

目录

AC1.9 对常见工具的控制.....	1
本文说明.....	1
第一部分 对常见工具的封堵.....	1
一、新建上网策略.....	1
二、关联策略到用户或用户组.....	5
三、调整用户或用户组的策略执行顺序.....	7
第二部分 对 P2P、P2P 流媒体的流控.....	9
一、配置线路带宽.....	9
二、配置流控策略.....	10
三、启用流量管理系统.....	11

AC1.9 对常见工具的控制

本文说明

本文主要介绍 AC1.9 版本对常见工具的控制,常见工具包括了 P2P、P2P 流媒体、下载工具、炒股软件、webmail 等。介绍主要分为两部分:第一部分:对 P2P、P2P 流媒体、下载工具、炒股软件、webmail 等常见工具的封堵,和第二部分:对 P2P、P2P 流媒体的流控。

第一部分 对常见工具的封堵

1.9 版本封堵常见工具的配置步骤为:

首先,新建上网策略对象,配置相应的封堵规则;

然后,关联策略到用户或者用户组;

最后,调整用户或用户组的策略执行顺序,保证新配置的策略会执行,不会因为与其他策略冲突而失效。

对 P2P、P2P 流媒体、下载工具、炒股软件、webmail 等常见工具的封堵,除了在配置策略时候不同外,其他的配置步骤都是一样的,下文主要详细描述策略的配置,而策略的关联和调整只做举例说明。

一、新建上网策略

1、以 admin 账户登陆设备控制台后,在上网行为管理---上网策略对象中,新增上网策略,如下图。



一条上网策略可以关联到多个组织结构中的用户或用户组，同时一个用户或用户组可以关联多条上网策略，但是这里需要注意的是，默认情况下一个用户或用户组最多可以关联 10 条上网策略。

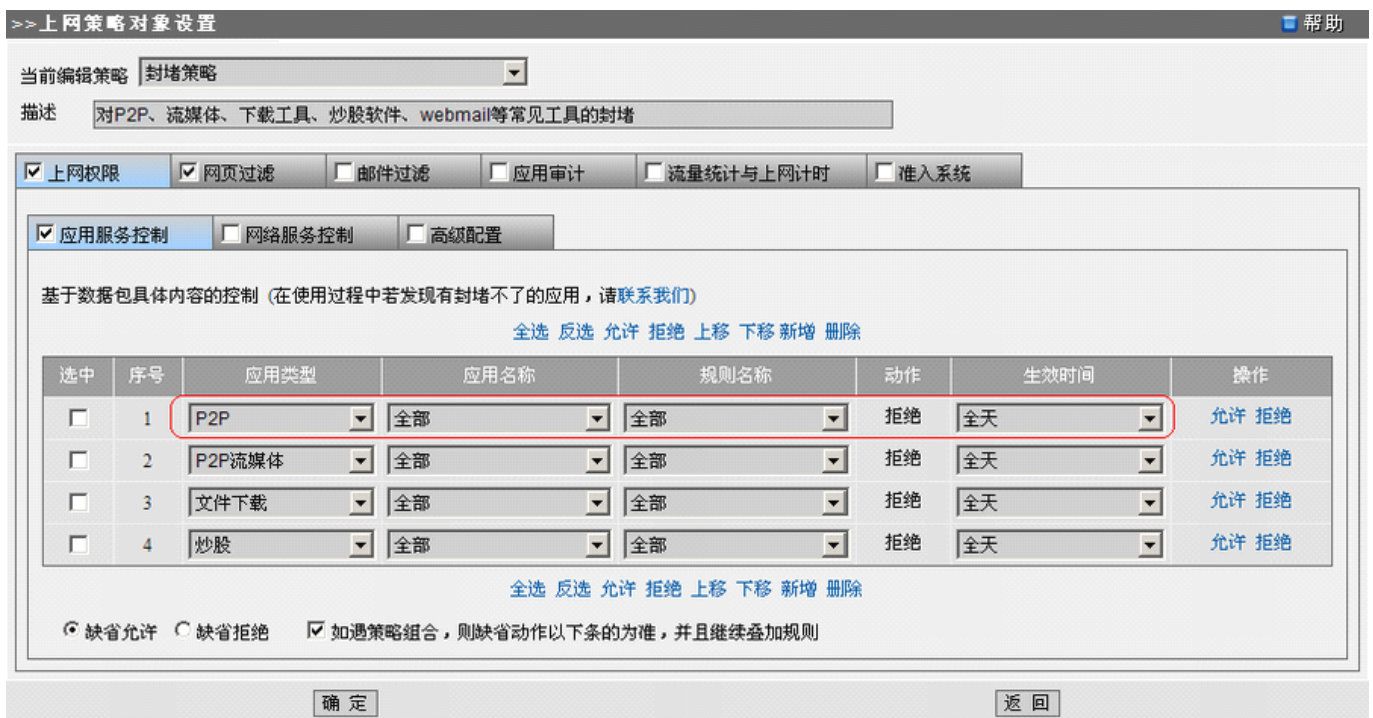
当一个用户或用户组关联到多条上网策略时，会有一个执行上的顺序。同在策略冲突的时候，会有一个处理机制，下文会对这部分做详细解释，所以首次配置策略时，建议尽量将规则配置在同一条策略中，避免策略的冲突对您的配置造成困扰。

