MIG 4.3 用户手册

2014 年 07 月

目录

声明

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系深信服电子科技有限公司客户服务部。

前言

1.1. 手册内容

第 1 部分 SANGFOR MIG 4.1 产品概述。该部分主要介绍 SANGFOR MIG 4.1 的外观特点和功能特性，以及连接前的准备和注意事项。

第 2 部分 SANGFOR MIG 4.1 的部署及配置介绍。

附录部分 SANGFOR MIG 4.1 网关升级客户端的使用。

本手册以深信服 MIG 200 型号为例进行配置。由于各型号产品硬件和软件规格存在一定差异，所有涉及产品规格的问题需要和深信服科技有限公司联系确认。

1.2. 本书约定

图形界面格式约定

文字描述	代替符号	举例
按钮	边框+阴影+底纹	“确定”按钮可简化为确定
菜单项	『 』	菜单项“系统设置”可简化为『系统设置』
连续选择菜单项及子菜单项	→	选择『系统设置』→『接口配置』
下拉框、单选框、复选框选项	[ ]	复选框选项“启用用户”可简化为[启用用户]
窗口名	【 】	如点击弹出【新增用户】窗口
提示信息	“”	提示框中显示“保存配置成功，配置已修改,需要重启 DLAN 服务才能生效，是否立即重启该服务?”

各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的

意义如下：

 **小心、注意：**提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。

 **警告：**该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。

 **说明、提示、窍门：**对操作内容的描述进行必要的补充和说明。

1.3. 技术支持

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

技术支持论坛： http://sangfor.360help.com.cn

公司网址：http://www.sangfor.com.cn

1.4. 致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

第 2 章 SANGFOR MIG 的安装

本部分主要介绍了 SANGFOR MIG 系列产品的硬件安装。硬件安装正确之后，您才可以进行配置和使用。

2.1. 环境要求

SANGFOR MIG 设备可在如下的环境下使用。

输入电压：110V~230V

温度：0～45℃

湿度：5～90％

为保证系统能长期稳定地运行，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，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

2.2. 电源

SANGFOR MIG 系列产品使用交流 110V 到 230V 电源。在您接通电源之前，请保证您的电源有良好的接地措施。

2.3. 产品外观

图 1 SANGFOR MIG1110 网关面板

从左到右的接口和指示灯分别是：

3G 指示灯（MIG 1110/MIG 1110-W）：3G 拨号过程中，该指示灯会闪烁；当设备通过 3G 拨号成功时，该指示灯会亮起。

WIFI 指示灯（MIG 1110-W）：当设备启用 WIFI 功能时，该指示灯会亮起；有 WIFI 连接时，该指示灯会闪烁。

POWER：MIG 设备电源指示灯。

ALARM：MIG 设备报警指示灯(设备启动时 1-2 分钟内长亮)。

WAN/WAN1：设备的 WAN1 接口。

WAN2(MIG 1200)：设备的 WAN2 接口。

DMZ：设备的 DMZ 接口。

LAN1：设备的 LAN 接口。

LAN2：设备的 LAN 接口。

LAN3（MIG 1110/MIG 1110-W）：设备的 LAN 接口。

RESET：恢复出厂配置键。MIG 设备通电状态下，按住 RESET 键 2 秒后松开，ALARM 红灯会开始闪烁，之后会红灯常亮，等红灯熄灭后即恢复默认配置成功。

USB 接口（MIG 1110/MIG 1110-W，背面板）：用来外接 3G Modem。

图片仅供参考，不同型号的产品外观请以实物为准。

CONSOLE 口仅供开发和测试调试时使用，用户需从设备网口通过浏览器登录设备进行配置。

2.4. 配置与管理

在配置 SANGFOR MIG 网关之前，您需要配备一台电脑，配置之前请确定该电脑的网页浏览器能正常使用（仅支持 Internet Explorer），然后把电脑与 SANGFOR MIG 连接在同一个局域网内，通过网络对设备进行配置。

2.5. 设备接线方式

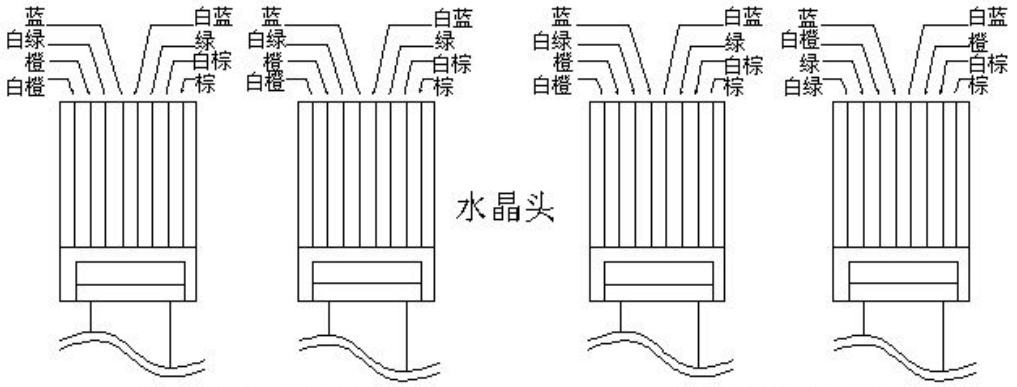
在背板上连接电源线，打开电源开关，此时前面板的 Power 灯(绿色，电源指示灯)和 Alarm 灯(红色，告警灯)会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明网关正常工作。

请用标准的 RJ-45 以太网线将 LAN 口与内部局域网连接，以便对 SANGFOR MIG 进行配置。

请用标准的 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。

SANGFOR MIG 正常工作时 POWER 灯常亮，WAN 口和 LAN 口 LINK 灯长亮，ACT 灯在有数据流量时会不停闪烁。ALARM 红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在正常使用时此红灯长亮，请将设备掉电重启，重启之后若红灯一直长亮不能熄灭，请与我们联系。

WAN 口直接连接 MODEM 应使用直通线、连接路由器应使用交叉线；LAN 口连接交换机应使用直通线、直接连接电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线序不同，如下图：



直连网线线序图示　　交叉网线线序图示

第 3 章 控制台的使用

3.1. 登录 WebUI 配置界面

设备出厂的默认 IP 见下表：

接口	IP 地址
LAN1、LAN2 和 LAN3	10.254.254.253/24
DMZ	10.254.253.253/24

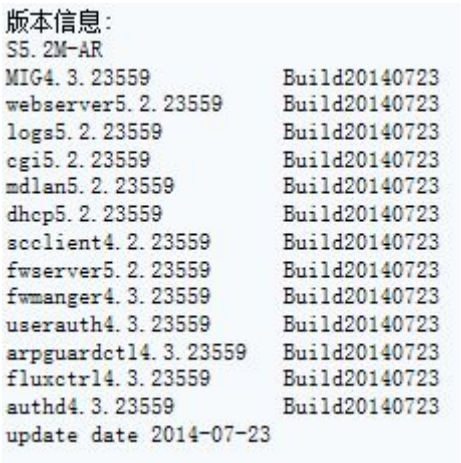
SANGFOR MIG 支持 WEB 管理，使用 443 端口登录，如果使用初始地址登录 LAN 口，那么登录的 URL 地址为：https://10.254.254.253

按照前面所示方法接好线后，通过 Web 界面来配置 SANGFOR MIG 硬件网关设备。方法如下：

首先为本机器配置一个 10.254.254.X 网段的 IP（如配置 10.254.254.100），掩码配置为 255.255.255.0，然后在 IE 浏览器中输入网关的默认 IP 地址及端口，输入 https://10.254.254.253，支持 IE11、chrome33、Firefox27。页面如下：

在登录框输入用户名和密码，点击登录按钮即可登录 SANGFOR MIG 网关进行配置，默认情况下的用户名和密码均为：admin。

如果需要查看当前网关的版本号，点击查看版本，即显示当前硬件的版本信息，页面如下：



登录 webUI 配置界面后，可以看到左树有以下配置选项：

运行状态：设备运行状态、VPN 运行状态、用户流量排名等状态信息。

系统设置：网络接口、路由等网关设备的基本信息设置。

SC 设置：SC 基本设置、SC 服务查看的基本信息设置。

对象设置：IP 组、URL 组、用户组、应用识别规则等对象设置。

IPSec VPN 信息设置：设置 SANGFOR VPN 或者标准 IPSec VPN。

访问控制：认证选项设置、访问策略设置。

流量管理：流控策略设置、线路带宽设置。

防火墙设置：过滤规则设置、NAT 设置等设置。

系统维护：新手导向、日志查看、策略故障排除、备份/恢复配置。

 **注意：**

1、所有配置界面中如果有确定或完成按钮，则配置完毕后，必须要点击该按钮才能使设置保存并生效，后面的文档不再赘述。

2、 所有配置界面右上角都有帮助按钮，可以点击查看当前配置项的简要说明。

3.2. 运行状态查看

『运行状态』用于查看硬件网关的工作状态，可以查看『设备运行状态』、『VPN 运行状态』、『用户流量排名』、『应用流量排名』、『上网行为记录』、『在线用户查看』、『DHCP 运行状态』等。

3.2.1. 设备运行状态

『设备运行状态』可以查看『CPU 占用率』、外网线路概况以及进行重启设备和重启服务等操作，如果需要从外网登录网关进行管理则勾选[允许远程连接]。

3.2.2. VPN 运行状态

此页面可以查看当前的 VPN 连接和网络流量信息。页面如下：

点击分支 NAT 状态可以查看当前接入分支的 NAT 状态，包括用户名、原子网网段、代理子网网段、网络类型和子网掩码，此页面在做了 VPN 隧道内 NAT 后才有。页面如下：

点击刷新状态，则显示实时的 vpn 连接信息以及流量信息。

点击显示选项，可以对显示的列进行筛选。页面如下：

点击停止服务/开始服务可停止或开启 VPN 服务。

在用户模糊搜索输入框中输入用户名，可以快速找到当前用户的连接情况。可以进行模糊搜索。

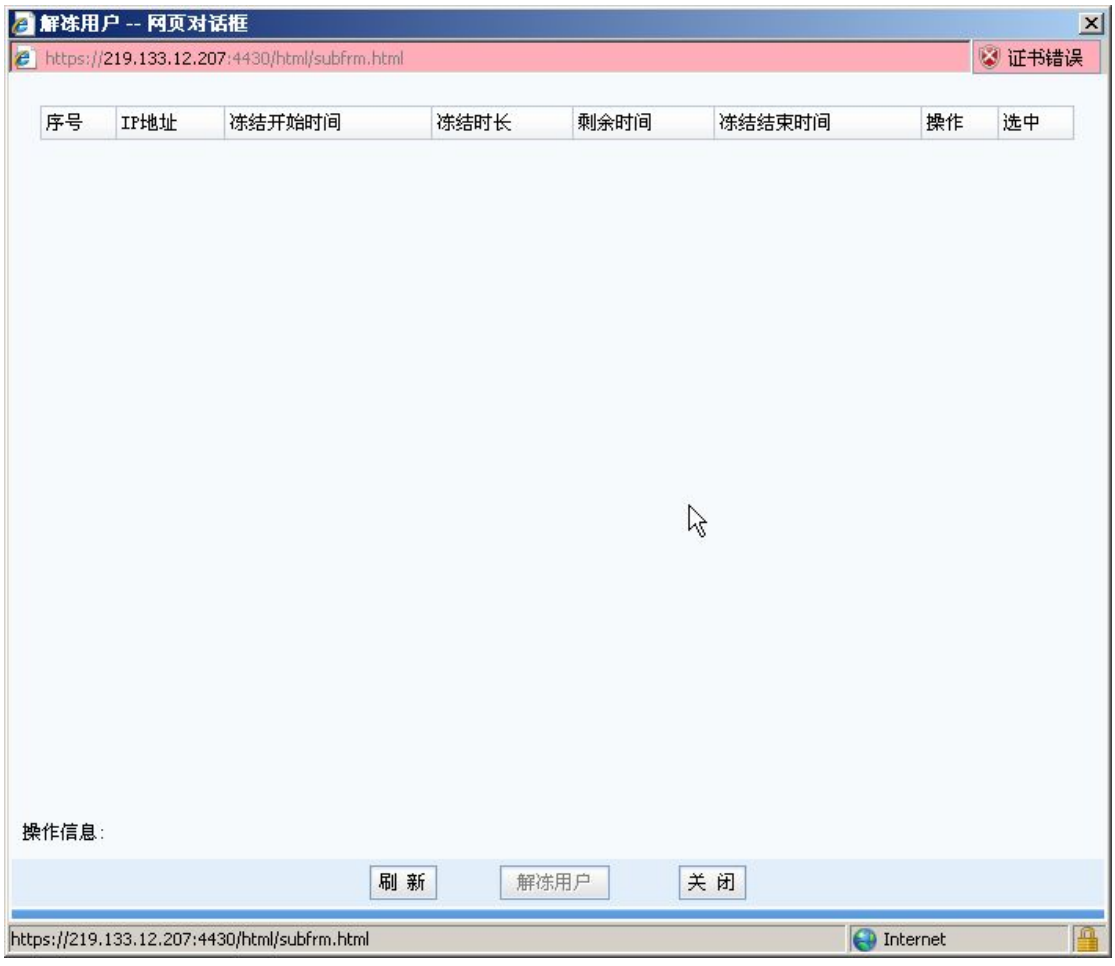
3.2.3. 用户流量排名

『用户流量排名』查看内网用户访问 Internet 的实时网络流量信息。可以对选中的用户进行冻结上网的操作。

点击刷新，手动刷新页面显示的流量排名情况。

选中要冻结的用户，设置冻结时间后点击冻结用户上网，即可冻结指定用户上行流量。

再手动点击刷新，发现无对应 IP 的上行流量（此时该 IP 已无法上网）；点击解冻用户，可以看到，该用户在解冻用户列表中。如下图：



点击解冻按钮则解冻这一个用户，勾选所有需解冻的用户，点击解冻用户，则解冻所有勾选用户。

3.2.4. 应用流量排名

『应用流量排名』可以查看内网用户使用的各种互联网应用占用带宽的排名，如下图：

手动点击刷新，显示实时的应用流量排名；

『序号』：应用排名的顺序；

『应用名称』：具体应用的名字；

『应用类型』：该应用属于的哪个应用类别；

『总流量百分比』：占用当前总流量的百分比；

『上行流量』：该应用向外发送的流量大小；

『下行流量』：该应用接收的流量大小；

『总流量』：该应用所产生的总流量。

3.2.5. 上网行为记录

『上网行为记录』可以查看到实时的内网用户 Internet 行为记录，页面如下：

点击刷新，显示实时的内网用户的上网行为记录。

『外部日志服务器设置』可以设置一个外部的 syslog 服务器进行上网行为记录的存储，包含以下部分：

『启用』：启用与 syslog 服务器通讯的功能。

『服务器 IP』：syslog 服务器的 ip 地址。

『服务器日志接受端口』：syslog 服务器开放的同步端口。

此页面只显示一百条记录，如果需要保存日志，则需要使用外部 Syslog 日志服务器。

3.2.6. 在线用户查看

『在线用户查看』可以查看在线的用户的信息，比如用户名、所属组、ip 地址、在线时长等，页面如下：

3.2.7. DHCP 运行状态

『DHCP 运行状态』可以查看 DHCP 的运行状态和给其他计算机分配 IP 的情况，页面如下：

点击刷新，显示实时的 DHCP 运行状态。

『分配的网口』：选择查看不同网口的 DHCP 运行状态。

3.3. 系统设置

包括『网络接口设置』、『序列号设置』、『系统时间设置』、『路由设置』、『多线路设置』、『本地子网列表』、『控制台设置』、『系统日志设置』、『dhcp 设置』、『wlan 设置』、『生成证书』、『应用识别库自动升级』模块。

3.3.1. 网络接口设置

用于配置设备的工作模式，有两种工作模式可供选择：单臂模式和网关模式。

选择单臂模式时，需要配置内网接口（LAN 口）IP 地址、子网掩码，默认网关，配置 DMZ 口 IP 地址、子网掩码，配置 DNS，以及 VLAN 配置。页面如下：

选择网关模式时，不仅需要配置内网接口，同时也必须配置相应的外网线路。配置页面如下：

『内网接口』：按照实际情况设置上对应的接口 IP 地址即可；

『VLAN 设置』：可以对 LAN 口网段进行多 VLAN 划分，实现多网段隔离。界面如下：

点击添加，以添加 VLAN 网段，配置界面如下：

“VLAN ID”是新增加的 VLAN 标签中的 VLAN 标识符，可设置范围为 1-4094。

“IP 地址和子网掩码”是该 VLAN 的地址接口地址，用于跟该 VLAN 的其他地址进行互联。

“是否允许访问其他 VLAN”用于设置 VLAN 之间的访问权限，包括允许访问、拒绝访问和只允许访问指定 VLAN。

『外网接口设置』可选择“线路 1”和“线路 2-3G 线路”（VPN 1110/VPN 1110-W）或者“线路 1”和“线路 2”（MIG 1200）。

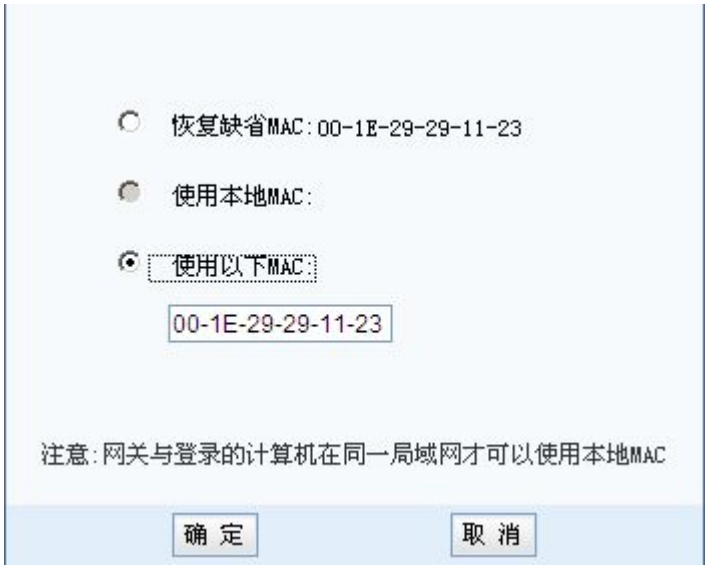
[线路 1 配置]：先选择[线路 1]，勾选[启用该线路]，然后设定[线路类型]，包括“以太网”、“ADSL”两种方式。界面如下：

线路 1 为 ADSL 拨号时，填写完[用户名]和[密码]信息后，注意勾上[自动拨号]，配置完毕点确定保存设置，设备将重启所有服务，重新登录后点击开始拨号，则以后设备在断线后就可以“自动重拨”了，另外可以点击查看日志实时显示拨号日志。

点击高级设置，用来设置 ADSL 拨号的掉线检测机制，可以选择[不进行掉线检测]

和[进行掉线检测]两种，如下图：

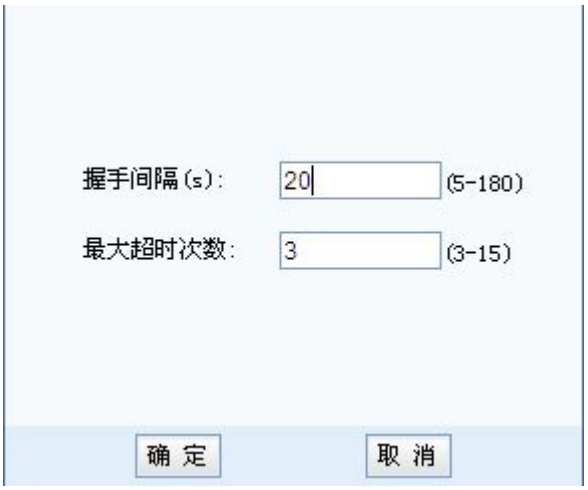
[MAC 设置]：MAC 设置主要用于修改设备 WAN 口的 MAC 地址。选择“使用本地 MAC”是指使用当前登录控制台 PC 网卡的 MAC。点击 MAC 设置，出现如下对话框，可以通过此对话框修改 WAN 接口的 MAC 地址：



[多 IP 绑定]：外网接口为以太网模式下方可启用，在设备外网接口能获取多个 IP，需要把这些 IP 都映射到内网服务器时使用。点击多 IP 绑定按钮，出现以下对话框，点击新增即可为 WAN 口绑定多个 IP。如下图：

[线路 2-3G 线路配置]：MIG 1110 和 MIG 1110-W 设备支持 3G 拔号功能，在线路中选择[线路 2-3G 线路]，勾选[启用该线路]，配置界面如下：

点击高级设置，可以设置 3G 拨号的握手间隔和最大超时次数，如下图：



点击查看兼容列表，将跳转到深信服官方网站，可以查看 MIG 1110 和 MIG 1110-W 设备支持的中国电信和中国联通 3G Modem 型号（更多型号详见：http://www.sangfor.com.cn/supportlist/modem_support_list.html），如下图：

支持的中国联通3G上网卡

序号	型号	厂商	支持版本说明
1	E153	HUAWEI	VPN4.66 Release
2	E1556	HUAWEI	VPN4.66 Release
3	E156G	HUAWEI	VPN4.66 Release
4	E160E	HUAWEI	VPN4.66 Release
5	E169	HUAWEI	VPN4.66 Release
6	E170	HUAWEI	VPN4.66 Release
7	E172	HUAWEI	VPN4.66 Release
8	E173	HUAWEI	VPN4.66 Release
9	E1750	HUAWEI	VPN4.66 Release
10	E1756	HUAWEI	VPN4.66 Release

支持的中国电信3G上网卡

序号	型号	厂商	支持版本说明
1	AC580	ZTE	VPN4.66 Release
2	AC581	ZTE	VPN4.66 Release
3	AC582	ZTE	VPN4.66 Release
4	AC583	ZTE	VPN4.66 Release
5	AC8710	ZTE	VPN4.66 Release
6	AC2736	ZTE	VPN4.66 Release
7	AC2746	ZTE	VPN4.66 Release
8	EC122	HUAWEI	VPN4.66 Release
9	EC1260	HUAWEI	VPN4.66 Release
10	EC1261	HUAWEI	VPN4.66 Release

点击查看日志，可以查看 3G 拨号的相关日志。

选择 3G 线路时，只需要将 3G Modem 正确插入设备背面板对应的 USB 插孔中，APN 码、拨号串、用户名和密码等信息会自动生成，一般不需要重新配置，若要修改，直接在文本框中编辑即可。

注意：MIG 1110 和 MIG 1110-W 设备只支持中国电信和中国联通 3G Modem，不支持中国移动 TD-SCDMA 的 3G Modem。

[分配策略]：此处是设定整个 MIG 设备对外网线路的选择策略，每个选项的详细介绍可以参照对话框上的帮助提示。点击分配策略按钮，出现以下对话框：

这里是用户上 Internet 时的选路策略，在物理线路和 3G 线路同时在线的情况下，若选前面三项，需考虑 3G 线路流量问题。

3.3.2. 序列号

『序列号』用于填写 SANGFOR MIG 硬件网关的序列号，该序列号控制硬件网关的可用外网线路数量、IPSec 分支、移动用户的授权数，不同的序列号对应着不同线路数量和接入用户数量，填入序列号时，这些授权数会自动生成。跨运营商模块序列号以及应用识别库升级序列号，用来决定 SANGFOR MIG 硬件网关是否支持跨运营商功能以及内置的应用识别库是否能自动升级。配置界面如下图，填写完各序列号，点确定保存即可。

『线路数』：该产品只有一个 wan 口，所以是 1，而且不可以修改。

『第三方对接授权数』：允许连多少个第三方对接，由『序列号』项自动生成，不可修改。

『移动用户授权数』：允许拥有多少个移动用户，由『序列号』项自动生成，不可修改。

『网关序号』：设备的硬件 ID，出厂默认，不可修改。

『序列号』：控制该设备的『第三方对接授权数』和『移动用户授权数』的序列号，如需增加授权需要购买新的序列号。

『跨运营商授权码』：激活跨运营商功能，解决跨运营商之间连接 IPsec VPN 丢包率很高的问题。

『应用识别库升级序列号』：该序列号是控制应用识别规则库升级的有效期，根据序列号不同，决定购买的应用识别库升级有效期。

3.3.3. 系统时间设置

用于设定 SANGFOR MIG 硬件网关的系统时间。点击取系统时间，即可刷新 SANGFOR MIG 硬件网关系统本身的时间。点击和本地同步，则修改 SANGFOR MIG 硬件网关的系统时间为当前 Web 登录所在计算机的时间，点击确定即可保存设置。页

面如下：

3.3.4. 路由设置

用来设置 SANGFOR MIG 设备的系统路由。包括静态和动态两种。页面如下：

3.3.4.1. 系统路由设置

『系统路由设置』主要用于实现两种功能：

1、代理多网段上网时添加回包路由；

2、需要访问 VPN 内部多子网时设置路由；

1、代理多网段上网时添加“回包路由”

当企业内网有多个网段，且这些内网网段都想通过 MIG 网关设备共享上网时，需要添加系统路由，使 MIG 网关设备能把不同网段的数据包回给正确的内网三层交换机或路由器。

例如：公司内网有两个网段 192.200.100.X 和 192.200.200.X，两个网段通过三层交换机互连互通，各网段内电脑网关指向三层交换机各自网段的网关 192.200.X.254，MIG 硬件设备的 LAN 口 IP 为 192.200.200.200，放在 192.200.200.X 网段，并配置 WAN 口连接 Internet。现 192.200.100.X 和 192.200.200.X 网段都想通过 MIG 作为公网出口，共享上网。

由于 192.200.100.X 网段和 MIG 的 LAN 口(192.200.200.X)不在同一网段，则 MIG 需要添加系统路由，以把 192.200.100.X 的数据包发回给内网三层交换机 192.200.200.254 才能出来，最终才能回到 192.200.100.X 网段的电脑上。配置如下：

A、添加多个代理网段：在 MIG 的 NAT 配置页面里添加 2 个子网网段，包括 192.200.100.0/24 和 192.200.200.0/24（具体设置参照 MIG 用户手册 2.9.2.1 小节『防火墙设置』→『NAT 设置』→『代理上网设置』部分）。

B、添加系统路由：在 MIG 的系统路由设置页面添加一条系统路由，192.200.100.0/24->192.200.200.254，页面如下：

2、需要访问 VPN 内部多子网时设置路由

当 VPN 网络中的总部或分支内部有多个网段的网络时，我们称之为 VPN 多子网。这些网络如果需要加入到 VPN 网络中，以便 VPN 中的分支、移动或总部内网各网段

