TP-LINK®

# 防火墙

TL-FW5600

# 用户手册

REV1.0.0

1910041011

# 声明

# 目录

# 第1章 前言

本手册旨在帮助您正确使用本款防火墙。内容包含对防火墙性能特征的描述以及配置防火墙的详细说明。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，

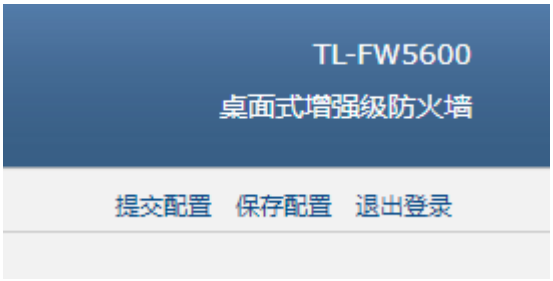
- 所提到的“防火墙”、“本产品”等名词，如无特别说明，系指TL-FW5600防火墙，下面简称为TL-FW5600。
- 用 >> 符号表示配置界面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 标签页**，其中，部分功能无二级菜单。
- 正文中出现的<>尖括号标记文字或图形，表示Web界面的按钮名称，如<确定>或<新增>。

本手册中使用的特殊图标说明如下：

| 图标 | 含义 |
| --- | --- |
| **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 保存配置

配置完成后，请务必点击页面右上角<提交配置><保存配置>，使配置内容生效。



# 第2章 产品介绍

## 2.1 产品描述

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路由器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-FW5600防火墙的固件采用了安全加密和数字签名机制，可有效阻止伪造、私自篡改固件，保障固件分发的安全可靠性，同时，防火墙还拥有固件升级的功能，可以在本地Web管理界面上进行升级，防火墙管理员可以在TP-LINK官网上下载最新的防火墙固件以实现整机功能的升级。

## 2.2 产品特性

### 硬件特性

- 采用64位双核网络专用处理器，单核主频1GHz；
- 配备容量为1GB的DDRIV高速内存；
- 提供5个10/100/1000M自适应以太网接口；
- 提供1个Console口；
- 内置高品质开关电源，无风扇静音设计；

### 功能特性

#### 接口

- 提供5个千兆物理端口，用户可自由定义端口类型（WAN/LAN/其他类型）；
- 提供多种逻辑接口类型，适应更多复杂的网络适用环境。

VPN

- 提供标准的IPSec VPN功能，支持数据完整性校验、数据源认证、防数据包重放和数据加密功能（DES、3DES、AES128、AES192、AES256等加密算法），支持IKE和手动模式建立VPN隧道，并支持通过域名方式配置VPN连接；
- 提供L2TP/PPTP VPN功能，支持L2TP/PPTP VPN服务器/客户端模式，可实现出差员工或分支结构远程安全接入公司网络。

Web认证

- 不需要客户端软件即可实现认证入网，降低网络维护工作量；
- 可自定义认证跳转页面，实现广告推送。

上网行为管理

- 应用限制：支持针对聊天类、P2P 类、金融类、游戏类、代理类及基础类等数十种常见应用的一键管控，有效限制可能降低企业员工工作效率的上网行为；同时支持基于用户组和时间段配置管控策略，方便灵活分配上网权限，保障关键用户的正常上网；
- 网址过滤：通过配置网站过滤和 URL 过滤规则，可对员工访问各种网站的权限进行管控，除了可以禁止/允许员工访问各种网站外，还可以记录其访问历史信息，甚至可以弹出警告页面。此外还支持网站分组功能，可方便地将庞杂的网站进行归类，供过滤规则调用，灵活而实用，同时防火墙出厂默认提供十多种网站分组，对于网管资源有限的中小型企业用户，可节省不少配置工作；
- 网页安全：支持禁止网页提交，可限制员工登录各种基于网页的论坛、网站、邮箱等发表信息，避免企业敏感数据外泄；支持过滤文件扩展类型，用户可方便地过滤内嵌在网页中的各种小文件，如 exe、rar、swf 文件等，避免病毒、木马等通过这些小文件侵入企业网络，危害网络安全；
- 行为审计：提供上网行为审计软件，可实时记录和审计员工上网行为，企业网络管理更简单。

防火墙

- 访问策略：通过配置访问控制策略，可允许或禁止特定应用数据流通过防火墙，比如FTP下载、收发邮件、Web浏览等，同时支持基于用户组和时间段配置策略，实现精细化管理；
- ARP 防护：支持 IP 与 MAC 地址自动扫描及一键绑定功能，可同时绑定 LAN 口（内网）、WAN 口（外网）主机的 IP 与 MAC 地址信息，有效防止 ARP 欺骗和非法接入；在遭受 ARP 欺骗时，防火墙可按照指定频率发送 ARP 更正信息，及时恢复网络正常状态；
- 攻击防护：支持内外网攻击防护功能，可有效防范各种常见的DoS攻击、扫描类攻击、可疑包攻击行为，如TCP Syn Flood、UDP Flood、ICMP Flood、WinNuke攻击、分片报文攻击、WAN口ping、TCP Scan（Stealth FIN/Xmas/Null）、IP欺骗等。

**带宽控制**

- 支持智能带宽控制功能，可根据实际的带宽利用率灵活启用带宽控制策略，可针对网络中每一台主机（IP）进行双向带宽控制，有效抑制BT、迅雷等P2P应用过度占用带宽，避免造成网络游戏卡、上网速度慢的问题，保障网络时刻畅通。

**连接数限制**

- 提供基于用户组的连接数限制功能，可限制每一台电脑的连接数占有量，合理利用有限的NAT连接数资源，防止少数用户过度占用大量连接数，确保游戏、上网、聊天、视频语音等顺畅进行。

**设备管理**

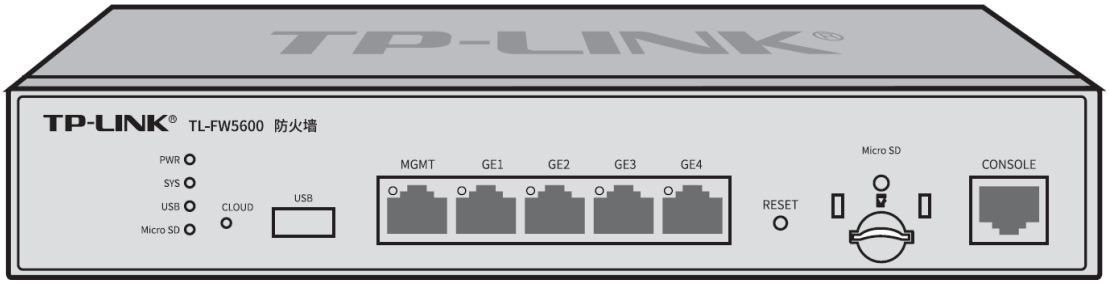
- 支持全中文Web网管，所有功能均可通过图形化界面进行配置，简单方便；
- 每一项配置均提供必要的帮助说明信息，有效降低配置难度。

**设备维护**

- 提供系统日志功能，详尽的日志信息便于快速发现网络异常并及时定位问题原因，实时监测 CPU 利用率等防火墙内部关键资源，及时发现潜在的各种危险和攻击；
- 支持本地及远程管理防火墙，方便远程协助；
- 支持Ping检测及Tracert检测等多种故障检测工具，并可备份和导入防火墙配置文件，方便快速确认网络连通状态。

## 2.3 产品外观

### 2.3.1 前面板




- USB接口

用于连接存储设备，TL-FW5600 可提供存储日志。

- 5个10/100/1000Mbps自适应RJ45接口

TL-FW5600支持10Mbps/100Mbps/1000Mbps速率的连接设备。每个接口对应一个Link/Ac指示灯。

- Reset键

复位键。在防火墙通电的情况下，使用尖状物长按防火墙的Reset按键，直至系统指示灯快速闪烁时松开，防火墙将自动恢复出厂设置并重启。防火墙出厂默认管理地址是http://192.168.1.1。

- Micro SD卡

用于插入 Micro SD 卡

- 1个Console接口

Console接口位于面板最右边，使用此接口可以对防火墙进行命令行配置。

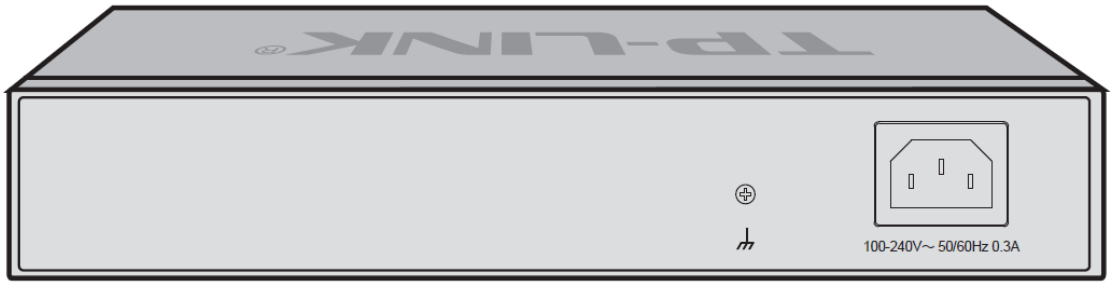
- 指示灯

通过指示灯可以监控防火墙的工作状态，下表将详细说明指示灯工作状态：

| 指示灯 | 名称 | 状态描述 |
| --- | --- | --- |
| PWR | 电源指示灯 | 常亮表示系统供电正常 |
| | | 常灭表示电源关闭或电源故障 |
| SYS | 系统指示灯 | 系统上电后，常灭约 40 秒后持续快闪，直至系统开始正常工作， |

| 指示灯 | 名称 | 状态描述 |
| --- | --- | --- |
| | | 如果需要加载的软件功能较多，系统启动时间可能需要数分钟，请耐心等待 |
| | | 系统正常工作时以每秒 1 次的频率闪烁 |
| | | 其他状态表示系统异常 |
| USB | 接口指示灯 | 常亮表示端口与设备正常连接 |
| | | 熄灭表示端口与设备未正常连接 |
| Micro SD | 接口指示灯 | 常亮表示 Micro SD 卡正常连接 |
| | | 熄灭表示 Micro SD 卡未正常连接 |
| CLOUD | 云管理指示灯 | 常亮表示连接到云管理平台 |
| | | 闪烁表示与云管理平台连接中，且有数据收发 |
| | | 熄灭表示未连接注册到云管理平台 |
| Link/Act | 连接状态指示灯 | 常亮表示相应端口已正常连接 |
| | | 闪烁表示相应端口正在传输数据 |
| | | 常灭表示相应端口未建立连接 |

## 2.3.2 后面板




- 电源接口

位于后面板右侧，设备正常工作时的输入电源参数为100-240V~ 50/60Hz，最大工作电流不超过0.3A，为保证设备及电源设施正常工作，请确保供电电源完全满足设备的要求。

- 防雷接地柱

请使用黄绿双色外皮的铜芯导线接地，以防雷击，具体请参考《设备防雷安装手册》。

**说明：**

- 请使用原装电源线。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

# 第3章 登录与快速配置

**说明：**

**第一次登录本地Web管理界面时，需要确认以下几点：**

- 1) 防火墙已正常加电启动，MGMT 口已与管理主机相连。
- 2) 管理主机已正确安装有线网卡及该网卡的驱动程序，且已至少安装一种以下浏览器：IE 8.0 或以上版本、FireFox 最新版本、Chrome 最新版本和 Safari 最新版本。
- 3) 管理主机 IP 地址已设为与防火墙 MGMT 口同一网段，即 192.168.1.X（X 为 2 至 254 之间的任意整数），子网掩码为 255.255.255.0，默认网关为防火墙管理地址 192.168.1.1。
- 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。

1. 打开 IE 浏览器，在地址栏输入 http://192.168.1.1 登录防火墙的 Web 管理界面。

2. 防火墙首次登录界面如下图所示。首次登录时，请先设置用户名和管理员密码。管理页密码是进入设备管理页面的凭证，确认提交前请牢记管理页账户和密码。


3. 重新输入新设置的用户名和密码，点击登录。

4. 成功登录后，进入系统>>快速配置 可对防火墙进行快速配置，点击下一步。


5. 首先配置基本信息，点击<下一步>,。


6. 配置系统时间，点击<下一步>。

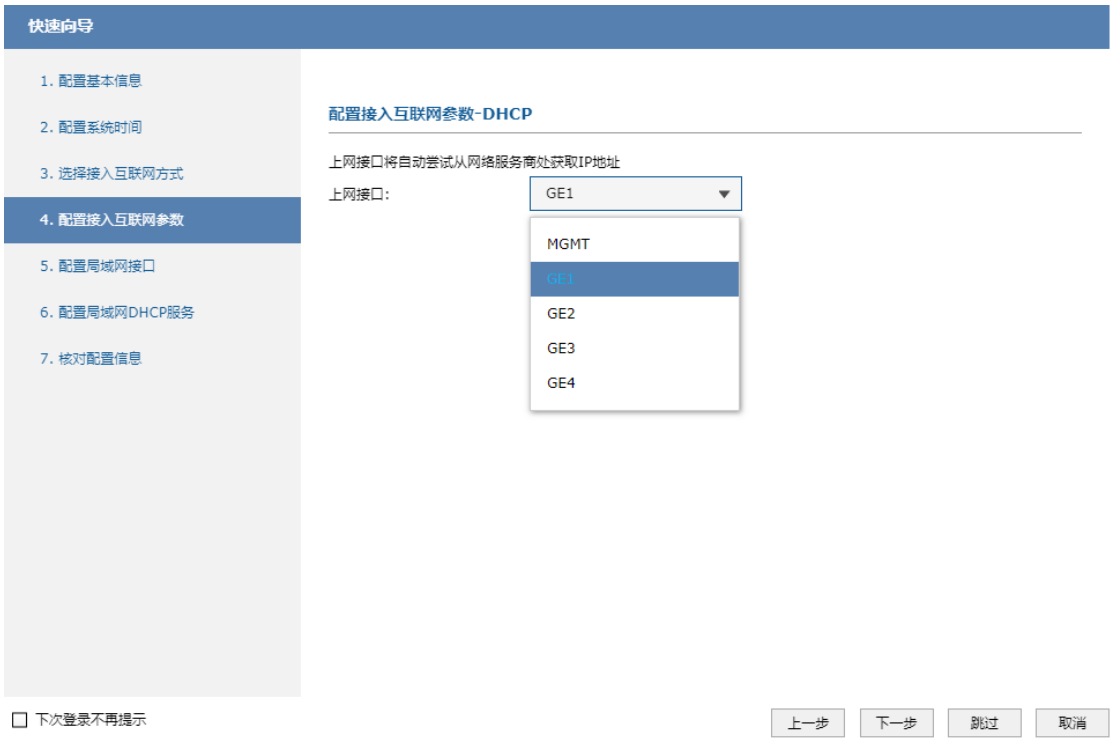

7. 选择互联网接入方式，点击<下一步>。


8. 配置接入互联网参数，点击<下一步>。


- 如果上网方式为“静态 IP”，即拥有网络服务商提供的固定 IP 地址，则需要填写以下内容。

| | |
|---|---|
| **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。 |


- 如果上网方式为“DHCP”，即可以自动从网络服务商处获取 IP 地址，需要选择上网接口。



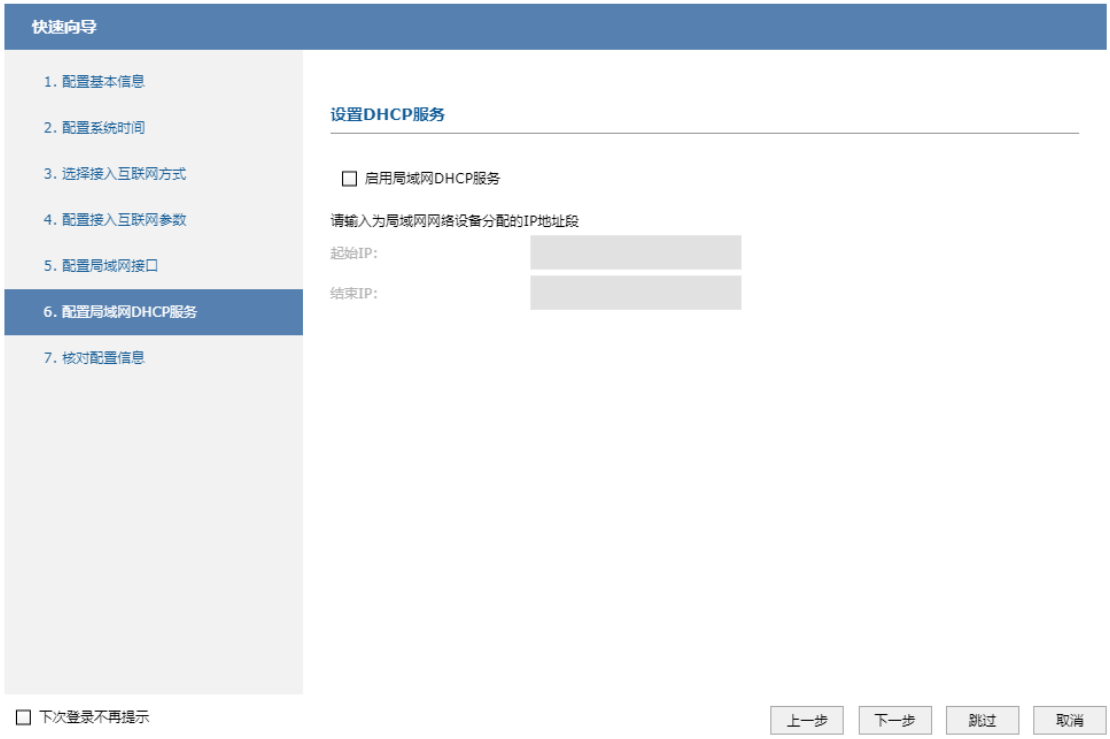

- 如果上网方式为“PPPoE 拨号”，即虚拟拨号方式，则需要填写以下内容：

| | |
|---|---|
| **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。 |
| --- | --- |

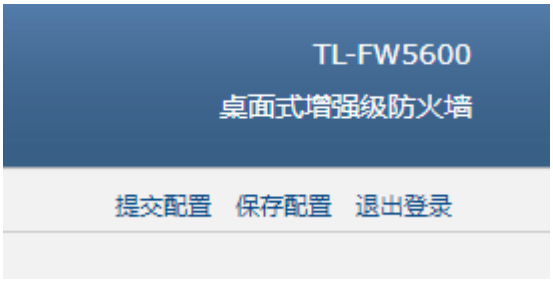

9. 配置局域网接口，点击<下一步>。


10. 配置局域网 DHCP 服务，点击<下一步>。




11. 核对配置信息，点击<应用>，完成配置。


12. 配置完成后，请点击页面右上角<提交配置><保存配置>，保存配置参数，避免退出管理页面有参数丢失。

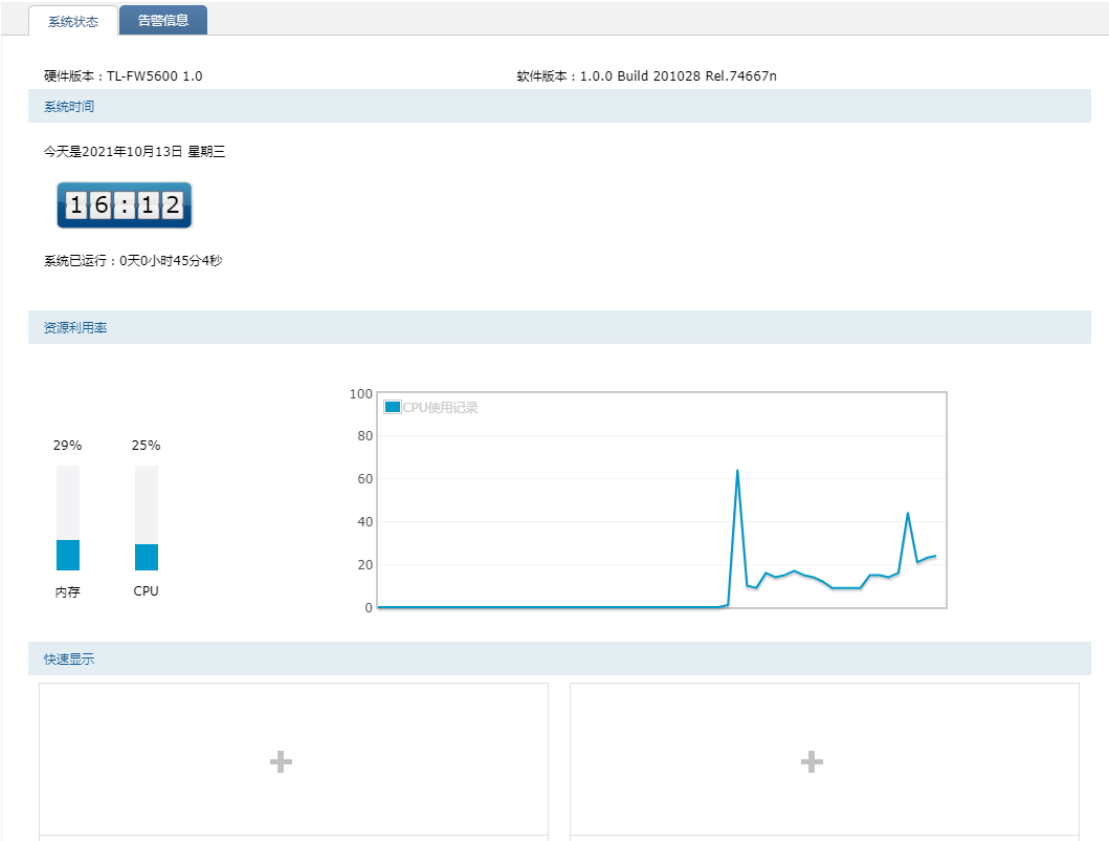


# 第4章 面板

## 4.1 系统状态

防火墙成功登录配置后可以看到防火墙的系统状态信息，如下图所示。

**进入界面：面板 >> 系统状态 >> 系统状态**




在系统状态界面中，可以查看防火墙的硬件和软件版本、系统时间、CPU 利用率和接口信息。

**系统时间**：显示防火墙当前的系统时间。

**资源利用率：在此区域可检测防火墙内存和 CPU 的利用率。**CPU 利用率平均推荐值为 50%左右，高于 85%表示防火墙处于高负载状态，高于 95%表示满负载状态，当 CPU 利用率持续较高时，部分功能可能将异常，此时可能是网络中出现异常，请进行排查。

**快速显示**：点击各区域的< + >按钮可添加并查看接口信息。

## 4.2 告警信息

可查看设备告警信息。

**进入界面：面板 >> 系统状态 >> 告警信息**


- 内容

点击<内容>，可筛选表格中是否显示时间、功能模块、严重等级、详细信息这四种内容。


- 清空

点击<清空>，可清除设备所有的报警信息。

- 搜索

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、严重等级、详细信息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；<br>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。 |

- 日志搜索

点击<日志搜索>，可搜索一个时间范围内，不同功能模块和不同严重等级的告警信息。


| | |
|---|---|
| **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。 |
| **严重等级** | 选择事件的严重等级。 |
| **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。 |

- 刷新

点击<刷新>，更新告警信息列表。

- 自动刷新

勾选<自动刷新>，设备自动更新告警信息列表。

# 第5章 监控

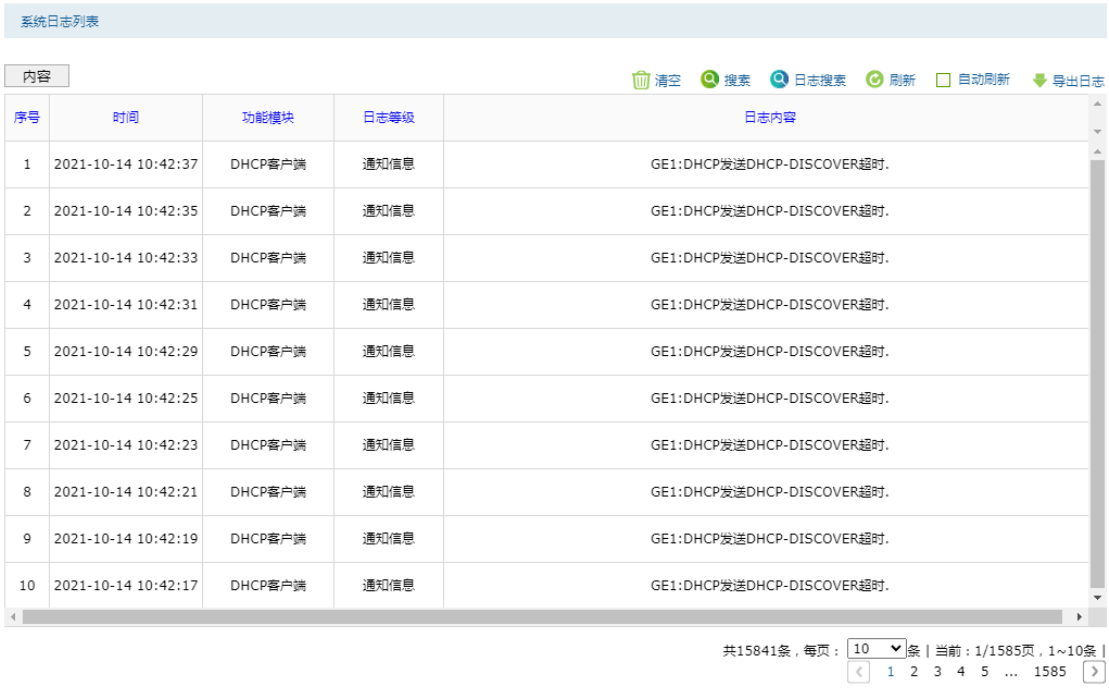
## 5.1 日志

通过查看日志，管理员可以及时了解设备在运行过程中产生的信息，监控设备运行状态和定位故障。

### 5.1.1 系统日志

您可以通过本页面来查看系统运行状况。日志记录了事件发生的日期时间、并对事件发生的主体、客体进行了描述

**进入界面：监控 >>日志 >> 系统日志**




- 内容

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。 |

- 清空

点击<清空>，可清除系统日志列表中所有信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **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；<br>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。 |

- 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。 |

- 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。

## 5.1.2 操作日志

**进入界面：监控 >>日志 >> 操作日志**


- 内容

点击<内容>，可筛选表格中是否显示时间、管理员、登录 IP 地址和详细内容。


- 清空

点击<清空>，可清除操作日志列表中所有信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择时间、管理员、登录 IP 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；<br>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。 |

- 日志搜索

点击<日志搜索>，可搜索特定时间范围内，不同管理员和不同登录 IP 的操作日志信息。


| | |
|---|---|
| **开始时间** | 设置开始时间。 |
| **结束时间** | 设置结束时间。 |
| **管理员** | 选择进行操作的管理员。 |
| **登录 IP 地址** | 选择进行操作的管理员的登录 IP。 |
| **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。 |

- 刷新

点击<刷新>，更新操作日志列表信息。

- 自动刷新

勾选<自动刷新>，自动更新操作日志列表信息。

- 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。

## 5.1.3 流量日志

**进入界面：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 | 协议 | 应用 | 应用组 | 上行流 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2021-10-14 11:06:19 | 2021-10-14 11:06:34 | trust | local | 192.168.1.3 | 192.168.1.1 | 55126 | 80 | --- | TCP | --- | --- | 918B |
| 2 | 2021-10-14 11:06:06 | 2021-10-14 11:06:34 | trust | local | 192.168.1.3 | 192.168.1.1 | 64338 | 53 | --- | UDP | --- | --- | 385B |
| 3 | 2021-10-14 11:06:14 | 2021-10-14 11:06:29 | trust | local | 192.168.1.3 | 192.168.1.1 | 55832 | 80 | --- | TCP | --- | --- | 918B |
| 4 | 2021-10-14 11:06:00 | 2021-10-14 11:06:28 | trust | local | 192.168.1.3 | 192.168.1.1 | 51523 | 53 | --- | UDP | --- | --- | 310B |
| 5 | 2021-10-14 11:06:00 | 2021-10-14 11:06:28 | trust | local | 192.168.1.3 | 192.168.1.1 | 54828 | 53 | --- | UDP | --- | --- | 310B |
| 6 | 2021-10-14 11:06:09 | 2021-10-14 11:06:24 | trust | local | 192.168.1.3 | 192.168.1.1 | 49939 | 80 | --- | TCP | --- | --- | 918B |
| 7 | 2021-10-14 11:06:04 | 2021-10-14 11:06:19 | trust | local | 192.168.1.3 | 192.168.1.1 | 57408 | 80 | --- | TCP | --- | --- | 918B |
| 8 | 2021-10-14 11:05:59 | 2021-10-14 11:06:14 | trust | local | 192.168.1.3 | 192.168.1.1 | 54330 | 80 | --- | TCP | --- | --- | 918B |
| 9 | 2021-10-14 11:05:54 | 2021-10-14 11:06:09 | trust | local | 192.168.1.3 | 192.168.1.1 | 55682 | 80 | --- | TCP | --- | --- | 918B |
| 10 | 2021-10-14 11:05:49 | 2021-10-14 11:06:04 | trust | local | 192.168.1.3 | 192.168.1.1 | 58122 | 80 | --- | TCP | --- | --- | 918B |

