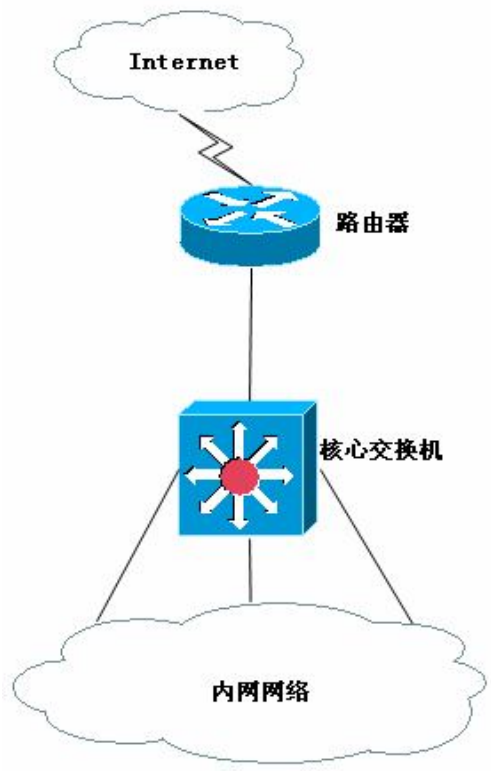
配置实例参考

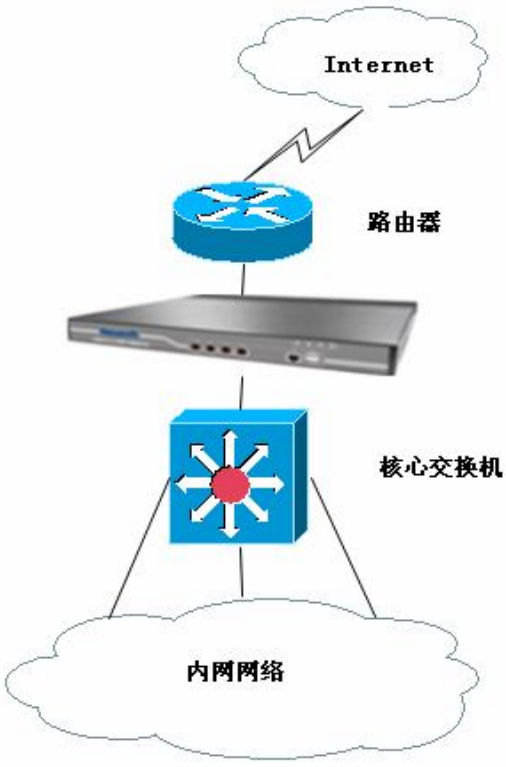
说明：NIBC 大部分情况下使用网桥模式，有时候用到路由模式

一、 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 NIBC 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。



