WayOS 防火墙产品
用户手册

尊敬的客户您好！

承蒙惠顾 WayOS 产品，谨致谢意！

目录

设备的安装：

设备接口说明：

LAN 口：用来连接局域网的交换机或者 PC 电脑的网卡。

WAN 口：用以 ADSL、光纤或者以太网的接入。

Reset：复位按钮，用来将设备参数恢复到出厂预设值。

指示灯说明：

Power：电源指示灯。灯亮表示设备通电正常。

System：系统指示灯。系统正常运行时此灯会亮。

WAN：WAN 口工作指示灯。灯亮表示该 WAN 口线路已连通。

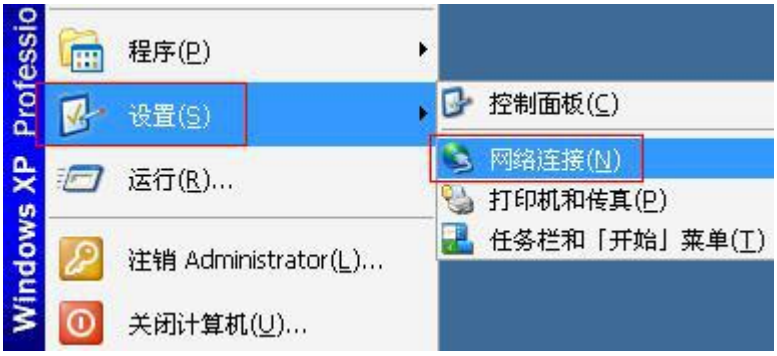
LAN：LAN 口工作指示灯。灯亮表示 LAN 口线路接通。

基本上网设置

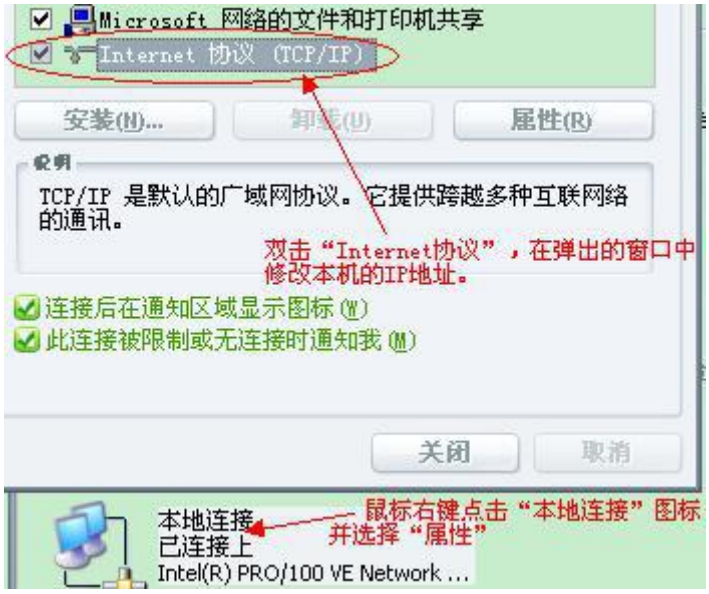
主要介绍在防火墙路由器连接好以后，通过登陆路由的 Web 管理页面，进行路由器的基本信息配置，达到快速上网的目的。

首先需要将您的电脑与路由器的 LAN 口用网线连接起来，并将本机的 IP 地址设置为 192.168.1.X 段。我们以 192.168.1.2 为例来介绍其设置方法：

鼠标右键点击桌面“网上邻居”图标，选择属性，打开‘网络连接’菜单，如图 1 所示，（或者点击“开始-设置-网络连接”也可以打开，如图 2 所示）。



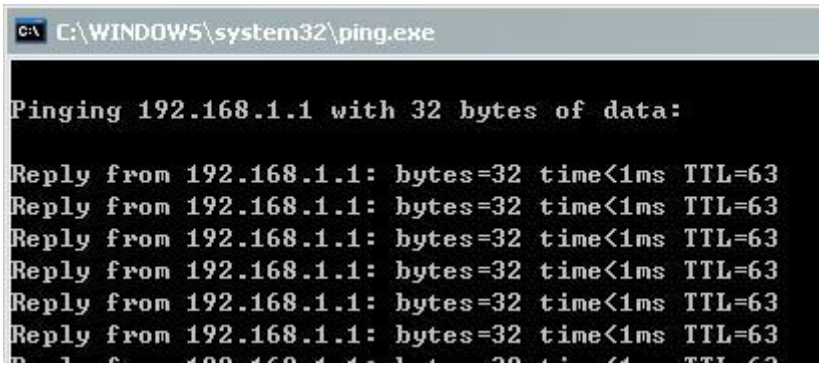
在打开的窗口中找到“本地连接”图标，鼠标右键点击此图标，并选择‘属性’选项，然后在接下来的窗口中选择“Internet 协议(TCP/IP)”并双击（如图 3 所示），进入 IP 地址修改窗口。

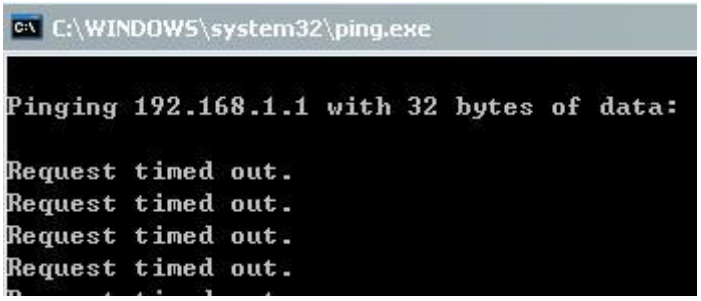


将本机 IP 地址修改为 192.168.1.2，子网掩码为 255.255.255.0，网关为 192.168.1.1，DNS 服务器地址填上网络供应商提供给您的 DNS 地址，若不清楚，可以直接填网关 IP，如图 4 所示：

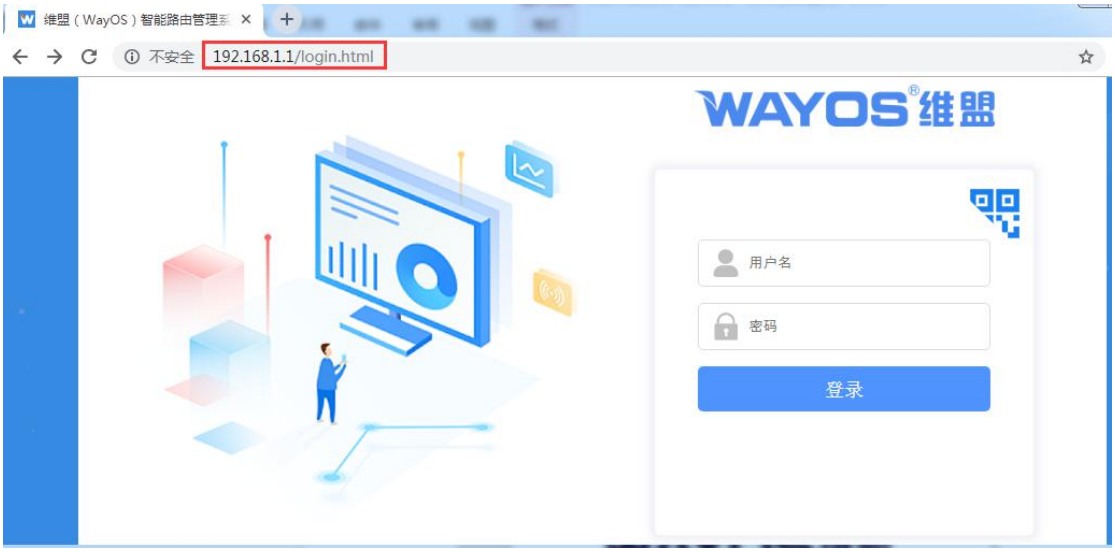
然后我们打开开始菜单，选择“运行”，并输入‘ping 192.168.1.1 -t’看看线路是否通畅。如图 5 所示：

若显示图 6 所示的结果，则表明网络连接正常；若显示图 7 所示的结果，则表明网络连接有问题，请检查网络连接状况。





当您与防火墙路由器正常连接以后，您就可以通过浏览器，在地址栏输入 https://192.168.1.1（路由器的默认 IP）进入路由器 WEB 设置界面。会出现图 8 所示的登陆画面：



防火墙路由器默认的用户名是“root”密码为“admin”，您可以在‘高级配置-访问设置’里自定义更改登陆的用户名及密码。

温馨提示：为了安全起见，我们强烈建议您在登陆以后更改管理员密码，并牢记此密码。若密码忘记，将无法再登陆到路由器的 Web 管理界面，必须 reset 恢复出厂设定值才能重新登陆。

一、 配置向导

设置向导可以协助您快速的配置好网络,只要按照步骤操作完成，即可设置好您的防火墙。

进入系统首页点击“配置向导”图标，出现配置向导界面。

步骤 1：WEB 访问设置，可以修改防火墙的登陆用户名及密码，如下图所示：

步骤 2：局域网设置，可以修改防火墙防火墙的 LAN 口 IP 地址，子网掩码，如图所示：

步骤 3：接口模式，此处用于对广域网/局域网数量进行设置。如图所示：

点击下方蓝色图标就可进行广域网/局域网的转换，点击之后 WAN/LAN 口将自动排序

注意：如果不需要用到这么多 WAN 口的用户可以把 WAN 口变为 LAN 口来使用，而当用户需要用到 WAN 口的时候，直接把 LAN 口又设置为 WAN 口，就可以了。

步骤 4：WAN 设置，此处用于对广域网接口参数进行配置。如图所示：

WAN 口：可以选择对应的广域网接口来进行设置。

连接方式：即广域网的接入类型选择，有：自动获取 IP、PPPOE 拨号、静态 IP 接入等多种接入方式，一般我们常用的有自动获取、PPPOE 和静态 IP 这 3 种。

静态 DNS：填入网络服务商提供的 DNS 服务器 IP 地址。(如果是 PPPOE 接入，可以不用设置 DNS 服务器地址，线路会自动获取到)

外网带宽：广域网的上下行带宽值，若不清楚带宽值的换算，可以使用参照值来自动填写。如果带宽不在参考值的范围之内，请手动设置出口带宽值大小。

带宽值参考：设置广域网出口带宽时的参考数值，可以参考此数值来设置。选择一个参照值之后，下面外网带宽的数值会自动填写上去。

设置好之后，点击完成，路由会显示‘正在操作中，请等待…’等待约十几秒，完成之

后，会自动返回到路由主界面。

设置好这些之后，即可正常连接互联网。

二、 系统状态

系统运行时的一些相关信息，从这些基本信息，我们可以了解到防火墙防火墙的工作情况。

2.1、 网络状态

广域网当前连接时间、连接方式、连接状态。局域网当前的 IP 地址，以及 MAC 地址、子网掩码等信息。

广域网口：显示每个广域网接口的信息；

MAC 地址：显示广域网口对应的 MAC 地址；

连接类型：表示当前广域网口的连接方式；如果是拨号接入，将显示 pppoe；如果固定 IP 接入，将显示 static；如果是 DHCP 自动获取，将显示 dhcp；

IP 地址：此处地址为对应广域网口的外网 IP 地址；

子网掩码：为相应 WAN 口的外部掩码；

网关：为相应 WAN 口的网关；

DNS：这里显示 ISP 提供商的 DNS 解析服务器 IP；显示结果将以手动填写为主，若没填

写，将自动从上级服务器获取。固定接入方式必须手动指定 DNS。

MTU：最大传输单元，一般此项是默认值，特殊情况在广域网设置处进行修改；

连接状态：Connected 表示连接成功，Connecting...表示正在连接；

连接时间：表示该广域网口与服务器建立连接的时间，以此时间可以判断 WAN 口是否掉线过；

操作：蓝色按钮表示重新获取 IP 地址，红色按钮表示释放 IP 也就是断开这个广域网。

2.2、 流量分析

广域网当前连接时间、连接方式、连接状态。局域网当前的 IP 地址，以及 MAC 地址、子网掩码等信息。

广域网口：显示每个广域网接口的信息；

MAC 地址：显示广域网口对应的 MAC 地址；

连接类型：表示当前广域网口的连接方式；如果是拨号接入，将显示 pppoe；如果固定 IP 接入，将显示 static；如果是 DHCP 自动获取，将显示 dhcp；

IP 地址：此处地址为对应广域网口的外网 IP 地址；

子网掩码：为相应 WAN 口的外部掩码；

网关：为相应 WAN 口的网关；

DNS：这里显示 ISP 提供商的 DNS 解析服务器 IP；显示结果将以手动填写为主，若没填写，将自动从上级服务器获取。固定接入方式必须手动指定 DNS。

MTU：最大传输单元，一般此项是默认值，特殊情况在广域网设置处进行修改；

连接状态：Connected 表示连接成功，Connecting...表示正在连接；

连接时间：表示该广域网口与服务器建立连接的时间，以此时间可以判断 WAN 口是否掉线过；

操作：蓝色按钮表示重新获取 IP 地址，红色按钮表示释放 IP 也就是断开这个广域网。

2.2、 流量分析

2.2.1 广域网

流量分析可以查看到每一条广域网的流量和总体使用的流量情况。

如上图，显示当前广域网的上传和下载流量分析图，并统计各种数据包类型，

选择查看的广域网：默认显示所有广域网总和的流量，如果需要查看单个广域网流量，请选择相应的广域网口；

上传/下载需求速度：为当前网络中，客户机对外发送请求所需要的流量；

上传/下载调配速度：防火墙通过 QoS 规则智能均衡计算之后，分配的速度值。

此处显示的速度单位为 KB，具体换算单位如下：

1.计算光纤传输的真实速度

使用光纤连接网络具有传输速度快、衰减少等特点，因此很多公司的网络出口都使用光纤。比如，网络服务商声称光纤的速度为 5M，那么他的下载真实速度是多少呢？我们来计

算一下。一般的情况下，5M 实际上就是 5000Kbit/s(按千进位计算）这就存在一个换算的问题。Byte 和 bit 是不同的。1Byte=8bit.而我们常说的下载速度都指的是 Byte/s 。因此 ISP 所说的“5M”经过还换算后就成为了（5000/8）KByte/s= 625KByte/s 这样我们平时下载速度最高就是 625KByte/s，常常表示 625KB/S。

在实际的情况中，理论值最高为 625KB/S。那么还要排除网络损耗以及线路衰减等原因，因此真正的下载速度可能还不到 600KB/S 不过只要是 550KB/S 以上都算正常。

2.计算 ADSL 的真实速度

ADSL 是大家经常使用的上网方式。那么电信和网通声称的 1 兆 ADSL 下载速度是多少？换算方法为 1Mbit/s=(1000/8)KByte/s=125KByte/s，考虑线路等损耗，实际的下载速度在 100KB/S 以上就算正常了。那么“2MB”呢？大家算算吧，答案是 256KByte/s 。

3.计算内网的传输速度

经常有人抱怨内网的传输的数度慢，那么真实情况下的 10/100Mbps 网卡的速度应该有多快？网卡的 100Mbps 同样是以 bit/s 来定义的，所以 100Mb/S ＝ 100000KByte/s=(100000/8)KByte/s=12500KByte/s 。在理论上 1 秒钟可以传输 12.5MB 的速据，考虑到干扰的因素，每秒传输只要超过 10MB 就是正常了。现在出现了 1Gbps 的网卡，那么速度就是 100MB/S 。

特别提示：

1.关于 bit(比特)/second(秒)与 Byte(字节)/s(秒)的换算说明：线路单位是 bps，表示 bit(比特)/second(秒)，注意是小写字母 b；用户在网上下载时显示的速率单位往往是 Byte(字节)/s(秒)，注意是大写字母 B。字节和比特之间的关系为 1Byte=8Bits；再加上 IP 包头、HTTP 包头等因网络传输协议增加的传输量，显示 1KByte/s 下载速率时，线路实际传输速率约 10kbps。例如：下载显示是 50KByte/s 时，实际已经达到了 500Kbps 的速度。切记注意单位！！！

2.用户申请的宽带业务速率指技术上所能达到的最大理论速率值，用户上网时还受到用户电脑软硬件的配置、所浏览网站的位置、对端网站带宽等情况的影响，故用户上网时的速率通常低于理论速率值。

3.理论上：2M（即 2Mb/s）宽带理论速率是：256KB/s（即 2048Kb/s），实际速率大约为 103-200kB/s；(其原因是受用户计算机性能、网络设备质量、资源使用情况、网络高峰期、网站服务能力、线路衰耗，信号衰减等多因素的影响而造成的)。4M（即 4Mb/s）的宽带理论速率是：512KB/s，实际速率大约为 200-440kB/s。

基础知识：

在计算机科学中，bit 是表示信息的最小单位，叫做二进制位；一般用 0 和 1 表示。Byte 叫做字节，由 8 个位（8bit）组成一个字节(1Byte)，用于表示计算机中的一个字符。bit 与 Byte 之间可以进行换算，其换算关系为：1Byte=8bit（或简写为：1B=8b）；在实际应用中一般用简称，即 1bit 简写为 1b(注意是小写英文字母 b)，1Byte 简写为 1B（注意是大写英文字母 B）。

在计算机网络或者是网络运营商中，一般，宽带速率的单位用 bps(或 b/s)表示；bps 表示比特每秒即表示每秒钟传输多少位信息，是 bit per second 的缩写。在实际所说的 1M 带宽的意思是 1Mbps（是兆比特每秒 Mbps 不是兆字节每秒 MBps）。

建议用户记住以下换算公式：

1B= 8b1B/s=8b/s(或 1Bps=8bps)

1KB=1024B　　1KB/s=1024B/s

1MB=1024KB　　1MB/s=1024KB/s

规范提示：实际书写规范中 B 应表示 Byte(字节)，b 应表示 bit(比特)，但在平时的实际书写中有的把 bit 和 Byte 都混写为 b ，如把 Mb/s 和 MB/s 都混写为 Mb/s，导致人们在实际计算中因单位的混淆而出错。切记注意！！！

2.2.2 应用协议

在此可以查看到所有被行为管理识别和未识别的应用协议流量使用情况，可以此来分析网络流量大致分布情况。

上传/下载总速度：当前查看协议被实别的实际上传/下载总的速度；

上传/下载总数据：当前查看协议被实别的总的数据；

应用协议：显示出当前查看协议包含的所有协议；

上传/下载速度：对应协议所使用网络的当前上传速度（‘|’左边为当前速度，右边为占用当前查看协议速度的百分比）；

上传/下载数据：对应协议所使用网络的总数据；

详细：查看当前协议里更详细的协议流量使用情况（当前协议已经为最详细时，不能再点详细进行查看）；

2.3、 主机监控

2.3.1 主机监控

‘主机监控’能显示内网所有用户的网络连接情况。位于"列表"上方的记录数，可以显示当前内网的在线机器数量。

在列表中，可以很直观的看出每台 PC 占用的网络情况，鼠标点击"查看连接"，还能显示该 PC 的网络访问情况，有进程管理的也可以点击查看正在使用的进程。如下图所示：

