

SANGFOR FGAP v3.0 深信服安全

隔离与信息单向导入系统

用户手册



深信服智安全
SANGFOR SECURITY

目录

目录.....	2
声明.....	4
手册内容.....	4
本书约定.....	5
技术支持.....	6
致谢.....	6
第 1 章 SANGFOR_FGAP 安全隔离与信息单向导入系统硬件设备的安装	7
1.1. 电源.....	7
1.2. 产品接口说明.....	7
1.3. 配置与管理.....	8
1.3.1. 开始使用.....	8
1.3.2. 设备关闭.....	9
1.3.3. WEB 管理.....	9
1.3.4. 登录/注销.....	9
1.3.5 功能区域介绍.....	10
1.4. 设备接线方式.....	11
第 2 章 SANGFOR_FGAP 安全隔离与信息单向导入系统硬件设备的部署	13
2.1.网络部署.....	13
第 3 章 SANGFOR_FGAP 安全隔离与信息单向导入系统硬件设备的配置	14
3.1.用户管理.....	14
3.1.1. 说明.....	14
3.1.2. 权限分立.....	14
3.1.3. 登录限制.....	16
3.1.4. 修改密码.....	16
3.2.系统管理.....	17
3.2.1. 基本设置.....	17
3.2.2. 设备时间.....	18
3.2.3. 双机热备.....	19
3.2.4. 设备管理.....	19
3.2.5. 网络接口.....	20
3.2.6. 诊断工具.....	22
3.2.7. 备份恢复.....	26
3.2.8. 系统升级.....	29
3.2.9. 设备状态.....	31
3.3. 策略管理.....	32
3.3.1. 地址绑定.....	34
3.3.2. 存储管理.....	35
3.3.3. 内容审查.....	36
3.3.4. 关键字过滤.....	36

3.3.5. 文件类型过滤.....	38
3.3.6 防病毒.....	39
3.3.7 数据传输.....	39
3.3.8 文件交换.....	42
3.3.9 邮件转发.....	45
3.3.10 组播策略.....	47
3.3.12 数据库同步.....	48
3.3.13 文件查看.....	51
3.3.14 校验传输.....	51
3.4. 日志审计.....	53
3.4.1. 管理日志.....	53
3.4.2. 审计员日志.....	55
3.4.3. 系统日志.....	56
3.4.4. 交换日志.....	57
3.4.5. 邮件日志.....	57
3.4.6. 连接日志.....	58
3.4.7. 内容过滤.....	58
3.4.8. 数据库同步日志.....	59
第 4 章 SANGFOR_FGAP 安全隔离与信息单向导入系统产品部署案例	60
4.1.FTP 自动交换.....	60
4.2.数据库同步.....	63
4.3.数据传输.....	65

声明

Copyright © 2019 深圳市深信服科技股份有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

为深圳市深信服科技股份有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系深信服科技股份有限公司客户服务部。

深信服科技股份有限公司（以下简称为深信服科技）

手册内容

第 1 部分 SANGFOR_FGAP 安全隔离与信息单向导入系统产品的硬件安装

第 2 部分 SANGFOR_FGAP 安全隔离与信息单向导入系统产品的硬件设备的部署

第 3 部分 SANGFOR_FGAP 安全隔离与信息单向导入系统产品的硬件设备的配置

第 4 部分 SANGFOR_FGAP 安全隔离与信息单向导入系统产品的部署案例



本手册以深信服 SANGFOR_FGAP 安全隔离与信息单向导入系统产品的常见问

题解答

SANGFOR_FGAP 安全隔离与信息单向导入系统以下也简称 SANGFOR 光闸

本书约定

图形界面格式约定

文字描述	代替符号	举例
按钮	边框+阴影+底纹	“确定”按钮可简化为
菜单项	『 』	菜单项“系统设置”可简化为『系统设置』
连续选择菜单项及子菜单项	→	选择『系统设置』→『接口配置』
下拉框、单选框、复选框选项	[]	复选框选项“启用用户”可简化为[启用用户]
窗口名	【 】	如点击弹出【新增用户】窗口
提示信息	""	提示框中显示“保存配置成功，配置已修改，需要重启 DLAN 服务才能生效，是否立即重启该服务？”

各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如

下：



小心、注意：提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。



警告：该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。



说明、提示、窍门：对操作内容的描述进行必要的补充和说明。

技术支持

用户支持邮箱：support@ sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

深信服社区：bbs.sangfor.com.cn

深信服服务商及服务有效期查询：

<http://bbs.sangfor.com.cn/plugin.php?id=service:query>

公司网址：www.sangfor.com.cn

致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

第1章 SANGFOR_FGAP 安全隔离与信息单向导入系统硬件设备的安装

本部分主要介绍了 SANGFOR_FGAP 安全隔离与信息单向导入系统产品（也称 SANGFOR 光闸）的硬件安装。硬件安装正确之后，您可以进行配置和调试。

硬件设备可在如下的环境下使用：

输入电压：220V

温度：0~45℃

湿度：最大相对湿度 5%-95%，不结露

为保证系统能长期稳定地运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

1.1. 电源

SANGFOR 光闸硬件设备使用交流 220V 电源。在您接通电源之前，请保证您的电源有良好的接地措施。

1.2. 产品接口说明

SANGFOR 光闸硬件设备可能会因为不同的型号拥有不同的网络接口数，上层接口为内网接口，连接到内网；下层接口为外网接口，连接到外网。其中上层接口中标记 MAN(管理口)、HA（热备口）、ETH1、ETH2、ETH3、ETH4 等为通信口，CONSOLE 为后台控制口；下层接口中标记 MAN(管理口)、HA（热备口）、NET1、NET2、NET3、NET4 等为通信口，CONSOLE 为后台控制口。



