TP-LINK®

防火墙

用户手册

1910041136 REV1.0.0

声明

Copyright © 2023 **普联技术有限公司**

版权所有，保留所有权利

未经普联技术有限公司明确书面许可，任何单位或个人不得擅自仿制、复制、誊抄或转译本手册部分或全部内容，且不得以营利为目的进行任何方式（电子、影印、录制等）的传播。

TP-LINK®为普联技术有限公司注册商标。本手册提及的所有商标，由各自所有人拥有。本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，所作陈述均不构成任何形式的担保。

目录

第1章　用户手册简介

本手册旨在帮助用户正确使用防火墙，以 TL-NFW8500 为例进行介绍。防火墙系列机型在硬件配置上存在差异，具体信息请查阅防火墙对应的安装手册；防火墙系列机型软件配置步骤基本相同，可统一参考 TL-NFW8500（本手册）进行配置。

本手册详细介绍登录企业防火墙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。

1.2　本书约定

在本手册中，

- 所提到的“防火墙”、“本产品”等名词，如无特别说明，系指 TP-LINK 防火墙产品。
- 全文如无特殊说明，Web 界面以 TL-NFW8500 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。

1.3 产品简介

TP-LINK 的防火墙产品一般用于对网络安全有要求的场所，在网络拓扑结构中一般作为外网防火墙和内网交换机的连接枢纽，能及时发现并处理潜在的安全风险、数据传输等问题。

TL-NFW8500 是 TP-LINK 推出的高性能防火墙产品，支持反病毒、入侵防御、恶意域名、应用识别等 4 种特征库，集防火墙策略、攻击防护、DPI 深度安全、安全审计、VPN 等多种功能于一身，在有效抵御网络风险、实现全面防护的同时，简化运维，保障企业核心应用与业务持续稳定运行，适用于企业、机关单位、园区、连锁酒店等场景。

回目录

第2章　登录及配置

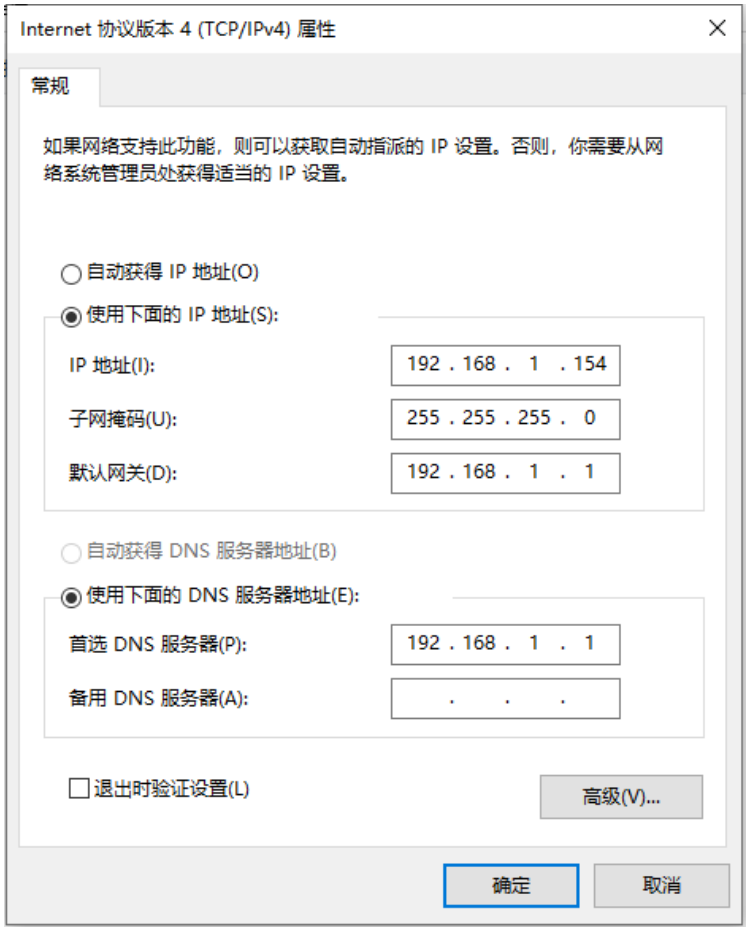
本章介绍如何通过本地 Web 界面，商用网络云平台和手机 APP 管理防火墙。

2.1　登录

2.1.1 登录准备

防火墙默认管理口为 MGMT，默认管理 IP 为 192.168.1.1，第一次登录时，需要确认以下几点：

1. 防火墙已正常加电启动，MGMT 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. 设置 PC 本地连接 IP 地址为 192.168.1.X，X 为 2~254 中的任意整数，子网掩码为 255.255.255.0，默认网关为 192.168.1.1，如图所示。



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。

说明：

- 防火墙出厂默认管理地址为 http://192.168.1.1。

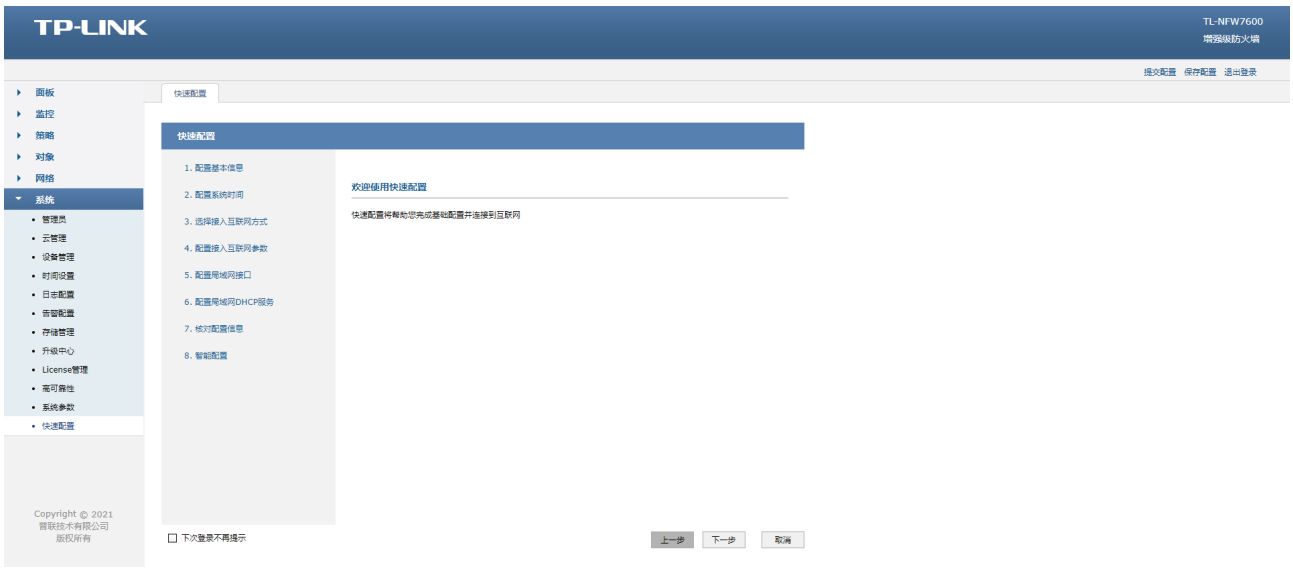
2.1.2 登录步骤

1. 打开浏览器，在地址栏中输入 http://192.168.1.1，按下 Enter 键，进入防火墙的 Web 管理界面。

2. 设置用户名和密码，点击<确认>。

3. 输入设置的用户名和密码，点击<确定>。

4. 登录进入防火墙 web 管理界面，首先进入：“系统>>快速配置”页面，快速配置将帮助您完成基础配置并连接到互联网。点击<下一步>开始快速联网配置；点击<跳过>，将关闭快速配置页面，进入防火墙系统状态页面。



勾选左下角<下次登录不再提示>，后续登录将不再打开快速配置页面。

2.1.3 快速配置

在首次登录防火墙 Web 管理页面时，可通过快速配置对防火墙进行基础配置并连接到互联网。

或者，可进入页面：系统 >> 快速配置 >> 快速配置，进行防火墙快速配置。

1. 配置基本信息：

   可修改主机名称及管理员密码，主机名称默认为“机型名称+硬件版本号”。

设置完成后，点击<下一步>配置系统时间。

说明：

- 如暂时不需要修改基本信息，可点击<跳过>进行下一步。
- 可进入页面：系统 >> 管理员 >> 管理员，修改管理员密码。
- 出厂状态下，防火墙设备云管理功能默认关闭，可进入页面：系统 >> 设备管理 >> 设备管理，查看并修改设备名称；开启云管理功能后，可进入 TP-LINK 商用网络云平台或使用 TP-LINK 商云 APP 修改设备基本信息。

2. 配置系统时间

防火墙支持通过网络获取系统时间或手动设置系统时间。

通过网络获取系统时间，防火墙将通过网络获取 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防火墙日期和时间。可点击<获取管理主机时间>来直接获取管理主机时间。

设置完成后，点击<下一步>。

说明：

- 如暂时不需要配置系统时间，可点击<跳过>进行下一步。
- 可进入页面：系统 >> 时间设置 >> 时间设置，修改管理员密码。

3. 接入互联网

根据网络服务商提供的信息选择互联网方式，并配置对应的网络参数。

静态 IP：拥有网络服务商提供的固定 IP 地址，需要填写以下内容：

上网接口	选择网络接入接口。
IP 地址	填入 ISP 提供的 IP 地址，不清楚可以向 ISP 询问。
子网掩码	填入 ISP 提供的子网掩码，一般为 255.255.255.0。
默认网关	填入 ISP 提供的网关地址，不清楚可以向 ISP 询问，允许留空。
首选 DNS 服务器	填入 ISP 提供的 DNS 服务器地址，不清楚可以向 ISP 询问，允许留空。
备用 DNS 服务器	如果 ISP 提供了两个 DNS 服务器地址，则可以把另一个 DNS 服务器的 IP 地址填于此处，允许留空。
上网接口	选择网络接入接口。

DHCP：自动从网络服务商处获取 IP 地址，需要选择上网接口。

PPPoE：虚拟拨号方式，需要填写以下内容。

上网接口	选择网络接入接口。
用户名	填入 ISP 提供的 IP 地址，不清楚可以向 ISP 询问。
密码	填入 ISP 提供的子网掩码，一般为 255.255.255.0。

配置完成后，点击<下一步>进行局域网配置。

说明：

- 可进入页面：网络 >> 接口设置，进行更详细的接口配置。具体请参考 ***4.1 接口模式***。

4. 配置局域网接口

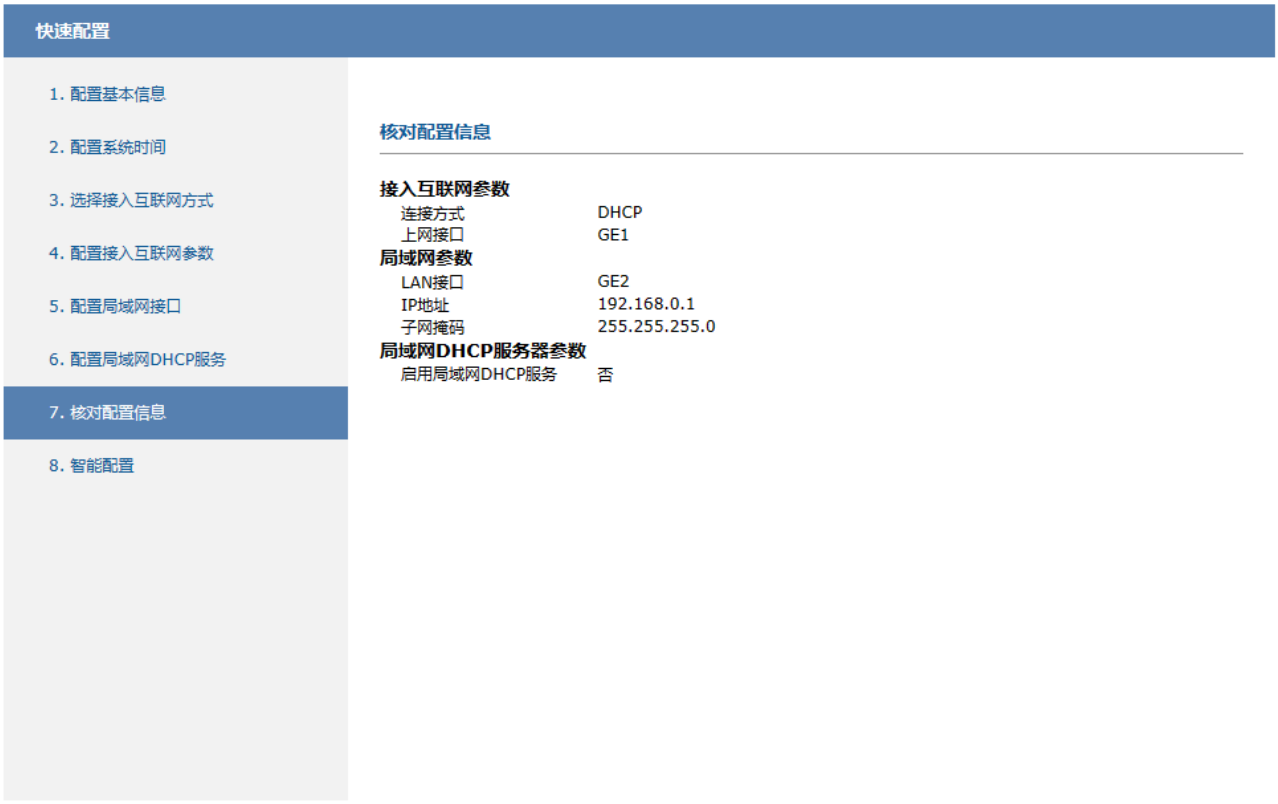
配置局域网接口，及其 IP 地址和子网掩码。

5. 配置局域网 DHCP 服务

可选择开启局域网 DHCP 服务，设置为局域网网络设备分配的 IP 地址池。

6. 核对配置信息

核对设备接入互联网参数、局域网参数及局域网 DHCP 服务器参数，确认无误后，点击<应用>。



7. 智能配置

智能配置可以自动发现全网设备、生成拓扑图，通过一台设备配通整个网络，实现全网一体化配置。

实现智能配置，需开启云管理功能，并确保设备成功连接网络。

点击<登录 TP-LINK 统一管理平台>，登录 TP-LINK 商用网络云平台。

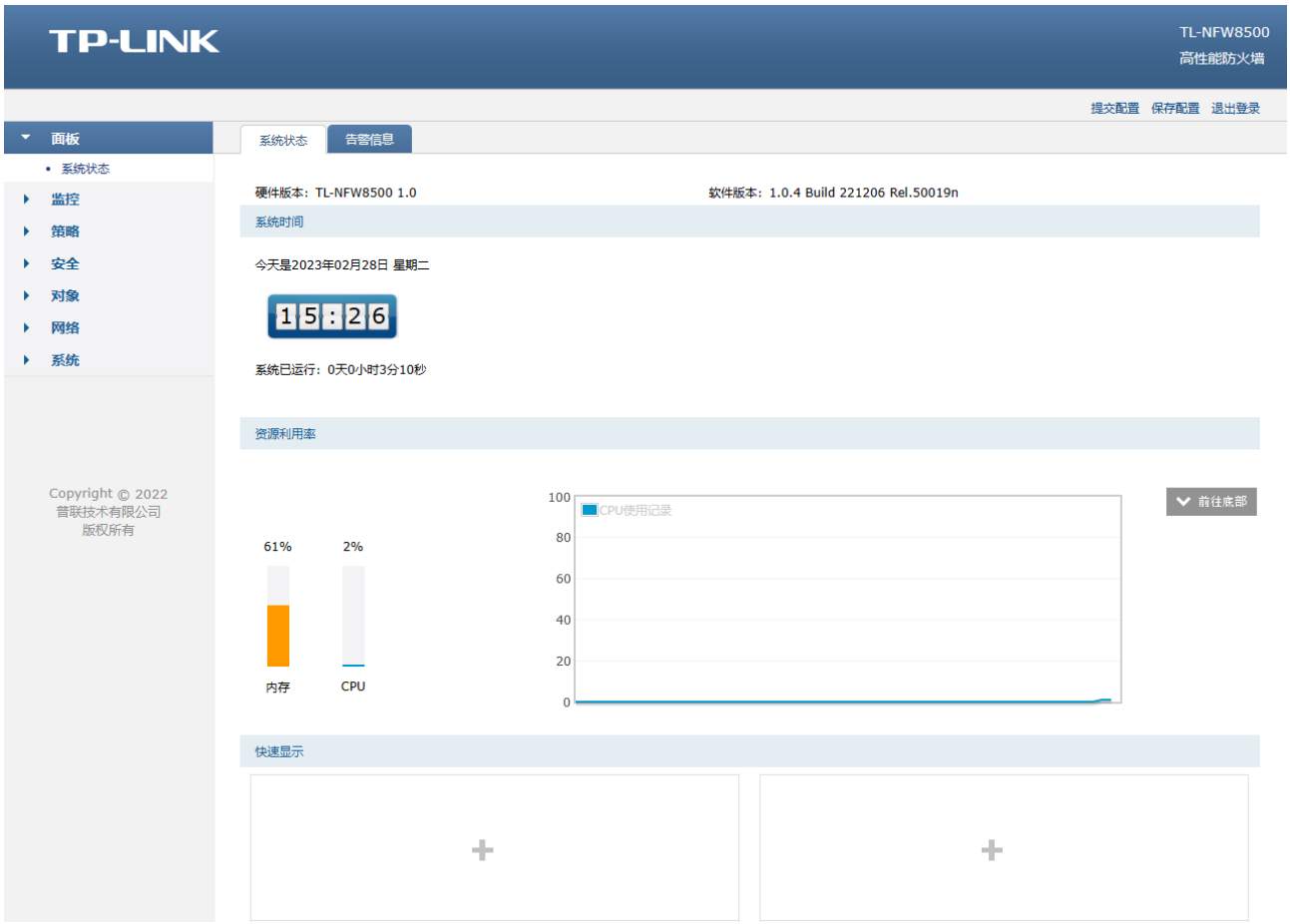
输入 TP-LINK ID 及密码，点击<登录>。若无 TP-LINK 账号，点击<创建 TP-LINK ID>注册。

选择已有项目，或点击<添加项目>创建新项目，点击<绑定设备>。出现“绑定成功”提示即完成绑定。

设备绑定成功后，将自动发现全网拓扑，可根据页面提示完成智能配置。

2.1.4 Web 管理界面

登录到 Web 管理界面后，进入到页面：面板 >> 系统状态，可查看系统相关信息，包括设备硬件版本、软件版本、系统时间、资源利用率等。



当配置策略规则或各项参数后，请点击页面右上角<提交配置>或<保存配置>，使配置信息生效。

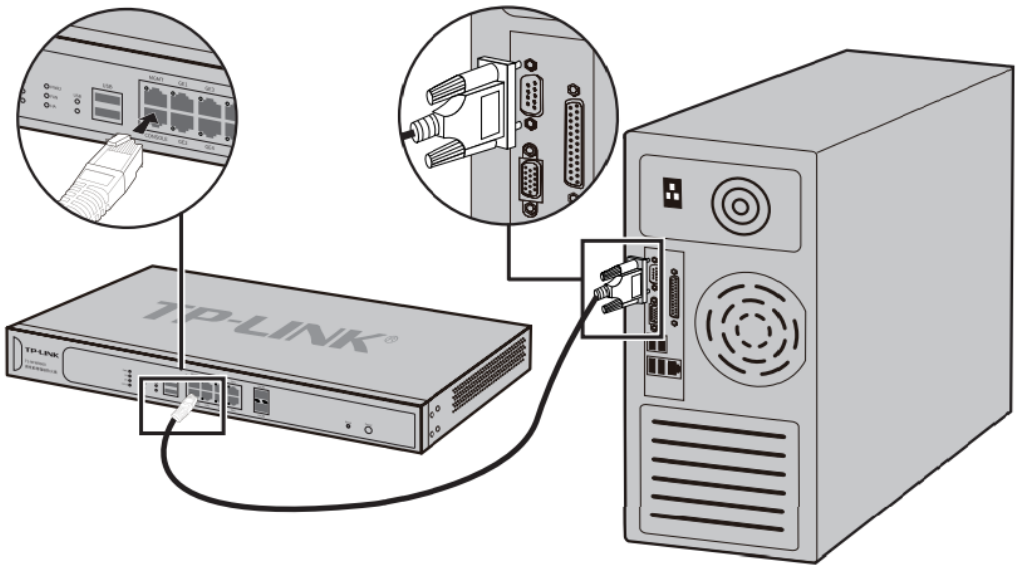
2.2 Console 接口登录

TP-LINK 防火墙可以通过 Console 接口进行管理，出厂配置下，使用 Console 接口管理防火墙不需要用户名和密码。

2.2.1 接口连接方式

防火墙提供一个 Console 端口，连接方式如下图所示。

1. 将 Console 连接线的 RJ45 端连入防火墙；
2. 将 Console 连接线的另一端 RS232 DB9 公头连入计算机，如下图所示：



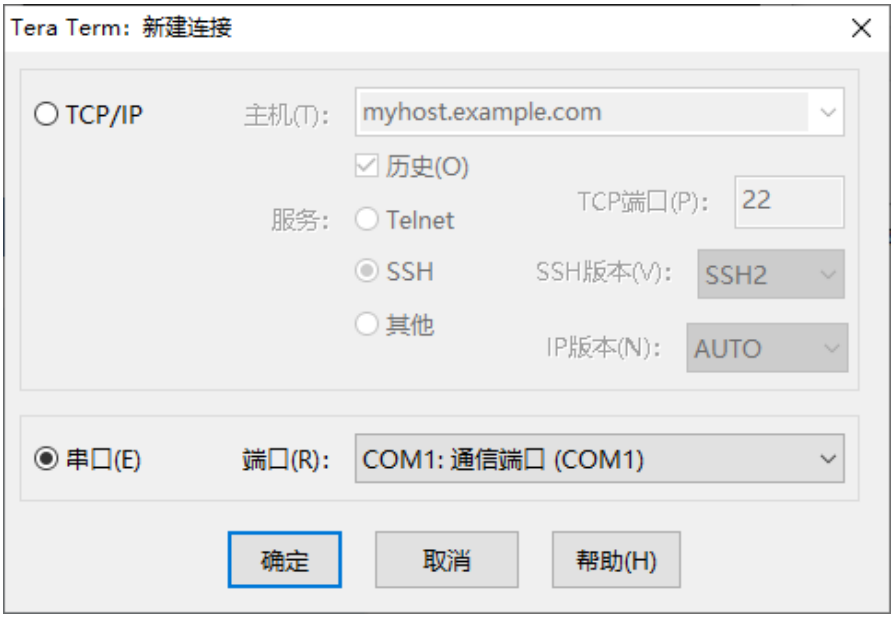
2.2.2 Console 接口管理

1. 安装驱动。

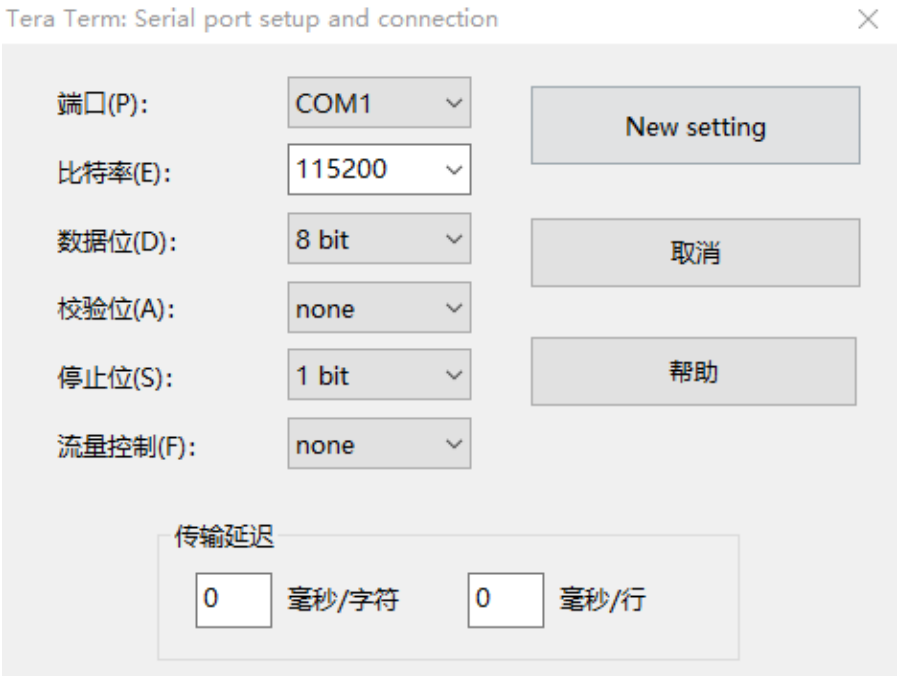
   如果电脑自带串口接口，则不需要安装驱动；

   如果使用 USB 转串口线，电脑上需要安装 USB 转串口线的驱动。

2. 电脑上安装串口通信客户端软件（比如 Tera Term、SecureCRT 等，本小节以 Tera Term 为例），在串口通信客户端软件上新建连接，选择 Serial，以及对应的通信端口（不同电脑的通信端口有所差别）。



3. 串口相关设置中设置波特率：115200bps、数据位：8bit、校验位：none、停止位：1bit、数据流控制：none。



4. 在主窗口中输入回车键，可以看到“TL-NFW8500>”的提示符，说明已成功登录防火墙。登录成功后，直接在窗口中输入管理 CLI 命令即可。

2.3 云管理

防火墙支持 TP-LINK 商用云平台统一管理，方便对防火墙、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。

2.3.1 TP-LINK 商用网络云平台

➢ **登录 TP-LINK 商用网络云平台管理**

1. 确认防火墙设备已联网，并开放相关安全策略。

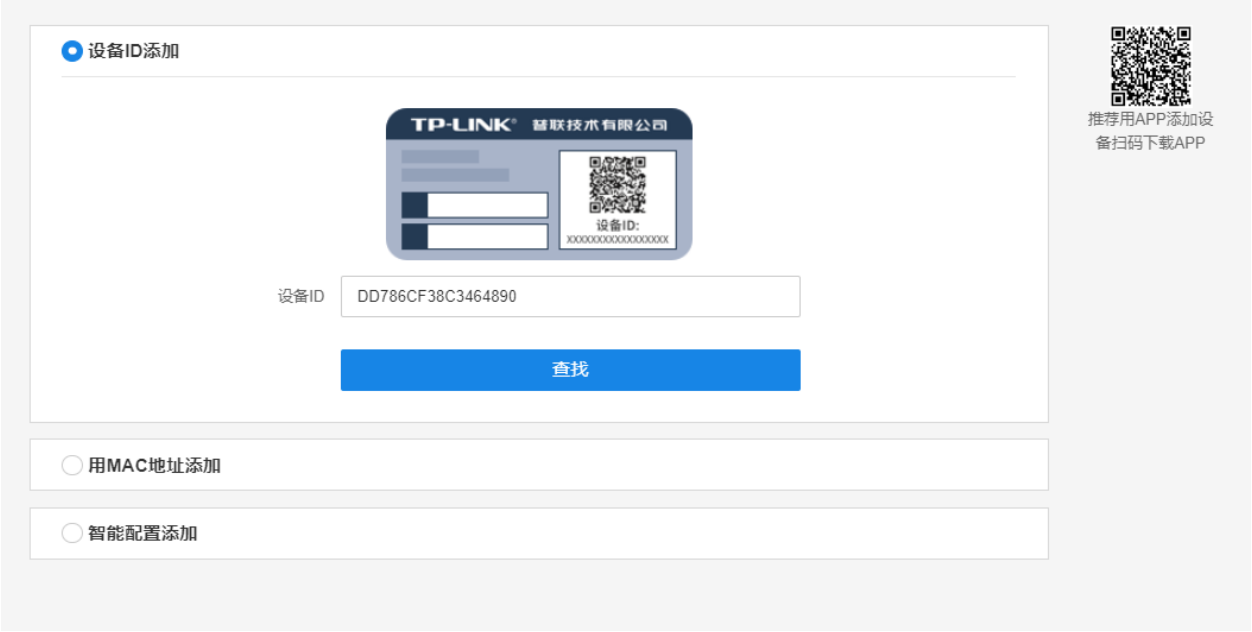
2. 进入页面：系统 >> 云管理，开启云管理功能，点击<设置>。

3. 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。

4. 进入页面：项目 >> 设备管理，点击右上角<添加设备>。

5. 支持通过设备 ID/MAC 地址/智能配置添加设备。

1）选择“设备 ID 添加”，设备 ID 可在防火墙底部标贴上查找。



2）选择“用 MAC 地址添加”，输入防火墙 MAC 地址和防火墙本地 Web 管理的用户名和密码，点击<添加>。

3） 选择“智能配置添加”，点击<开始智能配置>，可通过当前路由自动发现局域网中全部设备、统一添加、并进行集中管理。

6. 添加完成后在设备信息中找到对应防火墙设备，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。

2.3.2 TP-LINK 商云 APP

扫描二维码可获取 iOS 版 APP、Android 版 TP-LINK 商云 APP 最新版下载链接。将防火墙配置联网后可使用商云 APP 添加设备上云进行管理。

➢ 扫描设备 ID 二维码上云

1. 将防火墙配置联网并开放相关安全策略后，打开 TP-LINK 商云 APP，在项目中选择 添加设备 >> 网络设备 >> 扫码添加 ，扫描设备机身标贴上的二维码。

2. 设置账号密码，点击<添加>将设备添加上云：

3. 添加完成后，点击设备进入管理界面，可查看设备基本信息、端口配置信息和统计信息等。

➢ 手动输入 MAC 地址或设备 ID 上云

1. 将防火墙配置连网后，打开 TP-LINK 商云 APP，在项目中选择“添加设备 >> 网络设备 >> 扫码添加 >> 手动输入”，通过设备机身标贴上的 MAC 地址或设备 ID 添加上云：

2. 设置账号密码，点击<添加>将设备添加上云：

3. 添加完成后，点击设备进入管理界面，可查看设备基本信息、网络信息和安全策略信息等。

2.4 远程管理

远程管理功能可以在网络任何地方远程实时、安全地监控和配置网络。

➢ **远程管理配置步骤如下：**

1. 登录防火墙管理页面（默认地址：192.168.1.1）。进入页面：系统 >> 管理员 >> 远程管理。

2. 点击<新增>，添加路由条目：远程地址范围为 0.0.0.0/0，状态勾选为“启用”，点击<确定>（0.0.0.0/0 代表所有外网电脑均可以访问防火墙）。

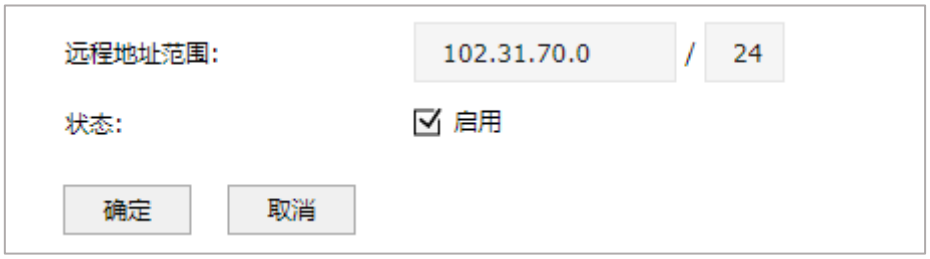
远程地址范围　　远程管理主机的地址范围

状态　　勾选“启用”对规则对应的地址范围内的主机进行远程管理。

3. 进入页面：系统 >> 管理员 >> 系统管理设置，配置 Http 服务端口。80、8080 等常用端口很可能被宽带服务商屏蔽，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。配置完成，点击<设置>。

➢ **配置实例**

如果地址段为 102.31.70.0/24 的主机（非 LAN 口网段）需要对设备进行远程管理，可以建立远程管理地址条目，点击<新增>，设置远程地址范围 102.31.70.0/24，状态勾选为启用，点击<确定>保存设置。



远程管理设置完成后，外网电脑可通过 http://防火墙 IP:端口号 对防火墙进行远程访问。如果防火墙上登录了动态域名，还可以使用 http://域名:端口 来访问。上网接口 IP 需要为外网 IP 地址。

注意：

- 80、8080 等常用端口很可能被宽带服务商屏蔽，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。

- 包含局域网地址的远程管理地址条目无效。
- 如果添加 0.0.0.0/0 的条目，将允许所有远程计算机访问设备，在非法攻击情况下可能无法访问设备。

2.5 IPv6 上网配置

IPv6 为 Internet 研究组织发布新的主机标识方法，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、防火墙、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；防火墙可以同时获取到 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：网络 >> 接口设置，选择关联的物理接口。

说明：

- 物理接口：物理接口是设备上实际存在的组件，本设备的物理接口命名为端口 1,端口 2，端口 3...端口 n，n 为物理接口个数。
- 接口：在逻辑上将一个物理接口划分为多个虚拟的接口，每个接口使用的带宽都来自于它所属的物理接口。

2. 选择关联的物理接口，例下图选择 GE1，点击<新增>，接口类型选择 PPPoE 接口，IP 协议类型选择 IPv6，状态选择启用。根据运营商提供的 IPv6 上网方式进行 IPv6 设置，开启前缀授权功能默认开启，配置完成后点击<确定>。

接口类型	选择运营商提供的 IPv6 上网连接方式方式，分为 Ethernet 和 PPPoE Ethernet 支持静态 IP 和 DHCP 的连接方式 PPPoE 支持 xDSL 拨号上网使用。新建 PPPoE 接口时，必须保证在同一物理接口下有 Ethernet 接口可供选择。
接口名称	设置一个名称来标识一个接口，仅可以使用英文、数字和下划线来命名，且不能以数字开头。
关联接口	指定关联的物理接口。
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。
用户名	ISP 提供 ADSL IPv6 独立虚拟拨号方式的帐号，若您不了解或遗忘账号密码，请向 ISP 询问。

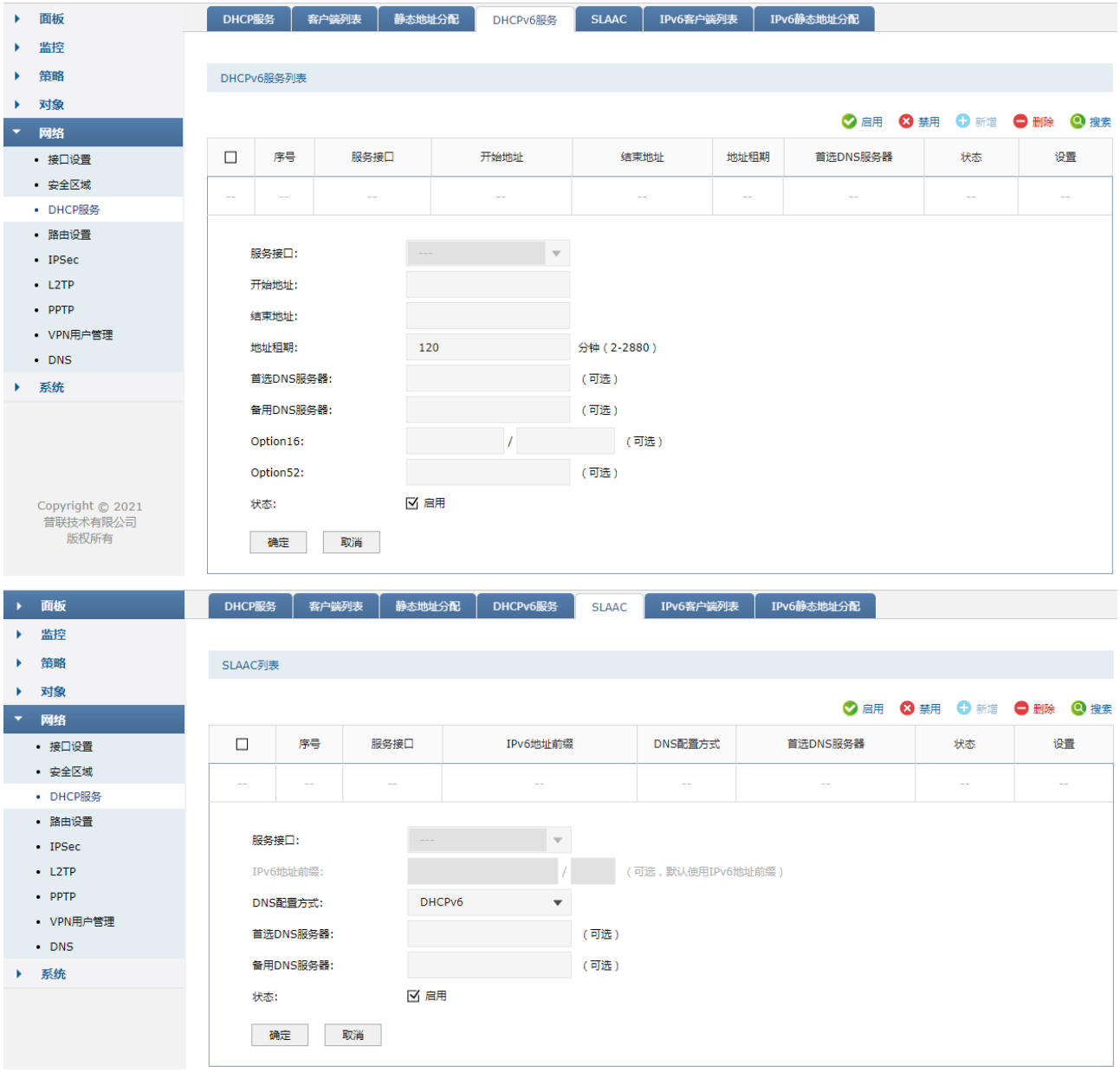
密码	ISP 提供 ADSL IPv6 独立虚拟拨号方式的密码，若您不了解或遗忘账号密码，请向 ISP 询问。
IPv6 地址获取协议	默认自动，也可以根据需要进行相应修改。 如果选择 DHCPv6，则直接由运营商动态分配一个 IPv6 地址； 如果选择 SLAAC，则由防火墙根据路由通告自动生成 IPv6 地址； 如果选择静态 IP，则使用运营商提供的固定 IPv6 地址进行上网。
前缀授权	当 IPv6 地址获取协议为自动、DHCPv6 或者 SLAAC 时，可以选择是否开启前缀授权功能。开启此功能后，防火墙将自动从运营商获取一个 IPv6 地址前缀，该前缀用于为局域网中设备生成 IPv6 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。一般情况下，前缀授权需要开启。
首选/备用 DNS 服务器	可选项，请填入 ISP 提供的 DNS 服务器，若不了解，请向 ISP 询问。
服务名	可选项，填入 ISP 提供的服务名称。缺省为空。
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。连接方式为 PPPoE 拨号时 ，MTU 范围为 576-1492，缺省值为 1492；连接方式为 自动获取 IP 地址 或 固定 IP 地址 时，MTU 范围为 576-1500，缺省值为 1500（接口开启 IPv6 功能时，动静态 IP 可设置范围为 1280-1500，PPPoE 可设置的最大范围是 1280-1492）。
连接方式	选择上网时连入互联网的方式，有自动连接、手动连接、定时连接三种方式。 自动连接：设备上电完成后，将自动拨号连入互联网。适合不限时的包月计费的用户。 手动连接：需要手动拨号连入互联网，适合按小时计费的拨号连接上网方式。 定时连接：在时间下拉列表中选择时间对象，适合于需要限时上网的场景。如需新建时间对象，请前往 对象管理->时间管理 页面。
时间	当连接方式选择为定时连接时，可以在下拉列表中选择合适的时间对象来进行拨号。如需新建时间对象，请前往 对象管理->时间管理页面。
上/下行带宽	设置接口的上/下行带宽。
管理接口开启	勾选该项使得该接口成为管理接口。

3. 选择关联的物理接口，下图以 GE1 为例，点击<新增>，接口类型选择 Ethernet 接口，IP 协议类型选择 IPv6，状态选择启用。Ethernet 接口配置如下：

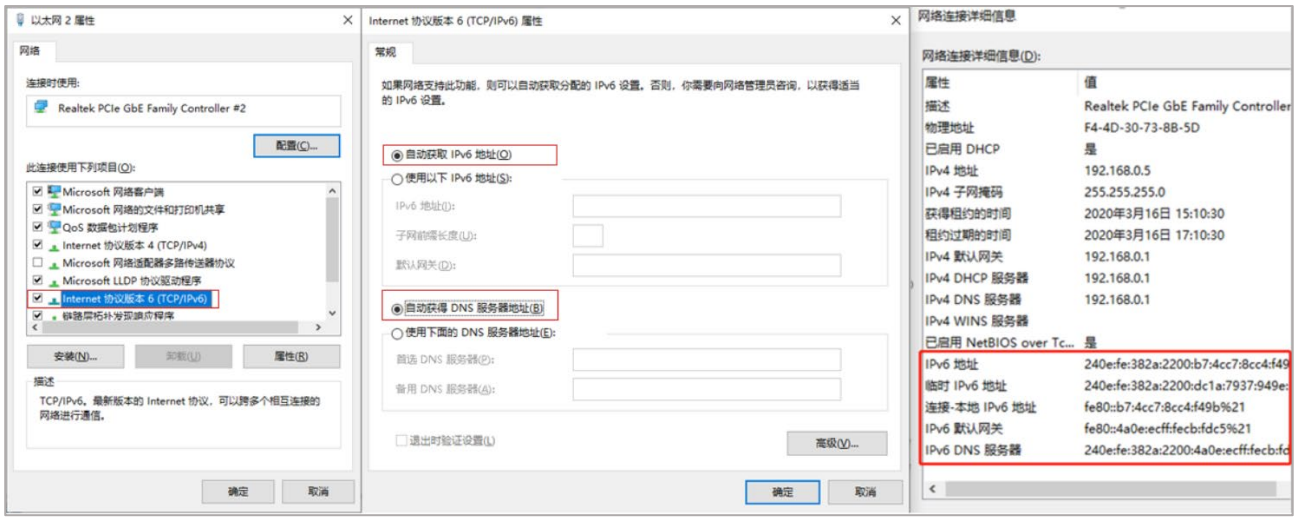
接口类型	选择运营商提供的 IPv6 上网连接方式方式，分为 Ethernet 和 PPPoE。 Ethernet 支持静态 IP 和 DHCP 的连接方式； PPPoE 支持 xDSL 拨号上网使用。新建 PPPoE 接口时，必须保证在同一物理接口下有 Ethernet 接口可供选择。
接口名称	设置一个名称来标识一个接口，仅可以使用英文、数字和下划线来命名，且不能以数字开头。
关联接口	指定关联的物理接口。
连接方式	提供静态 IP 和 DHCP 两种连接方式，选择静态 IP 连接方式，需要手动配置 IP；选择 DHCP 方式时，由设备动态获取 IP。
IP 协议类型	选择 IPv6 协议类型。
状态	勾选“启用”。
IPv6 地址获取协议	当选择 DHCP 连接方式时，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，则由防火墙根据路由通告自动生成 IPv6 地址； 如果选择静态 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，防火墙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。一般情况下，前缀授权需要开启。
地址配置方式	提供 EUI-64 和手动配置地址两种方式。
前缀授权接口	当选择 EUI-64（EUI-64 表示自动获取 64 位 IPv6 的前缀地址）地址配置方式时，选择开启前缀授权功能的接口。
IPv6 地址前缀	当选择 EUI-64 地址配置方式时，自定义 IPv6 地址前缀。
IP 地址	当选择手动地址配置方式时，自定义 IPv6 地址。
子网前缀长度	当选择手动地址配置方式时，设置 IPv6 子网前缀长度，一般为 64。
网关地址	设置网关地址。该项为可选项，允许留空。
首选/备选 DNS 服务器	DNS 即 Domain Name Server，域名解析服务器。设置首选/备选的 DNS 服务器，允许留空。
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。连接方式为 PPPoE 拨号时 ，MTU 范围为 576-1492，缺省值为 1492；连接方式为 自动获取 IP 地址 或 固定 IP 地址 时，MTU 范围为 576-1500，缺省值为 1500（接口开启 IPv6 功能时，动静态 IP 可设置范围为 1280-1500，PPPoE 可设置的最大范围是 1280-1492）。
上/下行带宽	设置接口的上/下行带宽。
MAC 地址	可更改防火墙的 MAC 地址。
管理接口开启	勾选该项使得该接口成为管理接口。

4. 进入页面“网络 >> DHCP 服务”，根据需要设置 IPv6 地址分配方式，可以选择 DHCPv6 或者 SLAAC（二选一），DNS 不填时默认为路由器的 IPv6 地址，路由器作 DNS 代理。其中 DHCPv6 是路由器手动设置一个范围下发地址；SLAAC 是根据地址前缀路由器随机下发地址。



5. 设置好防火墙的相关参数后，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，无法由防火墙给终端分配 IPv6 地址终端 IPv6 地址统一由运营商进行分配，需要防火墙支持 IPV6 桥模式。当开启 IPv6 桥模式后，防火墙 IPv6 工作在桥接模式，连接到防火墙的客户端由上联设备分配 IPv6 地址并提供路由服务。

进入页面：网络 >> 接口设置 >> IPv6 桥模式

开启 IPv6 桥模式　　勾选<启用>，开启 IPv6 桥模式。

广域网接口设置　　选取一个接口作为广域网接口。

局域网接口设置　　选取一个接口作为局域网接口。

桥模式下，PPPoE 接口和 Ethernet 接口的 IPv6 参数均不可设置。

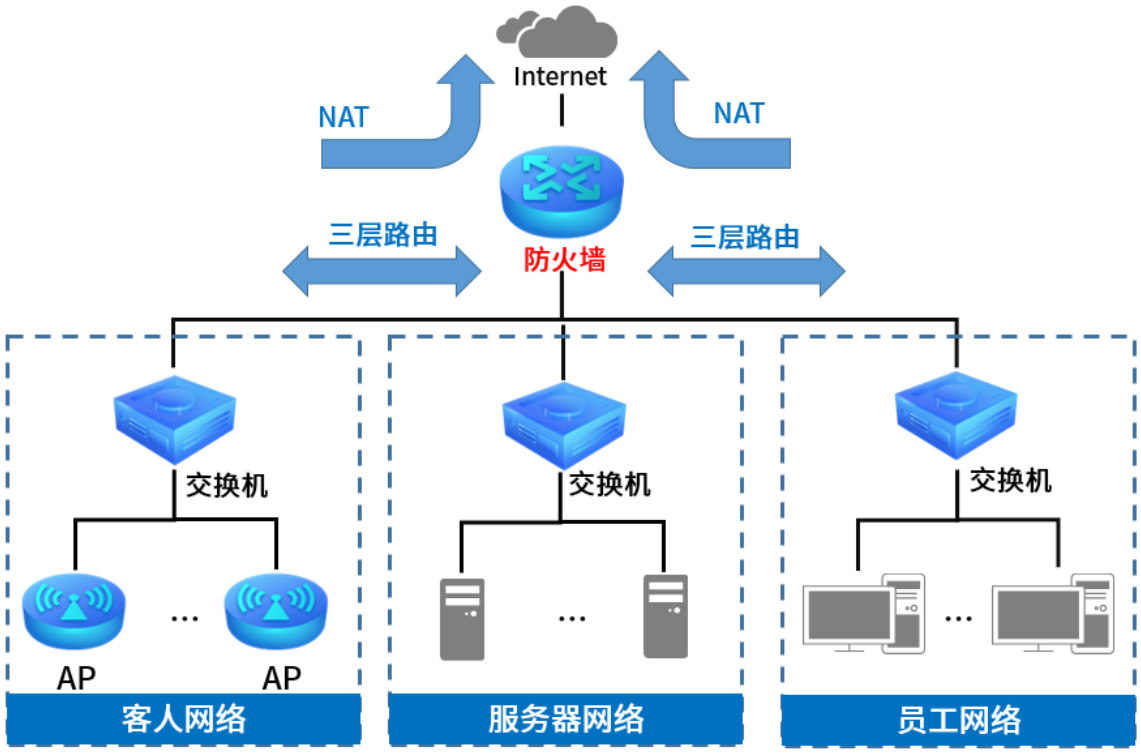
回目录

2.6　三层网关组网配置实例

防火墙可作为三层路由网关接入网络。可替代路由器使用防火墙业务接口地址作为所连接网段中设备的默认网关，实际部署时可能需要改变现有的网络拓扑结构，可在防火墙上启用路由和 NAT 功能，内部不同网段之间数据通信通过路由进行转发，内网和外网之间通过 NAT 地址转换后实现数据通信。