2、配置封堵 P2P、P2P 流媒体、下载工具、炒股软件、webmail 等常见工具的策略：

1) 封堵 P2P：

目前最常用的封堵 P2P 的方法是通过应用识别规则去封堵常见的 P2P 网络行为特征来实现的。

配置方法如下图，在策略对象的上网权限---应用服务控制中，点击新增，选择应用类型为 P2P，应用名称为全部，规则名称为全部，动作为拒绝，生效时间为全天，然后点击确认新增，最后点击页面最下方的确定。



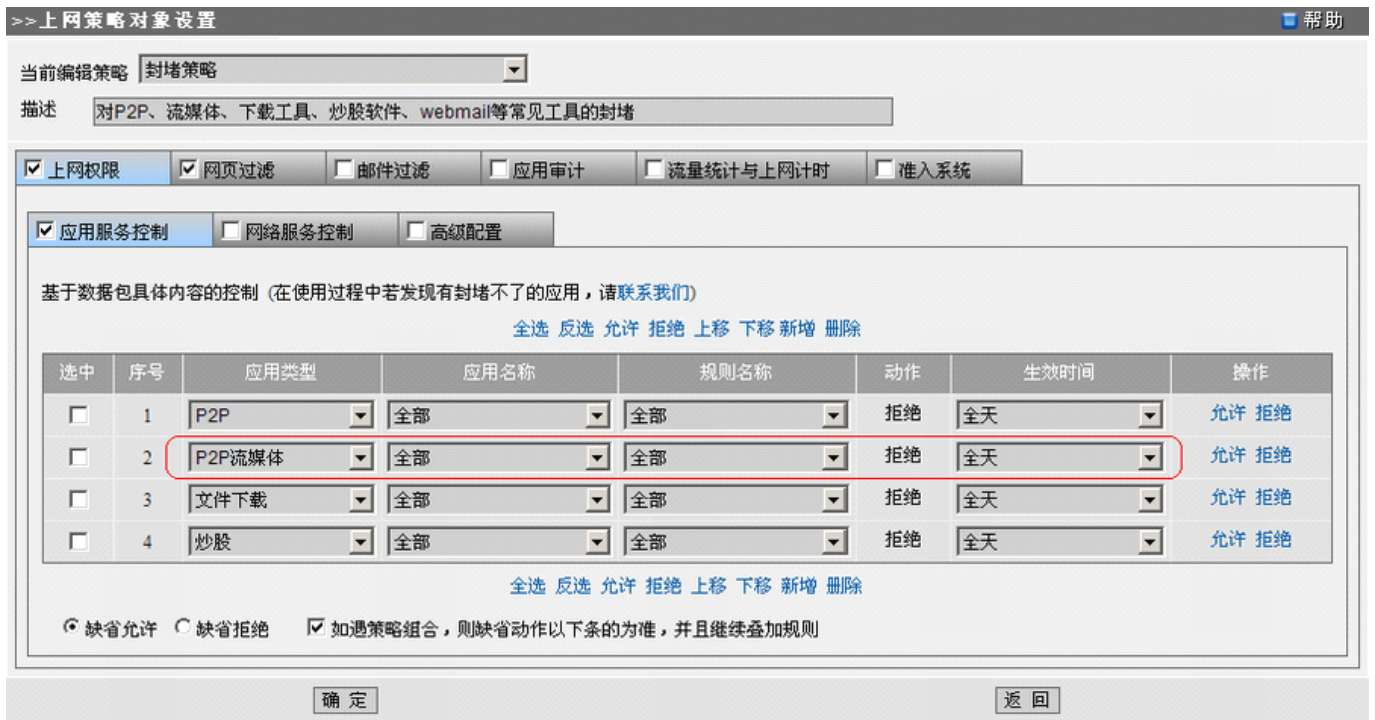
注意：这里的应用名称是可以针对需要封堵的应用来选择的，如只要求封堵 P2P 中的 skype 应用，则需要选择应用名称为 skype，其他的配置保持默认即可达到只封堵 skype 行为的目的。