点击"查看连接"后的效果：

协议	本地端口	远端IP	远端端口	运行时间	优先级	上传总数据	下载总数据	类型	接口	域名	控制	操作
TCP	52930	192.168.1.1	80	0秒	中 中	0 b	0 b	普通网页	LAN		允许	允许 阻止
TCP	52906	59.37.97.57	993	8分34秒	中 中	2.40 K	25.66 K	未识别	WAN1		允许	允许 阻止
TCP	52901	59.37.97.57	993	8分54秒	中 中	1.34 K	4.07 K	未识别	WAN1		允许	允许 阻止
TCP	52839	59.37.97.57	993	22分33秒	中 中	3.52 K	61.26 K	未识别	WAN1		允许	允许 阻止
TCP	52221	58.222.216.198	8081	42分11秒	中 中	321.26 K	896.47 K	普通网页	WAN1		允许	允许 阻止
TCP	52139	111.201.13.56	8088	44分40秒	中 中	311.83 K	396.76 K	普通网页	WAN1		允许	允许 阻止
TCP	51945	219.133.60.187	993	53分8秒	中 中	25.76 K	490.19 K	未识别	WAN1		允许	允许 阻止

在这个地方可以点击阻止和允许该连接是否使用。默认的是允许使用。如果需要阻止可以点击“阻止”按钮。

点击“详细信息”后的效果：

详细信息页面可以查看当前主机 IP 的规则限制，联机数使用情况及带宽使用情况等。

2.3.2 PPPoE 用户

该记录是显示通过 PPPOE 拨号到防火墙的用户信息。

2.3.3 DHCP 用户

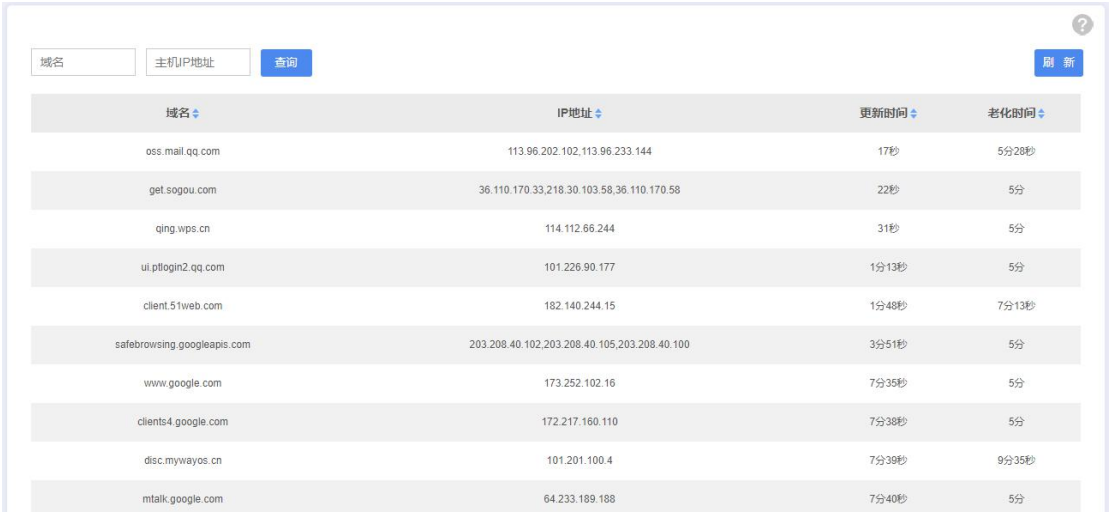
此列表将显示所有 DHCP 自动获取 IP 的用户信息。

2.3.4 聊天账号

列表显示防火墙下的用户聊天软件信息，包括有 QQ、MSN、飞信、淘宝旺旺等。

2.4、 DNS 缓存

此列表显示通过设备的 DNS 解析缓存



2.5、 登录记录

此列表将显示所有登陆防火墙的历史用户。

2.6、 系统日志

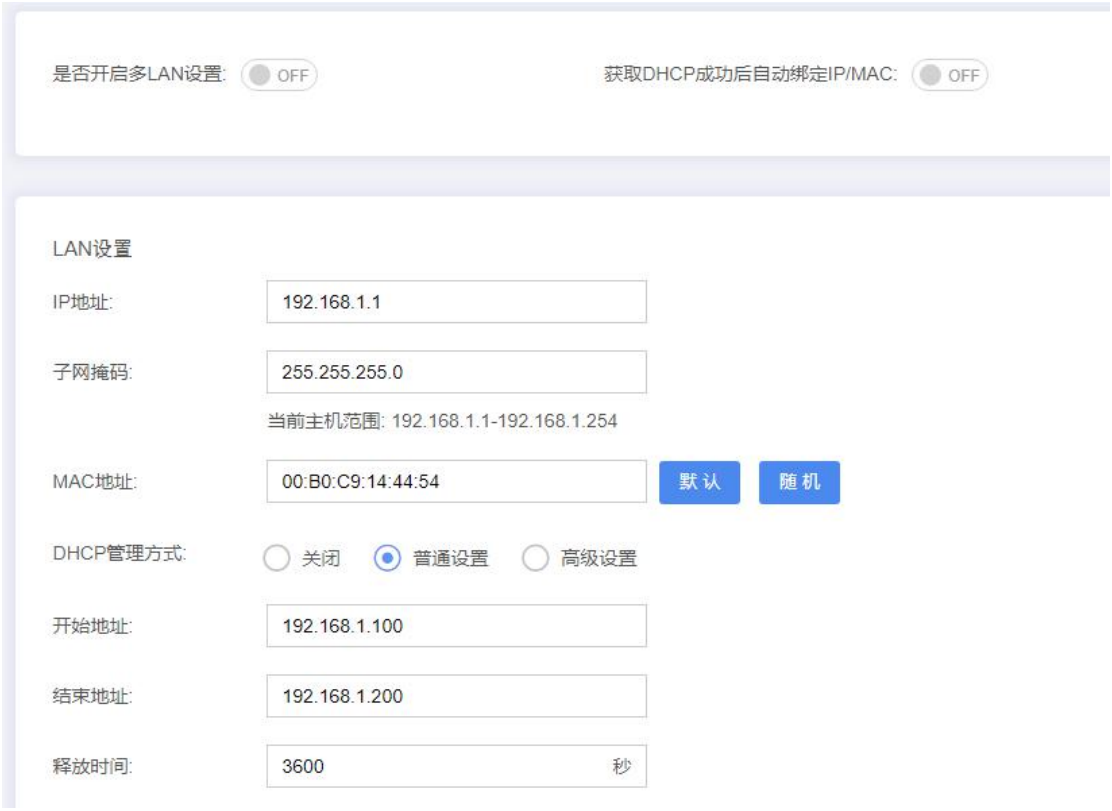
在这里可以显示系统日志、ARP 日志、流量攻击、DDOS 日志、PPPoE 日志、访问控制日志、通告系统日志、策略路由日志、行为管理等，所有的日志都可以在这里查看到。

三、 网络配置

路由的一些基本功能设置，包括局域网设置、广域网设置、DHCP 配置、及 DDNS 功能的设置。

3.1、 局域网

本页面主要用于局域网设置的相关参数，如下图所示：



是否开启多 LAN：开启多 LAN 功能后，LAN 口之间可独立出来且可使用 VLAN 功能，每个 LAN 口可以设置不同的网段；

开启 DHCP 自动绑定 IP/MAC 功能：DHCP 用户的 IP 和 MAC 会自动绑定为静态，在主机监控和 ARP 列表可以查看；

IP 地址：设置防火墙内网口的 IP 地址，这个地址就是内网计算机的网关地址。该地址出厂时设置为 192.168.1.1，可以根据需要改变它，如果改变了防火墙内网 IP 地址，需要重新连接防火墙；

子网掩码：根据内网规模设置合适的掩码值。防火墙默认使用的子网掩码是 255.255.255.0，可以根据需要更改；

MAC 地址：根据内网的网络情况，修改 MAC 地址。一般情况下默认的有 MAC 地址，不需要调整；

DHCP 管理方式：主要提供 DHCP 服务器功能。如果内网计算机的 TCP/IP 协议配置为“自动获得 IP 地址”，并且在内网没有 DHCP 服务器的情况下，可以使用该功能；

管理方式：可以选择普通、高级或者关闭。普通 DHCP 方式只能分配防火墙 LAN 口网段的 IP，高级 DHCP 方式可以任意分配 IP 段、掩码及 DNS 服务器地址；

开始地址：DHCP 服务器自动分配的内部 IP 的起始地址；

结束地址：DHCP 服务器自动分配的内部 IP 的结束地址；

释放时间：设定 DHCP 服务器为客户端租用 IP 地址保留的过期时间，默认是 3600 秒。可自行设置；

网关地址：DHCP 服务器给客户机分配的默认网关地址；

子网掩码：DHCP 服务器自动分配给客户机的掩码地址；

首选/备用 DNS 服务器地址：DHCP 服务器自动分配给客户机的 DNS 服务器地址。

多子网段：本防火墙内网口允许配置多个 IP 地址，当内部有多于一个子网时可以使用到该功能。其功能与防火墙内网地址基本一致，通常作为相应子网的网关使用。此地址不要跟 LAN 口地址设置到同一个子网中，否则可能引起冲突。

多子网段的设置如图所示：

所添加的 IP 地址相当于是 LAN 口虚拟的另一个网关地址，客户机可以使用添加的多子网 IP 作为网关地址来上网。此地址不要跟 LAN 口设置到同一个子网，否则可能会引起冲突。

3.2、 广域网

本页面主要用于配置 WAN 口相关参数，我们常用的广域网连接方式主要有自动获取 IP、static 静态接入跟 PPPOE 拨号接入三种。

1. 自动获取 IP

选择您要设置的广域网：选择我们需要配置的广域网口，从下拉列表框即可选择。

广域网批量设置：多个广域网需要设置的情况下，可以进行批量设置，不需要一个一个去选择，如下图所示：

当前接口：显示该广域网对应的实际物理接口

连接类型：选择自动获取 IP（动态获取地址）；

MAC 地址：根据网络情况，随机或克隆 MAC 地址。一般情况下默认的 MAC 地址，不需要调整；

外网带宽：广域网的上下行带宽值，若不清楚带宽值的换算，可使用参照值来自动填写。如果带宽不在参考值的范围之内，请手动设置出口带宽值大小；

线路侦测：启用线路侦测功能。线路侦测主要用于检测线路的通畅与否，对于多线路环境，若其中一根线路侦测失败，系统默认会将该线路移除，线路上的所有会话将会自动转移到另外侦测成功且参与均衡的线路上去；

高级参数：

802.1X：基于端口的网络接入控制协议，可选择使用或不使用该协议；

MTU 设置：即最大传输单元，系统默认使用 1500 字节。通常情况下这个参数不用设置，保持默认即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

静态 DNS：填入网络服务商提供给的 DNS 服务器 IP 地址，由网络服务商提供，可向网络服务商询问获得。

工作模式：通常我们都使用网关模式，接口做 NAT 地址转换；有些特殊环境可能会用到路由模式（如内网机器全部使用公网 IP 的时候）。

DNS 解析优先级：对于多 WAN 口接入时，此值的大小决定了 DNS 解析的出口。

防御信息检测：此功能用于防御运营商对线路的共享限制使用，开启此功能可能会导致某些应用异常，特殊网页打不开等。

运营商：所使用的广域网线路的运营商，例如网通或者电信。如果选择“不设置”，则该线路需与策略路由功能配合使用。单 WAN 口接入环境可以不设置运营商。

基于时间控制：根据设置的时间断开对应的广域网线路，过了设置的时间段会自动连接上。

2.静态 IP 接入

连接类型：选择静态 IP 上网方式；

IP 地址：申请的线路的广域网 IP 地址，由网络服务商提供，可向网络服务商询问获得；

子网掩码：前 IP 所对应的子网掩码，由网络服务商提供；

默认网关：当前 IP 所对应的网关，由网络服务商提供；

MAC 地址：根据内网的网络情况，随机或克隆 MAC 地址。一般情况下默认的 MAC 地址，不需要调整；

外网带宽：广域网的上下行带宽值，若不清楚带宽值的换算，可以使用参照值来自动填写。如果带宽不在参考值的范围之内，请手动设置出口带宽值大小；

高级参数：

802.1X：基于端口的网络接入控制协议，可选择使用或不使用该协议；

MTU 设置：即最大传输单元，系统默认使用 1500 字节。通常情况下这个参数不用设置，保持默认即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用；

静态 DNS：填入网络服务商提供的 DNS 服务器 IP 地址，由网络服务商提供，可向网络服务商询问获得；

工作模式：通常我们都使用网关模式，接口做 NAT 地址转换；有些特殊环境可能会用到路由模式（如内网机器全部使用公网 IP 的时候）；

DNS 解析优先级：对于多 WAN 口接入时，此值的大小决定了 DNS 解析的出口；

防御信息检测：此功能用于防御运营商对线路的共享限制，静态地址接入时，我们不需要开启此功能；

运营商：广域网线路的运营商，例如网通或者电信。如果选择“不设置”，则该线路需与策略路由功能配合使用。单 WAN 口接入环境可以不设置运营商；

基于时间控制：根据设置的时间断开对应的广域网线路，过了设置的时间段会自动连接上。

3.ADSL 拨号上网（PPPOE 拨号接入）

连接类型：选择 ADSL 拨号上网（PPPOE 拨号接入）；

用户名称：填入网络服务商提供的 PPPOE 线路帐号，可以向网络服务商询问获得；

用户密码：填入网络服务商提供的 PPPOE 线路口令，可以向网络服务商询问获得；

MAC 地址：根据内网的网络情况，随机或克隆 MAC 地址。一般情况下默认的 MAC 地址，不需要调整；

外网带宽：广域网的上下行带宽值，若不清楚带宽值的换算，可以使用参照值来自动填写。如果带宽不在参考值的范围之内，请手动设置出口带宽值大小；

高级参数：

服务名称：一般不填，某些特殊线路可能需要填入服务器名称才可以。

使用 ISP 指定的 IP 地址:手动填写运营商提供的 IP，拨号成功以后获取到的 IP 便是此处手动填写的；

获取指定的网关地址：手动填写拨号的网关地址，否则便是自动获取；

连接模式：有三种模式，一般选择保持连接即可；

连接检查间隔：用户自行设定重新拨接的时间，默认值为 30 秒；

MTU 设置：即最大传输单元，系统默认使用 1500 字节。通常情况下这个参数不用设置，保持默认即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用；

静态 DNS：填入网络服务商提供的 DNS 服务器 IP 地址，由网络服务商提供，可以向网

络服务商询问获得，PPPOE 拨号接入时可以不用填写 DNS 地址，若不想使用自动获取的 DNS 地址时，可以填入网络服务商提供的其他 DNS 服务器地址；

工作模式：通常我们都使用网关模式，接口做 NAT 地址转换；有些特殊环境可能会用到路由模式（如内网机器全部使用公网 IP 的时候）；

DNS 解析优先级：对于多 WAN 口接入时，此值的大小决定了 DNS 解析的出口；

防御信息检测：此功能用于防御运营商对线路的共享限制，静态地址接入时。我们不需要开启此功能；

运营商：广域网线路的运营商，例如网通或者电信。如果选择“不设置”，则该线路需与策略路由功能配合使用。单 WAN 口接入环境可以不设置运营商；

基于时间控制：定时重拨对应的广域网线路。

MAC 地址中的 

选项分别有如下定义：

“克隆”表示将该接口的 MAC 地址设置为与电脑的 MAC 一样的地址；

“默认”表示使用系统默认的 MAC 地址；

“随机”表示随机分配一个 MAC 地址给该接口。

某些网络服务商将提供给的线路同某一个固定的 MAC 地址绑定起来，在这种情况下，MAC 地址克隆就非常有用。

3.3、 动态域名

DDNS 动态域名解析服务主要用于将一个动态的 IP 解析成一个静态的域名，以便于网络来访问。

选择动态域名工作的广域网：选择一个需要绑定域名更新的广域网接口；

动态域名服务：选择一个需要绑定 IP 的域名服务商，后面提供有服务商的官方网址；

用户名称/密码：填写在域名服务商申请的账号名称及密码；

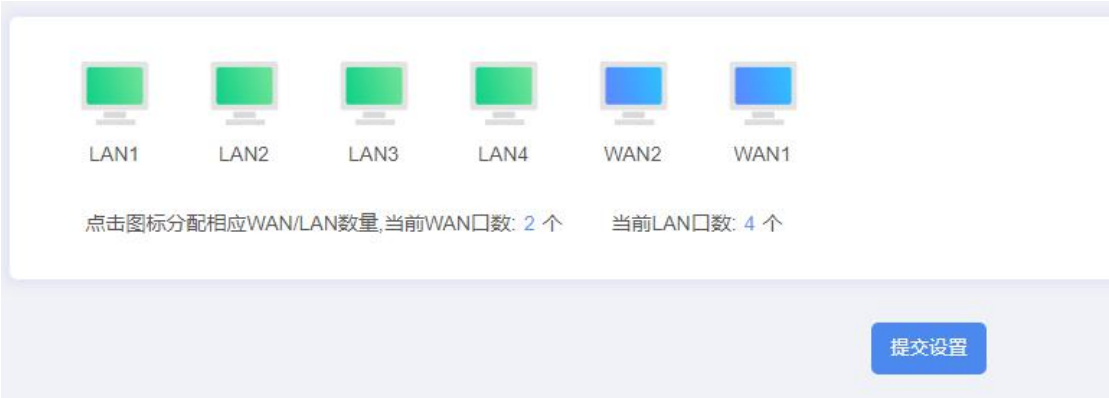
需要更新的域名：填写需要绑定此 IP 的一个域名，该域名必须为未被其他 IP 使用过。

设置完毕之后点击“添加”，加入到列表中即可。若域名更新成功，在‘最近响应状态’会显示“Update successful” 的字样，即更新成功的意思。

编号	接口	服务器名称	域名	最近IP地址	最近响应状态
1	广域网1	3322 - 动态地址	445[redacted].3322.org	2019-03-14 19:30:42: 192.168.22.160	2019-03-14 19:30:42 Update successful