- 内容

点击<内容>，可筛选表格中是否显示流量起始时间、流量结束时间、源安全区域、目的安全区域等内容。


- 清空

点击<清空>，可清除流量日志列表中所有信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择流量起始时间、流量结束时间等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；<br>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。 |

- 日志搜索

点击<日志搜索>，可搜索特定时间范围内，不同安全区域、不同地址等各种自定义条件的流量日志信息。


| | |
|---|---|
| **开始时间** | 设置开始时间。 |

| | |
|---|---|
| **结束时间** | 设置结束时间。 |
| **源安全区域** | 选择数据流源安全区域。 |
| **目的安全区域** | 选择数据流目的安全区域。 |
| **源地址** | 数据流源地址。 |
| **目的地址** | 数据流目的地址。 |
| **源端口** | 数据流源端口，仅对 TCP/UDP 有效。 |
| **目的端口** | 数据流目的端口，仅对 TCP/UDP 有效。 |
| **入接口** | 连接的入接口。 |
| **出接口** | 连接的出接口。 |
| **用户** | 数据流对应的用户。 |
| **协议** | 数据流协议。 |
| **应用** | 数据流应用。 |

- 刷新

点击<刷新>，更新流量日志列表信息。

- 自动刷新

勾选<自动刷新>，自动更新流量日志列表信息。

- 导出日志

点击<导出日志>，设备将以文件形式保存当前设备中的日志,最多支持导出最近的 100000 条日志。

## 5.1.4 策略命中日志

**进入界面：监控 >>日志 >> 策略命中日志**


- 内容

点击<内容>，可筛选表格中是否显示时间、源安全区域、目的安全区域等内容。


- 清空

点击<清空>，可清除策略命中日志列表中所有信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择时间、源安全区域、目的安全区域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；<br>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。 |

- 日志搜索

点击<日志搜索>，可搜索特定时间范围内，不同安全区域、不同地址等各种自定义条件的策略命中日志信息。


| | |
|---|---|
| **开始时间** | 设置开始时间。 |
| **结束时间** | 设置结束时间。 |
| **源安全区域** | 选择数据流源安全区域。 |
| **目的安全区域** | 选择数据流目的安全区域。 |
| **源地址** | 数据流源地址。 |
| **目的地址** | 数据流目的地址。 |
| **源端口** | 数据流源端口，仅对 TCP/UDP 有效。 |
| **目的端口** | 数据流目的端口，仅对 TCP/UDP 有效。 |
| **用户** | 数据流对应的用户。 |
| **协议** | 数据流协议。 |
| **应用** | 数据流应用。 |

| | |
|---|---|
| **动作** | 筛选阻止或放行的策略。 |
| **安全策略** | 选择已建立的安全策略。 |

- 刷新

点击<刷新>，更新策略命中日志列表信息。

- 自动刷新

勾选<自动刷新>，自动更新策略命中日志列表信息。

- 导出日志

点击<导出日志>，设备将以文件形式保存当前设备中的日志,最多支持导出最近的 100000 条日志。

## 5.1.5 威胁日志

**进入界面：监控 >>日志 >> 威胁日志**


- 内容

点击<内容>，可筛选表格中是否显示时间、威胁类型、源安全区域、目的安全区域等内容。


- 清空

点击<清空>，可清除威胁日志列表中所有信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择时间、威胁类型、源安全区域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；<br>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。 |

- 日志搜索

点击<日志搜索>，可搜索特定时间范围内，不同安全区域、不同地址等各种自定义条件的威胁日志信息。


| | |
|---|---|
| **开始时间** | 设置开始时间。 |
| **结束时间** | 设置结束时间。 |
| **源安全区域** | 选择数据流源安全区域。 |
| **目的安全区域** | 选择数据流目的安全区域。 |
| **源地址** | 数据流源地址。 |
| **目的地址** | 数据流目的地址。 |
| **源端口** | 数据流源端口，仅对 TCP/UDP 有效。 |

| | |
|---|---|
| **目的端口** | 数据流目的端口，仅对 TCP/UDP 有效。 |
| **协议** | 数据流协议。 |
| **应用** | 数据流应用。 |
| **安全策略** | 选择已建立的安全策略。 |
| **威胁类型** | 详细信息内，入侵防御检测到的威胁的类别。 |
| **威胁名称** | 防火墙检测到的威胁的名称。 |
| **威胁 ID** | 防火墙检测到的威胁的 ID 编号。 |
| **动作** | 筛选阻止或放行威胁处理动作。 |

- 刷新

点击<刷新>，更新威胁日志列表信息。

- 自动刷新

勾选<自动刷新>，自动更新威胁日志列表信息。

- 导出日志

点击<导出日志>，设备将以文件形式保存当前设备中的日志,最多支持导出最近的 100000 条日志。

## 5.1.6 URL 日志

**进入界面：监控 >>日志 >> URL 日志**


- 内容

点击<内容>，可筛选表格中是否显示时间、URL、URL 分组等内容。


- 清空

点击<清空>，可清除 URL 日志列表中所有信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择时间、URL、URL 分组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；<br>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。 |

- 日志搜索

点击<日志搜索>，可搜索特定时间范围内，不同安全区域、不同地址等各种自定义条件的 URL 日志信息。


| | |
|---|---|
| **开始时间** | 设置开始时间。 |
| **结束时间** | 设置结束时间。 |
| **源安全区域** | 选择数据流源安全区域。 |
| **目的安全区域** | 选择数据流目的安全区域。 |
| **源地址** | 数据流源地址。 |
| **目的地址** | 数据流目的地址。 |
| **源端口** | 数据流源端口，仅对 TCP/UDP 有效。 |
| **目的端口** | 数据流目的端口，仅对 TCP/UDP 有效。 |
| **用户** | 数据流对应的用户。 |
| **协议** | 数据流协议。 |
| **应用** | 数据流应用。 |
| **URL** | 被过滤的 URL。 |
| **URL 分组** | 被过滤的 URL 的分组。 |
| **URL 过滤类型** | 选择 URL 过滤类型。 |
| **动作** | 筛选阻止或放行的 URL 过滤处理动作。 |
| **安全策略** | 选择已建立的安全策略。 |
| **URL 过滤配置文件** | 匹配到安全策略对应的 URL 过滤配置文件。 |

- 刷新

点击<刷新>，更新 URL 日志列表信息。

- 自动刷新

勾选<自动刷新>，自动更新 URL 日志列表信息。

- 导出日志

点击<导出日志>，设备将以文件形式保存当前设备中的日志,最多支持导出最近的 100000 条日志。

## 5.1.7 内容日志

**进入界面：监控 >>日志 >> 内容日志**


- 内容

点击<内容>，可筛选表格中是否显示时间、类型、文件名等内容。


- 清空

点击<清空>，可清除内容日志列表中所有信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择时间、类型、文件名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；<br>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。 |

- 日志搜索

点击<日志搜索>，可搜索特定时间范围内，不同安全区域、不同地址等各种自定义条件的内容日志信息。


| | |
|---|---|
| **开始时间** | 设置开始时间。 |
| **结束时间** | 设置结束时间。 |
| **源安全区域** | 选择数据流源安全区域。 |
| **目的安全区域** | 选择数据流目的安全区域。 |
| **源地址** | 数据流源地址。 |
| **目的地址** | 数据流目的地址。 |
| **源端口** | 数据流源端口，仅对 TCP/UDP 有效。 |
| **目的端口** | 数据流目的端口，仅对 TCP/UDP 有效。 |
| **用户** | 数据流对应的用户。 |
| **协议** | 数据流协议。 |
| **应用** | 数据流应用。 |
| **动作** | 筛选阻止或放行的策略。 |
| **安全策略** | 选择已建立的安全策略。 |
| **类型** | 内容日志对应的内容或应用行为控制的类型。 |
| **文件名** | 数据流包含的文件的名称。 |
| **文件类型** | 选择文件类型。 |

- 刷新

点击<刷新>，更新内容日志列表信息。

- 自动刷新

勾选<自动刷新>，自动更新内容日志列表信息。

- 导出日志

点击<导出日志>，设备将以文件形式保存当前设备中的日志,最多支持导出最近的 100000 条日志。

## 5.1.8 邮件过滤日志

**进入界面：监控 >>日志 >> 邮件过滤日志**


- 内容

点击<内容>，可筛选表格中是否显示时间、源安全区域、目的安全区域等内容。


- 清空

点击<清空>，可清除邮件过滤日志列表中所有信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择时间、类型、文件名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；<br>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。 |

- 日志搜索

点击<日志搜索>，可搜索特定时间范围内，不同安全区域、不同地址等各种自定义条件的邮件过滤日志信息。


| | |
|---|---|
| **开始时间** | 设置开始时间。 |
| **结束时间** | 设置结束时间。 |
| **源安全区域** | 选择数据流源安全区域。 |
| **目的安全区域** | 选择数据流目的安全区域。 |
| **源地址** | 数据流源地址。 |
| **目的地址** | 数据流目的地址。 |
| **源端口** | 数据流源端口，仅对 TCP/UDP 有效。 |
| **目的端口** | 数据流目的端口，仅对 TCP/UDP 有效。 |
| **用户** | 数据流对应的用户。 |
| **邮件协议** | 数据流协议。 |
| **应用** | 数据流应用。 |
| **动作** | 筛选阻止或放行的策略。 |
| **安全策略** | 选择已建立的安全策略。 |
| **配置文件** | 命中安全策略对应邮件内容过滤配置文件名称。 |
| **发件人** | 过滤邮件的发件人。 |
| **收件人** | 过滤邮件的附收件人。 |

- 刷新

点击<刷新>，更新邮件过滤日志列表信息。

- 自动刷新

勾选<自动刷新>，自动更新邮件过滤日志列表信息。

- 导出日志

点击<导出日志>，设备将以文件形式保存当前设备中的日志,最多支持导出最近的 100000 条日志。

## 5.2 报表

管理员可以通过查看报表来获知当前使用网络的用户、应用、安全事件以及流经网络的通信流量特征，并根据报表统计分析结果进行相应的防护控制。

### 5.2.1 流量报表

以源地址、目的地址、安全策略、接口、应用、应用组、用户为统计条件，筛选流量报表。报表图可以折线图、柱状图、饼状图多种形状展示，并可导出为 pdf 和 CSV 文件。

**进入界面：监控 >>报表 >> 流量报表**

首先，选择源地址、目的地址、安全策略、接口、应用、应用组、用户中一个作为统计条件；其次，点击<时间>，选择过去一段时间或自定义时间范围；然后，选择查看上行流量、下行流量或总流量的报表，并选择报表以叠加图、折线图、柱状图或饼图的方式呈现；最后，点击<加载报表>，获取报表。

点击<导出 PDF>，当前报表将以 PDF 的形式导出到本地。

点击<导出 CSV>，当前报表将以 CSV 的形式导出到本地。


## 5.2.2 策略命中报表

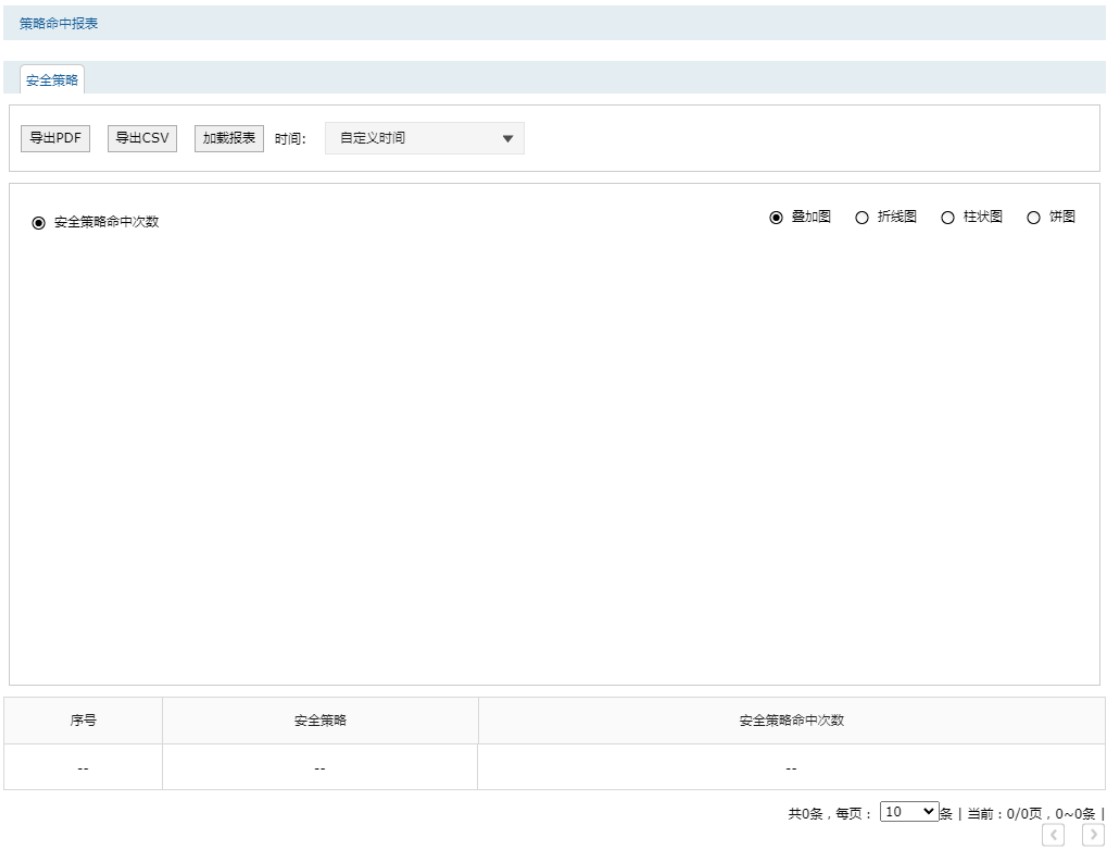
您可以安全策略为统计条件，筛选策略命中报表。报表图可以折线图、柱状图、饼状图多种形状展示，并可导出为 pdf 和 CSV 文件。

**进入界面：监控 >>报表 >> 策略命中报表**

首先，点击<时间>，选择过去一段时间或自定义时间范围；然后，选择报表以叠加图、折线图、柱状图或饼图的方式呈现；最后，点击<加载报表>，获取报表。

点击<导出 PDF>，当前报表将以 PDF 的形式导出到本地。

点击<导出 CSV>，当前报表将以 CSV 的形式导出到本地。




### 5.2.3 威胁报表

您可以攻击者、攻击目标、安全策略、威胁类型、威胁名称为统计条件，筛选威胁报表。报表图可以折线图、柱状图、饼状图多种形状展示，并可导出为 pdf 和 CSV 文件。

**进入界面：监控 >>报表 >> 威胁报表**

首先，选择攻击者、攻击目标、安全策略、威胁类型、威胁名称中一个作为统计条件；其次，点击<时间>，选择过去一段时间或自定义时间范围；然后，选择报表以叠加图、折线图、柱状图或饼图的方式呈现；最后，点击<加载报表>，获取报表。

点击<导出 PDF>，当前报表将以 PDF 的形式导出到本地。

点击<导出 CSV>，当前报表将以 CSV 的形式导出到本地。


## 5.3 系统统计

管理员可以通过查看报表来获知当前使用网络的用户、应用、安全事件以及流经网络的通信流量特征，并根据报表统计分析结果进行相应的防护控制。

### 5.3.1 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，以及 WAN 口的附加信息统计。

**进入界面：监控 >> 系统统计 >> 接口流量统计**


- 导出 pdf

点击<导出 pdf>，可将统计列表以 pdf 形式到本地。

- 清空

点击<清空>，可清除当前所有列表信息。

- 搜索

点击<搜索>，可根据接口、内容和方式进行搜索。


| | |
|---|---|
| **接口** | 默认以接口作为搜索关键列。 |
| **内容** | 选择需搜索的接口名称。 |
| **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；<br>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。 |

- 刷新

点击<刷新>，更新接口流量统计列表信息。

- 自动刷新

勾选<自动刷新>，自动更新接口流量统计列表信息。

## 5.3.2 IP 流量统计

IP 流量统计界面将显示指定 IP 范围之间各个 IP 的即时流量信息 。

**进入界面：监控 >> 系统统计 >> IP 流量统计**


- 导出 pdf

点击<导出 pdf>，可将统计列表以 pdf 形式到本地。

- 功能设置

| | |
|---|---|
| **启用 IP 流量统计** | 勾选该条目，启用 IP 流量统计功能。 |
| **监控 IP 范围** | 输入需监控的 IP 地址范围。 |
| **设置** | 点击设置，使功能设置配置生效。 |

- 清空

点击<清空>，可清除当前所有列表信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **接口** | 默认以 IP 地址作为搜索关键列。 |
| **内容** | 设置需搜索的 IP 地址。 |
| **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；<br>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。 |

- 刷新

点击<刷新>，更新 IP 流量统计列表信息。

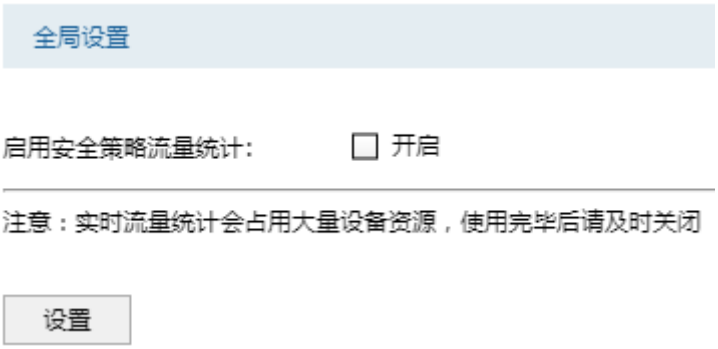
- 自动刷新

勾选<自动刷新>，自动更新 IP 流量统计列表信息。

## 5.3.3 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。

**进入界面：监控 >> 系统统计 >> 安全策略流量统计**

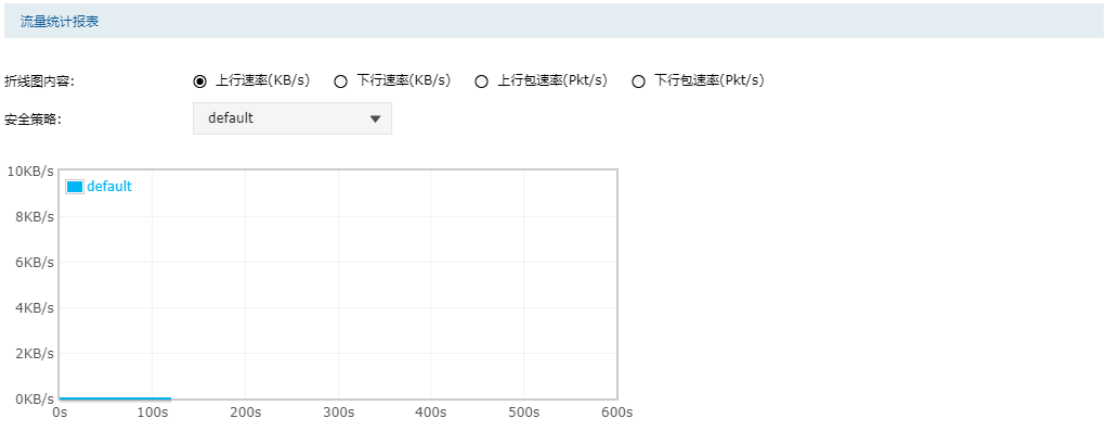



- 全局设置

| | |
|---|---|
| **启用安全策略流量统计** | 勾选该条目，启用安全策略流量统计功能。 |
| **设置** | 点击设置，使配置生效。 |

配置生效后，可查看流量统计报表和流量统计列表。

- 流量统计报表




| | |
|---|---|
| **折线图内容** | 选择需要实时查看的内容。 |
| **安全策略** | 选择需查看的安全策略。 |

- 流量统计列表


- 清空

点击<清空>，可清除当前所有列表信息。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **接口** | 默认以安全策略作为搜索关键列。 |
| **内容** | 选择需搜索的安全策略名称。 |
| **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；<br>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。 |

- 刷新

点击<刷新>，更新安全策略流量统计列表信息。

- 自动刷新

勾选<自动刷新>，自动更新安全策略流量统计列表信息。

# 5.4 诊断中心

## 5.4.1 诊断工具

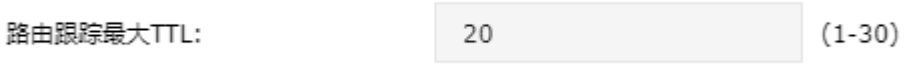
您可以通过诊断工具来检测和诊断当前的网络状况。

**进入界面：监控 >> 诊断中心 >> 诊断工具**


| | |
|---|---|
| **诊断工具类型** | 用于诊断网络状况的方式。有下面两种：<br>PING 通信检测；路由跟踪检测。 |
| **目的 IP/域名** | 需要进行 Ping 通信检测或者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 Ping 通信检测或者路由跟踪检测的接口。 |
| **开始** | 开始检测。 |

点击  >，可设置检测参数。


| | |
|---|---|
| **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。 |



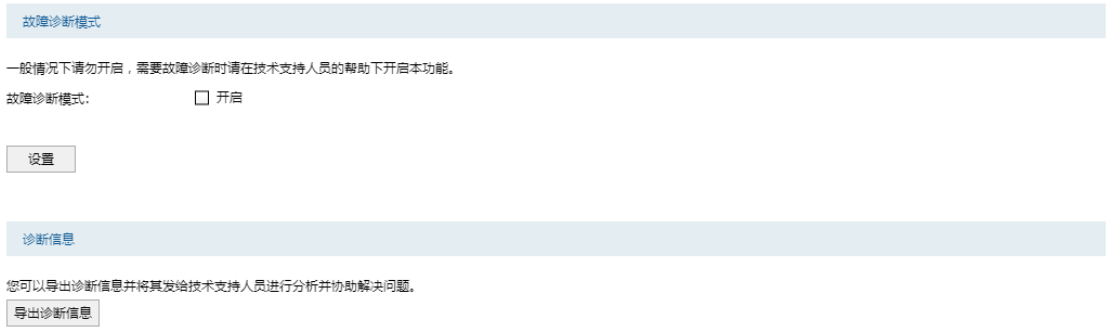

| | |
|---|---|
| **路由跟踪最大 TTL** | 设置路由跟踪检测发送数据包在网络中的最大转发跳数。 |

## 5.4.2 故障诊断

**进入界面：监控 >> 诊断中心 >> 故障诊断**

**说明：**

- 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。




- 故障诊断模式

| | |
|---|---|
| **故障诊断模式** | 勾选开启，打开故障诊断模式。 |
| **设置** | 点击设置，配置生效。 |

- 诊断信息

| | |
|---|---|
| **导出诊断信息** | 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。 |

# 第6章 策略

## 6.1 安全策略

### 6.1.1 安全策略

**进入界面：策略>> 安全策略 >> 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。


点击<新增>，新增策略规则。


| | |
|---|---|
| **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。 |
| **目的安全区域** | 指定安全策略匹配的数据流目的安全区域。 |
| **源地址** | 指定安全策略匹配的数据流源地址。 |
| **目的地址** | 指定安全策略匹配的数据流目的地址。 |
| **用户组** | 指定安全策略匹配的用户组。用户组的创建过程请参考 7.4.1 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 7.5.1 服务组。 |
| **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 7.7.1 应用组。 |
| **时间段** | 指定安全策略生效的时间段。 |
| **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。 |

点击< >，可编辑默认规则的动作为允许或禁止，编辑其它规则条目的各项信息。

点击<删除>，可批量删除策略规则，但不能删除默认规则。

## 6.1.2 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。

**进入界面：策略>> 安全策略 >> 策略冗余分析**

点击<开始分析>，策略冗余分析开始，分析结果将会。


点击<删除>，可批量删除冗余策略，可提供安全策略管理效率。

## 6.2 带宽策略

通过带宽策略可以对网络或主机对带宽的占用进行管理。对不同流量分配带宽和连接数可以有效地避免网络拥塞和网络体验的下降。

### 6.2.1 带宽控制

**进入界面：策略>> 带宽策略 >> 带宽控制**


- 功能设置

勾选<启用带宽控制>，开启带宽控制功能，可设置带宽利用率阈值，当带宽利用率高于该值时，带宽控制生效。

点击<设置>，使配置内容生效。

- 带宽控制规则列表

点击<新增>，新增带宽控制规则。


| | |
|---|---|
| **规则名称** | 设置带宽控制规则的条目名称。 |
| **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** | 设置地址组的带宽控制模式：共享表示地址组内 IP 共用带宽；独立表示地址组内 IP 独占带宽。 |
| **生效时间** | 选择规则生效的时间，Any 表示立即生效。 |
| **备注** | 为规则创建描述信息，以便于记忆。 |
| **添加到指定位置** | 将规则设置到指定的位置，从而配置规则的优先级。 |
| **状态** | 选择此规则是否启用。 |
| **确定** | 保存新策略规则。 |

点击<删除>，可批量删除带宽控制规则。

## 6.2.2 连接数限制

如果局域网内有部分主机向广域网发起的 TCP 和 UDP 数目过多，将可能影响局域网其他计算机的通信质量。通过设置连接数限制功能，可以限制每台计算机通过防火墙建立的连接数。

**进入界面：策略>> 带宽策略 >> 连接数限制**

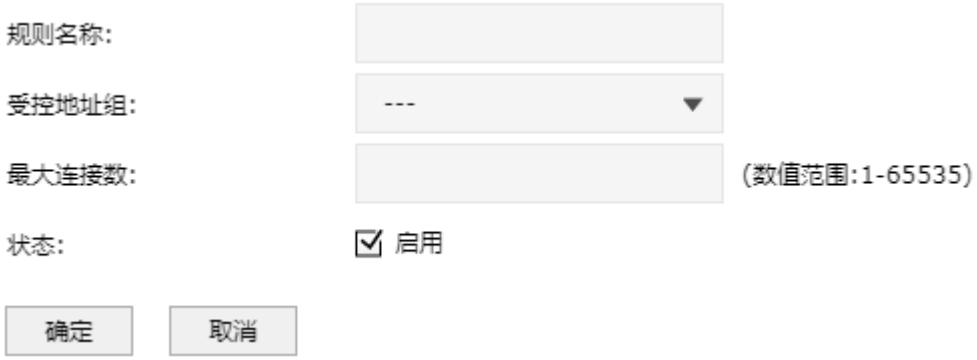

- 全局设置

勾选<启用连接数限制功能>，开启连接数限制功能。

点击<设置>，使配置内容生效。

- 连接数限制规则列表

点击< 新增 >，新增连接数限制规则，点击<确定>，使规则生效。




| | |
|---|---|
| **规则名称** | 设置带宽控制规则的条目名称。 |
| **受控地址组** | 设置受限的 IP 地址范围。 |
| **最大连接数** | 设置受限 IP 的最大连接数。 |

| | |
|---|---|
| 状态 | 选择此规则是否启用。 |

点击<删除>，可批量删除连接数限制规则。

### 6.2.3 连接数监控

可通过本页面查看已设置连接数限制规则的地址组内 IP 地址已建立的连接数。

**进入界面：策略>> 带宽策略 >> 连接数监控**


点击<刷新>，刷新当前列表内容。

## 6.3 NAT 策略

### 6.3.1 NAPT

当局域网中多台设备需要访问广域网时，而网络中只有少量接口连接到 Internet 时，NAPT 功能可以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。

**进入界面：策略>> NAT 策略 >> NAPT**


点击<新增>，新增 NAPT 规则，点击<确定>，使规则生效。


| | |
|---|---|
| **规则名称** | 输入该规则条目的名称。只能输入英文、数字和下划线。 |
| **出接口** | 选择该 NAPT 规则的生效接口，当数据包的源 IP 地址在源地址内，且从该接口转发时，路由器将对数据包进行 NAPT 地址转换。 |
| **源地址范围** | 设置 IP 地址范围，相应的 NAPT 规则条目只对源地址为设定范围内的数据包生效。 |
| **状态** | 勾选“启用”，则使该规则条目生效；<br>未勾选“启用”，则该规则条目无效。 |
| **备注** | 添加对本条目的说明信息，非必填项。 |