1. 图片仅供参考，不同型号的产品外观请以实物为准。
2. CONSOLE 口仅供开发和测试调试使用。最终用户需通过网口接入设备。
3. 系统出厂默认的 IP 地址、用户名、密码如下：

发送端（外网面板）MAN 口 IP: 10.252.252.12/24

接收端（内网面板）MAN 口 IP: 10.251.251.12/24

系统管理员账号/密码: sysuser/admin

安全保密员用户名/密码: secuser/admin

日志管理员用户名/密码: loguser/admin

1.3. 配置与管理

1.3.1. 开始使用

在正确安装完成 SANGFOR_FGAP 安全隔离与单向导入系统，并确保各种线缆（电源线、网线等）正确连接之后，您可开始使用 SANGFOR_FGAP 安全隔离与单向导入系统。

打开安全隔离设备背板上的电源开关，安全隔离设备随即启动，并加载上次关闭时的安全策略。如果您首次使用 SANGFOR_FGAP 安全隔离与单向导入系统，请参照具体章节说明配置符合您需要的网络参数以及安全策略以保护您的信息系统。

1.3.2. 设备关闭

关闭安全隔离设备背板上的电源开关，安全隔离设备随即停止运行。



1.3.3. WEB 管理

SANGFOR_FGAP 安全隔离与单向导入系统的所有管理、配置、监控工作均在 WEB 管理平台完成。



SANGFOR_FGAP(SANGFOR 光闸)由于外网面板和内网面板之间是单向光纤连接，两块面板的策略独立控制，使用时需要分别连接对应面板的 MAN 口。登录外网面板 <https://10.252.252.12> 内网面板 <https://10.251.251.12> 配置对应面板的策略。

1.3.4. 登录/注销

用户在对隔离设备进行操作之前，必须使用正确的用户凭据（『用户』、『口令』、证书）登录 WEB 管理，登录界面及说明如下图所示：



『用户名』：本系统用于区分用户身份的唯一标识，由具备用户管理权限的用户（如

sysuser、secuser、loguser 等）创建并维护。

系统管理员用户名：sysuser
系统管理员密码：admin
安全保密员用户名：secuser
安全保密员密码：admin
日志管理员用户名：loguser
日志管理员密码：admin

『口令』：系统用户的访问口令（密码），用户在正确登录之后可修改自身用户的口令。

『证书』：sysuser、secuser、loguser 用户登录 WEB 管理平台时的凭据，初始登录时输入对应账号名从界面上下载，即可获取到对应账号的初始登录证书。登录成功后如修改证书请注意下载保存新的证书，后续登录需要用新的证书登录。



管理员在第一次登录系统成功后，请及时修改系统默认密码。

WEB 管理登录成功界面如下图所示：



用户在完成管理工作后，可通过点击页面右上角  退出控制中心。

1.3.5 功能区域介绍

SANGFOR 光闸设备所有的业务功能均通过界面的功能列表进行选择，然后在右侧的主功能操作区域进行相应的操作。点击 **应用配置** 将保存修改内容并使设备生效。

图中 1 为功能列表。

2 为操作区域。

3 为管理设置

外网端如下图所示



内网端如下图所示图



1、内/外网端的配置管理有所不同，在内网端管理平台不包括如下选项：

- ❖ 『用户管理』
- ❖ 『访问用户』
- ❖ 『内容审查』
- ❖ 『数据传输』
- ❖ 『文件交换』
- ❖ 『邮件转发』
- ❖ 『组播策略』
- ❖ 『数据库同步』

2、请务必在发送端（外网面板）进行正确配置；并应用生效。

1.4. 设备接线方式

在背板上连接电源线，打开电源开关，此时前面板的 Power 灯（绿色，电源指示灯）

和 Alarm 灯（红色，告警灯）会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明网关正常工作。

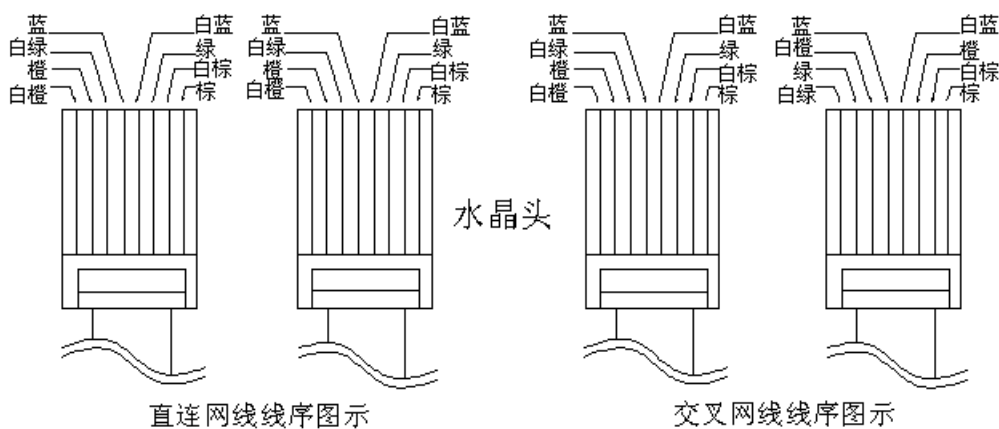
请用标准的 RJ-45 以太网线将 MAN 口与内部局域网连接，对 SANGFOR 光闸设备进行配置。