相互访问，需要添加本地子网列表及系统路由来实现。

例如：总部有两个网段 192.200.100.X 和 192.200.200.X，这两个网段通过三层交换机相连互通，三层交换机上连接这两个网段的端口 IP 分别为 192.200.100.254 和 192.200.200.254，我们的 MIG 设备的 LAN 口 IP 为 192.200.200.200，部署在 192.200.200.X 网段。

首先在 MIG『本地子网列表』，添加一个多子网 192.200.100.X，页面如下：

然后在 MIG 系统路由设置页面的『系统路由设置』中添加一条关于 192.200.100.X 的系统路由，把网关指向能通往 192.200.100.X 的三层交换机接口 192.200.200.254，如下图：

3.3.4.2. 动态路由设置

『动态路由设置』用于设置 MIG 设备通过 RIP v2 协议向其它路由设备通告路由信息，以实现内网路由设备 RIP 路由信息的动态更新。页面如下：

『启用路由选择信息协议』：整个动态路由更新功能的开关，激活后，MIG 设备会向所设置的内网路由设备通告已与本端建立 VPN 连接的对端网络的信息（更新其他设备的路由表，添加到 VPN 对端的路由指向 MIG，VPN 连接断开后会通告路由设备删除该路由）。

『启用密码验证』：用于设置交换 RIP v2 协议信息时需要验证的密码，可视具体情况进行设置。

『IP 地址』及『端口』：用于设置主动向哪个 IP（路由设备 IP）发布路由更新信息。

[需要触发更新]勾选后，MIG 在路由信息有变化时会触发路由更新信息过程，这时下面设置的 RIP 更新周期参数失效。

[记录日志]勾选，则 MIG 设备会记录 RIP 路由更新的日志信息。

最后点击确定保存配置。

3.3.5. 多线路设置

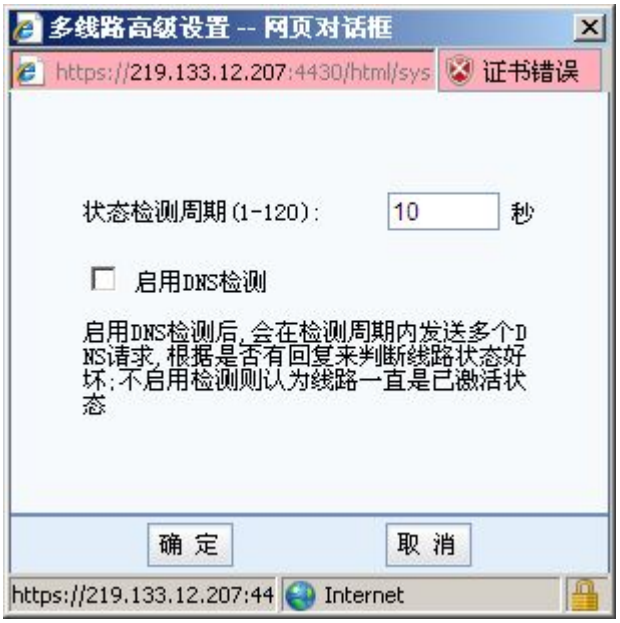
设备开启多线路授权的情况下，需要通过『多线路设置』来检测两条线路的健康状况，同时需要实现 MIG 多线路自动选路功能，也必须设置该选项。如下图：

[刷新]：用于刷新当前线路状态

[新增]：用于新增线路，此处要求将两条线路都新增上去，点击新增按钮，出现如下界面：

线路别名可以自行定义，例如“电信”、“联通”等等。测试域名一般填写正常情况下通过该线路可以正常解析的域名，设备会定期通过该线路解析该域名，能解析到则判断线路工作正常，需要在[高级]里启动 DNS 检测。其他设置请参考蓝色字体部分。设置好两条线路后界面如下：

[高级]：用于设置启用 DNS 检测，可以设置线路状态检测周期，以及关闭或者启用 DNS 检测。点击高级，界面如下：



设备双线路情况下，通过 调整线路顺序，可以修改设备的默认路由指向和设备默认 DNS 顺序。例如上述图中电信线路在上方，则设备的默认路由指向电信线路，设备本身及代理内网解析域名时优先使用电信线路 DNS。（DNS 探测使用『多线路设置』处添加线路时设置的 DNS）

3.3.6. 本地子网列表

当设备所处内网有三层交换机或者路由器之类设备，划分了多个网段，则需要在这里将除设备 lan 口所在网段之外的其他多个网段的信息给添加进去。

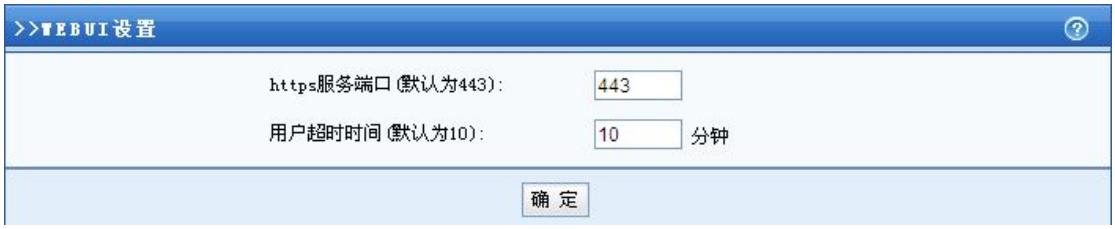
点新增，填入本端其他网段地址即可完成本地子网列表的添加。页面如下：

注意：设备 LAN 口和 DMZ 口所在网段，不需要添加到本地子网列表。只有本地内网有多网段情况，才需要添加其他网段到本地子网列表。

3.3.7. 控制台设置

3.3.7.1. WEBUI 设置

用于设置网关控制台的 http 服务端口（默认 443 端口）和用户登录设备控制台的超时时间，如修改了服务端口，下次登录需通过修改后的端口登录网关控制台，页面如下：

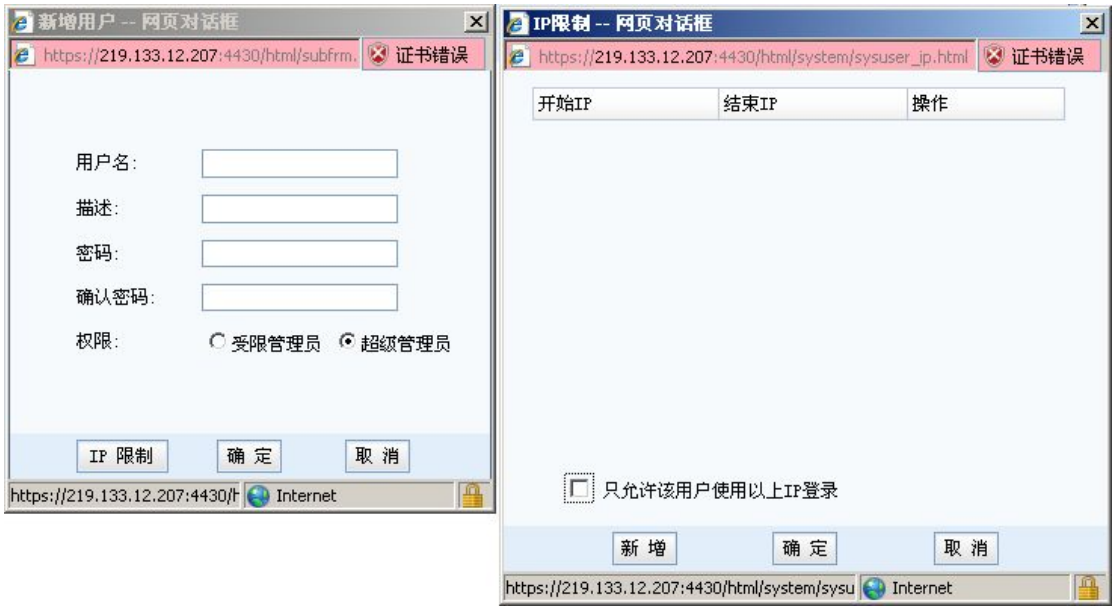


3.3.7.2. 管理员设置

『管理员设置』用于设置可登录网关控制台的管理账号。

点击在线用户，可以看到当前连接到该硬件设备的管理员状态，如下图所示：

点击新增弹出新增用户对话框，设置『用户名』、『密码』、『权限』及『IP 限制』。设置页面如下：



3.3.8. 系统日志设置

『系统日志设置』用于设置 syslog 服务器的 IP 地址和端口号，可以把 SANGFOR MIG 设备产生的系统日志发送到其他第三方的 syslog 服务器上。页面如下：

『启用』：启用与 Syslog 服务器通讯的功能。

『服务器 IP』：Syslog 服务器的 IP 地址。

3.3.9. 服务 DHCP 设置

DHCP 设置主要用于设置 DHCP 服务的一些参数。页面如下：

[分配的网口]可以选择是 LAN/WLAN 口或者 DMZ 口。

在[DHCP 网络配置]中设置适当的网关 IP 和有效的 DNS 服务器 IP，一般情况下[网关]处填写的是 VPN1110/1110-W/1200 设备的“LAN 口 IP”或“DMZ 口 IP”，[DNS]则填写当地 ISP 所提供的 DNS 服务器 IP。[WINS]服务器可根据自己的具体应用判断是否需要填写。

点击[DHCP IP 地址范围]下的新增按钮，出现以下对话框：

这里设定的是 DHCP 所分配的 IP 地址范围，直接填写起始 IP 和结束 IP 确定范围即可。

注意：1、加入内网机器某些电脑设置了固定私网 IP，这里填写的 IP 地址范围不要包含已使用的 IP，以免随机分配 IP 时产生 IP 冲突。

2、一般情况下 IP 地址范围不要把末尾为 0 和 255 的地址加上，这两个是网络地址和本网段广播地址。

[DHCP 保留 IP 设置]用于设置为某些计算机保留分配固定的 IP，点击下面的新增按钮，出现[编辑 DHCP 保留 IP]对话框，如下图：

[用户名]由用户自定义，可任意填写容易记忆理解的名字。

[IP]地址则填写需要保留分配给该用户的特定内网 IP。

DHCP 保留的条件可以根据用户电脑的“MAC 地址”或者“机器名”来绑定。

勾选相应的选项，然后填写对应的“MAC 地址”和“机器名”，也可点击根据 IP 获取来获得对应的参数，点击确定保存。

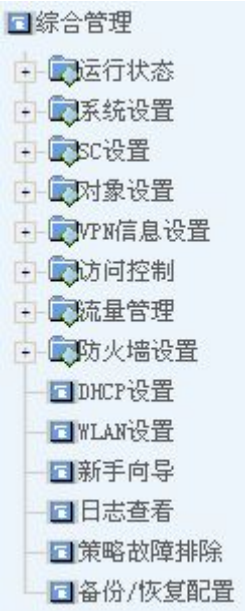
[高级]选项用于设置 DHCP 的租约时间，可自行修改(1-7200 分钟)，默认为 120 分钟。

如下图：

最后勾选[启用 DHCP 服务]，确定后即可激活 DHCP 功能。

3.3.10. WLAN 设置（MIG-1110-W）

MIG-1110-W 设备还支持局域网用户使用无线 WIFI 方式接入，在 MIG-1110-W 设备的配置界面可以看到 WIFI 相关的配置选项，如下图：



『WLAN 设置』配置界面如下：

勾选[启用 WLAN]，表示在设备上开启 WIFI 功能。

『SSID』用于设置 WIFI 的名称，无线 WIFI 客户端将显示对应的 SSID 名称。

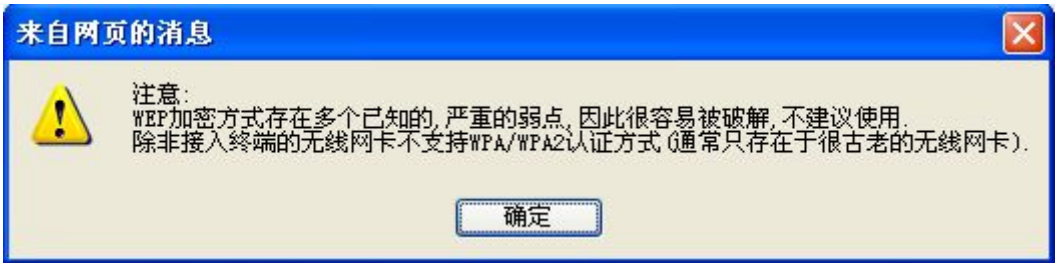
『信道』用于设置 WIFI 的无线信道，支持信道 1 至信道 13，也可以让设备自动选择。推荐使用自动选择方式来避免无线信道冲突造成的传输速率下降。

『工作模式』用于设置 WIFI 支持的工作模式，默认为 802.11 b/g/n 混合模式。

[启用 SSID 广播]用于设置是否广播 SSID，如果广播 SSID，则所有处于设备无线信号范围内的无线设备均能发现这个 WIFI 网络，默认该选项启用，如果需要较高的 WIFI 安全性则可以取消勾选该功能。

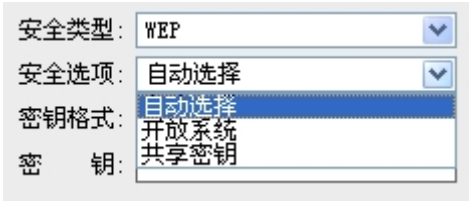
勾选[启用安全设置]，表示对 WIFI 网络进行加密保护，防止未经授权的无线用户擅自接入 WIFI 网络。

『安全类型』用于选择 WIFI 网络的加密协议，包括 WPA-PSK/WPA2-PSK 和 WEP 两种加密方式，默认为 WPA-PSK/WPA2-PSK。WEP 加密协议因为容易遭到破解，除非有无线设备不支持 WPA-PSK/WPA2-PSK，否则不建议使用 WEP，在切换到 WEP 方式时，设备也会有对应提示，如下图：



『安全选项』用来选择具体的加密协议，如果『安全类型』选择的是 WPA-PSK/WPA2-PSK 方式，则『安全选项』包括自动选择、WPA-PSK 和 WPA2-PSK 三种方式，如下图：

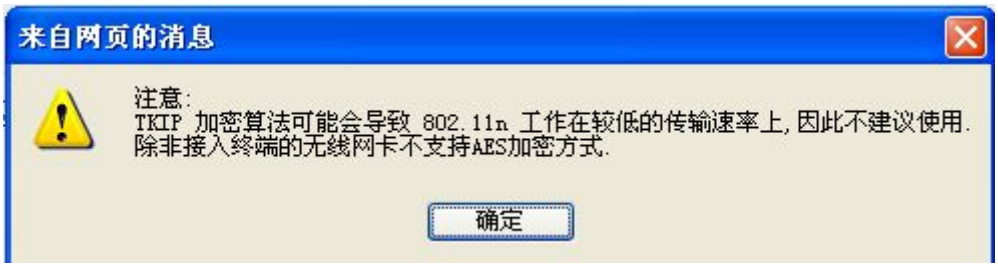
如果『安全类型』选择的是 WEP 方式，则『安全选项』包括自动选择、开放系统和共享密钥三种方式，如下图：



其中开放系统意味着不需要认证，任何无线客户端都可以接入 WIFI 网络。共享密钥则需要无线客户端接入的时候输入跟设备配置相符的共享密钥才能接入 WIFI 网络。

『加密算法』用来选择对应的加密算法，包括 AES 和 TKIP 两种，如下图：

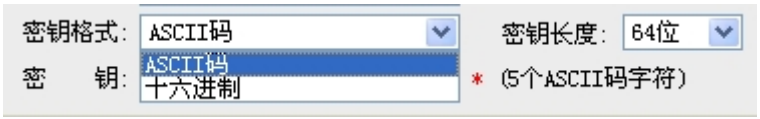
默认为 AES 算法，TKIP 加密算法会导致 WIFI 802.11n 工作在较低的传输速率，因此除非无线终端不支持 AES 算法，否则建议使用默认的 AES 算法，同时切换到 TKIP 算法时设备也会给出相应的提示，如下图：



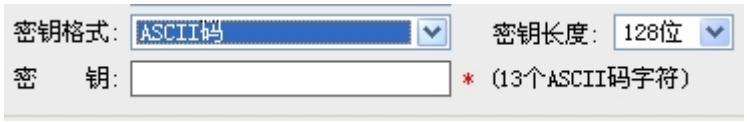
『PSK 密码』用来设置 WIFI 网络密码，长度为 8-63 个 ASCII 码字符，无线终端接入 WIFI 网络时需要输入正确的密码才能接入 WIFI 网络，如下图：

如果安全类型选择的是 WEP 方式，则没有加密算法和 PSK 密码设置选项，而是密钥格式、密钥长度及密钥选项，如下图：

『密钥格式』用来设置 WEP 加密的密钥格式，包括 ASCII 码和十六进制两种方式，密钥长度包括 64 位和 128 位两种，如下图：



『密钥』用来设置 WEP 方式的密钥，ASCII 码情况下长度为 5-13 个字符，十六进制情况下长度为 10-26 个十六进制字符，如下图：

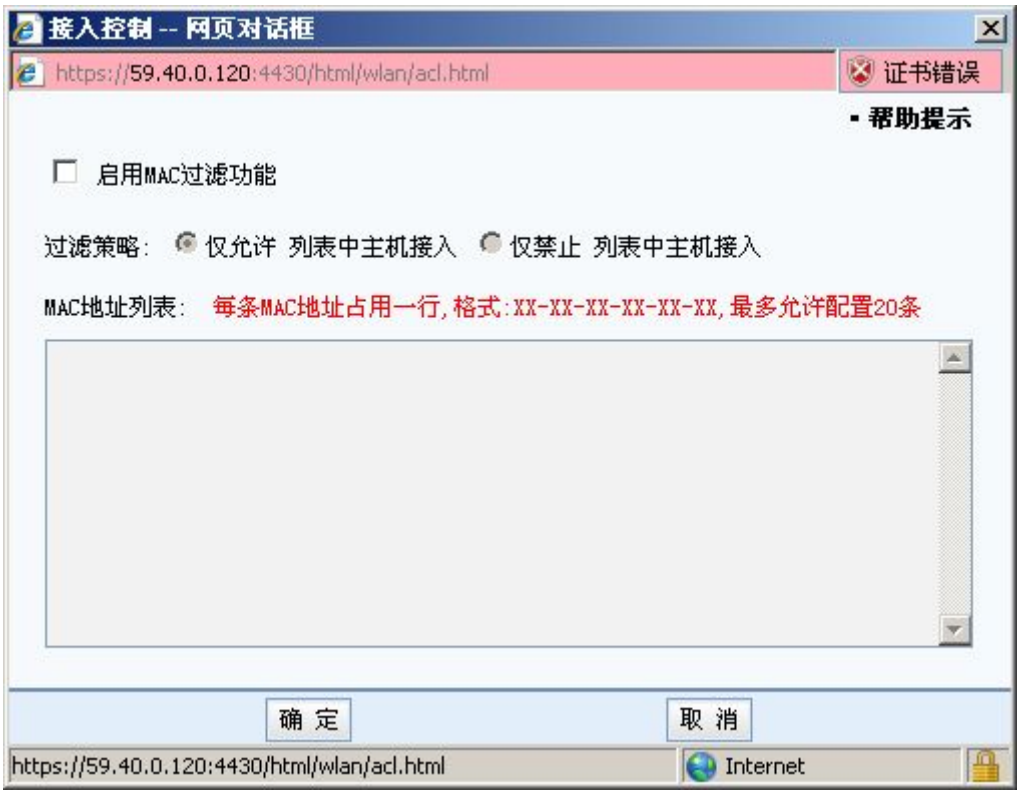


点击 DHCP 设置，可以跳转到 DHCP 设置页面，可以给 WIFI 用户配置 DHCP 地址池。

配置方式见 2.7 小节。

点击查看接入列表，可以查看当前接入的 WIFI 终端 MAC 地址，如下图：

点击访问控制，可以对 WIFI 终端做访问控制，只允许列表中指定 MAC 地址的无线终端接入或者禁止列表中指定 MAC 地址的无线终端接入，如下图



点击确定，保存 WLAN（WIFI）设置。

器端口』：Syslog 服务器开放的同步端口。

3.3.11. 生成证书

基于硬件特性的证书认证系统是深信服公司的发明专利之一。SANGFOR MIG 硬件设备也采用了该技术用于不同 VPN 节点之间的身份认证。该证书提取了 SANGFOR MIG 设备部分硬件特性生成加密的认证证书。由于硬件特性的唯一性，使得该证书也是唯一的、不可伪造的。通过对该硬件特性的验证，就保障了只有指定的硬件设备才能被授权接入网络，避免了安全隐患。

点击生成证书选择保存路径即可生成硬件证书并保存到本地计算机上。页面如下：

将生成好的证书发给总部管理员，由总部管理员在新建 VPN 用户账号的时候选择硬件鉴权，将用户和对应的硬件证书进行绑定即可。

3.3.12. 应用识别库自动升级

『应用识别库自动升级』主要包括两个部分，『当前相关库更新』和『服务器配置』，页面如下：

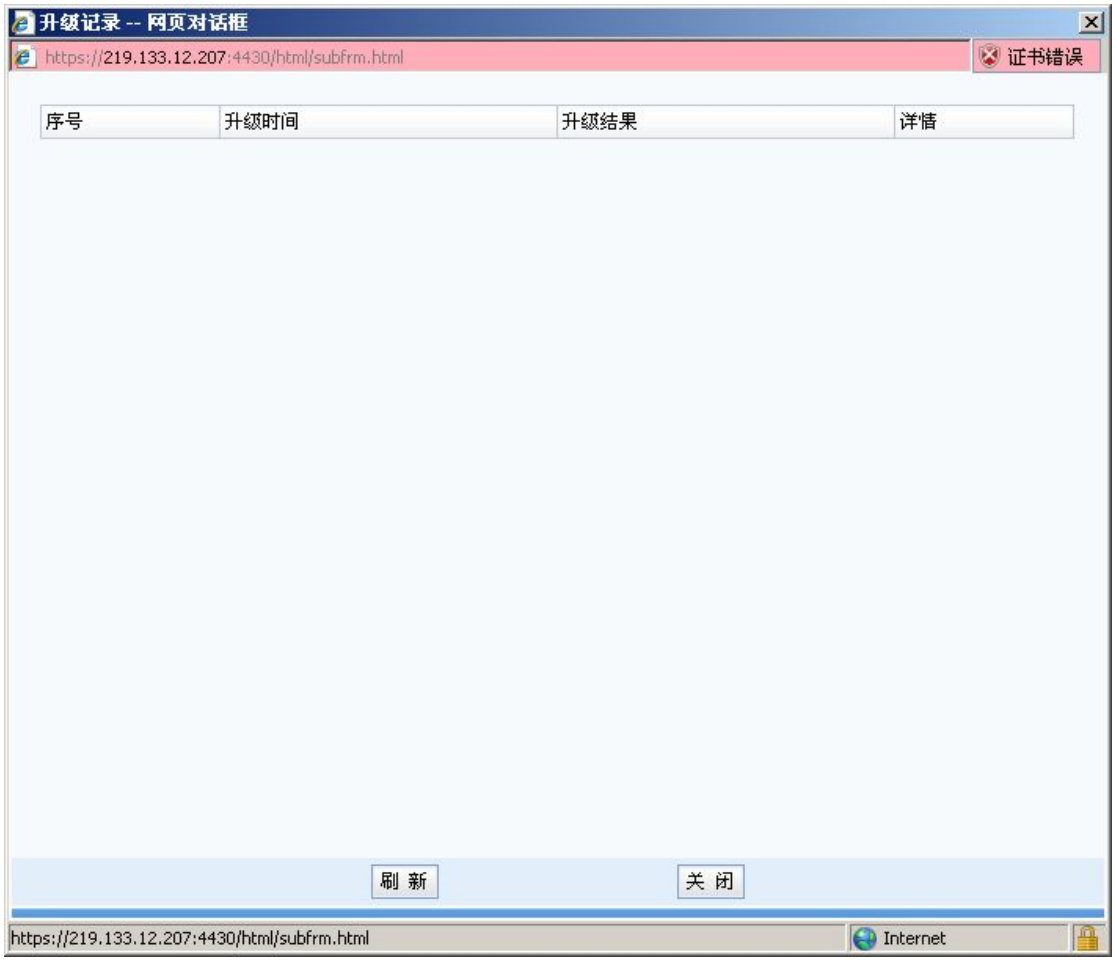
『启用自动升级』：启用自动升级应用识别库的功能，设备会定时去服务器检测是否有新的库更新，检测到更新了则会自动下载升级。

『相关库』：库名，在这里就是应用识别。

『当前版本』：当前应用识别库的版本。

『升级服务有效期』：在该时间之前都可以进行升级，如果过期了则不能继续升级，需要续费，获得到新的『应用识别库升级序列号』之后，填入该序列号生效之后才能继续升级。

『操作』：点击立即更新，会立即向服务器检测更新，如果检测到则立即下载并更新；点击查看升级记录，则弹出以下界面，显示应用识别库的升级记录。



『服务器选择』：选择适合自己的服务器进行升级。

3.4. SC 设置

『SC 设置』用来设置 MIG 设备加入深信服 SC 集中管理平台，可以实现 MIG 设备配置的集中管理，包括『SC 基本设置』和『SC 服务查看』。

3.4.1. SC 基本设置

『SC 基本设置』用来设置 MIG 设备是否需要加入 SC 集中管理平台，如下图：

『是否接入中心端』：用来设置 MIG 设备是否加入 SC 集中管理平台。

『与设备位于同一局域网』：当 SC 中心端设备跟 MIG 设备处于相同局域网时需要启用此项，否则保留默认值“否”。

『账户设置』：填写加入 SC 中心端时的用户账号和密码。

『共享密钥设置』：填写加入 SC 中心端的密钥，需与 SC 中心端的密钥一致。

『中心端地址设置』：填写 SC 中心端的 WEBAGENT 地址，点击测试，可测试 WEBAGENT 连通性。

点击确定，保存配置。

注意：加入 SC 集中管理后，设备上部分配置需从 SC 中心端统一下发，本机将不可配置。

3.4.2. SC 服务查看

『SC 服务查看』用来查看当前 MIG 设备的 SC 各项服务运行状态，包括 SC 通讯服务、

实时监控服务、配置管理服务、自动升级服务的运行状态。如下图：

3.5. 对象设置

3.5.1. 算法设置

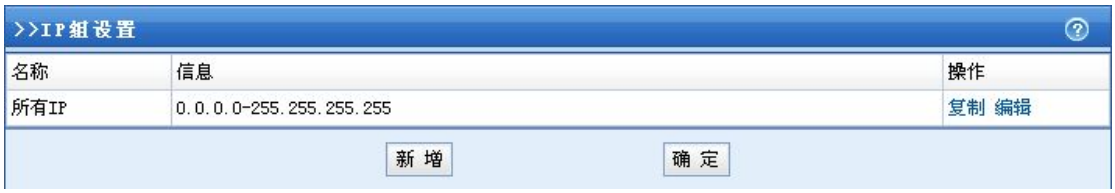
用来设置 VPN 连接所需要的加密和认证算法。页面如下：

>>算法查看

算法名称	类型	提供者	描述
DES	加密算法	Walter tuchman and Carl Meyer	Data Encryption Standard for encrypt data
3DES	加密算法	Walter tuchman and Carl Meyer	Triple-DES Standard for encrypt data
MD5	认证算法	Ronald L. Rivest of the RSA	Message-Digest Algorithm for Authentication
AES	加密算法	Joan Daemen and Vincent Rijmen	Advanced Encryption Standard for encrypt data
SHA-1	认证算法	US National Security Agency (NSA)	Secure Hash Algorithm 1 for Authentication
SANGFOR_DES	加密算法	SANGFOR VPN Group	Data Encryption Standard for encrypt data
SM2	认证算法	Country Code Management Committee	Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves
SM3	认证算法	Country Code Management Committee	SM3 Cryptographic Hash Algorithm
SM4	加密算法	Country Code Management Committee	Block cipher encryption and decryption algorithm

