
东软 NetEye 网络审计系统 V5.0

用 户 手 册

2014 年 9 月

目 录

第一部分	产品快速向导	1
1	图形界面格式约定	1
2	环境要求	1
3	接线方式	1
4	登录设备	2
5	刷新/保存/注销	3
6	密码恢复	3
第二部分	产品配置	4
7	设备状态	4
8	实时监控	6
8.1	设备资源	6
8.2	物理接口	7
8.3	服务监控	8
8.3.1	服务趋势叠加图	8
8.3.2	服务组趋势图	9
8.3.3	活跃服务统计	10
8.3.4	所有服务统计	10
8.4	用户监控	11
8.4.1	流量分析	11
8.4.2	会话分析	12
8.4.3	活跃会话	13
8.5	上网行为	14
8.6	在线用户	15
8.7	防共享上网	17
8.8	当前黑名单	18
8.9	应用限额用户	20
9	系统配置	21
9.1	设备工作模式	21
9.1.1	网桥模式	21
9.1.2	路由模式	23
9.1.3	旁路模式	24
9.2	系统维护	25
9.2.1	系统升级	25
9.2.2	自动升级	27
9.2.3	备份与恢复	28
9.2.4	重启/关机	29
9.3	系统管理员	30
9.3.1	配置系统管理员	30
9.3.2	角色管理	32
9.4	网管策略	33
9.5	网管参数	34

9.6	网络工具	35
9.6.1	Ping	35
9.6.2	TraceRoute	36
9.7	系统时间	37
9.8	系统信息	38
9.9	邮件配置	38
9.10	集中管理	39
10	系统对象	40
10.1	地址簿	40
10.2	网络服务	41
10.2.1	内置服务	41
10.2.2	自定义普通服务	42
10.2.3	自定义特征识别	43
10.2.4	自定义论坛/网评特征	44
10.2.5	协议剥离	45
10.3	时间计划	47
10.4	URL 库	48
10.5	关键字组	49
10.6	文件类型	50
11	网络配置	52
11.1	接口配置	52
11.1.1	物理接口	52
11.1.2	链路聚合	53
11.1.3	VLAN 接口	54
11.1.4	PPPoE	55
11.1.5	DHCP 客户端	56
11.1.6	GRE 隧道	56
11.2	配置 IP 地址	57
11.3	静态路由	58
11.4	OSPF 路由	59
11.4.1	网络配置	59
11.4.2	接口配置	60
11.4.3	参数配置	61
11.4.4	虚连接配置	62
11.4.5	信息显示	63
11.5	策略路由	65
11.5.1	策略路由	65
11.5.2	均衡策略	67
11.5.3	持续路由	69
11.5.4	链路健康检查	70
11.6	DNS 配置	72
11.7	DDNS 配置	73
11.8	智能 DNS	73
11.8.1	全局配置	74

11.8.2	线路配置	74
11.8.3	均衡策略	75
11.8.4	DNS 策略	77
11.9	ARP 表	79
11.10	DHCP 配置	80
11.10.1	基本参数	80
11.10.2	DHCP 中继	81
11.10.3	已分配 IP 地址	82
11.11	SNMP 服务器	82
11.12	代理服务器列表	82
11.13	代理配置	83
12	防火墙	85
12.1	安全策略	85
12.2	NAT 规则	87
12.2.1	内网代理	87
12.2.2	一对一地址转换	88
12.2.3	端口映射	90
12.2.4	服务器池	92
12.3	防 DOS 攻击	93
12.4	ARP 欺骗防护	94
12.5	应用层网关	95
12.6	加速老化	96
12.7	防病毒设置	97
12.8	移动终端管理	97
13	VPN 配置	99
13.1	IPSec	99
13.1.1	IPSec 隧道	99
13.1.2	IPSec 规则	100
13.2	PPTP	102
13.3	L2TP	103
13.4	VPN 用户	104
14	组织管理	105
14.1	组织结构	105
14.1.1	定位并选中当前操作对象	105
14.1.2	修改根组	106
14.1.3	新增子组	106
14.1.4	修改子组	107
14.1.5	新增普通用户	109
14.1.6	新增认证用户	110
14.1.7	修改用户	111
14.1.8	绑定检查	112
14.1.9	导出用户和组	116
14.1.10	移动用户和组	117
14.1.11	删除用户和组	118

14.1.12	查询用户和组	119
14.2	批量导入	120
14.3	LDAP/AD 导入	120
14.4	扫描内网主机	122
14.5	临时账户管理	124
14.5.1	临时账户设置	124
14.5.2	申请临时账户的步骤（页面与 Email 获取密码）	127
14.5.3	申请临时账户的步骤（短信获取密码）	129
14.5.4	未审核账户列表	130
14.5.5	已审核账户列表	131
14.5.6	批量生成	131
14.6	Dkey 管理	132
15	流量管理	133
15.1	线路带宽配置	133
15.2	基于策略的流控	134
15.3	基于用户的流控	137
16	行为管理	141
16.1	认证策略	142
16.2	上网策略	145
16.2.1	上网权限策略	145
16.2.2	终端提醒策略	155
16.2.3	准入策略	158
16.2.4	应用限额策略	162
16.2.5	黑名单策略	163
16.2.6	上网审计策略	166
16.3	认证选项	169
16.3.1	跨三层 MAC 识别	169
16.3.2	认证参数	170
16.3.3	自定义认证页面	171
16.3.4	未认证权限	172
16.3.5	SSO	173
16.3.6	短信认证	181
16.4	认证服务器	184
16.4.1	RADIUS 服务器	184
16.4.2	AD 服务器	185
16.4.3	LDAP 服务器	186
16.4.4	POP3 服务器	187
16.4.5	服务器测试	188
16.5	白名单管理	189
16.5.1	IP 白名单	190
16.5.2	URL 白名单	191
16.5.3	即时通讯白名单	192
17	酒店管理-即插即用	193
18	高可靠性(HA)	195

19	系统日志	197
19.1	命令日志	197
19.2	事件日志	198
19.3	PPTP/L2TP 日志	199
19.4	IPSec 日志	199
19.5	黑名单日志	200
19.6	安全日志	201
19.7	日志服务器	202
19.8	短信配置	203
19.9	告警配置	203
20	故障排除	209
20.1	捕获数据包	209
20.2	查看数据包	210
20.3	调试信息下载	210
20.4	上网故障调试	211
21	报表中心	212
21.1	报表中心配置	212
21.2	内置报表中心	213

第一部分 产品快速向导

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 环境要求

设备系列产品可在如下环境使用：

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

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

提示：

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

3 接线方式

请按照如下步骤进行设备的接线：



- 1、 在后面板电源插座上插上电源线,打开电源开关,前面板的 Power 灯(绿色,电源指示灯)和 Alarm 灯(红色,告警灯)会点亮。大约 1-2 分钟后 Alarm 灯熄灭,说明设备正常工作。
- 2、 用标准 RJ-45 以太网线将 LAN 口与内部局域网连接。
- 3、 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。
- 4、 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。每个桥之间是独立通信的,桥之间不能传递数据。
- 5、 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。

提示: 如果开机 5 分钟后,红灯还长亮,请关闭电源 5 分钟,然后重开。

4 登录设备

设备默认使用 LAN1 作为网管口,LAN1 出厂地址为 192.168.0.1/24。设备支持两种方式的 WEBUI 登录:

- 1、 安全的 HTTPS 登录,默认端口 9090。初始登录 URL 为: <https://192.168.0.1:9090>



- 2、 传统的 HTTP 登录,默认端口 9090。初始登录 URL 为: <http://192.168.0.1:9090>

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

提示:

- 1、 配置之前,必须保证用于网管的电脑与上网行为管理产品的网管口地址在同一个网段。如果第一次配置,请连接 LAN1 口,LAN1 出厂地址为 192.168.0.1/24,电脑的地址应配置为 192.168.0.0/24,但不允许为 192.168.0.1。
- 2、 连接后可以增加/修改物理端口或者网桥的 IP 地址,设备的每一个 IP 地址都可以用于

5 刷新/保存/注销

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



6 密码恢复

如果管理员密码丢失，请按以下步骤恢复系统默认密码：

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

第二部分 产品配置

7 设备状态

登录设备后，进入到设备首页，即设备状态页面。设备状态页面包含了设备版本信息、设备资源、实时网络流量、前十名服务实时速率分布、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1. 首页

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

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

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

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

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

“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。

8 实时监控

实时监控部分用于查看设备实时的工作状态，包括设备资源、物理接口、服务监控、用户监控、上网行为、在线用户、防共享上网、当前黑名单、应用限额用户共 9 个部分。

8.1 设备资源

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



图2. 设置资源

各分页详细说明如下：

- CPU 使用率：查看最近一小时 CPU 使用率；
- 内存使用率：查看最近一小时内存使用率；
- 活跃会话数：查看最近一小时活跃会话数的统计趋势图；
- 在线用户数：查看最近一小时在线用户数的统计趋势图；
- 在线认证用户数：查看最近一小时在线认证用户数的统计趋势图；

每个图的下方都显示了最新值(最近一个采样点的值)、最近一小时的最大值、最小值、平均值及每个值对应的时间点。图中还用箭头指明了最大值，如果这些值分布在多个时间点，则显示最后一个时间点。例如，最大值分布在 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。

8.2 物理接口

物理接口页面的内容含两部分：所有端口的全局信息、每个端口的速率趋势图。

第一：物理接口的全局信息，如下图：



图3. 物理接口统计图

全局信息包括了以下内容：

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

第二：单个物理接口的统计信息包括了总的速率、接收速率、发送速率，如下图：



图4. 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。

8.3 服务监控

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

8.3.1 服务趋势叠加图

服务趋势叠加图如下：



图5. 服务监控统计图

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

8.3.2 服务组趋势图

服务组趋势图如下：

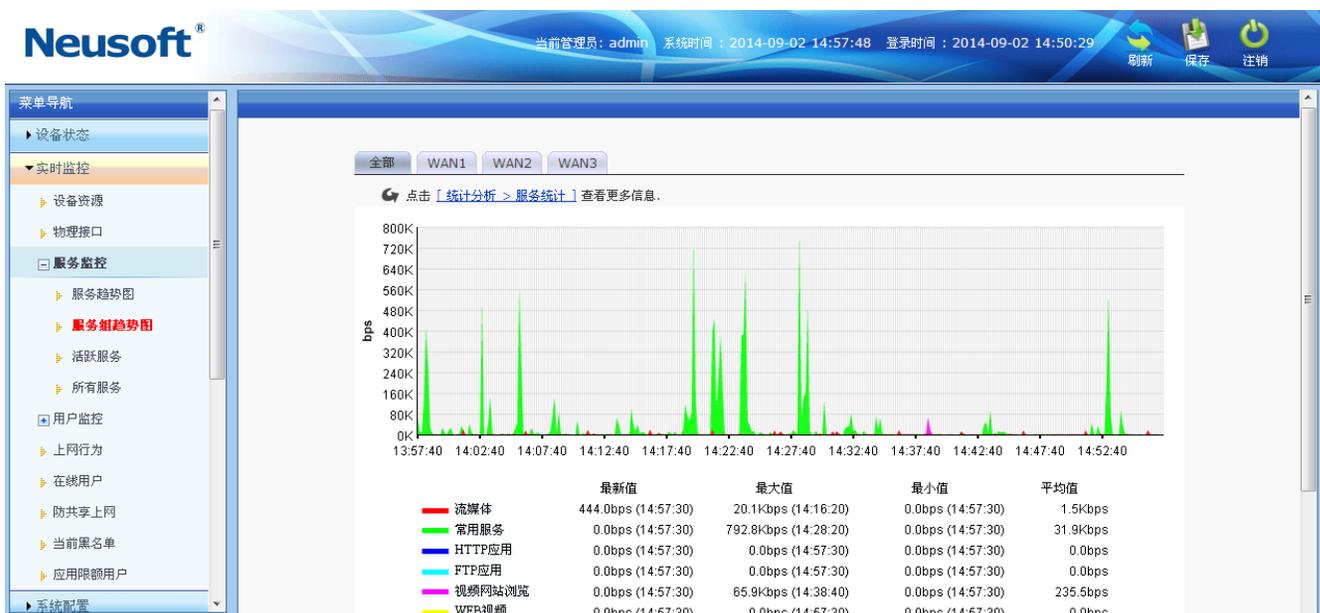


图6. 服务组监控统计图

这里显示了所有服务组的叠加趋势图，一共有自定义普通服务、自定义特征识别、自定义论坛/网评特征、常用服务、HTTP 应用、FTP 应用、视频网站浏览、P2P 下载、WEB 视频、流媒体、即时通讯、网络电话、网络游戏、股票行情、股票交易、网上银行、网络电话、文件上传、日常应用、网页邮箱、软件更新、远程控制、

数据库、其他服务等 24 种类型。

8.3.3 活跃服务统计

“活跃服务”将显示当前所有的活跃的服务，如下图：



图7. 活跃服务监控统计图

参数说明：

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

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

8.3.4 所有服务统计

“所有服务”将分类显示所有的服务统计值，如下图：



图8. 所有服务监控统计

参数说明:

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

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

8.4 用户监控

用户监控页面显示了前五十名用户的实时传输速率、新建会话速率和活跃会话数。

8.4.1 流量分析

前五十名用户的实时传输速率统计图如下:

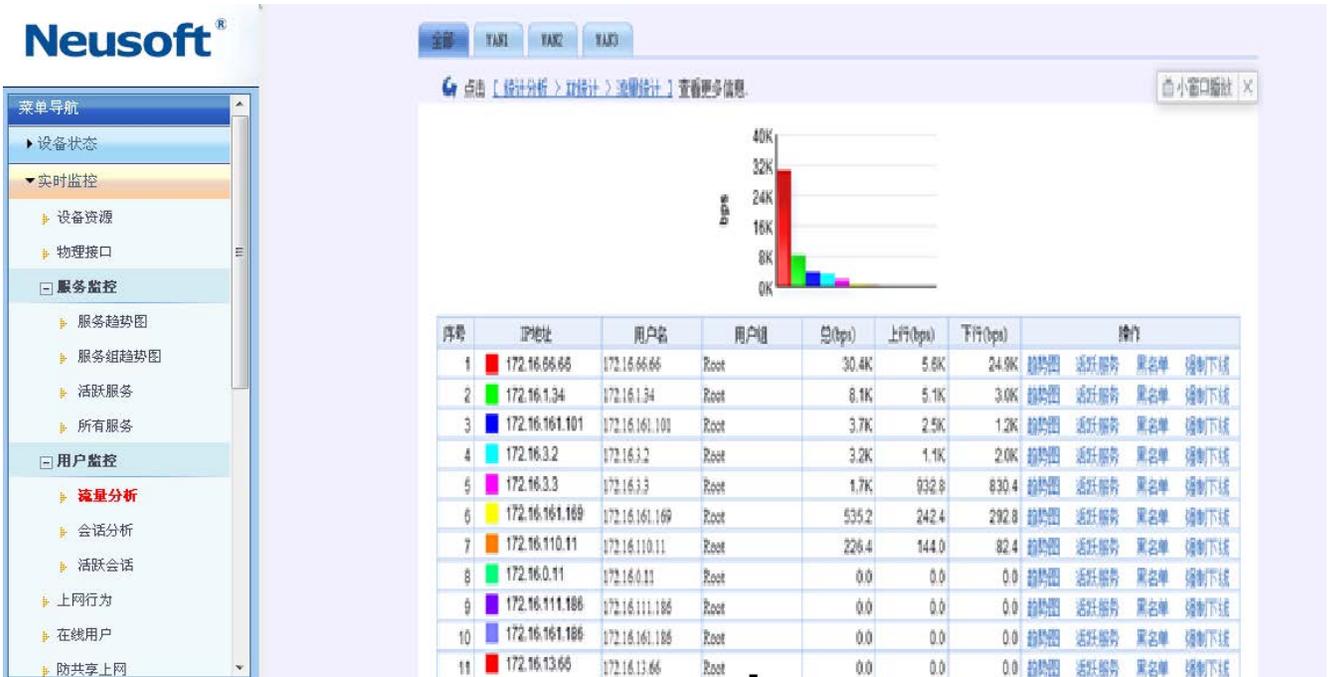


图9. 流量分析

点击<趋势图>按钮，查看该用户最近一小时的速率趋势图。

点击<活跃服务>按钮，查看该用户当前使用的服务的信息。

点击<黑名单>按钮，将该用户手动添加至黑名单。

点击<强制下线>按钮，将该用户强制下线。

8.4.2 会话分析

前五十名用户的新建会话的统计图如下：

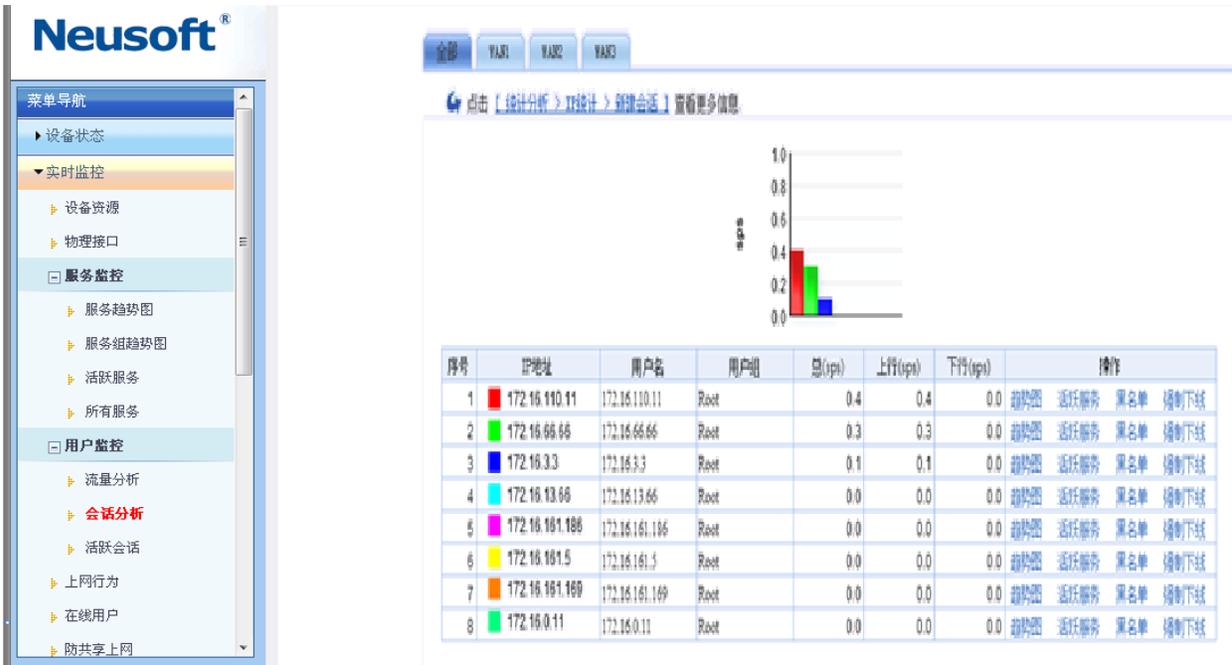


图10. 会话分析

点击<趋势图>按钮，查看该用户最近一小时的速率趋势图。

点击<活跃服务>按钮，查看该用户当前使用的服务的信息。

点击<黑名单>按钮，将该用户手动添加至黑名单。

点击<强制下线>按钮，将该用户强制下线。

8.4.3 活跃会话

前五名用户的当前活跃会话统计图如下：

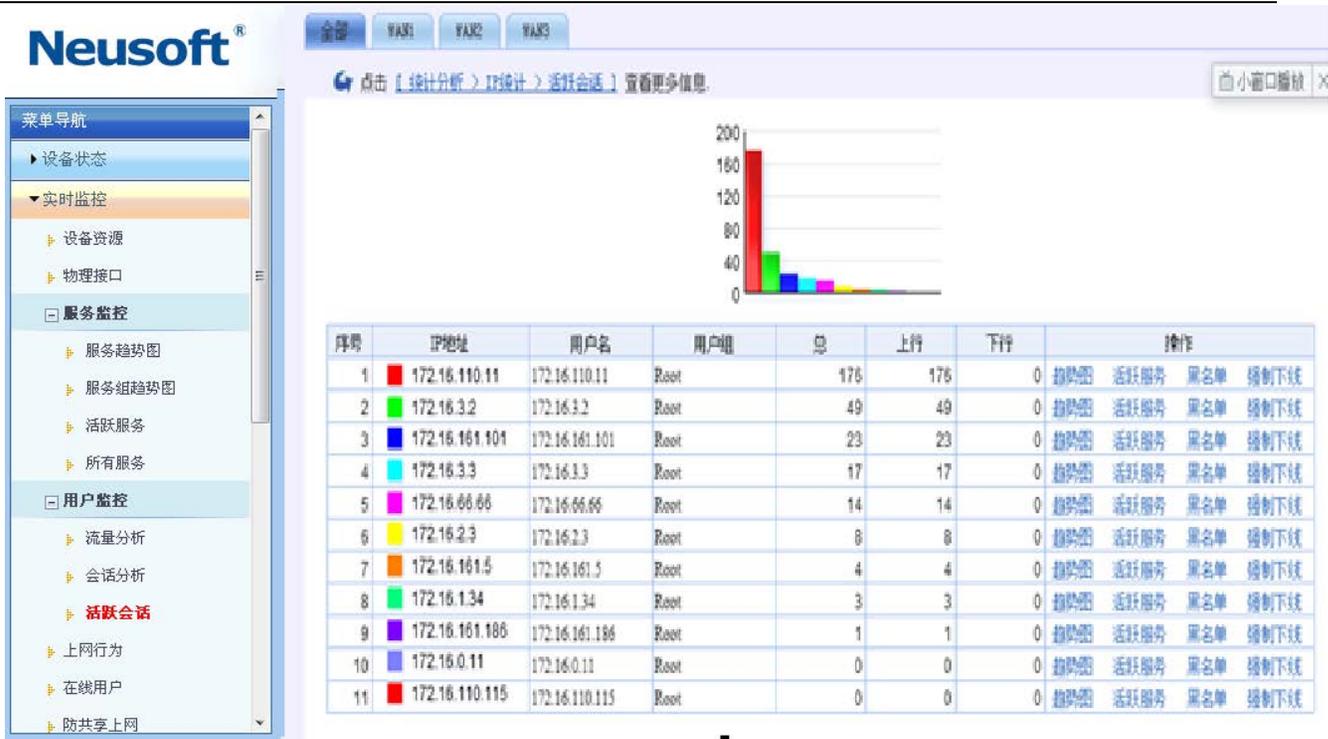


图11. 活跃会话

点击<趋势图>按钮，查看该用户最近一小时的速率趋势图。

点击<活跃服务>按钮，查看该用户当前使用的服务的信息。

点击<黑名单>按钮，将该用户手动添加至黑名单。

点击<强制下线>按钮，将该用户强制下线。

8.5 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12. 上网行为分析

8.6 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13. 在线用户统计

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。

显示项说明：

- 用户名/用户组：显示用户名称和所属组。
- IP 地址/MAC 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。
- 累计在线流量：用户从上线到当前时刻的流量总和。上箭头后面的值表示上行流量的值，下箭头后面的值表示下行流量的值。当用户下线后，其对应的在线流量会被清零。
- 最新速率：用户最后一个采样点的速率值。上箭头后面的值表示上行速率的值，下箭头后面的值表示下行速率的值。
- 活跃会话数：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。
- 安全客户端：用户是否安装了“安全客户端”。

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：强制对应在线用户下线。

- 强制下线：强制所有在线用户下线。

用户绑定说明：

- 绑定所选用户的 IP 地址：在第一列勾选需要绑定的用户后，选择“绑定所选用户的 IP 地址”再点击<确认>按钮，则将“IP 地址/MAC 地址”列所显示的 IP 地址绑定到对应用户。
- 绑定所选用户的 MAC 地址：在第一列勾选需要绑定的用户后，选择“绑定所选用户的 MAC 地址”再点击<确认>按钮，则将“IP 地址/MAC 地址”列所显示的 MAC 地址绑定到对应用户。
- 绑定所选用户的 IP 和 MAC 地址：在第一列勾选需要绑定的用户后，选择“绑定所选用户的 IP 和 MAC 地址”再点击<确认>按钮，则将“IP 地址/MAC 地址”列所显示的 IP 和 MAC 地址绑定到对应用户。
- 绑定所有用户的 IP 地址：选择“绑定所有用户的 IP 地址”再点击<确认>按钮，则将“IP 地址/MAC 地址”列所显示的 IP 地址绑定到对应用户。
- 绑定所选用户的 MAC 地址：选择“绑定所有用户的 MAC 地址”再点击<确认>按钮，则将“IP 地址/MAC 地址”列所显示的 MAC 地址绑定到对应用户。
- 绑定所选用户的 IP 和 MAC 地址：选择“绑定所有用户的 IP 和 MAC 地址”再点击<确认>按钮，则将“IP 地址/MAC 地址”列所显示的 IP 和 MAC 地址绑定到对应用户。
- 取消所选用户的绑定：选择“取消所选用户的绑定”再点击<确认>按钮，则取消对应用户绑定的 IP 或 MAC 地址。
- 取消所有用户的绑定：选择“取消所有用户的绑定”再点击<确认>按钮，则取消所有用户绑定的 IP 或 MAC 地址。

8.7 防共享上网

功能描述：查看当前共享上网的用户。

配置路径：【实时监控】>【防共享上网】

配置描述：

第一：进入【防共享上网】页面，如下图所示：

序号	用户名/用户组	IP地址/MAC地址	物理接口	上线时间	内部终端数	操作
1	Root	172.16.110.115 5404a6630a3c	LAN1	2014-06-28 09:14:49	2	黑名单 强制下线

图14. 防共享上网用户统计

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: 根据进入防共享的时间范围来查找。

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。

按钮说明:

- 黑名单: 跳转至黑名单页面, 可手动修改共享用户的惩罚方式和参数。
- 强制下线: 强制该共享用户下线。

8.8 当前黑名单

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: 【实时监控】> 【当前黑名单】

配置描述:

第一: 进入【当前黑名单】页面, 如下图:



图15. 黑名单用户统计

当前黑名单：显示当前的黑名单用户，相关按钮说明如下：

- 手动添加：手动将某个用户添加至黑名单。
- 解禁所有：解禁所有被限额的用户。
- 解除：解除某个被限额用户。
- 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<点击查看添加>按钮，手动添加黑名单，如下图所示：



图16. 手动添加黑名单

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。

8.9 应用限额用户

功能描述：查看当前被限额用户，以及手动解除被限额用户。

配置路径：【实时监控】>【应用限额用户】

配置描述：

第一：进入【应用限额用户】页面，如下图：

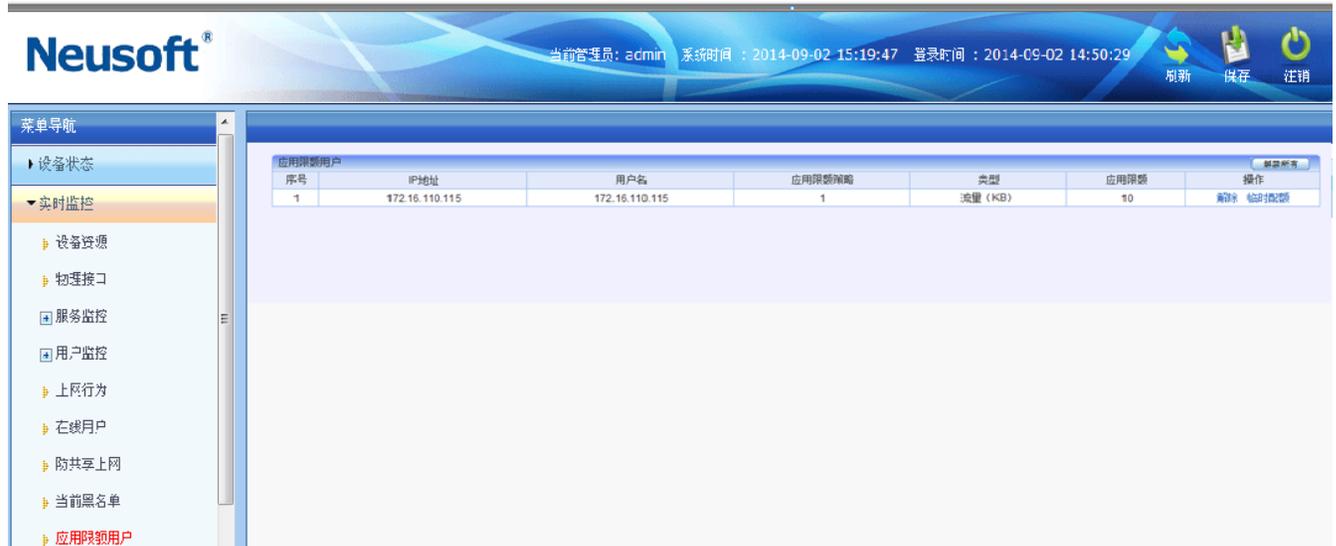


图17. 限额用户页面

当前被限额用户：显示当前被限额的用户列表，相关按钮说明如下：

- 解禁所有：解禁所有被限额的用户。
- 解除：解除某个被限额用户。
- 临时配额：临时为限额用户新增临时配额，如下图所示：



图18. 新增临时配额

9 系统配置

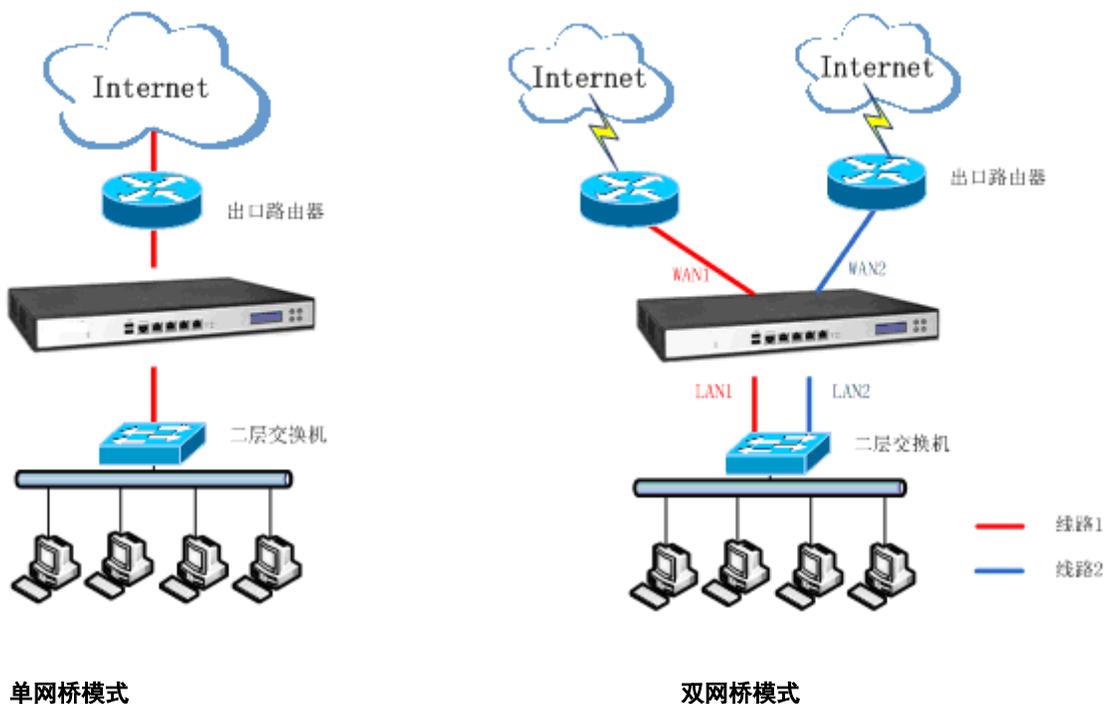
“系统配置”主要包括设备工作模式、系统维护、系统管理员、网络配置、网管策略、重启操作、关机操作、网络工具、系统信息等。

9.1 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。

9.1.1 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：



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19. 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。

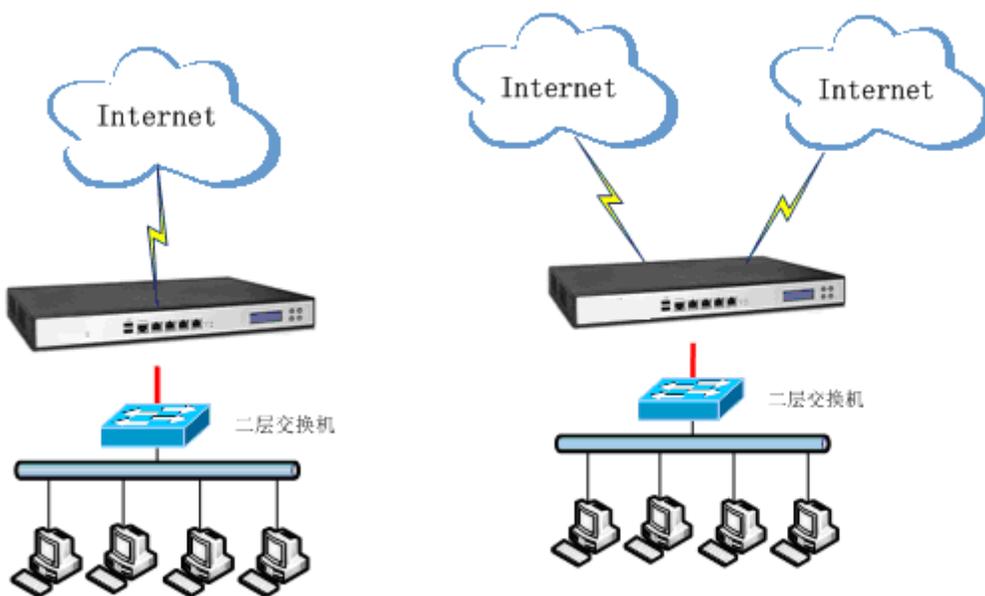
➤ 网关 IP: 默认路由 (0/0) 的的网关地址。若不在此处配置, 可以在【[网络配置>路由配置>静态路由](#)】页面进行默认路由的配置。

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

9.1.2 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:



单链路路由模式

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：



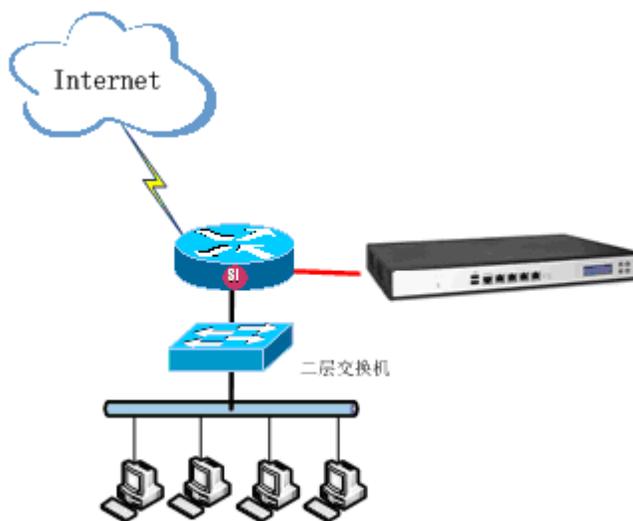
图20. 路由模式

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。

9.1.3 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：



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：

设备工作模式

工作模式 网桥模式 路由模式 旁路模式 (改变工作模式, 将会清除所有静态路由)

>>旁路配置<<

端口配置	LAN1 IP地址:	172.16.161.2	子网掩码:	255.255.0.0	格式范例:	16 或 255.255.0.0
	WAN1 IP地址:		子网掩码:		格式范例:	16 或 255.255.0.0
	LAN2 IP地址:	10.10.10.1	子网掩码:	255.255.255.0	格式范例:	16 或 255.255.0.0
	WAN2 IP地址:		子网掩码:		格式范例:	16 或 255.255.0.0
	LAN3 IP地址:		子网掩码:		格式范例:	16 或 255.255.0.0
	WAN3 IP地址:		子网掩码:		格式范例:	16 或 255.255.0.0

网关IP

监控网段列表

全部

一行一个地址对象, 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

阻断物理接口

无 (HUB做镜像时, 无需配置阻断物理接口; 交换机镜像口不具备业务转发的条件下, 旁路认证阻断接口与交换机另一物理接口相连, 完成旁路认证功能)

DNS劫持

启用 禁用 (旁路认证时, 一些认证客户端需要开启DNS劫持, 才能弹出认证界面)

快速链接 [静态路由](#) [内网代理](#)

工作模式仅用于初次网络部署, 对它的任何修改操作将清除所有静态路由, 可在【网络配置】-【配置IP地址】配置多个接口IP, 在【网络配置】-【静态路由】修改0.0.0.0/0的静态路由来修改缺省网关。

图21. 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。
- 阻断物理接口：HUB 做镜像时，无需配置阻断物理接口；交换机镜像口不具备业务转发的条件下，旁路认证阻断接口与交换机另一物理接口相连，完成旁路认证功能。
- DNS 劫持：旁路认证时，一些认证客户端需要开启 DNS 劫持，才能弹出认证界面。有“启用”和“禁用”两个选项。

9.2 系统维护

9.2.1 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。

- 系统固件：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：
 - ◇ 设备序列号：标示设备的唯一序列号。

- ◇ 授权类型：试用版/正式版；试用版是指给客户试用的版本，正式版是指正式销售的版本。
- ◇ 授权有效期：授权文件的有效期限。
- ◇ 升级服务有效期：正式版的升级服务有效期，在有效期之前可升级系统固件、应用特征库、URL 库，过期则不能升级。

配置路径：**【系统配置】>【系统维护】>【系统升级】**

配置描述：

第一：进入**【系统升级】**页面，可以查看设备的各种系统文件信息。如下图：



图22. 系统升级

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



图23. 系统升级

提示:

- 1、 未选中的文件类型后面显示当前的版本信息。
- 2、 升级系统固件后，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效。

9.2.2 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24. 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。

