安全隔离与信息交换系统

用户手册

AVCOMM恩创®

安全隔离与信息交换系统

用户手册

关于此用户手册

此用户手册旨在指导专业安装人员安装和配置安全隔离与信息交换系统。包括帮助避免意外发生问题的步骤。

注意:

只有合格且经过培训的人员才能对此产品进行安装、检查和维修。

免责声明

AVCOMM保留随时更改本手册或产品硬件的权利，恕不另行通知。此处提供的信息目的是为了保证其准确可靠。但是可能不会涵盖所有的细节和更改，也并未提供在安装、操作或维护过程中遇到的所有可能的意外情况。如需更多信息，或出现未完全包含在此手册中的特定问题，应将此提交给AVCOMM。用户有责任确定手册是否有任何针对添加的新信息和/或纠正可能的无意造成的技术或印刷错误进行的不定期更新和修订。AVCOMM对其被第三方使用不承担任何责任。

AVCOMM在线技术服务

在AVCOMM，您可以使用在线服务表来请求支持。提交的服务表保存在服务器上，供AVCOMM团队成员分配任务并监控您的服务状态。如遇任何困难，请随时发邮件至sales@n-tron.com.cn

目录

1. 前言 1

1.1 版权声明 1

1.2 手册内容 1

1.3 手册约定 1

2. 安装指南 2

2.1 环境要求 2

2.2 产品示意图 2

2.2.1 产品示意图 2

2.2.2 后面板示意图 2

2.2.3 LCM 液晶显示屏功能说明 3

2.3 网闸开机 3

2.4 配置管理 3

2.4.1 配置电脑IP 地址 4

2.4.2 管理浏览器配置 5

3. 系统概述 8

3.1产品概述 8

3.2系统架构 9

4. 系统管理篇 9

4.1 登录界面 9

4.2 帐号管理 11

4.2.1 系统参数设置 11

4.3 系统管理 12

4.3.1 运行控制 12

4.3.2 系统维护 13

4.3.3 系统时间 14

4.3.4 管理主机 14

4.3.5 网络配置 15

4.3.6 网络路由 17

4.3.7 DNS配置.....20
4.3.8 系统状态.....20
4.3.9 服务控制.....21
4.3.10 产品信息.....23
4.3.11 设备集中管理.....23
4.3.12 短信告警配置.....25
4.4 其他设置.....26
4.4.1 恢复出厂设置.....26
4.4.2 升级服务.....27
4.5 系统防护.....30
4.5.1 病毒库设置.....30
4.5.2 系统调试.....31
5. 应用功能篇.....32
5.1 链路聚合.....32
5.1.1 添加.....33
5.1.2 编辑.....34
5.1.3 删除.....34
5.2 负载均衡.....34
5.2.1 节点管理.....35
5.2.2 负载组管理.....35
5.2.3 功能配置.....36
5.3 其他设置.....37
5.3.1 入侵防御.....37
5.3.2 日志空间设置.....38
5.4 高可用功能.....39
5.5 数据交换.....40
5.5.1 FTP同步.....40
5.5.2 文件共享同步.....47
5.5.3 数据库同步.....56
5.6 路由映射.....62

5.6.1 对象管理 62
5.6.2 映射模式 64
5.6.3 网关模式 67
5.6.4 网桥模式 70
5.6.5 路由模式 72
5.7 视频网闸 74
5.7.1 视频互联 74
5.7.2 视频交换 77
5.7.3 视频流管理 79
5.8 工业网闸 81
5.8.1 对象管理 81
5.8.2 策略配置 83
5.9 组播策略 87
5.9.1 代理模式 87
5.9.2 透明代理 88
5.10 协议代理 88
5.10.1 TCP/UDP 代理 89
5.10.2 FTP 代理 94
5.10.3 数据库代理 95
5.11 文件交换 96
5.11.1 组织用户管理 96
5.11.2 AD 域信息管理 101
5.11.3 文件过滤 103
5.11.4 用户流量监控 104
5.11.5 文件存储策略 104
5.11.6 客户端访问管理 107
5.11.7 客户端参数设置 110
5.12 日志 110
5.13 文件审核管理 111
5.13.1 等待审核 111

5.13.2 审核已通过 112
5.13.3 审核未通过 112
5.14 认证管理 113
5.14.1 新增用户身份认证信息 113
5.14.2 用户登录认证 113
5.15 内网应用审计 113
5.15.1 用户登录日志 114
5.15.2 发送文件日志 114
5.15.3 接收文件日志 116
5.15.4 查杀病毒日志 118
5.16 外网应用审计 119
5.16.1 用户登录日志 119
5.16.2 发送文件日志 119
5.16.3 接收文件日志 120
5.16.4 查杀病毒日志 120
5.17 文件审计管理 120
5.17.1 删除日志 120
5.17.2 导出日志 121
5.17.3 导入日志 121
6. 日志管理 122
6.1 系统管理 122
6.1.1 日志下载 122
6.1.2 日志上传 122
6.1.3 日志删除 123
6.1.4 日志存储设置 123
6.2 内网日志 123
6.2.1 内网预警信息日志 124
6.2.2 内网FTP 同步日志 124
6.2.3 内网FTP 代理日志 125
6.2.4 内网链路日志 126

6.2.5 内网双机热备日志 126
6.2.6 内网数据库代理日志 127
6.2.7 内网工业网闸日志 127
6.2.8 文件共享同步日志 128
6.2.9 数据库同步日志 129
6.2.10 内网系统升级日志 129
6.2.11 系统管理员日志 129
6.2.12 内网短信警告日志 130
6.2.13 内网视频流管理日志 131
6.2.14 内网协议过滤日志 131
6.2.15 内网自动备份日志 131
6.2.16 音视频日志 132
6.3 外网日志 132
6.3.1 外网预警信息日志 132
6.3.2 外网FTP 同步日志 133
6.3.3 FTP 代理日志 133
6.3.4 外网链路日志 134
6.3.5 数据库代理日志 134
6.3.6 外网工业网闸日志 135
6.3.7 文件共享同步日志 135
6.3.8 外网系统升级日志 136
6.3.9 外网短信告警日志 136
6.3.10 外网协议过滤日志 137
7. 客户端用户篇 137
7.1 客户端安装 137
7.1.1 内网客户端下载 138
7.1.2 外网客户端下载 138
7.1.3 创建客户端桌面图标 138
7.2 客户端用户登录 139
7.3 客户端用户登出 141

7.4 客户端用户修改密码 141
7.5 设置客户端文件接收路径 142
7.6 开启自动下载功能 143
7.7 发送文件 143
7.7.1 选择接收用户 143
7.7.2选择发送文件 144
7.7.3 一对一发送文件 144
7.7.4 一对多发送文件 144
7.7.5 批量文件发送 145
7.7.6 文件夹发送 145
7.7.7 拖拽方式文件发送 146
7.8 接收文件 147
7.8.1 文件接收 147
7.8.2 文件/文件夹批量下载、另存为、删除 147
7.9 审核 148
7.9.1 文件待审核 148
7.9.2 审核通过 149
7.9.3 文件审核不通过 149
7.10客户端卸载 150
7.11 客户端升级 150

1. 前言

1.1 版权声明

本手册未经本公司书面许可，任何公司和个人不得将此文档中的任何部分公开、转载或以其他方式散发给第三方。否则，必将追究其法律责任。
由于产品版本升级或其它原因本手册内容会不定期进行更新，恕不另行通知。

1.2 手册内容

第一章 前言：该部分主要介绍产品版权声明和手册内容简介。
第二章 安装指南：该部分主要介绍网闸设备的外部接口、功能特性、性能参数，以及网闸的一些基本操作。第三章 系统概述：该部分主要介绍网闸的产品概述及系统架构。
第四章 系统管理篇：该部分主要介绍网闸相关基础功能的配置与说明。
第五章 应用功能篇：该部分主要介绍网闸相关应用功能的配置及使用说明。
第六章 日志管理篇：该部分主要介绍网闸运行情况的监测，网闸的操作应用日志，网闸使用状态的实时查看等功能的配置与说明。
第七章 客户端用户篇：该部分主要介绍文件交换客户端功能配置及使用说明。

1.3 手册约定

图形界面格式约定

文字叙述	替换符号	应用案例
按钮	边框+ 底纹	登录
菜单选项	『』	『用户管理』
下一步操作	→	『用户管理』→『用户设置』
下拉框、单选框、复选框选项	[ ]	[网卡]
窗口名	【】	【新建用户】
提示信息	””	”超过 30 分钟无任何操作，请重新登录”

注 1：本文中所有图例均为屏幕截取；
注 2：Web 界面中所有需要输入的 IP，其格式均为：点分十进制形式（*.*.*.*）；

2. 安装指南

本章节主要介绍产品的构成及安装，硬件正确安装后可进行配置与调试。

2.1 环境要求

网闸可在如下的环境中使用：

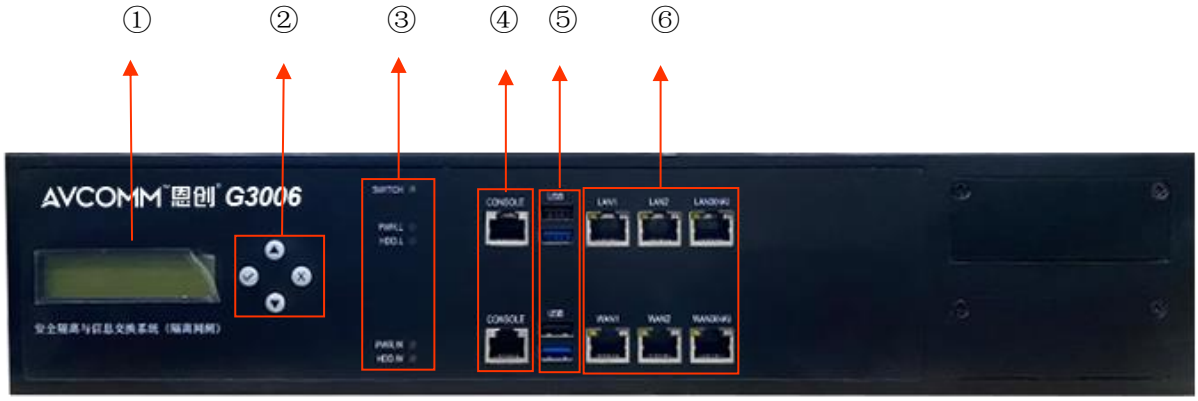
1. 输入电压：100V~240V
2. 温度：0~50℃
3. 湿度：5%~95%无凝露

为保证网闸能长期稳定的运行，请保证电源有良好的接地措施，保证使用环境的温度和湿度。本网闸设计符合国家标准，网闸的安放、使用、报废请按照国家相关法律、法规的标准。

2.2 产品示意图

以下产品示意图均以G3006为例

2.2.1 产品示意图

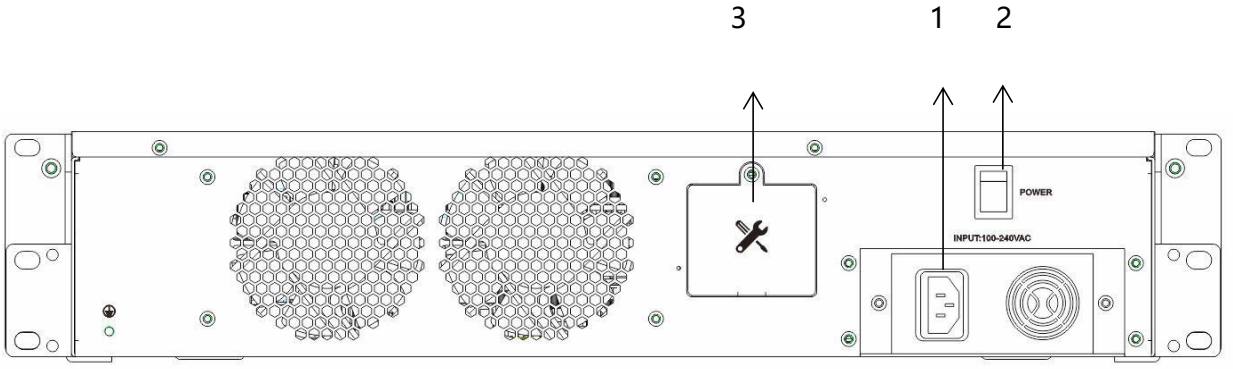


图示接口说明：

1. LCM 液晶显示屏
2. 按键：上键 下键 返回键 确定键
3. 指示灯
4. CONSOLE：内网调试串口
5. USB：USB 接口
6. LAN1-WLAN6(10/100/1000Mbps)：内网机：3个10/100/1000BASE-T接口（包含1个HA口），外网机：3个10/100/1000BASE-T接口（包含1个HA口）

▵**Tips：**串口仅供开发和测试调试使用，用户可通过网口接入网闸。

2.2.2 后面板示意图



后面版式图示接口说明：

1. 电源接口（市电，AC100V~240V）
2. 开/关机键
3. 维护窗口：内置一个内网VGA 接口（LAN），一个外网VGA 接口（WAN）

2.2.3 LCM 液晶显示屏功能说明

液晶显示功能菜单配置说明：

IP ADDRESS：查看内外网端机的 IP 地址和子网掩码

GAP STATUS：查看网闸内外端主机的资源使用情况

LOAD DEFAULT：恢复到出厂设置，并重新启动

CONNECT START：查看内外端机连接状况(是否连接成功)

SHUT DOWN：关机

REBOOT：重启

▵**Tips：**管理员可以通过操作按键，查看网闸内外网 IP 地址、CPU、内存、系列号等整机信息及应用程序加载情况；可操控整机复位、重启、恢复出厂等功能，并能在网闸出现问题时进行报警。

2.3 网闸开机

将电源适配器一端接入市电，一端插入网闸电源接口，轻按电源开关按键，此时前面板的POWER 指示灯长亮，说明网闸正常启动；SWITCH 指示灯闪烁 1-2 分钟后长亮，说明网闸内外网通讯正常工作。请准备两条标准的RJ45 以太网线，一条插入网闸的内网网口与内部网络相连，一条插入网闸的外网网口与外部网络相连。

▵**Tips：**网闸正常工作时，POWER 指示灯长亮，SWITCH 指示灯闪烁 1-2 分钟后长亮(若SWITCH 指示灯熄灭表示内外网通讯异常，请与我们联系)，HDD.W、HDD.L 指示灯在硬盘工作时会闪烁，网口指示灯在该网口接入网络时会闪烁。

需要关机时，按下电源旁边的关机按钮，关机后延迟 10 秒再拔出电源线。

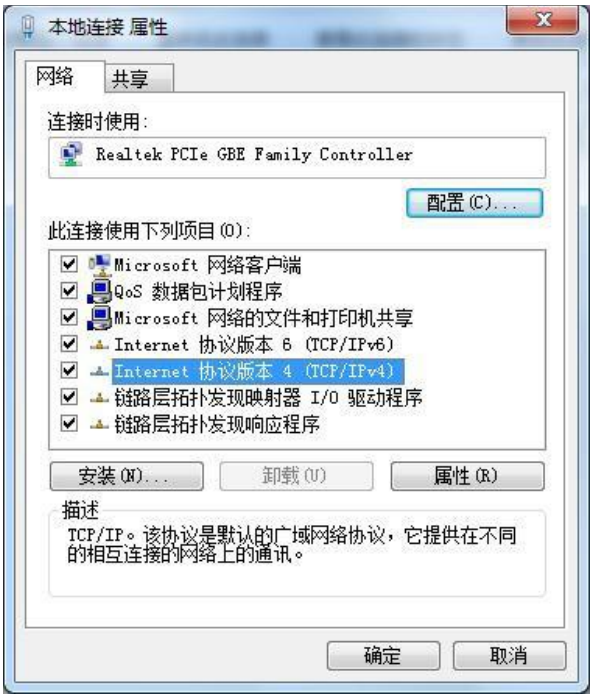
警告：本公司全系列产品均不可以强制断电。强制断电可能会导致数据丢失，或硬盘损坏、系统损坏等情况发生，建议采用正常方法关机。

2.4 配置管理

在配置网闸之前，需配备一台电脑且确定该电脑的 IE 浏览器（版本要求 IE9+或以上）或其他浏览器能正常使用，再给电脑配置一个与网闸同网段的 IP 地址，把电脑与网闸连接在同一局域网内，通过网络对网闸进行配置与管理。

2.4.1 配置电脑IP 地址

选择“本地连接”点击右键，选择[属性], 弹出本地连接属性设置界面→双击选择[Internet 协议版本（4 TCP/IPv4）]→点击高级→点击添加→输入与网闸同网段的IP 地址（如：192.168.1.2）、子网掩码（如：255.255.255.0）→点击添加,完成新建IP 地址。具体流程如下图所示：



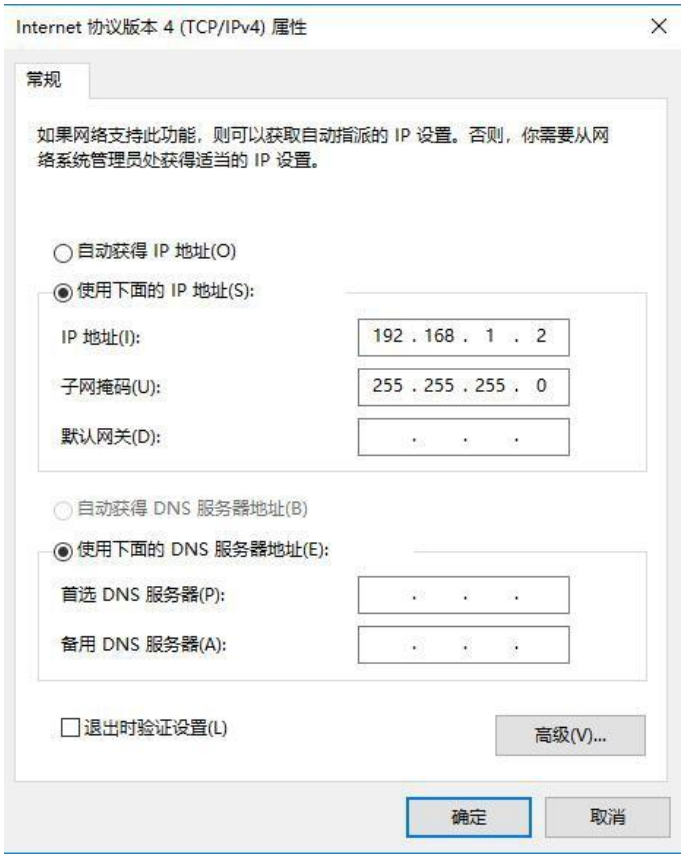


图 2.4.1-1 配置IP 地址流程示意图

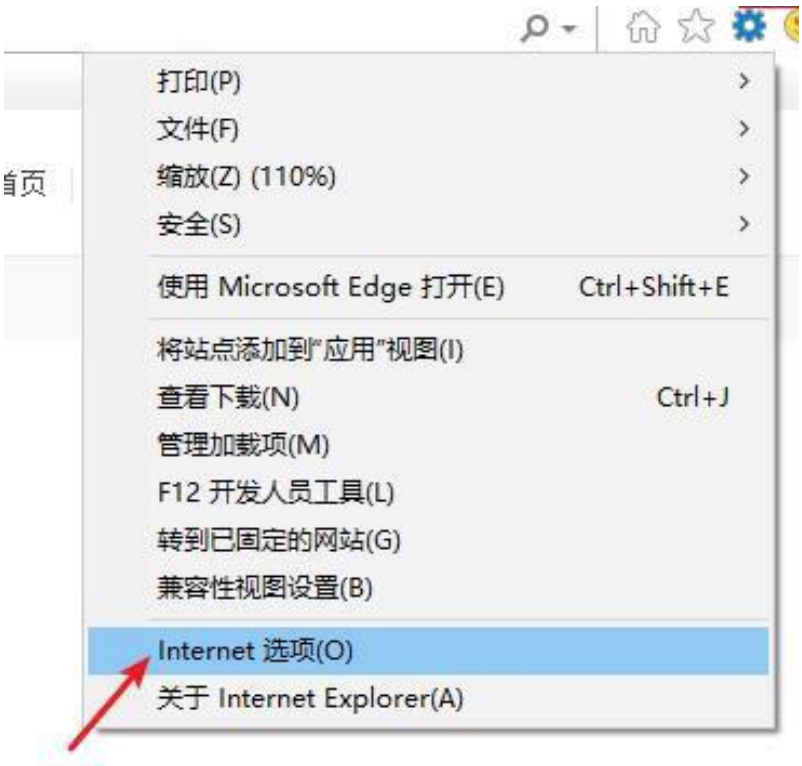
2.4.2 管理浏览器配置

登录网闸管理页面推荐使用 IE9 及以上版本（10,11）的浏览器，或者其他浏览器（谷歌浏览器、火狐浏览器）。

网闸管理页面登录之前，请先确保 PC 网络可以与网闸IP 通信，其次需要下载 USBKey 驱动并安装，以能够识别 USBKey 和登录管理界面。

由于USBKey 的驱动是私有签名证书，很多PC 下载安装不成功，以下是设置安装方法：

首先打开IE 浏览器，点击设置→Internet 选项

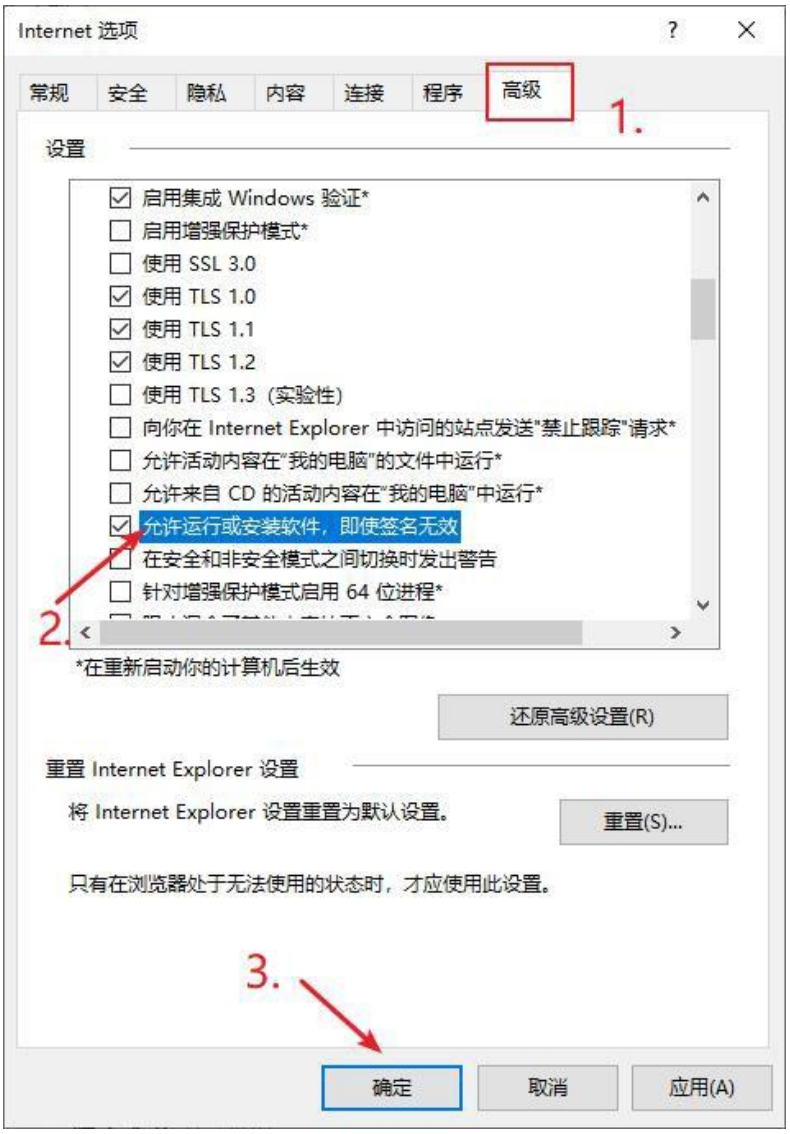

打印(P)
文件(F)
缩放(Z) (110%)
安全(S)
使用 Microsoft Edge 打开(E) Ctrl+Shift+E
将站点添加到"应用"视图(I)
查看下载(N) Ctrl+J
管理加载项(M)
F12 开发人员工具(L)
转到已固定的网站(G)
兼容性视图设置(B)
Internet 选项(O)
关于 Internet Explorer(A)

点击安全-自定义级别:


Internet 选项
1.
常规
安全
隐私
内容
连接
程序
高级
选择一个区域以查看或更改安全设置。
Internet
本地 Intranet
受信任的站点
受限制的站点
Internet
该区域适用于 Internet 网站，但不适用于在受信任和受限制区域中列出的网站。
站点(S)
该区域的安全级别(L)
自定义
自定义设置
- 要更改设置，请单击"自定义级别"
- 要使用推荐的设置，请单击"默认级别"
2.
启用保护模式(要求重新启动 Internet Explorer)(P)
自定义级别(C)...
默认级别(D)
将所有区域重置为默认级别(R)
确定
取消
应用(A)

找到『下载未签名的ActiveX 控件』，选择[提示]后点击确定：

再找到『高级』→勾选[允许运行或安装软件，即使签名无效]，点击确定：



修改完成之后，重启浏览器。输入网闸管理地址，内网：https://192.168.1.1，正常登陆时会提示下载驱动 SetUp.exe，安装完成后即可登录。

3. 系统概述

3.1产品概述

安全隔离与信息交换系统（简称“网闸”），是根据国内计算机网络的特有结构，利用国际上先进的技术手段，依靠自身的技术优势和安全体系结构方面的研究成果，成功开发出的一种快速、安全的网络物理隔离产品。该产品融入了完整的安全体系设计理念，采用国内独创的 DTP 物理隔离通道控制系统和嵌入式内核控制技术，以及多重安全措施，有效地防止了黑客攻击、病毒侵入和信息泄露等安全隐患，确保了内网与外网的可靠隔离和信息的可靠交换，是一种安全性极高的网络安全产品。

3.2系统架构

网闸根据实际应用需求，将网闸用户分为 3 个角色“安全保密员、安全审计员、系统管理员”。“安全保密员”主要是对网闸系统的一些应用功能进行配置与管理，对网闸用户及用户权限进行相关配置与管理；“系统管理员”对网闸运行情况的监测，详细记录网闸的操作日志，提供网闸使用状态的实时查看功能；“安全审计员”主要是对应用功能运行日志的记录。

4. 系统管理篇

在使用网闸之前，首先需要系统管理员对网闸进行相关功能的配置，用户才能正常使用网闸。系统管理员对网闸系统的一些应用功能进行配置与管理。功能包括『帐号管理』、『系统管理』、『其他设置』、『系统状态』、『关于我们』、『网络设置』、『路由映射』、『数据库同步』、『文件共享同步』、『FTP 同步』、『文件交换』、『TCP/UDP 代理』、『配置管理』、『视频网闸』、『工业网闸』、『组播代理』、『系统调试』等模块的配置与服务控制管理。

4.1 登录界面

选择与网闸在同一局域网内的电脑，按上述配置好电脑 IP→将网闸USB Key 插入电脑USB 接口中→再在网页浏览器（Internet Explore）中输入IP 地址https://192.168.1.1（默认IP，用户可自行配置，该 IP 对应网闸内网 LAN1 口）→轻按 Enter 键出现。如下图 5.1 所示安全提示窗口：

图 4.1-1 安全提示窗口

▵**Tips:** 网闸默认标配 5 个内网网口,可以使用内网所有网卡登录配置界面（具体网口开发数量以实物为准;如有LAN6 以及更多，IP 地址按照规律递增）。

1. LAN1 默认IP 地址：192.168.1.1
2. LAN2 默认IP 地址：192.168.2.1
3. LAN3 默认IP 地址：192.168.3.1
4. LAN4 默认IP 地址：192.168.4.1
5. LAN5 默认IP 地址：192.168.5.1

点击【继续浏览此网站（不推荐）】出现如下图所示登录界面:

图 4.1-2 系统登录界面

系统登录图示说明:

帐号：admin（系统管理员）、adminsafe（安全保密员），adminaudit（安全审计员）

密码：Admin123456（三个角色默认密码相同）

输入系统管理员用户名（admin）、密码（Admin123456）→点击登录，成功进入到系统状态界面。登录系统管理员账号后，可以看到菜单栏包含以下配置模块：『账号管理』、『系统管理』、『其他设置』、『系统防护』、『关于我们』，如下图所示:

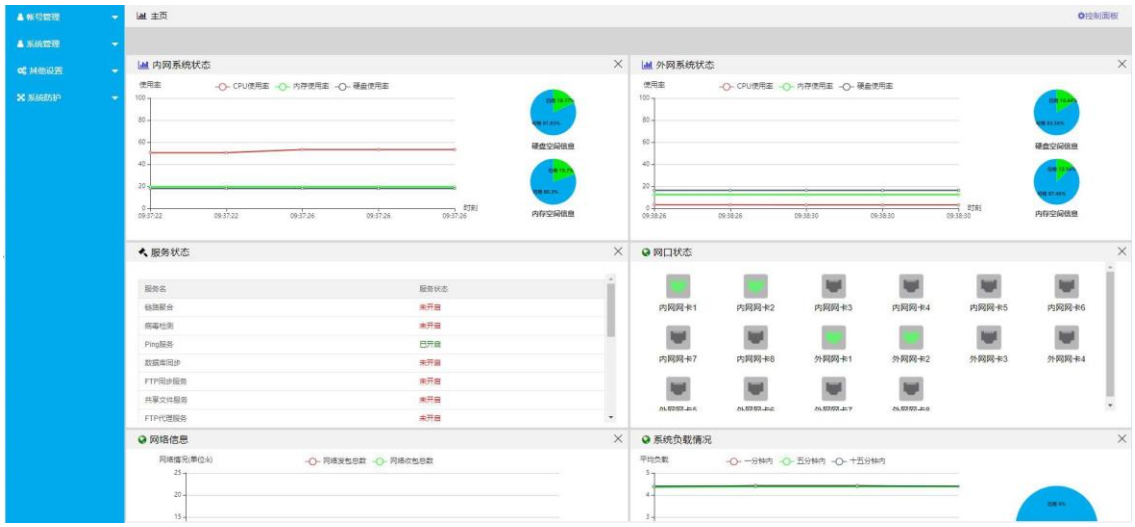


图 4.1-3 系统管理操作界面

系统管理操作界面图示说明：

内外网系统状态：展示实时的 CPU、内存、磁盘使用率

服务状态：展示当前服务控制中所有服务的开关状态

产品信息：展示产品名称、版本、设备型号、授权类型以及时间等信息

网口状态：展示内、外网所有网口的连接状态。亮绿色为已接连网线状态，灰色为未连接网线状态

网络信息：展示网络发包总数和网络收包总数

系统负载情况：展示交换内存使用情况

日志情况：展示系统日志信息情况

4.2 帐号管理

『帐号管理』主要用来对系统管理账号进行参数设置与管理，功能包含『系统参数设置』。

4.2.1 系统参数设置

对系统最大登录失败鉴别次数、系统定时锁定功能、系统超时重鉴别功能等功能进行管理设置。

系统管理操作界面→点击『帐号管理』→点击『系统参数设置』→根据需求合理设置密码过期时间、管理员及用户登录最大失败次数、页面登录超时设置等参数→点击保存→退出系统登录，参数设置在下次登陆时生效。如下图所示：

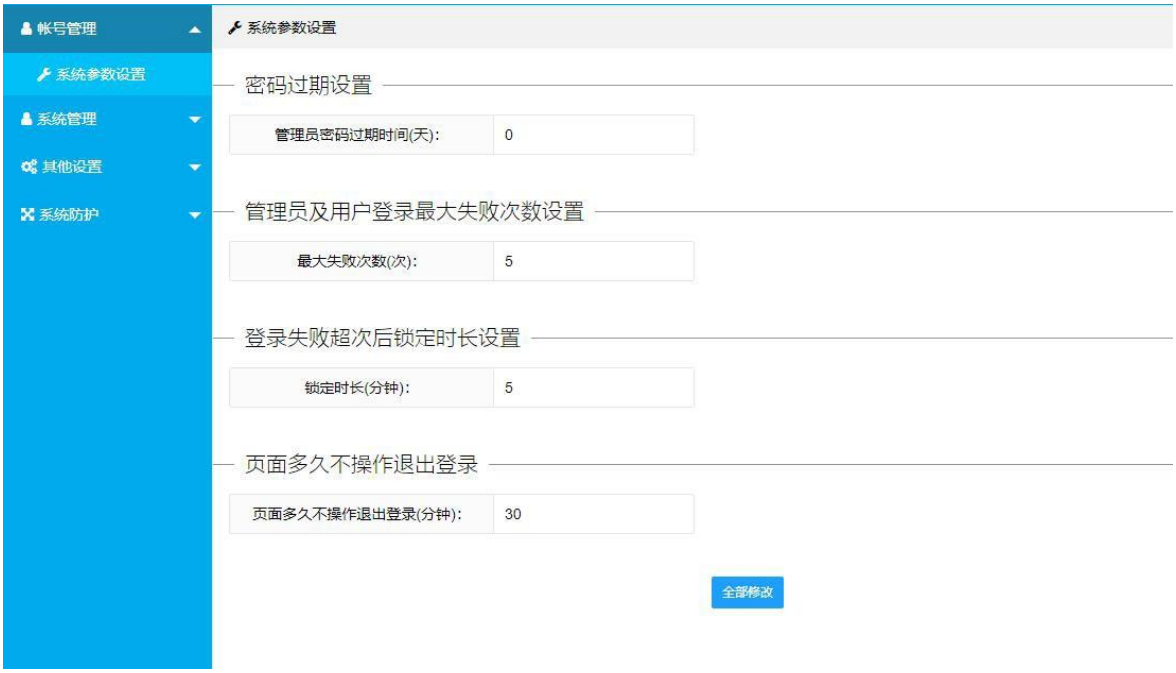


图 4.2.1-1 系统参数设置界面

系统参数图示说明：

密码过期设置：管理员密码周期超过设置值后，密码会过期，需设置新的密码

管理员及用户登录最大失败次数设置：允许登录失败的次数（范围：1-5 次），超过设置值系统锁定账号锁定时长：系统锁定账号的时长

页面登录超时设置：页面不操作的时间超出设置值后，将自动退出登录

4.3 系统管理

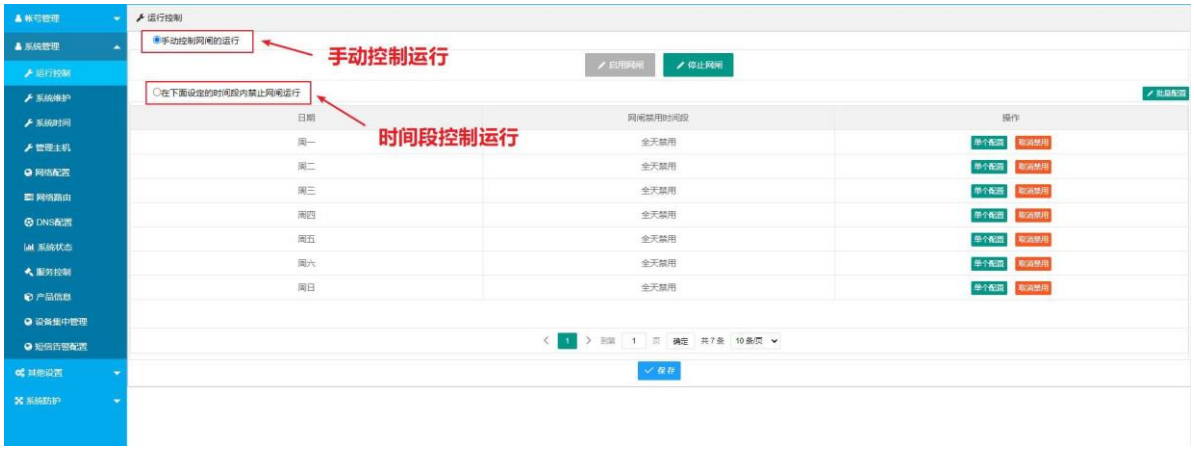
『系统管理』主要用来对网闸系统运行参数的配置管理，包含『运行控制』、『系统维护』、『系统时间』、『管理主机』、『网络配置』、『网络路由』、『DNS 配置』、『系统状态』、『服务控制』、『产品信息』、『设备集中管理』、『短信告警配置』等模块。

4.3.1 运行控制

『运行控制』主要用于设置与管理网闸的启用与停止、网闸的运行时间。包括【手动控制网闸运行】、【在下面设定的时间段内禁止网闸运行】。

系统管理操作界面→点击『系统管理』→点击『运行控制』进入到运行控制操作界面。如下图所示：

图 4.3.1-1 运行控制操作界面



运行控制配置参数说明：

1. 手动控制网闸运行：有“启用网闸”、“停止网闸”两个选项

- 启用网闸：启用网闸服务功能
- 停止网闸：网闸不提供任何应用服务，但管理员仍可通过程序对其进行管理

2. 在下面设定的时间段内禁止网闸运行：可点击批量配置、单个配置、取消禁用对网闸禁止运行时间段进行配置与管理

- 批量配置：周一到周日周期性设置网闸禁止时间段
- 单个配置：周一或周日单个设置网闸禁止时间段
- 取消禁止：取消限制时间段

4.3.2 系统维护

『系统维护』提供用户在界面对网闸进行重启、系统切换的操作。

系统管理员操作界面→点击『系统管理』→点击『系统维护』，进入【系统维护】操作界面。如下图所示：

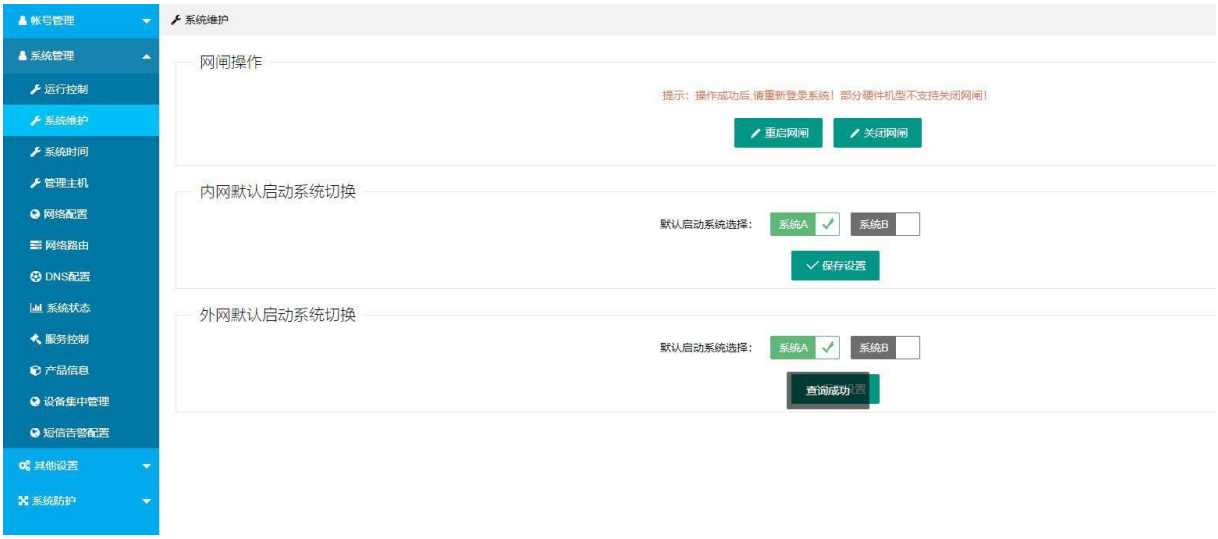


图 4.3.2-1 系统维护操作界面

系统维护操作界面图示说明：

网闸操作：点击重启网闸→弹出“是否要重启网闸？”提示窗口→点击确认，完成重启网闸操作。

内网默认启动系统切换：默认为系统 A，如需切换，点击系统 B→点击保存设置，

弹出“切换内网系统成功！”提示→手动重启网闸→完成内网启动系统切换。

外网默认启动系统切换：默认为系统 A，如需切换，点击系统 B→点击保存设置，

弹出“切换外网系统成功！”提示→手动重启网闸→完成外网启动系统切换。

4.3.3 系统时间

『系统时间』设置网闸的系统时间，包括[互联网时间]、[手动设置]。

系统管理操作界面→点击『系统管理』→点击『系统时间』进入到系统时间操作界面。如下图所示：

图 4.3.3-1 系统时间操作界面

系统时间支持两种设置方式：

[互联网时间]：网闸接入互联网，并配置 NTP 服务器地址，保存后即可自动与互联网时间同步。

[手动设置]：按照格式要求手动设置网闸系统时间→选择系统时间设置方式→[手动设置]→点保存设置，完成系统时间设置。

4.3.4 管理主机

『管理主机』功能是设置“网闸管理主机”的白名单。

系统管理操作界面→点击『系统管理』→点击『管理主机』进入到管理主机操作界面。如下图所示：

图 4.3.4-1 管理主机操作界面

管理主机配置参数说明：

内网中任意计算机均可管理网闸：内网中所有计算机均可管理网闸（系统默认配置）只允许以下IP 地址的客户机管理：仅列表内的计算机可管理网闸→通过点击新增主机、编辑主机、删除主机，对客户机进行配置与管理。

4.3.4.1 白名单

管理主机操作界面→勾选[只允许以下IP 地址的客户机管理]→点击新增主机，弹出添加主机窗口→输入内网中计算机的 IP、MAC 地址→点击确定→点击保存；完成管理主机白名单设置。如下图所示：

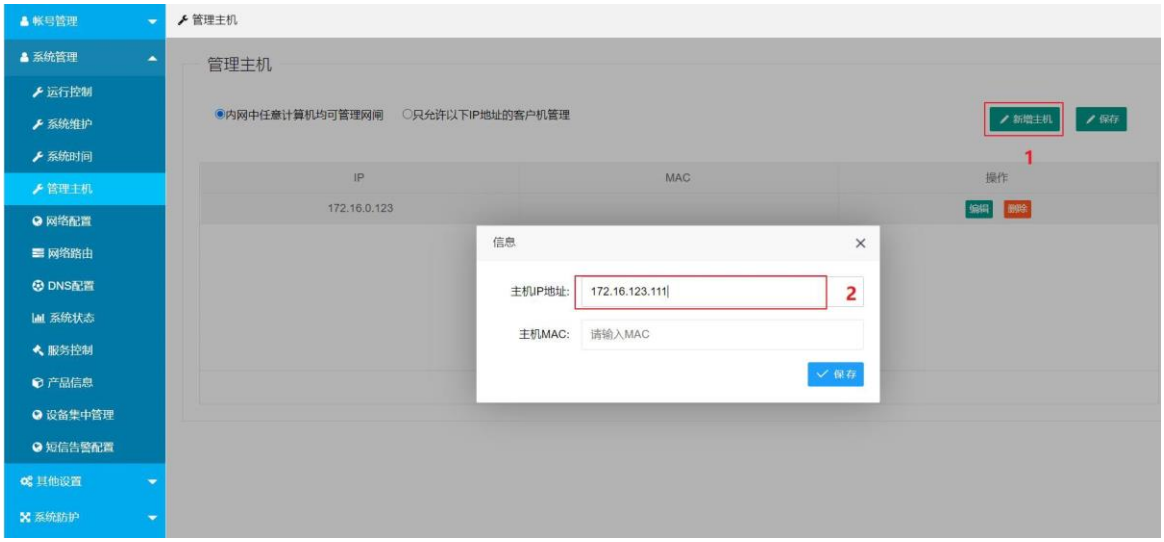


图 4.3.4_2 添加白名单主机操作界面

▵**Tips:** 当选择“只允许以下IP 地址的客户机管理”管理网闸时，请务必牢记配置的计算机IP 地址、MAC 地址信息！一旦忘记，很难再对网闸进行配置管理！跨交换机进行管理时 MAC 地址信息时交换机的 MAC 地址。

4.3.5 网络配置

『网络配置』对网闸的内外网网口参数进行设置，包含 IPV4 地址、IPV6 地址、子网掩码配置、MTU 值设置，以及网卡对应的 MAC 地址和运行状态显示。

4.3.5.1 网络地址

系统管理操作界面→点击『网络配置』，进入网口配置界面。如下图所示：

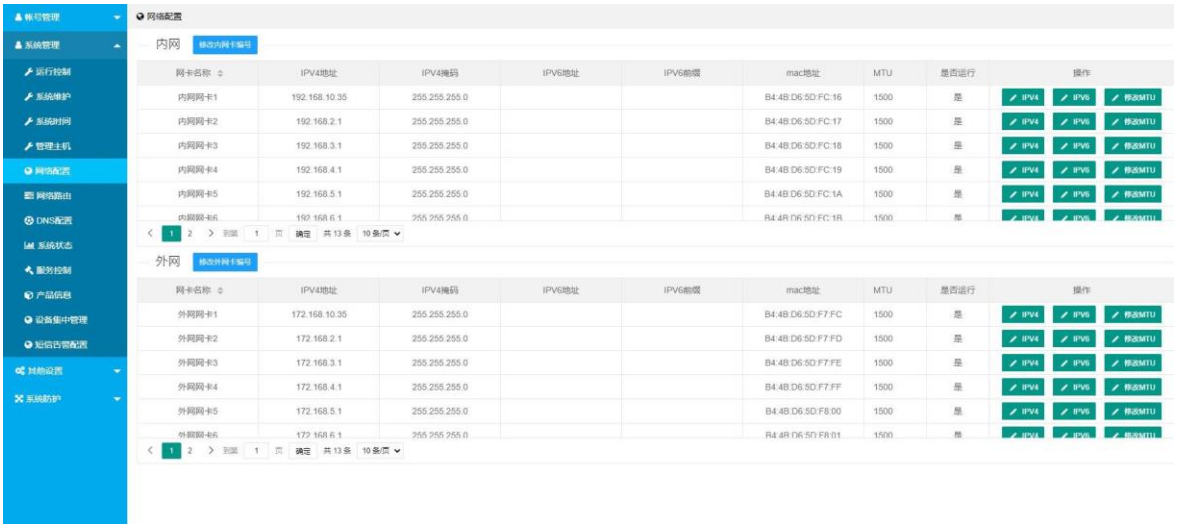


图 4.3.5.1-1 内网网口配置操作界面

内网网口配置参数说明：

网卡名称：内网网卡 1 对应网闸内网网口 LAN1，网卡序列说明在添加网卡配置时自动生成IPV4 地址：网络协议中的 IPV4 地址（IP 地址具有唯一性，请勿设置相同IP）

IPV4 掩码：必须结合 IPV4 地址一起使用，用于划分网络

IPV6 地址：网络协议中的 IPV6 地址（IP 地址具有唯一性，请勿设置相同IP）

IPV6 前缀：必须结合 IPV6 地址一起使用，用于划分网络

修改 MTU：设置网卡MTU 值

修改内网网卡编号：修改内网扩展网卡编号

修改外网网卡编号：修改外网扩展网卡编号

△**Tips:**

A：网卡IP 必须为合法且未被使用的

B：IP 不能设置为 10.0.1.* 网段地址

C：网卡机器的IP 分配原则，各网卡IP 地址不能同一网段

D：根据多网卡机器网关分配原则，只能有一个默认网关

4.3.5.2 配置 IPV4 地址

内网网络配置操作界面→点击IPV4，输入正确的网卡 IP 和子网掩码→点击保存，完成修改网卡 IPV4 地址的操作。如需修改外网网卡配置，在【网络配置】界面，选择【外网网络配置】，其他操作步骤与内网一致。如下图所示：

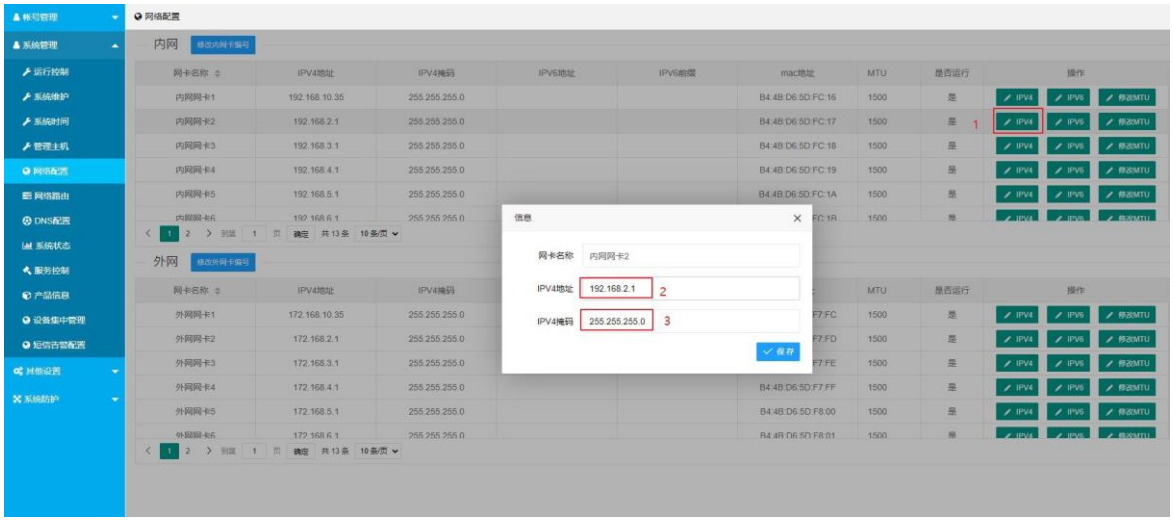


图 4.3.5.2-1 修改网卡 IPV4 地址对话框

4.3.5.3 配置 IPV6 地址

内网网络配置操作界面→点击IPV6，输入正确的网卡 IP 和子网掩码→点击保存，完成修改网卡 IPV6 地址的操作。如需修改外网网卡配置，在【网络配置】界面。选择【外网网络配置】，其他操作步骤与内网一致。如下图所示：

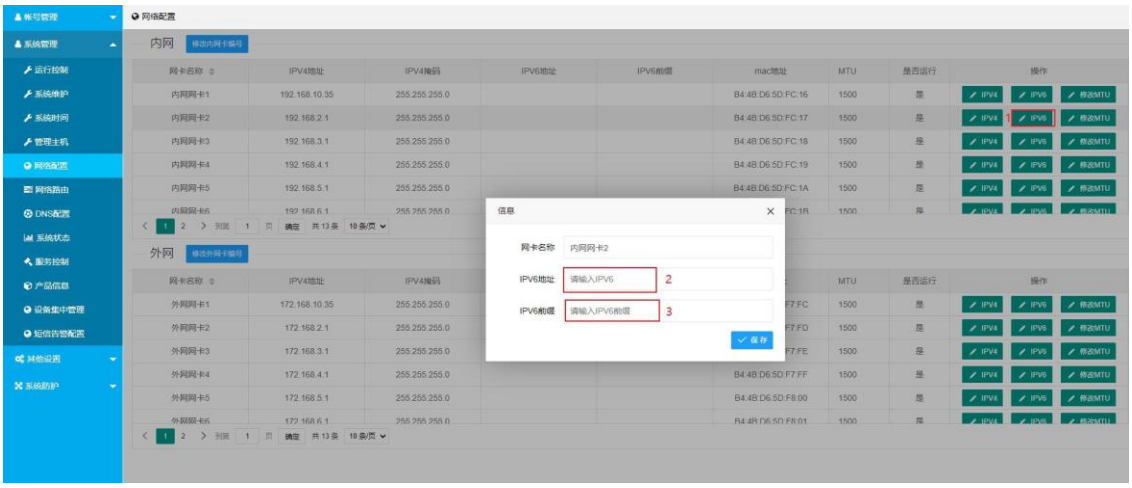


图 4.3.5.3-1 修改网卡 IPV6 地址对话框

4.3.6 网络路由

『网络路由』对网闸的内外网端的路由进行配置与管理，功能包括【内网路由设置】、【外网路由设置】，操作包括【添加】、【修改】、【删除】、【批量删除】。

系统管理操作界面→点击『网络路由』进入到网络路由配置操作界面。如下图所示：

图 4.3.6-1 网络路由配置操作界面

4.3.6.1添加

【网络路由】操作界面→默认选择[内网网络路由]配置界面→点击新增，弹出内网网络路由配置窗口。如下图所示：

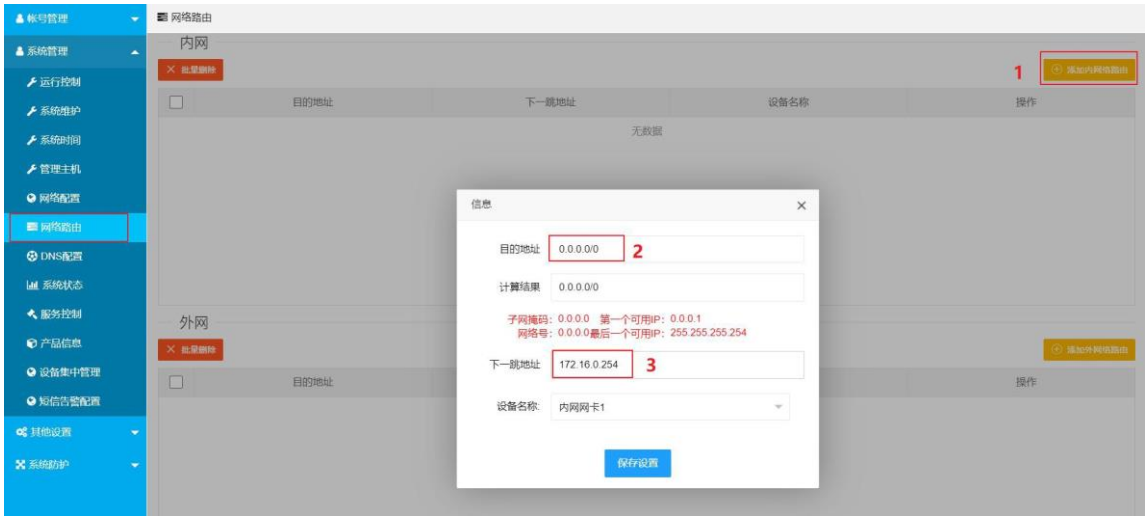


图 4.3.6.1-1 添加内网路由配置对话框

内网路由配置参数说明：

目的地址：目的服务器路由地址，可设置为一个IP 或一个IP 段

目的地址为IP：直接填写

目的地址为IP 段：填写IP 段的网络号加子网掩码。如：10.0.0.0/24

下一跳地址：下一跳路由地址

设备名称：网卡名称及编号

4.3.6.2 编辑

网络路由配置操作界面→选中需修改的内网路由→点击路由信息右侧的编辑按钮，弹出配置窗口（窗口与添加内网网络路由窗口一致）→输入目的地址、下一跳地址参数→选择[设备名称]→点击保存设置,完

成修改内网网络路由操作。如下图所示：

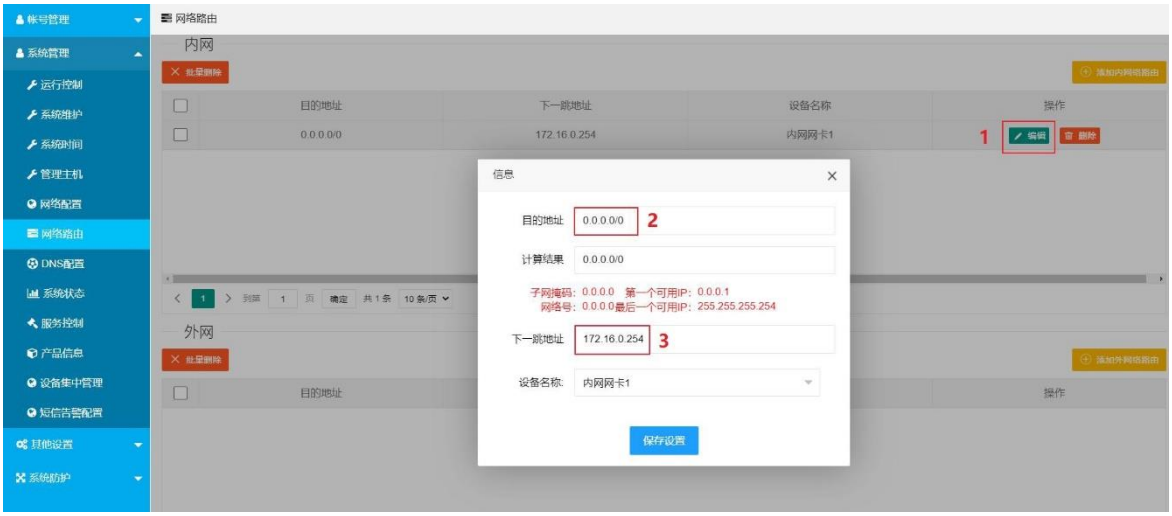


图 4.3.6.2-1 修改内网路由配置对话框

4.3.6.3 删除

网络路由配置操作界面→选中需删除的内网路由→点击路由信息右侧的删除，出现提示窗口→点击确定→完成删除内网路由操作。如下图所示：

图 4.3.6.3-1 删除内网路由提示窗口

4.3.6.4 批量删除

网络路由配置操作界面→选中需删除的内网路由→点击左上角批量删除，出现提示窗口→点击确定→执行配置生效操作，确定批量删除内网路由。如下图所示：

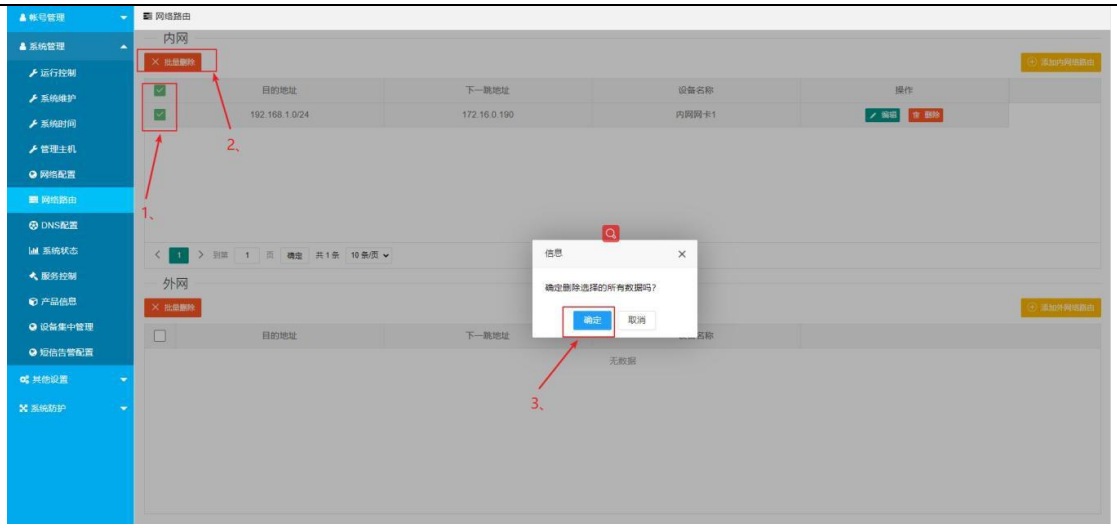


图 4.3.6.4-1 批量删除内网路由提示窗口

4.3.6.5 外网路由设置

『外网路由设置』主要用来对网闸的外网端路由进行配置与管理，目的地址可设置为一个IP 或一个IP 段，包括【添加】、【修改】、【删除】等操作。外网路由设置方法与内网路由设置一致，请参照内网路由设置，此处不再赘述。

4.3.7 DNS配置

『DNS 配置』主要用来对网闸的内外网端的 DNS 服务器进行配置，【DNS】和【备用DNS】配置。分别输入内外网DNS 地址，点击提交设置，完成DNS 配置操作。如下图所示：

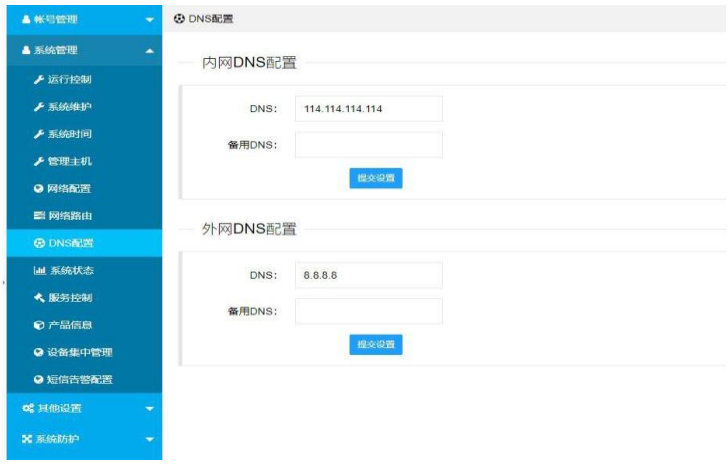


图 4.3.7-1 DNS 配置界面

4.3.8 系统状态

『系统状态』显示系统的『内网系统状态』、『外网系统状态』、『服务状态』、『产品信息』、『网口状态』、『网络信息』、『系统负载情况』、『日志情况』，如下图所示：

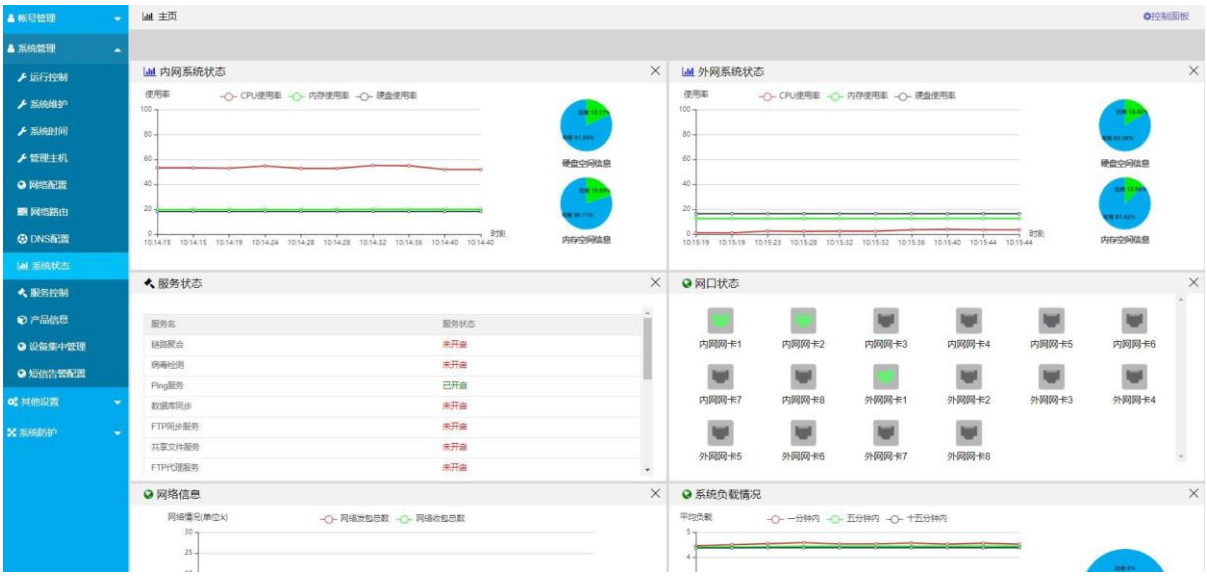


图 4.3.8-1 系统状态展示界面

系统状态参数说明：

内外网系统状态：展示实时的 CPU、内存、磁盘使用率

服务状态：展示当前服务控制中所有服务的开关状态

产品信息：展示产品名称、版本、设备型号、授权类型以及时间等信息

网口状态：展示内、外网所有网口的连接状态。亮绿色为已接连网线状态，灰色为未连接网线状态

网络信息：展示网络发包总数和网络收包总数

系统负载情况：展示交换内存使用情况

日志情况：展示系统日志信息情况

4.3.9 服务控制

为了提高网闸的使用性能，更好的为客户提供服务，系统提供服务的启用与禁用功能， 方便用户更好的使用各种应用。

『服务控制』包括【病毒检测】、【Ping 服务】、【设备集中管理】、【链路日志服务】、【工业网闸】、【视频网闸】、【视频流代理】、【音视频服务】、【数据库同步】、【FTP 同步】、【共享文件服务】、【路由映射服务】、【组播服务】、【TCP/UDP 代理】、【FTP 代理】、【数据库代理】、【新文件交换】等服务的启用与禁用功能。