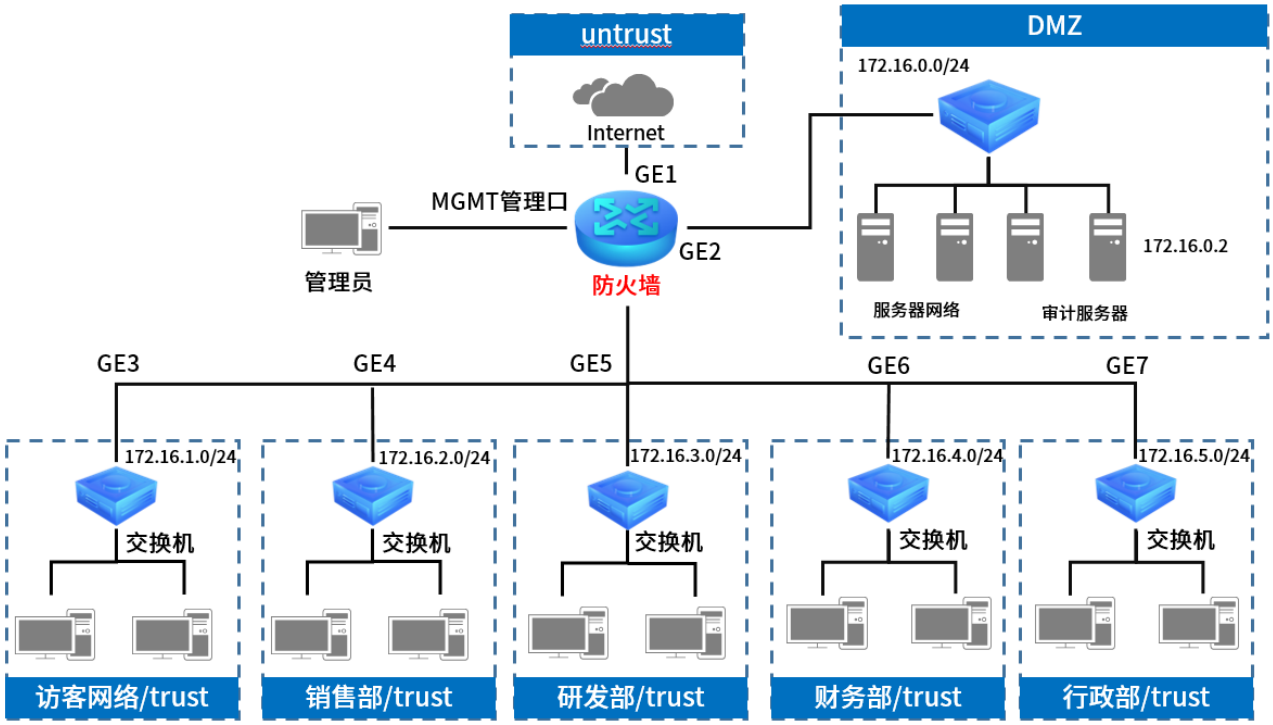
无论是内网不同网段之间的数据通信，还是内网与外网之间的数据通信，所有流量都需要经过防火墙转发，这种情况下防火墙的报文处理机制更加完善，对网络安全防护能力更强。

常用应用拓扑如下：



需求场景：

某公司使用 TL-FW6300 搭建网络，防火墙连接互联网，并划分多个网段内部使用，网络拓扑结构如下图所示。



安全需求：

- 访客网络可以访问互联网，但是不能访问内部其他网络；
- 销售部可以访问内部服务器网络以及互联网，但是禁止访问常见的游戏、视频、炒股类网站和应用；
- 研发部、财务部、行政部可以访问内部服务器网络，但是不能访问互联网，仅允许访问公司外部官方网站 www.test.com；
- 出差员工可以通过互联网访问内网的 8080 端口的 WEB 服务器；
- 内部各个部门以及访客区域之间禁止互相访问；
- 管理接口仅用于管理防火墙自身。

审计需求：

- 对所有流经防火墙的数据进行审计，并记录到审计日志；
- 将防火墙的审计日志、系统日志、操作日志、流量日志、策略命中日志全部上传至安装了 TP-LINK 安全审计系统的审计服务器。

配置思路：

第一步：配置接口参数：GE1 接入 Internet，GE2 接入服务器网络，GE3 接入访客网络，GE4 接入销售部，GE5 接入研发部，GE6 接入财务部，GE7 接入行政部。

第二步：设置 NAPT：配置各个网段通过 GE1 进行 NAT 联网。

第三步：设置 DHCP 服务器：为内网各网段设备动态分配 IP 地址。

第四步：设置安全区域：将 GE1 加入 untrust 区域，GE2 加入 DMZ 区域，其他接口加入 trust 区域。

第五步：设置对象。IP 地址对象：访客网络、销售部、研发部、财务部、行政部；服务对象：内部 web 服务器；网站对象：公司官网，应用对象：需禁止的游戏、视频、炒股类网站和应用；安全配置文件。

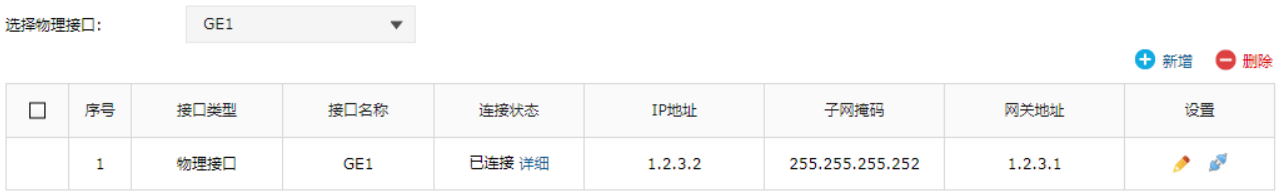
第六步：设置安全策略，满足安全需求。

第七步：设置审计策略，满足审计需求。

第八步：对接审计服务器。

配置步骤：

1. 进入页面：网络 >> 接口设置，选择物理接口 GE1，点击 ，按照运营商提供的联网参数进行填写，此处以静态 IP 联网方式为例。



2. 进入页面：网络 >> 接口设置，选择物理接口 GE2，点击 ，配置配置服务器接口 IP 地址为 172.16.0.0/24。

   配置方法与服务器网段相同，配置 GE3 的 IP 地址为 172.16.1.1，用作访客网络。

   配置方法与服务器网段相同，配置 GE4 的 IP 地址为 172.16.2.1，用作销售部网络。

   配置方法与服务器网段相同，配置 GE5 的 IP 地址为 172.16.3.1，用作研发部网络。

   配置方法与服务器网段相同，配置 GE6 的 IP 地址为 172.16.4.1，用作财务部网络。

   配置方法与服务器网段相同，配置 GE7 的 IP 地址为 172.16.5.1，用作行政部网络。

连接方式	设置接口 IP 地址的配置方式，本例中选择“静态 IP”。
IP 地址	设置接口的 IP 地址。
子网掩码	设置接口的子网掩码，本例中为“255.255.255.0”。
网关地址	设置接口的网关地址，本例中不填。
上行带宽	设置接口的上行带宽值，本例中保持默认。
下行带宽	设置接口的下行带宽值，本例中保持默认。
MTU	设置接口的 MTU 值，本例中保持默认。
首选 DNS 服务器	设置接口的首选 DNS 服务器 IP 地址，本例中保持默认，不填写。
备用 DNS 服务器	设置接口的备用 DNS 服务器地址，本例中保持默认，不填写。
MAC 地址	设置接口的 MAC 地址，本例中保持默认。
备注	添加备注，方便后期维护，如“服务器”等。

3. 进入页面：策略 >> NAT 策略 >> NAPT，设置 NAPT 规则，各网段通过 GE1 进行 NAT 联网。

出接口：选择连接宽带的接口，本例中为“GE1”。

源地址范围：设置为内部的网段，本例中为了简化设置，网段归纳为“172.16.0.0/16”。

4. 进入页面：网络 >> DHCP 服务 >> DHCP 服务，为内网设备分配 IP 地址。

DHCP服务列表

启用 禁用 新增 删除 搜索

	序号	服务接口	开始地址	结束地址	地址租期	网关地址	首选DNS服务器	状态	设置
	1	GE2	172.16.0.2	172.16.0.254	120	---	202.96.128.166	已启用	
	2	GE3	172.16.1.2	172.16.1.254	120	---	202.96.128.166	已启用	
	3	GE4	172.16.2.2	172.16.2.254	120	---	202.96.128.166	已启用	
	4	GE5	172.16.3.2	172.16.3.254	120	---	202.96.128.166	已启用	
	5	GE6	172.16.4.2	172.16.4.254	120	---	202.96.128.166	已启用	
	6	GE7	172.16.5.2	172.16.5.254	120	---	202.96.128.166	已启用	

为每个网段添加一个 DHCP 服务器，简化客户端配置。

5. 进入页面：网络 >> 安全区域，在 trust 条目下点击 ，将 GE3/4/5/6/7 和 MGMT 端口添加到 trust 安全区域。

在 untrust 条目下点击 ，将 GE1 端口添加到 untrust 安全区域。在 DMZ 条目下点击 ，将 GE1 端口添加到 DMZ 安全区域。

	序号	名称	优先级	接口	备注	编辑
--	1	local	100	---	---	
--	2	trust	85	GE3,GE4,GE5,GE6,GE7,MGMT	内网	
--	3	untrust	5	GE1	Internet	
--	4	dmz	50	GE2	服务器	

6. 进入页面：对象 >> 地址 >> 地址，点击<新增>，添加服务器地址段。

地址组 地址

	序号	地址名称	IP类型	IP段	备注	设置
--	--	--	--	--	--	--

地址名称: Servers (1-32个字符)

IP类型: IP段 IP/Mask

172.16.0.0 / 24

备注: 服务器区 (可选，1-50个字符)

确定 取消

新增服务器网段IP地址段

同服务器地址添加方法，添加访客、销售部、研发部、财务部、行政部地址段。

地址组 | 地址

地址列表

新增 删除 搜索 全局搜索

	序号	地址名称	IP类型	IP段	备注	设置
☐	1	Sales	IP/Mask	172.16.2.0/24	销售部	
☐	2	RD	IP/Mask	172.16.3.0/24	研发部	
☐	3	Finance	IP/Mask	172.16.4.0/24	财务部	
☐	4	Admin	IP/Mask	172.16.5.0/24	行政部	
☐	5	GUEST	IP/Mask	172.16.1.0/24	访客	
☐	6	Servers	IP/Mask	172.16.0.0/24	服务器区	

7. 进入页面：对象 >> 地址 >> 地址组，点击<新增>，建立服务器地址组，服务器地址组包含服务器地址段。

地址组 | 地址

组列表

新增 删除 搜索 全局搜索 导入 备份

	序号	组名称	地址名称	备注	设置
--	--	--	--	--	--

组名称: Servers (1-28个字符)

地址名称: Servers

备注: (可选，1-50个字符)

确定 取消

- Sales
- RD
- Finance
- Admin
- GUEST
- Servers

新增服务器网段IP地址组

1		---	IPGROUP_ANY	---	
2		---	中国所有IP地址	---	

按照此方式添加其他地址组，包括访客、销售部、研发部、财务部和行政部的地址组。另外单独添加一个包含研发部、财务部以及行政部的内网部门 Internal。

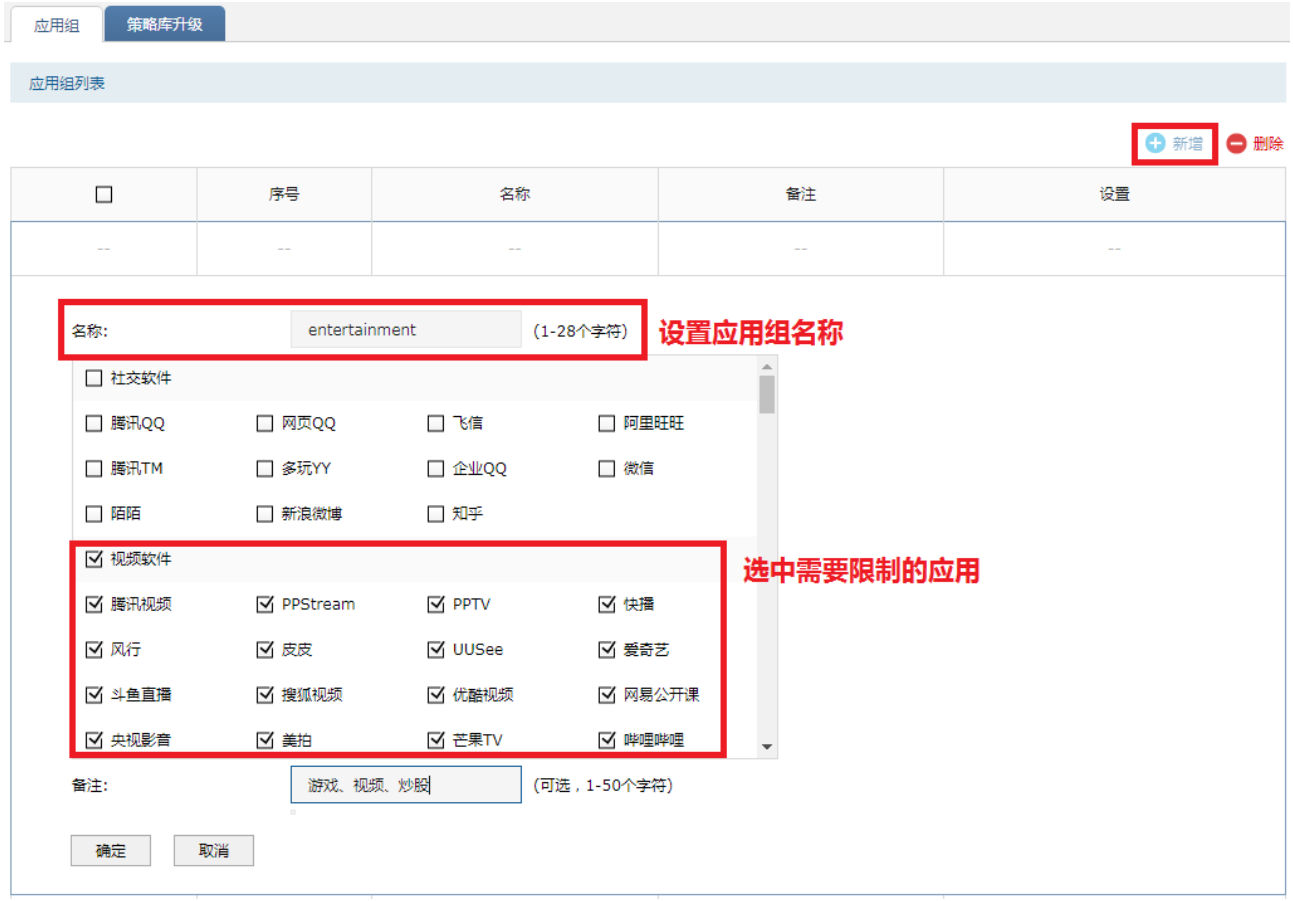
☐	8	Servers	Servers	服务器IP地址段	
☐	9	GUSET	GUEST	访客IP地址段	
☐	10	Sales	Sales	销售部IP地址段	
☐	11	RD	RD	研发部IP地址段	
☐	12	Finance	Finance	财务部IP地址段	
☐	13	Admin	Admin	行政部IP地址段	
☐	14	Internal	RD,Finance,Admin	内网部门	

8. 进入页面：对象 >> 服务 >> 服务，点击<新增>，设置外网可以访问的内部 WEB 服务器服务条目。

9. 进入页面：对象 >> 服务 >> 服务组，点击<新增>，建立 WEB 服务器组包含内部 WEB 服务器条目。

10. 进入页面：对象 >> 网站 >> 网站组，点击<新增>，内部网络可以访问的公司官网网址加入网站组。

11. 进入页面：对象 >> 应用 >> 应用组，点击<新增>，将销售部禁止访问的应用加入该组。



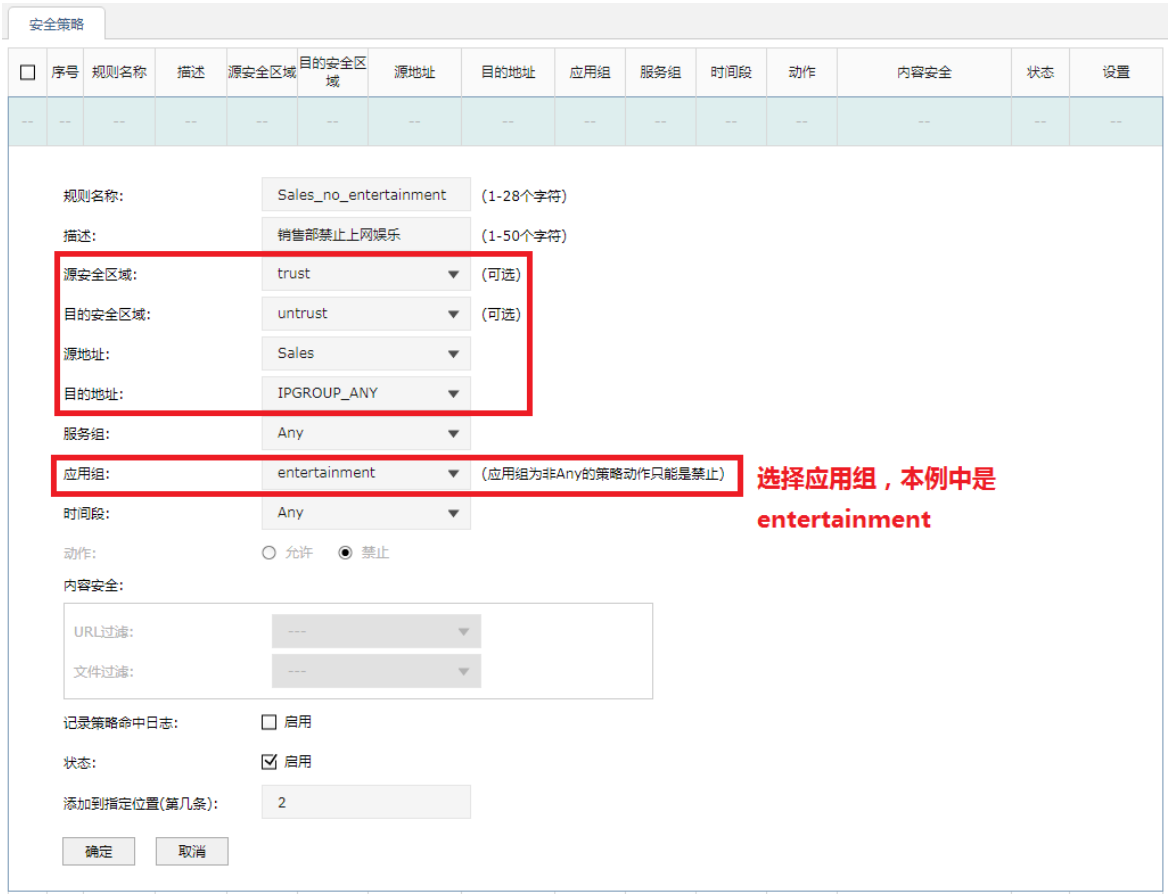
12. 进入页面：对象 >> 安全配置文件 >> URL 过滤，点击<新增>，设置 URL 过滤规则：仅允许访问公司官网。

13. 进入页面：策略 >> 安全策略，点击<新增>，如下图配置，设置第 1 条策略，访客网络可以访问互联网，配置参数如下图。

14. 进入页面：策略 >> 安全策略，点击<新增>，配置方法同步骤 13，源地址选择销售部。设置第 2 条策略：销售部可以访问互联网。

15. 进入页面：策略 >> 安全策略，点击<新增>，源地址选择销售部，目的地址选择服务器地址组。设置第 2 条策略：销售部可以访问内部服务器网络。

16. 进入页面：策略 >> 安全策略，点击<新增>，源地址选择销售部，应用组选择需禁用的娱乐应用组，动作选择禁止。设置第 2 条策略：销售部禁止访问常见的游戏、视频、炒股类网站和应用。



17. 进入页面：策略 >> 安全策略，点击<新增>，设置步骤 15，源地址选择研发部、财务部、行政部。设置完成第 3 条策略：研发部、财务部、行政部可以访问内部服务器网络。

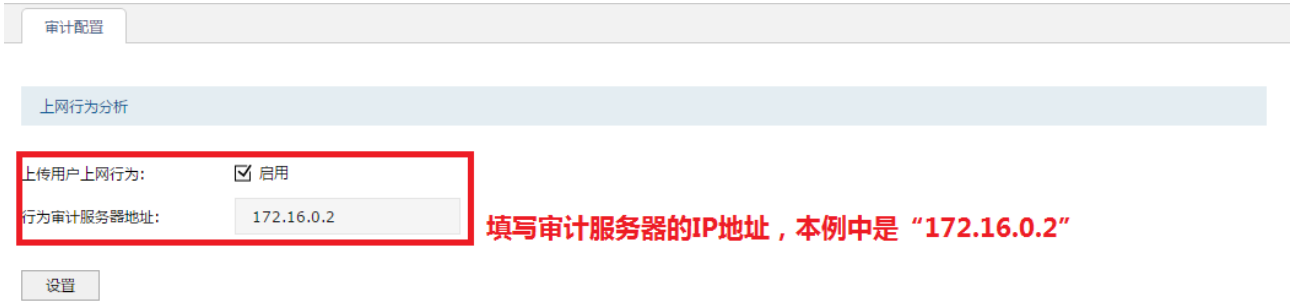
18. 进入页面：策略 >> 安全策略，点击<新增>，URL 过滤选择安全配置文件外部官网网站。设置完成第 3 条策略：研发部、财务部、行政部允许访问公司外部官网网站 www.test.com 。

19. 进入页面：策略 >> 安全策略，点击<新增>，目的地址选择服务器地址组，服务组选择外网可访问的服务组。设置完成第 4 条策略：出差员工可以通过互联网访问内网的 8080 端口的 WEB 服务器。

20. 以审计管理员身份登录防火墙，进入页面：对象 >> 审计配置文件，点击<新增>，需要审计所有 URL 和网站，启用“IM 行为审计”。

21. 以审计管理员身份登录防火墙，进入页面：策略 >> 安全策略，点击<新增>，审计配置文件选择步骤 20 配置的审计配置文件。设置完成审计需求：所有流经防火墙的数据进行审计。

22. 以审计管理员身份登录防火墙，进入页面：系统 >> 日志配置，勾选“上传用户上网行为”，填写审计服务器地址。



23. 以系统管理员身份登录防火墙，进入页面：对象 >> 地址 >> 地址，点击<新增>，添加审计服务器地址。

24. 以系统管理员身份登录防火墙，进入页面：对象 >> 地址 >> 地址组，点击<新增>，将审计服务器地址添加到地址组。

25. 进入页面：策略 >> 安全策略，点击<新增>，允许防火墙访问审计服务器地址组。

26. 以系统管理员身份登录防火墙，进入页面：系统 >> 日志配置，勾选“发送日志”，填写日志服务器地址。

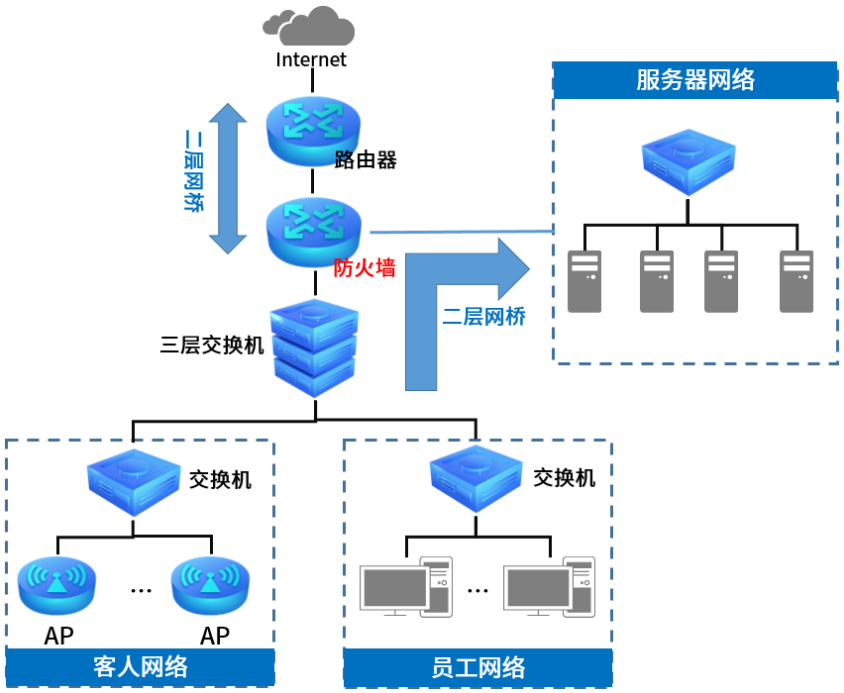
步骤 22/23/24/25/26 实现了审计需求：将防火墙的审计日志、系统日志、操作日志、流量日志、策略命中日志全部上传至安装了 TP-LINK 安全审计系统的审计服务器。

2.7 二层网桥组网配置实例

不改变原有网络结构使用二层网桥模式之后，原有网络中不同网段之间的数据转发还是依赖于网络中的路由器和三层交换机，但是只要数据流量经过防火墙的不同网络接口，就能够命中防火墙中的安全策略。

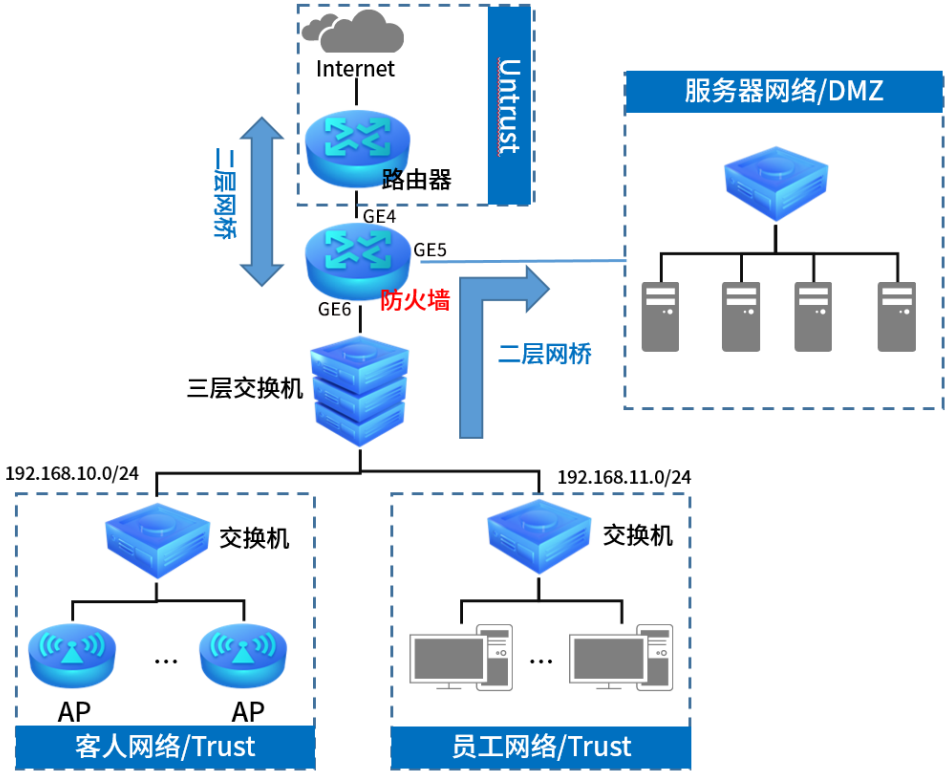
可以与路由模式共存在实际网络环境中，三层路由网关模式与二层透明网桥模式是可以共存的，我们可以将防火墙的部分接口设置成网桥模式，部分接口设置成路由模式，根据实际需求，选择最合适的组合，最大程度减少网络拓扑变化与配置工作量。

常用应用拓扑：



网络需求：

二层透明网桥下，防火墙在安全策略的设置上与三层路由网关模式一样，在 ***2.6 三层网关组网配置实例*** 中已经详细介绍，故这里只介绍二层透明网桥的基本设置，并以如下拓扑为例：



配置步骤：

1. 进入页面：网络 >> 接口设置 >> 网桥设置，点击<新增>，将需要用到的接口设置成网桥。

网桥名称：默认为 LAN，不可编辑；

包含接口：选择要设置成网桥的各个接口，本例中需要用到三个接口，故选择“GE4, GE5, GE6”。

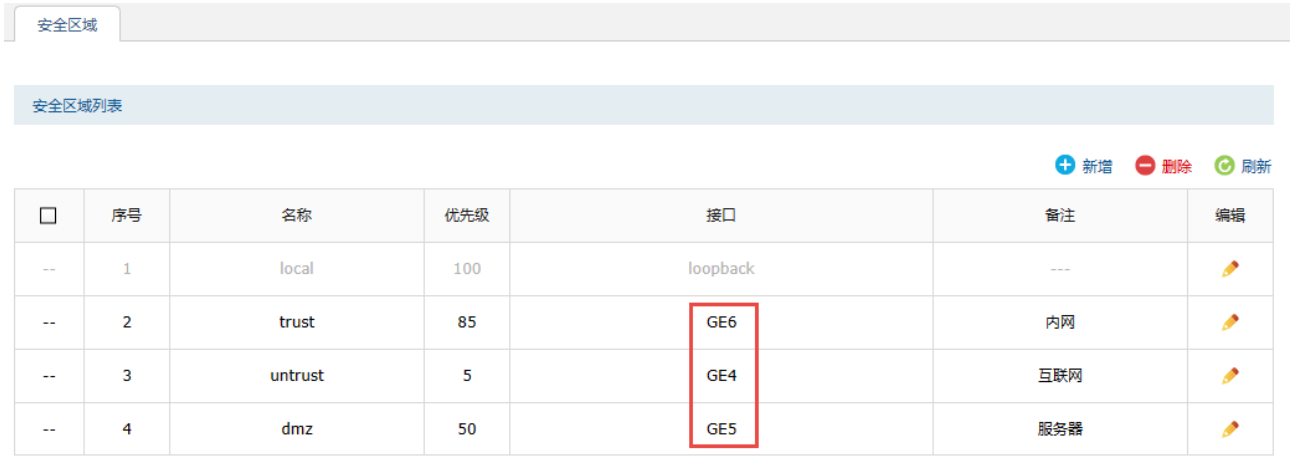
STP：生成树，本例中选择为“启用”。

注意：

- 防火墙只有在出厂状态下才能进行网桥设置，如果已经进行了其他配置，则此处不显示“新增”的按钮。

2. 进入页面：网络 >> 安全区域，可以看到系统默认有 4 个安全区域，其中三个可以编辑，如下图所示：

点击 将连接路由器的 GE4 划分至 untrust 区域，连接服务器的 GE5 添加到 dmz 区域，连接三层交换机的 GE6 划分至 trust 区域，如下图所示：



至此，就完成了防火墙作为二层透明网桥的基本设置。后面还需要进行的安全策略设置、审计策略设置等步骤，与三层路由网关模式一样，详情请参考 ***2.6 三层网关组网配置实例***。

回目录

第3章　监控管理

3.1　日志管理

增强级防火墙提供更加丰富的监控和审计功能，可以更好的记录展示设备信息、操作信息、安全策略信息及审计信息等，方便用户溯源查找。

日志管理中各图标说明：

：点击<内容>，可筛选表格中是否显示时间、功能模块、日志等级、日志内容。

日志等级描述：

所有等级	日志列表中将列出所有等级的日志记录。
调试信息	调试过程产生的信息。
信息报告	一般性的提示信息。
通知信息	正常状态下的重要提示信息。
警告信息	系统仍然正常运行，但可能存在隐患的提示信息，橙色显示。
一般错误	一般性的错误提示，橙色显示。
致命错误	导致系统不可用的错误，红色显示。
紧急错误	必须对其采取紧急措施的错误，红色显示。
严重错误	导致系统处于危险状态的错误，红色显示。

按键功能描述：

	点击<清空>，可清除系统日志列表中所有信息。
	点击<搜索>，可根据列名、内容和方式进行搜索。

列名	选择时间、功能模块、日志等级中的一个作为搜索关键列。

内容	输入需搜索的关键内容，该内容需与所选列名相关。
方式	在结果中搜索：在当前列表条目中搜索，通过该功能可实现多级搜索； 在所有条目中搜索：在所有列表条目中搜索。
搜索	点击搜索，搜索开始。
显示全部	显示全部列表内容。
返回	放弃本次搜索。

按键功能描述：

日志搜索	点击<日志搜索>，可搜索特定时间范围内，不同功能模块和不同日志等级的系统日志信息。

开始时间	设置开始时间。
结束时间	设置结束时间。
功能模块	选择认证、设备状态、网络等各种设备状态。
日志等级	选择日志等级。
搜索	点击搜索，搜索开始。
重置	恢复设置信息为默认。
返回	放弃本次搜索。

图标功能描述：

刷新	点击<刷新>，更新系统日志列表信息。
自动刷新	勾选<自动刷新>，自动更新系统日志列表信息。
导出日志	点击<导出日志>，设备将以 log 文件形式保存当前设备中最多 1000 条日志内容到本地。
	如对 web 页面参数有不清楚的地方，点击页面右上角问号可查找到更多信息。

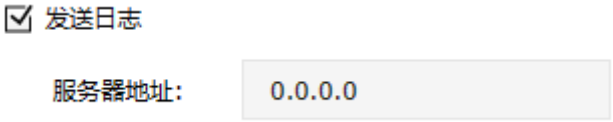
3.1.1 日志配置

进入页面的方法：系统 >> 日志配置

选中<选择系统日志等级>，将弹出系统日志等级复选框以供查看特定等级的系统日志信息。

选中<选择系统日志模块类别>，将弹出系统日志模块类别下拉框以供查看特定模块的系统日志信息。

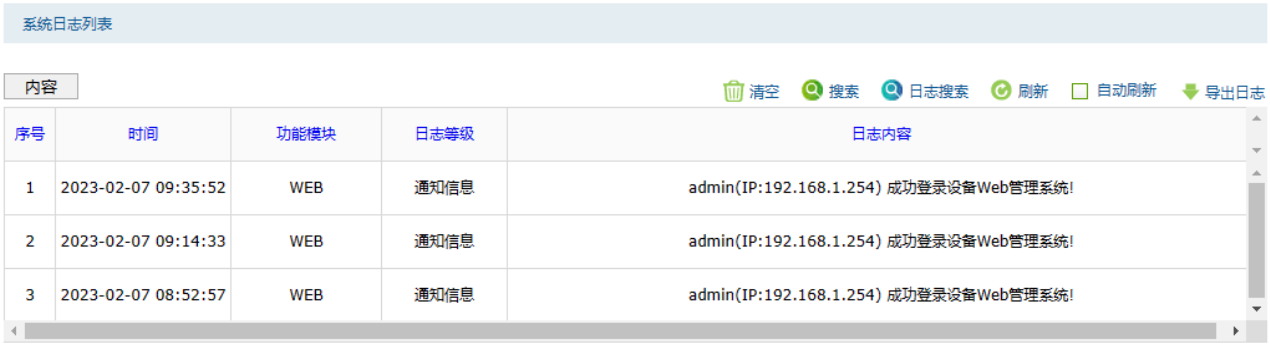
选中<发送日志>，可把日志发送到指定服务器。



3.1.2 系统日志

系统日志记录了系统运行状况，包含登录设备信息、DHCP 分配地址等。

进入页面的方法：监控 >> 日志 >> 系统日志



3.1.3 操作日志

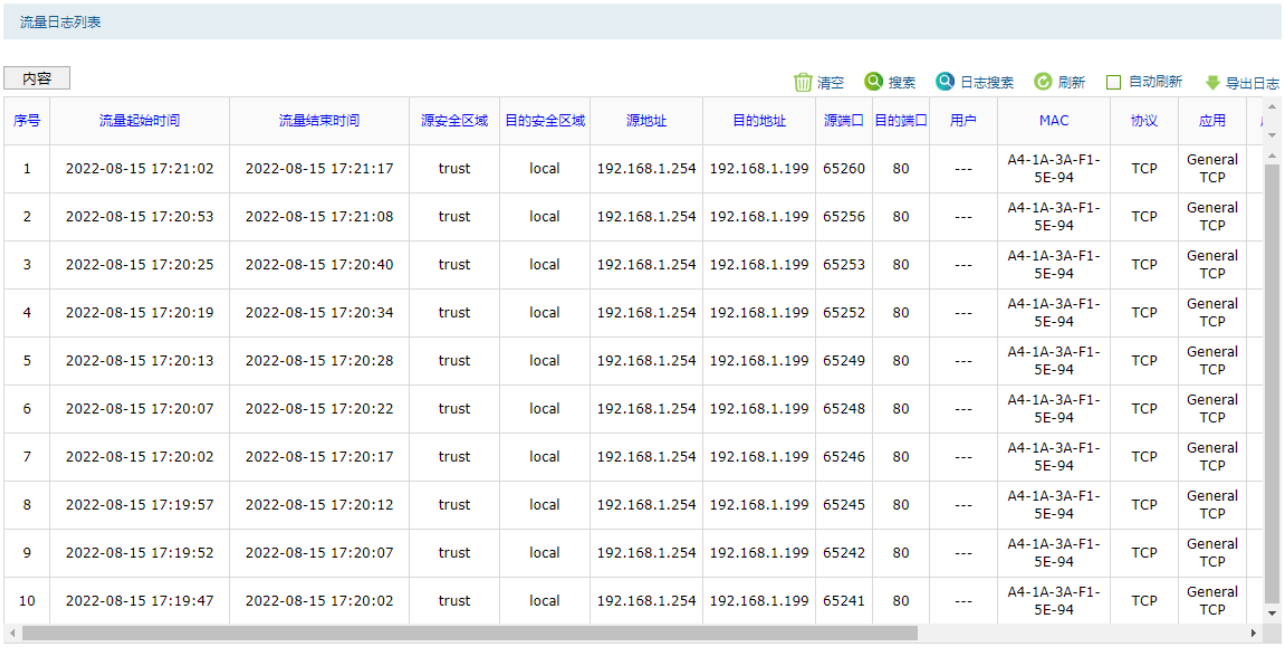
操作日志记录了安全策略、安全配置文件、管理员账号修改等安全相关的用户操作日志。

进入页面的方法：监控 >> 日志 >> 操作日志

3.1.4 流量日志

流量日志记录所有经过防火墙的流量信息，基于数据流进行详细展示。

进入页面的方法：监控 >> 日志 >> 流量日志



序号	流量起始时间	流量结束时间	源安全区域	目的安全区域	源地址	目的地址	源端口	目的端口	用户	MAC	协议	应用
1	2022-08-15 17:21:02	2022-08-15 17:21:17	trust	local	192.168.1.254	192.168.1.199	65260	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP
2	2022-08-15 17:20:53	2022-08-15 17:21:08	trust	local	192.168.1.254	192.168.1.199	65256	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP
3	2022-08-15 17:20:25	2022-08-15 17:20:40	trust	local	192.168.1.254	192.168.1.199	65253	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP
4	2022-08-15 17:20:19	2022-08-15 17:20:34	trust	local	192.168.1.254	192.168.1.199	65252	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP
5	2022-08-15 17:20:13	2022-08-15 17:20:28	trust	local	192.168.1.254	192.168.1.199	65249	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP
6	2022-08-15 17:20:07	2022-08-15 17:20:22	trust	local	192.168.1.254	192.168.1.199	65248	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP
7	2022-08-15 17:20:02	2022-08-15 17:20:17	trust	local	192.168.1.254	192.168.1.199	65246	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP
8	2022-08-15 17:19:57	2022-08-15 17:20:12	trust	local	192.168.1.254	192.168.1.199	65245	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP
9	2022-08-15 17:19:52	2022-08-15 17:20:07	trust	local	192.168.1.254	192.168.1.199	65242	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP
10	2022-08-15 17:19:47	2022-08-15 17:20:02	trust	local	192.168.1.254	192.168.1.199	65241	80	---	A4-1A-3A-F1-5E-94	TCP	General TCP

3.1.5 策略命中日志

策略命中日志记录了每一条数据流所匹配到的安全策略以及执行的动作，了解策略生效情况。

进入页面的方法：监控 >> 日志 >> 策略命中日志

3.1.6 威胁日志

威胁日志记录了入侵防御、恶意域名检查、反病毒相关拦截日志信息，确认当前网络是否收到安全威胁。

进入页面的方法：监控 >> 日志 >> 威胁日志

3.1.7 URL 日志

URL 日志记录了内容安全中 URL 过滤规则所产生的日志信息，包含放行或组织用户访问指定 URL 或网站。

进入页面的方法：监控 >> 日志 >> URL 日志

3.1.8 内容日志

内容日志记录了内容安全中文件过滤和应用行为控制规则所产生的日志信息，包含放行或阻止文件上传下载。

进入页面的方法：监控 >> 日志 >> 内容日志

3.1.9 邮件过滤日志

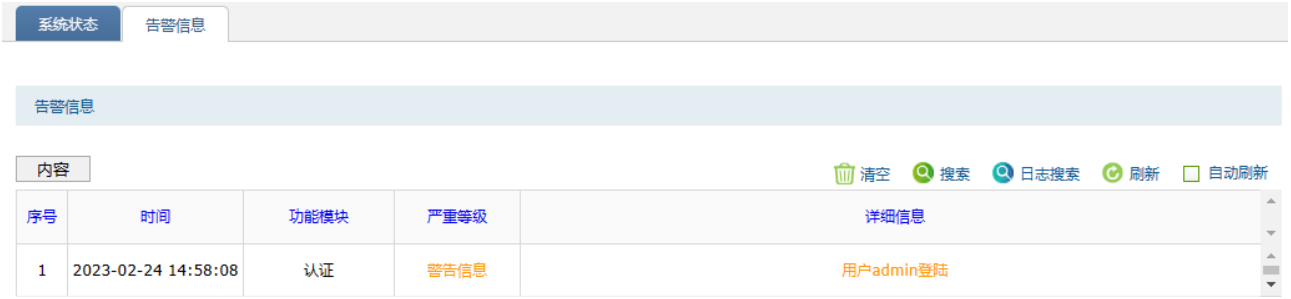
邮件过滤日志记录了内容安全中邮件过滤规则所产生的日志信息，包含执行动作、邮件协议和邮件收发人等。

进入页面的方法：监控 >> 日志 >> 邮件过滤日志

3.1.10 告警信息

进入页面的方法：面板 >> 系统状态 >> 告警信息

点击表头可切换告警信息排序方式。



3.1.11 告警事件配置

可配置设备告警功能。

进入页面的方法：系统 >> 告警配置 >> 事件配置

勾选<开启告警>，在<选择告警信息等级>复选框处选择上报/发送特定等级的告警信息，在<选择告警信息模块类别>复选框处选择上报/发送特定模块的告警信息。

3.1.12 告警邮件配置

可配置设备邮件告警功能。

进入页面的方法：系统 >> 告警配置 >> 邮件配置

选中<开启邮件告警>，将激活邮件相关配置项。

服务器地址	指定邮件发送所试用的 SMTP 服务器。
加密类型	STARTTLS——初始协商过程明文，其余均加密； SSL/TLS——全程加密。
端口号	指定发件过程与 SMTP 服务器通信的端口。
发件人	指定告警信息邮件的发件人地址。
收件人	指定告警信息邮件的收件人地址列表。
开启用户认证	选择是否开启用户认证，用于向 SMTP 服务器验证身份。
账号	当用户认证开启时，指定认证账号名。
密码	当用户认证开启时，指定认证账号对应的密码。
确认密码	请在此输入密码，确认所输密码准确性。

说明：

- 当前与 SMTP 服务器的连接均为加密连接，如遇第三方 SMTP 服务器不受信的情况，请至“对象 >> 证书”页面导入所需根证书。

邮件内容相关配置：

邮件主题　　指定告警信息邮件的主题。

发送间隔　　指定告警邮件之间的最小发送间隔。

邮件告警功能配置完成后，可点击<发送测试邮件>进行验证。

3.2　报表管理

3.2.1 流量报表

进入页面：监控 >> 报表 >> 流量报表，可查看上行/下行/总流量的统计图。

导出报表功能：

导出 PDF　　导出当前统计条件下的报表 PDF 文件。

导出 CSV　　导出当前统计条件下的报表 CSV 文件。

加载报表	加载当前报表页面。
时间	选择报表统计时间，可选择“过去 1 小时”、“过去 1 天”、“过去 1 周”、“过去 1 个月”、“自定义时间”，最长可选时间为 31 天。

3.2.2 策略命中报表

进入页面：监控 >> 报表 >> 策略命中报表，可查看命中不同安全策略的报表。

导出报表功能：

导出 PDF	导出当前统计条件下的报表 PDF 文件。
导出 CSV	导出当前统计条件下的报表 CSV 文件。
加载报表	加载当前报表页面。
时间	选择报表统计时间，可选择“过去 1 小时”、“过去 1 天”、“过去 1 周”、“过去 1 个月”、“自定义时间”，最长可选时间为 31 天。

3.2.3 威胁报表

进入页面：监控 >> 报表 >> 威胁报表，可查看设备中存储的威胁报表。

导出报表功能：

导出 PDF	导出当前统计条件下的报表 PDF 文件。
导出 CSV	导出当前统计条件下的报表 CSV 文件。
加载报表	加载当前报表页面。
时间	选择报表统计时间，可选择“过去 1 小时”、“过去 1 天”、“过去 1 周”、“过去 1 个月”、“自定义时间”，最长可选时间为 31 天。

3.3 系统统计

在流量统计列表中，点击表头中的文字，可以对该列进行升序/降序排序。

系统统计页面各图标说明：

清空	点击<清空>，可清除系统统计列表中所有信息。
搜索	点击<搜索>，可根据列名、内容和方式进行搜索。
刷新	点击<刷新>，更新系统统计列表信息。
自动刷新	勾选<自动刷新>，自动更新系统统计列表信息。

如对 web 页面参数有不清楚的地方，点击页面右上角问号可查找到更多信息。

列名	选择接口或 IP 地址作为搜索关键列。
内容	输入需搜索的关键内容，该内容需与所选列名相关。
方式	在结果中搜索：在当前列表条目中搜索，通过该功能可实现多级搜索； 在所有条目中搜索：在所有列表条目中搜索。
搜索	点击搜索，搜索开始。
显示全部	显示全部列表内容。
返回	放弃本次搜索。

3.3.1 接口流量统计

接口流量界面显示防火墙所有正在工作的接口的数据接收/发送速率。

进入页面的方法：监控 >> 系统统计 >> 接口流量统计

接口	发送速率(KB/s)	接收速率(KB/s)	发送包速率(Pkt/s)	接收包速率(Pkt/s)	发送总字节	接收总字节	发送总报文	接收总报文
10GE1	0	0	0	0	---	---	---	---
10GE2	0	0	0	0	---	---	---	---
10GE3	0	0	0	0	---	---	---	---
10GE4	0	0	0	0	---	---	---	---
GE1	0	0	0	0	---	---	---	---

点击<导出 pdf>，可将流量统计列表导出为 pdf 文档。

3.3.2 IP 流量统计

IP 流量统计界面显示指定 IP 范围之间各个 IP 的即时流量信息。

进入页面的方法：监控 >> 系统统计 >> IP 流量统计

勾选<启用 IP 流量统计>，设置监控 IP 范围，点击<设置>，配置生效。

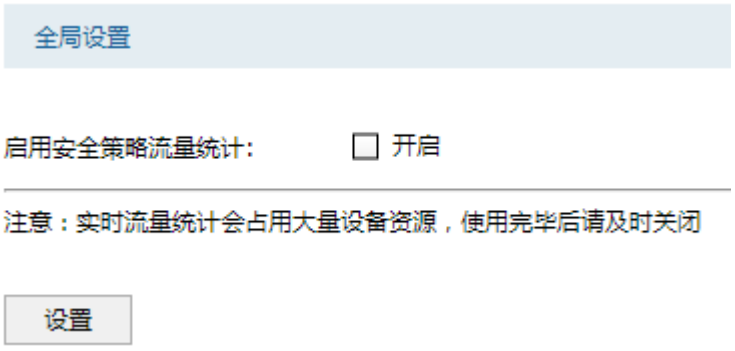
点击<导出 pdf>可将设备 IP 流量统计以 PDF 形式下载到本地。

3.3.3 安全策略流量统计

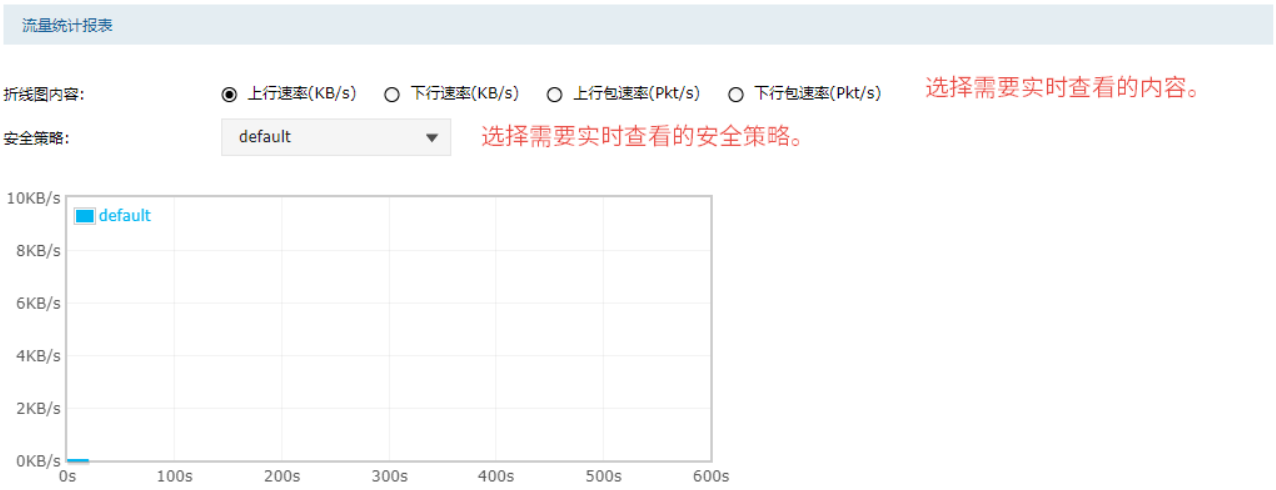
安全策略流量统计界面能够根据安全策略显示发送速率、接受速率、发送数据包、接收数据包的折线图，在流量统计列表中，能够显示匹配到各个安全策略的流量信息统计。

