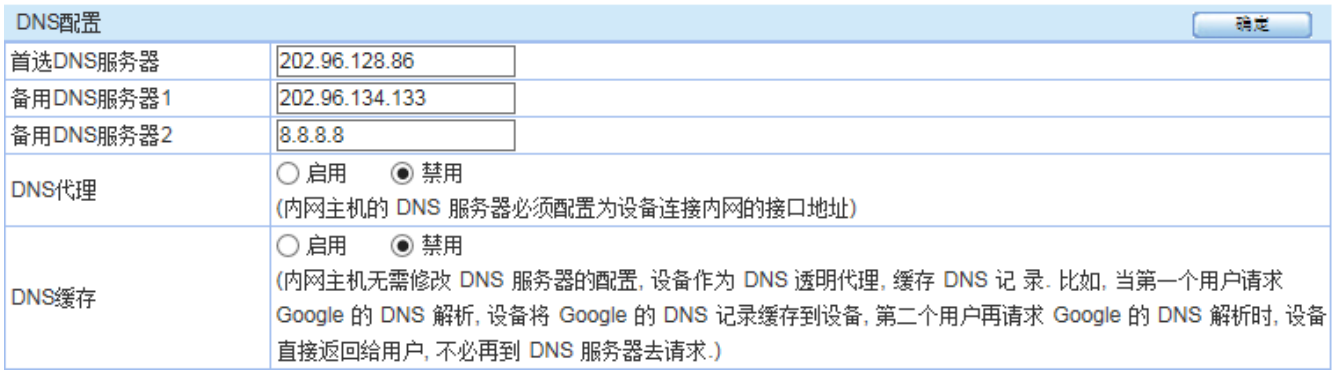
9.6 DNS 配置

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 9-38 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。

9.7 DDNS 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 9-39 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。

9.8 智能 DNS

智能 DNS：对于多 IP 的 DNS 解析，根据用户的来路而做出一些智能化的处理，然后把智能化判断后的 IP 返回给用户，而不需要用户进行选择。

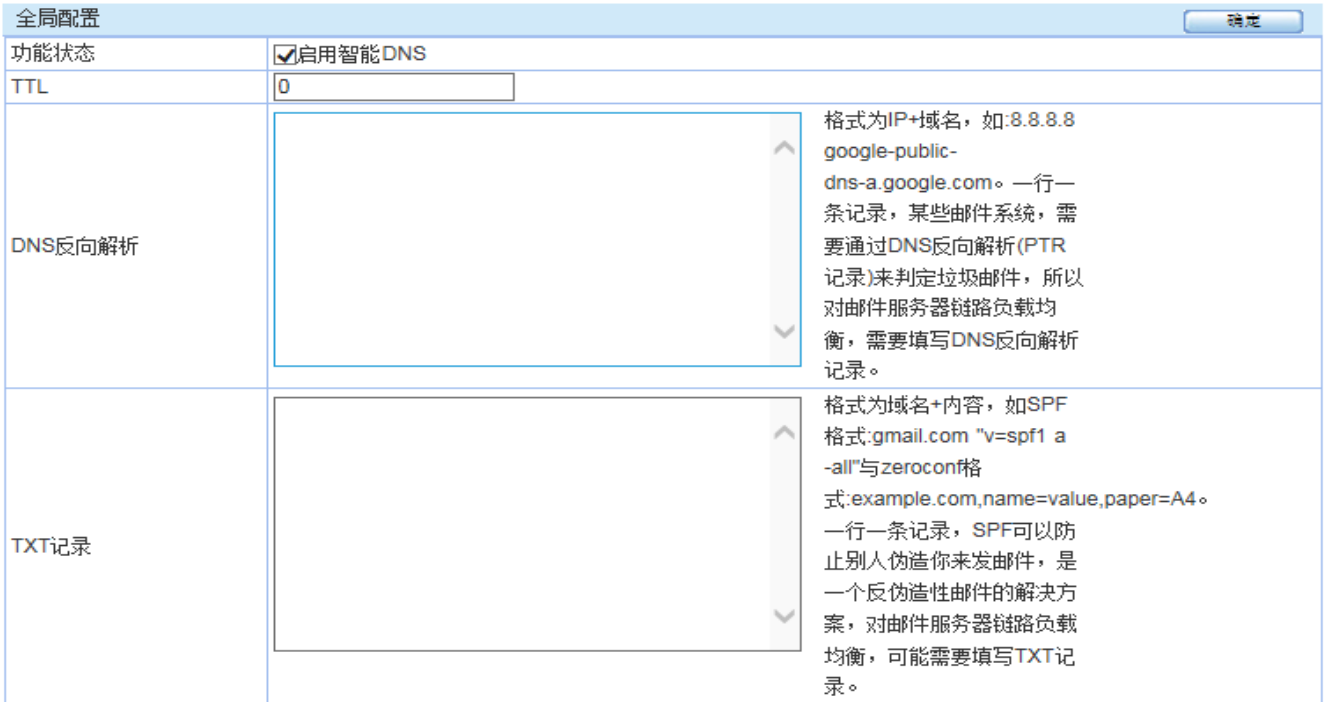
9.8.1 全局配置

功能描述：启用或禁用智能 DNS 功能。

配置路径：【网络配置】>【智能 DNS】>【全局配置】

配置描述：进入【全局配置】页面，启用或禁用智能 DNS 功能。如下图所示：

图 9-40 全局配置



9.8.2 线路配置

功能描述：配置 DNS 线路（用户来路）的相关参数。

配置路径：【网络配置】>【智能 DNS】>【线路配置】

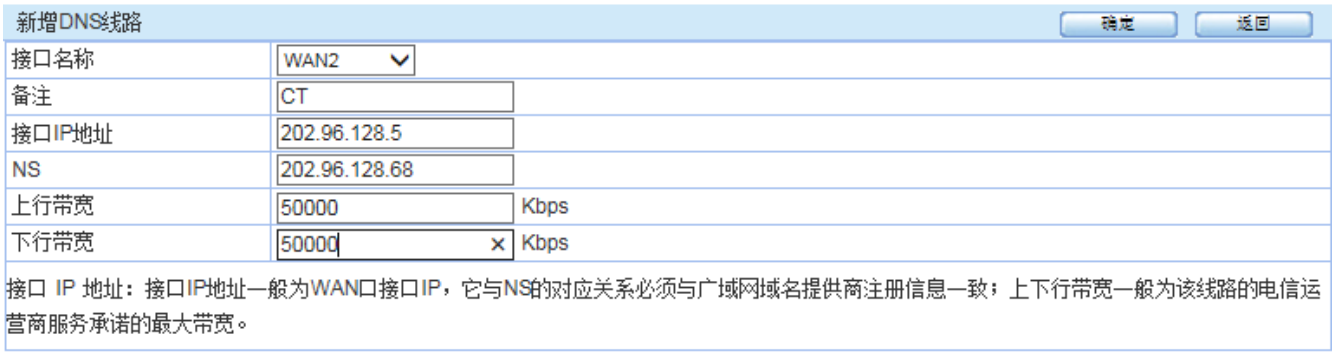
配置描述：

第一：进入【线路配置】页面，已配置的线路参数如下图所示：

图 9-41 线路配置

第二：点击<新增>按钮，增加线路配置。如下图：

图 9-42 新增线路配置



参数说明：

接口名称：选择出口线路的接口名称，如 WAN1。

备注：填写线路的注释。

接口 IP 地址：当出口接口有多个 IP 时，需要指定一个 NS 的 A 记录对应的 IP 地址。若接口有多个 IP 地址，但此处不配置 IP 地址，则系统随机选择一个 IP 地址。若接口只有一个 IP 地址，此处的 IP 地址无需配置。

NS：名字服务器（Name Server），用来指定该域名由哪个 DNS 服务器来进行解析。可配置为域名或 IP 地址。

上行带宽：出口线路的上行带宽值，运营商分配的实际带宽。

下行带宽：出口线路的下行带宽值，运营商分配的实际带宽。

9.8.3 均衡策略

功能描述：当一个域名对应多个 IP 的情况，进行 DNS 解析时采用的均衡策略。

配置路径：【网络配置】>【智能 DNS】>【均衡策略】

配置描述：

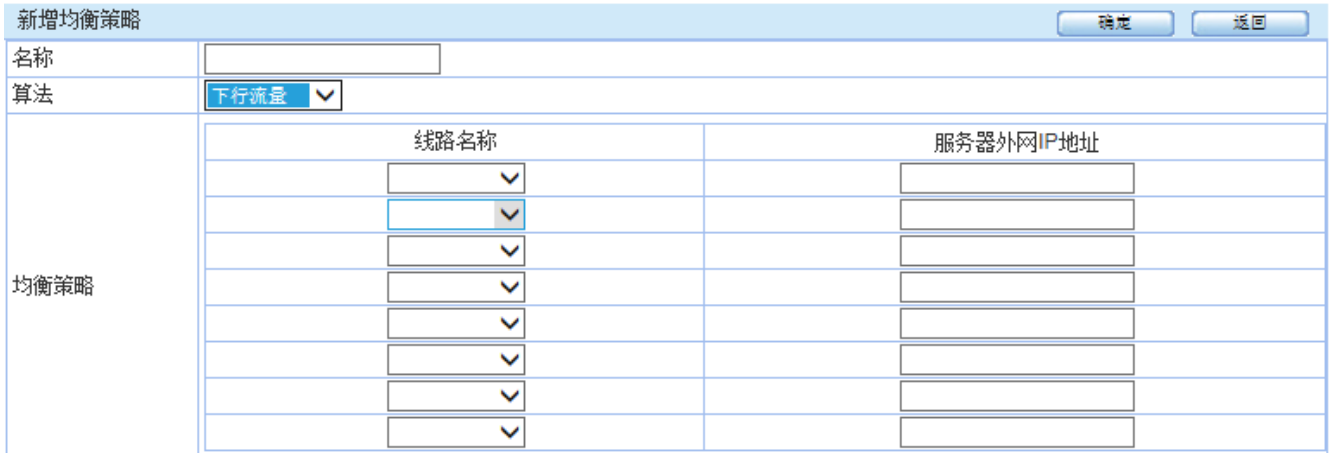
第一：进入【均衡策略】页面，已配置的策略参数如下图所示：

图 9-43 均衡策略

第二：点击<新增>按钮，增加策略配置。如下图：

图 9-44 新增策略配置-1

图 9-45 新增策略配置-2



参数说明：

名称：均衡策略的名称。

算法：选择 DNS 均衡算法，包括以下 3 种算法：

按权重：各线路按一定的权重比例分配。

按上行流量：根据线路的上行流量的使用情况进行分配，空闲的线路将被分配的几率大。

按下行流量：根据线路的下行流量的使用情况进行分配，空闲的线路将被分配的几率大。

按总流量：根据线路的总流量的使用情况进行比例，空闲的线路将被分配的几率大。

均衡策略：根据被选择的算法，配置每条线路对应的参数，包括：

线路名称：选择线路的名称，如 WAN1。

服务器外网 IP：需被进行 DNS 解析的内部服务器对应的公网 IP 地址，如果服务器无公网 IP 地址，需要在本设备上进行地址映射，具体配置参见【防火墙> NAT 规则】

权重比例：当算法选择为[按权重]时，需要配置每条线路所占权重的比例，所有线路的权重之后为 100%。

9.8.4 DNS 策略

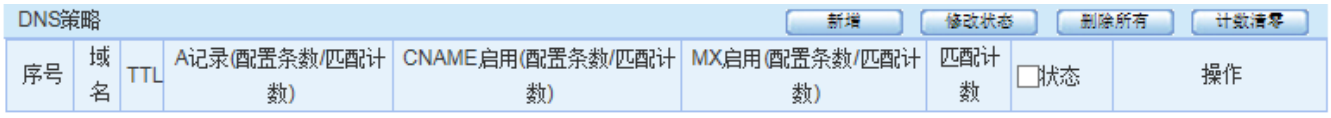
功能描述：配置 DNS 分配策略的的相关参数。

配置路径：【网络配置】>【智能 DNS】>【均衡策略】

配置描述：

第一：进入【DNS 策略】页面，已配置的策略如下图所示：

图 9-46 DNS 策略



第二：点击<新增>按钮，增加 DNS 策略配置。如下图：

图 9-47 新增 DNS 策略

参数说明：

域名：在此填入需要做多重定制的网域名称（Domain Name）。

TTL：DNS 查询回复时间。

A 记录：

主机名（Host Name）：输入主机名称的前置词。举例来说，如果主机名称为 www.abc.com，则在此填入 www。

源地址：查询本记录的 IP 地址。可以选择为：

地址簿：可选择已定义好的地址簿里面的地址，详见【系统对象>地址簿】

ISP 地址表：可选择系统已定义好的运营商的地址。

手动输入：手动输入 IP 地址，地址格式范例：192.168.11.5、192.168.11.5-192.168.11.50、192.168.11.0/24

任意地址：包含所有地址。

均衡策略：选择被解析的域名对应的均衡策略。

匹配计数：此策略被匹配的次数。

状态：策略是否开启。

CName 记录：

别名（Alias）：网域名称的别名。例如，想使用 www1.abc.com 来当作 www.abc.com 的别名，此处填入 www1。

主机名（Host Name）：输入主机名称的前置词。举例来说，如果主机名称为 www.abc.com，则在此填入 www。

匹配计数：此策略被匹配的次数。

状态：策略是否开启。

MX 记录：

主机名（Host Name）：输入主机名称的前置词。举例来说，如果主机名称为 www.abc.com，则在此填入 www。

优先级：设定邮件服务器的优先级，范围 0-65535，数字越小优先级越高。同一个域名的有多条不同优先级的 MX 记录，通常是用优先级高的。当优先级高的机器不能使用时，优先级低的就可以起到临时备份作用，代收邮件和转发。当优先级高的机器正常时，低级别的会尝试把信件转发给优先级高的服务器。只存在一条 MX 记录时，优先级没有意义。

匹配计数：此策略被匹配的次数。

状态：策略是否开启。

按钮说明：

新增： 增加策略条目。

修改状态：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)。

计数清零：把匹配计数清除，还原为零。

删除所有：删除所有策略条目。

上移：将此策略条目上移。

下移：将此策略条目下移。

插入：在此策略条目插入一条策略。

删除：删除一条策略。

9.9 ARP 表

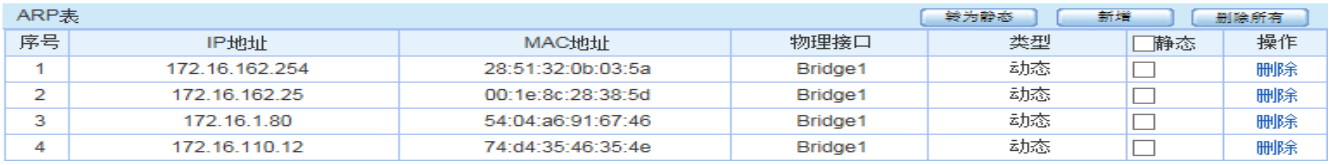
功能描述：查看 ARP 表，配置静态 ARP。

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：

图 9-48 ARP 表

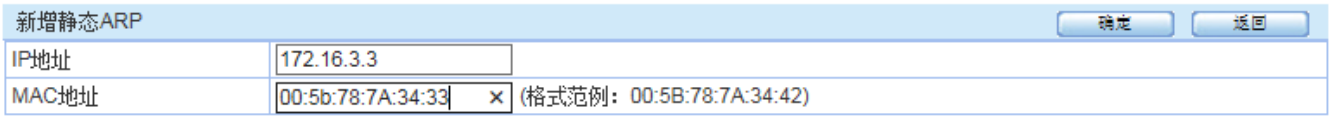


类型为“动态”代表自动学习到的 ARP 条目；为“静态”代表将固定的 IP 和 MAC 绑定在一起。

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：

图 9-49 新增静态 ARP



9.10 DHCP 配置

9.10.1 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：

图 9-50 DHCP 基本参数

超级作用域：启用后能实现一个接口分发多个逻辑 IP 网段（子网）的地址。

第二：进入点击<新增>按钮，增加 DHCP 配置。如下图：

图 9-51 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。

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 的地址必须在 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

子网掩码：配置 DHCP 客户端所获得的 IP 地址的掩码。

网管 IP：配置 DHCP 客户端所获得的网关 IP 地址。一般为第一行选择的接口的 IP。

租用期限：设置 DHCP 获得的 IP 地址的有效期，默认为永远有效。

Option43: 在 WLAN 的 AC + Fit AP 组网结构中，Fit AP 为了能够找到 AC 的网络位置，需要在网络的 DHCP 服务器上开启 option 43 选项

不同厂家的 DHCP 实现 option 43 的方式不一样。常见的厂家配置如下：

windows/linux/华为格式：
03 + 长度 + 单个 ip 数字的十六进制以及十六进制点号。
以 AC 的 IP 地址为 192.168.22.1 为例，对应的 Option 43 字段应该填写为：03:0C:31:39:32:2E:31:36:38:2E:32:32:2E:31。其中，03 为固定值，十六进制数 0C(“0C”等于十进制数“12”)代表 IP 地址 192.168.22.1 的长度，包含小数 点“.” ；十六进制数 31 对应“1”的 ACCII 值，32 对应“2”的 ASCII 值，以此类推，十六进制数 2E 对应小数点“.”的 ASCII 值，即值 31:39:32:2E:31:36:38:2E:32:32:2E:31 表示 AC 的 IP 地址 192.168.22.1。

锐捷格式：
f1:04 + 16 进制 IP。 以 AC 的 IP 地址为 192.168.22.1 为例，对应的 Option 43 字段应该填写为：f1:04:c0:a8:16:01。其中，f1:04 为固定值，c0:a8:16:01 代表十六进制 IP 地址。

大唐格式：
01:06:01:04 + 16 进制 IP。以 AC 的 IP 地址为 192.168.22.1 为例 对应的 Option 43 字段应该填写为 :01:06:01:04:c0:a8:16:01。其中，01:06:01:04 为固定值，c0:a8:16:01 代表十六进制 IP 地址。

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 LAN 口地址同网段，不要包含网络地址及网段广播地址，多个范围间地址不能重叠。

3、 固定 IP 地址应包含在 IP 地址池中。

4、 每个接口都可以启用 DHCP，包括桥接口，如 bridge1。

9.10.2 DHCP 中继

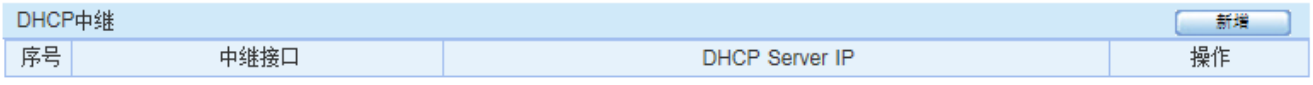
功能描述：配置 DHCP 中继。

配置路径：【网络配置】>【DHCP 配置】>【DHCP 中继】

配置描述：

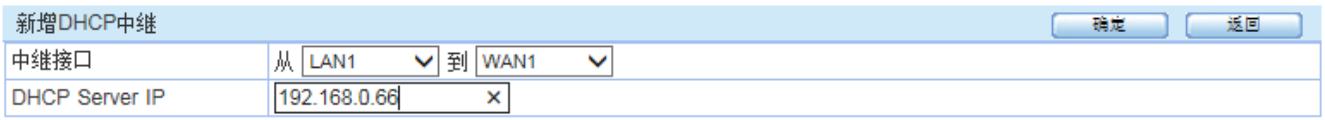
第一：进入【DHCP 中继】页面，可以看到当前已建立的 DHCP 中继配置。如下图：

图 9-52 DHCP 中继



第二：进入点击<新增>按钮，增加 DHCP 中继配置。如下图：

图 9-53 新增 DHCP 中继



参数说明：

中继接口：LAN 口是连接内网主机方向的端口，WAN 口是连接 DHCP 服务器方向的端口。

DHCP Server IP：DHCP 服务器 IP 地址。

9.10.3 已分配 IP 地址

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。

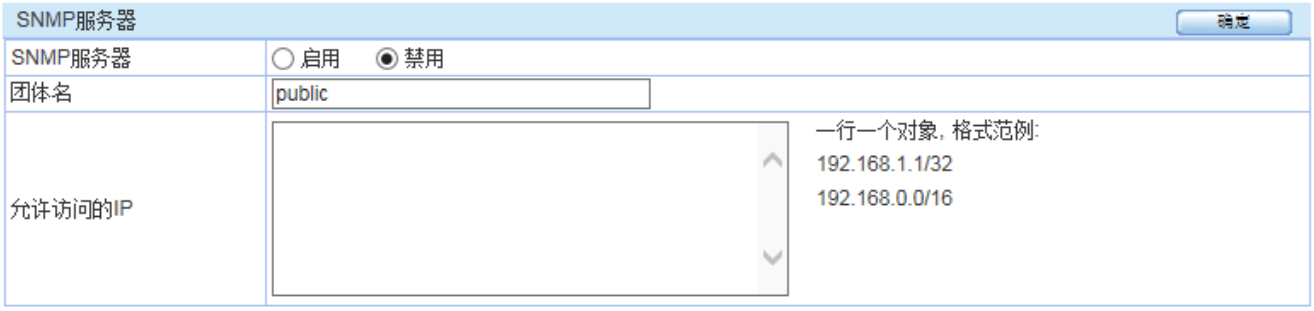
9.11 SNMP 服务器

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：【网络配置】>【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 9-54 SNMP 服务器



9.12 代理服务器列表

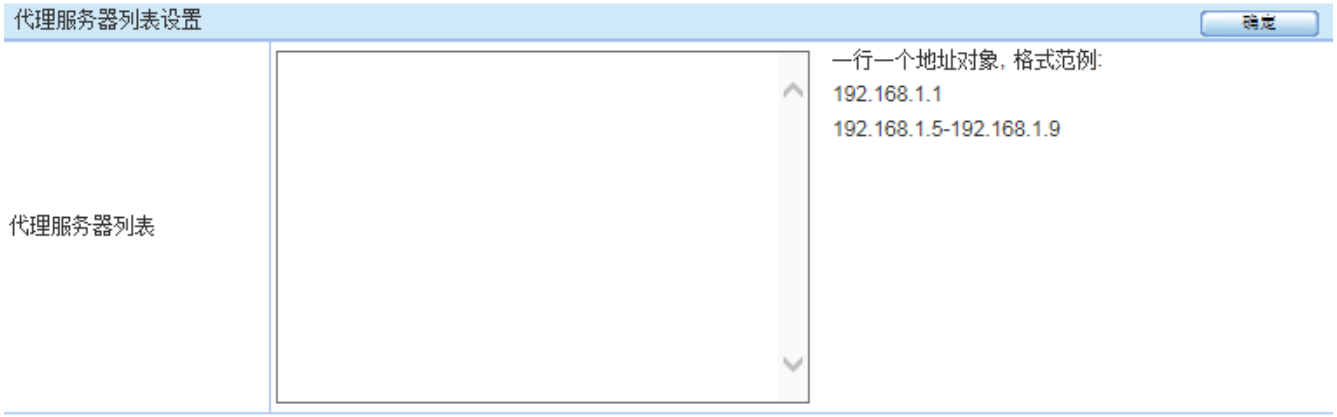
当内网使用了代理时，所有的数据报文都被重新封装，原来的特征库将不能识别这部分被代理封装的报文。系统对此处配置的代理服务器地址将先封装头再进行特征分析。若对所有报文都进行这样的分析，将消耗大量性能，所以通过此方法来减少对性能的无谓消耗。

功能描述：配置代理服务器的 IP 地址。

配置路径：【网络配置】>【代理服务器列表】

配置描述：进入【代理服务器列表】页面，代理服务器的 IP 地址。如下图：

图 9-55 代理服务器列表



9.13代理配置

对于 SSL 网页的分析和审计，默认是关闭的，若需要分析和审计需要设定相关的参数。

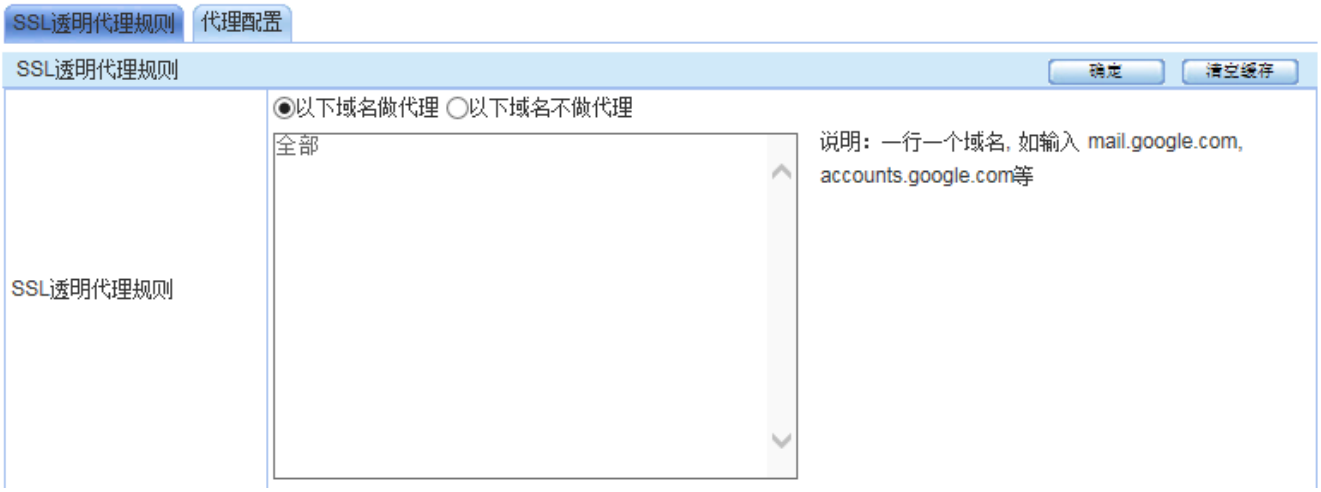
功能描述：设定需要做分析和审计的 SSL 域名。

配置路径：【网络配置】>【代理配置】

配置描述：

第一步：进入【代理配置】页面，配置需要代理的 SSL 页面的域名。如下图：

图 9-56 SSL 代理配置



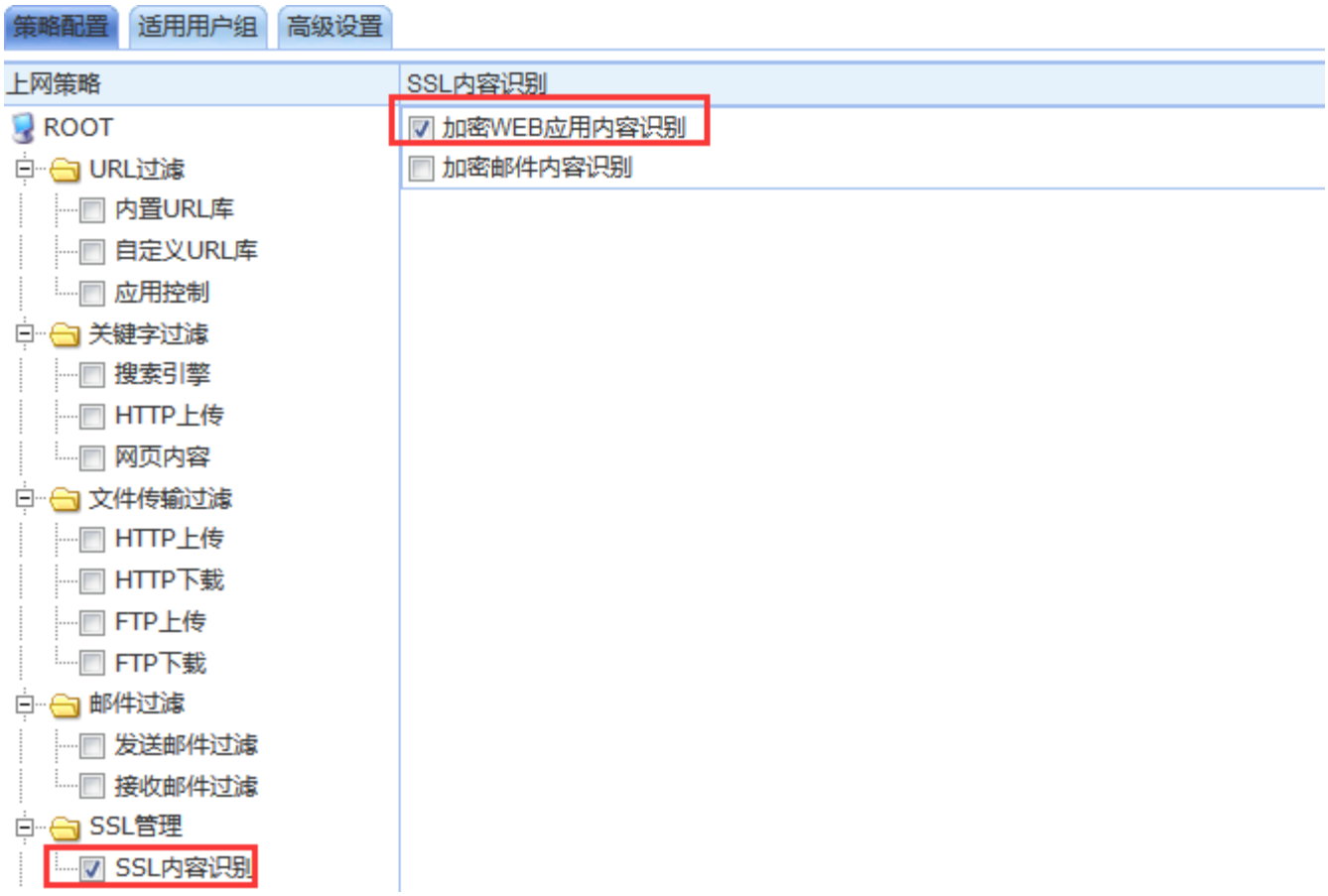
参数说明：

代理方式：选择需要被代理的域名设定方式。[以下域名做代理]表示在域名列表里面的域名需要进行 SSL 代理，以便于对这些 SSL 网站内容进行分析和审计。[以下域名不做代理] 表示除了在域名列表里面以外的域名需要进行 SSL 代理 ,以便于对这些 SSL 网站内容进行分析和审计。

域名列表：设定需要或不需要做 SSL 代理的域名，一行一个域名，可输入多个域名。

第二步：进入【行为管理】>【上网策略】>【上网权限策略】页面，在相应的用户组或者用户的配置界面启用 SSL 代理功能，如下图红色框所示。

图 9-57 启用 SSL 代理配置



00.

10 防火墙

“防火墙”设置包括安全策略、NAT 规则设置。NAT 规则包含内网代理、一对一地址转换、端口映射三部分。

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，如下图：

图 10-1 安全策略

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 LAN2→LAN2 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 10-2 新增安全策略

参数说明：

策略方向：代表数据流的方向。

源地址：数据流的源地址，可输入 IP 地址或选择地址簿。地址簿在【系统对象>地址簿】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：数据流的服务类型。

生效时间：本策略的有效时间段。

动作：安全策略允许、拒绝服务的动作。

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、 系统隐含了一条允许所有的安全策略，如果加入的安全策略都不匹配，数据包最后将匹配隐含的策略。所以系统在默认情况，是允许所有报文通过的。

10.2 NAT 规则

“NAT 规则”包括三种 NAT 方式，包括：内网代理、一对一地址转换、端口映射。

10.2.1 内网代理

功能描述：作为内部网络的代理网关，转换内部主机上网数据流的源 IP 地址。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。

内网代理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。

配置路径：【防火墙】>【NAT 规则】>【内网代理】

配置描述：

第一：进入【防火墙】页面，如下图：

图 10-3 内网代理规则

点击<删除所有>，将删除所有的内网代理规则。

点击<删除>，删除本条规则。

点击<修改>，修改本条规则的参数，但不能修改流量方向。

点击<插入>，在当前位置之前插入一条规则。

点击<移动>，改变对应规则的序号，从而改变规则的优先级。

改变状态栏复选框的值，再点击<修改状态>，可改变规则状态(“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，新增规则，如下图：

图 10-4 新增内网代理

参数说明：

规则名称：内网代理规则的名称。

流量方向：代表数据流的方向，方向必须从内网端口（LAN1、LAN2）到外网端口（WAN1、WAN2）。

内部源地址：内网主机发出的数据流的源地址，可输入 IP 地址或选择地址簿。地址簿在【系统对象>地址簿】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：选中的服务才可通过 NAT 转换上网。

转换后源地址：数据流从设备出去时的源 IP 地址，可选择外网口地址（如 WAN1 接口地址）或输入一个地址范围

状态：启用或禁用本规则，默认启用。

> **提示：**内网代理规则遵循从上向下匹配的原则，如果一个规则匹配了，就不会再向下匹配了，所以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。

10.2.2 一对一地址转换

功能描述：

将内网的私有 IP 转换为公有 IP，一个私有 IP 只能对应一个公有 IP，主要用于对内网服务器的转换。

配置路径：【防火墙】>【NAT 规则】>【一对一地址转换】

配置描述：

第一：进入【一对一地址转换】页面，如下图：

图 10-5 一对一地址转换

点击<删除所有>，将删除所有的内网代理规则。

点击<删除>，删除本条规则。

点击<修改>，修改本条规则的参数，但外网口不能修改。

改变状态栏复选框的值，再点击<修改状态>，可改变规则状态(“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，新增规则，如下图：

图 10-6 新增一对一地址转换规则

参数说明：

规则名称：一对一地址转换规则的名称

外网口：连接外网的物理接口，如 WAN1、WAN2

内部 IP 地址：内网主机的 IP 地址范围，与“对外映射 IP 地址”一一对应

对外映射 IP 地址：对外网映射的公网 IP 地址范围，与“内部 IP 地址”一一对应

状态：启用或禁用本规则，默认启用

提示：一次可以配置多个连续的转换 IP，但“内部 IP 地址”与“对外映射 IP 地址”的个数要相等。

10.2.3 端口映射

功能描述：

如果内网有服务器需要向 Internet 提供服务，且只提供某些端口的服务，那么就需要在网关上做端口映射。

配置路径：【防火墙】>【NAT 规则】>【端口映射】

配置描述：

第一：进入【端口映射】页面，如下图：

图 10-7 端口映射

点击<删除所有>，将删除所有的内网代理规则。

点击<删除>，删除本条规则。

点击<修改>，修改本条规则的参数，但外网口不能修改。

改变状态栏复选框的值，再点击<修改状态>，可改变规则状态(“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，新增规则，如下图

图 10-8 新增端口映射规则

当前管理员: admin
保存配置
在线客服
安全退出
设备状态
实时监控
系统配置
系统对象
网络配置
防 火 墙
安全策略
NAT规则
内网代理
一对一地址转换
端口映射
新增端口映射规则
确定
返回
规则名称
外网口
WAN1
(从该端口进出的数据流才转换)
内部地址
(单个IP, 如 192.168.5.3)
对外映射地址
外网口地址
(单个IP, 如 1.1.1.251)
协议号
TCP
UDP
内部端口
(与"对外映射端口"一一对应)
对外映射端口
(与 "内部端口" 一一对应)
状态
启用
禁用

参数说明：

外网口：连接外网的物理接口，如 WAN1、WAN2

内部地址：内网主机的 IP 地址，，与“对外映射 IP 地址”一一对应

对外映射地址：对外网映射的公网地址，与“内部 IP 地址”一一对应

协议号：需要转换的协议类型（TCP 或 UDP）

内部端口：服务器在内部网络中的端口号

对外映射端口号：提供给外网访问的端口号

状态：启用或禁用本规则，默认启用

10.2.4 服务器池

功能描述：当内网有多台服务器需要向 Internet 提供相同服务时，利用服务器池功能，可实现内部服务器之间的负载均衡和备份。

配置路径：【防火墙】>【NAT 规则】>【服务器池】

配置描述：

第一：进入【服务器池】页面，如下图：

图 10-9 服务器池

点击<删除所有>，将删除所有的服务器池规则。

点击<删除>，删除本条规则。

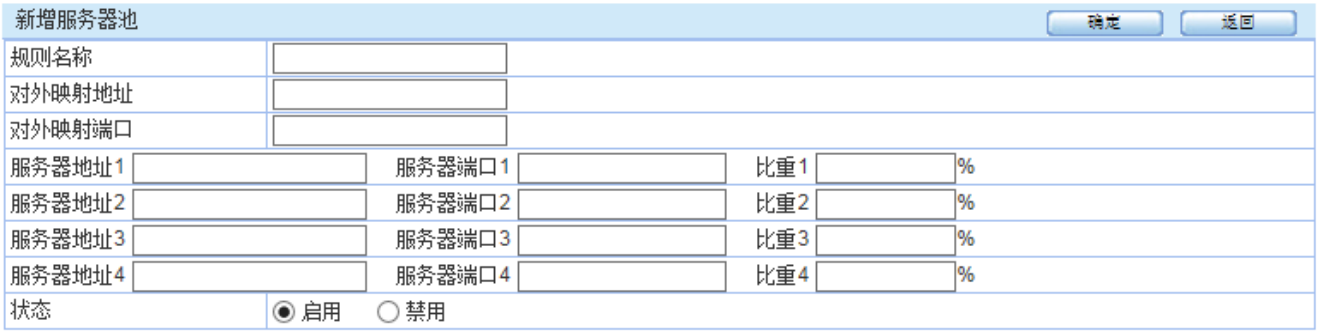
点击<修改>，修改本条规则的参数，但外网口不能修改。

点击<计数清零>，清除规则匹配计数。

改变状态栏复选框的值，再点击<修改状态>，可改变规则状态(“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，新增规则，如下图：

图 10-10 新增服务器池



参数说明：

规则名称：服务器池规则的名称；

对外映射地址：对外网映射的公网地址；

对外映射端口：提供给外网访问的端口号；

服务器地址：内部服务器的真实地址；

服务器端口：内部服务器的真实端口号；

状态：启用或禁用本规则，默认启用；

10.3防 DOS 攻击

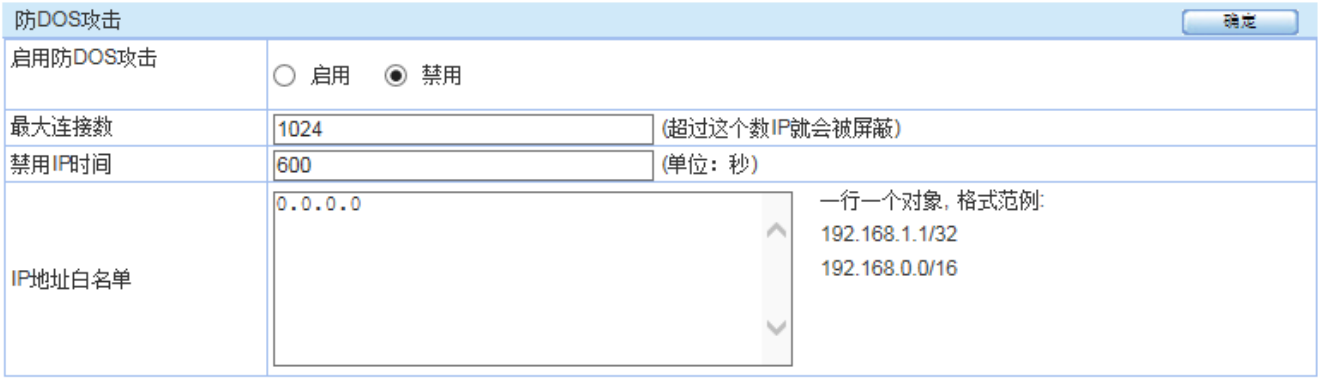
功能描述：防止某 IP 发起大量的对设备本身 TCP 连接，指对设备本身的 DDOS。

配置路径：【防火墙】>【防 DOS 攻击】

配置描述：

第一：进入【防 DOS 攻击】页面，如下图：

图 10-11 防 DOS 攻击



参数说明：

启用防 DOS 攻击：启用或禁用防 DOS 攻击功能。

最大连接数：允许单个 IP 可连接的最大 TCP 连接数，默认是 1024。当超过这个设定值时，这个 IP 地址就会被禁止连接设备。

禁用 IP 时间：当 IP 被禁用时，被禁用的时间。

IP 地址白名单：表示不受连接数限制的 IP 地址。

10.4 ARP 欺骗防护

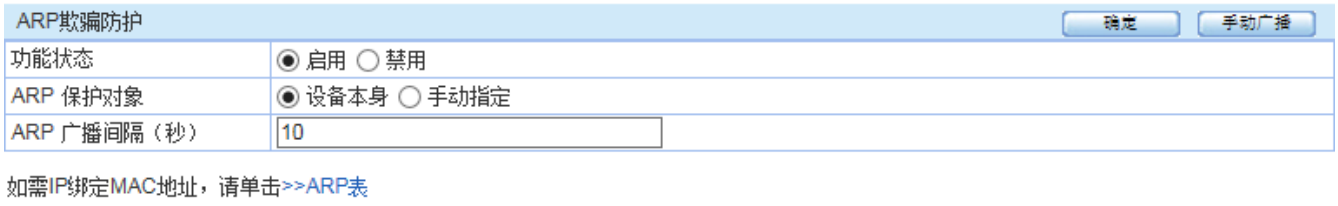
功能描述：防止设备本身或指定 IP 不受 ARP 欺骗。

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 10-12 ARP 欺骗防护



参数说明：

功能状态：启用或禁用 ARP 欺骗防护功能。

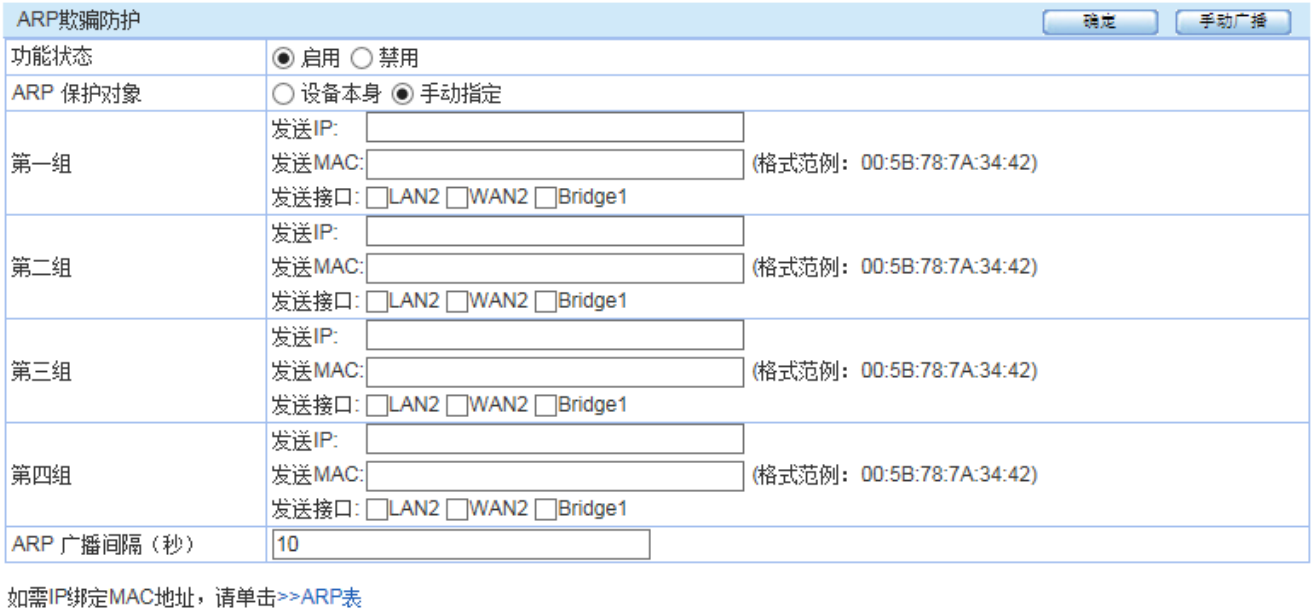
ARP 保护对象：防止被的 ARP 风暴的攻击的对象。

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 10-13 ARP 欺骗防护--手动指定



参数说明：

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

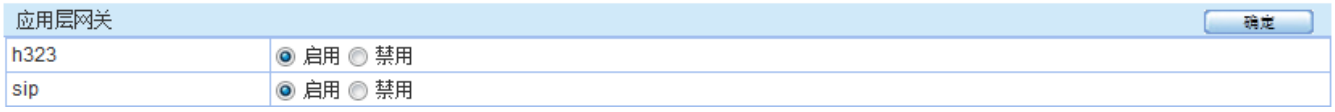
功能描述：启用或禁用应用层网关。

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 10-14 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。

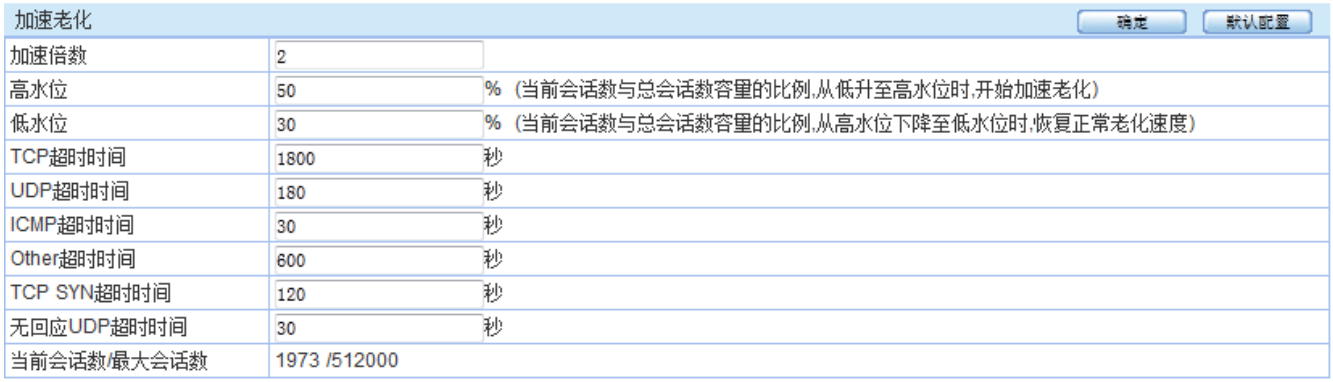
10.6 加速老化

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 10-15 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。

10.7 移动终端管理

功能描述：随着平板、手机等智能终端的流行，在无线和固网混合的网络环境下，有些公司内部员工可能自己私自拉一些无线 AP，通过无线 AP 到公司网络出口，而且这些 AP 由于安全措施薄弱，极容易被外人破解，可能导致内网暴漏，信息安全遭受威胁。无线热点发现功能能够帮助用户实现无线智能终端的管理，识别无线智能终端的接入，防范无线智能终端设备接入引起无线安全漏洞导致泄密。

。

配置路径：【防火墙】>【移动终端管理】

第一：进入【应用层网关】页面，如下图：

图 10-16 移动终端管理

参数说明：

启用移动终端管理：启用对移动终端进行管理。

发现移动终端后的行为：可选择拒绝该移动终端或是启用事件告警。

移动终端列表：显示接入的热点/移动终端的 IP、用户名、所属组以及最近发现流量等信息。无线热点发现通过流量特征来识别移动终端，如果 AP 是 NAT 模式，则显示的是热点 IP；如果是非 NAT 模式，则显示的是移动终端的 IP。

信任列表：用于添加管理员允许接入的 AP 或移动终端，对于这些 IP 或移动终端，设备不会拒绝他们上网。

提示：

1、移动终端管理只针对组织结构里面的用户/用户组生效，因此，首要事情就是把用户添加到组织结构。

2、移动终端管理仅对安卓、iPhone和iPad 做识别，暂不对其他操作系统做移动终端发现。

11 组织管理

“组织管理”包括组织结构的手动创建、批量导入、LDAP/AD 导入、扫描内网主机。

11.1 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。

11.1.1 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：【行为管理】>【组织管理】>【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 11-1 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。

11.1.2 修改根组

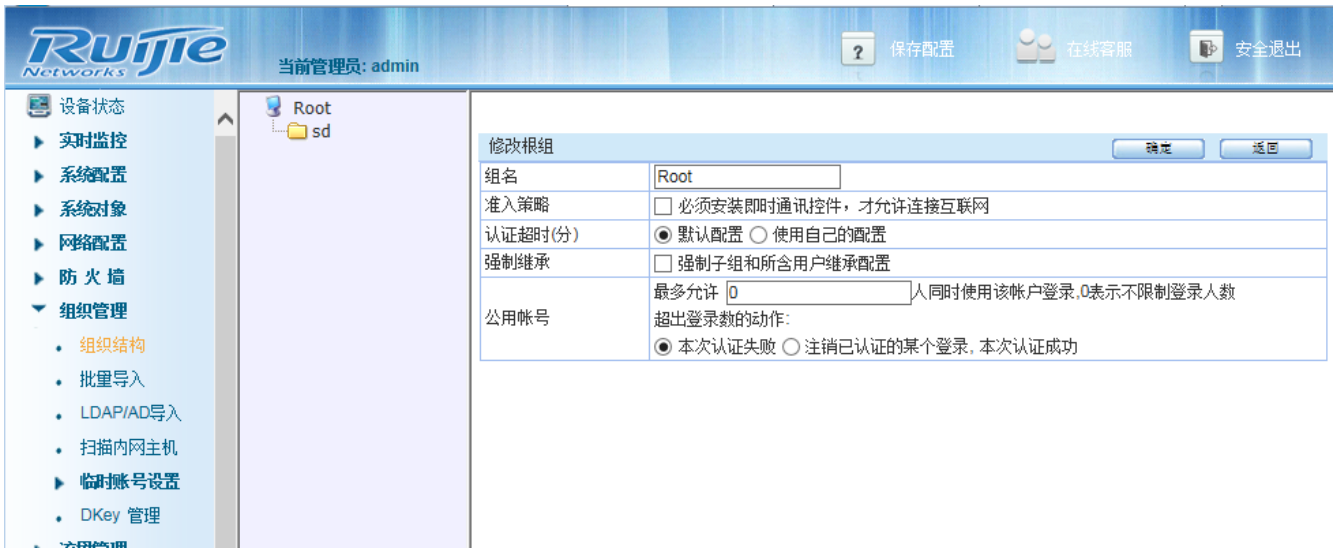
功能描述：修改根组的名称、上网策略、黑名单控制

配置路径：【行为管理】>【组织管理】>【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 11-2 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。

上网策略：引用上网策略里面已配置好的条目。默认不控制，即不对上网做任何限制。

黑名单控制：引用黑名单规则里已配置好的条目。默认不控制，即不做黑名单控制。黑名单规则配置详见 黑名单规则 部分。

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。

11.1.3 新增子组

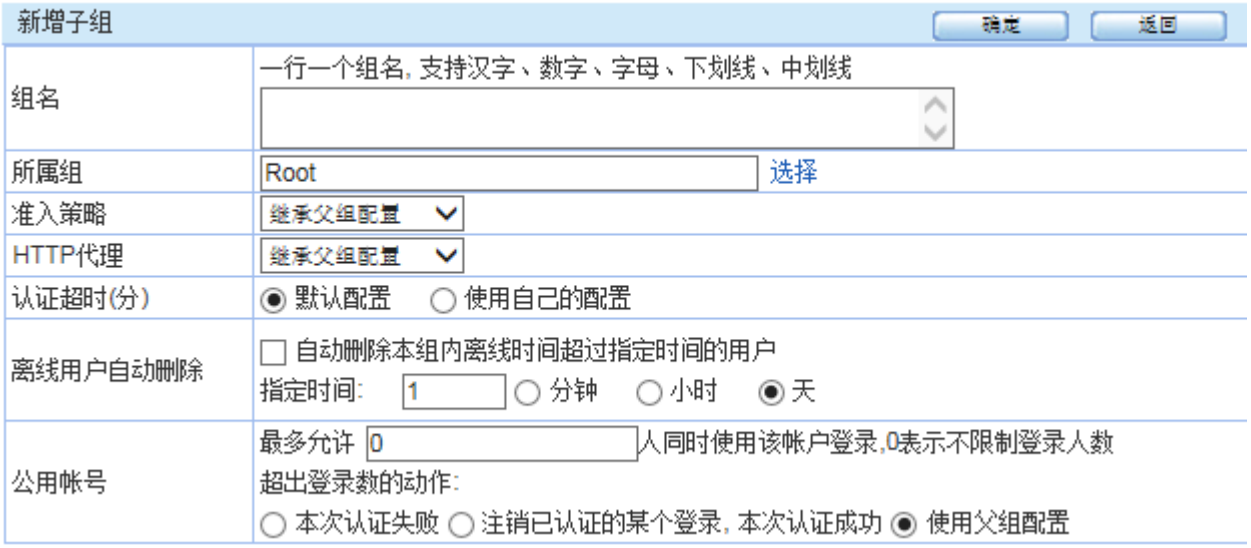
功能描述：新增子组，并设置子组的上网策略和黑名单控制

配置路径：【行为管理】>【组织管理】>【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 11-3 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。

上网策略：引用上网策略里面已配置好的条目。默认继承父组配置，也可选择自己独立的配置。

黑名单控制：引用黑名单规则里已配置好的条目。默认继承父组配置，也可选择自己独立的配置。黑名单规则配置详见 黑名单规则 部分。

准入规则：默认继承父组配置；若可选择自己独立的配置，需勾选[必须安装即时通讯控件，才允许连接互联网]。

SSL 代理：默认继承父组配置；若可选择自己独立的配置，需勾选[开启 SSL 代理]。

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，指定时间的单位可以是[分钟]、[小时]或[天]。

11.1.4 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：【行为管理】>【组织管理】>【组织结构】

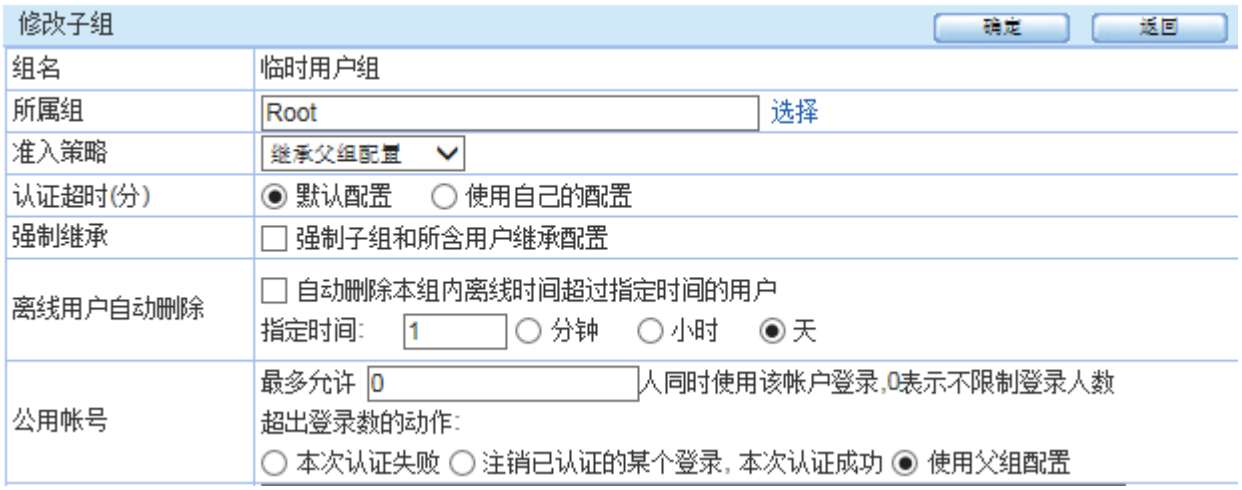
配置描述：

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 11-4 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 11-5 修改子组 2



参数说明：

组名：子组的名称，不可修改。

所属组：点击后面的<选择>按钮，出现选择用户组的框，可改变父组。

上网策略：引用上网策略里面已配置好的条目。

黑名单控制：引用黑名单规则里已配置好的条目。黑名单规则配置详见 黑名单规则 部分。

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，所含用户和子组的上网策略和黑名单控制都被修改为本组的配置。