3.5.2. IP 组设置

内网有不同的 IP 段或者 vlan 拥有不同的上网权限，在这里可以根据 IP 地址进行 IP 组的定义，页面如下：



例如，该客户内网有两个地址段 192.168.1.0/24 和 192.168.2.0/24，那在这里可以进行 IP 组的定义，可以定义单个 IP 也可以定义一段 IP，点新增，出现【IP 组编辑】页面：

『IP 组名称』：给需要定义的 IP 或 IP 段进行命名，可自定义。

『IP 组定义』：可以选择是单个 IP 或 IP 范围，填好之后，点击添加，则会加入 IP 组定义的框中；点确定，则添加到 IP 组定义列表中。

再点击该页面的确定保存配置。

3.5.3. URL 组设置

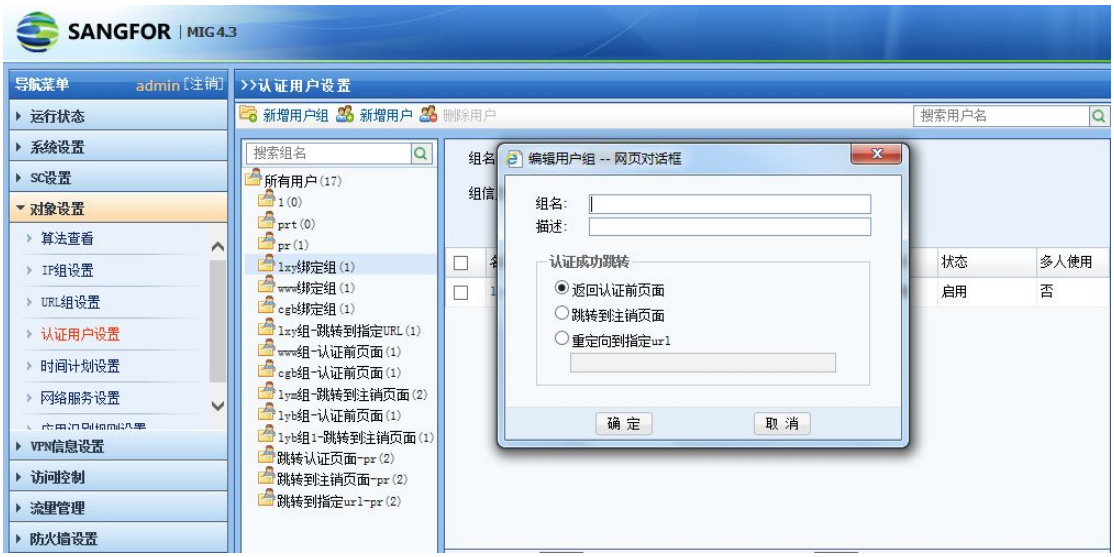
用于定义 URL 组，这些 URL 组可在『访问策略设置』中使用，页面如下：

点新增，出现【URL 组设置】对话框，页面如下：

此处可编辑一个新的 URL 组，URL 组中可包含多个 URL。添加完毕后点确定完成 URL 组的定义。

3.5.4. 认证用户设置

用于定义认证用户组，不同的认证用户组认证成功后可以跳转到不同的页面。页面如下：



『名称』：为用户组命名，名称不能为空且不能超过 30 个字符。

『描述』：对该用户组进行描述。

新增用户，用户名、描述、所属组、密码、ip/mac 绑定等信息 。如图

【新增用户】勾选[启用该用户]，填写[用户名]，[描述]和[当前所属组]。

勾选[本地密码]，在[密码]的输入框中输入用户登录认证的密码。

[绑定 IP/MAC 地址]用于将该用户和 IP/MAC 地址绑定。此例中需要：单向绑定 IP 范围（即限制登录的 IP 范围）为 192.168.1.2-192.168.1.100。

点击[绑定方式]，在弹出的页面中选择[用户和地址单向绑定]

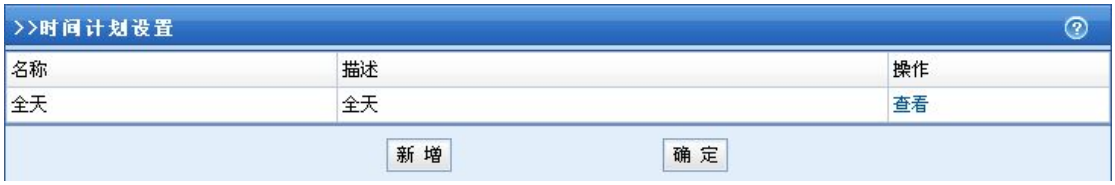
勾选[绑定 IP]，在输入框中填入 *192.168.1.2-192.168.1.100*。

[允许多人同时使用该账号登录]用于设置用户名密码认证的用户，是否可以多人同时用此账号登陆，勾选则表示允许多人同时登录。此例中该用户允许多人同时登陆，需要勾选。

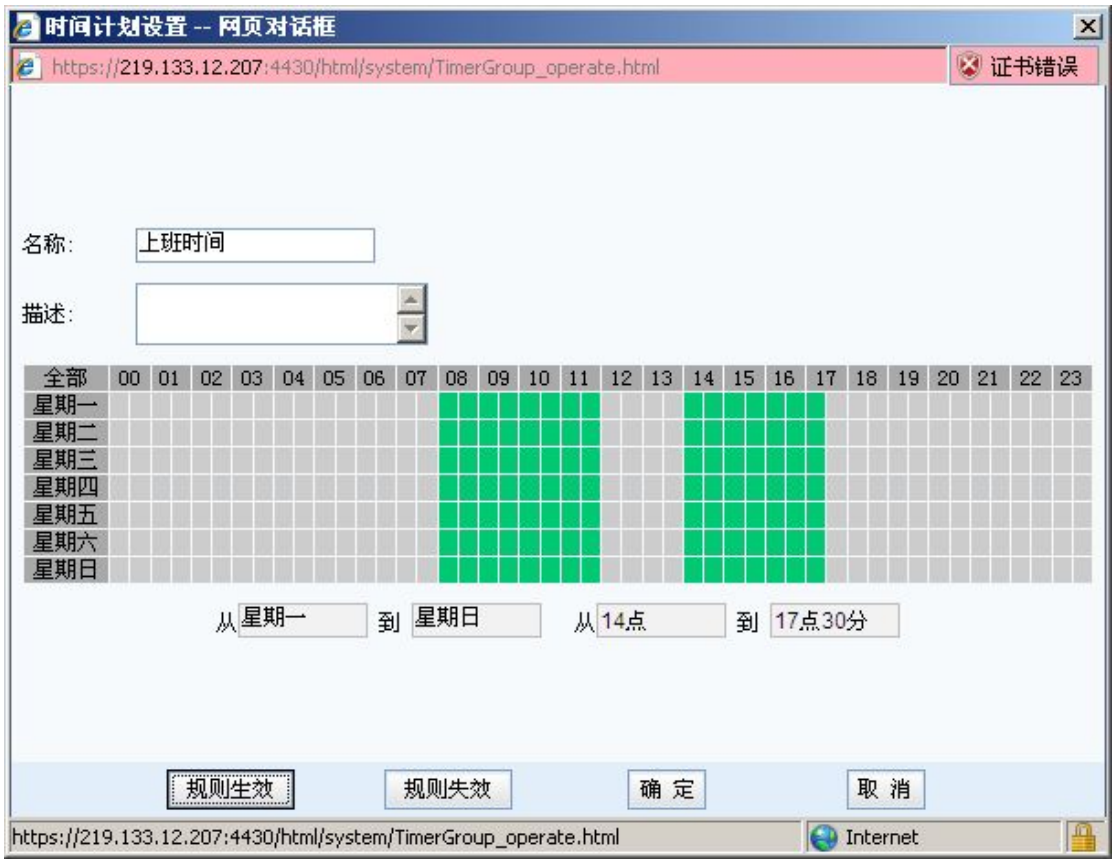
[过期时间]用于设置该用户的过期时间。

3.5.5. 时间计划设置

用于定义常用的时间段组合，这些时间组合可在『IPSEC VPN』、『访问控制』、『流量管理』及『防火墙』模块中使用，以设置相应的规则生/失效时间，该时间以设备上当前时间为准，页面如下：



点新增，出现【编辑时间计划】对话框，页面如下：

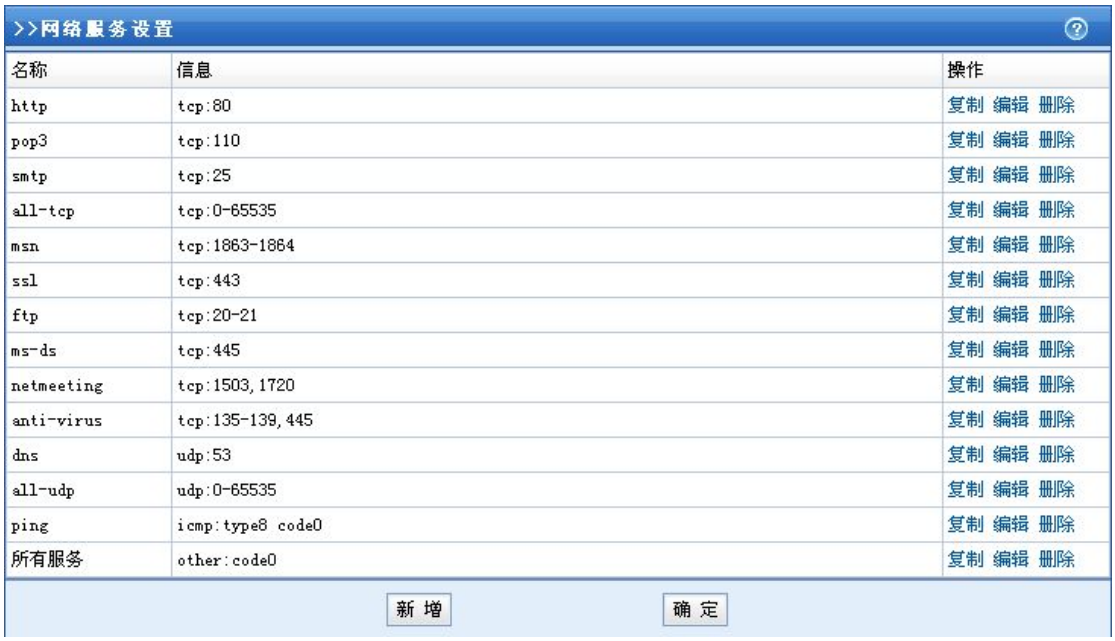


这里，定义了一个名称为“上班时间”的时间段，选取相应的时间段组合，绿色为生效时段，灰色为失效时段。点确定完成时间组的定义。

使用鼠标拖动选择时间范围，然后通过页面的规则生效或规则失效按钮对所选时间段进行设置，最后点击确定，保存此时间计划。

3.5.6. 网络服务设置

通过网络运行的软件和通信程序使用不同的传输协议和端口，在设定针对这些数据的防火墙规则之前需要先定义其传输协议和端口，页面如下：



例如：需要在 SANGFOR MIG 硬件网关上对 SQL SERVER 服务数据的传输设置规则，首先需要对 SQL SERVER 服务所使用的协议和端口进行定义，点击新增，出现【防火墙信息编辑】对话框，页面如下：

『服务名称』可自定义（本例中可设置为：SQL）。『协议』选择 TCP，『端口号』填写 1433，然后点添加，添加到服务定义的框中，点确定将该服务添加到网络服务设置定义列表中，点确定保存即可完成对 SQL SERVER 服务的定义。

在此新增复制功能，可以直接复制该服务规则，点击复制，则出现如下页面：

『服务名称』可以进行修改，添加端口的方式同上。如果客户有个 erp 系统，要用到 SQL 的服务端口，同时还需要 80 等服务端口，可以添加到这个表里面，放通规则的时候只要放通这一个服务就可以了。

3.5.7. 应用识别规则设置

BT、Emule 等下载软件会占用网络大量的带宽资源，QQ、MSN 和炒股软件等即时通讯工具占用上班时间降低工作效率，目前很多公司都明文禁止使用这类软件，但是这些软件在设计的时候就加入了突破防火墙的设置，一般网络防火墙很难阻隔它们。

应用识别规则可以根据协议、端口、方向、数据包长度匹配、数据包内容匹配等多个条件来检测流量，能够很好的检测 P2P 等流量内容。应用识别规则分为内置规则和自定义规则，内置规则不可修改，自定义规则可以增加、删除、修改等。应用识别规则按类型分类，检测出相应的类型流量，可以结合『访问控制』→『访问策略设置』

来做策略。

SNAGFOR MIG 硬件网关采用了应用识别的方式可以有效的阻隔这些软件。每个软件与外部网络通讯时，它所发送的数据包都会有固定的特征值，MIG 硬件网关通过检测数据包中的特征值来识别是否需要阻隔。如果该数据包包含我们设定的特征值，那么它就不能够被发送或者接收，从而达到有效阻隔的目的。

通过应用识别等手段来阻隔某些通讯，关键是分析出这些数据包的特征值，深信服公司会定期提供、更新常见 P2P、IM 等软件的特征值定义，用户也可以询问深信服技术支持申请应用识别规则包，手动导入，另外用户也可以自行分析数据包，定义自己的应用识别规则。点击新增按钮，出现【应用识别规则设置】对话框，如下图所示：

根据分析数据包的结果，设定里面的『匹配内容』特征码即可。

『应用识别规则设置』支持『导入』规则。

如要导入，在设置界面点击浏览选择并打开需要导入的规则（*.ccf 为后缀的规则文件），点击导入即可。

『规则搜索』应用于查找具体规则，在查找对话框内输入规则名称的关键字即可。

『规则优先』可以切换自定义规则和内置应用识别规则的优先顺序，点击更改即可切换，当前优先规则将以红色字体显示。

1．由于 BT 或 IM 软件版本的不同或更新，可能会使个别应用识别规则对有些版本的软件失效。深信服科技会定时更新应用识别规则。如要保证 MIG 能及时更新应用识别规则，请确保设备能正常上网。另外界面上当前内置规则库日期为规则库最后更新日期。

2． 内置规则是不能修改和查看的，只能修改其所在的规则类型。

3.6. VPN 信息设置

包括『基本设置』、『用户管理』、『连接管理』、『虚拟 IP 池』、『隧道间路由设置』、『第三方对接』、『高级设置』等模块。

3.6.1. 基本设置

用于设置 VPN 的一些基本参数。页面如下：

『基本设置』：包括『主、备 WEBAGENGT』、『MTU 值』、『最小压缩值』、『VPN 监听端口』、『直连/非直连』、『共享密钥』等。

『WEBAGENT』：指动态 IP 寻址文件在 WEB 服务器中的地址，包括主 Webagent 和备份 Webagent 地址。

如果是“动态寻址（总部非固定 IP）”请填写“Webagnet 网页地址”（一般为.php 结尾的网页地址），填写完 Webagent 后可以点击测试按钮查看是否能够连通，如果总部是“固定 IP”，请按照“IP 地址:端口”的格式填写，如 202.96.134.133:4009。点击修改密码可以设置 Webagent 密码，以防止非法用户盗用 Webagent 更新虚假 IP 地址，只对网页地址有效。点击共享密钥可以设置共享密钥，防止非法设备接入。

注意：如果设置了『Webagent 密码』，一旦遗失该密码则无法恢复，只能联系深信服科技客户服务中心重新生成一个不包含 Webagent 密码的文件并替换原有文件。如果设置了『共享密钥』，则所有 VPN 网点都必须设置相同的『共享密钥』才能相互连

接通信。如果是多线路且都是固定 IP 的情况下，可以采用“IP1#IP2:port”的方式来填写 Webagent。

『MTU 值』：用于设置 VPN 数据的最大 MTU 值，默认为 1500。

『最小压缩值』：用于设置对 VPN 数据启用压缩的最小数据包大小，默认为 99。

『VPN 监听端口』：用于设置 VPN 服务的监听端口，缺省为 4009，可根据需要设置。

『修改 MSS』：用于设置 UDP 传输模式下 VPN 数据的最大分片。

 **注：『MTU 值』、『最小压缩值』、『修改 MSS』一般情况下请保留默认值，如需设置，请在深信服技术支持工程师的指导下修改。**

『直连』、『非直连』：用于设置网关与 Internet 的连接方式，如果能直接获得 Internet IP 或者能通过端口映射等方式让 Internet 用户可以访问到网关设备的 VPN 端口，则可设置为“直连”，不能获得 Internet IP 的连接方式则需设置为“非直连”。

点击高级可以进行 VPN 性能设置，广播设置和组播设置，如下图所示：

3.6.2. 用户管理

『用户管理』用于管理 VPN 接入账号信息，设置允许接入 VPN 的用户账号、密码，是否启用硬件捆绑鉴权或 DKEY 认证、是否启用虚拟 IP、设置账号使用的加密算法、账号有效时间、账号的内网权限，对用户进行分组并设置组成员的公共属性等用户策略，页面如下：

『检测 DKey』：将检测当前登录网关控制台的计算机是否插入了 Dkey，如没有安装 DKey 驱动则提示用户是否需要下载，用户可以点击手动下载 DKey 驱动直接下载安装。

注意：生成 DKey 前必须安装好 DKey 驱动，否则计算机无法识别 DKey 硬件，

为避免因程序冲突导致 DKey 驱动无法正常安装，请在安装过程中关闭第三方杀毒软件、防火墙等程序。

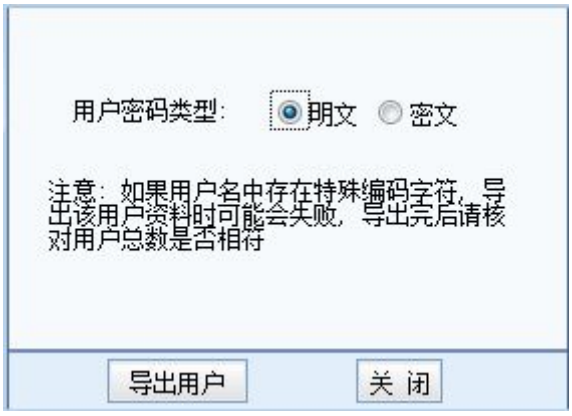
点击查询可对输入的用户名进行查找，以便对查找出来的用户进行编辑操作。

点击高级查询可对查询的用户增加一些过滤条件进行查找。如下图：

点击删除可对勾选的用户进行删除操作。

点击导入文本用户可从 TXT 或 CSV 文件中导入用户信息。

点击导出用户可从设备上将用户导出到本地进行保存，并可选择导出的用户密码是加密还是不加密。页面如下：



『新增组』：可设置用户组『名称』、『描述』以及组成员公共属性（包括『加密算法』、『启用网上邻居』、『内网权限』、『高级』四项设置），如下图：

『新增用户』：可依次设置接入账号的『用户名』、『密码』、『描述』、『算法』等信息，如下图：

『认证方式』：用于设置用户认证类型，这里只支持本地认证。

『类型』：可选移动或者是分支，移动必须启用虚拟 IP，分支不启用。

『使用组属性』：用于对用户进行分组，如勾选[使用组属性]，则可激活选择『用户组』设置，选择将该用户加入到某一个用户组并应用这个组的公共属性。

设置『使用组属性』前请先新增用户组。用户加入用户组后，该用户的『加密算法』、『启用网上邻居』、『权限设置』、『高级』将无法再单独设置。

『启用硬件捆绑鉴权』：用于设置基于硬件特性的证书认证，启用后请选择对应此用户的证书文件（*.id）。

『启用 DKEY』：用于设置是否对移动用户启用 DKey 认证，启用后请先将 DKey 插入计算机的 USB 接口再点击生成 DKEY。

『启用虚拟 IP』：用于给移动用户分配虚拟 IP。当选择用户类型为“移动”的时候，如果为该用户手动设定好一个虚拟内网 IP 地址（该 IP 必须在虚拟 IP 池范围内），则该用户接入后，会使用这个 IP 作为虚拟的内网 IP 地址。如果虚拟 IP 设置为 0.0.0.0，则系统会自动为该用户从虚拟 IP 池中分配一个内网 IP 地址。

『有效时间』和『启用过期时间』：用于设置“接入账号”的有效时间及过期时间。

如 VPN 接入用户需要使用网上邻居服务，则必须勾选[启用网上邻居]。

『启用压缩』：用于设置对网关设备与该用户之间传输的数据使用压缩算法进行压缩。

该设置是 SANGFOR VPN 的独特技术，在低带宽的环境下能有效利用有限带宽，加速数据传输，但并不适用于所有网络环境，实际应用中可根据情况进行设置。

『接入总部后禁止该用户上网』：只对移动用户生效。勾选该选项，则可以让移动用户在连通 VPN 后，只能访问总部 VPN 内网，而不能访问互联网。

『启用多用户登录』：用于设置是否允许多个用户同时共用该账号登录 VPN。

『禁止在线修改密码』：用于设置移动用户是否能够在连上 VPN 后自行修改移动端登录密码，不勾选表示允许用户自行修改密码。

『权限设置』：用于设置用户接入 VPN 后的访问权限，即设置用户只能访问某些服务，默认不做限制。

使用『权限设置』前，请先在『VPN 信息设置』→『高级设置』→『内网服务设置』处添加所需服务。

『高级』：用于设置用户接入 VPN 后的一些高级属性，包括组播服务设置、隧道参数设置。组播服务主要是满足总部和分支间有视频等需要组播支持的应用的需求；隧道内流控是指探测隧道的速度内流控主要是避免某个接入的分支 VPN 流量过大的问题；设置页面如下：

『隧道参数设置』：包括了 VPN 隧道超时时间、动态隧道探测、隧道内流控等内容。

『VPN 隧道超时时间』：在网络时延较大、丢包率较高环境下，SANGFOR VPN 可以针对这些网络设置专门的超时时间，每个隧道的超时时间以总部配置为准，默认超时时间为 20s，若在较差的网络环境中要适当延长超时时间。

『启用动态隧道速度探测』：在本端或对端拥有多线路情况下有效，此时 SANGFOR MIG 设备将会定时探测多线路里各条线路的延时及丢包情况综合选择最优线路进行数据传输。

『启用隧道内流控』：功能用在多个 VPN 分支或者移动用户接入时，为了避免其中某一个分支或者移动用户将总部带宽全部占满导致其他分支或者移动用户访问速度变慢，可以针对每个接入的用户分配一个上下行带宽，从而保证所有用户都能得到较理想的访问速度。

『启用隧道内流控』设置的限制值只是一个范围值，而不是准确值，例如：流控设为 100k，则实际流量会控制在 80-120k 的范围内，是在 100k 左右波动。

3.6.3. 连接管理

为了实现多个网络节点的互联（组成“网状”网络），VPN 硬件网关提供了对网络节点互联的自主管理和设置功能。可在『连接管理』中进行相关的设置。页面如下：

注意：连接管理只有此设备当分支使用需要连接其他 MIG 设备时才需要启用，否则本端是 VPN 总部设备的不需要启用连接管理。

『新增』：可以添加到一个到其他 VPN 总部的连接。页面如下：

『总部名称』：用于标记连接名称，可以任意填写。

『描述』：可自行定义描述信息。

『主/备份 Webagent』：用于填写需要连接的总部的对应 Webagent，点测试按钮可以测试 Webagent 是否工作正常，结果如下所示：

测试请求均是由 PC 机发起的而不是设备发起的。如果 webagent 是用域名形式，测试成功代表该网页存在，否则网页不存在。如果 webagent 采用固定 IP 方式，则测试成功代表填写的 IP:PORT 格式正确。该测试成功并不代表 VPN 就一定能连接成功。

『传输类型』：可选“TCP”或“UDP”，用于决定传输 VPN 数据包的类型，默认为 UDP 模式。

『用户名』和『密码』：请根据总部提供的接入账号信息来填写。

『跨运营商』：适用于总部分支采用了不同运营商线路互联且经常丢包的情况下。可以选择“低丢包率”、“高丢包率”和“手动设置”。

注意：跨运营商功能需要额外激活，否则该功能无效。只要总部激活跨运营商功能，则所有连接到该总部的移动用户均可启用跨运营商功能。如果是设备和设备之间互连，则需要双方都开启跨运营商序列号，否则该功能无效。

『内网权限』：可以对 VPN 连接对端进行权限设置，即指定 VPN 连接对端只能访问本端的那些服务，最后点击确定按钮保存设置信息。

3.6.4. 虚拟 IP 池

『虚拟 IP 池』：由 SANGFOR MIG 系列硬件设备指定设备内网中空闲的一段 IP 作为移动用户接入时的虚拟 IP。当移动用户接入后，分配一个虚拟 IP 给移动用户，移动用户对总部的任何操作都是以分配的 IP 作为源 IP、就完全和在总部局域网内一样。例如使用虚拟 IP 的移动接入后，无论总部局域网的计算机是否把网关指向总部 SANGFOR MIG 系列硬件设备，移动用户均可以访问，还可以为接入的移动用户指定 DNS 等网络属性。页面如下：