系统管理操作界面→点击『系统管理』→点击『服务控制』进入服务控制操作界面→选择需启用/禁用的服务→点击服务开关，完成服务控制的启用、禁用操作。如下图所示：

图 4.3.9-1 服务控制操作界面

服务控制配置参数说明：

- 病毒检测：病毒服务功能的启用与禁用
- PING 服务: 管理PING 服务的启用与禁用
- 设备集中管理：管理设备集中管理服务的启用与禁用
- 链路日志服务：管理链路日志服务的启用与禁用
- 工业网闸: 管理工业网闸服务的启用与禁用
- 视频网闸：管理视频网闸服务的启用与禁用
- 视频流代理：管理视频流代理服务的启用与禁用
- 音视频服务：管理视频互联服务的启用与禁用
- 数据库同步：管理数据库同步的启用与禁用
- FTP 同步服务：管理FTP 同步服务的启用与禁用
- 共享文件服务：管理文件共享同步服务的启用与禁用
- 路由映射服务：管理路由映射服务的启用与禁用
- 组播服务：管理组播代理的启用与禁用
- TCP/UDP 代理：管理TCP/UDP 代理的启用与禁用
- FTP 代理：管理FTP 代理的启用与禁用
- 数据库代理：管理数据库代理的启用与禁用
- 新文件交换：管理新文件交换的启用与禁用

▵**Tips：**系统默认服务控制中 [ping 服务]为启用状态，其他服务均为禁用状态，需开启服务开关，该服务功能才可使用。

4.3.10 产品信息

『产品信息』展示产品序列号、版本以及授权等信息，并且提供导入授权接口，设备需要授权方可正常使用，如下图所示：

图 4.3.10-1 产品信息界面

授权导入

如有需要，请联系售后提供授权文件，获取到授权文件后拷贝到登录 WEB 页面的电脑中→进入产品信息，点击导入授权文件，选择授权文件并确定→页面提示“系统授权成功”后，网闸即可正常使用。如下图所示：

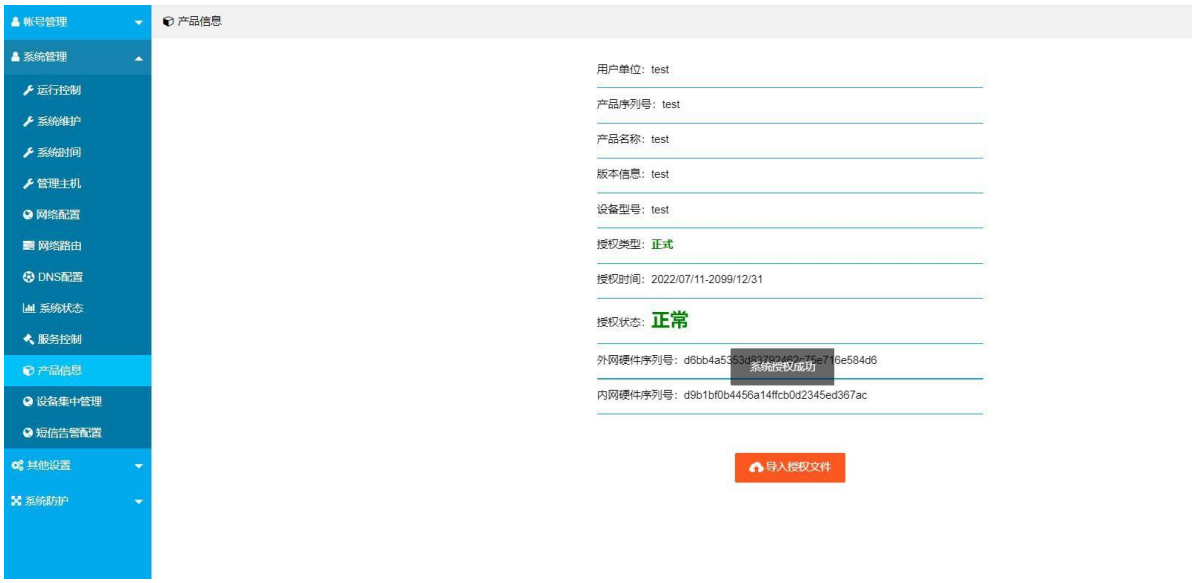


图 4.3.10-2 授权导入成功界面

4.3.11 设备集中管理

『设备集中管理』是以任意一台网闸作为主机，管理或者被管理以及监控其他设备当前系统状态的功能，主要有【设备系统状态】、【设备IP 号】、【设备控制】、【SNMP 配置】等信息展示，如下图所示：

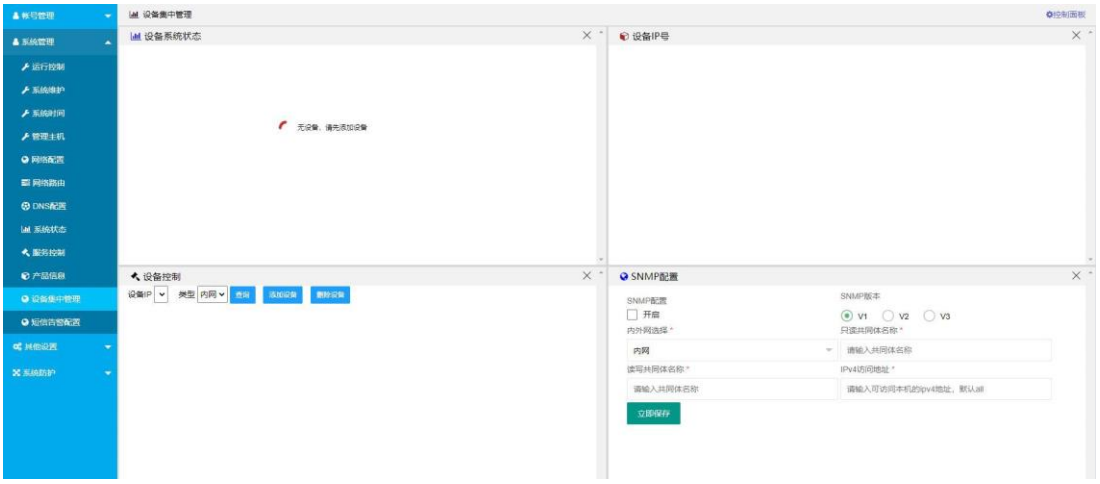


图 4.3.11-1 设备集中管理界面

4.3.11.1 设备控制

『设备控制』中，可以输入远程设备的 IP 地址，进行信息查询动作，还可以对远程设备进重启操作。点击添加设备按钮→添加设备IP→点击保存，再点击查询按钮，即可查询远程设备信息。如下图所示：

图 4.3.11.1-1 添加设备界面

4.3.11.2 SNMP 配置

『SNMP 配置』中，开启 SNMP 功能，可选版本有 V1、V2、V3，内外网配置相同。以内网配置为例：

1. V1 和V2 配置相同，分别自定义配置只读共同体名称、读写共同体名称、可访问本机的 IPV4 地址（不填默认为允许所有即 0.0.0.0）→点击立即保存，完成配置。如下图所示：

图 4.3.11.2-1 添加设备 V1V2 界面

2. V3 配置则需要配置安全用户名、认证方式（MD5\SHA）、认证密码、加密方式（DES\AES）、加密密码，管理主机需通过安全用户名认证、认证密码认证、加密密码认证管理网闸→点击立即保存，完成配置。如下图所示：

图 4.3.11_4 添加设备V3 界面

4.3.12 短信告警配置

『短信告警』是网闸出现磁盘预警信息时，通过短信通知管理员的功能。正确输入所有必填参数后→点击保存设置→出现提示：“短信告警配置设置成功”，完成短信告警操作。如下图所示：

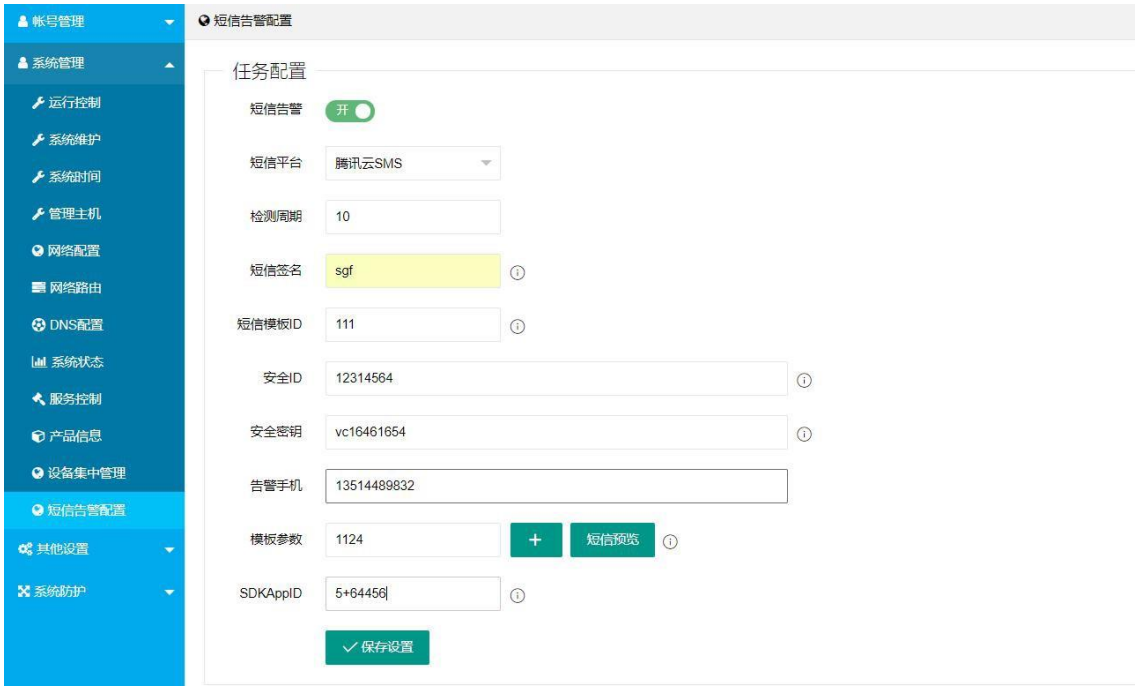


图 4.3.12 短信告警配置图

短信告警图示说明：

- 短信告警按钮：点击可开启、关闭短信告警
- 短信平台：有[腾讯云SMS]（默认）、[阿里云SMS]
- 检测周期：短信告警的检测周期
- 短信签名：可在短信控制台【国内消息-签名管理】添加，且填写的必须是已通过审核的短信签名
- 短信模板ID：短信控制台【国内消息-模板管理】添加，且填写的必须是已通过审核的模板ID
- 安全ID：用于识别API 调用者身份，前往【用户信息管理-安全信息管理】获取
- 安全密钥：用于加密签名字符串和服务器端验证签名字符串的密钥，可前往【用户信息管理-安全信息管理】获取
- 告警手机：接收告警短信手机号。最多保存 5 个号码，多个号码用英文“,”隔开
- 模板参数：+点击可添加模板参数；短信预览点击可预览短信

4.4 其他设置

4.4.1 恢复出厂设置

▵**Tips**：恢复出厂设置成功后，需要重新登录系统。 执行恢复出厂设置操作，网闸所有配置均恢复为出厂配置，请勿轻易执行此操作！

系统管理操作界面→点击『其他配置』→点击『恢复出厂设置』，进入恢复出厂设置操作界面。如下图所示：

图 4.4.1-1 恢复出厂设置操作界面

出厂设置操作界面→点击恢复出厂设置，出现提示窗口→点击恢复出厂设置，将网闸恢复出厂设置。如下图所示：

图 4.4.1-2 恢复出厂设置提示窗口

4.4.2 升级服务

4.4.2.1 系统更新

由于网闸的功能会根据实际应用的需要做一些调整，因此可能需要对服务器上的程序进行升级。为方便管理员操作，系统为其提供专门的系统功能。

系统管理操作界面→点击『其他设置』→点击『升级服务』进入到系统升级操作界面→点击选择文件即可自动上传，如下图所示：

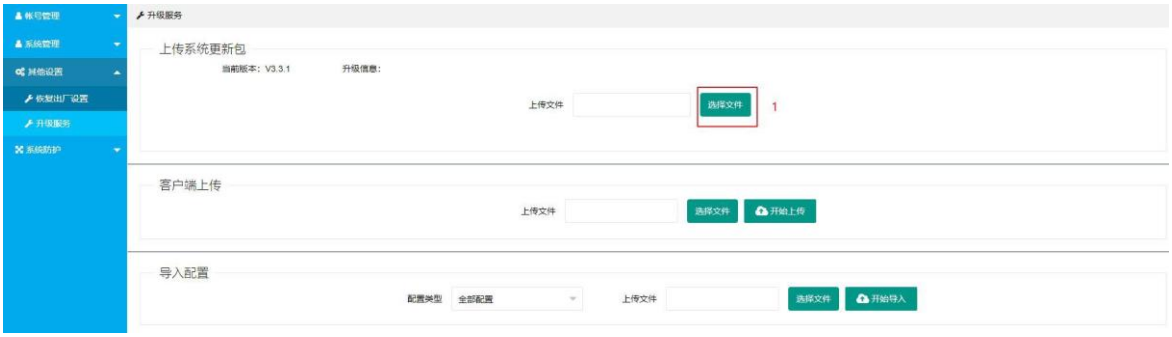


图 4.4.2.1-1 升级服务操作界面

4.4.2.2 客户端上传

上传最新的文件交换客户端安装包目前只支持后缀名为*.zip 文件，如下图所示：

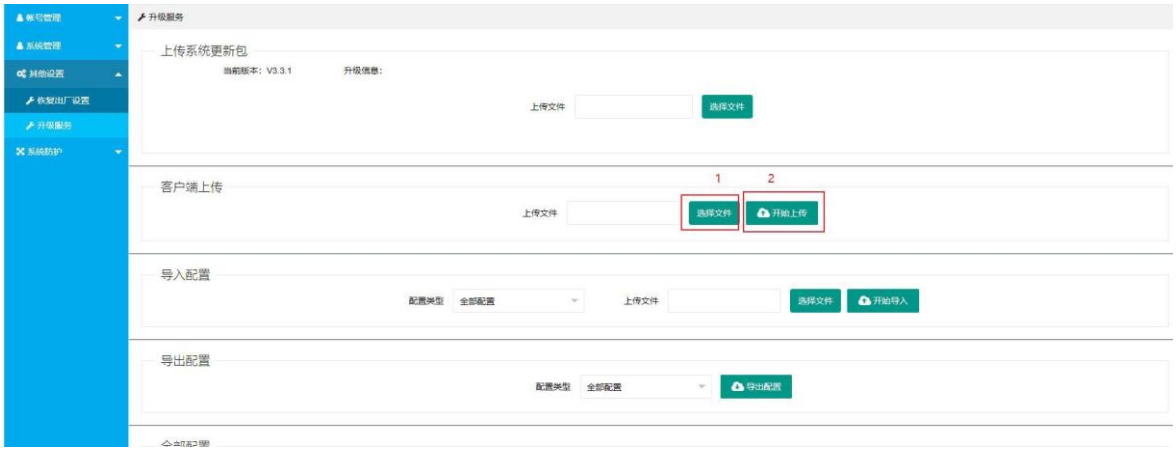


图 4.4.2.2-1 文件交换客户端上传

4.4.2.3 导入配置

为避免配置文件损坏后，管理员需要重新配置网闸任务的麻烦，隔离网闸提供网闸管理配置恢复的功能。该模块与导出配置文件配合使用。

系统管理操作界面→点击『其他设置』→点击『升级服务』进入到导入配置操作界面→选择配置类型，如：[全部配置]→点击选择文件→选择导入配置文件→点击开始导入→弹出提示界面：“确定要导入【全部配置】配置文件吗？”，点击确定，完成导入配置操作,如下图所示：

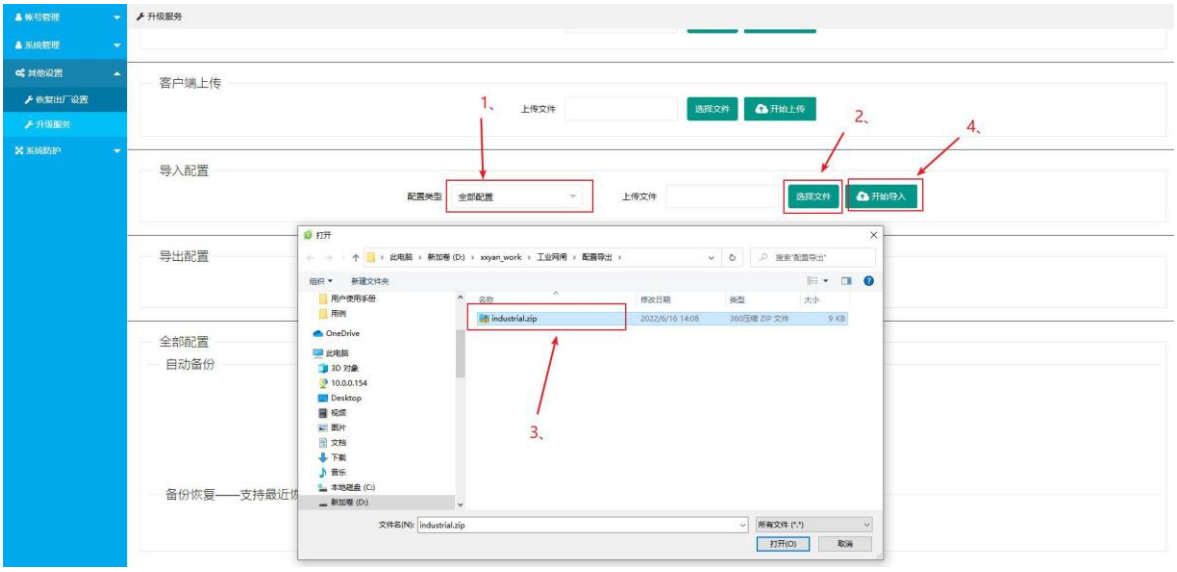


图 4.4.2.3-1 导入配置操作界面

▵**Tips:**

A：系统版本不同时，不能使用该功能来导入配置，以免配置文件不同导致系统无法运行

B：导入导出配置时，可选择配置类型为[全部配置]和对应模块配置，具体情况请根据实际应用进行选择

4.4.2.4 导出配置

为预防网闸在非正常情况下导致配置文件损坏或丢失给管理员带来配置任务时的繁琐工作，管理员在配

置好网闸后可以将配置导出备份。

系统管理操作界面→点击『其他设置』→点击『升级服务』进入到导出配置操作界面→选择配置类型，如：[全部配置]→点击导出配置→弹出提示信息：“确定要导出【全部配置】吗？”→点击确定，完成导出配置操作，如下图所示：

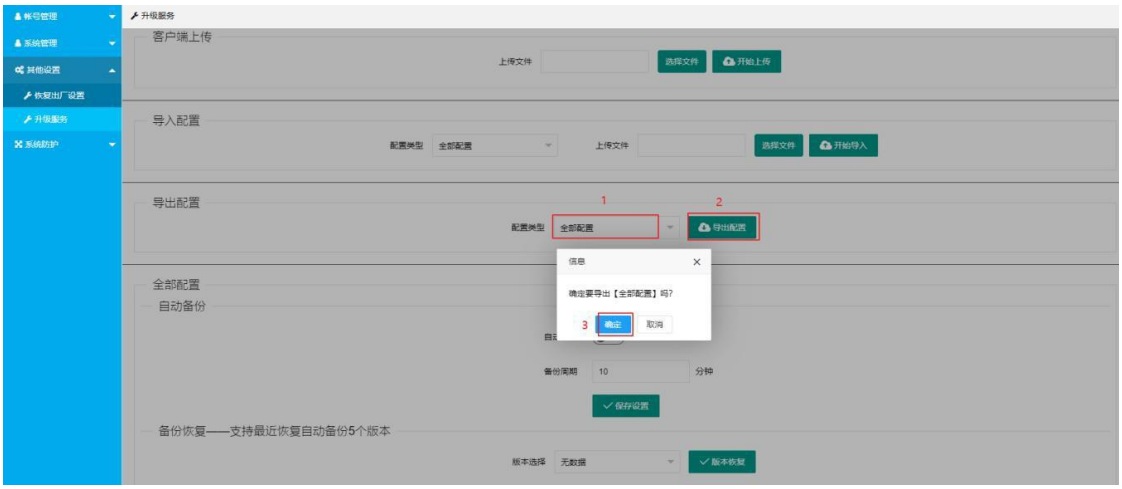


图 4.4.2.4-1 导出配置操作界面图

4.4.2.5 配置自动备份

该功能通过完成参数配置，启动自动备份任务，系统会备份全部配置到后台指定路径， 支持备份仅保留最近的 5 个记录。

系统管理操作界面→点击『其他设置』→点击『升级服务』进入到导出配置操作界面→开启自动备份→设置备份周期性→点击保存设置，系统会备份全部配置到后台指定路径，支持备份配置保存最近 5 个记录，如下图所示：

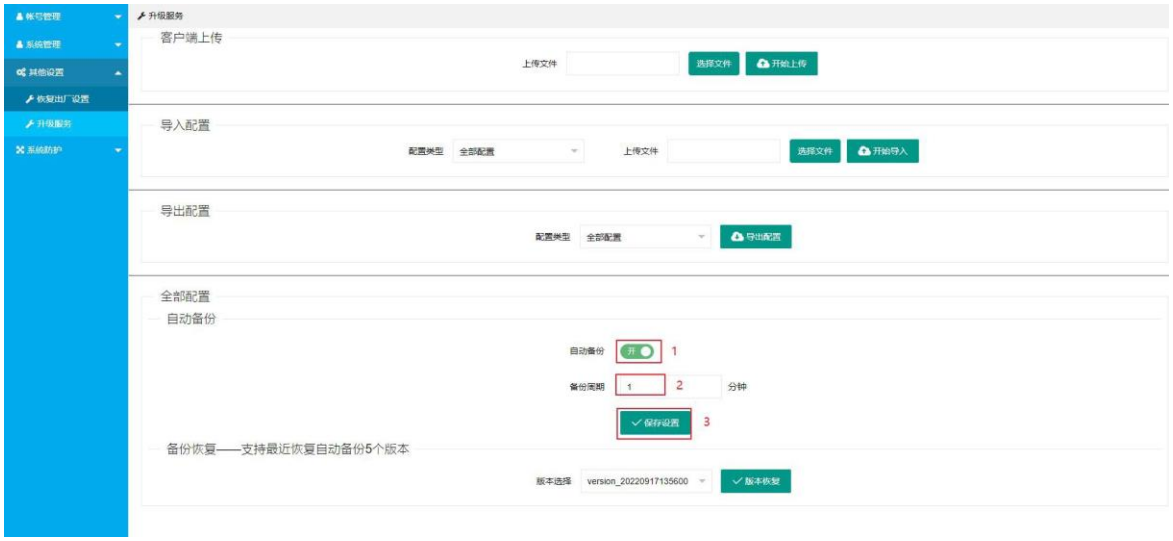


图 4.4.2.5-1 自动备份操作界面图

4.4.2.6 备份恢复

自动备份功能开启后，备份的版本会在下拉框中展示。管理员可通过该功能，进行版本备份的恢复操作。

系统管理操作界面→点击『其他设置』→点击『升级服务』进入到导出配置操作界面→进行[版本选择]→

点击版本恢复，完成备份恢复操作，如下图所示：

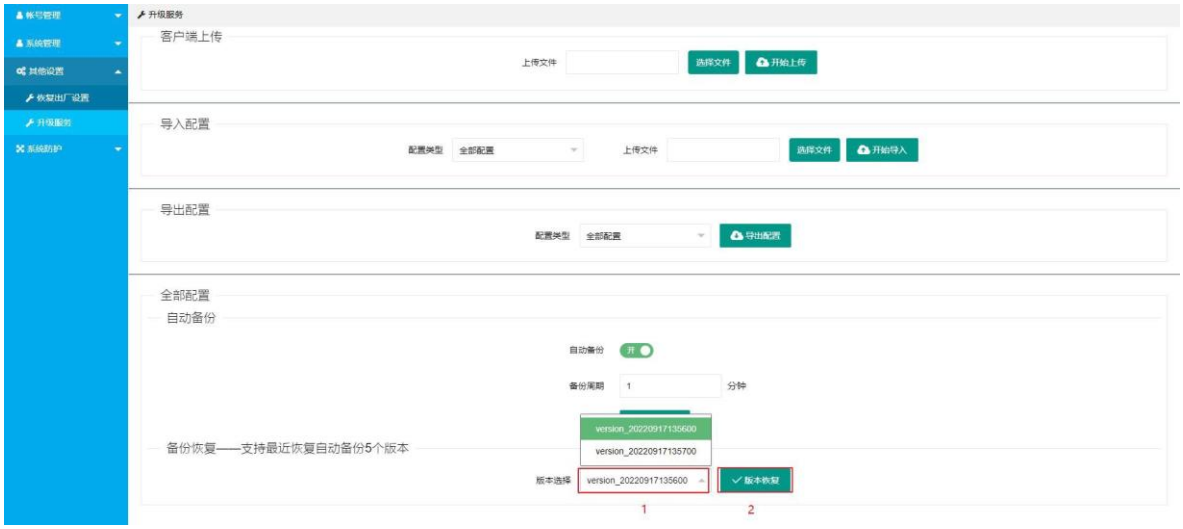


图 4.4.2.6-1 备份恢复操作界面

4.5 系统防护

『系统防护』包含两个模块：『病毒库设置』、『系统调试』。其中，『病毒库设置』是显示网闸当前病毒库信息，提供更新病毒库操作；『系统调试』是提供 traceroute、telnet、ping、arp、tcpdump 等网络调试操作。

4.5.1 病毒库设置

系统管理操作界面→点击『系统防护』→点击『病毒库设置』进入到病毒库操作界面， 如下图所示：

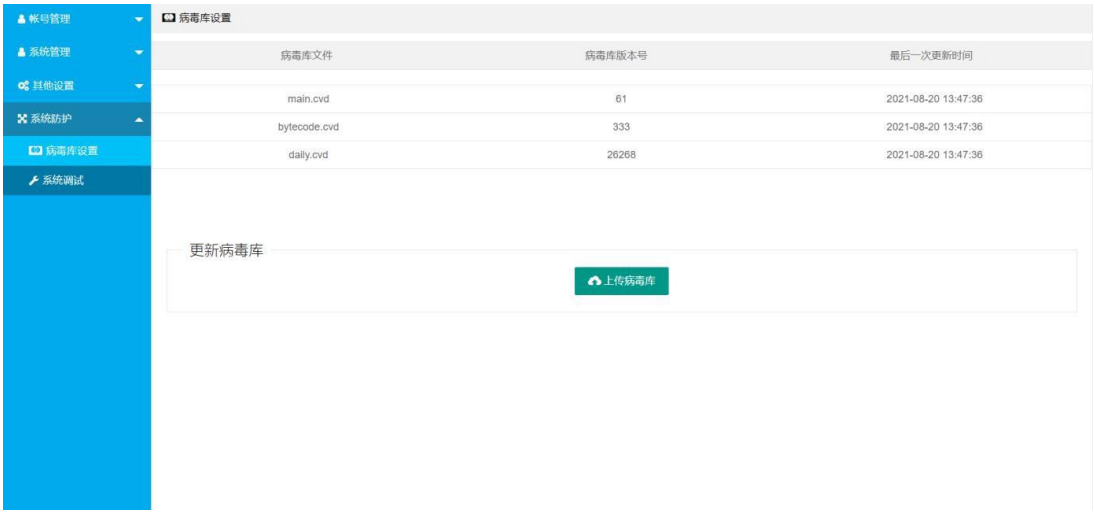


图 4.5.1-1 病毒库操作界面

在该界面可以看到病毒库文件名称、版本号以及最后一次更新时间。如需要更新病毒库，可以点击上传病毒库，选择病毒库文件点击打开，即可完成病毒库更新，如下图所示：

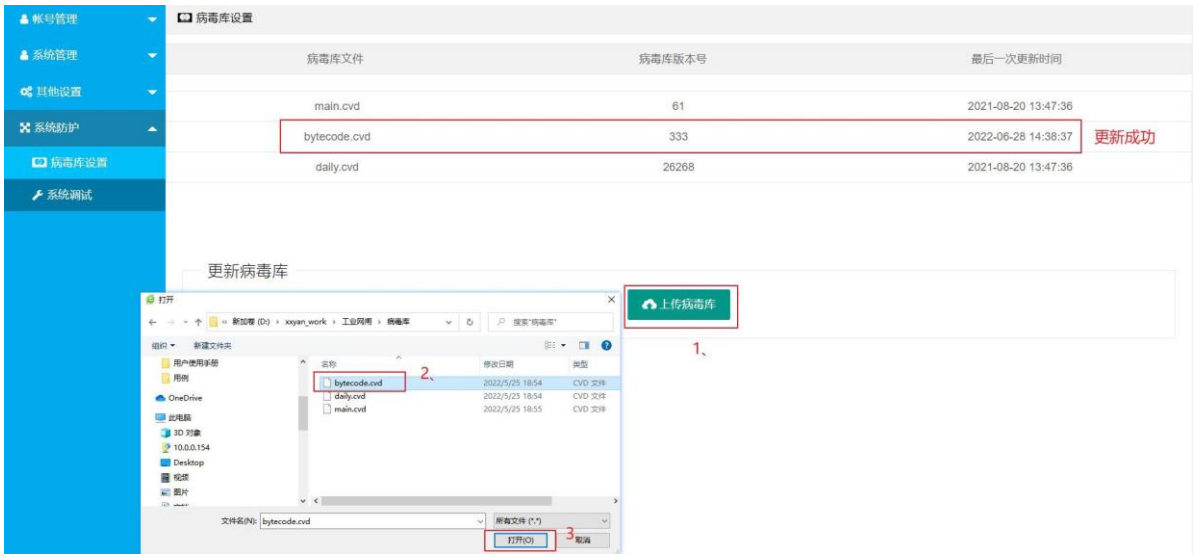


图 4.5.1-2 更新病毒库操作界面

4.5.2 系统调试

系统管理操作界面→点击『系统防护』→点击『系统调试』进入到系统调试操作界面→ 点击【系统调试】，如下图所示：

图 4.5.2-1 系统调试操作界面

系统调试工具说明：

- 测试工具：网络测试工具（共支持 traceroute、telnet、ping、arp、tcpdump 五种测试工具）
- 网卡：网闸网卡（内外网卡）
- 参数：测试工具不同，参数也不同

- traceroute 参数规范：X.X.X.X
- telnet 参数规范：X.X.X.X 24；X.X.X.X
- ping 参数规范：X.X.X.X
- arp 参数规范：无需填写参数

- tcpdump 参数规范：HOST X.X.X.X

△**Tips**：tcpdump 较特殊，须手动停止，停止之后提示是否需要将本次所抓的包导出网络检测操作界面→下拉选择[测试工具]、网卡→输入参数→点击测试，查看网络检测结果，如下图所示：

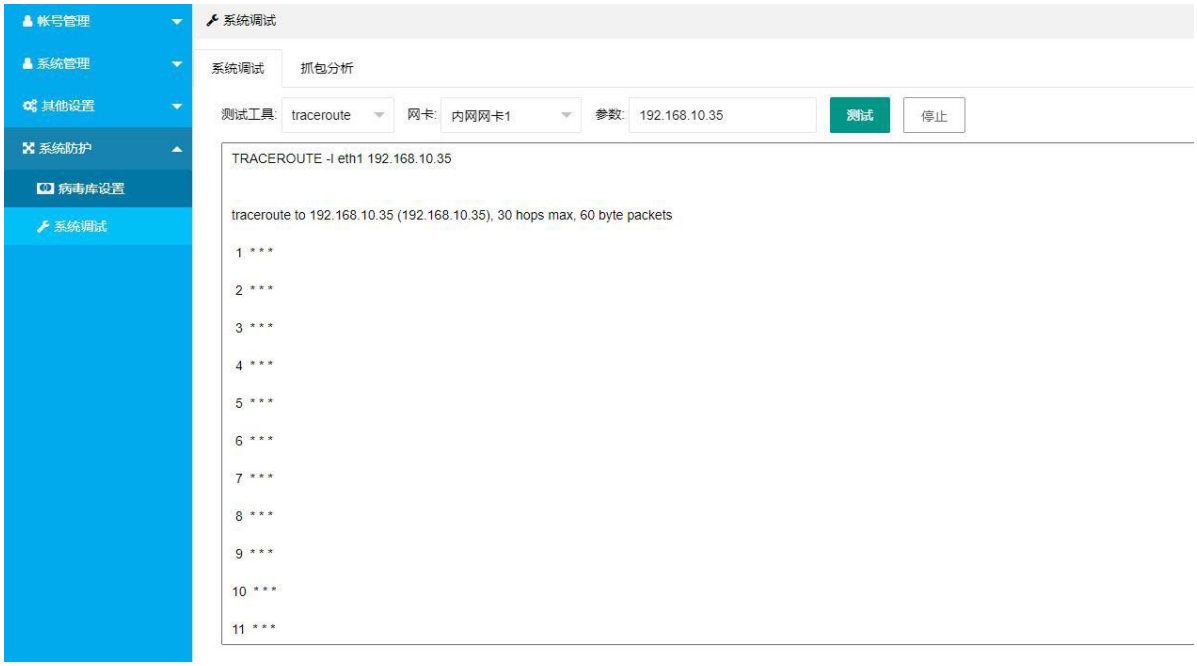


图 4.5.2-2 系统调试操作图

5. 应用功能篇

5.1 链路聚合

『链路聚合』将两个以上的网卡进行聚合使用，充分利用设备的端口及端口处理能力， 增加设备间的带宽，并且在其中一条链路出现故障时，可以快速地将流量转移到其他链路上。

【链路聚合设置】对内外网网卡进行聚合设置，操作包括【添加】、【修改】、【删除】。

系统管理操作界面→点击『链路聚合』→点击【链路聚合设置】进入到链路聚合操作界面，如下图所示：

图 5.1-1 链路聚合设置界面

链路聚合设置配置参数说明：

- 添加：添加链路聚合配置
- 修改：修改链路聚合配置
- 删除：删除链路聚合配置

5.1.1 添加

【链路聚合设置】操作界面→点击添加→在链路聚合对话框中按要求配置相关参数→点击确定，完成添加链路聚合操作，如下图所示界面：

图 5.1.1-1 添加链路聚合界面

添加链路聚合配置参数说明：

- 名称：名称不能为空，可以包含数字、字母和下划线，最多输入 10 个字符
- 内网网口聚合：选择至少 2 个及以上的内网聚合端口
- 外网网口聚合：选择至少 2 个及以上的外网聚合端口
- 发送策略：layer2 发送策略下，同时只有一个端口会收发数据；layer2+3 策略，同一个链路的数据只会从一个端口发送；layer3+4 策略，同一个链路的数据会动态使用所有参与聚合的端口发送
- 检测间隔时间：根据不同场景，可自定义设置时间，单位为毫秒，0 表示关闭
- LACP 发送速率：速率快、慢 （下拉选择）

5.1.2 编辑

【链路聚合设置】操作界面→选中链路聚合→点击编辑，弹出编辑窗口→按照添加链路聚合说明配置新的参数→点击提交→完成修改链路聚合操作。▵Tips：编辑聚合网卡配置后， 会重置聚合网卡 IP 信息。不建议使用聚合网卡作为管理口。如下图所示：

图 5.1.2-1 编辑链路聚合界面

5.1.3 删除

【链路聚合设置】操作界面→选中链路聚合→点击删除，弹出删除提示窗口→点击确定→完成删除链路聚合操作，如下图所示：

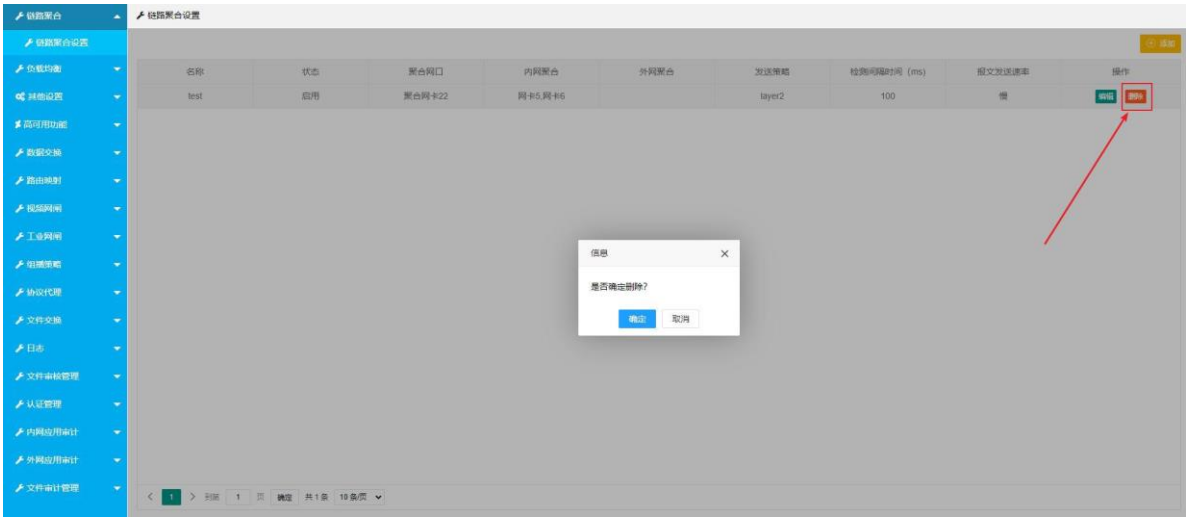


图 5.1.3-1 删除链路聚合界面

5.2 负载均衡

随着业务流量越来越大，单台服务器无论如何优化，采用多好的硬件，总会有性能天花板。当单服务器的性能无法满足业务需求时，就需要把多台服务器组成集群系统提高整体的处理性能。基于上述需求，要使用统一的流量入口对外提供服务，本质上就是需要一个流量调度器，通过均衡的算法，将用户大量

的请求流量均衡地分发到集群中不同的服务器上。

此版本支持负载均衡功能有：SMB 代理、POP3 协议代理、smtp 协议代理、tcp_single 协议代理、1bit 协议代理、tcp_custom 协议代理、HTTP 协议代理，其他协议暂不支持。

5.2.1 节点管理

『节点管理』，设备集群中每台设备都将作为一个节点，将需要加入负载设备集群的设备配置节点 ID，即设备集群内部所有设备除节点 ID 不同，其他配置保持一致即可。详情如下图所示:

图 5.2.1-1 节点管理配置界面

节点参数说明:

- 节点ID：负载设备ID，即负载设备集群节点 ID。加入设备集群的网闸都需要配置节点 ID 且不能重复
- 内、外网网卡接口：作为负载功能使用的网卡
- 内、外网IP 类型：根据需求使用IPV4 或IPV6 网络地址
- 内、外网虚拟IP：作为负载均衡设备集群对外的内外网业务IP

5.2.2 负载组管理

『负载组管理』配置业务类型及该业务所需负载设备集群的节点，可根据需求选择多个节点作为该业务功能的负载功能组。如下图所示:

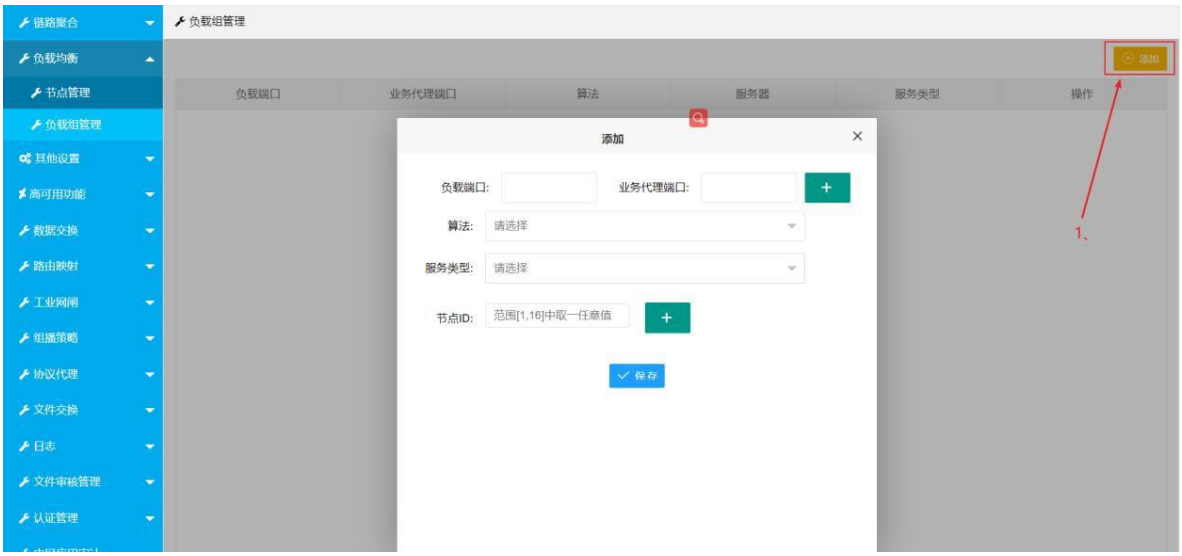


图 5.2.2-1 负载组管理

5.2.3 功能配置

下例中以两台设备作为负载设备集群:

设备 1：内网IP(172.16.48.156/16)、外网（172.16.48.157/16）、节点ID：7

设备 2：内网（172.16.120.228/16）、外网（172.16.120.229/16）、节点ID：8节点管理配置：配置节点参数，勾选启用负载均衡功能→点击保存。如下图所示:

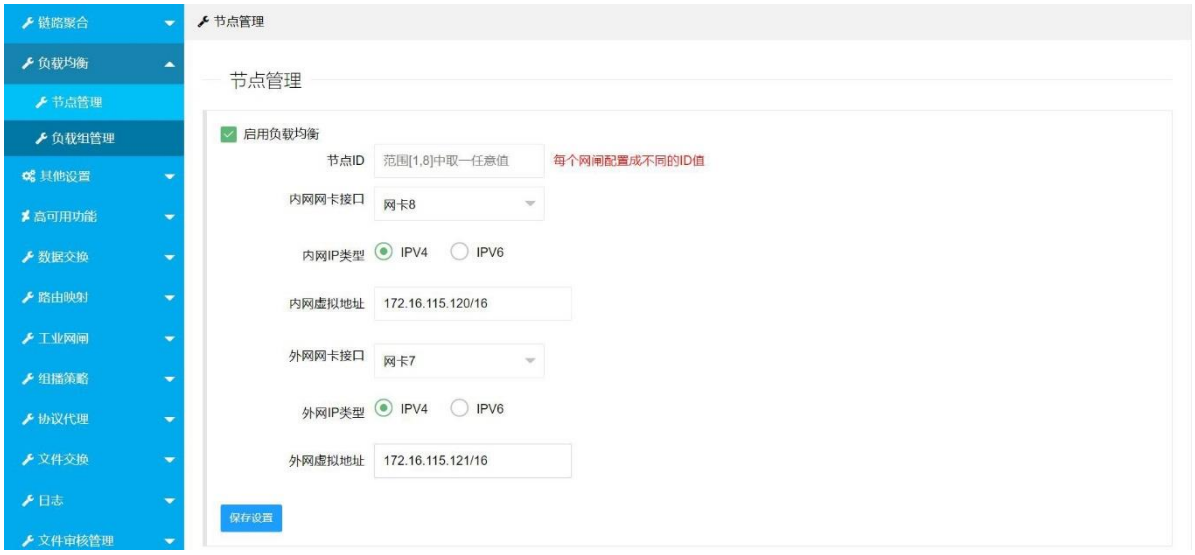


图 5.2.3-1 节点管理配置

负载组管理配置（以SMB 代理为例）→填写参数→点击保存。如下图所示:

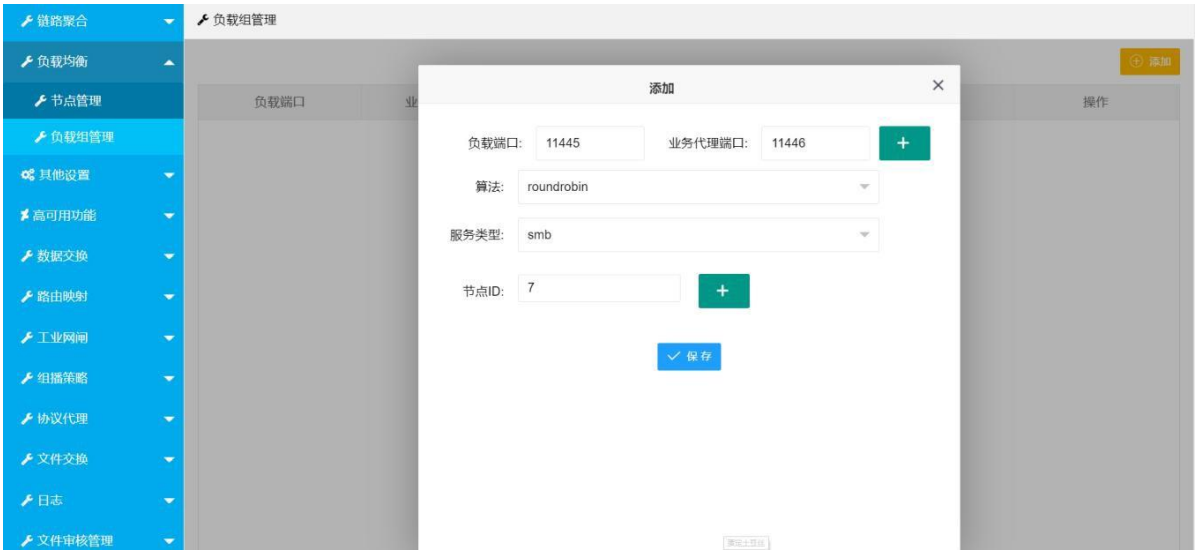


图 5.2.3-2 负载组管理配置

负载组管理参数说明：

1. 负载端口：负载功能所用端口，自定义空闲的合法端口即可
2. 业务代理端口：协议代理业务中的代理端口
3. 算法：负载任务分配算法

- roundrobin（轮询算法）
- leastconn（最小连接算法）
- source（源地址散列算法）
- random（随机算法）

4. 业务类型：使用负载功能的业务协议
5. 节点ID：指定多个节点作为负载组成员节点

5.3 其他设置

『其他设置』功能包括『入侵防御』、『日志空间设置』。

5.3.1 入侵防御

『入侵防御』针对外网被恶意攻击时， 及时做出防御的功能。可检测项目包括：BasicAttack、SMTP、FTP、DNS、DOS 攻击、DDOS 攻击、Port Scan 等。

系统管理操作界面→点击『其他设置』→选择『入侵防御』→勾选[需要检测项目]→勾选[需要检测的外网网卡]→点击保存，完成入侵防御界操作，如下图所示：

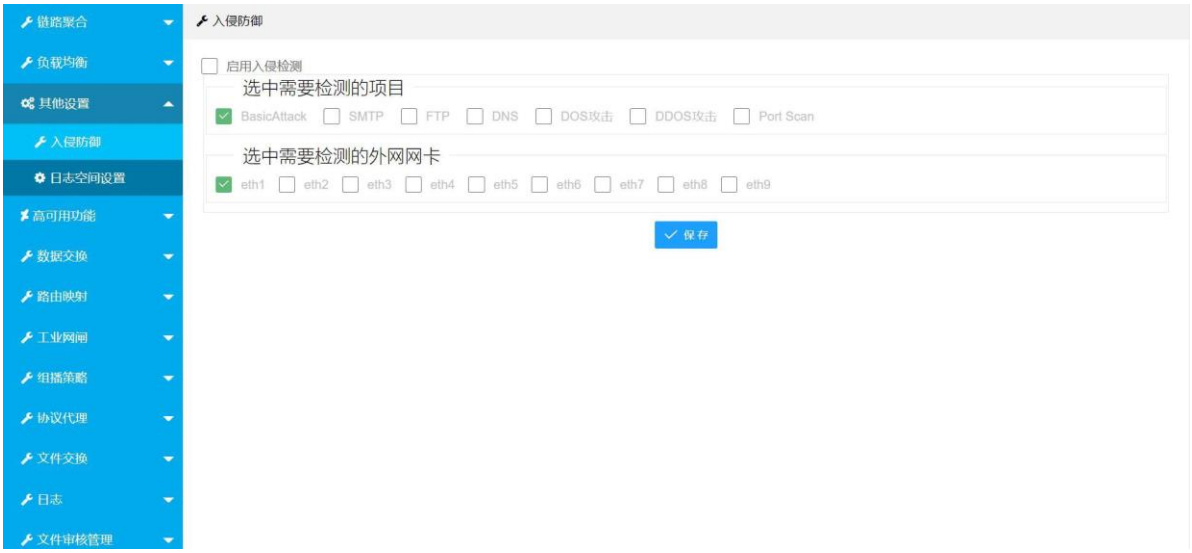


图 5.3.1-1 入侵防御操作界面

5.3.2 日志空间设置

『日志空间设置』对系统的内外网日志使用空间进行参数的设置和管理。

系统管理操作界面→点击『其他设置』→选择『日志空间设置』→依次设置需要的参数后→点击保存，完成日志空间设置操作，如下图所示：

图 5.3.2-1 日志空间设置界面

日志空间设置参数说明：

1. 日志空间大小：设置存储日志的空间大小，单位：MB，到达设置阈值会删除日志到告警阈值
2. 告警百分比：日志已使用空间占总日志空间的百分比，达到或超过设置的百分比值后， 系统会有日志空间不足告警提示
3. 日志留存天数：可保留日志的最大天数，日志周期超过该设置值，日志会被删除
4. 日志扫描：系统定时自动整理日志表空间

- 日志扫描时间点：设置日志表空间整理的时间点
- 间隔天数：设置日志表空间整理的间隔周期

5.4 高可用功能

『双机热备』基于两台网闸设备，一台作为网闸系统服务器的主机，另一台作为网闸系统服务器的备机，当两台设备构成主备状态后，若主机因为故障不能运行，备机自动切换为主机接管业务，保证业务的正常运行。

系统管理操作界面→点击『高可用功能』→点击『双机热备』进入到双机热备配置操作界面，如下图所示：

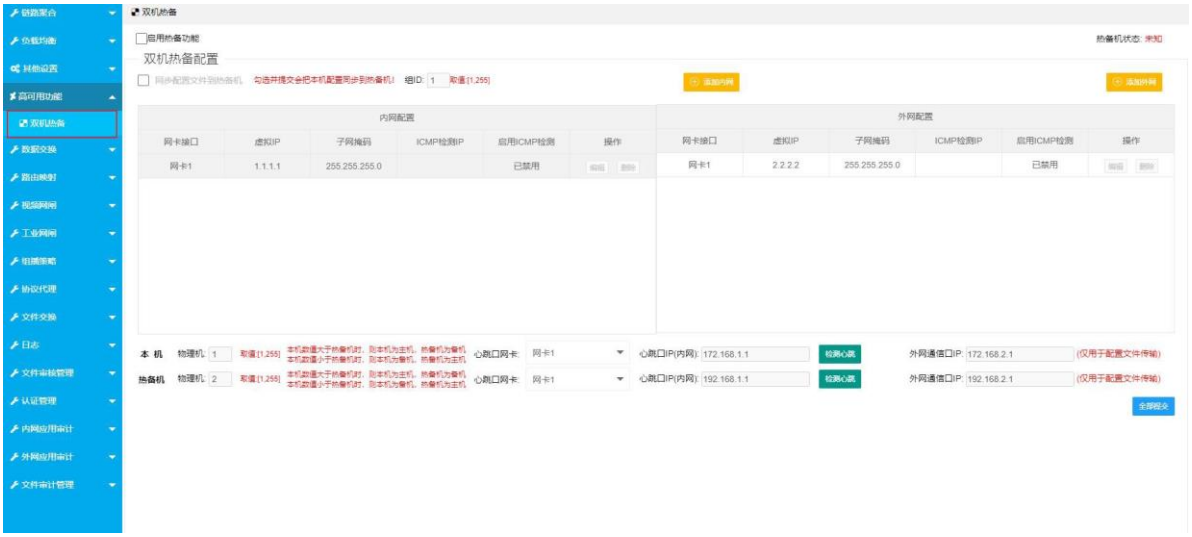


图 5.4-1 双机热备配置操作界面

双机热备配置参数说明：

1. 双机热备功能：控制热备功能启停
2. 同步配置文件到热备机：同步配置到热备机
3. 组 ID：设备集群组ID，相同组内的设备组ID 相同
4. 内网配置：

- 网卡接口：选择热备业务的内网网卡接口
- 虚拟IP：配置业务网卡 IP
- 子网掩码：虚拟IP 的子网掩码
- ICMP 检测：开启或关闭 ICMP 检测功能
- 检测IP：链路两端服务器或网关IP，判断网闸到服务器或网关链路是否正常

5. 外网配置：原理同内网配置
6. 本机：热备配置的当前机器

- 物理机：优先级的值范围为[1,255]，值大的为主机
- 心跳口网卡：主备机之间的心跳网卡

- 心跳口IP：为网卡真实IP，与选择的网卡IP 一致（选择了热备网卡，主备机心跳口需要配置同网段的 IP）
- 外网通信口IP：外网心跳口IP

7. 热备机：热备配置的备用机器

- 物理机：优先级的值范围为[1,255]，值大的为主机
- 心跳口网卡：主备机之间的心跳网卡
- 心跳口IP：为网卡真实IP，与选择的网卡IP 一致（选择了热备网卡，主备机心跳口需要配置同网段的 IP）
- 外网通信口IP：外网心跳口IP

5.5 数据交换

5.5.1 FTP 同步

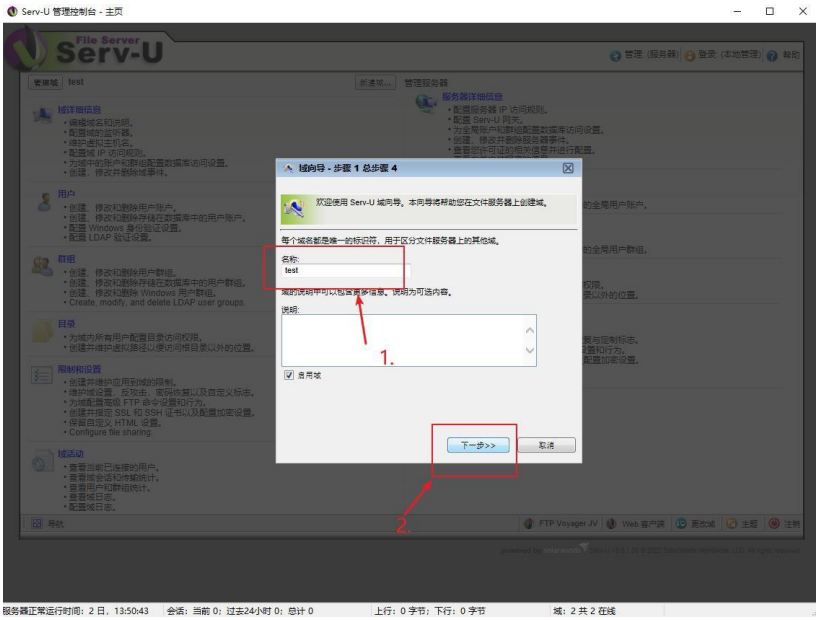
『FTP 同步』配置与管理 FTP 同步任务，进行FTP 文件的同步操作。包括添加任务、查看任务、修改任务、删除任务、批量删除等操作。

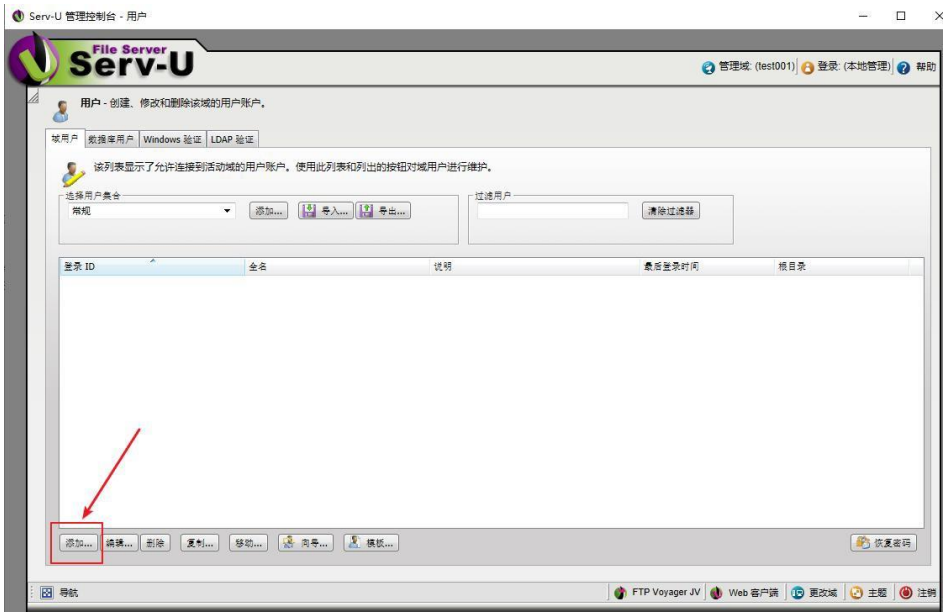
图 5.5.1-1 FTP 同步配置界面

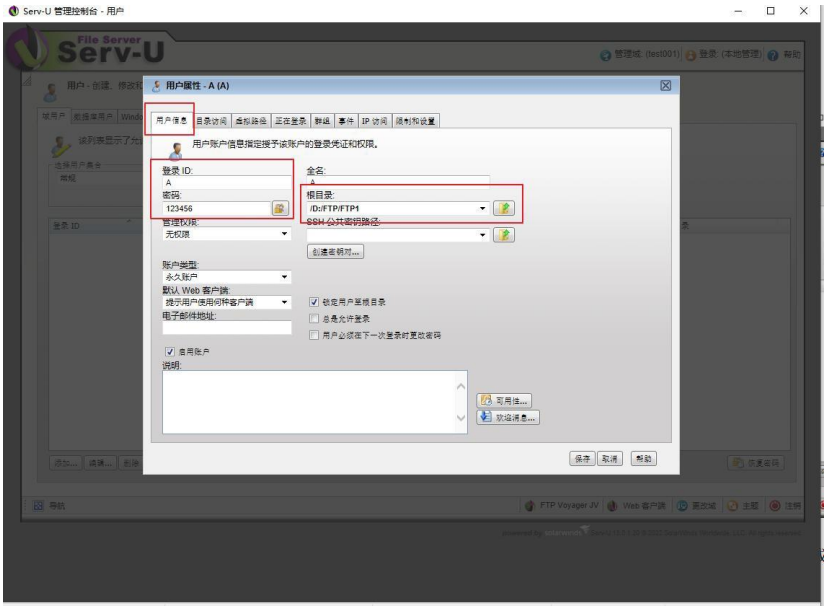
使用FTP 同步功能需先分别在内外网服务器上搭建 FTP 环境，并添加FTP 用户和文件存储路径，将用户权限设置为完全访问。FTP 用户权限设置步骤以serv-U 操作为例，如下图所示：

双机打开Serv-U 程序，点击新建域，弹出域配置窗口→输入域名，持续点击下一步，完成域创建，并进入域管理界面。

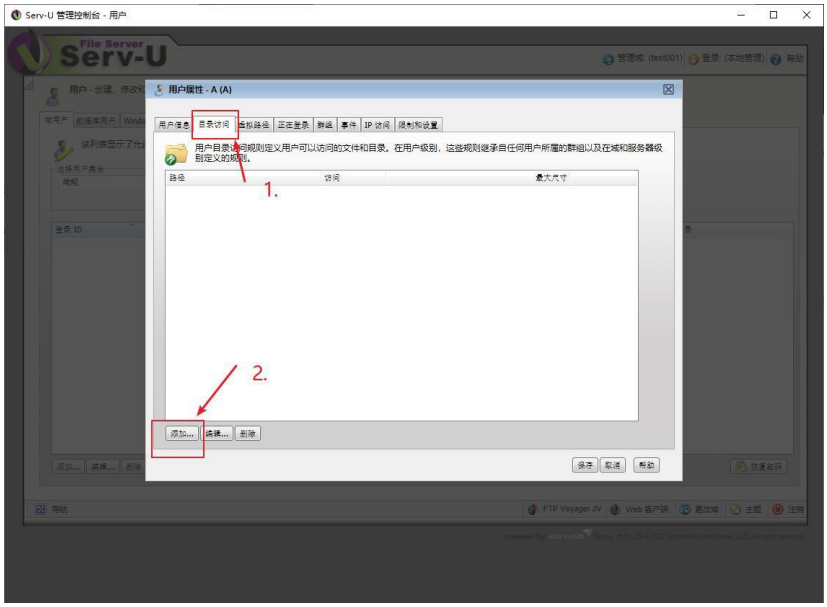
点击添加→设置用户信息：输入用户名、密码，选择文件存储路径，如下图所示：







设置目录访问权限：点击『目录访问』→点击添加→选择[路径]→点击完全访问，点击保存，完成 FTP 用户权限配置。如下图所示：



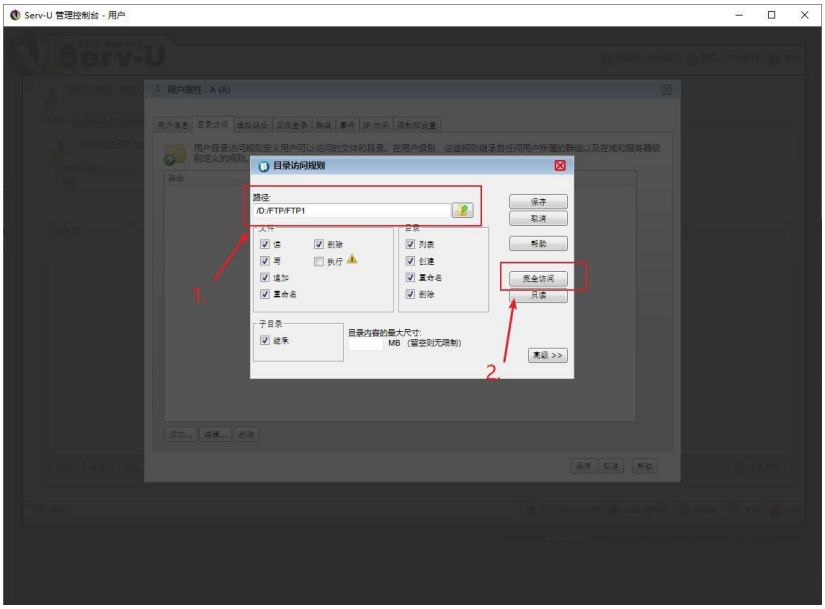


图 5.5.1_2 FTP 用户读写权限设置流程示意图

5.5.1.1 添加任务

【添加任务】包含【FTP 同步基本配置】、【高级设置】。FTP 同步配置操作界面→点击添加任务→进入【FTP 同步基任务】界面，如下图所示：

图 5.5.1.1-1 FTP 同步基本配置界面

同步基本配置参数配置说明：

1. 任务名：可以包含中文、数字、字母、下划线
2. 内网FTP 服务器参数：

- ip：内网FTP 服务器IP 地址
- 端口：内网FTP 服务器端口
- 账号：内网FTP 用户名称
- 密码：内网FTP 用户密码

3. 外网FTP 服务器参数：

- ip：外网FTP 服务器IP 地址
- 端口：外网FTP 服务器端口
- 账号：外网FTP 用户名称
- 密码：外网FTP 用户密码

4. 服务器模式：主动模式、被动模式，根据FTP 服务器实际环境进行选择
5. 同步类型：

- 周期同步：设置周期同步时间，单位：秒、分、时、天
- 定时同步：设置同步时间点，到达设置时间才会同步
- 时间段同步：设置同步时间段，在时间段内进行同步，时间段外不同步（时间段设置不支持跨天）

6. 同步模式：

- 先镜像后增量：任务启动后，先将源端 FTP 用户管理目录下所有文件进行一次镜像同步，之后只会进行增量同步
- 增量同步：只有任务启动后新增到源端的文件会同步到目的端，源端原有的文件不会同步
- 镜像同步：按照同步周期，每轮都将源端的所有文件同步到目的端

7. 同步方向：

- 由内网到外网：只将文件从内网FTP 服务器同步到外网FTP 服务器
- 由外网到内网：只将文件从外网FTP 服务器同步到内网FTP 服务器
- 双向：实现内外网FTP 服务器文件的双向同步

高级配置

完成FTP 同步基本配置→点击【高级配置】进入到高级配置界面→根据应用配置相关参数→点击确定提交→完成添加任务操作。如下图所示：

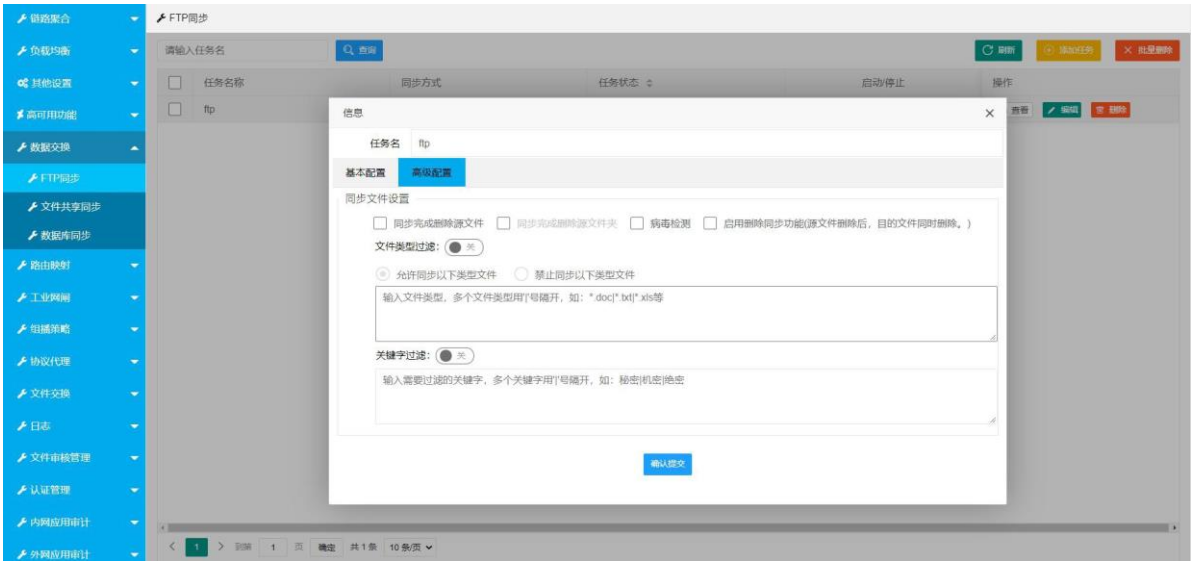


图 5.5.1.1-2 添加任务-FTP 同步高级配置对话框

FTP 同步高级配置参数配置说明：

1. 同步文件设置：

- 同步完成删除源文件：源文件夹中的文件同步到目的文件夹成功后，源文件夹中的文件会被删除（所有文件）
- 同步完成删除源文件夹：源文件夹中的文件同步到目的文件夹成功后，在源文件夹中的文件被删除后，源文件夹被删除

2. 病毒检测：源文件夹中的文件中有病毒时，病毒文件不会同步到目的文件夹中。
3. 删除同步功能：删除源文件夹中的文件，目的文件夹中的文件也会删除
4. 文件类型过滤：

- 允许同步以下类型文件：只会同步允许的文件类型，其它类型不会同步
- 禁止同步以下类型文件：被禁止的文件类型不会同步，其它类型文件全部同步
- 关键字过滤：开启此选项，设置关键字，文件名及文件内容包含关键字的文件不会同步

5.5.1.2 查看任务

FTP 同步配置操作界面→在要查看的FTP 任务右边，点击查看，如下图所示：

图 5.5.1.2-1 查看 FTP 同步任务信息

5.5.1.3 编辑任务

FTP 同步配置操作界面→在需要查看的 FTP 任务右边，点击编辑→出现【编辑】任务窗口→ 按照【添加任务】参数说明进行参数修改→点击确认提交→完成编辑 FTP 同步任务。如下图所示：

图 5.5.1.3-1 编辑 FTP 同步任务信息

5.5.1.4 删除任务

FTP 同步配置操作界面→点击需要删除的 FTP 同步任务的删除按钮，出现删除提示窗口→点击确定→完成删除FTP 同步任务。如下图所示：

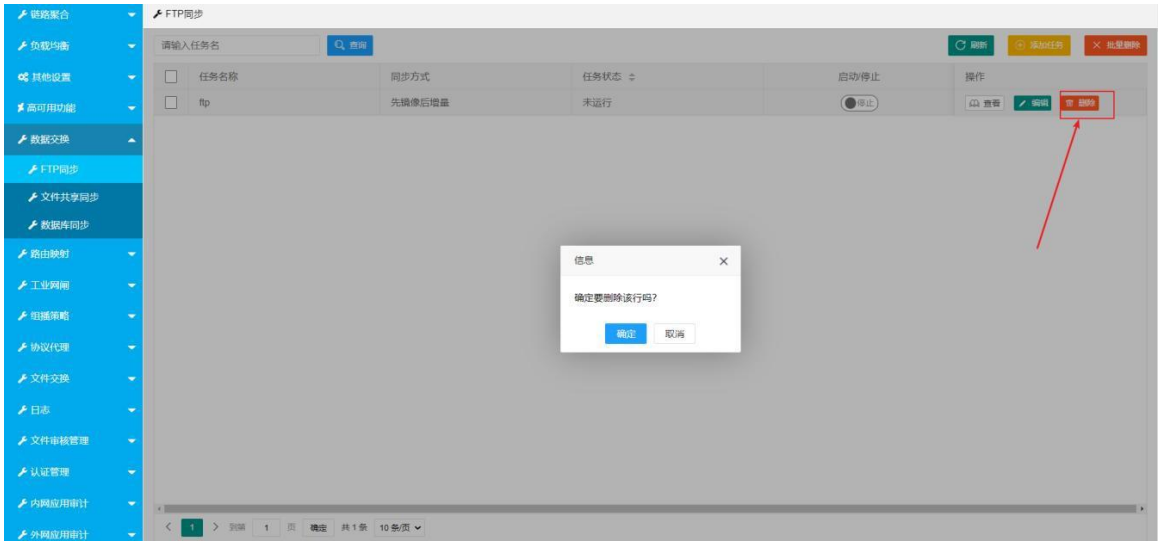


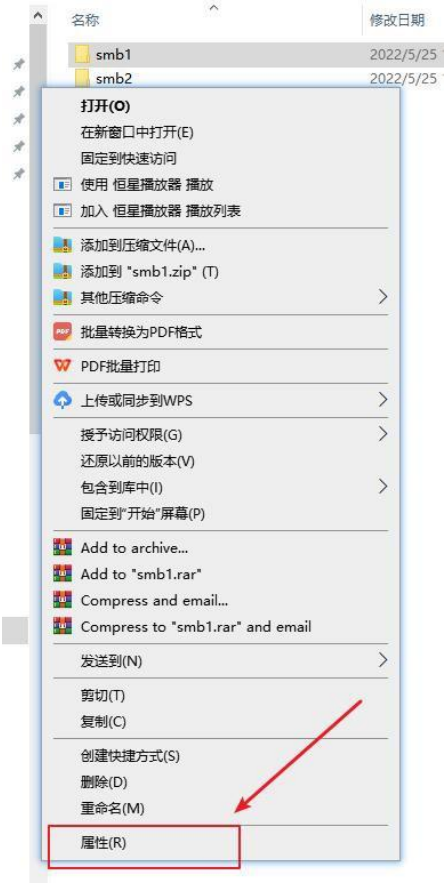
图 5.5.1.4-1 删除任务提示窗口

5.5.2 文件共享同步

『文件共享同步』配置与管理共享文件同步任务，包括【添加任务】、【修改任务】、【删除任务】等操作。

文件夹读写权限设置步骤：

右键“文件夹”选择【属性】进入文件夹属性设置界面→点击【共享】，点击高级共享→勾选[共享此文件夹]，点击权限→勾选【完全控制】权限→点击确定修改文件夹的读写权限。具体操作流程如下图所示：


名称
修改日期
smb1
2022/5/25
smb2
2022/5/25
打开(O)
在新窗口中打开(E)
固定到快速访问
使用 恒星播放器 播放
加入 恒星播放器 播放列表
添加到压缩文件(A)...
添加到 "smb1.zip" (T)
其他压缩命令
批量转换为PDF格式
PDF批量打印
上传或同步到WPS
授予访问权限(G)
还原以前的版本(V)
包含到库中(I)
固定到"开始"屏幕(P)
Add to archive...
Add to "smb1.rar"
Compress and email...
Compress to "smb1.rar" and email
发送到(N)
剪切(T)
复制(C)
创建快捷方式(S)
删除(D)
重命名(M)
属性(R)


smb1 属性
常规
共享
安全
以前的版本
自定义
smb1
类型:
文件夹
位置:
D:\SMB
大小:
0 字节
占用空间:
0 字节
包含:
0 个文件，0 个文件夹
创建时间:
2022年5月25日，19:12:06
属性:
只读(仅应用于文件夹中的文件)(R)
隐藏(H)
高级(D)...
确定
取消
应用(A)


smb1 属性
常规
共享
安全
以前的版本
自定义
网络文件和文件夹共享
smb1
不共享
网络路径(N):
不共享
共享(S)...
高级共享
设置自定义权限，创建多个共享，并设置其他高级共享选项。
高级共享(D)...
密码保护
用户必须具有此计算机的用户帐户和密码，才能访问共享文件夹。
若要更改此设置，请使用网络和共享中心。
确定
取消
应用(A)
1.
2.

