TP-LINK®

# 融合安全网关

# 用户手册

1910041043 REV1.0.0

# 声明

# 目录

# 第1章　用户手册简介

本手册详细介绍登录 Web 管理安全网关配置各项功能的方法，以及使用管理软件的方法。请在操作前仔细阅读本手册。

## 1.1　目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

本书约定

在本手册中，

- 所提到的“安全网关”、“本产品”等名词，如无特别说明，系指融合安全网关产品。
- 全文如无特殊说明，Web 界面以 TL-NR310-2C-S 机型为例，且本手册的 Web 界面仅为示例，请以实际网络 Web 界面为准。
- 用 >> 符号表示配置界面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 三级菜单**，其中，部分功能无二级菜单。
- 正文中出现的<>尖括号标记文字，表示 Web 界面的按钮名称，如<确定>。
- 正文中出现的“”双引号标记文字，表示 Web 界面出现的除按钮外名词，如“系统升级”界面。

本手册中使用的特殊图标说明如下：

| 图标 | 含义 |
| --- | --- |
| 注意： | 该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。 |
| 说明： | 该图标表示此部分内容是对相应设置、步骤的补充说明。 |

## 1.2 产品简介

TL-NR310-2C-S 是 TP-LINK 自主研发推出的多业务融合安全网关，具备路由功能，并深度融合 TP-LINK 安全审计系统与 TP-LINK 认证计费系统，可对接网监平台，适用于酒店、餐饮、娱乐、企业灯连锁分支机构，提供高性价比的组网解决方案。

# 第2章　联网配置

本章介绍如何通过本地 Web 界面，商用网络云平台和手机 APP 管理安全网关。

## 2.1　快速联网配置

### 2.1.1 登录准备

安全网关登录地址为 tplogin.cn，第一次登录时，需要确认以下几点：

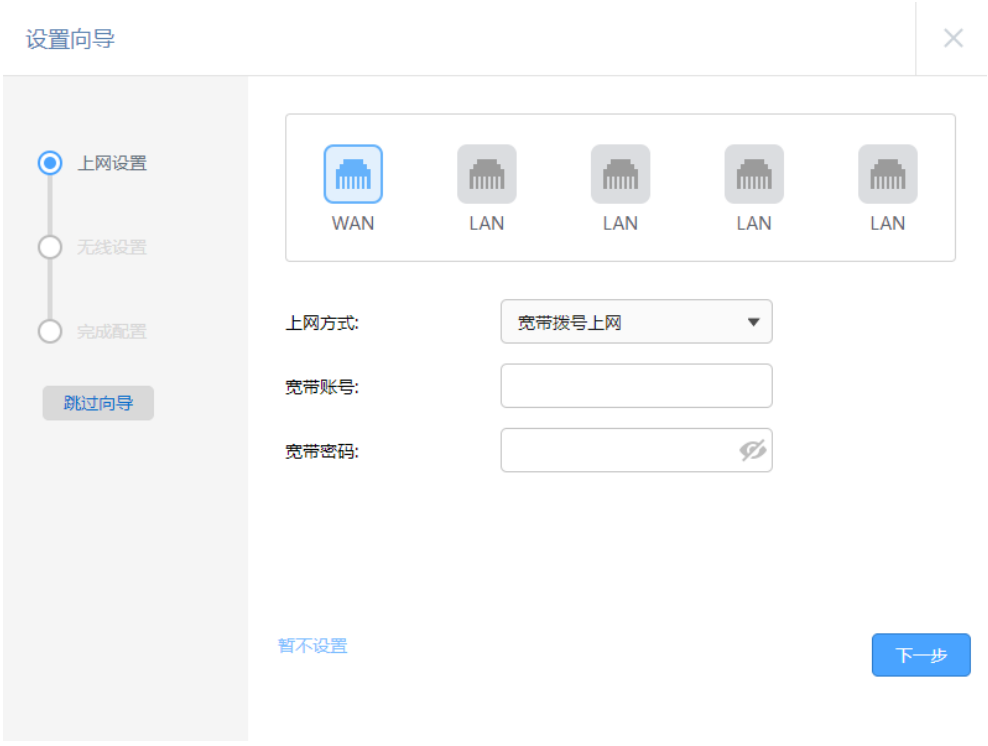
1. 安全网关已正常加电启动，任一 LAN 口已与管理主机相连。
2. 管理主机已至少安装一种以下浏览器：IE 8.0 或以上版本，最新版本的 FireFox、Chrome 和 Safari 浏览器。
3. 管理主机 IP 地址设置为自动获取 IP 地址。
4. 为保证能更好地体验 Web 界面显示效果，建议将显示器的分辨率调整到 1024×768 或以上像素。

### 2.1.2 登录步骤

1. 打开 IE 浏览器，在地址栏中输入安全网关默认管理地址 http://tplogin.cn 登录安全网关的 Web 管理界面。

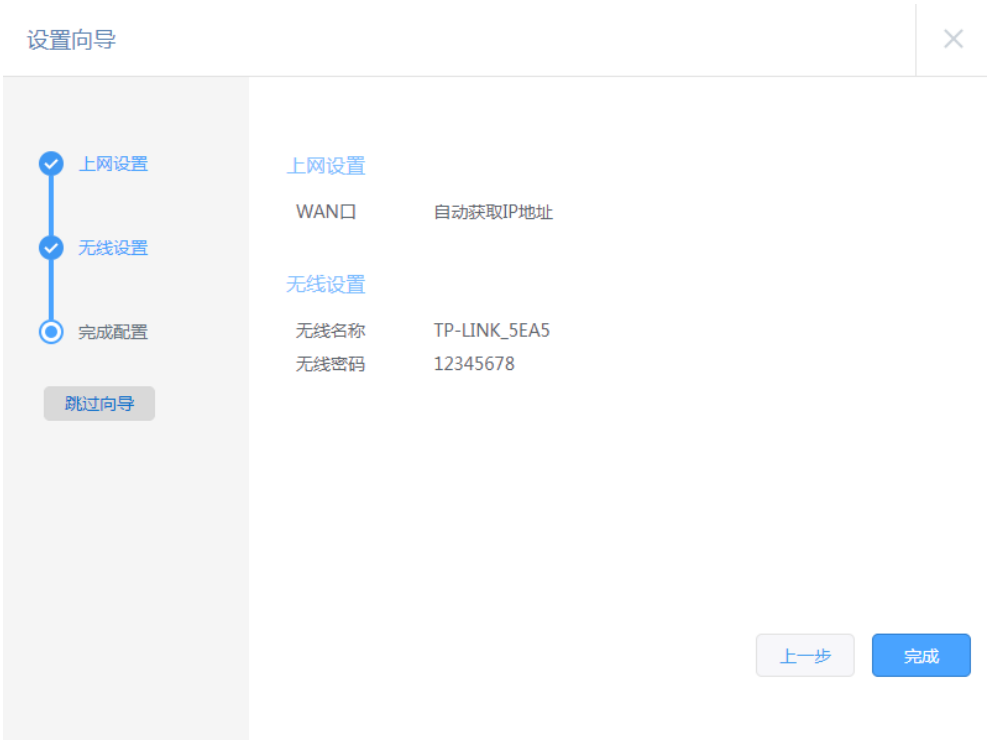

2. 设置用户名和密码，点击<确定>。设置完成后，重新输入用户名和密码，登录设备。


3. 根据网络实际情况选择上网方式：宽带拨号上网；自动获取 IP 地址；固定 IP 上网。设置完成后，点击<下一步>。




4. 设置无线网络名称和密码，当接入 AP 时，可自动同步无线网络。设置完成后，点击<下一步>。


5. 点击<完成>配置。



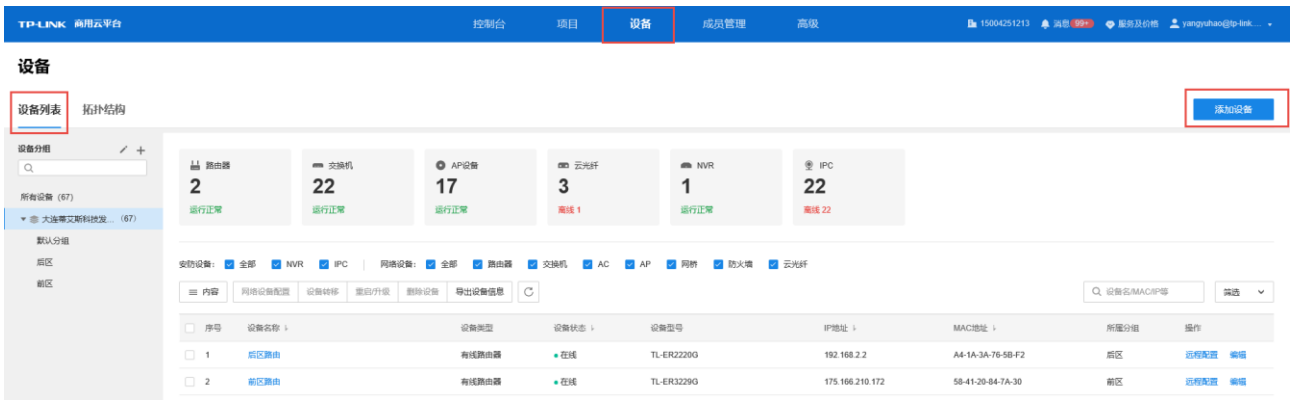

## 2.2 云管理

融合安全网关支持 TP-LINK 商用云平台统一管理，方便对内网安全网关、交换机、AP 等网络设备作出统一配置、管理，远程管理轻松方便。

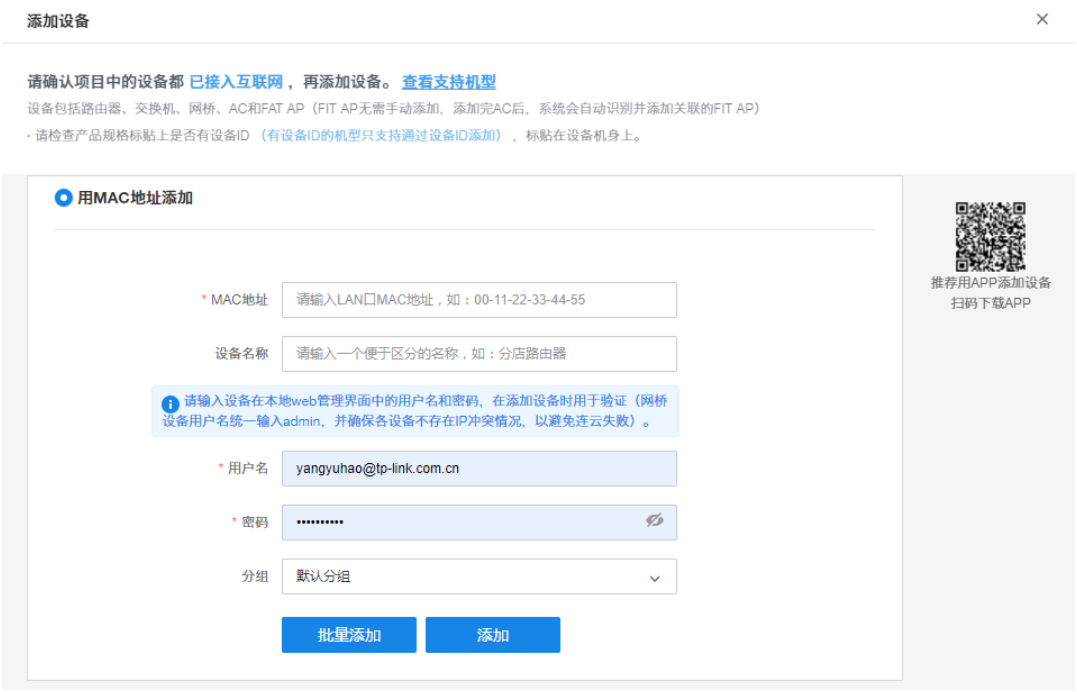
1. 进入页面“系统管理 >> 云管理”，开启云管理功能，点击<保存>。


2. 电脑登录 TP-LINK 商用网络云平台 (https://smbcloud.tp-link.com.cn/)，并且登录已经在平台注册的 TP-LINK ID。


3. 进入页面“项目集中管理 >> 设备 >> 设备列表”，点击<添加设备>。




4. 可选择“用 MAC 地址添加”，MAC 地址可在网关底部标贴上查找。




5. 点击添加完成后在设备信息中找到对应网关设备，点击条目后方”远程管理”，即可实现通过 TP-LINK 商用云平台远程管理设备。

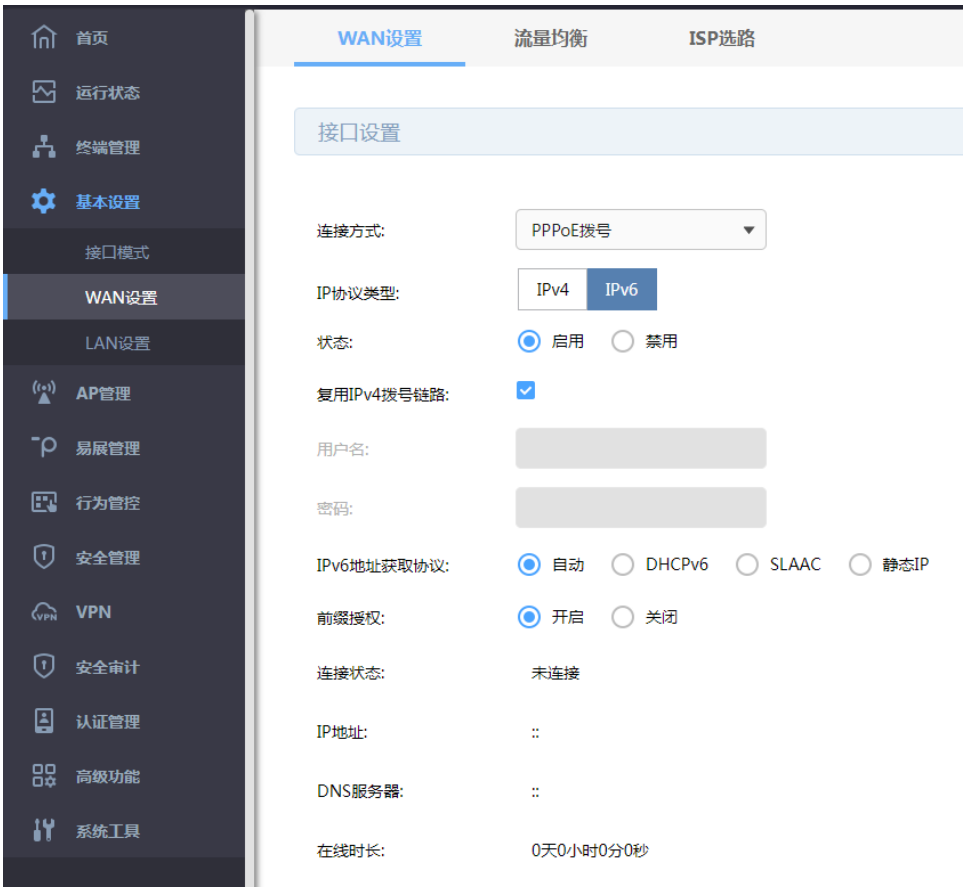

## 2.3 IPv6 上网配置

全球所有 43 亿个 IPv4 地址已全部用完，意味着没有更多的 IPv4 地址可以分配给 ISP 和其它大型网络基础设施提供商，因此 Internet 研究组织发布新的主机标识方法，即 IPv6。目前国内的网络正在快速的向 IPv6 升级中，从网络基础设施如运营商骨干网、城域网，到互联网服务商如各类云服务，以及各类终端设备厂商如手机、电脑、安全网关、交换机等。目前运营商提供的 IPv6 线路主要分为支持前缀授权和不支持前缀授权两种。

终端获取到一个 IPv6 公网地址，实现端到端通信，减小网络转发开销；安全网关 WAN 口可以同时获取到 IPv4 和 IPv6 地址，并且给支持双栈的终端分配 IPv4 和 IPv6 两个地址；终端访问 IPv4 的目标主机时走 IPv4，访问 IPv6 的目标主机时走 IPv6。

- **支持前缀授权的 IPv6 线路上网设置方法**

1. 进入页面“基本设置 >> WAN 设置 >> WAN 设置”，设置成功后可看到 WAN 口获取到的 IPv6 地址。

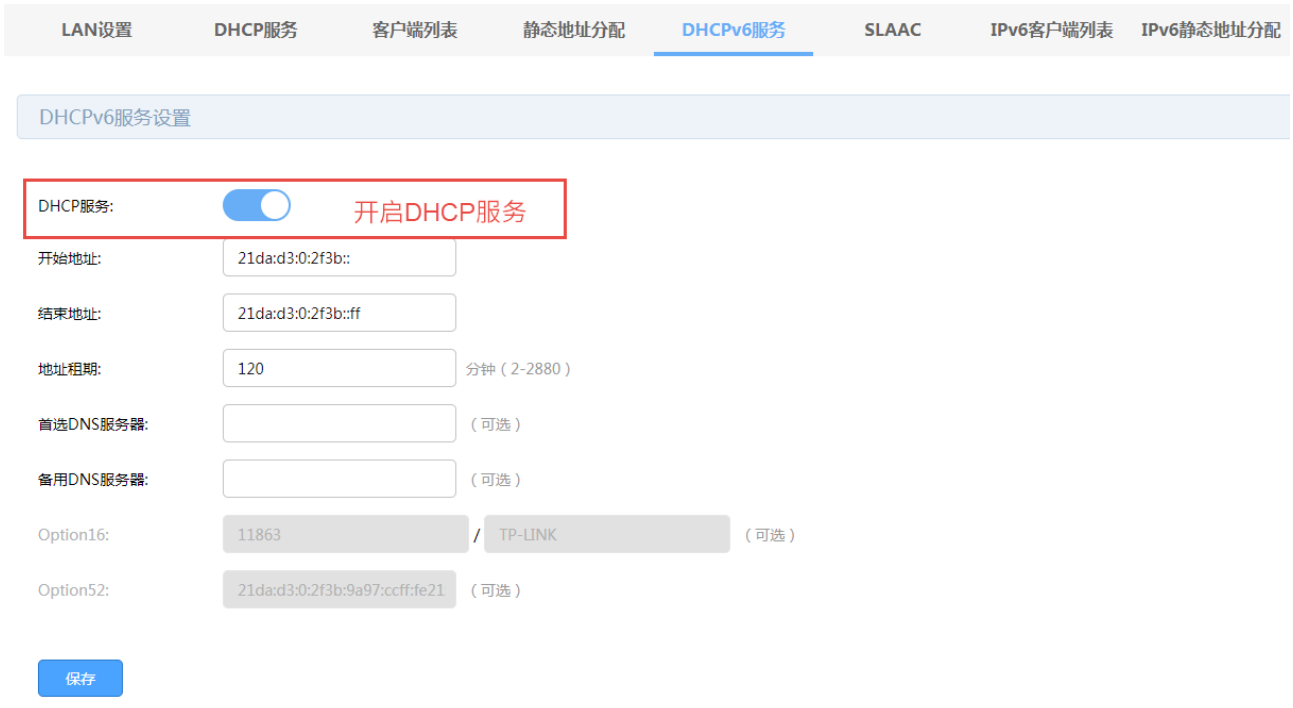



| | |
|---|---|
| 连接方式 | 选择运营商提供的 IPv6 上网连接方式方式 |
| IP 协议类型 | 选择 IPv6 协议类型 |
| 状态 | 勾选启用 |
| 复用 IPv4 拨号链路 | 当开启此功能后，IPv6 将使用 IPv4 账号密码进行拨号，不需要手动输入 IPv6 宽带账号及密码。请注意开启此功能需要运营商支持，请根据实际情况正确选择是否开启。 |
| IPv6 地址获取协议 | 默认自动，也可以根据需要进行相应修改。如果选择 DHCPv6，则直接由运营商动态分配一个 IPv6 地址；如果选择 SLAAC，则由安全网关根据路由通告自动生成 IPv6 地址；如果选择固定 IP，则使用运营商提供的固定 IPv6 地址进行上网。 |

| | |
|---|---|
| 前缀授权 | 当 IPv6 地址获取协议为自动、DHCPv6 或者 SLAAC 时，可以选择是否开启前缀授权功能。开启此功能后，安全网关将自动从运营商获取一个 IPv6 地址前缀，该前缀用于为局域网中设备生成 IPv6 地址。开启此功能需要运营商支持，请根据实际情况正确选择是否开启。 |

2. 进入页面“基本设置 >> LAN 设置 >> LAN 设置”，地址配置方式选择 EUI-64（EUI-64 表示自动获取 64 位 IPv6 的前缀地址），前缀接口选择刚才设置好的 WAN 口。


3. 根据需要设置 LAN 口 IPv6 地址分配方式，可以选择 DHCPv6 或者 SLAAC（二选一），DNS 不填时默认为安全网关的 IPv6 地址，安全网关作 DNS 代理。其中 DHCPv6 是安全网关手动设置一个范围下发地址；SLAAC 是根据地址前缀安全网关随机下发地址。





4. 设置好安全网关的相关参数后，终端（电脑、手机等）勾选 IPv6 协议，并开启自动获取 IPv6 地址和 DNS 服务器即可，获取 IP 结果如下。

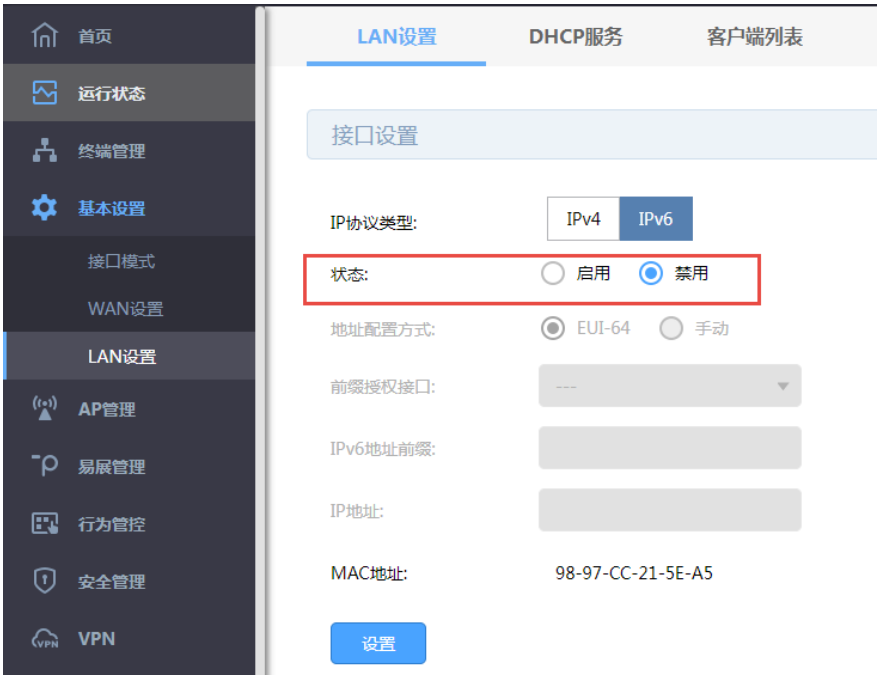
➢ **不支持前缀授权的 IPv6 线路上网设置方法**

对于不支持前缀授权的运营商线路，无法由安全网关给终端分配 IPv6 地址，终端 IPv6 地址统一由运营商

进行分配，因此需要安全网关支持 IPV6 桥模式，目前安全网关支持 IPv6 桥模式，具体配置方法如下：

1. 进入页面“基本设置 >> 接口模式 >> IPv6 桥模式”，启用桥模式，点击<保存>。


2. 开启桥模式后 WAN 口和 LAN 口的 IPv6 参数均不可设置。进入页面“基本设置 >> WAN 设置 >> WAN 设置”，禁用 WAN 口的 IPv6 功能；进入页面“基本设置 >> LAN 设置 >> LAN 设置”，禁用 LAN 口的 IPv6 功能。


首页
运行状态
终端管理
基本设置
接口模式
WAN设置
LAN设置
AP管理
易展管理
行为管控
安全管理
VPN
LAN设置
DHCP服务
客户端列表
接口设置
IP协议类型:
IPv4
IPv6
状态:
启用
禁用
地址配置方式:
EUI-64
手动
前缀授权接口:
---
IPv6地址前缀:
IP地址:
MAC地址:
98-97-CC-21-5E-A5
设置

# 第3章　基本配置

## 3.1　WAN 口设置

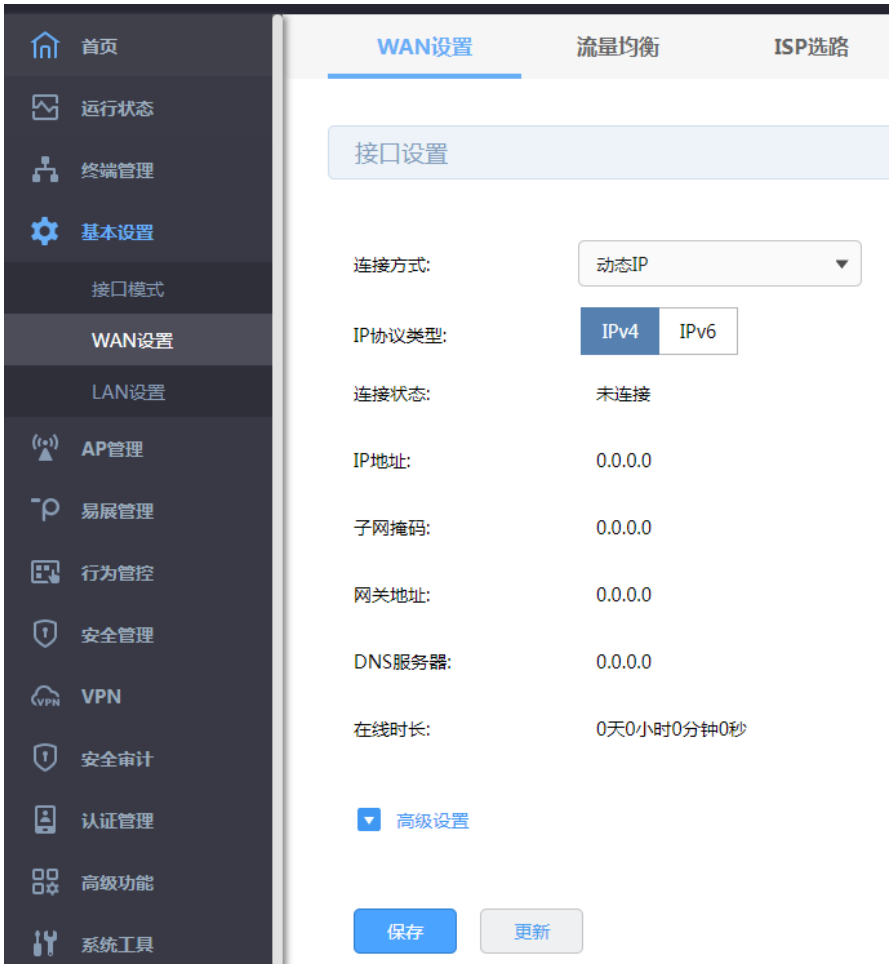
融合安全网关产品提供三种方式接入广域网：固定 IP 地址、自动获取 IP 地址、PPPoE 拨号，请根据 ISP（Internet Service Provider，网络服务提供商）提供的服务进行选择。

有线宽频一般使用自动获取 IP 地址连接方式；

光纤接入以及企业、网吧局域网内组网一般使用固定 IP 地址连接方式；

xDSL 拨号上网则使用 PPPoE 连接方式；

进入页面：基本设置 >> WAN 设置 >> WAN 设置。设置对应端口，选择对应连接方式。设置完成后，点击<保存>。



## 3.2 LAN 口配置

进入页面：基本设置 >>LAN 设置 >>LAN 设置。设置网关 LAN 口的 IP 参数。设置完成后，点击<保存>。


说明：

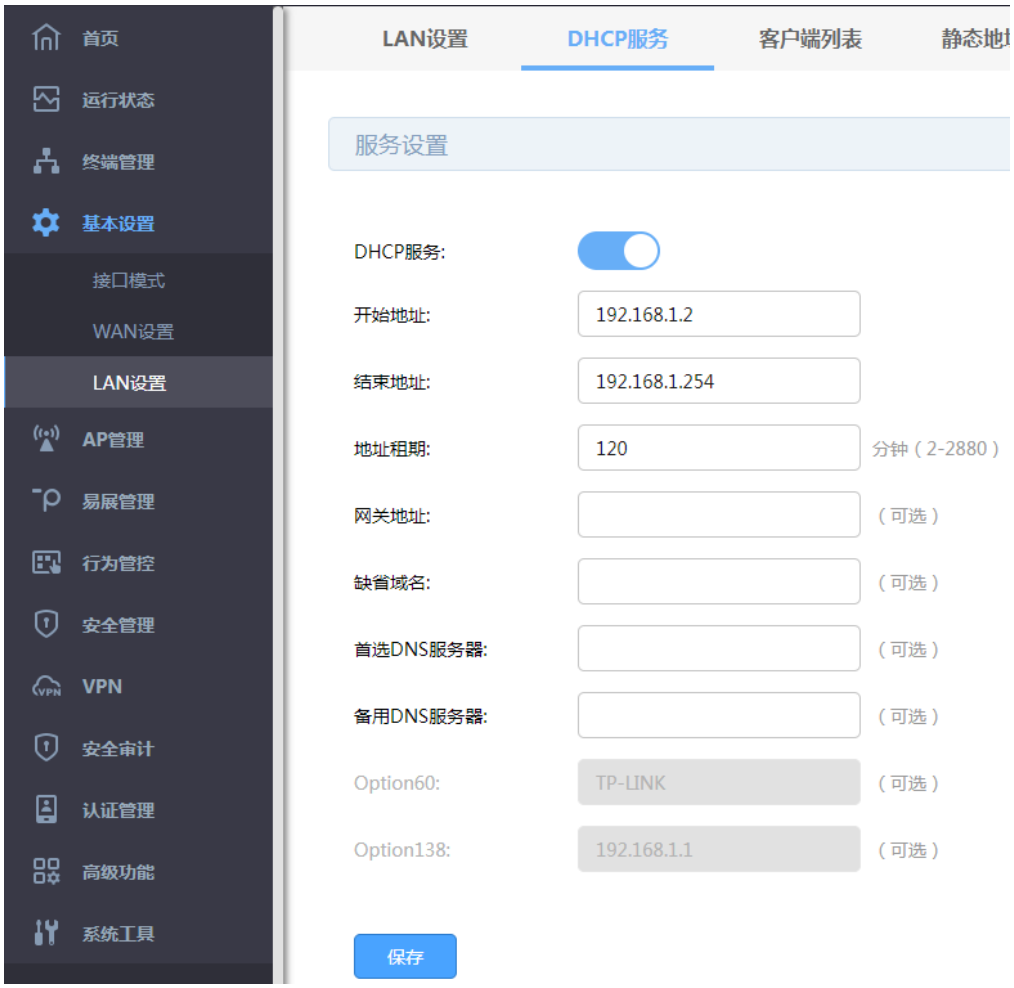
- 若 LAN 口 IP 地址有修改，必须在保存配置后使用新的 LAN 口地址登录网关 Web 管理界面。并且，局域网内所有计算机网关地址、子网掩码必须与修改后的 LAN 口设置保持一致，才能正常通信。

## 3.3 DHCP 服务

### 3.3.1 DHCP 服务

DHCP 服务器能够自动给局域网中的设备分配 IP 地址。

进入页面：基本设置 >> LAN 设置 >> DHCP 服务。配置成功后，点击<保存>。




| | |
|---|---|
| DHCP 服务器 | 网关的 DHCP 服务器默认开启。<br>若网络中已经有其他的 DHCP 服务器需要关闭该安全网关的 DHCP 服务器，请选择关，并点击保存。 |
| 开始/结束地址 | 设置 IP 地址池，DHCP 服务器开启状态下，安全网关自动从地址池（默认为 192.168.1.2~192.168.1.254）中给局域网中的设备分配 IP 地址。 |

点击页面，查看更多页面设置参数信息。

## 3.3.2 DHCPv6 服务

当网关开启了 IPv6 功能，可开启 DHCPv6 服务。

进入页面：基本设置 >> LAN 设置 >> DHCPv6 服务。配置成功后，点击<保存>。


| | |
|---|---|
| DHCP 服务器 | 网关的 DHCP 服务器默认开启。<br>若网络中已经有其他的 DHCP 服务器需要关闭该安全网关的 DHCP 服务器，请选择关，并点击保存。 |
| 开始/结束地址 | 设置 IP 地址池，DHCP 服务器开启状态下，安全网关自动从地址池中给局域网中的设备分配 IP 地址。 |

点击页面，查看更多页面设置参数信息。

# 3.4 客户端列表

## 3.4.1 客户端列表

客户端列表显示已由 DHCP 分配 IP 参数的主机信息。

进入页面：进入页面：基本设置 >> LAN 设置 >> 客户端列表。点击<刷新>，可获取最新列表信息。

### 3.4.2 IPv6 客户端列表

客户端列表显示已由 DHCP 分配 IP 参数的主机信息。

进入页面：基本设置 >> LAN 设置 >> IPv6 客户端列表。点击<刷新>，可获取最新列表信息。


## 3.5 静态地址分配

### 3.5.1 静态地址分配

可根据接入设备的 MAC 地址手动分配 IP 地址。当对应的客户端设备请求 DHCP 服务器分配 IP 地址时，DHCP 服务器将自动为其分配指定的 IP 地址。

进入页面：基本设置 >> LAN 设置 >> 静态地址分配。点击<新增>，输入对应的 MAC 地址和 IP 地址，点击<保存>。


### 3.5.2 IPv6 静态地址分配

可根据接入设备的 MAC 地址手动分配 IP 地址。当对应的客户端设备请求 DHCP 服务器分配 IP 地址时，

DHCP 服务器将自动为其分配指定的 IP 地址。

进入页面：基本设置 >> LAN 设置 >> IPv6 静态地址分配。点击<新增>，输入对应的 MAC 地址和 IP 地址，点击<保存>。


## 3.6 SLAAC

SLAAC（Stateless address autoconfiguration），无状态地址自动配置，网关为客户端指定网络前缀和前缀长度，客户端使用前缀和前缀长度自行创建 IPv6 地址。当部分客户端设备不支持 DHCPv6 服务器时，可选择使用 SLAAC。请在 LAN 设置中开启 IPv6 功能。

进入页面：基本设置 >> LAN 设置 >> SLAAC。开启服务接口，选择 DNS 配置方式。配置完成后，点击<保存>。

# 第4章　路由功能

路由是指安全网关根据数据包的目的 IP 地址选择最优路径，并转发到通往目标网络的下一个网络节点的过程。

在一次路由过程中选择最优路径是安全网关需要完成的最重要的工作。安全网关通过维护一张路由表来记录网络中的路径信息，并根据一定的路由选择协议在路由表中选择一条最优路径进行数据转发。路由表中的每一个路由条目基本都包含如下四种基本属性，路由转发时将根据数据包的目的 IP 地址查找最优路径：

1)　目的网络地址：用于标识该条路由条目所指向的目标网络。

2)　子网掩码：用于标识目标网络的子网掩码。

3)　下一跳地址：用于指定通往目标网络的下一跳路由节点，安全网关将数据转发给下一跳路由节点后，由下一跳路由节点将数据发往再下一跳路由节点或目标网络。下一跳路由必须是本地可达的，配置路由条目时可以通过 ping 工具测试是否可达。

4)　下一跳接口：用于标识数据从本地发出的出接口。

安全网关根据路由表进行数据转发，而路由条目的来源有三种，分别为直连路由、静态路由和动态路由，以下是三种路由的特点。

- 直连路由：通过数据链路层协议发现的，通常指向与安全网关直接连接的网络，如 VLAN。
- 策略路由：由网络管理员手动指定策略规则，设备根据策略进行路由选择，不随着网络拓扑的改变而自动变化。设备配置策略路由后，若接收的报文匹配策略路由的规则，则按照规则转发；若匹配失败，则根据目的地址按照正常转发流程转发。
- 静态路由：由网络管理员手动配置的一种特殊路由，不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。
- 动态路由：通过相互连接的安全网关之间交换彼此的路由信息，然后通过路由选择协议计算出自身的

路由表信息，可随着网络拓扑的改变而自动变化，简化了网络管理工作。常用的动态路由选择协议有RIP、OSPF 和 BGP 等等，不同的协议有不同的算法，对于发往同一目标网络的路径选择结果也可能不一样。

融合安全网关支持策略路由、静态路由。

## 4.1 设置策略路由

策略路由

设置策略路由，在传统路由转发的基础上根据自己定义的策略进行报文转发和选路。策略路由具有很强的灵活性，用户可根据实际需求指定策略路由，路由按规则选择转发。策略路由可提高链路的利用效率，当不同数据流通过不同的策略链路进行转发。

配置方法：

进入页面：高级功能 >> 路由设置 >> 策略路由，点击<新增>，设置策略规则，配置完成后，点击<确定>。

| | |
|---|---|
| 服务类型 | 选择策略选路功能生效的协议。 |
| 源/目的地址 | 设置策略生效的源/目的地址。也可自定义设置地址范围，更多地址组管理可参考 9.1.1 地址组管理。 |
| 出接口 | 设置数据包出接口。 |
| 添加到指定位置 | 指定添加的规则的位置，排在前面的规则比后面规则优先级高。 |

点击页面，查看更多页面设置参数信息。

## 4.1.1 策略路由配置实例

组网介绍：

某公司企业内部专网 10.17.0.0/16，需要实现下接的终端全部可以访问内网网段。拓扑如下：


配置步骤：

1. 进入页面“基本设置 >> WAN 设置”，设置企业内网 IP 地址。


2. 进入页面“高级功能 >> 路由设置 >> 策略路由”，点击<新增>，进行设置。

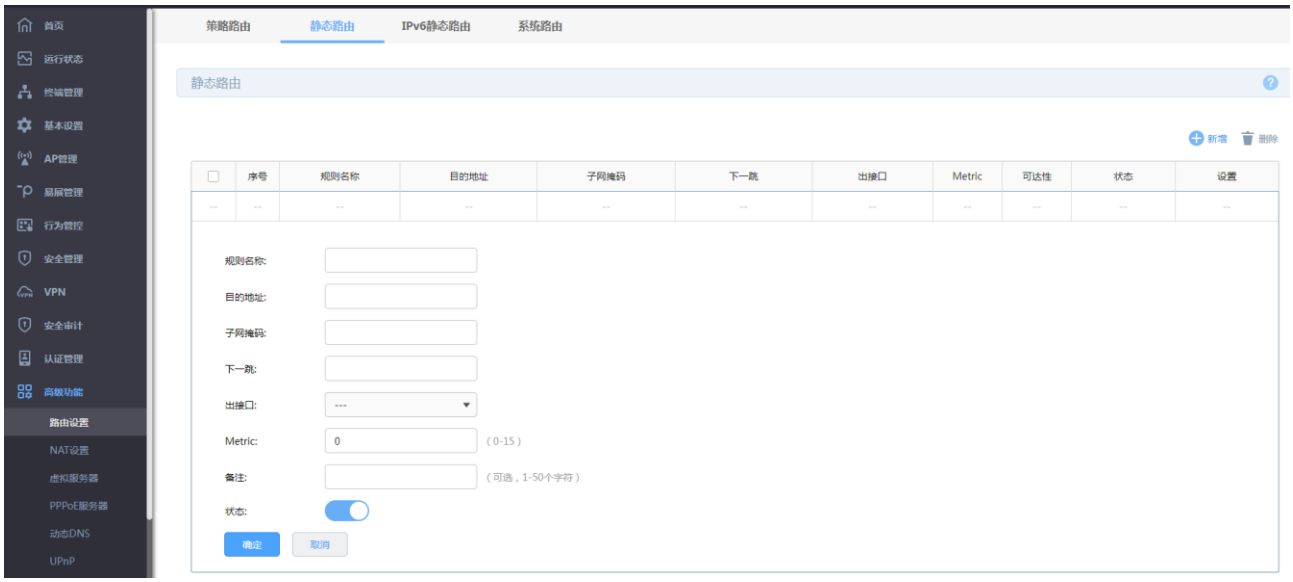
# 4.2 设置静态路径

## 4.2.1 静态路由

静态路由是由网络管理员手动设置的路由，一般在规模不大、拓扑结构固定的网络中配置，网络管理员只需配置少量静态路由即可实现网络互通。在网络中使用合适的静态路由可以减少路由选择问题，提高数据包的转发速度。当网络发生改变时则需要网络管理员手动修改路由配置以保证网络正常通信。

配置方法：

进入页面：高级功能 >> 路由设置 >> 静态路由，点击<新增>，设置静态路由规则，配置完成后，点击<确定>。



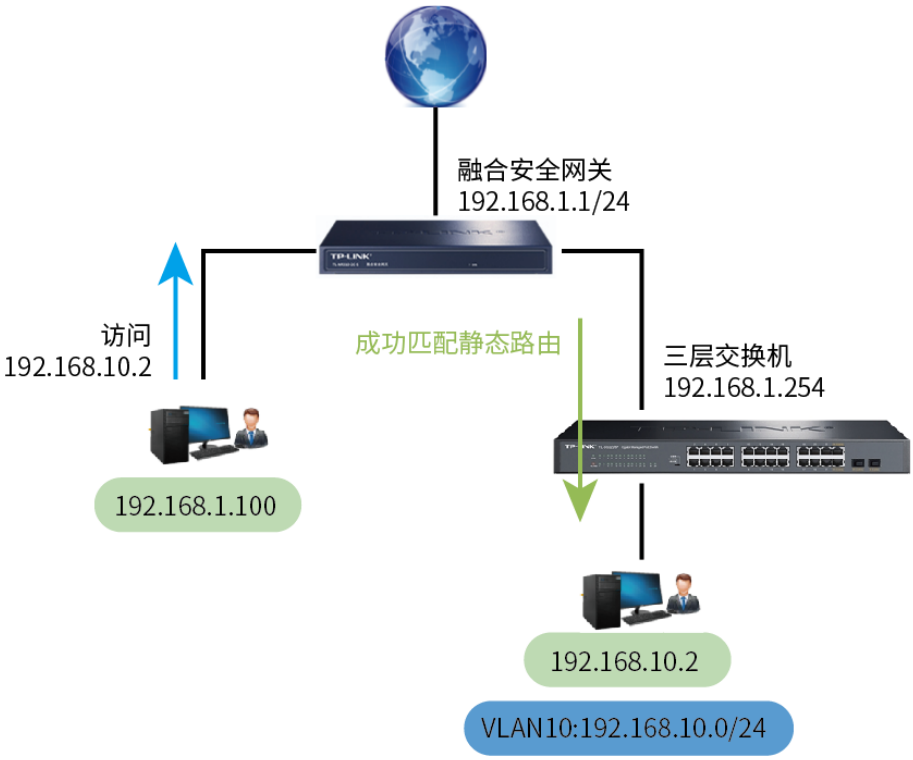

| | |
|---|---|
| 目的地址/子网掩码 | 设置目的地址和子网掩码，确定路由生效的网段。 |
| 下一跳 | 数据包将发往的下一个路由点。 |
| 出接口 | 设置数据包出接口。 |
| 添加到指定位置 | 指定添加的规则的位置，排在前面的规则比后面规则优先级高。 |
| Metric | 静态路由规则的度量值，数值越小优先级越高，默认为 0。 |

点击页面 ，查看更多页面设置参数信息。

## 4.2.2 静态路由配置实例

组网介绍：

某企业使用安全融合网关，下接三层交换机，交换机划分了 VLAN10，需要实现安全网关 LAN 网段的终端可以与三层交换机下的 VLAN10 网段的终端进行互访。，示意网络拓扑如下：




配置步骤：

高级功能 >> 路由设置 >> 静态路由，点击<新增>，进行设置。


## 4.3 NAT 设置

### 4.3.1 NAT 介绍

NAT（Network Address Translation，网络地址转换）可以实现局域网内的多台计算机通过 1 个或多个公网 IP 地址接入因特网。NAT 设备在向广域网转发局域网数据时，使用特定的 IP 地址转换数据包中的源 IP 地址和传输端口，使局域网中的计算机共用少量的广域网 IP 地址与广域网中的计算机通信。NAT 地址转换过程如下图所示：


如图所示，NAT 设备在向广域网转发数据包时，将数据包的源 IP 地址进行转换，将其转换为自身 NAT 接口的 IP 地址并将数据发送；当 NAT 收到广域网应答的数据包时，则根据 NAT 地址转换记录将数据包中的

目的 IP 地址进行转换，并将其发往局域网中的指定主机。在网络中使用 NAT 技术有效地解决了 IP 地址资源不足的问题，同时隐藏了局域网的计算机，使广域网计算机无法直接访问到局域网设备，为局域网提供了一定的安全保障。

- **NAT 分类**

为适应网络中不同的需求，在实际网络应用中 NAT 有三种应用类型，分别为一对一 NAT、动态 NAT、NAPT。

- 一对一 NAT：将私有网络的地址与广域网地址一对一映射，且映射关系是唯一的，某个私有网络 IP 地址转换为固定的公有 IP 地址。利用一对一 NAT 转换，可以实现内部网络中的特定设备（如服务器）对外部网络开放。
- 动态 NAT：将私有网络的地址与广域网地址进行转换时，转换关系是随机的。只要指定了可以进行转换的私有网络地址，以及合法的广域网地址，就可以进行动态地址转换。动态 NAT 需要指定多个合法的广域网地址，当能够进行 NAT 转换的广域网地址数略少于局域网计算机的数量时，可以采用动态 NAT。
- NAPT：将私有网络地址映射成一个合法的广域网地址，同时通过不同的传输协议端口号与不同的内部主机应用相对应。

本设备提供了一对一 NAT 和 NAPT 两种特性。

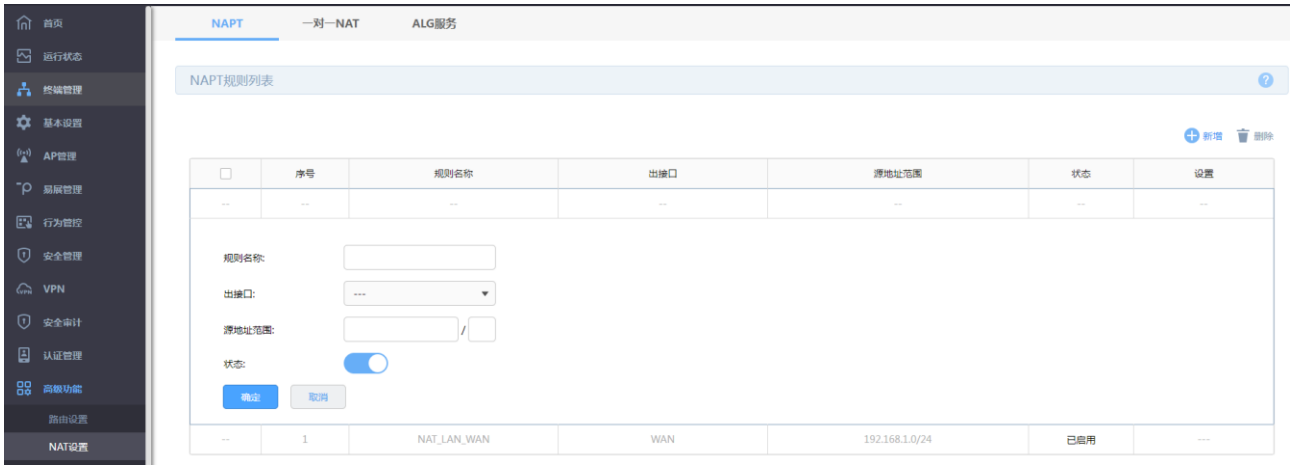
## 4.3.2 NAPT

当局域网中多台设备需要访问广域网时，而网络中只有少量接口连接到 Internet 时，需要配置 NAPT 功能，使多台设备能够共享 ISP 接口上网。设置本功能后，源地址范围内主机发出的数据包通过指定出接口转发时，将对数据包源 IP 地址和传输协议端口的 NAPT 地址转换，使用出接口的 IP 地址和传输协议端口与内网主机应用对应。