3.4、 接口设置

此处可更改防火墙上的原生物理口的 LAN/WAN 模式，不包括扩展口。



可以更改防火墙的 LAN/WAN 接口，LAN/WAN 口是连续的。修改提交后重启防火墙生效。

3.5、 安全区域

用于设置接口所属的区域，以供内容安全、IPS、防火墙等模块调用。
一个接口只能选择一个安全区域，一个安全区域可以容纳多个接口。

3.6、 策略路由

3.6.1 策略路由

策略主要用于设置内网用户对不同线路的走向。对于单线路用户，则无需对此功能进行设置。

状态：对规则的控制开关，选择开启表示激活该条规则；

描述：对该条规则的简单文字描述，该描述必须是唯一的；

执行顺序：以 1-65535 之间的数字来表示规则的执行顺序，数值大的规则优先执行；

主机 IP 地址范围：设置需要控制的主机范围。就是“内网地址”；

应用协议：选择需要管控的单个或者多个协议；

自定义 IP 协议：可自行定义远端 IP、域名及端口协议，并以此作为管控对象；

广域网的选择：当数据匹配上时，匹配的数据直接从选择接口出去，不再进行后面规则的匹配；

自动切换线路：开启后支持自动切换外网线路；

日志：对于匹配上的数据包，进行日志记录；

基于时间控制：如果启用了“基于时间控制”，那么该规则，将在指定的时间段内生效

每周：可设置一周的哪几天生效。

每天：可设置一天的哪些时段生效。

在列表下方可选择将设置的策略路由规则导入导出，如图所示：

3.6.2 负载均衡

负载均衡用于设置线路的均衡模式及侦测方式、均衡权值等。

负载均衡模式：分为 IP 地址均衡跟联机数均衡两种；

依 IP 地址均衡：依据内部用户的 IP 地址来决定线路的负载均衡；

依会话数均衡：依据用户的对外联机数来决定线路的负载均衡；

IP 均衡的作用，每条线路上的 IP 用户数目是等同的；会话数均衡的作用，每条线路上的对外联机数目是等同的。当使用会话数均衡的时候，就是将外网的几根线路都叠加起来，相当于是合并了总带宽；

身份绑定功能：如果配置了多线路，要使 QQ、网银等正常使用，请启用身份绑定功能；

选择广域网：选择需要设置的广域网接口；

该线路参与默认均衡策略：勾上即表示参与，若不需要让此线路参与均衡，去掉勾即可。不参与均衡的线路将只接受策略路由里绑定的规则数据走向，若策略路由里也没有绑定数据走该线路，那么该线路将不会有数据流量；

线路侦测：启用线路侦测功能。激活时高级参数的选项才能被启用，否则无效。线路侦测主要用于检测线路的通畅与否，对于多线路环境，若其中一根线路侦测失败，系统默认会将该线路移除，线路上的所有会话将会自动转移到另外侦测成功且参与均衡的线路；

均衡的权值：此值主要用于跟其他线路的均衡做比较，系统会根据值的大小来决定线路的负载大小，默认值是依靠带宽值的大小来自动判定，需填写出口带宽值才有效。若改为自定义，请根据线路的权衡比例来设置此参数，参数越大，通过的数据/用户就会越多；

侦测间隔：线路自动侦测的中间间隔时间；

侦测次数：线路侦测的次数；

当线路连接失败时：当线路检测失败时，对该线路的处理方式；

移除该线路并记录日志：将此线路删除，并记录到日志中，该线路上的所有连机将自动转移到其他线路上；仅记录到日志：仅在日志中记录下此次掉线日志，不删除该线路；

下载流量超过：下行流量超过设置值的时候才进行线路侦测；

侦测默认网关：勾选上即表示侦测此线路的外网网关。内容为空，表示侦测默认的网关。有些 ISP 的默认网关可能不允许 ping，那么可手动指定一个其他的广域网地址进行测试；

侦测远程服务器：填入一个稳定的域名或者广域网 IP 地址用于检测线路的通断与否。

注意：线路侦测默认是以 ping 来判断线路的通与断，所以，在填写侦测 IP 或者服务器地址的时候，请尽量选择一个长期稳定在线的地址。

3.6.3 地址范围

用于多条运营商线路的环境中使用策略路由。只要选择相应的线路，并设置策略方式即可实现电信网通分开走，互不干扰。

查询 IP 所在范围：查询该 ip 属于以下已经启用的地址范围列表中的哪一类。

可以在此界面自行更新电信/网通等的地址范围，或者自定义添加新的地址范围段。

3.6.4 线路状态

显示每根线路的在线状态及主机数、会话数信息。

主机数信息只有在均衡方式为 IP 均衡时才会显示，会话数信息是会实时显示的。

3.6.5 日志

用于记录广域网口线路的工作状态，如果线路有掉线等情况，将会在此日志里显示出来。

如果在策略路由中添加规则的时候，勾选了日志，那么策略规则产生的日志信息将会在日志中记录下来。

3.7、 静态路由

路由表，指防火墙或者其他互联网网络设备上存储的表，该表中存有到达特定网络终端的路径，在某些情况下，还有一些与这些路径相关的度量。防火墙的主要工作就是为经过防火墙的每个数据报寻找一条最佳传输路径，并将该数据有效地传送到目的站点。

3.7.1 当前路由表

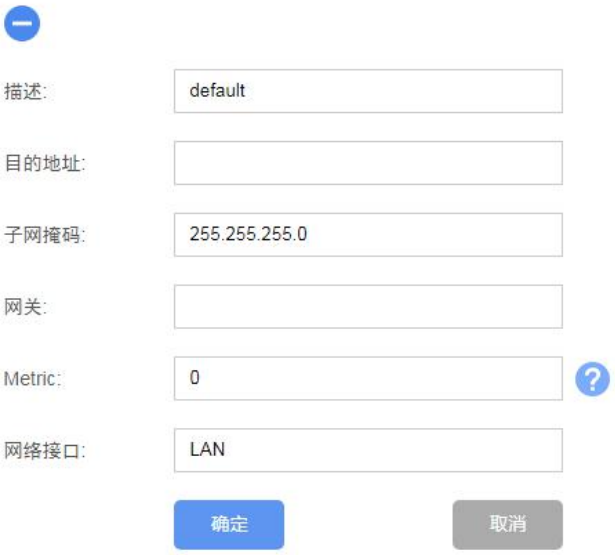
当前路由表是防火墙当前自动生成的静态路由表。

目的地址	网关	子网掩码	Metric	网络接口
10.198.1.0	*	255.255.255.0	0	pppsrv
172.16.1.0	10.198.1.1	255.255.255.0	0	pppsrv
192.168.10.0	*	255.255.255.0	0	LAN
127.0.0.0	*	255.0.0.0	0	lo

此路由表是系统自动生成的，提供给用户查看，不可以修改。

3.7.2 IPV4 静态路由表

在一些特殊环境中，我们也需要手动去指定静态路由表的走向，此时，我们需要手动去添加静态路由表，如图所示：



举例：如 wayos 路由下层挂接有一台三层交换机，交换机的 IP 为 192.168.1.244，该三层交换机下发的有一个 172.15.2.1/24 的网段，三层交换机下的主机使用 172.15.2.X 网段的 IP 上网，并使用 172.15.2.1 作为网关地址，那么，我们就需要添加如上图所示的静态路由，才可以使三层交换机下的主机正常上网。

四、 防火墙

4.1、 外网防护

通过该功能可以对外网数据包进行检测，过滤外网对内网的数据攻击。

名称：规则的名字

描述：对规则的描述信息

源区域：选择需要检测该区域的数据包。一般选择 WAN 侧的区域。

ARP 洪水防攻击：开启后可防御 ARP 洪水攻击，配合下面的区域阀值。

IP 地址扫描防护：开启后可防非法 IP 地址扫描，配合下面的区域阀值。

端口扫描防护：开启后可防非法端口扫描，配合下面的区域阀值。

DOS/DDOS 攻击防御：点击选择需要防护的攻击类型。

基于数据包攻击：点击选择数据包攻击类型

IP 协议报文侦测：点击选择 IP 协议报文攻击类型

TCP 协议报文侦测：点击选择 TCP 协议报文攻击类型

检测攻击后的动作：可选择被攻击后执行的操作

4.2、 内网防护

开启该功能后，防止内网设备因中毒或使用攻击工具发起的 DOS 攻击。

源区域：设置内网防护的区域，一般为 LAN 侧区域

源地址过滤：设置哪些 IP 可以经过防火墙。若勾选<允许任意源 IP 地址的数据包通过>，将不对过源区域的 IP 做限制。若勾选<仅允许以下 IP 地址的数据包通过>，则只有设置的 IP 才能经过防火墙，其余的 IP 包将被丢弃。

部署环境选择：选择防火墙与内网的部署环境。若设备和内网之间是通过二层交换机直接相连，没有过任何三层设备或者防火墙，则勾选<内网通过二层设备与本机直接相连>或<内部网络到本机通过三层交换设备相连>均可;若设备和内网之间是通过三层设备直接相连，则勾选<内部网络到本机通过三层交换设备相连>。

排除地址设置：配置不进行 DOS 防护的 IP 地址或域名。

TCP 最大链接数：限制同一 IP 地址在一分钟内向同意目标 IP 地址的同一端口发起的最大 TCP 链接数，若超过设定的值则把源 IP 封锁特定的时间。

最大攻击包次数：限制每个 IP 在每分钟内发起的最大攻击包次数（攻击包包括 SYN、ICMP、TCP/UDP 等小包），若超过设定的值则把该 IP 或 MAC 封锁特定的时间

封锁攻击时间：设置设备在检测到攻击以后对攻击主机的封锁时间，以分钟为单位，默认 3min。

检测攻击后的动作：设置是否对检测到攻击的数据包产生日志记录。

4.3、 访问控制

访问控制的方式：设置访问控制的方式，有三种选择

不启用访问控制：关闭访问控制功能，列表中的所有规则将都不生效；

允许规则之外通过：列表中的规则按照控制的方式来执行，列表之外的规则不受控制，直接允许通过；

禁止规则之外通过：列表中的规则按照控制的方式来执行，列表之外的规则受到控制，禁止被通过。要单独设置允许通过的，请在规则中添加相应规则来运行其通过。

状态:对规则的控制开关，选择启用表示激活该条规则；

描述：对此规则的简单描述。默认 default，建议修改为方便自己识别的描述；

控制方式：控制访问规则是允许通过还是禁止通过；

执行顺序：用来比较多条规则的优先级，值越大越优先执行。当出现有相互冲突的两条规则时，会优先执行数值大的那一条规则；

主机 IP 地址范围：需要进行控制的内部主机 IP 地址范围；

自定义 IP 协议：可以自行定义远端 IP、域名及端口协议，并以此作为管控对象；

协议：需要控制的协议和端口，可以选择 TCP，UDP 和 ICMP，也可以是内部端口和外网端口；

日志：对设置的规则记录日志，可以方便观察规则是否生效；

基于时间控制：是否启动按时间段管控功能（若启用，用户可自定义管控时间段）。

举例说明：

限制 IP 为 192.168.1.10-192.168.1.20 之间的机器只能上 QQ 跟浏览网页，其他机器不做限定，可以做如下设定：

1.选择访问控制的方式为‘允许规则之外的通过’，并点击提交按钮。如图所示：

2.先添加一条禁止 192.168.1.10-192.168.1.20 之间的 IP 访问任何地址的规则，如图所示：

3.再添加一条允许 192.168.1.10-192.168.1.20 之间的 IP 访问网页跟 QQ 的规则。如图所示：

此规则优先级必须高于被禁止的规则，否则此规则设置将无效。

由于大多数网页都是走的 TCP 协议的 80 跟 443 端口，QQ 程序一般都是使用 UDP 协议的 8000-8004 端口，所以我们将以此为例做限制。需要注意的是，设置协议端口时，我们一般使用的是外部端口，如图所示：

设定完毕之后请点击添加按钮，将规则添加进列表中即可. 规则会在添加之后立即生效，不需要重启防火墙。所以在做禁止的规则时，请先考虑好是否有正在使用的协议等在控制范围之内，否则一旦设置了禁止的规则，就会对现有的协议使用受到影响。

4.4、 访问控制日志

记录访问控制规则产生的日志记录，需要在添加规则的时候先勾选上日志选项才会记录。

4.5、 NAT 一对一规则

NAT 转换即为网络地址转换，允许一个整体机构以一个公用 IP（Internet Protocol）地址出现在 Internet 上。顾名思义，它是一种把内部私有网络地址（IP 地址）翻译成合法网络 IP 地址的技术。因此我们可以认为，NAT 在一定程度上，能够有效的解决公网地址不足的问题。

一对一即为将一台主机发送数据的源地址转换为对应的一个外网地址。

状态：对规则的控制开关，选择启用表示激活该条规则；

描述：对规则的简单描述；

内部地址：填入内部地址用于做一对一的网络地址转换。例如：192.168.0.50；

外部地址：填入外部地址用于做一对一的网络地址转换。例如：218.35.97.7；

开放协议：选择需要使用的协议；

开放端口：填入外部地址开放的端口。为空表示开放全部，格式：100,200,300:305；

接口：选择外部出口。

4.6、 NAT 多对多规则

NAT 转换即为网络地址转换，允许一个整体机构以一个公用 IP（Internet Protocol）地址出现在 Internet 上。顾名思义，它是一种把内部私有网络地址（IP 地址）翻译成合法网络 IP 地址的技术。因此我们可以认为，NAT 在一定程度上，能够有效的解决公网地址不足的问题。

NAT 多对多规则即为将一段主机发送数据的源地址转换为对应的一段外网地址。

状态：对规则的控制开关，选择启用表示激活该条规则；

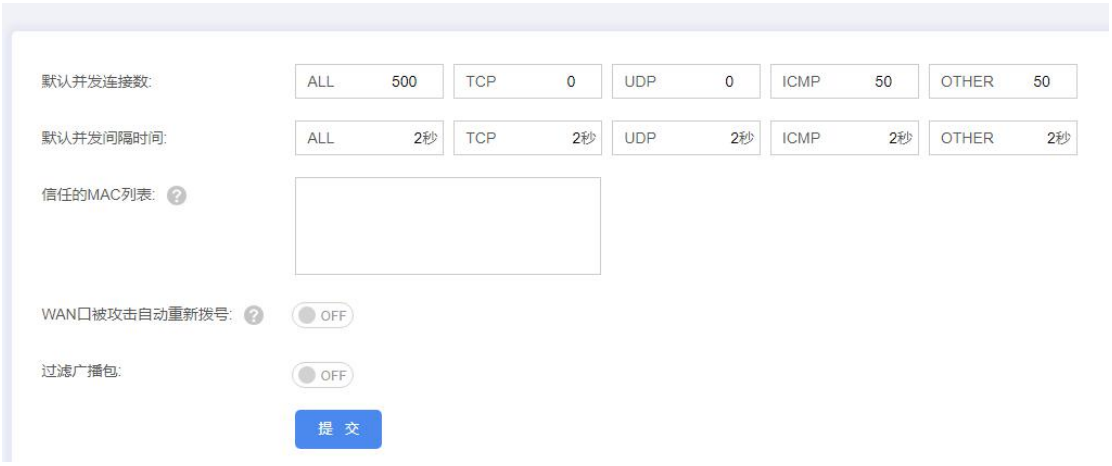
描述：对规则的简单描述；

设为内网扩展地址：开启设为内网扩展地址；

转换地址：填入可以设置一个 IP 地址作为转换地址，也可以设置一个地址段做为转换地址。设置地址段时，最大长度为 16 个地址，例如：221.18.10.6-221.18.10.21。

4.7、 DDOS 防御

对用户的并发连接进行限制。并发连接指一定时间内用户发起的连接的总数。



默认并发连接数：单位时间内可以发起的连接总数。规则之中的用户不受默认并发连接影响；

默认并发连接间隔时间：并发连接单位时间；

信任的 MAC 列表：填入这里的 MAC 地址将不受并发连接数的限制；

被攻击自动重拨：当监测到 WAN 被攻击时，将会自动重新拨号；

过滤广播包：开启后会自动过滤到异常的广播包；

激活：是否启用规则；

描述：对规则的简单描述；

主机 IP 地址范围：需要单独控制并发连接的主机对象；

并发连接类型：可以单独选择 TCP，UDP 或者所有；

并发连接数：单机所允许的最大并发连接数条目；

并发连接间隔时间：相应的间隔时间，单位为秒；

基于时间控制：如果启用了“基于时间控制”，那么该规则将只在设定的时间范围内生效；

4.8、 DDOS 自动防御

防火墙自动识别并且屏蔽攻击源，使防火墙能正常工作。并且防火墙会把攻击日志与攻击源的 MAC 地址记录在 DDOS 日志当中。

白名单状态：开启/关闭 是否开启白名单功能，此功能主要用于不受控制的终端设备

MAC 白名单列表：填入这里的 MAC 地址将不受并发连接数的限制；

被攻击类型：当选择你所需要设置防御的攻击类型。

攻击阀值：设置阀值，此值表示超过设置的阀值就认为是攻击

屏蔽攻击源：阻止有攻击的电脑再次发起攻击；

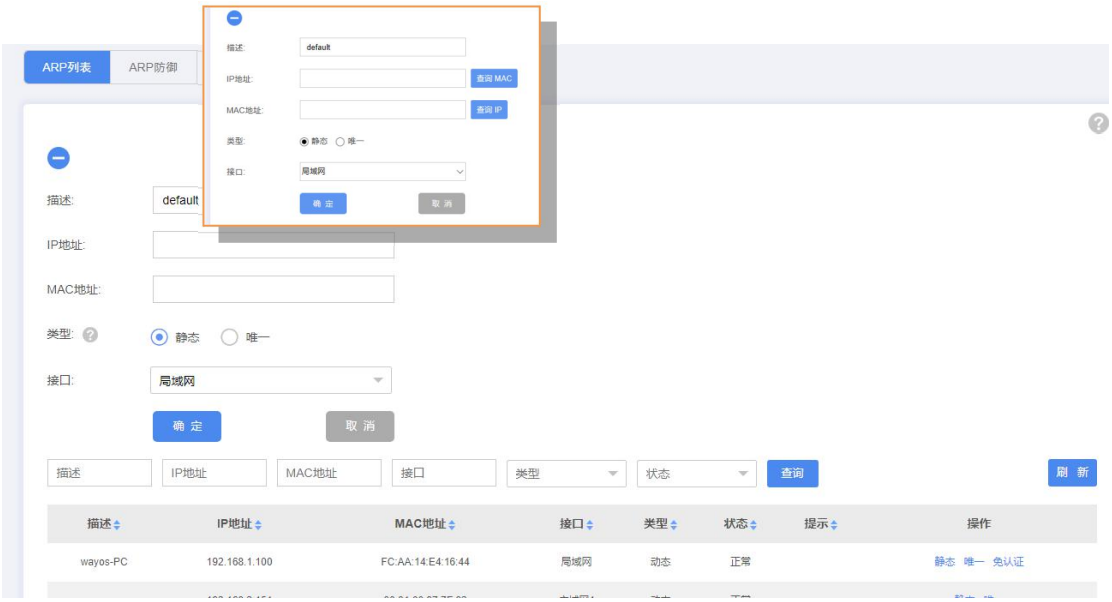
屏蔽持续时间：设置屏蔽与此攻击源的连接的时间。如果屏蔽时间到了之后，攻击源依然在对网络进行攻击，ddos 自动防御功能会再次屏蔽此攻击源。