进入页面：监控 >> 系统统计 >> 安全策略流量统计，可查看设备中安全策略的流量统计列表。

勾选<开启>，启用安全策略流量统计，点击<设置>使配置生效。



可查看流量统计报表和流量统计列表。



流量统计列表

清空 搜索 刷新 自动刷新

安全策略	上行速率(KB/s)	下行速率(KB/s)	上行包速率(Pkt/s)	下行包速率(Pkt/s)	上行总字节	下行总字节	上行总报文	下行总报文
default	0	0	1	0	299	---	1	---

注意：

- 实时流量统计会占用大量设备资源，使用完毕后请及时关闭。

回目录

第4章　网络

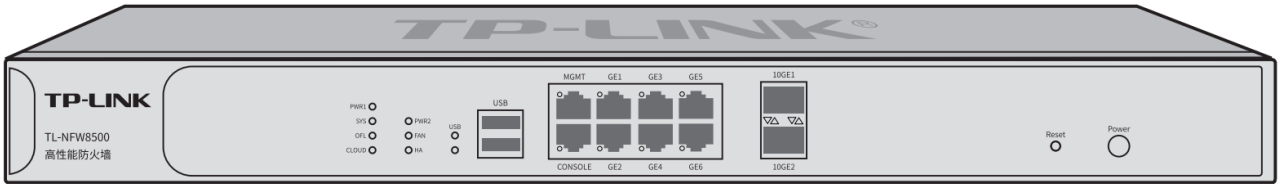
4.1　接口模式

为理解防火墙接口的含义，下面分别介绍物理接口和接口的概念：

➢ **物理接口**

物理接口是设备上实际存在的组件，接口命名约定因设备而异。物理接口的名称由媒体类型、插槽号（对于某些设备）及索引号组成，例如：ethernet3/2 或 ethernet2。

TL-NFW8500 的物理接口命名为端口 MGMT/GE1/GE2/GE3/GE4/GE5/GE6，只支持以太网这一种媒体类型，如下图所示。



➢ **接口**

在支持 VLAN（Virtual Local Area Network，虚拟局域网）的设备上，可以在逻辑上将一个物理接口划分为多个虚拟的接口，每个接口使用的带宽都来自它所属的物理接口。

TL-NFW8500 用来划分物理接口的接口有 Ethernet、PPPoE 两种类型。Ethernet 是以太网接口，功能上与以太网物理接口相同。Ethernet 接口由 802.1Q VLAN 标记进行区分，PPPoE 由相关的协议字段进行区分。

- Ethernet 接口：以太网接口，必须与一个 VLAN 和一个 MAC 地址相对应。提供静态 IP 与 DHCP 两种连接方式。一般光纤接入以及企业、网吧局域网内组网适用静态 IP 连接方式，有线宽频适用 DHCP 连接方式。
- PPPoE 接口：提供 PPPoE 连接方式的接口。xDSL 拨号上网使用 PPPoE 连接方式。新建 PPPoE 接口时，必须保证在同一物理接口下有 Ethernet 接口可供选择。

说明：

静态IP、DHCP和PPPoE三种接入方式都可以连接到广域网，具体使用情况请根据ISP（Internet Service Provider，网络服务提供商）提供的服务进行选择。

4.1.1 接口设置

在本页面可选择在不同的物理接口下创建不同的 Ethernet 接口和 PPPoE 接口。

进入页面的方法：网络 >> 接口设置 >> 接口设置

在接口设置页面中，选择物理接口作为关联接口，点击<新增>，可新建 Ethernet 或 PPPoE 接口。

- **Ethernet 接口**

Ethernet 接口有两种连接方式：静态 IP 连接方式和 DHCP 连接方式。

接口类型	选择 Ethernet 接口类型。
接口名称	设置一个名称来标识一个接口。只能输入英文、数字和下划线，且不能以数字开头。
关联接口	指定关联的物理接口。
关联 VLAN	输入一个该接口属于的 VLAN ID，当勾选“UNTAG”时，从该接口发出的报文不带 VLAN TAG；当不勾选“UNTAG”时，从该接口发出的报文带有 VLAN TAG。
连接方式	可以选择静态 IP 和 DHCP 自动分配两种连接方式。选择静态 IP 连接方式，需要手动配置 IP；选择 DHCP 方式时，由设备动态获取 IP。
IP 地址	接口的 IP 地址。
子网掩码	设置接口的子网掩码。
网关地址	设置网关地址。该项为可选项，允许留空。
上/下行带宽	设置接口的上/下行带宽。取值范围为 100-1000000Kbps，默认为 1000000Kbps。
MTU	MTU 即 Maximum Transmission Unit，最大传输单元。设置数据包的罪罚长度，取值范围为 576-1500，默认值为 1500。
首选/备选 DNS 服务器	DNS 即 Domain Name Server，域名解析服务器。设置首选/备选的 DNS 服务器，允许留空。
备注	可选填接口的备注信息。
管理接口开启	勾选该项使得该接口成为管理接口。

- **PPPoE 接口**

接口类型	选择 PPPoE 接口。
接口名称	设置一个名称来标识一个接口，仅可以使用英文、数字和下划线来命名，且不能以数字开头。
关联接口	指定关联的 Ethernet 接口。
用户名	PPPoE 拨号的用户名，由 ISP 提供。
密码	PPPoE 拨号的密码，由 ISP 提供。
连接方式	选择上网时连入互联网的方式，由自动连接、手动连接、定时连接三种方式选择。 自动连接：设备上电完成后，将自动拨号连入互联网。适合不限时的包月计费的用户。 手动连接：需要手动拨号连入互联网，适合按小时计费的拨号连接上网方式。 定时连接：在时间下拉列表中选择时间对象，适合于需要限时上网的场景。如需新建时间对象，请前往“对象 >> 时间段”页面。

时间	当连接方式选择为定时连接时，可以在下拉列表中选择合适的时间对象来进行拨号。
上/下行带宽	设置接口的上/下行带宽。取值范围为 100-1000000Kbps，默认为 1000000Kbps。
MTU	MTU 即 Maximum Transmission Unit，最大传输单元。设置数据包的罪罚长度，取值范围为 576-1500，默认值为 1500。
服务名	输入服务名称，由 ISP 提供。
首选/备选 DNS 服务器	DNS 即 Domain Name Server，域名解析服务器。设置首选/备选的 DNS 服务器，允许留空。
备注	可选填接口的备注信息。
管理接口开启	勾选该项使得该接口成为管理接口。

可以通过 IP 协议类型切换至 IPv6 协议。具体配置请参考 *2.5 IPv6 上网配置*。

4.1.2 网桥设置

通过创建网桥接口，可以将多个物理接口级联在一起（其中默认管理接口将会默认被包含），达到不同接口之间互通的目的。当前系统的网桥接口将作为“LAN”接口使用。而被桥接的接口配置其他任何业务都将无效。

进入页面的方法：网络 >> 接口设置 >> 网桥设置

点击<新增>，配置网桥。

包含接口	配置网桥包含接口。配置网桥接口后会将包含的物理接口级联在一起，达到不同接口之间胡同的目的，同时被桥接的接口单独配置其他任何业务都将无效。

STP	勾选以启用生成树协议。
接口	所有接口上已配置的功能列表。

说明：

设备需要在出厂设置状态下才能进行网桥接口配置，如需创建网桥，请先恢复出厂设置。

4.1.3 SFP+设置

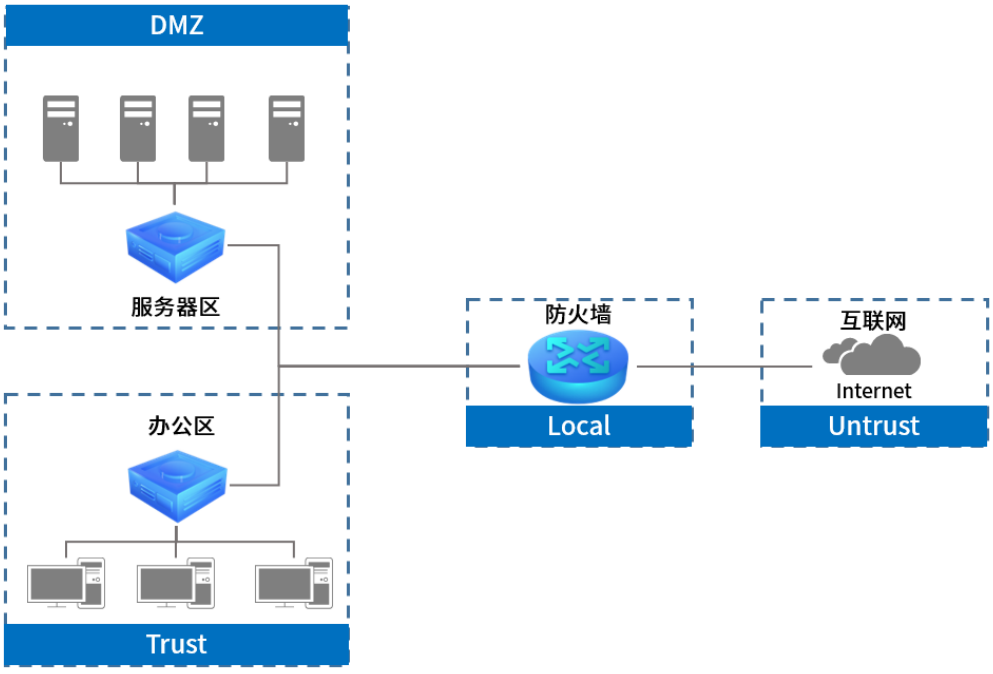
对于支持 SFP+口的防火墙，可进行 SFP+口配置。

注意：

- 切换 SFP+口速率，需要再重启后才会生效。

4.2 安全区域

防火墙构建了非常有效的网络安全模式，将整个网络划分为四个安全区域。分别是 Trust、DMZ、Untrust 以及 Local，工作模型如下：



- **Turst 区域**

可信任区域，主要用于连接局域网内部网络。比如企业网络中，通常将员工网络设置为 Trust 区域。

- **Untust 区域**

非信任区域，主要用于连接互联网。大部分情况下，非信任区域无法主动访问可信任区域。

- **DMZ 区域**

非军事化区域，作为非信任区域和信任区域之间的缓冲区。一般用于放置企业内部服务器，如：OA 服务器、邮件服务器等。

- **Local 区域**

防火墙本身，凡是防火墙主动发出的报文，均可认为是从 Local 区域发出的。

进入页面的方法：网络 >> 安全区域 >> 安全区域

□	序号	名称	优先级	接口	备注	编辑
--	1	local	100	loopback	---	
--	2	trust	85	MGMT	---	
--	3	untrust	5	---	---	
--	4	dmz	50	---	---	

点击<新增>，添加安全区域规则。点击<确定>保存配置。

名称　　标志防火墙安全区域的名称。

优先级　　防火墙安全区域的优先级，数字越大表示优先级越高。

备注　　防火墙安全区域包含的接口。

接口　　可以设置防火墙安全区域的备注，以方便管理和查找。备注最多支持 50 个字符。

点击<删除>，可批量删除安全区域规则。

点击< 刷新>，更新安全区域列表。

说明：

- 防火墙安全区域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。
- 防火墙安全区域可以为空(即不选择任何接口)，引用该防火墙安全区域的规则不会被命中。

4.3 DHCP 服务

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）协议应用于 TCP/IP 网络中，基于该协议标准，DHCP 服务器给网络中的 DHCP 客户端动态分配 IP 地址等网络参数，以便于网络管理员对网络中计算机的 TCP/IP 参数进行统一管理。

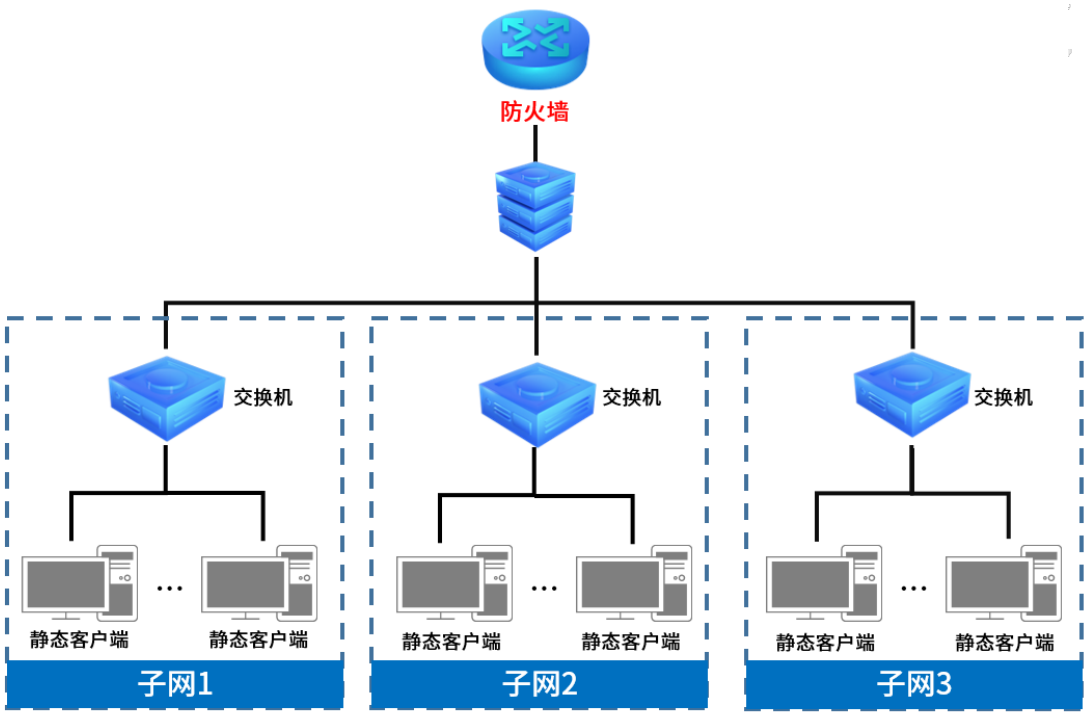
当网络规模扩大，计算机数量日益增多时，DHCP 功能能够高效的完成 TCP/IP 参数配置，并将 IP 地址循环运用，提高使用效率。而随着无线网络的广泛使用，计算机的位置也经常变化，其所连接的子网也处于动态变化的过程，由此产生的 TCP/IP 参数变更问题基于 DHCP 也能够高效解决。

DHCP 服务器可以在下列场景中高效完成网络设备的 IP 地址配置工作：

1) 网络规模大，为每台网络设备手工配置网络参数的工作量较大，且不便于对网络进行集中管理。

2) 网络中设备数目大于该网络支持的设备数量，相应的 IP 资源不足。例如，ISP 限制同时接入网络的用户数目，而网络中的设备并不需要同时访问网络，则用户可以动态按需获得网络 IP。

3) 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

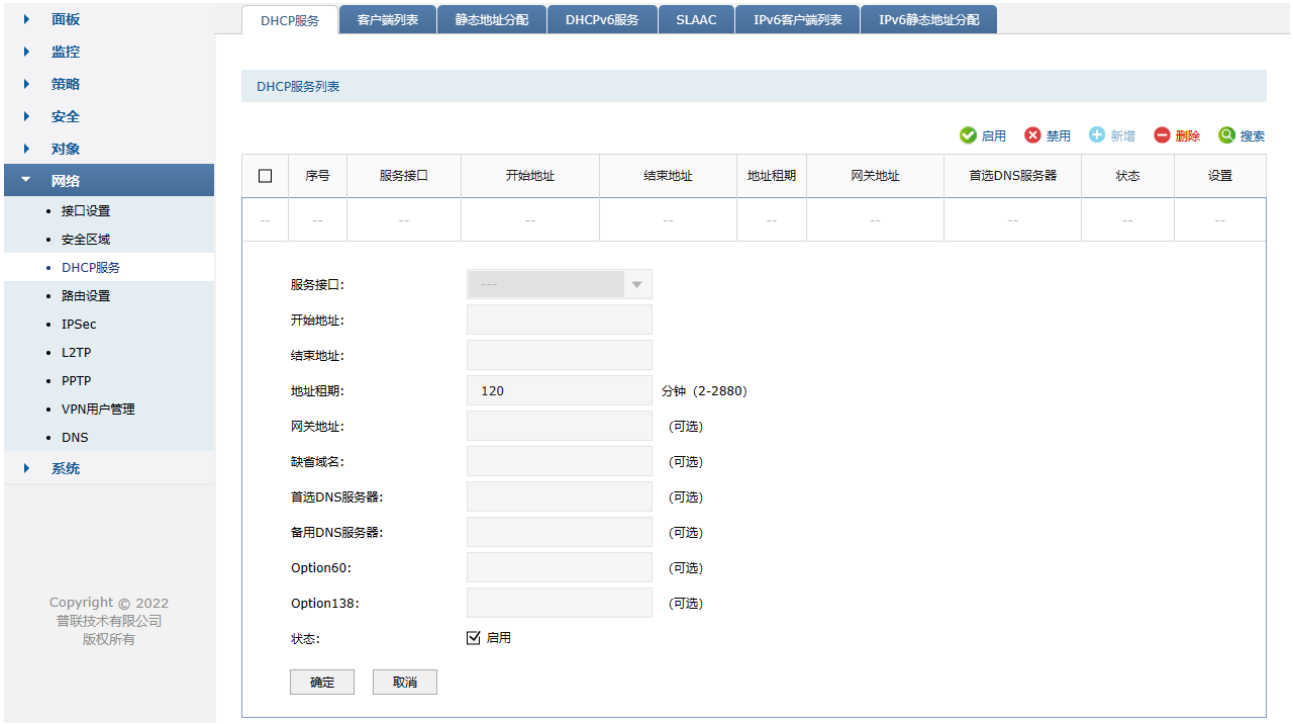


4.3.1 DHCP 服务

可查看 DHCP 服务的相关信息，还可以通过表格按钮进行相关操作。

进入页面的方法：网络 >> DHCP 服务 >> DHCP 服务

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮禁用条目，点击<>按钮删除条目。



服务接口	选择需要提供 DHCP 服务的 Ethernet 接口。
开始/结束地址	设置 IP 地址池，DHCP 服务器开启状态下，防火墙自动从地址池（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。
地址租期	DHCP 服务器所分配 IP 地址的有效使用时间，超时将重新分配。
网关地址	输入此地址给客户端分配的默认网关，建议填入当前 DHCP 服务生效接口的 IP 地址。
缺省域名	输入此地址池给客户指定的域，与 IP 地址一样共同表示相同子网的计算机集合，同一接口网络中的计算机通常配置为相同的域名。
首选/备用 DNS 服务器	输入此地址池给客户端分配的首选/备用 DNS 服务器，也可以将接口 IP 地址配置为 DNS 服务器地址，并由接口为客户端转发域名解析请求。
Option60	可选项，请填入厂商信息。具体厂商信息请咨询相关厂商，例如 TP-LINK 的厂商信息为 TP-LINK。
Option138	可选项，请填入 AC（无线控制器）IP 地址。

点击页面，查看更多页面设置参数信息。

注意：

DHCP 服务的服务接口 IP 和开始/结束地址池必须在同一网段，否则 DHCP 服务不生效。

4.3.2 DHCPv6 服务

当防火墙开启了 IPv6 功能，可开启 DHCPv6 服务。可查看 DHCPv6 服务的相关信息，还可以通过表格按钮进行相关操作。

进入页面的方法：网络 >> DHCP 服务 >> DHCPv6 服务

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮禁用条目，点击<>按钮删除条目。

服务接口	选择需要提供 DHCPv6 服务的 Ethernet 接口。
开始/结束地址	设置 IP 地址池，DHCP 服务器开启状态下，防火墙自动从地址池中给局域网中的设备分配 IPv6 地址。
地址租期	DHCP 服务器所分配 IP 地址的有效使用时间，超时将重新分配。
首选/备用 DNS 服务器	输入此地址池给客户端分配的首选/备用 DNS 服务器，也可以将接口 IPv6 地址配置为 DNS 服务器地址，并由接口为客户端转发域名解析请求。
Option16	可选项，请填入厂商信息。具体厂商信息请咨询相关厂商，例如 TP-LINK 的厂商信息为 TP-LINK。
Option52	可选项，请填入 AC（无线控制器）IP 地址。

点击页面，查看更多页面设置参数信息。

注意：

DHCPv6 服务的服务接口 IPv6 和开始/结束地址池必须在同一网段，否则 DHCPv6 服务不生效。

4.4 客户端列表

4.4.1 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。

进入页面的方法：网络 >> DHCP 服务 >> 客户端列表

点击<刷新>，可获取最新列表信息。

服务接口	客户端主机所属的服务接口。
主机名	通过 DHCP 获得 IP 地址的主机的名称，可用于识别不同的接入设备。
MAC 地址	分配到 IP 的客户端主机的 MAC 地址。
IP 地址	DHCP 服务器分配给客户端主机的 IP 地址。
剩余租期	DHCP 服务器所分配 IP 地址的剩余有效使用时间，超时将重新分配。

4.4.2 IPv6 客户端列表

IPv6 客户端列表显示已由 DHCP 分配 IPv6 参数的主机信息。

进入页面的方法：网络 >> DHCP 服务 >> IPv6 客户端列表

点击<刷新>，可获取最新列表信息。

服务接口	客户端主机所属的服务接口。
主机名	通过 DHCPv6 获得 IP 地址的主机的名称，可用于识别不同的接入设备。
MAC 地址	分配到 IPv6 的客户端主机的 MAC 地址。

IP 地址	DHCPv6 服务器分配给客户端主机的 IP 地址。
剩余租期	DHCPv6 服务器所分配 IPv6 地址的剩余有效使用时间，超时将重新分配。

4.5 静态地址分配

4.5.1 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。

进入页面的方法：网络 >> DHCP 服务 >> 静态地址分配

点击<新增>，输入对应的 MAC 地址和 IP 地址，点击<确定>。

MAC 地址	预留 IP 地址的主机 MAC 地址。
IP 地址	为指定主机预留的 IP 地址。
备注	可以设置静态地址分配条目备注，以方便您管理和查找。备注最多支持 32 个字符。
状态	可以通过启用/禁用来选择是否使该条目生效。

4.5.2 IPv6 静态地址分配

可根据接入设备的 MAC 地址手动分配 IPv6 地址。当对应的客户端设备请求 DHCP 服务器分配 IPv6 地址时， DHCP 服务器将自动为其分配指定的 IPv6 地址。

进入页面的方法：网络 >> DHCP 服务 >> 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<确定>。

MAC 地址	预留 IPv6 地址的主机 MAC 地址。
IP 地址	为指定主机预留的 IPv6 地址。
备注	可以设置静态地址分配条目备注，以方便您管理和查找。备注最多支持 32 个字符。
状态	可以通过启用/禁用来选择是否使该条目生效。
导入	点击<导入>按钮导入多个静态地址条目。可以通过备份功能获取符合规则的 CSV 文件，以查看文件的正确格式。 文件格式示例（必须包含首行提示栏）： 状态，MAC 地址，IP 地址，备注 1，XX-XX-XX-XX-XX-XX，2000:1:2:3:4:5:6:7，TP-LINK
备份	点击<备份>按钮备份所有静态地址条目。备份文件可直接通过“导入”功能重新添加到静态地址列表中。

4.6 SLAAC

SLAAC（Stateless Address Autoconfiguration），无状态地址自动配置，防火墙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。

进入页面的方法：网络 >>DHCP 服务 >> SLAAC

开启服务接口，选择 DNS 配置方式。配置完成后，点击<保存>。

说明：

请在接口设置中开启IPv6功能。

4.7 DNS 设置

DNS（Domain Name System，域名解析系统），是应用 UDP 协议工作，使用 UDP 53 端口进行通信，将指定域名解析为 IP 的过程。

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。

路由器作为动态 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。TP-LINK 防火墙支持花生壳动态域名、科迈动态域名和 3322 动态域名。

4.7.1 DNS 代理

可进行 DNS 代理设置。

进入页面的方法：网络 >> DNS >> DNS 代理

点击<新增>添加 DNS 代理规则。

规则名称　　为 DNS 代理条目设置规则名称。

服务接口　　配置 DNS 代理条目的接口。

出接口　　配置 DNS 代理条目的 Ethernet 接口，也可以选择自动（auto）。

4.7.2 花生壳动态域名

可通过本页面登录花生壳动态域名服务器，开启花生壳动态域名服务。

进入页面的方法：网络 >> DNS 设置 >> 花生壳动态域名

点击<新增>，添加花生壳动态域名服务。

服务接口　　花生壳动态域名服务生效的接口。

用户名　　花生壳动态域名服务账户的用户名。

密码　　花生壳动态域名服务账户的密码。

启用/禁用	选择是否在添加该账户后立即登录花生壳动态域名服务器，开启动态域名服务。
域名	从 DDNS 服务器获取的域名服务列表，最多可以显示 16 条域名信息。

4.7.3 科迈动态域名

可通过本页面登录科迈动态域名服务器，开启花生壳动态域名服务。

进入页面的方法：网络 >> DNS 设置 >> 科迈动态域名

点击<新增>，添加科迈动态域名服务。

服务接口	科迈动态域名服务生效的接口。
用户名	科迈动态域名服务账户的用户名。
密码	科迈动态域名服务账户的密码。
启用/禁用	选择是否在添加该账户后立即登录科迈动态域名服务器，开启动态域名服务。
域名	从 DDNS 服务器获取的域名服务列表，最多可以显示 16 条域名信息。

4.7.4 3322 动态域名

可通过本页面登录 3322 动态域名服务器，开启 3322 动态域名服务。

进入页面的方法：网络 >> DNS 设置 >> 3322 动态域名

点击<新增>，添加 3322 动态域名服务。

服务接口	3322 动态域名服务生效的接口。
用户名	3322 动态域名服务账户的用户名。
密码	3322 动态域名服务账户的密码。
启用/禁用	选择是否在添加该账户后立即登录 3322 动态域名服务器，开启动态域名服务。
域名	从 DDNS 服务器获取的域名服务列表，最多可以显示 16 条域名信息。

4.7.5 DDNS 配置实例

需求介绍：某企业使用防火墙，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。防火墙是宽带拨号上网，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，将端口 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端口 IP。

设置方法：

- **花生壳/科迈动态域名**

进入页面：网络 >> DNS >> 花生壳动态域名/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

进入页面：网络 >> DNS >> 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。

回目录

第5章　安全防护

5.1　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，包括防火墙和计算机在内，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。

5.1.1 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。

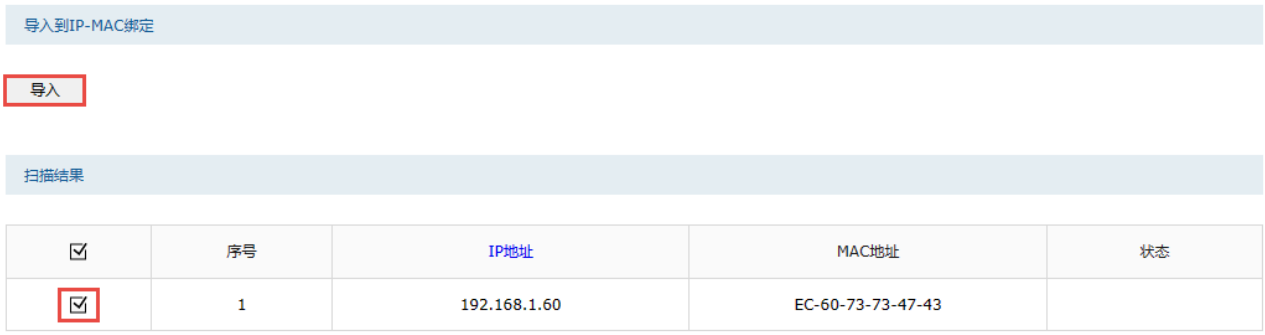
- **配置方法**

进入页面：安全 >> 安全防护

- **扫描绑定**

进入页面：安全 >> 安全防护 >> ARP 扫描，输入扫描的 IP 地址范围，点击<开始扫描>，防火墙会对该范围的 IP 地址进行 ARP 查询。

扫描结束后，扫描得到的结果会出现在扫描结果列表中。勾选扫描结果，点击<导入>，将扫描结果自动导入到 IP-MAC 绑定。



进入页面：安全 >> 安全防护 >> IP-MAC 绑定，可在 IP-MAC 绑定列表中查看绑定结果。

点击<>，可编辑该 IP-MAC 绑定规则的 IP 地址、MAC 地址、生效域及状态等信息。

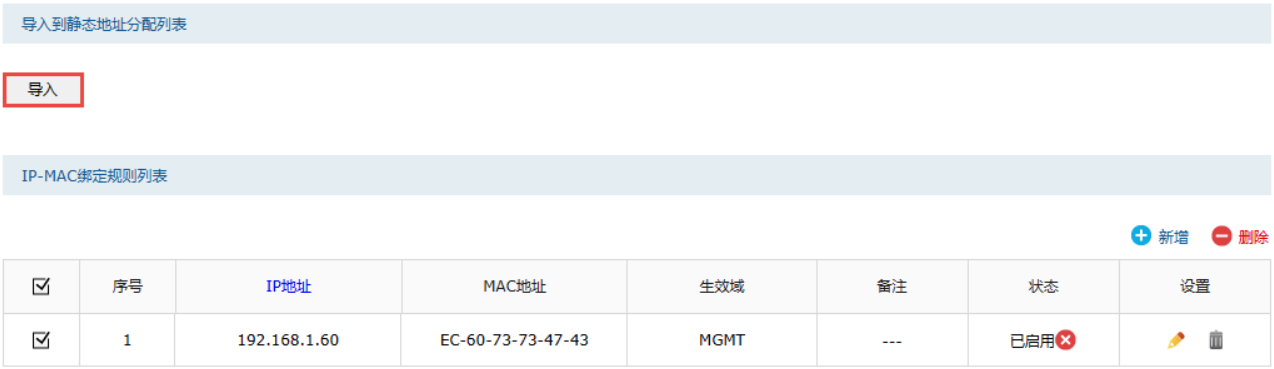
- **手动绑定**

进入页面：安全 >> 安全防护 >> IP-MAC 绑定，进入 IP-MAC 绑定规则列表，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	选择 IP-MAC 绑定规则生效的接口。

点击页面，查看更多页面设置参数信息。

选择多条 IP-MAC 绑定列表中的条目，点击<导入>按钮，可一次将多个条目导入到 DHCP 静态地址分配列表中。



5.1.2 ARP 防护

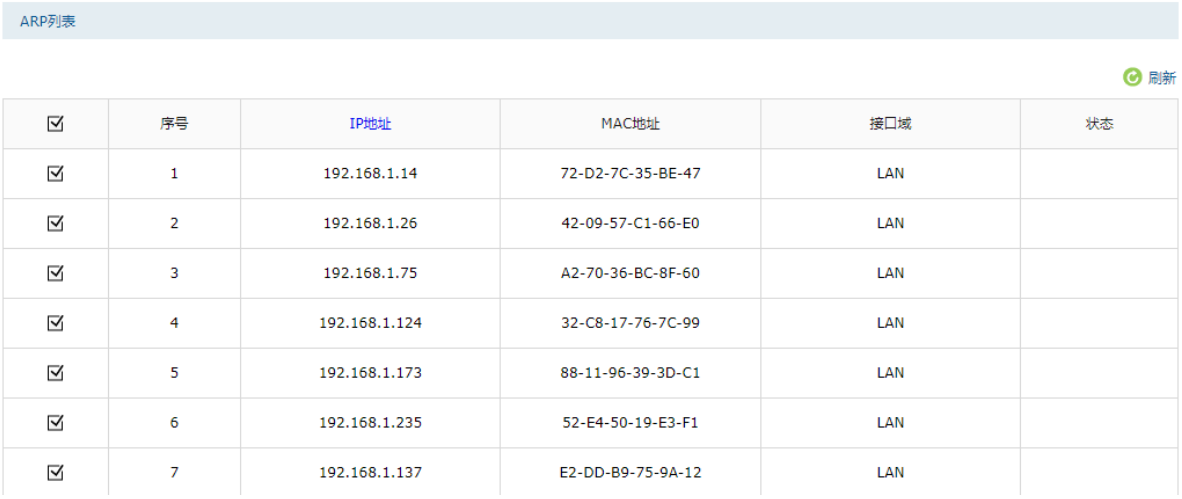
进入页面：安全 >> 安全防护 >> IP-MAC 绑定，在全局设置模块，勾选“启用 ARP 防欺骗功能 ，选择生效域（ARP 防欺骗功能所生效的接口）。若关闭该功能，禁止非 IP-MAC 绑定的数据包通过和发送 GARP 功能等功能都不会生效。

仅允许 IP-MAC 绑定的数据包通过	勾选该后，则防火墙只会放过在 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。

允许防火墙在发现 ARP 攻击时发送 GARP 包	勾选并设置发包间隔，防火墙收到与 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。

5.1.3 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<导入>，一次性添加到 IP-MAC 绑定列表中。

5.1.4 ARP 防护配置实例

ARP 是 IP 与 MAC 地址的解析协议，对网络通信至关重要。一般情况下，上网数据直接在主机和网关之间进行交互，ARP 欺骗主要针对网关和主机的 ARP 列表进行欺骗，导致通信异常。常见的 ARP 欺骗软件有“网络执法官”、“P2P 终结者”、“QQ 第六感”等。那么 ARP 防护就需要从两个方面着手，在网关上绑定主机的 ARP 信息，在主机上绑定网关的 ARP 信息，从而实现双向绑定，确保网络安全。

- **需求介绍**

某企业希望通过 TP-LINK 防火墙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。

- **设置方法**

1. 手动指定绑定电脑的 IP 地址

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，如下表所示：

使用人	IP 地址	MAC 地址	备注
张三	192.168.32.100	8C-16-45-9F-5B-B0	办公电脑
…	…	…	…

以上表格仅为示意，具体信息请根据实际需要记录。

2. 在防火墙上添加绑定条目

可采用手动添加或扫描添加两种方式。

- **手动添加**

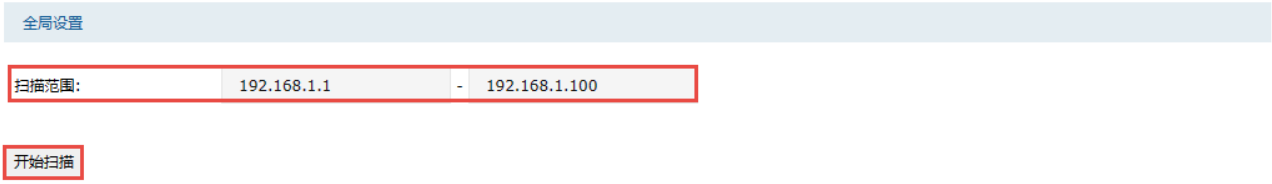
手动添加操作复杂，但是安全性高。在网络中已经存在 ARP 欺骗或者不确定网络中是否存在 ARP 欺骗的情况下，建议使用手动添加的方式。

进入页面：安全 >> 安全防护 >> IP-MAC 绑定，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：

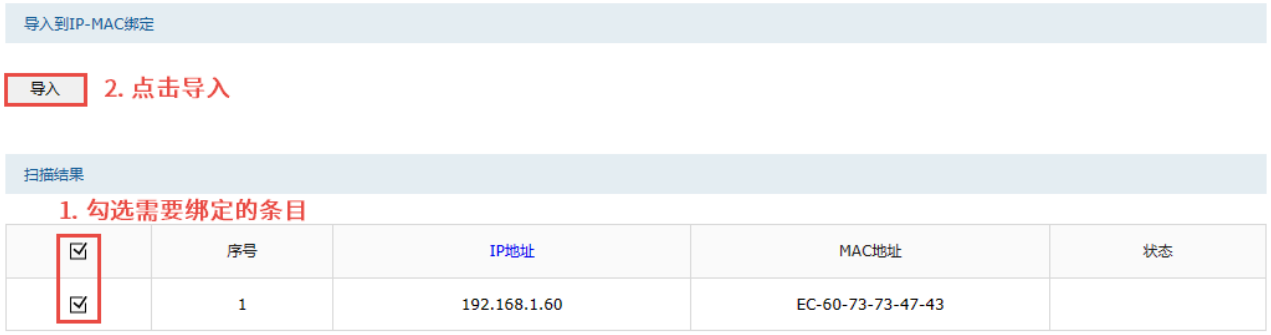
- **扫描添加**

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。

1. 进入页面：安全 >> 安全防护 >> ARP 扫描，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，防火墙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：



2. 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。

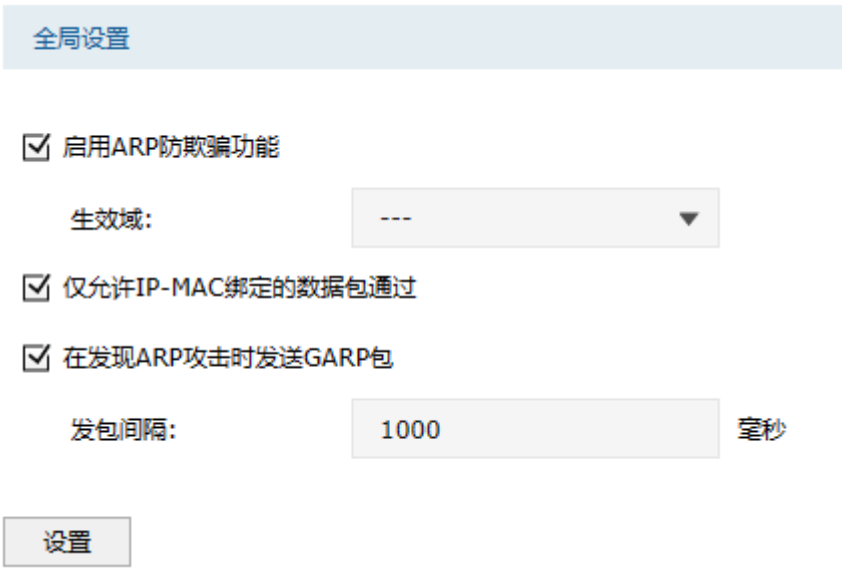


说明：

- 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，进入页面：安全 >> 安全防护 >> IP-MAC 绑定，确认已勾选“启用 ARP 防欺骗功能”，点击<设置>。如下图所示：



说明：

- 如果勾选“禁止非 IP-MAC 绑定的数据包通过防火墙”，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防火墙。

至此，防止 ARP 欺骗设置完成。

4. 电脑绑定防火墙 ARP 信息

仅在防火墙上绑定主机的 MAC 地址并不能完全解决 ARP 欺骗的问题，在主机上绑定防火墙的 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：

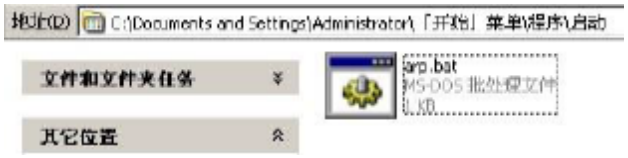
- **Windows XP 系统：**

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 是防火墙的管理地址（格式：192.168.1.1），MAC 是防火墙接口的 MAC 地址（格式：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。

5.2 MAC 地址过滤

5.2.1 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>> 安全防护 >> MAC 过滤，勾选“启用 MAC 地址过滤功能 ，选择规则类型及生效接口域，点击<设置>。

生效域

举例：禁止 LAN 网段上 MAC 地址为 00-00-11-11-11-F2 的主机访问外网。

1. 点击<增加>添加 MAC 地址为 00-00-11-11-11-F2 的 MAC 过滤规则条目。
2. 启用 MAC 地址过滤功能。
3. 选择仅禁止规则列表的 MAC 地址访问外网。

在 MAC 过滤规则列表模块，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>。

5.2.2 MAC 地址过滤配置实例

➢ **需求介绍**

某企业希望通过防火墙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 >> 安全防护 >> MAC 过滤，启用“MAC 地址过滤功能”，选择对应的规则类型，点击<设置>。

2. 添加 MAC 地址

进入页面：安全 >> 安全防护 >> MAC 过滤，点击<新增>，添加受控电脑的 MAC 地址。

上述设置完成后，只有规则列表中 MAC 地址的电脑如“zhangsan”才能上网，列表外的均无法上网。

说明：

- 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“仅禁止规则列表内的 MAC 地址访问外网”。

5.3 攻击防护

攻击防护可防止广域网对防火墙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：安全 >> 安全防护 >> 攻击防护，可设置攻击防护相关参数。

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，让目的防火墙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。

5.4 黑名单

查看手动和自动添加的黑名单项目，并管理它们。根据类型设置，来自或前往黑名单 IP 的流量将不进行任何处理，直接丢弃。

进入页面的方法：安全 >> 安全防护 >> 黑名单

IP 地址	显示或设置本条黑名单项目的 IP 地址。地址中的主机号部分将被自动清零。
类型	显示或设置本条黑名单项目匹配的方向。
添加原因	显示本条黑名单项目被添加的原因，例如在本页直接新增时为“手动添加”，通过入侵防御配置文件的例外签名阻断动作新增时为“入侵防御”。编辑一条非“手动添加”的条目后，其添加原因将变为“手动添加”。
剩余时间	显示或设置本条黑名单项目在多少分钟后自动失效，最长可以设置 35280 分钟，即 24.5 天。若为 0 则表示不过期、永久存在。
备注	显示或设置本条黑名单项目的注释信息，可选，最多 50 字。

5.5 白名单

可查看并管理白名单项目。根据类型设置，来自或前往白名单 IP 的流量将不进行黑名单匹配和内容安全检查，只要安全策略允许其通过，就可以直接放行。

进入页面的方法：安全 >> 安全防护 >> 白名单

IP 地址　　显示或设置本条白名单项目的 IP 地址。地址中的主机号部分将被自动清零。

类型　　显示或设置本条白名单项目匹配的方向。

备注　　显示或设置本条白名单项目的注释信息，可选，最多 50 字。

状态　　显示或设置本条白名单项目是否生效。

注意：

- 白名单的源地址/目的地址指的是报文的源地址/目的地址，不同于安全策略中值得是数据流的源地址/目的地址。
- 白名单的匹配在 NAT 之前，如果配置了 NAT 策略，需要将 NAT 转换前的 IP 地址加入白名单才能生效。

回目录

第6章　对象管理

6.1　地址管理

6.1.1 地址组

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。

进入页面的方法：对象 >> 地址 >> 地址组

□	序号	组名称	地址名称	备注	设置
--	1	IPGROUP_ANY	---	IPGROUP_ANY	---
--	2	ISP_CN_ALL	---	中国所有IP地址	---
--	3	ISP_CHINA_TELECOM	---	中国电信	---
--	4	ISP_UNICOM_CNC	---	中国联通/网通	---
--	5	ISP_CMCC_CRTC	---	中国移动/铁通	---
--	6	ISP_CERNET	---	中国教育网	---
--	7	ISP_CN_OTHERS	---	中国其他ISP	---

导入　　点击<导入>按钮导入多个地址组条目和地址条目。可以通过“备份”功能获取符合规则的 CSV 文件，以查看文件的正确格式。

备份　　点击<备份>按钮备份所有地址组条目和地址条目。备份文件可直接通过“导入”功能重新添加到地址组列表和地址列表中。

点击<新增>，输入组名称，选择地址名称，地址名称的设置见 ***6.1.2 地址***，点击<确定>。

组名称	标志地址组的名称。
地址名称	地址组所引用的地址对象（可多选），引用了该地址组的规则，对所有地址对象所包含的 IP 地址均会生效。
备注	可以设置地址组的备注，以方便管理和查找。最多支持 50 个字符。

新增的条目会在组列表里显示出来，如下图所示。

	序号	组名称	地址名称	备注	设置
--	1	IPGROUP_ANY	---	IPGROUP_ANY	---
☐	2	g_lan_ip	lan-ip	---	

如有需要，可点击条目后的<>按钮进行编辑。

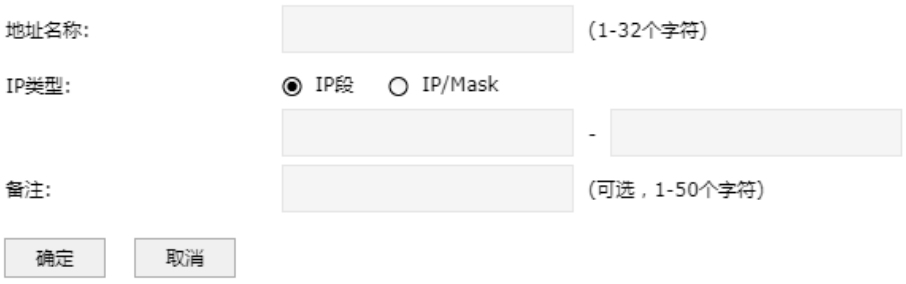
注意：

- 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。

6.1.2 地址

进入页面的方法：对象 >> 地址 >> 地址

点击<新增>，进入地址设置页面。填入地址名称，选择 IP 类型并填入 IP 信息，点击<确定>按钮手动添加条目。



地址名称	标志地址的名称。
IP 类型	用于设置地址对象的类型，不同类型计算得到 IP 集合的方式不同，有以下两种类型： IP 段：设置一个起始地址和一个结束地址，引用包含该地址对象地址组的规则在该地址段内均会生效。 IP/MASK：设置一个网络标识和一个子网掩码，得到 IP 网段，引用包含该地址对象地址组的规则在该网段内均会生效。
备注	设置地址对象的备注，以方便管理和查找。最多支持 50 个字符。

新增的条目会在**地址列表**里显示出来，如下图所示。

如有需要，可以点击条目后的<  >按钮进行编辑。条目1为系统默认条目，表示任何地址，不可操作。

6.2 时间段

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。

进入页面的方法：对象 >> 时间段 >> 时间段

点击<新增>，输入时间对象名称和时间段，时间设置可选择工作日历或手动设置，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  ，通过在日历上划分举行覆盖对应的时间区域来设置包含的时间段，只能精确到小时。

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>，通过手动输入生效时间段并勾选生效星期来设置一个时间段，精确到分钟，但一个对象最多只能设置 12 个时间段。

例如下图，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。

新增的条目会在时间对象列表里显示出来，如下图所示。

	序号	名称	工作日历	备注	设置
--	1	Any		Any time	
☐	2	t1		---	

如有需要，可以点击条目后的<>按钮进行编辑。条目 1 为系统默认条目，表示任何时间，不可操作。

点击<删除>，可批量删除时间对象列表条目。

6.3 IP 地址池

进入页面的方法：对象 >> IP 地址池 >> IP 地址池

点击<新增>按钮，进入 IP 地址池设置页面。填入地址池名称和起始、结束 IP 地址，点击<确定>按钮手动添加条目。

注意：

- 由地址池起始 IP 和地址池结束 IP 组成，且地址池起始 IP 必须不大于地址池结束 IP，而且不能与已有的地址池范围重叠。

新增的条目会在**地址池列表**里显示出来，如下图所示。

	序号	地址池名称	起始IP地址	结束IP地址	设置
☐	1	address	192.168.1.2	192.168.1.254	

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮可删除该地址池。

点击<删除>，可批量删除地址池列表条目。

6.4 服务对象

6.4.1 服务组

进入页面的方法：对象 >> 服务 >> 服务组

	序号	组名称	服务类型	备注	设置
--	1	Any	ALL	任意服务	---
--	2	Default_System_Service	DNS,NTP,TPLINK_CLOUD1,TPLINK_CLOUD2,TPLINK_CLOUD3,TPLINK_CLOUD4,TPLINK_CLOUD5,HTTPS,HTTP	系统默认服务	---
--	3	Default_Encrypted_Service	HTTPS	HTTPS 默认服务	---

点击<新增>，进入服务组设置页面。填入新地址组的名称，选择服务类型，服务类型的设置可参考 ***6.4.2 服务***，点击<确定>按钮手动添加条目。

组名称	标志服务组的名称。
服务类型	服务组所引用的服务对象（可多选），引用了该服务组的规则，对所有服务对象均会生效。
备注	可以设置服务组的备注，以方便管理和查找。最多支持 50 个字符。