准入规则：默认继承父组配置；若可选择自己独立的配置，需勾选[必须安装即时通讯控件，才允许连接互联网]。

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，指定时间的单位可以是[分钟]、[小时]或[天]。

11.1.5 新增普通用户

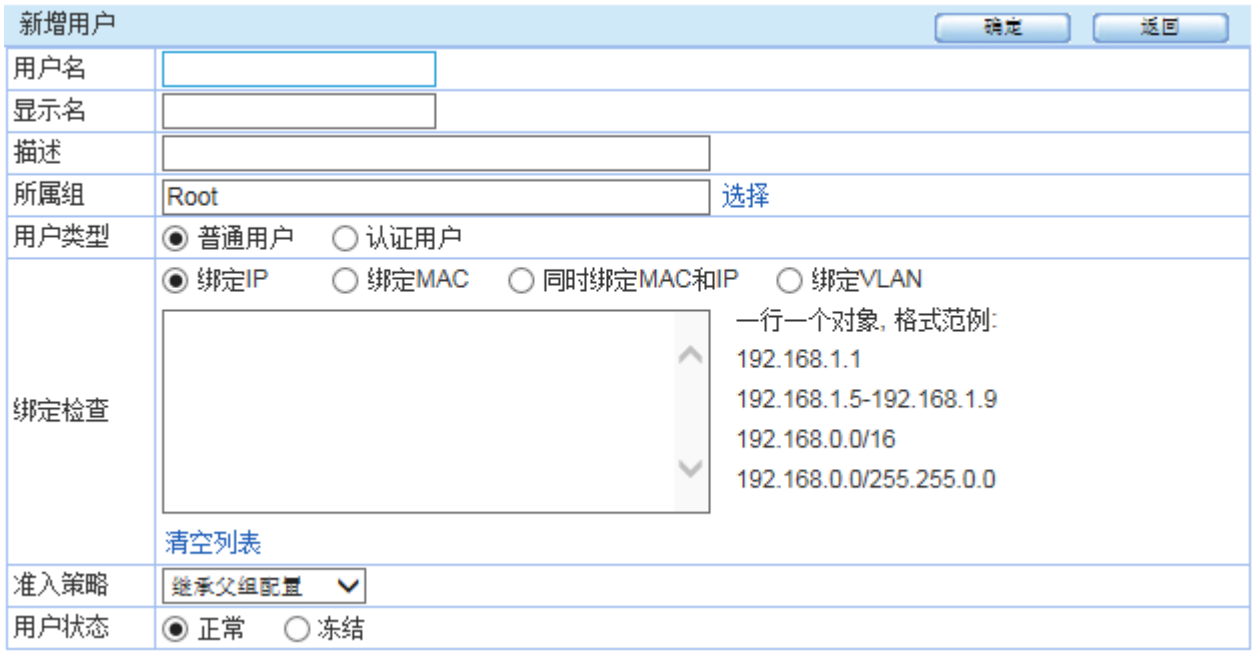
功能描述：新增普通用户，并设置子组的上网策略和黑名单控制

配置路径：【行为管理】>【组织管理】>【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 11-6 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，后面将详细描述。

上网策略：引用上网策略里面已配置好的条目。默认继承父组配置，也可选择自己独立的配置。

黑名单控制：引用黑名单规则里已配置好的条目。默认继承父组配置，也可选择自己独立的配置。黑名单规则配置详见 黑名单规则 部分。

准入规则：默认继承父组配置；若可选择自己独立的配置，需勾选[必须安装即时通讯控件，才允许连接互联网]。

SSL 代理：默认继承父组配置；若可选择自己独立的配置，需勾选[开启 SSL 代理]。

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。

11.1.6 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：【行为管理】>【组织管理】>【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 11-7 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。普通用户和认证用户的绑定含义不尽相同，后面将详细描述。

认证方式：包括本地认证、到服务器去认证。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、POP3 服务。

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

注销已认证的摸个登录，本次认证成功

使用全局缺省配置：使用全局配置的参数。路径【行为管理>认证选项>认证参数】

有效期：用户有效期，当有效期到了，就自动将该用户从设备中删除。默认为“永远有效”。

准入策略：默认继承父组配置；若可选择自己独立的配置，需勾选[必须安装即时通讯控件，才允许连接互联网]。

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。

11.1.7 修改用户

功能描述：修改用户的配置

配置路径：【行为管理】>【组织管理】>【组织结构】

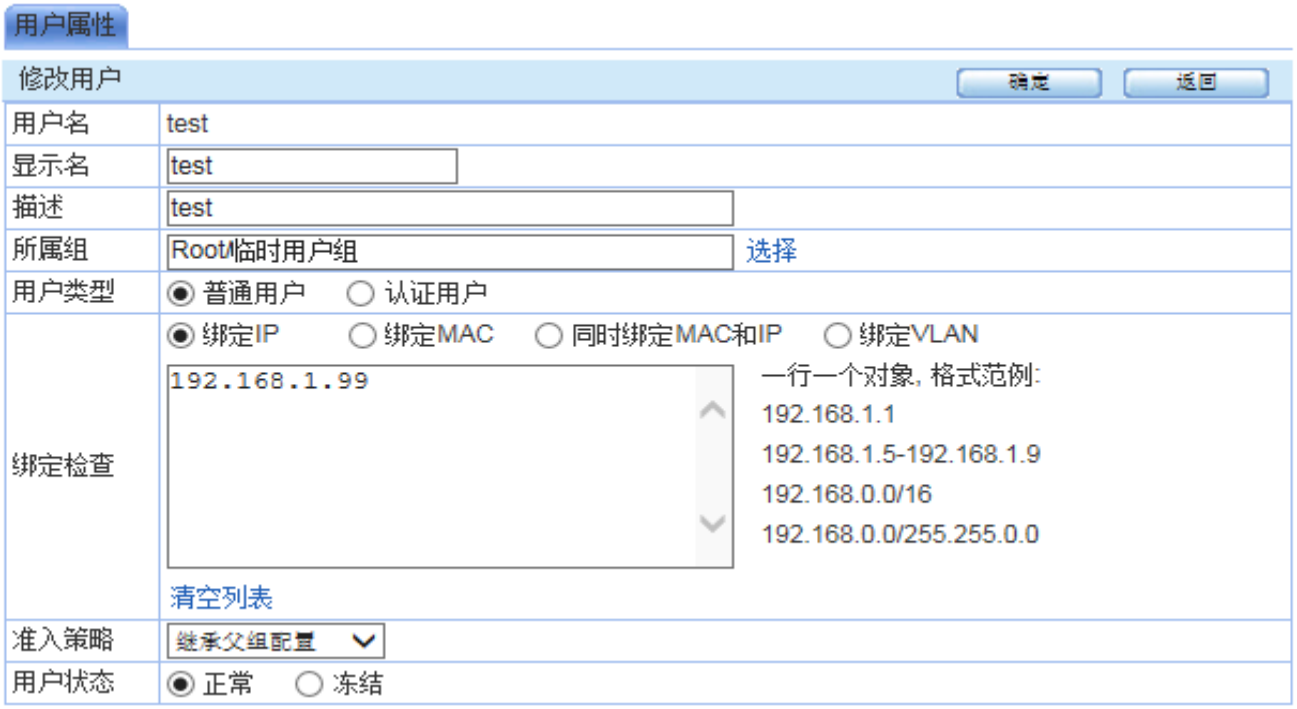
配置描述：

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 11-8 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 11-9 修改用户 2



11.1.8 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，后面将详细描述。

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。

11.1.8.1 绑定 IP

功能描述：绑定用户的 IP 地址

配置路径：【行为管理】>【组织管理】>【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 11-10 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。

11.1.8.2 绑定 MAC

功能描述：绑定用户的 MAC 地址

配置路径：【行为管理】>【组织管理】>【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：

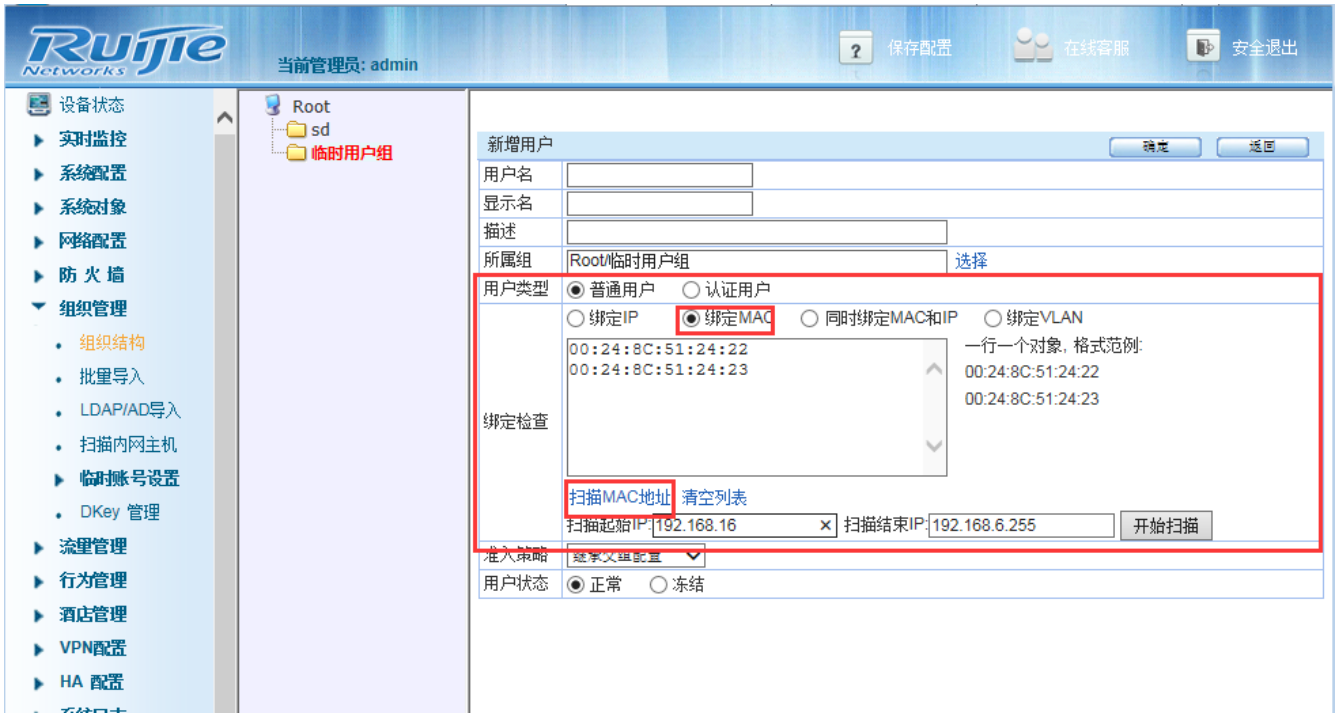
图 11-11 绑定 MAC

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：00:24:8C:51:24:22 或 00:19:e0:2b:92:c4#(172.16.3.126)，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 11-12 绑定 MAC-扫描 MAC



扫描的结构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 的一种注释。

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【行为管理>认证选项> SNMP 设置】

11.1.8.3 绑定 IP+MAC

功能描述：绑定用户的 IP 和 MAC 地址

配置路径：【行为管理】>【组织管理】>【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：

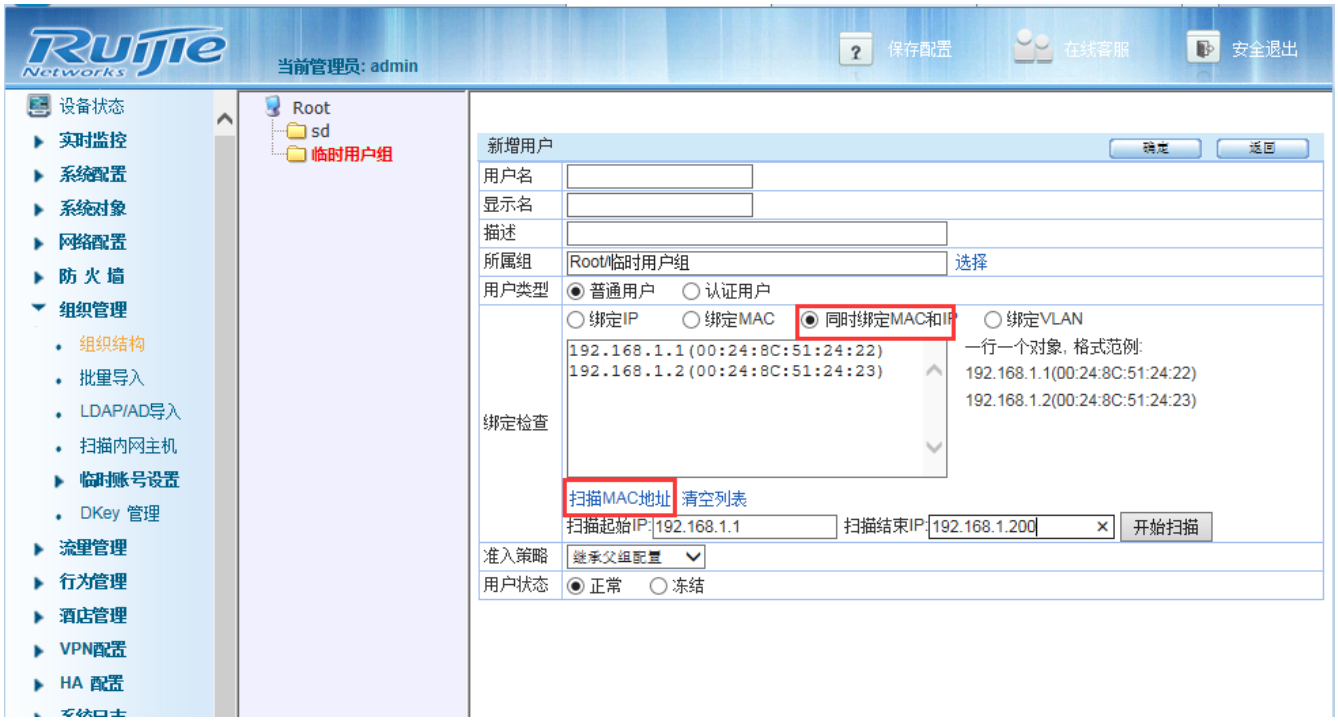
图 11-13 绑定 IP+MAC

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 192.168.1.2(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<立即扫描>按钮，即可扫描出对应 IP 的 MAC 地址。如下图：

图 11-14 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【行为管理>认证选项> SNMP 设置】

11.1.8.4 绑定 VLAN

功能描述：绑定用户的 VLAN ID

配置路径：【行为管理】>【组织管理】>【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 11-15 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。

11.1.9 导出用户和组

功能描述：导出用户和组的配置

配置路径：【行为管理】>【组织管理】>【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 11-16 导出用户和组

第二：将选中的用户和组保存到 PC。如下图：

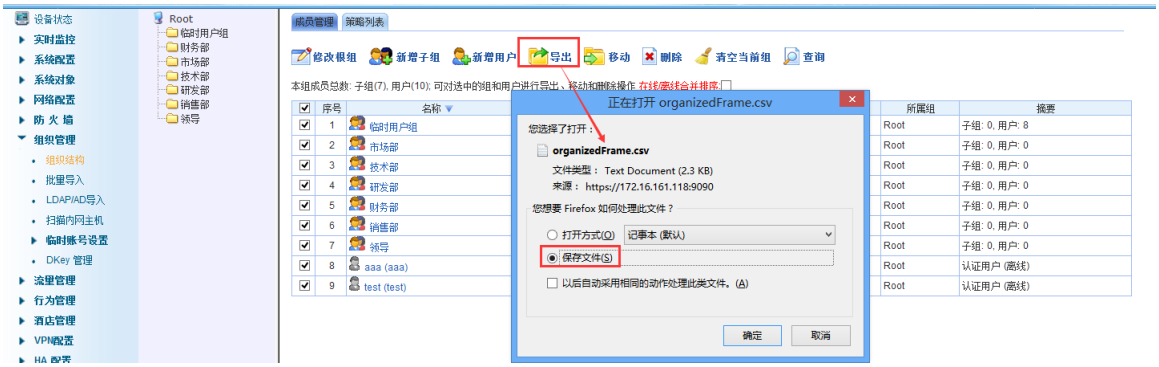


图 11-17 组织结构-导出用户和组 2

11.1.10移动用户和组

功能描述：移动用户和子组的到另外一个父组下。

配置路径：【行为管理】>【组织管理】>【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 11-18 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 11-19 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。

11.1.11 删除用户和组

功能描述：删除用户和组。

配置路径：【行为管理】>【组织管理】>【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 11-20 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。

11.1.12查询用户和组

功能描述：查询用户和组

配置路径：【行为管理】>【组织管理】>【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 11-21 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。

11.1.13在线离线合并排序

功能描述：在线离线合并排序

配置路径：【行为管理】>【组织管理】>【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 11-22 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。

11.1.14清空当前组

功能描述：清空当前组

配置路径：【行为管理】>【组织管理】>【组织结构】

配置描述：

第一：进入【组织结构】页面。如下图：

图 11-22 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

11.1.15策略列表

功能描述：策略列表

配置路径：【行为管理】>【组织管理】>【组织结构】

配置描述：

第一：进入【组织结构】页面。如下图

图 11-22 组织结构-策略列表

参数说明：

移除策略：选择 Root 中任意一组，点击<移除策略>会将属于该组下的策略删除，但是属于指定用户的策略不能被删除

查看该组策略集：选择 Root 中任意一组，点击<查看该组策略集>，可以看到所选组下的所有策略

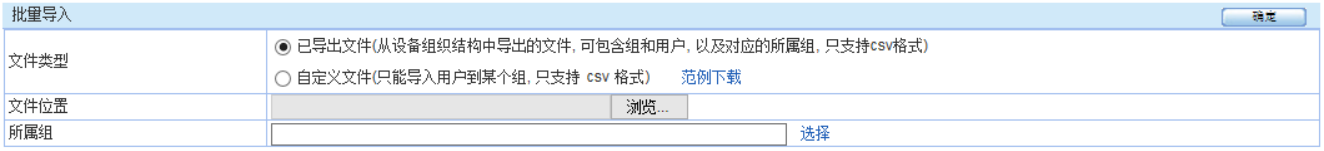
11.2批量导入

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：【行为管理】>【组织管理】>【批量导入】

配置描述：进入【批量导入】页面，如下图：

图 11-22 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，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。

11.3 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：【行为管理】>【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 11-23LDAP/AD 导入-匿名查询

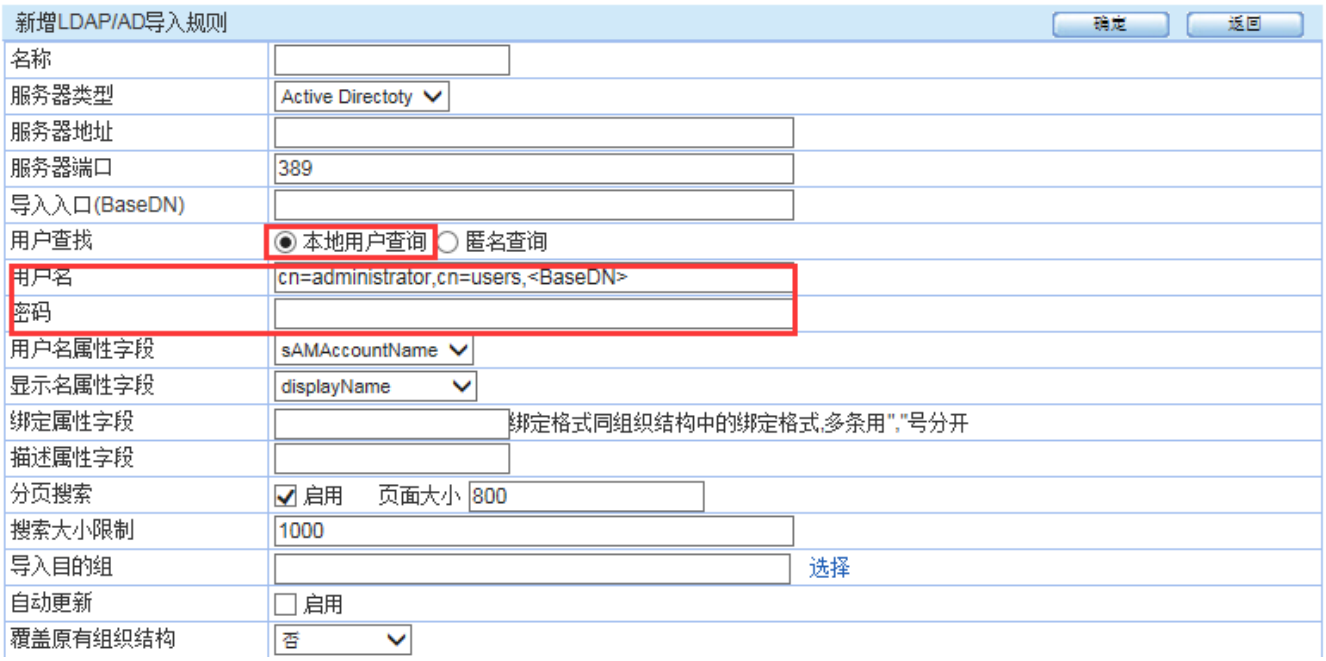
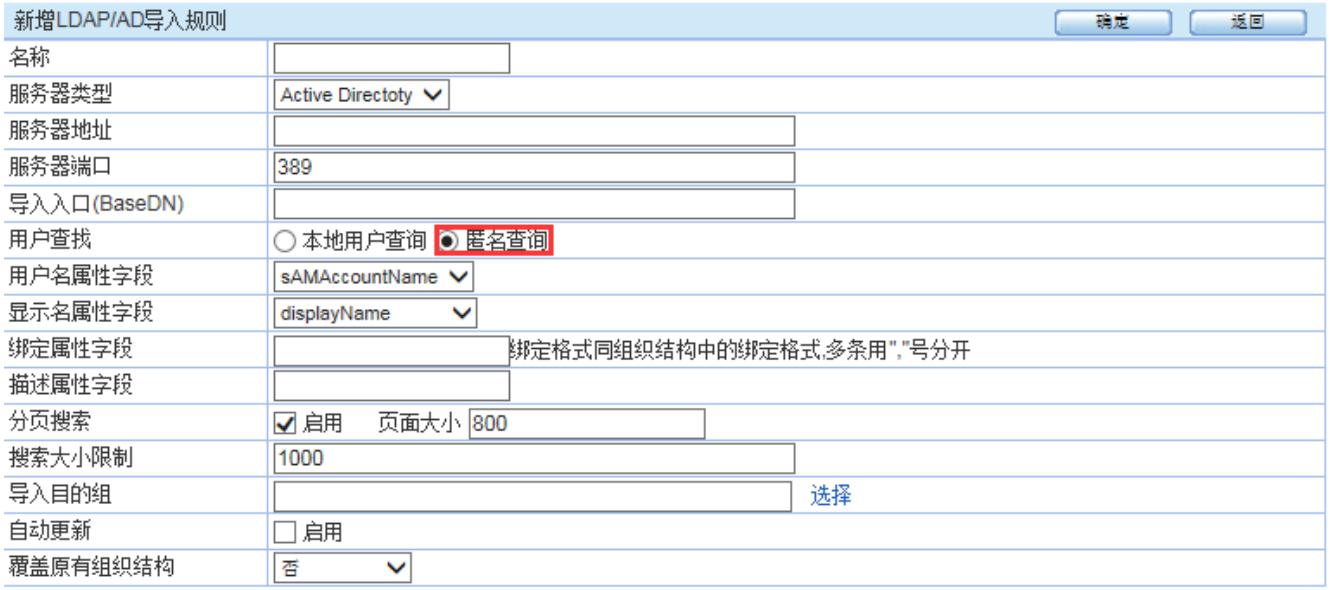


图 11-24LDAP/AD 导入-匿本地用户询



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。

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。

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。

11.4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：【行为管理】>【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 11-25 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 11-26 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>，选择所有用户的组。点击每个用户后面对应的<选择>按钮。

11.5 临时账号管理

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。

11.5.1 临时账号设置

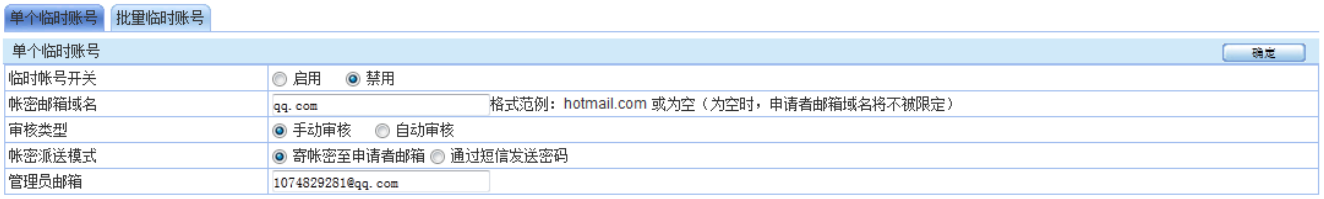
功能描述：设置临时账户的审核类型、用户组、使用期限。

配置路径：【组织管理】>【临时账号设置】

配置描述：进入【临时账号设置】配置页面，如下图：

图 11-27 临时账号设置

手动审核：



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。

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。

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，过了这个有效时间，临时账户不可用。

重点说明：配置了临时账户参数以后，还必须配置一条相关的认证策略，才能将临时账户的作用发挥出来。进入【行为管理】>认证策略】配置页面，新增认证策略，如下图：

图 11-28 新增临时用户的认证策略

参数说明：

名称：临时认证策略的名称。

IP 地址：临时用户可分配的内网地址。

认证方式：必须选择到服务器去认证，且认证服务器必须选择为[本地服务器]。

自动添加到组织结构：可不选择。

状态：选择启用。

11.5.2 批量生成

功能描述：批量生产临时帐号。

配置路径：【组织管理】>【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：

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。

11.5.3 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 11-29 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 11-30 新增临时用户的认证策略

若核定类型为自动核定，在点击【确定】并通过审批后，会弹出含有用户名和密码的提示框。用户即可用此用户名及密码进行用户认证。

若核定类型为手动核定，点击【确定】后，会弹出“等待审批”的提示框。审批通过后，用户名及密码信息将发到“联络 email”中。用户即可用此用户名及密码进行用户认证。

11.5.4 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。

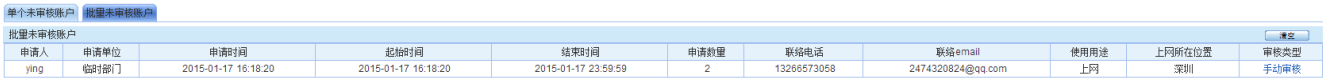
配置路径：【行为管理】>【组织结构】>【未审核账户列表】

配置描述：进入【未审核账户列表】配置页面，如下图：

图 11-31 未审核账户列表：

单个未审核账户：

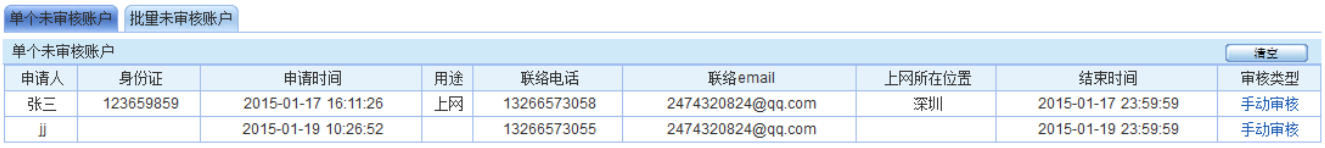
批量未审核账户：



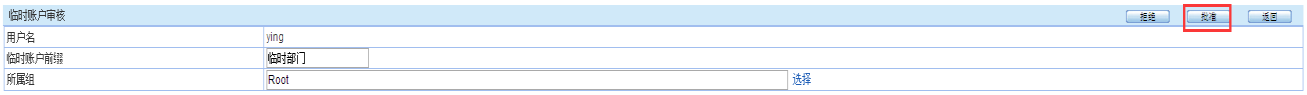
点击账户“锁定类型”栏的<手动>按钮，即可特定账户进行手动审核，如下图：

图 11-32 手动审核临时账户

单个未审核账户：



批量未审核账户：



11.5.5 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：

图 11-33 已审核账户列表

单个已审核账户：

批量已审核账户：

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。

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。

11.6 DKey 管理

DKey 管理：当用户电脑插上 DKey 后，其上网行为不会被设备监控记录。

功能描述：配置 DKey 的参数。

配置路径：【行为管理】>【组织结构】>【DKey 管理】

配置描述：

第一步：进入【DKey 管理】配置页面，点击<新增>按钮，增加 DKey。如下图：

图 11-34 新增 Dkey

参数说明：

名称：DKey 的名称。

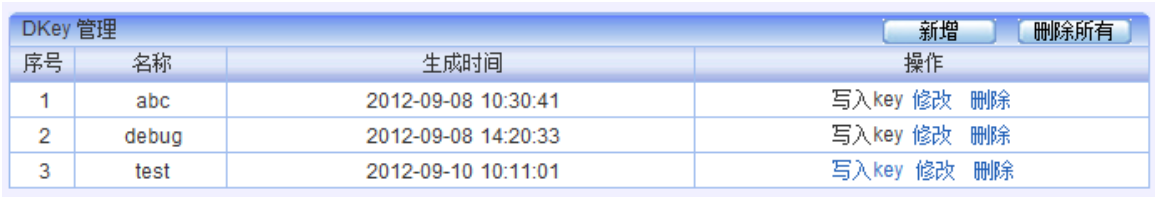
初始密码：管理员给这个 DKey 的一个初始密码，用户可在客户端修改自己的密码。

绑定 IP/MAC：选择是否绑定免监控电脑的 IP 或 MAC 地址，可绑定一个或多个 IP（或 MAC）地址，插入 DKey 的电脑满足任何一个 IP 或 MAC 地址都可以被免除监控。

IP/MAC：输入需要绑定的 IP 和 MAC 地址。

第二步：返回【DKey 管理】配置页面，点击<写入 Key>按钮，将 Key 内容写入到 DKey（USBKey）上。如下图：

图 11-35Dkey 管理



12 流量管理

“流量管理”包括线路带宽配置、基于策略的流控、基于用户的流控。

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。

基于策略的流控：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。

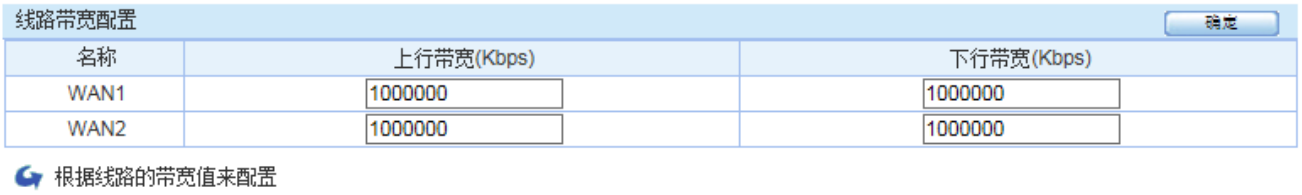
提示：三种流量控制方式同时生效，所以控制的结果是数字小的优先级高。

12.1 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 12-1 线路带宽配置



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

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

提示：要使用“基于策略的流控”，必须先配置相应的出口线路的带宽。

12.2 基于策略的流控

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、阻断流量的功能。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】>【基于策略的流控】

配置描述：

第一：进入【基于策略的流控】页面，如下图：

图 12-2 基于策略的流控

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，增加基于策略的流控规则，如下图：

图 12-3 新增策略流控规则（一级通道）

策略的匹配条件可以由以下几种条件任意组合而成：

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、选择地址簿或用户组。地址簿在【系统对象>地址簿】中配置，用户组在【组织管理>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、选择地址簿或用户组。

流控行为：选择“限制通道”，则对本规则流量做最大流量限制；选择“阻断流量”，则拒绝本规则的流量通过；选择“保障通道”，则对本规则流量做带宽保障，控制参数如下：

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。

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。

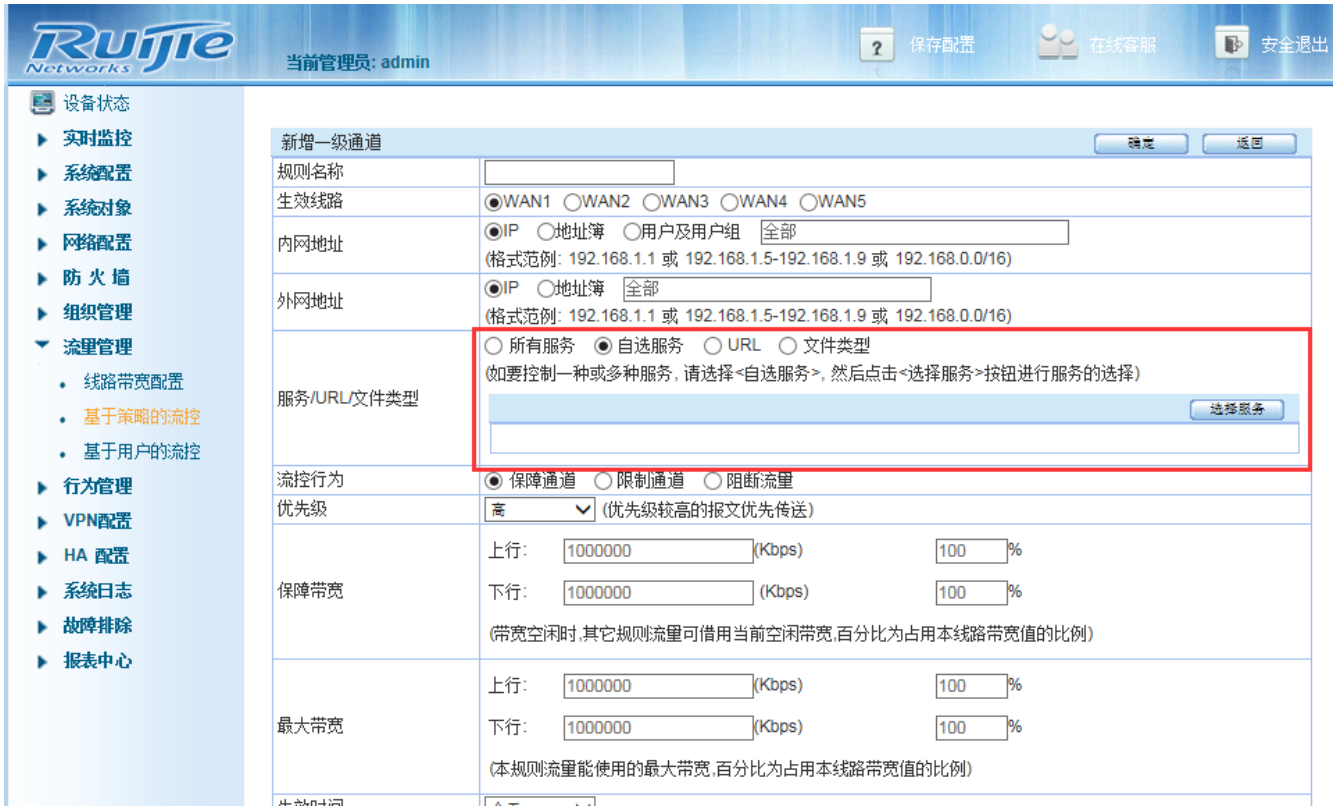
最大带宽：限制该通道最大带宽，百分比为占用本线路带宽值的比例。

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

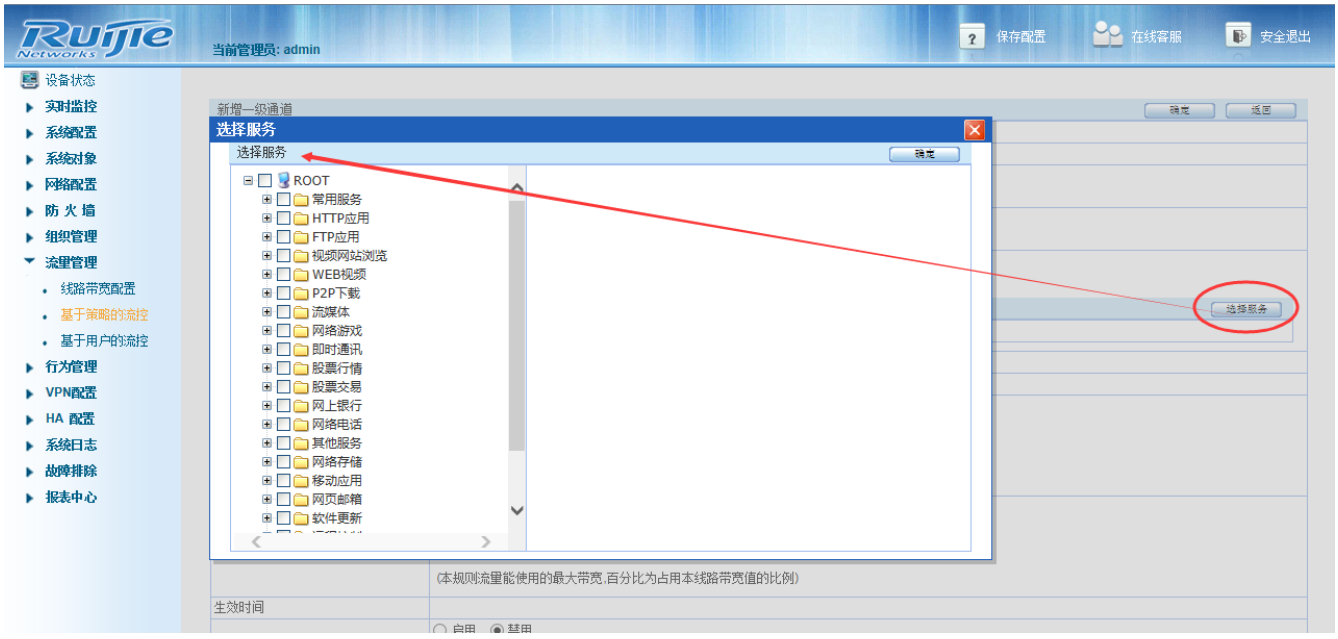
服务：默认选择“所有”，如要控制一种或多种服务，请选择<自选服务>。如下图：

图 12-4 自选服务



然后点击<选择服务>按钮，出现以下配置页面：

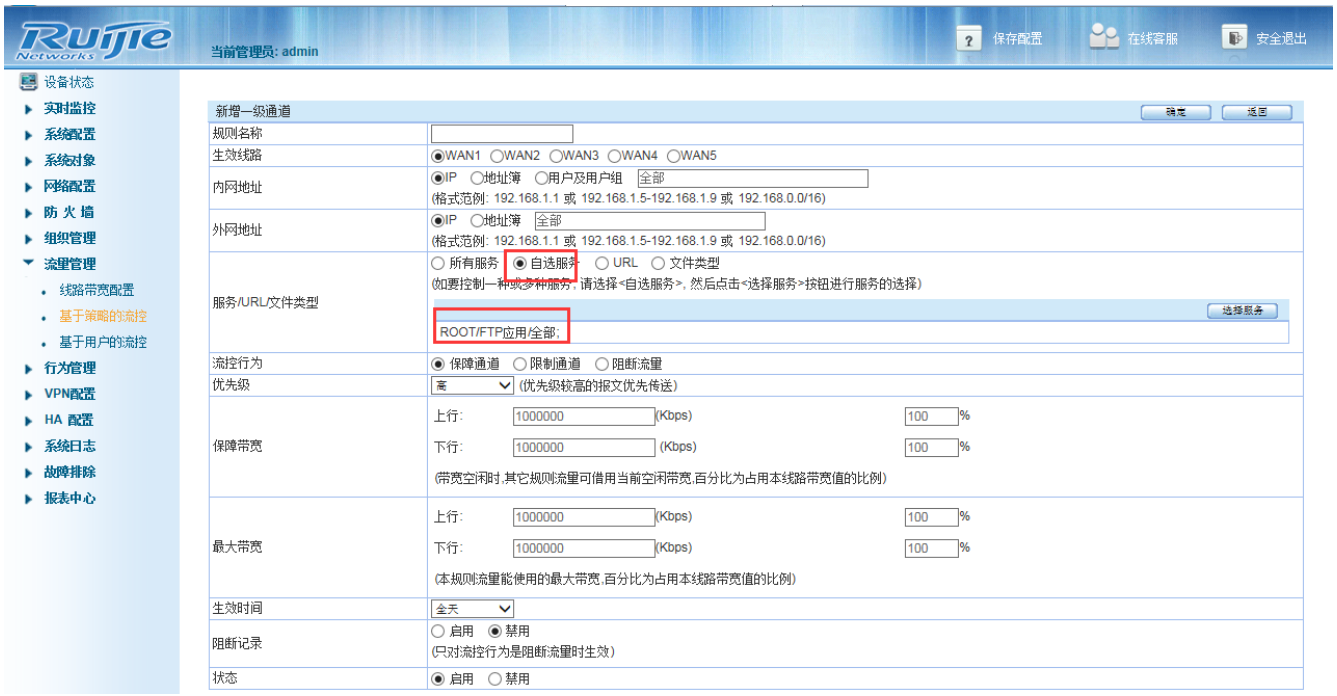
图 12-5 自选服务配置页面



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。

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

图 12-6 配置自选服务



服务：默认选择“所有”，需基于 URL 做流控，请选择<URL>。如下图：

图 12-7 配置 URL 流控

{其他操作与基于应用的流控一样}

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。

12.3 基于用户的流控

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】>【基于用户的控制】

配置描述：

第一：进入【基于用户的控制】页面，如下图：

图 12-8 基于 IP 的流控

“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 12-9 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、选择地址簿或用户组。地址簿在【系统对象>地址簿】中配置，用户组在【组织管理>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。

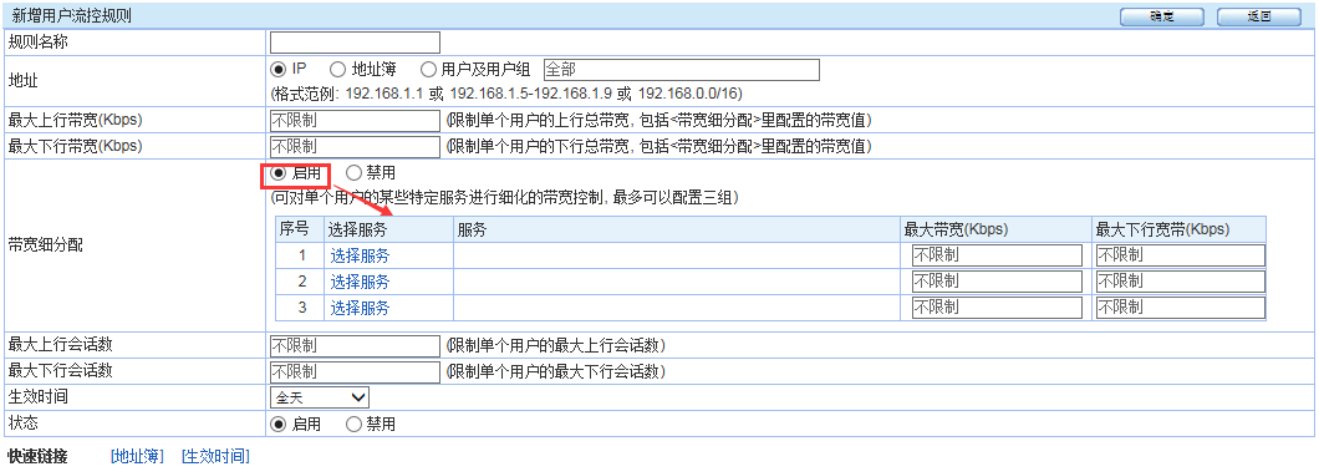
目的会话数：限制单个 IP/用户的目的会话数。

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 12-10 带宽细分配



此配置页面可以选择需要单独进行流量控制的服务，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。页面上端的“最大上行带宽”和“最大下行带宽”是控制这些选中的服务的最大带宽。再点击<确定>按钮，返回新增“新增用户流控规则”页面。

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。

13 行为管理

“行为管理”包括认证策略、上网策略、组织结构管理、认证选项、认证服务器、黑名单管理、在线用户等六部分。

13.1 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：【行为管理】>【认证策略】

配置描述：

第一：进入【认证策略】配置页面，如下图：

图 13-1 认证策略列表

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 13-2 新增认证策略 1

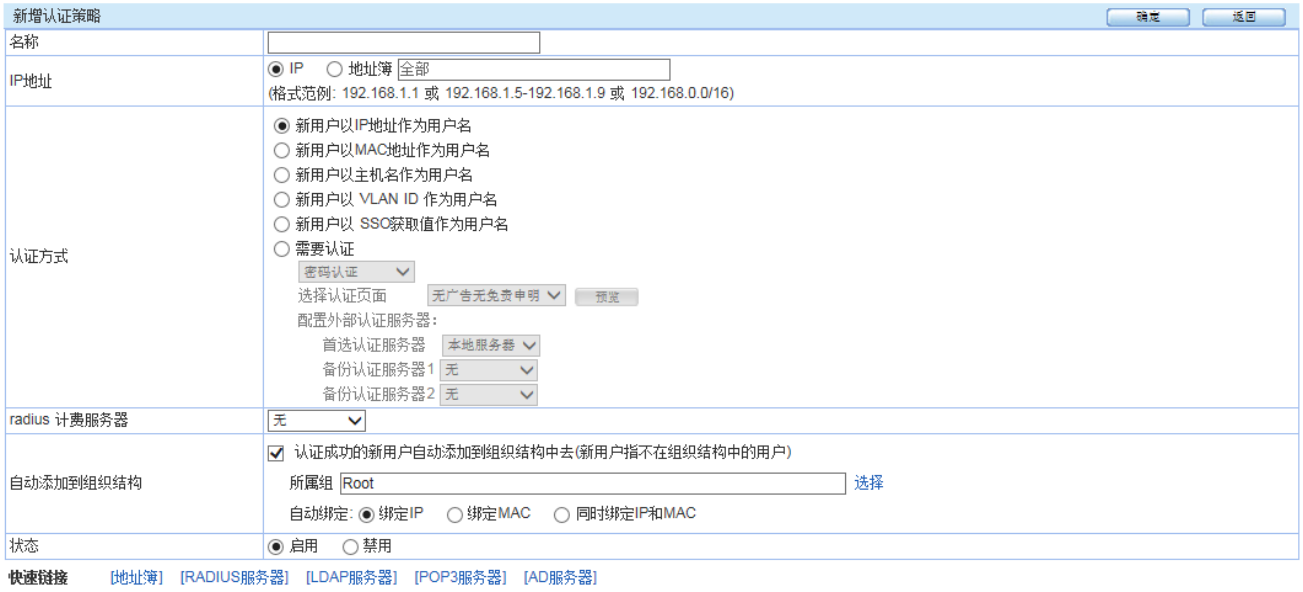
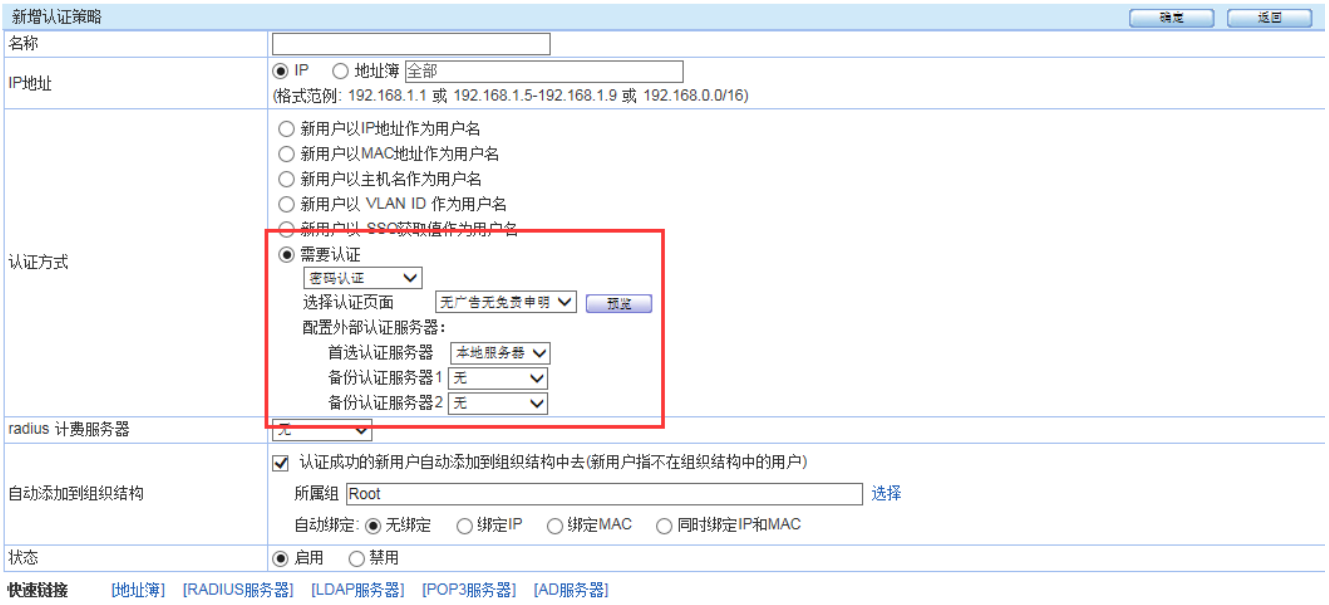


图 13-3 新增认证策略 2



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。

到服务器去认证：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。

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”。

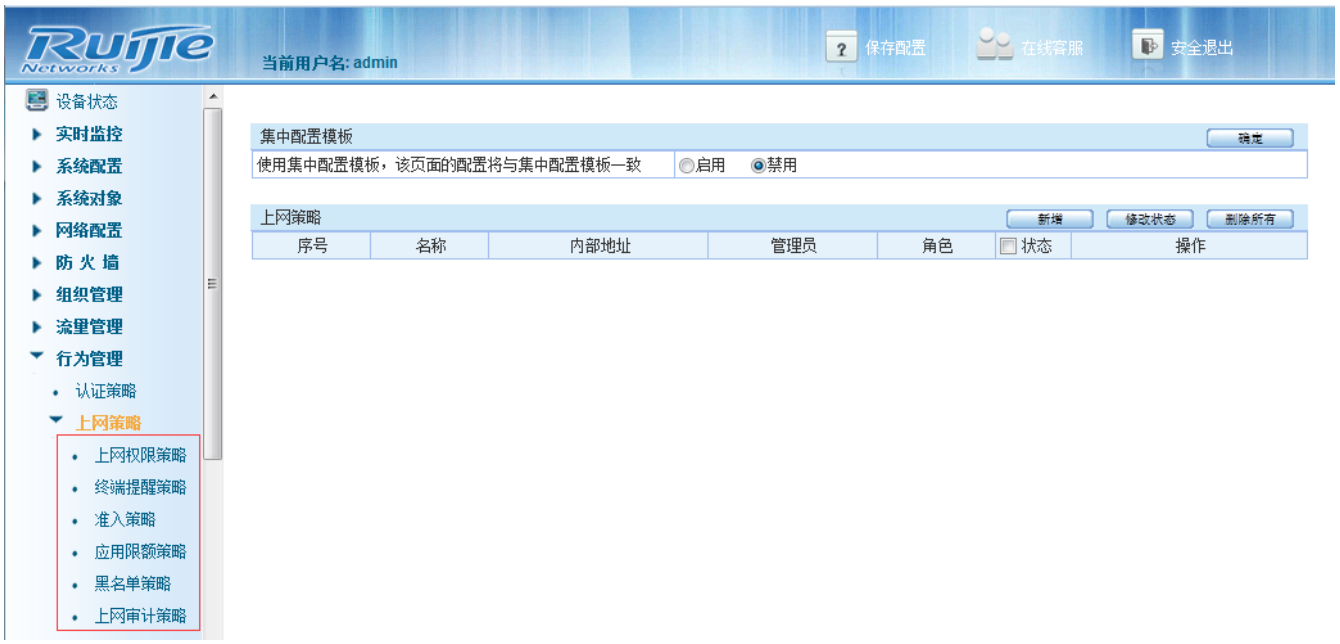
到服务器去认证：可以选择为“无绑定”、“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“无绑定”。

状态：启用或禁用本策略，默认启用。

13.2 上网策略

[上网策略]用于设置内网用户的上网策略。上网策略包括：上网权限策略、终端提醒策略、准入策略、应用限额策略、黑名单策略、上网审计策略。

图 13-4 上网策略



13.2.1 上网权限策略

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。上网策略包括：URL 过滤、关键字过滤、文件传输过滤、邮件过滤、SSL 管理和其他类。每个策略对象可以同时设置这 6 部分的内容。

配置路径：【行为管理】>【上网策略】>【上网权限策略】

配置描述：

第一：进入【上网权限策略】页面

图 13-5 上网权限策略

点击<新增>按钮，增加上网权限策略。

点击<删除所有>按钮，删除所有上网权限策略。

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 管理和其他类 6 种类型。下面详细说明：

☆URL 过滤

功能描述：对 URL 的 HTTP Get 进行过滤。

配置路径：【行为管理】>【上网策略】>【上网权限策略】

配置描述：

第一：进入【上网权限策略】页面，点击<新增>按钮，增加上网策略。

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 13-5 上网策略-增加上网策略

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>URL 库】页面定义的，可以通过<移动>和<插入>来调整 URL 条目的顺序。

关

☆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。

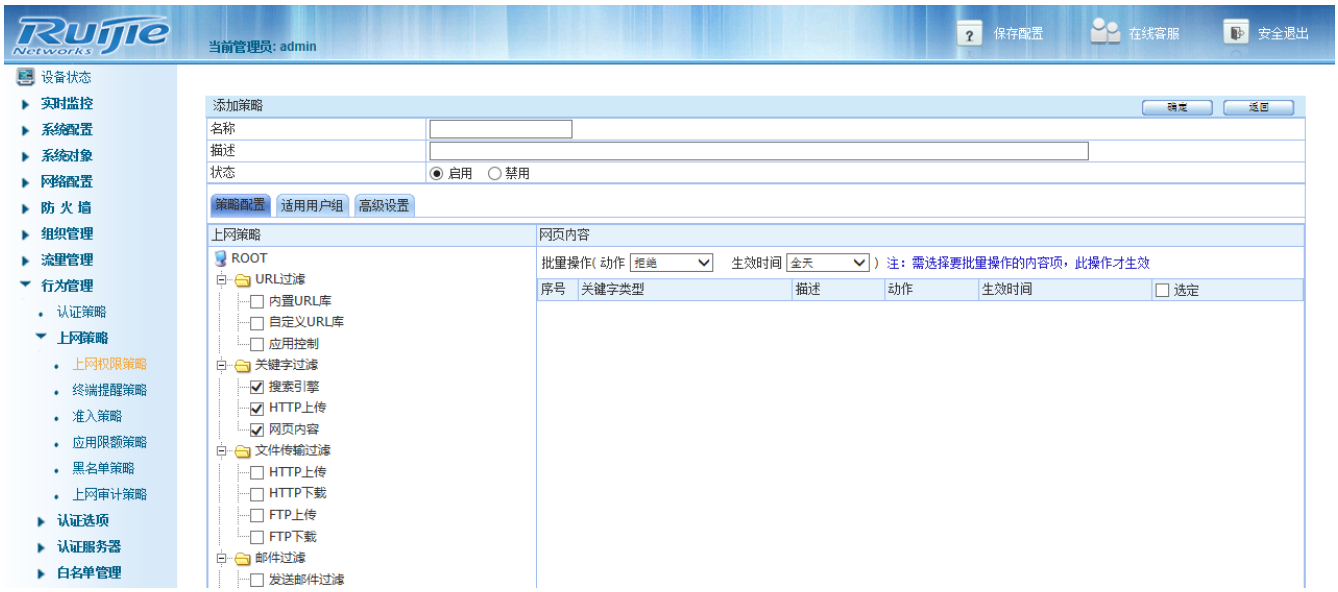
配置路径：【行为管理】>【上网策略】>【上网权限策略】

配置描述：

第一：进入【上网权限策略】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：

图 13-6 上网策略-关键字过滤-搜索引擎



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

图 13-7 上网策略-关键字过滤-发帖内容

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。

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。

☆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

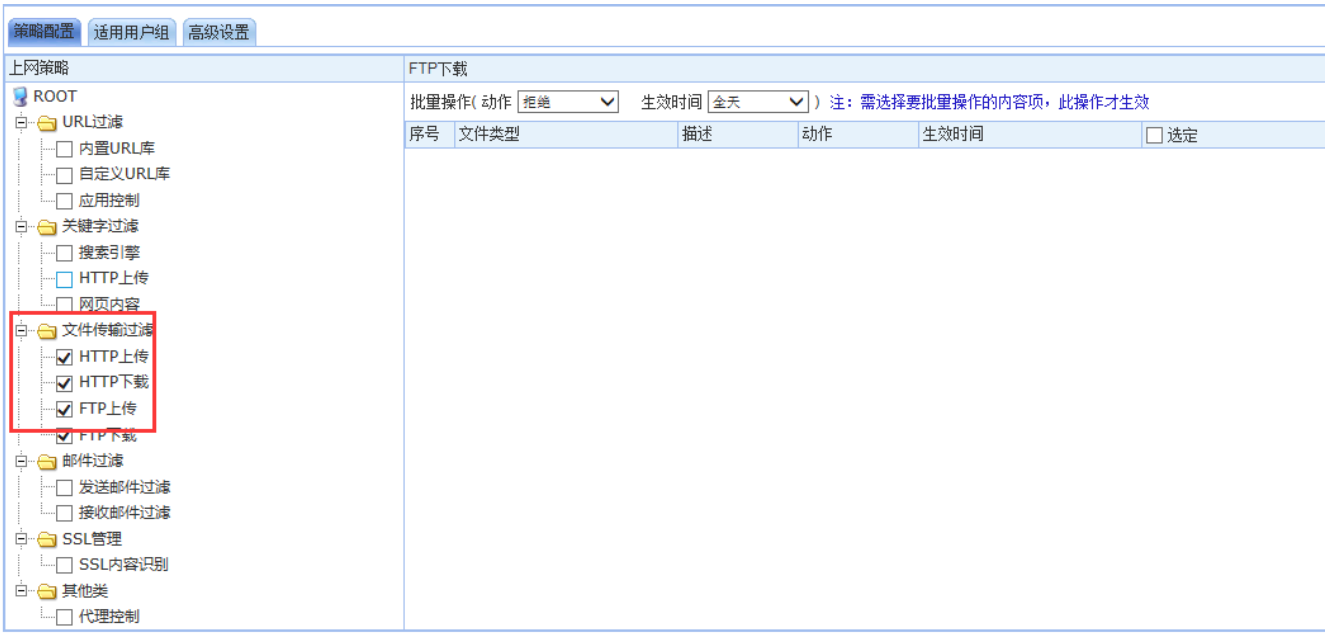
配置路径：【行为管理】>【上网策略】>【上网权限策略】

配置描述：

第一：进入【上网权限策略】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 13-8 上网权限策略-文件传输过滤



