Leadsec 网御

网御 SIS 安全隔离与信息交换系统

Web 界面操作手册

声明

- 本手册所含内容若有任何改动，恕不另行通知。
- 在法律法规的最大允许范围内，北京网御星云信息技术有限公司除就本手册和产品应负的瑕疵担保责任外，无论明示或默示，不作其它任何担保，包括（但不限于）本手册中推荐使用产品的适用性和安全性、产品的适销性和适合某特定用途的担保。
- 在法律法规的最大允许范围内，北京网御星云信息技术有限公司对于您的使用或不能使用本产品而发生的任何损坏（包括，但不限于直接或间接的个人损害、商业利润的损失、业务中断、商业信息的遗失或任何其它损失），不负任何赔偿责任。
- 本手册含受版权保护的信息，未经北京网御星云信息技术有限公司书面允许不得对本手册的任何部分进行影印、复制或翻译。

北京网御星云信息技术有限公司
中国北京海淀区中关村南大街 6 号中电信息大厦 8 层

章节目录

章节目录.....III
图目录.....VIII
表目录.....XIII
第 1 章 前言.....1
1.1 导言.....1
1.2 本书适用对象.....1
1.3 本书适合的产品.....1
1.4 手册章节组织.....1
1.5 相关参考手册.....2
第 2 章 如何开始.....3
2.1 网御 SIS 安全隔离网闸概述.....3
2.1.1 产品特点.....3
2.1.2 主要功能.....4
2.1.3 软件描述.....4
2.2 配置管理方法.....9
2.2.1 网络接口 Web 配置.....10
2.2.2 网络接口 CLI 配置.....10
2.2.3 本地串口 CLI 配置.....10
2.3 登录管理界面.....10
2.3.1 登录方法.....10
2.3.2 管理认证.....11
2.3.3 登录过程.....11
2.3.4 网御 SIS 安全隔离网闸的一般配置过程.....12
2.3.5 退出登录.....13
第 3 章 系统配置.....14
3.1 日期时间.....14
3.2 系统参数.....15
3.3 系统更新.....15
3.3.1 模块升级.....15
3.3.2 导入导出.....16
3.4 管理配置.....17
3.4.1 管理主机.....17
3.4.2 管理员帐号.....18
3.4.3 管理员证书.....19
3.4.4 管理方式.....21
3.5 报告设置.....21
3.5.1 日志服务器.....21
3.5.2 集中管理.....22
3.6 产品许可证.....24
第 4 章 网络配置.....25
4.1 网络设备.....25

4.1.1 物理设备.....25
4.1.2 别名设备.....27
4.1.3 冗余设备.....28
4.2 域名服务器.....30
4.3 静态路由.....31
4.4 高可靠性设置.....32
4.4.1 基本配置.....33
4.4.2 IP 探测.....34
4.4.3 虚拟地址.....35
4.4.4 负载均衡.....37
4.5 地址绑定.....39
第 5 章 资源定义.....44
5.1 地址.....44
5.1.1 地址列表.....44
5.1.2 地址组.....45
5.1.3 域名地址.....46
5.2 用户.....48
5.2.1 用户列表.....49
5.2.2 用户组.....50
5.3 时间.....52
5.3.1 时间列表.....52
5.3.2 时间组.....54
第 6 章 病毒防护.....55
6.1 引擎管理.....55
6.2 病毒库升级.....56
第 7 章 文件交换.....58
7.1 基本配置.....58
7.1.1 工作模式.....58
7.1.2 服务管理.....59
7.2 任务管理.....59
7.2.1 发送任务.....59
7.2.2 接收任务.....63
7.3 内容控制.....65
7.3.1 文件名控制.....65
7.3.2 内容黑名单.....68
7.3.3 内容白名单.....70
7.3.4 文件属性控制.....72
7.4 文件交换任务.....75
第 8 章 文件交换.....76
8.1 基本配置.....76
8.1.1 证书设置.....76
8.1.2 服务管理.....77
8.2 客户端.....77
8.3 服务端.....81

8.4 内容控制.....83
8.4.1 文件名控制.....83
8.4.2 内容黑名单.....86
8.4.3 内容白名单.....88
第 9 章 数据库同步.....91
9.1 基本配置.....91
9.1.1 证书设置.....91
9.1.2 服务管理.....92
9.2 客户端.....92
9.3 服务端.....96
第 10 章 安全浏览.....99
10.1 基本配置.....99
10.2 过滤选项.....100
10.2.1 URL 过滤.....100
10.2.2 MIME 类型过滤.....102
10.2.3 文件扩展名过滤.....104
10.2.4 过滤选项集.....106
10.3 客户端.....111
10.3.1 透明访问.....112
10.3.2 普通访问.....114
10.4 服务端.....117
10.4.1 普通访问.....117
第 11 章 FTP 访问.....121
11.1 基本配置.....121
11.2 过滤选项.....122
11.3 客户端.....127
11.3.1 透明访问.....127
11.3.2 普通访问.....130
11.4 服务端.....133
11.4.1 普通访问.....133
第 12 章 邮件访问.....137
12.1 过滤选项.....137
12.1.1 邮件地址.....137
12.1.2 内容关键字.....139
12.1.3 附件扩展名.....142
12.1.4 过滤选项集.....144
12.2 SMTP.....148
12.2.1 基本配置.....148
12.2.2 客户端.....149
12.2.3 服务端.....155
12.3 POP3.....158
12.3.1 基本配置.....158
12.3.2 客户端.....159
12.3.3 服务端.....165

第 13 章 数据库访问.....169
13.1 基本配置.....169
13.2 过滤选项.....170
13.2.1 用户过滤.....170
13.2.2 SQL 语句过滤.....172
13.2.3 过滤选项集.....174
13.3 客户端.....176
13.3.1 透明访问.....176
13.3.2 普通访问.....180
13.4 服务端.....183
第 14 章 定制访问.....187
14.1 定制 TCP.....187
14.1.1 基本配置.....187
14.1.2 客户端.....188
14.1.3 服务端.....194
14.2 定制 UDP.....197
14.2.1 基本配置.....197
14.2.2 客户端.....198
14.2.3 服务端.....204
第 15 章 安全通道.....208
15.1 基本配置.....208
15.2 客户端.....209
15.3 服务端.....213
第 16 章 消息传输.....216
16.1 基本配置.....216
16.1.1 证书设置.....217
16.1.2 服务管理.....218
16.2 客户端.....218
16.3 服务端.....221
16.4 内容控制.....224
16.4.1 文件名控制.....224
16.4.2 内容黑名单.....226
16.4.3 内容白名单.....229
16.5 用户管理.....231
16.5.1 用户认证.....231
16.5.2 用户权限.....233
第 17 章 抗攻击设置.....236
17.1 入侵检测.....236
17.1.1 基本配置.....236
17.1.2 策略配置.....237
17.1.3 自定义检测.....237
17.1.4 扫描检测配置.....238
17.1.5 自动响应配置.....239
17.1.6 检测结果.....239

17.2 抗 DDos 攻击.....240
第 18 章 系统监控.....242
18.1 网络设备.....242
18.2 资源状态.....243
18.3 日志信息.....245
18.4 用户信息.....245
18.5 网络调试工具.....246
18.6 批处理工具.....247
第 19 章 在线支持.....251
19.1 在线注册.....251
19.2 技术支持.....251
19.3 关于.....251
第 20 章 公共操作说明.....253
20.1 字符合法性说明.....253
20.2 通用操作说明.....253
20.2.1 分页显示.....254
20.2.2 查找.....254
20.2.3 排序.....255
第 21 章 附录.....256
21.1 常见问题说明.....256

图目录

图 2 1 SIS 安全隔离网闸工作原理 3
图 2 2 SIS 安全隔离网闸配置首页 4
图 2 3 使用 SecureCRT 3.4.3 登录 SIS 安全隔离网闸 11
图 2 4 SIS 安全隔离网闸登录界面 12
图 3 1 配置 SIS 安全隔离网闸时间 14
图 3 2 系统参数配置图 15
图 3 3 导入升级文件 15
图 3 4 导入导出配置文件 16
图 4 1 物理设备列表 26
图 4 2 物理设备可配置的属性 27
图 4 3 别名设备列表 28
图 4 4 别名设备可配置的属性 28
图 4 5 冗余设备列表 29
图 4 6 冗余设备属性配置 30
图 4 7 域名服务器配置 30
图 4 8 静态路由的显示 31
图 4 9 静态路由的维护 32
图 4 10 高可靠性配置 WEB 界面导航菜单 33
图 4 11 基本配置界面 33
图 4 12 IP 探测列表显示 34
图 4 13 添加 IP 探测地址 34
图 4 14 编辑探测 IP 地址 35
图 4 15 删除探测 IP 地址 35
图 4 16 虚拟地址列表显示 35
图 4 17 添加虚拟地址 36
图 4 18 编辑虚拟地址 36
图 4 19 删除虚拟地址 37
图 4 20 负载均衡配置列表显示 37
图 4 21 添加负载均衡配置 38
图 4 22 编辑负载均衡配置 39
图 4 23 删除负载均衡配置 39
图 4 24 地址绑定配置 40
图 4 25 IP/MAC 地址探测 40
图 4 26 探测到的 IP/MAC 对显示 41
图 4 27 绑定 IP/MAC 对配置 42
图 4 28 添加地址绑定 43
图 4 29 删除 IP/MAC 地址对 43
图 5 1 地址列表 44
图 5 2 地址列表维护 45
图 5 3 地址组列表 45
图 5 4 地址组添加 46

图 6 1 病毒防护 WEB 界面导航菜单.....55
图 6 2 引擎管理配置界面.....55
图 7 1 文件交换 WEB 界面导航菜单.....58
图 7 2 基本配置界面.....58
图 8 1 文件交换 WEB 界面导航菜单.....76
图 8 2 基本配置界面.....76
图 8 3 客户端任务列表显示.....78
图 8 4 添加客户端任务.....78
图 8 5 编辑客户端任务.....80
图 8 6 删除客户端任务.....80
图 8 7 服务端任务列表显示.....81
图 8 8 添加服务端任务.....81
图 8 9 编辑服务端任务.....83
图 8 10 删除服务端任务.....83
图 8 11 文件名控制列表显示.....83
图 8 12 启用文件名控制.....84
图 8 13 启用文件名控制.....84
图 8 14 添加文件名.....85
图 8 15 编辑文件名.....85
图 8 16 删除文件名.....85
图 8 17 内容黑名单列表显示.....86
图 8 18 启用黑名单控制.....86
图 8 19 添加禁止的内容.....87
图 8 20 编辑禁止的内容.....87
图 8 21 删除禁止的内容.....88
图 8 22 内容白名单列表显示.....88
图 8 23 启用白名单控制.....88
图 8 24 添加允许的内容.....89
图 8 25 编辑允许的内容.....90
图 8 26 删除禁止的内容.....90
图 9 1 数据库同步 WEB 界面导航菜单.....91
图 9 2 基本配置界面.....91
图 9 3 客户端任务列表显示.....93
图 9 4 添加客户端任务.....93
图 9 5 编辑客户端任务.....95
图 9 6 删除客户端任务.....95
图 9 7 服务端任务列表显示.....96
图 9 8 添加服务端任务.....96
图 9 9 编辑服务端任务.....97
图 9 10 删除服务端任务.....98
图 10 1 安全浏览 WEB 界面导航菜单.....99
图 10 2 基本配置界面.....99
图 11 1 FTP 访问 WEB 界面导航菜单.....121
图 11 2 基本配置界面.....121

图 11 13 透明访问列表显示.....127
图 11 14 添加透明访问.....128
图 11 15 编辑透明访问.....129
图 11 16 删除透明访问.....130
图 11 17 普通访问列表显示.....130
图 11 18 添加普通访问.....131
图 11 19 编辑普通访问.....132
图 11 20 删除普通访问.....133
图 11 21 FTP 服务端导航菜单.....133
图 11 22 FTP 服务端普通任务列表显示.....134
图 11 23 添加 FTP 服务端普通任务.....134
图 11 24 编辑 FTP 服务端普通任务.....135
图 11 25 删除 FTP 服务端普通任务.....135
图 12 1 8 SMTP WEB 界面功能菜单.....148
图 13 1 数据库访问基本配置界面.....169
图 14 1 定制 TCP WEB 界面功能菜单.....187
图 14 2 定制 TCP 基本配置界面.....187
图 14 3 定制 TCP 客户端透明任务列表显示.....188
图 14 4 添加定制 TCP 客户端透明任务.....189
图 14 5 编辑定制 TCP 客户端透明任务.....190
图 14 6 删除定制 TCP 客户端透明任务.....191
图 14 7 定制 TCP 客户端普通任务列表显示.....191
图 14 8 添加定制 TCP 客户端透明任务.....192
图 14 9 编辑定制 TCP 客户端普通任务.....193
图 14 10 删除定制 TCP 客户端普通任务.....194
图 14 11 定制 TCP 服务端导航菜单.....194
图 14 12 定制 TCP 服务端普通任务列表显示.....195
图 14 13 添加定制 TCP 服务端普通任务.....195
图 14 14 编辑定制 TCP 服务端普通任务.....196
图 14 15 删除定制 TCP 服务端普通任务.....196
图 14 16 定制 UDP WEB 界面功能菜单.....197
图 14 17 定制 UDP 基本配置界面.....197
图 14 18 定制 UDP 客户端透明任务列表显示.....198
图 14 19 添加定制 UDP 客户端透明任务.....199
图 14 20 编辑定制 UDP 客户端透明任务.....200
图 14 21 删除定制 UDP 客户端透明任务.....201
图 14 22 定制 UDP 客户端普通任务列表显示.....201
图 14 23 添加定制 UDP 客户端普通任务.....202
图 14 24 编辑定制 UDP 客户端普通任务.....203
图 14 25 删除定制 UDP 客户端普通任务.....204
图 14 26 定制 UDP 服务端导航菜单.....204
图 14 27 定制 UDP 服务端普通任务列表显示.....205
图 14 28 添加定制 UDP 服务端普通任务.....205
图 14 29 编辑定制 UDP 服务端普通任务.....206

图 14 30 删除定制 UDP 服务端普通任务.....206
图 15 1 安全通道基本配置界面.....208
图 15 2 列表显示安全通道客户端端任务.....209
图 15 3 添加安全通道客户端任务.....210
图 15 4 修改安全通道客户端任务.....212
图 15 5 删除安全通道客户端端任务.....212
图 16 1 消息传输 WEB 界面导航菜单.....216
图 16 2 基本配置界面.....217
图 16 3 客户端任务列表显示.....218
图 16 4 添加客户端任务.....219
图 16 5 编辑客户端任务.....221
图 16 6 删除客户端任务.....221
图 16 7 服务端任务列表显示.....222
图 16 8 添加服务端任务.....222
图 16 9 编辑服务端任务.....223
图 16 10 删除服务端任务.....224
图 16 11 文件名控制列表显示.....224
图 16 12 启用文件名控制.....225
图 16 13 启用文件名控制.....225
图 16 14 添加文件名.....226
图 16 15 编辑文件名.....226
图 16 16 删除文件名.....226
图 16 17 内容黑名单列表显示.....227
图 16 18 启用黑名单控制.....227
图 16 19 添加禁止的内容.....228
图 16 20 编辑禁止的内容.....228
图 16 21 删除禁止的内容.....229
图 16 22 内容白名单列表显示.....229
图 16 23 启用白名单控制.....229
图 16 24 添加允许的内容.....230
图 16 25 编辑允许的内容.....230
图 16 26 删除禁止的内容.....231
图 16 27 用户认证管理列表显示.....232
图 16 28 添加认证用户.....232
图 16 29 编辑本地用户.....232
图 16 30 删除本地用户.....233
图 16 31 用户权限管理列表显示.....233
图 16 32 设置用户权限.....234
图 16 33 编辑用户权限.....234
图 16 34 删除本地用户.....235
图 17 1 基本配置.....237
图 17 2 入侵检测策略配置.....237
图 17 3 自定义入检测.....238
图 17 4 自定义入侵规则.....238

图 17 5 扫描检测配置.....239
图 17 6 自动响应功能.....239
图 17 7 检测结果.....240
图 17 8 抗 DDos 攻击界面.....240
图 18 1 网络设备监控.....242
图 18 2 网络设备当前状态.....243
图 18 3 网络设备流量统计.....243
图 18 11 调试结果.....247
图 18 12 批处理工具.....248
图 18 13 执行批处理.....249
图 18 14 取消批处理.....249
图 19 1 网御 SIS 安全隔离网闸技术支持.....251
图 19 2 关于网御 SIS 安全隔离网闸.....252
图 20 1 分页显示操作区.....254
图 20 2 分页显示操作区.....254
图 20 3 排序显示操作区.....255
图 21 1 已经配置的普通访问任务.....256

表目录

表 2 1 工具栏中的按钮说明.....4
表 2 2 菜单分类和说明.....5
表 3 1 管理员级别与授权.....18
表 4 1 物理设备上可配置的属性.....25
表 4 2 别名设备可配置的属性.....27
表 4 3 冗余设备可配置的属性.....28
表 4 4 添加和编辑时参数说明.....32
表 4 5 基本配置参数说明.....33
表 4 6 IP/MAC 地址探测项说明.....41
表 4 7 绑定 IP/MAC 对配置项说明.....41
表 4 8 添加地址绑定项说明.....43
表 5 1 地址类型列表.....45
表 5 2 地址组添加元素表.....46
表 6 1 引擎管理配置参数说明.....55
表 10 1 基本配置参数说明.....99
表 10 2 设置 HTTP 请求方法参数说明.....108
表 11 1 基本配置参数说明.....121
表 11 2 设置用户控制参数说明.....123
表 12 1 基本配置参数说明.....148
表 12 2 基本配置参数说明.....158
表 13 1 基本配置参数说明.....169
表 14 1 基本配置参数说明.....188
表 14 2 基本配置参数说明.....197
表 15 1 基本配置参数说明.....208
表 18 1 调试工具及参数说明.....246
表 18 1 字符合法性规则说明.....253
表 18 2 资源定义分页功能列表.....254

第 1 章 前言

1.1 导言

《Web 界面操作手册》是网御 SIS 安全隔离与信息交换系统管理员手册中的一本。该手册介绍了如何使用 Web 界面对网御 SIS 安全隔离网闸进行管理。

1.2 本书适用对象

本手册适用于负责支持、维护 SIS 安全隔离网闸的安全管理员，是对网御 SIS 安全隔离网闸进行配置管理时的必备手册。

使用本手册的读者，应掌握 TCP/IP 协议，IP 地址及子网掩码等基本知识。

1.3 本书适合的产品

本书适合网御 SIS 安全隔离与信息交换系统系列产品，以后简称“网御 SIS 安全隔离网闸”，不再说明。

1.4 手册章节组织

本手册按照以下章节编排：

第1章 前言，描述本书适用的读者，手册章节组织及相关参考手册等。

第2章 如何开始，介绍产品特点和功能，配置管理SIS安全隔离网闸的一般方法。

第3章 系统配置，描述与SIS安全隔离网闸管理相关的配置，包括：系统时钟设置、时钟服务器同步、模块升级、系统配置、管理主机、管理员帐号、管理员证书、管理方式、用户认证服务器、日志服务器、集中管理等。

第4章 网络配置，描述与网络环境相关的配置，包括：网络接口属性、域名服务器、静态路由、HA 设置，以及地址绑定等。

第5章 资源定义，描述“地址”、“用户”、“时间”资源的定义方法，这些资源定义可供各种访问任务使用，包括：地址列表、地址组、域名地址；用户列表、用户组；时间列表、时间组等。

第6章 文件交换，描述内外网之间文件传输任务的配置，包括：基本配置、任务配置、内容控制等。

第7章 数据库同步，描述数据库同步网闸任务的配置，包括：基本配置、网闸客户端任务和网闸服务端任务。

第8章 消息模块，又称通用接入平台，该模块对外提供可编程API接口，跨网之间进行信息传输。消息形式包括字符串、文件等，包括基本配置、客户端和服务端任务管理、内容过滤、用户认证配置等；

第9章 FTP访问，描述内外网之间的FTP访问任务的配置，包括：基本配置、任务配置、内容过

滤等。

第10章 邮件访问，描述邮件访问任务的配置，包括：SMTP邮件发送的客户端和服务端任务、POP3邮件接收的客户端和服务端任务。

第11章 数据库访问，描述各种数据库类型传输任务的配置，包括：客户端下透明访问和普通访问任务的配置、服务端下透明访问和普通访问任务的配置。

第12章 安全浏览，描述HTTP&HTTPS浏览访问任务的配置，包括：基本配置、透明模式和普通模式访问任务的配置、用户认证、内容过滤等。

第13章 定制访问，描述基于TCP/UDP访问协议的定制访问任务的配置，包括：基于TCP协议的客户端和服务端任务的配置（透明模式和普通模式）、基于UDP协议的客户端和服务端任务的配置（透明模式和普通模式）。

第14章 安全通道，描述安全通道的配置方法，包括基本配置、客户端配置、服务端配置等。

第15章 抗攻击设置，描述各种入侵检测功能、抗攻击的设置，包括：入侵检测配置、抗DDos攻击配置。

第16章 系统监控，描述如何监控系统的运行状态，包括：网络设备、文件交换任务、资源状态、日志信息、网络调试工具、批处理工具等。

第17章 在线支持。

第18章 公共操作说明，描述了整体系统操作的一些公共属性和操作方法，包括：字符合法性说明、分页显示/查找/排序等通用操作说明。

第19章 附录，包括：常见问题解决等。

1.5 相关参考手册

《网御 SIS 安全隔离与信息交换系统 命令行操作手册》：介绍了如何通过命令行管理网御 SIS 安全隔离网闸。

第 2 章 如何开始

本章主要介绍网御 SIS 安全隔离网闸的产品功能和特点、开机登录配置管理界面的方法。如果您想尽快配置使用网御 SIS 安全隔离网闸，可跳过概述部分，直接阅读 2.2 节。

2.1 网御 SIS 安全隔离网闸概述

网御 SIS-3000 系列是网御依靠多年信息安全产品研发的积累， 严格遵照国家有关主管部门的设计规范要求， 具有完全自主知识产权的安全隔离与信息交换系统。它采用多主机隔离结构，在业内首次提出并实现专有 SIS 安全隔离技术，把安全性(Security)、智能性(Intellegence)、高效性(Speed)完美的结合在一起。其工作原理如下图：

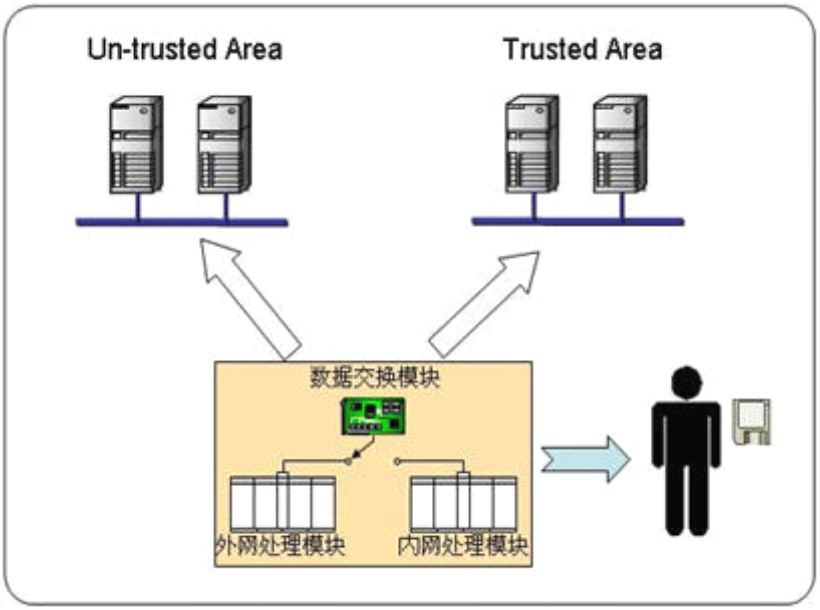


图 2 1 SIS 安全隔离网闸工作原理

2.1.1 产品特点

网御 SIS-3000 系列安全隔离与信息交换系统在业内首次提出并实现专有 SIS 安全隔离技术。SIS 技术体现了安全隔离与信息交换系统三大特点：安全性、智能性、高效性，具体体现在：

- 安全性：通过专有安全芯片实现安全隔离，不同于采用计算机系统所配备的标准 USB、串口、1394 协议等非网络接口实现安全隔离，具有高度安全性。
- 智能性：通过信息摆渡机制，在硬件底层采用独立控制逻辑技术自动实现网络协议阻断和数据交换，而在应用层通过专有协议转换模块的处理，用户可以透明的使用安全隔离与信息交换系统，体现了系统具有高度的智能性。
- 高效性：由于采用专有硬件进行交换，针对数据交换特点，内部设计了高速交换总线，采用 DMA 流水线传输技术，既不占用 CPU 时间，又能实现高速数据交换，实现了真正的高性能。

网御 SIS-3000 系列安全隔离与信息交换系统安装应用方便，通过对连接和数据包的获取、

阻断、分离、检测、重组、交换、恢复、连接等一系列安全操作完成数据的隔离与交换，而这些复杂的安全检测操作对用户而言是透明的，最大限度的保证了用户应用的方便性。

2.1.2 主要功能

网御 SIS-3000 系列安全隔离与信息交换系统根据不同的应用需求，量身定制多个功能模块，满足用户的不同应用需求，主要包括：

- 文件交换模块：实现不同安全等级网络间文件的安全交换，支持更新传输、改名传输、传输后删除等多种方式。
- 数据库访问模块：在内外网隔离环境下实现对多种数据库系统的安全访问和同步。目前已经支持 Oracle、SQLServer、MYSQL、DB2、SYBASE 等数据库类型，并且提供了安全、可靠的过滤控制。
- 邮件访问模块：在内外网隔离环境下实现内网用户安全访问外网邮件服务器。
- 安全浏览模块：在内外网隔离环境下保证内网用户安全浏览外网资源。
- FTP 访问模块：在内外网隔离环境下实现安全的 FTP 访问。
- TCP/UDP 访问模块：在内外网隔离环境下实现 TCP/UDP 协议的定制交换。
- 其他模块：其它定制用户专有应用模块。

2.1.3 软件描述

界面框架如图 2-2 所示：

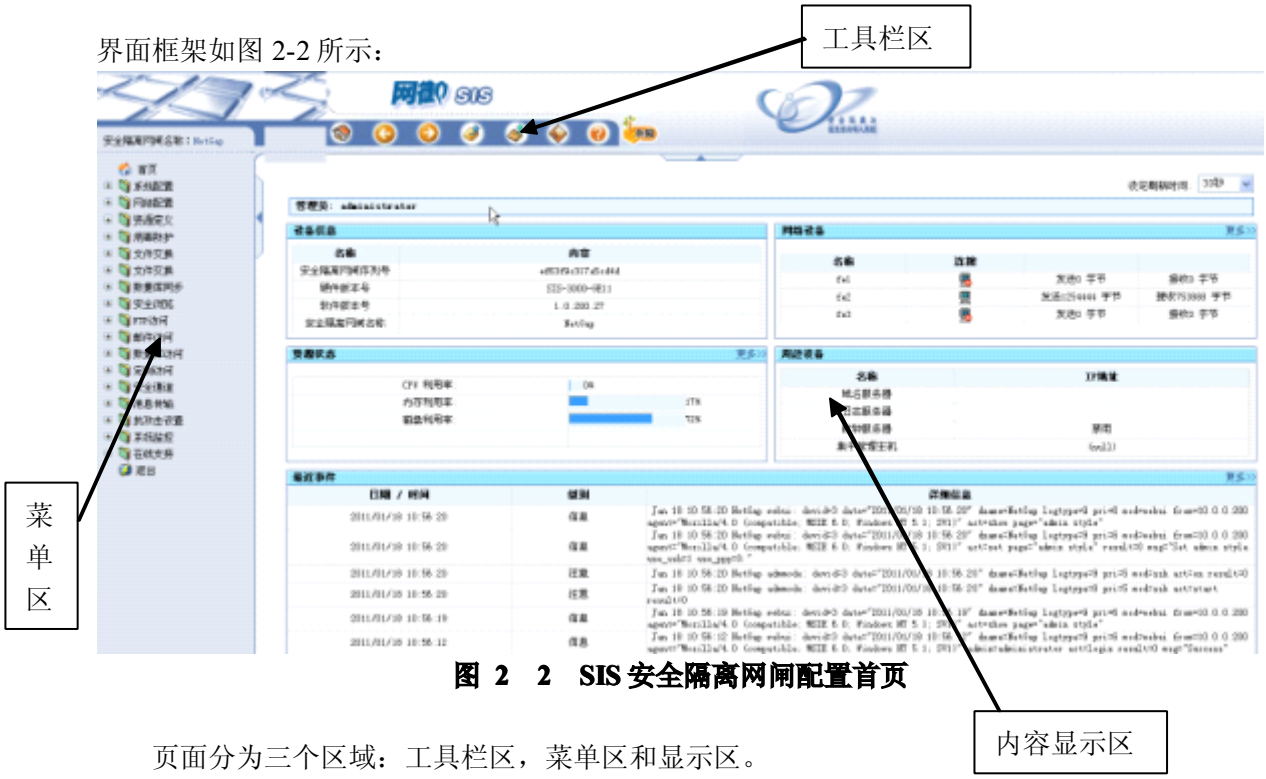


图 2 2 SIS 安全隔离网闸配置首页

页面分为三个区域：工具栏区，菜单区和显示区。

表 2 1 工具栏中的按钮说明

图标	功能说明
	直达首页
	回到本页的上一页

	前进到本页的下一页
	导出日志
	导出 SIS 安全隔离网闸配置
	保存所有 SIS 安全隔离网闸配置
	在线帮助

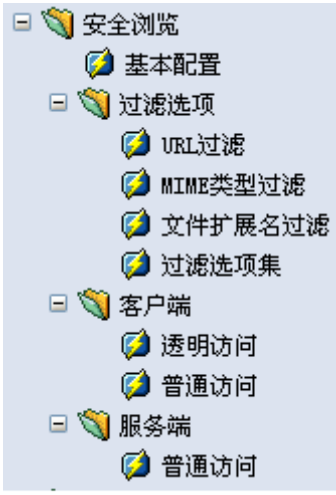
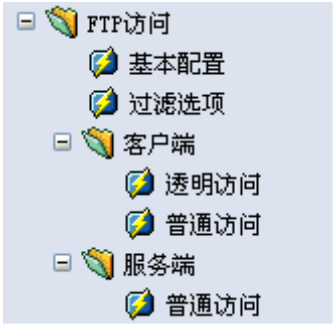
菜单采用类似 Windows 操作系统资源管理器的树型结构。

菜单的分类和排列含有逻辑关系，了解这些逻辑关系将有助于管理员记忆并快速定义操作页面。

表 2 2 菜单分类和说明

一级菜单	说明
系统配置 系统配置 日期时间 系统参数 系统更新 模块升级 导入导出 管理配置 管理主机 管理员帐号 管理员证书 管理方式 报告设置 日志服务器 集中管理 产品许可证	如何管理、升级、报告。包括： 调整日期时间 设置系统参数 系统更新 导入导出系统配置文件和模块升级 设置管理主机、管理员帐号、管理员证书和管理方式 设置日志服务器、集中管理等报警机制 导入产品许可证 配置管理员具有修改这些配置的权限，其中管理员帐号的修改只能由超级管理员 administrator 进行。
网络配置 网络配置 网络设备 域名服务器 静态路由 高可靠性设置 基本配置 IP探测 虚拟地址 负载均衡 地址绑定	作为一台网络设备，必须的一些配置，包括： 网络接口属性（工作模式、IP 地址等） 域名服务器 静态路由 高可靠性 地址绑定 配置管理员具有修改这些配置的权限。

资源定义 资源定义 地址 地址列表 地址组 域名地址 用户 用户列表 用户组 时间 时间列表 时间组	为简化 SIS 安全隔离网闸各类任务的维护工作，引入了资源定义，可以定义以下资源： 地址：地址、地址组、域名地址 用户：用户列表、用户组 时间：时间、时间组 资源只有被安全规则引用才能起作用，否则不起作用。并且，在配置任务中，已被引用的资源在此被修改，则不会对已经运行的任务起作用，即只能对后续引用的任务起作用。 策略管理员具有定义资源的权限。
病毒防护 病毒防护 引擎管理 病毒库升级	该模块为各应用模块提供病毒扫描和检测功能。菜单项包括： 引擎管理：用于控制病毒引擎的启停以及显示当前病毒引擎的启停状态。 病毒库升级：用于配置病毒库升级的基本参数。
文件交换 文件交换 基本配置 客户端 服务端 内容控制 文件名控制 内容黑名单 内容白名单	用于配置内外网的文件传输，包括： 基本配置：配置文件交换任务的运行状态等基本参数； 客户端：添加、修改、删除客户端任务； 服务端：添加、修改、删除服务端任务； 内容控制：用于配置文件传输时的参数
数据库同步 数据库同步 基本配置 客户端 服务端	用于跨网之间的数据库同步，包括： 基本配置：配置文件交换任务的运行状态等基本参数； 客户端：添加、修改、删除客户端任务； 服务端：添加、修改、删除服务端任务； （注：该模块需要外部同步客户端的配合使用）
安全浏览	该模块支持用户通过浏览器访问 Internet，提供普通和透明两种模式。菜单项包括： 基本配置：配置安全浏览的一些全局参数，如：本机监听地址及其端口，HTTP 方法、HTTP&HTTPS 可访问的端口，以及当前服务允许状态； 过滤选项：包括 URL 过滤，MIME 类型过滤，文件扩展名过滤和过滤选项集； 客户端：透明访问，普通访问； 服务端：普通访问；

	
FTP 访问 	用于配置内外网的 FTP 访问，包括： 基本配置：配置 FTP 访问的运行状态等基本参数； 过滤选项：配置 FTP 访问过滤选项集的参数； 客户端：透明访问，普通访问； 服务端：普通访问；
邮件访问 	“邮件访问”模块支持一侧网络用户访问另一侧网络的邮件服务器（包括 POP3 访问和 SMTP 访问）。菜单项包括： 过滤选项：包括邮件地址，内容关键字，附件扩展名，过滤选项集； SMTP 基本配置 客户端：透明访问任务、普通访问任务 服务端：普通访问任务 POP3 基本配置 客户端：透明访问任务、普通访问任务 服务端：普通访问任务
数据库访问	该模块支持内外网用户访问对方数据库。菜单项包括： 基本配置 过滤选项：包括用户过滤，SQL 语句过滤，过滤选项集； 客户端：透明访问任务、普通访问任务 服务端：普通访问任务

数据库访问 基本配置 过滤选项 用户过滤 SQL语句过滤 过滤选项集 客户端 透明访问 普通访问 服务端 普通访问	
定制访问 定制访问 TCP访问 基本配置 客户端 透明访问 普通访问 服务端 普通访问 UDP访问 基本配置 客户端 透明访问 普通访问 服务端 普通访问	定制访问支持基于 TCP/UDP 协议的、针对固定服务器地址和端口号的常规访问。菜单项包括： TCP 基本配置：配置 TCP 定制访问任务的服务启停状态； 客户端：透明访问任务、普通访问任务； 服务端：普通访问任务； UDP 基本配置：配置 UDP 定制访问任务的服务启停状态； 客户端：透明访问任务、普通访问任务； 服务端：普通访问任务；
安全通道 安全通道 基本配置 客户端 服务端	配置安全通道。菜单项包括： 基本配置：配置通道的启停状态； 客户端：配置客户端通道； 服务端：配置服务端通道；
消息传输	用于与第三方应用系统相结合，实现跨网信息传输，包括： 基本配置：配置文件交换任务的运行状态等基本参数； 客户端：添加、修改、删除客户端任务； 服务端：添加、修改、删除服务端任务； 内容控制：用于配置文件传输时的内容过滤参数； 用户管理：用于配置和管理认证用户、访问用户；

消息传输 基本配置 客户端 服务端 内容控制 文件名控制 内容黑名单 内容白名单 用户管理 本地用户认证 用户权限	
抗攻击设置 抗攻击设置 入侵检测 基本配置 策略配置 自定义检测 扫描检测配置 自动响应配置 显示检测结果 抗DDos攻击	配置设备的各种入侵检测，以及抗攻击开关。菜单项包括： 入侵检测：IDS 基本配置、策略配置、各类自定义配置、扫描检测、自动响应配置，以及显示检测结果等； 抗攻击：抗 DDos 攻击等
系统监控 系统监控 网络设备 资源状态 日志信息 用户信息 网络调试工具 批处理工具	可以监控 SIS 安全隔离网闸运行状态，包括： 网络设备状态：网口的实时状态和流入量流出量的统计信息 资源状态：CPU 利用率、内存利用率 日志信息：对日志简单分类和过滤 用户信息 网络调试工具 批处理工具
在线支持 在线支持 在线注册 技术支持 关于	在线注册、技术支持等

2.2 配置管理方法

网御 SIS 安全隔离网闸的配置界面有两种方式：基于 Web 的图形方式和基于 CLI 的命令行方式。其中通过命令行方式配置时，可以利用网络连接（SSH）或串口连接进行命令行配置。

2.2.1 网络接口 Web 配置

支持远程安全管理和集中安全管理两种方式，优越性更表现在其集中安全管理的特性上。

1. 远程安全管理——支持 SSL 协议，采用基于密码技术的 PKI-CA 证书认证和基于双因子硬件一次性口令认证技术的管理员身份认证，使得只有认证通过的管理员才能通过远程访问配置 Web 管理界面、操作相关文件，所有 SIS 安全隔离网闸配置文件及与安全有关的数据都经加密处理存放。

2. 集中式安全管理——管理员通过集中管理中心可以对全局网络中的 SIS 安全隔离网闸进行统一的配置与管理，支持 SNMP、SSL 协议，利用 SNMP 的 trap 机制实现安全事件报警。具体包括：

   （1）拓扑管理：具有设备自动发现功能，使管理员拥有对网御 SIS 安全隔离网闸设备信息的全局掌握和控制。

   （2）系统监测：监视网御 SIS 安全隔离网闸的设备运行状态和统计数据系统状态，并在事件发生时通过图形界面向管理员发出通知。

   （3）配置管理：可以对网络中的网御 SIS 安全隔离网闸进行统一的安全配置、管理和系统监视。

2.2.2 网络接口 CLI 配置

提供命令行方式的基本配置管理和灾难恢复功能，通过 SSH 方式进行 SIS 安全隔离网闸的安全管理和维护，并由管理员根据实际需要决定本功能的是否启用。

2.2.3 本地串口 CLI 配置

基于串口连接，提供命令行方式的基本配置管理和灾难恢复功能，提供了管理的安全、方便与灵活性。

2.3 登录管理界面

2.3.1 登录方法

SIS 安全隔离网闸共有三种管理方式：1）Web 界面管理 2）串口命令行管理 3）远程 SSH 登录管理。其中管理方式 1）和 2）是默认开启的，3）默认是关闭的。

在 Web 界面管理中，管理主机默认只能连接 SIS 安全隔离网闸（包括内网主机、外网主机）的管理口，如果需要连接其它网口，必须进行相应的设置。默认的管理主机 IP 地址是 10.0.0.200，Web 界面管理使用 SSL 协议来加密管理数据通信，因此使用 IE 来管理 SIS 安全隔离网闸时，在地址栏输入 https://a.b.c.d:8889/，来登录 SIS 安全隔离网闸，其中 SIS 安全隔离网闸的地址“a.b.c.d”，其中内网主机管理口的初始值为“10.0.0.1”，外网主机管理口的初始值为“10.0.0.2”。登录 SIS 安全隔离网闸的初始用户名和口令都是“administrator”，“administrator”中所有的字母都是小写的。

注：后续章节中，没有特别说明，均以内网主机为例，进行举例说明。

在串口命令行管理中，管理客户端的配置是 9600-8-N-1，管理主机默认连接 SIS 安全隔离网

闸的 CONSOLE。

注：用 Web 界面管理时，建议管理主机设成小字体，分辨率为 1024*768；其他字体和分辨率可能使界面显示不全或顺序混乱。

SSH 登录管理必须首先在系统菜单“配置>>管理配置>>管理方式”中设置允许 SSH 登录，才可以通过 SSH 协议远程登录 SIS 安全隔离网闸。以 SecureCRT 3.4.3 (Official)版本客户端为例，客户端设置选择协议为 ssh2，端口为 22，认证方式为 Password。此时客户端的 IP 必须是管理主机 IP 之一。

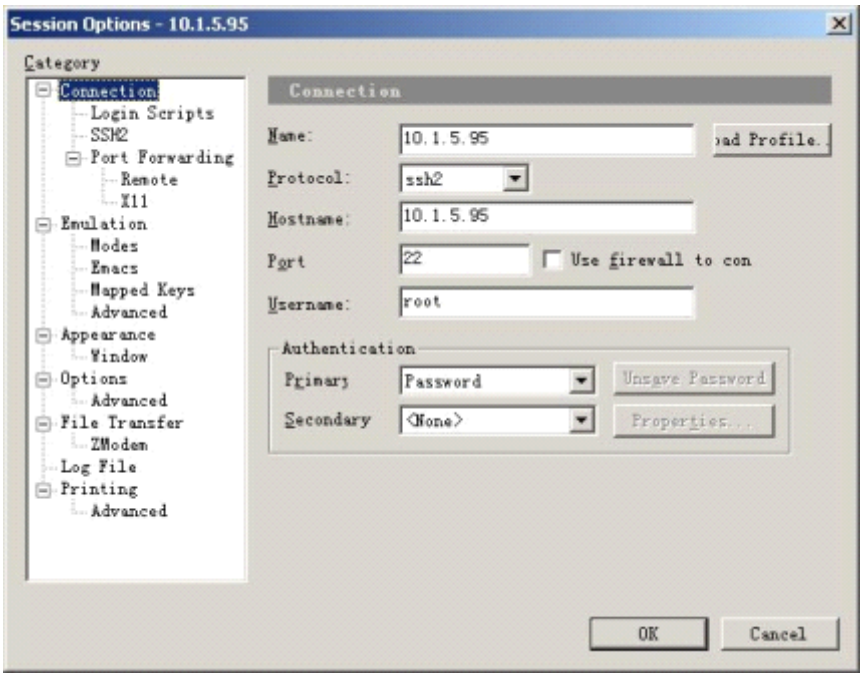


图 2 3 使用 SecureCRT 3.4.3 登录 SIS 安全隔离网闸

2.3.2 管理认证

管理员通过 Web 方式管理 SIS 安全隔离网闸使用证书认证方式。网御 SIS 安全隔离网闸设备中出产时已导入了一套证书（CA 中心证书、SIS 安全隔离网闸证书、SIS 安全隔离网闸密钥、管理员证书）。用户登录前先在本地 IE 中导入浏览器管理员证书后，即可通过登录 https://10.0.0.1:8889 管理 SIS 安全隔离网闸。浏览器管理员证书在网御 SIS 安全隔离网闸设备的随机附带的光盘中提供。

注：用户可以在 系统配置>>管理配置>>管理员证书 导入新的 CA 中心证书、SIS 安全隔离网闸证书、SIS 安全隔离网闸密钥、管理员证书，详细说明参见 3.4.2。

2.3.3 登录过程

登录

1. 接通电源，开启 SIS 安全隔离网闸，选用一台带以太网卡和光驱的 PC 机作为 SIS 安全隔离网闸的管理主机，操作系统应为 Window98/2000/XP，管理主机 IE 浏览器建议为 5.0 以上版本；

注意：SIS 安全隔离网闸正常启动后，会蜂鸣三声，未出现上述现象则表明 SIS 安全隔离网闸未正常启动，请您求助 SIS 安全隔离网闸技术支持人员。

2. 使用随机提供的交叉线，连接管理主机和 SIS 安全隔离网闸的管理接口；
3. 将管理主机的 IP 地址改为 10.0.0.200（SIS 安全隔离网闸出厂时默认指定的管理主机 IP）；
4. 使用上一节介绍的认证方法进行认证。
5. 打开 IE 浏览器，如果使用已经成功导入了浏览器管理员证书，浏览 https://10.0.0.1:8889，出现如下 SIS 安全隔离网闸登录界面：

图 2 4 SIS 安全隔离网闸登录界面

6. 在 SIS 安全隔离网闸登录界面中输入管理员口令 administrator，进入 SIS 安全隔离网闸的配置首页。默认的用户帐号和口令都是 administrator。

当您进入网御 SIS 安全隔离网闸的配置界面后，有关具体参数的说明和配置方法，请参考后续章节。

2.3.4 网御 SIS 安全隔离网闸的一般配置过程

以 Web 界面管理方式为例，配置 SIS 安全隔离网闸一般遵循以下步骤：

1. 登录管理界面，参考 2.3.1 登录方法和 2.3.3 登录过程
2. 选择“资源定义”菜单项中的子项，定义地址、时间等资源。
3. 选择“网络配置>>网络设备>>物理设备”，修改网口的工作模式和 IP 地址。选择“系统配置>>管理配置>>管理主机”，修改管理主机的 IP 地址配置。
4. 系统保存，单击上侧中部磁盘的图标，保存系统配置。如果没有保存就重新启动，系统将恢复到上一次保存的配置。
5. 在日常的维护中，经常观察 SIS 安全隔离网闸“系统监控”菜单下的内容和日志服务器中的日志信息，以便了解 SIS 安全隔离网闸的工作状态。

更详细的内容，请参阅 SIS 安全隔离网闸手册的相关部分。

2.3.5 退出登录

退出 SIS 安全隔离网闸配置管理界面，虽然可以采用直接关闭浏览器界面的方式，但请尽量采用点击界面上“退出”，因为这样可以通知 SIS 安全隔离网闸关闭这个会话，从而最大限度的保证安全性。直接退出还会少记一条管理员退出日志。如果直接关闭浏览器，SIS 安全隔离网闸没有收到结束会话的指令，则会误以为该管理员仍在线管理中，另外如果没有选择“允许多个管理员登录”，则会造成管理员无法登录。

第 3 章　系统配置

本章主要介绍 SIS 安全隔离网闸的系统配置，由以下部分组成：日期时间，系统参数，系统更新，管理配置，报告设置，用户认证服务器配置和产品许可证等。

3.1 日期时间

SIS 安全隔离网闸系统时间的准确性是非常重要的。可以采取两种方式来同步 SIS 安全隔离网闸的系统时钟：

1) 与管理主机时间同步
2) 与网络时钟服务器同步（NTP 协议）

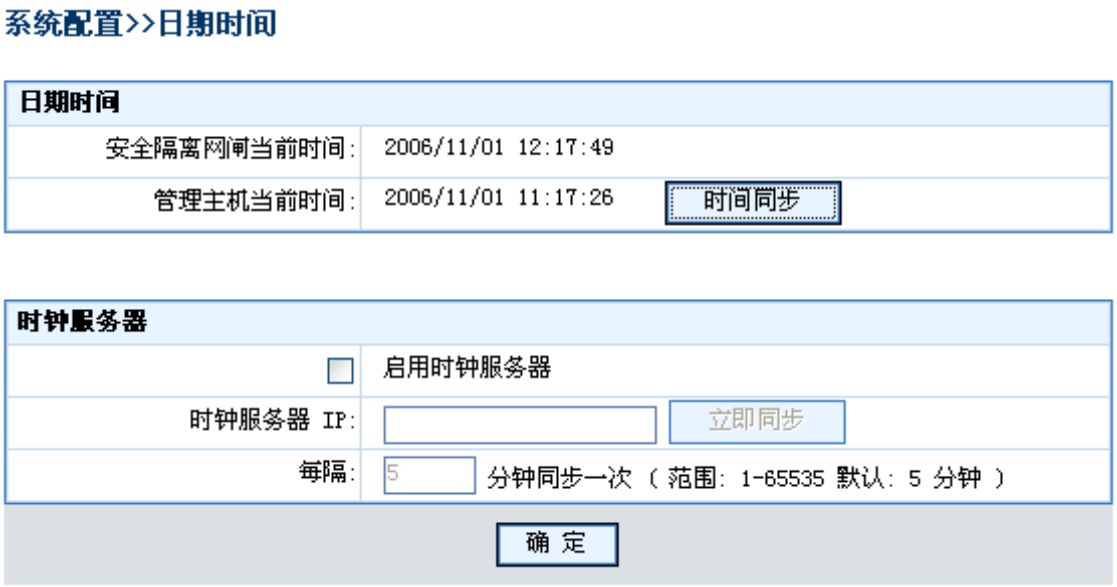


图 3　1　配置 SIS 安全隔离网闸时间

与管理主机时间同步

1. 调整管理主机时钟
2. 点击“时间同步”按钮

与时钟服务器时间同步有两种方式

1. 立即同步
2. 周期性自动同步

立即同步

1. 选中“启用时钟服务器”，输入“时钟同步服务器 IP”
2. 点击“立即同步”按钮

周期性自动同步

1. 选中“启用时钟服务器”，输入“时钟同步服务器 IP”

2. 设定同步周期
3. 点击“确定”按钮系统参数

注意事项：

SIS 安全隔离网闸的很多操作依赖于系统时间，改变系统时间会对这些操作发生影响，比如更改时间后配置管理界面登录超时等。

3.2 系统参数

系统参数设置 SIS 安全隔离网闸名称。

SIS 安全隔离网闸名称的最大长度是 20 个 ASCII 字符，不能有空格。默认的 SIS 安全隔离网闸名称是 NetGap，用户可以自己修改这个名称。

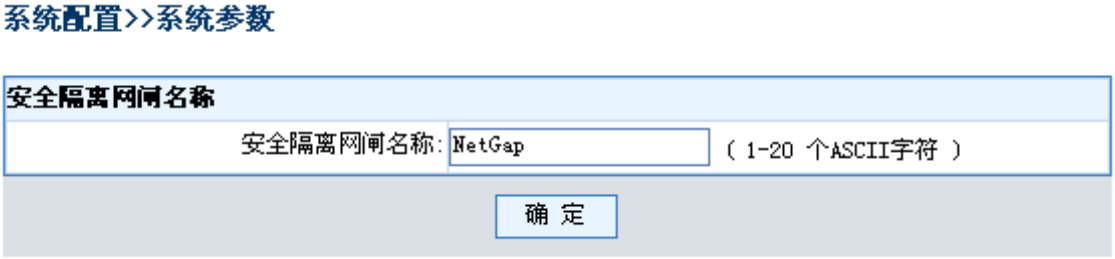


图 3 2 系统参数配置图

3.3 系统更新

3.3.1 模块升级

SIS 安全隔离网闸系统升级功能可以快速响应安全需求，保证 SIS 安全隔离网闸功能与安全的快速升级。

图 3 3 导入升级文件

模块升级界面包括以下功能

1. 模块升级
2. 导出升级历史
3. 检查最新升级包

4. 重启 SIS 安全隔离网闸

模块升级

1. 点击“浏览”按钮，选择管理主机上的升级包
2. 点击“升级”按钮

点击“重启安全隔离网闸”按钮，重启 SIS 安全隔离网闸完成升级

导出升级历史

点击“导出升级历史”按钮，导出升级历史做备份。

检查最新升级包

管理员可以查看“系统当前软件版本”，点“检查最新升级包”，系统会弹出新的 IE 窗口并连接网御安全服务网站（SIS 安全隔离网闸可以连接 Internet）。

重启 SIS 安全隔离网闸

点击“重启安全隔离网闸”按钮，SIS 安全隔离网闸将重新启动。

注意：重启安全隔离网闸前，记住要保存当前配置。“保存”快捷键：

3.3.2 导入导出

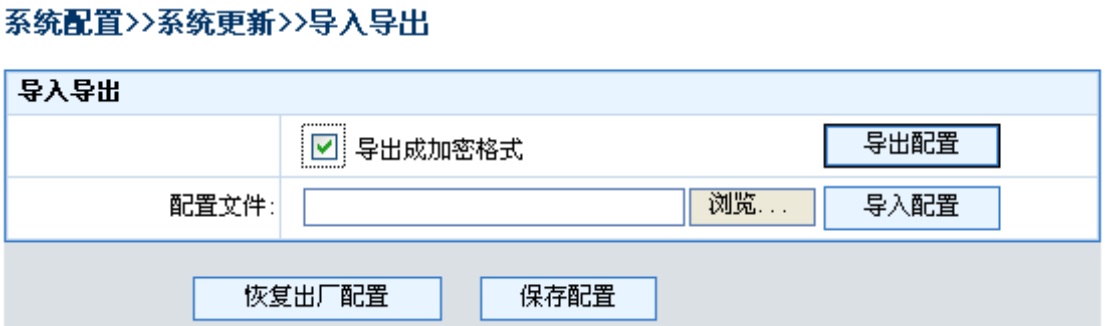


图 3 4 导入导出配置文件

导入导出界面包含以下功能

1. 导出系统配置
2. 导入系统配置
3. 恢复出厂配置
4. 保存配置
5. 查看当前配置

导出配置

点击“导出配置”按钮，导出最后一次保存的所有系统配置到管理主机，管理员的用户名和密码将不会被导出。选中“导出成加密格式”，则加密配置文件。

导入配置

点击“浏览”按钮，在管理主机上选择要导入的配置文件，点击“导入配置”按钮，导入配置文件，系统提示导入成功，重启 SIS 安全隔离网闸，导入的配置生效。注意：导出的配置文件

带有 SIS 安全隔离网闸软硬件版本的信息，不能导入到别的版本 SIS 安全隔离网闸中，而且如果同样的配置文件被导入到不同 SIS 安全隔离网闸中，且这些 SIS 安全隔离网闸位于同一网络时，可能会引起配置冲突，如 IP 地址，MAC 地址等。

恢复出厂配置

点击“恢复出厂配置”按钮，SIS 安全隔离网闸所有配置丢失，恢复到出厂配置，重启 SIS 安全隔离网闸后生效。

保存配置

点击“保存配置”，保存所有系统配置。也可以按上方保存快捷图标来保存。

3.4 管理配置

3.4.1 管理主机

管理员只有在管理主机上才能对 SIS 安全隔离网闸进行管理，最多支持 6 个管理主机 IP 和 1 个集中管理主机，至少有 1 个管理主机 IP 不能被删除。

SIS 安全隔离网闸出厂时的默认管理主机，10.0.0.200，子网掩码 255.255.255.255。

图 3 5 添加、编辑管理主机

此界面完成以下功能

1. 添加管理主机
2. 删除管理主机
3. 转到“系统配置>>报告设置>>集中管理”界面

添加管理主机

1. 输入管理主机 IP
2. 在“说明”中，输入描述性文字，此步骤可忽略
3. 点击“确定”按钮完成添加

修改管理主机

1. 从“管理主机 IP”列表中修改要修改的管理主机 IP
2. 点击“确定”按钮完成修改

删除管理主机

1. 从“管理主机 IP”列表中删除要删除的管理主机 IP
2. 点击“确定”按钮完成删除

转到“系统配置>>报告设置>>集中管理”界面

1. 点击“集中管理主机”链接，可以跳转到“系统配置>>报告设置>>集中管理”页面，进行集中管理设置。

3.4.2 管理员帐号

管理员按级别授权管理，说明如下：

表 3 1 管理员级别与授权

管理员级别	授权	备注
超级管理员	增加、删除管理员帐号，不能直接配置管理。	默认管理员帐号与密码为 administrator：administrator。 帐号 administrator 不能删除。
配置管理员	配置系统策略、网络配置、在线帮助。	无默认帐号
策略管理员	配置安全策略、资源定义、在线帮助。	无默认帐号
审计管理员	查看 SIS 安全隔离网闸日志信息、在线帮助。	无默认帐号

默认只能有一个管理员登录 SIS 安全隔离网闸进行配置管理，选择“允许多个管理员同时管理”时，SIS 安全隔离网闸系统才会允许多个管理员同时登录，但最好不要多个管理员同时进行修改配置。

图 3 6 显示管理员帐号

此界面可完成以下功能

1. 添加管理员帐号
2. 编辑管理员帐号
3. 删除管理员帐号

4. 允许或禁止多个管理员同时管理
5. 设定管理员登录超时时间

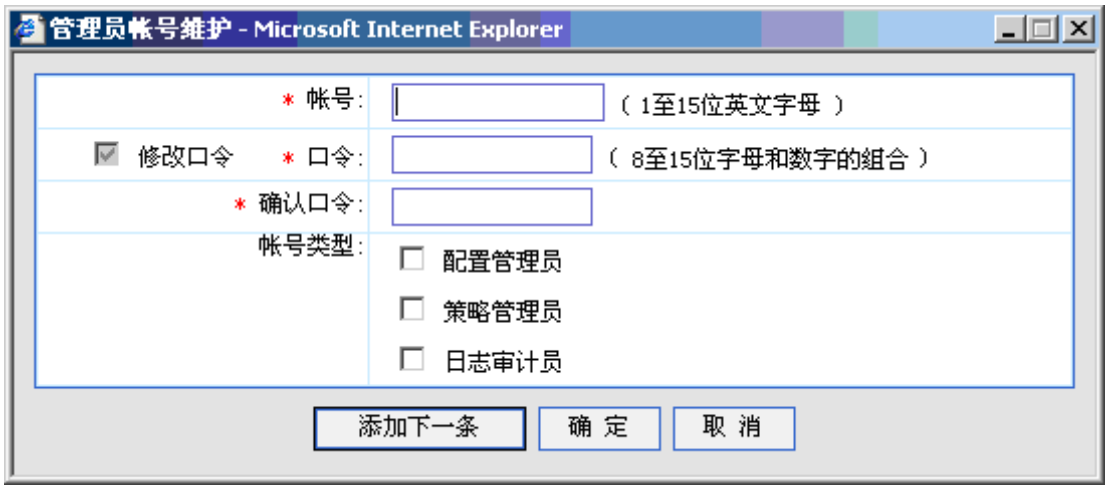


图 3 7 添加、编辑管理员帐号

添加管理员帐号

1. 点“添加”按钮，打开管理员帐号维护界面
2. 输入帐号、口令，并选择要添加的管理员帐号类型
3. 点“确定”按钮完成，点“添加下一条”可以继续添加管理员帐号

编辑管理员帐号

1. 点操作栏中“编辑”的快捷图标，打开管理员帐号维护界面
2. 修改口令或帐号类型
3. 点“确定”按钮完成

删除管理员帐号

1. 点操作栏中“删除”的快捷图标，弹出删除对话框
2. 点“确定”按钮完成删除

允许或禁止多个管理员同时管理

选择“允许多个管理员同时管理”时，SIS 安全隔离网闸系统才会允许多个管理员同时登录。

设定管理员登录超时时间

管理员登录后如果长时间没有操作，配置界面会超时，超时时间也在这里设置，缺省值是 600 秒，最大超时时间可设为 86400 秒（24 小时），0 是非法值。设置后点击“确定”生效。

注意：admin 是系统预设的一个帐号，密码为 admin123。

3.4.3 管理员证书

本界面完成主要的证书管理。管理证书为标准的 CA 证书。

SIS 安全隔离网闸是通过 https 协议访问，即使用管理证书完成 SSL 的加密。

管理员通过 IE 导入随机光盘的管理员证书后，可以访问 https://SIS 安全隔离网闸可管理 IP:8889，登录 SIS 安全隔离网闸配置界面，使用 SIS 安全隔离网闸 Web 服务器的客户端的证书进行信道加密。

如果用户觉得随机携带的证书不够安全，希望自己生成证书，可以在 SIS 安全隔离网闸中导入一套证书（CA 中心证书、SIS 安全隔离网闸证书、SIS 安全隔离网闸密钥、管理员证书），并在管理主机的 IE 中导入管理员证书。管理员可以点击 CA 中心证书的链接、SIS 安全隔离网闸证书的链接进行查看。管理员可以查看导入的管理员证书列表。

此界面包括以下功能

1. 到网御 CA 中心下载证书
2. 导入一套证书（CA 中心证书、SIS 安全隔离网闸证书、SIS 安全隔离网闸密钥、管理员证书）
3. CA 中心证书、SIS 安全隔离网闸证书查看
4. 管理员证书维护（生效、删除）

图 3 8 导入和显示管理证书

操作流程：

1. 管理员向 CA 中心申请证书，选择一套匹配的 CA 中心证书、安全隔离网闸证书、安全隔离网闸密钥“导入”。
2. 管理员要将选择匹配的管理员证书”导入”。点”生效”，使用相关管理员证书生效。
3. 登录 SIS 安全隔离网闸系统前，请将有效管理员证书导入管理主机的 IE 浏览器中，访问 https://SIS 安全隔离网闸可管理 IP:8889，进入 SIS 安全隔离网闸配置管理界面。

注意：CA 中心证书、安全隔离网闸证书、安全隔离网闸密钥必须是配套的。只接受 PEM 格式的证书。

下载证书

点“网御 CA 中心”按钮，打开网御 CA 中心的主页，下载证书

导入证书

点“浏览”按钮，分别导入一套匹配的 CA 中心证书、安全隔离网闸证书、安全隔离网闸密钥、管理员证书。CA 中心证书、安全隔离网闸证书、安全隔离网闸密钥必须同时更换。

管理员证书维护

管理员证书维护包括生效和删除，在“生效”一栏选择要生效的证书，点“生效”按钮则生效选中的证书。在“操作”一栏中，点“删除”的图标，删除此证书。

3.4.4 管理方式

SIS 安全隔离网闸提供 WEB 界面和 CLI 命令行两种管理方式。可以通过网口访问、串口访问。

WEB 管理方式和串口命令行方式默认打开，不可关闭。

使用 WEB 方式管理 SIS 安全隔离网闸，管理主机必须能通过网络访问 SIS 安全隔离网闸，并且其 IP 地址必须在 SIS 安全隔离网闸上设置（参考：系统配置>>管理配置>>管理主机）。

使用串口命令行方式管理，管理主机通过串口连接 SIS 安全隔离网闸的 CONSOLE 口登录。

“启用远程 SSH”后，管理主机可以通过网络连接（通用网口连接即可），利用 secure crt 或 putty 等终端管理软件登录 SIS 安全隔离网闸命令行界面进行管理。

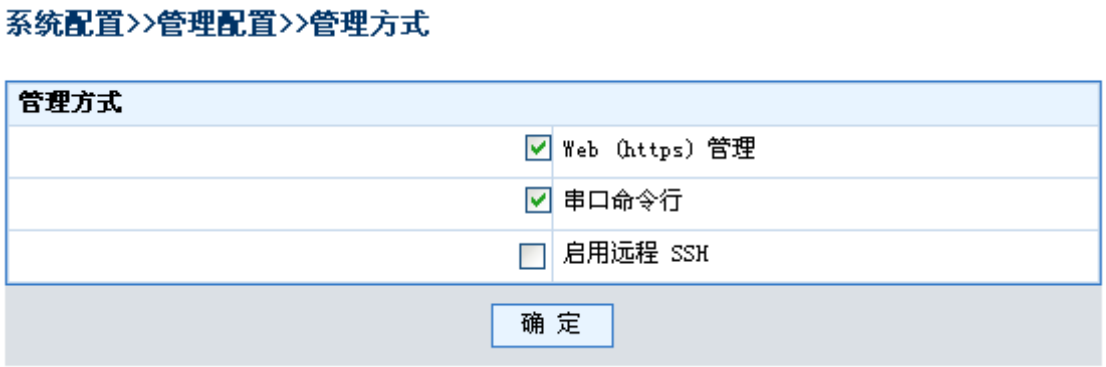


图 3 9 显示和配置管理方式

3.5 报告设置

3.5.1 日志服务器

SIS 安全隔离网闸各功能模块提供标准日志记录。

启用日志记录后，默认情况下日志存储在 SIS 安全隔离网闸本地。SIS 安全隔离网闸也可以将日志发往第三方的日志服务器，

日志服务器可以与 SIS 安全隔离网闸的任意网口连接。

SIS 安全隔离网闸提供随机日志服务器软件，提供强大的日志存储与审计功能。

图 3 10 日志服务器配置

此界面提供以下功能：

- 配置日志服务器
- 转到“系统监控>>日志信息”界面

配置日志服务器

需要管理员配置日志服务器 IP、SIS 安全隔离网闸与日志服务器通信的协议与端口。SIS 安全隔离网闸默认使用 syslog 方式向第三方发送日志，端口 514/ 协议 UDP。

转到“系统监控>>日志信息”界面

点“查看日志”按钮，转到“系统监控>>日志信息”界面

3.5.2 集中管理

支持安全隔离网闸的集中管理（SNMP v1&v2c 和 v3）。安全隔离网闸可以与网御集中安全管理系统无缝联动。

管理员配置集中管理主机的 IP、各项监控信息的阈值和 SNMP v1&v2c 的团体字串及 SNMPv3 的用户信息。网御集中安全管理系统,通过 SNMP 协议从安全隔离网闸获取监控信息，包括：系统名字版本号序列号、CPU 利用率、内存利用率、网络接口状态、网络连通状态等，同时当安全隔离网闸运行信息超过阈值后，通过 SNMP 协议向集中管理主机发 Trap 告警信息。通过 TRAP 信息发给集中管理中心，为网络管理人员提供全面、易用、高效的实时监控网络资源使用状况的工具和手段。相关信息也可以在安全隔离网闸的“系统监控>>网络设备”界面和“系统监控>>资源状态”查看。