NIBC放置前网络拓扑



NIBC放置后网络拓扑

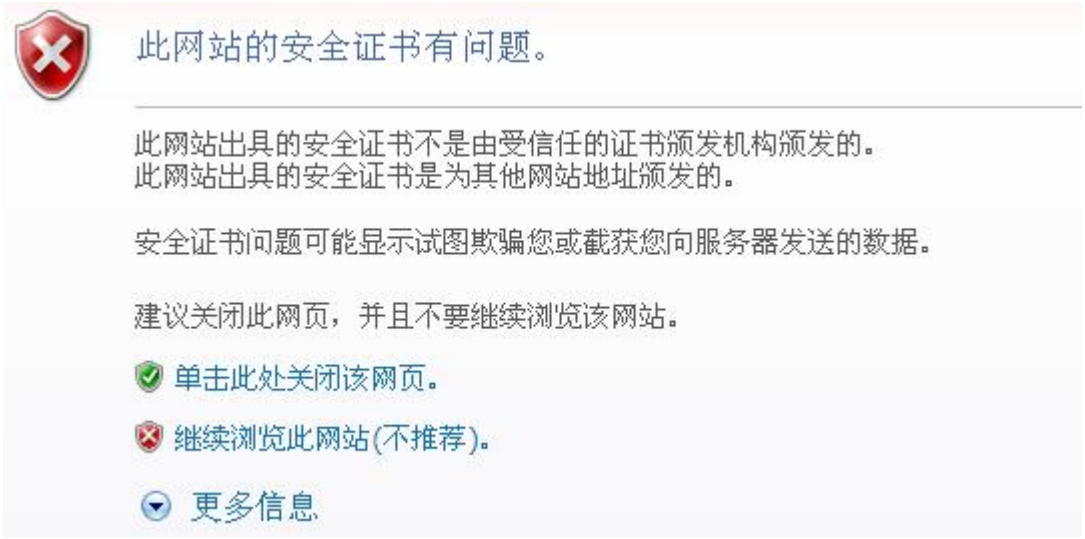
实施步骤

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 NIBC 的 LAN0 口（或者 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 NIBC。

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 NIBC）

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”.

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。

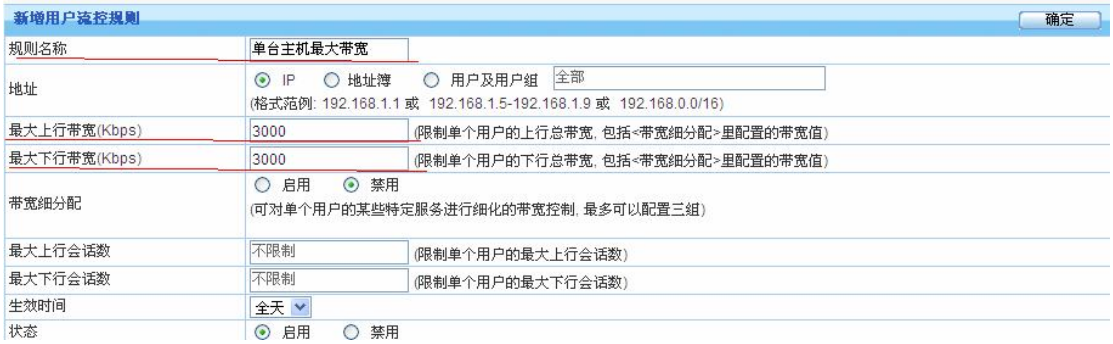
5、配置基于用户的流控

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

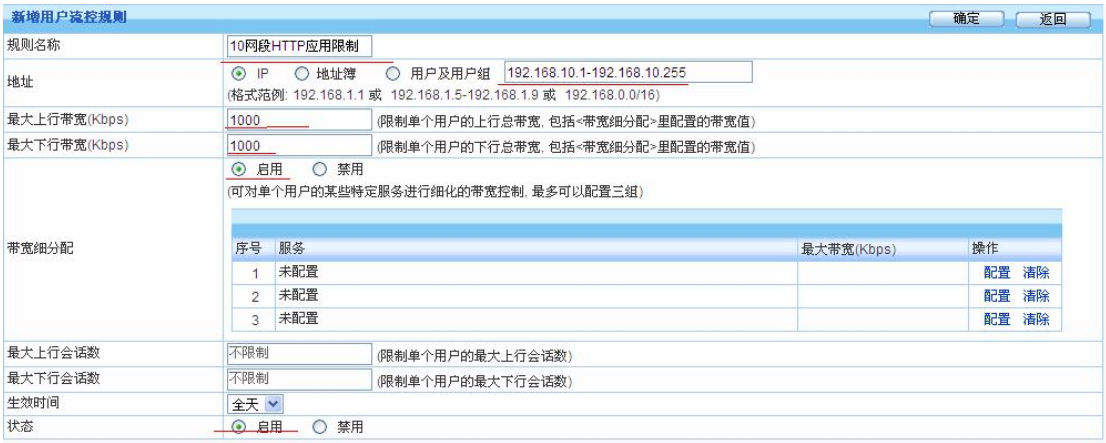
b) 在弹出的对话框中，在规则名称栏中输入自定义的名称，在最大上行带宽中输入 3000，在最大下行带宽中输入 3000，其他地方不需要配置，点击右上角的“确定”按钮即可完成该策略的配置。