4.9、 ARP 管理

设置防火墙安全防御信息，包括 ARP 管理与防御、联机数设置、DDOS 防御、访问控制等。

4.9.1 ARP 列表

ARP 列表显示当前局域网连接用户的 IP 及 MAC 信息，并且可以手动添加 ARP 绑定。



描述：对该条绑定信息的简单文字描述，便于管理员区分；

IP 地址：将要绑定的 IP 地址；

查询 MAC：如果该 IP 地址在线则可以点击该按钮查询到其使用的 MAC 地址。

MAC 地址：输入要进行 ARP 绑定的 MAC 地址,可以通过“查询 MAC”来设置 MAC。如果用户不在线则需要手动输入；

类型：分为两类:“静态”和“唯一”

“静态”:IP 与 MAC 地址绑定为静态以后，用户手动更改 IP 或者 MAC 地址不会影响网络使用，但其他用户不能占用此 IP 跟 MAC 地址；

“唯一”:不但限制这个 IP 地址只能在这个 MAC 上使用，同时也限制了这个 MAC 地址只能使用指定的 IP 地址，（等同于，这个 IP 地址只能指定网卡上使用，同时，这个网卡，也能使用指定的 IP 地址）。

接口：如果绑定的 IP 地址属于局域网请选择“局域网”，如果将要绑定的 IP 属于广域网请选择“广域网”；

将 LAN 所有未绑定的设为唯一： 将局域网未绑定过的用户一键绑定为唯一类型；

将 LAN 口所有为绑定的设为静态：将局域网为绑定过的用户一键绑定为静态类型

唯一：指只有 IP 和 MAC 地址对应才能连接网络；

静态：将该 IP 地址指定为只能在该 MAC 地址上使用，但是该 MAC 地址还可使用其

他 IP 地址连接网络。

4.9.2 ARP 防御

设定 ARP 主动防御的相关参数。

防御“LAN 口伪网关攻击”：防御常用的 ARP 攻击软件！如果“网络执法官”、“P2P 终结者”、等 ARP 攻击软件，对其他电脑的网关攻击!是否存在攻击，将记录在“ARP 日志”。 默认时间间隔是 200ms；

探测 LAN 口非法网关：检查内网是否有 IP 和防火墙的 LAN 的 IP 相同，如果有，将记录在“ARP 日志”。 默认检测时间是 10s；

处理级别：ARP 防御系统智能防御系统的处理级别，级别越高，越安全。可以根据网络环境做相应调节。

4.9.3 ARP 日志

ARP 日志：当网络出现广播回路，ARP 绑定错误或者 ARP 攻击时，防火墙会在日志里面记录相关信息。

6	03-19 10:08:48	规则 禁止 禁止 协议TCP, 本地(192.168.1.100:24411) 远端(117.48.124.214:80)
7	03-19 10:08:48	规则 禁止 禁止 协议TCP, 本地(192.168.1.100:24438) 远端(180.97.33.108:443)
8	03-19 10:08:49	规则 禁止 禁止 协议TCP, 本地(192.168.1.100:24439) 远端(182.140.178.88:80)
9	03-19 10:08:49	规则 禁止 禁止 协议TCP, 本地(192.168.1.100:24440) 远端(14.18.245.167:80)
10	03-19 10:08:49	规则 禁止 禁止 协议TCP, 本地(192.168.1.100:24441) 远端(101.226.211.106:80 80)

五、 防病毒策略

5.1、 防病毒策略

针对 HTTP、FTP、POP3 和 SMTP 这四种常用协议进行杀毒，来保护经过设备数据的安全。 一般用于保护内网用户不被病毒入侵。

名称：设置防病毒策略的名称。

描述：设置策略的描述信息。

源区域：设置需要保护的源区域，如保护内网区域的所有用户不被感染病毒。

目的区域：设置源区域用户访问哪些目标区域地址时才进行病毒防御。

源 IP：设置需要防护的源 IP。只有从源区域进入的匹配源 IP 的数据，才匹配该策略。

目的 IP:设置需要防护的目的 IP。配置同源 IP。

协议的流量：设置需要进行病毒防御的应用类型，有 HTTP 杀毒、FTP 杀毒、邮件杀毒（POP3 收邮件/SMTP 发邮件）四种。

文件类型杀毒：设置用于杀毒的文件扩展名。仅适用于 HTTP 杀毒和 FTP 杀毒。

排除域名/IP：勾选“启用”复选框，启用排除域名/IP，可设置某些特殊网站的数据不需要杀毒，仅适用于 HTTP 杀毒。

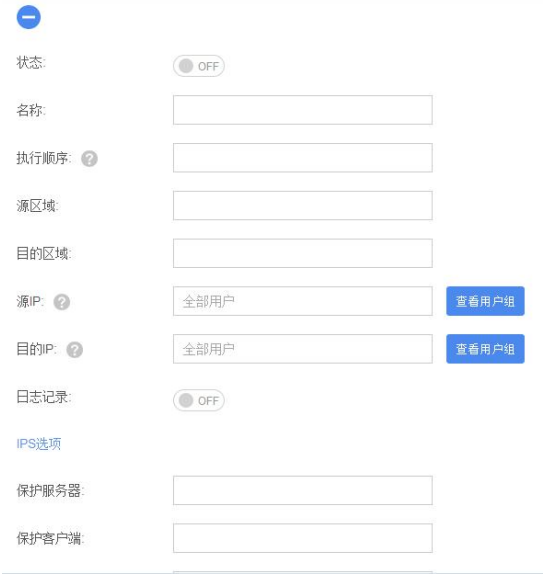
检测攻击后的动作：设置检测到带有病毒的数据时，设备处理的动作，有<日志记录>和<阻断>两种。

执行顺序：多条规则下，执行顺序越大的先执行

六、 IPS

6.1、 IPS

入侵防御系统（Intrusion Prevention System）依靠对数据包的检测来发现对内网系统的潜在威胁。IPS 将检查入网的数据包，确定这种数据包的真正用途，然后根据用户配置决定是否允许这种数据包进入目标区域网络。



状态：是否启用该条策略。

名称：设置 IPS 策略的名称。

执行顺序：多条规则下，执行顺序值越大的越优先执行

源区域：设置需要防护的源区域。保护客户端的源区域一般为内网区域，保护服务器的源区域一般为外网区域。

目的区域：设置访问的目标区域。保护客户端的目的区域一般为外网区域，保护服务器的目的区域一般为内网区域。

源 IP：设置需要防护的源 IP。只有从源区域进入的匹配源 IP 的数据，才匹配该策略。
目的 IP:设置需要防护的目的 IP。配置同源 IP。

日志:用于设置当发现保护的目标对象出 IPS 攻击后，是否记录到 IPS 日志中，勾选“启用”，则会记录 IPS 攻击包的攻击行为。可在系统日志中查看

- IPS 选项：设置需要保护的内容，包括保护客户端和保护服务器两部分。
  - 保护客户端：用于保护内网用户的网络安全。包括telnet、dns、shellcode、botnet、web-browse、system等漏洞攻击。点击<请选择客户端漏洞>后，可根据需要选择需要防护的漏洞。如下图：

  - 保护服务器：用于保护内网服务器的网络安全。包括ftp、worm、web、rpc等漏洞攻击。点击<请选择服务器漏洞>后，可根据需要选择需要防护的漏洞。如下图：

✧ **口令暴力破解防护：**用于保护内网服务器被暴力破解。包括FTP、IMAP、MYSQL、POP3/SMTP、SSH、TELNET等防口令破解。点击进入<请选择协议>后，弹出【选择防暴力破解的协议】编辑框，勾选相应的漏洞类型，设备对这种类型的暴力破解行为进行入侵防护。

✧ 恶意软件：用于保护内网受到后门软件、间谍软件、木马软件、蠕虫程序等攻击。包括Backdoor漏洞攻击、Spyware漏洞攻击、Trojan漏洞攻击、Worm漏洞攻击等。点击进入<请选择…>,弹出【选择恶意软件类型】编辑框，勾选相应的漏洞类型，则设备会对这种类型的客户端相关漏洞进行入侵防护。

检测攻击后的动作：用于设置当发现保护的目标对象出现 IPS 攻击后，该数据包是放行还是拒绝。若勾选“允许”，则放行该数据包；若勾选“拒绝”，则丢弃数据包。

七、 内容安全

7.1、 邮件管理

7.1.1 邮箱白名单

只需要开启监控功能，并填写监控者邮箱地址。系统即可开始监听内网所有基于客户端（foxmail、outlook 等）的邮件信息，在客户机发送邮件的同时，将自动复制相同的邮件内容发送至填写的邮箱。

监控状态：启用监控功能；

接收邮箱：填入的邮箱地址可以收到内网所有基于客户端的邮件信息；

对于白名单内的邮箱，将不会受到邮件监控功能的监管。（也就是白名单内的邮箱在发送邮件时，将不会抄送邮件至填写的接收邮箱）。

白名单状态：对该功能的控制开关，选择启用表示激活该功能；

描述：对该条规则的简单描述；

邮箱地址：增加该邮箱之后，对此邮箱不进行监控。

7.1.2 WEB 邮箱过滤

此功能即网址防火墙，默认添加了邮箱过滤功能，在此处添加的规则将会同步在网址防火墙里面显示出来，管控效果同理。

关闭：关闭访问控制功能，列表中的所有规则将都不生效

允许规则之外通过：列表中的规则按照控制的方式来执行，列表之外的规则不受控制，直接允许通过；

禁止规则之外通过：列表中的规则按照控制的方式来执行，列表之外的规则受到控制，禁止被通过。要单独设置允许通过的，请在规则中添加相应规则来允许其通过。

填出警告提示：选择开启，表示在打开被禁止的页面时，会弹出‘您访问的内容被管理员阻止’的警告提示；

状态：对规则的控制开关，选择启用表示激活该条规则；

描述：对该条规则的简单描述；

动作：规则的管控方式，该规则为允许通过还是禁止通过；

执行顺序：规则与规则之间的的执行优先等级，值越大的越被优先执行；

主机 IP 地址范围：需要管控的内部主机地址范围；

日志：对于匹配上的数据包，进行日志记录

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。

每周：一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。

7.1.3 WEB 邮箱白名单

添加到白名单里面的邮箱将不会受到网址防火墙（WEB 邮箱过滤）的限制。

描述：对该条规则的简单描述；

邮箱地址：填入需要排除限制的 WEB 邮箱地址。

7.2、 端口映射

7.2.1 端口映射

使外网可以通过 IP 地址或域名访问到内网机器映射出去的端口。

映射模式：映射模式有以下两种模式

模式 1：修改源 IP 为防火墙 LAN 口的 IP，可以做端口回流；

模式 2：不修改源 IP。

状态：对规则的控制开关，选择启用表示激活该条规则；

描述：对规则的简单描述；

状态：对规则的控制开关，选择启用表示激活该条规则；

描述：对规则的简单描述；

协议：分为 TCP、UDP、TCP 和 UDP；

源地址限制：限制只有处于填入的 IP 或者域名所在的网络才可以访问路由映射出去的端口。不填即表示所有广域网的 IP 都能访问到映射出去的端口；

外部端口：来自外部广域网的 IP 访问映射机器时的端口，可以自定义，但不能跟其他规则的端口相冲突；

内部端口：内部局域网络访问映射机器时使用的端口，一般由软件本身决定。若需要映射的内部端口跟外部端口一样，则可以不用填写内部端口；

内部主机地址：内网需要映射的机器 IP 地址；

广域网接口：选择需要映射的广域网接口，默认为所有接口 ALL。

举例：将内部机器 192.168.1.2 的 TCP-2000 端口映射为外网的 TCP-1000 端口，那么只需要按照上图这样设置就可以了。

内部机器访问 192.168.1.2 机器时使用 192.168.1.2:2000 这样的方式；外部广域网网络访问映射机器时就需要使用 WAN 口 IP:1000 这样的方式来访问映射机器了。

7.2.2 DMZ 设置

当将内部的某台机器 IP 填入到此 DMZ 选项时，防火墙 WAN 口的合法 IP 地址会直接对应给此台机器使用，也就是说从 WAN 端进来的封包，若是不属于内部的任何一台机器，都会传送到这台机器上（也就是把此机器完全的映射出去）。

启用 DMZ：选择开启即表示启用此功能；

目的地址：需要设为 DMZ 的内部机器 IP 地址；

源地址限制：该项为可选项，允许外部广域网口访问的地址或地址段。
允许输入—
"202.103.24.68","202.103.24.68-202.103.44.150","202.103.24.0/24"这三种格式。

7.2.3 UPNP 设置

UPnP(Universal Plug and Play)是微软 Microsoft 所制定的一项通讯协议标准，若使用的计算机支持 UPnP 机制且计算机 UPnP 功能为开启状态，可以将防火墙的 UPnP 功能启动。

开启 UPNP 之后，对 P2P 类的下载软件有一定加速作用，但同时对网络也会产生更大的负荷，过多的 P2P 下载将会影响到网络正常使用，请酌情使用此功能。

启用 UPNP：选择开启即表示启用此功能；

广域网接口：选择需要设置的网络接口；

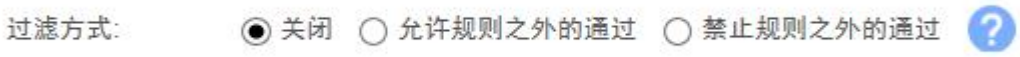
在网络中显示：选择开启之后需要自动映射端口的应用类型软件就会在列表中显示，便于管理员查看使用的软件类型。

7.3、 pingWAN 口

防火墙默认在外网是不可以 Ping 通 WAN 口的，如果需要在外网能够 Ping 通 WAN 口，请勾选此选项并提交设置。

7.4、 MAC 过滤

对 MAC 地址进行管理，允许或者禁止该 MAC 地址的用户通过。



MAC 地址过滤的方式：有‘不启用 MAC 地址过滤’、‘允许规则之外的通过’和‘禁止规则之外的通过’3 种选择，请根据需要来进行选择

不启用 MAC 地址过滤，对列表中添加的所有规则将不做任何控制；

允许规则之外的通过，列表中添加的规则按照控制方式来执行，列表之外的不受限制，直接通过；

禁止规则之外的通过，列表之中的规则按照控制方式来执行，列表之外的所有地址将都被禁止通过。

状态：选择是否激活此规则；

描述：对此规则的简单描述。默认值为 defaul，建议修改为方便识别的内容；

控制方式：分为‘允许’和‘阻止’两类。用户可以选择此规则是否允许通过；

MAC 地址：填入需要管控的 MAC 地址。格式为：00:0A:0B:0C:0D:0E；

基于时间控制：是否启动按时间段管控功能（若启用，用户可自定义管控时间段）。

7.5、 域名管理

主要是对域名解析、过滤、重定向。

7.5.1 域名解析

域名特殊解析主要是用来将一些特定的域名绑定到指定的线路上去解析。如图所示:

DNS 域名：需要绑定到线路上的域名或者域名关键字；

出口选择：选择一个广域网的接口用来解析指定的域名。

7.5.2 域名过滤

域名过滤主要是用于对一些域名或者域名关键字进行阻止。

DNS 过滤方式：包含不启用、允许规则之外的通过和禁止规则之外的通过三种方式

不启用：就是对列表中的规则不做任何控制，规则不会生效；

允许规则之外的通过：列表之外的规则允许通过，列表之中的规则受规则控制；

禁止规则之外的通过：规则之外的所有都不允许通过，规则之内的受规则管控。

DNS 域名：添加所需过滤的域名或者域名关键字。

7.5.3 域名重定向

DNS 域名：填入被转向的域名。不支持通配符 *；

重定向到：填入需要转向到的一个域名或者 IP。（此域名必须是服务器解析之后只有单一地址的。像 www.qq.com 解析出来就有多个 IP，这样的就不行。）

7.6、 URL 重定向

8.12.1 URL 重定向

URL 重定向是对域名重定向功能的补充跟完善，一些用域名重定向无法转向的域名，通过 URL 重定向就可以实现。

状态：选择是否激活应用此规则。

描述：对该条规则的简单描述。

URL 的主机名称：填入需要被转向的域名地址。

目录网页（URL）：填入被转向域名的目录网页，若没有，则可不填

网页的参数：填入被转向域名的网页参数，若没有，则可以不填

重定向到：需要被转向到的域名地址。

主机 IP 地址范围：内部需要被重定向的主机 IP 地址。

日志：是否需要在日志中显示记录。

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。

每周：一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。

8.12.2 URL 日志

记录 URL 重定向成功之后的日志。

八、 VPN 管理

8.1、 PPTP 配置

8.1.1 PPTP 服务

用于管理 PPTP 的 VPN 服务及借线相关。

状态：默认为关闭状态，开启状态后可配置 PPTP 相关参数；

PPTP 服务：控制 PPTP 服务端功能的开启与关闭。做服务端来使用的时候必须先开启服务，做客户端使用的时候不用开启；

端口：PPTP 连接默认使用的端口，尽量不用去修改，否则可能造成 PPTP 连接失败；

地址范围：服务端分配给客户端的 IP 地址范围。此 IP 是连接 VPN 时的虚拟 IP，请不要将此 IP 与路由上的其他 IP 设置在同样的网段内，否则会造成 IP 冲突，引起网络故障。因 VPN 连接之后会从中分配一个 IP 作为 VPN 网关地址，所以，此地址范围请设置至少 2 个以上的 IP 范围；

分配给客户的 DNS：服务端分配给客户端的 DNS 地址。只有在用到借线或者客户端需要连接到服务端进行上网时才需要用到 DNS，此处应该设置服务端网络的 DNS 地址。