<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。

☆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：【行为管理】>【上网策略】>【上网权限策略】

配置描述：进入【上网权限策略】页面，点击<新增>按钮，增加上网策略。选择“发送邮件过滤”选项卡，配置过滤条件。如下图：

图 13-9 上网权限策略-发送邮件过滤

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：【行为管理】>【上网策略】>【上网权限策略】

配置描述：进入【上网权限策略】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 13-10 上网权限策略-接收邮件过滤

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：

3、 如某个过滤条件未配置任何值，则不检查此项内容。

4、 <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。

☆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：配置路径：【行为管理】>【上网策略】>【上网权限策略】

配置描述：进入【上网权限策略】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 13-11 上网权限策略-SSL 内容识别

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。

☆其他类

功能描述：针对使用 HTTP 代理、Sock 代理，和在 HTTP 协议与 SSL 协议标准端口是其他协议的行为进行控制。

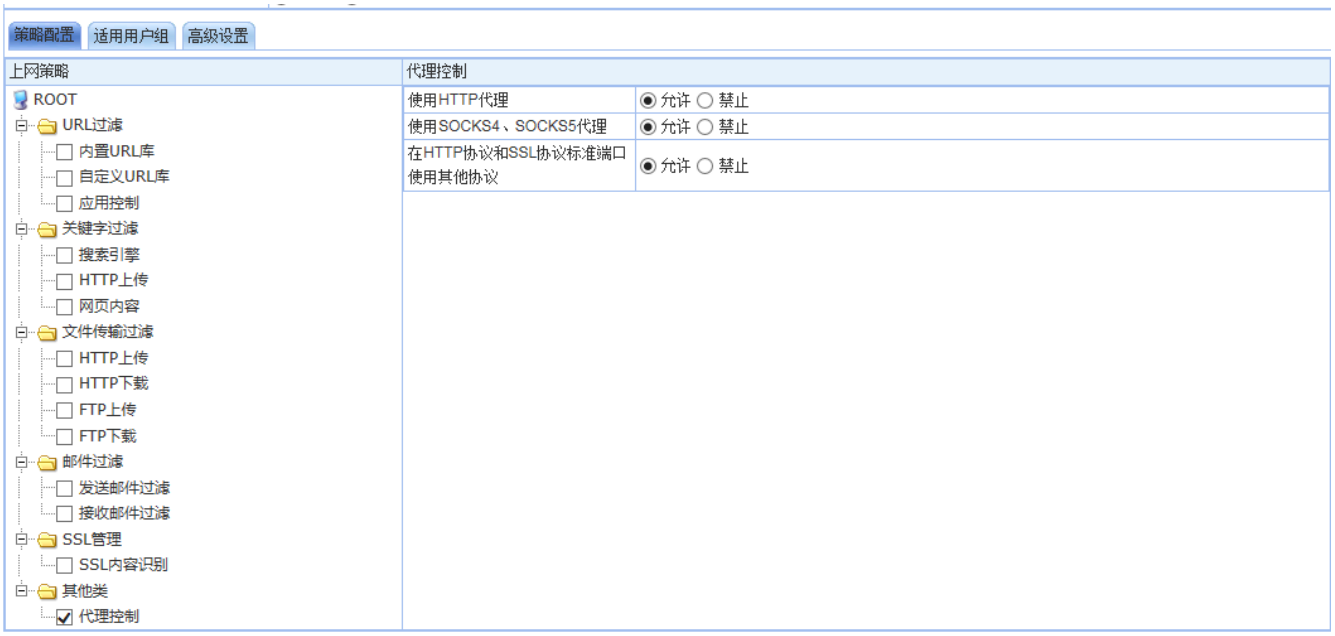
配置路径：【行为管理】>【上网策略】>【上网权限策略】

配置描述：

第一：进入【上网权限策略】页面，点击<新增>按钮，增加上网策略。

第二：选择“代理控制”选项卡，选择代理控制的选项。配置界面如下图：

图 13-11 新增上网策略-代理控制



参数说明：

使用 HTTP 代理：针对的是内网使用 HTTP 代理方式上网的行为，如果内网需要禁止用户使用此类代理，则勾选[禁止]，反之则勾选[允许]。

使用 SOCK4、SOCK5 代理：针对内网使用 SOCK 代理方式上网的行为，如果内网需要禁止用户使用此类代理，则勾选[禁止]，反之则勾选[允许]。

在 HTTP 协议和 SSL 协议标准端口使用其他协议：针对一些已知或未知的软件为了能够顺利的通过前面的防火墙，会选择常用知名端口（TCP80、TCP443）来通讯，但是通讯的内容是其私有协议格式，比如 QQ 是通过 SSL 进行登录。如果内网需要禁止用户使用非标准协议进行通信，则勾选[禁止]，反之则勾选[允许]。

13.2.2 终端提醒策略

功能描述：定期把 HTTP 流量重定向到指定的公告页面地址，从而把公告信息通过浏览器传送给终端用户。

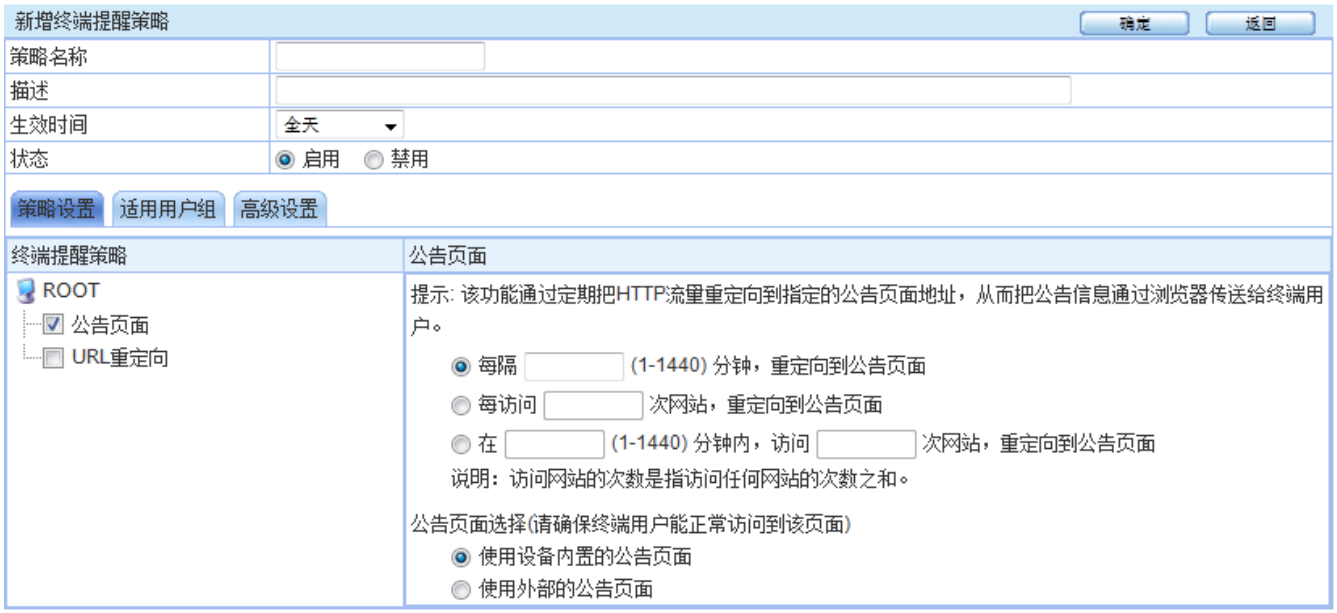
配置路径：【行为管理】>【上网策略】>【终端提醒策略】

配置描述：

第一：进入【终端提醒策略】页面，点击<新增>按钮，增加终端提醒策略。

第二：选择“终端提醒策略”选项卡。勾选需要进行控制的终端提醒规则的“选定”复选框，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。

图 13-12 新增上网策略--终端提醒策略



参数说明：

公告页面：选择每隔多长时间，每访问多少次网站以及在多少分钟内访问多少次网站之后，页面跳转到公告页面。公告页面可选择内置的公告页面，也可以使用外部自定义的公告页面。

URL 重定向：可自定义一个或多个 URL 被重定向到自定义的特定页面。

13.2.3 准入策略

功能描述：通过安装在客户端的一个准入程序，实现对内网电脑运行的进程进行检测，并限制进程的运行状态。

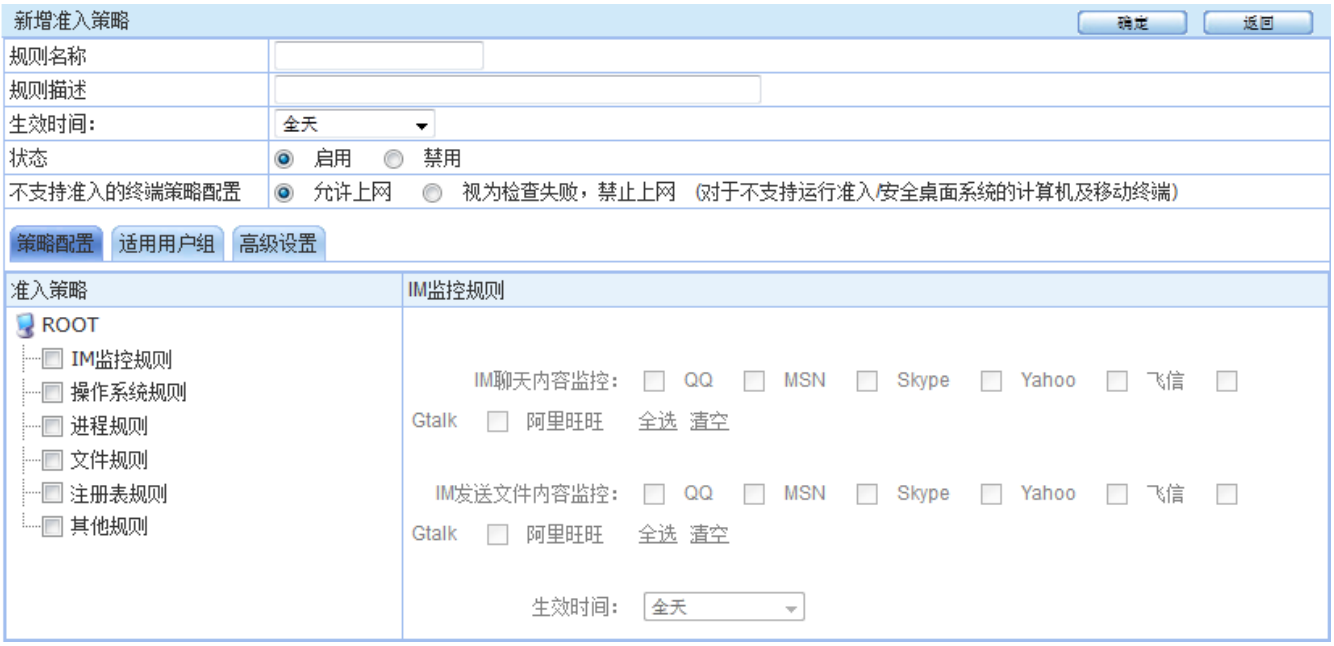
配置路径：【行为管理】>【上网策略】>【准入策略】

配置描述：

第一：进入【准入策略】页面，点击<新增>按钮，增加准入策略。

第二：选择“准入规则”选项卡。勾选需要进行控制的准入规则的“选定”复选框，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 13-13 新增上网策略--准入规则



备注：需要先定义准入规则库

参数说明：

IM 监控规则：通过安装在客户端的一个准入程序，监控 IM 聊天内容。比如：QQ、Skype、阿里旺旺等。

操作系统规则：只允许勾选的操作系统上网。否则禁止用户上网或发送日志。

进程规则：匹配进程的基本参数，包括进程名称、窗口名称、进程路径、进程状态、程序 MD5 值和程序大小，禁止用户上网或是禁止进程。

文件规则：匹配文件的基本内容，包括文件路径、文件状态、文件 MD5 值、文件大小以及更新日期，禁止用户上网或是删除文件。

注册表规则：匹配注册表的基本内容，包括注册表项、表项名称、表项数据以及表项状态，禁止用户上网或是删除注册表项。

13.2.4 应用限额策略

功能描述：针对用户每天的上网行为进行时长和流量的控制。

配置路径：【行为管理】>【上网策略】>【应用限额策略】

配置描述：

第一：进入【应用限额策略】页面，点击<新增>按钮，增加上网策略。

第二：对用户进行相应的策略配置，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 13-14 新增上网策略--应用限额策略

参数说明：

每日限额：每天允许上网的最大时长或者最高流量。

服务：对用户的何种应用服务进行限额。

每天登录次数：每天允许登录的次数。

单次在线时长：单次登录在线的时间，以分钟为单位。

提示：

1、查看用户是否违反应用限额规则，在【实时监控>应用限额用户】中查看。

13.2.5 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：【行为管理】>【上网策略】>【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 13-15 新增上网策略--黑名单策略

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、先定义黑名单规则，然后需在【行为管理>组织管理>组织结构】的用户和子组中引用黑名单规则。

3、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。

13.2.6 上网审计策略

功能描述：针对用户的上网行为进行审计。

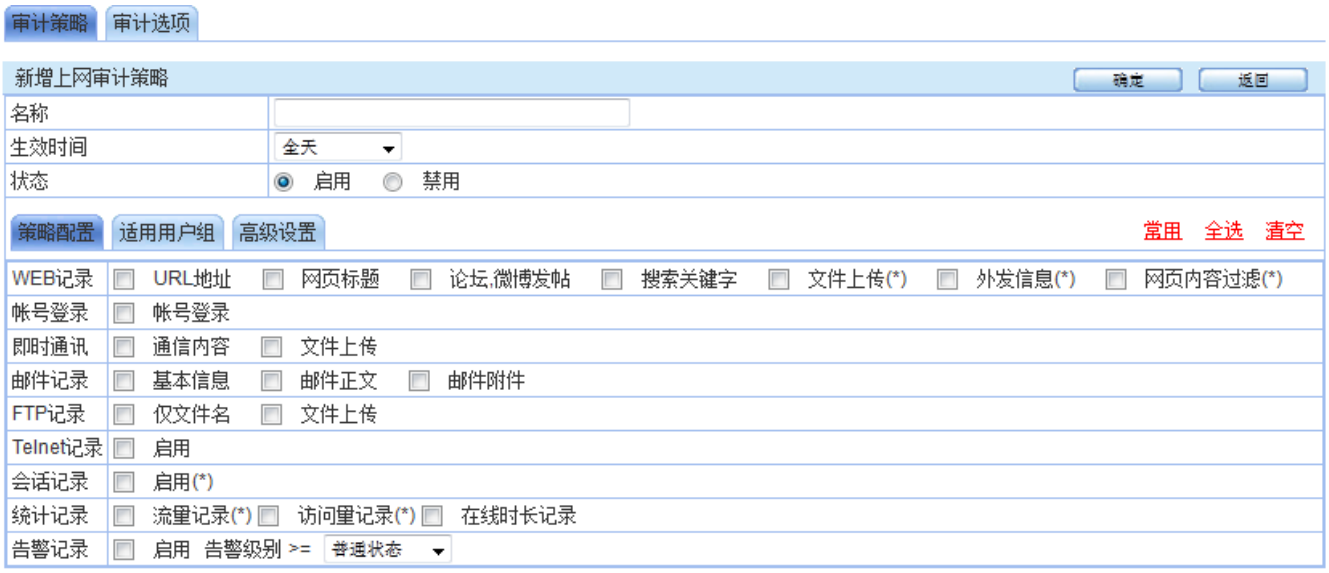
配置路径：【行为管理】>【上网策略】>【上网审计策略】

配置描述：

第一：进入【上网审计策略】页面，点击<新增>按钮，增加上网审计策略。

第二：选择“上网审计策略”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、账号登录记录、即时通讯记录、邮件记录、FTP 记录、Telnet 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“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 13-16 新增上网策略--上网审计策略



13.3认证选项

认证选项包含 跨三层 MAC 识别、认证参数和未认证权限、自定义认证画面、SSO 的配置。

13.3.1 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：【行为管理】>【认证选项】>【SNMP 设置】，配置页面如下：

图 13-13 配置跨 3 层 mac 识别

参数说明：

功能状态：选择<启用>或<禁用>开启或关闭“SNMP 设置”功能。当跨三层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 128 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，三层交换机必须开启 SNMP 服务，且正确配置三层交换机的 Community 和 SNMP 版本（版本为 v2）

2.内网如有多台交换机，配置如下：比如，在内网有 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。

13.3.2 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：【行为管理】>【认证选项】>【认证参数】，配置页面如下：

图 13-13 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。

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：启用，指定每天强制注所有用户的时间。

关闭登录页面退出登录：关闭认证成功界面即为注销认证。

认证页面欢迎语：自定义认证界面欢迎语，默认是“用户身份认证系统” 。

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。

13.3.3 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：【行为管理】>【认证选项】>【自定义认证页面】，配置页面如下：

图 13-14 自定义认证页面

参数说明：

定制对象：目前只有[WEB 认证]

页面编辑：根据需要，对认证页面相关的代码进行编辑，将达到您想要的效果。为简单期间，建议只修改图片和文字描述信息。

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。

预览：可以选择电脑效果和手机效果，其中电脑效果包括：口令认证、短信认证、短信认证/口令认证。手机效果包括：口令认证、短信认证、微信认证、短信认证/口令认证、微信认证/口令认证、短信认证/微信认证。

修改：根据需要，对认证页面的 logo、广告页面及公告内容进行编辑。

复制：对系统默认的页面进行复制后，与原有的参数进行对比并且修改，可达到您所需要的效果。

13.3.4 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：

图 13-15 未认证权限策略

点击<删除所有>，将删除所有的策略。

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 13-16 新增策略

参数说明：

流量方向：代表数据流的方向，例如：LAN->WAN1。

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>地址簿】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：数据流的服务类型。

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。

13.3.5 SSO

SSO(单点登录)指如果用户的网络中已经部署有身份认证系统，则本系统可以跟这些身份认证系统进行结合，以识别出某个 IP 地址上目前正在使用的用户 ,用户上网时不会再要求先输入用户名/密码 ,降低对上网用户的影响。包括 AD SSO、PPPOE SSO、WEB SSO、第三方设备 SSO、http 单点登录接口、SSO 镜像设置 等。

13.3.5.1 AD SSO

配置描述：AD SSO-单点登录一般适用于客户网络中已经采用 AD 域认证，希望通过 AD 域认证之后，自动通过设备认证，并且设备能获取到用户对应的域用户名，对用户进行控制和审计。域单点登录可以采用域脚本下发、浏览器强制下载身份认证工具方式或监听登录域的数据包三种方式实现。

配置路径：【行为管理】>【认证选项】>【SSO】，选择 [AD SSO]选项卡，如下图：

图 13-18 AD SSO

参数说明：

启用 AD SSO:域登录脚本方式：勾选后表示开启 AD SSO 功能，且设备作为在线方式，对用户进行 AD 域认证。适用于域脚本下发方式。

域服务器：可选择认证的 AD 域服务器或者不设定， 如果在【组织结构>LDAP/AD 导入】界面尚未导入 AD 域组织结构，但同时期望获取用户的“显示名”来统计各项数据的情况，需设定一个 AD 服务器；否则选择[不设定]。

启用 AD SSO：监听计算机登录域的数据，获取登录信息：勾选后表示开启 AD SSO 功能，设备不对用户进行 AD 域认证，即对于用户登录域的数据包不经过设备的情况，则需要把登录数据包镜像到设备。在"SSO 镜像设置"中启用镜像功能。

启用 AD SSO 功能：启用集成 windows 身份认证：勾选后表示开启 AD SSO 功能，设备开启” AD 启用集成 windows 身份验证” 认证方式 ,没有登录域的时候 ,浏览器会强制下载身份认证工具。这种情况将要求客户端计算机及设备本身都加入 Active Directory 域。

计算机名称：设备的系统名称

IP 地址：AD 服务器 IP 地址。

AD 域名：域控制器域名，例如 abc.com。

域账号：AD 域中的一个合法账号。

域账号密码：该用户在 AD 服务器中的密码。

13.3.5.2 PPPOE SSO

配置描述：PPPoE 单点登录一般适用于客户网络中已经采用 PPPoE 方式做认证，希望通过 PPPoE 认证之后，自动通过设备认证，且设备上的用户和 PPPoE 拨号账户名对应。适用于 PPPoE 服务器在外网的环境。数据流的大致过程如下：

1）PPPoE 客户端向 PPPoE 服务器发起认证或注销请求。

2）设备监听 PPPoE 通信数据包，提取出用户名做认证或注销

配置路径：【行为管理】>【认证选项】>【SSO】，选择 [PPPOE SSO]，开启 PPPOE SSO 功能。如下图：

图 13-19 PPPOE SSO

PC 通过 PPPoE 服务器的认证后，即可通过设备认证上网。

13.3.5.3 WEB SSO

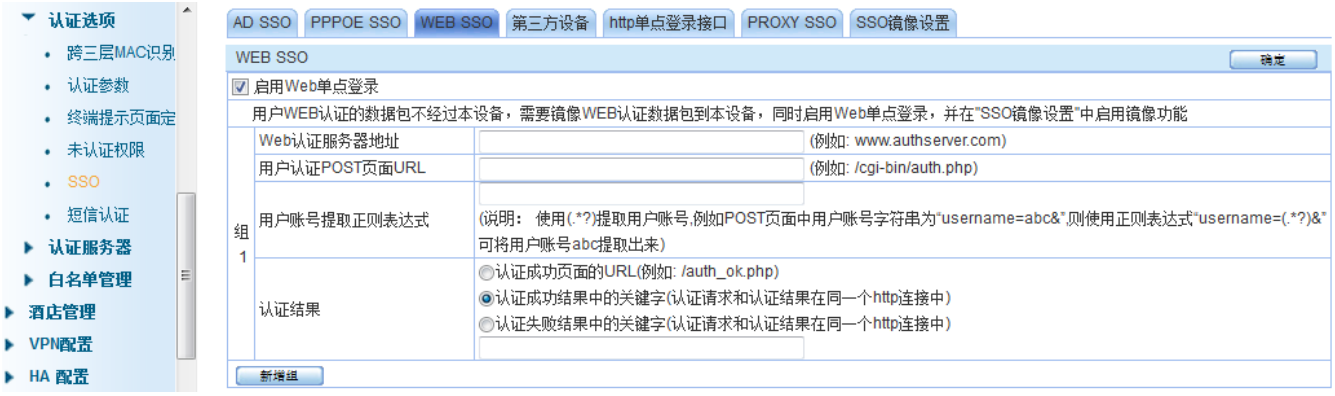
配置描述：WEB 单点登录一般适用于用户有自己的 WEB 服务器，且账号信息均保存在 WEB 服务器上，客户想要实现，用户上网前通过自己 WEB 服务器认证的同时也通过设备的认证。适用于 WEB 服务器在内网或外网的环境。数据流过程如下：

1、用户登录 WEB 服务器，整个过程是明文的，设备监听整个通信过程

2、通过用户认证后服务器反馈的关键字来判断认证成功与否，从而决定 WEB 单点登录成功或失败。

配置路径：【行为管理】>【认证选项】>【SSO】，选择 [WEB SSO]，如下图：

图 13-20 WEB SSO



参数说明：

启用 Web 单点登录：勾选则启用 web 单点登录功能。

WEB 认证服务器地址：填写 WEB 认证服务器地址，可以是 IP 地址或域名。

用户认证 POST 页面 URL：用户发送认证请求的 POST 字段。

用户账号提取正则表达式：使用(.*?)提取用户账号，例如 POST 页面中用户账号字符串为“username=abc&”，则使用正则表达式“username=(.*?)&”可将用户账号 abc 提取出来)。

认证结果：选择[认证成功页面的 URL]或[认证成功关键字]或者[认证失败关键字]，用来识别 WEB 登录是否成功的关键字。比如选了[认证成功结果中的关键字]，则在 POST 的返回结果中，如果包含了设定的关键字，则判断为 WEB 单点登录成功，选择了[认证失败结果中的关键字]，则在 POST 的返回结果中，如果包含了设定的关键字，则判断为 WEB 单点登录失败，反之单点登录成功。

新增组：点击新增组，即可新增单点登录的 web 服务器。

> 提示：
>
> 1.用户 WEB 认证的数据包不经过本设备 ,需要镜像 WEB 认证数据包到本设备 ,同时启用 Web 单点登录 ,并在"SSO 镜像设置"中启用镜像功能。
>
> 2.如果 WEB 服务器在外部，即认证数据经过本设备，则不需要进行[SSO 镜像设置]设置。

13.3.6 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：【行为管理】>【认证选项】>【短信认证】，如下图：

图 13-23 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。

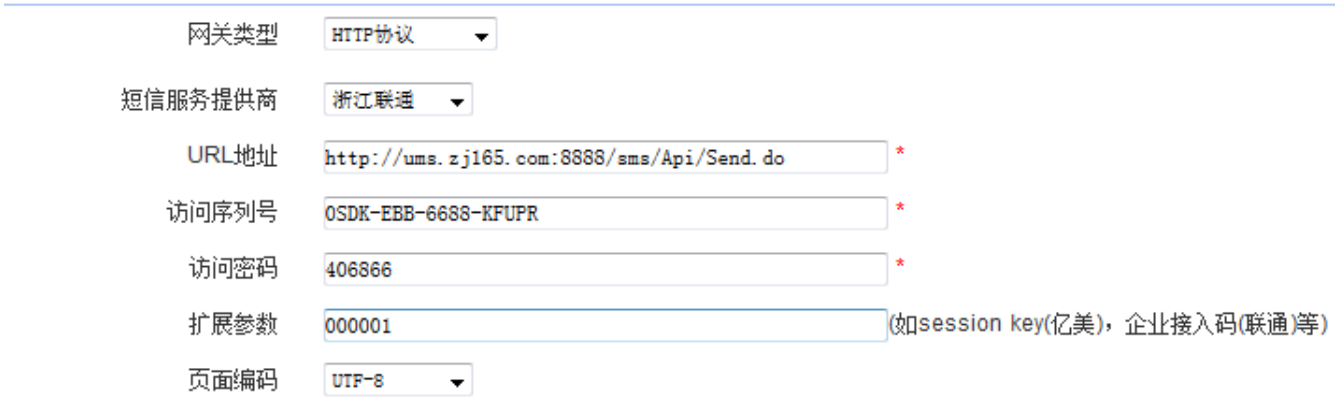
网关类型：可选择“GSM 短信猫”、“CDMA 短信猫”、“HTTP 协议”、“电信运营商”、及“自定义的服务器”

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 13-23 网关类型 - GSM 短信猫

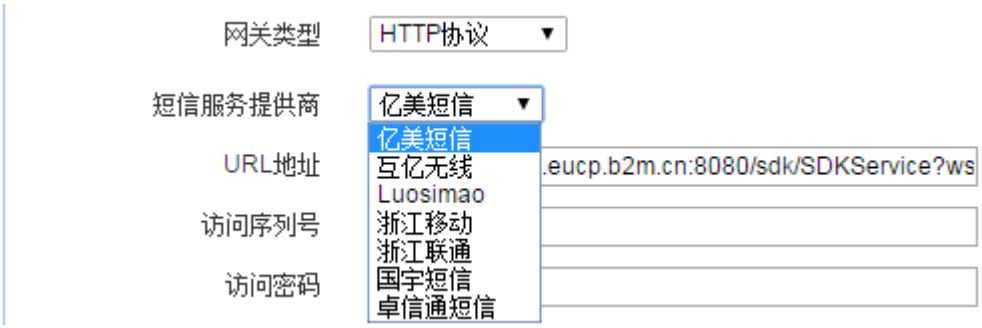
选择“HTTP 协议”，则还需要填写以下参数，如下图所示：

图 13-24 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、卓信通短信等。如下图所示：

图 13-25 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。

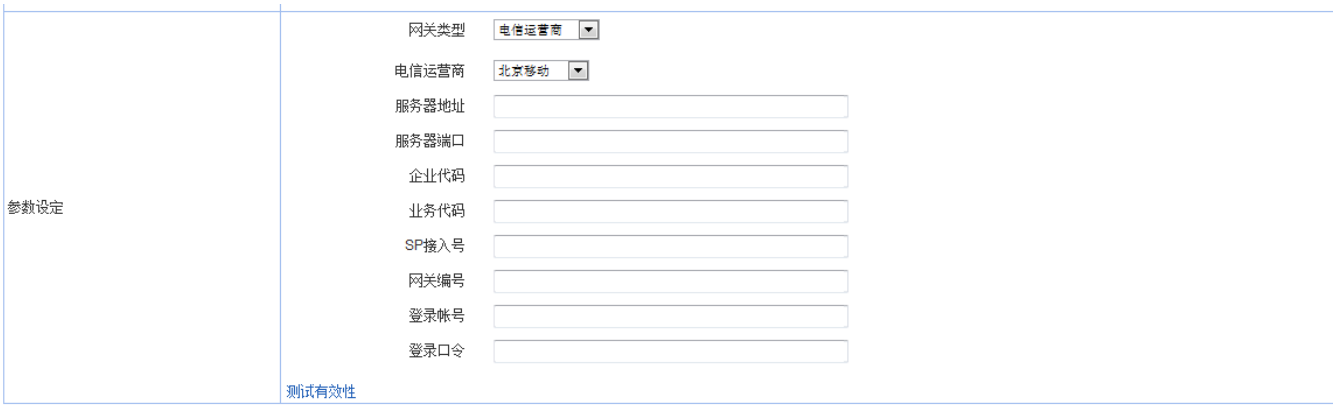
访问密码：填写由短信提供商提供的密码即可。

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 13-26 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。

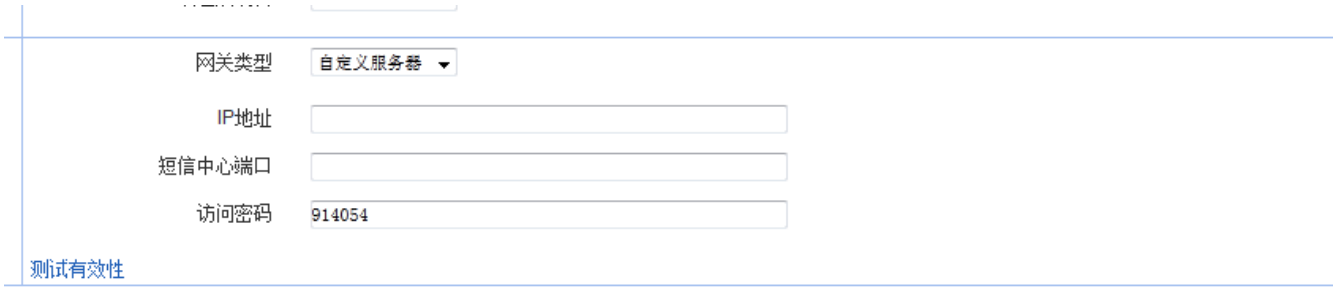
网关编号：电信运营商提供的网关编号。

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 13-27 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 13-25 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。

13.4认证服务器

认证服务器包括 RADIUS 服务器、AD 服务器、LDAP 服务器和 POP3 服务器。

13.4.1 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：

图 13-17 RADIUS 服务器配置列表

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	test	172.16.1.1	1812	1813	30	修改 删除

图1. 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 13-18 新增 RADIUS 认证服务器

新增RADIUS认证服务器 确定 返回

名称		
IP地址		
认证端口	1812	(1-65535)
计费端口	1813	(1-65535)
间隔传送时间	30	(秒)
共享密钥		
使用radius返回值作为用户组	□启用	

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。

13.4.2 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】

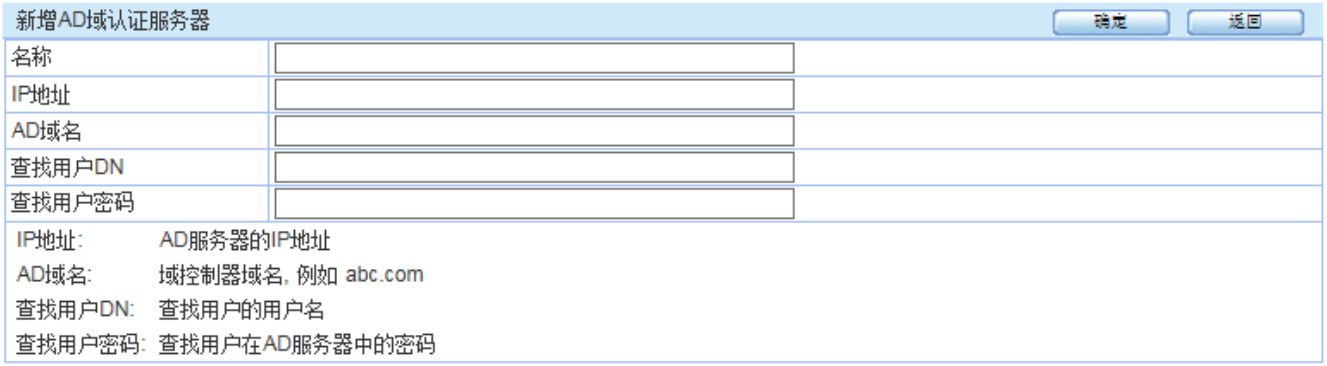
配置描述：

第一：进入【AD 服务器】页面，如下图：

图 13-19 AD 服务器列表

第二：点击<新增>按钮，配置 AD 认证服务器，如下图：

图 13-20 新增 AD 认证服务器



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。例如，域名＝abc.com，用户组为 software，用户名为 searcher，则查找用户 DN 的格式为 cn=searcher,cn=software,dc=abc,dc=com。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。

13.4.3 LDAP 服务器

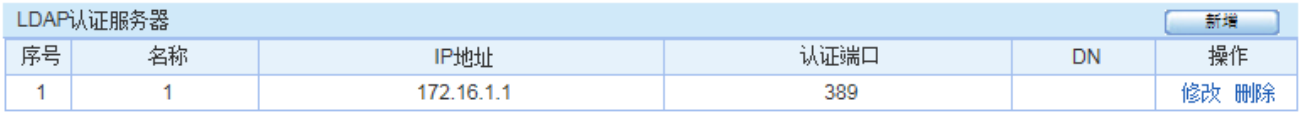
功能描述：配置 LDAP 认证服务器。

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 13-21 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 13-22 新增 LDAP 认证服务器

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。

选择用户查找的方式。

查找用户 DN: 所查找用户的路径，如 cn=searcher,ou=group1,dc=abc,dc=com

13.4.4 POP3 服务器

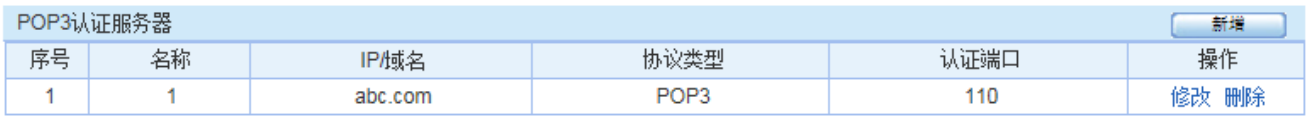
功能描述：配置 POP3 认证服务器。

配置路径：【用户认证】>【认证服务器】>【POP3 服务器】

配置描述：

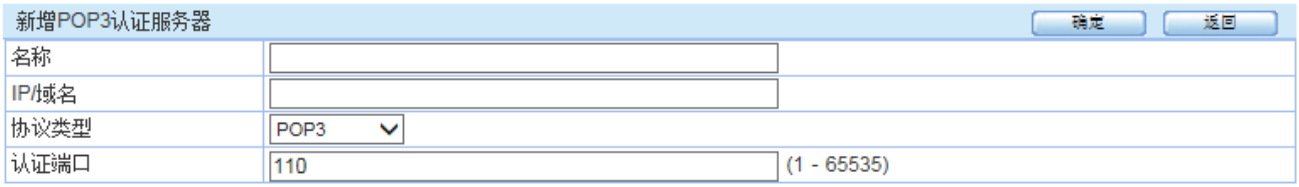
第一：进入【POP3 服务器】页面，如下图：

图 13-23 POP3 服务器列表



第二：点击<新增>按钮，配置 POP3 认证服务器，如下图：

图 13-24 新增 POP3 认证服务器



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/域名：POP3 服务器 IP 地址或域名。

13.4.5 SMP 服务器

功能描述：配置 SMP 认证服务器。

配置路径：【用户认证】>【认证服务器】>【SMP 服务器】

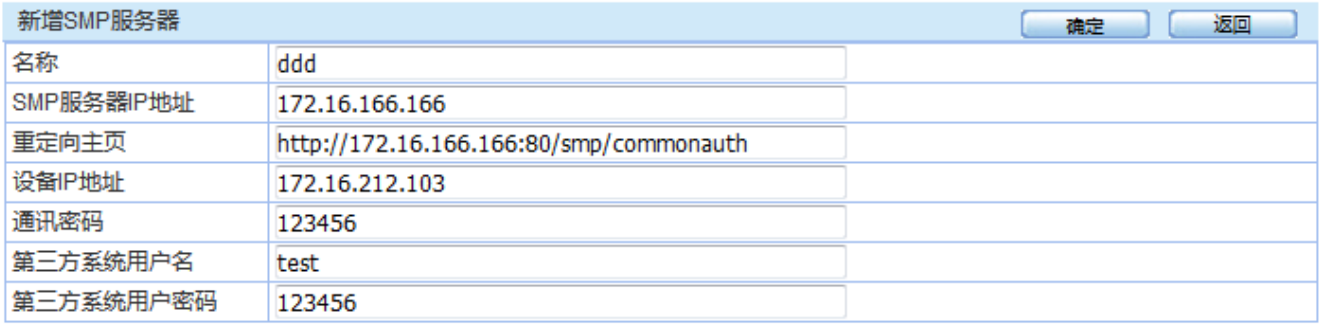
配置描述：

第一：进入【SMP 服务器】页面，如下图：

图 13-25 SMP 服务器列表

第二：点击<新增>按钮，配置 SMP 认证服务器，如下图：

图 13-26 新增 SMP 认证服务器



参数说明：

名称：SMP 策略名称

SMP 服务器 IP 地址：SMP 服务器的 IP 地址

重定向主页：SMP 服务器上面的普通用户认证重定向主页

设备 IP：需要认证的 UAC 设备地址

通讯密码：与 SMP 中 web 认证 key 相同

第三方系统用户名/密码：SMP 服务器中“系统维护”—“第三方系统注册”中配置的用户名密码填写一致

13.4.6 服务器测试

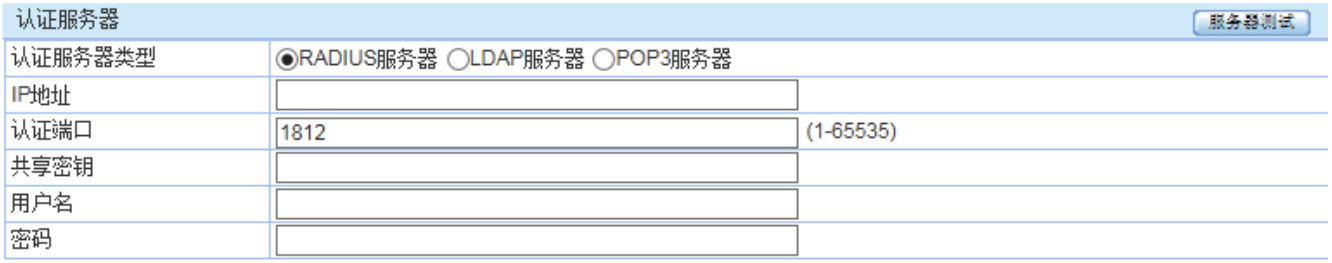
功能描述：测试认证服务器是否可达，是否正常工作。

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 13-27 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。

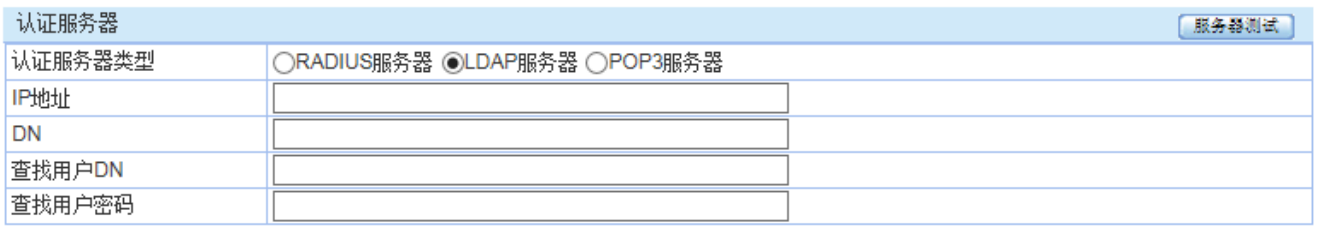
认证端口：服务器中用于认证的端口号，缺省 1812。

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 13-28 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。

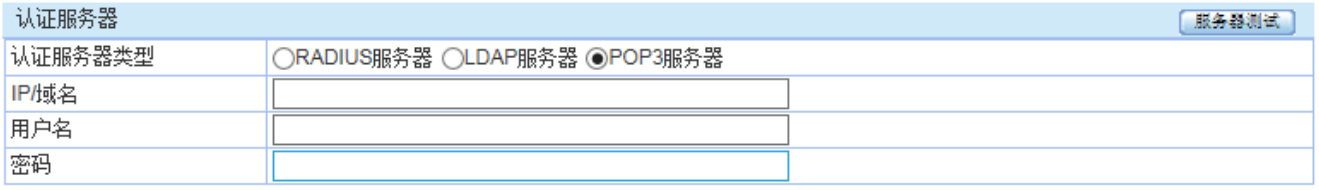
DN：LDAP 服务器用通用名称标识符搜索具体条目时所使用的路径，如 cn=searcher,cn=software,dc=abc,dc=com。

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。

第二：测试[POP3 服务器]，如下图：

图 13-29 POP3 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/域名：POP3 服务器 IP 地址或域名。

用户名/密码：用于测试的 Raduis 用户名和密码。

13.5 白名单管理

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、上网策略规则、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；上网行为的内容（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、上网策略规则、黑名单规则”的限制。

13.5.1 IP 白名单

配置路径：【行为管理】>【白名单管理】>【IP 白名单】

配置描述：配置 IP 白名单

第一：进入【IP 白名单】配置页面，如下图：

图 13-30IP 白名单规则

第二：点击<新增>按钮，增加白名单规则，如下图：

图 13-31 新增白名单规则

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：

a、IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；

b、地址簿：引用已定义好的地址簿；

c、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：

a、IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；

b、地址簿：引用已定义好的地址簿；

c、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。

13.5.2 URL 白名单

配置路径：【行为管理】>【白名单管理】>【URL 白名单】

配置描述：配置 URL 白名单

第一：进入【URL 白名单】配置页面，如下图：

图 13-32URL 白名单规则

第二：点击<新增>按钮，增加 URL 白名单规则，如下图：

图 13-33 新增 URL 白名单规则

参数说明：

名称：URL 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：

a、IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；

b、地址簿：引用已定义好的地址簿；

c、用户组：引用组织结构中定义的用户组

URL 白名单：不受控的 URL,一行一个 URL 关键字（或 URL 全名）；

生效时间：URL 白名单规则的生效时间。生效时间以外，该规则不起作用。

13.5.3 即时通讯白名单

配置路径：【行为管理】>【白名单管理】>【即时通讯白名单】

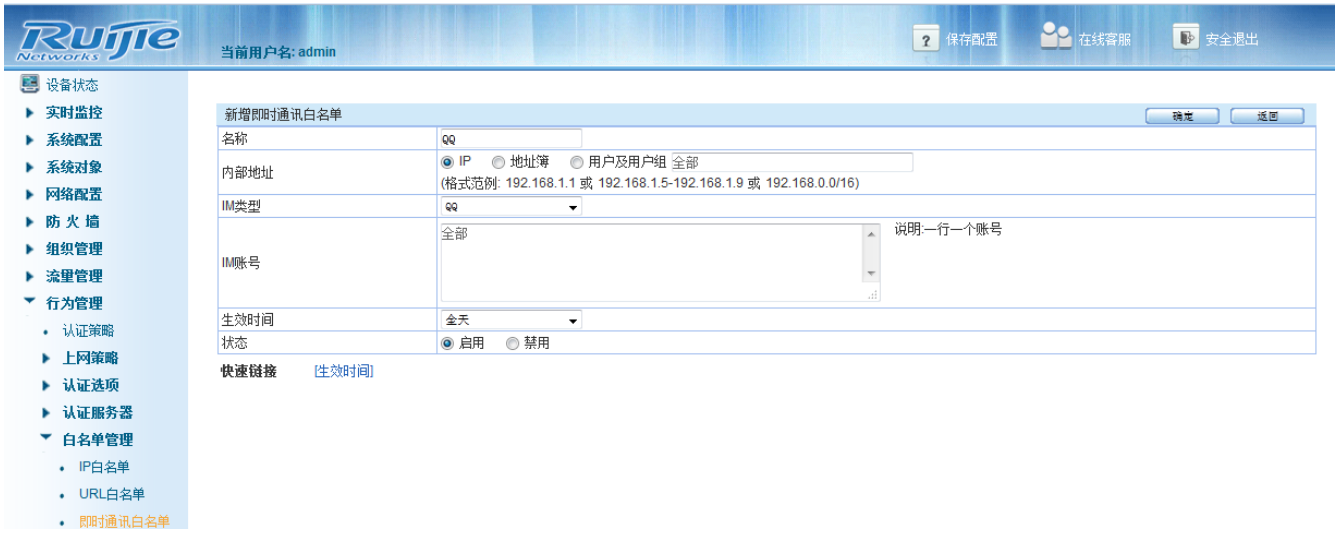
配置描述：配置即时通讯白名单

第一：进入【即时通讯白名单】配置页面，如下图：

图 13-34 即时通讯白名单规则

第二：点击<新增>按钮，增加即时通讯白名单规则，如下图：

图 13-35 新增即时通讯白名单规则



参数说明：

名称：即时通讯白名单规则的名称。

内部地址：不受控的用户的地址,有三种输入方式，详细说明如下：

a、IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；

b、地址簿：引用已定义好的地址簿；

c、用户组：引用组织结构中定义的用户组

IM 类型：不受控的即时通讯的类型；

IM 账号：不受控的即时通讯的账号；

生效时间：URL 白名单规则的生效时间。生效时间以外，该规则不起作用。

13.6黑名单管理

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。使用黑名单功能，需先定义黑名单规则，然后在【行为管理>组织管理>组织结构】的用户和子组中引用黑名单规则。

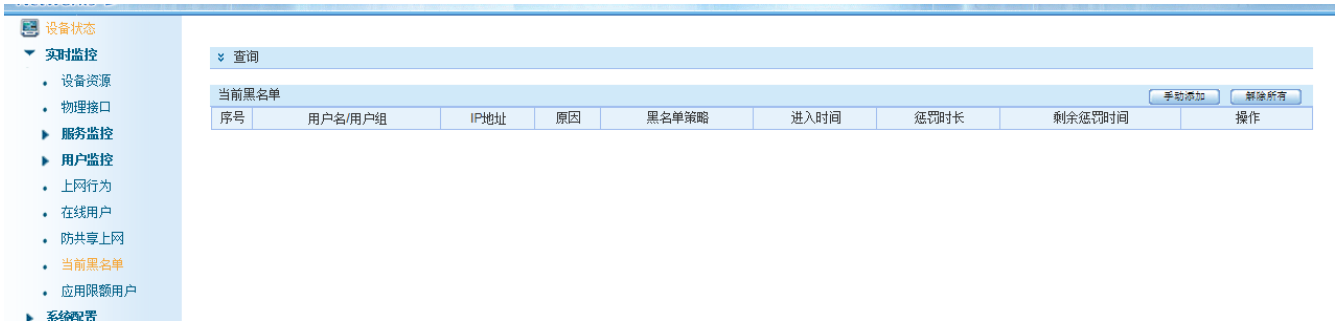
功能描述：查看当前黑名单用户，以及手动添加和解除黑名单用户。

配置路径：【行为管理】>【黑名单管理】>【当前黑名单】

配置描述：

第一：进入【当前黑名单】页面，如下图：

图 13-36 当前黑名单



查询条件：

用户名：根据用户名来查找。

原因：根据进入黑名单的原因来查找。

黑名单规则：根据黑用户引用的黑名单规则来查找。

时间范围：根据进入黑名单的时间范围来查找。

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 13-37 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。

14 酒店管理

14.1 即插即用

由于客人的电脑的 IP 地址配置各不相同，经常需要网管人员为其进行一番配置后才能正常上网。开启即插即用功能，就可实现客人的电脑插上网线即可上网。

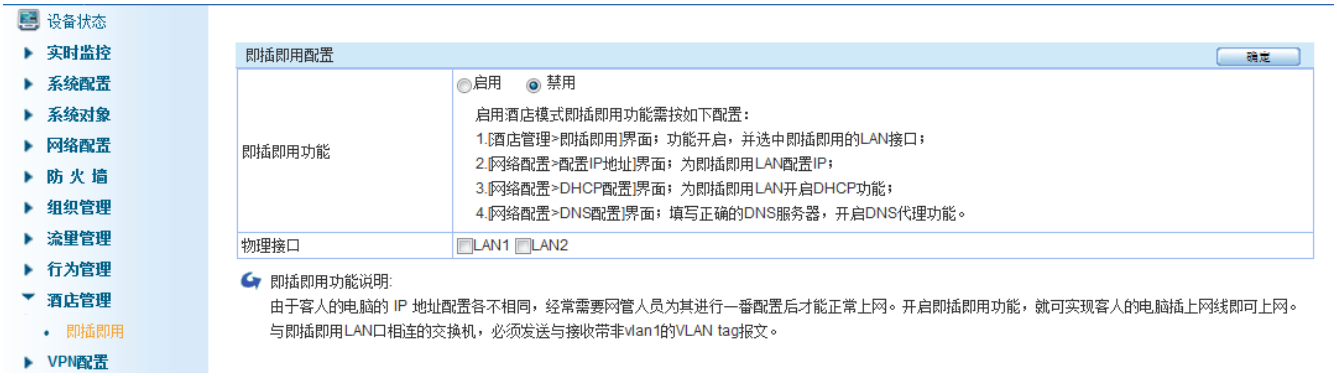
功能描述：配置即插即用功能。

配置路径：【酒店管理】>【即插即用】

配置描述：

第一：进入【即插即用】页面，如下图：

图 14-1 即插即用配置



参数说明：

即插即用功能：选择<启用>或<禁用>开启或关闭“即插即用”功能。启用即插模式即插即用功能需按如下配置：

1）[酒店管理>即插即用]界面：功能开启，并选中即插即用的 LAN 接口；
2）[网络配置>配置 IP 地址]界面：为即插即用 LAN 配置 IP；
3）[网络配置>DHCP 配置]界面：为即插即用 LAN 开启 DHCP 功能；
4）[网络配置>DNS 配置]界面：填写正确的 DNS 服务器，开启 DNS 代理功能。

物理接口：选择要启用即插即用功能的物理接口。

> 提示：
>
> 1、如果需要使用酒店管理必须使用路由模式，一般单独用一个 LAN port 来做酒店管理接口。
>
> 2、一般拓扑是(ACCESS)二/三层交换机(TRUNK) ------行为管理------防火墙，或者行为管理直接放在出口。
>
> 3、与即插即用 LAN 口相连的交换机，必须发送与接收带非 vlan1 的 VLAN tag 报文。即插即用 LAN 口不需要配置任何 vlan 接口，不需要配置任何子接口。
>
> 4、如果有客户的办公网和酒店管理是分开的，如办公网走行为管理的 LAN1，酒店管理使用 LAN2，这种情况，办公网和酒店管理两者 PC 不能互通。