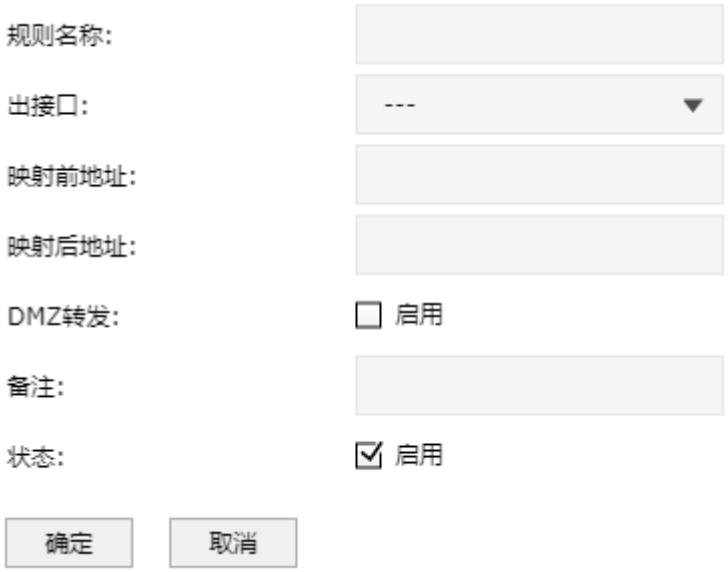
点击<删除>，可批量删除 NAPT 规则。

## 6.3.2 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。

**进入界面：策略>> NAT 策略 >> 一对一 NAT**


点击<新增>，新增一对一 NAT 规则，点击<确定>，使规则生效。




| | |
|---|---|
| **规则名称** | 输入该映射条目的名称，例如可以根据服务器提供的服务特性命名。只能输入英文、数字和下划线。 |
| **出接口** | 选择此一对一 NAT 映射规则的生效接口。当数据包从该接口转发时，设备根据映射后的地址对数据包进行地址转换；对映射后地址的访问请求将转发到局域网中的服务器上。 |
| **映射前地址** | 输入服务器的局域网 IP 地址。 |
| **映射后地址** | 填写映射后的 IP 地址。 |
| **DMZ 转发** | 设置是否开启该条 NAT 映射条目的 DMZ 转发。启用 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，将把数据包转发给局域网服务器。如果广域网用户需要自由的访问局域网服务器，需要启用 DMZ 转发，若不开启，路由器将拒绝用户对服务器的访问。 |
| **备注** | 添加对本条目的说明信息，非必填项。 |
| **状态** | 勾选“启用”，则使该规则条目生效；<br>不勾选“启用”，则使该规则条目失效。 |

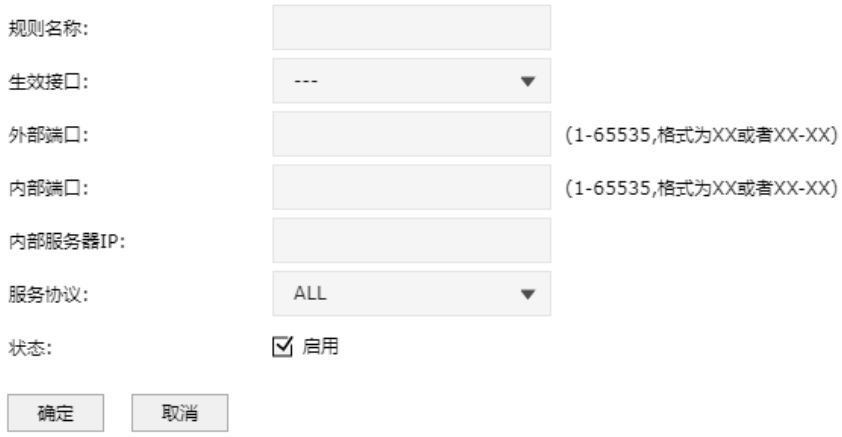
点击<删除>，可批量删除一对一 NAT 规则。

### 6.3.3 服务器映射

通过服务器映射功能，在设置了 NAPT 特性的接口上开放固定的传输层协议端口，当开放端口收到访问请求时，将把访问请求转发到指定的服务器上，此接口中的用户便能成功访问网络中的服务器，同时不影响网络安全。

**进入界面：策略>> NAT 策略 >> 服务器映射**


点击<新增>，新增服务器映射规则，点击<确定>，使规则生效。




| | |
|---|---|
| **规则名称** | 输入该虚拟服务器的名称，例如可以根据服务器提供的服务特性命名。只能输入英文、数字和下划线。 |
| **生效接口** | 选择规则生效接口，当此处设置的接口收到特定外部端口的访问请求时将把数据发给局域网服务器。 |
| **外部端口** | 输入路由器提供给广域网访问时使用的端口（范围），端口组之间不允许重叠。 |
| **内部端口** | 输入局域网服务器提供服务的端口。 |
| **内部服务器 IP** | 输入服务器的局域网 IP 地址。 |
| **服务协议** | 选择 TCP，UDP 协议，或者可以都选（根据内网服务器提供的服务类型而定）。 |
| **状态** | 勾选“启用”，则使该规则条目生效；<br>不勾选“启用”，则使该规则条目失效。 |

点击<删除>，可批量删除服务器映射规则。

### 6.3.4 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。

**进入界面：策略>> NAT 策略 >> NAT-DMZ**


点击<新增>，新增 NAT DMZ 规则，点击<确定>，使规则生效。


| | |
|---|---|
| **服务名称** | 输入该 NAT 转发规则的名称，例如可以根据 DMZ 主机特性命名。只能输入英文、数字和下划线。 |
| **出接口** | 选择规则生效接口，当此处设置的接口收到的访问请求无法匹配现有的 NAT 规则时，将把数据发给 DMZ 主机。 |
| **主机地址** | 输入 DMZ 主机的局域网 IP 地址。 |
| **状态** | 勾选“启用”，则使该规则条目生效；<br>不勾选“启用”，则使该规则条目失效。 |
| **确定** | 保存新策略规则。 |

点击<删除>，可批量删除 NAT DMZ 规则。

## 6.3.5 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，路由器开启了 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路由器上打开相应的端口，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。

**进入界面：策略>> NAT 策略 >> UPnP**


- 功能设置

| | |
|---|---|
| **服务接口** | 指定一组接口集，所设置的接口将会开放 UPnP 服务。 |
| **对外生效接口** | 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。 |
| **启用/禁用服务** | 选择启用或禁用 UPnP 服务。 |

点击<设置>，保存功能配置信息。

- 服务列表

点击<删除>，可删除 UPnP 规则。

点击<刷新>，刷新列表信息。

# 6.4 ALG 策略

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路由器 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。 |
| 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。 |
| 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。 |

**进入界面：策略 >> ALG 策略 >> ALG 服务**

在界面的 ALG 服务区域，针对特殊应用类型开启 ALG 服务。


防火墙支持 4 种特殊应用的 ALG 服务。默认情况下，3 种 ALG 服务均已经启用，建议保持默认设置不做改变。

# 6.5 安全防护

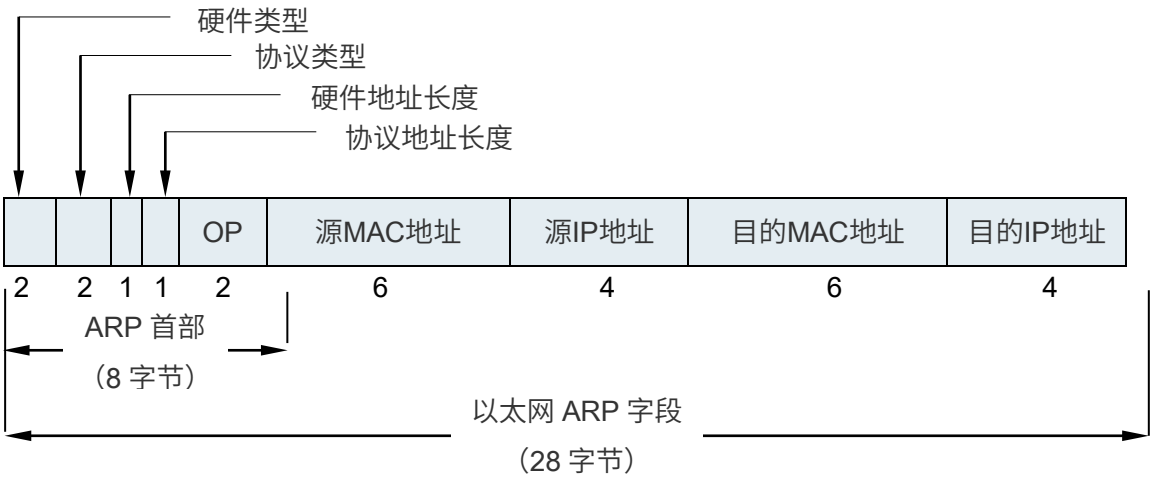
## 6.5.1 ARP 简介

ARP（Address Resolution Protocol，地址解析协议），是一种将主机的IPv4地址解析成MAC地址的网络协议。

在同一个局域网中，一台主机要与其他主机直接通信，必须确定目的主机的MAC地址。在已知目的主机IP地址的情况下，通过ARP协议可以获取目的主机的MAC地址信息。

## ■ ARP 报文格式

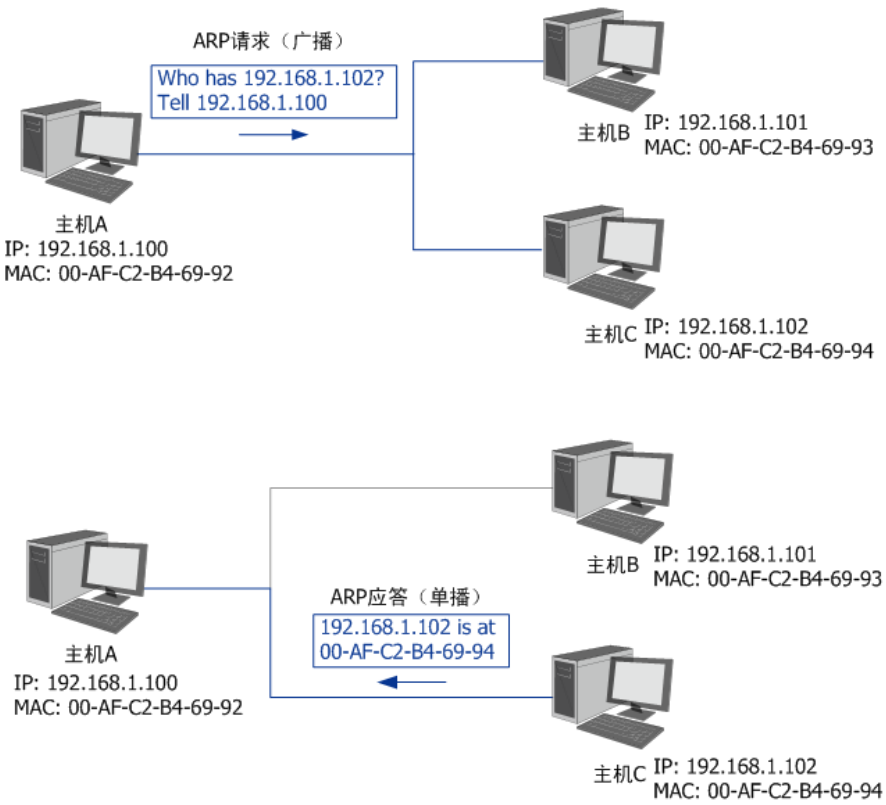
ARP报文的格式如下图所示：




| | |
|---|---|
| **硬件类型** | 应用 ARP 的网络类型，对于以太网该值为 1。 |
| **协议类型** | 要映射的协议类型，对于 IP 协议该值为 0x0800（0x 表示十六进制）。 |
| **硬件地址长度** | 硬件地址即 MAC 地址，共 48 位，长度为 6 个字节，该值为 6。 |
| **协议地址长度** | 协议地址即 IP 地址，共 32 位，长度为 4 个字节，该值为 4。 |
| **OP** | OP 为操作码，1 表示 ARP 请求；2 表示 ARP 应答。 |
| **源 MAC 地址** | 发送报文一方的 MAC 地址。 |
| **源 IP 地址** | 发送报文一方的 IP 地址。 |
| **目的 MAC 地址** | 接收报文一方的 MAC 地址（ARP 请求报文中该字段全 0）。 |
| **目的 IP 地址** | 接收报文一方的 IP 地址。 |

## ■ ARP 解析过程

在一次ARP通信中，源主机会首先向自己所在网段广播一个ARP请求报文，网段中的所有主机都会收到这个请求报文，但只有符合请求报文中目的IP地址的主机会做出回应，回应的ARP应答报文将会携带该主机的MAC地址信息，以单播形式发送给源主机。如下图所示：



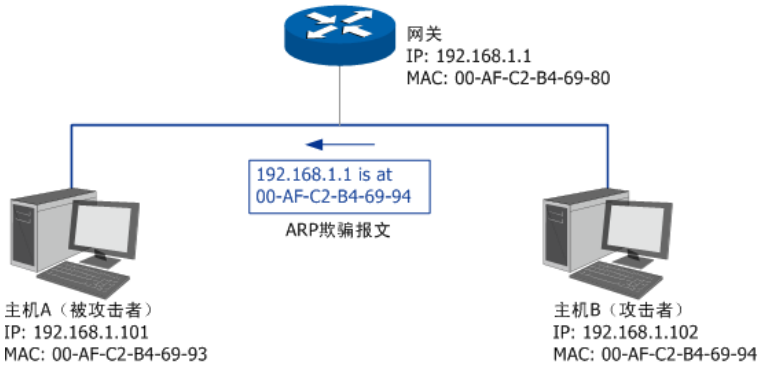

网络中的所有主机，包括防火墙和计算机在内，都各自维护一份ARP列表，该列表建立了主机IP地址和MAC地址一一对应关系。主机通过数据包的交互学习到其他主机的IP地址和MAC地址信息，并将这些信息添加至自身的ARP表中。每次通信时会先根据IP地址在表中查找对应MAC地址，减少网络上的ARP通信量。

## 6.5.2 ARP 攻击简介

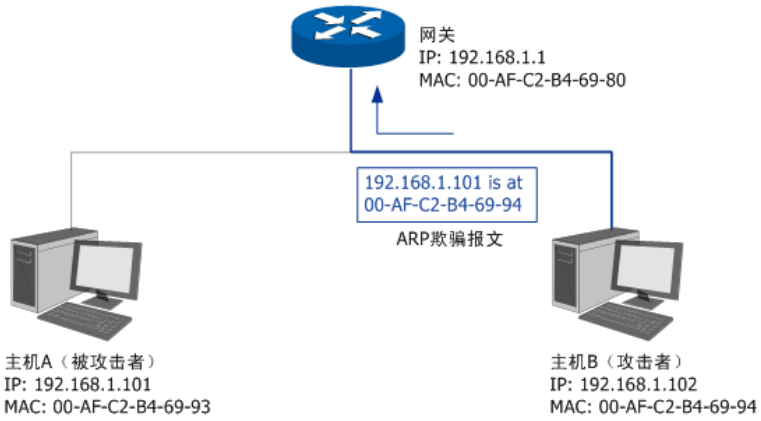
按照ARP协议的设计，主机在接收ARP应答报文时只会机械地使用最新ARP信息替换自身ARP列表，这就为“ARP攻击”创造了条件。

ARP攻击的主要形式为ARP欺骗，通常由局域网中的攻击主机发送ARP欺骗包，将伪造的IP与MAC对应关系替换主机ARP列表中的记录，共有三种欺骗方式：欺骗主机、欺骗网关、双向欺骗。

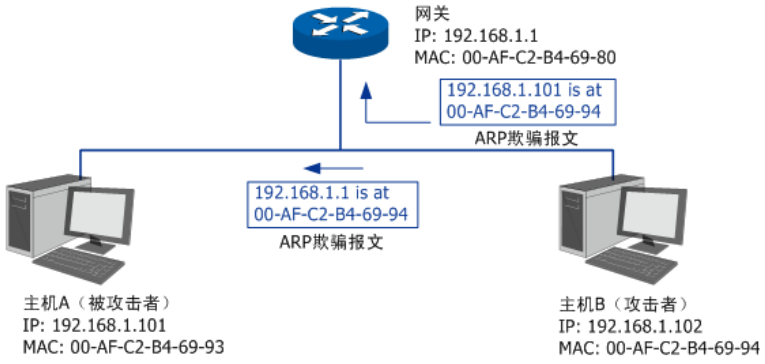
- 欺骗主机：仿冒网关给主机发送错误的ARP报文，通常欺骗报文中会伪造发送者MAC地址。




- 欺骗网关：仿冒主机向网关发送错误的ARP报文，通常欺骗报文中会伪造发送者IP或MAC地址。



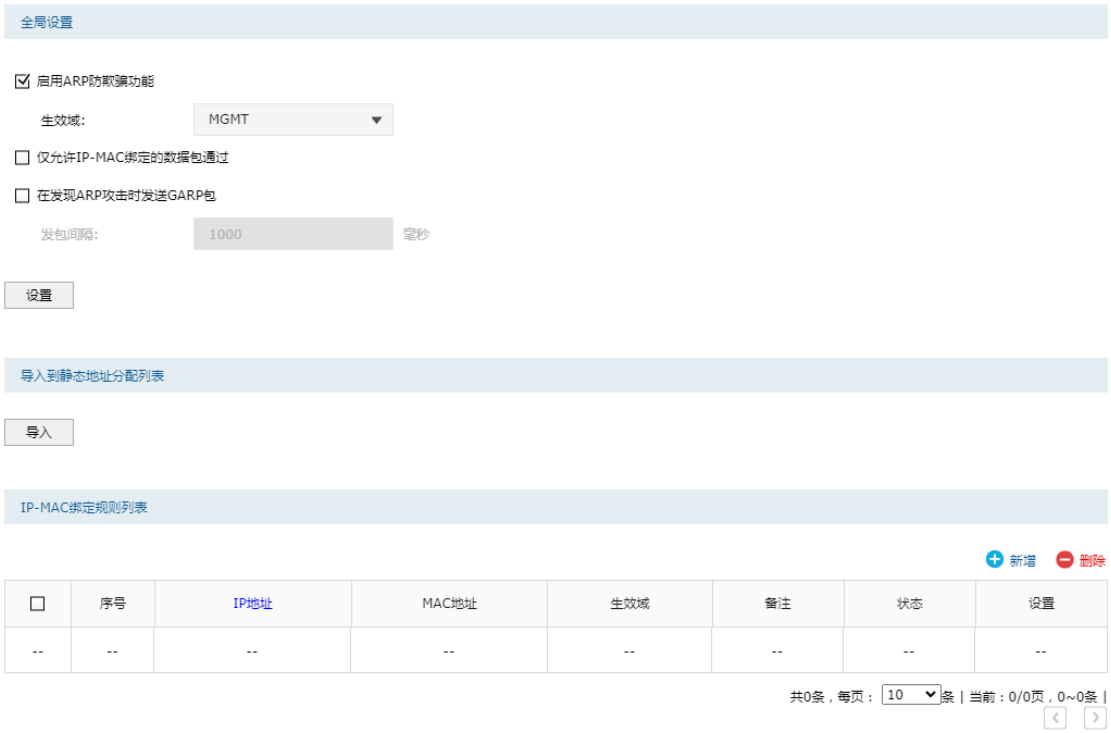

- 双向欺骗：前面两种欺骗方式的结合，伪造不同的ARP报文，同时发送给主机和网关。




ARP欺骗可能会造成局域网内部分主机无法访问网络，还可能造成通信数据被非法窃听或篡改，严重影响了局域网内部通信及安全，由此便产生了ARP防护技术。ARP防护的根源在于杜绝伪造的ARP报文刷新ARP列表。绑定正确的IP MAC地址信息可以有效防止ARP欺骗。

## 6.5.3 IP-MAC 绑定

**进入界面：策略>> 安全防护 >> IP-MAC 绑定**




- 全局设置

勾选<启用 ARP 防欺骗功能>，开启该功能后，选择生效接口域。

勾选<仅允许 IP-MAC 绑定的数据包通过>，强制局域网内主机进行 IP-MAC 绑定，没有绑定的主机将无法访问网络。推荐在需要防止非法客户端接入时勾选，勾选条目前请确认已绑定包含管理主机在内的指定主机的 IP-MAC 地址信息。

勾选<在发现 ARP 攻击时发送 GARP 包>，当路由器发现局域网内主机存在 ARP 冲突时，路由器会将自身正确的 IP-MAC 地址信息以 GARP（Gratuitous ARP，免费 ARP）包的方式主动发送给被攻击的主机，替换该主机错误的 ARP 列表信息。可在发包间隔处指定发包速率。推荐勾选。

点击<设置>，使配置生效。

- 导入到静态地址分配列表

在 IP-MAC 绑定规则列表中选择条目，并在**导入到静态地址分配列表**区域点击<导入>，可将条目导入到静态地址分配列表中。

- IP-MAC 绑定规则列表

点击< 新增 >，新增 IP-MAC 绑定规则，点击<确定>，使规则生效。

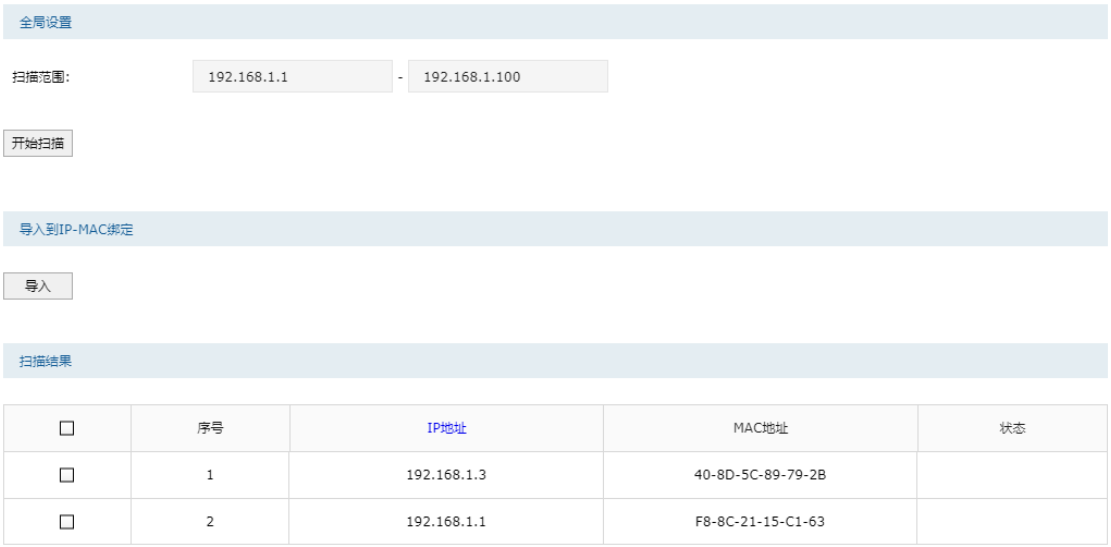

| | |
|---|---|
| **IP 地址** | 输入一个 IPv4 地址。 |
| **MAC 地址** | 输入与上方 IP 地址正确对应的主机 MAC 地址。 |
| **生效域** | 选择绑定的接口。 |
| **备注** | 添加对本条目的说明信息，非必填项。 |
| **状态** | 选择“启用”，则使该绑定条目生效；<br>选择“禁用”，则使该绑定条目失效。 |

点击< 删除 >，可批量删除 IP-MAC 绑定规则。

## 6.5.4 ARP 扫描

通过 ARP 扫描界面得到局域网内活动主机的 IP-MAC 对应信息，然后可以将扫描结果导入到 IP-MAC 绑定规则中。

**进入界面：策略>> 安全防护 >> ARP 扫描**




- 全局设置

在扫描范围中填入起始及结束的 IP 地址，点击<开始扫描>按钮，路由器会将该范围内所有正在工作主机的 IP-MAC 地址信息显示在扫描结果中。

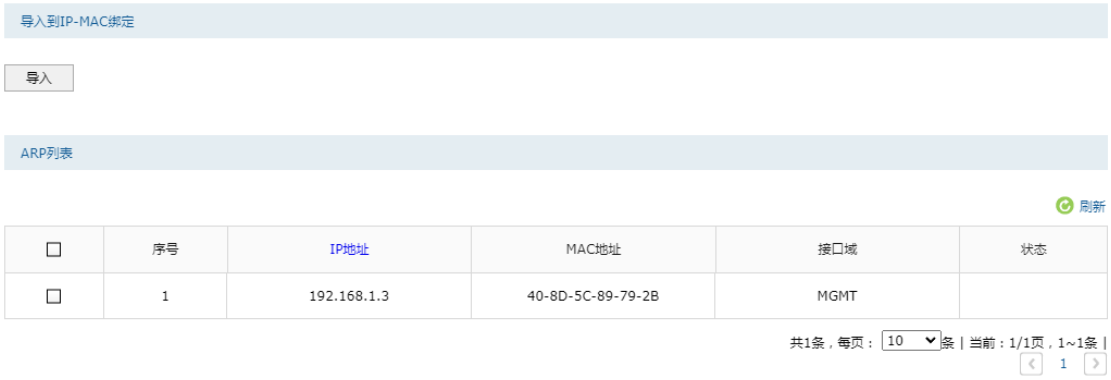
- 导入到 IP-MAC 绑定

如需将扫描结果进行绑定，请选择条目，然后点击<导入>按钮，在与已绑定条目不冲突的情况下，导入后绑定立即生效，这些批量绑定的条目会出现在 IP- MAC 绑定界面的 IP-MAC 绑定规则列表中。