8.1.2 PPTP 用户

管理 PPTP 的帐号，包括帐号的创建、修改与删除以及帐号类型的设置。

用户状态：勾选上表示禁用此账号；

用户名：PPTP 客户端创建的账号。可以由英文字母或数字组成；

密码：PPTP 客户端设定的密码。可以由英文字母或数字组成；

指定 IP：如果不使用用服务端自动分配的 IP，就可以在此处手动指定一个 IP，且指定的 IP 必须与 VPN 服务端分配的 IP 处于同一个网段内；

类型：有‘VPN 隧道’和‘VPN 借线’两种模式可以选择

VPN 隧道：用来连接服务端，与服务端的网络组建一个虚拟的局域网环境，可以共享服务端内部资源；

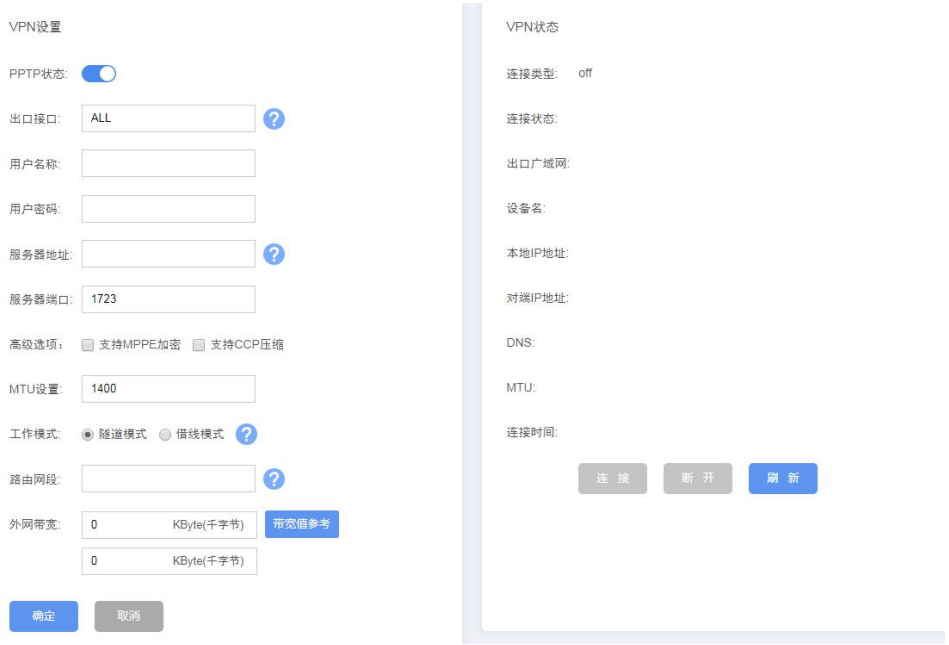
VPN 借线：借用服务端的线路出口作为网络接口来上网，共享服务端的网络出口。

客户端内网网段：仅隧道模式有用。填入连接 VPN 的客户端的内网网段地址，格式：192.168.1.0/24 。例如：客户端使用的网段是 192.168.10.X，那么就应该填入:192.168.10.0/24；

备注：对添加的用户账户的简单信息描述，由用户自定义。

8.1.3 PPTP 客户端

PPTP 用户状态可在此菜单由 VPN 设置和 VPN 状态组成。



VPN 设置：使用防火墙作为 VPN 客户端的时候需要用到 VPN 借线功能，可以实现路由对路由的 VPN 连接或者 VPN 借线功能。

PPTP 状态：开启即为打开客户端；

出口接口：选择路由使用的 VPN 接口，防火墙的型号不同，支持连接 VPN 网络的条数也不同，默认使用 VPN1 接口；

连接类型：选择 PPTP 表示启用 VPN 客户端功能，默认是关闭状态；

出口接口：可以选择用哪个广域网作为 VPN 的出口，请尽量选择带宽大且稳定的线路做出口，以保证 VPN 连接的稳定性。默认是 ALL（表示全部）；

用户名称/密码：填入 VPN 服务端创建的 PPTP 用户名及密码；

服务器地址：VPN 服务端的广域网接口 IP 地址或者动态域名；

服务器端口：填写服务器端口，默认为 1723；

MTU 设置：VPN 连接所使用的 MTU 值，默认是 1400。此值一般不做改动，使用默认值即可。

工作模式：有隧道模式与借线模式两种。默认是隧道模式

隧道模式下，路由只作为 VPN 连接使用，可以共享虚拟网段的内部资源，但不能访问服务端的外部资源（也就是不能使用借线功能）；

借线模式下，防火墙客户端可以借用服务端的网络，通过服务端的网络来访问外部资源，但不能访问服务端内部资源。

路由网段：只有在选择隧道模式时此项才生效。此处填写服务端所在的网段（比如，服务器为 192.168.2.X 段的 IP，那么此处就填 192.168.2.0/24）；

外网带宽：设置 VPN 线路所占用服务端的带宽值。0 表示不设置，即不限制 VPN 接口的带宽。VPN 接口的出口带宽仍需占用客户端实际的网络带宽资源，能使用的最大带宽取决于客户端的网络出口带宽值大小。

带宽参考值：可选择一个参考的带宽来自动填入上下行带宽值。

VPN 状态：用于查看 VPN 客户端与 VPN 服务端之间的 VPN 连接状态。只有当路由作为客户端并与服务端连接以后，才会显示连接状态。

8.2、 IPSec 配置

8.2.1 IPSec 网对网

用于管理 IPSec 网对网服务的建立与连接，如果需要使用此功能，需要连接的两边防火墙都开启 IPSec 功能。

IPSec 网对网配置：开启/关闭 IPSec 网对网配置；

名称：填写此规则的名称，由英文字母或数字组成；

IPSec 网对网主动连接：启用 IPSec 网对网的主动连接；

本地隧道接口：选择使用哪个广域网口来进行隧道连接；

模式：默认为主动模式，如果无法连接，则可以使用野蛮模式；

本地网络：填写本地的内网的网段。（比如，本地网络现在是 192.168.2.X 段的 IP，那么这里就填 192.168.2.0）；

远程隧道地址：填写对端的防火墙的广域网 IP 地址或者动态域名；

远程网络：填写对端防火墙的内网网段；

IKE 验证模式：默认的加密类型；

PSK 密钥：设置密钥的密码。由数字和字母组成。连接隧道的两边防火墙必须设置相同的密钥，否则连接不会成功；

IPSec 高级配置：显示 IPSec 服务的参数配置。

8.2.2 IPSec 点对网

IPSec 点对网服务：启用或关闭 IPSec 点对网服务；

本地网络：填写本地内网的网段。（比如，本地网络现在是 192.168.1.X 段的 IP，那么这里就填 192.168.1.0）；

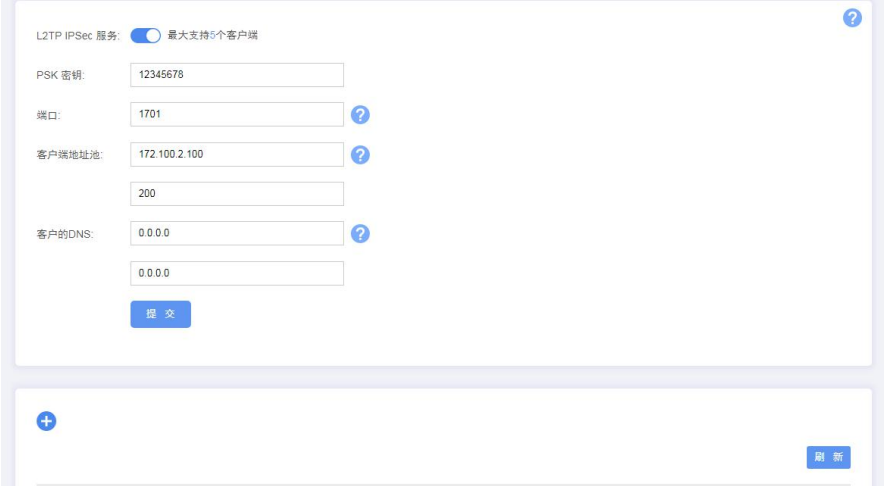
IKE 验证模式：默认加密类型；

PSK 密钥：设置密钥的密码。由数字和字母组成。客户端在连接时，必须输入与此相同的密钥。

高级参数：显示 IPSec 服务的参数配置。

IPSec 点对网客户端连接需要使用到专门的 VPN 连接软件，推荐使用 ”vpn-client-2.1.7-release.exe“。

8.2.3 L2TP IPSec



L2TP IPSec 服务：开启或者关闭 L2TP IPSec 服务；

PSK 密钥：设置密钥的密码。由数字和字母组成，L2TP 客户端连接时需要填入与此相同的密钥；

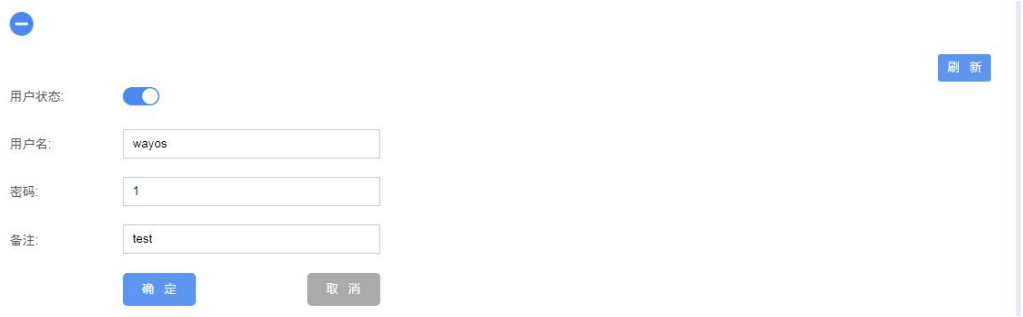
端口：L2TP IPSec 服务的端口默认为 1701。L2TP 连接默认使用的端口尽量不做修改，否则可能造成 PPTP 连接失败；

客户端地址池：服务端分配给客户端的 IP 地址范围。此 IP 是连接 L2TP 时的虚拟 IP，请不要将此 IP 与路由上的其他 IP 设置在同样的网段内，否则会造成 IP 冲突，引起网络故障；

客户的 DNS：服务端分配给客户端的 DNS 地址。只有用于借线或客户端需要连接到服务端进行上网时才需要用到 DNS，此处应该设置服务端网络的 DNS 地址。

L2TP 客户端连接 VPN 时，需要使用系统自带的虚拟专用网络来创建 L2TP 连接。

下方的添加按钮为 L2TP IPSec 用户创建按钮。用于创建 L2TP 客户端连接 VPN 时拨号的用户。



用户状态：是否禁用此账号；

用户名/密码：创建 L2TP 连接使用的账号及密码。可以由英文字母或数字组成；

备注：对添加的用户账户的简单信息描述，由用户自定义。

8.3、 OVPN 配置

8.3.1 OVPN 设置

状态：OVPN 默认为关闭状态；

OVPN 模式：分为三种模式

关闭：不启用 VPN 服务；

服务端：将此路由作为 OVPN 连接的服务器端；

客户端：将此路由作为 OVPN 客户端；

防火墙的 VPN 连接方式分为路由与路由的连接和路由对 PC 机的连接两种：

路由对路由:即网关对网关的连接方式。也就是将其中一端的路由设置为服务端，另一端路的由设置为客户端。在这种连接模式下，两端的路由若外网连接都正常，两者将会

自动进行 VPN 连接，VPN 连接成功之后，服务端下面的所有用户与客户端下面的所有用户就组成了一个虚拟的局域网；

路由对 PC 客户机：即路由对客户机的连接方式。就是把防火墙作为 OVPN 服务端，然后客户机利用 OVPN 连接软件来与服务端进行连接。在这种连接模式下，客户机必须利用 OVPN 软件手动去连接服务端，VPN 连接成功之后，该客户机就与服务端下面的所有用户组成了一个虚拟的局域网，即加入到服务端的局域网内。

VPN 服务端是提供给客户端做 VPN 连接而用，我们需要在服务端上建立不同的用户，分配给客户端用来连接 VPN。其中分为 PC 客户端的用户建立与防火墙客户端的账号建立两种。

OVPN 模式中选择‘服务端’，如下图所示：

协议类型：自定义 OVPN 服务所走的协议。默认为 TCP 协议；

超时检测时间：在设定的时间内，未收到客户端的数据，则判断为连接超时；

MTU 设置：定义 VPN 传送数据的 MTU 值，用于特殊环境中使用，一般保持默认即可；

端口：自定义一个 OVPN 服务使用的端口。默认为 4443，可以修改为其他未被占用的端口；

OVPN 虚拟网段地址/掩码：自定义一个用来连接 VPN 的虚拟网段地址及子网掩码。（请避开正在使用的网段。如正在使用的是 192.168.X.X，请使用 10.X 或者 172.X 的 IP 段）；

用户之间互通：即 VPN 客户端与 VPN 客户端之间相互通信的功能。默认允许。

在防火墙 OVPN 设置中选择客户端可以使用路由作为客户端来连接 OVPN，其设置方法较简单，只需要填写几项关键参数就即可，如图所示：

协议类型：选择 VPN 连接所使用的协议类型，必须与服务端的协议类型一致，否则无法正常连接 VPN。

超时检测时间：在设定的时间内，未收到客户端的数据，则判断为连接超时。

MTU 设置：VPN 连接的 MTU 值大小，可由用户自定义，一般使用默认值即可。

用户名/密码：请填入在服务端建立的路由客户端用户名及密码，并再次确认密码。

服务器地址：填写服务端的 WAN 口 IP（外网 IP）地址或者动态域名。冒号后面填入与服务端相同的协议端口号。

下方添加按钮为添加 OVPN 用户。

状态：启用/禁用此账号；

用户类型：请根据用户类型来建立相应的帐号；

客户端是 PC：建立的帐号只能用于 PC 电脑作为客户端使用 OVPN 客户端软件来连接 VPN 时使用。

客户端是防火墙：建立的帐号只能用于防火墙作为客户端时连接 VPN 使用。

用户名/密码：新建一个客户端用来连接 VPN 的账号及密码。（此账号是客户端路由用来连接服务端而使用的，用户账号可以由用户自行定义，请使用英文或者数字作为用户名/密码）；

内部网段地址/掩码：此项仅对客户端是防火墙时适用 。填入客户端连接 VPN 所用的内部 IP 地址及子网掩码。(此处 IP 不能与服务端内网处于同一网段。如，服务端路由 IP 为 192.168.1.X 段，客户端路由 IP 为 192.168.100.X 段，那么此处就需要填 192.168.100.0）。

8.3.2 OVPN 证书

主要用于用户下载原有的证书文件，或者自行导入新的证书。其中，ca.crt 证书文件是 PC 客户端连接 VPN 必须的文件，可将其下载下来保存好，以提供给 PC 客户端连接 VPN 时使用。

鉴于稳定性，建议用户使用默认的证书，以免使用自行导入的证书时出现问题。若需自定导入的证书在使用时出现问题，请点击右上方按钮将证书恢复到默认值。

8.3.3 OVPN 日志

主要用于记录 OVPN 连接时出现的日志信息。

九、 AC 服务

9.1、 AC 服务

AC 平台服务端用于管理维盟内网中的 AP，可对 AP 连接状态等查看，也可对在线 AP 进行参数配置下发。

状态：开启状态并比较后，AC 服务端开启；

主路模式：防火墙作为网关和 AC 管理器。

旁路模式：若防火墙只做为 AC 管理器接入内网，即需要使用此功能；同时需要填写好相应的 IP、网关、DNS；

LAN 口 IP：填入开启旁路模式后设定的 LAN 口 IP；

默认网关：填入开启旁路模式后设定的默认网关地址；

DNS：填入开启旁路模式后设定的 DNS，格式为用空格分隔，如：8.8.8.8 8.8.4.4；

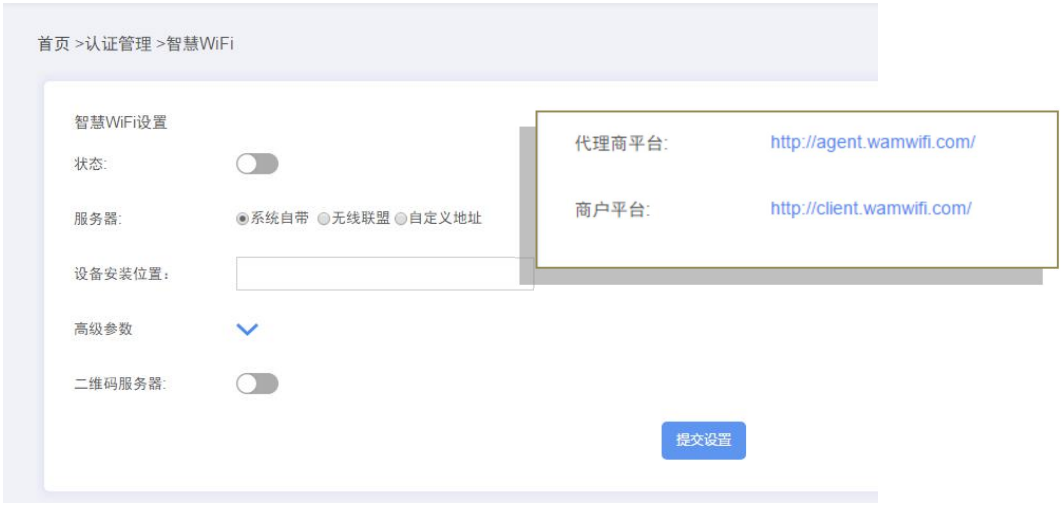
注意：开启旁路模式之前，请先将所有广域网口的接入类型设置为关闭状态，同时关闭 DHCP 服务器，修改 LAN 口 IP 地址。

申请控制：AC 状态开启状态下，申请控制按钮才会显示出来；该状态默认为关闭，如需申请 AC 远程控制，请手动点击“申请控制”。

十、 认证管理

10.1、 智慧 WiFi

一种云端认证的模式，云端提供多种认证方式，例如：微信关注公众号认证、短信验证码认证、用户名认证、打赏认证、开放认证等。如下图：



服务器：可选择不同的智慧 WiFi 服务器

系统自带：标准智慧 WiFi 服务器；

无线联盟：带 WiFi 变现功能的智慧 WiFi 服务器；

自定义地址：可联系维盟市场部申请协助架设独属于自己的智慧 WiFi 服务器。

设备安装位置：用于备注该设备安装在哪里，方便以后查询，该信息会上传到智慧 WiFi 服务器；

二维码服务器：内置一个二维码服务器，用于终端用户扫码上网。一般用于网吧类公共场所，方便终端用户的移动终端扫码连接 WiFi；

增值开关：当智慧 WiFi 连接的是无线联盟服务器时，开启该功能可以实现微信吸粉功能；

允许蹭网：开启后，终端不用输入验证信息也可以正常连接互联网；

工作接口：对防火墙哪个接口下面的用户生效；

超级验证码：该验证码对所有终端生效；

登录次数：一个账号允许同时登录的次数；

SSID：二维码服务器指定的无线信号；

认证完成跳转页面：终端经过认证后跳转的页面地址；

客户端名称：显示在终端电脑上的客户端名称；

温馨提示内容：客户端提示区域的内容；

技术支持内容：客户端技术支持区域的显示内容。

10.2、 认证配置

该功能是本地认证方式参数配置。即认证全部都有防火墙来完成，不依靠第三方服务器。如下图所示：

允许上网的方式： 选择允许用户上网的认证方式

ARP 绑定用户直接上网：IP 与 MAC 地址进行绑定过的用户可以直接上网；

PPPoE 用户直接上网：利用 PPPOE 协议拨号到防火墙端的用户验证通过之后才可以上网；

用户账号到期提前通知：账号到期之前提醒用户的通知时间。默认为提醒时间内每天第

一次开启网页时出现，直到账号到期（或者延长期限）为止；

用户帐号到期查询间隔：此功能用于检测帐号到期但仍持续在线的用户，在帐号到期以后，达到设置的时间之后，在线用户将被强制踢下线，避免了因为到期用户长期不下线导致的带宽资源浪费。此值可以尽量设置大一点，效果更佳。