15 VPN 配置

15.1 IPSec

15.1.1 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 15-1 IPSec 隧道配置

第二：进入点击<新增>按钮，增加 IPSec 隧道。如下图：

图 15-2 新增 IPSec 隧道

参数说明：

本地网关：指行为管理设备 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。

15.1.2 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 15-3 配置 IPSec 规则

第二：进入点击<新增>按钮，增加 IPSec 规则。如下图：

图 15-4 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。

15.2 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 15-5 PPTP 配置

参数说明：

PPTP 状态：启用或禁用 PPTP 服务器功能。

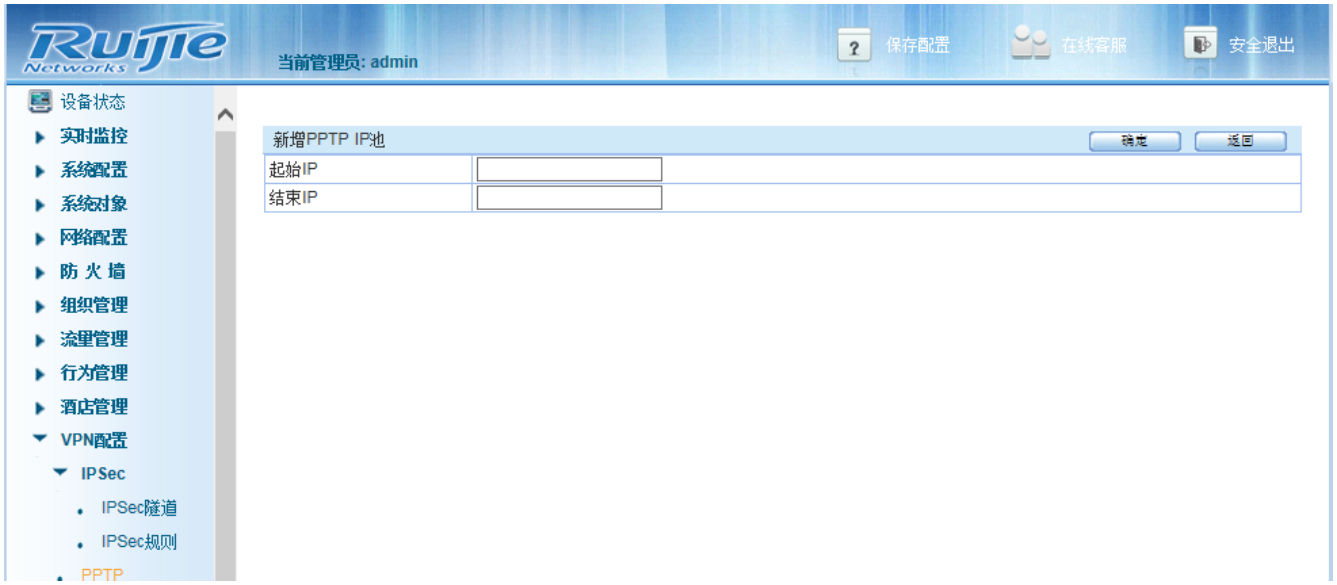
服务器 IP：本机作为 PPTP 服务器的接口 IP 地址。

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。

第二：进入点击<新增>按钮，增加 PPTP IP 池。如下图：

图 15-6 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。

15.3 L2TP

功能描述：配置 L2TP VPN

配置路径：【VPN】>【L2TP】

配置描述：进入【L2TP】页面，开始设置 L2TP 的相关参数。 如下图：

图 15-7 L2TP 配置

参数说明：

L2TP 状态：启用或禁用 L2TP 功能。

服务器 IP：本机作为 L2TP 服务器的 IP 地址，须填写外网口 IP 地址。

预共享密钥：L2TP IPSEC VPN 客户端预共享密钥。

L2TP 本地 IP：L2TP VPN 客户端协商成功后的网关 IP。

L2TP IP 范围：分配给 L2TP 拨号用户的 IP 地址段。

首选 DNS 服务器：分配给 L2TP 拨号用户的首选 DNS 服务器。

备用 DNS 服务器：分配给 L2TP 拨号用户的备用 DNS 服务器。

认证方式：选择 L2TP 用户的认证方式。可以选择：

RADIUS 认证：使用外部的 RADIUS 服务器来认证。

IP 地址：RADIUS 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 RADIUS 服务器交换数据时进行加密的密钥。

VPN 用户本地认证：需先在【VPN > VPN 用户】配置好 L2TP VPN 用户。

15.4VPN 用户

功能描述：配置 VPN 的用户，该用户可应用于 PPTP VPN 和 IPSec VPN。

配置路径：【VPN】>【VPN 用户】

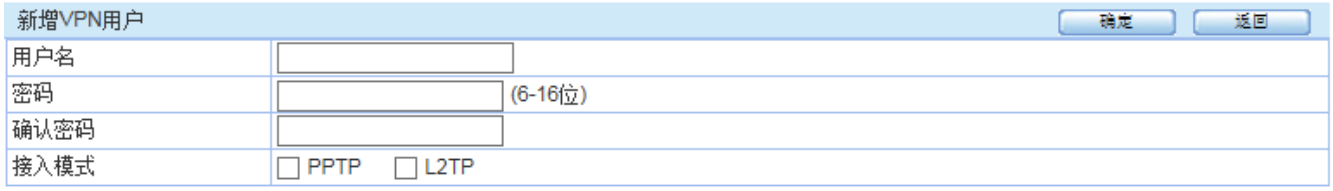
配置描述：

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：

图 15-8 配置 VPN 用户

第二：进入点击<新增>按钮，增加 PPTP 用户。如下图：

图 15-9 新增 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哪些 VPN 协议，可选择为 PPTP、IPSec。

提示：VPN 用户可应用于 PPTP VPN 和 IPSec VPN 的拨号用户。

16 HA 配置

系统支持一主一备，或一主多备的 HA 模式；也支持多个主设备(多主一备/多主多备)的 HA 模式，多个主设备间可实现负载均衡。

功能描述：设置设备的 HA 模式，以便实现多机热备。

配置路径：【HA 配置】>【HA 配置】

配置描述：进入【HA 配置】页面，如下图：

图 16-1 HA 配置 1

图 16-2 HA 配置 2

参数说明：

自动同步：启用自动同步，则每次保存配置时都会同步配置文件到指定设备（同步 IP 地址所代表的设备）；

同步 IP 地址：网络可达的备用设备 IP 地址，一般为备用设备的心跳口 IP 地址

立即同步：点击此按钮，会将配置立即同步到指定设备。

功能状态：启用或禁用 HA 功能；

心跳间隔：HA 集群的节点设备之间传递心跳报文的间隔，默认 2 秒；

死亡时间：备用设备在该时间段内没有收到主设备的心跳报文，则立即转换为主设备，默认 30 秒；

心跳端口：选择用于连接对方节点设备的 HA 专用端口，可以选择串口或者以太网物理口；

本地节点名称：本端节点设备的系统名称，与【系统配置>系统信息】页面配置的系统名称相同；

其他节点名称：HA 集群的其他节点的名称，多个节点之间用英文逗号分隔；

主设备：配置 HA 集群的主设备。配置一个主设备，则为主备模式；

强制抢占：主设备状态由故障恢复正常后，是否要强制转换为主设备；

关闭 WAN 口：当切换到备用设备时自动关闭上游接口 WAN 口；

链路健康检查：检测上游链路健康状态，故障时自动切换为备用状态。

17 系统日志

“系统日志”包含：命令日志、事件日志、用户日志、黑名单日志、日志服务器的配置。

17.1 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 17-1 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。

17.2 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 17-2 事件日志

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，清空所有的事件日志。

17.3 PPTP/L2TP 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 17-3 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。

17.4 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：

图 17-4 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。

17.5 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 17-5 Syslog 服务器

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。

17.6短信配置

功能描述：短信配置。

配置路径：【系统日志】>【短信配置】

配置描述：进入【短信配置】页面，

如下图：图 17-7 短信配置

参数说明：

短信配置：启动或者禁用该功能；

手机号码：填写接收告警信息的手机号码，多个号码已“；”隔离。

17.7 告警配置

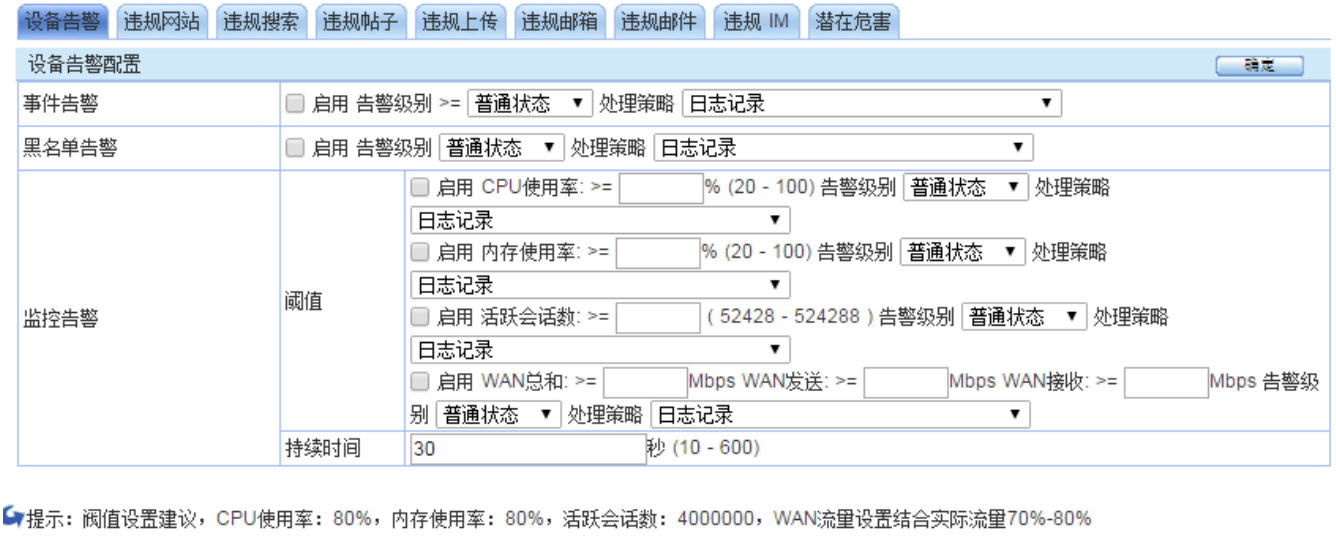
功能描述：配置告警规则

配置路径：【系统日志】>【告警配置】

配置描述：进入【告警配置】页面，如下图：

图 17-8 告警配置

第一：勾选设备的 告警配置



提示：阈值设置建议，CPU使用率：80%，内存使用率：80%，活跃会话数：4000000，WAN流量设置结合实际流量70%-80%

参数说明：

事件告警：启用，选择告警级别，处理策略根据需要选择；

黑名单告警：启用，选择告警级别，处理策略根据需要选择，需要结合黑名单规则，参考<典型功能-上网策略-黑名单策略>完成配置；

监控告警：启用，选择告警级别，处理策略根据需要选择;

提示：阀值设置建议，CPU 使用率：80%，内存使用率：80%，活跃会话数：4000000，WAN 流量设置结合实际流量 70%-80%

18 故障排除

18.1 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：【故障排除】>【捕获数据包】

配置描述：进入【捕获数据包】页面，如下图：

图 18-1 故障排除-捕获数据包 1

图 18-2 故障排除-捕获数据包 1

参数说明：

捕获包数：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，“--”代表没有连接任何接口；

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【故障排除>查看数据包】页面去查看捕获到的数据包文件。

18.2 查看数据包

功能描述：查看已捕获的数据报文。

配置路径：【故障排除】>【查看数据包】

配置描述：进入【查看数据包】页面，如下图：

图 18-3 故障排除-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，也可以点击在<详细>按钮里查看。

18.3调试信息下载

功能描述：下载调试信息。

配置路径：【故障排除】>【调试信息下载】

配置描述：进入【调试信息下载】页面，如下图：

图 18-4 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。

18.4上网故障调试

功能描述：下载调试信息。

配置路径：【故障排除】>【上网故障调试】

配置描述：进入【上网故障调试】页面，如下图：

图 18-5 下载调试信息

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。

19 报表中心

设备提供了内置报表中心，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，行为分析等所有的记录。行为分析部分也可根据需要选择记录部分内容，具体配置方法参照【内容记录配置】。

19.1 报表中心配置

功能描述：配置内置报表中心用以查看统计记录。

配置路径：【报表中心】>【报表中心配置】

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 19-1 报表中心配置

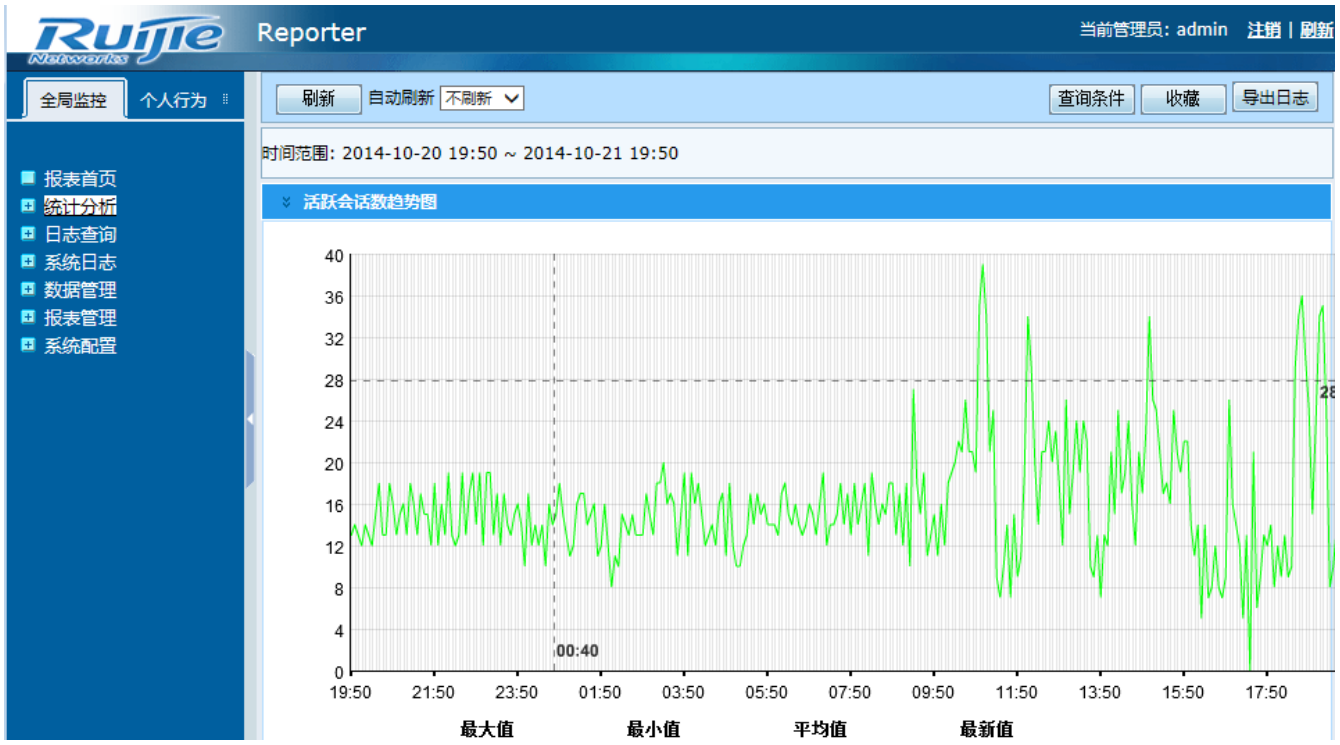
19.2 内置报表中心

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 19-2 内置报表中心首页


Ruijie Networks
Reporter
当前管理员: admin 注销 | 刷新
全局监控
个人行为
刷新
自动刷新
不刷新
查询条件
收藏
导出日志
时间范围: 2014-10-20 19:50 ~ 2014-10-21 19:50
报表首页
统计分析
日志查询
系统日志
数据管理
报表管理
系统配置
活跃会话数趋势图
40
36
32
28
24
20
16
12
8
4
0
00:40
19:50
21:50
23:50
01:50
03:50
05:50
07:50
09:50
11:50
13:50
15:50
17:50
最大值
最小值
平均值
最新值

20 登录报表中心

20.1 登录内置报表中心

登录内置报表中心有两种方法：

- 从设备管理界面直接转到内置报表中心界面

  首先登录设备管理界面，然后点击【报表中心>内置报表中心】，即可进入内置报表中心界面。

- 直接进入报表中心界面

  设备默认使用 LAN1 作为网管口，LAN1 出厂地址为 192.168.1.200/24。采用 HTTP 登录，默认端口 9091。初始登录 URL 为：http://192.168.1.200:9091。

  默认的管理员账号是 admin，密码是 firewall。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。

20.1.1 首页

成功登录报表中心后，其首页如下：

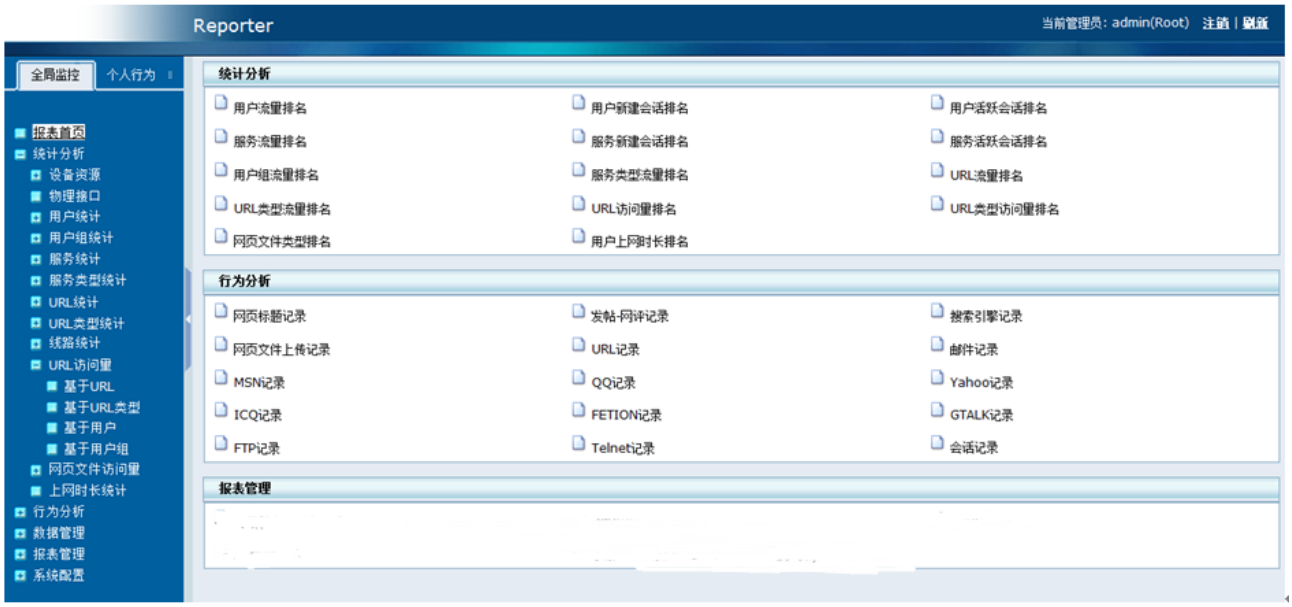


图2. 报表中心首页

首页涵盖以下几部分：

- 全局监控：显示经过设备是所有数据流的统计与上网行为信息。
- 个人行为：以用户为单位，统计个人的上网行为信息。
- 统计分析：显示了统计分析栏里的部分页面的快速连接，点击对应的连接即可进入到对应的页面。
- 行为分析：显示了行为分析栏里的部分页面的快速连接，点击对应的连接即可进入到对应的页面。
- 报表管理：显示了手动或者自动产生的报表里部分页面的快速连接，点击对应的连接即可进入到对应的页面。

在管理界面的右上角有两个按钮，分别是<刷新>和<注销>。点击<刷新>按钮，可手动刷新当前页。点击<注销>按钮并确认后，即可退出当前系统，返回到登录界面。

21 统计分析

报表中心提供统计功能，本章对上网流量、上网速率、新建会话、活跃会话、网站访问情况、URL 排名、上网时长等参数进行详细的统计和排名。

[统计分析]的每个统计对象都根据多个时间周期来进行采样分析统计。在每个统计对象的页面上方都用多个分页来分别显示每个周期的统计结果。如图:

- 自定义时间段：显示自定义时间段的统计信息。

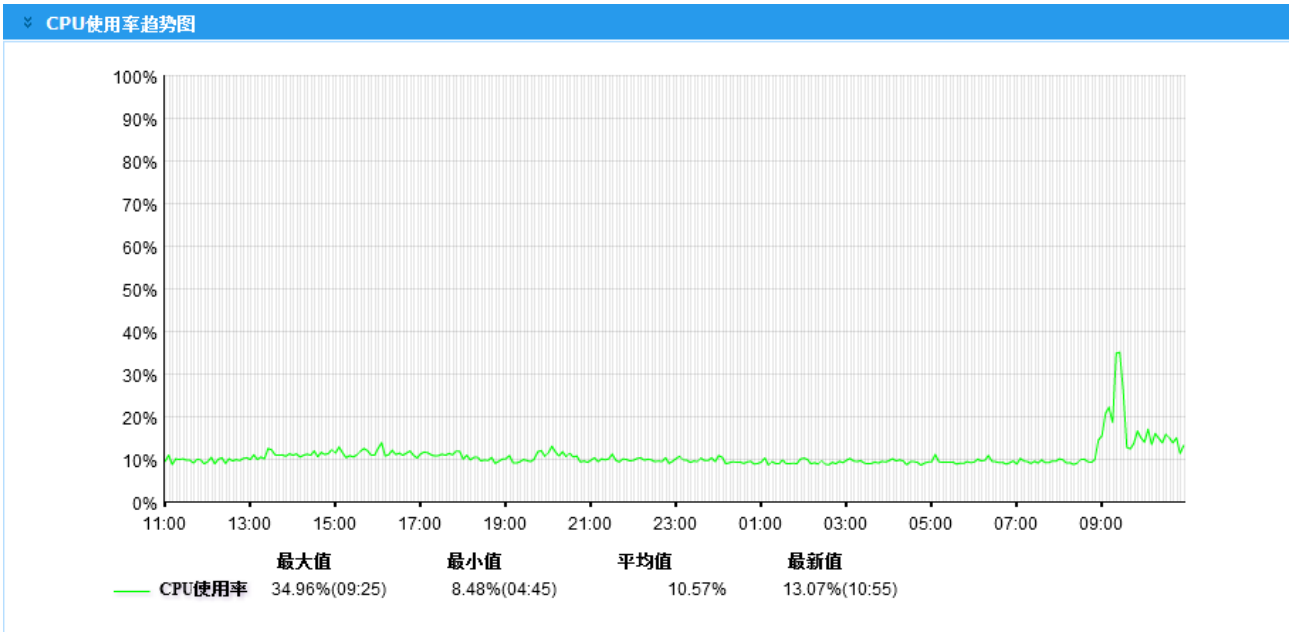
21.1.1 设备资源

21.1.1.1 CPU 使用率

功能描述：显示 CPU 使用率。

配置路径：【统计分析】>【设备资源】>【CPU 使用率】

配置描述：进入【CPU 使用率】页面，对 CPU 使用率的统计如下：



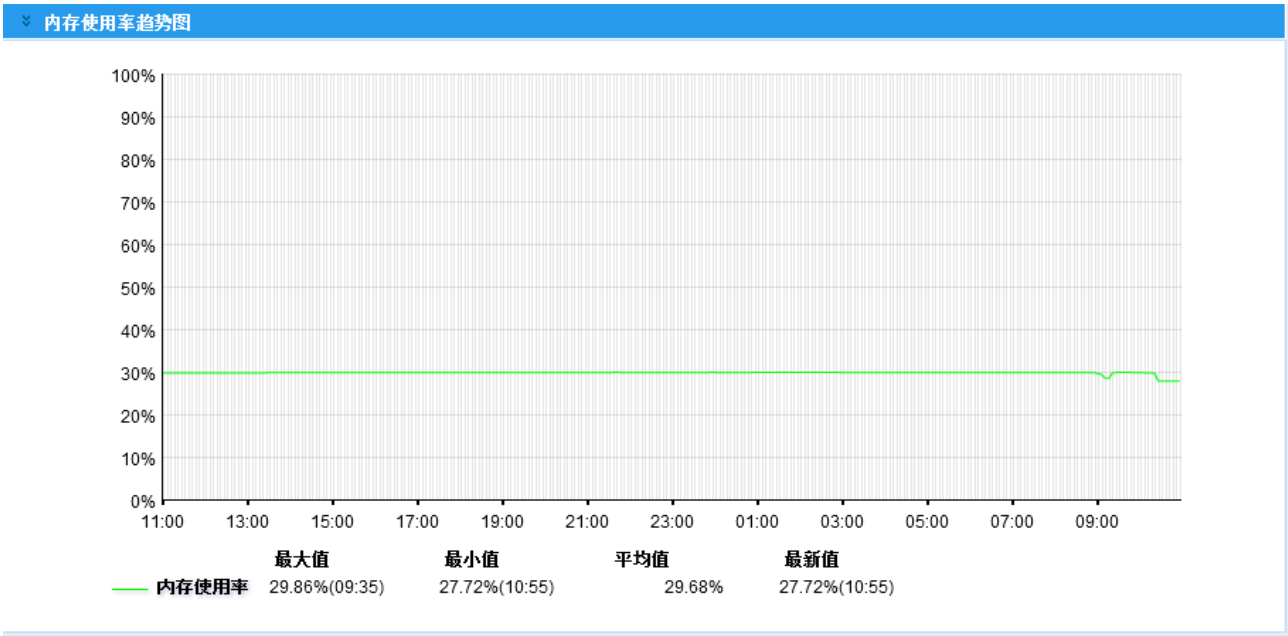
图的下方显示了最大值、最小值、平均值、最新值(最近一个采样点的值)，以及每个值对应的时间点。

21.1.1.2 内存使用率

功能描述：显示内存使用率。

配置路径：【统计分析】>【设备资源】>【内存使用率】

配置描述：进入【内存使用率】页面，对内存使用率的统计如下：



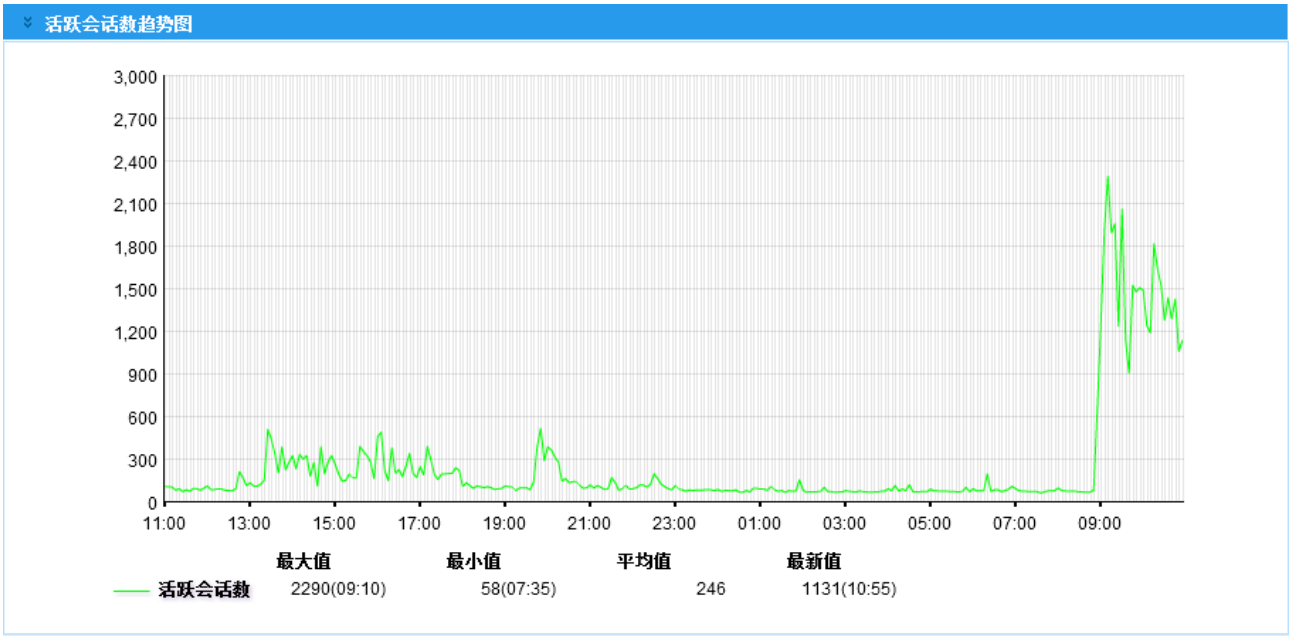
图的下方显示了最大值、最小值、平均值、最新值(最近一个采样点的值)，以及每个值对应的时间点。

21.1.1.3 活跃会话数

功能描述：显示活跃会话数。

配置路径：【统计分析】>【设备资源】>【活跃会话数】

配置描述：进入【活跃会话数】页面，对活跃会话数的统计如下：



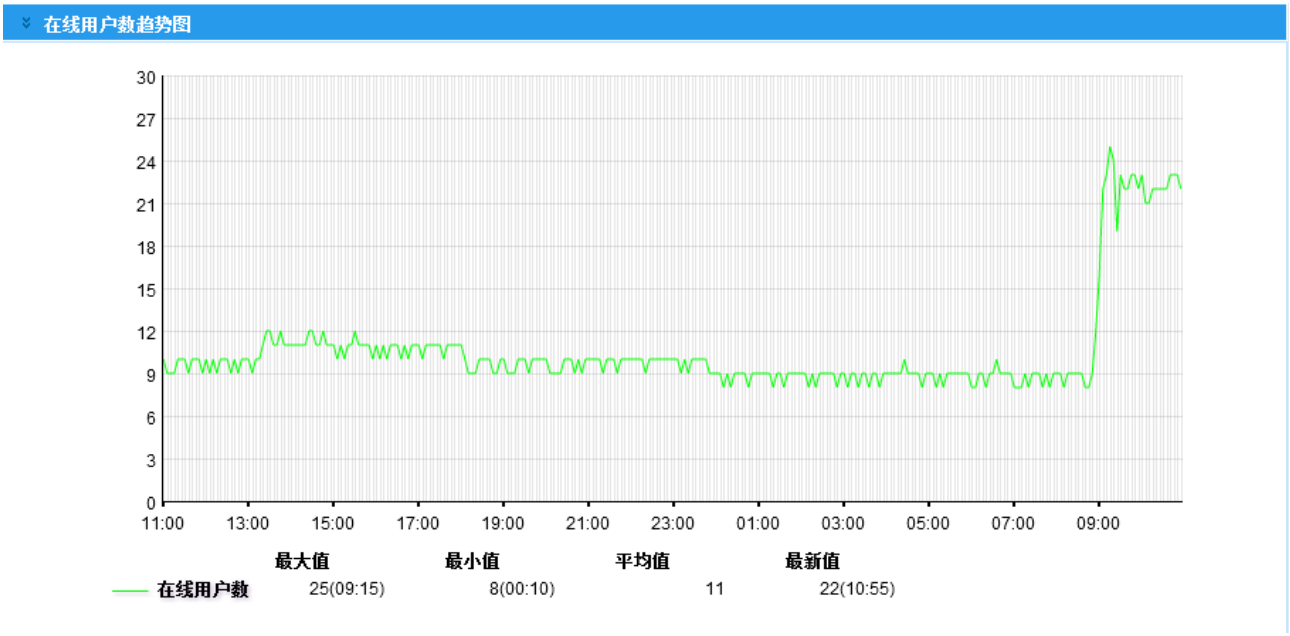
图的下方显示了最大值、最小值、平均值、最新值(最近一个采样点的值)，以及每个值对应的时间点。

21.1.1.4 在线用户数

功能描述：显示在线用户数。

配置路径：【统计分析】>【设备资源】>【在线用户数】

配置描述：进入【在线用户数】页面，对在线用户数的统计如下：



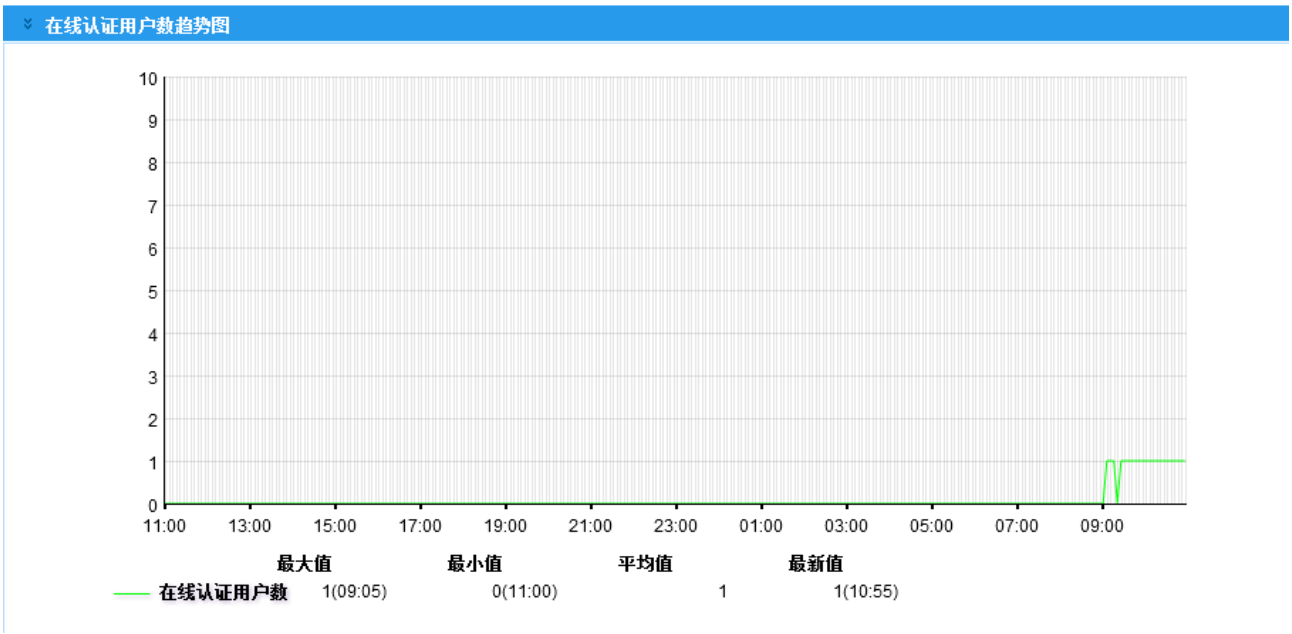
图的下方显示了最大值、最小值、平均值、最新值(最近一个采样点的值)，以及每个值对应的时间点。

21.1.1.5 在线认证用户数

功能描述：显示在线认证用户数。

配置路径：【统计分析】>【设备资源】>【在线认证用户数】

配置描述：进入【在线认证用户数】页面，对在线认证用户数的统计如下：



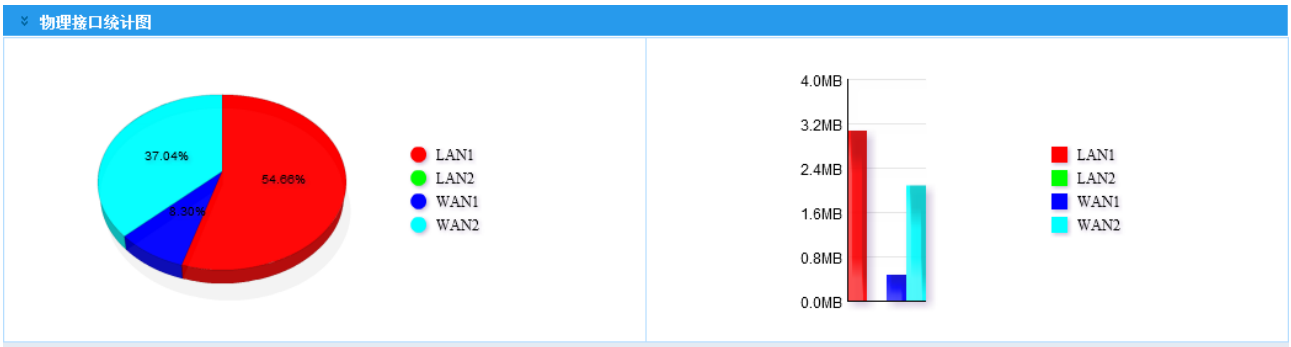
图的下方显示了最大值、最小值、平均值、最新值(最近一个采样点的值)，以及每个值对应的时间点。

21.1.2 物理接口

功能描述：显示物理接口收发报文的信息和流量统计。

配置路径：【统计分析】>【物理接口】

配置描述：进入【物理接口】页面，对物理接口的统计如下：

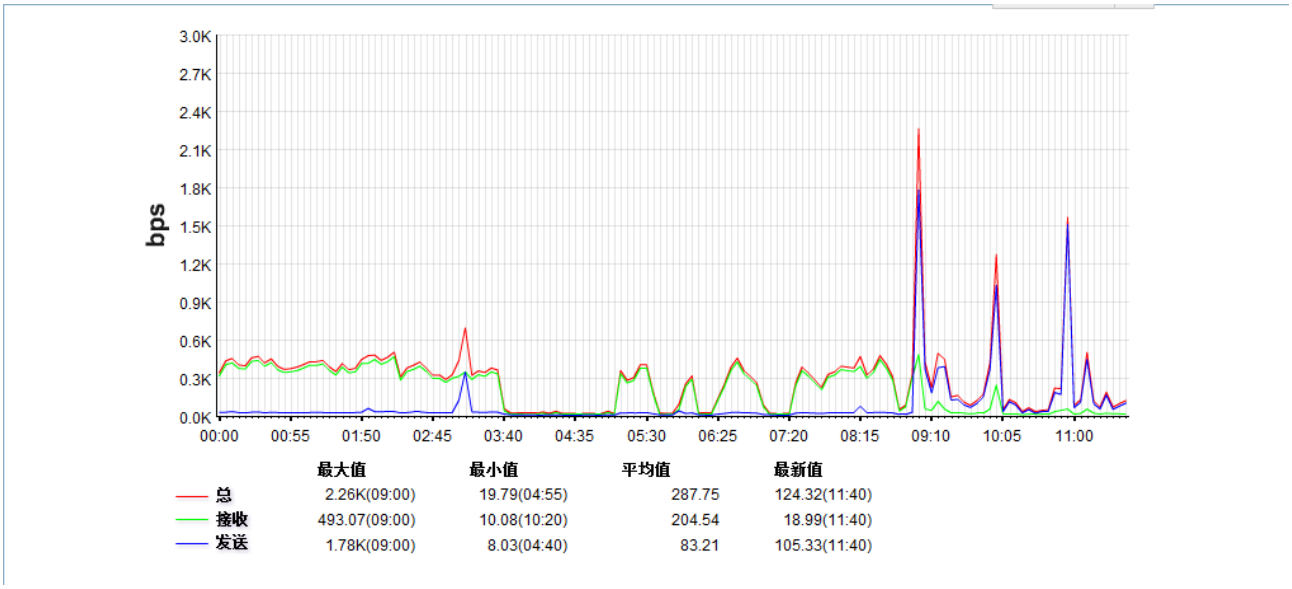


物理接口列表

序号	物理接口	百分比	详细	流里(Byte)			平均速率(bps)			峰值速率(bps)			链路平均速率百分比		
				总	接收	发送	总	接收	发送	总	接收	发送	总	接收	发送
	总计	100.00%		5.61M	3.10M	2.51M	544.64	300.89	243.76						
1	LAN1	54.66%		3.07M	1.19M	1.88M	297.70	115.29	182.41	8.15K	7.85K	4.54K			
2	LAN2	0.00%		0	0	0	0.00	0.00	0.00	0.00	0.00	0.00			
3	WAN1	8.30%		476.62K	348.55K	128.06K	45.19	33.05	12.14	1.06K	989.33	582.53	0.00 %	0.00 %	0.00 %
4	WAN2	37.04%		2.08M	1.57M	518.97K	201.75	152.54	49.21	4.47K	4.22K	1.77K	0.00 %	0.00 %	0.00 %

参数说明：

- 物理接口统计图：[饼图]显示各个物理接口接收的流量占总流量的比例，[柱图]显示各个物理接口接收的流量值。
- 物理接口列表：分别显示各个接口接收的流量值、平均速率以及峰值速率。点击[详细]栏的<趋势图>按钮，可显示指定物理接口的收发报文的趋势图。如下：



21.2 用户统计

21.2.1 流量统计

功能描述：以用户为统计对象，对其收发的流量、速率进行排名统计。

配置路径：【统计分析】>【用户统计】>【流量统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

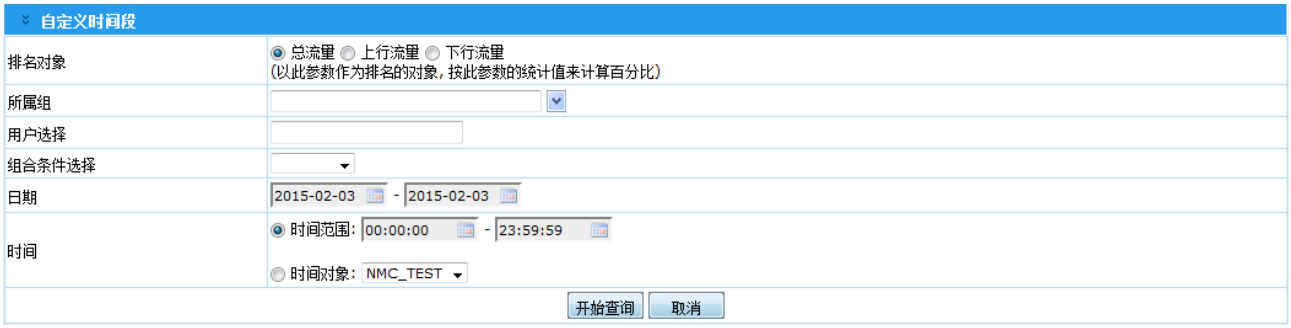


图3. 用户统计-流量统计-统计条件

参数说明：

- 排名对象：以总流量、上行流量、或下行流量为对象进行排名。
- 所属组：选择需要进行流量排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 用户选择：选择需要进行流量排名统计用户。
- 组合条件选择：选择需要进行流量排名统计的服务名称/网站名称/网站类型/出口线路。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的用户中，每个用户的流量占总流量的比例。[柱图]显示排名前十的用户的流量及排名。

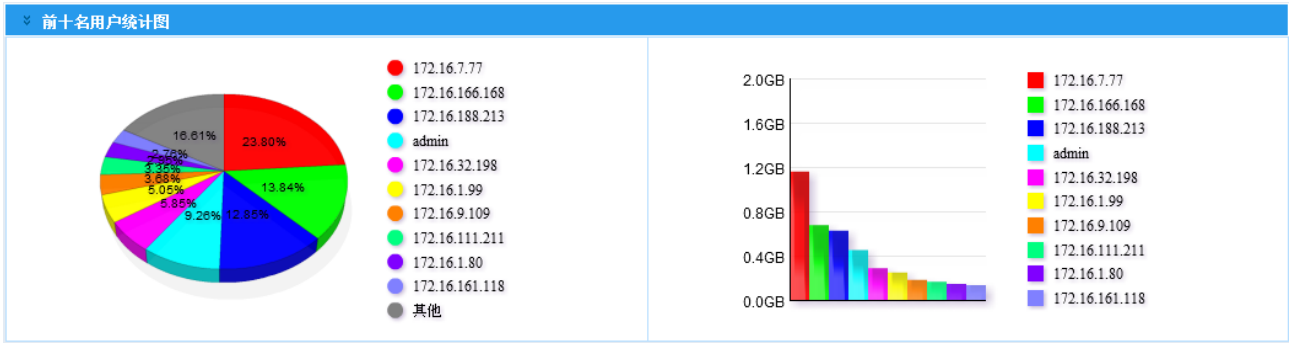


图4. 用户统计-流量统计-前十名统计图

第三、 排名列表。显示符合统计条件的用户的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

用户排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	用户名	百分比	详细	流量(Byte)			平均速率(bps)			峰值速率(bps)		
				总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		5.05G	1.87G	3.18G	973.89K	359.92K	613.97K			
1	172.16.7.77	22.96%		1.16G	1010.25M	177.25M	223.63K	190.25K	33.38K	1.47M	458.51K	1.44M
2	172.16.166.168	13.38%		692.10M	32.53M	659.58M	130.34K	6.13K	124.21K	4.25M	166.56K	4.09M
3	172.16.188.213	12.47%		644.86M	28.38M	616.48M	121.44K	5.35K	116.10K	4.36M	186.50K	4.18M
4	admin	9.58%		495.67M	106.41M	389.26M	93.35K	20.04K	73.31K	1.56M	1.17M	1.46M
5	172.16.32.198	6.35%		328.60M	121.47M	207.13M	61.88K	22.88K	39.01K	947.00K	830.87K	352.83K
6	172.16.1.99	4.88%		252.15M	230.06M	22.09M	47.49K	43.32K	4.16K	294.32K	270.68K	23.79K
7	172.16.9.109	3.72%		192.36M	92.37M	99.99M	36.23K	17.40K	18.83K	1.53M	896.70K	977.99K
8	172.16.111.211	3.25%		168.12M	15.98M	152.14M	31.66K	3.01K	28.65K	1.21M	60.36K	1.15M
9	172.16.1.80	3.04%		157.27M	65.72M	91.55M	29.62K	12.38K	17.24K	1.02M	986.29K	516.76K
10	172.16.161.118	2.66%		137.45M	40.56M	96.89M	25.88K	7.64K	18.25K	1.24M	63.71K	1.17M

图5. 用户统计-流量统计-排名列表

参数与按钮说明：

- 流量：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户传输流量的累计值。
- 平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户传输速率的平均值。
- 峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户传输速率的最大值。
- <趋势图>：点击此按钮，显示指定用户传输速率的趋势图。
- <基于服务的统计>：点击此按钮，显示指定用户访问的服务的流量、传输速率的排名情况。
- <基于服务类型的统计>：点击此按钮，显示指定用户访问的服务类型的流量、传输速率的排名情况。
- <基于 URL 的统计>：点击此按钮，显示指定用户访问的 URL 的流量、传输速率的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示指定用户访问的 URL 类型的流量、传输速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定用户在多条出口链路上的流量、速率的分布与排名情况。

21.2.2 会话统计

功能描述：以用户为统计对象，对其新建会话数、新建会话速率进行排名统计。

配置路径：【统计分析】>【用户统计】>【会话统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

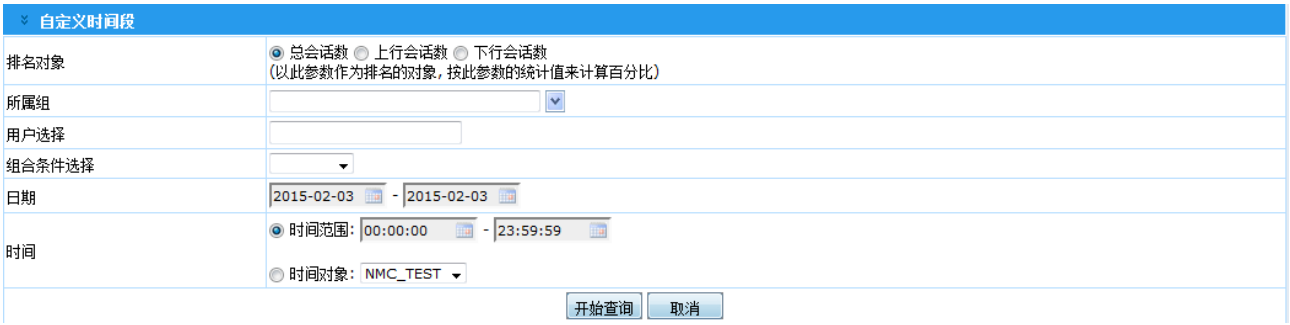


图6. 用户统计-会话统计-统计条件

参数说明：

- 排名对象：以总会话数、上行会话数、或下行会话数为对象进行排名。
- 所属组：选择需要进行会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 用户选择：选择需要进行会话排名统计用户。
- 组合条件选择：选择需要进行会话排名统计的服务名称/网站名称/网站类型/出口线路。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的用户中，每个用户的会话数占总会话数的比例。[柱图]显示排名前十的用户的会话数及排名。

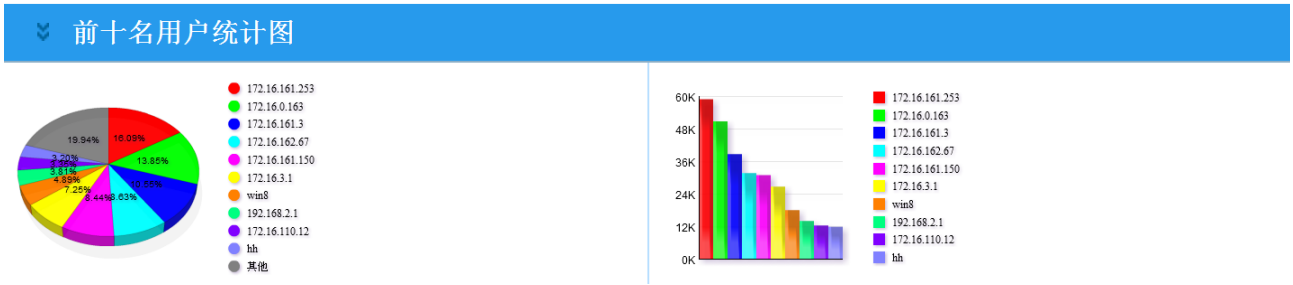


图7. 用户统计-会话统计-前十名统计图

第三、 排名列表。显示符合统计条件的用户的排名情况。受篇幅所限，下图仅截取前 15 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

用户排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	用户名	百分比	详细	新建会话数			新建会话平均速率(sps)			新建会话峰值速率(sps)		
				总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		161.00K	160.77K	231	3.70	3.70	0.01			
1	admin	15.21%		24.48K	24.48K	0	0.56	0.56	0.00	5.30	5.30	0.00
2	172.16.161.3	14.18%		22.83K	22.61K	225	0.52	0.52	0.01	0.60	0.59	0.03
3	172.16.7.77	13.47%		21.69K	21.69K	0	0.50	0.50	0.00	1.81	1.81	0.00
4	172.16.1.80	11.77%		18.95K	18.95K	0	0.44	0.44	0.00	2.15	2.15	0.00
5	172.16.32.198	9.85%		15.85K	15.85K	0	0.36	0.36	0.00	2.56	2.56	0.00
6	172.16.161.253	3.09%		4.97K	4.97K	0	0.11	0.11	0.00	1.48	1.48	0.00
7	172.16.111.211	2.79%		4.48K	4.48K	0	0.10	0.10	0.00	2.65	2.65	0.00
8	172.16.1.99	2.57%		4.14K	4.14K	0	0.10	0.10	0.00	0.19	0.19	0.00
9	172.16.1.23	2.37%		3.82K	3.82K	0	0.09	0.09	0.00	1.17	1.17	0.00
10	172.16.161.65	2.33%		3.75K	3.75K	0	0.09	0.09	0.00	0.86	0.86	0.00

图8. 用户统计-会话统计-排名列表

参数与按钮说明：

- 新建会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户新建会话的累计值。
- 新建会话平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户新建会话速率的平均值。
- 新建会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户新建会话速率的最大值。
- <趋势图>：点击此按钮，显示指定用户新建会话速率的趋势图。
- <基于服务的统计>：点击此按钮，显示指定用户访问的相关服务的新建会话数、新建会话速率的排名情况。
- <基于服务类型的统计>：点击此按钮，显示指定用户访问的相关服务类型的新建会话数、新建会话速率的排名情况。
- <基于 URL 的统计>：点击此按钮，显示指定用户访问的 URL 的新建会话数、新建会话速率的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示指定用户访问的 URL 类型的新建会话数、新建会话速率的排名情况。
- <基于线路的统计>:点击该按钮,显示指定用户在多条出口链路上的新建会话数、新建会话速率的排名情况。

21.2.3 活跃会话

功能描述：以用户为统计对象，对其活跃会话数进行排名统计。

配置路径：【统计分析】>【用户统计】>【活跃会话】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

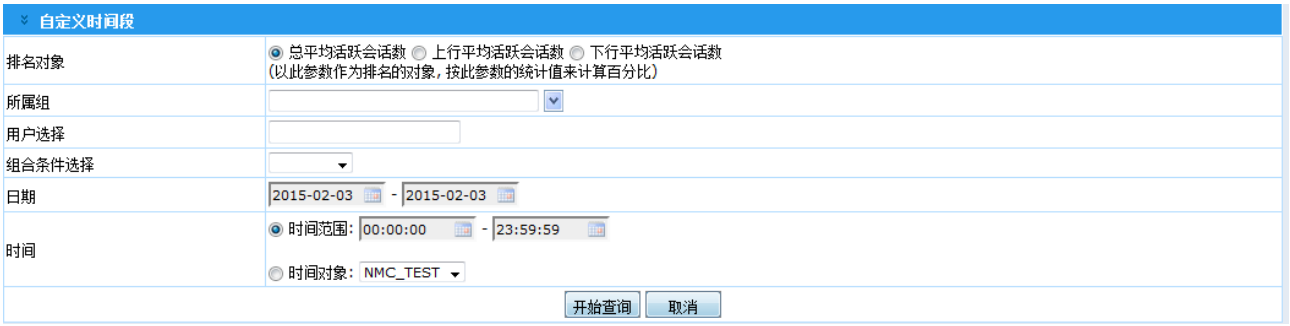


图9. 用户统计-活跃会话-统计条件

参数说明：

- 排名对象：以总平均活跃会话数、上行平均活跃会话数、或下行平均活跃会话数为对象进行排名。
- 所属组：选择需要进行活跃会话数排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 用户选择：选择需要进行活跃会话数排名统计用户。
- 组合条件选择：选择需要进行活跃会话数排名统计的服务名称/网站名称/网站类型/出口线路。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的用户中，每个用户的活跃会话数占总活跃会话数的比例。[柱图]显示排名前十的用户的活跃会话数及排名。

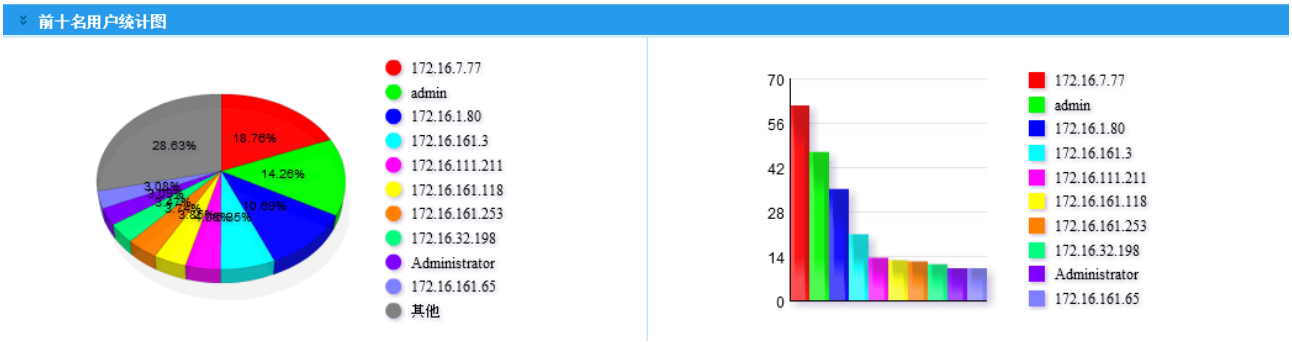


图10. 用户统计-活跃会话-前十名统计图

第三、 排名列表。显示符合统计条件的用户的排名情况。受篇幅所限，下图仅截取前 21 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

用户排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	用户名	百分比	详细	平均活跃会话数			峰值活跃会话数		
				总	上行	下行	总	上行	下行
	总计	100.00%		335.54	335.43	0.11			
1	172.16.7.77	17.97%		60.31	60.31	0.00	175.70	175.70	0.00
2	admin	15.21%		51.02	51.02	0.00	474.26	474.26	0.00
3	172.16.1.80	10.36%		34.77	34.77	0.00	169.52	169.52	0.00
4	172.16.161.3	6.23%		20.90	20.80	0.10	35.02	35.02	1.77
5	172.16.111.211	3.96%		13.28	13.28	0.00	287.46	287.46	0.00
6	172.16.161.253	3.81%		12.80	12.80	0.00	145.37	145.37	0.00
7	172.16.161.118	3.69%		12.37	12.37	0.00	219.42	219.42	0.00
8	172.16.32.198	3.53%		11.86	11.86	0.00	266.13	266.13	0.00
9	Administrator	3.32%		11.15	11.15	0.00	145.27	145.27	0.00
10	172.16.161.65	3.11%		10.43	10.43	0.00	105.34	105.34	0.00

图11. 用户统计-活跃会话-排名列表

参数与按钮说明：

- 平均活跃会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户的活跃会话速率的平均值。
- 活跃会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户的活跃会话速率的最大值。
- <趋势图>：点击此按钮，显示指定用户活跃会话数的趋势图。
- <基于服务的统计>：点击此按钮，显示指定用户访问的相关服务的活跃会话数的排名情况。
- <基于服务类型的统计>：点击此按钮，显示指定用户访问的相关服务类型的活跃会话数的排名情况。
- <基于 URL 的统计>：点击此按钮，显示指定用户访问的 URL 的活跃会话数的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示指定用户访问的 URL 类型的活跃会话数的排名情况。
- <基于线路的统计>：点击该按钮，显示指定用户在多条出口链路上的的活跃会话数的排名情况。