集中管理的配置页面如下：

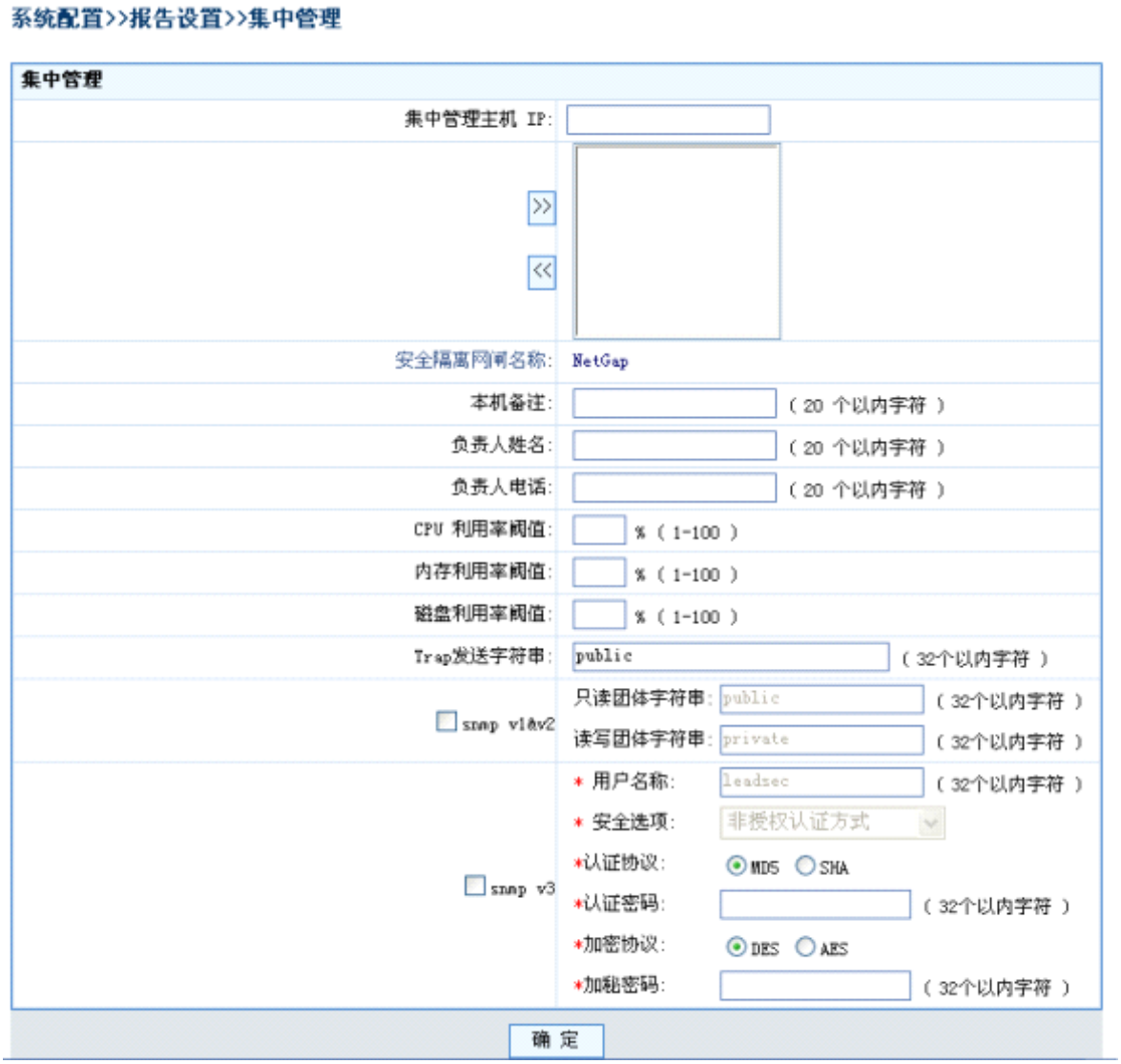


图 3 11 集中管理配置图

表 3 2 集中管理配置元素表

配置项名称	说明
集中管理主机 IP	只有集中管理主机 IP 才能通过 SNMP 访问设备，并接收到 Trap 信息。支持多个集中管理主机 IP，点击“〉〉”添加，“〈〈”删除
安全隔离网闸名称	SIS 安全隔离网闸名称
本机备注	对 SIS 安全隔离网闸的描述
负责人姓名	负责人姓名
负责人电话	负责人电话
CPU 利用率阈值	如果实际利用率超过该值，则向集中管理主机发送报警信息
内存利用率阈值	如果实际利用率超过该值，则向集中管理主机发送报警信息
磁盘利用率阈值	如果实际利用率超过该值，则向集中管理主机发送报警信息
snmp v1&v2	通过此选项控制是否启用 SNMPv1&v2c
只读团体字符串	通过 SNMPv1&v2c 读取设备信息时的认证标识
读写团体字符串	通过 SNMPv1&v2 读/写设备信息时的认证标识
Trap 发送字符串	设备向集中管理主机发送 Trap 报警信息时的标识

snmp v3	通过此选项控制是否启用 SNMPv3
用户名称	SNMP v3 授权用户名
安全选项	选择 SNMP v3 用户访问的安全级别，分为：加密授权认证方式、非加密授权认证方式和非授权认证方式，当选择加密授权认证方式时必须设置认证和加密相关项；当选择非加密授权认证必须设置认证相关项。
认证协议	选择 SNMP v3 用户认证的协议
认证密码	设置 SNMP v3 用户认证的密码
加密协议	选择 SNMP v3 加密协议
加密密码	设置 SNMP v3 加密密码

输入以上各域内容，点“确定”完成集中管理主机配置。同时通过点击“启动 SNMP 代理”/“停止 SNMP 代理”按钮控制安全隔离网闸上的 SNMP 代理服务启动或停止。

3.6 产品许可证

通过本页面可以将您获取到的 SIS 安全隔离网闸模块的许可证上载，并导入到 SIS 安全隔离网闸。上载成功后，请您重新登陆 SIS 安全隔离网闸界面,便可看到 SIS 安全隔离网闸模块已经生效。

图 3 13 产品许可证上载页面

可用模块的启用状态：

License启用信息

序号	模块名	截止时间	状态
1	文件交换	永不过期	启用
2	安全浏览	永不过期	启用
3	FTP访问	永不过期	启用
4	邮件传输	永不过期	启用
5	数据库传输	永不过期	启用
6	定制访问	永不过期	启用
7	抗攻击设置	永不过期	启用
8	高可靠性设置	永不过期	启用

图 3 14 模块的启用状态

第 4 章 网络配置

本章主要介绍 SIS 安全隔离网闸的网络配置，由以下部分组成：网络设备、域名服务器、静态路由、高可靠性设置和地址绑定等。

4.1 网络设备

网御 SIS 安全隔离网闸可配置的网络设备包括：物理设备、别名设备和冗余设备。下面对各类设备的特点做一简要说明。

物理设备：SIS 安全隔离网闸中实际存在的网口设备，不能删除，也不能添加。增减网络接口硬件模块会自动在网络配置中显示出来，不需要手动操作。其中第二个物理设备 **fe2** 是默认的管理设备，它的默认 IP 地址是 10.0.0.1，这个地址允许管理，PING 和 TRACEROUTE。物理设备是其他设备的基础，如果增减网络接口硬件模块，与这个设备相关的其它设备都会受到影响，这一点需要特别注意。

别名设备：用于给物理设备配置多个 IP 地址。每个物理设备可以关联的别名设备是 253 个，这些 IP 具有“用于管理”，“允许 PING”，“允许 TRACEROUTE”等属性。同时要注意的是别名设备的 IP 地址不能重复。

冗余设备：是将多个物理设备捆绑在一起而成的虚拟设备。冗余设备捆绑的物理设备共同完成收发工作，组成一个逻辑链路供系统使用。捆绑的物理设备可以相互备份，一个物理设备失效，其它物理设备可接替它的工作。

配置 SIS 安全隔离网闸的过程中，必须首先配置网络设备，再配置 SIS 安全隔离网闸安全策略。如果网络设备的配置发生了改变，建议对相关的安全策略也进行调整。

4.1.1 物理设备

物理设备初始情况下工作在路由模式，也就是说该设备上绑定有 IP 地址，可以与其它设备进行数据包的路由转发。其中第二个物理设备 **fe2** 是默认的可管理设备。它的默认 IP 地址是 10.0.0.1，子网掩码为 255.255.255.0，这个地址允许管理，PING 和 TRACEROUTE（默认管理主机的 IP 地址是 10.0.0.200，请参考系统配置>>管理配置>>管理主机）。

物理设备是其他设备的基础。在 WEB 配置管理界面和 CLI 配置管理界面上可配置的物理设备是在系统启动时能够检测到的设备，如果系统启动时，检测不到相应的设备，那么这个设备在界面上就不会显示。

表 4 1 物理设备上可配置的属性

属性名称	描述
名称	设备名称，不能修改
MAC 地址	设备的 MAC 地址，可以修改。如果忘记了设备最初的 MAC 地址，可以将 MAC 地址置为空值并重启 SIS 安全隔离网闸，SIS 安全隔离网闸会自动探测出设备的 MAC 地址。
链路工作模式	设备的链路工作模式，有以下三种 1：自适应 2：全双工

	3：半双工
链路速度	设备的链路速度，有以下三种 1：10 2：100 3：1000
MTU	设备的 MTU（最大传输单位）。百兆网络设备可设置的范围是 68 到 1504，千兆网络设备可设置的范围是 64 到 16128。
工作模式	设备的工作模式，目前可以为：路由模式、冗余模式。在路由模式下，必须配置设备的 IP 地址。
IP 地址获取	IP 地址的获取方式，目前支持的有以下两种 1：静态指定 2：通过 DHCP 获取，即防火墙相应物理设备作为 DHCP 客户端获得 IP 地址。
IP 地址	IP 地址配置只在 IP 地址获取方式为静态指定时可配置
掩码	掩码只在 IP 地址获取方式为静态指定时可配置
开启 IPMAC 地址绑定	是否开启此设备上的 IPMAC 地址绑定检查功能
允许未绑定的 IPMAC 地址通过	未绑定的 IP 地址是否允许通过
开启 IP 地址欺骗检查	开启此设备上的 IP 地址欺骗检查
用于管理	此设备的 IP 地址是否能用于管理。设备 fe2 默认选中，且不能修改。
允许 PING	此设备的 IP 地址是否允许被 PING 到
允许 TRACEROUTE	此设备的 IP 地址是否允许被 TRACEROUTE 到
是否启用	是否启用此设备

图 4 1 物理设备列表

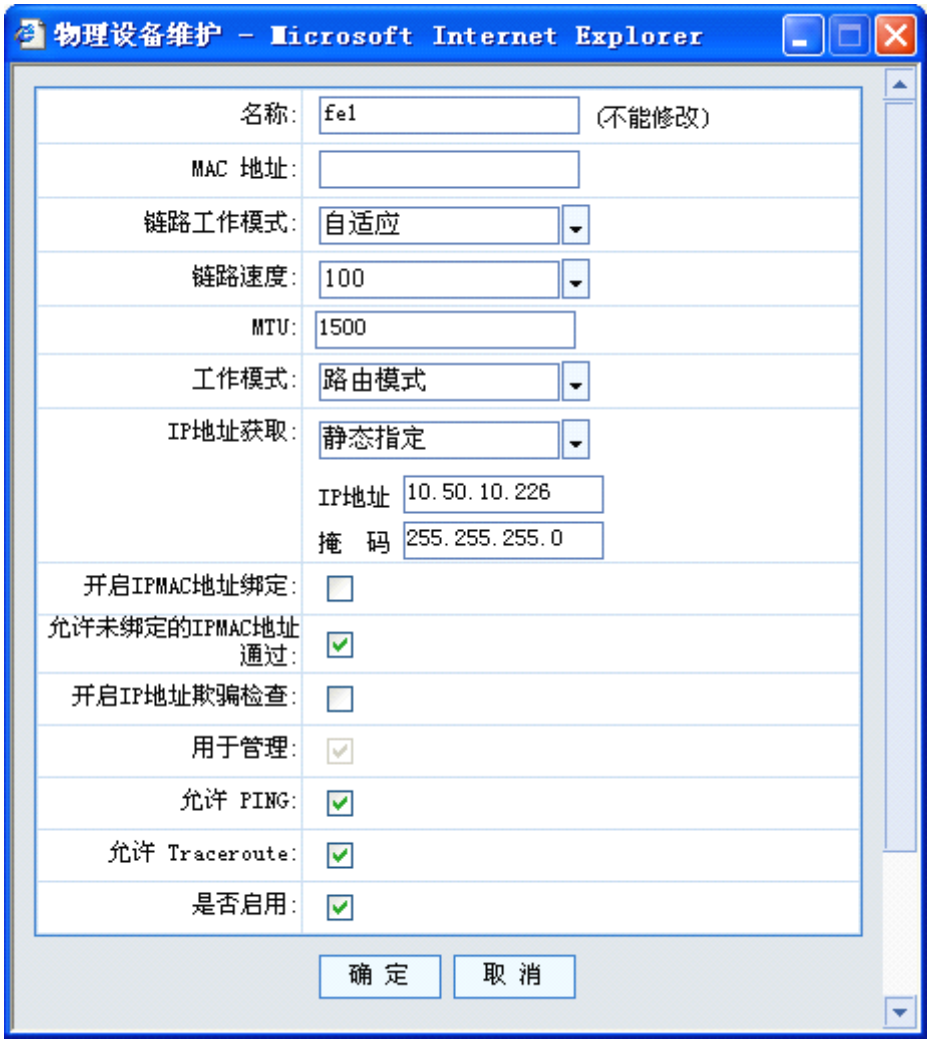


图 4 2 物理设备可配置的属性

4.1.2 别名设备

别名设备的作用是给物理设备配置多个 IP 地址。每个物理设备可以关联的别名设备是 253 个，这些 IP 具有“用于管理”，“允许 PING”，“允许 TRACEROUTE”等属性。同时要注意的是别名设备的 IP 地址不能重复。

表 4 2 别名设备可配置的属性

属性名称	描述
绑定设备名称	绑定设备的名称，可选的绑定设备只能为已启用的工作在路由模式下的物理设备
别名 ID	别名设备的别名 ID，允许值是 0－252
IP 地址	别名设备必须配置 IP 地址
掩码	别名设备必须配置掩码
用于管理	设备的 IP 地址是否能用于管理
允许 PING	是否允许 PING 设备的 IP
允许 TRACEROUTE	是否允许 TRACEROUTE 设备的 IP
是否启用	是否启用设备

图 4 3 别名设备列表

图 4 4 别名设备可配置的属性

注意：别名设备的总数不能超过 1024 个。

4.1.3 冗余设备

通过将几个物理设备捆绑在一起组成一个虚拟的冗余设备。冗余设备的作用有：

- 提高链路可靠性。冗余设备捆绑的物理设备相互动态备份，一个成员设备的链路中断（网口掉线），其它成员设备可以迅速接替它的工作，与生成树（STP）不同，对冗余设备之外是不可见，即成员之间的备份只限制所属冗余设备内部，对其它冗余设备无效。
- 增加防火墙带宽。冗余设备的使用可以提供一个经济有效的提高防火墙带宽的方法。通过捆绑多个物理设备，可以使防火墙提供更大的带宽，冗余设备的带宽理论上等于绑定的物理设备的带宽之和。冗余设备按照均衡算法将流量分配给绑定的物理设备，实现链路级的负载均衡。

冗余设备的高级设置可以设置冗余设备工作的模式，修改工作模式需要保存并重启防火墙才能生效。

- 轮循方式：冗余设备在绑定设备中采用轮循方式发送数据包
- 热备方式：冗余设备只有一个物理设备转发数据包，其它设备处于备份状态。
- 802.3ad 方式：冗余设备在绑定设备中采用 802.3ad 协议的方式接收发送数据包。

表 4 3 冗余设备可配置的属性

属性名称	描述
名称	冗余设备名称，不能修改
工作模式	设备的工作模式，目前支持只支持路由模式。在路由模式下，必须配置设备的 IP 地址。
IP 地址获取	IP 地址的获取方式，目前支持的有以下两种 1：静态指定 2：通过 DHCP 获取，即防火墙相应物理设备作为 DHCP 客户端获得 IP 地址。
IP 地址	IP 地址配置只在 IP 地址获取方式为静态指定时可配置
掩码	掩码只在 IP 地址获取方式为静态指定时可配置
开启 IPMAC 地址绑定	是否开启此设备上的 IPMAC 地址绑定检查功能
允许未绑定的 IPMAC 地址通过	未绑定的 IP 地址是否允许通过
开启 IP 地址欺骗检查	开启此设备上的 IP 地址欺骗检查
绑定设备选择	供冗余设备捆绑的物理设备（选择了冗余模式的物理设备），冗余设备至少有一个绑定设备
允许 PING	此设备的 IP 地址是否允许被 PING 到
允许 TRACEROUTE	此设备的 IP 地址是否允许被 TRACEROUTE 到
是否启用	是否启用此设备

图 4 5 冗余设备列表

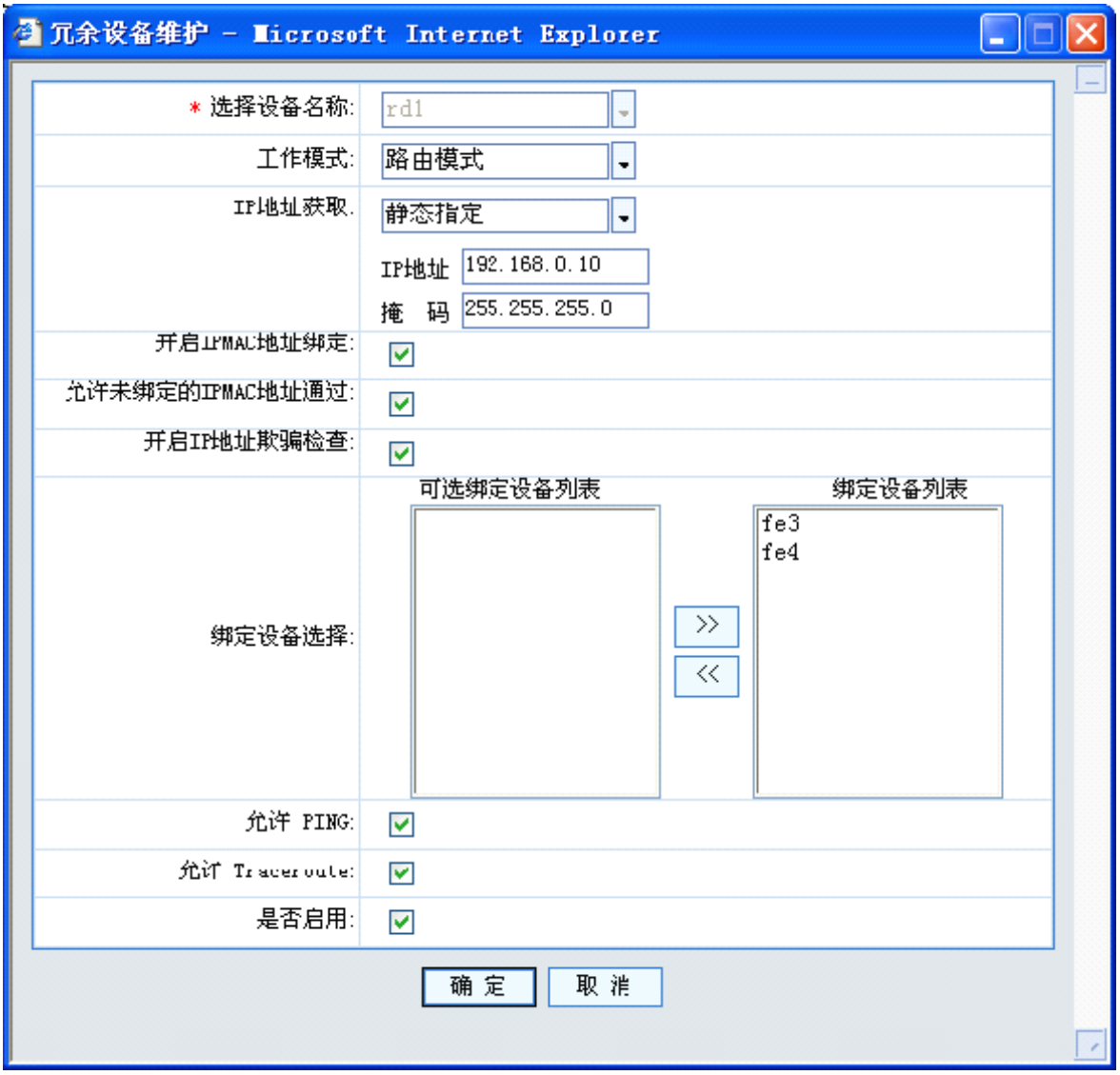


图 4 6 冗余设备属性配置

4.2 域名服务器

如果管理员设置了邮件代理等服务，则需要配置 SIS 安全隔离网闸的域名服务器，用于 SIS 安全隔离网闸自身向外发数据包时的域名解析。例如 SIS 安全隔离网闸如果需要配置动态域名，也必须设定此处的域名服务器。

图 4 7 域名服务器配置

此界面完成配置 SIS 安全隔离网闸的域名服务器的功能，可以配置域名服务器 1 和域名服务器 2，其中域名服务器 1 具有较高的优先级。点“确定”按钮完成配置。

4.3 静态路由

网御 SIS 安全隔离网闸提供静态路由功能。

SIS 安全隔离网闸静态路由支持按目的地址的路由，即按数据包中的目的 IP 地址来决定下一跳地址。修改网络设备的 IP 地址可能会影响到相应的路由规则。建议首先配置网络设备的地址，再配置路由规则。

管理员可以添加，编辑，删除，启用或者禁用静态路由规则。静态路由规则的参数包括目的地址、掩码、下一跳地址和网络接口。下一跳地址应该和相应的网络接口在同一网段内。

注意：特别指出的是，“网络接口”不能为已配置成虚拟地址的别名设备，否则该路由失效。

图 4 8 静态路由的显示

此界面可以完成以下功能：

1. 添加静态路由
2. 编辑静态路由
3. 删除静态路由
4. 启用/禁用静态路由规则

添加静态路由

1. 点“添加”按钮，进入“静态路由维护”
2. 添加静态路由参数
3. 点“确定”按钮完成添加

编辑静态路由

1. 点“操作”一栏中的“编辑”图标，打开“静态路由维护”界面
2. 执行修改操作
3. 点击“确定”按钮完成修改

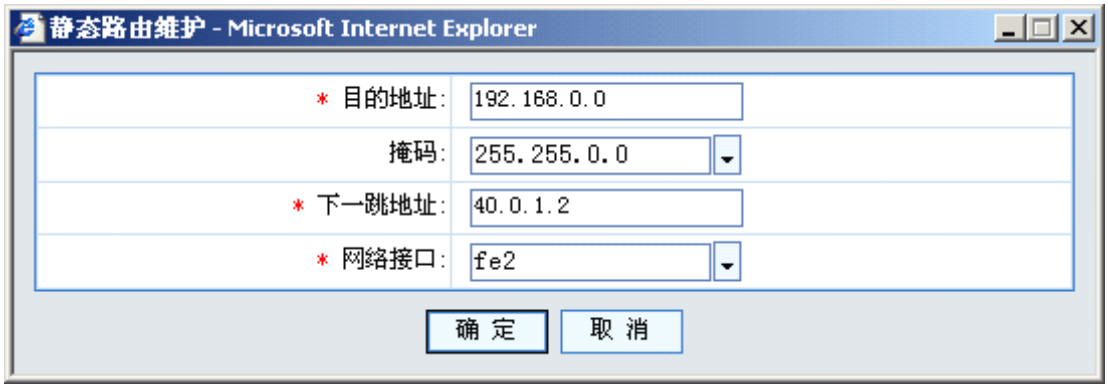


图 4 9 静态路由的维护

表 4 4 添加和编辑时参数说明

参数名称	说明	和其他界面的关系
目的地址和掩码	设置目的 IP 地址，可以设置 IP 地址/子网掩码	
下一跳地址	设置网关的 IP 地址	
网络接口	接口和下一跳地址须在同一网段内	从网络配置>>网络设备中选取接口

删除静态路由

1. 点“操作”一栏中的 “删除”图标，弹出删除对话框
2. 点击“确定”按钮完成删除

启用/禁用静态路由规则

点“是否启用”一栏中的图标，如果原来是✔，点击后变成✘，表示由启用状态变成禁用，如果原来是✘，点击后变成✔，表示由禁用状态变成启用。

4.4 高可靠性设置

本模块用于双机热备和动态负载均衡配置。出于对网络应用的稳定性考虑，用户可以配置两台 SIS 安全隔离网闸，分别作为主机和备份机，当主机断电或无法正常工作的情况下，备份机可自动代替主机的部分功能。

目前双机热备功能可支持以下模块：文件交换、安全浏览、邮件访问、FTP 访问、数据库访问、定制模块、入侵检测。

本模块主要包括：基本配置、虚拟地址管理、负载均衡三个配置项。双机热备功能在系统的客户端一侧的主机和备份机分别进行配置。当用户的网络流量过大时，可以考虑使用多台 SIS 安全隔离网闸进行负载均衡，将流量均分到每一台 SIS 安全隔离网闸。负载均衡功能目前支持如下模块：安全浏览、邮件访问、FTP 访问、数据库访问，以及定制访问和入侵检测。

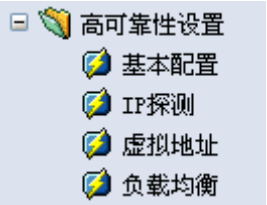


图 4 10 高可靠性配置 WEB 界面导航菜单

4.4.1 基本配置

该部分显示本机的主机名称、工作角色和当前服务状态。对本机的工作角色以及对端主机名称进行设置。控制服务启停。WEB 界面示意图如下：

图 4 11 基本配置界面

参数说明如下表：

表 4 5 基本配置参数说明

参数名称	描述
工作角色	设置本地主机的工作角色，本地主机作为主闸或本机作为从闸
本地主机名	显示本机的主机名称
对端主机名	设置对端主机的主机名称
当前服务状态	显示服务当前的运行状态，启动或停止
当前工作角色	显示当前本机的工作角色，有“本机作为主闸”、“本机作为从闸”和“正在协商中…”三种状态。当服务停止时无显示内容

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

4.4.2 IP 探测

Ip 探测用于探测与网闸相连交换机的状态，弱交换机异常，网闸会执行相应的切换动作。WEB 界面示意图如下：

图 4 12 IP 探测列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

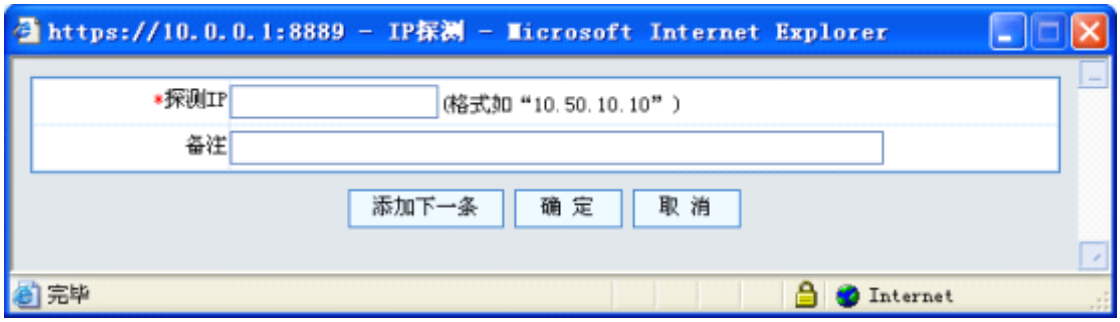


图 4 13 添加 IP 探测地址

图中虚拟地址的配置项，说明如下：

◆ **探测 IP**

与网闸相连主机的 ip 地址

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个虚拟地址后面的编辑图标，弹出编辑窗口，如下图：

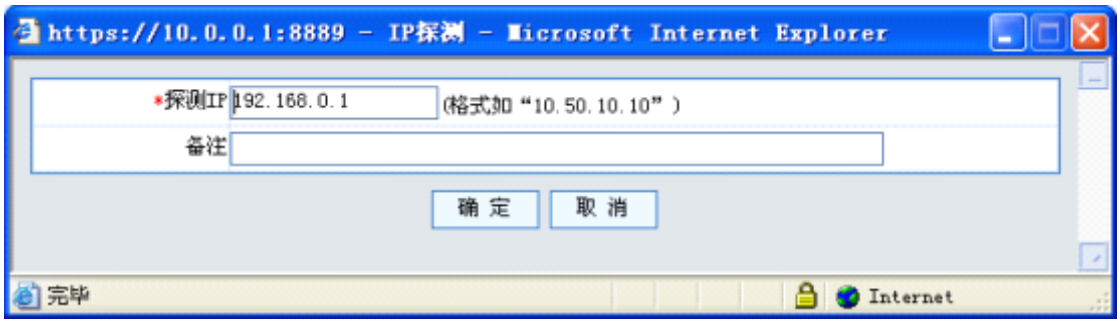


图 4 14 编辑探测 IP 地址

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个探测 IP 后面的删除图标，弹出编辑窗口，如下图：

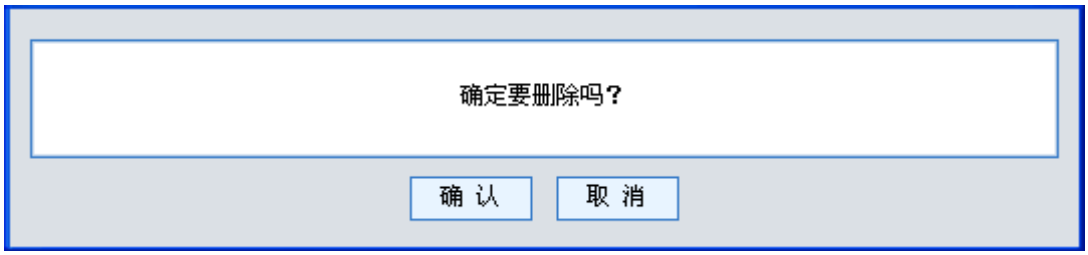


图 4 15 删除探测 IP 地址

点击“确认”按钮，删除该探测 IP 地址；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

4.4.3 虚拟地址

虚拟地址用于两个方面：一是用于配置双机热备，二是供负载均衡任务引用。WEB 界面示意图如下：

图 4 16 虚拟地址列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

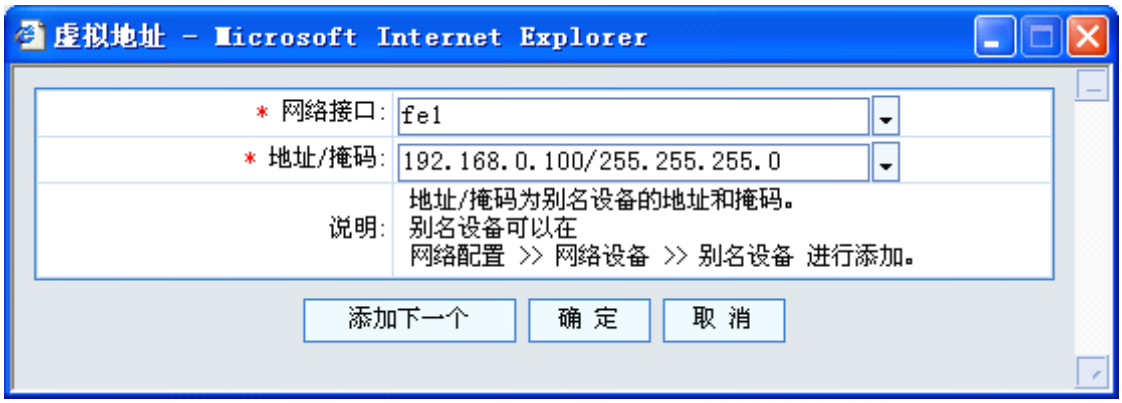


图 4 17 添加虚拟地址

图中虚拟地址的配置项，说明如下：

◆ **网络接口**

网络接口名称，必须从已启用的物理接口中选择。

要启用物理接口请在 网络配置 >> 网络接口 >> 物理设备 处进行修改。

注意：工作在冗余模式下的物理接口不会出现在列表中。

◆ **地址/掩码**

别名设备的地址/掩码，必须从已选定的物理设备对应的别名设备中选择。其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项。

该配置项必填。

要添加新的别名设备请在 网络配置 >> 网络接口 >> 别名设备 处进行添加。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个虚拟地址后面的编辑图标，弹出编辑窗口，如下图：

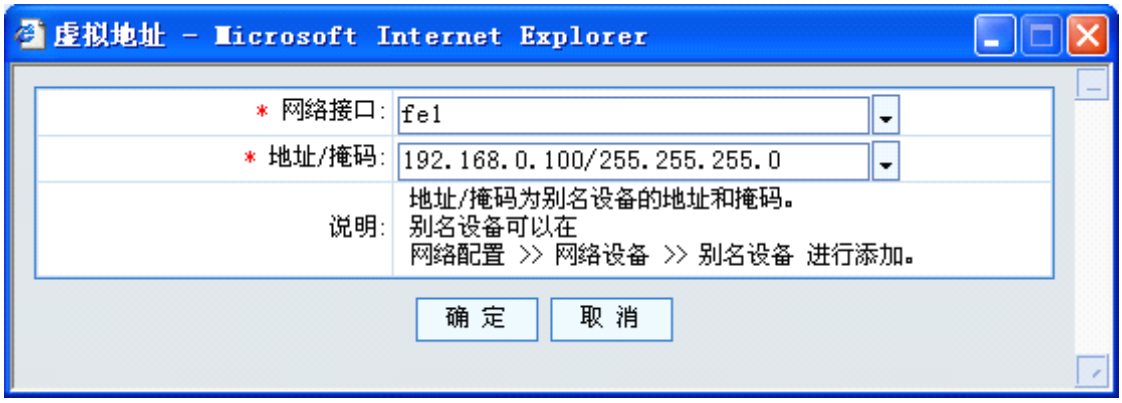


图 4 18 编辑虚拟地址

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个虚拟地址后面的删除图标，弹出编辑窗口，如下图：

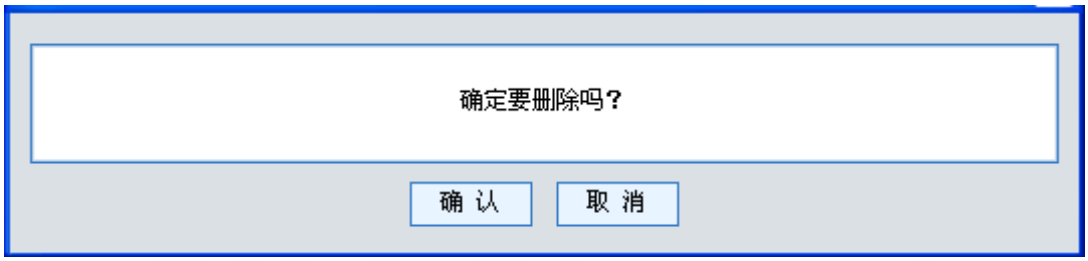


图 4 19 删除虚拟地址

点击“确认”按钮，删除该虚拟地址；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

注意：当虚拟地址被负载均衡设置使用时，无法删除。请先删除使用该虚拟地址的负载均衡设置。有关负载均衡的说明请参见下一节“负载均衡”。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

特别指出：

1. 配置好虚拟地址并且在基本配置中设置好后，启动服务即可实现双机热备功能。在主闸和从闸上需配置相同的虚拟地址，该地址即为网闸对外表现的地址。
2. 若配置了负载均衡功能后，此时网闸实现负载均衡功能；若把负载均衡功能删除而不删除虚拟地址规则，网闸实现双机热备功能。

4.4.4 负载均衡

该模块用于配置负载均衡任务。配置时在系统客户端一侧的主机进行配置。WEB 界面示意图如下：

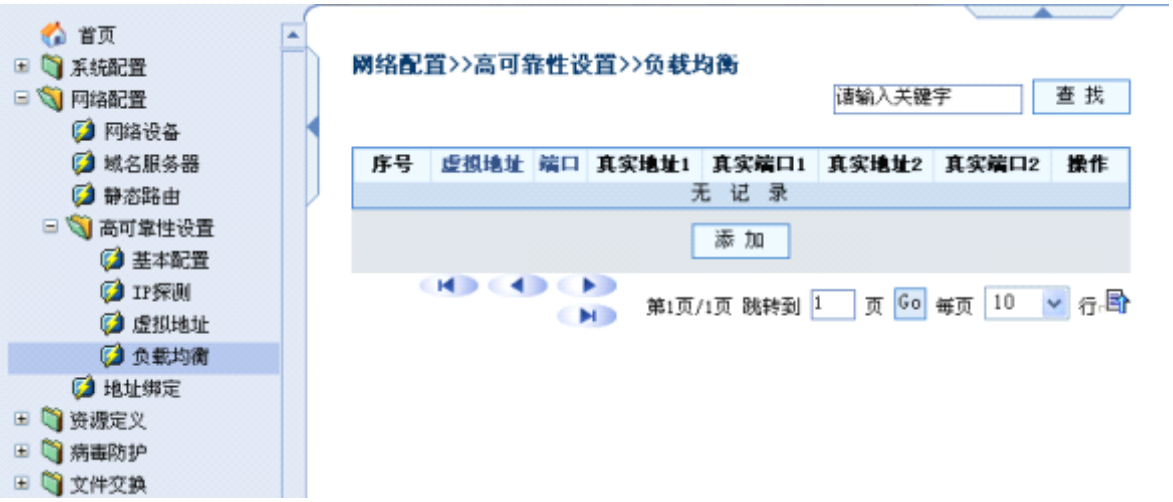


图 4 20 负载均衡配置列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

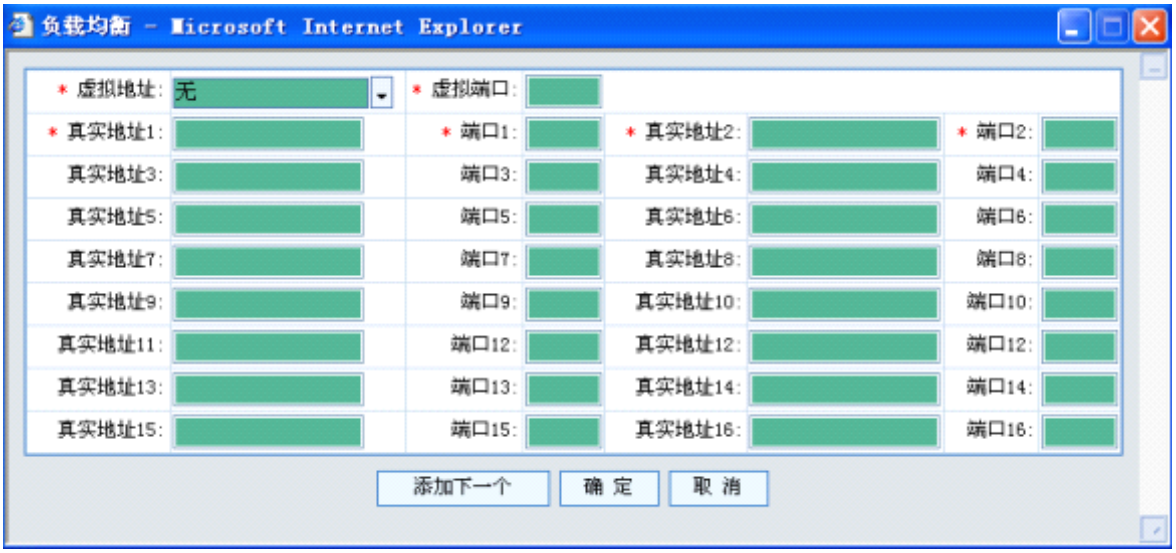


图 4 21 添加负载均衡配置

图中负载均衡的配置项，说明如下：

◆ **虚拟地址**

该虚拟地址用于向客户端提供相应的服务，且必须为客户端用户能访问到的 IP 地址，否则导致网络无法连接。该地址必须为网闸设备上各物理设备的别名设备 IP 地址，可以从已添加的虚拟地址中选择。虚拟地址可以在 高可靠性设置 >> 虚拟地址 处进行添加。具体操作可参照上一节“虚拟地址”。

◆ **端口**

虚拟地址对应的端口，用于向客户端用户提供服务的端口。

◆ **真实地址 1**

网络中实际进行转发数据包的网络接口地址，亦实际网络设备 1 的用于负载均衡的 IP 地址。该 IP 地址错误或不可达，将导致该链路无法进行负载均衡。

◆ **真实端口 1**

真实地址 1 用于提供服务的端口。若该端口与真实地址 1 上相应服务的使用端口不一致，将导致该链路无法进行负载均衡。

◆ **真实地址 2**

网络中实际进行转发数据包的网络接口地址，亦实际网络设备 2 的用于负载均衡的 IP 地址。该 IP 地址错误或不可达，将导致该链路无法进行负载均衡。

◆ **真实端口 2**

真实地址 2 用于提供服务的端口。若该端口与真实地址 2 上相应服务的使用端口不一致，将导致该链路无法进行负载均衡。

注意：负载均衡功能至少需要两台设备，最多可以支持 16 台设备。

设置完各配置项后，点击“添加下一条”，继续添加设置；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

特别指出：目前负载均衡只支持普通访问类型。

2) 修改操作

在列表显示图中，点击列表中每个负载均衡设置后面的编辑图标，弹出编辑窗口，如下图：

图 4 22 编辑负载均衡配置

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个负载均衡设置后面的删除图标，弹出编辑窗口，如下图：

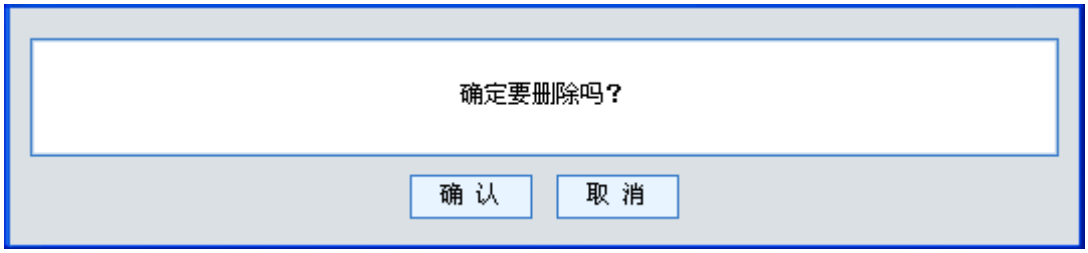


图 4 23 删除负载均衡配置

点击“确认”按钮，删除该项设置；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

4.5 地址绑定

IP/MAC 地址绑定用于解决网络管理中 IP 地址盗用的现象。

如果“网络配置>>地址绑定”中的 IP/MAC 检查启用，当 SIS 安全隔离网闸接收数据包时，

将根据数据包中的源 IP 地址与源 MAC 地址，检查管理员设置好的 IP/MAC 地址绑定表。如果地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按在“网络配置>>网络设备>>物理设备”中的编辑对话框中是否选中“允许未绑定 IP/MAC 对的包通过”的设置处理。

图 4 24 地址绑定配置

“网络配置>>地址绑定”可以完成以下功能：

- 探测 IP/MAC 地址对。其中，探测方式有两种：
  （1） 按网口探测
  （2） 按 IP 探测
- 绑定 IP/MAC 地址对。其中，绑定方式有两种：
  （1） 探测 IP/MAC 地址对后选择并绑定
  （2） 手工输入 IP 与 MAC 对。

探测 IP/MAC 地址对

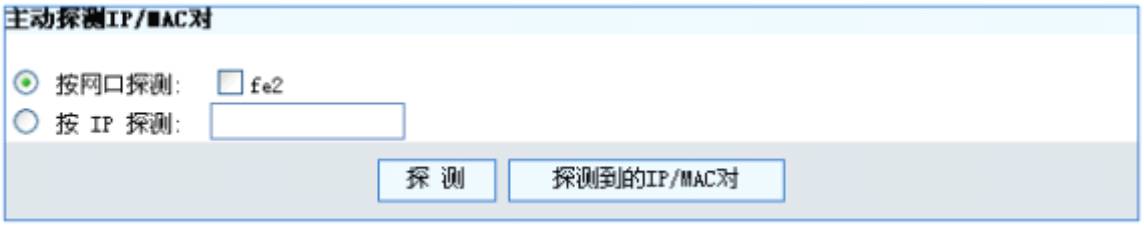


图 4 25 IP/MAC 地址探测

表 4 6 IP/MAC 地址探测项说明

参数名称	说明
按网口探测	IP/MAC 地址探测方式。
fe2 等网口	当前已激活的网口列表 管理员根据需求指定要做 IP/MAC 探测的网口，可以多选
按 IP 探测	IP/MAC 地址探测方式
输入框	输入 IP 地址或网段
探测	点击后，对指定网口进行 IP/MAC 地址对的探测 探测完成时，指定网口前的选择中符号消失，管理员可以点击“探测到的 IP/MAC 对”进行查看。
探测到的 IP/MAC 对	点击后，显示当前探测到的 IP，MAC 和网口的列表。

按网口探测 IP/MAC 地址对的操作步骤：

1. 点击“网络配置>>地址绑定”菜单，弹出“网络配置>>地址绑定”界面。
2. 选择“按网口探测”，可以指定要做 IP/MAC 探测的网口（可以多选）。
3. 点击“探测”，系统对指定网络设备进行 IP/MAC 地址对的探测。界面将提示“正在探测，请稍候…”，根据应用环境的不同，可能需要几十秒钟的时间。
4. 当出现提示“探测完毕，请点击按钮<探测到的 IP/MAC 对>查看探测结果。”点击“确定”后，点击“探测到的 IP/MAC 对”，
5. 弹出”探测到的 IP/MAC 地址对”界面，显示在指定网口当前探测到的 IP、MAC、网口，管理员可以根据探测到的 IP/MAC 地址对，完成绑定功能。详见“探测到的 IP/MAC 对” 界面的操作说明。

按 IP 探测 IP/MAC 地址对的操作步骤：

1. 点击“网络配置>>地址绑定”菜单，弹出“网络配置>>地址绑定”界面
2. 选择“按 IP 探测”，在输入框中输入待探测的主机 IP 地址。
3. 点击“探测”，系统对指定网络设备进行 IP/MAC 地址对的探测。界面将提示“正在探测，请稍候…”，根据应用环境的不同，可能需要几十秒钟的时间。
4. 当出现提示“探测完毕，请点击按钮<探测到的 IP/MAC 对>查看探测结果。”点击“确定”后，点击“探测到的 IP/MAC 对”，
5. 弹出“探测到的 IP/MAC 地址对”界面，显示在指定网口当前探测到的 IP、MAC、网口，管理员可以根据探测到的 IP/MAC 地址对，完成绑定功能。详见“探测到的 IP/MAC 对” 界面的操作说明。

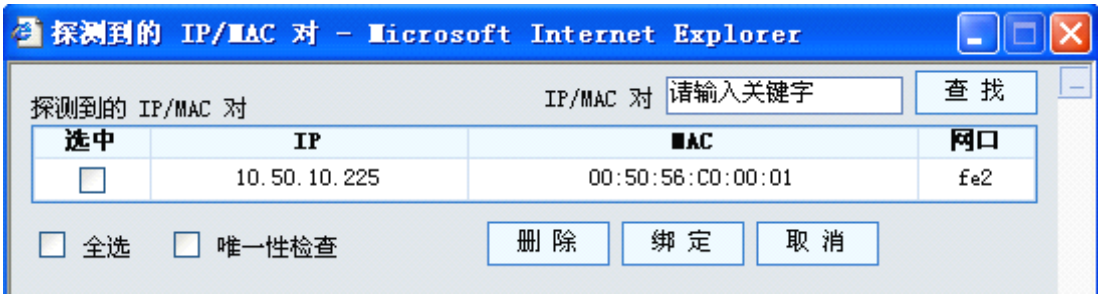


图 4 26 探测到的 IP/MAC 对显示

表 4 7 绑定 IP/MAC 对配置项说明

配置项名称	说明
IP/MAC 对	输入要查找的 IP/MAC 对
查找	点击后，在该界面列表项中查找指定的地址对
选中	选中该 IP/MAC 对，可以根据选择进行删除或绑定操作
IP 地址	探测到的 IP 地址，不能是组播地址
MAC 地址	探测到的 MAC 地址，不能是组播地址
网口	IP/MAC 对是该网口探测到的
全选	全部选中探测到的 IP/MAC 对，可以根据选择进行删除或绑定操作
唯一性检查	当用户选择“唯一性检查”时，IP 与 MAC 建立一一对应，不选择“唯一性检查”时，一个 MAC 可以绑定多个 IP. 如果地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按缺省策略（允许或禁止）执行。
删除	从当前列表中删除选中的 IP/MAC 地址对
绑定	将选中列表项中的 IP/MAC/网口进行绑定，绑定成功后的 IP/MAC 对将显示在已绑定 IP/MAC 对的列表中
取消	取消本次操作

探测到的 IP/MAC 对界面操作说明：

1. 管理员可以根据情况选中相应地址对表项，也可以点击“全选”选中所有地址对表项。
2. 选择唯一性检查时，选中的地址对表项都进行唯一性检查。
3. 针对选中的地址对表项，点击删除，则地址对从当前的列表中清除；点击绑定，则地址对完成绑定功能，绑定成功后界面关闭。

二、绑定 IP/MAC 地址对

图 4 27 绑定 IP/MAC 对配置

图 4 28 添加地址绑定

表 4 8 添加地址绑定项说明

参数名称	说明
IP 地址	要绑定的 IP 地址
MAC 地址	要绑定的 IP 地址，不能是组播地址。
唯一性检查	当用户选择“唯一性检查”时，IP 与 MAC 建立一一对应，不选择“唯一性检查”时，一个 MAC 可以绑定多个 IP. 如果在地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按缺省策略（允许或禁止）执行。

手工添加 IP/MAC 地址对绑定规则的操作流程：

1. 点击“网络配置>>地址绑定”菜单，弹出“网络配置>>地址绑定”界面
2. 在已绑定 IP/MAC 地址对栏中，点击“添加”，弹出“地址绑定维护”界面
3. 在该界面添加已知的需要进行绑定的 IP/MAC 地址对，点击“确定”，则添加本条规则成功后关闭本窗口；如果点击“添加下一条”，则添加本条规则成功后窗口仍旧打开，可以继续添加下一条规则。

手工删除 IP/MAC 地址对的操作流程：

1. 点击“网络配置>>地址绑定”菜单，弹出“网络配置>>地址绑定”界面
2. 在已绑定 IP/MAC 地址对栏中，选择删除，弹出删除确认界面
3. 可以选择删除当前纪录、全部记录，还可以选择删除地址段内的绑定对。

图 4 29 删除 IP/MAC 地址对

第 5 章　资源定义

为了简化 SIS 安全隔离网闸安全规则的配置和维护工作，引入了资源定义。网御 SIS 安全隔离网闸系统可以定义以下资源：

- 地址：地址、地址组、服务器地址、域名地址等
- 时间：时间（包括一次性调度和周循环调度）、时间组等

5.1 地址

在定义各种访问任务之前，一般需要按照特定的原则（比如：按部门、按人员等）定义地址资源，这样制定的访问任务比较容易阅读和理解。当部门或者人员的 IP 地址发生变化时，只需在本列表中更新即可，无需再更改访问任务。

注意：添加地址资源时最好不要超过 512 条，否则对系统性能影响较大。

5.1.1　地址列表

图 5　1　地址列表

地址列表可以被 FTP 访问、邮件访问、数据库访问、安全浏览、定制访问等模块的访问任务引用，还可以被地址组对象引用。

地址列表可以按三种方式来定义地址：

（1）　IP 地址/掩码

（2）　反 IP 地址/掩码

（3）　地址范围 IP1 － IP2。

注意：在修改地址资源时，不能修改地址的类型。

如下图所示：

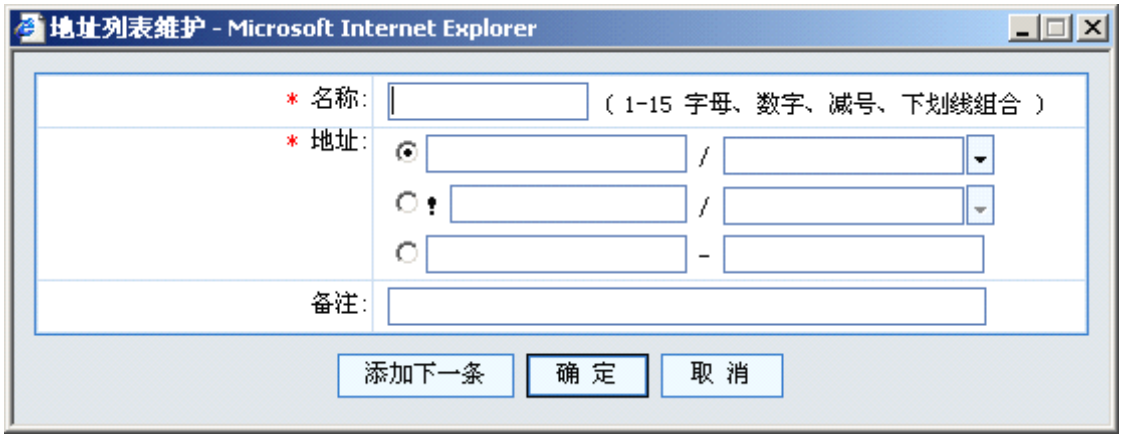


图 5 2 地址列表维护

表 5 1 地址类型列表

值域	说明
IP/MASK 地址	用 IP 和掩码表示一个网段 自动用 IP 和掩码进行运算，添加成功的为一个网段。例如：输入 192.168.25.22/255.255.255.0 ，则添加成功后变为 192.158.25.0/255.255.255.0。 如果希望指定一台主机，请选择掩码为 255.255.255.255
反 IP/MASK 地址	定义 IP 和掩码表示的网段之外的所有地址
IP1-IP2 地址段	IP1 必须小于或等于 IP2 如果只指定一台主机，可以让 IP1 和 IP2 相等

注意：可以定义 A 类、B 类和 C 类地址。

5.1.2 地址组

图 5 3 地址组列表

地址组可以被 FTP 访问、邮件访问、数据库访问、安全浏览、定制访问等模块的访问任务引用。

地址组的成员只能为“资源定义>>地址>>地址列表”中已经定义过的地址。

在“资源定义>>地址>>地址组”，点击 ，将弹出以下界面：

图 5 4 地址组添加

表 5 2 地址组添加元素表

值域	说明
地址列表	列出所有在“资源定义>>地址>>地址列表”中定义的地址，“服务器地址”不能作为地址组的成员。 属于地址的成员将被移动到成员列表中，不再显示于本列表中。
地址组成员	该地址组的所有成员，成员只能是在“资源定义>>地址>>地址列表”中定义的地址。 地址组至少要有一个成员。

操作	说明
	添加成员，点击 把选中的地址移动到成员列表
	删除成员，点击 把选中的成员移动到地址列表中

5.1.3 域名地址

“域名地址”可用于配置各模块访问任务中的源地址和目的地址。

图 5 5 域名地址列表

注：图标代表刷新域名地址的自动解析记录。域名地址支持定时自动刷新，也可以在启用“自动解析”的情况下，手工刷新域名地址对应的 IP 地址。

在“资源定义>>地址>>域名地址”，点击 添 加 ，将弹出以下界面：

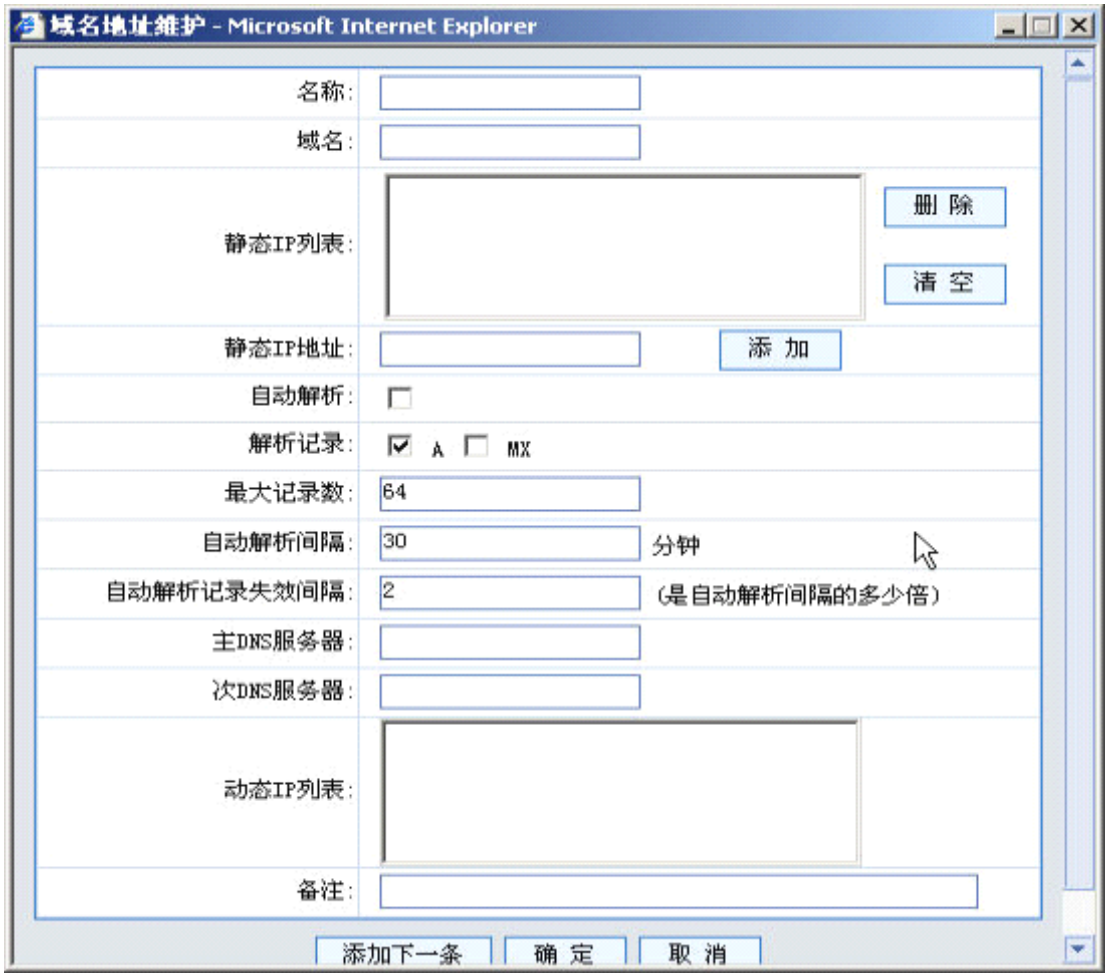


图 5 6 域名地址添加

表 5-3 域名地址参数说明

值域	说明
名称	域名地址资源名称
域名	完整、合法的域名地址，不支持通配符
静态 IP 列表	手动添加的域名地址的 IP 地址列表。选择 IP 地址并点击“删除“，可以将 IP 地址从列表中删除；点击“清空”可以将 IP 列表清空。接着点击“确定”，可以使之生效。
静态 IP 地址	输入 IP 地址，然后点击“添加”，就可以将 IP 地址加入静态 IP 列表，接着点击“确定”，就可以使之生效
最大记录数	一个域名可以对应的静态 IP 地址和动态 IP 地址的最大数目，如果超出这个值，动态解析的 IP 地址会自动删除最旧的地址
自动解析	是否自动解析域名地址对应的 IP 地址，自动解析只有在开启自动解析服务的情况下才有效，如果关闭自动解析服务而开启或关闭自动解析都会出现错误，所以，请在开启自动解析服务时开启自动解析；在关闭所有的自动解析之后关闭自动解析服务
解析记录	自动解析域名地址对应的哪些记录，A 记录（DNS 主机记录），MX 记录（DNS 邮件交换记录）
自动解析间隔	自动解析启用的时间间隔
自动解析记录失效间隔	自动解析的记录多长时间失效，这个值用自动解析间隔的倍数来表示
主 DNS 服务器	主 DNS 服务器
次 DNS 服务器	次 DNS 服务器
动态 IP 列表	自动解析的 IP 地址列表，不能添加和删除
备注	域名地址的说明

5.2 用户

用户认证与各访问类应用模块配合使用，在相应的任务中选择“认证用户组”，则此连接必须需要经过认证，才能被“允许”。

认证服务器在“系统配置>>用户认证服务器”中设置，支持两种认证方式：

1) RADIUS 认证
2) 本地认证

注意：在此“资源定义>>用户”界面中定义的用户和用户组均为本地用户认证库，只能为本地认证使用。

如果使用 RADIUS 认证方式，则用户信息在 RADIUS 认证服务器上进行设置。

如果需要使用用户认证，必须定义用户库。在本地用户认证库中，提供了两种形式：

1) 用户：通常指单个人，如小王、小李。
2) 用户组：通常指有共性的人，比如同一个部门，同一种职位，等等。

注意：

1) 用户组中可以没有任何一个用户：如要成立一个新部门，还没有任何员工；又如，有一种职位，还没有任何员工
2) 同一个用户只能属于一个组。
3) 如果用户属性和组属性发生冲突，以用户属性为准

通常，推荐先定义用户，再定义用户组。

5.2.1 用户列表

图 5 7 用户列表

删除所有用户按钮用来将系统中所有的用户全部删除，同时将所有用户组的用户属性清空。

添加用户界面如下：

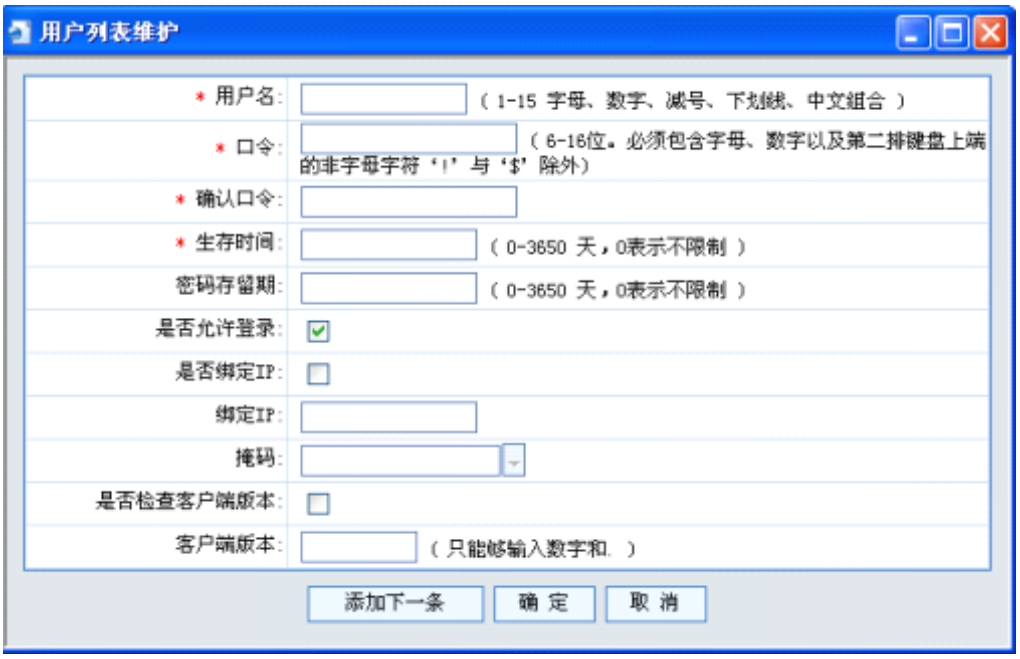


图 5 8 用户添加

表 5 4 用户添加元素列表

值域	说明
用户名	名称必须唯一
口令	该用户用于认证的口令
生存时间	表示该用户从创建时间开始算起，可以有效使用的天数
是否允许登录	是否启用本帐号
是否绑定 IP	用户是否启用绑定 IP 功能
绑定 IP	需要绑定的 IP 地址
掩码	相应的掩码
是否检查客户端版本	是否启用客户端版本检查
客户端版本	客户端所需的最低版本

点击相应的“编辑”按钮，弹出以下界面：

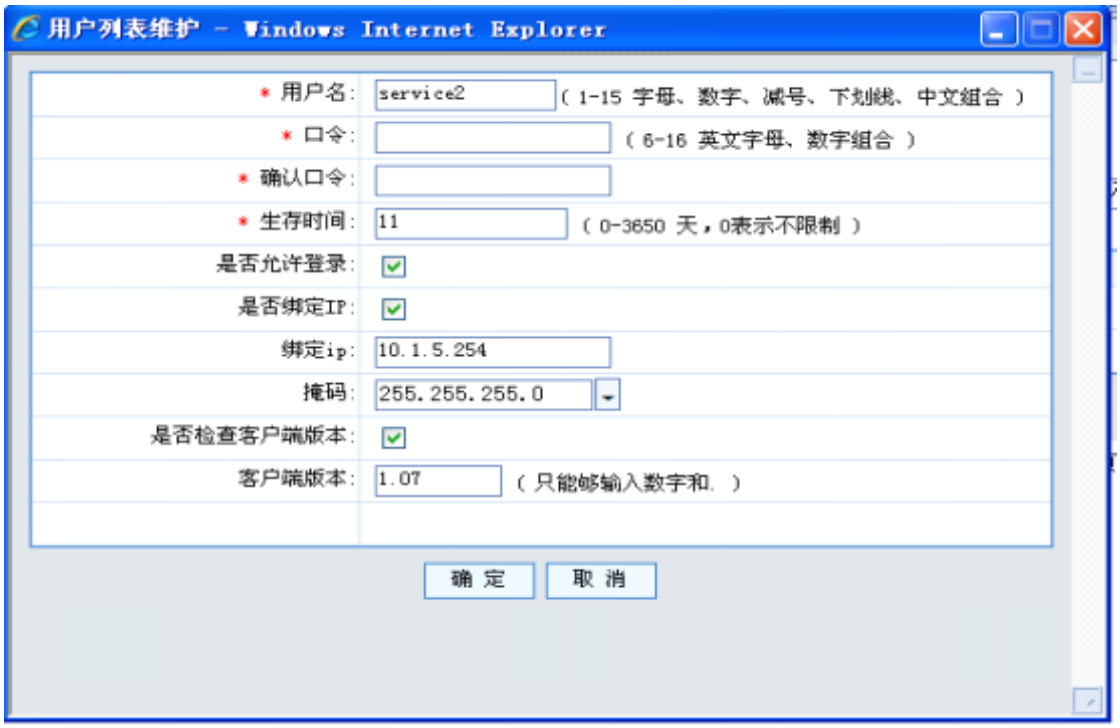


图 5 9 用户维护

编辑用户时，口令域可以不用填，这时候表示不修改该用户的当前密码。

特别指出：

当选择第三方 Radius 认证模式时，用户资源的所有动作均无效，即第三方 Radius 认证模式无需在网闸配置用户。

5.2.2 用户组

图 5 10 用户组列表

图 5 11 用户组维护

表 5 5 用户组维护元素表

值域	说明
名称	名称必须唯一
分配时间	给该用户组中每个用户分配的时间 分配时间使用完毕后用户帐号将无法登录，重置后才能恢复使用 0 表示没有限制
本组用户	左边的列表框列出了在“用户”中定义的所有用户。 右边的列表框列出了属于本组的用户 用户组可以无任何成员
进程检查	提示用户是否启用进程检查功能

	若启用，则必须在右侧添加需要检查的进程的详细信息。 URL 只支持 http、https、ftp 三种协议，且不能够有分号、逗号和加号
进程策略	进程检查失败后，是否允许客户端登陆 当进程检查启用后进程策略才能被操作

特别指出：

在用户认证工作于 Radius 模式下的时候，用户组的修改动作无效，用户组的分配时间和本组用户属性无效。同时，只需配置一个不包括任何用户成员的用户组，但该用户组的名称必须第三方 Radius 认证服务器中配置的用户组名称相同。

5.3 时间

很多访问控制和时间有紧密的关系。比如，上班时间不能上网浏览新闻，但是，下班时间可以。这样，就需要有时间调度策略。在“资源定义>>时间”中，可以定义灵活的时间调度方式。可以按照一次性调度和周循环调度两种方式，来定义时间。还可以把多个时间段组合成时间组。