设备正常工作时 **POWER** 灯常亮，接线的数据接口 **LINK** 灯长亮，**ACT** 灯在有数据流量时会不停闪烁。**ALARM** 红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在安装时此红灯长亮，请将设备断电重启，重启之后若红灯一直长亮不能熄灭，请与我们联系。



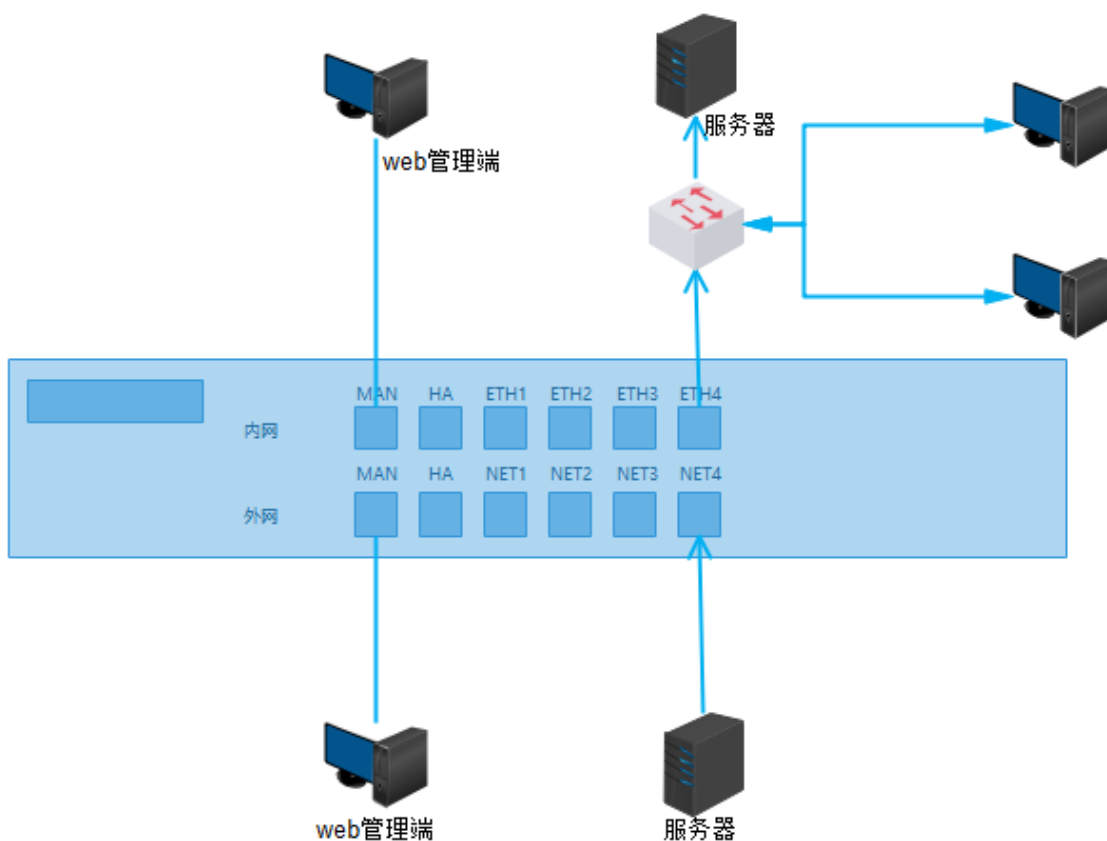
网口直接连接 **MODEM** 和交换机应使用直连线、连接路由器和电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线序不同，如下图：



第2章 SANGFOR_FGAP 安全隔离与信息单向导入系统硬件设备的部署

2.1.网络部署

SANGFOR 光闸硬件设备安装在两个不同业务网络之间或者安装在重要服务器之前，实现网络之间的数据安全隔离交互，其具体部署情况如下图所示：



第3章 SANGFOR_FGAP 安全隔离与信息单向导入系统硬件设备的配置

3.1. 用户管理

3.1.1. 说明

SANGFOR_FGAP 安全隔离与单向导入系统是多用户系统。具备用户管理权限的用户可完成系统用户的维护工作。用户管理界面如下图所示：



3.1.2. 权限分立

SANGFOR_FGAP 安全隔离与单向导入系统采用权限分立的组织方法，划分了 3 个角色的管理员： sysuser/secuser/loguser，分别对应着系统管理员、安全保密员、安全审计员三个角色。