不需要认证的内部主机(基于 IP)：所添加的 IP 用户将不受任何一种认证方式的管制，可以直接上网，即认证排除的内网 IP；

不需要认证的内部主机（基于 MAC）：所添加的终端 MAC 将不受任何认证方式的管制，可以直接上网，即认证排除的内网 MAC；

允许访问的外网范围(基于 IP)：没有进行认证的用户也能访问的外网 IP 地址范围；

允许访问的外网范围(基于域名)：没有进行认证的用户也能访问的外网域名；

会话存活超时时间：当检测到用户处于非活跃状态时，超过设定的最大时间时，强制用户下线并需要重新认证；

MAC 自动认证老化时间：用户认证离线后，在设定的老化时间范围内再次上线时将免认证，否则需要重新认证；

接口免认证：从所选接口接入的终端用户可以免认证上网；

包时用户定时重设时长：对包时用户，可以在指定的时间点重置用户的上网可用时长；

导入认证例外信息：当有比较多的终端用户信息需要加入到认证白名单时，可事先在文本文档中编辑好，一次性导入。编辑时，请点击‘导出认证例外信息’，下载一个标准格式文件，按照其中的格式进行填写。

10.3、 跨三层识别

跨三层 MAC 识别，该功能支持 SNMP 协议，开启便可以管理三层下的设备，主要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。

状态：开启/关闭，是否开启该功能。

SNMP 服务器 IP：服务器 IP 填三层设备地址

读团体字：保持和三层设置一样即可

连接状态：查看和三层设备是否连接成功，如果连接无问题，会显示连接成功！

注意：如果需要使用此功能，需要三层交换机也支持该协议。

10.4、 页面管理

认证页面管理用于对认证用户或者未经认证的用户所弹出的提示页面进行管理，该通告内容允许用户自定义其中的内容或者替换新的通告文件。需要修改通告内容时，可自行编辑好文件内容再上传，文件内容不能大于 8KB。

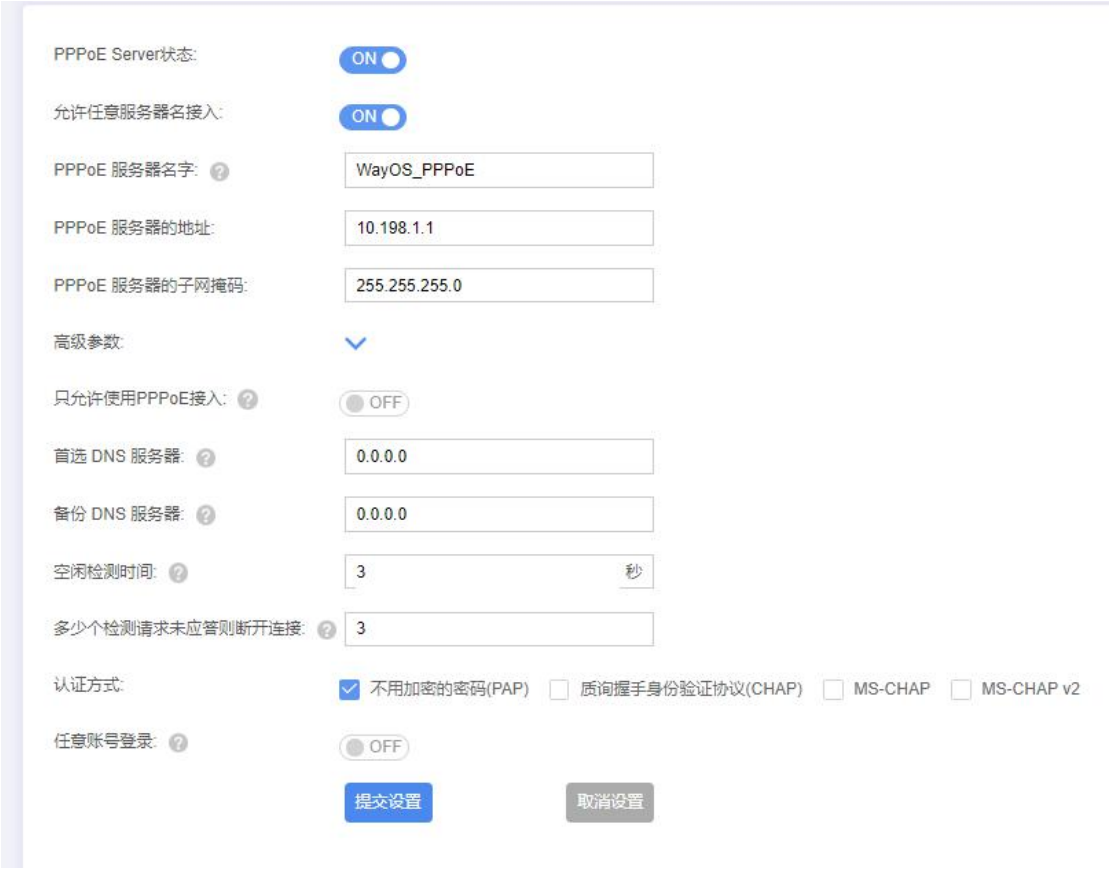
账户到期提前通知页面：认证用户帐号到期之前的通知提醒页面，用户帐号快到期时，终端用户访问 HTTP 类数据时会自动弹出此通告内容；

阻止上网通告：在开启了 arp 认证或者 pppoe 认证，没有认证的用户将会收到此通告文件的提醒；

上网到期的通告页面：当计时类认证用户到期后，再访问网络资源时，会自动弹出页面提示用户网络服务器到期提醒。

10.5、 PPPoE 设置

提供对 PPPOE 拨号服务端的参数设置。



PPPoE Server 状态：是否启用 PPPoE 拨号服务端功能。默认为启用状态，若关闭了此功能，客户机将无法通过 PPPoE 拨号到防火墙；

允许任意服务器名接入： 开启该功能将会不验证客户端在拨号时填入的服务器名称，否则需要验证服务器名称和账号密码；

PPPoE 服务器名字：拨号服务器的名称，用户可以自定义更改；

PPPoE 服务器的地址：即 PPPoE 拨号用户的网关地址；（PPPoE 用户可以通过此地址来访问防火墙配置页面）

PPPoE 服务器的子网掩码：即 PPPoE 服务器的掩码地址，可以根据环境需求来修改此地址；

只允许使用 PPPoE 接入：激活之后将只有通过 PPPoE 拨号的用户才能访问到防火墙跟上网；（且只能使用下方的‘PPPoE 服务器地址’才能访问防火墙 WEB 界面，若使用 LAN 口 IP 将无法访问到防火墙 WEB 界面）

首选 DNS 服务器：PPPOE 服务器分配给客户机的 DNS 服务器地址；

备份 DNS 服务器：PPPOE 服务器分配给客户机的 DNS 服务器地址；

空闲检测时间：在达到设定的时间之后，若客户机与服务器之间还没有数据通信，则开

始检测客户端是否掉线。默认值为 3 秒；

多少个检测请求未应答则断开连接： 在设定的请求个数之后，客户机若无数据通信应答，则断开其连接。默认值为 3 个；

认证方式：对于不同应用环境，可以采取不同的认证方式类型。对于一般 PC 电脑，都是采用的 PAP 模式。如果是采用下级路由进行拨号，可以把所有的认证方式都勾选上；

任意账号登录：开启后，服务器将不再准确验证终端的拨号账号信息，用户随意输入都可以通过认证。

10.6、 PPPoE 扩展设置

可以添加多个 PPPOE 地址池，一般用来区分不同类型的用户，方便对不同类型的用户进行带宽限制或者访问限制等操作。

组名：分组的描述，根据方便识别的填写即可。

扩展 PPPOE 服务器的 IP 地址：为 IP 地址，格式：10.198.1.1 不要和防火墙中任何其它地方的 IP 地址冲突。

扩展 PPPOE 服务器的子网掩码：一般默认即可，如果使用该地址池的用户超过 254 个，可修改子网掩码。修改时，如果有不清楚的，请联系技术人员协助。

DNS 服务器：分配给终端用户的 DNS 服务器地址。

速度限制：对使用该组地址池的用户进行单独限制。

10.7、 用户管理

针对 PPPoE 用户进行账号的添加、修改或删除的操作，如用户账号的建立、到期时间、

MAC 地址的绑定、备注信息等设置。

定时删除未锁定的用户：开启后，在指定的时间自动删除状态为未锁定的账号。一般用于临时账号比较多的环境；

用户状态：选择禁用即表示禁用此用户，禁用后此用户将不能进行拨号上网（用户当前连接断开以后才生效）；

用户名/密码：为用户创建一个登录用户名及密码；

PPPOE 扩展组：为该账号选择一个 IP 地址分配组，便于后面做行为规则管理；

MAC 地址：有不绑定、自动绑定、手动绑定 3 种形式可供选择；

到期：可以对用户的上网期限进行限定。有按日期、包时、包流量；

允许登录的用户数：设定该账号可以允许被多少个用户同时登录使用,即一号多拨功能；（当允许登录的用户数设置大于 1 时，绑定的 MAC 地址将只会对第一个拨号的用户有效）

IP 地址：用于手动给用户指定 IP 地址。pppoe 用户手动绑定的 IP 为 pppoe 拨号服务器 IP,WEB 认证可以选择自动绑定 IP 和手动绑定 IP。WEB 认证的 IP 为局域网自动获取或者手动填写的 IP；