配置方法：

进入页面： 高级功能 >> NAT 设置 >> NAPT，点击<新增>，设置规则名称，选择出接口，设置源地址范

围，点击<确定>。




如下设置部分 NAPT 规则，代表的含义如下：

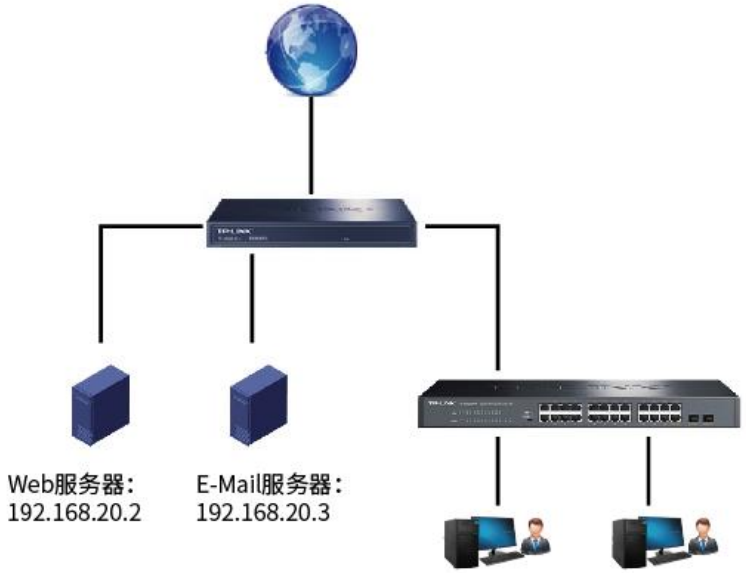
| 序号 | 规则名称 | 出接口 | 源地址范围 | 状态 | 设置 |
|---|---|---|---|---|---|
| 1 | NAT_LAN_WAN | WAN | 192.168.1.0/24 | 已启用 | --- |
| 2 | 2 | WAN | 192.168.0.0/24 | 已启用 | |
| 3 | 3 | WAN | 192.168.3.52/32 | 已启用 | |

- 序号为 1 和 2 的规则表示 192.168.0.0/24 和 192.168.1.0/24 两个子网中的计算机通过“WAN”接口访问外部网络时均需要进行 NAPT 地址转换，共用接口的 IP 地址上网；
- 序号为 3 的规则表示计算机 192.168.3.52 通过“eth0”接口上网时需要进行 NAT 地址转换，使用接口的 IP 地址上网；
- 当局域网中所有主机均需要访问 Internet 时，您需要为所有子网都建立 NAPT 规则，此时可以通过设置全 0 规则快速设置，源地址范围设置为 0.0.0.0/0 即可，如下图所示，图中创建的规则表示所有从“WAN”接口转发的数据均做地址转换。

## 4.3.3 NAPT 配置实例

组网介绍：

某公司内网上搭载了Web 服务器和 E-Mail 服务器需要对外开放，Web 服务器的内网 IP 为 192.168.20.20，E-Mail 服务器的内网 IP 为 192.168.20.30，其余主机不使用 192.168.20/24 网段。拓扑如下：




配置步骤：

1. 进入页面“高级功能 >> NAT 设置 >> NAPT”，点击<新增>。

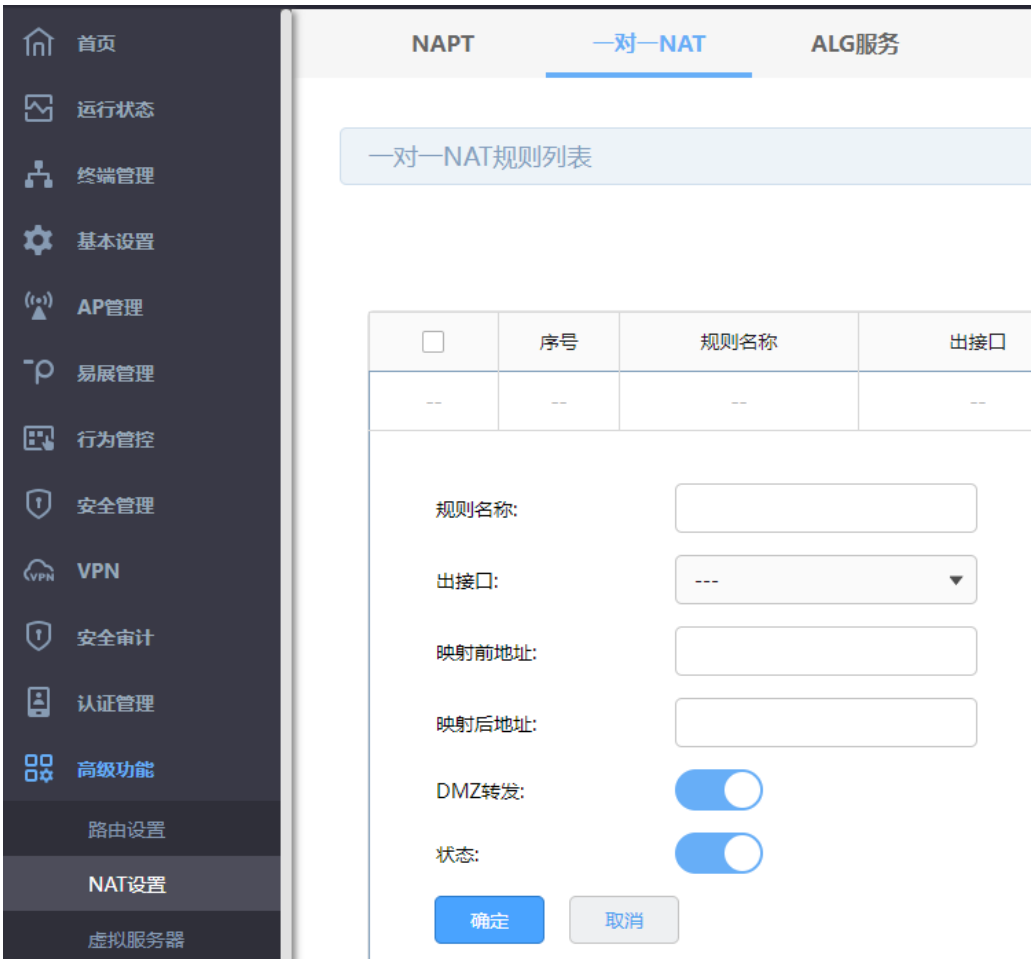
2. 设置 NATP 规则。

## 4.3.4 一对一 NAT

一对一 NAT，可以将局域网 IP 地址与广域网 IP 地址唯一对应，通常用于局域网内的服务器搭建。用户可以通过一对一 NAT 映射后的广域网地址访问局域网中的服务器，配置动态 DNS 功能则可以通过域名来访问服务器。

配置方法：

进入页面： 高级功能 >> NAT 设置 >> 一对一 NAT，点击<新增>，配置完成后，点击<确定>。



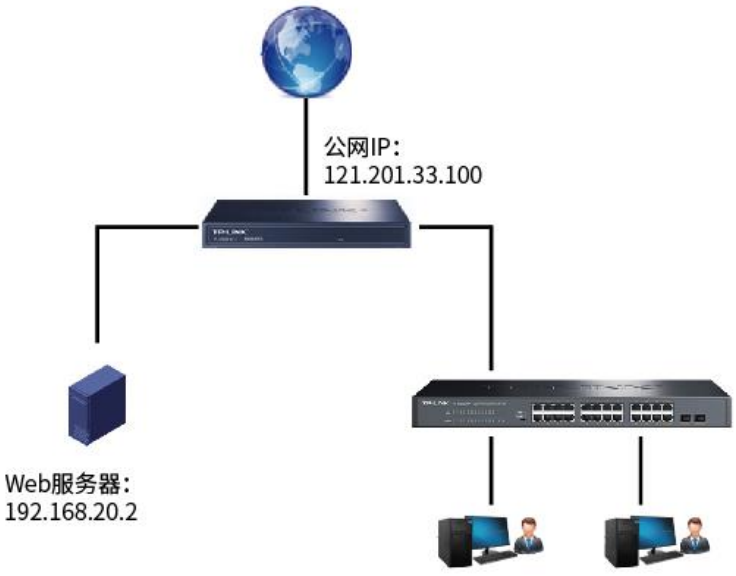

| | |
|---|---|
| 出接口 | 一对一 NAT 规则只允许选择静态 IP 的出接口。<br>当出接口从静态 IP 更改为非静态 IP，对应出接口的已配置的一对一 NAT 规则会被自动禁用。 |
| 映射前/后地址 | 规则生效的地址对象。映射前/后地址不能为各个接口的广播，网段和接口 IP 地址。 |

| | |
|---|---|
| DMZ 转发 | 设置是否开启该条 NAT 映射条目的 DMZ 转发。开启 DMZ 转发后，规则生效接口收到目的 IP 地址为映射后地址的数据包时，将把数据包转发给该局域网 IP 地址。如果广域网用户需要自由的访问该局域网 IP 地址，需要开启 DMZ 转发，若不开启，安全网关将拒绝用户对该局域网 IP 地址的访问。 |

点击页面，查看更多参数信息。

## 4.3.5 一对一 NAT 配置实例

某公司有一个公网地址 121.201.33.100，内网上搭载了 Web 服务器需要对外开放，Web 服务器的内网 IP 为 192.168.20.2。现有需求将该 Web 服务器与公网 IP 一对一转换。拓扑如下：

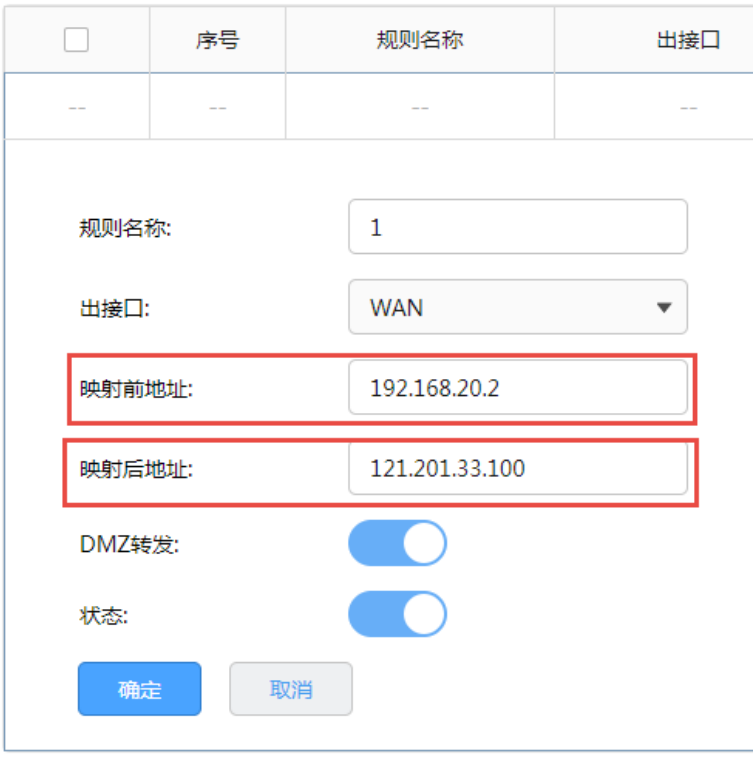



配置步骤：

1. 进入页面“基本设置 >> WAN 设置 >> WAN 设置”，接口连接方式为静态 IP，地址为 121.201.33.100。


2. 进入页面“高级功能 >> NAT 设置 >> 一对一 NAT”，点击<新增>。

3. 设置一对一 NAT 规则。



## 4.4 ALG 服务

通常情况下，局域网中的计算机共享公网地址上网时，安全网关均会对数据包做 NAT 地址转换。然而，对于一些特殊的协议，例如访问服务器 FTP、VPN 隧道连接等，此类应用的数据包中的内容可能包含 IP 地址或端口信息，这些内容不能被 NAT 进行有效地转换，因此此类应用在通过安全网关 NAT 时就可能会出现问题。例如，FTP 应用是由数据连接和控制连接共同完成的，而且数据连接基于的传输层端口由控制连接过程中的数据包内容动态地决定，这就需要 ALG 特性来完成数据包内容的转换，来保证后续数据连接的正确建立。下表为常见的需要 ALG 的一些应用层协议。

| 应用名称 | 应用场景 |
| --- | --- |
| FTP | 用于局域网设备使用 FTP 协议访问广域网设备时，如访问 FTP 服务器，此时需要启用 FTP ALG。 |
| H.323 | 局域网中的 IP 电话与广域网中的 IP 电话使用 H.323 协议进行通信时，需要启用 H.323 ALG。 |
| SIP | 局域网中存在 Internet 多媒体会议、IP 电话等应用是基于 SIP 协议的，需要启用 SIP ALG |
| PPTP | 用于安全网关使用 PPTP 方式进行拨号，或者提供 PPTP 隧道连接服务时，需要启用 PPTP ALG |

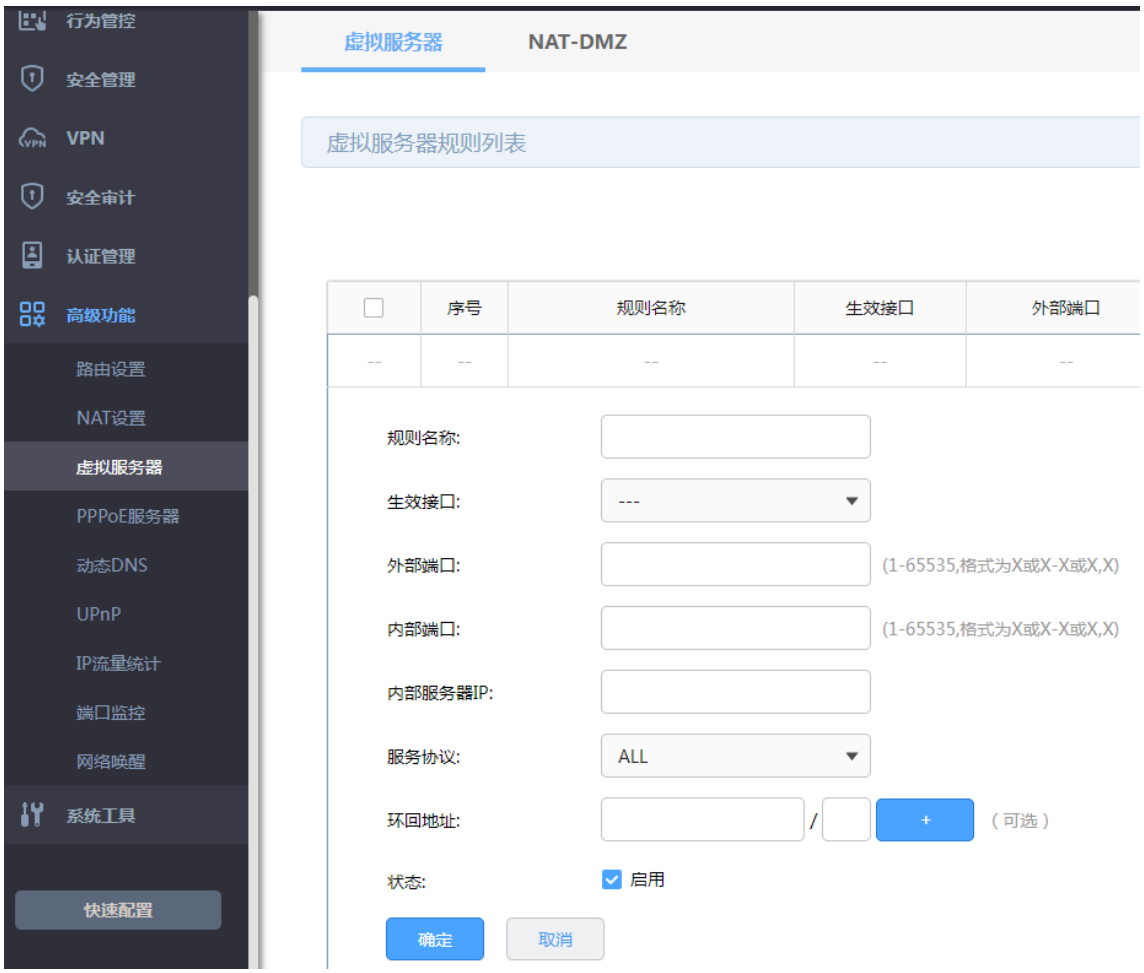
配置方法：进入页面： 高级功能 >> NAT 设置 >> ALG 服务，勾选对应 ALG 服务，点击<保存>。

# 4.5 虚拟服务器

## 4.5.1 虚拟服务器

企业在内部搭建各种服务器，如 FTP 服务器、Web 服务器、邮件服务器、监控服务器等。而这些服务器并不仅仅是针对内网用户开放的，外网的用户也需要通过互联网来访问。虚拟服务器功能可以实现将内网的服务器映射到 Internet，从而实现外网的访问。

进入页面：高级功能 >> 虚拟服务器 >> 虚拟服务器。点击<新增>，设置完成后，点击<确定>。




| | |
|---|---|
| 生效接口 | 规则生效的出接口 |
| 外部端口 | 安全网关提供给广域网的服务端口（范围）。端口组之间不允许重叠。 |
| 内部端口 | 局域网主机的服务端口。 |
| 内部服务器 IP | 局域网中建立服务的主机地址。 |

| | |
|---|---|
| 服务协议 | 触发条目生效的协议类型。选择 ALL 表示所有协议均生效。 |
| 环回地址 | 添加除 LAN 网段之外需要环回的地址段。LAN 网段默认支持环回。 |

点击页面，查看更多参数信息。

## 4.5.2 虚拟服务器配置实例

组网介绍：

企业在内部搭建各种服务器，如 FTP 服务器、Web 服务器、邮件服务器、监控服务器等。而这些服务器并不仅仅是针对内网用户开放的，外网的用户也需要通过互联网来访问。虚拟服务器功能可以实现将内网的服务器映射到 Internet，从而实现外网的访问。示意网络拓扑如下：


企业需要将网页服务器对外网开放。通过虚拟服务器功能实现该需求。用户网络参数如下：

| 服务器类型 | 外部端口 | 内部端口 | 服务器 IP 地址 |
|---|---|---|---|
| Web 服务器 | 9000 | 80 | 192.168.1.10 |

外部端口是指外网用户访问服务器使用的端口，内部端口是指内部服务器开放的服务端口。

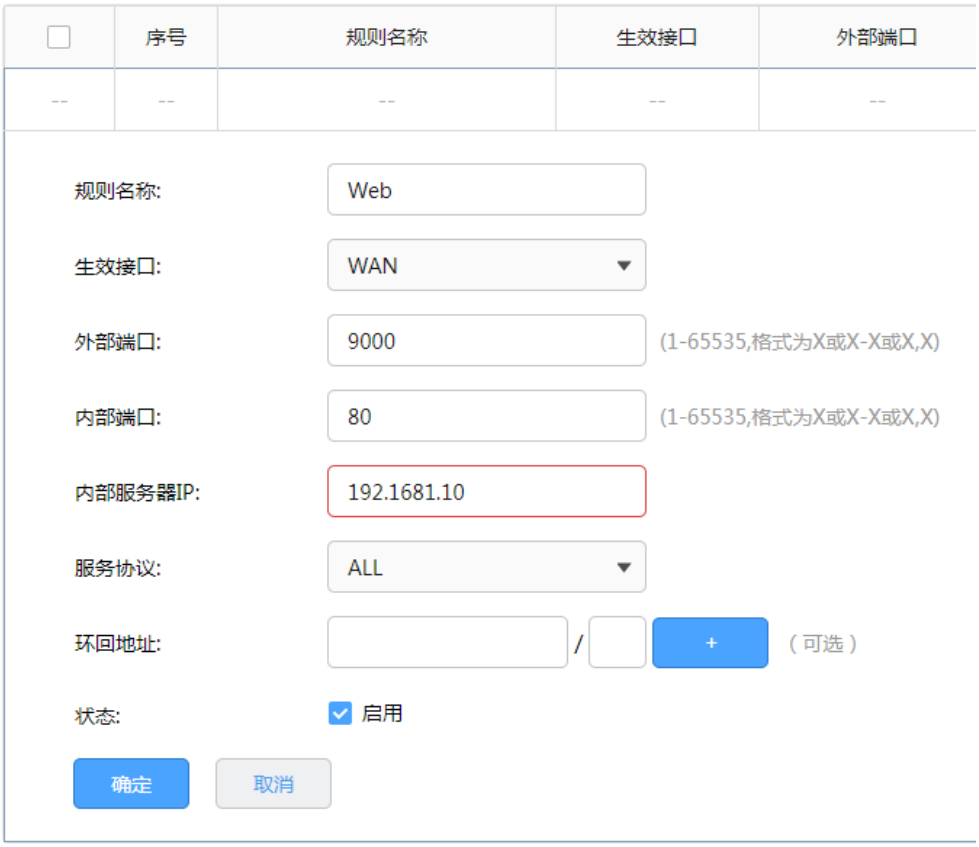
配置步骤：

1. 确认服务器搭建成功：

| | |
|---|---|
| 服务器 | 服务器设置为固定 IP 地址，默认网关为安全网关的管理地址。 |
| 防火墙 | 建议关闭服务器的防火墙与杀毒软件。 |

| | |
|---|---|
| 局域网 | 确认局域网的电脑可以通过服务器的 IP 地址和开放的端口访问到服务器。 |

2. 进入页面高级功能 >> 虚拟服务器 >> 虚拟服务器，点击<新增>，设置映射规则，设置完成后，点击<确定>。




# 4.6 NAT-DMZ

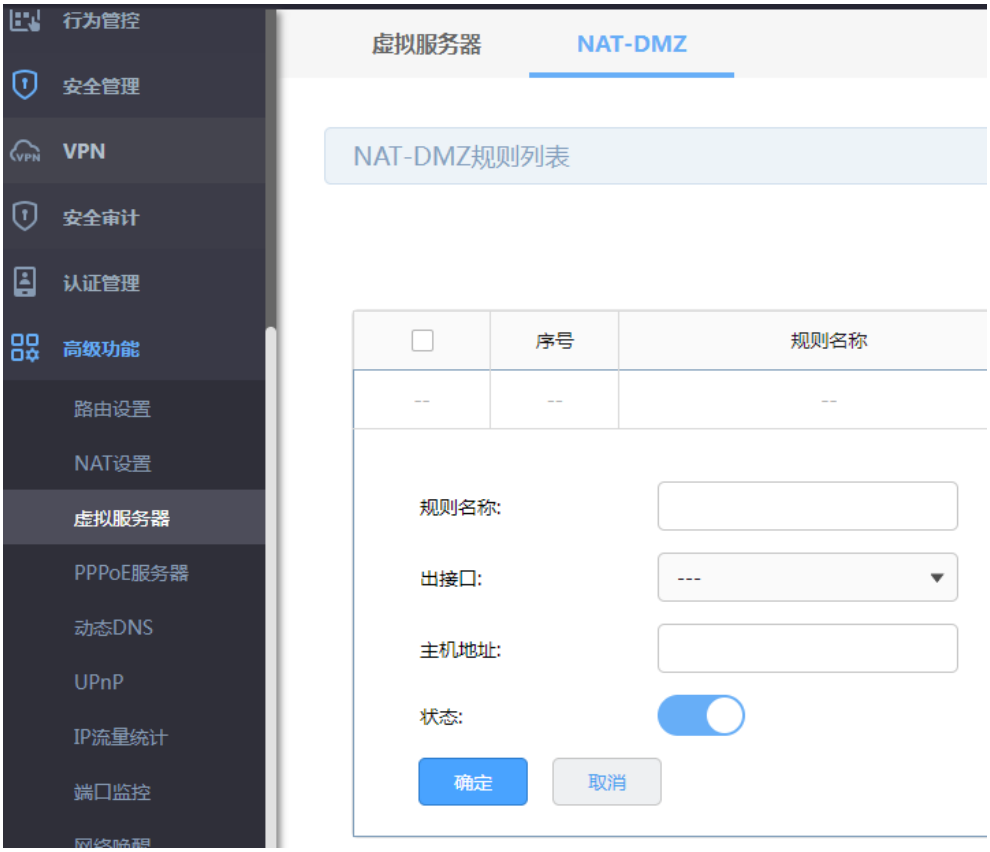
## 4.6.1 NAT-DMZ

DMZ（Demilitarized Zone，非军事区域）也称隔离区。位于 DMZ 区的主机完全暴露在广域网中，通常多用于放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。

NAT DMZ 即 DMZ 主机的 NAT 转发规则，指定接口收到数据包时，查看所有的 NAT 规则，如果没有匹配项，则将数据包进行 NAT 地址转换后发往位于 DMZ 区指定的局域网计算机上。

配置方法：

进入页面：高级功能 >> 虚拟服务器 >> NAT-DMZ。点击<新增>，选择出接口，设置主机地址，点击<确定>。




## 4.6.2 NAT-DMZ 配置实例

某小型企业需要将 Web 服务器、FTP 服务器、监控服务器对外网开放，且希望内外网都可以使用协议默认的端口进行访问。用户网络参数如下：

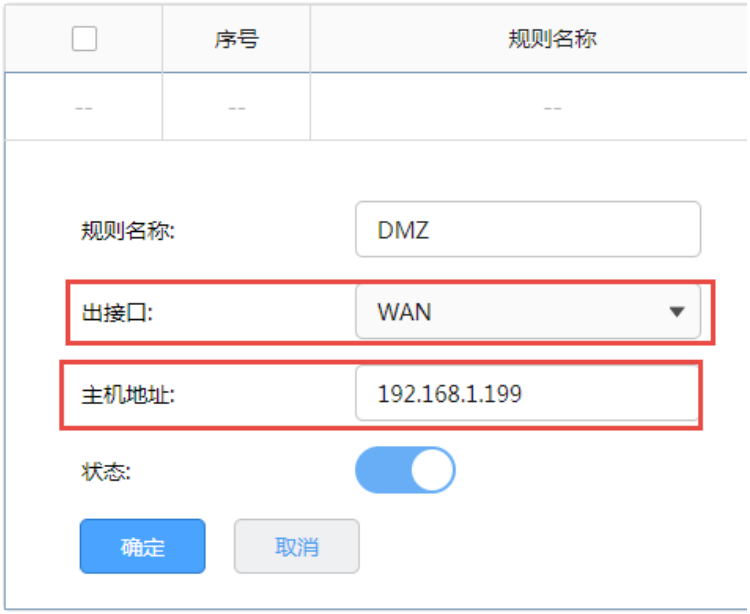
| 服务器类型 | 默认端口 | 服务器 IP 地址 |
| --- | --- | --- |
| Web 服务器 | 80/442 | 192.168.1.199 |
| FTP 服务器 | 20/21 | |
| 监控服务器 | 8888 | |

配置步骤：

1. 确认服务器搭建成功：

| | |
| --- | --- |
| 服务器 | 服务器设置为固定 IP 地址，默认网关为安全网关的管理地址。 |
| 防火墙 | 建议关闭服务器的防火墙与杀毒软件。 |
| 局域网 | 确认局域网的电脑可以通过服务器的 IP 地址和开放的端口访问到服务器。 |

2. 进入页面“高级功能 >> 虚拟服务器 >> NAT-DMZ”，点击<新增>，添加如下规则，点击<确定>。




## 4.7 查看系统路由

进入页面“高级功能 >> 路由设置 >> 系统路由”，可查看安全网关当前的路由表。

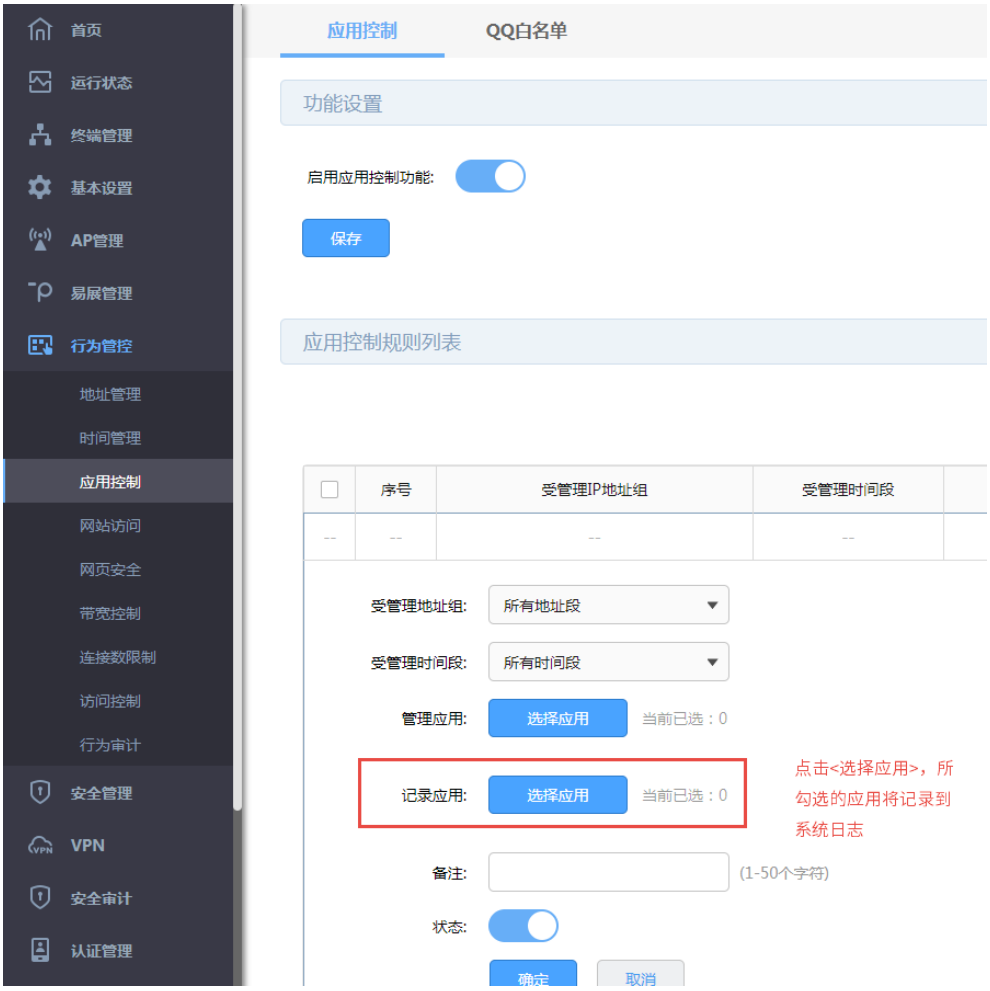
# 第5章　安全审计

TP-LINK 融合安全网关产品深度融合 TP-LINK 安全审计系统，上报网络用户的安全审计信息，增强安全管控等级。通过插件扩展的方式，对接网监数据平台，满足公共场合的无线覆盖要求。

## 5.1　行为审计模块记录到系统日志

- **将应用控制记录到系统日志**

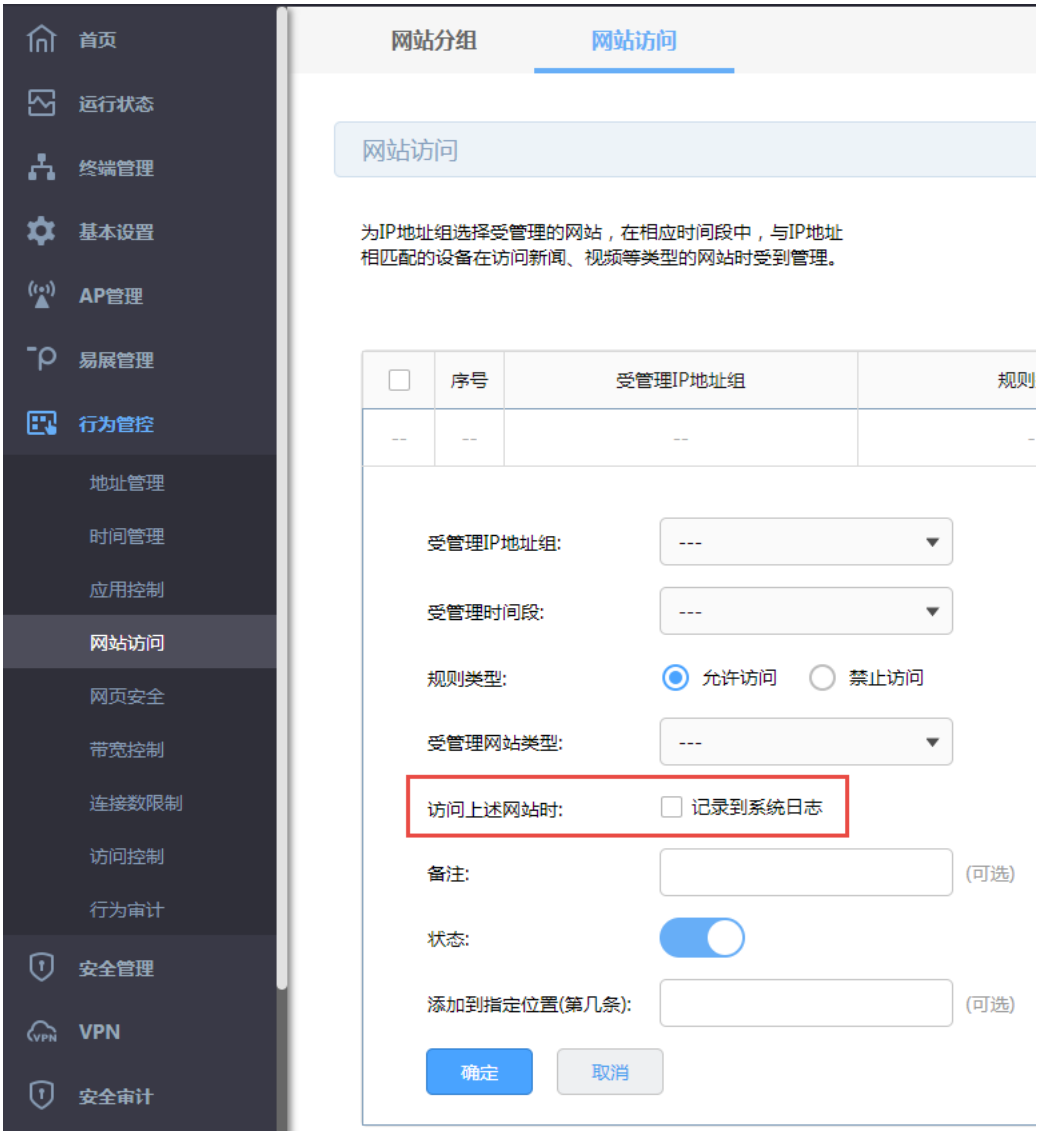
进入页面：行为管控 >> 应用控制 >> 应用控制，应用控制功能默认开启，点击<新增>，设置应用规则。在该条应用规则中点击<选择应用>，所勾选的应用将记录到系统日志。




- **将网站访问记录到系统日志**

进入页面：行为管控 >> 网站访问 >> 网站访问，点击<新增>，设置网站访问规则。

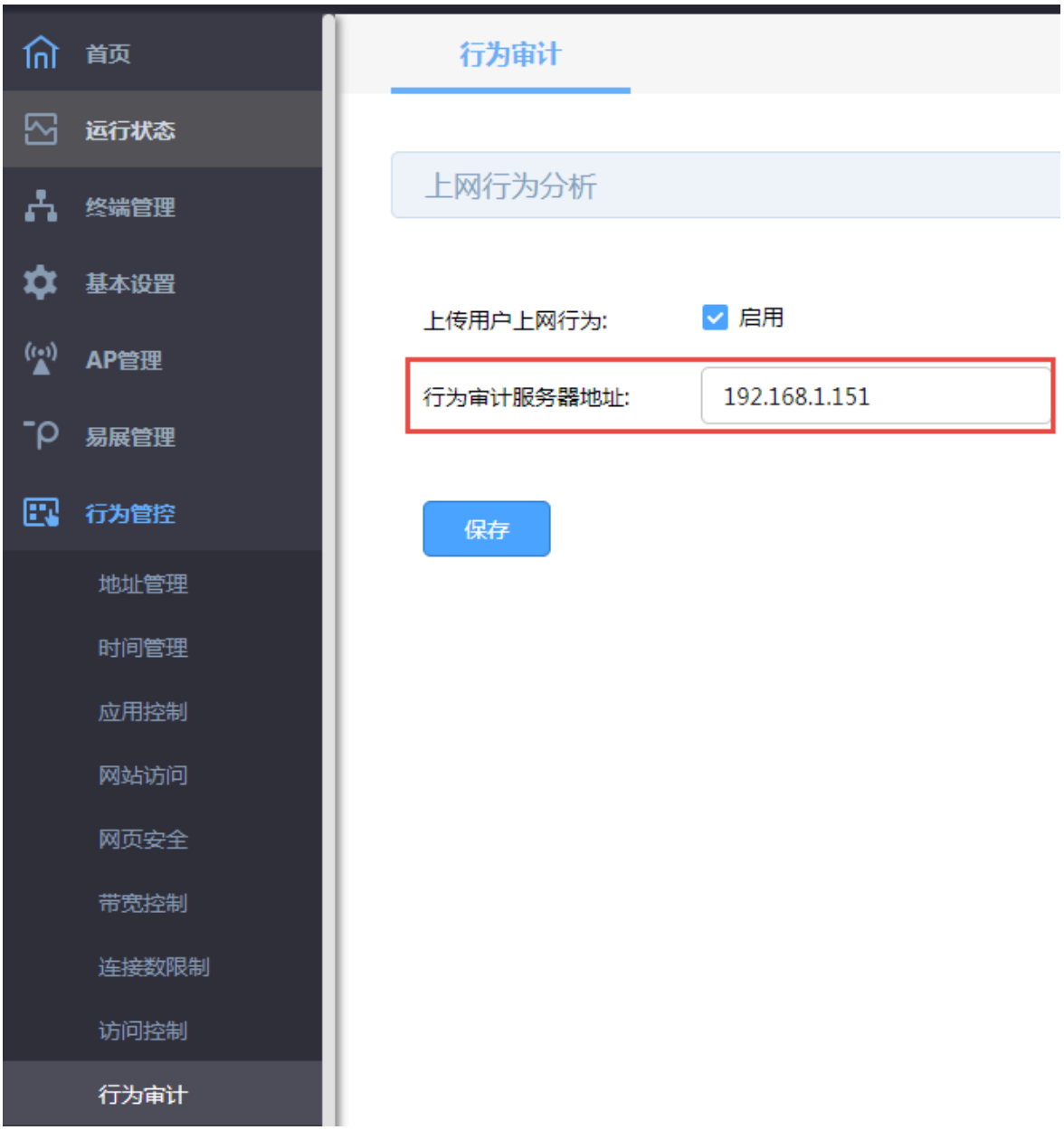
在该条应用规则中勾选<记录到系统日志>，访问上述网站将记录到系统日志。




## 5.2 行为日志发送到服务器

进入页面:行为管控 >> 行为审计 >> 行为审计。启用上传用户上网行为功能,设置行为审计服务器地址。

点击<保存>。



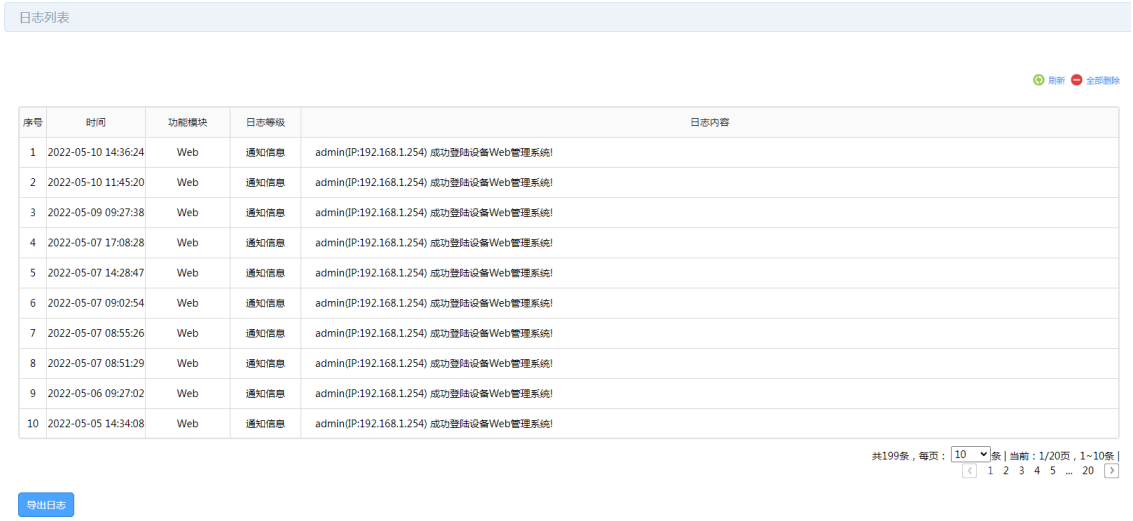

注意：

- 服务器地址，若局域网部署，直接填写服务器 IP，若公网部署请填写设备 WAN 口 IP。
- 若需要在某台主机上查看用户上网行为信息，请首先在这台主机上安装 TP-LINK 安全审计系统。

## 5.3 系统日志发送到服务器

进入页面：系统工具 >> 系统日志 >> 系统日志，可选择日志等级和模块类别，勾选“发送系统日志”，设置服务器地址，点击<保存>。

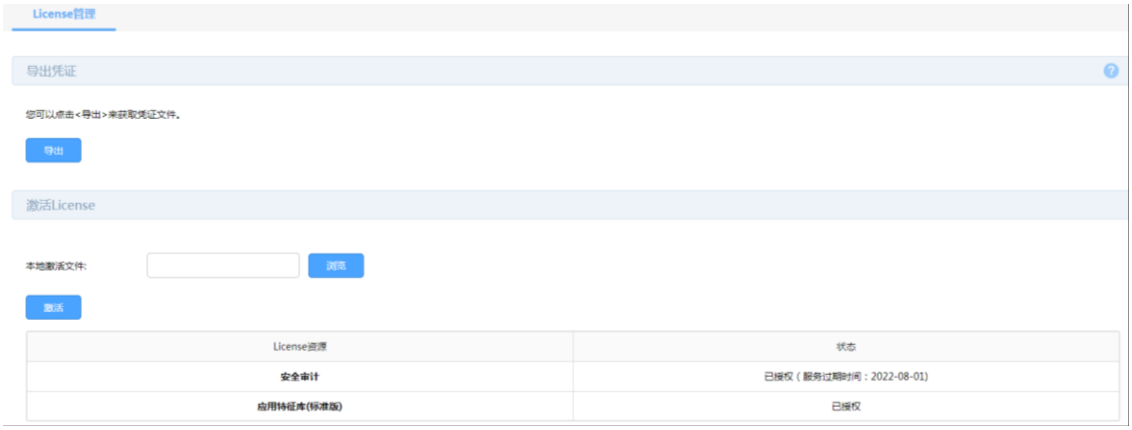

可通过日志列表查看日志信息。




# 5.4 安全审计对接网监平台

## 5.4.1 激活 License

进入页面：系统工具 >> License 管理。点击<导出>可获取凭证文件。点击<浏览>导入本地的 License 激活文件，点击<激活>文件，License 授权后可使用对应资源。



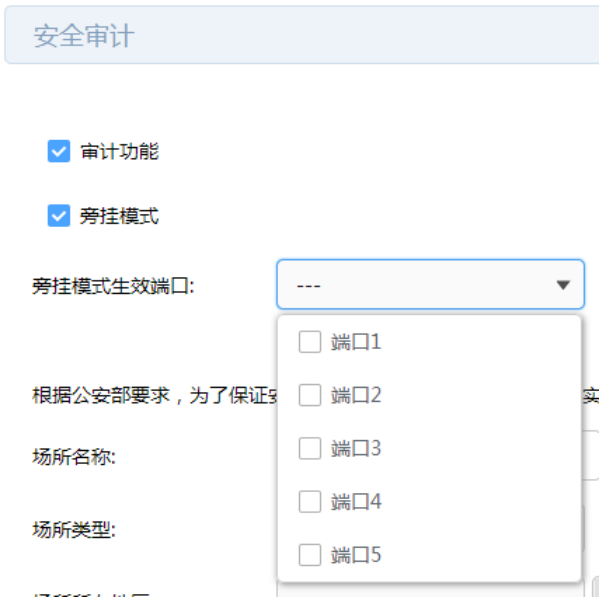

## 5.4.2 安全审计功能配置

当 License 资源已授权，进入页面：安全审计。勾选“审计功能”，准确填写各信息，点击<保存>，安全审计信息将同步至公安网监平台。

| | |
|---|---|
| 审计功能 | 使安全审计功能生效。 |
| 旁挂模式 | 旁挂模式可以针对生效接口内的所有网络流量进行审计，建议启用该模式时，当前设备仅作为安全审计功能使用。 |
| 旁挂模式生效端口 | 选择旁挂模式生效端口 |
| 场所名称 | 当前设备所在的场所名称。 |
| 场所类型 | 当前设备所在的场所类型。 |
| 场所所在地区 | 当前设备所在的场所地区。 |
| 场所详细地址 | 当前设备所在的场所详细地址。 |
| 联系人姓名 | 当前设备联系人姓名。 |
| 联系人电话 | 当前设备联系人电话。 |
| ftp 服务器地址 | 设置审计 ftp 服务器的地址。 |
| ftp 服务器端口号 | 设置审计 ftp 服务器的端口号。 |
| ftp 服务器用户名 | 设置审计 ftp 服务器的用户名。 |
| ftp 服务器密码 | 设置审计 ftp 服务器的密码。 |
| 数据产生源标识 | 系统所属机构的标识（如某省厅，某地市等），每个节点标识由公安机关机构（GA/T 380-2011）代码前六位统一确定。例如：320000 表示江苏省厅；320100 表示南京市局。可以查询中国行政区划代码进行参考。 |
| 数据传输目的标识 | 系统所属机构的标识（如某省厅，某地市等），每个节点标识由公安机关机构（GA/T 380-2011）代码前六位统一确定。例如：320000 表示江苏省厅；320100 表示南京市局。可以查询中国行政区划代码进行参考。 |

点击页面，查看更多页面设置参数信息。

勾选旁挂模式，选择生效端口，可以针对生效端口内的所有网络流量进行审计，建议启用该模式时，当前设备仅作为安全审计功能使用。




## 5.5 开启安全审计功能

该功能主要应用场景为，网络中使用本机来做短信认证，同时有安全审计网关用于对接公安网监平台，开启此功能可将用户的认证信息和上下线信息发送给安全审计网关，如果本机同时做短信认证和网监对接，则不需要开启此功能。

进入页面：系统工具 >> 系统日志 >> 安全审计，勾选安全审计功能开关，输入支持安全审计功能路由器的 LAN 口 IP 地址。

# 第6章　终端管理

## 6.1　限制终端上网速度

进入页面：终端管理 >> 终端管理，可查看当前设备所连终端。


说明：

- 请确认 IP 流量统计功能已经开启，否则将无法查看到正确的上行速率和下行速率。IP 流量统计功能设置可查看 13.5 IP 流量统计。

点击，选择限速，设置最大上/下行速率。设置完成后点击<确定>。

## 6.2 限制终端上网时间

进入页面：终端管理 >> 终端管理，可查看当前设备所连终端。


说明：

- 请确认 IP 流量统计功能已经开启，否则将无法查看到正确的上行速率和下行速率。IP 流量统计功能设置可查看 13.5 IP 流量统计。

点击，选择限速，设置“允许上网时间”，可选择日历设置或手动设置。，设置完成后点击<确定>。


## 6.3 黑名单管理

加入黑名单的终端将无法上网。

进入页面：终端管理 >> 终端管理，可查看当前设备所连终端，点击 ，选择限速，点击<移入黑名单>，在跳出弹窗中点击<确定>。


说明：

- 请确认 IP 流量统计功能已经开启，否则将无法查看到正确的上行速率和下行速率。IP 流量统计功能设置可查看 13.5 IP 流量统计。

进入页面：终端管理 >> 黑名单，可查看被禁止上网的设备。点击<恢复上网>，终端将从黑名单中移除，可以上网。

# 第7章　AP 管理

网关路由器能自动发现所有工作在瘦 AP（FIT AP）模式下的 TP-LINK AP，并对 AP 进行统一配置和管理。


## 7.1　AP 设置

### 7.1.1 AP 设置

本部分主要介绍全局开启 AP 管理功能，查看 AP 列表，AP 升级和配置 AP 参数。

进入 AP 管理 >> AP 设置，勾选<启用 AP 管理功能>，点击<保存>，AP 管理功能全局开启。在“显示类型”部分，选择 AP 设备列表中显示目前在线的 AP，离线的 AP 和所有 AP。