21.3 用户组统计

21.3.1 流量统计

功能描述：以用户组为统计对象，对其收发的流量、速率进行排名统计。

配置路径：【统计分析】>【用户组统计】>【流量统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

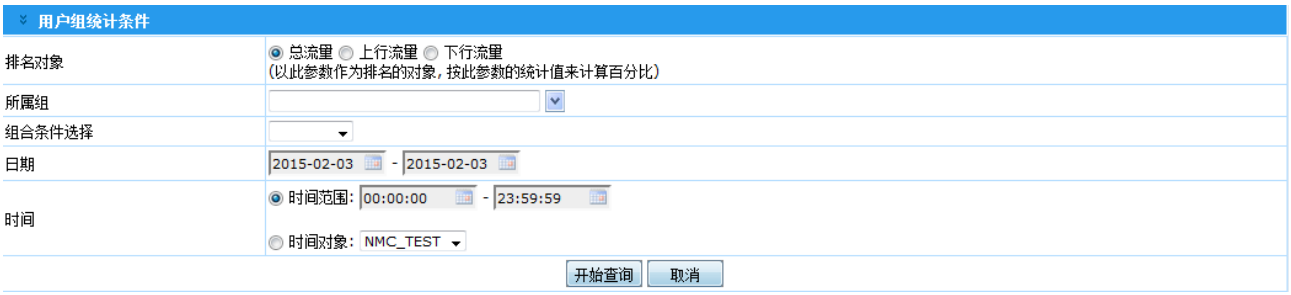


图12. 用户组统计-流量统计-统计条件

参数说明：

- 排名对象：以总流量、上行流量、或下行流量为对象进行排名。
- 所属组：选择需要进行流量排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 组合条件选择：选择需要进行流量排名统计的服务名称/网站名称/网站类型/出口线路。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的用户组中，每个用户组的流量占总流量的比例。[柱图]显示排名前十的用户组的流量及排名。

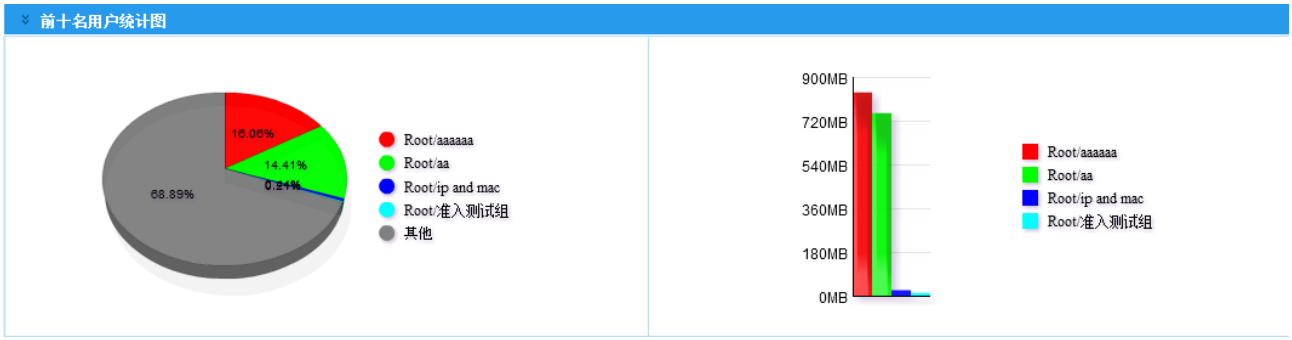


图13. 用户组统计-流量统计-前十名统计图

第三、 排名列表。显示符合统计条件的用户组的排名情况。

用户组排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	用户组	百分比	详细	流量(Byte)			平均速率(bps)			峰值速率(bps)		
				总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		5.09G	1.88G	3.21G	974.33K	359.37K	614.95K			
1	Root/aaaaaa	16.06%		836.48M	75.35M	761.13M	156.45K	14.09K	142.35K	4.25M	166.56K	4.09M
2	Root/aa	14.41%		750.77M	332.49M	418.28M	140.42K	62.19K	78.23K	1.21M	986.29K	1.15M
3	Root/ip and mac	0.44%		22.85M	10.16M	12.69M	4.27K	1.90K	2.37K	50.84K	4.00K	46.84K
4	Root/准入测试组	0.21%		10.76M	1.29M	9.47M	2.01K	247.68	1.77K	202.03K	6.51K	195.52K

图14.　　用户组统计-流量统计-排名列表

参数与按钮说明：

- 流量：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户组传输流量的累计值。
- 平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户组传输速率的平均值。
- 峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户组传输速率的最大值。
- <趋势图>：点击此按钮，显示指定用户组传输速率的趋势图。
- <基于用户的统计>：点击此按钮，显示指定用户组包含的所有用户(包括该组的直接用户和子组包含的用户)访问网络的流量、传输速率的排名情况。
- <基于子用户组的统计>：点击此按钮，显示指定用户组包含的直接子组访问网络的流量、传输速率的排名情况。如包含多级子组，可以一级一级往下看。
- <基于服务的统计>：点击此按钮，显示指定用户组访问的服务的流量、传输速率的排名情况。
- <基于服务类型的统计>：点击此按钮，显示指定用户组访问的服务类型的流量、传输速率的排名情况。
- <基于 URL 的统计>：点击此按钮，显示指定用户组访问的 URL 的流量、传输速率的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示指定用户组访问的 URL 类型的流量、传输速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定用户组在多条出口链路上的流量、速率的分布与排名情况。

21.3.2 会话统计

功能描述：以用户组为统计对象，对其新建会话数、新建会话速率进行排名统计。

配置路径：【统计分析】>【用户组统计】>【会话统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第四、　统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

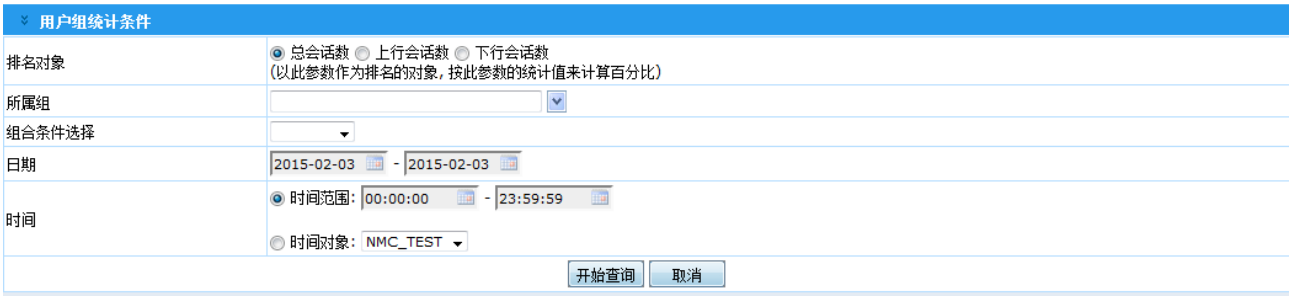


图15.　　用户组统计-会话统计-统计条件

参数说明：

- 排名对象：以总会话数、上行会话数、或下行会话数为对象进行排名。
- 所属组：选择需要进行会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 组合条件选择：选择需要进行会话排名统计的服务名称/网站名称/网站类型/出口线路。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第五、　前十名统计图。[饼图]显示排名前十的用户组中，每个用户组的会话数占总会话数的比例。[柱图]显示排名前十的用户组的会话数及排名。

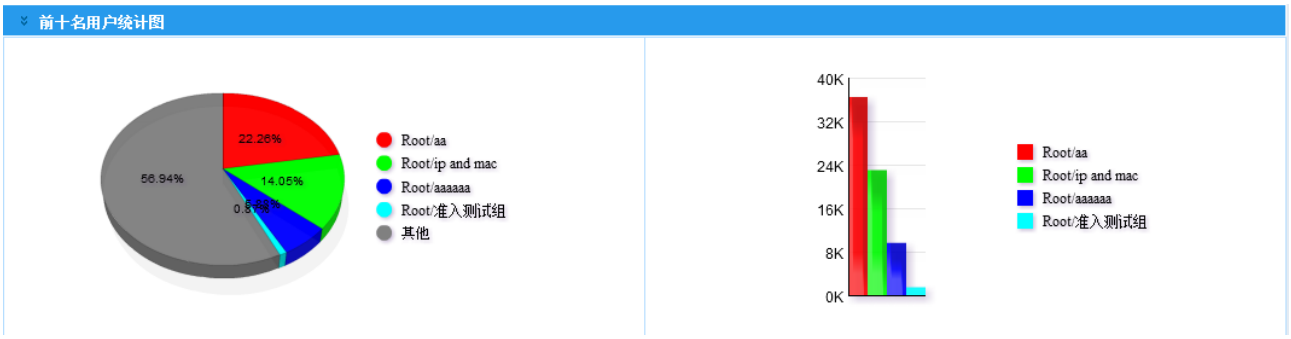


图16.　　用户组统计-会话统计-前十名统计图

第六、　排名列表。显示符合统计条件的用户组的排名情况。

序号	用户组	百分比	详细	新建会话数			新建会话平均速率(sps)			新建会话峰值速率(sps)		
				总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		360.69K	360.45K	230	4.17	4.17	0.00			
1	Root/aa	17.75%		64.04K	64.04K	0	0.74	0.74	0.00	12.71	12.71	0.00
2	Root/准入测试组	3.99%		14.38K	14.38K	4	0.17	0.17	0.00	3.31	3.31	0.00
3	Root/aaaaaa	1.62%		5.85K	5.85K	0	0.07	0.07	0.00	1.33	1.33	0.00
4	Root/深圳	0.04%		147	147	0	0.00	0.00	0.00	0.28	0.28	0.00

图17.　　用户组统计-会话统计-排名列表

参数与按钮说明：

- 新建会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户组新建会话的累计值。
- 新建会话平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户组新建会话速率的平均值。

- 新建会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户组新建会话速率的最大值。
- <趋势图>：点击此按钮，显示指定用户组新建会话速率的趋势图。
- <基于用户的统计>：点击此按钮，显示指定用户组包含的所有用户(包括该组的直接用户和子组包含的用户)访问网络的新建会话数、新建会话速率的排名情况。
- <基于子用户组的统计>：点击此按钮，显示指定用户组包含的直接子组访问网络的新建会话数、新建会话速率的排名情况。如包含多级子组，可以一级一级往下看。
- <基于服务的统计>：点击此按钮，显示指定用户组访问的相关服务的新建会话数、新建会话速率的排名情况。
- <基于服务类型的统计>：点击此按钮，显示指定用户组访问的相关服务类型的新建会话数、新建会话速率的排名情况。
- <基于 URL 的统计>：点击此按钮，显示指定用户组访问的 URL 的新建会话数、新建会话速率的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示指定用户组访问的 URL 类型的新建会话数、新建会话速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定用户组在多条出口链路上的新建会话数、新建会话速率的排名情况。

21.3.3 活跃会话

功能描述：以用户组为统计对象，对其活跃会话数进行排名统计。

配置路径：【统计分析】>【用户组统计】>【活跃会话】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第四、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

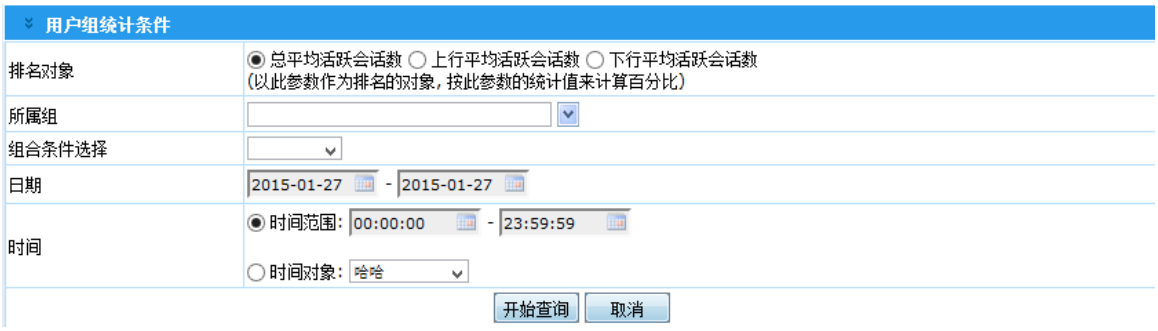


图18. 用户组统计-活跃会话-统计条件

参数说明：

- 排名对象：以总平均活跃会话数、上行活跃会话数、或下行活跃会话数为对象进行排名。
- 所属组：选择需要进行活跃会话数排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 组合条件选择：选择需要进行活跃会话数排名统计的服务名称/网站名称/网站类型/出口线路。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第五、 前十名统计图。[饼图]显示排名前十的用户组中，每个用户组的活跃会话数占总活跃会话数的比例。[柱图]显示排

名前十的用户组的活跃会话数及排名。

图19.　　用户组统计-活跃会话-前十名统计图

第六、　排名列表。显示符合统计条件的用户组的排名情况。

序号	用户组	百分比	详细	平均活跃会话数			峰值活跃会话数		
				总	上行	下行	总	上行	下行
	总计	100.00%		328.82	328.67	0.15			
1	Root/aa	18.59%		61.12	61.12	0.00	704.07	704.07	0.00
2	Root/准入测试组	4.56%		14.99	14.99	0.00	244.42	244.42	0.00
3	Root/aaaaaa	2.86%		9.41	9.41	0.00	96.09	96.09	0.00
4	Root/深圳	0.04%		0.13	0.13	0.00	23.44	23.44	0.00

图20.　　用户组统计-活跃会话-排名列表

参数与按钮说明：

- 平均活跃会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户组的活跃会话速率的平均值。
- 活跃会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个用户组的活跃会话速率的最大值。
- <趋势图>：点击此按钮，显示指定用户组活跃会话数的趋势图。
- <基于用户的统计>：点击此按钮，显示指定用户组包含的所有用户(包括该组的直接用户和子组包含的用户)访问网络的活跃会话数的排名情况。
- <基于子用户组的统计>：点击此按钮，显示指定用户组包含的直接子组访问网络的活跃会话数的排名情况。如包含多级子组，可以一级一级往下看。
- <基于服务的统计>：点击此按钮，显示指定用户组访问的相关服务的活跃会话数的排名情况。
- <基于服务类型的统计>：点击此按钮，显示指定用户组访问的相关服务类型的活跃会话数的排名情况。
- <基于 URL 的统计>：点击此按钮，显示指定用户组访问的 URL 的活跃会话数的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示指定用户组访问的 URL 类型的活跃会话数的排名情况。
- <基于线路的统计>：点击该按钮，显示指定用户组在多条出口链路上的的活跃会话数的排名情况。

21.4服务统计

21.4.1 流量统计

功能描述：以服务为统计对象，对其收发的流量、速率进行排名统计。

配置路径：【统计分析】>【服务统计】>【流量统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

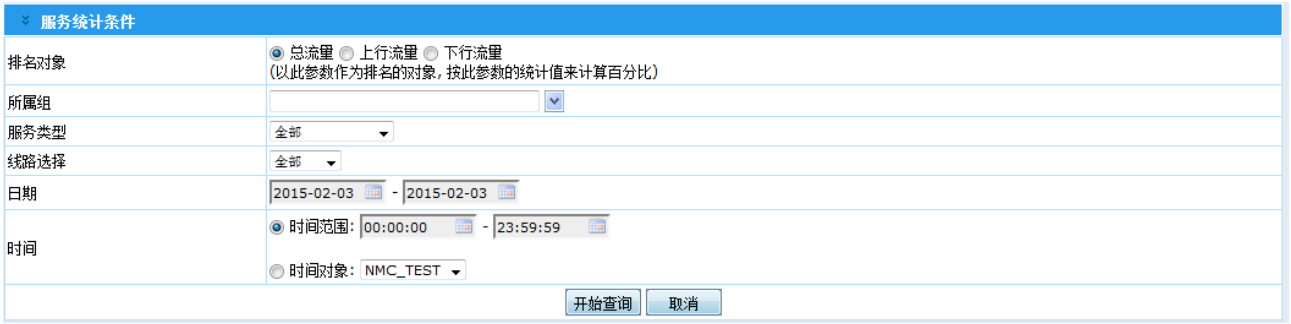


图21. 服务统计-流量统计-统计条件

参数说明：

- 排名对象：以总流量、上行流量、或下行流量为对象进行排名。
- 所属组：选择需要进行流量排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 服务类型：选择需要进行流量排名统计服务的类型，如 WEB 视频、P2P 下载。
- 线路选择：选择需要进行流量排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的服务中，每种服务的流量占总流量的比例。[柱图]显示排名前十的服务的流量及排名。

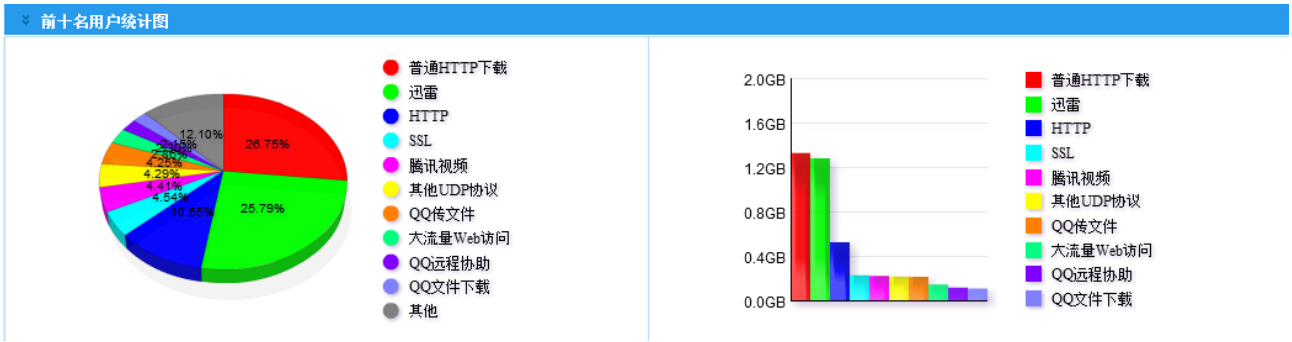


图22. 服务统计-流量统计-前十名统计图

第三、 排名列表。显示符合统计条件的服务的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

序号	服务名称	服务类型	百分比	详细	流量(Byte)			平均速率(bps)			峰值速率(bps)		
					总	上行	下行	总	上行	下行	总	上行	下行
	总计		100.00%		4.96G	1.85G	3.10G	969.15K	362.03K	607.12K			
1	普通HTTP...	HTTP应用	26.75%		1.33G	51.21M	1.28G	259.22K	9.78K	249.44K	5.49M	232.17K	5.26M
2	迅雷	P2P下载	25.79%		1.28G	1.19G	89.64M	249.92K	232.80K	17.12K	713.63K	670.35K	120.19K
3	HTTP	常用服务	10.55%		535.48M	75.02M	460.46M	102.25K	14.33K	87.93K	882.53K	116.26K	766.26K
4	SSL	常用服务	4.54%		230.61M	67.48M	163.13M	44.04K	12.89K	31.15K	485.19K	84.39K	414.15K
5	腾讯视频	流媒体	4.41%		223.80M	7.36M	216.44M	42.74K	1.41K	41.33K	2.25M	63.15K	2.19M
6	其他UDP...	其他服务	4.29%		217.66M	91.40M	126.26M	41.56K	17.45K	24.11K	1.53M	896.14K	977.47K
7	QQ传文件	即时通讯	4.25%		215.82M	209.57M	6.26M	41.21K	40.02K	1.19K	1.78M	1.74M	58.14K
8	大流量We...	HTTP应用	2.86%		145.39M	5.49M	139.90M	27.76K	1.05K	26.72K	668.59K	25.84K	642.75K
9	QQ远程协助	远程控制	2.30%		116.91M	11.63M	105.28M	22.32K	2.22K	20.10K	221.49K	33.97K	206.04K
10	QQ文件下载	即时通讯	2.15%		109.03M	2.62M	106.41M	20.82K	512.88	20.32K	1.47M	37.30K	1.44M

图23.　　服务统计-流量统计-排名列表

参数与按钮说明：

- 流量：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务传输流量的累计值。
- 平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务传输速率的平均值。
- 峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务传输速率的最大值。
- <趋势图>：点击此按钮，显示指定服务传输速率的趋势图。
- <基于用户的统计>：点击此按钮，显示访问指定服务的相关用户的流量、传输速率的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定服务的相关用户组的流量、传输速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定服务在多条出口链路上的流量、速率的分布与排名情况。

21.4.2 会话统计

功能描述：以服务为统计对象，对其新建会话数、新建会话速率进行排名统计。

配置路径：【统计分析】>【服务统计】>【会话统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、　统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

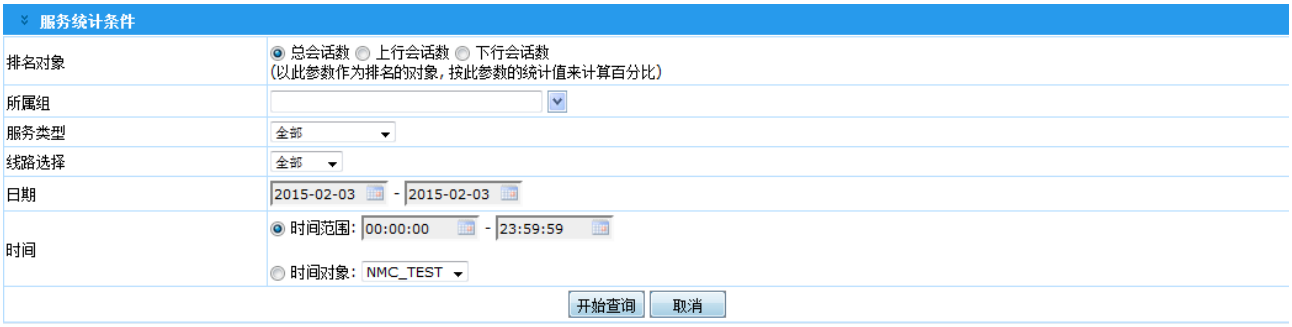


图24.　　服务统计-会话统计-统计条件

参数说明：

- 排名对象：以总会话数、上行会话数、或下行会话数为对象进行排名。
- 所属组：选择需要进行会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 服务类型：选择需要进行会话排名统计服务的类型，如 WEB 视频、P2P 下载。
- 线路选择：选择需要进行会话排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、　前十名统计图。[饼图]显示排名前十的服务中，每种服务的会话数占总会话数的比例。[柱图]显示排名前十的服务的会话数及排名。

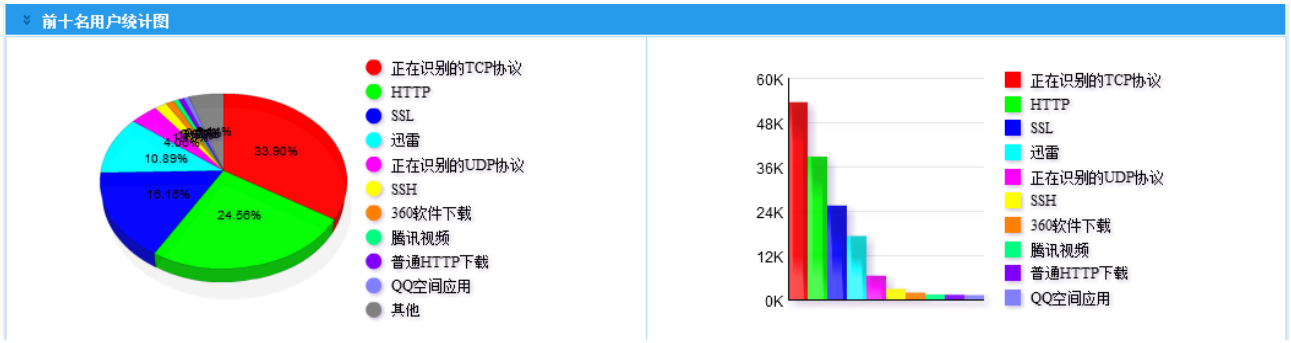


图25.　　服务统计-会话统计-前十名统计图

第三、　排名列表。显示符合统计条件的服务的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

服务排名列表

1 2 3 下一页> 总纪录数为104条!

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	服务名称	服务类型	百分比	详细	新建会话数			新建会话平均速率(sps)			新建会话峰值速率(sps)		
					总	上行	下行	总	上行	下行	总	上行	下行
	总计		100.00%		157.45K	157.15K	300	3.67	3.66	0.01			
1	正在识别的...	其他服务	33.90%		53.37K	53.21K	162	1.24	1.24	0.00	3.91	3.91	0.02
2	HTTP	常用服务	24.56%		38.67K	38.53K	138	0.90	0.90	0.00	7.74	7.73	0.02
3	SSL	常用服务	16.16%		25.45K	25.45K	0	0.59	0.59	0.00	3.33	3.33	0.00
4	迅雷	P2P下载	10.89%		17.15K	17.15K	0	0.40	0.40	0.00	0.64	0.64	0.00
5	正在识别的...	其他服务	4.06%		6.39K	6.39K	0	0.15	0.15	0.00	0.61	0.61	0.00
6	SSH	远程控制	1.78%		2.81K	2.81K	0	0.07	0.07	0.00	0.12	0.12	0.00
7	360软件下...	P2P下载	1.17%		1.83K	1.83K	0	0.04	0.04	0.00	1.62	1.62	0.00
8	腾讯视频	流媒体	0.83%		1.31K	1.31K	0	0.03	0.03	0.00	0.87	0.87	0.00
9	普通HTTP...	HTTP应用	0.80%		1.26K	1.26K	0	0.03	0.03	0.00	0.28	0.28	0.00
10	QQ空间应用	HTTP应用	0.71%		1.12K	1.12K	0	0.03	0.03	0.00	0.55	0.55	0.00

图26.　　服务统计-会话统计-排名列表

参数与按钮说明：

- 新建会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务新建会话的累计值。
- 新建会话平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务新建会话速率的平均值。
- 新建会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务新建会话速率的最大值。
- <趋势图>：点击此按钮，显示指定服务新建会话速率的趋势图。
- <基于用户的统计>：点击此按钮，显示访问指定服务的相关用户的新建会话数、新建会话速率的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定服务的相关用户组的的新建会话数、新建会话速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定服务在多条出口链路上的新建会话数、新建会话速率分布与排名情况。

21.4.3 活跃会话

功能描述：以服务为统计对象，对其活跃会话数进行排名统计。

配置路径：【统计分析】>【服务统计】>【活跃会话】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、　统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

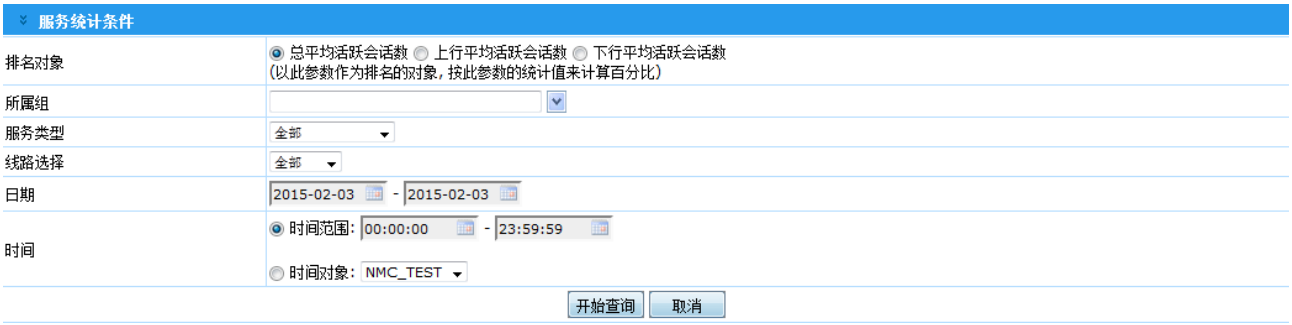


图27.　　服务统计-活跃会话-统计条件

参数说明：

- 排名对象：以总平均活跃会话数、上行平均活跃会话数、或下行平均活跃会话数为对象进行排名。
- 所属组：选择需要进行活跃会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 服务类型：选择需要进行活跃会话排名统计服务的类型，如 WEB 视频、P2P 下载。
- 线路选择：选择需要进行活跃会话排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的服务中，每种服务的活跃会话数占总活跃会话数的比例。[柱图]显示排名前十的服务的活跃会话数及排名。

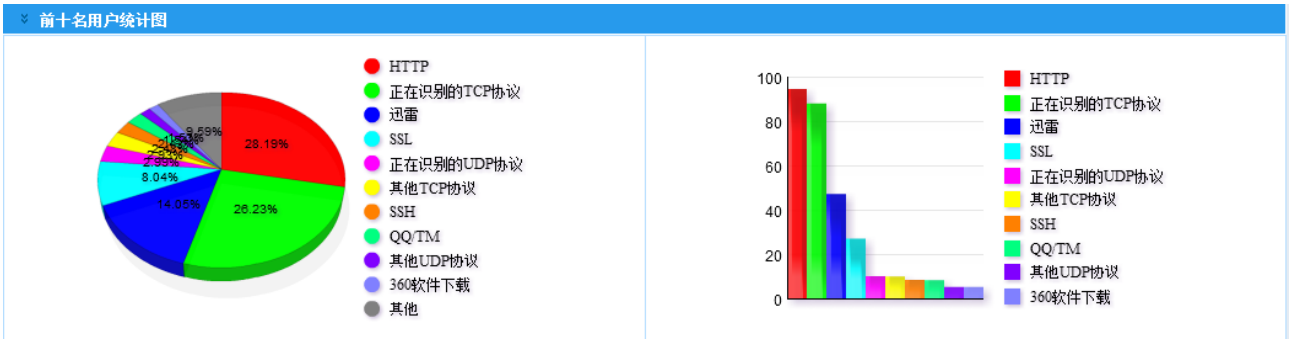


图28.　　服务统计-活跃会话-前十名统计图

第三、 排名列表。显示符合统计条件的服务的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

服务排名列表

1 2 3 下一页> 总纪录数为104条!

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	服务名称	服务类型	百分比	详细	平均活跃会话数			峰值活跃会话数		
					总	上行	下行	总	上行	下行
	总计		100.00%		335.14	334.79	0.36			
1	HTTP	常用服务	28.19%		94.47	94.39	0.08	858.07	858.01	1.67
2	正在识别的TC...	其他服务	26.23%		87.91	87.64	0.28	365.26	365.19	1.74
3	迅雷	P2P下载	14.05%		47.10	47.10	0.00	80.04	80.04	0.00
4	SSL	常用服务	8.04%		26.95	26.95	0.00	155.63	155.63	0.00
5	正在识别的UD...	其他服务	2.99%		10.02	10.02	0.00	43.23	43.23	0.00
6	其他TCP协议	其他服务	2.93%		9.81	9.81	0.00	34.84	34.84	0.00
7	SSH	远程控制	2.48%		8.30	8.30	0.00	17.15	17.15	0.00
8	QQ/TM	即时通讯	2.43%		8.16	8.16	0.00	30.80	30.80	0.00
9	其他UDP协议	其他服务	1.54%		5.15	5.15	0.00	25.12	25.12	0.00
10	360软件下载	P2P下载	1.53%		5.11	5.11	0.00	162.19	162.19	0.00

图29.　　服务统计-活跃会话-排名列表

参数与按钮说明：

- 平均活跃会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务的活跃会话速率的平均值。
- 活跃会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务的活跃会话速率的最大值。
- <趋势图>：点击此按钮，显示指定服务活跃会话数的趋势图。
- <基于用户的统计>：点击此按钮，显示访问指定服务的相关用户的活跃会话数的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定服务的相关用户组的活跃会话数的排名情况。
- <基于线路的统计>：点击该按钮，显示指定服务在多条出口链路上的活跃会话数的分布与排名情况。

21.5 服务类型统计

21.5.1 流量统计

功能描述：以服务类型为统计对象，对其收发的流量、速率进行排名统计。

配置路径：【统计分析】>【服务类型统计】>【流量统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、　统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

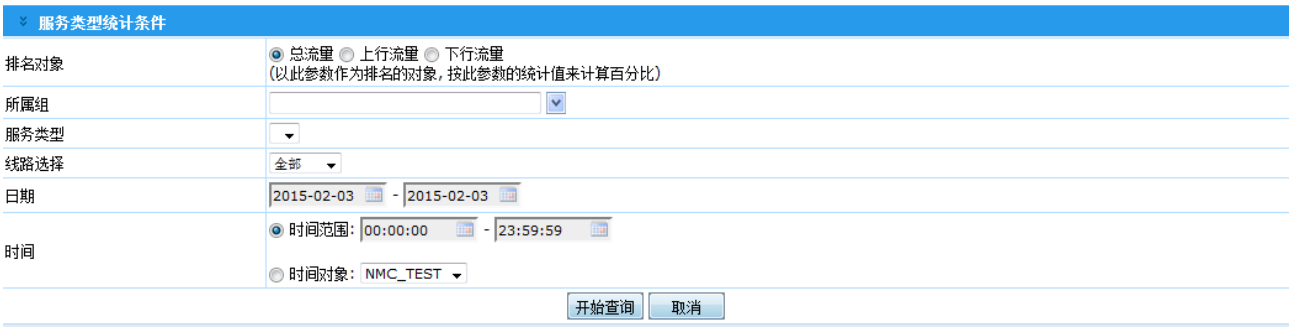


图30.　　服务类型统计-流量统计-统计条件

参数说明：

- 排名对象：以总流量、上行流量、或下行流量为对象进行排名。
- 所属组：选择需要进行流量排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 线路选择：选择需要进行流量排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、　前十名统计图。[饼图]显示排名前十的服务类型中，每种服务类型的流量占总流量的比例。[柱图]显示排名前十的服务类型的流量及排名。

图31.　　服务类型统计-流量统计-前十名统计图

第三、　排名列表。显示符合统计条件的服务类型的排名情况。

序号	服务名称	服务类型	百分比	详细	流量			平均速率			峰值速率		
					总	上行	下行	总	上行	下行	总	上行	下行
	总计		100.00%		12.33G	3.17G	9.16G	1.56M	410.33K	1.16M			
1	迅雷	P2P下载	38.19%		4.71G	622.29M	4.10G	609.66K	78.67K	530.99K	31.92M	2.17M	29.75M
2	百度网盘(上传)	网络存储	11.62%		1.43G	1.39G	42.02M	185.46K	180.15K	5.31K	6.14M	5.97M	174.03K
3	百度网盘	网络存储	8.52%		1.05G	48.26M	1.00G	136.06K	6.10K	129.96K	11.07M	378.43K	10.70M
4	HTTP	常用服务	7.27%		918.71M	129.34M	789.36M	116.14K	16.35K	99.79K	969.01K	134.78K	834.22K
5	普通HTTP下载	HTTP应用	5.36%		676.77M	24.75M	652.03M	85.56K	3.13K	82.43K	2.06M	64.26K	2.00M
6	百度文库	网络存储	5.12%		646.58M	21.48M	625.09M	81.74K	2.72K	79.02K	8.48M	226.24K	8.26M
7	SSL	常用服务	3.85%		486.67M	198.41M	288.26M	61.53K	25.08K	36.44K	632.35K	521.59K	588.67K
8	其他TCP协议	其他服务	2.14%		270.41M	20.14M	250.27M	34.19K	2.55K	31.64K	1.26M	122.30K	1.23M

图32.　　服务类型统计-流量统计-排名列表

参数与按钮说明：

- 流量：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务类型传输流

量的累计值。

- 平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务类型传输速率的平均值。
- 峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务类型传输速率的最大值。
- <趋势图>：点击此按钮，显示指定服务类型传输速率的趋势图。
- <基于服务的统计>：点击此按钮，显示指定服务类型里被访问的相关服务的流量、传输速率的排名情况。
- <基于用户的统计>：点击此按钮，显示访问指定服务类型的相关用户的流量、传输速率的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定服务类型的相关用户组的流量、传输速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定服务类型在多条出口链路上的流量、速率的分布与排名情况。

21.5.2 会话统计

功能描述：以服务类型为统计对象，对其新建会话数、新建会话速率进行排名统计。

配置路径：【统计分析】>【服务类型统计】>【会话统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第四、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

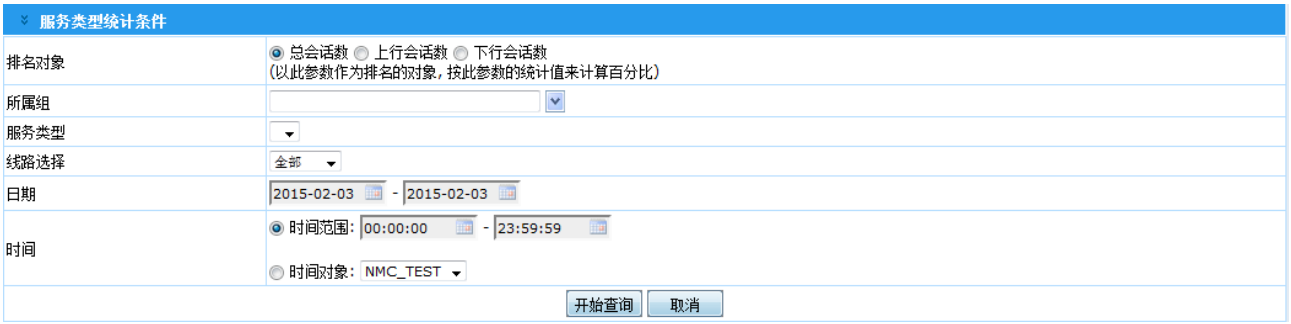


图33. 服务类型统计-会话统计-统计条件

参数说明：

- 排名对象：以总会话数、上行会话数、或下行会话数为对象进行排名。
- 所属组：选择需要进行会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 线路选择：选择需要进行会话排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第五、 前十名统计图。[饼图]显示排名前十的服务类型中，每种服务类型的会话数占总会话数的比例。[柱图]显示排名前十的服务类型的会话数及排名。

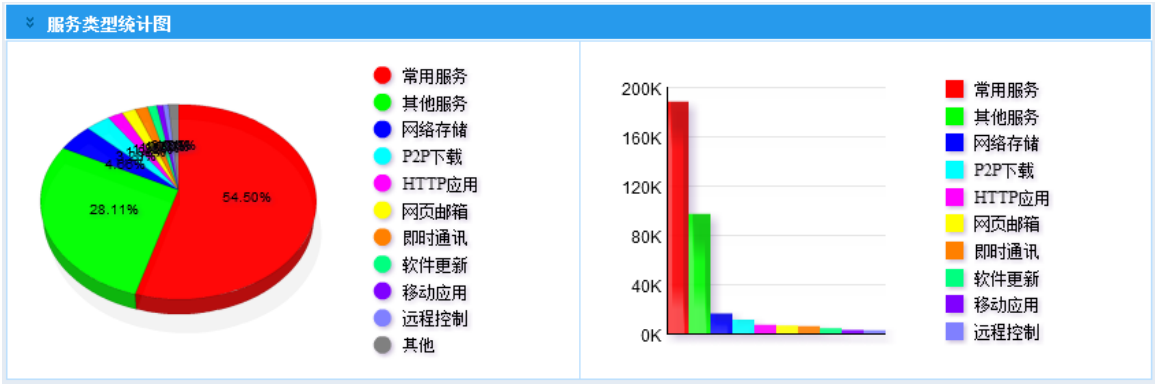


图34.　　服务类型统计-会话统计-前十名统计图

第六、　排名列表。显示符合统计条件的服务类型的排名情况。

服务类型排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	服务类型	百分比	详细	新建会话数			新建会话平均速率			新建会话峰值速率		
				总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		344.94K	344.52K	417	5.30	5.29	0.01			
1	常用服务	54.50%		187.98K	187.94K	44	2.89	2.89	0.00	6.61	6.61	0.02
2	其他服务	28.11%		96.97K	96.61K	364	1.49	1.48	0.01	7.28	7.28	0.03
3	网络存储	4.66%		16.08K	16.08K	0	0.25	0.25	0.00	1.12	1.12	0.00
4	P2P下载	3.20%		11.04K	11.04K	0	0.17	0.17	0.00	3.65	3.65	0.00
5	HTTP应用	1.98%		6.85K	6.85K	0	0.11	0.11	0.00	1.48	1.48	0.00
6	网页邮箱	1.82%		6.27K	6.27K	0	0.10	0.10	0.00	0.45	0.45	0.00
7	即时通讯	1.66%		5.72K	5.72K	0	0.09	0.09	0.00	2.02	2.02	0.00
8	软件更新	1.23%		4.23K	4.23K	0	0.06	0.06	0.00	2.08	2.08	0.00
9	移动应用	0.80%		2.77K	2.77K	0	0.04	0.04	0.00	0.40	0.40	0.00
10	远程控制	0.71%		2.45K	2.44K	9	0.04	0.04	0.00	0.06	0.06	0.01
11	视频网站浏览	0.66%		2.29K	2.29K	0	0.04	0.04	0.00	0.67	0.67	0.00
12	流媒体	0.36%		1.25K	1.25K	0	0.02	0.02	0.00	0.54	0.54	0.00
13	WEB视频	0.09%		305	305	0	0.00	0.00	0.00	0.08	0.08	0.00
14	网络游戏	0.04%		141	141	0	0.00	0.00	0.00	0.18	0.18	0.00
15	网络电话	0.04%		125	125	0	0.00	0.00	0.00	0.16	0.16	0.00
16	股票行情	0.03%		111	111	0	0.00	0.00	0.00	0.18	0.18	0.00
17	网上银行	0.01%		44	44	0	0.00	0.00	0.00	0.06	0.06	0.00
18	FTP应用	0.00%		2	2	0	0.00	0.00	0.00	0.00	0.00	0.00

图35.　　服务类型统计-会话统计-排名列表

参数与按钮说明：

- 新建会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务类型新建会话的累计值。
- 新建会话平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务类型新建会话速率的平均值。
- 新建会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务类型新建会话速率的最大值。
- <趋势图>：点击此按钮，显示指定服务类型新建会话速率的趋势图。
- <基于服务的统计>：点击此按钮，显示指定服务类型里被访问的相关服务的新建会话数、新建会话速率的排名情况。
- <基于用户的统计>：点击此按钮，显示访问指定服务类型的相关用户的新建会话数、新建会话速率的排名情况。

- <基于用户组的统计>：点击此按钮，显示访问指定服务类型的相关用户组的的新建会话数、新建会话速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定服务类型在多条出口链路上的新建会话数、新建会话速率分布与排名情况。

21.5.3 活跃会话

功能描述：以服务类型为统计对象，对其活跃会话数进行排名统计。

配置路径：【统计分析】>【服务类型统计】>【活跃会话】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

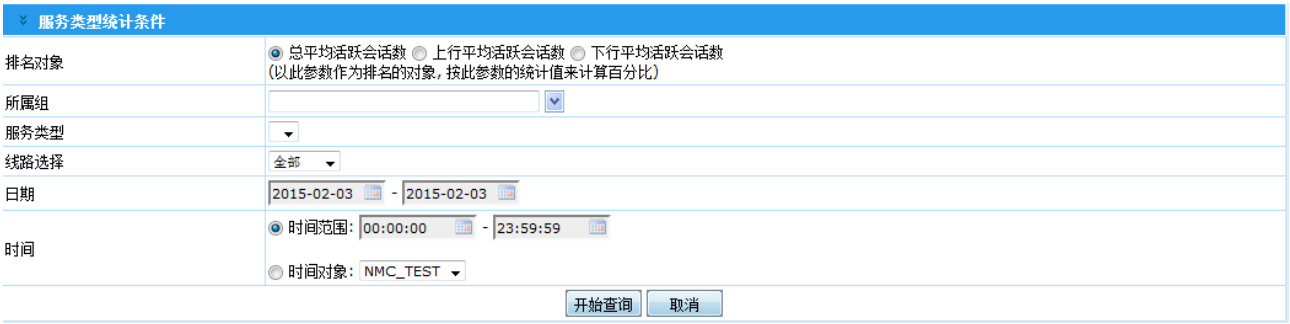


图36. 服务类型统计-活跃会话-统计条件

参数说明：

- 排名对象：以总平均活跃会话数、上行平均活跃会话数、或下行平均活跃会话数为对象进行排名。
- 所属组：选择需要进行活跃会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 线路选择：选择需要进行活跃会话排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的服务类型中，每种服务类型的活跃会话数占总活跃会话数的比例。[柱图]显示排名前十的服务类型的活跃会话数及排名。

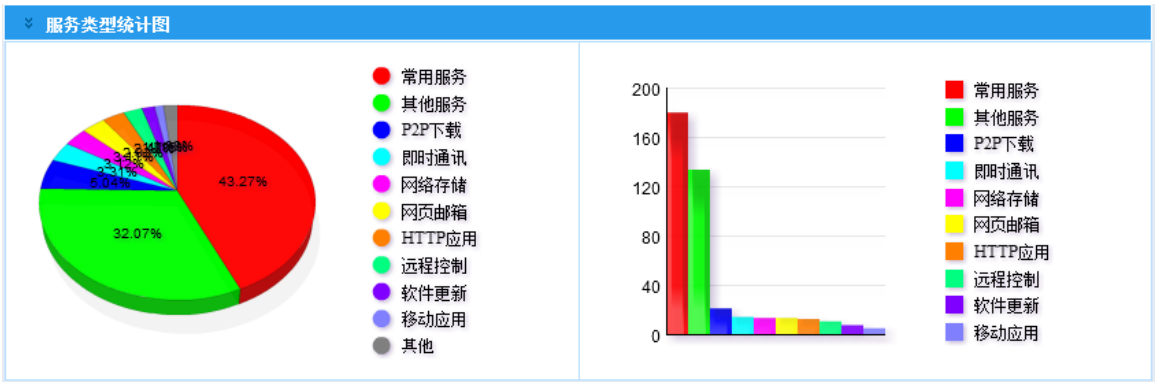


图37. 服务类型统计-活跃会话-前十名统计图

第三、 排名列表。显示符合统计条件的服务类型的排名情况。

服务类型排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	服务类型	百分比	详细	平均活跃会话数			峰值活跃会话数		
				总	上行	下行	总	上行	下行
	总计	100.00%		415.30	412.46	2.84			
1	常用服务	43.27%		179.70	179.63	0.07	934.48	934.48	1.20
2	其他服务	32.07%		133.19	132.57	0.62	575.45	574.38	2.92
3	P2P下载	5.04%		20.92	20.92	0.00	502.89	502.89	0.00
4	即时通讯	3.31%		13.75	13.75	0.00	234.84	234.84	0.00
5	网络存储	3.12%		12.95	12.95	0.00	82.77	82.77	0.00
6	网页邮箱	3.11%		12.90	12.90	0.00	49.08	49.08	0.00
7	HTTP应用	2.93%		12.18	12.18	0.00	153.24	153.24	0.00
8	远程控制	2.48%		10.31	8.15	2.16	361.49	181.73	179.76
9	软件更新	1.70%		7.07	7.07	0.00	221.34	221.34	0.00
10	移动应用	1.15%		4.76	4.76	0.00	45.63	45.63	0.00
11	视频网站浏览	0.90%		3.74	3.74	0.00	72.20	72.20	0.00
12	流媒体	0.54%		2.23	2.23	0.00	65.42	65.42	0.00
13	WEB视频	0.15%		0.62	0.62	0.00	7.58	7.58	0.00
14	网络游戏	0.06%		0.26	0.26	0.00	20.16	20.16	0.00
15	网络电话	0.06%		0.25	0.25	0.00	15.60	15.60	0.00
16	股票行情	0.04%		0.16	0.16	0.00	17.33	17.33	0.00
17	网上银行	0.01%		0.06	0.06	0.00	4.45	4.45	0.00
18	FTP应用	0.00%		0.01	0.01	0.00	1.38	1.38	0.00

图38.　　服务类型统计-活跃会话-排名列表

参数与按钮说明：

- 平均活跃会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务类型的活跃会话速率的平均值。
- 活跃会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某种服务类型的活跃会话速率的最大值。
- <趋势图>：点击此按钮，显示指定服务类型活跃会话数的趋势图。
- <基于服务的统计>：点击此按钮，显示指定服务类型里被访问的相关服务的活跃会话数的排名情况。
- <基于用户的统计>：点击此按钮，显示访问指定服务类型的相关用户的活跃会话数的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定服务类型的相关用户组的活跃会话数的排名情况。
- <基于线路的统计>：点击该按钮，显示指定服务类型在多条出口链路上的活跃会话数的分布与排名情况。

21.6 URL 统计

21.6.1 流量统计

功能描述：以 URL 为统计对象，对其收发的流量、速率进行排名统计。

配置路径：【统计分析】>【 URL 统计】>【流量统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

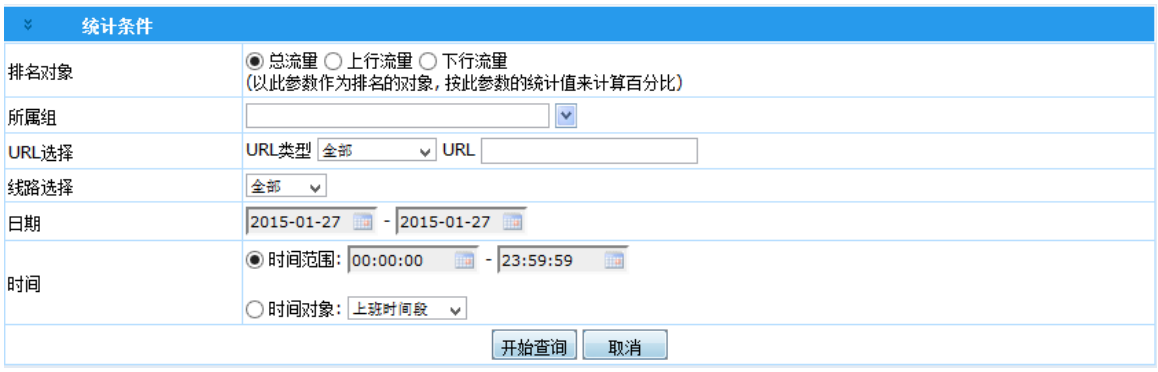


图39.　　URL 统计-流量统计-统计条件

参数说明：

- 排名对象：以总流量、上行流量、或下行流量为对象进行排名。
- 所属组：选择需要进行流量排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- URL 选择：选择需要进行流量排名统计的 URL 类型或者单个 URL。
- 线路选择：选择需要进行流量排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第二、　前十名统计图。[饼图]显示排名前十的 URL 中，每个 URL 的流量占总流量的比例。[柱图]显示排名前十的 URL 的流量及排名。

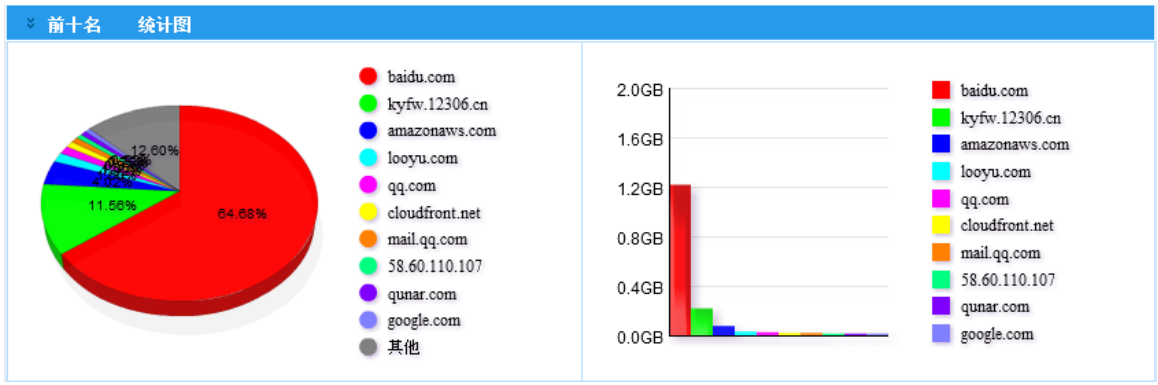


图40.　　URL 统计-流量统计-前十名统计图

第三、　排名列表。显示符合统计条件的 URL 的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

序号		类型	百分比	详细	流量			平均速率			峰值速率		
					总	上行	下行	总	上行	下行	总	上行	下行
	总计		100.00%		1.88G	1.37G	529.01M	241.36K	175.09K	66.26K			
1	baidu.com	搜索引擎	64.68%		1.22G	1.15G	64.55M	156.12K	148.04K	8.09K	4.97M	4.83M	141.36K
2	kyfw.12306.cn	电子银行	11.56%		222.66M	70.13M	152.54M	27.89K	8.78K	19.11K	413.17K	51.43K	361.75K
3	amazonaws.com	其他网站	4.02%		77.38M	74.91M	2.47M	9.69K	9.38K	317.27	518.04K	504.52K	13.52K
4	looyu.com	教学	1.60%		30.84M	1.14M	29.70M	3.86K	145.59	3.72K	832.40K	23.50K	808.90K
5	qq.com	新闻门户	1.32%		25.41M	11.19M	14.23M	3.18K	1.40K	1.78K	56.40K	11.35K	47.77K
6	cloudfront.net	其他网站	1.06%		20.49M	564.38K	19.94M	2.57K	70.69	2.50K	559.42K	15.05K	544.37K
7	mail.qq.com	Webmail	0.97%		18.67M	10.72M	7.96M	2.34K	1.34K	1020.74	26.15K	10.92K	16.78K
8	58.60.110.107	其他网站	0.75%		14.48M	710.41K	13.79M	1.81K	88.99	1.73K	34.33K	1.85K	33.08K
9	qunar.com	其他网站	0.72%		13.89M	2.17M	11.72M	1.74K	278.06	1.47K	60.02K	8.68K	52.62K
10	google.com	搜索引擎	0.72%		13.80M	613.44K	13.20M	1.73K	76.84	1.65K	115.24K	3.92K	111.33K
11	hao123.com	IT相关	0.68%		13.17M	1.38M	11.79M	1.65K	177.41	1.48K	29.69K	3.16K	26.53K
12	sogou.com	搜索引擎	0.63%		12.11M	5.22M	6.89M	1.52K	669.02	884.06	17.82K	7.55K	13.31K
13	122.226.184.133	其他网站	0.41%		7.95M	178.94K	7.77M	1019.39	22.41	996.98	217.02K	4.77K	212.25K
14	sohu.com	新闻门户	0.41%		7.89M	922.56K	6.99M	1011.81	115.56	896.25	115.49K	5.90K	109.70K
15	apple.com	IT相关	0.39%		7.57M	1.66M	5.91M	970.88	213.30	757.58	55.84K	2.84K	52.99K
16	microsoft.com	IT相关	0.35%		6.65M	2.49M	4.16M	852.99	319.68	533.32	11.31K	5.85K	8.32K
17	121.201.33.146	其他网站	0.31%		6.03M	935.06K	5.12M	773.71	117.13	656.58	16.07K	3.43K	14.23K
18	sina.com.cn	新闻门户	0.28%		5.44M	519.48K	4.93M	697.26	65.07	632.19	41.26K	4.09K	37.17K
19	people.com.cn	周刊媒体	0.26%		5.00M	367.45K	4.64M	641.61	46.03	595.58	62.65K	3.42K	59.23K
20	sznews.com	新闻门户	0.24%		4.70M	256.15K	4.45M	602.92	32.09	570.83	51.60K	2.69K	48.92K

图41.　　URL 统计-流量统计-排名列表

参数与按钮说明：

- 流量：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 传输流量的累计值。
- 平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 传输速率的平均值。
- 峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 传输速率的最大值。
- <趋势图>：点击此按钮，显示指定 URL 传输速率的趋势图。
- <基于用户的统计>：点击此按钮，显示访问指定 URL 的相关用户的流量、传输速率的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定 URL 的相关用户组的流量、传输速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定 URL 在多条出口链路上的流量、速率的分布与排名情况。

21.6.2 会话统计

功能描述：以 URL 为统计对象，对其新建会话数、新建会话速率进行排名统计。

配置路径：【统计分析】>【 URL 统计】>【会话统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第七、　统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

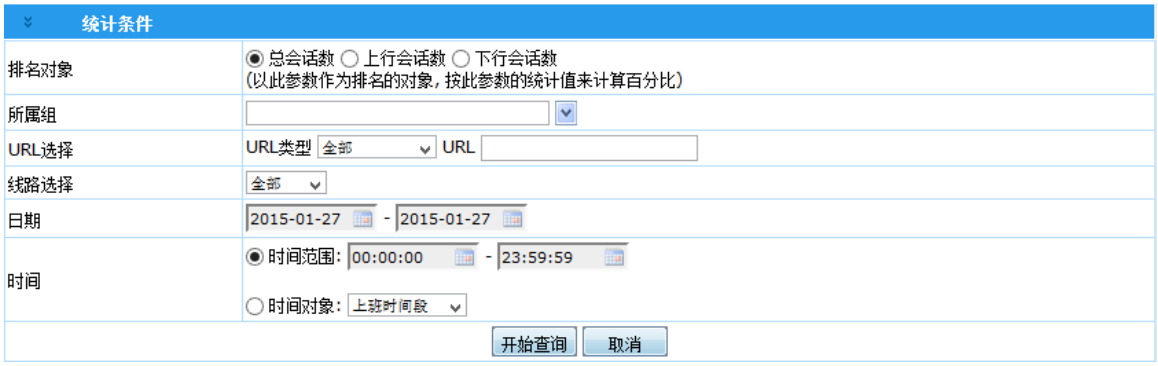


图42.　　URL 统计-会话统计-统计条件

参数说明：

- 排名对象：以总会话数、上行会话数、或下行会话数为对象进行排名。
- 所属组：选择需要进行会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- URL 选择：选择需要进行会话排名统计的 URL 类型或者单个 URL。
- 线路选择：选择需要进行会话排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第八、　前十名统计图。[饼图]显示排名前十的 URL 中，每个 URL 的会话数占总会话数的比例。[柱图]显示排名前十的 URL 的会话数及排名。

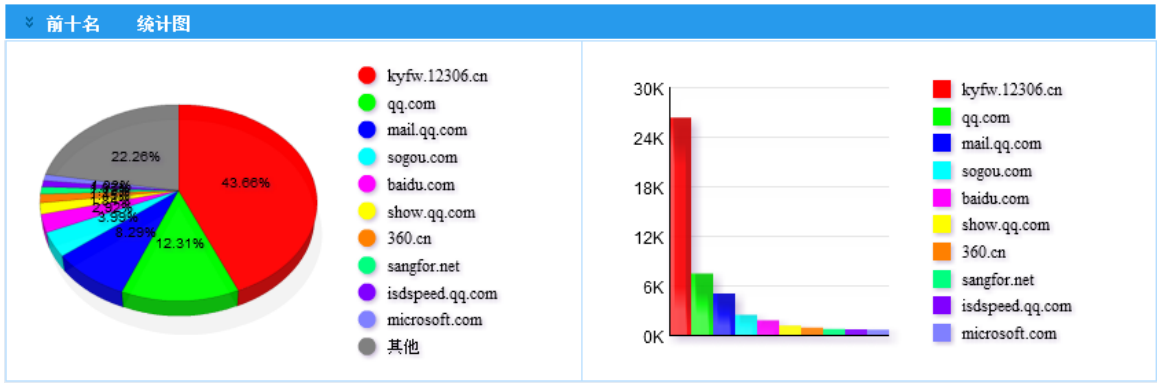


图43.　　URL 统计-会话统计-前十名统计图

第九、　排名列表。显示符合统计条件的 URL 的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

排名列表

1 2 3 4 5 6 7 8 9 10 ... 下一页> 记录数大于750条!