## 6.5.5 ARP 列表

**进入界面：策略>> 安全防护 >> ARP 列表**

ARP 列表界面可以得到正在与防火墙进行通信的主机的 IP-MAC 对应信息。




- 导入到 IP-MAC 绑定

列表中未绑定的条目并不是一直存在，除了会被新的 IP-MAC 对应信息更替之外，还会由于长时间未通信或物理连接中断而自动从列表中删除。

如需将列表中的条目绑定，请选择条目，然后点击<导入>按钮，在与已绑定条目不冲突的情况下，导入后绑定立即生效，ARP 列表中的条目状态也会随之变更。

若防火墙此时已连入外网，也可以通过 ARP 列表获取网关的 IP-MAC 地址信息，并进行绑定，以抵御来自外网的 ARP 攻击。

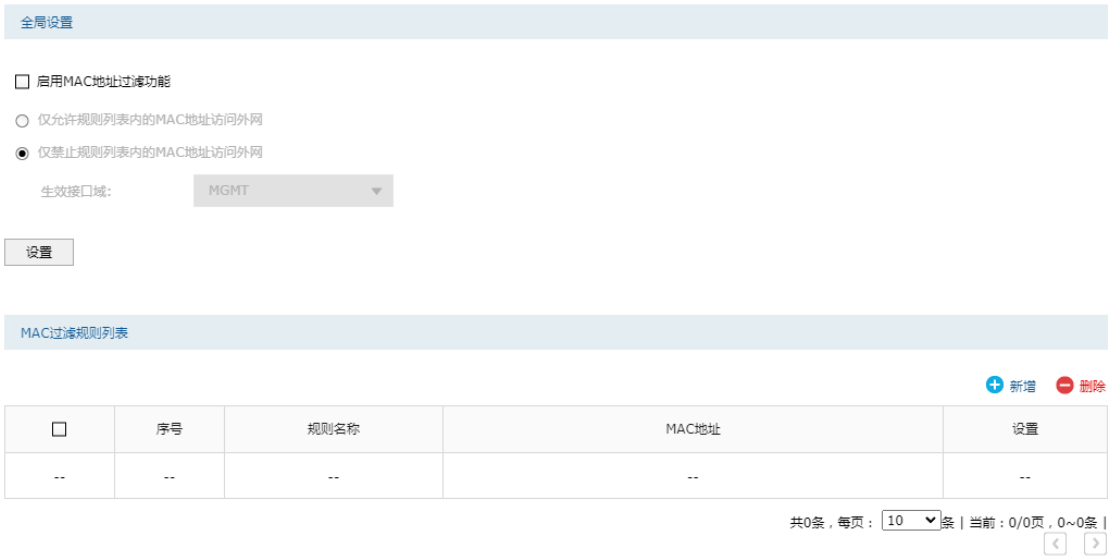
- ARP 列表

点击< 刷新>，获取最新 ARP 列表信息。

## 6.5.6 MAC 过滤

在此可以通过指定 MAC 地址对部分局域网主机进行过滤。

**进入界面：策略>> 安全防护 >> MAC 过滤**




- 全局设置

勾选<启用 MAC 地址过滤功能>，开启 MAC 地址过滤功能。

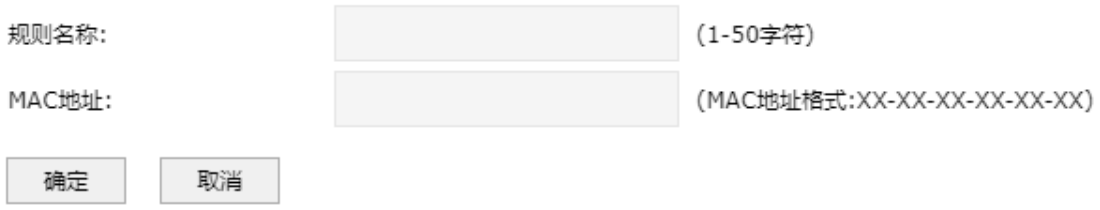
选择<仅允许规则列表内的 MAC 地址访问外网>，选择生效接口域。

选择<仅禁止规则列表内的 MAC 地址访问外网>，选择生效接口域。

点击<设置>，使配置生效。

- MAC 地址过滤规则列表

点击<新增>，新增 MAC 地址过滤规则，点击<确定>，使规则生效。



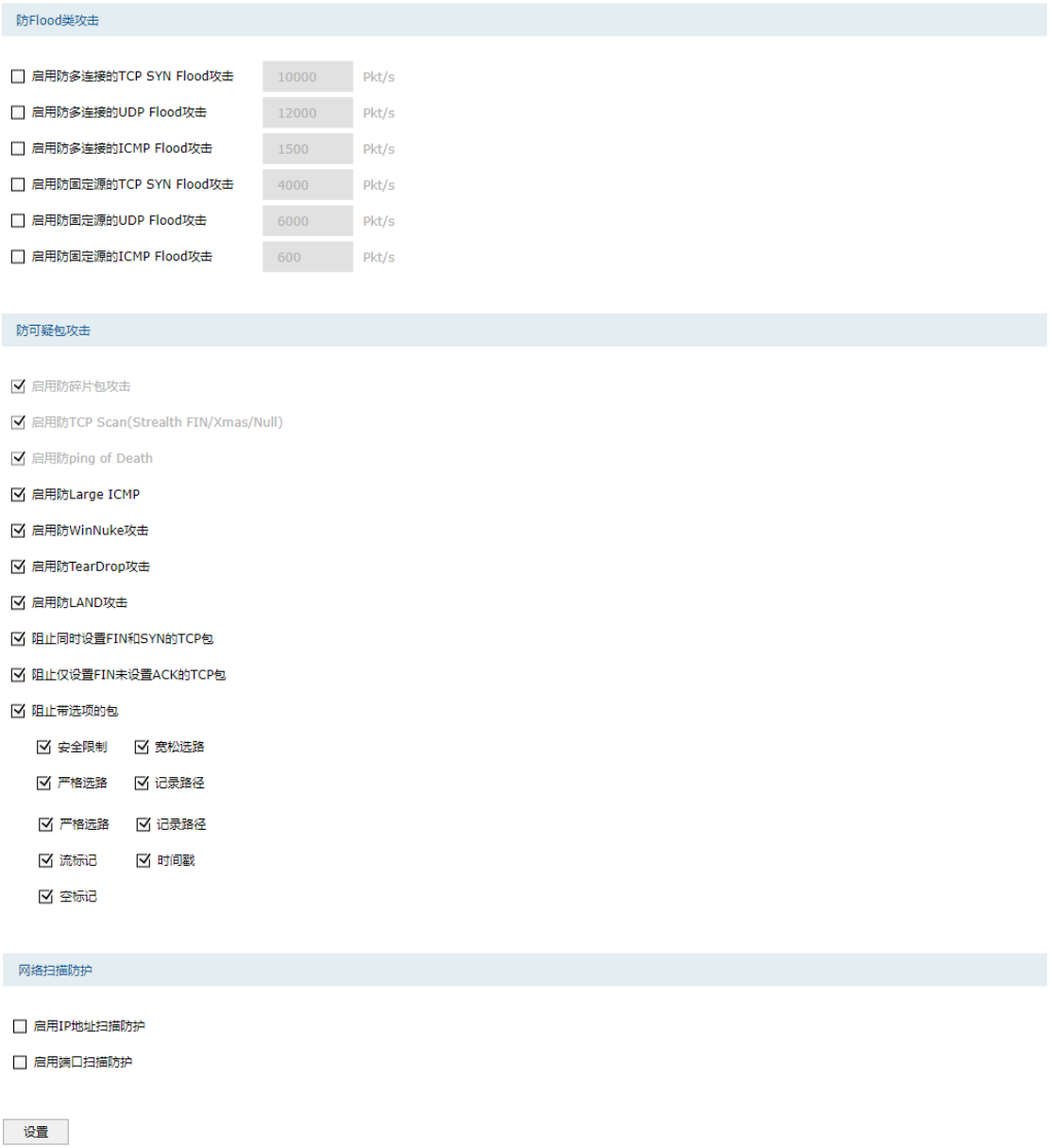

| | |
|---|---|
| **规则名称** | 输入该规则条目的名称。 |
| **MAC 地址** | 输入需要控制的局域网主机 MAC 地址。 |

点击<删除>，可删除 MAC 地址过滤规则。

## 6.5.7 攻击防护

攻击防护可防止广域网对局域网内设备进行端口扫描和恶意攻击，以此来保证它们的安全运行。

**进入界面：策略>> 安全防护 >> 攻击防护**




- 防 Flood 类攻击

Flood 类攻击是 DoS 攻击的一种常见形式。DoS（Denial of Service，拒绝服务）是一种利用发送大量的请求服务占用过多的资源，让目的路由器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。

- 防可疑包攻击

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。

- 网络扫描防护

开启 IP 地址扫描防护和端口扫描防护，需设置最大扫描速率和黑名单老化时间。当发现某台主机的地址或端口扫描行为的速率超过了最大扫描速率，系统将其判断为攻击者，并将其加入黑名单。加入黑名单的表项在超过黑名单老化时间后自动从黑名单中删除。

## 6.5.8 黑名单

来自或前往黑名单 IP 的流量将不进行任何处理，直接丢弃。

**进入界面：策略>> 安全防护 >> 黑名单**


点击<刷新>，刷新黑名单列表。

勾选<自动刷新>，自动更新黑名单列表。

点击<删除>，可批量删除黑名单列表。

点击<新增>，可新增黑名单列表，点击<确定>，使规则生效。


| | |
|---|---|
| **IP 地址** | 显示或设置本条黑名单项目的 IP 地址。 |
| **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。 |
| **状态** | 显示或设置本条黑名单项目是否生效。 |

## 6.5.9 白名单

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。

**进入界面：策略>> 安全防护 >> 白名单**


点击< 新增 >，可新增黑名单列表，点击<确定>，使规则生效。


| | |
|---|---|
| **IP 地址** | 显示或设置本条黑名单项目的 IP 地址。 |
| **类型** | 显示或设置本条黑名单项目匹配的方向。 |
| **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。 |
| **状态** | 显示或设置本条黑名单项目是否生效。 |

点击< 删除 >，可批量删除黑名单列表。

# 第7章 对象管理

## 7.1 地址管理

### 7.1.1 地址组

可以在本页面设置自定义地址组，以方便对用户进行组管理。

**进入界面：对象 >> 地址 >> 地址组**


- 新增

点击<新增>按钮，进入地址组设置页面。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。


| | |
|---|---|
| **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。 |
| **地址名称** | 勾选该组可以包含的地址或子组，此地址就包含在所选的组中。 |

| | |
|---|---|
| **备注** | 添加对当前组的说明信息。 |

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。条目1为系统默认条目，不可操作。

- 点击<删除>，可删除地址组条目。
- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择组名称或备注作为搜索关键列。 |
| **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；<br>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。 |

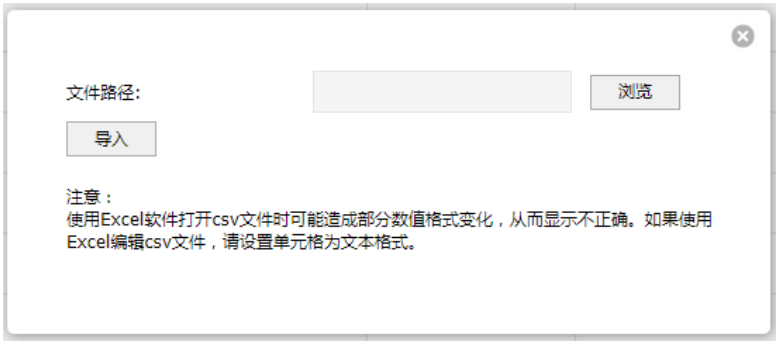
- 日志搜索

点击<日志搜索>，可搜索不同列名和自定义内容的地址组信息。


| | |
|---|---|
| **列名** | 选择组名称、地址名称、备注中的一个为搜索基础列。 |
| **内容** | 设置结束时间。 |
| **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。 |

- 导入

点击<导入>，可批量导入地址组信息。




- 备份

点击<备份>，可将地址组信息保存到本地。

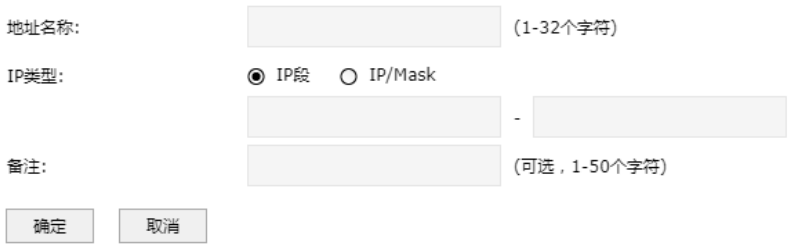
## 7.1.2 地址

可以在本页面自定义地址，并加入到已有的组中进行组管理。

**进入界面：对象>> 地址>> 地址**


- 新增

点击<新增>按钮，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** | 输入一个名称来标识地址。只能输入英文、数字和下划线。 |
| **IP 类型** | 在此建立源地址范围。主要有以下 2 种表示方式。<br>IP 段：由起始 IP 地址到结束 IP 地址确定 IP 地址范围。<br>IP/MASK：由 IP 地址和子网掩码确定 IP 地址范围。 |
| **备注** | 添加对当前地址的说明信息。 |

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。

- 点击<删除>，可批量删除地址条目。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择地址名称、IP 段、备注作为搜索关键列。 |
| **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；<br>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。 |

- 全局搜索

点击<全局搜索>，可搜索一个时间范围内，不同列名和自定义内容的系统日志信息。


| | |
|---|---|
| **列名** | 选择地址名称、IP 段、备注中的一个为搜索基础列。 |
| **内容** | 设置结束时间。 |
| **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。 |

## 7.2 时间段

可以通过本页面创建时间对象，从而对时间进行管理。

**进入界面：对象>> 时间段 >> 时间段**


点击<新增>按钮，进入时间对象设置页面。填入该时间对象的名称，时间设置可选择工作日历或手动设置。


| | |
|---|---|
| **时间对象名称** | 自定义的时间对象名称。只能输入英文、数字和下划线。 |
| **时间设置** | 选择“工作日历”。 |
| **工作日历** | 在此设置一个日历对象，点击图标后可设置具体的工作时间。 |
| **备注** | 输入对时间对象的具体描述。 |

“工作日历”设置界面如下图所示。


手动设置页面如下：


| | |
|---|---|
| **时间对象名称** | 自定义的时间对象名称。只能输入英文、数字和下划线。 |
| **时间设置** | 选择手动设置。 |
| **星期** | 选择工作日期。 |
| **时间段** | 选择工作时间段。 |
| **备注** | 输入对时间对象的具体描述。 |

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。

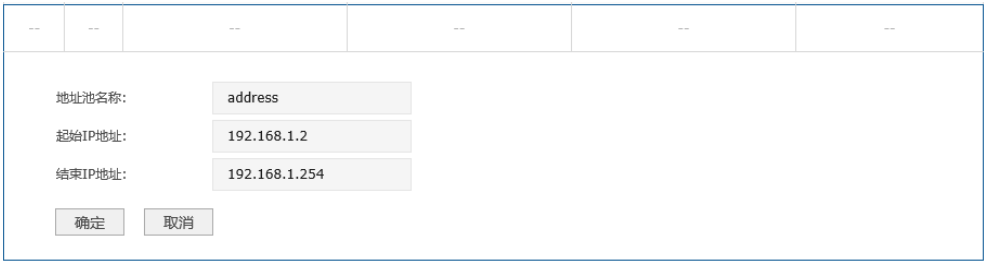
点击<删除>，可批量删除时间对象列表条目。

## 7.3 IP 地址池

可以通过本页面设置IP地址池条目，进行地址池的管理。

**进入界面：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。




| | |
|---|---|
| **地址池名称** | 自定义地址池的名称。只能输入英文数字和下划线。 |
| **起始/结束 IP 地址** | 输入地址池起始 IP 和地址池结束 IP，且起始 IP 必须不大于结束 IP，而且不能与已有的地址池范围重叠。当前一个地址池最多可以包含 1024 个 IP 地址。 |

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。

# 7.4 用户

## 7.4.1 用户组

可以在本页面设置自定义用户组，以方便对用户进行组管理。

**进入界面：对象 >> 用户 >> 用户组**


- 新增

点击<新增>按钮，进入地址组设置页面。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。


| | |
|---|---|
| **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。 |
| **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。


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>，可批量删除用户组列表条目。

- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 默认组名称作为搜索关键列。 |
| **内容** | 输入与组名称相关的搜索关键内容。 |
| **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；<br>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。 |

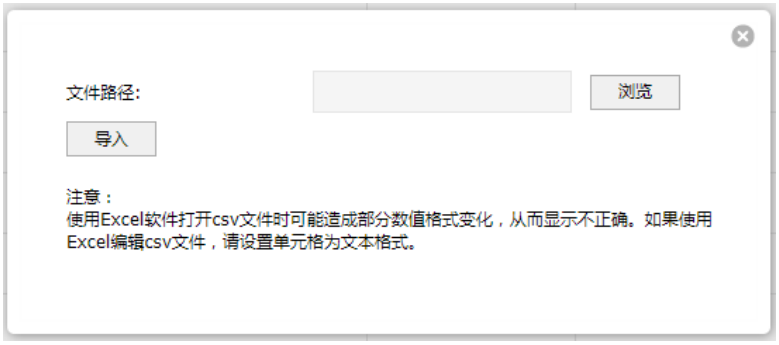
- 全局搜索

点击<全局搜索>，可搜索不同列名和自定义内容的地址组信息。


| | |
|---|---|
| **列名** | 选择成员列表、组名称为搜索基础列。 |
| **内容** | 设置需搜索的关键内容，该内容需与列名相关。 |
| **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。 |

- 导入

点击<导入>，可批量导入用户组信息。




- 备份

勾选<备份>，可将用户组信息保存到本地。

## 7.4.2 用户

可以在本页面自定义用户，并加入到已有的组中进行组管理。

**进入界面：对象>> 用户>> 用户**


- 新增

点击<新增>按钮，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。<br>正式用户：存留在系统中的正式用户，具有一定的有效期，且可以绑定相应的设备 MAC 地址。可以记录更多用户的资料信息。<br>免费用户：免费用户具有一定的上网时长限制。 |
| **用户名** | 用于认证登录的用户名。 |
| **密码** | 用户登录所使用的密码。 |
| **有效期至** | 正式用户的有效期。 |
| **允许认证时间段** | 允许用户进行认证的时间。 |
| **MAC 地址绑定方式** | 选择是否绑定 MAC 地址，以及绑定的方式。<br>不绑定：不绑定用户的 MAC 地址。<br>静态绑定：手动输入认证客户端 MAC 地址，绑定对应用户名。<br>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。<br>最多允许同时使用该账号登录的用户数量。 |
| **姓名** | 可选记录当前用户姓名。 |
| **电话** | 可选记录当前用户电话。 |
| **备注** | 可选记录当前用户备注。 |
| **状态** | 是否启用当前用户规则。 |

新增的条目会在**地址列表**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。条目1为系统默认条目，表示任何地址，不可操作。

- 点击<删除>，可批量删除用户列表条目。

## 7.4.3 用户状态

可统一查看管理已认证的用户。

**进入界面：对象>> 用户>> 用户状态**


点击<刷新>，可查看最新的用户状态列表。

勾选用户条目，点击<下线>，可断开用户连接。

| | |
|---|---|
| **刷新** | 手动刷新认证用户列表 |
| **下线** | 可实现批量断开用户连接。 |
| **认证方式** | 显示用户登录所使用的认证方式。 |
| **接入时间** | 显示用户接入网络时的时间。 |
| **IP 地址** | 显示用户的 IP 地址。 |
| **设置** | 可断开用户连接。 |

## 7.4.4 跳转页面

**进入界面：对象>> 用户>> 跳转页面**

点击新增，新增跳转页面模板。设置完成后，请点击<确定>，保存配置。


| | |
|---|---|
| **跳转页面名称** | 设置跳转页面名称。 |
| **模板类型** | 选择本地模板或云模板。<br>选择云模板，设备将向云端服务器获取页面样式，需联网才能使用。 |
| **备注** | 设置跳转页面的备注信息，方便管理和查找。 |

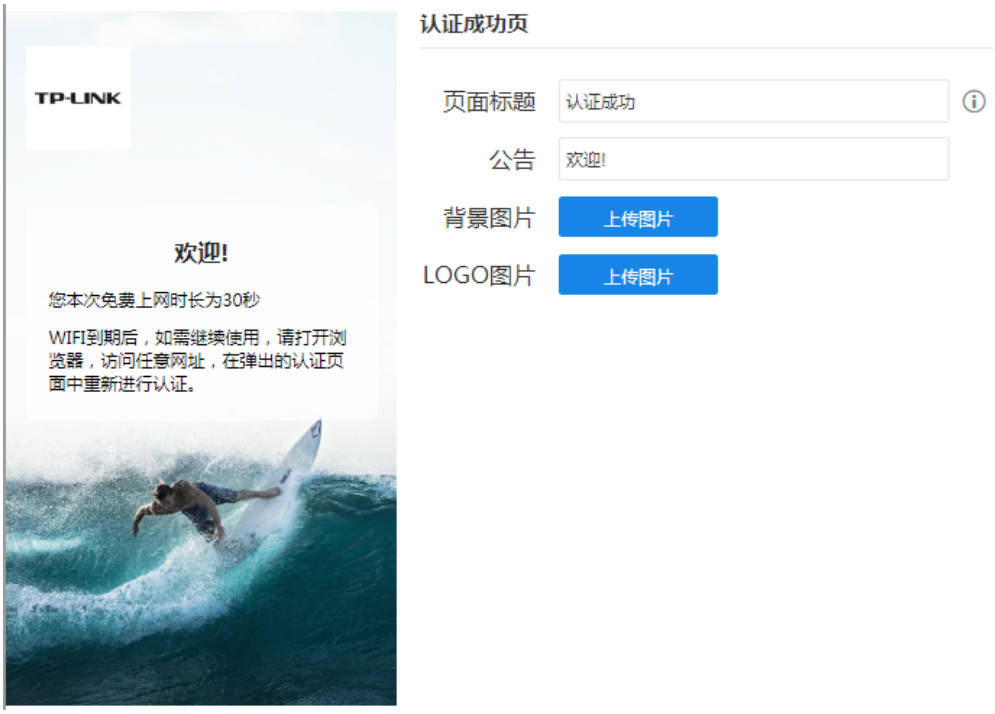
选中模板后，需要设置认证页和认证成功页的图片文案信息。

- 设置认证页


| | |
|---|---|
| **选择接入方式** | 选择一键上网、账号登录还是手机登录。 |

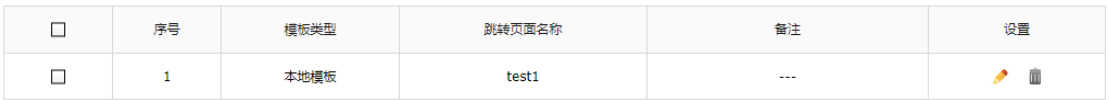
| | |
|---|---|
| **页面标题** | 跳转页面的页面标题。 |
| **欢迎语** | 显示跳转页面的欢迎信息。 |
| **版权信息** | 显示跳转页面的版权声明信息。 |
| **背景图片** | 用于页面的背景展示图，图片大小限制在 200KB 以内。 |
| **Logo 图片** | 设置页面的 Logo 图片，图片大小限制在 100KB 以内。 |

- 设置认证成功页




| | |
|---|---|
| **页面标题** | 跳转页面的页面标题。 |
| **公告** | 设置页面的提示信息。 |
| **背景图片** | 用于页面的背景展示图，图片大小限制在 200KB 以内。 |
| **Logo 图片** | 设置页面的 Logo 图片，图片大小限制在 100KB 以内。 |

设置完成后，可查看到当前已有的跳转页面。




点击< 删除 >，可批量删除跳转页面列表信息。

点击< 搜索 >，可根据关键内容进行搜索。


| | |
|---|---|
| **列名** | 选择模板类型、跳转页面名称、备注作为搜索关键列。 |
| **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；<br>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。 |

## 7.4.5 组合认证

**进入界面：对象>> 用户>> 组合认证**


点击<启用>，可批量启用认证规则。

点击<禁用>，可批量禁用认证规则。

点击<新增>，新增认证条目。设置完成后，请点击<确定>，保存配置。


| | |
|---|---|
| **跳转页面名称** | 选择该条目认证方式下的跳转页面模板。<br>跳转页面设置请参考错误!未找到引用源。错误!未找到引用源。 |
| **生效接口** | 选择该条目生效对应的接口。 |
| **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。 |
| **备注** | 设置组合认证条目的备注信息，以方便管理和查找。 |
| **认证方式** | 仅支持 web 认证方式。 |
| **状态** | 默认启用 web 认证状态。 |
| **认证服务器类型** | 仅支持本地服务器认证。 |

**说明：**

- 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。

点击< 删除 >，可批量删除跳转页面列表信息。

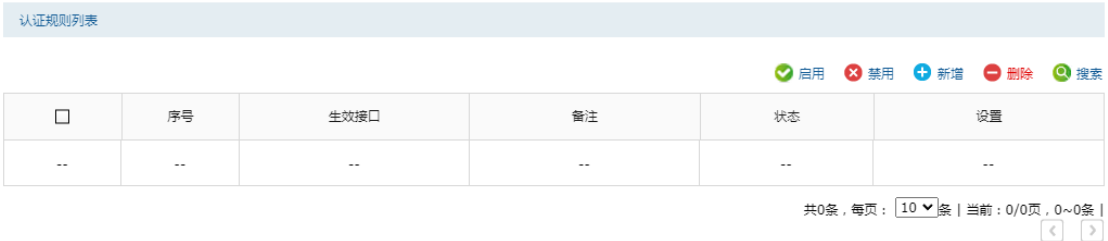
点击< 搜索 >，可根据关键内容进行搜索。


| | |
|---|---|
| **列名** | 选择跳转页面名称、生效接口、备注作为搜索关键列。 |
| **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;<br>在所有条目中搜索：在所有列表条目中搜索。 |
| **状态** | 选择认证规则是已启用或禁用。 |
| **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。 |

## 7.4.6 远程 Portal

您可以通过本页面设置和查看远程 Portal 认证条目。

**进入界面：对象>> 用户>> 远程Portal**




点击 启用，可批量启用远程 Portal 认证规则。

点击 禁用，可批量禁用远程 Portal 认证规则。

点击 新增，新增远程 Portal 条目。设置完成后，请点击<确定>，保存配置。


| | |
|---|---|
| **生效接口** | 选择该条目生效对应的接口。 |
| **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** | 选择认证服务器为本地服务器或者远程服务器。 |
| **备注** | 设置组合认证条目的备注信息，以方便管理和查找。 |

**说明：**

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

点击 删除，可批量删除认证规则。

点击 搜索，可根据筛选条件搜索规则。


| | |
|---|---|
| **列名** | 选择生效接口、备注作为搜索关键列。 |
| **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;<br>在所有条目中搜索：在所有列表条目中搜索。 |
| **状态** | 选择认证规则是已启用或禁用。 |
| **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。 |

### 7.4.7 免认证策略

可以通过本界面设置和查看免认证策略。免认证策略可配置用户在认证成功前能够免费访问的资源。

**进入界面：对象>> 用户>> 免认证策略**


点击 启用，可批量启用免认证策略规则。

点击 禁用，可批量禁用免认证策略规则。

点击 新增，新增免认证策略条目。路由器支持两种**免认证方式**：五元组方式和 URL 方式。设置完成后，请点击确定，保存配置。

- 五元组方式

五元组方式：主要依据 IP 地址范围、MAC 地址、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** | 设置免认证策略的名称。只能输入英文、数字和下划线。 |
| **免认证方式** | 选择五元组方式。 |
| **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。 |
| **源端口范围** | 设置免认证策略的源端口范围。 |
| **目的 IP 地址范围** | 设置免认证策略的目的 IP 地址和网络掩码。 |
| **目的端口范围** | 设置免认证策略的目的端口范围。 |
| **服务协议** | 设置免认证策略的服务协议。 |
| **生效接口域** | 选择生效接口，可以针对指定接口设置免认证策略。 |
| **备注** | 设置条目的备注，以方便管理和查找。 |
| **状态** | 勾选“启用”，则使该策略生效；<br>不勾选“启用”，则该策略无效。 |

- URL 方式

URL 方式：主要依据 URL 设置策略，当已知 URL 时，推荐使用 URL 方式。


| | |
|---|---|
| **策略名称** | 设置免认证策略的名称。只能输入英文、数字和下划线。 |
| **免认证方式** | 选择 URL 方式。 |
| **URL 地址** | 设置免认证策略的 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** | 选择生效接口，可以针对指定接口设置免认证策略。 |
| **备注** | 设置条目的备注，以方便管理和查找。 |
| **状态** | 勾选“启用”，则使该策略生效；<br>不勾选“启用”，则该策略无效。 |

新增的条目会在免认证策略列表里显示出来，如下图所示。

| ☐ | 序号 | 策略名称 | 免认证方式 | 源IP地址范围 | 目的IP地址范围 | 源端口 | 目的端口 | 服务协议 | 状态 | 设置 |
|---|---|---|---|---|---|---|---|---|---|---|
| -- | 1 | dhcp client | 五元组方式 | --- | --- | 68-68 | 67-67 | UDP | 已启用 | --- |
| -- | 2 | dhcp server | 五元组方式 | --- | --- | 67-67 | 68-68 | UDP | 已启用 | --- |
| -- | 3 | dns client | 五元组方式 | --- | --- | --- | 53-53 | UDP | 已启用 | --- |
| -- | 4 | dns server | 五元组方式 | --- | --- | 53-53 | --- | UDP | 已启用 | --- |
| ☐ | 5 | test1 | URL方式 | --- | --- | --- | --- | --- | 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，可批量删除免认证策略规则。

## 7.4.8 认证参数

本页可以进行认证的全局参数的设置。

**进入界面：对象>> 用户>> 认证参数**


| | |
|---|---|
| **认证老化** | 勾选开启认证老化功能。 |
| **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。不能与其他的服务端口重复。 |
| **认证模式** | 设置 Portal 认证的认证模式，现支持基于 SSID 和基于接口两种模式。 |

# 7.5 服务

## 7.5.1 服务组

可以在本页面设置自定义服务组，以方便对用户进行组管理。

**进入界面：对象 >> 服务 >> 服务组**


点击<新增>按钮，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。


| | |
|---|---|
| **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。 |
| **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** | 您可以设置服务组的备注，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。