在 AP 设备列表部分，可查看当前网络中 AP 列表，并进行 AP 管理。点击 可开启或关闭 AP 指示灯，点击 ，可对 AP 设备进行配置。

AP 配置页面如下，点击<升级>，将升级全部同型号的 AP，升级过程中请不要断电。


| | |
|---|---|
| 设备名称 | 可自定义 AP 名称。 |
| 软件升级 | 点击<升级>，升级当前软件。 |

| | |
|---|---|
| LED 默认状态 | 开启或关闭 AP 的指示灯。 |
| 最大接入设备数量 | 显示 AP 射频单元关联客户端的最大数目。 |
| 信道 | 设置 AP 射频单元实际工作的信道。 |
| 发射功率 | 设置 AP 射频单元的发射功率。 |
| 射频模式 | 设置 AP 射频单元的工作模式。 |
| 频段带宽 | 当射频模式支持 11n 或者 11ac 时，设置频段带宽。 |
| 弱信号限制 | 设置 AP 接受新客户端接入的最小信号强度值，可以设置（-95～0）内的值，单位为 dBm，建议最大值不超过-40。如果试图连接到 AP 的客户端与 AP 之间由于障碍物、距离远等原因导致相对于 AP 的信号强度低于阈值，那么将被 AP 拒绝接入。 |

点击页面，查看更多页面设置参数信息。

## 7.1.2 AP 定时重启

进入 AP 管理 >> AP 设置，在全局设置部分，开启<定时重启>功能，设置重启日期和时间。配置完成，点击<保存>。


## 7.1.3 AP 指示灯开关

进入页面：首页，点击右下角<开启指示灯>可统一开启 AP 指示灯，点击右下角<关闭指示灯>可统一关闭

指示灯。


如需关闭某一个 AP 的指示灯，进入页面 AP 管理 >> AP 设置，在 AP 设备列表中，点击点击  可开启或关闭 AP 指示灯。

## 7.2 无线网络设置

通过本页面，可以统一管理所有 AP 的无线网络，实现无线网络加密，设置无线网络定时开关等。

### 7.2.1 无线网络设置

进入页面：AP 管理 >> 无线网络设置 >> 无线网络设置。

网关路由器有两个默认无线网络，分别对应 2.4GHz 网络和 5GHz 网络。当开启多频合一功能时，2.4G 和 5G 无线网络使用相同的无线名称，在终端连接 Wi-Fi 时，路由器会根据网络情况自动为终端选择上网频段。访客网络仅支持 2.4GHz 无线网络。

开启多频合一页面如下：

关闭多频合一页面如下：


| | |
|---|---|
| 多频合一 | 开启多频合一，2.4G 和 5G 无线网络使用相同的无线名称，在终端连接 Wi-Fi 时，路由器会根据网络情况自动为终端选择上网频段。 |
| AP 设置（显示全部） | 使用当前无线网络名称的 AP 设备。 |
| 状态 | 切换该无线网络的启用或禁用状态。 |

点击页面  ，查看更多参数信息。

点击“设置”下的  ，可编辑该无线网络的设置参数。

| | |
|---|---|
| AP 设备 | 点击<绑定 AP>，设置使用该无线名称的 AP。 |
| 内部隔离 | 启用内部隔离，可以使连接到 AP 的无线终端不能互相通信，此功能不能跨 AP 生效。 |
| 隐藏无线网络 | 启用隐藏无线网络，局域网中无线终端将搜不到该无线名称。 |
| 加密方式 | 用于无线网络连接时的加密方式，有三种加密方式可选。<br>不设密码：无线终端无需密码即可连接到 AP 上。<br>WPA-PSK/WPA2-PSK(推荐)：使用 WPA2-PSK/WPA-PSK 加密方式，该加密方式无需自设认证服务器，设置无线密码即可。<br>WPA/WPA2:使用 WPA/WPA2 加密方式，该加密方式需要自行配置 Radius 服务器进行相关认证。<br>WPA2-PSK/WPA3-SAE：基于共享密钥的 WPA2 或 WPA3 模式 |
| 无线密码 | 选择 WPA-PSK/WPA2-PSK 加密时连接无线网络的密码，由 8-63 个 ASCII 码字符或 8-64 个十六进制字符组成。 |

点击页面，查看更多参数信息。

在无线网络设置部分，点击<新增>，添加新的无线网络。该无线网络自动绑定所有 AP 页面如下：

该无线网络手动选择 AP 页面如下：


| | |
|---|---|
| 无线网络名称 | 设置无线网络名称。 |
| AP 设备 | 选择自动绑定所有 AP 或手动选择 AP |
| 射频选择 | 选择无线网络应用的频段：<br>2.4G1：2.4G 频段第一个射频，所有 AP 均拥有此射频。<br>2.4G2：2.4G 频段第二个射频，四频高密度 AP 拥有此射频。<br>5G1：5G 频段第一个射频，所有双频 AP 均拥有此射频。<br>5G2：5G 频段第二个射频，三频以上高密度 AP 拥有此射频。 |
| 绑定 VLAN | 设置该无线网络绑定的 VLAN，仅在接入交换机时填写对应 VLAN，否则将导致错误。 |
| AP 列表 | 点击<绑定 AP>，设置使用该无线名称的 AP。 |
| 内部隔离 | 启用内部隔离，可以使连接到 AP 的无线终端不能互相通信，此功能不能跨 AP 生效。 |

| | |
|---|---|
| 隐藏无线网络 | 启用隐藏无线网络，局域网中无线终端将搜不到该无线名称。 |
| 加密方式 | 用于无线网络连接时的加密方式，有三种加密方式可选。<br>不设密码：无线终端无需密码即可连接到 AP 上。<br>WPA-PSK/WPA2-PSK(推荐)：使用 WPA2-PSK/WPA-PSK 加密方式，该加密方式无需自设认证服务器，设置无线密码即可。<br>WPA/WPA2:使用 WPA/WPA2 加密方式，该加密方式需要自行配置 Radius 服务器进行相关认证。<br>WPA2-PSK/WPA3-SAE：基于共享密钥的 WPA2 或 WPA3 模式 |
| 无线密码 | 选择 WPA-PSK/WPA2-PSK 加密时连接无线网络的密码，由 8-63 个 ASCII 码字符或 8-64 个十六进制字符组成。 |

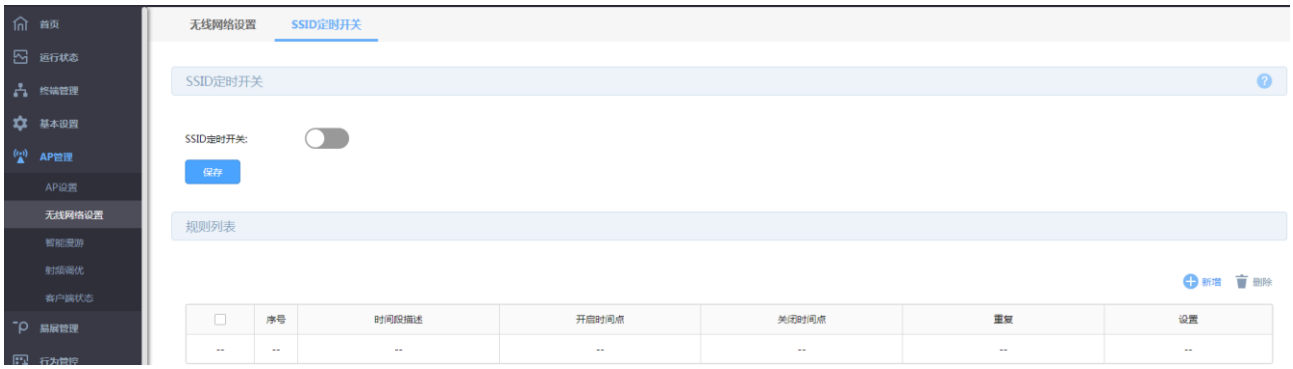
点击页面，查看更多参数信息。

说明：

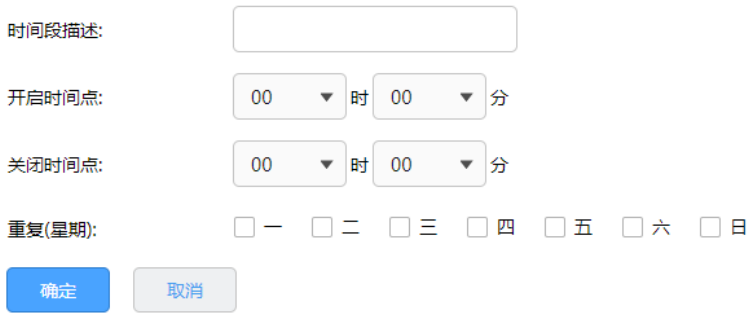
- 默认无线网络不能删除，新增的无线网络支持删除功能。

## 7.2.2 SSID 定时开关

进入页面：AP 管理 >> 无线网络设置 >> SSID 定时开关，开启<SSID 定时开关>功能，点击<保存>。



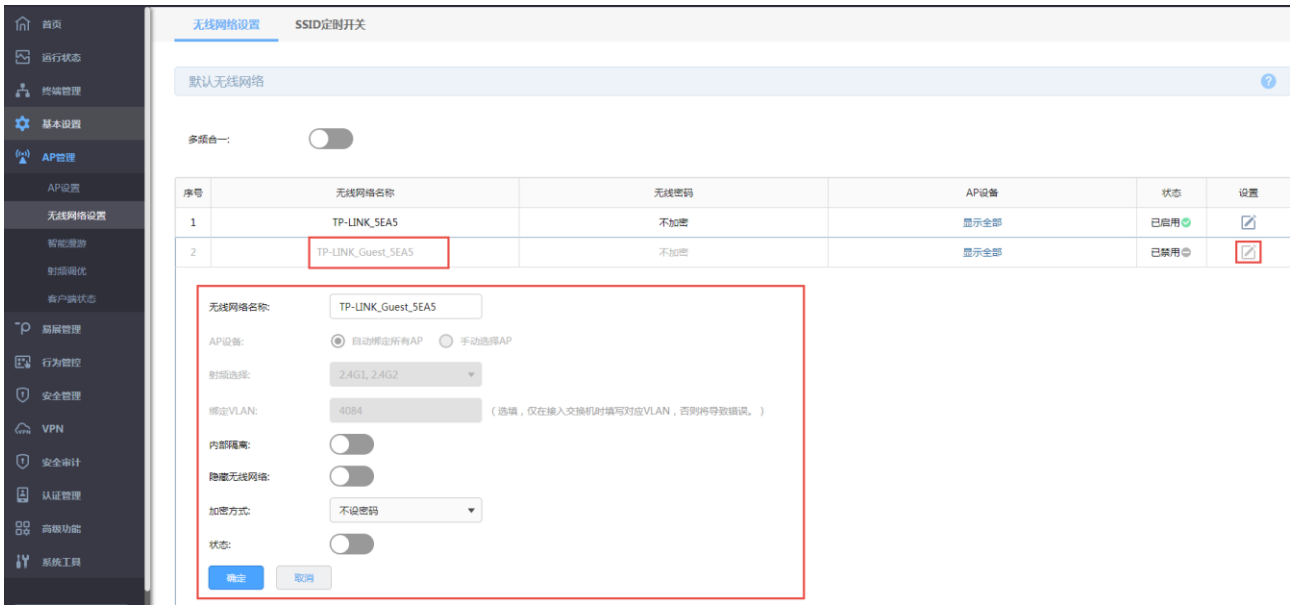

点击<新增>，添加新的定时开关规则，设置时间段名称、开启时间点、结束时间点和每周重复的时间，点击<确定>。




## 7.2.3 访客网络设置

方法一：进入页面：首页，开启访客网络，设置无线名称和无线密码，点击<保存>。


方法二：进入页面：AP 管理 >> 无线网络设置 >> 无线网络设置，在“默认无线网络”部分可发现 TP-LINK_Guest_XXXX 访客网络条目，点击  ，可对访客网络进行编辑。



# 7.3 智能漫游

## 7.3.1 智能漫游

本栏用于配置智能漫游的参数，以调节不同环境下无线终端的漫游效果。智能漫游的作用在于，对于无线体验较差的终端，AC 主动选取更优的候选 AP，并建议或迫使终端切换到所选择的候选 AP 上，以改善无线上网体验。

进入页面：AP 管理 >> 智能漫游。


802.11k/v/r 快速漫游　　启用/禁用 802.11k/v/r 快速漫游功能。

| | |
|---|---|
| 检测漫游阈值类型 | 配置主动触发用户漫游的检测策略。基于信号强度：在信号强度低于阈值时触发终端漫游；基于速率：在终端速率低于阈值时触发终端漫游。同时启用时，只要满足其中一个条件，就会触发终端漫游。。 |
| 触发漫游 RSSI 阈值 | 当终端的信号强度低于所设阈值时，将主动触发终端漫游。触发漫游 RSSI 阈值不能小于弱信号用户下线阈值。 |
| 弱信号用户下线 | 启用/禁用弱信号用户踢除功能，启用并设置踢除阈值，将在终端有更合适的目标 AP 可漫游，且信号强度低于设置的踢除阈值时，踢除终端，以迫使终端连接到体验更好的 AP 上。弱信号用户下线阈值不能大于触发漫游 RSSI 阈值。 |

点击页面，查看更多参数信息。

点击<高级设置>，配置更多漫游参数。


| | |
|---|---|
| 漫游阈值检查周期 | 检测终端 RSSI 或速率的时间间隔。 |
| 漫游差值 | 触发终端主动漫游的信号强度差值，只有当邻居 AP 的信号强度减去当前连接 AP 的信号强度大于漫游差值时，才建议终端进行主动漫游。。 |
| 终端禁止接入时间 | 当触发终端进行主动漫游时，将在非漫游目标的 AP 上设置黑名单，在终端禁止接入时间范围内不让终端接入。 |

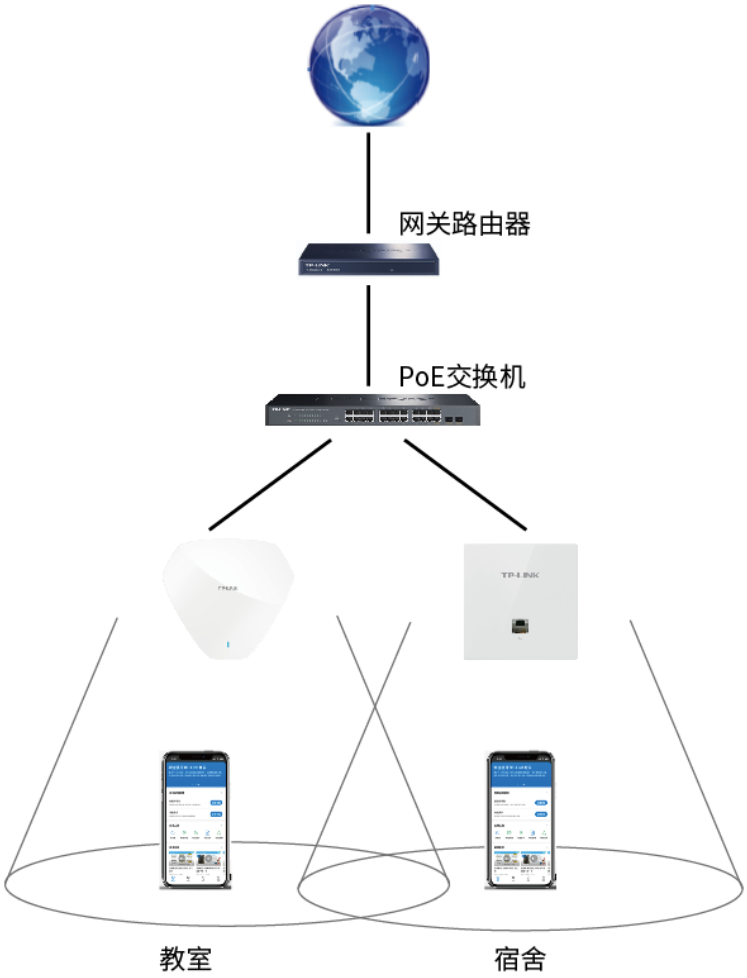
| | |
|---|---|
| 终端探测上报 | 开启时 AP 会探测周围终端信息并上报给 AC，AC 根据这些信息构建在线终端的 AP 邻居表，对不支持 802.11k 的终端漫游有辅助作用。 |

点击页面，查看更多参数信息。

## 7.3.2 智能漫游配置实例

需求介绍：随着手机、平板和电脑等终端的使用率日益增长，人们对无线的需求愈来愈大，对无线使用体验需求也愈来愈高，而无线漫游则是无线使用体验的重要组成部分。

网络拓扑如下：




无线漫游条件：

(1) 无线网络覆盖时多个 AP 都配置了相同的 SSID 和密码；

(2) 不同 AP 之间信号覆盖范围有一定的重叠；

(3) 无线终端在无线网络覆盖区域内移动。

配置步骤：

进入网关路由器管理界面，点击“AP 管理 >> 智能漫游”设置智能漫游参数。


# 7.4 射频调优

## 7.4.1 射频调优

TP-LINK 的射频调优功能可以实现一键自动规划 AP 的信道和功率，调优过程 5 分钟内即可完成，智能减少 AP 之间的信号干扰。射频调优是通过动态信道分配（Dynamic Channel Assignment，DCA）和发射功率调整（Transmit Power Control，TPC）实现统一对 AP 的信道和功率进行规划，尽可能的提高覆盖率，减少整个系统的信道干扰，从而提高整个无线网络的上网体验。


射频调优的工作过程主要分为三个步骤，分别为收集邻居关系、动态信道调整、发射功率调整。

- **收集邻居关系**

控制器下发收集邻居关系的命令后，所有 AP 工作在同一信道并周期性发送特定的报文，所有 AP 将监听到的邻居信息上报给控制器进行后续处理。

- **动态信道调整**

控制器根据收集到的邻居关系，通过 DCA 算法得到一个最优的 AP 信道划分结果，并将结果下发给所有 AP。

- **发射功率调整**

控制器根据邻居关系、动态信道调整的结果，通过 TPC 算法得到一个最优的 AP 功率划分结果，尽可能的提高覆盖率，同时减少整个系统的同信道干扰，并将结果下发给所有的 AP。

进入页面：AP 管理 >> 射频调优，可以通过点击<立即调优>按钮立即进行射频调优。


| | |
|---|---|
| 信道调优 | 开启/关闭信道调优功能。 |
| 频段带宽 | 设置对应频段（2.4G/5G）的调优频段带宽。 |
| 2.4G/5G 信道集合 | 设置对应频段（2.4G/5G）的调优信道集合。 |
| 功率调优 | 开启/关闭功率调优功能。注意：只有信道调优功能开启时，才能开启功率调优功能。 |

| | |
|---|---|
| 覆盖阈值 | 当开启功率调优时，对于 AP 的布放场景不同，AP 布放距离不同或 AP 布放高度不同，TPC 的覆盖阈值不同，实际使用时需要根据 AP 的实际布放调整 AP 的 TPC，以使 TPC 的结果能达到最优的覆盖效果。阈值越大，TPC 调整的功率值会整体提高。 |
| 最大/小功率 | 设置功率调优时，AP 允许调节的最大/最小功率。配置最大调优功率值和最小调优功率值后，AP 在进行功率调优后，最终生效的功率会在这两个值之间。 |
| 定时调优 | 开启/关闭定时射频调优功能，并设置定时调优的时间。 |

点击页面  ，查看更多参数信息。

 注意：

- 射频调优过程需要大约五分钟时间，且会导致 AP 无线中断。
- 定时调优的时间须与 AP 定时重启的时间间隔至少 10 分钟。
- 只有信道调优功能开启时，才能开启功率调优功能。。

## 7.4.2 射频调优配置实例

需求介绍：在一些酒吧、餐厅、宿舍等密集接入环境下，每个 AP 下都可能存在较大的无线流量，AP 与 AP 之间可能就存在较大的无线干扰，从而影响到整体网络的使用体验，典型的现象就是人少的时候网络很快，使用的人一多网络就慢了。使用 TP-LINK 的射频调优功能对网络的信道进行自动规划，功率进行自动调整，将网络中的干扰降到最小，保障无线使用的体验。

网络拓扑如下：


配置方法：

1. 进入页面：AP 管理 >> 射频调优，开启信道调优，设置调优参数。2.4G 的频段带宽会统一设置为 20MHz，信道集合可以设置为 1/6/11 和 1/5/9/13；5G 的频段带宽可选设置为 20MHz 或 40MHz，信道集合可选设置为 36/44/149/157、40/48/153/161、36/48/149/161。


2. 开启功率调优，设置覆盖阈值和最大/小功率，一般保持默认即可。


3. 考虑到调优过程中 AP 会有最长 5min 无法正常使用，射频调优支持设置一个特定的时间进行定时调优，避免因为射频调优带来的断网影响。


## 7.5 客户端状态

可以通过本页面来查看客户端状态。

进入页面：AP 管理 >> 客户端状态。点击 可断开客户端与当前网络的连接，点击<刷新>可获取最新客户端列表。

# 第8章　易展管理

随着互联网技术的快速发展，需求无线网络覆盖的地方越来越多，此时出现了一些传统网络无法解决的复杂区域和快速完成组网的需要，也有个人用户不想破坏原有的装修环境来进行网络覆盖。对于一些区域来说传统网络的组网方案不仅复杂且成本较高。为了解决这些问题，TP-LINK 新推出了带有“易展”功能的 AP，能够实现快速组网，无需布线，简单实现组网，且可以替换某些传统组网，优化整个网络。

- **易展 AP**

传统的无线 AP 组网，设备众多，且需要专业人员施工，费时、费力、费钱。TP-LINK“易展”系列 AP 产品颠覆传统 AP 复杂的布线方式，通过 TP-LINK Mesh 技术，无需布线，可实现最多 8 台“易展”AP 一键无线互联，仅需简单设备单台 AP 网络配置，即可自动同步到所有 AP，让 AP 组网、管理更加省时、省力、省钱。

易展 AP 的无线 Mesh 组网模式，作为传统有线组网的扩展和补充，推荐用于终端密度不高的场所，优势在于免布线，便捷且成本低，对于带机量要求较高的高密度场景，建议采用传统有线组网方式。

- **易展 AP 组网**


- **如何辨别易展 AP**

产品型号中有“易展”二字，或设备上有“易展”按键的 AP 产品就是易展 AP。

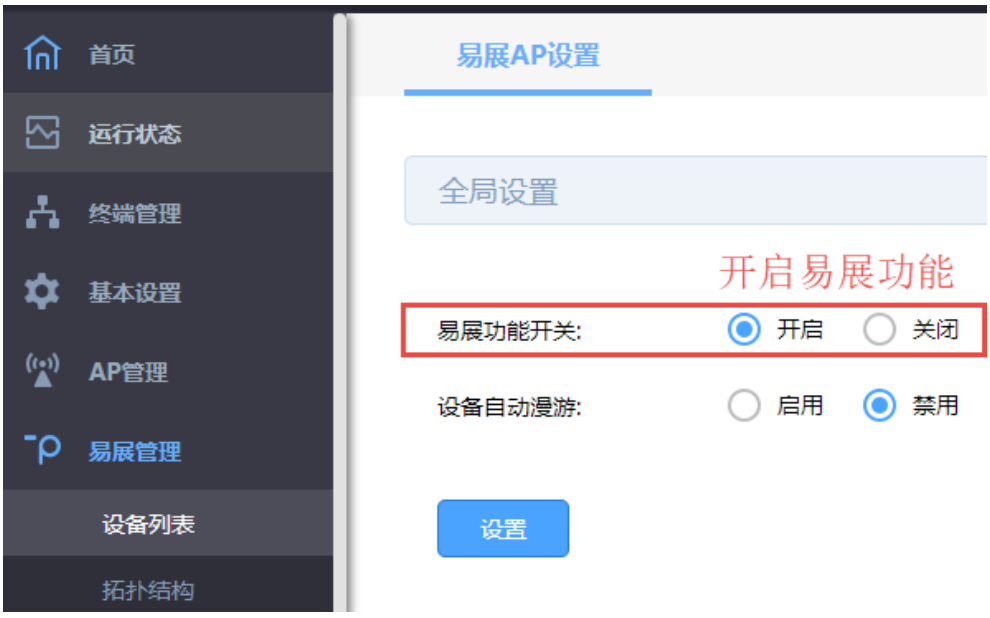
下面介绍如何使用安全融合网关产品添加和管理易展 AP。

## 8.1 添加易展 AP

请将易展 AP 处于 FIT 模式，并按照如下步骤添加易展 AP。

1. 进入页面：AP 管理 >> AP 设置，勾选<启用 AP 管理功能>，点击<保存>。

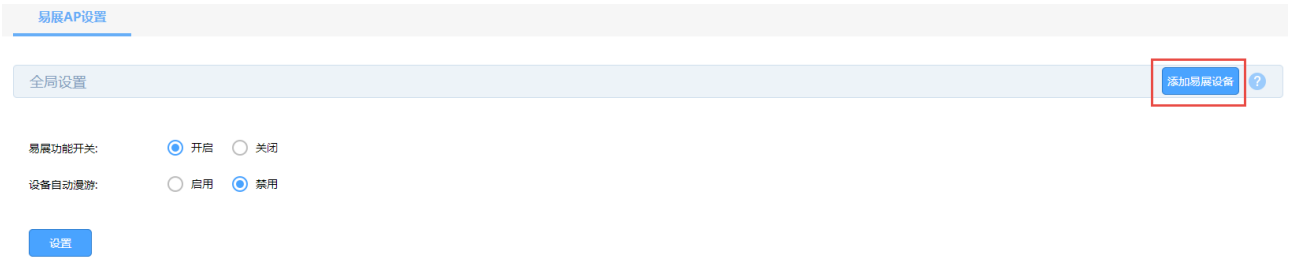

2. 进入页面：易展管理 >> 设备列表 >> 易展 AP 设置，在“全局设置”部分，开启“易展功能开关”，点击<设置>。易展 AP 将自动识别并工作在 FIT 模式，此时连接的 AP 作为主 AP。




设备自动漫游　　功能开启后，当前端主设备离线或与主设备连接质量较差时，子设备将自动尝试切换至连接质量更好的主设备。切换后，子设备将自动从新的主设备同步无线服务及射频配置。

点击页面，查看更多参数信息。

3. 点击页面右上角<添加易展设备>，同时按下易展子 AP 上的“易展”按键。




注意：

- 易展子 AP 必须为未配置过的出厂状态，若易展子 AP 已配置过请长按 reset 按键恢复出厂设置状态。

4. 易展主 AP 会自动搜索发现周围待配对的易展子 AP，发现设备后点击<添加>，等待一会儿即可完成配对。如需批量添加多个易展子 AP，点击<全部添加>即可。


5. 在“易展主 AP 设备”和“易展子 AP 设备”列表中，可查看当前网络中的易展主/子 AP 设备。

# 8.2 管理易展 AP

进入页面：易展管理 >> 设备列表 >> 易展 AP 设置，在易展主 AP 设备列表和易展子 AP 设备列表中，可对易展 AP 进行多种管理操作。


点击  ，可开启或关闭易展 AP 指示灯。

点击  ，可编辑主子设备信息。


设备名称　　可自定义 AP 名称。

软件版本　　点击<升级>，升级当前软件。

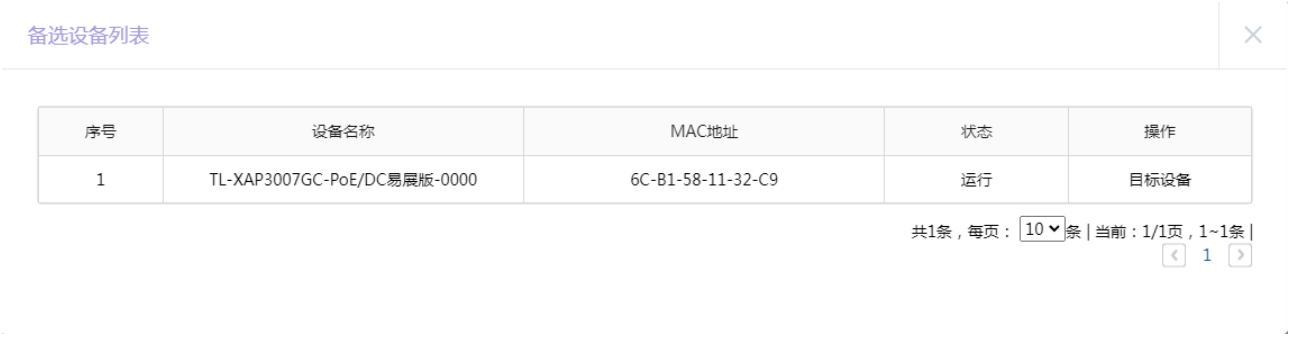
| | |
|---|---|
| LED 默认状态 | 开启或关闭 AP 的指示灯。 |
| 最大接入设备数量 | 显示 AP 射频单元关联客户端的最大数目。 |
| 信道 | 设置 AP 射频单元实际工作的信道。 |
| 发射功率 | 设置 AP 射频单元的发射功率。 |
| 射频模式 | 设置 AP 射频单元的工作模式。 |
| 频段带宽 | 当射频模式支持 11n 或者 11ac 时，设置频段带宽。 |
| 弱信号限制 | 设置 AP 接受新客户端接入的最小信号强度值，可以设置（-95～0）内的值，单位为 dBm，建议最大值不超过-40。如果试图连接到 AP 的客户端与 AP 之间由于障碍物、距离远等原因导致相对于 AP 的信号强度低于阈值，那么将被 AP 拒绝接入。 |

点击页面  ，查看更多页面设置参数信息。

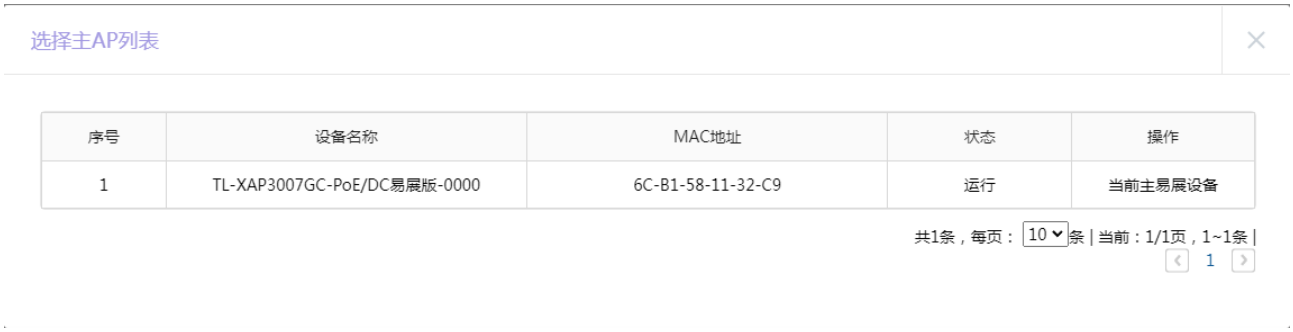
点击  ，可断开与易展 AP 的连接。

点击  ，可对易展 AP 重新启动。

在易展主 AP 列表，点击  ，主设备冗备功能，可以通过此功能，将某个主 AP 的设备备份到新加入的主 AP，主要是用于主 AP 故障/替换的场景。




在易展子 AP 列表，点击  ，子设备更换主设备功能，灵活调整组网，可以通过手动设置将子 AP 关联到信号更好的主 AP 上。




## 8.3 查看网络拓扑结构

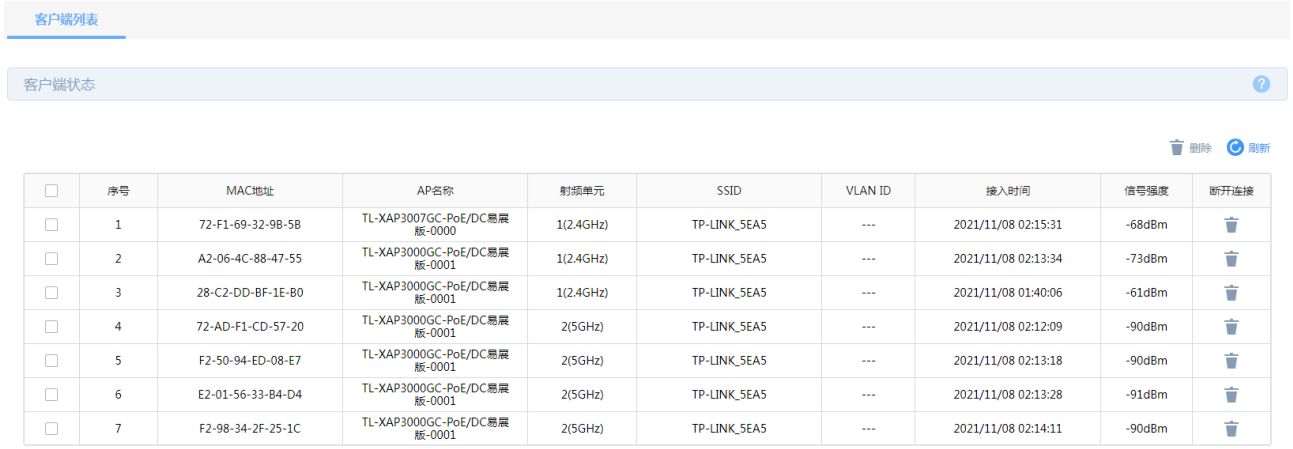
进入页面易展管理 >> 拓扑结构，查看当前网络拓扑结构。


说明：

- 点击页面右上角<添加易展 AP>可添加易展 AP 至当前拓扑，详细添加步骤可参考 8.1 添加易展 AP。

## 8.4 查看客户端列表

进入页面易展管理 >> 客户端列表，查看接入易展 AP 的终端设备信息。点击 可断开客户端与当前网络的连接，点击<刷新>可获取最新客户端列表。




| 序号 | MAC地址 | AP名称 | 射频单元 | SSID | VLAN ID | 接入时间 | 信号强度 | 断开连接 |
|---|---|---|---|---|---|---|---|---|
| 1 | 72-F1-69-32-9B-5B | TL-XAP3007GC-PoE/DC易展版-0000 | 1(2.4GHz) | TP-LINK_5EA5 | --- | 2021/11/08 02:15:31 | -68dBm | |
| 2 | A2-06-4C-88-47-55 | TL-XAP3000GC-PoE/DC易展版-0001 | 1(2.4GHz) | TP-LINK_5EA5 | --- | 2021/11/08 02:13:34 | -73dBm | |
| 3 | 28-C2-DD-BF-1E-B0 | TL-XAP3000GC-PoE/DC易展版-0001 | 1(2.4GHz) | TP-LINK_5EA5 | --- | 2021/11/08 01:40:06 | -61dBm | |
| 4 | 72-AD-F1-CD-57-20 | TL-XAP3000GC-PoE/DC易展版-0001 | 2(5GHz) | TP-LINK_5EA5 | --- | 2021/11/08 02:12:09 | -90dBm | |
| 5 | F2-50-94-ED-08-E7 | TL-XAP3000GC-PoE/DC易展版-0001 | 2(5GHz) | TP-LINK_5EA5 | --- | 2021/11/08 02:13:18 | -90dBm | |
| 6 | E2-01-56-33-B4-D4 | TL-XAP3000GC-PoE/DC易展版-0001 | 2(5GHz) | TP-LINK_5EA5 | --- | 2021/11/08 02:13:28 | -91dBm | |
| 7 | F2-98-34-2F-25-1C | TL-XAP3000GC-PoE/DC易展版-0001 | 2(5GHz) | TP-LINK_5EA5 | --- | 2021/11/08 02:14:11 | -90dBm | |

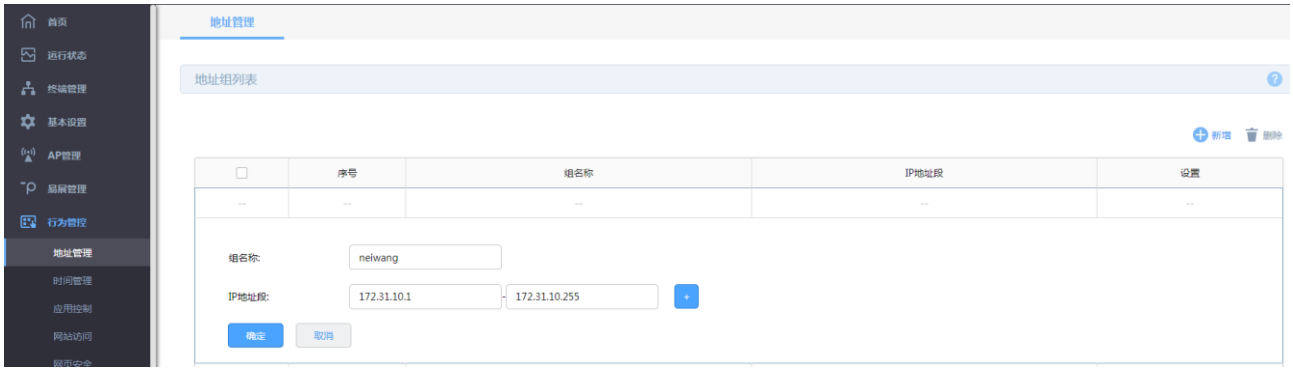
# 第9章　行为管控

## 9.1　对象管理

### 9.1.1 地址组管理

设置地址组，每个地址组包含不同 IP 地址段，引用该地址组的规则在该地址段内均会生效。一个地址组可包含多个不同的 IP 地址段。

进入页面：行为管控 >> 地址管理，点击<新增>，输入组名称和 IP 地址段，点击<确定>。



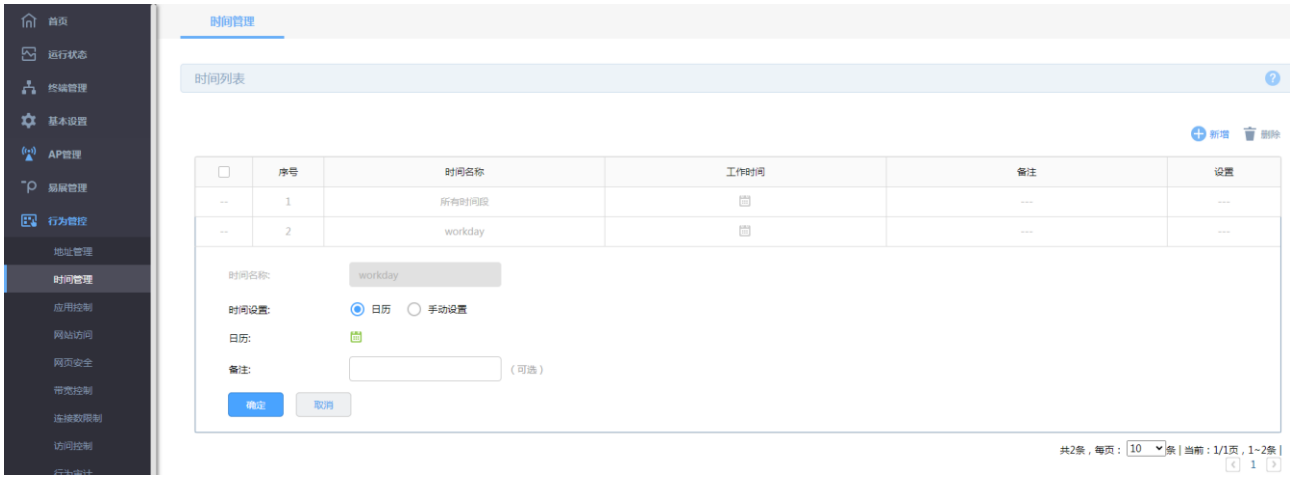

注意：

- 地址组一旦在其他地方被引用则无法在本页面被删除，除非解除引用。

### 9.1.2 时间管理

设置时间对象，每个时间对象包含不同时间段，引用该时间对象的规则在该时间段内均会生效。一个时间对象可包含多个不同的时间段。

进入页面：行为管控 >> 时间管理，点击<新增>，输入时间对象名称和时间段，点击<确定>。

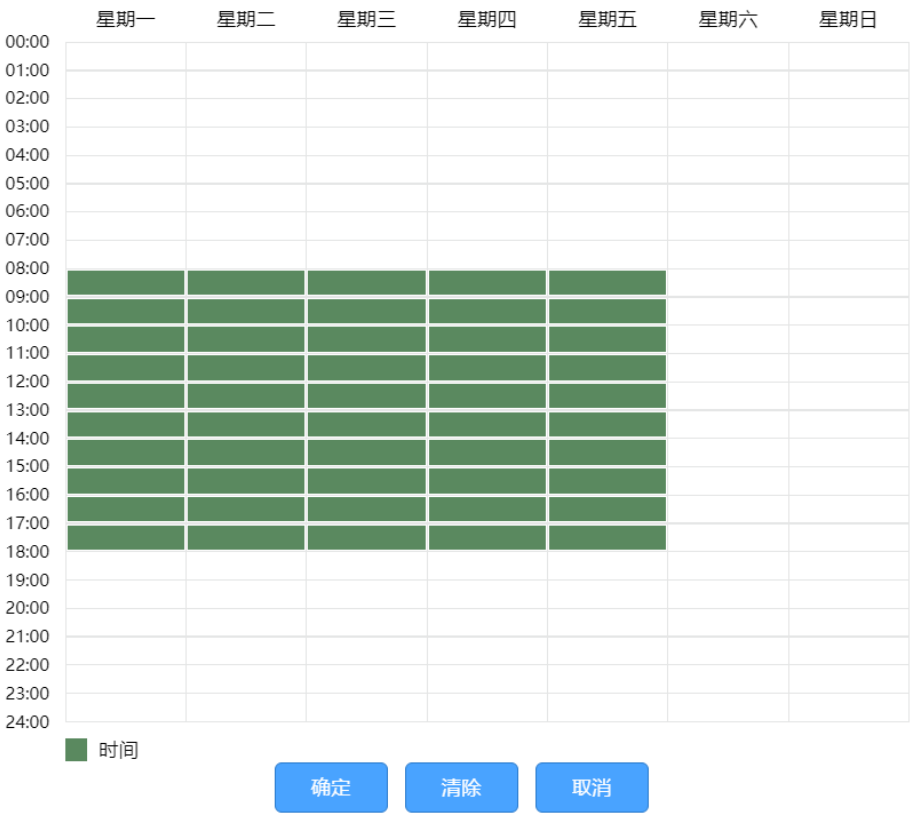



注意：

- 时间对象一旦在其他地方被引用则无法在本页面被删除，除非解除引用。

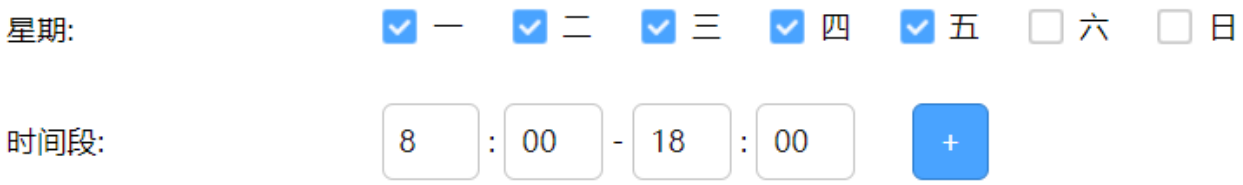
➢ **日历时间设置**

在“时间设置”中选择<日历>，点击 ，点击所选择的时间段即可。例如下，选择星期一到星期五 8：00 到 18：00 的时间段。点击<确定>，保存配置。




➢ **手动设置时间**

在“时间设置”中选择<手动设置>，勾选生效的日期，设置生效的时间段。例如下，选择星期一到星期五 8：00 到 18：00 的时间段。点击<确定>，保存配置。




# 9.2 应用控制

## 9.2.1 应用控制

您可以通过本页面进行相应的应用限制。

进入页面：行为管控 >> 应用控制 >> 应用控制，开启<启用应用控制功能>，点击<保存>。

进入应用控制规则列表，点击<新增>。


| | |
|---|---|
| 受管理的地址组 | 规则生效的地址组，地址组设置请见 9.1.1 地址组管理。 |
| 受管理时间段 | 规则生效的，时间对象管理请见 9.1.2 时间管理。 |
| 管理应用: | 选择需要禁用的应用。 |

| | |
|---|---|
| 记录应用 | 选择需要记录到日志的应用。 |

点击页面，查看更多页面设置参数信息。

## 9.2.2 QQ 白名单

QQ 白名单可以管理用户对 QQ 的使用情况。

进入页面：行为管控 >> 应用控制 >> QQ 白名单，点击<新增>。


| | |
|---|---|
| 受管理 IP 地址组 | 规则生效的地址组，地址组设置请见 9.1.1 地址组管理。 |
| 受管理时间段 | 规则生效的，时间对象管理请见 9.1.2 时间管理。 |
| QQ 号码 | 设置被管理的 QQ 号码。选择当使用上述 QQ 号码时，是否记录到系统日志。 |

点击页面，查看更多页面设置参数信息。

# 9.3 网站访问控制

## 9.3.1 网站分组

通过网站分组，可集中管理一类网址。

进入页面：行为管控 >> 网站访问 >> 网站分组，点击，可修改当前网站组的组成员，点击<新增>，，设置组名称，输入可添加网站组。


| | |
|---|---|
| 组成员 | 网站分组成员，您可以同时输入多个网站进行批量添加。<br>组成员可以为域名，如 www.tp-link.com.cn,也可以在域名前面加通配符'*'，如*.tp-link.com.cn。但是'*'只允许输入在最前面，而不能夹杂在域名中间或后面。 |
| 文件路径 | 您可以通过文件导入的形式为网站分组添加成员，文件格式为 txt 格式。 |

点击页面，查看更多页面设置参数信息。

## 9.3.2 网站访问

为 IP 地址组选择受管理的网站，在相应时间段中，与 IP 地址相匹配的设备在访问新闻、视频等类型的网

站时受到管理。

进入页面：行为管控 >> 网站访问 >> 网站访问，点击<新增>，设置网站访问规则。


| | |
|---|---|
| 受管理的 IP 地址组 | 规则生效的地址组，地址组设置请见 9.1.1 地址组管理。 |
| 受管理时间段 | 规则生效的，时间对象管理请见 9.1.2 时间管理。 |
| 规则类型 | 设置受管理 IP 地址组在受管理时间段允许访问或者禁止访问受管理网站。 |
| 受管理网站类型 | 选择需要记录到日志的应用，网站组设置见 9.3.1 网站分组。 |

点击页面 ，查看更多页面设置参数信息。

## 9.3.3 网站访问配置实例

企业网络环境中，不同部门允许访问的网页权限也不同。、如：市场部需要访问各类网站，但对游戏、视频、购物类的网站则无需求。企业安全网关的网址过滤功能可以实现对不同地址组的网页访问权限设置，从而

实现合理管控网络权限。

需求介绍：某企业需要限制公司不同部门的网络权限，需求如下：

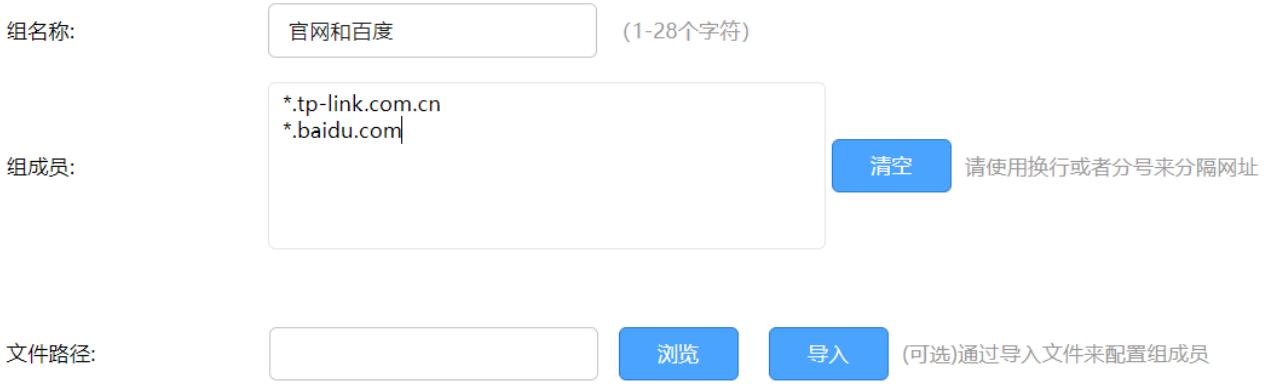
| 部门 | 网络权限 |
| --- | --- |
| 市场部 | 禁止访问视频、游戏、购物类网站 |
| 其他部门 | 仅允许访问公司网站及百度 |

设置方法：

1. 设置地址组。添加市场部和其他部门的地址组，方便后续的控制规则针对地址组进行控制。在安全网关界面，点击“行为管控 >> 地址管理”，点击<新增>，添加市场部地址组。


同样的方法添加其他部门的地址组，添加完成的地址组如下：


2. 添加网站分组，点击“行为管控 >> 网站访问 >> 网站分组”，点击<新增>，添加其他部门允许访问的网站分组。




说明：

- 在组成员中可以使用通配符（*）的方式来添加网站（例如*.baidu.com，即可匹配 www.baidu.com、

news.baidu.com、mp3.baidu.com 等网页。

3. 设置网站访问规则

- **添加市场部规则**

在“行为管控 >> 网站访问 >> 网站访问”，点击<新增>，添加市场部的过滤规则，即禁止市场部访问视频、游戏、购物类的网站。


- **添加其他部门的规则**

在“行为管控 >> 网站访问 >> 网站访问”，点击<新增>，添加允许其他部门访问官网及百度。


再点击<新增>，添加禁止其他部门访问所有网站.