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号		类型	百分比	详细	新建会话数			新建会话平均速率			新建会话峰值速率		
					总	上行	下行	总	上行	下行	总	上行	下行
	总计		100.00%		60.18K	60.18K	0	0.92	0.92	0.00			
1	kyfw.12306.cn	电子银行	43.66%		26.28K	26.28K	0	0.40	0.40	0.00	2.76	2.76	0.00
2	qq.com	新闻门户	12.31%		7.41K	7.41K	0	0.11	0.11	0.00	0.69	0.69	0.00
3	mail.qq.com	Webmail	8.29%		4.99K	4.99K	0	0.08	0.08	0.00	0.45	0.45	0.00
4	sogou.com	搜索引擎	3.99%		2.40K	2.40K	0	0.04	0.04	0.00	0.26	0.26	0.00
5	baidu.com	搜索引擎	2.92%		1.76K	1.76K	0	0.03	0.03	0.00	0.26	0.26	0.00
6	show.qq.com	交友聊天	1.84%		1.11K	1.11K	0	0.02	0.02	0.00	0.12	0.12	0.00
7	360.cn	软件下载	1.45%		873	873	0	0.01	0.01	0.00	0.21	0.21	0.00
8	sangfor.net	公司企业	1.19%		715	715	0	0.01	0.01	0.00	0.12	0.12	0.00
9	isdspeed.qq.com	交友聊天	1.07%		645	645	0	0.01	0.01	0.00	0.35	0.35	0.00
10	microsoft.com	IT相关	1.03%		620	620	0	0.01	0.01	0.00	0.15	0.15	0.00
11	video.qq.com	电影	0.98%		591	591	0	0.01	0.01	0.00	0.32	0.32	0.00
12	hao123.com	IT相关	0.65%		393	393	0	0.01	0.01	0.00	0.10	0.10	0.00
13	taobao.com	网上购物	0.65%		392	392	0	0.01	0.01	0.00	0.12	0.12	0.00
14	apple.com	IT相关	0.65%		391	391	0	0.01	0.01	0.00	0.07	0.07	0.00
15	xunlei.com	电影	0.62%		374	374	0	0.01	0.01	0.00	0.20	0.20	0.00

图44.　　URL 统计-会话统计-排名列表

参数与按钮说明：

- 新建会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 新建会话的累计值。
- 新建会话平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 新建会话速率的平均值。
- 新建会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 新建会话速率的最大值。
- <趋势图>：点击此按钮，显示指定 URL 新建会话速率的趋势图。
- <基于用户的统计>：点击此按钮，显示访问指定 URL 的相关用户的新建会话数、新建会话速率的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定 URL 的相关用户组的的新建会话数、新建会话速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定 URL 在多条出口链路上的新建会话数、新建会话速率分布与排名情况。

21.6.3 活跃会话

功能描述：以 URL 为统计对象，对其活跃会话数进行排名统计。

配置路径：【统计分析】>【 URL 统计】>【活跃会话】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第四、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

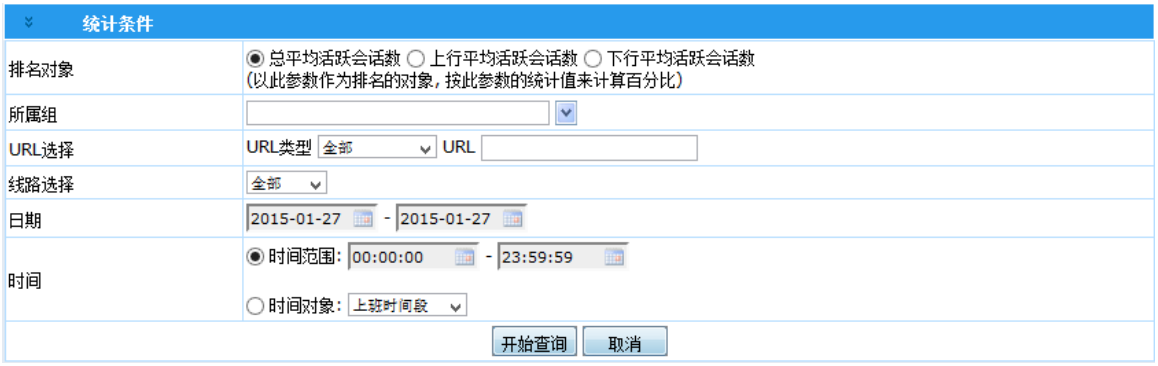


图45.　　URL 统计-活跃会话-统计条件

参数说明：

- 排名对象：以总平均活跃会话数、上行平均活跃会话数、或下行平均活跃会话数为对象进行排名。
- 所属组：选择需要进行活跃会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- URL 选择：选择需要进行活跃会话排名统计的 URL 类型或者单个 URL。
- 线路选择：选择需要进行活跃会话排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第五、　前十名统计图。[饼图]显示排名前十的 URL 中，每个 URL 的活跃会话数占总活跃会话数的比例。[柱图]显示排名前十的 URL 的活跃会话数及排名。

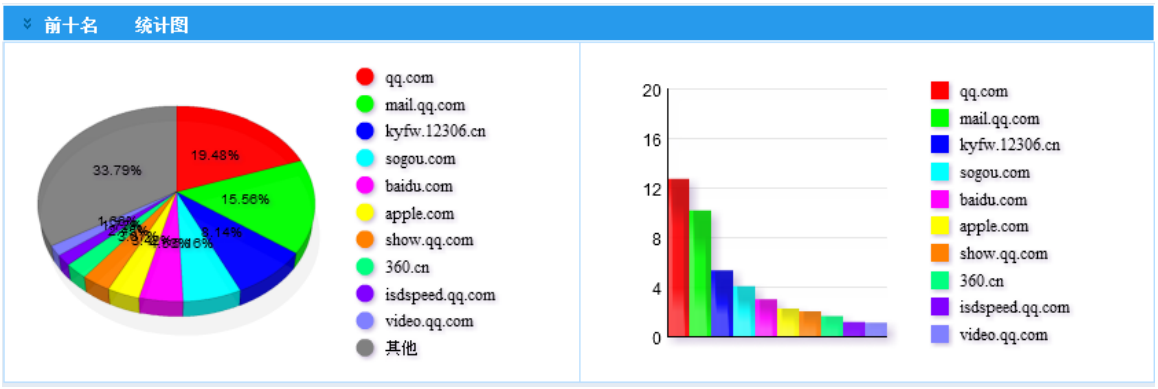


图46.　　URL 统计-活跃会话-前十名统计图

第六、　排名列表。显示符合统计条件的 URL 的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

排名列表

1 2 3 4 5 6 7 8 9 10 ... 下一页> 记录数大于750条!

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号		类型	百分比	详细	平均活跃会话数			峰值活跃会话数		
					总	上行	下行	总	上行	下行
	总计		100.00%		65.20	65.20	0.00			
1	qq.com	新闻门户	19.48%		12.70	12.70	0.00	82.41	82.41	0.00
2	mail.qq.com	Webmail	15.56%		10.14	10.14	0.00	50.25	50.25	0.00
3	kyfw.12306.cn	电子银行	8.14%		5.31	5.31	0.00	29.25	29.25	0.00
4	sogou.com	搜索引擎	6.16%		4.02	4.02	0.00	29.38	29.38	0.00
5	baidu.com	搜索引擎	4.53%		2.96	2.96	0.00	27.70	27.70	0.00
6	apple.com	IT相关	3.42%		2.23	2.23	0.00	16.61	16.61	0.00
7	show.qq.com	交友聊天	3.07%		2.00	2.00	0.00	13.38	13.38	0.00
8	360.cn	软件下载	2.45%		1.60	1.60	0.00	23.63	23.63	0.00
9	isdspeed.qq.com	交友聊天	1.73%		1.13	1.13	0.00	29.11	29.11	0.00
10	video.qq.com	电影	1.66%		1.08	1.08	0.00	30.46	30.46	0.00
11	microsoft.com	IT相关	1.60%		1.04	1.04	0.00	20.96	20.96	0.00
12	taobao.com	网上购物	1.11%		0.73	0.73	0.00	13.77	13.77	0.00
13	rising.cn	新闻门户	1.05%		0.68	0.68	0.00	20.42	20.42	0.00
14	jd.com	网上购物	0.91%		0.59	0.59	0.00	22.97	22.97	0.00

图47.　　URL 统计-活跃会话-排名列表

参数与按钮说明：

- 平均活跃会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 的活跃会话速率的平均值。
- 活跃会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 的活跃会话速率的最大值。
- <趋势图>：点击此按钮，显示指定 URL 活跃会话数的趋势图。
- <基于用户的统计>：点击此按钮，显示访问指定 URL 的相关用户的活跃会话数的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定 URL 的相关用户组的活跃会话数的排名情况。
- <基于线路的统计>：点击该按钮，显示指定 URL 在多条出口链路上的活跃会话数的分布与排名情况。

21.7 URL 类型统计

21.7.1 流量统计

功能描述：以 URL 类型为统计对象，对其收发的流量、速率进行排名统计。

配置路径：【统计分析】>【 URL 类型统计】>【流量统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第四、　统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

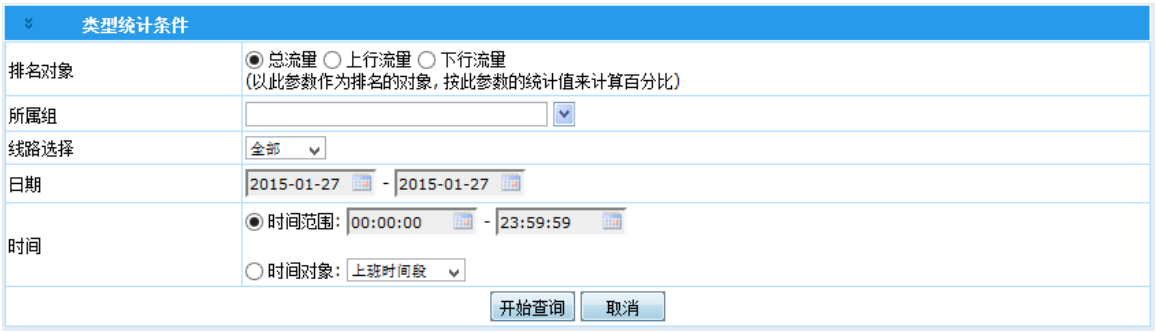


图48.　　URL 类型统计-流量统计-统计条件

参数说明：

- 排名对象：以总流量、上行流量、或下行流量为对象进行排名。
- 所属组：选择需要进行流量排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 线路选择：选择需要进行流量排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第五、　前十名统计图。[饼图]显示排名前十的 URL 类型中，每个 URL 类型的流量占总流量的比例。[柱图]显示排名前十的 URL 类型的流量及排名。

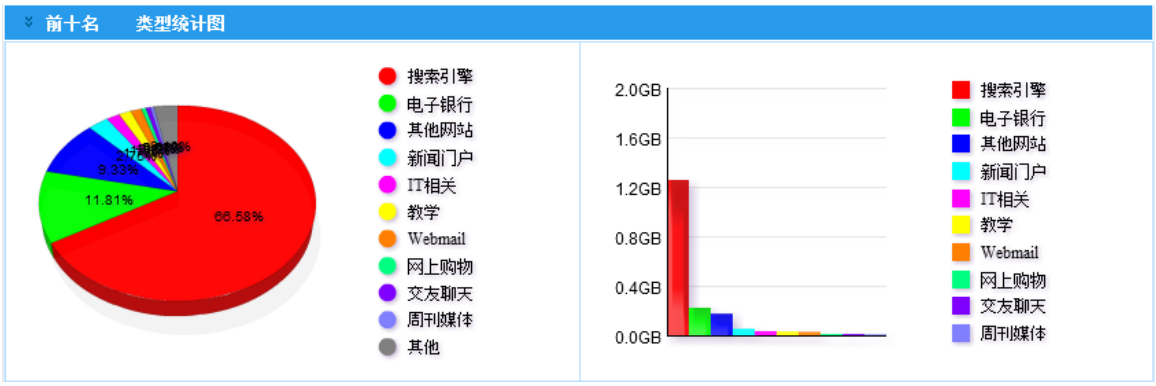


图49.　　URL 类型统计-流量统计-前十名统计图

第六、　排名列表。显示符合统计条件的 URL 类型的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

类型排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	类型	百分比	详细	流量			平均速率			峰值速率		
				总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		1.88G	1.37G	531.31M	239.58K	173.63K	65.95K			
1	搜索引擎	66.58%		1.25G	1.16G	95.31M	159.51K	147.68K	11.83K	4.97M	4.83M	141.36K
2	电子银行	11.81%		227.98M	70.95M	157.03M	28.30K	8.81K	19.49K	413.17K	51.43K	361.75K
3	其他网站	9.33%		180.04M	86.10M	93.95M	22.35K	10.69K	11.66K	559.42K	504.52K	544.37K
4	新闻门户	2.75%		52.99M	11.28M	41.71M	6.58K	1.40K	5.18K	115.49K	11.27K	109.70K
5	IT相关	1.73%		33.35M	6.61M	26.74M	4.14K	840.42	3.32K	55.84K	5.85K	52.99K
6	教学	1.63%		31.49M	1.24M	30.25M	3.91K	157.86	3.75K	832.40K	23.50K	808.90K
7	Webmail	1.40%		27.10M	12.40M	14.70M	3.36K	1.54K	1.82K	34.73K	10.92K	33.51K
8	网上购物	0.63%		12.07M	2.54M	9.53M	1.50K	323.46	1.18K	19.75K	7.66K	12.09K
9	交友聊天	0.59%		11.37M	3.27M	8.10M	1.41K	415.96	1.00K	11.89K	2.93K	11.12K
10	周刊媒体	0.46%		8.81M	1.02M	7.79M	1.09K	129.70	990.46	62.65K	3.42K	59.23K

图50.　　URL 类型统计-流量统计-排名列表

参数与按钮说明：

- 流量：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 类型传输流量的累计值。
- 平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 类型传输速率的平均值。
- 峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 类型传输速率的最大值。
- <趋势图>：点击此按钮，显示指定 URL 类型传输速率的趋势图。
- <基于 URL 的统计>:点击此按钮,显示指定 URL 类型里被访问的相关 URL 的流量、传输速率的排名情况。
- <基于用户的统计>：点击此按钮，显示访问指定 URL 类型的相关用户的流量、传输速率的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定 URL 类型的相关用户组的流量、传输速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定 URL 类型在多条出口链路上的流量、速率的分布与排名情况。

21.7.2 会话统计

功能描述：以 URL 类型为统计对象，对其新建会话数、新建会话速率进行排名统计。

配置路径：【统计分析】>【 URL 类型统计】>【会话统计】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第十、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

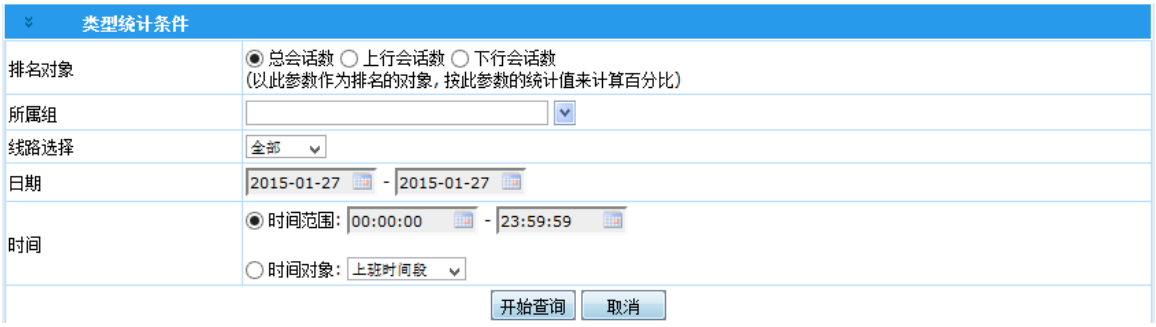


图51. URL 类型统计-会话统计-统计条件

参数说明：

- 排名对象：以总会话数、上行会话数、或下行会话数为对象进行排名。
- 所属组：选择需要进行会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 线路选择：选择需要进行会话排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第十一、前十名统计图。[饼图]显示排名前十的 URL 类型中，每个 URL 类型的会话数占总会话数的比例。[柱图]显示排名前十的 URL 类型的会话数及排名。

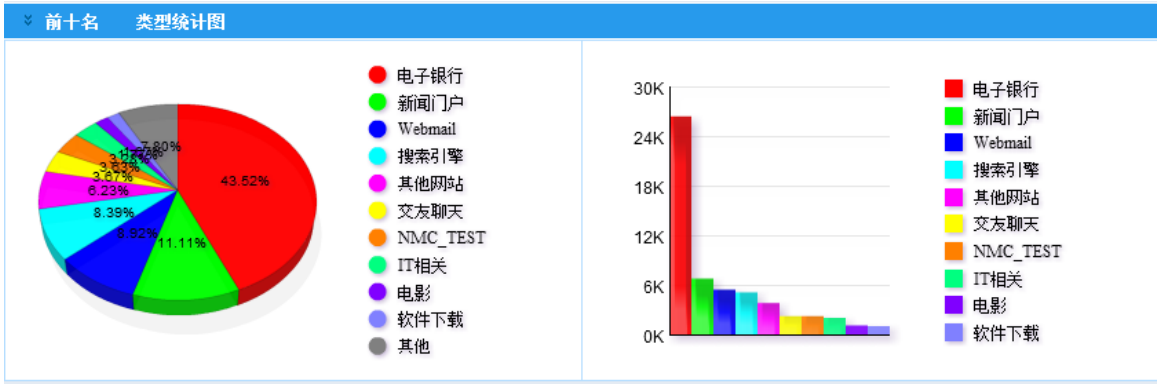


图52. URL 类型统计-会话统计-前十名统计图

第十二、排名列表。显示符合统计条件的 URL 类型的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

类型排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	类型	百分比	详细	新建会话数			新建会话平均速率			新建会话峰值速率		
				总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		60.60K	60.60K	0	0.92	0.92	0.00			
1	电子银行	43.52%		26.38K	26.38K	0	0.40	0.40	0.00	2.76	2.76	0.00
2	新闻门户	11.11%		6.73K	6.73K	0	0.10	0.10	0.00	0.69	0.69	0.00
3	Webmail	8.92%		5.40K	5.40K	0	0.08	0.08	0.00	0.45	0.45	0.00
4	搜索引擎	8.39%		5.08K	5.08K	0	0.08	0.08	0.00	0.26	0.26	0.00
5	其他网站	6.23%		3.78K	3.78K	0	0.06	0.06	0.00	0.19	0.19	0.00
6	交友聊天	3.67%		2.23K	2.23K	0	0.03	0.03	0.00	0.35	0.35	0.00
7	NMC_TEST	3.63%		2.20K	2.20K	0	0.03	0.03	0.00	0.69	0.69	0.00
8	IT相关	3.28%		1.99K	1.99K	0	0.03	0.03	0.00	0.27	0.27	0.00
9	电影	1.77%		1.07K	1.07K	0	0.02	0.02	0.00	0.32	0.32	0.00
10	软件下载	1.67%		1.01K	1.01K	0	0.02	0.02	0.00	0.21	0.21	0.00
11	网上购物	1.57%		950	950	0	0.01	0.01	0.00	0.16	0.16	0.00
12	广告营销	1.19%		722	722	0	0.01	0.01	0.00	0.10	0.10	0.00
13	公司企业	1.18%		718	718	0	0.01	0.01	0.00	0.12	0.12	0.00
14	周刊媒体	0.90%		548	548	0	0.01	0.01	0.00	0.16	0.16	0.00
15	博客	0.38%		233	233	0	0.00	0.00	0.00	0.06	0.06	0.00
16	生活休闲	0.36%		216	216	0	0.00	0.00	0.00	0.18	0.18	0.00
17	土豆	0.31%		187	187	0	0.00	0.00	0.00	0.15	0.15	0.00
18	手机	0.24%		144	144	0	0.00	0.00	0.00	0.07	0.07	0.00

图53. URL 类型统计-会话统计-排名列表

参数与按钮说明：

- 新建会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 类型新建会话的累计值。
- 新建会话平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 类型新建会话速率的平均值。
- 新建会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 类型新建会话速率的最大值。
- <趋势图>：点击此按钮，显示指定 URL 类型新建会话速率的趋势图。
- <基于 URL 的统计>：点击此按钮，显示指定 URL 类型里被访问的相关 URL 的新建会话数、新建会话速率的排名情况。
- <基于用户的统计>：点击此按钮，显示访问指定 URL 类型的相关用户的新建会话数、新建会话速率的排名情况。

- <基于用户组的统计>：点击此按钮，显示访问指定 URL 类型的相关用户组的的新建会话数、新建会话速率的排名情况。
- <基于线路的统计>：点击该按钮，显示指定 URL 类型在多条出口链路上的新建会话数、新建会话速率分布与排名情况。

21.7.3 活跃会话

功能描述：以 URL 类型为统计对象，对其活跃会话数进行排名统计。

配置路径：【统计分析】>【 URL 类型统计】>【活跃会话】

配置描述：该页面分为三部分，分别是：统计条件、前十名统计图、排名列表。

第七、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

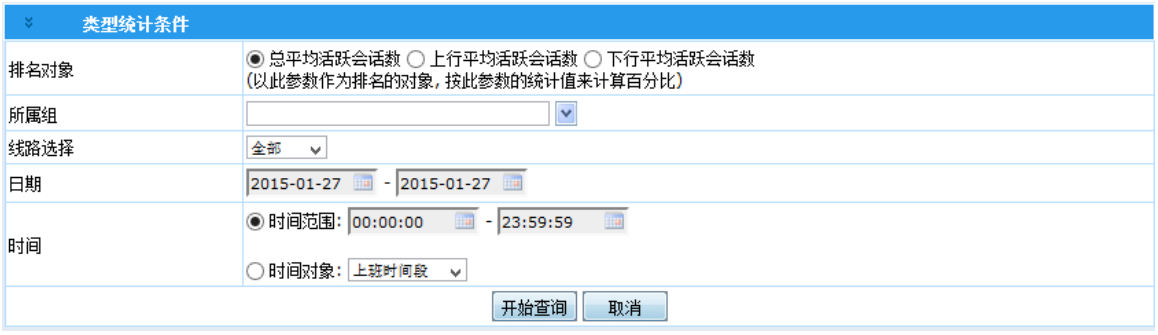


图54. URL 类型统计-活跃会话-统计条件

参数说明：

- 排名对象：以总平均活跃会话数、上行平均活跃会话数、或下行平均活跃会话数为对象进行排名。
- 所属组：选择需要进行活跃会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 线路选择：选择需要进行活跃会话排名统计的出口线路，如 WAN1、WAN2。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[前十名统计图]和[排名列表]中显示，详细说明如后。

第八、 前十名统计图。[饼图]显示排名前十的 URL 类型中，每个 URL 类型的活跃会话数占总活跃会话数的比例。[柱图]显示排名前十的 URL 类型的活跃会话数及排名。

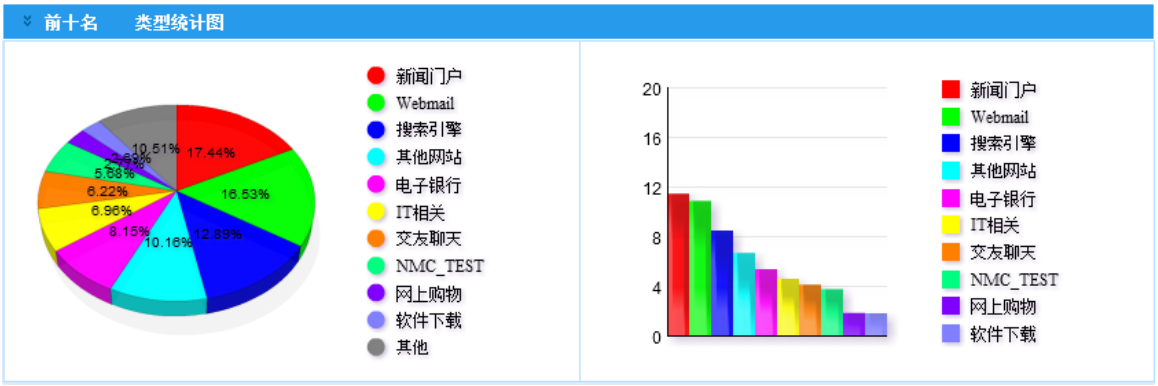


图55. URL 类型统计-活跃会话-前十名统计图

第九、 排名列表。显示符合统计条件的 URL 类型的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<

跳转>到指定页，查看更多信息。

类型排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	类型	百分比	详细	平均活跃会话数			峰值活跃会话数		
				总	上行	下行	总	上行	下行
	总计	100.00%		65.45	65.45	0.00			
1	新闻门户	17.44%		11.42	11.42	0.00	82.41	82.41	0.00
2	Webmail	16.53%		10.82	10.82	0.00	50.25	50.25	0.00
3	搜索引擎	12.89%		8.44	8.44	0.00	29.38	29.38	0.00
4	其他网站	10.16%		6.65	6.65	0.00	21.22	21.22	0.00
5	电子银行	8.15%		5.34	5.34	0.00	29.25	29.25	0.00
6	IT相关	6.96%		4.55	4.55	0.00	21.87	21.87	0.00
7	交友聊天	6.22%		4.07	4.07	0.00	29.11	29.11	0.00
8	NMC_TEST	5.68%		3.72	3.72	0.00	79.57	79.57	0.00
9	网上购物	2.77%		1.81	1.81	0.00	22.97	22.97	0.00
10	软件下载	2.69%		1.76	1.76	0.00	23.63	23.63	0.00
11	电影	2.52%		1.65	1.65	0.00	30.46	30.46	0.00
12	广告营销	1.84%		1.21	1.21	0.00	12.34	12.34	0.00
13	周刊媒体	1.29%		0.84	0.84	0.00	16.19	16.19	0.00
14	博客	0.64%		0.42	0.42	0.00	6.87	6.87	0.00
15	土豆	0.56%		0.36	0.36	0.00	16.77	16.77	0.00
16	生活休闲	0.49%		0.32	0.32	0.00	20.95	20.95	0.00
17	公司企业	0.41%		0.27	0.27	0.00	3.10	3.10	0.00

图56.　　URL 类型统计-活跃会话-排名列表

参数与按钮说明：

- 平均活跃会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 类型的活跃会话速率的平均值。
- 活跃会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 类型的活跃会话速率的最大值。
- <趋势图>：点击此按钮，显示指定 URL 类型活跃会话数的趋势图。
- <基于 URL 的统计>：点击此按钮，显示指定 URL 类型里被访问的相关 URL 的活跃会话数的排名情况。
- <基于用户的统计>：点击此按钮，显示访问指定 URL 类型的相关用户的活跃会话数的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定 URL 类型的相关用户组的活跃会话数的排名情况。
- <基于线路的统计>：点击该按钮，显示指定 URL 类型在多条出口链路上的活跃会话数的分布与排名情况。

21.8线路统计

21.8.1 流量统计

功能描述：以线路为统计对象，对分布于每条线路上的流量、速率进行排名统计。

配置路径：【统计分析】>【线路统计】>【流量统计】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第一、　统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

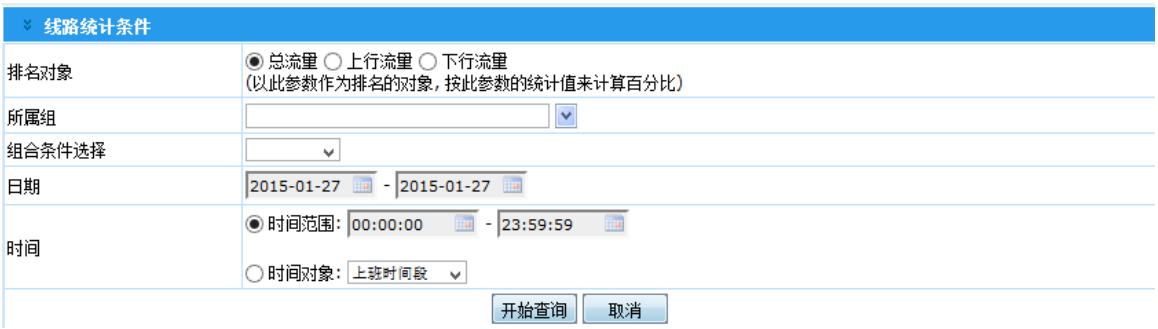


图57.　　线路统计-流量统计-统计条件

参数说明：

- 排名对象：以总流量、上行流量、或下行流量为对象进行排名。
- 所属组：选择需要进行流量排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 组合条件选择：选择需要进行流量排名统计的服务名称/网站名称/网站类型/出口线路。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第二、　统计图。[饼图]显示每条线路的流量占总流量的比例。[柱图]显示每条线路的流量及排名。

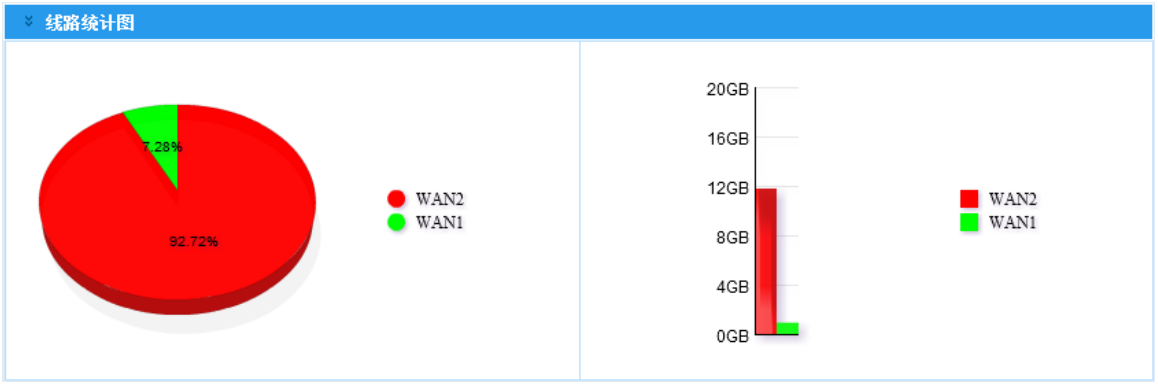
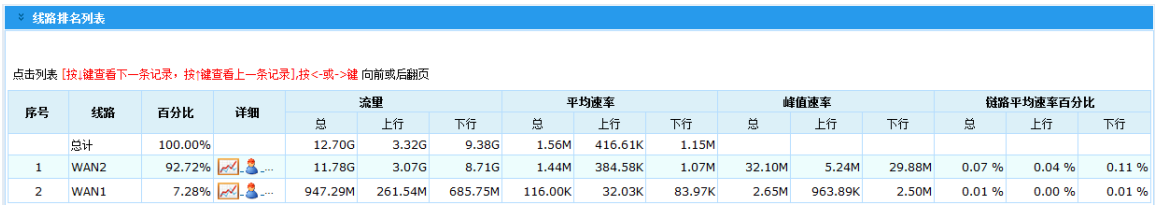


图58.　　线路统计-流量统计-统计图

第三、　排名列表。显示符合统计条件的线路的排名情况。



序号	线路	百分比	详细	流量			平均速率			峰值速率			链路平均速率百分比		
				总	上行	下行	总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		12.70G	3.32G	9.38G	1.56M	416.61K	1.15M						
1	WAN2	92.72%		11.78G	3.07G	8.71G	1.44M	384.58K	1.07M	32.10M	5.24M	29.88M	0.07 %	0.04 %	0.11 %
2	WAN1	7.28%		947.29M	261.54M	685.75M	116.00K	32.03K	83.97K	2.65M	963.89K	2.50M	0.01 %	0.00 %	0.01 %

图59.　　线路统计-流量统计-排名列表

参数与按钮说明：

- 流量：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个线路传输流量的累计值。
- 平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个线路传输速率的平均值。
- 峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个线路传输速

率的最大值。

- <趋势图>：点击此按钮，显示分布于指定线路传输速率的趋势图。
- <基于用户的统计>：点击此按钮，显示分布于指定线路的用户访问网络的流量、传输速率的排名情况。
- <基于用户组的统计>：点击此按钮，显示分布于指定线路的用户组访问网络的流量、传输速率的排名情况。
- <基于服务的统计>：点击此按钮，显示分布于指定线路的被访问的服务的流量、传输速率的排名情况。
- <基于服务类型的统计>：点击此按钮，显示分布于指定线路的被访问的服务类型的流量、传输速率的排名情况。
- <基于 URL 的统计>：点击此按钮，显示分布于指定线路的被访问的 URL 的流量、传输速率的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示分布于指定线路的被访问的 URL 类型的流量、传输速率的排名情况。

21.8.2 会话统计

功能描述：以线路为统计对象，对分布于每条线路上的新建会话数、新建会话速率进行排名统计。

配置路径：【统计分析】>【线路统计】>【会话统计】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

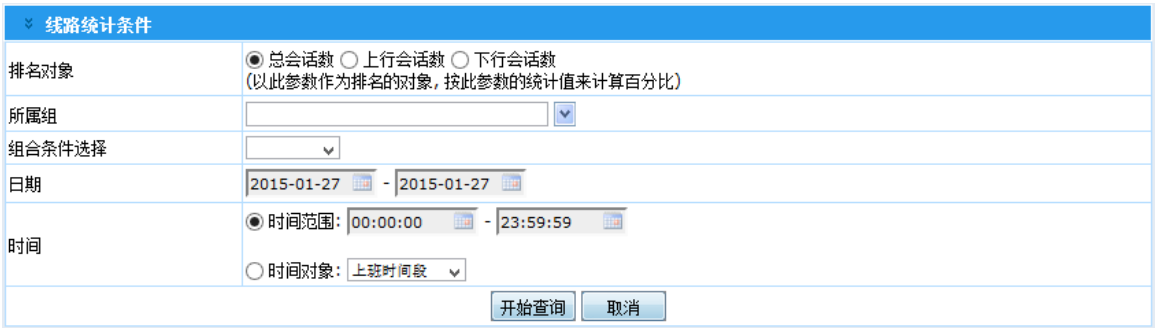


图60. 线路统计-会话统计-统计条件

参数说明：

- 排名对象：以总会话数、上行会话数、或下行会话数为对象进行排名。
- 所属组：选择需要进行会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 组合条件选择：选择需要进行会话排名统计的服务名称/网站名称/网站类型/出口线路。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第二、 统计图。[饼图]显示每条线路的会话数占总会话数的比例。[柱图]显示每条线路的会话及排名。

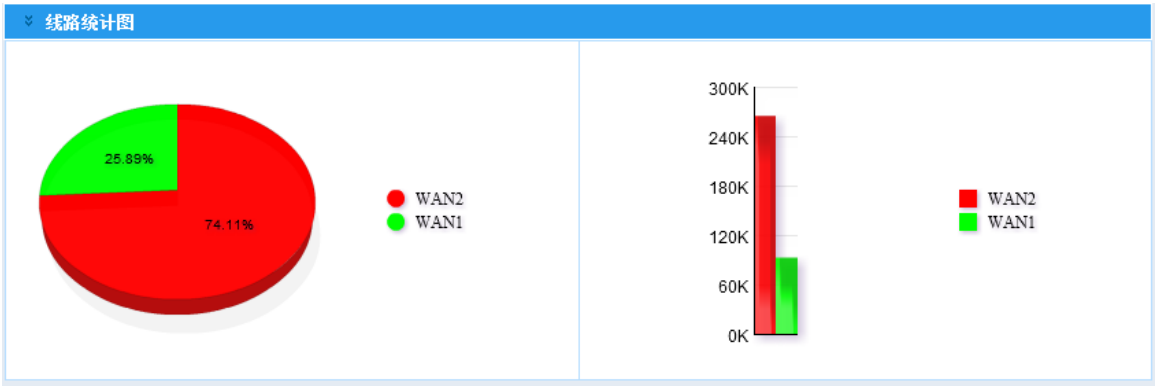
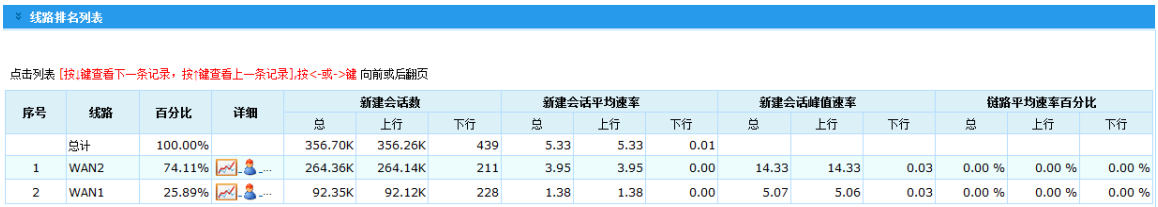


图61.　　线路统计-会话统计-统计图

第三、　排名列表。显示符合统计条件的线路的排名情况。



序号	线路	百分比	详细	新建会话数			新建会话平均速率			新建会话峰值速率			链路平均速率百分比		
				总	上行	下行	总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		356.70K	356.26K	439	5.33	5.33	0.01						
1	WAN2	74.11%		264.36K	264.14K	211	3.95	3.95	0.00	14.33	14.33	0.03	0.00 %	0.00 %	0.00 %
2	WAN1	25.89%		92.35K	92.12K	228	1.38	1.38	0.00	5.07	5.06	0.03	0.00 %	0.00 %	0.00 %

图62.　　线路统计-会话统计-排名列表

参数与按钮说明：

- 新建会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个线路新建会话的累计值。
- 新建会话平均速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个线路新建会话速率的平均值。
- 新建会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个线路新建会话速率的最大值。
- <趋势图>：点击此按钮，显示分布于指定线路新建会话速率的趋势图。
- <基于用户的统计>：点击此按钮，显示分布于指定线路的用户访问网络的新建会话数、新建会话速率的排名情况。
- <基于用户组的统计>：点击此按钮，显示分布于指定线路的用户组访问网络的新建会话数、新建会话速率的排名情况。
- <基于服务的统计>：点击此按钮，显示分布于指定线路的被访问的服务的新建会话数、新建会话速率的排名情况。
- <基于服务类型的统计>：点击此按钮，显示分布于指定线路的被访问的服务类型的新建会话数、新建会话速率的排名情况。
- <基于 URL 的统计>：点击此按钮，显示分布于指定线路的被访问的 URL 的新建会话数、新建会话速率的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示分布于指定线路的被访问的 URL 类型的新建会话数、新建会话速率的排名情况。

21.8.3 活跃会话

功能描述：以线路为统计对象，对分布于每条线路上的活跃会话数进行排名统计。

配置路径：【统计分析】>【线路统计】>【活跃会话】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

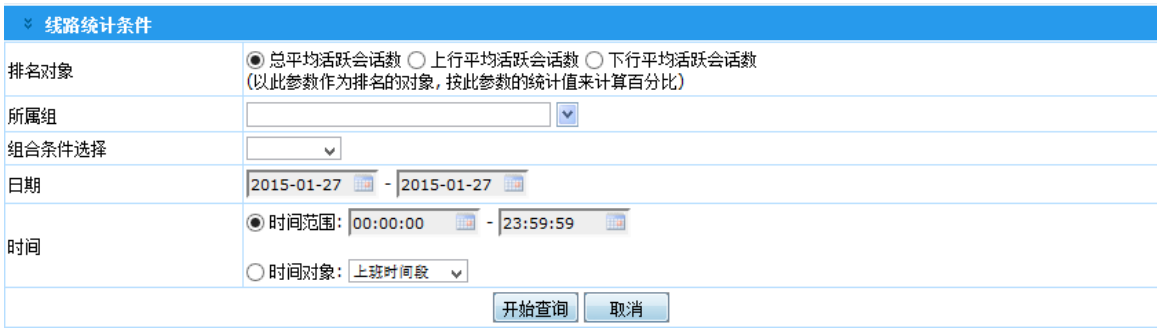


图63. 线路统计-活跃会话-统计条件

参数说明：

- 排名对象：以总平均活跃会话数、上行平均活跃会话数、或下行平均活跃会话数为对象进行排名。
- 所属组：选择需要进行活跃会话排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 组合条件选择：选择需要进行活跃会话数排名统计的服务名称/网站名称/网站类型/出口线路。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第二、 统计图。[饼图]显示每条线路的活跃会话数占总活跃会话数的比例。[柱图]显示每条线路的活跃会话数及排名。

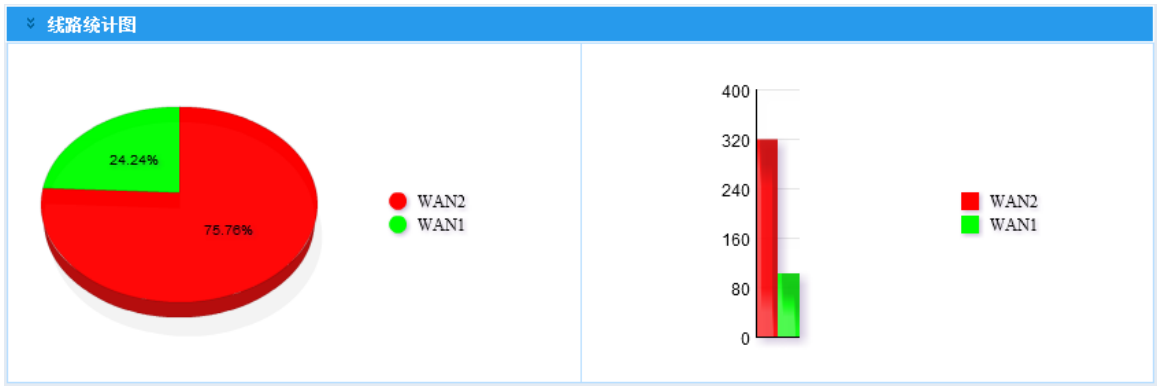


图64. 线路统计-活跃会话-统计图

第三、 排名列表。显示符合统计条件的线路的排名情况。

序号	线路	百分比	详细	平均活跃会话数			峰值活跃会话数			链路平均速率百分比		
				总	上行	下行	总	上行	下行	总	上行	下行
	总计	100.00%		420.74	417.95	2.80						
1	WAN2	75.76%		318.75	317.96	0.79	1.34K	1.34K	60.28	0.00 %	0.00 %	0.00 %
2	WAN1	24.24%		102.00	99.99	2.01	524.55	484.19	179.76	0.00 %	0.00 %	0.00 %

图65. 线路统计-活跃会话-排名列表

参数与按钮说明：

- 平均活跃会话数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个线路的活跃会话速率的平均值。
- 活跃会话峰值速率：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个线路的活跃会话速率的最大值。
- <趋势图>：点击此按钮，显示分布于指定线路活跃会话数的趋势图。
- <基于用户的统计>：点击此按钮，显示分布于指定线路的用户访问网络的活跃会话数的排名情况。
- <基于用户组的统计>：点击此按钮，显示分布于指定线路的用户组访问网络的活跃会话数的排名情况。
- <基于服务的统计>：点击此按钮，显示分布于指定线路的被访问的服务的活跃会话数的排名情况。
- <基于服务类型的统计>：点击此按钮，显示分布于指定线路的被访问的服务类型的活跃会话数的排名情况。
- <基于 URL 的统计>：点击此按钮，显示分布于指定线路的被访问的 URL 的活跃会话数的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示分布于指定线路的被访问的 URL 类型的活跃会话数的排名情况。

21.9 URL 访问量统计

21.9.1 基于 URL 统计

功能描述：以 URL 为统计对象，对 URL 被访问的次数进行排名统计。

配置路径：【统计分析】>【URL 访问量】>【基于 URL】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

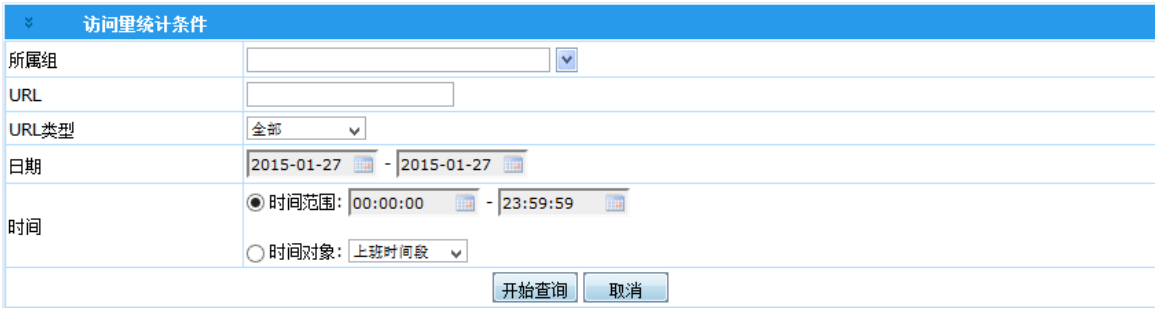


图66. URL 访问量-基于 URL-统计条件

参数说明：

- 所属组：选择需要进行流量排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- URL：选择需要进行统计排名的 URL 或 URL 关键字。
- URL 类型：选择需要进行统计排名的 URL 类型，如博客、WebMail 等。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的 URL 中，每个 URL 的访问量占总访问量的比例。[柱图]显示排名前十的 URL 的访问量及排名。

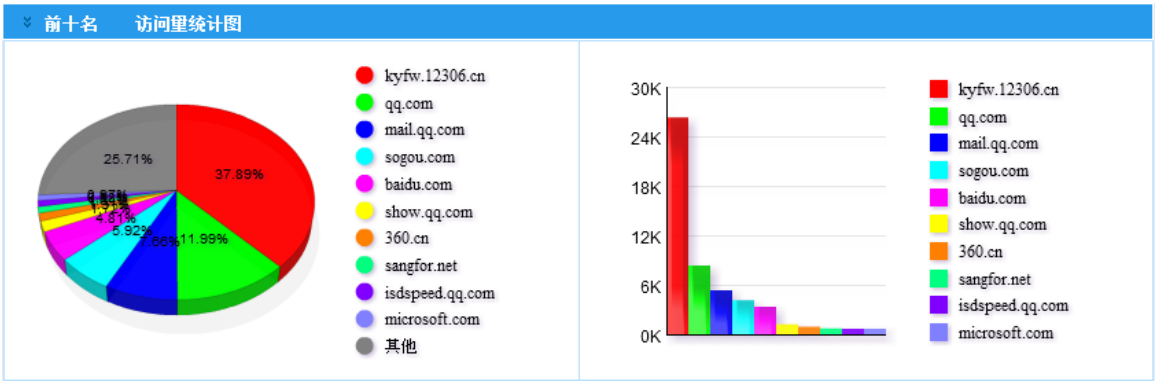


图67. URL 访问量-基于 URL-统计图

第三、 排名列表。显示符合统计条件的 URL 访问次数的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

序号		类型	访问次数	百分比	详细
	总计		69380	100.00%	
1	kyfw.12306.cn	电子银行	26286	37.89%	
2	qq.com	新闻门户	8318	11.99%	
3	mail.qq.com	Webmail	5315	7.66%	
4	sogou.com	搜索引擎	4104	5.92%	
5	baidu.com	搜索引擎	3340	4.81%	
6	show.qq.com	交友聊天	1192	1.72%	
7	360.cn	软件下载	908	1.31%	
8	sangfor.net	公司企业	724	1.04%	
9	isdspeed.qq.com	交友聊天	677	0.98%	
10	microsoft.com	IT相关	675	0.97%	
11	121.201.33.146	其他网站	670	0.97%	
12	video.qq.com	电影	620	0.89%	
13	hao123.com	IT相关	585	0.84%	
14	sohu.com	新闻门户	484	0.70%	
15	taobao.com	网上购物	445	0.64%	
16	apple.com	IT相关	423	0.61%	
17	xunlei.com	电影	385	0.55%	

图68. URL 访问量-基于 URL-排名列表

参数与按钮说明：

- 访问次数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 被访问的次数的累计值。
- <趋势图>：点击此按钮，显示指定 URL 在各时刻被访问的次数的趋势图。
- <基于用户的统计>：点击此按钮，显示访问指定 URL 的相关用户的访问次数的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定 URL 的相关用户组的访问次数的排名情况。

21.9.2 基于 URL 类型统计

功能描述：以 URL 类型为统计对象，对 URL 被访问的次数进行排名统计。

配置路径：【统计分析】>【URL 访问量】>【基于 URL 类型】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

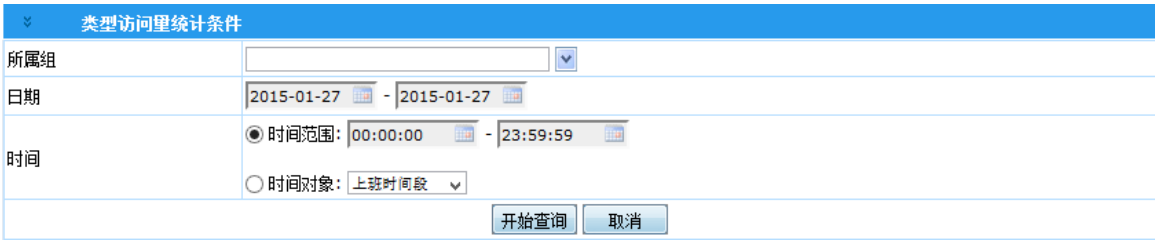


图69. URL 访问量-基于 URL 类型-统计条件

参数说明：

- 所属组：选择需要进行流量排名统计的用户组。点击<选择组>按钮，进行用户组的选择。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的 URL 类型中，每个 URL 类型的访问量占总访问量的比例。[柱图]显示排名前十的 URL 类型的访问量及排名。

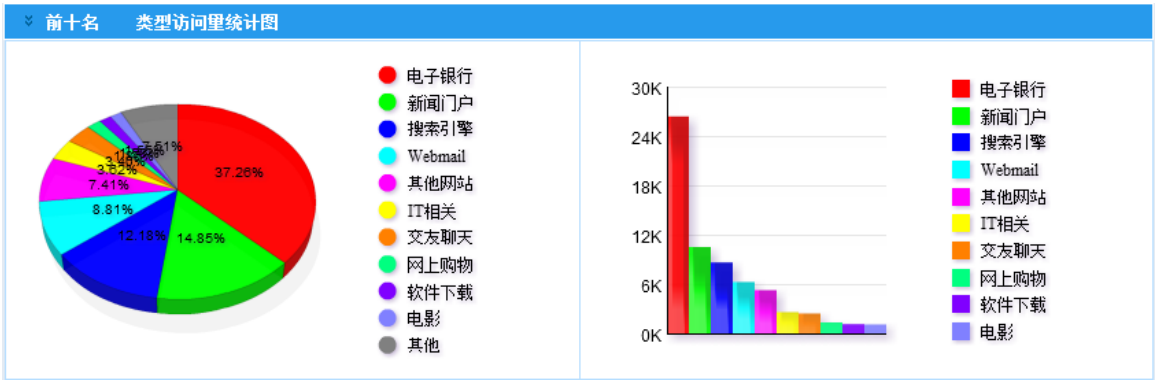


图70. URL 访问量-基于 URL 类型-统计图

第三、 排名列表。显示符合统计条件的 URL 访问次数的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

类型访问里排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	类型	访问次数	百分比	详细
	总计	70809	100.00%	
1	电子银行	26383	37.26%	
2	新闻门户	10513	14.85%	
3	搜索引擎	8622	12.18%	
4	Webmail	6235	8.81%	
5	其他网站	5244	7.41%	
6	IT相关	2561	3.62%	
7	交友聊天	2408	3.40%	
8	网上购物	1316	1.86%	
9	软件下载	1116	1.58%	
10	电影	1094	1.55%	
11	公司企业	952	1.34%	
12	广告营销	898	1.27%	
13	周刊媒体	815	1.15%	

图71. URL 访问量-基于 URL 类型-排名列表

参数与按钮说明：

- 访问次数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 被访问的次数的累计值。
- <趋势图>：点击此按钮，显示指定 URL 类型在各时刻被访问的次数的趋势图。
- <基于 URL 的统计>：点击此按钮，显示指定 URL 类型里被访问的相关 URL 的访问次数的排名情况。
- <基于用户的统计>：点击此按钮，显示访问指定 URL 类型的相关用户的访问次数的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定 URL 类型的相关用户组的访问次数的排名情况。

21.9.3 基于用户统计

功能描述：以用户为统计对象，对 URL 被访问的次数进行排名统计。

配置路径：【统计分析】>【URL 访问量】>【基于用户】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