定义的时间和时间组对象可以被 FTP 访问、邮件访问、数据库访问、安全浏览、定制访问等模块的访问任务引用

5.3.1 时间列表

图 5 12 时间列表

可以按照一次性调度和周循环调度两种方式，来定义时间。如下图所示：

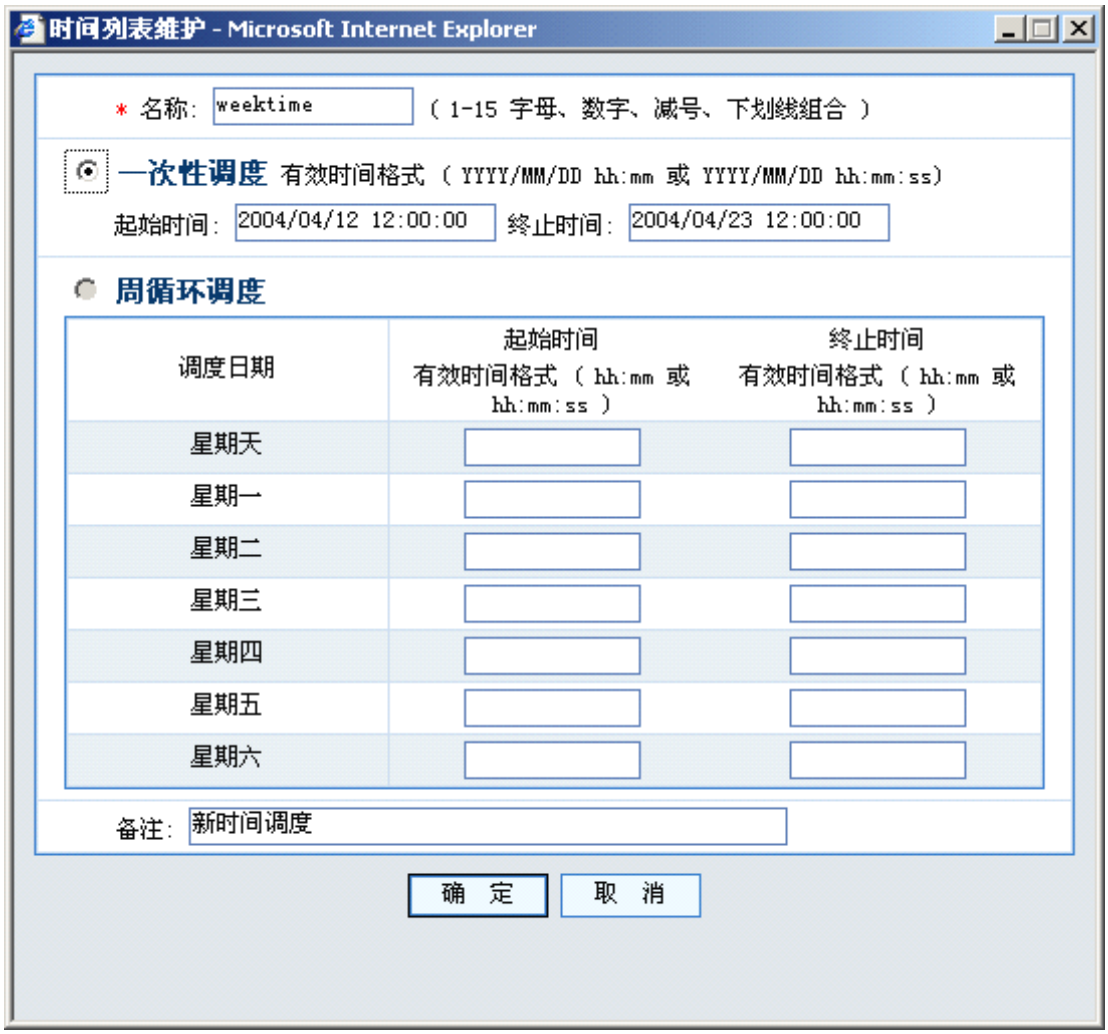


图 5 13 时间资源维护

表 5 6 时间资源维护元素表

值域	说明
一次性调度	指定起始和终止 年月日 时分秒 例如：2004/10/01 00:00:00 至 2004/10/07 23:59:59 为放假时间，禁止所有内部主机访问外部 INTERNET。则可在时间定义中定义一条一次性时间，再在添加任务时生效时段参数引用该时间定义即可。
周循环调度	以一周为循环周期，分别从星期天开始到星期六。每天可以单独指定时间，时间格式为：hh:mm[:ss]。使用方式如同一次性时间。

5.3.2 时间组

图 5 14 时间组列表

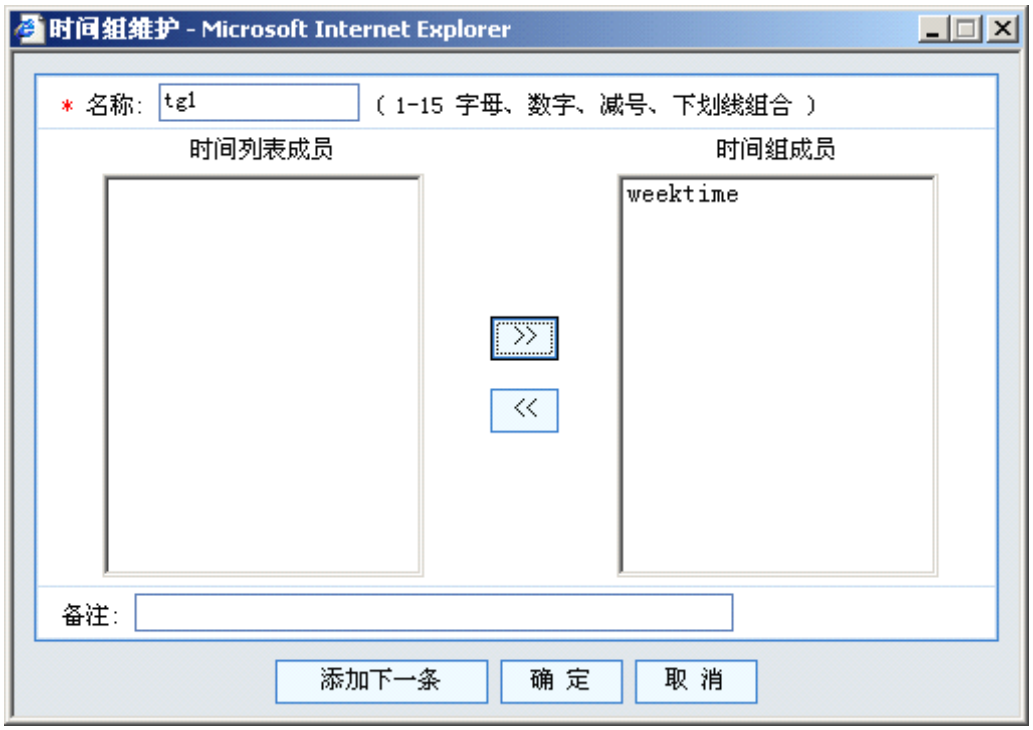


图 5 15 时间组维护

值域	说明
时间列表	列出所有在“资源定义>>时间>>时间列表”中定义的时间。 时间组成员不再显示于本列表中。
时间组成员	该时间组的所有成员。

操作	说明
	添加成员，点击 把选中的时间移动到成员列表
	删除成员，点击 把选中的成员移动到时间列表中

第 6 章 病毒防护

病毒防护功能为各应用模块提供病毒扫描和检测功能。在该模块中，主要包括病毒扫描引擎的启停管理和病毒特征库的升级功能，而是否进行病毒的策略配置则在各应用模块中设置。特别指出，只有开启本模块的病毒扫描引擎，才能让各应用模块中配置病毒扫描策略参数。

病毒扫描策略参数配置详见各应用模块说明，本章重点说明引擎管理、病毒库升级功能的操作说明。WEB 界面导航菜单如下：

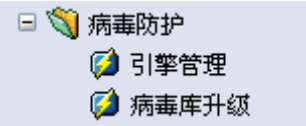


图 6 1 病毒防护 WEB 界面导航菜单

6.1 引擎管理

“引擎管理”部分，用于控制病毒引擎的启停以及显示当前病毒引擎的启停状态。WEB 界面示意图如下：

图 6 2 引擎管理配置界面

参数说明如下表：

表 6 1 引擎管理配置参数说明

参数名称	参数描述
当前服务状态	表示引擎管理任务的系统运行状态。若为“启动”，则表示当前任务已处于运行状态，且在此状态下，任务一旦添加，随即运行；否则，即使添加了任务，系统也不运行。 服务状态值：“启动”或“停止”。

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

6.2 病毒库升级

“病毒库升级”部分，用于配置病毒库升级的基本参数，包括“自动升级”、“手动升级”、“导出升级历史”等参数。WEB 界面示意图如下：

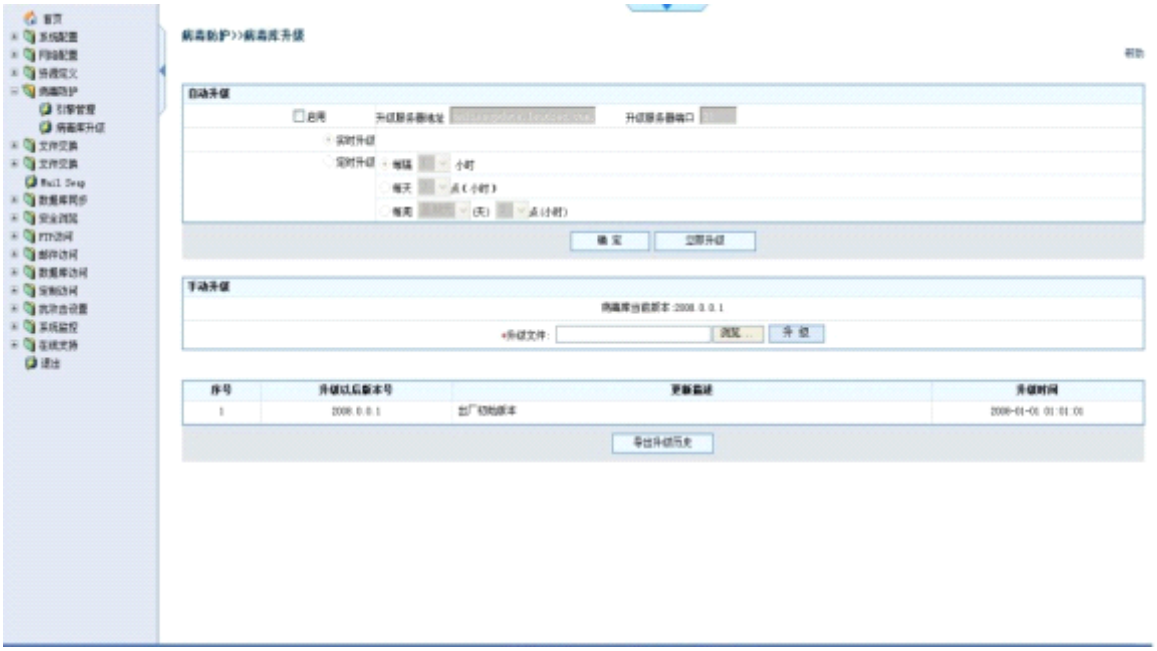


图 6 3 病毒库升级配置界面

一、**自动升级**

该模块用于配置病毒库的自动升级。WEB 界面示意图如下：

图 6 4 病毒库自动升级配置界面

参数说明如下表：

表 6 2 自动升级配置参数说明

参数名称	参数描述
启动	“启动”选项设置是否启动病毒库的自动升级，默认不勾选，此时其他选项全部不可用。
升级服务器地址	当勾选“启动”时，文本框中输入的是自动升级选择的服务器地址，默认为 onlineupdate.leadsec.com.cn。
升级服务器端口	当勾选“启动”时，文本框中输入的是自动升级选择的服务器端口，默认为 21。

实时升级	该选项选择自动升级的模式为实时升级，当用户点击下面的立即升级按钮时会自动连接升级服务器进行病毒库升级。
定时升级	该选项选择自动升级的模式为定时升级，用户可选择三种定时升级模式，当满足用户定制时间要求时，网闸会动连接升级服务器进行病毒库升级。

设置完各配置项后，点击“确定”，保存当前配置，并刷新该界面。

二、**手动升级**

该模块用于配置病毒库的手动升级。WEB 界面示意图如下：

图 6 5 病毒库手动升级配置界面

配置操作步骤为：

1. 点击“浏览”按钮，选择管理主机上的升级包;
2. 点击“升级”按钮，完成病毒库的升级。

三、**导出升级历史**

点击“导出升级历史”按钮，导出升级历史做备份。

第 7 章　文件交换

文件交换模块支持各种类型文件在内、外网之间的安全传输。整个模块由四个部分组成：基本配置、任务管理、内容控制和文件交换任务。在此，主要介绍网闸系统的操作说明。其 WEB 界面导航菜单如下：

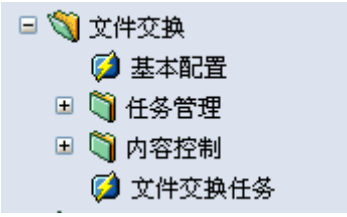


图 7　1　文件交换 WEB 界面导航菜单

7.1 基本配置

“基本配置”部分，主要配置文件交换任务的工作模式、当前服务状态等。WEB 界面示意图如下：

图 7　2　基本配置界面

7.1.1　工作模式

工作模式用于控制网闸提供文件交换服务的工作模式。分为可接收发送，仅接收，仅发送三种工作模式。默认为可接收发送模式。WEB 界面示意图如下：

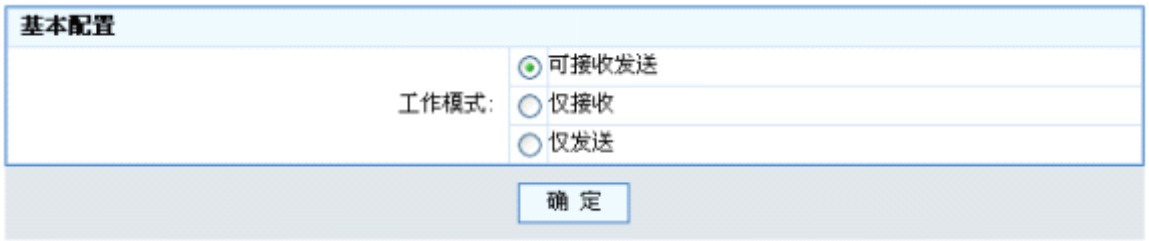


图 7 3 工作模式配置界面

7.1.2 服务管理

服务管理用于控制文件交换服务的运行状态。操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

7.2 任务管理

7.2.1 发送任务

该部分可以对文件交换中的发送任务进行添加、修改和删除等操作。WEB 界面示意图如下：

图 7 4 发送任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

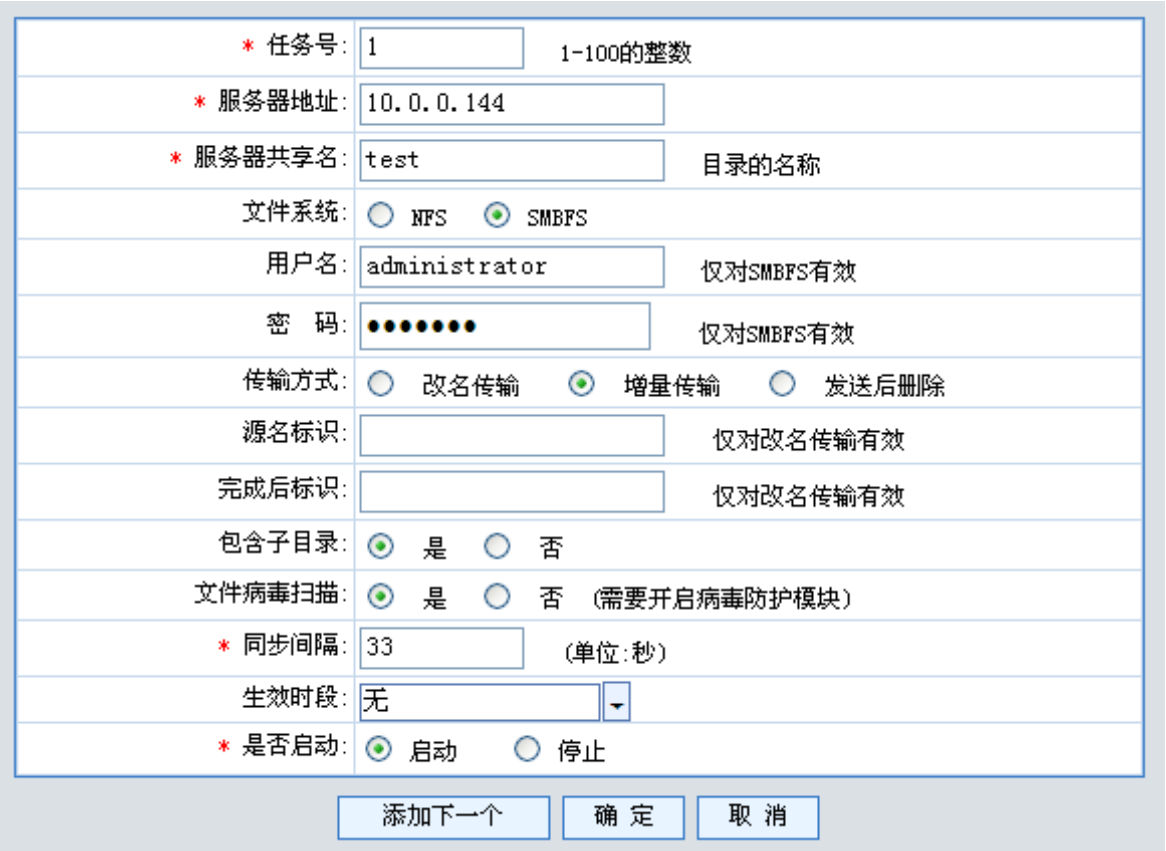


图 7 5 添加发送任务

图中发送任务的配置项，说明如下：

◆ **任务号**

任务号是文件交换的基础，每个发送任务的任务号必须与接收任务相应的任务号一一对应，否则文件无法正常传输。

任务号只用数字表示，最多可以添加 100 个任务。该配置项必填。

◆ **服务器地址**

服务器地址指出网闸访问的共享服务器地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也支持 IP 地址 0.0.0.0。

该配置项为必填项。

◆ **服务器共享名**

服务器共享名为网闸访问的服务器共享文件目录名。注：若所选文件系统为 SMBFS，则服务器共享名不须填写完整路径，只填写共享文件目录名即可。

该配置项为必填项。

◆ **文件系统**

文件系统为网闸访问的服务器主机文件系统类型，分为 NFS 和 SMBFS 两种。默认为 NFS 文件系统。若选择 NFS 文件系统，则不需填写用户名和密码，用户名和密码输入框不可用。若选择 SMBFS 文件系统，则需填写用户名和密码，其中用户名和密码为登陆共享服务器所用的用

户名和密码。WEB 界面示意图如下：

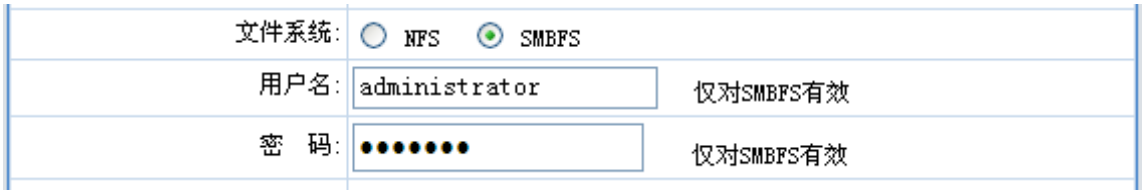


图 7 6 文件系统配置界面

◆ **传输方式**

传输方式为设置共享文件传输的处理动作。分为改名传输，增量传输和传输后删除三种方式。默认为改名传输。三种方式分别介绍如下：

1) 改名传输

仅发送文件名形如"*_源名标记"的文件，发送完成后将文件名修改为"*_完成后标记"。若选择改名传输，则需填写源名标记和完成后标记。

2) 增量传输

首次发送全部共享文件，发送完成后每次同步时检查共享文件有无添加或修改，如有更新，仅发送更新的共享文件。若选择增量传输，则不需填写源名标记和完成后标记。

3) 传输后删除

发送全部共享文件，发送完成后删除共享文件。若选择传输后删除，则不需填写源名标记和完成后标记。

WEB 界面示意图如下：

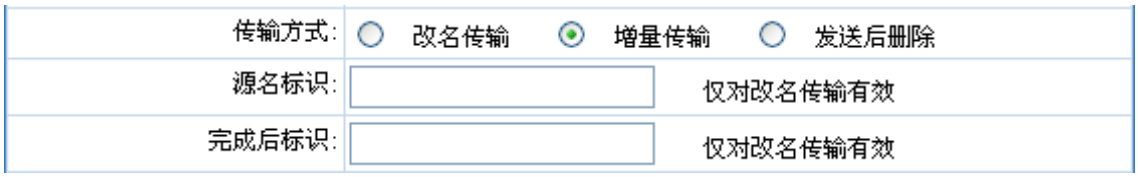


图 7 7 传输方式配置界面

◆ **包含子目录**

设置发送任务是否包含共享文件夹的子目录。默认为“是”。

◆ **文件病毒扫描**

设置是否对发送的共享文件进行病毒扫描。默认为“是”。启动文件病毒扫描需要开启病毒防护模块。

◆ **同步间隔**

设置网闸同步共享服务器的时间间隔，默认单位为妙。

该配置项为必填项。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **是否启动**

设置是否启动该发送任务。默认为“启动”。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个发送任务后面的编辑图标，弹出编辑窗口，如下图：

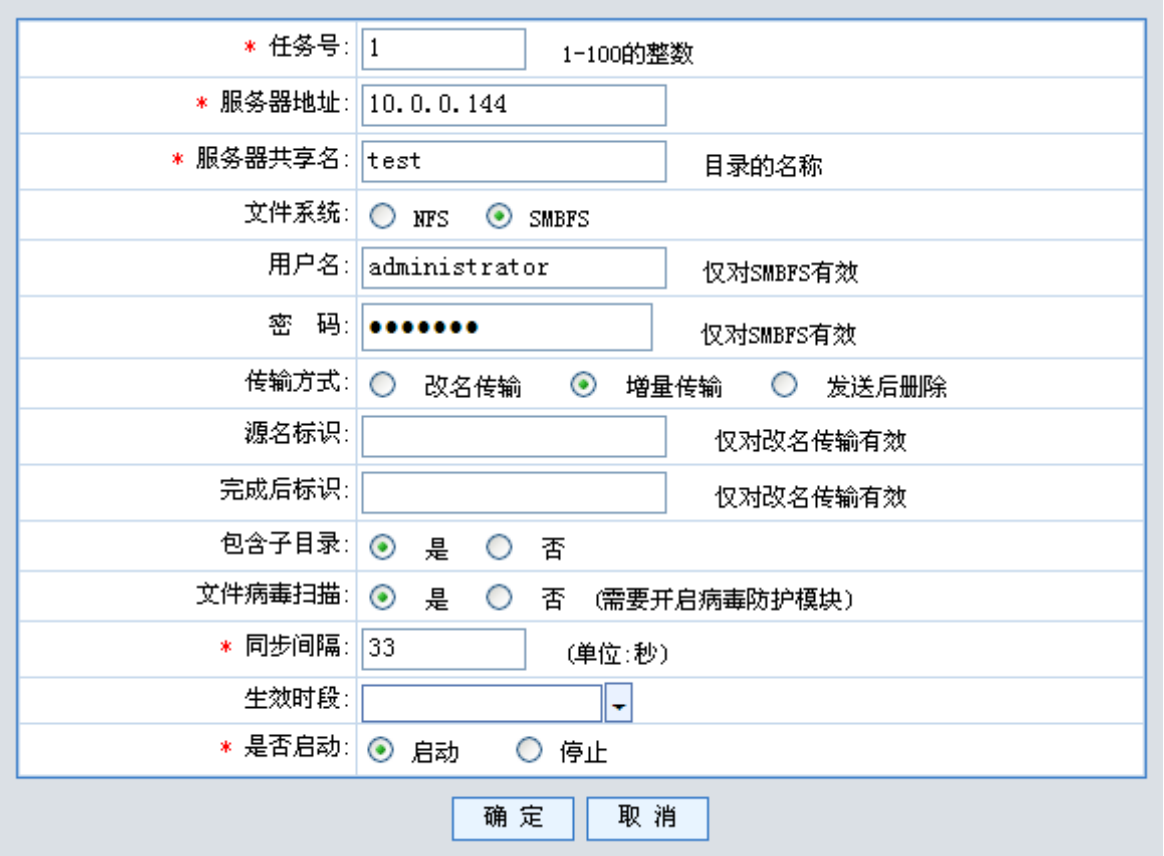


图 7 8 编辑发送任务

编辑操作时，与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个发送任务后面的删除图标，弹出编辑窗口，如下图：

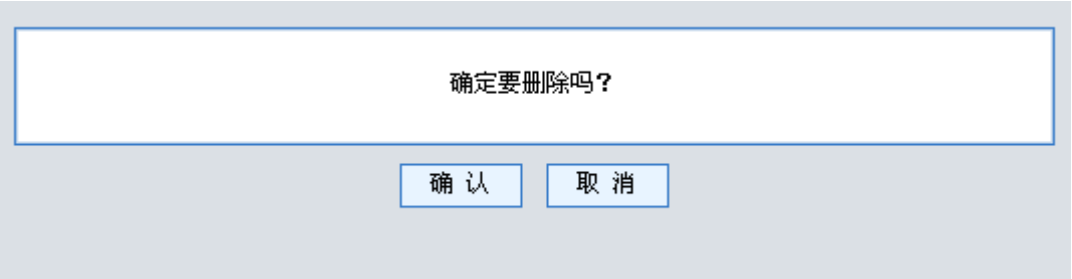


图 7 9 删除发送任务

点击“确认”按钮，删除该发送任务；点击“取消”按钮，取消当前操作。然后返回列表显

示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

7.2.2 接收任务

该部分可以对文件交换中的接收任务进行添加、修改和删除等操作。WEB 界面示意图如下：

图 7 10 接收任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

图 7 11 添加接收任务

图中接收任务的配置项，说明如下：

◆ **任务号**

任务号是文件交换的基础，每个接收任务的任务号必须与发送任务相应的任务号一一对应，

否则文件无法正常传输。

任务号只用数字表示，最多可以添加 100 个任务。该配置项必填。

◆ **服务器地址**

服务器地址指出网闸访问的共享服务器地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也支持 IP 地址 0.0.0.0。

该配置项为必填项。

◆ **服务器共享名**

服务器共享名为网闸访问的服务器共享文件目录名。

该配置项为必填项。

◆ **文件系统**

文件系统为网闸访问的服务器主机文件系统类型，分为 NFS 和 SMBFS 两种。默认为 NFS 文件系统。若选择 NFS 文件系统，则不需填写用户名和密码，用户名和密码输入框不可用。若选择 SMBFS 文件系统，则需填写用户名和密码，其中用户名和密码为登陆共享服务器所用的用户名和密码。WEB 界面示意图如下：

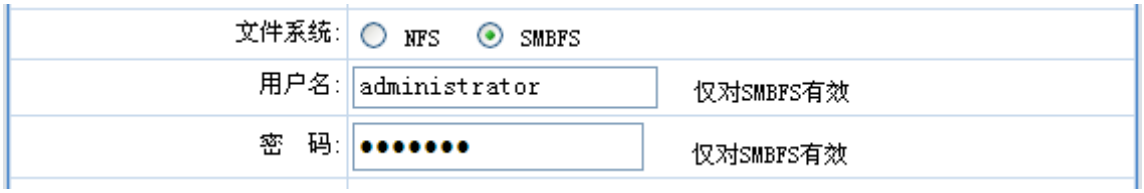


图 7 12 文件系统配置界面

◆ **是否启动**

设置是否启动该接收任务。默认为“启动”。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个接收任务后面的编辑图标，弹出编辑窗口，如下图：

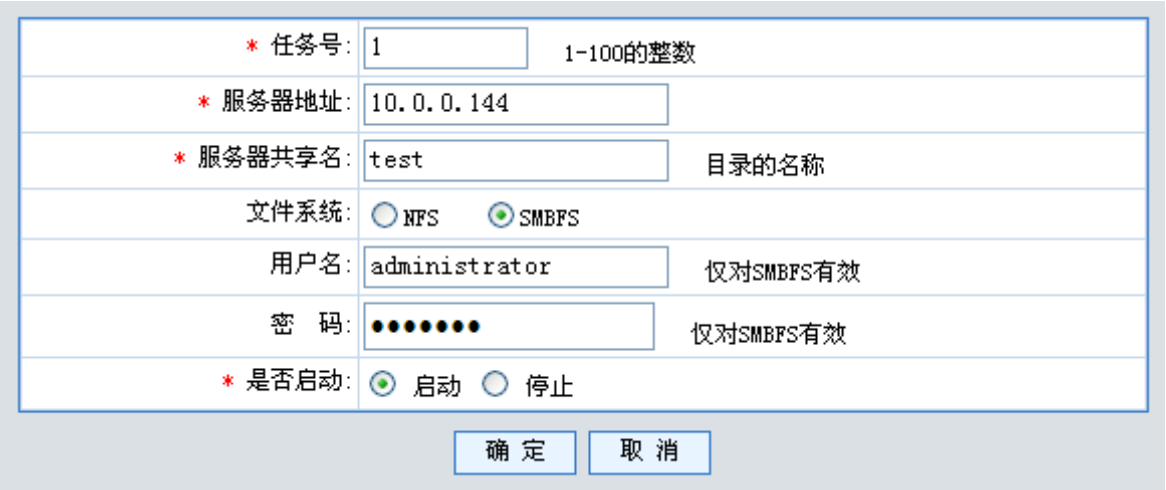


图 7 13 编辑接收任务

编辑操作时，与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个接收任务后面的删除图标，弹出编辑窗口，如下图：

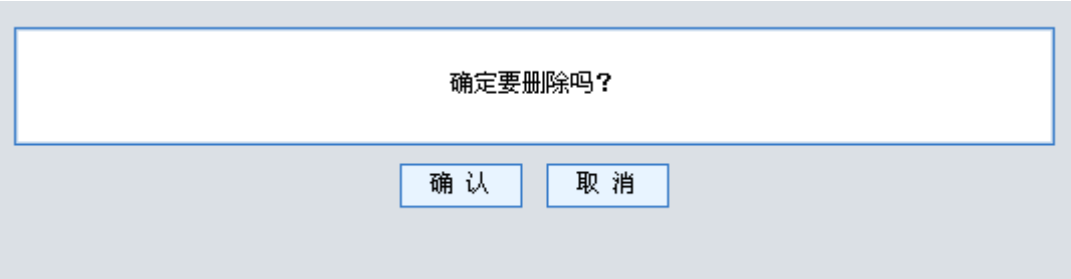


图 7 14 删除接收任务

点击“确认”按钮，删除该接收任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

7.3 内容控制

该部分用于所有与文件交换任务中内容控制有关的配置，包括：文件名控制、内容黑名单和内容白名单和文件属性控制四个过滤选项。

7.3.1 文件名控制

WEB 界面示意图如下：

图 7 15 文件名控制列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

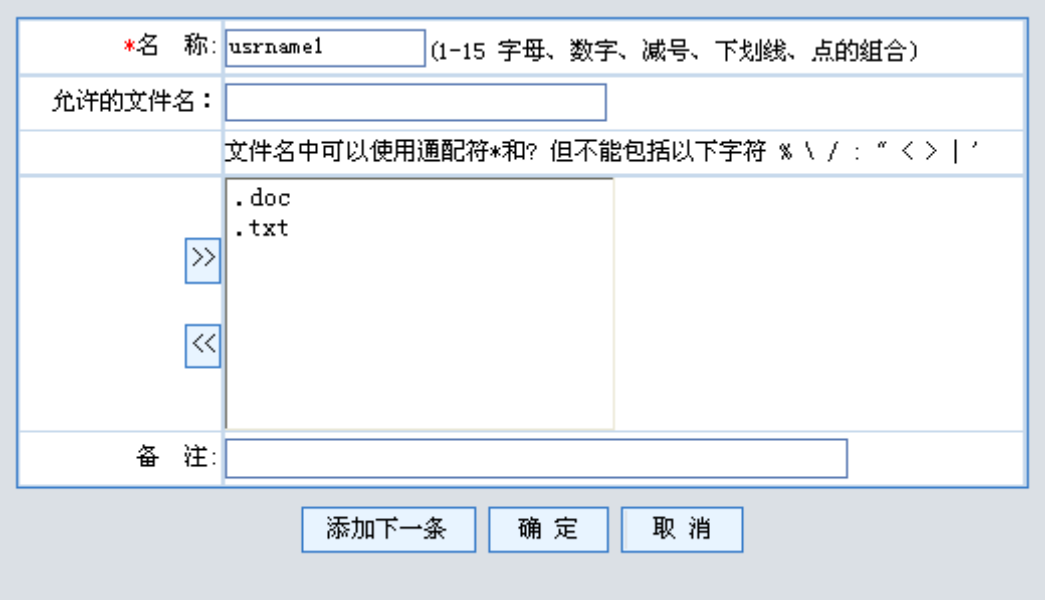


图 7 18 添加文件名

图中添加文件名的配置项，说明如下：

◆ **名称**

文件名组名称，可以是数字、点、减号、字母、下划线的组合。

名称不能为空且必须唯一。

◆ **允许的文件名**

为“允许通过”的文件名。

其格式为：以点号开始，后接具体名称。单个点号表示所有没有扩展名的文件。名称由 0 至多个合法字符（合法性说明参考公共操作说明），且字符总数不超过 30 个。文件名中可以使用通配符*和?。

点击 >> 按钮将输入的文件名加入白名单组，新加入的文件名会在下方的白名单组显示框中显示出来，继续输入文件名点击 >> 可以重复添加；

选中白名单组显示框中一项，点击<<可以删除此文件名；

◆ **备注**

该文件名的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加文件名；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个文件名后面的编辑图标，弹出编辑窗口，如下图：

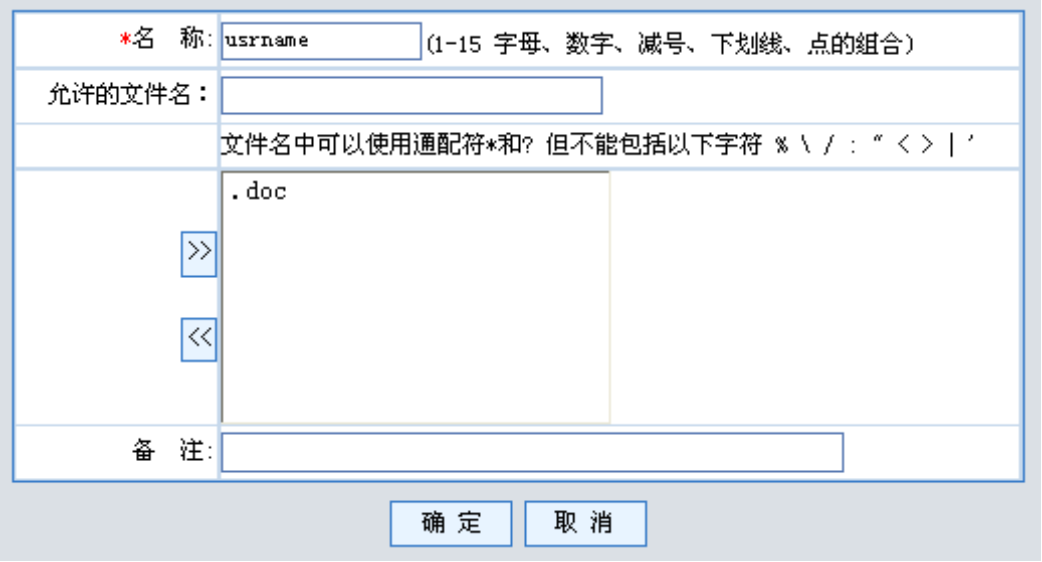


图 7 19 编辑文件名

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个文件名后面的删除图标，弹出编辑窗口，如下图：

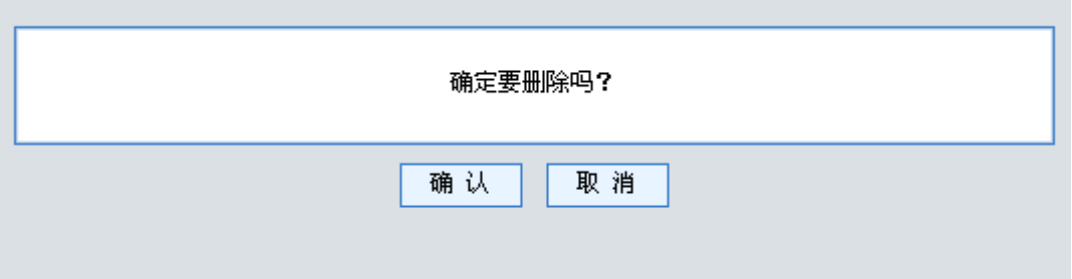


图 7 20 删除文件名

点击“确认”按钮，删除该文件名；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

7.3.2 内容黑名单

WEB 界面示意图如下：

图 7 21 内容黑名单列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

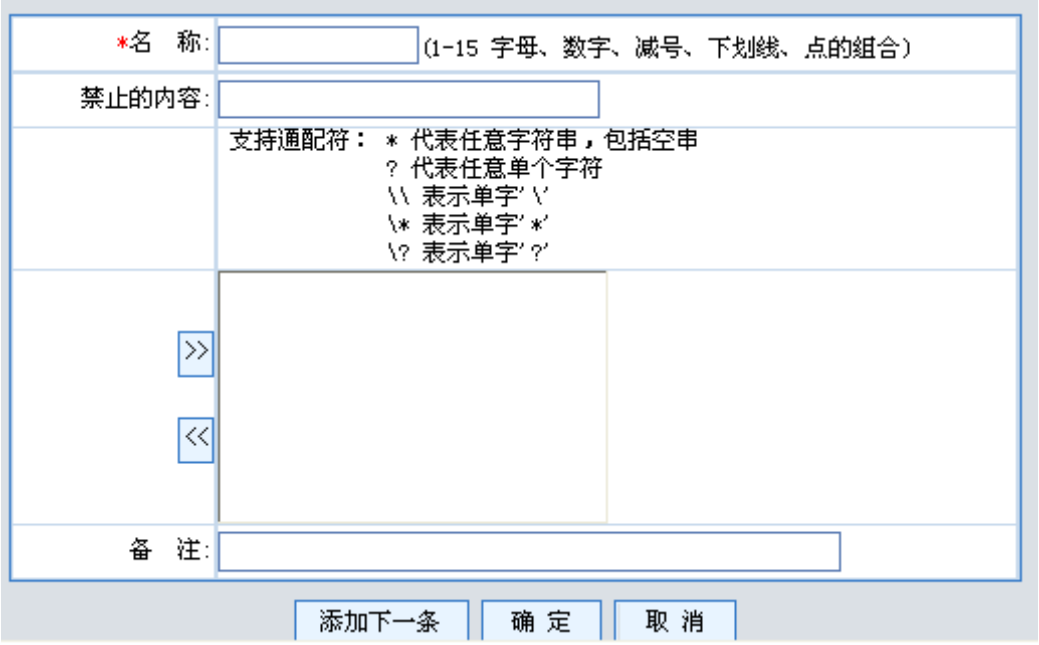


图 7 23 添加禁止的内容

图中添加黑名单的配置项，说明如下：

◆ **名称**

内容黑名单组名称，可以是数字、点、减号、字母、下划线的组合。

名称不能为空且必须唯一。

◆ **禁止的内容**

向列表中添加一个禁止的内容，内容支持通配符:

* 代表任意字符串，包括空串

? 代表任意单个字符

\\ 表示单个字符'\'

* 表示单个字符'*'
\? 表示单个字符'?'

点击 按钮将输入的内容加入黑名单组，新加入的内容会在下方的黑名单组显示框中显示出来，继续输入内容点击 可以重复添加；

选中黑名单组显示框中一项，点击 可以删除此内容；

◆ **备注**

该禁止内容的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个内容后面的编辑图标，弹出编辑窗口，如下图：

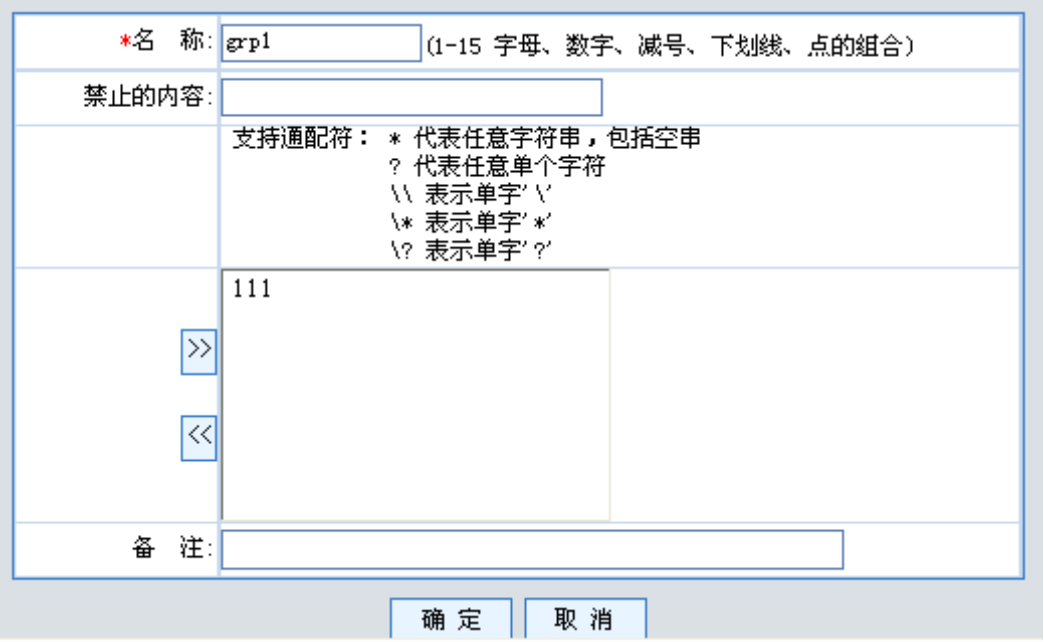


图 7 24 编辑禁止的内容

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个内容后面的删除图标，弹出编辑窗口，如下图：

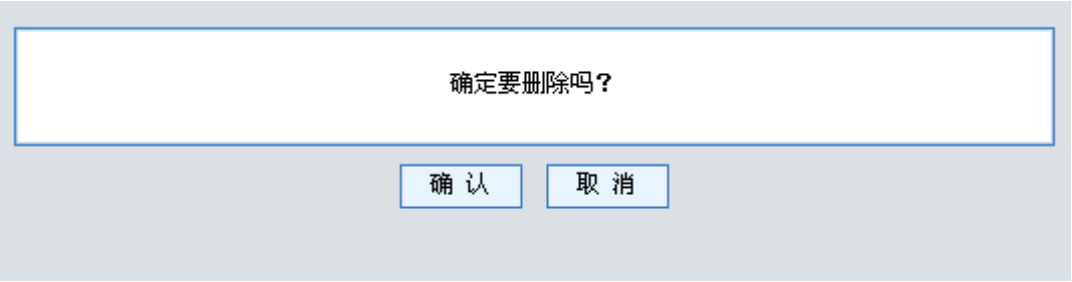


图 7 25 删除禁止的内容

点击“确认”按钮，删除该内容；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

7.3.3 内容白名单

WEB 界面示意图如下：

图 7 26 内容白名单列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

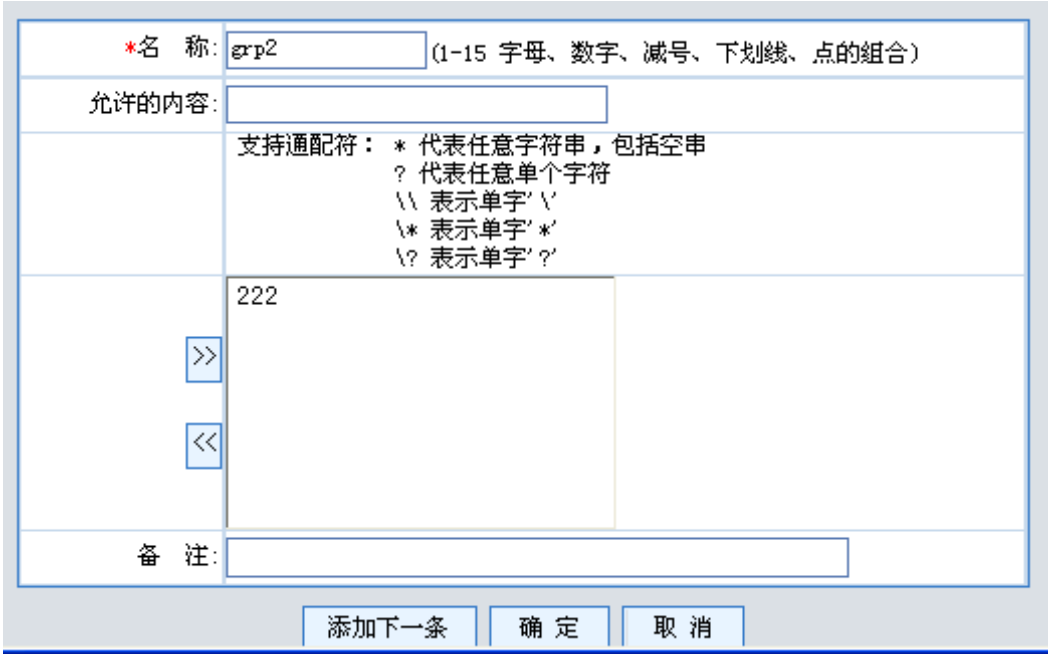


图 7 28 添加允许的内容

图中添加白名单的配置项，说明如下：

◆ **名称**

内容白名单组名称，可以是数字、点、减号、字母、下划线的组合。

名称不能为空且必须唯一。

◆ **允许的内容**

向列表中添加一个允许的内容，内容支持通配符：

* 代表任意字符串，包括空串

? 代表任意单个字符

\\ 表示单个字符'\'

* 表示单个字符'*'

\? 表示单个字符'?'

点击 按钮将输入的内容加入白名单组，新加入的内容会在下方的白名单组显示框中显示出来，继续输入内容点击 可以重复添加；

选中白名单组显示框中一项，点击 可以删除此内容；

◆ **备注**

该禁止内容的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个内容后面的编辑图标，弹出编辑窗口，如下图：

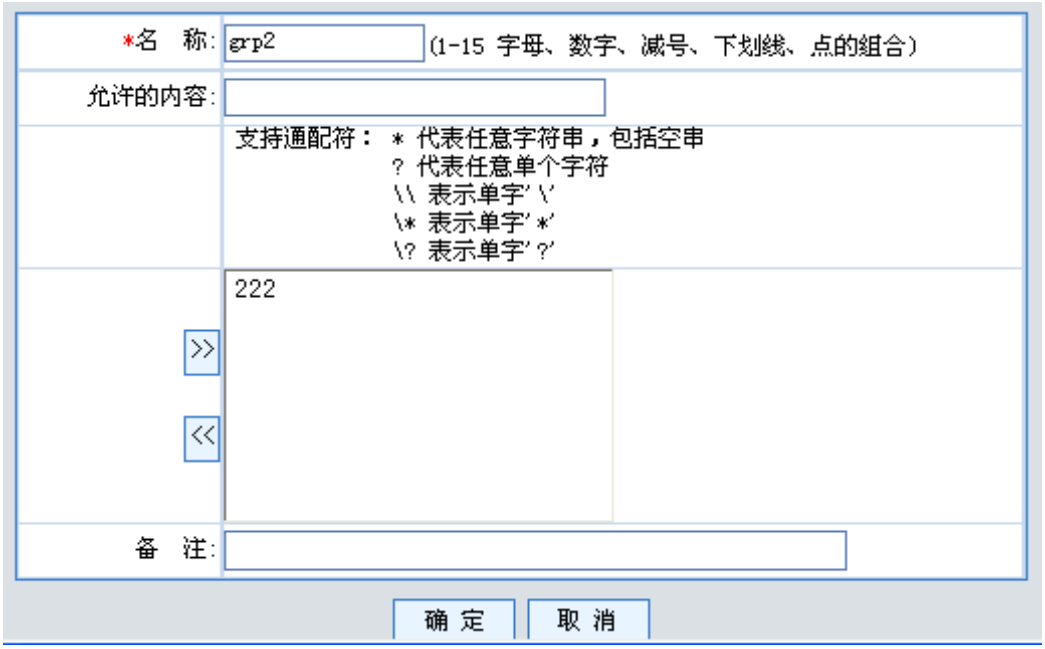


图 7 29 编辑允许的内容

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个内容后面的删除图标，弹出编辑窗口，如下图：

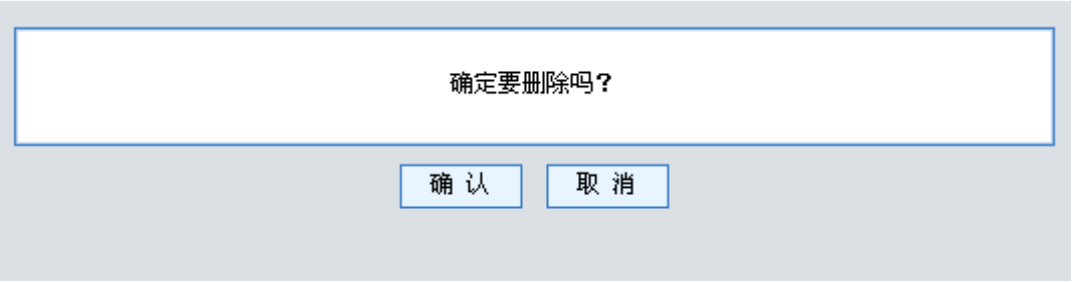


图 7 30 删除禁止的内容

点击“确认”按钮，删除该内容；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

注意:

若黑白名单控制同时启用，则以文件名控制、内容黑名单及内容白名单的顺序依次过滤。

7.3.4 文件属性控制

WEB 界面示意图如下：

图 7　31　文件属性控制显示界面

该模块包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

图 12　15　添加文件属性控制

图中文件属性控制的配置项，说明如下：

◆　**名称**

文件属性控制名称，可以是数字、中文、字母、下划线的组合。名称不能为空且必须唯一。

◆　**允许文件名组**

该选项用于设置允许文件名组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

下拉列表初始只有“无”菜单选项，其菜单项来源于“文件名控制”中定义的允许文件名组。

◆　**内容黑名单组**

设置不允许通过的内容组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

下拉列表初始只有“无”菜单选项，其菜单项来源于“内容黑名单”中定义的内容黑名单组。

◆ **内容白名单组**

设置允许通过的内容组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

下拉列表初始只有“无”菜单选项，其菜单项来源于“内容白名单”中定义的内容白名单组。

◆ **文件类型**

设置需要过滤的文件类型。

◆ **类型过滤动作**

设置对选中文件类型的过滤动作。

◆ **文件大小**

设置允许通过的文件大小上限和下限。默认单位为 K。

◆ **文件修改时间**

设置允许通过的文件的修改时间范围。

◆ **备注**

该文件属性控制的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加文件属性控制；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个文件属性控制后的编辑图标，弹出编辑窗口，如下图：

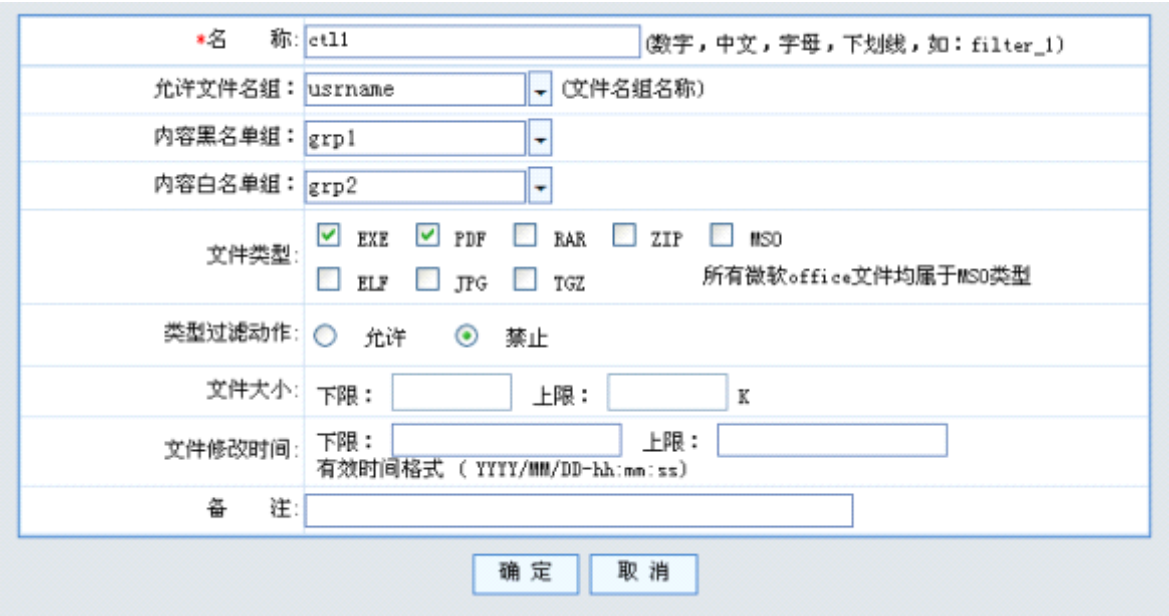


图 12 16 修改文件属性控制

编辑操作时，除名称不能修改外，其他与添加操作类似。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个文件属性控制后的删除图标，弹出编辑窗口，如下图：

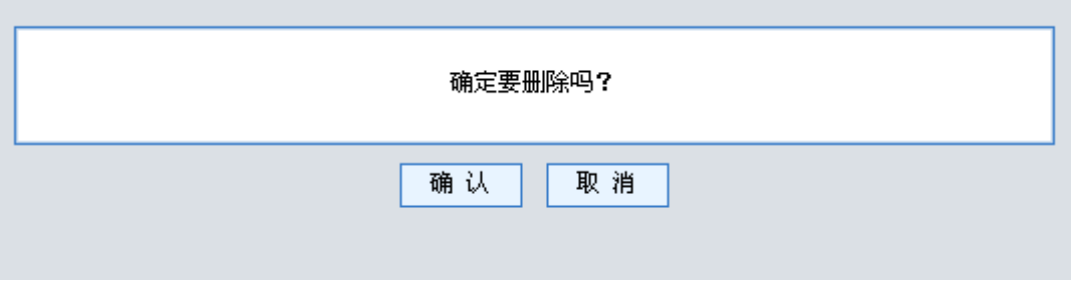


图 12　17　删除文件属性控制

点击“确认”按钮，删除该文件属性控制；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

7.4 文件交换任务

文件交换任务显示网闸当前启动的发送或者接受任务列表。WEB 界面示意图如下：

图 7　33　文件交换任务列表显示

第 8 章　文件交换

文件交换模块支持各种类型文件在外部网和涉密网之间的安全传输，文件传输支持以数字证书方式的强用户认证和通讯加密，强化文件交换的安全性和保密性。整个模块由两个部分组成：文件交换客户端系统、网闸系统。客户端系统的操作说明请参见客户端系统操作手册。在此，主要介绍网闸系统的操作说明。

网闸系统的基本功能包括基本配置、客户端、服务端、内容控制等四个模块，导航菜单如下图：

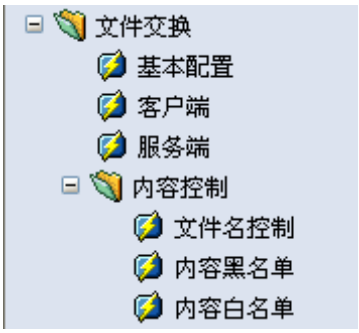


图 8　1　文件交换 WEB 界面导航菜单

8.1 基本配置

“基本配置”部分，主要配置本地证书、文件交换服务的启停控制等。WEB 界面示意图如下：

图 8　2　基本配置界面

8.1.1　证书设置

本地证书及其相关文件的导入，对于采用身份认证和通信 SSL 加密模式是必须的。需导入

的对象包括：CA 证书、用户证书、用户证书的私钥、私钥口令等四个。其中，CA 证书必须与通信对端的用户证书的 CA 证书一致，即通信双方的用户证书都必须由同一个 CA 签发。用户证书、用户证书私钥、私钥口令三者必须一致，否则通信无法正常进行。

操作方法：

1) CA 证书、用户证书、用户证书的私钥等三项可以点击“浏览”按钮引入相应文件，也可以直接在文本框中直接输入文件路径；
2) 私钥口令：直接在文件框中输入即可；
3) 以上四项都输入完毕后，点击“导入”按钮；
4) 导入完毕后，在 WEB 页面的下面的“文件交换证书列表”中，会显示导入的证书信息。对于 CA 证书、用户证书私钥，不显示其公共名、过期时间。用户也可以点击该表每项右边的删除按钮，删除该项。

特别说明:

- ✧ 当文件交换的任务采用身份认证/通讯加密传输模式时，必须在此导入证书相关的文件，否则相应的任务无法正常运行。而对于普通的非认证、非加密模式下的文件交换，本地导入的证书不会被使用；
- ✧ 证书的合法性和有效性的检查，在相应的访问任务初始化时进行，若失败，相应的访问任务立即中止，并在日志中有相关说明。而在导入的过程中，则不做检查；
- ✧ 导入时，CA 证书、用户证书、用户证书的私钥、私钥口令等四项必须同时填写，否则报错，并中止导入。

8.1.2 服务管理

服务管理主要用于控制服务的运行状态。操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

8.2 客户端

该部分可以对文件交换中的客户端任务进行添加、修改和删除等操作。WEB 界面示意图如下：

图 8 3 客户端任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

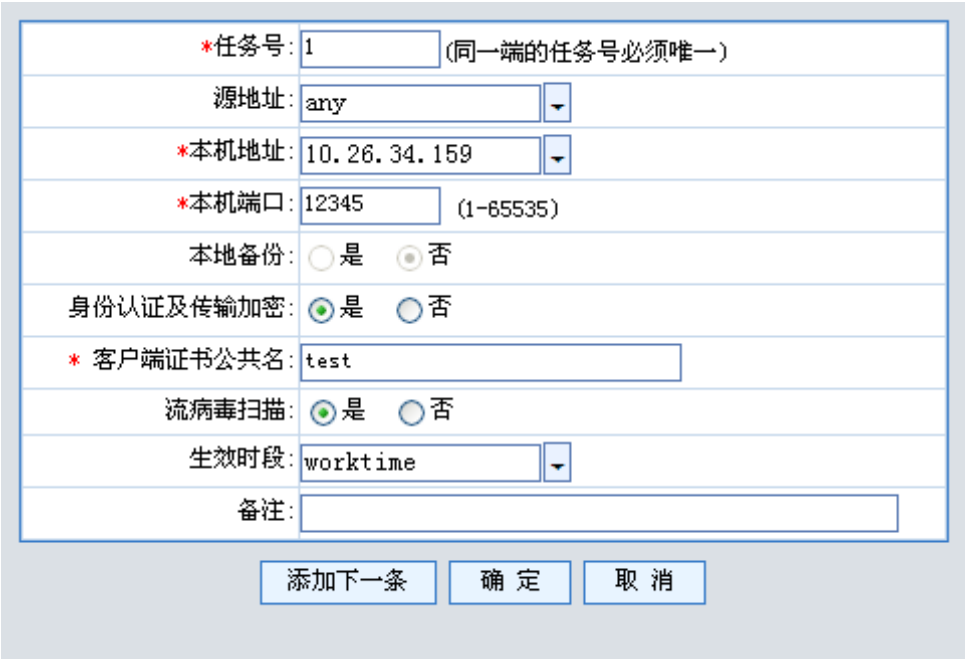


图 8 4 添加客户端任务

图中发送任务的配置项，说明如下：

◆ **任务号**

任务号是文件交换的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则文件无法正常传输。

任务号只用数字表示，最多可以添加 100 个任务。该配置项必填。

◆ **源地址**

源地址指出允许访问本机的源客户端的地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置>>网络接口”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

本机端口为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535。

该配置项为必填项。

◆ **本地备份**

设置文件在传输过程中是否在网闸中进行备份，默认为“否”。特别指出的是，若采用本地备份模式，则必须考虑到实际传输的单个文件的最大容量：如果单个文件的最大容量超过网闸本机的实际缓存（与网闸的运行状态有关）大小，将导致该文件无法正确传输。

非特殊情况，建议用户不要备份。网闸出厂时的标准配置中，该选项被关闭。

◆ **身份认证及传输加密**

设置是否进行身份认证，并在文件的传输过程中采用 SSL 加密方式，默认为“是”。

◆ **客户端证书公共名**

对端（客户端）证书的主题公共名，仅在启用身份认证及传输加密时有效。不同访问任务之间，其对端证书的公共名可以不同。

◆ **流病毒扫描**

设置是否对文件传输流进行病毒扫描，默认为“是”。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后面的编辑图标，弹出编辑窗口，如下图：

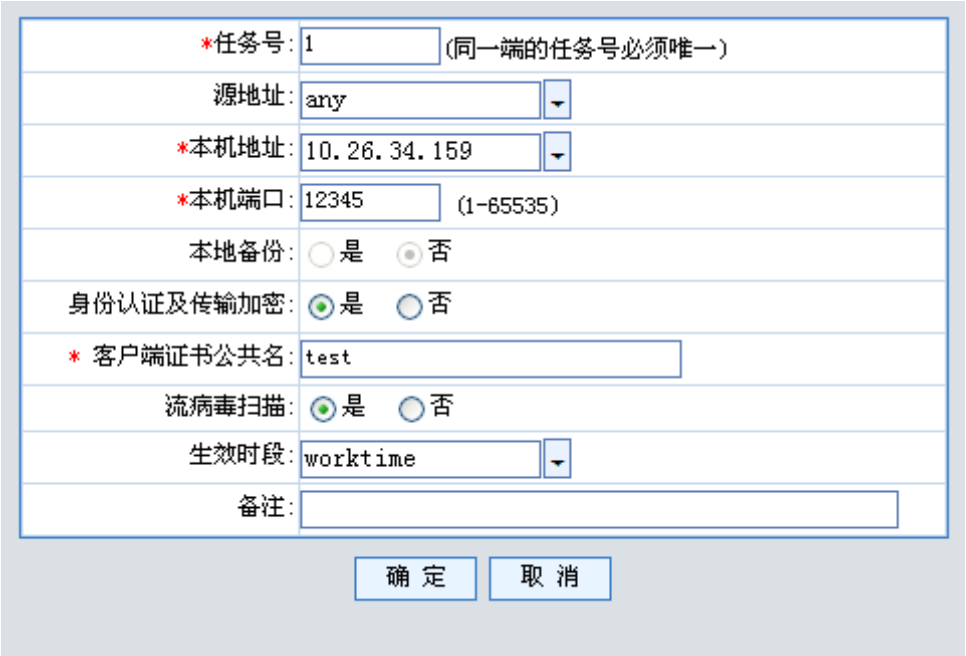


图 8 5 编辑客户端任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后面的删除图标，弹出编辑窗口，如下图：

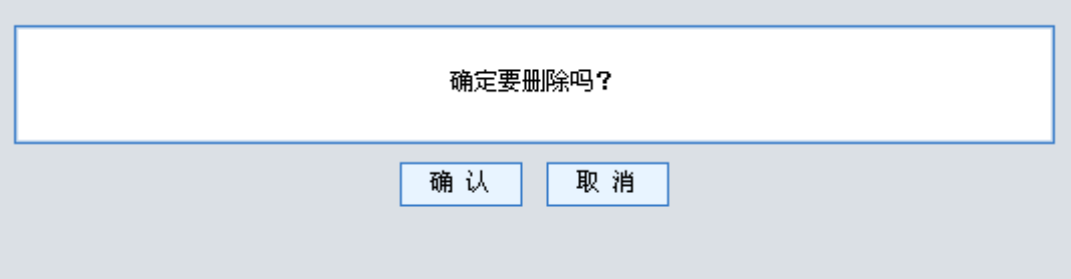


图 8 6 删除客户端任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

8.3 服务端

该部分可以对文件交换中的服务端任务进行添加、修改和删除等操作。WEB 界面示意图如下：

图 8 7 服务端任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

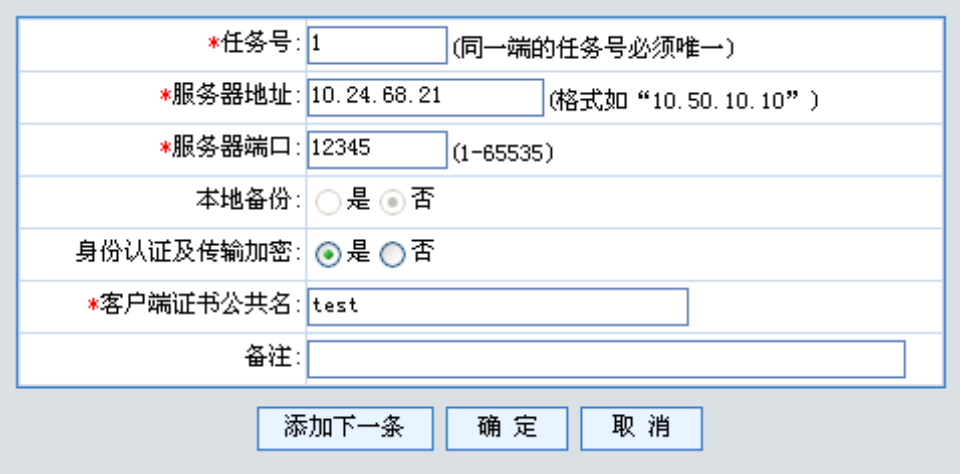


图 8 8 添加服务端任务

图中发送任务的配置项，说明如下：

◆ **任务号**

任务号是文件交换的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则文件无法正常传输。

任务号只用数字表示，最多可以添加 100 个任务。该配置项必填。

◆ **服务器地址**

服务器地址为文件交换目的客户端的 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也支持 IP 地址 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问文件交换客户端所在的服务器的真实端口。

取值范围：1－65535。

该配置项为必填项。

◆ **本地备份**

设置文件在传输过程中是否在网闸中进行备份，默认为“否”。特别指出的是，若采用本地备份模式，则必须考虑到实际传输的单个文件的最大容量：如果单个文件的最大容量超过网闸本机的实际缓存（与网闸的运行状态有关）大小，将导致该文件无法正确传输。

非特殊情况，建议用户不要备份。网闸出厂时的标准配置中，该选项被关闭。

◆ **身份认证及传输加密**

设置是否进行身份认证，并在文件的传输过程中采用 SSL 加密方式，默认为“是”。

◆ **客户端证书公共名**

对端（客户端）证书的主题公共名，仅在启用身份认证及传输加密时有效。不同访问任务之间，其对端证书的公共名可以不同。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后面的编辑图标，弹出编辑窗口，如下图：

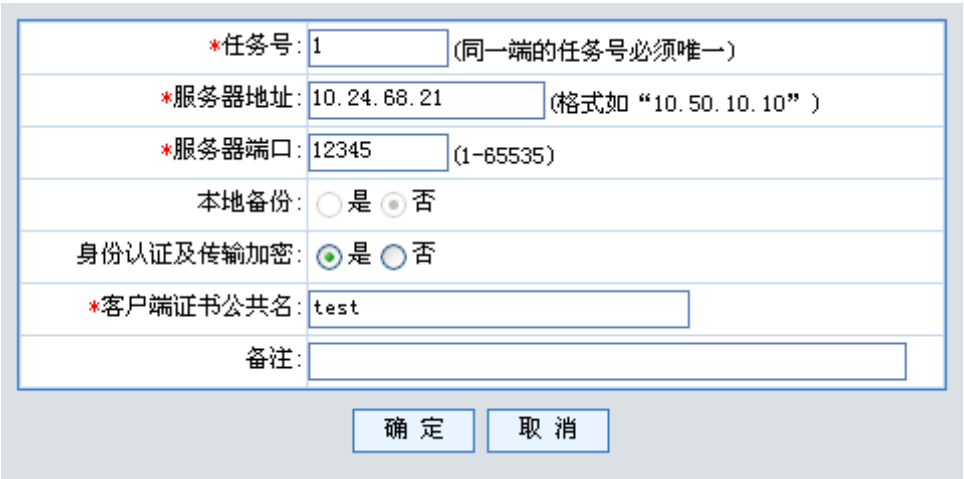


图 8 9 编辑服务端任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后面的删除图标，弹出编辑窗口，如下图：

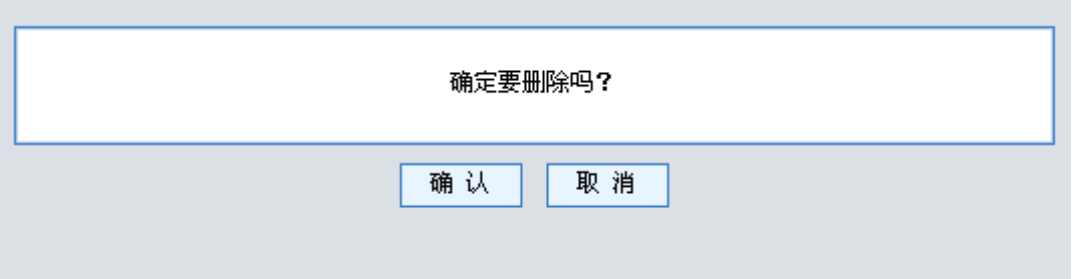


图 8 10 删除服务端任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

8.4 内容控制

该部分用于所有与文件交换任务中内容控制有关的配置，包括：文件名控制、内容黑名单和内容白名单等三个过滤选项。

8.4.1 文件名控制

该部分可以设置文件交换任务中是否启用文件名控制，是否允许二进制文件，以及对的文件名控制列表进行添加、修改和删除等操作。WEB 界面示意图如下：

图 8 11 文件名控制列表显示

一. 启用文件名控制

WEB 界面如下图（红色方框内为配置开关）：

图 8 12 启用文件名控制

✧ 选中复选框：启用文件名控制，此时只有符合文件名列表中的文件才能够被传输。

✧ 取消复选框：停止文件名控制，此时任意文件名的文件都可以被传输。

二. 允许二进制文件

WEB 界面如下图（红色方框内为配置开关）：

图 8 13 启用文件名控制

✧ 选中复选框：允许二进制文件（非纯文本文件）通过。

✧ 取消复选框：禁止二进制文件（非纯文本文件）通过。

三. 文件名控制列表

当启用文件名控制时，只有在文件名列表中的文件才可以被传输。

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

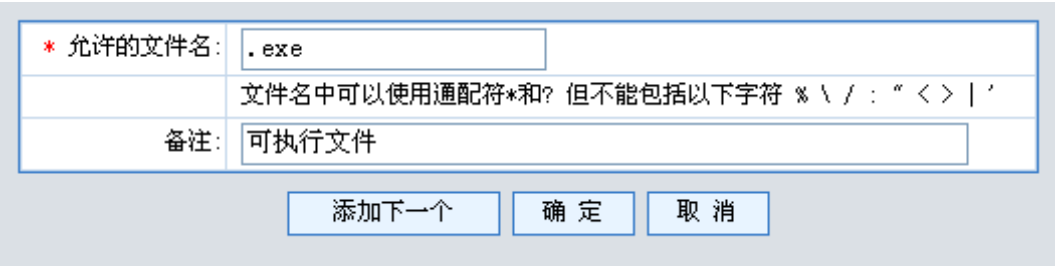


图 8 14 添加文件名

图中添加文件名的配置项，说明如下：

◆ **允许的文件名**

向文件名列表中添加一个文件名，在启用文件名控制时，符合文件名列表的文件才可以被传输。文件名中可以使用通配符*和? 但不能包括以下字符 %\/:"<>|'

◆ **备注**

该文件名的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加文件名；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个文件名后面的编辑图标，弹出编辑窗口，如下图：

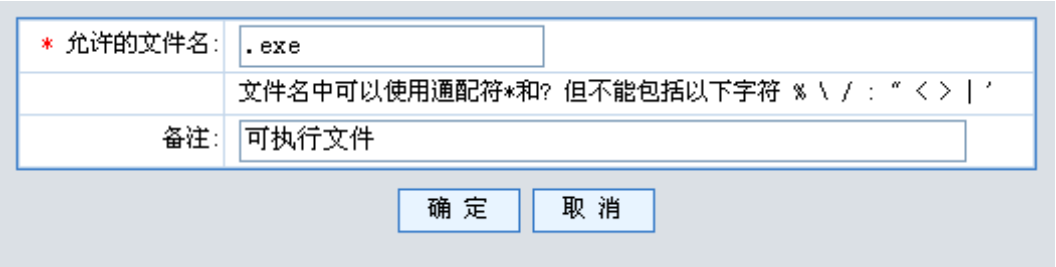


图 8 15 编辑文件名

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个文件名后面的删除图标，弹出编辑窗口，如下图：

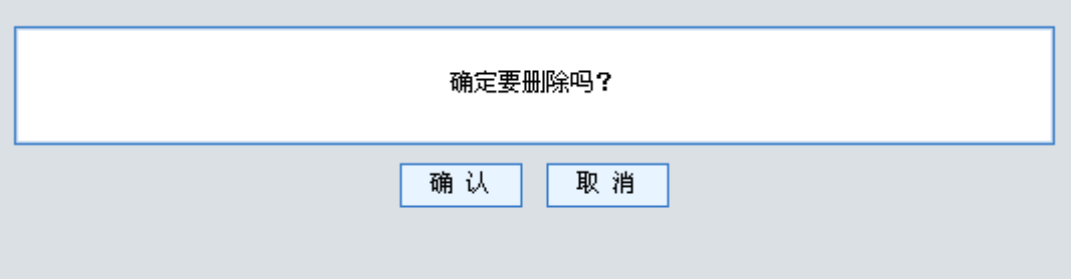


图 8 16 删除文件名

点击“确认”按钮，删除该文件名；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

8.4.2 内容黑名单

该部分可以设置文件交换任务中是否启用内容黑名单控制以及对内容黑名单控制列表进行添加、修改和删除等操作。包含此关键字的文件将不被发送。只有“启用黑名单控制”选项选中后，设置的关键字才会生效 WEB 界面示意图如下：

图 8 17 内容黑名单列表显示

一. 启用黑名单控制

WEB 界面如下图（红色方框内为配置开关）：

图 8 18 启用黑名单控制

- ✧ 选中复选框：启用黑名单控制，此时包含黑名单列表中任意一项的文件都会被禁止传输。
- ✧ 取消复选框：停止黑名单控制，此时黑名单列表不起作用，所有的文件都能被传输。

注：如果选中复选框，但未添加任何被禁止的关键字，则所有文件允许通过。

二. 内容黑名单列表

当启用内容黑名单控制时，只要包含任意一项禁止内容的文件都会被禁止传输。该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

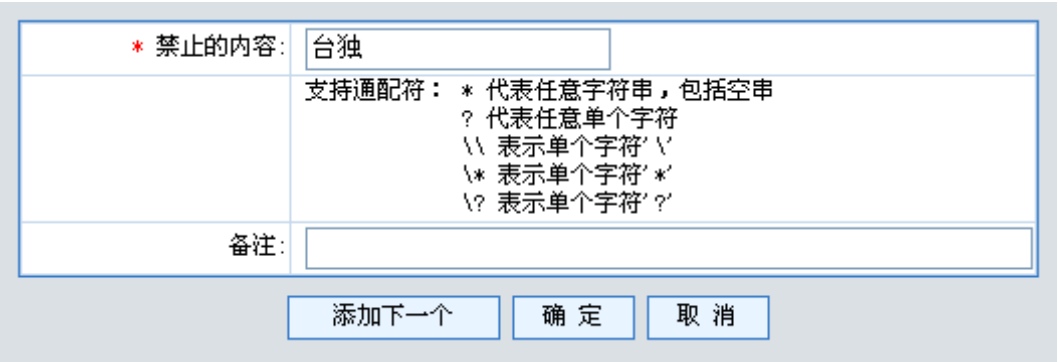


图 8 19 添加禁止的内容

图中添加黑名单的配置项，说明如下：

◆ **禁止的内容**

向列表中添加一个禁止的内容，在启用内容黑名单控制时，只要包含此项内容的文件都会被禁止传输。内容支持通配符： * 代表任意字符串，包括空串

? 代表任意单个字符

\\ 表示单个字符'\'

* 表示单个字符'*'

\? 表示单个字符'?'