1、创建移动虚拟 IP 池。虚拟 IP 池中的 IP 相当于是直连在 SANGFOR MIG 网关设备的网段。

点击新增按钮，出现【虚拟 IP 设置】对话框，选择虚拟 IP 池的类型，设置“IP 池”的起止 IP 即可。页面如下：

点击『虚拟 IP 池』的高级选项可以设置要分配给移动客户端虚拟网卡上的虚拟 IP 子网掩码、DNS、WINS 服务器信息。页面如下：

设定移动虚拟 IP 池后，在『VPN 信息设置』→『用户管理』新建用户，用户类型选『移动』，如果设置虚拟 IP 为 0.0.0.0 表示自动分配虚拟 IP，当移动用户接入后，总部 SANGFOR MIG 硬件网关从虚拟 IP 池中选择一个空闲 IP 分配给移动，也可以为移动用户指定某个固定的虚拟 IP。

注意：当设置了“虚拟 IP 池”的『高级选项』之后，移动客户端电脑中的虚拟网

卡“Sangfor VPN virtual network adapter”必须设置为自动获取 IP 和 DNS，否则“高级选项”里面设置的内容不会分配到移动客户端的虚拟网卡上。

2、创建分支虚拟 IP 池。分支虚拟 IP 池中的虚拟 IP 段提供给分支接入到总部时将分支的原网段替换成虚拟 ip 池中的一个网段，以解决当两个相同网段的分支同时接入到总部时的内网 IP 冲突问题。设置时设定虚拟 IP 的开始 IP、设定虚拟 IP 的掩码和分支的网段数，点击计算可以自动结算出符合要求的结束 IP。页面如下：

『起始 IP』：分支虚拟 IP 段的第一个 IP 地址。

『结束 IP』：分支虚拟 IP 段的最后一个 IP 地址。

『计算』：自动计算虚拟 IP 段的最后一个 IP 地址

『网段数』：需要多少个虚拟 IP 段。

『子网掩码』：虚拟 IP 段的子网掩码。与分支端子网掩码保持一致。

设定分支虚拟 IP 段后，在『VPN 信息设置』→『用户管理』里新建用户，用户类型选『分支』，然后在『高级』→『隧道内 NAT 设置』里配置需要转换的分支网段。

3.6.5. 隧道间路由设置

SANGFOR MIG 系列硬件网关提供了强大的 VPN 隧道间路由功能，通过设置隧道间路由，可轻松实现多个 VPN（软/硬件）之间的互联，真正实现“网状”VPN 网络。

点新增，可以添加一条隧道间路由，如下图：

『网络号(源)』：用来设置隧道间路由的源 IP 地址。

『子网掩码(源)』：用来设置隧道间路由的源子网网段。

『网络号(目的)』：用来设置隧道间路由的目的 IP 地址。

『子网掩码(目的)』：用来设置隧道间路由的目的子网网段。

『目的路由用户』：用来选择隧道间路由条目的目的用户（例如，A 跟 B 之间建立了 VPN 连接，使用的是用户“A”，现在 A 想通过 B 访问到 C，则对 A 设备而言，目的路由用

户为用户“A”）。

勾选[启用]，则该条隧道间路由生效。

勾选[通过目的路由用户上网]，则所有通过该设备的 Internet 流量都将被发往隧道间路由所指目的路由用户，通过目的路由用户把流量转发至 Internet。

 **1.启用通过目的路由用户上网功能时，VPN 远程接入端设备必须部署为网关模式，本端设备网关、单臂部署均可。**

2.新建隧道间路由之前，需先确认在该 VPN 设备的『VPN 信息设置』->『用户管理』中已经建好了用户或者连接管理中配置了连接管理，否则将无法创建隧道间路由。

3. 其中目的路由用户是指:用户管理中未启用多用户登录选项的用户以及连接管理中配置了的用户(不包括二者重名或已禁用的用户)。

勾选[启用路由]，则启用隧道间路由功能。

3.6.6. 第三方对接

SANGFOR MIG 系列硬件设备提供了与第三方 MIG 设备互联的功能，能与第三方的 MIG 设备建立标准 IPSec VPN 连接。

 **第三方对接需要 SANGFOR 设备拥有分支授权才能正常连接，一个第三方连接需要一个分支授权。**

3.6.6.1. 第一阶段

『第一阶段』用于设置需要与 SANGFOR MIG 硬件网关建立标准 IPSec 连接的对端 MIG 设备的相关信息，也就是标准 IPSec 协议协商的第一阶段。页面如下：

设备列表中的某设备已在出入站策略中使用时，该设备不能被删除或改名。

在右上角输入框中可以搜索设备名称和设备地址。

第三方对接必须固定线路出口，默认为线路 1。单臂多线路部署模式下，出口线路自动使用线路 1。

选择线路出口，然后点击新增，页面如下：

『设备名称』：可自行定义。

『描述』：可自行定义。

『设备地址类型』：包括对端是固定 IP、对端是动态 IP、对端是固定域名三种。请根据实际情况选择。选择固定 IP，就填写上对端的 IP 地址；选择动态域名，就填写上对端外网绑定的域名。

注意：标准 IPSEC 不允许连接的双方都是动态 IP，只能允许其中一方为动态 IP。

『预共享密钥』及『确认密钥』：填入正确的预共享密钥，并确保连接双方采用的都是相同的预共享密钥。

点击高级，显示【高级选项】对话框，可进行其它高级设置，如下图：

『ISAKMP 存活时间』：标准 IPSEC 协商的第一阶段存活时间，只支持按秒计时方式。

『重试次数』：当 VPN 故障断开后，重试连接的次数，超过次数还未能连上，则不再主动发起连接，除非有 VPN 流量触发才能再次主动发起连接。

『支持模式』：包括主模式和野蛮模式两种类型。主模式适用于双方均为固定 IP 或者一方固定 IP 一方动态域名方式，并且不支持 NAT 穿透；野蛮模式适用于其中一方为拨号的情况，并且支持 NAT 穿透。

『D-H 群』：设置 Diffie-Hellman 密钥交换的群类型，包括 1、2、5 三种，请与对端设备配置保持一致。

『启用 DPD』：IPSEC 使用 DPD（Dead Peer Detection）功能来检测对端 Peer 是否

存活。“DPD 设置”包括检测间隔和超时次数，多次检测超时后，设备会认为对端失效而断开连接。

『ISAKMP 算法列表』包括认证算法和加密算法：

“认证算法”：选择数据认证的 Hash 算法，包括 MD5、SHA-1、SM3 等。

“加密算法”：选择数据加密的算法，包括 DES、3DES、AES、SANGFOR_DES、SCB2、SM4 等。

SANGFOR_DES 算法，只有在连接双方都是 SANGFOR 设备时才能使用，与其他厂商设备互联时无法使用。

野蛮模式的身份 ID 有 2 种表达方式，一种为域名字符串（FQDN）格式，可以为任意的网址或者一串字符串；另一种为用户字符串（USER_FQDN），需要是“xxx@xxx.xxx”这种格式。

3.6.6.2. 第二阶段

『入站策略』用于设置由对端发到本端的数据包规则，策略较多时自动分页显示。可以在右上角搜索策略名称、源 IP、对端设备名称等；其中对于源 IP 是“子网+掩码”的策略，仅搜索的是子网，不搜索掩码。

点击新增，显示策略设置对话框，页面如下：

『策略名称』及『描述』：可自行定义。

『源 IP 类型』：包括单个 IP、子网+掩码两种类型。分别指定对端 VPN 数据的源 IP 是单个 IP 还是整个网段，并正确填入对端 VPN 数据的源地址。

『对端设备』：该出站策略跟对端哪个设备相关联。

『入站服务』：定义对端哪些类型的服务允许进入 VPN 隧道传输至本端内网。

『生效时间』及『过期时间』：在什么时间范围内，该入站策略有效。

『出站策略』：用于设置从本端发往对端的数据包规则，点击新增，显示【策略设置】对话框，页面如下：

『策略名称』及『描述』：可自行定义。

『源 IP 类型』：包括单个 IP、子网+掩码两种类型。分别指定 VPN 数据的源 IP 是单个 IP 还是整个网段，并正确填入 VPN 数据的源地址。

『对端设备』：该出站策略跟对端哪个设备相关联。

『安全选项』：该出站策略跟哪个安全选项相关联。

『SA 生存时间』：标准 IPSEC 第二阶段协商的存活时间，同样只支持按秒计时。

『出站服务』：定义哪些类型的服务允许进入 VPN 隧道传输至对端内网。

『生效时间』及『过期时间』：在什么时间范围内，该出站策略有效。

注意：『生效时间』模块，只在连接双方都是 SANGFOR 设备情况下生效，与其他厂商设备互联时无效。

『启用密钥完美向前保护』：根据对端设备情况而定，如果对端启用了 PFS，则本端也需要勾上此选项，否则不用勾选。

注意：『出站策略』和『入站策略』中的『出站服务』、『入站服务』和『时间设置』均为 SANGFOR 扩展的规则，此类规则仅在本端设备生效，在与第三方设备建立 VPN 连接的过程中不会协商此类规则。『出站策略』和『入站策略』中策略所对应的源 IP 地址是指『源 IP 类型』和『本/对端服务』中所设置的源 IP 的交集。

3.6.6.3. 安全选项

『安全选项』用于与对端建立标准 IPSec 连接时所使用的参数，页面如下：

在建立与第三方设备的 IPSec 连接前，请先确定对端设备采用何种连接策略，包括：使用的『协议』（AH 或 ESP）、『认证算法』（MD5 或 SHA-1）、『加密算法』（DES、3DES、AES）。点击新增，添加新的选项，页面如下：

SANGFOR MIG 系列硬件设备会使用设置好的连接策略与对端协商建立 IPSec 连接。

『安全选项』中的『加密算法』用于设置标准 IPSec 连接的第二阶段所使用的数据加密算法，如果要与多个采用不同连接策略的设备互联，需要分别将各个设备使用的连接策略添加到『安全选项』中。

3.6.7. 高级设置

包括『内网服务设置』、『VPN 接口设置』、『组播服务设置』等模块。

3.6.7.1. 内网服务设置

SANGFOR 系列硬件设备可以为接入的 VPN 用户指定相应的访问权限，可以限制分支用户内网的某个 IP、某个移动用户只能访问内网的特定计算机的特定服务和与第三方设备互连时设置出入站策略的服务参数。

例如：仅允许用户 test 访问总部的 WEB 服务器的 WEB 服务，对 WEB 服务器其它服务的访问请求都将被拒绝；仅允许分支用户 test 内网的一个 IP 访问总部的 SQL 服务器，分支内网其它 IP 的访问请求将被拒绝等等。通过适当的权限设置，对服务进行访问授权即可实现 VPN 隧道内的安全管理。页面如下：

点击新增，可根据协议类型手动添加内网服务，如下图：

『服务名称』和『描述』可自定义，方便管理即可。

『协议』选择要定义的内网服务所使用的协议

选择[TCP 列表]或[UDP 列表]，还可以设置源 IP、源端口、目标 IP，目标端口等，点击

新增，如下图：

选择为[ICMP 协议]，可设置源 IP 范围和目标 IP 范围，如下图：

所有配置完成后，点击确定保存配置

3.6.7.2. VPN 接口设置

用于设置 VPN 网段的子网掩码，即属于掩码范围之内的 IP 地址就认为是 VPN 数据，其他网段 IP 地址都为非 VPN 数据。页面如下：

“VPN 内网设置”包括 LAN 口和 DMZ 口的 VPN 内网子网掩码设置，“自动同步掩码”是直接使用 LAN 口或 DMZ 口的子网掩码，“自定义掩码”是手动填写 VPN 接口的子网掩码。

“本机 VPN 接口”设置用于设置本端设备的 VPN 接口 IP 地址，可以自动分配或者手动定义 VPN 接口 IP。

3.6.7.3. 组播服务设置

为满足 VOIP 和视频会议等应用，SANGFOR MIG 硬件网关支持组播服务在隧道间传输。在这里可以定义组播的服务，ip 范围是 224.0.0.1-239.255.255.255，端口范围是 1-65535。页面如下：

点击新增出现组播服务编辑页面，在这里可以设置组播服务所用的组播地址和端

口。页面如下：

定义『名称』和『描述』，点新增，可以设置组播服务所用的组播地址和端口。

定义好组播服务后，在『VPN 信息设置』→『用户管理』新建用户，然后在『高级』→『组播服务设置』里配置组播服务。页面如下：

3.7. 访问控制

包括『ipmac 认证设置』、『认证选项设置』、『访问策略设置』三个子模块，注意该功能只对正常上网的数据流有效，对 VPN 数据流无效。

3.7.1. IPMAC 认证设置

『IPMAC 认证设置』主要是用于设置 MIG 硬件网关与用户认证相关的配置信息。设置界面如下图所示：

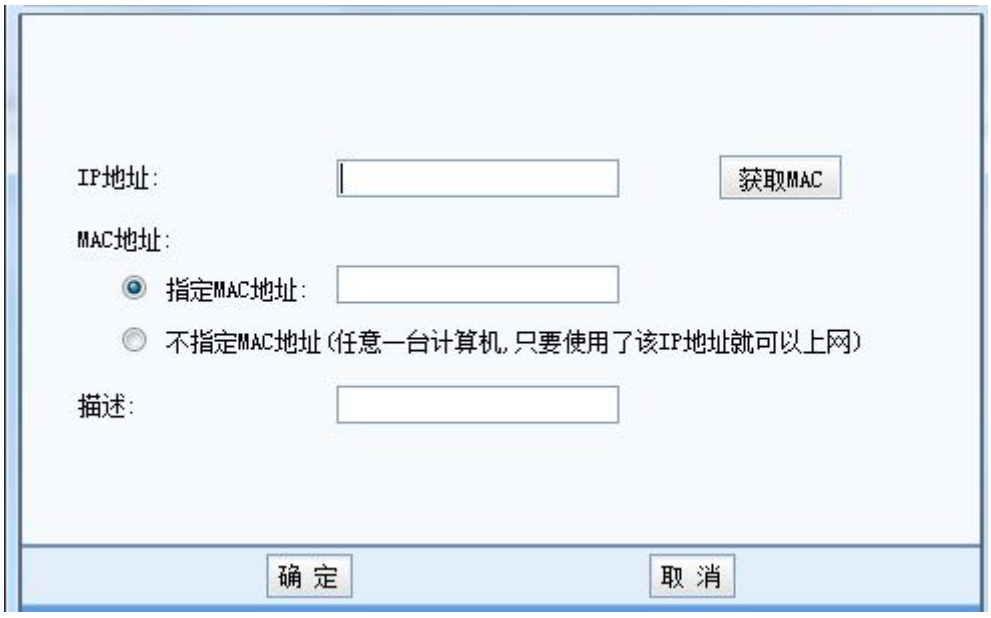
有启用『仅允许授权列表的计算机上网』及『新计算机自动添加到授权列表中』

的功能。

勾选『仅允许授权列表的计算机上网』，指仅允许授权列表中的并且通过了 IP 或者 MAC 绑定认证的计算机上网，不在该列表中的，或者 IP/MAC 绑定不匹配的则不允许上网。

勾选『新计算机自动添加到授权列表中』，即启用自动添加新用户到授权列表的功能。

『指定 MAC 地址』：点击新增，填写 IP 和 MAC 信息，用于 IP/MAC 地址的绑定。或者只输入 IP 地址，点击自动获取以获取对应计算机的 MAC 地址信息。设置界面如下图所示：



『不指定 MAC 地址』：则指绑定 IP，任何一台电脑只要配置了该 IP 就会匹配这条授权规则。

点击获取 mac，设置搜索范围，系统将自动在所设置的 IP 地址范围内搜索存在的计算机的 IP/MAC 信息。设置界面如下图所示：

点击删除可对勾选的授权规则进行删除操作。

点击确定按钮保存设置信息。

IP/MAC 绑定功能，在内网存在三层环境情况下，可以采用计算机 IP 绑定三层设备 MAC 地址的方式实现。因为我们设备支持多 IP 对应一个 MAC，但是不支持多 MAC 对应一个 IP。

自动搜索只可以获取本机所在局域网的 IP 和对应的 MAC 地址，同时会自动更新已有的 IP 对应的 MAC 地址，当添加达到 100 条后，将不再添加。该功能只能在二层环境下使用。

3.7.2. 认证选项设置

『认证选项设置』主要是用于设置内网用户的上网认证的测试，认证 ip 范围，自动认证设置，其他选项　设置如图

启用认证弹框认证(默认开启所有 ip 认证)，

排除 ip 列表中的 ip 将不再受认证策略控制

自动认证

自动绑定用户的 ip/mac 并且以 ip 显示用户。认证成功后添加对应的组里面，使用对应的组策略。自动绑定三种方式①绑定 ip ；②绑定 mac ；③绑定 ip 和 mac 分两种[绑定方式]：单向绑定和双向绑定。

单向绑定：用户只能使用指定的地址认证，但其它用户也允许使用该地址进行认证。

双向绑定：用户只能使用指定的地址认证，并且指定的地址仅供该用户使用。

其他认证选项

自定义认证页面支持用户自定义网页，但是必须是 zip 文件格式。
自动注销无流量用户，如果用户在设置的时间内网无流量产生，该用户将被注销掉。

3.7.3. 访问策略设置

『访问策略设置』主要是用于设置内网用户的上网策略，上网策略包括『应用服务控制』、『网络服务控制』、『URL 控制』，此处设置的策略对象可以适用于多个用户组同时用于上网行为的控制。设置界面如下图所示：

『访问策略列表』用于显示已经设置完成的策略对象。显示内容包括『策略名称』、

『用户组』、『调整』、『操作』，访问策略列表从上到下依次匹配。

点击『访问策略设置』中的立即生效，生效当前所有策略。

点击『访问策略设置』中的新增，进入策略编辑页面，如下图：

『策略名称』可填写便于理解记忆的文字，建议使用便于标识的文字。

『适用用户组』可选“全部”、“自定义”。选取已经定义好的用户组。

『应用服务控制』：为了方便网络管理人员对内部局域网用户的上网行为做出限制，SANGFOR MIG 硬件网关提供了基于数据包内容检测来实现对具体应用服务的控制。

点击新增，出现添加的界面如下：

选择好『应用类型』、『应用名称』、『规则名称』、『动作』、『生效时间』，最后点击添加，即完成一条『应用服务控制』规则的设置。例如：限制内网只能访问基于 HTTP 协议的应用，即把所有 HTTP 的应用和 DNS 应用允许即可。（应用类型、应用名称、规则名称的定义，请参见前面『对象设置』的相关章节。）

通过全选和反选的组合可快速的选中要编辑的上网权限。

单击允许，拒绝或删除对选定的上网权限进行相应的操作。

单击上移和下移可移动选定上网权限的顺序。

『缺省允许』、『缺省拒绝』一般和上面列表所定义的上网权限规则配合使用。匹配不了上面列表的规则，就会执行这里的缺省操作。

最后点击确认，保存设置。

『网络服务控制』为了方便网络管理人员对内部局域网用户的上网行为做出限制，SANGFOR MIG 硬件网关提供了根据目的 IP、协议端口、时间段等来实现网络服务控制的功能。

点击新增，出现添加的界面如下：

选择好『目标 IP 组』、『服务』、『动作』和『生效时间』之后，点击添加，即完成一条『网络服务控制』规则的设置。例如想限制内网用户上班时间不能浏览网页，可以把 HTTP 服务拒绝掉即可（目标 IP 组、服务、时间的定义，请参见前面『对象设置』的相关章节）。

通过全选和反选的组合可快速的选中要编辑的上网权限。

单击允许，拒绝或删除对选定的上网权限进行相应的操作。

单击上移和下移可移动选定上网权限的顺序。

『缺省允许』、『缺省拒绝』一般和上面列表所定义的上网权限规则配合使用。匹配不了上面列表的规则，就会执行这里的缺省操作。

最后点击确认，保存设置。

『URL 控制』用于对内网用户访问网页的控制。

点击新增按钮，选择好『URL 组名称』、『动作』和『生效时间』之后，点击添加，即完成一条『URL 控制』规则的设置。例如想限制内网用户上班时间不能浏览优酷等在线视频网站，可以在『URL 组名称』里面选择视频网站，动作选择拒绝，生效时间选择上班时间即可。如下图：

通过全选和反选的组合可快速的选中要编辑的上网权限。

单击允许，拒绝或删除对选定的上网权限进行相应的操作。

单击上移和下移可移动选定上网权限的顺序。

『缺省允许』和『缺省拒绝』选项，代表不能匹配上面设定的 URL 规则时，所执行的操作。

最后点击确认，保存设置。

3.7.3.1. 案例学习

某公司的上海分公司新购买了一台深信服 MIG2.0 的硬件网关设备，设备网关模式部署，分公司内网 30 个用户需要分成 2 个上网组：一个是受限组，IP 地址范围是 192.168.1.2 至 192.168.1.20，只允许打开网页。另一个为仅拒绝 P2P 流量组，IP 地址访问是 192.168.1.21 至 192.168.1.32，禁止 P2P 相关流量。实施步骤如下：

第一步：将用户划分到不同的用户组。在『对象设置』的『用户组设置』页面新增 2 个用户组，分别将 192.168.1.2 至 192.168.1.20 划分到受限组，将 192.168.1.21 至 192.168.1.32 划分到仅拒绝 P2P 流量组。点击新增按钮新增受限组和仅拒绝 P2P 流量组：

点击立即生效按钮，生效策略。

第二步：在『访问控制』的『访问策略设置』页面，点击新增按钮，新增一条只允许访问网页的策略，适用用户组选择“受限制组”，应用服务控制选择缺省拒绝，仅放

行 DNS 服务和 HTTP 应用。然后点击确定按钮。如下图：

再点击新增按钮，新增一条仅拒绝 P2P 流量的策略，适用用户组选择仅拒绝 P2P 流量组，应用服务控制选择缺省允许，拒绝 MEDIA、P2P 流媒体、P2P、文件下载，然后点击确定按钮。如下图：

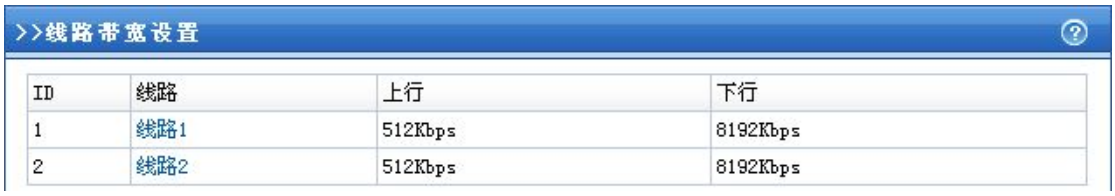
最后点击立即生效按钮，生效策略。

3.8. 流量管理

MIG4.3 流量管理系统提供了强大的带宽保证和带宽限制功能，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、单用户建立带宽保证和带宽限制策略。

3.8.1. 线路带宽配置

用于配置设备外网线路的实际上、下行带宽，是带宽保证和带宽限制的基础。配置界面如下所示：



ID	线路	上行	下行
1	线路1	512Kbps	8192Kbps
2	线路2	512Kbps	8192Kbps

『线路带宽』：用于设置设备外网线路实际的上下行带宽。

『线路类型』：用于设置线路的两种方式，以太网和 ADSL，配置为 ADSL 后，流控策略中设置的带宽会自动乘以 90%，比如流控策略中设置限制带宽为 30%，设置为 ADSL 后，实际限制的带宽为 27%（显示的百分比不变，但对应的实际值会变成“带宽*90%*30%”）。

线路带宽配置不当可能造成带宽浪费（配小了）或线路拥塞（配大了）。

3.8.2. 流控策略设置

MIG 硬件网关提供的带宽分配功能，用于保证和限制上网带宽。根据应用服务、适用对象、生效时间来选择带宽分配策略，定义流量通道。实现带宽保证或带宽限制的目的，在流控策略列表中，匹配顺序自上而下依次匹配，可以通过上移或者下移的操作调整策略的匹配顺序。配置界面如下：

『系统配置』用于开启流量管理功能，选择『启用』或『禁用』并点击确定开启或者关闭此功能。

『流控策略列表』显示用户已经配置好的流控策略。

点击新增，出现以下页面：

『策略名称』：为策略命名，名称不能为空且不能超过 30 个字符。

『启用策略』：选择是否启用该策略。

『适用用户组』：用于规则所生效的用户组，可以应用于所有用户组，也可以选择某些用户组。界面如下所示：

『适用应用服务』：用于定义该策略适用的具体服务，若选择自定义，可以新增服务类型，界面如下所示：

点击新增按钮，可选择『应用类型』下属的『应用名称』，则可根据需要来选择应用类型和应用名称；

『生效时间』：应用于规则生效的时间范围。

『带宽分配策略类型』：应用于选择流量策略是带宽保证还是带宽限制。如果选择的是带宽保证策略，保证的是用户的最低带宽，同时可以限制最大上下行。若选择带宽限制，则只对上网服务做带宽限制。带宽保证界面如下图所示：

『优先级』：可以选择优先级 1、优先级 2、优先级 3、优先级 4。优先保证带宽在带宽有空闲的情况下优先占用空闲带宽。

『保证上行带宽』和『保证下行带宽』：用于设置预留带宽占总上网带宽的比例。

『最大上行带宽』和『最大下行带宽』：用于设置限制此通道上下行带宽的总上限。

带宽限制设置界面如下图所示：

『限制单用户最高带』：应用于限制单个用户的最大上、下行带宽，勾选[启用]开启。

单用户带宽限制设置的是固定带宽而非百分比，不受线路带宽设置改变的影响；而带宽保证与带宽限制是当前流量的百分比，受线路带宽设置大小变化而改变。

3.9. 防火墙设置

SANGFOR MIG 硬件网关集成了高性能的企业级状态检测防火墙，能有效保护内部网络免受来自包括 Internet、VPN 连接的其它局域网等多方面的攻击。同时，内置的防 DOS 攻击功能，不仅可以有效防范来自外部网络的 DOS 攻击，对于内网计算机发起的 DOS 攻击，SANGFOR MIG 硬件网关也可以进行防御。包括『过滤规则设置』、『NAT 设置』、『防 DOS 设置』、『ARP 欺骗防护』模块。

3.9.1. 过滤规则设置

SANGFOR MIG 硬件网关防火墙采用状态检测包过滤技术，可在多个数据传输方向上结合时间计划实现基于协议类型、源 IP、目的 IP 的数据包过滤。

『过滤规则设置』包括了本机规则、LAN<->DMZ、DMZ<->WAN、WAN<->LAN、

VPN<->LAN、VPN<->WAN、VPN<->DMZ，四种网络接口，十二个方向的规则设置。

所有的 VPN 数据都会经由 VPN 接口传输（例如：本端设备 LAN 接口下的计算机与 VPN 对端计算机的数据通信是经由设备 LAN 接口与 VPN 接口传输），因此可以通过防火墙的过滤规则对 VPN 数据进行控制。