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。

## 7.5.2 服务

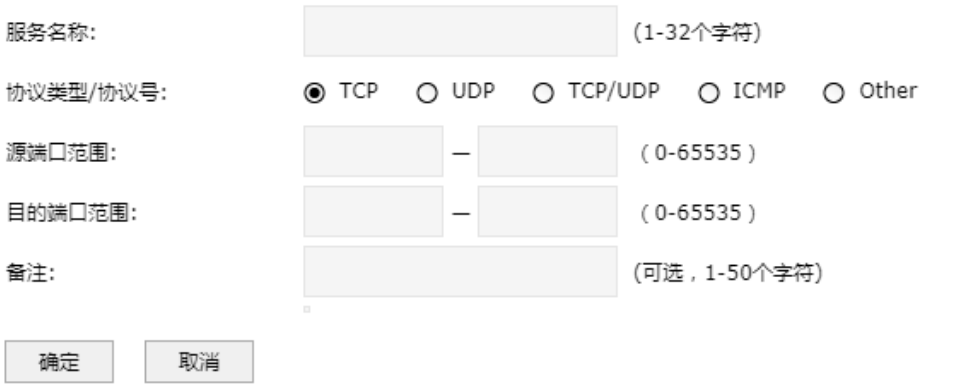
可以在本页面自定义服务类型，并加入到已有的组中进行组管理。

**进入界面：对象>> 服务>> 服务**


| □ | 序号 | 服务名称 | 协议类型/协议号 | 详细信息 | 备注 | 设置 |
|---|---|---|---|---|---|---|
| -- | 1 | ALL | 0-255 | --- | ALL | --- |
| -- | 2 | FTP | TCP | 源端口 = 0-65535; 目的端口 = 21-21 | FTP | --- |
| -- | 3 | SSH | TCP | 源端口 = 0-65535; 目的端口 = 22-22 | SSH | --- |
| -- | 4 | TELNET | TCP | 源端口 = 0-65535; 目的端口 = 23-23 | TELNET | --- |
| -- | 5 | SMTP | TCP | 源端口 = 0-65535; 目的端口 = 25-25 | SMTP | --- |
| -- | 6 | DNS | UDP | 源端口 = 0-65535; 目的端口 = 53-53 | DNS | --- |
| -- | 7 | HTTP | TCP | 源端口 = 0-65535; 目的端口 = 80-80 | HTTP | --- |
| -- | 8 | HTTPS | TCP | 源端口 = 0-65535; 目的端口 = 443-443 | HTTPS | --- |
| -- | 9 | POP3 | TCP | 源端口 = 0-65535; 目的端口 = 110-110 | POP3 | --- |
| -- | 10 | SNTP | UDP | 源端口 = 0-65535; 目的端口 = 123-123 | SNTP | --- |



点击<新增>按钮，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** | 您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。您可以选择 TCP，UDP，TCP/UDP 或 ICMP，也可以选择 other 并输入协议号(0-255)。 |
| **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。 |
| **备注** | 您可以对服务类型进行描述。 |

点击<删除>，可删除服务条目。

# 7.6 网站

## 7.6.1 网站组

可以在本页面设置自定义网站分组，以方便对网站进行组管理。

**进入界面：对象 >> 网站 >> 网站组**


点击<新增>按钮，进入网站组设置页面。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。


| | |
|---|---|
| **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，您可以同时输入多个网站进行批量添加。<br>组成员可以为域名，如 www.tp-link.com.cn,也可以在域名前面加通配符'*'，如*.tp-link.com.cn。但是'*'只允许输入在最前面，而不能夹杂在域名中间或后面。 |
| **清空** | 您可以清空组成员中输入的内容。 |
| **文件路径** | 您可以通过文件导入的形式为网站分组添加成员，文件格式为 txt 格式。 |
| **备注** | 您可以为分组添加 50 字符以内的备注。 |

新增的条目会在**组列表**里显示出来，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>，可批量删除网站组条目。

# 7.7 应用

## 7.7.1 应用组

可以在本页面设置自定义应用组，以方便对不同应用进行组管理。

**进入界面：对象 >> 应用 >> 应用组**


- 识别模式

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。

勾选<启用智能识别模式>，点击<设置>，开启智能识别。

- 应用组列表

点击<新增>按钮，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。


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>，可批量删除应用组条目。

点击<搜索>，可批量查找不同的应用组。


| | |
|---|---|
| **列名** | 默认名称作为搜索关键列。 |
| **内容** | 输入与名称相关的搜索关键内容。 |
| **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;<br>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。 |

## 7.7.2 应用

**进入界面：对象>> 应用>> 应用**


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。

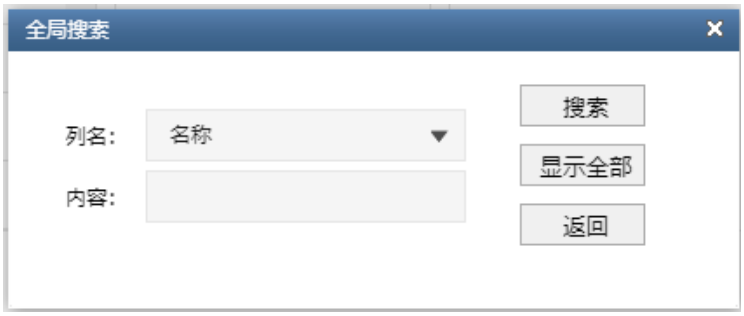

| | |
|---|---|
| **名称** | 自定义应用名称。 |
| **类别** | 选择应用类别，分为商务应用、社交娱乐、互联网访问、网络基础应用。 |
| **子类别** | 选择应用的子类别，分为网络基础协议、网络电话会议、网络代理、VPN 隧道和其它。 |
| **数据传输方式** | 选择应用的数据传输方式：客户端/服务器、浏览器、网络、端到端或其它未指定的方式。 |
| **标签** | 为应用添加风险等级、技术维度、功能维度、风险维度和其它等特性标签。 |
| **备注** | 您可以对应用进行描述，便于后续查找和管理。 |

点击<删除>，可删除应用条目。

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 默认名称作为搜索关键列。 |
| **内容** | 输入与应用名称相关的关键内容。 |
| **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；<br>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。 |

点击<全局搜索>，可搜索不同列名和自定义内容的地址组信息。




| | |
|---|---|
| **列名** | 选择组名称、地址名称、备注中的一个为搜索基础列。 |
| **内容** | 设置结束时间。 |
| **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。 |

# 7.8 安全配置文件

## 7.8.1 URL 过滤

在此可以配置对 URL 进行过滤的规则。

**进入界面：对象 >> 安全配置文件 >> URL过滤**


点击<新增>，配置 URL 过滤规则。点击<确定>保存配置。


| | |
|---|---|
| **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。 |
| **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。 |

点击<删除>，可批量删除 URL 过滤规则条目。

## 7.8.2 文件过滤

在此可以配置对文件进行过滤的规则。

**进入界面：对象 >> 安全配置文件 >> 文件过滤**


点击<新增>，配置文件过滤规则。点击<确定>保存配置。


| | |
|---|---|
| **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。 |
| **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。 |

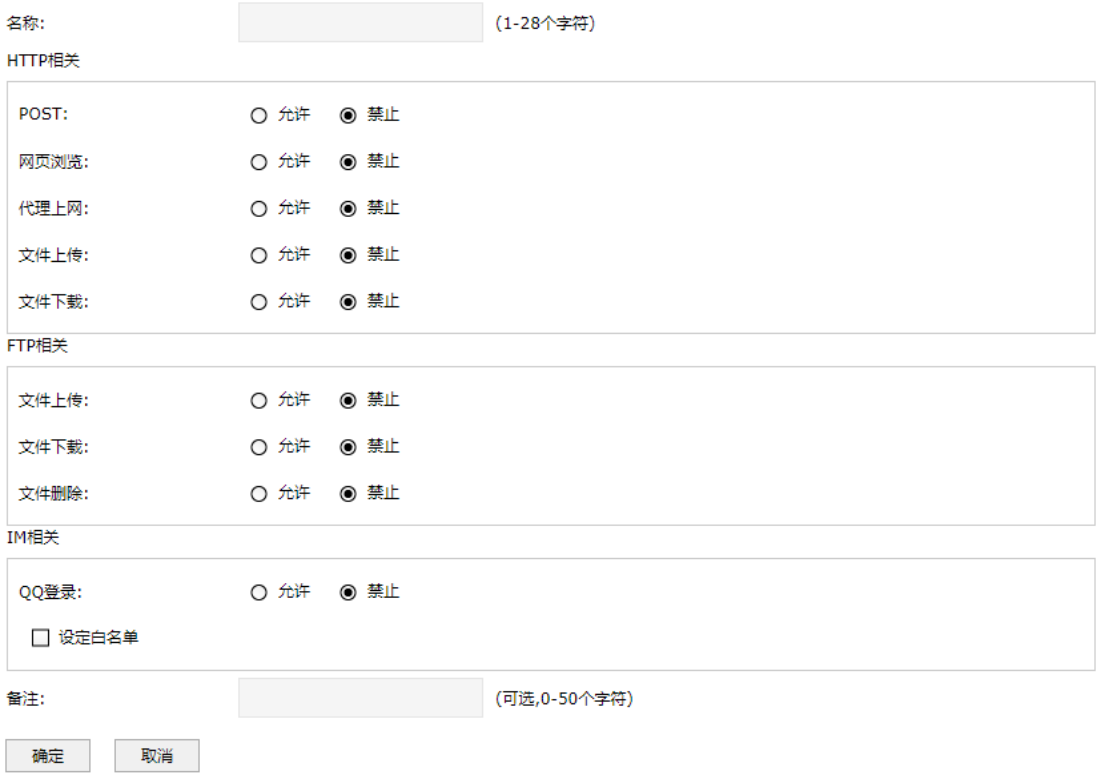
点击<删除>，可批量删除文件过滤规则条目。

## 7.8.3 应用行为控制

在此可以配置对对应用行为控制的规则。

**进入界面：对象 >> 安全配置文件 >> 应用行为控制**


点击<新增>，配置应用行为控制规则。点击<确定>保存配置。




| | |
|---|---|
| **名称** | 设置应用行为控制规则的名称。 |
| **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。 |
| **设定白名单** | 输入可登录的 QQ 账号，当 QQ 登录的默认安全动作为禁止时，登录白名单生效。 |
| **备注** | 您可以为该规则添加备注，50 字符以内。 |

点击<删除>，可批量删除应用行为控制规则条目。

## 7.8.4 邮件内容过滤

在此可以配置对邮件内容过滤的规则。

**进入界面：对象 >> 安全配置文件 >> 邮件内容过滤**


点击<新增>，配置邮件过滤规则。点击<确定>保存配置。


| | |
|---|---|
| **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。 |
| **POP3** | 选择针对 POP3 协议的默认安全动作，可选允许/禁止。 |
| **IMAP** | 选择针对 IMAP 协议的默认安全动作，可选允许/禁止。 |
| **备注** | 您可以为该规则添加备注，50 字符以内。 |

点击<删除>，可批量删除邮件内容过滤规则条目。

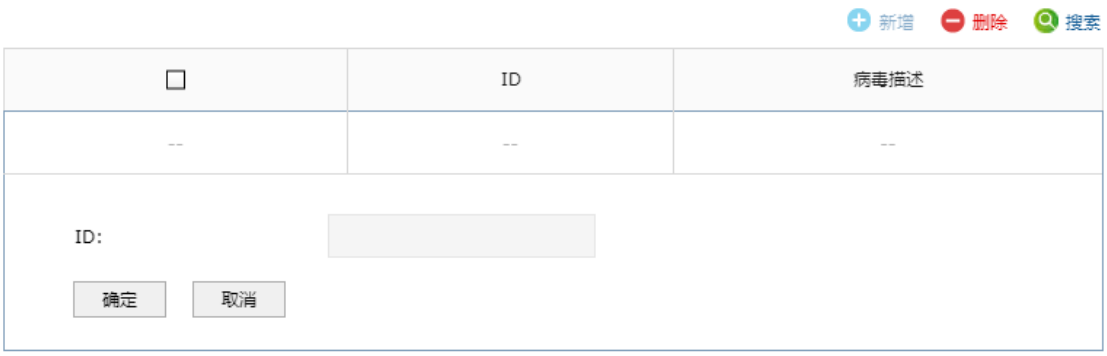
## 7.8.5 反病毒

**进入界面：对象 >> 安全配置文件 >> 反病毒**


点击<新增>，配置应用行为控制规则。点击<确定>保存配置。


| | |
|---|---|
| **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。



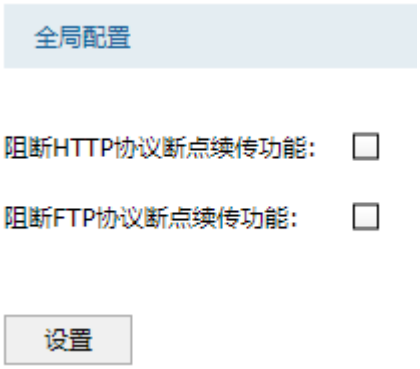

点击<删除>，可批量删除反病毒配置文件条目。

点击<搜索>，可批量查找不同的反病毒配置文件。


| | |
|---|---|
| **列名** | 默认名称作为搜索关键列。 |
| **内容** | 输入与名称相关的搜索关键内容。 |
| **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;<br>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。 |

### 7.8.6 全局配置

**进入界面：对象 >> 安全配置文件 >> 全局配置**




| | |
|---|---|
| **阻断 HTTP 协议断点续传功能** | 配置该功能后，HTTP 协议将无法断点续传。 |
| **阻断 FTP 协议断点续传功能** | 设置该功能后，FTP 协议将无法断点续传。 |

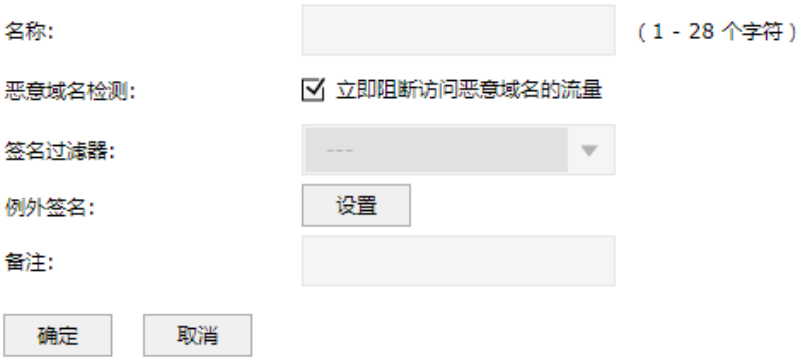
## 7.9 入侵防御

### 7.9.1 配置文件

您可以通过本页面设置 IPS 配置文件列表，并在安全策略中引用。

**进入界面：对象 >> 入侵防御 >> 配置文件**


点击<新增>，添加配置文件规则。点击<确定>保存配置。




| | |
|---|---|
| **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 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** | 对于警告应用中发现的病毒文件采取例外动作。 |

点击<删除>，可批量删除 IPS 配置文件。

## 7.9.2 签名过滤器

您可以通过本页面设置签名过滤器列表，用来将适合您的需求的签名组成集合，供 IPS 配置文件使用。

**进入界面：对象 >> 入侵防御 >> 签名过滤器**


点击<新增>，添加配置文件规则。点击<确定>保存配置。


| | |
|---|---|
| **名称** | 设置签名过滤规则的名称。 |
| **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。 |
| **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。 |

点击<删除>，可批量删除签名过滤器列表条目。

## 7.9.3 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。

**进入界面：对象 >> 入侵防御 >> 签名列表**


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。


| | |
|---|---|
| **列名** | 选择签名 ID、目标、严重性等作为搜索关键列。 |
| **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；<br>在所有条目中搜索：在所有列表条目中搜索。 |
| **状态** | 选择规则已启用或已禁用。 |
| **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。 |

点击<全局搜索>，可搜索不同内容、不同列名的列表信息。


| | |
|---|---|
| **列名** | 选择签名 ID、目标、严重性、操作系统、应用程序、协议和威胁类别进行搜索。 |
| **内容** | 输入搜索关键内容，该内容需与列名相关。 |
| **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。 |

# 第8章 网络

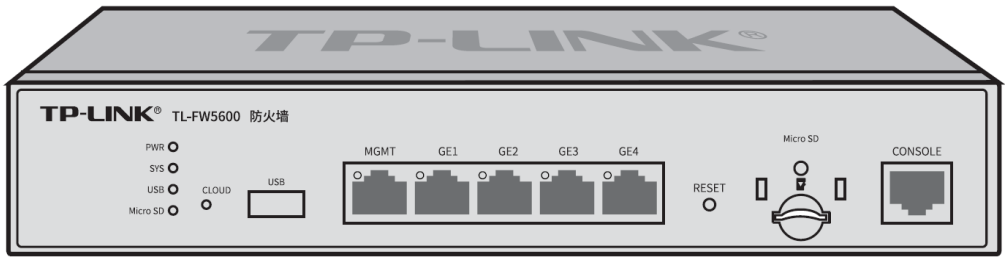
## 8.1 接口设置

为理解本防火墙接口的含义，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-FW5600的物理接口命名为端口MGMT/GE1/GE2/GE3/GE4，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-FW5600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。

TL-FW5600提供Ethernet和PPPoE两种类型的接口：

- 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、网吧局域网内组网使用静态IP连接方式，有线宽频使用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。

**说明：**

- 以上提到的三种接入方式：静态 IP、DHCP 和 PPPoE 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。

## 8.1.1 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。

**进入界面：网络 >> 接口设置 >> 接口设置**


在**接口设置**界面中，选择物理接口作为关联接口，点击<新增>按钮，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。

- 静态 IP 连接方式


| | |
|---|---|
| **接口类型** | 选择 Ethernet 接口类型。 |
| **接口名称** | 输入一个名称来标识一个接口。只能输入英文、数字和下划线。 |
| **关联接口** | 在此选择一个物理接口作为其关联接口。 |
| **关联 VLAN** | 输入一个该接口所属 VLAN 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** | 选择连接方式，有静态 IP 和 DHCP 两种连接方式。<br>选择静态 IP 连接方式，需要进行手动配置 IP 地址；选择 DHCP 连接方式，由防火墙动态获取 IP 地址。 |
| **IP 地址** | 设置接口的 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，允许留空。 |
| **上行带宽** | 设置接口的上行带宽，取值范围为 100-1000000Kbps，默认为 1000000Kbps。 |

| | |
|---|---|
| **下行带宽** | 设置接口的下行带宽，取值范围为 100-1000000Kbps，默认为 1000000Kbps。 |
| **MTU** | MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是 576-1500 之间的整数，默认值为 1500。若 ISP 未提供 MTU 值，请保持默认值不变。 |
| **首选 DNS 服务器** | 设置 DNS（Domain Name Server，域名解析服务器）地址，允许留空。 |
| **备用 DNS 服务器** | 设置备用 DNS 地址，允许留空。 |
| **MAC 地址** | 设置接口的 MAC 地址。 |
| **备注** | 填写对该接口的备注信息。 |
| **管理接口开启** | 勾选该项使该接口成为管理接口。 |

- DHCP 连接方式


| | |
|---|---|
| **接口类型** | 选择 Ethernet 接口类型。 |
| **接口名称** | 输入一个名称来标识一个接口。只支持英文、数字和下划线。 |
| **关联接口** | 在此选择一个 Ethernet 接口作为其关联接口。 |

| | |
|---|---|
| **关联 VLAN** | 输入一个该接口所属 VLAN 的 VLAN ID。当勾选“UNTAG”时，从该接口发出的报文不带 VLAN TAG；当勾选“UNTAG”时，从该接口发出的报文带有 VLAN TAG。 |
| **连接方式** | 选择连接方式，有静态 IP 和 DHCP 两种连接方式。<br>选择静态 IP 连接方式，需要进行手动配置 IP 地址；选择 DHCP 连接方式，由防火墙动态获取 IP 地址。 |
| **主机名** | 输入用于标识防火墙的名称。 |
| **上行带宽** | 设置接口的上行带宽，取值范围为 100-1000000Kbps，默认为 1000000Kbps。 |
| **下行带宽** | 设置接口的下行行带宽，取值范围为 100-1000000Kbps，默认为 1000000Kbps。 |
| **MTU** | MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是 576-1500 之间的整数，默认值为 1500。若 ISP 未提供 MTU 值，请保持默认值不变。 |
| **首选 DNS 服务器** | 设置 DNS（Domain Name Server，域名解析服务器）地址。 |
| **备用 DNS 服务器** | 设置备用 DNS 地址。 |
| **MAC 地址** | 设置接口的 MAC 地址。 |
| **备注** | 输入对该接口的备注信息。 |
| **管理接口开启** | 勾选该项使该接口成为管理接口。 |

## ■ PPPoE 接口


| | |
|---|---|
| **接口类型** | 选择 PPPoE 接口类型。 |
| **接口名称** | 输入一个名称来标识一个接口。只支持英文、数字以及/ \ . _ - @ 六个特殊字符，最多可以输入 15 个字符。 |
| **关联接口** | 在此选择一个 Ethernet 接口作为其关联接口。 |
| **用户名** | PPPoE 拨号的用户名，由 ISP 提供。可以输入 1-100 个字符，不支持中文字符。 |
| **密码** | PPPoE 拨号的密码，由 ISP 提供。可以输入 1-100 个字符，不支持中文字符。 |

| | |
|---|---|
| **连接方式** | 选择上网时连入互联网的方式，共有自动连接、手动连接和定时连接三种方式可供选择。<br>• 自动连接：每次接通防火墙电源，防火墙便自动拨号连入互联网，适合不限时间的包月计费拨号连接上网方式。<br>• 手动连接：需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。<br>• 定时连接：在**时间**下拉列表中选择时间表，设置连接时段，在此时段内防火墙如果开启则自动拨号连接，适合用于需要限时上网的场合。如需新建时间表，请参考**时间管理** |
| **上行带宽** | 设置接口的上行带宽，取值范围为 100-1000000Kbps，默认为1000000Kbps。 |
| **下行带宽** | 设置接口的下行行带宽，取值范围为 100-1000000Kbps，默认为1000000Kbps。 |
| **MTU** | MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是 576-1492 之间的整数，默认值为 1492。若 ISP 未提供 MTU 值，请保持默认值不变。 |
| **服务名** | 输入服务名称，由 ISP 提供。 |
| **首选 DNS 服务器** | 设置 DNS（Domain Name Server，域名解析服务器）地址，允许留空。 |
| **备用 DNS 服务器** | 设置备用 DNS 地址，允许留空。 |
| **备注** | 输入对该接口的备注信息。 |
| **管理接口开启** | 勾选该项使该接口成为管理接口。 |

**配置接口步骤：**

1) 创建Ethernet接口。必须操作。创建界面：网络 >> 接口设置 >> 接口设置，点击<新增>按钮，在显示的新增接口设置页面，选择接口类型为Ethernet，选择关联的VLAN，输入接口名称等必要信息，点击<确定>按钮完成。
2) 创建PPPoE接口。必须操作。创建界面：网络 >> 接口设置 >> 接口设置，点击<新增>按钮，在显示的新增接口设置页面，选择接口类型为PPPoE，选择其关联接口，输入接口名称等必要信息，点击<确定>按钮完成。

## 8.1.2 网桥设置

网桥可以在数据链路层上实现局域网互连，并对网络数据的流通进行管理。在TL-FW5600中，通过创建网桥接口，可以将多个物理接口级联在一起，达到不同接口之间互通的目的 。

当前系统的网桥接口一般作为"LAN"接口使用。而被桥接的接口配置其它任何业务都将无效。

**进入界面：网络 >> 接口设置 >> 网桥设置**

**说明：**

- 防火墙需要在出厂设置状态下才能进行网桥接口配置，请先到“系统工具->设备管理->恢复出厂配置”页面进行恢复设置。

点击<新增>按钮，进入网桥设置页面

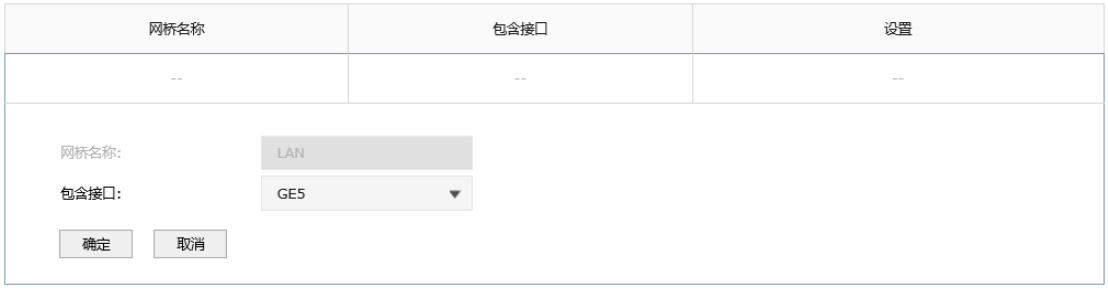



图 8-1 网桥设置

| | |
|---|---|
| **网桥名称** | 默认为“LAN”，不可更改。 |
| **包含接口** | 选择网桥所需包含的接口。 |

新增的条目会在**网桥设置列表**里显示出来，如下图所示。

| 网桥名称 | 包含接口 | 设置 |
|---|---|---|
| LAN | GE1,GE5 | |

点击条目后的<>按钮可删除网桥。

## 8.2 安全区域

您可以通过本页面设置防火墙安全区域。

**进入界面：网络 >> 接口设置 >> 安全区域**


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** | 您可以设置防火墙安全区域的备注，以方便您管理和查找。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。

## 8.3 DHCP 服务

当网络存在以下需求时，可以通过DHCP服务器完成网络设备的IP地址配置：

- 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时。

- 网络中设备数量远远大于该网络可使用的IP地址数量，而同一时间上网的设备数目却不多。例如，ISP限制同时接入网络的用户数目，而网络中的用户并不需要同时访问网络，则用户可以动态按需获得网络IP。
- 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。

### 8.3.1 DHCP 协议介绍

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。

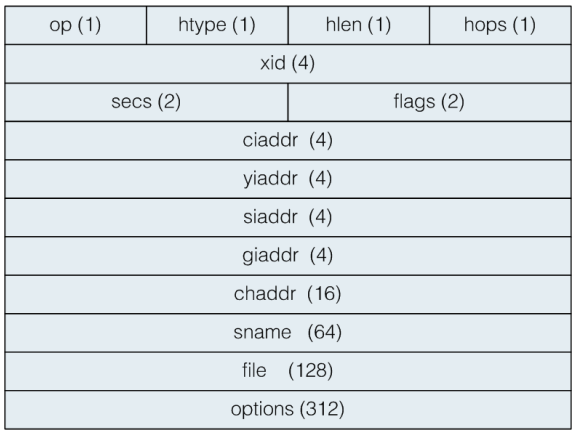
当网络规模扩大，计算机数量日益增多时，DHCP功能能够高效的完成TCP/IP参数配置，并将IP地址循环运用，提高使用效率。而随着无线网络的广泛使用，计算机的位置也经常变化，其所连接的子网也处于动态变化的过程，由此产生的TCP/IP参数变更问题基于DHCP也能够高效解决。

本防火墙可以作为 DHCP 服务器为网络中的计算机分配 TCP/IP 参数。

本小节主要介绍DHCP工作过程中采用的**DHCP报文格式**以及**DHCP地址分配过程**。

#### ■ DHCP 报文格式

DHCP报文的封装格式如下图所示：




| | |
|---|---|
| **OP** | 报文类型，分为请求类型报文和应答类型报文，1 表示此数据包为客户端发出 DHCP 请求报文，2 表示此数据包为服务器相应客户端的 DHCP 应答报文。 |
| **htype** | DHCP 客户端的网卡类型，常见的类型有 ethernet，当 htype 字段值为 1 时表示 DHCP 客户端的网卡为以太网网卡。 |

| | |
|---|---|
| **hlen** | DHCP 客户端的网卡地址长度，如果是以太网网卡，则 hlen 字段值为 6 字节。 |
| **hops** | DHCP 客户端发出 DHCP 请求报文时，此字段值设置为 0，请求报文在网络中每经过一个 DHCP 中继，该字段值自动加 1，通过此字段可以确定 DHCP 客户端与服务器之间经过了几个网络。 |
| **xid** | DHCP 客户端发出 DHCP 请求报文时，在此字段设置一个随机数，网络中不同的 DHCP 请求过程可通过不同的 xid 字段值进行区分，DHCP 服务器对每个不同的 DHCP 请求分配不同的地址，DHCP 客户端只能接受响应给他的 DHCP 应答报文，并接受第一个 DHCP 应答报文分配的 IP 地址。 |
| **secs** | DHCP 客户端开始 DHCP 请求时，在 DHCP 报文的 secs 字段设置为 0，并作为起始时间来统计 DHCP 请求过程总共花费的时间。目前没有使用，固定为 0。 |
| **flags** | 此字段的第一个 bit 位表示 DHCP 应答报文的发送方式，1 表示广播报文，0 表示单播报文，其余 bit 位目前保留，固定为 0。 |
| **ciaddr** | DHCP 客户端的 IP 地址，DHCP 客户端发出请求报文时可根据需要填入原先获得的 IP 地址。 |
| **yiaddr** | DHCP 服务器分配给客户端的 IP 地址。 |
| **siaddr** | 为 DHCP 客户端分配 IP 地址等信息的服务器 IP 地址。 |
| **giaddr** | DHCP 中继设备的 IP 地址。 |
| **chaddr** | DHCP 客户端的硬件地址，以太网网卡的 MAC 地址。 |
| **sname** | DHCP 服务器名称，可选项。 |
| **file** | DHCP 服务器为客户端指定的启动配置文件名称及路径信息。 |
| **options** | 可选变长选项字段，选项中可以记录 DHCP 报文类型、有效租期、DNS 服务器 IP 等配置信息。本设备暂不提供 options 选项识别及通过 options 选项分配 IP 地址。 |