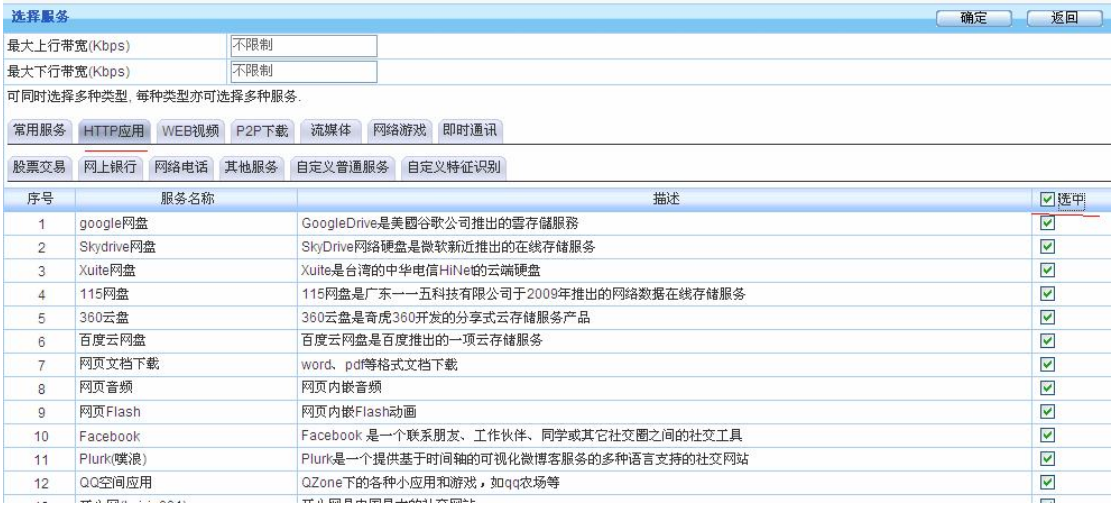
需求二：限制网段 192.168.10.1~192.168.10.255 内的单台主机 HTTP 应用最大上下行带宽为 1Mbps

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。



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。



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。

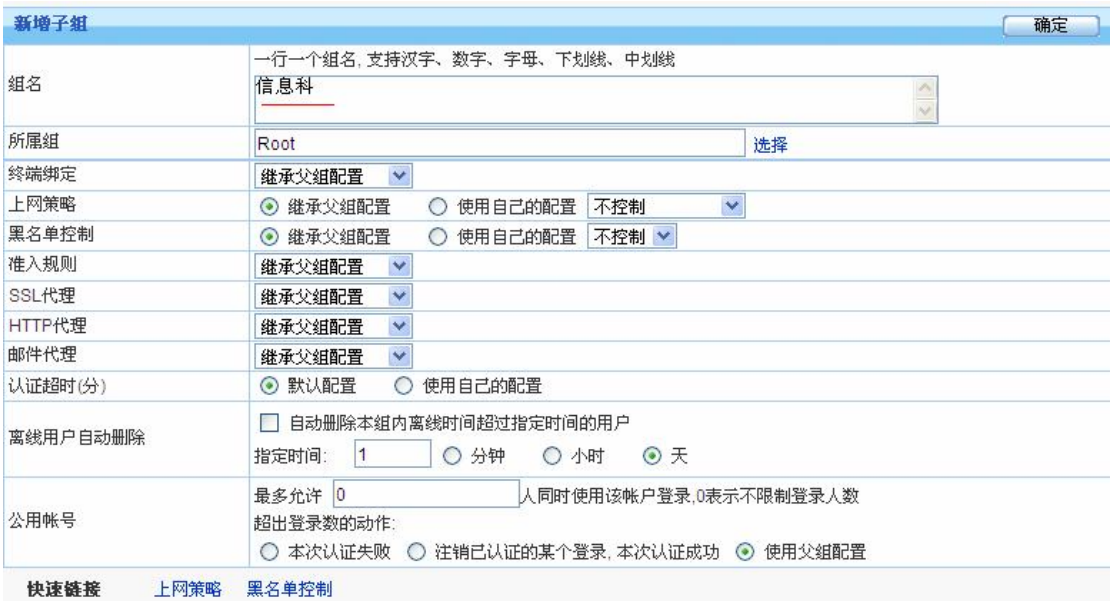
（1） 建立组

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”