2) 封堵 P2P 流媒体：

目前最常用的封堵 P2P 流媒体的方法是通过应用识别规则去封堵常见 P2P 流媒体的网络行为特征来实现的。

配置方法如下图，在策略对象的上网权限---应用服务控制中，点击新增，选择应用类型为 P2P 流媒体，应用名称为全部，规则名称为全部，动作为拒绝，生效时间为全天，然后点击确认新增，最后点击页面最下方的确定。

确定。

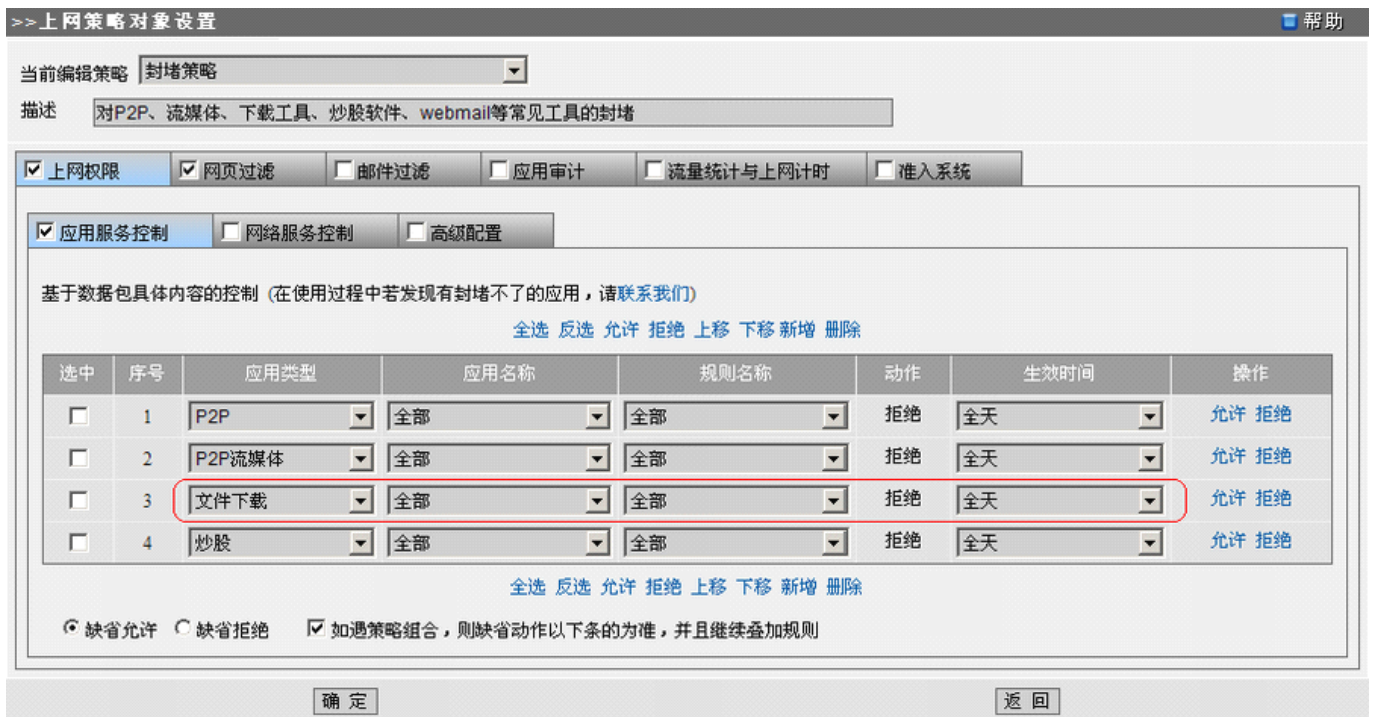


注意：这里的应用名称是可以针对需要封堵的应用来选择的，如只要求封堵 P2P 流媒体中的迅雷看看的应用，则选择应用名称为迅雷看看，其他的配置保持默认即可达到只封堵迅雷看看的目的。