『本机规则』用于设置外网用户通过公网 IP 配置、管理、维护等权限。

『LAN<->DMZ』用于设置 SANGFOR MIG 设备的 LAN 接口与 DMZ 接口之间双向数据传输的防火墙过滤规则。

『DMZ<->WAN』用于设置 SANGFOR MIG 设备的 DMZ 接口与 WAN 接口之间双向数据传输的防火墙过滤规则。

『WAN<->LAN』用于设置 SANGFOR MIG 设备的 WAN 接口与 LAN 接口之间双向数据传输的防火墙过滤规则。

『VPN<->LAN』用于设置 SANGFOR MIG 设备的 VPN 接口与 LAN 接口之间双向数据传输的防火墙过滤规则。

『VPN<->WAN』用于设置 SANGFOR MIG 设备的 VPN 接口与 WAN 接口之间双向数据传输的防火墙过滤规则（如果 VPN 连接对端在『隧道间路由设置』中设置了以本端作为『目的路由用户』并启用『通过目的路由用户上网』，则在本端可通过设置 VPN<->WAN 的过滤规则实现对分支上网数据的控制）。

『VPN<->DMZ』用于设置 SANGFOR MIG 设备的 VPN 接口与 DMZ 接口之间双向数据传输的防火墙过滤规则。

下面以本机规则、LAN<->WAN、VPN<->LAN 为例介绍过滤规则设置的一般步骤：

1、本机规则

此页面用于设置外网用户通过公网 IP 配置、管理、维护等权限，页面如下：

『允许外网到本机的 ping 和 tracert』：允许外网用户直接 ping 本地的 wan 口，主要用于测试网络的连通性等

『允许外网登录设备查看实时日志』：用于厂商人员的维护

『允许外网使用升级客户端进行维护』：用于外网通过升级客户端连接设备进行升级、调试等操作。

2、LAN<->WAN

此界面用于设置 LAN 口与 WAN 口之间数据传输的防火墙过滤规则，可根据实际环境设置放行某类服务数据或拒绝某类服务数据。例如要使 LAN 与 WAN 口之间完全互通并且能够使用 PING 命令进行测试，则需要在两个方向上开放所有的 TCP、UDP 以及 ICMP 过滤规则。页面如下：

点击上移或者下移按钮，可以将规则向上或者向下移动一条。防火墙规则是自上而下依次匹配的，可以使用上移或者下移来满足不同策略的优先级。

点击拖动按钮，并按住鼠标左键不松，可以将该规则移动到想要的位置。

点击复制按钮，可以复制该规则，并且可以在该规则的基础之上进行修改，并保存为一条新的规则。

勾选[显示隐式规则]，则会显示出在代理上网或者端口映射规则自动放通的防火墙过滤规则，无需再手动放通一次。

设置规则时需要注意数据的方向和动作，页面如下：

『规则名称』：自定义规则名称。

『规则方向』：设置此规则对哪个方向的数据生效。

『规则动作』：设置数据匹配此规则后的执行动作。

『服务对象』：设置规则要匹配的服务类型。

『源 IP 组』：设置规则要匹配的源 IP 地址。

『目的 IP 组』：设置规则要匹配的目的 IP 地址。

『时间组』：设置规则生效的时间。

勾选[启用规则]选项，则此规则设置完成后立即生效。

勾选[启用日志]选项，则所有匹配此规则的数据包经过设备时日志系统都将记录日志，一般情况下请不要启用，以免系统产生大量日志。

3、VPN<->LAN

此界面用于设置 VPN 接口与 LAN 接口之间数据传输的防火墙过滤规则，默认规则已放行了双向的所有 TCP、UDP、ICMP 数据，页面如下：

3.9.1.1. 案例学习

某公司总部只允许接入总部的 VPN 分支（172.16.1.0/24）的其中一部分 IP 地址（172.16.1.100-172.16.1.200）访问总部内网服务器（192.168.10.20）的 WEB 服务，但禁止这一部分 IP 访问总部内网服务器的 SQL SERVER 服务。

设置步骤如下：

首先进行『IP 组设置』，在『对象设置』→『IP 组设置』中进行配置。

VPN 分支配置页面如下：

『IP 组名称』：给需要定义的 IP 或 IP 段进行命名，可自定义。

『IP 组定义』：选择 IP 范围，填入分支允许访问的 IP 地址段起始 IP：172.16.1.100，结束 IP：172.16.1.200 之后，点击添加，则会加入 IP 组定义的框中；点确定，则完成“vpn 分支 1”IP 组的设置。

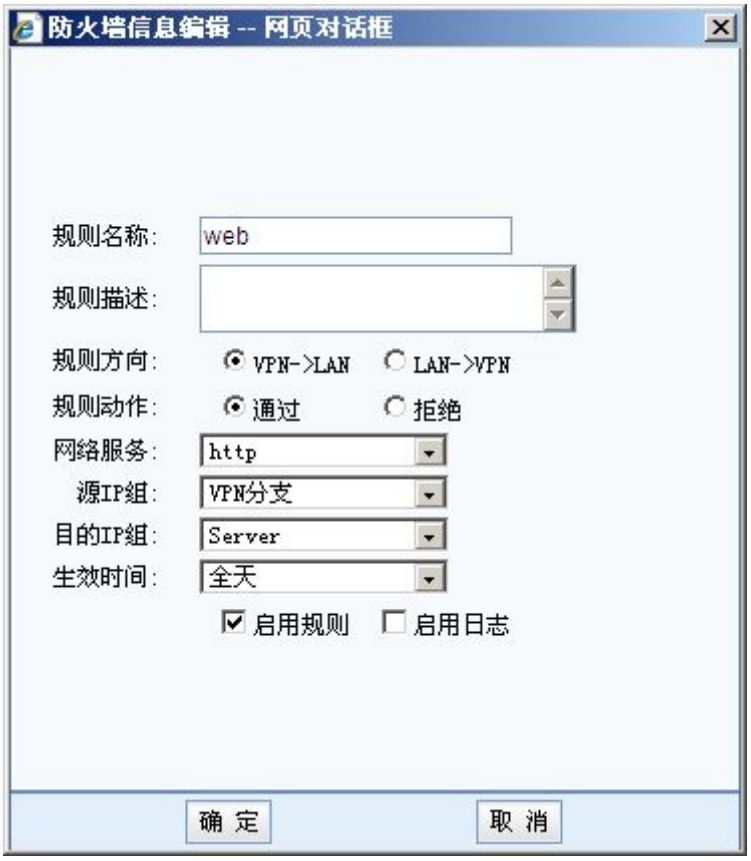
内网服务器配置界面如下：

『IP 组名称』：给需要定义的 IP 或 IP 段进行命名，可自定义。

『IP 组定义』：选择单个 IP192.168.10.20，填好之后，点击添加，则会加入 IP 组定义的框中；点确定，则添加到『对象设置』→『IP 组设置』列表中。

再点击该页面的确定保存配置。

然后新建 WEB 服务过滤规则，配置页面如下：



『规则名称』：自定义规则名称。

『规则方向』：设置为 VPN->LAN。

『规则动作』：设置为对此类数据通过。

『服务对象』：设置为 HTTP。

『源 IP 组』：选择设置好的 IP 组“vpn 分支”。

『目的 IP 组』：选择设置好的 IP 组“Server”。

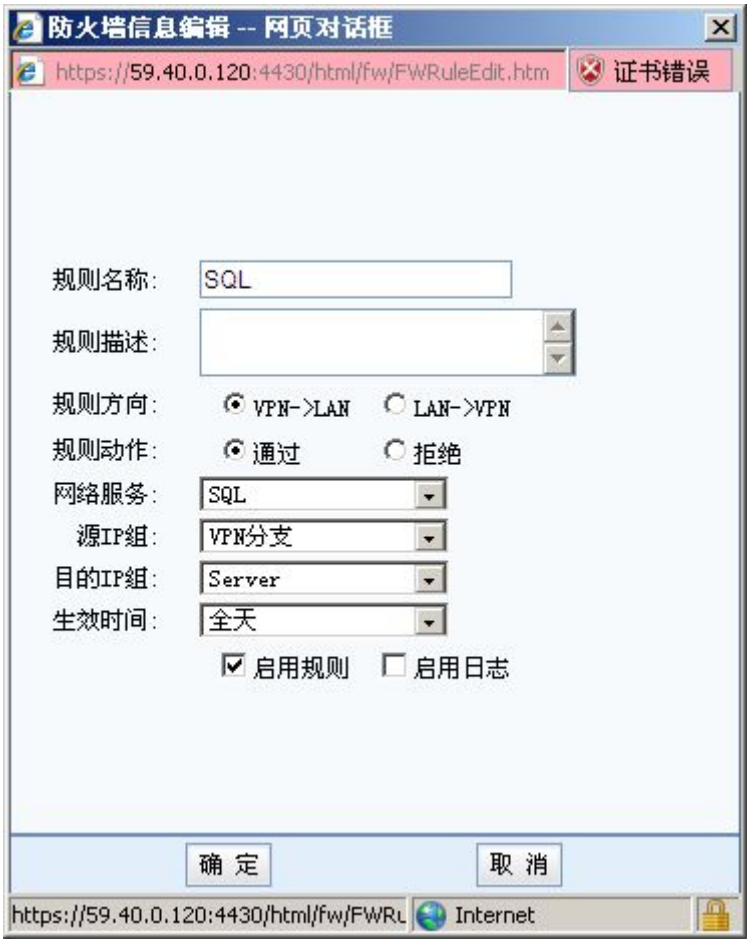
『时间组』：设置规则生效的时间。

勾选[启用规则]选项，点确定完成。

接下来设置 SQL SERVER 服务过滤规则，首先进行服务定义，页面如下：

『服务名称』可自定义（本例中可设置为：SQL）。『协议』选择 TCP，『端口号』填写 1433，然后点添加，添加到服务定义的框中，点确定将该服务添加到『对象设置』→『网络服务设置』列表中，点确定保存即可完成对 SQL SERVER 服务的定义。

接着设置 SQL SERVER 服务过滤规则，页面如下：



『名称』：自定义为 SQL。

『方向』：设置为 VPN->LAN。

『规则动作』：设置对此类数据拒绝。

『服务对象』：设置为 SQL。

『源 IP 组』：设置为分支内网的部分 IP 地址 172.16.1.100-172.16.1.200。

『目的 IP 组』：设置为总部内网的服务器 IP192.168.10.20。

『时间组』：设置规则全天生效。

勾选[启用规则]选项，点确定完成。

完成上述设置后，即可实现案例所述需求。

其他如限制总部访问分支服务、限制分支通过总部上网的数据等需求都可以通过在相应接口之间设置过滤规则实现。

3.9.2. NAT 设置

NAT 设置包括『代理上网设置』、『端口映射设置』内容。

3.9.2.1. 代理上网设置

『代理上网设置』用于设置防火墙代理局域网上网的规则，SANGFOR MIG 硬件网关不仅有基本的 NAT 代理上网功能，还可通过与过滤规则进行配合对内网的上网服务进行控制，在该页面中的代理上网的规则可以分别通过『状态』、『名称』、『源接口』、『源地址』、『目的接口』等进行排序，页面如下：

设备缺省设置中不包含代理规则，需要手动添加，点击新增，『名称』可自定义，填写代理网段，并点击确定，页面如下：

[名称]用于自定义规则名称

[转换条件/源地址]源接口用于设置数据包的源接口地址，表示从该接口过来的数据会继续往下匹配，可以选择 LAN、DMZ、VPN 三种。子网网段和子网掩码用于设置需要转换的源地址网段。

[转换条件/目的地址]目的接口用于设置数据包的出接口地址，表示从该接口出去的数据会计息往下匹配，可选择 LAN、DMZ、VPN 三种。子网网段和子网掩码用于设置匹配条件，表示数据包的目标 IP 地址在设置的范围内，则可以匹配到该规则。

[源地址转换为]用于设置符合指定条件的数据包转换源地址为“目的接口地址”或者“指定地址”。选择目的接口地址，则会将数据包源地址转换为“目的接口”选择的接口 IP 地址。选择“指定地址”则需要手动设置一个 IP 地址。

勾选[启用规则]，则规则生效，防火墙会自动对应的过滤规则。

下面以一个简单的示例来说明代理上网规则如何设置。举例如下：

常用代理上网设置示例一：

某客户出口是一台 MIG 1200 设备，WAN 口为 ADSL 拨号，LAN 口 IP 地址为 192.168.1.1，内网 PC 都是 192.168.1.0/24 网段，网关指向 192.168.1.1。部署 MIG 1200 设备后，需要保证内网 PC 可以访问公网。配置方法如下：

第一步：配置设备接口 IP 地址，IP 地址配置请参考『系统设置』-『网络接口设置』章节。此处不赘述。

第二步： 配置代理上网，源接口选择 LAN，子网网段填写 LAN 口网段，出接口为上公网的 WAN 口，目的 IP 地址为所有 IP 地址，将源地址转换为 WAN 口 IP，界面如下：

常用代理上网设置示例二：

某客户总部与分支用 SANGFOR VPN 对接，连上了 VPN 隧道，总部使用 MIG 1200 设备，分支使用 VPN 1110 设备，分支内网网段为 192.168.1.0/24。客户希望分支的用户全部通过总部上网，而不通过分支的网络上网。配置方法如下：

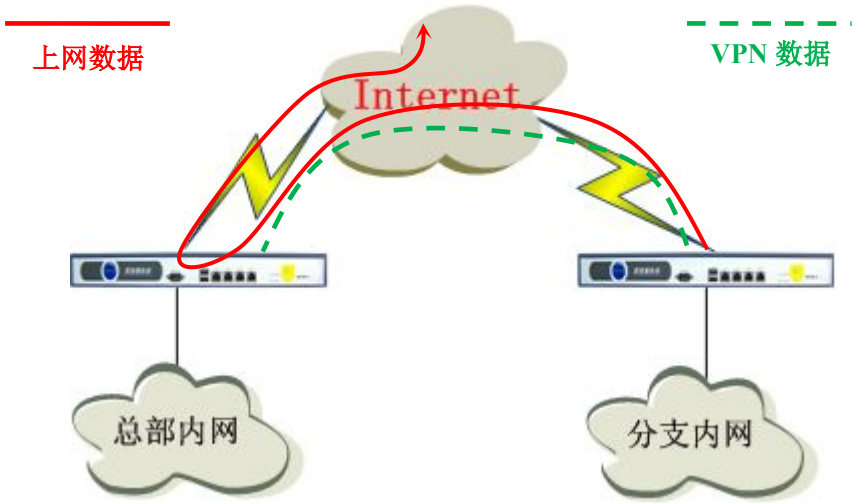
第一步：在分支端的 MIG 设备配置隧道间路由，并且勾选“通过目的路由用户上网”，详细请参考『VPN 信息设置』-『隧道间路由设置』章节。

第二步：在总部端的 MIG 设备配置代理上网规则，源接口选择 VPN 接口（因为是从 VPN 对端过来的数据），源地址填写 192.168.1.0/24，目的接口选择 WAN，界面如下：

关于源接口选择 VPN 的高级应用场景及案例请参考『案例学习』

案例学习

总部 SANGFOR 设备采用路由模式部署，分支（172.16.10.0/24）需通过 VPN 接入总部后上网，拓扑图如下：



则在 VPN 正常连接的情况下，分支 SANGFOR 设备需要添加隧道间路由（详见 2.6.5『隧道间路由设置』小节），总部 SANGFOR 设备需添加『内网接口』为 VPN 的代理规则并添加分支的内网网段，页面如下：

防火墙规则是会自动放通，无需手动去放通。点击『防火墙设置』→『过滤规则设置』→『VPN<->WAN』，勾选显示隐式规则，则可看到自动放通的防火墙规则，页面如下：

>>代理上网配置

状态	名称	源接口	源地址	目的接口	目的地址	转换后IP	操作
启用	代理上网	LAN	10.254.254.0/255.255.255.0	WAN	所有IP	目的接口地址	复制 编辑 删除
启用	代理VPN上网	VPN	172.16.10.0/255.255.255.0	WAN	所有IP	目的接口地址	复制 编辑 删除

新 增　　确 定

3.9.2.2. 端口映射设置

『端口映射设置』用于设置防火墙的 DNAT 规则，如果局域网内的服务器需要向外网提供服务，则需要添加『端口映射设置』，在该页面中的端口映射的规则可以分别通过『状态』、『规则名称』、『源接口』、『源 IP』、『源端口』、『目的接口』、『目的 IP』、『目的端口』、『协议』进行排序，页面如下：

点击新增，用来增加一条端口映射，页面如下：

[名称]用于自定义规则名称

[转换条件/源地址]源接口用于设置数据包的源接口地址，表示从该接口进来的数据会继续往下匹配，可以选择 LAN、DMZ、WAN 三种。选择 WAN 口在双线路情况下还需要线路对应的线路，子网网段和子网掩码用于设置源地址匹配条件，表示数据包的源 IP 地址在设置的范围内，则可以往下匹配。

[转换条件/协议]用于设置协议的转换条件，表示数据包的封装协议符合设定的条件，则继续往下匹配。

[转换条件/目的地址]用于设置转换条件，表示数据包的目的地址符合设定的条件，则继续往下匹配。

[转换条件/端口]用于设置转换条件，表示数据包的目的端口符合设定的条件，则继续往下匹配。

[转换为/目的接口]用于设置符合上述条件的数据包的出接口，表示符合上述的设置条件，又从该目的接口出去的数据包进行目的地址转换和目的端口转换。

[转换为/目的地址]用于设置转换的数据包目的地址，表示符合上述所有条件的数据包，将该数据包的目的地址转换成设置的值。

[转换为/目的端口]用于设置转换的数据包目的端口，表示符合上述所有条件的数据包，防火墙会将该数据包的目的端口转换成设置的值

勾选[启用规则]，则规则生效，防火墙会自动对应的过滤规则。

下面以一个简单的示例来说明代理上网规则如何设置。举例如下：

端口映射设置示例：

某客户出口部署 MIG 1200，一条电信线路接到设备的线路 1，WAN 口 IP 地址为 202.96.137.75，LAN 口 IP 地址为 192.168.1.1，内网有一台 WEB 服务器（80 端口提供服务）IP 地址为 192.168.1.100，现在客户希望公网的用户也能访问到 192.168.1.100 这台服务器。配置方法如下：

第一步：基础网络配置，配置接口 IP 地址信息，请参考网络接口配置章节，此处不赘述。

第二步：配置端口映射，本案例中的配置信息如图所示：

注意：通过 SANGFOR VPN 硬件设备设置端口映射向外网提供服务的内网服务器，必须是以 VPN 硬件设备作为 NAT 代理上网（网关指向 VPN 或上网路由最终指向 VPN），否则端口映射将无法生效。

3.9.3. 防 DOS 攻击

防火墙不仅肩负着阻隔 Internet 上的用户对局域网非法攻击的任务，很多时候由于局域网内有电脑中毒，会向网关发送大量的数据包，这样有可能会造成带宽阻塞或者网关死机。SANGFOR MIG 系列硬件设备内部集成了『防 DOS 攻击』功能，可以监测单位时间内某个 IP 向网关发送了多少数据量，当超过一定值时则 MIG 系列硬件设备会认为受到此 IP 的 DOS 攻击，并会阻断此 IP 一段时间从而保护自己。页面如下：

在『内网网段列表』中添加局域网所包含的网段，当这里为空的时候即表示不检查 IP 地址。当添加了内网网段后，当源 IP 不属于『内网网段列表』所列网段范围之内，则该数据包会被直接丢弃。属于『内网网段列表』范围时，则会进行下面防 DOS 攻击各项设置的计算和探测，以进行相应的处理。

同理，『内网路由器列表』的功能和『内网网段列表』功能类似，当添加了内网路由器地址后，MIG 设备会自动获取内网路由器的 mac 地址，针对路由器的 mac 地址将不做防 DOS 攻击检测。如果不正确填写，则可能导致误将内网路由器封锁掉，从而导致所有通过该路由器的用户无法正常上网。

其它选项可根据情况来进行相应设置，包括『最大 TCP 连接数』,『最大 SYN 包数』及『防 DOS 攻击的封锁时间』等。

3.9.4. ARP 欺骗防护

ARP 欺骗是一种常见的内网病毒，中病毒的电脑，不定时的向内网发 ARP 欺骗的广播包，使内网机器的正常通信受到干扰和破坏，严重时会导致整网断网。

MIG 通过不接受有攻击特征的 ARP 请求或回复来保护 MIG 本机的 ARP 缓存，实现自身的免疫。如果 MIG 访问控制的授权列表中有绑定的 IP/MAC，则 MIG 会以绑定

的 IP/MAC 信息为准。

配置界面如下所示：

『启用 ARP 欺骗防护』：是启用 ARP 欺骗防护的总开关。

『静态 ARP 设置』：可以勾选[启用]，启用之后如果内网 PC 的网关不是 MIG 的接口，那就需要在这里设置，否则 MIG 当收到内网 PC 网关的 IP 的时候因为 IP/MAC 不对应会被丢包；如果内网 PC 的网关是 MIG，则这里不需要进行设置。

『网关 MAC 广播时间』：是设置广播网关（即 AC 的内网接口）的 MAC 的时间间隔。建议设成 10 秒。

点击确定可保存该部分的配置。

点击广播网关 MAC 用于立即广播设备内网接口的 MAC 地址。当内网 ARP 欺骗被清除后，可通过该按钮迅速恢复内网 PC 的 ARP 表。

3.10. 系统维护

3.10.1. 新手向导

在这里可以按照向导完成您的配置。

新手向导可以根据您的需求，按照配置提示，点击相应的链接进行配置。

3.10.2. 日志查看

『日志查看』用于查看设备的运行日志及错误提示。运行日志包括了两种类型，一种为服务日志，可以查看当前设备的系统日志信息。选择要查看的日期，会显示相应时间下的日志记录。页面如下：

点选项设置，可以设置指定查看的系统日志范围。页面如下：

另一种为管理日志，可以查看当前设备管理员对设备进行的操作日志信息。选择要查看的日期，会显示相应时间下的日志记录。

3.10.3. 策略故障排除

『策略故障排除』用于查询一个数据包在通过网关时是被哪个模块拒绝，是什么原因被拒绝，以便快速定位配置错误，也可用来测试一些规则是否生效，如下图：

点击设置开启条件可设置各种条件进行过滤，包括『IP 地址』、『协议类型』和『端口』等，如下图：

『IP 地址』：用于设置对指定的 IP 地址开启拒绝列表，默认包括所有网段。

『协议类型』和『端口』：设置对符合指定协议类型、端口的数据包的拒绝情况才输出到访问控制列表中。

点击开启拒绝列表将打开拒绝列表，此时设备所有的策略依然生效，符合策略设置应该拒绝的数据包会被设备拒绝掉，同时会将符合策略设置应该拒绝数据包的情况输出到一个 WEB 页面里。点点击此处查看，可以打开页面查看数据包被拒绝的情况。

点击开启拒绝列表并直通可以打开拒绝列表同时开启直通。此时设置的访问策略、流控策略、认证选项将不生效，符合策略设置应该拒绝的数据包会被设备放行，同时会将符合策略设置应该拒绝数据包的情况输出到一个 WEB 页面里，通过该功能可以快速定位是哪个模块配置错误而导致网络中断等错误并手动恢复策略配置错误带来的网络故障。点点击此处查看，会自动打开浏览器查看数据包的拒绝情况。

关闭拒绝列表用于关闭拒绝列表输出，并关闭直通。

点点击此处查看，会自动打开浏览器查看数据包的拒绝情况。如下图：

Drop list enable=No,bypass=No

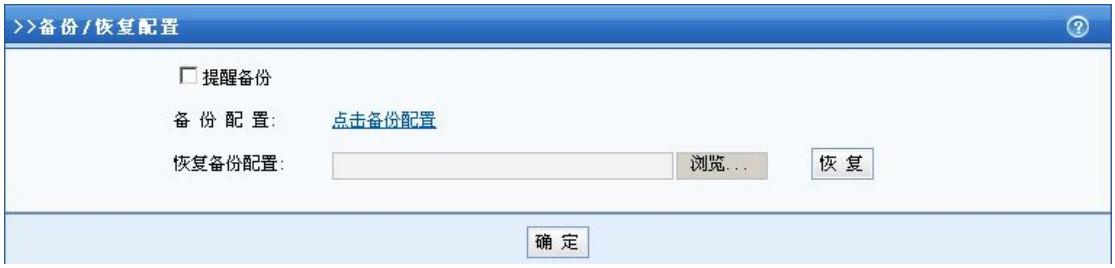
	Time	Source	Action	Proto	IP	Dev	Len	Line	dropflag/appname/apprule
029	16:24:29	fw_drv	this packet has been dropped by AppControl rule:eMule[TCP]!	tcp	20.254.254.26:1050 -> 88.140.123.107:6518	eth0->ppp0	189	0	appcontrol/eMule/eMule[TCP]
028	16:24:28	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	189.48.90.249:42135 -> 20.254.254.26:4173	ppp0->eth0	50	0	appcontrol/eMule/eMule[UDP]
027	16:24:27	fw_drv	this packet has been dropped by AppControl rule:eMule[TCP]!	tcp	20.254.254.26:1052 -> 151.67.30.151:4662	eth0->ppp0	189	0	appcontrol/eMule/eMule[TCP]
026	16:24:26	fw_drv	this packet has been dropped by AppControl rule:eMule[TCP]!	tcp	20.254.254.26:1050 -> 88.140.123.107:6518	eth0->ppp0	189	0	appcontrol/eMule/eMule[TCP]
025	16:24:25	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 58.19.23.79:4600	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
024	16:24:25	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 58.19.23.79:4600	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
023	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 119.182.129.137:18207	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
022	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 119.182.129.137:18207	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
021	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 87.13.89.236:4672	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
020	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 87.13.89.236:4672	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
019	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 125.230.99.190:17368	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]