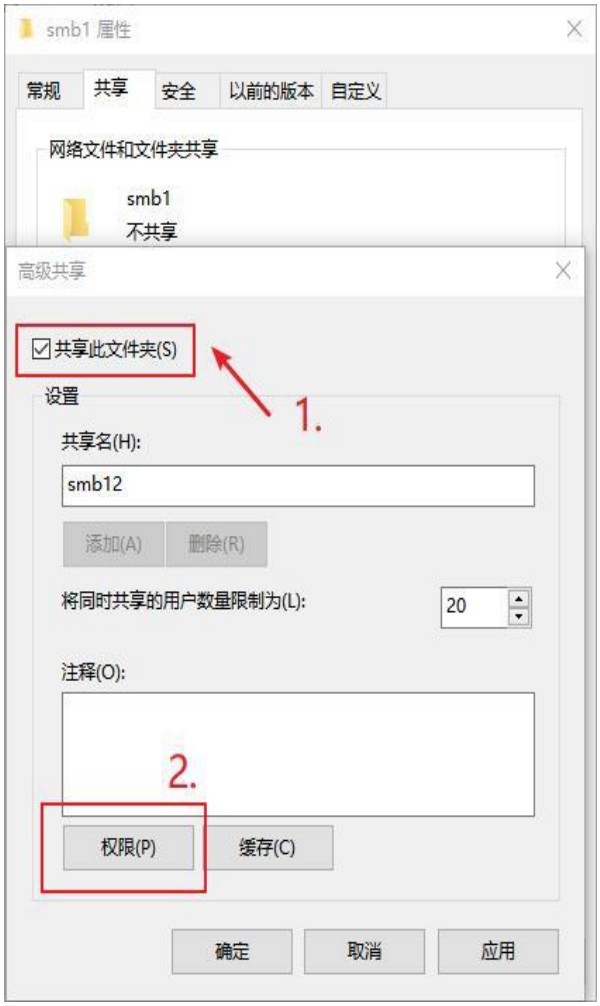

smb1 属性
常规
共享
安全
以前的版本
自定义
网络文件和文件夹共享
smb1
不共享
高级共享
共享此文件夹(S)
设置
共享名(H):
smb12
添加(A)
删除(R)
将同时共享的用户数量限制为(L):
20
注释(O):
权限(P)
缓存(C)
确定
取消
应用
1.
2.

图 5.5.2-1 文件夹读写权限设置流程示意图

系统管理操作界面→点击『数据交换』→点击『文件共享同步』进入到文件共享同步配置操作界面；如下图所示：

图 5.5.2-2 文件同步配置操作界面

文件同步配置参数说明：

- 添加任务：新增文件共享同步任务
- 编辑：修改文件共享同步任务
- 删除：删除文件共享同步任务
- 批量删除：批量删除文件共享同步任务
- 启动/停止：启动或停止任务
- 查询：按名称查询任务信息

5.5.2.1 添加任务

文件同步配置界面→点击【添加任务】弹出添加任务对话框,如下图所示：

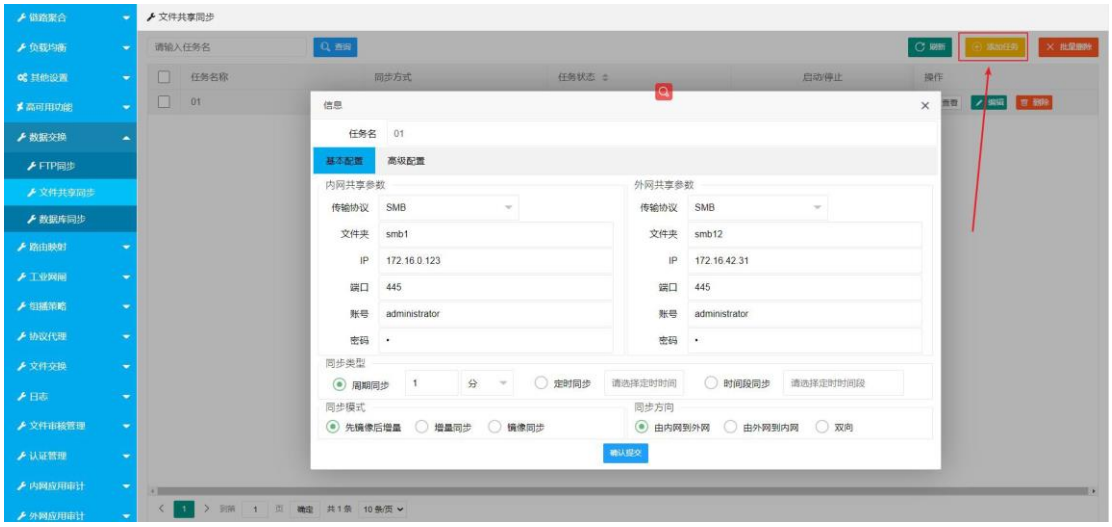


图 5.5.2.1-1 添加任务 文件共享同步基本参数对话框

文件共享同步基本参数设置说明：

1. 任务名：可以包含数字、字母、下划线（必填项）
2. 同步类型：

- 周期同步：设置周期同步时间，单位：秒、分、时、天
- 定时同步：设置同步时间点，到达设置时间才会同步
- 时间段同步：设置同步时间段，在时间段内进行同步，时间段外不同步（时间段设置不支持跨天）

3. 同步模式：

- 先镜像后增量：任务启动后，先将源文件夹进行一次镜像同步，之后只会进行增量同步
- 增量同步：只有任务启动后新增到源文件夹的文件或文件夹才会同步到目的端， 源端原有的文件不会同步
- 镜像同步：按照同步周期，每轮都将源端的所有文件同步到目的端

4. 同步方向：

- 由内网到外网：只将文件从内网文件服务器同步到外网文件服务器
- 由外网到内网：只将文件从外网文件服务器同步到内网文件服务器
- 双向：实现内外网文件服务器文件的双向同步

5. 内网参数：

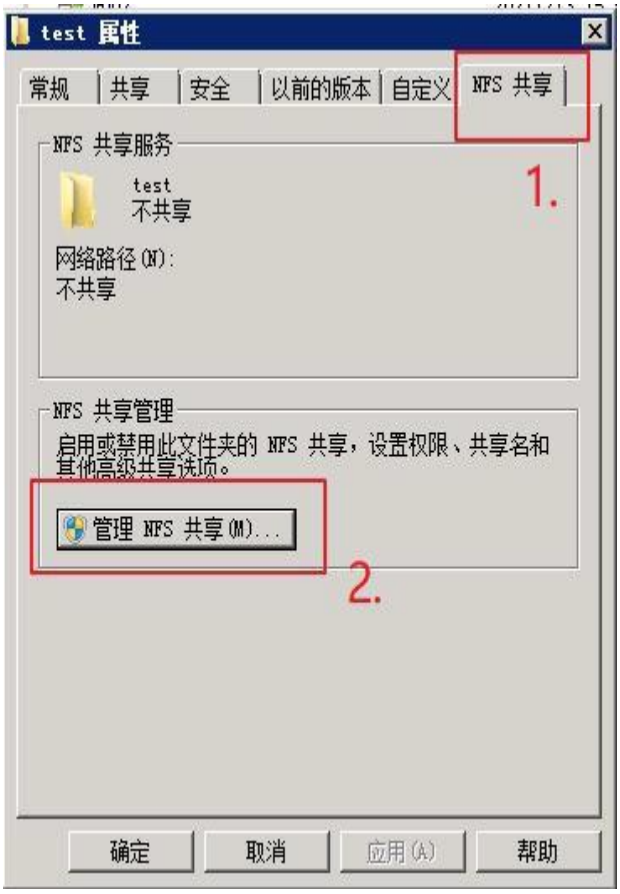
- 传输协议：支持“SMB”和“NFS”,系统默认选择“SMB”
- 文件夹：内网服务器共享文件夹名称
- IP：内网服务器 IP 地址
- 账号：内网服务器的用户名
- 密码：内网服务器用户名匹配的密码

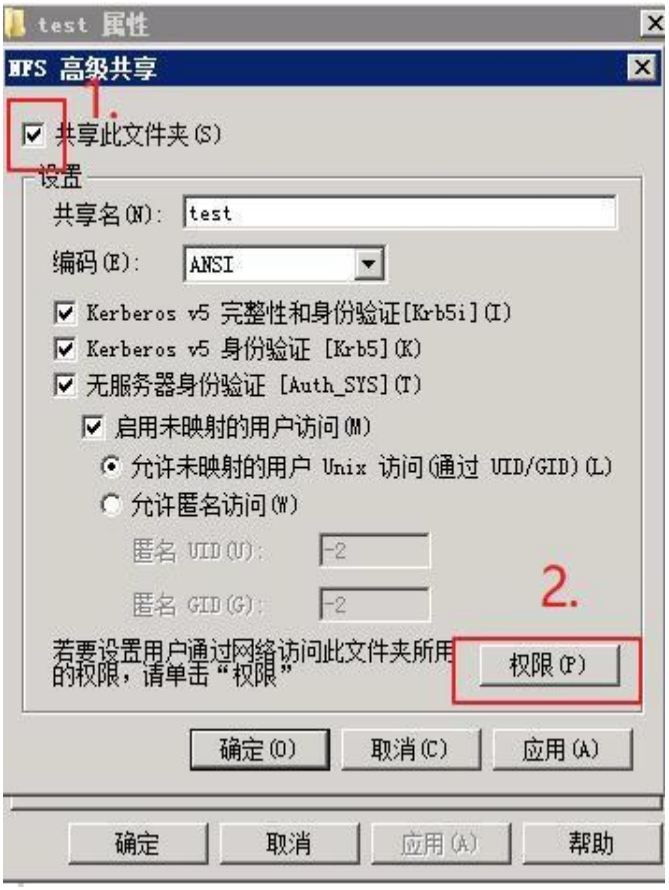
6. 外网参数：参考内网参数

NFS 共享具体操作步骤如下：

1. 右键“文件夹”选择【属性】进入文件夹属性设置界面→点击【NFS 共享】，点击管理NFS 共享→勾选【共享此文件夹】→点击【权限】→选择访问类型为【读写】，勾选【允许根目录访问】→点击【确定】，操作流程如下图所示：


test 属性
常规
共享
安全
以前的版本
自定义
NFS 共享
test
类型: 文件夹
位置: E:\NFS
大小: 0 字节
占用空间: 0 字节
包含: 0 个文件，0 个文件夹
创建时间: 2022年5月25日，19:22:33
属性:
只读(仅应用于文件夹中的文件)(R)
隐藏(H)
高级(D)...
确定
取消
应用(A)
帮助


test 属性
常规
共享
安全
以前的版本
自定义
NFS 共享
NFS 共享服务
test
不共享
网络路径(N):
不共享
1.
NFS 共享管理
启用或禁用此文件夹的 NFS 共享，设置权限、共享名和其他高级共享选项。
管理 NFS 共享(M)...
2.
确定
取消
应用(A)
帮助



高级配置

完成共享文件同步基本参数配置→点击【高级配置】进入到高级配置界面；如下图所示：

图 5.5.2.1-2 添加任务-高级设置对话框

高级设置参数配置说明:

同步文件设置:

- 同步完成删除源文件：源文件夹中的文件同步到目的文件夹成功后，源文件夹中的文件会被删除（所有文件）
- 同步完成删除源文件夹：源文件夹中的文件同步到目的文件夹成功后，会删除源文件夹中的文件后再删除源文件夹

病毒检测：源文件夹中存在病毒时，病毒文件不会同步到目的文件夹。

删除同步功能：删除源文件夹中的文件，目的文件夹中的文件也会删除

文件类型过滤:

- 允许同步以下类型文件：只会同步允许的文件类型，其它类型不会同步
- 禁止同步以下类型文件：被禁止的文件类型不会同步，其它类型文件全部同步
- 关键字过滤：开启此选项，设置关键字，文件名及文件内容包含关键字的文件不会同步

5.5.2.2 修改任务

文件同步配置操作界面→选中需修改的文件同步任务→点击编辑→ 按照“添加任务”配置说明修改参数→点击确认提交→完成修改文件同步任务。如下图所示:

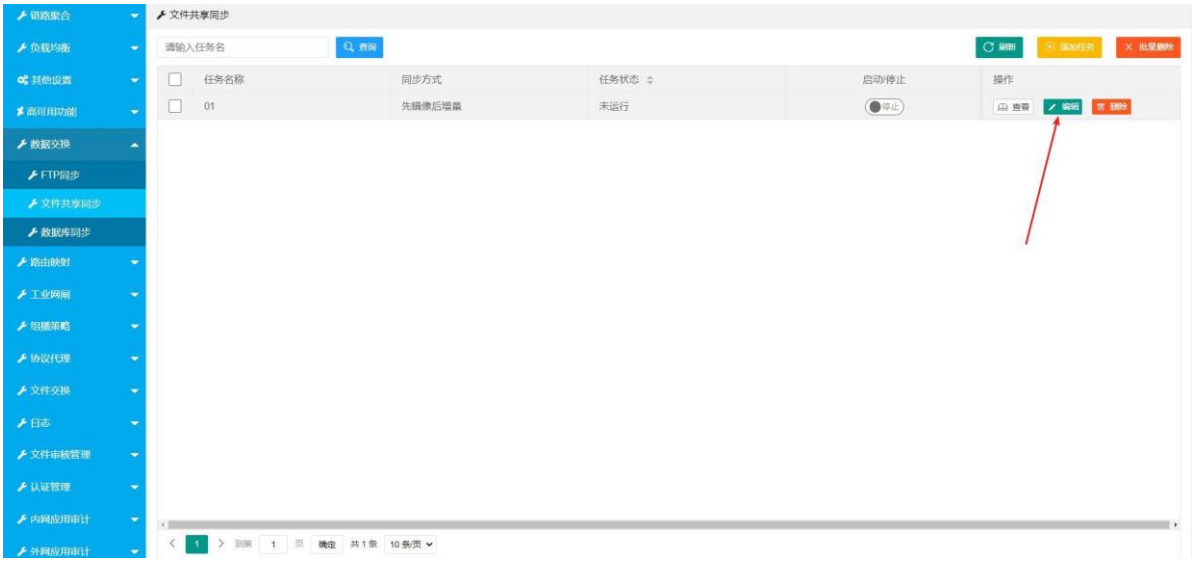


图 5.5.2.2-1 添加任务-高级设置对话框

5.5.2.3 删除任务

文件同步配置操作界面→选中需删除的文件同步任务→点击删除任务（出现删除提示窗口）→点击确定→完成删除文件同步任务。如下图所示：

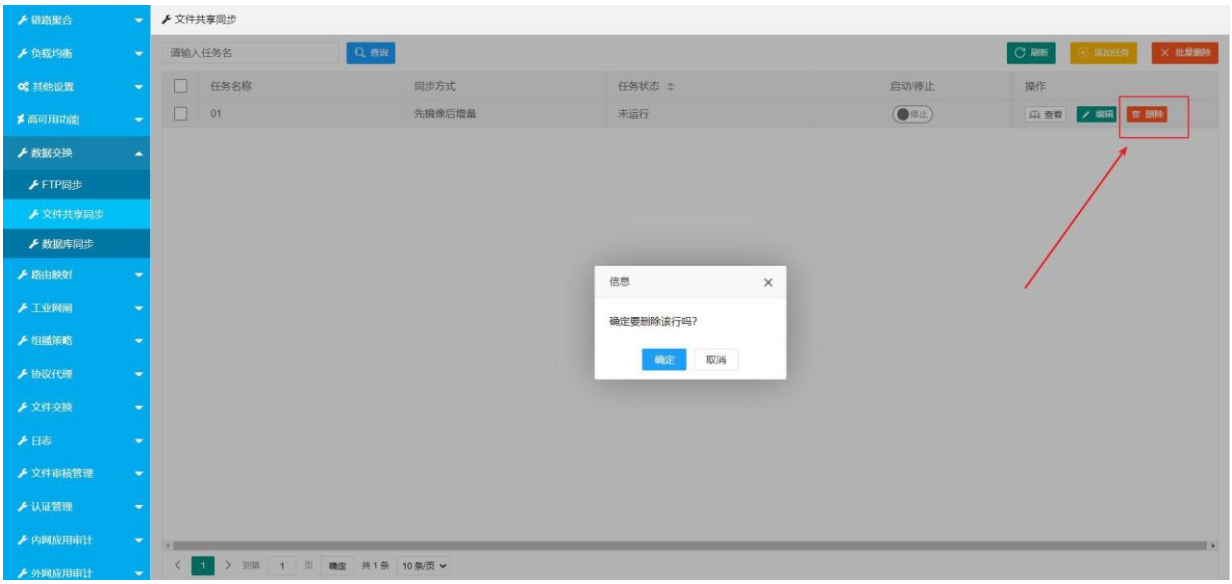


图 5.5.2.3-1 删除任务提示窗口

5.5.3 数据库同步

『数据库同步』功能支持Oracle（10g、11g、12c）；SQL Server（2008、2012、2014、2016、2017）；MySql（支持 5.5、5.6、5.7、8.0）、DB2(11.5)、Sybase(16.0)、Postgresql(12.3)、Kingbase(V7)、达梦(V7)等多种数据库类型。支持数据库单、双向同步；支持 MySql-Oracle、MySql-SQL Server、SQL Server-Oracle 部分字段相互异构同步。

5.5.3.1 数据库同步配置说明

数据库同步功能使用之前，需要在路由映射中配置映射规则，数据库程序才能正常访问外网端数据库。具体流程：点击【路由映射】→【对象管理】进行对象添加，完成后如下图所示界面：

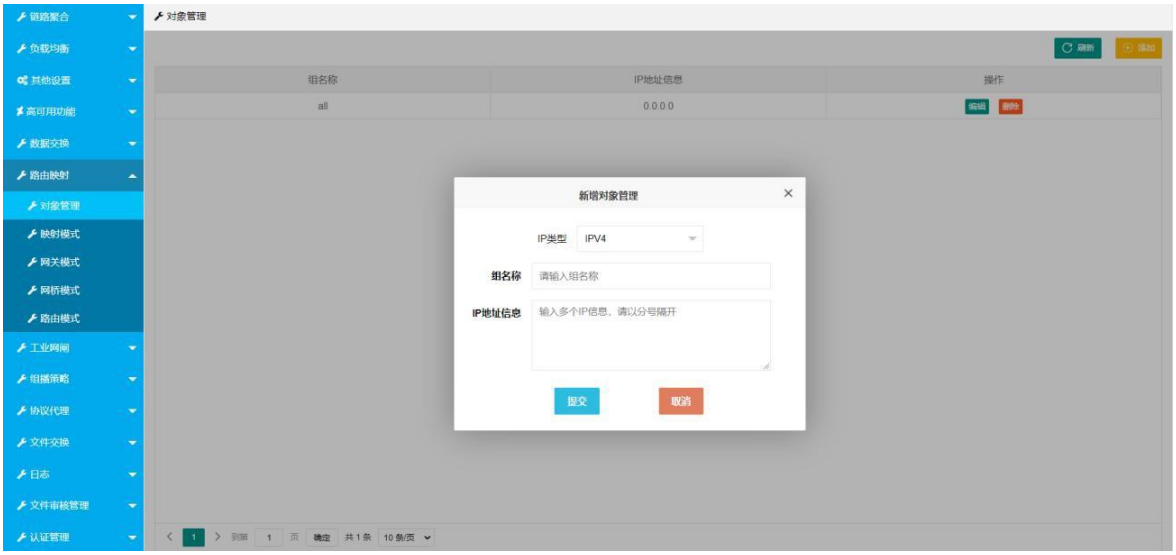


图 5.5.3.1-1 添加映射对象

再点击【路由映射】→【映射管理】→映射规则配置完成后，启动规则，即可进行下一步配置。

△**Tips：源对象必须为 all！**如下图所示：

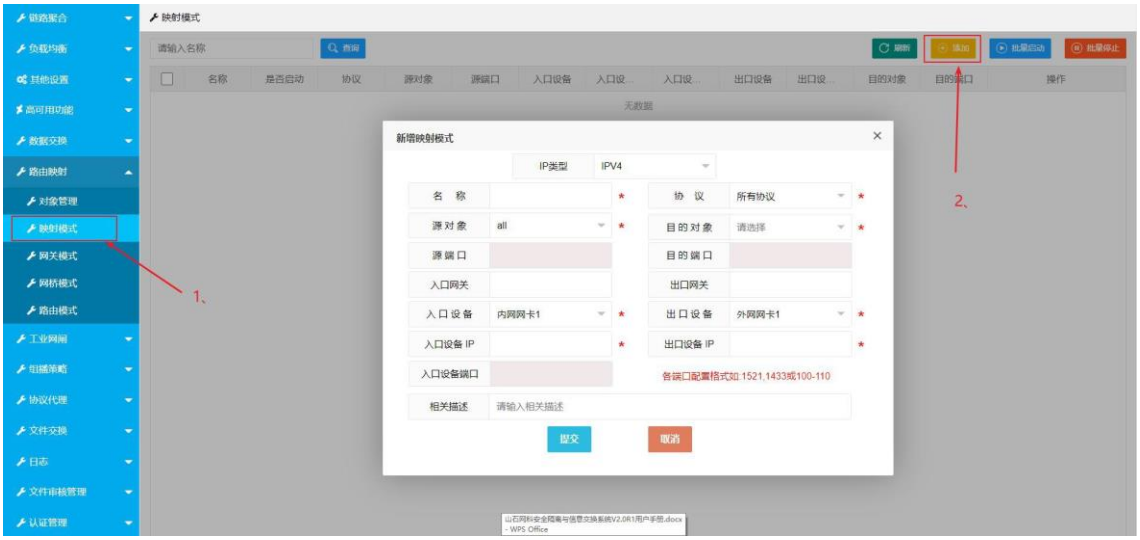


图 5.5.3.1-2 添加映射规则

5.5.3.2 新增任务

『数据库同步』配置与管理数据库同步任务。包括【添加】、【编辑】、【删除】、【任务启动】、【任务停止】、【查询】等操作。『数据交换』→『数据库同步』→添加任务→【基本配置界面】界面→填写[基本配置]参数→测试连接→提示： “测试连接成功” →[高级配置]→[同步表选择]→[同步表配置]→点击确认提交，如下图所示：

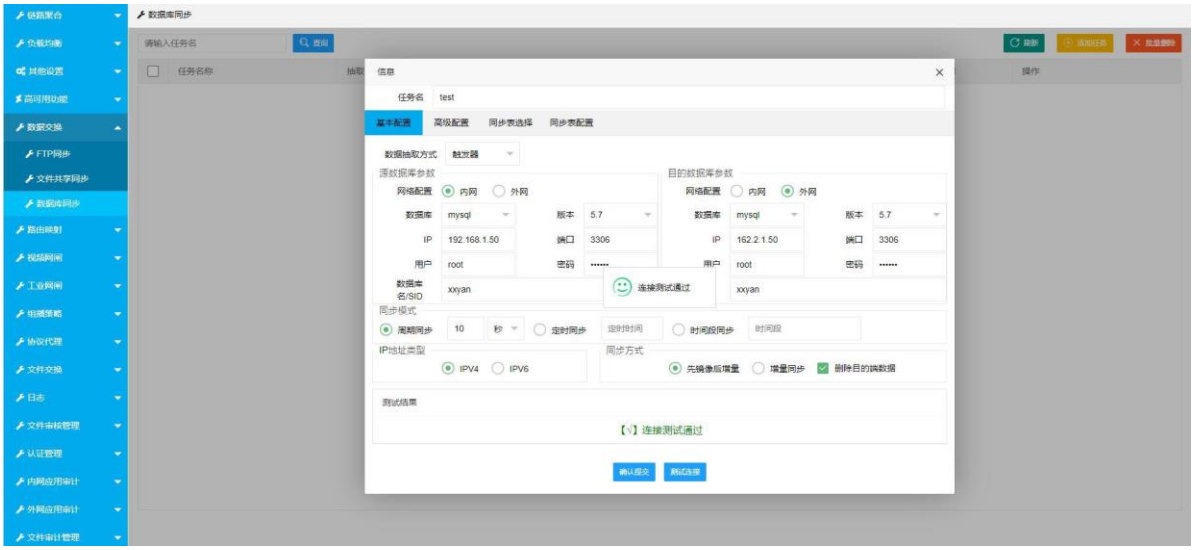


图 5.5.3.2-1 数据库同步基本操作界面

数据库库同步基本配置参数说明：

1. 任务名：可以包含数字、字母、汉字、下划线、为必填项
2. 源数据库参数 (这里以源端为例，目的端对应填写)：

- 网络配置：单选按钮，选择内网或者外网。源端和目的端不能选一样的网络配置， 只能是内到外或是外到内，不能内到内或是外到外
- 数据库：选择数据库类型
- 版本：选择数据库版本
- IP：源端数据库服务器的IP
- 端口：数据库端口号，如：sqlserver:1433、mysql:3306、oracle:1521
- 用户：数据库用户名
- 密码：数据库密码
- 数据库名SID：数据表所在的数据库名字

3. 同步类型：

- 周期同步：设置周期同步时间，单位：秒、分、时、天
- 定时同步：设置同步时间点，到达设置时间才会同步
- 时间段同步：设置同步时间段，在时间段内进行同步，时间段外不同步（时间段设置不支持跨天）

4. 同步模式：

- 先镜像后增量：任务启动后，先将源表进行一次镜像同步，之后只会进行增量同步
- 增量同步：只有任务启动后新增到将源的数据才会同步到目的表，源表原有的数据不会同步
- IP 地址类型：IPV4: X.X.X.X；IPV6: X:X::X:X
- 测试连接：确认网闸和内外网端数据库服务器的连接状态

测试连接成功后，再点击【高级配置】界面，可以进行同步方式、处理方式配置，如下图所示：

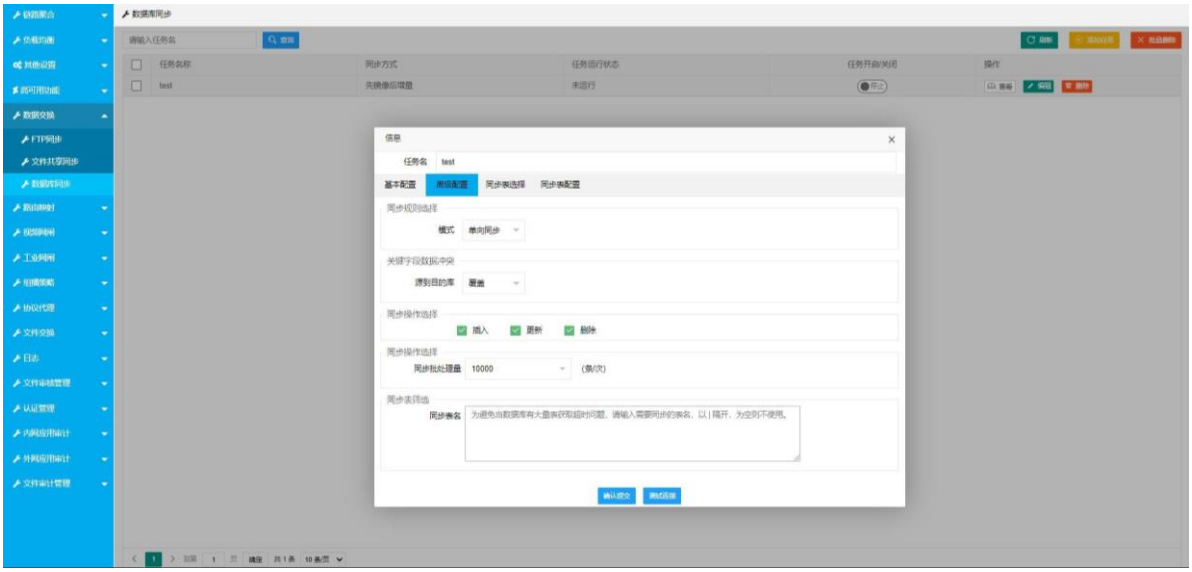


图 5.5.3.2-2 高级配置界面

高级配置参数说明：

1. 同步规则选择：

单向同步：默认，仅支持源数据库到目的数据库数据同步

双向同步：支持数据库双向同步

2. 关键字段冲突（此功能只支持新增操作）：

丢弃：源表新增数据与目的表数据存在主键冲突，该冲突数据不同步

覆盖：源表新增数据与目的表数据存在主键冲突，源表数据覆盖目的表数据

3. 同步操作选择：

插入：支持新增同步

更新：支持更新同步

删除：支持删除同步

4. 同步批处理量：单次同步的数据量，单位：N 条/次

5. 同步表筛选：当源库存在大量表时，可进行同步表筛选方便表查找，配置表名后，需要重新点击测试连接[高级配置]完成→点击[同步表选择]（加载数据时间长为正常现象请耐心等待）→勾选需要同步

的表，如下图所示：

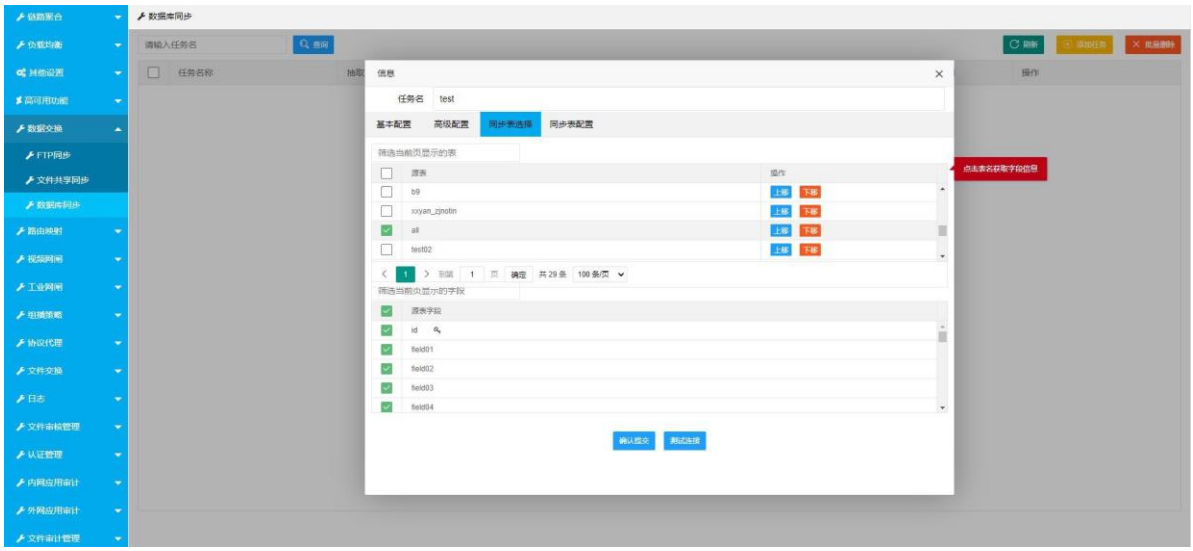


图 5.5.3.2-3 同步表选择界面

同步表选择配置参数说明：

- 源表：选择源端同步表
- 源表字段：选择源表的同步字段
- 操作：上移：同步表上移；下移：同步表下移

▵**Tips：**源表和目的表为无主键表时，需要手动设置主键，否则在任务中无法选择。

[同步表选择]完成→点击[同步表配置]（加载数据时间长为正常现象请耐心等待），如下图所示：

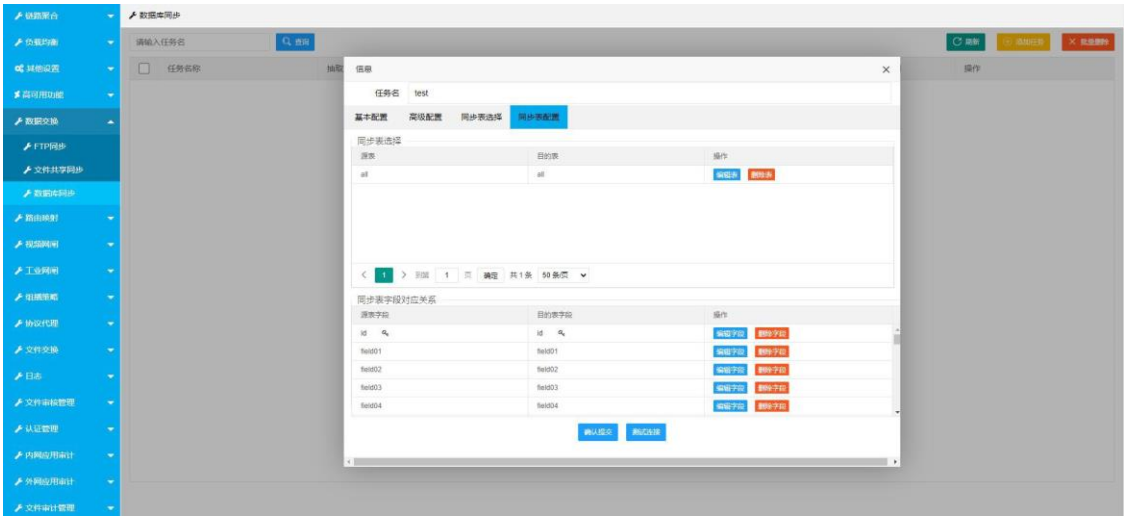


图 5.5.3.2-4 数据库同步基本配置界面

同步表配置参数说明：

编辑表：可以手动选择需要同步的目的表

删除表：可以手动选择需要删除的目的表

编辑字段：可以手动选择需要同步的表字段

删除字段：可以手动选择需要删除的表字段

5.5.3.3 编辑任务

当需要修改任务参数时，只需要选中任务信息，点击编辑，输入想要替换的参数。

▵**Tips**: 当数据库同步任务状态显示“已启动”时，无法对该同步任务进行修改、删除操作。

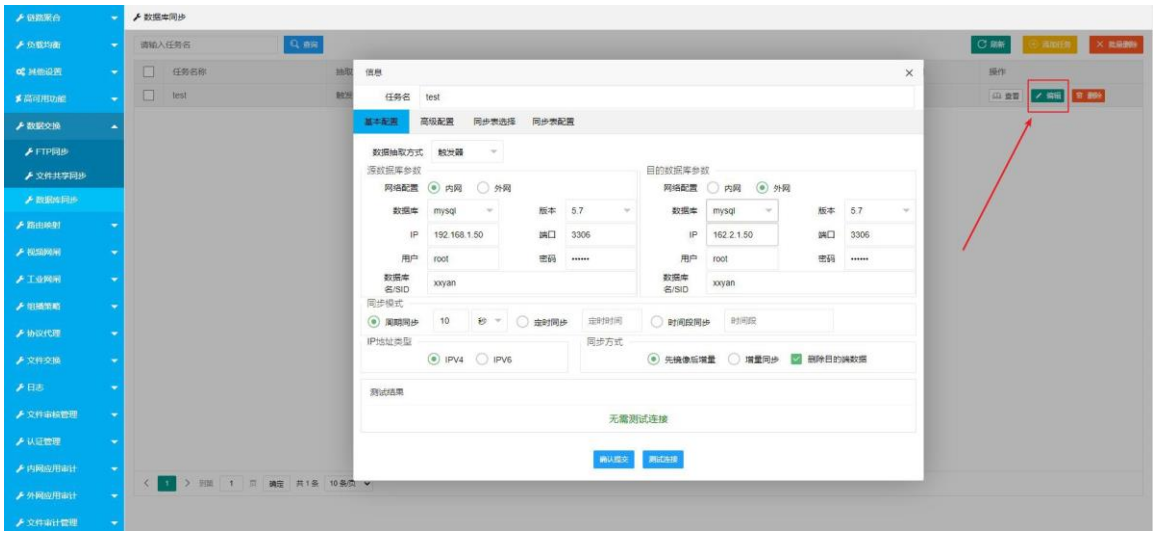


图 5.5.3.3-1 编辑任务界面

5.5.3.4 查看、删除任务

需要查看任务信息或者删除任务时，只需要点击任务列表的【查看】或【删除】按钮即可进行相应操作，如下图所示：

图 5.5.3.4-1 查看或删除

5.5.3.5 保存基本配置页面信息

数据库同步基本配置页面填写好→点击右上方的×，弹出提示窗口→点击保存或关闭→完成基本配置的暂存工作，当下次点击添加任务时，该配置页面会弹出，如下图所示：

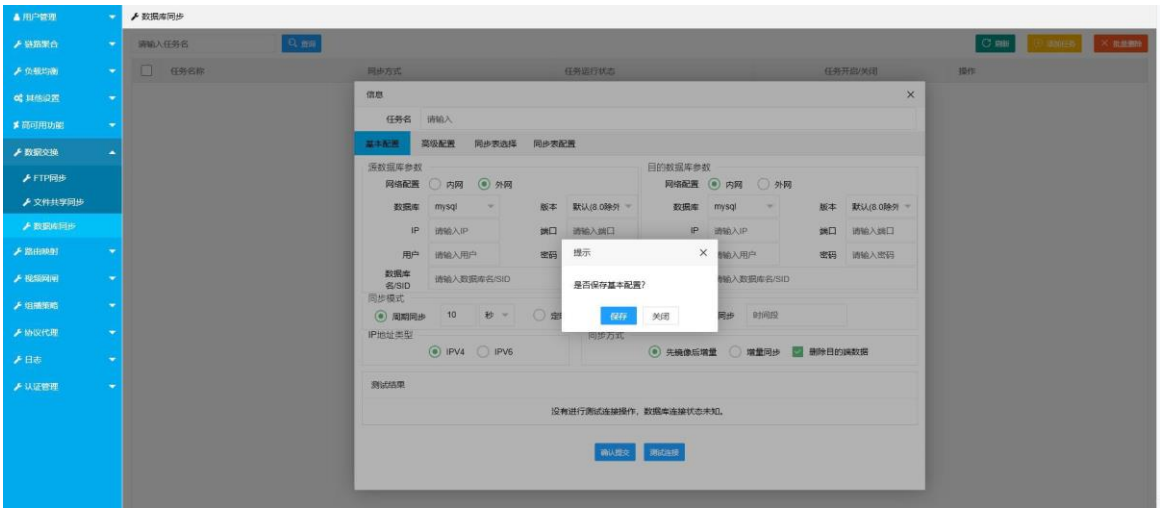


图 5.5.3.5-1 保存基本配置信息

5.6 路由映射

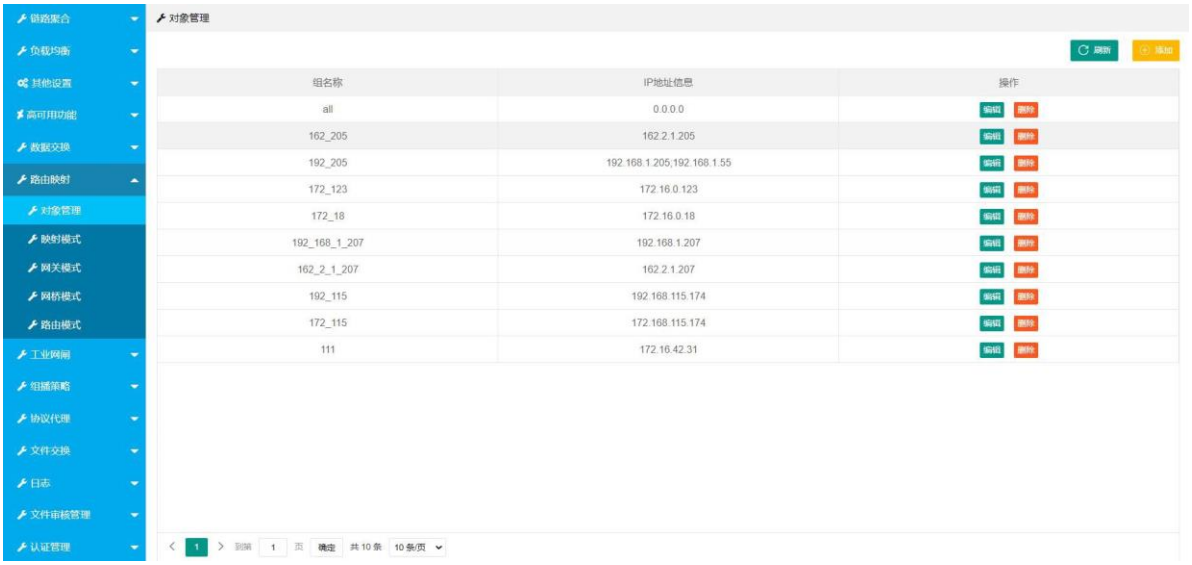
『路由映射』建立网络数据链路通道，让两个不同网络的服务器实现网络互访（只能做一端到另一端的网络访问，即 “内网到外网”、“外网到内网”；不能“内网到内网”，或者“外网到外网”）。功能包括『对象管理』、『映射模式』、『网关模式』、『网桥模式』、『路由模式』。

▵**Tips**：网桥模式与映射模式、网关模式同时使用时，规则的源对象或目的对象不能为相同网段。

5.6.1 对象管理

『对象管理』通过管理路由映射的 IP 地址；建立组，用组来管理IP 地址（组与IP 是一对多的关系），对象组表示该组中所有的 IP 都可以被映射，而且 IP 类型可以分为IPV4 和IPV6 两种类型。包括【新建组】、【编辑组】、【删除组】等操作。

系统管理操作界面→点击『路由映射』→点击『对象管理』进入到对象管理配置操作界面。如下图所示：



组名称	IP地址信息	操作
all	0.0.0.0	编辑 删除
162_205	162.2.1.205	编辑 删除
192_205	192.168.1.205,192.168.1.55	编辑 删除
172_123	172.16.0.123	编辑 删除
172_18	172.16.0.18	编辑 删除
192_168_1_207	192.168.1.207	编辑 删除
162_2_1_207	162.2.1.207	编辑 删除
192_115	192.168.115.174	编辑 删除
172_115	172.168.115.174	编辑 删除
111	172.16.42.31	编辑 删除

图 5.6.1-1 对象管理配置操作界面

5.6.1.1 新建对象

对象管理操作配置界面→点击添加，弹出添加组对话框→输入需映射的用户组名称及 IP地址信息→点击提交，完成新建组操作。如下图所示：

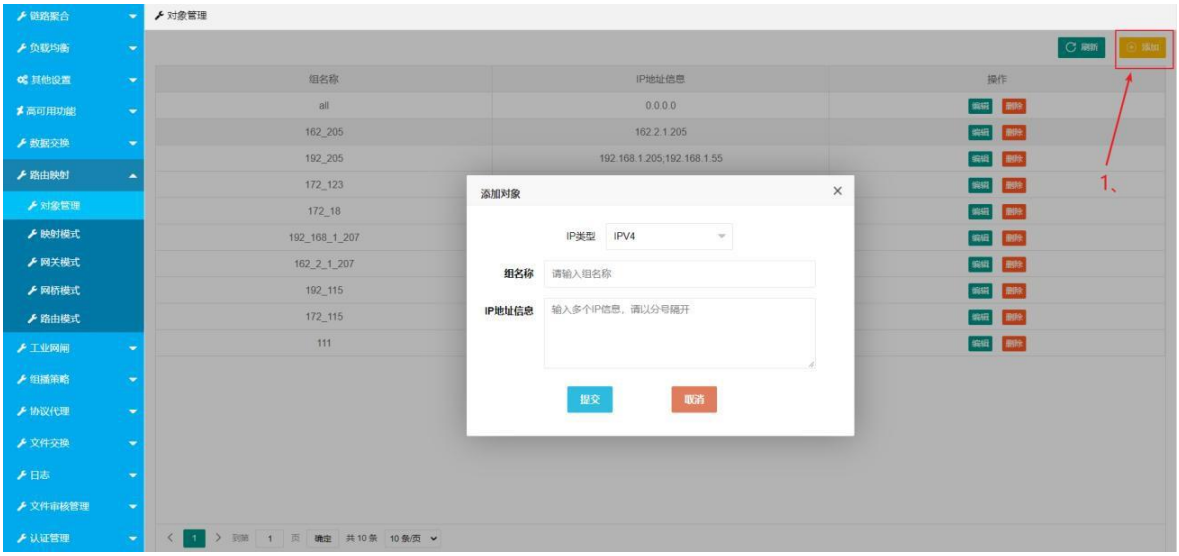


图 5.6.1.1-1 新建组对话框

新建对象配置参数说明：

1. IP 类型：选择新增对象的地址类型（IPV4 和IPV6 使用功能不同且有限制）
2. 组名称：可以包含数字、字母和下划线，最多 50 个字符（必填项）
3. IP 地址信息：支持单个IP、多个IP、子网格式IP 和范围IP。IPV6 暂不支持网段对象

- 单个IP：192.168.10.11
- 多个IP： “;”号隔开，例如：172.168.10.10;192.168.10.10
- 子网格式：192.168.2.0/24
- 范围IP：192.168.3.10-192.168.3.30

5.6.1.2 编辑对象

对象管理操作配置界面→选中需编辑的组→点击编辑，出现编辑对象管理界面→参照新建组说明要求，修改参数→点击提交，完成修改组操作。如下图所示：

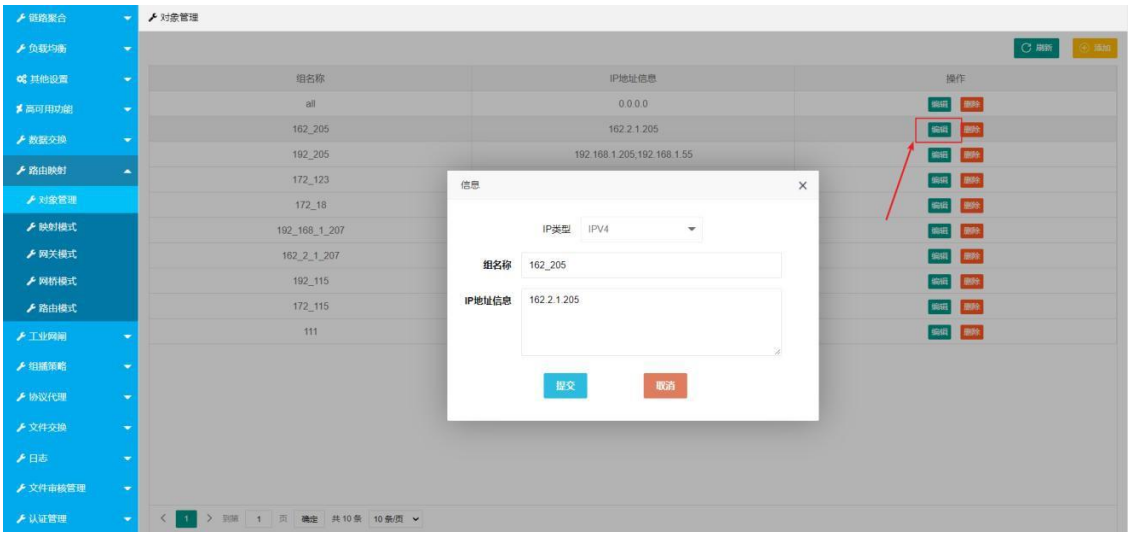


图 5.6.1.2-1 修改组信息对话框

5.6.1.3 删除对象

对象管理操作配置界面→选中需删除的组→点击删除，弹出提示窗口→点击确定，完成删除组操作。如下图所示：

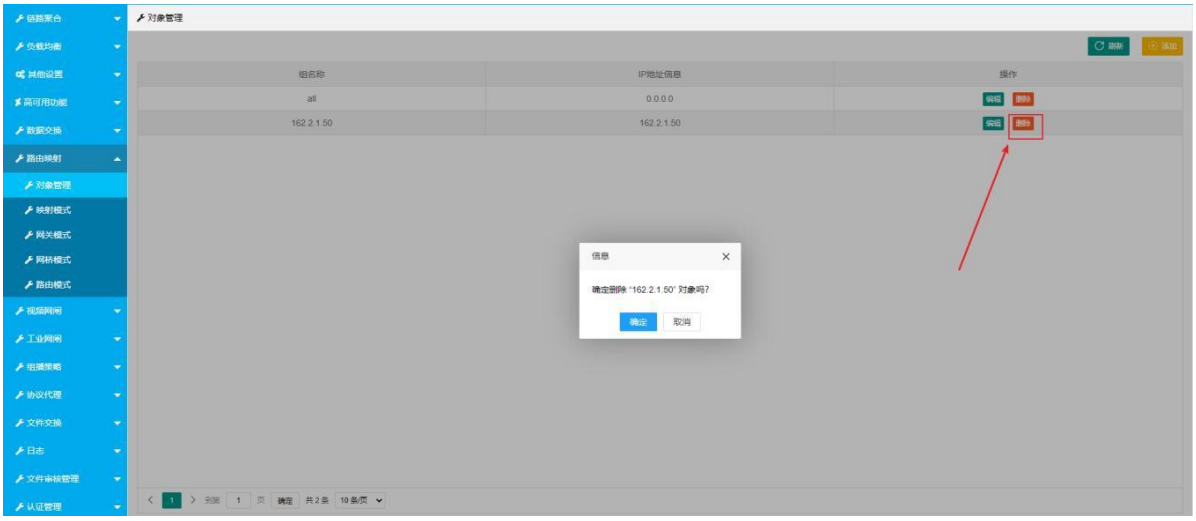


图 5.6.1.3-1 删除组提示窗口

5.6.2 映射模式

映射模式提供内（外）网到外（内）网通过映射方式（PNAT）访问，这种模式把目的IP 和端口转化为网闸外（内）端的虚拟 IP。包括【添加】、【修改】、【删除】等操作。

系统管理操作界面→点击『路由映射』→点击『映射模式』进入到映射模式操作界面； 如下图所示：

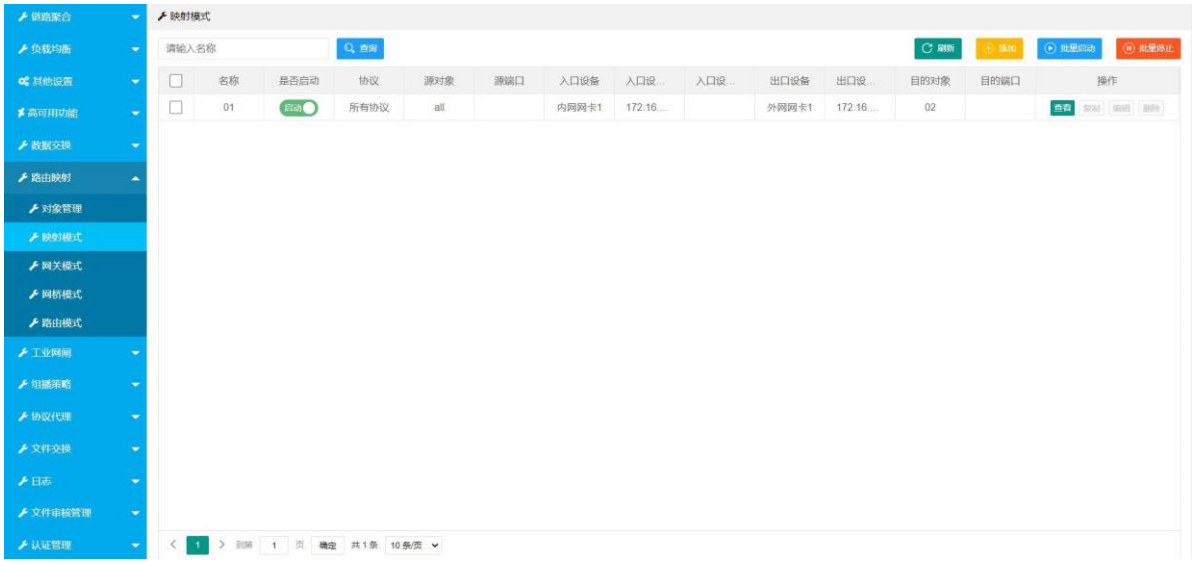


图 5.6.2-1 映射模式操作界面

映射模式操作界面配置参数说明：

- 添加：添加映射模式
- 编辑：修改映射模式信息（任务开启状态下无法编辑）
- 删除：删除映射模式
- 刷新：刷新当前页面
- 查询：输入名称进行检索查询
- 是否启动：开关任务状态
- 批量启动：批量启动任务状态
- 批量停止：批量停止任务状态

5.6.2.1 添加

映射模式操作界面→点击添加，弹出新增映射模式对话框→按要求配置相关参数→点击提交，完成添加映射模式操作。如下图所示：

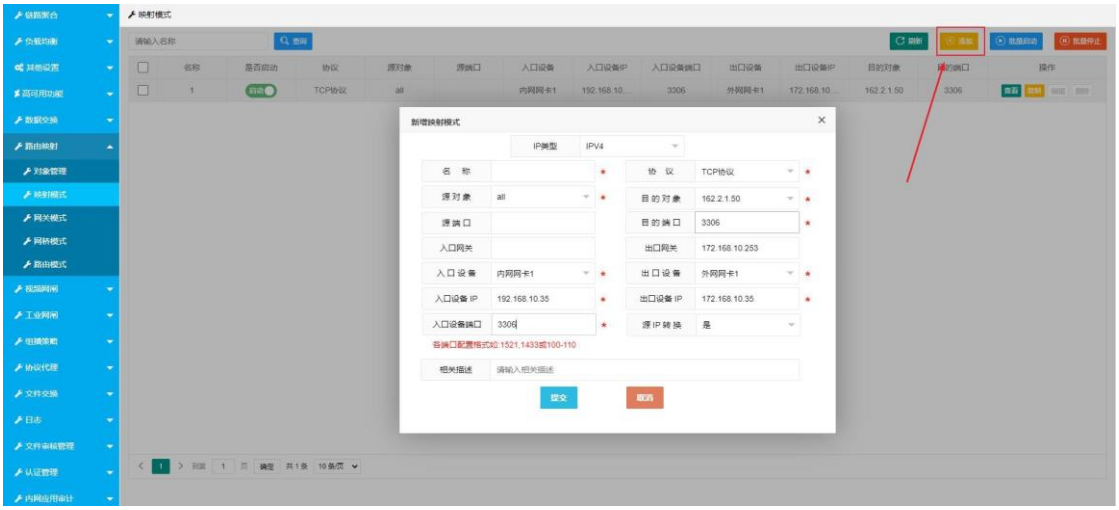


图 5.6.2.1-1 添加映射模式对话框

添加映射模式配置参数说明：

- IP 类型：可选IPV4 和IPV6 两种类型
- 名称：可以包含数字、字母、下划线，最多 16 个字符（必填项）
- 协议选择：所有协议、TCP 协议、UDP 协议、ICMP 协议、FTP 协议、H323 协议、TFTP 协议
- 源对象：源组（下拉选择）
- 目的对象：目的组（下拉选择）
- 目的端口：目的对象地址的端口号
- 入口网关：如果与源对象之间存在三层交换机，需要填入网关地址
- 出口网关：如果与目的对象之间存在三层交换机，需要填入网关地址
- 入口设备：入口网卡信息（下拉选择）
- 出口设备：出口网卡信息（下拉选择）
- 入口设备IP：入口网卡IP 地址（推荐使用虚拟IP）
- 出口设备IP：出口网卡IP 地址（推荐使用虚拟IP）
- 入口设备端口：入口网卡端口号