设置完成，可以查看到网站访问的列表如下：

| | 序号 | 受管理IP地址组 | 规则类型 | 受管理网站类型 | 受管理时间段 | 状态 | 备注 | 设置 |
|---|---|---|---|---|---|---|---|---|
| | 1 | Others | 允许访问 | 官网和百度 | 所有时间段 | 已启用 | --- | |
| | 2 | Marketing | 禁止访问 | 视频,游戏,购物 | 所有时间段 | 已启用 | --- | |
| | 3 | Others | 禁止访问 | 所有网站 | 所有时间段 | 已启用 | --- | |

至此，网站访问功能设置完成，企业所有部门员工将按照设置的规则来上网。

## 9.4 网页安全

### 9.4.1 网页安全

企业网络环境中，对于访问网络的安全性的要求较高，对上传和下载有严格的要求，尤其是对于一些 exe、rar、txt 等类型文件有严格限制。网页安全功能可以限制内网用户通过网络提交信息，同时可以对下载文件的扩展类型进行管控，对常见扩展类型的文件的下载权限进行限制，从而实现网络应用安全。

进入页面：行为管控 >> 网站安全，点击<新增>，设置网页安全规则。


| | |
|---|---|
| 受管理的地址组 | 规则生效的地址组，地址组设置请见 9.1.1 地址组管理。 |
| 受管理时间段 | 规则生效的，时间对象管理请见 9.1.2 时间管理。 |
| 禁止网页提交 | 对网页提交禁止。 |
| 文件下载 | 对符合规则的文件下载放行或禁止。 |

| | |
|---|---|
| 过滤文件类型 | 填写要过滤的文件的关键字，例如 exe，txt 等。 |

点击页面，查看更多页面设置参数信息。

## 9.4.2 网页安全配置实例

需求介绍：某企业网络环境中，为了确保内部网络安全，需求如下：

- 禁止企业内部人员对网页内容的上传和网站、论坛等用户名密码的登录；
- 禁止企业内部人员从网页上下载 exe，rar 后缀的文件。

设置方法:

登录网关的管理界面，点击 “行为管控 >> 网页安全”，选择相应的地址组，选择禁止网页提交（禁止上传和网站、论坛等用户名密码的登录），填写需要过滤文件的扩展类型，设置完成后，点击<确定>。


过滤文件类型：即文件的类型，如压缩包 rar、zip 等，安装软件 exe 等。网页安全功能目前仅对采用 HTTP

协议的上传和下载生效。

至此，网页安全设置完成，局域网内的电脑在上网的过程中，将会按照上述的设置的规则使用网络。

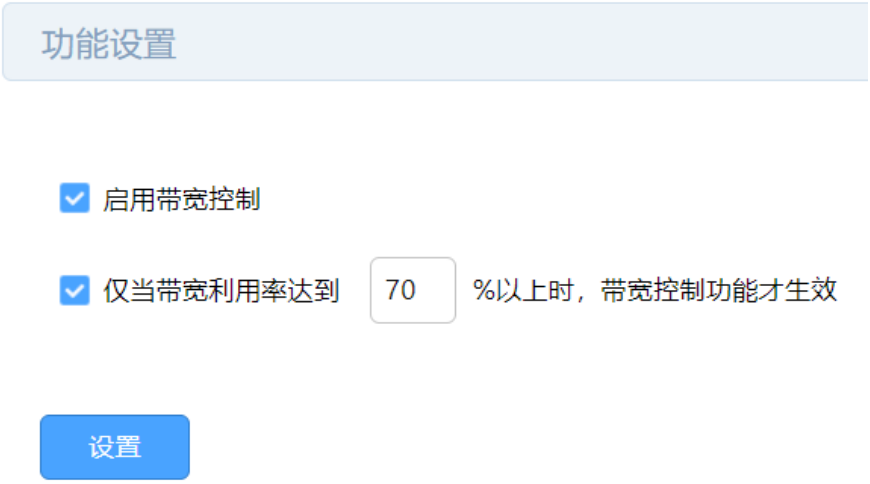
## 9.5　配置带宽控制功能

### 9.5.1 带宽控制介绍

网络的带宽资源时有限的，而且宽带使用时经常会出现“20%的主机占用了 80%的资源”的问题，导致网络的应用出现“上网慢、网络卡”等现象。安全融合网关提供了基于 IP 地址的带宽控制功能，可以有效防止少部分主机占用大多数的资源，为整个网络贷款资源的合理利用提供保证。

配置方法：

进入页面：行为管控 >> 带宽控制，勾选<启用带宽控制>，设置带宽利用率阈值，仅当带宽利用率高于这个值，带宽分配功能才会开启。




在带宽控制规则列表部分，点击<新增>，设置带宽控制规则。


| | |
|---|---|
| 受管理 IP | 规则生效的地址组，地址组设置请见 9.1.1 地址组管理。 |
| 受管理时间段 | 规则生效的时间段，时间对象管理请见 9.1.2 时间管理。 |
| 带宽模式 | 共享表示地址组内 IP 共用设定的上下行带宽；独立表示地址组内所有 IP 均独占设定的上下行带宽。 |
| 数据流向 | 选择规则控制的数据流向。 |
| 最小/大上行带宽 | 规则定义的数据流的最小上行/下行保证带宽（单位为 Kbps）。 |
| 最小/大下行带宽 | 规则定义的数据流的最大上行/下行带宽（单位为 Kbps）。 |

点击页面 ，查看更多页面设置参数信息。

## 9.5.2 例外管理

您可以通过本页面设置和查看带宽控制例外管理信息，例外管理用来配置指定用户不受 IP 带宽控制和应用带宽控制的限制。

进入页面：行为管控 >> 例外管理，点击<新增>，


| | |
|---|---|
| 源/目的 IP 地址范围 | 规例外管理的源/目的 IP 地址和网络掩码。 |
| 源 MAC 地址 | 规设置例外管理的源 MAC 地址。 |
| 源端口范围 | 设置例外管理的源/目的端口范围。 |
| 服务协议 | 设置例外管理的服务协议。 |

点击页面 ，查看更多页面设置参数信息。

## 9.5.3 带宽控制配置实例

需求介绍：某企业 20M 光纤宽带接入，内网电脑 IP 地址设置为手动指定，根据需求，指定以下需求表格：

| 部门 | 带宽需求 | IP 地址段 | 最大带宽分配 |
| --- | --- | --- | --- |
| 市场部 10 人 | 浏览网页、下载内容、需要较大的带宽 | 192.168.1.10-19 | 每人 3000Kbps |
| 其他部门 30 人 | 浏览网页，收发邮件满足一般上网应用 | 192.168.1.20-49 | 每人 1000Kbps |

配置步骤：

1. 进入页面：基本设置 >> WAN 口设置 >> WAN 口设置，选择连接外网的 WAN 口，点击<高级设置>，填写宽带线路真实的上行、下行带宽（本例中上下行带宽均为 20Mbps），并点击<保存>。


注意：

- 1Mbps=1024Kbps，为了便于计算，文档以 1Mbps=1000Kbps 为例。

2. 添加市场部和其他部门的地址组，后续的宽带控制规则中针对地址组进行控制。点击“行为管控 >> 地址管理”，点击<新增>，添加如下地址，点击<确定>。


其他部门地址组的添加，也是相同操作。

3. 设置带宽控制规则：进入页面行为管控 >> 带宽限制，点击<新增>，为市场部设置如下的带宽控制规则。


同样方法，新增其他部门的带宽控制规则。

4. 设置智能带宽控制：设置好带宽控制规则后，需要勾选“启用带宽控制”并点击“设置”后，带宽控制规则才会生效；智能带宽控制表示仅当前带宽利用率超过设置的百分比时，带宽控制功能才开始生效。具体计算公式为：第一步中填写的线路实际下行带宽╳设置的百分比。


## 9.6 连接数限制

### 9.6.1 连接数限制

通信过程中，点与点之间建立的任何一个独立连接均会在安全网关上进行维护，从而确保通信数据正常转发。安全网关内部维护着一张连接表，用来存放连接信息，该列表会动态占用内存、CPU 资源。由于表的总大小是固定的，如果某个时候，表中的连接达到最大数目，此时新的连接无法建立，导致数据转发异常。简单理解为：安全网关的连接总数是固定值（有上限的），如果其中的一部分电脑消耗了过多的连接数（如BT、迅雷下载等），可能会导致其余的电脑无法正常上网。连接数限制功能可以控制主机占用的连接数，从而均衡网络应用，确保平稳使用。

配置方法：

进入页面：行为管控 >> 连接数限制，点击<新增>，设置受管理 IP 地址组和该 IP 地址组的最大连接数，点击<确定>。


IP 地址组配置请参考 9.1.1 地址组管理。

## 9.6.2 连接数限制配置实例

需求介绍：某公司网关安全网关经常有电脑使用迅雷或 BT 下载，连接数可以达到上千，占用过多连接数，影响其他电脑的应用。为了避免局域网部分主机占用过多的连接，通过设置连接数限制优化网络应用。

配置步骤：

进入页面：行为管控 >> 连接数限制，点击<新增>，添加连接数限制规则。


说明：

- 普通上网应用，建议设置最大连接数为 200-300。

# 9.7 访问控制

## 9.7.1 访问控制

企业办公网络环境中，需要对内部办公电脑进行网络权限差异化设置，从而提升办公效率和网络安全。访问控制功能通过对源/目的 IP 地址、端口及访问时间进行控制，实现上网权限的差异化设置，满足企业用户的需求。

配置方法：

进入页面：行为管控 >> 访问控制，点击<新增>，设置受管理 IP 地址组和该 IP 地址组的最大连接数，点击<确定>。


策略类型　　指明这条规则对符合条件的数据包放行还是丢弃。

| | |
|---|---|
| 服务类型 | 选择生效的协议，ALL 表示所有协议。同时可以自定义服务类型。<br>协议类型/协议号：服务所使用的协议。您可以选择 TCP，UDP，TCP/UDP 或 ICMP，也可以选择 other 并输入协议号(0-255)。<br>源端口范围：服务所使用的源端口范围，仅 TCP 或 UDP 协议需要设置。<br>目的端口范围：服务所使用的目的端口范围，仅 TCP 或 UDP 协议需要设置。<br>ICMP：ICMP 协议的类型(type)和编码(code)，填充 255 时表明所有类型/编码。 |
| 生效接口域 | 在安全网关接口中选择该规则对应生效的接口，ALL 表示所有的接口。 |
| 源/目的地址范围 | 规则生效的源/目的地址组，地址组设置请见 9.1.1 地址组管理。 |
| 生效时间 | 规则生效的时间段，时间对象管理请见 9.1.2 时间管理。 |

点击页面  ，查看更多页面设置参数信息。

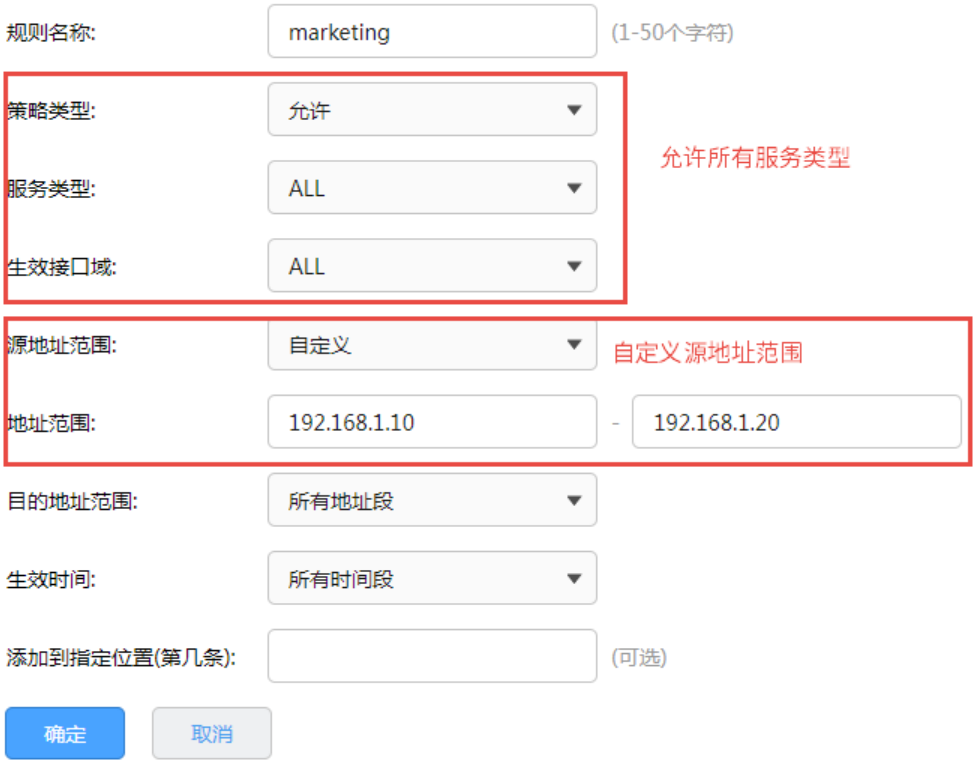
## 9.7.2 访问控制配置实例

需求介绍：某企业使用需要实现市场部上网不受限制，其它部门只能浏览网页。根据需求，制定以下配置表：

| 部门 | 允许的上网行为 |
|---|---|
| 市场部 | 所有网络应用 |
| 其它部门 | 浏览网页 |

配置步骤：

1. 设置市场部访问规则：进入页面：行为管控 >> 访问控制，点击<新增>，允许市场部访问所有网络应用。




2. 设置其他部门访问规则：进入页面：行为管控 >> 访问控制，点击<新增>，其它部门的员工，只允许浏览网页，即需要开放 HTTP、HTTPS、以及 DNS 服务。

设置其他部门能访问 HTTP


设置其他部门能访问 DNS:


3. 由于访问控制规则默认为“允许”，需设置其他部门禁止访问一切。


设置完成后，规则如下：

| | 序号 | 规则名称 | 源地址范围 | 目的地址范围 | 策略类型 | 服务类型 | 生效接口域 | 生效时间 | 设置 |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | marketing | 192.168.1.10-192.168.1.20 | 所有地址段 | 允许 | ALL | ALL | 所有时间段 | |
| ☐ | 2 | others_HTTP | 192.168.1.21-192.168.1.50 | 所有地址段 | 允许 | HTTP | LAN | 所有时间段 | |
| ☐ | 3 | others_DNS | 192.168.1.21-192.168.1.50 | 所有地址段 | 允许 | DNS | LAN | 所有时间段 | |
| ☐ | 4 | forbid_all | 所有地址段 | 所有地址段 | 阻塞 | ALL | ALL | 所有时间段 | |

# 第10章 安全防护

## 10.1 ARP 防护

一台主机向局域网内另一台主机发送 IP 数据包，此时设备需要通过 MAC 地址确定目的接口才能进行通信，而 IP 数据包中不包含有 MAC 地址信息，因此需要将 IP 地址解析为 MAC 地址。ARP（Address Resolution Protocol，地址解析协议）正是用来实现这一目的的网络协议。网络中的所有设备，包括安全网关和计算机在内，都各自维护一份 ARP 列表，该列表建立了主机 IP 地址和 MAC 地址一一对应关系。

按照 ARP 协议的设计，设备通过数据包的交互学习到其他设备的 IP 地址和 MAC 地址信息，并将这些信息添加至自身的 ARP 表中。每次通信时会先通过该表查找对应地址，减少网络上过多的 ARP 通信量。但设备同时也会接收不是自己主动请求的 ARP 应答，这就为“ARP 欺骗”创造了条件。

ARP 欺骗是局域网的攻击主机发送 ARP 欺骗包，将伪造的 IP 与 MAC 对应关系替换设备 ARP 列表中的记录，从而导致局域网内计算机不能正常上网。这类 ARP 攻击严重影响了局域网内部通信，由此便产生了 ARP 防护技术。

### 10.1.1 IP-MAC 绑定

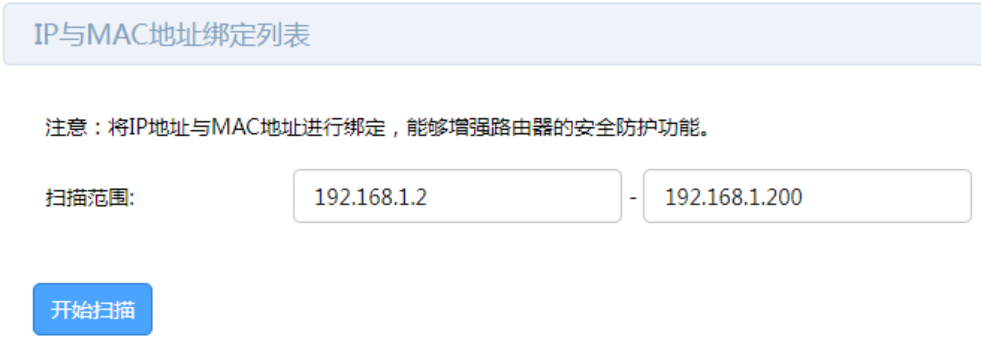
IP-MAC 绑定是一种防护技术，能够防止 ARP 列表被伪造的 IP-MAC 对应信息替换。

配置方法：

进入页面：安全管理 >> ARP 防护 >> IP-MAC 绑定。

- **扫描绑定**

输入扫描的 IP 地址范围，点击<开始扫描>，安全网关会对该范围的 IP 地址进行 ARP 查询。扫描结束后，扫描得到的结果会出现在 IP 与 MAC 地址绑定列表中。




- **手动绑定**

点击<新增>，可手动增加 IP 与 MAC 绑定规则。


| | |
|---|---|
| IP 地址 | 输入待绑定的 IP 地址。 |
| MAC 地址 | 输入待绑定的 MAC 地址，格式为 xx-xx-xx-xx-xx-xx。 |
| 生效域 | 针对局域网中的 ARP 绑定请选择 LAN 口；如果需要对于 WAN 口绑定请选择对应的 WAN 口。 |

点击页面 ，查看更多页面设置参数信息。

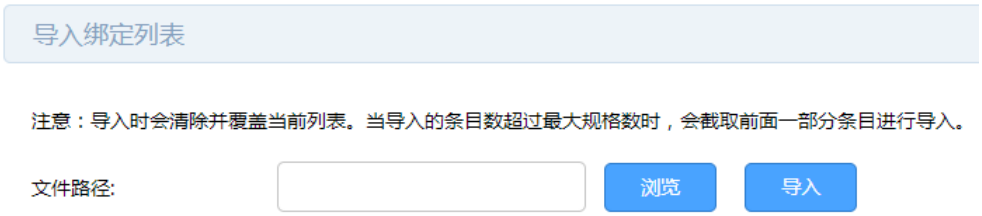
点击<添加到静态地址分配列表>，选择多条 IP-MAC 绑定列表中的条目，点击 “添加到静态地址分配列表” 按钮，可一次将多个条目一次性导入到 DHCP 静态地址分配列表中，您可以在 基本设置 LAN 设置静态地址分配中查看。

- **备份绑定列表**

点击<备份>，将 IP 与 MAC 地址绑定列表备份到您的计算机中。


➢ **导入绑定列表**

点击<浏览>，选择需导入的文件，点击<导入>将合法的 IP 与 MAC 地址绑定列表导入到安全网关。




## 10.1.2 ARP 防护

进入页面：安全管理 >> ARP 防护 >> ARP 防护。

勾选<启用 ARP 防欺骗功能>，若关闭该功能，禁止非 IP-MAC 绑定的数据包通过和发送 GARP 功能等功能都不会生效。

勾选<禁止非 IP-MAC 绑定的数据包通过安全网关>，则网关只会放过在 IP-MAC 绑定规则中的数据包。如要开启该功能，需要先开启 ARP 防欺骗功能。

勾选<发现 ARP 攻击时发送 GARP 包>，设置发包间隔，安全网关收到与 IP-MAC 绑定列表中不一致的报文时，会发送 GARP。如要开启该功能，需要先开启 ARP 防欺骗功能。

## 10.1.3 ARP 列表

进入页面：安全管理 >> ARP 防护 >> ARP 列表，可以查看系统中 ARP 列表。

可以选择多条 ARP 列表中的条目，点击<添加到绑定列表>，一次性添加到 IP-MAC 绑定列表中。

## 10.1.4 ARP 防护配置实例

需求介绍：某企业希望通过安全网关的设置来防范内网发生 ARP 欺骗问题而导致终端无法上网，影响企业正常办公。

配置步骤：

1. 在设置 ARP 绑定之前，请给需要绑定的电脑手动指定 IP 地址。

   如果不清楚如何设置，请参考：如何给终端手动指定 IP 地址。

   同时，建议查看对应电脑的 MAC 地址，制作 IP、MAC、电脑的表格，便于后续维护，如下图所示：

| 使用人 | IP 地址 | MAC 地址 | 备注 |
| --- | --- | --- | --- |
| 张三 | 192.168.1.100 | 50-E5-49-1E-91-F3 | 办公 |
| ..... | .. | .. | .. |

以上表格仅为示意，具体信息请根据实际需要记录。

2. 在网关上添加绑定条目：进入页面：安全管理 >> ARP 防护 >> IP-MAC 绑定，在 IP-MAC 绑定界面添加绑定条目。可采用手动添加或扫描添加两种方式。

- **手动添加**

手动添加操作复杂，但是安全性高。在网络中已经存在 ARP 欺骗或者不确定网络中是否存在 ARP 欺骗的情况下，建议使用手动添加的方式。手工进行添加，先点击<新增>，填写需要绑定的电脑的 IP 和 MAC 地址，选择生效域，填写备注信息，并点击<确定>。如下图所示：

➢ **扫描添加**

简单快捷，但是要确定网络中没有 ARP 欺骗，否则绑定错误的 IP/MAC 条目可能导致内网部分主机无法上网。在扫描范围输入需要扫描的 IP 地址段后，点击<开始扫描>，此时等待一会，安全网关会自动查找当前内网的主机，并显示主机的 IP 和 MAC 地址信息，如下图所示：


勾选所有条目，再点击<添加到绑定列表>，所有的绑定条目就设置完成了。


说明：

- ARP 扫描的功能也可以扫描 WAN 口的网段，可以通过扫描绑定 WAN 口网关地址防止前端 ARP 欺骗（宽带拨号无需绑定）。
- ARP 扫描只能检测当前网络中的活动主机，如果主机处于关机状态，则 ARP 扫描无法发现该主机。

3. 启用 ARP 绑定功能：局域网中电脑的 IP 与 MAC 全部绑定完成后，在“安全管理 >> ARP 防护 >> ARP 防护”中，确认已勾选“启用 ARP 防欺骗功能”，点击<保存>。如下图所示：


说明：

- 如果勾选“禁止非 IP-MAC 绑定的数据包通过安全网关”，则不在绑定列表或与绑定列表冲突的电脑不能上网或管理安全网关。

至此，防止 ARP 欺骗设置完成。

4. 电脑绑定网关 ARP 信息：仅在安全网关上绑定主机的 MAC 地址并不能完全解决 ARP 欺骗的问题，在主机上绑定安全网关的 MAC 地址，即双向绑定，就可以彻底解决欺骗问题。以下介绍不同操作系统电脑的绑定方法：

➢ **Windows XP 系统：**

在电脑上建立一个文本文件，写入 ARP 绑定命令：“arp –s IP MAC”，如下图所示：


说明：

- IP 是安全网关的管理地址（192.168.1.1），MAC 是安全网关 LAN 口的 MAC 地址（01-02-03-04-05-06）。

保存之后将该文件修改为.bat 后缀的批处理文件，比如“arp.bat”。然后将其放入系统启动项中，以后系

统每次开机时都会执行该绑定命令。如下图所示：


- **Windows 7/ Windows 8/ Windows 10 系统：**

（1） 打开命令提示符，使用命令：“netsh i i show in”查看网卡 idx 编号；

（2） 查询到网卡 idx 编号后，再使用命令“ netsh –c i i add neighbors idx ip mac”进行 ARP 绑定，

如下图所示：


说明：

- Windows 8/ Windows 10 系统中以太网为有线网卡。Windows 8 系统中 Wi-Fi 为无线网卡，Windows 10 系统中 WLAN 为无线网卡。

（3）使用 arp –a 的命令可以查询到绑定是否生效。

设置完成后，电脑重启，ARP 绑定条目也不会失效。

说明：

- 如果需要删除 ARP 绑定条目，只需要输入命令：netsh –c i i delete neighbors idx(idx 表示编号)，重启电脑后，绑定删除。

至此全部的设置就完成了，后续无需担心 ARP 欺骗给网络带来的影响。

# 10.2 MAC 地址过滤

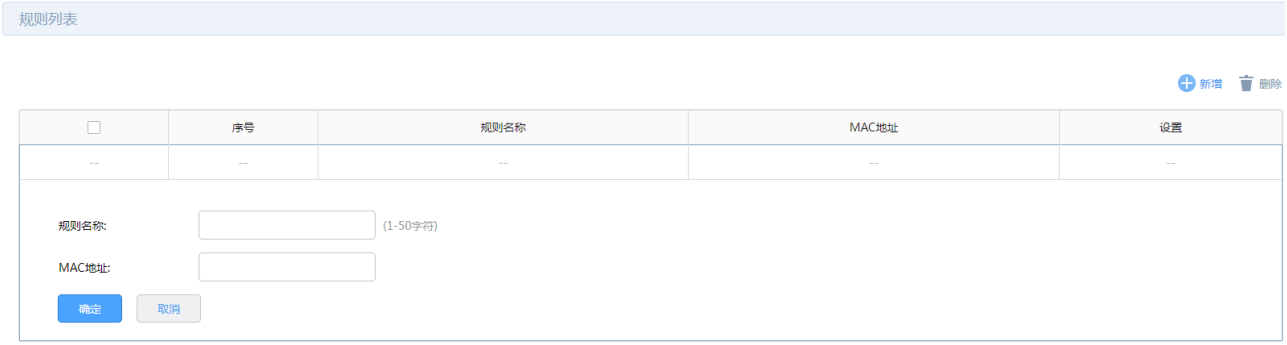
## 10.2.1 MAC 地址过滤

每个网络设备都有一个唯一的标识，即 MAC 地址。MAC 地址过滤功能可以有效控制电脑的网络接入权限，并且还可以避免因电脑 IP 地址变化而导致规则不生效的问题。

进入页面：安全管理 >> MAC 地址过滤，勾选<启用 MAC 地址过滤功能>，选择规则类型，点击<保存>。


| | |
|---|---|
| 白名单 | 白名单规则中的设备允许访问外网。 |
| 黑名单 | 黑名单规则中的设备不允许访问外网。 |

点击<新增>，添加需过滤的 MAC 地址。设置规则名称和 MAC 地址，点击<确定>。




## 10.2.2 MAC 地址过滤配置实例

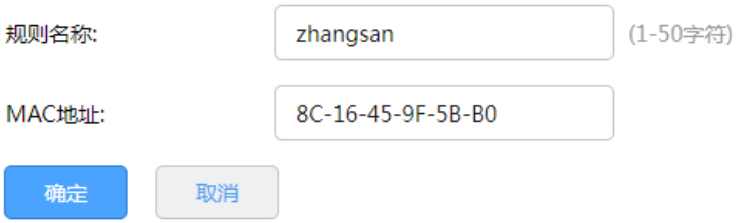
需求介绍：某企业希望通过安全网关的设置来实现仅允许某些电脑接入网络，防止不被允许的电脑接入企

业的网络进行通信。

设置方法：

1. 启用 MAC 地址过滤功能：进入页面“安全管理 >> MAC 地址过滤”，启用“MAC 地址过滤功能”，选择对应的规则类型，此处选择“白名单”，表示仅允许规则列表中的设备访问外网，点击<保存>。


2. 添加 MAC 地址：进入页面“安全管理 >> MAC 地址过滤”，点击<新增>，添加受控电脑的 MAC 地址。



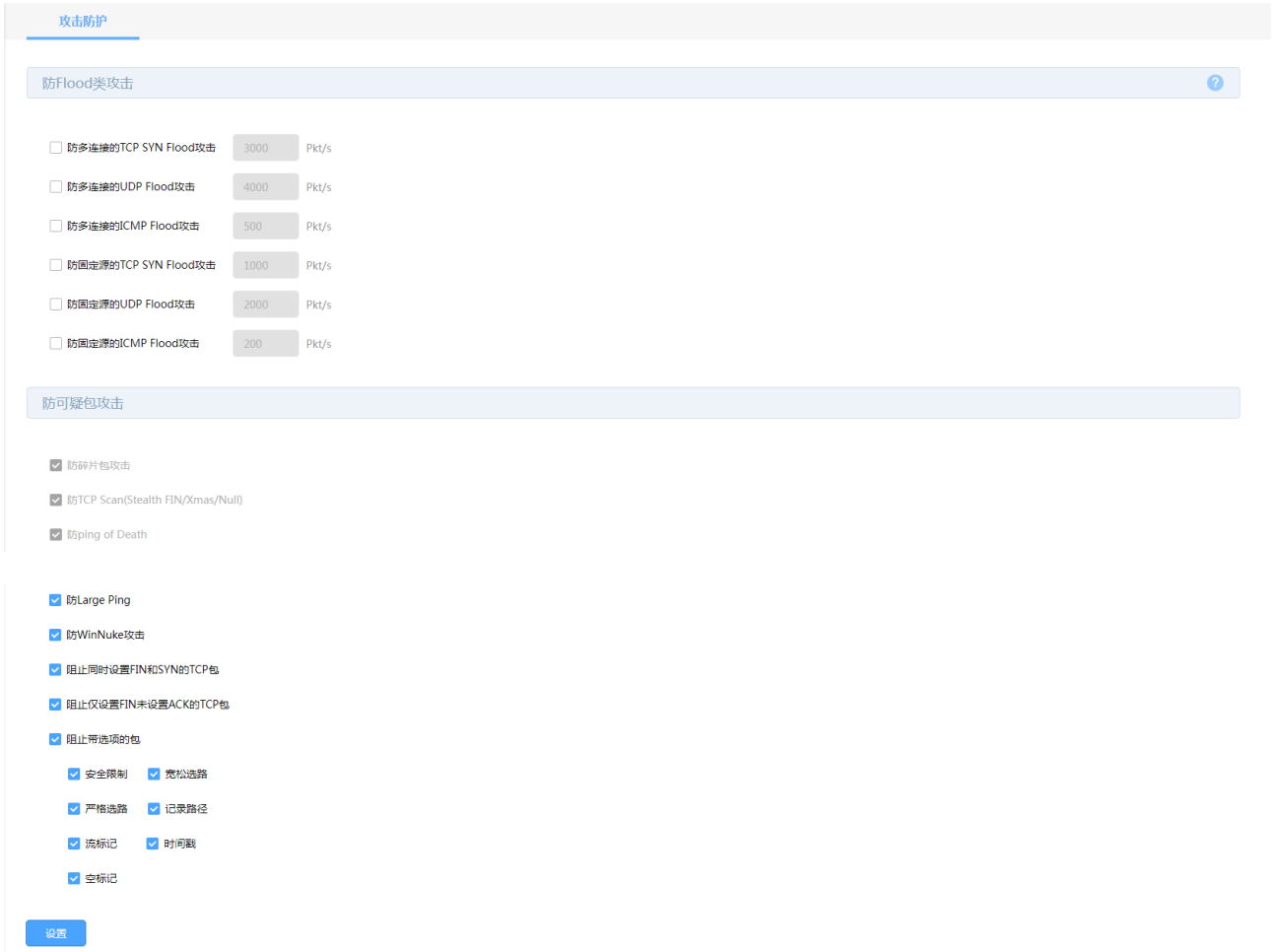

说明：

- 注意：如果您的需求为列表中 MAC 地址的电脑不能上网，列表外的均能上网。那么需要将第一步中的规则类型选择为“黑名单（不允许设备访问外网）”。

## 10.3 攻击防护

攻击防护可防止广域网对安全网关或局域网内计算机进行端口扫描和恶意攻击，以此来保证它们的安全运行。

进入页面：进入页面：安全管理 >> 攻击防护




| | |
|---|---|
| 防 Flood 类攻击 | Flood 类攻击是 DoS 攻击的一种常见形式。DoS（Denial of Service，拒绝服务）是一种利用发送大量的请求服务占用过多的资源，让目的安全网关和服务器忙于应答请求或等待不存在的连接回复，而使正常的用户请求无法得到响应的攻击方式。常使用的 Flood 洪水攻击包括 TCP SYN，UDP，ICMP 等。推荐勾选界面上所有防 Flood 类攻击选项并设定相应阈值，如不确定，请保持默认设置不变。。 |
| 防可疑包类 | 可疑包即非正常数据包，有可能是病毒或攻击者的扫描试探。推荐勾选界面上所有防可疑包选项。 |

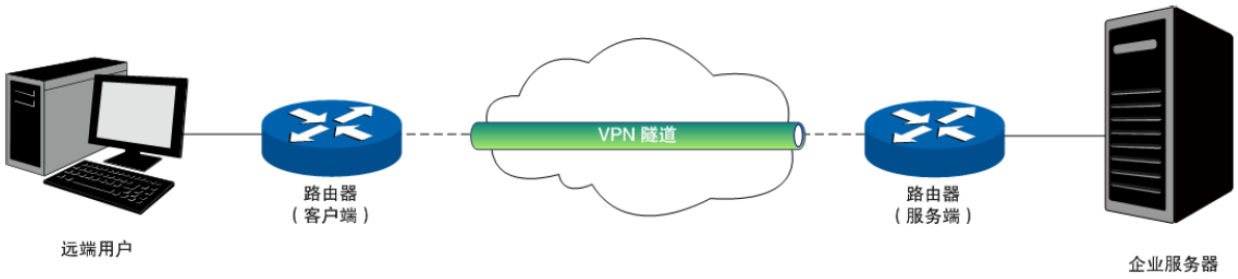
点击页面，查看更多页面设置参数信息。

# 第11章 VPN

VPN （Virtual Private Network，虚拟专用网）是一个建立在公用网（通常是因特网）上的专用网络，但因为这个专用网络只是逻辑存在并没有实际物理线路，故称为虚拟专用网。

随着因特网的发展壮大，越来越多的数据需要在因特网上进行传输共享，不过当企业将自身网络接入因特网时，虽然各地的办事处等外部站点可以很方便地访问企业网络，但同时也把企业内部的私有数据暴露给因特网上的所有用户。于是在这种开放的网络环境上搭建专用线路的需求日益强烈，VPN 应运而生。

VPN 通过隧道技术在两个站点间建立一条虚拟的专用线路，使用端到端的认证和加密保证数据的安全性。典型拓扑图如所示。




隧道是通过对数据报的封装实现的，因为数据报封装和解封的过程都是在安全网关上完成，所以对于用户来说是透明的。安全融合网关支持的隧道协议包括三层隧道协议 IPsec 和二层隧道协议 L2TP/PPTP。

## 11.1 IPSec

### 11.1.1 IPSec 安全策略

- IPSec

IPSec（IP Security，IP 安全性）是一系列服务和协议的集合，在 IP 网络中保护端对端通信的安全性、防止网络攻击。

为了实现安全通信，通信双方的 IPSec 协议必须协商确定用于编码数据的具体算法、用于理解对方数据格式的安全协议，并通过 IKE 交换解密编码数据所需的密钥。

在 IPSec 中有两个重要的安全性协议 AH（Authentication Header，鉴别首部）和 ESP（Encapsulating

Security Payload，封装安全性载荷）。AH 协议用于保证数据的完整性，若数据报文在传输过程中被篡改，报文接收方将在完整性验证时丢弃报文；ESP 协议用于数据完整性检查以及数据加密，加密后的报文即使被截取，第三方也难以获取真实信息。

IPSec VPN 多用于实现企业站点之间搭建安全的数据传输通道，将接入 Internet 的企业分支机构与总部网络通过安全隧道互联，实现资源、信息共享。

- **IKE**

在 IPsec VPN 中，为了保证信息的私密性，通信双方需要使用彼此都知道的信息来对数据进行加密和解密，所以在通信建立之初双方需要协商安全性密钥，这一过程便由 IKE（Internet Key Exchange，互联网密钥交换）协议完成。

IKE 其实并非一个单独的协议，而是三个协议的混合体。这三个协议分别是 ISAKMP（Internet Security Association and Key Management Protocol，互联网安全性关联和密钥管理协议），该协议为交换密钥和 SA（Security Association，安全联盟）协商提供了一个框架；Oakley 密钥确定协议，该协议描述了密钥交换的具体机制；SKEME 安全密钥交换机制，该协议描述了与 Oakley 不同的另一种密钥交换机制。

整个 IKE 协商过程被分为两个阶段。第一阶段，通信双方将协商交换验证算法、加密算法等安全提议，并建立一个 ISAKMP SA，用于在第二阶段中安全交换更多信息。第二阶段，使用第一阶段中建立的 ISAKMP SA 为 IPsec 的安全性协议协商参数，创建 IPsec SA，用于对双方的通信数据进行保护。至此，IKE 协商完毕。

配置方法：

进入页面：VPN >> IPSec >> IPSec 安全策略，点击<新增>，设置 IPSec 安全策略。


| | |
|---|---|
| 对端网关 | 设置对端网关，可以填写对端的 IP 地址或域名，作为响应者的时候可以将对端网关设为“0.0.0.0”,表示对端地址可以任意。 |
| 绑定接口 | 从下拉列表中指定本地使用的 WAN 口；对端网关设置的"对端网关地址"必须与该 WAN 口的 IP 地址相同。 |
| 本地子网范围 | 设置受保护的数据流的本地子网范围，由 IP 地址和子网掩码来确定。 |
| 对端子网范围 | 设置受保护的数据流的对端子网范围，由 IP 地址和子网掩码来确定。 |
| 预共享密钥 | 对于每对<绑定接口，对端网关>，都必须指定唯一的预共享密钥作为它们之间相互认证的凭证。 |

点击页面 ，查看更多页面设置参数信息。

点击<高级设置>，配置更多参数。一般情况，用户不需要配置高级设置，采用默认值即可。


阶段 1 设置：

| | |
|---|---|
| 安全提议 | 用于 IKE 协商方式下选择 IPSec 安全提议，在 IKE 协商模式下可以最多选择四条不同安全提议，主模式协商可以选择 4 条，野蛮模式协商可以选择 1 条。 |

| | |
|---|---|
| 交换模式 | 交换模式必须与对端相同。IKEv1 版本支持两种模式：主模式和野蛮模式，默认是选择主模式。<br>主模式（Main mode）：该模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。<br>野蛮模式（Aggressive mode）：又称主动模式，该模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。 |
| 协商模式 | 初始者模式会主动向对端发起连接，此时要求对端网关是路由可达，而响应者模式仅仅会等待对端发起连接。 |
| 本地 ID 类型 | 作为对端的身份标识，支持两种类型：IP 地址和 NAME，默认选择 "IP 地址",如果选择 NAME 类型，则需要输入任意的字符串作为本地 ID。 |
| 对端 ID 类型 | 作为对端的身份标识，支持两种类型：IP 地址和 NAME，默认选择 "IP 地址",如果选择 NAME 类型，则需要输入任意的字符串作为对端 ID。 |
| 生存时间 | 用于 IKE 协商方式下设置第一阶段 IPSec 会话密钥的生存时间。 |
| DPD 检测开启 | 选择是否开启 DPD 检测功能，开启该功能会定时发送 DPD 数据包以快速发现对端是否在线。 |
| DPD 检测周期 | 仅在 DPD 检测开启启用之后生效，用于指定相邻两次发送 DPD 检测数据包的时间间隔。 |

点击页面  ，查看更多页面设置参数信息。


阶段 2 设置：

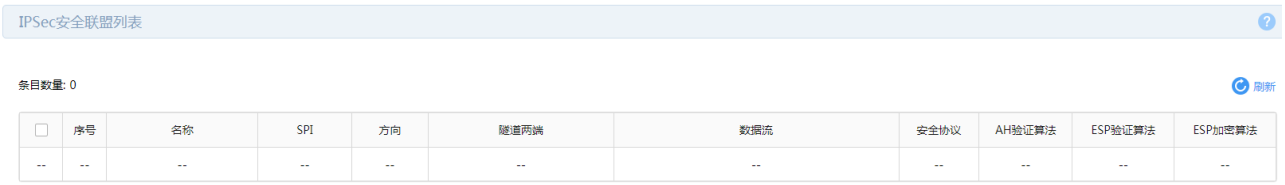
| | |
|---|---|
| 封装模式 | 指定该策略是隧道模式还是传输模式，必须与对端相同。两者的区别在于：前者会在原始 IP 报文外多增加一个 IP 头，后者则不会。从安全性来将，隧道模式优于传输模式，适用于更普遍的 VPN 应用。出书模式适用于主机直接访问设备时之间的加密传输。 |
| 安全提议 | 用于 IKE 协商方式下选择 IPSec 安全提议，在 IKE 协商模式下可以最多选择四条不同安全提议，主模式协商可以选择 4 条，野蛮模式协商可以选择 1 条。 |
| PFS | 用于 IKE 协商方式下设置 IPSec 会话密钥的 PFS 属性，对端的 PFS 属性必须与本地的 PFS 属性一致。 |
| 生存时间 | 用于 IKE 协商方式下设置第二阶段 IPSec 会话密钥的生存时间。 |

点击页面 ，查看更多页面设置参数信息。

## 11.1.2 IPSec 安全联盟

您可以通过本页面查看当前建立的安全联盟。

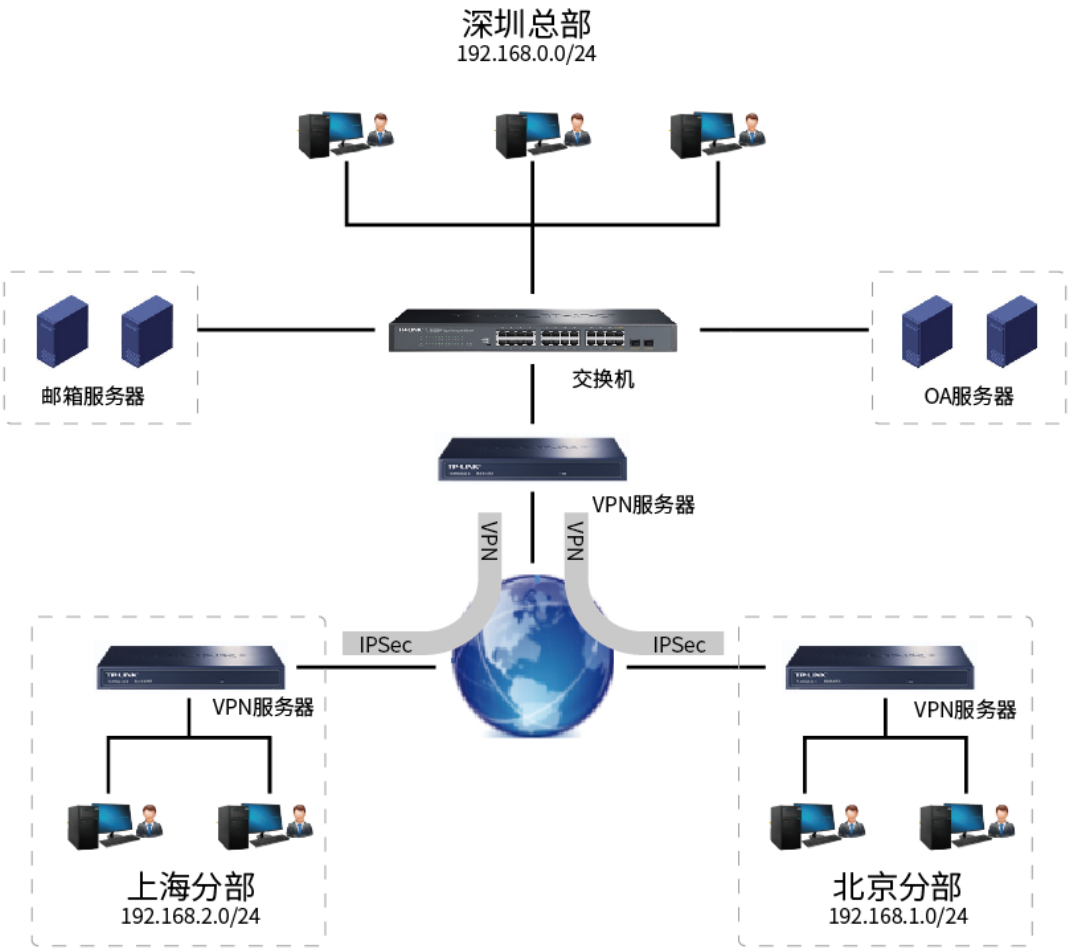
进入页面：VPN >> IPSec >> IPSec 安全联盟，点击<刷新>，可更新最新的安全联盟列表。




## 11.1.3 IPSec 配置实例

需求介绍：

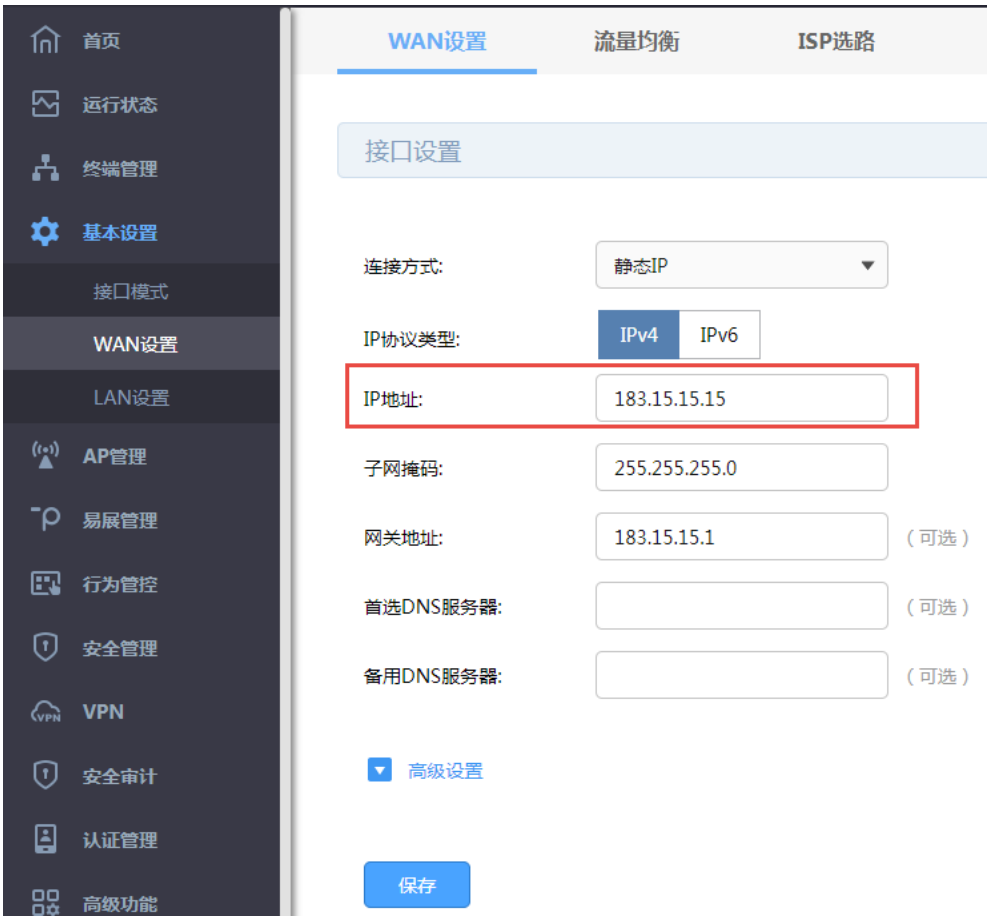
某公司总公司位于深圳，在北京、上海两地有分公司，现需要组建一个网络，达到三个机构能资源共享的目的，本文将通过一个实例来展示 TL-NR310-2C-S 与 TL-NR310-2C-S 搭建 IPSec VPN 的解决方案和配置过程。深圳总公司局域网网段为“192.168.0.0/24”，WAN 口为公网 IP：183.15.15.15；北京分公司为“192.168.1.0/24”，WAN 口为公网 IP：183.15.15.30；上海分公司为“192.168.2.0/24”。拓扑如下：