9.2.3 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25. 配置备份与恢复

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

第二：选择备份或恢复，点击<确定>

9.2.4 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/关闭】

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



图26. 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。

9.3 系统管理员

9.3.1 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27. 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28. 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;
- 口令策略: 包括手工配置口令和自动生成(邮件通知)口令。手工配置密码可以直接在下面的密码、确认密码框中输入用户密码;
- 密码强度: 系统会根据密码强度规则自动检测用户输入密码的安全强度;
- 设置密码/确认密码: 不限字符, 但不能设置空格键; [必选项]
- 使用 Dkey 认证: 当 Dkey 认证功能启用时, 该用户只有使用 Dkey 认证才有权限进行日志查询。
- 自动生成密码: 要求[邮箱地址]为必填项, 系统生成的密码发到该邮箱地址中。如下图:

图29. 新增系统管理员

- 真实姓名: 输入对应登录名的真实姓名, 不限字符; [必选项]
- 手机号码: 即管理员的手机号码; [可选项]
- 邮箱地址: 即管理员的邮箱地址, 当管理员的配置信息有变更时, 系统会通过邮件方式通知管理员;
- 角色: 将定义的用户分配一个角色; [必选项]。

系统默认配置了三个角色(超级管理员、Guest、审计员), 您可以根据准备工作中确定的用户权

限来灵活自定义分配的角色。如果要自定义角色，请参见本文【[角色管理](#)】章节。

➤ 所属组：报表中心 (Reporter) 的权限。例如，一个名为 Mary 的管理员，“所属组”配置为“Root/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：



- 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. 自动生成密码：要求[邮箱地址]为必填项，且必须在【[系统配置>邮件配置](#)】中设置好邮件服务器的相关参数才会生效。
2. DKEY 写入操作前，需先下载并安装 DKEY 驱动；一个 DKEY 只能仅存一个用户的 Dkey 信息，写入 DKEY 将覆盖上一个用户的 Dkey 信息。

9.3.2 角色管理

功能描述：配置系统管理员的角色分类，即管理权限。

配置路径：【系统配置】>【系统管理员】

配置描述：

第一：进入管理员新增页面，点击<角色配置>按钮，进入下图：

系统角色			新增
序号	角色名称	角色描述	操作
1	超级管理员	具有全部编辑、读取权限	修改 删除
2	Guest	仅具读取权限	修改 删除
3	审计管理员	具有Reporter全部的权限	修改 删除

图30. 系统管理员角色

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

网管模块	编辑权限 <input checked="" type="checkbox"/>	查看权限 <input checked="" type="checkbox"/>
实时监控	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
设备资源	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
物理接口	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
服务监控	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
用户监控	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
系统配置	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
工作模式	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
系统维护	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
系统管理员	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
网管策略	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
网管参数	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
网络工具	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
日期时间	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
系统信息	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

图31. 新增系统角色

参数说明:

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

提示:

- 1、 系统默认配置了三个管理员:
 - admin: 具有所有权限, 可以配置设备、查看设备、管理 Reporter。
 - guest: 仅具有查看设备权限, 默认密码为 guest*PWD。
 - reporter: 管理 Reporter, 所属组为根组, 默认密码为 reporter*PWD。
- 2、 系统默认的管理员(admin、guest、reporter)不能删除, 可修改密码。
- 3、 超级管理员可以修改其它管理员的属性, 其它管理员只能修改自己的密码。
- 4、 新增的用户可以修改密码, 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。

9.4 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：

网管策略							新增 修改状态			
策略类型	<input type="radio"/> 允许所有IP网管 <input checked="" type="radio"/> 根据下面策略进行控制									
序号	规则名称	允许网管设备的IP	服务	动作	描述	状态	操作			
1	1	172.16.111.1-172.16.111.200	ALL	允许	本网段	<input checked="" type="checkbox"/>	修改	插入	移动	删除
2	2	192.168.0.0/16	ALL	允许		<input checked="" type="checkbox"/>	修改	插入	移动	删除
3	3	10.1.1.0/24	HTTP	允许		<input checked="" type="checkbox"/>	修改	插入	移动	删除

图32. 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”。

新增网管策略		确定	返回
规则名称	5		
IP地址	10.1.1.0/24 (格式范例: 192.168.1.1 或 192.168.1.1-192.168.1.9 或 192.168.0.0/16)		
服务	SSL		
动作	<input checked="" type="radio"/> 允许 <input type="radio"/> 拒绝		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
描述	只允许HTTPS协议		

图33. 新增网管策略

第四：改变“状态”栏的值，再点击<修改状态>可以改变配置条目的状态。

提示：

- 1、策略类型：默认为“允许所有 IP 网管”，这时所有 IP 都可以网管设备。
- 2、策略类型选择为“根据下面策略进行控制”时，如果网管策略里没有配置任何策略，则所有 IP 都可以网管设备；如果配置了策略，则只有符合这些策略的才可以网管设备。
- 3、状态复选框：勾选，表示此条配置的状态为“启用”。不勾选，即此条配置的状态为“禁用”，即此策略未生效。

9.5 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】

网管参数			确定
WEBUI 网管方式	<input checked="" type="radio"/> HTTPS <input type="radio"/> HTTP		
WEBUI 登录端口	9090	(1-65535)	
WEBUI 超时(分)	10	(1-1440)	
REPORTER 登录端口	9091	(1-65535)	
REPORTER 超时(分)	10	(1-1440)	
SSH 登录端口	2222	(1-65535)	

图34. 网管参数

参数说明:

- WEBUI 网管方式: 支持安全的 HTTPS 方式和传统的 HTTP 方式, 默认为 HTTPS 方式。
- WEBUI 登录端口: 为安全起见, 系统的 WEB 网管默认采用 TCP 9090 端口, 可以改成 TCP 协议的其它端口, 不能改成 80 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。

9.6 网络工具

“网络工具”包括 Ping 和 TraceRoute

9.6.1 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:

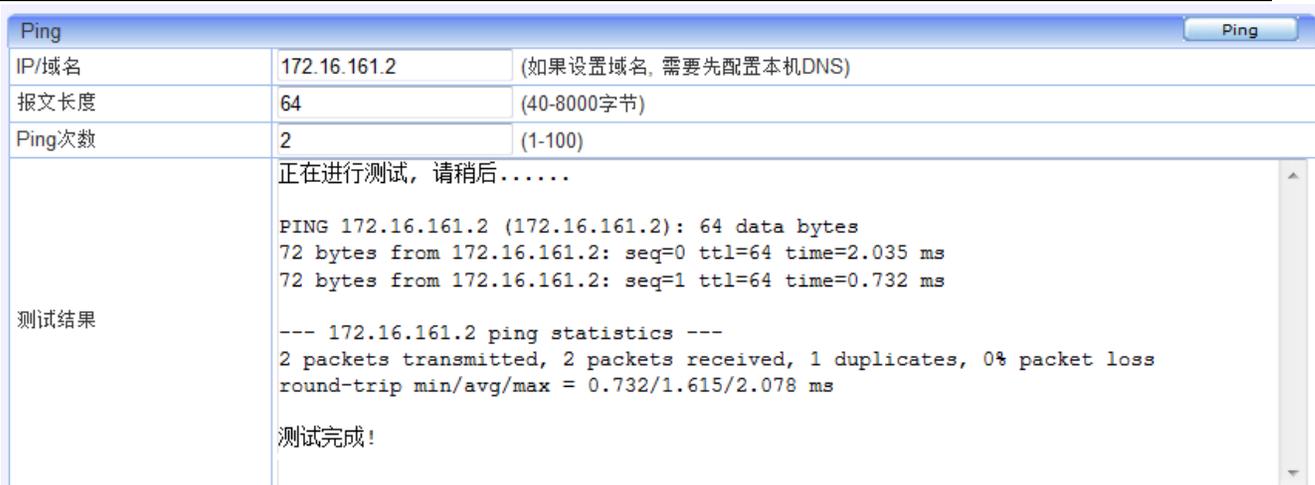


图35. PING 工具

参数说明:

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

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

9.6.2 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:

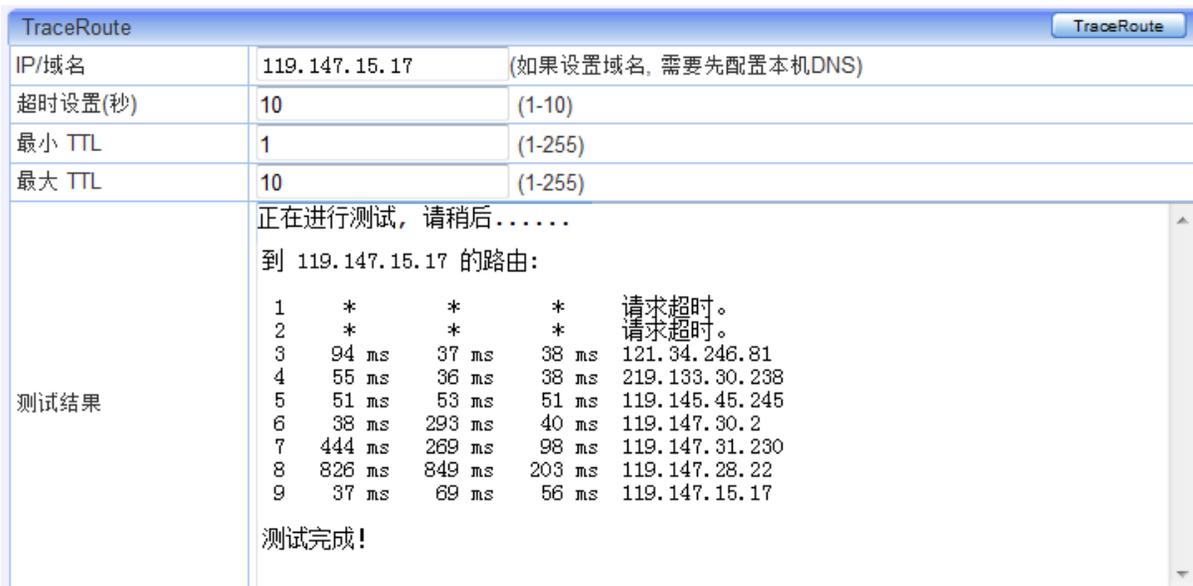


图36. TraceRoute 工具

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](#)】。

9.7 系统时间

功能描述: 用于设定设备的系统时间。

配置路径: 【系统配置】>【系统时间】, 设置界面如下图:



图37. 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[SNTTP 服务器]和[同步间隔]。如下图：

日期和时间		确定	立即同步
当前时间	2011-08-02 17:49:31		
系统时区	(GMT+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐		
系统日期	2011	年	8
		月	2
		日	
系统时间	17	时	49
		分	31
		秒	
SNTP	<input checked="" type="checkbox"/> 自动与SNTP服务器同步		
SNTP服务器	time-ns.nist.gov		
同步间隔	59	(1-59分钟)	

图38. 设置系统时间

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。

9.8 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：

系统信息		确定
系统名称	HOSTNAME	(1 - 20个字符)
产品型号	TEST	
设备识别号	d310bf7fef2d2fe71b23940a6156cfa6	

图39. 系统信息

9.9 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：

邮件配置		确定
邮件配置	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
邮件使用语言	简体中文 ▼	
邮件服务器	smtp.163.com	
端口号	25	
发件人	one@163.com	
发件人显示名称	Admin	
需要认证	<input checked="" type="checkbox"/> 需要认证	
用户名	one@163.com	
密码	••••••	
收件人	two@163.com three@163.com four@163.com	一行一个收件人邮箱地址

图40. 邮件配置

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。
- 端口号：设置邮件端口号。
- 发件人：设置告警邮件的发送者。
- 发件人显示名：设置告警邮件发送者显示的姓名。
- 需要认证：选择是否需要进行密码安全认证。
- 用户名：需要安全认证时，必须填入用户名。
- 密码：需要安全认证时，必须填入用户密码。
- 收件人：设置告警邮件的收件人邮箱地址，可以设置多个，一行一个收件人地址。

9.10 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：

集中管理		确定
启用集中管理	<input type="checkbox"/> 加入集中管理	
中心端地址	172.16.5.99	(IP/域名)
通讯端口	1194	(与中心端一致)
网点名称	133	
数据加密密钥	●●●●●●	(与中心端上该网点的密钥一致)
已获取的虚拟IP	未获取到	
与中心端连接状态	断开 最后响应: 2012-06-29 15:18:10	

图41. 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。

10 系统对象

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

10.1 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](#)】、【[上网策略](#)】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:

地址簿				新增
序号	名称	IP地址	操作	
1	NMC_财务部	192.168.3.0/24	修改	删除
2	NMC_IT部	192.168.5.0/24 192.168.6.0/24	修改	删除

图42. 地址簿

第二：点击<新增>按钮，增加地址簿，如下图：

新增地址簿		确定	返回
名称	IT管理部		
IP地址	192.168.1.2-192.168.1.250 192.168.8.0/24	一行一个地址对象, 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	

图43. 新增地址簿

提示：如果某地址簿已经被引用，则不能被删除。删除前必须先解除引用。

10.2 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、FTP 应用、视频网站浏览、WEB 视频、P2P 下载、流媒体、网络游戏、即时通讯、股票行情、股票交易、网上银行、网络电话、文件上传、日常应用、网页邮箱、软件更新、远程控制、数据库、其他服务等。其中[自定义普通服务]与[常用服务]是基于端口的服务，在【[防火墙>安全策略](#)】中被引用；其他服务都是基于内容识别的服务，在【[流量管理](#)】中将被引用。

10.2.1 内置服务

功能描述：定义了系统内置的服务。包括：常用服务、HTTP 应用、FTP 应用、视频网站浏览、WEB 视频、P2P 下载、流媒体、网络游戏、即时通讯、股票行情、股票交易、网上银行、网络电话、文件上传、日常应用、网页邮箱、软件更新、远程控制、数据库、其他服务。

配置路径：【系统对象】>【网络服务】>【内置服务】

第一：进入【内置服务】页面，可看到当前的内置服务，如下图：



10.2.2 自定义普通服务

功能描述：自定义基于端口的四层服务

配置路径：【系统对象】>【网络服务】>【自定义普通服务】

配置描述：

第一：进入【自定义普通服务】页面，可看到当前已定义的服务，如下图：

自定义普通服务 新增				
序号	名称	服务描述(协议类型/源端口:目的端口)	优先级	操作
1	NMC_路由协议	UDP/520 IP/88 IP/89	高于内置服务	修改 删除
2	NMC_OA协议	TCP/8852-8861 TCP/7781-7785	高于内置服务	修改 删除

图44. 自定义普通服务

第二：点击表格右上角的<新增>按钮，增加服务，配置页面如下：

新增自定义普通服务 确定 返回	
名称	OA
服务配置	<div style="display: flex; justify-content: space-around; border-bottom: 1px solid black;"> TCP UDP ICMP IP </div> <div style="display: flex; align-items: flex-start;"> <div style="flex: 1;"> <input type="text" value="881"/> <input type="text" value="852-853"/> </div> <div style="flex: 2; padding-left: 10px;"> <p>一行一组端口，格式说明： 80 表示目的端口为 80 的服务 81-90 表示目的端口范围为 81-90 的服务 222/333 表示源端口为 222，目的端口为 333 的服务 100-200/80-90 表示源端口范围为 100-200，目的端口范围为 80-90 的服务</p> </div> </div>
	优先级

图45. 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。

10.2.3 自定义特征识别

功能描述：自定义基于特征识别的 7 层服务

配置路径：【系统对象】>【网络服务】>【自定义特征识别】

配置描述：

第一：进入【自定义特征识别】页面，可看到当前已定义的服务，如下图：

特征识别规则									新增
序号	名称	协议类型	目的端口	IP地址	数据长度	特征字符串	优先级	操作	
1	NMC-新浪发件特征	TCP	80-80	全部	300-800	^POST /classic/sendmail\.php(.\n)+Host: .*mail\.sina\.com\.cn	低于内置服务	修改	删除

图46. 自定义特征识别规则

第二：点击表格右上角的<新增>按钮，增加服务，配置页面如下：

新增服务特征		确定	返回
名称	新浪发件特征		
协议类型	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> TCP+UDP		
目的端口	<input type="radio"/> 所有端口 <input checked="" type="radio"/> 端口范围 <input type="text" value="80"/> - <input type="text" value="80"/>		
IP地址	<input checked="" type="radio"/> 所有IP地址 <input type="radio"/> 指定IP地址 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)		
数据长度	<input type="radio"/> 任意数据长度 <input checked="" type="radio"/> 指定数据长度 <input type="text" value="300"/> - <input type="text" value="800"/> (不算TCP/UDP头, 即Payload的值)		
特征字符串	<input type="text" value="^POST /classic/sendmail\.php(.\n)+Host: .*mail\.sina\.com\.cn"/> (正则表达式)		
优先级	<input checked="" type="radio"/> 低于内置服务 <input type="radio"/> 高于内置服务		
说明:以上各条件是“与”的关系,即每个条件都满足,才能匹配到本条特征 报文数据部分的特征字符串,用正则表达式来表示,如^w3C(.\n){2,6}w4D,表示报文数据部分的起始值为3C,紧接着是不含0的任意字符出现最少2次,最多6次,再后面会出现字符4D			

图47. 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。

10.2.4 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，如下图所示：

自定义论坛/网页评论特征									新增
序号	名称	URL	HOST	编码类型	是否MIME型	主题关键字	内容关键字	优先级	操作
1	NMC-新浪论坛1	post.php	bbs.sina.com.cn	GBK	否	subject	message	低于内置服务	修改 删除
2	NMC-新浪论坛2	post.php	bbs.sina.com.cn	GBK	是	subject	message	低于内置服务	修改 删除

图48. 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：

新增自定义论坛/网页评论特征		确定	返回
名称	NMC-新浪论坛2		
URL	post.php	(此项填HTTP报文第一行POST头与HTTP/1.1之间的内容，如：post.jsp)	
HOST	bbs.sina.com.cn	(此项填HTTP报文的HOST字段的内容，如：www.sina.com.cn或者IP地址)	
编码类型	<input type="radio"/> UTF-8 <input type="radio"/> GB2312 <input checked="" type="radio"/> GBK <input type="radio"/> BIG5		
是否MIME型	<input checked="" type="radio"/> 是 <input type="radio"/> 否 (Content-Type字段有 boundary=---即为MIME型)		
主题关键字	subject	(此项填title、topic、subject或其他)	
内容关键字	message	(此项填message、content、body、remark或其他)	
优先级	<input checked="" type="radio"/> 低于内置服务 <input type="radio"/> 高于内置服务		

图49. 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/1.1 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50. 发表帖子



图51. 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。

10.2.5 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：

协议剥离		确定
<input type="checkbox"/>	名称	端口
<input type="checkbox"/>	L2TP协议剥离	1701
<input type="checkbox"/>	GRE协议剥离	-

自定义协议剥离		确定
协议剥离	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
匹配协议头特征	从以太网头部开始偏移的字节数 1 (1-100) 特征值等于 格式：十六进制数以分隔，最多不超过10个 如 08:00:ff	
IP头起始位置	从以太网头部开始偏移的字节数 15 (15-100)	

图52. 自定义协议剥离

参数说明：

- L2TP协议剥离：如要对L2TP协议进行剥离，可直接勾选“L2TP协议剥离”。
- GRE协议剥离：如要对GRE协议进行剥离，可直接勾选“GRE协议剥离”。
- 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（含以太网头）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。

10.3 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：

时间计划			新增
序号	名称	时间计划	操作
1	上班时间	星期一：09:00-19:00 星期二：09:00-19:00 星期三：09:00-19:00 星期四：09:00-19:00	修改 删除

图53. 时间计划

第二：点击<新增>按钮，增加时间计划，如下图：

新增时间计划		确定	返回																						
名称	时间																								
时间计划	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
	星期一	■	■	■	■	■	■	■	■																
	星期二	■	■	■	■	■	■	■	■																
	星期三	■	■	■	■	■	■	■	■																
	星期四	■	■	■	■	■	■	■	■																
	星期五																								
	星期六																								
星期日																									

图54. 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。

10.4 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>上网权限策略>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:

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

图55. 内置 URL 库

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

内置URL库		自定义URL库		
自定义URL库				新增
序号	名称	描述	优先级	操作
1	gmail阻挡	自定义Gmail阻挡	高于内置URL库	修改 插入 移动 删除
2	OA-URL	OA系统地址	高于内置URL库	修改 插入 移动 删除

图56. 自定义 URL 库

操作说明:

➤ **【[上网权限策略>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**【[上网权限策略>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:

新增URL关键字		确定	返回
URL组名称	OA-URL		
描述			
URL	提示: 一行一个 URL 关键字(或 URL 全名); 采用子串匹配方式, 如输入 xyz.com, 将匹配 www.xyz.com、www.xyz.com.cn、www.xyz.com/hardware 等 www.abc.com www.bce.com www.one.com www.two.com		
优先级	<input type="radio"/> 低于内置URL库 <input checked="" type="radio"/> 高于内置URL库		

图57. 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。

10.5 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**【[上网权限策略>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:

关键字组			新增
序号	名称	描述	操作
1	NMC_暴力类	与暴力有关的关键字	修改 插入 移动 删除
2	NMC_色情类	与色情有关的关键字	修改 插入 移动 删除
3	NMC_娱乐类	娱乐、电影、音乐有关	修改 插入 移动 删除
4	NMC_恐怖活动类	与恐怖活动有关	修改 插入 移动 删除

图58. 关键字组

操作说明:

➤ **【[上网权限策略>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**【[上网权限策略>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：

新增关键字组		确定	返回
名称	娱乐		
描述			
关键字	提示：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 快乐男生 超级女生 酷6		

图59. 新增关键字组

10.6 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**【[上网权限策略>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，可以看到当前已定义的文件类型分组。如下图：

文件类型列表			新增
序号	名称	描述	操作
1	NMC_Word和PDF	所有Word和PDF文件	修改 插入 移动 删除
2	NMC_可执行文件	所有可执行文件	修改 插入 移动 删除
3	NMC_压缩文件	所有压缩文件	修改 插入 移动 删除
4	NMC_Excel和文本	Excel和文本文件	修改 插入 移动 删除

图60. 文件类型

操作说明:

➤ **【[上网权限策略>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**【[上网权限策略>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:

新增文件类型		确定	返回
名称	压缩文件		
描述			
文件类型	提示: 一行一个文件类型; 格式为".后缀名", 如 .zip .rar .zap		

图61. 新增文件类型

11 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。

11.1 接口配置

包括物理接口、VLAN 接口、PPPoE、GRE 隧道 四部分。

11.1.1 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：

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:C1:9E:FA	0M	自协商	1500	未连接	修改
LAN2	6C:62:6D:4A:43:3D	100M	自协商	1500	连接	修改
LAN3	6C:62:6D:4A:43:3F	0M	自协商	1500	未连接	修改
WAN1	6C:62:6D:C1:9E:FB	0M	自协商	1500	未连接	修改
WAN2	6C:62:6D:4A:43:3E	100M	自协商	1500	连接	修改
WAN3	6C:62:6D:4A:43:40	0M	自协商	1500	未连接	修改

图62. 物理端口

提示：物理接口的状态为“未连接”时，工作速率为 0 M

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：

修改物理接口参数		确定	返回
名称	LAN2		
MAC地址	6C:62:6D:4A:43:3D		
协商类型	<input checked="" type="radio"/> 自协商 <input type="radio"/> 全双工		
工作速率	<input type="radio"/> 1000M <input checked="" type="radio"/> 100M <input type="radio"/> 10M		
MTU	<input type="text" value="1500"/> (256-1500)		

图63. 修改物理端口参数

提示：当协商类型为自协商时，工作速率不可配置。

11.1.2 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：

- (1) 参与捆绑的物理端口必须属于同一个 VLAN。
- (2) 参与捆绑的物理端口必须属于 LAN 口或同属于 WAN 口。
- (3) 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：

链路聚合							新增
序号	接口名称	物理接口	均衡算法	主接口	哈希算法	侦测目标	操作
1	LCG2	LAN2,LAN3	轮循	-	-	172.16.3.2	修改 删除
2	WCG2	WAN2,WAN3	主备	WAN2	-	10.2.3.5	修改 删除

图64. 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：

新增链路汇聚		确定	返回
物理接口	<input checked="" type="checkbox"/> LAN1 <input checked="" type="checkbox"/> LAN2 <input checked="" type="checkbox"/> LAN3 <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3		
均衡算法	轮循		
侦测目标	172.16.8.123 192.168.1.23 (多个IP地址需要单空格分隔)		

 提示：修改“均衡算法”需重新配置静态路由

图65. 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。

11.1.3 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：

VLAN接口				新增
序号	接口名称	物理接口	VLAN ID	操作
1	LAN1.2	LAN1	2	删除
2	LAN1.3	LAN1	3	删除
3	WAN1.8	WAN1	8	删除

图66. VLAN 接口

接口名称是物理接口和 VLAN ID 的组合。例如，LAN1.2 表示物理接口为 LAN1，VLAN ID 为 2 的 VLAN 接口。然后在【网络配置>配置 IP 地址】处，可以为 VLAN 接口配置 IP 地址。

第二： 点击<新增>按钮，增加 VLAN 接口。如下图：

新增VLAN接口		确定	返回
物理接口	LAN1		
VLAN ID	5 (1-4094)		

图67. 新增 VLAN 接口

11.1.4 PPPoE

功能描述： 配置 PPPoE 拨号账号，实现 PPPoE 拨号。

配置路径：【网络配置】>【接口配置】>【PPPoE】

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

PPPoE配置								新增
序号	名称	外网口	帐号	IP地址	子网掩码	网关	连接状态	操作
1	2699350	WAN1	2699350@163.gd				断线	修改 删除

图68. PPPoE

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。
- 账号：PPPoE 的账号
- 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“连接”；未成功时，状态为“断线”。

第二： 点击<新增>按钮，增加 PPPoE 配置。如下图：

新增PPPoE		确定	返回
名称	link2		
外网口	WAN2		
帐号	332389@@163.com		
密码	●●●●●●●●		

图69. 新增 PPPoE

11.1.5 DHCP客户端

功能描述: 配置 WAN 口的 DHCP 客户端。

配置路径: 【网络配置】>【接口配置】>【DHCP 客户端】

第一: 进入【DHCP 客户端】界面，可以看到当前已启用 DHCP 客户端的接口的配置。如下图：

DHCP客户端			
名称	已自动获得的IP地址	已自动获得的网关	操作
WAN1	-	-	开启 更新 释放
WAN2	-	-	开启 更新 释放
WAN3	0.0.0.0/0.0.0.0	0.0.0.0	关闭 更新 释放

图70. DHCP 客户端

第二: 默认情况，所有 WAN 口的 DHCP 客户端功能都关闭。点击对应接口操作栏的<开启>按钮，开启 DHCP 客户端功能。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。

11.1.6 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：

GRE隧道						新增
序号	隧道名称	隧道IP	子网掩码	源地址	目的地址	操作
1	TCenter	192.168.2.3	255.255.255.0	12.1.1.2	58.60.3.123	修改 删除

图71. GRE

第二: 点击<新增>按钮，增加 PPPoE 配置。如下图：

新增GRE隧道		确定	返回
隧道名称	TCenter		
隧道IP	192.168.2.3	(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	255.255.255.0	(隧道IP的子网掩码)	
源地址	12.1.1.2	(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	58.60.3.123	(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)	

图72. 新增 PPPoE

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。

11.2 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:

IP地址				新增
接口名称	IP地址	子网掩码	操作	
WAN1	58.60.34.23	255.255.252.0	修改	删除
Bridge2	172.16.5.133	255.255.0.0	修改	删除

图73. IP 地址配置

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:

新增IP地址		确定	返回
接口名称	WAN1		
IP地址	58.60.34.23		
子网掩码	255.255.252.0	(格式范例: 16 或 255.255.0.0)	

图74. 物理端口名称

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。

11.3 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：

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	操作		
1	192.168.2.0/24	直连	192.168.2.3	TCenter	修改	删除	
2	58.60.32.0/22	直连	58.60.34.23	WAN1	修改	删除	
3	172.16.0.0/16	直连	172.16.5.133	Bridge2	修改	删除	
4	0.0.0.0/0	静态	172.16.161.2	Bridge2	修改	删除	

图75. 静态路由

第二: 点击<新增>按钮，增加静态路由。如下图：

新增静态路由		确定	返回
目的IP	192.168.3.0/24 192.168.5.0/24 192.168.7.0/24	一行一个地址对象, 格式范例: 1.1.0.0/16 或 1.1.0.0/255.255.0.0	
网关	<input checked="" type="radio"/> IP地址 <input type="radio"/> GRE隧道 <input type="radio"/> PPPoE 172.16.3.33		

图76. 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。

11.4 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。

11.4.1 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，可以看到当前配置的网段。如下图所示：

网络配置				新增	删除所有
序号	运行网段	区域ID	操作		
1	172.16.161.2/16	0.0.0.1	修改	删除	
2	192.168.1.10/24	192.168.1.10	修改	删除	

图77. 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：

新增网络配置			确定	返回
运行网段	10.1.0.0/16	(例如：10.1.1.1/255.255.0.0 或 10.1.1.1/16)		
区域ID	1	(格式范例：192.168.1.1 或 0-4294967295之间)		

图78. 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。

11.4.2 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:

接口配置								
序号	接口名称	接口IP地址	被动接口	认证方式	邻居老化时间	选举优先级	重传时间间隔	操作
1	LAN1	172.16.161.2/16	no	simple	40	1	5	修改
2	LAN2	192.168.1.10/24	no	simple	40	1	5	修改

图79. 接口信息

点击<修改>按钮, 修改接口信息, 如下图所示:

修改接口配置		确定
接口名称	LAN1	
接口IP地址	172.16.161.2/16	
被动接口	<input type="radio"/> 是 <input checked="" type="radio"/> 否	
认证方式	<input checked="" type="radio"/> 明文 <input type="radio"/> MD5 <input type="radio"/> 不认证	
认证口令	<input type="text"/>	
接口开销	<input type="text" value="10"/> (1-65535)	
邻居老化时间	<input type="text" value="40"/> (1-65535)	
发送报文间隔时间	<input type="text" value="10"/> (1-65535)	
选举优先级	<input type="text" value="1"/> (0-255)	
重传时间间隔	<input type="text" value="5"/> (3-65535)	

图80. 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。

11.4.3 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：

参数配置		确定
Router ID	<input type="text"/>	
域内优先级	<input type="text" value="10"/>	(1-255)
域间优先级	<input type="text" value="110"/>	(1-255)
外部优先级	<input type="text" value="150"/>	(1-255)
SPF计算间隔	<input type="text" value="10"/>	秒 (0-4294567295)
路由重分布配置		
引用直连路由	<input type="text" value="否"/>	
引用静态路由	<input type="text" value="否"/>	
默认度量值	<input type="text" value="0"/>	(0-16777214)

图81. 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。

11.4.4 虚连接配置

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：

虚连接配置									
序号	区域ID	Router ID	Hello间隔	重传间隔	传输时延	失效间隔	认证方式	认证口令	操作
1	0.0.0.22	172.16.161.2	65535	10	5	40	md5	dddd	修改 删除
2	0.0.0.17	172.16.161.2	10	10	5	40	md5	00000000	修改 删除

图82. 虚连接配置

进入点击<新增>按钮，增加 OSPF 运行网段。如下图：

新增虚连接		确定
区域ID	<input type="text"/>	(arealDTip)
Router ID	<input type="text"/>	
Hello 间隔	<input type="text" value="10"/>	秒 (1-65535)
重传间隔	<input type="text" value="10"/>	秒 (1-65535)
传输时延	<input type="text" value="5"/>	(1-65535)
失效间隔	<input type="text" value="40"/>	秒 (1-65535, 一般为 Hello 间隔的4倍)
认证方式	<input checked="" type="radio"/> 明文 <input type="radio"/> MD5 <input type="radio"/> 不认证	
认证口令	<input type="text"/>	

图83. 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。

11.4.5 信息显示

11.4.5.1 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:

OSPF链路信息								
序号	Type	Router ID	Adv Router	Seq	Age	Opt	Cksum	Len
1	router-LSA	192.168.1.10	192.168.1.10	1040	80000027	2	0xc58d	24
2	router-LSA	192.168.1.10	192.168.1.10	892	8000000c	2	0x3ed4	48
3	router-LSA	192.168.1.10	192.168.1.10	1040	80000027	2	0xc58d	24
4	router-LSA	192.168.1.10	192.168.1.10	1040	80000027	2	0xc58d	24
5	router-LSA	192.168.1.10	192.168.1.10	1040	80000027	2	0xc58d	24
6	router-LSA	192.168.1.10	192.168.1.10	1195	80000028	2	0xc38e	24

图84. 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。

11.4.5.2 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:

OSPF路由信息	
N	172.16.0.0/16 [10] area: 0.0.0.1 directly attached to LAN1
N	192.168.1.0/24 [10] area: 0.0.0.1 directly attached to LAN2

图85. OSPF 路由信息

11.4.5.3 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:

OSPF邻接关系						
序号	Neighbor ID	Pri	State	Dead Time	Addresss	Interface

图86. 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。

11.4.5.4 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：

序号	Interface	IP	Area	State	DR	BDR
1	LAN1	172.16.161.2/16	0.0.0.1	DR	192.168.1.10	No
2	LAN2	192.168.1.10/24	0.0.0.1	DR	192.168.1.10	No

图87. 网络配置

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。

11.5 策略路由

11.5.1 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：

序号	物理接口	源地址	目的地址	服务	网关	生效时间	匹配计数	<input type="checkbox"/> 状态	操作
1	ALL-LAN	全部	全部	ALL	下行流量	上班时间	0	<input checked="" type="checkbox"/>	修改 插入 移动 删除
2	LAN1	全部	全部	ALL	下行流量	下班时间	0	<input checked="" type="checkbox"/>	修改 插入 移动 删除

图88. 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：

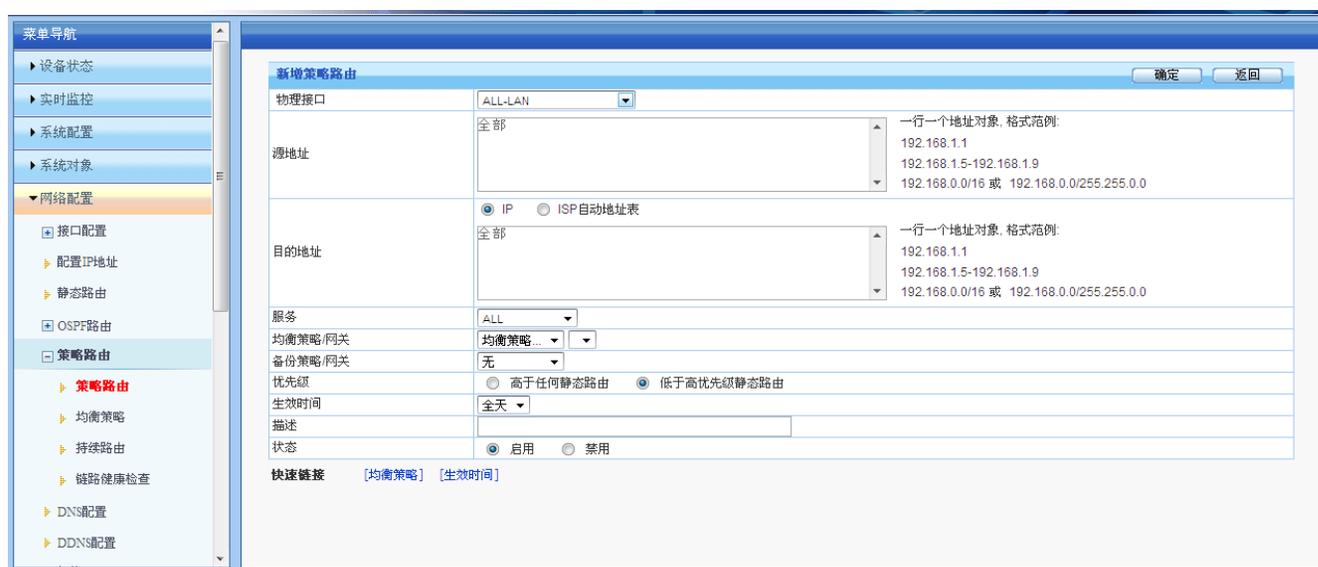


图89. 新增策略路由

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。
- 优先级：有“高于任何静态路由”和“低于高优先级静态路由”两种选择。
- 生效时间：本条策略路由的生效时间。
- 描述：对本条策略路由作一个简单的描述。
- 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。

11.5.2 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，可以看到当前配置的均衡策略。如下图所示：

均衡策略				
序号	名称	算法	网关/配置参数/匹配计数	操作
1	poll_flow	轮循IP算法	192.168.1.1(75%)(0/0) 192.168.0.224(25%)(0/0)	修改 删除
2	up_flow	上行流量	192.168.0.224(200 Kbps)(0/0) 192.168.1.1(200 Kbps)(0/0)	修改 删除
3	down_flow	下行流量	192.168.1.1(10000 Kbps)(12408/189180) 192.168.0.224(5000 Kbps)(176772/189180)	修改 删除
4	total_flow	总流量	192.168.0.224(5000 Kbps)(0/0) 192.168.1.1(2500 Kbps)(0/0)	修改 删除
5	best_path	最佳路径	192.168.1.1(0/0) 192.168.0.224(0/0)	修改 删除

网关参数：均衡策略的网关的 IP 地址或 PPPoE 的名称。

配置参数：根据均衡算法对应的配置值，比如重、带宽值，固定指派与最佳路径算法无该值。

匹配计数：以会话为统计单位，斜杠前面的值为该线路的匹配计数，斜杠后面的值为该策略的匹配总数。

图90. 均衡策略

第二：进入点击<新增>按钮，增加策略路由。如下图：

图91. 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 7 种算法，分别如下：
 - ✧ 固定指派：固定指派某条链路。
 - ✧ 轮询（源IP+目的IP）：按照源IP和目的IP进行轮询。
 - ✧ 上行流量：根据链路上行流量所占的比重，进行计算选路。
 - ✧ 下行流量：根据链路的下行流量所占的比重，进行计算选路。
 - ✧ 总流量：根据链路的总流量所占的比重，进行计算选路。
 - ✧ 最佳路径：设备按照一定的协议（ping或者TCP）去侦测网关，选出最佳路径，根据最佳路径进行计算选路。
 - ✧ 轮询（源IP）：按照源IP进行轮询。
- 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。