5.6.2.2 编辑

映射模式操作界面→选中需修改的映射模式→点击修改→修改参数→点击提交，完成修改映射模式操作如下图所示：

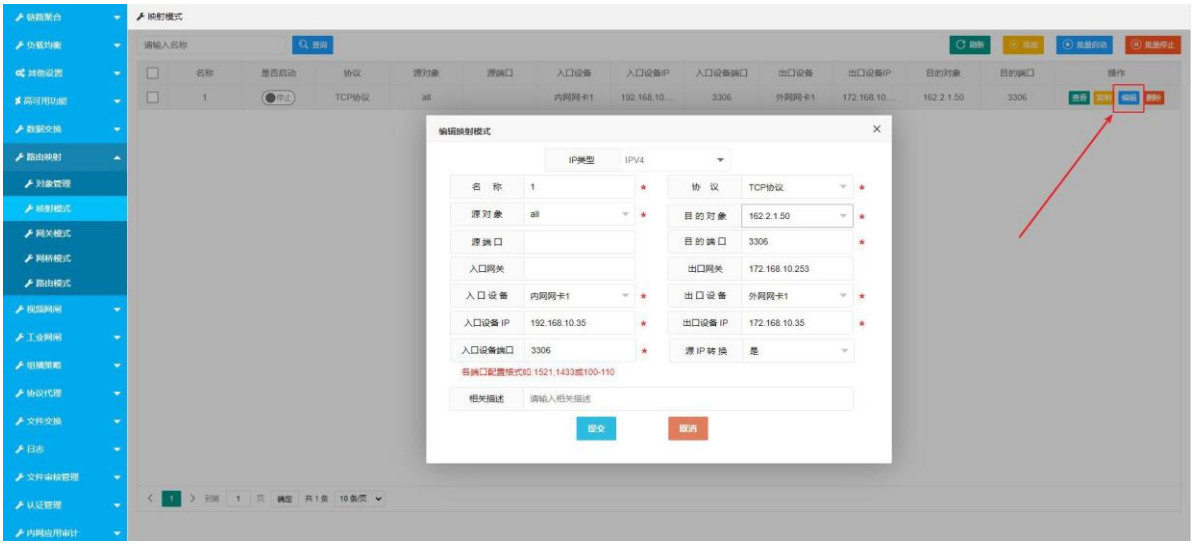


图 5.6.2.2-1 修改映射模式对话框

5.6.2.3 删除

映射模式操作界面→选中需删除的映射模式→点击删除，弹出提示窗口→点击确定，完成删除映射模式操作。如下图所示：

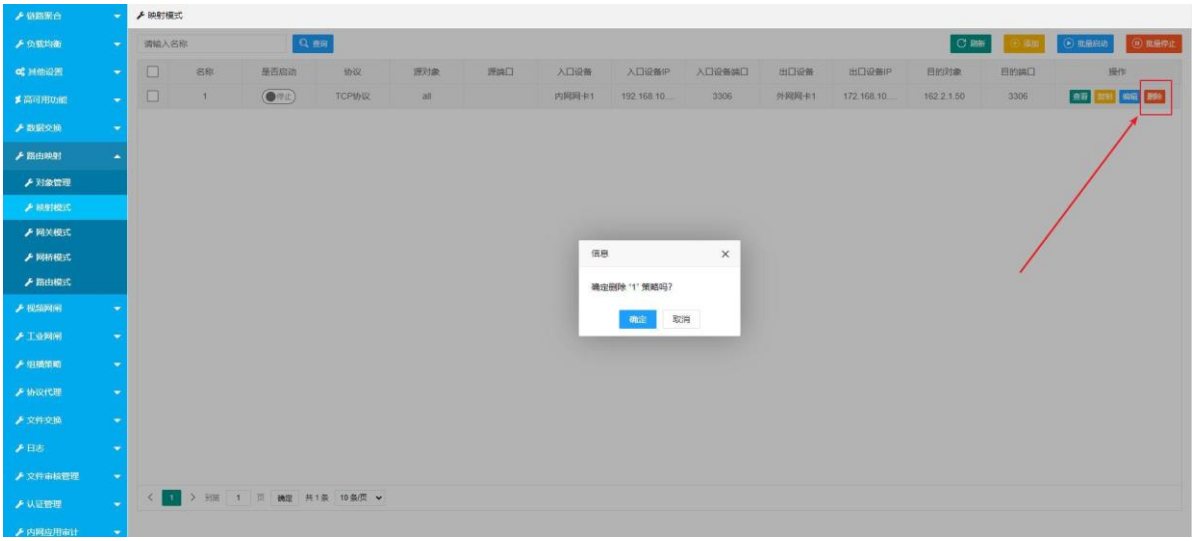


图 5.6.2.3-1 删除映射模式提示窗口

5.6.3 网关模式

网关模式提供内（外）网到外（内）网通过网关模式（NAT）访问，这种模式下所有的源地址经过了SNAT（源地址转换）。包括【添加】、【修改】、【删除】等操作。

系统管理操作界面→点击『路由映射』→点击『网关模式』进入到网关模式操作界面； 如下图所示：

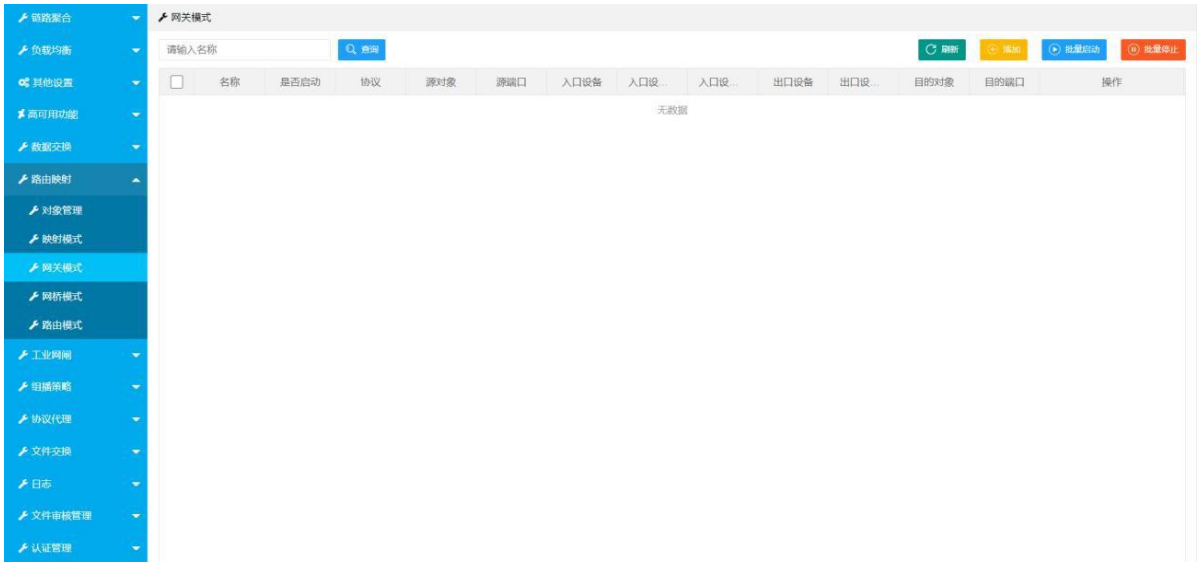


图 5.6.3-1 网关模式操作界面

5.6.3.1 添加

网关模式操作界面→点击添加，弹出添加网关模式对话框。如下图所示：

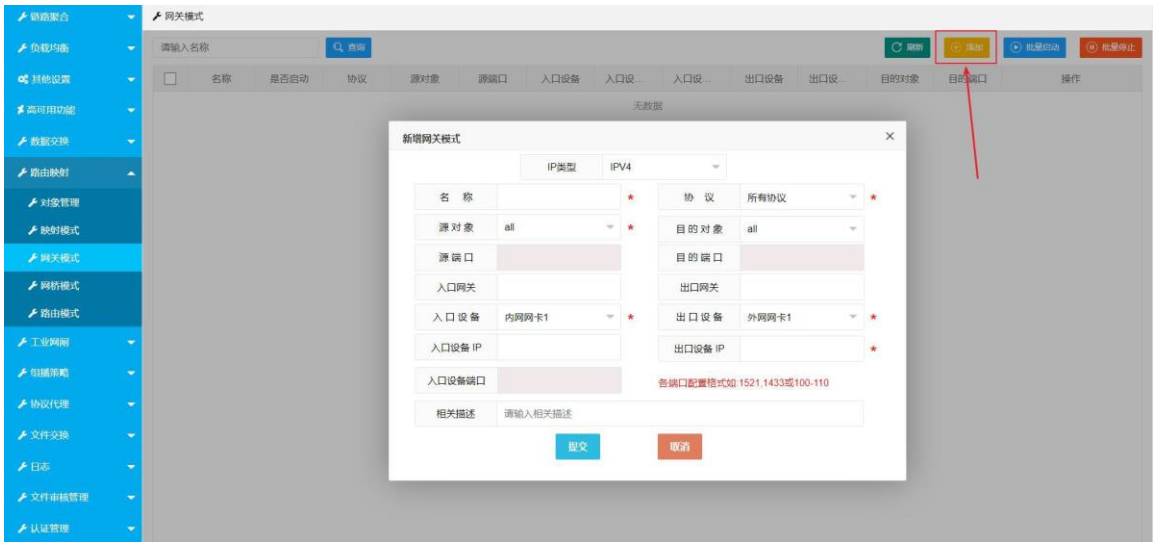


图 5.6.3.1-1 添加网关模式对话框

添加网关模式配置参数说明：

1. IP 类型：当源和目的对象为 IPV4 地址类型时选择IPV4，当源和目的对象为IPV6 地址类型时选择IPV6。一个任务中参数同时只能选择一种类型。
2. 名称：可以包含数字、字母、下划线，最多 16 个字符（必填项）
3. 协议选择：所有协议、TCP 协议、UDP 协议、ICMP 协议、FTP 协议、H323 协议、TFTP 协议
4. 源对象：源组（下拉选择）

5. 目的对象：目的组（下拉选择）
6. 目的端口：目的对象地址的端口号
7. 入口网关：如果与源对象之间存在三层交换机，需要填入网关地址；
8. 出口网关：如果与目的对象之间存在三层交换机，需要填入网关地址；
9. 入口设备：入口网卡信息（下拉选择）
10. 出口设备：出口网卡信息（下拉选择）
11. 入口设备IP：入口网卡IP 地址（推荐使用虚拟IP）
12. 出口设备IP：出口网卡IP 地址（推荐使用虚拟IP）
13. 入口设备端口：入口网卡端口号（多个时用“,”或者“-”分隔）

5.6.3.2编辑

网关模式操作界面→选中需修改的网关模式→点击编辑，出现编辑网关模式对话框→按照添加网关模式说明配置新的参数→点击提交，完成修改网关模式操作。IP 类型无法编辑更换。如下图所示：

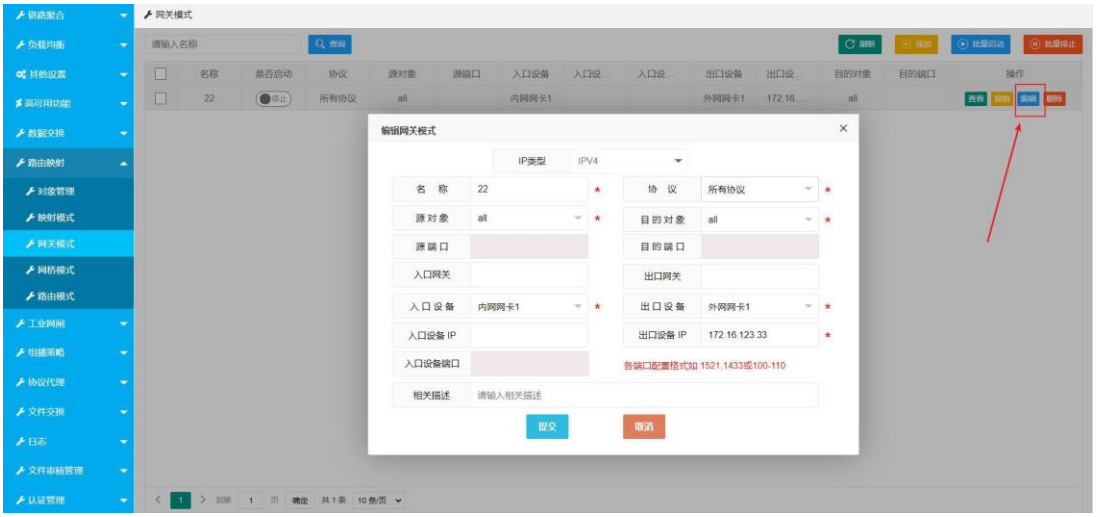


图 5.6.3.2-1 修改网关模式对话框

5.6.3.3 删除

网关模式操作界面→选中需删除的网关模式→点击删除，弹出提示窗口→点击确定，完成删除网关模式操作如下图所示：

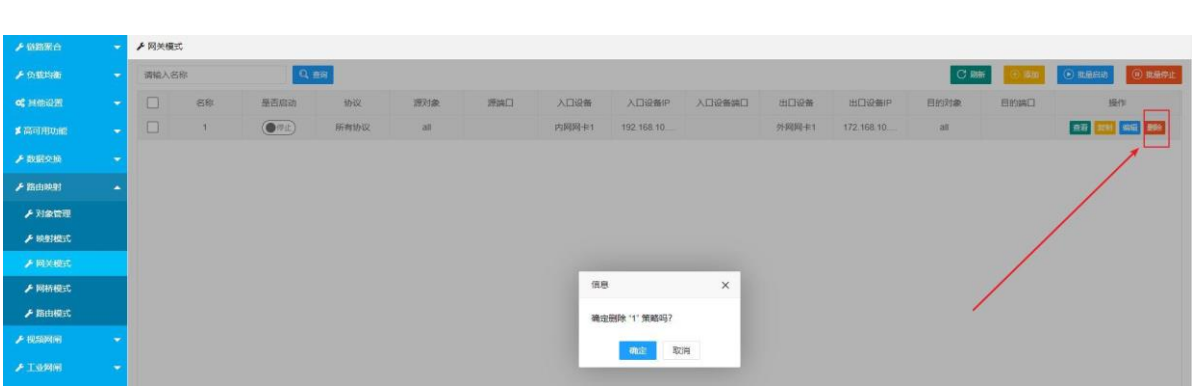


图 5.6.3.3-1 删除网关模式提示窗口

5.6.4 网桥模式

网桥模式提供内（外）网到外（内）网的透明代理（Transparent Proxy）访问，这种模式下保留源地址的真实 IP。包括【添加】、【修改】、【删除】等操作。

系统管理操作界面→点击『路由映射』→点击『网桥模式』进入到网桥模式操作界面； 如下图所示：

图 5.6.4-1 网桥模式配置窗口

网桥模式配置参数说明：

- 添加：添加映射模式
- 编辑：修改映射模式信息（任务开启状态下无法编辑）
- 删除：删除映射模式
- 刷新：刷新当前页面
- 查询：输入名称进行检索查询
- 是否启动：开关任务状态
- 批量启动：批量启动任务状态
- 批量停止：批量停止任务状态

5.6.4.1 添加

网桥模式操作界面→点击添加，弹出添加网桥模式对话框，如下图所示：

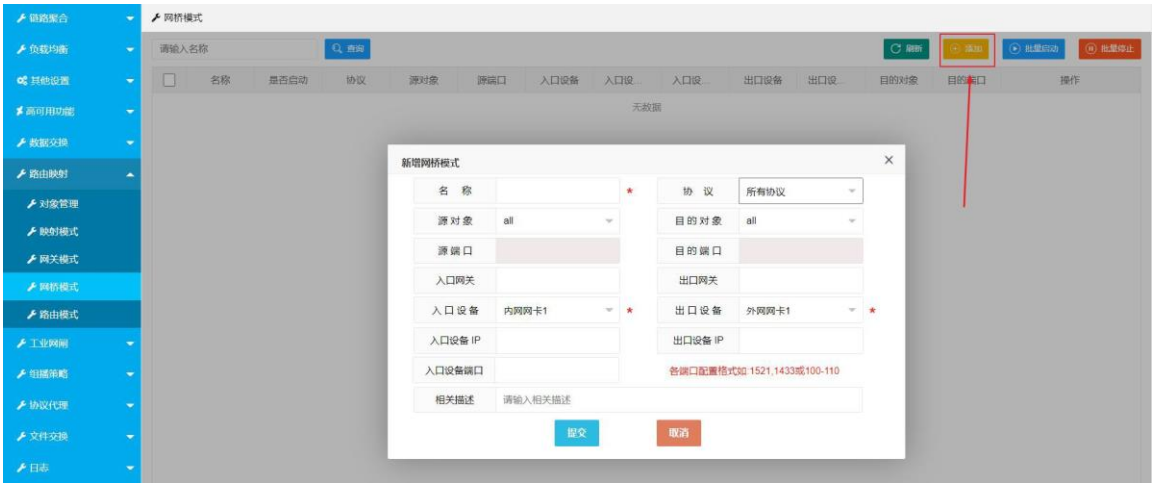


图 5.6.4.1-1 添加网桥模式对话框

配置参数说明：

- 名称：可以包含数字、字母、下划线，最多 16 个字符（必填项）
- 协议选择：协议选择：所有协议、TCP 协议、UDP 协议、ICMP 协议、FTP 协议、H323 协议、TFTP 协议
- 源对象：源组（下拉选择）
- 目的对象：目的组（下拉选择）
- 入口设备：入口网卡信息（下拉选择）
- 出口设备：出口网卡信息（下拉选择）

5.6.4.2 编辑

网桥模式操作界面→选中需修改的网桥模式→点击编辑，修改参数→点击提交，完成修改网桥模式操作。如下图所示：

图 5.6.4.2-1 编辑网桥模式对话框

5.6.4.3 删除

网桥模式操作界面→选中需删除的网桥模式→点击删除，弹出提示窗口→点击确定，完成删除网桥模式操作。如下图所示：

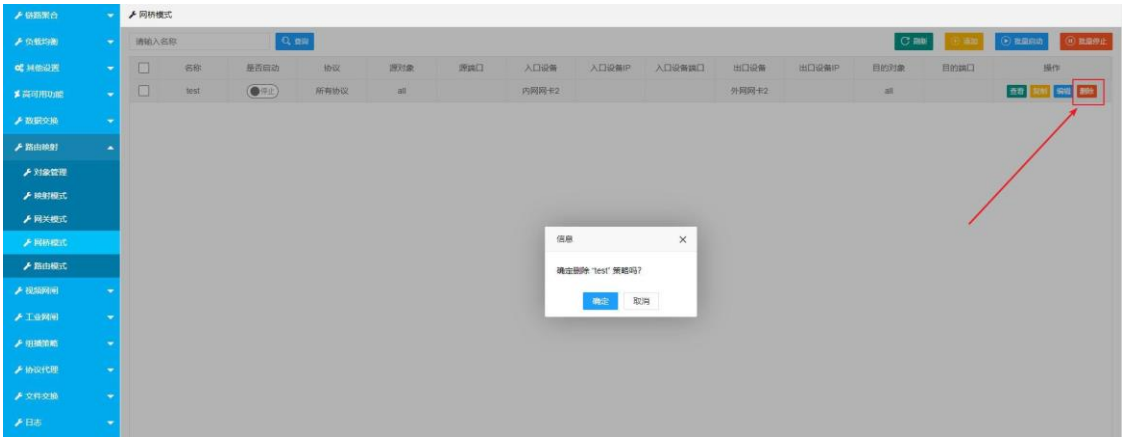


图 5.6.4.3-1 删除网桥模式提示窗口

5.6.5 路由模式

路由模式提供内（外）网到外（内）网通过纯路由方式代理访问，这种模式不会 NAT 转换，但是需要在源和目的服务器分别添加路由下一跳指定入口设备 IP 或出口设备IP。包括【添加】、【修改】、【删除】等操作。

系统管理操作界面→点击『路由映射』→点击『路由模式』进入到路由模式操作界面； 如下图所示：

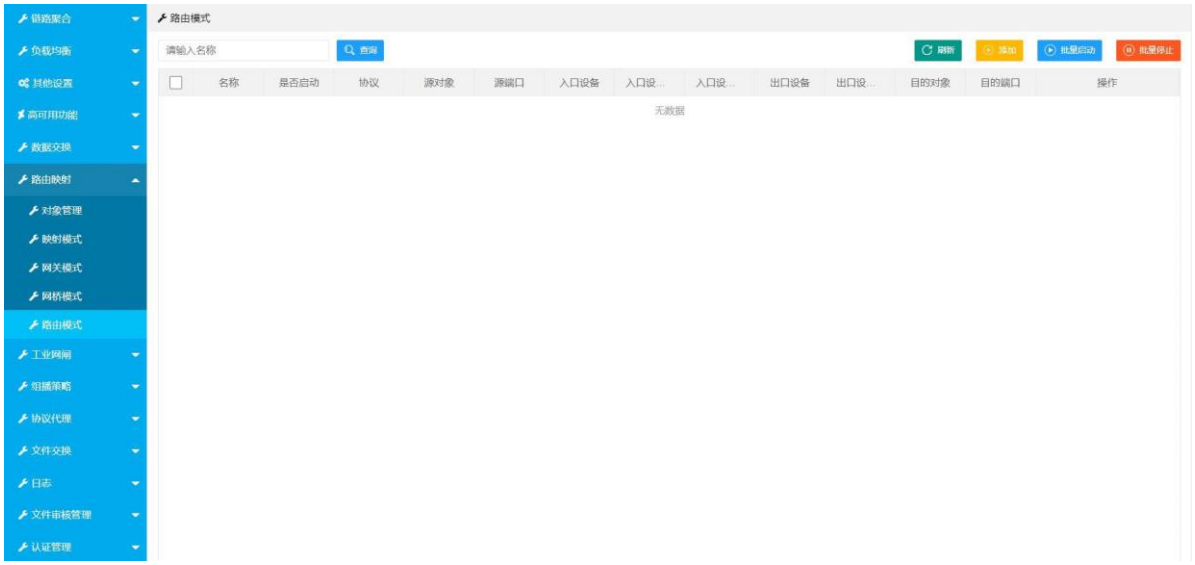


图 5.6.5-1 路由模式操作界面

路由模式配置参数说明：

- 添加：添加路由模式
- 编辑：修改路由模式信息（任务开启状态下无法编辑）
- 删除：删除路由模式
- 刷新：刷新当前页面
- 查询：输入名称进行检索查询
- 是否启动：开关任务状态
- 批量启动：批量启动任务状态
- 批量停止：批量停止任务状态

5.6.5.1 添加

路由模式操作界面→点击添加，弹出添加路由模式对话框→按要求配置相关参数→点击提交，完成添加路由模式操作，如下图所示：

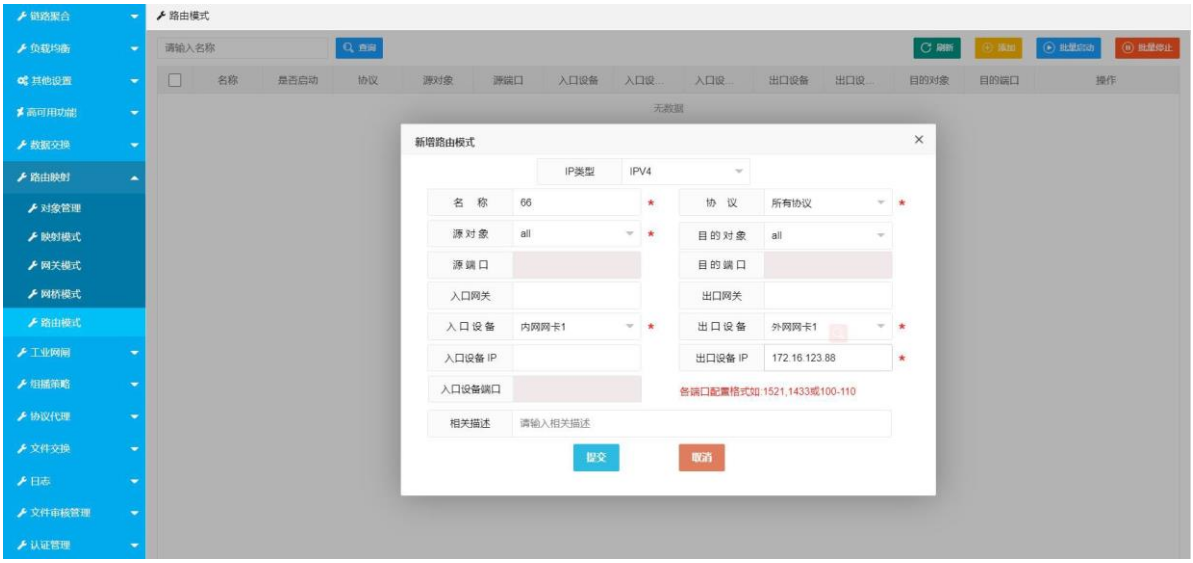


图 5.6.5.1-1 添加路由模式对话框

添加路由模式配置参数说明：

- 名称：可以包含数字、字母、下划线，最多 16 个字符（必填项）
- 协议选择：协议选择：所有协议、TCP 协议、UDP 协议、ICMP 协议、FTP 协议、H323 协议、TFTP 协议
- 源对象：源组（下拉选择）
- 目的对象：目的组（下拉选择）
- 入口网关：如果与源对象之间存在三层交换机，需要填入网关地址；
- 出口网关：如果与目的对象之间存在三层交换机，需要填入网关地址；
- 入口设备：入口网卡信息（下拉选择）
- 出口设备：出口网卡信息（下拉选择）

5.6.5.2 编辑

路由模式操作界面→点击编辑，弹出添加路由模式对话框→按要求配置相关参数→点击提交，完成编辑路由模式操作，如下图所示：

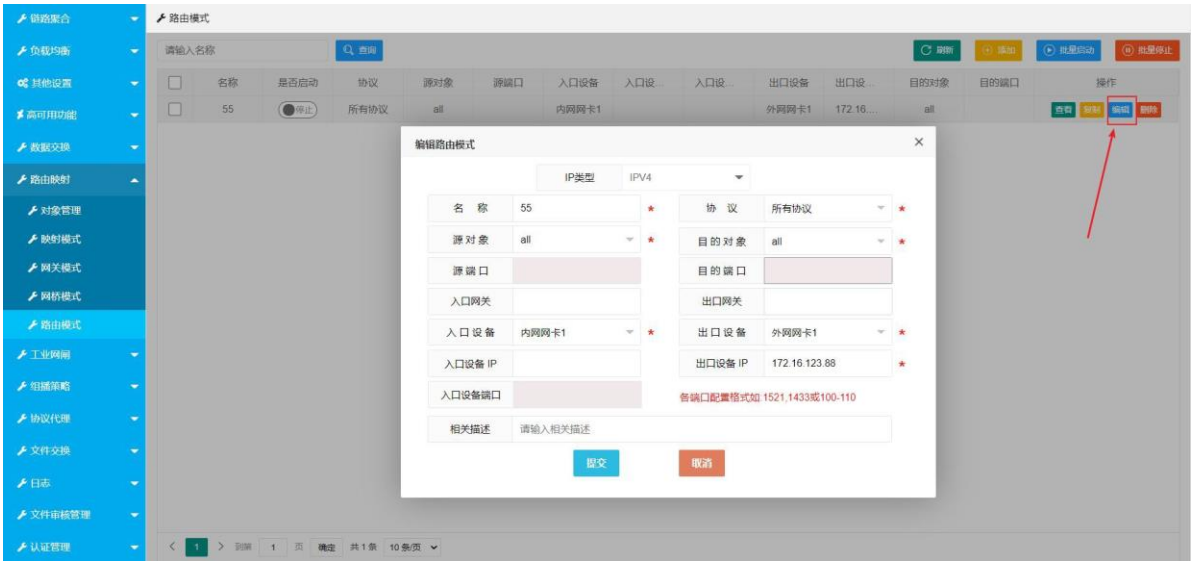


图 5.6.5.2-1 编辑路由模式对话框

5.6.5.3 删除

路由模式操作界面→选中需删除的路由模式→点击删除，弹出提示窗口→点击确定，完成删除路由模式操作。如下图所示：

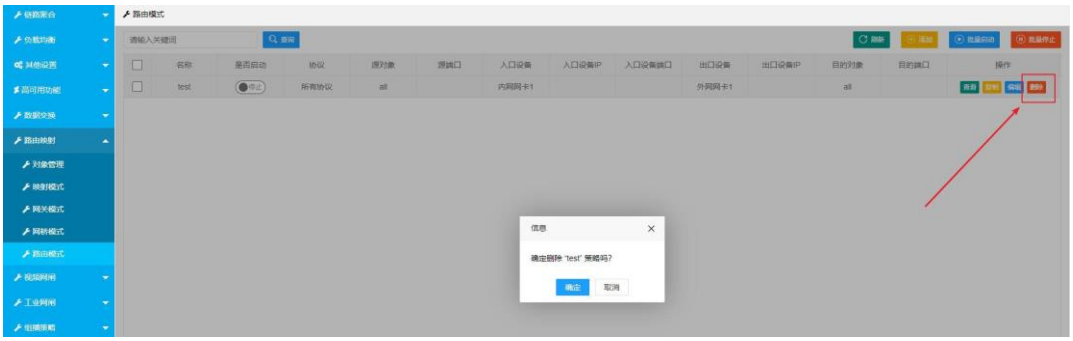


图 5.6.5.3-1 删除路由模式提示窗口

5.7 视频网闸

5.7.1 视频互联

视频互联提供SIP 协议注册、呼叫、点播和信令拦截等视频代理功能。

5.7.1.1 用户管理

用户管理可以添加上级设备的 SIP 服务器编号和下级设备的设备编号，提供给规则设置使用。

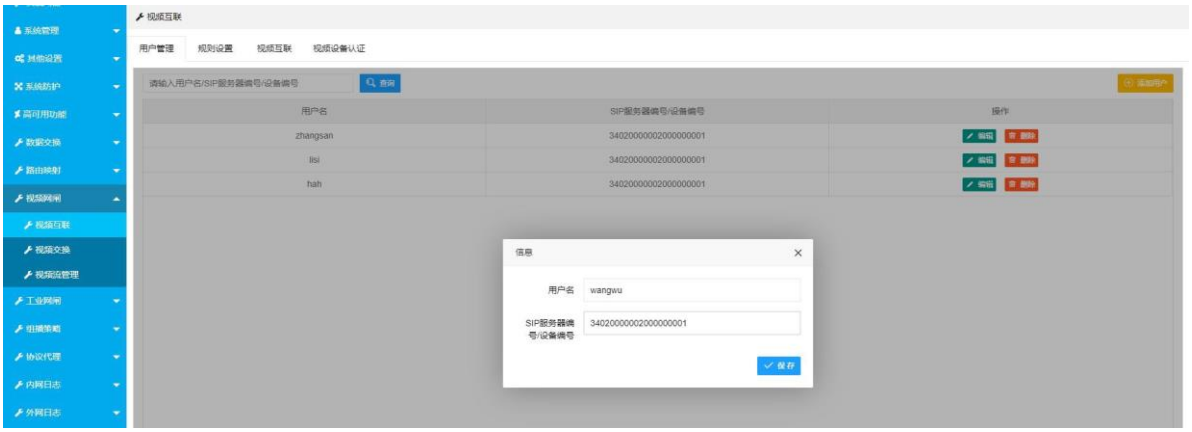


图 5.7.1.1-1 用户管理

用户管理参数说明：

- 用户名：上下级设备的用户名
- SIP 服务器编号/设备编号：上级的SIP 服务器编号或者下级的设备编号

5.7.1.2 规则设置

规则设置提供配置上下级交互规则功能，一般需要配置上级到下级和下级到上级互通， 如下图所示：

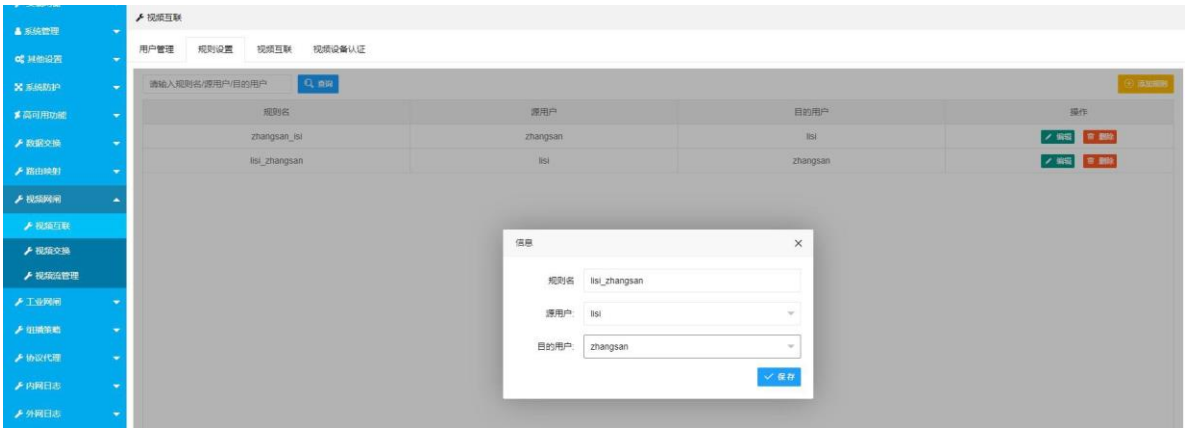


图 5.7.1.2-1 规则设置

规则设置参数说明：

- 规则名：规则的名称，由字母、数字、下划线组成
- 源用户：规则交互的源用户
- 目的用户：规则交互的目的用户

5.7.1.3 视频互联

视频互联的任务配置，如下图所示：

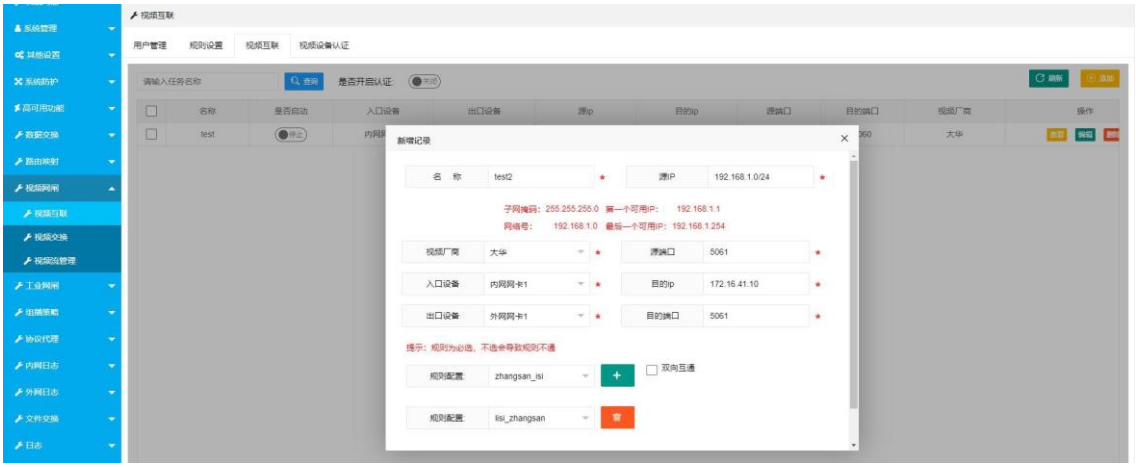


图 5.7.1.3-1 视频互联

视频互联参数说明：

- 名称：视频互联的任务名
- 源 IP：下级视频设备(ipc、nvr、dvr 等)的服务器IP（仅支持IP/网段）
- 视频厂商：包含海康、大华、华三、华为、公安一所、天地伟业、天视达、宇视、科达、数码视讯、藏愚、合众、汉邦、东方电子、中星和其他厂商
- 源端口：下级服务器的信令端口
- 入口设备：与下级服务器连接的网口
- 目的IP：上级服务器信令IP
- 出口设备：与上级服务器连接的网口
- 目的端口：上级服务器的信令端口
- 规则配置：在5.5.1.2 中的规则设置中添加后选择（一般需选两条规则：上级至下级； 下级至上级）
- 双向互通：勾选此项，规则配置只需选择一条规则

5.7.1.4 视频设备认证

视频设备认证提供上下级服务设备黑白名单控制功能。开启白名单时，只有白名单设备拥有注册和点播权限；开启黑名单时除黑名单用户外均拥有注册和点播权限（系统默认开启黑名单但不设置 IP，即默认放行所有IP）。配置如下图所示：

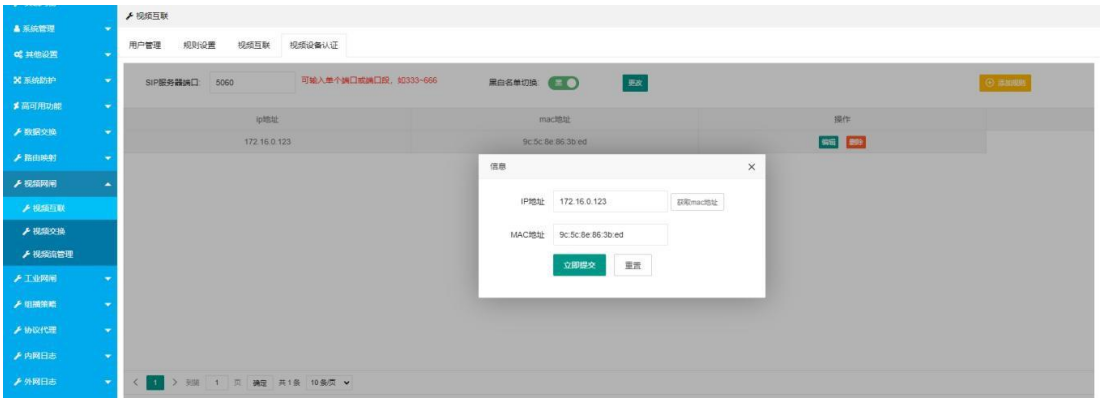


图 5.7.1.4-1 视频设备认证

视频设备认证参数说明：

- IP 地址：上级、下级信令 IP 地址
- MAC 地址：上级、下级设备的MAC 地址，跨交换机的即获取网关 MAC 地址
- 规则位置：规则生效位置；内网规则仅在内网生效，外网规则在外网生效

5.7.2 视频交换

根据GB28181 要求，独立研发了视频网闸，对应用服务区进入内网的数据进行协议剥离。视频数据（即经压缩编码且通过视频协议传输的二进制数据）和控制信令（即设备间建立会话并控制视频传输的一系列协议、命令和指令的总称）通过专用数据块的方式“摆渡”传输， 实现内网和应用服务区之间的安全数据交换。视频网闸断开内外网 TCP/IP 连接，视频数据和控制信令数据采取不同的传输方式传输，信令采取双向传输，视频流采用单向传输。既确保数据安全传输，也能确保视频服务质量。

5.7.2.1 基本配置

基本配置页面，通信网口配置默认 eth1 网卡，视频协议默认 SIP 协议，端口 5060，网闸模式支持两种模式，选择完提交即可。如下图所示：

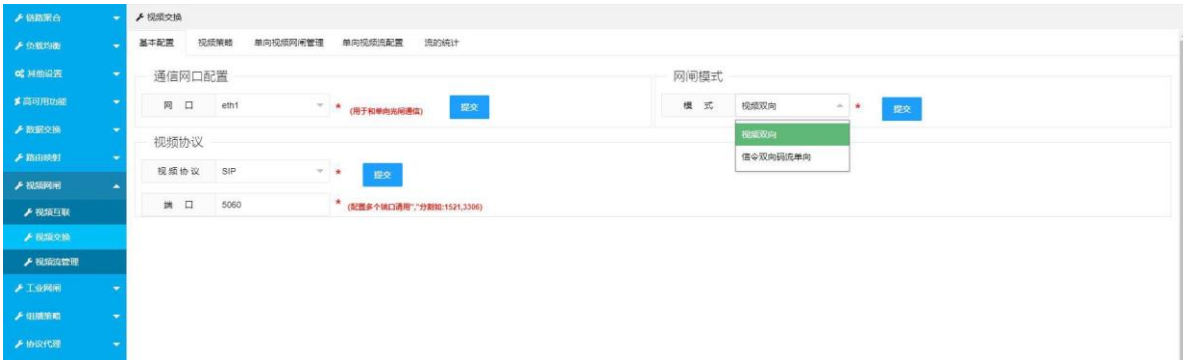


图 5.7.2.1-1 视频交换基本配置

视频交换配置参数说明：

- 通信网口配置：选择网闸外网和单向光闸通信的网卡（外网），用于下发规则，当“网闸模式”选择[信令双向码流单向]时才需配置
- 网闸模式：支持视频双向、信令双向码流单向
- 视频协议：支持sip 和rtsp 协议
- 端口：上下游信令服务器端口

5.7.2.2 视频策略

视频策略可配置信令服务器交互规则，根据部署场景选择代理模式、路由模式、透明模式（流媒体服务器规则不需要配置）。如下图所示：

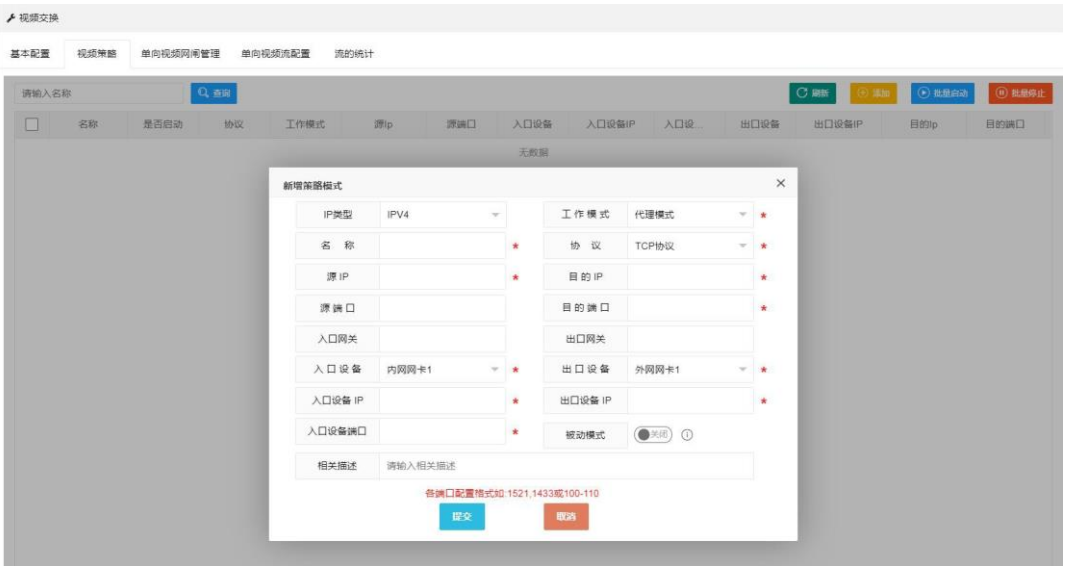


图 5.7.2.2-1 视频策略

5.7.2.3 单向视频网闸管理

当网闸模式选择[信令双向码流单向]时，才需要配置『单向视频网闸管理』。IP 需要填写单向设备的业务口 IP，端口默认:60001，如下图所示：

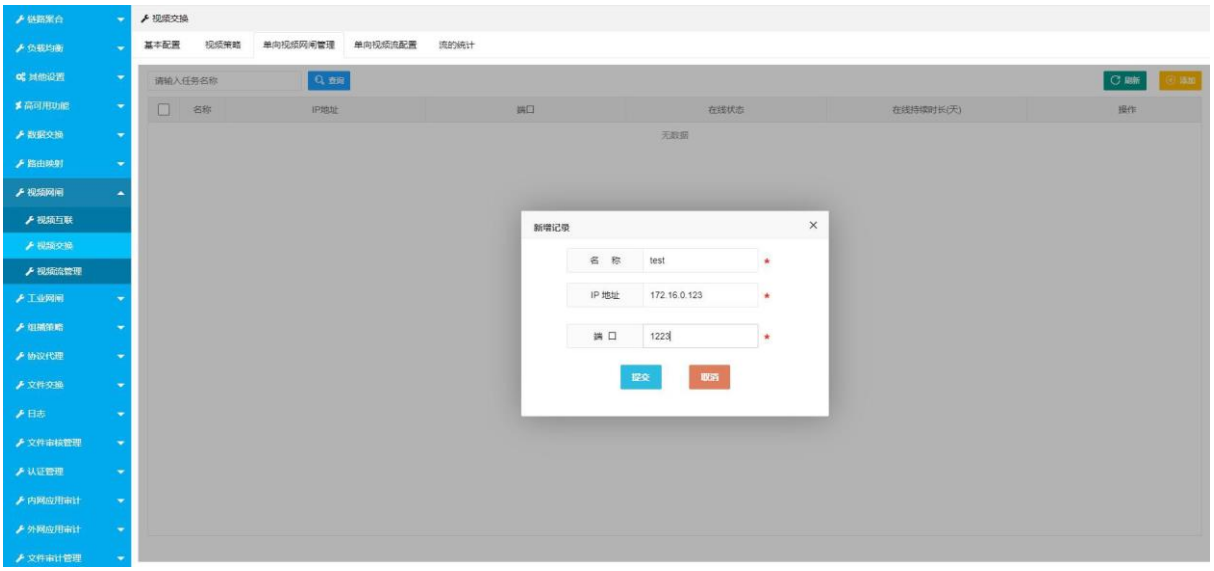


图 5.7.2.3-1 添加单向网闸

添加单向网闸配置参数说明：

- 名称：支持字母、数字、下划线
- IP 地址：填写单向光闸外网ip，格式 xxx.xxx.xxx.xxx(xxx为0-255)
- 端口：单向光闸视频服务监听端口（默认：60001）

5.7.2.4 单向视频流配置

单向视频流配置是配置网闸向光闸下发的放行规则。如下图所示：

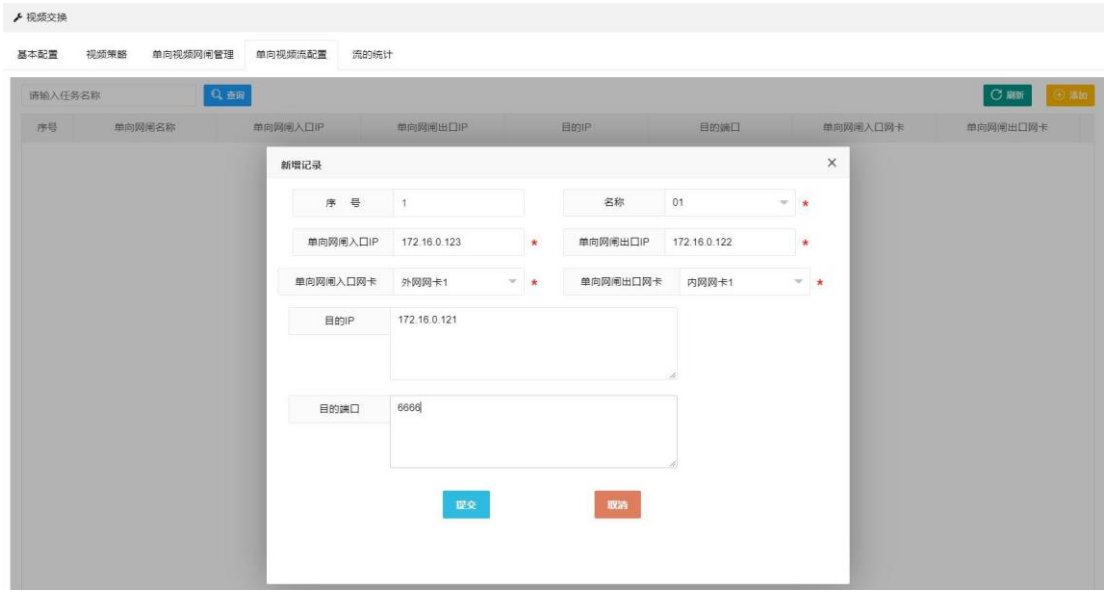


图 5.7.2.4-1 单向视频流配置任务

单向视频流配置参数说明：

- 序号：自动生成的序列号
- 名称：选择单向视频网闸管理任务的名称
- 单向光闸入口ip：ip 格式xxx.xxx.xxx.xxx(xxx为0-255)
- 单向网闸出口ip：ip 格式xxx.xxx.xxx.xxx(xxx为0-255)
- 单向网闸入口网卡：选取作为业务的网卡
- 单向网闸出口网卡：选取作为业务的网卡
- 目的IP：上游流媒体服务器的 IP 地址
- 目的端口：上游流媒体服务器端口

5.7.2.5 流的统计

流的统计，是对各信令和流数据包的统计（仅支持视频双向），如下图所示

图 5.7.2.5-1 流的统计

5.7.3 视频流管理

视频流管理支持RTSP、RTMP 协议推拉流代理功能，推流服务器推流至网闸内网或外网， 网闸将视频流转换为外网或内网其他接口的流媒体源。

5.7.3.1 流代理设置

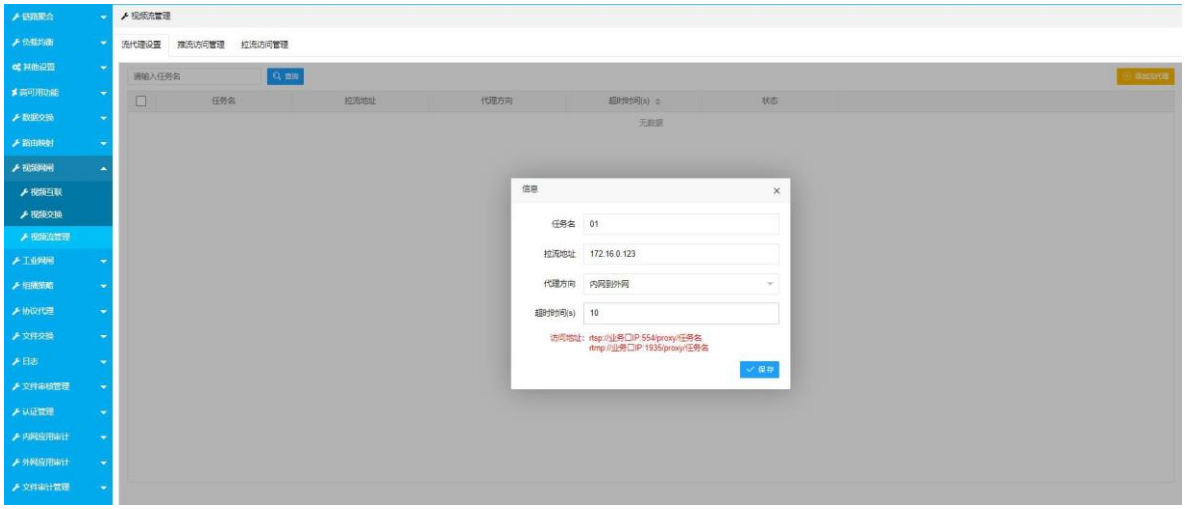


图 5.7.3.1-1 添加流代理任务

添加流代理配置参数说明：

- 任务名：任务名只能由字母、数字和下划线组成
- 拉流地址：rtsp/rtmp 推流服务器地址
- 代理方向：支持内到外代理或外到内代理
- 超时时间：拉流超时时间范围 1-60s

△**Tips：**正常开启需要先开始推流再点击页面开启任务，或者点击开启任务马上开始推流即可正常开启任务，否则就会无法正常开启任务。如下图所示：

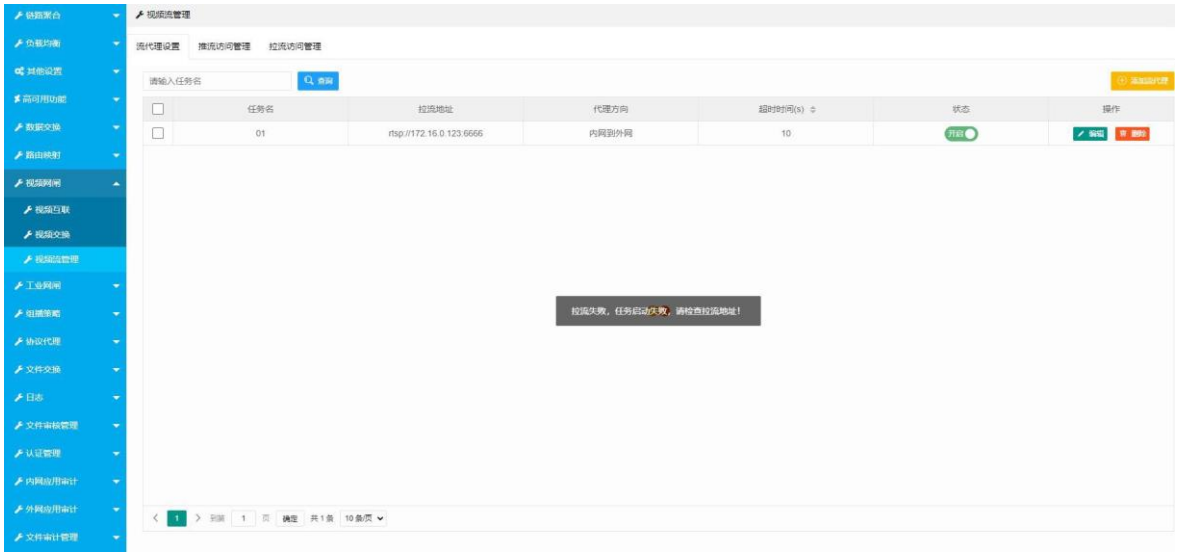


图 5.7.3.1-2 无推流任务开启失败图

5.7.3.2 推流访问管理

『推流访问管理』配置推流服务器的黑白明单，开启白名单即只有白名单上的 ip 可以推流，开启黑名单则只有上面的 ip 不可推流。

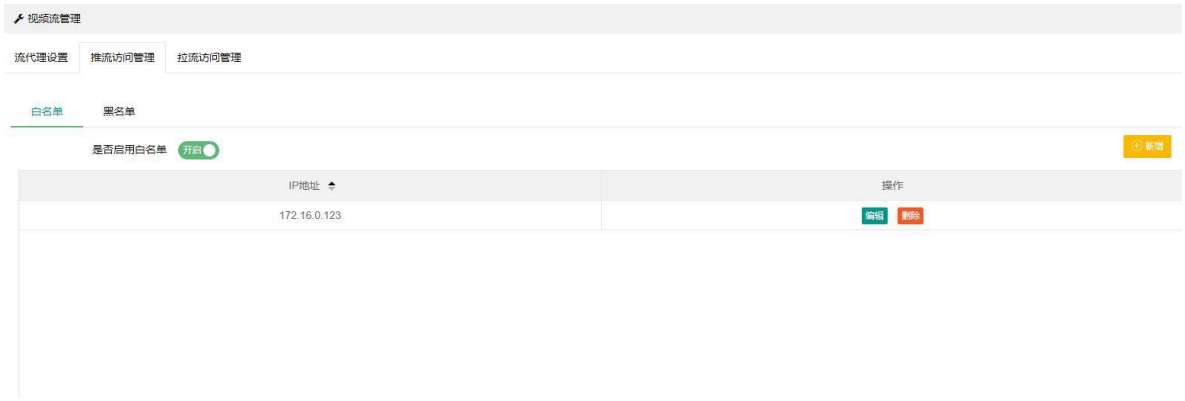


图 5.7.3.2-1 开启推流白名单

5.7.3.3 拉流访问管理

『拉流访问管理』配置拉流服务器的黑白名单。注意：若开启拉流访问管理白名单，需要将网闸出口的业务口 ip 也加入到白名单里。如下图所示：

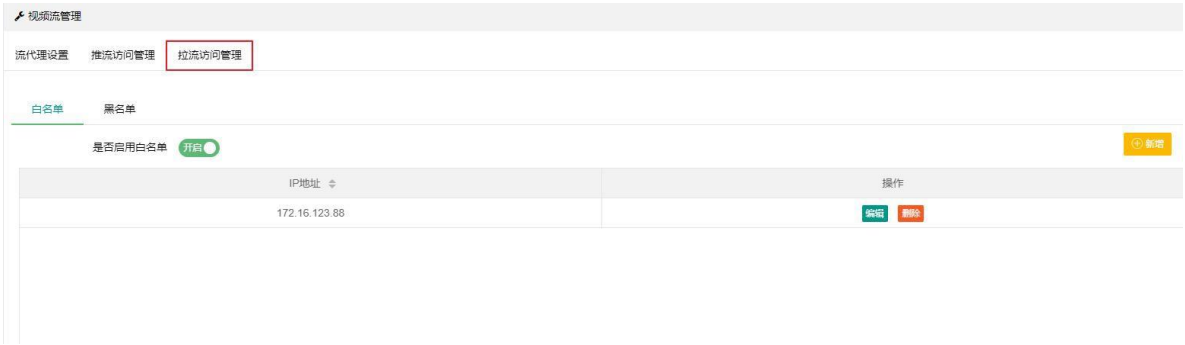


图 5.7.3.3-1 拉流白名单

5.8 工业网闸

工业控制网闸系统采用“2+1 双主机架构模式” 系统由内部处理系统、外部处理系统和专用数据通道控制系统三部分组成。专用数据传输通道控制扮演了“船闸”控制的角色，采用自主研发的 DTP 隔离技术，将内外网从物理上分开，彻底阻断了TCP/IP 协议连接，把工业控制网与以太网进行物理隔离，达到安全隔离的目的，保证传输数据的安全、可靠、稳定。支持OPC、MODBUS、S7、DNP3、IEC104 等工业协议。

5.8.1 对象管理

5.8.1.1 添加对象

点击『工业网闸』→点击『对象管理』→点击添加，进入任务配置页面，如下图所示：

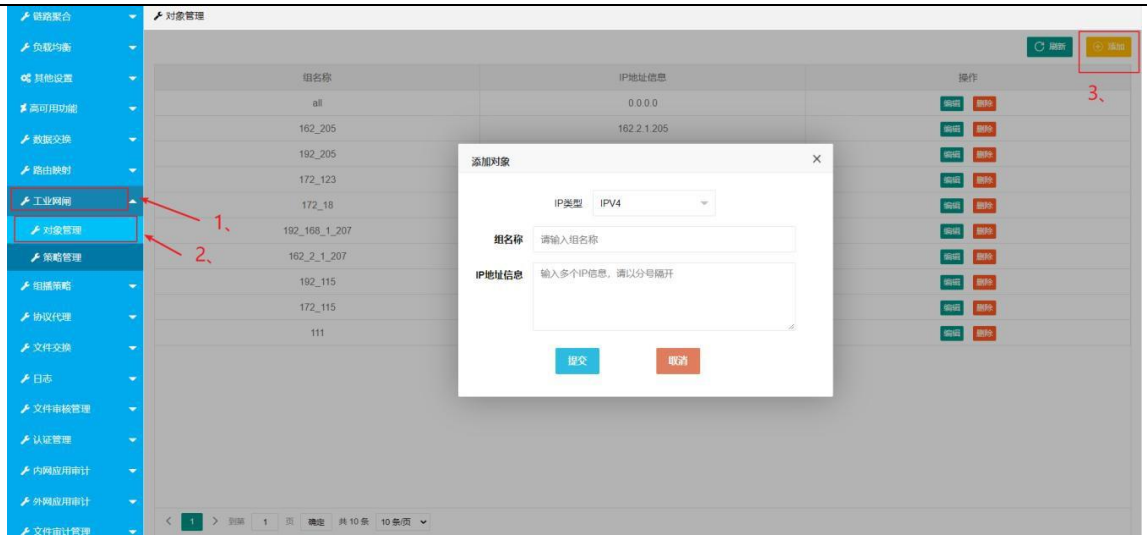


图 5.8.1.1-1 添加对象界面

添加对象参数说明：

1、IP 类型：对象的IP 类型，IPV4 或者IPV6

2、组名称：对象的名称（配置后不可修改）

3、IP 地址信息：对象IP，格式：x.x.x.x；多个 IP 用英文“;”隔开，如：x.x.x.x;y.y.y.y

5.8.1.2 编辑对象

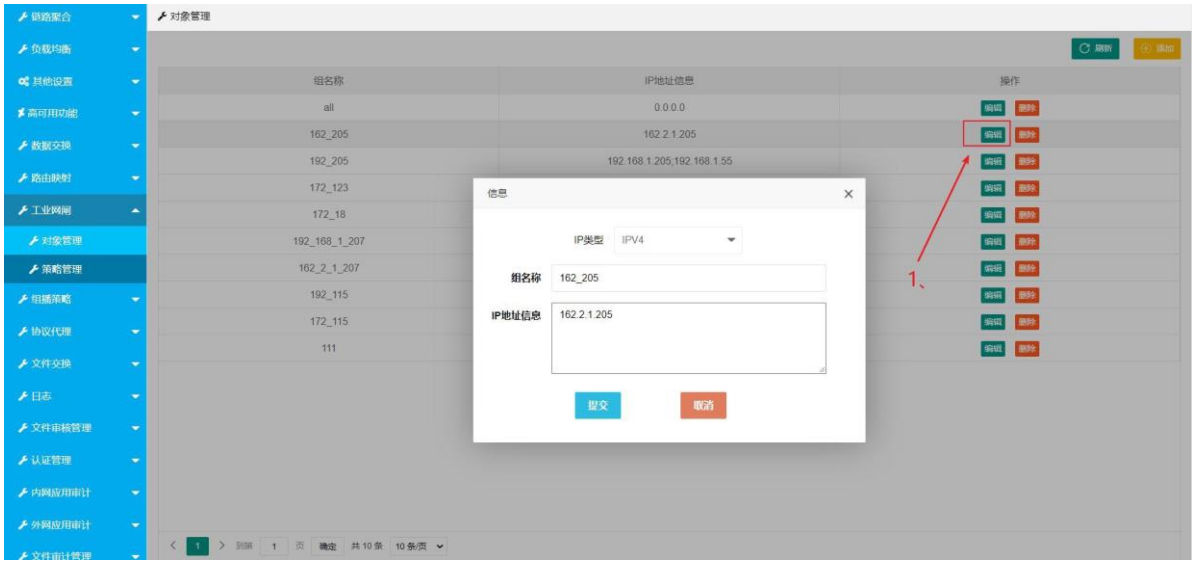


图 5.8.1.2-1 编辑对象界面

5.8.1.3 删除对象

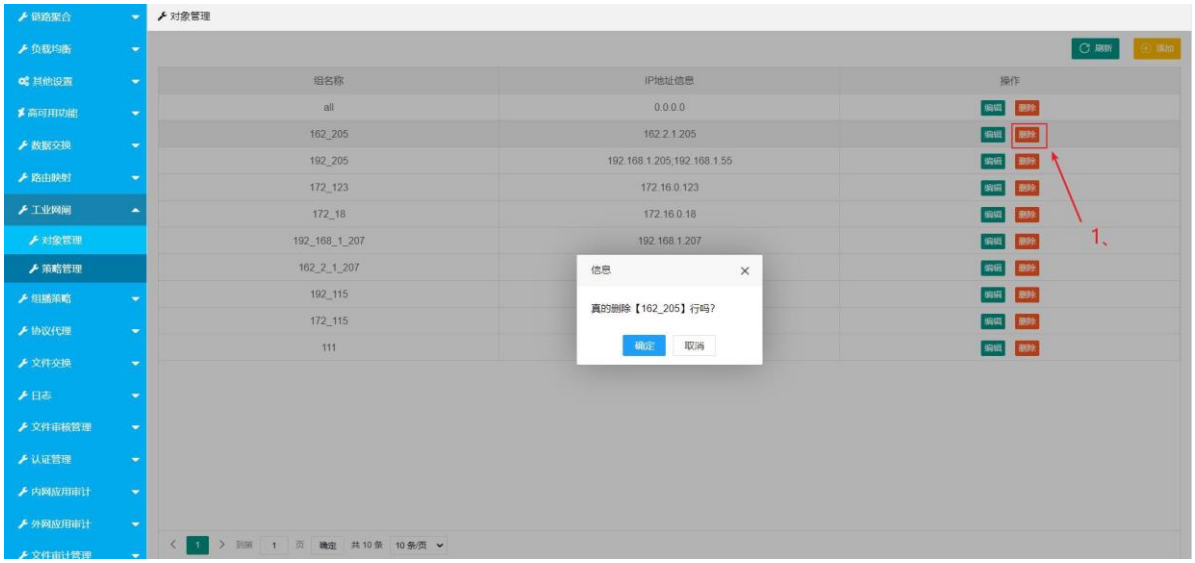


图 5.8.1.3-1 删除对象界面

5.8.2 策略配置

点击『工业网闸』→点击『策略管理』→点击添加，进入任务配置页面，如下图所示：

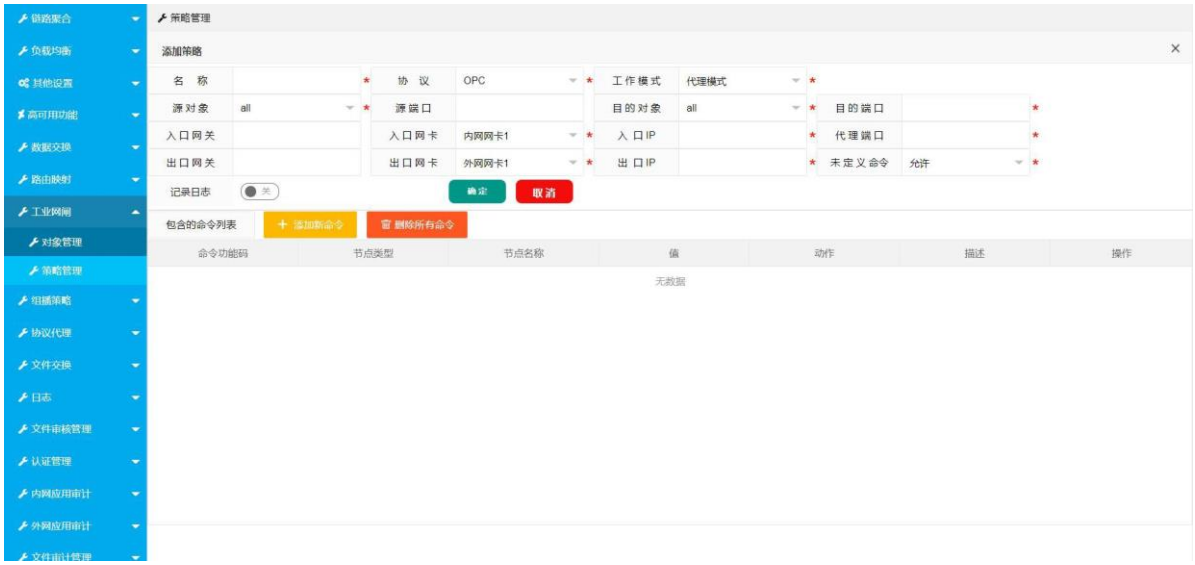


图 5.8.2-1 任务配置界面

任务配置参数说明：

- 名称：任务名称。支持中文、英文、特殊字符和数字
- 协议：客户端（主机）与服务端（从机）之间的通信协议。支持 OPC、Modbus(TCP)、DNP3、
- S7、IEC104
- 工作模式：协议之间通信的方式。支持代理模式、路由模式、透明模式
- 源对象：源对象 IP 地址，一般为客户端(主机)IP 地址。在对象管理中设置
- 目的对象：目的对象 IP 地址，一般为服务器(从机)IP 地址。在对象管理中设置
- 源端口：源对象访问连接端口号，为客户端(主机)发起连接的端口号
- 目的端口：目的对象访问连接端口号，为服务端(从机)监听的端口号