系统管理员主要负责系统运行维护。

安全保密员主要负责用户『账号管理』、『策略管理』以及『审计员日志』的审查分析。

安全审计员主要负责对系统管理员和安全保密管理员的操作行为进行审计。

不同角色只能添加或修改自身角色权限信息，而不能修改其他类别的角色信息。

使用 sysuser 系统管理员登录，可创建本权限下的子管理员，可分配的权限为：『基本设置』、『网络接口』、『诊断工具』、『备份恢复』、『系统升级』、『设备状态』。如下图所示：

使用 secuser 安全保密员登录，可创建本权限下的子管理员，可分配的权限为：『访问用户』、『主机安全』、『地址绑定』、『存储管理』、『内容审查』、『数据传输』、『文件交换』、『邮件转发』、『组播策略』、『数据库同步』、『文件查看』、『校验传输』、『审计员日志』。如下图所示：

使用 loguser 安全审计员登录，可创建本权限下的子管理员，可分配的权限为：『管理日志』、『系统日志』、『交换日志』、『邮件日志』、『连接日志』、『内容过滤』、『数据库同步日志』。如下图所示：



深信服安全隔离与信息单向导入系统

用户管理 管理员账户

系统管理 策略管理 日志审计

添加账户

用户名:

密码: (*请用8位及以上字母与数字组合字符)

确认密码:

类别: 安全审计员

权限:

☐ 管理日志 ☐ 系统日志 ☐ 交换日志

☐ 邮件日志 ☐ 连接日志 ☐ 内容日志

☐ 数据库同步日志

描述:

确定 取消

3.1.3. 登录限制

『自动超时退出』: 无任何操作，WEB 管理平台在设置时间到时时自动退出。

『最大尝试次数』: 用户登录失败允许重试次数，超过此限制后账户将被锁定，禁止再次登录。

『锁定等待解锁时间』: 账户锁定后在锁定时间内，被限制用户禁止再次登录。

『密码更换周期』: 密码存在有效期，规定的时间修改。

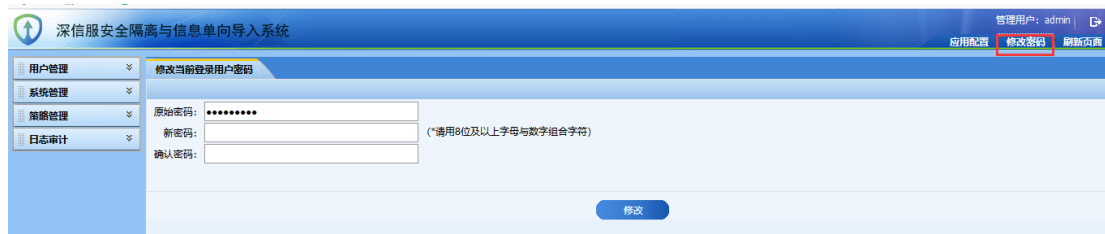
『密码长度最少』: 密码长度限制。



修改完登录限制条件后，点击**保存设置**将保存修改内容并使设备生效

3.1.4. 修改密码

点击 WEB 管理界面右上角的**修改密码**



深信服安全隔离与信息单向导入系统

管理用户: admin | 应用配置 **修改密码** 刷新页面

修改当前登录用户密码

原始密码:

新密码: (*请用8位及以上字母与数字组合字符)

确认密码:

修改



退出登录后生效。

3.2.系统管理

3.2.1. 基本设置

包含『基本设置』、『设备时间』、『双机热备』、『设备管理』四个标签页。

以具备管理系统设置权限的用户（如 sysuser）登录在『基本设置』的操作区设置设备信息。

主要有修改『设备别名』、日志设置、『发送冗余』倍数、『存储空间设置』、[不保留历史交换文件]、『临时文件后缀』、安全模块和『管理者 IP 设置』。

[开启策略日志记录]，当勾选此项时表示开启策略日志记录。记录日志可能对系统性能有一定的影响，请根据实际需要选择是否开启。

[开启 SYSLog 日志]，当勾选此项系统会按一定周期把日志信息以 SYSLog 的形式，发送到远端服务器，以便管理人员查看设备系统日志。请确保设置的『接收日志服务器 IP』、『端口』的正确性。如下图所示：

The screenshot shows the 'Basic Settings' (基本设置) tab in the Sangfor Security Management System. The interface includes a left sidebar with navigation options like 'User Management', 'System Management', 'Policy Management', and 'Log Audit'. The main content area contains various configuration fields:

- 设备别名 (Device Alias): FGAP001
- 日志设置 (Log Settings):
 - ☐ 开启策略日志记录 (Enable Policy Log Recording)
 - ☒ 开启SYSLog日志 (Enable SYSLog Log) - This option is highlighted with a red box.
- 接收日志服务器IP (Receive Log Server IP): 192.168.1.59
- 端口 (Port): 514
- 发送冗余 (Send Redundancy): 2 (倍数范围 1-10) and 50 (参数范围 1-99)
- 存储空间设置 (Storage Space Settings):
 - 空间低于 4000 MB (范围 1000-9999 MB) 时报警 (Alarm when space is below 4000 MB)
 - ☒ 不保留历史交换文件 (Do not retain historical exchange files)
- 临时文件后缀 (Temporary File Suffix): .sutmp (如 .tmpfile)
- 安全模块 (Security Module):
 - ☐ 开启抗 Dos/DDos 攻击 (Enable Anti-Dos/DDos Attack)
 - ☐ 开启抗 SYN/ICMP 洪流 (Enable Anti-SYN/ICMP Flood)
- 管理者IP设置 (Administrator IP Setting): 0.0.0.0/0 (非必要请勿修改该设置! 范围IP格式: IP/24)

An '应用配置' (Apply Configuration) button is located at the bottom right of the configuration area.