配置步骤：

- **首先设置深圳总部 TL-NR310-2C-S。**

1. 设置 WAN 口网络参数，进入页面：基本设置 >>WAN 口设置，设置 WAN 口固定 IP 为 183.15.15.15。




2. 配置 IPSec 安全策略基本设置：VPN >> IPSec，进入 IPSec 安全策略标签页，点击<新增>，设置 IPSec 安全策略。


说明：

- 策略名称：设置 IPSec 安全策略名称。

- 对端网关：填写对端 IPSec VPN 服务器的 IP 地址或者域名，此处为北京分公司 WAN 口 IP 地址 183.15.15.30。
- 绑定接口：从下拉列表中指定本地使用的接口；对端网关设置的"对端网关地址"必须与该接口的 IP 地址相同。
- 本地子网范围：设置本地子网范围，即深圳总公司局域网 192.168.0.0 /24。
- 对端子网范围：设置对端子网范围，即北京分公司局域网 192.168.1.0 /24。
- 预共享密钥：设置 IKE 认证的预共享密钥，通信双方的预共享密钥必须相同。
- 状态：设置勾选启用时，当前策略生效。

3. 配置 IPSec 安全策略高级设置：在基本设置完成后，点击<高级设置>，包括两个部分：阶段 1 设置和阶段 2 设置。一般地，用户不需要配置高级设置，采用默认值即可。


➢ **NAT 下的 IPSec VPN 配置**

VPN 两端路由器 WAN 口需要公网 IP，如没有公网 IP 则需要考虑 NAT 下的 IPSec 应用，见链接：NAT 下的 IPSEC VPN 配置实例。

注意：

- 注意：VPN 两端安全网关 WAN 口需要公网 IP，如没有公网 IP 则需要考虑 NAT 下的 IPSec 应用，首先阶段 1 设置中，本地/对端 ID 类型选择 NAME，其次，由于 NAT 模型与 IPSEC 中的 AH 协议的设计理念是完全相违背的，所以，阶段 2 设置中，在选择 IPSEC 协议的的时候，只能选择 ESP 协议。

阶段1设置

安全提议: md5-3des-dh2

安全提议: ---

安全提议: ---

安全提议: ---

交换模式: ○ 主模式 ◉ 野蛮模式 交换模式必须选择“野蛮模式”

协商模式: ◉ 初始者模式 ○ 响应者模式

本地ID类型: ○ IP地址 ◉ NAME

本地ID: test1 （1-28个非空字符）

ID类型必须选择NAME

对端ID类型: ○ IP地址 ◉ NAME

对端ID: test1 （1-28个非空字符）

生存时间: 28800 秒(60-604800)

DPD检测开启: ◉ 启用 ○ 禁用

DPD检测周期: 10 秒(1-300)

阶段2设置

封装模式: ◉ 隧道模式 ○ 传输模式

安全提议: esp-md5-3des

只能选择esp类型

安全提议: ---

安全提议: ---

安全提议: ---

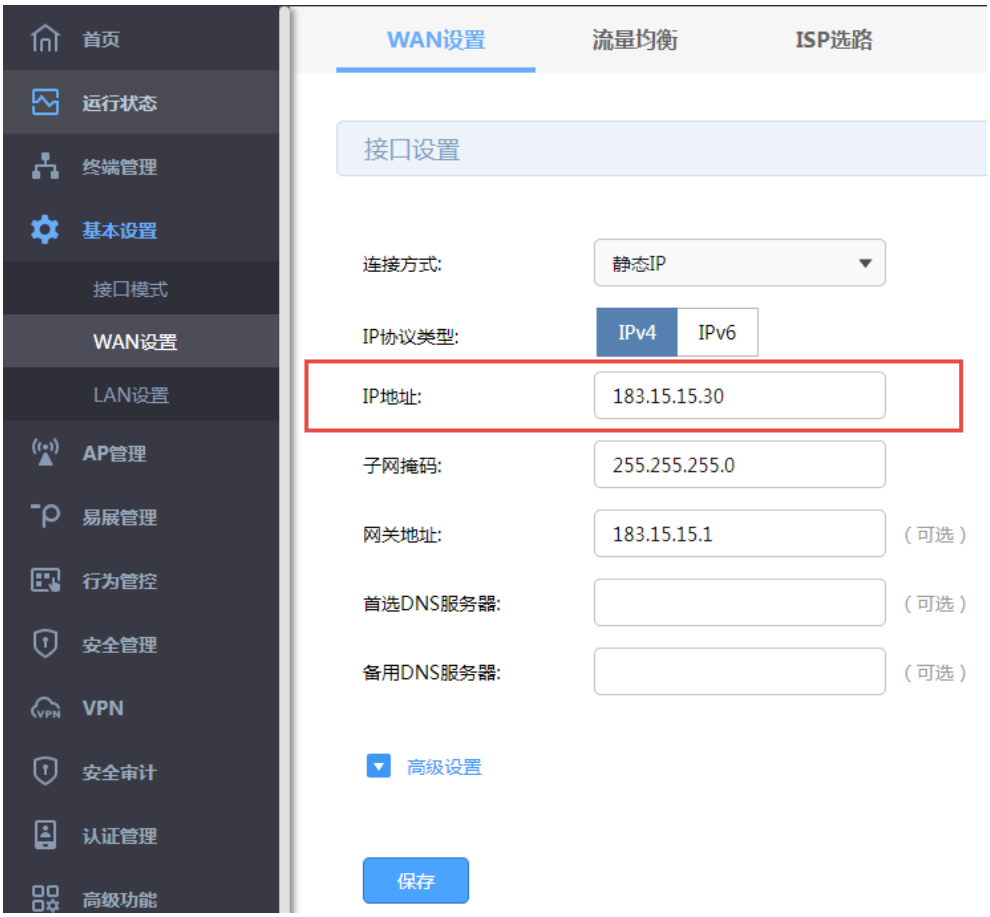
PFS: none

生存时间: 28800 秒(120-604800)

确定 取消

- 设置北京、上海分公司 TL-NR310-2C-S

1. 设置 WAN 口网络参数，进入页面：基本设置 >> WAN 口设置，设置 WAN 口固定 IP 为 183.15.15.30。




2. 配置 IPSec 安全策略基本设置，进入页面：VPN >> IPSec >> IPSec 安全策略，点击<新增>，设置 IPSec 安全策略。

3. 配置 IPSec 安全策略高级设置，进入页面：VPN >> IPSec >> IPSec 安全策略，点击<新增>，基本设置完成后点击高级设置，进行 IKEv1 阶段 1 和阶段 2 配置。如果总部保持的默认配置，分部也保存默认配置即可，如果总部做了修改，则分部应保持一致。 本例中总部高级设置均为默认参数，且分部与总部 Web 界面相同，此处不再展示。

4. 配置完成后点击保存，在 IPSec 安全策略列表中会出现相应条目。


配置完成，IPSec 安全联盟建立成功后，可以在 IPSec 安全联盟中看到相应条目。

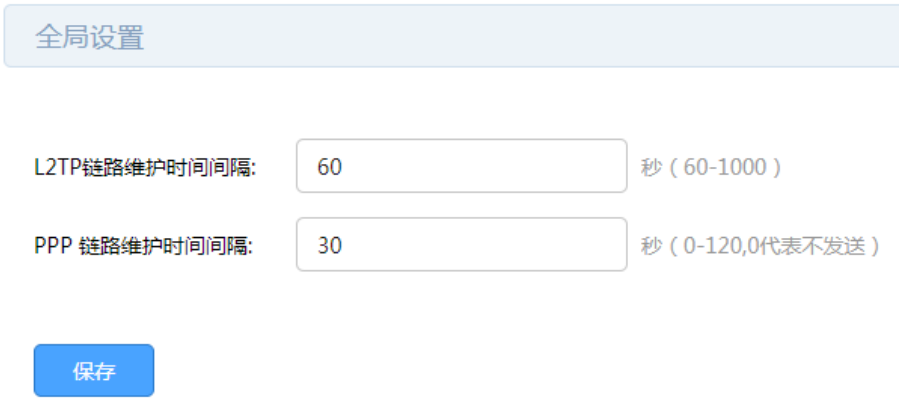
## 11.2 L2TP

企业安全网关提供多类 VPN 功能，其中 L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）是二层 VPN 隧道协议，使用 PPP（Point to Point Protocol，点到点协议）进行数据封装，并都为数据增添额外首部。L2TP VPN 可以实现企业站点之间搭建安全的数据传输通道，将接入 Internet 的企业分支机构与总部网络通过安全隧道互联，实现资源、信息共享；同时，也使得远端用户（如企业驻外机构和出差人员）利用 PPP 接入公共网络后，能够通过 L2TP 隧道访问企业内部网络资源，满足外出员工移动办公需求 。

### 11.2.1 L2TP 服务器

进入页面：VPN >> L2TP >> L2TP 服务器，进行全局设置和 L2TP 服务器设置。

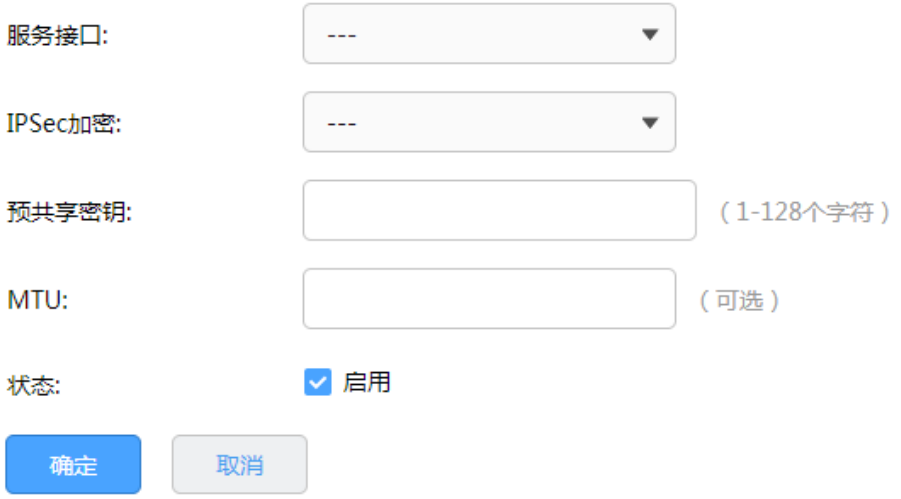
- **全局设置**




| | |
|---|---|
| L2TP 链路维护时间间隔 | VPN 拨通成功后，发送 L2TP 链路维护检测报文的时间间隔。 |
| PPP 链路维护时间间隔 | VPN 拨通成功后，发送 PPP 链路维护检测报文的时间间隔。 |

- **服务器设置**

点击<新增>，添加服务器设置条目。



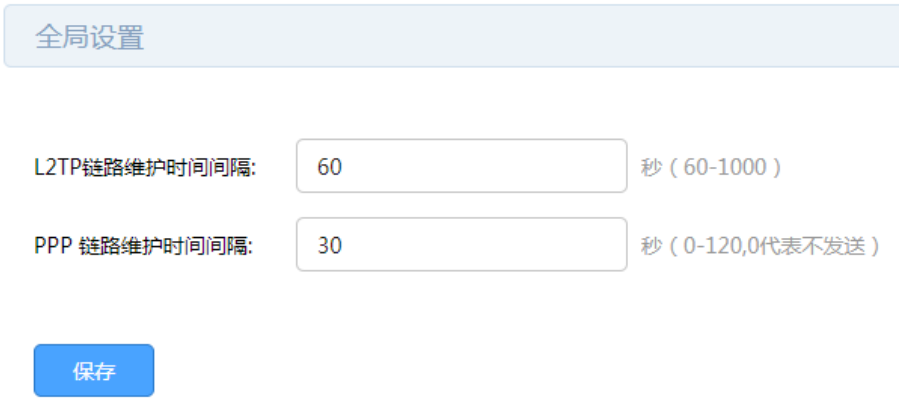

| | |
|---|---|
| 服务接口 | L2TP 服务器监听的接口，只有来自服务接口的报文才会被处理。 |
| IPSec 加密 | 是否对隧道进行加密。若加密，则使用 IPSec 对 L2TP 隧道加密。若可选加密，则 L2TP 隧道按客户端的需求决定是否进行 IPSec 加密。 |
| 预共享密钥 | IPSec 设置为加密或可选加密后，需设置 IPSec 的预共享密钥。 |
| MTU | MTU（Maximum Transmission Unit，最大传输单元），在一定物理网络中能传送的最大数据单元。 |

点击页面，查看更多页面设置参数信息。

## 11.2.2 L2TP 客户端

进入页面：VPN >> L2TP >> L2TP 客户端，进行全局设置和 L2TP 服务器设置。

- **全局设置**




| | |
|---|---|
| L2TP 链路维护时间间隔 | VPN 拨通成功后，发送 L2TP 链路维护检测报文的时间间隔。 |
| PPP 链路维护时间间隔 | VPN 拨通成功后，发送 PPP 链路维护检测报文的时间间隔。 |

- **客户端设置**

点击<新增>，添加客户端设置条目。


| | |
|---|---|
| 隧道名称 | L2TP 隧道的名称，用于区分不同的隧道。 |
| 用户名/密码 | L2TP 隧道用户身份认证的用户名密码，为服务器端设置的用户名和密码。 |
| 出接口 | L2TP 报文收发的接口。 |
| 服务器地址 | L2TP 服务器的地址，可以为 IP 或域名。 |
| IPSec 加密 | 是否对隧道进行加密。若启用，则使用 IPSec 对 L2TP 隧道加密。 |
| 预共享密钥 | IPSec 设置为加密后，需设置 IPSec 加密时的预共享密钥。 |

| | |
|---|---|
| 对端子网 | L2TP 隧道对端局域网使用的 IP 地址范围（一般可以填隧道对端设备 LAN 口的 IP 地址范围），由 IP 和子网掩码组成。 |
| 上/下行带宽 | 安全网关会根据上下行带宽进行流量均衡的计算。 |
| MTU | MTU（Maximum Transmission Unit，最大传输单元），在一定物理网络中能传送的最大数据单元。 |
| 工作模式 | NAT：对经过此 L2TP 隧道的数据包进行 NAT 转换（数据包的源 IP 替换为 L2TP 隧道的本地虚拟 IP）。<br>路由：对经过此 L2TP 隧道的数据包只进行路由转发。 |

点击页面  ，查看更多页面设置参数信息。

## 11.2.3 隧道信息列表

您可以获得 L2TP 隧道的信息。

进入页面：VPN >> L2TP >> 隧道信息列表，点击<刷新>，可更新最新的隧道信息列表。

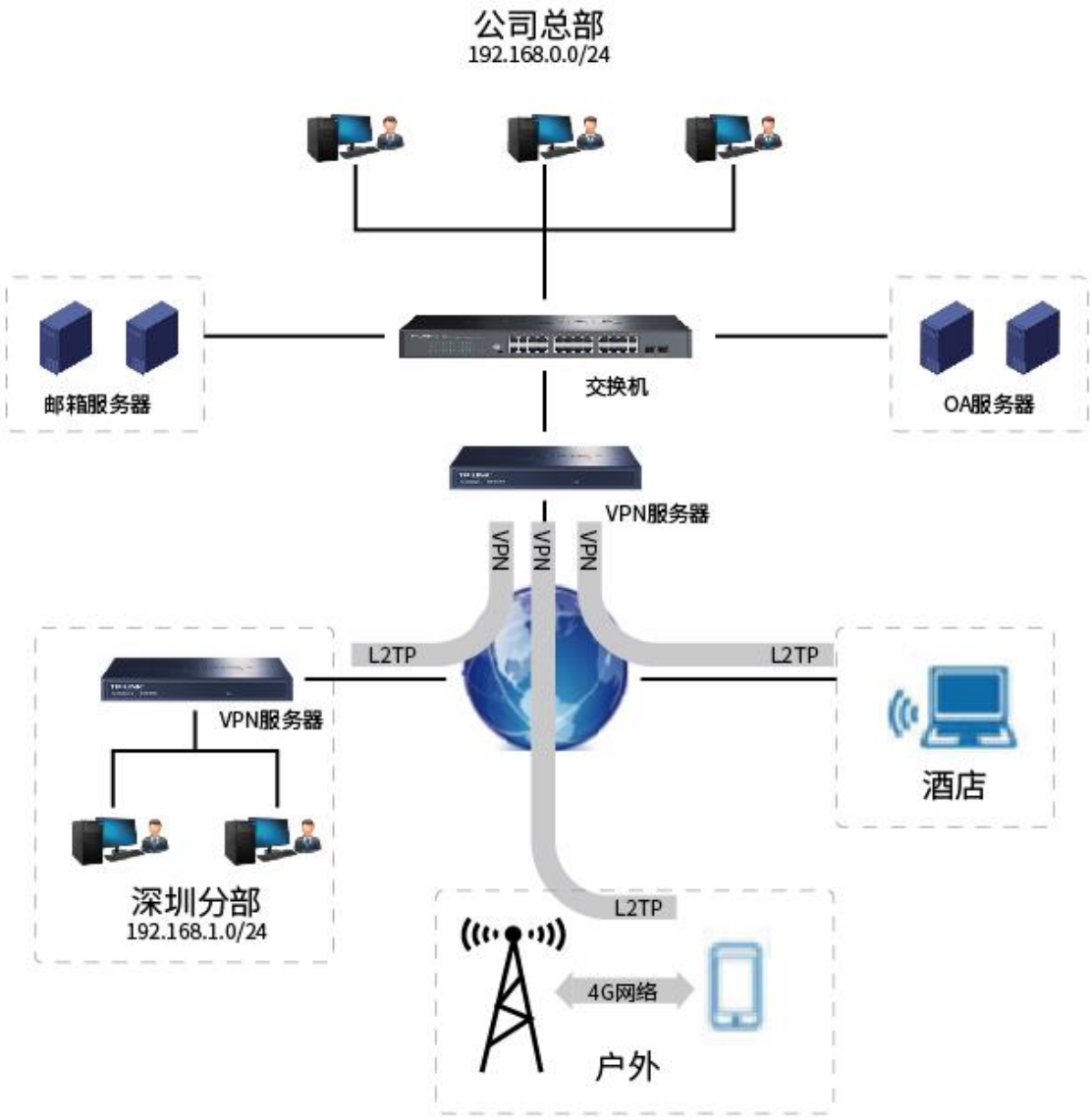

## 11.2.4 L2TP 配置实例

需求介绍：某公司的总部与分部均使用安全融合网关产品。需要实现将北京总部与深圳分公司通过 VPN 互联，实现资源相互访问，同时要求数据传输的安全性。需求参数如下：

| | |
|---|---|
| L2TP 账号/密码 | 123/123 |
| VPN 本地虚拟 IP | 10.10.10.10 |
| 地址池 | 10.10.10.11~10.10.10.200 |
| 加密 | 开启 |

| | |
|---|---|
| 总部外网 IP | 183.15.15.15 |
| 总部网段 | 192.168.0.0/24 |
| 分部外网 IP | 183.15.15.30 |
| 分部网段 | 192.168.1.0/24 |

拓扑如下：




本节将分别介绍 L2TP VPN 站点到站点设置方法和 L2TP VPN PC 到站点设置方法。

- **L2TP 站点到站点的设置方法**

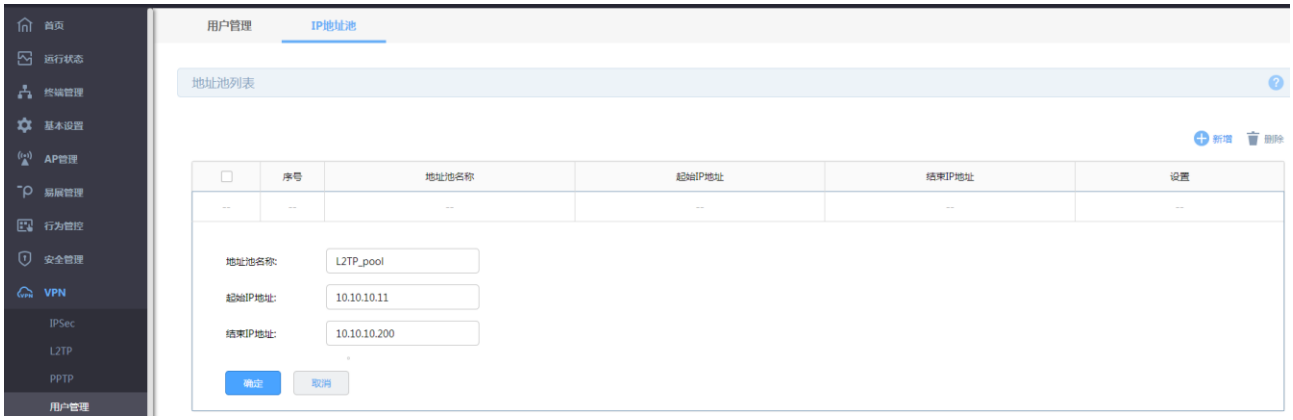
1. 在 VPN 服务器端上，进入管理页面：基本设置 >> LAN 设置 >> LAN 设置，设置接口 IP 网段为 192.168.0.0/24。


2. 在 VPN 服务器端上，进入管理页面：基本设置 >>WAN 设置 >>WAN 设置，设置静态 IP 方式上网或者 PPPoE 方式上网（如果使用的是 PPPoE 上网，由于获取的 IP 地址会变化，此时建议使用动态域名 DDNS)，本例使用静态 IP：183.15.15.15。


说明:

- 服务器端 WAN 口 IP 推荐为公网 IP，若非公网 IP，需要在前端设备做映射。。

3. 在 VPN 服务器端上，进入页面：VPN >> 用户管理 >> IP 地址池，新增隧道地址池(L2TP VPN 隧道通信时使用的 IP 地址)。




4. 在 VPN 服务器端上，进入页面：VPN >> 用户管理 >> 用户管理，进行用户管理配置，点击<新增>。


5. 在 VPN 服务器端上，进入页面：VPN >> L2TP >> L2TP 服务器，在服务器设置部分点击<新增>，添加 L2TP 服务器规则。

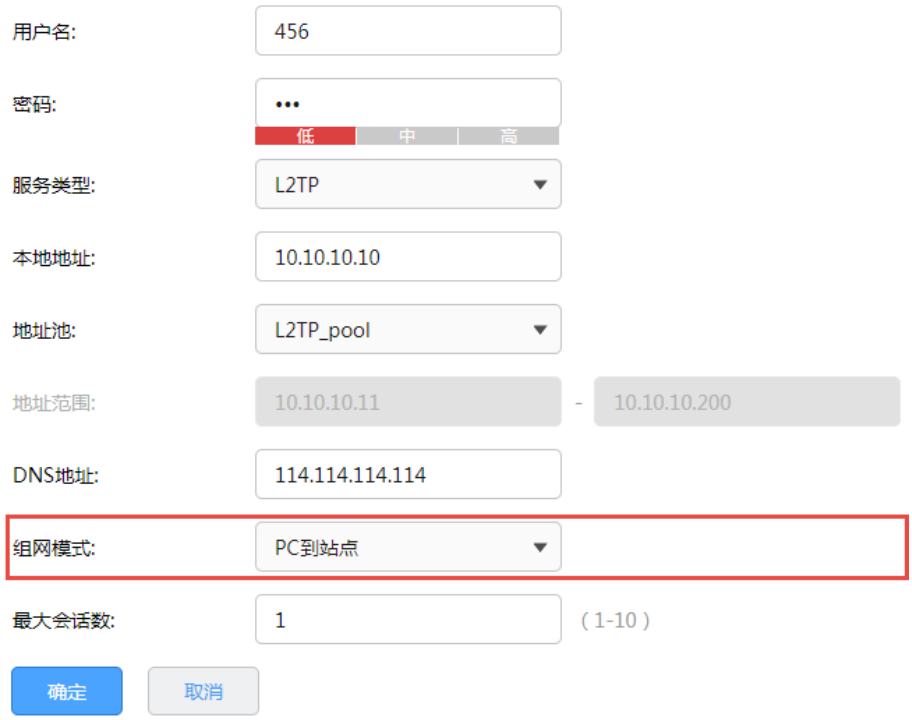

6. 在 VPN 客户端，进入管理页面：基本设置 >> LAN 设置 >> LAN 设置，设置接口 IP 网段为 192.168.1.0/24；进入管理页面：基本设置 >> WAN 设置 >> WAN 设置，正确设置 WAN 口上网方式，保证安全网关可以正常上网。

7. 在深圳分部的 VPN 安全网关上，进入页面：VPN >> L2TP >> L2TP 客户端，在客户端设置部分点击<新增>，添加 L2TP 客户端规则。


8. 成功启动总部的服务器端条目和深圳分布的客户端条目，L2TP 隧道信息列表中将有如下条目：


➢ L2TP PC 到站点的设置方法

1. 在 VPN 服务器端，需要在用户管理配置中添加 PC 到站点的用户账号密码，组网模式选择 PC 到站点，其余设置步骤与上面站点到站点的设置方法相同。




说明：

- 最大会话数：每个用户允许接入的最大客户端数量。注意：用户类型为自动的用户，意味着 L2TP 和 PPTP 的最大接入客户端数量均为最大会话数。

2. 进行 L2TP PC 到站点客户端的拨号设置。

不同 L2TP 客户端的配置方式有所差异，请选择客户端操作系统，参考对应指导文档：

[Windows XP] L2TP VPN 客户端拨号操作步骤

[Windows 7] L2TP VPN 客户端拨号操作步骤

[Windows 8] L2TP VPN 客户端拨号操作步骤

[Android] L2TP VPN 客户端拨号操作步骤

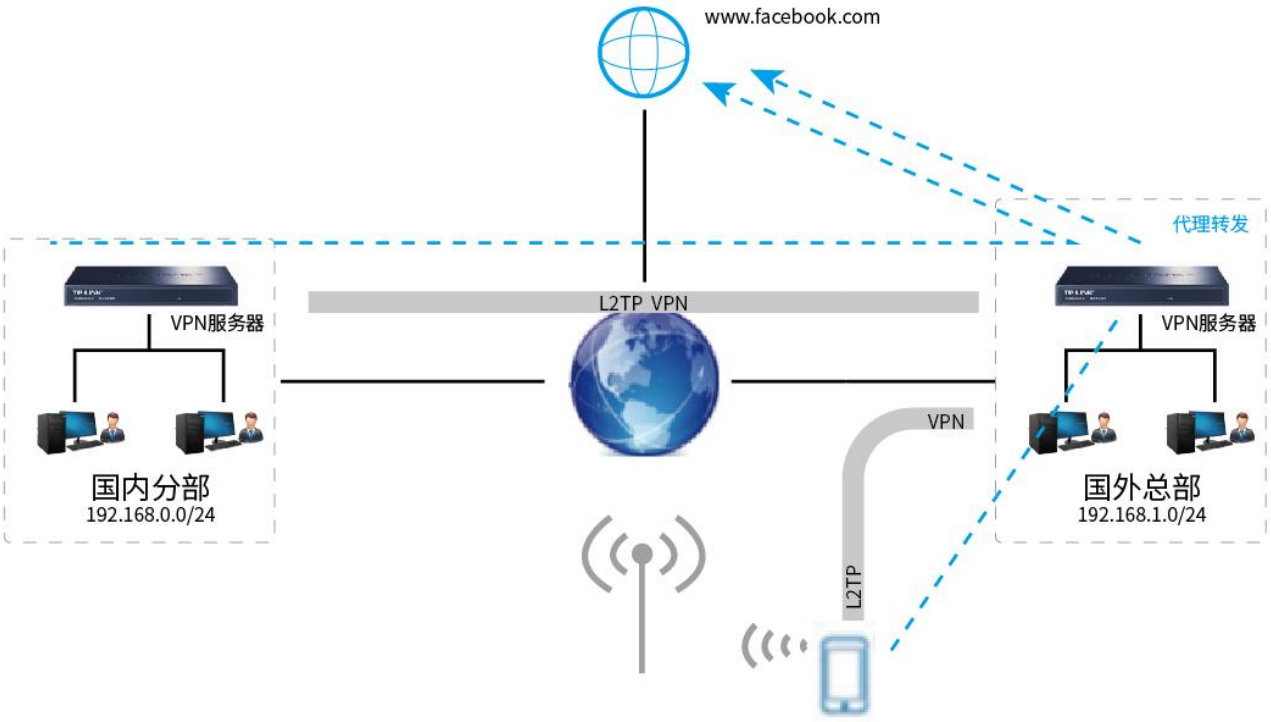
3. 电脑拨号成功后，系统默认勾选了 VPN 连接 IPv4 高级设置中的“在远程网络上使用默认网关”，则电脑所有数据优先从 VPN 接口转发，即可正常访问总部资源。

如果需要通过总部进行代理转发访问分部资源，可在分部安全网关上进入页面“高级功能 >> 路由设置 >> 静态路由”设置静态路由如下即可：


## 11.2.5 L2TP 代理配置实例

需求介绍：某公司的总部与分部均使用安全融合网关产品，需要实现将国内分部与国外总部通过 VPN 互联，实现资源相互访问，同时要求数据传输的安全性；且国内分部以及移动办公人员需要通过国外总部代理转发去访问一些国外的网站资源。

拓扑如下：




➢ **站点到站点客户端设置方法**

1. 首先搭建 L2TP VPN 隧道，设置方法见 11.2.4 L2TP 配置实例。

2. 在 VPN 服务器端上设置针对 VPN 地址池的 NAPT 规则，出接口选择上网口。


3. 在 VPN 客户端安全网关上，点击”VPN >> L2TP >> L2TP 客户端”，点击设置 VPN 条目，设置对端子网为 0.0.0.0/0，工作模式设置为 NAT 模式。


4. 在 VPN 客户端安全网关上，进入页面高级功能 >> 路由设置 >> 策略路由，添加策略路由使所有数据优先走 VPN 接口。


- **PC 到站点客户端设置方法**

PC 到站点拨号方法见链接：

[Windows XP] L2TP VPN 客户端拨号操作步骤

[Windows 7] L2TP VPN 客户端拨号操作步骤

[Windows 8] L2TP VPN 客户端拨号操作步骤

[Android] L2TP VPN 客户端拨号操作步骤

PC 拨通 VPN 后，设置”VPN 连接 >>IPv4 选项 >> 高级设置”中，系统已经默认勾选“在远程网络上使用默认网关”，即可实现所有数据走 VPN 接口，实现 VPN 代理上网效果。果未能实现代理上网，可以检查确认 PC 端此处设置：

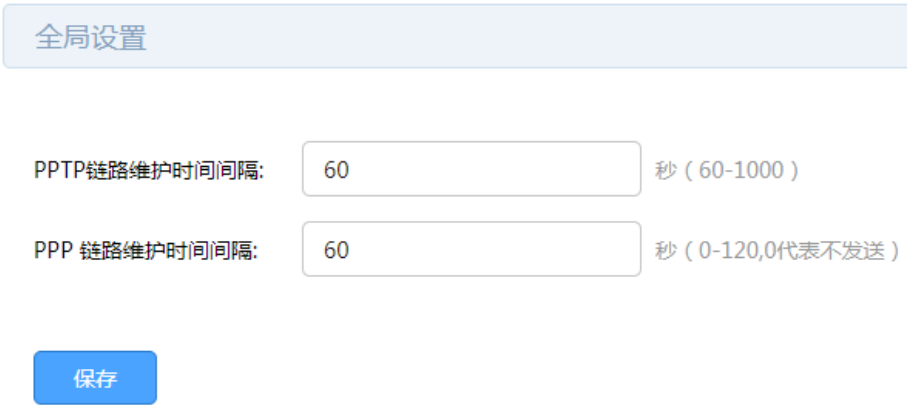

## 11.3 PPTP

企业安全网关提供多类 VPN 功能。其中 PPTP VPN 可以实现企业站点之间搭建安全的数据传输通道，将接入 Internet 的企业分支机构与总部网络通过安全隧道互联，实现资源、信息共享；并支持 PC 端建立 PPTP VPN 隧道，满足外出员工移动办公需求 。

### 11.3.1 PPTP 服务器

进入页面：VPN >> PPTP >> PPTP 服务器，进行全局设置和 PPTP 服务器设置。

- **全局设置**



| | |
|---|---|
| PPTP 链路维护时间间隔 | VPN 拨通成功后，发送 PPTP 链路维护检测报文的时间间隔。 |
| PPP 链路维护时间间隔 | VPN 拨通成功后，发送 PPP 链路维护检测报文的时间间隔。 |

- **服务器设置**

点击<新增>，添加服务器设置条目。

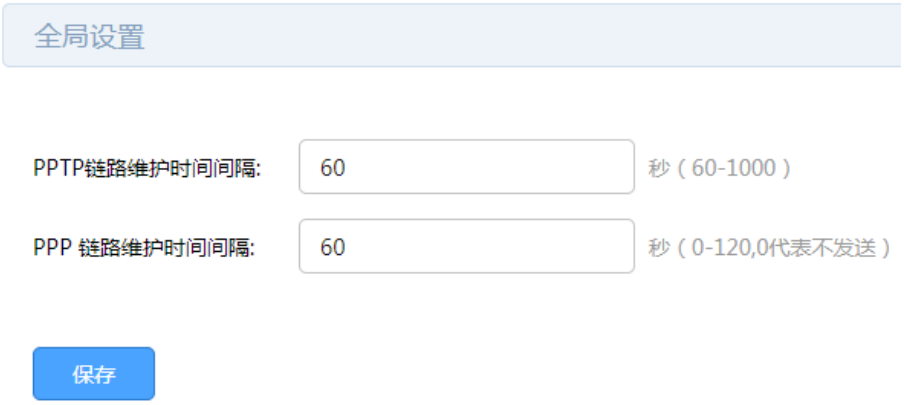

| | |
|---|---|
| 服务接口 | PPTP 服务器监听的接口，只有来自服务接口的报文才会被处理。 |
| MPPE 加密 | 是否对隧道进行加密。若启用，则使用 MPPE 对 PPTP 隧道加密。 |
| MTU | MTU（Maximum Transmission Unit，最大传输单元），在一定物理网络中能传送的最大数据单元。 |

点击页面 ，查看更多页面设置参数信息。

## 11.3.2 PPTP 客户端

进入页面：VPN >> L2TP >> L2TP 客户端，进行全局设置和 L2TP 服务器设置。

- **全局设置**




PPTP 链路维护时间间隔　　VPN 拨通成功后，发送 PPTP 链路维护检测报文的时间间隔。

PPP 链路维护时间间隔　　VPN 拨通成功后，发送 PPP 链路维护检测报文的时间间隔。

- **客户端设置**

点击<新增>，添加客户端设置条目。

| | |
|---|---|
| 隧道名称 | PPTP 隧道的名称，用于区分不同的隧道。 |
| 用户名/密码 | PPTP 隧道用户身份认证的用户名密码，为服务器端设置的用户名和密码。 |
| 出接口 | PPTP 报文收发的接口。 |
| 服务器地址 | PPTP 服务器的地址，可以为 IP 或域名。 |
| MPPE 加密 | 是否对隧道进行加密。若启用，则使用 MPPE 对 PPTP 隧道加密。 |
| 对端子网 | PPTP 隧道对端局域网使用的 IP 地址范围（一般可以填隧道对端设备 LAN 口的 IP 地址范围），由 IP 和子网掩码组成。 |
| 上/下行带宽 | 安全网关会根据上下行带宽进行流量均衡的计算。 |
| MTU | MTU（Maximum Transmission Unit，最大传输单元），在一定物理网络中能传送的最大数据单元。 |
| 工作模式 | NAT：对经过此 PPTP 隧道的数据包进行 NAT 转换（数据包的源 IP 替换为 PPTP 隧道的本地虚拟 IP）。<br>路由：对经过此 PPTP 隧道的数据包只进行路由转发。 |

点击页面，查看更多页面设置参数信息。

## 11.3.3 隧道信息列表

您可以获得 PPTP 隧道的信息。

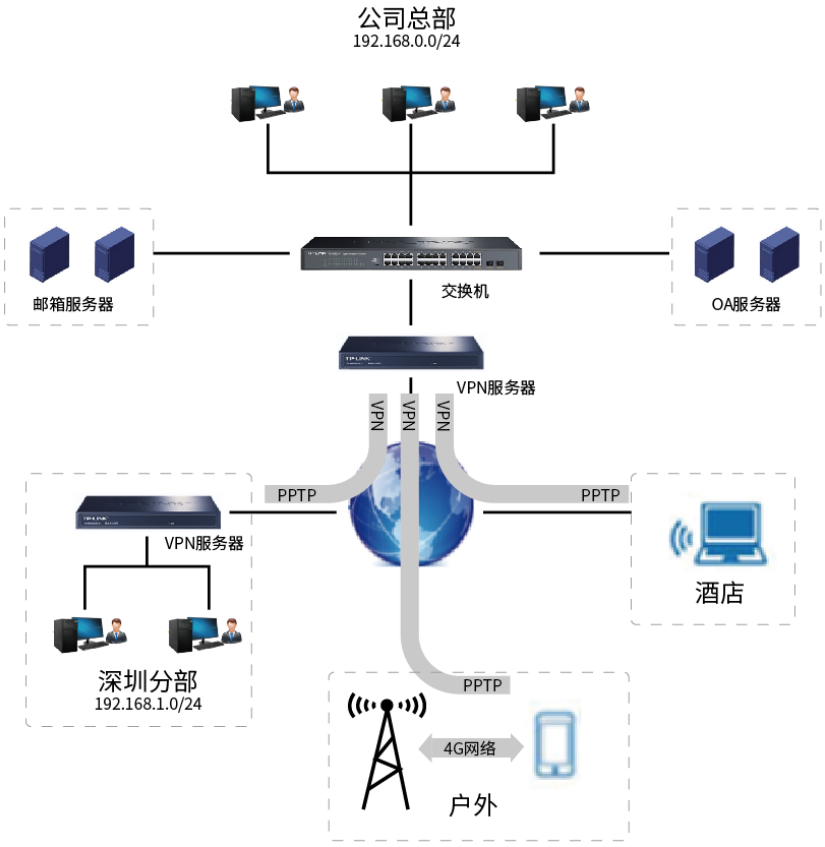
进入页面：VPN >> PPTP >> 隧道信息列表，点击<刷新>，可更新最新的隧道信息列表。

## 11.3.4 PPTP 配置实例

需求介绍：某公司的总部与分部均使用安全融合网关产品。需要实现将北京总部与深圳分公司通过 VPN 互联，实现资源相互访问，同时要求数据传输的安全性。需求参数如下：

| | |
|---|---|
| L2TP 账号/密码 | 123/123 |
| VPN 本地虚拟 IP | 10.10.10.10 |
| 地址池 | 10.10.10.11~10.10.10.200 |
| 加密 | 开启 |
| 总部外网 IP | 183.15.15.15 |
| 总部网段 | 192.168.0.0/24 |
| 总部外网 IP | 183.15.15.30 |
| 分部网段 | 192.168.1.0/24 |

拓扑如下：



本节将分别介绍 PPTP VPN 站点到站点设置方法和 PPTP VPN PC 到站点设置方法。

- **PPTP 站点到站点的设置方法**

1. 在总部 VPN 安全网关上，进入管理页面：基本设置 >> LAN 设置 >> LAN 设置，设置接口 IP 网段为 192.168.0.0/24。


2. 在总部 VPN 安全网关上，进入管理页面：基本设置 >> WAN 设置 >> WAN 设置，设置静态 IP 方式上网或者 PPPoE 方式上网（如果使用的是 PPPoE 上网，由于获取的 IP 地址会变化，此时建议使用动态域名 DDNS），本例使用静态 IP：183.15.15.15。


说明：

- 服务器端 WAN 口 IP 推荐为公网 IP，若非公网 IP，需要在前端设备做映射。

3. 在总部 VPN 安全网关上，进入页面：VPN >> 用户管理 >> IP 地址池，新增隧道地址池(PPTP VPN 隧道通信时使用的 IP 地址)。


4. 在总部 VPN 安全网关上，进入页面：VPN >> 用户管理 >> 用户管理，进行用户管理配置，点击<新增>。


5. 在总部 VPN 安全网关上，进入页面：VPN >> PPTP >> PPTP 服务器，在服务器设置部分点击<新增>，添加 PPTP 服务器规则。

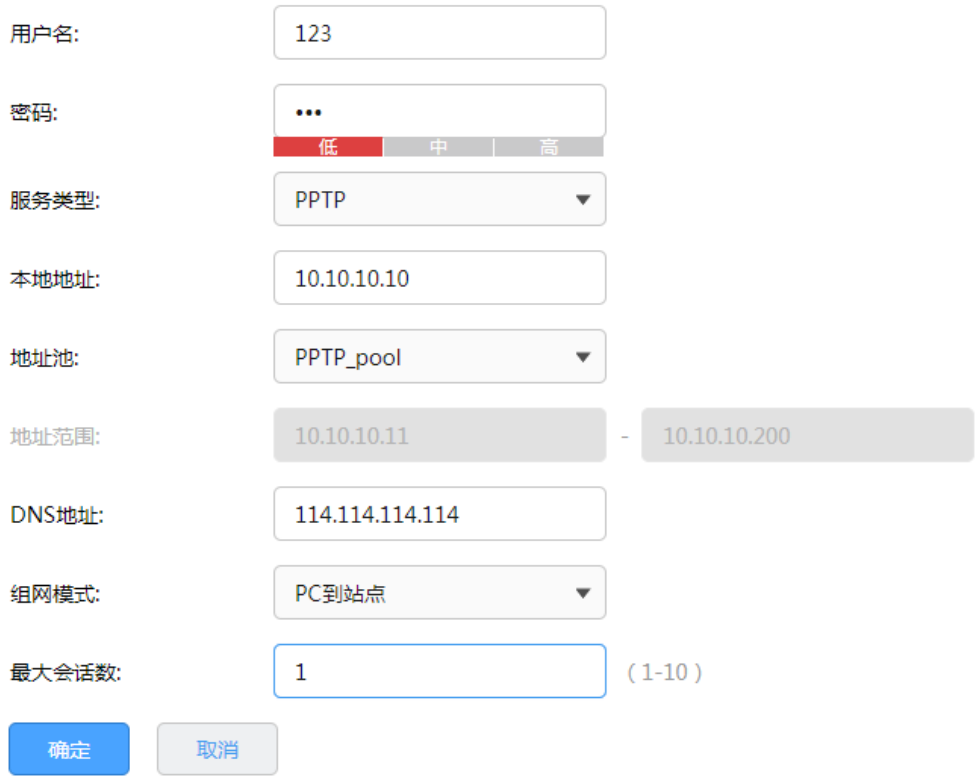

6. 在深圳分部的 VPN 安全网关上，进入管理页面：基本设置 >> LAN 设置 >> LAN 设置，设置接口 IP 网段为 192.168.1.0/24；进入管理页面：基本设置 >> WAN 设置 >> WAN 设置，正确设置 WAN 口上网方式，保证安全网关可以正常上网。

7. 在深圳分部的 VPN 安全网关上，进入页面：VPN >> PPTP >> PPTP 客户端，在客户端设置部分点击<新增>，添加 PPTP 客户端规则。


8. 成功启动总部的服务器端条目和深圳分布的客户端条目，L2TP 隧道信息列表中将有如下条目：


➢ PPTP PC 到站点的设置方法

1. 在总部的 VPN 安全网关上，需要在用户管理配置中添加 PC 到站点的用户账号密码，组网模式选择 PC 到站点，其余设置步骤与上面站点到站点的设置方法相同。




说明：

- 最大会话数：每个用户允许接入的最大客户端数量。注意：用户类型为自动的用户，意味着 L2TP 和 PPTP 的最大接入客户端数量均为最大会话数。

2. 进行 PPTP PC 到站点客户端的拨号设置。

不同 PPTP 客户端的配置方式有所差异，请选择客户端操作系统，参考对应指导文档：

[Windows XP] PPTP VPN 客户端拨号操作步骤

[Windows 7] PPTP VPN 客户端拨号操作步骤

[Windows 8] PPTP VPN 客户端拨号操作步骤

[Android] PPTP VPN 客户端拨号操作步骤

[iOS] PPTP VPN 客户端拨号操作步骤

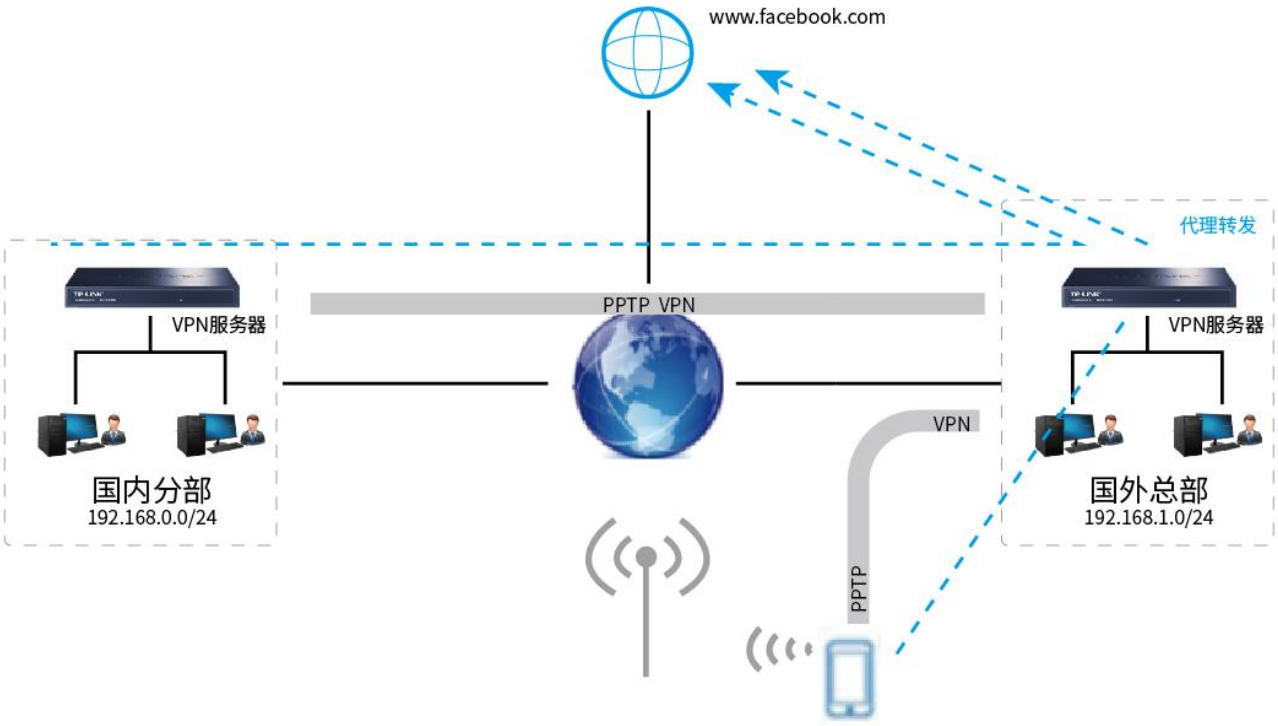
3. 电脑拨号成功后，系统默认勾选了 VPN 连接 IPv4 高级设置中的“在远程网络上使用默认网关”，则电脑所有数据优先从 VPN 接口转发，即可正常访问总部资源。

如果需要通过总部进行代理转发访问分部资源，可在分部安全网关上进入页面“高级功能 >> 路由设置 >> 静态路由”设置静态路由如下即可：


## 11.3.5 PPTP 代理配置实例

需求介绍：某公司的总部与分部均使用安全融合网关产品，需要实现将国内分部与国外总部通过 VPN 互联，实现资源相互访问，同时要求数据传输的安全性；且国内分部以及移动办公人员需要通过国外总部代理转发去访问一些国外的网站资源。