网关	类型 IP地址...	IP地址	比重	%	描述
1.	类型 IP地址...	172.16.11.34	比重 30	%	描述 电信
2.	类型 IP地址...	192.168.3.56	比重 70	%	描述 网通
3.	类型 IP地址...		比重	%	描述
4.	类型 IP地址...		比重	%	描述
5.	类型 IP地址...		比重	%	描述
6.	类型 IP地址...		比重	%	描述
7.	类型 IP地址...		比重	%	描述
8.	类型 IP地址...		比重	%	描述

图92. 新增均衡策略-轮询(源 IP)

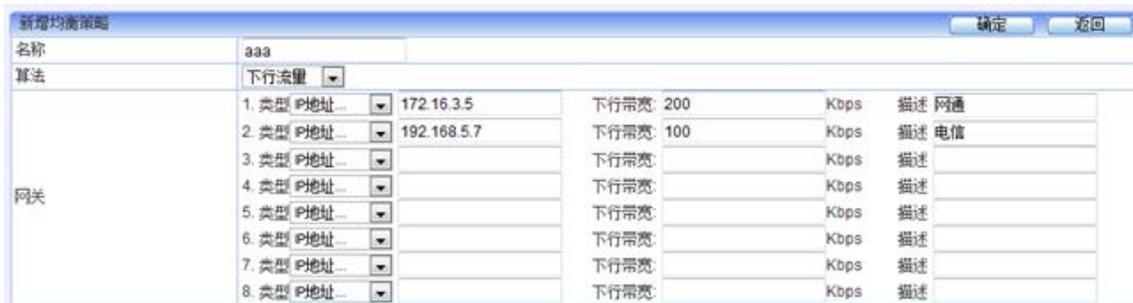


图93. 新增均衡策略-下行流量

11.5.3 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：

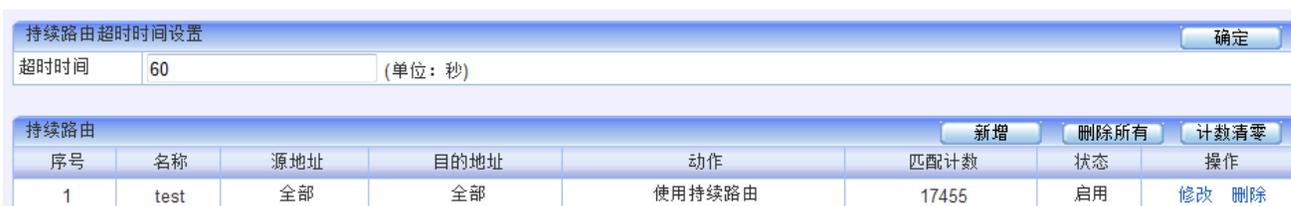


图94. 持续路由

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95. 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”。

11.5.4 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:

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	链路状态	<input type="checkbox"/> 状态	操作				
1	isp_wan	192.168.1.1	3	3	2	27644/29174	94.756%	断开	<input checked="" type="checkbox"/>	修改 删除				
2	isp_simul	192.168.0.224	3	3	3	442/29174	1.5150%	正常	<input checked="" type="checkbox"/>	修改 删除				

图96. 链路健康检查

第二: 进入点击<新增>按钮, 增加联络健康检查规则。如下图:

新增链路健康检查		确定	返回
名称	<input type="text"/>		
网关	类型 <input type="text" value="IP地址"/> <input type="text"/>	(ISP提供的网关IP地址)	
侦测目标	<input type="text"/> 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	<input type="text" value="3"/> (1-600秒)		
重试次数	<input type="text" value="3"/> (1-20)		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
静态路由检查	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
静态路由切换	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
目的子网	<input type="text"/> 一行一个地址对象，格式范例： 1.1.0.0/16 或 1.1.0.0/255.255.0.0		
备份网关	类型 <input type="text" value="无"/>		

图97. 新增链路健康检查

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。

11.6 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98. 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。
- DNS 重定向：使设备的域名不通过 DNS 服务器进行解析，直接访问该域名对应的 IP 地址。

11.7 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：

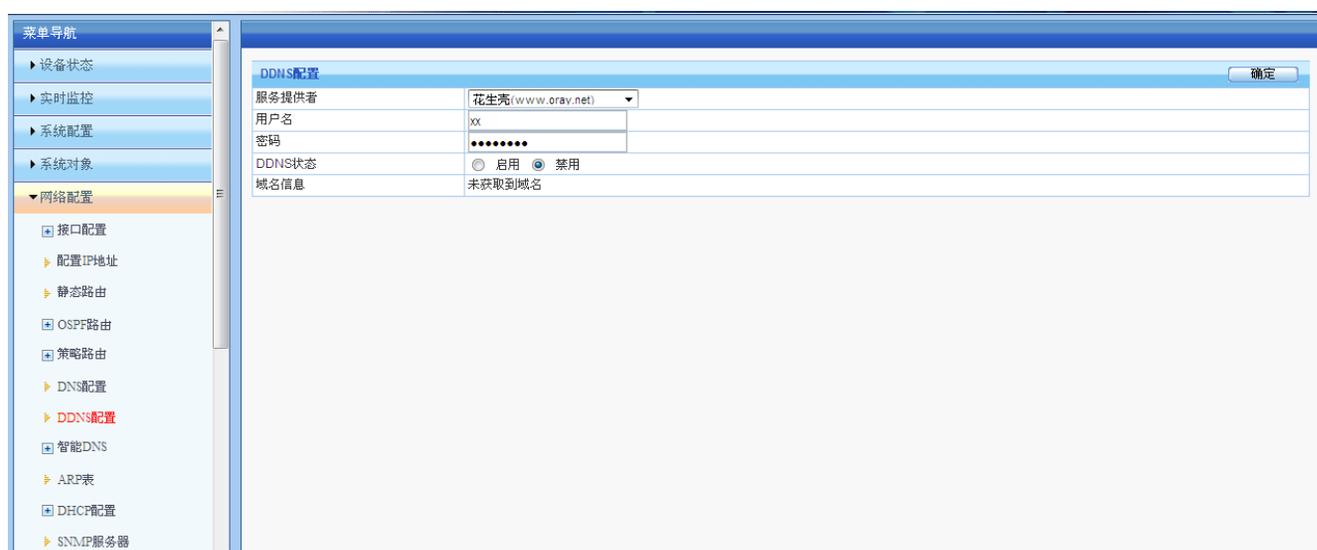


图99. DDNS 配置

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。

11.8 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。

11.8.1 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100. 全局配置

11.8.2 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：

线路配置								新增	删除所有	计数清零
序号	接口名称	备注	接口IP地址	NS	上行带宽(Kbps)	下行带宽(Kbps)	匹配计数	操作		
1	WAN1	wan1	0.0.0.0	1.1.1.1	1000	2000	0	修改	删除	
2	WAN2	wan2	0.0.0.0	2.2.2.2	2000	4000	0	修改	删除	
3	WAN3	wan3	0.0.0.0	3.3.3.3	3000	6000	0	修改	删除	

图101. 线路配置

第二： 点击<新增>按钮，增加线路配置。如下图：

图102. 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。

11.8.3 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：

均衡策略						新增	删除所有	计数清零
序号	名称	算法	配置信息	匹配计数	操作			
1	Policy-A	权重	202.96.128.6 WAN1(80%) 58.60.231.2 WAN2(20%)	0	修改 删除			
2	Policy-B	下行流量	202.96.128.6 WAN1(2000Kbps) 58.60.231.2 WAN2(4000Kbps)	0	修改 删除			

图103. 线路配置

第二： 点击<新增>按钮，增加策略配置。如下图：

新增均衡策略

名称: Policy-A

算法: 按权重

线路名称	服务器外网IP地址	权重比(%)
WAN1	202.96.128.6	80
WAN2	58.60.231.2	20
WAN1		

图104. 新增均衡策略-1

修改均衡策略

名称: Policy-B

算法: 下行流量

线路名称	服务器外网IP地址
WAN1	202.96.128.6
WAN2	58.60.231.2
WAN1	0.0.0.0

图105. 新增均衡策略-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%。

11.8.4 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：

DNS策略									新增	修改状态	删除所有	计数清零
序号	域名	TTL	A记录(配置条数/匹配计数)	CNAME启用(配置条数/匹配计数)	MX启用(配置条数/匹配计数)	匹配计数	<input type="checkbox"/> 状态	操作				
1	huasheng.com	86400	2/0	1/0	1/0	0	<input checked="" type="checkbox"/>	修改 删除				
2	Shan.com	86400	2/0	0/0	0/0	0	<input checked="" type="checkbox"/>	修改 删除				

图106. 线路配置

第二：点击<新增>按钮，增加 DNS 策略配置。如下图：

新增DNS策略										确定	返回	修改状态	计数清零	删除所有
域名	Shan.com													
TTL	86400													
A记录	序号	主机名	源地址		均衡策略	匹配计数	<input type="checkbox"/> 状态	操作						
	1	Xue	ISP地址表	电信	Policy-A		<input checked="" type="checkbox"/>	上移	下移	插入	删除			
	2	Xue	ISP地址表	网通	Policy-A		<input checked="" type="checkbox"/>	上移	下移	插入	删除			
新增														
CName记录	序号	别名	主机名		匹配计数	<input type="checkbox"/> 状态	操作							
	1					<input checked="" type="checkbox"/>	上移	下移	插入	删除				
新增														
MX记录	序号	主机名	优先级	邮件服务器	匹配计数	<input type="checkbox"/> 状态	操作							
	1					<input checked="" type="checkbox"/>	上移	下移	插入	删除				
新增														

序号越小，策略的优先级越高

图107. 新增 DNS 策略

参数说明：

- 域名：在此填入需要做多重定制的名称（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): 定制名称的别名。

◇ 主机名 (Host Name): 输入主机名称的前置词。

◇ 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。

11.9 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：

ARP表							转为静态	新增	删除所有
序号	IP地址	MAC地址	物理接口	类型	<input type="checkbox"/> 静态	操作			
1	172.16.111.199	00:1A:80:56:46:5F	Bridge2	动态	<input type="checkbox"/>	删除			
2	172.16.161.2	8C:89:A5:7D:E3:12	Bridge2	动态	<input type="checkbox"/>	删除			

图108. ARP 表

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

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

第三：点击<新增>按钮，可添加静态 ARP 条目，如下图：

新增静态ARP		提交	返回
IP地址	<input type="text" value="172.16.3.3"/>		
MAC地址	<input type="text" value="00:5B:78:7A:34:33"/>	(格式范例: 00:5B:78:7A:34:42)	

图109. 新增静态 ARP

11.10 DHCP配置

11.10.1 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：

基本参数								新增
序号	接口名称	DNS服务器	IP地址池	网关	租用期限	状态	操作	
1	LAN1	202.96.134.23	192.168.2.2-192.168.2.230	192.168.2.1	永不过期	禁用	修改 删除	

图110. 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：

DHCP基本参数		确定	返回
接口名称	LAN1		
首选DNS服务器	202.96.134.23 (必填)		
备用DNS服务器			
IP地址池	一行一个地址，格式范例：192.168.2.1 或 192.168.2.2-192.168.2.253 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。 192.168.2.2-192.168.2.230 (必填)		
固定IP	一行一个固定IP，固定IP的地址不能在IP地址池范围内，名称不能为中文； 格式范例：名称/IP/MAC，如 Tom/192.168.1.1/00:19:21:3f:a1:11 Anna/192.168.2.11/00:19:21:3f:a1:01 Pat/192.168.2.12/00:19:21:3f:a1:45		
子网掩码	255.255.255.0 (必填，格式范例：24或255.255.255.0)		
网关IP	192.168.2.1 (一般为接口IP)		
租用期限	<input checked="" type="radio"/> 永不过期 <input type="radio"/> 3 日 0 时 0 分		

图111. 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。

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。

11.10.2 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：

DHCP中继				新增
序号	中继接口	DHCP Server IP	操作	
1	LAN1-->WAN1	172.16.111.48	修改 删除	

图112. DHCP 中继

第二：进入点击<新增>按钮，增加 DHCP 中继配置。如下图：

新增DHCP中继		确定	返回
中继接口	从 LAN1 到 WAN1		
DHCP Server IP	192.168.5.33		

图113. 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。

11.10.3 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。

11.11 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:

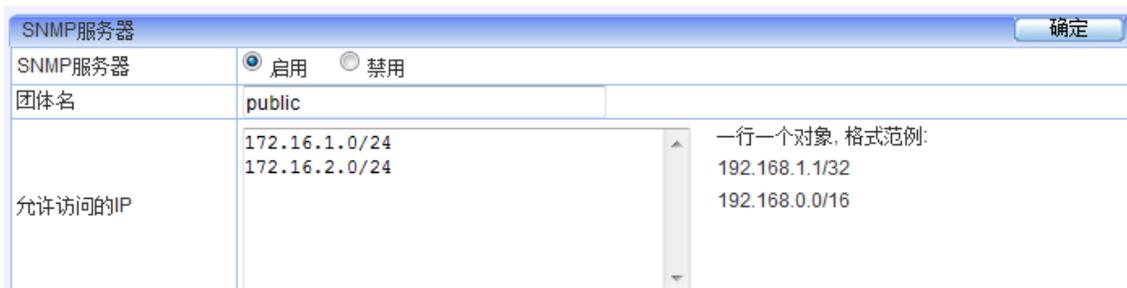


图114. SNMP 服务器

11.12 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:

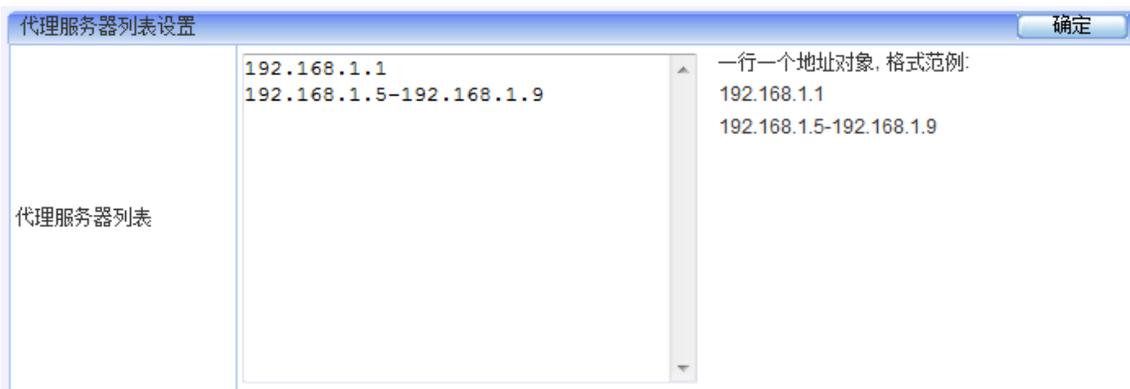


图115. 代理服务器列表

11.13 代理配置

代理配置包括两种，一是SSL透明代理，一种是对http代理、SSL代理、SOCKS5代理的配置。

功能描述：SSL透明代理可以设定需要做分析和审计的SSL域名。而代理配置页面可用来设定内网是否使用HTTP代理、SSL代理和SOCKS5代理等。

配置路径：【网络配置】>【代理配置】

配置描述：

第一步：进入【SSL透明代理配置】页面，配置需要代理的SSL页面的域名。如下图：

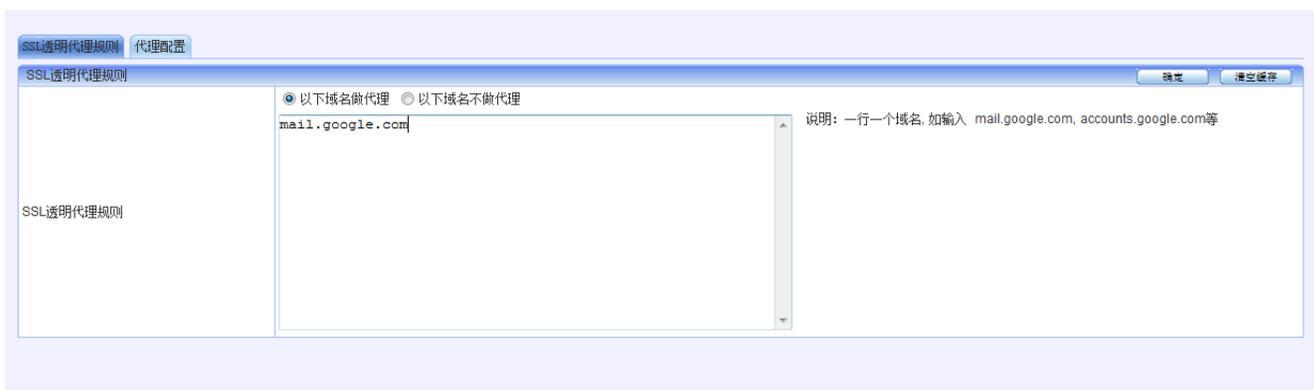


图116. SSL透明代理配置

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】>【上网管理】>【上网权限策略】页面，开启 SSL 管理，对 SSL 页面进行审计。如下图所示：

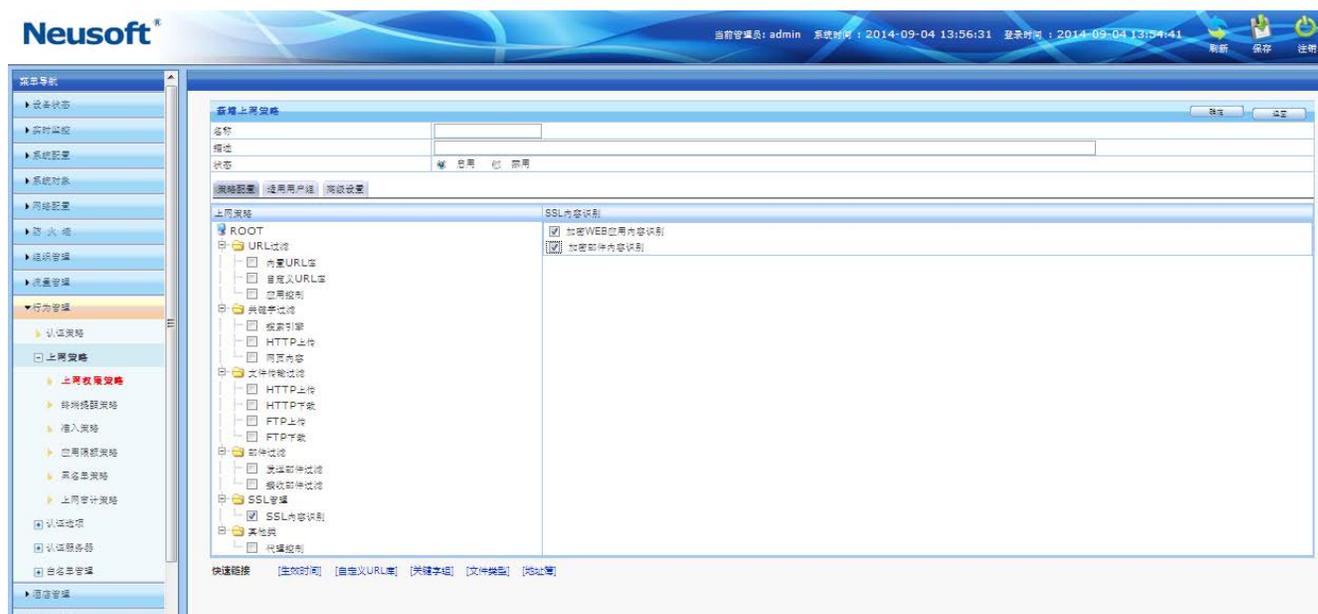


图117. 启用 SSL 代理配置

第三步：进入代理配置选项页面，如下图所示：

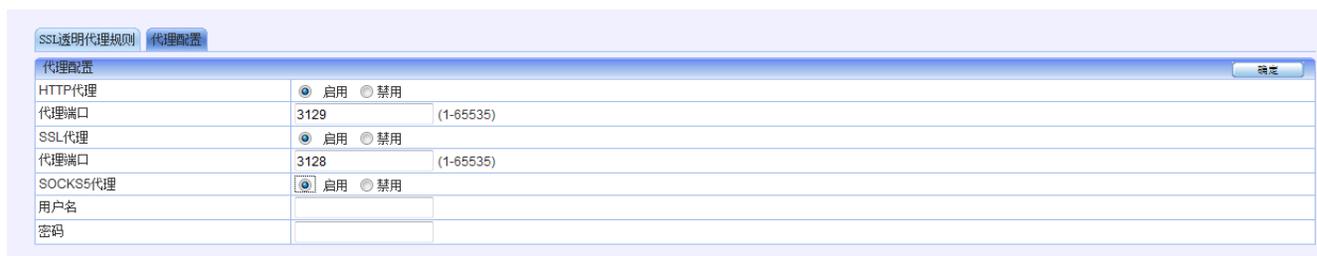


图118. 代理配置

参数说明：

- HTTP 代理：勾选“启用”，则设备会对 HTTP 服务进行代理。代理端口可以自定义，默认是 3129。勾选“禁用”则不会对 HTTP 服务进行代理。
- SSL 代理：勾选“启用”，则设备会对 SSL 服务进行代理。代理端口可以自定义，默认是 3128。勾选“禁用”则不会对 SSL 服务进行代理。
- SOCKS5 代理：勾选“启用”，则设备会对 SOCKS 服务进行代理，如果 socks 协议需要认证的话还需要输入用户名密码等信息。勾选“禁用”则不对 SOCKS 服务进行代理。

第四步：如果配置了代理，则需要浏览器的[工具—internet 选项—连接—局域网参数]中设定代理参数。如下图所示：

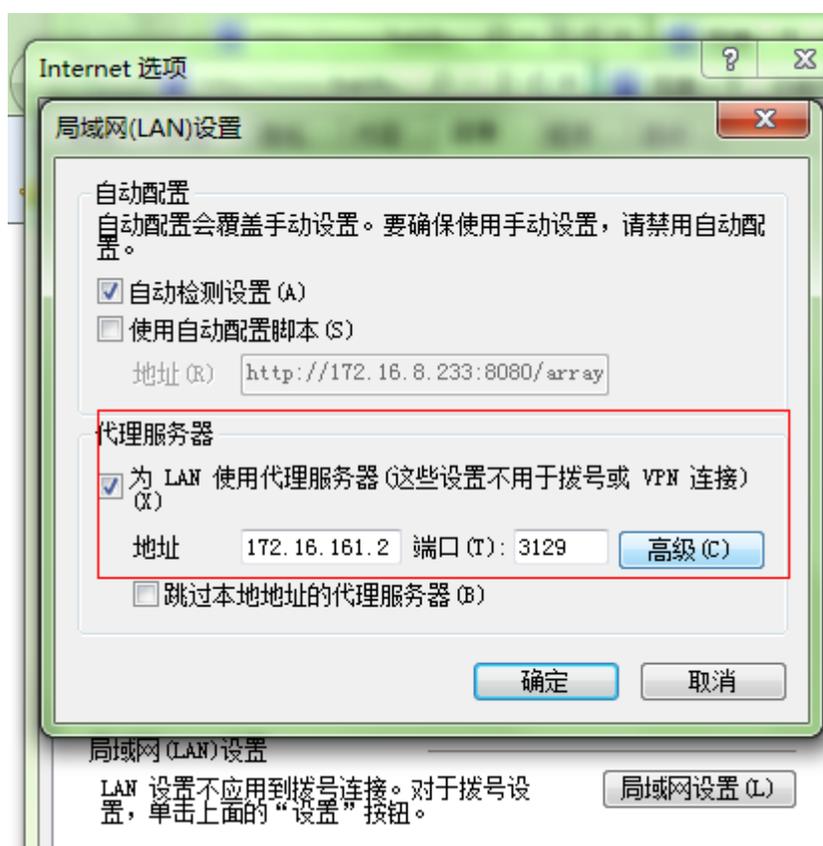


图119. 浏览器中代理服务器设置

12 防火墙

“防火墙”设置包括安全策略、NAT 规则、防DOS攻击、ARP欺骗防护、应用层网关、加速老化、移动终端管理。NAT 规则又包含内网代理、一对一地址转换、端口映射、服务器池四部分。

12.1 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120. 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→WAN2 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：

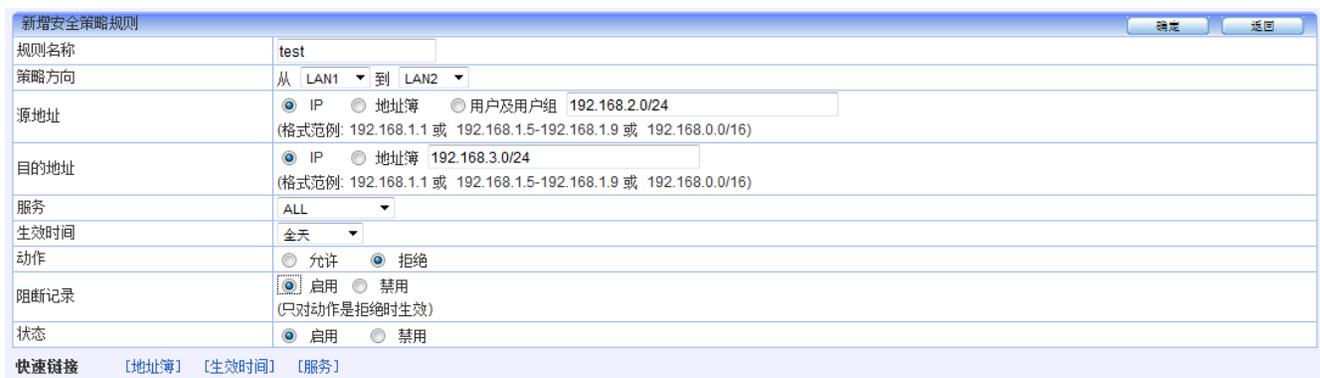


图121. 新增安全策略

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。

12.2 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。还包含了服务器池。

12.2.1 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【内网代理】页面，如下图：

序号	规则名称	流量方向	内部源地址	目的地址	服务	转换后源地址	匹配计数	状态	操作
1	test	LAN1 -> WAN1	全部	全部	ALL	WAN1端口地址	0	<input checked="" type="checkbox"/>	修改 插入 移动 删除

提示：序号越小的规则优先级越高，可通过<插入>或<移动>来改变规则的先后顺序。

图122. 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123. 新增内网代理规则

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。

12.2.2 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124. 一对一静态地址转换

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125. 新增转换规则

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

12.2.3 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126. 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：

新增端口映射规则		确定	返回
规则名称	<input type="text"/>		
外网口	WAN1 (从该端口进出的数据流才转换)		
内部地址	<input type="text"/> (单个IP, 如 192.168.5.3)		
对外映射地址	<input checked="" type="radio"/> 外网口地址 <input type="radio"/> <input type="text"/> (单个IP, 如 1.1.1.251)		
协议号	<input checked="" type="radio"/> TCP <input type="radio"/> UDP		
内部端口	<input type="text"/> - <input type="text"/> (与“对外映射端口”一一对应)		
对外映射端口	<input type="text"/> - <input type="text"/> (与“内部端口”一一对应)		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		

图127. 新增端口映射

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

12.2.4 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:

服务器池							
序号	规则名称	对外映射地址	对外映射端口	服务器地址	匹配计数	<input type="checkbox"/> 状态	操作
1	aaasdfad	1.2.3.4	11	1.1.1.1 2.2.2.2	0	<input type="checkbox"/>	修改 删除
5	FTP-Server	202.96.123.32	322	192.168.33.250 192.168.33.251 192.168.33.252 192.168.33.253	0	<input checked="" type="checkbox"/>	修改 删除

图128. 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：

新增服务器池							确定	返回
规则名称	FTP-Server							
对外映射地址	202.96.123.32							
对外映射端口	322							
服务器地址1	192.168.33.250	服务器端口1	21	比重1	30	%		
服务器地址2	192.168.33.251	服务器端口2	21	比重2	30	%		
服务器地址3	192.168.33.252	服务器端口3	21	比重3	20	%		
服务器地址4	192.168.33.253	服务器端口4	21	比重4	20	%		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用							

图129. 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；

12.3 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：

防DOS攻击		确定
启用防DOS攻击	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	
最大连接数	1024	(超过这个数IP就会被屏蔽)
禁用IP时间	600	(单位: 秒)
IP地址白名单	0.0.0.0 一行一个对象, 格式范例: 192.168.1.1/32 192.168.0.0/16	

图130. 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。

12.4 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:

ARP欺骗防护		确定	手动广播
功能状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
ARP 保护对象	<input checked="" type="radio"/> 设备本身 <input type="radio"/> 手动指定		
ARP 广播间隔 (秒)	40		

如需IP绑定MAC地址, 请单击>>ARP表

图131. 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：

1. 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）。
2. 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：

ARP欺骗防护		确定	手动广播
功能状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
ARP 保护对象	<input type="radio"/> 设备本身 <input checked="" type="radio"/> 手动指定		
第一组	发送IP: 172.168.33.201 发送MAC: 00:5B:78:7A:34:43 (格式范例: 00:5B:78:7A:34:42) 发送接口: <input checked="" type="checkbox"/> LAN1 <input type="checkbox"/> WAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> WAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN3.3 <input type="checkbox"/> LAN2.4094		
第二组	发送IP: 10.3.3.201 发送MAC: 00:5B:78:7A:34:45 (格式范例: 00:5B:78:7A:34:42) 发送接口: <input type="checkbox"/> LAN1 <input type="checkbox"/> WAN1 <input checked="" type="checkbox"/> LAN2 <input type="checkbox"/> WAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN3.3 <input type="checkbox"/> LAN2.4094		
第三组	发送IP: 发送MAC: (格式范例: 00:5B:78:7A:34:42) 发送接口: <input type="checkbox"/> LAN1 <input type="checkbox"/> WAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> WAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN3.3 <input type="checkbox"/> LAN2.4094		
第四组	发送IP: 发送MAC: (格式范例: 00:5B:78:7A:34:42) 发送接口: <input type="checkbox"/> LAN1 <input type="checkbox"/> WAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> WAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN3.3 <input type="checkbox"/> LAN2.4094		
ARP 广播间隔 (秒)	40		

如需IP绑定MAC地址，请单击>>ARP表

图132. 防 DOS 攻击

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。

12.5 应用层网关

功能描述：标准的SIP或者H323，当设备为路由模式，做NAT的时候，视频电话的数据是私网IP，启用这个功能把数据业务的私网IP装成公网IP（相当于映射），来实现视频语音业务的互通。

配置路径：【防火墙】>【应用层网关】

配置描述：点击【应用层网关】页面，如图：



图133. 应用层网关

12.6 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】

配置描述: 进入【加速老化】页面，如下图：

加速老化		
加速倍数	2	
高水位	50	% (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	30	% (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	21600	秒
UDP超时时间	180	秒
ICMP超时时间	30	秒
Other超时时间	600	秒
TCP SYN超时时间	120	秒
无回应UDP超时时间	30	秒
当前会话数/最大会话数	58 / 512000	

图134. 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。

12.7 防病毒设置

功能描述：主要用于在传输文件的过程中，比如病毒文件，通过匹配本地的病毒库和扫描的文件类型判断是否存在病毒，如果识别出是病毒文件，则自动删除。默认不开启。

配置路径：【防火墙】>【防病毒设置】

配置描述：进入【防病毒设置】页面，如下图：



勾选则扫描该文件类型，不勾选则不扫描

12.8 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】

配置描述：进入【移动终端管理】页面，如下图：

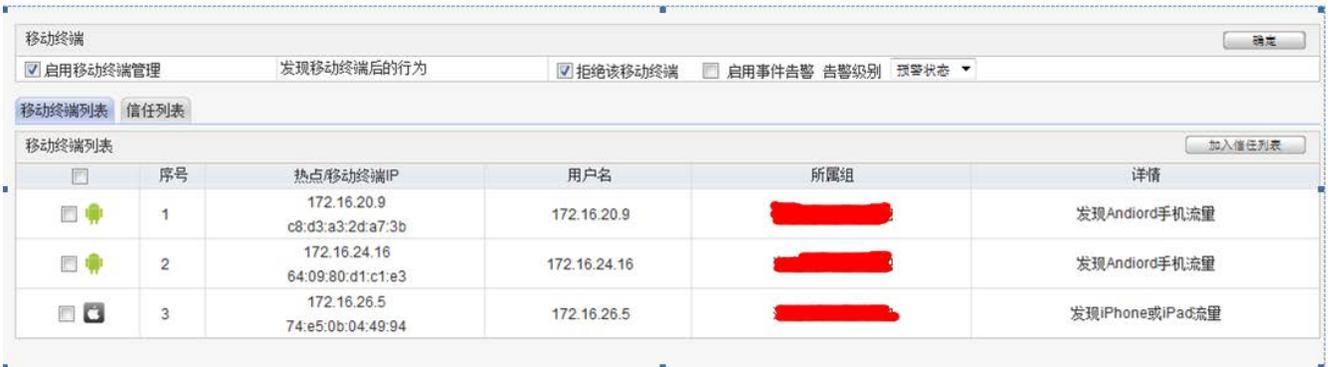


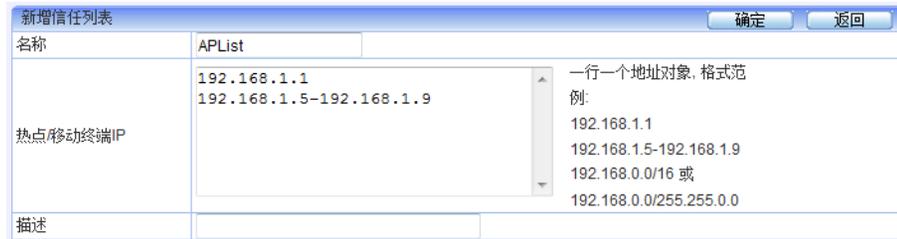
图135. 无线热点发现

参数说明:

- 启用移动终端管理：用于全局的开启或关闭移动终端管理功能。
- 发现移动终端后的行为：可以是[拒绝该移动终端]或者是[启用事件告警]。若未勾选“拒绝该移动终端”，设备将放行移动终端列表中的AP或移动终端。
 - 无线热点列表：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时间等信息。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。



点击<新增>按钮，弹出如下对话框，填写 AP 的 IP 或者是 AP 做 DHCP 的网段即可。



备注：如果 AP 做无线路由器，直接填 AP 的 IP；如果 AP 做无线网桥，填上 AP 做 DHCP 的网段。加入信任列表的热点/移动终端将不再出现在无线热点列表中。

13 VPN配置

13.1 IPSec

13.1.1 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136. IPSec 隧道配置

第二：进入点击<新增>按钮，增加 IPSec 隧道。如下图：



图137. 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。

13.1.2 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138. 配置 IPSec 规则

第二：进入点击<新增>按钮，增加IPSec规则。如下图：



图139. 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。

13.2 PPTP

功能描述：配置 PPTP VPN。

配置路径：【VPN】>【PPTP】

配置描述：进入【PPTP】页面，开始设置 PPTP的相关参数。如下图：

PPTP设置				确定
PPTP状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用			
服务器IP	14.127.235.165	(此项填外网口IP)		
首选DNS服务器	202.96.134.133			
备用DNS服务器	8.8.8.8			
认证方式	<input checked="" type="radio"/> Radius认证 <input type="radio"/> VPN用户本地认证			
IP地址				
认证端口	1812	(1-65535)		
计费端口	1813	(1-65535)		
共享密钥	●●●●●●●●			

PPTP IP池				新增	删除所有
序号	起始IP	结束IP	操作		
1	172.16.3.216	172.16.3.220	修改	删除	
2	10.5.3.3	10.5.3.30	修改	删除	

图140. 配置 PPTP

参数说明：

- PPTP 状态：启用或禁用 PPTP 服务器功能。
- 服务器 IP：本机作为 PPTP 服务器的接口 IP 地址。
- 首选 DNS 服务器：分配给 PPTP 拨号用户的首选 DNS 服务器。
- 备用 DNS 服务器：分配给 PPTP 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 PPTP VPN 用户。

第二：进入点击<新增>按钮，增加 PPTP IP 池。如下图：

新增PPTP IP池		确定	返回
起始IP	10.5.3.3		
结束IP	10.5.3.30		

图141. 新增 PPTP IP 池

参数说明:

- 起始 IP: 分配给 PPTP 拨号用户的 IP 地址段的起始地址。
- 结束 IP: 分配给 PPTP 拨号用户的 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 拨号用户。

13.3 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:

L2TP设置		确定
L2TP状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
服务器IP	172.16.161.2	(此项填外网口IP)
预共享密钥	123456	(L2TP IPSEC VPN客户端预共享密钥)
L2TP本地IP	10.203.123.200	(L2TP VPN客户端协商成功后的网关IP)
L2TP IP范围		
起始IP	10.203.123.201	
结束IP	10.203.123.210	
首选DNS服务器	202.96.134.133	
备用DNS服务器	8.8.8.8	
认证方式	<input checked="" type="radio"/> Radius认证 <input type="radio"/> VPN用户本地认证	
IP地址		
认证端口	1812	(1-65535)
计费端口	1813	(1-65535)
Radius共享密钥	●●●●●●●●	

图142. 配置 L2TP

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。
- 与共享密钥: 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。

13.4 VPN 用户

功能描述：配置 VPN 的用户，该用户可应用于 PPTP VPN 和 L2TP VPN 的客户端。

配置路径：【VPN】>【VPN 用户】

配置描述：

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

VPN用户				新增	删除所有
序号	用户名	接入模式	操作		
1	James	PPTP模式	修改	删除	
2	Linda	PPTP模式	修改	删除	
3	Jobs	PPTP模式	修改	删除	

图143. 配置 VPN 用户

第二：进入点击<新增>按钮，增加 PPTP 用户。如下图：

新增VPN用户		确定	返回
用户名	Tim		
密码	●●●●●● (6-16位)		
确认密码			
接入模式	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP		

图144. 配置 VPN 用户

参数说明：

- 用户名：VPN 用户的名称；
- 密码：VPN 用户的密码；
- 确认密码：VPN 用户的确认密码；
- 接入模式：选择该用户可以应用于哪些 VPN 协议，可选择为 PPTP、L2TP。

提示：VPN 用户可应用于 PPTP VPN 和 L2TP VPN 的拨号用户。

14 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、临时账号设置、DKey 管理。

14.1 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。

14.1.1 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：【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：

The screenshot shows the Neusoft management interface. The top navigation bar includes the Neusoft logo, user information (admin), system time (2014-09-04 14:05:53), and login time (2014-09-04 13:54:41). The left sidebar contains a menu with '组织管理' (Organization Management) expanded to show '组织结构' (Organization Structure). The main content area shows a table of users and groups.