上传/下载速度：对该帐号的带宽使用做以限制，只允许使用指定的带宽速度值。默认为 0，表示不做限制；

速度控制方式：可以选择单独限制或者共享限制

单独限制：对帐号做单独限制，用户使用的最大速度不超多限制的速度值；

共享限制：对一号多拨的用户有效，可以限制一个帐号在多人共享使用时，多人共享限制的速度值。

姓名：选填内容，用于条件查询；

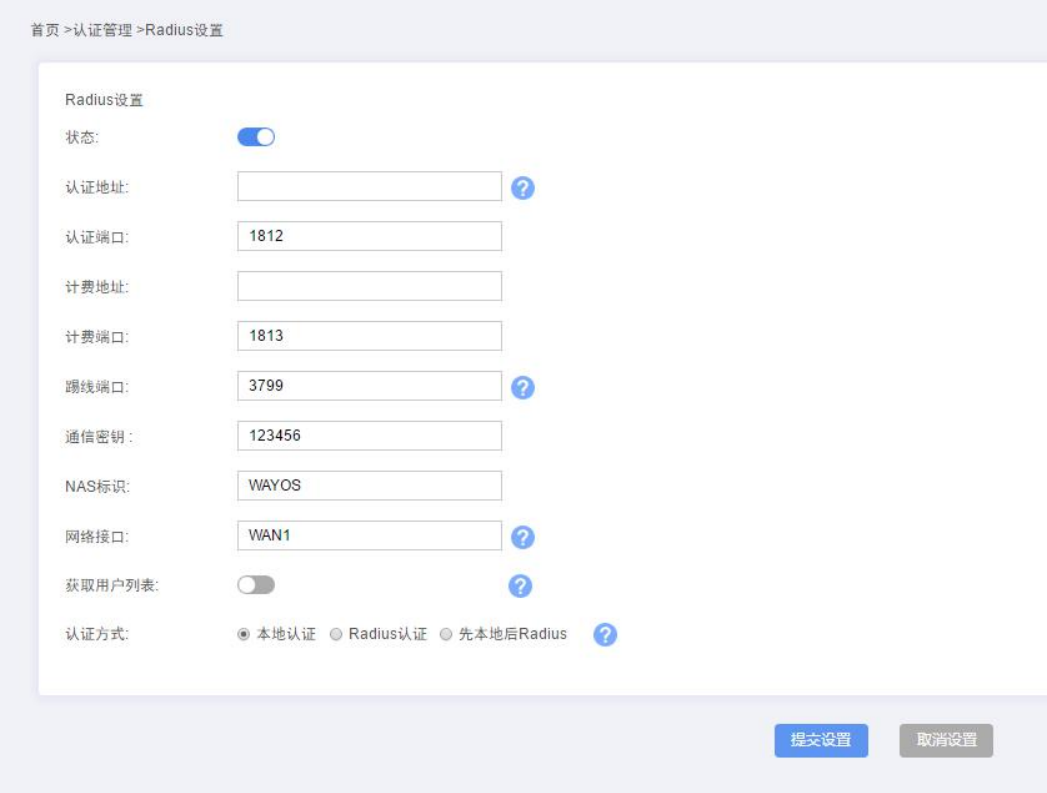
电话：选填内容，用于条件查询；

身份证：选填内容，用于条件查询；

备注：选填内容，用于条件查询。

10.8、 Radius 服务器

该功能为标准协议的 radius 协议，可对接市面上的标准 radius 服务器，用来做认证计费使用。



认证地址：可访问到的 radius 认证服务器 IP 地址；

认证端口：服务器上开放的是什么认证端口就填对应的端口，与服务器保持一致；

计费地址：可访问到的 radius 计费服务器 IP 地址；

计费端口：服务器上开放的是什么计费端口就填对应的端口，与服务器保持一致；

踢线端口：服务器上开放的是什么踢线端口就填对应的端口，与服务器保持一致；

通信密钥：与服务器的通信密钥保持一致；

NAS 标识：填写目标服务器的标识；

网络接口：radius 数据从哪个接口出去；

获取用户列表：开启后将从 radius 服务器获取用户列表信息，注意这里仅支持 PAP 加密方式；

认证方式：选择终端用户的认证方式顺序。

10.9、 云计费

开启后，可对接维盟专用的云计费平台。可实现对内网用户的开户、计费、用户自注册等操作。

没有账号，可点击‘没有账号？立即注册’进行注册。

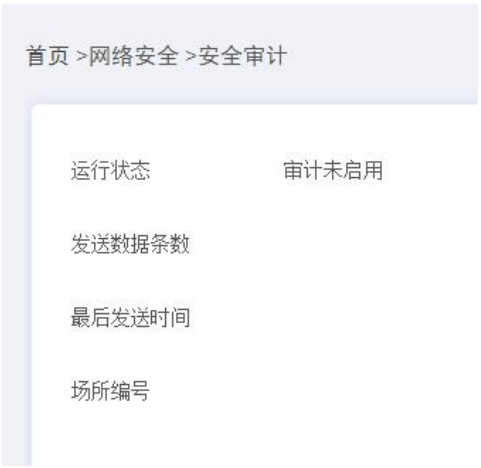
设备密钥默认和注册时的密码一致，建议在平台上修改为和密码不一致。

设备组名：将由服务器下发。

十一、 安全审计

11.1、 安全审计

与审计平台相对接，查看是否对接成功。符合公安关于网络安全第 82 号令的审计要求。



十二、 应用控制

12.1、 行为识别

用于对指定范围的内部主机进行应用协议上的管控，允许或者禁止指定协议的通过。

行为控制的方式：分别有关闭、允许规则之外的通过、禁止规则之外的通过三种状态

关闭：该功能不生效；

允许规则之外的通过：除了下面规则中的不能进行，其他不在规则中的用户是可以正常进行；

禁止规则之外的通过：允许下面规则中的用户进行，不在规则中的用户不能进行。

状态：对规则的控制开关，选择启用表示激活该条规则；

描述：对该条规则的简单描述；

控制方式：允许和禁止。对该条规则的控制方式，选择允许或者禁此规则的协议通过；

执行顺序：规则与规则之间的的执行优先等级，值越大的越被优先执行；

主机 IP 地址范围：填入需要管控的内部主机地址范围；

应用协议：选择需要管控的协议类型；

自定义 ip 协议：可以自行定义远端 IP、域名及端口协议，并以此作为管控对象；

日志：对于匹配上的数据包，进行日志记录；

基于时间控制：是否启动按时间段管控功能。若启用，规则将只会在自定义的管控时间段内生效；默认不启用，表示所有时间段都生效。

每周：：一周的哪几天生效；

每天：一天的哪些时段生效。

12.2、 行为管理日志

用于记录行为识别、高级管理中的规则记录，如果开启了对应的日志功能，将会在此日志里显示出来。

12.3、 网址防火墙

网址过滤功能可以自定义设置规则用来控制用户对网页的访问，如下图所示：

网址过滤方式：有不启用、允许规则之外的通过和禁止规则之外的通过三种方式

不启用：就是对列表中的规则不做任何控制，规则不会生效；

允许规则之外的通过：列表之外的规则允许通过，列表之中的规则受规则控制；

禁止规则之外的通过：规则之外的所有都不允许通过，规则之内的受规则管控。

弹出警告提示：选择开启，表示在打开被禁止的页面时，会弹出‘您访问的内容被管理员阻止’的警告提示；

状态：是否启用该规则；

描述：对规则的一个描述；

动作：该规则为允许通过还是禁止通过；

执行顺序：规则的执行优先等级；

主机 IP 地址范围：所受限制的 IP；

网站地址组：选择需要控制的网址分类组；

日志：是否在日志中记录该规则的发生情况；

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。

每周：一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。

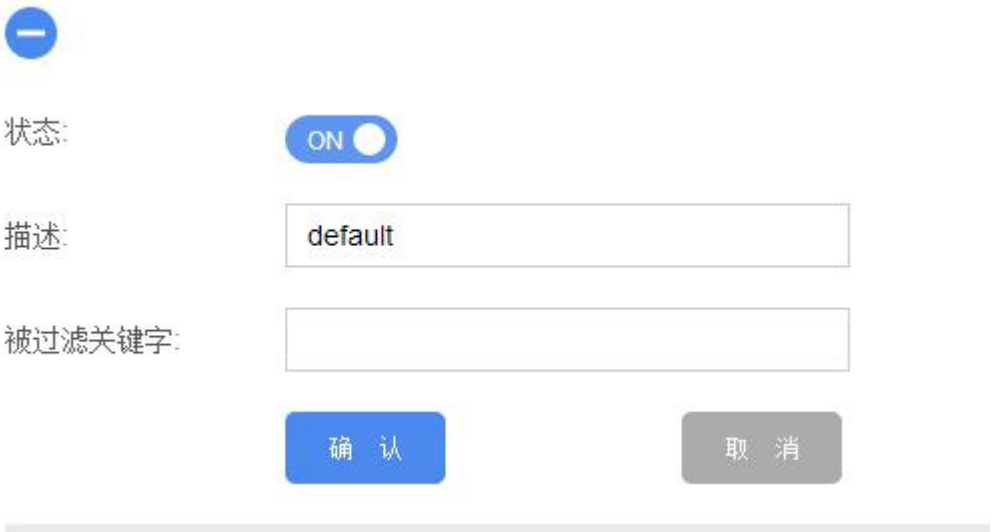
12.4、 关键字过滤

屏蔽敏感字符，只对非 HTTPS 网页生效。

控制状态：选择是否启用关键字过滤功能；

日志：是否记录规则执行产生的日志；

弹出警告提示：选择开启，表示在访问被过滤的关键字时，会弹出“您访问的内容被管理员阻止”的警告提示；



状态：对规则的控制开关，选择启用表示激活该条规则；

描述：给该规则命名备注，便于识别；

被过滤关键字：要禁止搜索的关键字，支持中文、英文跟数字字符。

如果在搜索引擎搜索了已经被进制的关键字，那么路由器将会弹出阻止的提示通告。

12.5、 禁止 web 提交

该功能是禁止/允许客户机向网络上的服务器的上传行为，比如邮件中的上传附件等。

控制状态：分别有关闭、允许规则之外的通过、禁止规则之外的通过三种状态

关闭：该功能不生效；

允许规则之外的通过：除了下面规则中的不能进行 web 提交外，其他不在规则中的用户是可以正常进行 web 提交行为；

禁止规则之外的通过：允许下面规则中的用户进行 web 提交，不在规则中的用户不能进行 web 提交行为。

状态：开启使该规则生效；

描述：给该规则命名的备注信息，便于识别规则；

主机 IP 地址范围：表示该规则中对内网哪些用户生效；

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。

每周：一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。

12.6、 文件传输过滤

该功能是禁止/允许客户机访问网络上带有规则中指定的后缀名的文件。

控制状态：分别有关闭、允许规则之外的通过、禁止规则之外的通过三种状态

关闭：不启用该功能；

允许规则之外的通过：除了下面规则中的不能进行 web 提交外，其他不在规则中的用户是可以正常进行 web 提交行为；

禁止规则之外的通过：允许下面规则中的用户进行 web 提交，不在规则中的用户不能进行 web 提交行为。

弹出警告提示：选择开启，表示在访问过滤的后缀名时，会弹出‘您访问的内容被管理员阻止’的警告提示；

状态：开启使该规则生效；

描述：给该规则命名的备注，便于识别；

主机 IP 地址范围：填入需要掌控的 IP；

后缀名：勾上即表示该规则对勾上的后缀名生效。

手动输入后缀名：路由器中提供的后缀名没有需要的后缀名，可以在这里手动填上，当添加多个后缀名的时候，用‘，’（逗号是英文半角输入法下的符号）分开。

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。

每周：一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。

12.7、 聊天软件管理

此功能用于对 QQ、淘宝旺旺、飞信、MSN 这几个聊天软件的封锁限制。

QQ 黑白名单

过滤方式：有关闭、允许如下号码，禁止其它、阻止如下号码，允许其它三种状态

关闭:不启用该功能；

允许如下号码，禁止其它:允许列表内添加的号码使用，禁止其他的号码使用；

阻止如下号码，允许其它:禁止列表内的号码使用，允许其它号码使用。

描述：对该条规则的简单描述；

号码：填入需要管控的 QQ 号码；

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。

每周：一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。淘宝旺旺黑白名单

过滤方式：分为关闭、允许如下号码，禁止其它、阻止如下号码，允许其他三种状态

关闭:不启用该功能；

允许如下号码，禁止其他:允许列表内添加的号码使用，禁止其他的号码使用；

阻止如下号码，允许其他:禁止列表内的号码使用，允许其它号码使用。

描述：对该条规则的简单描述；

号码：填入需要管控的淘宝旺旺号码；

基于时间控制:如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。

每周：一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。移动 QQ 黑白名单

过滤方式：分为关闭、允许如下号码，禁止其它、阻止如下号码，允许其他三种状态

关闭:不启用该功能；

允许如下号码，禁止其他:允许列表内添加的号码使用，禁止其他的号码使用；

阻止如下号码，允许其他:禁止列表内的号码使用，允许其它号码使用。

描述：对该条规则的简单描述；

号码：填入需要管控的移动 QQ 号码；

基于时间控制:如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。

每周：一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。

十三、 智能流控

智能流控主要对网络带宽使用进行管理，以保证网络带宽使用达到最佳效果。

13.1、 优先级设置

用于控制路由数据、用户数据的处理优先级别。

状态：对规则的控制开关，选择启用表示激活该条规则；

描述：对该条规则的简单信息描述；

执行顺序：规则与规则之间的执行顺序值，值越大的越被优先读取执行；

应用协议：选择需要管控的单个或者多个协议。点击空白框，会弹出应用协议选择框，如图所示：

自定义 IP：设置需要控制的主机范围（单个机器 IP 或者是某段 IP），点击空白框，会弹出 IP 添加窗口，如图所示：

全局优先级：在整个局域网内具有优先级，规则中的数据在通过防火墙的所有数据中的优先级，分高、默认、低三个级别；

局部优先级：单个主机中匹配该规则的数据在该主机所有数据中的优先级，分高、默认、低三个级别；

首先选择 IP 控制类型，然后填入管控的 IP 范围，并将 IP 添加至列表中，然后点击完成，IP 范围就添加好了；

包含关系：对协议的包含关系。全部，表示应用协议与自定义协议都匹配；部分，表示应用协议与自定义协议可以只匹配其中一种；

主机 IP 地址范围：设置需要控制的主机范围（单个机器 IP 或者是某个 IP 段），点击空白框，会弹出 IP 添加窗口，如图所示：

广域网选择：选择需要管控的协议对应的广域网。

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。

每周：设置一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：设置一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。

13.2、 带宽限制

宽带限制模块对内部机器的带宽使用进行自由控制。

状态：控制规则是否生效。勾上，则表示该规则生效；

描述：对该规则的描述；

控制方式：（单独限制）此范围内每个 IP 的速度将被限制在设定的速度内，即对设定范围内的每个 IP 进行单独限速；（共享限制）此范围内所有 IP 的全部速度总和将被限制设定的速度内；

应用协议：选择需要管控的单个或者多个协议；

自定义 IP 协议：可以自行定义远端 IP、域名及端口协议，并以此作为管控对象；

包含关系：对协议的包含关系。全部，表示应用协议与自定义协议都匹配；部分，表示应用协议与自定义协议可以只匹配其中一种；

上传速度：上传最高速度限制值。如设置为 0 表示不限制；

下载数度：下载最高速度限制值。如设置为 0 表示不限制；

主机 IP 地址范围：设置需要控制的主机范围（单个机器 IP 或者是某个 IP 段）；

广域网选择：选择需要管控的协议对应的广域网；

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效；

每周：设置一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：设置一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。

带宽保证的具体设置方法跟速度限制设置相同。其不同之处在于，速度限制是对单个 IP 或者范围 IP 进行的流量限制；而带宽保证则是对单个 IP 或者范围 IP 提供的一个带宽值保障。

13.3、 带宽保证

状态：控制规则是否生效。勾上，则表示该规则生效；

描述：对该规则的描述；

应用协议：选择需要管控的单个或者多个协议；

自定义 IP 协议：可自定义远端 IP、域名及端口协议，并以此作为管控对象；

上传速度：上传最高带宽保证值。如设置为 0 表示不保证；

下载速度：下载最高带宽保证值。如设置为 0 表示不保证；

控制方式：分为独占宽带和共享宽带

独占宽带：此范围内每个 IP 独立享有设定的带宽保证值；

共享宽带：此范围内所有 IP 共享有设定的带宽保证值。

包含关系：对协议的包含关系。全部，表示应用协议与自定义协议都匹配；部分，表示应用协议与自定义协议可以只匹配其中一种；

主机 IP 地址范围：设置需要控制的主机范围（单个机器 IP 或者是某个 IP 段）；

广域网选择：选择需要管控的协议对应的广域网；

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效

每周：设置一周的哪几天生效，如果没有设置，则表示每天都生效；

每天：设置一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。

13.4、 控制例外

该功能可以对外部服务器的访问限制排除在外，不受智能 QOS 的控制。访问该服务器的流量将不会在主机监控、流量分析里显示出来。

流量控制例外(基于 IP)：填入需要排除的不受 QOS 控制的广域网 IP 地址。设置之后终端访问到该地址时，流量使用不受智能 QOS 规则的限制；

流量控制例外(基于域名)：填入需要排除的不受 QOS 控制的广域网域名地址（域名格式

为：www.qq.com、*.baidu.com、xunlei 等）。设置之后终端访问到该域名时，流量不受智能 QOS 规则的限制。

注意：当设置了 QOS 例外之后，访问该地址时的流量统计不会在流量监控显示出来，且主机监控也不显示。

十四、 双机热备

14.1、 双机热备

用于设置 HA 主/备选举、链路监控、接口监控的相关参数，实现负载均衡和备份的功能

十五、 高级配置

15.1、 端口镜像

端口镜像功能主要用于监控端口数据流量，以方便管理人员对网络数据进行分析。

状态：选择是否启用端口镜像功能；

选择镜像的数据方向：选择监控的数据包走向，出去的数据或者进来的数据，或是所有的数据；

镜像出口方式：选择是镜像到主机 ip 或者镜像到端口；

将数据包镜像到内部主机的 IP：设置一个需要用来作为监控的主机 IP 地址，选择“镜像到主机 IP”时有效；

选择镜像的端口：选择镜像的端口，选择“镜像到端口”时有效。

15.2、 访问设置

对防火墙 WEB 界面的访问权限设置，包括用户名/密码的修改、管理员用户及普通用户

的修改及远程访问功能的开启与关闭。

HTTP 访问端口：本地局域网访问防火墙时的端口。默认为 80；

HTTPS 访问端口：本地局域网使用 https 协议访问防火墙 WEB 管理界面时使用。默认 9090 。

认证通告端口：认证页面、通告页面等页面的弹出时使用的端口，如果为 0，表示和管理端口相同；

远程访问：勾上表示激活远程访问。激活之后，在广域网也能访问到的防火墙 WEB 控制界面，方便管理员进行远程维护。默认为不启用；

远程访问端口：广域网远程访问路由 WEB 控制界面时的端口。默认为 8080；

HTTPS 远程访问端口：开启该功能后，远程访问防火墙 WEB 界面时，必须加上对应端口。

管理员/密码：自定义的管理员账户与密码。管理员具有对防火墙的最高管理权限；

启用 guest 用户：是否启用 guest 用户。Guest 用户只能查看路由设置，不能对路由设置做任何更改。默认不启用；

guest 用户/密码：自定义的 guest 用户名及密码。

管理员用户可以修改防火墙任何设置，guest 用户只能查看设置，不能修改设置。忘记管理员用户/密码之后只能通过按下 reset 按钮来恢复到出厂默认值，请牢记的管理员用户名及密码。默认管理员用户名是 **root** 密码是 **admin**；guest 用户名与密码都是 **guest**。

15.3、 DNS 代理

DNS 代理功能可以缓存最近一段时间之内路由解析的域名与 IP 对应关系表，当用户下次访问“DNS 缓存列表”中的域名时，路由会优先读取缓存列表里的对应 IP 地址，这样便加快了网页访问的速度。

15.3.1 DNS 代理

DNS 代理：选择开启表示启用此功能，默认为开启。有些特殊环境可能解析方式不一样，若有网页不能解析的情况，我们可以尝试关闭此

功能。

老化时间：域名解析的 IP 对应关系在 DNS 列表中缓存的最大时间。

主机连接信息中显示远端 IP 域名：在主机监控中，查看详细连接。显示出远端 IP 对应的域名地址，如下图所示：

协议	本地端口	远端IP	远端端口	运行时间	优先级	上传总数据	下载总数据	类型	接口	域名	控制	操作
TCP	51239	183.61.51.39	443	0秒	中 中	3.22 K	5.39 K	HTTPS	WAN1	p.l.qq.com	允许	允许 阻止
TCP	51238	183.36.108.190	80	1秒	中 中	1.06 K	466 b	腾讯网网页	WAN1	btrace.qq.com	允许	允许 阻止
TCP	51237	183.3.226.58	443	1秒	中 中	1.59 K	5.37 K	HTTPS	WAN1	fw.qq.com	允许	允许 阻止
TCP	51236	183.3.235.211	443	1秒	中 中	1.59 K	4.35 K	HTTPS	WAN1	coral.qq.com	允许	允许 阻止

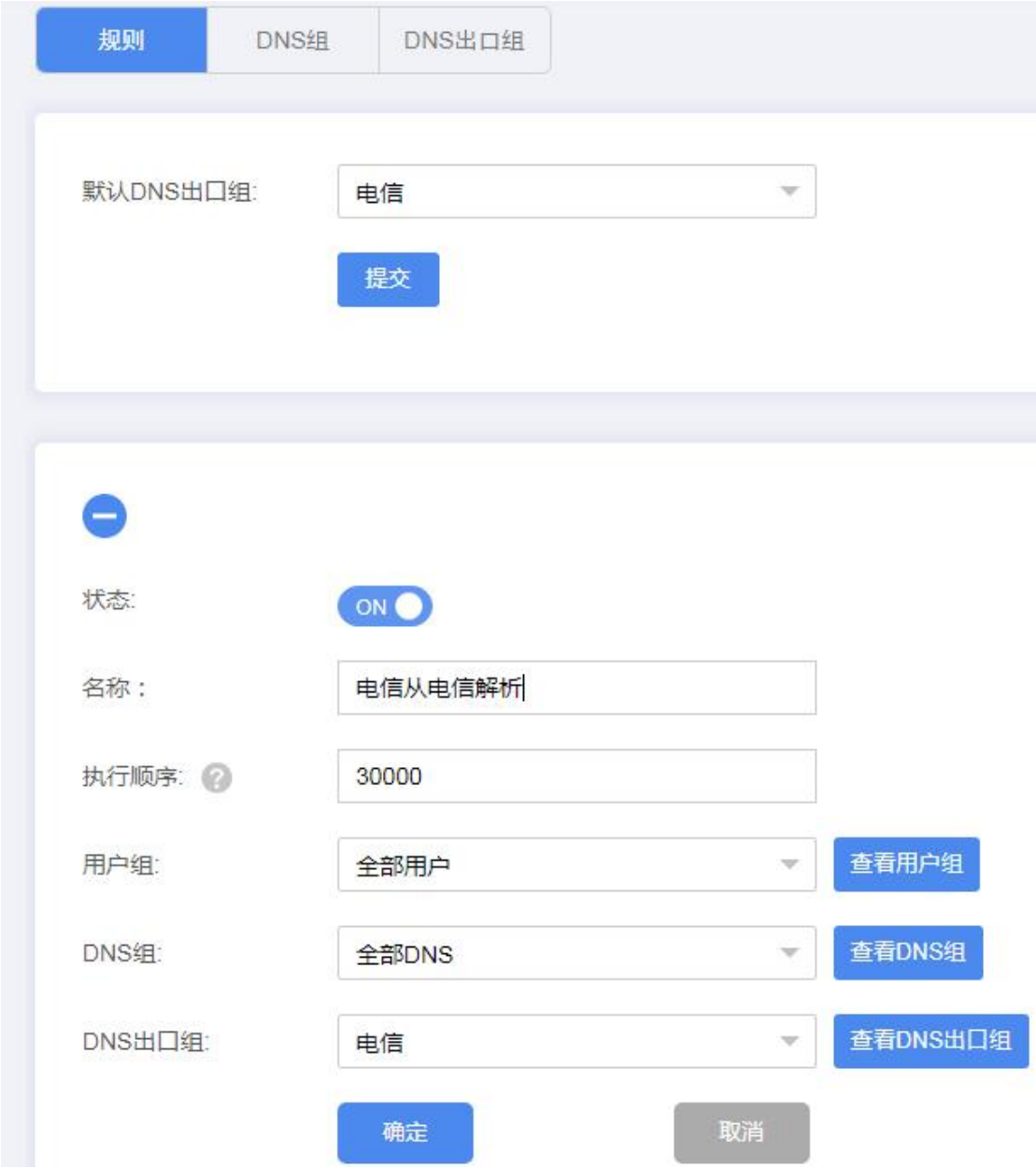
15.3.2 DNS 缓存

DNS 缓存列表会记录下所有用户 DNS 最大老化时间内缓存的域名解析信息，超过时间的缓存信息将会自动老化掉。对某域名做过规则或该域名正被连续使用，将会加长老化时间。

15.4、 DNS 策略

我们在网络使用的过程中，熟知了很多常用域名，例如 hao123.com、 baidu.com、sina.com.cn、163.com 等等。当然这些都是我们熟悉的，那么还有不常用的，不熟悉的呢？例如 PPS、爱奇艺里面的高清视频域名等，这些隐藏的域名都是用户不熟悉的。使用 DNS 策略，用户可以通过域名进行策略路由，如配置网络通过特定的某条外网线路去进行解析等。

15.4.1 规则



默认 DNS 出口组：未做策略规则的 DNS，全部默认从此处选择的出口组去解析。

状态：关闭/开启.控制本条规则开关，表示是否启用该条规则

名称：对此规则的简单描述

执行顺序：多条规则下，值越大的越优先执行

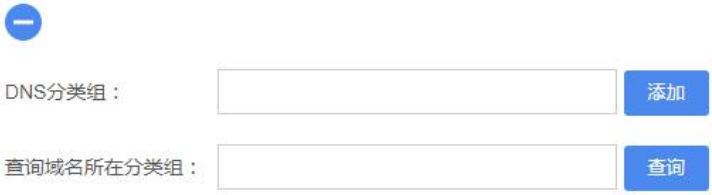
用户组： 用户组即通过内部 IP 地址方式建立的用户组，通过添加用户组后可实现多个用户的统一功能配置。在系统维护-系统对象-IP 组菜单创建

DNS 组：里面包含了用户自定义的和系统自带的 DNS 组，选择需要的组即可

DNS 出口组：从对应 DNS 出口去解析

15.4.2 DNS 组

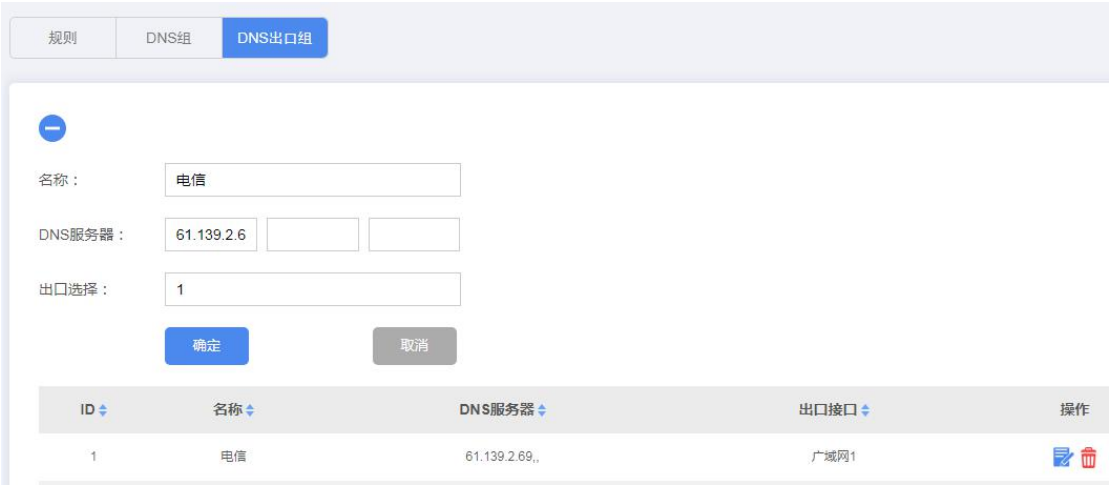
系统自定义了一些常用的 DNS 组，用户也可以手动添加自己需要的。



ID	名称	类型
1	视频	系统创建
2	P2P	系统创建
3	网页	系统创建
4	QQ网吧特权	系统创建
5	网络游戏	系统创建
6	国外应用	系统创建
252	test2	用户定义
253	test1	用户定义