新增的条目会在组列表里显示出来，如下图所示。

	序号	组名称	成员列表	设置
--	1	Any		---
	2	group_1		

如有需要，可点击条目后的<>按钮进行编辑。条目 1 为系统默认条目，不可操作。

点击<删除>，可批量删除服务组条目。

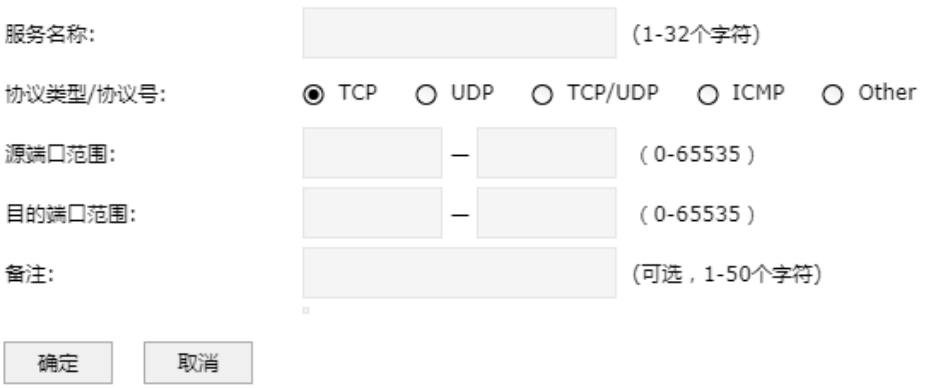
注意：

- 服务组对象一旦在其他地方被引用则无法在本页面被伤处，除非解除引用。
- 服务组可以为空（即不选择任何地址对象），引用该服务组的规则对所有服务均不生效。

6.4.2 服务

进入页面的方法：对象 >> 服务 >> 服务

点击<新增>，进入地址设置页面。填入地址名称，选择 IP 类型并填入 IP 信息，点击<确定>按钮手动添加条目。



服务名称	将要设置的服务类型的名称，注意不能与系统预定义服务类型名称重复。
协议类型/协议号	服务所使用的协议。可以选择 TCP，UDP，TCP/UDP 或 ICMP，也可以选择 other 并输入协议号(0-255)。
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。
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。
ICMP	ICMP 协议的类型（type）和编码（code），填充 255 时表明所有类型/编码。
备注	可以对服务类型进行描述。

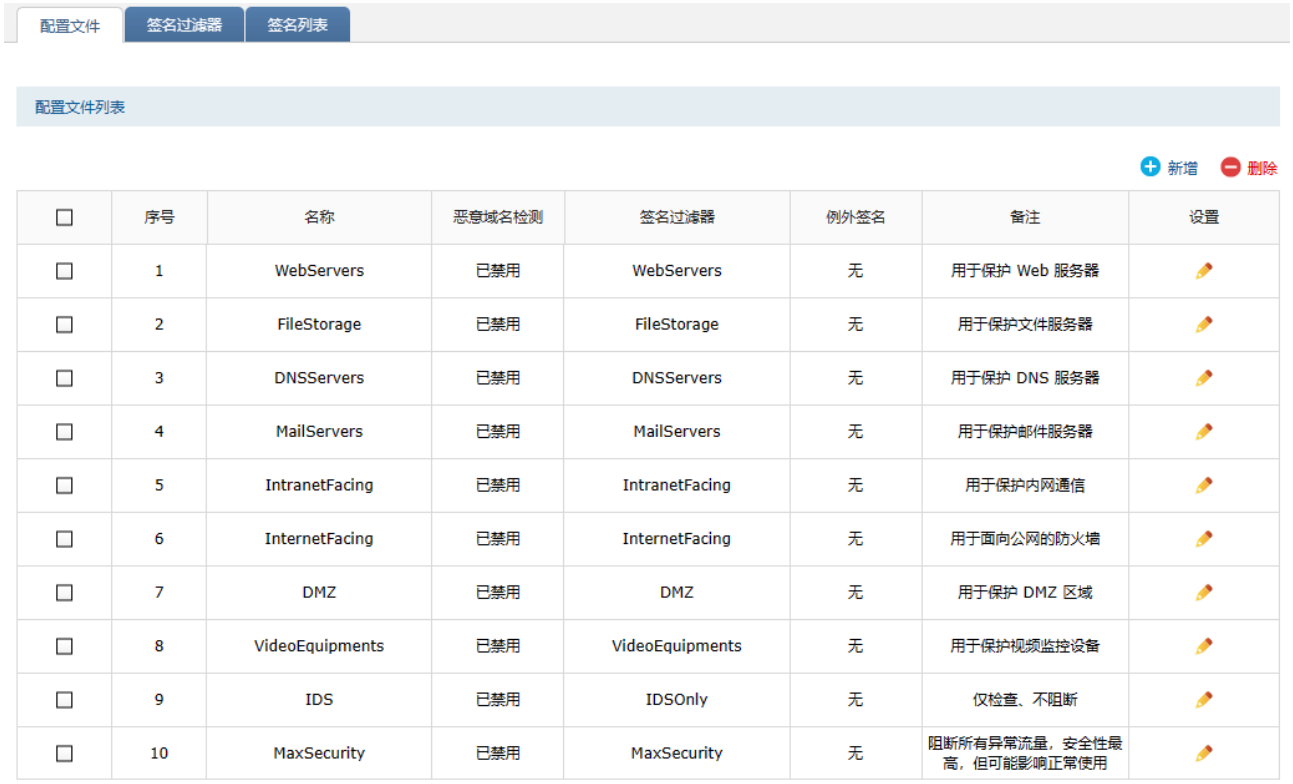
6.5 入侵防御

随着网络攻击技术的不断提高和网络安全漏洞的不断发现，传统防火墙技术加传统 IDS 的技术，已经无法应对一些安全威胁。在这种情况下，IPS(Intrusion-prevention System)入侵防御技术应运而生，入侵防御技术可以深度感知并检测流经的数据流量，对恶意报文进行丢弃以阻断攻击，对滥用报文进行限流以保护网络带宽资源。

6.5.1 配置文件

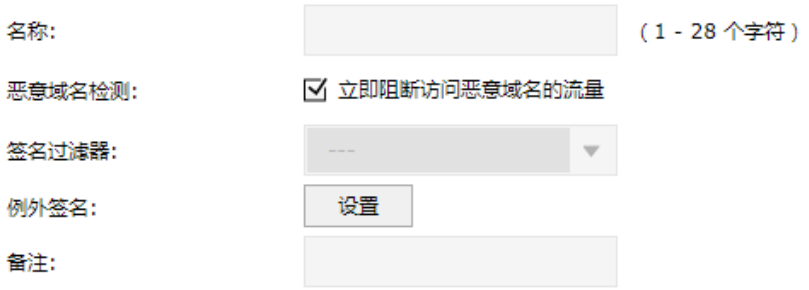
可以通过本页面设置 IPS(Intrusion-prevention System)配置文件列表，并在安全策略中引用。

进入页面的方法：安全 >> 入侵防御 >> 配置文件



	序号	名称	恶意域名检测	签名过滤器	例外签名	备注	设置
☐	1	WebServers	已禁用	WebServers	无	用于保护 Web 服务器	
☐	2	FileStorage	已禁用	FileStorage	无	用于保护文件服务器	
☐	3	DNSServers	已禁用	DNSServers	无	用于保护 DNS 服务器	
☐	4	MailServers	已禁用	MailServers	无	用于保护邮件服务器	
☐	5	IntranetFacing	已禁用	IntranetFacing	无	用于保护内网通信	
☐	6	InternetFacing	已禁用	InternetFacing	无	用于面向公网的防火墙	
☐	7	DMZ	已禁用	DMZ	无	用于保护 DMZ 区域	
☐	8	VideoEquipments	已禁用	VideoEquipments	无	用于保护视频监控设备	
☐	9	IDS	已禁用	IDSOnly	无	仅检查、不阻断	
☐	10	MaxSecurity	已禁用	MaxSecurity	无	阻断所有异常流量，安全性最高，但可能影响正常使用	

点击<新增>，添加新的配置文件。



名称　　设置 IPS 配置文件的名称。

恶意域名检测　　选中后，该配置文件还会同时检测对恶意域名的访问。访问恶意域名的流量将被立即阻断。该功能需要具有有效的“恶意域名远程查询”授权、安装了“恶意域名特征库”，且与互联网连接时才有效。

签名过滤器　　设置本配置文件使用的签名过滤器，以确定需检验的签名集合。请在“安全 >> 入侵防御 >> 签名过滤器”页面配置。

例外签名　　设置本配置文件的例外签名，这里设定的签名将会先于签名过滤器进行匹配，匹配成功后的动作以这里的设定为准。

备注　　设置本配置文件的备注，50 字以内。

说明：

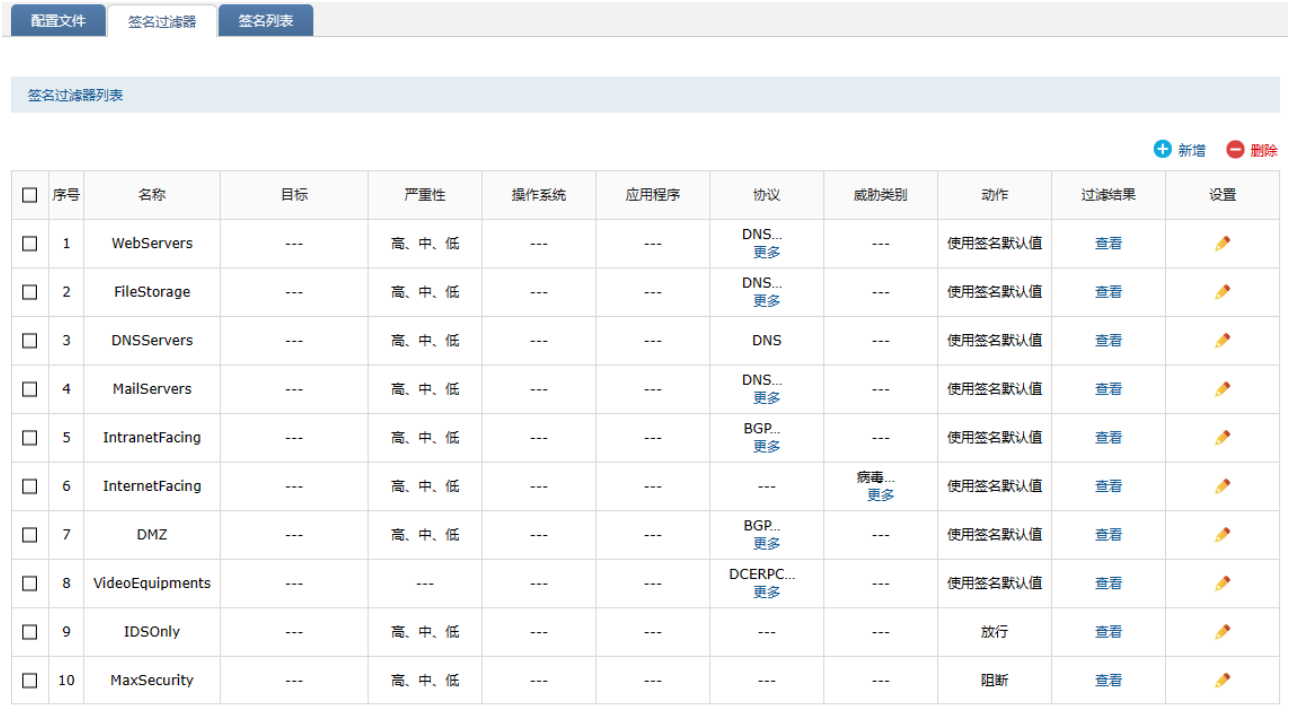
预置条目不允许编辑除例外签名之外的属性，也不允许删除。

6.5.2 签名过滤器

签名过滤器用来描述网络中攻击行为的特征，防火墙通过将数据流和签名过滤器进行比较来检测和防范攻击。签名过滤器是满足指定过滤条件的集合，过滤条件包括：签名的类别、对象、协议、严重性、操作系统等。只有同时满足所有过滤条件的签名才能加入签名过滤器中。一个过滤条件中如果配置多个值，多个值之间是“或”的关系，只要匹配任意一个值，就认为匹配了这个条件。

可通过设置签名过滤器列表，用来将适合需求的签名组成集合，拱 IPS 配置文件使用。

进入页面的方法：安全 >> 入侵防御 >> 签名过滤器



	序号	名称	目标	严重性	操作系统	应用程序	协议	威胁类别	动作	过滤结果	设置
☐	1	WebServers	---	高、中、低	---	---	DNS... 更多	---	使用签名默认值	查看	
☐	2	FileStorage	---	高、中、低	---	---	DNS... 更多	---	使用签名默认值	查看	
☐	3	DNSServers	---	高、中、低	---	---	DNS	---	使用签名默认值	查看	
☐	4	MailServers	---	高、中、低	---	---	DNS... 更多	---	使用签名默认值	查看	
☐	5	IntranetFacing	---	高、中、低	---	---	BGP... 更多	---	使用签名默认值	查看	
☐	6	InternetFacing	---	高、中、低	---	---	---	病毒... 更多	使用签名默认值	查看	
☐	7	DMZ	---	高、中、低	---	---	BGP... 更多	---	使用签名默认值	查看	
☐	8	VideoEquipments	---	---	---	---	DCERPC... 更多	---	使用签名默认值	查看	
☐	9	IDSOnly	---	高、中、低	---	---	---	---	放行	查看	
☐	10	MaxSecurity	---	高、中、低	---	---	---	---	阻断	查看	

点击<新增>，添加新的签名过滤器。

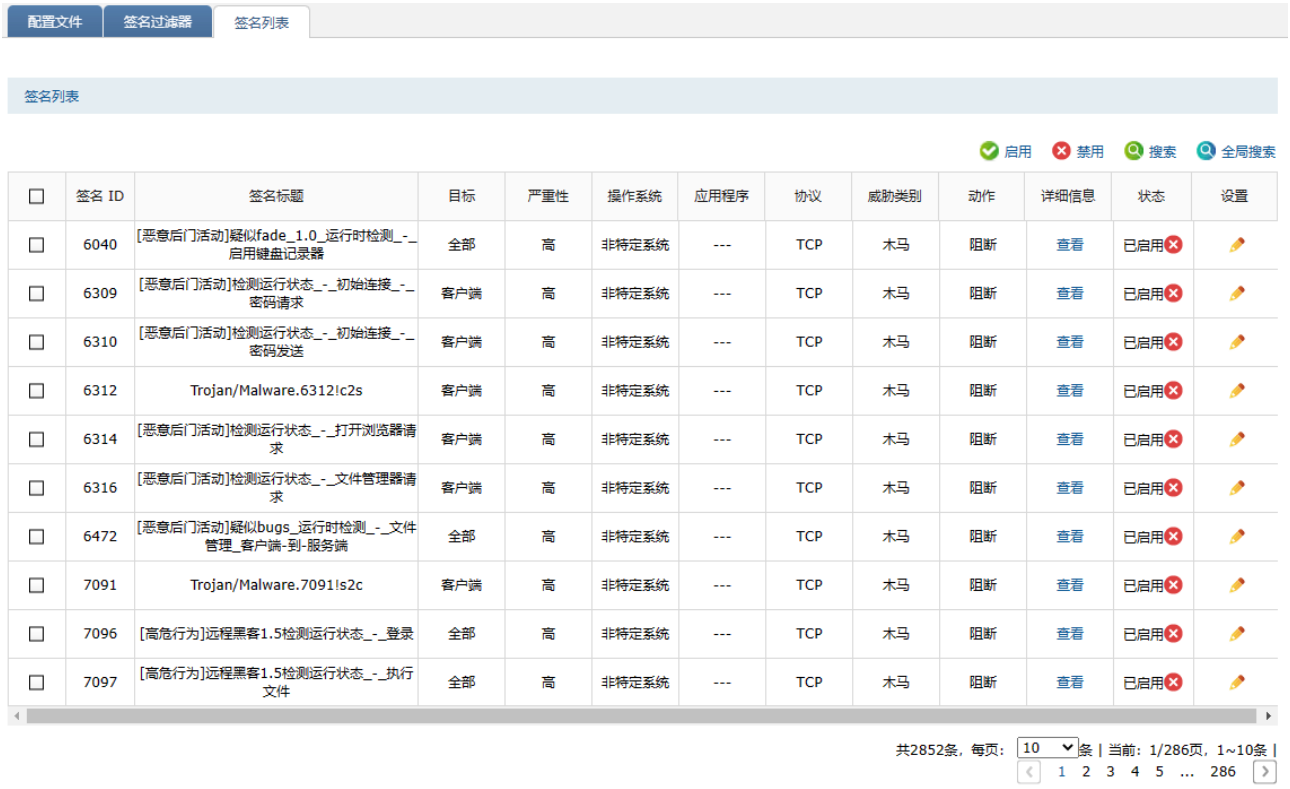
名称	设置签名过滤器的名称。
目标	选择需要保护的目标。不选择等同于不判断此条件。
严重性	筛选指定严重程度的签名。不选择等同于不判断此条件。

操作系统	筛选影响指定操作系统的签名。不选择等同于不判断此条件。
应用程序	筛选影响指定应用程序的签名。不选择等同于不判断此条件。
协议	筛选利用指定协议的威胁的签名。不选择等同于不判断此条件。
威胁类别	筛选签名对应的威胁类别。不选择等同于不判断此条件。
动作	选择本签名过滤器所选签名的默认动作。 放行：对命中签名的报文放行，不记录日志 阻断：丢弃命中签名的报文，阻断该报文所在的数据流，并记录日志。
备注	设置本签名过滤器的备注，50 字以内。
过滤结果	点击可查看当前条件所筛选出的签名及动作。

6.5.3 签名列表

您可以通过本页面查看签名详细信息，并设置设备自带签名的默认动作。

进入页面的方法：安全 >> 入侵防御 >> 签名列表



签名 ID	显示本条签名的 ID。可在 IPS 配置文件的例外签名设置中使用。
签名标题	显示本条签名的标题。可在日志中看到。
目标	显示本条签名要保护的目标。

严重性	显示本条签名所述威胁的严重等级。
操作系统	显示本条签名所述威胁影响的操作系统。
应用程序	显示本条签名所述威胁影响的应用程序。
协议	显示本条签名所述威胁影响的网络协议。
威胁类别	显示本条签名所述威胁的分类。
动作	选择本条签名命中后的默认动作。
备注	设置本签名的备注，50 字以内。
详细信息	点击可查看本条签名的详细信息。
状态	选择本条签名是否要被纳入检测流程。

点击<启用>，可批量启用签名规则。

点击<禁用>，可批量禁用签名规则。

点击<搜索>，可根据列名、内容、方式和方式进行搜索。

点击<全局搜索>，可搜索不同内容、不同列名的列表信息。

6.6 服务器 CA 证书

进入页面的方法：对象 >> 证书 >> 服务器 CA 证书

点击<上传>，上传服务器 CA 证书文件。

按需求填写待上传证书内容，点击<确认>即可完成上传。

证书文件	支持的证书文件后缀为.cer、.der、pem、.crt、.p12、.pfx。
密码	仅 pkcs12 格式的证书文件导入时会对此值进行校验，其他格式的证书导入时会忽略此值。

6.7 地址组的设置与管理实例

防火墙的应用控制、网站访问、网页安全、带宽控制等行为管控功能均是基于地址组的，将需要进行同一个管控策略的一个或多个 IP 添加到同一个地址组，就可以针对该地址组内的所有 IP 来进行上网行为的管控。

➢ 需求介绍

某公司办公网络包含市场、人事等部门，需要进行上网行为管控，以下为各部门的网段：

部门	IP 地址段
人事部（10 人）	192.168.1.100-192.168.1.109
市场部（10 人）	192.168.1.120-192.168.1.149

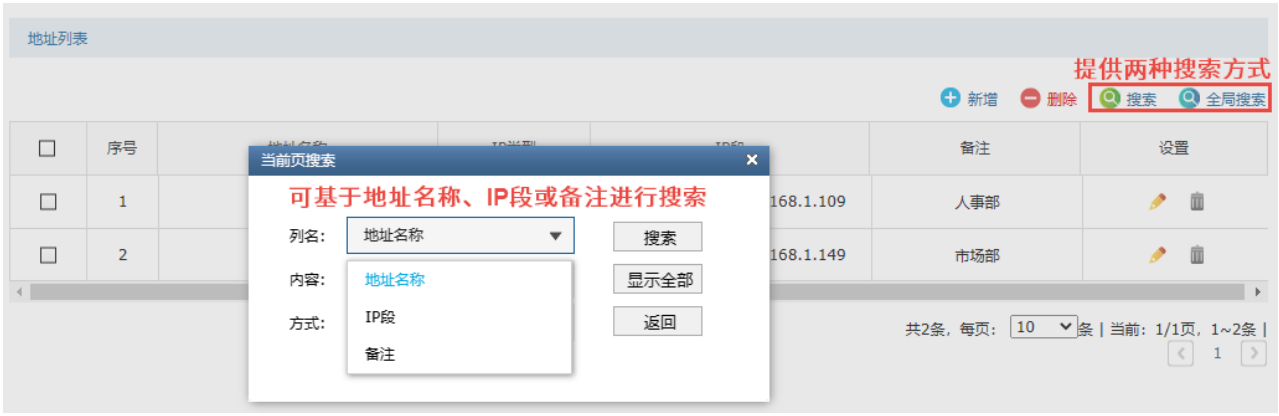
➢ 设置方法

1. 地址的添加与管理

进入页面：对象>> 地址>> 地址，点击<新增>，填写地址名称和包含的地址，其中地址有两种类型：IP 段、IP/mask，此处选择相对灵活的 IP 段类型，还可以根据需求填写备注，点击确定即可完成添加。

按照需求中的要求，新增的两个地址组如下图所示，可点击对应条目后的<编辑>或<删除>按钮对已添加地址组进行管理，勾选对应条目点击页面上方<删除>按钮也可以对多个条目进行批量删除。

为了地址条目较多的应用场景，此页面还提供了<搜索>和<全局搜索>两种条目搜索方式，可基于地址组的地址名称、IP 段、备注等信息进行条目搜索，包括在所有条目中/结果中进行搜索。



2. 地址组的添加与管理

进入页面：对象 >> 地址 >> 地址组，点击<新增>，填写地址组名称，勾选地址组包含的地址（此处可勾选多个地址），还可以根据需求填写备注，点击<确定>完成添加。

除了与地址管理页面相同的删除、编辑、搜索功能之外，此页面还提供了地址组的<备份>和<导入>功能。可以通过备份功能获取符合规则的 CSV 文件，以查看文件的正确格式，备份文件也可直接通过导入功能重新添加到地址组列表和地址列表中。

3. 地址组的使用

在行为管控相关功能的源、目的地址范围处选择已添加的地址组，即可对此地址组内的 IP 进行对应的行为管控。

以应用控制为例，如下图所示，进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，源地址选择已添加的地址组，点击<点击修改>选择需要管控的应用并选择动作，其他内容根据实际需要填写即可。填写完成后，点击<确定>完成添加。

回目录

第7章　行为管控

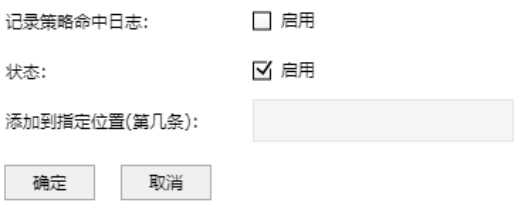
TP-LINK 防火墙采用最小安全原则，支持基于安全区域、源 IP 地址、目的 IP 地址、源端口、目的端口、服务组、应用组、用户组、时间段、黑白名单、网站、内部服务器证书、加密流量检测策略、反病毒、URL 过滤、文件过滤、应用行为控制、邮件内容过滤、入侵防御、审计配置文件等对象的安全策略，用户可自定义组合，设定访问规则，全面高效管控内外网通信安全。

7.1.1 安全策略

防火墙默认存在一条所有区域、地址段允许或禁止所有应用的规则，默认规则只能修改规则内容，不能删除。

进入页面的方法：策略 >> 安全策略 >> 安全策略

点击<新增>，添加安全策略规则。



规则名称	安全策略名称。
描述	安全策略的描述信息，便于后续分类查找。
源安全区域	指定安全策略匹配的数据流源安全区域。安全区域配置可参考 ***4.2 安全区域***。
目的安全区域	指定安全策略匹配的数据流目的安全区域。安全区域配置可参考 ***4.2 安全区域***。
源地址	指定安全策略匹配的数据流源地址。地址组配置可参考 ***6.1 地址管理***。
目的地址	指定安全策略匹配的数据流目的地址。地址组配置可参考 ***6.1 地址管理***。
用户组	指定安全策略匹配的用户组。
服务组	指定安全策略匹配的数据流协议及端口。服务组的创建过程请参考 ***6.4 服务对象***。
应用组	指定安全策略匹配的应用组，也可以单选应用。当策略动作选择允许时，会放行相关的网络基础协议。应用组的创建过程请参考 ***7.3 应用控制***。
时间段	指定安全策略生效的时间段。时间段的配置请参考 ***6.2 时间段***。
动作	允许或者禁用上述条件过滤出来的数据。
内容安全	对满足上述过滤条件的流量数据进行更深入一步的内容安全的检查。
URL 过滤	选择安全配置文件中的 URL 过滤配置对 URL 请求进行检查。
反病毒	选择安全配置文件中的反病毒配置对病毒文件进行检查。
入侵防御	选择安全配置文件中的入侵防御配置对入侵行为进行检查。
文件过滤	选择安全配置文件中的文件过滤配置对下载和上传的文件类型进行检查。
应用行为控制	选择安全配置文件中的应用行为控制配置对多种应用的行为进行控制。
邮件内容过滤	选择安全配置文件中的邮件内容过滤配置对邮件内容进行检查。
记录策略命中日志	选择安全配置文件中的 URL 过滤配置对 URL 请求进行检查。
状态	勾选是否启用该安全策略规则。

添加到指定位置（第几条）	设置安全策略添加到指定位置。

7.1.2 策略冗余分析

策略冗余分析将比较策略的源安全区域、目的安全区域、源地址、目的地址、服务组、应用组、用户组和时间段，从而得出其中的冗余策略。

进入页面的方法：策略 >> 安全策略 >> 策略冗余分析

点击<开始分析>，添加安全策略规则。

点击<删除>，可批量删除冗余策略，可提供安全策略管理效率。

7.2 安全配置文件

7.2.1 邮件过滤

进入页面的方法：安全 >> 安全配置文件 >> 邮件过滤

点击<新增>，设置邮件过滤规则。

名称	文件过滤配置文件的名称。
SMTP	选择针对 SMTP 协议的默认安全动作，可选允许/禁止。
设定发/收件人白名单	白名单中人员不受 SMTP 邮件过滤规则限制
POP3	选择针对 POP3 协议的默认安全动作，可选允许/禁止。
设定发/收件人白名单	白名单中人员不受 POP3 邮件过滤规则限制
IMAP	选择针对 IMAP 协议的默认安全动作，可选允许/禁止。
设定发/收件人白名单	白名单中人员不受 IMAP 邮件过滤规则限制
备注	您可以为该规则添加备注，50 字符以内。

7.2.2 内容过滤

进入页面的方法：安全 >> 安全配置文件 >> 内容过滤

点击<新增>，设置内容过滤规则。

名称	内容过滤配置文件的名称。
应用	选择进行文件过滤的应用。
方向	选择进行文件过滤的方向。
动作	选择文件过滤的命中动作，可选允许/告警/禁止。
文件后缀列表	添加待过滤的文件后缀，各个后缀之间以换行隔开。
备注	您可以为该规则添加备注，50 字符以内。

7.2.3 关键字组

进入页面的方法：对象 >> 安全配置文件 >> 关键字组

点击<新增>，设置关键字组。

名称	关键字组的名称。
预定义关键字	引用预先定义好的关键字（银行卡、信用卡、手机号、身份证号）来进行过滤，银行卡和信用卡仅限于招行的银联卡。支持在文本关键字和正则表达式中自定义关键字。
文本关键字列表	进行精确匹配的关键字，支持中文，区分大小写，长度为 3-200 字节。一个英文全角符、中文全角符、汉字占用 2 字节，一个英文半角符占用 1 字节。
正则表达式列表	使用正则表达式时，请输入标准 pcre 语法的关键字。不支持中文匹配，可考虑改为\x01 形式的十六进制输入。不支持正则表达式的定位符。
备注	您可以为该规则添加备注，50 字符以内。

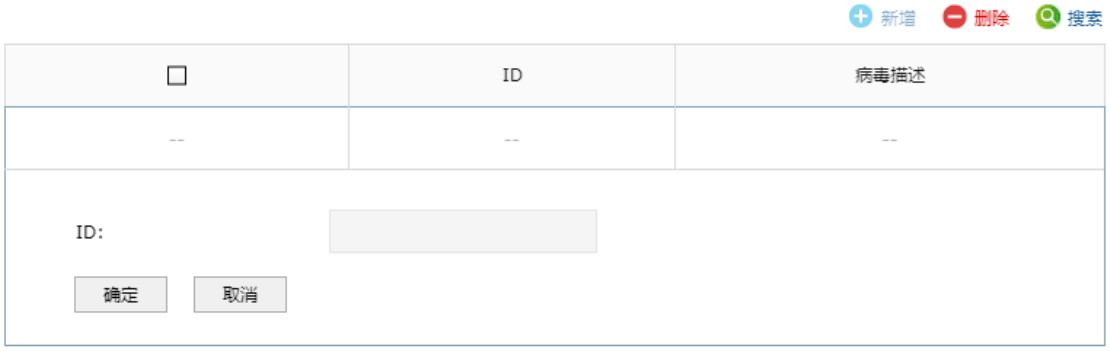
7.2.4 反病毒

进入页面的方法：对象 >> 安全配置文件 >> 反病毒

点击<新增>，设置反病毒规则。

名称	设置反病毒配置文件的名称。
描述	反病毒配置文件具体介绍。
HTTP/FTP/SMTP/POP3/IMAP	支持病毒检测的协议类型。
应用例外-允许	对于允许应用中发现的病毒文件采取例外动作。
应用例外-警告	对于警告应用中发现的病毒文件采取例外动作。
应用例外-阻断	对于阻断应用中发现的病毒文件采取例外动作。

点击<病毒例外>，对于指定 id 的病毒不进行处理，点击<新增>，输入病毒 ID，点击<确定>，保存配置。



7.2.5 病毒家族

病毒家族即广义的病毒名称，同一病毒家族的病毒通常具有相似的特征。

进入页面的方法：安全 >> 反病毒 >> 病毒列表

病毒列表

搜索

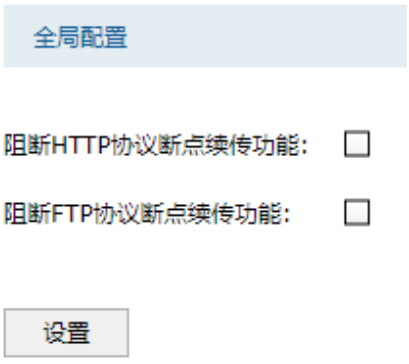
序号	病毒家族
1	Andr.Adware.Adflex
2	Andr.Adware.Admogo
3	Andr.Adware.Adwo
4	Andr.Adware.Airpush
5	Andr.Adware.Andup
6	Andr.Adware.Appad
7	Andr.Adware.Appoffer
8	Andr.Adware.Autosms
9	Andr.Adware.Clevernet
10	Andr.Adware.Cyfin

点击<搜索>，可通过病毒家族名称对列表内容进行搜索。

7.2.6 断点续传

可设置是否阻断 HTTP/FTP 协议断点续传功能。断点续传功能关闭后，网络断开后，将不能从断开的位置继续传输数据。

进入页面的方法：安全 >> 安全配置文件 >> 全局配置



7.3 应用控制

7.3.1 应用组

应用组识别模式分为全量识别和智能识别。全量识别模式下，全部开启应用识别功能，有可能造成性能下降。建议开启智能识别模式，根据生效的策略是否包含应用或应用组配置，自动选择是否开启应用识别功能。

进入页面的方法：安全 >> 应用 >> 应用组

勾选<启用智能识别模式>，点击<设置>，开启智能识别。

点击<新增>，进入服务组设置页面。填入新地址组的名称和备注信息，点击<确定>按钮手动添加条目。

名称　　应用组名称。

预览　　查看已选择的应用。

应用　　选择该应用组包含的应用。

备注	您可以设置应用组的备注，以方便您管理和查找。备注最多支持 50 个字符。

新增的条目会在组列表里显示出来，如下图所示。

	序号	名称	应用列表	备注	设置
☐	1	A1	微信 更多	社交	

7.3.2 应用

进入页面的方法：安全 >> 应用 >> 应用

在页面上方，可根据类别、子类别、标签、数据传输方式和风险等级对已有应用列表进行筛选查看。

点击<新增>按钮，设置各应用参数，点击<确定>按钮手动添加条目。

名称	自定义应用名称。
类别	选择应用用途类别。
子类别	选择应用用途子类别。
数据传输方式	选择应用的数据传输方式。
风险等级	应用风险成都，系统根据勾选的风险维度标签数量计算出风险级别。
标签	为应用添加风险等级、功能维度、风险维度和其它等特性标签。
备注	您可以对应用进行描述，便于后续查找和管理。

点击<应用匹配列表>，点击<新增>可为应用添加匹配规则。用户自定义的应用匹配规则优先级比应用识别特征库优先级更高。

名称	应用名称。
目的地址	连接接收方地址，一般为服务器地址，与发起方相对。
目的端口	连接接收方端口。
协议	应用使用的四层协议。

关键字	应用识别匹配的关键字，关键字与匹配字段、检测方向、检测模式必须全选或全部不选。 使用正则表达式模式时，请输入标准 pcre 语法的关键字；不支持中文匹配，可考虑改为\x10 形式的十六进制输入并使用政策表达式模式；不支持政策表达式的定位符。
匹配字段	应用识别可选的匹配字段。
检测方向	需要匹配的报文的传输方向，对于未设定目的地址和目的端口的规则，如果实际传输层协议为 UDP，该匹配规则有在任意方向均生效的风险。
检测模式	关键字匹配的模式。
备注	设置备注信息。

7.3.3 应用行为控制

进入页面的方法：安全 >> 安全配置文件 >> 应用行为控制

点击<新增>，设置应用行为控制规则。

名称	设置应用行为控制规则的名称。

告警阈值	输入被允许通过的应用行为的告警阈值。
阻断阈值	输入被允许通过的应用行为的阻断阈值。

HTTP 相关：

POST	选择针对 HTTP POST 操作的安全动作，可选允许/禁止。如需保证高质量的 HTTP POST，建议放行一定阈值的文件上传。
网页浏览	选择针对 HTTP 网页浏览的安全动作，可选允许/禁止。如需保证高质量的网页浏览，建议放行一定阈值的文件下载。
代理上网	选择针对 HTTP 代理上网的安全动作，可选允许/禁止。
文件上传	选择针对 HTTP 文件上传的安全动作，可选允许/禁止。
文件下载	选择针对 HTTP 文件下载操作的安全动作，可选允许/禁止。

FTP 相关：

文件上传	选择针对 FTP 文件上传的安全动作，可选允许/禁止。
文件下载	选择针对 FTP 文件下载操作的安全动作，可选允许/禁止。
文件删除	选择针对 FTP 文件删除操作的安全动作，可选允许/禁止。

IM 相关：

QQ 登录	选择针对 QQ 登录的默认安全动作，可选允许/禁止。
QQ 登录黑/白名单	输入不允许/允许登录的 QQ 账号，当 QQ 登录的默认安全动作为允许时，登录黑名单生效。
备注	您可以为该规则添加备注，50 字符以内。

7.3.4 应用控制配置实例

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、购物类的应用则无需求。防火墙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：

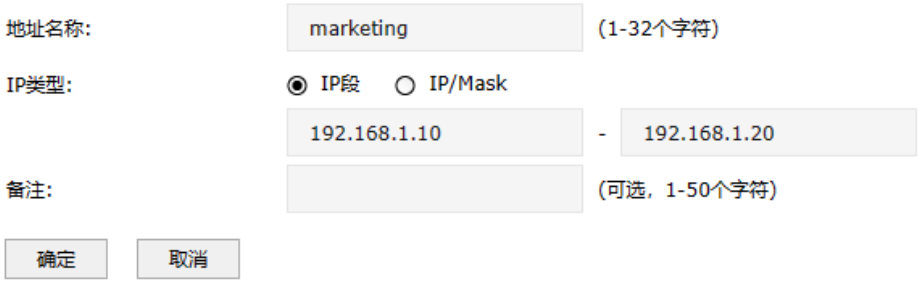
1. 仅允许市场部员工登录企业 QQ、微信、阿里旺旺（相对于限制列表）；
2. 允许市场部员工登录 12345678，987654321 这两个 QQ 号码；

3. 其他部门不做限制。

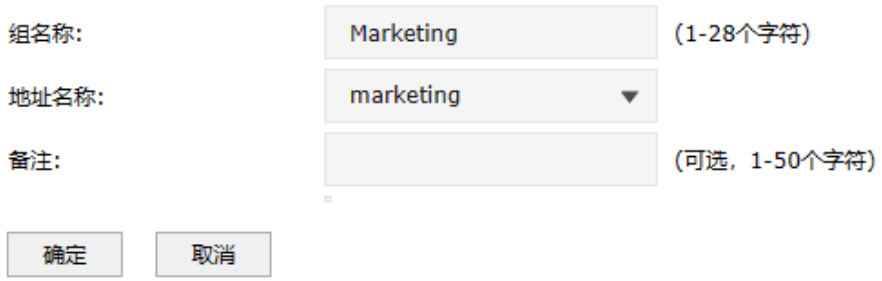
➢ **设置方法**

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。在防火墙界面，进入页面：对象 >> 地址 >> 地址，点击<新增>，添加市场部地址。

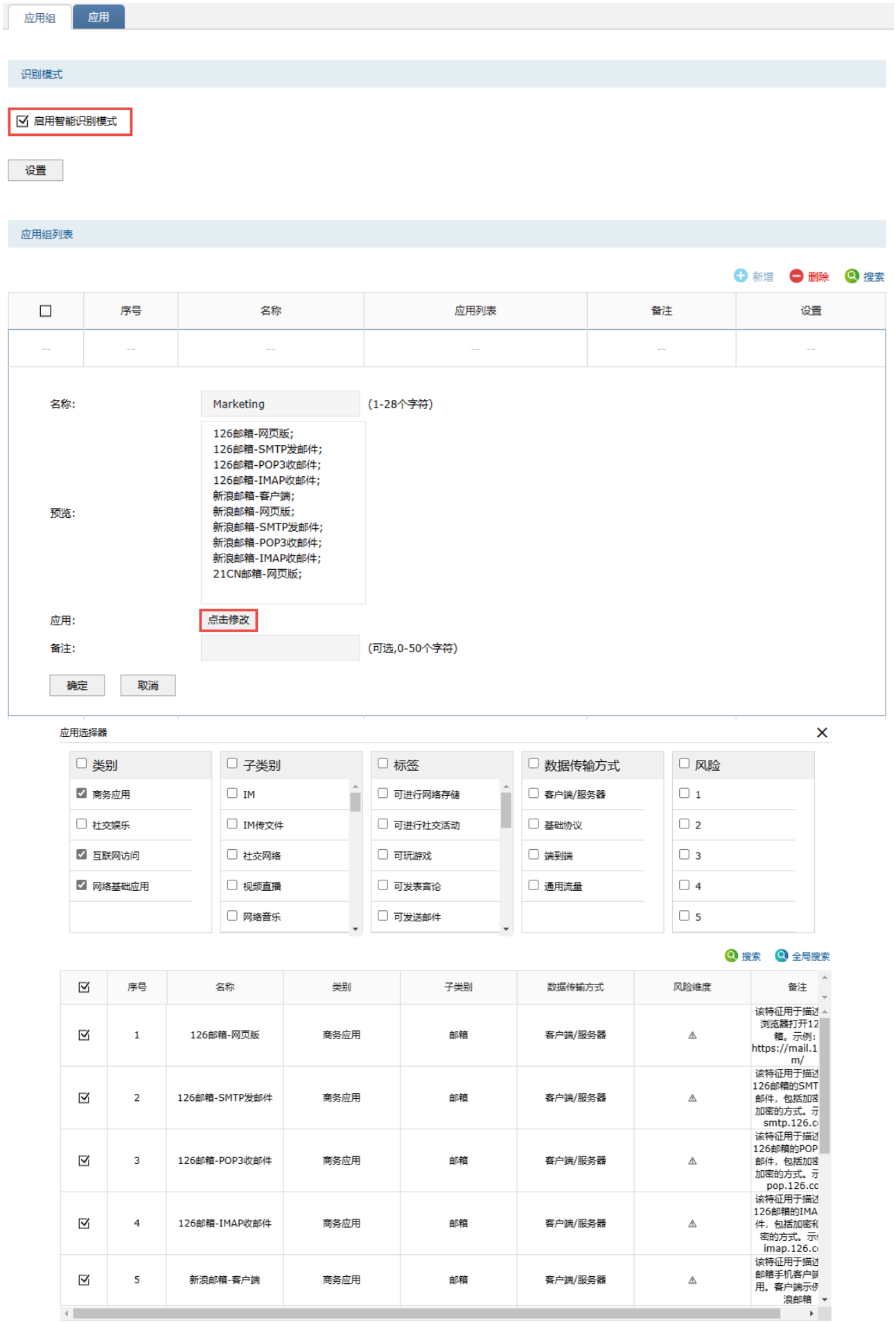


在防火墙界面，进入页面：对象 >> 地址 >> 地址组，点击<新增>，将市场部 IP 地址添加到市场部地址组中。



2. 添加应用分组

进入页面：对象 >> 应用 >> 应用组，点击<新增>，在列表中勾选允许市场部使用的应用：



3. 启用并设置 QQ 白名单

进入页面：安全 >> 安全配置文件 >> 应用行为控制，点击<新增>，允许市场部进行网页浏览，在“IM 相关”中勾选“设定白名单”，设置允许市场部登录如下 QQ，点击<确定>。

4. 进入页面：策略 >> 安全策略 >> 安全策略，添加市场部规则，源地址选择市场部地址组，应用组选择步骤 2 中设置的应用组“Marketing”，在内容安全中，选择为市场部设置的应用行为规则“Marketing”。

至此，应用控制功能设置完成，市场部的员工在使用网络过程中，视频软件、购物软件、P2P 软件、网络游戏、炒股等上网行为将会被禁止。

7.4 网站访问控制

7.4.1 网站分组

进入页面的方法：安全 >> 网站 >> 网站组

网站分组列表

新增 删除

☐	序号	组名称	自定义组成员	备注	设置
--	1	视频	- 更多	---	
--	2	游戏	- 更多	---	
--	3	财经	- 更多	---	
--	4	社交	- 更多	---	
--	5	购物	- 更多	---	
--	6	生活	- 更多	---	

点击<新增>或< >，进入网站组设置页面。填入新网站组的名称和备注信息，点击<确定>按钮手动添加条目。

组名称　　输入一个名称来标识一个组。只能输入英文、数字和下划线。

自定义组成员　　网站分组成员，可以同时输入多个网站进行批量添加。
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。

清空　　可以清空组成员中输入的内容。

文件路径　　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。

备注　　可以为分组添加 50 字符以内的备注。

7.4.2 URL 过滤

URL 过滤规则可以允许/禁止访问网站分组或者有关的 URL。

进入页面的方法：安全 >> 安全配置文件 >> URL 过滤

点击<新增>，设置 URL 过滤规则。

名称	URL 过滤配置文件的名称。
策略类型	对符合规则的网址放行或禁止。当选择"仅允许访问下列的 URL"时，会将不匹配的 URL 数据丢弃，选择"禁止访问下列的 URL"时，仅丢弃匹配的 URL 数据。
过滤方式	"网站分组"是根据"对象"中的网站组来对 URL 进行匹配，"URL"关键字是用自定义的关键字对 URL 进行部分匹配，"完整 URL"是指自定义 URL 进行完全匹配。
网站分组	当过滤方式为“网站分组”时，选择需要过滤的网站分组。网站分组配置请参考 *7.4.1 网站分组*。
过滤内容列表	当过滤方式为 URL 关键字、完整 URL 时，填写需要过滤的内容。其中单独符号.表示任意 URL，也就是与任意 URL 匹配。.规则只能配置一条，表示对任意的 URL 禁止或者允许，并且该规则只能在规则列表最后面。
备注	添加对本规则的说明信息。

7.4.3 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。防火墙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：

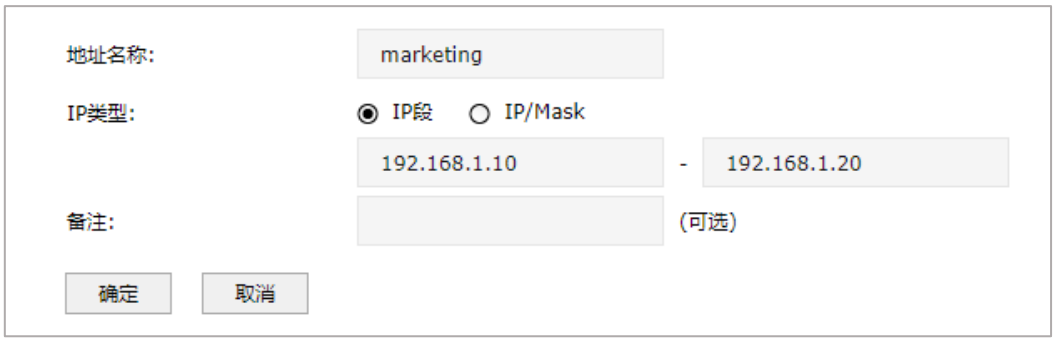
部门	网络权限
市场部	禁止访问视频、游戏、购物类网站
其他部门	仅允许访问公司网站及百度

设置方法：

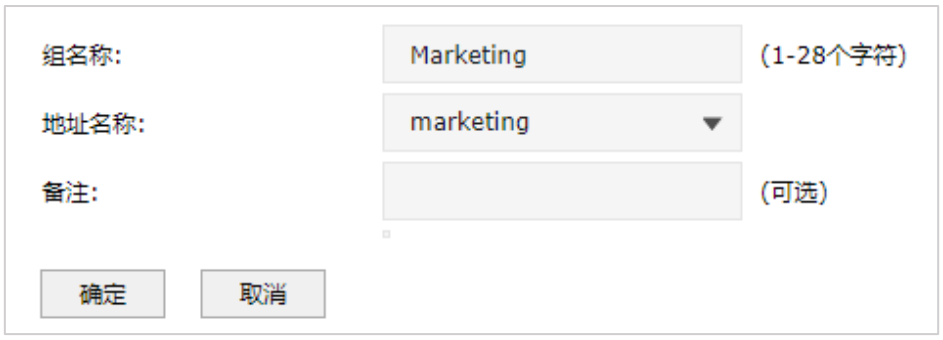
1. 设置地址组

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。

在防火墙界面，进入页面：对象 >> 地址 >> 地址，点击<新增>，添加市场部地址组。



在防火墙界面，进入页面：对象 >> 地址 >> 地址组，点击<新增>，将市场部 IP 地址添加到市场部地址组中。



以同样的方法添加其他部门的地址组。

2. 添加网站分组

进入页面：安全 >> 网站>> 网站组，点击<新增>，添加其他部门允许访问的网站分组，如下：

注意：

- 在组成员中可使用通配符（*）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. 设置网站过滤规则

进入页面：安全 >> 安全配置文件 >> URL 过滤

添加市场部的规则：

在规则列表中，点击<新增>，添加市场部的过滤规则。禁止市场部访问视频、游戏、购物类的网站，如下图：

添加其他部门的规则：

点击<新增>，添加一条规则，仅允许其他部门访问官网及百度，如下图：

4. 设置安全策略

进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>添加市场部规则。

源地址选择步骤 1 中添加的市场部地址组，在内容安全部分，选择步骤 3 中添加的市场部规则。

添加其他部门规则：

源地址选择步骤 1 中添加的其他部门地址组，在内容安全部分，选择步骤 3 中添加的其他部门规则。

至此，网站过滤功能设置完成，企业所有部门员工将按照设置的规则来上网。

7.4.4 URL 过滤配置实例

URL（统一资源定位符）是万维网资源定位标志，就是通常所讲的网址（如：www.tp-link.com.cn）。URL 过滤功能即针对 URL 中的关键字或者完整的 URL 进行限制或允许，实现访问对应网站的权限的控制。防火墙的 URL 过滤针对地址组进行控制，可以实现网页访问限制、行为审计等功能。