1.『开启条件』一般来说要详细设定，这样可以有效的过滤无用信息，使排错过程更简单。

2．使用完该功能后切记关闭拒绝列表。因为该功能会消耗一定的系统资源。另外，如果开启直通功能后没有关闭拒绝列表会导致所有限制功能失效。

3.10.4. 备份/恢复配置

用来备份和恢复 SANGFOR MIG 网关设备的配置。页面如下：



『提醒备份』：可以设置间隔多少天内没有备份配置则在登录设备配置界面之后进行提醒。

『备份配置』：点点击备份配置将设备当前配置备份到本地，

『恢复上一次配置』：点点击恢复备份配置将本地备份配置文件恢复到设备上。点点击恢复配置将设备上一个备份时间点自动备份的配置恢复到当前配置。

1．恢复配置时，必须确保配置文件的版本型号必须和当前设备的版本型号一致，否则可能导致异常。

2．为防止不小心改乱配置，建议您定时备份配置。

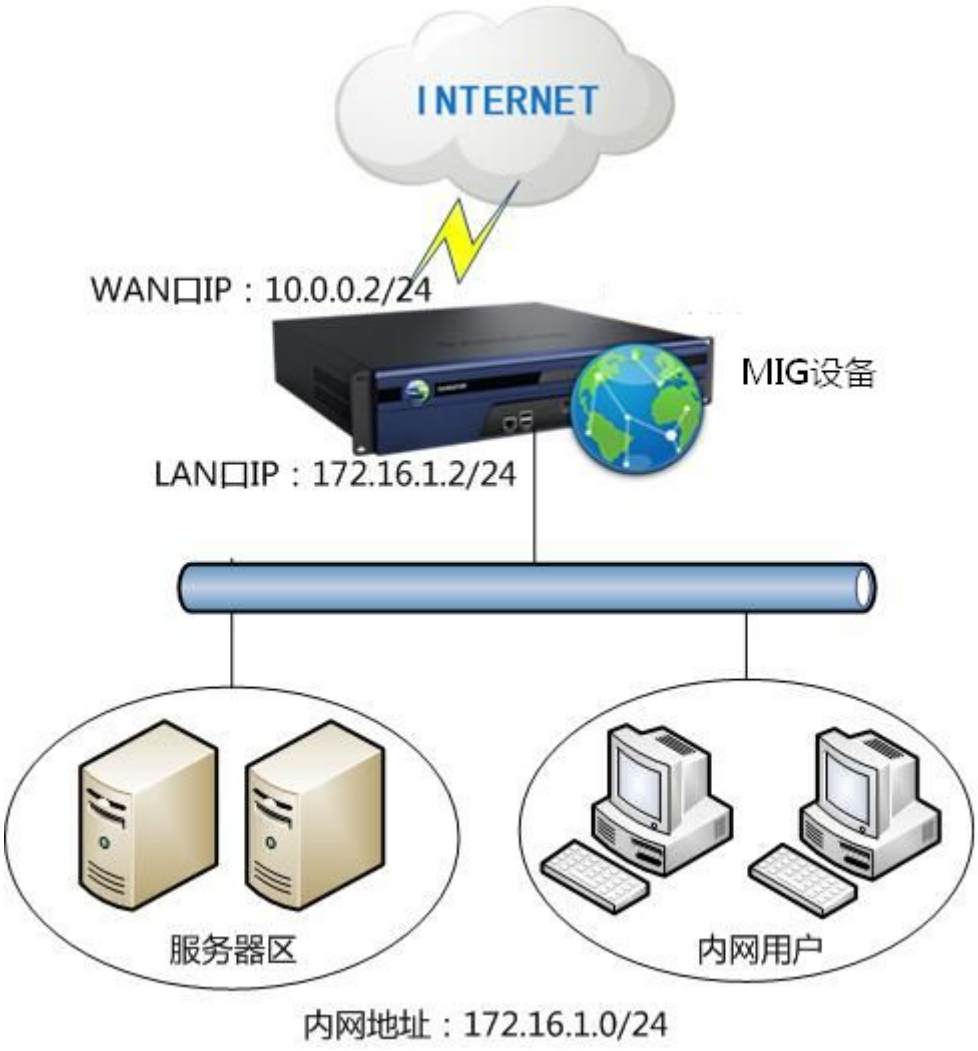
注意：必须是同型号同版本的配置才能实现互导，例如 MIG 1200 的配置不能导入到 MIG1110 设备，DLAN 4.3 版本的配置不能导入到 DLAN 4.6 版本的设备。

MIG4.0 版本开始支持 H323、GRE、PPTP、FTP、TFTP 常用协议穿透。

第 4 章 案例集

4.1. 路由模式部署案例

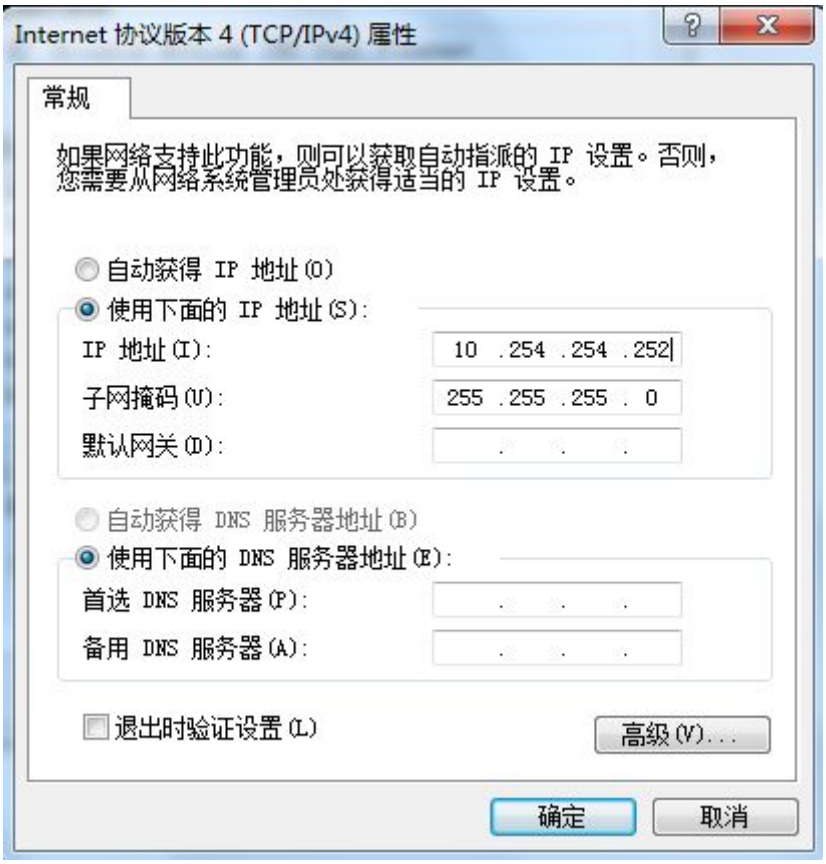
客户环境与需求：某客户网络拓扑如下，有一条运营商链路，原有一个路由器做出口，希望用 MIG 设备网关模式部署在网络出口，代理内网用户和服务器上网，并且最终与其他 MIG 设备建立 VPN 连接。



配置方法：

第一步：首先将设备开机，用网线接设备的 EHT0 口（LAN），将电脑网卡的 IP 配置成

10.254.254.252，界面如下：



第二步：登录设置页面，打开 IE 浏览器，输入 https://10.254.254.253，即可到登录界面，输入设备出厂默认的账号密码 admin/admin，界面如下：

第三步：接口配置，进入『系统设置』→『网络接口配置』，选择设备工作模式为网关模式，设置好 LAN 口和 WAN 口地址，DNS 等信息，点击确定，界面如下：

第四步：代理上网设置，进入『防火墙设置』→『NAT 设置』→『代理上网设置』，新增一条规则，定义规则名称，选择内网接口，并设置好子网网段和子网掩码，点击确定，界面如下：

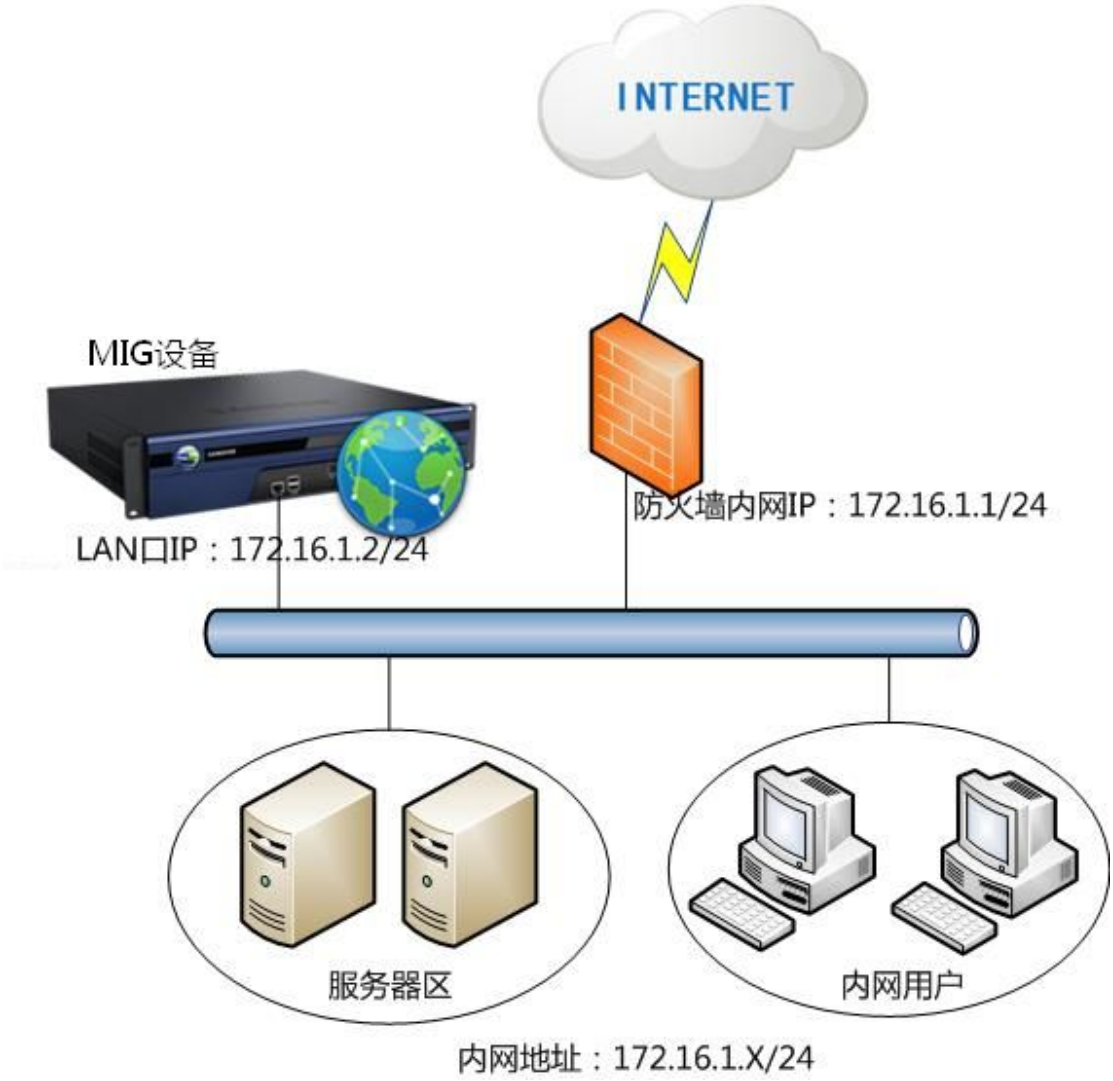
以上步骤配置完毕，则可以将设备 LAN 口接内网交换机，WAN 口接公网链路，将内网电脑网关指向设备 LAN 口，设备即可代理内网上网。

配置外网线路时，线路类型根据实际需求，可以选择以太网或 ADSL。

配置完设备的内网外接口后，本机 IP 需要修改成与配置后的 LAN 口同网段的 IP。

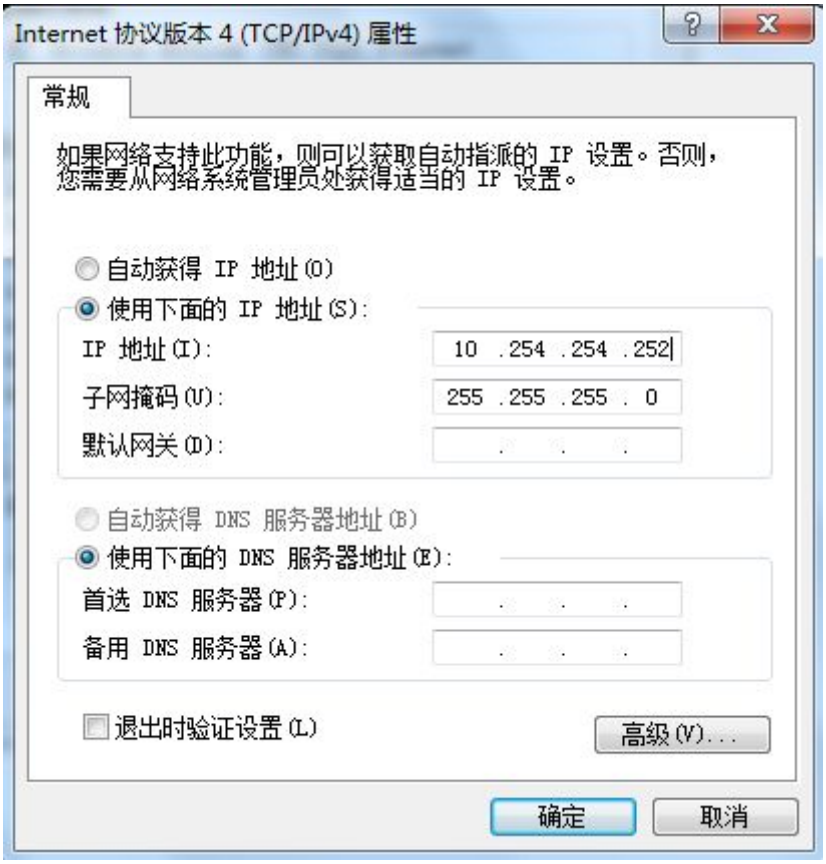
4.2. 单臂模式部署案例

客户环境与需求：某客户拓扑如下，有一条运营商链路，内网用户通过防火墙代理上网。客户希望 MIG 设备单臂模式部署到内网，最终实现与其他设备的 VPN 互联。



配置方法：

第一步：首先将设备开机，用网线接设备的 EHT0 口（LAN），将电脑网卡的 IP 配置成 10.254.254.252，界面如下：



第二步：登录设置页面，打开 IE 浏览器，输入 https://10.254.254.253，即可到登录界面，输入设备出厂默认的账号密码 admin/admin，界面如下：

第三步：选择工作模式并配置接口地址，进入『系统设置』→『网络接口设置』，选择设备工作模式为单臂模式，配置 LAN 口 IP 地址、子网掩码、网关，并配置正确的 DNS，点击确定，界面如下：

第四步，由于 MIG 设备接在内网，若该设备做 VPN 连接时是以总部部署，需要在前置路由器或防火墙上做端口映射，VPN 连接的端口为 TCP/UDP4009. 若做网对网的连接，还需要在前置网关设备上添加路由，到 VPN 对端内网网段，下一跳交给本端的 VPN，各个厂

家设置方法有所不同，此处不截图说明。

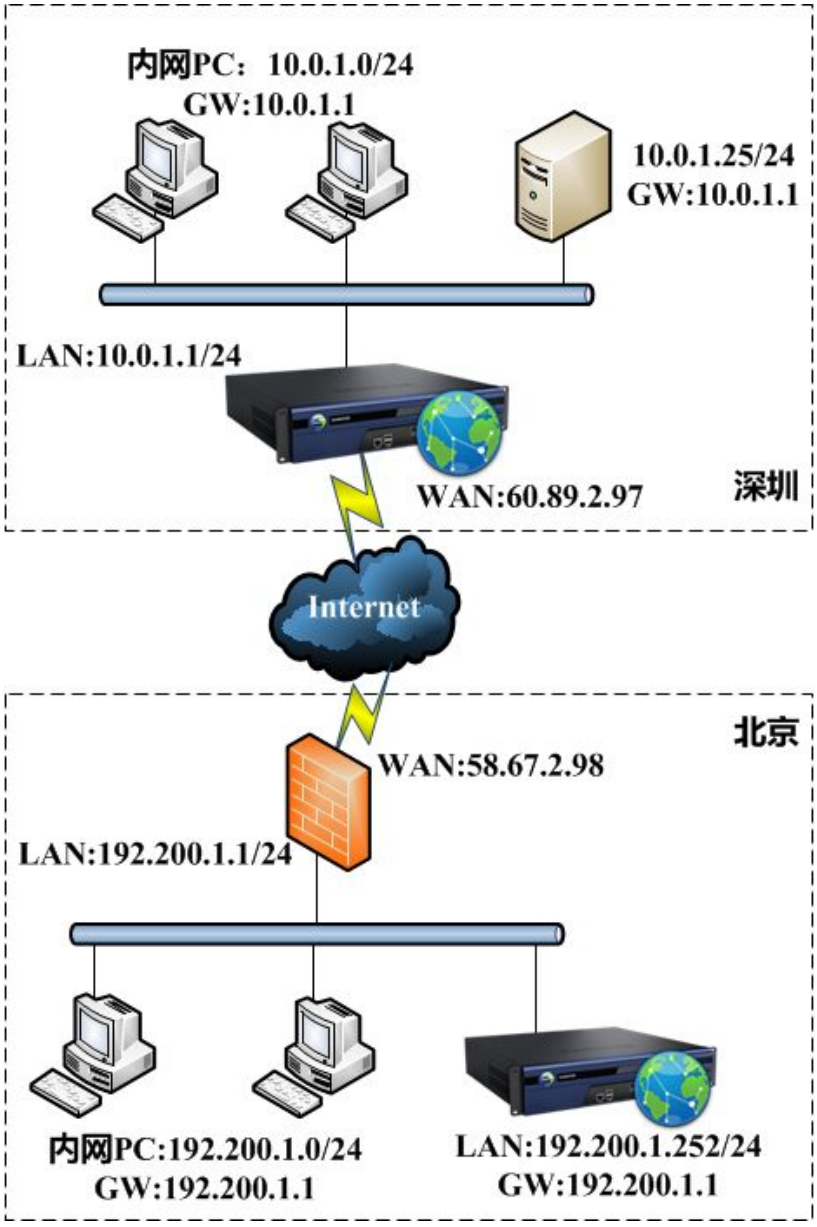
以上步骤配置完毕，则可以将设备 LAN 口接到交换机上，并检查设备与内网通讯是否正常。

TCP/UDP 4009 端口为设备出厂默认的 VPN 监听端口，可以做修改，如做了修改，则端口映射需要映射修改后的监听端口。

单臂模式必须接设备 LAN 口到内网交换机。

4.3. SANGFOR VPN 互连案例

客户网络拓扑如下，深圳和北京分别有一台 MIG 设备，分别以网关模式和单臂模式部署到两个局域中，客户希望 192.200.1.0/24 的 PC 可以访问服务器 10.0.1.25.



配置思路：

1.按照 3.1 与 3.2 章节的方法将设备部署上架

2.要两端内网电脑能通讯，必须先建立 VPN 连接。

3.选择一台 MIG 设备做 VPN 总部，另一台 MIG 设备做 VPN 分支。

4.总部需要配置 WEBAGENT 信息与用户，同时保证 VPN 监听端口可被分支设备访问、内网 PC 数据经过 VPN。分支需要配置连接管理即可。

以下配置以北京的设备做为总部，深圳的设备做为分支进行配置。

总部 VPN 配置步骤

第一步：将深信服 MIG 设备配置成网关模式并且上架，详细请参考 2.1 章节。北京设备接口配置如下：

第二步：配置 WEBAGENT，进入『VPN 信息设置』→『基本设置』，设置好主 WEBAGENT 信息，MTU 和最小压缩值默认即可，监听端口采用默认值，本案例配置界面如下：

第三步：为分支建一个 VPN 账号，进入『VPN 信息设置』→『用户管理』，新增一个 VPN 账号，选择类型为分支，配置界面如下：

第四步：在前置的防火墙映射 58.67.2.98 的 TCP 和 UDP 4009 端口到 MIG 设备，各厂家配置不一样，此处不一一例举。

第五步：由于本端的 MIG 设备单臂模式部署，内网 PC 的网关指向防火墙，为了保证访问 10.0.1.25 的数据经过 MIG 设备，还需要在防火墙上添加静态路由，目标网络为 10.0.1.0/24，下一条地址为 192.200.1.252。

以上步骤结束，总部配置完成。

分支 VPN 配置步骤

第一步：将深信服 MIG 设备配置成网关模式并且上架。深圳设备接口地址设置如下：

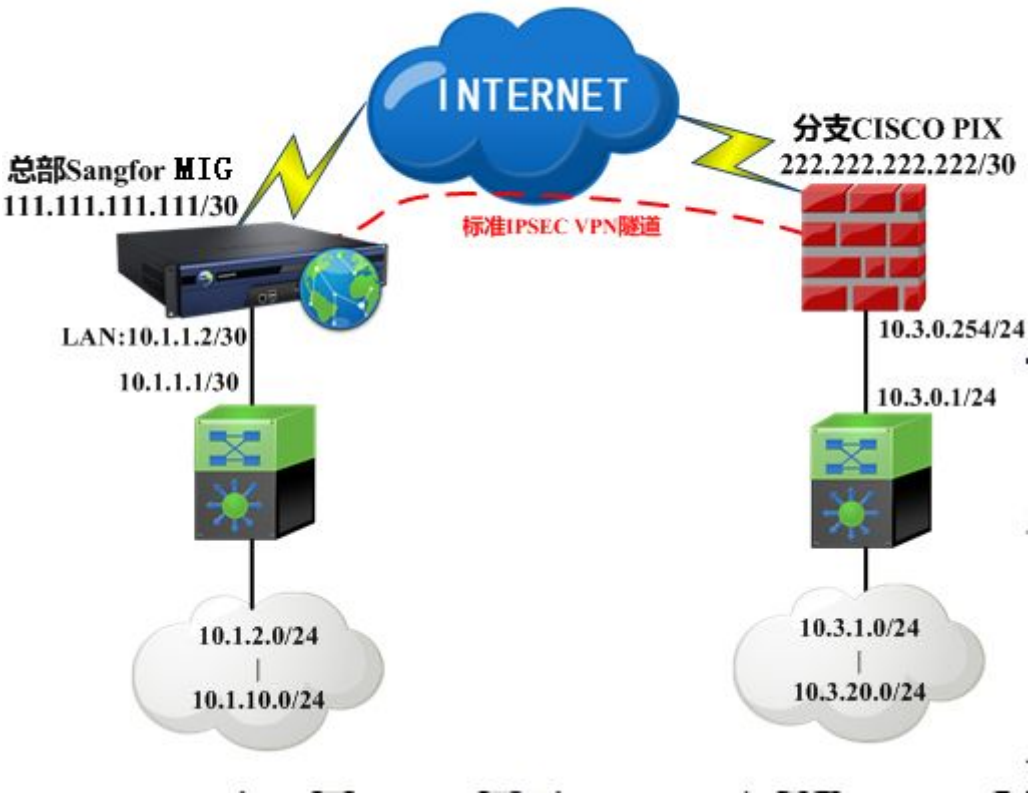
第二步：建立 VPN 连接，进入『VPN 信息设置』→『连接管理』，新建一个连接，填写总部设置的 WEBAGNET，总部建的 VPN 账号，界面如下：

以上配置结束后，完成总部与分支 VPN 连接的所有步骤，若 VPN 连接成功，可以通过 DLAN 运行状态查看连接情况。

两台设备做 VPN 互联时，必须保证至少有一台设备的 VPN 连接端口在公网上能通。

4.4. 与 CISCO PIX 标准 IPSEC VPN 互连案例

某公司拓扑图如下，Cisco Route 和 SANGFOR MIG 设备建立标准 IPSEC 连接，各分支需要访问总部 10.1.10.0/24 服务器网段。总部的网段是 10.1.0.0/16　分支的网段是 10.3.0.0/16。