## ■ DHCP 地址分配过程

在一个DHCP获取网络参数的过程中，其应用的传输层协议为UDP，客户端向服务器的DHCP服务端口67发出DHCP请求，服务器向客户端的DHCP用户端口68回复响应信息。DHCP客户端和服务器均按照DHCP协议标准格式报文发送DHCP报文。客户端通过动态分配地址的方式获取IP地址时，其获取IP地址的过程如下图所示：

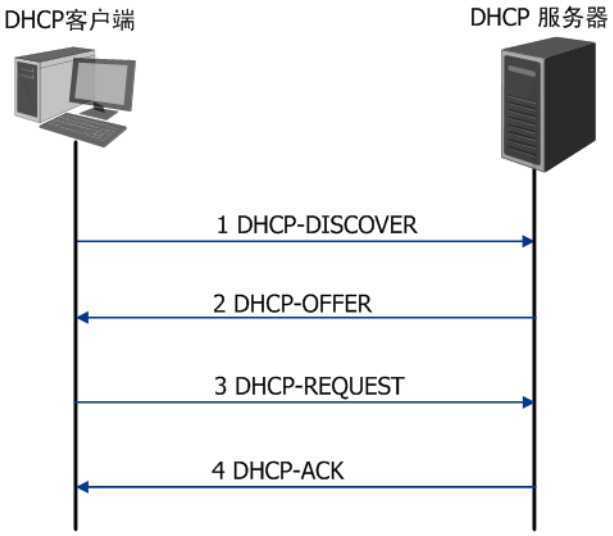



图 8-2　动态获取IP地址的过程

1) 发现阶段，客户端以广播方式发送DHCP-DISCOVER报文寻找DHCP服务器。

2) 提供阶段，DHCP服务器接收到客户端发送的DHCP-DISCOVER报文后，根据IP地址分配的优先次序从设定的地址段中选出一个IP地址，与其它参数一起通过DHCP-OFFER报文发送给客户端，发送方式由客户端发送的DHCP-DISCOVER报文中的flag字段决定，具体请见DHCP报文格式的介绍。

3) 请求阶段，如果有多台DHCP服务器向该客户端发来DHCP-OFFER报文，客户端只接受第一个收到的DHCP-OFFER报文，然后以广播方式发送DHCP-REQUEST报文，该报文的option字段包含DHCP服务器在DHCP-OFFER报文中分配的IP地址，具体请见DHCP报文格式的介绍。

4) 确认阶段，DHCP服务器收到DHCP客户端发来的DHCP-REQUEST报文后，只有DHCP客户端选择的服务器会进行如下操作：如果确认地址分配给该客户端，则返回DHCP-ACK报文；否则将返回DHCP-NAK报文，表明地址不能分配给该客户端。

5) 当客户端通过动态获取IP地址时，则DHCP服务器分配给客户端的IP地址具有一定的租期，当租期满后服务器将收回该IP地址。如果DHCP客户端希望继续使用该IP地址，在地址租期到达一半时，可以向服务器发送单播的DHCP-REQUEST报文续约IP地址。

## 8.3.2 DHCP 功能介绍

本节主要介绍在TL-FW5600防火墙上实现的DHCP服务器功能细节，主要包括五部分内容，动态地址分配策略、**DHCP服务器功能典型应用环境**、**DHCP服务器功能实现细节**、**IP地址重复分配检测**和**分配IP地址的优先次序**。

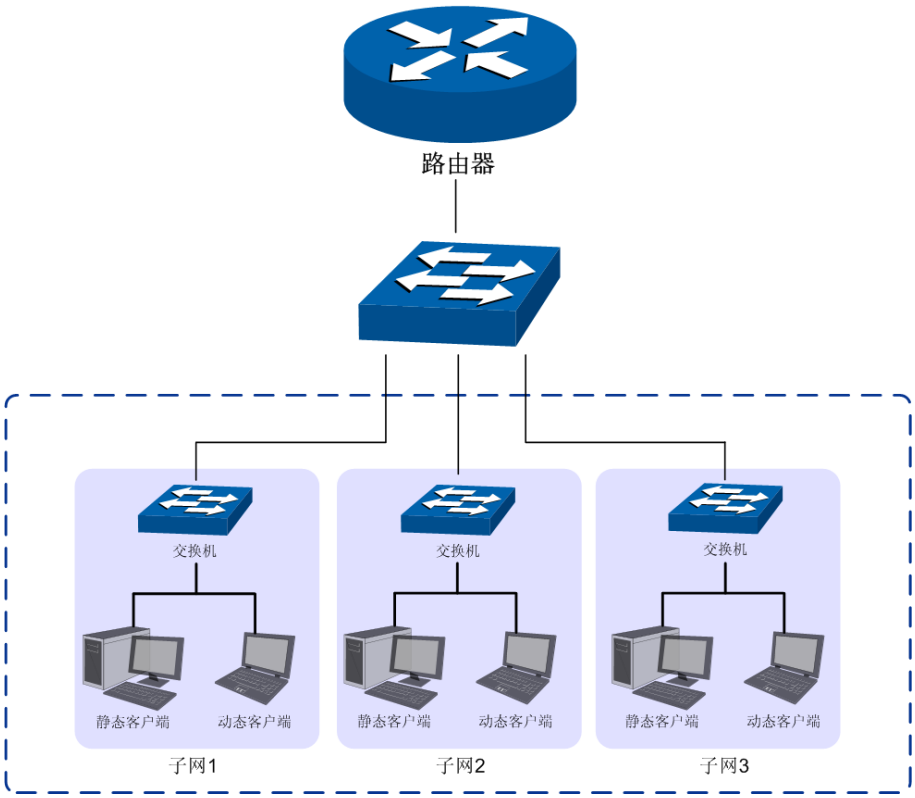
### ■ 动态地址分配策略

TL-FW5600防火墙支持两种地址动态分配策略：

- 为普通客户端分配具有一定有效期限的IP地址，如果客户端希望能够持续访问网络，在租约到期前客户端可以向服务器续约；
- 为特殊客户端静态绑定固定的IP地址，当收到来自特殊客户端的DHCP请求时，为其分配无限期的IP地址。

### ■ DHCP 服务器功能典型应用环境

下图为防火墙TL-FW5600配置为DHCP服务器时的网络拓扑图使用示范，具体的网络环境可根据实际需要调整。




如图所示，某IT企业网络按照研发部门的分类分为软件小组、硬件小组和测试小组3个子网，在每个子网中，动态客户端通过“自动获取IP地址”的方式从TL-FW5600防火墙上获得各自所属子网的IP地址，静态客户端手动设置IP地址。

## ■ DHCP 服务器功能实现细节

为了使网络中的设备能够安全顺利的获得IP地址，保证网络的稳定性，TL-FW5600防火墙的DHCP服务器功能可以完成如下任务：

1) TL-FW5600可以为多达64个Ethernet接口类型网络分配地址。

**说明：**

- 如果 Ethernet 类型接口的 IP 地址是动态获取的，由于其 IP 地址的不确定性，因此暂不提供此类接口的 DHCP 服务器功能。
- 对于 PPPoE 接口，由于其 IP 地址的不确定性，TL-FW5600 防火墙也暂不提供 DHCP 服务器功能。

2) 当TL-FW5600收到DHCP请求报文时，将根据数据包中的VLAN ID信息选择相应接口设定的地址段来分配地址。

3) 为Ethernet类型接口网络中的特殊客户端手动绑定静态IP，当此接口收到特殊客户端的DHCP服务请求时，防火墙将为客户端分配无限期的固定的IP地址。此类IP地址也会为特殊的客户端保留不会分配给其他客户端。

4) IP地址重复分配检测功能，为避免待分配地址已在网络中被使用，而导致分配后造成网络中IP冲突，防火墙在分配一个IP地址前，会向所有接口网络发起待分配地址的Ping检测，从而避免IP冲突。

### ■ IP 地址重复分配检测

防火墙在分配一个IP地址前，会向所有接口网络发起目的地址为待分配地址的ICMP回显请求报文，如果任意一个接口在等待时间内收到响应报文，DHCP服务器从设定的地址段中选择新的IP地址，并重复上述探测操作；如果在指定时间内没有收到回显响应报文，则继续发送ICMP回显请求报文，直到发送的回显请求报文达到最大值，如果仍然没有收到回显响应报文，则将此待分配地址分配给客户端，从而确保客户端被分得的IP地址是网络中唯一的。

### ■ 分配 IP 地址的优先次序

TL-FW5600防火墙为客户端分配IP地址时将遵循以下分配规则秩序：

1) DHCP服务器中与客户端MAC地址手动绑定的IP地址。

2) DHCP服务器曾经分配给客户端的IP地址。

3) 客户端发送的DHCP-DISCOVER报文中指定的IP地址。

4) 选择合适的地址段，从中顺序查找可供分配的第一个IP地址。

## 8.3.3 DHCP 服务

DHCP功能配置主要分为配置IP地址段、为特殊客户端绑定静态地址和查看当前所有的DHCP三部分进行配置。如下介绍配置IP地址段步骤。

**进入界面：网络 >> DHCP服务 >> DHCP服务**

点击<启用>，可批量启用 DHCP 服务规则。

点击<禁用>，可批量禁用 DHCP 服务规则。

在DHCP服务界面点击<　　>按钮，进入DHCP服务设置页面。


| | |
|---|---|
| **服务接口** | 选择需要提供 DHCP 服务的 Ethernet 接口。 |
| **开始/结束地址** | DHCP 服务器自动分配的 IP 的开始/结束地址。 |
| **地址租期** | 输入此地址段中的 IP 地址在每次分配后可供客户端使用的租期。 |
| **网关地址** | 输入此地址段的给客户端分配的默认网关，也可以将接口 IP 地址配置为默认网关。 |
| **缺省域名** | 输入此地址段的给客户端指定的域，与 IP 地址一样共同表示相同子网的计算机的集合，同一接口网络中的计算机通常配置为相同的域名。 |
| **首选 DNS 服务器** | 输入此地址段的给客户端分配的首选 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。 |
| **备用 DNS 服务器** | 输入此地址段的给客户端分配的备用 DNS 服务器，当首选 DNS 服务器失效时客户端可以向备用 DNS 服务器申请域名解析。 |
| **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。 |
| **状态** | 选择“启用”，则使该绑定条目生效；<br>未选择“启用”，则使该绑定条目失效。 |

配置完成的地址段信息会在**DHCP服务器列表**区域显示出来，如下图所示。

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 | 192.168.0.1 | 192.168.0.254 | 120 | 192.168.0.0 | --- | 已启用 | |

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。

点击<删除>，可批量删除 DHCP 服务规则。

点击<搜索>，可根据列名、内容、方式和方式进行搜索。


| | |
|---|---|
| **列名** | 选择服务接口、开始地址、结束地址等作为搜索关键列。 |
| **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；<br>在所有条目中搜索：在所有列表条目中搜索。 |
| **状态** | 选择规则已启用或已禁用。 |
| **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。 |

## 8.3.4 客户端列表

本栏用于查看 DHCP 的客户端相关信息。

**进入界面：网络 >> DHCP服务 >> 客户端列表**


- 搜索

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择服务接口、主机名、MAC 地址、IP 地址作为搜索关键列。 |
| **内容** | 输入与列名相关的搜索关键内容。 |
| **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；<br>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。 |

- 全局搜索

点击<全局搜索>，可搜索一个时间范围内，不同服务接口的客户端列表信息。


| | |
|---|---|
| **列名** | 选择服务接口、主机名、MAC 地址、IP 地址作为搜索关键列。 |
| **内容** | 输入与列名相关的搜索关键内容。 |
| **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。 |

- 刷新

点击<刷新>，更新客户端列表信息。

- 自动刷新

勾选<自动刷新>，自动更新客户端列表信息。

## 8.3.5 静态地址分配

**说明：**

- 如果为特殊客户端绑定了静态地址，又设置了 ARP 防护功能的 IP&MAC 绑定，此时，请确保两处设置的表项互不冲突，否则对应的客户端可能无法上网。建议将 ARP 绑定表导出，然后再将其导入到 DHCP 静态绑定地址表中，请参考批量导入静态绑定的 IP/MAC 地址表进行配置。

**进入界面：网络 >> DHCP服务 >> 静态地址分配**

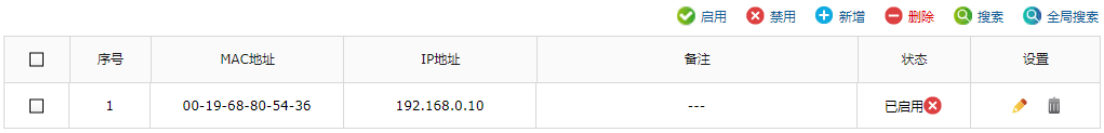
点击<新增>按钮，进入静态地址设置页面。在界面中为具有设定MAC地址的客户端手动绑定静态IP，当条目服务接口收到来自设定客户端的DHCP服务请求时，防火墙将为客户端分配租期为无限长的固定的IP地址，点击<确定>按钮手动创建条目。


| | |
|---|---|
| **MAC 地址** | 输入特殊客户端的 MAC 地址。 |
| **IP 地址** | 输入需要为特殊客户端保留的 IP 地址。该静态 IP 地址需与接口 IP 地址在同一网段。 |
| **备注** | 输入字符串描述该静态地址以便识别。 |
| **状态** | 选择“启用”，则使该绑定条目生效；<br>不选择“启用”，则使该绑定条目失效。 |

**说明：**

- 当其他非服务接口收到特殊客户端的 DHCP 请求时，将无法获得绑定的静态地址。若其他非服务接口也提供 DHCP 服务功能，则给特殊客户端分配其接口的 IP 地址段中的地址；如果其他非服务接口没有开启 DHCP 服务功能，特殊客户端将无法获得 IP 地址。

新增的静态地址绑定条目会在下方的**地址列表**区域显示出来，如下图中所示。




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

点击<启用>，可批量启用静态地址。

点击<禁用>，可批量禁用静态地址。

点击<删除>，可批量删除静态地址。

点击<搜索>，可根据列名、内容、方式和方式进行搜索。


| | |
|---|---|
| **列名** | 选择 MAC 地址、IP 地址、备注作为搜索关键列。 |
| **内容** | 输入与列名相关的搜索关键内容。 |
| **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;<br>在所有条目中搜索：在所有列表条目中搜索。 |
| **状态** | 选择已启用或已禁用的状态 |
| **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。 |

点击< 全局搜索>可搜索，一个时间范围内，不同服务接口的静态地址分配信息。


| | |
|---|---|
| **列名** | 选择 MAC 地址、IP 地址、备注作为搜索关键列。 |
| **内容** | 输入与列名相关的搜索关键内容。 |
| **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。 |

## 8.4 路由设置

本防火墙提供多种负载均衡策略，包括特殊应用程序选路，智能均衡，ISP 选路，线路备份等。

### 8.4.1 基本设置

通过基本配置，可实现流量均衡。

**进入界面：网络 >> 路由设置 >> 基本设置**


- 全局设置

勾选<启用流量均衡>，则全局开启流量均衡功能，点击<设置>按钮保存配置。若不勾选，则所有流量均衡功能关闭。

- 功能设置

勾选<启用特殊应用程序选路功能>，点击<设置>按钮使配置生效。启用此功能后，防火墙会将数据包的源 IP 地址与目的 IP 地址，或者源 IP 地址与特殊目的端口作为一个整体，记

录其通过的接口信息。后续一定时间内如果有同一源 IP 地址和目的 IP/端口地址的数据包通过，则优先转发至上次记录的接口。该功能主要用于保证多连接应用程序的正常工作。

勾选<启用智能均衡>，选择参与智能均衡的接口，点击<设置>按钮使配置生效。

**说明：**

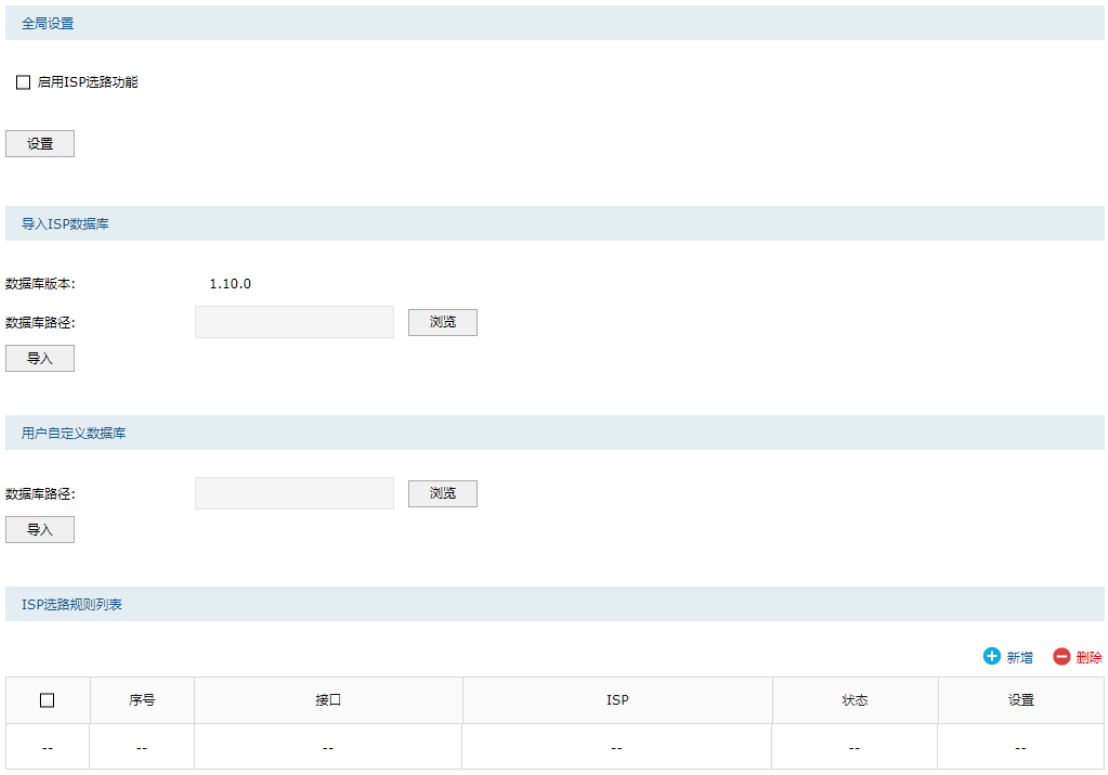
- 在实际应用中，如果某些接口没有连接到因特网，那么这些接口将不会参与到智能均衡，请勿勾选。

设置完成后，在路由器没有设置其它选路规则的情况下，路由器将自动进行流量均衡。

## 8.4.2 ISP 选路

在 ISP 选路中，通过选择接口和 ISP，可以将数据包转发至对应的 ISP 线路上，从而减少数据包在网络中被转发的次数，提高网络性能。

**进入界面：网络 >> 路由设置 >> ISP选路**




- 全局设置

勾选<启用 ISP 选路功能>，则全局开启 IPS 选路功能，点击<设置>按钮保存配置。

- 导入 ISP 数据库

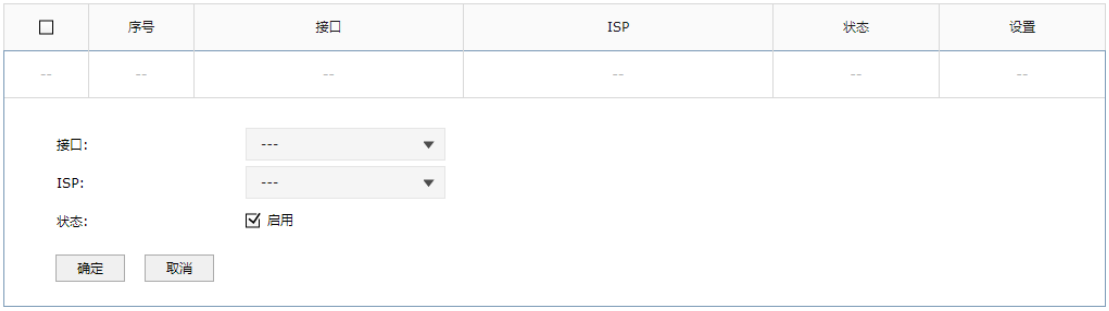
ISP 数据库即各 ISP 所拥有的 IP 地址段的数据库，通过匹配数据包目的 IP 地址与 ISP 数据库，路由器会将数据包从相应 ISP 所对应的接口转发。请在我司官方网站下载最新 ISP 数据库，单击<浏览>按钮，选择保存路径下的文件，点击<导入>即可。

- 用户自定义数据库

用户也可导入自定义的数据库，单击<浏览>按钮，选择保存路径下的文件，点击<导入>即可。

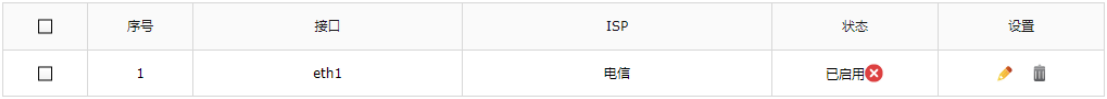
- ISP 选路规则列表

点击<新增>按钮，手动添加 ISP 选路条目。




| | |
|---|---|
| **接口** | 选择进行 ISP 选路的接口。 |
| **ISP** | 在下拉列表中选择 ISP。 |
| **状态** | 勾选后启用该 ISP 选路规则。 |

新增的条目会在选路列表里显示出来，如下图所示。




如有需要，可以点击条目后的<>按钮进行编辑。

点击<删除>，可批量删除ISP选路规则。

**说明：**

- 智能均衡、策略路由、ISP 选路三个功能可以同时工作，但当三个功能设置有冲突时，路由器执行的优先顺序为：策略路由 > ISP 选路 > 智能均衡。

## 8.4.3 线路备份

根据实际需要合理设置线路备份，可以减轻接口流量负担，提高网络效率。当一个接口出现故障时，路由器能够及时地把数据切换到其它正常的接口上，为网络稳定性提供强大保证。

**进入界面：网络 >> 路由设置 >>线路备份**

点击<新增>按钮，进入备份规则设置页面。设置主备接口并选择备份模式，点击<确定>按钮手动添加条目。


| | |
|---|---|
| **主接口** | 选择一个接口作为主接口。接口设置请参考 3.2.1 接口设置。 |
| **备接口** | 选择一个接口作为备接口用来备份主接口的流量。接口设置请参考 3.2.1 接口设置。 |
| **备份模式** | 可以选择定时备份或故障备份。选择定时备份时，下方可进行备份生效时间设置；选择故障备份时，主接口发生故障时启动备份接口。 |
| **生效时间** | 当备份模式为定时备份时，需要在此指定生效时间。在生效时间内启动备份接口，关闭主接口。时间设置请参考 5.2 时间管理。 |
| **故障备份** | 当备份模式为故障备份时，在主接口正常工作时备份接口不工作，主接口发生故障时启动备份接口。 |
| **状态** | 勾选“启用”，则使该规则条目生效；<br>不勾选“启用”，则使该规则条目失效。 |

新增的条目会在线路备份规则列表里显示出来，如下图所示。


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

点击<删除>，可批量删除线路备份规则。

## 8.4.4 策略路由

通过对服务类型、源地址、目的地址、生效接口和生效时间的设置，可以更加精确的控制路由器进行选路。

**进入界面：网络 >> 路由设置 >> 策略路由**

点击<新增>按钮，进入策略路由规则设置页面。填入策略名称，并选择服务类型、源地址、目的地址、生效接口和生效时间，选择启用规则并点击<确定>按钮手动添加条目。


| | |
|---|---|
| **规则名称** | 用户自定义，标识一条选路规则。只能输入英文、数字和下划线。 |
| **服务类型** | 在下拉列表中选择本条规则所针对的服务类型，不属于指定范围内的协议将不会应用选路规则。如果列表中没有您想指定的协议类型，可以在对象管理 >> 服务类型界面设置，详细配置过程请参考 5.4 服务类型小节。 |
| **源地址** | 在下拉列表中选择需要应用选路规则的源地址范围。源地址可以在对象管理 >> 地址管理 >> 地址界面设置。详细配置过程请参考 5.1 地址管理小节。 |
| **目的地址** | 在下拉列表中选择需要应用选路规则的目的地址范围。源地址可以在对象管理 >> 地址管理 >> 地址界面设置。详细配置过程请参考 5.1 地址管理小节。 |
| **生效接口** | 选择指定数据包转发接口。 |
| **生效时间** | 选择规则生效的时间。生效时间可以在对象管理 >> 时间管理界面进行设置。详细配置过程请参考 5.2 时间管理小节。 |
| **强制** | 勾选该条目，接口不在线时仍应用此规则 |
| **备注** | 添加对本条规则的说明信息。 |
| **添加到指定位置** | 输入本条规则在规则列表中的序号以设定该规则的优先级，序号越小表示优先级越高。若留空则系统将按照规则设定的先后顺序对规则进行依次排序。 |

| | |
|---|---|
| **状态** | 勾选“启用”，则使该规则条目生效；<br>不勾选“启用”，则使该规则条目失效。 |

新增的条目会在**规则列表**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，点击<>按钮启用条目，点击<>按钮禁用条目。

## 8.4.5 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。

**进入界面：网络 >> 路由设置 >> 静态路由**

点击<新增>按钮，进入静态路由设置页面。输入静态路由各项参数，点击<确定>按钮手动添加条目。


| | |
|---|---|
| **规则名称** | 输入该规则条目的名称。只能输入英文、数字和下划线。 |
| **目的地址** | 设置静态路由规则条目指向的目标网络地址。 |
| **子网掩码** | 设置静态路由规则条目指向的目标网络的子网掩码。 |
| **下一跳** | 设置通往目标网络的路由路径上下一个节点的 IP 地址。 |

| | |
|---|---|
| **出接口** | 设置数据从本地发出的出接口。 |
| **Metric** | 设置路由规则的优先级，数值越低则优先级越高，0 为最高优先级。当网络中存在多条路由可以到达同一目的地址，可以通过调整 Metric 来调整路由规则的优先级，数据包将按照 Metric 值最小的路径转发。 |
| **备注** | 添加对本条规则的说明信息。 |
| **启用/禁用规则** | 勾选“启用”，则使该规则条目生效；<br>未勾选“启用”，则该规则条目失效。 |

新增的静态路由条目会在**规则列表**中显示出来，如下图所示。


如图所示，静态路由规则“rule1”表示：发往目标网络 192.168.3.0/24 的数据可以通过接口 GE2 发往 192.168.1.2 节点上，节点 192.168.1.2 将执行下一个转发任务，此静态路由规则的 Metric 值为 0 拥有最高优先级。可达性为“不可达”，说明该静态路由无效。

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

点击<启用>，可批量启用静态路由规则。

点击<禁用>，可批量禁用静态路由规则。

点击<删除>，可批量删除静态路由规则。

点击<搜索>，可根据列名、内容、方式和方式进行搜索。


| | |
|---|---|
| **列名** | 选择规则名称、目的地址、子网掩码等作为搜索关键列。 |
| **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;<br>在所有条目中搜索：在所有列表条目中搜索。 |
| **状态** | 选择规则已启用或已禁用。 |
| **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。 |

## 8.4.6 系统路由

**进入界面：路由 >> 路由设置 >> 系统路由**

系统路由下显示了路由器建立的所有路由规则条目，如下图所示。

条目数量: 3 刷新

| 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 | 192.168.0.0 | 255.255.255.0 | 0.0.0.0 | GE2 | 0 |
| 3 | 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | MGMT | 0 |

| | |
|---|---|
| **目的地址** | 该路由规则条目指向的目标网络地址。 |
| **子网掩码** | 该路由规则条目指向的目标网络的子网掩码。 |
| **下一跳** | 通往目标网络的路由路径上下一个节点的 IP 地址。 |

| | |
|---|---|
| 出接口 | 数据从本地发出的出接口。 |
| Metric | 路由规则的优先级，数值越低则优先级越高，0 为最高优先级。当网络中存在多条路由可以到达同一目的地址，可以通过调整 Metric 来调整路由规则的优先级，数据包将按照 Metric 值最小的路径转发。 |

## 8.5 IPSec

IPSec（IP Security）是保证网络安全的一系列服务和协议的集合，主要依赖密码技术提供验证和加密机制，可实现如下安全服务：

☐ 数据机密性（Confidentiality）：发送方在传输数据前对数据包进行加密，有效避免传输过程中数据包被截取所带来的风险。

☐ 数据完整性（Data Integrity）：接收方接收数据时利用散列函数对每个数据包重新生成一个校验和，与发送方生成的校验和相比较，二者不符则丢弃相应数据包，防止数据在传输过程中被篡改。