➢ **需求介绍**

某企业使用 TL-NFW8500 防火墙，为了规范网络使用情况，制定不同部门的网络访问权限如下：

部门	网络权限
市场部	只能访问公司官网（https://www.tp-link.com.cn）

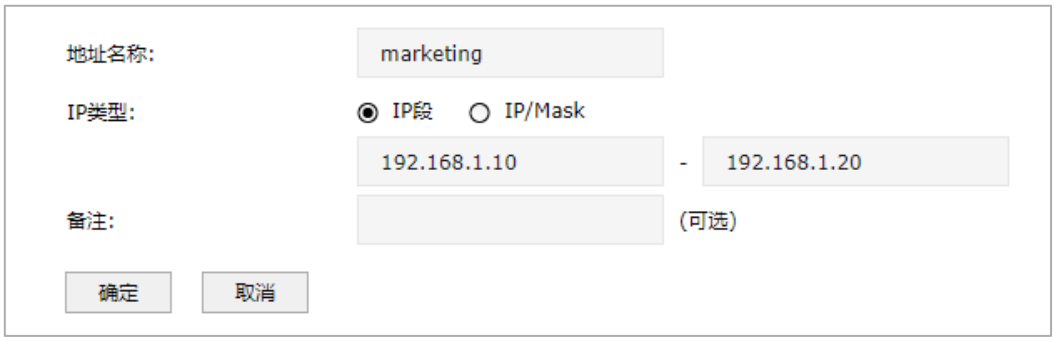
其他部门	禁止访问所有网页

➢ **设置方法**

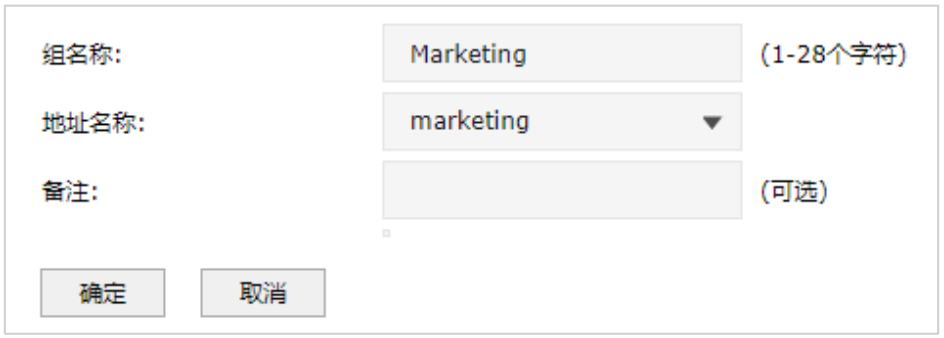
1. 添加地址组

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。

在防火墙界面，进入页面：对象 >> 地址 >> 地址，点击<新增>，添加市场部地址组。



在防火墙界面，进入页面：对象 >> 地址 >> 地址组，点击<新增>，将市场部 IP 地址添加到市场部地址组中。



以同样的方法添加其他部门的地址组。

2. 设置 URL 过滤规则

进入页面：安全 >> 安全配置文件 >> URL 过滤

添加市场部规则

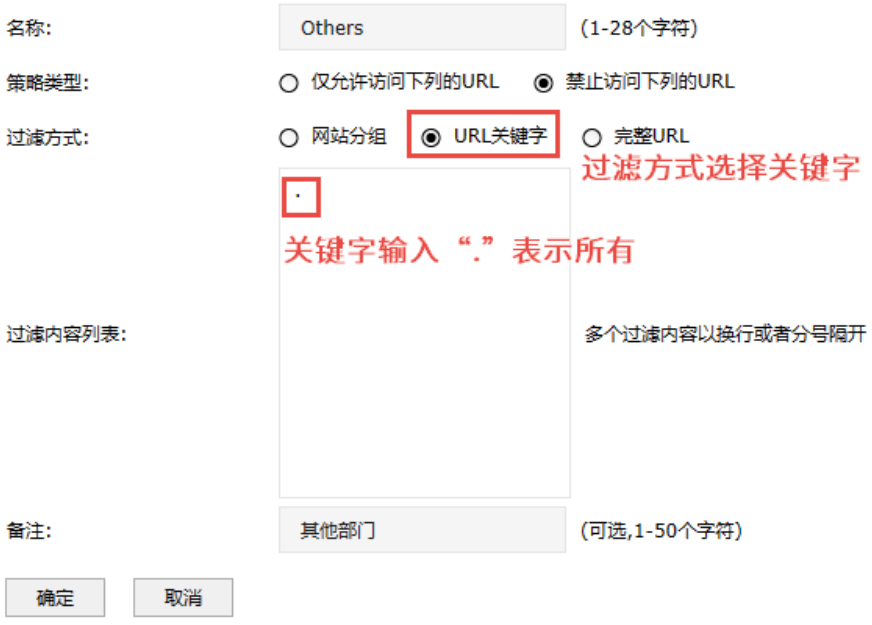
策略类型为“仅允许访问下列的 URL”，过滤方式选择“URL 关键字”，过滤内容列表输入公司官网的关键字，点击<确定>，详细设置见下图：

注意：

- 关键字指域名中的任何字符，比如 www.tp-link.com.cn 中的“www”、“tp-link”、“com”、“cn”、“.”等。如果网站域名中添加关键字，表示受控地址组中的成员可以访问带有该关键字的任何网址。

添加其他部门的规则

策略类型为“禁止访问下列的 URL”，过滤方式选择“URL 关键字”，过滤内容列表输入“.”代表所有网址，点击<确定>，详细设置见下图：



3. 设置安全策略

进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>添加市场部规则。

源地址选择步骤 1 中添加的市场部地址组，在内容安全部分，选择步骤 2 中添加的市场部 URL 过滤规则。

添加其他部门规则：

源地址选择步骤 1 中添加的其他部门地址组，在内容安全部分，选择步骤 2 中添加的其他部门 URL 过滤规则。

注意：

- 如果需要记录所有用户访问的网页或拦截的网页，可勾选以上规则中的“记录到策略命中日志”。

至此，URL 过滤规则设置完成，局域网的所有电脑浏览网页的权限将按照 URL 规则来执行。

7.5 文件过滤

7.5.1 文件过滤

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。文件过滤规则，可对特定应用组内的特定文件，允许/禁止其上传或下载，或当其上传或下载时，发出告警信息。

进入页面的方法：安全 >> 安全配置文件 >> 文件过滤

点击<新增>，设置文件过滤规则。

名称	文件过滤配置文件的名称。
应用	选择进行文件过滤的应用。应用组设置请参考 ***7.3 应用控制***。
方向	选择进行文件过滤的方向，可选上传/下载/双向。
动作	选择文件过滤的命中动作，可选允许/告警/禁止。
文件后缀列表	添加待过滤的文件后缀，各个后缀之间以换行隔开。
备注	您可以为该规则添加备注，50 字符以内。

7.5.2 文件过滤配置实例

文件过滤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。

➢ **需求介绍**

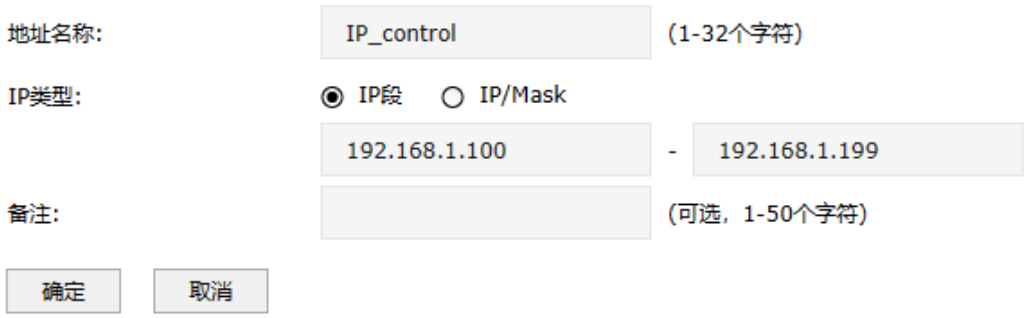
某企业网络环境中，为了确保内部网络安全，需求如下：

- 禁止企业内部人员在网页上上传或下载 exe，rar 后缀的文件。

➢ **设置方法**

1. 添加用户组

添加受控终端的用户组，方便后续的控制规则针对用户组进行控制。进入页面： 对象 >> 地址 >> 地址，点击<新增>，添加受控 IP 地址。



进入页面： 对象 >> 地址 >> 地址组，点击<新增>，将受控 IP 地址添加到地址组中：

2. 设置文件过滤从规则

进入页面：安全 >> 安全配置文件 >> 文件过滤

在文件过滤规则列表中，点击<新增>，选择 HTTP 应用，填写需要过滤文件的扩展类型，方向选择“双向”，设置完成后，点击<确定>。如下图所示：

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。

文件过滤功能目前仅对采用 HTTP /FTP/SMTP/POP3/IMAP 协议的上传和下载生效。

3. 设置安全策略

进入页面：策略 >> 安全策略 >> 安全策略

点击<新增>添加文件过滤规则，源 IP 选择步骤 1 中添加的地址组，内容安全部分选择步骤 2 中设置的文件过滤规则。

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。

7.6 带宽策略

7.6.1 带宽策略介绍

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。防火墙提供了基于 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：策略 >> 带宽策略 >> 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。

源接口	选择规则控制的数据源端。
目的接口	选择规则控制的数据目的端。
受控地址组	选择 IP 地址组对象，以建立规则条目作用的 LAN 地址范围。
地址类型	选择地址组是源地址或者目的地址。
最大带宽	选择规则定义的数据流的最大上行带宽（单位为 Kbps）。
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。
生效时间	选择规则生效的时间，Any 表示立即生效。
添加到指定位置（第几条）	设置安全策略添加到指定位置。

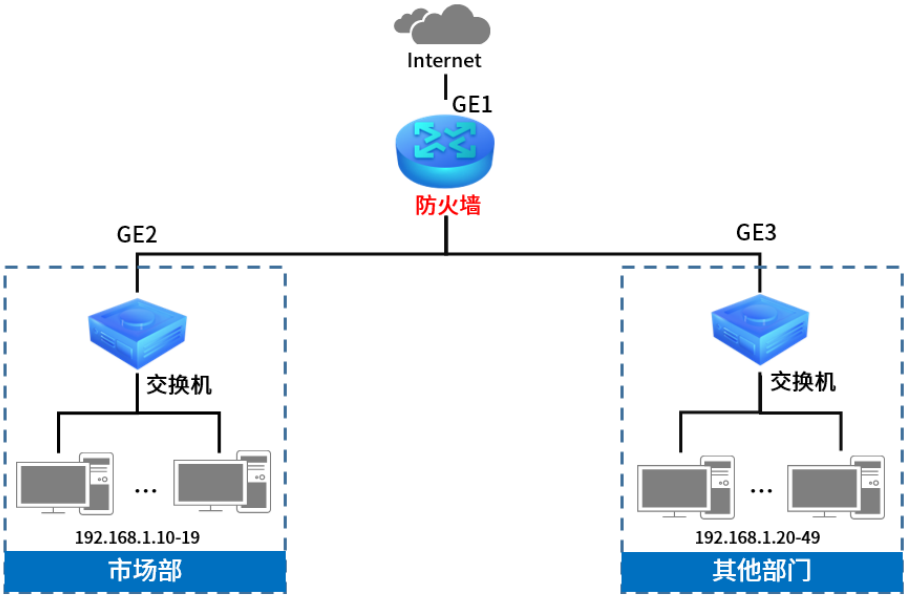
点击页面 ，查看更多页面设置参数信息。

7.6.2 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



➢ **设置方法**

1. 进入页面：网络 >> 接口设置 >> 接口设置，选择连接外网的接口，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<确定>（此处以自动获取 IP 地址上网为例）。

注意：

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

2. 添加地址组

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。进入页面：对象 >> 地址管理 >> 地址，点击<新增>，添加如下地址，点击<确定>。

同一页面，选择 地址组 ，点击<新增>，选择之前添加的地址，点击<确定>。

其他部门地址组的添加，也是相同操作方法。

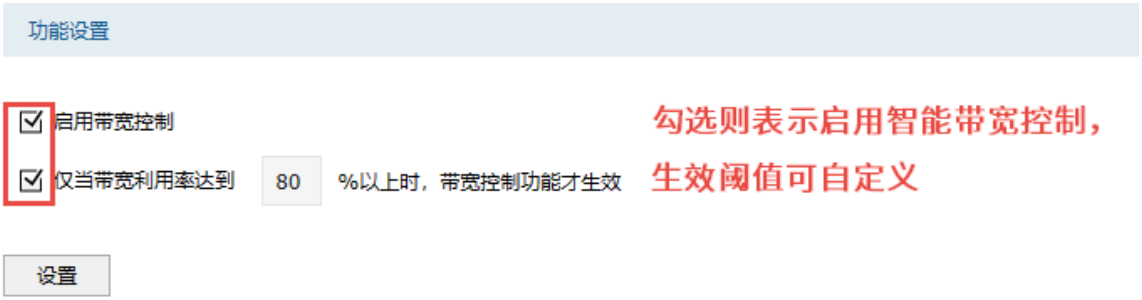
3. 设置带宽控制规则

进入页面：策略 >> 带宽策略 >> 带宽控制，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>，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。



至此，带宽控制设置完成，企业员工的电脑将按照带宽控制规则中的设置来使用网络。

7.7 连接数限制

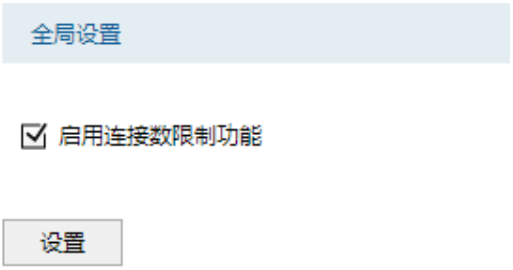
7.7.1 连接数限制

通信过程中，点与点之间建立的任何一个独立连接均会在防火墙上进行维护，从而确保通信数据正常转发。防火墙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：防火墙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：策略 >> 带宽策略 >> 连接数限制，勾选“启用连接数限制功能”，点击<设置>。



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 *6.1 地址管理*。

7.7.2 连接数监控

进入页面：策略 >> 带宽策略 >> 连接数监控，可查看已设置连接数限制规则的地址组内的 IP 地址已建立的连接数。

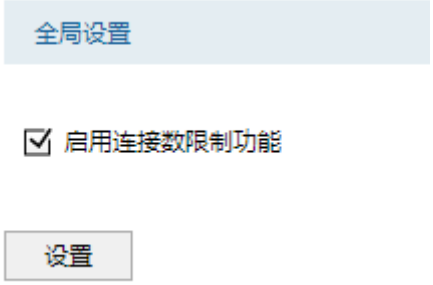
7.7.3 连接数限制配置实例

➢ **需求介绍**

某公司内网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：策略 >> 带宽策略 >> 连接数限制，勾选“启用连接数限制功能”。



点击<新增>，添加连接数限制规则。

说明:

- 如最大连接数设置为 300，所有受控用户的最大连接数均为 300。
- 普通上网应用，建议设置最大连接数为 200-300。
- 地址组设置请参考 *6.7 地址组的设置与管理实例*。

7.8 行为审计

7.8.1 记录策略命中日志

策略命中日志记录了每一条数据流所匹配到的安全策略以及执行的动作，了解策略生效情况。

进入页面：策略 >> 安全策略 >> 安全策略

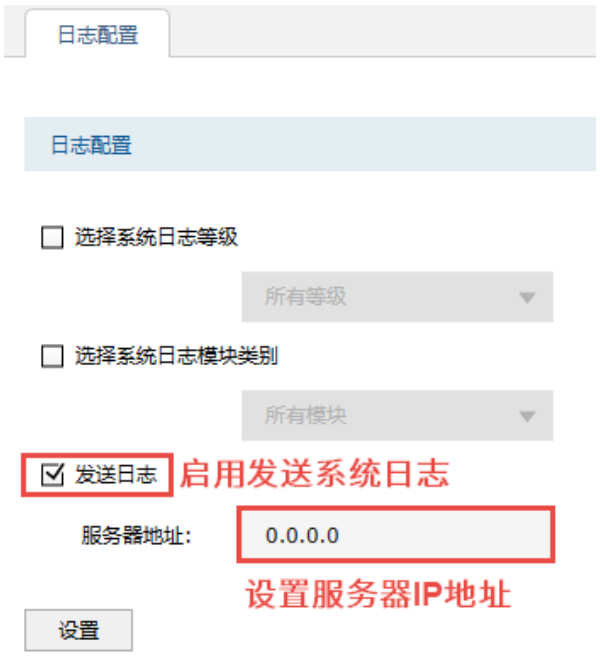
完成规则设置，并在内容安全模块选择相应的安全配置文件后，可启用“记录策略命中日志”，匹配到该条安全策略后，将记录到策略命中日志中。

进入页面：监控 >> 日志 >> 策略命中日志，可查看日志详情。

7.8.2 将系统日志发送到服务器

进入页面的方法：系统 >> 日志配置 >> 日志配置

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<设置>。


日志配置
日志配置
选择系统日志等级
所有等级
选择系统日志模块类别
所有模块
发送日志
启用发送系统日志
服务器地址:
0.0.0.0
设置服务器IP地址
设置

回目录

第8章　传输控制

8.1　路由设置

路由是指防火墙根据数据包的目的 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防火墙需要完成的最重要的工作。防火墙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，防火墙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。

防火墙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，通常指向与防火墙直接连接的网络，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：通过相互连接的防火墙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。

TP-LINK 防火墙支持策略路由和静态路由。

8.1.1 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。

进入页面的方法：网络 >> 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	可以选择服务类型，以确定选路规则条目的协议。当服务对应的协议为 TCP、UDP、TCP/UDP 时，还将确定源、目的端口范围。
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 ***6.1 地址管理***。
生效接口	设置数据包出接口。
强制	可以选择规则在出接口不在线时是否仍然执行。在所有出接口都不在线时，若强制，将转发到该规则中已连接的接口，如没有已连接的接口则丢包；若非强制，将跳过此规则。在任何其他情况下，将转发到在线的接口。
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。
状态	选择启用使规则生效。

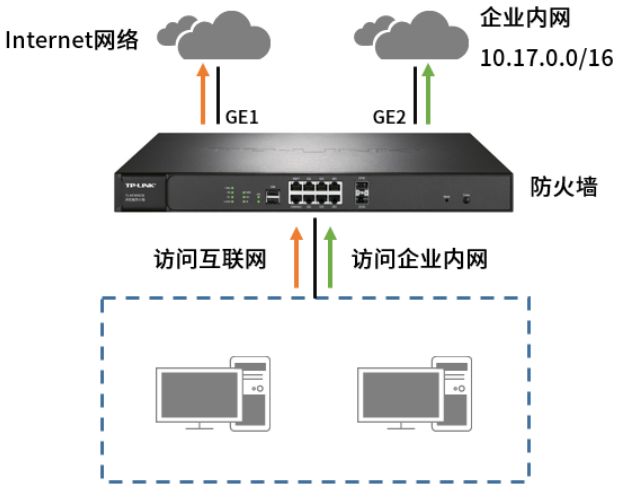
点击页面 ，查看更多页面设置参数信息。

8.1.2 策略路由配置实例

- **组网介绍：**

某企业接入了两条外网线路，GE1 口接运营商拨号宽带线路，用于连接互联网；GE2 口接企业内部专网，专网网络是 10.17.0.0/16，只能用于访问内网资源，无法访问互联网。

需要实现下接的终端既能访问互联网，也能正常访问企业内部网络。



- **配置步骤**

1. 进入页面：网络 >> 接口设置 >> 接口设置，选择接入内网网线的接口，设置企业内网 IP 地址。

2. 进入页面：对象 >> 地址 >> 地址，点击<新增>，添加内网 IP 和局域网 IP。

进入页面：对象 >> 地址 >> 地址组，点击<新增>，将内网 IP 和局域网 IP 分别添加到地址组中：

3. 进入页面：网络 >> 路由设置 >> 策略路由，点击<新增>，进行设置。

1） 设置规则：访问专网 10.17.0.0/16 的数据只能从 GE2 口转发，如下图：

2） 再设置一条规则：访问外网的数据只能从 GE1 口转发，如下图：

注意：

- 策略路由规则时由上往下逐条匹配的，两者规则必须按照以上添加顺序添加。

至此，策略路由功能设置完成，局域网网段的终端访问企业内网或访问 Internet 都将按照规则来实现。

8.1.3 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：网络 >> 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。一般不修要修改。
可达性	路由条目的实际生效情况。 当出接口与下一跳相互匹配时，显示<可达>; 当出接口与下一跳不匹配时，或者条目被禁用时，显示<不可达>。 仅当条目“可达”时，才是生效的。

点击页面 ，查看更多页面设置参数信息。

8.1.4 IPv6 静态路由

➢ **配置方法：**

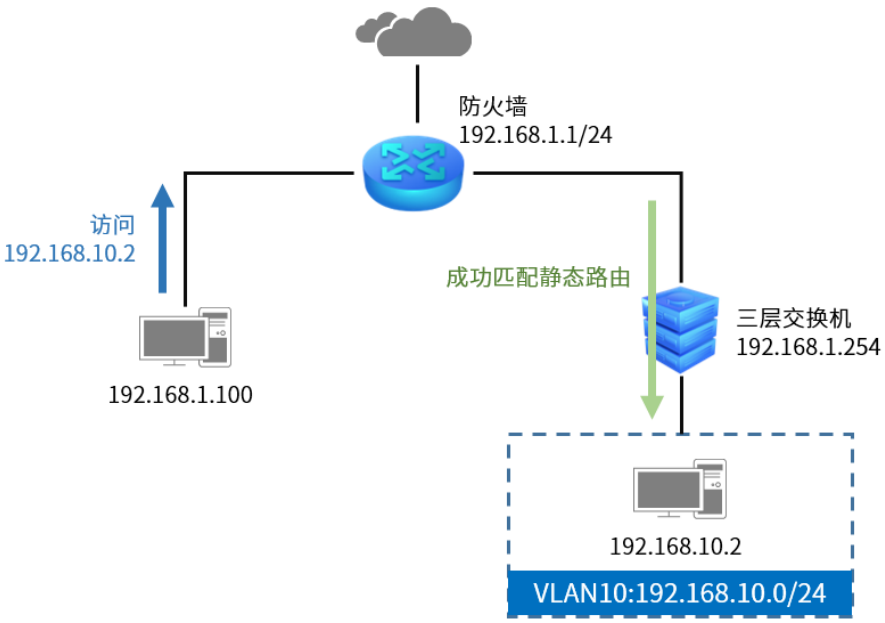
进入页面：网络 >> 路由设置 >> IPv6 静态路由，点击<新增>，设置静态路由规则，配置完成后，勾选“启用”，点击<确定>。

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	路由条目的优先级，其数值越低优先级越高。默认值为 1，一般不需要修改。
可达性	路由条目的实际生效情况。 当出接口与下一跳互相匹配时，显示<可达>； 当出接口与下一跳不匹配，或者条目被禁用时，显示<不可达>。 仅当条目“可达 时，才是生效的。

8.1.5 静态路由配置实例

➢ **需求介绍**

某企业使用 TP-LINK 防火墙，下接三层交换机，交换机划分了 VLAN10，需要实现防火墙 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**

进入页面：网络 >> 路由设置 >> 静态路由，点击<新增>，进行设置。

8.1.6 系统路由

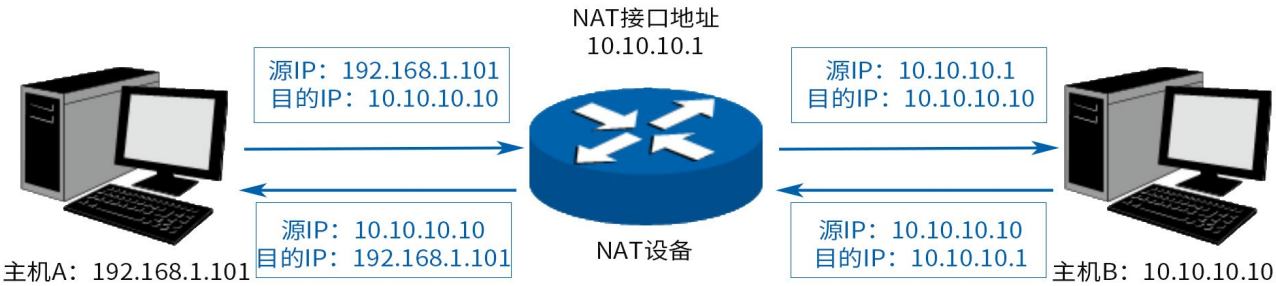
进入页面：网络 >> 路由设置 >> 系统路由，可查看当前的系统路由表。点击<刷新>获取最新的系统路由表。

序号	目的地址	子网掩码	下一跳	出接口	Metric
1	127.0.0.0	255.0.0.0	0.0.0.0	loopback	0
2	192.168.1.0	255.255.255.0	0.0.0.0	MGMT	0

8.2 NAT 策略

8.2.1 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。

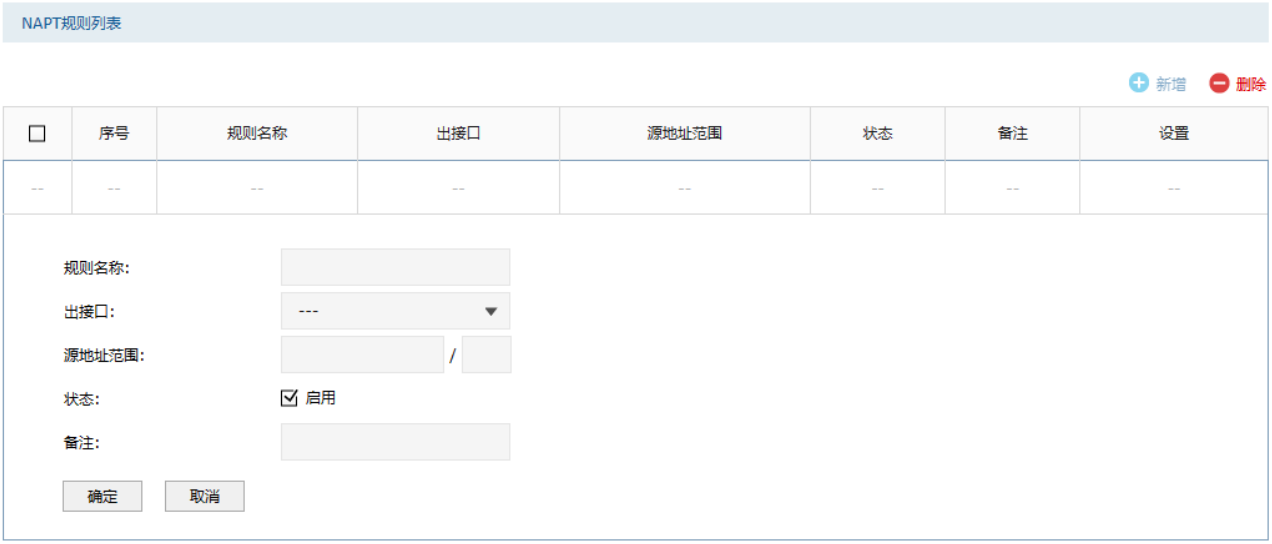
TP-LINK 防火墙提供一对一 NAT 和 NAPT 两种应用。

8.2.2 NAPT

当局域网中多台设备需要访问广域网，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： 策略 >> NAT 策略 >> 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	备注	设置
1	1	GE1	192.168.1.0/24	已启用	---	
2	2	GE2	192.168.1.0/24	已启用	---	
3	3	GE1	192.168.0.0/24	已启用	---	
4	4	GE1	192.168.3.52/32	已启用	---	

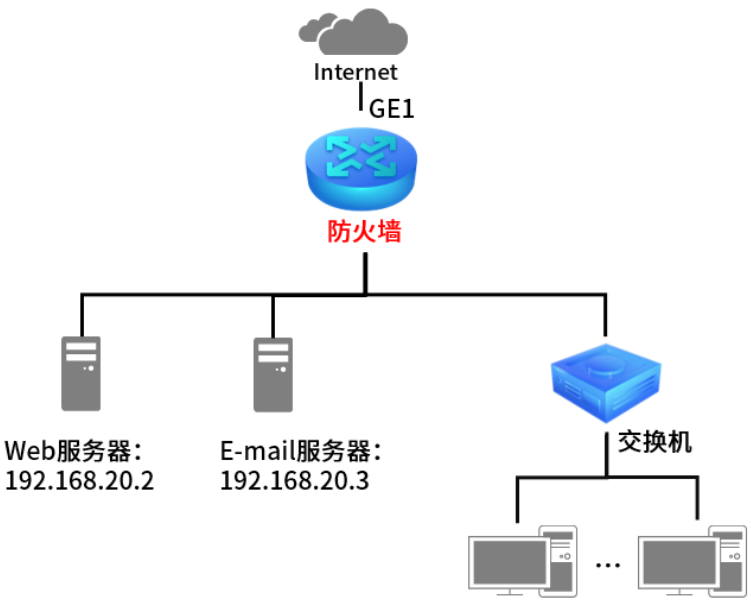
- 序号为 1 和 2 的规则表示 192.168.0.0/24 子网中的计算机通过“GE1”和“GE2”接口访问外部网络时均需要进行 NAPT 地址转换，共用接口的 IP 地址上网；
- 序号为 3 的规则表示 192.168.0.0 子网中的计算机通过“GE1”接口访问外部网络时需要进行 NAPT 地址转换，共用接口的 IP 地址上网；

- 序号为 4 规则表示计算机 192.168.3.52 通过“GE1”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“GE1”接口转发的数据均做地址转换。

8.2.3 NAPT 配置实例

➢ **组网介绍**

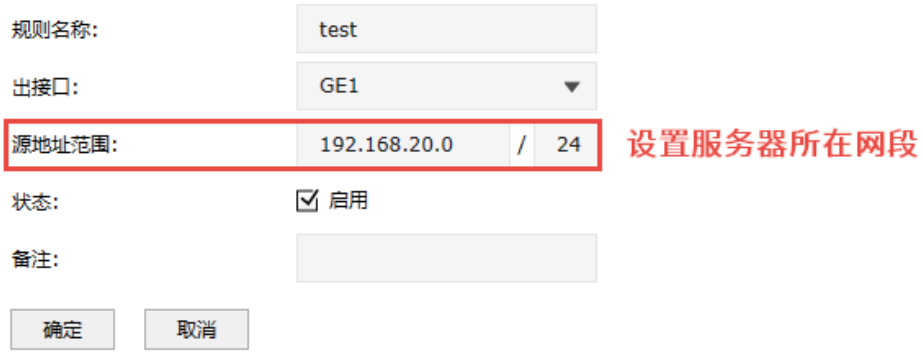
某公司内网上搭载了 Web 服务器和 E-Mail 服务器需要对外开放，Web 服务器的内网 IP 为 192.168.20.20，E-Mail 服务器的内网 IP 为 192.168.20.30，其余主机不使用 192.168.20/24 网段。拓扑如下：



➢ **配置步骤**

1. 进入页面：策略>> NAT 策略 >> NAPT，点击<新增>。

2. 设置 NATP 规则。

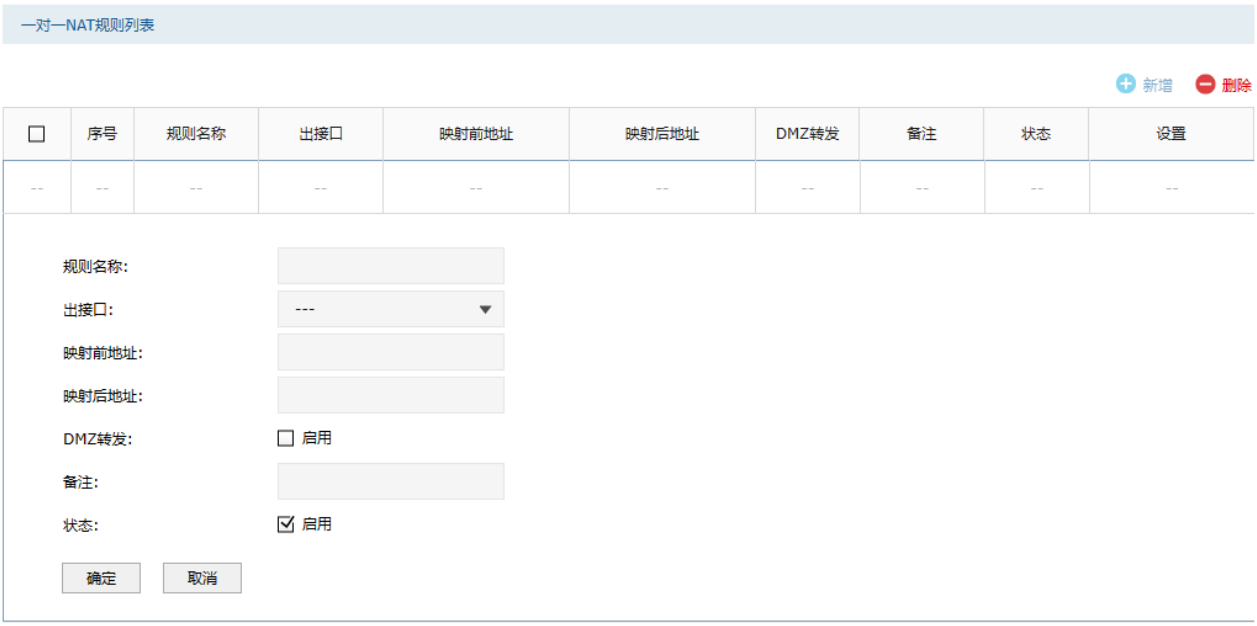


8.2.4 一对一 NAT

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： 策略 >> NAT 策略 >> 一对一 NAT，点击<新增>，配置完成后，点击<确定>。



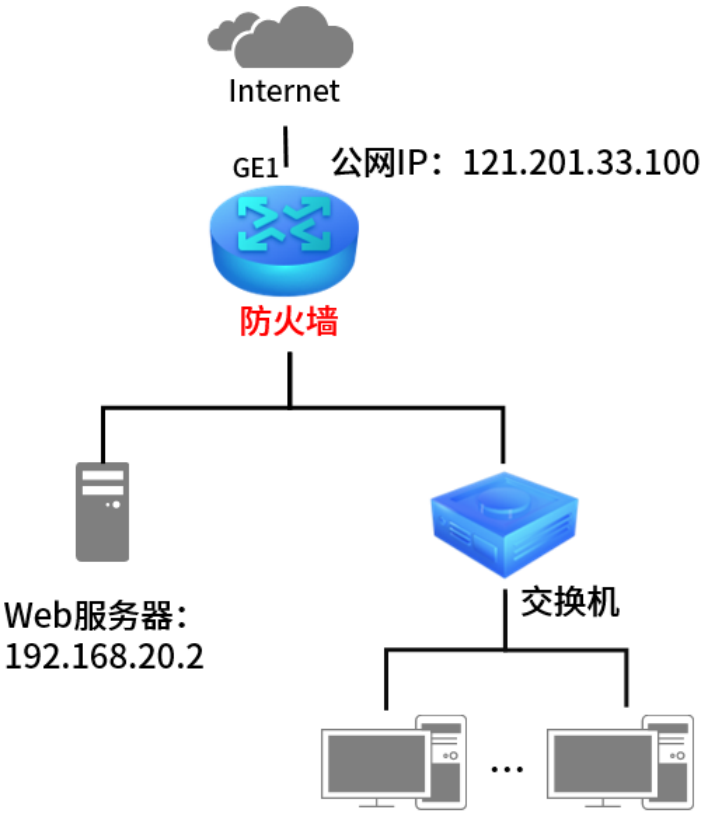
出接口	一对一 NAT 规则只允许选择静态 IP 的出接口。 当出接口从静态 IP 更改为非静态 IP，对应出接口的已配置的一对一 NAT 规则会被自动禁用。
映射前/后地址	规则生效的地址对象。映射前/后地址不能为各个接口的广播，网段和接口 IP 地址。

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，防火墙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。

8.2.5 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：

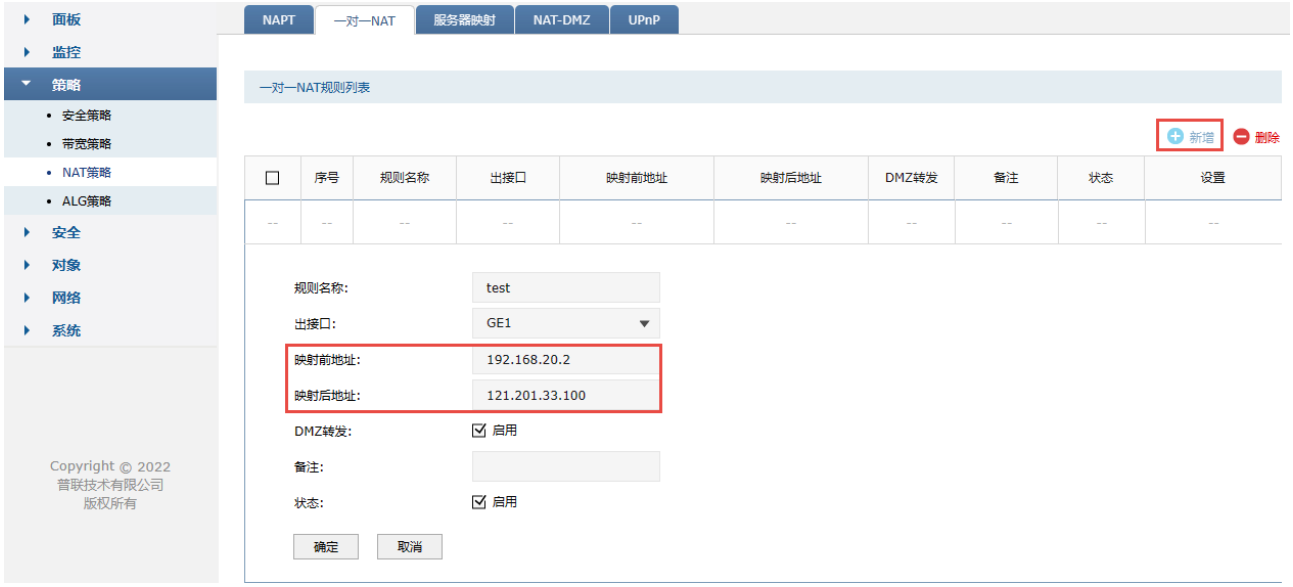


➢ **配置步骤**

1. 进入页面：网络 >> 接口设置，选择连接公网的 GE1 口，点击<>，将其接口连接方式为固定 IP 地址，地址为 121.201.33.100。

2. 进入页面：策略 >> NAT 策略 >> 一对一 NAT，点击<新增>。

3. 设置一对一 NAT 规则，出接口选择第 1 步中设置的接口。



8.3 NAT-DMZ

8.3.1 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：策略 >> NAT 策略 >> NAT-DMZ。点击<新增>，选择出接口，设置主机地址，点击<确定>。

8.3.2 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，默认网关为防火墙的管理地址。
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：策略 >> NAT 策略 >> NAT-DMZ，点击<新增>，添加如下规则，点击<确定>。

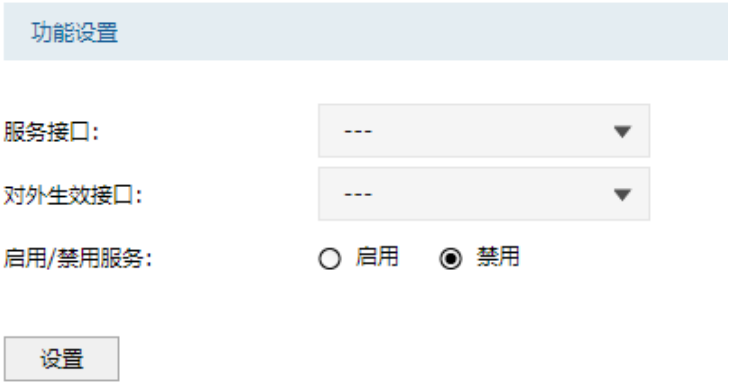
8.3.3 UPnP

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，防火墙开启了 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防火墙上打开相应的端口，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：策略 >> NAT 策略 >> 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。
服务接口	可以指定一组接口集，该集合包含的接口作为 UPnP 的内部接口。

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 协议向防火墙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：

- 应用时不仅要在防火墙上启用 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。

8.4 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，防火墙均会对数据包做 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防火墙 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	用于防火墙使用 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**

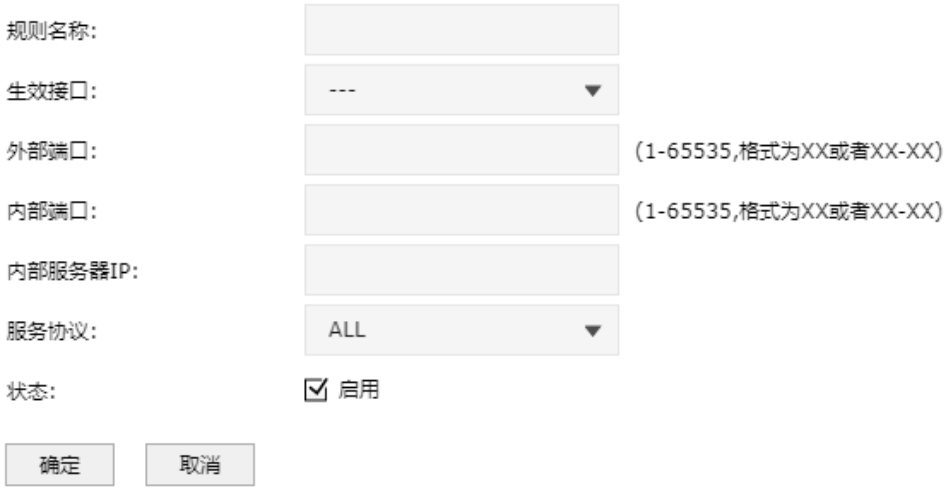
进入页面： 策略 >> ALG 策略 >> ALG 服务，勾选对应 ALG 服务，点击<设置>。

8.5 虚拟服务器

8.5.1 服务器映射

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：策略 >> NAT 策略 >> 服务器映射。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	防火墙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。

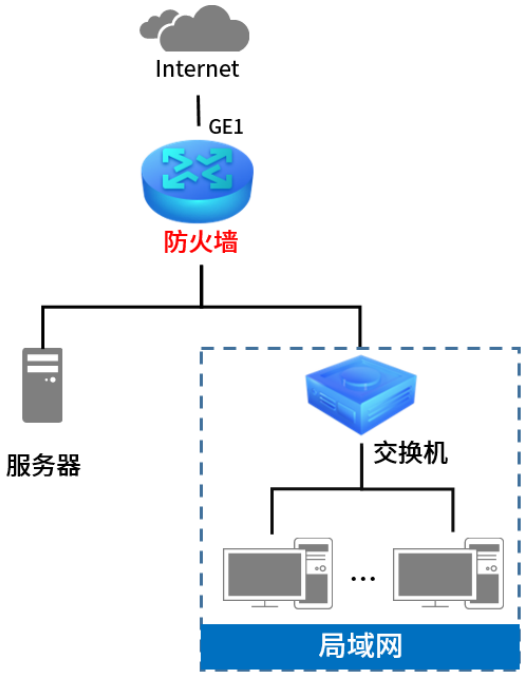
服务协议	触发条目生效的协议类型。选择 ALL 表示所有协议均生效。

点击页面 ，查看更多参数信息。

8.5.2 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。

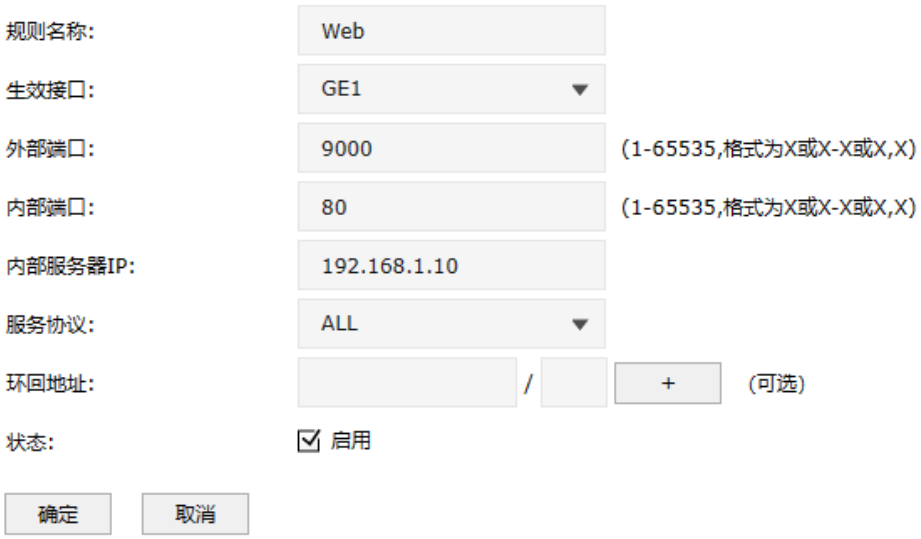
➢ **配置步骤**

1. 确认服务器搭建成功：

服务器	服务器设置为固定 IP 地址，默认网关为防火墙的管理地址。
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：策略 >> NAT 策略 >> 服务器映射，点击<新增>，设置映射规则，设置完成后，点击<确定>。

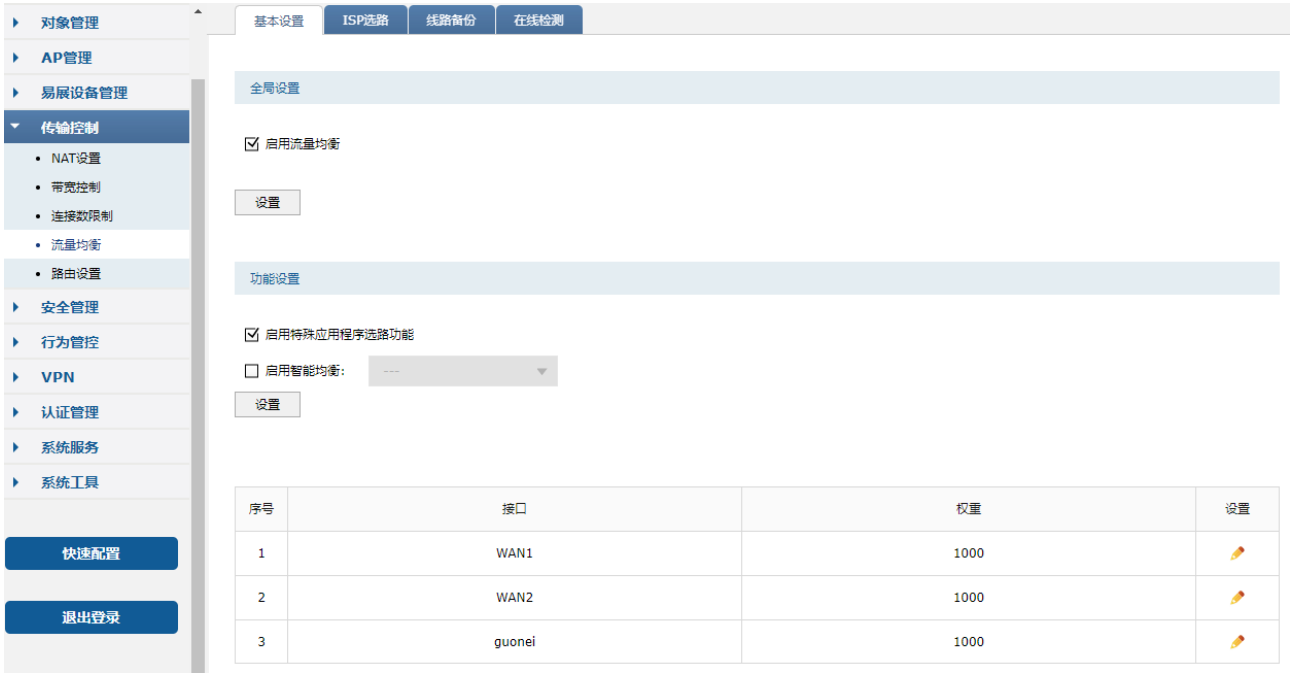


8.6 流量均衡

流量均衡决定了防火墙每个接口的数据流量占比。

8.6.1 基本设置

进入页面：网络 >> 路由设置 >> 流量均衡，可进行流量均衡的基本设置。



启用流量均衡	流量均衡的全局开关，勾选以启用流量均衡功能。
启用特殊应用程序选路功能	选中后，设备把属于同一个网络应用的多条连接通过同一个出接口转发，避免多出接口下由于该应用的多条连接通过不同处接口转发导致应用异常的问题。例如某内网主机访问外网服务器，启用特殊应用程序选路后，可以保证该内网发往服务器的所有数据通过同一个出接口转发，避免因流量均衡导致数据通过多个出接口转发而引起服务异常。
启用智能均衡	可以在复选框中选择需要启用智能均衡的接口。

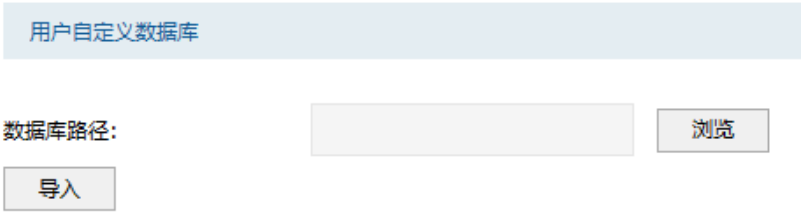
注意：

- 若要使智能均衡生效，请先到页面：网络 >> 接口设置及 网络 >> PPTP/L2TP >> 客户端 设置各接口的上下行带宽。
- 智能均衡中各接口的流量比等于各接口的带宽比。