『发送冗余』，表示发送端给接收端发包的次数和发包间隔时间（单位为微秒）。

『存储空间设置』告警，表示存储空间低于设定的大小时，发出蜂鸣器告警，并记录系统日志。

[不保留历史交换文件]，发送端发送文件成功后会删除本地缓存文件。

『临时文件后缀』：文件传输未完成时，生成的临时文件的后缀。

『安全模块』，分为[开启抗 Dos/DDos 攻击]和[开启抗 SYN/ICMP 洪流]两种安全模式。

『管理者 IP 设置』，通过该项可以设置允许登录并管理设备的管理者的 IP。该 IP 可以是单个 IP，也可以是掩码形式的 IP 段。管理者 IP 无限制，请选用默认的 0.0.0.0/0。如下图所示：

深信服安全隔离与信息单向导入系统

用户管理 系统管理 基本设置 网络接口 诊断工具 备份恢复 系统升级 设备状态 策略管理 日志审计

基本设置 设备时间 双机热备 设备管理

设备别名: FGAP001

日志设置: ☐ 开启策略日志记录 ☐ 开启SYSLog日志

发送冗余: 2 (倍数范围 1-10) 50 (参数范围 1-99)

存储空间设置: 空间低于 4000 MB (范围 1000-9999 MB) 时报警 ☒ 不保留历史交换文件

临时文件后缀: .sutmp (如 .tmpfile)

安全模块: ☐ 开启抗 Dos/DDos攻击 ☐ 开启抗 SYN/ICMP洪流

管理者IP设置: 0.0.0.0/0 (非必要请勿修改该设置! 范围IP格式: IP/24)

应用配置



管理者 IP 决定哪些 IP 设备可以管理安全隔离设备，修改时一定要确定好再填写。

3.2.2. 设备时间

SANGFOR_FGAP 安全隔离与单向导入系统设备支持手动获取时间/设置时间和时间服务器校时。

手动设置时间：选择要更改的时间，点击设置时间。

时间服务器校时：在『时间服务器』输入时间服务器地址，点击立刻校时。

如：输入 windows 的服务器 “time.windows.com”。

深信服安全隔离与信息单向导入系统

用户管理 系统管理 基本设置 网络接口 诊断工具 备份恢复 系统升级 设备状态 策略管理 日志审计

基本设置 设备时间 双机热备 设备管理

设备时间: 2018-10-17 16:03:15 获取时间 设置时间

时间服务器校时

时间服务器: 立刻校时

3.2.3. 双机热备

[主设备]: 采用主从模式，是主要的工作设备。

[从设备]: 当主设备异常时，切换为工作状态；主设备恢复正常后，将停止工作。

『心跳频率』: 主从设备间隔时间发送一次心跳包。



[主设备]与[从设备]心跳频率必须相同，设备心跳线正确连接外网端 HA 口。

3.2.4. 设备管理

下图中: 1 为重启设备操作，实现设备软重启。

2 为设备初始化，设备会恢复到出厂设置。

3 为关闭设备，实现设备关机。

4 为界面设备维护管理口。

5 为清空数据表。



1、设备初始化时可以设置是否清理数据库。

2、设备维护为维护人员使用通道。

3.2.5. 网络接口

包括『网络设置』、『管理口』两个标签页。

网络设置

管理口

接口列表

接口	描述	IP地址	状态	接收/发送 数据	操作
ETH3	通信口		断开	--/--	IP地址管理
ETH2	通信口		断开	--/--	IP地址管理
ETH1	通信口		断开	--/--	IP地址管理
ETH0	通信口		连线	408 KB/167 KB	IP地址管理

3.2.5.1 网络设置

在接口列表部分，可以对设备的网络接口 IP 进行管理。同一个网络接口可以包含不同网段或者相同网段的多个 IP，但设备同一侧不同的网络接口，请不要设置相同网段的 IP。也可以对添加的 IP 进行删除，点击删除。如添加 IP 需进入 IP 地址管理，在输入框输入要添加的『IP 地址』和『掩码』，点击添加完成添加。

添加 IP 方法如下图所示：

网络设置		管理口			
接口列表					
接口	描述	IP地址	状态	接收/发送 数据	操作
ETH3	通信口		断开	--/--	IP地址管理
ETH2	通信口		断开	--/--	IP地址管理
ETH1	通信口		断开	--/--	IP地址管理
ETH0	通信口		连线	408 KB/167 KB	IP地址管理