拓扑如下：




➢ **站点到站点客户端设置方法**

1. 首先搭建 PPTP VPN 隧道，设置方法见 11.3.4 PPTP 配置实例。

2. 在 VPN 服务器端上设置针对 VPN 地址池的 NAPT 规则，出接口选择上网口。


3. 在 VPN 客户端安全网关上，点击”VPN >> PPTP >> PPTP 客户端”，点击设置 VPN 条目，设置对端子网为 0.0.0.0/0，工作模式设置为 NAT 模式。


4. 在 VPN 客户端安全网关上，进入页面高级功能 >> 路由设置 >> 策略路由，添加策略路由使所有数据优先走 VPN 接口。


- **PC 到站点客户端设置方法**

PC 到站点拨号方法见链接：

[Windows XP] PPTP VPN 客户端拨号操作步骤

[Windows 7] PPTP VPN 客户端拨号操作步骤

[Windows 8] PPTP VPN 客户端拨号操作步骤

[Android] PPTP VPN 客户端拨号操作步骤

[iOS] PPTP VPN 客户端拨号操作步骤

PC 拨通 VPN 后，设置”VPN 连接 >> IPv4 选项 >> 高级设置”中，系统已经默认勾选“在远程网络上使用默认网关”，即可实现所有数据走 VPN 接口，实现 VPN 代理上网效果。果未能实现代理上网，可以检查确认 PC 端此处设置：


# 11.4 用户管理

## 11.4.1 用户管理

可以配置 L2TP/PPTP 服务器的用户信息。

进入页面：VPN >> 用户管理 >> 用户管理，点击<新增>，设置完成后，点击<确定>即可。

| | |
|---|---|
| 用户名/密码 | 允许拨入的用户名称和密码。 |
| 服务类型 | 根据不同的 VPN 类型选择。 |
| 本地地址 | VPN 隧道的本地虚拟 IP 地址。此地址可以任意设置，对端拨通后可通过此 IP 管理安全网关。 |
| 地址池 | L2TP/PPTP 服务器分配给客户端的 IP 地址从地址池内获取。 |
| DNS 地址 | L2TP/PPTP 服务器分配给客户端的 DNS 地址，如 8.8.8.8。 |
| 组网模式 | PC 到站点：拨入的客户端是个人用户，往往由单个计算机拨入实现远端计算机与本地局域网的通信。<br>站点到站点：拨入的客户端是一个网段的用户，往往通过一个安全网关拨入，实现隧道两端局域网的通信。 |
| 最大会话数 | 每个用户允许接入的最大客户端数量。注意：用户类型为自动的用户，意味着 L2TP 和 PPTP 的最大接入客户端数量均为最大会话数。 |
| 对端子网 | L2TP/PPTP 隧道对端局域网使用的 IP 地址范围（一般可以填隧道对端设备 LAN 口的 IP 地址范围），由 IP 和子网掩码组成。 |

点击页面  ，查看更多页面设置参数信息。

## 11.4.2 IP 地址池

可以配置 L2TP/PPTP 服务器的地址池信息。

进入页面：VPN >> 用户管理 >> IP 地址池，点击<新增>，设置地址池名称和起始/结束 IP 地址，设置完成后点击<确定>。

地址池名称:

起始IP地址:

结束IP地址:

确定 取消

# 第12章 认证管理

安全融合网关提供 Portal 认证服务，包括 Web 认证、一键上网和远程 Portal 认证方式，以及跳转页面、免认证策略和认证参数相关功能。

说明：

- 在进行 Portal 认证的相关设置之前，请先确保无线控制器管理 AP 的接口 IP 地址与待认证客户端的 IP 地址之间路由可达。

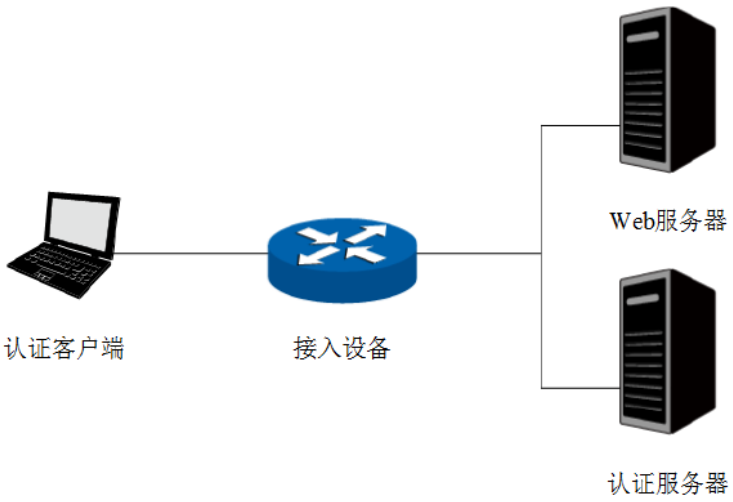
## 12.1 认证设置

### 12.1.1 Web 认证介绍

网关提供 Web 认证功能，在采用 Web 认证的网络中，用户需要先登录认证页面，输入用户名和密码进行认证，认证成功后才可以访问网络资源。

用户主动访问已知的 Web 认证网站，这种开始 Web 认证的方式称作主动认证。反之，如果用户试图通过 HTTP 访问其他网站，将被强制访问 Web 认证网站，从而开始 Web 认证过程，这种方式称作强制认证。

- **Web 认证系统**




认证客户端：需要访问网络资源的用户，将进行 Web 认证。

接入设备：宽带接入设备的统称，包括路由器、交换机和无线控制器等。主要作用有：

1)　　认证前，将用户的所有 HTTP 请求都重定向到 Web 服务器；

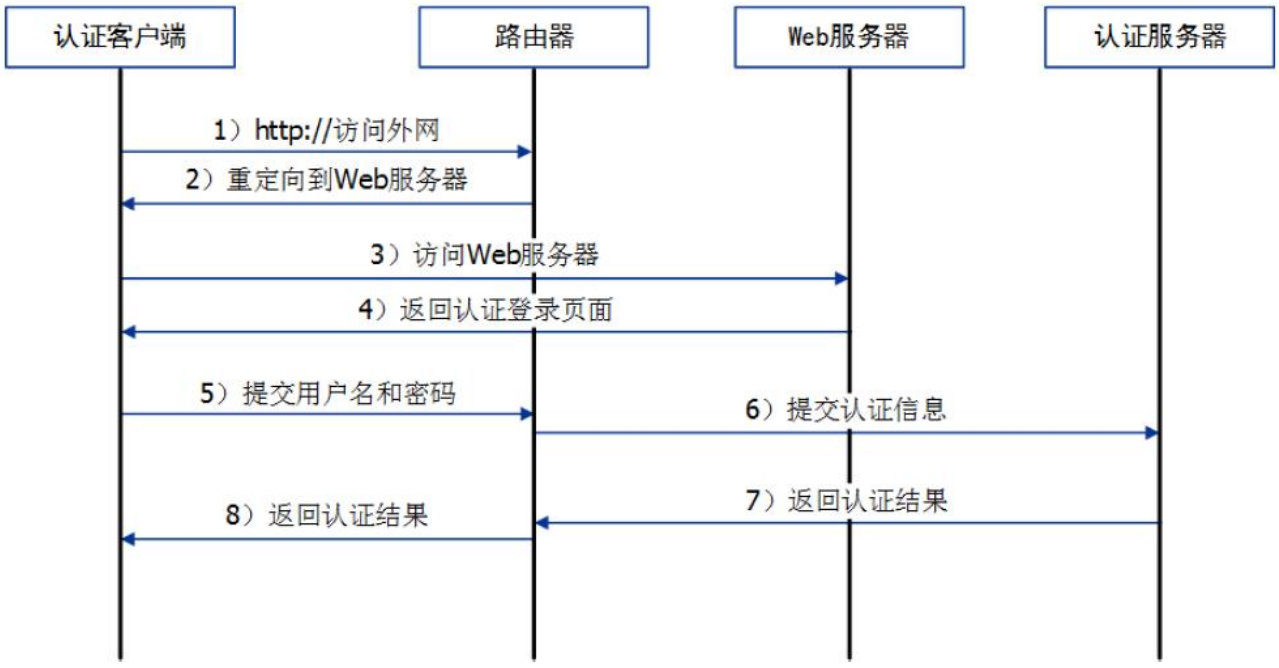
2)　　认证过程中，与认证服务器交互，完成用户的身份认证；

3)　　认证通过后，允许用户访问被管理员授权的网络资源。

Web 服务器：接收认证客户端的 Web 认证请求，提供基于 Web 认证的页面。Web 服务器可以是接入设备之外的独立实体，也可以是存在于接入设备之内的内嵌实体。

认证服务器：与接入设备进行交互，完成对用户的认证。认证服务器可以是接入设备之外的独立实体，也可以是存在于接入设备之内的内嵌实体。

- **Web 认证过程**




1)　认证客户端接入网络，未进行过 Web 认证，通过 HTTP 访问外网；

2)　路由器返回重定向 URL，将认证客户端重定向到 Web 服务器；

3)　认证客户端访问 Web 服务器；

4)　Web 服务器为认证客户端返回认证登录页面；

5)　认证客户端在认证登录页面输入用户名和密码，该信息将提交到路由器；

6)　路由器向认证服务器提交该用户的认证信息；

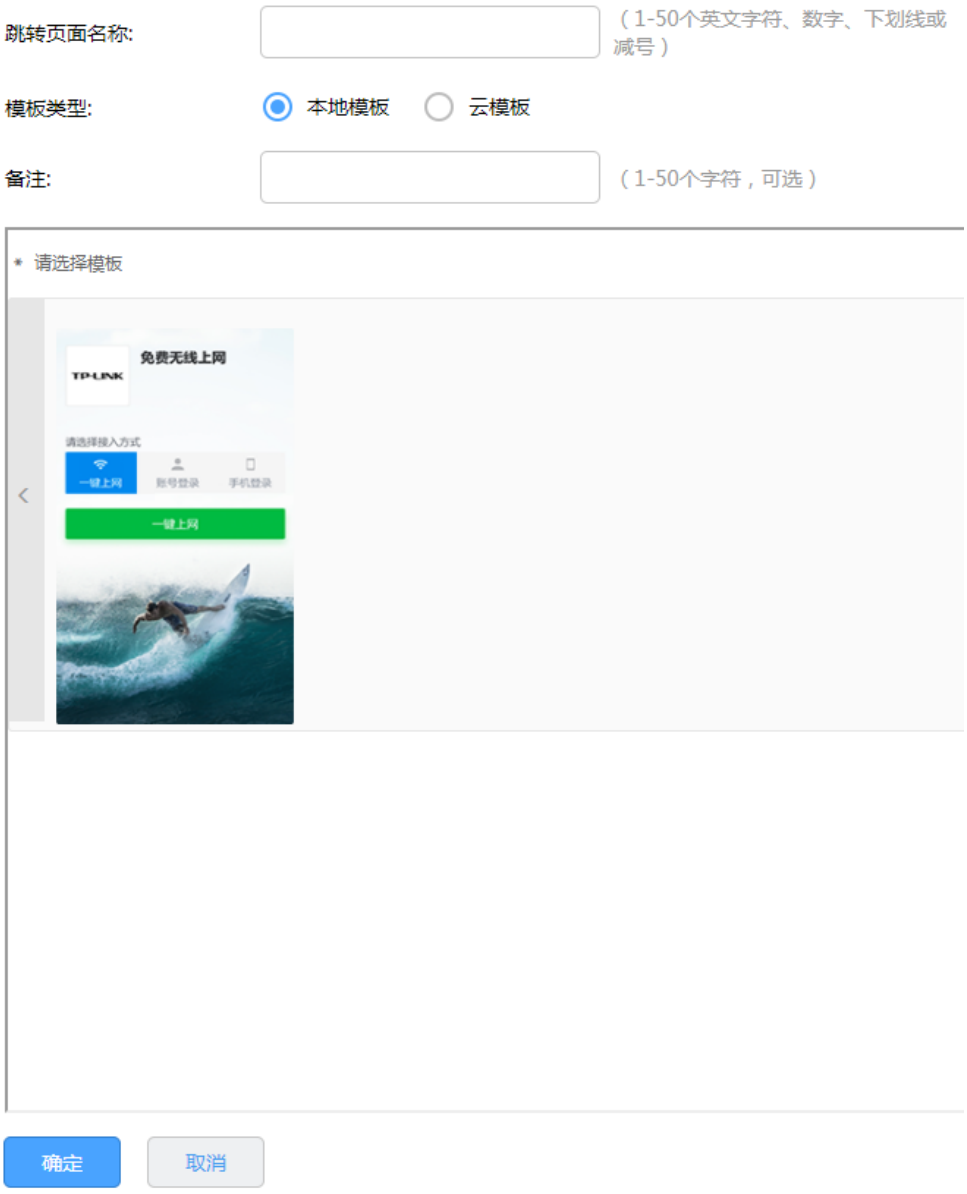
7)　认证服务器向路由器返回认证结果；

8)　路由器向认证客户端返回该认证结果。

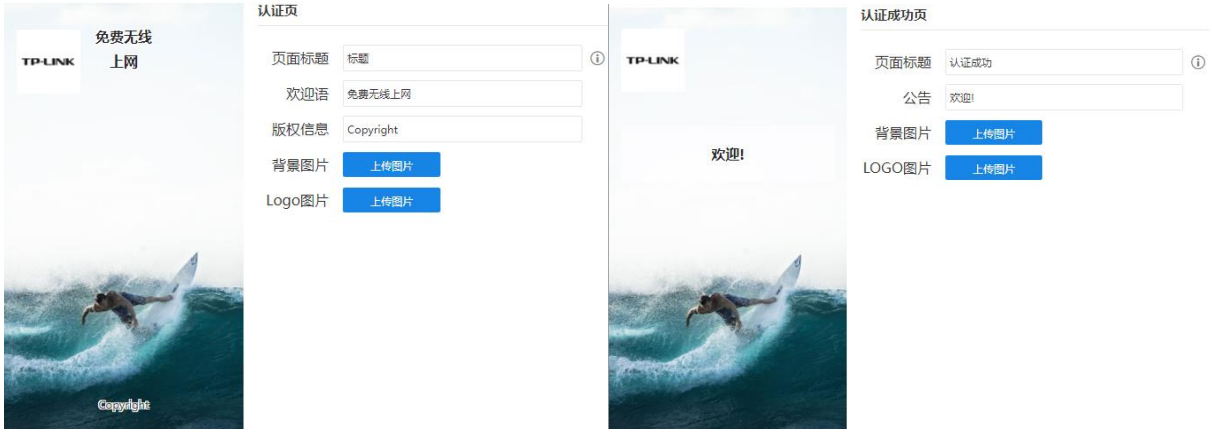
## 12.1.2　跳转页面

在此设置用户认证过程中所看到的认证页面和认证成功页面，可通过图片上传、外部链接或使用默认模板，满足推送广告，推广微信公众号等需求。

进入页面：认证管理 >> 认证设置 >> 跳转页面，点击<新增>，添加认证跳转页面。设置跳转页面名称，选择模板类型，可使用本地模板或自动往上加载云模板。




点击模板，设置认证页面和认证成功页面的标题、内容和背景图片。设置完成后，点击<确定>。




## 12.1.3 组合认证

安全融合网关提供一键上网、Web 认证、短信认证三种认证方式。

进入页面：认证管理 >> 认证设置 >> 组合认证，点击<新增>设置认证规则。

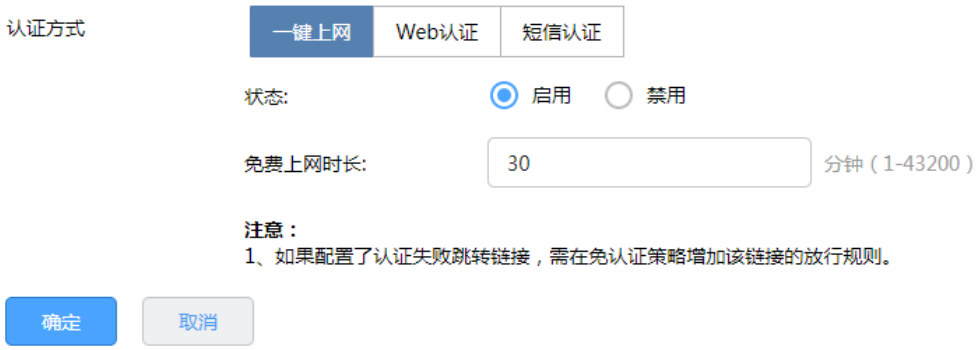

| | |
|---|---|
| 跳转页面名称 | 选择所设置的跳转页面模板，模板设置可参考 12.1.1 |
| 生效 SSID | 选择该认证规则生效的无线网络。 |

| | |
|---|---|
| 认证成功跳转链接 | 设置认证成功后跳转的 URL 地址。 |
| 认证失败跳转连接 | 设置认证失败后跳转的 URL 地址。 |

下面介绍一键上网、Web 认证、短信认证三种认证方式的设置方法。

- **一键上网**

认证方式选择一键上网，启用该认证方式，设置认证用户可以免费上网的时长。若 radius 服务器设置了免费上网时长，生效的时间为 radius 服务器设置的时间。点击<确定>。




注意：

- 如果配置了认证失败跳转链接，需在免认证策略增加该链接的放行规则。

- **Web 认证**

认证方式选择 Web 认证，启用该认证方式，选择认证服务器类型。点击<确定>。


| | |
|---|---|
| 认证服务器类型 | 选择本地服务器或远程服务器进行认证。 |
| 认证服务器组 | 选择进行远程 Portal 认证的服务器组。 |

| | |
|---|---|
| 免费上网时长 | 选择远程服务器进行认证时，若服务器未配置用户上网时长，则使用该时长作为用户的免费上网时长。 |

点击页面，查看更多页面设置参数信息。

注意：

- 如果配置了认证失败跳转链接，需在免认证策略增加该链接的放行规则。
- 认证服务器类型为远程服务器时，若服务器配置了用户上网时间，则免费上网时长为服务器返回的时间，否则为本页面配置的免费上网时长。

➢ **短信认证**

在第三方平台中设置短信服务，详细设置方法请点击参考不同平台短信服务的设置方法。

认证方式选择短信认证，启用该认证方式，设置各项参数，点击<确定>。


| | |
|---|---|
| 状态 | 启用短信认证方式 |
| 免费上网时长 | 设置认证用户可以免费上网的时长。若 radius 服务器设置了免费上网时长，生效的时间为 radius 服务器设置的时间。 |

| | |
|---|---|
| 验证码有效期 | 用户在该时间内输入验证码进行验证有效，否则需重新获取验证码。 |
| 通道类型 | 选择发送短信的平台，本产品支持阿里云、网易云信、腾讯云、百度云和 HTTP 协议五种平台。 |

点击页面 ，查看更多页面设置参数信息。

注意：

- 如果配置了认证失败跳转链接，需在免认证策略增加该链接的放行规则。
- 配置了短信认证条目，为了无线 PC 能够顺利完成认证，需要保证设备可以联网。
- 使用短信认证功能前，必须要先在“系统工具->时间设置”中正确地配置本机系统时间。。

## 12.1.4 远程认证

可以通过本页面设置使用外部 Web 服务器的认证方式，查看远程 Portal 认证条目。

进入页面：认证管理 >> 认证设置 >> 远程认证，点击<新增>设置远程认证规则。

| | |
|---|---|
| 跳转页面名称 | 选择所设置的跳转页面模板，模板设置可参考 12.1.1 |
| 生效 SSID | 选择该认证规则生效的无线网络。 |
| 认证成功跳转链接 | 设置认证成功后跳转的 URL 地址。 |
| 认证失败跳转连接 | 设置认证失败后跳转的 URL 地址。 |
| 远程 Portal 地址 | 每个用户允许接入的最大客户端数量。注意：用户类型为自动的用户，意味着 L2TP 和 PPTP 的最大接入客户端数量均为最大会话数。 |
| 认证服务器类型 | 选择本地服务器或远程服务器进行认证。 |
| 认证服务器组 | 选择进行远程 Portal 认证的服务器组。 |
| 免费上网时长 | 选择远程服务器进行认证时，若服务器未配置用户上网时长，则使用该时长作为用户的免费上网时长。 |

点击页面  ，查看更多页面设置参数信息。

## 12.1.5 免认证策略

目前越来越多的公共场所（如商场、酒店、景区等）需要提供免费网络供访客使用，访客连接网络后需要通过认证才可以免费使用网络。免认证策略可以实现客户端不需要认证就能访问指定的网站或者服务器。

进入页面：认证管理 >> 认证设置 >> 免认证策略，点击<新增>设置远程认证规则。

免认证策略提供两种认证方式：五元组方式和 URL 方式。

- **五元组方式**

主要依据 IP 地址范围、MAC 地址、VLAN ID、端口和服务协议设置策略，当需要限制的免认证参数种类较多时，推荐使用五元组方式。


| | |
|---|---|
| 策略名称 | 填写免认证策略条目的名称。 |
| 免认证方式 | 免认证策略的匹配方式：五元组方式 |
| 源/目的 IP 地址范围 | 设置免认证策略的源/目的 IP 地址和网络掩码。。 |
| 源 MAC 地址 | 设置免认证策略的源 MAC 地址。 |
| 源/目的端口范围 | 设置免认证策略的源/目的端口范围。 |
| 服务协议 | 设置免认证策略的服务协议。 |

点击页面 ，查看更多页面设置参数信息。

- URL 方式

主要依据 URL 设置策略，当已知 URL 时，推荐使用 URL 方式。


| | |
|---|---|
| 策略名称 | 填写免认证策略条目的名称。 |
| 免认证方式 | 免认证策略的匹配方式： URL 方式 |
| URL 地址 | 输入 URL 地址 |
| 源 IP 地址范围 | 设置免认证策略的源 IP 地址和网络掩码。。 |
| 源 MAC 地址 | 设置免认证策略的源 MAC 地址。 |

点击页面，查看更多页面设置参数信息。

## 12.1.6 全局参数

通过本页面可设置认证老化时间和 Portal 认证端口。

进入页面：认证管理 >> 认证设置 >> 全局参数，设置认证老化时间和 Portal 认证端口，点击<保存>。

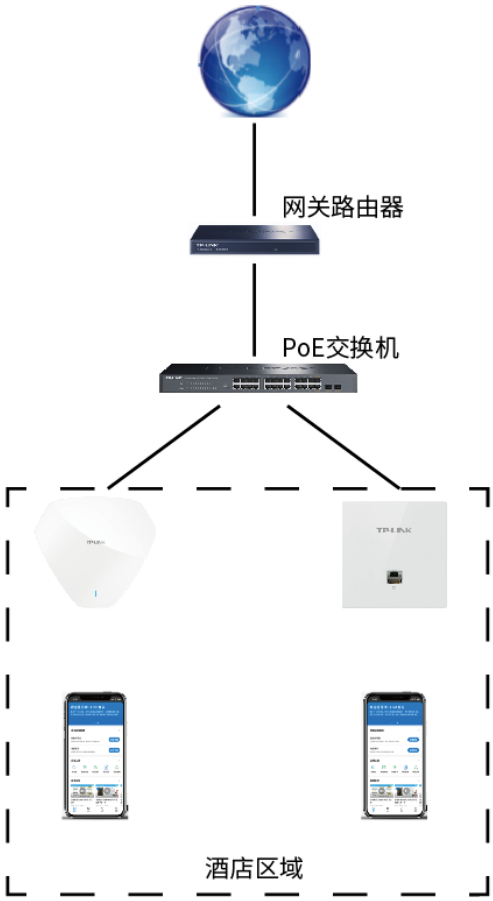

| | |
|---|---|
| 认证老化时间 | 当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。 |
| Portal 认证端口 | 用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。 |
| 认证模式 | 支持基于 SSID 和基于接口两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于接口表示与这个接口相连的终端都需要认证才能上网。默认基于 SSID。 |

# 12.2 认证设置配置实例

## 12.2.1 一键上网配置实例

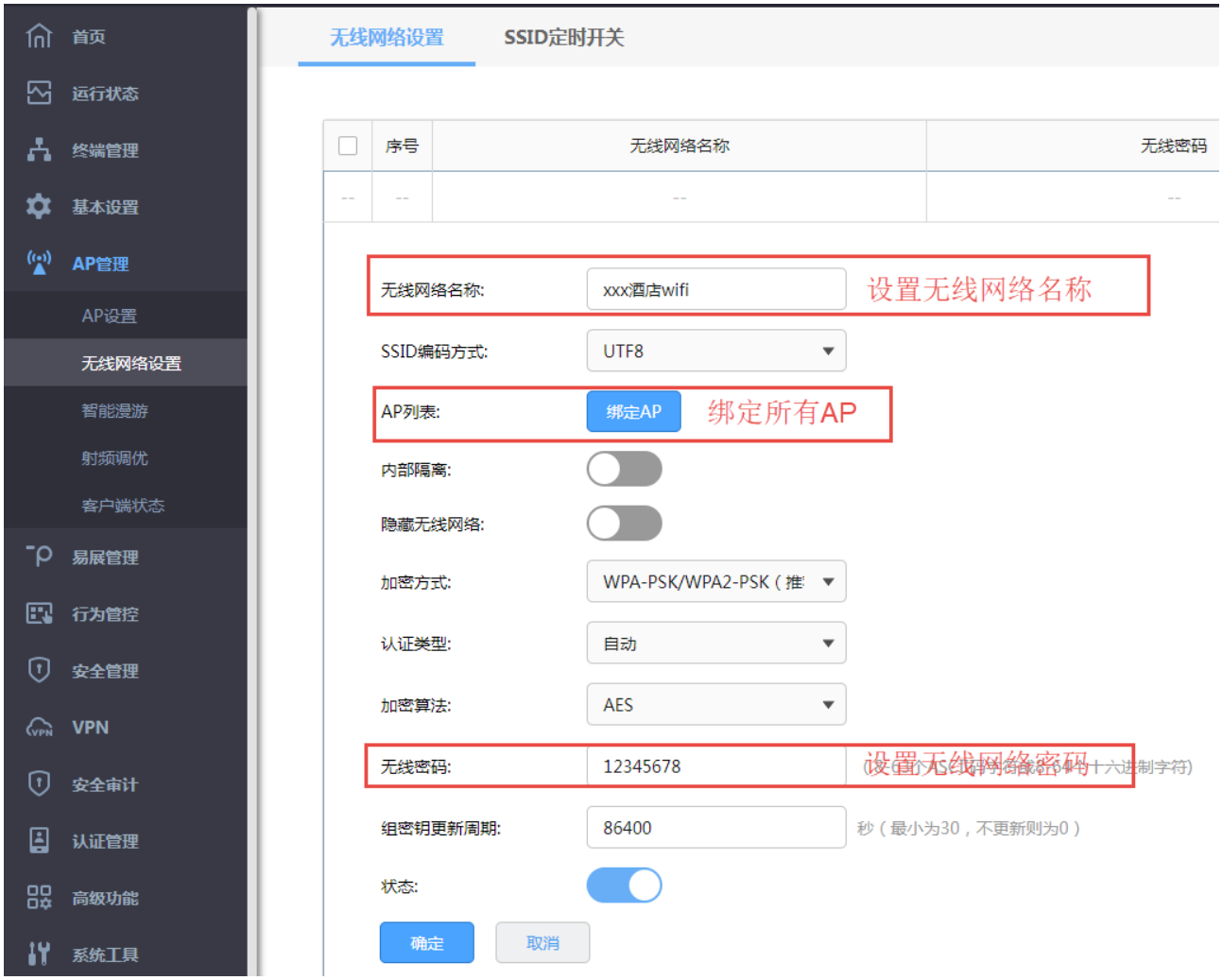
需求介绍：目前越来越多的公共场所（如商场、酒店、景区等）需要提供免费网络供访客使用，访客接入网络的方式有很多，一键认证就是其中的一种。商户可以通过一键认证推送广告，而访客无需账号密码，一键免费上网。某酒店需要实现无线覆盖，为顾客提供无线网络接入，有以下需求：顾客连接无线后可以收到酒店推送的广告页面，且无需用户填写登录信息。

拓扑如下：



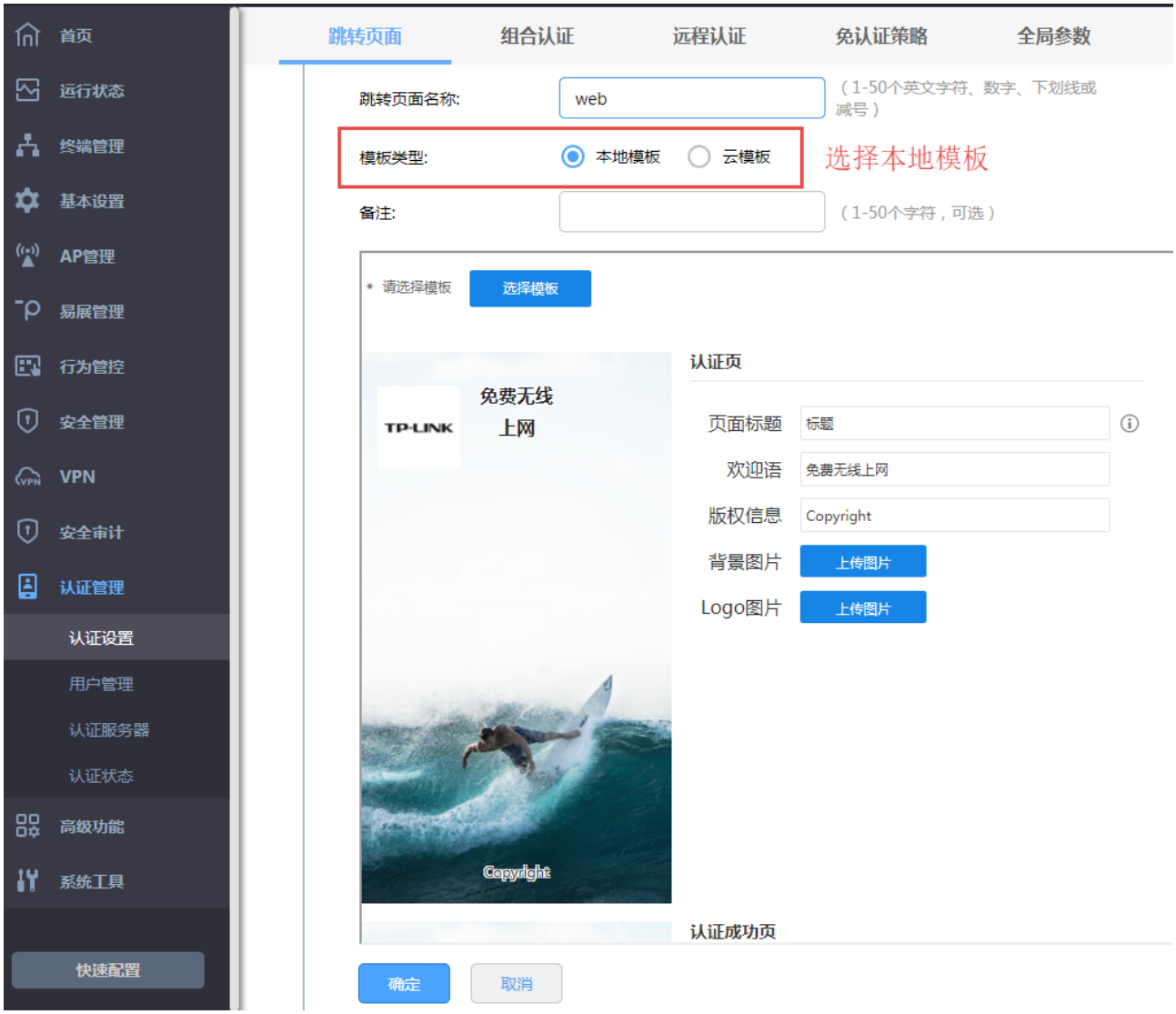

配置方法如下：

1. 新增无线网络并进行射频绑定，进入页面 AP 管理 >> 无线网络设置，在“无线网络设置”部分点击 <新增>，设置酒店 SSID。




2. 设置认证参数，进入页面“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式。

3. 配置内置 Web 服务器，进入页面认证管理 >> 认证设置 >> 跳转页面，更具实际需求设置跳转页面标贴、欢迎信息等，背景图片和 LOGO 可以自助上传。




4. 配置内置认证服务器，进入页面认证管理 >> 认证设置 >> 组合认证，点击新增，认证方式选择一键上网。

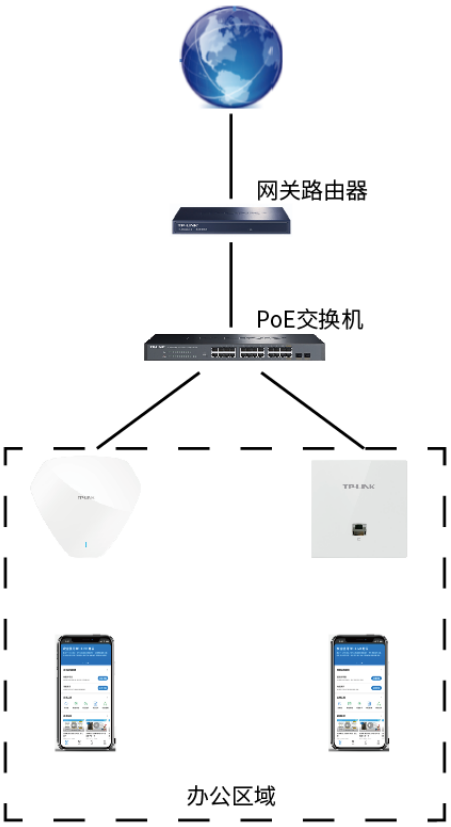

## 12.2.2 短信认证配置实例

目前越来越多的公共场所（如商场、酒店、景区等）需要提供免费网络供访客使用，访客连接网络后需要通过认证才可以免费使用网络。接入认证方式有很多，短信认证就是其中的一种，访客需要输入手机号获取验证码并通过验证后才能免费上网。 我司网关路由器的短信认证功能支持和阿里云、腾讯云、百度云、网易云信以及第三方使用 HTTP 协议的服务器进行对接，从而实现短信认证上网的需求。

注意：

- 使用短信认证时，短信服务平台会收取通信服务费，具体收费标准请参考云平台。

需求介绍：某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求： 办公区员工连接无线后需要在 Web 页面中输入手机号进行短信认证，认证通过之后才能上网。



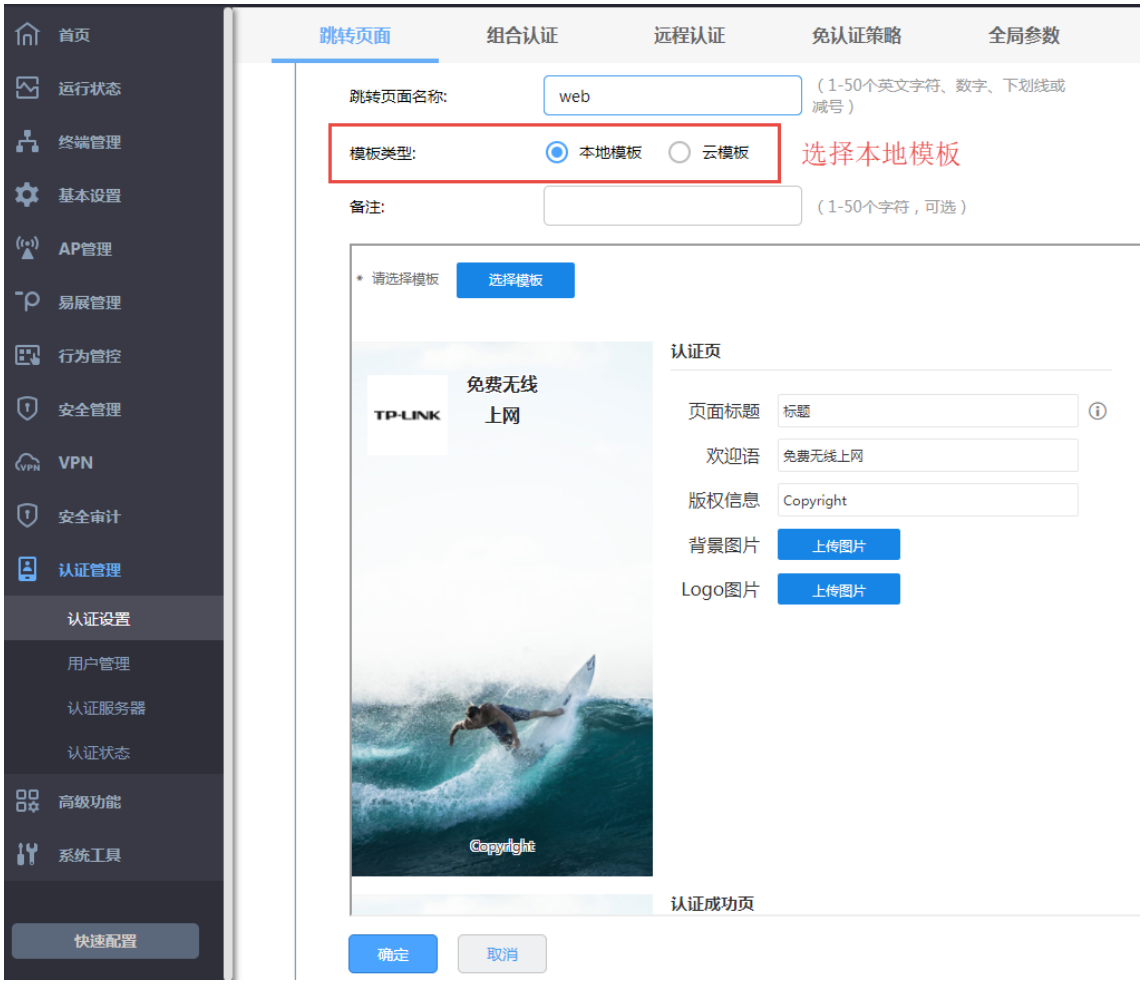

配置方法：

1. 在第三方平台中设置短信服务，详细设置方法请点击参考不同平台短信服务的设置方法。

2. 新增无线网络并进行射频绑定，进入页面 AP 管理 >> 无线网络设置，在“无线网络设置”部分点击<新增>，设置公司 SSID。

3. 设置认证参数，进入页面“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式。


4. 配置内置 Web 服务器，进入页面认证管理 >> 认证设置 >> 跳转页面，更具实际需求设置跳转页面标贴、欢迎信息等，背景图片和 LOGO 可以自助上传。



5. 配置内置认证服务器，进入页面认证管理 >> 认证设置 >> 组合认证，点击新增，认证方式选择短信认证，根据实际需要设置免费上网时长和验证码有效期等信息。

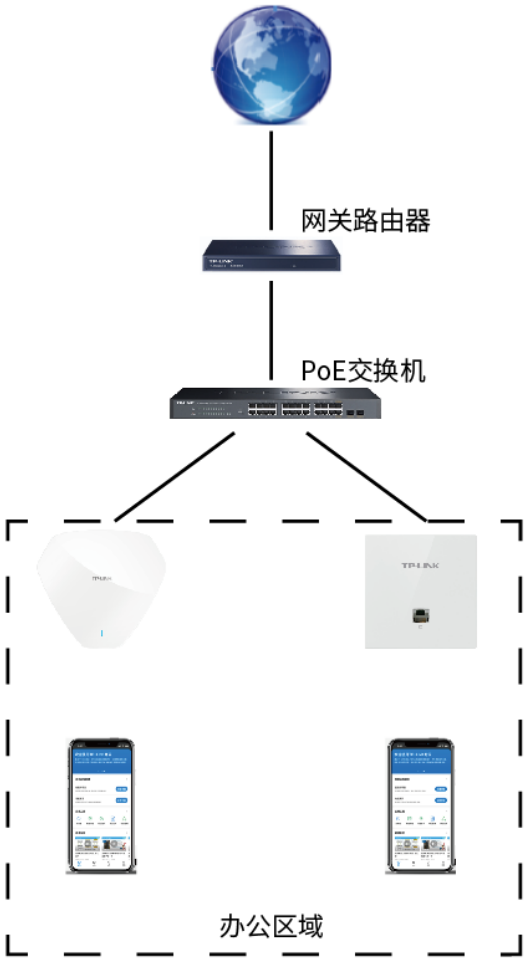

通道类型填写所使用的第三方平台（阿里云、腾讯云、百度云、网易云信、HTTP 协议的服务器），以及填写相应的参数信息（详细设置方法请点击参考不同平台短信服务的设置方法），填写完毕点击<确定>。

## 12.2.3 Web 认证配置实例—使用内置 Web 服务器和内置认证服务器

随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户

提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。安全融合网关支持 Portal 功能，认证方式灵活，支持广告推送。

需求介绍：某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求：办公区员工连接无线后需在 Web 页面中输入正确的用户名和密码，认证通过之后才能上网。拓扑如下：

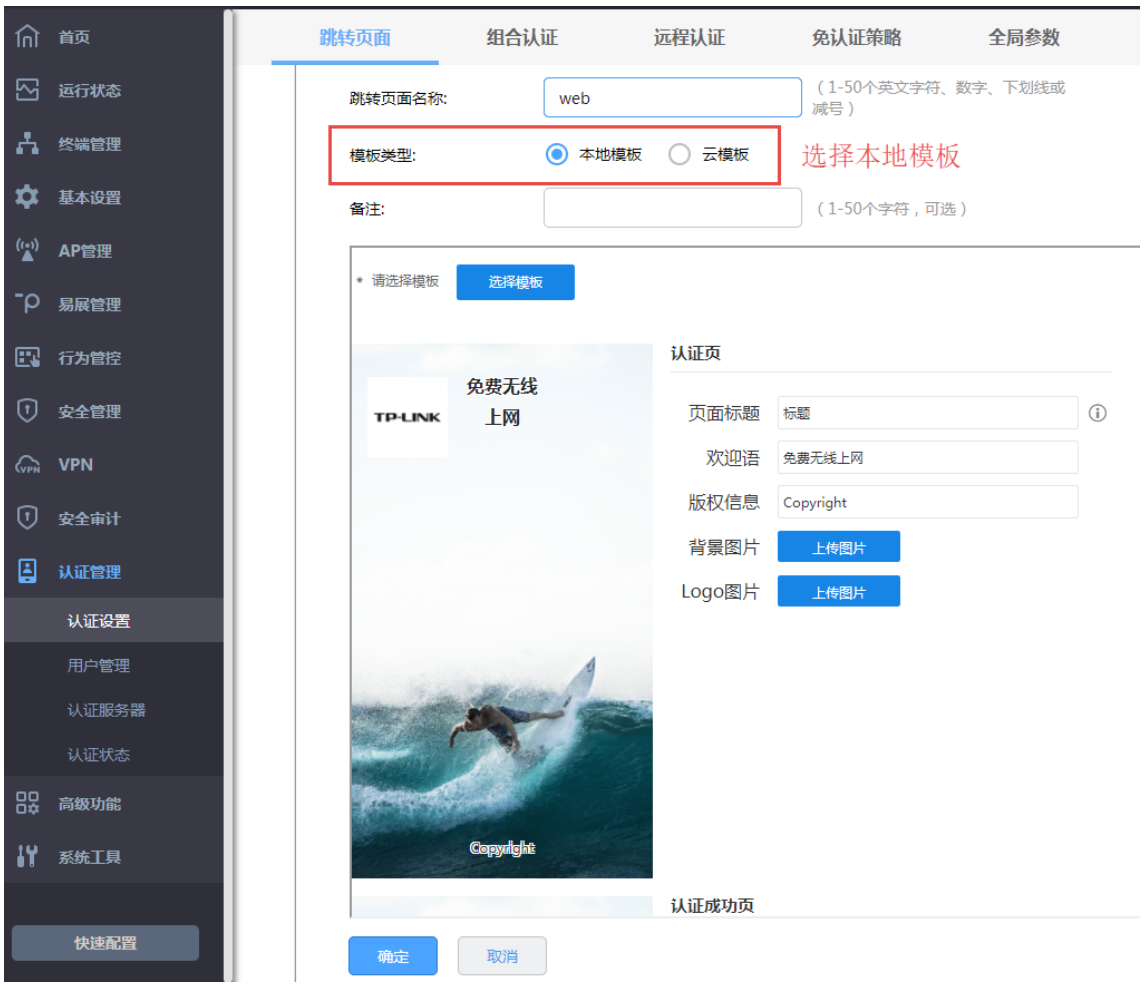



配置方法：

1. 新增无线网络并进行射频绑定，进入页面 AP 管理 >> 无线网络设置，在“无线网络设置”部分点击<新增>，设置公司 SSID。


2. 设置认证参数，进入页面“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式。


3. 配置内置 Web 服务器，进入页面认证管理 >> 认证设置 >> 跳转页面，根据实际需求设置跳转页面标贴、欢迎信息等，背景图片和 LOGO 可以自助上传。




4. 配置内置认证服务器，进入页面认证管理 >> 认证设置 >> 组合认证，点击新增，认证方式选择 Web 认证，认证服务器类型选择本地服务器。

5. 点击“认证管理 >> 用户管理 >> 认证用户管理”，点击<新增>，设置认证用户名和密码，根据实际需求可以设置免费用户和正式用户，并设置其他参数，如下图：


以上内容配置完毕，网关的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

## 12.2.4 Web 认证配置实例—使用内置 Web 服务器和外部认证服务器

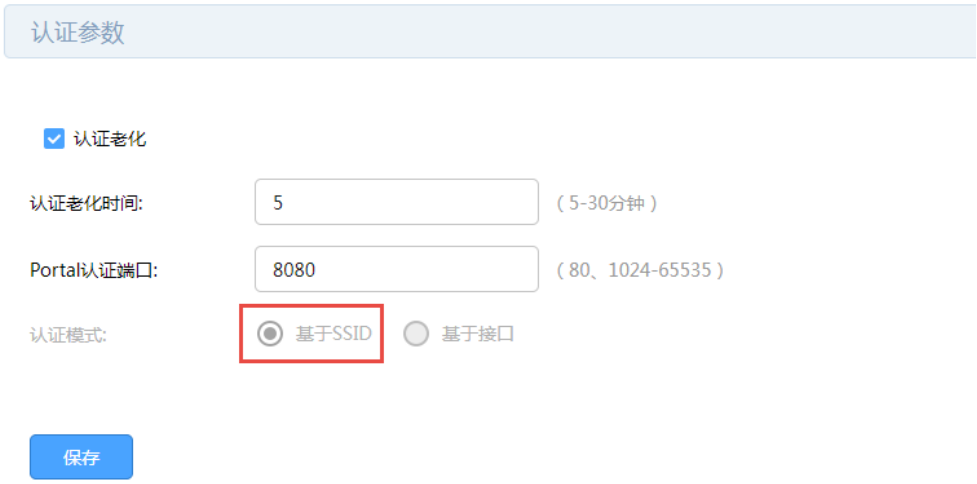
随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。安全融合网关支持 Portal 功能，认证方式灵活，支持广告推送。

需求介绍：某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求：办公区员工连接无线后需在 Web 页面中输入正确的用户名和密码，认证通过之后才能上网。拓扑如下：