3) 封堵下载工具：

目前最常用的封堵下载工具的方法是通过应用识别规则去封堵常用下载工具的网络行为特征来实现的。

配置方法如下图，在策略对象的上网权限——应用服务控制中，点击新增，选择应用类型为文件下载，应用名称为全部，规则名称为全部，动作为拒绝，生效时间为全天，然后点击确认新增，最后点击页面最下方的确定。



注意：这里的应用名称是可以针对需要封堵的应用来选择的，如只要求封堵文件下载中的迅雷资源的应用，则选择应用名称为迅雷资源，其他的配置保持默认即可达到只封堵迅雷资源的下载的目的。

4) 封堵炒股软件:

目前最常用的封堵炒股软件的方法是通过应用识别规则去封堵常见炒股软件的网络行为特征来实现的。

配置方法如下图, 在策略对象的上网权限——应用服务控制中, 点击新增, 选择应用类型为炒股, 应用名称为全部, 规则名称为全部, 动作为拒绝, 生效时间为全天, 然后点击确认新增, 最后点击页面最下方的确定。

The screenshot shows the 'Internet Policy Object Settings' window. The current strategy is 'Blocking Strategy'. The description is 'Blocking common tools like P2P, streaming media, download tools, stock trading software, and webmail'. Under 'Application Service Control', the 'Application Service Control' tab is selected. A table lists rules for blocking applications:

选中	序号	应用类型	应用名称	规则名称	动作	生效时间	操作
<input type="checkbox"/>	1	P2P	全部	全部	拒绝	全天	允许 拒绝
<input type="checkbox"/>	2	P2P流媒体	全部	全部	拒绝	全天	允许 拒绝
<input type="checkbox"/>	3	文件下载	全部	全部	拒绝	全天	允许 拒绝
<input type="checkbox"/>	4	炒股	全部	全部	拒绝	全天	允许 拒绝

At the bottom, there are radio buttons for 'Default Allow' (selected), 'Default Deny', and a checked option 'If strategy combination, then default action is based on the following rules, and continue to add rules'. Buttons for 'Confirm' and 'Return' are at the bottom.

注意: 这里的应用名称是可以针对需要封堵的应用来选择的, 如只要求封堵软件中的大智慧软件, 则选择应用名称为大智慧, 其他的配置保持默认即可达到, 只封堵大智慧这个炒股软件的目的。

以上规则封堵的是常用的一些炒股软件, 如果封堵效果不是很好, 可以尝试封堵炒股网站的 url 地址。

封堵股票交易网站的 url 地址的方法: 如下图, 在策略对象的网页过滤——url 过滤中, 点击未生效的 URL 组, 选中规则-股票交易, 动作为拒绝, 点击生效, 最后点击页面下方的确定。

The screenshot shows the 'Internet Policy Object Settings' window. The current strategy is 'Blocking Strategy'. The description is 'Blocking common tools like P2P, streaming media, download tools, stock trading software, and webmail'. Under 'Web Filtering', the 'URL Filtering' tab is selected. A table lists URL filtering rules:

选中	序号	名称	描述	动作	生效时间	操作
<input type="checkbox"/>	1	Web邮件	提供Webmail服务的网站	拒绝	全天	允许 拒绝
<input type="checkbox"/>	2	股票交易	提供股票基金信息的网站	拒绝	全天	允许 拒绝

At the bottom, there are radio buttons for 'Default Allow' (selected), 'Default Deny', and a checked option 'If strategy combination, then default action is based on the following rules, and continue to add rules'. Buttons for 'Confirm' and 'Return' are at the bottom.

5) 封堵 webmail:

目前最常用的封堵 webmail 的方法是通过封堵大型门户网站的邮件服务器的 URL 地址来实现的。

配置方法如下图, 在策略对象的网页过滤——url 过滤中, 点击未生效的 URL 组, 选中规则-Web 邮件, 动作为拒绝, 点击生效, 最后点击页面下方的确定。



二、关联策略到用户或用户组

在上网行为管理——组织结构中, 选择策略需要关联到的用户或用户组, 点击该组或该用户的上网策略列表选项卡, 点击添加策略, 选择之前新建的上网策略, 点击添加, 最后点击页面下方的确定。