序号	名称	绑定检查	所属组	摘要
1	gong		网域科技	子组: 48, 用户: 19
2	test		网域科技	子组: 0, 用户: 1
3	user		网域科技	子组: 0, 用户: 1
4	192.168.0.11 (192.168.0.11)	192.168.0.11	网域科技	普通用户 (在线)
5	192.168.0.155 (192.168.0.155)	192.168.0.155	网域科技	普通用户 (在线)
6	192.168.0.227 (192.168.0.227)	192.168.0.227	网域科技	普通用户 (在线)
7	192.168.0.92 (192.168.0.92)	192.168.0.92	网域科技	普通用户 (在线)
8	111 (111)		网域科技	认证用户 (离线)
9	172.16.254.1 (172.16.254.1)	172.16.254.1	网域科技	普通用户 (离线)
10	172.16.254.10 (172.16.254.10)	172.16.254.10	网域科技	普通用户 (离线)
11	172.16.254.13 (172.16.254.13)	172.16.254.13	网域科技	普通用户 (离线)
12	172.16.254.14 (172.16.254.14)	172.16.254.14	网域科技	普通用户 (离线)
13	172.16.254.15 (172.16.254.15)	172.16.254.15	网域科技	普通用户 (离线)
14	172.16.254.21 (172.16.254.21)	172.16.254.21	网域科技	普通用户 (离线)
15	172.16.254.8 (172.16.254.8)	172.16.254.8	网域科技	普通用户 (离线)

图145. 组织结构-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。右边是左边已定组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。

14.1.2 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：

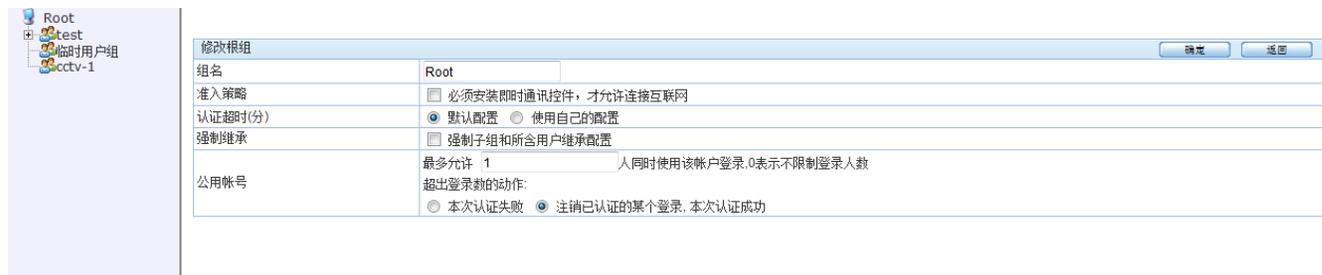


图146. 组织结构-修改根组

参数说明：

- ◇ 组名：根组的名称，默认 Root，可填入需要修改的名称。
- ◇ 准入策略：必须安装即时通讯控件，才允许连接互联网。默认不启用。
- ◇ 认证超时：默认配置是指“行为管理—认证选项—认证参数”中的超时时间。也可使用自己的配置。
- ◇ 强制继承：强制子组和所含用户继承准入策略的配置，默认未启用。启用后，所有的用户和子组的准入策略都被修改为根组的配置。
- ◇ 公用帐号：

14.1.3 新增子组

功能描述：新增子组，并设置子组的准入策略的HTTP代理。

配置路径：【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：

新增子组		确定	返回
组名	一行一个组名,支持汉字、数字、字母、下划线、中划线		
所属组	Root	选择	
准入策略	继承父组配置		
HTTP代理	继承父组配置		
认证超时(分)	<input checked="" type="radio"/> 默认配置 <input type="radio"/> 使用自己的配置		
离线用户自动删除	<input type="checkbox"/> 自动删除本组内离线时间超过指定时间的用户 指定时间: 1 <input type="radio"/> 分钟 <input type="radio"/> 小时 <input checked="" type="radio"/> 天		
公用帐号	最多允许 0 人同时使用该帐户登录,0表示不限制登录人数 超出登录数的动作: <input type="radio"/> 本次认证失败 <input type="radio"/> 注销已认证的某个登录,本次认证成功 <input checked="" type="radio"/> 使用父组配置		

图147. 组织结构-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。

◇ 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]。

◇ 认证超时：默认配置是指“行为管理—认证选项—认证参数”中的超时时间。也可使用自己的配置。

◇ 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]。

◇ 公用帐号：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。
- 使用父组配置。

14.1.4 修改子组

功能描述：修改子组的配置。

配置路径：【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：

序号	名称	绑定检查	所属组	摘要
1	cctv-1		Root	子组: 0, 用户: 1
2	test		Root	子组: 4, 用户: 1
3	临时用户组		Root	子组: 0, 用户: 0
4	172.16.110.115 (172.16.110.115)	172.16.110.115	Root	普通用户 (在线)
5	172.16.0.191 (172.16.0.191)	172.16.0.191	Root	普通用户 (离线)
6	192.168.100.101 (192.168.100.101)	192.168.100.101	Root	普通用户 (离线)
7	192.168.16.3 (192.168.16.3)	192.168.16.3	Root	普通用户 (离线)
8	192.168.200.9 (192.168.200.9)	192.168.200.9	Root	普通用户 (离线)
9	192.168.200.90 (192.168.200.90)	192.168.200.90	Root	普通用户 (离线)
10	192.168.31.100 (192.168.31.100)	192.168.31.100	Root	普通用户 (离线)
11	192.168.31.105 (192.168.31.105)	192.168.31.105	Root	普通用户 (离线)
12	192.168.31.2 (192.168.31.2)	192.168.31.2	Root	普通用户 (离线)
13	192.168.31.90 (192.168.31.90)	192.168.31.90	Root	普通用户 (离线)
14	v10 (v10)	10	Root	普通用户 (离线)
15	v100 (v100)	100	Root	普通用户 (离线)
16	v14 (v14)	14	Root	普通用户 (离线)
17	v15 (v15)	15	Root	普通用户 (离线)
18	v31 (v31)	31	Root	普通用户 (离线)

图148. 组织结构-修改子组

第二：进入子组的修改页面，填入需要修改的值。如下图：

图149. 组织结构-修改子组

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。

◇ 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]。

◇ 认证超时：认证超时：默认配置是指“行为管理—认证选项—认证参数”中的超时时间。也可使用自己的配置。

◇ 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。

◇ 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]。

◇ 公用帐号：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。
- 使用父组配置。

◇ 安全组成员：如果启用了 ad 域，则有些用户可能会属于安全组成员。

14.1.5 新增普通用户

功能描述：新增普通用户。

配置路径：【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：

新增用户		确定	返回
用户名	<input type="text"/>		
显示名	<input type="text"/>		
描述	<input type="text"/>		
所属组	Root	选择	
用户类型	<input checked="" type="radio"/> 普通用户 <input type="radio"/> 认证用户		
绑定检查	<input checked="" type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input type="radio"/> 同时绑定MAC和IP <input type="radio"/> 绑定VLAN		
	<input type="text"/>		一行一个对象, 格式范例: 192.168.1.1 192.168.1.5-192.168.1.9 192.168.0.0/16 192.168.0.0/255.255.0.0
准入策略	继承父组配置		
用户状态	<input checked="" type="radio"/> 正常 <input type="radio"/> 冻结		

图150. 组织结构-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。
- ◇ 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。

14.1.6 新增认证用户

功能描述：新增认证用户。

配置路径：【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：

新增用户		确定	返回
用户名	<input type="text"/>		
显示名	<input type="text"/>		
描述	<input type="text"/>		
所属组	Root 选择		
用户类型	<input type="radio"/> 普通用户 <input checked="" type="radio"/> 认证用户		
绑定检查	<input checked="" type="radio"/> 无绑定 <input type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input type="radio"/> 同时绑定MAC和IP <input type="radio"/> 绑定VLAN		
认证方式	<input checked="" type="radio"/> 本地认证 <input type="radio"/> 到外部服务器认证 (此处选择的目的是为了是否配置密码) 密码: <input type="password"/> 确认密码: <input type="password"/>		
公用帐号	最多允许 <input type="text" value="0"/> 人同时使用该帐户登录。0表示不限制登录人数 超出登录数的动作: <input type="radio"/> 本次认证失败 <input type="radio"/> 注销已认证的某个登录, 本次认证成功 <input checked="" type="radio"/> 使用父组配置		
有效期	<input checked="" type="radio"/> 永远有效 <input type="radio"/> 在 <input type="text" value="1"/> 小时之内有效 (用户登录后) <input type="radio"/> 在 <input type="text" value="2014-06-20 10:02:14"/> 之间有效 (格式: yyyy-mm-dd)		
准入策略	继承父组配置		
用户状态	<input checked="" type="radio"/> 正常 <input type="radio"/> 冻结		

图151. 组织结构-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
 - 使用父组配置: 继承父组的配置。
- ◇ 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。

14.1.7 修改用户

功能描述: 修改用户的配置

配置路径: 【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/cctv-1 下面的 Susan 用户。先定位到 Root/cctv-1，然后单击名称列的 Susan 用户的链接，如下图所示：



图152. 组织结构-修改用户

第二：进入用户的修改页面，填入需要修改的值。如下图：

用户名	susan
显示名	susan
描述	主播
所属组	Root/cctv-1 选择
用户类型	<input checked="" type="radio"/> 普通用户 <input type="radio"/> 认证用户
绑定检查	<input checked="" type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input type="radio"/> 同时绑定MAC和IP <input type="radio"/> 绑定VLAN 192.168.3.6 一行一个对象, 格式范例: 192.168.1.1 192.168.1.5-192.168.1.9 192.168.0.0/16 192.168.0.0/255.255.0.0 清空列表
准入策略	继承父组配置
用户状态	<input checked="" type="radio"/> 正常 <input type="radio"/> 冻结

图153. 组织结构-修改用户

14.1.8 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。

14.1.8.1 绑定IP

功能描述：绑定用户的IP地址

配置路径：【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：

修改用户	确定 返回	
用户名	172.16.0.191	
显示名	172.16.0.191	
描述	IP: 172.16.0.191 MAC:60:eb:69:d1:99:29	
所属组	Root	选择
用户类型	<input checked="" type="radio"/> 普通用户 <input type="radio"/> 认证用户 <input checked="" type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input type="radio"/> 同时绑定MAC和IP <input type="radio"/> 绑定VLAN	
绑定检查	<input type="text" value="172.16.0.191"/>	一行一个对象, 格式范例: 192.168.1.1 192.168.1.5-192.168.1.9 192.168.0.0/16 192.168.0.0/255.255.0.0
	清空列表	
准入策略	继承父组配置	
用户状态	<input checked="" type="radio"/> 正常 <input type="radio"/> 冻结	

图154. 组织结构-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。

14.1.8.2 绑定MAC

功能描述：绑定用户的 MAC 地址

配置路径：【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：

修改用户	确定 返回	
用户名	susan	
显示名	susan	
描述	主播	
所属组	Root/cctv-1	选择
用户类型	<input type="radio"/> 普通用户 <input type="radio"/> 认证用户 <input type="radio"/> 绑定IP <input checked="" type="radio"/> 绑定MAC <input type="radio"/> 同时绑定MAC和IP <input type="radio"/> 绑定VLAN	
绑定检查	<input type="text" value="00:24:8C:51:24:22"/>	一行一个对象, 格式范例: 00:24:8C:51:24:22 00:24:8C:51:24:23
	扫描MAC地址 清空列表	
准入策略	继承父组配置	
用户状态	<input checked="" type="radio"/> 正常 <input type="radio"/> 冻结	

图155. 组织结构-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156. 组织结构-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](#)】

14.1.8.3 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：

修改用户		确定	返回
用户名	susan		
显示名	susan		
描述	主播		
所属组	Root/cctv-1 选择		
用户类型	<input checked="" type="radio"/> 普通用户 <input type="radio"/> 认证用户 <input type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input checked="" type="radio"/> 同时绑定MAC和IP <input type="radio"/> 绑定VLAN		
绑定检查	<div style="border: 1px solid red; padding: 2px;">192.168.1.1 (00:24:8C:51:24:22)</div> <div style="font-size: small; margin-top: 5px;"> 一行一个对象，格式范例： 192.168.1.1(00:24:8C:51:24:22) 192.168.1.2(00:24:8C:51:24:23) </div>		
准入策略	继承父组配置		
用户状态	<input checked="" type="radio"/> 正常 <input type="radio"/> 冻结		

图157. 组织结构-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：

修改用户		确定	返回
用户名	susan		
显示名	susan		
描述	主播		
所属组	Root/cctv-1 选择		
用户类型	<input checked="" type="radio"/> 普通用户 <input type="radio"/> 认证用户 <input type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input checked="" type="radio"/> 同时绑定MAC和IP <input type="radio"/> 绑定VLAN		
绑定检查	<div style="border: 1px solid red; padding: 2px;">192.168.1.1 (00:24:8C:51:24:22)</div> <div style="font-size: small; margin-top: 5px;"> 一行一个对象，格式范例： 192.168.1.1(00:24:8C:51:24:22) 192.168.1.2(00:24:8C:51:24:23) </div>		
	<div style="border: 1px solid red; padding: 2px; margin-top: 5px;"> 扫描MAC地址 清空列表 扫描起始IP: 192.168.1.1 扫描结束IP: 192.168.1.100 开始扫描 </div>		
准入策略	继承父组配置		
用户状态	<input checked="" type="radio"/> 正常 <input type="radio"/> 冻结		

图158. 组织结构-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](#)】

14.1.8.4 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：

The screenshot shows the 'Modify User' configuration page. The user name is 'susan' and the group is 'Root/cctv-1'. Under 'User Type', the 'Bind VLAN' option is selected. The 'Binding Check' section has a text input field containing '10' and a 'Clear List' button. To the right of the input field, there is a list of examples: '108' and '108-109'. The 'User Status' is set to 'Normal'.

图159. 组织结构-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 VLAN。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。

14.1.9 导出用户和组

功能描述：导出用户和组的配置

配置路径：【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 and 用户，然后点击<导出>按钮，如下图：

修改根组 新增子组 新增用户 导出 移动 删除 清空当前组 查询

本组成员总数: 子组 (7), 用户 (17); 可对选中的组和用户进行导出、移动和删除操作

序号	名称	绑定检查	所属组	摘要
1	cctv-1		Root	子组: 0, 用户: 1
2	test		Root	子组: 4, 用户: 1
3	临时用户组		Root	子组: 0, 用户: 0
4	172.16.110.115 (172.16.110.115)	172.16.110.115	Root	普通用户 (在线)
5	172.16.0.191 (172.16.0.191)	172.16.0.191	Root	普通用户 (离线)
6	192.168.100.101 (192.168.100.101)	192.168.100.101	Root	普通用户 (离线)
7	192.168.16.3 (192.168.16.3)	192.168.16.3	Root	普通用户 (离线)
8	192.168.200.9 (192.168.200.9)	192.168.200.9	Root	普通用户 (离线)
9	192.168.200.90 (192.168.200.90)	192.168.200.90	Root	普通用户 (离线)
10	192.168.31.100 (192.168.31.100)	192.168.31.100	Root	普通用户 (离线)
11	192.168.31.105 (192.168.31.105)	192.168.31.105	Root	普通用户 (离线)
12	192.168.31.2 (192.168.31.2)	192.168.31.2	Root	普通用户 (离线)
13	192.168.31.90 (192.168.31.90)	192.168.31.90	Root	普通用户 (离线)
14	v10 (v10)	10	Root	普通用户 (离线)
15	v100 (v100)	100	Root	普通用户 (离线)
16	v14 (v14)	14	Root	普通用户 (离线)
17	v15 (v15)	15	Root	普通用户 (离线)
18	v31 (v31)	31	Root	普通用户 (离线)

图160. 组织结构-导出用户和组

第二: 将选中的用户和组保存到 PC。

Neusoft[®] 当前管理员: admin 系统时间: 2014-09-04 14:09:13 登录时间: 2014-09-04 13:54:41

菜单导航: 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 (选中), 流量管理, 行为管理, 酒店管理

组织管理子菜单: 组织结构 (选中), 批量导入, LDAP/AD导入, 扫描内网主机, 临时账号设置, DKey 管理

另存为对话框: 保存至 (D:) 360Downloads, 文件名为 organizedFrame.csv, 保存类型为 Microsoft Excel 工作表

序号	名称	绑定检查	所属组	摘要
9				
10				
11				
12				
13				
14				
15				
16	192.168.0.111 (192.168.0.111)	192.168.0.111	网域科技	普通用户 (离线)
19	192.168.0.15 (192.168.0.15)	192.168.0.15	网域科技	普通用户 (离线)
20	192.168.0.201 (192.168.0.201)	192.168.0.201	网域科技	普通用户 (离线)

14.1.10 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: 【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, 勾选要移动的用户和组, 然后点击<移动>按钮, 如下图所示:



图161. 组织结构-移动用户和组

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：

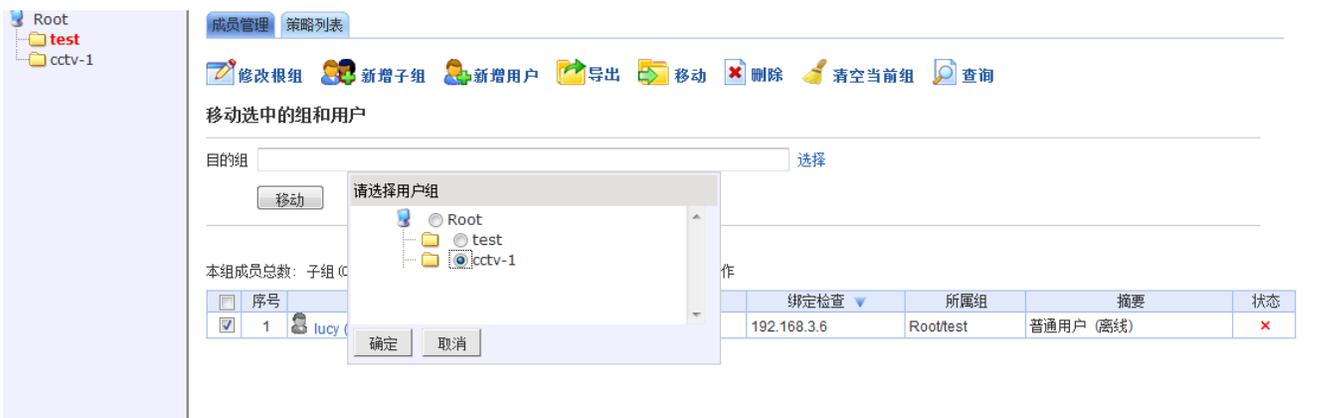


图162. 组织结构-移动用户和组

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。

14.1.11 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163. 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。

14.1.12 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164. 组织结构-删除用户和组

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。

14.2 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：

批量导入		确定
文件类型	<input checked="" type="radio"/> 已导出文件(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, 只支持csv格式) <input type="radio"/> 自定义文件(只能导入用户到某个组, 只支持 csv 格式) 范例下载	
文件位置	<input type="text"/> 浏览...	
所属组	<input type="text"/> 选择	

图165. 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 and 用户放于哪个父组下面。

14.3 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166. LDAP/AD 导入-匿名查询

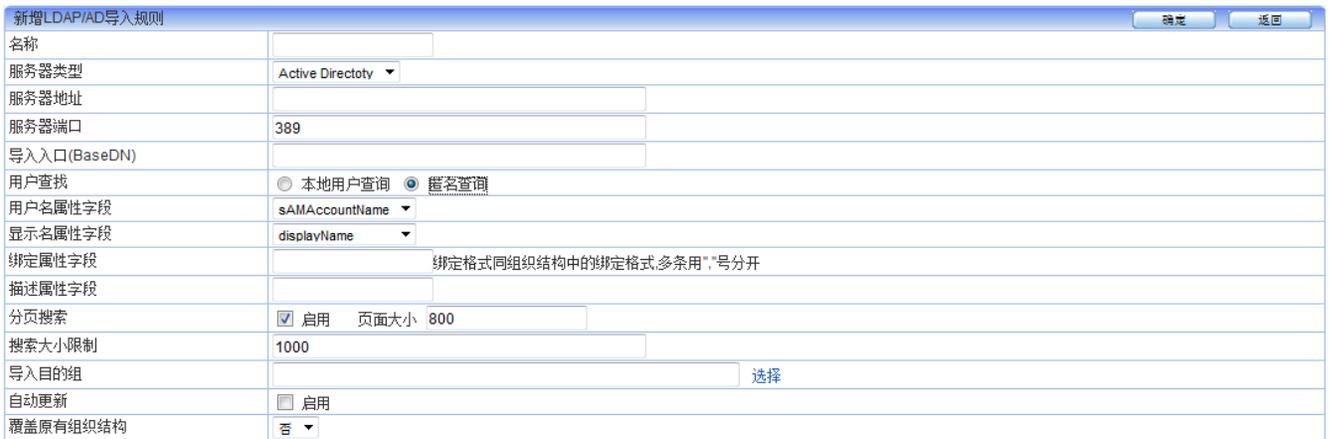


图167. LDAP/AD 导入-匿名查询

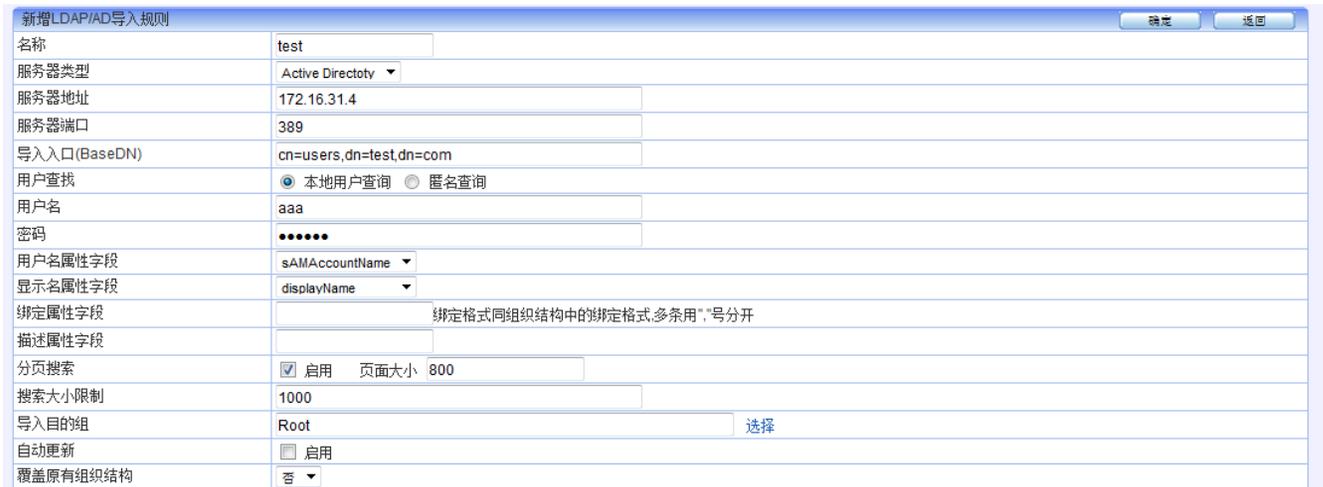


图168. LDAP/AD 导入-本地用户查询

第二：配置各个参数，参数说明如下：

- 名称：本条导入规则的名称。

- 服务器类型：有以下 4 种：Active Directory、openldap、lotus ldap 以及 other ldap。
- 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。
- 用户名：LDAP/AD 中任何一个用户的名称。
- 密码：对应上面输入的用户名的密码。用
- 户名属性字段：可选择 sAMAccountName（Windows NT 使用者名称系统）、cn（组名）、uid（userid）或者自定义的值作为用户名。默认是 sAMAccountName。
- 显示名属性字段：可选择 sAMAccountName、displayname、userPrincipalName（使用者主体名称）、cn、uid 或者自定义值作为显示名属性字段。默认是 displayname 值。
- 绑定属性字段：
- 描述属性字段：
- 分页搜索：在组织结构较大的环境里面，可启用分页搜索。
- 搜索大小限制：限制搜索大小。
- 导入目的组：可定义将 LDAP/AD 服务器上的用户和组信息导入至哪个组下面。
- 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。
- 覆盖原有组织结构：选择是否覆盖原有的组织结构，默认不覆盖。

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>

14.4 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：

序号	IP地址	MAC地址	主机名	是否已加入组织结构
1	172.16.161.69	08:00:27:8e:97:41	LOCALHOST	是 (Root\172.16.161.69)
2	172.16.161.72	2c:59:e5:50:a0:c7	HP2C59E550A0C7	是 (Root\172.16.161.72)
3	172.16.161.169	78:45:c4:a1:83:53	ZHANGHUANAN-PC	是 (Root\172.16.161.169)
4	172.16.161.177	00:23:5a:32:6b:20	START-PC	是 (Root\172.16.161.177)
5	172.16.161.225	94:de:80:b8:9f:32	JINXIN-PC	是 (Root\172.16.161.225)

图169. 组织结构-扫描内网主机

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 192.168.0.1/24。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：

用户名	显示名	绑定IP	绑定MAC	主机名	所属组
172.16.161.69		172.16.161.69	08:00:27:8e:97:41	LOCALHOST	选择

冲突处理： 覆盖已存在的用户

图170. 组织结构-扫描内网主机

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，选择希某个用户的组。如下图：

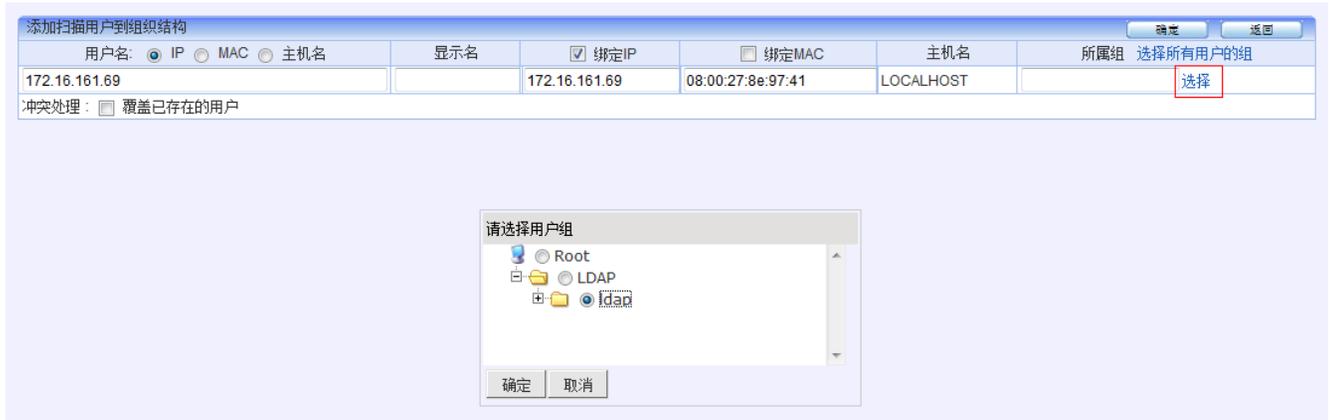


图171. 组织结构-扫描内网主机

14.5 临时账户管理

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。

14.5.1 临时账户设置

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：【组织结构】>【临时账户设置】>【基本配置】

配置描述：

第一：进入【基本配置】配置页面，首先看到[单个临时账号]选项，如下图：



图172. 临时账户设置—基本设置—单个临时账号

参数说明:

- 临时账户开关: [开启]或[关闭]单个临时账户功能。
- 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。
- 核定类型: 自动核定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; 手动核定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。
- 审核类型: 审核类型有“手动核定”和“自动核定”两种。
 - 如果是“手动核定”, 需要填写管理员邮箱, 系统会将申请信息发送至管理员邮箱, 以便及时对申请信息进行核定。
 - 如果是“自动审核”, 账密派送模式, 支持以下四种模式。
 - ◇ 页面显示账密: 在认证页面直接显示账户和密码。
 - ◇ 寄账密至申请者邮箱: 将账户和密码发送至申请者邮箱
 - ◇ 通过短信发送密码: 用户名为手机号, 密码通过短信发送到申请者手机。
 - ◇ 页面显示二维码与账密: 在认证页面直接显示账户和密码, 使用该账号和密码登录后, 在认证成功页面显示二维码, 移动终端通过扫描二维码进行认证上网。

“自动审核”页面如下:

单个临时账号		批量临时账号	确定
临时账号开关	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
帐密邮箱域名	格式范例: hotmail.com 或为空 (为空时, 申请者邮箱域名将不被限定)		
审核类型	<input type="radio"/> 手动审核 <input checked="" type="radio"/> 自动审核		
所属组	Root <input type="button" value="选择"/>		
帐密派送模式	<input type="radio"/> 页面显示帐密 <input type="radio"/> 寄帐密至申请者邮箱 <input checked="" type="radio"/> 通过短信发送密码 <input type="radio"/> 页面显示二维码与帐密		
有效时间	<input checked="" type="radio"/> 在 2014-06-24 之间有效(格式: yyyy-mm-dd)		
	<input type="radio"/> 在 _____ 小时之内有效 (用户登录后)		
	<input type="radio"/> 用户申请结束时间		

图173. 自动审核页面

- 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174. 新增临时账号用户的认证策略

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。

第二：进入“批量申请临时账号”选项卡。

功能描述：批量申请临时账号。

配置路径：【组织结构】>【临时账户设置】>【基本配置】

配置描述：进入“批量临时账号”选项卡，如下图：

参数说明:

- 临时账号开关：[启用]或[禁用]批量临时账号
- 管理员邮箱：填写网络管理者邮箱，用来接收包含临时账号用户名和密码的 Excel 表格的

邮件。

14.5.2 申请临时账户的步骤（页面与Email获取密码）

第一步：在【行为管理>认证策略】页面配置一条策略，[认证方式]选择[到服务器去认证]，[首选认证服务器]为[本地服务器]。如下图：

名称	认证策略
IP地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 <input type="radio"/> 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)
认证方式	<input type="radio"/> 新用户以IP地址作为用户名 <input type="radio"/> 新用户以MAC地址作为用户名 <input type="radio"/> 新用户以主机名作为用户名 <input type="radio"/> 新用户以 VLAN ID 作为用户名 <input type="radio"/> 新用户以 SSO获取值作为用户名 <input checked="" type="radio"/> 到服务器去认证 首选认证服务器: 本地服务器 备份认证服务器1: 无 备份认证服务器2: 无
radius 计费服务器	无
自动添加到组织结构	<input checked="" type="checkbox"/> 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: Root 选择 自动绑定: <input checked="" type="radio"/> 无绑定 <input type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input type="radio"/> 同时绑定IP和MAC
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

第二步：在【组织管理>临时账号设置>基本配置】页面，选择开启临时账号开关，[账密派送模式]选择[寄帐密至申请者邮箱]，如下图：

临时账号开关	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
帐密邮箱域名	格式范例: hotmail.com 或为空 (为空时, 申请者邮箱域名将不被限定)
审核类型	<input type="radio"/> 手动审核 <input checked="" type="radio"/> 自动审核
所属组	Root 选择
帐密派送模式	<input type="radio"/> 页面显示帐密 <input checked="" type="radio"/> 寄帐密至申请者邮箱 <input type="radio"/> 通过短信发送密码 <input type="radio"/> 页面显示二维码与帐密
有效时间	<input checked="" type="radio"/> 在 2014-09-05 之间有效(格式: yyyy-mm-dd) <input type="radio"/> 在 小时之内有效 (用户登录后) <input type="radio"/> 用户申请结束时间

第三步：访问网络，出现 Portal 认证窗口，进入【用户认证】页面，如下图：



图175. 新增临时用户的认证策略

第二、点击【申请临时账号】按钮，开始申请临时帐户，如下图：



图176. 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。

14.5.3 申请临时账户的步骤（短信获取密码）

第一步：在【行为管理>认证策略】页面配置一条策略，[认证方式]选择[到服务器去认证]，[首选认证服务器]为[本地服务器]。如下图：

新增认证策略		确定	返回
名称	认证策略		
IP地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 <input type="radio"/> 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)		
认证方式	<input type="radio"/> 新用户以IP地址作为用户名 <input type="radio"/> 新用户以MAC地址作为用户名 <input type="radio"/> 新用户以主机名作为用户名 <input type="radio"/> 新用户以 VLAN ID 作为用户名 <input type="radio"/> 新用户以 SSO获取值作为用户名 <input checked="" type="radio"/> 到服务器去认证 首选认证服务器 本地服务器 备份认证服务器1 无 备份认证服务器2 无		
radius 计费服务器	无		
自动添加到组织结构	<input checked="" type="checkbox"/> 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 Root 选择 自动绑定: <input checked="" type="radio"/> 无绑定 <input type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input type="radio"/> 同时绑定IP和MAC		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		

第二步：在【组织管理>临时账号设置】页面，[临时账号开关]选择[开启临时账号]，[账密派送模式]选择[通过短信发送密码]，如下图：

菜单导航	
▶ 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	
▶ 组织结构	
▶ 批量导入	
▶ LDAP/AD导入	
▶ 扫描内网主机	
□ 临时账号设置	
▶ 基本配置	
▶ 未审核账户	
▶ 已审核账户	

单个临时账号 批量临时账号		确定
临时账号开关	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
帐密邮箱域名	格式范例: hotmail.com 或为空 (为空时, 申请者邮箱域名将不被限定)	
审核类型	<input type="radio"/> 手动审核 <input checked="" type="radio"/> 自动审核	
所属组	Root 选择	
帐密派送模式	<input type="radio"/> 页面显示帐密 <input type="radio"/> 寄帐密至申请者邮箱 <input checked="" type="radio"/> 通过短信发送密码 <input type="radio"/> 页面显示二维码与帐密	
有效时间	<input checked="" type="radio"/> 在 2014-09-05 之间有效(格式: yyyy-mm-dd) <input type="radio"/> 在 小时之内有效 (用户登录后) <input type="radio"/> 用户申请结束时间	

第三步：访问网络，出现 Portal 认证窗口，进入【用户认证】页面，如下图：



The image shows a 'User Authentication' (用户认证) interface. It features a blue header with the title '用户认证'. Below the header, there are two input fields: '用户名' (Username) and '密码' (Password), both highlighted in yellow. To the right of the password field is a blue link labeled '短信申请密码' (SMS Apply Password). At the bottom center, there is a blue button labeled '登录' (Login).

点击上图的【短信申请密码】按钮，开始申请临时帐户，如下图：



The image shows a 'Temporary Account Application' (临时账号申请) interface. It has a blue header with the title '临时账号申请'. Below the header, there is a '联系电话' (Contact Phone) field containing the number '139012345678'. At the bottom, there are three blue buttons: '确定' (Confirm), '清空' (Clear), and '返回' (Return).