◆ **备注**

该禁止内容的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个内容后面的编辑图标，弹出编辑窗口，如下图：

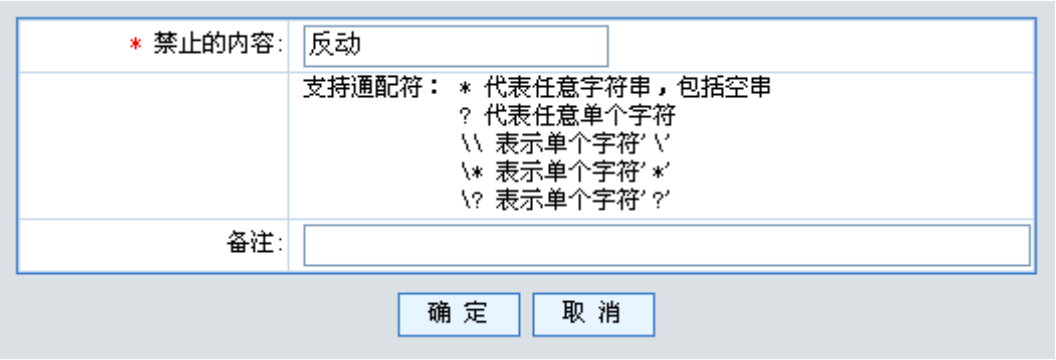


图 8 20 编辑禁止的内容

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个内容后面的删除图标，弹出编辑窗口，如下图：

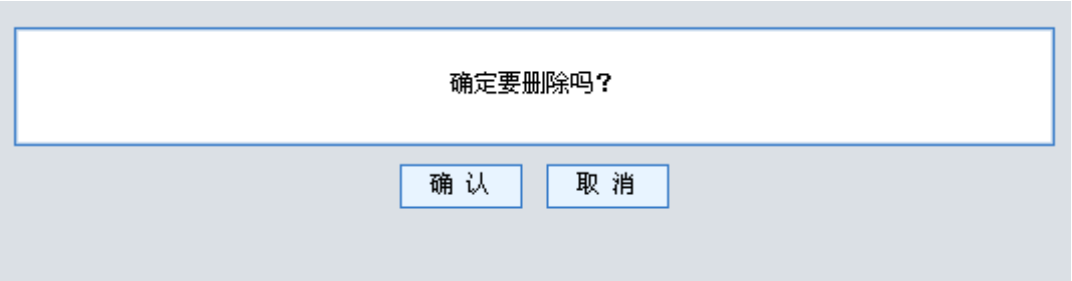


图 8 21 删除禁止的内容

点击“确认”按钮，删除该内容；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

8.4.3 内容白名单

该部分可以设置文件交换任务中是否启用内容白名单控制以及对内容白名单控制列表进行添加、修改和删除等操作。没有包含此关键字的文件将不被发送。只有“启用白名单控制”选项选中后，设置的关键字才会生效。

WEB 界面示意图如下：

图 8 22 内容白名单列表显示

一. 启用白名单控制

WEB 界面如下图（启用白名单控制为配置开关）：

图 8 23 启用白名单控制

✧ 选中复选框：启用白名单控制，此时只包含白名单列表中至少任意一项的文件才能被传

输。

✧ 取消复选框：停止白名单控制，此时白名单列表不起作用，所有的文件都能被传输。

注：如果选中复选框，但未添加任何被允许的关键字，则所有文件允许通过。

二. 内容白名单列表

当启用内容白名单控制时，只有包含任意一项允许内容的文件才能够被传输。该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

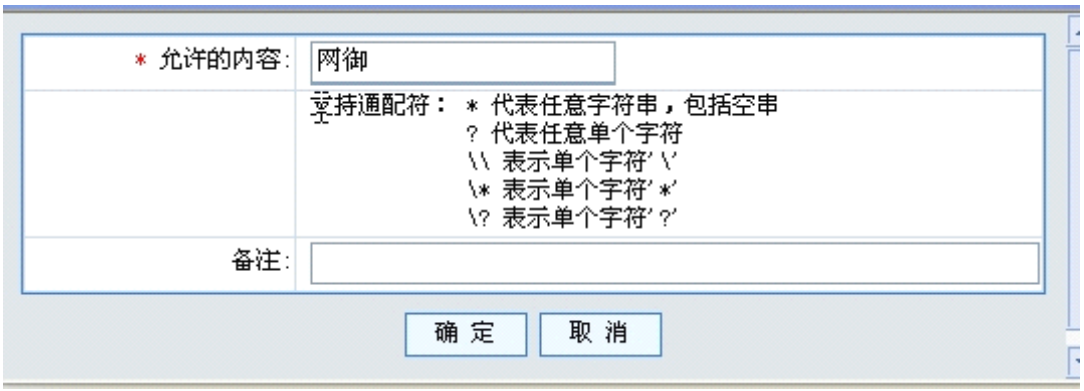


图 8 24 添加允许的内容

图中添加白名单的配置项，说明如下：

◆ **允许的内容**

向列表中添加一个允许的内容，在启用内容白名单控制时，包含此项内容的文件才会被传输。

内容支持通配符： * 代表任意字符串，包括空串
? 代表任意单个字符
\\ 表示单个字符'\'
* 表示单个字符'*'
\? 表示单个字符'?'

◆ **备注**

该禁止内容的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个内容后面的编辑图标，弹出编辑窗口，如下图：

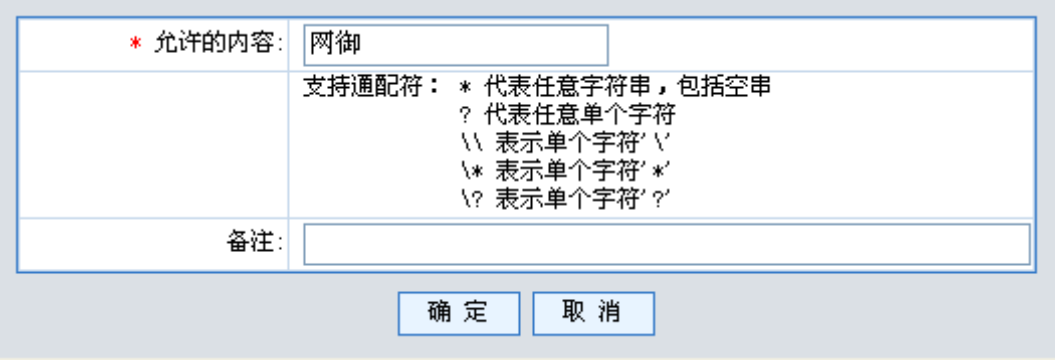


图 8 25 编辑允许的内容

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个内容后面的删除图标，弹出编辑窗口，如下图：

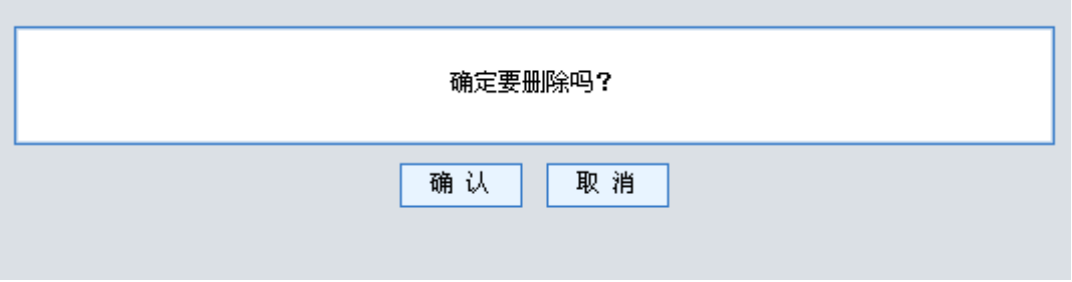


图 8 26 删除禁止的内容

点击“确认”按钮，删除该内容；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

注意:

若黑白名单控制同时启用，则以文件名控制、内容黑名单及内容白名单的顺序依次过滤。

第 9 章　数据库同步

数据库同步模块提供分布在外部网和涉密网之间的数据库系统之间进行安全、可靠的数据同步，支持包括 SQLSERVER、ORACLE、SYBASE、DB2 等在内的多种主流数据库系统的各种版本。身份认证方式支持以数字证书方式的强用户认证，整个数据通讯过程采取全过程 SSL 加密，以确保数据同步的高安全性。而且，数据库系统之间的双向同步模式能更好地满足用户的需求。

整个系统由两个部分组成：客户端系统、网闸系统。客户端系统的操作说明请参见客户端系统操作手册。在此，主要介绍网闸系统的操作说明。

网闸系统的基本功能包括基本配置、客户端配置和服务端配置等三个模块，导航菜单如下图：

图 9　1　数据库同步 WEB 界面导航菜单

9.1 基本配置

“基本配置”部分，主要配置本地证书、数据库同步服务的启停控制等。WEB 界面示意图如下：

图 9　2　基本配置界面

9.1.1　证书设置

本地证书及其相关文件的导入，对于采用身份认证和通信 SSL 加密模式是必须的。需导入的对象包括：CA 证书、用户证书、用户证书的私钥、私钥口令等四个。其中，CA 证书必须与通信对端的用户证书的 CA 证书一致，即通信双方的用户证书都必须由同一个 CA 签发。用户证

书、用户证书私钥、私钥口令三者必须一致，否则通信无法正常进行。

操作方法：

1) CA 证书、用户证书、用户证书的私钥等三项可以点击“浏览”按钮引入相应文件，也可以直接在文本框中直接输入文件路径；
2) 私钥口令：直接在文件框中输入即可；
3) 以上四项都输入完毕后，点击“导入”按钮；
4) 导入完毕后，在 WEB 页面的下面的“文件交换证书列表”中，会显示导入的证书信息。对于 CA 证书、用户证书私钥，不显示其公共名、过期时间。用户也可以点击该表每项右边的删除按钮，删除该项。

特别说明:

- ✧ 当文件交换的任务采用身份认证/通讯加密传输模式时，必须在此导入证书相关的文件，否则相应的任务无法正常运行。而对于普通的非认证、非加密模式下的文件交换，本地导入的证书不会被使用；
- ✧ 证书的合法性和有效性的检查，在相应的访问任务初始化时进行，若失败，相应的访问任务立即中止，并在日志中有相关说明。而在导入的过程中，则不做检查；
- ✧ 导入时，CA 证书、用户证书、用户证书的私钥、私钥口令等四项必须同时填写，否则报错，并中止导入。

9.1.2 服务管理

服务管理主要用于控制服务的运行状态。操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

9.2 客户端

该部分可以对数据库同步的客户端任务进行添加、修改和删除等操作。WEB 界面示意图如下：

图 9 3 客户端任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

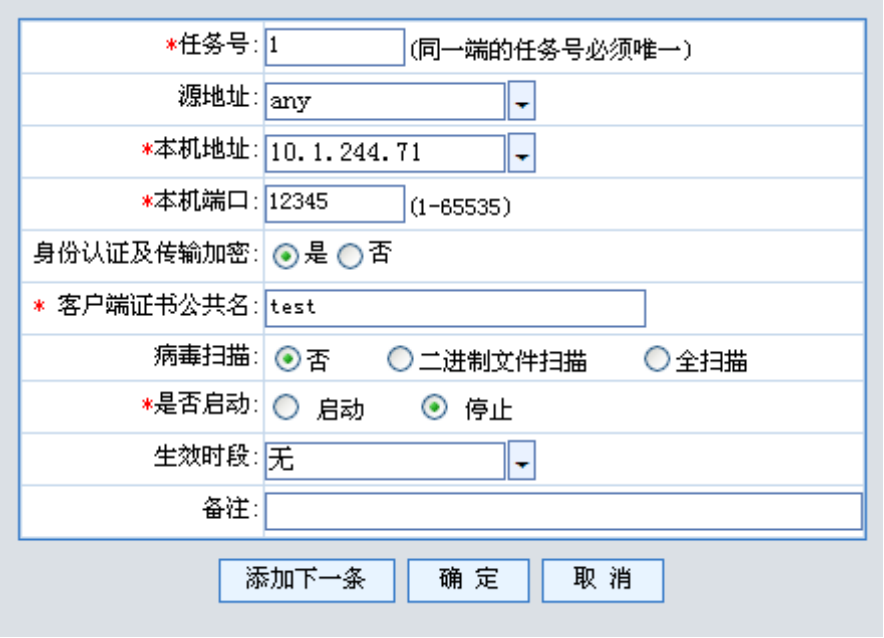


图 9 4 添加客户端任务

图中发送任务的配置项，说明如下：

◆ **任务号**

任务号是文件交换的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则文件无法正常传输。

任务号只用数字表示，最多可以添加 100 个任务。该配置项必填。

◆ **源地址**

源地址指出允许访问本机的源客户端的地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置>>网络接口”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

本机端口为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535。

该配置项为必填项。

◆ **身份认证及传输加密**

设置是否进行身份认证，并在文件的传输过程中采用 SSL 加密方式，默认为“是”。

◆ **客户端证书公共名**

对端（客户端）证书的主题公共名，仅在启用身份认证及传输加密时有效。不同访问任务之间，其对端证书的公共名可以不同。

◆ **病毒扫描**

该选项设置是否对数据流进行病毒扫描，可选“无”，“二进制文件扫描”，“全扫描”三种选项，默认选择“无”。其中“二进制文件扫描”仅针对二进制文件字段进行病毒扫描，“全扫描”则针对全部数据流进行病毒扫描，包括二进制文件字段和文本文件字段。

◆ **是否启动**

该选项设置是否启动客户端任务，默认为“停止”。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后面的编辑图标，弹出编辑窗口，如下图：

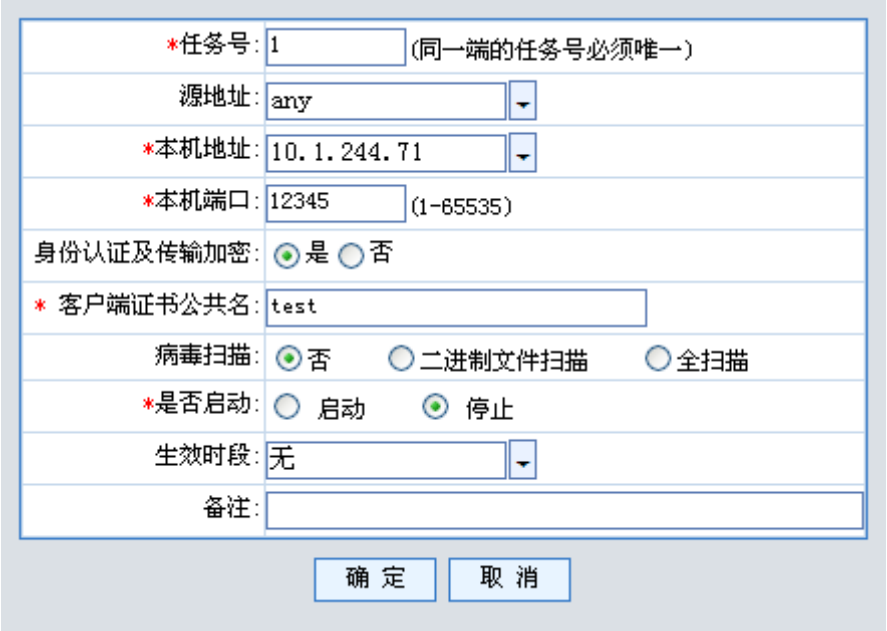


图 9 5 编辑客户端任务

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后面的删除图标，弹出编辑窗口，如下图：

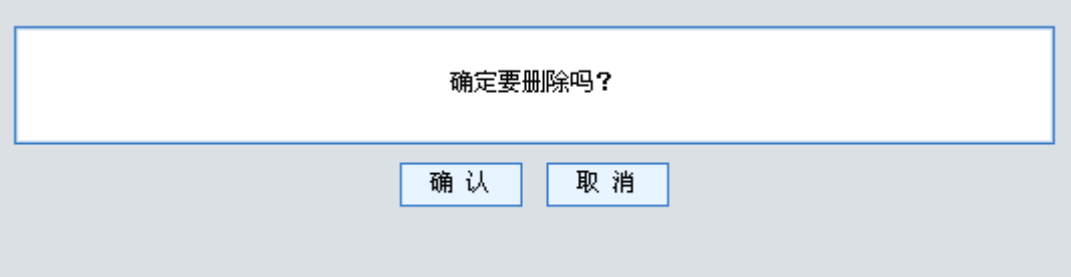


图 9 6 删除客户端任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

9.3 服务端

该部分可以对数据库同步的服务端任务进行添加、修改和删除等操作。WEB 界面示意图如下：

图 9 7 服务端任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

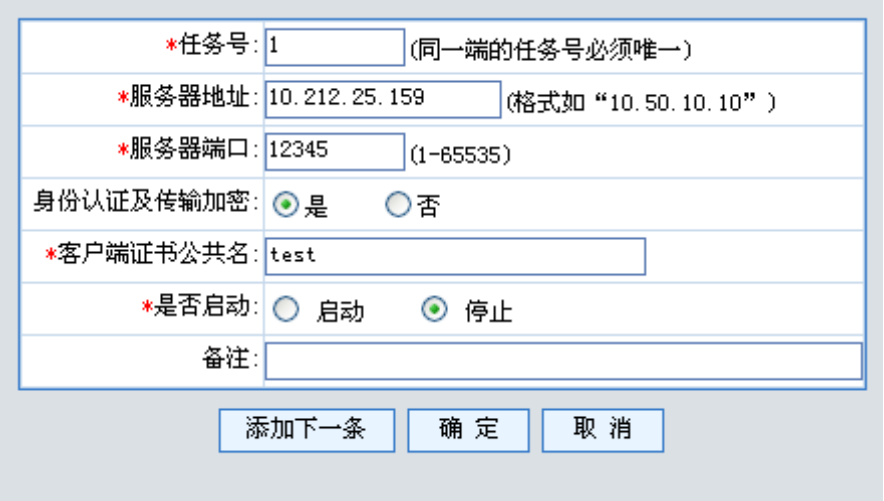


图 9 8 添加服务端任务

图中发送任务的配置项，说明如下：

◆ **任务号**

任务号是文件交换的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则文件无法正常传输。

任务号只用数字表示，最多可以添加 100 个任务。该配置项必填。

◆ **服务器地址**

服务器地址为文件交换目的客户端的 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也支持 IP 地址 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问文件交换客户端所在的服务器的真实端口。

取值范围：1－65535。

该配置项为必填项。

◆ **身份认证及传输加密**

设置是否进行身份认证，并在文件的传输过程中采用 SSL 加密方式，默认为“是”。

◆ **客户端证书公共名**

对端（客户端）证书的主题公共名，仅在启用身份认证及传输加密时有效。不同访问任务之间，其对端证书的公共名可以不同。

◆ **是否启动**

该选项设置是否启动服务端任务，默认为“停止”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后面的编辑图标，弹出编辑窗口，如下图：

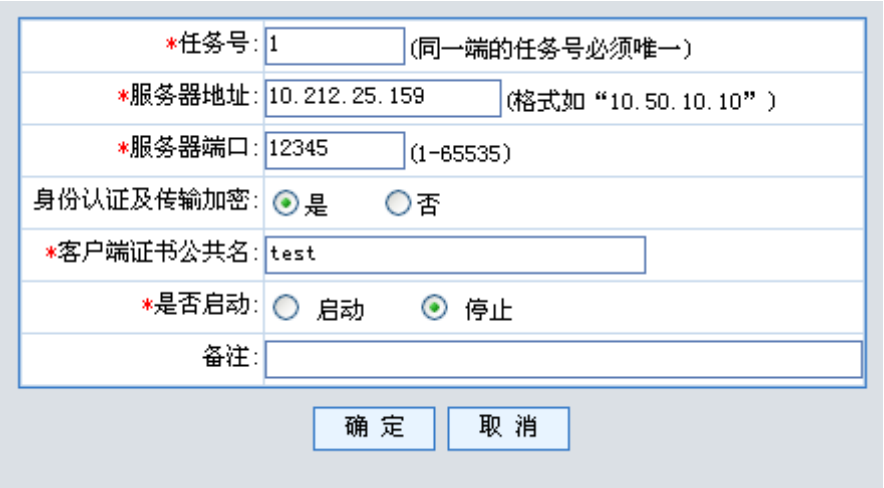


图 9 9 编辑服务端任务

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后面的删除图标，弹出编辑窗口，如下图：

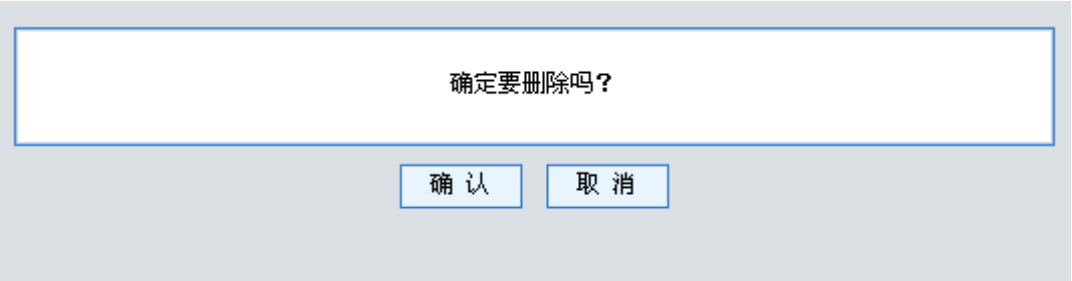


图 9 10 删除服务端任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

第 10 章　安全浏览

该模块支持用户通过浏览器访问 Internet，提供普通和透明两种模式。普通模式需要用户客户端配置代理服务器，代理服务器的地址和端口即网闸的地址和服务端口，透明模式客户端不需要任何配置。WEB 界面导航菜单如下：

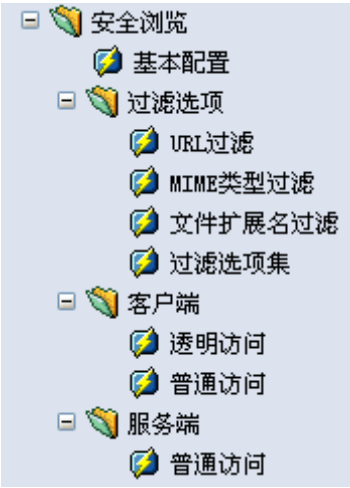


图 10　1 安全浏览 WEB 界面导航菜单

10.1 基本配置

“基本配置”部分，用于配置安全浏览任务的基本参数，目前仅包括“当前服务状态”参数。WEB 界面示意图如下：

图 10　2 基本配置界面

参数说明如下表：

表 10　1　基本配置参数说明

参数名称	参数描述
当前服务状态	表示安全浏览任务的系统运行状态。若为“启动服务”，则表示当前所有任务已处于可运行状态，在此状态下，任务一旦添加且单独启停按钮为“启动”时，任务随即运行；若为“停止服务”，即使添加了任务且单独启停按钮为“启动”，任务也不运行。 服务状态值：“启动服务”或“停止服务”。

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

10.2 过滤选项

该部分用于所有与安全浏览中与内容过滤有关的配置，这些设置主要用于保护内网的上网用户不受危险页面的侵害，以及对内网用户上网所浏览内容的控制，这个部分包括：URL 过滤，MIME 类型过滤，文件扩展名过滤和过滤选项集四个子模块。

10.2.1 URL 过滤

该模块用于配置过滤内网用户访问的域名，WEB 界面示意图如下：

图 10 3 URL 过滤列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

图 10 4 添加 URL 过滤列表

图中添加 URL 过滤组的配置项，说明如下：

◆ **名称**

URL 过滤组名称，名称必须唯一且不能为空。

◆ **URL 过滤列表**

添加需要过滤的域名，多个域名之间用逗号","分割。内网用户能否访问被过滤域名，取决于过滤选项集中的 URL 过滤动作，具体参见 9.2.4 “过滤选项集”。域名前加"."表示包括该域名及其子域名，否则表示只包括该域名。比如：*.sina.com.cn 表示包括 www.sina.com.cn 的同时也包括了 news.sina.com.cn, sports.sina.com.cn 等等子域名。

◆ **备注**

该 URL 的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个 URL 后面的编辑图标，弹出编辑窗口，如下图：

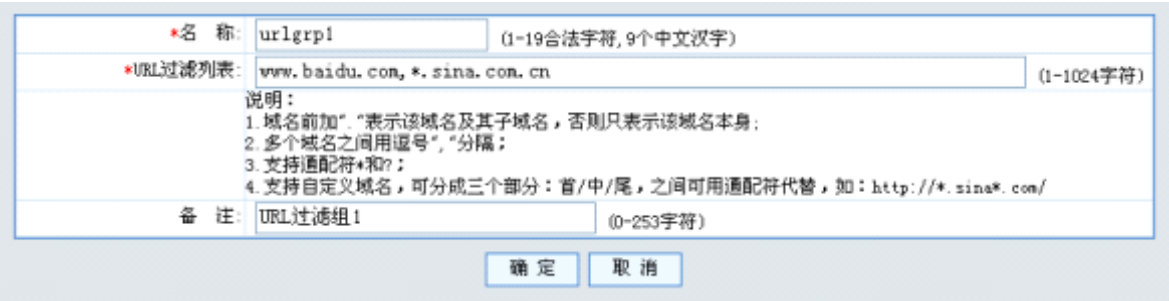


图 10 5 编辑 URL 过滤列表

编辑操作时，除名称不能修改外，其他与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个 URL 过滤组后面的删除图标，弹出编辑窗口，如下图：

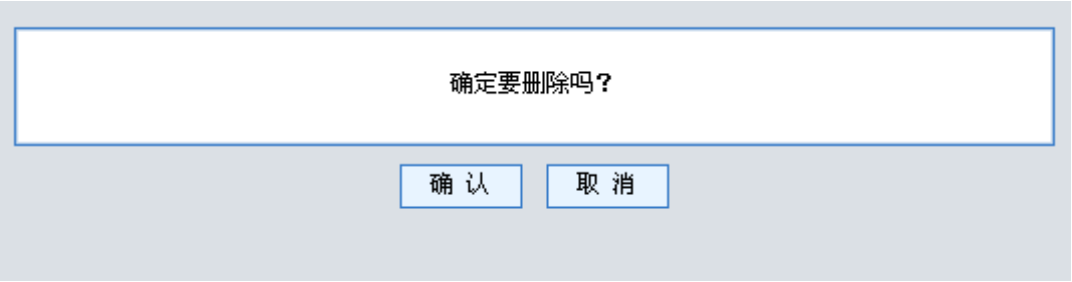


图 10 6 删除 URL 过滤列表

点击“确认”按钮，删除该 URL 过滤组；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

10.2.2 MIME 类型过滤

该模块用于配置用于过滤 Internet 上的各种 MIME 类型，WEB 界面示意图如下：

图 10 7 MIME 类型过滤配置界面

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

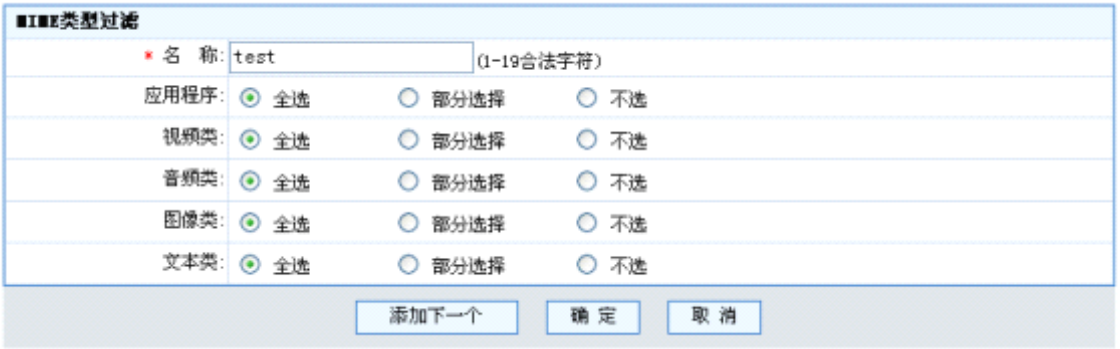


图 10 8 添加 MIME 类型过滤

图中添加用户的配置项，说明如下：

◆ **名称**

当前 MIME 类型过滤名称，名称必须唯一且不能为空。

◆ **过滤选项**

过滤分为“应用程序”，“视频类”，“音频类”，“图像类”和“文本类”五种类型，用户可以根据提供的选项选择不同的 MIME 类型，被选中的 MIME 类型是否被允许或者被禁止取决于过滤选项集中 MIME 类型的动作设置，具体参见 9.2.4“过滤选项集”：

✧ **全选**

如果选择“全选”方式，则所有的 MIME 类型都被选中。通过“部分选择”可以查看所有的可过滤类型。（见“部分选择”项）

✧ **不选**

如果选择“不选”方式，则所有的 MIME 类型都不被选中。通过“部分选择”可以查看所有的可过滤类型。（见“部分选择”项）

✧ **部分选择**

如果选择“部分选择”方式，则在选择“部分选择”之后可选择的 MIME 类型会展开，界面见下图：

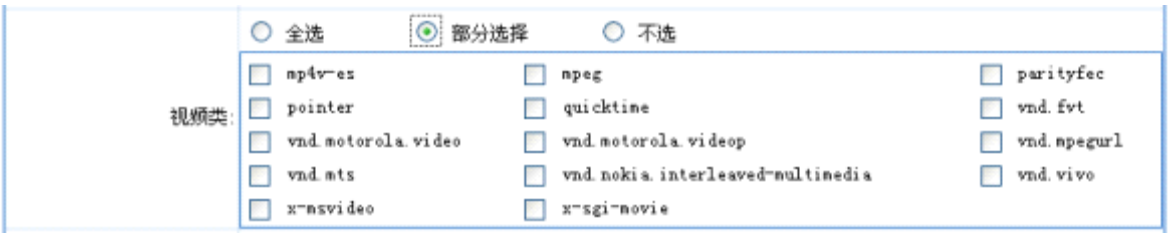


图 10 9 部分选择展开界面

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个 MIME 类型后面的编辑图标，弹出编辑窗口，如下图：

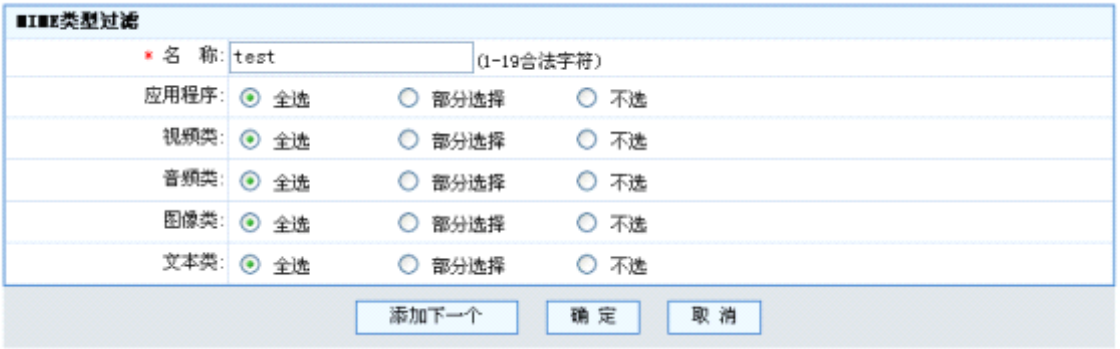


图 10 10 编辑 MIME 类型过滤

编辑操作与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个 MIME 类型后面的删除图标，弹出编辑窗口，如下图：

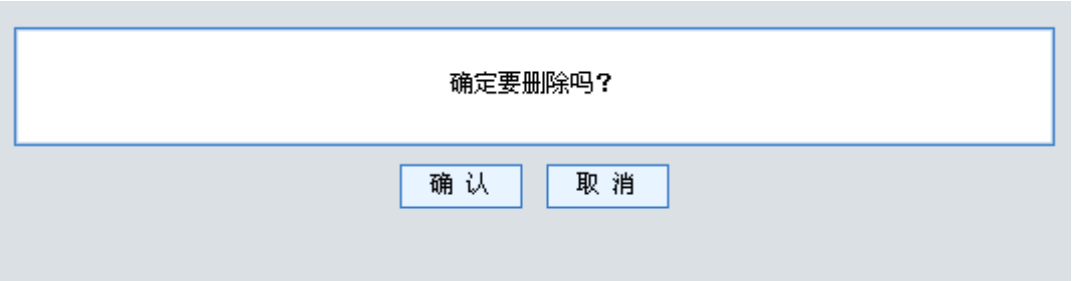


图 10 11 删除 MIME 类型过滤

点击“确认”按钮，删除该 MIME 类型；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

10.2.3 文件扩展名过滤

该模块用于过滤内网用户访问的文件扩展名过滤组，WEB 界面示意图如下：

图 10　12　文件扩展名过滤列表显示

该模块主要包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

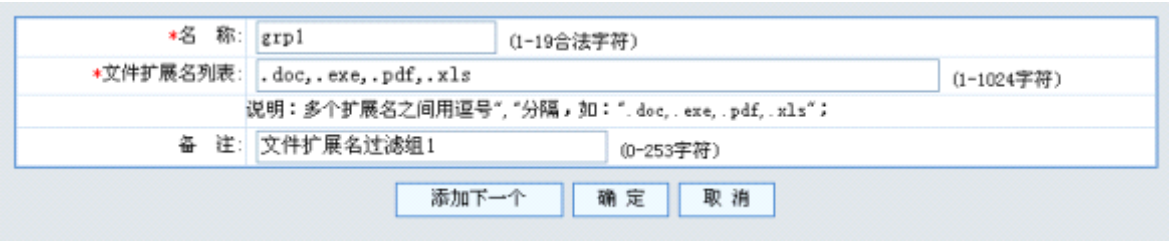


图 10　13　添加文件扩展名过滤列表

图中添加文件扩展名过滤组的配置项，说明如下：

◆　**名称**

当前文件扩展名过滤组名称，名称必须唯一且不能为空。

◆　**文件扩展名列表**

设置需要过滤的文件扩展名，多个扩展名之间用逗号""隔开，如配置：".doc,.exe"，内网用户能否访问被过滤扩展名的文件，取决于过滤选项集中的文件扩展名过滤动作，具体参见 9.2.4“过滤选项集”。

◆　**备注**

该文件扩展名过滤组的备注或说明。文件扩展名不支持通配符。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2)　修改操作

在列表显示图中，点击列表中每个文件扩展名过滤组后面的编辑图标，弹出编辑窗口，如

下图：

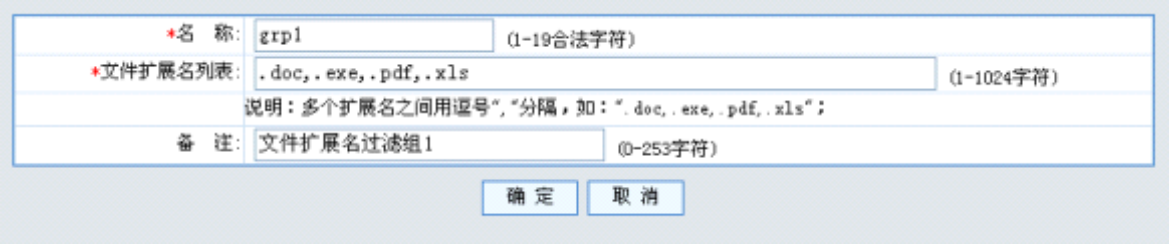


图 10 14 编辑文件扩展名过滤列表

编辑操作时，除名称不能修改外，其他与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个文件扩展名过滤组后面的删除图标，弹出编辑窗口，如下图：

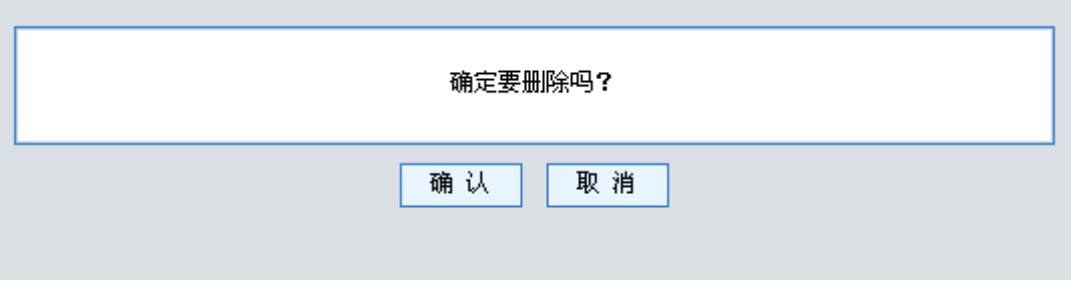


图 10 15 删除文件扩展名过滤列表

点击“确认”按钮，删除该文件扩展名过滤组；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

10.2.4 过滤选项集

“过滤选项集”部分，用于 HTTP 协议过滤，包括 HTTP 请求方法限制，URL 过滤，MIME 类型，文件扩展名过滤，病毒扫描，缓存文件上限，HTTP 协议头部长度上限，用于实现安全浏览模块的安全控制。WEB 界面示意图如下：

图 10　16　过滤选项集界面

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

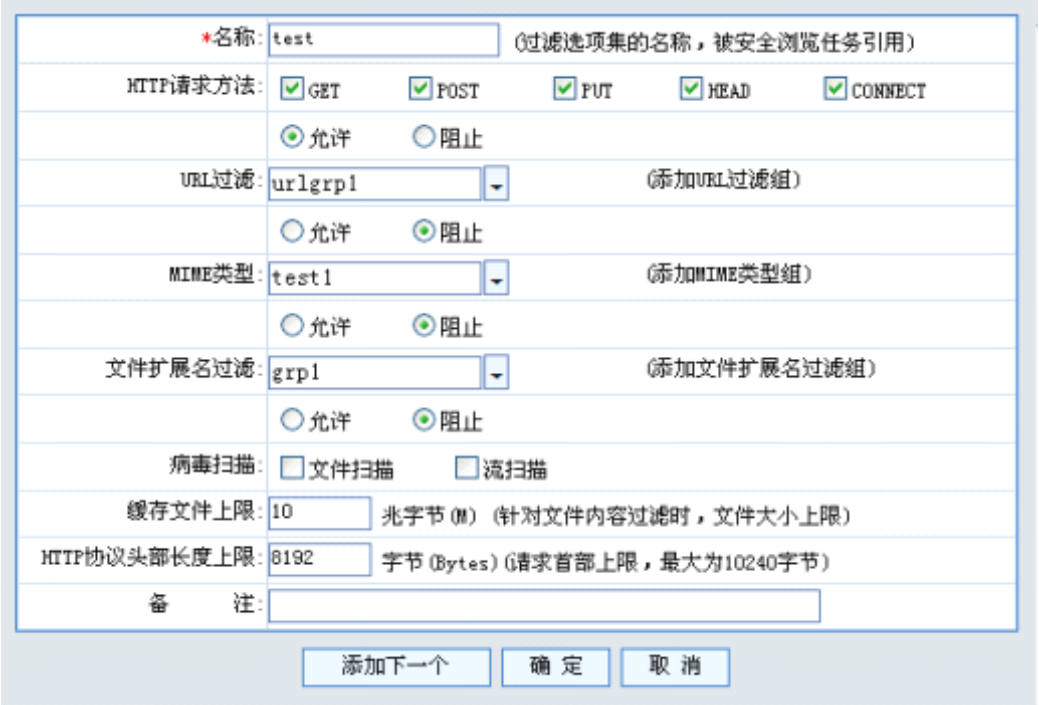


图 10　18　过滤选项集列表显示

图中过滤选项的配置项，说明如下：

◆ **名称**

为当前过滤选项集规定一个名称，名称必须唯一且不能为空。

◆ **HTTP 请求方法**

规则允许或者阻止的 HTTP 方法，分别为 GET、POST、PUT、HEAD、CONNECT 等，WEB 界面示意图如下：

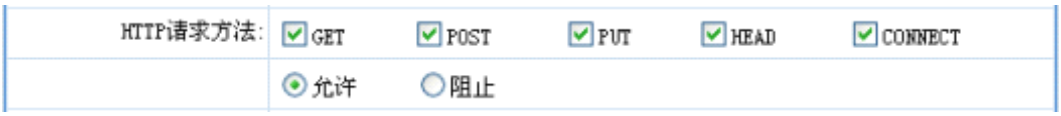


图 10-19 HTTP 请求方法配置选项

参数说明如下表：

表 10 2 设置 HTTP 请求方法参数说明

参数名称	描述
允许	选中此项则允许上面命令列表中被选中的 HTTP 请求方法。
阻止	选中此项则阻止下面命令列表中被选中的 HTTP 请求方法。

◆ **URL 过滤**

该模块用于选择允许或者阻止的 URL 过滤组。WEB 界面示意图如下：

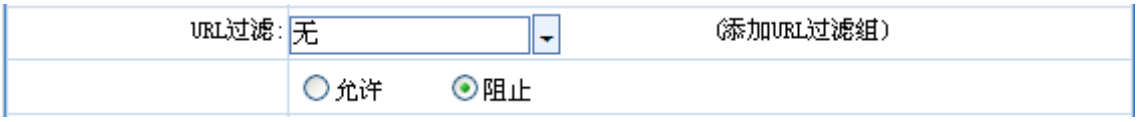


图 10-20 URL 过滤配置选项

参数说明如下表：

表 9 3 设置命令控制参数说明

参数名称	描述
URL 过滤	其值从下拉列表中选取即可，可以为空。其菜单项来源于“URL 过滤”中定义的 URL 过滤组。
允许	选中此项则该组中的各个 URL 在访问网闸时允许通过， 不在该组中的 URL 则禁止通过。
阻止	选中此项则该组中的各个 URL 在访问网闸时禁止通过， 不在该组中的 URL 则允许通过。

◆ **MIME 类型**

该模块用于选择允许或阻止的 MIME 类型过滤组。WEB 界面示意图如下：

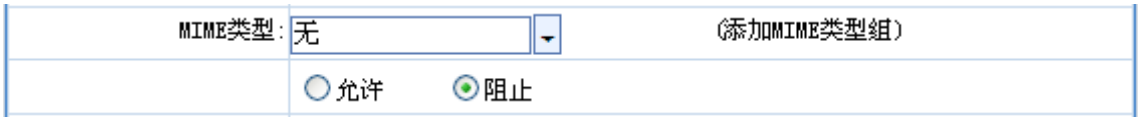


图 10-21 MIME 类型配置选项

参数说明如下表：

表 10 4 设置 MIME 类型参数说明

参数名称	描述

MIME 类型	其值从下拉列表中选取即可，但不能为空，可以选取“无”菜单选项，默认为“无”。其菜单项来源于“MIME 类型过滤”中定义的 MIME 类型过滤组。
允许	选中此项则该组中的各个 MIME 类型在访问网闸时动作为不禁止，若文件病毒扫描关闭，则直接放行；若文件病毒扫描开启，则进行文件缓存。不在该组中的 MIME 类型则禁止通过。
阻止	选中此项则该组中的各个 MIME 类型在访问网闸时禁止通过， 不在该组中的 MIME 类型则动作为不禁止，若文件病毒扫描关闭，则直接放行；若文件病毒扫描开启，则进行文件缓存。

◆ **文件扩展名过滤**

该模块用于选择允许或阻止的文件扩展名过滤组。WEB 界面示意图如下：

图 10-22 文件扩展名配置选项

参数说明如下表：

表 10　5 设置文件扩展名参数说明

参数名称	描述
文件扩展名过滤	其值从下拉列表中选取即可，但不能为空，可以选取“无”菜单选项，默认为“无”。其菜单项来源于“文件扩展名过滤”中定义的文件扩展名过滤组。
允许	选中此项则该组中的文件扩展名在访问网闸时动作为不禁止，若文件病毒扫描关闭，则直接放行；若文件病毒扫描开启，则进行文件缓存。不在该组中的文件扩展名则禁止通过。
阻止	选中此项则该组中的文件扩展名在访问网闸时禁止通过， 不在该组中的文件扩展名则动作为不禁止，若文件病毒扫描关闭，则直接放行；若文件病毒扫描开启，则进行文件缓存。

◆ **病毒扫描**

该选项用于配置病毒扫描。WEB 界面示意图如下：

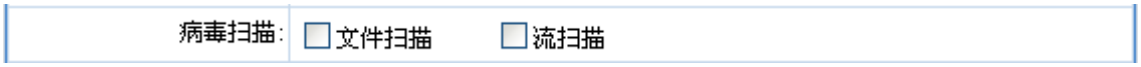


图 10-23 病毒扫描配置选项

参数说明如下表：

表 10　6 设置病毒扫描参数说明

参数名称	描述
文件扫描	选中该选项则将文件存储在缓冲区中，进行文件扫描。默认不选中。
流扫描	选中该选项则在 socket 中创建 buffer，对 HTTP 传输流进行扫描。默认为不选中。

◆ **缓存文件上限**

该模块用于配置进行文件扫描时文件缓冲区的大小，单位为兆字节（M）。WEB 界面示意图如下：

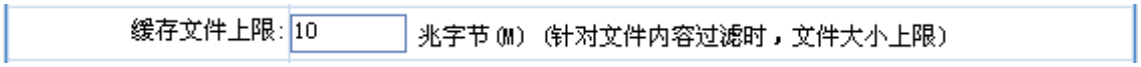


图 10-24 缓存文件上限配置选项

◆ **HTTP 协议头部长度上限**

该模块用于配置 HTTP 协议头部长度上限，单位为字节（Bytes）， 界面上提供了默认值 8192 字节。WEB 界面示意图如下：

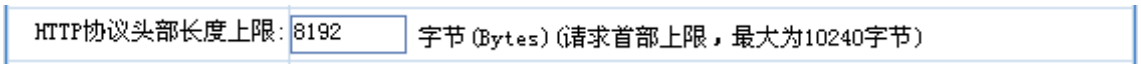


图 10　25　　HTTP 协议头部长度上限配置选项

◆ **备注**

该文件扩展名的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个过滤选项集后面的编辑图标，弹出编辑窗口，如下图：

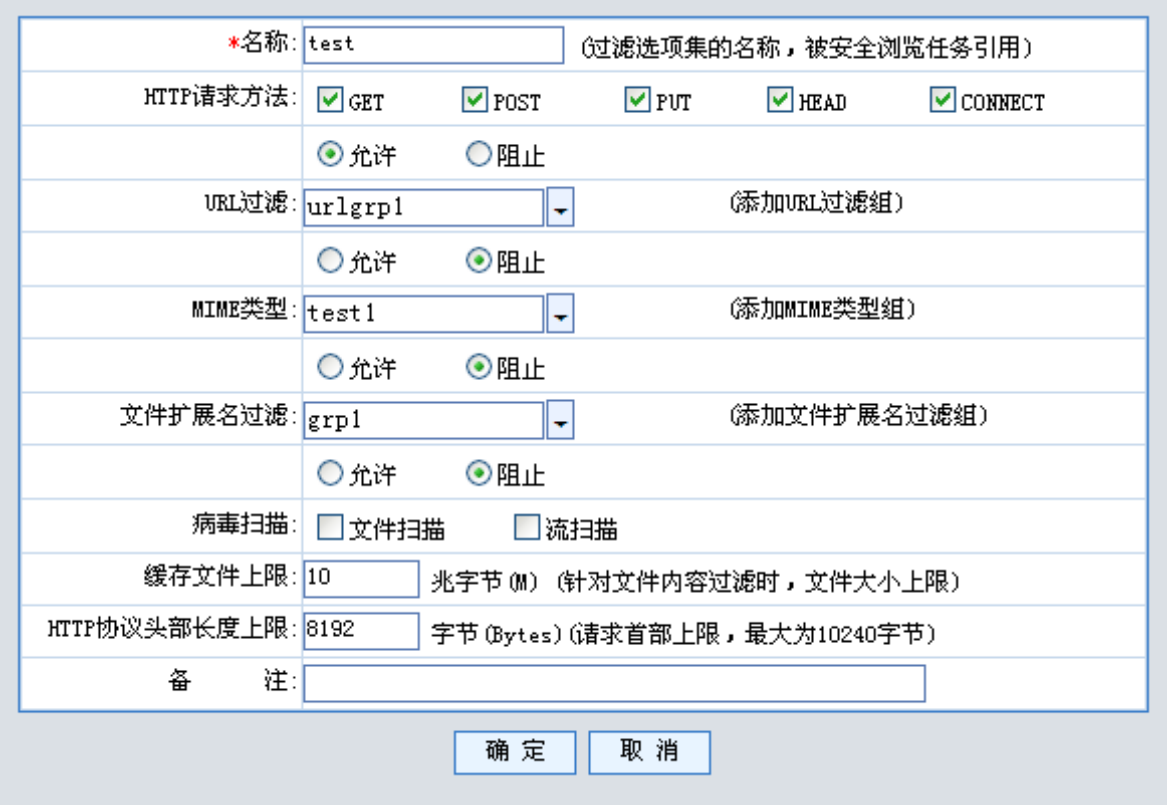


图 10 26 编辑安全浏览过滤选项集

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个过滤选项集后面的删除图标，弹出编辑窗口，如下图：

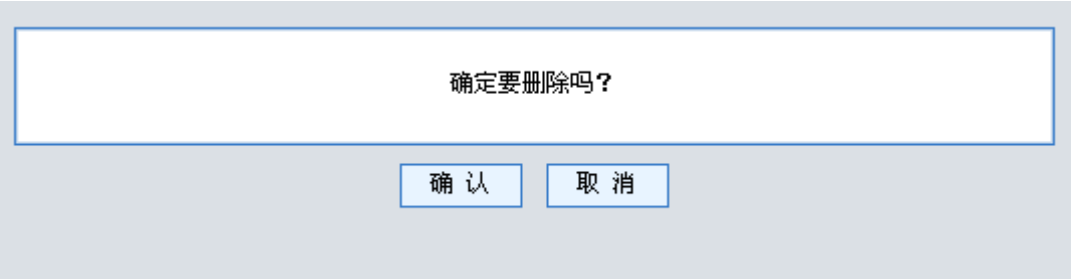


图 10 27 删除安全浏览过滤选项集

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

10.3 客户端

该部分用于配置所有的安全浏览客户端的访问任务，包括：透明模式的客户端任务、普通模式的客户端任务。普通模式需要用户客户端配置代理服务器，代理服务器的地址和端口即网闸的

地址和服务端口，透明模式客户端不需要任何配置。具体配置依次说明如下：

10.3.1 透明访问

该部分用于配置透明方式的访问控制，对用户上网的源地址、目的地址、访问端口、过滤选项以及上网时段等进行控制。WEB 界面示意图如下：

图 10 28 透明访问列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

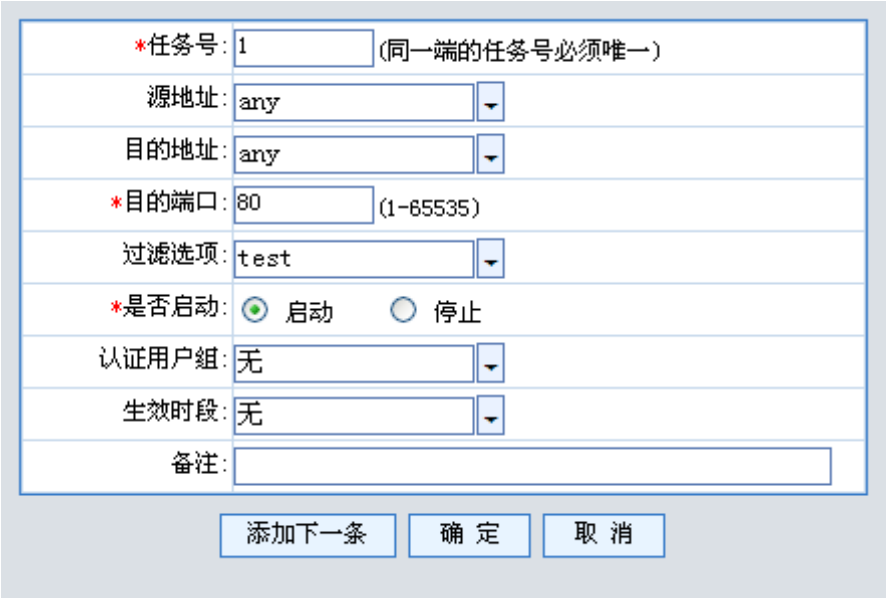


图 10 29 添加透明访问

图中透明访问的配置项，说明如下：

◆ **任务号**

任务号是安全浏览的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则安全浏览无法正常连接。

任务号只用数字表示，该配置项必填。

◆ **源地址**

源地址指出允许访问通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、域名地址等四类地址。

◆ **目的地址**

目的地址表示被访问的目的服务器的 IP 地址或域名。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的端口**

目的端口指被访问的目的服务器的真实端口。

取值范围：1－65535，默认为 80 端口。

该配置项必填。

◆ **过滤选项**

设置该浏览应用的过滤选项。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

其菜单项来源于“过滤选项”中定义的过滤选项集。

◆ **是否启动**

该选项用于设置是否启动本访问规则。默认为“启动”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该条访问控制规则在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个透明访问规则后面的编辑图标，弹出编辑窗口，如下图：

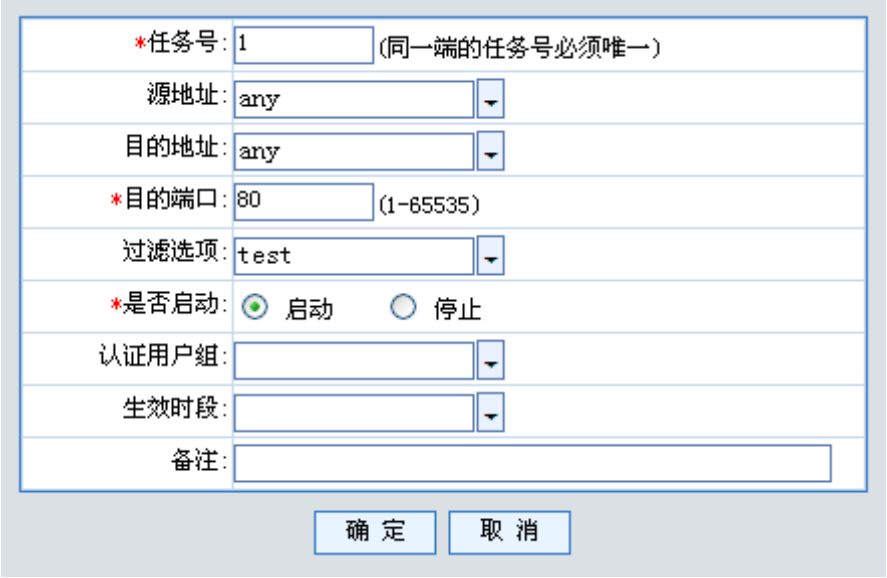


图 10 30 编辑透明访问

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个透明访问规则后面的删除图标，弹出编辑窗口，如下图：

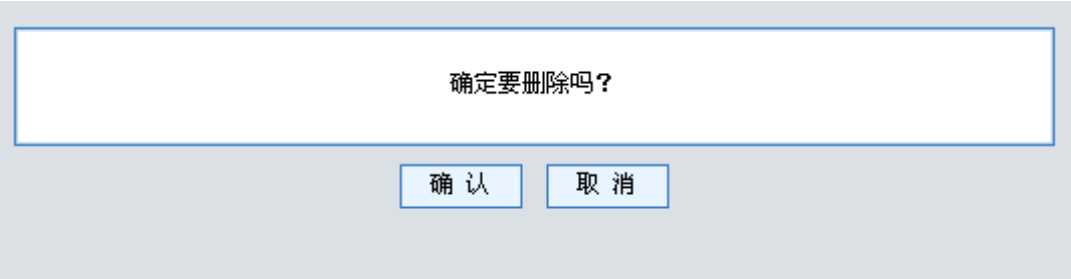


图 10 31 删除透明访问

点击“确认”按钮，删除该透明访问规则；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

10.3.2 普通访问

该部分用于配置普通方式的访问控制，对用户上网的源地址、目的地址、访问端口以及上网时段等进行控制。WEB 界面示意图如下：

图 10　32　普通访问列表显示

该模块主要包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

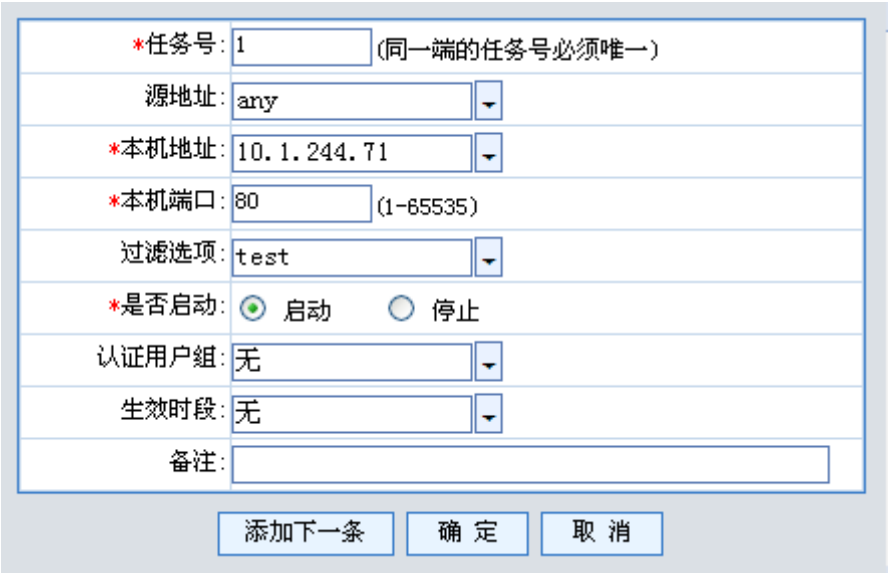


图 10　33　添加普通访问

图中普通访问的配置项，说明如下：

◆　**任务号**

任务号是安全浏览的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则安全浏览无法正常连接。

任务号只用数字表示，该配置项必填。

◆　**源地址**

源地址指出允许访问通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、

地址组、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置“>>”网络设备”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535，默认为 21 端口。