如下图, 对组织结构关联新建的封堵策略, 其效果是属于根组 (root 组) 的用户上网时会去匹配该条上网策略。



如果想要使客服组、销售组、行政组、主管组都会去匹配该条上网策略, 有 2 种配置方法, 一种是强制子组继承, 另一种是使用父组策略。两者的区别如下图, 配置方法见下文:

	策略特征	子组是否可以新增策略	规则配置位置
强制子组继承	继承父组指定策略	可以新增, 继承的父组策略最优先	在父组配置
使用父组策略	完全使用父组策略	不可以新增	在子组配置

- **强制子组继承的配置方法:** 在父组的上网策略列表选项卡中, 勾选需要子组继承的策略栏里相应的强制

子组继承的勾，并点击确定，即可实现对父组中包含的所有的子组都强制其继承父组的该条策略。

1、如下图中可以看到，对根组(root 组)的策略——【封堵策略】勾选了强制子组继承。

组名	root
所属组路径	/
描述	
创建属性	管理员创建
组信息	子组个数:4,用户个数:0

提交

组织成员及上网策略设置

成员列表 上网策略列表

全选/反选	策略对象	强制子组继承(或被强制继承)	
<input type="checkbox"/>	封堵策略	<input checked="" type="checkbox"/>	对P2P、流媒体、

添加策略 上移 下移 删除

确定

2、如下图中可以看到，客服组属于根组，该组继承了由根组强制子组继承的策略——【封堵策略】。

注意，该组除了被强制继承的策略外，还可以关联其他的策略，但是由父组继承的策略是最优先执行的，是无法通过下移来修改该策略的执行顺序的。

组名	客服
所属组路径	/
描述	
创建属性	管理员创建
组信息	子组个数:0,用户个数:0

提交

组织成员及上网策略设置

成员列表 上网策略列表

使用父组策略

全选/反选	策略对象	强制子组继承(或被强制继承)	
<input type="checkbox"/>	封堵策略	<input checked="" type="checkbox"/>	对P2P、
<input type="checkbox"/>	客服策略	<input type="checkbox"/>	

添加策略 上移 下移 删除

确定

➤ **使用父组策略的配置方法：**在子组的上网策略列表选项卡中，勾选使用父组策略，并点击确定，即可实现该子组完全继承和使用父组的所有策略。

如下图可以看出，销售组也是属于根组的，该组在勾选了使用父组策略后，该组可以关联策略全部都是由父组继承下来的——【封堵策略】，本组不可以再新增别的策略，也无法调整策略的执行顺序。

此时如果父组有新增、修改、删除自己的策略，子组的策略也是会一并由父组完全继承下来。

组名	销售
所属组路径	/
描述	
创建属性	管理员创建
组信息	子组个数:0,用户个数:0

提交

组织成员及上网策略设置

成员列表 上网策略列表

<input checked="" type="checkbox"/> 使用父组策略	
全施/反施	策略对象
<input type="checkbox"/> 封堵策略	<input checked="" type="checkbox"/> 强制子组继承(或被强制继承)

添加策略 上移 下移 删除

确定

三、调整用户或用户组的策略执行顺序

一个用户或用户组可以关联到多条策略，多条策略之间存在一定的执行顺序，是由上向下执行的。

如下图可知，当一个用户或用户组关联到策略 1、策略 2、策略 3 时，策略执行顺序是：第一步执行策略 1 的网络服务控制，第二步执行策略 2 的网络服务控制，第三步执行策略 3 的网络服务控制，第四步执行策略 1 的应用服务控制，第五步执行策略 2 的网络服务控制，以此类推，依此执行下去。



下文以客服组的策略配置为例做说明。

如下图：对客服组关联了两条上网策略：【客服策略】和【封堵策略】，置顶的策略是【客服策略】。

组名	客服
所属组路径	/
描述	
创建属性	管理员创建
组信息	子组个数:0,用户个数:0

组织成员及上网策略设置

使用父组策略

全选/反选	策略对象	强制子组继承(或被强制继承)	描述
<input type="checkbox"/>	客服策略	<input type="checkbox"/>	允许文件下载
<input type="checkbox"/>	封堵策略	<input type="checkbox"/>	对P2P、流媒体、下载工具、炒股软件、webmail等常见工具的封堵

其中，【客服策略】是允许文件下载的，其他的策略为缺省允许。

当前编辑策略

描述

上网权限
 网页过滤
 邮件过滤
 应用审计
 流量统计与上网计时
 准入系统

应用服务控制
 网络服务控制
 高级配置

基于数据包具体内容的控制 (在使用过程中若发现有封堵不了的应用, 请联系我们)