配置方法：

1. 新增无线网络并进行射频绑定，进入页面 AP 管理 >> 无线网络设置，在“无线网络设置”部分点击<新增>，设置公司 SSID。

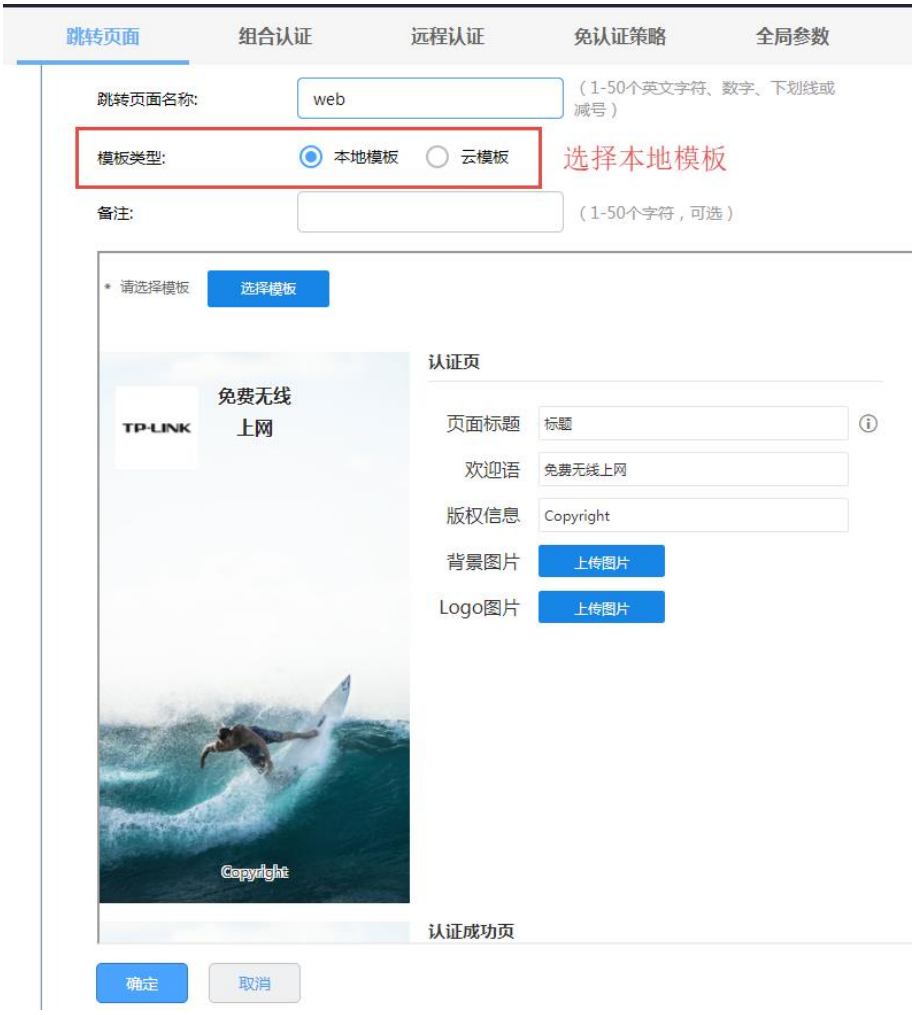
2. 设置认证参数，进入页面“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式。




3. 配置外部认证服务器，进入页面“认证管理 >> 认证服务器 >> Radius 服务器”，根据自己设置的外部认证服务器在路由器添加条目。


4. 添加外部服务器组，进入页面“认证管理 >> 认证服务器 >> 认证服务器”，点击<新增>，设置认证服务器组。


5. 配置内置 Web 服务器，进入页面认证管理 >> 认证设置 >> 跳转页面，更具实际需求设置跳转页面标贴、欢迎信息等，背景图片和 LOGO 可以自助上传。



6. 配置内置认证服务器，进入页面认证管理 >> 认证设置 >> 组合认证，点击新增，认证方式选择 Web 认证，认证服务器类型选择本地服务器。


7. 点击“认证管理 >> 用户管理 >> 认证用户管理”，点击<新增>，设置认证用户名和密码，根据实际需求可以设置免费用户和正式用户，并设置其他参数，如下图：

以上内容配置完毕，网关的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

## 12.2.5 Web 认证配置实例—使用外置 Web 服务器和内置认证服务器

随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。安全融合网关支持 Portal 功能，认证方式灵活，支持广告推送。

需求介绍：某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求：办公区员工连接无线后需在 Web 页面中输入正确的用户名和密码，认证通过之后才能上网。拓扑如下：


配置方法：

1. 新增无线网络并进行射频绑定，进入页面 AP 管理 >> 无线网络设置，在“无线网络设置”部分点击<新增>，设置公司 SSID。


2. 设置认证参数，进入页面“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式。


3. 配置外部 Web 服务器，进入页面“认证管理 >> 认证设置 >> 远程认证”，点击<新增>，认证服务器类型选择本地服务器。

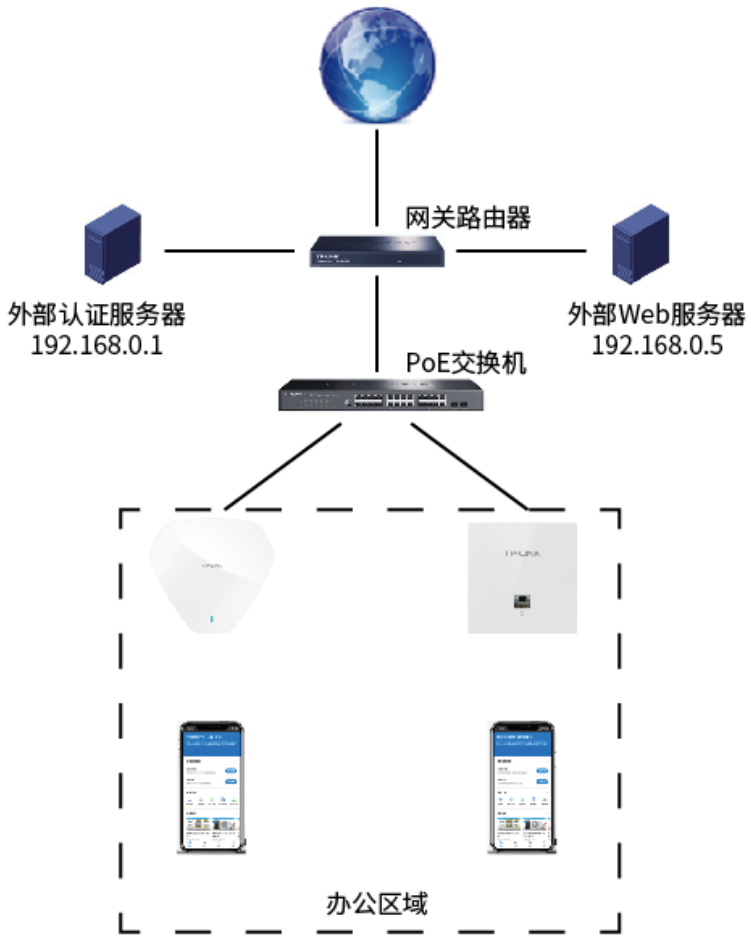

4. 点击“认证管理 >> 用户管理 >> 认证用户管理”，点击<新增>，设置认证用户名和密码，根据实际需求可以设置免费用户和正式用户，并设置其他参数，如下图：

以上内容配置完毕，网关的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

## 12.2.6 Web 认证配置实例—使用外置 Web 服务器和外置认证服务器

随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。安全融合网关支持 Portal 功能，认证方式灵活，支持广告推送。

需求介绍：某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求：办公区员工连接无线后需在 Web 页面中输入正确的用户名和密码，认证通过之后才能上网。拓扑如下：




配置方法：

1. 新增无线网络并进行射频绑定，进入页面 AP 管理 >> 无线网络设置，在“无线网络设置”部分点击<新增>，设置公司 SSID。


2. 设置认证参数，进入页面“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式。


3. 配置外部认证服务器，进入页面“认证管理 >> 认证服务器 >> Radius 服务器”，根据自己设置的外部认证服务器在路由器添加条目。


4. 添加外部服务器组，进入页面“认证管理 >> 认证服务器 >> 认证服务器”，点击<新增>，设置认证服务器组。


5. 配置外部 Web 服务器，进入页面“认证管理 >> 认证设置 >> 远程认证”，点击<新增>，认证服务器类型选择本地服务器。


6. 点击“认证管理 >> 用户管理 >> 认证用户管理”，点击<新增>，设置认证用户名和密码，根据实际需求可以设置免费用户和正式用户，并设置其他参数，如下图：

以上内容配置完毕，网关的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

## 12.2.7　免认证策略配置实例

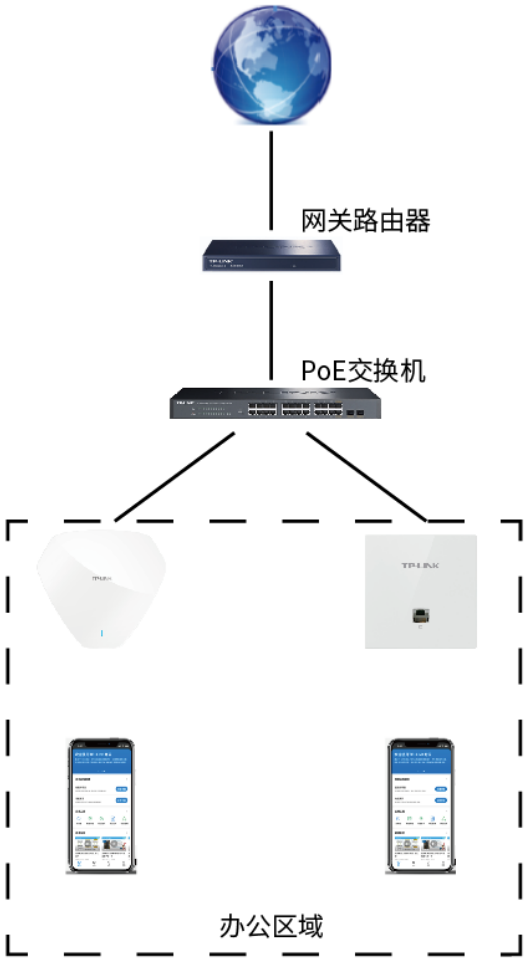
需求介绍：某办公室需要实现无线覆盖，员工需要通过认证后才能上网，有以下需求：

1)　特定终端如打印机不需要认证即可上网；

2)　员工无需认证也可以访问公司外网服务器；

3)　员工无需认证也可以访问公司网站；

拓扑如下：




设置方法：

1. 首先实现固定设备无需认证即可上网。进入路由器界面，点击“认证管理 >> 认证设置 >> 免认证策略”，点击<新增>添加免认证策略，使特定终端无需上网认证即可。


由于终端上网可能即需要使用 UDP 协议又需要使用 TCP 协议，所以一个终端设备需要建立两条免认证策略服务协议分别选择 UDP 和 TCP。

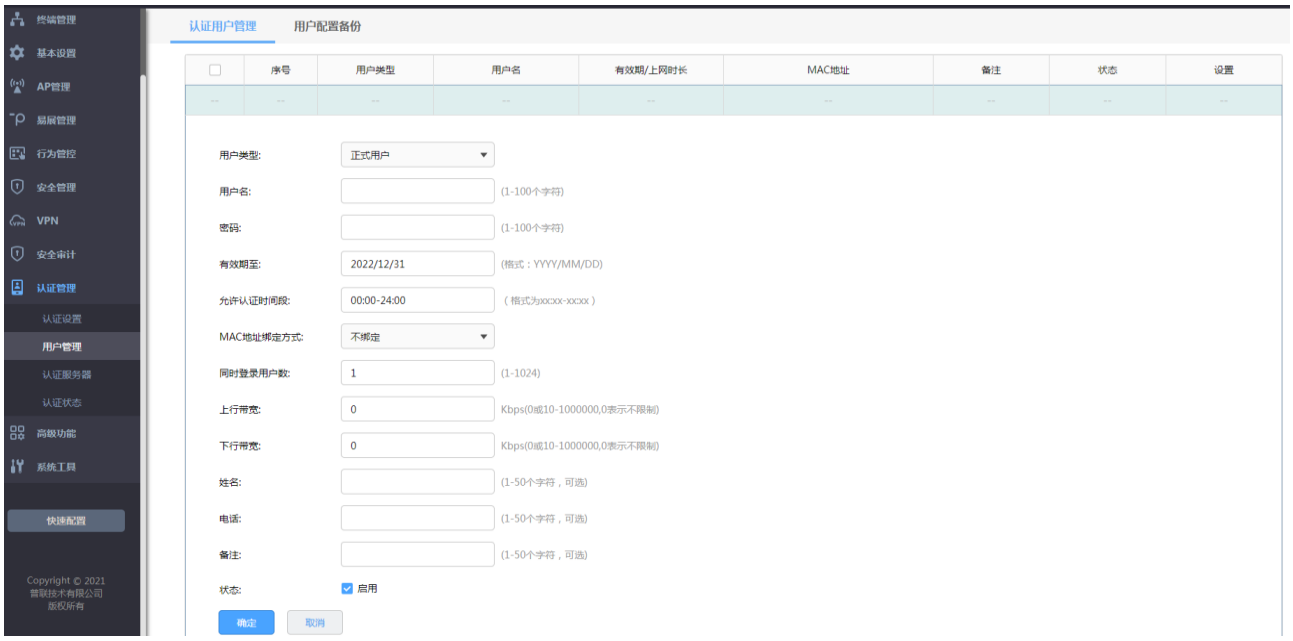
2. 设置无需认证即可访问到指定的外网服务器，点击“认证管理 >> 认证设置 >> 免认证策略”，点击<新增>添加免认证策略。


3. 设置无需认证即可访问到指定的网站，进入路由器界面，点击“认证管理 >> 认证设置 >> 免认证策略”，添加免认证策略。

# 12.3 用户管理

## 12.3.1 认证用户管理

进入页面：认证管理 >> 用户管理 >> 认证用户管理，可查看已添加的认证用户列表。点击<新增>，添加用户账号。




| | |
|---|---|
| 用户类型 | 选择用户类型。<br>正式用户：存留在系统中的正式用户，具有一定的有效期，且可以绑定相应的设备 MAC 地址。可以记录更多用户的资料信息。<br>免费用户：免费用户具有一定的上网时长限制。 |
| 用户名 | 用于认证登录的用户名。 |
| 密码 | 用户登录所使用的密码。 |
| 有效期至 | 正式用户的有效期。 |
| 允许认证时间段 | 允许用户进行认证的时间。 |

| | |
|---|---|
| MAC 地址绑定方式 | 选择是否绑定 MAC 地址，以及绑定的方式。<br>不绑定：不绑定用户的 MAC 地址。<br>静态绑定：绑定一个静态的 MAC 地址。<br>动态绑定：进行动态绑定。 |
| 同时登录用户数 | 最多允许同时使用该账号登录的用户数量。 |
| 上/下行带宽 | 当前用户允许的上/下行带宽，以 Kbps 为单位，0 表示不限制。当开启此功能时，系统默认的 NAT 加速功能将会被关闭，因此转发性能会受到一定程度的影响。 |
| 姓名 | 可选记录当前用户姓名。 |
| 电话 | 可选记录当前用户电话。 |

点击页面，查看更多页面设置参数信息。

## 12.3.2 用户配置备份

进入页面：认证管理 >> 用户管理 >> 用户配置备份。

点击<备份>，可将当前信息保存至本地。

点击<浏览>，选择用户配置文件，点击<导入>可批量导入用户信息。

# 12.4 认证服务器

网关提供指定外部 Radius 服务器进行认证的功能。

外部 Radius 服务器认证，即当用户接入时，无线控制器将用户的身份认证信息提交给外部服务器，由外部服务器认证身份信息。

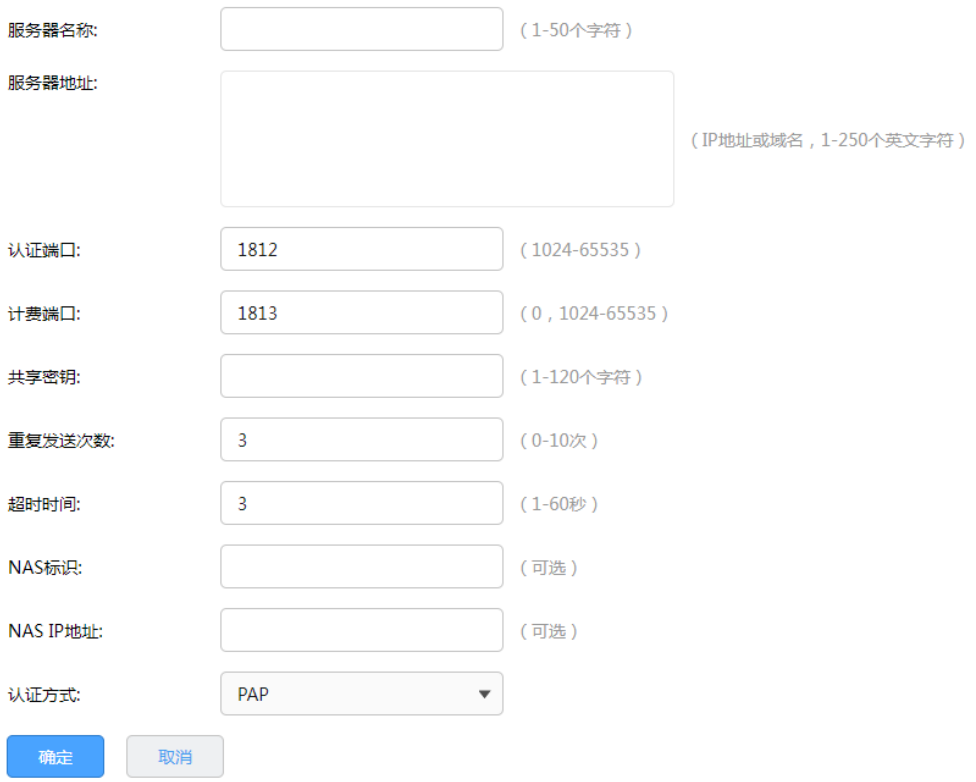
- **配置 Radius 认证服务器步骤**

1. 设置 Radius 服务器。必须操作。配置界面：认证管理 >> 认证服务器 >> Radius 服务器。
2. 设置服务器组。必须操作。配置界面：认证管理 >> 认证服务器 >> 认证服务器。

## 12.4.1 Radius 服务器

可以通过本界面添加、修改或删除一个外部 Radius 服务器。Radius 支持认证服务和计费服务功能。

进入页面：认证管理 >> 认证服务器 >> Radius 服务器，点击<新增>，设置 Radius 服务器。




| | |
|---|---|
| 服务器名称 | 您可以配置 Radius 服务器的名称。 |
| 服务器地址 | 设置服务器的地址，IPv4 地址或者 DNS 域名。 |

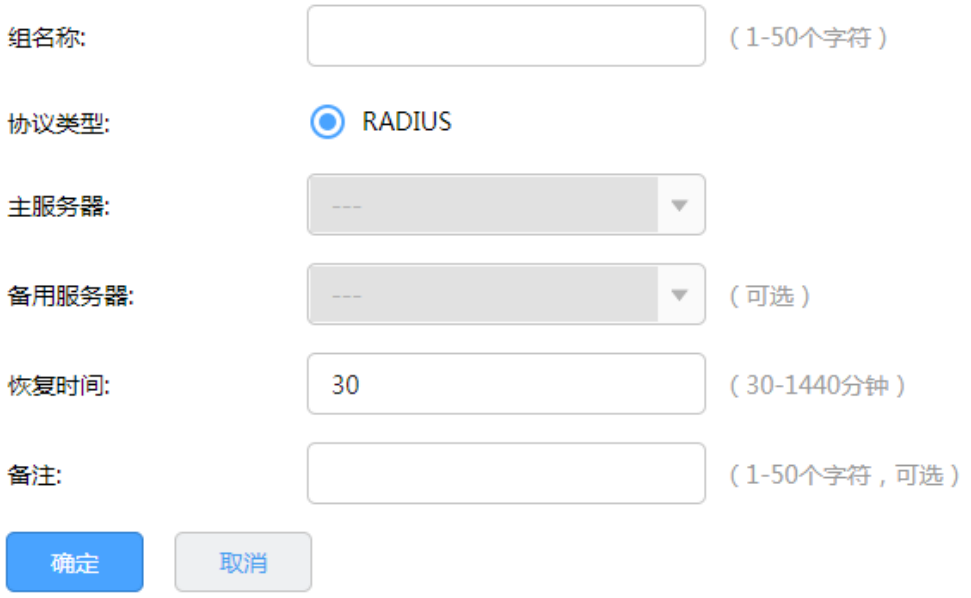
| | |
|---|---|
| 认证端口 | 服务器监听认证报文的端口。 |
| 计费端口 | 服务器监听计费报文的端口，0 表示不启用计费功能。 |
| 共享密钥 | Radius 服务器配置的共享密钥。 |
| 重复发送次数 | 当客户端发送请求后，如果没有收到回复，重复发送请求的次数。 |
| 超时时间 | 当客户端发送请求后，数据包超时时间。 |
| NAS 标识 | 进行 Radius 认证或计费时，用于标识 NAS 设备。 |
| NAS IP 地址 | 进行 Radius 认证或计费时，NAS-IP-Address 字段的 IP 地址值（一般填写 AC 与 Radius 服务器交互的实际 IP 地址，也可以为空）。 |
| 认证方式 | 使用的认证方式，有 PAP、CHAP、MSCHAP 和 MSCHAPv2。 |

点击页面 ，查看更多页面设置参数信息。

## 12.4.2 认证服务器

可以通过本界面设置和查看认证服务器组。

进入页面：认证管理 >> 认证服务器 >> Radius 服务器，点击<新增>，设置认证服务器组。




| | |
|---|---|
| 组名称 | 自定义的认证服务器组名称，注意不能与已有服务器组名称重复。。 |

| | |
|---|---|
| 协议类型 | 该组中认证服务器的类型，目前只支持 Radius。 |
| 主服务器 | 选择特定类型的认证服务器为该组的主服务器，主服务器在认证过程中将优先被使用。 |
| 备用服务器 | 备用服务器在主服务器发生故障时启用，备份服务器为可选项。 |
| 恢复时间 | 当主服务器发生故障后，重新尝试使用主服务器的时间间隔。 |

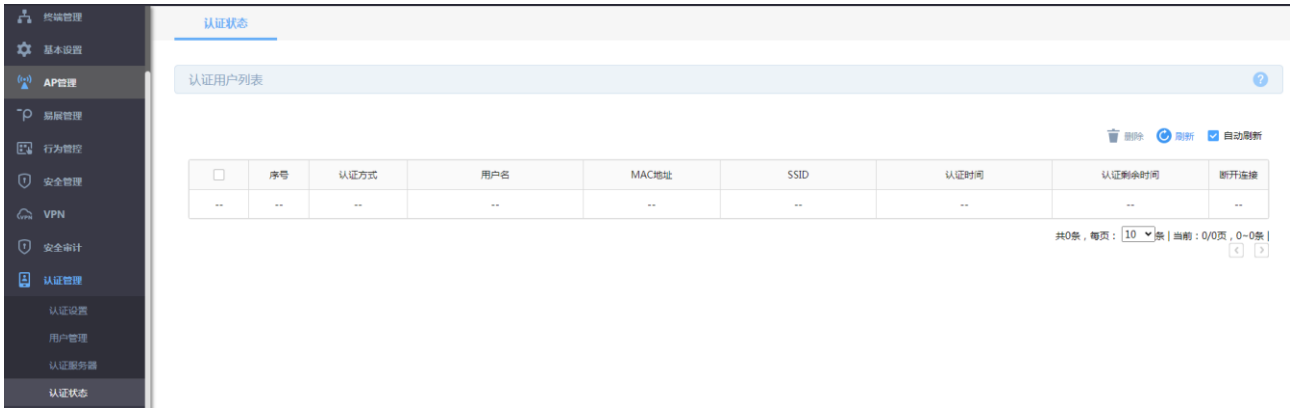
点击页面 ，查看更多页面设置参数信息。

## 12.5 认证状态

可以通过本页面来查看认证状态。

进入页面：认证管理 >> 认证状态，可查看当前已生效的认证事件。

点击<刷新>可获取最新的认证用户列表，勾选<自动刷新>，每隔一段时间系统将自动更新列表。



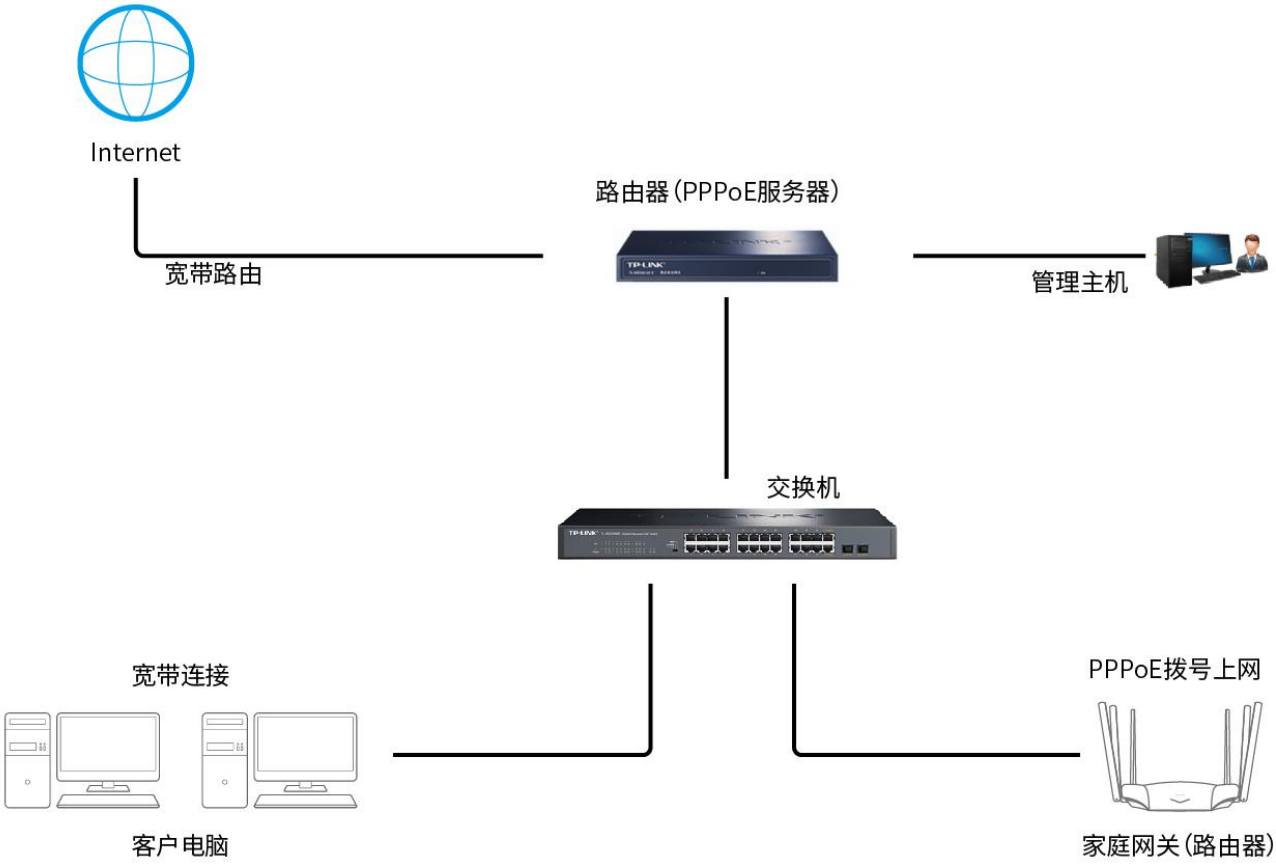

## 12.6 认证管理配置实例

# 第13章 高级功能

## 13.1 PPPoE 服务器

PPPoE 即 PPP over Ethernet，是指在以太网中传输 PPP 的技术。目前国内大多数宽带服务商使用 PPPoE 作为宽带接入技术，通过给用户分配宽带账号密码，结合认证、计费服务器实现宽带运营服务。终端用户通过在电脑或家庭网关（安全网关）上进行宽带拨号，实现连接到网络上网。

PPPoE 拨号可以避免局域网 ARP 欺骗、隔离用户间的访问，一定程度上保证网络安全稳定，如下图：




### 13.1.1 全局设置

进入页面：高级功能 >> PPPoE 服务器 >> 全局设置，设置全局参数，点击<保存>。


| | |
|---|---|
| PPPoE 服务器 | 选择<启用>，开启 PPPoE 服务器功能；选择<禁用>，关闭 PPPoE 服务器功能。 |
| 强制 PPPoE 拨号 | 选择<启用>，开启强制 PPPoE 拨号功能；选择<禁用>，关闭 PPPoE 强制拨号功能。功能开启后，生效接口下仅有拨号用户和例外 IP 的用户能使用网络。设置例外 IP，请到例外 IP 管理页面进行设置。 |

| | |
|---|---|
| 拨号用户互访 | 选择<允许>，开启拨号用户互访功能；选择<禁止>，禁止拨号用户互访功能。拨号用户互访功能允许拨号用户之间互相通信。 |
| 服务接口 | 该用户接入网络的接口。PPPoE 服务器的生效接口。 |
| 首选/备选 DNS 服务器地址 | 请正确填写，作为 DNS 服务器地址，缺省为空。。 |
| 系统最大会话数 | 设置会话数的最大值。 |
| 最大未应答 LCP 包数 | 作为最大未应答 LCP 包数，缺省为 10。当一条连接的未应答 LCP 包数超过这个数值时，PPPoE Server 会自动断开这条连接。 |
| 空闲断线时间 | 作为最大空闲断线时间，缺省为 30。请填写 0-10080 (分钟)，即最大为 7 天。0 代表不空闲断线。 |
| 认证方式 | 提供四种认证方式，请至少选择一种。 |

点击页面 ，查看更多页面设置参数信息。

## 13.1.2 IP 地址池

进入页面：高级功能 >> PPPoE 服务器 >> IP 地址池，点击<新增>，设置地址池名称和起始/结束 IP 地址，设置完成后点击<确定>。

## 13.1.3 账号管理

您可以查看账号设置信息，还可以通过表格按钮对账号设置信息条目进行操作。

进入页面：高级功能 >> PPPoE 服务器 >> 账号管理，点击<新增>，设置账号信息。


| | |
|---|---|
| 账号 | 账号规则设置的名称。 |
| 密码 | 账号的密码。 |

| | |
|---|---|
| 地址池 | PPPoE 服务器分配给客户端的 IP 地址从地址池获取。地址池设置请参考 13.1.2 IP 地址池。 |
| 最大会话数 | 用户允许该账户的最大设备数量。 |
| 账号到期时间 | 设置会话数的最大值。 |
| 带宽模式 | 设置账号带宽控制模式：共享表示账号的所有用户共用带宽；独立表示账号的所有用户独占带宽。 |
| 上/下行带宽 | 当前账号用户允许的上/下行带宽，以 Kbps 为单位，0 表示不限制。 |
| 账号高级设置 | 设置账号的高级属性，如 MAC 绑定、定时断线等。 |
| MAC 绑定方式 | 不绑定：不进行用户和 MAC 的绑定。<br>静态绑定：静态绑定一个 MAC 地址，该账户只能在该 MAC 的主机上登录。<br>动态绑定：当用户第一次登录的时候记录其 MAC，以后用户的登录必须使用该 MAC。 |
| MAC 地址 | 当选择 MAC 绑定方式为静态绑定时须填写的 MAC 地址。 |
| 定时断线时间 | 设置定时断线的时间，当定时断线时间为 0 时，表示不会定时断线。 |

点击页面 ，查看更多页面设置参数信息。

## 13.1.4 例外 IP 管理

进入页面：高级功能 >> PPPoE 服务器 >> 例外 IP 管理，点击<新增>，设置 IP 信息。


| | |
|---|---|
| 起始/结束 IP 地址 | IP 地址段的起始/结束 IP 地址，且起始 IP 地址必须小于或等于结束 IP 地址，而且不能与已有的 IP 地址范围重叠。 |
| 启用/禁用规则 | 您可以选择<启用>，使该规则生效。您也可以选择<禁用>，使该规则失效。 |

点击页面 ，查看更多页面设置参数信息。

## 13.1.5 账号信息列表

通过账号信息列表，可查看当前账号的有关信息。

进入页面：高级功能 >> PPPoE 服务器 >> 账号信息列表，点击<刷新>可获取最新信息。


## 13.1.6 PPPoE 服务器配置实例

需求介绍：某小区宽带服务商接入宽带为 500M 光纤，小区有 10 家宽带用户。该宽带服务商需要为用户分配宽带账号密码，让有账号的用户通过拨号上网，没有账号的用户无法上网，同时宽带服务商的管理主机（192.168.1.2-12）无需拨号即可上网。

设置方法：

1. 设置 IP 地址池。进入页面：高级功能 >> PPPoE 服务器 >> IP 地址池，点击<新增>，自定义设置地址池名称、地址池的起始 IP 地址和结束 IP 地址，点击 <确定>。


2. 用户在该时间内输入验证码进行验证有效，否则需重新获取验证码。设置用户账号。进入页面“高级功能 >> PPPoE 服务器 >> 账号管理”，点击<新增>，添加用于拨号上网的账号密码。设置最大会话数（表示设定数量的用户可同时使用该账号拨号）和账号到期时间，设置账号带宽控制模式：其中共享表示账号的所有用户共用的带宽；独立表示账号的所有用户独占设置的带宽，选择启用账号后点击<确定>。


“启用”账号高级设置，支持设置 MAC 绑定和定时断线时间（当定时断线时间为 0 时表示不会定时断线）。


3. 将宽带服务商的管理主机（192.168.1.2-12）设置为例外 IP。进入页面“高级功能 >> PPPoE 服务器 >> 例外 IP 管理”，点击<新增>，根据需求，设置规则如下，点击<确定>。


4. 设置全局参数。进入页面“高级功能 >> PPPoE 服务器 >> 全局设置”，启用 PPPoE 服务器和强制 PPPoE 拨号，在首选 DNS 及备用 DNS 服务地址的位置输入当地宽带线路的 DNS，其它参数可保持默认，点击<保存>。


至此，PPPoE 服务器设置完成，局域网中的宽带用户均需要使用分配的账号密码拨号才可以上网，管理员主机无需拨号即可上网，没有账号或账号过期的用户，不可以上网。

在“高级功能 >> PPPoE 服务器 >> 账号信息列表”页面可以查看到 PPPoE 拨号用户的连接信息，也可

对已连接用户进行断开连接操作。

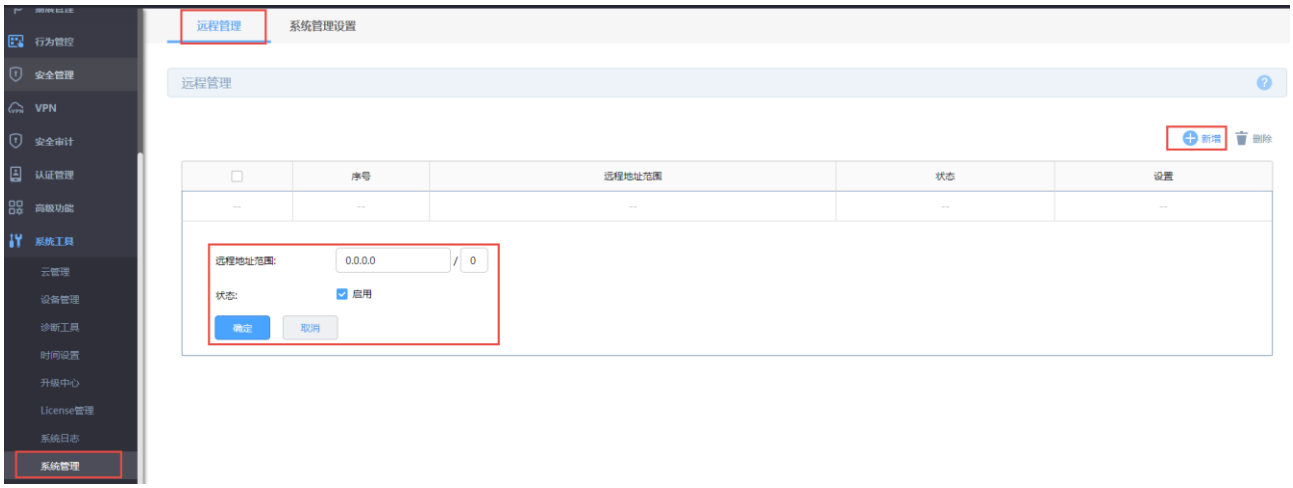
## 13.2 Web 远程管理

远程管理功能可以在网络任何地方远程实时、安全的监控和配置网络。

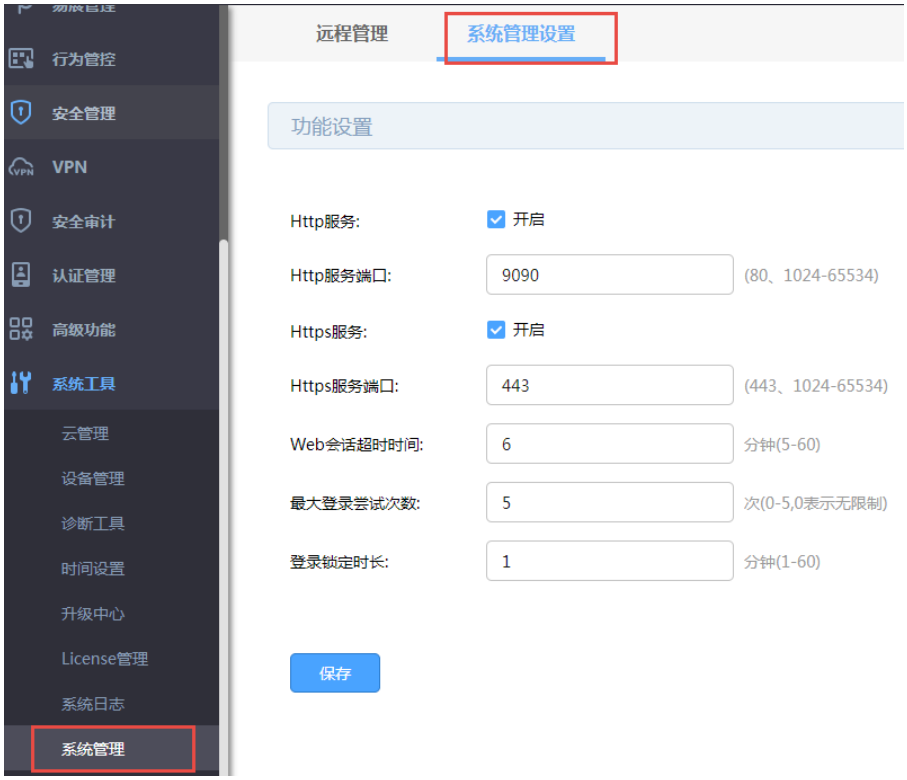
➢ **远程管理配置步骤如下：**

5. 登录安全网关管理页面 tplogin.cn。进入页面“系统工具 >> 系统管理 >> 远程管理”。

点击<新增>，添加路由条目：远程地址范围为 0.0.0.0，状态勾选为启用。(0.0.0.0/0 代表所有外网电脑均可以访问安全网关)。




6. 进入页面“系统工具 >> 系统管理 >> 系统管理设置”，配置 http 服务端口，点击<保存>。

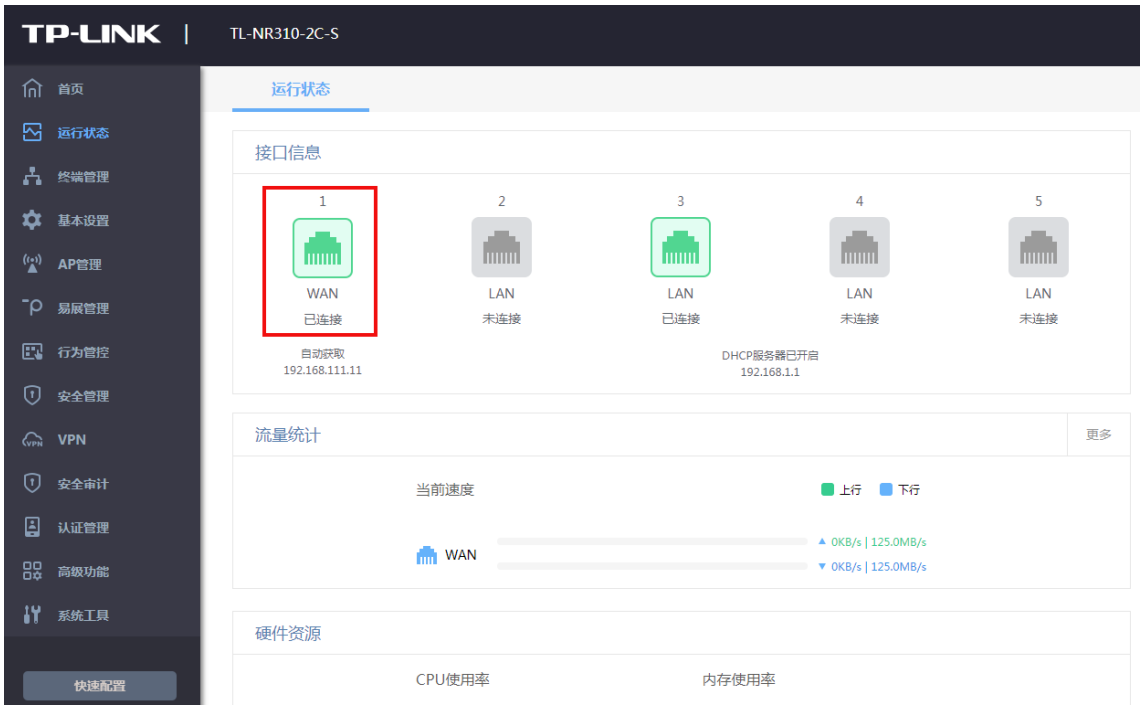



注意：80、8080 等常用端口容易被宽带服务商屏蔽，因此建议将 Web 管理端口设置为不常用端口，如 9000 以上的端口。

➢ **远程访问步骤：**

7. 进入页面“运行状态”，查看 WAN 口 IP 地址。

通过 WAN 口 IP 在外网远程管理网关需要 WAN 口 IP 为公网 IP。



8. 外网电脑输入 http://WAN 口 IP：端口号 进行进行远程访问。如果安全网关上登录了动态域名，还可以使用 http://域名:端口 来访问。

## 13.3 动态 DNS

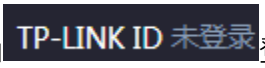
广域网中，许多 ISP 使用 DHCP 分配公共 IP 地址，因此用户端获得的公网 IP 是不固定的。当其它用户需要访问此类 IP 动态变化的用户端时，很难实时获取它的最新 IP 地址。

DDNS（Dynamic DNS，动态域名解析服务）服务器则为此类用户端提供了一个固定的域名，并将其与用户端最新的 IP 地址进行关联。当服务运行时，DDNS 用户端把最新的 IP 地址通知 DDNS 服务器，服务器会更新 DNS 数据库中域名与 IP 的映射关系。而对于访问它的用户端，将会得到正确的 IP 地址并成功访问服务端。DDNS 常用于 Web 服务器搭建个人网站、FTP 服务器

提供文件共享等，访问的用户可以便捷地获取服务。

安全网关作为动态 DNS 客户端，本身并不提供动态 DNS 服务。因此，在使用此功能之前，必须进入动态 DNS 服务提供商的官方主页注册，以获得用户名、密码和域名等信息。TL-ER6520G 安全网关提供花生壳动态 DNS 客户端。

### 13.3.1 TP-LINK 动态域名

如需使用 TP-LINK 动态域名，请先登录 TP-LINK ID，点击管理页面右上角 

登录。

进入页面：高级功能 >> 动态 DNS >> TP-LINK 动态域名。


## 13.3.2 花生壳动态域名

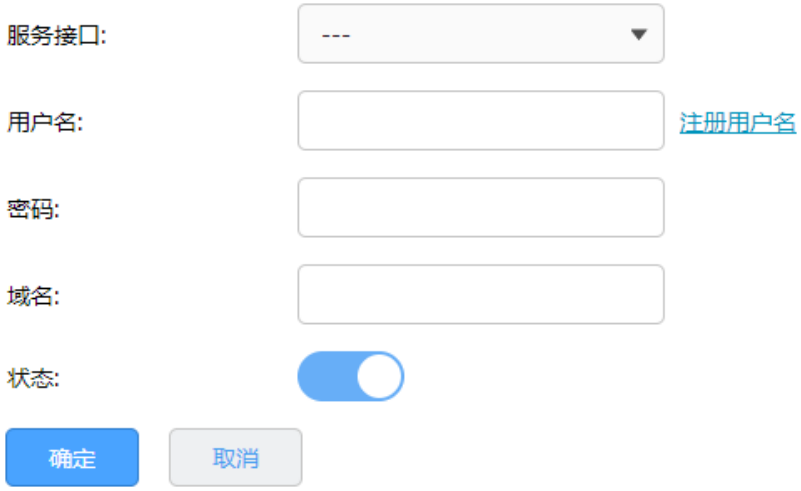
进入页面：高级功能 >> 动态 DNS >> 花生壳动态域名，点击<新增>，设置服务接口、用户名和密码，点击<确定>。


## 13.3.3 科迈动态域名

进入页面：高级功能 >> 动态 DNS >> 科迈动态域名，点击<新增>，设置服务接口、用户名和密码，点击<确定>。


## 13.3.4 3322 动态域名

进入页面：高级功能 >> 动态 DNS >> 3322 动态域名，点击<新增>，设置服务接口、用户名、密码和域名，点击<确定>。




| | |
|---|---|
| 服务接口 | 3322 动态域名服务生效的接口。 |
| 域名 | 用户名绑定的域名信息。 |

点击页面，查看更多页面设置参数信息。

## 13.3.5 DDNS 配置实例

需求介绍：某企业使用安全融合网关，内网有台服务器通过虚拟服务器映射端口到公网，需要在外网可以访问到该服务器。安全网关是带宽拨号上网，获取的是动态 IP 地址，使用 IP+端口的方式需要经常变化 IP 地址，使用十分麻烦。

可以通过 DDNS，将 WAN 口 IP 绑定到某个域名上。通过域名+端口的形式访问内网服务器，域名会实时更新绑定当前 WAN 口 IP。

设置方法：

- **TP-LINK 动态域名**

进入页面“高级功能 >> 动态 DNS>>TP-LINK 动态域名”，使用 TP-LINK 动态域名需要先登录 TP-LINK ID，如果没有可以在安全网关中免费注册一个。登录账号之后，根据需要创建域名。


创建域名之后，绑定到对应接口即可。

- **花生壳/科迈动态域名**

选择使用花生壳动态域名或科迈动态域名只需要选择对应的服务接口并登录相应的账号密码即可。


- **3322 动态域名**

选择使用 3322 动态域名配置过程与花生壳基本一致，只需要填写账号密码与域名信息然后绑定对应接口即可。

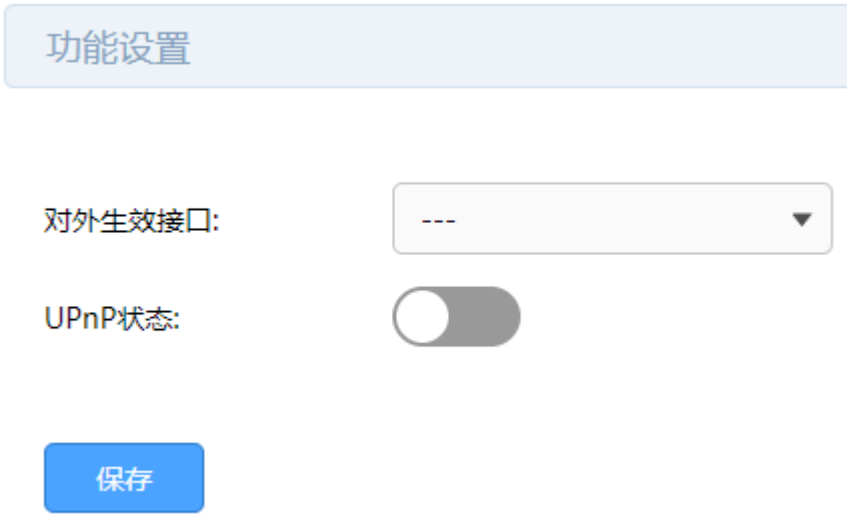
## 13.4 UPnP

UPnP（Universal Plug and Play， 通用即插即用）协议，遵循此协议的不同厂商的各种设备可以自动发现对方并进行连接。

如果应用程序支持 UPnP 协议，而局域网中的主机安装了 UPnP 组件，安全网关开启了 UPnP 服务后，局域网中的主机就可以根据软件的需要自动地在安全网关上打开相应的端口，使得外部主机上的应用程序在需要时能够通过打开的端口访问内部主机上的资源，这样原本受限于 NAT 的功能便可以正常使用。例如，Windows XP 和 Windows ME 系统上安装的 MSN Messenger，在使用音频和视频通话时就可以利用 UPnP 协议，而无需设置 NAT 相关转发规则，对于此类传输层协议端口不固定的应用会更加方便。

进入页面：高级功能 >> UPnP，可进行功能设置和查看服务列表。

- **功能设置**




| | |
|---|---|
| 对外生效接口 | 可以指定一组接口集，该集合包含的接口将被配置以端口映射的功能。 |
| UPnP 状态 | 滑块为灰色表示禁用，滑块为蓝色表示启用。 |