15.4.3 DNS 出口组

设置每个广域网口的 DNS，并选择对应的出口



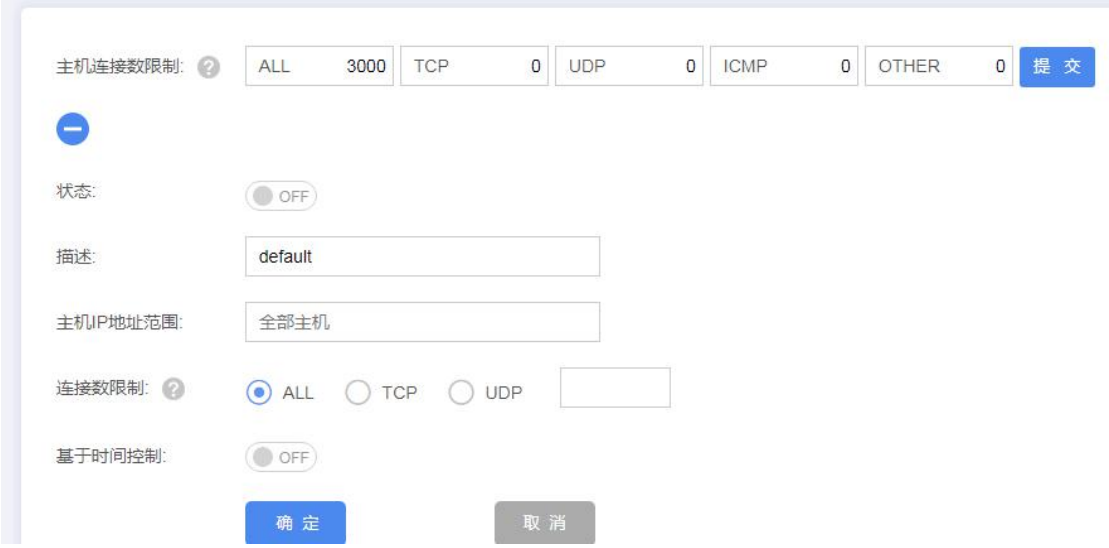
15.5、 连接数设置

连接数限制可以控制整个网络对外的连机数量。若对单个 IP 的连接数进行管控可以控制内网的计算机最多能同时建立的连接数。这个功能对网管人员在控制内网使用 P2P 软件如 BT、迅雷、emule 等会造成大量发出连接数的软件提供了非常有效的管理。设置恰当的允许连接数可以有效控制 P2P 软件下载时所能产生的连接数，相对也使带宽使用量达到一定的限制。另外，若内网有计算机中了类似冲击波的病毒而产生大量对外发联机请求时，也可以达到抑制作用。

15.5.1 连接数设置

主要用于设置防火墙最大对外联机数目，默认连接数是根据机器内存自动获取的，默认情况下不需要做修改。

15.5.2 连接数限制



默认主机连接数限制：所有用户默认主机的连接数限制。当客户机连接数满了之后，由于新的连接出不去，就形同断网，所以请谨慎设置；

激活：是否启用规则，激活之后规则才会生效；

描述：对规则的简单描述；

主机 IP 地址范围：对指定的 IP 地址范围单独设置连接数规则，那么这些 IP 地址将只受规则限制，不受默认主机连接限制；

连接数限制：可以单独对 TCP/UDP 连接限制或者做全部的限制；

基于时间控制：如果启用了“基于时间控制”，那么该规则将只在设定的时间范围内生效。

15.6、 端口设置

用于强行修改路由接口的工作模式，一般情况下不需要修改工作模式，否则可能引起接口工作不正常。

点击列表中操作栏对应的网络接口，可以修改端口的工作模式；

提供四种工作模式供选择：10M/全双工、10M/半双工、100M/全双工、100M/半双工；

通常情况下网络接口之间自动协商工作模式，用户不需要手动配置，保留“自动”即可。

15.7、 NAT 快速转发

启用 NAT 快速转发可以提高数据处理速度，开启 NAT 快速转发后 WEB 关键字过滤、邮件监控，酒店模式，3G/4G 上网等功能可能会失效。

15.8、 USB 存储

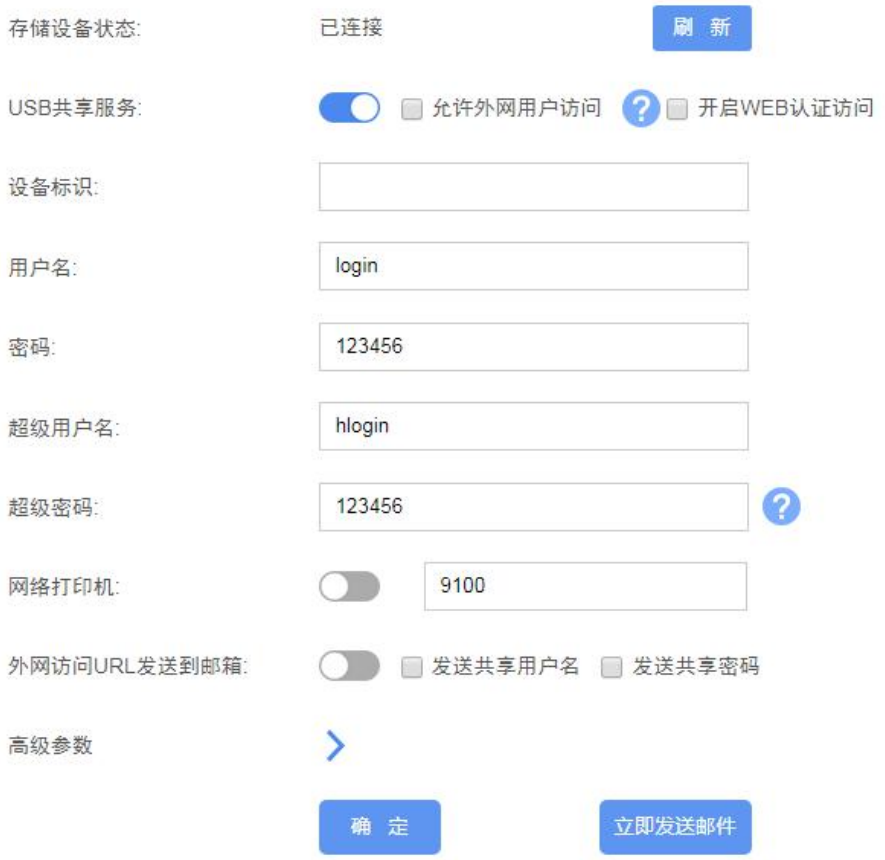
在路由上插入 USB 设备，实现文件、资料的共享，无需单独建立文件共享服务器。

15.8.1 设置状态

设备状态可以查看到当前已连接的 USB 设备信息，在 USB 不使用时，请将 USB 设备移除。

15.8.2 共享服务

USB 设备连接之后，存储状态将显示连接信息。如需使用共享服务需手动开启。



USB 共享：贡献按钮默认为关闭，需要手动开启；

允许外网用户访问：开启后允许外网用户访问 USB 共享；

开启 WEB 认证访问：开启后访问者需要通过下方设置的账号密码认证，方可访问 USB 共享；

网络打印机：当打印机连接本设备后启用网络打印机，可访问 USB 共享的用户也是使用该打印；

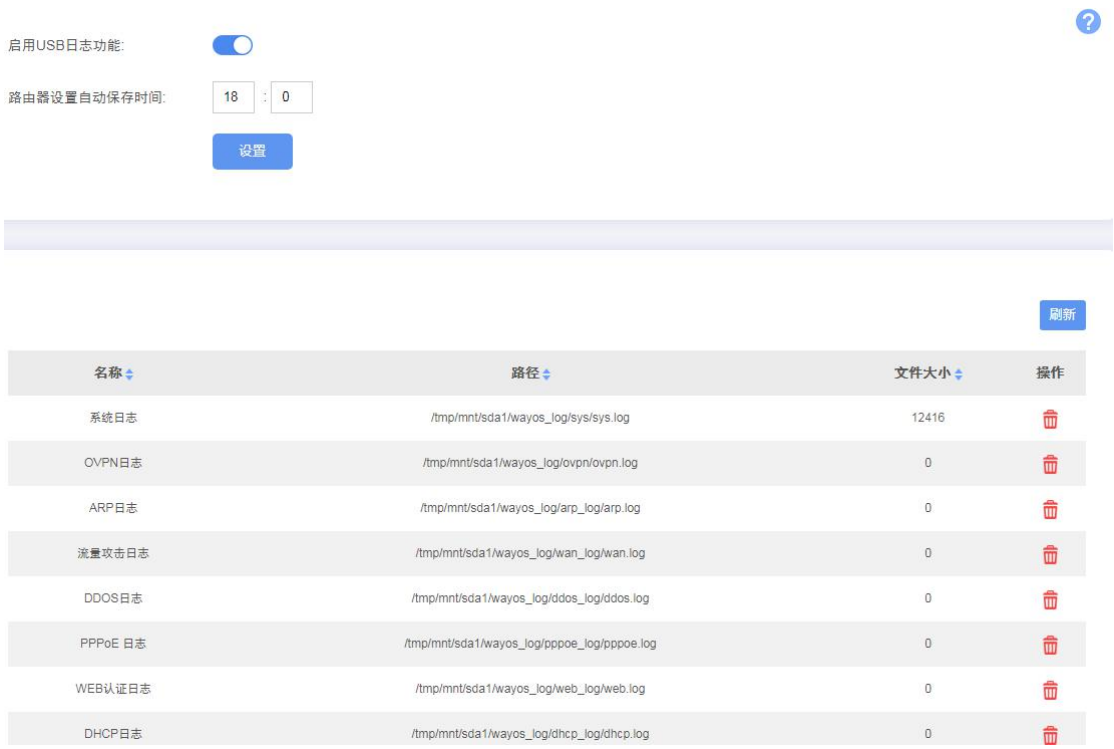
外网访问 URL 发送到邮箱：开启后将 USB 共享地址发送到指定邮箱；

高级参数：用于设定指定 IP 和 MAC 可直接访问 USN 共享的用户终端；

添加：主要用于添加外网访问 URL 发送的邮箱地址。

15.8.3 USB 日志

使用这个功能的前提是需要 USB 存储设备已连接的状态；USB 日志的功能为路由当中所记录的使用日志，由于路由重启后日志都会清空，如果加上 USB 日志记录到 USB 中，日志便于查询。



启用 USB 日志功能，设置自动保存时间-提交设置。防火墙将按设置的时间自动将日志保存在 USB 设备中并且在日志信息列表中会有相关信息。

日志记录的文件夹会存储在 USB 设备中，文件夹名为 wayos_log，打开之后里面所有的格式都是 log，使用记事本打开就可以查看到。

十六、 系统维护

管理路由相关参数设置，包括授权信息、系统对象 ping 检测、系统控制、固件升级、系统参数管理。

16.1、 使用协议

此处协议内容是在本地认证页面上的网络协议中显示，用于展示给终端网络用户阅读，以此规避部分风险。

16.2、 授权信息

显示防火墙防火墙的授权相关信息，包括支持的 WAN 口数、用户数、授权时间等。此授权是固定唯一的。也就是防火墙的 SN 序列号

16.3、 系统对象

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

16.3.1 IP 组

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

提示：如果某 IP 组已经被引用，则不能被删除。删除前必须先解除引用

16.3.2 URL 库

包括内置和自定义的 URL 库。URL 库可用于【防火墙>安全策略】实现对 URL 的过滤。

16.3.3 特征库更新

应用特征库更新：对应用协议的识别进行更新。

16.3.4 ISP 漏洞库

对 ISP 漏洞进行更新

16.3.5 病毒库

病毒库的自动更新与手动升级，可以查看到当前病毒库的版本和 SVN

16.4、 ping 检测

用于方便管理者了解网络对外联机的实际状况，可以借由此功能判断网络的状况。

输入地址：填写需要检测的 IP 或者域名；

网络接口：指定需要检测的网络接口，如果留空，表示从默认的路由出口进行检测；

Ping 包计数：ping 数据包的检测个数；

Ping 包大小：每个 ping 数据包的大小限制。

16.5、 系统控制

用于将路由参数导入导出、升降级固件、设备恢复默认参数以及对路由执行重启操作。

恢复系统参数：将预先保存的系统配置文件导入到防火墙（配置文件为.cfg 格式的）。请不要将其他防火墙的配置文件导入到本防火墙，否则将导致防火墙不能工作；

系统参数备份：保存的防火墙配置参数数据。以备防火墙调试后出现问题时能及时恢复到以前的状态；

恢复默认设置：选择“恢复路由默认设置“，并点击确定。恢复之后防火墙会自动重启，重启完之后请使用默认 IP 及用户名/密码登录路由。防火墙默认 IP：192.168.1.1，默认用户名为 root 密码为 admin；

定时重启防火墙：

激活：启用之后设定的规则将只会在指定的时间段内生效；

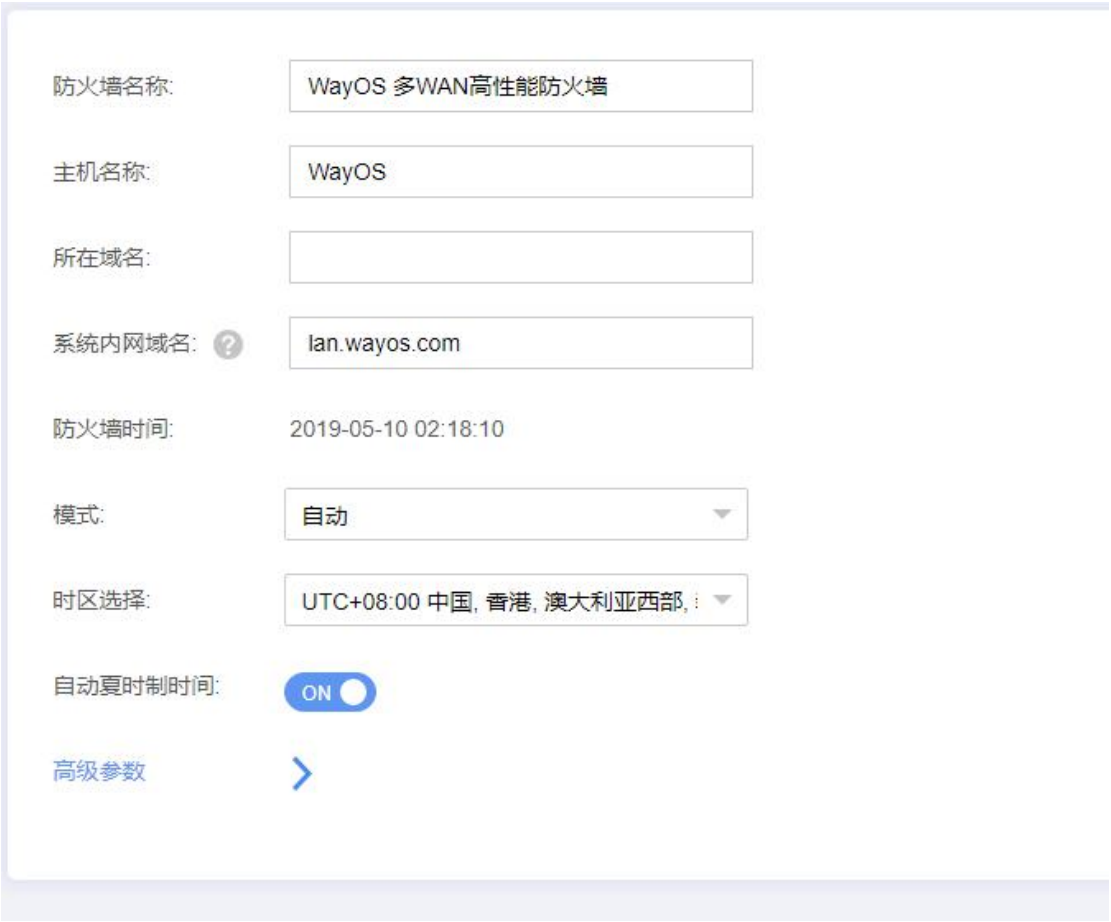
每周：可以设置一周的哪几天生效；

每天：可以设置一天的哪些时段生效；

重启防火墙：点击“重启防火墙”按钮，在弹出的对话框中选择“是“，路由将会重新启动一次。

16.6、 系统配置

在这里您可以查看到防火墙名称、主机名称，所在域名信息。以及系统时间设置等



路由名称：默认为 WayOS 多 WAN 高性能防火墙，您可以自行修改。

主机名称：默认为 WayOS，您可以自行修改。

所在域名：默认为空，您可以自行修改。

系统内网域名：设置此域名后，可在内网通过此域名访问防火墙。

自动夏时制时间：此功能可对设备系统时间进行设定。

16.7、 系统更新

该界面可以对防火墙进行固件升级操作及软恢复操作。如图所示：

固件升级：升级前请先确认好防火墙的当前版本，看是否需要进行升级操作。点击‘浏览’按钮，选择新版本的存放路径之后，按下‘升级’按钮开始升级操作。升级时间一般会在二分钟左右完成，各型号升级时间也不一致。

温馨提示：

升级防火墙的时候，请不要刷新页面，并且保证机器在不断电的情况完成升级操作，否则将造成防火墙升级失败！请尽量选择本地升级防火墙，远程升级防火墙受到网络影响容易导致升级失败！

16.8、 申请控制

申请控制运用于远程控制配置防火墙。该功能默认为关闭状态，如需使用，请手动点击“立即申请”。

重启后自动申请控制：开启申请控制并开启此功能，设备重启后将会把新的申请链接发至下方设置的邮箱中；

描述：对规则的简单描述；

远程访问 URL 发送到邮箱：填入申请控制新链接接收邮箱地址；

定时发送模式：启用之后设定的规则将只会在指定的时间段内生效；

运行间隔：设备在设置的运行间隔时间发送一次控制链接；

每天：可以设置一天的哪些时段发送链接；

十七、 快捷菜单

17.1、 快捷菜单

快捷菜单用于添加快捷按钮到首页，方便管理员快捷访问。