[全选](#)
[反选](#)
[允许](#)
[拒绝](#)
[上移](#)
[下移](#)
[新增](#)
[删除](#)

选中	序号	应用类型	应用名称	规则名称	动作	生效时间	操作
<input type="checkbox"/>	1	文件下载	全部	全部	允许	全天	允许 拒绝

[全选](#)
[反选](#)
[允许](#)
[拒绝](#)
[上移](#)
[下移](#)
[新增](#)
[删除](#)

缺省允许
 缺省拒绝
 如遇策略组合, 则缺省动作以下条的为准, 并且继续叠加规则

而，【封堵策略】是封堵了文件下载、P2P、P2P 流媒体、炒股软件、webmail 的，其他的策略为缺省允许。

当前编辑策略 **封堵策略**

描述 **对P2P、流媒体、下载工具、炒股软件、webmail等常见工具的封堵**

上网权限
 网页过滤
 邮件过滤
 应用审计
 流量统计与上网计时
 准入系统

应用服务控制
 网络服务控制
 高级配置

基于数据包具体内容的控制 (在使用过程中若发现有封堵不了的应用, 请联系我们)

[全选](#)
[反选](#)
[允许](#)
[拒绝](#)
[上移](#)
[下移](#)
[新增](#)
[删除](#)

选中	序号	应用类型	应用名称	规则名称	动作	生效时间	操作
<input type="checkbox"/>	1	P2P	全部	全部	拒绝	全天	允许 拒绝
<input type="checkbox"/>	2	P2P流媒体	全部	全部	拒绝	全天	允许 拒绝
<input type="checkbox"/>	3	文件下载	全部	全部	拒绝	全天	允许 拒绝
<input type="checkbox"/>	4	炒股	全部	全部	拒绝	全天	允许 拒绝

[全选](#)
[反选](#)
[允许](#)
[拒绝](#)
[上移](#)
[下移](#)
[新增](#)
[删除](#)

缺省允许
 缺省拒绝
 如遇策略组合, 则缺省动作以下条的为准, 并且继续叠加规则

由于客服组关联到两条策略, 于是就会按照上文中所说的顺序进行匹配策略, 执行相关规则。

但是这里有一点需要注意的是, 当规则执行到缺省策略时, 如果未勾选【如遇策略组合, 则缺省动作以下条的为准, 并且继续叠加规则】, 则会直接匹配该条策略规则的缺省策略, 而不会匹配到下条策略的同一规则项。例如: 【客服策略】是允许文件下载的, 但是没有勾选该项, 那么两条策略组合的结果就是文件下载是允许的, 同时【封堵策略】里对 P2P、P2P 流媒体、炒股软件、webmail 等的拒绝也会被允许。所以这个勾要不要勾选是需要慎重处理的操作。

第二部分 对 P2P、P2P 流媒体的流控

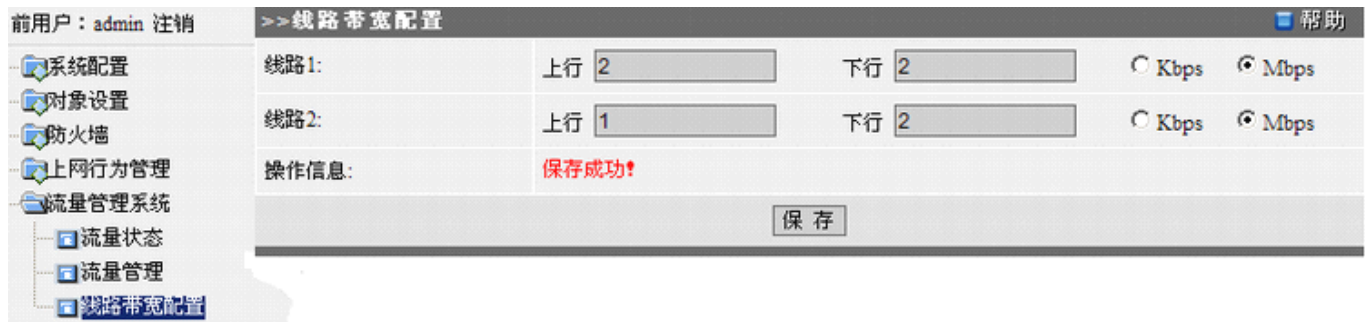
对内网用户上网行为的流控配置方法如下:

首先, 配置线路带宽; 然后, 配置流控策略; 最后, 启用流量管理系统。

下文将以 P2P、P2P 流媒体为例做流控配置方法的介绍。

一、配置线路带宽

在流量管理系统——线路带宽配置里, 配置已有线路的实际带宽值。这里线路带宽配置填写要求必须为实际值的原因是: 在流量管理系统中, 带宽的百分比是以此为依据来计算的, 如果填写错误会导致流控不准确。



注意，这里的线路带宽的单位有 Kbps 和 Mbps 两种，这个单位是跟运营商提供的线路带宽单位相同的。

而在流量管理系统中流控规则配置的时候，带宽的单位是 KB/s，这 2 个单位是不同的，两者间存在 8 倍的关系，即 $1\text{Mbps}=1024\text{Kbps}=(1024\div 8)\text{KB/s}=128\text{KB/s}$ 。

二、配置流控策略

如下图，在流量管理系统——流量管理中，点击新增，新建流控策略。



对客服组的用户针对 P2P、P2P 流媒体做带宽限制，限制带宽为总带宽的 10%。策略配置如下：

- **【自定义服务】**：选择为 P2P 和 P2P 流媒体。注意，这里服务同时选择了 P2P 和 P2P 流媒体时，是对这两个服务合起来一起做限制，2 个服务之间带宽分配关系是相互竞争的。如果需要对不同的服务限制不同的通道大小，则需要分别新建规则来做限制。
- **【选择对象】**：可以选择组也可以选择用户，支持多选。但是目前 AC1.9 版本选择用户时必须手动填写正确的用户名。
- **【带宽通道类型】**：要控制 P2P 和 P2P 流媒体占用线路带宽大小，则要选择类型为限制通道。
- **【最大上行带宽和最大下行带宽】**：根据内网的实际限制值做配置，可以填写线路带宽的百分比，也可以直接填写带宽值的大小，单位为 KB/s。
- **【限制单用户最高带宽】**：根据单用户带宽限制的峰值来填写。注意这个是针对匹配了该条策略的所有在线用户做的限制，属于该组但是不在线用户不受限制。
- **【生效时间】**：流控规则的生效时间范围。在对象设置的时间计划中配置时间范围，然后在此处选择即可。
- **【生效线路】**：只有一条外网线路时，只可以选择为线路 1。一次只能选择一条生效线路。如果要选择多条线路都生效，需要以本条为模板再配置一条选择其他线路的流控策略。
- **【目标 IP 组】**：指提供该项网络服务的服务器的 IP 段，该 IP 段多数为公网地址段。在对象设置的 ip

组中配置，然后在此处选择即可。

➤ **【启用通道】**：是否立刻启用流控策略。对于暂时无需使用的流控策略可以禁用之。

>> 带宽通道编辑 帮助

格式：一行一个通道名称,不能与已存在的通道重名.

通道名称:

适用服务与应用 所有 自定义

服务类型	服务名称	操作	选中
P2P	全部	编辑	<input type="checkbox"/>
P2P流媒体	全部	编辑	<input type="checkbox"/>

全选 反选 新增 删除

适用对象 所有 自定义

选择对象:

已选组

已选用户

提示：已选组和已选用户是或的关系，通道的生效对象包括已选的组以及已选的用户，需要单独选择用户时，请在上面的输入框中输入用户名，每行一个用户名

带宽通道类型: 保证通道 限制通道

最大上行带宽: % KB/s - 需要借用别的通道的空闲带宽

最大下行带宽: % KB/s - 需要借用别的通道的空闲带宽

用户间带宽分配策略: 公平分配 - 提示：不同用户的数据在通道内采用轮转调度的方式，轮流得到发送机会，以公平地使用该通道的带宽

限制单用户最高带宽: 启用 上行 KB/s 下行 KB/s

生效时间:

生效线路:

目标IP组:

启用通道: 启用 禁用

注意：流控策略是对在线用户列表中用户生效的，不在线用户是不会匹配流控规则的。

三、启用流量管理系统

如下图，在流量管理系统——流量管理中，点击启用流量管理系统。



此时只要存在启用状态的流控策略，用户一旦匹配上了流控策略，那么该用户超过了限制值的占用带宽的数据包就会被设备延迟发送，以达到流控的目的。