点击页面，查看更多页面设置参数信息。

- **服务列表**

在服务列表中，您会看到通过 UPnP 协议向安全网关请求的端口映射条目。您可以通过表格按钮对这些条

目进行操作。

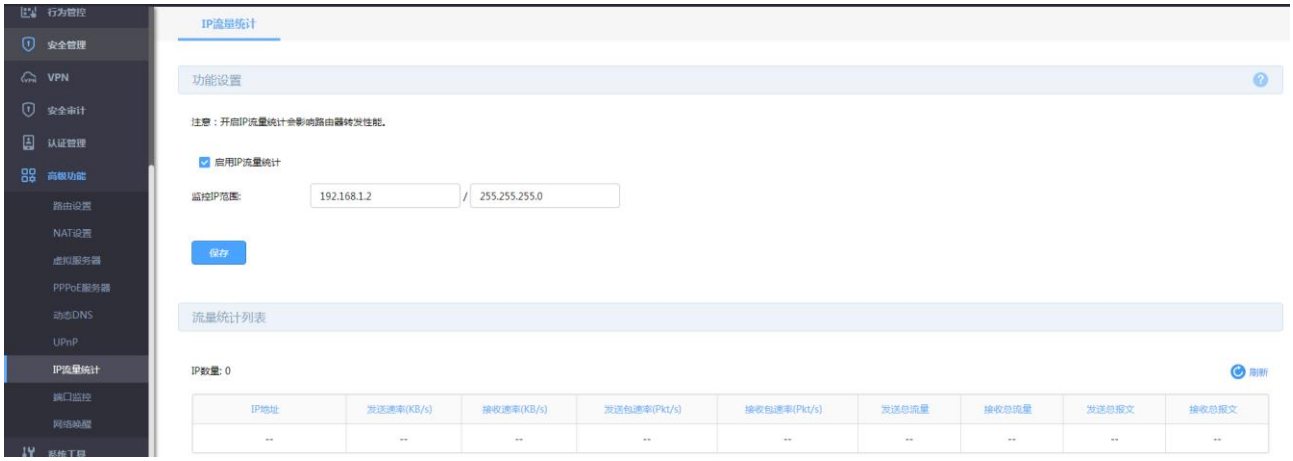

说明：

- 应用时不仅要在安全网关上启用 UPnP 服务，还需要确认主机操作系统和应用程序也支持此服务，即 Windows XP 系统需安装 UPnP 组件；应用程序本身需支持 UPnP，如 MSN 最新版、电驴、迅雷等。
- 一些木马、病毒可能会利用 UPnP 服务打开特定的端口，使局域网主机成为黑客的攻击目标，因此需谨慎应用 UPnP 服务。

## 13.5 IP 流量统计

IP 流量统计功能将显示安全网关所有正在工作的接口的数据接收/发送速率等流量信息。

进入页面：高级功能 >> IP 流量统计，勾选<启用 IP 流量统计>，输入监控 IP 范围，点击<保存>，即可监控 IP 的发送/接收速率、总流量和总报文。




## 13.6 端口监控

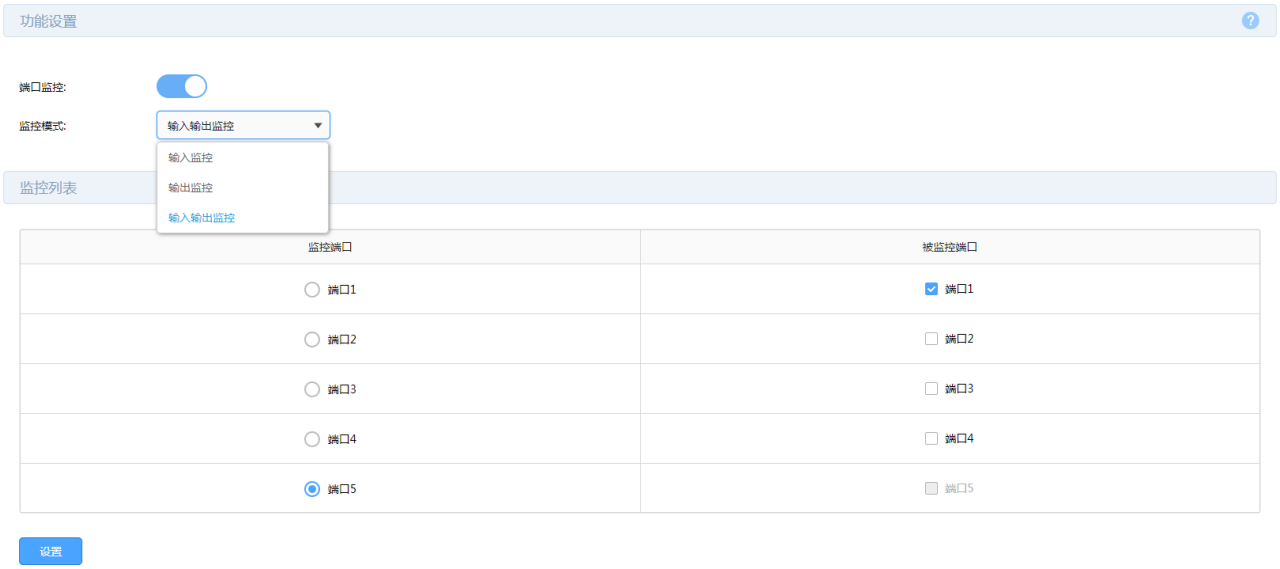
### 13.6.1 端口监控介绍

端口监控是一种数据包获取技术，通过配置安全网关，可以实现将一个/几个端口（被监控端口）的数据包

复制到一个特定的端口（监控端口），在监控端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。

配置方法：

进入页面：高级功能 >> 端口监控，开启端口监控功能。




- **功能设置**

监控模式　　端口监控有下面三种监控模式：

输出输入监控：流入流出被监控端口的数据帧将被复制到监控端口。

输入监控：流入被监控端口的数据帧将被复制到监控端口。

输出监控：流出被监控端口的数据帧将被复制到监控端口。

- **监控列表**

选择监控端口和被监控端口，被监控端口的数据帧将被复制到监控端口。

点击页面  ，查看更多页面设置参数信息。

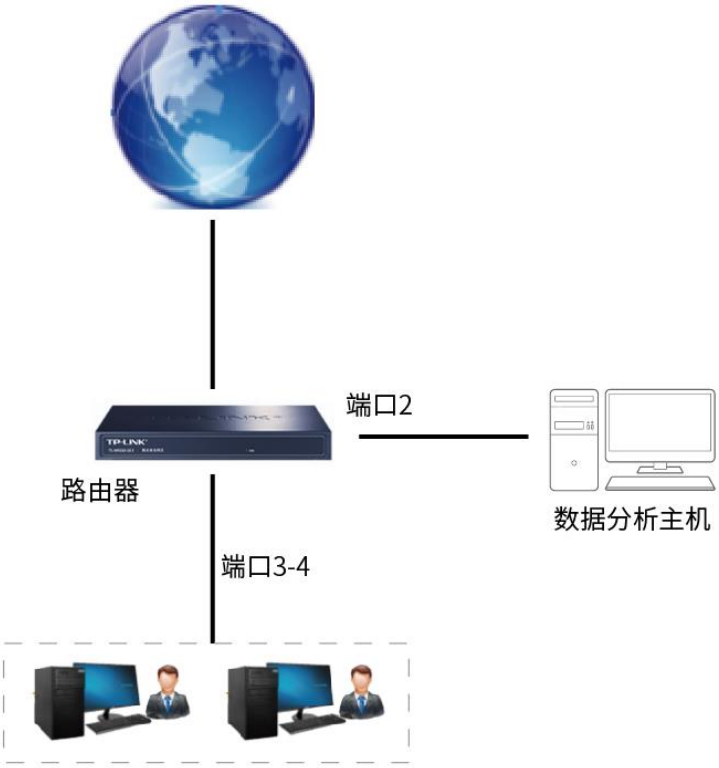
注意：

- 一个端口不能同时作为监控端口和被监控端口。
- 只能设置一个监控端口。

## 13.6.2　端口监控配置实例

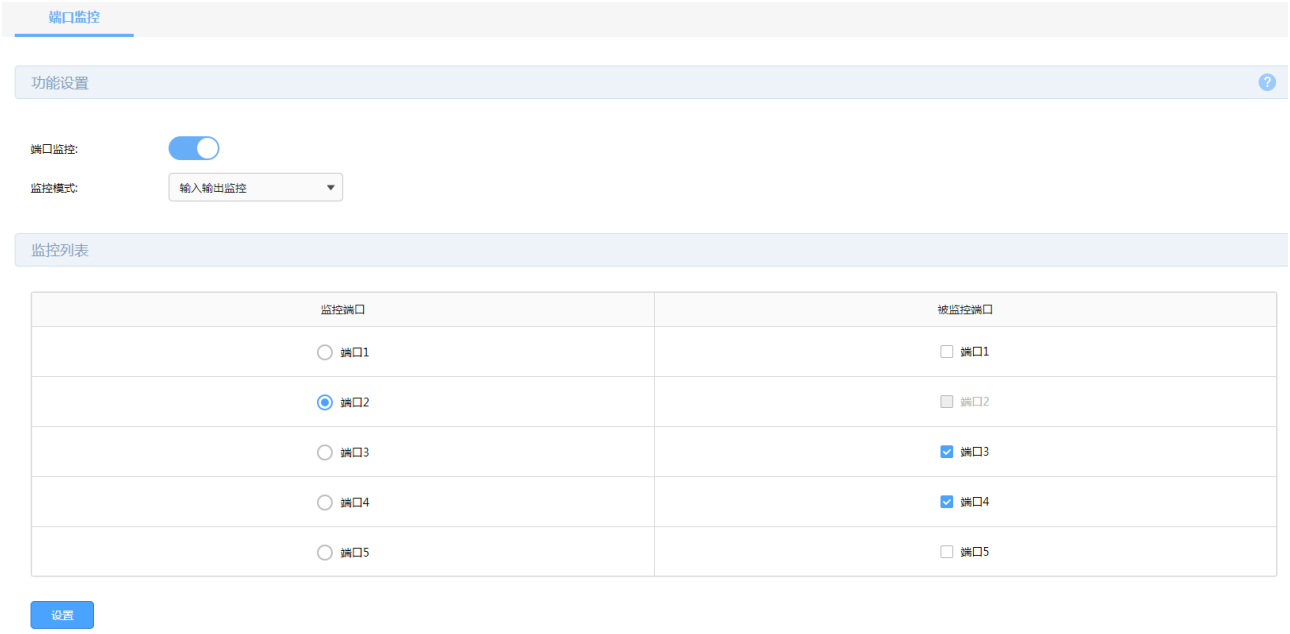
组网介绍：

网络中有一台安装了数据包分析软件的主机连接在安全网关的 3 号端口，需要对网络中电脑的上网行为进行监控。示意网络拓扑如下：




配置步骤：

进入页面高级功能 >> 端口监控，开启端口监控功能，选择“输入输出监控”模式，选择相应监控端口 2，被监控端口 3 和 4，点击<设置>。




注意：

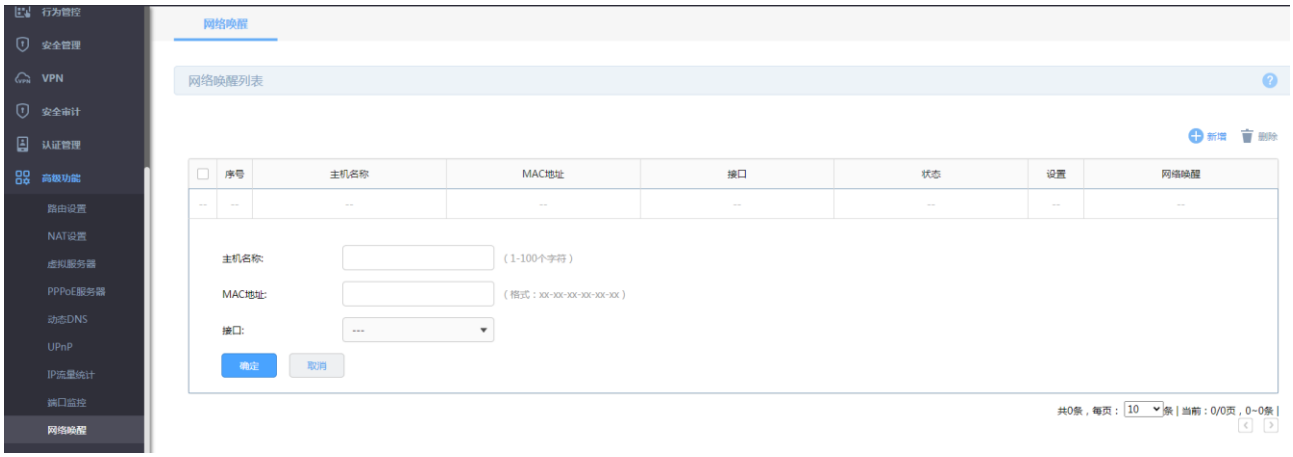
- 一个端口不能同时作为监控端口和被监控端口。
- 只能设置一个监控端口。

# 13.7 网络唤醒

## 13.7.1 网络唤醒介绍

许多用户朋友为了方便网络管理，需要远程唤醒内网已经关机的 PC/NAS/Server 等设备，对网络唤醒功能有着强烈的需求。但之前为了完成网络唤醒，需要进行复杂的步骤：在安全网关 WAN 口地址是公网地址的前提下，还需要设置 IP 静态地址分配、arp 绑定、虚拟服务器、动态 DDNS 且还需要下载专门的远程唤醒工具才能实现，远程唤醒十分不方便。现在此功能添加到企业安全网关中，方便大家使用。

进入页面：高级功能 >> 网络唤醒，点击<新增>，设置唤醒终端的主机名称、MAC 地址和所在接口，点击<确定>。



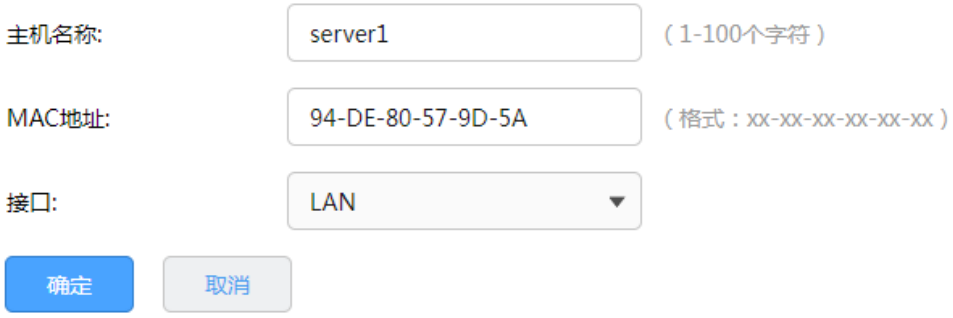

添加完成后，点击唤醒按钮即可唤醒终端。


## 13.7.2 网络唤醒功能配置实例

需求介绍：某企业内网有台 Server 设备平时是关闭的，只有需要时才会打开，且不想专门跑到设备旁边开机，需要远程唤醒此设备，已知该设备支持并开启了远程唤醒，设备的 MAC 地址是 94-DE-80-57-9D-5A。

配置方法：

1. 在“高级功能 >> 网络唤醒”，点击<新增>，自定义主机名称，输入需要远程唤醒的设备的 MAC 地址，选择此主机所在内网网段的接口，此处被唤醒设备在默认的 LAN 网段，因此是选择 LAN 口，点击<确定>。



说明：

- 远程唤醒的是个同一局域网内才可生效的功能，只有 LAN 网段的设备才可以支持唤醒。

2. 远程登录到安全网关的 Web 界面，进行远程唤醒，此时安全网关需要设置开启远程管理，同时需要 WAN 口为公网 IP。在“高级功能 >> 网络唤醒”的列表中，找到对应的设备，点击网络唤醒按钮，即可一键唤醒内网设备。


还可以通过 TP-LINK 商云管理平台和 TP-LINK 商云 APP 进行唤醒。

➢ **TP-LINK 商云管理平台唤醒**

将安全网关添加至“商云”进行管理，电脑登陆 TP-LINK 商云管理平台，点击<设备列表>，找到对应设备的<远程管理> 按钮，点击后即可实现远程管理，在“高级功能 >> 网络唤醒”的列表中，点击网络唤醒即可成功唤醒内网设备。


➢ **TP-LINK 商云 APP 进行唤醒**

手机打开“TP-LINK 商云”APP，点击页面下方<项目>，选择对应安全网关所在项目，点击页面下方的”设备”，找到安全网关后点击如下图所示对应位置后，点击<远程管理>，或者点击设备列表中的相应安全网关，页面下方也有<远程管理>按钮，点击即可进入安全网关管理页面，在“高级功能 >> 网络唤醒”的列表中，点击网络唤醒即可成功唤醒内网设备。

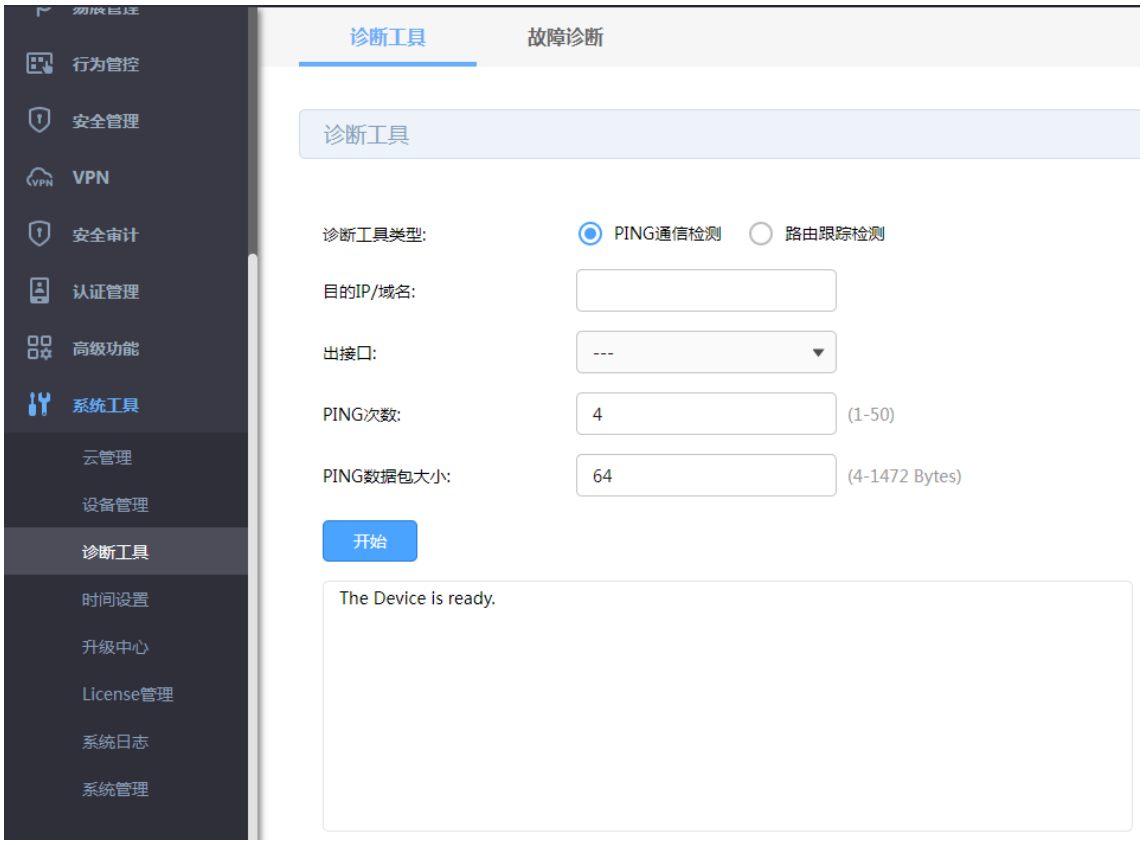
# 13.8 故障诊断

## 13.8.1 诊断工具

安全融合网关的诊断工具包包括两种类型：PING 通信测试和路由跟踪检测，可分别用于测试外网的连通性和检测数据包访问目的 IP/域名所经过的路由节点及延迟。

进入页面：系统工具 >> 诊断工具 >> 诊断工具，选择诊断工具类型，设置参数，点击<开始>。

- PING 通信检测




| | |
|---|---|
| 诊断工具类型 | 选择“PING 通信检测”，用于检测到达网络中的某节点是否连通。 |
| 目的 IP/域名 | 需要进行 Ping 通信检测的主机地址，支持 IP 地址和域名。 |
| 出接口 | 需要进行 Ping 通信检测的接口。。 |
| PING 次数 | 设置 Ping 通信检测时发送 Ping 包的数量。 |
| PING 数据包大小 | 设置 Ping 通信检测时发送的 Ping 包的大小。 |

点击页面，查看更多页面设置参数信息。

当出接口能够 PING 通目的 IP 和域名，则会显示 PING 回复时间；当无法 PING 通目的 IP 和域名，则不会显示 PING 回复时间，而是显示“Request timed out”，请求超时；或者无法解析域名时，显示“There is no response from DNS”，如下图所示。



- **路由跟踪检测**


| | |
|---|---|
| 诊断工具类型 | 选择“路由跟踪检测”，用于检测到达联络中的某节点经过节点的个数以及节点地址。 |
| 目的 IP/域名 | 需要进行路由跟踪检测的主机地址，支持 IP 地址和域名。 |
| 出接口 | 需要进行路由跟踪检测的接口。。 |

| | |
|---|---|
| 路由跟踪最大 TTL | 设置路由跟踪检测发送数据包在网络中的最大转发跳数。。 |

点击页面  ，查看更多页面设置参数信息。

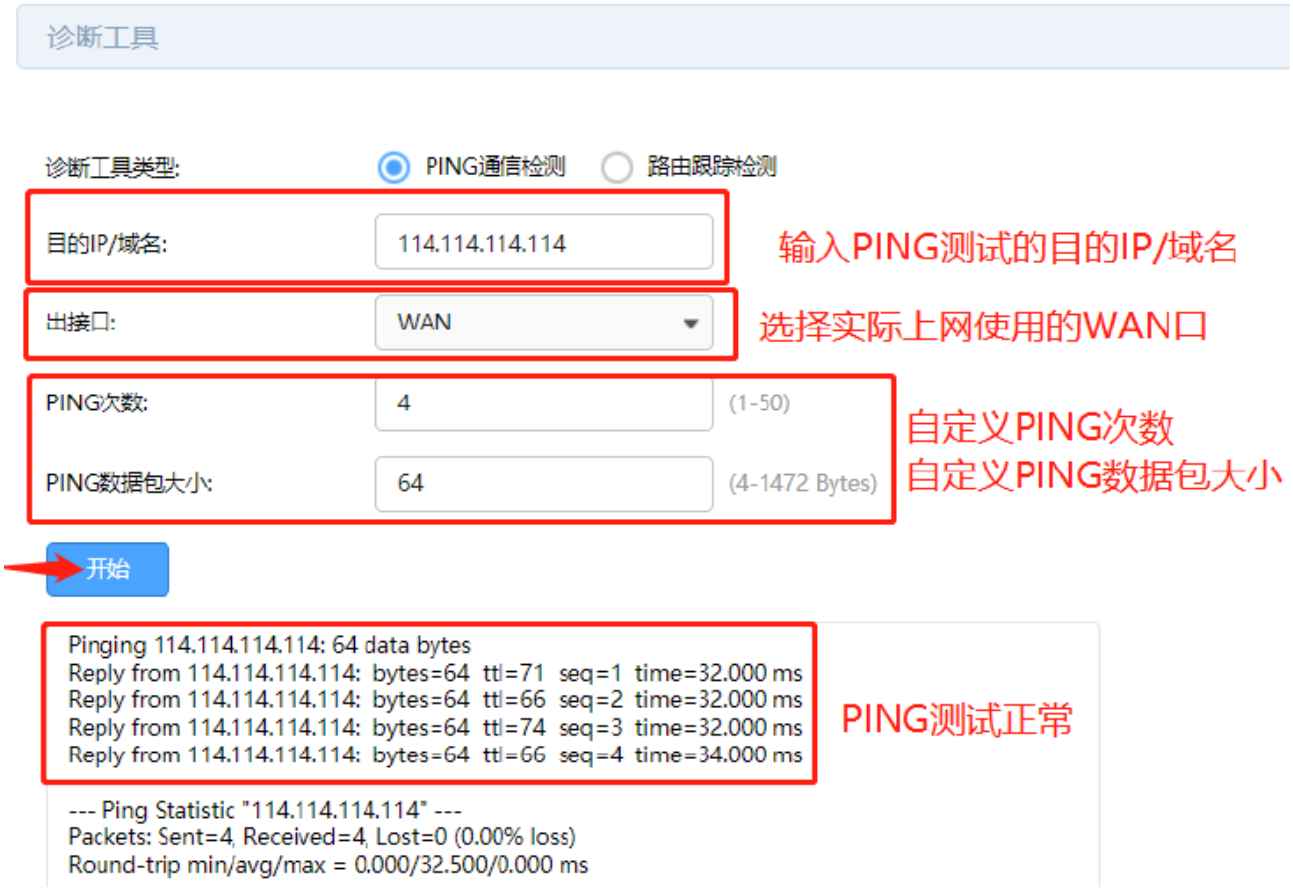
## 13.8.2 诊断工具配置实例

需求介绍：某用户内网无法上外网，希望可以通过安全网关诊断下问题原因所在。此时可以通过 PING 通信检测来判断 WAN 口与外网之间是否连通（出接口选择对应 WAN 口），或者可以检测安全网关与内网主机之间是否连通（出接口选择对应 LAN 口）；也可以通过路由跟踪检测来检测数据包访问目的 IP/域名所经过的路由节点及延迟。

设置方法：

- **PING 通信检测**

诊断工具类型选 择“PING 通信检测”，目的 IP/域名选择常见 DNS 服务器如 114.114.114.114 或者门户网站如 www.qq.com，出接口则选择实际上网使用的 WAN 口，还可以自定义“PING 次数”（1-50）和“PING 包大小”（4-1472 Bytes），点击<开始>，测试结果如下图所示即为正常，也可以根据测试结果中的 time 判断延迟是否正常。




而当 WAN 口无法 PING 通目的 IP 和域名，则不会显示 PING 回复时间，而是显示“Request timed out”，请求超时；或者无法解析域名时，显示“There is no response from DNS”，如下图所示。


- **路由跟踪检测**

诊断工具类型选择“路由跟踪检测”，目的 IP/域名选择常见 DNS 服务器如 114.114.114.114 或者门户网站如 www.qq.com，出接口则选择实际使用的 WAN 口，还可以自定义“路由跟踪最大 TTL”（Time To Live，生存时间值），点击<开始>。测试结果如下图所示即为正常，可以看到访问目的 IP/域名所经过的路由节点及延迟。


## 13.8.3 故障诊断

当安全网关发生故障时，可先自行使用“诊断工具”功能检测，参考**错误!未找到引用源。错误!未找到引用源。**。如未能发现问题，建议联系技术支持人员，在技术支持人员指导下进行故障诊断。

进入页面：统工具 >> 设备管理 >> 自动清理。

开启故障诊断模式，一般情况下请勿开启，需要故障诊断时请在技术支持人员的帮助下开启本功能。

点击<导出诊断信息>，可以导出诊断信息并将其发给技术支持人员进行分析并协助解决问题。

点击<一键清理>，以协助解决问题。该功能需在技术支持人员的协助下使用。

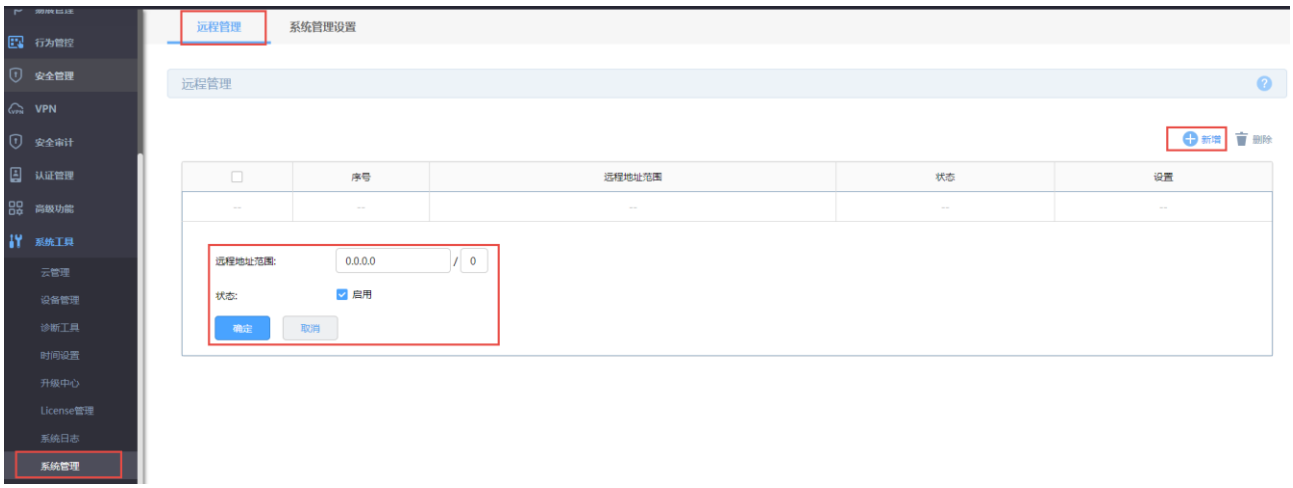

## 13.9 Web 远程管理

远程管理功能可以在网络任何地方远程实时、安全的监控和配置网络。

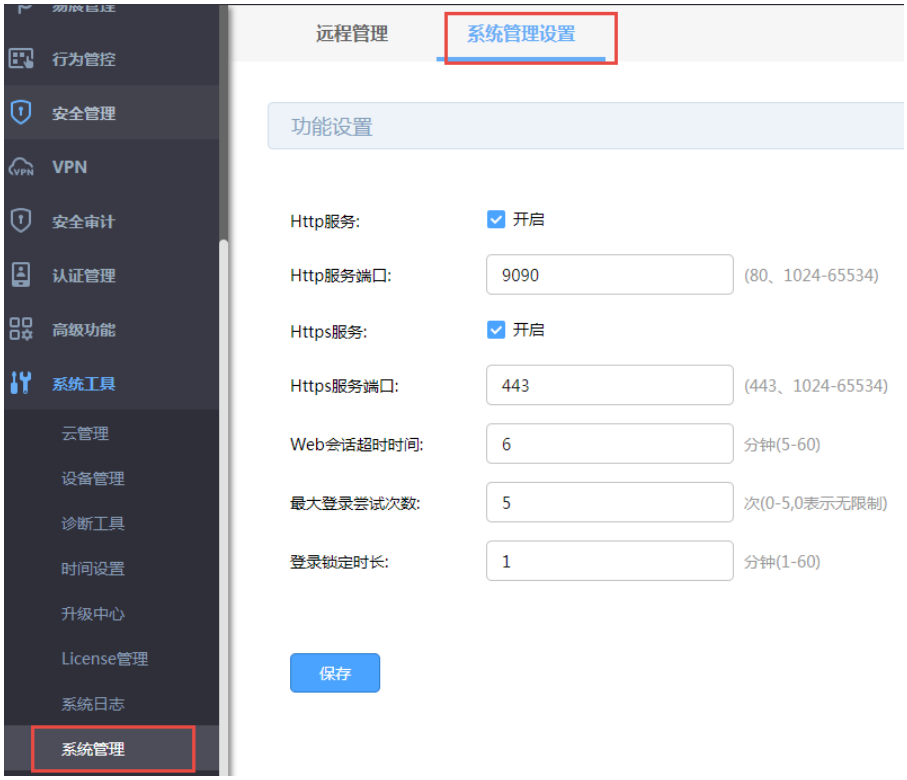
- **远程管理配置步骤如下：**

3. 登录安全网关管理页面 tplogin.cn。进入页面“系统工具 >> 系统管理 >> 远程管理”。

点击<新增>，添加路由条目：远程地址范围为 0.0.0.0，状态勾选为启用。(0.0.0.0/0 代表所有外网电脑均可以访问安全网关)。




4. 进入页面“系统工具 >> 系统管理 >> 系统管理设置”，配置 http 服务端口，点击<保存>。

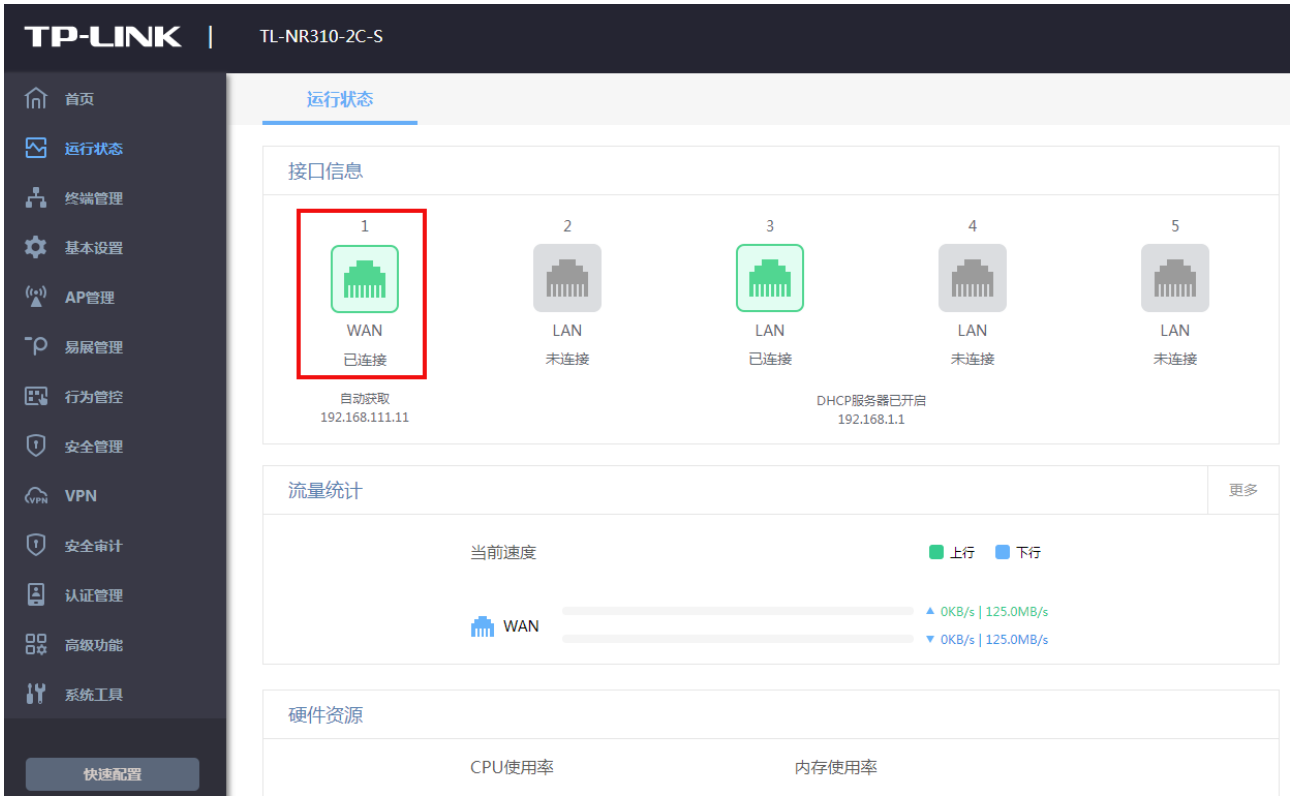



注意：80、8080 等常用端口容易被宽带服务商屏蔽，因此建议将 Web 管理端口设置为不常用端口，如 9000 以上的端口。

- **远程访问步骤：**

5. 进入页面“运行状态”，查看 WAN 口 IP 地址。

   通过 WAN 口 IP 在外网远程管理网关需要 WAN 口 IP 为公网 IP。




6. 外网电脑输入 http://WAN 口 IP：端口号 进行进行远程访问。如果安全网关上登录了动态域名，还可以使用 http://域名:端口 来访问。

# 第14章 系统配置

## 14.1 云管理

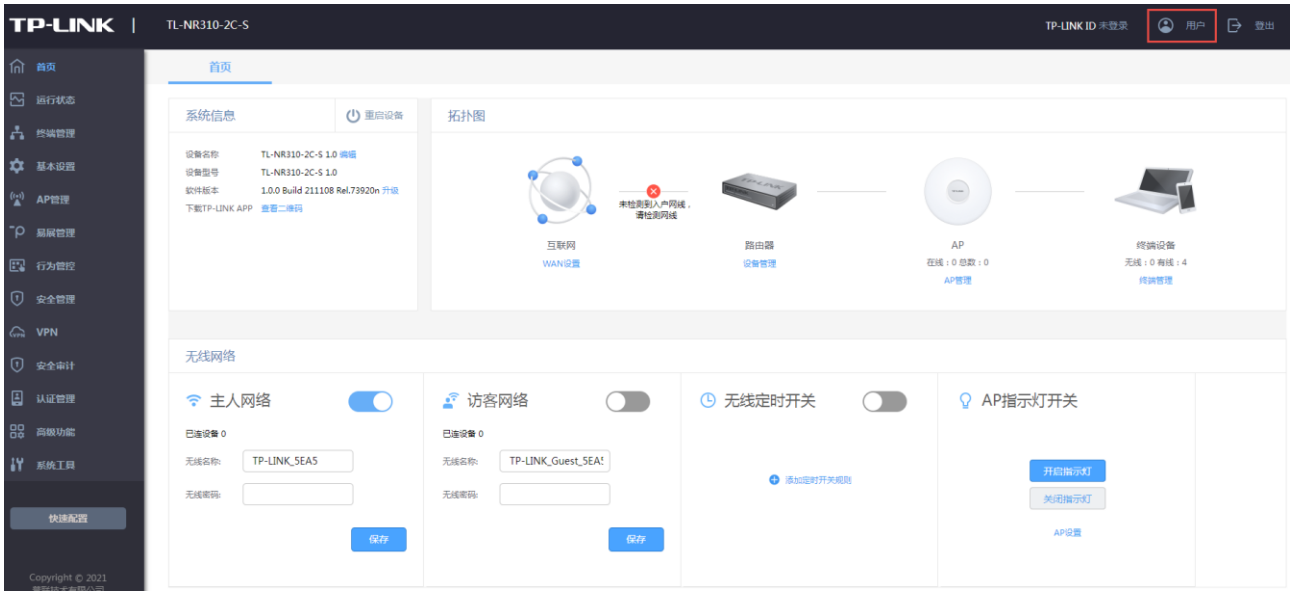
安全网关默认开启云管理，可通过按键开关或进入页面“系统管理 >> 云管理”来管理安全网关。

相关配置请参考 2.2 云管理。

## 14.2 设置用户名和密码

1. 点击安全网关管理页面右上角 

，设置用户名和密码。




2. 设置用户名和密码，点击<保存>。


## 14.3 恢复出厂配置

进入页面：系统工具 >> 设备管理 >> 恢复出厂配置，点击<恢复出厂配置>。恢复出厂设置后，当前的配置信息将会丢失，如果您想保留当前配置请注意备份。


## 14.4 备份与导入配置

进入页面：系统工具 >> 设备管理 >> 备份与导入配置。可查看当前软件版本信息。点击<备份>，将系统文件保存到本地。点击<浏览>选择可导入的配置文件，再点击<导入>，恢复已备份的配置。


## 14.5 重启安全网关

进入页面：系统工具 >> 设备管理 >> 设备管理，在重启安全网关部分，点击<重启安全网关>，重启过程不要断电。

## 14.6 自动清理

您可以通过本页面来设置自动恢复/自动清理功能。

进入页面：系统工具 >> 设备管理 >> 自动清理。


- **自动恢复**

开启自动恢复功能后，当本设备出现异常时将会尝试自动恢复。

- **自动清理**

开启自动清理功能，设置每周固定时间，安全网关将在指定时间进行自动清理，以获得更好的体验。设置完成后点击<保存>。

说明：

- 自动清理功能仅在获取到网络时间或者手动设置时间后生效，时间设置请参考 14.7 时间设置。

## 14.7 时间设置

设置系统时间，进入页面：系统工具 >> 时间设置，可设置通过网络获取系统时间或者手动设置系统时间。

通过网络获取系统时间，安全网关将通过网络获取 GMT 时间，选择时区和 NTP 服务器，点击<设置>。


手动设置系统时间，可以通过手动输入的方式来设置安全网关日期和时间。可点击<获取管理主机时间>来直接获取管理主机时间。


# 14.8 升级系统

## 14.8.1 在线和本地升级

进入页面：系统工具 >> 设备管理 >> 设备管理。点击<检查新版本>，安全网关自动检测当前软件是否为

最新并更新软件。点击<浏览>选择本地升级文件，点击<升级>，更新软件。


说明：

- 使用在线升级的时候请确保设备正常联网。
- 请确保在安全网关升级过程中，不要将安全网关断电，不要对页面进行刷新。升级完毕，安全网关将自动重启。
- 您可以到网址 www.tp-link.com.cn 下载最新的升级软件。

注意：

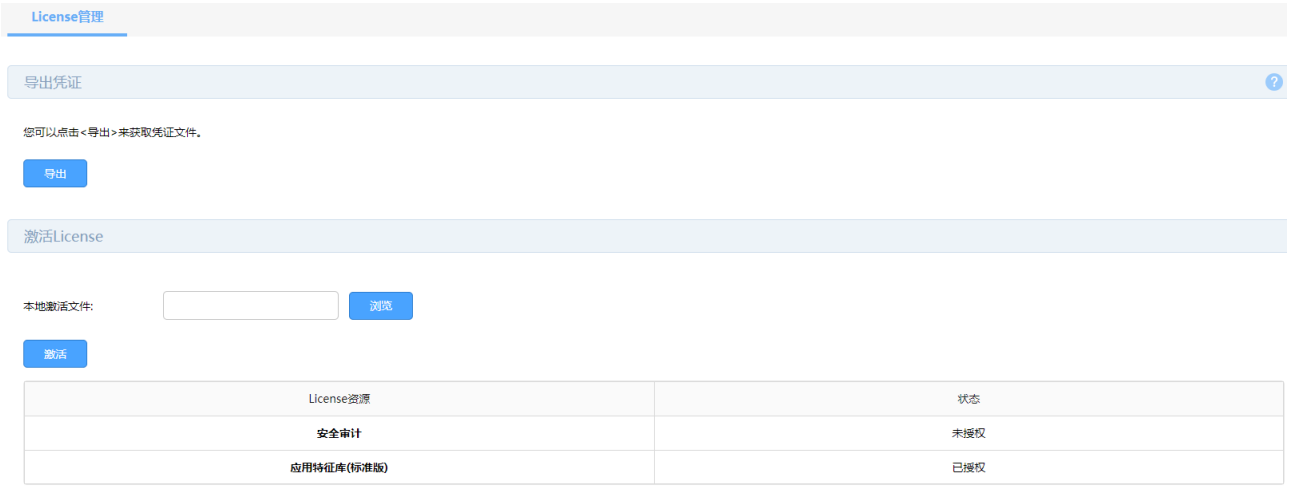
- 在安全网关升级过程中，请不要将安全网关断电。
- 进行软件升级后，当前的配置信息可能会丢失。请您在升级前备份产品配置信息。

## 14.8.2 应用特征库升级

进入页面：系统工具 >> 升级中心，可对应用特征库进行升级操作。

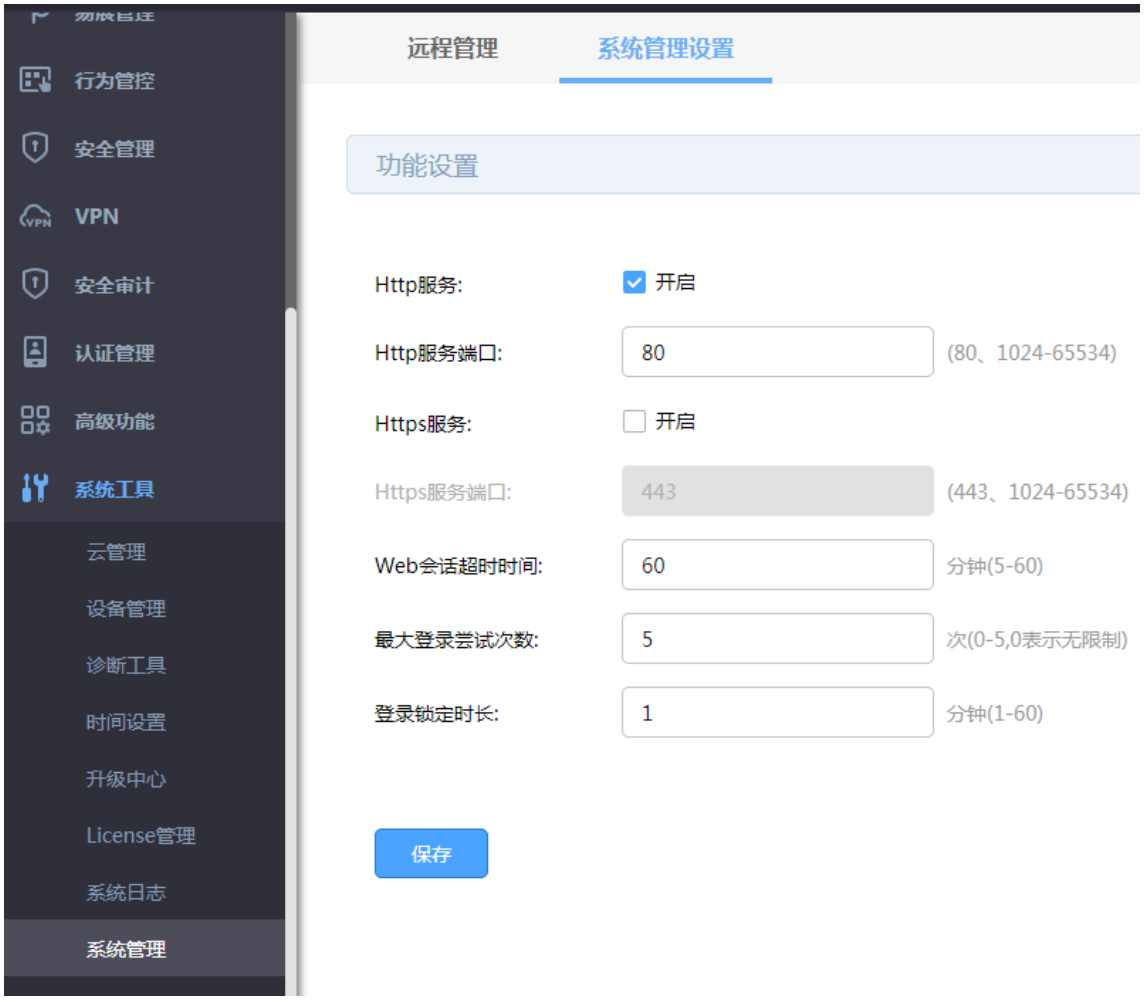

| | |
|---|---|
| 定时升级 | 是否定时升级该特征库，如果为'是'，则会按照规定的时间，定时升级特征库。 |
| 定时升级特征库时间 | 定时升级特征库的时间，请尽量选在使用较少的时间段升级，升级过程中会消耗一定程度设备性能。 |
| 在线升级 | 通过连接云端服务器下载并安装特征库。 |
| 本地升级 | 从本地电脑中导入和安装特征库。 |

点击页面 ，查看更多页面设置参数信息。




# 14.9 系统管理设置

进入页面：系统工具 >> 系统管理 >> 系统管理设置，可以通过本页面进行服务端口和会话超时时间的管理。




| | |
|---|---|
| Http 服务 | Http 服务默认打开，当取消勾选该项时，将无法通过 Http 的方式对 Web 进行管理。 |
| Http 服务端口 | 用于 Web 管理界面的 Http 服务端口，默认为 80 端口。不能与其他的服务端口重复。 |
| Https 服务 | 勾选可开启 Https 服务。 |
| Https 服务端口 | 用于 Web 管理界面的 Https 服务端口，默认为 443 端口。不能与其他的服务端口重复。 |
| Web 会话超时时间 | 如果在会话超时时间内都没有进行操作，系统将自动退出登录，以保证设备和网络的安全。 |
| 最大登录尝试次数 | 当连续尝试登陆失败达到该次数时，将会在一段时间内锁定设备不允许继续登录。 |

| | |
|---|---|
| 登录锁定时长 | 当连续登陆失败次数达到最大登录尝试次数后，将会在锁定时长期间无法进行登录。 |

点击页面  ，查看更多页面设置参数信息。