Cisco VPN 配置：

crypto ipsec transform-set *sangfor* esp-des esp-md5-hmac **crypto map** *mymap 10* **ipsec-isakmp**

crypto map *mymap 10* **match address** *102*

crypto map *mymap 10* **set pfs** group2

crypto map *mymap 10* **set peer** *111.111.111.111*

crypto map *mymap 10* **set transform-set** *sangfor*

crypto map *mymap* **interface** outside

isakmp enable outside

isakmp key *test123* **address** *222.222.222.222* **netmask** *255.255.255.252*

isakmp identity address

isakmp policy *10* **authentication** pre-share

isakmp policy *10* **encryption** des

isakmp policy *10* **hash** md5

isakmp policy *10* **group** 2

isakmp policy *10* **lifetime** 28800

access-list *102* **permit ip** *10.3.0.0 255.255.0.0 10.1.0.0 255.255.0.0*

access-list *nonat* **permit ip** *10.3.0.0 255.255.0.0 10.1.0.0 255.255.0.0* **global (outside)** 1 *222.222.222.222*

nat (inside) *0* **access-list** *nonat*

nat (inside) 1 *10.3.0.0 255.255.0.0 0 0*

SANGFOR MIG 设备的 VPN 配置：

第一步：配置第一阶段，如下图：

『名称』自定义第一阶段策略名称为 cisco。

『地址类型』选择为固定 IP。

『固定 IP』配置为 222.222.222.222。

『预共享密钥』设置协商双方的共享密钥。

勾选[启用]和[自动连接]选项，则此策略设置完成后立即生效。

点击高级，设置如下参数，界面如下：

『ISAKMP 存活时间』用来设置第一阶段策略的生存期为 28800。

『重试次数』用来设置第一阶段协商时的重试次数为 10 次。

『模式』选择第一阶段协商所使用的模式为主模式。

『D-H 群』用来设置协商双方的 Differ-Hellman 群为 GROUP 2。

『ISAKMP 加密算法』选择第一阶段的加密算法为 DES。

『ISAKMP 认证算法』选择第一阶段的认证算法为 MD5。

依此点击确定，保存配置。

第二步：配置第二阶段安全选项，『VPN 信息设置』->『第三方对接』->『安全选项』，

如下图：

『名称』定义为 cisco。

『协议』选择协议为 ESP 协议。

『认证算法』选择认证算法为 MD5。

『加密算法』选择加密算法为 DES。

依此点击确定保存配置。

第三步：配置第二阶段出站策略及入站策略，『VPN 信息设置』->『第三方对接』->『第二阶段』：

入站策略配置界面如下：

『名称』自定义入站名称为 cisco。

『服务』选择允许所有的入站服务。

『源 IP 类型』设置 VPN 对端允许访问本端的 IP 地址或 IP 地址段为子网，子网网段为 10.3.0.0，子网掩码为 255.255.0.0。

出站策略配置如下图：

『名称』自定义出站名称为 cisco。

『服务』选择允许的所有服务出站。

『源 IP 类型』设置本端允许访问 VPN 对端的 IP 地址或 IP 地址段为子网，子网网段为 10.1.0.0，子网掩码为 255.255.0.0。

『对端设备』选择对端设备为 cisco，该设备在第一阶段中已经过定义为 cisco。

『安全选项』选择双方协商时的安全策略为 cisco。

『SA 保活时间』定义策略生存期时间为 28800。

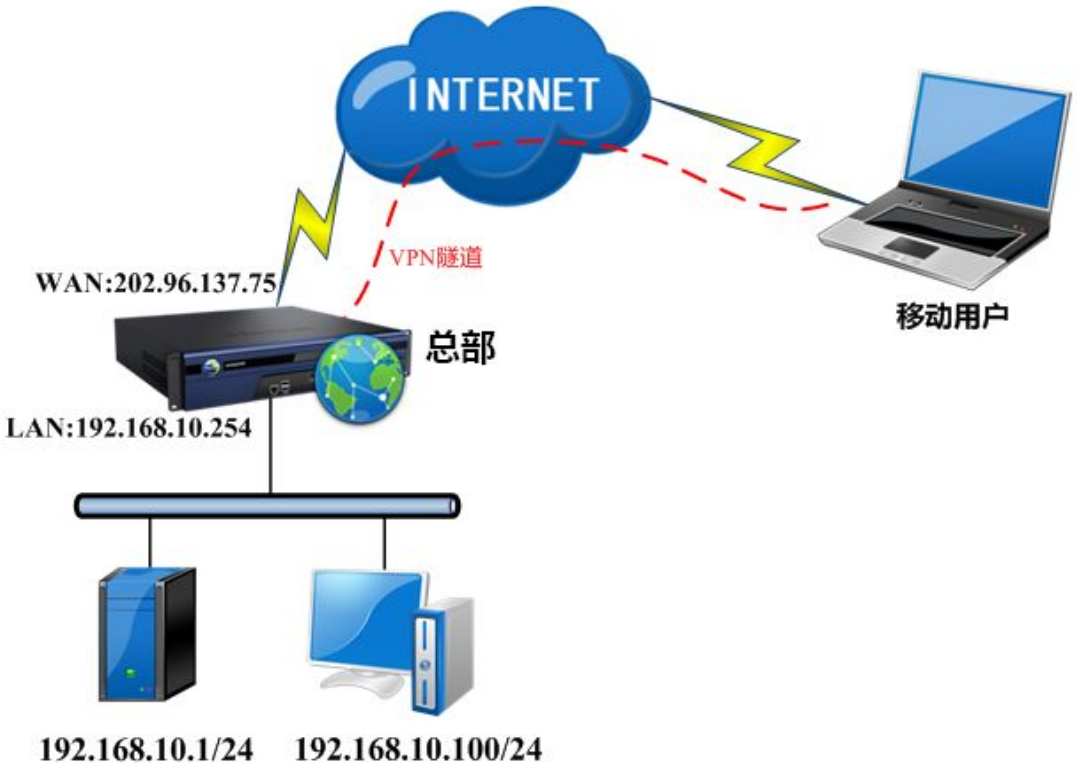
勾选[启用该策略]启用该策略，因为 cisco 设备设置了 PFS，则同时勾上[启用密钥完美向前保密]。点击确定后保存并启用规则。

以上步骤配置完成，即可完成标准 IPSEC VPN 对接。

在配置第三方对接前，请确认开通了第三方对接授权，『系统设置』->『序列号设置』，如查看到“第三方对接授权数”为 0，则表示没有授权，授权数表示可以建立标准 IPSEC VPN 的隧道数。界面如下：

4.5. 移动 PDLAN 用户接入 VPN 案例

用户总部 MIG 1200 设备采用路由模式部署，外地移动办公用户需要通过 PDLAN 接入到总部远程办公，访问到 OA 服务器。如下图：



配置步骤如下：

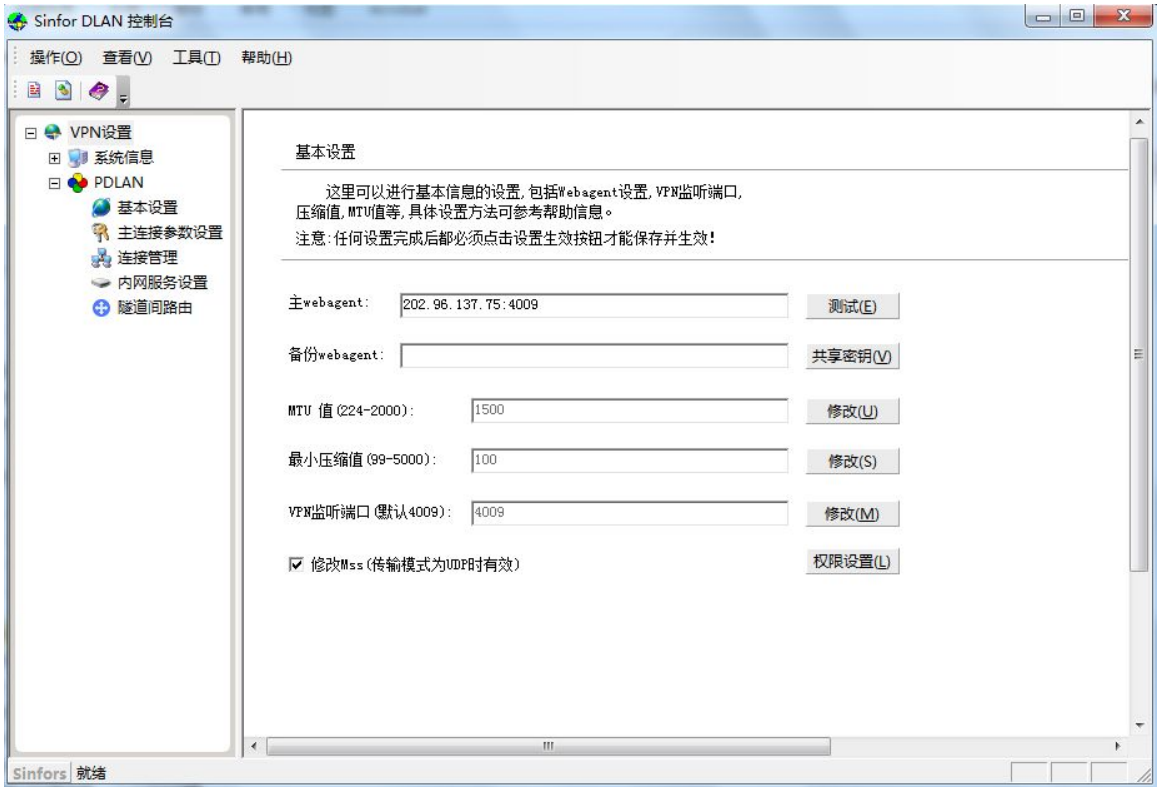
第一步：配置 MIG 设备接口 IP 地址、代理上网信息。详细请参考 3.1 章节。

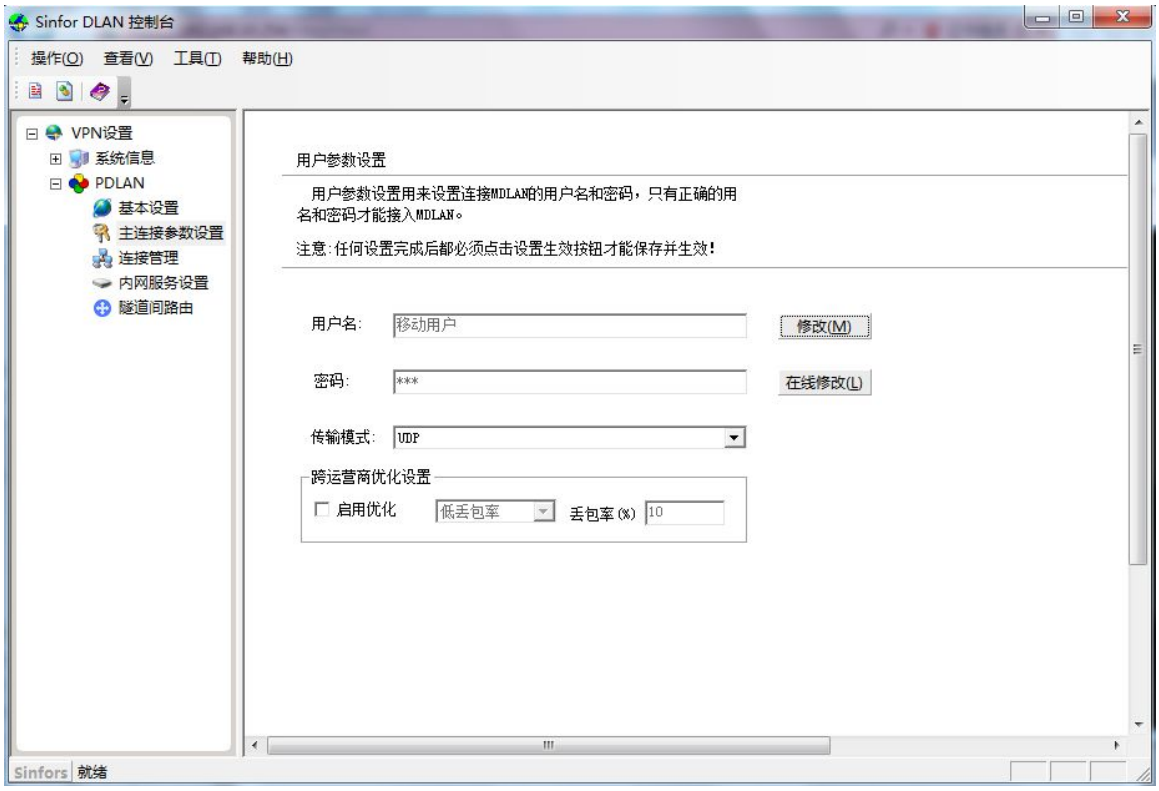
第二步：配置『基本信息设置』，本案例配置界面如下：

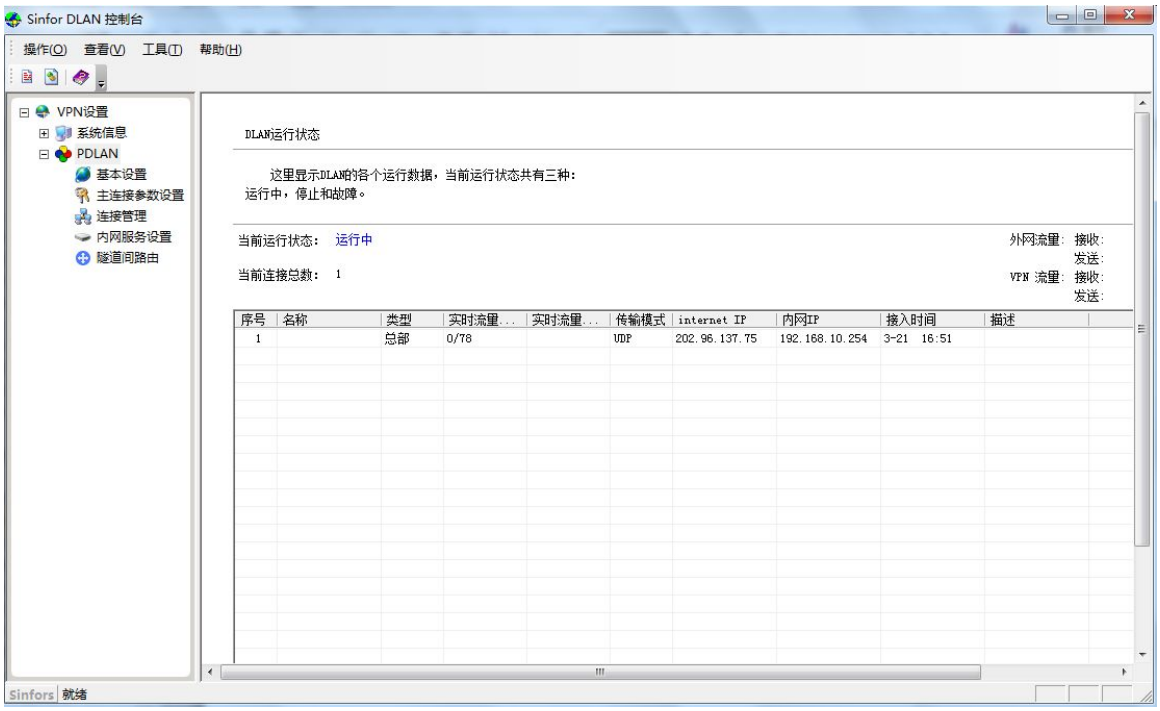
第三步：在『虚拟 IP 池』中新增一条规则，设置和设备 LAN 口相同网段且没有被内网用户所使用的 IP 地址段。如下图：

第四步：在『用户管理』中新增用户，类型选择[移动]。虚拟 IP 默认为“0.0.0.0”则表示自动分配虚拟 IP，如需指定用户的虚拟 IP，则设置相应的虚拟 IP 即可。

第五步：在移动用户的客户端上安装 PDLAN（安装方法略），并且配置好 WEBAGENT 和用户名密码，即可连接上 MIG 设备，界面如下：

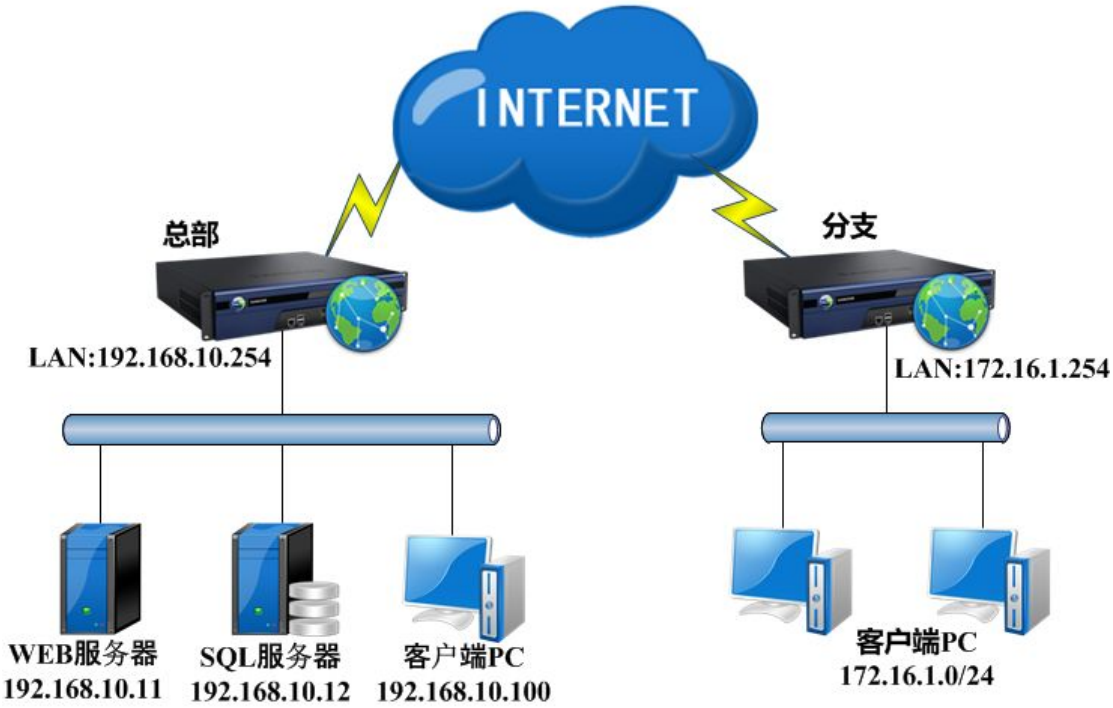






4.6. VPN 内网权限的设置案例

某总部和分支部署了两台 MIG 设备，现总部的 MIG 设备做为 VPN 总部与分支建立了 VPN 连接，用户要求对分支访问总部的服务器进行权限控制，只允许分支网络的 PC 访问总部的 WEB 服务器（80 端口），禁止访问其他的任何服务器（包括 PC 客户端）。如下图：

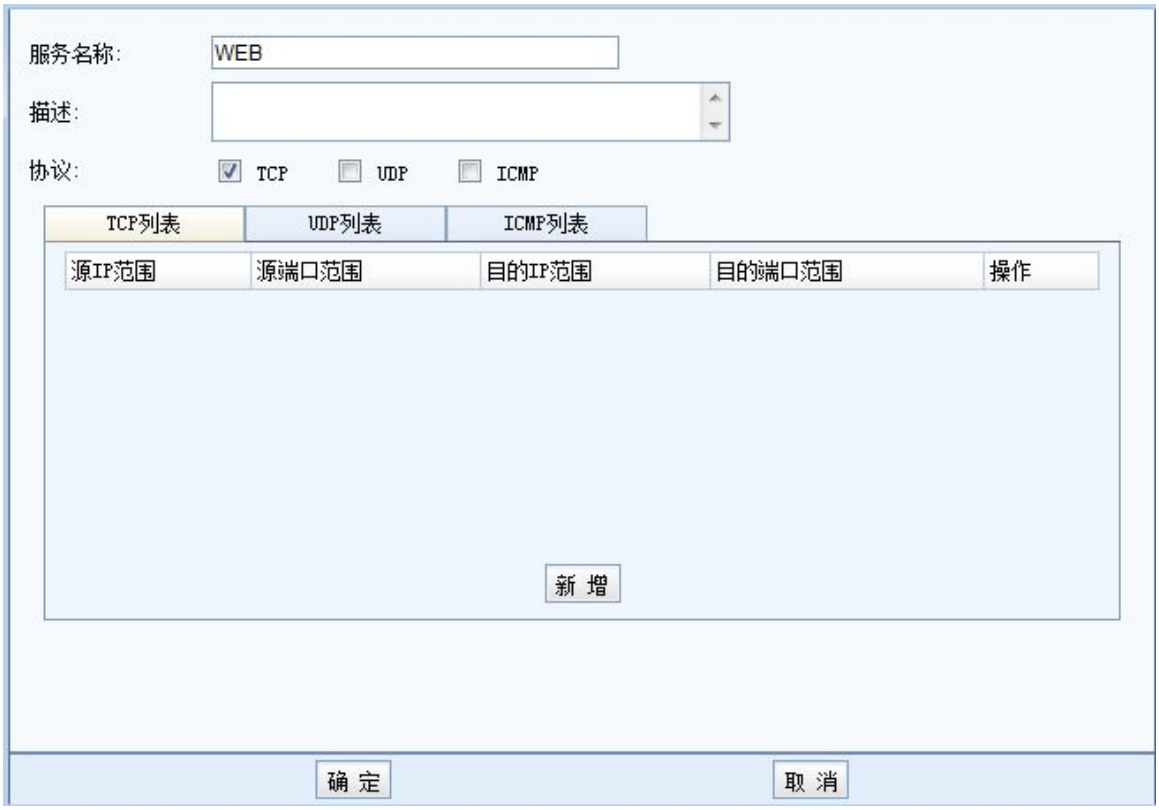


该客户需求一共有两种方法可以实现，通过 VPN 内网权限与通过防火墙过滤规则，下面分别介绍两种情况下如何配置：

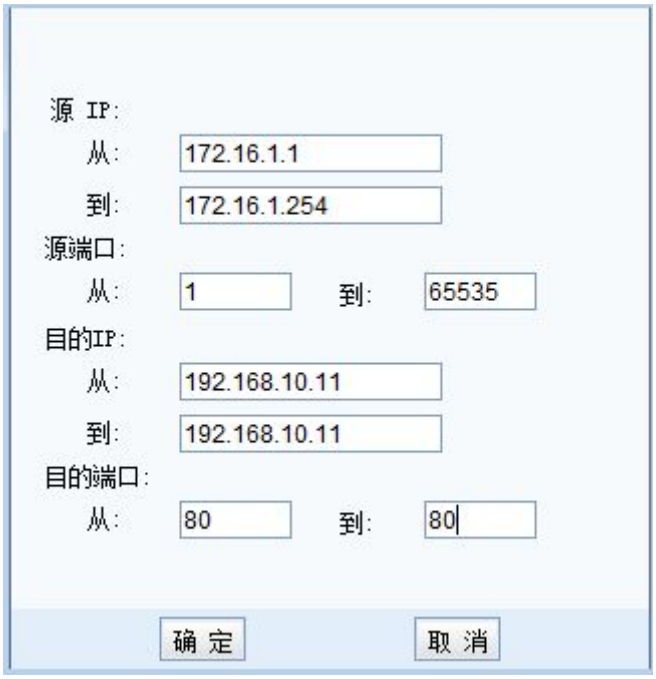
配置方法一：通过 VPN 内网权限实现。

第一步：在总部 MIG 设备的『VPN 信息设置』->『高级设置->『内网服务设置』页面，新增一个 WEB 的内网服务，如下图：

点新增，设置服务名称，选择 TCP 协议，如下图：



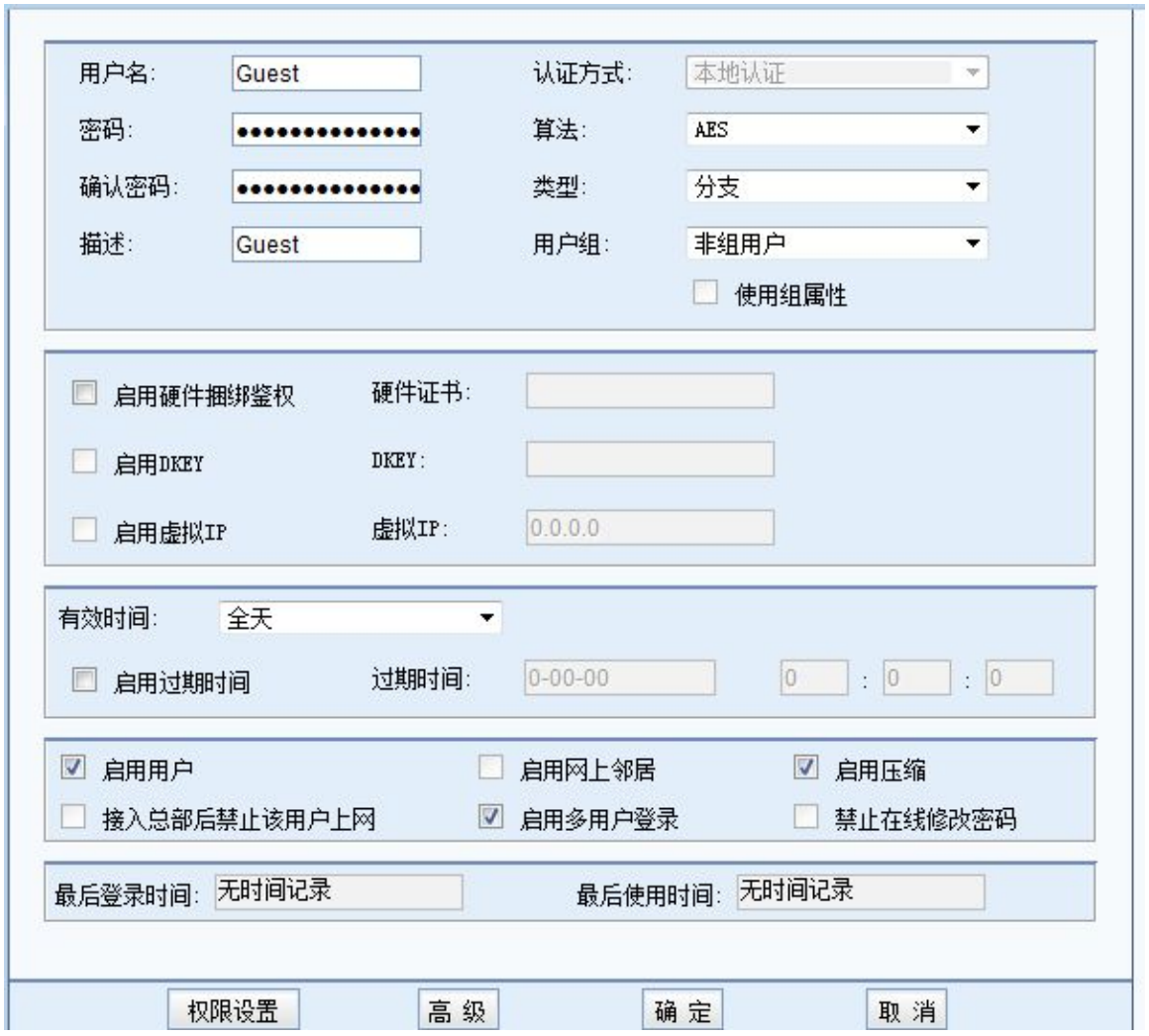
再点新增，设置 IP 及端口范围，如下图：



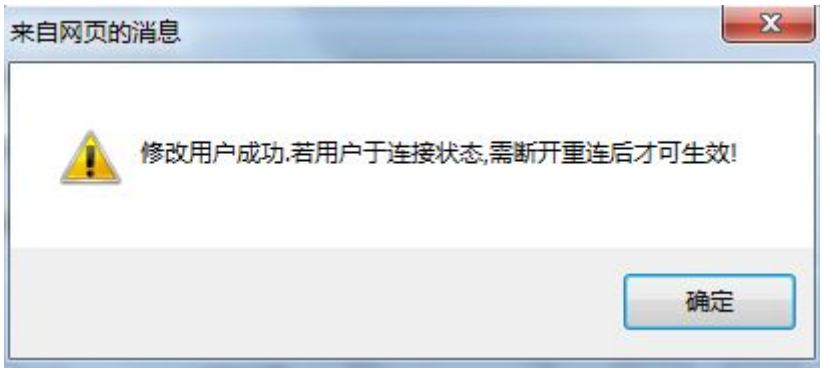
本案例中，源 IP 为分支的内网网段，源端口必须选择 1-65535，因为发起连接的端口均为随机端口。目标 IP 可为总部的内网 WEB 服务器 IP，目的端口为 WEB 端口 80。