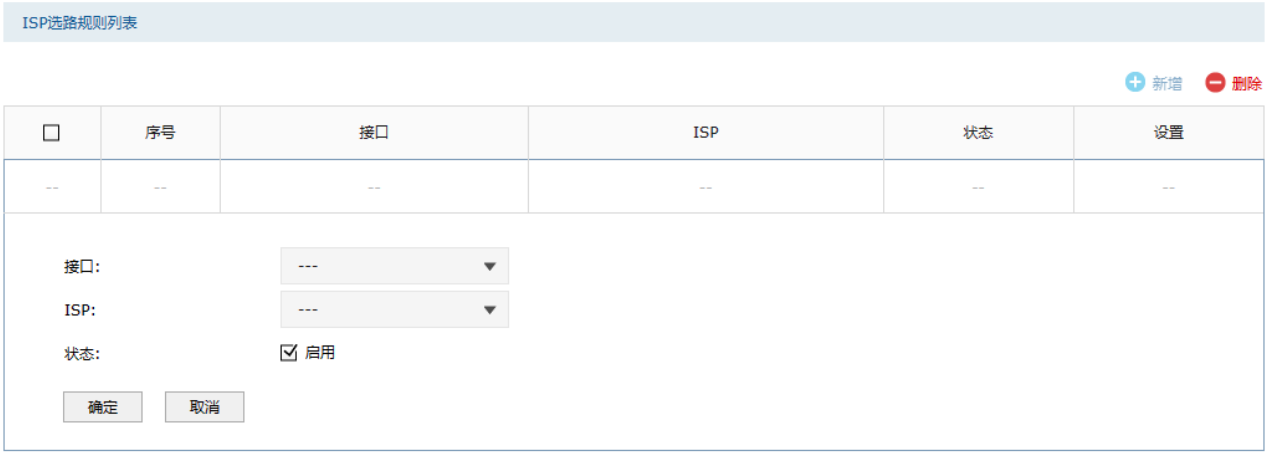
8.6.2 ISP 选路

进入页面：网络 >> 路由设置 >> ISP 选路，可进行 ISP 选路设置，导入 ISP 数据库。

启用 ISP 地址段选路功能	根据 ISP 进行选路。
导入	可以导入 ISP 数据库对系统预设的 ISP 选路进行升级。



导入　　自定义数据库文件格式为每行由“IP/mask”组成，如“12.12.12.12/24”，总个数不超过 2048 条。文件格式为 txt 格式。



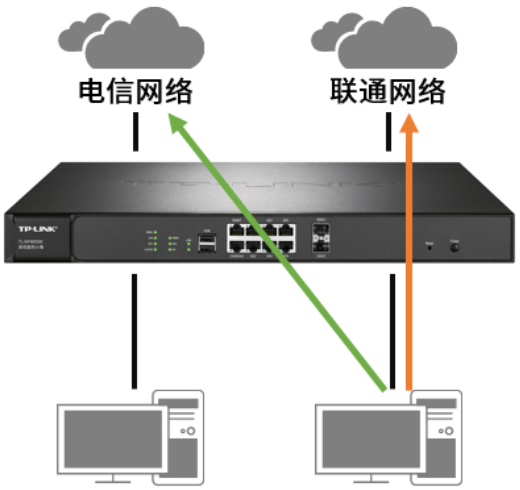
接口　　选择 ISP 选路的接口。

ISP　　选择 ISP（Internet Service Provider，网络提供服务商）。

状态　　选择此规则是否启用。

8.6.3 ISP 选路设置指南

多接口防火墙接入多条宽带线路可以实现带宽叠加、线路备份的作用，从而提高网络的稳定性。但是，如果接入的多条宽带线路不是同一运营商（宽带服务商），则可能引起访问瓶颈（例如访问电信网络的数据走联通网络），导致网络延迟大、丢包等现象。多接口防火墙的 ISP 选路功能可以避免以上问题发生，实现访问对应 ISP 网络的数据走正确的出接口。



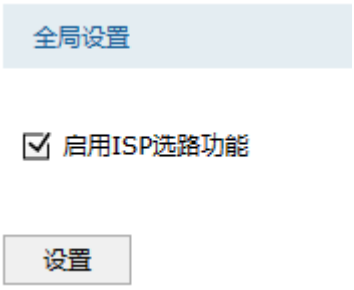
本节介绍防火墙的 ISP 选路功能设置方法。

➢ **需求介绍**

某企业使用 TP-LINK 防火墙，连接两条宽带线路，GE1 使用电信宽带，GE2 是联通宽带，需要实现所有访问电信服务器的流量走电信线路，所有访问联通服务器的流量走联通线路。

➢ **设置方法**

1. 登录到防火墙 WEB 管理界面，进入页面： 网络 >> 路由设置 >> ISP 选路，在全局设置模块，勾选“启用 ISP 选路功能”，点击<设置>。



2. 进入页面：网络 >> 接口设置 >> 接口设置，分别配置 GE1 和 GE2 的上网参数。
3. 进入页面：网络 >> 路由设置 >> ISP 选路，在 ISP 选路规则列表，点击<新增>，分别将 GE1 和 GE2 接口的 ISP 设置为电信和联通，并启用规则。

目前 TP-LINK 防火墙将国内 ISP 分为 电信 、 联通 、 教育网 、 移动 和 国内其他 （如长城宽带、广电宽带等）这几类，国外的 ISP 则放在 其他 类别中。用户也可以进入页面：网络 >> 路由设置 >> ISP 选路，导入 ISP 数据库及用户自定义数据库。

至此，ISP 选路功能设置完成，访问电信站点的流量由电信线路转发，访问联通站点的流量由联通线路转发，实现更快速地访问网络资源。

8.6.4 线路备份

防火墙的线路备份功能可以在主接口出现异常时，防火墙能及时地把数据切换到备接口上，为网络稳定性提供强大保证。

进入页面：网络 >> 路由设置 >> 线路备份，点击<新增>，可进行线路备份设置。选择主接口、备接口以及备份模式，勾选 启用 ，点击<确定>。

说明：

- 定时备份：在设置的生效时间内，所有上网数据均由备接口转发。生效时间设置请前往页面：对象 >> 时间段。
- 故障备份：主接口未联网时，所有上网数据均由备接口转发。

8.6.5 在线检测

进入页面：系统 >> 高可靠性 >> 在线检测，可查看设置接口是否已经连接外网。

点击接口对应<✎>按钮，可设置不同的检测方式。

接口名	进行在线检测的接口。对所有参与流量均衡的接口，均会进行在线检测。
检测模式	选择外网连接状态的检测方式。 自动模式：通过使用在设置接口时设置的 DNS 服务器进行 DNS 检测，判断是否连接外网。 手动模式：通过使用在本页面上手动设置的 DNS 服务器和 IP 地址进行 DNS 检测和 PING 检测，判断是否连接外网。 永远在线：不进行检测，在页面上永远显示为在线状态。
PING 检测	可以指定一个 IP 地址，让对应的接口 Ping 该地址，从而判断是否连接外网。只能在手动模式下设置。
DNS 检测	指定一个 DNS 服务器的 IP 地址，让对应接口通过该 DNS 服务器使用默认的域名进行 DNS 查询，从而判断是否连接外网，只能在手动模式下设置。

8.6.6 多带宽均衡配置实例

防火墙连接多条宽带的目的主要有以下 2 个：

1）增加带宽：上网主机可以通过任意宽带上网，从应用角度讲，相当于一条更高速的宽带。

2）冗余备份：如果其中一条宽带出现故障，可以使用其他宽带上网，保证网络畅通无中断。

➢ **需求介绍**

某企业接入两条电信的线路，一条 500M，另一条 300M。需要充分利用两条线路的带宽。

➢ **工作原理**

在接入多条宽带时，多接口企业防火墙可以通过设置流量均衡策略，充分利用各接口的带宽。均衡模式分为连接均衡和带宽均衡两种。

1. 连接均衡：根据总连接数合理分配给各个接口，保证每个接口利用率相同（防火墙默认设置为连接均衡）。
2. 带宽均衡：各条宽带的流量比等于设置的各接口带宽比。如果接口 1 和接口 2 带宽比为 5：3，那么启用“带宽均衡”后，通过接口 1 和接口 2 的实际流量比约为 5：3。

➢ **设置方法**

1. 进入页面：网络 >> 路由设置 >> 基本设置，勾选“启用智能均衡”，勾选 GE1 和 GE2，点击<设置>。

2. 进入页面：网络 >> 接口设置 >> 接口设置，设置 GE1 和 GE2 接口的上下行带宽。智能均衡中各接口的流量比等于各接口的带宽比。

至此，流量均衡功能设置完成。如果玩游戏、浏览网页和服务器的行为较多，建议选择连接均衡模式；如果看视频、下载和上传大文件的行为较多，建议选择带宽均衡模式。

两种模式各有优缺点，建议根据实际使用场景选择合适的均衡模式。

回目录

第9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三层路由网关上完成，所以对于用户来说是透明的。防火墙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。

9.1　IPSec

9.1.1 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：网络 >> IPSec >> IPSec 安全策略，勾选 启用 ，点击<设置>。

在 IPSec 安全隧道列表，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。 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。 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。
本地 ID	仅仅在本地 ID 类型选择 NAME 的时候生效，用于存储用户输入对应的字符串。
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。
对端 ID	仅仅在对端 ID 类型选择 NAME 的时候生效，用于存储用户输入对应的字符串。
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。传输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。

9.1.2 IPSec 安全联盟

可以查看当前建立的安全联盟。

进入页面的方法：网络 >> IPSec >> IPSec 安全联盟

点击<刷新>，可更新最新的安全联盟列表。

SPI	显示安全联盟的 SPI（Security Parameter Index，安全参数索引），注意每一个安全联盟的 SPI 都不相同。
方向	显示安全联盟的方向（in：流出/out：流出）。
隧道两端	显示安全联盟两端的网关地址。
数据流	显示安全联盟两端的子网范围。

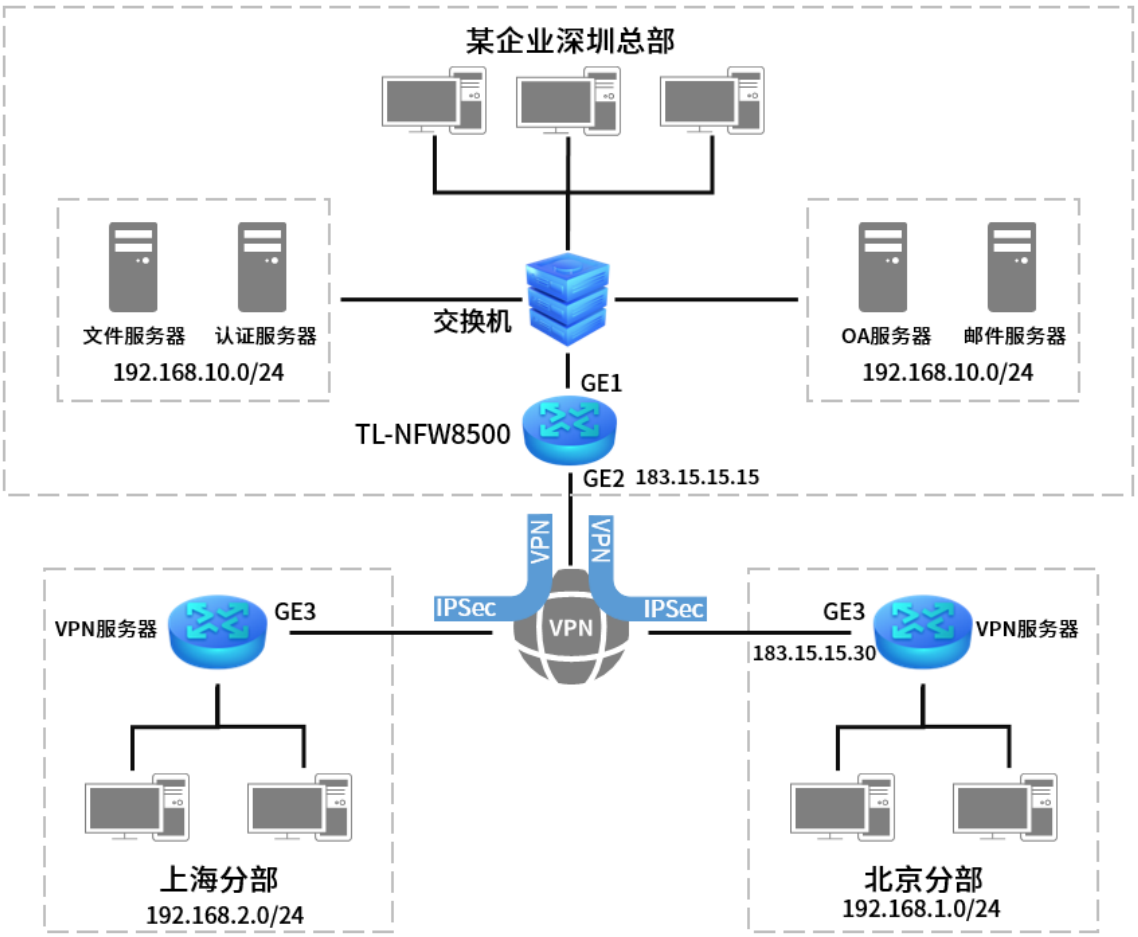
点击页面，查看更多页面参数信息。

9.1.3 IPSec 配置实例

VPN 功能的实用性毋庸置疑，公司总部与分布之间搭建安全隧道来实现内网资源的安全共享等需求都可以通过 VPN 来实现。与路由器配置方法的不同，防火墙不仅需要进行 VPN 相关配置，还需要开放 VPN 相关的安全策略。

- **需求介绍**

某公司总公司位于深圳，在上海、北京两地有分公司，现需要通过防火墙的 VPN 功能，在总部与分布之间搭建安全隧道，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-NFW8500 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“192.168.10.0/24”，GE2 口为公网 IP：183.15.15.15；北京分公司为“192.168.20.0/24”，GE3 口为公网 IP：183.15.15.30；上海分公司为“192.168.30.0/24”。拓扑如下：



- **配置方法**

防火墙在使用设备本身的某个功能时，首先要开启对应功能，其次需要考虑该功能需要实现所需要开放的服务或者权限，以 VPN 为例，在设置好 VPN 以后需要开放的服务或权限包括：允许外网设备与防火墙建立 VPN、允许外网访问内网服务器、允许外网通过防火墙进行代理上网等，具体配置方法如下：

- **首先设置深圳总部 TL-NFW8500。**

1. 设置 GE2 口网络参数。

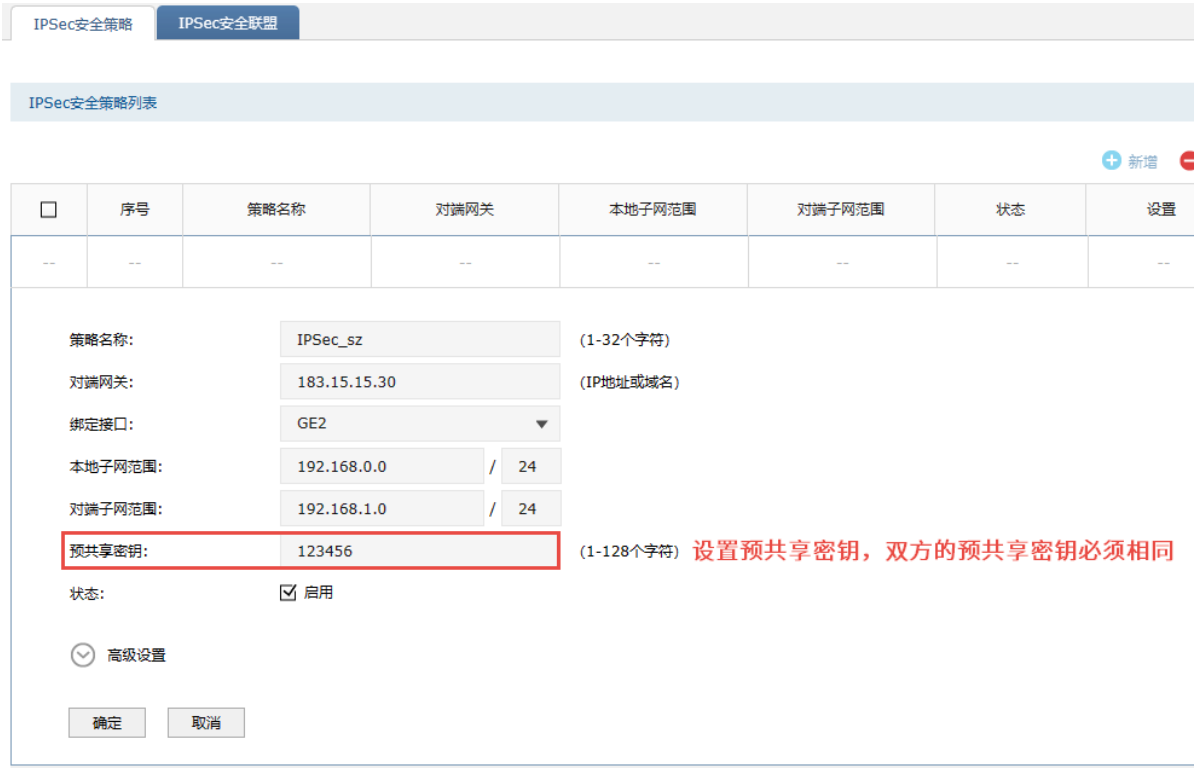
   进入页面：网络 >> 接口设置 >> 接口设置，设置 GE2 口网络参数以及该线路的上下行带宽值。此例中设置 GE2 口为固定 IP：183.15.15.15。

2. **配置 IPSec 安全策略基本设置：**

   进入页面：网络 >> IPSec >> IPSec 安全策略，进入 IPSec 安全策略标签页，点击<新增>，设置 IPSec 安全策略。

   设置开启对应接口的 IPSec 安全策略，对端网关可以填写对端的 IP 地址或者域名（如此例中北京分部对端 IP 为 183.15.15.30），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，绑定要对接 VPN 的上网接口（此例中为 GE2），本地子网和对端子网范围都按照实际需求填写。

   填写预共享密钥（对端也必须填写完全相同的密钥）。

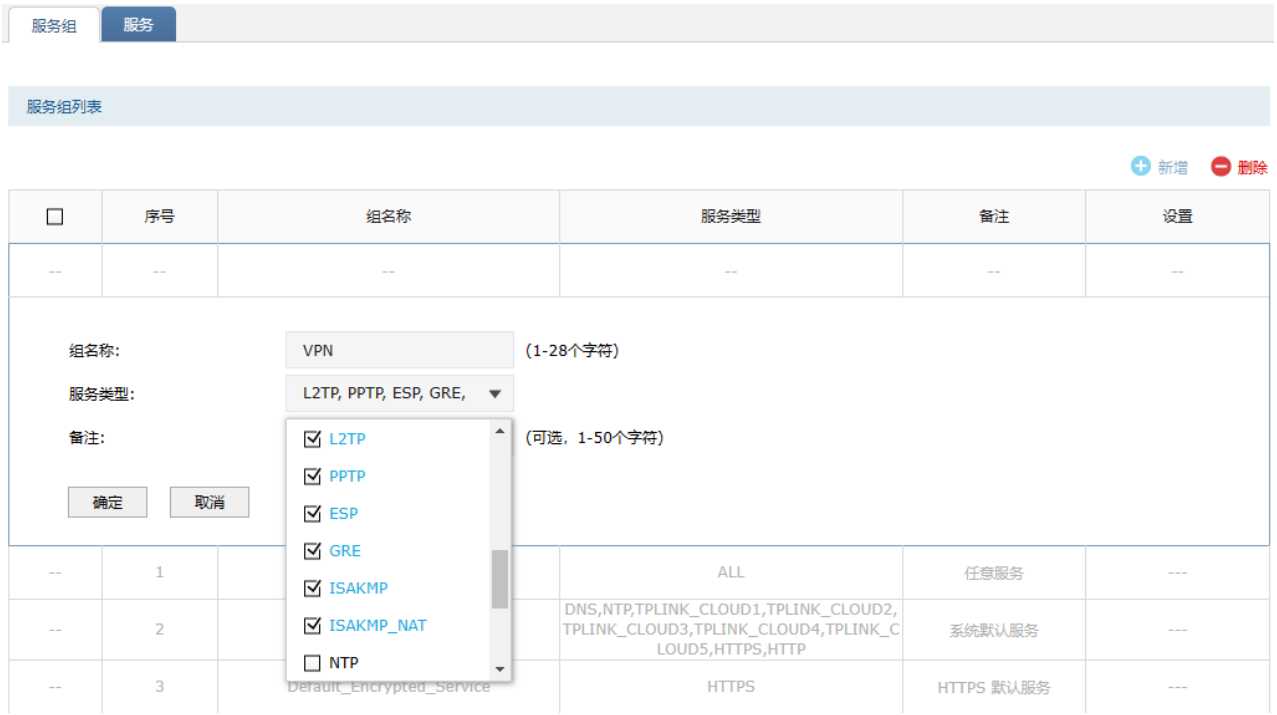


配置 IPSec 安全策略高级设置：

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。

3. 进入页面：对象 >> 服务 >> 服务组，设置 VPN 服务组并绑定防火墙内置的 VPN 相关服务。

   此处为了配置方便，可绑定三类 VPN 相关的服务。



4. 设置允许 VPN 拨号的安全策略。

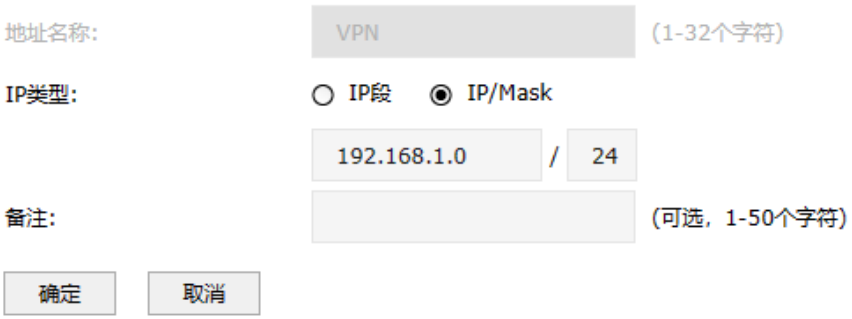
   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，选择 local 到 untrust 安全区域。源 IP 为 WAN 口的 IP（可以在页面“对象 >> 地址 >> 地址组”中添加对应地址的地址组，此例中为 GE2 口的地址），目的 IP 是对端 WAN 口的公网 IP（此处填写的所有 IP），服务组选择上一步中设置的“VPN”，动作选择“允许”。

IPSec VPN 不区分服务器端和客户端，对端防火墙的设置如前文所述即可。

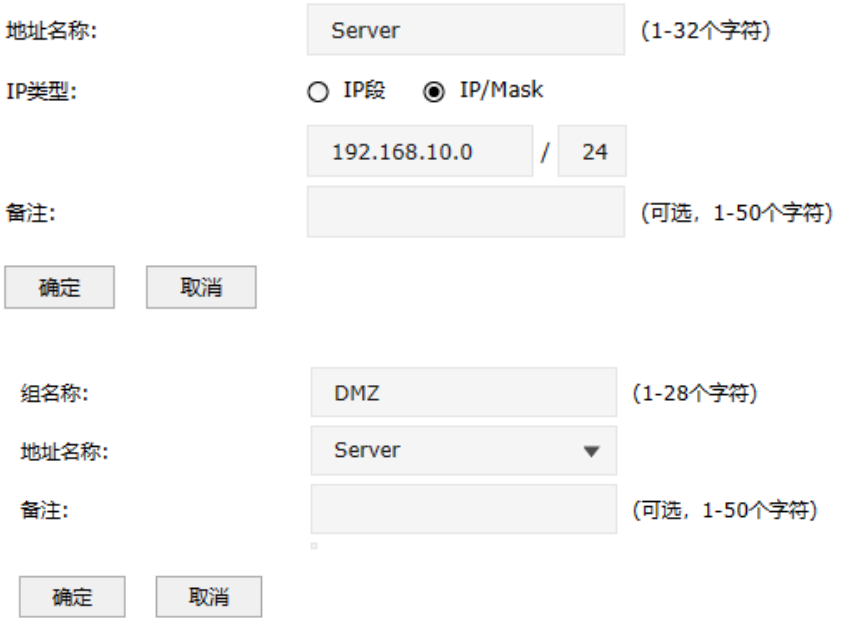
此时，在对端设置正确时，在 IPSec 安全联盟中可以查看到已搭建成功的 VPN 隧道。

序号	名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法
1	IPsec_bj	3222533904	in	183.15.15.30<--183.15.15.15	192.168.1.0/24 <-- 192.168.0.0/24	ESP	--	MD5	3DES
2	IPsec_bj	3240553103	out	183.15.15.30-->183.15.15.15	192.168.1.0/24 --> 192.168.0.0/24	ESP	--	MD5	3DES

5. 进入页面：对象 >> 地址 >> 地址/地址组，添加步骤 1 中设置的对端子网对应的地址段到“VPN”地址组。



将服务器对应的地址段添加到“DMZ”地址组。



6. 如果要允许对端的 VPN 用户访问内网服务器，需要开放相应的安全策略：

进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择从 untrust 到 DMZ，源地址选择上一步骤中设置的“VPN”，目的地址为服务器所在的“DMZ”，动作为“允许”。

7. 如果要允许内网终端访问位于外网的对端内网服务器，需要开放相应的安全策略：

进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择从 trust 到 untrust，源地址为允许访问服务器的内网的地址（此处设置为“neiwang”），目的地址为位于外网的对端内网服务器对应的地址组（此处为方便设置为所有 IP 地址“IPGROUP_ANY”），动作为允许，同时还可以设置 URL 过滤、反病毒等内容安全相关的检查策略。

IPSec VPN 不区分服务器端和客户端，对端防火墙的设置如前文所述即可。

➢ **NAT 下的 IPSec VPN 配置**

VPN 两端防火墙接口需要公网 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：

- VPN 两端防火墙接口需要公网 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。

9.2 L2TP

防火墙提供多类 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 。

9.2.1 L2TP 服务器

进入页面：网络 >> 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。

点击页面 ，查看更多页面设置参数信息。

9.2.2 L2TP 客户端

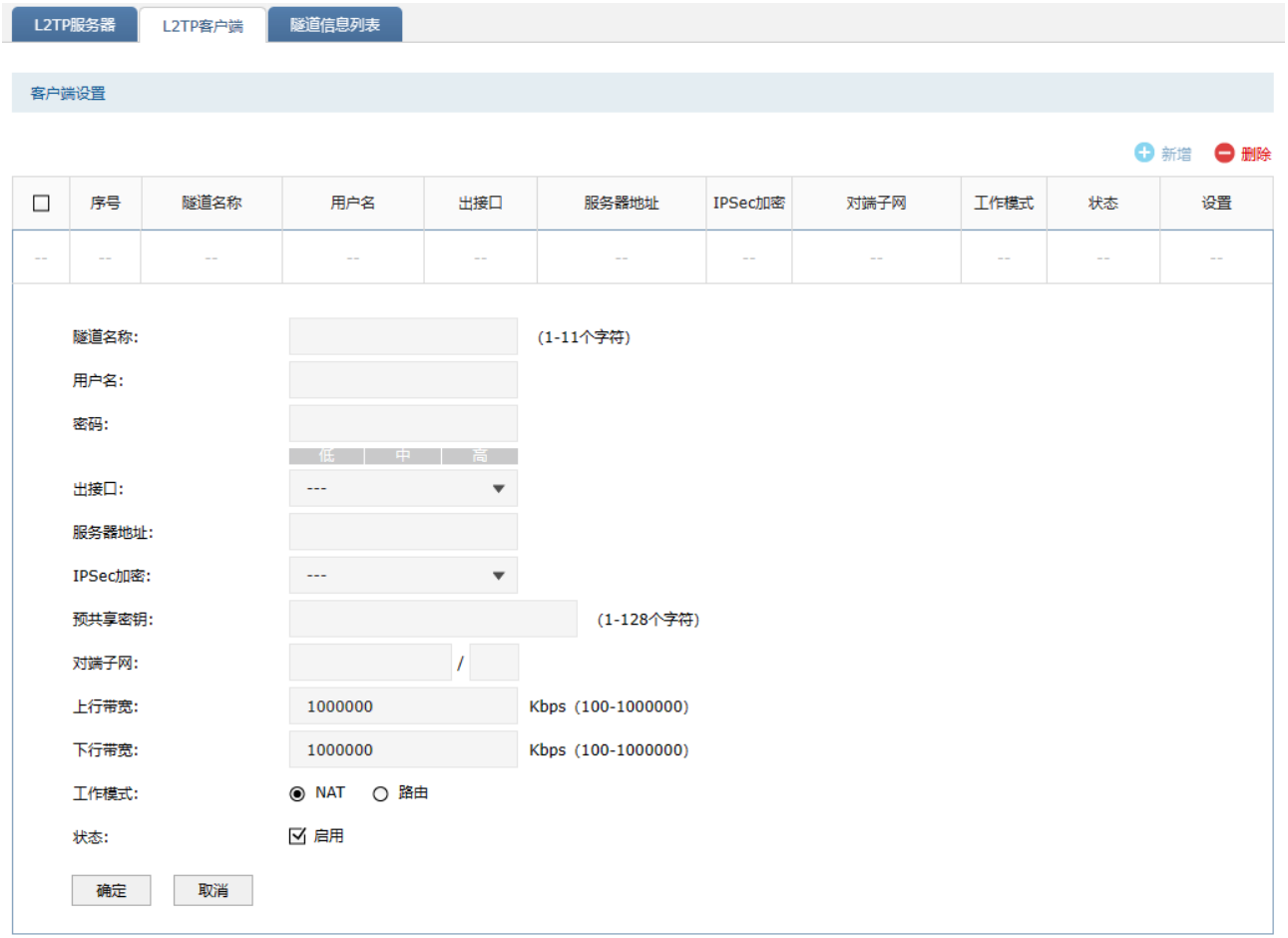
进入页面：网络 >> L2TP >> L2TP 客户端，进行全局设置和 L2TP 服务器设置。

- **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	防火墙会根据上下行带宽进行流量均衡的计算。
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）。 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。

9.2.3 隧道信息列表

可以获得 L2TP 隧道的信息。

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

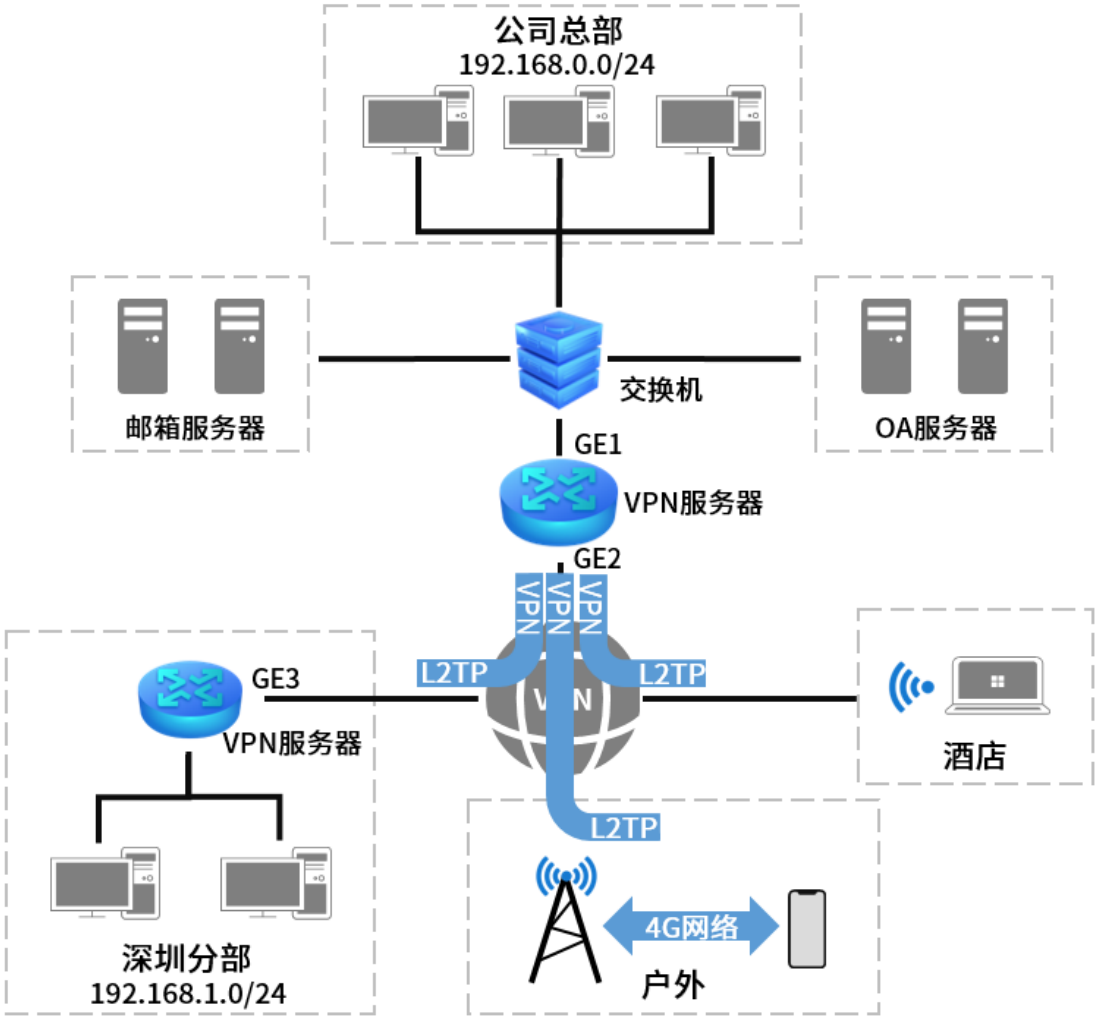
9.2.4 L2TP 配置实例

➢ **需求介绍**

某公司的总部与分部均使用 TP-LINK 防火墙产品。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	123/123456
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**

服务器端的设置（以 TL-NFW8500 为例）

1. 进入页面：对象 >> IP 地址池 >> IP 地址池，新增隧道地址池（L2TP VPN 隧道通信时使用的 IP 地址）。该地址池应与防火墙各接口 IP 不在同一网段。

2. 进入页面：网络 >> VPN 用户管理 >> VPN 用户管理，进行用户管理配置，点击<新增>。设置用于 VPN 通讯的虚拟本地地址，选择上一步骤中设置的 IP 地址池，设置 DNS 服务器，组网模式选择站点到站点，填入实际的对端子网。

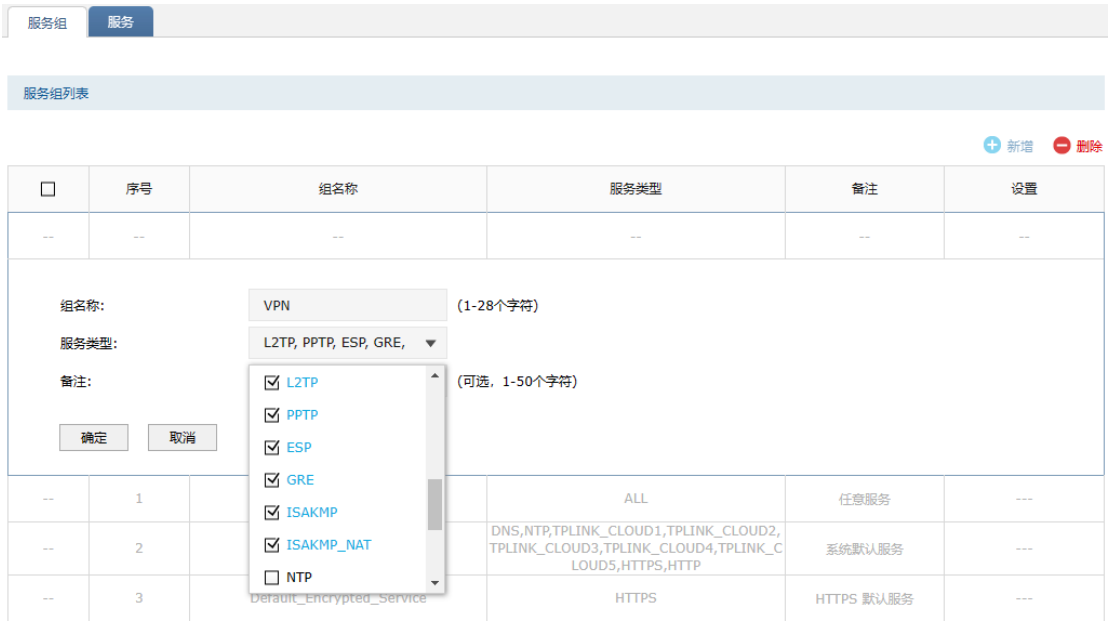
用户名	客户端与服务器端建立连接的用户名。
密码	客户端与服务器端建立连接的密码。
服务类型	L2TP：本用户只用于 L2TP； PPTP：本用户只用于 PPTP； 自动：本用户既可用于 L2TP 也可用于 PPTP。
本地地址	VPN 隧道的本地虚拟 IP 地址。
地址池	选择上一步骤中建立的隧道地址池。
组网模式	PC 到站点：拨入的客户端时个人用户，往往由单个计算机拨入实现远端计算机与本地局域网的通信； 站点到站点：拨入的客户端是一个网段的用户，往往通过一个设备拨入，实现隧道两端局域网的通信。
对端子网	L2TP/PPTP 隧道对端局域网使用的 IP 地址范围（一般可以填隧道对端设备 LAN 口的 IP 地址范围），由 IP 和子网掩码组成。
最大会话数	每个用户允许接入的最大客户端数量。在站点到站点组网模式下不需填写，PC 到站点模式下可填写 1-10。

3. 进入页面：网络 >> L2TP >> L2TP 服务器，在服务器设置部分点击<新增>，选择对应接口（此例中为 GE2），添加 L2TP 服务器规则。

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，可选择加密、不加密、可选加密。
预共享密钥	设置 IPSec 加密时的预共享密钥，VPN 两端需要保持一致。

4. 进入页面：对象 >> 服务 >> 服务组，设置 VPN 服务组并绑定防火墙内置的 VPN 相关服务。

   此处为了配置方便，可绑定三类 VPN 相关的服务。

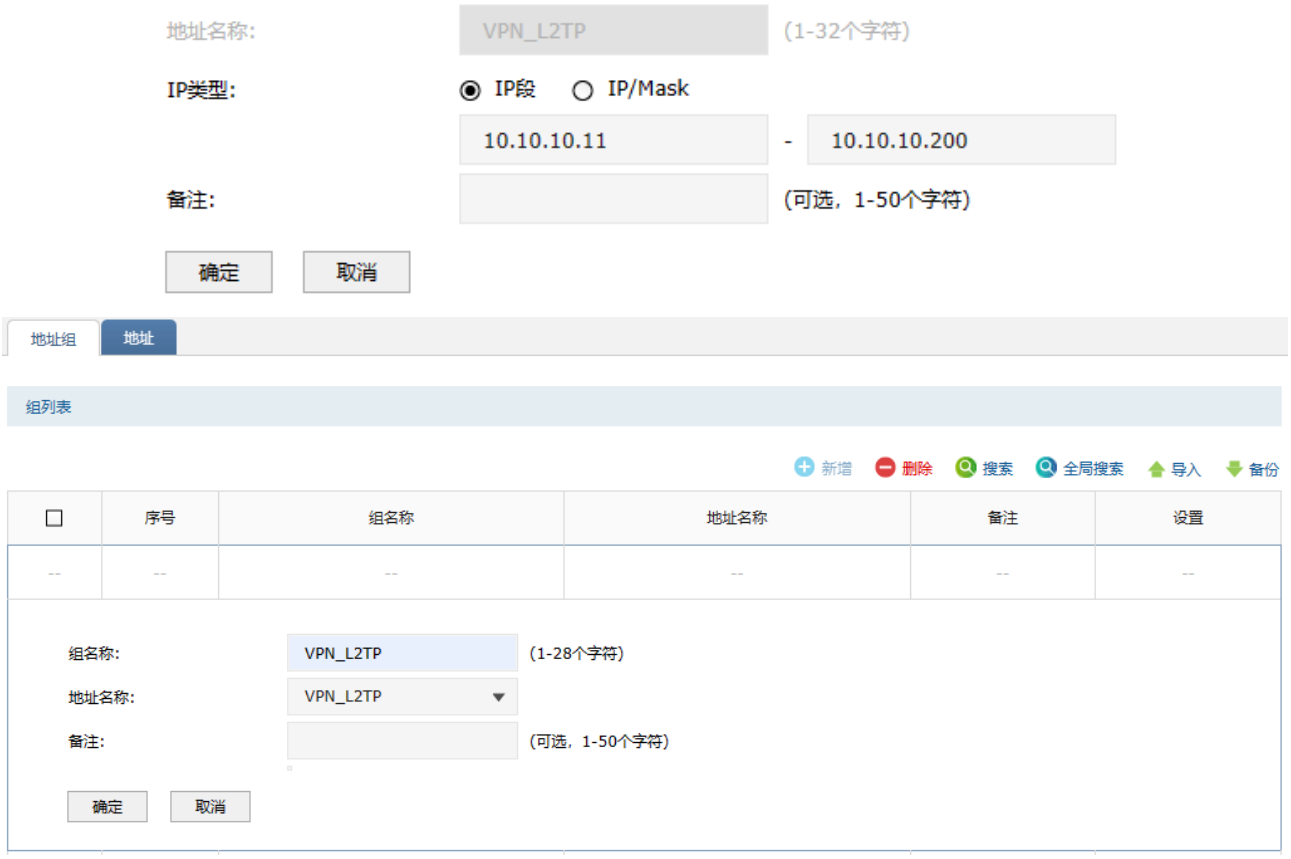


5. 设置 VPN 安全策略。

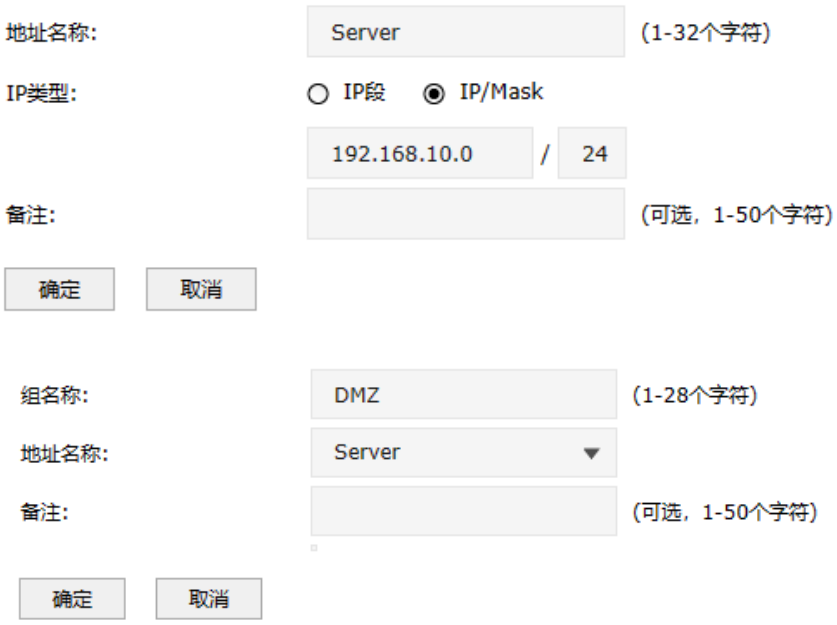
   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，设置源安全区域为 untrust，目的区域为 local，源地址选择所有，目的地址设置为开启 VPN 的接口的 IP（此例中为 GE2，可在“对象 >> 地

址 >> 地址组”页面添加对应地址的地址组），如果该地址非固定 IP，目的地址可选择为所有地址“IPGROUP_ANY”，服务组为 4 中设置“VPN”，动作为“允许”。

6. 进入页面：对象 >> 地址 >> 地址/地址组，添加步骤 1 中所设地址池对应的地址段到“VPN_L2TP”地址组。



将服务器对应的地址段添加到“DMZ”地址组。



7. 如果要允许 VPN 客户端的 VPN 用户访问内网服务器，则需要开放相应的安全策略。

   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择从“untrust”到“dmz”，源地址为上一步骤中设置的“VPN_L2TP,”目的地址为服务器所在网段“DMZ”，动作为“允许“。

客户端设置

1. 在深圳分部的防火墙上，进入页面：网络 >> 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。

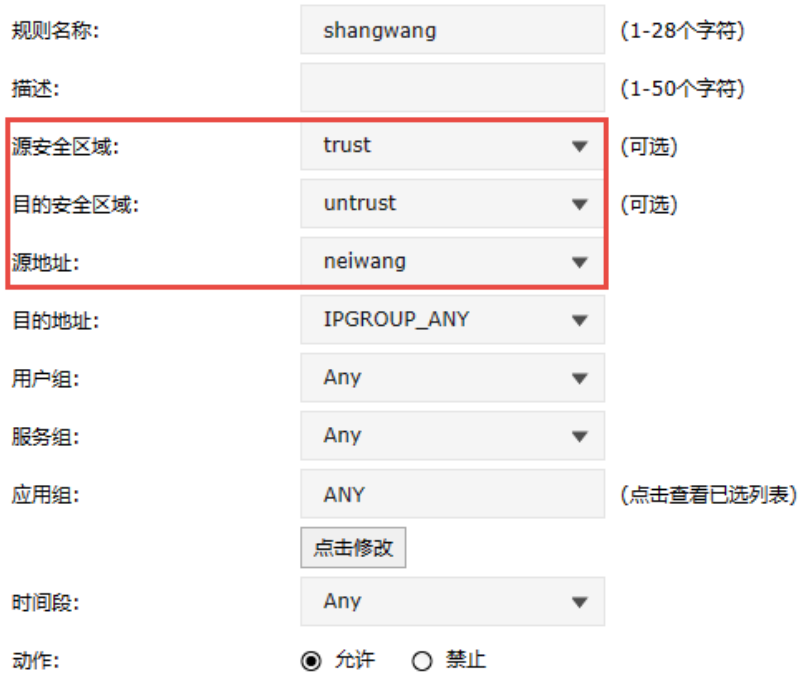
用户名	服务器端设置的用户名。
密码	服务器端设置的密码。
出接口	选择已经设置上网的接口。
服务器地址	服务器 WAN 口地址，或者填域名：例如 vs.yueshen.gd（服务器端申请的动态域名）
IPSec 加密	选择是否加密，与服务器端设置一致。
预共享密钥	选择加密时需要填写预共享密钥，与服务器端保持一致。
对端子网范围	服务器端 LAN 口的网段（与本地 LAN 不同网段）。
工作模式	NAT：对经过此 L2TP 隧道的数据包进行 NAT 转换（数据包的源 IP 替换为 L2TP 隧道的本地虚拟 IP）； 路由：对经过此 L2TP 隧道的数据包进行路由转发。

2. 设置允许 VPN 拨号的安全策略。进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择“local”到“untrust”，源地址是 WAN 口 IP（此处为 GE3 口地址），目的地址是对端接口的公网 IP（此处填写的为所有地址“IPGROUP_ANY”），服务组选择“VPN”，动作选择“允许”。

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

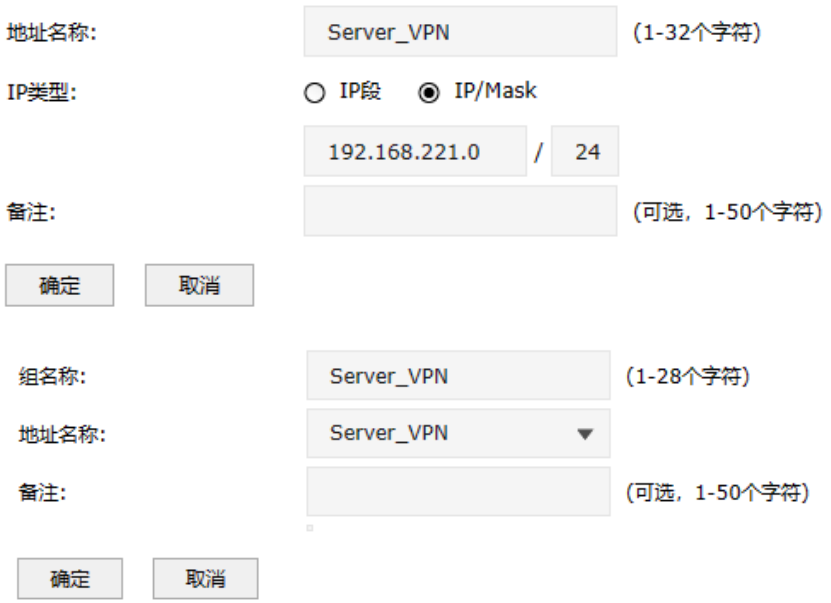
4. 如果要允许内网 trust 区域的设备访问 VPN 服务器端的内网服务器，还需要添加对应的安全策略。

   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择“trust”到“untrust”，源地址为允许访问服务器的内网的地址组，目的地址为服务器 IP 对应的地址组，此处为方便设置为所有地址“IPGROUP_ANY”，动作为“允许”。