☐ 数据来源验证（Data Authentication）：接收方及发送方相互进行身份验证，确保数据来源的合法性。

☐ 防重放（Anti-Replay）：接收方可识别并丢弃重发的报文，防止第三方利用截取的报文进行攻击。

IPSec 在 IP 层实现了验证、加密、访问控制等多种安全技术，通过通信双方建立双向安全联盟，在互联网中形成一个安全可靠的 IPSec 隧道，确保数据的安全传输。

IPSec 协议集主要包括认证头协议 AH（Authentication Header）、封装安全载荷协议 ESP（Encapsulating Security Payload）及互联网密钥交换协议 IKE（Internet Key Exchange），其中 AH 协议和 ESP 协议通过对传输数据的处理提供安全性保证；IKE 协议则通过实现密钥的协商、交换、分发提供了处理传输数据的相应规则。

## 8.5.1 IPSec 安全策略

**进入界面：网络>> IPSec >> IPSec安全策略**


点击<新增>，进行 IPSec 基本设置。


| | |
|---|---|
| **策略名称** | 为 IPSec 安全策略命名。 |
| **对端网关** | 输入对端 IPSec 链路的绑定接口，可以填写对端接口的 IP 地址或域名。可设置为"0.0.0.0"，表示任意地址。 |
| **绑定接口** | 绑定本地 IPSec 链路的出接口；对端路由器设置的"对端网关"必须与该接口的 IP 地址或域名相同。 |
| **本地子网范围** | 设定本地子网地址，以子网掩码值划分地址范围。 |
| **对端子网范围** | 设定对方子网地址，以子网掩码值划分地址范围。 |
| **预共享秘钥** | 设置通信双方互相认证的密钥，双方必须使用同一字符串作为预共享密钥，可输入英文字母和数字的组合。 |
| **状态** | 选择启用或禁用当前策略条目。 |

点击<高级设置>，进行 IPSec 高级设置。


阶段 1 设置

| | |
|---|---|
| **安全提议** | 指定相应的 IKE 安全提议，最多可选择四个安全提议。 |
| **交换模式** | 设置 IKE 协商第一阶段的交换模式，该交换模式必须与对端相同。交换模式有以下两种：<br>主模式：该模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。<br>野蛮模式：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** | 设置 IKE 协商的模式，该协商模式可以与对端不同。协商模式有以下两种：<br>初始者模式：配置该模式后，IKE 才能主动发起协商。 本地和对端至少有一方必须设置为初始者模式。<br>响应者模式：配置该模式后，IKE 不会主动发起协商，需要等待对端发起协商。本地和对端不能同时为响应者模式。 |
| **本地/对端 ID 类型** | 设置本地和对端的 ID（Identity，身份标识）类型，用于进行 ID 的交换与认证，可以选择“IP 地址”或“NAME”，通信双方的设置需保持一致。 |
| **本地/对端 ID** | ID 类型选择“IP 地址”时，无需进行设置；ID 类型选择“NAME”时，可自定义本地/对端的 ID（任意英文字母和数字的组合）。本地设备的“本地 ID”需与对端设备的“对端 ID”保持一致，而“对端 ID”则需与对端设备的“本地 ID”保持一致。 |
| **生存时间** | 设定 IKE SA 的生存时间，单位为秒。 |
| **DPD 检测开启** | DPD（Dead Peer Detect，对端存活检测）开启后，IKE 一端能够周期性主动检测对端的链路连接状态。 |


阶段 2 设置

| | |
|---|---|
| **封装模式** | 设置隧道中数据报文的封装模式，该封装模式必须与对端相同。封装模式有以下两种：<br>隧道模式：在该模式下，AH 或 ESP 插在原始 IP 报文头之前，另外生成一个新的 IP 报头放到 AH 或 ESP 之前。从安全性来讲，隧道模式优于传输模式。适用于更普遍的 VPN 应用。<br>传输模式：在该模式下，AH 或 ESP 被插入到 IP 报头之后但在所有传输层协议之前，或所有其他 IPSec 协议之前。适用于主机直接访问设备时的加密传输。 |
| **安全提议** | 指定相应的 IPsec 安全提议，最多可选择四个安全提议。 |
| **PFS** | 选择是否启用 PFS（Perfect Forward Secrecy，完全前向保密），通信双方的 PFS 设置需保持一致。 |
| **生存时间** | 设定 IPSec SA 的生存时间，单位为秒。 |

**说明：**

- 子网掩码值的相关设置请参考附录 A 常见问题中的问题 4。

## 8.5.2 IPSec 安全联盟

在此将列出防火墙上所有已成功建立的 IPSec 安全联盟相关信息。

**进入界面：网络 >> IPSec >> IPSec安全联盟**

IPSec安全联盟列表

条目数量：0　　刷新

| ☐ | 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_1 | 337435911 9 | in | 192.168.10.100<-172.29.85.199 | 192.168.1.0/24:0 <-192.168.0.0/24:0,any | ESP | -- | MD5 | 3DES |
| -- | 2 | IPsec_1 | 781159572 | out | 192.168.10.100->172.29.85.199 | 192.168.1.0/24:0->192.168.0.0/24:0,any | ESP | -- | MD5 | 3DES |

IPSec 隧道的安全提议等相关设置需与对端设备设置相同。

由于安全联盟是单向的，所以当 IPSec 隧道成功建立后，每条隧道会产生一对出和入的安全联盟。出和入的 SPI 值是不同的，但与对端的入和出 SPI 值相同，即本端方向 in 的 SPI 值与对端方向 out 的 SPI 值相同。这条隧道在对端的连接信息如下图所示，SPI 值为 IKE 自动协商得出。


| ☐ | 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_2 | 781159572 | in | 172.29.85.199 <-<br>192.168.10.100 | 192.168.0.0/24:0 <-<br>192.168.1.0/24:0,any | ESP | -- | MD5 | 3DES |
| -- | 2 | IPsec_2 | 337435911 9 | out | 172.29.85.199 ->192.168.10.100 | 192.168.0.0/24:0->192.168.1.0/24:0,any | ESP | -- | MD5 | 3DES |

## 8.6 L2TP

L2TP（Layer 2 Tunneling Protocol， 第二层隧道协议）是二层 VPN 隧道协议，它的实现基于 C/S（Client/Server，客户端/服务器）模型，在客户端和服务器间建立起 L2TP 隧道。客户端任选一个空闲的端口向服务器的 UDP 1701 端口发送报文，服务器收到报文后，也任选一个空闲的端口向客户端回送报文，至此，双方的端口选定，在该隧道连通的时间内保持不变。

L2TP 协议本身并不提供连接的安全性，但它可依赖于 PPP 提供的认证（比如 CHAP、PAP 等），因此具有 PPP 所具有的所有安全特性。L2TP 可与 IPSec 结合起来实现数据安全，这使得通过 L2TP 所传输的数据更难被攻击。L2TP 还可根据特定的网络安全要求在 L2TP 之上采用隧道加密技术、端对端数据加密或应用层数据加密等方案来提高数据的安全性。

### 8.6.1 L2TP 服务器设置

当路由器作为 L2TP 服务器时，则还需进入 VPN 用户管理界面设置用户账号。

**进入界面：网络 >>L2TP >> L2TP服务器**

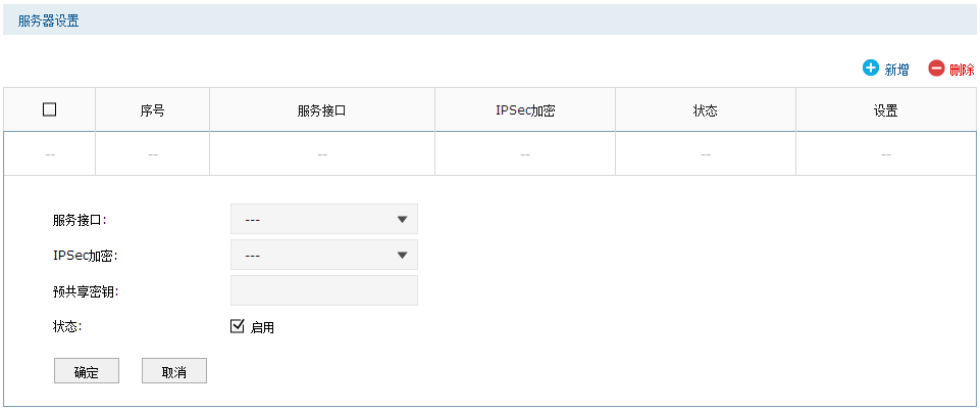

- 全局设置

| | |
|---|---|
| **L2TP 隧道维护时间间隔** | 设置 L2TP 隧道维护的时间间隔，范围是 60 秒至 1000 秒。设置此时间间隔，服务器按照设定间隔发出报文，用以确定 L2TP 隧道的连接状态。如无特别要求，请保持默认设置。 |

| | |
|---|---|
| **PPP 链路维护时间间隔** | 设置 L2TP 隧道里的 PPP 链路维护的时间间隔。范围是 0 秒至 120 秒，0 代表不发送。设置此时间间隔，服务器按照设定间隔发出报文，用以确定 PPP 链路的连接状态。如无特别要求，请保持默认设置。 |

- 服务器设置

点击<新增>，进行服务器设置。点击<确定>，使配置生效。




| | |
|---|---|
| **服务接口** | 绑定接口为服务器端路由器 WAN 端口上出链路接口。如有多条上网链路，请根据实际情况，选择其中一条链路承载 L2TP VPN 隧道。此接口的 IP 地址即为 L2TP 服务器的 IP 地址。 |
| **IPSec 加密** | 选择是否使用 IPSec 对 L2TP 隧道加密。可选项有：加密，不加密，可选加密。 |
| **预共享秘钥** | 设置 IPSec 加密时通信双方互相认证的密钥，双方必须使用同一个预共享密钥。 |
| **状态** | 选择启用或禁用本 L2TP 隧道。 |

## 8.6.2 L2TP 客户端设置

**进入界面：网络 >> L2TP >> L2TP 客户端**


- 全局设置

| | |
|---|---|
| **L2TP隧道维护时间间隔** | 设置L2TP隧道维护的时间间隔，范围是60秒至1000秒。设置此时间间隔，服务器按照设定间隔发出报文，用以确定L2TP隧道的连接状态。如无特别要求，请保持默认设置。 |
| **PPP链路维护时间间隔** | 设置L2TP隧道里的PPP链路维护的时间间隔。范围是0秒至120秒，0代表不发送。设置此时间间隔，服务器按照设定间隔发出报文，用以确定PPP链路的连接状态。如无特别要求，请保持默认设置。 |

- 客户端设置

点击<新增>，进行客户端设置。点击<确定>，使配置生效。


| | |
|---|---|
| **隧道名称** | 设置隧道名称。 |

| | |
|---|---|
| **用户名** | 设置 L2TP 认证时客户端使用的用户名。客户端与服务器的设置需保持一致。 |
| **密码** | 设置 L2TP 认证时客户端使用的密码。客户端与服务器的设置需保持一致。 |
| **出接口** | 服务器端路由器 WAN 端口上出链路接口。如有多条上网链路，请根据实际情况，选择其中一条链路承载 L2TP VPN 隧道。 |
| **服务器地址** | 设置对端服务器地址。 |
| **IPsec 加密** | 选择是否使用 IPSec 对 L2TP 隧道加密。 |
| **预共享秘钥** | 设置 IPSec 加密时的预共享密钥。 |
| **对端子网** | 设置 L2TP 隧道对端局域网所使用的 IP 地址范围（一般可以填 VPN 隧道对端设备的 LAN 口 IP 地址范围），由 IP 和子网掩码组成。 |
| **上行带宽** | 设置最大上行带宽。 |
| **下行带宽** | 设置最大下行带宽。 |
| **工作模式** | 选择 NAT 模式或路由模式。 |
| **状态** | 选择启用或禁用本 L2TP 隧道。 |

### 8.6.3 隧道信息列表

在此将列出路由器上所有里 L2TP 隧道的相关信息。

**进入界面：网络 >> L2TP >> 隧道信息列表**

点击< 刷新>，获取最新的隧道信息列表。


## 8.7 PPTP

PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）定义于 IETF 的 RFC2637 中，是一种在 PPP（Point to Point Protocol，点到点）协议基础上开发的支持按需、多协议 VPN 的二层隧道技术，通过跨越基于 TCP/IP 的数据网络创建 VPN，实现安全的远程访问连接。

PPTP 的实现基于 C/S（Client/Server，客户端/服务器）模型，在客户端和服务器间建立起 PPTP 隧道。客户端使用服务器提供的账户信息拨号连接到服务器上，服务器默认在 TCP 1723 端口上监听服务，从而实现双方的通信。

PPTP 的通信要建立两条连接，即控制连接和数据连接。控制连接使用 TCP 作为传输协议，用于对呼叫的控制和管理，负责建立、维护和拆除客户端和服务器间的数据隧道；数据连接使用 PPP 协议对原始报文进行封装，使用增强的 GRE（Generic Routing Encapsulation，通用路由封装）协议作为隧道协议，并添加新的 IP 头用于数据在互联网上路由。

安全性上，PPTP 利用了 PPP 提供的认证机制，支持 PAP（Password Authentication Protocol，密码认证协议）、CHAP（Challenge Handshake Authentication Protocol，询问握手认证协议）、MS-CHAP（微软 CHAP）等身份验证方式，可选用 MPPE（Microsoft Point-to-Point Encryption，微软点对点加密）协议进行加密。MPPE 加密技术支持 40、56、128 位三种长度的加密，其安全性被普遍认为比较弱，因此，如涉及到敏感数据传输，一般不推荐使用 PPTP VPN。

### 8.7.1 PPTP 服务器设置

当路由器作为 PPTP 服务器时，还需进入 VPN 用户管理界面设置用户账号。

**进入界面：网络 >>PPTP >> PPTP 服务器**


- 全局设置

| | |
|---|---|
| **PPTP 隧道维护时间间隔** | 设置 PPTP 隧道维护的时间间隔，范围是 60 秒至 1000 秒。设置此时间间隔，服务器按照设定间隔发出报文，用以确定 PPTP 隧道的连接状态。如无特别要求，请保持默认设置。 |
| **PPP 链路维护时间间隔** | 设置 PPTP 隧道里的 PPP 链路维护的时间间隔。范围是 0 秒至 120 秒，0 代表不发送。设置此时间间隔，服务器按照设定间隔发出报文，用以确定 PPP 链路的连接状态。如无特别要求，请保持默认设置。 |

- 服务器列表

点击<新增>，进行隧道设置。点击<确定>，使配置生效。


| | |
|---|---|
| **服务接口** | 请选择绑定的接口。当前用户仅对绑定的接口提供 PPTP 服务。 |
| **MPPE 加密** | 选择是否使用 MPPE 对 PPTP 隧道加密。 |
| **状态** | 选择启用或禁用本 PPTP 隧道。 |

## 8.7.2 PPTP 客户端设置

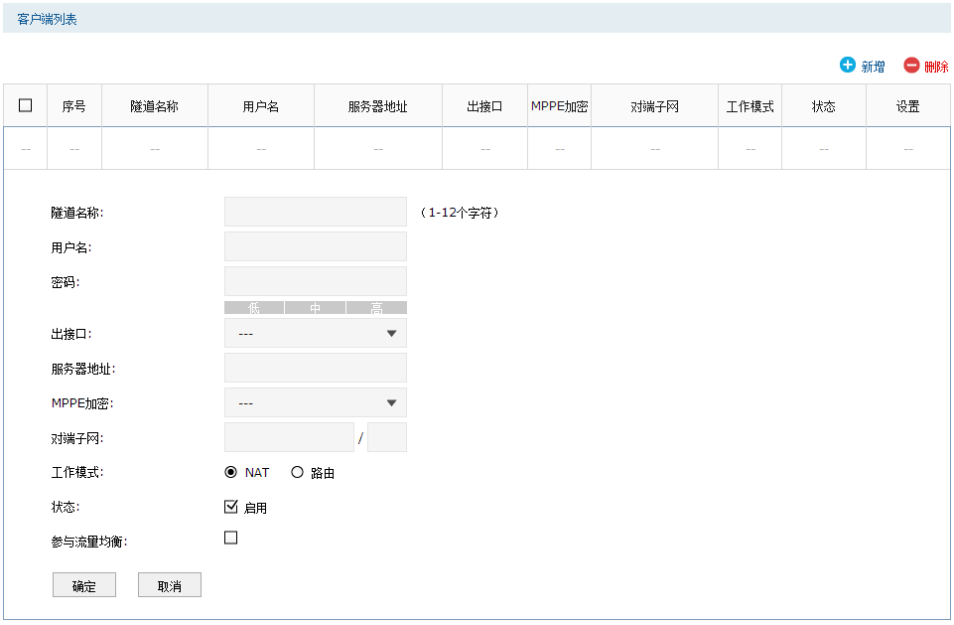
**进入界面：网络 >>PPTP >> PPTP 客户端**


- 全局设置

| | |
|---|---|
| **PPTP 隧道维护时间间隔** | 设置 PPTP 隧道维护的时间间隔，范围是 60 秒至 1000 秒。设置此时间间隔，服务器按照设定间隔发出报文，用以确定 PPTP 隧道的连接状态。如无特别要求，请保持默认设置。 |
| **PPP 链路维护时间间隔** | 设置 PPTP 隧道里的 PPP 链路维护的时间间隔。范围是 0 秒至 120 秒，0 代表不发送。设置此时间间隔，服务器按照设定间隔发出报文，用以确定 PPP 链路的连接状态。如无特别要求，请保持默认设置。 |

- 客户端列表

点击<新增>，进行隧道设置。点击<确定>，使配置生效。




| | |
|---|---|
| **隧道名称** | 设置隧道名称。 |
| **用户名** | 设置 PPTP 认证时客户端使用的用户名。客户端与服务器的设置需保持一致。 |
| **密码** | 设置 PPTP 认证时客户端使用的密码。客户端与服务器的设置需保持一致。 |
| **服务器地址** | 设置对端服务器地址。 |
| **出接口** | 服务器端路由器 WAN 端口上出链路接口。如有多条上网链路，请根据实际情况，选择其中一条链路承载 PPTP VPN 隧道。 |
| **MPPE 加密** | 选择是否使用 MPPE 对 PPTP 隧道加密。 |
| **对端子网** | 设置 PPTP 隧道对端局域网所使用的 IP 地址范围（一般可以填 VPN 隧道对端设备的 LAN 口 IP 地址范围），由 IP 和子网掩码组成。 |
| **工作模式** | 选择 NAT 模式或路由模式。 |
| **状态** | 选择启用或禁用本 PPTP 隧道。 |
| **参与流量均衡** | 选择是否参与流量均衡。 |

### 8.7.3 PPTP 服务器隧道信息

在此将列出路由器上所有 PPTP 隧道的相关信息。

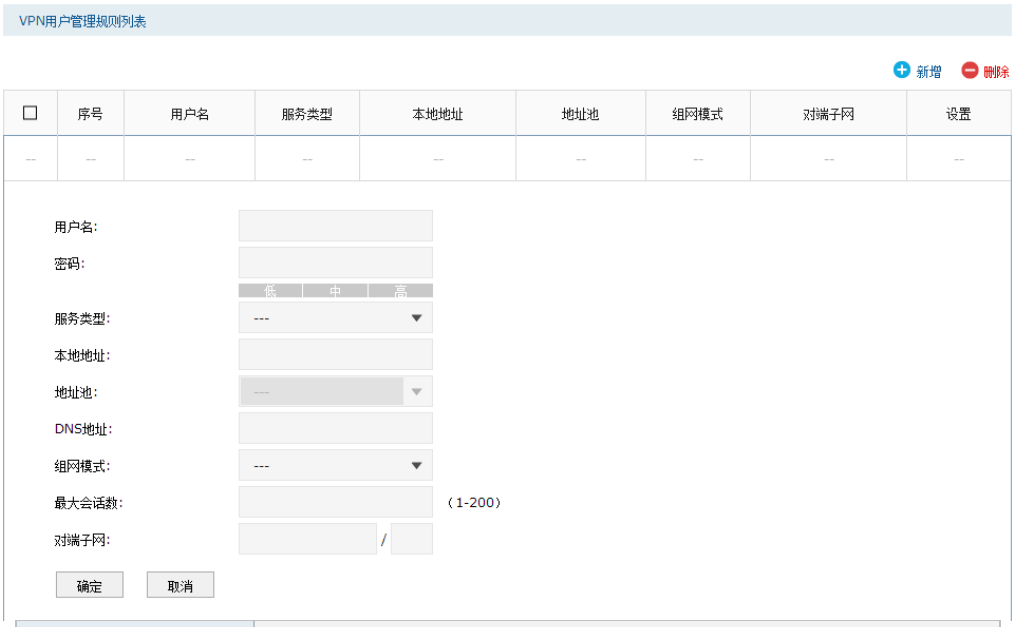
**进入界面：VPN >> PPTP >> 隧道信息列表**


点击<刷新>，获取最新的隧道信息列表。

## 8.8 VPN 用户管理

**进入界面：网络 >> VPN 用户管理**

当防火墙作为 L2TP 服务器或 PPTP 服务器时，需创建用户账号。点击<新增>，进行账号设置。点击<确定>，使配置生效。




| | |
|---|---|
| **用户名** | 设置认证时客户端使用的用户名。客户端与服务器的设置需保持一致。 |
| **密码** | 设置认证时客户端使用的密码。客户端与服务器的设置需保持一致。 |
| **服务类型** | 可选择 L2TP，PPTP 或自动。若选择自动，则该账号可根据客户端的配置自动适配相应的服务类型。 |
| **本地地址** | 设置隧道中本端使用的 IP 地址。 |
| **地址池** | 服务器分配给客户端的地址范围，由地址池名称所对应的 IP 地址范围确定。 |

| | |
|---|---|
| **DNS 地址** | 设置提供给客户端的 DNS 服务器的地址。如果需要客户端使用特定的 DNS 服务器，请进行设置。可以填入 0.0.0.0 表示任意地址。 |
| **组网模式** | 当远程接入用户为接入路由器的一个网段时，请选择“站点到站点”模式；<br>当远程接入用户是单个计算机时，请选择“PC 到站点”模式。 |
| **最大会话数** | 选择启用或禁用本 PPTP 隧道。 |
| **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<  >，可编辑默认规则的动作为允许或禁止，编辑其它规则条目的各项信息。

点击<  >，可批量删除用户管理规则。

## 8.9 DNS

广域网中，许多 ISP 使用 DHCP 分配公共 IP 地址，因此用户端获得的公网 IP 是不固定的。当其它用户需要访问此类 IP 动态变化的用户端时，很难实时获取它的最新 IP 地址。DDNS(Dynamic DNS，动态域名解析服务）服务器则为此类用户端提供了一个固定的域名，并将其与用户端最新的 IP 地址进行关联。当服务运行时，DDNS 用户端把最新的 IP 地址通知 DDNS 服务器，服务器会更新 DNS 数据库中域名与 IP 的映射关系。而对于访问它的用户端，将会得到正确的 IP 地址并成功访问服务端。DDNS 常用于 Web 服务器搭建个人网站、FTP 服务器提供文件共享等，访问的用户可以便捷地获取服务。

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。**TL-ER6225G 工业级**路由器提供花生壳动态 DNS 客户端、科迈动态 DNS 客户端和 3322 动态 DNS 客户端。

### 8.9.1 DNS 代理

**进入界面：网络 >> DNS >> DNS 代理**

可以通过本页面设置接口的 DNS 代理功能。

点击<  >，增加 DNS 代理规则。点击<确定>，使配置生效。


| | |
|---|---|
| **规则名称** | 输入规则名称。只能输入英文、数字和下划线。 |
| **服务接口** | 选择在哪些接口上面使用 DNS 代理功能。 |
| **出接口** | 指定转发的 DNS 请求报文发往哪一个接口上的 DNS server，如果选择的是 auto，路由器将提供一套默认规则来选择 server（当指定出接口时，请确认该接口有配置 DNS 地址）。 |

新增的条目会在 **DNS 代理规则列表**里显示出来，如下图所示。


点击  >，可编辑规则条目的各项信息。

点击  >，可批量删除 DNS 代理规则。

## 8.9.2 花生壳动态域名

**进入界面：网络 >> DNS >> 花生壳动态域名**

点击  >，增加花生壳动态域名规则。点击<确定>，使配置生效。


| | |
|---|---|
| **服务接口** | 选择登录花生壳动态域名服务器的接口。 |

| | |
|---|---|
| **用户名** | 填入在花生壳网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录花生壳网站进行注册。 |
| **密码** | 填入在花生壳网站注册该用户名时所设置的密码。 |
| **状态** | 勾选“启用”，则该条目生效；<br>不勾选“启用”，则该条目不生效。 |

点击<删除>，可批量删除 DNS 代理规则。

## 8.9.3 科迈动态域名

**进入界面：系统服务 >> 动态 DNS >> 科迈动态域名**

点击<新增>，增加科迈动态域名规则。点击<确定>，使配置生效。


| | |
|---|---|
| **服务接口** | 选择登录科迈动态域名服务器的接口。 |
| **用户名** | 填入在科迈网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录科迈网站进行注册。 |
| **密码** | 填入在科迈网站注册该用户名时所设置的密码。 |
| **状态** | 勾选“启用”，则该条目生效；<br>不勾选“启用”，则该条目不生效。 |

点击<删除>，可批量删除 DNS 代理规则。

## 8.9.4 3322 动态域名

**进入界面：系统服务 >> 动态 DNS >> 3322 动态域名**

点击<新增>，增加 3322 动态域名规则。点击<确定>，使配置生效。


| | |
|---|---|
| **服务接口** | 选择登录 3322 动态域名服务器的接口。 |
| **用户名** | 填入在 3322 网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录 3322 网站进行注册。 |
| **密码** | 填入在 3322 网站注册该用户名时所设置的密码。 |
| **域名信息** | 用户名绑定的域名信息。 |
| **状态** | 勾选“启用”，则该条目生效；<br>不勾选“启用”，则该条目不生效。 |

点击<删除>，可批量删除 DNS 代理规则。

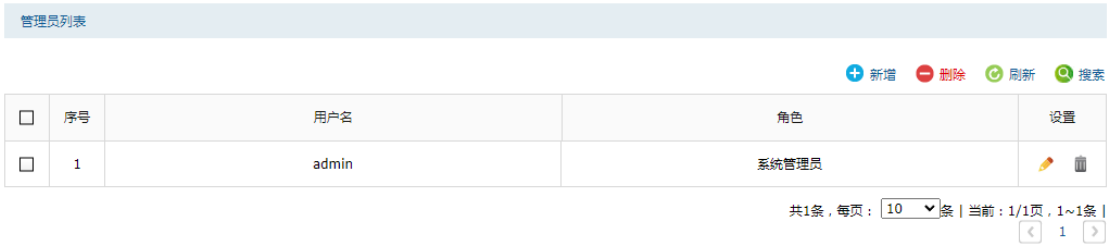
# 第9章 系统

## 9.1 管理员

### 9.1.1 管理员列表

您可以通过本页面来管理管理账户的用户名和密码。

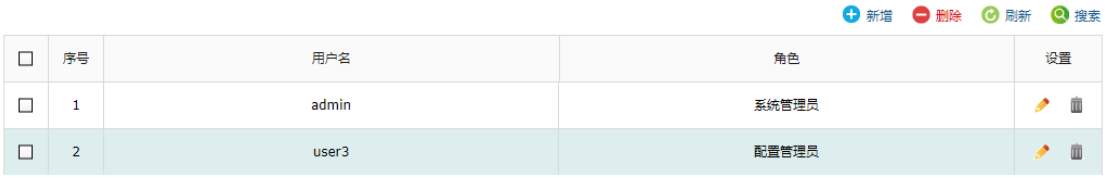
**进入界面：系统>> 管理员 >> 管理员**




点击<新增>按钮，进入管理员设置页面。设置新用户名和密码，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** | 您可以设置一个新的密码。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。 |
| **确认新密码** | 请您再输入一遍新设置的密码，来确认新密码。 |
| **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。 |