点击【确定】即可收到短信，短信内容为密码，用户名为申请人的手机号。**注意：申请人不能手动修改密码，若需修改密码，必须让管理员修改。**

第四步：再次访问网络，出现 Portal 认证页面，可用此手机号码及密码进行用户认证。

14.5.4 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：【组织管理】>【临时账号设置】>【未审核账户】

配置描述：进入【未审核账户列表】配置页面，如下图：

申请账户列表						清空
申请人	申请时间	用途	联系电话	联络email	上网所在位置	核定类型
张三	2011-04-02 16:27:21	上网发送Email	13012345678	zhangsan@163.com	深圳	手动

图177. 未审核账户列表

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178. 手动审核临时账户

14.5.5 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【已审核账户列表】配置页面，如下图：

已审批账户列表										清空
申请人	申请时间	用途	联络电话	联络email	上网所在位置	核定类型	密码	核定时间	操作	
sss	2012-05-03 10:31:33			331565760@qq.com		自动	vbwppx	2012-05-03 10:31:33	删除	
aaa	2012-05-03 10:33:56			331565760@qq.com		自动	ohzoeg	2012-05-03 10:33:56	删除	
www	2012-05-03 10:07:50			331565760@qq.com		手动	ayuggn	2012-08-22 17:28:56	删除	
qq	2012-08-30 15:16:44	ww				自动	arkusi	2012-08-30 15:16:44	删除	
aaa	2012-08-30 15:17:13			222222@qq.com		自动	gpxmdz	2012-08-30 15:17:13	删除	

图179. 已审核临时账户列表

按钮说明：

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

14.5.6 批量生成

功能描述：批量生成临时账号。

配置路径：【组织管理】>【临时账号设置】>【批量生成】

配置描述：

批量生成		确定
帐号名		
产生数量		(1-50000)
使用时数		(1-500)
所属组		选择
管理员邮箱		(请在 [系统配置>邮件配] 页面启用 [邮件配置] 功能)

参数说明:

- 帐号名: 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。

14.6 Dkey管理

免审计 Key (DKey): 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: 配置免审计 Key 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:

新增 key		确定	返回
名称	Susan		
初始密码	●●●●●	下载 DKey 驱动	
绑定 IP/MAC	<input checked="" type="checkbox"/> 绑定IP <input checked="" type="checkbox"/> 绑定MAC		
IP/MAC	192.168.8.9 192.168.9.5 00:23:8C:51:43:12 清空列表	一行一个对象, 格式范例: 192.168.1.3 192.168.2.5 00:24:8C:51:24:22	
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。			
提示: 请先插入 DKey, 并确认已安装 DKey 驱动			

图180. 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：

DKey 管理				新增	删除所有
序号	名称	生成时间	操作		
1	abc	2012-09-08 10:30:41	写入key	修改	删除
2	debug	2012-09-08 14:20:33	写入key	修改	删除
3	test	2012-09-10 10:11:01	写入key	修改	删除

图181. Dkey 管理

15 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。

15.1 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：

线路带宽配置				确定
名称	上行带宽(Kbps)	下行带宽(Kbps)	描述	
WAN1	10240	10240	根据WAN1连接的线路的带宽值来配置	
WAN2	1000000	1000000	根据WAN2连接的线路的带宽值来配置	
WAN3	1000000	1000000	根据WAN3连接的线路的带宽值来配置	

图182. 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

WAN3: WAN3 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。

15.2 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。

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:

策略流控规则										新增通道	修改状态	删除所有	计数清零
规则名称	内网地址	外网地址	服务/URL	带宽(Kbps)	生效时间	生效线路	匹配计数	状态	操作				
WAN1-First	全部	全部	所有	最大: ↑10240, ↓10240 保障: ↑10240, ↓10240	全天	WAN1	0	<input checked="" type="checkbox"/>	新增子通道 修改 插入 移动 删除				
1-1	全部	全部	HTTP应用 全部	最大: ↑2560, ↓2560 保障: ↑2048, ↓2048	全天	WAN1	0	<input checked="" type="checkbox"/>	新增子通道 修改 插入 移动 删除				
1-2	全部	全部	所有	最大: ↑10240, ↓10240 保障: ↑10240, ↓10240	全天	WAN1	0	<input checked="" type="checkbox"/>	新增子通道 修改 插入 移动 删除				
WAN2-First	全部	全部	所有	最大: ↑10240, ↓10240 保障: ↑10240, ↓10240	全天	WAN1	0	<input checked="" type="checkbox"/>	新增子通道 修改 插入 移动 删除				
2-1	全部	全部	常用服务 全部	最大: ↑1024, ↓1024 保障: ↑1024, ↓1024	全天	WAN1	0	<input checked="" type="checkbox"/>	新增子通道 修改 插入 移动 删除				
2-2	全部	全部	所有	最大: ↑10240, ↓10240 保障: ↑10240, ↓10240	全天	WAN1	0	<input checked="" type="checkbox"/>	新增子通道 修改 插入 移动 删除				

提示: 不同线路的通道策略互相独立, 没有优先顺序。同一线路的同级通道策略, 按从前往后的顺序匹配, 可通过<插入>或<移动>来改变策略的先后顺序。匹配到父通道策略之后, 再进一步匹配子通道策略。

图183. 策略流控

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：

新增一级通道		确定	返回
规则名称	<input type="text" value="aaa"/>		
生效线路	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2		
内网地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 <input type="radio"/> 用户及用户组 <input type="text" value="全部"/> (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)		
外网地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 <input type="text" value="全部"/> (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)		
服务/URL/文件类型	<input checked="" type="radio"/> 所有服务 <input type="radio"/> 自选服务 <input type="radio"/> URL <input type="radio"/> 文件类型 (如要控制一种或多种服务, 请选择<自选服务>, 然后点击<选择服务>按钮进行服务的选择)		
流控行为	<input checked="" type="radio"/> 保障通道 <input type="radio"/> 限制通道 <input type="radio"/> 阻断流量		
优先级	高 <input type="button" value="v"/> (优先级较高的报文优先传送)		
保障带宽	上行:	<input type="text" value="1300"/> (Kbps)	<input type="text" value="100"/> %
	下行:	<input type="text" value="20000"/> (Kbps)	<input type="text" value="100"/> %
(带宽空闲时,其它规则流量可借用当前空闲带宽,百分比为占用本线路带宽值的比例)			
最大带宽	上行:	<input type="text" value="1300"/> (Kbps)	<input type="text" value="100"/> %
	下行:	<input type="text" value="20000"/> (Kbps)	<input type="text" value="100"/> %
(本规则流量能使用的最大带宽,百分比为占用本线路带宽值的比例)			
生效时间	<input type="text" value="全天"/> <input type="button" value="v"/>		
阻断记录	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用 (只对流控行为是阻断流量时生效)		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
快速链接 [地址簿] [自定义URL库] [生效时间]			

图184. 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。新增一级通道时，生效线路可以选择。修改一级通道、新增或修改子通道时，生效线路不可以选择。
- 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（在多条通道下有效）。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/URL/文件类型：
 - ◇ 默认选择“所有服务”，如需控制一种或多种服务，请选择<自选服务>，然后点击<选择服务>按钮，出现以下配置页面：

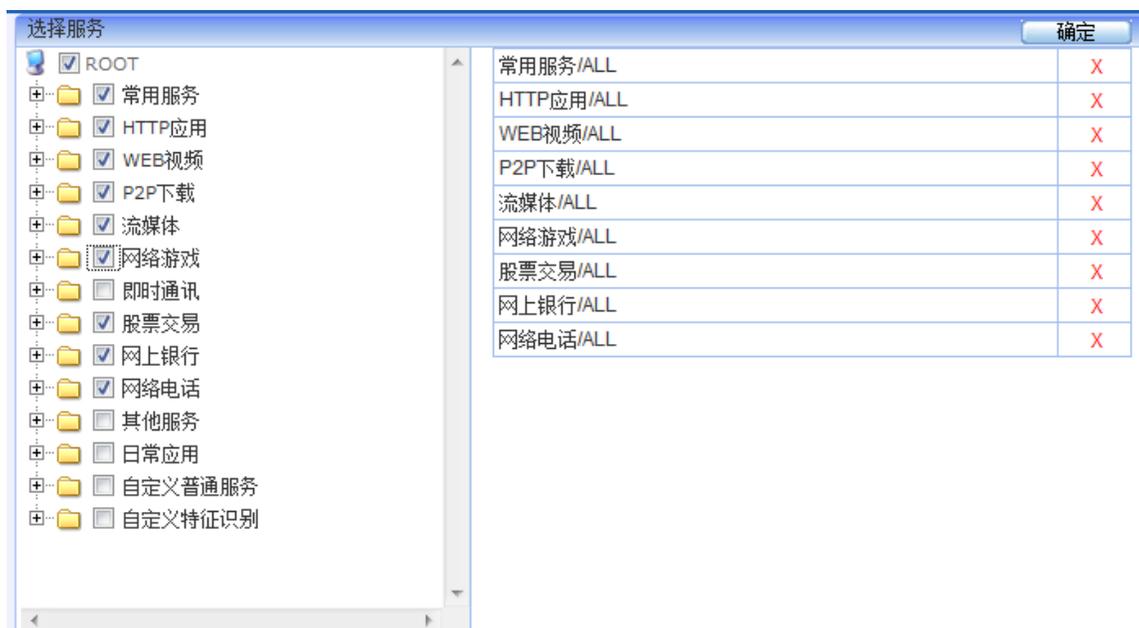


图185. 自选服务配置页面

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，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，继续配置其他项。

- ◇ 若需基[URL]做流控，请选择<URL>，再点击<选择URL>按钮，进行 URL 的配置。其他操作与基于应用的流控一样。
- ◇ 若需基于[文件类型]做流控，请选择<文件类型>，再点击<选择文件类型>按钮，进行文件类型的配置。其他操作与基于应用的流控一样。

提示：

- 1、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。
- 2、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。
- 3、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。
- 4、不同线路的通道策略互相独立，没有优先顺序。同一线路的同级通道策略，按从前往后的顺序匹配，可通过<插入>或<移动>来改变策略的先后顺序。匹配到父通道策略之后，再进一步匹配子通道策略。

15.3 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

前向后匹配，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186. 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187. 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:

Neusoft® 当前管理员: admin 系统时间: 2014-09-04 15:33:00 登录时间: 2014-09-04 14:41:54 刷新 保存 注销

菜单导航

- 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
 - 线路带宽配置
 - 基于策略的流控
 - 基于用户的流控
- 行为管理
- 酒店管理
- VPN配置

新增用户流控规则

规则名称:

地址: IP 地址簿 用户及用户组 全部
(格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)

最大上行带宽(Kbps): 不限制 (限制单个用户的上行总带宽, 包括<带宽细分配>里配置的带宽值)

最大下行带宽(Kbps): 不限制 (限制单个用户的下行总带宽, 包括<带宽细分配>里配置的带宽值)

启用 禁用
(可对单个用户的某些特定服务进行细化的带宽控制, 最多可以配置三组)

序号	选择服务	服务	最大带宽(Kbps)	最大下行带宽(Kbps)
1	选择服务		不限制	不限制
2	选择服务		不限制	不限制
3	选择服务		不限制	不限制

最大上行会话数: 不限制 (限制单个用户的最大上行会话数)

最大下行会话数: 不限制 (限制单个用户的最大下行会话数)

生效时间: 全天

状态: 启用 禁用

快速链接: [地址簿] [生效时间]

确定 返回

图188. 带宽细分配

点击<清楚>按钮, 删除本组服务与带宽的配置, 恢复到“未配置”状态。

点击<选择服务>按钮, 进入服务与带宽配置页面, 如下图:

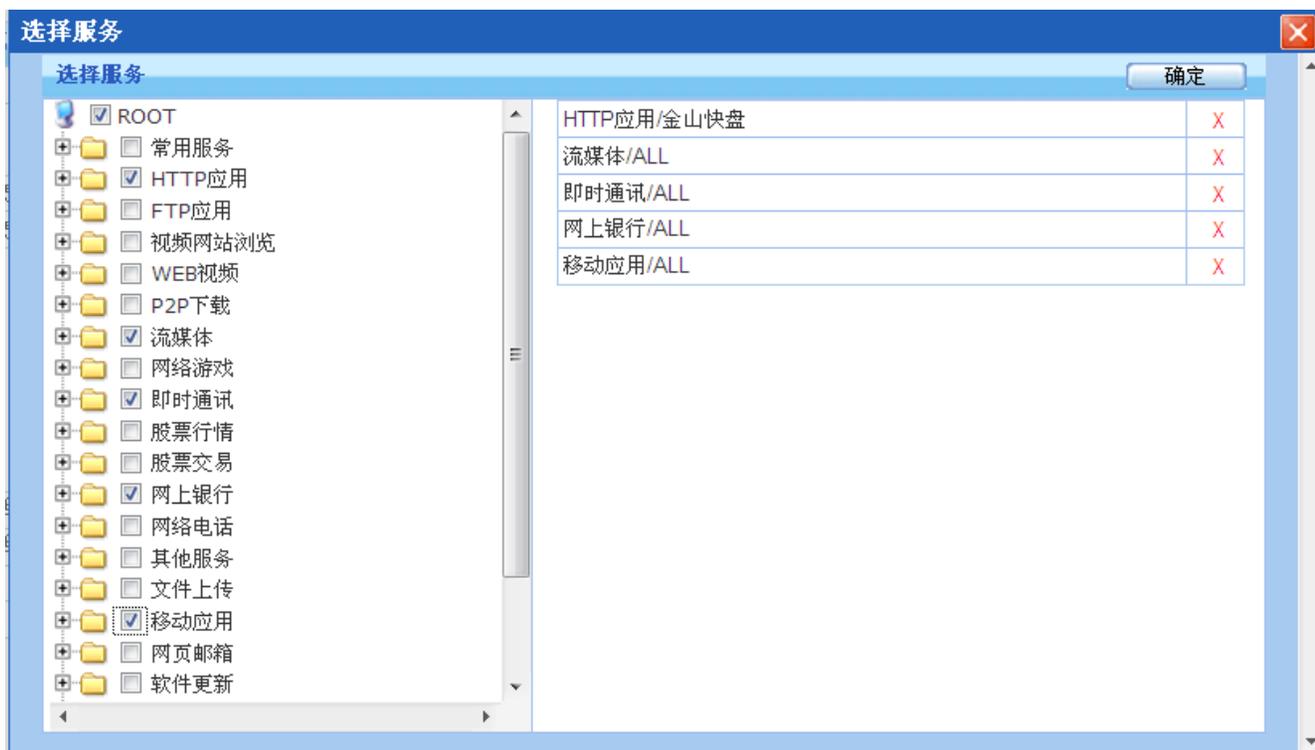


图189. 带宽细分配

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。

16 行为管理

“行为管理”包括认证策略、上网策略、认证选项、认证服务器、白名单管理等六部分。

16.1 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190. 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：

新增认证策略		确定	返回
名称	财务部		
IP地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 192.16.5.0/24 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)		
认证方式	<input checked="" type="radio"/> 新用户以IP地址作为用户名 <input type="radio"/> 新用户以MAC地址作为用户名 <input type="radio"/> 新用户以主机名作为用户名 <input type="radio"/> 新用户以 VLAN ID 作为用户名 <input type="radio"/> 到服务器去认证		
radius 计费服务器	无		
自动添加到组织结构	<input checked="" type="checkbox"/> 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 Root财务部 选择 自动绑定: <input checked="" type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input type="radio"/> 同时绑定IP和MAC		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		

图191. 新增认证策略 1

新增认证策略		确定	返回
名称			
IP地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)		
认证方式	<input type="radio"/> 新用户以IP地址作为用户名 <input type="radio"/> 新用户以MAC地址作为用户名 <input type="radio"/> 新用户以主机名作为用户名 <input type="radio"/> 新用户以 VLAN ID 作为用户名 <input type="radio"/> 新用户以 SSO获取值作为用户名 <input type="radio"/> 短信认证 <input checked="" type="radio"/> 到服务器去认证 首选认证服务器 本地服务器 备份认证服务器1 无 备份认证服务器2 无		
radius 计费服务器	无		
自动添加到组织结构	<input checked="" type="checkbox"/> 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 Root 选择 自动绑定: <input checked="" type="radio"/> 无绑定 <input type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input type="radio"/> 同时绑定IP和MAC		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
快速链接 [地址簿] [RADIUS服务器] [LDAP服务器] [POP3服务器] [AD服务器]			

图192. 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

动以用户的主机名作为用户名。

- ◇ 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。
 - ◇ 新用户以SSO获取值作为用户名：内网用户需要密码认证，并且需要开启单点登录，并且当该用户不在组织结构中时，以从单点登录获取到的帐号作用用户名。
 - ◇ 短信认证：内网需要密码认证，以手机号作为用户名申请密码，设备发送验证码至用户手机。并且当该用户不在组织结构中时，以手机号作为用户名。
 - ◇ 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”。
 - ◇ 新用户以SSO获取值作为用户名：可以选择为“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“无绑定”。
 - ◇ 短信认证：可以选择为“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“无绑定”。
 - ◇ 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。

16.2 上网策略

[上网策略]用于设置内网用户的上网策略，管理员可以根据内网用户的权限分配情况，设置不同的上网策略。上网策略分六种类型，其中包括[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]。

16.2.1 上网权限策略

上网权限策略包括：[URL 过滤](#)、[关键字过滤](#)、[文件传输过滤](#)、[SSL 管理](#)、[其它类](#)。每个策略对象可以同时设置这五部分的内容。

配置路径：【行为管理】>【上网策略】>【上网权限策略】

某条上网权限策略规则可同时被多个用户组/用户引用，从而对内网用户进行上网行为的控制。



图193. 上网权限策略

点击<删除所有>，删除所有的上网权限策略。

点击<删除>，删除某条上网权限策略。

点击<修改>，修改本条上网权限策略。

点击<修改>，修改本条上网权限策略。

点击<插入>，在当前位置插入一条上网权限策略。

点击<移动>，改变上网权限策略的序号。

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。

16.2.1.1 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，增加上网策略对象。

第二：选择“URL 过滤>内置 URL 库”。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194. 新增上网权限策略-内置 URL 库过滤

第三：选择“URL 过滤>自定义 URL 库”选项卡，配置方法与“内置 URL 库”相同。界面如下图：



图195. 新增上网权限策略-自定义 URL 库过滤

“自定义 URL 库”需要先定义 URL 库，详见【[系统对象>URL 库](#)】的配置。

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。

第四：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。如下图所示：

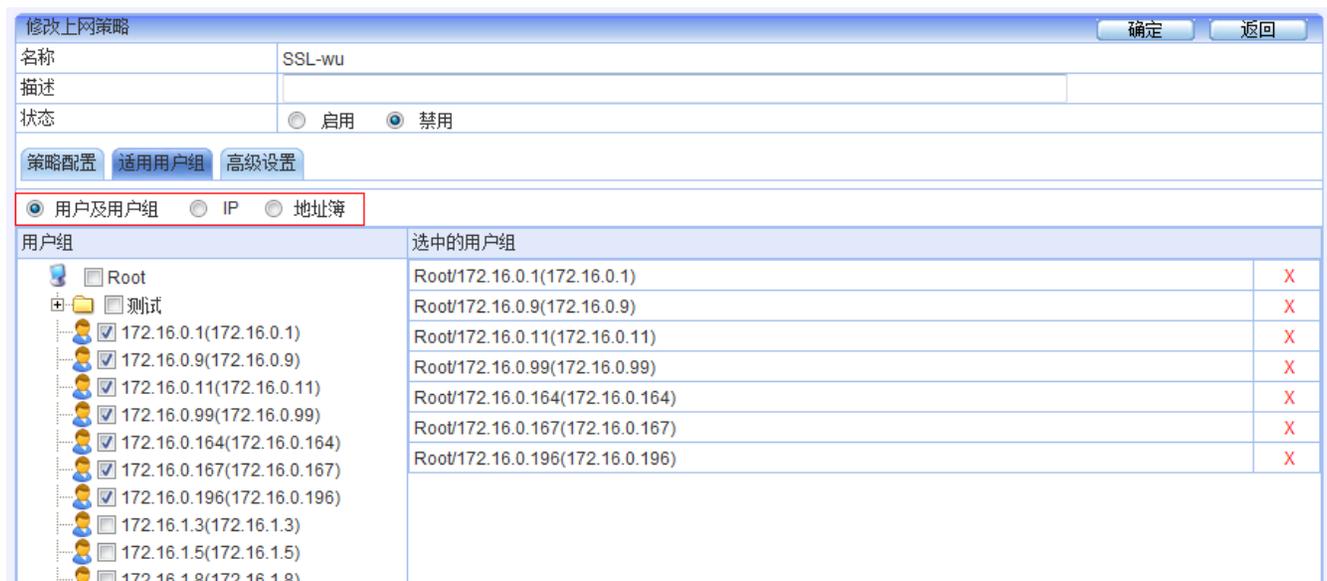


图196. 新增上网权限策略-适用用户组

参数说明： [适用用户组]可以是组织结构中的[用户及用户组]，也可以是单个 IP 或 IP 段；或者是定义好的[地址簿]。

第五： 在[高级设置]选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。如下图所示：



图197. 新增上网权限策略-高级设置

参数说明： 同级别管理员可以选择[允许查看]和[允许编辑]。此处的“同级别管理员”指的是在【系统配置>系统管理员】中属于同一角色的管理员，如果勾选[允许查看]，则同级别管理员可以查看此策略，而不能进行修改。如果勾选[允许编辑]，则同级别管理员默认拥有[允许查看]权限，并且可以对此策略进行修改。

16.2.1.2 关键字过滤

功能描述： ① 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 对通过HTTP协议上传的关键字进行过滤。③ 对网页内容中包含的关键字进行过滤。

配置路径： 【行为管理】>【上网策略对象】

配置描述： 【行为管理】>【上网策略】>【上网权限策略】

第一： 进入【上网权限策略】页面，点击<新增>按钮，增加上网权限策略。或者继续前面新增的策略对象的基础上配置关键字过滤。

第二： 勾选“关键字过滤>搜索引擎”选项。而后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198. 上网权限策略-关键字过滤

〈HTTP 上传〉、〈网页内容〉选项，配置方法与〈搜索引擎〉相同。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

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向后匹配的原则，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。

16.2.1.3 文件传输过滤

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

配置路径：【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，增加上网权限策略。或者继续前面新增的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。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199. 上网策略对象-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。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

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。

16.2.1.4 邮件过滤

功能描述：用于对内网用户使用邮件客户端(SMTP/WEBMail)协议发送邮件或者使用邮件客户端(POP3/WEBMail)协议接受邮件时，对发送或接收的邮件地址、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：

第一：进入【上网权限策略】页面，点击<新增>按钮，增加上网权限策略。或者继续前面新增的策略对象的基础上配置邮件过滤。

第二：选择“发送邮件过滤”选项卡，配置过滤条件。如下图：

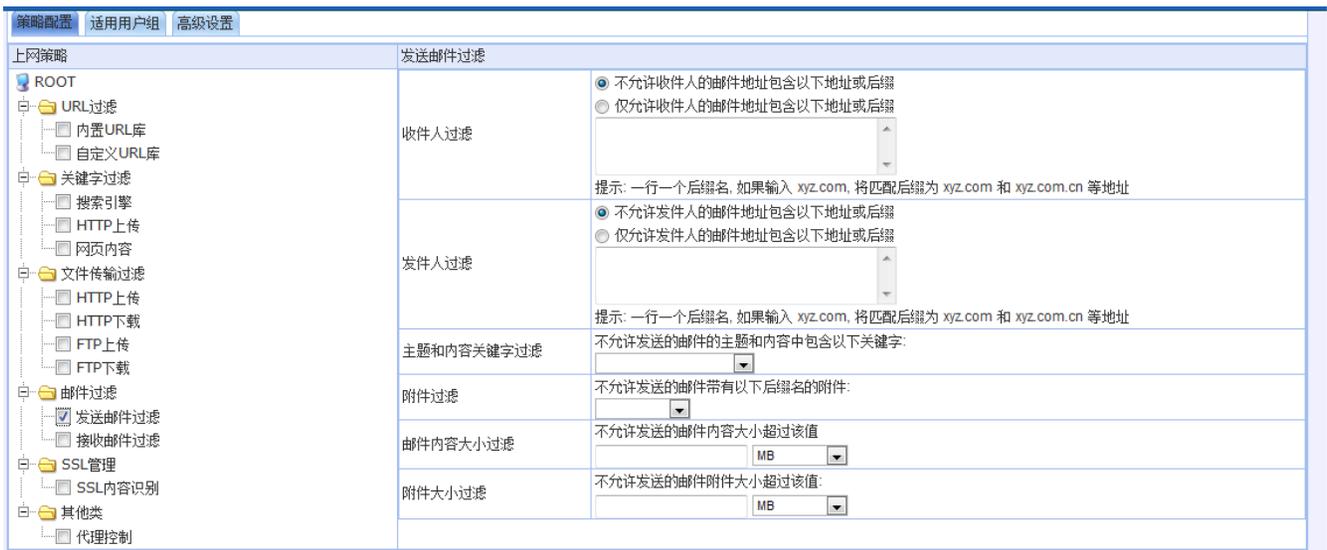


图200. 上网权限策略-发送邮件过滤

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>，在后面的文本框中输入“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>，在后面的文本框中输入“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。

第三：选择“接收邮件过滤”选项卡，配置过滤条件。如下图：



图201. 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>，在后面的文本框中输入“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>，在后面的文本框中输入“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。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

提示：

- 1、如某个过滤条件未配置任何值，则不检查此项内容。
- 2、<收件人过滤>、<发件人过滤>、<主题和内容关键字过滤>、<附件过滤>、<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。

16.2.1.5 SSL管理

功能描述： 针对加密的web应用内容以及加密的邮件进行识别和控制。

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，增加上网策略对象。或者继续前面新增的策略对象的基础上配置邮件过滤。

第二： 选择“SSL 内容识别”选项卡，配置界面如下图：



图202. 新增上网权限策略-SSL 内容识别

参数说明：

- 加密 web 应用内容识别： 主要对加密的 web 页面进行识别。比如对 https://www.google.com.hk 等加密 web 页面的审计。
- 加密邮件内容识别： 主要对加密邮件的内容进行识别和审计。如 gmail 邮箱的审计。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

16.2.1.6 其它类

功能描述： 包括是否允许HTTP代理、SOCK代理的选项等。您可以通过这些选项，来设置内网用户是否可以使用HTTP代理、SOCK代理等。选项[不允许在HTTP，SSL协议的标准端口上使用其它协议]用于防止一些应用程序使用标准的HTTP端口（TCP 80）和SSL端口（TCP 443）来传输自己的数据，从而逃避设备的限制。

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，增加上网权限策略。或者继续前面新增的策略对象的基础上配置邮件过滤。

第二： 选择“代理控制”选项，选择代理控制的选项。配置界面如下图：



图203. 新增上网权限策略-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（TCP 80、TCP 443）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]。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

16.2.2 终端提醒策略

功能描述：用于定期向内网用户弹出指定的页面。

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，如下图所示：



图204. 终端提醒策略

点击<删除所有>，删除所有的终端提醒策略。

点击<删除>，删除本条终端提醒策略。

点击<修改>，修改本条终端提醒策略。

点击<插入>，在当前位置插入一条终端提醒策略。

点击<移动>，改变终端提醒策略的序号。

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

第二：点击<新增>按钮,新增一条终端提醒策略,如下图所示:

图205. 新增终端提醒策略

参数说明:

- 规则名称: 定义该条终端提醒策略的名称。
- 规则描述: 可对该条终端提醒策略进行一个简单的描述。
- 生效时间: 该条终端提醒策略的生效时间。
- 状态: [启用]或[禁用]该条终端提醒策略。
- 终端提醒策略: 终端提醒策略包含两种: [公告页面]和[URL 重定向]。
 - 公告页面: 通过定期把 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。如下图所示:

图206. 新增终端提醒策略—公告页面

参数说明:

- ◆ 每隔__（1-1440）分钟，重定向到公告页面：可自定义。
- ◆ 每访问_次网站，重定向到公告页面：每访问超过定义的次数的网站，就会重定向至公告页面。
- ◆ 在__（1-1440）分钟，访问_次网站，重定向到公告页面：在定义的时间范围内（最大是1440分钟），访问定义的网站次数后就会重定向至公告页面。
- ◆ 公告页面选择：公告页面可以是“设备内置的公告页面”，在行为管理—认证选项—自定义认证页面的公告页面中可以编辑自定义内容。也可以选择“外部的公告页面”，将外部公告页面的URL输入进去。

- URL 重定向：浏览某个网址时，将其重定向至另一个网址。如下图所示：



图207. 新增终端提醒策略—URL 重定向

参数说明:

- ◆ URL 源地址：填入需要进行重定向的源地址，一行一个 URL 关键字或 URL 全名。
- ◆ 开启精确匹配模式：如果勾选“开启精确匹配模式”，则只有在与URL源地址完全相同的情况下才会进行重定向。
- ◆ 被重定向为：填入被重定向后的URL地址。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

16.2.3 准入策略

功能描述：对内网电脑运行的进程进行检测，并限制进程的运行状态。检测的内容包括操作系统、进程、文件、注册表等。

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，如下图所示：



序号	名称	内部地址	生效时间	管理员	角色	状态	操作
1	fff	用户及用户组:	全天	admin	超级管理员	<input checked="" type="checkbox"/>	修改 插入 移动 删除

图208. 新增准入策略

点击<删除所有>，删除所有的准入策略。

点击<删除>，删除本条准入策略。

点击<修改>，修改本条准入策略。

点击<插入>，在当前位置插入一条准入策略。

点击<移动>，改变准入策略的序号。

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

16.2.3.1 操作系统规则

功能描述：可对操作系统进行检测，并进行控制。

配置路径：【行为管理】>【上网策略】>【准入策略】

配置描述：

第一：点击<新增>按钮，新增一条准入策略，[规则类型]选择“操作系统类型”，配置界面如下图：



图209. 新增准入规则—操作系统规则

参数说明：

- 规则名称：定义该条准入策略的名称。
- 规则描述：可对该条准入策略进行一个简单的描述。
- 状态： [启用]或[禁用]该条准入策略。
- 系统版本：可勾选“window xp”、“window 2003”、“windows Vista”、“windows 2008”、“” window 7”、“windows 2008R2”、“windows 8”、“windows 2012”中的一种或多种。
- 违规操作：可以选择设备对不符合规则的用户的操作，可以选[禁止用户上网]或者[不操作]（不操作是指对客户端数据不采用任何操作，此时会在数据中心记录日志）。
- 生效时间：选择准入策略的生效时间。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

16.2.3.2 进程规则

功能描述：可对用户进程进行检测，并进行控制。

配置路径：【行为管理】>【上网策略】>【准入策略】

配置描述：

第一：点击<新增>按钮，新增一条准入策略，[规则类型]选择“进程规则”，配置界面如下图：

策略配置		适用用户组	高级设置
规则类型	进程规则		
进程状态	正在运行		
违规操作	禁止用户上网		
进程名称	a.exe		
程序路径	c:\windows\la.exe		
生效时间	全天		

图210. 新增准入策略—进程规则

参数说明：

- 进程状态：可选择“正在运行”和“没有运行”。
- 违规操作：当检测到用户的电脑上对应的进程符合配置的[进程状态]时，采取的动作，包含[禁止用户上网]、[禁止进程]和[不操作]三种。
- 进程名称：填写需要进行控制的进程名称。
- 程序路径：填写进程对应的程序路径。
- 生效时间：准入策略生效的时间。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

16.2.3.3 文件规则

功能描述：可对用户文件进行检测，并进行控制。

配置路径：【行为管理】>【上网策略】>【准入策略】

配置描述：

第一：点击<新增>按钮，新增一条准入策略，[规则类型]选择“文件规则”，配置界面如下图：

策略配置		适用用户组	高级设置
规则类型	文件规则		
文件状态	存在		
违规操作	禁止用户上网		
文件路径			
生效时间	全天		

图211. 新增准入策略—文件规则

参数说明：

- 文件状态：可选择“存在”或“不存在”。
- 违规操作：在[文件状态]选择“文件存在”时，[规则操作]可以选择[禁止用户上网]、[删除文件]或[不操作]；在[文件状态]选择“文件不存在”时，[规则操作]可以选择[禁止用户上网]或[不操作]。
- 文件路径：填写需要进行控制的文件路径。

➤ 生效时间：准入策略的生效时间。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

16.2.3.4 注册表规则

功能描述：可对用户注册表进行检测，并进行控制。

配置路径：**【行为管理】>【上网策略】>【准入策略】**

配置描述：

第一：点击<新增>按钮，新增一条准入策略，[规则类型]选择“注册表规则”，配置界面如下图：

策略配置	适用用户组	高级设置
规则类型	注册表规则	
表项状态	注册表中含有	
违规操作	禁止用户上网	
注册表项		
表项名称		
表项数据		
生效时间	全天	

图212. 新增准入策略—注册表规则

参数说明：

- 表项状态：可选择“注册表中含有”或者“注册表中没有”。
- 违规操作：在[表项状态]选择“注册表中含有”时，[规则操作]可以选择[禁止用户上网]、[删除注册表项]或[不操作（仅提交报告）]；在[表项状态]选择“表项不存在”时，[规则操作]可以选择[禁止用户上网]、[添加注册表项]或[不操作（仅提交报告）]。
- 注册表项：填写要控制的注册表项。
- 表项名称：填写要控制的注册表项的名称。
- 表项数据：填写要控制的注册表项的数据。
- 生效时间：准入规则的生效时间。

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

16.2.4 应用限额策略

功能描述：限制具体应用能使用多少流量或多少时长。

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】界面，如图：



图213. 应用限额策略

点击<删除所有>，删除所有的应用限额策略。

点击<删除>，删除本条应用限额策略。

点击<修改>，修改本条应用限额策略。

点击<插入>，在当前位置插入一条应用限额策略。

点击<移动>，改变应用限额策略的序号。

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

第二：点击<新增>按钮，新增一条<应用限额策略>，如下图所示：



图214. 新增应用限额策略

参数说明：

- 名称：定义该条应用限额策略的名称。
- 状态：应用限额策略的状态，可选择[启用]或[禁用]。
- 每日限额：当天可供规则内应用占用的带宽总量或使用时长。有“时长”和“流量”两种选择。
- 生效时间：应用限额的生效时间。下拉框内容为事先定义好的“时间计划”名称
- 服务：可选择在[系统对象—网络服务—内置服务]中的服务。如下图所示：

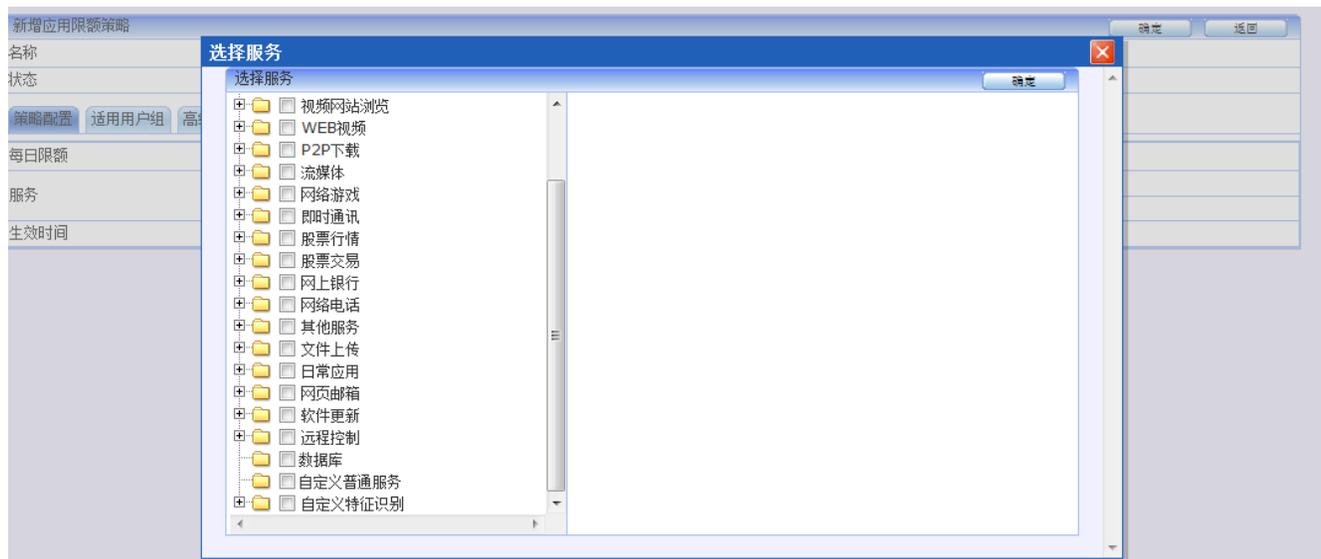


图215. 新增应用限额策略—选择服务

第三：策略设置完成后，在[适用用户组]选项卡需要设置被控制的组/用户才会生效。

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

16.2.5 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，以示惩罚。

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【黑名单规则】配置页面，如下图：



图216. 黑名单策略

点击<删除所有>，删除所有的应用限额策略。

点击<修改>，修改本条应用限额策略。

点击<插入>，在当前位置插入一条应用限额策略。

点击<移动>，改变应用限额策略的序号。

点击<删除>，删除本条应用限额策略。

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

第二： 点击<新增>按钮，增加黑名单规则，如下图：



图217. 新增黑名单规则

参数说明:

- 名称: 黑名单规则的名称。
- 状态: [启用]或[禁用]黑名单。
- 拒绝共享内部上网: 选择“启用”，则当内网有用户在共享上网的时候，会被加入黑名单。“共享单 ip 的终端数”的值表示允许该 ip 共享的终端数，默认是只允许 1 个终端。选择“禁用”则不会对共享用户进行控制。
- 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。
- 最大速率: 连续多少分钟内，速率超过一定阈值，上行速率和下行速率分开计算。
- 最大会话数: 连续多少分钟内，速率超过一定阈值，上行速率和下行速率分开计算。
- 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阈值后，将被加倍惩罚。比如，惩罚时间将变为原来的 3 倍。
- 生效时间: 在生效时间内才进行黑名单的控制；在生效时间外，不对用户的速率和会话进行限制，用户