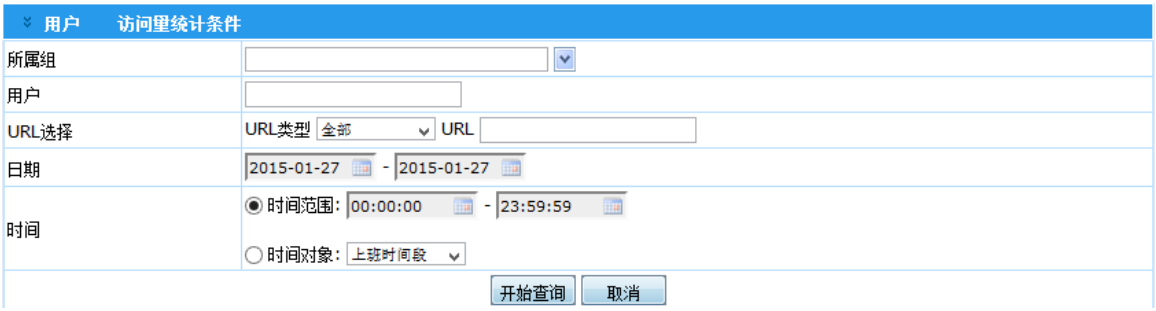


图72. URL 访问量-基于用户-统计条件

参数说明：

- 所属组：选择需要进行访问次数排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 用户：输入需要进行访问次数排名统计的用户。
- URL 选择：选择需要进行访问次数排名统计的 URL 类型/URL 关键字。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的用户中，每个用户的访问量占总访问量的比例。[柱图]显示排名前十的用户的访问量及排名。

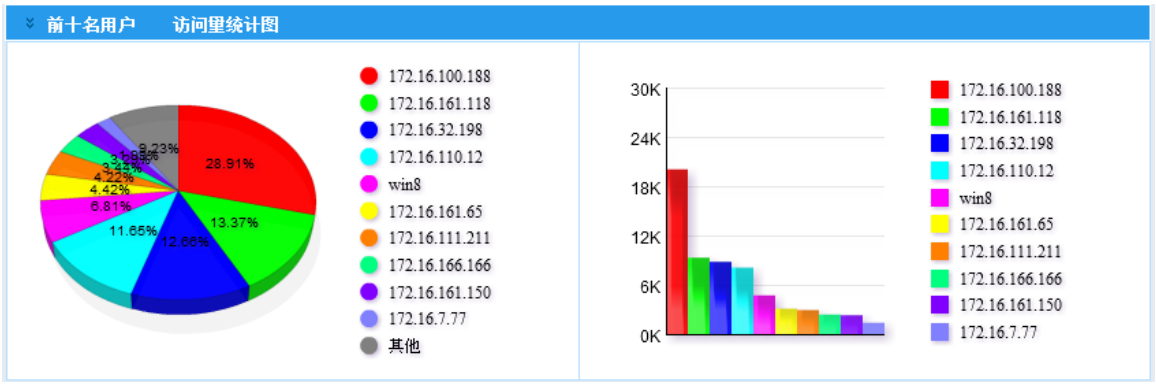


图73. URL 访问量-基于用户-统计图

第三、 排名列表。显示符合统计条件的 URL 访问次数的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

用户 访问里排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	用户	访问次数	百分比	详细
	总计	69360	100.00%	
1	172.16.100.188	20055	28.91%	
2	172.16.161.118	9275	13.37%	
3	172.16.32.198	8784	12.66%	
4	172.16.110.12	8077	11.65%	
5	win8	4722	6.81%	
6	172.16.161.65	3066	4.42%	
7	172.16.111.211	2926	4.22%	
8	172.16.166.166	2386	3.44%	
9	172.16.161.150	2285	3.29%	
10	172.16.7.77	1383	1.99%	
11	172.16.161.253	1334	1.92%	
12	172.16.166.168	1320	1.90%	
13	172.16.251.251	1151	1.66%	
14	172.16.122.199	944	1.36%	
15	172.16.55.129	512	0.74%	
16	172.16.161.231	372	0.54%	

图74. URL 访问量-基于用户-排名列表

参数与按钮说明：

- 访问次数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 被访问的次数的累计值。
- <趋势图>：点击此按钮，显示指定基于用户在各时刻被访问的次数的趋势图。
- <基于 URL 的统计>：点击此按钮，显示指定用户里被访问的相关 URL 的访问次数的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示指定用户访问的相关 URL 类型的访问次数的排名情况。

21.9.4 基于用户组统计

功能描述：以用户组为统计对象，对 URL 被访问的次数进行排名统计。

配置路径：【统计分析】>【URL 访问量】>【基于用户组】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

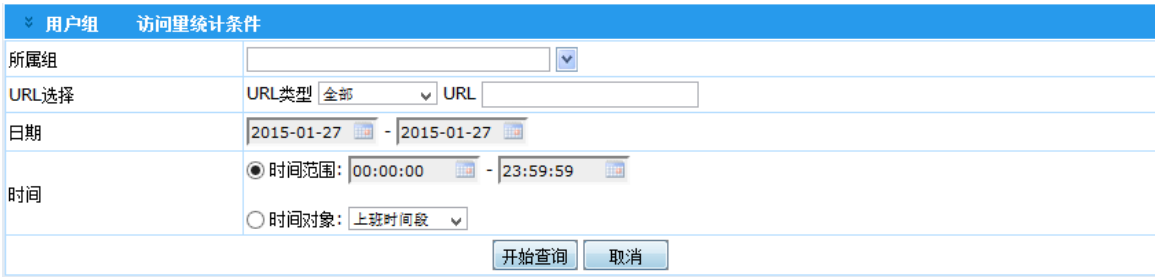


图75. URL 访问量-基于用户组-统计条件

参数说明：

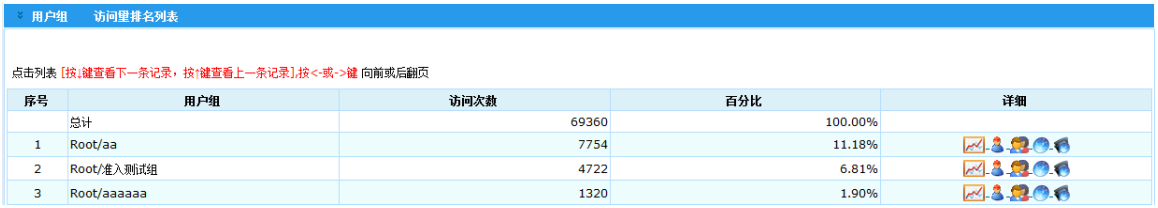
- 所属组：选择需要进行访问次数排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- URL 选择：选择需要进行访问次数排名统计的 URL 类型/URL 关键字。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的用户组中，每个用户组的访问量占总访问量的比例。[柱图]显示排名前十的用户组的访问量及排名。

图76. URL 访问量-基于用户组-统计图

第三、 排名列表。显示符合统计条件的 URL 访问次数的排名情况。



序号	用户组	访问次数	百分比	详细
	总计	69360	100.00%	
1	Root/aa	7754	11.18%	
2	Root/准入测试组	4722	6.81%	
3	Root/aaaaaa	1320	1.90%	

图77. URL 访问量-基于用户组-排名列表

参数与按钮说明：

- 访问次数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某个 URL 被访问的次数的累计值。
- <趋势图>：点击此按钮，显示指定基于用户组在各时刻被访问的次数的趋势图。
- <基于用户的统计>：点击此按钮，显示指定用户组包含的所有用户(包括该组的直接用户和子组包含的用户) 访问的相关 URL 的访问次数的排名情况。

- <基于子用户组的统计>：点击此按钮，显示指定用户组包含的直接子组访问的相关 URL 的访问次数的。如包含多级子组，可以一级一级往下看。
- <基于 URL 的统计>：点击此按钮，显示指定用户组里被访问的相关 URL 的访问次数的排名情况。
- <基于 URL 类型的统计>：点击此按钮，显示指定用户组访问的相关 URL 类型的访问次数的排名情况。

21.10 网页文件访问次数统计

21.10.1 基于文件类型统计

功能描述：以文件类型(如 doc、jpg)为统计对象，对通过网页下载文件的次数进行排名统计。包括手动下载和

配置路径：【统计分析】>【文件类型访问次数】>【基于文件类型】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第四、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

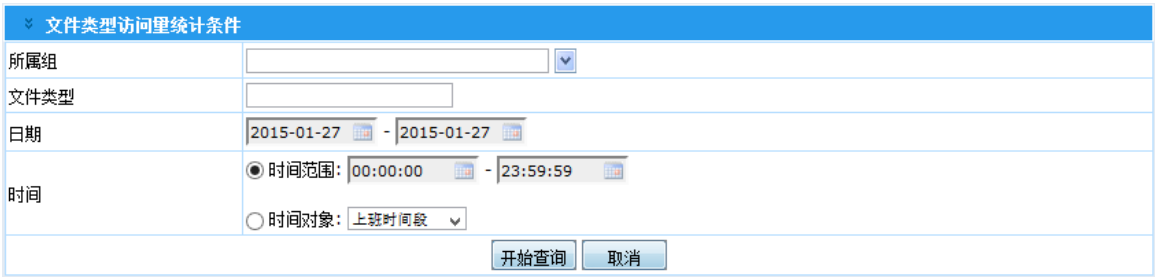


图78. 文件类型访问量-基于文件类型-统计条件

参数说明：

- 所属组：选择需要进行下载的次数排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 文件类型：选择需要进行下载的次数排名统计的文件类型。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第五、 前十名统计图。[饼图]显示排名前十的文件类型中，每个文件类型的访问次数占总访问次数的比例。[柱图]显示排名前十的文件类型的访问次数及排名。

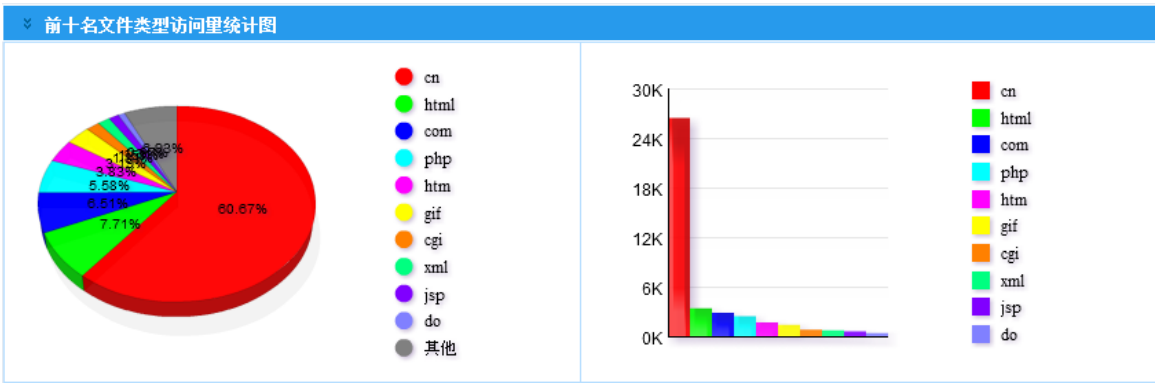


图79.　　文件类型访问量-基于文件类型-统计图

第六、　排名列表。显示符合统计条件的文件访问次数的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

文件类型访问量排名列表

1 2 下一页> 总纪录数为73条!

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	文件类型	访问次数	百分比	详细
	总计	43549	100.00%	
1	cn	26421	60.67%	
2	html	3359	7.71%	
3	com	2833	6.51%	
4	php	2431	5.58%	
5	htm	1668	3.83%	
6	gif	1391	3.19%	
7	cgi	788	1.81%	
8	xml	689	1.58%	
9	jsp	572	1.31%	
10	do	381	0.87%	
11	dll	332	0.76%	
12	aspx	325	0.75%	
13	shtml	261	0.60%	
14	js	205	0.47%	
15	dat	172	0.39%	
16	cab	149	0.34%	
17	jpg	146	0.34%	

图80.　　文件类型访问量-基于文件类型-排名列表

参数与按钮说明：

- 访问次数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某类型的文件被下载的次数的累计值。
- <趋势图>：点击此按钮，显示指定文件类型在各时刻被下载的次数的趋势图。
- <基于用户的统计>：点击此按钮，显示访问指定文件类型的相关用户的访问次数的排名情况。
- <基于用户组的统计>：点击此按钮，显示访问指定文件类型的相关用户组的访问次数的排名情况。

21.10.2基于用户统计

功能描述：以用户为统计对象，对通过网页下载的各种类型的文件的次数进行排名统计。

配置路径：【统计分析】>【文件类型访问量】>【基于用户】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第一、　统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

用户文件类型访问量统计条件

所属组	
用户	
文件类型	
日期	2015-01-27 - 2015-01-27
时间	◉ 时间范围: 00:00:00 - 23:59:59 ○ 时间对象: 上班时间段

开始查询　取消

图81.　　文件类型访问量-基于用户-统计条件

参数说明：

- 所属组：选择需要进行访问次数排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 用户：输入需要进行访问次数排名统计的用户。
- 文件类型：选择需要进行访问次数排名统计的文件类型。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第二、　前十名统计图。[饼图]显示排名前十的用户中，每个用户的下载文件的次数占总访问次数的比例。[柱图]显示排名前十的用户的下载文件的次数及排名。

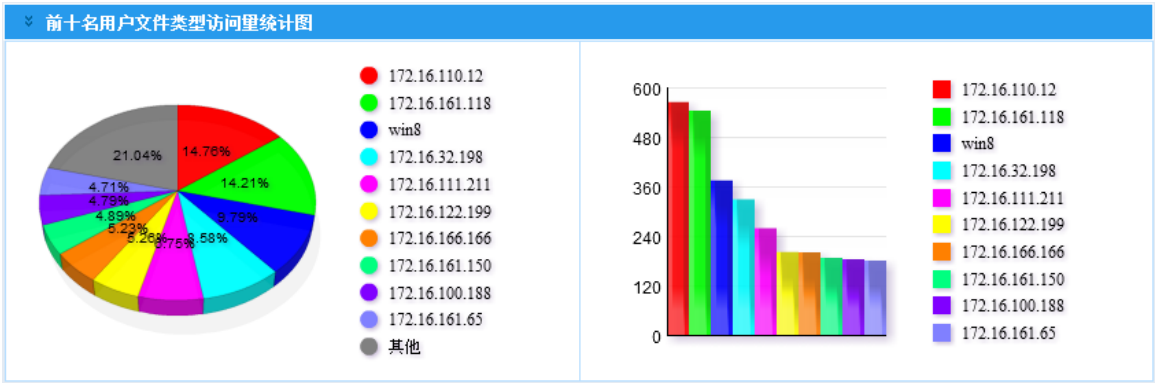


图82.　　文件类型访问量-基于用户-统计图

第三、　排名列表。显示符合统计条件的文件访问次数的排名情况。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

用户文件类型访问量排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	用户	访问次数	百分比	详细
	总计	3822	100.00%	
1	172.16.110.12	564	14.76%	
2	172.16.161.118	543	14.21%	
3	win8	374	9.79%	
4	172.16.32.198	328	8.58%	
5	172.16.111.211	258	6.75%	
6	172.16.122.199	201	5.26%	
7	172.16.166.166	200	5.23%	
8	172.16.161.150	187	4.89%	
9	172.16.100.188	183	4.79%	
10	172.16.161.65	180	4.71%	
11	172.16.166.168	164	4.29%	
12	172.16.7.77	127	3.32%	
13	172.16.161.253	121	3.17%	
14	172.16.161.3	73	1.91%	
15	172.16.55.129	63	1.65%	

图83.　　文件类型访问量-基于用户-排名列表

参数与按钮说明：

- 访问次数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某类型的文件被下载的次数的累计值。
- <趋势图>：点击此按钮，显示指定基于用户在各时刻被下载的次数的趋势图。
- <基于 URL 的统计>：点击此按钮，显示指定用户里被访问的相关 URL 的访问次数的排名情况。

- <基于文件类型的统计>：点击此按钮，显示指定用户访问的相关文件类型的访问次数的排名情况。

21.10.3基于用户组统计

功能描述：以用户组为统计对象，对通过网页下载的各种类型的文件的次数进行排名统计。

配置路径：【统计分析】>【文件类型访问次数】>【基于用户组】

配置描述：该页面分为三部分，分别是：统计条件、统计图、排名列表。

第一、 统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

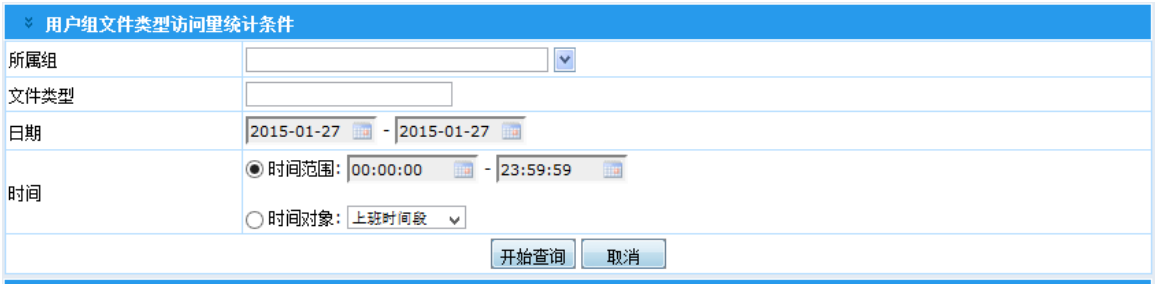


图84. 文件类型访问量-基于用户组-统计条件

参数说明：

- 所属组：选择需要进行访问次数排名统计的用户组。点击<选择组>按钮，进行用户组的选择。
- URL 选择：选择需要进行访问次数排名统计的 URL 类型/URL 关键字。

点击<统计>按钮，生成统计信息。统计信息以图形和表格的形式在[统计图]和[排名列表]中显示，详细说明如后。

第二、 前十名统计图。[饼图]显示排名前十的用户组中，每个用户组的访问次数占总访问次数的比例。[柱图]显示排名前十的用户组的访问次数及排名。

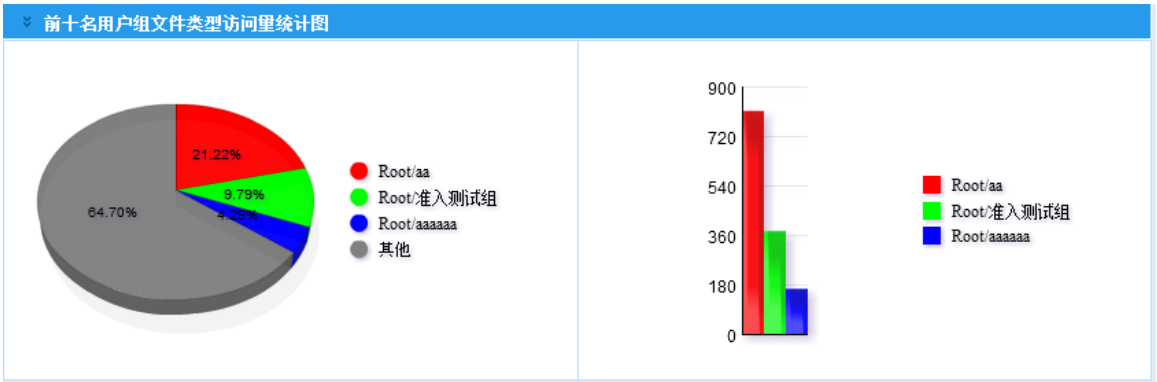


图85. 文件类型访问量-基于用户组-统计图

第三、 排名列表。显示符合统计条件的线路的排名情况。

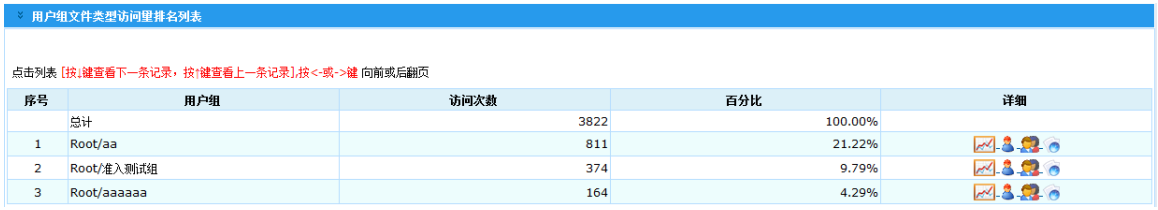


图86.　　文件类型访问量-基于用户组-排名列表

参数与按钮说明：

- 访问次数：在指定时间段（最近一小时、最近一天、最近一周、最近一月、自定义时间段）内，某类型的文件被下载的次数的累计值。
- <趋势图>：点击此按钮，显示指定基于用户组在各时刻被下载的次数的趋势图。
- <基于用户的统计> :点击此按钮 ,显示指定用户组包含的所有用户(包括该组的直接用户和子组包含的用户) 访问的相关 URL 的访问次数的排名情况。
- <基于子用户组的统计>：点击此按钮，显示指定用户组包含的直接子组访问的相关 URL 的访问次数的。如包含多级子组，可以一级一级往下看。
- <基于 URL 的统计>：点击此按钮，显示指定用户组里被访问的相关 URL 的访问次数的排名情况。
- <基于文件类型的统计>：点击此按钮，显示指定用户组访问的相关文件类型的访问次数的排名情况。

21.10.4 上网时长统计

功能描述：对用户上网的时长进行统计。

配置路径：【统计分析】>【上网时长统计】

配置描述：该页面分为两部分，分别是：统计条件、排名列表。

第一、　统计条件。默认显示指定时间段内所有的统计信息，通过选择统计条件来生成符合条件的统计信息。

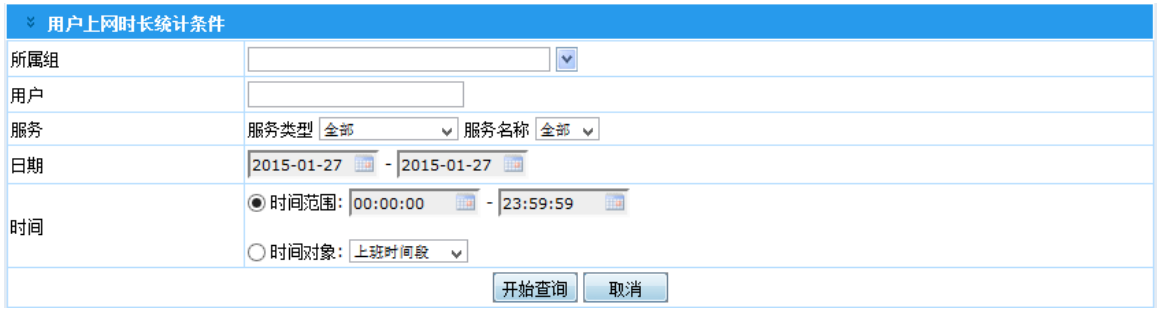


图87.　　上网时长统计-统计条件

参数说明：

- 所属组：选择需要进行上网时长统计的用户组。点击<选择组>按钮，进行用户组的选择。
- 用户：输入需要上网时长排名统计的用户名称。
- 服务：选择需要进行上网时长统计的服务类型/服务名称。

点击<统计>按钮，生成统计信息。统计信息以表格的形式在[排名列表]中显示，详细说明如后。

第二、 排名列表。显示符合统计条件的线路的排名情况。

用户上网时长排名列表

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

序号	用户	上网时长	详细
1	win8	23小时42分15秒	其他服务[23小时42分15秒],常用服务[23小时42分15秒],网络存...
2	172.16.161.118	23小时42分8秒	其他服务[23小时42分8秒],远程控制[21小时37分6秒],常用服务[1...
3	172.16.161.3	23小时40分28秒	其他服务[23小时40分28秒],常用服务[2小时24分17秒],HTTP应用...
4	172.16.3.221	17小时11分51秒	常用服务[17小时11分51秒]
5	172.16.122.199	14小时24分57秒	常用服务[12小时43分7秒],其他服务[12小时38分15秒],P2P下载[...
6	172.16.4.221	11小时21分47秒	常用服务[11小时21分47秒],HTTP应用[2分]
7	172.16.0.163	10小时40分56秒	其他服务[10小时40分56秒],常用服务[30秒]
8	172.16.161.65	10小时28分49秒	其他服务[10小时1分40秒],即时通讯[10小时1分2秒],常用服务[9...
9	172.16.100.188	9小时50分	即时通讯[9小时50分],其他服务[9小时50分],常用服务[9小时50分]...
10	172.16.166.168	9小时35分2秒	常用服务[9小时32分40秒],其他服务[9小时22分54秒],即时通讯[5...
11	172.16.1.99	9小时31分28秒	其他服务[9小时31分19秒],常用服务[2小时24分26秒],软件更新[2...
12	172.16.161.253	9小时24分	远程控制[6小时5分20秒],其他服务[3小时30分],即时通讯[3小时2...
13	172.16.32.198	9小时5分49秒	常用服务[9小时4分4秒],即时通讯[9小时2分34秒],其他服务[8小时...
14	172.16.166.171	8小时52分47秒	其他服务[7小时17分22秒],常用服务[1小时56分13秒],HTTP应用[...
15	172.16.110.12	8小时43分58秒	常用服务[8小时42分49秒],即时通讯[8小时36分51秒],其他服务[8...
16	172.16.111.211	8小时43分42秒	即时通讯[8小时38分25秒],其他服务[8小时27分31秒],常用服务[8...
17	172.16.7.77	5小时57分56秒	即时通讯[5小时49分28秒],其他服务[5小时43分51秒],常用服务[5...
18	172.16.161.150	4小时2分17秒	常用服务[3小时58分28秒],即时通讯[3小时53分21秒],其他服务[3...

图88. 上网时长统计-排名列表

参数说明：

- 上网时长：用户上线至下线的时间长度。
- 详细：用户每类访问上网时长的详细统计。点击链接，可查看该用户每类访问上网时长的详细统计。如下图：

详细【172.16.32.198】

序号	服务类型	上网时长
1	常用服务	9小时4分4秒
2	即时通讯	9小时2分34秒
3	其他服务	8小时55分43秒
4	HTTP应用	3小时1分21秒
5	移动应用	1小时44分40秒
6	网页邮箱	1小时3分7秒
7	网络存储	27分9秒
8	软件更新	18分46秒
9	视频网站浏览	17分22秒
10	WEB视频	15分32秒
11	P2P下载	12分21秒
12	网络游戏	12分
13	流媒体	7分20秒
14	网络电话	2分

图89. 上网时长统计-排名列表

22 日志查询

报表中心提供行为分析功能，本章对 WEB 访问、邮件收发、即时通讯、FTP 传输、报文会话、报文阻断等模块的行为进行详细的记录与分析整理。

22.1 上网行为

22.1.1 所有行为

配置路径：【日志查询】>【上网行为】>【所有行为】，如下图：

序号	用户名	组名	主机IP地址	目标地址	应用类型	具体应用	日期与时间	动作	详细
1	172.16.161.118	Root/	172.16.161.118	218.30.103.111	HTTP	HTTP_POST	2015-02-03 10:3...	允许	详细
2	172.16.161.118	Root/	172.16.161.118	220.181.125.38	HTTP	访问网站-搜索引擎	2015-02-03 10:3...	允许	详细
3	172.16.161.118	Root/	172.16.161.118	180.149.156.73	HTTP	访问网站-搜索引擎	2015-02-03 10:3...	允许	详细
4	172.16.161.118	Root/	172.16.161.118	218.30.103.111	HTTP	HTTP_POST	2015-02-03 10:3...	允许	详细
5	172.16.161.118	Root/	172.16.161.118	180.149.156.143	HTTP	HTTP_POST	2015-02-03 10:3...	允许	详细
6	172.16.161.118	Root/	172.16.161.118	218.30.103.111	HTTP	HTTP_POST	2015-02-03 10:3...	允许	详细
7	172.16.161.118	Root/	172.16.161.118	14.17.42.125	HTTP	访问网站-新闻门户	2015-02-03 10:3...	允许	详细
8	172.16.161.118	Root/	172.16.161.118	180.149.156.143	HTTP	HTTP_POST	2015-02-03 10:3...	允许	详细
9	172.16.161.118	Root/	172.16.161.118	218.30.103.111	HTTP	HTTP_POST	2015-02-03 10:3...	允许	详细
10	172.16.161.118	Root/	172.16.161.118	218.30.103.111	HTTP	HTTP_POST	2015-02-03 10:3...	允许	详细

图90. 上网行为-所有行为记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

目标地址：访问的目标地址。

应用类型：该应用属于那个类型，如：HTTP。

具体应用：应用类型以及所访问的具体应用。

日期与时间：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

时间：选择记录的开始时间与截止时间。

动作：选择访问目标网站的条件，支持多选。

应用类型：选择应用的分类，比如 HTTP、搜索引擎等。

具体应用：默认为应用所有。

22.1.2 网页标题

配置路径：【日志查询】>【上网行为】>【网页标题】，如下图：

序号	用户名	组名	主机IP地址	网站标题	网站链接	网站类别	日期与时间	动作	详细
1	172.16.161.118	Root/	172.16.161.118	新浪首页	http://www.sina.com....	新闻门户	2015-02-03 10:3...	允许	详细
2	172.16.161.118	Root/	172.16.161.118	联系我们-关于亿美-亿美软...	http://www.emay.cn/c...	其他网站	2015-02-03 10:3...	允许	详细
3	172.16.161.118	Root/	172.16.161.118	新浪首页	http://www.sina.com....	新闻门户	2015-02-03 10:2...	允许	详细
4	172.16.161.118	Root/	172.16.161.118	shared page	http://chat.live800.co...	交友聊天	2015-02-03 10:2...	允许	详细
5	172.16.161.118	Root/	172.16.161.118	您的移动商务伙伴-亿美软...	http://www.emay.cn/	其他网站	2015-02-03 10:2...	允许	详细
6	172.16.161.118	Root/	172.16.161.118	火狐新标签推荐	http://newtab.firefoxc...	搜索引擎	2015-02-03 10:2...	允许	详细
7	172.16.161.118	Root/	172.16.161.118	火狐新标签推荐	http://newtab.firefoxc...	搜索引擎	2015-02-03 10:2...	允许	详细
8	172.16.161.118	Root/	172.16.161.118	新浪首页	http://www.sina.com....	新闻门户	2015-02-03 10:2...	允许	详细
9	172.16.161.118	Root/	172.16.161.118	新浪首页	http://www.sina.com....	新闻门户	2015-02-03 10:1...	允许	详细
10	172.16.7.77	Root/	172.16.7.77	百度一下，你就知道	http://www.baidu.com/	搜索引擎	2015-02-03 10:1...	允许	详细

图91. 上网行为-网页标题记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

网页标题：WEB 网页的标题。

网站类型：该网页属于那个类型的网站。

网站标题：网页对应的 URL 地址。如果 URL 地址过长，默认将省略后面字符的显示。点击 URL 地址，链接到该页面。

日期与时间：记录该信息的时间。

查询条件：

日期范围：选择记录的开始日期与截止日期。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

时间：选择记录的开始时间与截止时间。

网站类型：选择网站的分类，比如 IT 相关、军事等。

关键字：[网页标题]或[URL 地址]的关键字，支持模糊查询。

目标 IP：所访问的某个网页解析的 IP 地址。

22.1.3 网页 URL

配置路径：【日志查询】>【上网行为】>【网页 URL】，如下图：

序号	用户名	组名	主机IP地址	网站链接	网站类别	日期与时间	动作	详细
1	172.16.161.118	Root/	172.16.161.118	http://v.qdt.qq.com/qdt_stats.fcg?stkey=c8d7be...	新闻门户	2015-02-03 10:3...	允许	详细
2	172.16.161.118	Root/	172.16.161.118	http://101.226.11.128/file_health_info.php	其他网站	2015-02-03 10:3...	允许	详细
3	172.16.161.118	Root/	172.16.161.118	https://fe2.update.microsoft.com	IT相关	2015-02-03 10:3...	允许	详细
4	172.16.161.118	Root/	172.16.161.118	http://client.show.qq.com/cgi-bin/qqshow_user_...	交友聊天	2015-02-03 10:3...	允许	详细
5	172.16.161.118	Root/	172.16.161.118	http://v.qdt.qq.com/qdt_stats.fcg?stkey=c8d7be...	新闻门户	2015-02-03 10:3...	允许	详细
6	172.16.161.118	Root/	172.16.161.118	http://cloudex.pinyin.sogou.com/lca.php?z=0&t=...	搜索引擎	2015-02-03 10:3...	允许	详细
7	172.16.161.118	Root/	172.16.161.118	http://w.sugg.sogou.com/sugg/suggestajaj.jsp?...	搜索引擎	2015-02-03 10:3...	允许	详细
8	172.16.161.118	Root/	172.16.161.118	http://v.qdt.qq.com/qdt_stats.fcg?stkey=c8d7be...	新闻门户	2015-02-03 10:3...	允许	详细
9	172.16.161.118	Root/	172.16.161.118	http://cloudex.pinyin.sogou.com/lca.php?z=0&t=...	搜索引擎	2015-02-03 10:3...	允许	详细
10	172.16.161.118	Root/	172.16.161.118	http://w.sugg.sogou.com/sugg/suggestajaj.jsp?...	搜索引擎	2015-02-03 10:3...	允许	详细

图92.　　上网行为-URL 记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

主机 IP 地址：客户机 IP 地址。

网站类别：URL 的分类，如法律、军事。

网站链接：详细的 URL 地址。点击该地址，可以打开对应网页。

日期与时间：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

时间：选择记录的开始时间与截止时间。

动作：选择访问目标网站的条件，支持多选。

网站类型：选择网站的分类，比如 IT 相关、军事等。

关键字：[网页标题]或[URL 地址]的关键字，支持模糊查询。

目标 IP：所访问的某个网页解析的 IP 地址。

22.1.4 网页搜索

配置路径：【日志查询】>【上网行为】>【网页搜索】，如下图：

序号	用户名	组名	主机IP地址	搜索关键字	搜索类型	日期与时间	动作	详细
1	172.16.7.77	Root/	172.16.7.77	行为管理	百度-百度-网页	2015-02-02 18:09:23	允许	详细
2	172.16.7.77	Root/	172.16.7.77	行为管理	百度-百度-网页	2015-02-02 18:09:23	允许	详细
3	172.16.7.77	Root/	172.16.7.77	江西人事考试网首页	百度-百度搜索建议	2015-02-02 18:08:49	允许	详细

图93.　　上网行为-网页搜索记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

搜索关键字：在搜索引擎上搜索的关键字。

搜索类型：搜索引擎的分类，如 Googel、百度。

时间与日期：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

时间：选择记录的开始时间与截止时间。

动作：选择访问目标网站的条件，支持多选。

搜索类型：选择搜索引擎的分类，比如百度、搜狗等，默认所有应用。

搜索关键字：[网页标题]或[URL 地址]的关键字，支持模糊查询。

目标 IP：所访问的某个网页解析的 IP 地址。

22.1.5 邮件收发

配置路径：【日志查询】>【上网行为】>【邮件收发】，如下图：

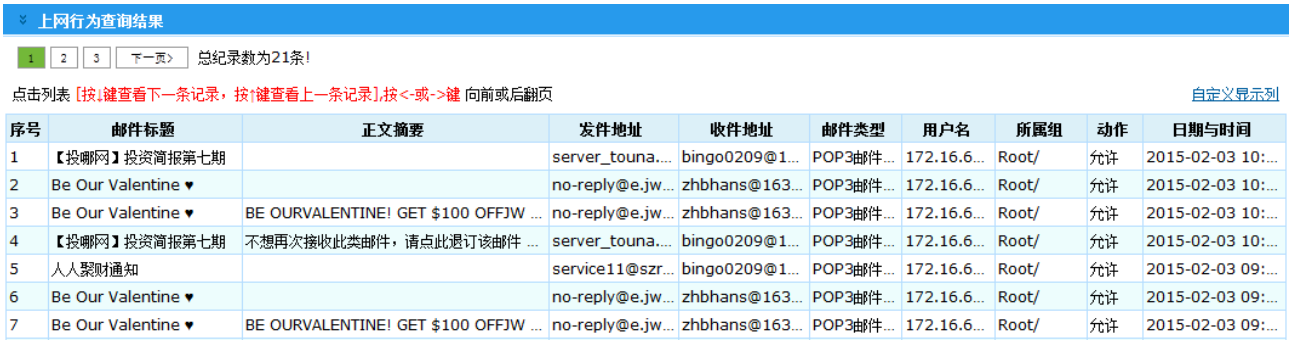


图94. 上网行为-邮件收发记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

邮件标题：邮件的主题。

正文摘要：搜索引擎的分类，如 Googel、百度。

发件地址：邮件发送方

收件地址：邮件接收方

邮件类型：邮件的类型，如：POP3。

时间与日期：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

时间：选择记录的开始时间与截止时间。

邮件类型：邮件的类型，如：POP3 邮件，WEB 邮件等。

发件地址：发信人邮件地址。

收件地址：收信人邮件地址。

标题关键字：邮件主题的关键字，支持模糊查询。

正文关键字：邮件内容的关键字，支持模糊查询。

22.1.6 IM 聊天

配置路径：【日志查询】>【上网行为】>【IM 聊天】，如下图：

图95. 上网行为-IM 聊天记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

发送账号：发送消息方。

接受账号：接受消息方。

聊天摘要：IM 聊天的记录摘要。

应用类型：IM 聊天的平台，如：qq 平台。

日期与时间：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

时间：选择记录的开始时间与截止时间。

动作：选择访问目标网站的条件，支持多选。

应用类型：默认所有类型。

发送账号：发送方账号信息。

接受账号：接收方账号信息。

聊天内容：聊天记录内容，支持模糊查询。

22.1.7 论坛微博

配置路径：【日志查询】>【上网行为】>【论坛微博】，如下图：

图96.　　上网行为-论坛微博记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

标题：发送的帖子的标题。

正文摘要：发送帖子的正文内容。

应用类型：在哪个论坛上发的帖子，论坛的分类，如娱乐、军事

做 URL：帖子的 URL 地址。

日期：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

时间：选择记录的开始时间与截止时间。

动作：选择访问目标网站的条件，支持多选。

应用类型：选择应用的分类，如：军事，体育等，默认所有的应用。

关键字：[论坛标题]或[URL 地址]的关键字，支持模糊查询。

目标 IP：所访问的某个网页解析的 IP 地址。

22.1.8 账号登录

配置路径：【日志查询】>【上网行为】>【账号登录】，如下图：

序号	登录帐号	主机IP地址	应用类型	用户名	所属组	日期与时间	动作	详细
1	670409248@qq.com	172.16.111.206	邮箱-QQ邮箱	172.16.111.206	Root/aa/aa/	2015-02-03 10:5...	允许	详细
2	524757350	172.16.55.129	即时通信-QQ	172.16.55.129	Root/	2015-02-03 10:5...	允许	详细
3	523738786	172.16.161.150	邮箱-QQ邮箱	172.16.161.150	Root/	2015-02-03 10:5...	允许	详细
4	866571024159173	172.16.161.118	手机ID-IMEI	Administrator	Root/	2015-02-03 10:4...	允许	详细
5	524757350	172.16.55.129	即时通信-QQ	172.16.55.129	Root/	2015-02-03 10:4...	允许	详细
6	12791115	172.16.166.168	即时通信-微信	172.16.166.168	Root/aaaaaa/	2015-02-03 10:4...	允许	详细
7	2463600232@qq.com	172.16.162.67	邮箱-QQ邮箱	172.16.162.67	Root/	2015-02-03 10:3...	允许	详细
8	524757350	172.16.55.129	即时通信-QQ	172.16.55.129	Root/	2015-02-03 10:3...	允许	详细
9	12791115	172.16.166.168	即时通信-微信	172.16.166.168	Root/aaaaaa/	2015-02-03 10:3...	允许	详细
10	524757350	172.16.55.129	即时通信-QQ	172.16.55.129	Root/	2015-02-03 10:2...	允许	详细

图97. 上网行为-账号登录记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

登录账号：记录登录的账号。

应用类型：在哪个平台上登录的。

日期与时间：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

时间：选择记录的开始时间与截止时间。

动作：选择访问目标网站的条件，支持多选。

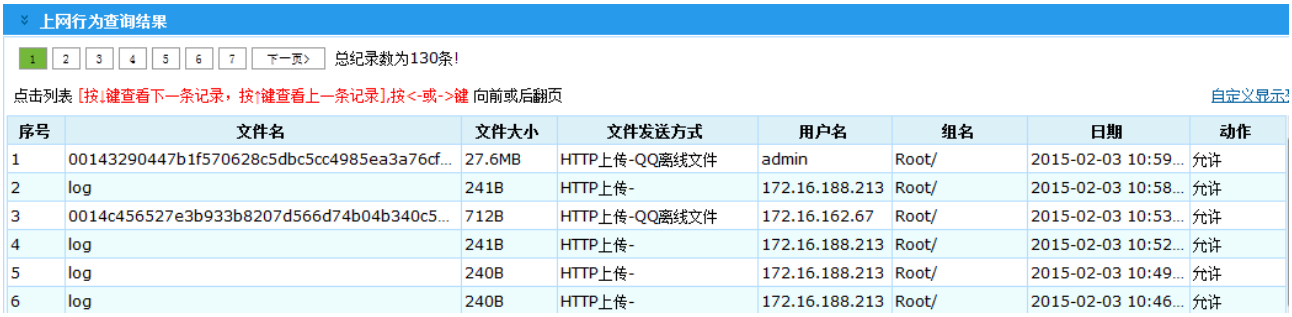
应用类型：选择登录账号的种类，如：购物，邮箱，论坛等。

登录账号：登录的账号信息。

目标 IP：所访问的某个网页解析的 IP 地址。

22.1.9 外发文件

配置路径：【日志查询】>【上网行为】>【外发文件】，如下图：


上网行为查询结果

1 2 3 4 5 6 7 下一页> 总纪录数为130条!

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页 自定义显示?

序号	文件名	文件大小	文件发送方式	用户名	组名	日期	动作
1	00143290447b1f570628c5dbc5cc4985ea3a76cf...	27.6MB	HTTP上传-QQ离线文件	admin	Root/	2015-02-03 10:59...	允许
2	log	241B	HTTP上传-	172.16.188.213	Root/	2015-02-03 10:58...	允许
3	0014c456527e3b933b8207d566d74b04b340c5...	712B	HTTP上传-QQ离线文件	172.16.162.67	Root/	2015-02-03 10:53...	允许
4	log	241B	HTTP上传-	172.16.188.213	Root/	2015-02-03 10:52...	允许
5	log	240B	HTTP上传-	172.16.188.213	Root/	2015-02-03 10:49...	允许
6	log	240B	HTTP上传-	172.16.188.213	Root/	2015-02-03 10:46...	允许

图98.　　上网行为-外发文件记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

文件名：发送的文件名称。

文件大小：发送的文件大小。

文件发送方式：文件发送采取的方式，如：HTTP 上传。

日期：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

动作：选择访问目标网站的条件，支持多选。

文件发送方式：选择发送的方式，比如 HTTP 上传、FTP 传文件等。

文件名关键字：所传文件名的关键字，支持模糊查询。

22.1.10外发信息

配置路径：【日志查询】>【上网行为】>【外发信息】，如下图：

上网行为查询结果 扩展显示 列表显示

1 2 3 4 5 6 7 8 9 10 ... 下一页> 记录数大于200条!

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页 自定义显示列

序号	用户名	所属组	主机IP地址	日期与时间	动作	上传信息
1	172.16.110.16	Root/	172.16.110.16	2015-02-03 11:00:58	允许	详细
2	172.16.7.77	Root/	172.16.7.77	2015-02-03 11:00:58	允许	详细
3	172.16.166.168	Root/aaaaaa/	172.16.166.168	2015-02-03 11:00:53	允许	详细
4	admin	Root/	172.16.110.12	2015-02-03 11:00:52	允许	详细
5	admin	Root/	172.16.110.12	2015-02-03 11:00:46	允许	详细
6	172.16.110.16	Root/	172.16.110.16	2015-02-03 11:00:33	允许	详细
7	172.16.32.198	Root/	172.16.32.198	2015-02-03 11:00:28	允许	详细
8	172.16.111.211	Root/aa/aa/	172.16.111.211	2015-02-03 11:00:25	允许	详细
9	172.16.162.67	Root/	172.16.162.67	2015-02-03 11:00:21	允许	详细
10	172.16.111.211	Root/aa/aa/	172.16.111.211	2015-02-03 11:00:08	允许	详细

图99.　　上网行为-外发信息记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

用户名：该外发信息的用户名。

日期：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

时间：选择记录的开始时间与截止时间。

动作：选择访问目标网站的条件，支持多选。

所有应用：选择网站的分类，比如购物、邮箱等，默认应用所有应用。

包含内容：访问目标网站内容的关键字，支持模糊查询。

目标 IP：所访问的某个网页解析的 IP 地址。

22.1.11 telnet 命令

配置路径：【日志查询】>【上网行为】>【telnet 命令】，如下图：

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

用户名：用户的用户名。

组名：用户的组名。

主机 IP 地址：用户的 ip 地址。

Telnet 命令：用户输入的 telnet 命令。

Telnet 结果：输入该 telnet 命令后输出的结果。

日期与时间：记录该信息的时间和时间。

详细：点击详细按钮，可查询该条 telnet 命令的详细信息。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

命令关键字：可根据 telnet 命令内容进行过滤，支持模糊查询。。

目标 IP：用户的 IP 地址。

22.1.12阻断记录

配置路径：【日志查询】>【上网行为】>【阻断记录】，如下图：

上网行为查询结果

扩展显示 列表显示

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页

自定义显示列

序号	源(IP: 端口)	目的(IP: 端口)	转换(IP: 端口)	协议类型	服务类型	报文长度	应用类型	规则名称	记录时间
1	172.16.7.77:51890 局域网	180.97.33.72:80 江苏省苏州市电信	0.0.0.0	TCP	常用服务:HTTP	40	行为阻断		2015...
2	172.16.7.77:51890 局域网	180.97.33.72:80 江苏省苏州市电信	0.0.0.0	TCP	常用服务:HTTP	40	行为阻断		2015...
3	172.16.7.77:51890 局域网	180.97.33.72:80 江苏省苏州市电信	0.0.0.0	TCP	常用服务:HTTP	40	行为阻断		2015...
4	172.16.7.77:51879 局域网	180.97.33.108:80 江苏省苏州市电信	0.0.0.0	TCP	常用服务:HTTP	40	行为阻断		2015...
5	172.16.7.77:51895 局域网	180.97.33.108:80 江苏省苏州市电信	0.0.0.0	TCP	常用服务:HTTP	40	行为阻断		2015...
6	172.16.7.77:51879 局域网	180.97.33.108:80 江苏省苏州市电信	0.0.0.0	TCP	常用服务:HTTP	40	行为阻断		2015...

图100. 上网行为-阻断记录

参数说明：

默认列表显示，可点击扩展显示查看对应扩展信息。

源（IP:端口）：主机的 IP 地址与所使用的端口号。

目的（IP:端口）：目标网络的 IP 以及目标相应的服务端口。

转换（IP:端口）：主机 IPNAT 后的地址以及端口号

协议类型：TCP/UDP 类型。

服务类型：属于哪种服务。

报文长度：报文的长度。

应用类型：属于哪种应用类型阻断。

规则名称：阻断来自于哪条规则。

记录时间：记录该信息的时间。

查询条件：

日期范围：选择记录的开始时间与截止时间。

按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

动作：选择访问目标网站的条件，支持多选。

网站类型：选择网站的分类，比如 IT 相关、军事等。

关键字：[网页标题]或[URL 地址]的关键字，支持模糊查询。

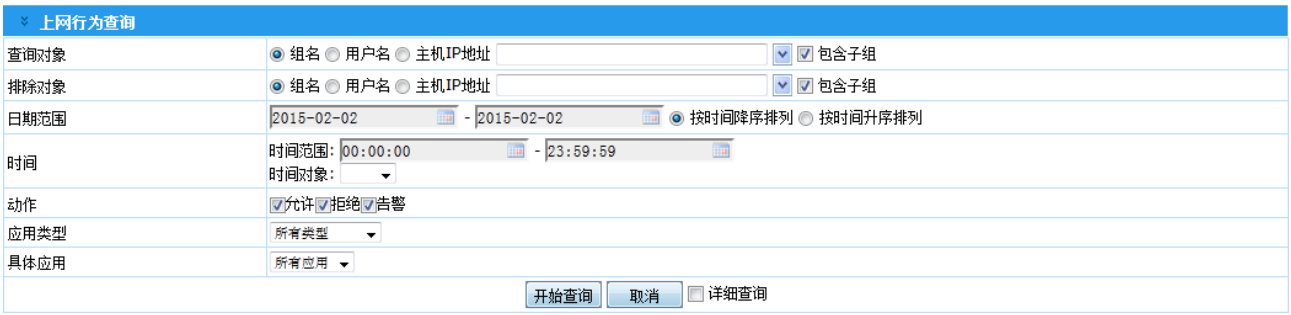
目标 IP：所访问的某个网页解析的 IP 地址。

功能描述：记录被访问网页的标题和 URL 地址，没有标题的网页不被记录。

配置路径：【日志查询】>【上网行为】>【所有行为】

配置描述：该页面分三部分，分别是：查询条件、网页记录、详细信息。

第一、 查询条件。默认显示当天的网页记录，即当天“0:00-当前时刻”的网页访问记录。



参数说明：

- 查询对象：选择需要查询的用户组、用户或是主机 IP 地址。勾选<包含子组>，进行子组的选择。
- 排除对象：选择需要查询的用户组、用户或是主机 IP 地址。勾选<包含子组>，进行子组的选择。
- 日期范围：选择想要查询的日期。
- 时间：选择想要查询的具体时间。
- 动作：选择查询的操作是允许、拒绝或是告警。
- 应用类型：选择查看的应用类型。
- 具体应用：选择查看的具体应用。

点击<开始查询>按钮，网页记录列表中将显示符合查询条件的所有行为的详细记录，详细说明如后。

第二、 网页记录。显示符合查询条件的所有行为的详细记录。

上网行为查询结果 扩展显示 列表显示

1 2 3 4 5 6 7 8 9 10 ... 下一页> 记录数大于200条!

点击列表 [按↓键查看下一条记录，按↑键查看上一条记录],按<-或->键 向前或后翻页 自定义显示列

序号	用户名	组名	主机IP地址	目标地址	应用类型	具体应用	日期与时间	动作	详细
1	192.168.1.126	Root/	192.168.1.126	192.168.1.200	HTTP	访问网站-其他网站	2015-02-02 18:3...	允许	详细
2	192.168.1.126	Root/	192.168.1.126	192.168.1.200	HTTP	访问网站-其他网站	2015-02-02 18:3...	允许	详细
3	192.168.1.126	Root/	192.168.1.126	192.168.1.200	HTTP	访问网站-其他网站	2015-02-02 18:3...	允许	详细
4	192.168.1.126	Root/	192.168.1.126	192.168.1.200	HTTP	访问网站-其他网站	2015-02-02 18:3...	允许	详细
5	172.16.7.77	Root/	172.16.7.77	113.108.16.83	HTTP	访问网站-邮箱	2015-02-02 18:3...	允许	详细
6	172.16.7.77	Root/	172.16.7.77	191.237.6.13	HTTP	访问网站-其他网站	2015-02-02 18:3...	允许	详细
7	172.16.7.77	Root/	172.16.7.77	137.116.224.167	HTTP	访问网站-手机	2015-02-02 18:3...	允许	详细
8	172.16.7.77	Root/	172.16.7.77	14.17.42.125	HTTP	访问网站-新闻门户	2015-02-02 18:3...	允许	详细
9	172.16.161.118	Root/	172.16.161.118	14.17.42.125	HTTP	访问网站-新闻门户	2015-02-02 18:3...	允许	详细
10	172.16.7.77	Root/	172.16.7.77	219.133.60.209	HTTP	访问网站-邮箱	2015-02-02 18:3...	允许	详细

- 用户/用户组：显示用户名和用户组。
- 主机 IP 地址：用户的 IP 地址。
- 目标 IP 地址：被访问的 IP 地址
- 应用类型：应用的类别。
- 具体应用：属于何种具体的应用。
- 日期与时间：记录访问网页的时间。
- 动作：用户访问网页是否允许。

22.2 会话记录

功能描述：记录经过设备传输的所有数据的会话信息。

配置路径：【日志查询】>【会话记录】

配置描述：该页面分两部分，分别是：查询条件和会话记录。

第一、 查询条件。默认显示当天的会话记录消息，即当天“0:00-当前时刻”的记录。

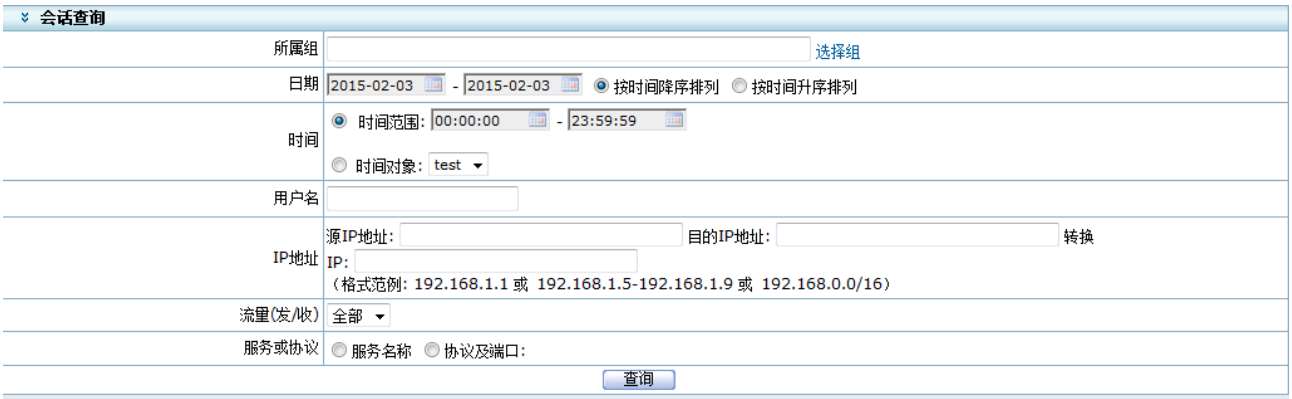


图101. 会话记录-查询条件

参数说明：

- 所属组：选择发起或接收会话的用户组。点击<选择组>按钮，进行用户组的选择。
- 时间范围：选择发起或接收会话的时间。查询结果可以选择[按时间降序排列]或[按时间升序排列]。

- 用户名：选择发起或接收会话的用户名。
- IP 地址：选择发起或接收会话的 IP 地址，或者会话被转换的 IP 地址。
- 服务或协议：选择会话的服务名称或端口号。

点击<查询>按钮，会话记录中将显示符合查询条件的记录，详细说明如后。

第二、 会话记录。显示符合查询条件的会话记录消息。受篇幅所限，下图仅截取前 6 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

会话记录

导出为XML 导出为HTML

1 2 3 4 5 6 7 8 9 10 ... 下一页> 记录数大于200条!