- 代理端口：任务中的代理端口
- 入口网关：如果与源对象之间存在三层交换机，需要填入网关地址
- 出口网关：如果与源对象之间存在三层交换机，需要填入网关地址
- 入口网卡：业务入口的网卡信息
- 出口网卡：业务出口的网卡信息
- 入口IP：ip 格式xxx.xxx.xxx.xxx(xxx为0-255)
- 出口IP：ip 格式xxx.xxx.xxx.xxx(xxx为0-255)
- 未定义命令：协议所支持且没有添加在定义命令中的所有命令

5.8.2.1 OPC 协议配置

配置OPC 任务，如下图所示：

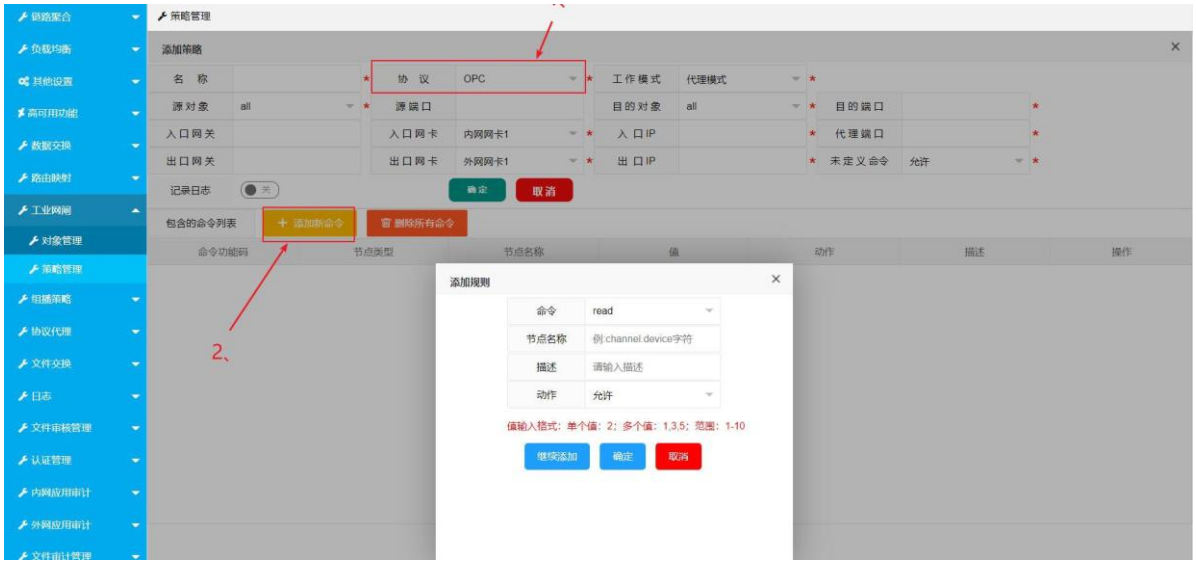


图 5.8.2.1-1 OPC 协议配置界面

OPC 协议添加新命令参数说明：

- 命令：OPC 协议的功能码
- 节点名称：OPC 协议支持的节点名称
- 描述：命令的备注说明，非必填项
- 动作：可配置允许或者拒绝。配置允许，当客户端(主机)对服务端(从机)做对应的读写操作时，该定义命令会放行；配置拒绝，当客户端(主机)对服务端(从机)做对应的读写操作时， 该定义命令会被拦截。

5.8.2.2 MODBUS 协议配置

支持MODBUS 协议数据过滤、安全控制。可根据设备 ID、功能码、对应的读写控制地址对数据包进行过滤，如下图所示：

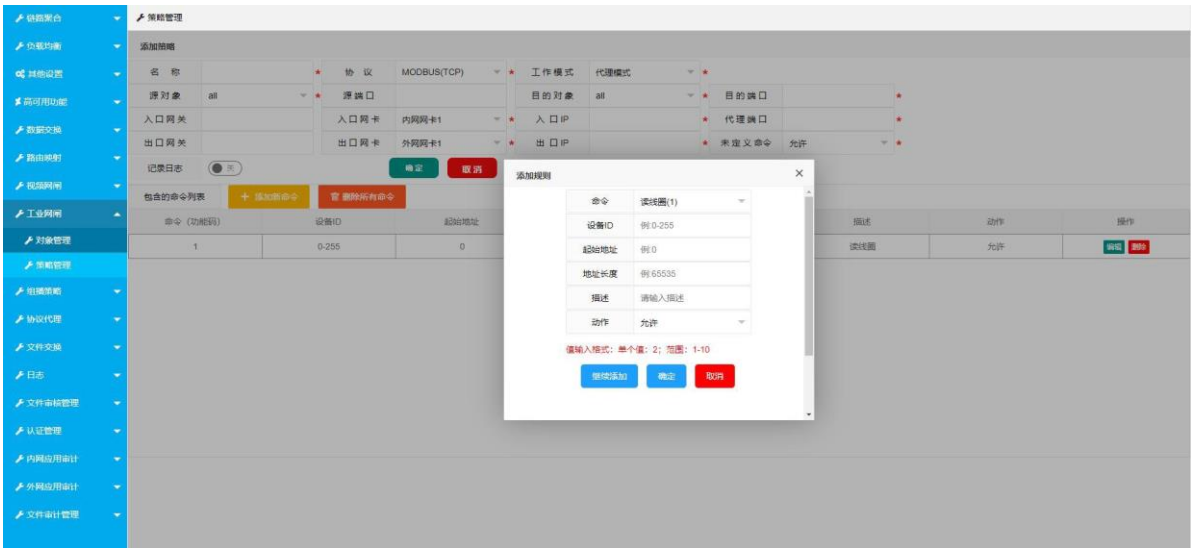


图 5.8.2.2-1 Modbus(TCP)协议新命令配置界面

Modbus(TCP)协议添加新命令参数说明：

- 命令：Modbus(TCP)协议支持的功能码
- 设备ID：允许客户端(主机)连接服务端(从机)的设备ID号
- 起始地址：允许客户端(主机)对服务端(从机)做对应的读写操作的地址起始值
- 地址长度：指定地址的长度。如起始地址为1，地址长度为10，那么可操作的地址范围是[1-11]
- 描述：命令的备注说明，非必填项
- 动作：可配置允许或者拒绝。配置允许，当客户端(主机)对服务端(从机)做对应的读写操作时，该定义命令会放行；配置拒绝，当客户端(主机)对服务端(从机)做对应的读写操作时， 该定义命令会被拦截。

5.8.2.3 DNP3 协议配置

支持DNP3 协议数据过滤、安全控制，可根据源 IP、目的IP、源端口、目的端口、协议类型、收发者地址和功能码对数据包进行过滤，配置如下图所示：

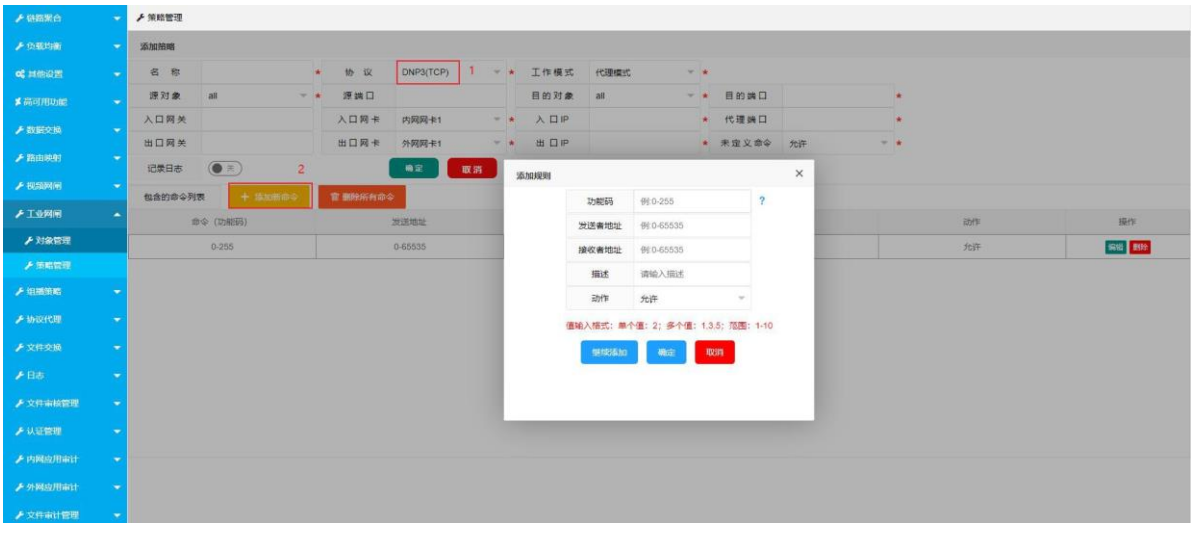


图 5.8.2.3-1 DNP3 协议配置界面

DNP3 协议配置参数说明：

- 功能码：DNP3 协议支持的功能码
- 发送者地址：客户端(主机)对服务端(从机)做对应的读写操作的地址范围
- 接收者地址：服务端(从机)接收客户端(主机)对应读写操作的地址范围
- 描述：命令的备注说明，非必填项
- 动作：可配置允许或者拒绝。配置允许，当客户端(主机)对服务端(从机)做对应的读写操作时，该定义命令会放行；配置拒绝，当客户端(主机)对服务端(从机)做对应的读写操作时，该定义命令会被拦截。

5.8.2.4 IEC104 协议配置

支持IEC 协议数据过滤、安全控制，可根据源 IP、目的 IP、源端口、目的端口、ASDU（应用服务数据单元）地址、数据单元中的信息对象地址、传输原因和控制命令进行过滤、传输， 配置如下图所示：

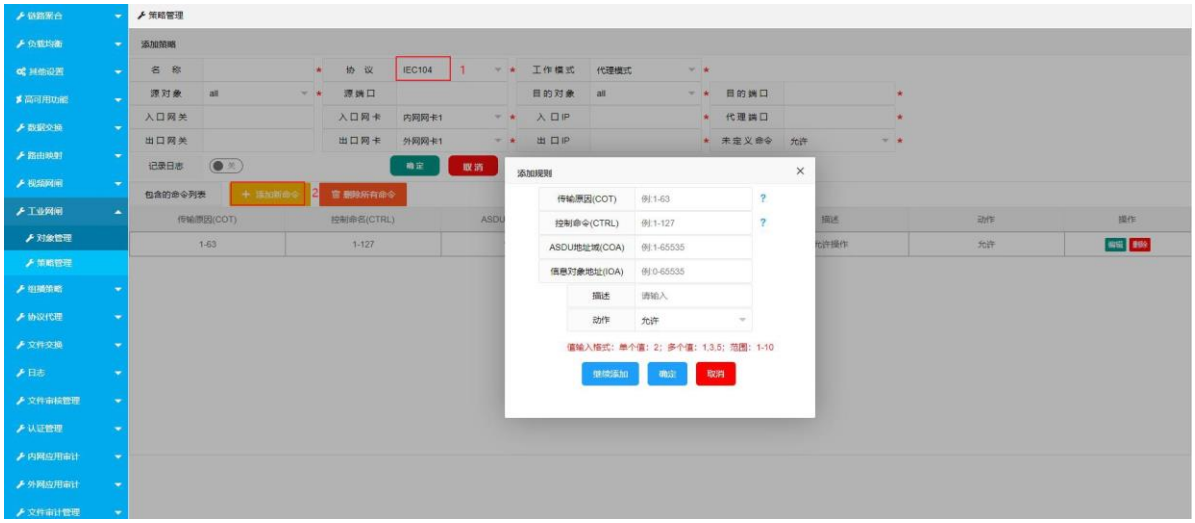


图 5.8.2.4-1 IEC104 协议配置界面

IEC104 协议配置参数说明：

- 传输原因（COT）：数据单元中的传输原因 ID 进行过滤控制
- 控制命令（CTRL）：针对控制命令过滤，只允许客户端（主机）对服务端（从机）做符合该控制命令的操作
- ASDU 地址域（COA）：应用服务数据单元地址控制
- 信息对象地址（IOA）：针对应用服务数据单元中的一个或多个信息对象的地址进行控制；
- 描述：命令的备注说明，非必填项
- 动作：可配置允许或者拒绝。配置允许，当客户端(主机)对服务端(从机)做对应的读写操作时，该定义命令会放行；配置拒绝，当客户端(主机)对服务端(从机)做对应的读写操作时，该定义命令会被拦截。

5.8.2.5 西门子S7 协议配置

支持S7 协议数据过滤、安全控制，可根据源 IP、目的IP、源端口、目的端口、功能组和功能码进行过滤、传输。如下图所示：

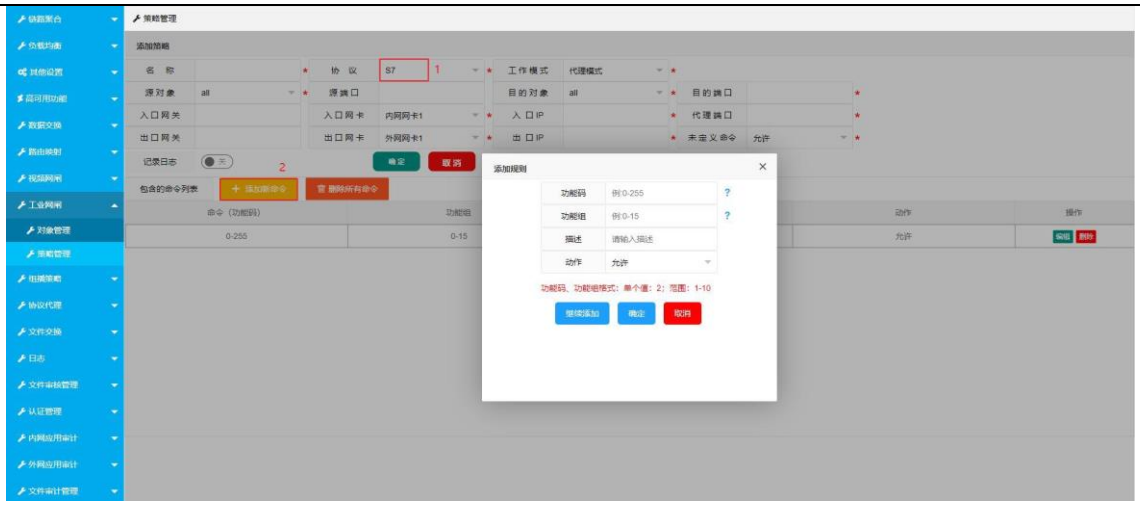


图 5.8.2.5-1 西门子 S7 协议配置界面

西门子S7 协议配置参数说明：

- 功能组：针对功能组，只允许客户端（主机）对服务端（从机）做符合该功能码组或某一类功能的操作；
- 功能码：针对功能码过滤，只允许客户端（主机）对服务端（从机）做符合该功能码的操作；
- 描述：命令的备注说明，非必填项
- 动作：可配置允许或者拒绝。配置允许，当客户端(主机)对服务端(从机)做对应的读写操作时，该定义命令会放行；配置拒绝，当客户端(主机)对服务端(从机)做对应的读写操作时，该定义命令会被拦截。

5.9 组播策略

组播转发功能主要提供在组播包经过网闸之后能够按照用户需求转发到对应的设备上的功能，IGMP / MLD 代理提供了将本地多播网络与更大的多播基础结构结合在一起的可能性。与多播路由器相比，代理是轻量级的，不需要支持 PIM 或 DVMRP 等多播路由协议。常见的用例是通过隧道与远程多播路由域互连的本地存根网络。

5.9.1 代理模式

代理模式下，客户端需要往源组播 IP、端口发送组播流，实现组播代理。如下图所示：

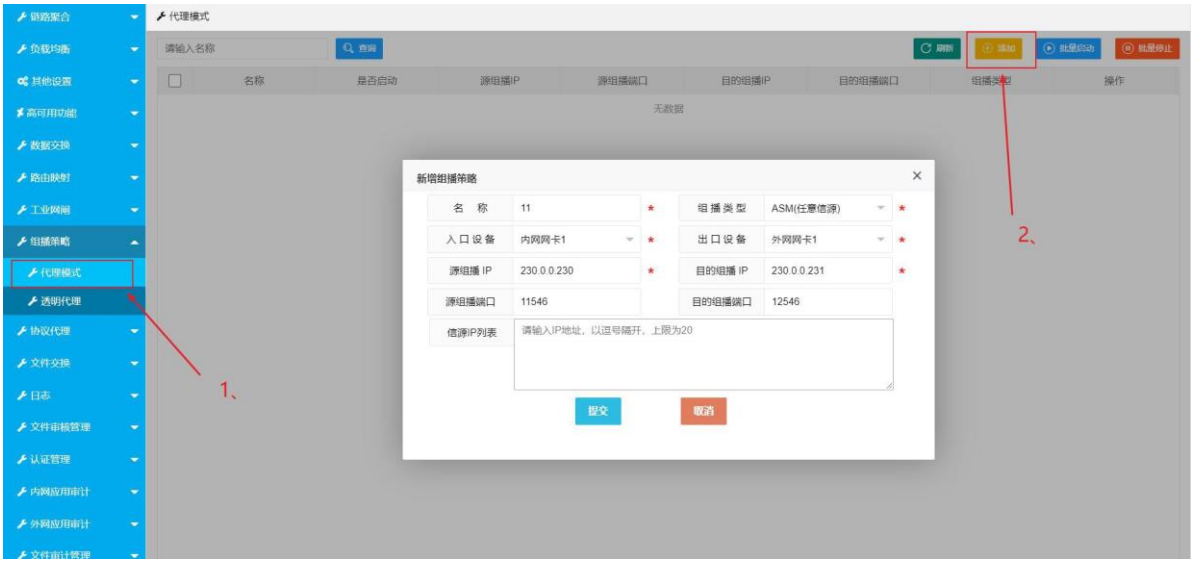


图 5.9.1-1 代理模式配置

代理模式配置参数说明:

- ASM（任意信源）：当为任意信源,对信源IP 不做任何限制
- SSM（指定信源）：当为指定信源,信源IP 列表用作白名单模式
- SFM（过滤信源）：当为过滤信源,信源IP 列表用作黑名单模式

5.9.2 透明代理

在透明代理模式下,客户端需要往目的IP 发送组播流，经过网闸只是纯转发,不做DNAT。如下图所示:

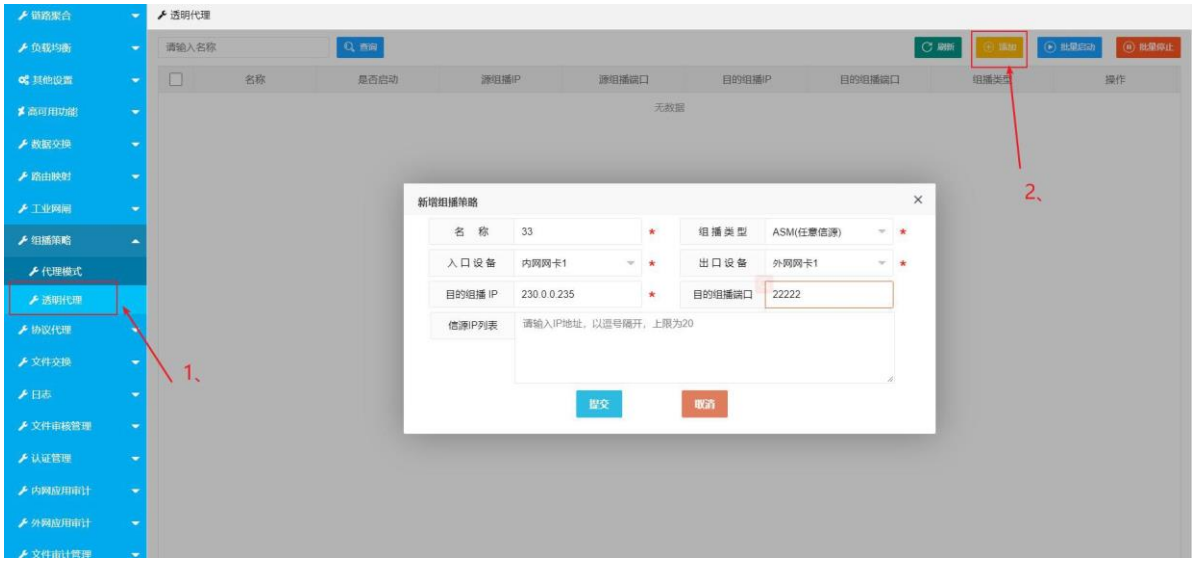


图 5.9.2-1 透明模式配置

5.10 协议代理

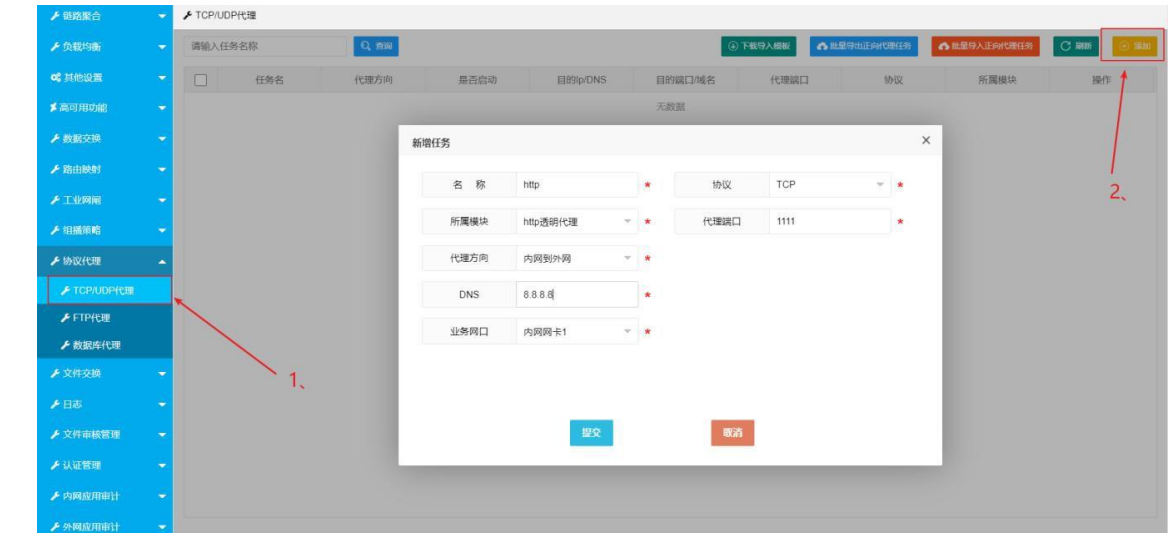
协议代理功能包括『TCP/UDP 代理』、『FTP 代理』、『数据库代理』功能。流代理模块主要支持smtp 协

议、pop3 协议、smb 协议、ntp 协议、1bit 协议、tcp 单向协议、dns 协议、snmp 协议和udp 单向协议以及命令过滤功能。网页代理模块主要支持http 和https 代理。

5.10.1 TCP/UDP 代理

5.10.1.1 http/https 代理

http/https 代理对用户代理上网和访问进行控制。支持方式：正向代理和透明代理。透明代理：需要在客户端的浏览器中作关于代理的设置，启用代理后直接访问目的服务器。配置如下图所示：



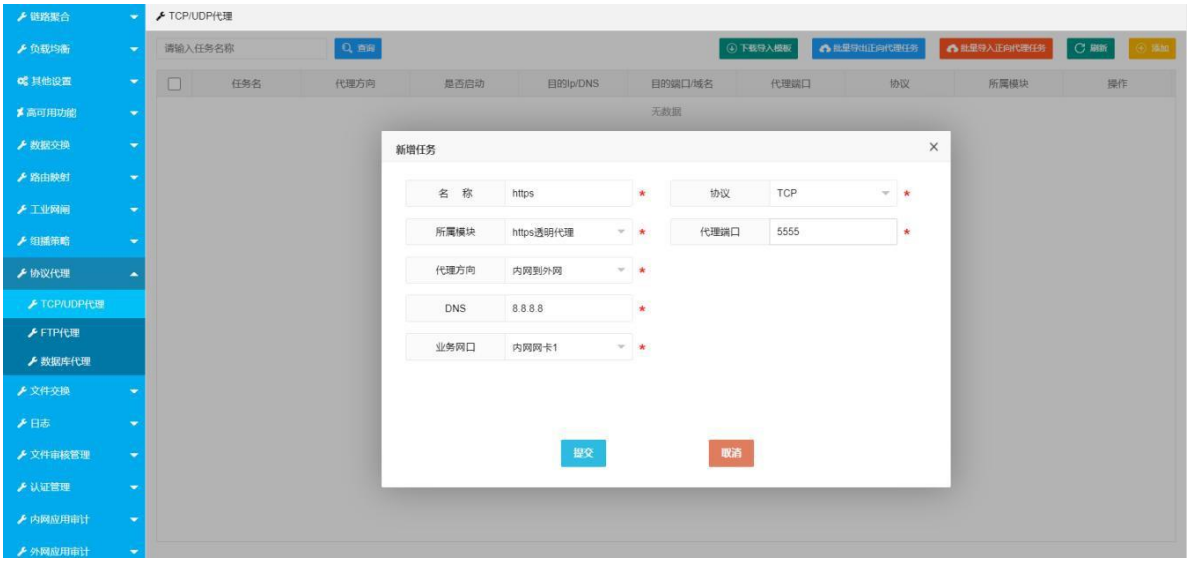
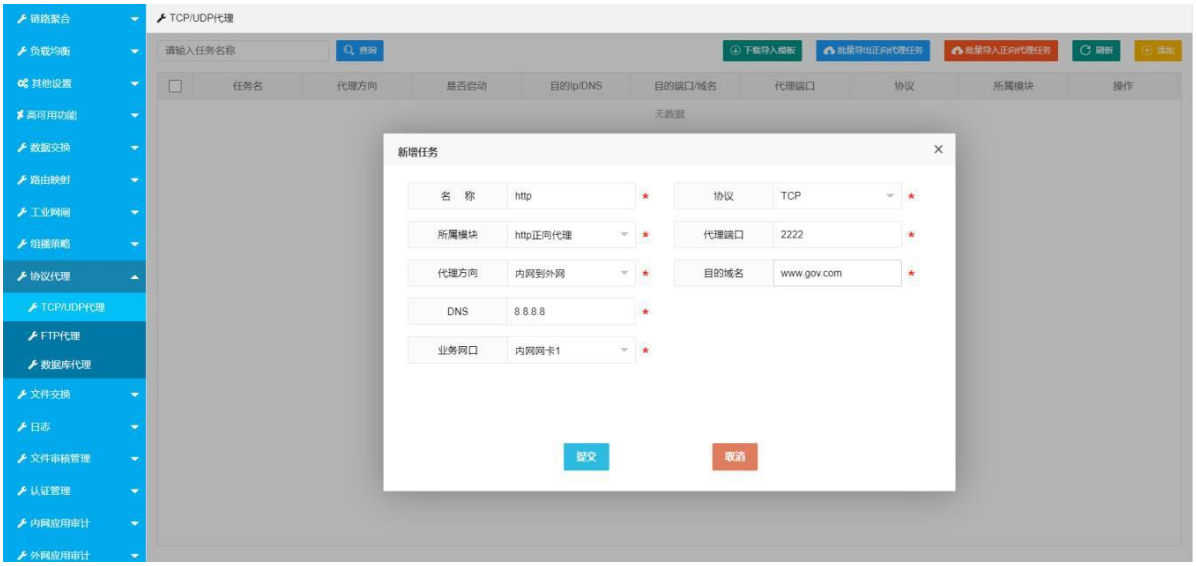


图 5.10.1.1-1 http/https 透明代理任务配置界面

正向代理：代理对客户端来说是不可见的，并不需要在客户端的浏览器中作关于代理的设置，而是通过访问网闸入口IP 后映射到目的服务器。配置如下图所示：



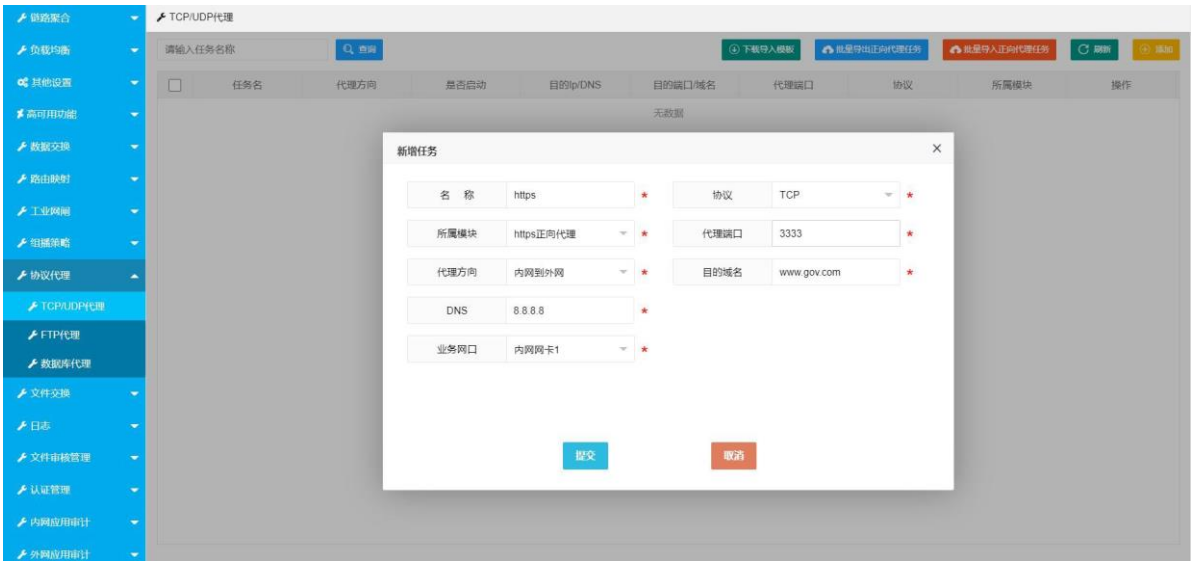


图 5.10.1.1-2 http/https 正向代理任务配置界面

△**Tips：**http 透明代理除了代理访问外，还能实现对访问请求方式进行允许、禁止功能。点击编辑-点击导入内置命令或添加自定义命令可以对一些常用的请求方式进行允许或拦截配置。如下图所示：

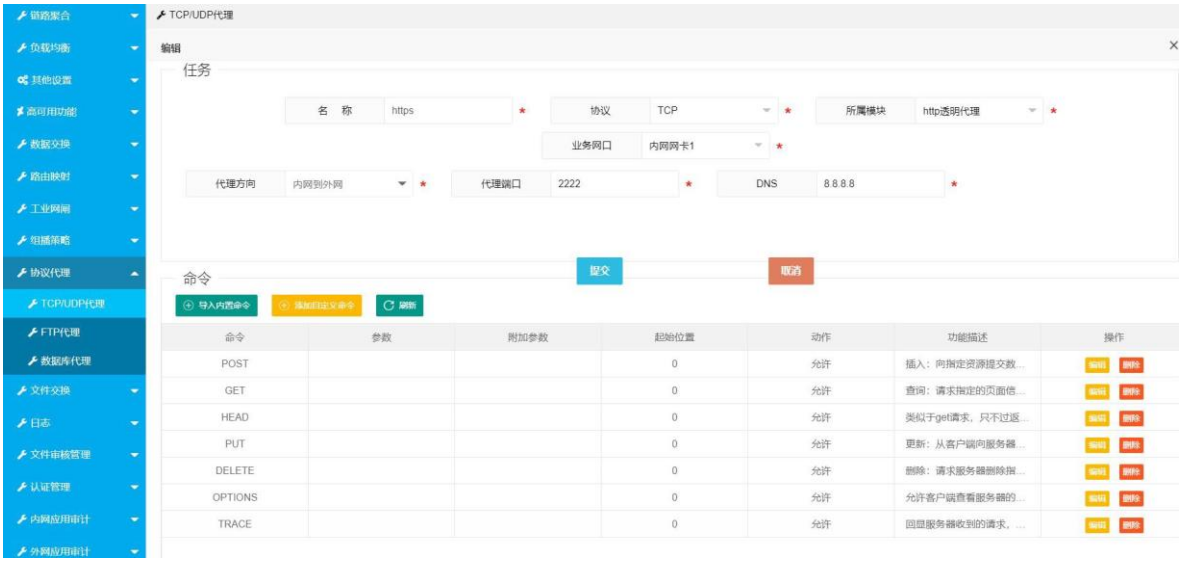
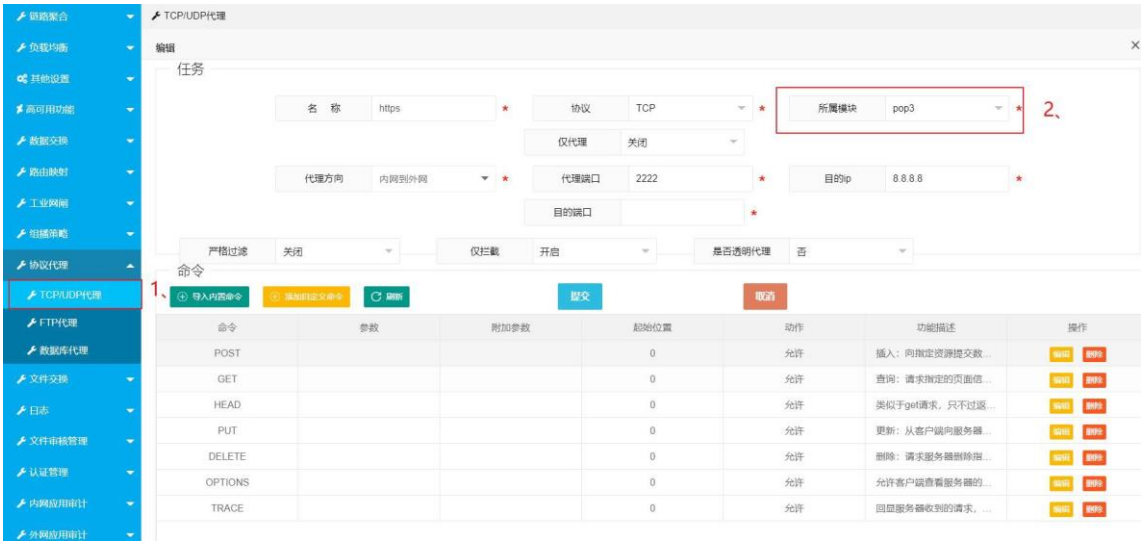


图 5.10.1.1-3 http 透明代理过滤操作界面

5.10.1.2 pop/smtp 代理

『邮件代理』提供用户的邮件发送、邮件接收等相关参数进行配置与管理。可在编辑界面对相关命令进行允许或禁止配置。pop3/smtp 代理建议同时使用，否则仅有接收邮件或者仅有发送邮件的权限。



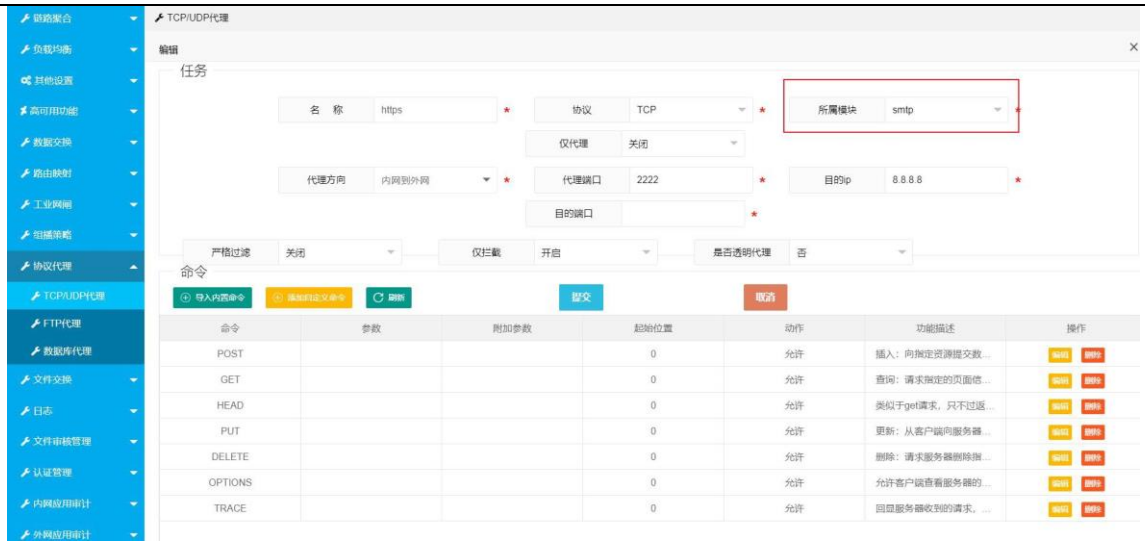
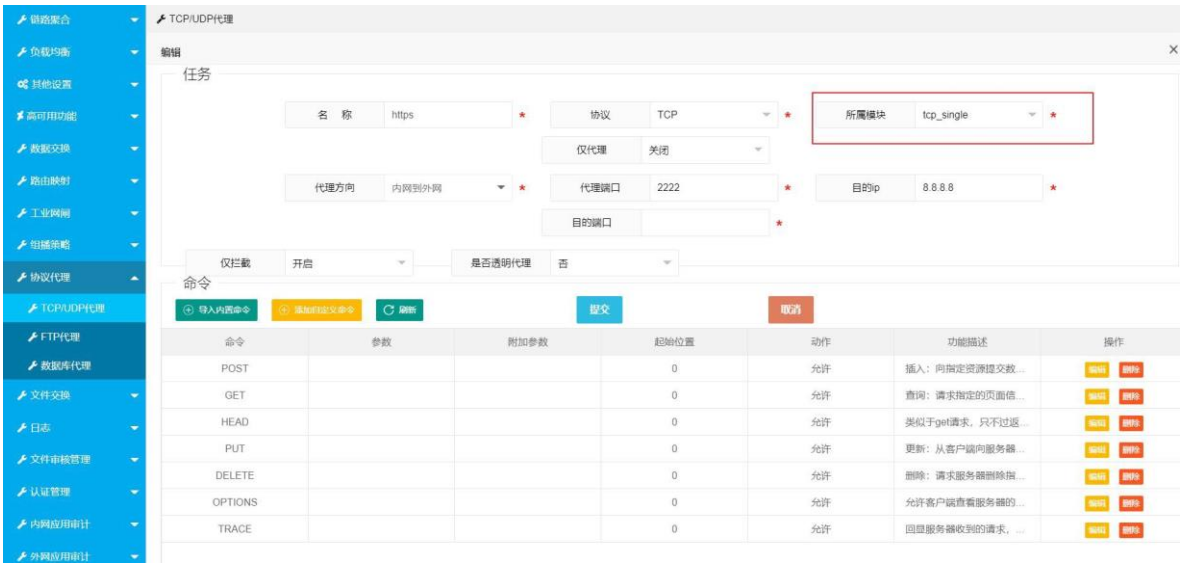


图 5.10.1.2-1 pop3/smtp 代理配置界面

5.10.1.3 tcp_single/tcp_custom 代理

Tcp_single 实现单向数据传输代理，数据只能从一个方向到另一个方向，tcp_custom 实现自定义设置 tcp 访问。



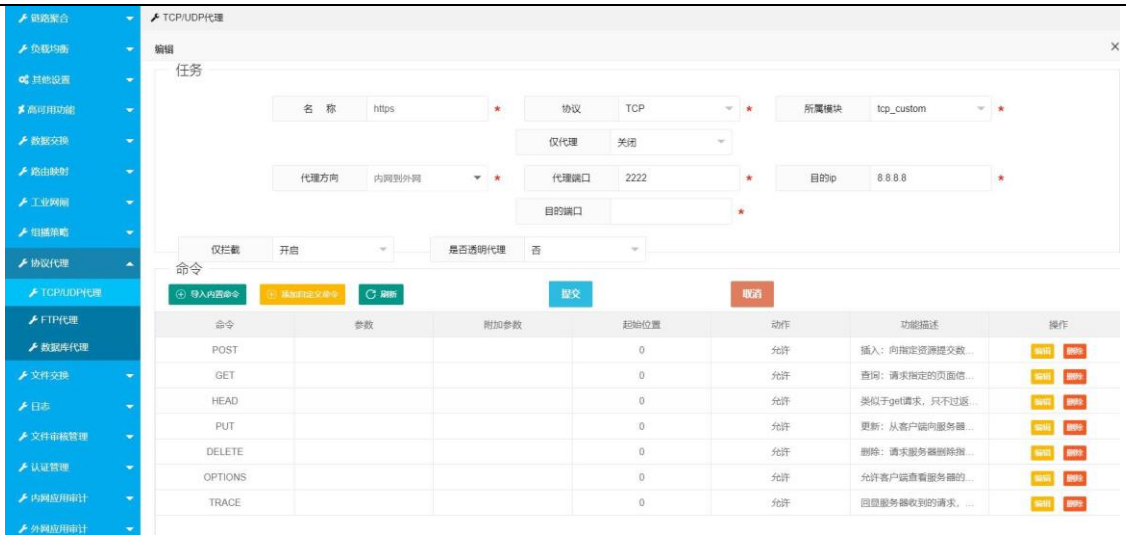


图 5.10.1.3-1 tcp_single/tcp_custom 配置界面

5.10.1.4 1bit 代理

1bit 协议代理实现访问服务器只能回复 1bit 长度的信息，其他内容会被拦截，客户端发送则没有限制。

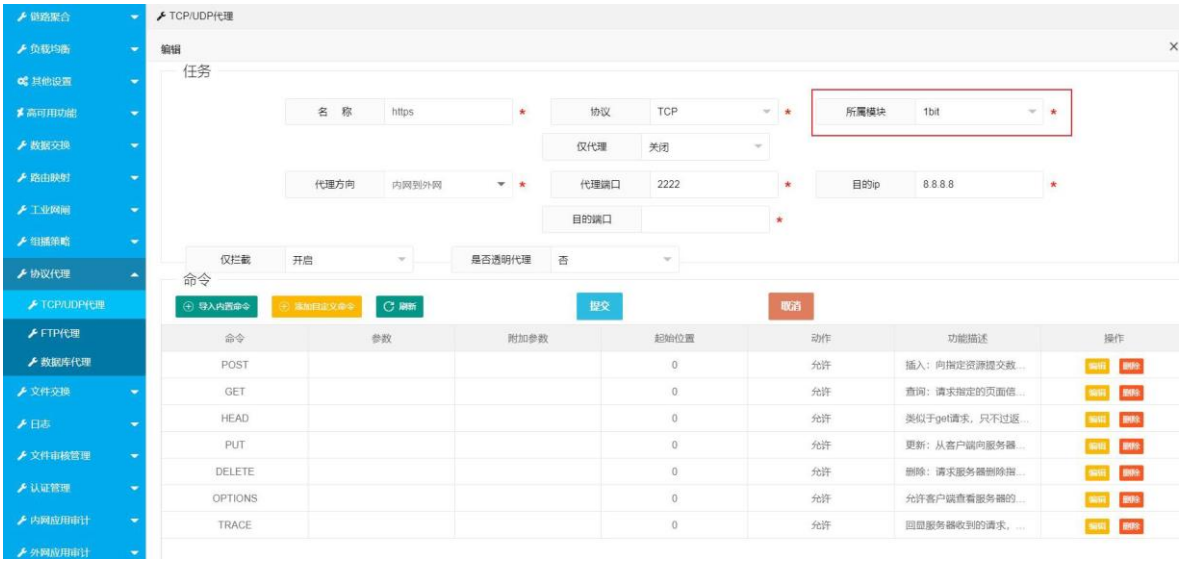


图 5.10.1.4-1 1bit 协议配置界面

5.10.1.5 smb 代理

smb 理实现代理访问 SMB 服务器，进行查看、上传、下载等功能，在编辑界面还可以对相关命令进行允许、拦截配置。

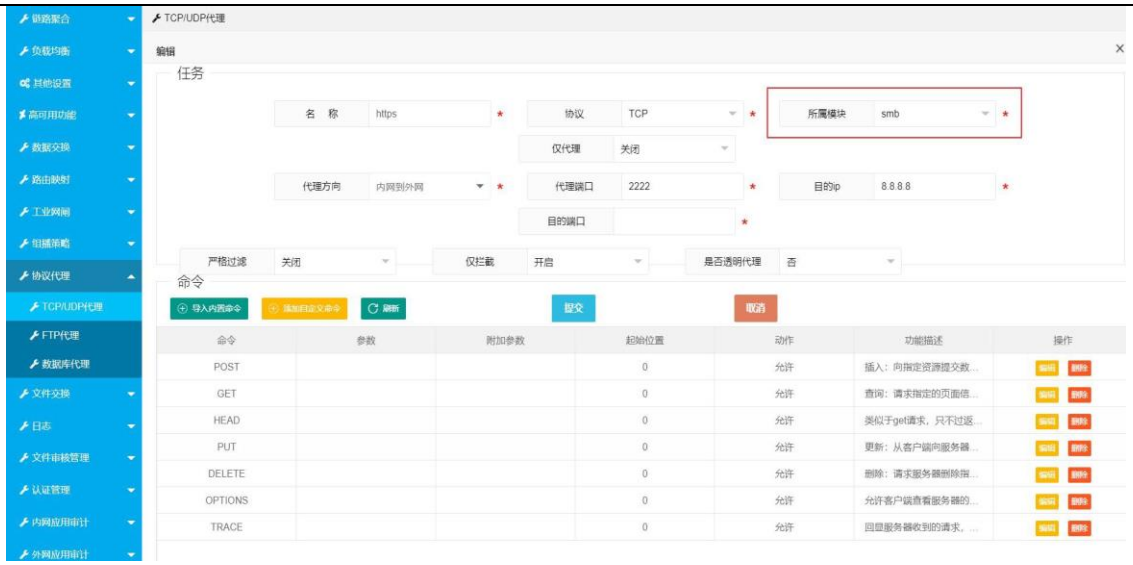


图 5.10.1.5-1 smb 协议配置界面

TCP/UDP 代理配置总参数说明：

- 仅代理：仅实现代理访问功能，不涉及过滤功能。
- 透明代理：用户直接访问目的服务器
- 非透明代理：用户通过访问网闸IP 和代理端口实现目的服务器的访问
- 仅拦截：当访问存在拦截命令的时候，仅做拦截，而不是直接断开连接
- 严格过滤：会把协议携带的命令进行拦截

5.10.2 FTP 代理

『FTP 代理』实现用户 FTP 服务代理访问、FTP 服务器地址过滤以及 FTP 代理拦截等相关参数的配置与管理。

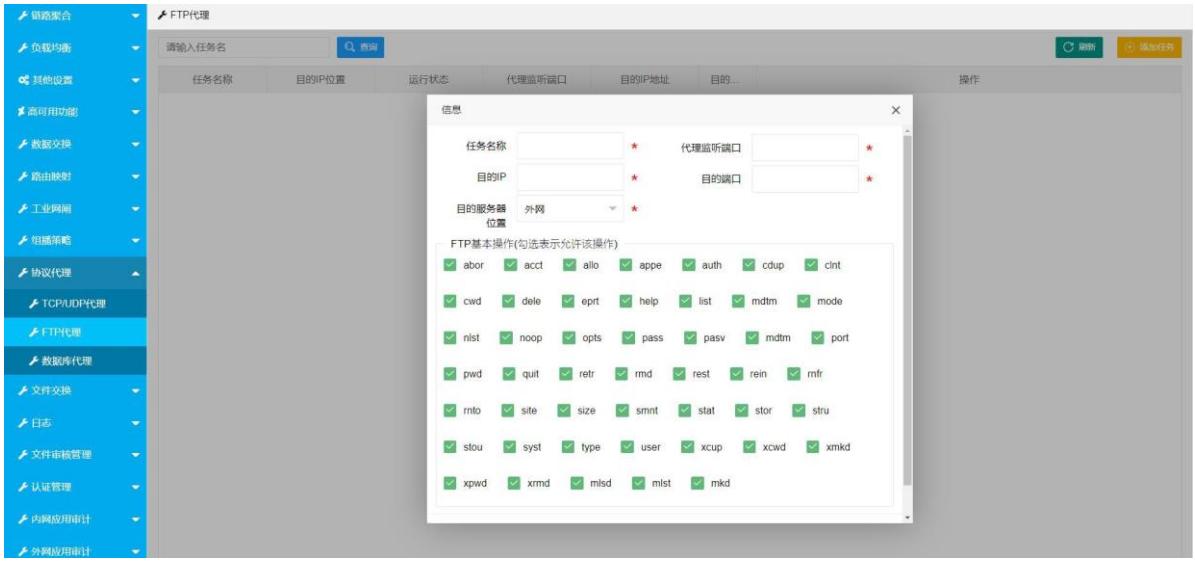


图 5.10.2-1 FTP 代理配置操作界面

FTP 代理参数说明：

- 任务名称：代理任务的名称
- 代理监听端口：网闸监听的代理端口
- 内网业务网口：选择内网业务网卡
- 外网业务网口：选择外网业务网卡
- 目的IP：目的FTP 服务器IP
- 目的端口：目的 FTP 服务器端口
- 目的服务器位置：选择内网或外网
- FTP 基础操作（勾选表示运行该操作）：FTP 基础操作的拦截与放行

5.10.3 数据库代理

『数据库代理』主要用来实现数据库代理访问，和可以对相关 sql 进行配置，目前支持代理的数据库有MySQL、SQLServer、Sybase、db2 和达梦。如下图所示：

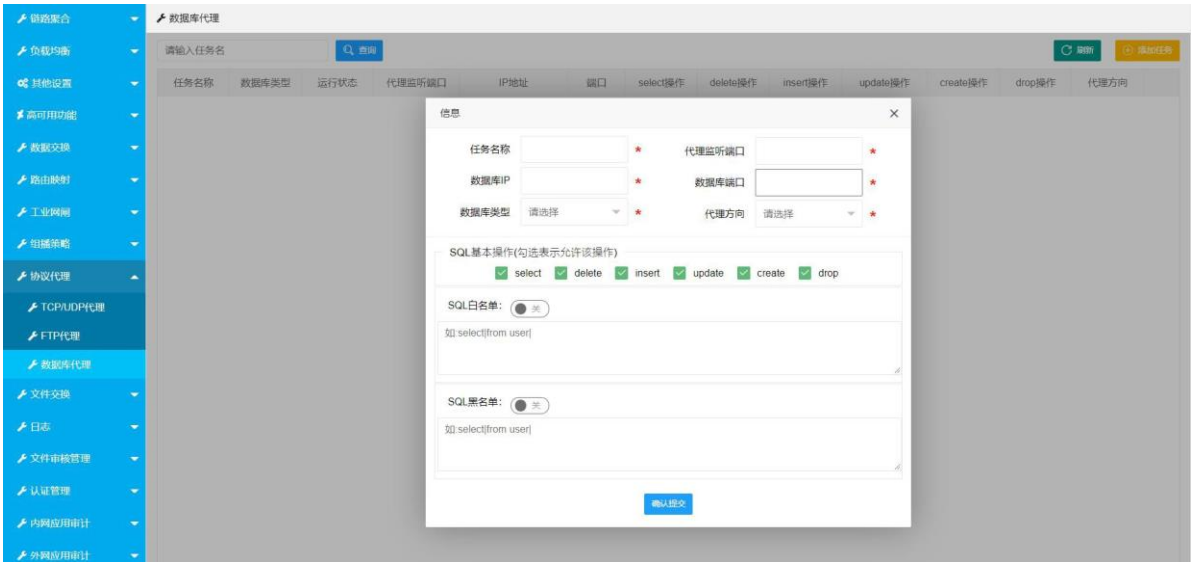


图 5.10.3-1 数据库代理配置操作界面

数据库代理参数说明：

- 任务名称：代理的任务名称
- 代理监听端口：网闸监听的代理端口
- 数据库IP：目的数据库IP
- 数据库端口：目的数据库端口
- 数据库类型：目的数据库类型
- 代理方向：选择内到外或外到内方向
- SQL 基础操作(勾选表示允许该操作)：数据库中增删改查操作的拦截与放行
- SQL 白名单：开启后，包含白名单中关键字的 SQL 语句才会放行
- SQL 黑名单：开启后，包含黑名单中关键字的 SQL 语句均被拦截

▵**Tips**：SQL 基础操作优先级高于SQL 黑白名单！

5.11 文件交换

提供以客户端的形式进行文件的发送、接收、拦截过滤等配置与管理，文件交换客户端在暂时只支持 Windows 版本。

5.11.1 组织用户管理

普通组织用户信息配置可以通过新增部门、新增用户、导出用户和导入用户。

图 5.11.1-1 组用户管理界面

组用户管理配置参数说明：

- 编辑：点击某用户信息记录末尾的编辑按钮，可以修改用户基本信息、设置内/外网登录绑定IP、修改所在部门、设置文件传输上限大小、配置用户文件交换相关权限
- 重置：选择某用户信息记录，点击重置，用户初始密码默认为：a12345678
- 隐藏：隐藏的用户无法登录客户端，未隐藏用户登录客户端无法查看隐藏的用户信息
- 删除：永久删除选中的用户，并且不可恢复
- 解锁：手动解除用户锁定状态
- 查询：根据登录名或者显示名查询用户

5.11.1.1 新增部门

在普通组织结构树形图，点击新增部门按钮，弹出新增部门界面,如下图所示：

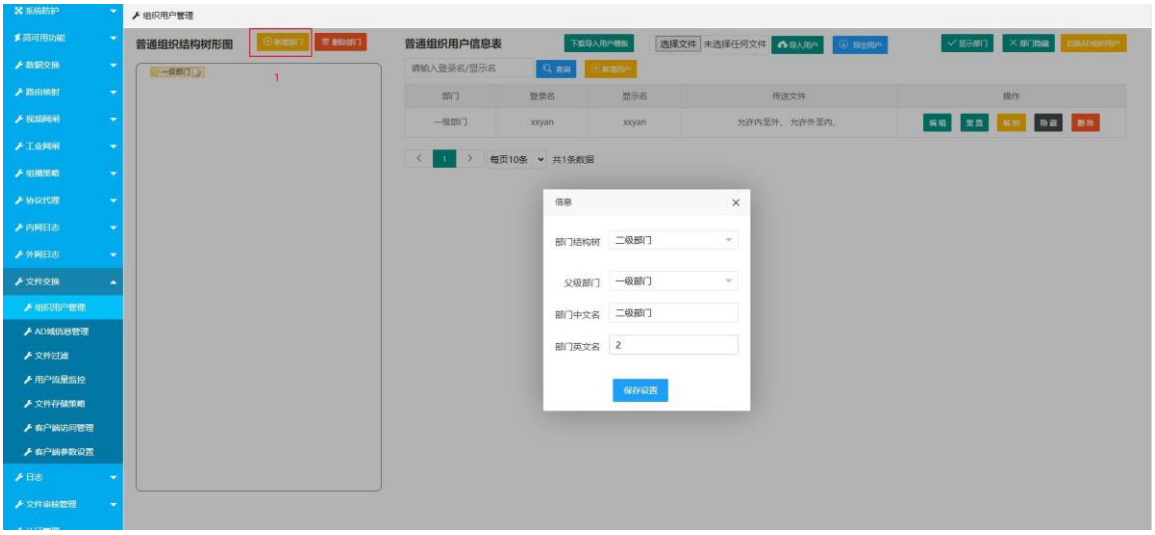


图 5.11.1.1-1 组织用户管理新增部门

新增部门配置参数说明：

- 部门结构树：部门分为四个级别，可根据级别划分部门等级。
- 部门中文名：部门中文名称，可自行设置。
- 部门英文名：部门英文名称，可自行设置。

5.11.1.2 删除部门

图 5.11.1.2-1 组织用户管理删除部门

5.11.1.3 新增用户

在普通组织用户信息表界面→点击新增用户按钮，弹出新增用户界面→用户信息修改完成→点击保存设置，保存用户信息，如下图所示：

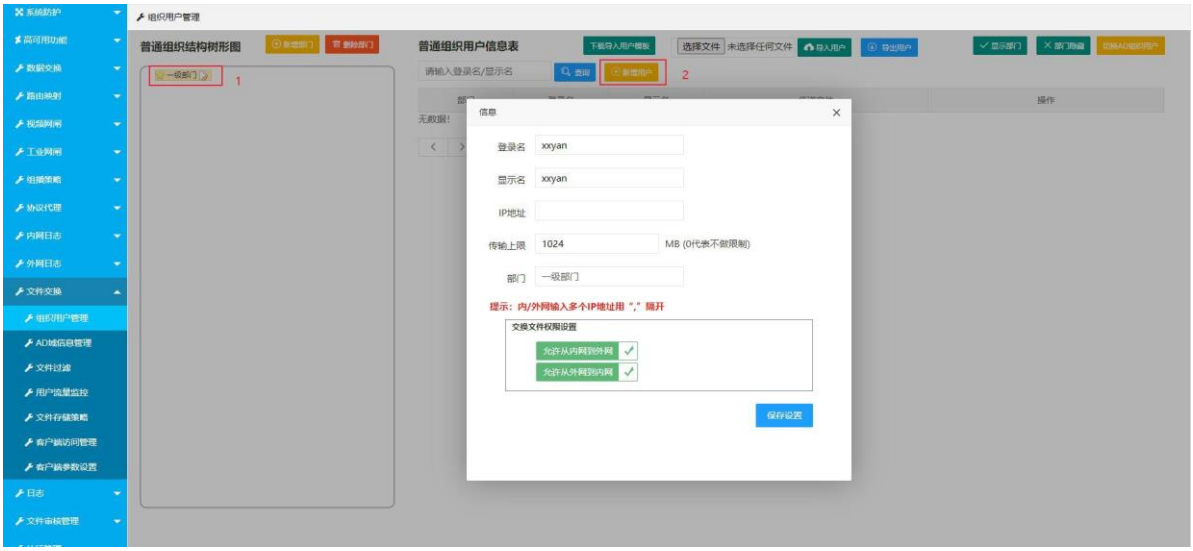


图 5.11.1.3-1 组织用户管理新增用户

新增用户配置参数说明：

- 登录名：用于登录文件交换客户端的账号，必填项
- 显示名：用于登录客户端后显示在左侧菜单的名称，必填项
- IP 地址：限制客户端登录 IP，选填项
- 文件传输上限：默认 1024M，自行修改，输入 0 为不限制
- 部门：用户所属部门，默认不可修改
- 交换文件权限设置：是否允许用户从外网向内网、内网向外网、外网向外网、内网向内网发送文件，默认允许，可以修改

5.11.1.4 导入用户

导入用户前需要严格按照模板中的格式进行编辑用户→浏览选择要导入用户的文件→确认要导入的文件→点击导入用户，即可在所选的部门下导入文件中的用户，如下图所示：

图 5.11.1.4-1 导入用户前下载导入用户模板

5.11.1.5 导出用户

在普通组织用户信息表界面→选择所要导出用户的所属部门→点击导出用户，弹出提示界面→点击确认，导出用户，如下图所示：

图 5.11.1.5-1 导出用户

△**Tips:** 导出用户不是根据部门级别进行导出（选择一级部门导出的用户并不包含二、三、四级别部门下的用户），而是根据选中的部门导出该部门下的用户。

5.11.1.6 用户查询

用户查询，根据用户登录名或显示名搜索用户：输入目标用户登录名或显示名，点击查询。

图 5.11.1.6-1 用户查询

5.11.1.7 普通用户组织架构

在普通组织用户信息表界面：

图 5.11.1.7-1 显示部门

5.11.1.8 AD 域用户组织架构

组织用户管理支持Windows AD/LDAP 域帐号组织架构信息切换（仅同步 AD 域用户名及组织结构信息，用户密码独立管理），点击切换 AD 域组织用户，可切换AD 域用户组织架构。如下图所示：

图 5.11.1.8-1 切换 AD 用户组织架构

5.11.1.9 部门隐藏

在普通组织用户信息表界面，选中已存在的部门，点击部门隐藏按钮，弹出界面。

图 5.11.1.9-1 部门隐藏操作界面

△Tips：选中已存在的部门，点击部门隐藏，使用隐藏部门后的用户登录客户端，客户端左下角会提示该用户已被后台隐藏，同时使用未被隐藏的用户登录客户端，客户端界面左侧菜单不会显示被隐藏部门和用户信息。