该配置项为必填项。

◆ **过滤选项**

设置该浏览应用的过滤选项。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

其菜单项来源于“过滤选项”中定义的过滤选项集。

◆ **是否启动**

该选项用于设置是否启动本访问规则。默认为“启动”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该条访问控制规则在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个普通访问规则的编辑图标，弹出编辑窗口，如下图：

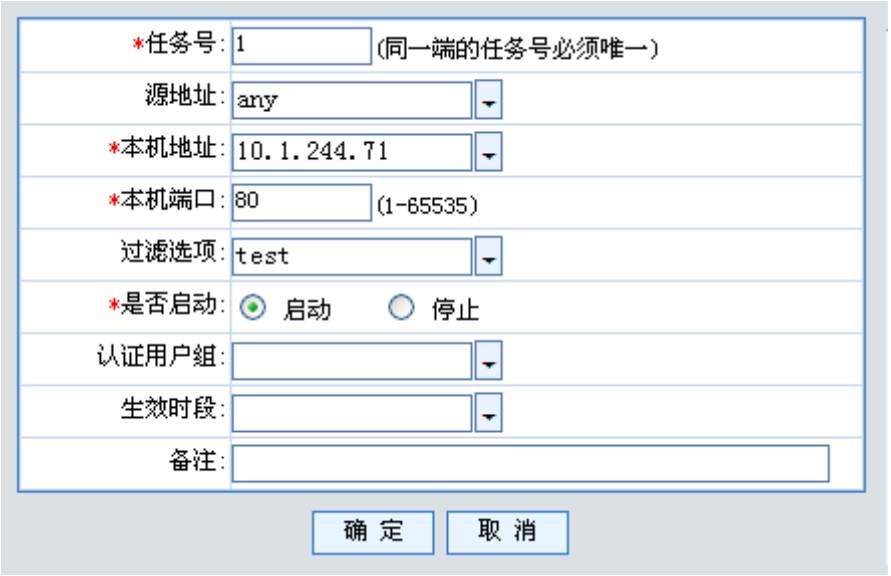


图 10 34 编辑普通访问

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个普通访问规则的删除图标，弹出编辑窗口，如下图：

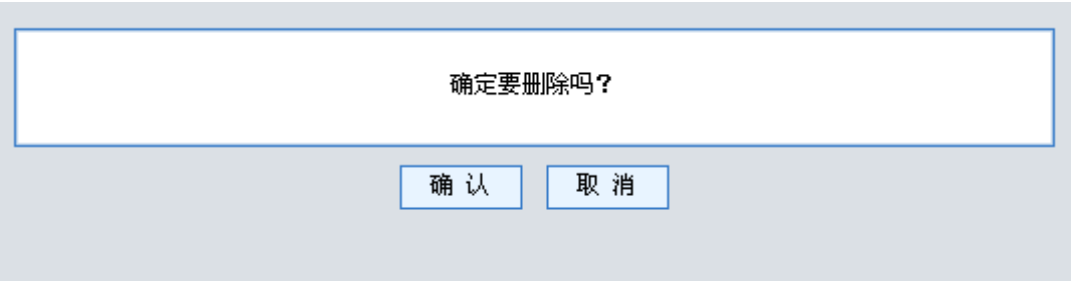


图 10 35 删除普通访问

点击“确认”按钮，删除该普通访问规则；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

10.4 服务端

该部分用于配置安全浏览服务端的访问任务。特别指出的是，与客户端不同，服务端只需配置普通模式下的访问任务，对于透明模式的服务端任务，系统内部已经配置好，无需用户配置。

10.4.1 普通访问

普通访问 WEB 界面导航菜单如下：

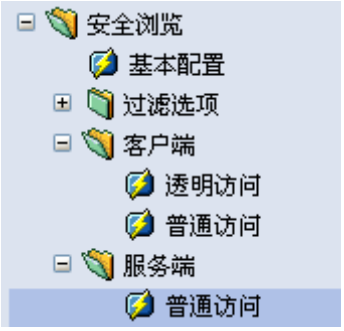


图 10　36　安全浏览服务端导航菜单

下面详细介绍服务端的普通模式的任务配置：WEB 界面显示如下：

图 10　37　安全浏览服务端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

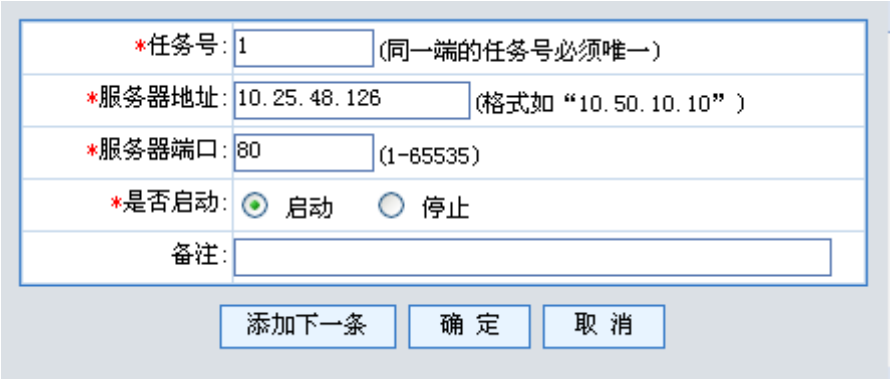


图 10　38　添加安全浏览服务端普通任务

图中安全浏览普通模式的服务端任务的配置项，说明如下：

◆　**任务号**

任务号是客户端正常访问的基础，所以一个服务端任务的任务号必须与对方主机模块中相对应的客户端任务的任务号完全相同，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号,而且，在整个安全浏览模块内必须唯一。

该配置项必填。

◆ **服务器地址**

服务器地址为目标访问网络中的邮件服务器的真实 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也不能为 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问网络中的邮件服务器的真实端口。

取值范围：1－65535。

该配置项为必填项。

◆ **是否启用**

该选项用于选择是否启用客户端任务，默认为不启用。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

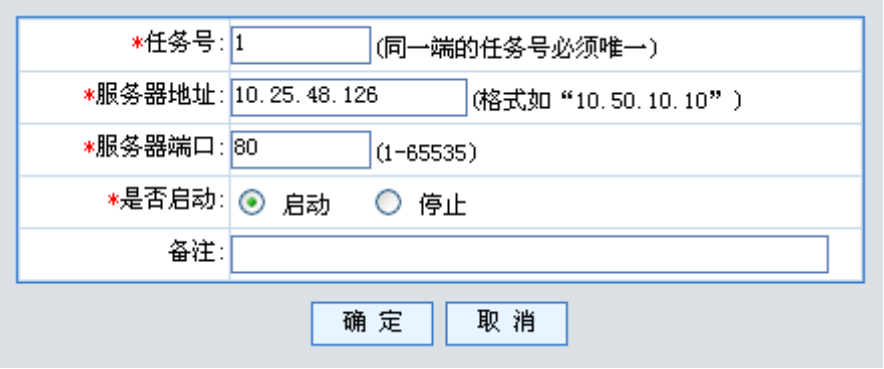


图 10 39 编辑安全浏览服务端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

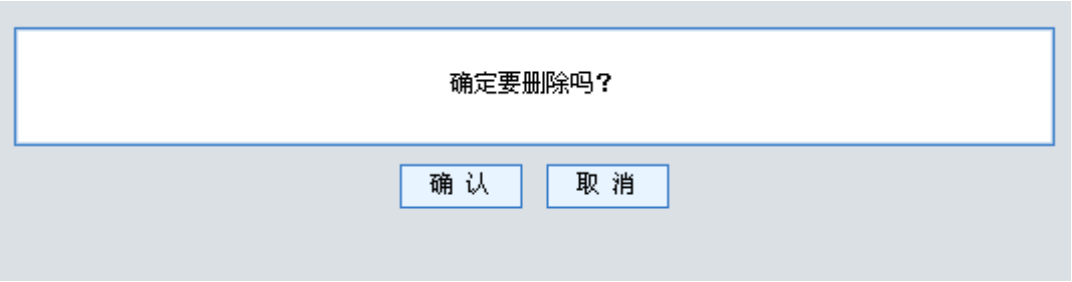


图 10　40　删除安全浏览服务端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

第 11 章 FTP 访问

FTP 访问模块支持一侧网络用户通过 SIS 安全隔离网闸访问另一侧网络的 FTP 服务器。整个模块由三个部分组成：FTP 客户端系统、网闸系统、FTP 服务器端系统。其中，FTP 客户端和服务器支持各种通用服务器。在此，主要介绍网闸系统的操作说明。其 WEB 界面导航菜单如下：

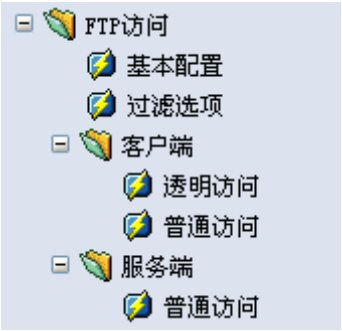


图 11 1 FTP 访问 WEB 界面导航菜单

11.1 基本配置

“基本配置”部分，用于配置 FTP 访问任务的基本参数，目前仅包括“当前服务状态”参数。WEB 界面示意图如下：

图 11 2 基本配置界面

参数说明如下表：

表 11 1 基本配置参数说明

参数名称	参数描述
当前服务状态	表示 FTP 访问任务的系统运行状态。若为“启动服务”，则表示当前所有任务已处于可运行状态，在此状态下，任务一旦添加且单独启停按钮为“启动”

	时，任务随即运行；若为“停止服务”，即使添加了任务且单独启停按钮为“启动”，任务也不运行。 服务状态值：“启动服务”或“停止服务”。

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

其他参数，配置完毕后，点击“确定”即可。

11.2 过滤选项

“过滤选项”部分，用于内容过滤，包括用户控制、命令控制、上传控制、下载控制、缓存控制、Banner 保护，用于实现 FTP 访问模块的安全控制。WEB 界面示意图如下：

图 11 3 过滤选项界面

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

图 11 4 过滤选项列表显示

图中过滤选项的配置项，说明如下：

◆ **名称**

为当前过滤选项规定一个名称，名称必须唯一。

◆ **用户控制**

对通过 SIS 安全隔离网闸进行 FTP 访问用户的用户名进行控制，可以选择设置阻止访问的用户名或允许访问的用户名两种控制模式。WEB 界面示意图如下：

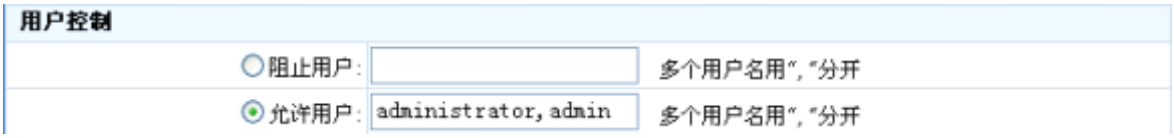


图 11-5 用户控制配置选项

参数说明如下表：

表 11 2 设置用户控制参数说明

参数名称	描述
阻止用户	选中此项则阻止后面文本框中用户名的用户通过。多个用户名用逗号分开，例如：

	administrator,admin
允许用户	选中此项则允许后面文本框中用户名的用户通过。多个用户名用逗号分开，例如：administrator,admin

◆ **命令控制**

该模块用于配置允许或禁止 FTP 的协议命令。WEB 界面示意图如下：

图 11-6 命令控制配置选项

参数说明如下表：

表 11 3 设置命令控制参数说明

参数名称	描述
禁止命令	选中此项则阻止下面命令列表中被选中的 FTP 客户端命令。
允许命令	选中此项则允许下面命令列表中被选中的 FTP 客户端命令。

◆ **上传控制**

该模块用于配置允许或禁止上传的文件类型。WEB 界面示意图如下：

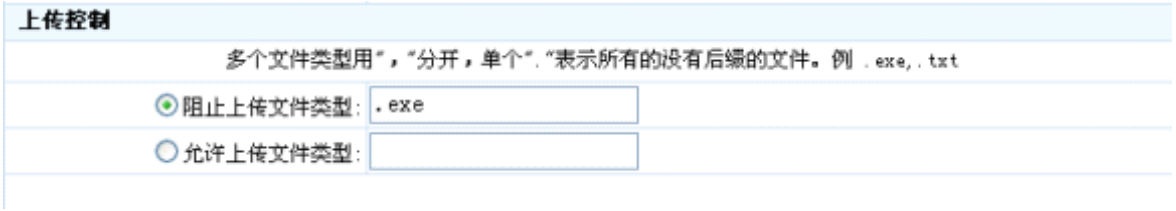


图 11-7 上传控制配置选项

参数说明如下表：

表 11 4 设置上传控制参数说明

参数名称	描述
阻止上传文件类型	选中此项则阻止上传后面文本框中的文件类型的文件。
允许上传文件类型	选中此项则允许上传后面文本框中的文件类型的文件。

特别指出:

每个文件类型必须以“.”开头，文件类型中不能包括以下字符：\ / : * ? " < > | ' % 。多个文件类型用","分开，只有“.”表示所有的没有后缀的文件。例 .exe, .txt

◆ **下载控制**

该模块用于配置允许或禁止下载的文件类型。WEB 界面示意图如下：

图 11-8 下载控制配置选项

参数说明如下表：

表 11 5 设置下载控制参数说明

参数名称	描述
阻止下载文件类型	选中此项则阻止下载后面文本框中的文件类型的文件。
允许下载文件类型	选中此项则允许下载后面文本框中的文件类型的文件。

特别指出:

每个文件类型必须以“.”开头，文件类型中不能包括以下字符：\ / : * ? ″ < > | ’ % 。多个文件类型用″,″分开，只有“.”表示所有的没有后缀的文件。例 .exe, .txt

◆ **缓存控制**

该选项用于配置缓存。WEB 界面示意图如下：

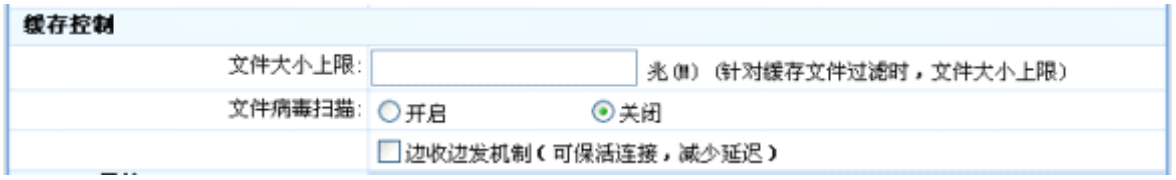


图 11-9 缓存控制配置选项

参数说明如下表：

表 11 6 设置缓存控制参数说明

参数名称	描述
文件大小上限	此项用于设置文件大小上限，单位为 MB。
文件病毒扫描	此项用于设置是否在文件的传输过程中对文件进行病毒扫描，默认选中“关闭”。
边收边发机制	此项用于设置是否启用边收边发机制，该机制可保活连接，减少延迟，默认不选中。

◆ **Banner 保护**

该模块用于配置 Banner 保护信息，替换 Banner 信息可以防止 FTP 服务器版本信息的泄露，减少针对特定版本服务器漏洞的攻击。WEB 界面示意图如下：

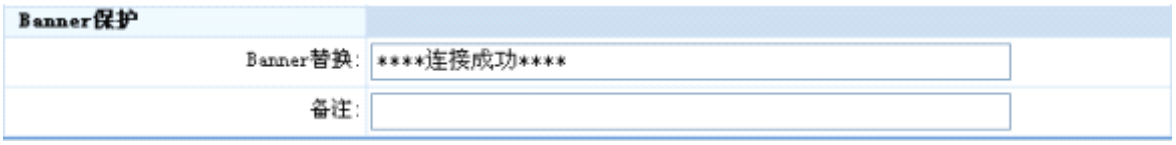


图 11-10 Banner 保护配置选项

参数说明如下表：

表 11 7 设置 Banner 保护参数说明

参数名称	描述
Banner 替换	此项用于设置 Banner 替换为的内容，默认为空。
备注	该任务的备注或说明。

设置完各配置项后，点击“确定”，添加成功，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后面的编辑图标，弹出编辑窗口，如下图：

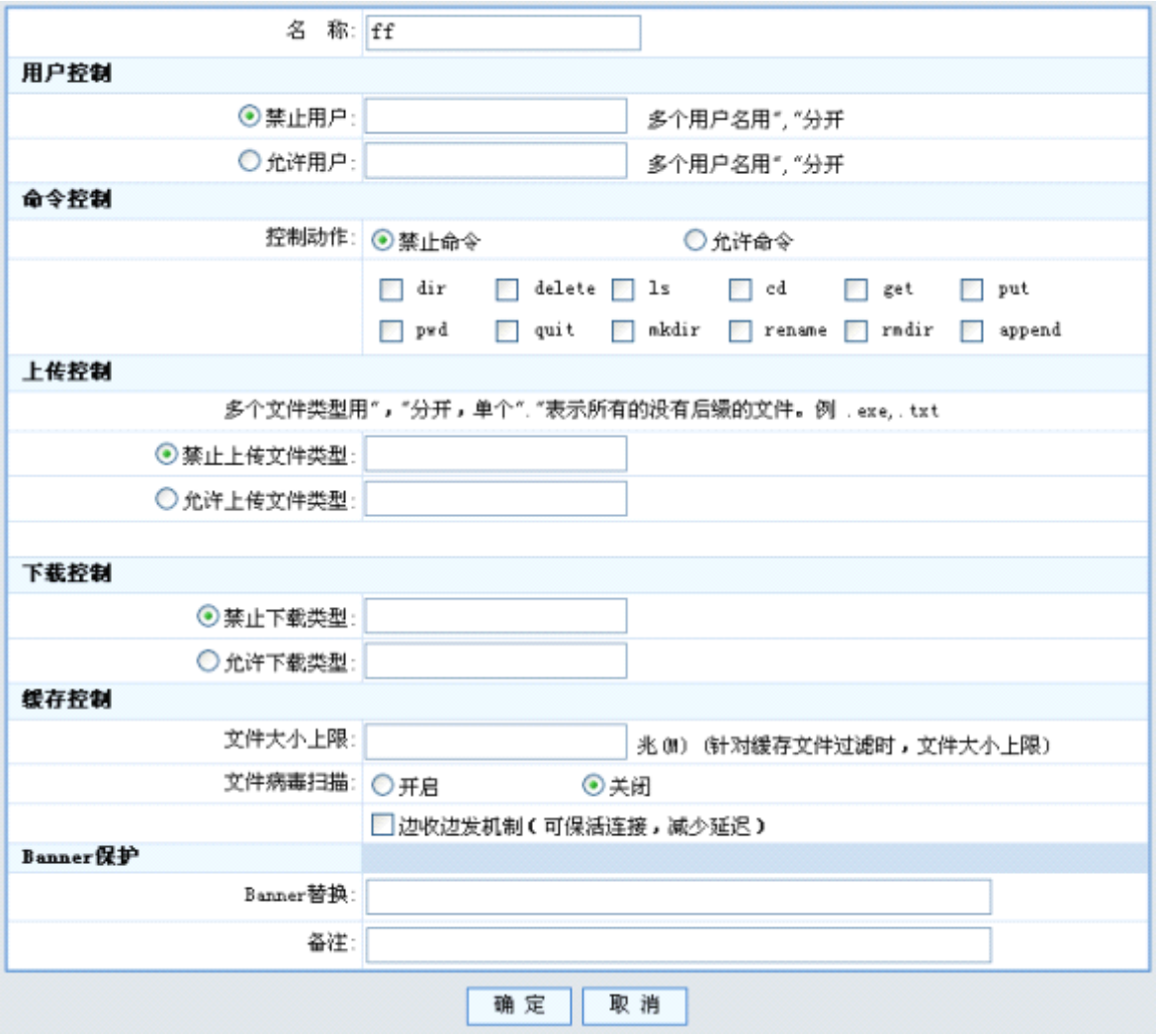


图 11-11 编辑 FTP 过滤选项

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后面的删除图标，弹出编辑窗口，如下图：

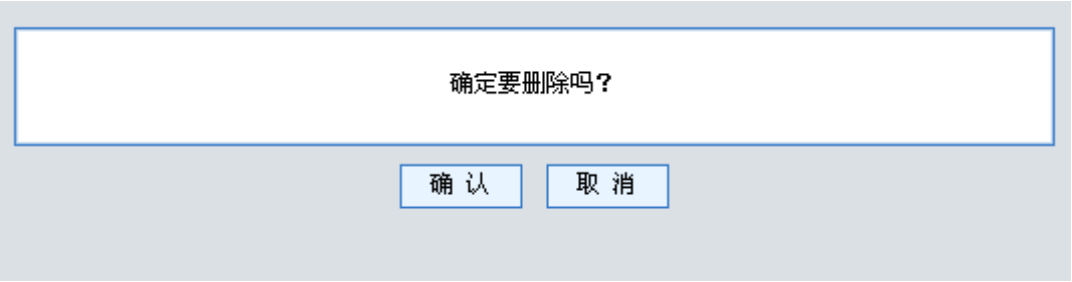


图 11-12 删除 FTP 过滤选项

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

11.3 客户端

该部分用于配置所有的 FTP 客户端的访问任务，包括：透明模式的客户端任务、普通模式的客户端任务。采用透明方式访问时，用户直接访问 FTP 服务器的地址，用户名和口令按照正常方式输入既可。采用普通模式访问时，用户访问的是网闸的地址，用户名和口令也按照正常方式输入，网闸应该连接的服务器地址填入普通访问任务中的 ftp 地址处。

具体配置依次说明如下：

11.3.1 透明访问

该部分用于配置透明方式的 FTP 客户端任务，对用户访问 FTP 服务器的源地址、目的地址、目的端口、过滤选项、生效时段以及是否启用进行控制。WEB 界面示意图如下：

图 11 13 透明访问列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

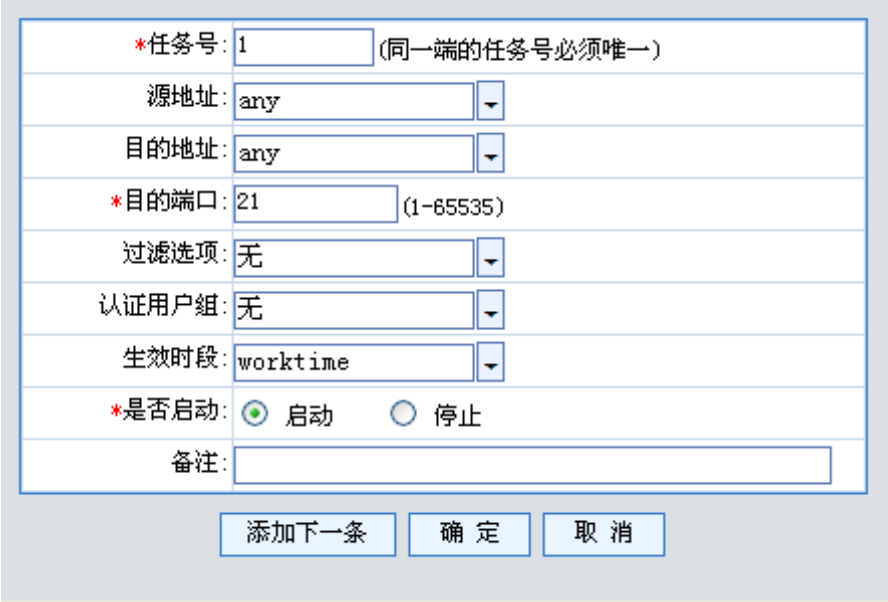


图 11 14 添加透明访问

图中透明访问的配置项，说明如下：

◆ **任务号**

任务号是 FTP 访问的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则 FTP 无法正常连接。

任务号只用数字表示，该配置项必填。

◆ **源地址**

源地址指出允许访问通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、域名地址等。

◆ **目的地址**

目的地址表示被访问的目的服务器的 IP 地址或域名。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的端口**

目的端口指被访问的目的服务器的真实端口。

取值范围：1－65535，默认为 21 端口。

该配置项必填。

◆ **过滤选项**

过滤选项用于指出该客户端任务应用的过滤选项。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“FTP 访问”>>“过滤选项”中的过滤选项。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该条访问控制规则在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **是否启用**

该选项用于选择是否启用客户端任务，默认为不启用。

◆ **备注**

该任务的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个透明访问规则后面的编辑图标，弹出编辑窗口，如下图：

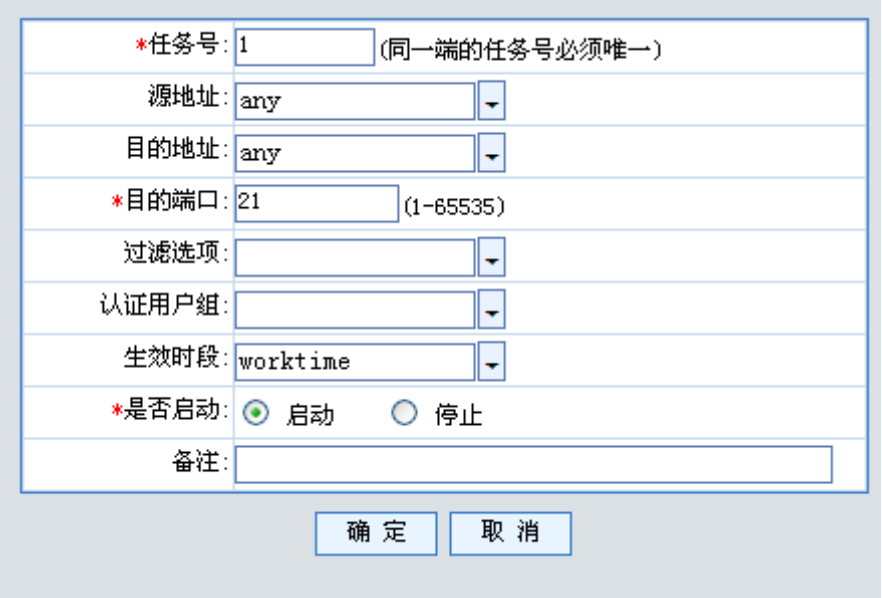


图 11 15 编辑透明访问

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个透明访问规则后面的删除图标🗑，弹出编辑窗口，如下图：

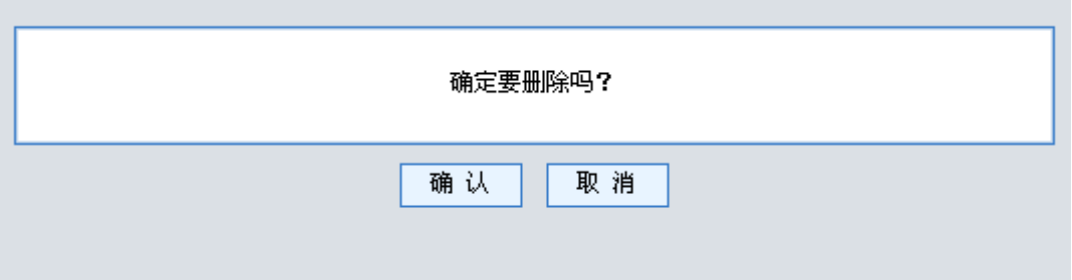


图 11 16 删除透明访问

点击“确认”按钮，删除该透明访问规则；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

11.3.2 普通访问

该部分用于配置普通方式的 FTP 客户端任务，对用户访问 FTP 服务器的源地址本机地址、本机端口、过滤选项、生效时段以及是否启用进行控制。WEB 界面示意图如下：

图 11 17 普通访问列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

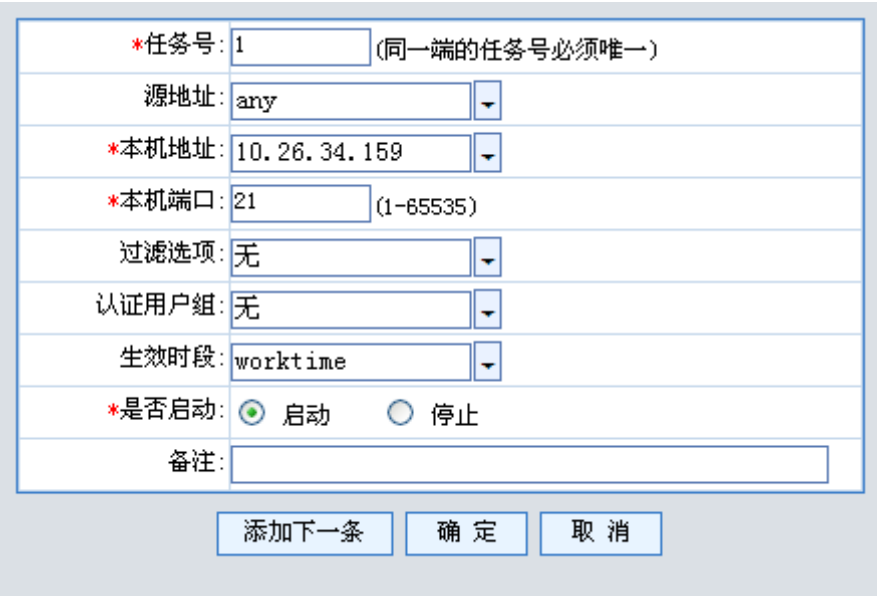


图 11 18 添加普通访问

图中普通访问的配置项，说明如下：

◆ **任务号**

任务号是 FTP 访问的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则 FTP 无法正常连接。

任务号只用数字表示，该配置项必填。

◆ **源地址**

源地址指出允许访问通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置“>>”网络设备”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535，默认为 21 端口。

该配置项为必填项。

◆ **过滤选项**

过滤选项用于指出该客户端任务应用的过滤选项。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“FTP 访问”>>“过滤选项”中的过滤选项。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该条访问控制规则在指定的时间段内生效，其它时间内为失效状态。其值从下拉列表中选取，可以选择“无”，默认为“无”。下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **是否启用**

该选项用于选择是否启用客户端任务，默认为不启用。

◆ **备注**

该任务的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个普通访问规则的编辑图标，弹出编辑窗口，如下图：

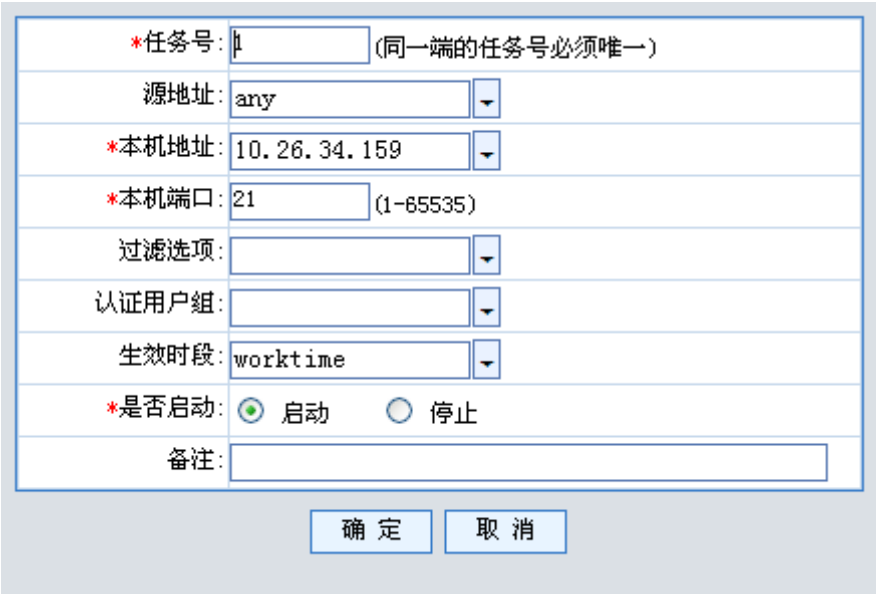


图 11 19 编辑普通访问

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个普通访问规则的删除图标，弹出编辑窗口，如下图：

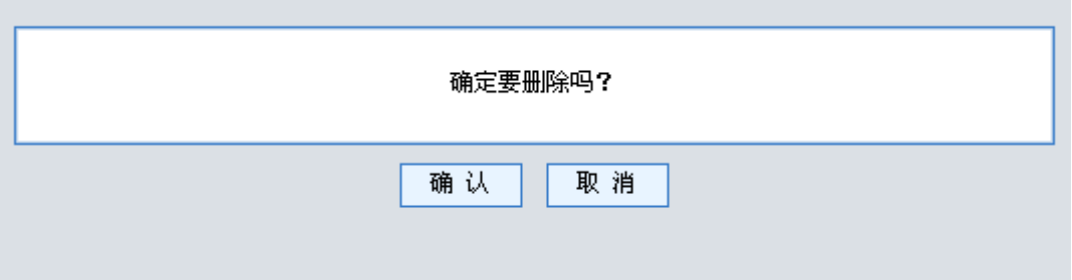


图 11 20 删除普通访问

点击“确认”按钮，删除该普通访问规则；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

11.4 服务端

该部分用于配置所有的 FTP 服务端的访问任务。特别指出的是，与客户端不同，服务端只需配置普通模式下的访问任务，对于透明模式的服务端任务，系统内部已经配置好，无需用户配置。WEB 界面导航菜单如下：

图 11 21 FTP 服务端导航菜单

下面详细介绍服务端的普通模式的任务配置：

11.4.1 普通访问

WEB 界面显示如下：

图 11 22 FTP 服务端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

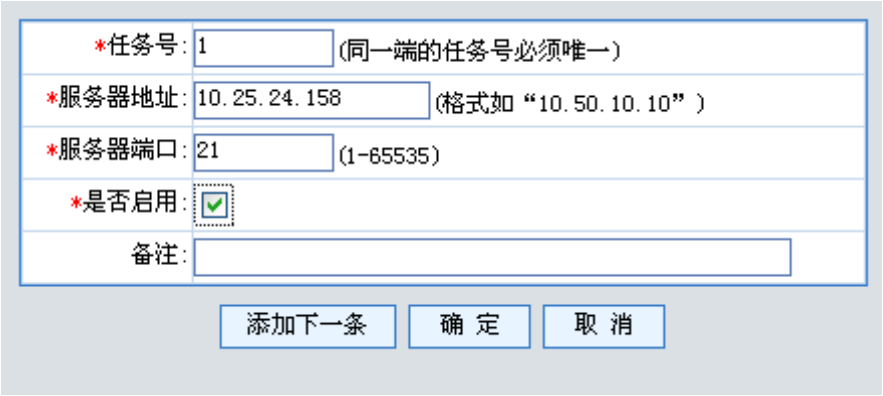


图 11 23 添加 FTP 服务端普通任务

图中 SMTP 普通模式的服务端任务的配置项，说明如下：

◆ **任务号**

任务号是客户端正常访问的基础，所以一个服务端任务的任务号必须与对方主机模块中相对应的客户端任务的任务号完全相同，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号,而且，在整个 FTP 访问模块内必须唯一。

该配置项必填。

◆ **服务器地址**

服务器地址为目标访问网络中的邮件服务器的真实 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也不能为 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问网络中的邮件服务器的真实端口。

取值范围：1－65535。

该配置项为必填项。

◆ **是否启用**

该选项用于选择是否启用客户端任务，默认为不启用。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

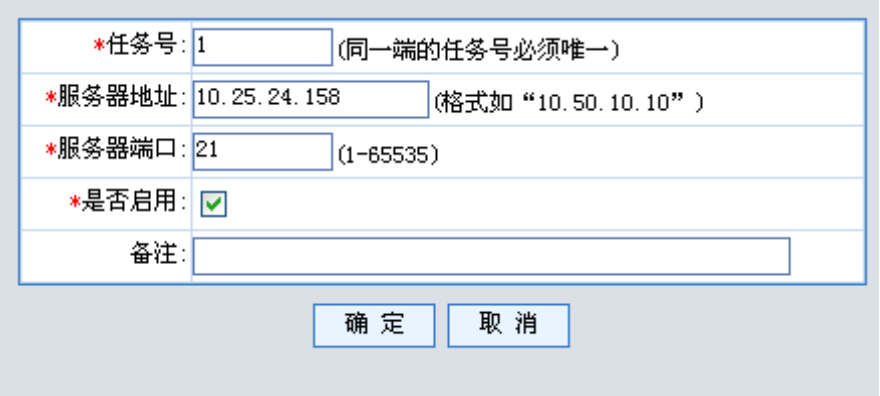


图 11 24 编辑 FTP 服务端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

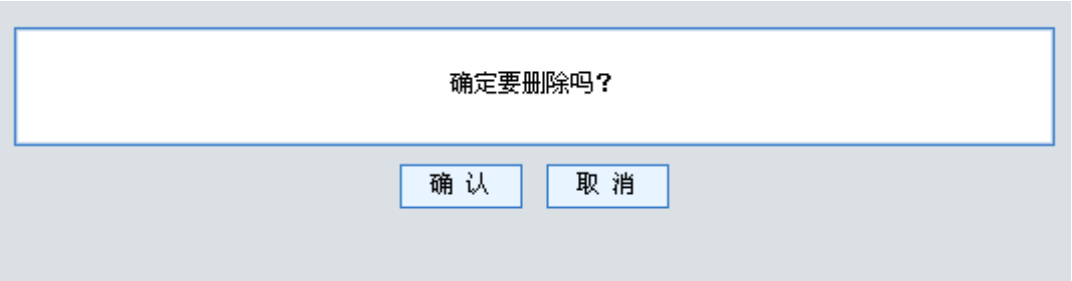


图 11 25 删除 FTP 服务端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

第 12 章　邮件访问

“邮件访问”模块支持一侧网络用户访问另一侧网络的邮件服务器(包括 SMTP 访问和 POP3 访问)。该模块由过滤选项、SMTP 任务配置（包括客户端和服务端）和 POP3 任务配置（包括客户端和服务端）三个部分组成。

12.1 过滤选项

过滤选项用于控制本地用户的邮件访问操作。过滤选项包括邮件地址、内容关键字、附件扩展名以及过滤选项集。其中，邮件地址、内容关键字、附件扩展名可以被过滤选项集引用。WEB 界面导航菜单如下：

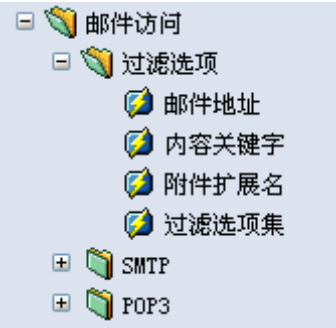


图 12　1　过滤选项 WEB 界面导航菜单

12.1.1　邮件地址

邮件地址，用于对客户端收发邮件的邮件地址进行控制。WEB 界面显示如下：

图 12　2　邮件地址过滤

该模块主要包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

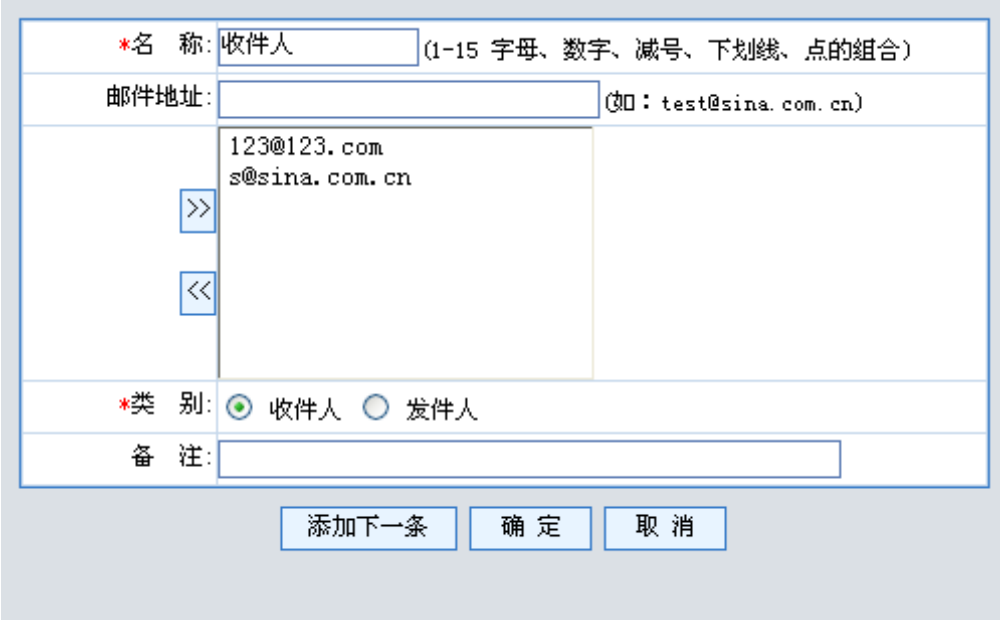


图 12 3 添加邮件地址过滤组

图中邮件地址的配置项，说明如下：

◆ **名称**

邮件地址过滤组名称，可以是 1-15 字母、数字、减号、下划线、点的组合，并且名称必须唯一，不能为空。

◆ **邮件地址**

添加需要过滤的邮件地址。

其格式为“*@*.*”，其中*表示 1 至多个合法字符（合法性说明参考公共操作说明），且整个邮件地址的字符总数不超过 30 个。

点击 >> 按钮将填入的邮件地址加入邮件地址组，新加入的邮件地址会在下方的邮件地址组显示框中显示出来，继续输入邮件地址点击 >> 可以重复添加；

选中邮件地址显示框中一项，点击 << 可以删除此邮件地址；

◆ **类型**

选择邮件地址过滤组类别，可选择”收件人”或”发件人”。

该选项必选并且默认为收件人。

◆ **备注**

该邮件地址的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个邮件地址后的编辑图标，弹出编辑窗口，如下图：

图 12 4 编辑邮件地址过滤组

编辑操作时，与添加操作类似。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个邮件地址后的删除图标，弹出编辑窗口，如下图：

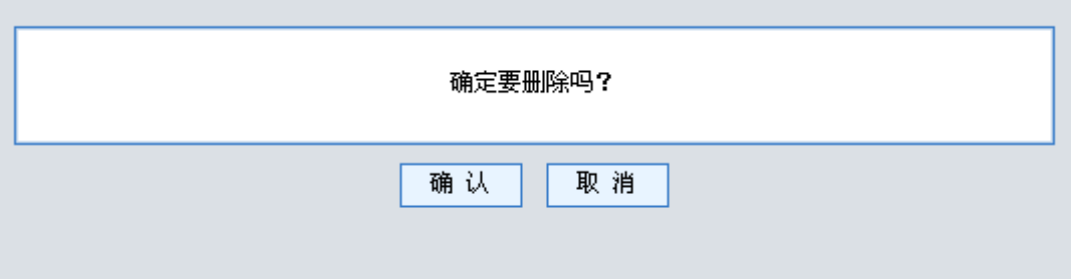


图 12 5 删除邮件地址过滤组

点击“确认”按钮，删除该邮件地址过滤组；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

12.1.2 内容关键字

内容关键字过滤，用于对客户端收发邮件的“主题”、“邮件内容”和“文本附件内容”进行控制。WEB 界面显示如下：

图 12 6 邮件内容关键字过滤

该模块包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

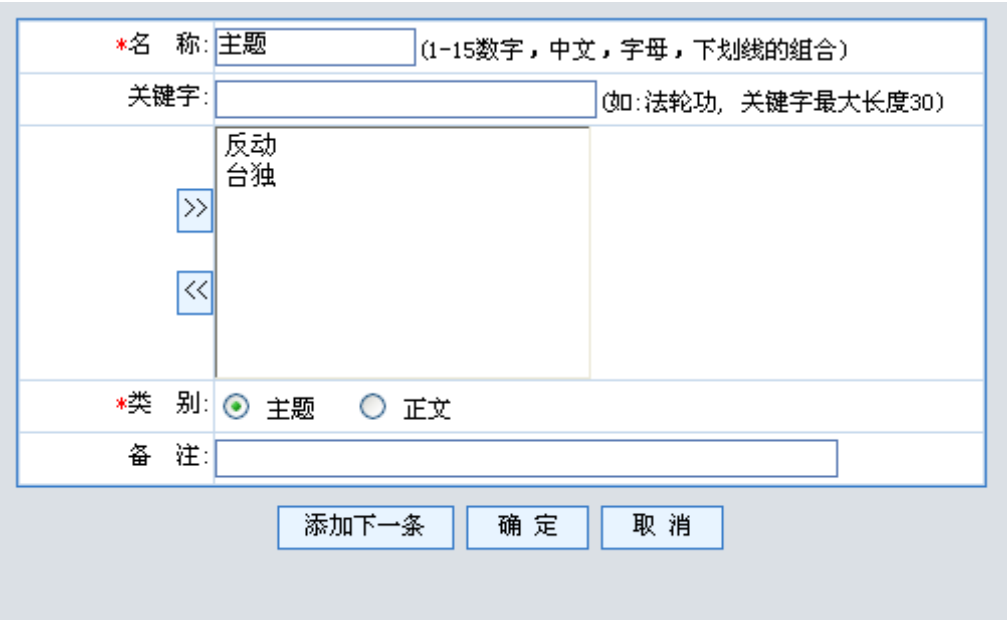


图 12 7 添加内容关键字

图中内容关键字的配置项，说明如下：

◆ **名称**

内容关键字过滤组名称，可以是数字、中文、字母、下划线的组合。

名称不能为空且必须唯一。

◆ **关键字**

关键字为“不允许”通过的主题关键字黑名单或正文关键字黑名单。

其由 1 至多个合法字符（合法性说明参考公共操作说明），且整个正文关键字的字符总数不

超过 30 个。

点击 按钮将输入的关键字加入关键字黑名单组，新加入的关键字会在下方的关键字黑名单组显示框中显示出来，继续输入关键字点击 可以重复添加；

选中关键字黑名单组显示框中一项，点击 可以删除此关键字；

◆ **类别**

选择内容关键字过滤组类别，可选择”主题”或”正文”；
类别必选且默认选择主题。

◆ **备注**

该关键字的备注或说明。
取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加内容关键字；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个内容关键字后的编辑图标，弹出编辑窗口，如下图：

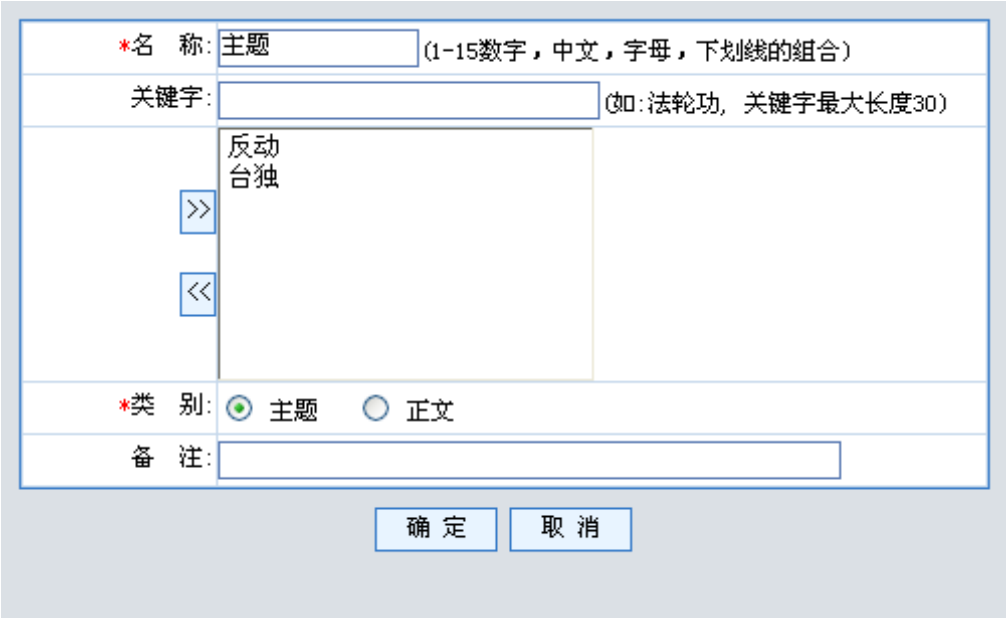


图 12 8 编辑内容关键字

编辑操作时，与添加操作类似。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个内容关键字后的删除图标，弹出编辑窗口，如下图：

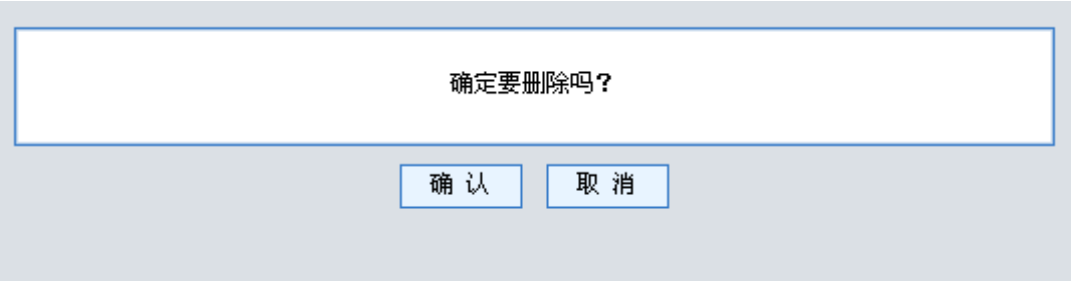


图 12 9 删除内容关键字

点击“确认”按钮，删除该内容关键字；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

12.1.3 附件扩展名

附件扩展名，用于对客户端收发邮件的附件扩展名进行控制。WEB 界面显示如下：

图 12 10 邮件附件扩展名过滤

该模块包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

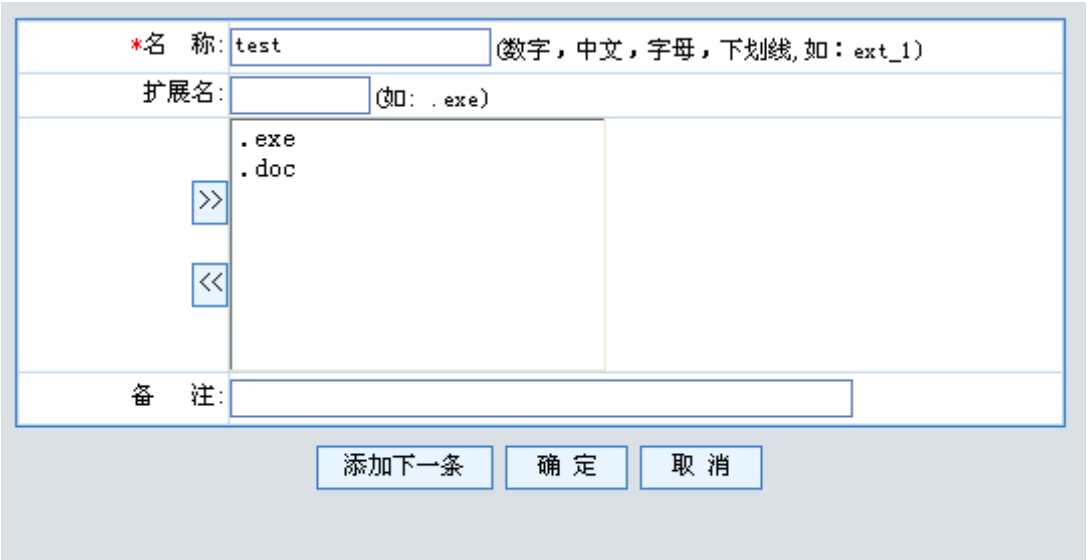


图 12 11 添加附件扩展名

图中附件扩展名的配置项，说明如下：

◆ **名称**

附件扩展名过滤组名称，可以是数字、中文、字母、下划线的组合。

名称不能为空且必须唯一。

◆ **扩展名**

扩展名为“允许通过”的附件扩展名。

其格式为：以点号开始，后接具体名称。单个点号表示所有没有扩展名的附件。名称由 0 至多个合法字符（合法性说明参考公共操作说明），且字符总数不超过 30 个。

点击 >> 按钮将输入的附件扩展名加入扩展名白名单组，新加入的附件扩展名会在下方的扩展名白名单组显示框中显示出来，继续输入附件扩展名点击 >> 可以重复添加；

选中扩展白名单组显示框中一项，点击 << 可以删除此附件扩展名；

◆ **备注**

该扩展名的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加附件扩展名；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个附件扩展名后的编辑图标，弹出编辑窗口，如下图：

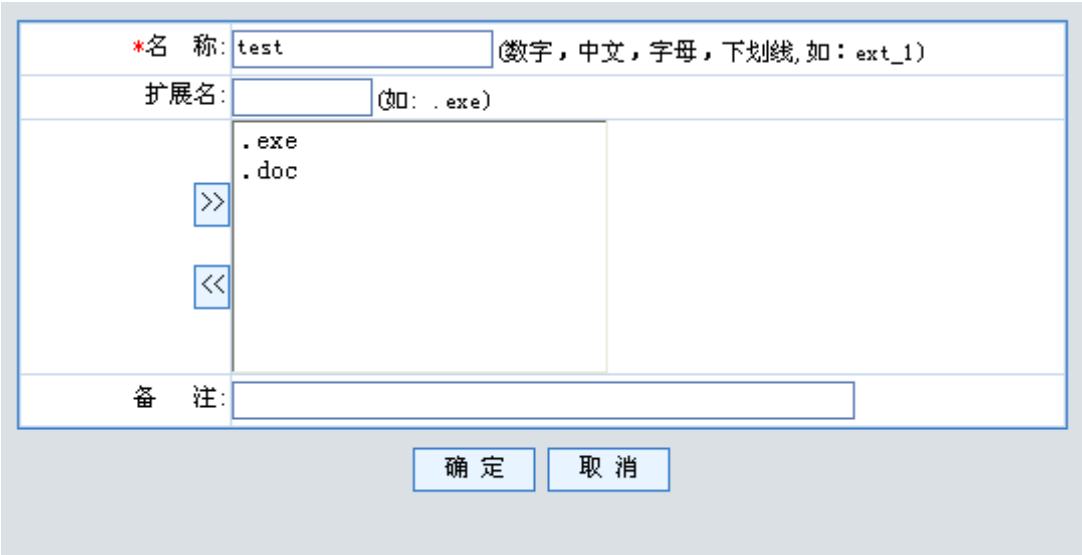


图 12 12 编辑附件扩展名

编辑操作时，与添加操作类似。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个附件扩展名后的删除图标，弹出编辑窗口，如下图：

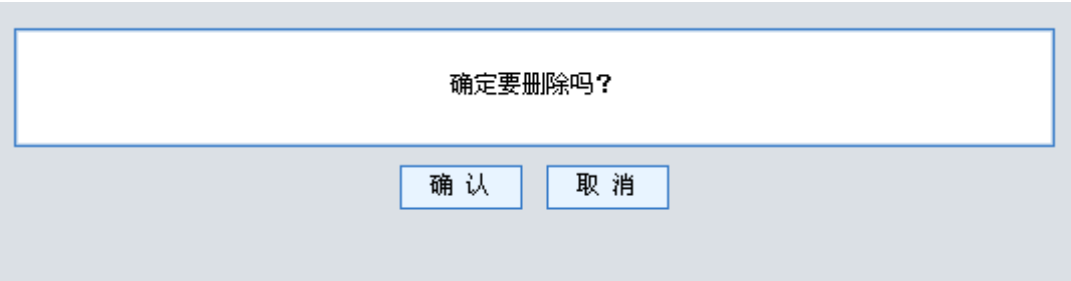


图 12 13 删除附件扩展名

点击“确认”按钮，删除该附件扩展名；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

12.1.4 过滤选项集

过滤选项集，通过引用上述邮件地址、内容关键字、附件扩展名的引用组成完整的过滤规则，对客户端收发邮件进行控制。WEB 界面显示如下：

图 12　14　过滤选项集列表显示

该模块包括四类操作，依次说明如下：

5) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

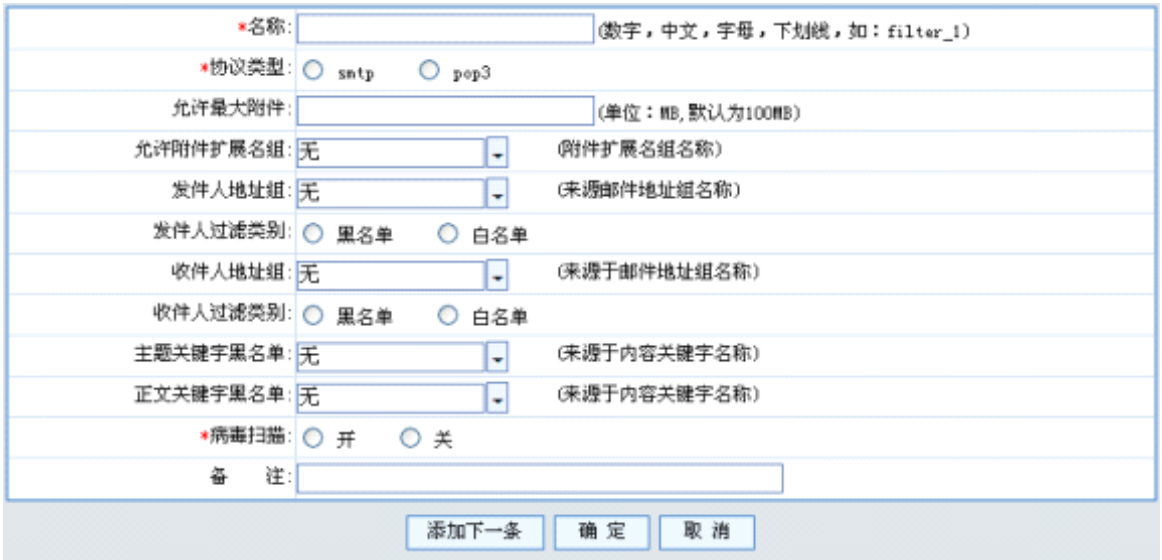


图 12　15　添加过滤选项集

图中过滤选项集的配置项，说明如下：

◆ **名称**

过滤选项集名称，可以是数字、中文、字母、下划线的组合。名称不能为空且必须唯一。

◆ **协议类型**

过滤选项集适用协议类型，可选择”SMTP”或”POP3”。

协议类型必选。

◆ **允许最大附件**

该选项用于设置允许通过的最大附件，默认为 100MB。

◆ **允许附件扩展名组**

该选项用于设置允许通过的邮件附件扩展名组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

下拉列表初始只有“无”菜单选项，其菜单项来源于“附件扩展名”中定义的附件扩展名组。

◆ **发件人地址组**

该选项用于设置需要过滤的邮件发件人地址组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

下拉列表初始只有“无”菜单选项，其菜单项来源于“邮件地址”中定义的邮件发件人地址组。

◆ **发件人过滤类别**

设置发件人地址组过滤动作，可选择“黑名单”或“白名单”。

若选择“黑名单”则禁止所选发件人地址组邮件通过；反之选择“白名单”则允许通过。

◆ **收件人地址组**

该选项用于设置需要过滤的邮件收件人地址组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

下拉列表初始只有“无”菜单选项，其菜单项来源于“邮件地址”中定义的邮件收件人地址组。

◆ **收件人过滤类别**

设置发收件人地址组过滤动作，可选择“黑名单”或“白名单”。

若选择“黑名单”则禁止所选收件人地址组邮件通过；反之选择“白名单”则允许通过。

◆ **主题关键字黑名单**

设置不允许通过的邮件主题关键字组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

下拉列表初始只有“无”菜单选项，其菜单项来源于“内容关键字”中定义的邮件主题关键字组。

◆ **正文关键字黑名单**

设置不允许通过的邮件正文关键字组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

下拉列表初始只有“无”菜单选项，其菜单项来源于“内容关键字”中定义的邮件正文关键字组。

◆ **病毒扫描**

设置是否对邮件附件进行病毒扫描。

该选项必选。

◆ **备注**

该过滤选项集的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加过滤选项集；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

6) 修改操作

在列表显示图中，点击列表中每个过滤选项集后的编辑图标，弹出编辑窗口，如下图：

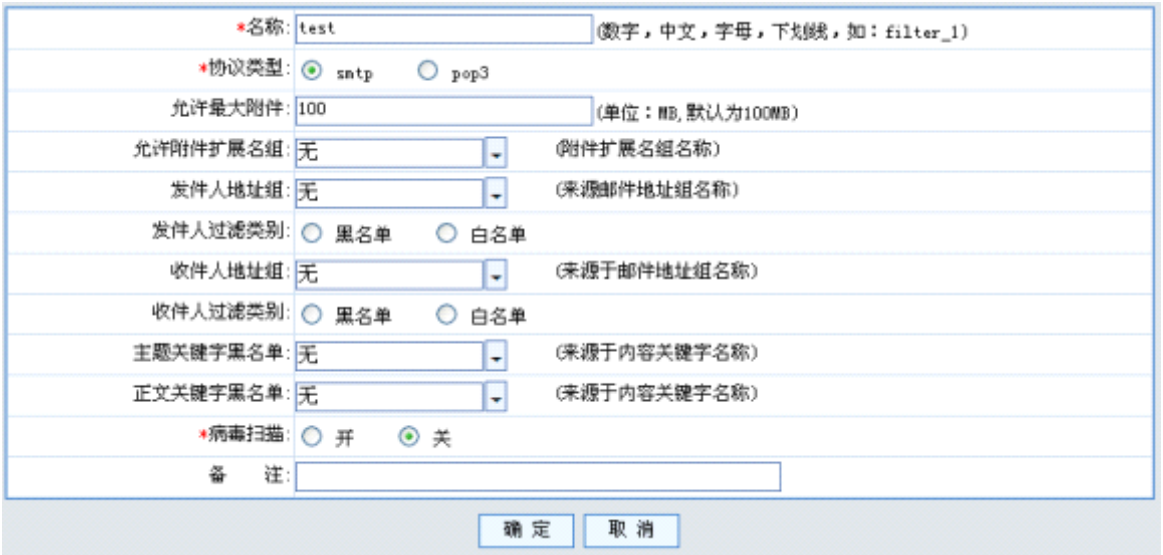


图 12 16 修改过滤选项集

编辑操作时，除名称不能修改外，其他与添加操作类似。具体参照添加操作。

7) 删除操作

在列表显示图中，点击列表中每个过滤选项集后的删除图标，弹出编辑窗口，如下图：

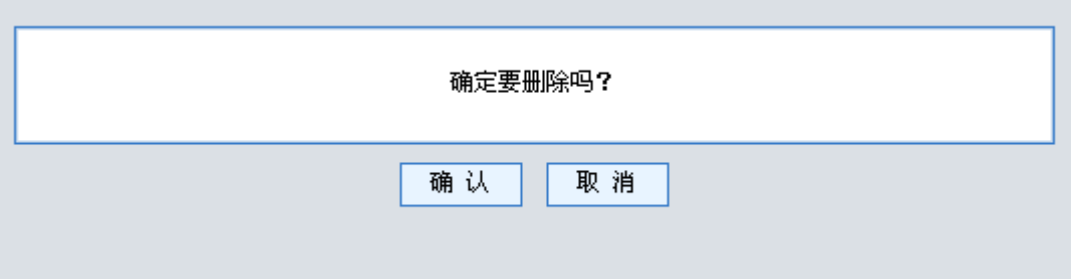


图 12 17 删除过滤选项集

点击“确认”按钮，删除该过滤选项集；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

8) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

12.2 SMTP

该部分用于配置所有与 SMTP 有关的邮件访问任务，及相关的参数配置，包括：基本参数配置、SMTP 客户端任务配置、SMTP 服务端任务配置等三个子模块。WEB 界面示意图如下：

图 12 18 SMTP WEB 界面功能菜单

12.2.1 基本配置

“基本配置”部分，用于配置 SMTP 访问任务的基本参数，目前仅包括“当前服务状态”参数。WEB 界面示意图如下：

图 12 19 SMTP 基本配置界面

参数说明如下表：

表 12 1 基本配置参数说明

参数名称	说 明
当前服务状态	表示 SMTP 访问任务的系统运行状态。若为“启动服务”，则表示当前所有任务已处于可运行状态，在此状态下，任务一旦添加且单独启停按钮为“启动”时，任务随即运行；若为“停止服务”，即使添加了任务且单独启停按钮为“启动”，任务也不运行。 服务状态值：“启动服务”或“停止服务”。

操作方法：

■ **启动服务：**

单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

■ **停止服务：**

单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

12.2.2 客户端

该部分用于配置所有的 SMTP 客户端的访问任务，包括：透明模式的客户端任务、普通模式的客户端任务。依次说明如下：

一. 透明模式的 SMTP 客户端任务

WEB 界面显示如下：

图 12 20 SMTP 客户端透明任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

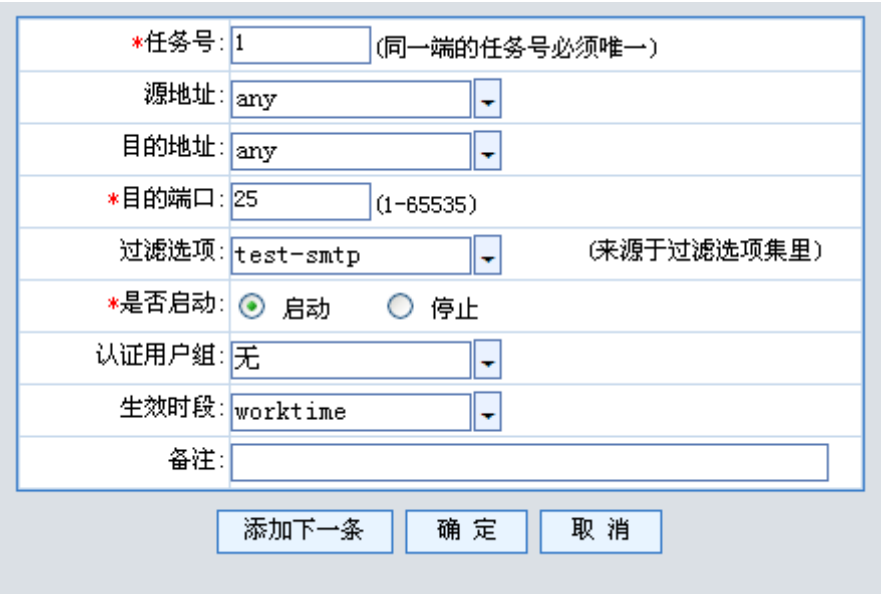


图 12 21 添加 SMTP 客户端透明任务

图中 SMTP 透明模式的客户端任务的配置项，说明如下：

◆ **任务号**

用于表示该任务。用于表示该任务。对于透明访问任务，任务号相当于序号的作用。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个定制访问模块内必须唯一。

该配置项必填。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的地址**

目的地址表示对方网络中邮件客户端所需访问的邮件服务器的 IP 地址或域名。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的端口**