产生的流量也不计入黑名单的流量配额内

第三：选择黑名单规则的[适用组和用户]，可输入“IP”，选择“用户”、“用户及用户组”或“地址簿”。如下图：

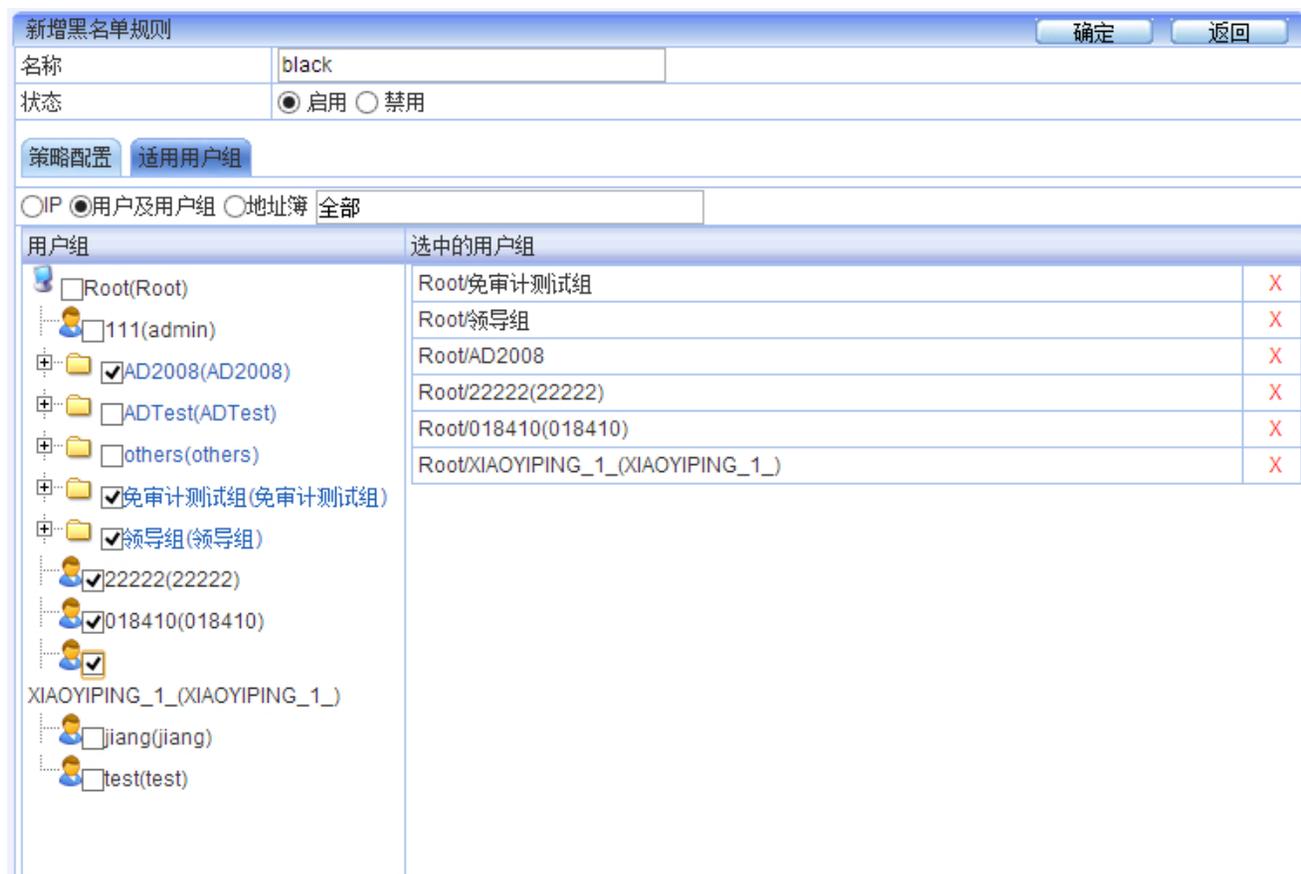


图218. 黑名单规则的适用用户组

第四：在高级设置选项卡中包含[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

提示：流量配额、最大速率、最大会话数里面的每个阈值是或的关系，只有一个值达到阈值，则都会进入黑名单。

16.2.6 上网审计策略

功能描述：过滤报表中心行为分析的记录内容，如：对某些用户只启用 URL 记录和 FTP 记录等。

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，如下图：



图219. 上网审计策略

第二：点击<新增>按钮，新增一条上网审计策略，如下图所示：



图220. 新增上网审计策略

参数说明：

- 即时通讯：可复选“登录信息”和“通讯内容”。“登录信息”记录即时通讯的登录信息。“通讯内容”记录聊天内容、文件传输、语音记录。
- 邮件记录：可复选“基本信息”、“邮件正文”和“邮件附件”。“基本信息”记录的信息包括：发件人、收件人、邮件主题、日期。“邮件正文”记录邮件的基本信息和邮件正文的内容。“邮件附件”记录邮件的基本信息和邮件附件，附件将保存到硬盘中，可以下载到本地。
- WEB记录：可复选“URL地址”、“网页标题”、“HTTP上传”、“搜索关键字”、“文件上传”、“网页登录”和“网页内容过滤”。“URL地址”记录URL的全址。“网页标题”记录WEB页面的标题。“HTTP上传”记录通过HTTP协议上传的内容。“搜索关键字”记录在搜索引擎上搜索的关键字。“文件上传”记录通过WEB上传的文件的记录。“网页登录”记录登录网页的信息。“网页内容过滤”记录
- FTP记录：启用FTP记录，可记录FTP的登录信息，上传下载文件信息。
- Telnet记录：启用Telnet记录，可以记录Telnet的登录信息，操作信息。

- 会话记录：记录会话信息。
- 告警记录：记录告警信息。可选择级别大于或等于某个级别的时候才会记录。其中级别有以下四种：普通状态、预警状态、严重状态、紧急状态。
- 状态：启用或禁用本规则，默认启用。

第三：选择[上网审计策略的]的[适用组和用户]，可输入“IP”，选择“用户”、“用户及用户组”或“地址簿”。如下图：

第三：进入“审计选项”页面，如下图所示：



图221. 审计选项

参数说明：

- 审计方式：可选择“全部审计”和“根据审计策略规则审计”。“全部审计”会对所有的上网行为进行审计。“根据审计策略审计”则会根据定义的审计规则进行审计。
- 会话审计方式：可选择“只审计有效会话”和“全部审计”。
- 文件大小上限：在邮件记录、网页附件上传等地方，设备记录并存储的文件的最大尺寸；大于设定值的附件将只记录文件名而不存储文件；默认 1M。
- 访问网站日志记录选项：包括“优化日志记录”、“仅记录含有网页标题的访问”、“仅记录到网站根目录的访问”、“记录所有网页访问”。默认选择“优化日志记录”。
 - 选择“优化日志记录”，会对所有的网页访问进行记录，但是会对内容日志进行优化。
 - 选择“仅记录含有网页标题的访问”，则会只记录含有网页标题的访问，其余的不记录。

- 选择“仅记录到网站根目录的访问”，则会只记录根目录的访问，子目录的不记录。
- 选择“记录所有网页访问”，则会记录所有的访问记录。

16.3 认证选项

认证选项包含 SNMP 设置、认证参数、自定义认证页面、未认证权限和 SSO 的配置。

16.3.1 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】>【跨三层 MAC 识别】，配置页面如下：

功能状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 (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	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 172.16.7.200/8C:89:A5:7D:E3:13/.1.3.6.1.2.1.4.22.1.2/public	
超时设置	1	(1-5秒)
访问间隔	5	(5-300秒, 访问SNMP服务器的时间间隔)

图222. SNMP 设置

参数说明：

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

提示:

- 1、如果启用“跨三层 MAC 识别”功能，三层交换机必须支持 SNMP 服务，且正确配置三层交换机的 Community 和 SNMP 版本（版本为 v2）
- 2、比如，在实例中内网有 3 台三层交换机，其中一台为核心交换机，另外两台分别为连接到核心交换机的三层交换机 A 和 B，A 和 B 分别连接到内网的两个部门。则三台交换机的 IP/MAC/Oid/Community 都必须填入到 SNMP 服务器列表中。核心交换机不要求一定能支持 SNMP，但是设置[SNMP 服务器列表]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。

16.3.2 认证参数

功能描述: 设置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:

用户认证参数		确定
用户语言	繁體中文	
认证方式	<input checked="" type="radio"/> http <input type="radio"/> https	
认证端口	80	(1-65535)
认证超时(分)	10	(0-100000,0表示不限制)
其他认证选项	<input type="checkbox"/> 每天强制注销所有用户	
认证页面欢迎栏		(默认为:用户身份认证系统)
公告信息		(字符长度不能超过512)
黑名单公告信息		
认证通过跳转	<input checked="" type="radio"/> 用户上网信息页面 <input type="radio"/> 最近请求页面 <input type="radio"/> 自定义页面	

图223. 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。
- 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。
- 黑名单公告信息：管理员可以设置一些信息公告给每个用户，将在用户进入黑名单时显示到客户端。
- 认证通过跳转：可选择认证通过后跳转的页面。选择“用户上网信息页面”则跳转至系统自带的用户上网认证页面；选择“最近请求页面”则跳转最近请求的页面。选择“自定义页面”则转至“自定义页面”。

16.3.3 自定义认证页面

功能描述：自定义认证界面的风格与参数

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224. 自定义认证页面

参数说明：

- 定制对象：可定制[WEB认证]、[认证成功]、[URL禁止访问]、[短信申请]、[准入策略]、[公告页面]、[短信认证]。
- 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。

按钮说明：

- 预览：可对定制页面进行预览。
- 恢复初始页面：对页面进行修改后，如果想要重新恢复初始页面，直接点击恢复初始页面即可。

16.3.4 未认证权限

配置路径：【行为管理】>【认证选项】>【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：

序号	规则名称	内部源地址	目的地址	服务/URL	生效时间	匹配计数	状态	操作
1	80	172.16.26.107	全部	80	全天	0	<input type="checkbox"/>	修改 插入 移动 删除

提示：序号越小的规则优先级越高，可通过<插入>或<移动>来改变规则的先后顺序。

图225. 未认证权限

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：

新增未认证权限规则

规则名称: GRE

内部源地址: IP 地址簿 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)

目的地址: IP 地址簿 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)

服务/URL: 服务 URL
GRE (当用户未通过认证时可以访问该服务)

生效时间: 全天

状态: 启用 禁用

快速链接: [地址簿] [生效时间] [服务]

图226. 新增策略

参数说明：

- 内部源地址：数据流的源地址（内网主机地址），可输入 IP 地址或选择地址簿。地址簿在【系统对象>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。

16.3.5 SSO

单点登录指如果组织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。

16.3.5.1 AD 单点登录

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

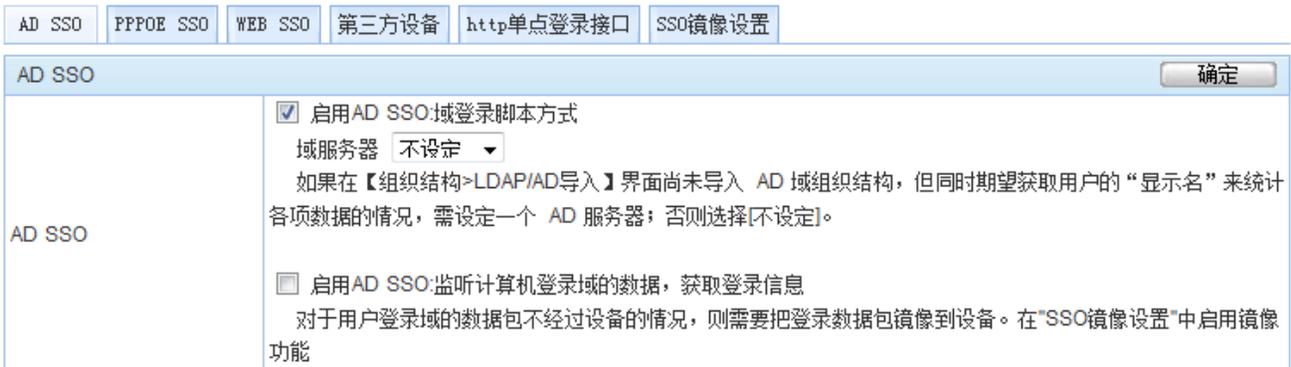


图227. AD SSO

参数说明：

- 启用 AD SSO 功能：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。
 - ✧ 域服务器[不设定/AD 域服务器名称]的作用：如果在**【组织结构>LDAP/AD导入】**界面尚未导入 AD 域组织结构，但同时期望在统计数据中以用户的“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 功能：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。

16.3.5.2 PPPOE 单点登录

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：



AD SSO	PPPOE SSO	WEB SSO	第三方设备SSO	http单点登录接口	SSO镜像设置
PPPOE SSO					确定
PPPOE SSO	<input checked="" type="checkbox"/>	启用			

PC 通过 PPPoE 服务器的认证后，即可通过设备认证上网。

16.3.5.3 WEB单点登录

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：



AD SSO	PPPOE SSO	WEB SSO	第三方设备SSO	http单点登录接口	SSO镜像设置
WEB SSO					确定
<input checked="" type="checkbox"/> 启用Web单点登录					
Web认证服务器地址	www.authserver.com	(例如: www.authserver.com)			
用户认证POST页面URL	/cgi-bin/auth.php	(例如: /cgi-bin/auth.php)			
用户账号提取正则表达式	(说明: 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)				
1	<input checked="" type="radio"/> 认证成功页面的URL(例如: /auth_ok.php)				
认证结果	<input type="radio"/> 认证成功结果中的关键字(认证请求和认证结果在同一个http连接中)				
	<input type="radio"/> 认证失败结果中的关键字(认证请求和认证结果在同一个http连接中)				
	auth_ok.php				
新增组					

配置步骤：

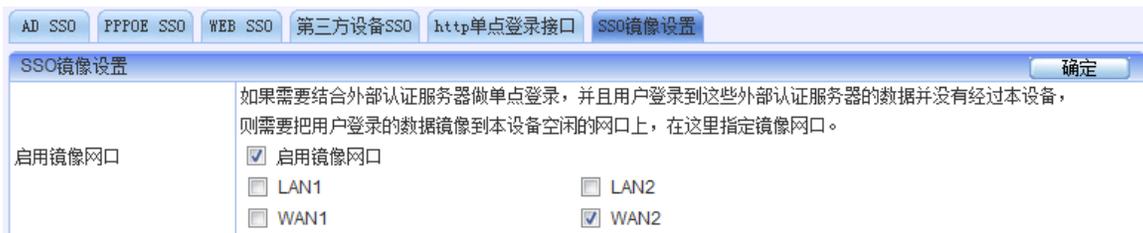
第一步：设置以下参数

- 启用WEB单点登录：启用或禁用 WEB 单点登录。

- **WEB 认证服务器地址：**填写 WEB 认证服务器地址。
- **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。

第二步：SSO 镜像设置

- 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。
- 如果 WEB 服务器在内外，即认证数据未经过本设备，则需要设置监听口。点[SSO镜像设置]，勾选[启用镜像网口]，选择监听口。并且在内部交换机上需要把 WEB 认证数据镜像到本设备。



第三步： PC 上网先登录设置的网站，如例子中的 BBS，登录成功后即可上网。

16.3.5.4 第三方设备单点登录

某些网络环境中已经存在其他的第三方认证系统做用户认证和组织结构的管理，此时设备能够跟这些第三方的认证系统结合使用，做单点登录。目前设备支持的其他第三方厂商的认证系统有城市热点和 H3C IMC 系统。

配置路径：【行为管理】>【认证选项】>【SSO】，选择 [WEB SSO]，启用[城市热点 SSO]或[H3C IMC SSO]。

如下：



16.3.5.4.1 城市热点 SSO说明

城市热点是一套认证计费管理系统，广泛应用于教育、电信、广电、政府等各个领域，不管城市热点使用的B/S认证还是C/S认证，本设备都能够与之结合进行用户认证。用户上网前必须通过城市热点系统的身份认证，用户通过城市热点系统的认证/注销后，自动在本设备上完成认证/注销。数据流的过程如下：

1. PC 通过城市热点认证服务器的认证/注销。
2. 城市热点认证服务器通知本设备认证/注销用户，实现单点登录和注销。

附录：城市热点 DrCOM SOLS 在线用户管理系统与第三方监控系统接口

一、接口描述

第三方监控系统接口使用 UDP 协议通信，接口分为：

- 用户信息同步接口：是将用户信息（主要是账号与 IP 的映射关系）发送给第三方监控系统；
- 第三方监控系统告警反馈接口：是将监视到的用户事件反馈给 SOLS 系统，由 SOLS 系统依据告警信息对用户进行管理；

二、接口内容

协议： UDP

监听端口： 5850

数据结构，Dr.COM 发送的用户信息数据：

序号	名称	类型	长度(字节)	取值范围	是否有数据
1	命令代码	int	4	0x00000000 发送用户上下线事件	有
2	子命令代码	int	4	暂时保留	有
3	发送的数据长度	int	4		有
4	事件发生时间	string	20	yyyy-mm-dd hh:MM:ss 有结束符'\0'	有

5	账号	string	32		暂无
6	真实姓名	string	32		暂无
7	证件类型	short	2		暂无
8	证件号码	string	20		暂无
9	居住、单位地址	string	32		暂无
10	国籍	string	12		暂无
11	备注	string	56		暂无
12	计费组 ID	unsigned short	2		有
13	带宽组 ID	unsigned short	2		有
14	行政组 ID	unsigned short	2		有
15	协议主版本号	unsigned short	2	0x0001	有
16	协议次版本号	unsigned short	2	0x0001	有
17	校验和	unsigned int	4	此值置为 0 后,所有数据 (包含命令代码)按照字节相加的和	有
18	事件类型	unsigned short	1	1=登陆, 2=注销	有
19	登录 IP 地址	unsigned int	4		有
20	登录 MAC 地址	unsigned char	6		有
21	备用	unsigned short	3		暂无

第三方监控系统接收用户信息的返回数据:

序号	名称	类型	长度 (字节)	取值范围
1	命令代码	int	4	成功: 0x8000000,

				失败(接收的数据格式不正确):0x8080000
2	子命令代码	int	4	暂时保留

三、重传机制

我方程序在发送失败或未接收到对方的响应，会重新发送，超过一定时间（可在配置文件中配置）仍然不能成功发送，就认为对方接口已经结束运行，不再重试发送，并定时发送一条在线事件检测对方接口是否恢复运行，对方接口恢复运行后，我方接口会重发所有在线用户信息给对方接口。

16.3.5.4.2 H3C IMC系统

H3C IMC 系统是一套认证管理系统，用户上网前必须通过 H3C IMC 系统的身份认证，用户通过 H3C IMC 系统的认证/注销后，自动在本设备上完成认证/注销。数据流的过程如下：

1. PC 通过 H3C IMC 系统认证服务器的认证/注销。
2. H3C IMC 系统通知本设备认证/注销用户，实现单点登录和注销。

附录：H3C IMC 使用说明

(一) 准备工作

安装 IMC 系统

- 1、iMC-PLAT-3.20-R2606L15 以上平台
- 2、iMC-UAM-3.60-E6301P04 以上平台

客户端

iNodeSetup3.60-6308.exe

(二) 配置信息

1、与本设备配置结合的配置信息

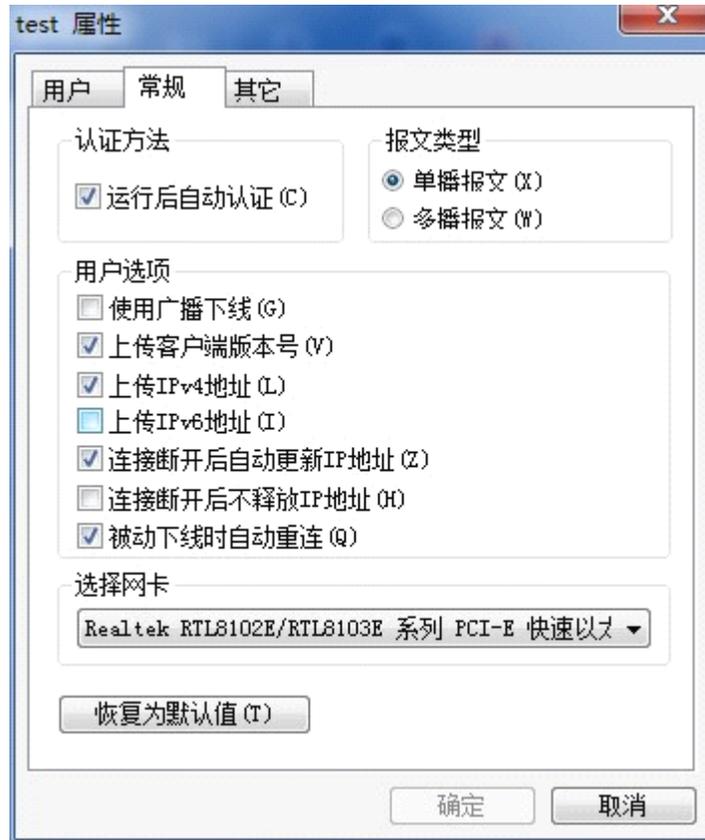
服务器 IP: 连接的本设备的 IP 地址;

服务器端口: 本设备开启的 UDP 端口 5850;

共享密钥: 暂可忽略不计, 无影响;

2、客户端配置

客户端 PC 安装 iNodeSetup3.60-6308.exe ，输入正确的用户名和密码后，需勾选：上传 IPv4 地址；



(三) 本设备单点登录实现原理：用户通过 H3C 的 IMC 系统认证后，IMC 系统向本设备发送一个 UDP 包（UDP 包，Radius 协议）；本设备通过 authd 创建一个线程进行监听，如果收到 IMC 上线通知包，解析出上线用户名和 IP，走单点登录流程，将用户添加到组织结构，然后上线；

用户在IMC 系统认证成功后，IMC 系统发送的上线通知包结构(使用Radius协议)：

code = 252 //上线通知报文号

属性：

1 号属性：用户登录名

2 号属性：用户姓名（iMC 上开户时输入的用户全名）

3 号属性：用户接入开始时间（上网开始时间）

8 号属性：认证用户 IP 地址

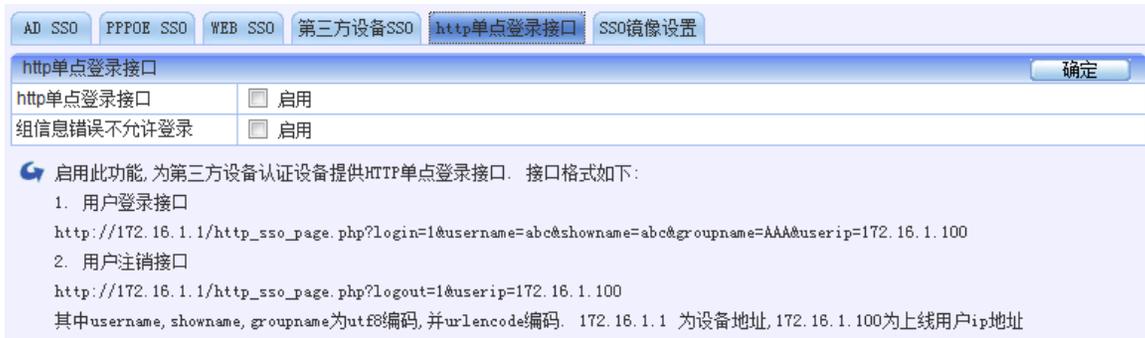
31 号属性：认证用户 MAC 地址

16.3.5.5 HTTP单点登录接口

HTTP 单点登录接口，可以向任何第三方认证设备，提供基于 HTTP(S) 协议，GET 方法的单点登录/注销功能。数据流的过程如下：

1. PC 通过 http/https 方式访问 WEB 认证服务器，并通过 WEB 认证服务器的认证/注销。
2. WEB 认证服务器认证/注销页面做处理，使得能通知设备上线/注销对应用户，完成单点登录。PC 通过设备认证，正常上网。

配置路径：【行为管理】>【认证选项】>【SSO】，选择 [HTTP 单点登录接口]，如下：



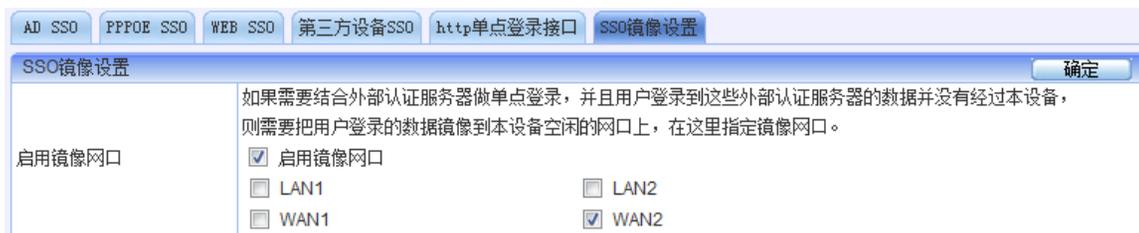
参数说明：

- 启用[HTTP 单点登录接口]，可以为第三方设备认证设备提供 HTTP 单点登录接口。接口格式如下：
 1. 用户登录接口：
http://172.16.1.1/http_sso_page.php?login=1&username=abc&showname=abc&groupname=AAA&userip=172.16.1.100
 2. 用户注销接口：http://172.16.1.1/http_sso_page.php?logout=1&userip=172.16.1.100
 3. 接口说明：
 - (1) 对 username（用户名）、showname（显示名）、groupname（组名）进行 utf8 编码；
 - (2) 对（1）的结果再进行 urlencode 编码；
 - (3) 172.16.1.1 为设备地址，172.16.1.100 为上线用户 IP 地址，根据实际环境替换对应的 IP 地址。
- 启用[组信息错误不允许登录]，当组信息错误时，不允许用户上网。

16.3.5.6 SSO镜像设置

如果认证服务器在外部，即认证数据经过本设备，则不需要进行[SSO 镜像设置]设置。如果认证服务器服务器在内网，即认证数据未经过本设备，则需要设置监听口。点[SSO 镜像设置]，勾选[启用镜像网口]，选择监听口。并且在内部交换机上需要把认证数据镜像到本设备。在 POP3 单点登录以及 WEB 单点登录等实现

时均需要设置。此处的镜像网口还可以用于设备旁路部署模式下，监听镜像上网数据。



16.3.6 短信认证

功能描述：对短信认证参数进行设置。

配置路径：【行为管理】>【认证选项】>【短信认证】

配置描述：

第一：进入【行为管理】>【认证选项】>【短信认证】页面，如下图所示：



图228. 短信认证页面

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。
- **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。

- 有效时长：用户认证通过后的有效时长。可选择“分钟”、“小时”、“天”。
- 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”，则在有效时长内浏览器的 cookie 值相同就不需要再次进行认证。如是选择“基于 mac 地址”，则在有效时长内只要用户的 mac 相同就不需要再次进行认证。
- 认证后跳转：认证成功后页面可选择“最近访问页面”和“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”则需要将短信猫连接在设备的 usb 接口。如下图所示：



图229. 短信猫配置参数

◇ 选择“HTTP 协议”，则还需要填写以下参数，如下图所示：



图230. HTTP 协议配置参数

- ◆ 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、浙江移动等。
- ◆ 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。

◇ 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：

参数设定	网关类型	电信运营商
	电信运营商	北京移动
	服务器地址	<input type="text"/>
	服务器端口	<input type="text"/>
	企业代码	<input type="text"/>
	业务代码	<input type="text"/>
	SP接入号	<input type="text"/>
	网关编号	<input type="text"/>
	登录帐号	<input type="text"/>
	登录口令	<input type="text"/>
		测试有效性

图231. 电信运营商配置参数

- ◆ 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：

网关类型	自定义服务器	
IP地址	<input type="text"/>	
短信中心端口	<input type="text"/>	
访问密码	914054	
		测试有效性

图232. 自定义服务器配置参数

- ◆ 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。

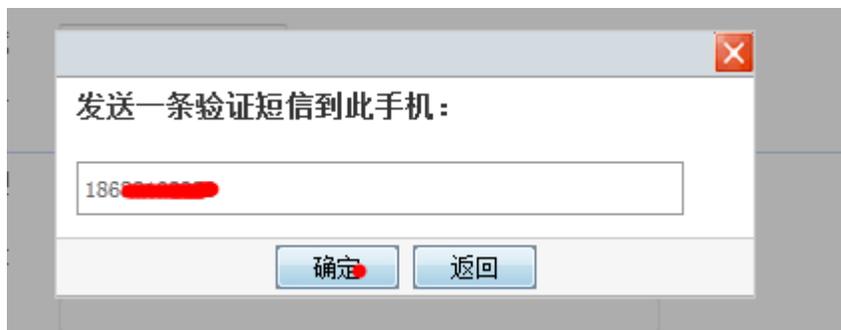


图233. 测试短信认证

16.4 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。

16.4.1 RADIUS 服务器

功能描述：配置 RADIUS 认证服务器。

配置路径：【用户认证】>【认证服务器】>【RADIUS 服务器】

配置描述：

第一：进入【RADIUS 服务器】页面，如下图：

RADIUS认证服务器						新增
序号	名称	IP地址	认证端口	计费端口	间隔传送时间	操作
1	radius	172.16.5.233	1812	1813	1	修改 删除
2	jiang	172.16.111.168	1812	1813	30	修改 删除
3	e	1.1.1.1	1812	1813	65535	修改 删除
4	说是	172.16.161.1	1812	1813	30	修改 删除
5	窝窝	172.16.161.2	1812	1813	30	修改 删除

图234. 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：

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				

图235. 新增 RADIUS 服务器

参数说明:

- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP地址：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。
- 间隔传送时间：可用于设置传送时间间隔。
- 共享密钥：与RADIUS服务器交换数据时进行加密的密钥。

16.4.2 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:

AD域认证服务器					新增
序号	名称	IP地址	AD域名	查找用户DN	操作
1	到底	172.16.12.50	jxq.local	test	修改 删除
2	AD	192.168.0.1	qing.com	user1	修改 删除
3	xiaoshen	172.16.5.233	pp.com	jiang	修改 删除
4	jiang	172.16.6.86	x86ad.com	test	修改 删除
5	172199	172.16.111.199	dn=abc	aaa	修改 删除

图236. AD 服务器配置列表

第二: 点击<新增>按钮，配置 AD 认证服务器，如下图:

新增AD域认证服务器		确定	返回
名称	<input type="text"/>		
IP地址	<input type="text"/>		
AD域名	<input type="text"/>		
查找用户DN	<input type="text"/>		
查找用户密码	<input type="text"/>		
IP地址:	AD服务器的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中用户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		
查找用户密码:	查找用户在AD服务器中的密码		

图237. 新增 AD 服务器

参数说明:

- 名称: 合法的字符是数字(0-9), 字母(A-Z, a-z)和下划线, 中划线及中文汉字。
- IP 地址: AD 服务器 IP 地址。
- AD 域名: 域控制器域名, 例如 abc.com。
- 查找用户DN: AD 服务器中的用户认证是基于用户 DN 完成的, 为了完成认证用户名到 AD域 用户 DN 的转换, 需要根据用户输入的用户名在 AD 服务器中执行查找操作。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。

16.4.3 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:

LDAP认证服务器						新增
序号	名称	IP地址	认证端口	DN	操作	
1	LDAP1	192.168.1.23	389	ou=group1,dc=abc,dc=com	修改	删除

图238. 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：

新增LDAP认证服务器		确定	返回
名称	LDAP1		
IP地址	192.168.1.23		
认证端口	389	(1 - 65535)	
DN	ou=group1,dc=abc,dc=com		
用户查找	<input type="radio"/> 匿名查询 <input checked="" type="radio"/> 本地用户查询		
查找用户DN	cn=searcher,ou=group1,dc=abc,dc=com		
查找用户密码	●●●●●●		
认证端口：默认为389			
DN：所查找用户组的路径，如ou=group1,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			

图239. 新增 LDAP 服务器

参数说明：

- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP地址：LDAP 服务器IP地址。
- 认证端口：服务器中用于认证的端口号，缺省为 389。
- DN：LDAP 服务器用通用名称标识符搜索具体条目时所使用的路径，如 cn=searcher,cn=software,dc=abc,dc=com。
- 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

16.4.4 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：

POP3认证服务器				新增
序号	名称	IP/域名	操作	
1	163	pop3.163.com	修改 删除	

图240. 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：

新增POP3认证服务器		确定	返回
名称	<input type="text"/>		
IP/域名	<input type="text"/>		

图241. 新增 POP3 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。

16.4.5 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[RADIUS 服务器], 如下图:

认证服务器		服务器测试
认证服务器类型	<input checked="" type="radio"/> RADIUS服务器 <input type="radio"/> LDAP服务器 <input type="radio"/> POP3服务器	
IP地址	<input type="text"/>	
认证端口	1812	(1-65535)
共享密钥	<input type="text"/>	
用户名	<input type="text"/>	
密码	<input type="text"/>	

图242. RADIUS 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: 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。
- 共享密钥: 与RADIUS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 RADIUS 用户名和密码。

第二: 测试[LDAP 服务器], 如下图:

认证服务器		服务器测试
认证服务器类型	<input type="radio"/> RADIUS服务器 <input checked="" type="radio"/> LDAP服务器 <input type="radio"/> POP3服务器	
IP地址	<input type="text"/>	
DN	<input type="text"/>	
查找用户DN	<input type="text"/>	
查找用户密码	<input type="text"/>	

图243. 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：

认证服务器		服务器测试
认证服务器类型	<input type="radio"/> RADIUS服务器 <input type="radio"/> LDAP服务器 <input checked="" type="radio"/> POP3服务器	
IP/域名	<input type="text"/>	
用户名	<input type="text"/>	
密码	<input type="text"/>	

图244. 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 RADIUS 用户名和密码。

16.5 白名单管理

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、上网策略对象规则、黑名单规则”的控制，上网的流量和上网行为的内容（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。

16.5.1 IP 白名单

功能描述：被管理的目标白名单为 IP 地址。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。IP 白名单功能可以很好的满足这些需求。

配置路径：【行为管理】>【白名单管理】>【IP 白名单】

配置描述：

第一：进入【IP 白名单】配置页面，如下图：



序号	名称	内网地址	控制白名单	生效时间	操作
1	总经理	172.16.99.111	全部	全天	修改 删除
2	重要用户	192.168.9.11-192.168.9.55	全部	全天	修改 删除
3	内网OA系统	全部	10.1.1.0/24	全天	修改 删除

提示：IP 白名单策略包含的流量全部放行，不受任何策略的控制，也不被审计。

图245. 白名单规则

第二：点击<新增>按钮，增加白名单规则，如下图：



名称	内网OA系统
内网地址	IP地址... 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)
控制白名单	IP地址... 10.1.1.0/24 (对在白名单内的目的IP地址不做控制)
生效时间	全天

图246. 新增白名单规则

参数说明：

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

◇ 地址簿：引用已定义好的地址簿；

➤ 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。

16.5.2 URL 白名单

功能描述：被管理的目标白名单为 URL 地址。

配置路径：【行为管理】>【白名单管理】>【URL 白名单】

配置描述：

第一：进入【URL 白名单】配置页面，如下图：



URL白名单						新增	修改状态	删除所有
序号	名称	内部地址	生效时间	<input type="checkbox"/> 状态	操作			
1	QQwenjian chuanshu	IP地址...全部	全天	<input checked="" type="checkbox"/>	修改 删除			
2	lixianwenjianchuanshu	IP地址...全部	全天	<input checked="" type="checkbox"/>	修改 删除			
3	特殊URL	IP地址...全部	全天	<input checked="" type="checkbox"/>	修改 删除			

提示：URL 白名单包含的流量全部放行，不受任何策略的控制，也不被审计。

图247. 白名单规则

第二：点击<新增>按钮，增加白名单规则，如下图：



新增URL白名单

名称: 特殊URL

内部地址: IP 地址簿 用户及用户组 全部
(格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)

URL白名单: 提示：一行一个 URL 关键字(或 URL 全名); 采用子串匹配方式, 如输入 xyz.com, 将匹配 www.xyz.com、www.xyz.com.cn、www.xyz.com/hardware 等。支持通配符比较, ‘?’表示匹配任意一个字节长度字符, ‘*’表示匹配任意长度字符串, ‘^’表示从起始处进行比较
news.sina
baidu

生效时间: 全天

状态: 启用 禁用

图248. 新增白名单规则

参数说明：

➤ 名称：白名单规则的名称。

➤ 内网地址：不受控的用户的地址,有三种输入方式，详细说明如下：

◇ IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；

- ◇ 地址簿：引用已定义好的地址簿；
- ◇ 用户组：引用组织结构中定义的用户组
- URL 白名单：一行一个 URL 关键字(或 URL 全名)。采用子串匹配方式，如输入 xyz.com，将匹配 www.xyz.com 或 www.xyz.com.cn 或 www.xyz.com/hardware 等。支持通配符比较，‘?’表示匹配任意一个字节长度字符，‘*’表示匹配任意长度字符串，‘^’表示从起始处进行比较。
- 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。

16.5.3 即时通讯白名单

功能描述：被管理的目标白名单为即时通讯协议的账号。

配置路径：【行为管理】>【白名单管理】>【即时通讯白名单】

配置描述：

第一：进入【即时通讯白名单】配置页面，如下图：

即时通讯白名单							新增	修改状态	删除所有
序号	名称	内部地址	IM类型	生效时间	状态	操作			
1	QQ白名单	IP地址...全部	QQ	全天	<input checked="" type="checkbox"/>	修改 删除			
2	MSN白名单	IP地址...172.16.5.3-172.16.5.15	MSN	全天	<input checked="" type="checkbox"/>	修改 删除			

提示：只有在‘即时通讯白名单’策略里的账号才能登录和使用，但其通讯记录是否被审计由【报表中心>内容记录配置】页面的配置来决定。

图249. 白名单规则

第二：点击<新增>按钮，增加白名单规则，如下图：

新增即时通讯白名单		确定	返回
名称	QQ白名单		
内部地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 <input type="radio"/> 用户及用户组 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)		
IM类型	QQ		
IM账号	12345678 22345678 32345678 说明:一行一个账号		
生效时间	全天		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		

图250. 新增白名单规则

参数说明：

- 名称：白名单规则的名称。

-
- 内网地址：不受控的用户的地址, 有三种输入方式, 详细说明如下:
 - ✧ IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网;
 - ✧ 地址簿：引用已定义好的地址簿;
 - ✧ 用户组：引用组织结构中定义的用户组
 - IM 类型：选择即时通讯协议的类型, 包含：MSN、QQ、Yahoo、ICQ、飞信、Gtalk、阿里旺旺等。
 - IM 账号：输入即时通讯协议的账号, 一行一个账号。
 - 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。

提示：

- 1、当‘即时通讯白名单’的某个协议未配置任何白名单策略时, 该协议的所有账号都可以登录和使用。一旦某个协议配置了白名单策略时, 只有在‘即时通讯白名单’策略里的账号才能登录和使用。比如, 白名单里配置了 QQ 账号 22345678 和 32345678, 则只有这 2 个账号可以登录和使用, 其它 QQ 账号都不能使用, 但未配置白名单的其它协议（如 MSN）不受任何限制。
- 2、即时通讯是否被审计由【报表中心>内容记录配置】页面的配置来决定, 不受‘即时通讯白名单’策略的控制。

17 酒店管理-即插即用

由于酒店客人的电脑的 IP 地址配置各不相同, 经常需要酒店网管人员为其进行一番配置后才能正常上网。既费时费力, 又降低了客人的满意度。开启酒店即插即用功能, 不论其电脑的 IP 地址、网关, DNS 服务器怎样配置, 都能实现客人的电脑插上网线即可正常上网。大大方便了客人的使用, 又降低了酒店的运作成本。

功能描述：酒店客人的电脑插上网线即可正常上网。

配置路径：【酒店管理】>【即插即用】

注：如果在界面没有界面上没有显示, 则需要在后台/home 目录下创建一个 ace_menu_config.conf 的文件在文件中添加一条!hotel 的内容。具体如图:



配置描述：进入【即插即用】界面，如上图：

图251. 即插即用

参数说明：

➤ 即插即用：选择<启用>或<禁用>开启或关闭“即插即用”功能。启用酒店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：选择启用即插即用的 LAN 口。