5.11.1.10 用户机解锁

用户机锁定是指用在一定登录失败的次数后该用户账户被锁定，在用户机解锁页面可进行解锁操作。

图 5.11.1.10-1 用户解锁配置界面

5.11.2 AD 域信息管理

文件交换系统支持Windows AD/LDAP 域组织架构及用户信息同步。配置AD 域参数，如图所示：

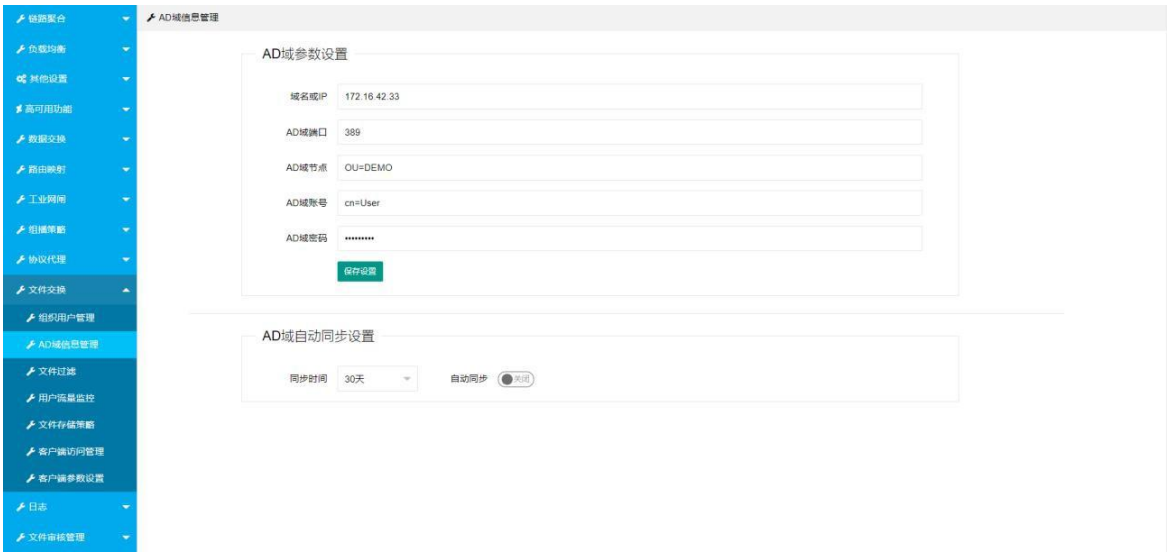


图 5.11.2-1 AD 域参数配置界面

AD 域参数说明：

- 域名或IP：AD 域的IP(172.16.42.33)、域名（如：win-gmmp0p49p70.JNTL.COM.CN）
- AD 域端口：AD 域的端口，如 389
- AD 域节点：AD 域的节点，如OU=BYH,OU=JNTL,DC=JNTL,DC=COM,DC=CN
- AD 域账号：AD 域的账号，如cn=administrator,cn=Users,DC=JNTL,DC=COM,DC=CN
- AD 域密码：AD 域的密码

5.11.2.1 域自动同步设置

AD 域自动同步功能，指定周期同步AD 域组织用户信息，如图所示：

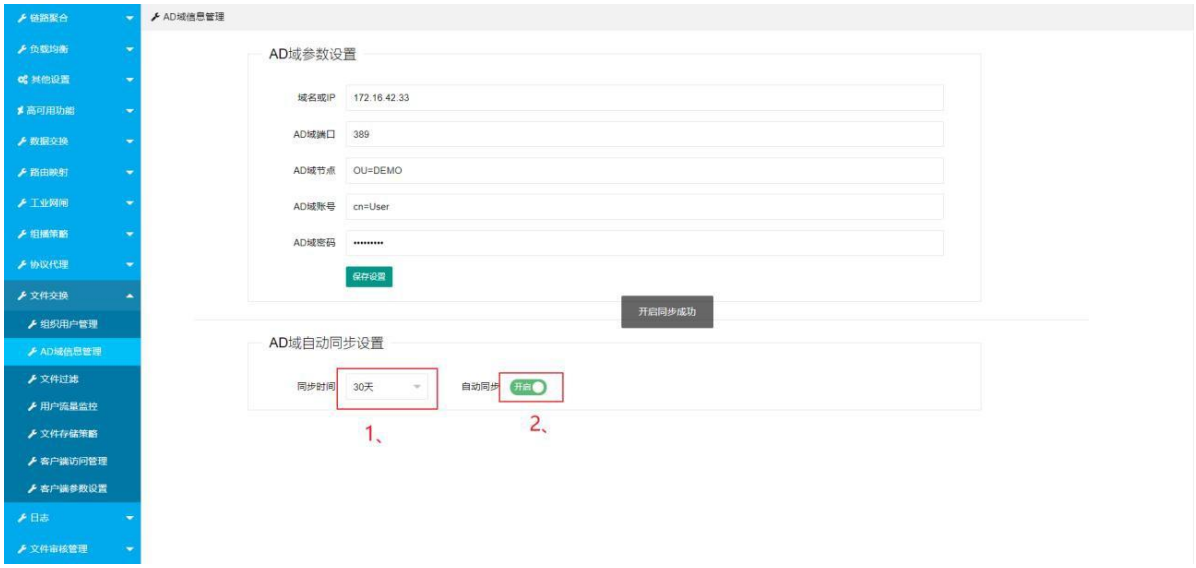


图 5.11.2.1-1 AD 域自动同步配置界面

参数说明：

- 同步周期：同步 AD 域信息的频率，可供选择 1 天、7 天、15 天、30 天

- 自动同步：开启自动同步功能的开关

5.11.3 文件过滤

5.11.3.1 文件扩展名过滤

文件交换系统可以过滤指定类型的文件，被过滤的文件信息会记录在等待审核界面，等待用户审核。

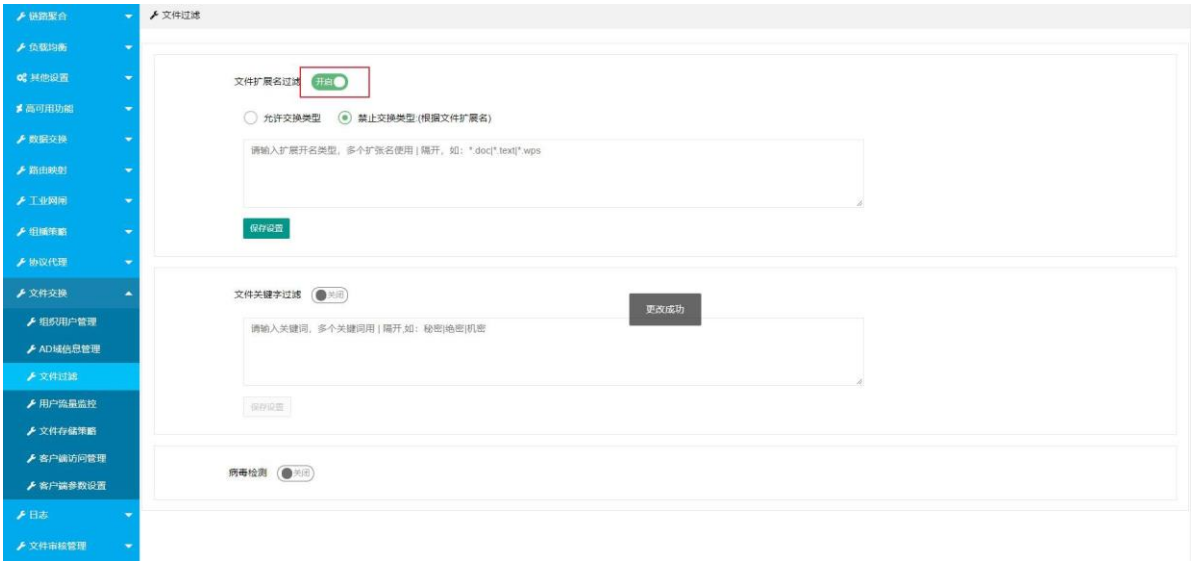


图 5.11.3.1-1 文件扩展名过滤规则配置界面

文件扩展名过滤规则配置参数说明：

- 文件扩展名过滤：绿色表示开启，置灰表示关闭
- 允许交换类型：点击后表示只能接收以下设置的文件类型
- 禁止交换类型：点击后表示不能接收以下设置的文件类型
- 扩展名：需要限制的文件类型，必须以符号“*.”开头
- 扩展名过滤规则配置完成后，点击保存设置按钮，成功添加过滤扩展名信息

5.11.3.2 文件关键词过滤

文件交换系统可以过滤含有指定关键词的文件，被过滤的文件会显示在等待审核界面， 等待用户审核。

图 5.11.3.2-1 文件关键字过滤界面

文件关键字过滤配置参数说明：

- 文件关键字过滤：绿色表示开启，置灰表示关闭
- 关键词：输入需要过滤的关键词
- 扩展名过滤规则配置完成后，点击保存设置按钮，成功添加过滤关键字信息

5.11.3.3 文件病毒检测

文件交换系统可以检测病毒文件，并将检测到的文件删除，用户将接收不到此文件。病毒检测功能需要先开启病毒检测的服务控制。病毒检测系统默认为关闭状态，可手动启停。

图 5.11.3.3-1 文件病毒监测

5.11.4 用户流量监控

主要记录用户发送文件的流量情况，可以精确查询各部门下的用户文件发送情况，如下图所示：

图 5.11.4-1 用户文件发送情况

5.11.5 文件存储策略

『文件存储策略管理』可以配置文件存储策略，并制定文件在服务器上的保存时间，文件存储策略管理分为停止服务、覆盖策略、特定文件存储策略三种管理策略。

5.11.5.1 文件存储策略-停止服务

『文件存储策略-停止服务』可以指定文件存储达到设定的警告阈值时，管理界面会提醒管理员磁盘空间存储达到阈值；同时可设置文件在服务器上的保存时间，文件保存时间超出配置值后，将被系统删除；文件存储空间达到 95%时，文件交换的服务程序停止运行；特定文件存储策略可以限制一种或者多种文件类型存储在网闸服务器的天数，达到天数直接删除设置的类型文件。如下图所示：

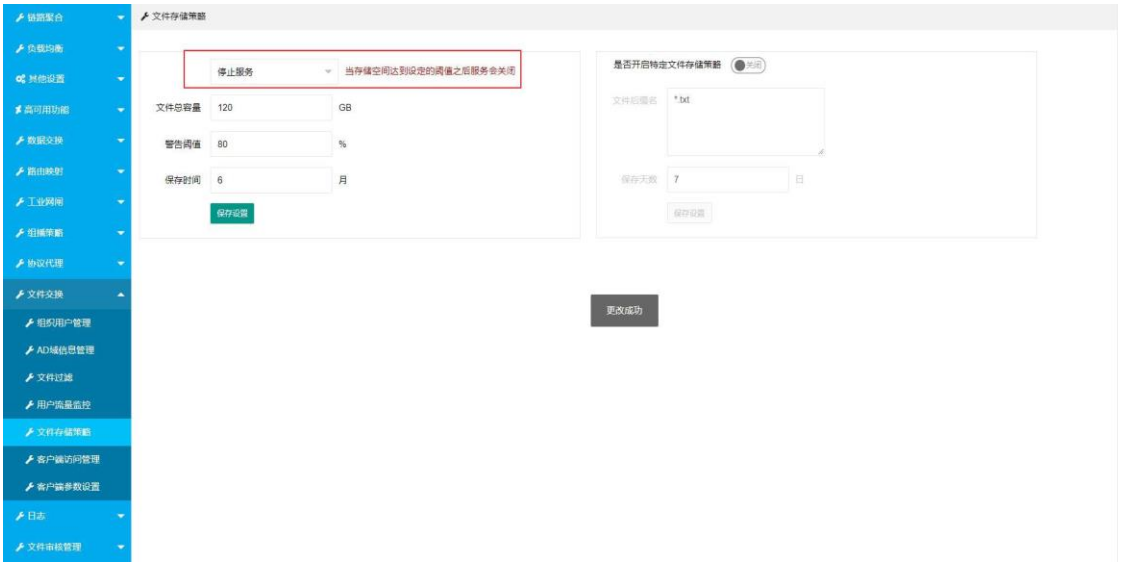


图 5.11.5.1-1 文件存储策略-停止服务

在策略类型列表中的停止服务行，可以配置文件类型的保存时间，系统默认 24 个月，同时可配置系统存储空间达到警告阈值，修改时，点击下方的保存设置即可

停止服务配置参数说明：

- 策略类型：可根据下拉框选择停止服务的类型
- 文件总容量：表示文件接收的最大和存储容量
- 警告阈值：管理员可以配置，配置为 1%-90%的范围
- 保留周期：管理员可以配置，配置为 1-24 个月
- 系统覆停止服务配置完成后后，点击保存设置按钮，弹出修改成功提示信息，系统成功保存配置信息，界面展示修改后的值。

5.11.5.2 文件存储策略-覆盖

『文件存储策略-覆盖』可以指定服务器的最大存储空间，服务器上存储的文件超过此配置值时，系统会删除服务器上保存时间最长的文件，以确保系统的可用性，同时文件存储达到设定的警告阈值时，管理界面会提醒管理员磁盘空间存储达到阈值。

在菜单栏左侧选择『文件存储策略』，选择覆盖策略，策略类型中的覆盖行可以配置系统最大存储空间。如下图所示：

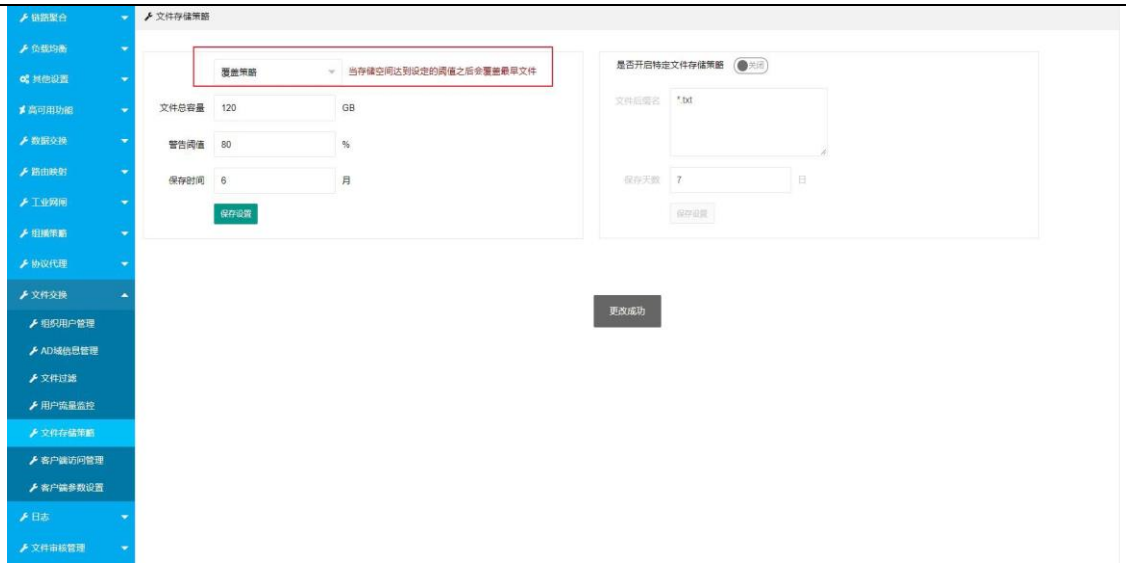


图 5.11.5.2-1 覆盖策略配置界面

覆盖策略配置参数说明：

- 策略类型：可根据下拉框选择覆盖策略的类型
- 文件总容量：表示文件接收的最大和存储容量
- 警告阈值：管理员可以配置，配置为 1%-90%的范围
- 保留周期：管理员可以配置，配置为 1-24 个月
- 添加备注：可以根据需要添加备注信息

覆盖策略配置完成后，可以开启特定文件存储策略，点击保存设置按钮，文件存储策略覆盖值修改成功，如下图所示：

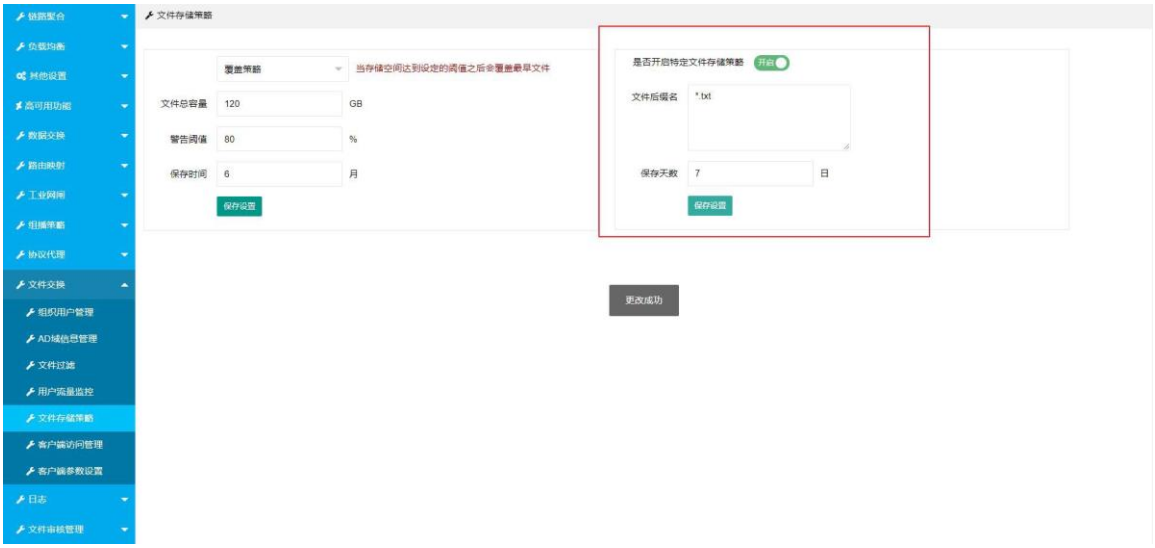


图 5.11.5.2-2 特定文件存储策略配置信息界面

特定文件存储策略参数说明：

- 特定文件存储策略：开启后以下设置的文件格式进行特定保存时间
- 文件后缀名：指的是所特定保留文件的格式
- 保存天数：指的是特定文件格式的文件所保存的天数

5.11.6 客户端访问管理

访问管理提供管理 IP 黑白名单配置，白名单是只允许名单内指定 IP 进行登录客户端， 黑名单是不允许指定IP 进行登录客户端。

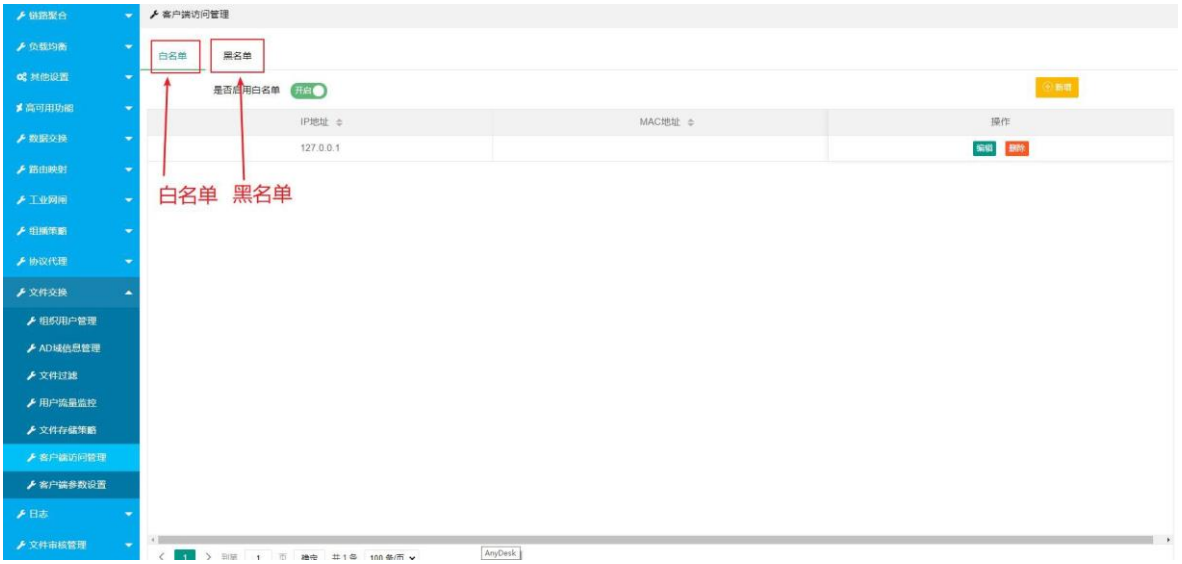


图 5.11.6-1 客户端访问管理界面

5.11.6.1 白名单新增

点击右上角新增按钮，弹出新增 IP 地址和 mac 地址的框架，填写正确的的格式进行登录使用客户端。

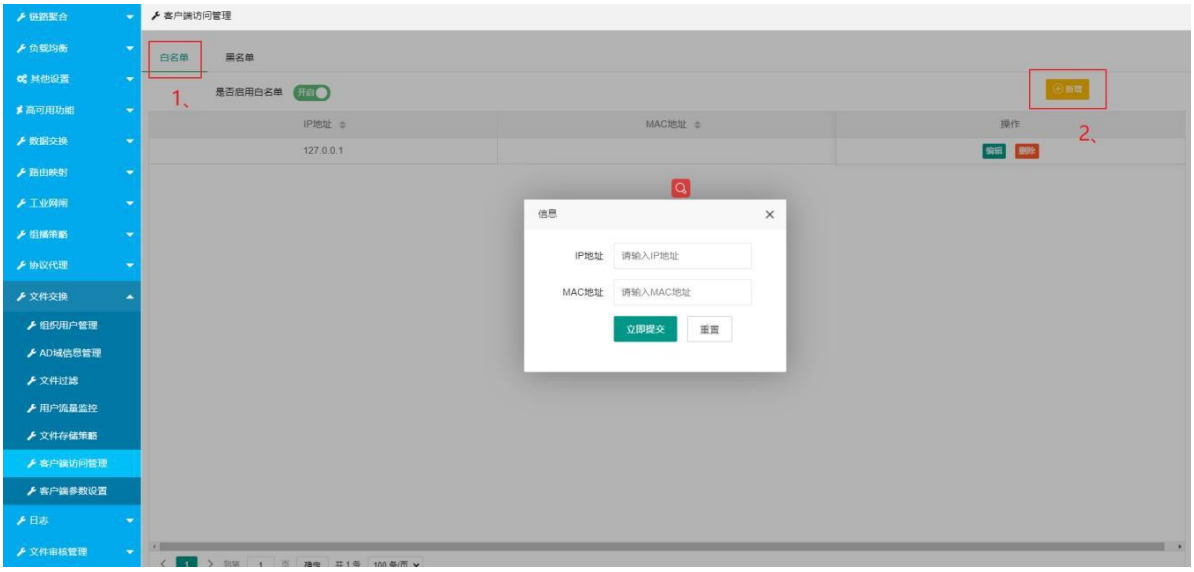


图 5.11.6.1-1 白名单新增界面

5.11.6.2 白名单编辑

更改想要修改的ip 地址和mac 地址。

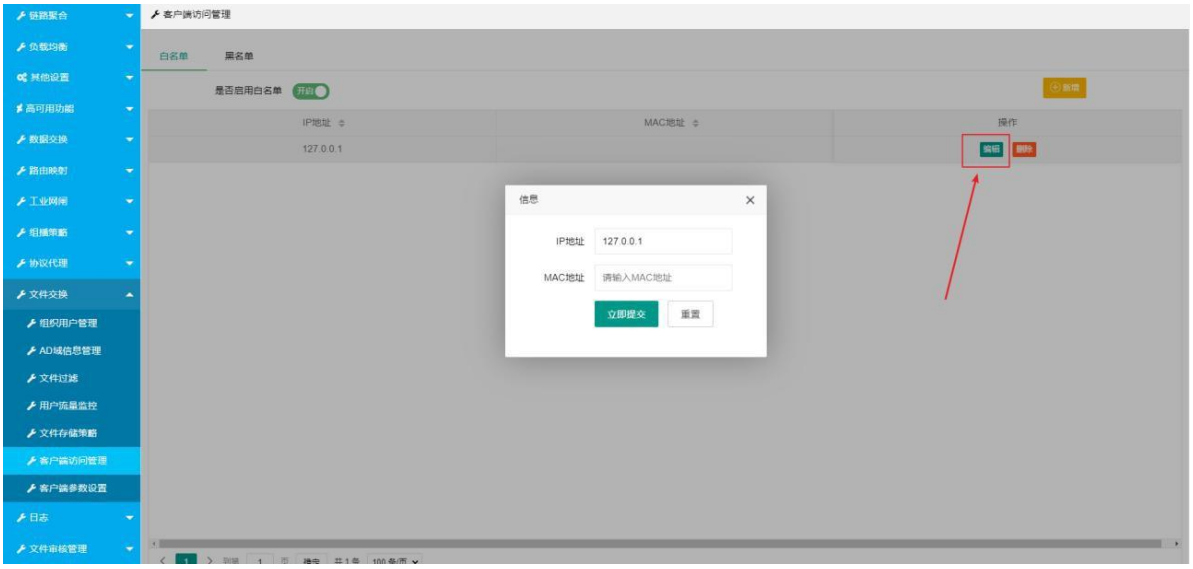


图 5.11.6.2-1 白名单编辑界面

5.11.6.3 白名单删除

点击删除按钮，提示“是否删除提示信息”，点击确认，删除此设置的黑名单 IP 地址。

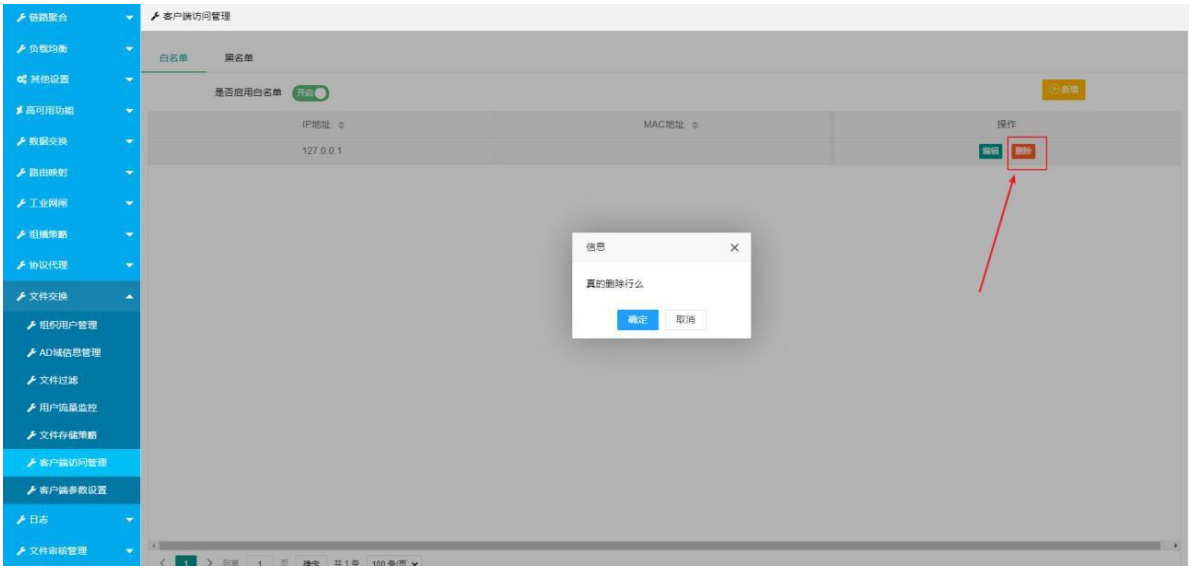


图 5.11.6.3-1 白名单删除界面

5.11.6.4 黑名单新增

点击右上角新增按钮，弹出新增IP 地址和mac 地址的框架，填写正确的的格式，开启按钮后不允许登录使用客户端

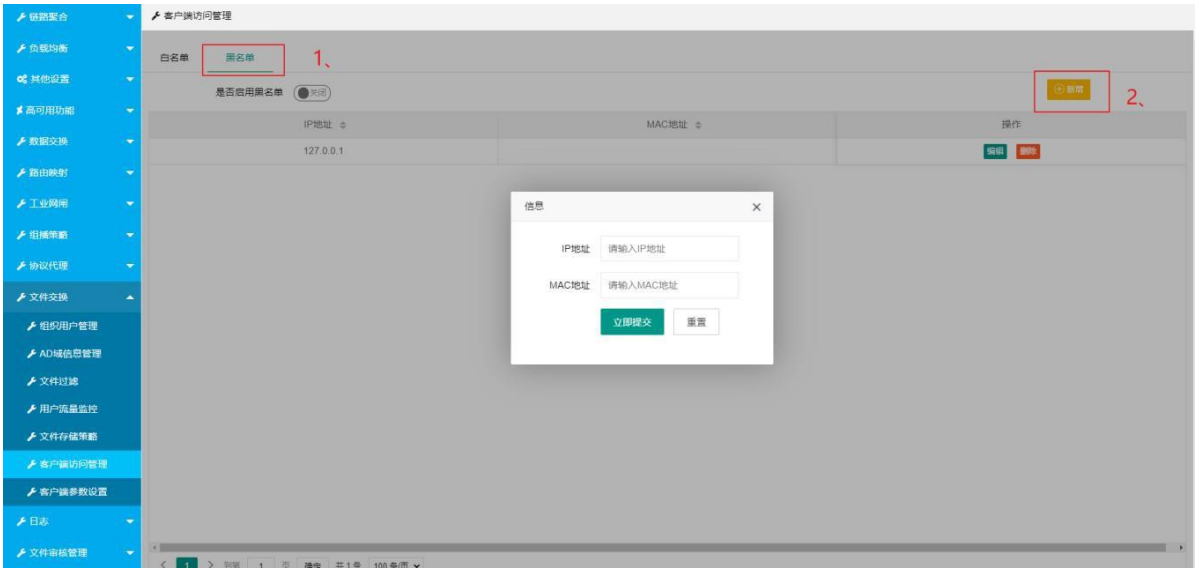


图 5.11.6.4-1 黑名单新增界面

5.11.6.5 黑名单编辑

更改想要修改的ip 地址和mac 地址，不允许登录的 IP 地址和mac 地址。

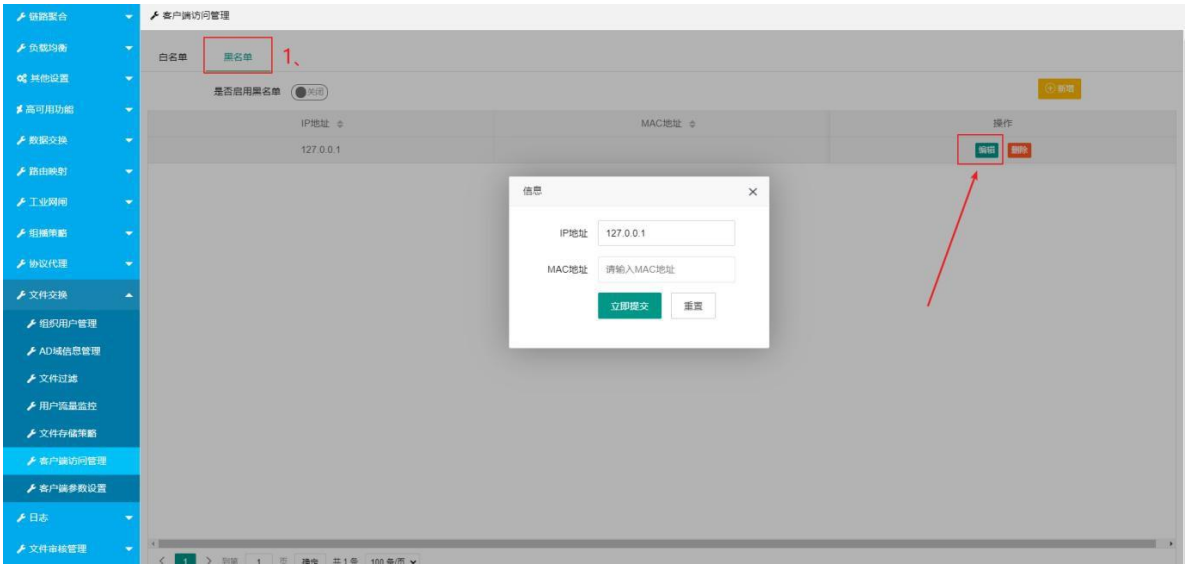


图 5.11.6.5-1 黑名单编辑界面

5.11.6.6 黑名单删除

选中所要删除的黑名单IP 地址后，即用户可以正常登录使用客户端，如下图所示：

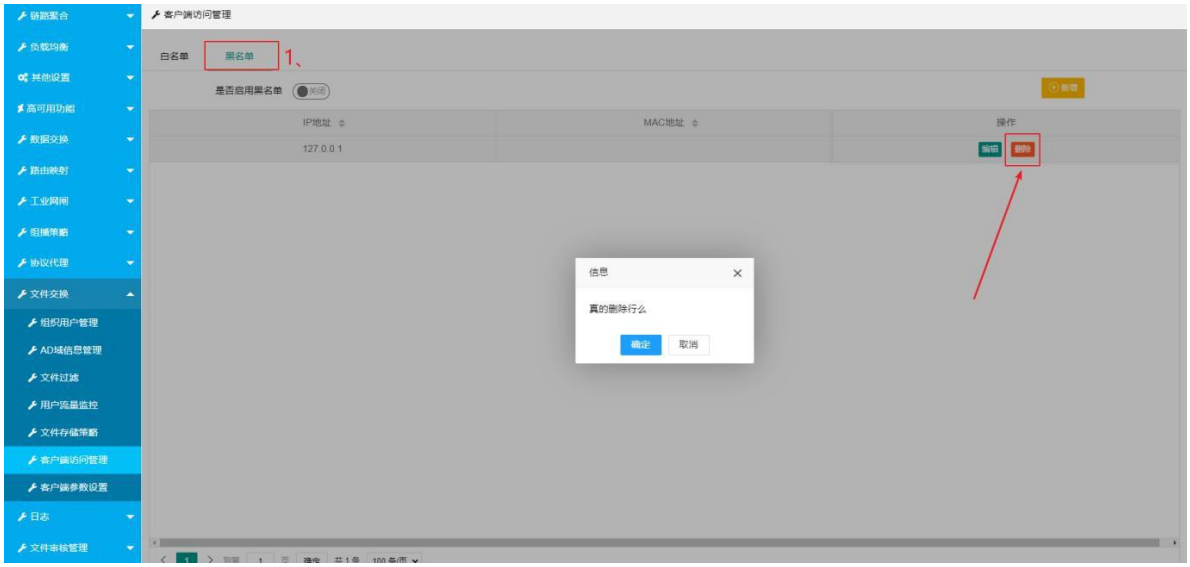


图 5.11.6.6-1 黑名单删除界面

5.11.7 客户端参数设置

文件交换系统客户端支持配置用户密码过期时间、登录超出次数锁定等功能，如下图所示：

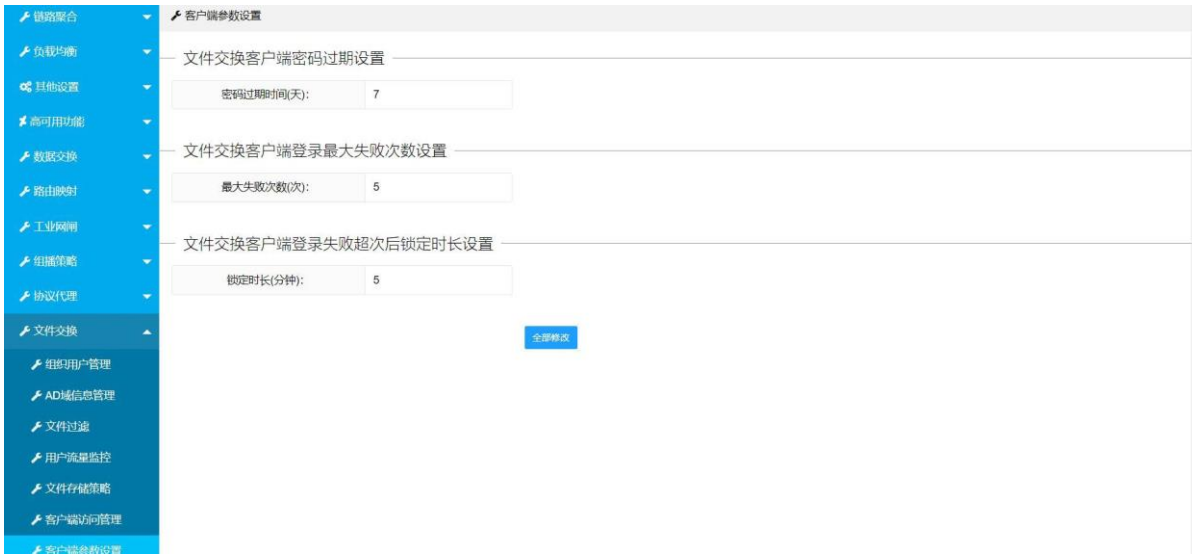


图 5.11.7-1 客户端参数设置界面

客户端参数设置说明：

- 文件交换客户端密码过期设置-密码过期时间： 单位为天，以当前密码修改时间为开始时间计算，配置天数后，客户端自动弹出提示及修改密码窗口
- 登录最大失败次数：单位为次，登录失败次数等于配置次数后，该用户账号被锁定， 在锁定时间内该用户无法登录客户端
- 锁定时长：单位为分钟，指定用户锁定的时长，在该时长内用户被锁定无法登录，该时长后用户账号解锁可正常登录

5.12 日志

安全保密员日志主要记录安全审计员用户登录的信息，如下图所示：

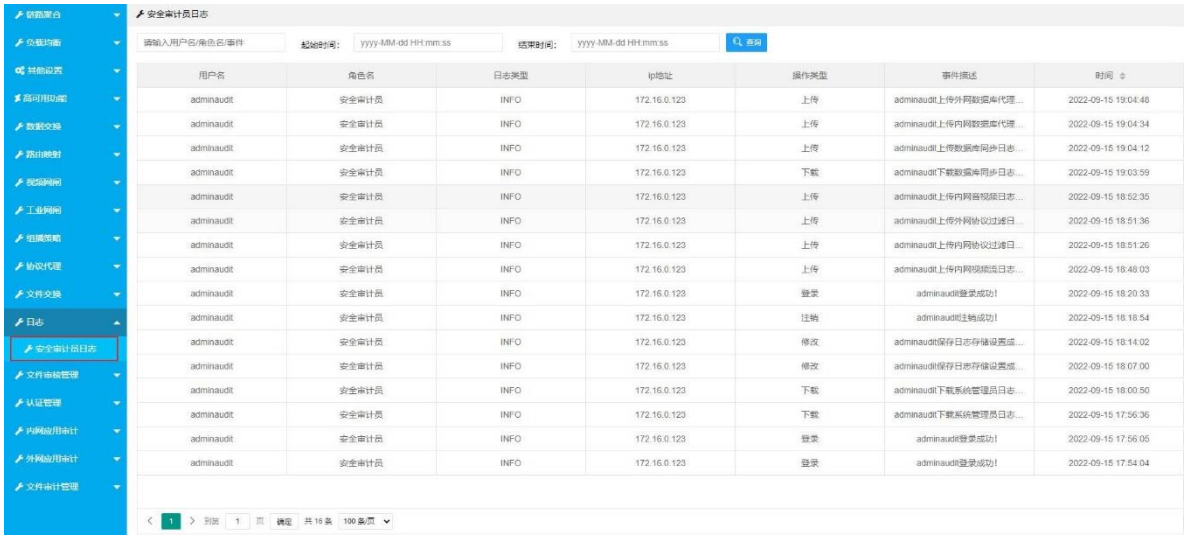


图 5.12-1 客户端参数设置界面

5.13 文件审核管理

『审核管理』可以对被系统过滤的文件进行审核，查看审核通过和审核不通过的文件信息。『审核管理』包括『等待审核』、『审核已通过』和『审核未通过』三个界面。

5.13.1 等待审核

『等待审核』界面会展示所有被系统过滤的文件信息，可以将文件下载后进行审核，审核通过的文件才允许接收，审核不通过的文件将不会被用户接收。

在菜单栏左侧选择『审核管理』→『等待审核』，进入等待审核界面。如下图所示：

图 5.13.1-1 等待审核界面

等待审核参数说明：

- 下载审核操作：可以将文件下载下来进行审核。

- 允许接收操作：文件审核通过，接收用户可以接收到此文件
- 不允许接收操作：文件审核不通过，接收用户无法接收此文件。

5.13.2 审核已通过

『审核已通过』界面展示用户审核通过的文件记录，用户可以下载审核通过的文件，查看文件内容。在菜单栏左侧选择『审核管理』→『审核已通过』，进入审核已通过列表界面→点击下载审核，可以将此文件下载下来查看文件内容。如下图所示：

图 5.13.2-1 审核已通过界面

5.13.3 审核未通过

『审核未通过』界面展示用户审核通过的文件记录，用户可以下载审核通过的文件，查看文件内容。在菜单栏左侧选择『审核管理』→『审核未通过』，进入审核未通过列表界面，进入审核已通过列表界面→点击下载审核，可以将此文件下载后查看文件内容，如图所示。

图 5.13.3-1 审核未通过界面

5.14 认证管理

5.14.1 新增用户身份认证信息

新提供视频呼叫限制功能，如下图所示：

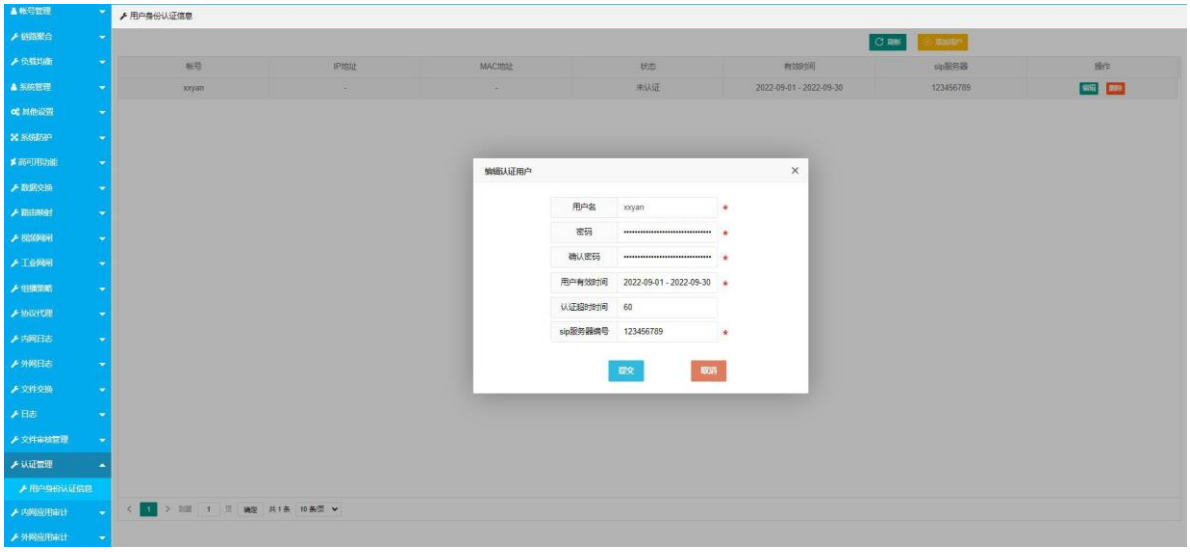


图 5.14.1-1 新增用户身份认证信息

认证管理配置参数说明：

- 用户名：认证的用户名称
- 密码：认证用户的密码
- 确认密码：认证用户的确认密码
- 用户有效时间：用户可认证的有效时间
- 认证有效时间：允许上级发起视频呼叫的有效时间
- sip 服务器编号：上级sip 服务器编号

5.14.2 用户登录认证

用户登录http://192.168.1.1（默认管理口IP），进行用户登录认证。如下图所示：

图 5.14.2-1 用户登录认证

5.15 内网应用审计

『内网应用审计』记录用户在内网登录文件交换客户端的操作日志，审计管理员通过查看『内网应用审计』了解用户登录文件交换客户端的操作信息。包括『用户登录日志』、『发送文件日志』、『接收文件日志』、『查杀病毒日志』。

5.15.1 用户登录日志

『用户登录日志』主要用来记录用户登录文件交换客户端的登录日志。

在左侧菜单栏选择 『内网应用审计』→『用户登录日志』,进入用户日志界面。如下图所示:

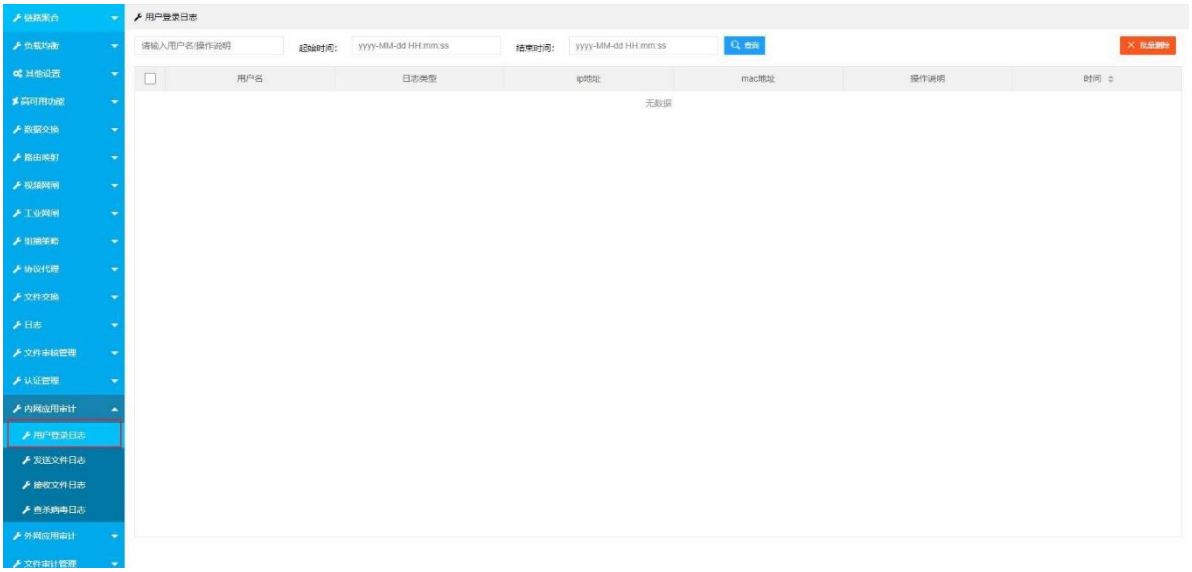


图 5.15.1-1 用户登录日志界面

5.15.1.1 查找

在用户登录日志列表界面，输入关键字如：用户名，操作说明，IP 地址，mac 地址，也可输入起始时间、结束时间，然后点击查询按钮进行过滤筛选。如图下图所示:

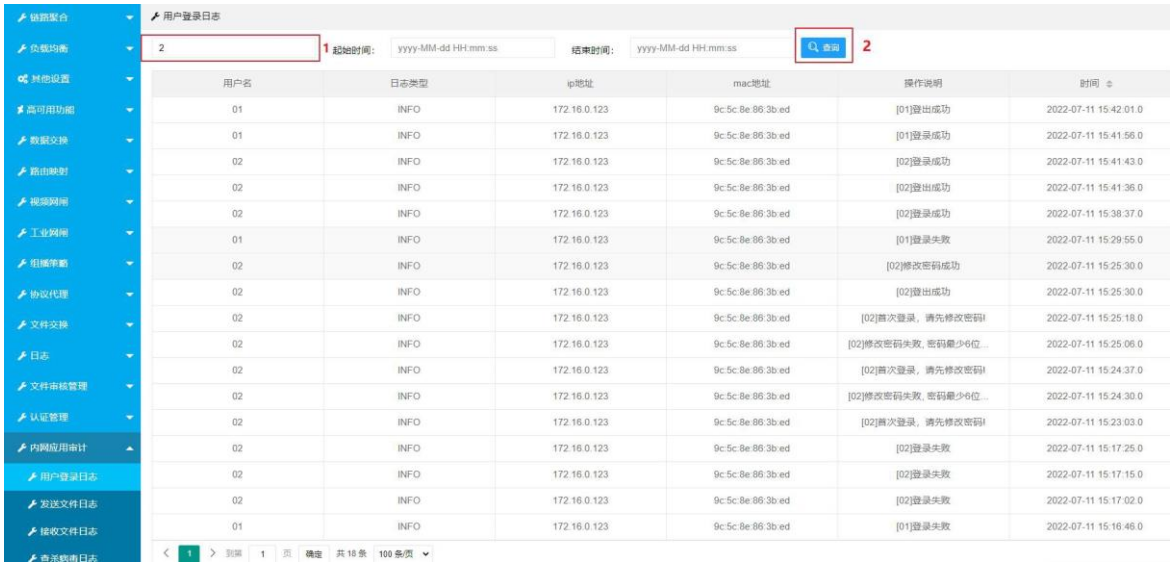


图 5.15.1.1-1 日志查找条件配置界面

5.15.2 发送文件日志

『发送文件日志』记录用户登录文件交换客户端发送文件的日志。选择『内网应用审计』

→『发送文件日志』,进入发送文件日志界面，如下图所示:

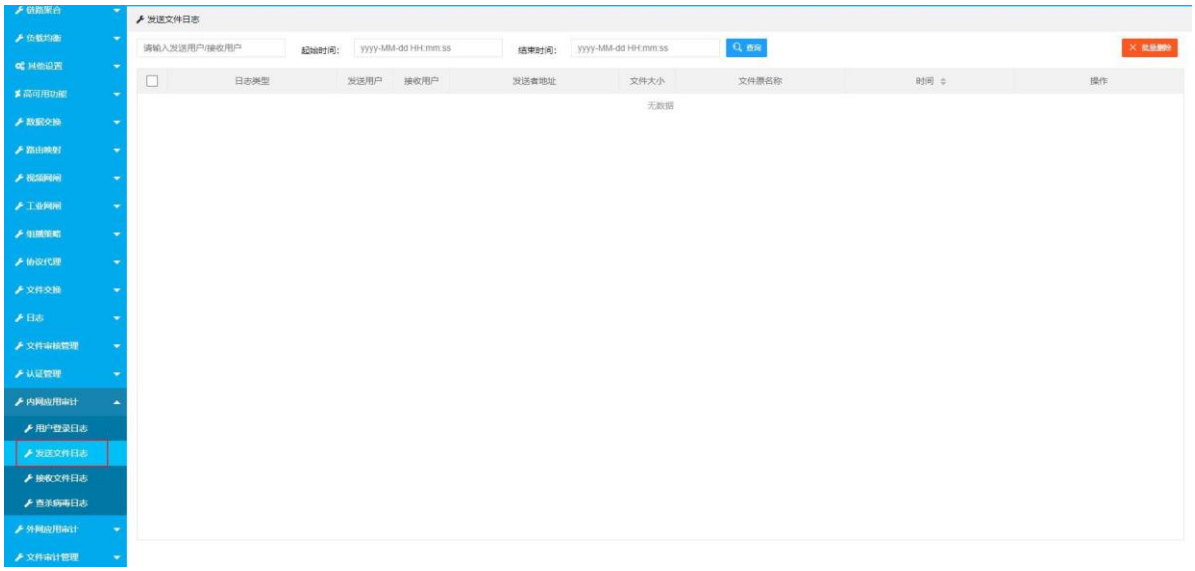


图 5.15.2-1 用户发送文件日志界面

5.15.2.1查找

在发送文件日志界面，输入关键字如：发送用户名或接收用户名，文件名称，发送者IP地址，还可输入起始时间、结束时间，然后点击查询按钮进行过滤筛选。如下图所示:

图 5.15.2.1-1 发送日志查询条件输入界面

5.15.2.2下载文件

在发送文件日志界面，在每条日志记录的右侧，点击下载按钮，下载已发送的文件。如下图所示:

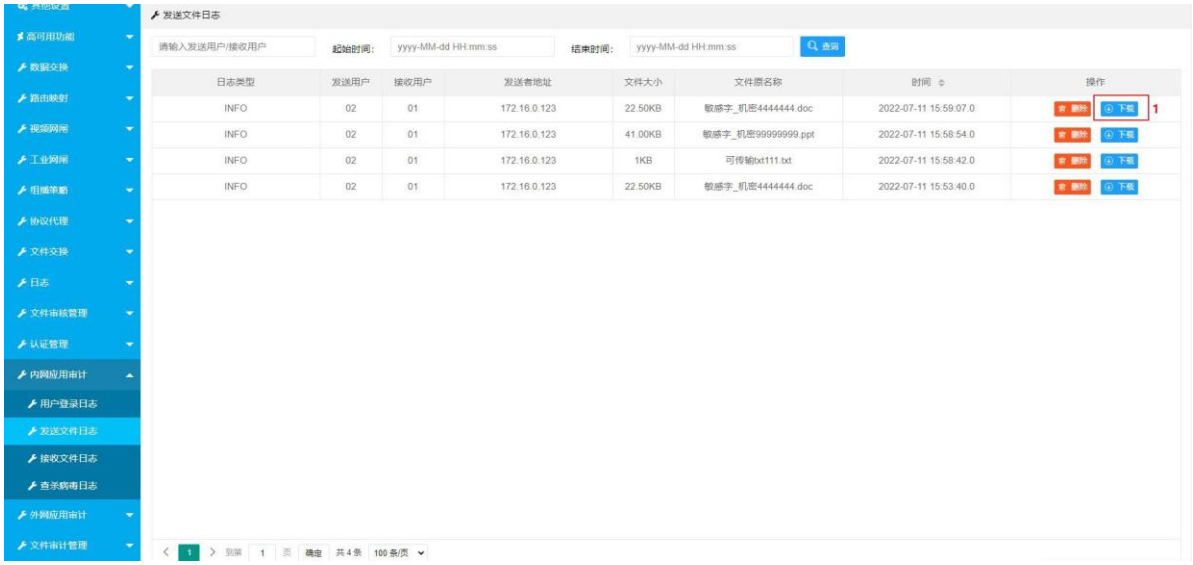


图 5.15.2.2-1 下载已发送文件界面

5.15.2.3 删除发送文件记录

在发送文件日志界面，在每条日志记录的右侧，点击删除按钮，删除此条发送记录，如下图所示：

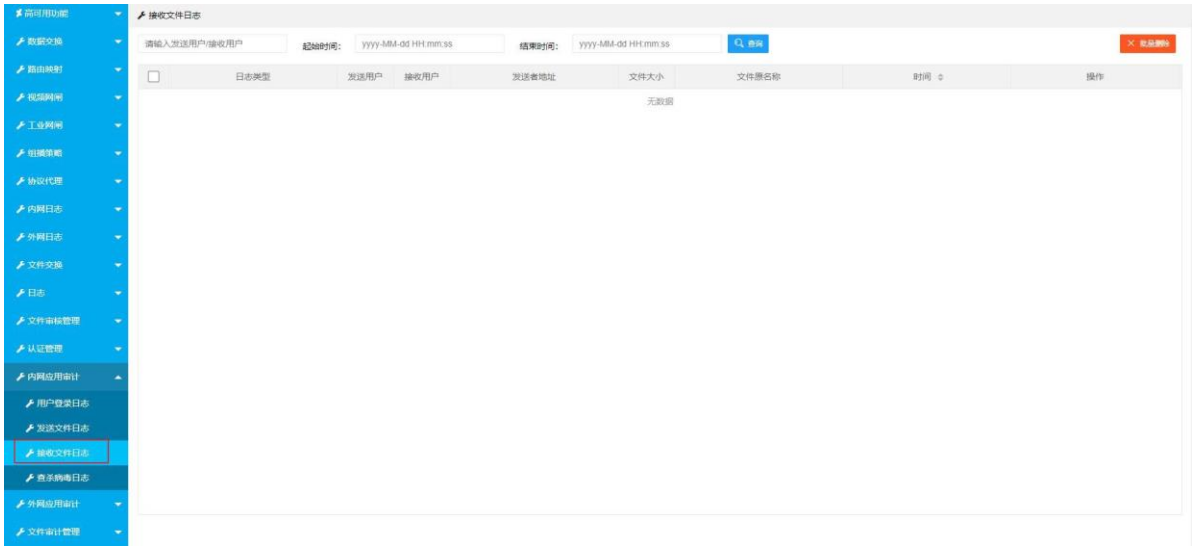


图 5.15.2.3-1 删除文件发送记录

5.15.3 接收文件日志

『接收文件日志』记录用户接收文件的日志。选择 『内网应用审计』→『接收文件日志』，进入接收文件日志界面，如下图所示：

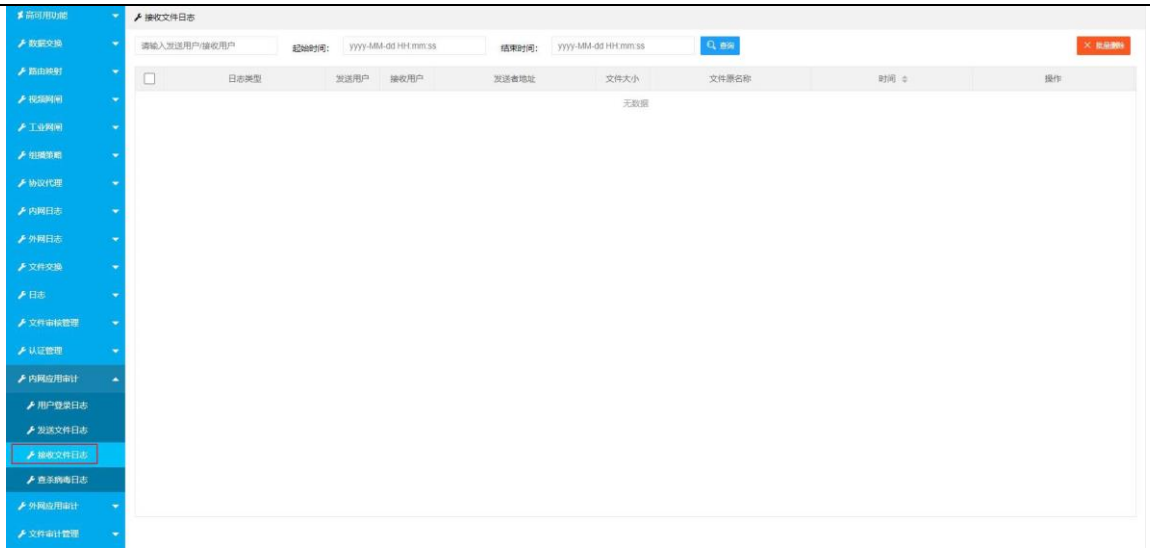


图 5.15.3-1 用户接收文件日志界面

5.15.3.1 查找

在接收文件日志界面，输入关键字如：发送用户名或接收用户名，文件名称，发送者IP地址，还可输入起始时间、结束时间，然后点击查询，如下图所示：

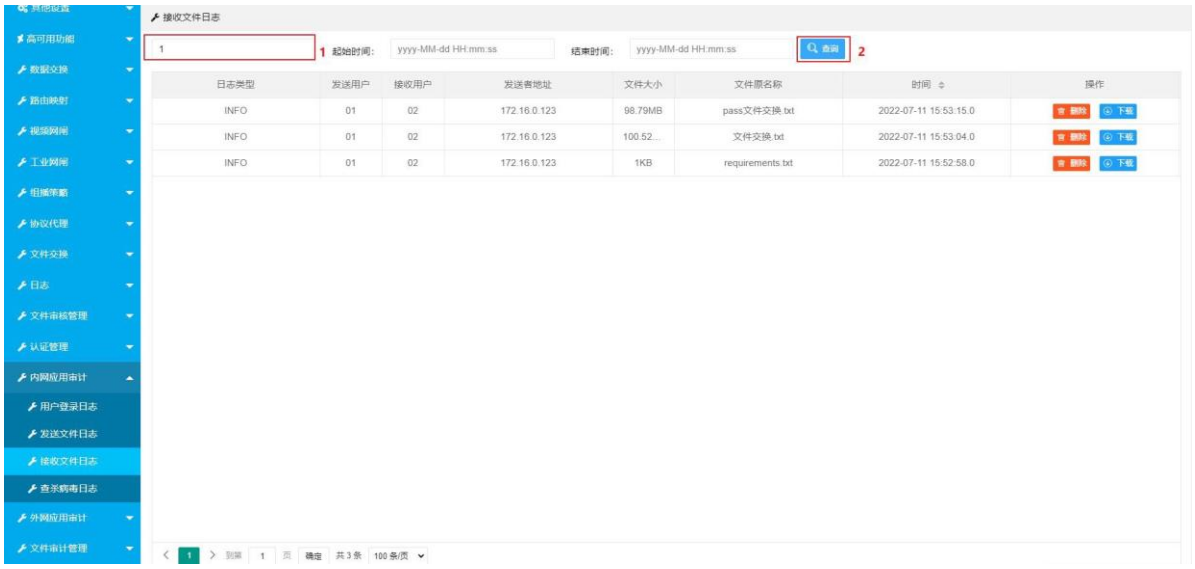


图 5.15.3.1-1 接收日志条件查询界面

5.15.3.2下载文件

在接收文件日志界面，在每条日志记录的右侧，点击下载按钮，下载已发送的文件。如下图所示：

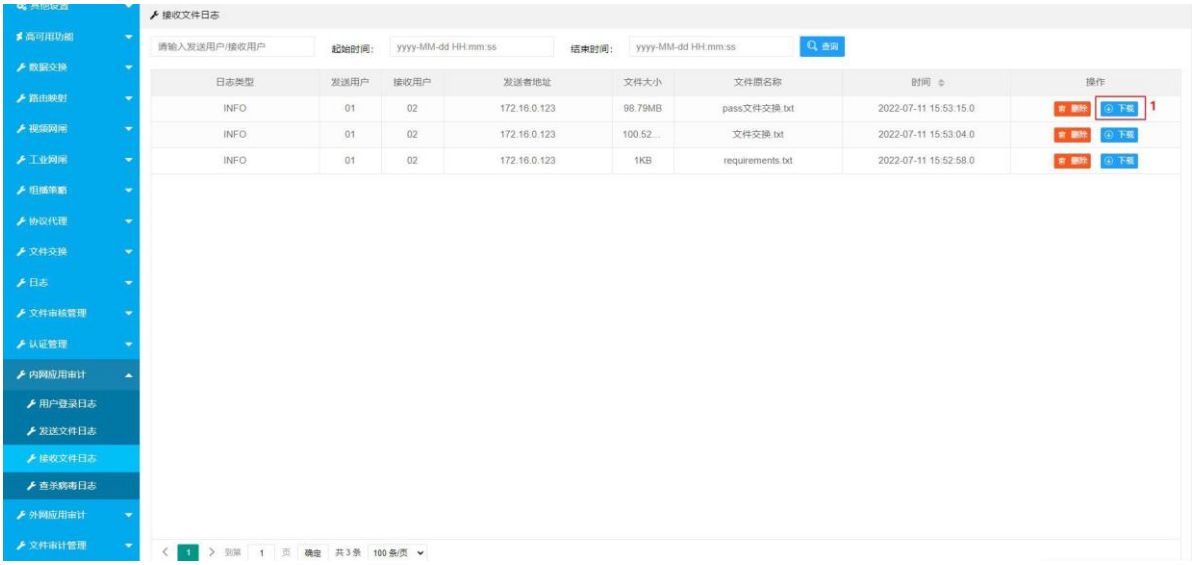


图 5.15.3.2-1 接收日志下载界面

5.15.3.3 删除接收文件记录

在接收文件日志界面，在每条日志记录的右侧，点击删除按钮，删除此条接收文件记录。如下图所示：

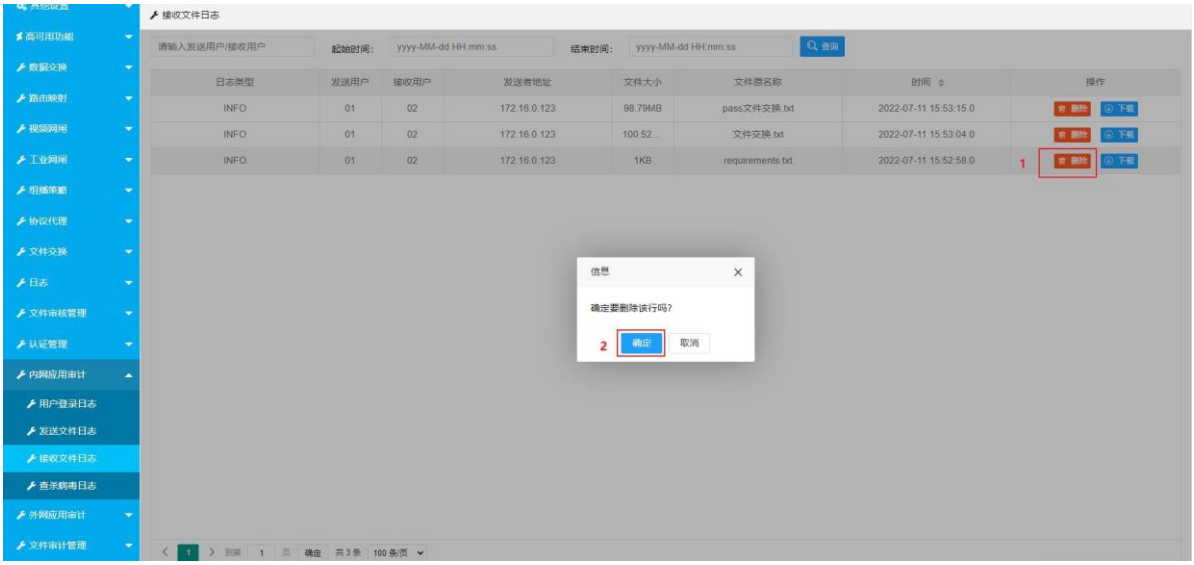


图 5.15.3.3-1 日志删除界面

5.15.4 查杀病毒日志

『查杀病毒日志』记录系统查杀病毒文件的日志。

在左侧菜单栏选择 『内网应用审计』→『查杀病毒日志』,进入查杀病毒日志界面，如下图所示：

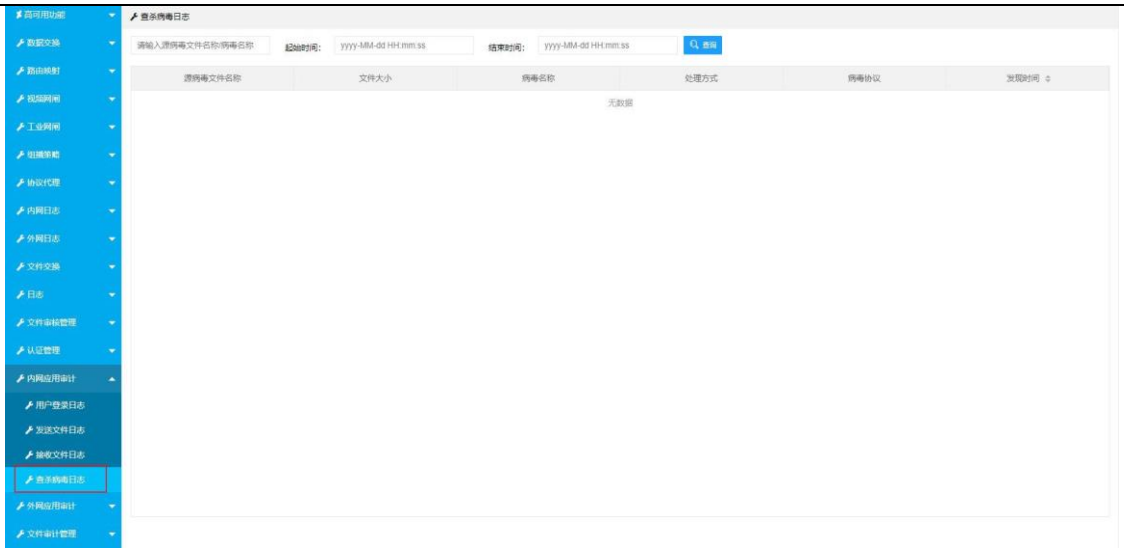


图 5.15.4-1 查杀病毒日志界面

5.15.4.1 查找

在接收文件日志界面，输入关键字如：源病毒文件名称，病毒名称，还可输入起始时间、结束时间，然后点击查询按钮，如下图所示：

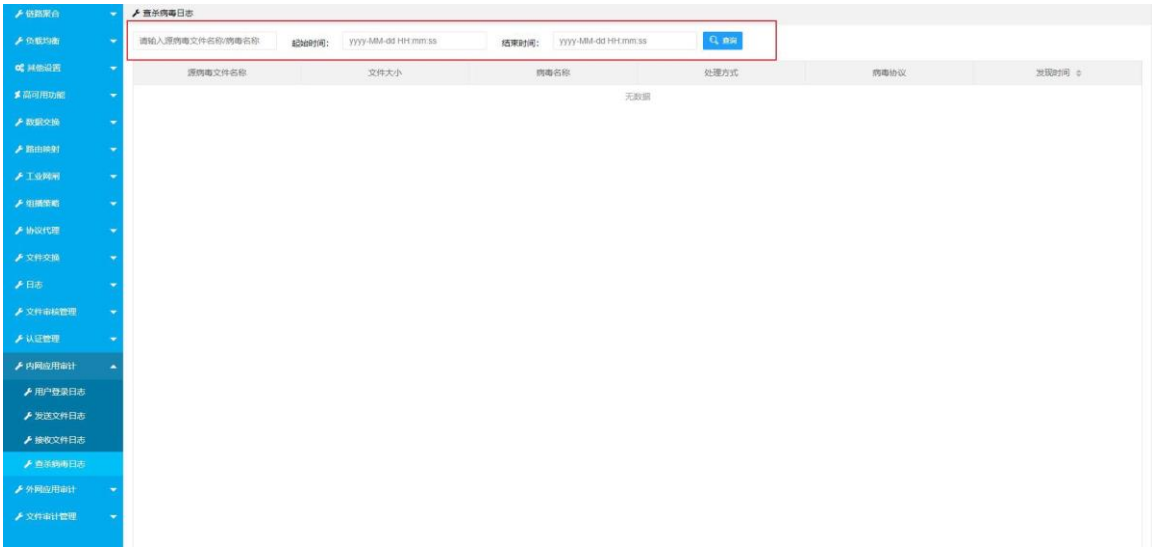


图 5.15.4.1-1 日志查找过滤条件输入界面

5.16 外网应用审计

『外网应用审计』记录用户在外网登录文件交换客户端的操作日志，审计管理员可以根可以通过查看『外网应用审计』了解外网用户登录文件交换客户端的操作信息。

『外网应用审计』包括『用户登陆日志』、『发送文件日志』、『接收文件日志』、『查杀病毒日志』。

5.16.1 用户登录日志

具体操作同内网应用审计用户登录日志，可参考 5.14.1 章节的用户登录日志。

5.16.2 发送文件日志

具体操作同内网应用审计发送文件日志，可参考 5.14.2 章节『发送文件日志』。

5.16.3 接收文件日志

具体操作同内网应用审计接收文件日志，可参考 5.14.3 章节『接收文件日志』。

5.16.4 查杀病毒日志

具体操作同内网应用审计查杀病毒日志，可参考 5.14.4 章节『查杀病毒日志』。

5.17 文件审计管理

『文件审计管理』功能包括『删除日志』、『导入日志』、『导出日志』。如下图所示:

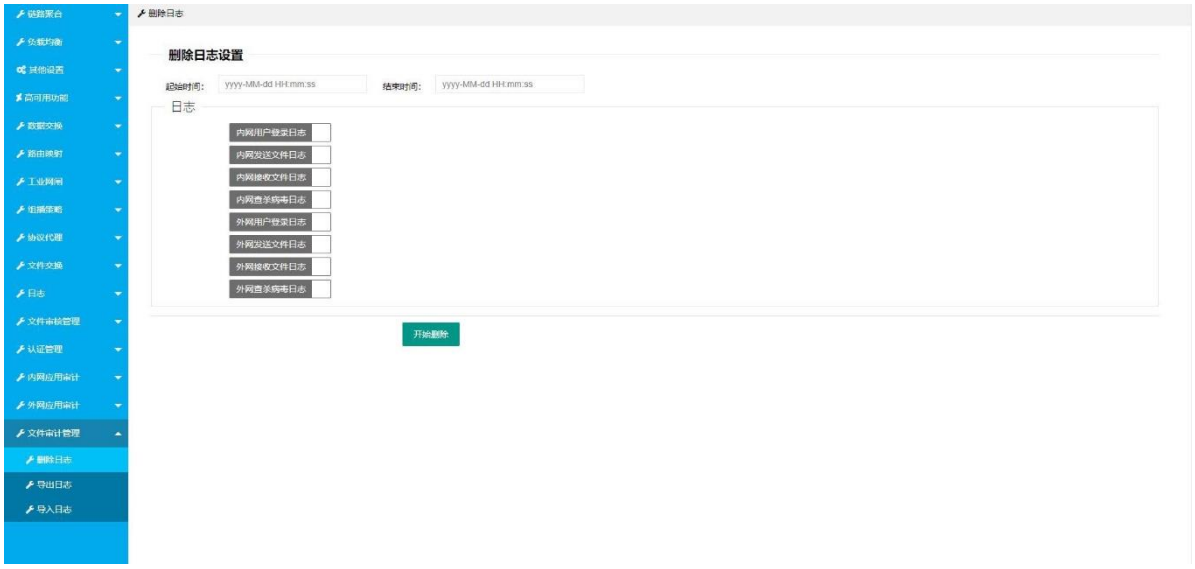


图 5.17.1 文件审计管理界面

5.17.1 删除日志

『删除日志』删除系统日志和网闸内外网应用审计中的应用。

点击『审计管理』→左侧菜单栏选择『删除日志』,进入删除日志设置界面→选择开始时间和结束时间→选择要删除的[日志类别]→点击开始删除，此类别日志对应时间段内的日志被删除。

如果不选择开始时间和结束时间，只选择日志类型，直接点击开始删除，则默认删除被选择日志的所有日志信息。删除步骤如下图所示:

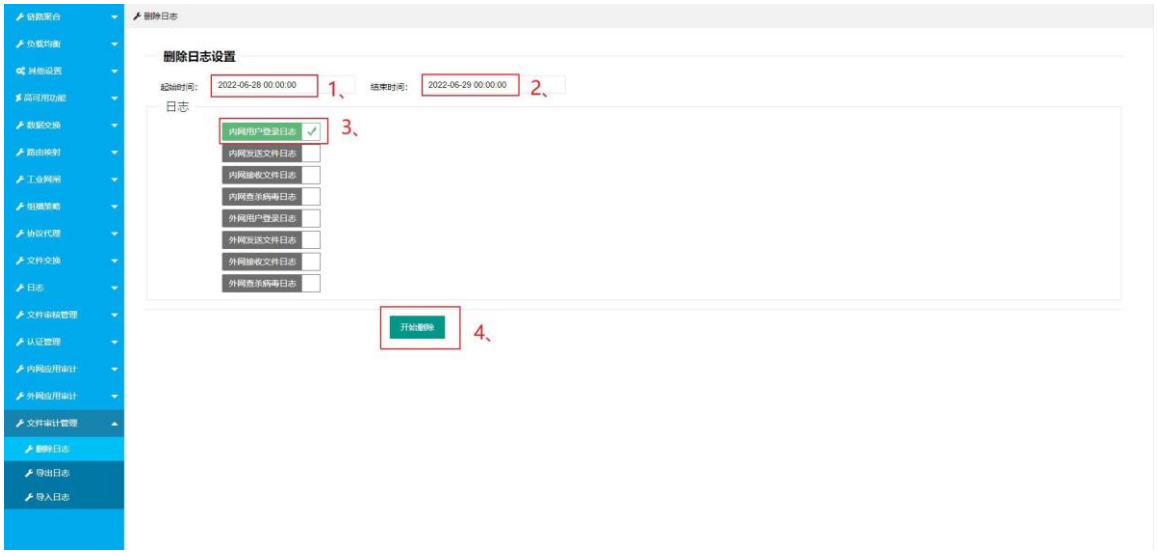


图 5.17.1-1 删除日志界面

5.17.2 导出日志

『导出日志』当文件交换系统存储满后，可以将文件备份到硬盘或电脑，并且在电脑上提供程序，方便查看审计备份后的文件及日志信息。

在左侧菜单栏选择 『审计管理』→『导出日志』,进入导出日志界面，如下图所示。

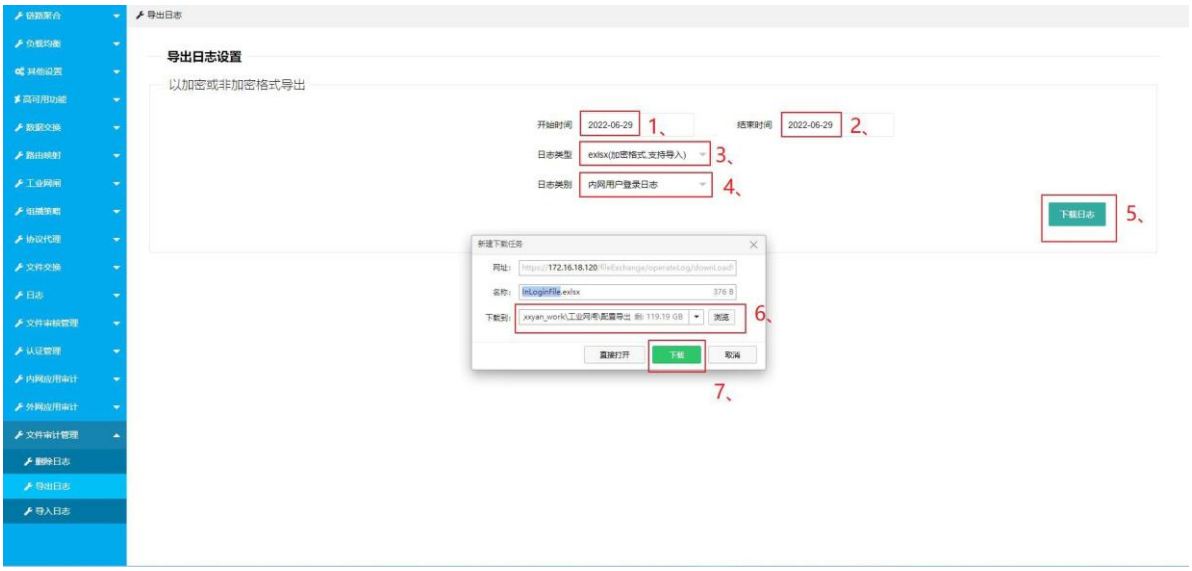


图 5.17.2-1 导出日志设置界面

导出日志配置说明:

1．[开始时间]：需删除日志时间段的开始时间

2．[结束时间]：需删除日志时间段的结束时间

3．[日志类型]：xlsx(默认，非加密格式，不支持导入)；exlsx(加密格式，支持导入)日志类别可以选择：用户登录日志（默认）、文件发送日志、文件接受日志、查杀病毒日志

5.17.3 导入日志

『导入日志』将备份的日志信息，上传到页面进行查看审计。

在左侧菜单栏选择 『审计管理』→『导入日志』,进入导入日志界面，如下图所示:

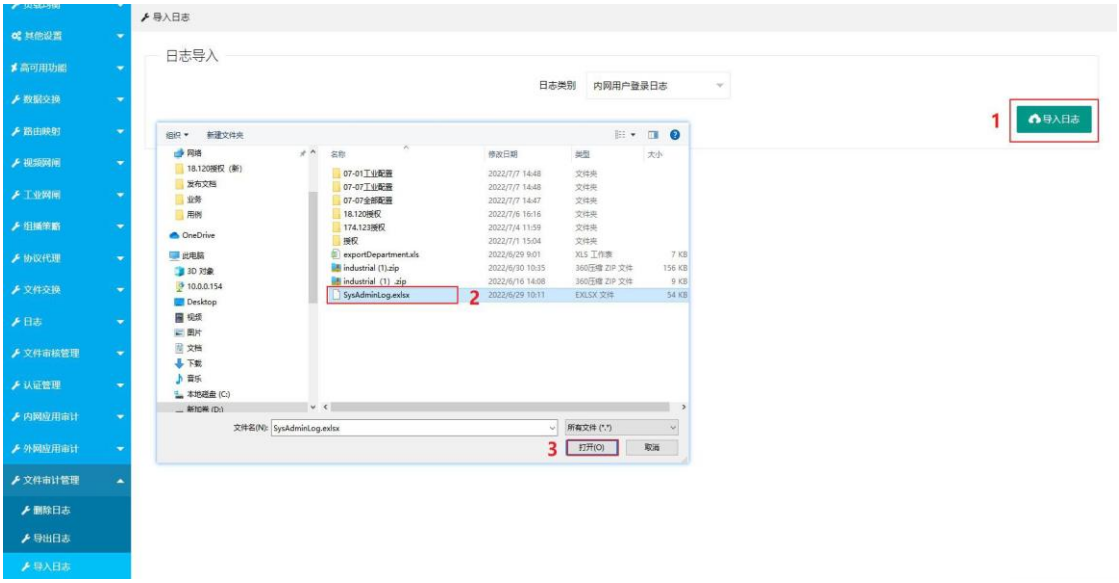


图 5.17.3-1 导入日志界面

6. 日志管理

6.1 系统管理

6.1.1 日志下载

系统管理操作界面→点击『系统管理』→点击『日志管理』进入到日志管理界面→点设置开始及结束时间、日志类型和加密类型→点击下载日志，在下面弹框中点击打开或者保存，进行日志下载，如下图所示：

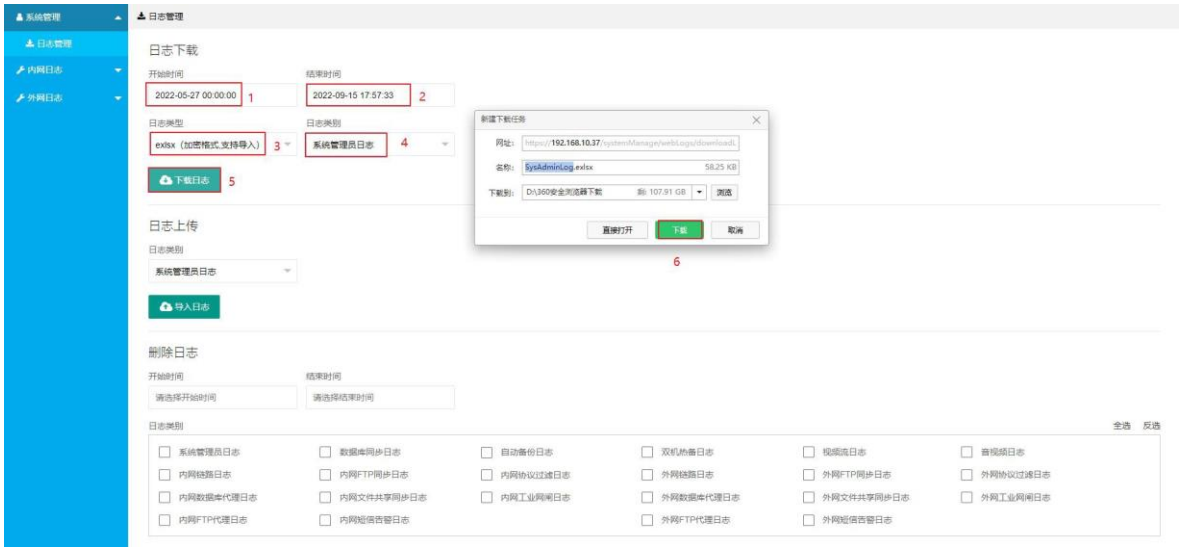


图 6.1.1-1 下载日志界面

6.1.2 日志上传

点击『导入日志』，选择日志文件进行导入操作。注：上传的日志文件格式需要与导出的日志格式对应，否则会出现导入失败！如下图所示：

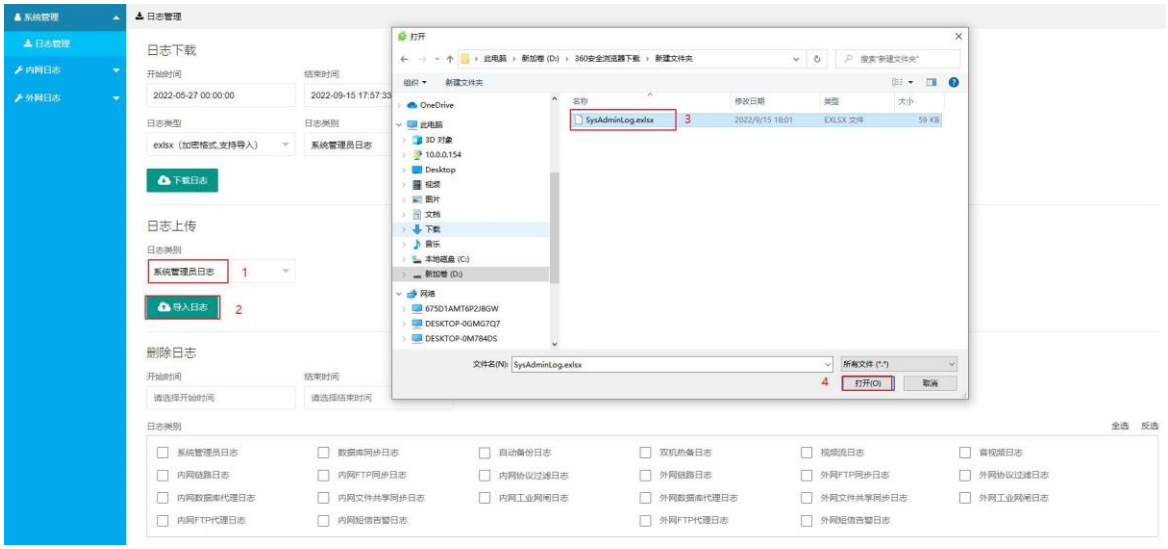


图 6.1.2-1 上传日志界面

6.1.3 日志删除

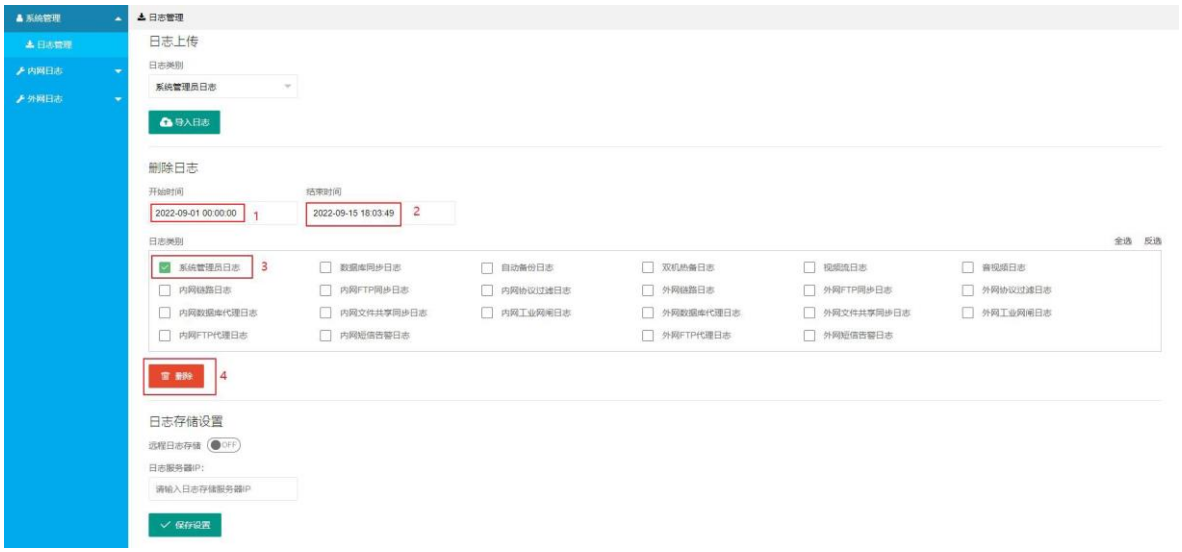


图 6.1.3-1 日志删除设置界面

6.1.4 日志存储设置

点击『日志存储设置』，打开存储开关，输入日志存储服务器地址，如下图所示：

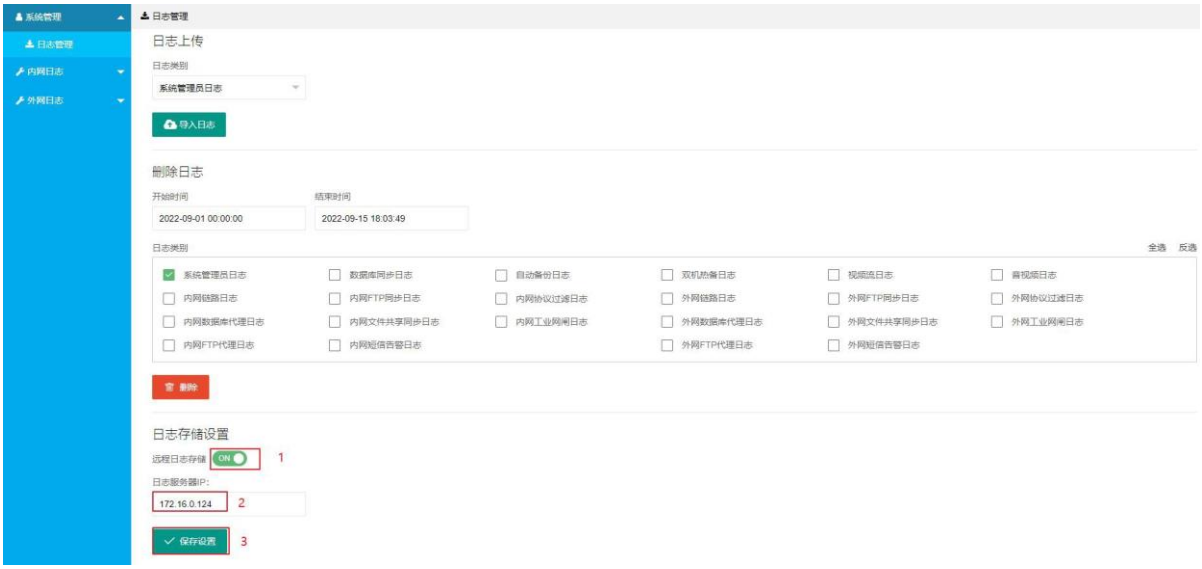


图 6.1.4-1 日志存储设置界面

6.2 内网日志

『内网日志』包括『内网预警信息日志』、『内网 FTP 同步日志』、『内网 FTP 代理日志』、『内网链路日志』、『内网双机热备日志』、『数据库代理日志』、『内网工业网闸日志』、『文件共享同步日志』、『数据库同步日志』、『系统管理员日志』、『内网系统升级日志』、『内网短信告警日志』、『内网视频流管理日志』、『内网协议过滤日志』、『内网自动备份日志』、『音视频日志』。

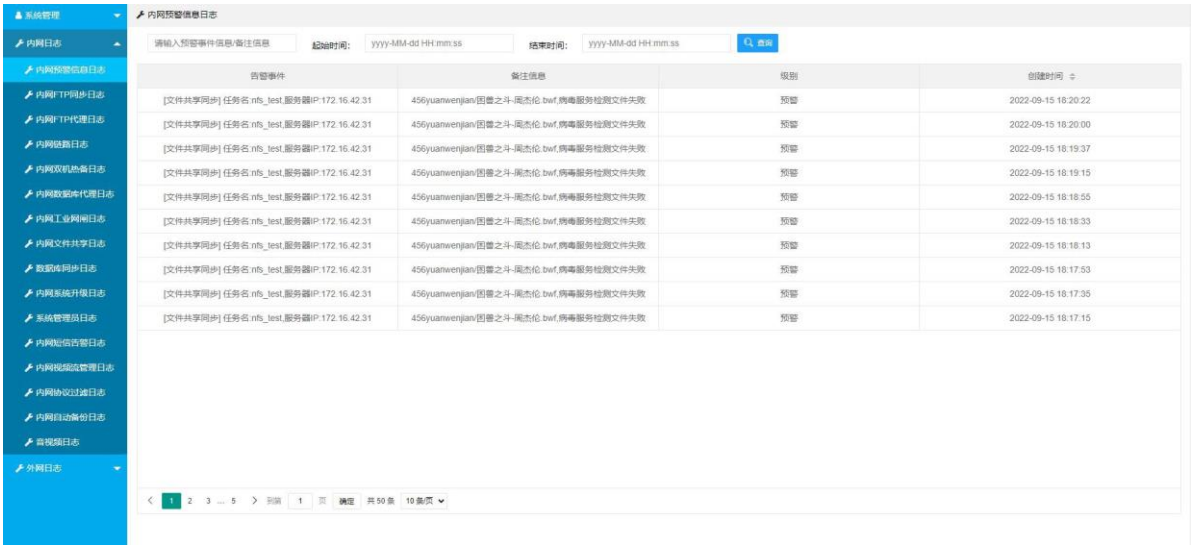


图 6.2-1 内网预警信息日志图

6.2.1 内网预警信息日志

内网预警信息日志包含了入侵告警日志和 FTP、文件同步等运行告警信息，当存在外部入侵时，会有相应的日志记录，可在内外网的预警信息日志中查看。如下图所示：

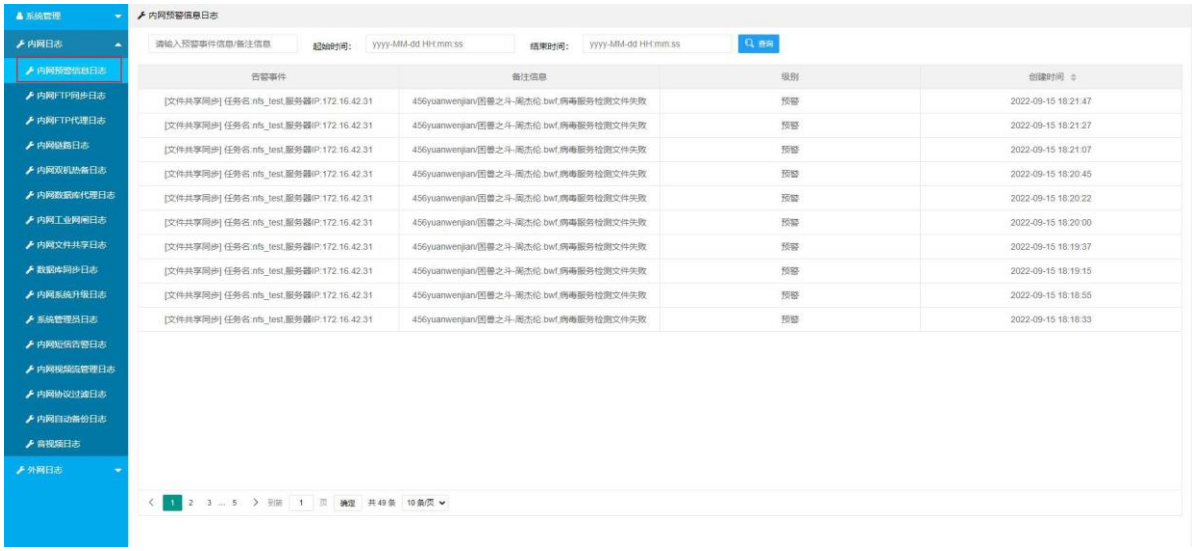


图 6.2.1-1 内网预警信息日志图

6.2.2 内网FTP 同步日志

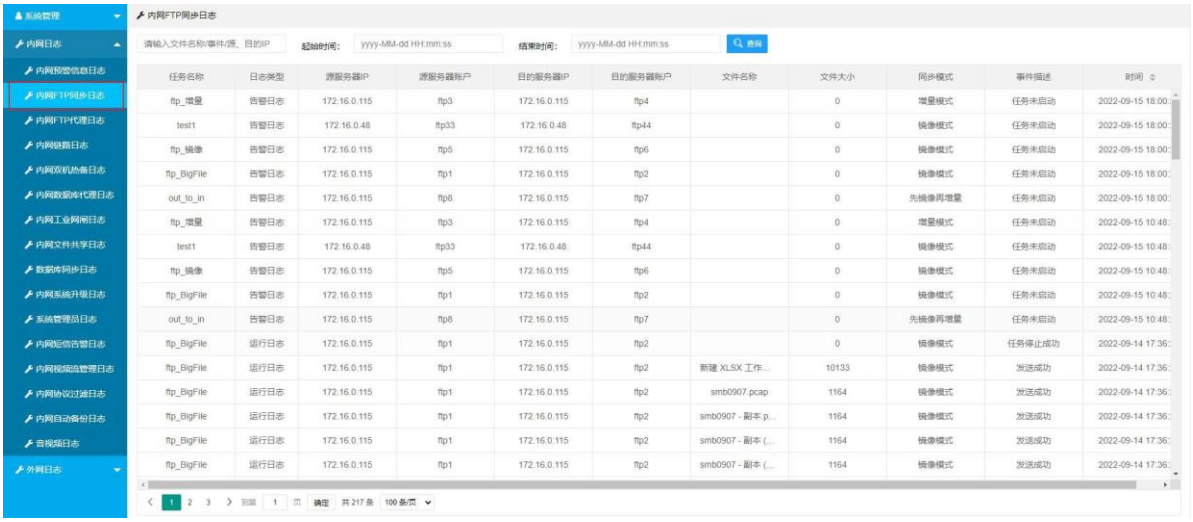


图 6.2.2-1 内网 FTP 同步日志图

内网FTP 同步日志参数说明：

- 请输入文件名和事件： 模糊查询到同步的文件名或者事件进行快速查询该事件
- 起始时间：同步任务开启时间
- 结束时间：同步任务完成结束时间
- 任务名称：创建任务的名称
- 日志类型：日志种类
- 源服务器IP：内网FTP 服务器ip
- 源服务器账户：内网 FTP 服务器账户
- 目的服务器IP: 外网FTP 服务器ip
- 目的服务器账户：外网 FTP 服务器账户
- 文件名称：要同步文件的文件名
- 文件大小：同步文件的大小
- 同步模式：同步的模式，例如：先镜像后增量或者增量模式
- 事件描述：任务同步的状态是成功还是失败
- 时间：任务完成后时间，也就是结束时间

6.2.3 内网FTP 代理日志

FTP 代理日志记录了FTP 代理功能的文件上传下载、拦截日志。

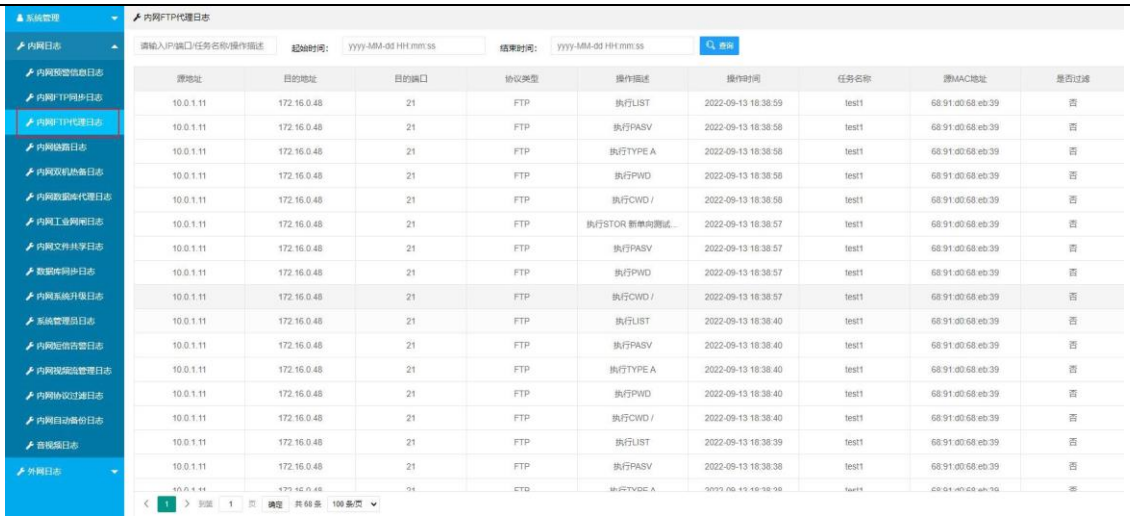


图 6.2.3-1 FTP 代理日志

6.2.4 内网链路日志

链路日志分为历史链路和实时链路日志，所记录的链路均是从外部发起的链路日志（网闸同步程序发起的主动连接将不会记录），可以根据需要进行查询历史链路或者当前存在的链路。如下图所示：

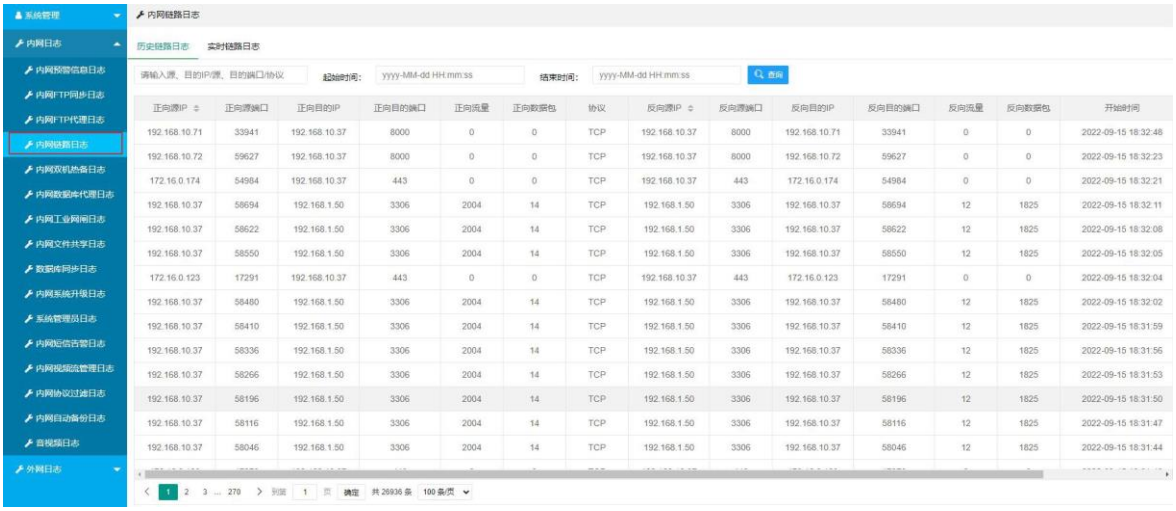


图 6.2.4-1 内网链路日志

6.2.5 内网双机热备日志

双机热备日志记录的是主备机切换的日志信息。

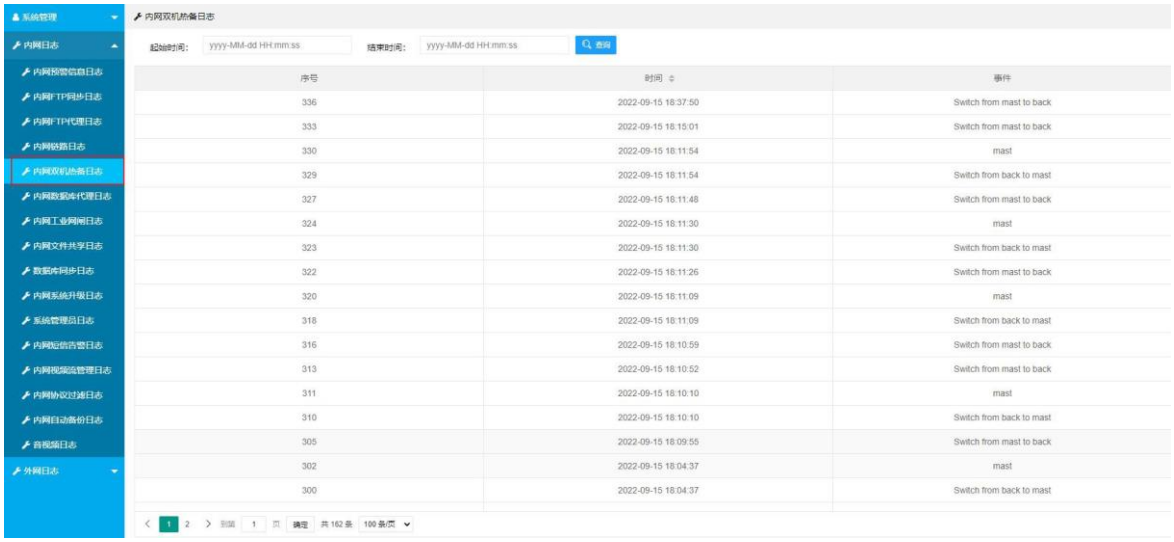


图 6.2.5-1 内网双机热备日志

6.2.6 内网数据库代理日志

数据库代理日志记录的是数据库代理拦截日志信息。

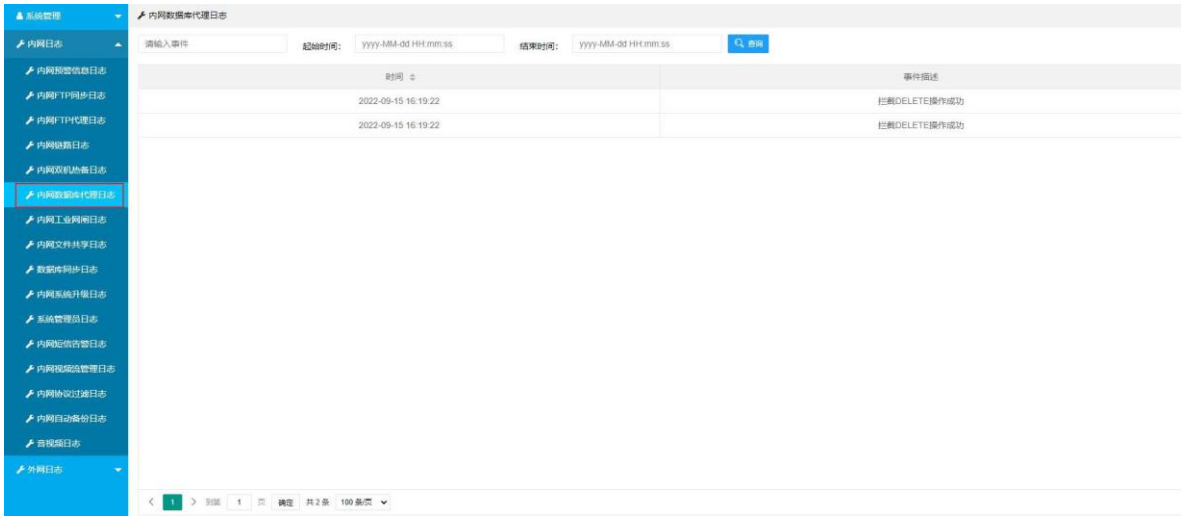


图 6.2.6-1 数据库代理

6.2.7 内网工业网闸日志

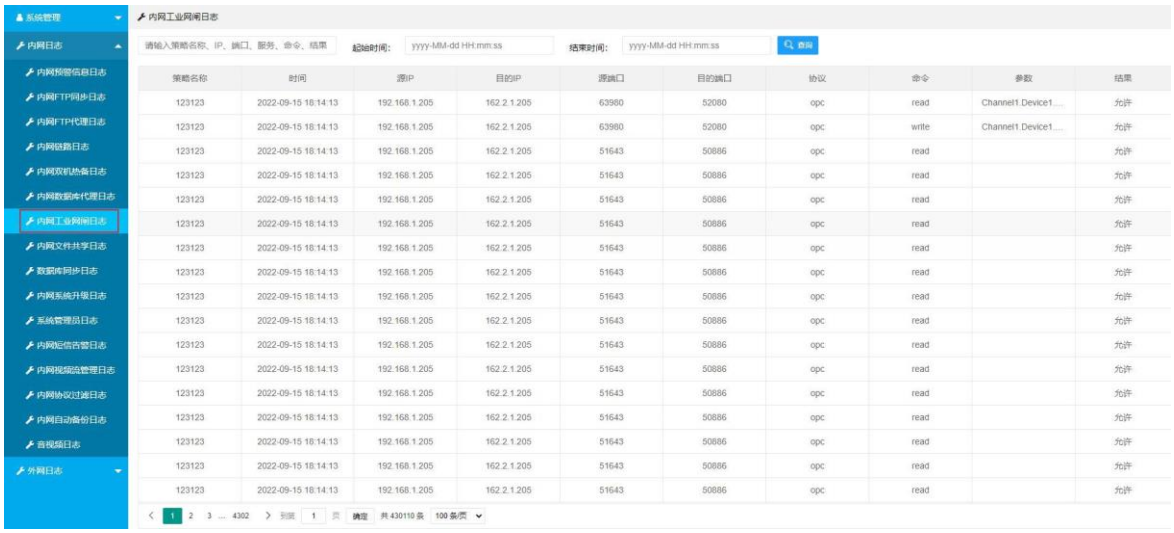


图 6.2.7-1 工业网闸日志图

6.2.8 文件共享同步日志

文件共享同步日志记录的是文件共享同步日志信息。

图 6.2.8-1 文件共享同步日志图

文件共享同步日志参数说明：

- 请输入文件名和事件： 模糊查询到同步的文件名或者事件进行快速查询该事件
- 起始时间：同步任务开启时间
- 结束时间：同步任务完成结束时间
- 任务名称：创建任务的名称
- 日志类型：日志种类
- 源服务器IP: 内网服务器ip
- 源连接协议：SMB、NFS
- 源服务器账户：内网服务器账户
- 源共享名：源端共享文件夹名字

- 目的服务器IP：外网服务器ip
- 目的连接协议：SMB、NFS
- 目的服务器账户：外网服务器账户
- 目的共享名：目的端共享文件夹名字
- 文件名：要同步的文件名
- 文件大小：同步文件大小
- 同步模式：同步的模式，例如：先镜像后增量或者增量模式
- 事件描述：任务同步的状态是成功还是失败
- 时间：任务结束时间

6.2.9 数据库同步日志

数据库同步日志记录的是数据库同步传输的文件信息记录，如下图所示：

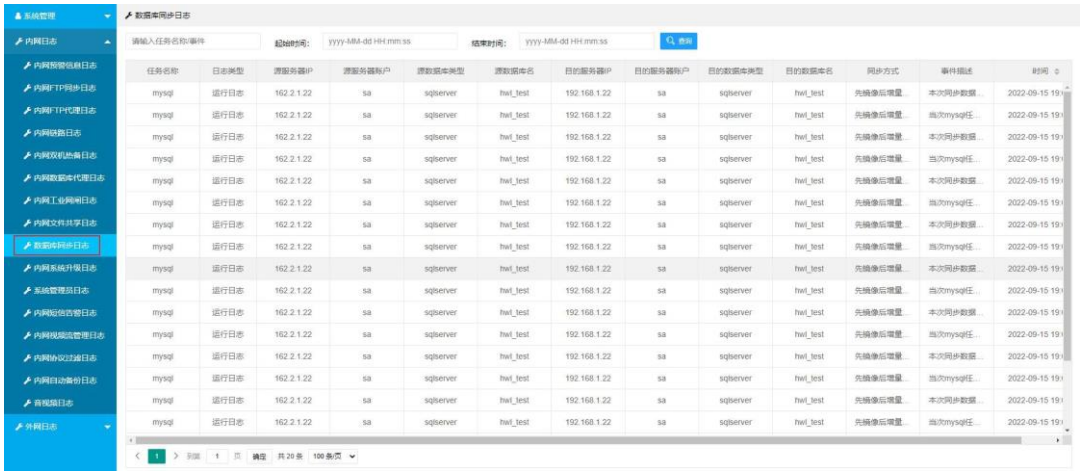


图 6.2.9-1 数据库同步日志图

6.2.10 内网系统升级日志

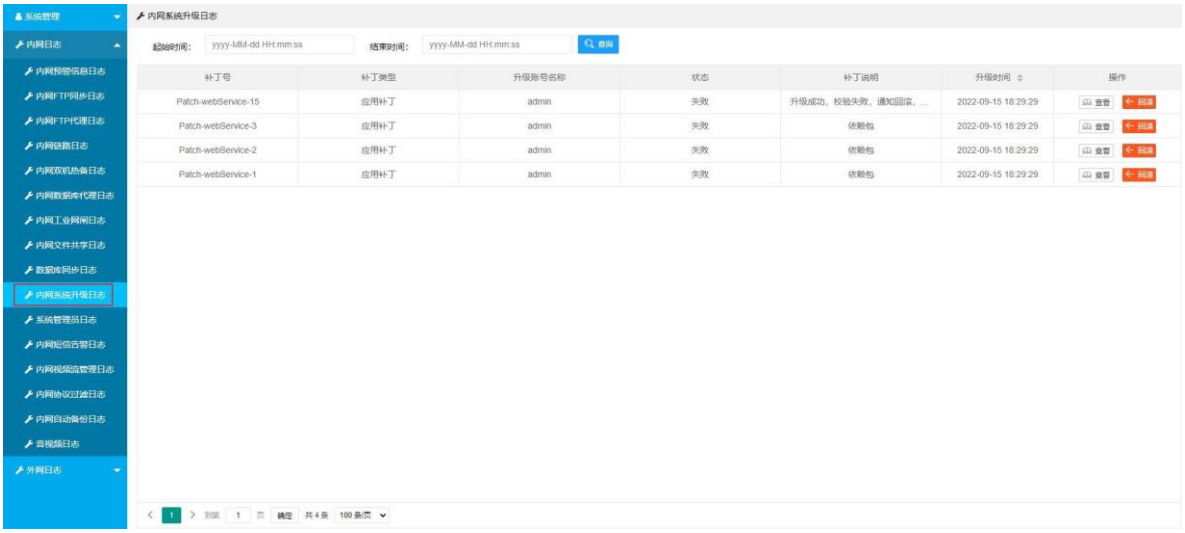


图 6.2.10-1 内网系统升级日志图

6.2.11 系统管理员日志

系统管理员日志记录的是系统管理员登录信息记录，如下图所示：

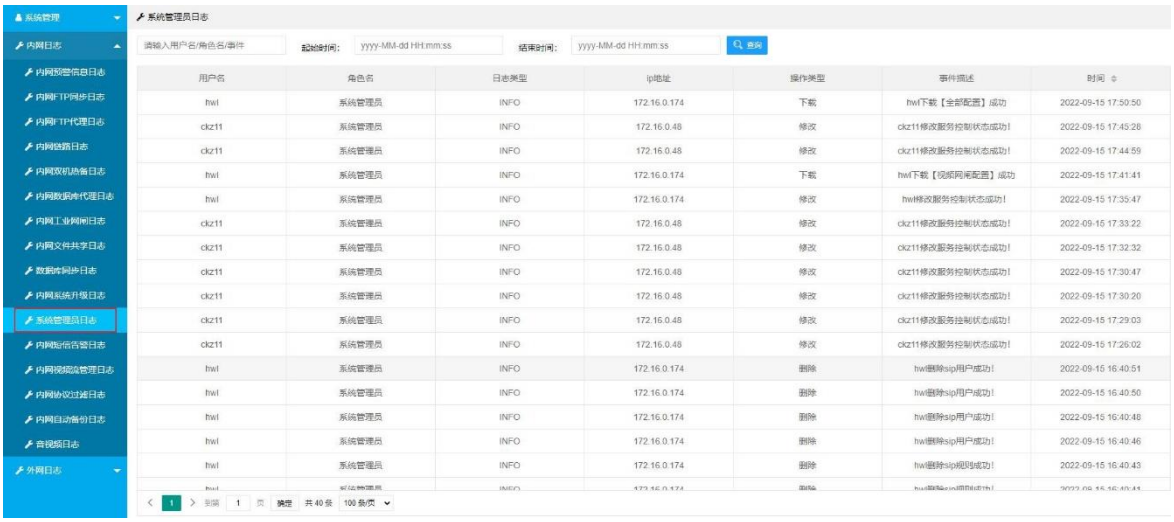


图 6.2.11-1 系统管理员日志图

系统管理员日志参数说明：

- 起始时间：系统管理员用户登录时间
- 结束时间：系统管理员用户退出系统时间
- 用户名：系统管理员登录名字
- 角色名：系统管理员使用的角色
- 日志类型：FATAL 指出每个严重的错误事件将会导致应用程序的退出。该级别较高， 属于重大错误，出现该错误应该直接停止程序
- IP 地址：对应的设备ip
- 操作类型：系统管理员进行了什么操作，例如，登录、注销，增删改操作等
- 事件描述：系统管理员进行的系列操作状态，记录操作是成功还是失败，正确或错误
- 时间：系统管理员进行操作的时间