（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 NIBC 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，NIBC 没法获取主机的 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。

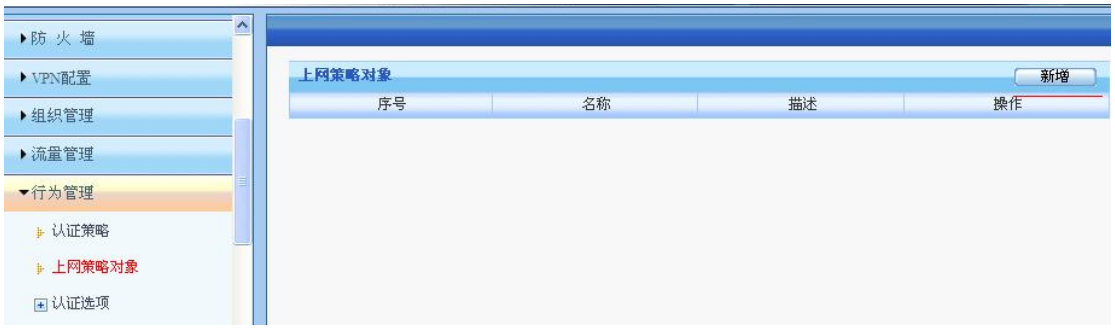
这样就完成了对“信息科”组的配置。