网络设置		管理口					
接口ETH0地址列表:							
IP地址:	192.168.1.33	掩码:	255.255.255.0	添加			
IP地址	子网掩码						
返回							

『默认网关』，设置默认网关。

『DNS』，设置可开启 DNS。

[启用 SNMP 报警]，可以更改『端口』和『SNMP 共同体名称』。

路由列表，可以添加网络路由、也可以添加主机路由。例如：目标段为 10.10.0.0 子网掩码为 255.255.0.0 的路由，下一跳为 192.168.1.1 可以设置为：route add - net 10.10.0.0

netmask 255.255.0.0 gw 192.168.1.1 到目标地址为 172.10.1.158 的路由，下一跳为 192.168.2.1 可以设置为：route add - host 172.10.1.158 gw 192.168.2.1 到所有未知目标地址的路由，下一跳为 192.168.20.1 可以在默认网关中填写地址 192.168.20.1。如下图错误!未找到引用源。所示：

默认网关: DNS: ☒ 启用SNMP报警 端口: SNMP共同体名称:

路由列表:

(*书写格式如: route add -net 172.10.28.0 netmask 255.255.255.0 gw 192.168.1.1)

应用配置

3.2.5.2 管理口

SANGFOR_FGAP 安全隔离与单向导入系统设备中，具有相应权限的用户，可通过『管理口』界面修改『管理口 IP』地址、『子网掩码』、『管理端口』等信息。[开启多口管理]为，把所有存在 ip 地址的通信口，当作管理口使用。请根据需要谨慎修改。

网络设置 管理口

管理口配置

☐ 开启多口管理 管理口IP: 子网掩码: 管理端口: (请使用1000以上的端口)

(*请按需谨慎修改, 修改完成后使用新修改的IP, 端口登录管理设备!)

应用配置



『管理口 IP』：为 MAN 口 IP 地址，需要连接此 IP 地址管理设备。

- ❖ 外网默认管理口 IP 为 10.252.252.12/24
- ❖ 内网默认管理口 IP 为 10.251.251.12/24
- ❖ 子网掩码：根据实际网络环境配置

『开启多口管理』

光闸默认 MAN 口登陆，开启多口管理后所有的通信口都可以作为管理口。内外网主机分别都需要勾选。

3.2.6. 诊断工具

系统提供的多个诊断工具，了解网络的连通状况，进行系统异常排查。

Ping 工具

『目标主机』是 IP 地址或域名。如下图所示：



Traceroute 工具

『目标主机』是 IP 地址或域名。如下图所示：



Tcp 服务

可以查看要连接服务器是否正常运行。如下图所示：

The screenshot shows the 'Tcp服务' (TCP Service) tab selected in the SANGFOR service detection tool. The interface includes a header with navigation tabs: Ping, Traceroute, Tcp服务, FTP服务, SMB服务, and DB服务. Below the header, the title 'Tcp服务检测工具' is displayed. The main area contains two input fields: '目标主机:' (Target Host) and '服务端口:' (Service Port), followed by a blue button labeled '服务测试' (Service Test). Below these fields is a label '结果:' (Result) and a large empty space for displaying the test results.

FTP 服务

可以查看要连接的 FTP 服务器是否网络环境正常，可以读写。有两种方式，一种为手动写入，一种为导入本地配置的策略。如下图所示：

The screenshot shows the 'FTP服务' (FTP Service) tab selected in the SANGFOR service detection tool. The interface includes a header with navigation tabs: Ping, Traceroute, Tcp服务, FTP服务, SMB服务, and DB服务. Below the header, the title 'FTP服务检测工具' is displayed. The main area contains several input fields: '选择策略:' (Select Strategy) with a dropdown menu showing '[空]' (Empty), '服务器IP地址:' (Server IP Address), '端口:' (Port) with the value '21', '用户名:' (Username), '密码:' (Password), and '目录:' (Directory). At the bottom, there are two blue buttons: '写测试' (Write Test) and '读测试' (Read Test).

如网络环境错误或用户认证错误或没有读写权限，如下图错误!未找到引用源。所示：

Ping Traceroute Tcp服务 **FTP服务** SMB服务 DB服务

FTP服务检测工具

选择策略: [空]

服务器IP地址: 192.168.88.99

端口: 21

用户名: 123

密码: ●●●

目录:

写测试 读测试

结果: 失败!



FTP 服务检测工具，要读的目录下存在 `anmit.tst` 文件，写测试会在 FTP 上传/下载目录下写入 `anmit.tst` 文件。

SMB 服务

可以查看要连接的 SMB 服务器是否网络环境正常，可以读写。有两种方式，一种为手动写入，一种为导入本地配置的策略。如下图所示：

Ping Traceroute Tcp服务 FTP服务 **SMB服务** DB服务

SMB服务检测工具

选择策略: [空]

服务器IP地址:

用户名:

密码:

共享名:

子目录:

写测试 读测试

如网络环境错误或用户认证错误或没有读写权限，如下图所示：



SMB 服务检测工具，要读的目录下存在 `anmit.tst` 文件，写测试会在 SMB 上传/下载目录下写入 `anmit.tst` 文件。

DB 服务

可以查看要连接的数据库是否网络环境正常，可以读到表。有两种方式，一种为手动写入，一种为导入本地配置的策略。如下图所示：



如网络环境错误或用户认证错误或库表错误或没有读表权限，如下图所示：

Ping
Traceroute
Tcp服务
FTP服务
SMB服务
DB服务

DB服务检测工具

选择策略: [空]
DB类型: Oracle
数据库IP: 192.168.4.22
端口: 80
DB名称: TEST
用户ID: ROOT
密码:
字符集:
表名: Table-3

读表测试

结果: 失败!