6.2.12 内网短信警告日志

内网短信警告日志记录的是内网短信警告信息记录，如下图所示：

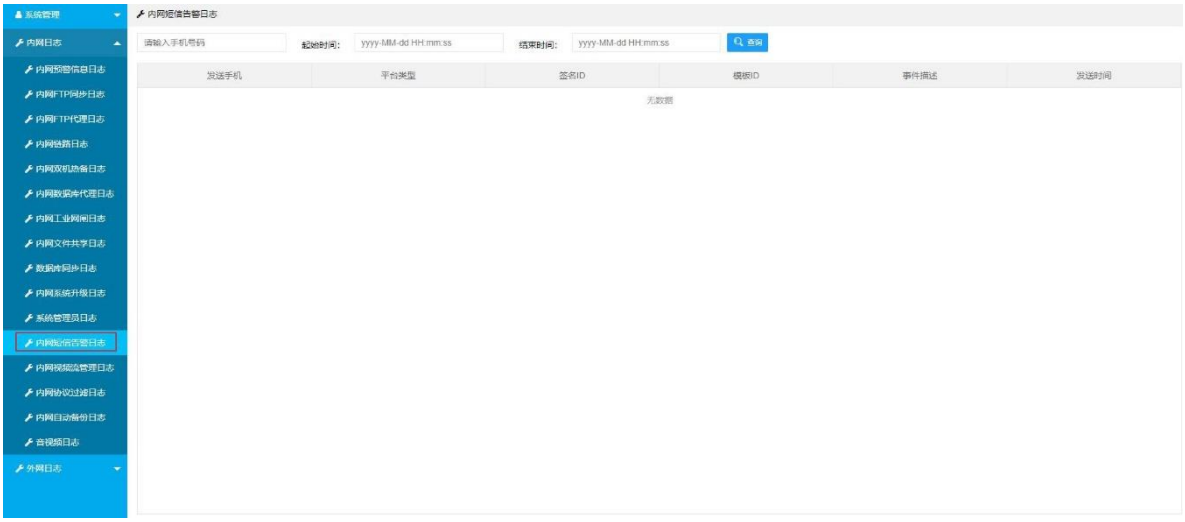


图 6.2.12-1 内网短信警告日志

6.2.13 内网视频流管理日志

内网视频流管理日志记录的是内网视频流管理信息记录，如下图所示：

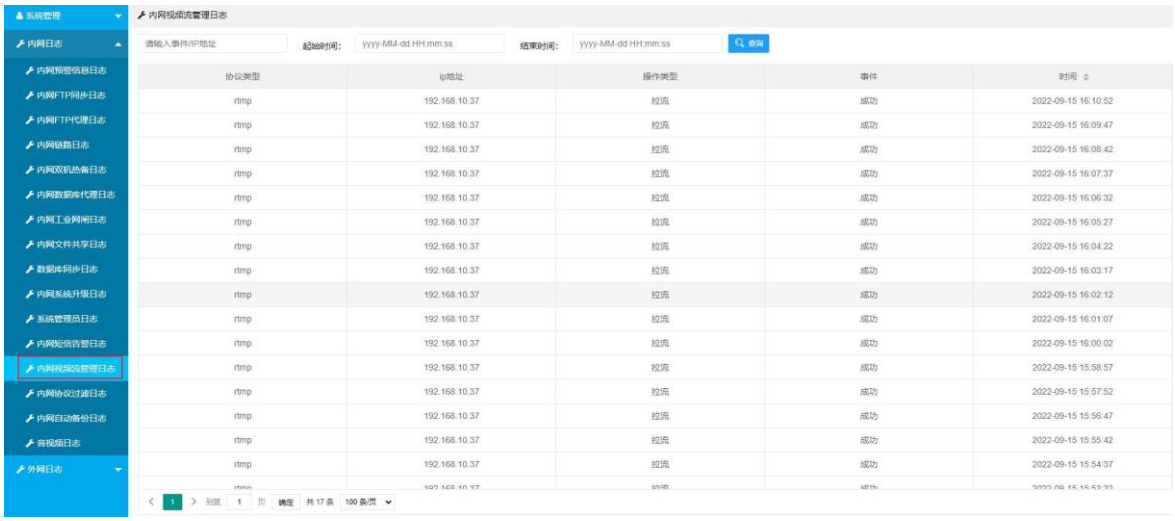


图 6.2.13-1 内网视频流管理日志

6.2.14 内网协议过滤日志

内网协议过滤日志记录的是内网协议过滤信息记录，如下图所示：

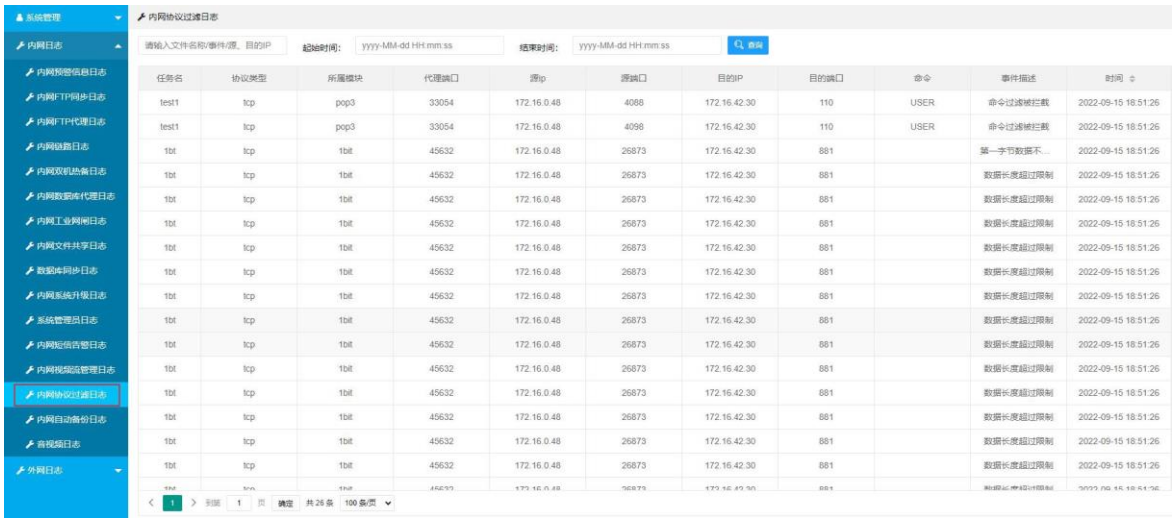


图 6.2.14-1 内网协议过滤日志

6.2.15 内网自动备份日志

内网自动备份日志记录的是内网自动备份信息，如下图所示：

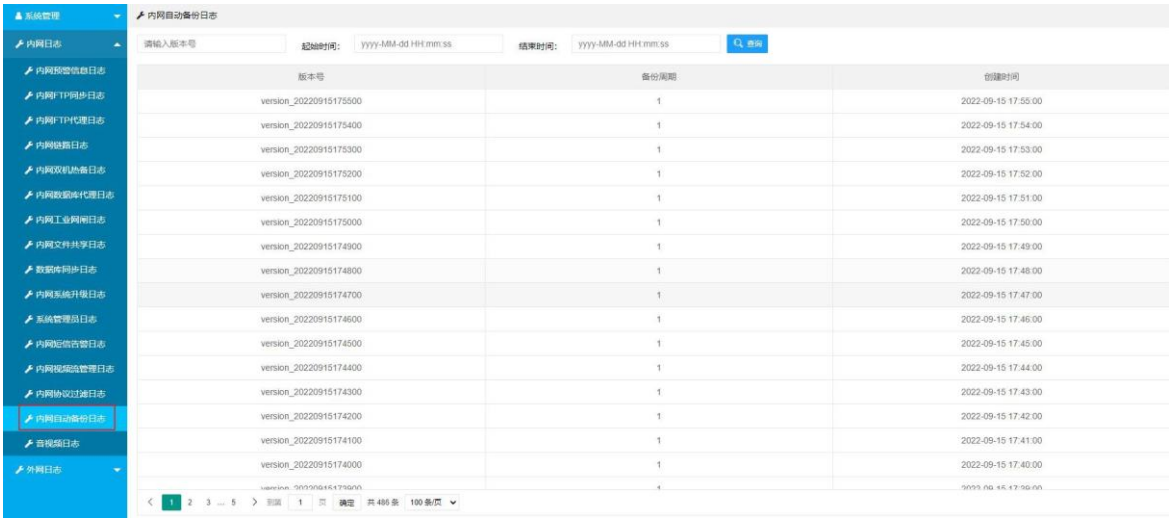


图 6.2.15-1 内网自动备份日志

6.2.16 音视频日志

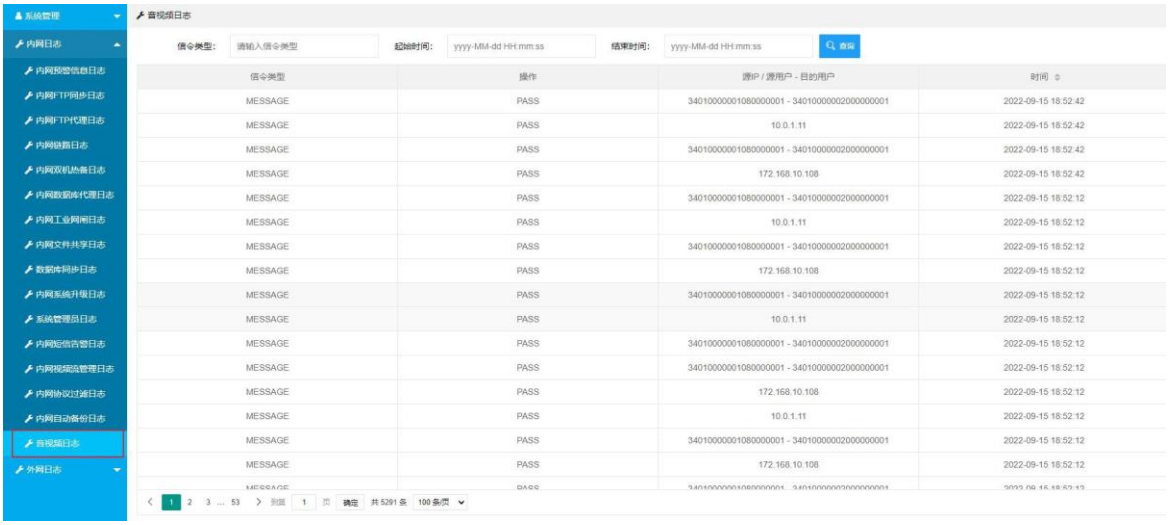


图 6.2.16-1 内网音视频日志

6.3 外网日志

6.3.1 外网预警信息日志

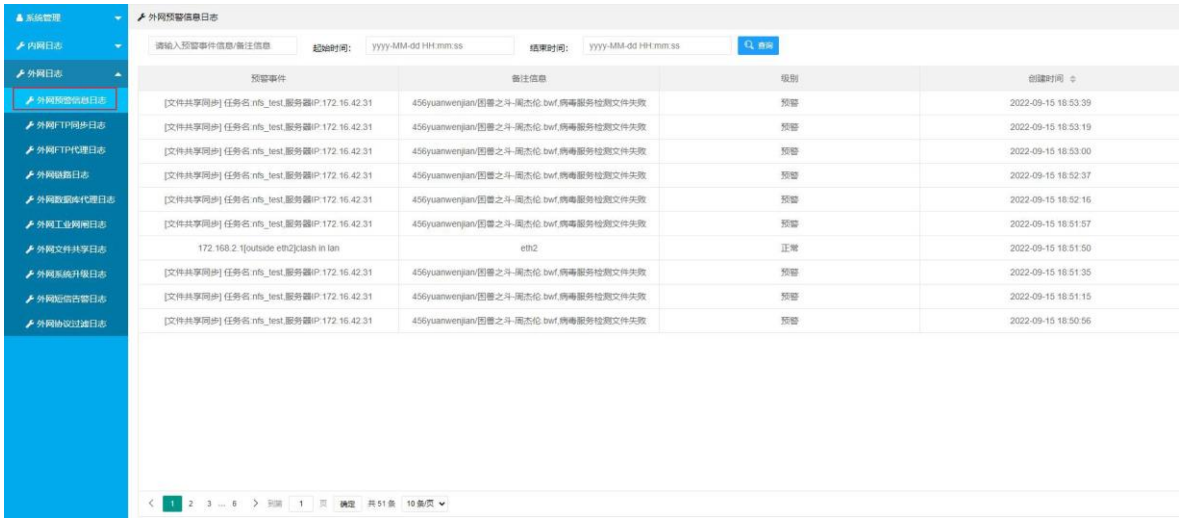


图 6.3.1-1 外网预警信息日志

6.3.2 外网FTP 同步日志

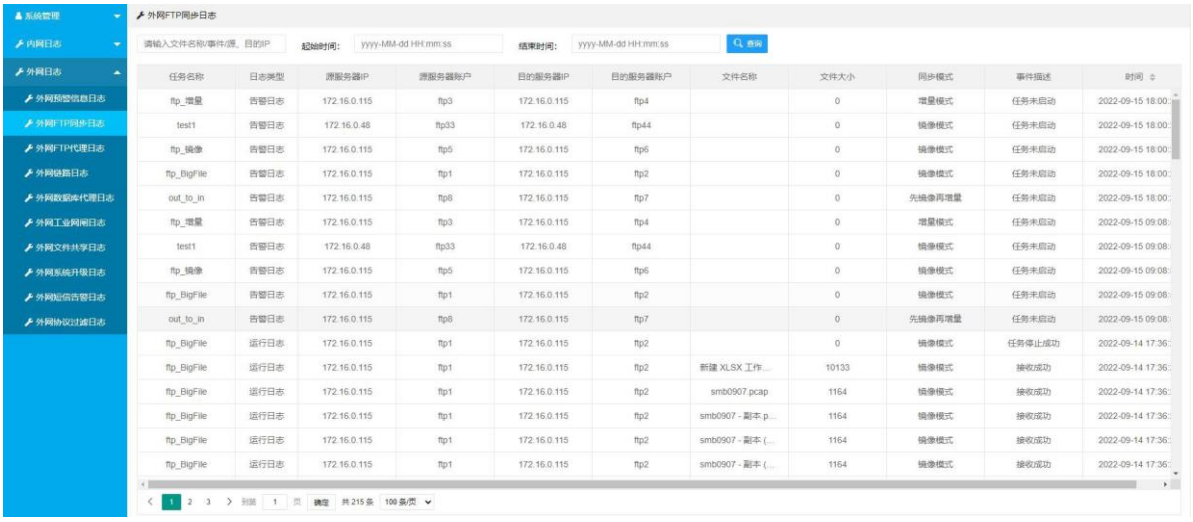


图 6.3.2-1 外网 FTP 同步日志

6.3.3 FTP 代理日志

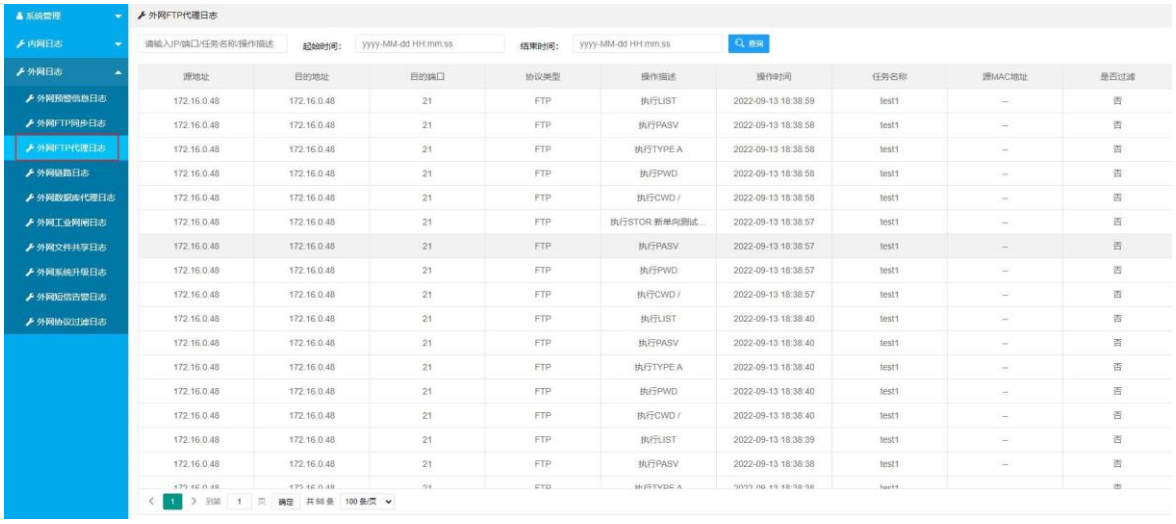


图 6.3.3-1 FTP 代理日志

6.3.4 外网链路日志

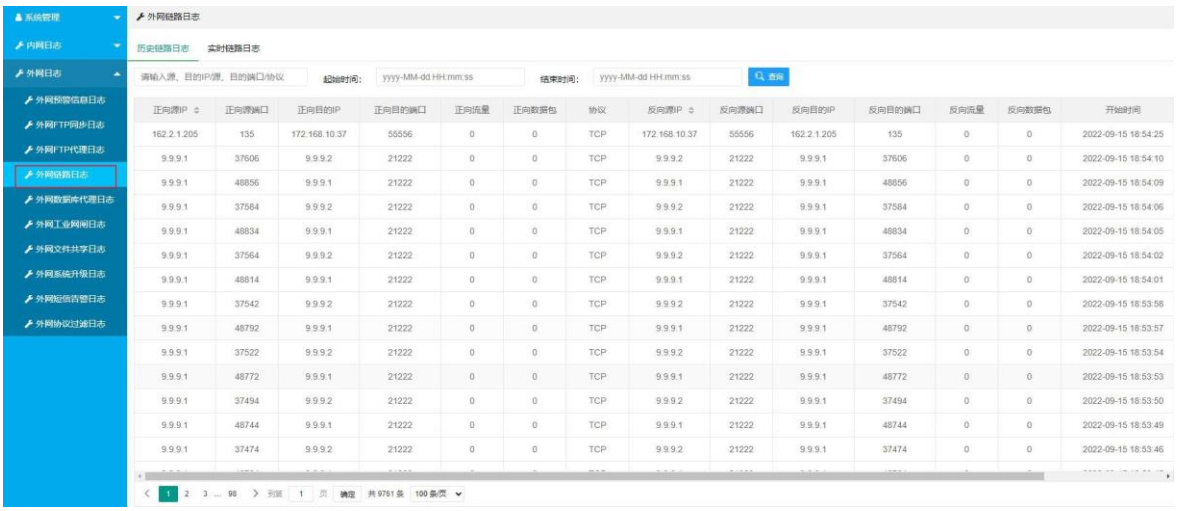


图 6.3.4-1 外网链路日志

6.3.5 数据库代理日志

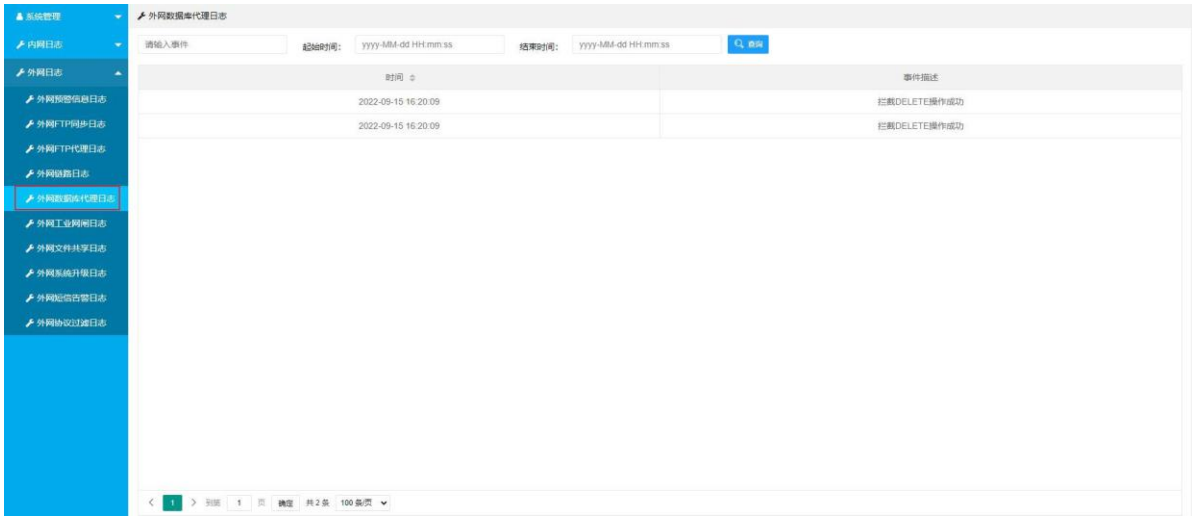


图 6.3.5-1 数据库代理日志

6.3.6 外网工业网闸日志

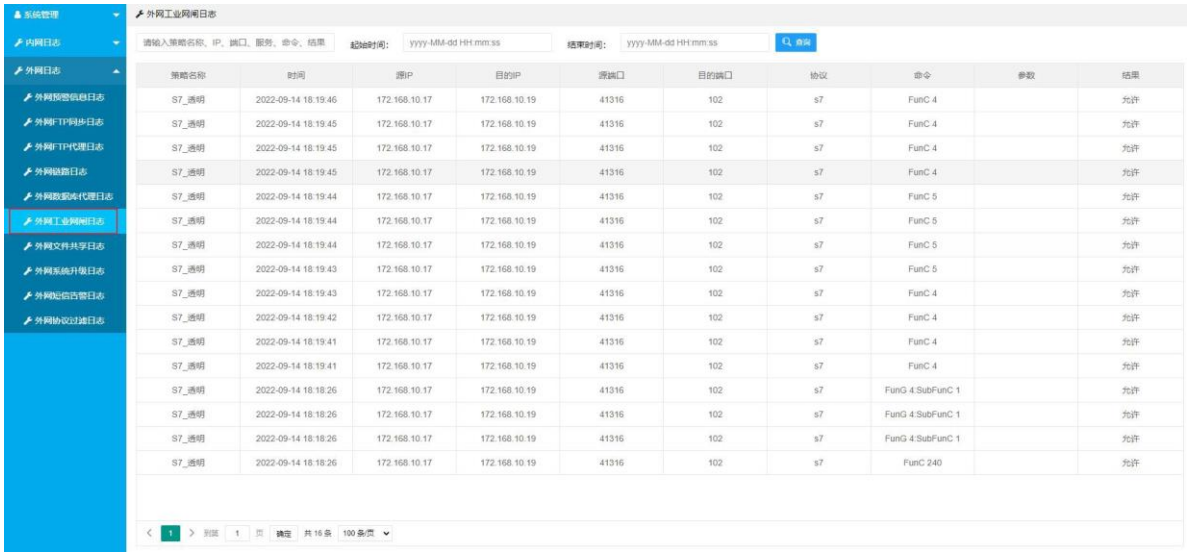


图 6.3.6-1 工业网闸日志

6.3.7 文件共享同步日志

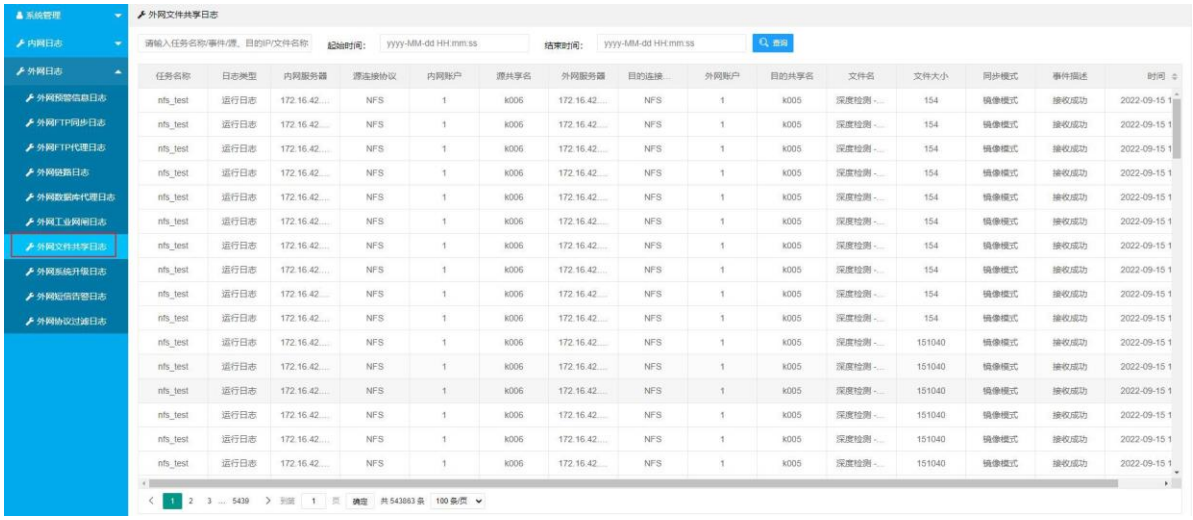


图 6.3.7-1 文件共享同步日志

6.3.8 外网系统升级日志

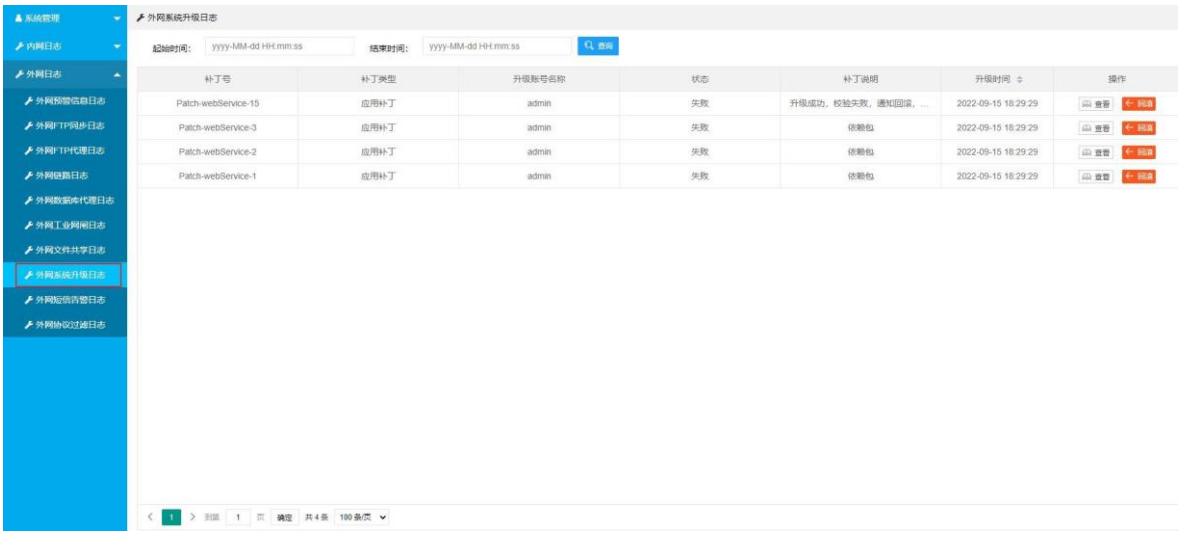


图 6.3.8-1 外网系统升级日志

6.3.9 外网短信告警日志

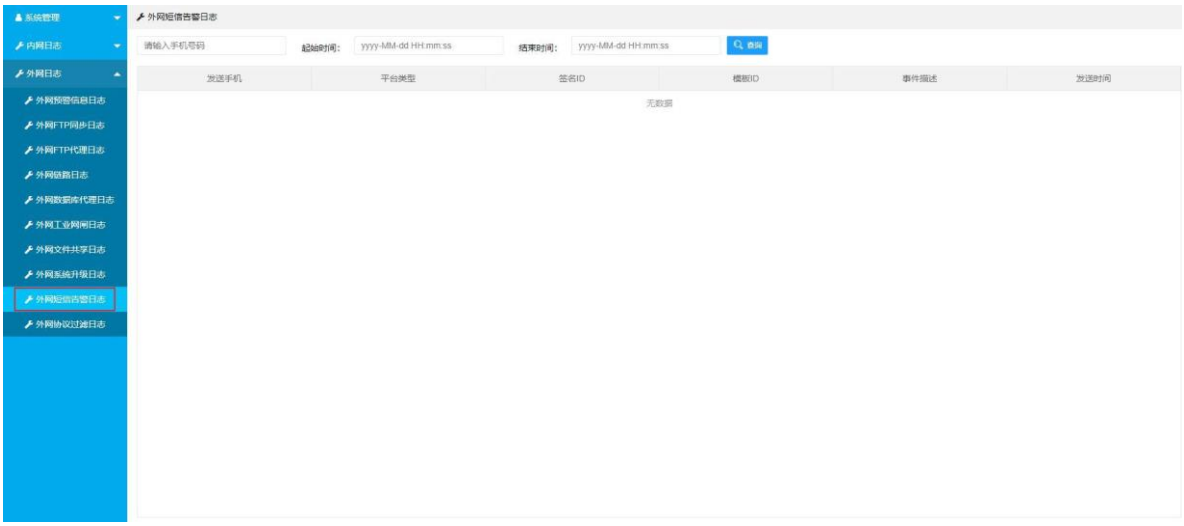


图 6.3.9-1 外网短信告警日志

6.3.10 外网协议过滤日志

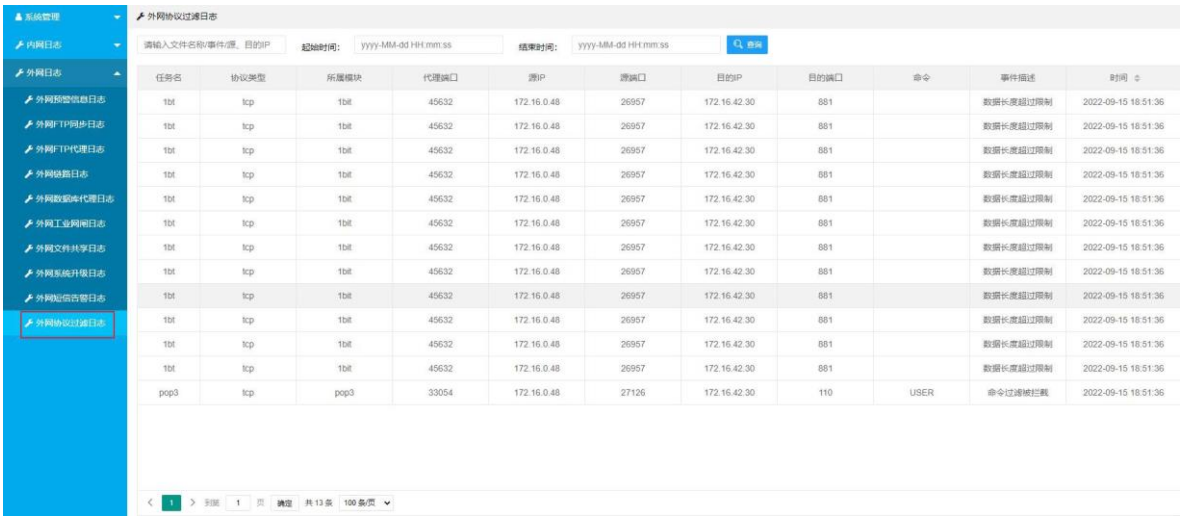


图 6.3.10-1 外网协议过滤日志

7. 客户端用户篇

网闸为用户提供了在两个网络之间安全、迅速的文件交换服务。要使用文件交换功能， 必须安装文件交换客户端软件。

『文件交换』主要包括『发送文件』、『接收文件』、『删除文件』。**用户想要使用文件交换功能，需满足以下几个条件:**

- 应用管理员有在应用管理界面设置该用户信息
- 要交换的文件必须是系统管理员设定的允许交换的类型
- 需交换文件的客户机有安装文件交换客户端软件

7.1 客户端安装

7.1.1 内网客户端下载

选择与网闸在同一局域网内的电脑，按上述配置好电脑 IP→在浏览器（例如 InternetExplore）中输入IP地址https://192.168.1.1/login（默认IP，用户可自行配置，该IP 对应网闸内网 LAN1 口）→按Enter 键出现如下图 6.1.1_1 所示界面：

图 7.1.1-1 内网下载客户端界面

7.1.2 外网客户端下载

选择与网闸在同一局域网内的电脑，按上述配置好电脑 IP→在浏览器（例如 InternetExplore）中输入IP地址https://172.168.1.1/login（默认IP，用户可自行配置，该IP 对应网闸内网 LAN1 口）→按Enter 键出现.如下图所示：

图 7.1.2-1 外网下载客户端界面

▵**Tips:**

内网网闸客户端下载网址：https://192.168.1.1/login（默认LAN1 口IP，用户可自行配置，该IP 对应网闸内网LAN1 口）。

外网网闸客户端下载网址：https://172.168.1.1/login（默认WAN1 口IP，用户可自行配置，该IP 对应网闸内网LAN1 口）。

7.1.3 创建客户端桌面图标

客户端下载成功，解压 fileSwitchClient_pack_2.1.11 安装;打开系解压路径，找到fileSwitchClient.exe，右键发送到桌面，如下图所示：

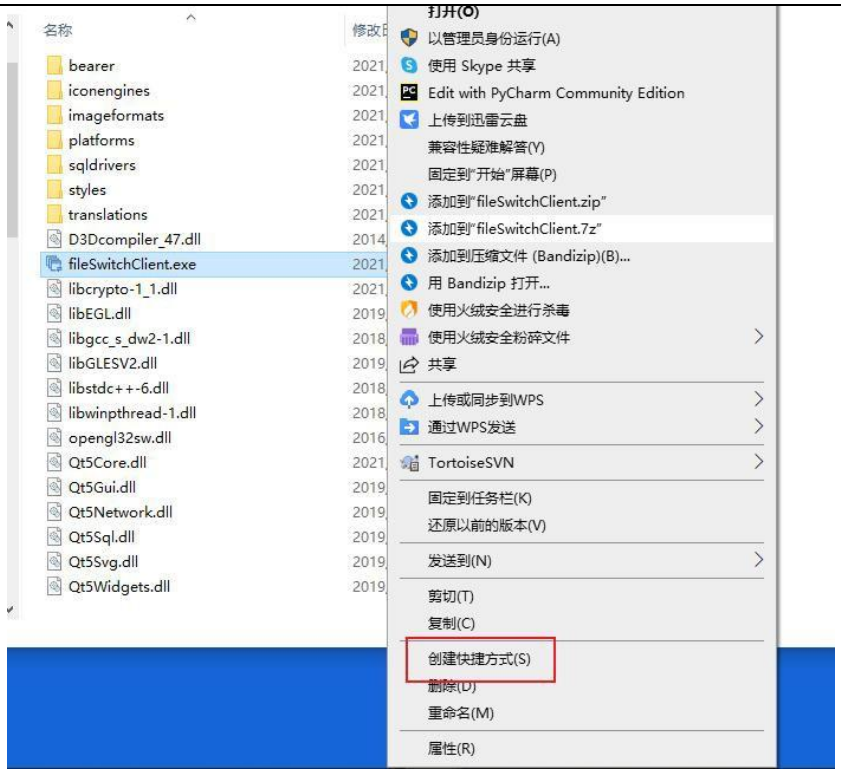


图 7.1.3-1 创建快捷方式

图 7.1.3-2 创建客户端桌面图标

7.2 客户端用户登录

文件交换客户端安装成功及创建桌面图标后→双击“fileSwitchClient”快捷方式，进入到文件交换客户端操作界面，如下图所示：

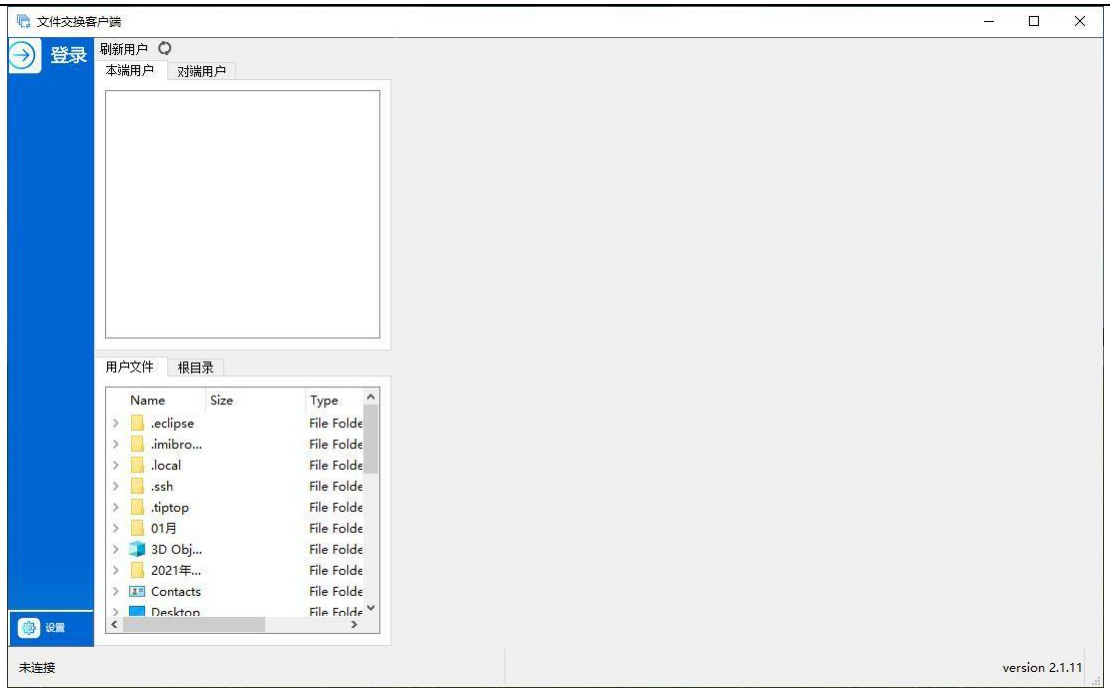


图 7.2-1 文件交换客户端用户界面

文件交换客户端用户界面配置参数说明：

- 用户名：用户登录名称
- 密码：用户登录密码，默认密码a12345678
- 自动登录：勾选此选项，用户连接服务器时无需再进行身份验证，默认勾选，可更改
- 记住密码：勾选此选项，记住用户密码，默认勾选，可更改
- 登录后进入客户端操作界面；如下图所示：

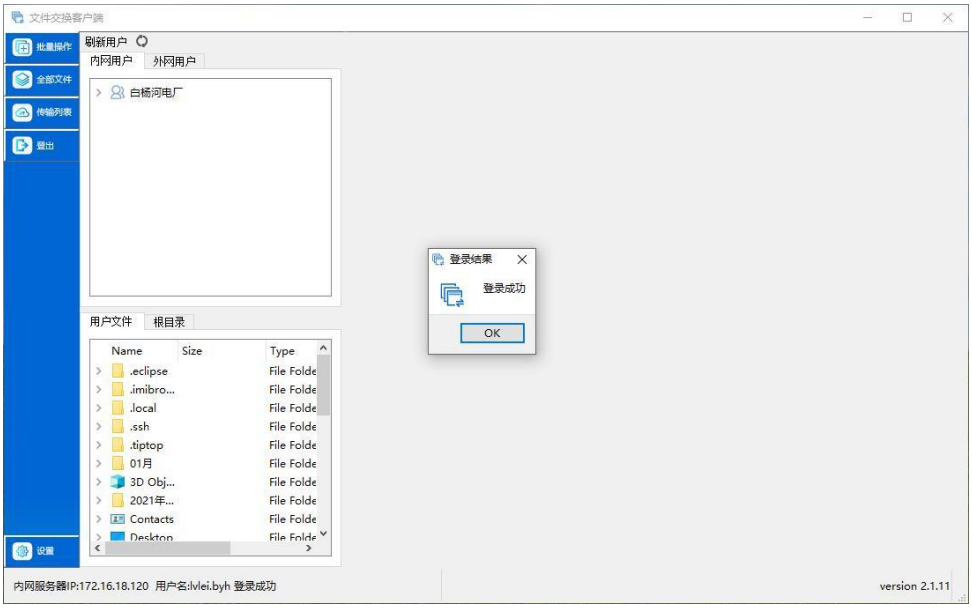


图 7.2.2 文件交换客户端登录成功状态显示

7.3 客户端用户登出

客户端登录后，点击登出按钮，页面弹出提示信息→点击 ok，客户端进入未登录状态，如下图所示。

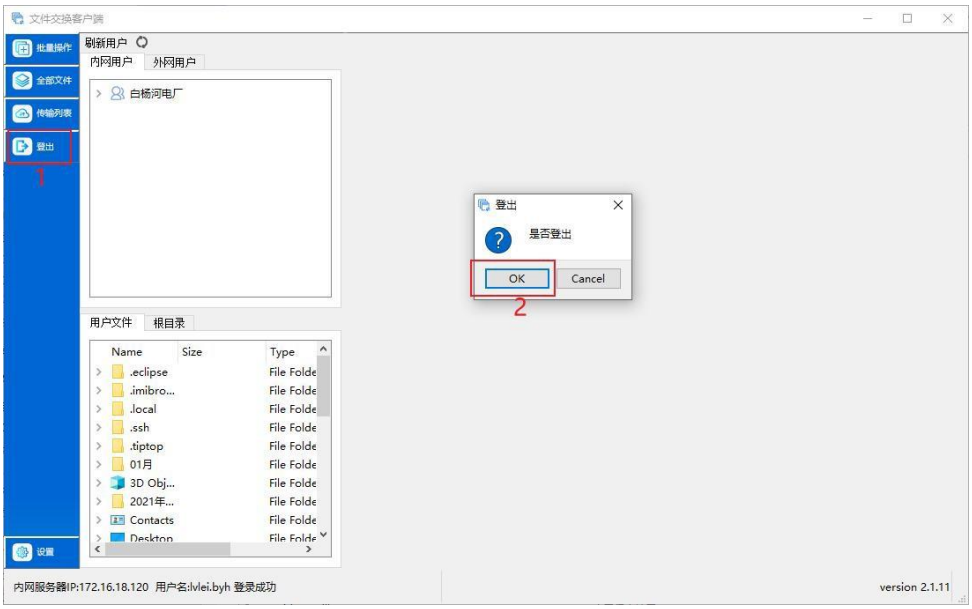
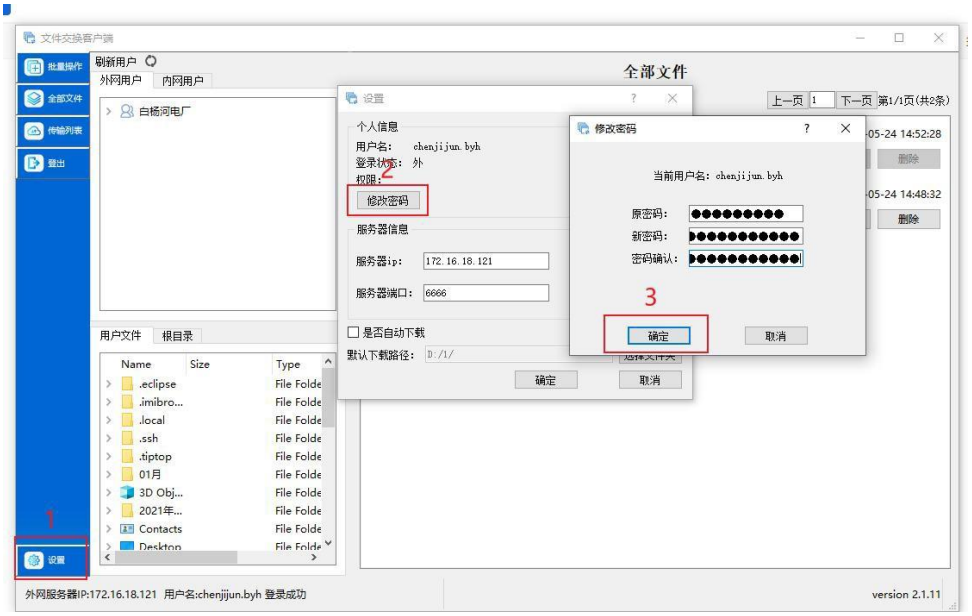


图 7.3-1 客户端用户登出

7.4 客户端用户修改密码

客户端用户密码修改，点击设置，点击修改密码，填入原密码、新密码和确认密码（与新密码一致），点击修改。如下图所示：



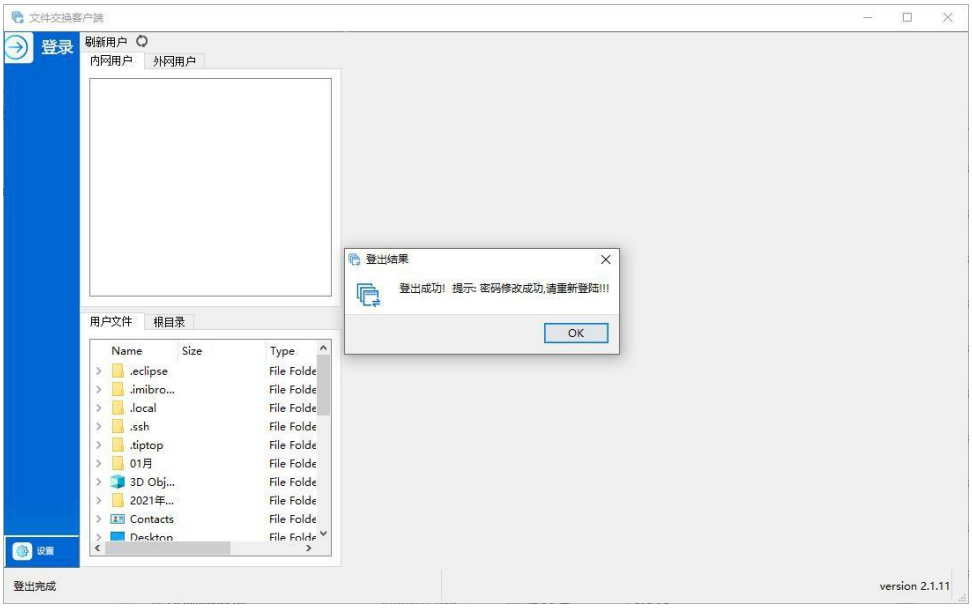


图 7.4-1 修改密码界面

修改密码配置参数说明：

- 原密码：输入原始密码
- 新密码：修改新的密码
- 确认密码：对输入新的密码进行确认

7.5 设置客户端文件接收路径

点击设置→弹出设置窗口，点击选择文件夹→选择好对应文件夹，点击选择文件夹，完成设置客户端文件接收路径设置，如下图所示：

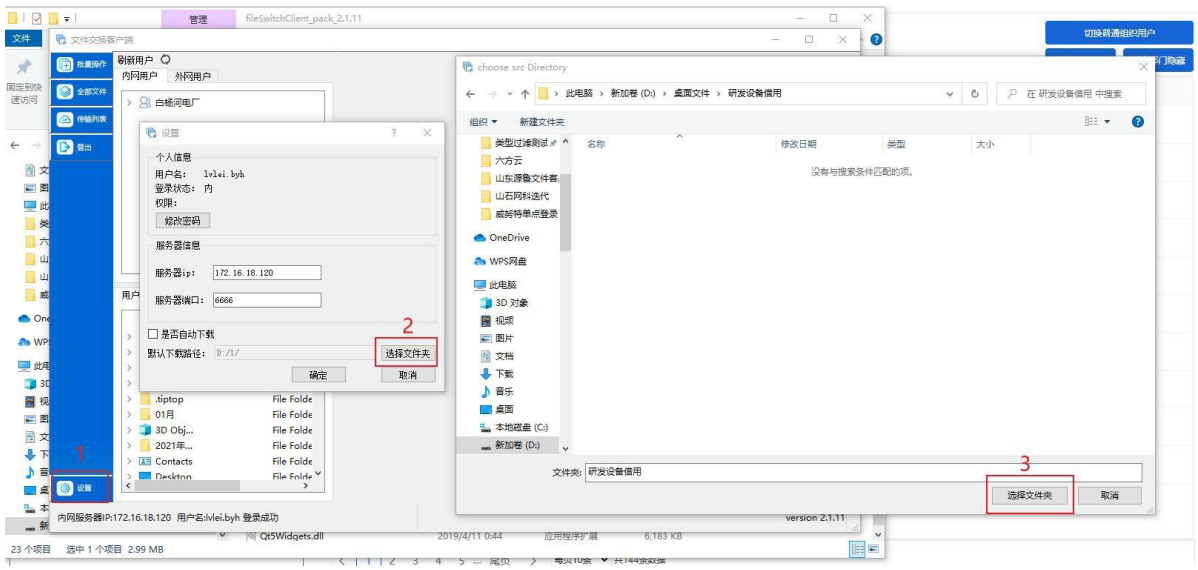


图 7.5-1 文件交换客户端登录配置下载路径

7.6 开启自动下载功能

设置文件自动下载功能，自动下载默认不勾选，如下图所示：

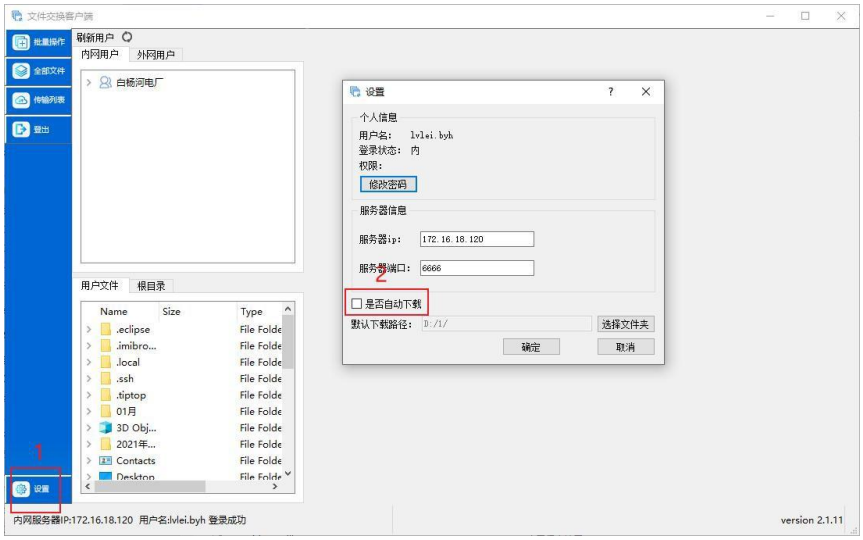


图 7.6-1 客户端开启自动下载

7.7 发送文件

用户成功连接服务器后，选择接收文件的用户，向其发送文件。支持一对一、一对多发送文件。

7.7.1 选择接收用户

用户第一次发送文件前，需要在客户端左侧组织用户栏选择接收文件用户，否则客户端就会提示未检测到默认接收人。

在客户端左侧的组织用户列表→选择[内网用户]或者[外网用户]→选择[部门]→选择对应[用户]，如下图所示：

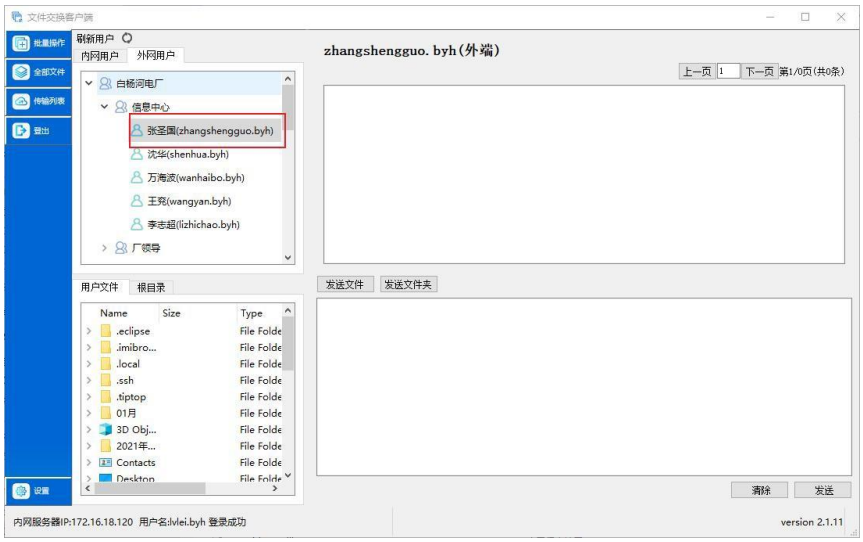


图 7.7.1-1 客户端选择接收用户

7.7.2选择发送文件

用户指定完后选择接收文件、发送文件，如下图所示：

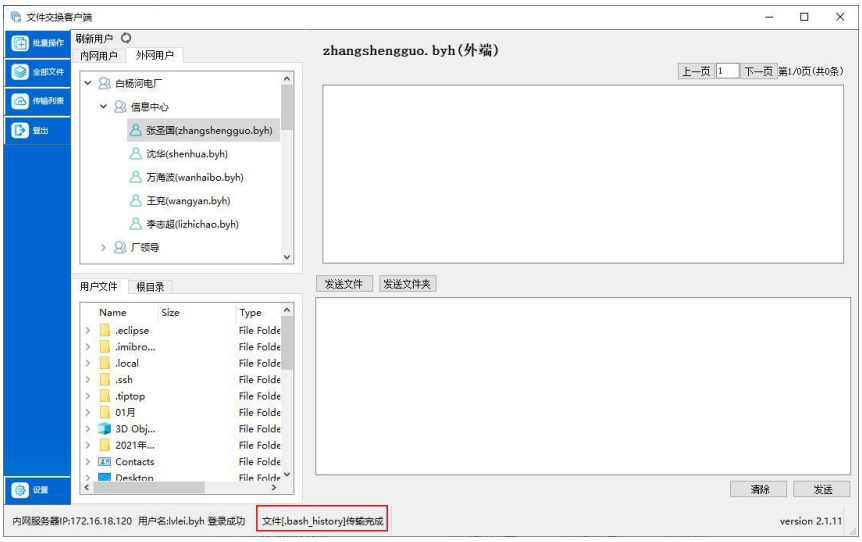


图 7.7.2-1 文件发送

7.7.3 一对一发送文件

选择一个文件接收用户→双击目标用户→点击发送文件→点击发送，如下图所示：

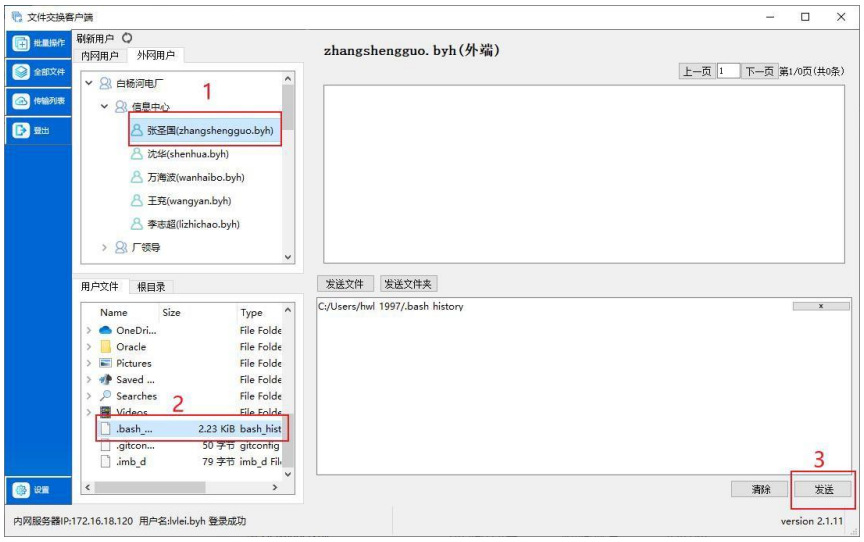


图 7.7.3-1 一对一文件发送

7.7.4 一对多发送文件

如需对多个用户发送相同的文件，可点击批量操作按钮，双击目标用户，将用户加入接收人列表，选中发送文件，点击发送。如下图所示：

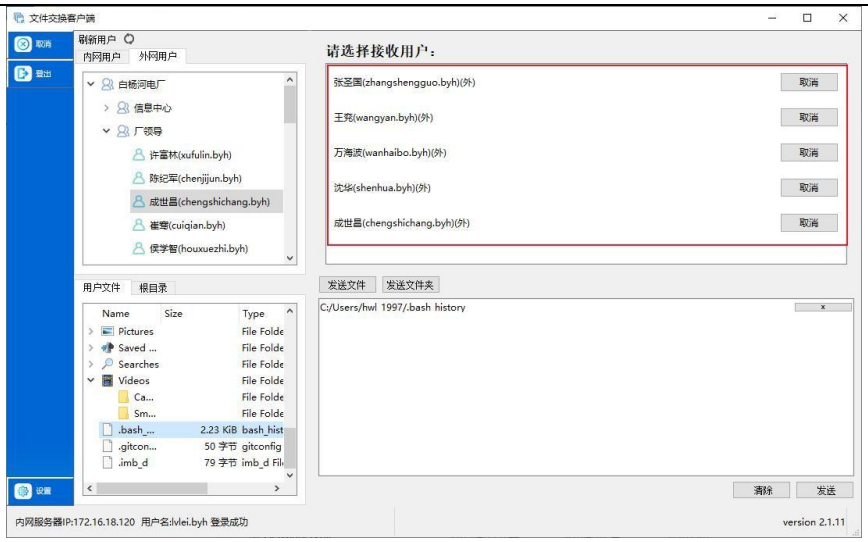


图 7.7.4-1 一对多文件发送

7.7.5 批量文件发送

如需对用户发送批量文件，选中一个或多个文件接收用户，双击多个文件，将文件加入发送文件列表，点击发送，如下图所示：

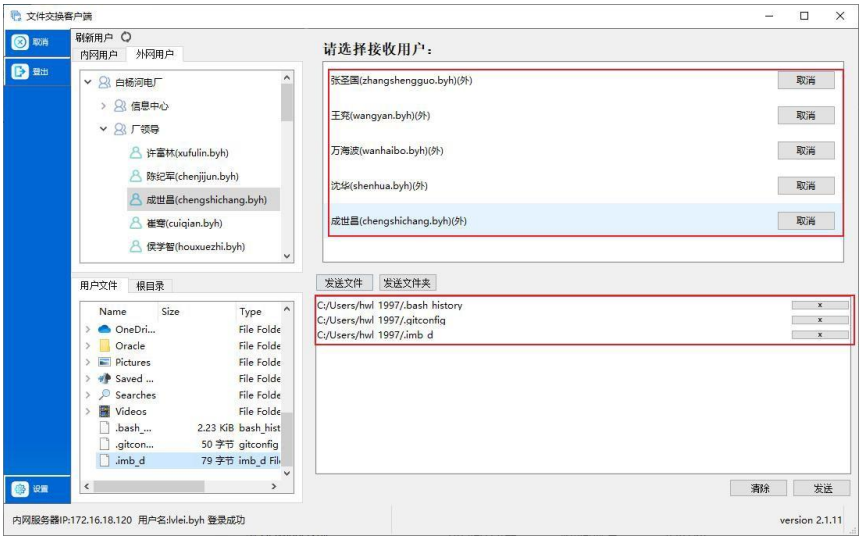


图 7.7.5-1 批量文件发送

7.7.6 文件夹发送

客户端支持以文件目录（文件夹）为单位进行传输，接收对象可为一个或多个用户。

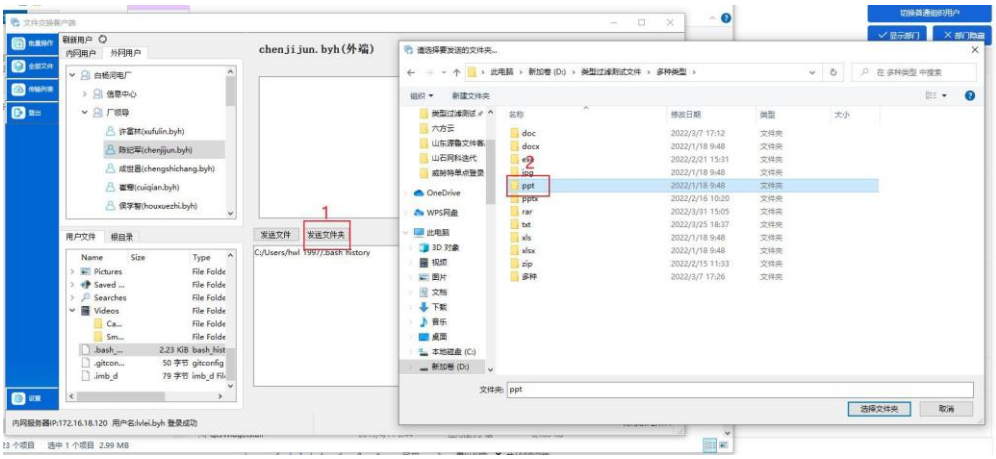


图 7.7.6-1 文件夹发送

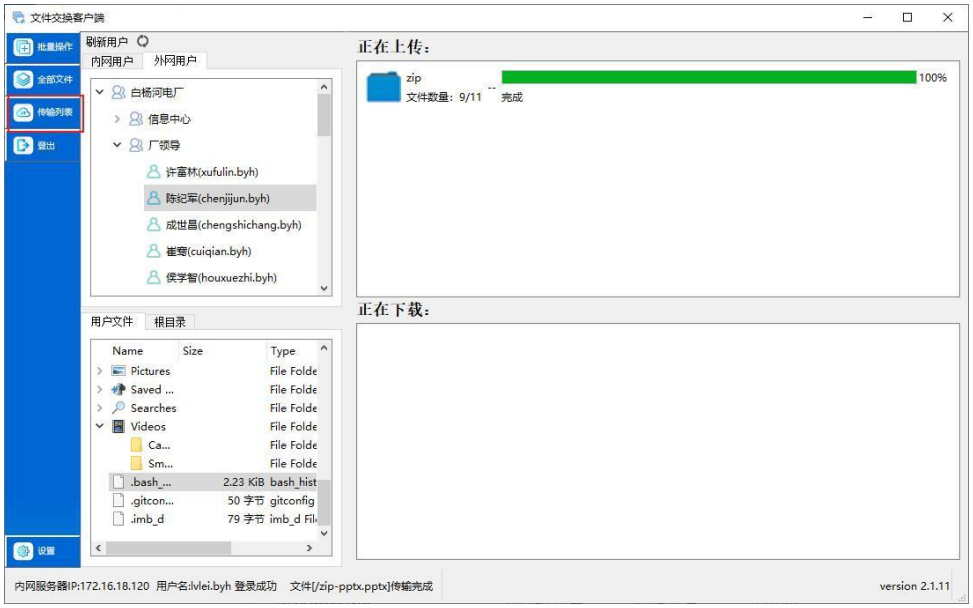


图 7.7.6-2 查看传输列表

7.7.7 拖拽方式文件发送

文件交换系统客户端支持拖拽方式批量或单个文件、文件夹发送，如下图所示：

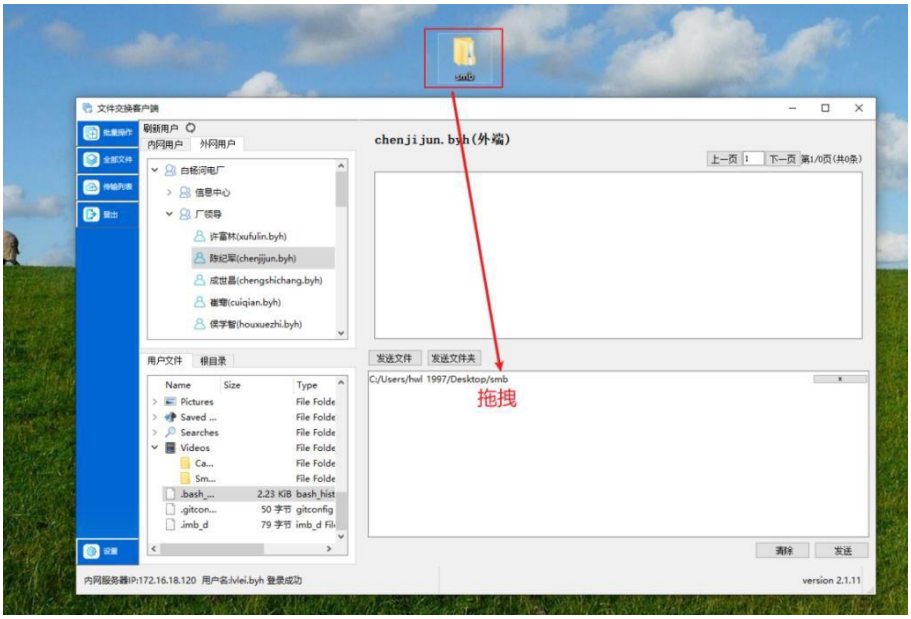


图 7.7.7-1 拖拽方式发送

7.8 接收文件

7.8.1 文件接收

文件交换系统客户端支持文件自动下载和手动下载，并将下载的文件保存到系统设置中配置的路径下，或者可以将其存放在其他路径；如果不需要该文件，可以将其删除。打开全部文件，如下图所示：

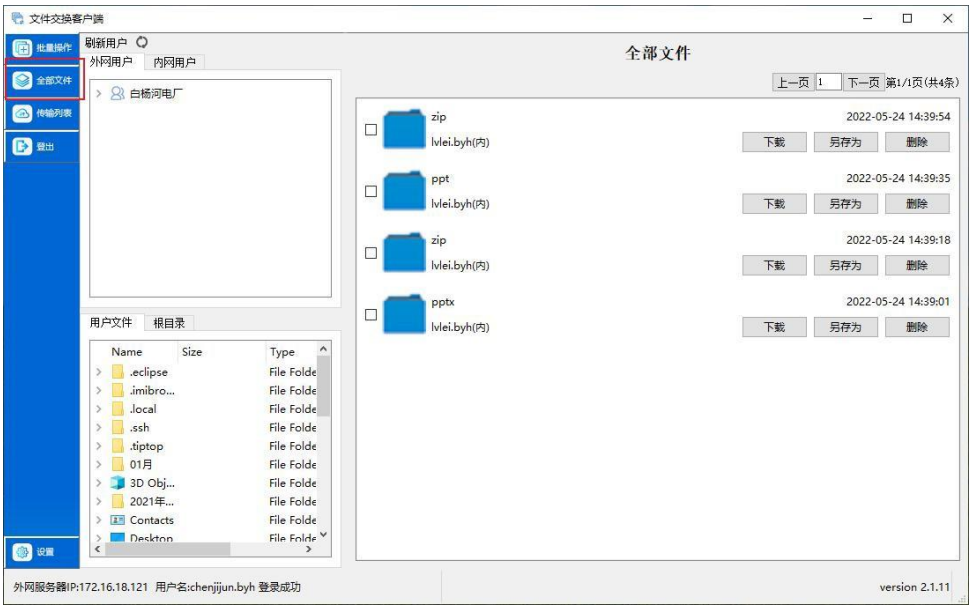


图 7.8.1-1 文件接收

7.8.2 文件/文件夹批量下载、另存为、删除

客户端支持文件或文件夹接收端的批量下载、另存为、删除、取消多选等操作，如图 7.8.2_1 所示勾选文件过文件夹前端的勾选框，对选中目标文件或文件夹进行下载、另存为、删除、取消多选操作：

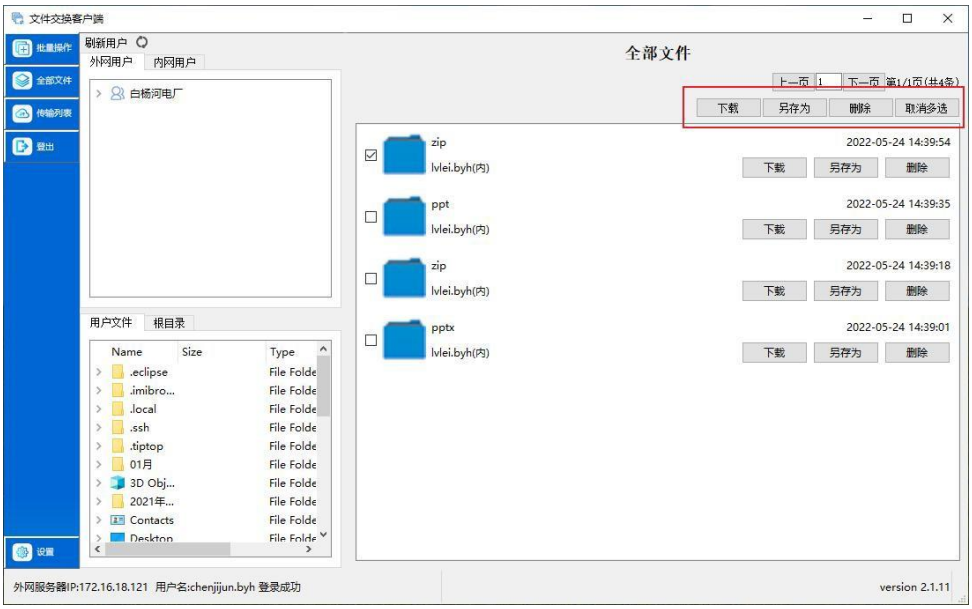


图 7.8.2-1 批量下载、另存为、删除、取消多选

7.9 审核

7.9.1 文件待审核

发送文件如符合文件过滤规则，该文件将会进入待审核状态，该文件在管理员审核之前不可做下载、另存为、删除等操作，且按钮为灰白色不可操作状态，如图 7.9.1_1 和7.9_2 所示：

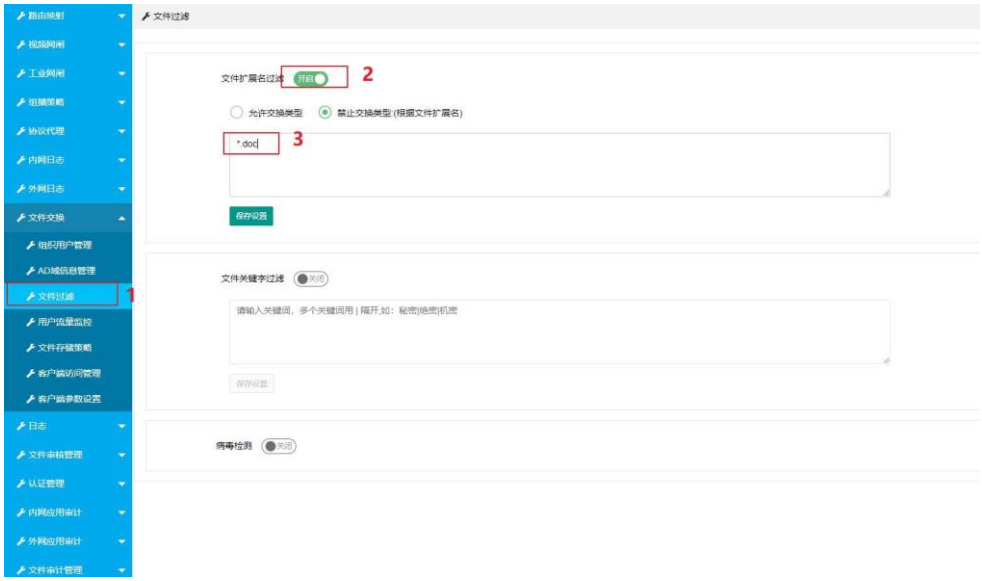
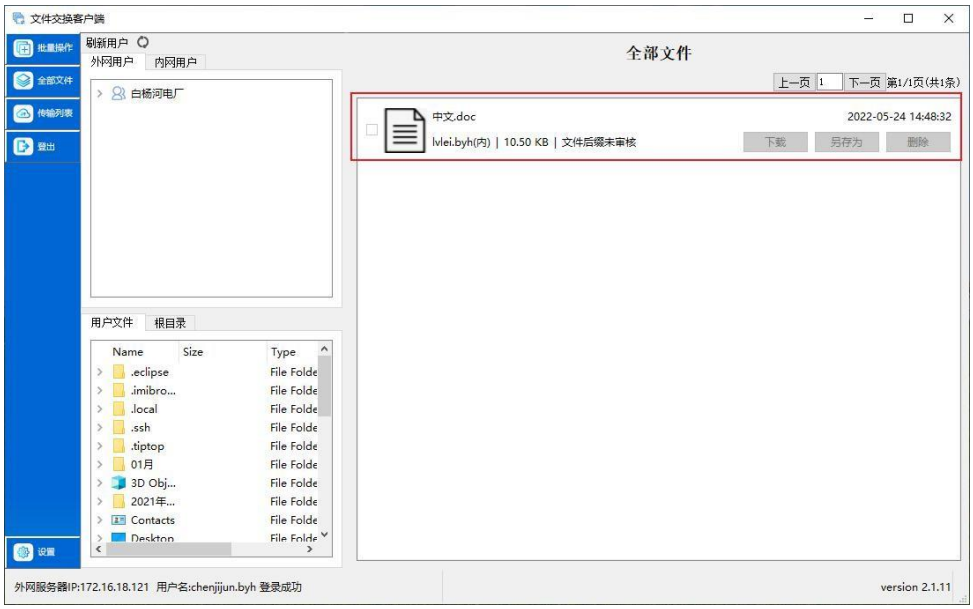


图 7.9.1-1 文件待审核不可操作状态



7.9.2 审核通过

如果文件经管理员审核通过后，文件可做下载、另存为、删除等操作，操作按钮改变为可操作状态，如下图所示：

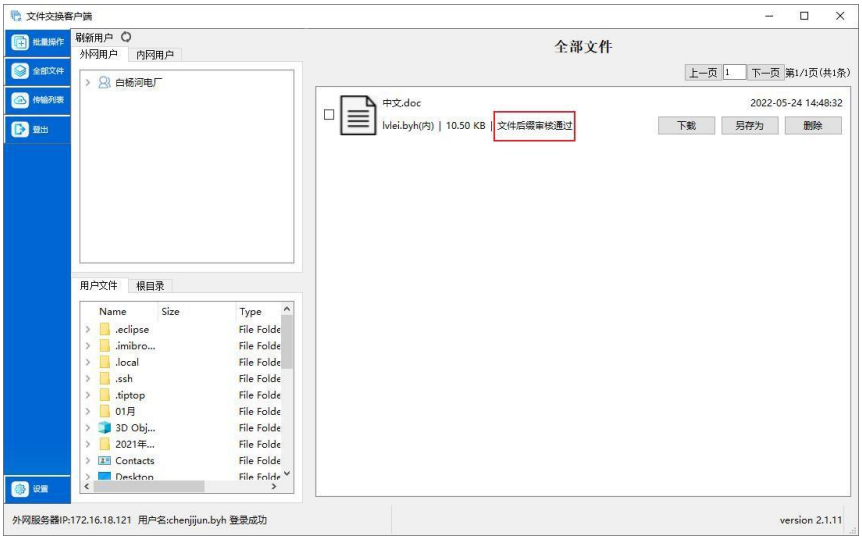


图 7.9.2-1 文件审核通过

7.9.3 文件审核不通过

如果文件经管理员审核不通过，该文件保持为不可接收等操作状态，如下图所示：

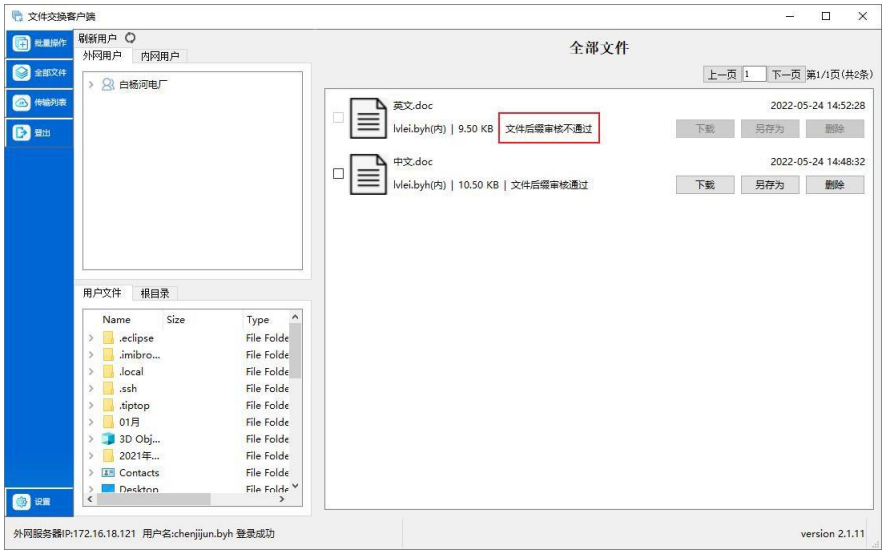


图 7.9.3-1 文件审核不通过

7.10客户端卸载

客户端卸载，只需要删除客户端安装包解压的文件夹即可。

7.11 客户端升级

客户端手动升级，先卸载后再安装，参考 7.10 章节进行客户端卸载，再参考 7.1 章节安装新版本客户端。