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

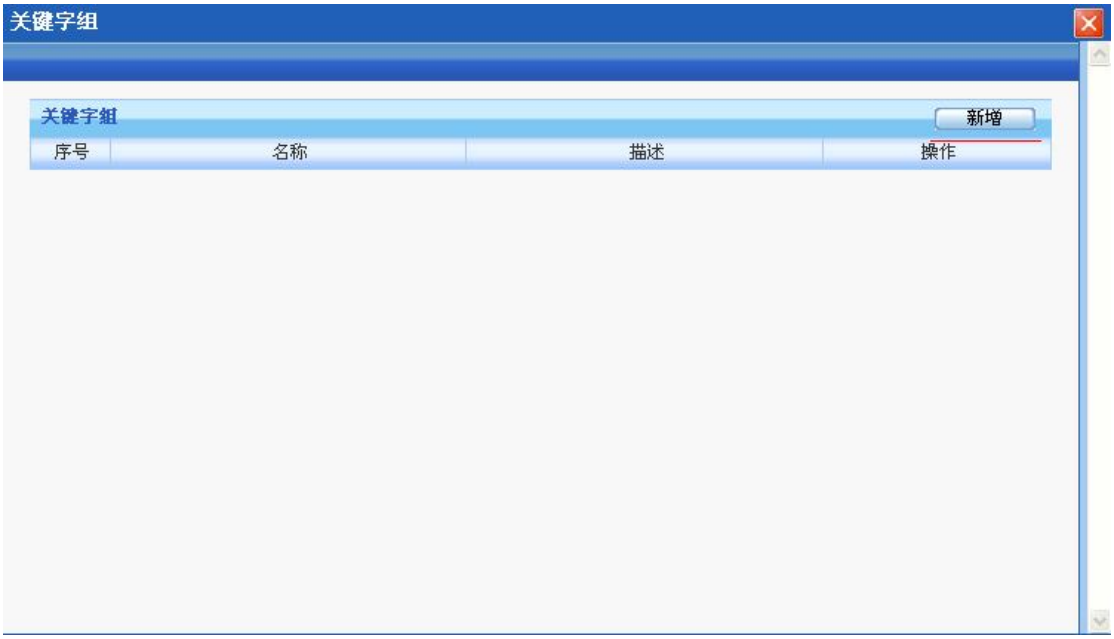
需求：过滤掉关键字为“法轮功”的网页

a) 菜单：行为管理—-上网策略对象，点击“新增”按钮

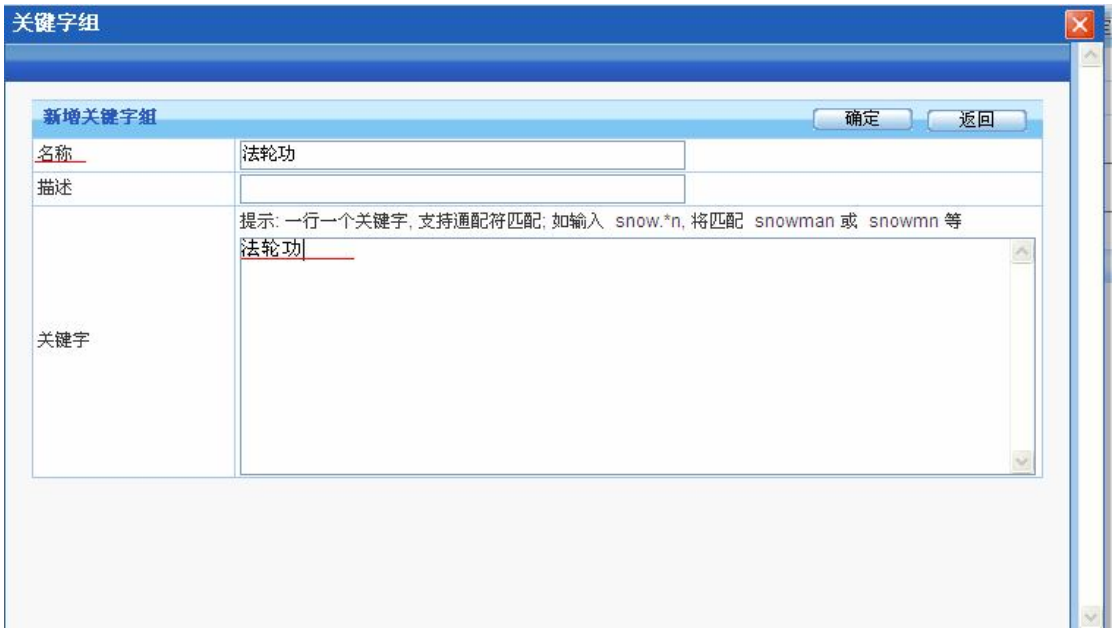


b) 在弹出的对话框中，在名称栏中输入策略名称，然后点击“关键字过滤”，再点击下边快速链接中的“关键字”