3.2.7. 备份恢复

『备份恢复』区分为**导入恢复**、**导出备份**。

导出备份分为，手动备份、自动备份。

导入恢复：从文件恢复系统配置，选择**浏览**，然后选择以前备份的配置，点击**导入恢复**即完成恢复系统设置。如下图所示：

备份恢复

策略恢复

选择备份文件: 浏览... 未选择文件。
导入恢复

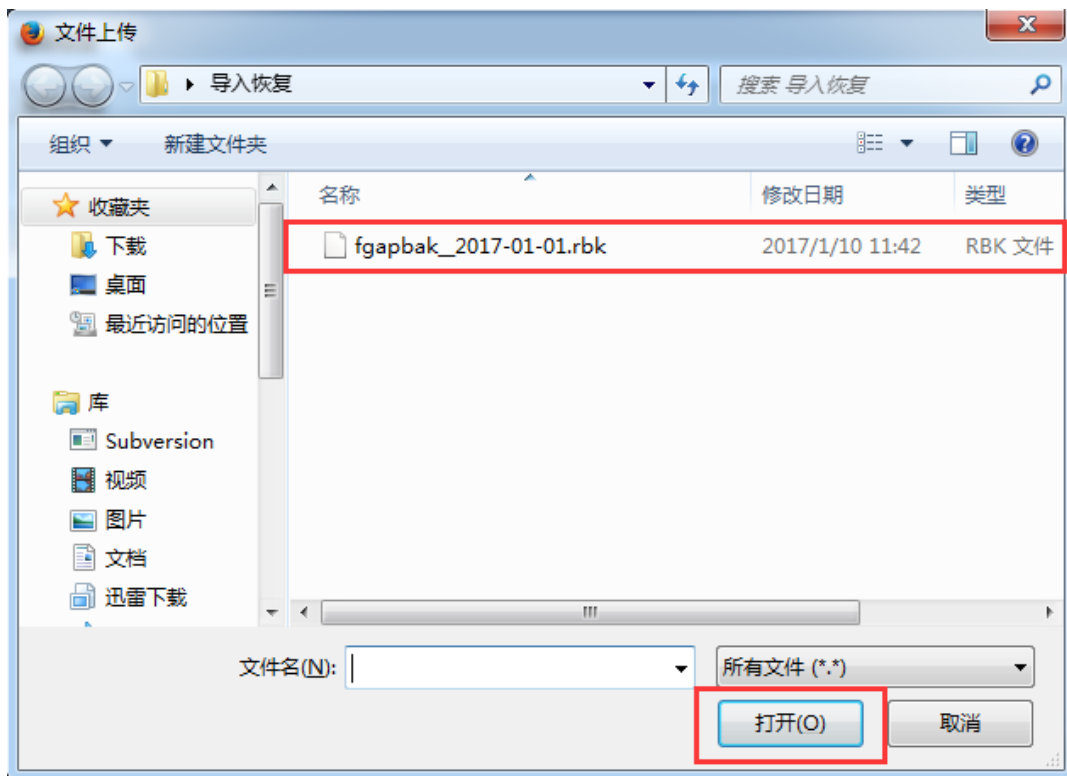
未选择文件。

策略备份

导出当前策略: 导出备份

自动备份开关: ☐ 开启策略自动备份

应用配置



手动导出备份：点击**导出备份**，选择导出的路径，点击**确定**，完成导出备份。如下图所示：

备份恢复

策略恢复

选择备份文件：

浏览...