注：低端设备开启此功能将消耗设备 CPU 部分资源，但不影响产品中任何功能的使用。中高端设备则无任何影响

18 高可靠性(HA)

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：

HA 配置同步		确定	立即同步
自动同步	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	(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上)	
同步IP地址			

HA 配置		确定
功能状态	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	

图252. HA 配置 01

HA 配置同步		确定	立即同步
自动同步	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	(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上)	
同步IP地址	1.1.1.1		

HA 配置		确定
功能状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
心跳间隔	2 (1-10秒)	
死亡时间	30 (1-60秒)	
心跳端口	<input type="checkbox"/> LAN1 <input type="checkbox"/> WAN1 <input checked="" type="checkbox"/> LAN2 <input type="checkbox"/> WAN2 <input type="checkbox"/> LAN1.100 <input type="checkbox"/> LAN1.200	
本地节点名称	X	
对端节点名称	fffad,ww1,ww2 (多节点之间用英文逗号分隔)	
主设备	格式为: 节点名称 虚拟IP/虚拟IP掩码/广播地址, 虚拟IP为内网的网关IP (不能与设备上配置的真实IP地址相同)。 如需修改虚拟IP, 请先禁用HA, 然后启用修改为预期IP。 IPv4格式如 node1 192.168.2.1/24/192.168.2.255 或 node1 192.168.2.1/24/LAN1/192.168.2.255 IPv6格式如 node1 IPv6addr::2001:0:0:0:0:0:1111/64 或 node1 IPv6addr::2001:0:0:0:0:0:1111/64/LAN1 <pre>node1 IPv6add ::0:0:ade:0:0:0:0f:0/128/lam2</pre>	
强制抢占	<input checked="" type="checkbox"/> 启用 (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	<input type="checkbox"/> 启用 (当切换到备机的时候关闭WAN口)	
链路健康检查	<input checked="" type="checkbox"/> 启用 (当检测到链路故障时, 就切换到备份状态) <input checked="" type="radio"/> 检查对象: 一行一个IPv4地址或IPv6地址; 只要其中一个IP不可到达, 就认为链路状态就不正常; <input type="radio"/> 检查对象: 一行一个IPv4地址或IPv6地址; 如果全部IP都不可到达, 就认为链路状态不正常; 12.1.1.1	

图253. HA 配置 02

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。

19 系统日志

“系统日志”包含：命令日志、事件日志、PPTP/L2TP 日志、IPSEC 日志、用户日志、日志服务器、告警配置。

19.1 命令日志

功能描述：将管理员对设备配置的命令记录下来，以便查询。

配置路径：【系统日志】>【命令日志】

配置描述：进入【命令日志】页面，如下图：



图254. 查看命令日志

查询条件：

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

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

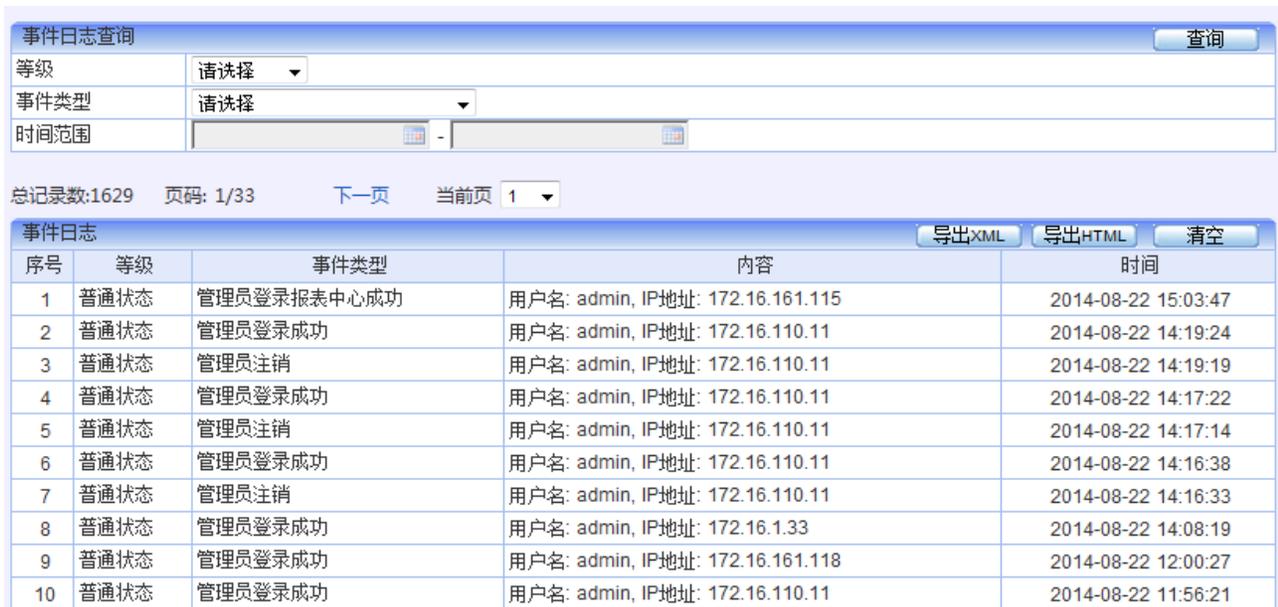
点击<清空>按钮，清空所有的命令日志。点击<导出>按钮，可以将命令日志以 HTML、XML 的格式导出。

19.2 事件日志

功能描述：设备提供事件日志，用于监视系统事件的发生。

配置路径：【系统日志】>【事件日志】

配置描述：进入【事件日志】页面，如下图：



The screenshot shows a web interface for querying event logs. At the top, there is a search form with fields for '等级' (Level), '事件类型' (Event Type), and '时间范围' (Time Range). Below the form, it displays '总记录数:1629' (Total records: 1629) and '页码: 1/33' (Page: 1/33). The main part of the interface is a table titled '事件日志' (Event Log) with columns for '序号' (Serial Number), '等级' (Level), '事件类型' (Event Type), '内容' (Content), and '时间' (Time). The table contains 10 rows of log entries, all with '普通状态' (Normal Status) and '管理员登录成功' (Administrator login successful) as event types. The content column shows details like '用户名: admin, IP地址: 172.16.161.115' and the time column shows timestamps such as '2014-08-22 15:03:47'. There are also buttons for '导出XML', '导出HTML', and '清空' (Clear).

序号	等级	事件类型	内容	时间
1	普通状态	管理员登录报表中心成功	用户名: admin, IP地址: 172.16.161.115	2014-08-22 15:03:47
2	普通状态	管理员登录成功	用户名: admin, IP地址: 172.16.110.11	2014-08-22 14:19:24
3	普通状态	管理员注销	用户名: admin, IP地址: 172.16.110.11	2014-08-22 14:19:19
4	普通状态	管理员登录成功	用户名: admin, IP地址: 172.16.110.11	2014-08-22 14:17:22
5	普通状态	管理员注销	用户名: admin, IP地址: 172.16.110.11	2014-08-22 14:17:14
6	普通状态	管理员登录成功	用户名: admin, IP地址: 172.16.110.11	2014-08-22 14:16:38
7	普通状态	管理员注销	用户名: admin, IP地址: 172.16.110.11	2014-08-22 14:16:33
8	普通状态	管理员登录成功	用户名: admin, IP地址: 172.16.1.33	2014-08-22 14:08:19
9	普通状态	管理员登录成功	用户名: admin, IP地址: 172.16.161.118	2014-08-22 12:00:27
10	普通状态	管理员登录成功	用户名: admin, IP地址: 172.16.110.11	2014-08-22 11:56:21

图255. 查看命令日志

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

点击<清空>按钮，清空所有的命令日志。

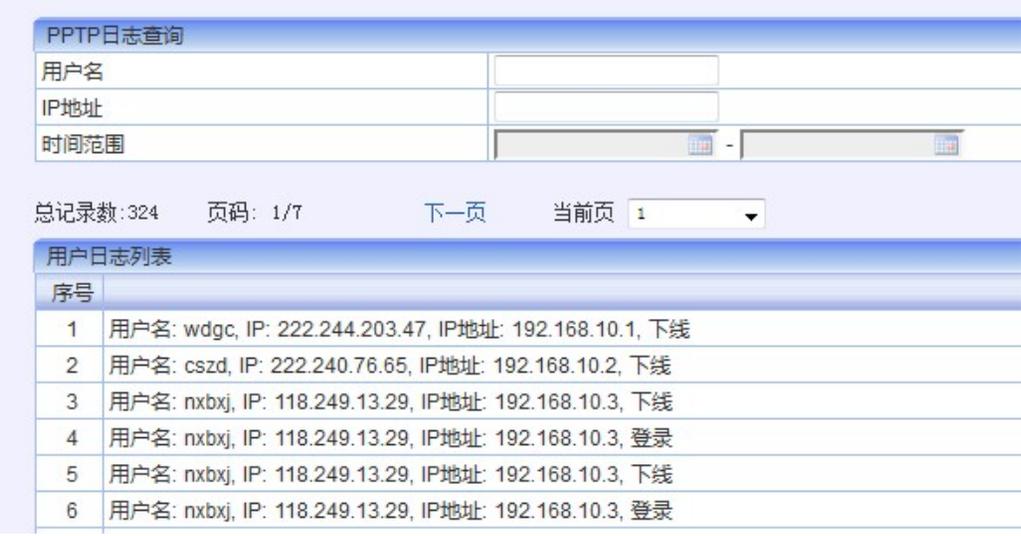
19.3 PPTP/L2TP日志

功能描述：记录 PPTP 他 L2TP 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：



PPTP日志查询

用户名

IP地址

时间范围 -

总记录数: 324 页码: 1/7 下一页 当前页 1

用户日志列表

序号	
1	用户名: wdgc, IP: 222.244.203.47, IP地址: 192.168.10.1, 下线
2	用户名: cszd, IP: 222.240.76.65, IP地址: 192.168.10.2, 下线
3	用户名: nxbxj, IP: 118.249.13.29, IP地址: 192.168.10.3, 下线
4	用户名: nxbxj, IP: 118.249.13.29, IP地址: 192.168.10.3, 登录
5	用户名: nxbxj, IP: 118.249.13.29, IP地址: 192.168.10.3, 下线
6	用户名: nxbxj, IP: 118.249.13.29, IP地址: 192.168.10.3, 登录

图256. 查看 PPTP 日志

查询条件：

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

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

点击<清空>按钮，清空所有的用户日志。

19.4 IPSec日志

功能描述：记录 IPSec VPN 连接的日志。

配置路径：【系统日志】>【IPSec 日志】

配置描述：

第一：进入【IPSec 日志】页面，如下图：

IPSec日志查询		
时间范围		
总记录数:4760 页码: 1/96 下一页 当前页: 1		
IPSec日志列表		
序号	内容	时间
1	183.14.1.231[4500] used as isakmp port (fd=28)	2014-07-09 08:52:15
2	183.14.1.231[4500] used for NAT-T	2014-07-09 08:52:15
3	183.14.1.231[500] used as isakmp port (fd=27)	2014-07-09 08:52:15
4	183.14.1.231[500] used for NAT-T	2014-07-09 08:52:15
5	unsupported PF_KEY message REGISTER	2014-07-09 08:52:05
6	192.168.234.1[4500] used as isakmp port (fd=26)	2014-07-09 08:52:05
7	192.168.234.1[4500] used for NAT-T	2014-07-09 08:52:05
8	192.168.234.1[500] used as isakmp port (fd=25)	2014-07-09 08:52:05
9	192.168.234.1[500] used for NAT-T	2014-07-09 08:52:05
10	192.168.14.1[4500] used as isakmp port (fd=24)	2014-07-09 08:52:05
11	192.168.14.1[4500] used for NAT-T	2014-07-09 08:52:05
12	192.168.14.1[500] used as isakmp port (fd=23)	2014-07-09 08:52:05
13	192.168.14.1[500] used for NAT-T	2014-07-09 08:52:05
14	172.16.161.2[4500] used as isakmp port (fd=22)	2014-07-09 08:52:05
15	172.16.161.2[4500] used for NAT-T	2014-07-09 08:52:05
16	172.16.161.2[500] used as isakmp port (fd=21)	2014-07-09 08:52:05
17	172.16.161.2[500] used for NAT-T	2014-07-09 08:52:05
18	127.0.0.1[4500] used as isakmp port (fd=20)	2014-07-09 08:52:05
19	127.0.0.1[4500] used for NAT-T	2014-07-09 08:52:05
20	127.0.0.1[500] used as isakmp port (fd=19)	2014-07-09 08:52:05
21	127.0.0.1[500] used for NAT-T	2014-07-09 08:52:05

图257. 查看 IPSec 日志

时间范围：根据 IPSec VPN 连接时间范围来查找

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

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

19.5 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：

第一：进入【黑名单日志】页面，如下图：

黑名单日志						
序号	用户名/用户组	IP地址	MAC地址	内容	黑名单策略	时间
1	7.200 Root	172.16.7.200	8c:89:a5:7d:e3:13	原因: 手动解除	ceshi	2014-08-14 13:06:56
2	7.200 Root	172.16.7.200	8c:89:a5:7d:e3:13	原因: 检测到内部共享上网	ceshi	2014-08-14 12:39:25
3	7.200 Root	172.16.7.200	8c:89:a5:7d:e3:13	原因: 手动解除	ceshi	2014-08-14 11:56:42
4	7.200 Root	172.16.7.200	8c:89:a5:7d:e3:13	原因: 检测到内部共享上网	ceshi	2014-08-14 11:55:09
5	1 Root	172.16.110.11	74:d4:35:46:35:4e	原因: 手动解除	44	2014-08-12 15:53:04

图258. 查看黑名单日志

查询条件:

- 用户名: 根据用户名称来查找, 支持模糊查询。
- 原因: 根据进入或解除黑名单的原因来查找。
- 时间范围: 根据进入或解除黑名单的时间范围来查找。

默认显示所有黑名单日志。输入查询条件后, 点击<查询>按钮, 显示满足查询条件的黑名单日志。

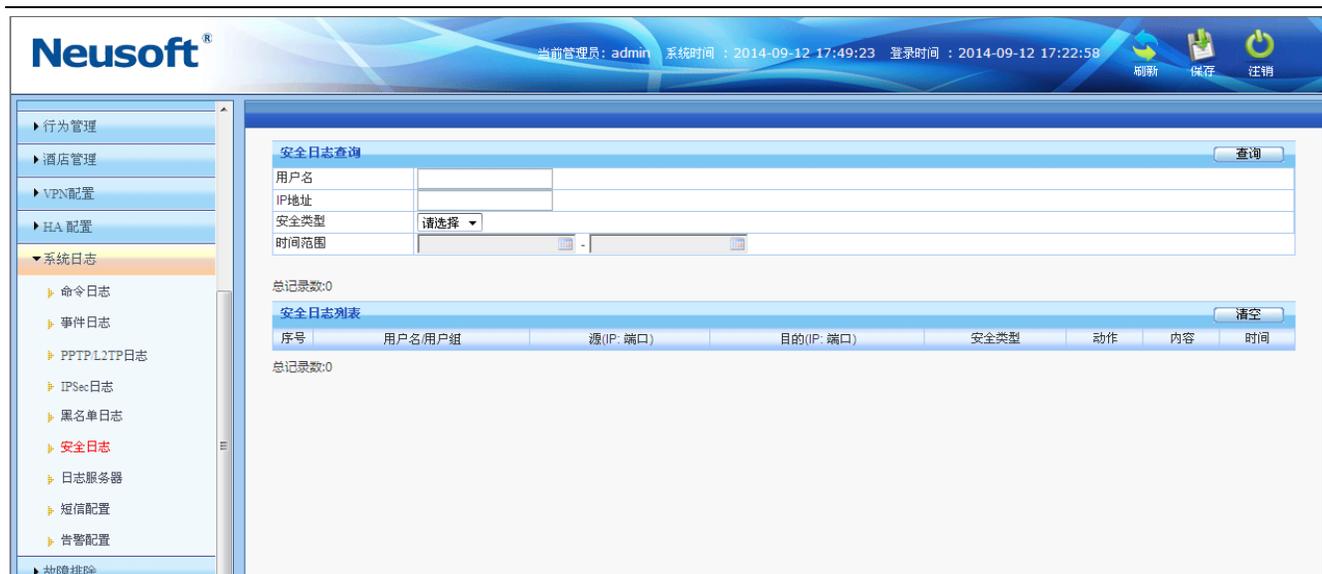
点击<清空>按钮, 清空所有的黑名单日志。点击<导出>按钮, 可以将黑名单日志以 HTML、XML 的格式导出。

19.6 安全日志

功能描述: 显示被识别为网络攻击或者病毒文件的记录

配置路径: 【系统日志】>【安全日志】

配置描述: 进入【日志服务器】页面, 如下图:



19.7 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：



日志服务器配置窗口，包含以下配置项：

- 日志服务器：启用或禁用 Syslog 服务器，当前选择禁用。
- 服务器地址：输入框。
- 服务器端口：514。
- 勾选框列表：
 - 命令日志 (勾选)
 - 事件日志 (勾选)
 - 用户日志 (勾选)
 - 黑名单日志 (勾选)
 - URL地址 (未勾选)
 - 网页标题 (未勾选)
 - HTTP上传 (未勾选)
 - 搜索关键字 (未勾选)
 - 文件上传 (未勾选)
 - 网页登陆 (未勾选)
 - 即时通讯 (未勾选)
 - 邮件记录 (未勾选)
 - FTP记录 (未勾选)
 - Telnet记录 (未勾选)
 - 会话记录 (未勾选)

图259. Syslog 服务器配置

参数说明：

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

19.8 短信配置

功能描述：配置日志短信提醒（注：设备需要在设备上安装一个 USB 短信猫）

配置路径：【系统日志】>【短信配置】，配置页面如下：



短信配置窗口，包含以下配置项：

- 短信配置：启用或禁用短信配置，当前选择启用。
- 手机号码：输入框，提示为“多个号码以“,”分隔”。

手机号码：接收信息的手机号码

19.9 告警配置

功能描述：配置告警的参数。

配置路径：【系统日志】>【告警配置】，配置页面如下：



图260. 告警配置

告警级别：普通状态、预警状态、严重状态、紧急状态。

处理策略：日志记录、邮件告警+日志记录、SYSLOG+日志记录、发送短信+日志记录、邮件告警+SYSLOG+日志记录、邮件告警+发送短信+日志记录、SYSLOG+发送短信+日志记录、邮件告警+SYSLOG+发送短信+日志记录。

邮件告警在【[系统配置>邮件配置](#)】里面进行配置邮件告警收件人。

SYSLOG 在【[系统日志>日志服务器](#)】里面进行配置日志服务器。

发送短信需要在【[行为管理>认证选项>短信认证](#)】中开启短信认证功能。

一、首先看到是“设备告警”选项卡。

参数说明：

- 事件告警：系统级别的事件日志将产生告警，如接口 UP/Down、系统重启等。勾选“启用”则生效。
- 黑名单告警：用户进出黑名单的产生告警。勾选“启用”则生效。
- 监控告警：当 CPU 和内存使用率、活跃会话数以及 WAN 总和大于预设阈值时，产生告警。“勾选”启用则生效。

二、选择“违规网站”，可对网站类型进行告警，如下图所示：



图261. 违规网站告警配置页面

参数配置：

- 自定义网站类型：可在【[系统对象>URL 库>自定义的 URL 库](#)】中自定义网站类型。
- 告警级别：可为违规网站定义不同告警级别。默认是普通状态。
- 处理策略：可为违规网站选择处理策略，默认是日志记录。
- 操作：点击删除按钮可以删除该条违规网站告警。
- 添加条目：点击添加条目按钮可新增违规网站告警配置。

三、选择“违规搜索”选项卡，可对搜索内容进行告警。如下图所示：

序号	关键字组	告警级别	处理策略	操作
1	AAA1	普通状态	日志记录	删除
2	BBB2	普通状态	邮件告警+发送短信+日志记录	删除
3	11	普通状态	邮件告警+SYSLOG+发送短信+日志记录	删除

图262. 违规搜索告警配置页面

参数说明：

- 关键字组：需要在【[系统对象>关键字组](#)】中先定义要告警的关键字。
- 告警级别：可为关键字组定义不同告警级别。默认是普通状态。
- 处理策略：可为关键字组选择处理策略，默认是日志记录。
- 操作：点击删除按钮可以删除该条违规搜索告警。
- 添加条目：点击添加条目按钮可以添加新的违规搜索告警。

三、选择“违规帖子”选项卡，可对发帖内容进行告警。如下图所示：

序号	关键字组	告警级别	处理策略	操作
1	11	普通状态	邮件告警+SYSLOG+日志记录	删除
2	AAA1	普通状态	SYSLOG+发送短信+日志记录	删除
3	BBB2	普通状态	发送短信+日志记录	删除

图263. 违规帖子告警配置页面

参数说明:

- 关键字组: 需要在[系统对象—关键字组](#)中先定义要告警的关键字。
- 告警级别: 可为关键字组定义不同告警级别。默认是普通状态。
- 处理策略: 可为关键字组选择处理策略, 默认是日志记录。
- 操作: 点击删除按钮可以删除该条违规帖子告警。
- 添加条目: 点击添加条目按钮可以添加新的违规帖子告警。

四、选择“违规上传”选项卡, 可对上传的文件类型进行告警。如下图所示:

序号	文件类型	告警级别	处理策略	操作
1	测试	普通状态	SYSLOG+日志记录	删除
2	压缩	严重状态	SYSLOG+发送短信+日志记录	删除
3	可执行	普通状态	邮件告警+SYSLOG+发送短信+日志记录	删除

图264. 违规上传告警配置页面

参数说明:

- 关键字组: 需要在【[系统对象>文件类型](#)】中先定义要告警的文件类型。
- 告警级别: 可为文件类型定义不同告警级别。默认是普通状态。
- 处理策略: 可为文件类型选择处理策略, 默认是日志记录。
- 操作: 点击删除按钮可以删除该条违规上传告警条目。
- 添加条目: 点击添加条目按钮可以添加新的违规上传告警。

五、选择“违规邮箱”选项卡, 可对违规的邮件发送者及接收者进行告警。如下图所示:

设备告警 违规网站 违规搜索 违规帖子 违规上传 违规邮箱 违规邮件 违规 IM 潜在危害

违规邮件发送者告警设置 确定

序号	关键字组	告警级别	处理策略	操作
1	11	普通状态	日志记录	删除
2	AAA1	普通状态	发送短信+日志记录	删除
3	BBB2	普通状态	邮件告警+发送短信+日志记录	删除

添加条目

违规邮件接收者告警设置 确定

序号	关键字组	告警级别	处理策略	操作
1	11	预警状态	发送短信+日志记录	删除
2	AAA1	严重状态	邮件告警+SYSLOG+发送短信+日志记录	删除
3	BBB2	紧急状态	邮件告警+发送短信+日志记录	删除

添加条目

图265. 违规邮箱告警配置页面

[邮件发送者]和[邮件接收者]分开设置。

参数说明：

- 关键字组：需要在【[系统对象>关键字组](#)】中先定义要告警的邮件接收者或发送者。
- 告警级别：可为邮件发送者或者接收者定义不同告警级别。默认是普通状态。
- 处理策略：可为邮件发送者或者接收者选择处理策略，默认是日志记录。
- 操作：点击删除按钮可以删除该条违规邮箱告警条目。
- 添加条目：点击添加条目按钮可以添加新的违规邮箱告警。

五、选择“违规邮件”选项卡，可对违规的邮件主题和内容或者附件类型进行告警。如下图所示：

设备告警 违规网站 违规搜索 违规帖子 违规上传 违规邮箱 违规邮件 违规 IM 潜在危害

违规邮件主题和内容告警设置 确定

序号	关键字组	告警级别	处理策略	操作
1	11	普通状态	日志记录	删除
2	AAA1	普通状态	发送短信+日志记录	删除
3	BBB2	普通状态	邮件告警+发送短信+日志记录	删除

添加条目

违规邮件附件告警设置 确定

序号	文件类型	告警级别	处理策略	操作
1	压缩	普通状态	发送短信+日志记录	删除
2	可执行	预警状态	邮件告警+发送短信+日志记录	删除

添加条目

图266. 违规邮件告警配置页面

可分别为邮件主题和内容、附件类型进行告警。

参数说明：

- 违规邮件主题和内容关键字组：需要在【[系统对象>关键字组](#)】中先定义要告警的邮件的主题和内容关键字。
- 违规邮件附件文件类型：需要在【[系统对象>文件类型](#)】中先定义要告警的邮件附件文件类型。
- 告警级别：可为邮件主题内容或者附件定义不同告警级别。默认是普通状态。
- 处理策略：可为邮件主题内容或者附件选择处理策略，默认是日志记录。
- 操作：点击删除按钮可以删除该条违规邮件告警条目。
- 添加条目：点击添加条目按钮可以分别添加新的违规邮件主题内容或者附件告警。

六、选择“违规 IM”选项卡，可对 IM 的关键字进行告警。如下图所示：

序号	关键字组	告警级别	处理策略	操作
1	AAA1	普通状态	日志记录	删除
2	BBB2	预警状态	发送短信+日志记录	删除

图267. 违规 IM 告警配置页面

参数说明：

- 关键字组：需要在【[系统对象>关键字组](#)】中先定义要告警的关键字。
- 告警级别：可为关键字组定义不同告警级别。默认是普通状态。
- 处理策略：可为关键字组选择处理策略，默认是日志记录。
- 操作：点击删除按钮可以删除该条违规 IM 告警。
- 添加条目：点击添加条目按钮可以添加新的违规 IM 告警。

七、选择“潜在危害”选项卡，可自定义可能出现的一些潜在危害行为并进行告警。如下图所示：

序号	关键字组	出现频率	出现周期	告警级别	处理策略	操作
1	AAA1	3	一小时	普通状态	日志记录	删除
2	AAA1	5	二小时	普通状态	日志记录	删除

图268. 潜在危害告警配置页面

参数说明:

- 关键字组: 需要在【[系统对象>关键字组](#)】中先定义要告警的关键字。
- 出现频率: 该关键字出现的次数。
- 出现周期: 定义关键字出现次数的时间。
- 操作: 点击删除按钮可以删除该条潜在危害告警。
- 添加条目: 点击添加条目按钮可以添加新的潜在危害告警。

20 故障排除

20.1 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269. 故障排除-捕获数据包

参数说明:

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

host 1.1.1.1 and tcp;

- IP地址：要捕获数据包的IP地址的范围。
- 端口：要捕获数据包的端口范围。
- 协议类型：要捕获的数据包的协议类型。可选择捕获所有的协议，也可以选择tcp、udp、ICMP或者ARP。

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。

20.2 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：

查看数据包 删除所有			
序号	文件名称	文件大小	操作
2	capture_20140704144509.cap	1097 bytes	下载 详细 删除

点击”下载“后，下载的文件可以用Sniffer或Ethereal等抓包软件查看

图270. 故障排除-查看数据包

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

20.3 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：

调试信息下载	
说明：调试信息的下载需要一定的时间，请耐心等待	下载

图271. 故障排除-调试信息下载 1

点击<下载>按钮后，可将当前调试信息保存至指定的文件夹，如下图所示：

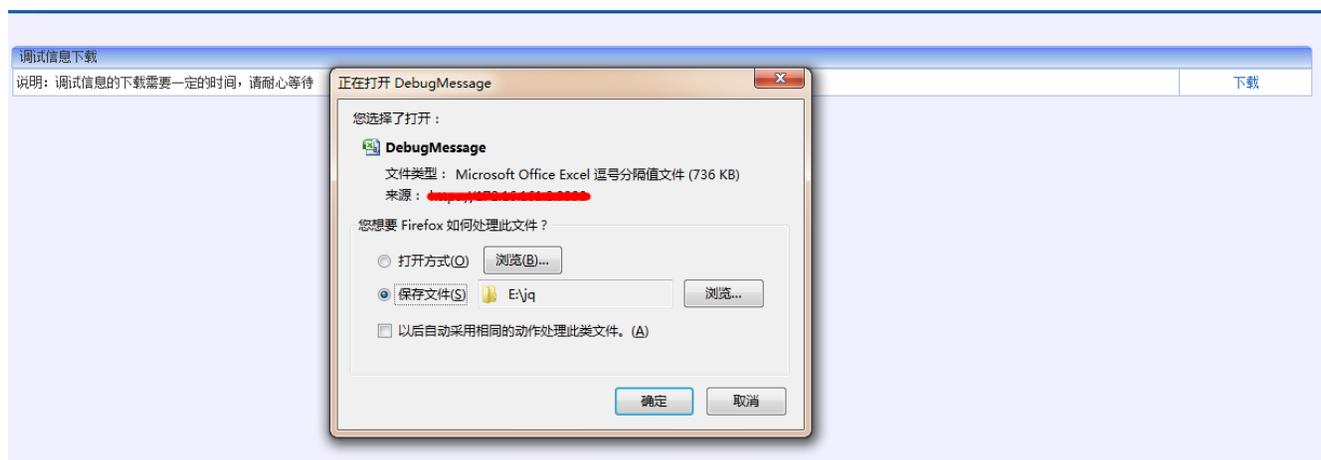


图272. 故障排除-调试信息下载 2

下载完成后，可通过 debugview 等工具对调试信息进行查看分析。

20.4 上网故障调试

功能描述：可对某些地址或端口进行上网故障调试

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：

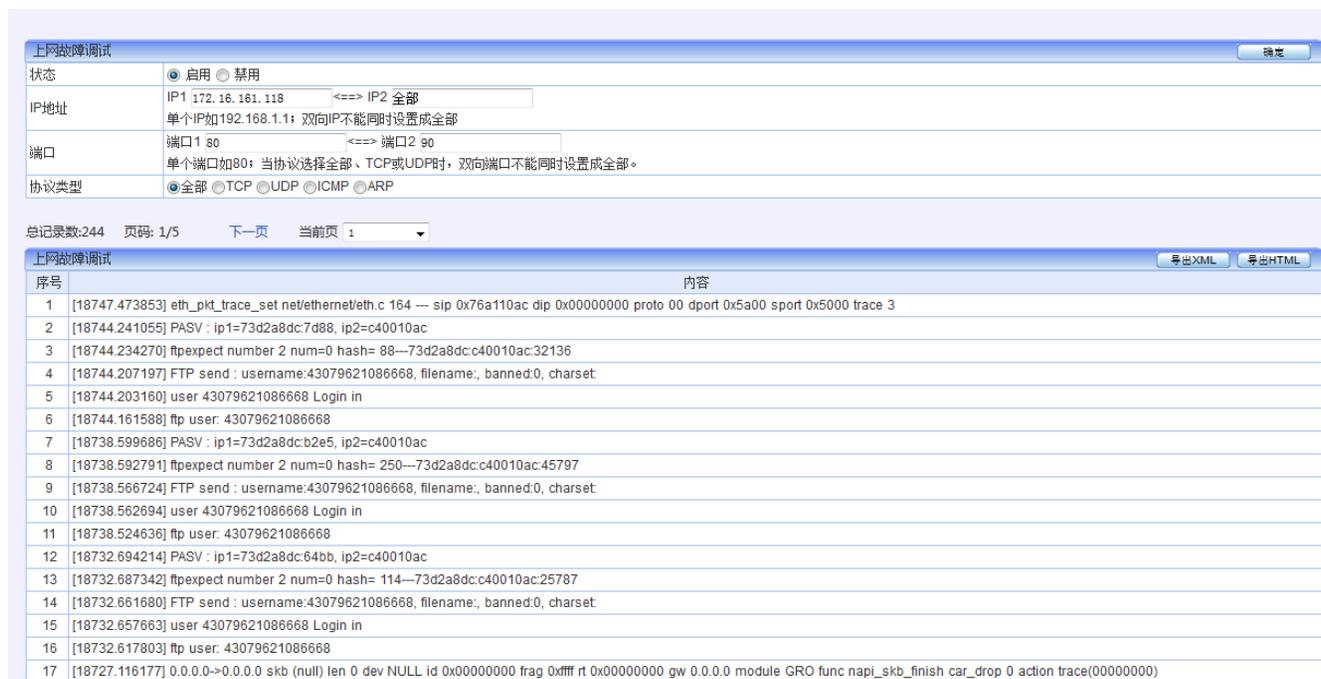


图273. 故障排除-上网故障调试

参数说明：

- 状态：可选择[启用]或[禁用]。
 - IP 地址：选择要调试的 IP 地址范围，单个 IP 如 192.168.1.1；双向 IP 不能同时设置成全部
 - 端口：选择要调试的端口范围，单个端口如 80；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：选择要进行调试的协议。可选择全部、也可选择单个协议，如 TCP、UDP、ICMP 或者 ARP。
- 点击<导出>按钮，可以将调试信息以 HTML、XML 的格式导出。

21 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。

21.1 报表中心配置

功能描述：配置报表中心相关参数。

配置路径：【报表中心】>【报表中心】

配置描述：点击【报表中心】，进入配置页面。如下图：

报表中心配置		确定
启用外置报表	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
网点名称	514	
外置报表IP地址	172.16.4.221	
同步数据内容	全部	
同步数据方式	<input checked="" type="radio"/> 实时上传 <input type="radio"/> 定时上传	
启用内置报表	<input checked="" type="radio"/> 是 <input type="radio"/> 否	

图274. 报表中心配置

参数说明：

- 启用外置报表：启用或者禁用外置报表功能。
- 网点名称：配置设备在外置报表中心界面中显示的设备名称。须与外置报表中心上配置的设备名称一致。
- 外置报表IP地址：外置报表中心的IP地址。
- 同步数据内容：可选择全部、除去会话记录和URL记录、除去会话记录、和除去URL记录。

- 同步数据方式：可选择实时上传和定时上传。选择实时上传则会将数据实时的传送至外置报表，选择定时上传则会在指定的时间上传数据。
- 启用内置报表：启用或禁用内置报表。

21.2 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：



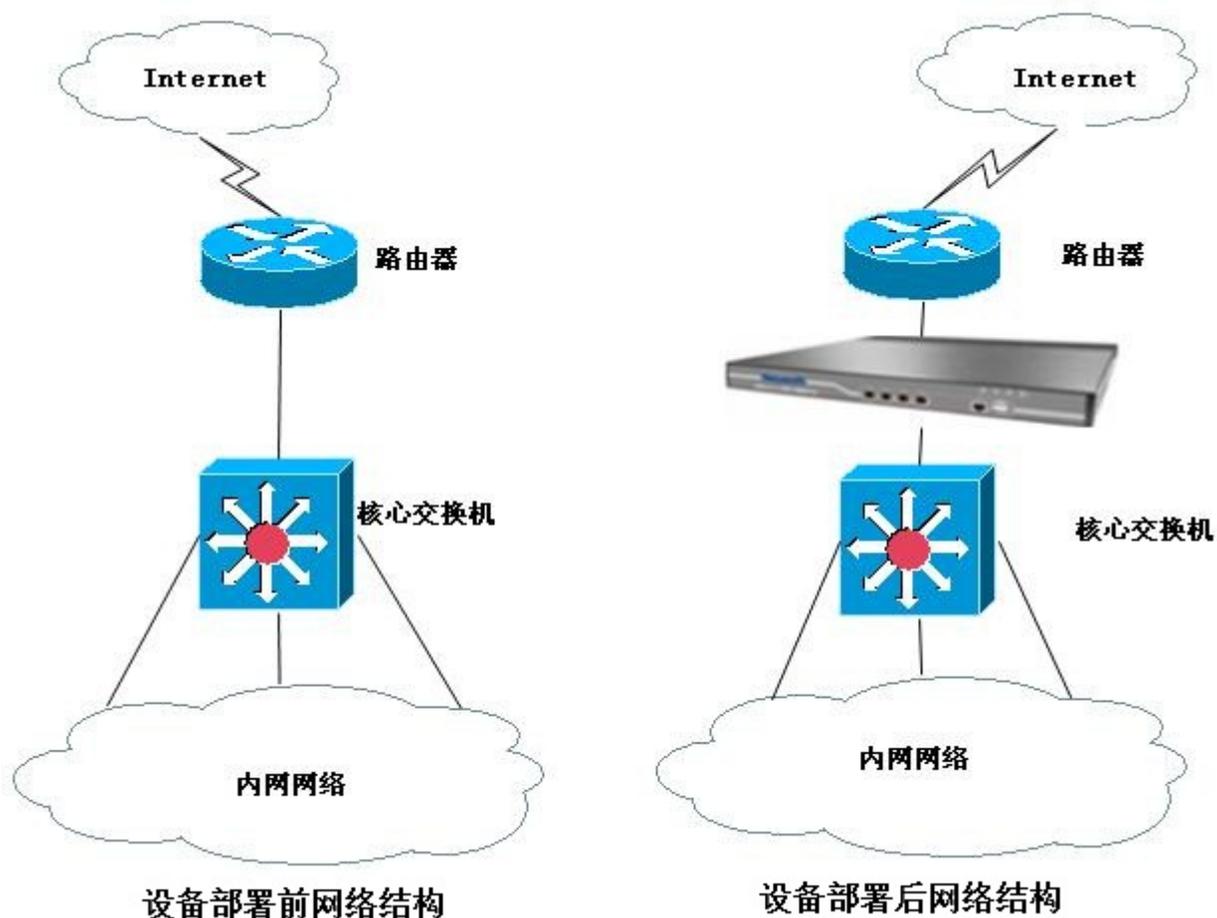
图275. 内置报表中心首页

22 配置实例

说明：ESM 的典型应用模式为旁路模式。

22.1 网桥模式

使用环境：在客户网络中已经存在路由器，且能够正常上网的情况下，建议使用网桥模式，网桥模式就是将设备以透明的方式接入客户的网络环境中，对客户原有的网络环境几乎不产生任何影响。



实施步骤

1、登录设备

- (1) 将管理电脑 IP 设置成 192.168.0.x/24;
- (2) 用网线将管理主机连接到设备的 LAN1 口
- (3) 打开 Web 浏览器，在地址栏中输入 <https://192.168.0.1:9090>，回车