点确定，完成配置。最后点击控制台的确定按钮保存配置。

第二步：在总部设备的『VPN 信息设置』->『用户管理』页面编辑分支用户，点击权限设置，如下图：



点击确定，再点击对话框[编辑用户-分支]中的确定，出现如下提示：



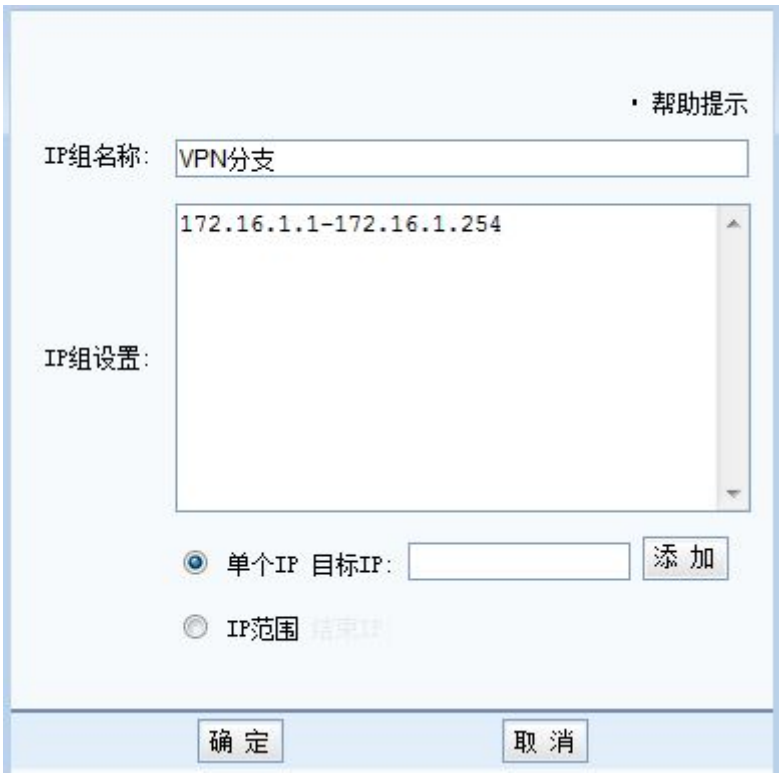
以上步骤完成，VPN 隧道需要重新建立连接即可生效。

注意：一旦设置了 VPN 内网权限，不光 VPN 对端访问本端受到限制，本端访问 VPN 对端一样会受到内网权限的控制。因为内网权限只检查数据包的 IP 和端口，不管这个数据包是 VPN 对端主动发起的还是本端主动发起 VPN 对端响应的，只要符合规则条件的数据包都会做相同的处理。通过防火墙过滤规则可做到更细化的控制。

配置方法二：通过防火墙过滤规则实现。

第一步：在总部的 MIG 设备『防火墙设置』->『IP 组定义』定义好分支网段的 IP 组，

与总部 WEB 服务器的 IP 组，界面如下：

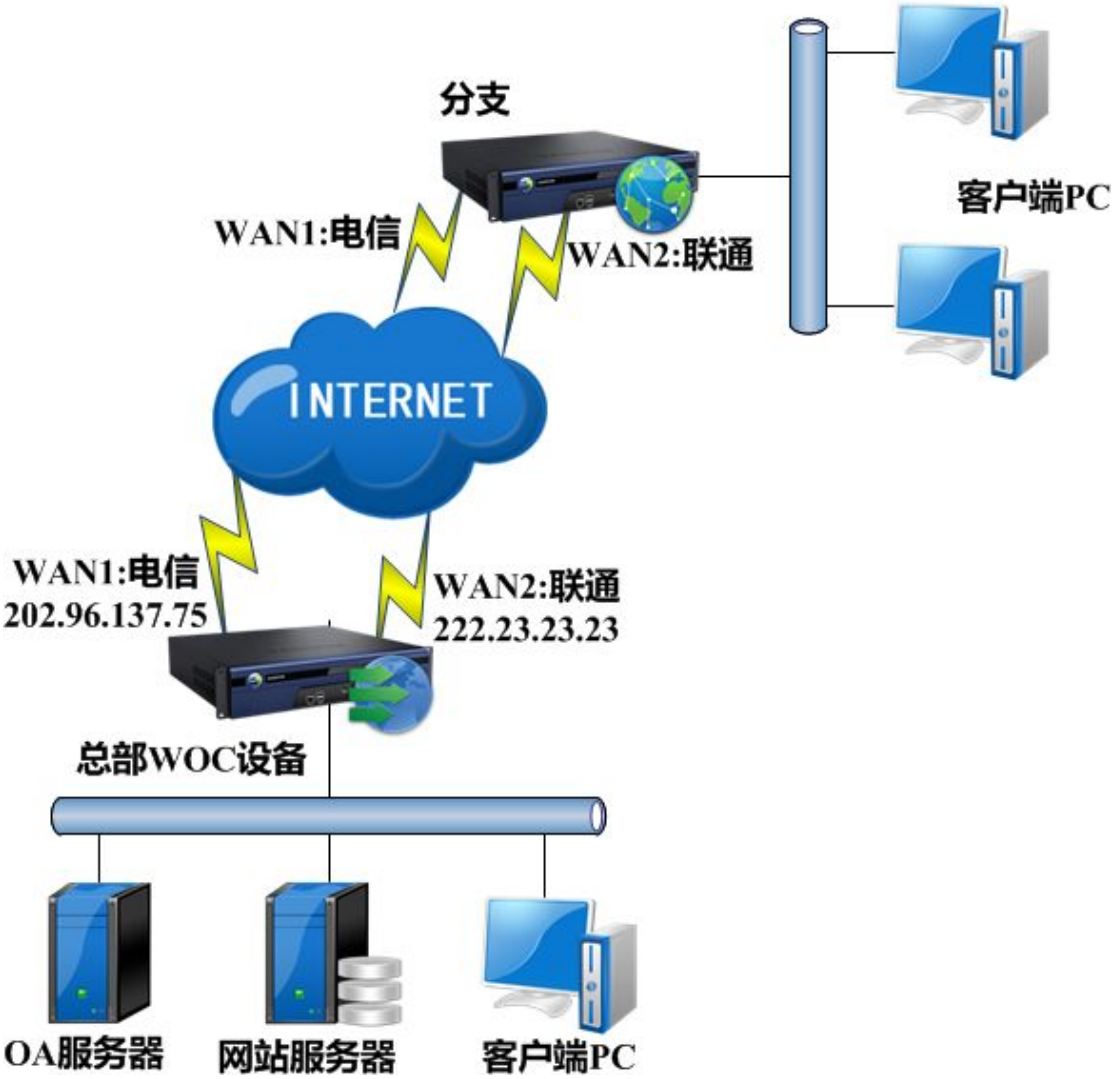


最后点击**确定**，保存配置。

第二步：在总部 MIG 设备的『防火墙设置』->『过滤规则设置』->『VPN<->LAN』，删除 VPN->LAN 的三条规则（因为 VPN->LAN 默认是放通所有数据的），然后添加一条规则，界面如下：

4.7. VPN 多线路配置案例

某用户总部是双线路，部署了一台 SANGFOR WOC 设备。分支为 MIG 1200，也是双线路。用户需要实现线路备份，分支端任意一条线路出问题，则走另外一条线路。两条线路都正常情况下自动选择最快线路传输 VPN 数据。



配置步骤如下：

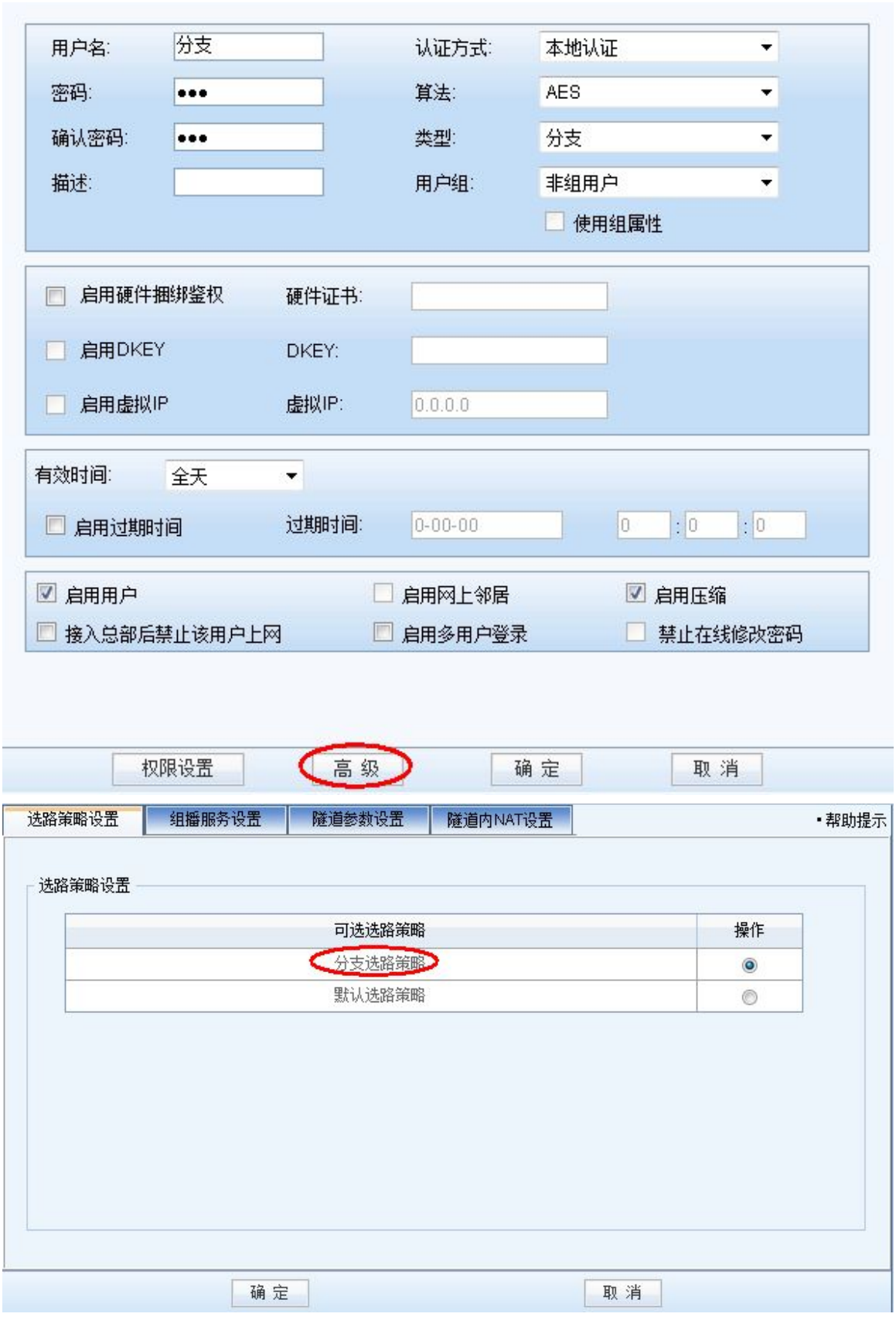
总部 WOC 设备的配置方法

第一步：在总部 WOC 设备上配置好 IP 地址、代理上网、WEBAGENT 等信息。

第二步：在总部 WOC 设备[系统]-[部署设置]-[多线路设置]配置好[多线路设置]，界面如下：

第三步：在总部 WOC 设备[Sangfor VPN]-[多线路]设置好多线路选路策略，本案例中设置界面如下：

第四步：在[Sangfor VPN]-[服务端]-[用户管理]里新建分支连接总部的账户，点击高级将选路策略下发给该用户，界面如下：


用户名:
分支
认证方式:
本地认证
密码:
算法:
AES
确认密码:
类型:
分支
描述:
用户组:
非组用户
使用组属性
启用硬件捆绑鉴权
硬件证书:
启用DKEY
DKEY:
启用虚拟IP
虚拟IP:
0.0.0.0
有效时间:
全天
启用过期时间
过期时间:
0-00-00
启用用户
启用网上邻居
启用压缩
接入总部后禁止该用户上网
启用多用户登录
禁止在线修改密码
权限设置
高 级
确 定
取 消
选路策略设置
组播服务设置
隧道参数设置
隧道内NAT设置
帮助提示
选路策略设置
可选选路策略
操作
分支选路策略
默认选路策略
确 定
取 消

依此点击确定保存配置。

分支 MIG 1200 配置的配置方法：

第一步：配置接口 IP 地址等基础网络配置信息。

第二步：『系统设置』->『多线路设置』处配置好多线路信息。界面如下：

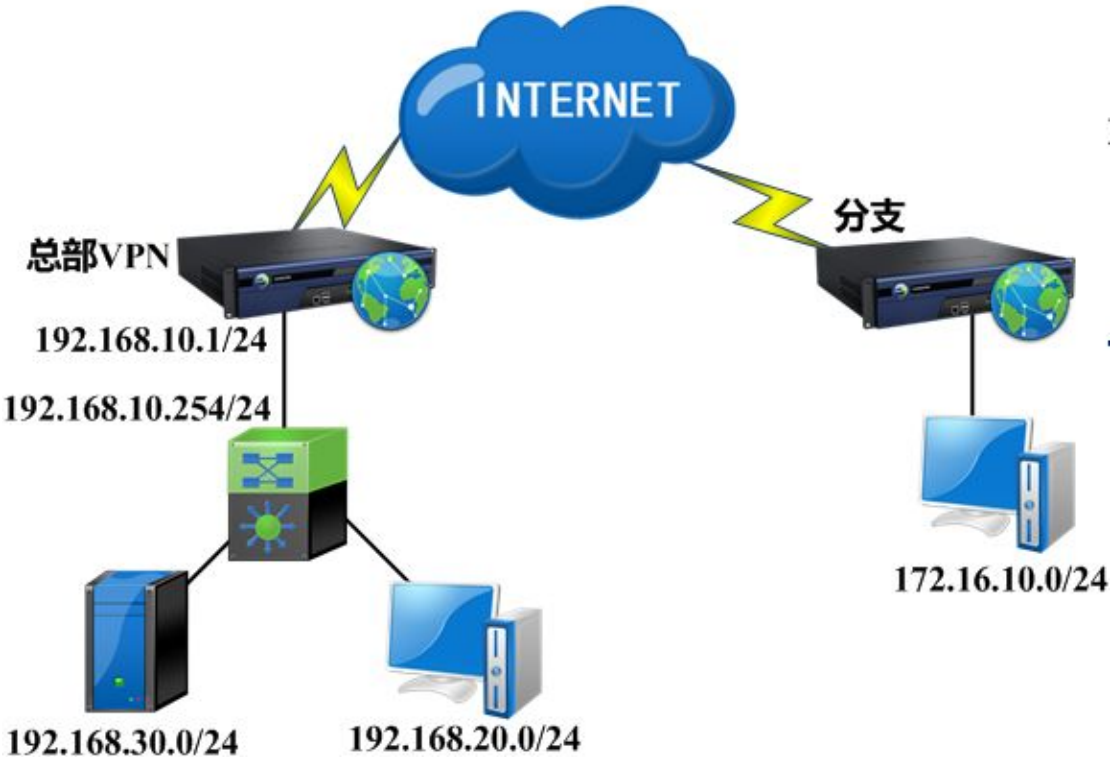
第三步：『VPN 信息设置』->『连接管理』里新建连接管理，配置好 WEBAGENT 信息和账号密码信息。本案例中 WEBAGENT 配置为 202.96.137.75#222.23.23.23:4009，界面如下：

以上步骤配置完成，即可实现多线路自动选路功能。

1.MIG 1200 无法配置多线路选路策略。MIG 1200 的多线路一般情况下用于分支双线路冗余备份的场景。

4.8. VPN 多子网配置案例

总部有三个子网（192.168.10.0/24、192.168.20.0/24 和 192.168.30.0/24），分支通过 VPN 接入总部后，需要访问总部内网的的三个子网。拓扑图如下：



通过配置『本地子网』，添加 192.168.20.0/24 和 192.168.30.0/24 网段以及对应的静态路由才能实现这个需求。

具体配置如下：（略过 VPN 配置步骤）

第一步：在总部 MIG 设备的『本地子列表』里分别添加 192.168.20.0/24 和 192.168.30.0/24 两个子网段，如下图：

第二步：在『系统设置』->『路由设置』->『系统路由设置』中为这两个 VPN 本地子网设置静态路由。如下图：

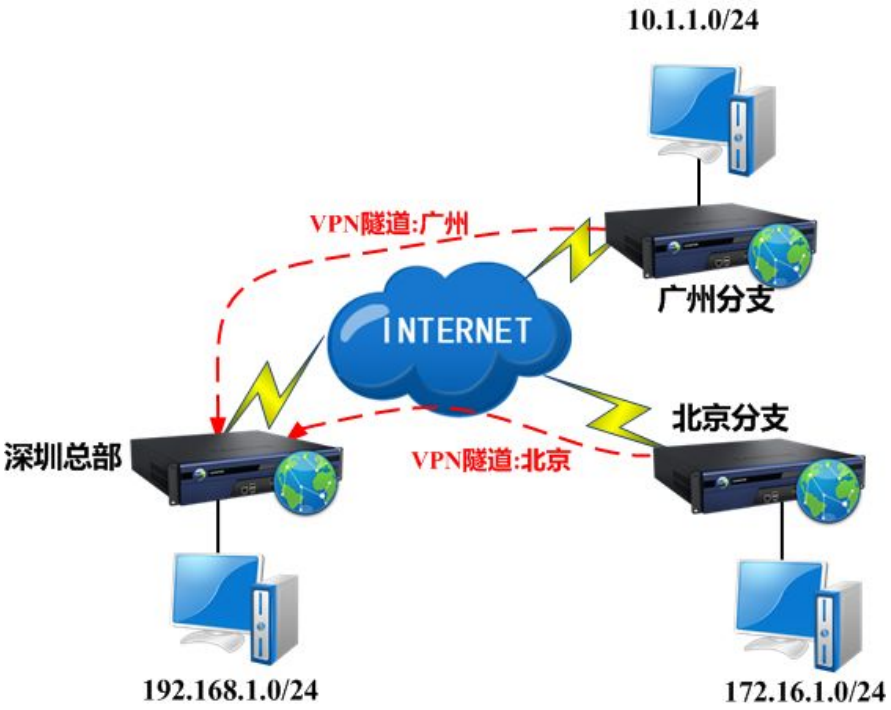
配置完成后，分支接入总部之后，就可以正常访问总部的所有三个网段。

1.这里的[本地子网]仅相当于一种“声明”作用，在此定义的网段，都会被我们的 MIG 设备和软件客户端视为 VPN 网段，所有访问这些网段的数据包经过 MIG 设备或软件后，都会被封装到 VPN 隧道传输中。所以，一般情况下，在『本地子网』里添加了子网网段，需要配合『静态路由』来完成对多子网的访问。

2.如果在设备上架的时候就配置过静态路由，则此处不需要重复配置。保证设备系统路由里有达到内网网段的路由即可。

4.9. 通过隧道间路由实现分支间互访案例

总部（“深圳”192.168.1.0/24）同时与分支（“北京”172.16.1.0/24）、（“广州”10.1.1.0/24）建立了 VPN 连接（分支“北京”、“广州”通过设置连接管理实现与总部互联），但“北京”与“广州”之间没有 VPN 连接，通过设置适当的隧道间路由规则，即可实现“北京”与“广州”之间的相互访问。拓扑图如下：



配置步骤如下：

第一步：首先配置两个分支与总部的 VPN 互联（配置过程略）。

第二步：在北京分支的『隧道间路由』中勾选[启用路由]，点击新增，添加到“广州”的路由，配置如下图：

[网络号（源）]：设置源地址网络号，本例中应设置为 172.16.1.0。

[子网掩码（源）]：设置源地址子网掩码，本例中应设置为 255.255.255.0。

[网络号（目的）]：设置目的地址网络号，本例中应设置为 10.1.1.0。

[子网掩码（目的）]：设置目的地址子网掩码，本例中应设置为 255.255.255.0。

[目的路由用户]：设置路由指向的 VPN 连接用户，本例中应设置为“北京”。

注意：『网络号（源）』、『网络号（目的）』用于匹配数据的源 IP 地址、目的 IP 地址，当 VPN 隧道中传输的数据匹配设置时，则此路由设置生效，数据将被转发给相应的 MIG 设备。『目的路由用户』可理解为，“要将路由的数据发往哪一个 MIG 设备”，本例中北京分支在『连接管理』中设置了使用用户名『北京』与总部建立了 VPN 连接，因此以用户名『北京』标志将隧道间路由的数据发往深圳总部。

注意：用于添加隧道间路由的用户必须是不允许多用户登录的用户。

第三步：在分支“广州”的『隧道间路由设置』中勾选[启用]，点击新增，添加到“北京”的路由，配置如下图：

[网络号（源）]：设置源地址网络号，本例中应设置为 10.1.1.0。

[子网掩码（源）]：设置源地址子网掩码，本例中应设置为 255.255.255.0。

[网络号（目的）]：设置目的地址网络号，本例中应设置为 172.16.1.0。

[子网掩码（目的）]：设置目的地址子网掩码，本例中应设置为 255.255.255.0。

[目的路由用户]：设置路由指向的 VPN 连接用户，本例中应设置为“广州”。

隧道间路由不需要在总部设置，仅需在两个分支端配置好即可实现两个分支间的互访。

4.10. 通过目的路由用户上网案例

Sangfor MIG 设备内的隧道间路由还可用于设置将分支的上网数据全部发往总部，通过总部的公网出口上网，例如，在分支“深圳”设置通过总部“上海”上网，拓扑图如下：

配置步骤如下：

VPN 隧道配置步骤略，在 VPN 隧道已经建立的基础上做如下配置：

第一步：在“深圳”设备上添加隧道间路由，『VPN 信息设置』->『隧道间路由』，点新增，填入本端内网网段，并勾选[通过目的路由用户上网]选项，如下图：

[网络号（源）]：设置源地址网络号，设置本端需要通过总部上网的网络号，如 172.16.1.0。

[子网掩码（源）]：设置源地址子网掩码，本例中应设置为 255.255.255.0。

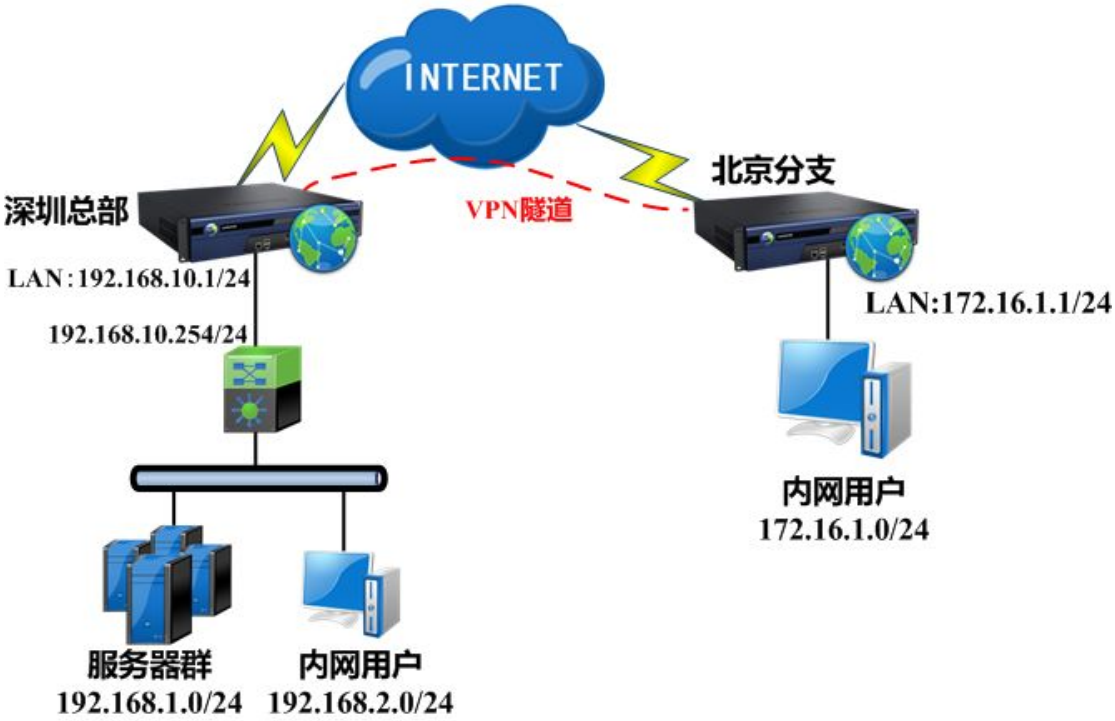
[目的路由用户]：设置路由指向的 VPN 连接用户，本例中应设置为“深圳”。

最后勾选[通过目的路由用户上网]，启用设置。勾选后目的 IP 和掩码均变为 0.0.0.0

第二步：在“上海”设备上添加代理上网规则，『防火墙』->『NAT』->『代理上网设置』对分支“深圳”发过来的数据进行代理上网，如下图：

4.11. VPN 隧道 LAN 口 SNAT 案例

某用户网络结构如下，深圳总部与北京分支分别部署了一台 MIG 设备，已经建立了 VPN 隧道。由于服务器限制了源 IP 地址的访问，只允许总部 192.168.0.0/16 网段访问，其余网段均访问不到服务器。因此北京分支的用户通过 VPN 访问不到服务器，用户希望北京分支的用户访问总部服务器的数据包源 IP 地址全部转换成 192.168.10.1 来解决该问题。



配置步骤如下：

第一步：VPN 互连配置，该拓扑中总部需要配置 WEBAGENT、用户管理、本地子网，系统路由。分支配置连接管理。详细请参考 3.3 章节，不再赘述。

第二步：VPN 隧道连通之后，在深圳总部的 MIG 设备上设置 VPN 隧道的代理上网规则，『防火墙』->『NAT』->『代理上网设置』，新增一条规则。

[源地址/源接口]：由于数据是从 VPN 对端发送过来的，所以选择源接口为 VPN

[源地址/子网网段/子网掩码]：VPN 对端的内网网段是 172.16.1.0/24，所以此处填写该网段。

[目的地址/目的接口]：VPN 对端访问服务器的数据在 MIG 设备 LAN 口方向，数据需要从 LAN 口转发，因此出接口选择 LAN 口。

[目的地址/子网网段/子网掩码]：填写服务器段的 IP 地址。

[源 IP 转换为]：客户需求需要转换成 192.168.10.1，也即 MIG 设备 LAN 口地址。

依此点击确定，保存配置。

以上规则配置生效后分支访问总部服务器网段 192.168.1.0/24 的时候会转换成 LAN 口

IP 地址 192.168.10.1，也即服务器看到的数据包源 IP 地址为 192.168.10.1。但是分支端访问总部内网用户 192.168.2.0/24 的时候仍然是以原来的 IP 地址 172.16.1.0/24，因为以上规则目的地址转换条件填写的网段没有包含内网用户。

附录 通过 RESET 键恢复默认配置

MIG 设备通电状态下，按住 RESET 键不放，2 秒钟以后 ALARM 红灯会开始闪烁，此时松开 RESET 键，之后 ALARM 红色告警灯会常亮，等 ALARM 灯熄灭后即恢复默认配置成功，此时可通过设备 LAN/DMZ 口使用默认出厂 IP 地址登录设备，登录用户名密码也恢复到默认值。