新增的条目会在**组列表**里显示出来，如下图所示。




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  ，可批量删除管理员条目。

点击  ，获取最新的管理员列表。

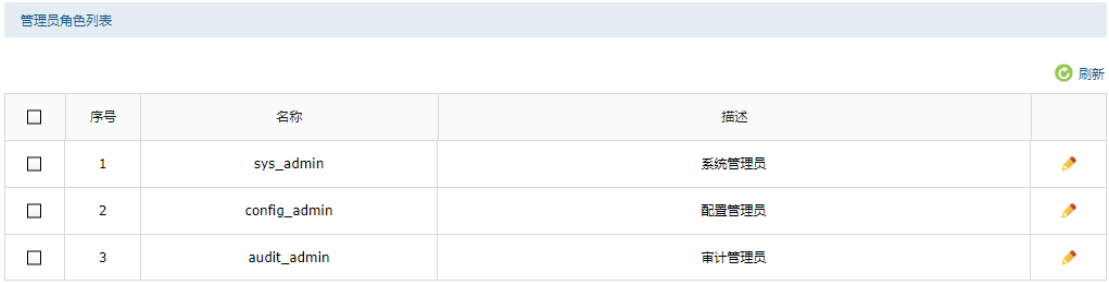
点击  ，可批量查找不同的应用组。


| | |
|---|---|
| **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;<br>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。 |

## 9.1.2 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。

**进入界面：系统>> 管理员 >> 管理角色**

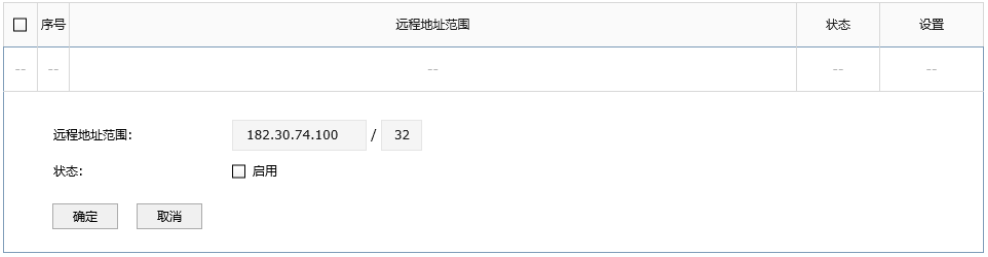



点击条目后的<>按钮查看权限划分。

## 9.1.3 远程管理

可以在远程管理界面对允许远程登录的 IP 地址范围进行设置和修改。

**进入界面：系统>> 管理员 >> 远程管理**




| | |
|---|---|
| **远程地址范围** | 设置需要从外部网络登录防火墙的主机地址，可指定单个 IP 或一个网段。 |
| **启用/禁用规则** | 选择启用或禁用该规则。 |

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，点击<>按钮启用条目，点击<>按钮禁用条目。

点击<删除>，可批量删除远程管理条目。

## 9.1.4 系统管理设置

可以在服务端口界面对Web、Telnet服务的端口进行设置和修改。

**进入界面：系统>> 管理员 >> 系统管理设置**


| | |
|---|---|
| **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。<br>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** | 当连续尝试登陆失败达到该次数时，将会在一段时间内锁定设备不允许继续登录。 |
| **登录锁定时长** | 当连续登陆失败次数达到最大登录尝试次数后，将会在锁定时长期间无法进行登录。 |

**应用举例**

某企业防火墙地址为210.10.10.50，为方便管理，希望广域网210.10.10.0/24网段的IP地址能对防火墙进行远程管理。

可以通过设置Web服务器实现此需求。首先需要设置远端访问防火墙的地址段，点击系统>>管理员>>远程管理，新增管理规则，并选择启用该访问规则，如下图所示：

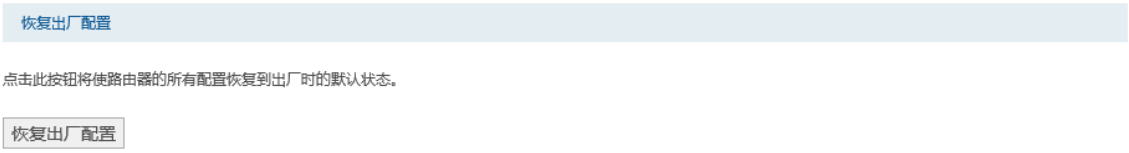

其次，在服务端口界面为Web服务器开放相应的服务端口，点击系统>>管理员>>系统管理设置，设置如下图所示：


在浏览器地址栏输入防火墙地址210.10.10.50登录防火墙Web界面。

# 9.2 设备管理

## 9.2.1 恢复出厂配置

**进入界面：系统>> 设备管理 >> 恢复出厂配置**




点击<恢复出厂配置>按钮，防火墙将会恢复所有设置的默认值。建议在网络配置错误、组网环境变更等情况时使用此功能。

防火墙出厂默认IP地址为192.168.1.1。

## 9.2.2 备份与导入配置

**进入界面：系统>> 设备管理 >> 备份与导入配置**


- 版本信息

显示当前防火墙软件版本。

- 备份配置信息

单击<备份>按钮，防火墙会将目前所有已保存配置导出为文件。建议在修改配置或升级软件前备份当前的配置信息。

- 导入配置信息

单击<浏览>按钮，选择已备份的配置文件；或者在文件路径输入框中填写完整的配置文件路径，然后点击<导入>按钮，将防火墙恢复到以前备份的配置状态。

**说明：**

- 备份及导入文件过程中请保持电源稳定，避免强行断电。
- 导入的配置文件版本与防火墙当前配置版本差距过大，将有可能导致防火墙现有配置信息丢失，如果有重要的配置信息，请谨慎操作。

## 9.2.3 重启设备

**进入界面：系统>> 设备管理 >> 重启设备**


单击<重启防火墙>按钮，防火墙将会重新启动。

重新启动不会丢失已保存的配置，在重启的过程中，网络连接将会暂时中断。

**说明：**

- 重启过程中请保持电源稳定，避免强行断电。

## 9.2.4 软件升级

**进入界面：系统工具 >> 设备管理 >> 软件升级**


TP-LINK官方网站（http://www.tp-link.com.cn）会不定期更新TL-FW5600的软件升级文件，可将升级文件下载保存在本地。登录防火墙后进入软件升级界面，单击<选择文件>按钮，选择保存路径下的升级文件，点击<升级>进行软件升级。

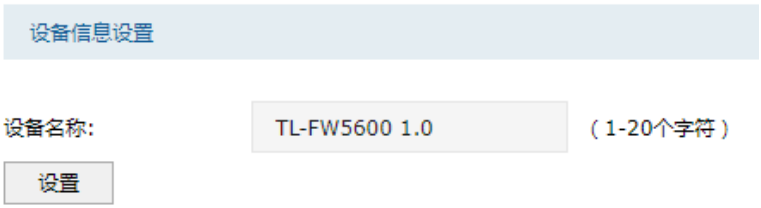
**说明：**

- 软件升级成功后防火墙将会自动重启，在防火墙重启完成前请保证电源稳定，避免强行断电。
- 软件升级后由于新旧版本软件的差异可能会恢复出厂默认配置，如有重要配置信息，请在升级前备份。

## 9.2.5 设备管理

**进入界面：系统>> 设备管理 >> 设备管理**

自定义设备名称，点击<设置>，使配置生效。




## 9.3 时间设置

时间设置界面允许对防火墙的系统时间进行设置。若时间设置发生改变，将会影响一些与其相关的功能，如防火墙规则的生效时间、PPPoE 定时拨号、日志等。

设置时间的方法分为两种：“通过网络获取系统时间”和“手动设置系统时间”。

**进入界面：系统工具 >> 时间设置 >> 时间设置**

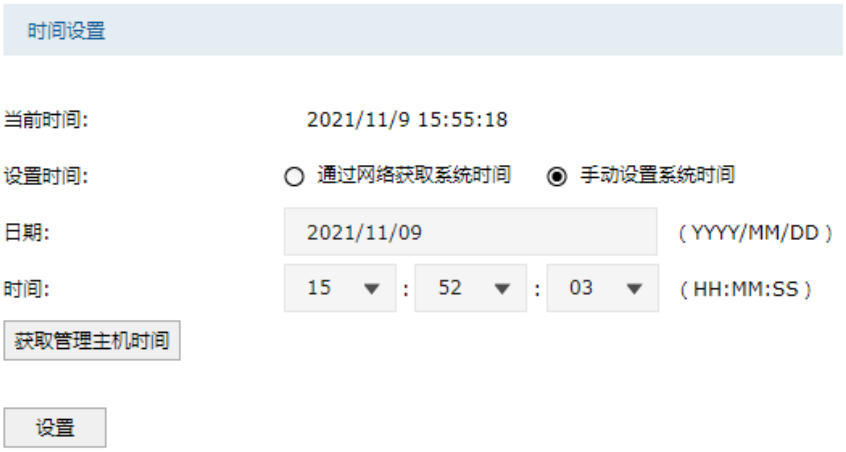
- 通过网络获取系统时间

若防火墙可以访问网络，可以选择<通过网络获取系统时间>，设置完毕后点击<设置>生效。


| | |
|---|---|
| **当前时间** | 显示目前系统时间。 |
| **设置时间** | 选择“通过网络获取系统时间”。 |
| **时区** | 选择时区。 |
| **首选/备选 NTP 服务器** | 选择“通过网络获取系统时间”后，防火墙将在内置 NTP（Network Time Protocol，网络校时协议）服务器地址列表中搜索可用地址，并获取时间。若获取失败，请手动设置 NTP 服务器地址，由于 NTP 服务器并非固定不变，推荐搜索两个不同的地址，分别填入首选、备用 NTP 服务器输入框，NTP 服务器地址可以为 IP 地址也可以为域名。设置完毕后点击<设置>按钮，防火墙会通过指定的 NTP 服务器获取网络时间。 |

- 手动设置系统时间

若防火墙暂时不能访问互联网，可以选择对系统时间进行手动设置设置完毕后点击<设置>生效。




| | |
|---|---|
| **当前时间** | 显示当前系统时间。 |
| **设置时间** | 选择“手动设置系统时间”。 |
| **日期** | 手动设置系统日期。 |
| **时间** | 手动设置系统时间。 |
| **获取管理主机时间** | 点击按钮可以获取当前主机的系统时间。 |

**说明：**

- 如果不能正常使用<获取管理主机时间>功能，请在主机的防火墙软件中增加一条 UDP 端口为 123 的例外条目。
- 断电重启后，断电之前设置的时间将失效，重新变为“通过网络获取时间”，如果未能连网获取时间，请手动设置系统时间。

## 9.4 日志配置

可以在日志界面查看防火墙系统事件的记录信息。

**进入界面：系统>>日志配置 >>日志配置**


日志配置部分可以对日志系统进行简单的配置。

勾选<选择系统日志等级>，选择日志等级可使日志列表中列出指定等级的日志记录

| | |
|---|---|
| **所有等级** | 日志列表中将列出所有等级的日志记录。 |
| **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。 |
| **一般错误** | 一般性的错误提示，橙色显示。 |
| **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。 |
| **通知信息** | 正常状态下的重要提示信息。 |
| **信息报告** | 一般性的提示信息。 |
| **调试信息** | 调试过程产生的信息。 |

勾选<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您查看特定模块的系统日志信息。

勾选<发送日志>，设置服务器地址，将日志发送到特定服务器。

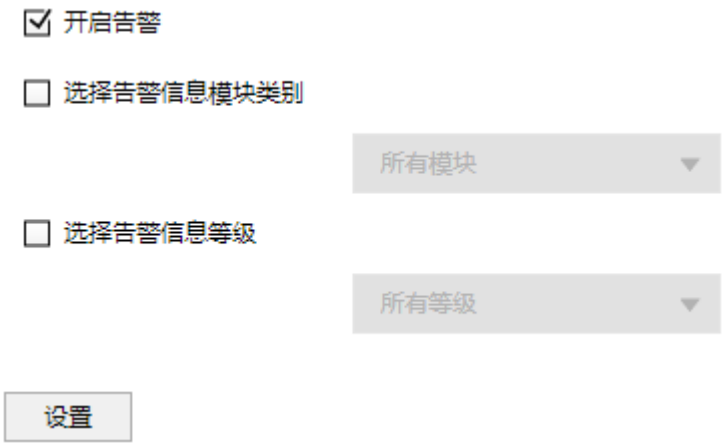
点击<设置>，使配置内容生效。

# 9.5 告警配置

## 9.5.1 事件配置

您可以通过本页面来配置设备告警功能。

**进入界面：系统 >> 告警配置 >>事件配置**




勾选<开启告警>，开启防火墙报警功能。

勾选<选择告警信息模块类别>，将弹出告警信息模块类别下拉框以供您查看特定模块的告警信息。

勾选<选择告警信息等级>，将弹出告警信息严重等级复选框以供您查看特定等级的告警信息。

点击<设置>，使配置内容生效。

| | |
|---|---|
| **所有等级** | 日志列表中将列出所有等级的日志记录。 |
| **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。 |
| **一般错误** | 一般性的错误提示，橙色显示。 |
| **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。 |
| **通知信息** | 正常状态下的重要提示信息。 |

| | |
|---|---|
| **信息报告** | 一般性的提示信息。 |
| **调试信息** | 调试过程产生的信息。 |

## 9.5.2 邮件配置

您可以通过本页面来配置设备告警功能。

**进入界面：系统>>告警配置 >> 邮件配置**


- 邮件服务器

勾选<开启邮件告警>，告警信息将会发送到相关邮箱。

| | |
|---|---|
| **服务器地址** | 指定邮件发送所使用的 SMTP 服务器。 |

| | |
|---|---|
| **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。 |

勾选<开启用户认证>，用于向 SMTP 服务器验证身份。

| | |
|---|---|
| **账号** | 指定认证账号名。 |
| **密码** | 指定认证账号对应的密码。 |

- 邮件内容

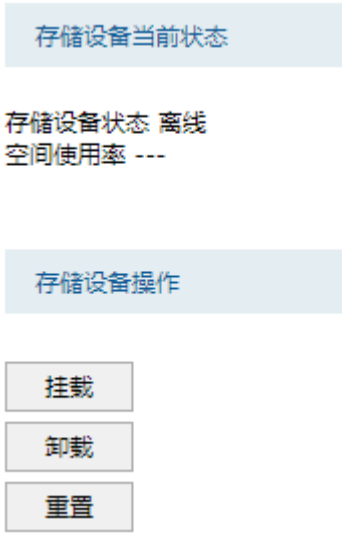
设置邮件主题和邮件发送间隔，点击<设置>保存配置。点击<发送测试邮件>，可测试配置信息是否正确。

# 9.6 存储管理

## 9.6.1 存储设备管理

您可以通过本页面来查看设备中的存储设备（硬盘/SD 卡）的状态并对其进行管理。

**进入界面：系统 >> 存储管理 >> 存储设备管理**




- 存储设备当前状态

可查看存储设备是否在线，和存储设备的空间使用比率。

- 存储设备操作

| | |
|---|---|
| **挂载** | 点击<挂载>按钮来进行存储设备挂载操作。 |
| **卸载** | 点击<卸载>按钮来进行存储设备卸载操作。 |
| **重置** | 点击<重置>按钮来进行存储设备重置操做，重置会清除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，此时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做的过程中，不要将设备断电，不要拔出存储器。

### 9.6.2 日志存储管理

**进入界面：系统>> 存储管理 >> 日志存储管理**

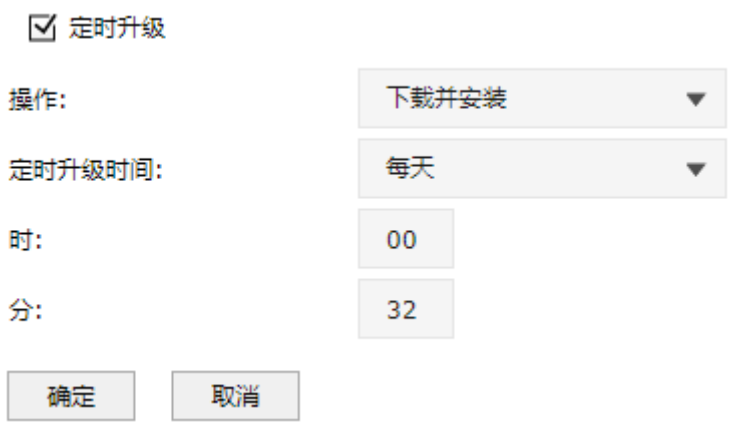
可查看存储设备当前状态。

## 9.7 升级中心

**进入界面：系统>> 升级中心 >> 升级中心列表**

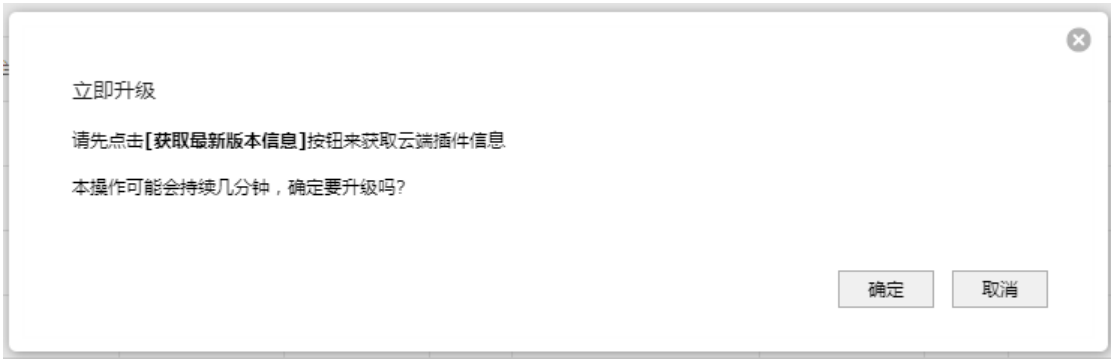

点击<获取最新版本信息>，点击后，会同步云端信息,获取当前最新的版本库信息，设置了自动升级，设备会在自动升级前，自动拉取云端信息

在定时升级时间条目下，点击已设置的升级时间例如< 每天00:32(下载并安装) >，可自定义升级时间。点击<确定>保存配置。




| | |
|---|---|
| **定时升级** | 勾选<定时升级>，开启定时升级功能，在特定时间升级特征库。 |
| **操作** | 选择下载并安装或仅安装特征库。 |
| **定时升级时间** | 设置定时升级重复的时间。 |
| **时** | 设置定时升级重复的时间。 |
| **分** | 设置定时升级重复的时间。 |

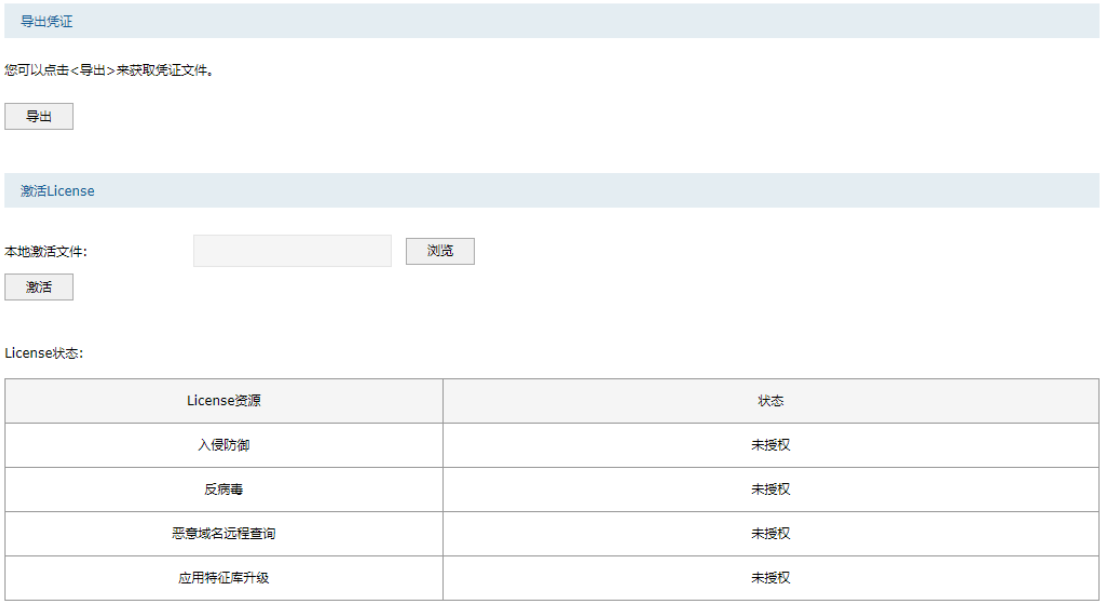
点击在线升级条目下的< >，在线升级前请线获取最新版本信息，点击<确定>保存配置。




点击<本地升级>，点击<浏览>上传特征库 bin 文件，点击<升级>完成本地升级。


## 9.8 License 管理

**进入界面：系统>> License管理 >> License管理**




| License资源 | 状态 |
| --- | --- |
| 入侵防御 | 未授权 |
| 反病毒 | 未授权 |
| 恶意域名远程查询 | 未授权 |
| 应用特征库升级 | 未授权 |

- 导出凭证

点击<导出>获取凭证文件。

- 激活 License

点击<浏览>上传本地激活文件，点击<激活>文件。

## 9.9 高可靠性

### 9.9.1 主备倒换

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。

**进入界面：系统>> 高可靠性 >> 主备倒换**


- 主备倒换设置

主备机器通过心跳接口进行通信，为保证主备倒换功能正常进行，请保证心跳接口的连通性。

选择<心跳接口>，设置主备倒换设置状态为<启用>还是<禁用>，点击<设置>使配置生效。

**说明：**

- 接口的具体信息请到 接口设置 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 >，新增主备规则列表。


| | |
|---|---|
| **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。<br>非抢占：主设备从挂掉到恢复，不再将服务抢占过来。<br>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。 |
| **状态** | 启用禁用主备倒换功能。 |

**说明：**

- 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

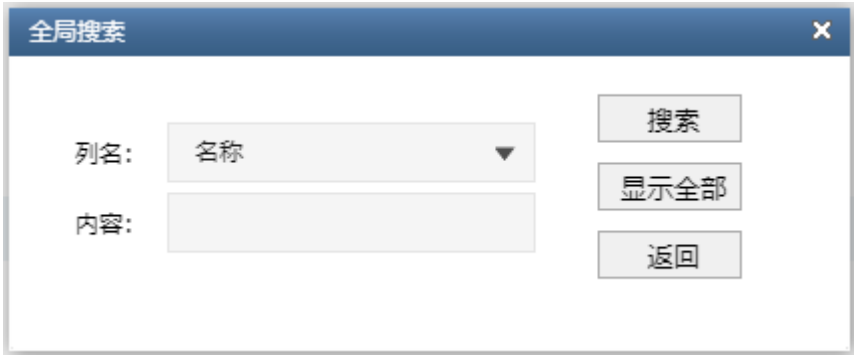
地址和 DNS 服务器，那么可以前往接口设置功能页面重新配置

点击<删除>，可批量删除主备规则。

点击<搜索>，可根据列名、内容和方式进行搜索。


| | |
|---|---|
| **列名** | 选择名称、虚拟 IP 地址等作为搜索关键列。 |
| **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；<br>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。 |

点击<日志搜索>，可搜索不同列名和自定义内容的地址组信息。




| | |
|---|---|
| **列名** | 选择名称、虚拟 IP 地址等作为搜索关键列。 |
| **内容** | 输入搜索关键内容，该内容需与列名相关。 |

| | |
|---|---|
| **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。 |

## 9.9.2 在线检测

您可以通过本页面设置不同的检测方式，并查看设备接口是否已经连接外网。

**进入界面：系统>> 高可靠性 >> 在线检测**


点击< >，设置端口检测模式，点击<确定>，保存配置。


| | |
|---|---|
| **接口名** | 需要检测的端口名称。 |
| **检测模式** | 选择检测外网连接状态模式。<br>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；<br>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；<br>永远在线：不进行检测，而在页面上永远显示为在线状态。 |

| | |
|---|---|
| **PING 检测** | 手动检测模式下，指定一个 IP 地址，让对应的接口去 ping 这个地址，从而判断是否连接外网，只能在手动模式下设置。 |
| **DNS 检测** | 手动检测模式下，指定一个 DNS 服务器的 IP 地址，让对应的接口通过这个 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，只能在手动模式下中设置。 |

# 9.10 系统参数

您可以通过本页面设置逻辑接口的路由Metric信息。

**进入界面：系统>> 系统参数 >> Metric设置**


| | |
|---|---|
| **静态 IP 接口** | 填写静态拨号时的路由 Metric 信息。 |
| **DHCP 接口** | 填写动态拨号时的路由 Metric 信息。 |
| **PPPoE 接口** | 填写 PPPoE 拨号时的路由 Metric 信息。 |
| **L2TP 接口** | 填写 L2TP 拨号时的路由 Metric 信息。 |
| **PPTP 接口** | 填写 PPTP 拨号时的路由 Metric 信息。 |

# 第10章 附录 A 常见问题

**问题1：无法登录防火墙Web管理界面该如何处理?**

1) 观察指示灯的状态，检查相应端口线缆是否正常连接，同时确认端口没有被禁用，可以换另外一个物理端口登录防火墙。

2) 如果是通过本地计算机管理防火墙，请确保计算机IP地址与防火墙IP地址处于同一网段。

3) 通过Ping命令检查网络连接。通过“开始”→“运行”输入“cmd”命令，点击“确定”后，可以打开命令窗口。输入ping 127.0.0.1检查计算机的TCP/IP协议是否安装；输入ping 192.168.1.1（防火墙管理接口的IP地址，如果防火墙设有多个管理接口，也可以ping其它管理接口的IP地址）检查计算机与防火墙的连接是否正常。

4) 如果确认物理连接正常，但是还是无法管理，建议通过Console口管理防火墙，检查防火墙VLAN和管理IP相关配置信息。

5) 如果修改过防火墙的管理端口，则注意下次登录时需要以“http://管理IP:XX”的方式登录，XX为修改后的端口号，如http://192.168.1.1:8080。

6) 如果恢复出厂配置后仍然无法登录或开始一段时间能登录，但过一段时间后又不能登录，则可能是遭受了ARP欺骗，建议查找欺骗源、查杀病毒或或将其他所有网络设备移除，电脑单机接防火墙尝试。

**问题2：忘记防火墙用户名和密码怎么办?**

忘记用户名、密码时可以通过Reset键将防火墙恢复至出厂配置。需要注意的是：恢复出厂配置时防火墙原有配置信息将丢失。

恢复出厂配置操作方法：在防火墙通电的情况下，使用尖状物长按防火墙的Reset按键，直至系统指示灯快速闪烁时松开，防火墙将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为http://192.168.1.1，需重新设置用户名和密码。

**问题3：忘记防火墙管理IP或管理端口怎么办?**

出于对防火墙管理安全的考虑，在用户不知道防火墙管理IP或者端口的情况下，需要对防火墙进行管理，建议使用Reset键将防火墙恢复出厂设置。需要注意的是：恢复出厂配置时防火墙原有配置信息将丢失。

恢复出厂配置操作方法：在防火墙通电的情况下，使用尖状物按住防火墙的Reset键，等待2-5秒后，观察到系统指示灯快速闪烁1-2秒，松开按键，防火墙将自动恢复出厂设置并重启。防火墙出厂默认管理地址是http://192.168.1.1。

**问题4：防火墙某些功能设置需要填写子网掩码值划分地址范围，一般子网掩码都有哪些值?**

子网掩码是一个32位的二进制地址，以此来区别网络地址和主机地址。子网划分时，子网掩码不同，所得到的子网不同，每个子网能容纳的主机数目不同。

常用的子网掩码值有8（即A类网络的缺省子网掩码255.0.0.0）、16（即B类网络的缺省子网掩码255.255.0.0）、24（即C类网络的缺省子网掩码255.255.255.0）、32（即单个IP地址的缺省子网掩码255.255.255.255）。

**问题5：不能正常浏览管理界面**

**请通过以下方面进行检查：**

1. 页面显示异常，请升级或更换其他浏览器；
2. 窗口弹出被禁止，请降低浏览器安全设置等级。

# 第11章　附录 B 规格参数

| 参数项 | 参数内容 |
| --- | --- |
| 支持的标准和协议 | IEEE 802.3、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3x、IEEE 802.1x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、L2TP、PPTP、IPSec |
| 网络介质 | 10BASE-T：3类或以上UTP/STP（≤100m） |
| | 100BASE-TX：5类或以上UTP/STP（≤100m） |
| | 1000BASE-T：超5类或以上UTP/STP（≤100m） |
| LED指示 | PWR电源指示灯、SYS系统指示灯、Link/Act连接状态指示灯、Speed速率指示灯 |
| 电源输入 | 100-240V~ 50/60Hz |
| 工作温度 | 0ºC ~ 40ºC |
| 存储温度 | -40ºC ~ 70ºC |
| 工作湿度 | 10% ~ 90%RH 不凝结 |
| 存储湿度 | 5% ~ 90%RH 不凝结 |