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

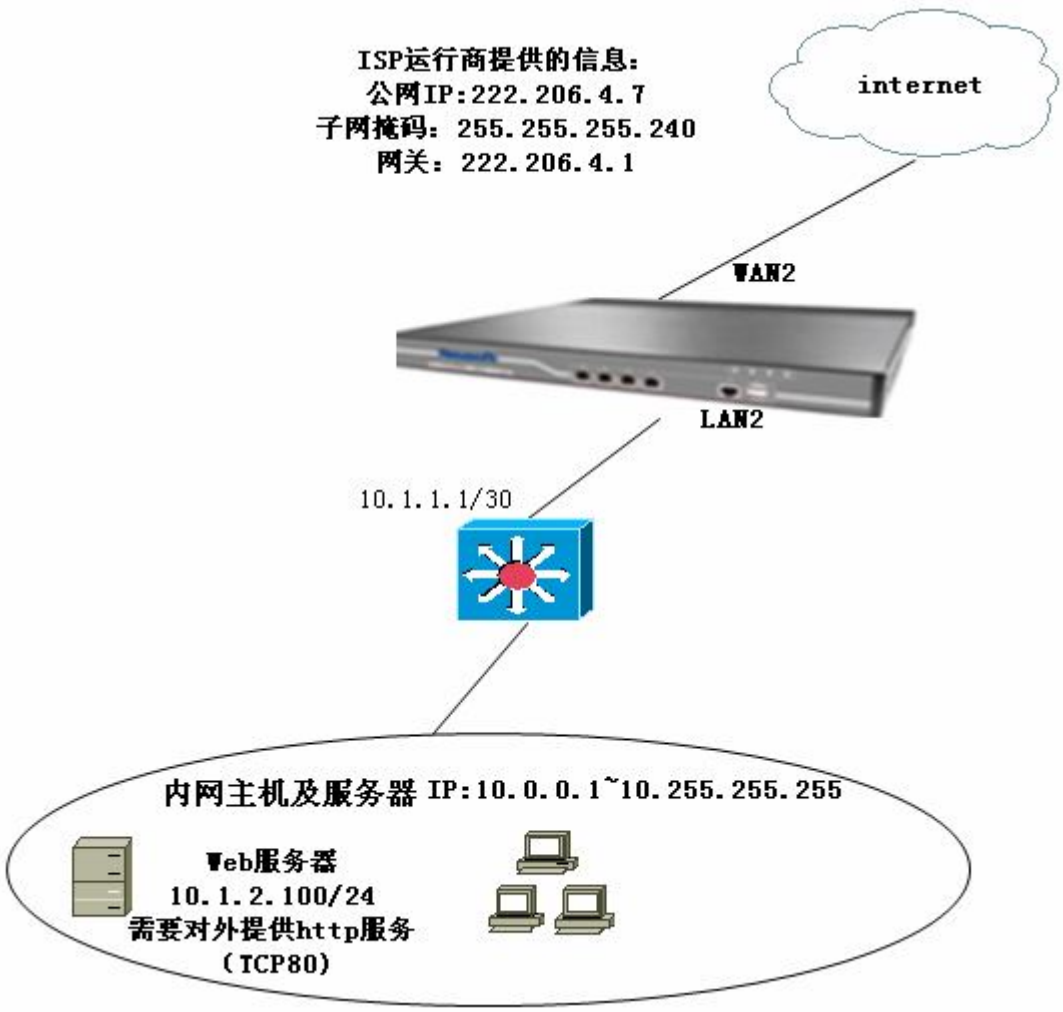
行为管理策略配置完成。

至此 NIBC 设置基本完成 NIBC 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

二、 路由模式

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

举例：（如下图）



设置步骤：

1、 登录设备（详见网桥模式的第 1 部）

2、 设置工作模式

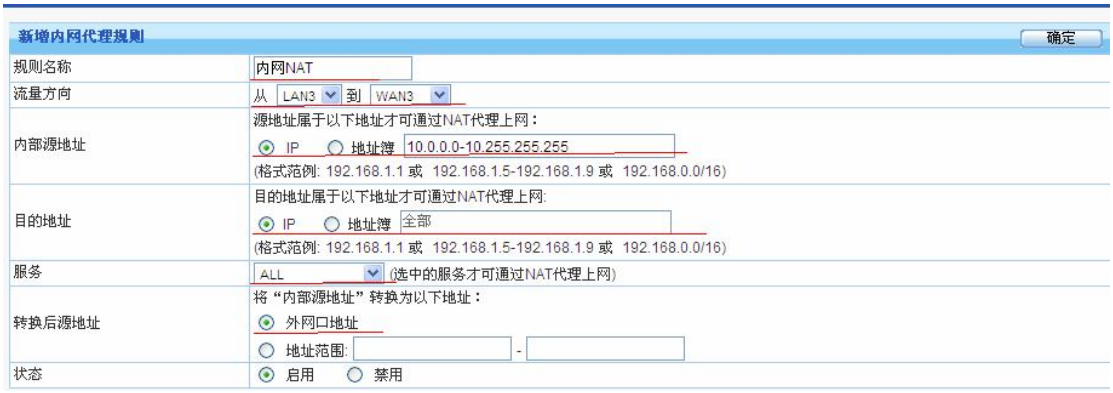
（1） 点击菜单：系统配置—工作模式；即进入工作模式配置界面

（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 IP222.106.4.7，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。

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。