目的端口指明对方网络中邮件客户端所需访问的邮件服务器的真实端口。

取值范围：1－65535，默认为 25 端口。

该配置项必填。

◆ **过滤选项**

过滤选项用于选择该客户端任务适用的过滤选项。

其值从下拉列表中选取即可，但不能为空，可以选取“无”菜单选项，默认为“无”。

其菜单项来源于“过滤选项集”中定义的过滤选项。

◆ **是否启动**

是否启动选项用于启动该客户端任务。默认为“启动”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

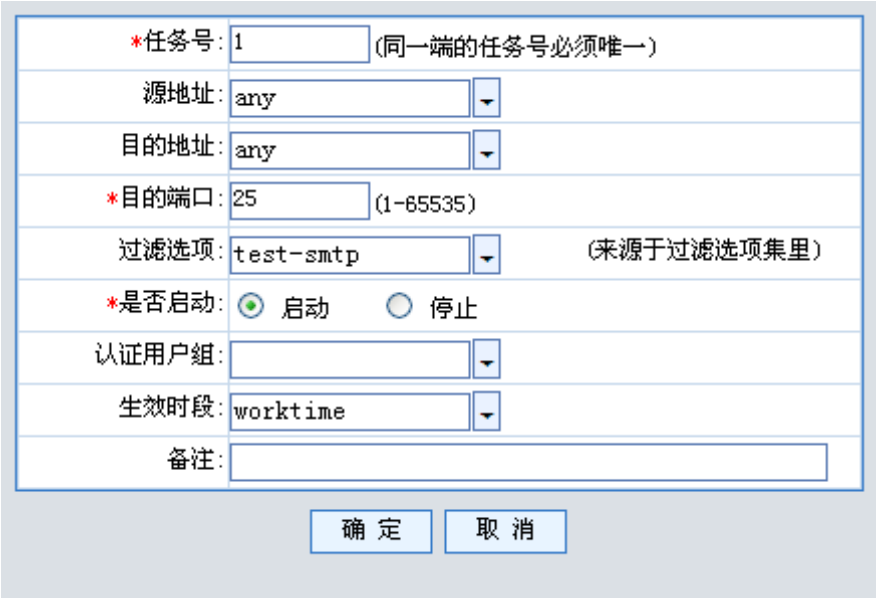


图 12 22 编辑 SMTP 客户端透明任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

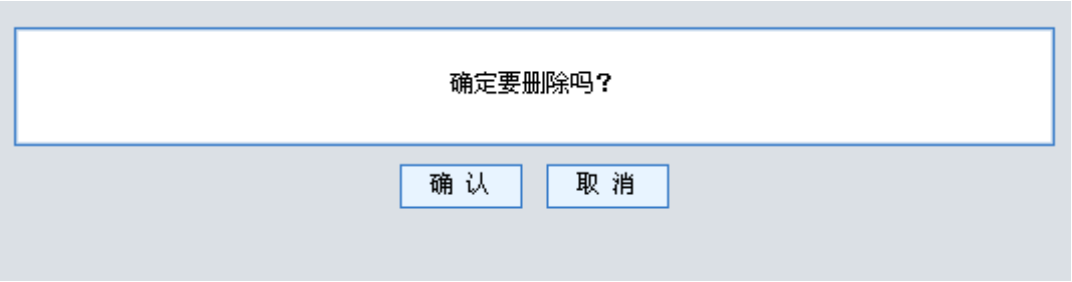


图 12　23　删除 SMTP 客户端透明任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4)　其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

二. 普通模式的 SMTP 客户端任务

WEB 界面显示如下：

图 12　24　SMTP 客户端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

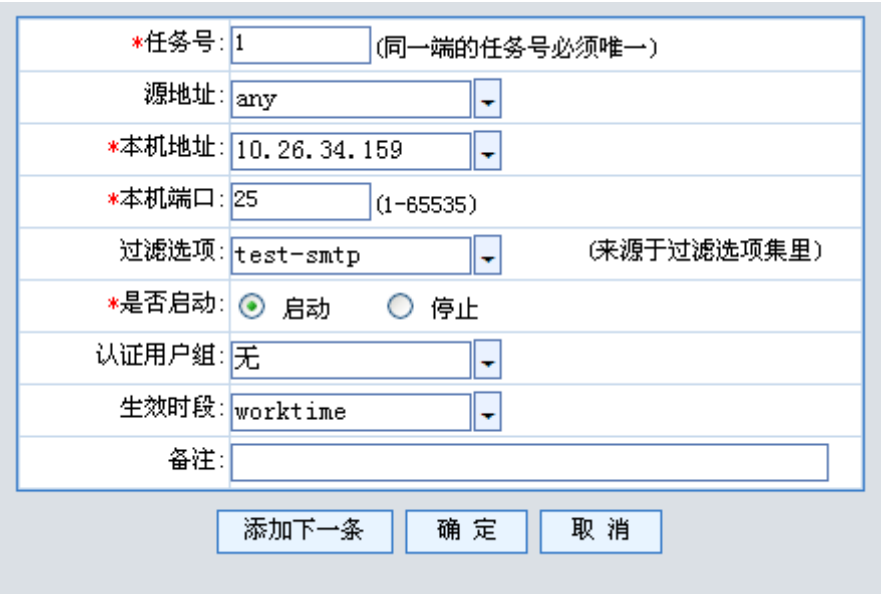


图 12　25　添加 SMTP 客户端透明任务

图中 SMTP 普通模式的客户端任务的配置项，说明如下：

◆ **任务号**

任务号是通用 SMTP 客户端正常访问的基础，每个任务号必须与对方主机模块配置的相对应的通用邮件服务端任务的任务号完全相同，即客户端任务的任务号必须服务端相应的任务号一一对应，否则无法正常访问。

任务号用 0—9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个邮件访问模块内必须唯一。

该配置项必填。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置>>网络接口”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

本机端口为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535，默认为 25 端口。
该配置项为必填项。

◆ **过滤选项**

过滤选项用于选择该客户端任务适用的过滤选项。
其值从下拉列表中选取即可，但不能为空，可以选取“无”菜单选项，默认为“无”。
其菜单项来源于“过滤选项集”中定义的过滤选项。

◆ **是否启动**

是否启动选项用于启动该客户端任务。默认为“启动”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。
其值从下拉列表中选取，可以选择“无”，默认为“无”。
下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。
取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

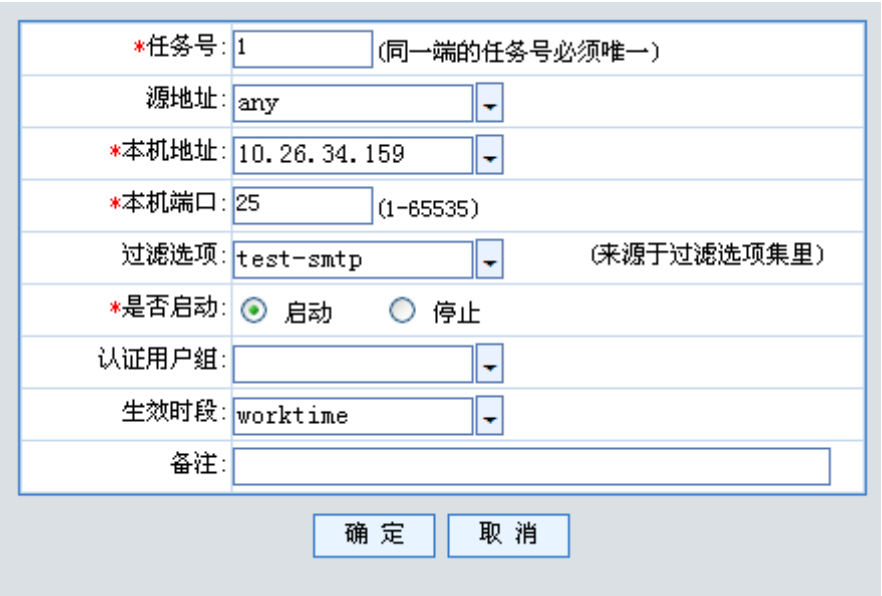


图 12　26　编辑 SMTP 客户端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

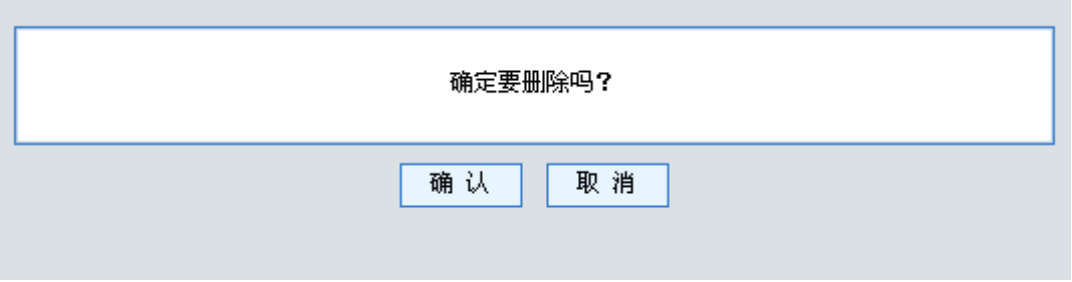


图 12　27　删除 SMTP 客户端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

✧

12.2.3　服务端

该部分用于配置所有的 SMTP 服务端的访问任务。特别指出的是，与客户端不同，服务端只需配置普通模式下的访问任务，对于透明模式的服务端任务，系统内部已经配置好，无需用户配置。WEB 界面导航菜单如下：

图 12　28　SMTP 服务端导航菜单

下面详细介绍服务端的普通模式的任务配置：

一. 普通模式的 SMTP 服务端任务

WEB 界面显示如下：

图 12　29　SMTP 服务端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

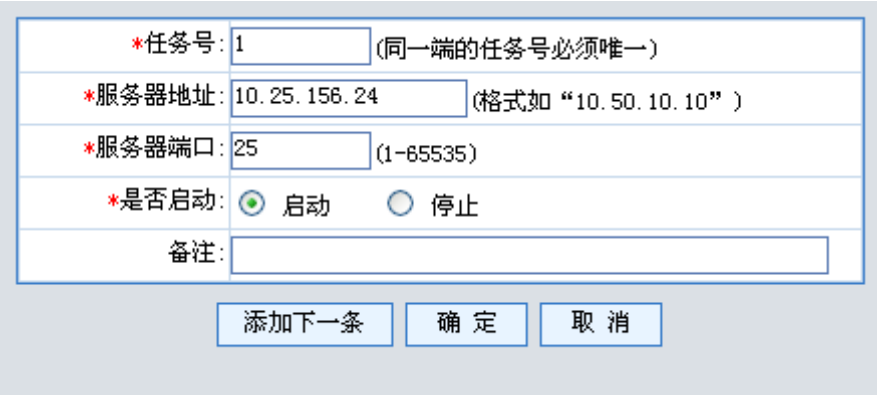


图 12　30　添加 SMTP 服务端普通任务

图中 SMTP 普通模式的服务端任务的配置项，说明如下：

◆ **任务号**

任务号是客户端正常访问的基础，所以一个服务端任务的任务号必须与对方主机模块中相对应的客户端任务的任务号完全相同，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个邮件访问模块内必须唯一。

该配置项必填。

◆ **服务器地址**

服务器地址为目标访问网络中的邮件服务器的真实 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也不能为 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问网络中的邮件服务器的真实端口。

取值范围：1－65535，默认为 25 端口。

该配置项为必填项。

◆ **是否启动**

是否启动选项用于启动该服务器任务。默认为“启动”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

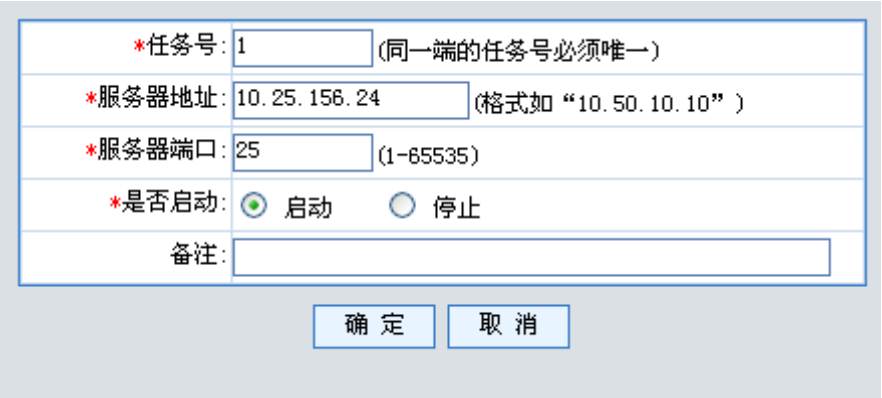


图 12 31 编辑 SMTP 服务端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

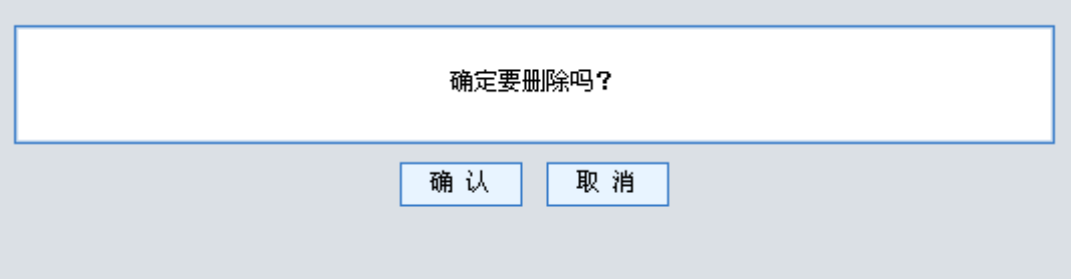


图 12 32 删除 SMTP 服务端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

12.3 POP3

该部分用于配置所有与 POP3 有关的邮件访问任务，及相关的参数配置，包括：基本参数配置、POP3 客户端任务配置、POP3 服务端任务配置等三个子模块。WEB 界面示意图如下：

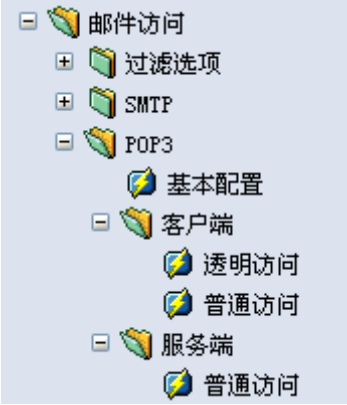


图 12　33　POP3 WEB 界面功能菜单

12.3.1　基本配置

“基本配置”部分，用于配置 POP3 访问任务的基本参数，目前仅包括“当前服务状态”参数。WEB 界面示意图如下：

图 12　34　POP3 基本配置界面

参数说明如下表：

表 12　2　基本配置参数说明

参数名称	说　明

当前服务状态	表示 POP3 访问任务的系统运行状态。若为“启动服务”，则表示当前所有任务已处于可运行状态，在此状态下，任务一旦添加且单独启停按钮为“启动”时，任务随即运行；若为“停止服务”，即使添加了任务且单独启停按钮为“启动”，任务也不运行。 服务状态值：“启动服务”或“停止服务”。

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

12.3.2 客户端

该部分用于配置所有的 POP3 客户端的访问任务，包括：透明模式的客户端任务、普通模式的客户端任务。依次说明如下：

一. 透明模式的 POP3 客户端任务

WEB 界面显示如下：

图 12 35 POP3 客户端透明任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

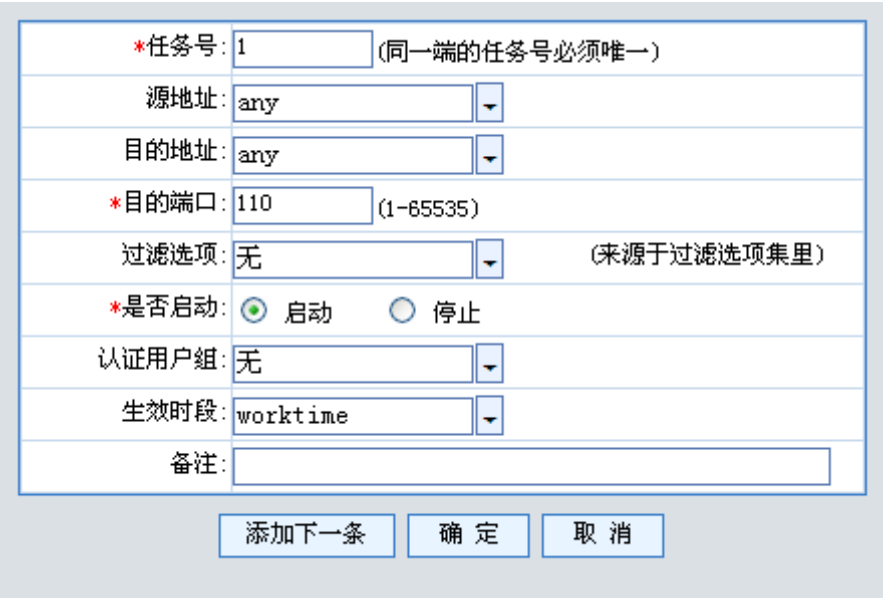


图 12 36 添加 POP3 客户端透明任务

图中 POP3 透明模式的客户端任务的配置项，说明如下：

◆ **任务号**

用于表示该任务。用于表示该任务。对于透明访问任务，任务号相当于序号的作用。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个定制访问模块内必须唯一。

该配置项必填。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的地址**

目的地址表示对方网络中邮件客户端所需访问的邮件服务器的 IP 地址或域名。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的端口**

目的端口指明对方网络中邮件客户端所需访问的邮件服务器的真实端口。

取值范围：1－65535，默认为 110 端口。

该配置项必填。

◆ **过滤选项**

过滤选项用于选择该客户端任务适用的过滤选项。

其值从下拉列表中选取即可，但不能为空，可以选取“无”菜单选项，默认为“无”。

其菜单项来源于“过滤选项集”中定义的过滤选项。

◆ **是否启动**

是否启动选项用于启动该客户端任务。默认为“启动”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

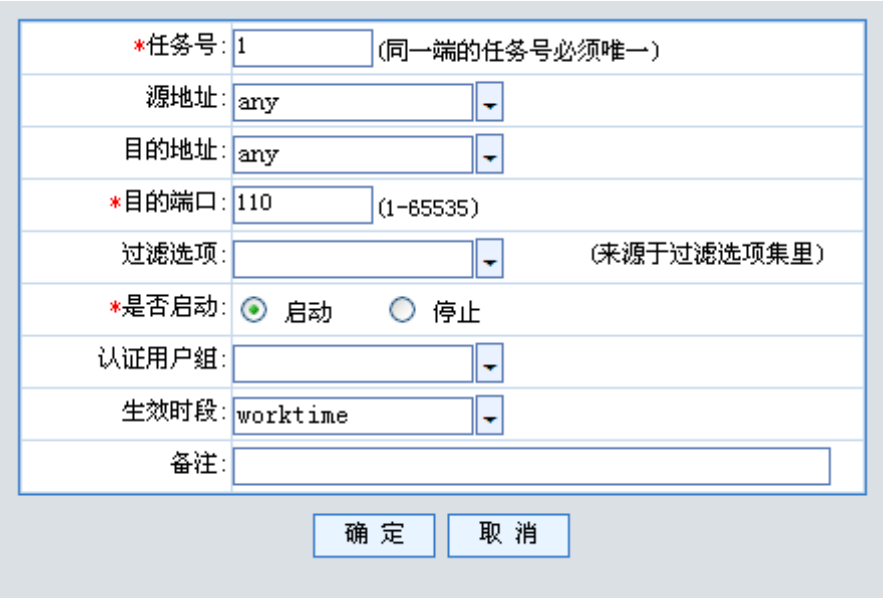


图 12 37 编辑 POP3 客户端透明任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

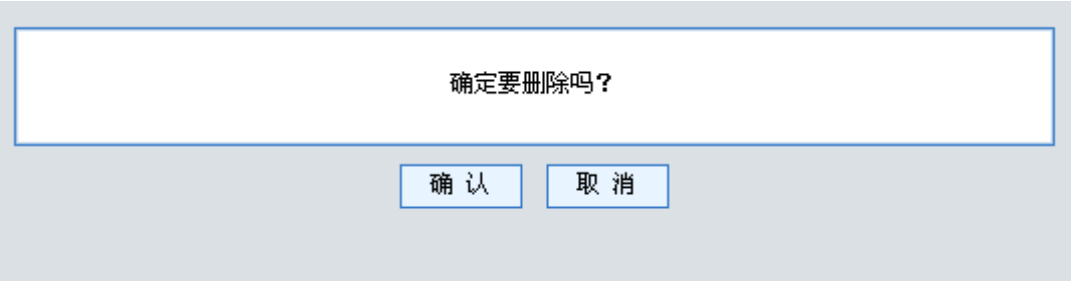


图 12　38　删除 POP3 客户端透明任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4)　其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

✧

二. 普通模式的 POP3 客户端任务

WEB 界面显示如下：

图 12　39　POP3 客户端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

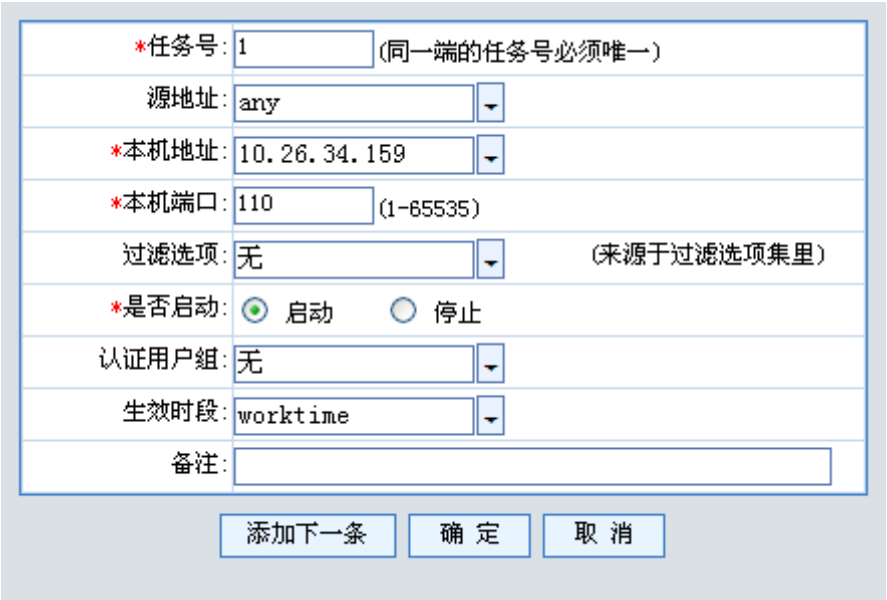


图 12 40 添加 POP3 客户端普通任务

图中 POP3 普通模式的客户端任务的配置项，说明如下：

◆ **任务号**

任务号是通用 POP3 客户端正常访问的基础，每个任务号必须与对方主机模块配置的相对应的通用邮件服务端任务的任务号完全相同，即客户端任务的任务号必须服务端相应的任务号一一对应，否则无法正常访问。

任务号用 0—9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个邮件访问模块内必须唯一。

该配置项必填。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置>>网络接口”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

本机端口为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535，默认为 110 端口。
该配置项为必填项。

◆ **过滤选项**

过滤选项用于选择该客户端任务适用的过滤选项。
其值从下拉列表中选取即可，但不能为空，可以选取“无”菜单选项，默认为“无”。
其菜单项来源于“过滤选项集”中定义的过滤选项。

◆ **是否启动**

是否启动选项用于启动该客户端任务。默认为“启动”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。
其值从下拉列表中选取，可以选择“无”，默认为“无”。
下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。
取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

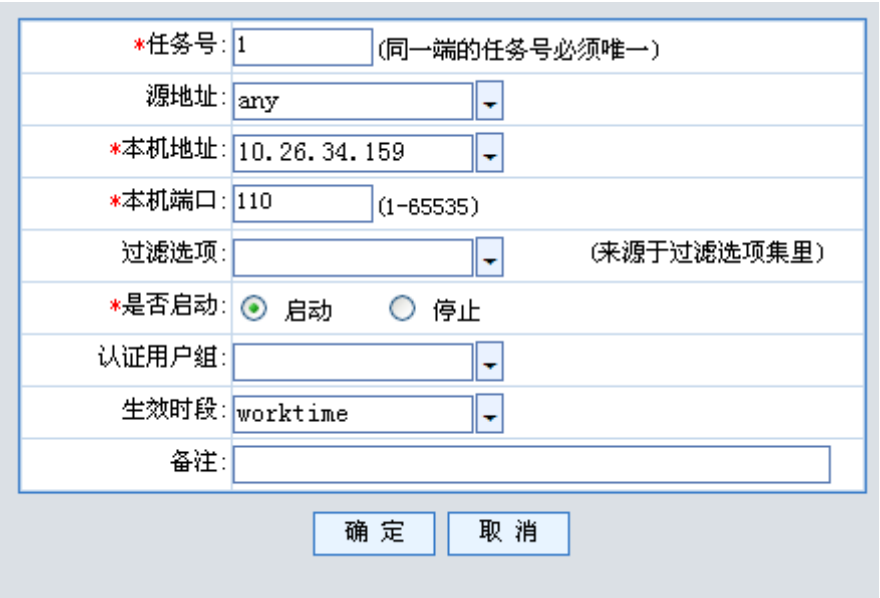


图 12 41 编辑 POP3 客户端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

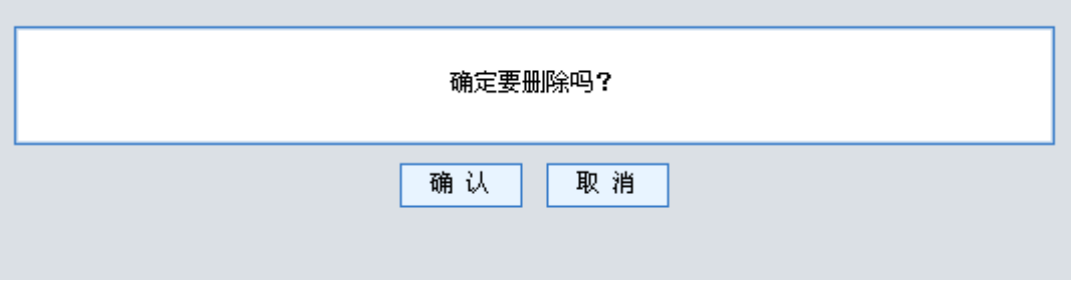


图 12 42 删除 POP3 客户端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

✧

12.3.3 服务端

该部分用于配置所有的 POP3 服务端的访问任务。特别指出的是，与客户端不同，服务端只需配置普通模式下的访问任务，对于透明模式的服务端任务，系统内部已经配置好，无需用户配置。WEB 界面导航菜单如下：

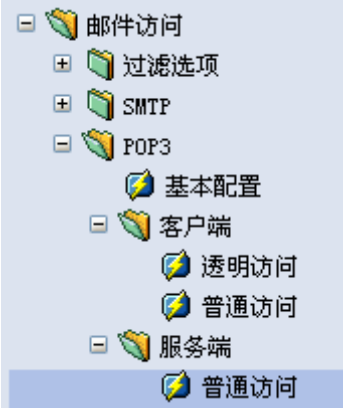


图 12 43 POP3 服务端导航菜单

下面详细介绍服务端的普通模式的任务配置：

一. 普通模式的 POP3 服务端任务

WEB 界面显示如下：

图 12　44　POP3 服务端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

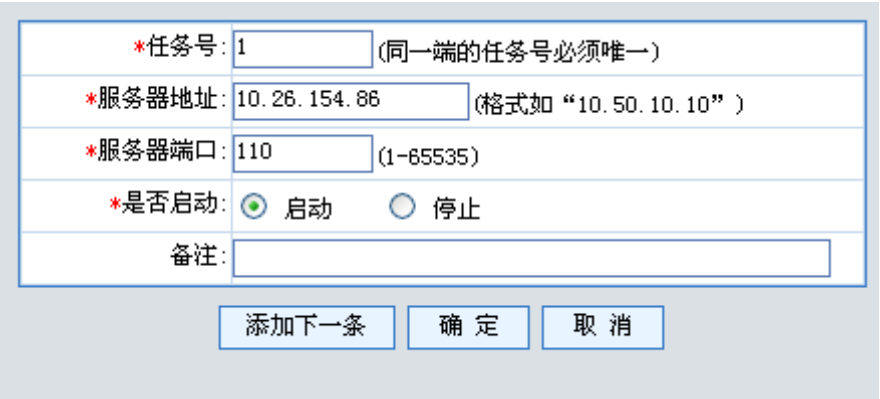


图 12　45　添加 POP3 服务端普通任务

图中 POP3 普通模式的服务端任务的配置项，说明如下：

◆ **任务号**

任务号是客户端正常访问的基础，所以一个服务端任务的任务号必须与对方主机模块中相对应的客户端任务的任务号完全相同，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个邮件访问模块内必须唯一。

该配置项必填。

◆ **服务器地址**

服务器地址为目标访问网络中的邮件服务器的真实 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也不能为 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问网络中的邮件服务器的真实端口。

取值范围：1－65535，默认为 110 端口。

该配置项为必填项。

◆ **是否启动**

是否启动选项用于启动该客户端任务。默认为“启动”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

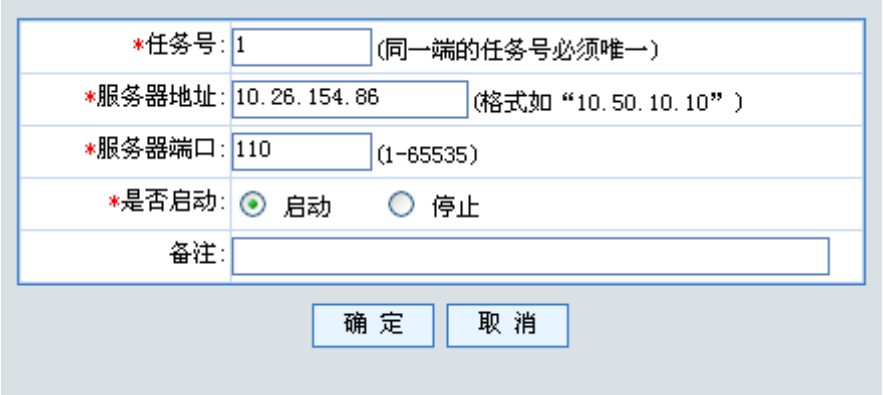


图 12 46 编辑 POP3 服务端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

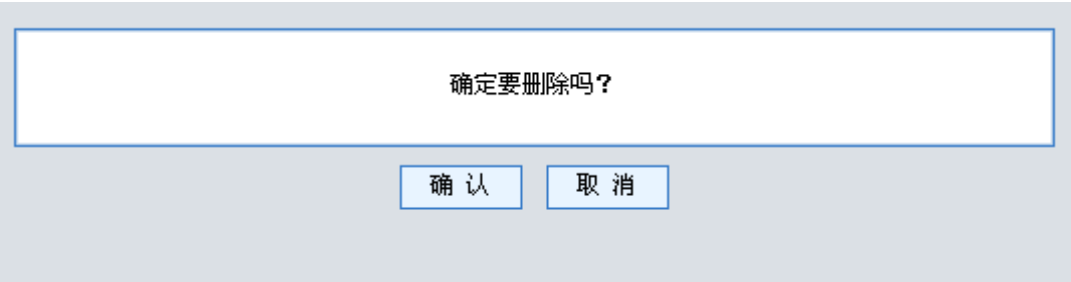


图 12 47 删除 POP3 服务端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

✧

第 13 章 数据库访问

该模块支持内外网用户访问对方数据库。通过配置数据库服务端和客户端任务，实现访问，同时通过“访问控制”中的数据库服务器 IP 地址、访问用户等选项，更大限度地控制数据库的访问请求，达到更加安全的效果。

该模块包括：基本配置、过滤选项、客户端任务配置、服务端任务配置等四个模块。

13.1 基本配置

“基本配置”部分，用于配置数据库访问任务的基本参数，目前仅包括“当前服务状态”参数。WEB 界面示意图如下：

图 13 1 数据库访问基本配置界面

参数说明如下表：

表 13 1 基本配置参数说明

参数名称	说 明
当前服务状态	表示数据库访问任务的系统运行状态。若为“启动服务”，则表示当前所有任务已处于可运行状态，在此状态下，任务一旦添加且单独启停按钮为“启动”时，任务随即运行；若为“停止服务”，即使添加了任务且单独启停按钮为“启动”，任务也不运行。 服务状态值：“启动服务”或“停止服务”。

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

13.2 过滤选项

13.2.1 用户过滤

用户过滤，用于控制数据库客户端用户访问数据库服务器的访问权限。WEB 界面如下：

图 13 2 用户过滤列表显示

该模块包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

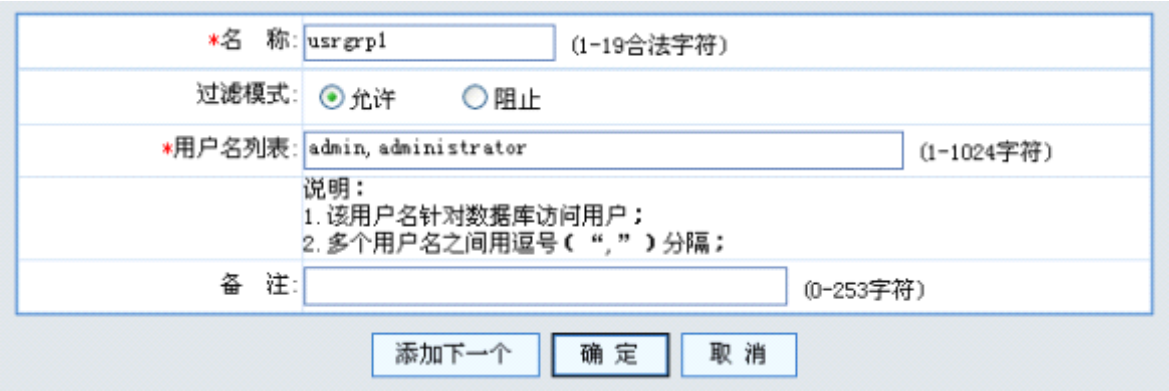


图 13 3 添加用户过滤列表

图中各配置项，说明如下：

◆ **名称**

为当前用户过滤组设置名称，名称必须唯一且不能为空。

◆ **过滤模式**

配置当前用户过滤组的控制动作。

选中“允许”，则允许“用户名列表”中输入的用户通过；选中“阻止”，则阻止“用户名列表”中输入的用户通过；默认为“阻止”。

◆ **用户名列表**

在此添加受控的用户名列表。

允许一次添加多个用户名，用户名之间用逗号隔开。缺省默认为没有用户。该输入框最多允许 48 个字符。用户名的命名合法性参考“公共操作”一章中的相关描述。

◆ **备注**

该关键字的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加主题关键字；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每条用户过滤组后的编辑图标，弹出编辑窗口，如下图：

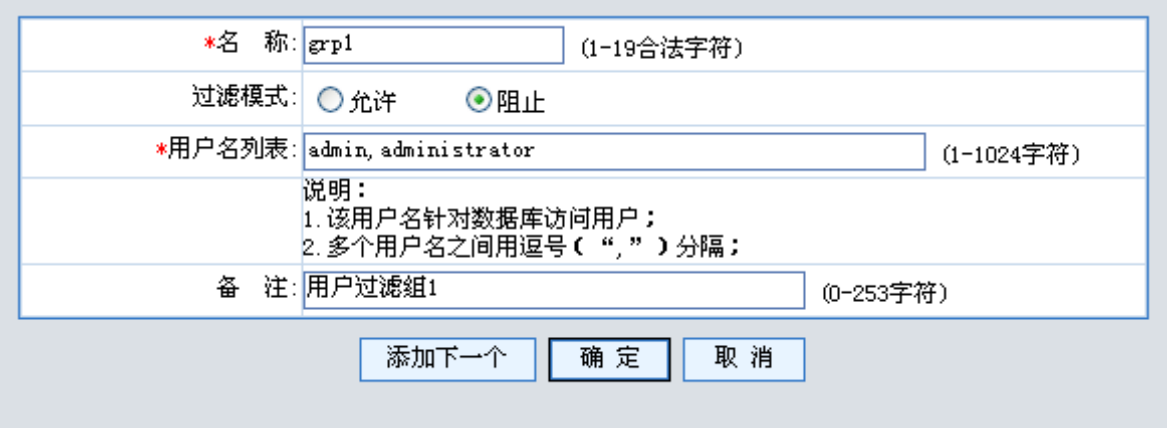


图 13 4 编辑用户过滤列表

编辑操作时，除名称不能修改外，其他与添加操作类似。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每条用户过滤组后的删除图标，弹出编辑窗口，如下图：

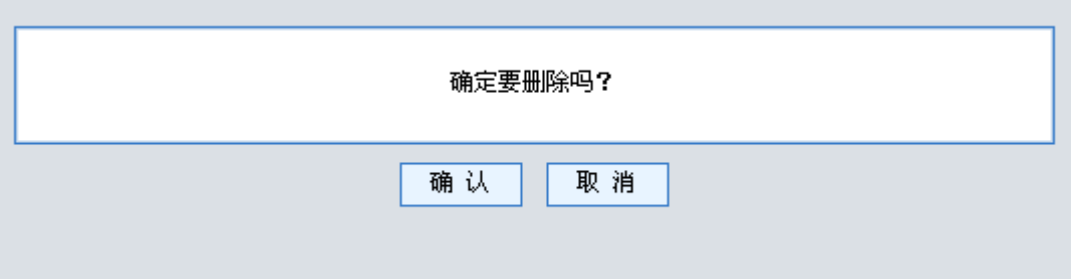


图 13 5 删除用户过滤列表

点击“确认”按钮，删除该条用户过滤组；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

13.2.2 SQL 语句过滤

数据库访问 SQL 语句过滤，用于控制数据库客户端用户访问数据库服务器的所使用的 SQL 语句。目前支持 SQL Server 和 Oracle（不包含 8i 版本）数据库。

SQL 语句过滤的属性包括：过滤模式、SQL 语句列表等控制项。WEB 界面如下：

图 13 6 SQL 语句过滤列表显示

该模块包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

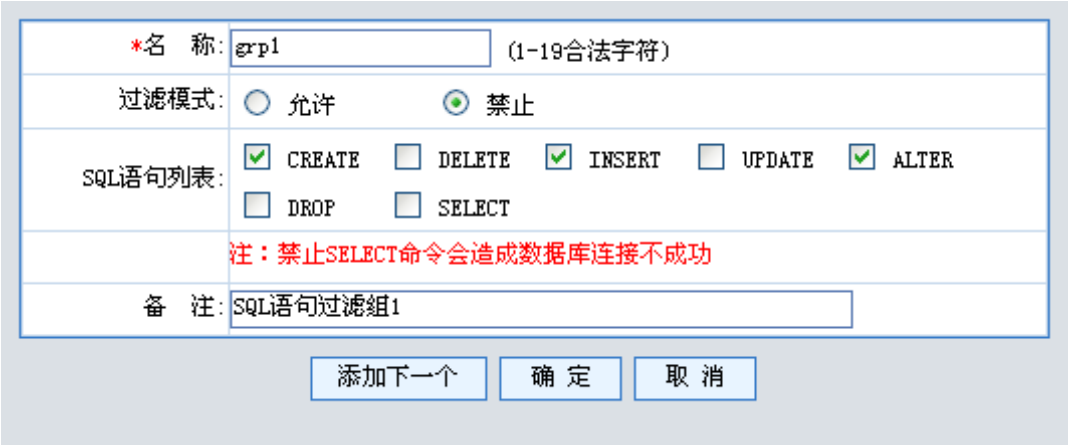


图 13 7 添加 SQL 语句过滤

图中各配置项，说明如下：

◆ **名称**

为当前 SQL 语句过滤组设置名称，名称必须唯一且不能为空。

◆ **过滤模式**

配置当前 SQL 语句过滤的控制动作。

选中“允许”，则允许执行“SQL 语句列表”中勾选的语句；选中“禁止”，则禁止执行“SQL 语句列表”中勾选的语句。默认为“禁止”。

◆ **SQL 语句列表**

在此勾选受控的 SQL 语句列表。

可以从该列表中选择一个或者多个受控命令。

◆ **备注**

该关键字的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加 SQL 语句过滤组；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每条 SQL 语句过滤组后的编辑图标，弹出编辑窗口，如下图：

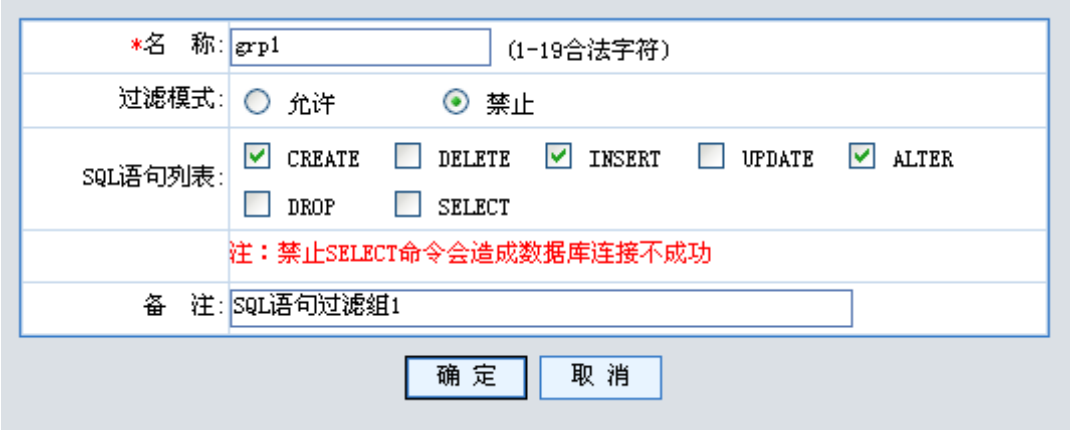


图 13 8 编辑 SQL 语句过滤

编辑操作时，除名称不能修改外，其他与添加操作类似。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每条 SQL 语句过滤组后的删除图标，弹出编辑窗口，如下图：

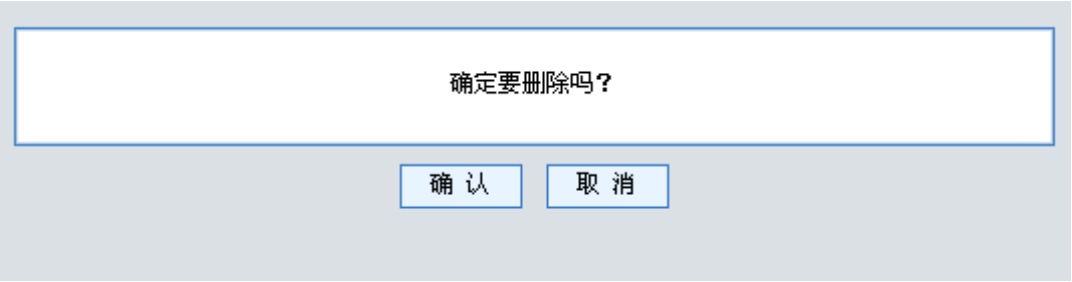


图 13　9　删除 SQL 语句过滤

点击“确认”按钮，删除该条 SQL 语句过滤组；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4)　其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

13.2.3　过滤选项集

“过滤选项集”部分，用于数据库访问过滤，包括用户名过滤组，SQL 语句过滤组，流病毒扫描，用于实现数据库访问模块的安全控制。WEB 界面示意图如下：

图 13　10　过滤选项集界面

该模块主要包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

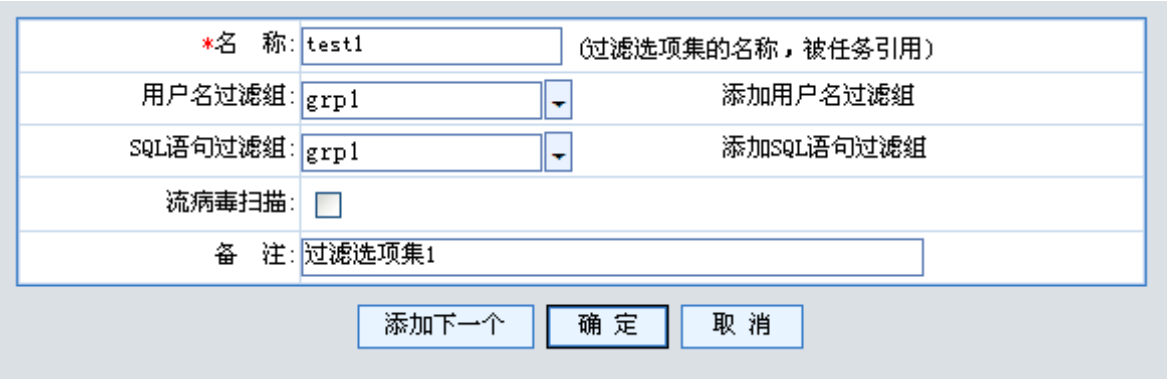


图 13 11 添加过滤选项集

图中过滤选项集的配置项，说明如下：

◆ **名称**

为当前过滤选项集规定一个名称，名称必须唯一且不能为空。

◆ **用户名过滤组**

该选项用于设置此过滤选项集应用的用户名过滤组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

其菜单项来源于“用户过滤”中定义的用户过滤组。

◆ **SQL 语句过滤组**

该选项用于设置此过滤选项集应用的 SQL 语句过滤组。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

其菜单项来源于“SQL 语句过滤”中定义的 SQL 语句过滤组。

◆ **流病毒扫描**

该选项用于配置流病毒扫描。默认为不选中。

◆ **备注**

该文件扩展名的备注或说明。

取值说明请参考“通用操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加过滤选项集；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个过滤选项集后面的编辑图标，弹出编辑窗口，如下图：

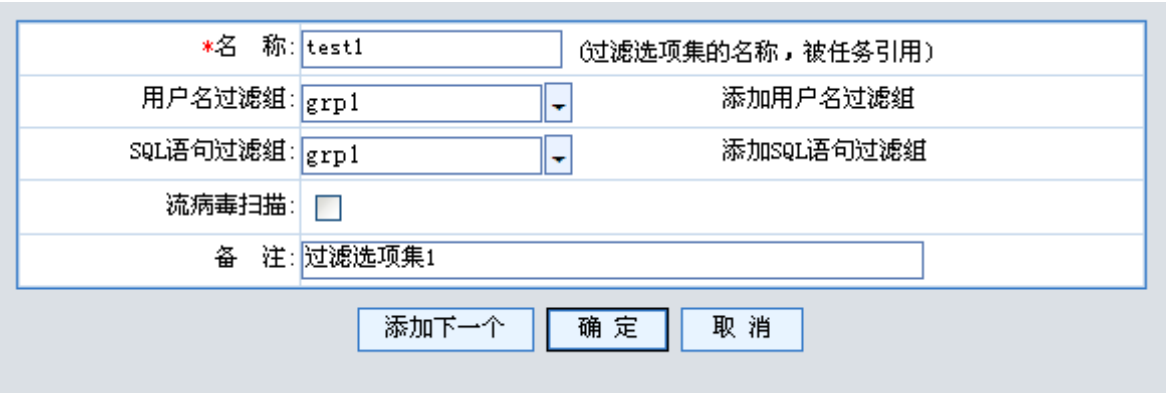


图 13-12 编辑过滤选项集

编辑操作时，除名称不能修改外，其他与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个过滤选项集后面的删除图标，弹出编辑窗口，如下图：

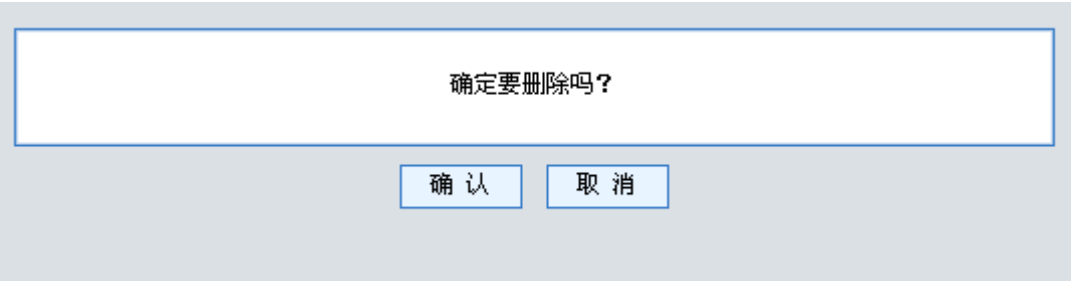


图 13-13 删除过滤选项集

点击“确认”按钮，删除该过滤选项集；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

13.3 客户端

该部分用于配置所有的数据库访问的客户端任务，包括：透明模式的客户端任务、普通模式的客户端任务。依次说明如下：

13.3.1 透明访问

WEB 界面显示如下：

图 13　14　客户端透明任务列表显示

该模块主要包括五类操作，依次说明如下：

1) 设置 ORACLE 数据通道 IP 地址

该参数仅针对 ORACLE 数据库类型而配置，且对于客户端的透明任务才需配置。对其他数据库类型无效。设置时只要在其后面的下拉列表框中选取相应的 IP 地址即可。其下拉菜单项来源于本机网络接口地址。

对于 ORACLE 数据库的客户端的透明任务，该通道必须配置，不能为“无”。

2) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

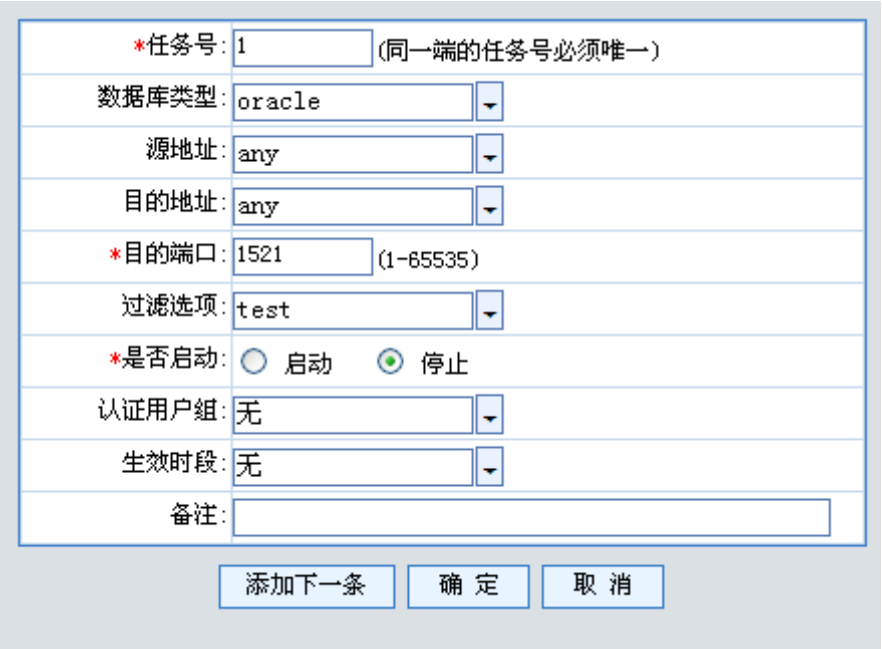


图 13　15　添加数据库访问客户端透明任务

图中透明模式的客户端任务的各配置项，说明如下：

◆ **任务号**

用于表示该任务。用于表示该任务。对于透明访问任务，任务号相当于序号的作用。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个定制访问模块内必须唯一。

该配置项必填。

◆ **数据库类型**

数据库类型表示该任务所使用的数据库。目前支持 oracle、sqlserver、mysql、sybase、DB2 等类型。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“oracle”。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的地址**

目的地址表示对方网络中客户端所需访问的数据库服务器的 IP 地址或域名。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的端口**

目的端口指明对方网络中客户端所需访问的数据库服务器的真实端口。

取值范围：1－65535，默认为 1521 端口。

该配置项必填。

◆ **过滤选项**

该选项设置应用的过滤选项。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

其菜单项来源于“过滤选项集”中定义的过滤选项集。

◆ **是否启动**

该选项用于设置是否启动该客户端任务。默认为“停止”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

3) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

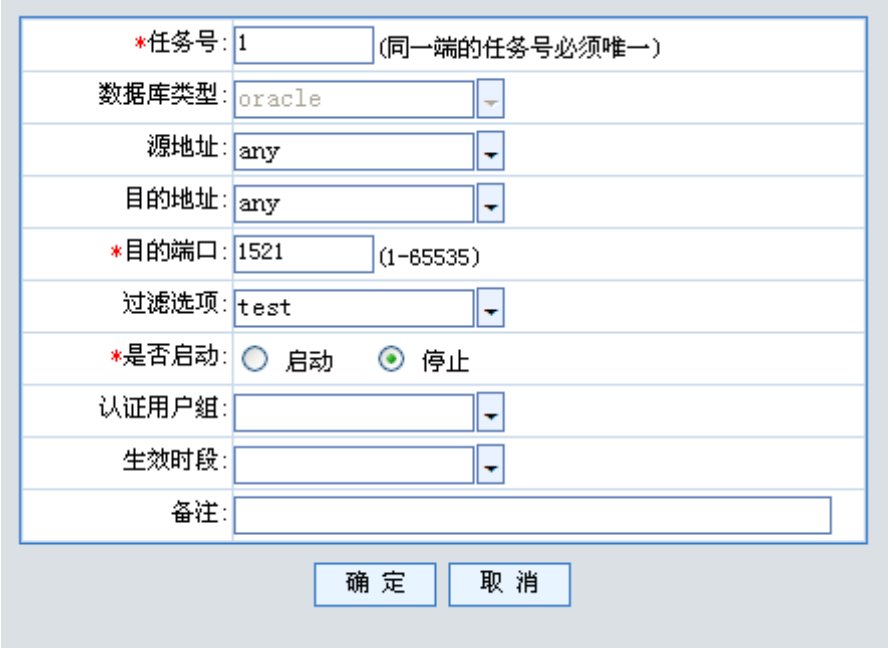


图 13 16 编辑数据库访问客户端透明任务

编辑操作时，除“任务号”、“数据库类型”不能编辑外，其他与添加操作相同。具体参照添加操作。

4) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

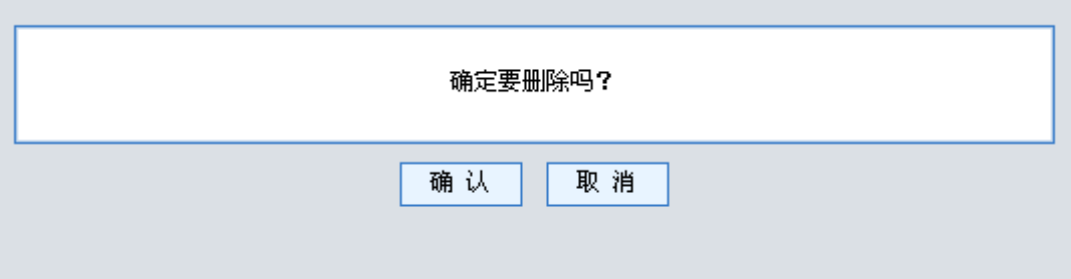


图 13 17 删除数据库访问客户端透明任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

5) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

13.3.2 普通访问

WEB 界面显示如下：

图 13 18 客户端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

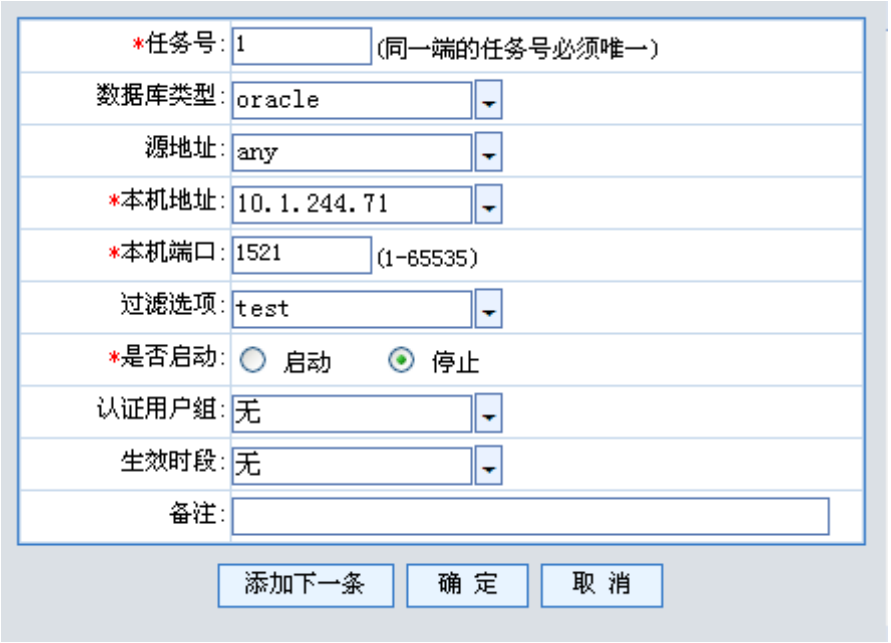


图 13 19 添加普通模式的客户端任务

图中任务的各配置项，说明如下：

◆ **任务号**

任务号是数据库任务正常访问的基础，每个任务号必须与对方主机模块配置的相对应的服务

端任务的任务号完全相同，即客户端任务的任务号必须服务端相应的任务号一一对应，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个数据库访问模块内必须唯一。

该配置项必填。

◆ **数据库类型**

数据库类型表示该任务所使用的数据库。目前支持的数据库类型有 ORACLE、SQLSERVER、DB2、MYSQL、SYBASE 等。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“oracle”。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置>>网络接口”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

本机端口为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535，默认为 1521 端口。

该配置项为必填项。

◆ **过滤选项**

该选项设置应用的过滤选项。

其值从下拉列表中选取即可，不能为空，但可以选取“无”菜单选项，默认为“无”。

其菜单项来源于“过滤选项集”中定义的过滤选项集。

◆ **是否启动**

该选项用于设置是否启动该客户端任务。默认为“停止”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

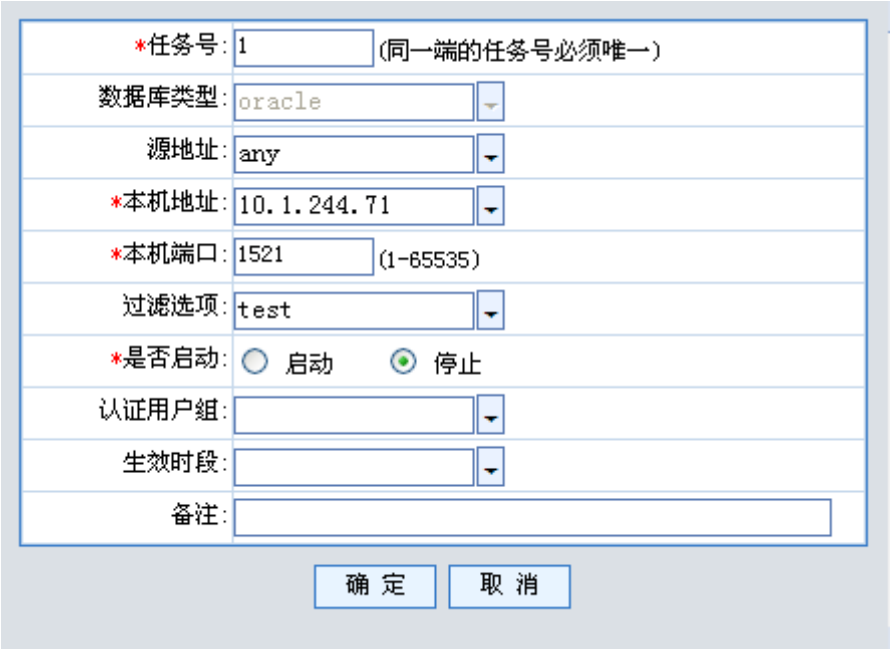


图 13 20 编辑数据库访问客户端普通任务

编辑操作时，除“任务号”、“数据库类型”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

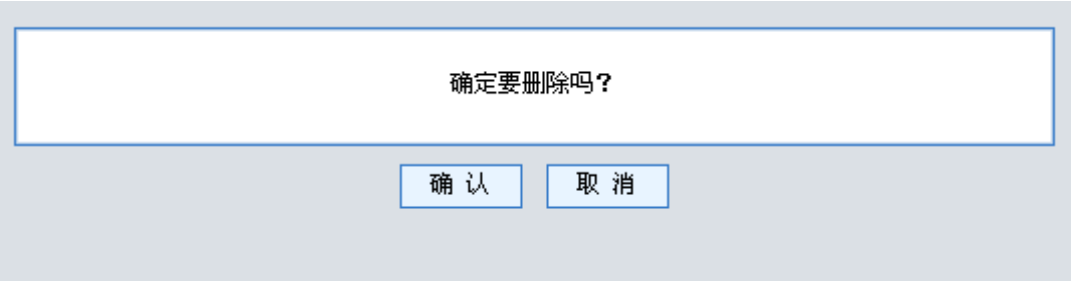


图 13　21　删除数据库访问客户端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

13.4 服务端

该部分用于配置所有的数据库访问的服务端任务。特别指出的是，与客户端不同，服务端只需配置普通模式下的访问任务，对于透明模式的服务端任务，系统内部已经配置好，无需用户配置。WEB 界面导航菜单如下：

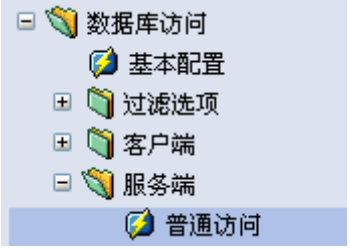


图 13　22　数据库访问服务端导航菜单

下面详细介绍服务端的普通模式的任务配置，WEB 界面显示如下：

图 13　23 数据库访问服务端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

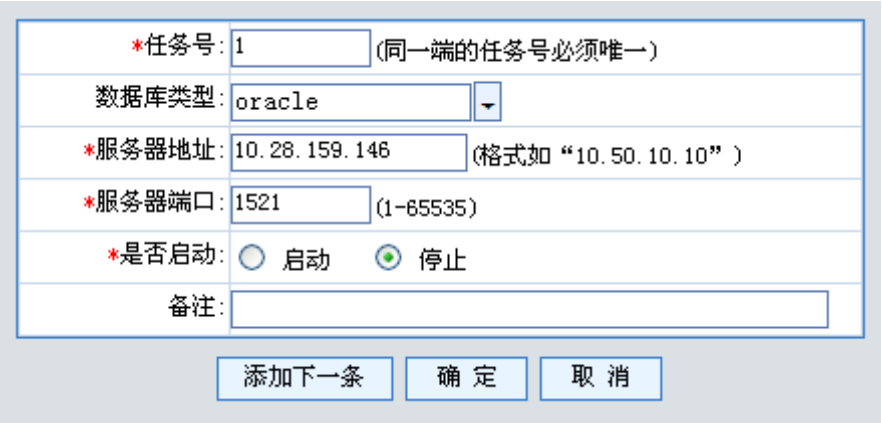


图 13　24　添加数据库访问服务端普通任务

图中各配置项，说明如下：

◆ **任务号**

任务号是客户端正常访问的基础，所以一个服务端任务的任务号必须与对方主机模块中相对应的客户端任务的任务号完全相同，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个邮件访问模块内必须唯一。

该配置项必填。

◆ **数据库类型**

数据库类型表示该任务所使用的数据库。目前支持的数据库类型有 ORACLE、SQLSERVER、DB2、MYSQL、SYBASE 等。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“oracle”。

◆ **服务器地址**

服务器地址为目标访问网络中的数据库服务器的真实 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也不能为 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问网络中的数据库服务器的真实端口。

取值范围：1－65535，默认为 1521 端口。

该配置项为必填项。

◆ **是否启动**

该选项用于设置是否启动该服务端任务。默认为“停止”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

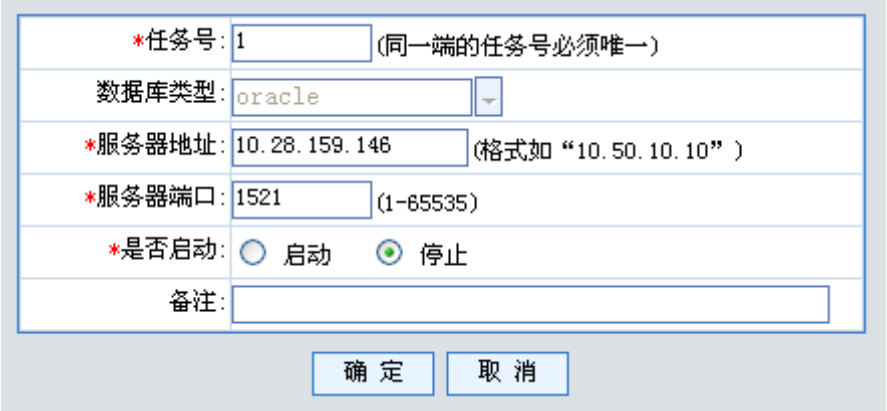


图 13 25 编辑数据库访问服务端普通任务

编辑操作时，除“任务号”、“数据库类型”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

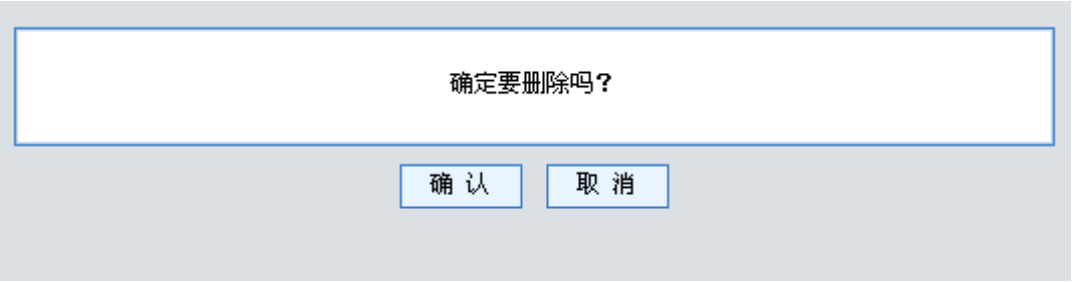


图 13　26　删除数据库访问服务端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

第 14 章　定制访问

定制模块包含“TCP 访问”、“UDP 访问”两个模块，可以支持基于 TCP/UDP 协议的、针对固定服务器地址和端口号的常规访问。访问模式包括透明访问和普通访问。对于透明访问，管理员只需在 SIS 安全隔离网闸的内网主机配置一条访问任务即可；而普通访问，需要在 SIS 安全隔离网闸的内、外网两个主机系统分别添加“客户端任务”和“服务端任务”，并且两条任务的任务号应一一对应，具体说明如下。

14.1 定制 TCP

TCP 访问模块用于配置通过 SIS 安全隔离网闸基于 TCP 协议的访问任务。主要包括：基本配置、TCP 客户端、TCP 服务端等三个子模块。该模块的作用是在 SIS 安全隔离网闸两侧建立基于 TCP 协议的一一对应的任务（以一一对应任务号的方式），通过加密传输的方式搭建起一条单向安全访问通道。WEB 界面示意图如下：