5. 如果要允许 VPN 服务器端的设备访问内网服务器，则需要添加相应的安全策略。

   进入页面：对象 >> 地址 >> 地址/地址组，添加服务器端有访问需求的网段到地址组“Server_VPN”。

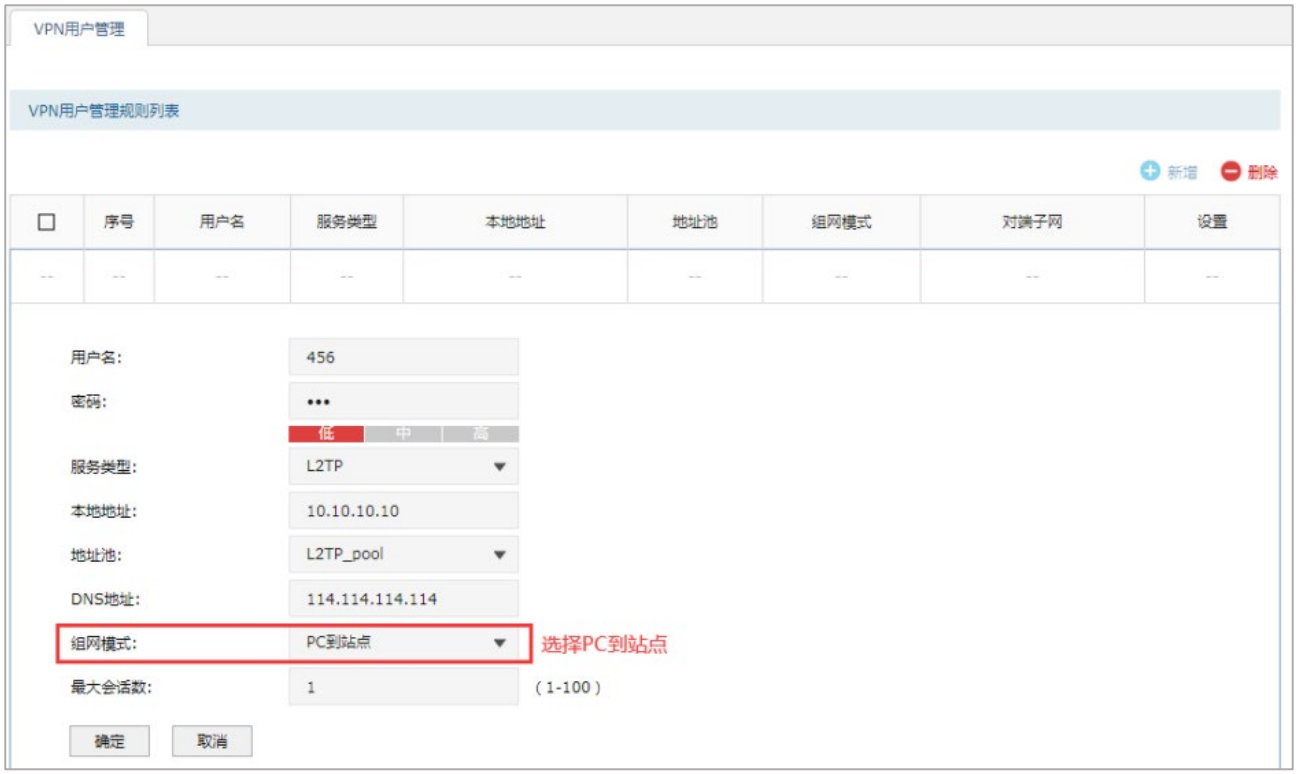


   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择“untrust”到“DMZ”，源地址为服务器端有访问需求的网段“Server_VPN”，目的地址为服务器网段地址“DMZ”，动作为“允许”，还可以设置 URL 过滤、反病毒等内容安全相关的检查策略。

- **L2TP PC 到站点的设置方法**

服务器端设置

1. 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。

客户端设置

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

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。

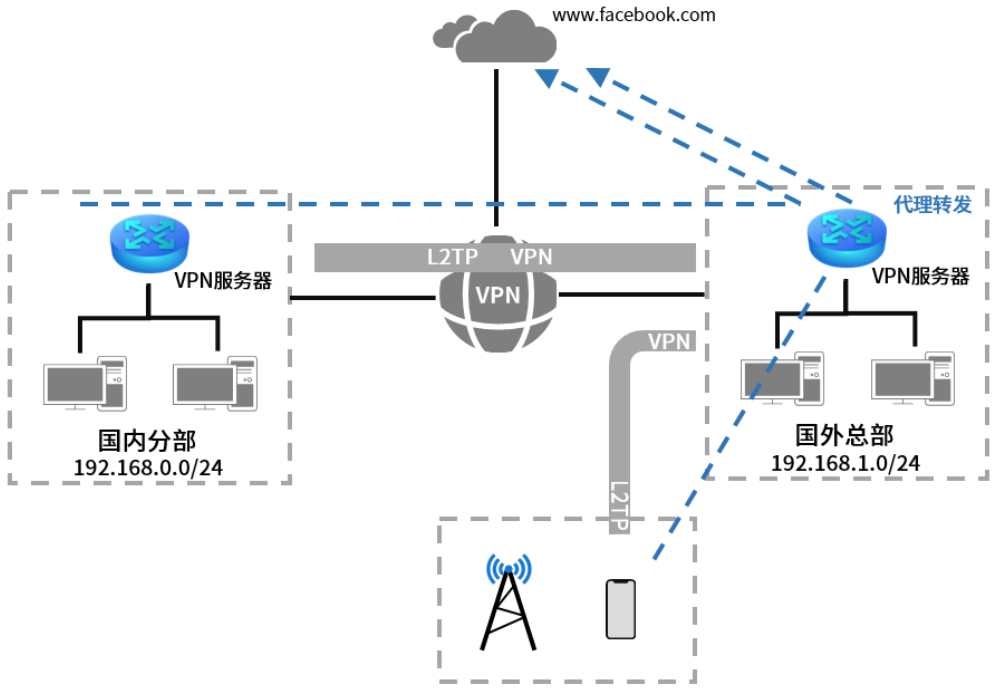
如果需要通过总部进行代理转发访问分部资源，可在分部防火墙上进入页面“网络 >> 路由设置 >> 静态路由”设置静态路由如下即可：

9.2.5 L2TP 代理配置实例

➢ 需求介绍

某公司的总部与分部均使用 VPN 防火墙产品，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 ***9.2.4 L2TP 配置实例***。

2. 进入页面：策略 >> NAT 策略 >> NAPT，在 VPN 服务器端设置针对 VPN 地址池的 NAPT 规则，出接口选择上网口。

3. 在 VPN 客户端防火墙上，进入页面：网络 >> L2TP >> L2TP 客户端，点击<新增>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 客户端上，进入页面：网络 >> 路由设置 >> 策略路由，点击<新增>添加策略路由，使所有数据优先走 VPN 接口。

5. 如果 VPN 客户端内网主机需要通过防火墙代理上网，则需要添加相应的安全策略。

进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域从“untrust”到“untrust”，源地址为“VPN_L2TP”，目的地址为所有地址“IPGROUP_ANY”，动作为“允许”。

- **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。如果未能实现代理上网，可以检查确认 PC 端此处设置：

9.3 PPTP

VPN 防火墙提供多类 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 。

9.3.1 PPTP 服务器

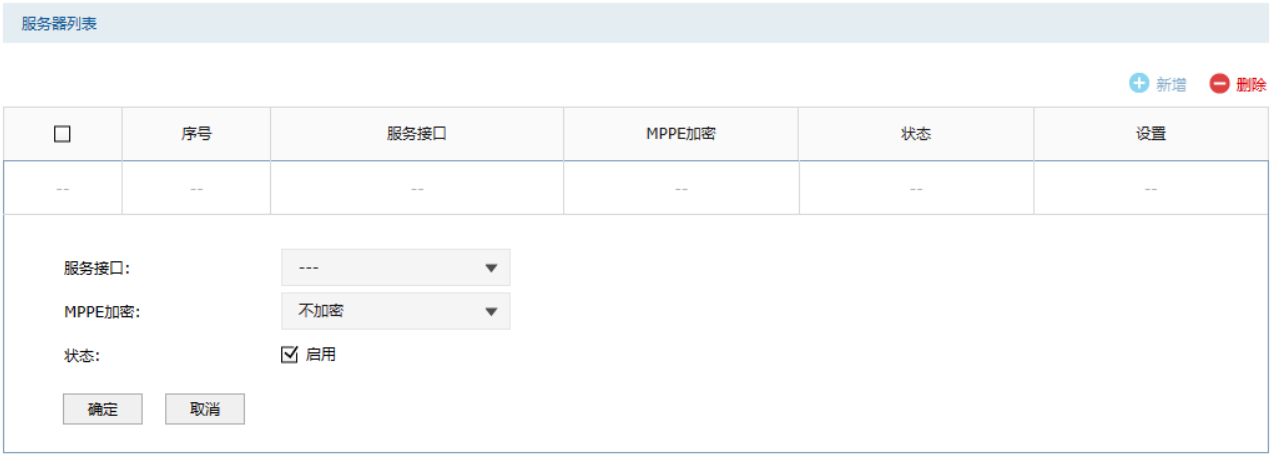
进入页面：网络 >> PPTP >> PPTP 服务器，进行全局设置和 PPTP 服务器设置。

- **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。



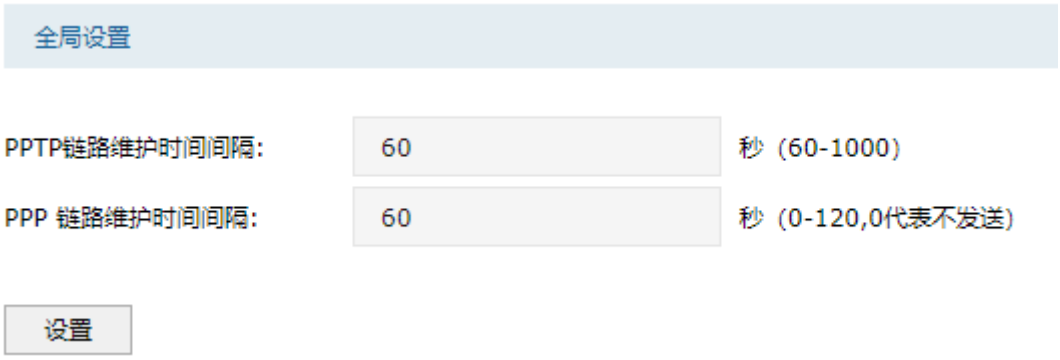
服务接口	PPTP 服务器监听的接口，只有来自服务接口的报文才会被处理。
MPPE 加密	是否对隧道进行加密。若启用，则使用 MPPE 对 PPTP 隧道加密。

点击页面 ，查看更多页面设置参数信息。

9.3.2 PPTP 客户端

进入页面：网络 >> PPTP >> PPTP 客户端，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。

- **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	防火墙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）。 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。

9.3.3 隧道信息列表

可以获得 PPTP 隧道的信息。

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

9.3.4 PPTP 配置实例

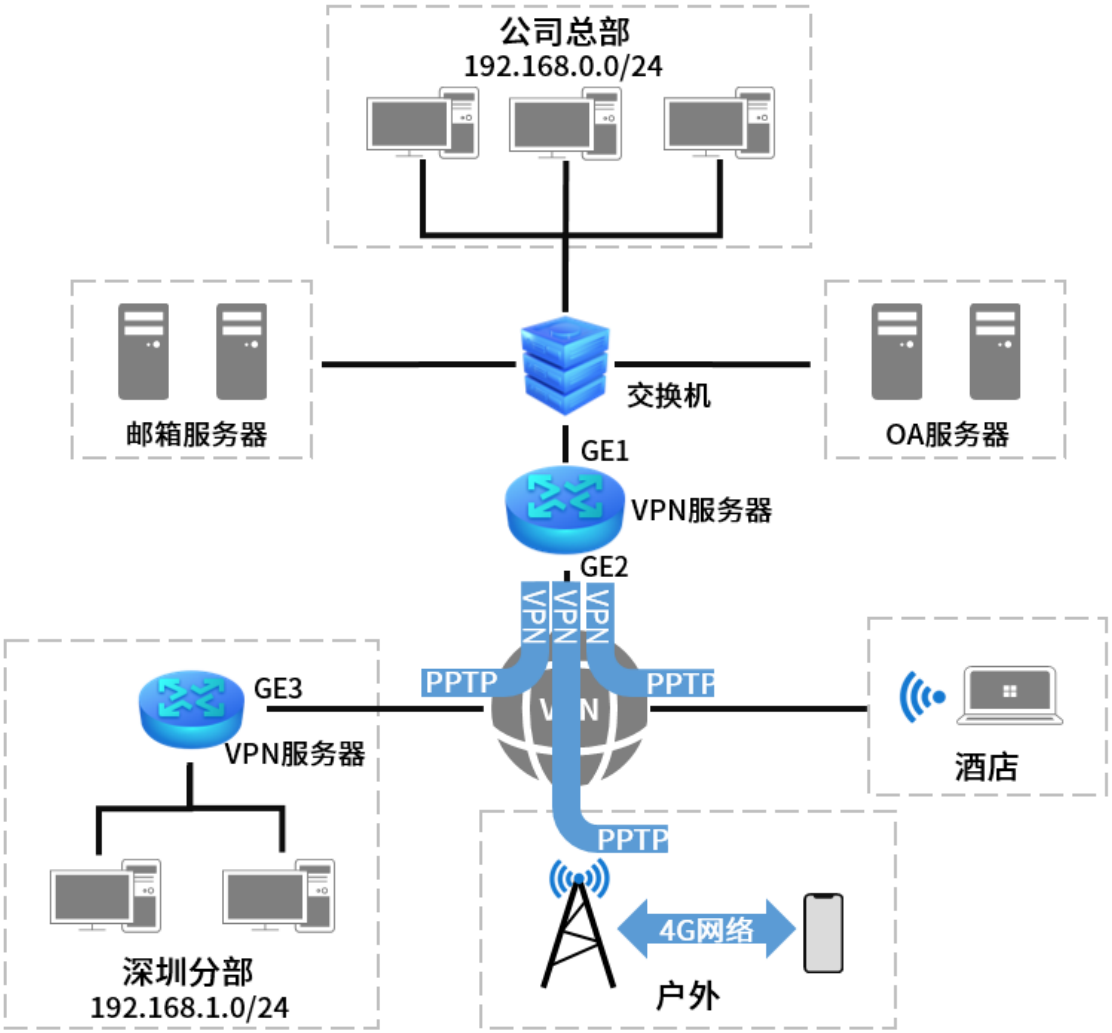
➢ **需求介绍**

某公司的总部与分部均使用 TP-LINK 防火墙产品。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：

PPTP 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。

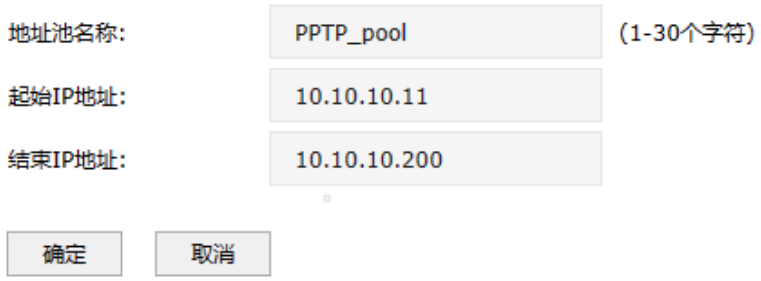
注意：

为使 PPTP 服务正常运行，需前往“策略 >> ALG 策略 >> ALG 服务”页面，开启“PPTP ALG”。

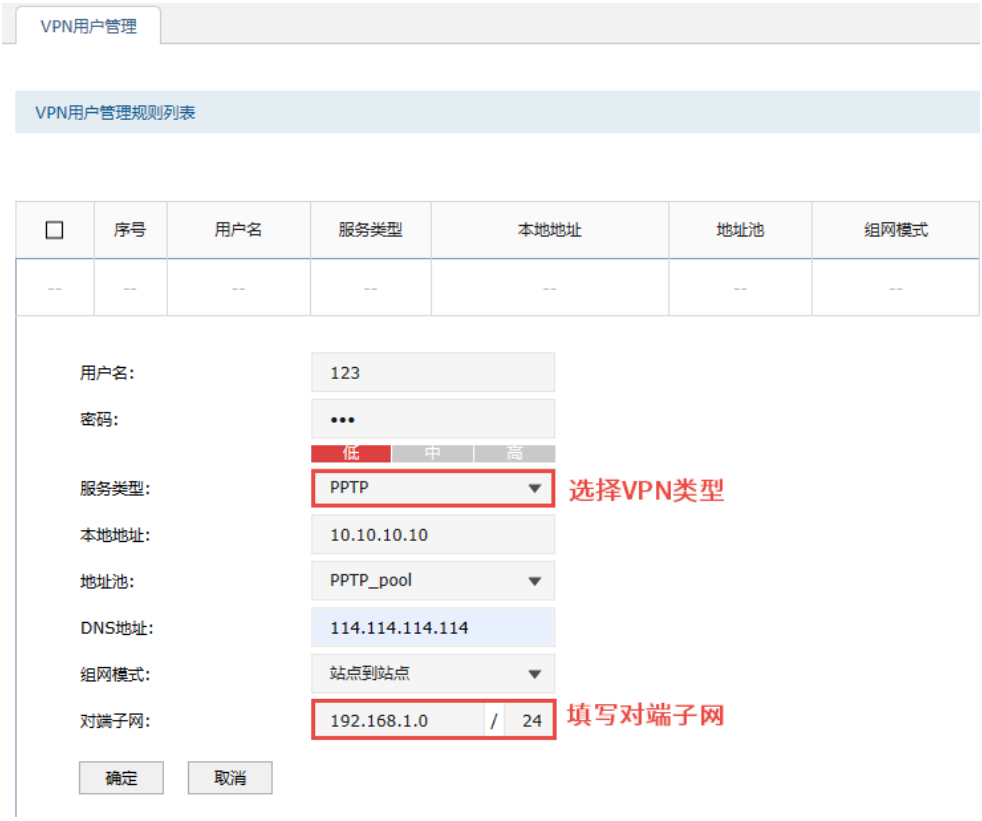
- **PPTP 站点到站点的设置方法**

  服务器端设置（以 TL-NFW8500 为例）

1. 进入页面：对象 >> IP 地址池 >> IP 地址池，新增隧道地址池（PPTP VPN 隧道通信时使用的 IP 地址）。该地址池应与防火墙各接口 IP 不在同一网段。



2. 进入页面：网络 >> VPN 用户管理 >> VPN 用户管理，进行用户管理配置，点击<新增>。设置用于 VPN 通讯的虚拟本地地址，选择上一步骤中设置的 IP 地址池，设置 DNS 服务器，组网模式选择站点到站点，填入实际的对端子网。



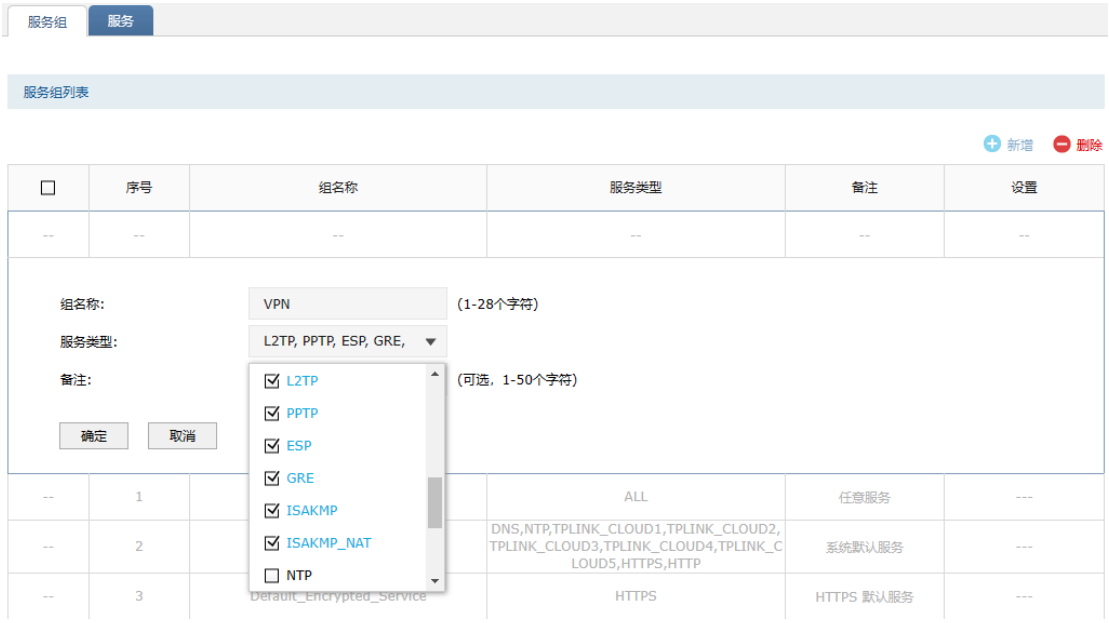
用户名	客户端与服务器端建立连接的用户名。
密码	客户端与服务器端建立连接的密码。
服务类型	L2TP：本用户只用于 L2TP； PPTP：本用户只用于 PPTP； 自动：本用户既可用于 L2TP 也可用于 PPTP。
本地地址	VPN 隧道的本地虚拟 IP 地址。
地址池	选择上一步骤中建立的隧道地址池。

组网模式	PC 到站点：拨入的客户端时个人用户，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； 站点到站点：拨入的客户端是一个网段的用户，往往通过一个设备拨入，实现隧道两端局域网的通信。
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。
最大会话数	每个用户允许接入的最大客户端数量。在站点到站点组网模式下不需填写，PC 到站点模式下可填写 1-10。

3. 进入页面：网络 >> PPTP >> PPTP 服务器，在服务器设置部分点击<新增>，选择对应接口（此例中为 GE2），添加 PPTP 服务器规则。

4. 进入页面：对象 >> 服务 >> 服务组，设置 VPN 服务组并绑定防火墙内置的 VPN 相关服务。

   此处为了配置方便，可绑定三类 VPN 相关的服务。

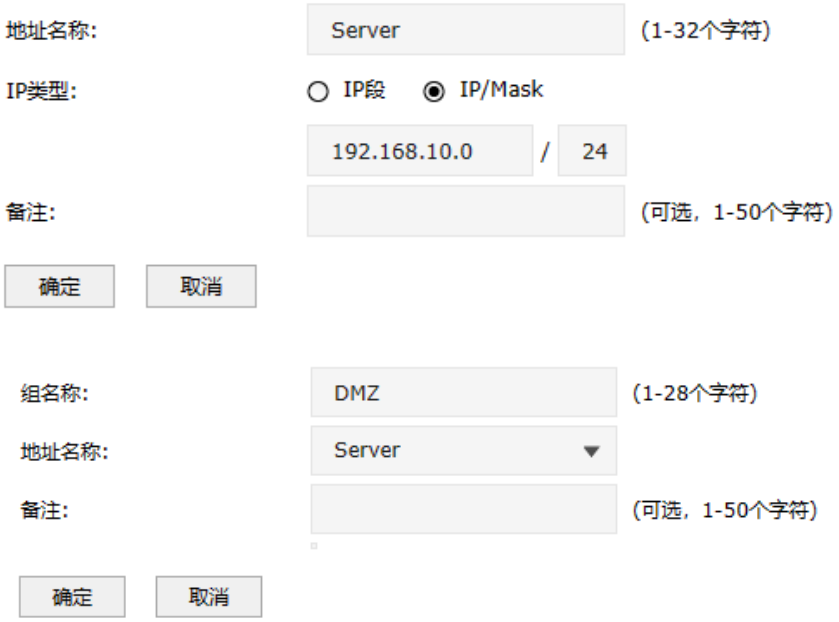


5. 设置 VPN 安全策略。

进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，设置源安全区域为 untrust，目的区域为 local，源地址选择所有，目的地址设置为开启 VPN 的接口的 IP（此例中为 GE2，可在“对象 >> 地址 >> 地址组”页面添加对应地址的地址组），如果该地址非固定 IP，目的地址可选择为所有地址“IPGROUP_ANY”，服务组为 4 中设置“VPN”，动作为“允许”。

6. 进入页面：对象 >> 地址 >> 地址/地址组，添加步骤 1 中所设地址池对应的地址段到“VPN_PPTP”地址组。

将服务器对应的地址段添加到“DMZ”地址组。



7. 如果要允许 VPN 客户端的 VPN 用户访问内网服务器，则需要开放相应的安全策略。

   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择从“untrust”到“dmz”，源地址为上一步骤中设置的“VPN_PPTP,”目的地址为服务器所在网段“DMZ”，动作为“允许“。

客户端设置

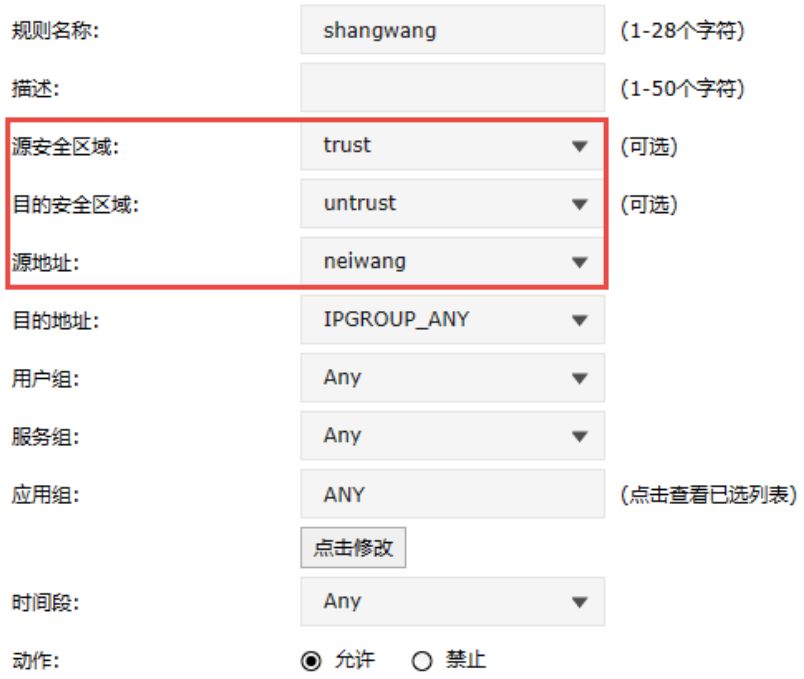
1. 在深圳分部的防火墙上，进入页面：网络 >> PPTP >> PPTP 客户端，在客户端设置部分点击<新增>，添加 PPTP 客户端规则。

2. 设置允许 VPN 拨号的安全策略。进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择“local”到“untrust”，源地址是 WAN 口 IP（此处为 GE3 口地址），目的地址是对端接口的公网 IP（此处填写的为所有地址“IPGROUP_ANY”），服务组选择“VPN”，动作选择“允许”。

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

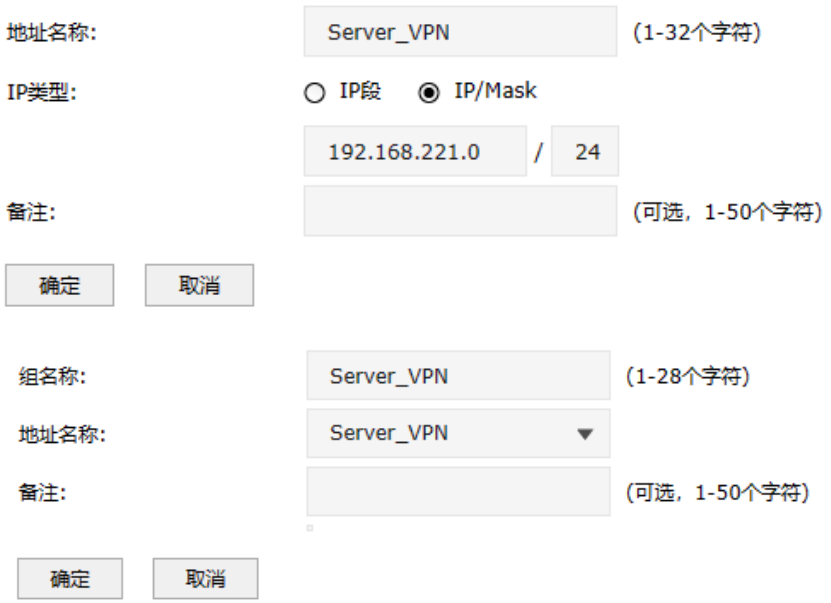
4. 如果要允许内网 trust 区域的设备访问 VPN 服务器端的内网服务器，还需要添加对应的安全策略。

   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择“trust”到“untrust”，源地址为允许访问服务器的内网的地址组，目的地址为服务器 IP 对应的地址组，此处为方便设置为所有地址“IPGROUP_ANY”，动作为“允许”。



5. 如果要允许 VPN 服务器端的设备访问内网服务器，则需要添加相应的安全策略。

   进入页面：对象 >> 地址 >> 地址/地址组，添加服务器端有访问需求的网段到地址组“Server_VPN”。

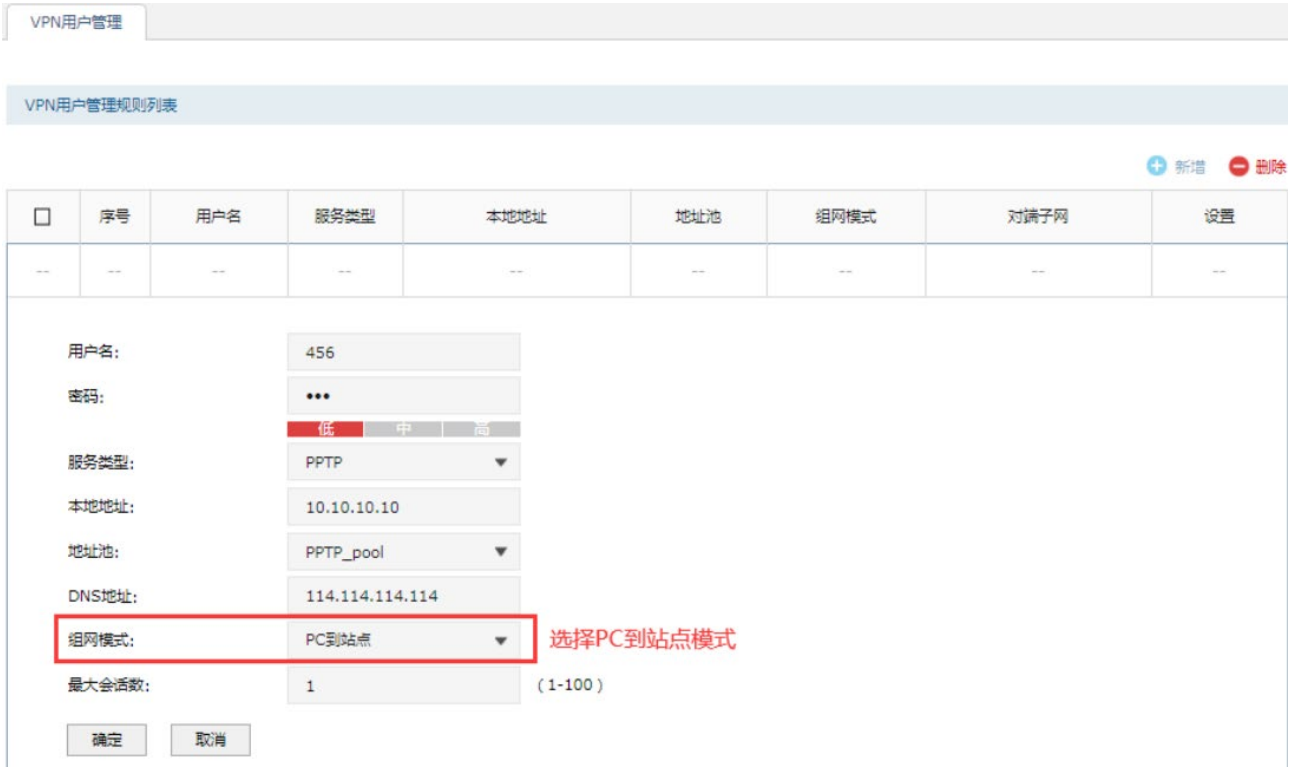


   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域选择“untrust”到“DMZ”，源地址为服务器端有访问需求的网段“Server_VPN”，目的地址为服务器网段地址“DMZ”，动作为“允许”，还可以设置 URL 过滤、反病毒等内容安全相关的检查策略。

- **PPTP PC 到站点的设置方法**

服务器端设置

1. 在总部的 VPN 防火墙上，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。

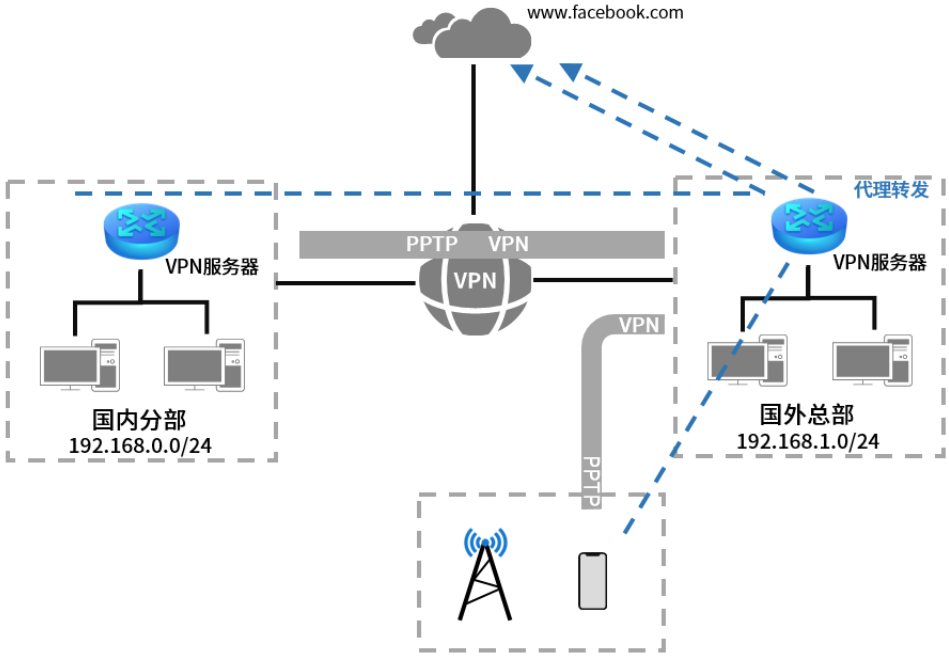
如果需要通过总部进行代理转发访问分部资源，可在分部防火墙上进入页面“网络 >> 路由设置 >> 静态路由”设置静态路由如下即可：

9.3.5 PPTP 代理配置实例

➢ **需求介绍**

某公司的总部与分部均使用 VPN 防火墙产品，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 ***9.3.4 PPTP 配置实例***。

2. 进入页面：策略 >> NAT 策略 >> NAPT，在 VPN 服务器端设置针对 VPN 地址池的 NAPT 规则，出接口选择上网口。

3. 在 VPN 客户端防火墙上，进入页面：网络 >> L2TP >> L2TP 客户端，点击<新增>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 客户端上，进入页面：网络 >> 路由设置 >> 策略路由，点击<新增>添加策略路由，使所有数据优先走 VPN 接口。

5. 如果 VPN 客户端内网主机需要通过防火墙代理上网，则需要添加相应的安全策略。

   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，安全区域从“untrust”到“untrust”，源地址为“VPN_L2TP”，目的地址为所有地址“IPGROUP_ANY”，动作为“允许”。

- **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。如果未能实现代理上网，可以检查确认 PC 端此处设置：

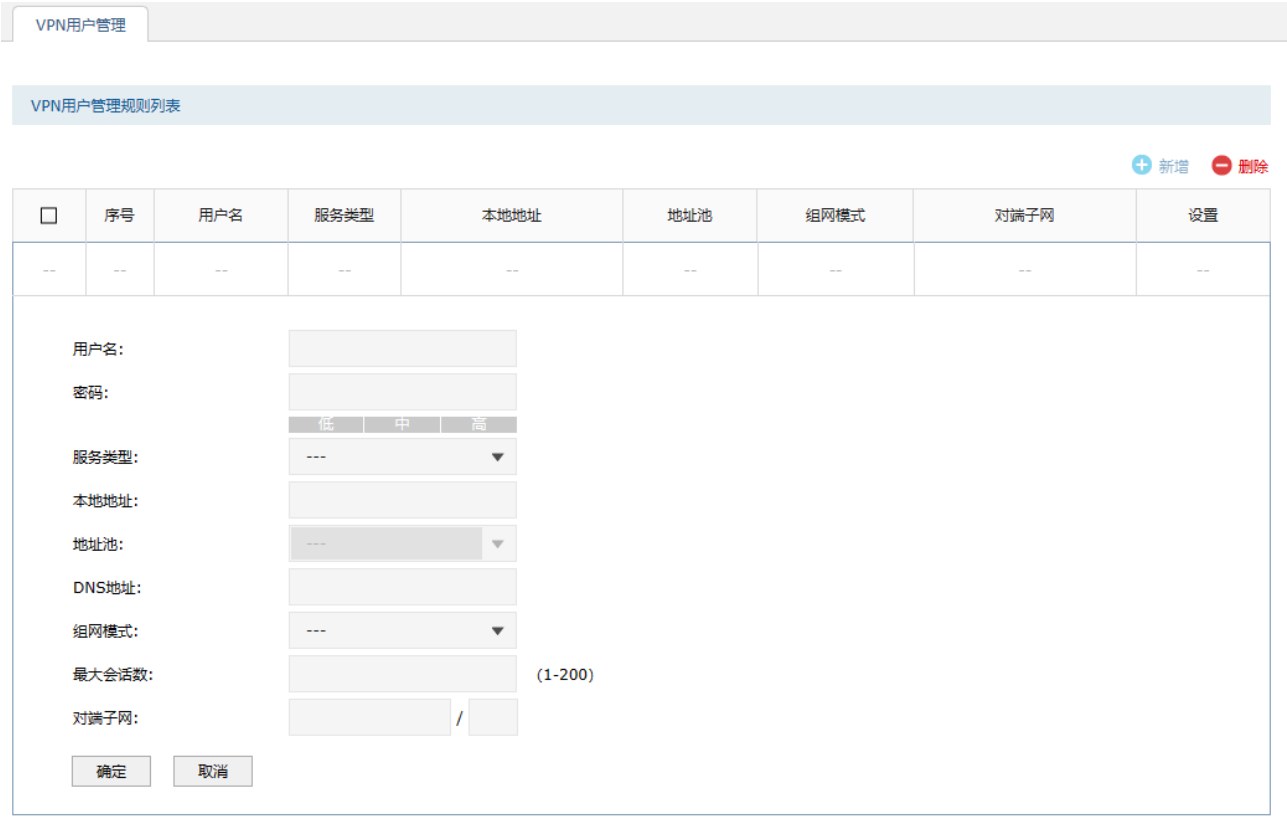
9.4 VPN 用户管理

9.4.1 VPN 用户管理

可以配置 L2TP/PPTP 服务器的用户信息。

进入页面的方法：网络 >> VPN 用户管理 >> VPN 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。 L2TP：本用户只用于 L2TP； PPTP：本用户只用于 PPTP； 自动：本用户既可用于 L2TP 也可用于 PPTP。
本地地址	VPN 隧道的本地虚拟 IP 地址。
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。 站点到站点：拨入的客户端是一个网段的用户，往往通过一个防火墙拨入，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。

9.4.2 IP 地址池

可以配置 L2TP/PPTP 服务器的地址池信息。

具体请参考 *6.3 IP 地址池*。

回目录

第10章 认证管理

TP-LINK 防火墙提供 Portal 认证服务，包括 Web 认证和远程 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。

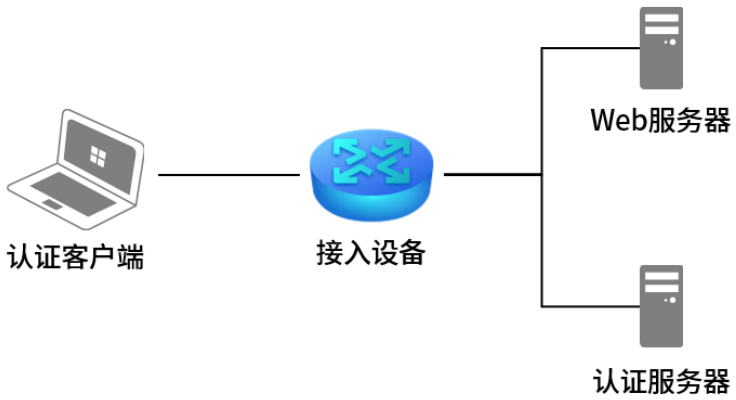
10.1 认证设置

10.1.1 Web 认证介绍

防火墙提供 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，包括防火墙、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；

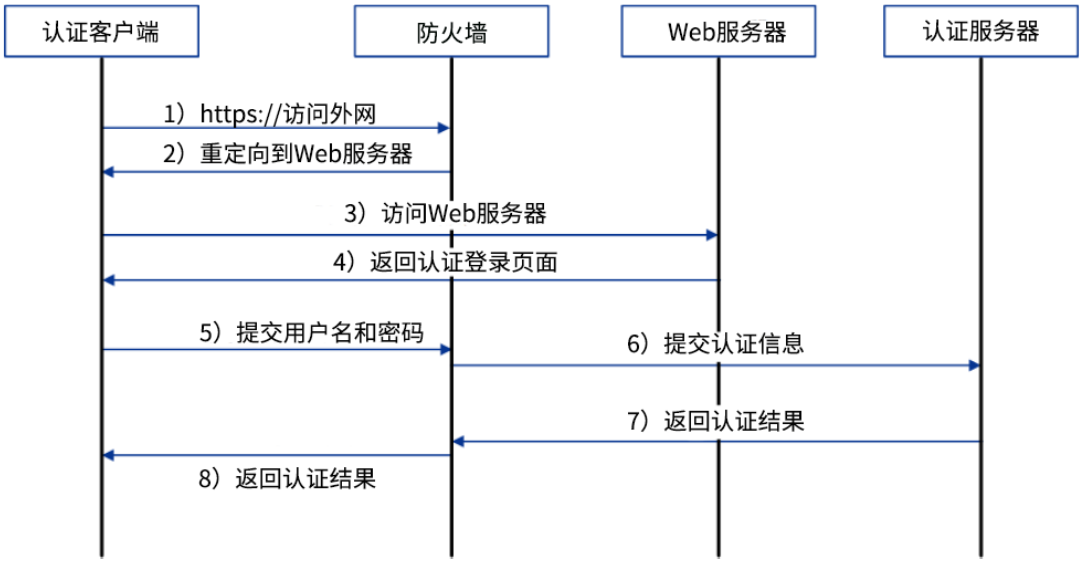
2) 认证过程中，与认证服务器交互，完成用户的身份认证；

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) 防火墙返回重定向 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，该信息将提交到防火墙；

6) 防火墙向认证服务器提交该用户的认证信息；

7) 认证服务器向防火墙返回认证结果；

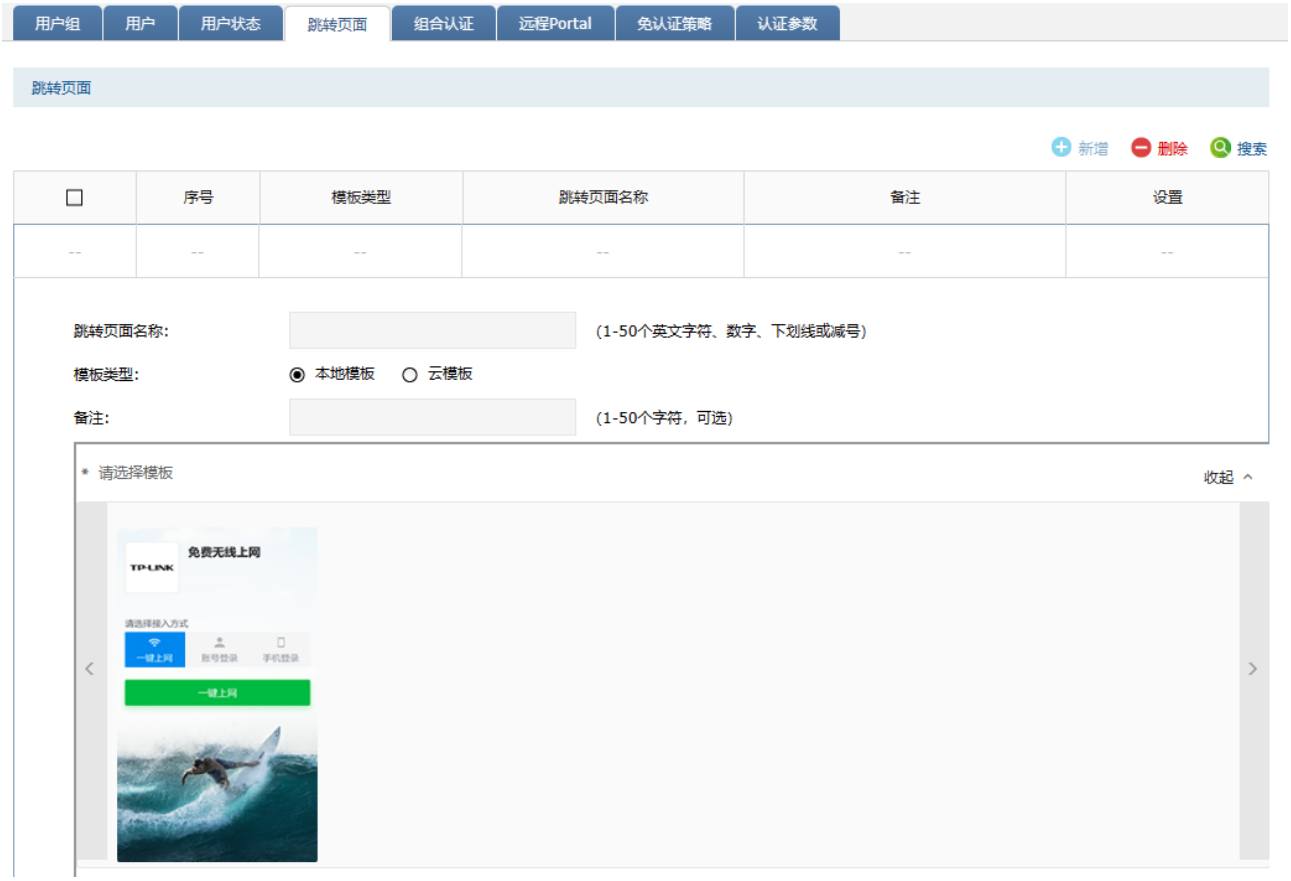
8) 防火墙向认证客户端返回该认证结果。

10.1.2 跳转页面

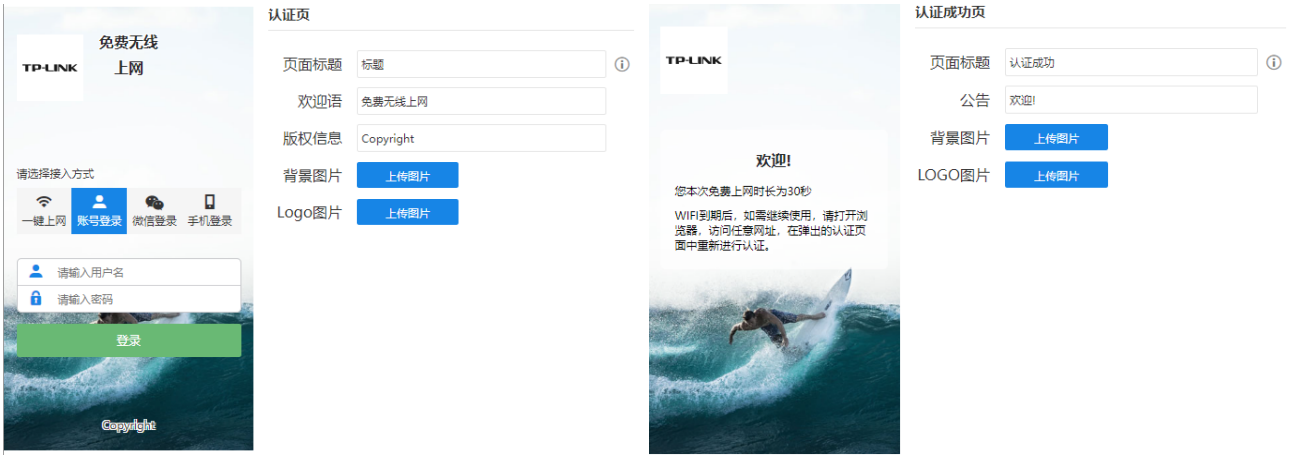
在此设置用户认证过程中所看到的认证页面和认证成功页面，可通过图片上传、外部链接或使用默认模板，满足推送广告，推广微信公众号等需求。

进入页面的方法：对象 >> 用户 >> 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，可使用本地模板或向云端服务器获取云模板。



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>。



10.1.3 组合认证

TP-LINK 防火墙提供 Web 认证方式，可通过本页面对组合认证功能进行详细配置。

进入页面的方法：对象 >> 用户 >> 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 ***10.1.2 跳转页面***。
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。

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。
- 当默认安全策略为禁止时，需要添加放行认证端口（默认为 8080，在“对象 >> 用户 >> 认证参数”页面可查看）和 DNS 端口的安全策略规则，重定向页面才能正常弹出。

10.1.4 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。

进入页面的方法：对象 >> 用户 >> 远程 Portal

点击<新增>设置远程认证规则。

生效接口	选择需要进行远程 Portal 认证的接口。
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	填写远程 Portal 服务器的地址。
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。

点击页面 ，查看更多页面设置参数信息。

10.1.5 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。

进入页面的方法：对象 >> 用户 >> 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。

生效接口域	设置免认证策略的生效接口。
备注	可设置免认证策略的备注，以方便管理和查找。备注最多支持 50 个字符

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，当已知目的网络 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。
生效接口域	设置免认证策略的生效接口。