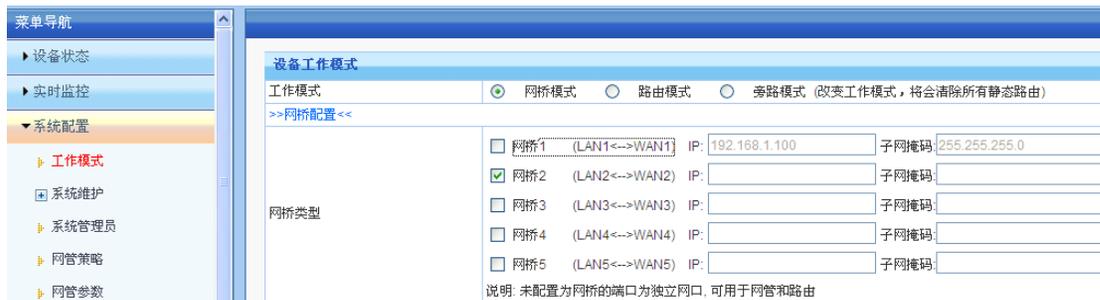
- (4) 点击“继续浏览此网站”，弹出以下对话框



(5) 输入用户名 admin；密码 admin*PWD，点击“登录”即可成功登录。

2、设置工作模式

(1) 点击菜单：系统配置—工作模式；即进入工作模式配置界面



(2) 在工作模式栏中，选择“网桥模式”；

(3) 勾选使用“网桥 2”，当然也可以选择其他桥接口（这里的 IP 可以不做配置；如果设置 IP，也可以在网络中通过这个 IP 来登录管理设备）

3、设置流量管理策略（主要根据需求设置相关的策略）

(1) 进行线路带宽配置（这一步的配置必须进行）

a)、点击菜单：流量管理——线路带宽配置



b)、在 WAN2 的上行带宽中输入线路的上行总带宽值，在下行带宽中输入下行总带宽值（这个值需要跟用户确定，注意这里的单位是 Kbps 而不是 KBps, 8Kbps=1KBps,我们常说的运营商带宽单位是 Kbps 或者 Mbps, 1Mbps=1024Kbps）

4、设置基于策略的流控

（这个配置的作用是对整个网段做相应的流量限制，同一条策略里面的所有主机来说所分配的带宽是共享的），以下是根据不同需求进行设置实例

需求一：限制网络中的所有主机进行 P2P 下载、网络游戏，并记录阻断日志

a) 菜单：流量管理---基于策略的流控；点击“新增通道按钮”



b) 在弹出的对话框中，输入规则名称（名称自定义），生效线路选择 WAN2，内网机外网 IP 为“全部”，服务及文件类型选择“自选服务”；流控行为选择“阻断流量”，生效时间为“全天”，阻断记录“启用”，状态“启用”



c) 点击上图服务及文件类型栏目中的“选择服务”，在弹出的对话框中，选择“P2P 下载”，并选中所有的条目，点击“确定”，并按照相同的办法选择“网络游戏”项。



d)最后，点击右上角的“确定”按钮即可完成对“限制 P2P 及网络游戏”的操作

需求二：任何时间段 HTTP 应用上下行流量保障带宽 50Mbps，最大带宽 70Mbps

a) 菜单：流量管理---基于策略的流控；点击“新增通道按钮”

b) 在弹出的对话框中，输入规则名称（名称自定义），生效线路选择 WAN2，内网机外网 IP 为“全部”，服务及文件类型选择“自选服务”；流控行为选择“保障通道”，在保障带宽栏目上下行流量输入 50000Kpbs，在最大带宽栏中上下行流量输入 70000Kpbs；生效时间为“全天”，阻断记录“启用”，状态“启用”。

最大带宽	上行: <input type="text" value="70000"/> (Kbps) <input type="text" value="70"/> %
	下行: <input type="text" value="70000"/> (Kbps) <input type="text" value="70"/> %
	(本规则流量能使用的最大带宽,百分比为占用本线路带宽值的比例)
生效时间	<input type="text" value="全天"/>
阻断记录	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 (只对流控行为是阻断流量时生效)
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

c) 点击上图服务及文件类型栏目中的“选择服务”，在弹出的对话框中，选择“HTTP 应用”，并选中所有的条目，点击“确定”



d)最后，点击右上角的确定即可成功添加关于 HTTP 应用的策略带宽。

5、配置基于用户的流控

这个配置的主要作用是对单个主机的流量及会话数限制。

需求一：限制网络中的所有主机的最大流量不得超过 3Mbps

a)菜单：流量管理—基于用户的流控，点击“新增”按钮



b) 在弹出的对话框中，在规则名称栏中输入自定义的名称，在最大上行带宽中输入 3000，在最大下行带宽中输入 3000，其他地方不需要配置，点击右上角的“确定”按钮即可完成该策略的配置。



需求二：限制网段 192.168.10.1~192.168.10.255 内的单台主机 HTTP 应用最大上下行带宽为 1Mbps

a) 菜单：流量管理—基于用户的流控，点击“新增”按钮



b)在弹出的对话框中，在规则名称栏中输入自定义的名称，在地址栏中输入ip段 192.168.10.1-192.168.10.255（也可以用户及用户组方式，具体操作详见“组织管理”介绍）；启用带宽分配细则，其他地方不需要改动。

序号	服务	最大带宽(Kbps)	操作
1	未配置		配置 清除
2	未配置		配置 清除
3	未配置		配置 清除

c) 在上图的带宽细分配栏中，点击“操作”下的配置“按钮”，在弹出的对话框中，选择“HTTP应用”，并选中所有条目，点击确定。

序号	服务名称	描述	选中
1	google网盘	GoogleDrive是美国谷歌公司推出的云存储服务	<input checked="" type="checkbox"/>
2	Skydrive网盘	SkyDrive网络硬盘是微软新近推出的在线存储服务	<input checked="" type="checkbox"/>
3	Xuite网盘	Xuite是台湾的中华电信HiNet的云端硬盘	<input checked="" type="checkbox"/>
4	115网盘	115网盘是广东一一五科技有限公司于2009年推出的网络数据在线存储服务	<input checked="" type="checkbox"/>
5	360云盘	360云盘是奇虎360开发的分享式云存储服务产品	<input checked="" type="checkbox"/>
6	百度云网盘	百度云网盘是百度推出的一项云存储服务	<input checked="" type="checkbox"/>
7	网页文档下载	word、pdf等格式文档下载	<input checked="" type="checkbox"/>
8	网页音频	网页内嵌音频	<input checked="" type="checkbox"/>
9	网页Flash	网页内嵌Flash动画	<input checked="" type="checkbox"/>
10	Facebook	Facebook 是一个联系朋友、工作伙伴、同学或其它社交圈之间的社交工具	<input checked="" type="checkbox"/>
11	Plurk(噗浪)	Plurk是一个提供基于时间轴的可视化微博客服务的多种语言支持的社交网站	<input checked="" type="checkbox"/>
12	QQ空间应用	QZone下的各种小应用和游戏，如qq农场等	<input checked="" type="checkbox"/>

如果用户的需求只需要对带宽进行限制，只需要进行流量管理设置即可，如果还需要进行行为管理，比如过滤网页关键字、检查邮件内容、过滤传输的文件等，则需要进行行为管理的设置。

4、组织管理的设置

行为管理的策略，需要到“组织结构”下启用才生效，所以我们先进行组织管理的配置。

(1) 建立组

根据实际需求，给网络的主机进行分组（系统默认是所有主机都在跟组 root 下，可以根据需要进行细分），举例将网段 192.168.20.0/24 网段的主机放在新建的“信息科”组下。

a) 先建立组名

菜单：组织管理---组织结构，点击“新增子组”



b) 在弹出的对话框中，输入组名“信息科”，其他地方的设置先不要更改，点击右上角的“确定”

新增子组		确定
组名	一行一个组名,支持汉字、数字、字母、下划线、中划线 信息科	
所属组	Root 选择	
终端绑定	继承父组配置	
上网策略	<input checked="" type="radio"/> 继承父组配置 <input type="radio"/> 使用自己的配置 不控制	
黑名单控制	<input checked="" type="radio"/> 继承父组配置 <input type="radio"/> 使用自己的配置 不控制	
准入规则	继承父组配置	
SSL代理	继承父组配置	
HTTP代理	继承父组配置	
邮件代理	继承父组配置	
认证超时(分)	<input checked="" type="radio"/> 默认配置 <input type="radio"/> 使用自己的配置	
离线用户自动删除	<input type="checkbox"/> 自动删除本组内离线时间超过指定时间的用户 指定时间: 1 <input type="radio"/> 分钟 <input type="radio"/> 小时 <input checked="" type="radio"/> 天	
公用帐号	最多允许 0 人同时使用该帐户登录,0表示不限制登录人数 超出登录数的动作: <input type="radio"/> 本次认证失败 <input type="radio"/> 注销已认证的某个登录,本次认证成功 <input checked="" type="radio"/> 使用父组配置	
快速链接 上网策略 黑名单控制		

(2)、往“信息科”组里添加用户，添加用户有很多种方式：

例如：1、手动添加，由于手动添加工作量太大，不推荐

2、扫描内网主机，由于可能有一些电脑安装防火墙软件，不允许扫描，导致扫描结果不准确，不推荐

3、通过外部认证服务器（AD 服务器或者 LDAP 服务器）导入，前提是用户需先配置好外部服务器，才可用这个方法，不推荐

4、通过设置本地认证策略，将经过设备的主机 IP 自动添加到各组中，设置使用简单方面，推荐此方法。

以第 4 种方法增加新用户步骤

a) 菜单：行为管理----认证策略，点击“新增”



c) 在弹出的对话框中，在名称栏中输入自定义的名称，在 IP 地址栏中，输入信息科主机的网段 192.168.20.0/24，认证方式一般选择以 IP 地址作为用户名，选择绑定 IP 的方式，自动添加到新建的“信息科”组下。

如果需要绑定 MAC 地址，则注意：跨网段的时候，设备无法获取主机的 MAC，需要交换机通过 SNMP 设置把 MAC 信息发送过来，SNMP 设置另作介绍。

这样就完成了对“信息科”组的配置。

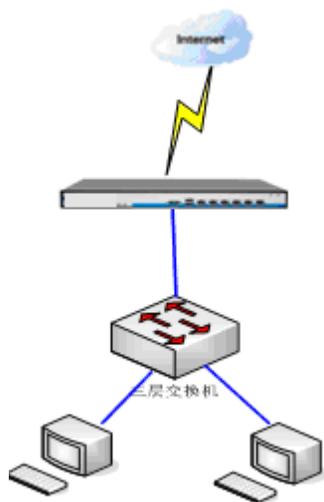
补充：SNMP 实现 IP-MAC 绑定策略的配置说明。

说明:在跨三层交换机的情况下，数据经过三层交换机后源 mac 地址都变成交换机的 mac 地址，这样导致设备识别不到内网用户的真实 mac 地址，绑定 MAC 地址也就失效了，我们可以通过 SNMP 协议读取三层交换机的 ARP 表来获取内网用户的真实 mac 地址，从而达到绑定正确 mac 地址的效果

原理：设备作为 SNMP 客户端，向三层交换机的 161 端口发送获取其 mac 地址表的请求，三层交换机作为服务端，收到请求后，回应其 mac 地址表给设备(前提是设备和三层交换机都开启了 SNMP 协议),设备将获得的 mac 地址表同设备上绑定的 mac 或者 ip+mac 的用户信息做比较,如果 mac 地址信息跟设备上绑定的信息一致,则认证通过,不一致认证失败(在有些跨三层环境下,用户同时绑定 ip+mac,而没有开启 SNMP 协议的话,那么会导致内网用户都上不了网的情况)。

配置步骤:

1. 单台三层交换机的情况



步骤 1: 开启三层交换机的 SNMP 协议,如果交换机本身已经开启 SNMP 协议则无需配置,主要是获取三层交换机的 community 值,交换机必须支持 SNMP V2 及以上的版本

华为交换机的配置命令:

Snmp-agent community read public community 值为 public

Snmp-agent sys-info version all 支持 snmp 所有版本

配置这 2 条命令即可

思科交换机的配置命令:

Cdp run

Snmp-server community public ro

步骤 2: 开启设备的 SNMP 协议

在“行为管理-认证选项-SNMP 设置”页面进行相关参数的配置,如下图:

SNMP 服务器列表: IP 和 mac 填写的为三层交换机离设备最近的接口 ip 和 mac 地址

Oid: 填示例中.1.3.6.1.2.1.4.22.1.2 或 .1.3.6.1.2.1.3.1.1.2 都可以

Community 和三层交换机配置的值对应就可以

配置好 SNMP 协议以后,在“行为管理-认证策略”页面配置认证方式为新用户以 mac 地址加到组织结构,绑定 mac 或者 ip+mac。如果用户已经配置了新用户以 IP 加入组织结构,现在想修改成 绑定 ip+mac,在修改策略完成后,必须在“行为管理-在线用户页面”,先把所有用户强制下线,然后绑定所有用户的 ip 和 mac 地址,因为之前没开启 snmp 协议,上线的用户学习到的 mac 地址都是交换机的 mac,必须强制所有用户下线,重新学习用户的 mac 地址,如下图:

修改认证策略 确定 返回

名称	ad
IP地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 <input type="radio"/> 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)
认证方式	<input type="radio"/> 新用户以IP地址作为用户名 <input checked="" type="radio"/> 新用户以MAC地址作为用户名 <input type="radio"/> 新用户以主机名作为用户名 <input type="radio"/> 新用户以 VLAN ID 作为用户名 <input type="radio"/> 到服务器去认证
radius 计费服务器	无
自动添加到组织结构	<input checked="" type="checkbox"/> 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: Root 选择 自动绑定: <input type="radio"/> 绑定IP <input type="radio"/> 绑定MAC <input checked="" type="radio"/> 同时绑定IP和MAC
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

在线用户 查询

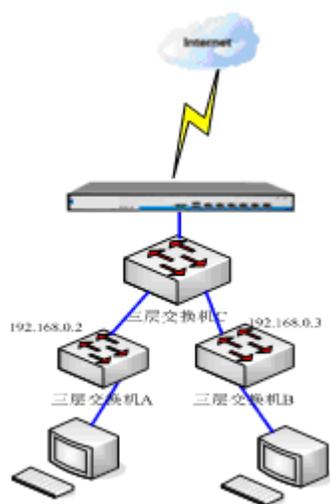
用户名	<input type="text"/>	所属组	<input type="text"/> 选择
IP地址	<input type="text"/>	MAC地址	<input type="text"/>
时间范围	<input type="text"/> - <input type="text"/>		

已认证且在组织结构中
 已认证但不在组织结构中
 未通过认证用户
 强制所有用户下线

总记录数: 15 页码: 1/1

在线用户	序号	用户名/用户组	IP地址/MAC地址	物理接口	累计在线流量(Byte)	最新速率(bps)	活跃会话数	操作
<input type="checkbox"/>	1	192.168.1.2 Root	192.168.1.2 00:50:56:a8:1c:e6	LAN1	↑459.0K, ↓892.3K	↑170.0, ↓266.0	↑3, ↓0	绑定所选用户的IP地址 绑定所选用户的MAC地址 绑定所选用户的IP和MAC地址 取消所选用户的绑定 取消全部用户的绑定 绑定全部用户的IP地址 绑定全部用户的MAC地址 绑定全部用户的IP和MAC地址
<input type="checkbox"/>	2	192.168.1.5 Root	192.168.1.5 00:50:56:a5:2c:3f	LAN1	↑4.3M, ↓6.7M	↑878.0, ↓666.0	↑0, ↓9	绑定所选用户的IP地址 绑定所选用户的MAC地址 绑定所选用户的IP和MAC地址 取消所选用户的绑定 取消全部用户的绑定 绑定全部用户的IP地址 绑定全部用户的MAC地址 绑定全部用户的IP和MAC地址

2. 多台三层交换机的情况



步骤 1: 必须开启离 pc 最近的三层交换机的 SNMP 协议 (交换机 A 和交换机 B), 其他如上述

步骤 2: 开启设备的 SNMP 协议

在“行为管理-认证选项-SNMP 设置”页面进行相关参数的配置, 如下图:



SNMP 服务器列表：IP：必须填写交换机 A 和交换机 B 的 IP

Mac:必须填写交换机 C 的 mac 地址

Oid:填示例中.1.3.6.1.2.1.4.22.1.2 或 .1.3.6.1.2.1.3.1.1.2 都可以

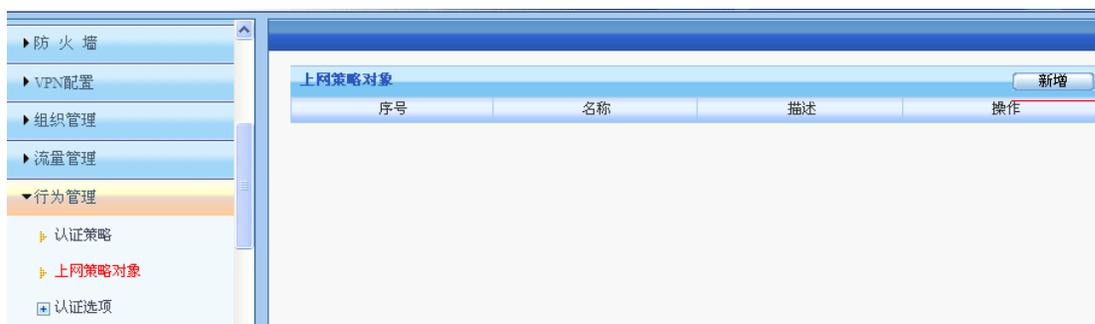
Community 和三层交换机配置的值对应就可以

5、行为管理配置

对信息科（网段 192.168.20.0/24）设置行为管策略

需求：过滤掉关键字为“法轮功”的网页

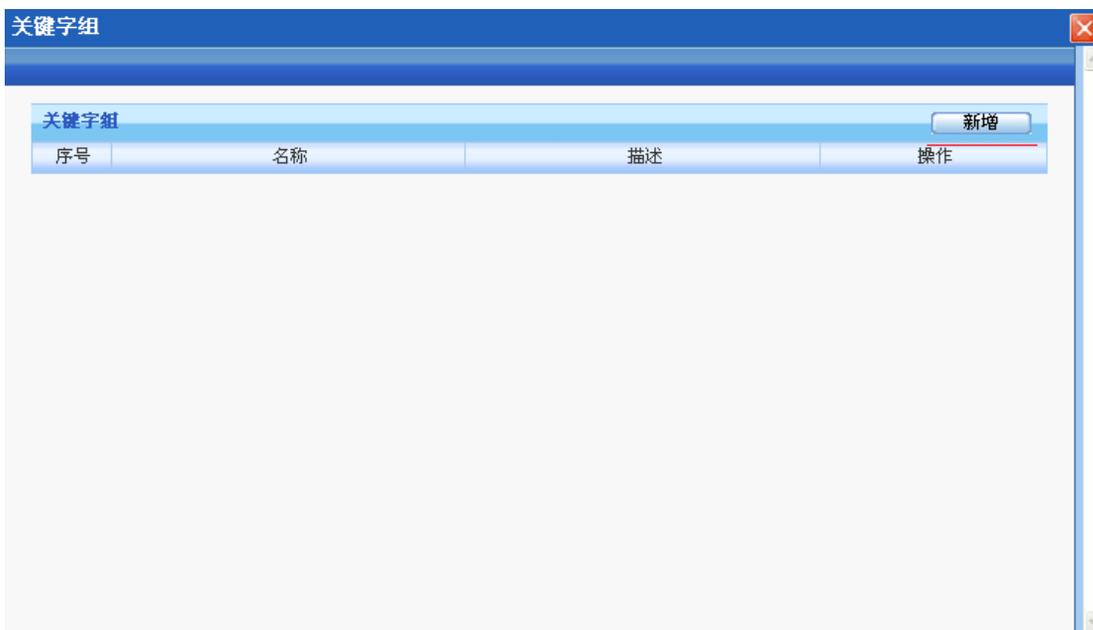
a) 菜单：行为管理—上网策略对象，点击“新增”按钮



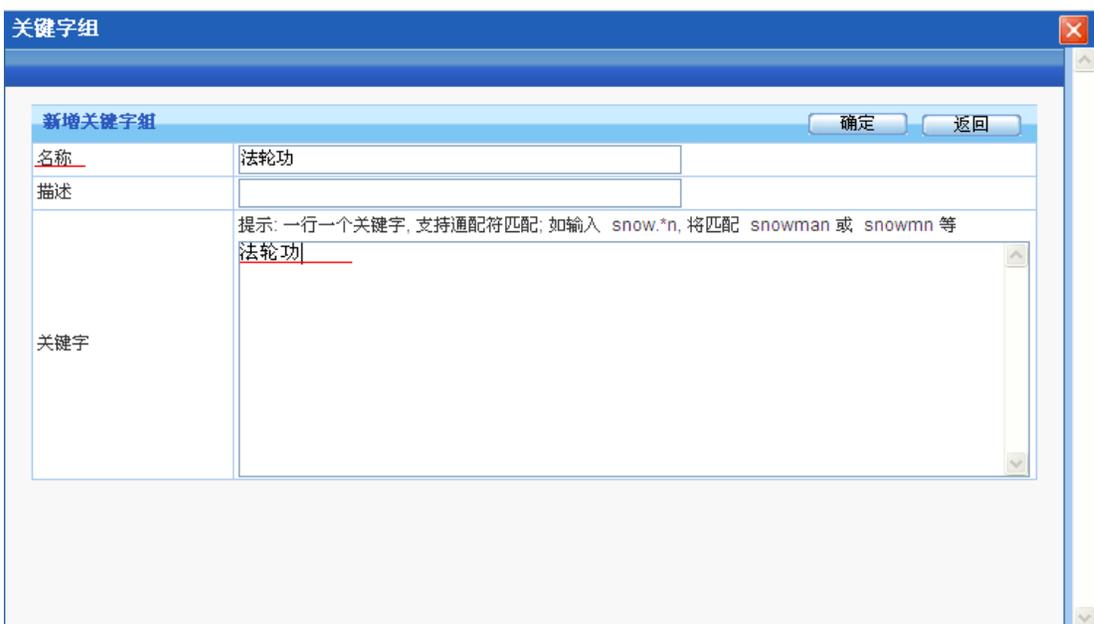
b) 在弹出的对话框中，在名称栏中输入策略名称，然后点击“关键字过滤”，再点击下边快速链接中的“关键字”



c)在弹出的对话框中，新增关键字组



d) 在名称框中输入自定义的名称，在关键字栏中输入“法轮功”，然后点击确定回到先前的对话框。



e) 返回上网策略菜单，选定“法轮功”关键字过滤。



f) 最后，到组织架构下，针对信息科启用“关键字过滤”的上网策略

修改子组	
组名	信息科
所属组	Root 选择
终端绑定	继承父组配置
上网策略	<input type="radio"/> 继承父组配置 <input checked="" type="radio"/> 使用自己的配置 关键字过滤
黑名单控制	<input checked="" type="radio"/> 继承父组配置 <input type="radio"/> 使用自己的配置 不控制
准入规则	继承父组配置
SSL代理	继承父组配置
HTTP代理	继承父组配置
邮件代理	继承父组配置
认证超时(分)	<input checked="" type="radio"/> 默认配置 <input type="radio"/> 使用自己的配置
强制继承	<input type="checkbox"/> 强制子组和所含用户继承配置
离线用户自动删除	<input type="checkbox"/> 自动删除本组内离线时间超过指定时间的用户 指定时间: <input type="text" value="1"/> <input type="radio"/> 分钟 <input type="radio"/> 小时 <input checked="" type="radio"/> 天
公用帐号	最多允许 <input type="text" value="0"/> 人同时使用该帐号登录,0表示不限制登录人数 超出登录数的动作: <input type="radio"/> 本次认证失败 <input type="radio"/> 注销已认证的某个登录,本次认证成功 <input checked="" type="radio"/> 使用父组配置

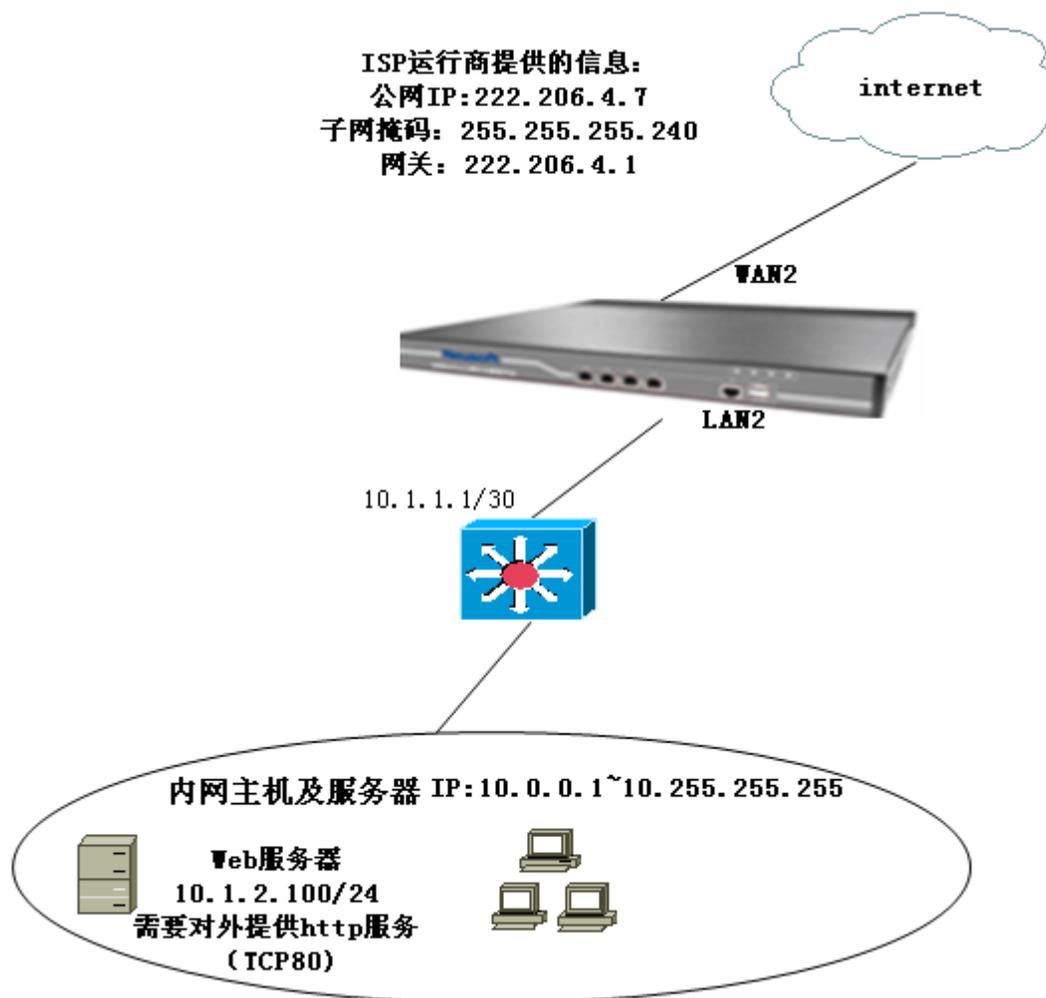
行为管理策略配置完成。

至此基本完成产品主要的功能是流量管理和行为管理，其他功能可以根据需求设置

22.2 路由模式

使用环境：客户先前没有路由器，或者想将设备当路由器使用的情况下需使用路由模式。

举例：（如下图）



实施步骤:

1、登录设备（详见网桥模式）

2、设置工作模式

(1) 点击菜单：系统配置—工作模式；即进入工作模式配置界面



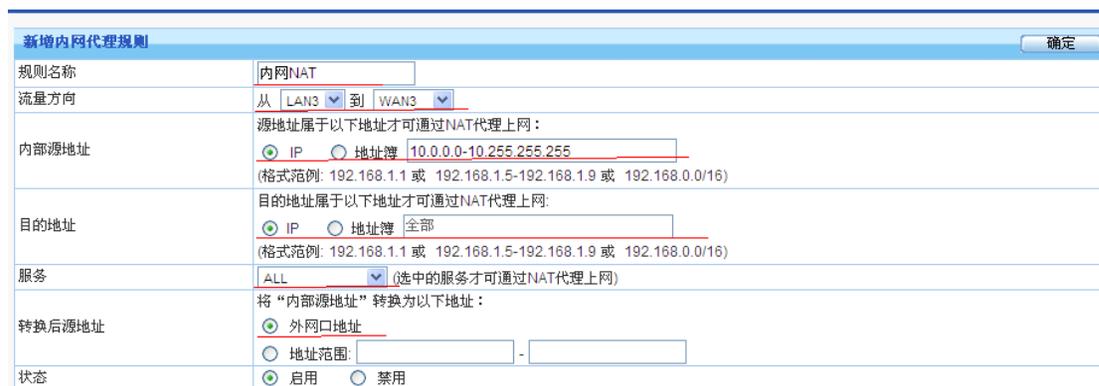
(2) 在“工作模式”栏中选择“路由模式”，在端口设置中给 WAN3 配置 IP 10.1.1.2，掩码 255.255.255.252，给 LAN3 配置 IP 222.106.4.7，掩码 255.255.255.240，并点击确认。

3、设置 NAT 规则

(1) 点击菜单：防火墙—NAT 规则—内网代理，点击“新增”



- (2) 在弹出的对话框中，在规则名称栏中输入自定义的名称，流量方向为 LAN3 到 WAN3,内部 IP 为 10.0.0.0-10.255.255.255(或者保存原来的配置，即为全部 IP)，目的地址及服务为“全部”（不做配置），转换后地址为“外网口地址”。



- (3) 设置端口映射，将内网 Web 服务器的 TCP80 端口映射成功公网 IP222.206.4.7 的 TCP80 端口。菜单：防火墙——NAT 规则——端口映射，点击“新增”



- (4) 在弹出的对话框中，在规则名称栏输入自定义的名称，外网口选择 WAN3，内部地址 10.1.2.100，对外映射地址选择外网口地址，协议号选择 TCP，内部端口为 80，对外映射端口为 80，点击确定即可。

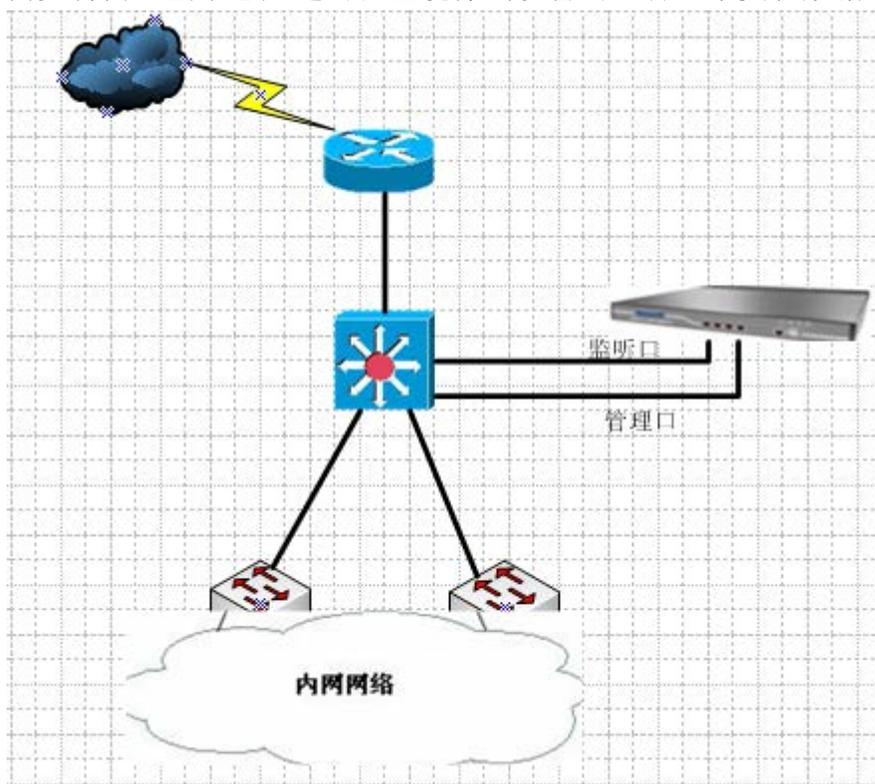
新增端口映射规则		确定
规则名称	Web	
外网口	WAN3 (从该端口进来的数据流才转换)	
内部地址	10.1.2.100 (单个IP, 如 192.168.5.3)	
对外映射地址	<input checked="" type="radio"/> 外网口地址	
协议号	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	
内部端口	80 - 80 (与“对外映射端口”一一对应)	
对外映射端口	80 - 80 (与“内部端口”一一对应)	
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	

至此网络基础设置完成，先检查能内网主机能否正常上网，能正常上网再进行流量管理及行为管理的设置。

说明：路由模式与网桥模式的流量管理、行为管理设置跟网桥模式下的流量管理、行为管理一样，这里不再阐述。

22.3 旁路模式

使用环境:在客户网络环境已经定型，要求在现有网络环境下不改变任何配置和拓扑架构，能够实现对数据进行审计，对现有网络不造成任何影响，则可以使用旁路模式。旁路模式需要将内网当中感兴趣的流量镜像到设备的监听口来实现数据监听，具体拓扑如图；



为了避免监听口流量过大造成线路拥塞，设备使用两个口来相连，比如 LAN1 做监听，WAN1 做管理。

实施步骤

- 1、登录设备（详见网桥模式）。
- 2、设置工作模式

(1) 点击菜单：系统配置—工作模式；即进入工作模式配置界面

设备工作模式

工作模式： 网桥模式 路由模式 旁路模式 (改变工作模式，将会清除所有静态路由)

>>旁路配置<<

端口配置	接口	IP地址	子网掩码	格式范例
LAN1	IP地址:			格式范例: 16 或 255.255.0.0
WAN1	IP地址:	192.168.0.100	子网掩码: 24	格式范例: 16 或 255.255.0.0
LAN2	IP地址:			格式范例: 16 或 255.255.0.0
WAN2	IP地址:			格式范例: 16 或 255.255.0.0

网关IP: 192.168.0.254

监控网段列表: 192.168.0.0/16, 172.16.0.0/16, 10.0.0.0/8

阻断物理接口: 无 (HUB做镜像时，无需配置阻断物理接口；交换机镜像口不具备业务转发的条件下，旁路认证阻断接口与交换机另一物理接口相连，完成旁路认证功能)

DNS劫持: 启用 禁用 (旁路认证时，一些认证客户端需要开启DNS劫持，才能弹出认证界面)

快速链接: [静态路由](#) [内网代理](#)

工作模式仅用于初次网络部署，对它的任何修改操作将清除所有静态路由，可在【网络配置】-【配置IP地址】配置多个接口IP，在【网络配置】-【静态路由】修改0.0.0.0/0的静态路由来修改缺省网关。

(2) 在工作模式栏中，选择“旁路模式”；

(3) 配置管理口：在任一接口设置做为管理的 IP 地址即可。

(4) 配置监听口：在设定工作模式为旁路模式后，设备上所有的网络接口即成为监听接口，监听口不需配置 IP 地址，为了避免监听口流量过大造成线路拥塞，建议监听口与管理口分开，即使用除管理口外的独立网络接口做为监听口。

(5) 阻塞物理端口，一般选择无（HUB，交换机开启镜像会自动将数据转发过来），只有一种情况下需要开启阻塞某个端口，即做旁路模式下做旁路认证，审计认证服务器上面的用户名，通过阻塞设备某个网口的数据转发来实现监听并学习服务器返回过来的用户名

(6) DNS 劫持，选择禁用，只有一种情况下需要开启阻塞某个端口，即做旁路模式下做旁路认证，审计认证服务器上面的用户名，通过阻塞设备某个网口的数据转发来实现监听并学习服务器返回过来的用户名

注

默认只附件审计只能审计 1M,如需审计跟大请按图下进行设置

比如将文件大小审计设置成 100M

审计策略 审计选项

审计选项

审计方式: 全部审计

会话审计方式: 只审计有效会话 全部审计

文件大小上限: 100 M(1-4000)

访问网站日志记录选项:

- 优化日志记录
- 仅记录含有网页标题的访问
- 仅记录到网站根目录的访问
- 记录所有网页访问
- 但不记录以下类型的访问

 (提示: 一行一个文件类型, 格式为"后缀名", 如 .zip)

至此旁路模式的设置以完成，内置报表及实时状态将出现数据审计，在旁路模式下，无法对网络进行流量管理、行为管理等控制，只能基于 IP/MAC/计算机名/用户名查看网络使用情况，详细的审计配置请参见手册中“上网审计策略”模块的配置说明。



交换机配置

Cisco (锐捷、神马等等其他小厂商基本按这套)
以 2950/3750 为列 (其他型号请参照相关资料配置)

```

C:\ Telnet 192.168.0.2

interface FastEthernet0/24
?
interface Vlan1
 ip address 192.168.0.2 255.255.255.0
 no ip route-cache
?
 ip default-gateway 192.168.0.253
 ip http server
?
 line con 0
 line vty 0 4
  exec-timeout 0 0
  privilege level 15
  password netsys
  login
 line vty 5 15
  login
?
?
?
 monitor session 1 source interface Fa0/8
 monitor session 1 destination interface Fa0/1
 end

Switch#

```

monitor session 1 source interface f0/8 //定义被监听的端口 (及镜像端口)

monitor session 1 destination interface f0/1 //定义接分析工具的端口 (行为管理监听口 (即监听端口))

华为、华三配置

以 3550/5700/为列

```
vlan batch 5 8 to 12 14 to 15 100 200 to 201
#
cluster enable
ntdp enable
ntdp hop 16
ndp enable
#
dhcp enable
#
undo http server enable
#
drop illegal-mac alarm
#
observe-port 1 interface GigabitEthernet0/0/1
#
```

observe-port 1 interface GigabitEthernet0/0/1 ///定义接分析工具的端口（行为管理监听口（即监听端口）

```
bpdu enable
#
interface GigabitEthernet0/0/4
ntdp enable
ndp enable
bpdu enable
port-mirroring to observe-port 1 both
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 172.16.161.100
"
```

port-mirroring to observe-port 1 both //定义被监听的端口（及镜像端口）