图 14　1　定制 TCP WEB 界面功能菜单

14.1.1　基本配置

“基本配置”部分，用于配置定制 TCP 访问任务的基本参数，目前仅包括“当前服务状态”参数。WEB 界面示意图如下：

图 14　2　定制 TCP 基本配置界面

参数说明如下表：

表 14　1　基本配置参数说明

参数名称	说　明
当前服务状态	表示定制 TCP 访问任务的系统运行状态。若为“启动服务”，则表示当前所有任务已处于可运行状态，在此状态下，任务一旦添加且单独启停按钮为“启动”时，任务随即运行；若为“停止服务”，即使添加了任务且单独启停按钮为“启动”，任务也不运行。 服务状态值：“启动服务”或“停止服务”。

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

14.1.2　客户端

该部分用于配置所有的定制 TCP 客户端的访问任务，包括：透明模式的客户端任务、普通模式的客户端任务。依次说明如下：

一. 透明模式的定制 TCP 客户端任务

WEB 界面显示如下：

图 14　3　定制 TCP 客户端透明任务列表显示

该模块主要包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

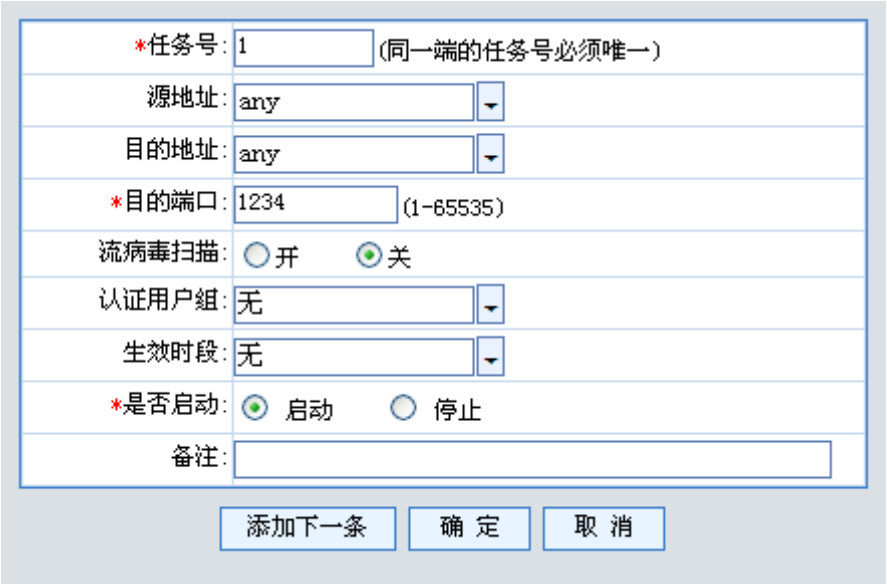


图 14 4 添加定制 TCP 客户端透明任务

图中定制 TCP 透明模式的客户端任务的配置项，说明如下：

◆ **任务号**

用于表示该任务。对于透明访问任务，任务号相当于序号的作用。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个定制访问模块内必须唯一。

该配置项必填。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的地址**

目的地址表示目标访问网络中真实服务器的 IP 地址或域名。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的端口**

目的端口指明对方网络中服务器的真实端口。

取值范围：1－65535。

该配置项必填。

◆ **流病毒扫描**

设置是否对文件传输流进行病毒扫描，默认为“关”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端

到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **是否启动**

该选项用于设置是否启动该客户端任务。默认为“启动”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

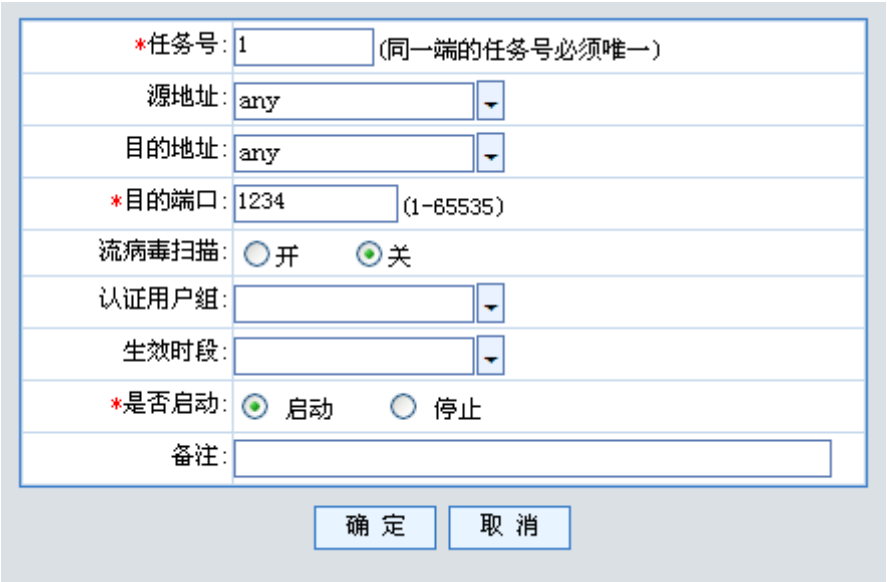


图 14 5 编辑定制 TCP 客户端透明任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

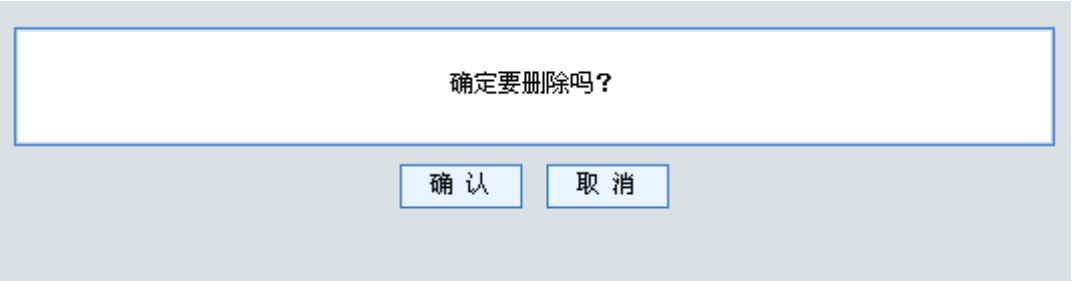


图 14 6 删除定制 TCP 客户端透明任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

二. 普通模式的定制 TCP 客户端任务

WEB 界面显示如下：

图 14 7 定制 TCP 客户端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

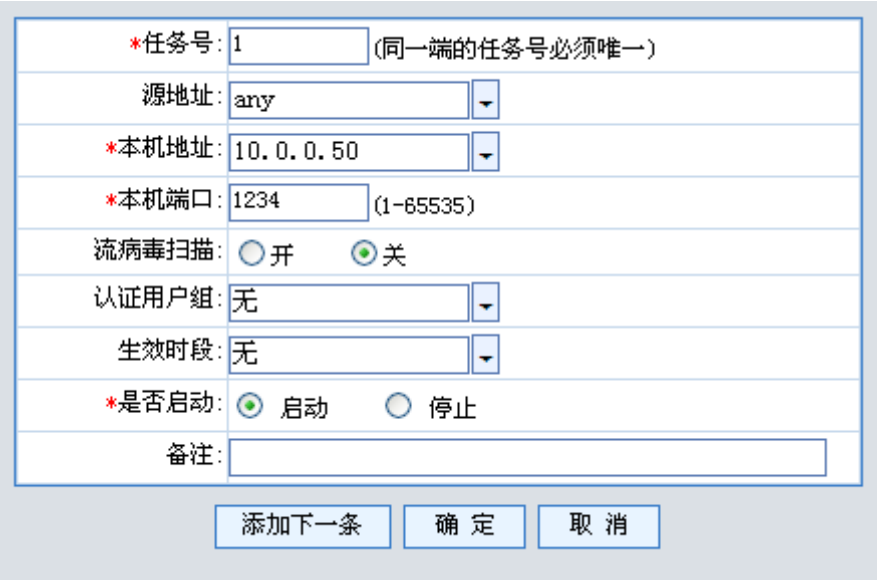


图 14 8 添加定制 TCP 客户端透明任务

图中定制 TCP 普通模式的客户端任务的配置项，说明如下：

◆ **任务号**

任务号是定制 TCP 客户端正常访问的基础，每个任务号必须与对方主机模块配置的相对应的服务端任务的任务号完全相同，即客户端任务的任务号必须与服务端相应的任务号一一对应，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个定制访问模块内必须唯一。

该配置项必填。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置>>网络接口”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

本机端口为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535。

该配置项为必填项。

◆ **流病毒扫描**

设置是否对文件传输流进行病毒扫描，默认为“关”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **是否启动**

该选项用于设置是否启动该客户端任务。默认为“启动”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

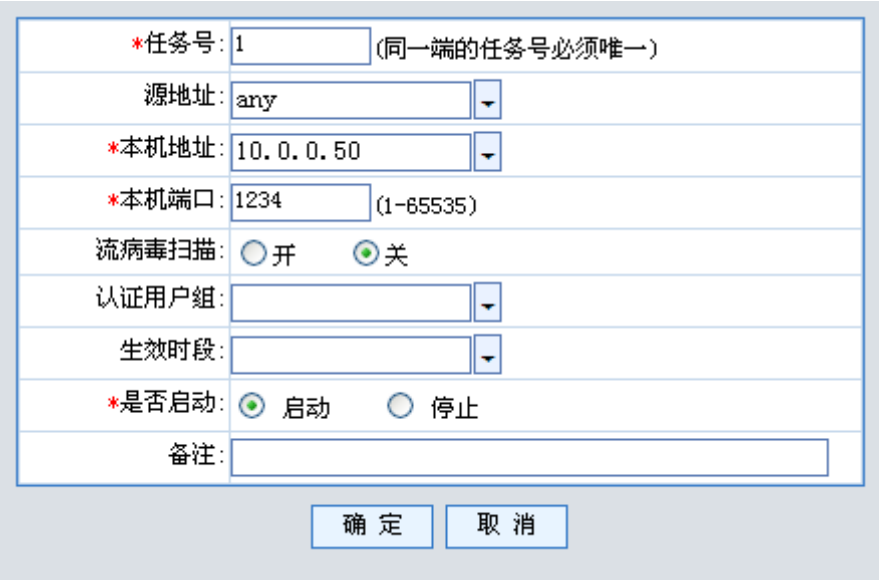


图 14 9 编辑定制 TCP 客户端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

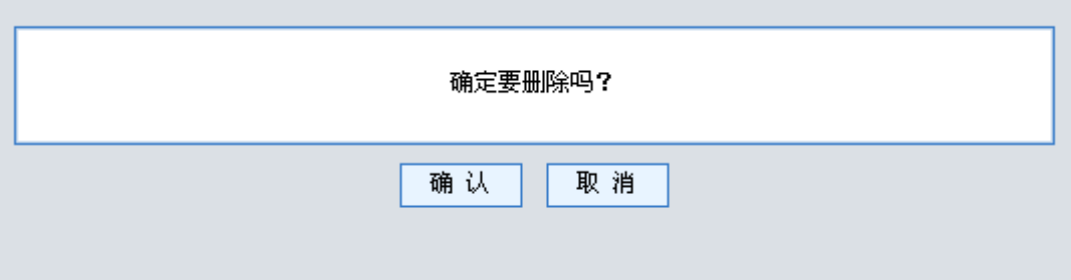


图 14 10 删除定制 TCP 客户端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

14.1.3 服务端

该部分用于配置所有的定制 TCP 服务端的访问任务。特别指出的是，与客户端不同，服务端只需配置普通模式下的访问任务，对于透明模式的服务端任务，系统内部已经配置好，无需用户配置。WEB 界面导航菜单如下：

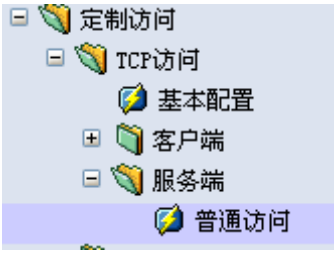


图 14 11 定制 TCP 服务端导航菜单

下面详细介绍服务端的普通模式的任务配置：

一. 普通模式的定制 TCP 服务端任务

WEB 界面显示如下：

图 14　12　定制 TCP 服务端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

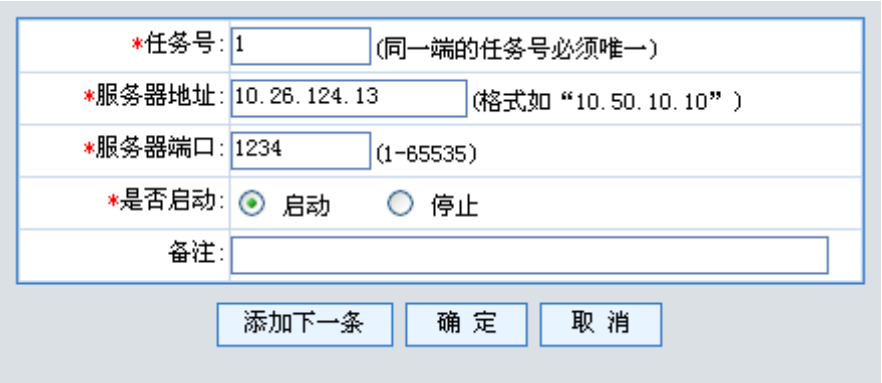


图 14　13　添加定制 TCP 服务端普通任务

图中定制 TCP 普通模式的服务端任务的配置项，说明如下：

◆ **任务号**

任务号是客户端正常访问的基础，所以一个服务端任务的任务号必须与对方主机模块中相对应的客户端任务的任务号完全相同，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个定制访问模块内必须唯一。

该配置项必填。

◆ **服务器地址**

服务器地址为目标访问网络中的服务器的真实 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也支持 IP 地址 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问网络中的服务器的真实端口。

取值范围：1－65535。

该配置项为必填项。

◆ **是否启动**

该选项用于设置是否启动该服务端任务。默认为“启动”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

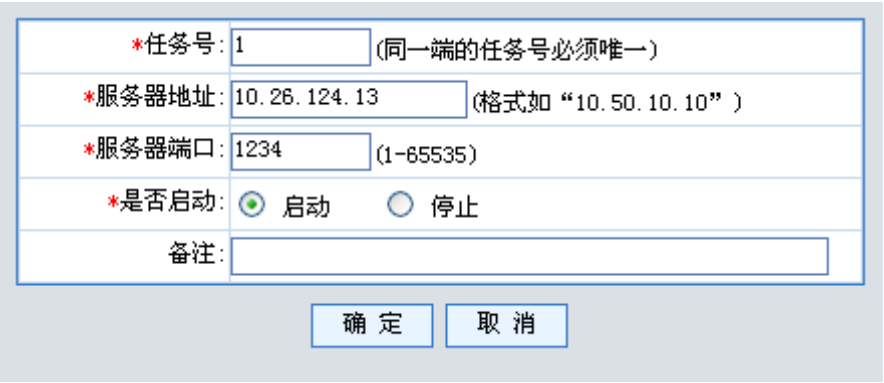


图 14 14 编辑定制 TCP 服务端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

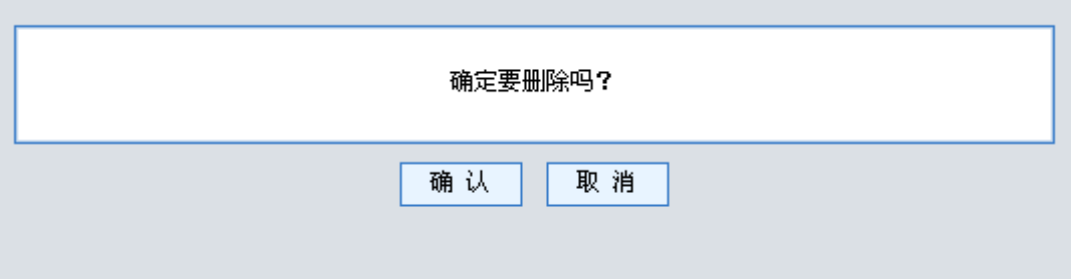


图 14 15 删除定制 TCP 服务端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

14.2 定制 UDP

UDP 访问模块用于配置通过 SIS 安全隔离网闸基于 UDP 协议的访问任务。该模块的作用在 SIS 安全隔离网闸两侧建立基于 UDP 协议的一一对应的任务（通过任务号来一一对应），通过加密传输的方式搭建起一条单向安全访问通道。

该模块用于配置所有与定制 UDP 有关的访问任务，及相关的参数配置，包括：基本参数、UDP 客户端、UDP 服务端等三个子模块。WEB 界面示意图如下：

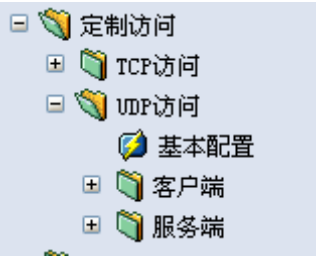


图 14 16 定制 UDP WEB 界面功能菜单

14.2.1 基本配置

“基本配置”部分，用于配置定制 UDP 访问任务的基本参数，目前仅包括“当前服务状态”参数。WEB 界面示意图如下：

图 14 17 定制 UDP 基本配置界面

参数说明如下表：

表 14 2 基本配置参数说明

参数名称	说 明
当前服务状态	表示定制 UDP 访问任务的系统运行状态。若为“启动服务”，则表示当前所有任务已处于可运行状态，在此状态下，任务一旦添加且单独启停按钮为“启

	动”时，任务随即运行；若为“停止服务”，即使添加了任务且单独启停按钮为“启动”，任务也不运行。 服务状态值：“启动服务”或“停止服务”。

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

14.2.2 客户端

该部分用于配置所有的定制 UDP 客户端的访问任务，包括：透明模式的客户端任务、普通模式的客户端任务。依次说明如下：

一. 透明模式的定制 UDP 客户端任务

WEB 界面显示如下：

图 14 18 定制 UDP 客户端透明任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

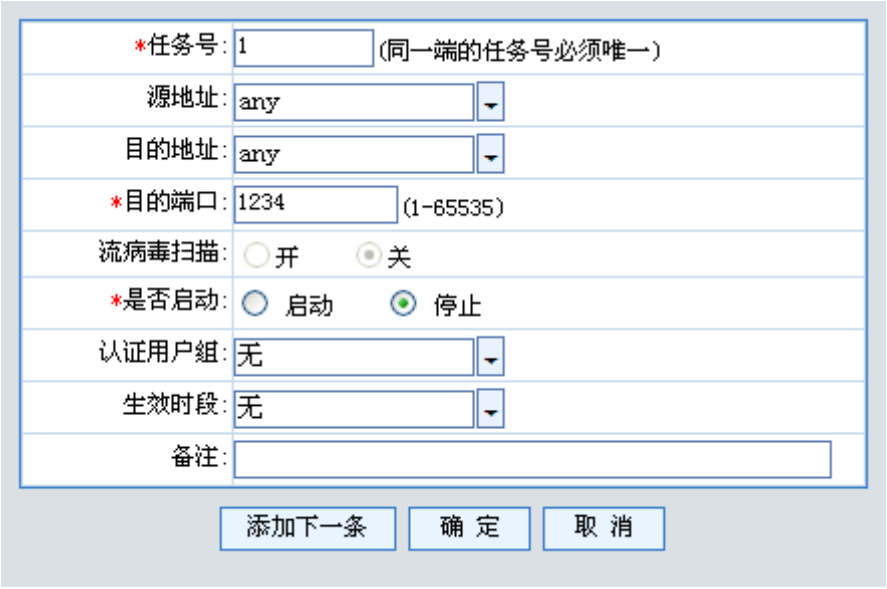


图 14 19 添加定制 UDP 客户端透明任务

图中定制 UDP 透明模式的客户端任务的配置项，说明如下：

◆ **任务号**

用于表示该任务。用于表示该任务。对于透明访问任务，任务号相当于序号的作用。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个定制访问模块内必须唯一。

该配置项必填。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的地址**

目的地址表示对方网络中的真实服务器的 IP 地址或域名。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的端口**

目的端口指明对方网络中的服务器的真实端口。

取值范围：1－65535。

该配置项必填。

◆ **流病毒扫描**

设置是否对 UDP 流进行病毒扫描，默认为“关”。

◆ **是否启动**

该选项用于设置是否启动该客户端任务。默认为“停止”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

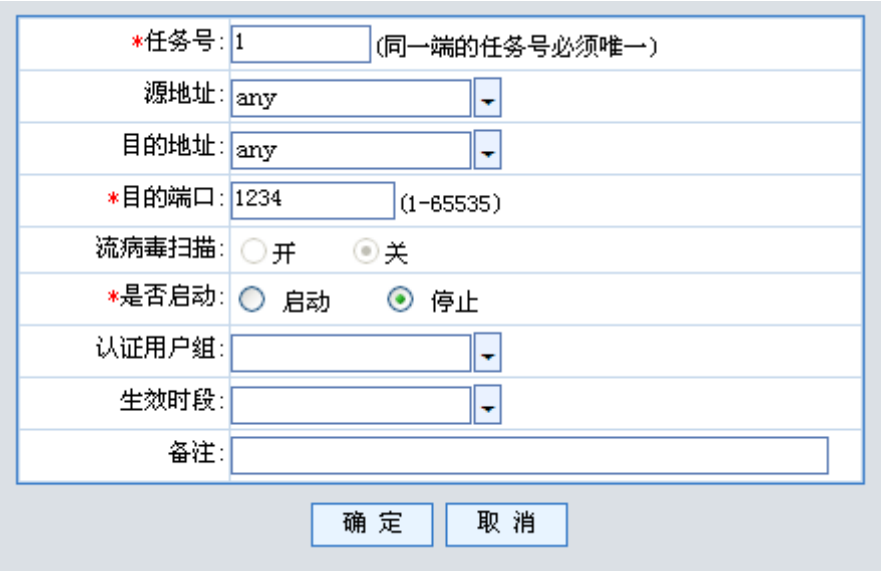


图 14 20 编辑定制 UDP 客户端透明任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

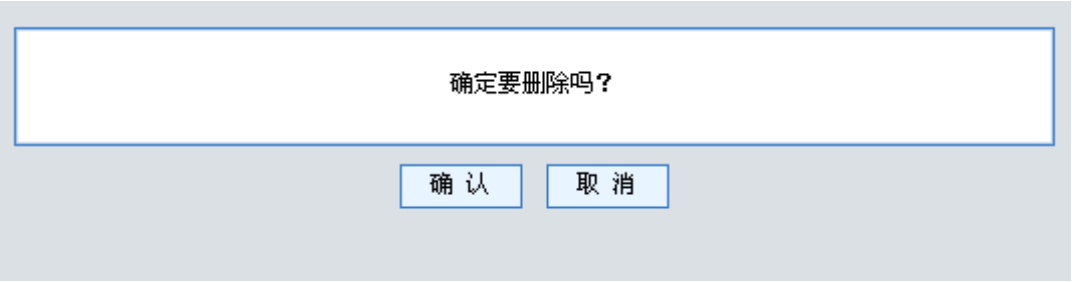


图 14　21　删除定制 UDP 客户端透明任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4)　其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

二. 普通模式的定制 UDP 客户端任务

WEB 界面显示如下：

图 14　22　定制 UDP 客户端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1)　添加操作

在上图中，点击“添加”按钮，弹出界面如下：

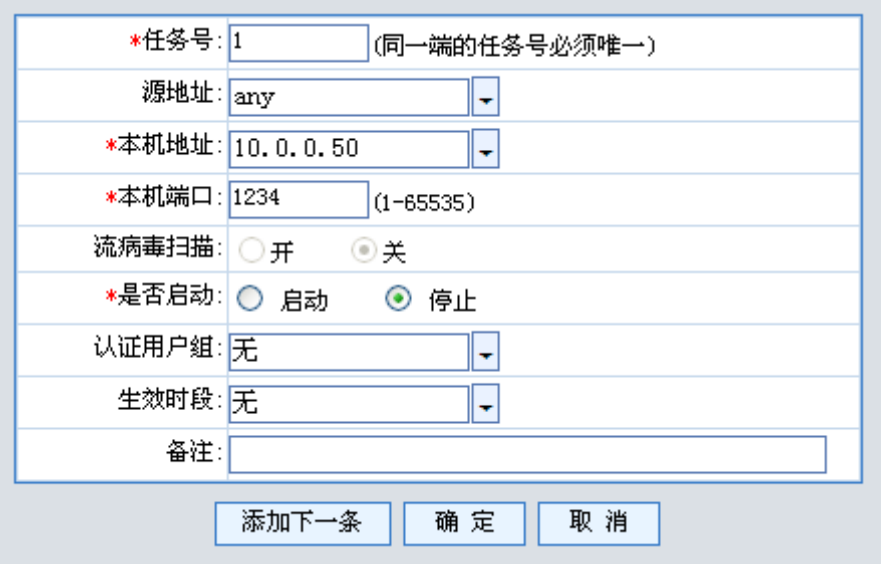


图 14 23 添加定制 UDP 客户端普通任务

图中定制 UDP 普通模式的客户端任务的配置项，说明如下：

◆ **任务号**

任务号是定制 UDP 客户端正常访问的基础，每个任务号必须与对方主机模块配置的相对应的服务端任务的任务号完全相同，即客户端任务的任务号必须与服务端相应的任务号一一对应，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个定制访问模块内必须唯一。

该配置项必填。

◆ **源地址**

源地址指出该任务允许通过的源地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置>>网络接口”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

本机端口为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535。

该配置项为必填项。

◆ **流病毒扫描**

设置是否对 UDP 流进行病毒扫描，默认为“关”。

◆ **是否启动**

该选项用于设置是否启动该客户端任务。默认为“停止”。

◆ **认证用户组**

对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

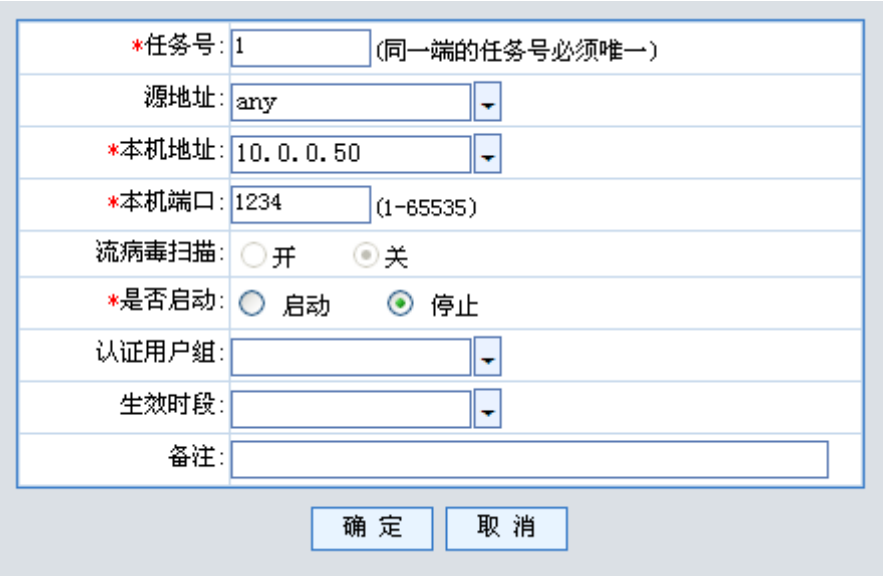


图 14 24 编辑定制 UDP 客户端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

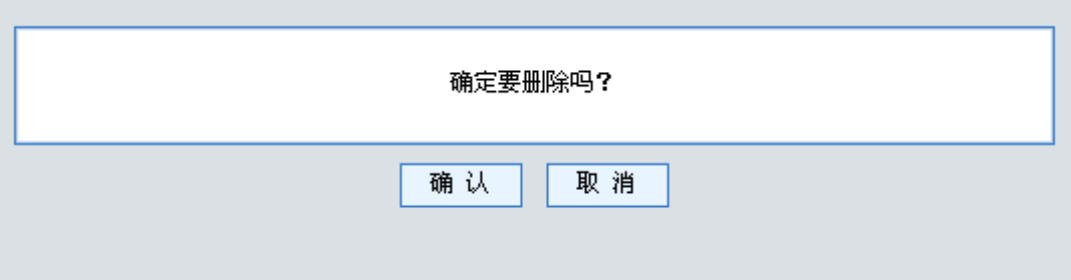


图 14 25 删除定制 UDP 客户端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

✧

14.2.3 服务端

该部分用于配置所有的定制 UDP 服务端的访问任务。特别指出的是，与客户端不同，服务端只需配置普通模式下的访问任务，对于透明模式的服务端任务，系统内部已经配置好，无需用户配置。WEB 界面导航菜单如下：

图 14 26 定制 UDP 服务端导航菜单

下面详细介绍服务端的普通模式的任务配置：WEB 界面显示如下：

图 14　27　定制 UDP 服务端普通任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

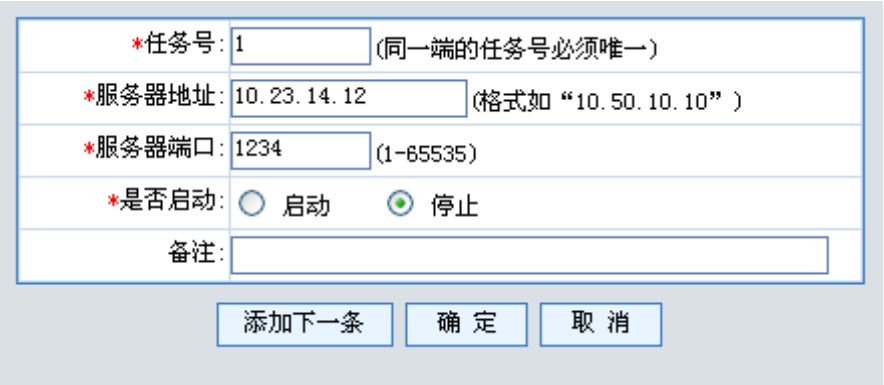


图 14　28　添加定制 UDP 服务端普通任务

图中定制 UDP 普通模式的服务端任务的配置项，说明如下：

◆ **任务号**

任务号是客户端正常访问的基础，所以一个服务端任务的任务号必须与对方主机模块中相对应的客户端任务的任务号完全相同，否则无法正常访问。

任务号用 0－9 等 10 个数字表示的序号，最多可以添加 1000 个任务。而且，在整个定制访问模块内必须唯一。

该配置项必填。

◆ **服务器地址**

服务器地址为目标访问网络中的服务器的真实 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也支持 IP 地址 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问网络中的服务器的真实端口。

取值范围：1－65535。

该配置项为必填项。

◆ **是否启动**

该选项用于设置是否启动该服务端任务。默认为“停止”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

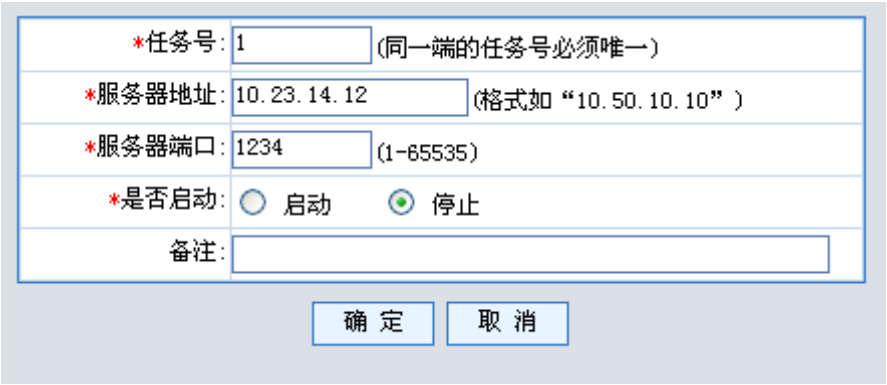


图 14 29 编辑定制 UDP 服务端普通任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

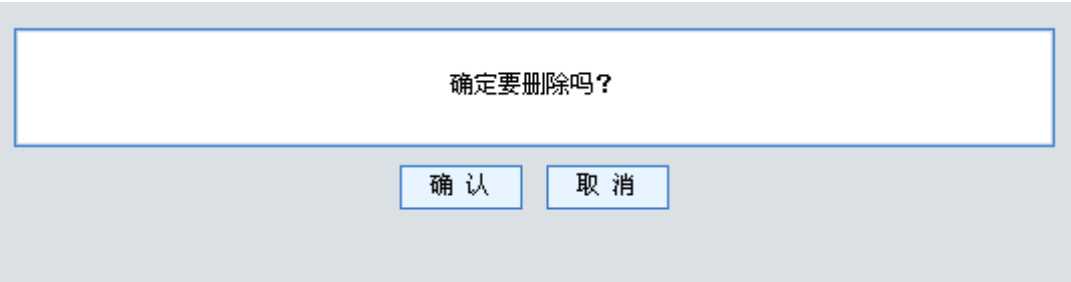


图 14 30 删除定制 UDP 服务端普通任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

第 15 章 安全通道

该模块支持内外网用户安全快速地访问所有应用服务器。通过配置安全通道服务端和客户端任务，实现访问，更大限度地控制应用服务的访问请求，达到更加安全的效果。

该模块包括：基本配置、客户端任务配置、以及服务端任务配置等三个模块。

15.1 基本配置

“基本配置”部分，用于配置安全通道任务的基本参数，目前仅包括“当前服务状态”参数。WEB 界面示意图如下：

图 15 1 安全通道基本配置界面

参数说明如下表：

表 15 1 基本配置参数说明

参数名称	说 明
当前服务状态	表示安全通道任务的系统运行状态。若为“启动服务”，则表示当前所有任务已处于可运行状态，在此状态下，任务一旦添加且单独启停按钮为“启动”时，任务随即运行；若为“停止服务”，即使添加了任务且单独启停按钮为“启动”，任务也不运行。 服务状态值：“启动服务”或“停止服务”。

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

15.2 客户端

该部分用于配置所有的安全通道的客户端任务。WEB 界面显示如下：

图 15 2 列表显示安全通道客户端端任务

该模块主要包括四类操作，依次说明如下：

1) 添加任务操作

在上图中，点击“添加”按钮，弹出界面如下：

图 15 3 添加安全通道客户端任务

图中安全通道客户端任务的各配置项，说明如下：

◆ **任务号**

发送任务号，只能为 1-200 的数字。该项配置必须填写。任务号是安全通道访问的基础，网闸同侧的任务号必须唯一。

特别指出：若配置“普通访问”任务，则要求客户端与服务端对应的任务号一致，否则会导致运行不正常。

◆ **访问类型**

访问类型包括普通访问、透明访问，默认选中透明访问。

普通访问，指与网闸相连的外部客户端访问的目的主机是网闸客户端公开服务地址，网闸通过隔离交换模块将用户请求转到服务端相同任务号的任务所指定的实际服务器。这种访问类型，配置任务时，需要分别在网闸的客户端、服务端配置任务，且任务号必须相同。支持网闸两侧 IP 地址同属一网段的网络。

透明访问，访问原理与普通访问类型完全相同，区别在于此时外部客户端访问的目的地址是网闸另一侧的实际服务器地址，且往往网闸两则的 IP 地址在不同网段。这种类型最大的好处在于无需修改用户的网络拓扑，实现透明接入。

注：透明访问模式不支持内外网为同一网段的网络应用。

◆ **源地址**

源地址指出该任务允许通过的源地址。其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **源端口**

源端口指出该任务允许通过的源端口。取值范围：1－65535，其值输入形如：1234 或 120:3000。

◆ **目的地址**

目的地址表示对方网络中客户端所需访问的服务器的 IP 地址或地址对象。若网闸内外网同网段，目的地址必须是 IP 地址形式，且为真实服务器 IP 地址，该真实服务器 IP 地址必须绑定到网闸上；若网闸内外网不在同一网段，目的地址必须是地址对象，且为真实服务器 IP 地址对象。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”或映射 IP 地址，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **目的端口**

目的端口指明对方网络中客户端所需访问的服务器的真实端口。

取值范围：1－65535，其值输入形如：1234 或 120:3000。若未填，则依据服务类型决定端口号。若已填，但又选择知名服务(非 tcp_any、非 udp_any)，则所填端口号无效。

◆ **服务类型**

服务类型从下拉列表中选择即可，目前支持的类型有 H323、IRC、MMS、HTTP、HTTPS、DNS、FTP、SMTP、POP3 等。

◆ **是否启动**

该选项用于设置是否启动该客户端任务。默认为“启动”。

◆ **开启日志**

此项允许用户是否开启安全通道模块的日志，“开”表示将记录业务日志，“关”则不记录业务日志，默认“关”。

◆ **抗攻击**

此选项可以开启或关闭抗攻击功能，并可以设置抵抗攻击的每秒个数，默认为不使用抗攻击功能。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

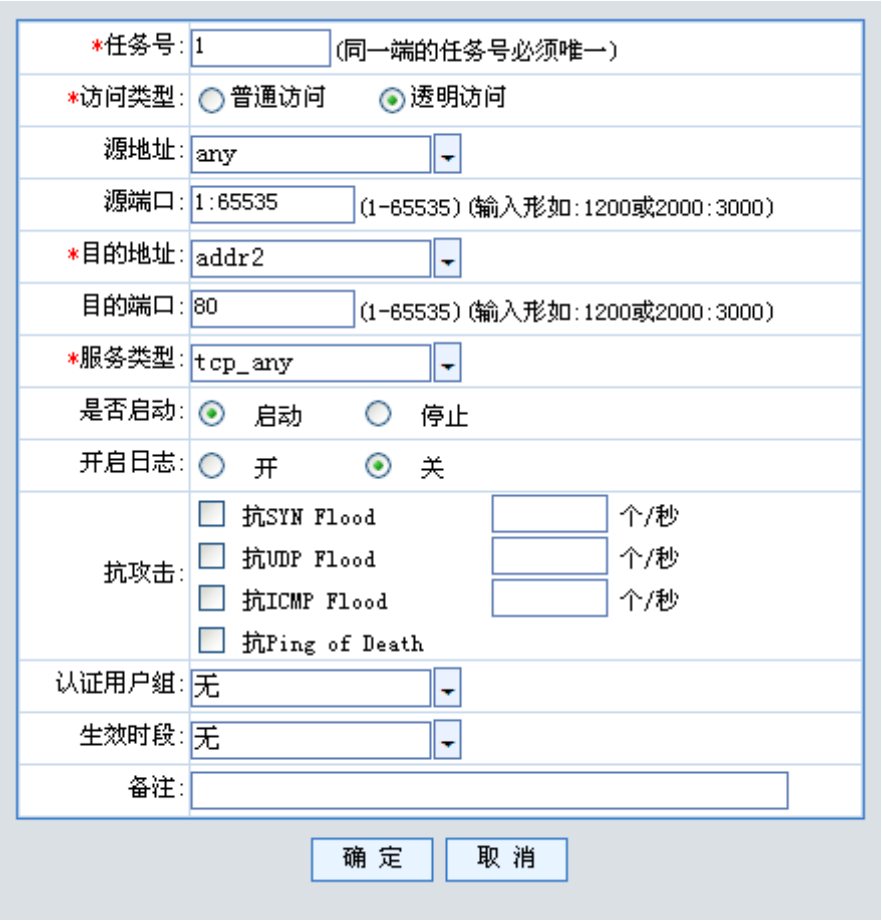


图 15 4 修改安全通道客户端任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

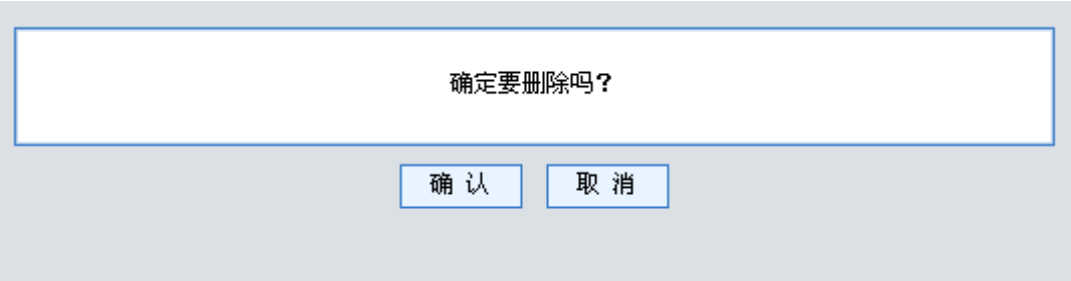


图 15 5 删除安全通道客户端端任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

15.3 服务端

该部分用于配置所有的安全通道的服务端任务。特别指出的是，与客户端不同，只有配置普通访问任务时，才需要服务端任务，对于透明访问任务，服务端的任务系统内部已经配置好，无需用户配置。WEB 界面显示如下：

图 15 6 列表显示安全通道服务端任务

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

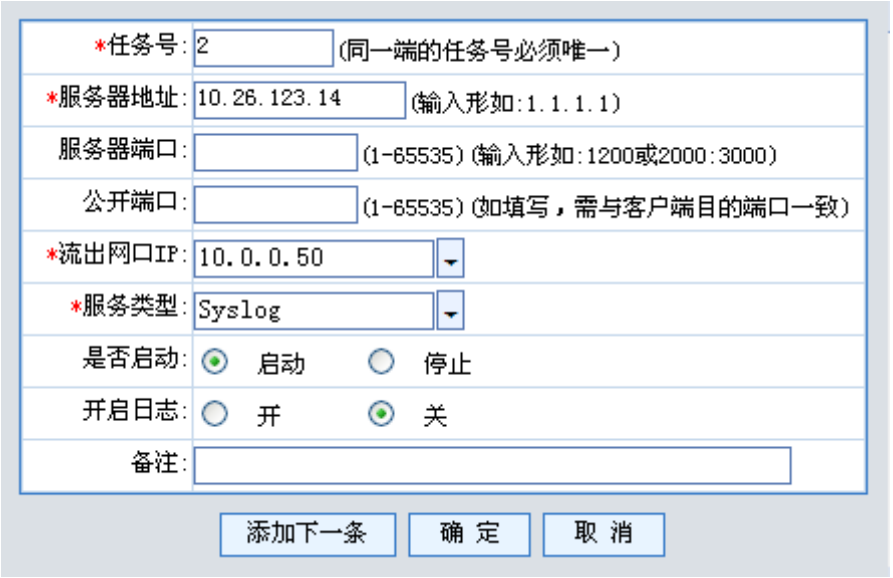


图 15 7 添加安全通道服务端任务

图中各配置项，说明如下：

◆ **任务号**

接收任务号，只能为 1-200 的数字。该项配置必须填写。任务号是安全通道访问的基础，网闸同侧的任务号必须唯一。要求与发送端的任务号一一对应。

◆ **服务器地址**

服务器地址为目标访问网络中的服务器的真实 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也不能为 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问网络中的服务器的真实端口。

取值范围：1－65535，其值输入形如：1234 或 120:3000。若未填，则依据服务类型决定端口号。若已填，但又选择知名服务(非 tcp_any、非 udp_any)，则所填端口号无效。

◆ **流出网口 IP**

指名网络流量从哪个口出去，到达目标服务器。其值为网闸内外网 IP 地址，在列表框中选择。

◆ **服务类型**

服务类型从下拉列表中选择即可，目前支持的类型有 H323、IRC、MMS、HTTP、HTTPS、DNS、FTP、SMTP、POP3 等。

◆ **是否启动**

该选项用于设置是否启动该服务端任务。默认为“启动”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，允许继续添加任务；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后的编辑图标，弹出编辑窗口，如下图：

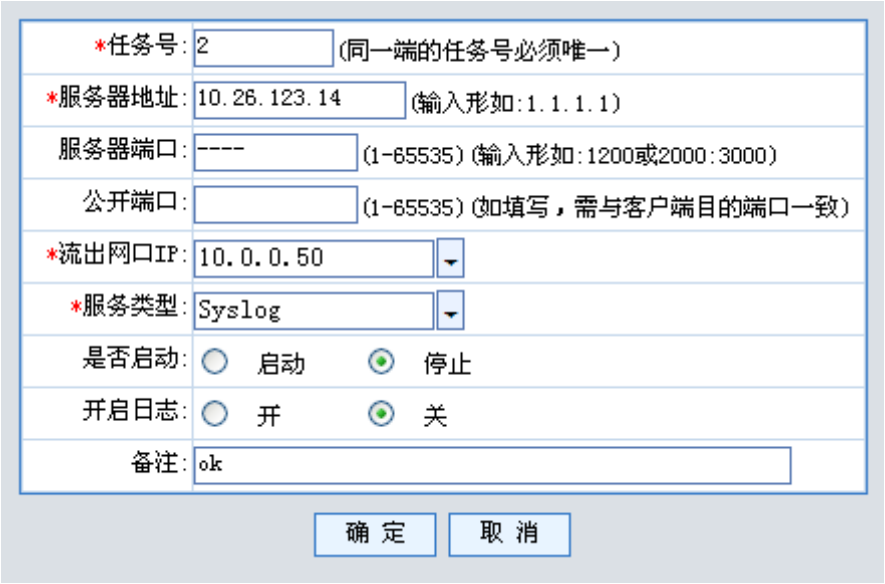


图 15 8 编辑安全通道服务端任务

编辑操作时，除“任务号”不能编辑外，其他与添加操作相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后的删除图标，弹出编辑窗口，如下图：

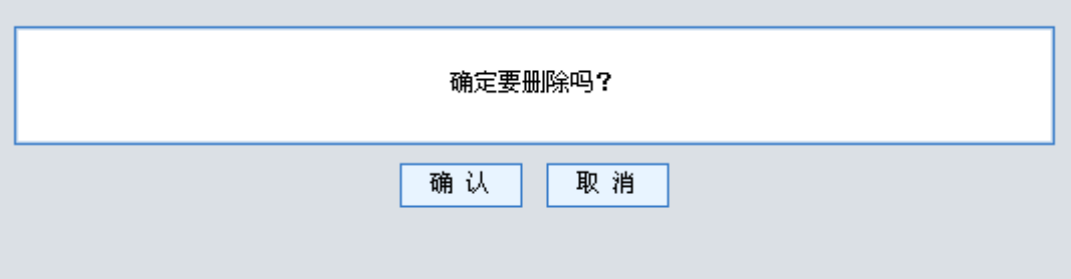


图 15 9 删除安全通道服务端任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“公共操作”一章中的相关描述。

第 16 章　消息传输

消息传输模块支持各种消息在外部网和涉密网之间的安全传输，消息类型包括文件和字符串。消息传输支持以数字证书方式的强用户认证和通讯加密，以及用户口令认证，强化消息交换的安全性和保密性。整个模块由两个部分组成：消息传输客户端系统、网闸系统。客户端系统的操作说明请参见客户端系统操作手册。在此，主要介绍网闸系统的操作说明。

网闸系统的基本功能包括基本配置、客户端任务、服务端任务、内容控制和用户管理等五个模块，导航菜单如下图：

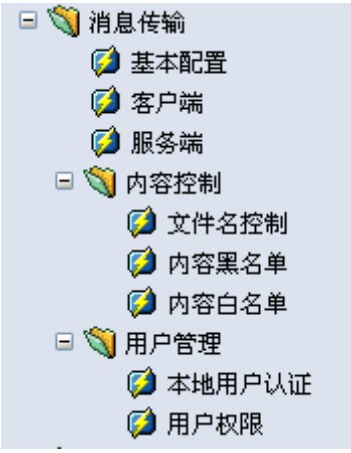


图 16　1　消息传输 WEB 界面导航菜单

16.1 基本配置

“基本配置”部分，主要配置本地证书、消息传输服务的启停控制等。WEB 界面示意图如下：

图 16 2 基本配置界面

16.1.1 证书设置

本地证书及其相关文件的导入，对于采用身份认证和通信 SSL 加密模式是必须的。需导入的对象包括：CA 证书、用户证书、用户证书的私钥、私钥口令，以及对端证书公共名等四个。其中，CA 证书必须与通信对端的用户证书的 CA 证书一致，即通信双方的用户证书都必须由同一个 CA 签发。用户证书、用户证书私钥、私钥口令三者必须一致，否则通信无法正常进行。

操作方法：

1) CA 证书、用户证书、用户证书的私钥等三项可以点击“浏览”按钮引入相应文件，也可以直接在文本框中直接输入文件路径；
2) 私钥口令：直接在文件框中输入即可；
3) 对端证书公共名：指明与本主机通信的对端客户端证书中使用的公共名；
4) 以上各项都输入完毕后，点击“导入”按钮；
5) 导入完毕后，在 WEB 页面的下面的“文件交换证书列表”中，会显示导入的证书信息。对于 CA 证书、用户证书私钥，不显示其公共名、过期时间。用户也可以点击该表每项右边的删除按钮，删除该项。

特别说明:

✧ 当消息传输的任务采用身份认证/通讯加密传输模式时，必须在此导入证书相关的文件，否则相应的任务无法正常运行。而对于普通的用户口令认证、非加密模式下的消息传输，本地导入的证书不会被使用；

✧ 证书的合法性和有效性的检查，在相应的访问任务初始化时进行，若失败，相应的访问任务立即中止，并在日志中有相关说明。而在导入的过程中，则不做检查；

导入时，CA 证书、用户证书、用户证书的私钥、私钥口令、对端证书公共名等各项必须同时填写。

16.1.2 服务管理

服务管理主要用于控制服务的运行状态。操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服务”按钮被 Enable。

- **停止服务：**

  单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

16.2 客户端

该部分可以对网闸中消息传输模块的客户端任务进行添加、修改和删除等操作。WEB 界面示意图如下：

图 16 3 客户端任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

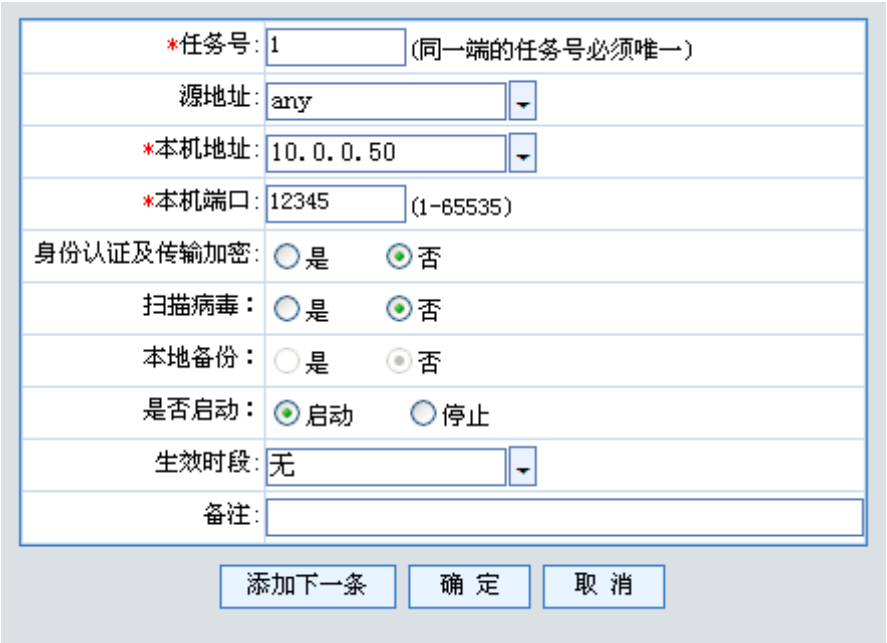


图 16 4 添加客户端任务

图中客户端的配置项，说明如下：

◆ **任务号**

任务号是消息传输的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则消息无法正常传输。

任务号只用数字表示，最多可以添加 1000 个任务。该配置项必填。

◆ **源地址**

源地址指出允许访问本机的源客户端的地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“any”。

下拉列表初始只有两项：“无”、“any”，其菜单项来源于“资源定义”中定义的地址列表、地址组、服务器地址、域名地址等四类地址。

◆ **本机地址**

本机地址为本机供客户端网络访问的设备 IP 地址，包括本机物理设备地址、别名设备地址、冗余设备地址。

其值从下拉列表中选取即可，但不能为空，也不能选取“无”菜单选项，默认为“无”。并且，此处选择的本地地址必须为客户端可以访问到的地址。

下拉列表的值来源于“网络配置>>网络接口”中设置的物理设备及其别名设备的 IP 地址，以及冗余设备地址。

该配置项为必填项。

◆ **本机端口**

本机端口为本机提供该任务的监听端口，管理员可以根据实际需求进行选择配置。管理员进行配置时，还需了解每条访问任务所使用的端口（固定端口号），配置的端口不能和其它任务冲突。

取值范围：1－65535。

该配置项为必填项。

◆ **身份认证及传输加密**

设置是否进行身份认证，并在消息的传输过程中采用 SSL 加密方式，默认为“否”。

◆ **扫描病毒**

设置是否在消息的传输过程中对消息进行病毒扫描，默认为“否”。

网闸出厂时的标准配置中，该选项被关闭。

◆ **本地备份**

设置消息在传输过程中是否在网闸中进行备份，默认为“否”。特别指出的是，若采用本地备份模式，则必须考虑到实际传输的单个消息的最大容量：如果单个消息的最大容量超过网闸本机的实际缓存（与网闸的运行状态有关）大小，将导致该消息无法正确传输。

非特殊情况，建议用户不要备份。网闸出厂时的标准配置中，该选项被关闭。

◆ **生效时段**

“生效时段”指出该任务在指定的时间段内生效，其它时间内为失效状态。

其值从下拉列表中选取，可以选择“无”，默认为“无”。

下拉列表初始仅有“无”一项，其菜单项来源于“资源定义”>>“时间”中的时间列表、时间组两类。

◆ **是否启动**

该选项用于设置是否启动该客户端任务。默认为“启动”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后面的编辑图标，弹出编辑窗口，如下图：

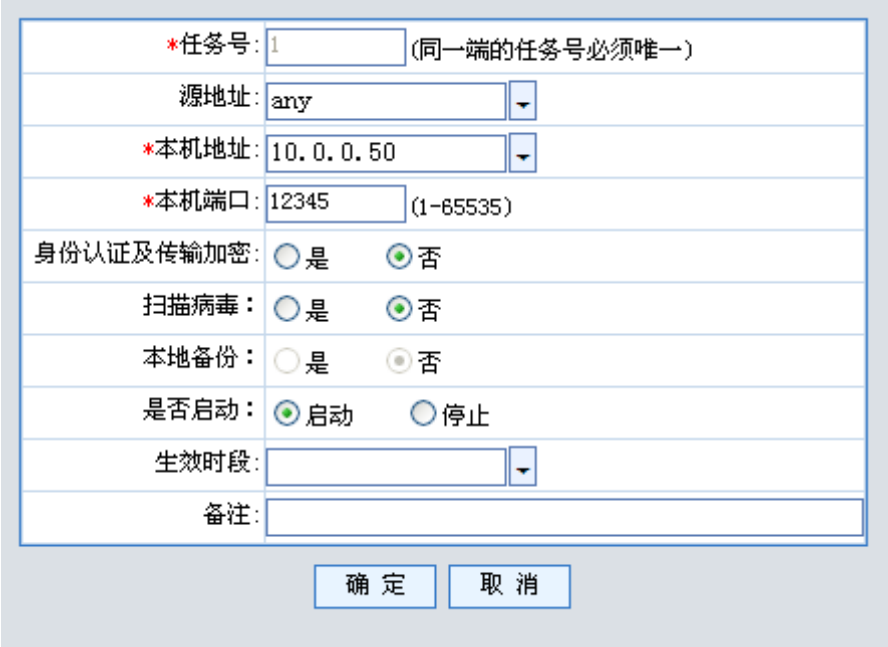


图 16 5 编辑客户端任务

编辑操作时，除任务号不能修改外，其他与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后面的删除图标，弹出编辑窗口，如下图：

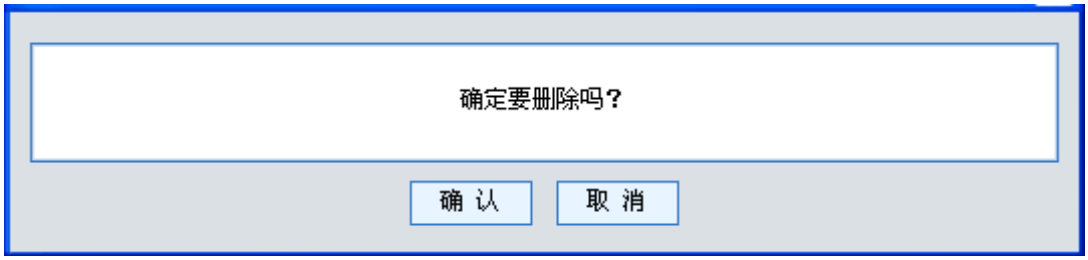


图 16 6 删除客户端任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

16.3 服务端

该部分可以对网闸中消息传输模块的服务端任务进行添加、修改和删除等操作。WEB 界面示意图如下：

图 16 7 服务端任务列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

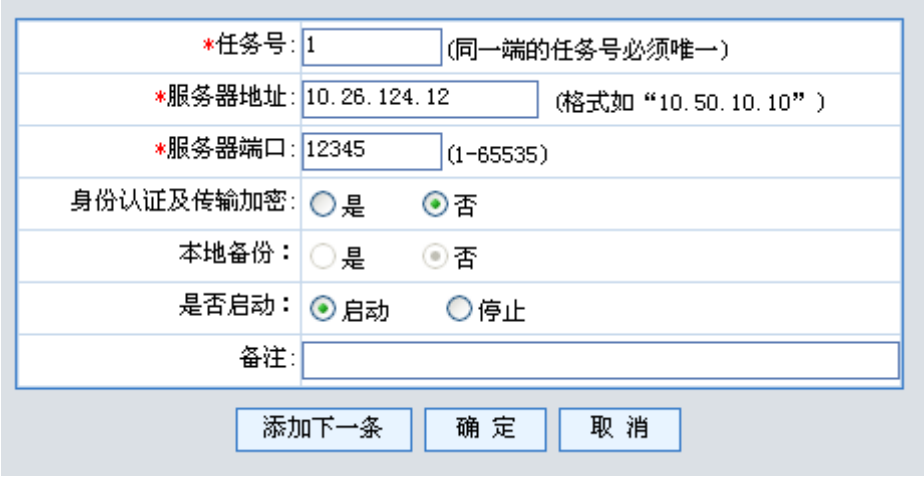


图 16 8 添加服务端任务

图中服务端任务的配置项，说明如下：

◆ **任务号**

任务号是消息传输的基础，每个客户端任务的任务号必须与服务端相应的任务号一一对应，否则消息无法正常传输。

任务号只用数字表示，最多可以添加 1000 个任务。该配置项必填。

◆ **服务器地址**

服务器地址为消息传输目的客户端的 IP 地址。

其值直接在文本框中输入，其格式必须符合 IP 地址的形式，如：10.50.10.10，且不带掩码，也支持 IP 地址 0.0.0.0。

该配置项为必填项。

◆ **服务器端口**

服务器端口为目标访问消息传输客户端所在的服务器的真实端口。

取值范围：1－65535。

该配置项为必填项。

◆ **身份认证及传输加密**

设置是否进行身份认证，并在消息的传输过程中采用 SSL 加密方式，默认为“是”。

◆ **本地备份**

设置消息在传输过程中是否在网闸中进行备份，默认为“否”。特别指出的是，若采用本地备份模式，则必须考虑到实际传输的单个消息的最大容量：如果单个消息的最大容量超过网闸本机的实际缓存（与网闸的运行状态有关）大小，将导致该消息无法正确传输。

非特殊情况，建议用户不要备份。网闸出厂时的标准配置中，该选项被关闭。

◆ **是否启动**

该选项用于设置是否启动该服务端任务。默认为“启动”。

◆ **备注**

该任务的备注或说明。

取值说明请参考“公共操作”一章中的相关描述。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个任务后面的编辑图标，弹出编辑窗口，如下图：

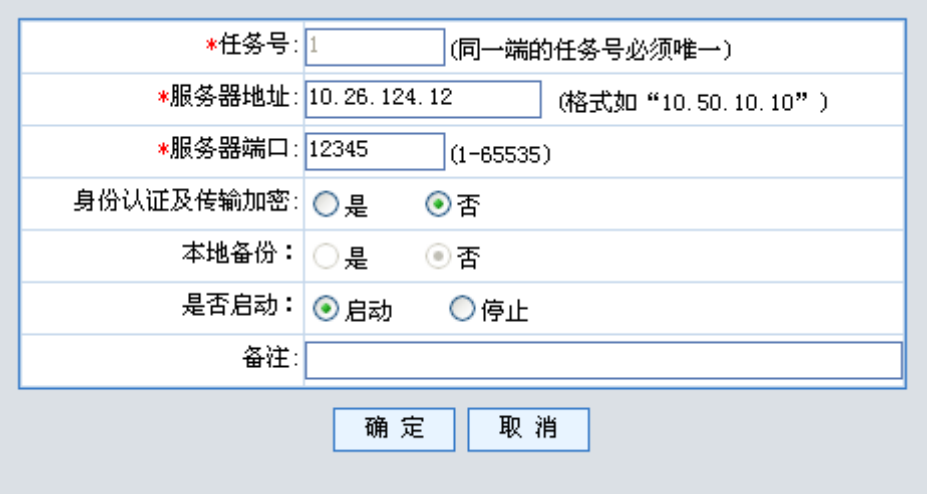


图 16 9 编辑服务端任务

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个任务后面的删除图标，弹出编辑窗口，如下图：

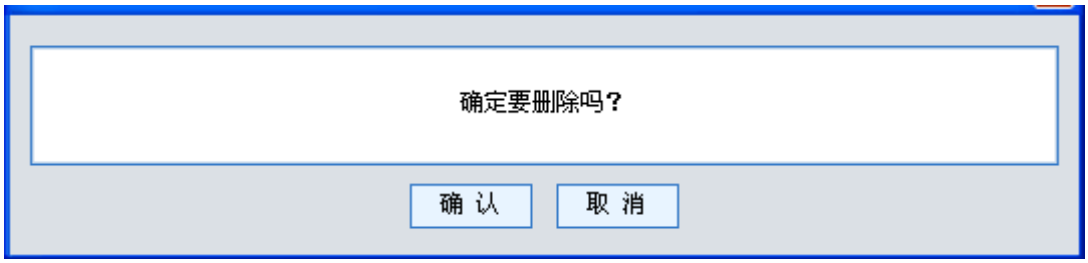


图 16 10 删除服务端任务

点击“确认”按钮，删除该任务；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

16.4 内容控制

该部分用于所有与消息传输任务中内容控制有关的配置，包括：文件名控制、内容黑名单和内容白名单等三个过滤选项。

16.4.1 文件名控制

该部分可以设置消息传输任务中是否启用文件名控制，是否允许二进制文件，以及对的文件名控制列表进行添加、修改和删除等操作。WEB 界面示意图如下：

图 16 11 文件名控制列表显示

一. 启用文件名控制

WEB 界面如下图（红色方框内为配置开关）：

图 16 12 启用文件名控制

✧ 选中复选框：启用文件名控制，此时只有符合文件名列表中的文件才能够被传输。

✧ 取消复选框：停止文件名控制，此时任意文件名的文件都可以被传输。

二. 允许二进制文件

WEB 界面如下图（红色方框内为配置开关）：

图 16 13 启用文件名控制

✧ 选中复选框：允许二进制文件（非纯文本文件）通过。

✧ 取消复选框：禁止二进制文件（非纯文本文件）通过。

三. 文件名控制列表

当启用文件名控制时，只有在文件名列表中的文件才可以被传输。

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

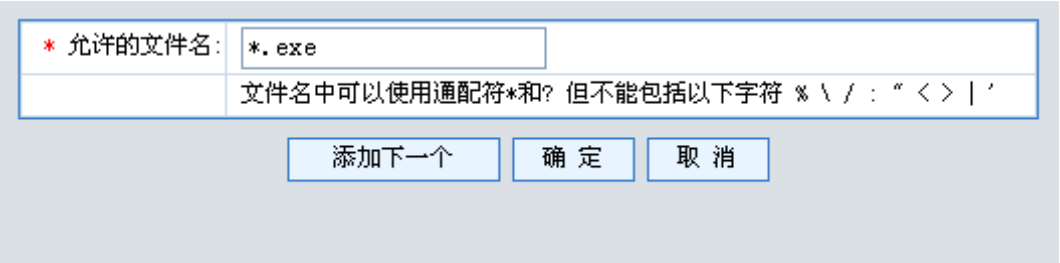


图 16 14 添加文件名

图中添加文件名的配置项，说明如下：

◆ **允许的文件名**

向文件名列表中添加一个文件名，在启用文件名控制时，符合文件名列表的文件才可以被传输。文件名中可以使用通配符*和? 但不能包括以下字符 %\/:"<>|'

设置完各配置项后，点击“添加下一条”，继续添加文件名；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个文件名后面的编辑图标，弹出编辑窗口，如下图：

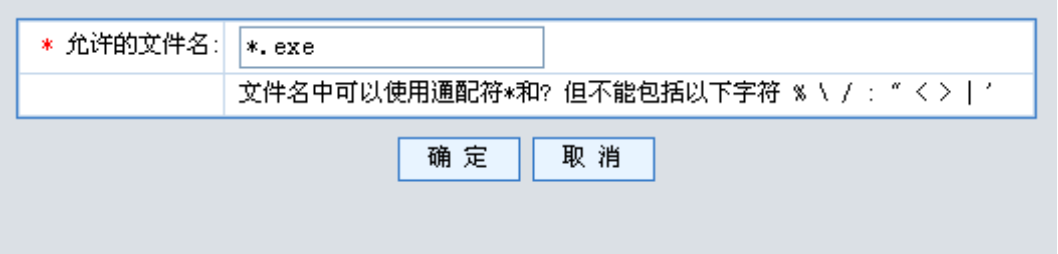


图 16 15 编辑文件名

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个文件名后面的删除图标，弹出编辑窗口，如下图：

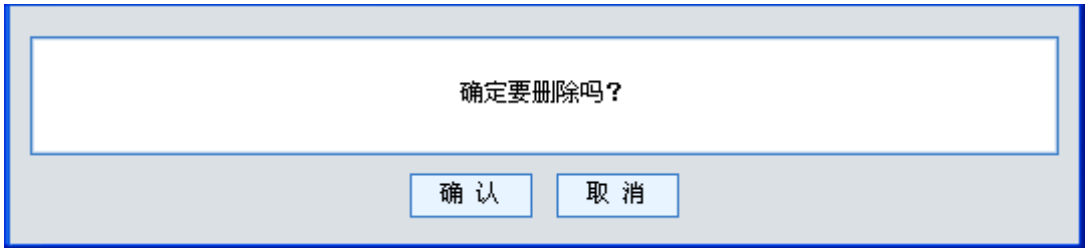


图 16 16 删除文件名

点击“确认”按钮，删除该文件名；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

16.4.2 内容黑名单

该部分可以设置消息传输任务中是否启用内容黑名单控制以及对内容黑名单控制列表进行添加、修改和删除等操作。包含此关键字的消息将不被发送。只有“启用黑名单控制”选项选中后，设置的关键字才会生效 WEB 界面示意图如下：

图 16　17　内容黑名单列表显示

一. 启用黑名单控制

WEB 界面如下图（红色方框内为配置开关）：

图 16　18　启用黑名单控制

- ✧ 选中复选框：启用黑名单控制，此时包含黑名单列表中任意一项的消息都会被禁止传输。
- ✧ 取消复选框：停止黑名单控制，此时黑名单列表不起作用，所有的消息都能被传输。

注：如果选中复选框，但未添加任何被禁止的关键字，则所有消息允许通过。

二. 内容黑名单列表

当启用内容黑名单控制时，只要包含任意一项禁止内容的消息都会被禁止传输。该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

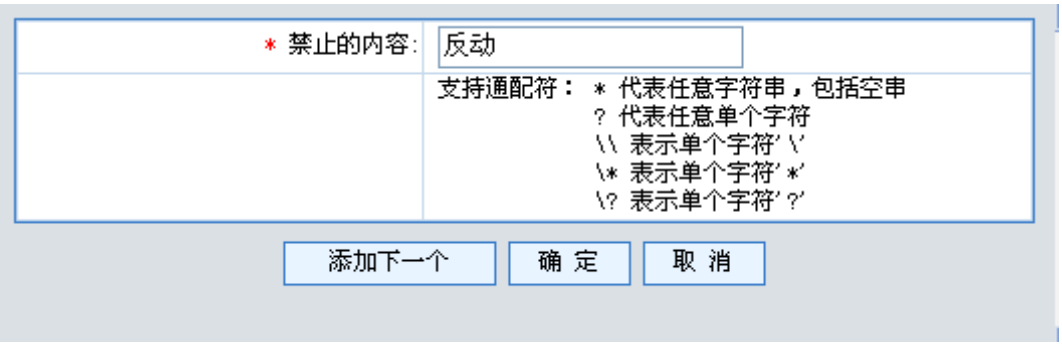


图 16 19 添加禁止的内容

图中添加黑名单的配置项，说明如下：

◆ **禁止的内容**

向列表中添加一个禁止的内容，在启用内容黑名单控制时，只要包含此项内容的消息都会被禁止传输。内容支持通配符： * 代表任意字符串，包括空串

? 代表任意单个字符

\\ 表示单个字符'\'

* 表示单个字符'*'

\? 表示单个字符'?'