点击页面，查看更多页面设置参数信息。

10.1.6 全局参数

通过本页面可设置认证老化时间和 Portal 认证端口。

进入页面的方法：对象 >> 用户 >> 认证参数

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。

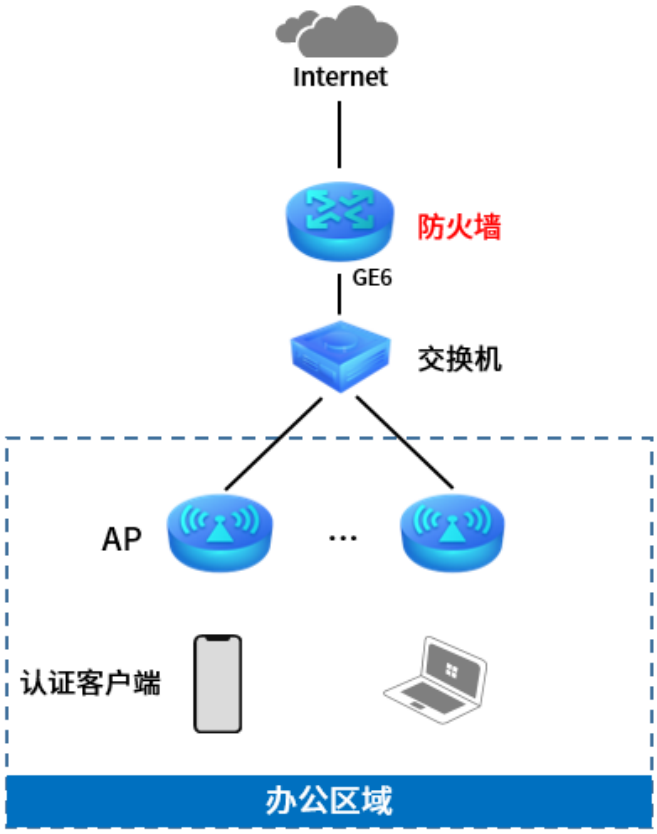
10.2 认证设置配置实例

10.2.1 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。TP-LINK 防火墙支持 Portal 功能，认证方式灵活，支持广告推送。

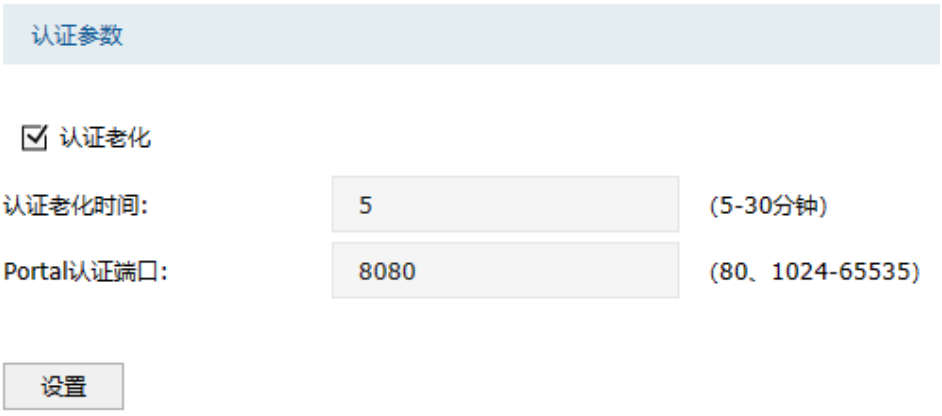
- **需求介绍**

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：

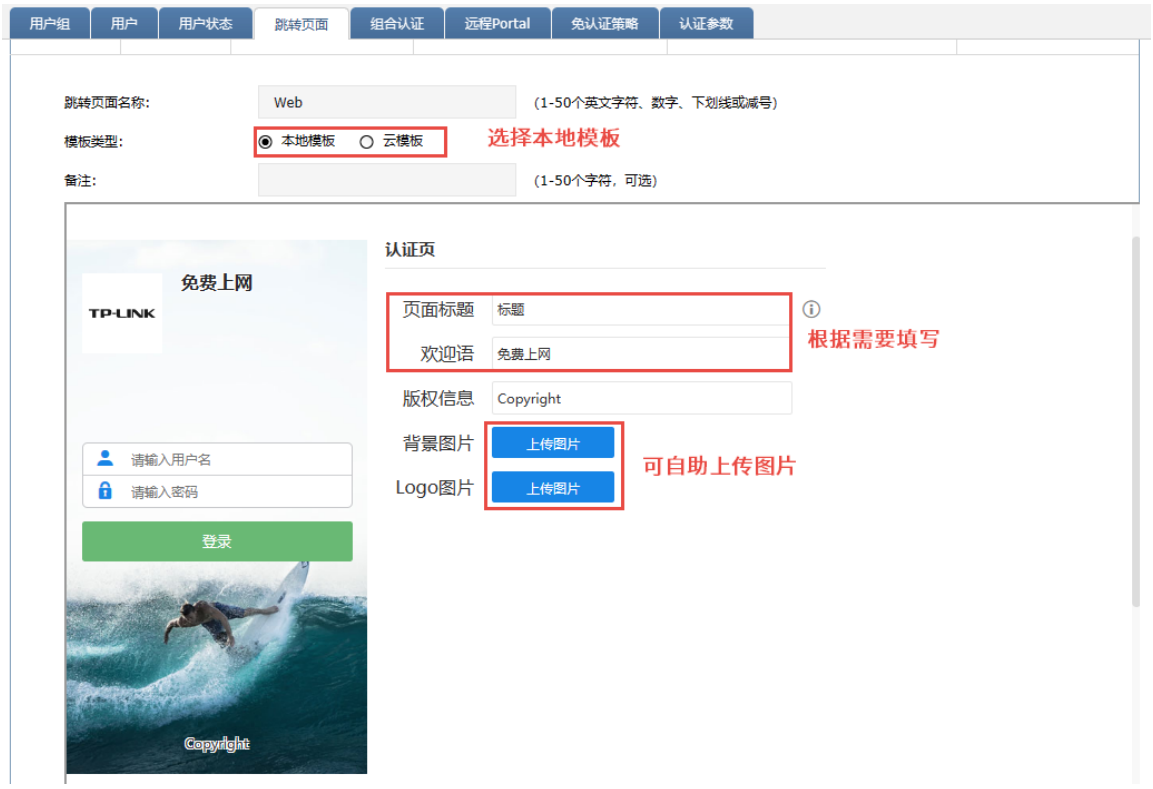


➢ **配置方法**

1. 设置认证参数，进入页面：对象 >> 用户 >> 认证参数，配置认证老化时间和认证模式。



2. 配置内置 Web 服务器，进入页面：对象 >> 用户 >> 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。



3. 配置内置认证服务器，进入页面：对象 >> 用户 >> 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。

4. 进入页面：对象 >> 用户>> 用户，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：

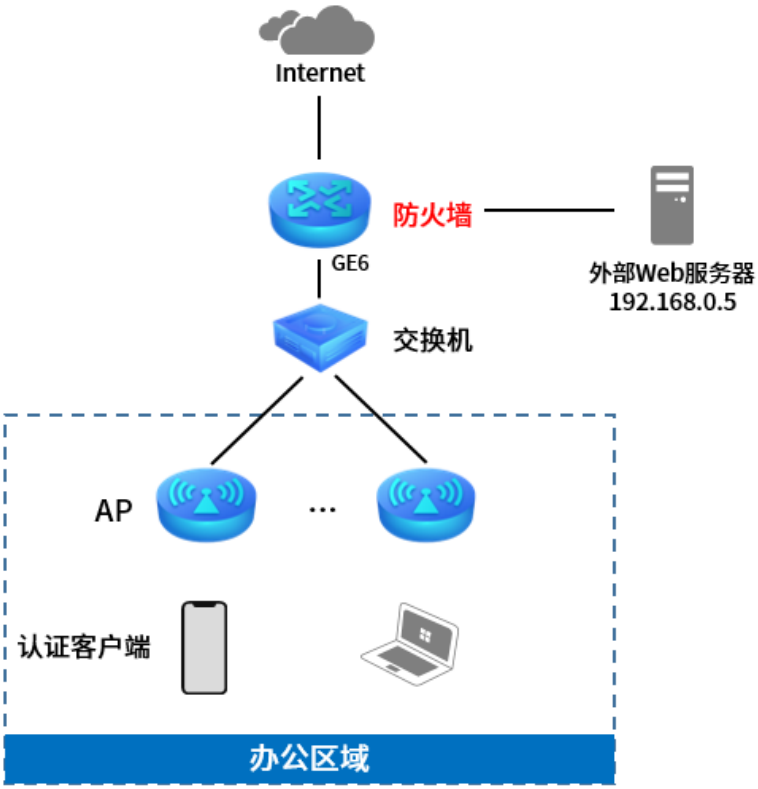
以上内容配置完毕，防火墙的 Portal 认证服务设置成功，连接办公区的网络输入用户名和密码认证通过后即可上网。

10.2.2 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。防火墙支持 Portal 功能，认证方式灵活，支持广告推送。

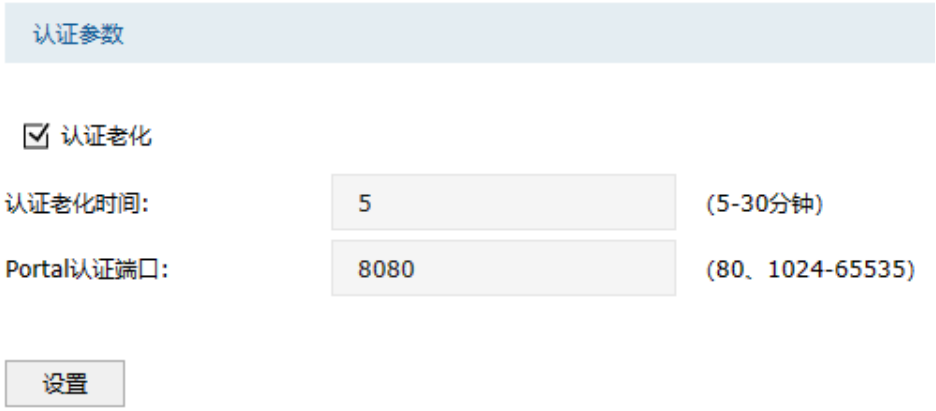
➢ 需求介绍

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：

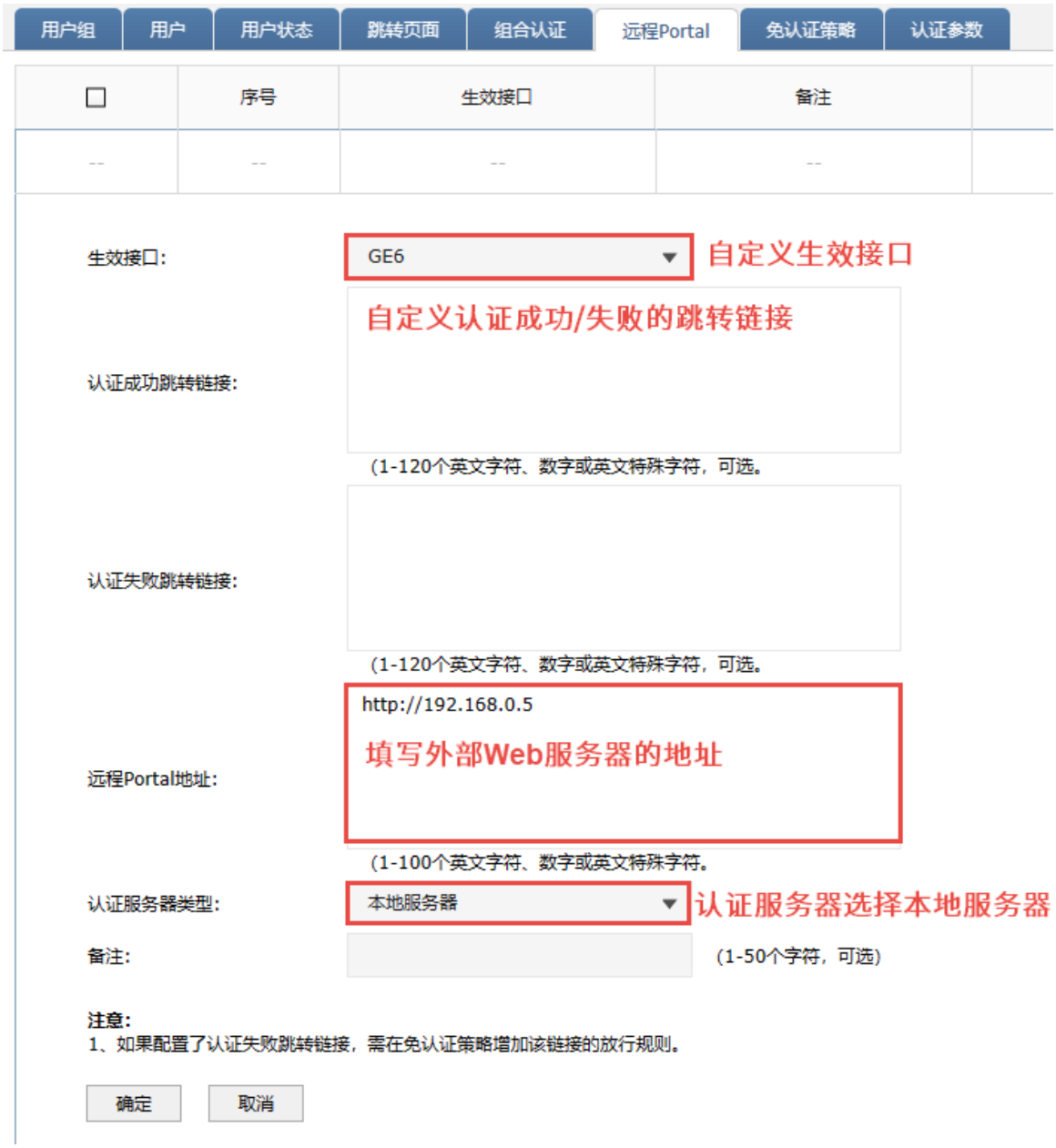


➢ **配置方法**

1. 设置认证参数，进入页面：对象 >> 用户 >> 认证参数，配置认证老化时间。



2. 配置外部 Web 服务器，进入页面：对象 >> 用户>> 远程 Portal，点击<新增>，认证服务器类型选择本地服务器。



3. 进入页面：对象 >> 用户>> 用户，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，防火墙的 Portal 认证服务设置成功，连接办公区的网络输入用户名和密码认证通过后即可上网。

10.2.3 免认证策略配置实例

➢ **需求介绍**

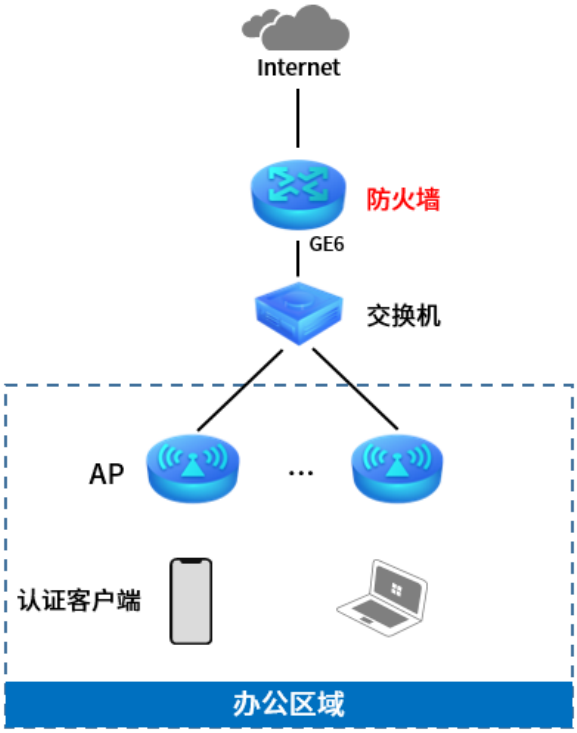
某办公室需要实现无线覆盖，员工需要通过认证后才能上网，有以下需求：

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。进入防火墙界面，进入页面：对象 >> 用户 >> 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。

说明:

- 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，进入页面：对象 >> 用户 >> 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，进入防火墙界面，进入页面：对象 >> 用户 >> 免认证策略，点击<新增>，添加免认证策略。

10.3 用户管理

10.3.1 用户组

进入页面的方法：对象 >> 用户 >> 用户组

导入　　点击<导入>按钮导入多个用户组条目和用户条目。可以通过“备份”功能获取符合规则的 CSV 文件，以查看文件的正确格式。

备份　　点击<备份>按钮备份所有用户组条目和用户条目。备份文件可直接通过“导入”功能重新添加到用户组列表和用户列表中。

点击<新增>，设置用户组名称，选择成员列表，点击<确定>。

成员列表　　用户组所引用的用户对象(可多选)，引用了该用户组的规则，对所有用户对象所包含的地址均会生效。

新增的条目会在组列表里显示出来，如下图所示。

	序号	组名称	成员列表	设置
--	1	Any		---
☐	2	group_1		

如有需要，可点击条目后的< >按钮进行编辑。条目 1 为系统默认条目，不可操作。

注意：

用户组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。

10.3.2　用户

可设置和查看已添加的认证用户列表。

进入页面的方法：对象 >> 用户 >> 用户

点击<新增>，进入地址设置页面。填入地址名称，选择 IP 类型并填入 IP 信息，点击<确定>按钮手动添加条目。

用户类型	用户类型分为正式用户或免费用户。 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。 免费用户：免费用户具有一定的上网时长限制。
用户名	自定义的用户名，注意不能与已有用户名重复。
密码	新增用户时，需要输入密码。修改用户配置时，可以输入新密码，不输入则表示不修改。
有效期/上网时长	正式用户的有效期。
免费时长	免费用户上网时间限制。
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。 不绑定：不绑定用户的 MAC 地址。 静态绑定：手动输入认证客户端 MAC 地址，绑定对应用户名。 动态绑定：系统自动绑定第一个使用该用户名认证成功的客户端 MAC 地址。
同时登录用户数	仅当“MAC 地址绑定方式”为“不绑定”时，可设。 允许同时使用该用户名认证的客户端最大数目。
姓名	客户姓名备注，可选项。
电话	客户电话备注，可选项。
备注	您可以对本地用户进行描述。
状态	设置该用户是否生效。

新增的条目会在列表里显示出来，如下图所示。

☐	序号	用户类型	用户名	有效期/上网时长	MAC地址	备注	状态	设置
☐	1	免费用户	test1	---	---	---	已启用	

如有需要，可以点击条目后的<  >按钮进行编辑。

点击<删除>，可批量删除用户列表条目。

10.4 用户状态

可查看当前已生效的用户认证状态。

进入页面的方法：对象 >> 用户 >> 用户状态

刷新	获取最新的认证用户列表。
下线	可实现批量断开用户连接。
认证方式	用户登录所使用的认证方式。
认证时间	用户登录时间。
IP 地址	用户的 IP 地址
设置	可断开用户的连接。

回目录

第11章 系统工具

11.1 管理员

11.1.1 设置用户名和密码

进入页面：系统工具 >> 管理账号 >> 管理账号，可修改管理账户用户名和密码。

11.1.2 系统管理设置

进入页面：系统工具 >> 管理账号 >> 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。

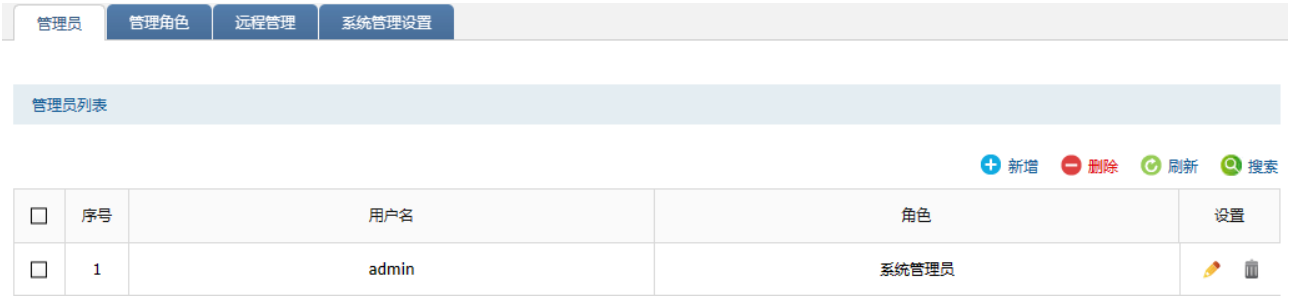
Http 服务端口	用于 Web 管理界面的 Http 服务端口，默认为 80 端口。不能与其他的服务端口重复。
Https 服务端口	用于 Web 管理界面的 Https 服务端口，默认为 443 端口。不能与其他的服务端口重复。
Web 会话超时时间	如果在会话超时时间内都没有进行操作，系统将自动退出登录，以保证设备和网络的安全。
最大尝试登录次数	连续登录 Web 页面的最大登录次数。
登录锁定时长	当连续登录 Web 页面的次数超过最大尝试登录次数，防火墙将锁定一段时间，该时间内将不能再登录 Web 页面。

点击页面  ，查看更多页面设置参数信息。

11.1.3 管理员列表

您可以通过本页面来管理账户的用户名和密码。

进入页面的方法：系统 >> 管理员 >> 管理员



管理员列表图标说明：

	编辑管理员账号信息。
	勾选管理员账号，可批量删除。
	获取最新的管理员列表。
	查找管理员账号。

搜索页面说明：

列名	选择用户名或角色作为搜索关键列。
内容	输入搜索关键内容，该内容需与列名相关。
方式	在结果中搜索：在当前列表条目中搜索，通过该功能可实现多级搜索； 在所有条目中搜索：在所有列表条目中搜索。
搜索	点击搜索，搜索开始。
显示全部	显示全部列表内容。
返回	放弃本次搜索。

添加管理员：

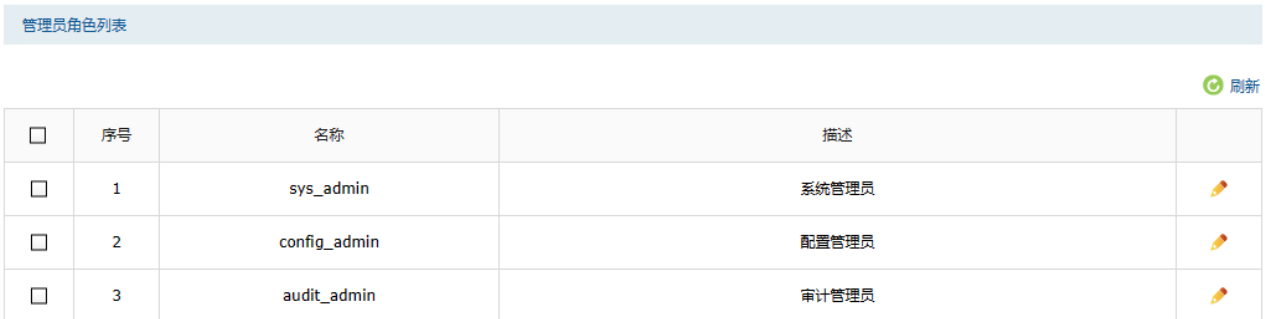
点击<新增>按钮，设置用户名和密码，选择角色，点击<确定>按钮手动添加条目。

用户名	您可以设置一个新的用户名。可以使用字母、数字及英文特殊符号的组合，不能使用中文、空格以及中文特殊符号。
密码	需要使用强度较高的密码以保证设备及网络的安全。“低、中、高”表示密码的复杂程度。
角色	不同的管理员角色对应不同的管理权限，具体的权限划分可以在"管理角色"页面查看。

11.1.4 管理角色

您可以通过本页面查看各个管理员角色的权限划分。

进入页面的方法：系统 >> 管理员 >> 管理角色



点击条目后的<>按钮查看权限划分。

11.1.5 系统管理设置

您可以通过本页面进行服务端口和会话超时时间的管理。

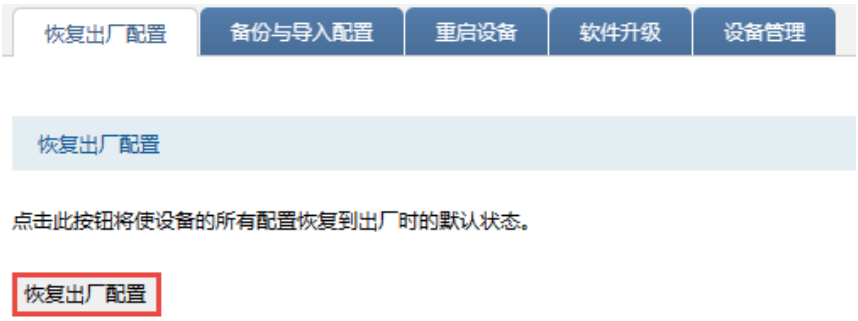
Http 服务	开启 http 服务。
Http 服务端口	设置防火墙的 Http 服务端口。
Https 服务端口	设置防火墙的 Https 服务端口。
Web 会话超时时间	设置通过 Web 访问防火墙的超时时间，Web 登录防火墙后，用户在该设定时间内如无任何指令，防火墙将自动断开连接。 设置超时时间后，新的超时时间将在下一次登录时生效。
最大登录尝试次数	当连续尝试登录失败达到该次数时，将会在一段时间内锁定设备不允许继续登录。
登录锁定时长	当连续登录失败次数达到最大登录尝试次数后，将会在锁定时长期间无法进行登录。

11.2 设备管理

11.2.1 恢复出厂设置

可通过恢复出厂设置，将设备的所有配置重置为出厂时的默认配置。

进入页面的方法：系统工具 >> 设备管理 >> 恢复出厂配置



注意：

- 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。系统备份请前往：系统 >> 设备管理 >> 备份与导入配置。
- 恢复出厂配置后，设备将自动重启。

11.2.2 备份与导入配置

可保存或恢复系统配置。

进入页面的方法：系统工具 >> 设备管理 >> 备份与导入配置

点击<备份>保存当前的配置信息。设备将以文件形式保存系统设置，建议在进行软件升级前进行备份。

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。

注意：

- 如果导入的配置文件版本与现有版本差距过大，有可能导致配置信息丢失。。
- 导入配置信息后，设备将自动重启。

11.2.3 重启设备

设备的部分配置修改需要重启设备才能生效，可通过本页面来重启设备

进入页面的方法：系统 >> 设备管理 >> 重启设备

注意：

- **在设备重启过程中，请不要将设备断电！**

11.2.4 设备管理

在未开启云管理时，可以查看并设置设备名称。设备名称用于标识区分，默认为设备机型名及硬件版本号。

进入页面的方法：系统工具 >> 设备管理 >> 设备管理

开启云管理后，可登录 TP-LINK 商用网络云平台设置部分参数。

点击<登录 TP-LINK 商用网络云平台>进入 TP-LINK 商用云平台官网。

说明：

- 如需开启或管理云平台管理功能，请前往页面：系统 >> 云管理 >> 基本配置。

11.3 时间设置

可通过本页面查看和设置系统时间。

进入页面的方法：系统 >> 时间设置 >> 时间设置

通过网络获取系统时间，防火墙将通过网络获取 GMT 时间，选择时区和 NTP 服务器，点击<设置>。

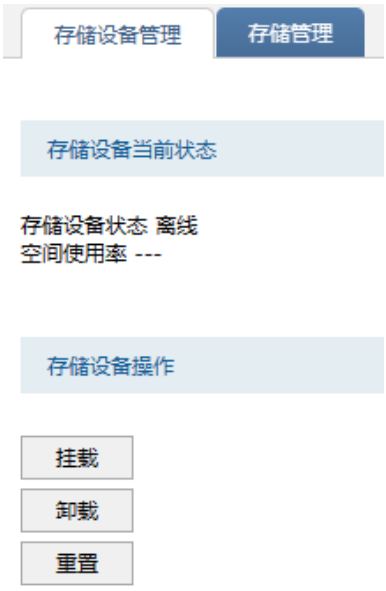
手动设置系统时间，可以通过手动输入的方式来设置防火墙日期和时间。可点击<获取管理主机时间>来直接获取管理主机时间。

11.4 存储管理

11.4.1 存储设备管理

可查看设备中的存储设备（硬盘/SD 卡）的状态并对其进行管理。

进入页面的方法：系统 >> 存储管理 >> 存储设备管理



挂载　　进行存储设备挂载操作。

卸载　　进行存储设备卸载操作。

重置　　进行存储设备重置操作，重置会清楚存储器中的所有数据，请谨慎操作。

说明：

- 首次插入的存储设备在挂载时会进行初始化，期间会清空插入设备中的所有数据。
- 请确保在进行存储设备的操作的过程中，不要将设备断电，不要拔出存储器。

11.4.2 存储管理

可查看设备中的日志/报表存储状态并对各类日志/报表的存储空间进行管理。

进入页面的方法：系统 >> 存储管理 >> 存储管理

告警阈值设置：

当任何一类日志/报表的存储空间达到或超过配置的“告警阈值”时（例如流量日志分配了 10%的存储空间、配置阈值为 85%，当其实际存储空间达到 8.5%时），系统会定时产生告警日志通知管理员尽快进行清理。

说明：

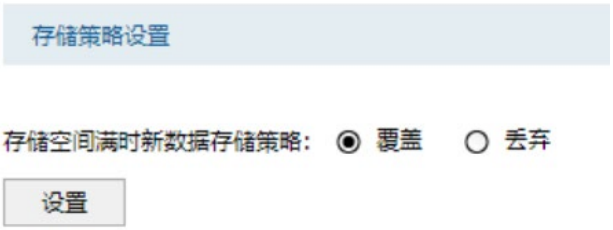
- 如需查看告警信息，请前往：面板 >> 系统状态 >> 告警信息；
- 如需进行告警配置请前往：系统 >> 告警配置。

存储策略设置：

设置硬盘空间满时的日志/报表处理方式。

覆盖：新产生的日志/报表覆盖旧数据。

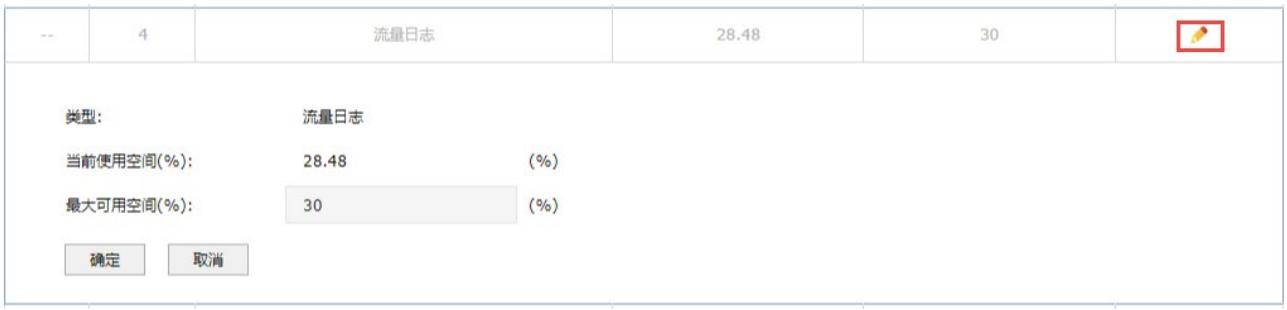
丢弃：不存储新产生的日志/报表。



存储空间列表：

可以通过该列表查看各类日志/报表当前使用空间大小并对每一类数据的最大可用空间进行配置。

点击<>可配置各类型日志的最大可使用空间。



11.5 诊断中心

11.5.1 诊断工具

防火墙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：监控 >> 诊断中心 >> 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。

11.5.2 诊断工具配置实例

- **需求介绍**

某用户内网无法上外网，希望可以通过防火墙诊断下问题原因所在。此时可以通过 PING 通信检测来判断接口与外网之间是否连通（出接口选择外网对应接口），或者可以检测防火墙与内网主机之间是否连通（出接口选择对应局域网接口）；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接口，此处因为仅用 GE1 口上网，所以选择 GE1 。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。

而当接口无法 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。

点击<开始>下方的圆形按钮，还可以自定义“PING 次数”（1-50）和“PING 包大小”（4-1472 Bytes）。

- **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接口，可以看到访问目的 IP/域名所经过的路由节点及延迟。

点击<开始>下方的圆形按钮，还可以自定义 路由跟踪最大 TTL （Time to Live，生存时间值），TTL 是 IP 数据包在计算机网络中可以转发的最大跳数，可设置值为 1-30。

11.5.3 故障诊断

当防火墙发生故障时，可先自行使用“诊断工具”功能检测，参考 ***11.5.1 诊断工具***。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。

进入页面的方法：监控 >> 诊断中心 >> 故障诊断

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。

故障诊断模式	开启本功能后可以配置技术支持人员对设备进行诊断。 勾选表示开启诊断模式；取消勾选表示诊断模式关闭。
诊断信息	点击<导出诊断信息>下载基本的诊断信息，将其提供给技术人员以协助分析和解决问题。

注意：

- 一般情况下请不要随意开启本功能。
- 需要诊断时，请先联系技术支持人员，在其协助下打开并使用本功能。

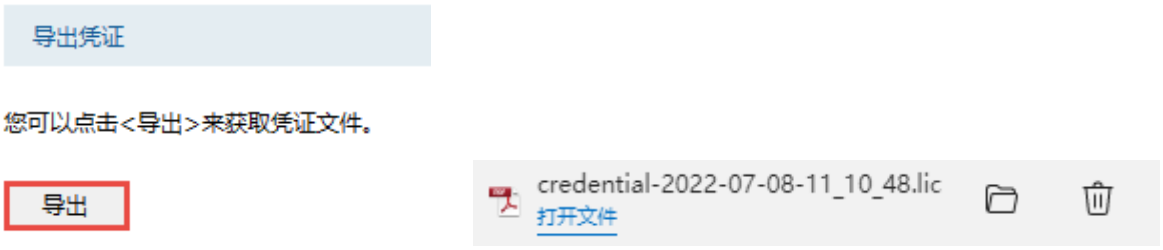
11.6 License 管理

可查看 License 资源授权情况。入侵防御、反病毒、恶意域名远程查询功能需要 License 授权使用。

进入页面的方法：系统 >> License 管理 >> License 管理

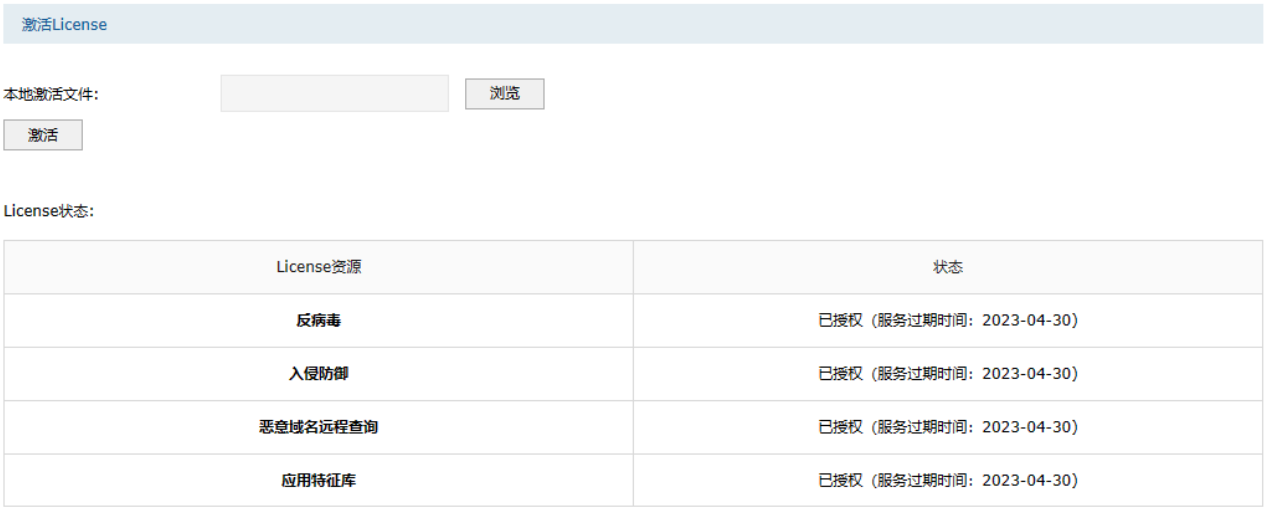
配置方法：

1. 点击<导出>可将凭证文件下载到本地，文件名称格式为“credential+时间.lic”。



2. 联系当地经销商，或拔打 TP-LINK 服务热线：400-8863-400，获取 License 授权文件。

3. 点击<浏览>从本地导入 License 激活文件，点击<激活>，License 授权激活成功后可使用对应的应用资源。



License资源	状态
反病毒	已授权（服务过期时间：2023-04-30）
入侵防御	已授权（服务过期时间：2023-04-30）
恶意域名远程查询	已授权（服务过期时间：2023-04-30）
应用特征库	已授权（服务过期时间：2023-04-30）

说明：

- 您可以到 TP-LINK 官网 特征库升级中心 下载最新的特征库。
- 如需升级特征库请前往页面：系统 >> 升级中心 >> 升级中心列表

11.7 系统升级

11.7.1 软件升级

可查看并升级设备软件。

进入页面的方法：系统 >> 设备管理 >> 软件升级

在线升级：点击<检查新版本>，防火墙自动检测当前软件是否为最新并更新软件。

本地升级：点击<浏览>选择本地升级文件，点击<升级>，更新软件。

说明：

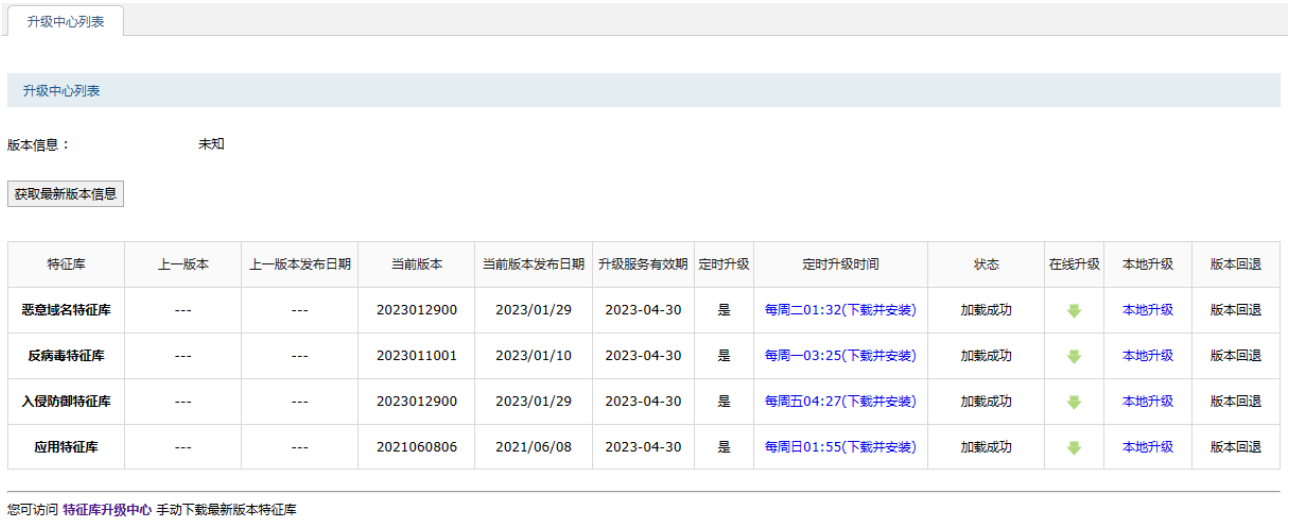
- 使用在线升级的时候请确保设备正常联网。
- 请确保在防火墙升级过程中，不要将防火墙断电，不要对页面进行刷新。升级完毕，防火墙将自动重启。
- 您可以到 TP-LINK 官网 www.tp-link.com.cn 下载最新的升级软件。

注意：

- 在防火墙升级过程中，请不要将防火墙断电。
- 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。

11.7.2 特征库升级

进入页面：系统 >> 升级中心，可对防火墙特征库进行升级操作。



获取最新版本信息	点击后，会同步云端信息，获取当前最新的版本库信息。如设置了自动升级，设备会在自动升级前，自动拉取云端信息。
升级服务有效期	用户购买的特征库的升级服务的有效期限，超出有效期后，无法升级过期的特征库。
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。
版本回退	将特征库版本回退到上一个版本。可以再次点击版本回退，回退到原来的版本。

您可以到 TP-LINK 官网 特征库升级中心 获取最新的特征库。

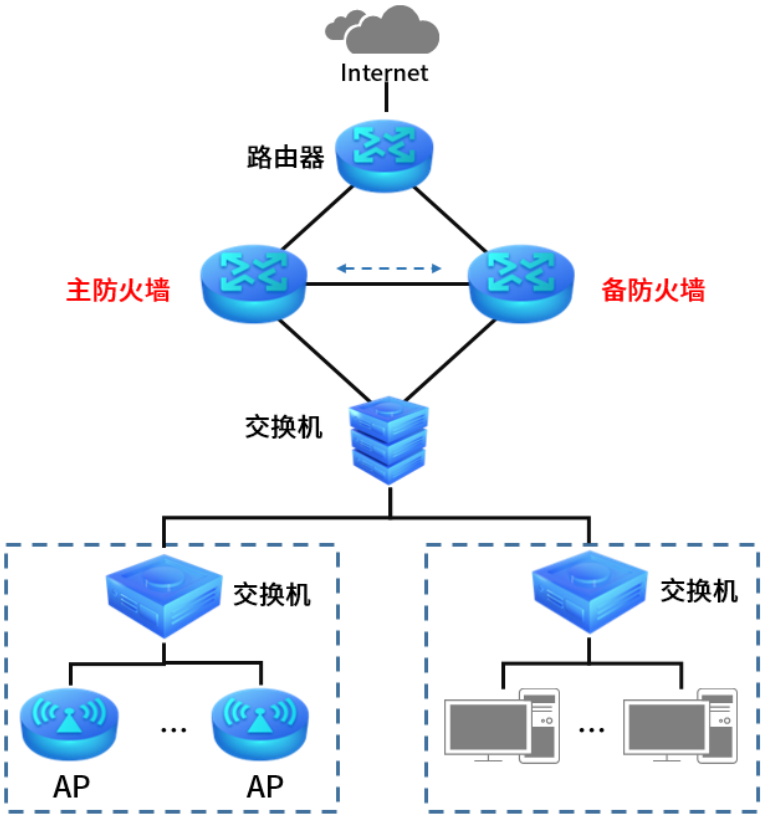
点击页面 ，查看更多页面设置参数信息。

说明：

- 如需获取功能授权，请参考 *11.6 License 管理*。

11.8 主备倒换

在主备模式下，主备机器之间会定时通过心跳接口发送心跳信号，通过选举运行主备状态，当异常发生时能够进行主备倒换。当主设备挂起时，业务自动切换到备用设备。



11.8.1 主备倒换设置

进入页面的方法：网络 >> 高可靠性 >> 主备倒换

主备倒换设置：

心跳接口	主备机器通过该接口进行通信，为保证主备倒换功能正常进行，请保证心跳接口的连通性。
状态	心跳接口的状态一旦启用后，将被设置为静态 IP，且无法进行其他业务。

注意：

- 接口的具体信息请到“接口设置”页面中设置成功后才可选中。拥有静态 IP 地址，且不是管理接口的以太网接口才可以成为心跳接口。只能存在一个心跳接口。

规则列表：

点击<新增>，添加主备倒换规则。

抢占模式配置	主设备配置为主模式且抢占，备设备配置备模式。
非抢占模式配置	主设备配置为主模式且非抢占，备设备配置备模式。

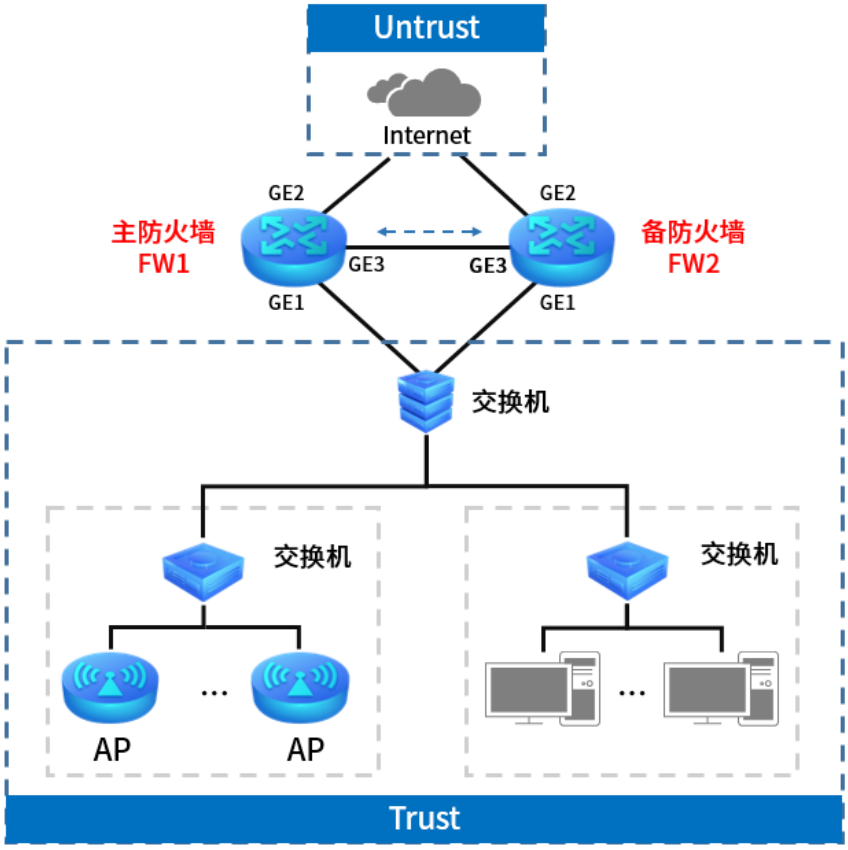
名称	条目名称。方便记忆和检索条目。
主备状态	设置设备为主设备或者备设备。
生效接口	主备倒换生效的接口。
VRID	虚拟路由器的 ID（VRID），可用值为 1-255。同一个 VRRP 组 VRID 必须相同。
通告间隔	通告时间间隔，单位是秒。同一个 VRRP 组通告间隔必须相同。
模式	设置主备模式。 非抢占：主设备从挂掉到恢复，不再将服务抢占过来。 抢占：主设备从挂掉到恢复，将服务抢占过来。
虚拟 IP 地址	虚拟路由器的 IP 地址。同一个 VRRP 组虚拟 IP 地址必须相同。
运行状态	设备正在运行的主备状态。
状态	启用禁用主备倒换功能。

注意：

- 当默认安全策略为禁止时，需要添加放行 VRRP 服务（该服务为系统预置）的安全策略规则，主备倒换功能才能正常使用。
- 虚拟 IP 地址会跟生效接口对应网关地址和 DNS 服务器自动保持同步。如果要使用自定义的网关地址和 DNS 地址，那么可以前往接口设置功能页面重新配置。
- 建议主备防火墙使用相同型号的设备，否则进行主备倒换后在性能上可能会有差异。

11.8.2 主备倒换配置实例

某公司为保证业务的可靠性，防止内外网业务中断，使用 TL-NFW8500 防火墙进行双机备份，拓扑图如下：



1. 该公司的安全策略默认为禁止，需要添加 VRRP 服务。

   进入页面：对象 >> 服务 >> 服务组，点击<新增>，选择 VRRP 服务，点击<确定>添加服务组。

   进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>，添加允许 VRRP 服务通过的策略。

2. 主防火墙（FW1）设置：

进入页面：网络 >> 接口设置 >> 接口设置，设置 GE2/3 接口的 IP 地址。

GE2：根据 ISP 提供的方式进行设置，保证设备能正常联网。

GE3：作为心跳接口，点击<新增>，选择 Ethernet 接口，添加静态 IP 地址，确认管理接口为关闭状态。

进入页面：网络 >> 安全区域 >> 安全区域，将 GE1 添加到 Trust，GE2 添加到 Untrust。

安全区域列表

新增 删除 刷新

	序号	名称	优先级	接口	备注	编辑
--	1	local	100	loopback	---	
--	2	trust	85	GE1	---	
--	3	untrust	5	GE2	---	
--	4	dmz	50	---	---	

为保证正常上网，需配置放行 Trust 到 Untrust 的安全策略。

进入页面：策略 >> 安全策略 >> 安全策略，点击<新增>添加安全策略，源安全区域选择 untrust，目的安全区域选择 trust，源地址选择内网地址组（可进入页面：对象 >> 地址 >> 地址组进行添加），动作为允许，内容安全部分可根据需求进行配置即可。

备防火墙（FW2）配置参考主防火墙（FW1）。

3. 主备倒换设置：

在主备设备（FW1、FW2）中，进入页面：系统 >> 高可靠性 >> 主备倒换，心跳接口选择在 GE3 接口处添加的 Ethernet 接口，主备倒换设置选择“开启”，点击<设置>使设置生效。

在主设备端（FW1）添加主备倒换规则如下，生效接口选择 GE1：

在备设备端（FW2）添加主备倒换规则如下，生效接口选择 GE1，VRID 及虚拟 IP 地址与主设备配置保持一致：

4. 将终端的网关配置为虚拟 IP。

至此，完成主备倒换配置。当主防火墙 FW1 挂起时，业务自动切换到备防火墙 FW2。

11.9 系统参数

可以通过本页面设置逻辑接口的 metric 参数。

静态 IP 接口	填写静态 IP 时的路由 Metric 信息。
DHCP 接口	填写 DHCP 获取动态 IP 时的路由 Metric 信息。
PPPoE 接口	填写 PPPoE 拨号时的路由 Metric 信息。
L2TP 接口	填写 L2TP 的路由 Metric 信息。
PPTP 接口	填写 PPTP 的路由 Metric 信息。

回目录