序号	用户名/用户组	源信息	目的信息	协议及服务	流里(发/收)	持续时间	记录时间
1	172.16.7.77 Root	LAN1 172.16.7.77:52718 FC:AA:14:77:D9:F9	WAN1 14.17.42.125:80 广东省	TCP 常用服务 HTTP	1.0KB 811B	120秒	2015-02-03 10:54:09
2	172.16.7.77 Root	LAN1 172.16.7.77:53000 FC:AA:14:77:D9:F9	WAN1 172.16.161.2:9091 局域网	TCP 常用服务 SSL	1.1KB 670B	10秒	2015-02-03 10:54:08
3	172.16.7.77 Root	LAN1 172.16.7.77:57157 FC:AA:14:77:D9:F9	WAN1 202.96.134.133:53 广东省电信DNS服务器	UDP 常用服务 DNS	84B 313B	30秒	2015-02-03 10:54:07
4	172.16.161.118 Root	LAN1 172.16.161.118:53442 00:0C:F2:85:A9:BC	WAN1 118.123.240.228:80 四川省成都市光华电信IDC机房	TCP 即时通讯 Live800	872B 541B	10秒	2015-02-03 10:54:05
5	172.16.7.77 Root	LAN1 172.16.7.77:52707 FC:AA:14:77:D9:F9	WAN1 180.97.63.155:80 江苏省苏州市电信	TCP 软件更新 360杀毒更新	1.5KB 1.2KB	120秒	2015-02-03 10:54:03
6	172.16.7.77 Root	LAN1 172.16.7.77:52703 FC:AA:14:77:D9:F9	WAN1 172.16.161.2:9090 局域网	TCP 常用服务 SSL	4.0KB 22.7KB	120秒	2015-02-03 10:54:02

图102. 会话记录

按钮及参数说明：

- 导出为 Excel：将查询结果导出为 Excel 表格文件。
- 导出为 HTML：将查询结果导出为 HTML 文件。
- 用户/用户组：显示用户名和用户组。
- 源（IP：端口）：会话的源 IP 地址及源端口。
- 目的（IP：端口）：会话的目的 IP 地址及目的端口。
- 协议及服务：协议类型以及具体的服务。
- 发送流量：内部用户发送的流量值。
- 接收流量：内部用户接收的流量值。
- 持续时间：会话持续的时间长度。
- 记录时间：记录该会话消息的时间。

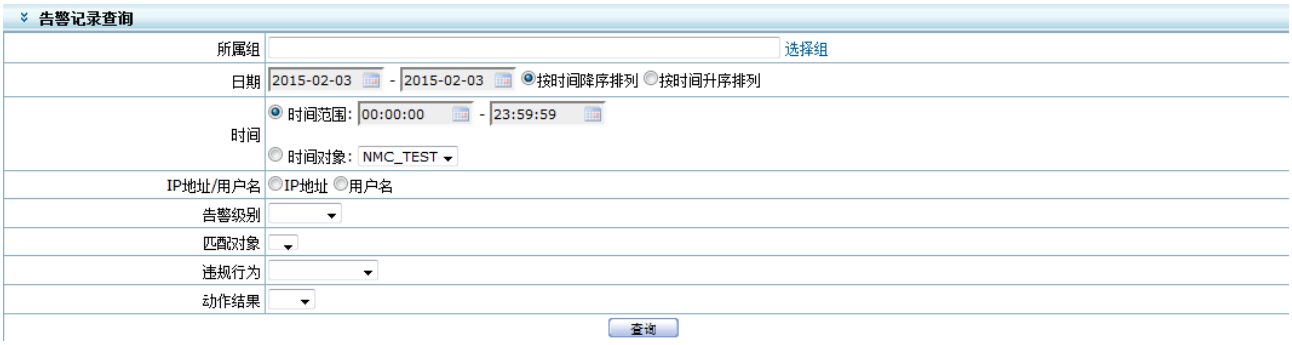
22.3 告警记录

功能描述：记录经过设备传输的所有数据的告警信息。

配置路径：【日志查询】>【告警记录】

配置描述：该页面分两部分，分别是：查询条件和会话记录。

第一、查询条件。默认显示当天的会话记录消息，即当天“0:00-当前时刻”的记录。



参数说明：

- 所属组：选择发起或接收会话的用户组。点击<选择组>按钮，进行用户组的选择。
- 时间范围：选择发起或接收会话的时间。查询结果可以选择[按时间降序排列]或[按时间升序排列]。
- 用户名：选择发起或接收会话的用户名。
- IP 地址：选择发起或接收会话的 IP 地址，或者会话被转换的 IP 地址。
- 告警级别：选择告警的级别，主要有四种：普通状态、预警状态、严重状态以及紧急状态。
- 违规行为：违规的操作。
- 动作结果：对该动作是允许还是过滤。

点击<查询>按钮，告警记录中将显示符合查询条件的记录，详细说明如后。

第二、告警记录。显示符合查询条件的告警记录消息。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

告警记录　　统计　导出为XML　导出为HTML

1 2 3 4 下一页> 总纪录数为66条!

序号	用户/用户组	目的IP地址	告警级别	匹配对象	违规行为	动作结果	告警内容	记录时间	操作
1	172.16.7.77 Root	180.97.33.107 江苏省苏州市电信	严重状态	汪涵 汪涵	搜索违规内容	允许	关键字: 汪涵	2015-02-03 11:13:07	详细
2	172.16.7.77 Root	180.97.33.72 江苏省苏州市电信	严重状态	汪涵 汪涵	搜索违规内容	允许	关键字: 汪涵	2015-02-03 11:13:06	详细
3	172.16.7.77 Root	180.97.33.107 江苏省苏州市电信	严重状态	汪涵 汪涵	搜索违规内容	允许	关键字: 汪涵	2015-02-03 11:13:06	详细
4	172.16.7.77 Root	183.60.15.162 广东省深圳市	普通状态	邮箱 mail.qq.com	非法网站	允许	http://rl.mail.qq.com/cgi-bin/getinvesti...	2015-02-03 11:12:56	详细
5	172.16.7.77 Root	183.60.15.162 广东省深圳市	普通状态	邮箱 mail.qq.com	非法网站	允许	http://rl.mail.qq.com/cgi-bin/getinvesti...	2015-02-03 11:12:56	详细
6	172.16.7.77 Root	113.108.16.61 广东省深圳市	普通状态	邮箱 mail.qq.com	非法网站	允许	http://set3.mail.qq.com/cgi-bin/laddr_fr...	2015-02-03 11:12:56	详细
7	172.16.7.77 Root	113.108.16.61 广东省深圳市	普通状态	邮箱 mail.qq.com	非法网站	允许	http://set3.mail.qq.com/cgi-bin/folderli...	2015-02-03 11:12:56	详细
8	172.16.7.77 Root	113.108.16.61 广东省深圳市	普通状态	邮箱 mail.qq.com	非法网站	允许	http://set3.mail.qq.com/cgi-bin/compose_...	2015-02-03 11:12:56	详细
9	172.16.7.77 Root	113.108.16.61 广东省深圳市	预警状态	汪涵 汪涵	违规邮件	允许	邮件帐户: 1074829281 发件人: 1074829281@qq.com 收件人: "俊英"<2474320824@qq.com> 邮件主题: 汪涵	2015-02-03 11:12:55	详细
10	172.16.7.77 Root	113.108.16.83 广东省深圳市	普通状态	邮箱 mail.qq.com	非法网站	允许	http://wp.mail.qq.com/poll?r=0.849789303...	2015-02-03 11:12:51	详细

按钮及参数说明：

- 导出为 Excel：将查询结果导出为 Excel 表格文件。

- 导出为 HTML：将查询结果导出为 HTML 文件。
- 用户/用户组：显示用户名和用户组。
- 目的（IP：端口）：目的 IP 地址及目的端口。
- 告警级别：操作对应的告警级别。
- 匹配对象：告警匹配的对象。
- 违规行为：产生告警所对应的违规行为。
- 动作结果：该行为是否被允许。
- 告警内容：产生告警所对应的内容。
- 记录时间：记录产生告警的时间。

23 系统日志

[系统日志]包括命令日志、事件日志、认证日志、PPTP 日志、黑名单日志。

23.1 命令日志

功能描述：记录管理员配置设备的各功能的命令的详细信息。

配置路径：【系统日志】>【命令日志】

配置描述：该页面分两部分，分别是：查询条件、日志列表。

第一、 查询条件。默认显示当前一个月的命令日志。

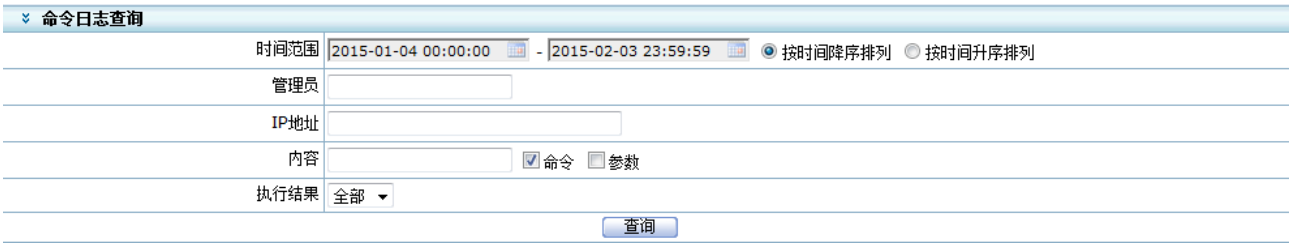


图103. 命令日志-查询条件

参数说明：

- 时间范围：选择日志的时间段。查询结果可以选择[按时间降序排列]或[按时间升序排列]。
- 管理员：配置设备的管理员名称。
- IP 地址：管理员的 IP 地址。
- 内容：执行的命令/参数的内容。
- 执行结果：命令执行成功或者失败。

点击<查询>按钮，命令日志中将显示符合查询条件的记录，详细说明如后。

第二、 命令日志。显示符合查询条件的命令日志。受篇幅所限，下图仅截取前 6 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

序号	管理员	IP地址	内容	执行结果	记录时间
1	admin	172.16.7.77	**访问非法网站告警设置**	成功	2015-02-03 11:14:27
2	admin	172.16.7.77	**搜索违规内容告警设置**	成功	2015-02-03 11:14:25
3	admin	172.16.7.77	**违规邮件主题和内容告警设置**	成功	2015-02-03 11:14:20
4	admin	172.16.7.77	**潜在危害设置**	成功	2015-02-03 11:14:15
5	admin	172.16.7.77	**潜在危害设置** 关键字组: 汪涵 告警级别: 紧急状态 处理策略: 日志记录 出现频率: 2 出现周期: 1	成功	2015-02-03 11:12:11
6	admin	172.16.7.77	**违规邮件主题和内容告警设置** 主题和内容 关键字组: 汪涵 告警级别: 预警状态 处理策略: 日志记录	成功	2015-02-03 11:11:55

图104. 命令日志

按钮说明：

- 导出为 Excel：将查询结果导出为 Excel 表格文件。
- 导出为 HTML：将查询结果导出为 HTML 文件。

23.2 事件日志

功能描述：记录设备发生的各种事件的日志信息。

配置路径：【系统日志】>【事件日志】

配置描述：该页面分两部分，分别是：查询条件、日志列表。

第一、 查询条件。默认显示当前一个月的事件日志。

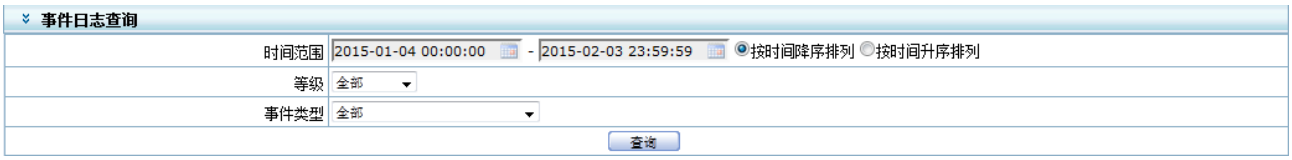


图105. 事件日志-查询条件

参数说明：

- 时间范围：选择日志的时间段。查询结果可以选择[按时间降序排列]或[按时间升序排列]。
- 等级：事件的严重级别，普通状态、预警状态、严重状态、紧急状态。
- 事件类型：管理员登录成功、管理员注销等等。

点击<查询>按钮，事件日志中将显示符合查询条件的记录，详细说明如后。

第二、 事件日志。显示符合查询条件的事件日志。受篇幅所限，下图仅截取前 10 行，请点<下一页>，或<跳转>到指定页，查看更多信息。

序号	等级	事件类型	内容	记录时间
1	普通状态	管理员登录成功	用户名:guest, IP地址:172.16.161.253	2015-02-03 11:20:57
2	普通状态	管理员登录成功	用户名:guest, IP地址:172.16.161.253	2015-02-03 11:19:48
3	普通状态	管理员注销	用户名:admin, IP地址:172.16.161.253	2015-02-03 11:19:40
4	普通状态	管理员登录成功	用户名:admin, IP地址:172.16.166.166	2015-02-03 10:53:40
5	普通状态	管理员登录成功	用户名:admin, IP地址:172.16.7.77	2015-02-03 10:52:04
6	普通状态	管理员登录失败	用户名:amdin, IP地址:172.16.7.77	2015-02-03 10:51:59
7	普通状态	管理员登录成功	用户名:admin, IP地址:172.16.161.253	2015-02-03 10:32:23
8	普通状态	管理员登录失败	用户名:admin, IP地址:172.16.161.253	2015-02-03 10:32:16
9	普通状态	管理员登录成功	用户名:admin, IP地址:172.16.7.77	2015-02-03 09:57:10
10	普通状态	管理员登录失败	用户名:admin, IP地址:172.16.7.77	2015-02-03 09:57:00

图106.　事件日志

按钮说明：

- 导出为 Excel：将查询结果导出为 Excel 表格文件。
- 导出为 HTML：将查询结果导出为 HTML 文件。

23.3认证日志

功能描述：记录用户上、下线及认证模块相关的日志信息。

配置路径：【系统日志】>【认证日志】

配置描述：该页面分两部分，分别是：查询条件、日志列表。

第一、　查询条件。默认显示当前一个月的认证日志。

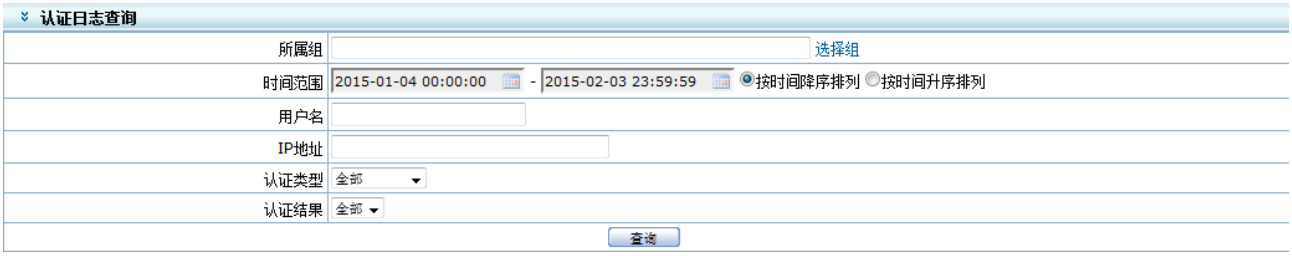


图107.　认证日志-查询条件

参数说明：

- 所属组：选择发起认证请求的用户组。点击<选择组>按钮，进行用户组的选择。
- 时间范围：选择日志的时间段。查询结果可以选择[按时间降序排列]或[按时间升序排列]。
- 用户名：用户名称。
- IP 地址：用户的 IP 地址。
- 认证类型：非 WEB 认证、WEB 认证。[非 WEB 认证]表示不需要进行用户名及密码验证的“普通用户”的自动登录。[WEB 认证]表示需要进行用户名及密码验证，认证方式包括：本地认证、RADIUS 认证、LDAP 认证、AD 认证、POP3 认证.

点击<查询>按钮，认证日志中将显示符合查询条件的记录，详细说明如后。

第二、　认证日志。显示符合查询条件的认证日志。

序号	用户/用户组	IP地址/MAC地址	上线时间	下线时间	发送流量	接收流量	认证信息
1	172.16.9.113	172.16.9.113/A8:66:7F:D5:B3:7B	2015-02-03 11:31:25				认证结果:成功(非WEB认证)
2	172.16.9.113	172.16.9.113/A8:66:7F:D5:B3:7B	2015-02-03 11:30:05	2015-02-03 11:31:23	976	2.47K	认证结果:成功(非WEB认证)
3	172.16.251.251 Root	172.16.251.251/00:E0:4C:36:7D:BA	2015-02-03 11:29:45	2015-02-03 11:30:59	421	614	认证结果:成功(非WEB认证)
4	172.16.0.10	172.16.0.10/08:00:27:00:EA:54	2015-02-03 11:30:43				认证结果:成功(非WEB认证)
5	172.16.166.166	172.16.166.166/74:D4:35:4F:E6:3D	2015-02-03 11:30:23				认证结果:成功(非WEB认证)
6	172.16.110.133	172.16.110.133/08:7A:4C:CF:04:1A	2015-02-03 11:30:17				认证结果:成功(非WEB认证)
7	172.16.6.200	172.16.6.200/8C:89:A5:C1:6D:68	2015-02-03 11:30:06				认证结果:成功(非WEB认证)
8	172.16.9.113	172.16.9.113/A8:66:7F:D5:B3:7B	2015-02-03 11:30:05				认证结果:成功(非WEB认证)
9	172.16.122.199 Root/aa/aa	172.16.122.199/54:04:A6:61:3B:5A	2015-02-03 11:29:55				认证结果:成功(非WEB认证)
10	172.16.16.234	172.16.16.234/BC:30:5B:9C:69:71	2015-02-03 11:29:50				认证结果:成功(非WEB认证)

图108.　认证日志

按钮说明：

- 导出为 Excel：将查询结果导出为 Excel 表格文件。
- 导出为 HTML：将查询结果导出为 HTML 文件。

23.4 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：该页面分两部分，分别是：查询条件、日志列表。

第一、　查询条件。默认显示当前一个月的 PPTP 日志。

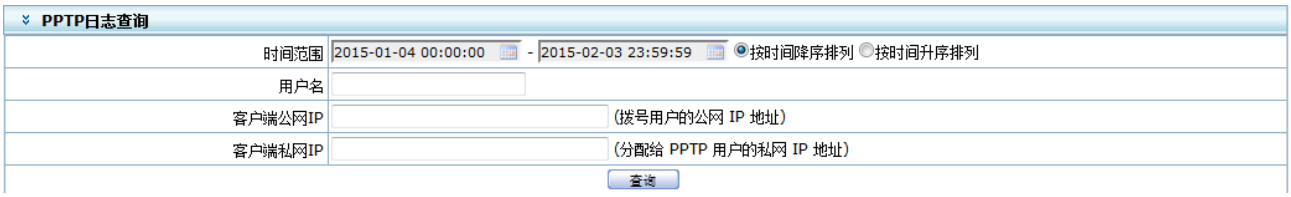


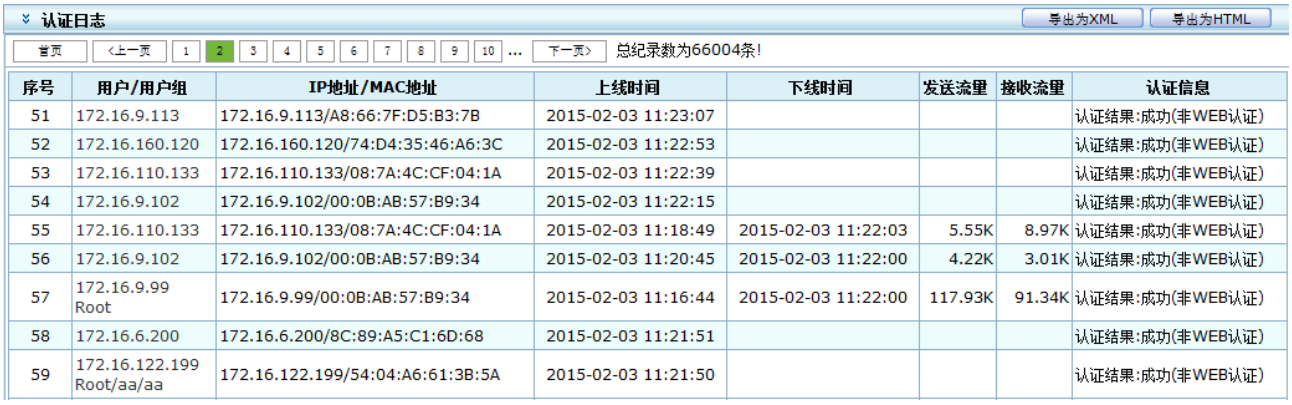
图109.　PPTP-查询条件

参数说明：

- 时间范围：选择日志的时间段。查询结果可以选择[按时间降序排列]或[按时间升序排列]。
- 用户名：拨号客户端的用户名称。
- 客户端公网 IP：拨号用户的公网 IP 地址。
- 客户端私网 IP：分配给 PPTP 用户的私网 IP 地址。

点击<查询>按钮，黑名单日志中将显示符合查询条件的记录，详细说明如后。

第二、　PPTP 日志。显示符合查询条件的 PPTP 日志。



序号	用户/用户组	IP地址/MAC地址	上线时间	下线时间	发送流量	接收流量	认证信息
51	172.16.9.113	172.16.9.113/A8:66:7F:D5:B3:7B	2015-02-03 11:23:07				认证结果:成功(非WEB认证)
52	172.16.160.120	172.16.160.120/74:D4:35:46:A6:3C	2015-02-03 11:22:53				认证结果:成功(非WEB认证)
53	172.16.110.133	172.16.110.133/08:7A:4C:CF:04:1A	2015-02-03 11:22:39				认证结果:成功(非WEB认证)
54	172.16.9.102	172.16.9.102/00:0B:AB:57:B9:34	2015-02-03 11:22:15				认证结果:成功(非WEB认证)
55	172.16.110.133	172.16.110.133/08:7A:4C:CF:04:1A	2015-02-03 11:18:49	2015-02-03 11:22:03	5.55K	8.97K	认证结果:成功(非WEB认证)
56	172.16.9.102	172.16.9.102/00:0B:AB:57:B9:34	2015-02-03 11:20:45	2015-02-03 11:22:00	4.22K	3.01K	认证结果:成功(非WEB认证)
57	172.16.9.99 Root	172.16.9.99/00:0B:AB:57:B9:34	2015-02-03 11:16:44	2015-02-03 11:22:00	117.93K	91.34K	认证结果:成功(非WEB认证)
58	172.16.6.200	172.16.6.200/8C:89:A5:C1:6D:68	2015-02-03 11:21:51				认证结果:成功(非WEB认证)
59	172.16.122.199 Root/aa/aa	172.16.122.199/54:04:A6:61:3B:5A	2015-02-03 11:21:50				认证结果:成功(非WEB认证)

图110.　PPTP 日志

参数和按钮说明：

- 用户名：拨号客户端的用户名称。
- 客户端 IP 地址：拨号客户端用户的 IP 地址。
- 接口：设备作为 PPTP 服务器的接口名称。
- 服务器 IP 地址：设备作为 PPTP 服务器的 IP 地址。
- 上线时间：PPTP 客户端上线的时间。
- 下线时间：PPTP 客户端下线的时间。
- 导出为 Excel：将查询结果导出为 Excel 表格文件。
- 导出为 HTML：将查询结果导出为 HTML 文件。

23.5 黑名单日志

功能描述：显示用户进入和解除黑名单的日志信息。

配置路径：【系统日志】>【黑名单日志】

配置描述：该页面分两部分，分别是：查询条件、日志列表。

第三、　查询条件。默认显示当前一个月的黑名单日志。

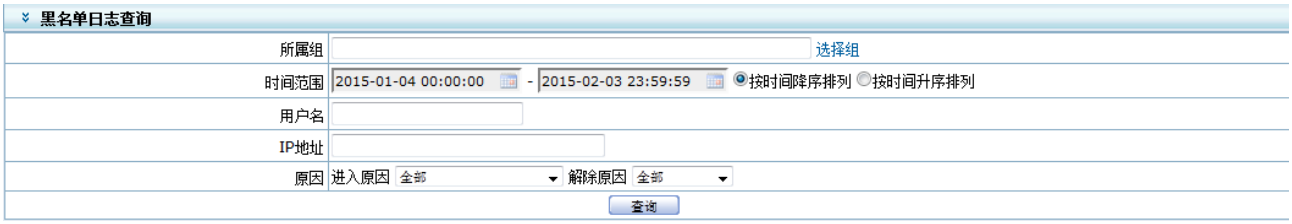


图111.　黑名单日志-查询条件

参数说明：

- 所属组：选择进出黑名单的用户组。点击<选择组>按钮，进行用户组的选择。
- 时间范围：选择日志的时间段。查询结果可以选择[按时间降序排列]或[按时间升序排列]。
- 用户名：用户名称。

- IP 地址：用户的 IP 地址。
- 原因：选择[进入黑名单]和[解除黑名单]的原因。

点击<查询>按钮，黑名单日志中将显示符合查询条件的记录，详细说明如后。

第四、 黑名单日志。显示符合查询条件的黑名单日志。

黑名单日志

导出为XML 导出为HTML

序号	用户/用户组	IP地址	MAC地址	进入原因	进入时间	解除原因	解除时间	黑名单规则
1	172.16.7.89	172.16.7.89	FC:AA:14:77:D9:F9		2015-01-21 13:36:52	惩罚时间到期	2015-01-21 14:36:57	TEST
2	172.16.110.140	172.16.110.140	A0:ED:CD:21:4B:CE	超出每日总流量配额 进入值: 0.000G 限定值: 0.000G	2015-01-13 16:53:58	惩罚时间到期	2015-01-13 17:54:10	手机
3	aaaaaaaaaaa			手动加入黑名单	2015-01-05 18:32:32	手动解除	2015-01-05 18:32:36	
4	ddddddddd			手动加入黑名单	2015-01-05 18:32:29	手动解除	2015-01-05 18:32:36	
5	sssssssssssssssssssssss			手动加入黑名单	2015-01-05 18:32:26	手动解除	2015-01-05 18:32:36	
6	ddddddddddddddd			手动加入黑名单	2015-01-05 17:50:24	手动解除 aaaaaaaaaa	2015-01-05 18:26:06	
7	nnnnnnnnn			手动加入黑名单	2015-01-05 17:50:21	手动解除 ddddddddd	2015-01-05 18:26:02	
8	ppppppppppp			手动加入黑名单	2015-01-05 17:18:45	手动解除 aaaaaaa	2015-01-05 17:18:48	

图112. 黑名单日志

参数和按钮说明：

- 用户/用户组：进入黑名单的用户名及其用户组。
- IP 地址：黑名单用户的 IP 地址。
- MAC 地址：黑名单用户的 MAC 地址。
- 进入原因：以何种原因进入黑名单，如：超出每日总流量配额、超出最大下行速率等。
- 进入时间：进入黑名单的时间。
- 解除原因：以何种原因退出黑名单。如：惩罚时间到期、或管理员手动解除。
- 解除时间：退出黑名单的时间。
- 黑名单规则：被哪一条黑名单规则所控制。
- 导出为 Excel：将查询结果导出为 Excel 表格文件。
- 导出为 HTML：将查询结果导出为 HTML 文件。

24数据管理

“数据管理”包含了对数据库里存储的各类数据的显示、删除和备份。

24.1 数据列表

功能描述：显示当前数据库里存储的各类数据的相关信息。

配置路径：【数据管理】>【数据列表】

配置描述：进入该页面，可以看到各类数据的大小、磁盘空间占有率、以及记录的数据的起始至结束的时间范围。如下图所示：

数据列表

数据类型	大小(byte)	磁盘占用率	时间范围
所有行为	497.52M	0.17%	2014-12-05 - 2015-02-03
网页标题	55.62M	0.02%	2014-12-05 - 2015-02-03
网页URL	528.14M	0.18%	2014-12-05 - 2015-02-03
网页搜索	10.11M	0.00%	2014-12-05 - 2015-02-03
邮件收发	4.97M	0.00%	2014-12-05 - 2015-02-03
IM聊天	3.00M	0.00%	2014-12-05 - 2015-02-03
论坛微博	2.96M	0.00%	2014-12-05 - 2015-02-03
帐号登录	4.23M	0.00%	2014-12-05 - 2015-02-03
外发文件	27.44M	0.01%	2014-12-05 - 2015-02-03
外发信息	118.43M	0.04%	2014-12-05 - 2015-02-03
telnet 命令	60.00K	0.00%	2014-12-05 - 2015-02-03
阻断记录	2.67M	0.00%	2014-12-05 - 2015-02-03
会话记录	1.42G	0.49%	2014-12-05 - 2015-02-03
告警记录	644.00K	0.00%	2014-12-05 - 2015-02-03
系统日志	30.17M	0.01%	2014-12-05 - 2015-02-03
统计分析数据	1.14G	0.40%	2014-12-05 - 2015-02-03

磁盘总空间: 288.75G　已用空间: 17.66G(6.11%)　可用空间: 256.19G(93.89%)

图113.　数据列表

备注：若因存储的数据量很大，读取本页时可能需要花一点时间，请耐心等待。

24.2 数据删除

功能描述：删除当前数据库里的存储数据。

配置路径：【数据管理】>【数据删除】

配置描述：进入该页面，选择需要删除的数据。如下图所示：

图114.　数据删除

参数说明：

- 删除类型：选择“删除所有数据”或者“按以下配置删除”。如果选择“删除所有数据”，则将整个数据库里的数据全部删除。如果选择“按以下配置删除”，则按照后面的配置选项来删除其中一部分数据。
- 时间范围：选择需要删除的数据的时间范围。比如删除 2011-11-03 至 2011-11-04 的数据。
- 删除内容：选择需要删除的数据的类型，比如删除“会话记录”。

25 报表管理

[报表管理]是将存储在数据库里的数据生成 PDF、Excel 或 HTML 的格式的报表，并可以邮件的方式发送到管理员邮箱。[报表管理]包含[自动报表]和[手动报表]两种。[自动报表]是指设定一个周期时间，设备在每个周期对应的时间点自动将数据生成报表文件。[手动备份]是根据需要手动设置一个时间点生成一次性的报表。

25.1 自动报表列表

功能描述：显示、下载或删除已生成的自动报表。

配置路径：【报表管理】>【自动报表列表】

配置描述：进入该页面，已生成的自动报表如下图所示：

图115. 自动报表列表

参数及按钮说明：自动报表按照[日报]、[周报]、[月报]、[年报]分页显示。

- 日报：每日的数据生成一个报表。
- 周报：每周的数据生成一个报表。
- 月报：每月的数据生成一个报表。
- 年报：每年的数据生成一个报表。
- 语言：报表文件的语言，可能为简体中文、繁體中文、English。
- 日期：显示[日报]的日期。
- 周：显示[周报]的日期范围。
- 月份：显示[月报]的年月。
- 年：显示[年报]的年份。
- 创建时间：生成报表的时间。
- 报表格式：报表的文件格式，目前为 PDF。
- 清空：点击<清空>按钮，清除当前选项卡对应的报表文件。
- 下载：点击<下载>按钮，下载对应报表文件。
- 删除：点击<删除>按钮，删除对应报表文件。

25.2 自动报表配置

功能描述：设置自动生成报表的相关参数，设备将根据设置定期自动的生成报表文件。

配置路径：【报表管理】>【自动报表配置】

配置描述：进入该页面，配置自动报表的相关参数。如下图所示：

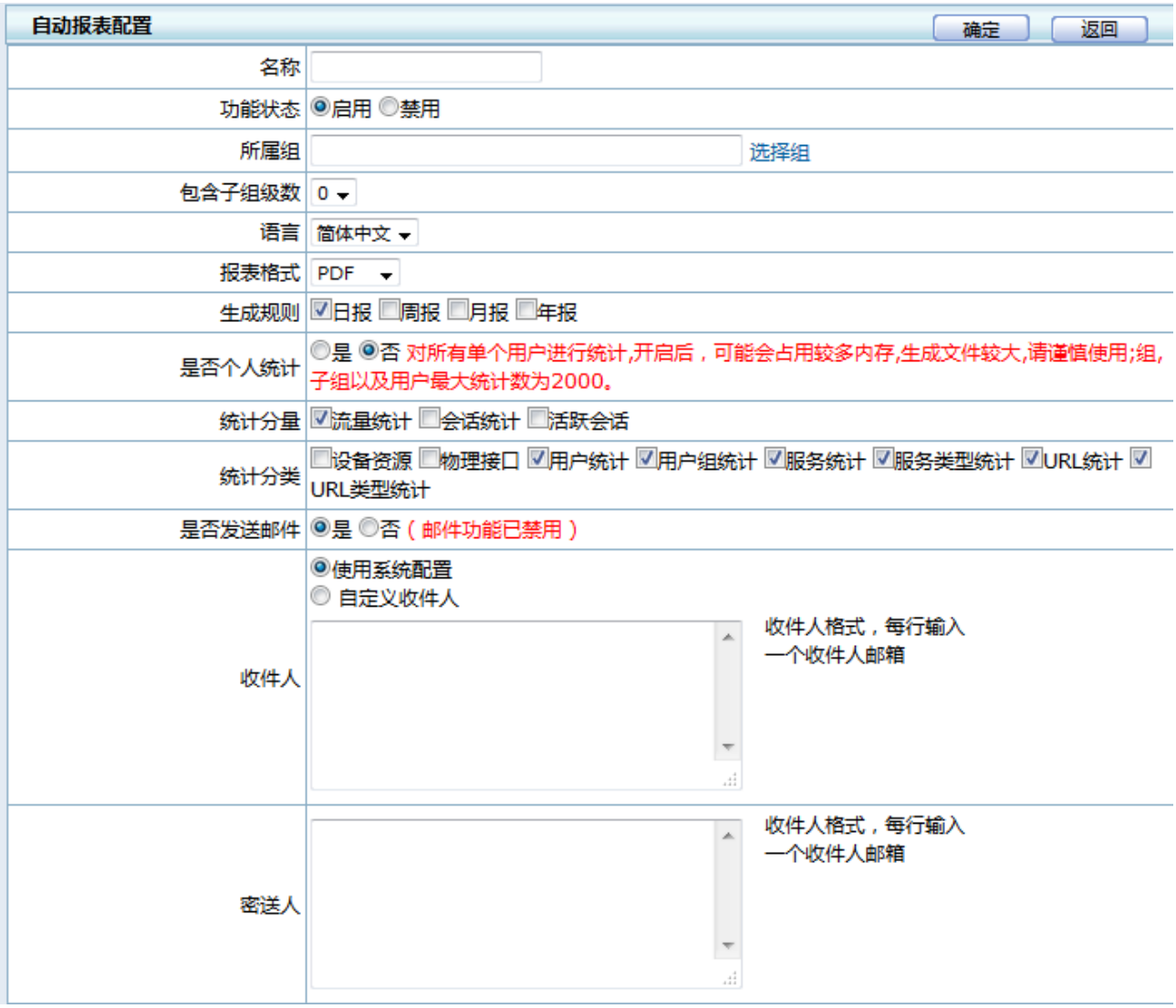


图116.　自动报表

参数说明：

- 功能状态：[启用]或[禁用]自动生成报表的功能。
- 包含子组级数：从根开始，包含子组的级数，根组为 0 级。大于所设定的级数的子组，将自动提升为与设定的子组平级。例如，组织结构包含 5 级子组，[包含子组级数]设定为 3，在报表文件中，则第 4、5 两级子组自动与第 3 组平级显示。
- 语言：选择报表文件的语言，简体中文、繁体中文、英语。
- 报表格式：可选择生成 PDF、Excel 或 HTML 的格式的报表。
- 生成规则：可定义生成的自动报表是日报、周报、月报还是年报。
- 是否个人统计：是否开启对单个用户的统计。注：当开启个人统计后，可能会占用较多内存,生成文件较大,请谨慎使用;组,子组以及用户最大统计数为 2000。
- 统计分量：选择需要生成报表的模块，包括流量统计、会话统计、活跃会话统计。
- 统计分类：选择需要生成报表的内容，包括物理接口、用户统计、用户组统计、服务统计、服务类型统计、URL 统计、URL 类型统计。

- 是否发送邮件：是否将报表文件以邮件的方式发送给管理员。若选择[是]，则继续设置[收件人]。
- 收件人：接收报表文件的邮箱地址。默认[使用系统配置]，即在设备配置页面设定的邮件配置的收件人，括号里面显示当前系统配置收件人地址。[自定义收件人]表示可自定义收件人邮箱地址，可定义多个地址，一行一个地址。
- 密送人：接收报表文件的密送邮箱地址，每行一个收件人邮箱，可定义多个地址。

25.3 手动报表

功能描述：根据需要手动生成报表，设备将根据设置的参数在指定时间生成报表文件，仅生成一次。

配置路径：【报表管理】>【手动报表】

配置描述：

第一：进入该页面，将看到当前已设置好的报表策略及已经生成的报表文件。如下图所示：

图117.　手动报表

按钮说明：

- 新增：新增一条手动报表策略。
- 清空：清空当前所有手动报表策略。
- 删除：删除某条手动报表策略。
- 下载：下载已生成的报表文件。

第二：点击<新增>按钮，增加手动报表策略，如下图：

图118.　新增手动报表

参数说明：

- 时间范围：选择需要生成报表的数据的时间范围。
- 语言：选择报表文件的语言，简体中文、繁体中文、英语。

- 报表格式：可选择生成 PDF、Excel 或 HTML 的格式的报表。
- 所属组：选择报表的用户组。
- 包含子组级数：从根开始，包含子组的级数，根组为 0 级。大于所设定的级数的子组，将自动提升为与设定的子组平级。例如，组织结构包含 5 级子组，[包含子组级数]设定为 3，在报表文件中，则第 4、5 两级子组自动与第 3 组平级显示。
- 统计分量：选择需要生成报表的模块，包括流量统计、会话统计、活跃会话统计。
- 是否发送邮件：是否将报表文件以邮件的方式发送给管理员。若选择[是]，则继续设置[收件人]。
- 计划执行时间：设置开始生成本次报表的时间。

26 系统配置

功能描述：配置[每页显示的记录数]和[最大导出记录数]。

配置路径：【系统配置】>【参数配置】

配置描述：进入该页面，[每页显示的记录数]和[最大导出记录数]如下图所示：

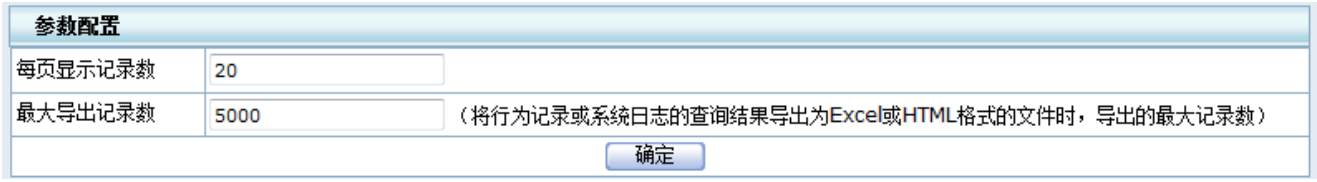


图119. 系统参数设置

参数说明：

- 每页显示的记录数：设置每页显示的记录数，即行数。
- 最大导出记录数：将行为记录或系统日志的查询结果导出为 Excel 或 HTML 格式的文件时，导出的最大记录数。随着数据存储时间的增长，比如 1 年、2 年，行为记录或系统日志的条目数可能会很多，这里设定导出的最大条目数。

27 个人行为

“个人行为”是对内网中单个用户的上网行为进行汇总与记录，包括：综合记录、WEB 记录、邮件收发、IM 聊天、账号登入、外发文件、Telnet 命令、导出。

点击网页左上角的<**个人行为**>选项卡，进入个人行为记录的菜单。个人行为记录的整体页面分 6 个区域，结合下图分别说明每个区域的功能。

1. 区域 1：[个人行为]选项卡。
2. 区域 2：用户组的显示，可选择需要查看的用户组。
3. 区域 3：选择某个用户组后，此处显示该组包含的用户，可选择需要查看的用户。最上面的输入框中输入用户名或 IP 地址可以查询符合条件的用户。

-

：表示该组共 3 个用户，有 1 个用户在线。
- ：表示该用户在线。
- ：表示该用户离线。

4. 区域 4：功能区，包括：综合记录、WEB 记录、邮件收发、IM 聊天、账号登入、外发文件、Telnet 命令、导出。
5. 区域 5：内容显示区，显示被选中的用户对应的行为内容的记录。
6. 区域 6：查询区，选择需要查看的行为记录的时间段，然后点击<查询>按钮，区域 5 将显示对应时间段的行为记录。

图120. 个人行为-整体风格说明

27.1 综合记录

“综合记录”是对单个用户的上网行为的各类数据进行汇总显示。分别包括 WEB 记录、邮件收发、IM 聊天、账号登入、外发文件、Telnet 命令。**配置路径：**【个人行为】>【选择用户组】>【选择用户】>【综合】

- WEB 记录：用户网页访问的各种记录，详细如下。
  - 网页标题：对各类网站访问记录的汇总，如下图。

网页标题

URL类型	网页标题数
总计	194
Webmail	44
搜索引擎	37
电子银行	34
其他网站	25
新闻门户	17
交友聊天	15
论坛	5
IT相关	4
博客	3
游戏	2
软件下载	2
网上购物	1
周刊媒体	1

- ✧ 网页搜索：在各种搜索引擎上搜索次数的汇总，如下图

网页搜索

搜索引擎名称	总计	百度搜索建议	百度-网页
搜索次数	141	84	57

- ✧ 论坛微博：在各类网站发表的帖子或者网页评论的汇总。
- ✧ 外发文件：对在外发信息次数记录的汇总。

外发信息

外发信息次数	总计
1007	1007

- ✧ URL 记录：显示占前 5 名的 URL 的访问次数，如下图。

URL

URL	总计	12306.cn	qq.com	mail.qq.com	sogou.com	show.qq.com
访问次数	8781	5271	1460	434	285	277

- ➢ 邮件收发：用户邮件收发的各种记录，详细如下。
  - ✧ 邮件记录：各邮箱帐号对应的发送邮件的数量和接收邮件的数量的汇总，如下图。

邮件记录

邮件帐号	发件数	收件数
3654456 - QQ邮箱	7	0
lyqjixian@126.com - 126邮箱	1	0
lyqjixian@163.com - 163邮箱	1	0

- ➢ IM 聊天：各种 IM 聊天类型的记录，详细如下。
  - ✧ IM 聊天，分别记录、登录次数、聊天记录数各种即时通讯软件的统计内容相似，下图 QQ 记录的截图：

IM聊天

聊天类型	聊天帐号	聊天数
QQ	24743208241	29

- ➢ 账号登入：登录账号的次数汇总，如下图。

帐号登录

登录网站	总计	Skype
网页登录次数	1	1

- 外发文件：记录外发文件的类型和文件数量的汇总，如下图。

外发文件

文件类型	文件数量
总计	8
HTTP上传	1
IM传文件	5
EMAIL传文件	2

- Telnet 命令：记录 Telnet 命令数汇总，如下图。

telnet 命令

命令数
0

27.2 WEB 记录

[WEB 记录]是对单个用户访问网页时进行分类统计，包括：网页标题、网页搜索、论坛微博、外发信息、URL。

27.2.1 网页标题

配置路径：【个人行为】>【选择用户组】>【选择用户】>【WEB 记录】>【网页标题】，如下图：

图121. 个人行为-WEB 记录-网页标题记录

参数说明：

- 网页标题：WEB 网页的标题。
- URL 类型：该网页属于那个类型的网站。
- URL 地址：网页对应的 URL 地址。如果 URL 地址过长，默认将省略后面字符的显示。
  - 点击 URL 地址，链接到该页面。

- ✧ 点击<展开>按钮，可以将整个 URL 地址显示出来。
- ✧ 点击<收起>按钮，将 URL 地址中过长的字符省略显示。

➢ 记录时间：记录该信息的时间。

查询条件：

➢ 开始时间：选择记录的开始时间。

➢ 结束时间：选择记录的截至时间。

➢ 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。

➢ 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。

➢ 关键字：[网页标题]或[URL 地址]的关键字，支持模糊查询。

➢ URL 类型：选择 URL 的分类，比如新闻门户、搜索引擎等。

➢ 每页显示记录数：每页显示的最大行数。

27.2.2 网页搜索

配置路径：【个人行为】>【选择用户组】>【选择用户】>【WEB 记录】>【网页搜索】，如下图：

图122. 个人行为-WEB 记录-网页搜索

参数说明：

➢ 关键字：在搜索引擎上搜索的关键字。

➢ 搜索引擎名称：搜索引擎的名称，如百度-网页、百度-图片。

➢ 搜索引擎类型：搜索引擎的分类，如 Googel、百度。

➢ 记录时间：记录该信息的时间。

查询条件：

➢ 开始时间：选择记录的开始时间。

- 结束时间：选择记录的截至时间。
- 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。
- 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。
- 关键字：在搜索引擎上搜索的关键字，支持模糊查询。
- 搜索引擎类型：搜索引擎的分类，如 Googel、百度。
- 搜索引擎名称：搜索引擎的名称，如百度-网页、百度-图片。
- 每页显示记录数：每页显示的最大行数。

27.2.3 论坛微博记录

配置路径：【个人行为】>【选择用户组】>【选择用户】>【WEB 记录】>【论坛微博】，如下图：

图123. 个人行为-WEB 记录-发帖及网评记录

参数说明：

- 论坛名称：在哪个论坛上发的帖子。
- 论坛类型：论坛的分类，如微博博客、娱乐、军事。
- 发帖标题：发送的帖子的标题。
- 发帖内容：发送帖子的正文内容。
- 发帖附件：帖子中附带的文件。
- 记录时间：记录该信息的时间。

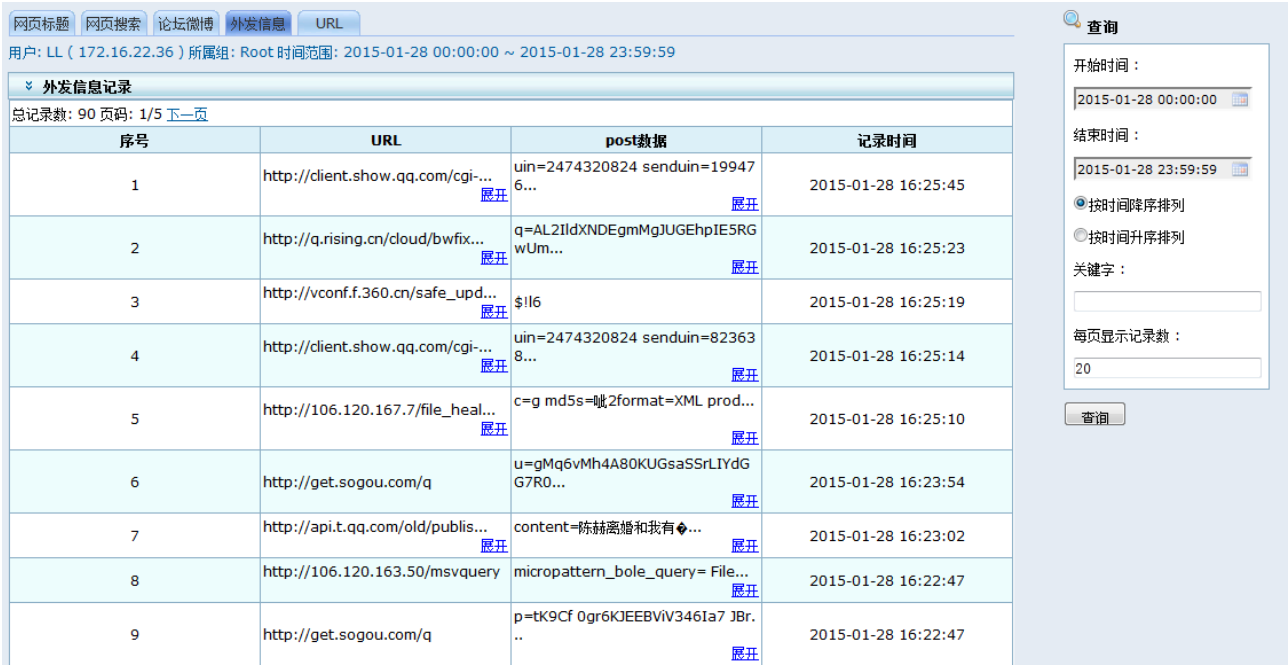
查询条件：

- 开始时间：选择记录的开始时间。

- 结束时间：选择记录的截至时间。
- 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。
- 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。
- 关键字：发帖标题、发帖内容、发帖附件的名称所包含的关键字，支持模糊查询。
- 论坛类型：论坛的分类，如娱乐、军事。
- 论坛名称：在哪个论坛上发的帖子。

27.2.4 外发信息

配置路径：【个人行为】>【选择用户组】>【选择用户】>【WEB 记录】>【外发信息】，如下图：



参数说明：

- URL：外发信息的 URL。
- post 数据：显示 post 数据。
- 记录时间：记录该信息的时间。

查询条件：

- 开始时间：选择记录的开始时间。
- 结束时间：选择记录的截至时间。
- 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。
- 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。
- 关键字：发帖标题、发帖内容、发帖附件的名称所包含的关键字，支持模糊查询。
- 每页显示记录数：每页显示的最大行数。

27.2.5 URL

配置路径：【个人行为】>【选择用户组】>【选择用户】>【WEB 记录】>【URL】，如下图：

图124. 个人行为-WEB 记录-URL

参数说明：

- URL：URL 地址的前缀。
- URL 类型：URL 的分类，如博客、IT 相关、法律、军事。
- URL 地址：详细的 URL 地址。点击该地址，可以打开对应网页。
- 记录时间：记录该信息的时间。

查询条件：

- 开始时间：选择记录的开始时间。
- 结束时间：选择记录的截至时间。
- 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。
- 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。
- 关键字：URL 或 URL 地址包含的关键字，支持模糊查询。
- URL 类型：URL 的分类，如法律、军事。
- 每页显示记录数：每页显示的最大行数。

27.3 邮件收发

配置路径：【个人行为】>【选择用户组】>【选择用户】>【邮件收发】，如下图：

图125.　个人行为-邮件收发

参数说明：

- WebMail 收发件：若使用 WebMail 收发过邮件。若是 QQ 邮箱，便会出现[QQ 邮箱]。若是新浪邮箱，便会出现[新浪邮箱]。点击此，右边区域显示以 WebMail 方式收发的邮件。

查询条件：

- 开始时间：选择记录的开始时间。
- 结束时间：选择记录的截至时间。
- 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。
- 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。
- 关键字：邮件主题、邮件附件。邮件内容的关键字，支持模糊查询。
- 每页显示记录数：每页显示的最大行数。

邮件详细信息：

- 点击上图某条邮件记录，查看该邮件的详细信息，如下图：

图126.　个人行为-邮件记录-详细信息

- 点<返回>按钮，返回到邮件列表页面。

27.4 IM 聊天

“IM 聊天”是对单个用户的即时通讯软件的通信记录，包含登录记录、聊天记录、文件传输记录。支持的即时通信软件包括：QQ、MSN、Yahoo、ICQ、飞信、Gtalk、阿里旺旺、飞信。

27.4.1 QQ 通讯记录

配置路径：【个人行为】>【选择用户组】>【选择用户】>【即时通讯】>【QQ】，如下图：

图127.　个人行为-即时通讯-QQ 聊天记录

QQ 聊天记录页面模仿 QQ 聊天工具的方式呈现。

- 区域 1：内网用户的 QQ 账户，括号里面的数字表示该 QQ 账户与几个好友有聊天记录。点击账户，可展开与该账户有聊天记录的好友列表。
- 区域 2：与内网用户有聊天记录的 QQ 好友账户。选择某个好友，区域 3 即呈现与该好呀的聊天记录。
- 区域 3：好友聊天记录。

查询条件：

- 开始时间：选择记录的开始时间。
- 结束时间：选择记录的截至时间。
- 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。
- 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。
- 关键字：查询聊天记录，支持模糊查询。

- 每页显示记录数：每页显示的最大行数。

27.4.2 MNS 通讯记录

MNS 通讯记录的查看方式与 QQ 通讯记录相同，此处省略。

27.4.3 Yahoo 通讯记录

Yahoo 通讯记录的查看方式与 QQ 通讯记录相同，此处省略。

27.4.4 SKYPE 通讯记录

SKYPE 通讯记录的查看方式与 QQ 通讯记录相同，此处省略。

27.4.5 Gtalk 通讯记录

Gtalk 通讯记录的查看方式与 QQ 通讯记录相同，此处省略。

27.4.6 阿里旺旺通讯记录

阿里旺旺通讯记录的查看方式与 QQ 通讯记录相同，此处省略。

27.4.7 飞信通讯记录

飞信通讯记录的查看方式与 QQ 通讯记录相同，此处省略。

27.5 账号登入

27.5.1 账号登入记录

配置路径：【个人行为】>【选择用户组】>【选择用户】>【账号登入】，如下图：

图128.　个人行为-账号登入

参数说明：

- 帐号登入：记录登录的账户。
- 应用类型：显示应用的类型。
- 记录时间：记录该信息的时间。

查询条件：

- 开始时间：选择记录的开始时间。
- 结束时间：选择记录的截至时间。
- 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。
- 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。
- 登入账号：输入要查询的账号。
- 登入网站的类型：选择登陆网站的类型。
- 登入网站：选择登入的网站。
- 每页显示记录数：每页显示的最大行数。

27.6外发文件

“外发文件”是记录单个用户的外发文件不同类型的信息

27.6.1 外发文件

配置路径：【个人行为】>【选择用户组】>【选择用户】>【外发文件】，如下图：

参数说明：

- 文件名：记录外发的文件名称以及其后缀如.ppt、.docx 等等。
- 文件大小：记录文件的大小。
- 发送方式：记录文件的发送方式，比如 POP3 邮件发送方式、QQ 发送方式等等。
- 记录时间：记录该信息的时间。

查询条件：

- 开始时间：选择记录的开始时间。
- 结束时间：选择记录的截至时间。
- 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。
- 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。
- 关键字：输入关键字进行查询，支持模糊查询。
- 每页显示记录数：每页显示的最大行数。

27.7 Telnet 命令

“Telnet 命令”是记录单个用户的外发文件不同类型的信息

27.7.1 Telnet 命令

配置路径：【个人行为】>【选择用户组】>【选择用户】>【Telnet 命令】，如下图：

参数说明：

- Telnet 命令：记录 Telnet 的命令。
- Telnet 命令结果：记录 Telnet 命令的结果。
- 记录时间：记录该信息的时间。

查询条件：

- 开始时间：选择记录的开始时间。
- 结束时间：选择记录的截至时间。
- 按时间降序排列：查询结果按时间降序排练，最近是记录放在最前面。
- 按时间升序排列：查询结果按时间升序排练，最早是记录放在最前面。
- 关键字：Telnet 命令、Telnet 命令结果的关键字，支持模糊查询。
- 每页显示记录数：每页显示的最大行数。

图129.　个人行为-Telnet 命令

27.8导出个人行为记录

“导出个人行为记录”是将单个用户的上网行为的数据导出为 Excel 或 HTML 文件。

配置路径：【个人行为】>【选择用户组】>【选择用户】>【导出】，如下图：

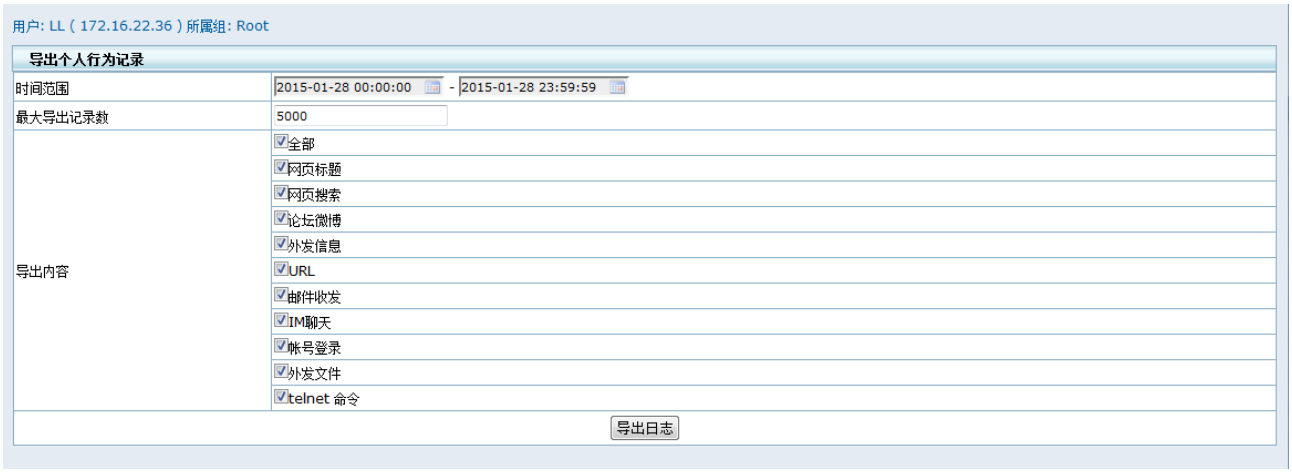


图130.　个人行为- 导出个人行为记录

参数和按钮说明：

- 时间范围：选择需要导出的数据的时间范围。比如删除 2011-11-03 至 2011-11-04 的数据。
- 最大导出记录数：将数据导出为 Excel 或 HTML 格式的文件时，导出的最大记录数（1-100000）。随着数据存储时间的增长，比如 1 年、2 年，数据的条目数可能会很多，这里设定导出的最大条目数。
- 导出内容：选择需要导出的数据的类型，比如导出“网页标题记录”。

  导出日志：将所选数据导出，默认导出