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个内容后面的编辑图标，弹出编辑窗口，如下图：

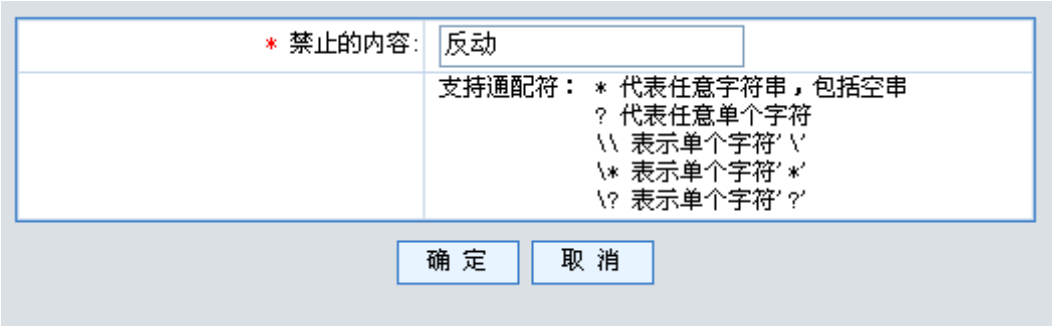


图 16 20 编辑禁止的内容

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个内容后面的删除图标，弹出编辑窗口，如下图：

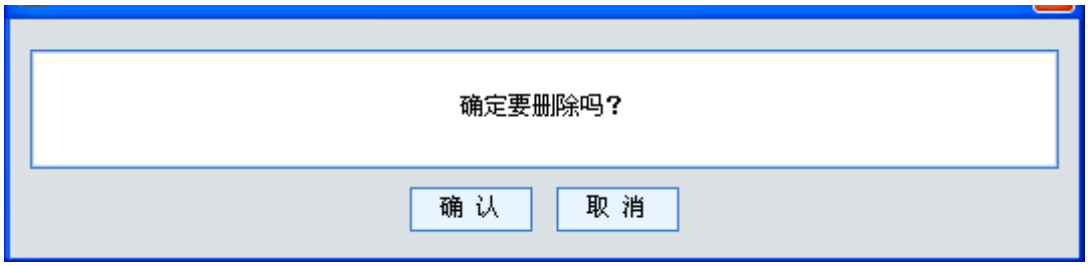


图 16 21 删除禁止的内容

点击“确认”按钮，删除该内容；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

16.4.3 内容白名单

该部分可以设置消息传输任务中是否启用内容白名单控制以及对内容白名单控制列表进行添加、修改和删除等操作。没有包含此关键字的消息将不被发送。只有“启用白名单控制”选项选中后，设置的关键字才会生效。

WEB 界面示意图如下：

图 16 22 内容白名单列表显示

一. 启用白名单控制

WEB 界面如下图（启用白名单控制为配置开关）：

图 16 23 启用白名单控制

- ✧ 选中复选框：启用白名单控制，此时只包含白名单列表中至少任意一项的消息才能被传输。
- ✧ 取消复选框：停止白名单控制，此时白名单列表不起作用，所有的消息都能被传输。

注：如果选中复选框，但未添加任何被允许的关键字，则所有消息允许通过。

二. 内容白名单列表

当启用内容白名单控制时，只有包含任意一项允许内容的消息才能够被传输。该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

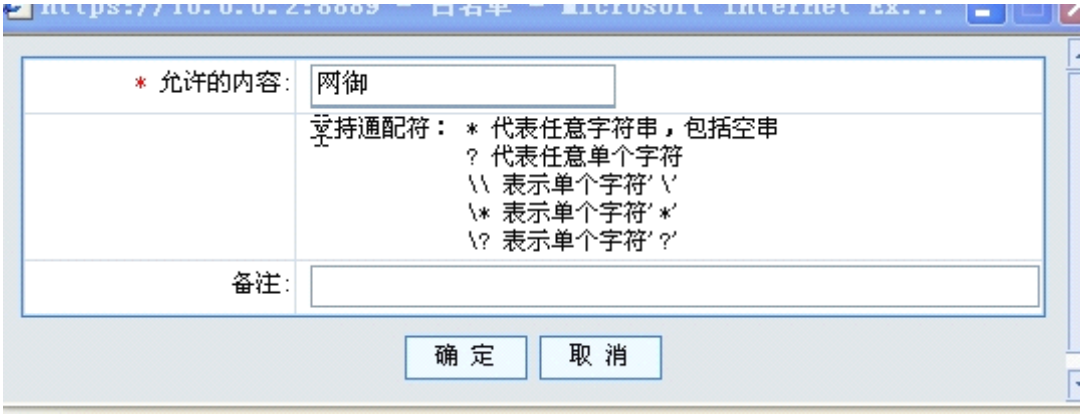


图 16 24 添加允许的内容

图中添加白名单的配置项，说明如下：

◆ **允许的内容**

向列表中添加一个允许的内容，在启用内容白名单控制时，包含此项内容的消息才会被传输。

内容支持通配符： * 代表任意字符串，包括空串
? 代表任意单个字符
\\ 表示单个字符'\'
* 表示单个字符'*'
\? 表示单个字符'?'

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个内容后面的编辑图标，弹出编辑窗口，如下图：

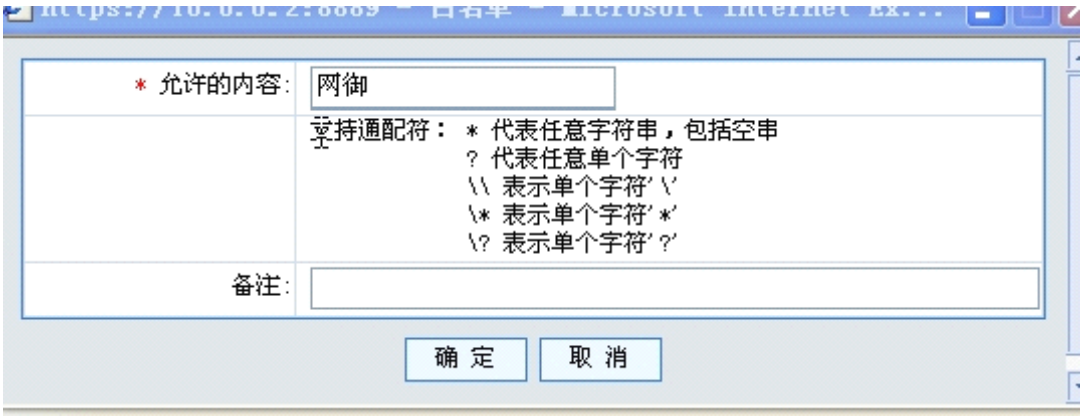


图 16 25 编辑允许的内容

编辑操作时，与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个内容后面的删除图标，弹出编辑窗口，如下图：

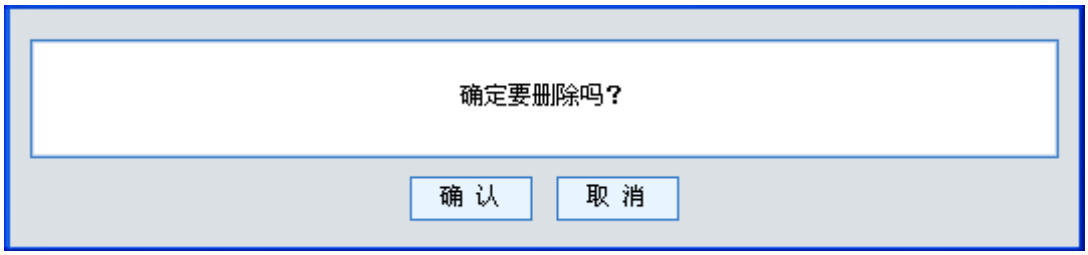


图 16 26 删除禁止的内容

点击“确认”按钮，删除该内容；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

注意：

若黑白名单控制同时启用，则以文件名控制、内容黑名单及内容白名单的顺序依次过滤。

16.5 用户管理

该部分可以配置消息传输的用户认证及用户权限。

16.5.1 用户认证

当用户在“用户管理”中选择了“用户认证”时，可以在此处配置认证用户管理。WEB 界面示意图如下：

图 16 27 用户认证管理列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

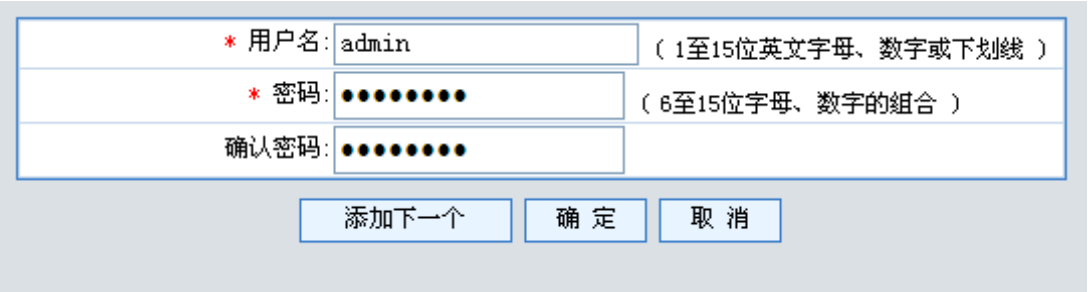


图 16 28 添加认证用户

图中添加用户的配置项，说明如下：

◆ **用户名**

需要认证的用户名，由 1 至 15 位英文字母组成。

◆ **密码**

该用户的认证需要的密码，6 至 15 位字母、数字的组合。

◆ **确认密码**

再次输入密码以保证输入正确。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个用户名后面的编辑图标，弹出编辑窗口，如下图：

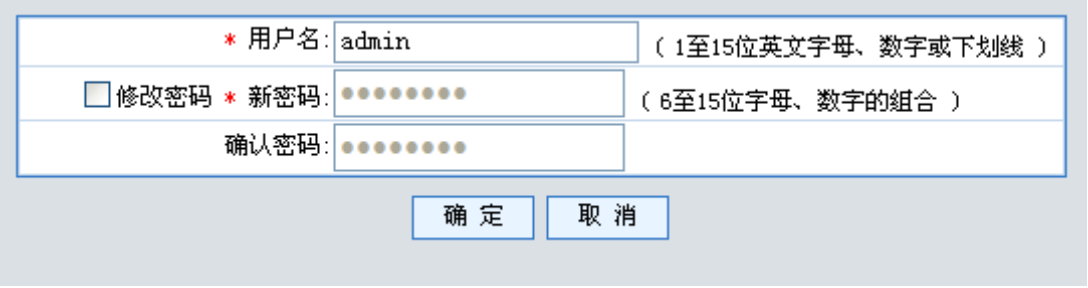


图 16 29 编辑本地用户

图中编辑用户的配置项，说明如下：

◆ **修改密码**

选中该选项可以修改密码，如果不需要修改密码，请取消复选框。

◆ **新密码**

当选中修改密码选项时，输入该用户的认证需要的新密码，6 至 15 位字母、数字的组合。

◆ **确认密码**

再次输入新密码以保证输入正确。

其它编辑操作与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个用户名后面的删除图标，弹出编辑窗口，如下图：

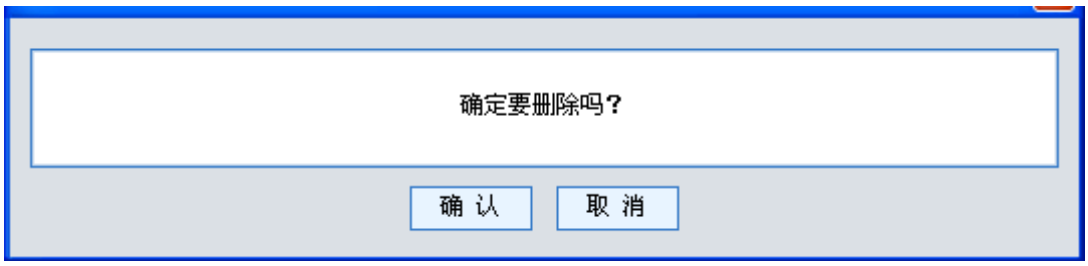


图 16 30 删除本地用户

点击“确认”按钮，删除该用户名；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

16.5.2 用户权限

当用户在“用户管理”中选择了“用户权限”时，可以在此处配置本地用户的消息传输权限。WEB 界面示意图如下：

图 16 31 用户权限管理列表显示

该模块主要包括四类操作，依次说明如下：

1) 添加操作

在上图中，点击“添加”按钮，弹出界面如下：

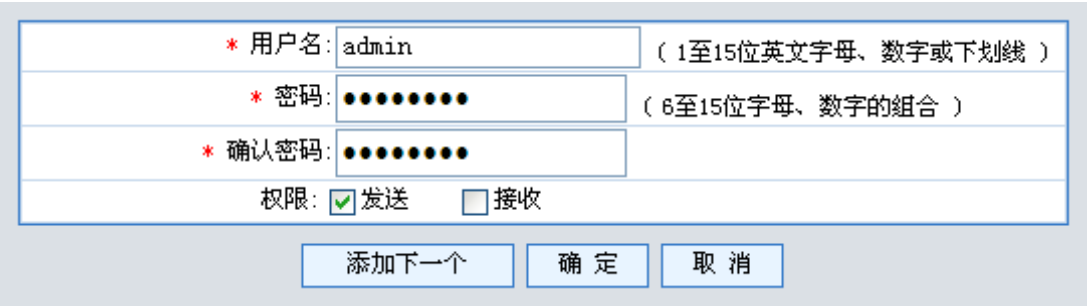


图 16 32 设置用户权限

图中添加用户权限的配置项，说明如下：

◆ **用户名**

用户名，由 1 至 15 位英文字母组成。

◆ **密码**

该用户传输消息所需要的密码，6 至 15 位字母、数字的组合。

◆ **确认密码**

再次输入密码以保证输入正确。

◆ **权限**

设置此用户的权限，包括发送权限和接收权限。

设置完各配置项后，点击“添加下一条”，继续添加；点击“确定”，返回列表显示界面，并刷新该界面；点击“取消”，返回列表显示界面。

2) 修改操作

在列表显示图中，点击列表中每个用户名后面的编辑图标，弹出编辑窗口，如下图：

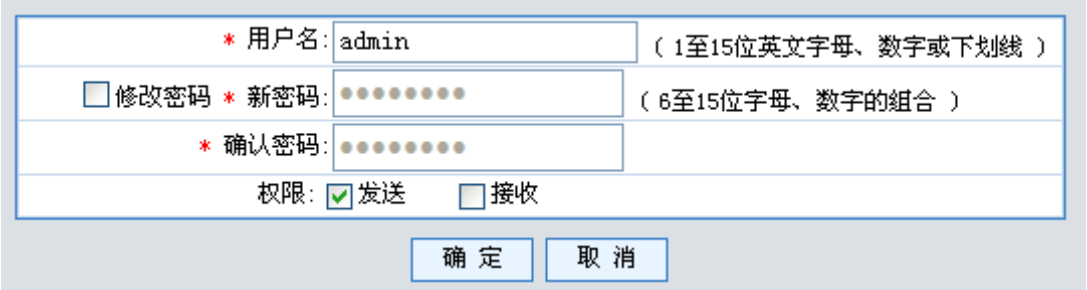


图 16 33 编辑用户权限

图中编辑用户的配置项，说明如下：

◆ **修改密码**

选中该选项可以修改密码，如果不需要修改密码，请取消复选框。

◆ **新密码**

当选中修改密码选项时，输入该用户传输消息所需要的新密码，6 至 15 位字母、数字的组合。

◆ **确认密码**

再次输入新密码以保证输入正确。

◆ **权限**

修改用户的权限，包括发送权限和接收权限。

其它编辑操作与添加操作基本相同。具体参照添加操作。

3) 删除操作

在列表显示图中，点击列表中每个用户名后面的删除图标，弹出编辑窗口，如下图：

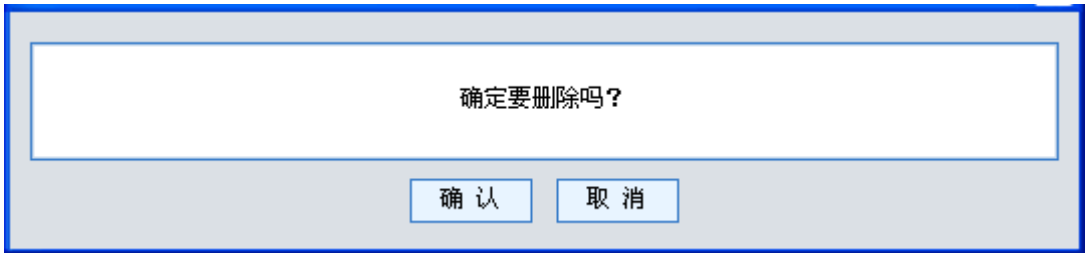


图 16 34 删除本地用户

点击“确认”按钮，删除该用户名；点击“取消”按钮，取消当前操作。然后返回列表显示界面。

4) 其他操作

其他操作包括：查找、翻页、排序等。操作方法参考“通用操作”一章中的相关描述。

第 17 章 抗攻击设置

17.1 入侵检测

入侵检测技术是 SIS 安全隔离网闸技术的逻辑补偿。作为一种数据通信监视手段，入侵检测技术对于每一个进出数据包都要进行解码分析和模式匹配，如果发现该数据包中含有与已知的攻击方法特征库相匹配的数据，则断定有入侵事件发生，发出警报提醒管理员注意，并可以自动阻断源 IP 地址，及时地将攻击者拒之门外。网御 SIS 安全隔离网闸将入侵检测技术无缝地集成到自身当中，极大地提高了 SIS 安全隔离网闸检测数据驱动型攻击的能力。由于 SIS 安全隔离网闸本身部署的特点，只能对通过 SIS 安全隔离网闸的数据包进行检测，如果用户需要对整个网络的潜在攻击进行监控，建议选用网御系列入侵检测产品。

入侵检测模块主要功能特点包括：

- **实时网络数据流监控**

实时监视进出 SIS 安全隔离网闸的所有通信流，分析网络通信会话轨迹。信息收集与分析同步进行，快速反应，一旦发现可疑信息，及时报警并响应。

- **网络攻击模式匹配**

预置的已知攻击模式规则库，能检测多种攻击行为，最大限度地防范黑客的入侵和内部用户的非法使用。规则库可以在线升级，确保能够识别最新的黑客攻击手段。

- **针对入侵行为的实时自动响应**

能够自动响应入侵事件，除了报警和写日志外，可以做到实时阻断可疑连接，同时 SIS 安全隔离网闸还可以和其它厂商的 IDS 产品如“天阗”、“天眼”IDS 实现联动，威力强大。

- **灵活的检测策略设置**

内置十六种检测策略，用户可以随意组合使用，做到量体裁衣，突出重点。

- **支持用户添加自定义检测规则**

用户可以根据自己的实际情况和感兴趣的安全事件添加自定义检测规则，体现个性化服务。

- **支持高级用户调整检测规则**

管理员可根据 IDS 保护的网络的具体情况，调整检测策略中的检测规则，将容易引起误报的规则禁用，更好地提高入侵检测的效率。

- **全天候报警方式**

可自动将报警信息传送到管理员的电子邮箱，显现在移动通讯设备上，实现离线监控。

17.1.1 基本配置

首先，登录 SIS 安全隔离网闸配置管理界面后，通过左侧菜单栏的“抗攻击设置>>入侵检测>>基本配置”，即出现入侵检测的基本配置管理界面。

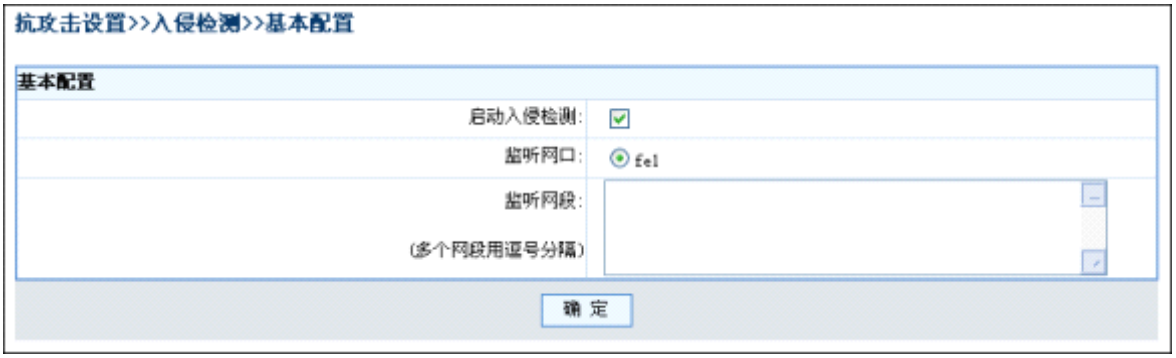


图 17 1 基本配置

基本配置可以设置是否启动入侵检测，及监听的网口和网段。

监听网段格式举例：1.1.1.0/24,5.1.1.2/32

除了自定义检测，修改其它配置项时会自动启动入侵检测。

17.1.2 策略配置

策略配置可以允许管理员选择列表中一项或者多项检测策略并使之生效，以对付入侵。

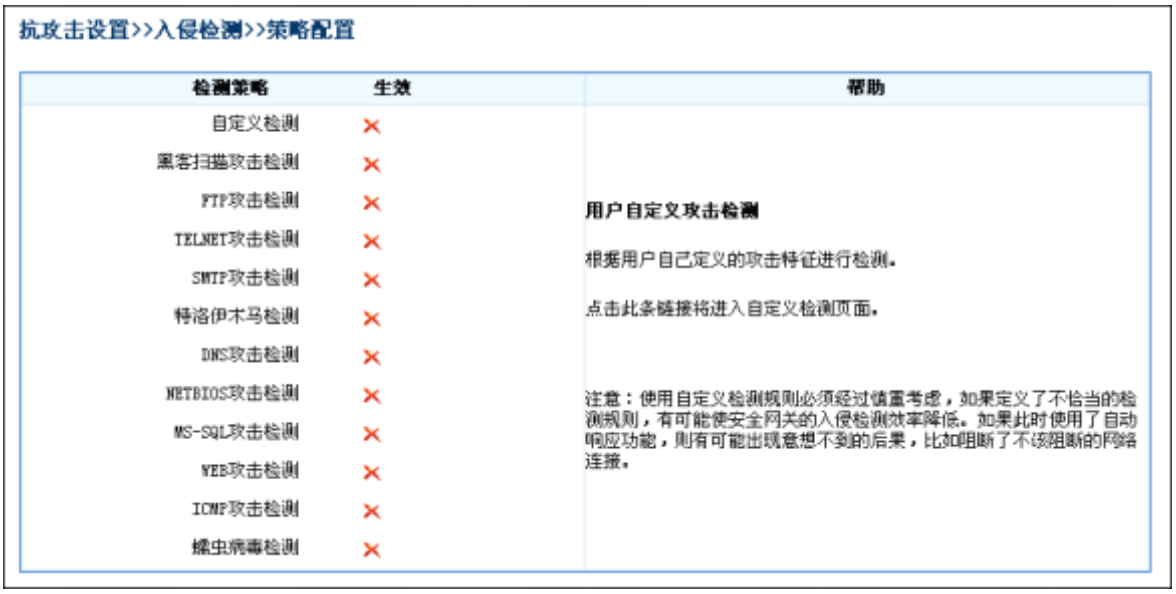


图 17 2 入侵检测策略配置

17.1.3 自定义检测

从列表中可以查看当前的所有的自定义规则，管理员可以生效或失效一条规则，来检测或取消检测某一类入侵事件。

图 17 3 自定义入检测

管理员可以添加一条自定义规则，如下所示：

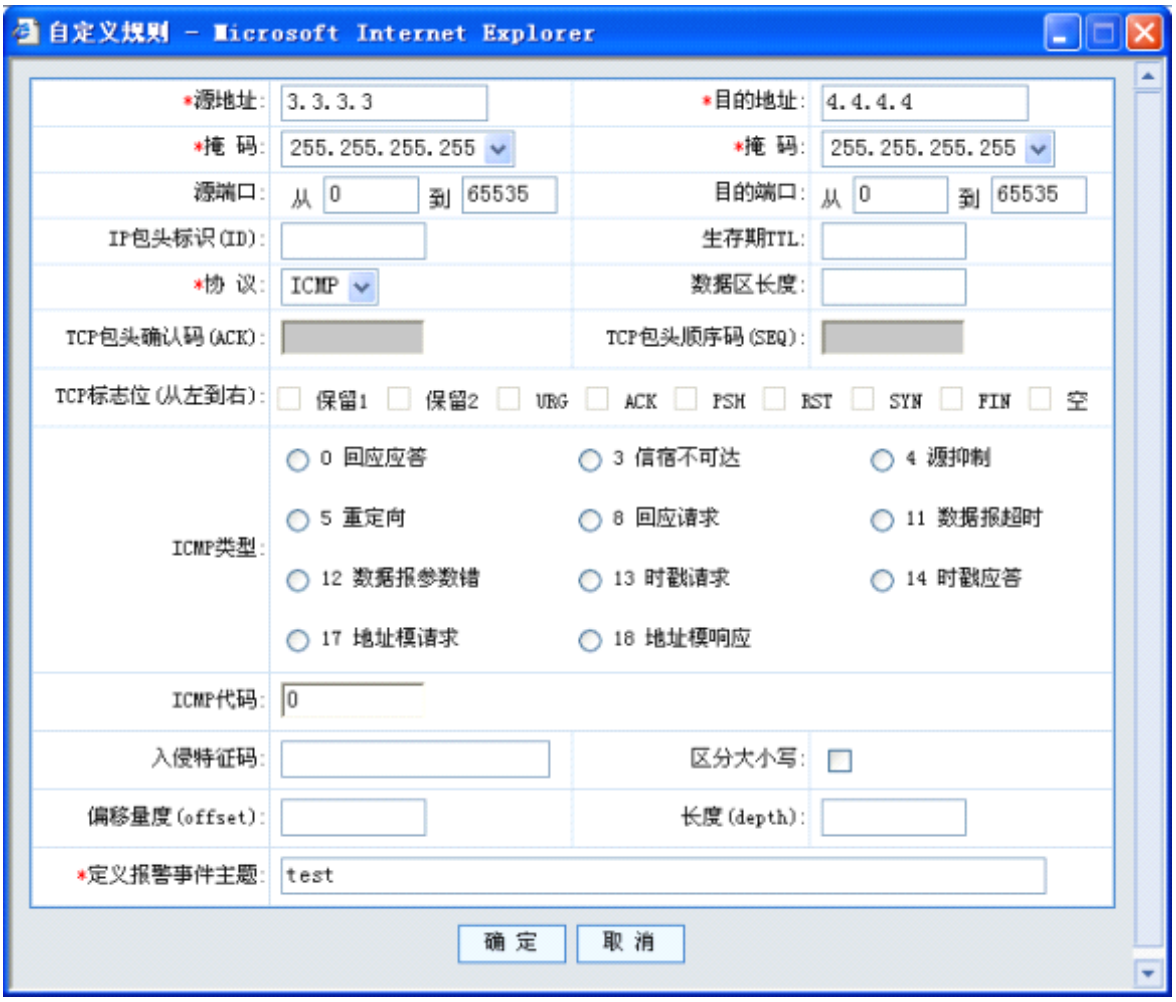


图 17 4 自定义入侵规则

注意事项：

- 如果正常的网络行为引起某条规则大量误警，可以将该条规则禁用。自动响应功能最好在正常运行一段时间后，当误报已经减少到很低程度时再启用。
- 有时 FTP 服务器或 DNS 服务器会引发扫描报警，这属于误报，可以调整扫描时间阈值或者将这些服务器的 IP 地址添加到忽略扫描报警的地址列表中。
- 有时在检测结果中会看到对外服务器的 IP 出现在攻击者的源地址中，比如从对外服务器的 80 端口到某个外部 IP 地址的高端口，报警信息为发现了 403 forbidden 的特征字符串。这条报警信息并不意味着对外服务器是攻击者，恰恰相反，正是由于某个外部 IP 通过 SIS 安全隔离网闸向对外服务器发起了非法的 Web 请求，导致服务器返回“403 禁止访问”的信息，所以攻击者是外部 IP 地址主机。但是由于 SIS 安全隔离网闸的自动响应功能只阻断检测结果中的源 IP 地址，因此为了确保服务器不被阻断，最好将服务器的 IP 地址放入忽略自动阻断的地址列表中。

17.1.4 扫描检测配置

管理员点击“扫描检测配置”，将扫描时间阈值由 3 分钟内发现 5 次端口连接调整为 10 秒钟

内发现 3 次端口连接。如下图所示。

注意：忽略扫描的源 IP 地址的数量最多为 30 个

图 17 5 扫描检测配置

17.1.5 自动响应配置

管理员可以启用自动响应功能，并设置阻断时间为 12 秒。如下图所示：

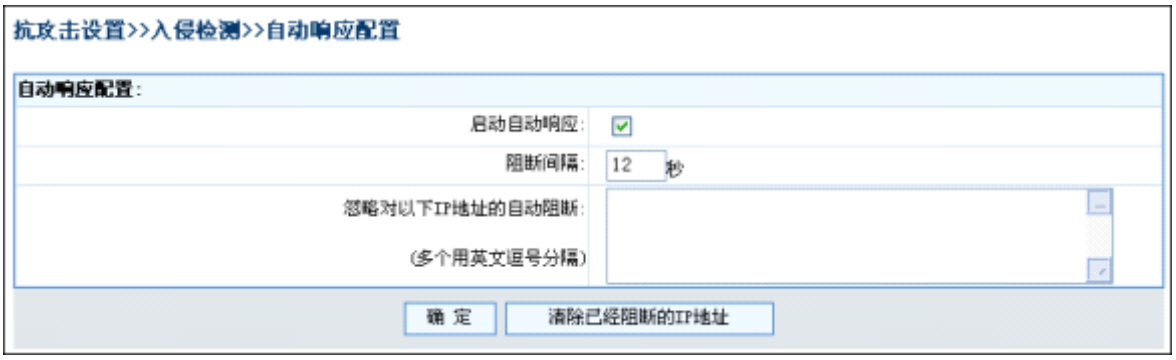


图 17 6 自动响应功能

设置完毕后，自动响应功能生效。一旦有触发检测规则的可疑事件发生，出现在检测结果中的源 IP 地址立即被自动列入系统黑名单中，发起者的通信被 SIS 安全隔离网闸阻断，可疑行为将无法继续进行下去。

管理员可以自定义阻断时间（以秒为单位），如果不填写时间，则视为永远不解除阻断。对于只有同一种入侵一直攻击的情况，如果定义阻断时间小于 60 秒，系统将会在阻断定义的时间后，不再阻断，直到 60 秒后继续阻断。

清除已经阻断的 IP 地址，可以清除 SIS 安全隔离网闸系统的所有已经阻断的 IP 地址，包括 ids 联动系统阻断的地址。

注意：攻击者可以伪造地址进行攻击，所以开启该项功能有可能导致对被伪造 IP 的 DOS 攻击或网络通信异常，因此推荐一般情况下不要打开此项功能。

17.1.6 检测结果

管理员点击界面中的“检测结果”，可以查看所有的入侵，页面如下所示。

抗攻击设置>>入侵检测>>检测结果

行号	时间	攻击者 源地址	端口	被攻击者 目的地址	端口	协议类型	事件主题	风险级别
1	Mar 17 15:28:05	10.50.10.160	--	--	--		端口扫描报告：发现来自 10.50.10.160的扫描行为！	中
2	Mar 17 15:28:10	10.50.10.160	--	--	--		端口扫描报告：10.50.10.160正在进行扫描，对62台主机进行了62次扫描，其中TCP连接62次，UDP连接0次	中
3	Mar 17 15:28:14	10.50.10.160	--	--	--		端口扫描报告：10.50.10.160正在进行扫描，对40台主机进行了40次扫描，其中TCP连接40次，UDP连接0次	中
4	Mar 17 15:28:19	10.50.10.160	--	--	--		端口扫描报告：10.50.10.160正在进行扫描，对60台主机进行了60次扫描，其中TCP连接60次，UDP连接0次	中
5	Mar 17 15:28:23	10.50.10.160	--	--	--		端口扫描报告：10.50.10.160正在进行扫描，对40台主机进行了40次扫描，其中TCP连接40次，UDP连接0次	中
6	Mar 17 15:28:28	10.50.10.160	--	--	--		端口扫描报告：10.50.10.160正在进行扫描，对60台主机进行了60次扫描，其中TCP连接60次，UDP连接0次	中
7	Mar 17 15:28:32	10.50.10.160	--	--	--		端口扫描报告：10.50.10.160正在进行扫描，对40台主机进行了40次扫描，其中TCP连接40次，UDP连接0次	中
8	Mar 17 15:28:36	10.50.10.160	--	--	--		端口扫描报告：10.50.10.160正在进行扫描，对40台主机进行了40次扫描，其中TCP连接40次，UDP连接0次	中
9	Mar 17 15:28:41	10.50.10.160	--	--	--		端口扫描报告：10.50.10.160正在进行扫描，对60台主机进行了60次扫描，其中TCP连接60次，UDP连接0次	中
10	Mar 17 15:28:45	10.50.10.160	--	--	--		端口扫描报告：10.50.10.160正在进行扫描，对40台主机进行了40次扫描，其中TCP连接40次，UDP连接0次	中

清 空

第1页/20页 跳转到 1 页 Go 每页 10 行

图 17 7 检测结果

17.2 抗 DDos 攻击

分布式拒绝服务攻击(Distributed Denial Of Service)是利用攻击者已经侵入并控制的主机（可能是数百台），对某一单机发起攻击。在悬殊的带宽力量对比下，被攻击的主机会很快失去反应。开启抗 DDos 攻击服务可以使 SIS 安全隔离网闸免受 DDos 攻击的影响。该部分 WEB 界面示意图如下：

图 17 8 抗 DDos 攻击界面

操作方法：

- **启动服务：**

  单击“启动服务”按钮即可，服务状态变为“启动”。该按钮随后被 Disable，“停止服

务”按钮被 Enable。

- **停止服务：**

单击“停止服务”按钮即可，服务状态变为“停止”。该按钮随后被 Disable，“启动服务”按钮被 Enable。

第 18 章　系统监控

系统监控能够显示 SIS 安全隔离网闸当时的工作状态，为 SIS 安全隔离网闸管理员提供了功能强大的监控工具。与网御集中管理软件共同使用，可以搭建全面的安全管理平台。

18.1 网络设备

网络设备监控的是启用的物理收发包的情况，如图：

系统监控>>网络设备

网络设备	状态	流量			
fe1		发送 0 字节	接收 0 字节	当前状态	统计图
fe2		发送 2524369 字节	接收 858411 字节	当前状态	统计图
fe3		发送 1385409 字节	接收 2740659 字节	当前状态	统计图

图 18　1　网络设备监控

图中的网络设备是当前有效的物理设备，状态图标表示设备处于启用状态，图标表示设备处于停止状态。流量栏中显示了当前设备总发送和总接收的字节数。点击“当前状态”可以查看设备更详细的信息，点击“统计图”可以查看设备收发数据的统计图示。

网闸隔离卡状态	

上图中显示的是安全网闸隔离卡的工作状态，图标表示网闸隔离卡当前正常工作，图标表示网闸隔离卡工作状态不正常。

如果要查看设备一段时间内的监控信息，必须先启用设备监控服务，如下图：

设备监控服务		停　止	刷　新	清空数据文件

图标表示监控服务正在运行，图标表示监控服务已经停止。点击“停止”按钮可以停止监控服务，点击“启动”按钮可以启动监控服务。点击“刷新”按钮可以刷新设备状态。启动监控服务后，才可以在统计图中查看到统计数据；停止监控服务后，仍然可以查看当前设备收发数据的情况，但是无法查看历史数据。如果要清除以前的统计数据，可以点击“清空数据文件”将之清除。

点击“当前状态”后，显示如下图所示的页面：

系统监控>>网络设备>>当前状态

设备： fe2 刷新

网络设备 fe2 当前接受状态					
Bytes	881921	Packets	5881	Errs	0
Drop	0	Fifo	0	Frame	0
Compressed	0	multicast	0		
网络设备 fe2 当前发送状态					
Bytes	2711822	Packets	17731	Errs	0
Drop	0	Fifo	0	colls	0
carrier	0	compressed	0		

图 18 2 网络设备当前状态

页面中显示了设备的详细信息。

点击“统计图”后，显示如下图所示的页面：

系统监控>>网络设备>>统计图

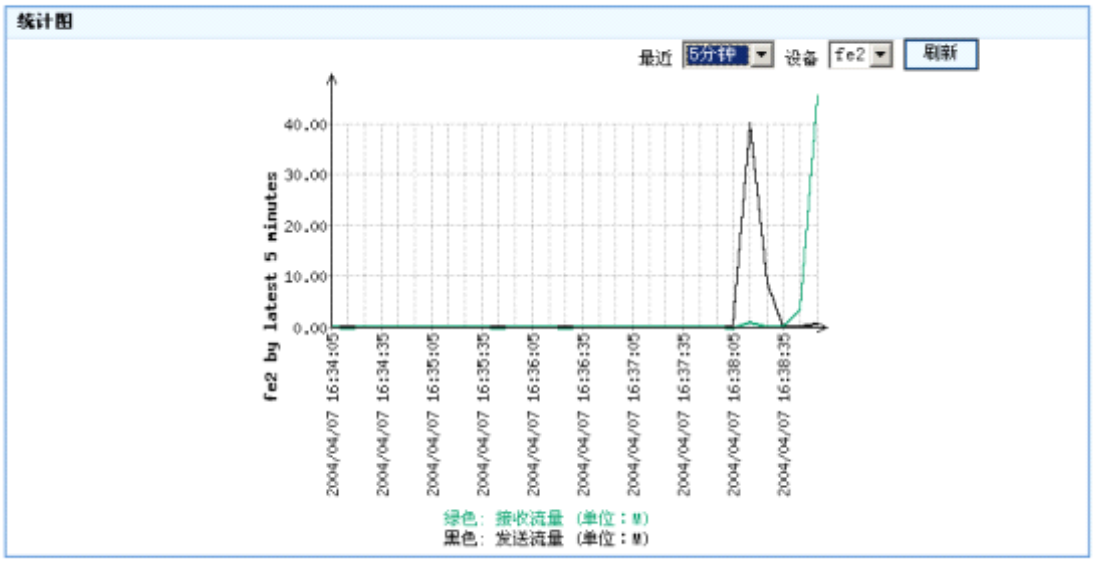


图 18 3 网络设备流量统计

上图显示了设备“5 分钟”，“30 分钟”，“3 小时”，“一天”之内的流量统计信息，每个设备都有自己的统计图。流量的单位是兆字节，如果选择最近 5 分钟的数据，则系统每 10 秒钟记录一次流量信息，如果选择查看的时间较长，则系统记录流量信息的间隔也相应增大。如果单位时间内流量一直小于 1 兆字节，则绘制的曲线会比较贴近横坐标，不很醒目。

18.2 资源状态

系统监控>>资源状态

系统资源当前利用率				
CPU 利用率	0%			统计图
内存利用率	58%		详细信息	统计图
磁盘利用率	48%		详细信息	

资源监控服务 停 止 清空数据文件

图 18 4 资源状态列表图

该列表显示当前 CPU、内存和磁盘的利用率。

点击对应的详细信息可以查看详细的使用情况，如下图所示：

系统监控>>资源状态>>详细信息

内存信息	
总内存	255572 KB
空闲内存	113292 KB
共享内存	0 KB
buffers内存	3136 KB
缓冲内存	93216 KB
总交换内存	0 KB
空闲交换内存	0 KB

图 18 5 详细信息查看图

点击对应的“统计图”链接，可以查看相应的统计信息，如下图所示：

系统监控>>资源状态>>查看

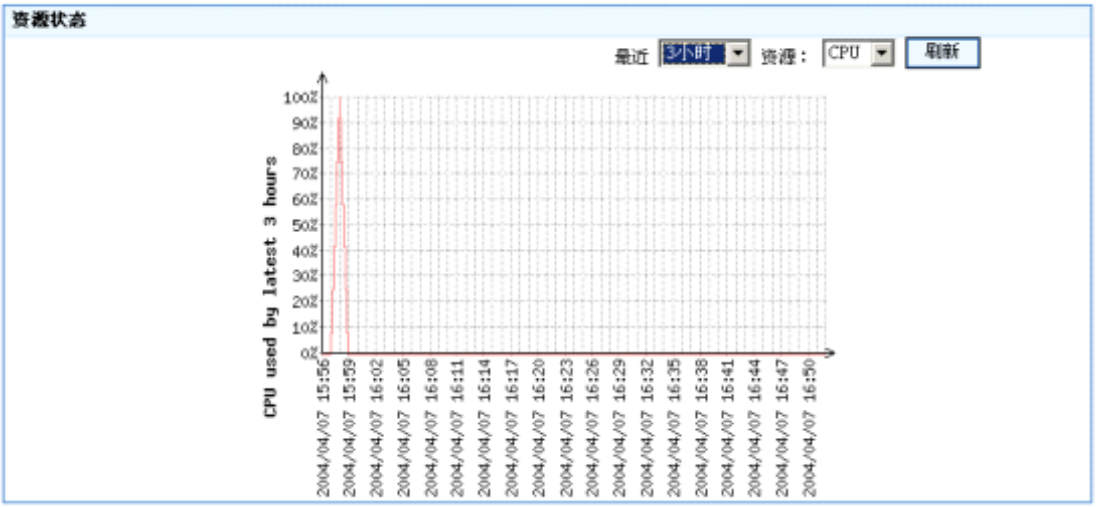


图 18 6 统计图查看

点击“启用”或“停止”按钮可以启动或关闭资源统计服务，当资源统计文件超过一定大小（400K）时，自动进行空间清理；用户也可以点击“清空数据文件”，强制删除后台统计的数据存储文件。

18.3 日志信息

SIS 安全隔离网闸上各功能模块均记录了详细的日志信息。

日志信息有两种处理方式：

（1） 发送给日志服务器处理：日志服务器上需安装相应的日志服务器程序。日志服务器程序提供丰富的查询、统计、报表功能，可以保存数量庞大的日志信息（受日志服务器上硬盘容量限制）。

（2） SIS 安全隔离网闸上保留的日志：由于受到资源的限制，最多保存 2M 日志。日志信息不能保存，断电即丢失。查询功能有限，只能按日志类型、日志级别和关键词进行查找，同时日志的可读性也远不如日志服务器。

推荐使用日志服务器来接收、保存、查询、统计日志信息。日志服务器的配置可以在“系统配置>>报告设置>>日志服务器”中通过设置“日志服务器 IP”和“端口”等项来实现。

图 18 7 日志信息查看

日志级别包括：警报（紧急，一般和临界），事件（错误，警告，注意，信息和调试）和所有。

注意：

1. 选中类型和级别后，需要点击“查找”按键才可以进行查找。
2. 如果关键词输入框中有内容，则同时按关键词进行查找，如果没有内容，则不按关键词查找。

18.4 用户信息

监控在线认证用户信息。界面如下：

图 18 8 在线用户

点击强制断开按钮，可以强制该用户下线，并拒绝该用户再次访问。

点击查看连接详细信息按钮，可以查看该用户详细的连接信息，如下图：

图 18 9 在线用户连接信息

18.5 网络调试工具

网御 SIS 安全隔离网闸提供网络调试工具。本页用来选择网络调试工具和参数。

图 18 10 调试工具

表 18 1 调试工具及参数说明

调试工具名称	说明	参数	说明

ping	检测一帧数据从当前主机传送到目的主机所需要的时间	IP 地址	目的主机
traceroute	判定数据包到达目的主机所经过的路径	IP 地址	目的主机
tcpdump	检测经过 SIS 安全隔离网闸的数据包	网络接口	检测的网络接口
arp	检查 SIS 安全隔离网闸所能得到的 IP 与 MAC 地址对	无	
routeshow	检查各种路由信息，包括连接路由、静态路由、动态路由、策略路由等等	无	

选择“开始调试”进入系统监控>>网络调试工具>>调试结果。

使用 ping 工具进行调试的结果显示如下图：

系统监控>>网络调试工具>>调试结果

工具名称:ping 参数:10.50.10.151

```
PING 10.50.10.151 (10.50.10.151) 56(84) bytes of data.
64 bytes from 10.50.10.151: icmp_seq=1 ttl=128 time=0.615 ms
64 bytes from 10.50.10.151: icmp_seq=2 ttl=128 time=0.323 ms
64 bytes from 10.50.10.151: icmp_seq=3 ttl=128 time=0.324 ms
64 bytes from 10.50.10.151: icmp_seq=4 ttl=128 time=0.323 ms
64 bytes from 10.50.10.151: icmp_seq=5 ttl=128 time=0.322 ms

--- 10.50.10.151 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.322/0.381/0.615/0.118 ms
```

图 18　11 调试结果

18.6 批处理工具

网御 SIS 安全隔离网闸提供对命令行进行批处理。该页提供的功能如下：

a) 查看 SIS 安全隔离网闸上执行命令行的历史记录。

b) 清空 SIS 安全隔离网闸上执行命令行的历史记录，点击”清空”按钮。

c) 下载 SIS 安全隔离网闸上执行命令行的历史记录，点击”导出”按钮。

d) 编辑将要执行的命令行批处理文件，在编辑框中输入想要执行的命令行语句，每一个命令行为一行，并可加入 sleep 和 beep 语句，点击”重写”按钮，可进行重新编辑，编辑完成的命令，将以黑色显示，提示用户这些命令尚未提交至 SIS 安全隔离网闸。点击”提交”按钮，提交所编辑好的命令行批处理文件。

e) 上载已有的命令行批处理文件，点击”浏览”按钮，选择将要上载的命令行批处理文件，

点击”导入”按钮，将该文件上载至 SIS 安全隔离网闸。

f) 执行已经提交或上载了的命令行批处理文件。当已经提交或上载了批处理文件，但尚未执行时，批处理编辑框中的命令将以蓝色显示，提示用户这些命令尚未执行。点击”执行批处理”按钮，将执行批处理。

g) 执行过程中，如果要中断批处理执行，请点击弹出窗口中的”取消执行”按钮。

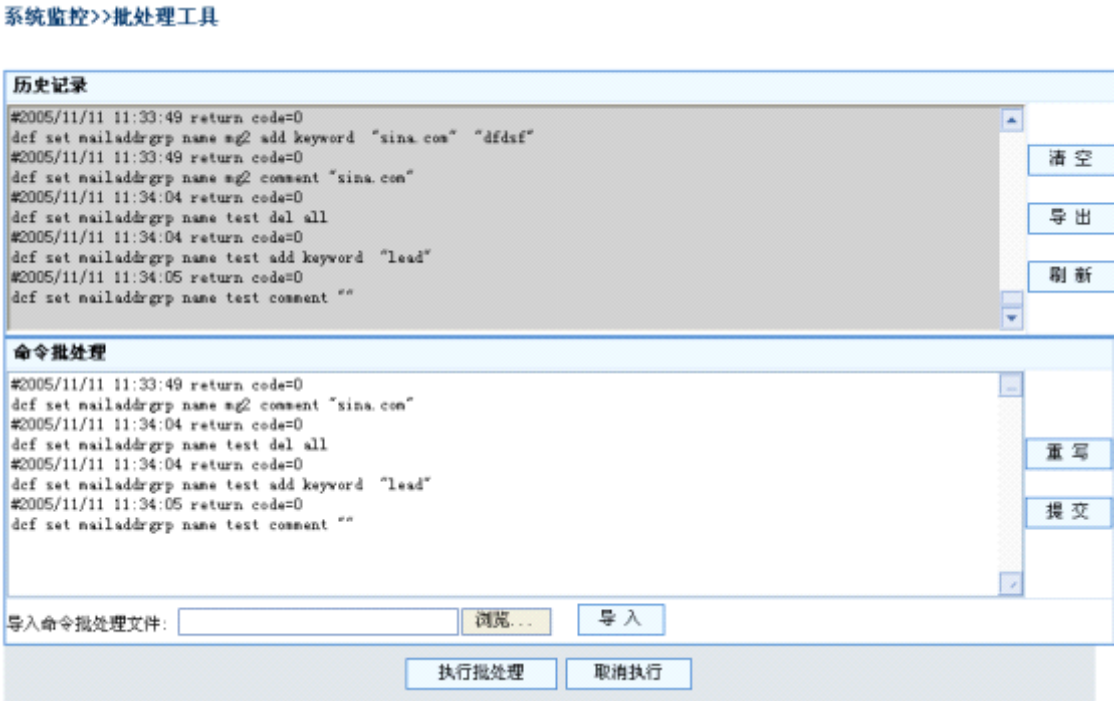


图 18 12 批处理工具

图 18 13 执行批处理

图 18 14 取消批处理

注意：

1.在批处理执行过程中，请不要关闭弹出的窗口，也不要刷新该弹出窗口。

2.每一个命令行请顶格写，前面不要有空格。

3.sleep 和 beep 命令的格式为关键字 + 空格 + 秒数， 如：sleep 2

第 19 章　在线支持

19.1 在线注册

在线注册直接连接到网御的信息安全网站 http://www.leadsec.com.cn/，用户可以在网站上注册 SIS 安全隔离网闸。

19.2 技术支持

当您在使用 SIS 安全隔离网闸时，如果遇到了什么问题，您可以选择“技术支持”，将为您提供几种解决问题的办法。

1. 参考随机的 SIS 安全隔离网闸帮助手册
2. 登录到网御的 SIS 安全隔离网闸支持网站 http://www.leadsec.com.cn/寻求帮助
3. 给网御的 SIS 安全隔离网闸支持人员打电话寻求帮助，热线电话是：400-810-7766

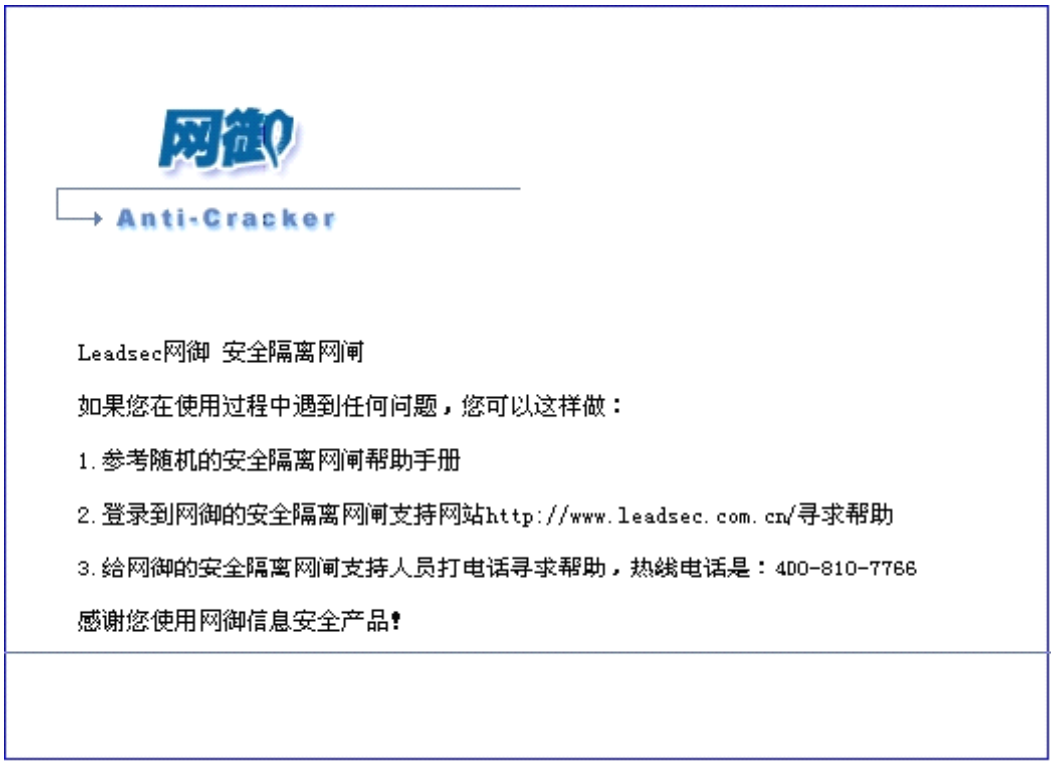


图 19　1　网御 SIS 安全隔离网闸技术支持

19.3 关于

选择“关于”，出现网御 SIS 安全隔离网闸的简单说明。

图 19 2 关于网御 SIS 安全隔离网闸

第 20 章　公共操作说明

20.1 字符合法性说明

本节针对各个模块经常使用的配置项、属性等的合法性规则，作一个统一的说明。除非各模块中有特别说明，否则所有相同或类似的配置项的合法性检查都遵守以下规则。具体参见如下表格。

表 18　1　字符合法性规则说明

名称	合法字符	最大长度	备注
任务号	0－9 等 10 个数字	8	文件交换的任务号范围为 1-100; 邮件访问、数据库访问、定制访问等模块中建议任务号在 500 以下。
IP 地址	格式：*.*.*.*，星号表示 1－3 个数字字符。各部分之间由点号隔开。每个部分的数值不大于 255	15	包括：源地址、目的地址、本机地址等
邮件地址	格式：*@*.*，星号表示 1－3 个有效字符。有效字符为：数字字符 0－9，英文大小字母 A－Z | a－z，下划线、横线等	30	
备注	有效字符为：英文字母、数字、中文及常用标点符号等。	254	
关键字	有效字符为：英文字母、数字、中文及常用标点符号等。搜索关键字中不能含有’(单引号)	30	包括：正文关键字、主题关键字，黑、白名单控制中的内容等。
文件名	文件名中可以使用通配符*和? 但不能包括以下字符 %\/ : " < > | '	30	用于文件交换中的文件名控制。
文件扩展名	格式：必须以 . 开头，不能包括以下字符：\/ : * ? " < > | ' %	30	用于邮件访问模块的附件扩展名和文件名后缀过滤等
用户名	必须以英文字母开头，少于或等于 15 位英文字母。	15	
密码	6 至 15 位字母、数字的组合	15	

20.2 通用操作说明

通用操作指在各模块都会包括的一些操作，如：分页显示、查找、排序等。下面对这些通用操作依次说明如下：

20.2.1 分页显示

各列表界面均有“分页功能”，其工具条通常位于表格的下方，如下图所示：

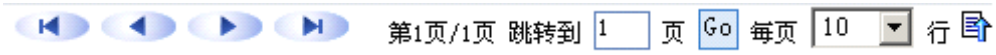


图 20 1 分页显示操作区

例如，点击“资源定义>>地址>>地址列表”，显示地址列表页面，就能看到上述工具条。实际上，所有资源的列表页面都有该项功能。

具体如下：

表 18 2 资源定义分页功能列表

功能	说明
	第一页
	前一页
	后一页
	最后一页
第1页/1页	当前页面/总页码
跳转到 1 页 Go	当有很多页时，可以直接跳转。输入希望跳转的页码，点击 Go 即可。 页码框只接受正整数。 如果输入页面大于总页码，则跳转到最后一页。
每页 10 行 10 20 50 100 全部	每页显示的行数
	如果出现竖向滚动条，则点击 可以回到该页页首。

20.2.2 查找

为便于查找已经定义过的资源，各列表界面均提供了查找功能，通常位于标题和列表之间，靠右排列。如下图所示：

图 20 2 分页显示操作区

功能	说明

查找	通常为按“名称”和“备注”进行查找。 在输入框中输入待查找的关键词，点击“查找”即可。 如果输入框中为空或者默认值，则不进行筛选，列出所有资源。 注意：搜索关键字中不能含有‘(单引号)

20.2.3 排序

为便于查看比较资源，各列表界面均提供了排序功能。

具体如下：

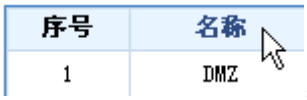
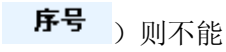
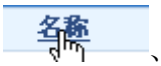
功能	说明
排序	在列表的标题部分，有两种不同的字体，如图所示  ，蓝粗体（如 ）表示可以进行排序，黑粗体（如  ）则不能进行排序。用鼠标点击（如 ）则进行排序，升序降序交替进行，如前一次为升序排序，则下一次为降序排序。 通常按照字符串顺序进行排序（如  、 ，如果为数字项，则按数字大小进行排序（如 ）。

图 20 3 排序显示操作区

第 21 章 附录

21.1 常见问题说明

1. 配置普通模式的访问任务时，对本机端口的配置是否被使用的检测规则。

在配置邮件访问、数据库访问、定制访问等任务的“本机端口”参数时，配置完毕提交时，系统会自动检测该端口是否已被使用。指出的是，检测时只检查本机已经使用的端口，对于那些已经配置但未启动的任务的端口，不在系统检查的范围。

例如，当前系统已经配置如下任务（当前系统服务处在停止状态），如下图。此时，再添加一个普通访问任务，将其本机端口号也设置为 25，提交该任务时，系统不会报错。

任务号	源地址	本机地址	本机端口	生效时段	备注	操作
12	any	10.50.10.226	25			

图 21 1 已经配置的普通访问任务

2. 添加访问任务时，任务号在本模块中必须唯一。

这些访问任务包括：邮件访问模块、数据库访问模块、定制访问模块等。

3. 数据库访问模块中 ORACLE 数据库类型无法实现负载均衡。

网御 SIS 网闸设备的数据库访问模块，目前支持的 ORACLE 数据库类型的版本为 9i 和 10i，但不支持 ORACLE8i 版本。所以用户请检查当前使用的数据库版本是否为 ORACLE8i 版本。

4. 访问任务中，若同时存在透明模式和普通模式的任务，其访问的优先级问题。

在 FTP 访问、邮件访问、数据库访问、安全浏览、定制访问等模块中，若同时存在透明模式普通模式的访问任务，则透明访问优先，普通访问次之。

特别需要注意的是，如果用户按普通模式进行的访问可以匹配透明访问的安全策略，就算有符合条件的普通访问安全策略，也会出现访问不通的现象，因为系统已经按透明方式进行处理。

5. 数据库访问模块中，若使用的数据库类型为 oracle，需要在客户端作相关配置。

此时，需要修改本地客户端系统中修改相应的数据库服务器 IP 地址，修改文件是：C:\WINDOWS\system32\drivers\etc 中的 hosts 文件。比如：

oracle 数据库客户端(IP:10.50.10.206)相连的网闸那一侧的 IP 地址是：10.50.10.205。服务器的 IP 地址是 192.168.2.101。客户端定义对象主机名为 yusb。

普通模式下在 hosts 文件中添加如下一行：

10.50.10.205 yusb

透明模式下在 hosts 文件中添加如下一行：

192.168.2.101 yusb

6. 数据库访问模块中，oracle 和 sqlserver 两种类型的数据库支持访问控制项，其他类型不支持访问控制。

7. 数据库访问模块中，sqlserver 数据库支持网络访问，但不支持管道访问。

8. 数据库访问模块中，若有数据库任务正在传输，此时重新修改数据库访问控制项，则当前所有连接的会话都被中断，当前正在传输的任务也随即中断。

解决方法：修改数据库访问模块中的访问控制项后，需要重新连接数据库服务器。

9. 修改物理设备、别名设备、冗余设备（网络配置>>网络设备）的 IP 地址/掩码后，无法直接对已经建立的任务生效。

当修改了物理设备、别名设备、冗余设备的 IP 地址和掩码后，对所有已经引用了该设备的任务则仍然沿用修改前的值，即修改操作无法使其配置立即生效。如果要使相应的任务使用修改后的配置，则应该重新修改这些任务的所引用的值。

特别指出的是，对于高可靠性设置模块中的负载均衡功能中，除了上述对原先的负载均衡任务中相应的 IP/netmask 进行修改后，还应该重新启动服务（高可靠性设置>>基本配置>>服务管理）才能生效。

10. 在网闸的高可靠性设置中，如果某个 ip 被选择用做虚拟地址时，删除此虚拟地址项后，如果需要把此 ip 地址用于其他物理设备或别名设备时，须重启网闸再进行设置。

11. 修改“资源定义”中的地址、时间等对象的设置后，其新值无法直接对已经引用了该资源对象的任务生效。

当修改“资源定义”中的地址、时间等对象的设置时，也无法对已经引用了该对象的任务直接生效。若要使新修改的值生效，则必须重新修改相应的任务的相关对象。

12. 在“网络配置>>静态路由”中配置本机默认网关时，若已经开启物理设备中的 DHCP 方式获取 IP，就可能同时获得一个相应的默认网关，此时会导致两个默认网关产生冲突，建议配置时两者不要同时配置。

13. 网闸设备的模块许可证和接口许可证成功导入后，建议用户重新启动网闸设备，否则部分功能可能无法运行。

14. 文件交换模块中，在接收客户端、发送客户端的主机中，若打开个人防火墙等 PC 保护程序，有可能导致文件交换访问被禁止；

15. 文件交换模块中，所有访问任务（包括客户端、网闸任务）中的发送用户名、接收用户名的大小不得超过 31 个字符；

16. 文件交换模块中，在网闸上配置访问任务时，若选择“本地备份”模式，则单个文件的容量不得超过本机缓存（内存、硬盘都支持）的最大物理容量，否则该文件将无法正常传输；

17. 文件交换模块中，在外部客户端、网闸（内/外主机）导入证书时，CA 证书、用户证书、用户证书私钥、私钥口令、对端证书公共名等必须都正确，否则，所有采用身份认证/通信加密模式的访问任务将无法正常运行；

18. 文件交换模块中，在外部客户端系统中导入证书时，当前的用户证书即表示自己的身份，对

于该客户端运行的所有任务（包括发送任务、接收任务）来说，都共用一套证书与网闸进行身份认证；

19. 文件交换模块中，随机附带的证书共有 4 套，可分别用于文件交换源客户端、目的客户端，网闸内、外网主机等 4 个部件，理论上这 4 套证书可以随便部署在任一部件上，但建议用户按照部署结构对应使用；

20. 文件交换模块的外部客户端系统中，在导入证书过程中，若私钥口令错误，可能会导致服务停止。此时，用户需要重新导入正确的证书、匹配的私钥口令、对端证书主题公共名等即可；

21. 文件交换模块中，网闸上的文件交换任务要求客户端与服务端的对应任务的配置（包括身份认证模式、本地备份模式等）项必须一致，否则，将导致该任务无法正确运行；

22. 安全浏览模块中，MIME 类型过滤中音频类部分禁止可能无效。

mime类型的过滤不是基于文件名字后缀(这种可以基于文件类型过滤），而是基于http头上的mimetype, 如果服务器提供的http文件中不包含该信息，则该功能失效。

23. 安全浏览模块中，配置任务时注意，先配置“基本配置”页面，再配置“访问控制”页中的任务，否则后修改的基本配置参数可能在访问任务中无法自动刷新。

24. 设置好邮件访问规则后，必须在过滤选项>>邮件地址中设置允许哪些地址通过，默认情况下是禁止所有地址的邮件通过。

25. 在邮件访问模块中，当把一封邮件同时发送（包括抄送、暗送等）多个收件人时，而这些收件人中部分禁止接收，部分则允许接收，此时，系统统一默认所有人都能接收。

26. 数据库访问模块中，对透明访问任务的“访问控制”进行配置时，请注意：访问控制参数“服务器 IP 地址”必须为“Oracle 数据通道 IP 地址”（该地址在配置数据库透明访问任务中配置），否则其访问控制的过滤会失效。

27. “消息模块”中，与文件交换、数据库同步模块类似，不区分透明访问和普通访问，访问方式只有一种，需要分别配置客户端任务和服务端任务。

28. “安全通道”模块中，无论时透明访问方式，还是普通访问方式，都不支持负载均衡。

29. “安全通道”模块中，若采用透明访问方式，则只需配置客户端的通道，无需配置服务端。

原因：对于透明方式，为了减少用户配置操作，服务端的通道配置已经内置，无需用户再配置。

30. “安全通道”模块中，透明访问的任务 ID 号最大支持 155。

31. “安全通道”模块中，若要支持客户端与服务器的 IP 地址同属一个网段的情况，则必须采用“普通方式”配置，并且把与网闸服务端连接的真实服务器 IP 地址绑定到网闸客户端的一个别名设备中。

32. 统一用户认证使用时，若需要在使用过程中切换认证模式（本地认证模式、第三方 Radius 认证模式），则在切换前必须先清空原来的用户列表、用户组等配置；

33. 统一用户认证中，当采用第三方 Radius 认证模式时，在资源定义中无需配置“用户列表”，只需配置不含任何用户的用户组即可，然后，在具体的应用模块中配置访问任务时引用该用户组即可；

34. “统一用户认证”功能，其应用是与各个访问类应用模块（数据库访问、邮件访问、FTP 访问、安全浏览、定制访问等）相结合的，而不是一个独立的应用模块。若要使用统一用户认证功能，则必须对相应的应用模块进行升级；