未选择文件。

导入恢复

策略备份

导出当前策略：

导出备份

自动备份开关：

☒ 开启策略自动备份

间隔时间：

5

分钟（范围 5-600分钟）

FTP服务器IP：

备份服务端口：

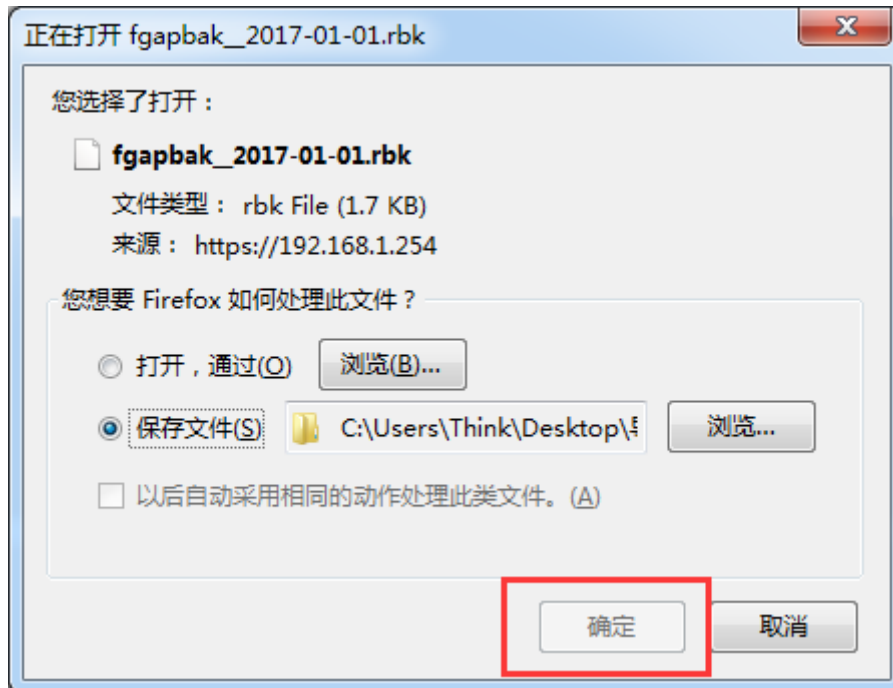
0

用户名：

密码：

上传路径：

应用配置



自动导出备份：勾选[开启策略自动备份]，输入正确的参数，在设定的时间会发送备份到指定路径。



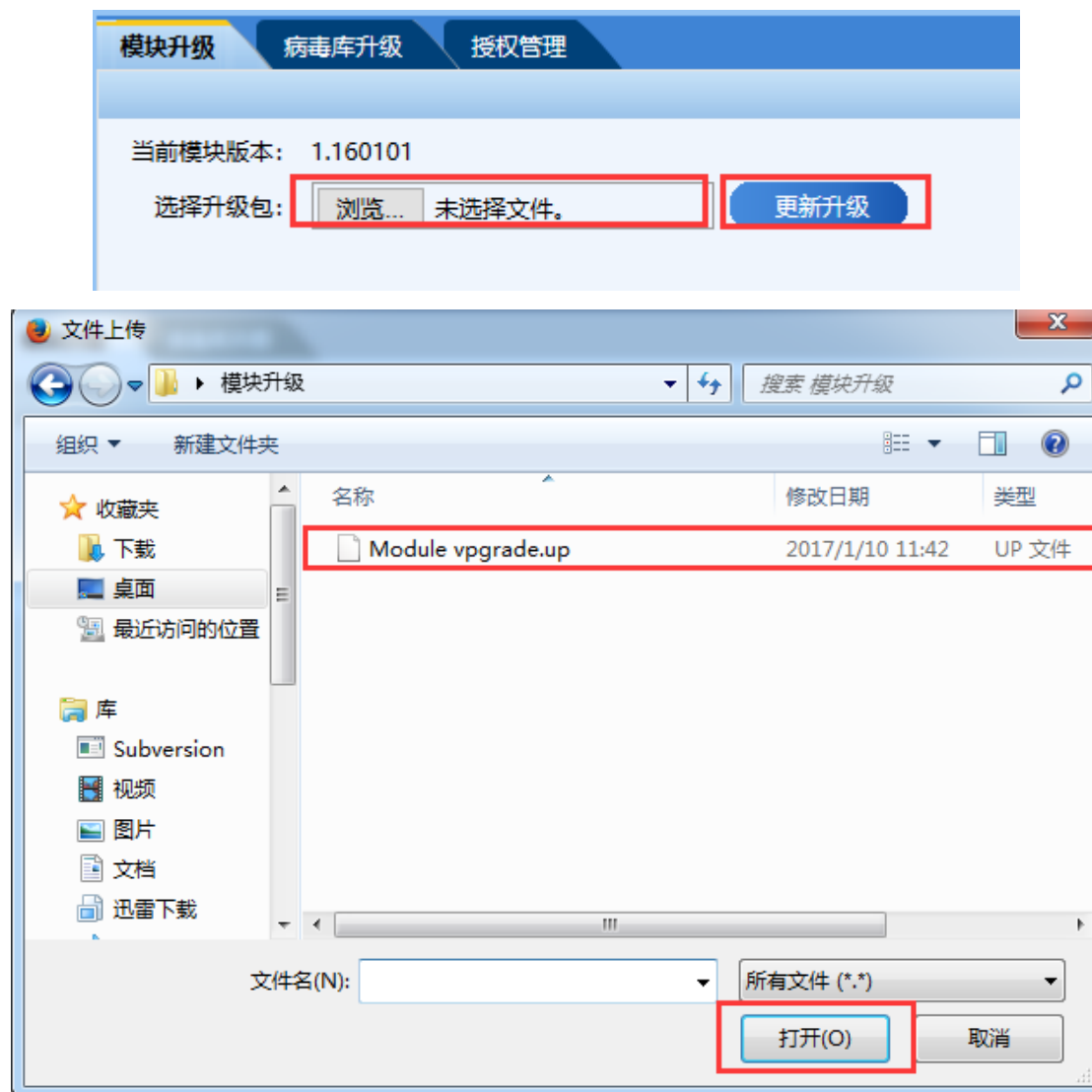
1、上图需要勾选[开启策略自动备份]

2、默认备份的策略上传到 FTP 服务器的根目录，『上传路径』填写的是子路径

3.2.8. 系统升级

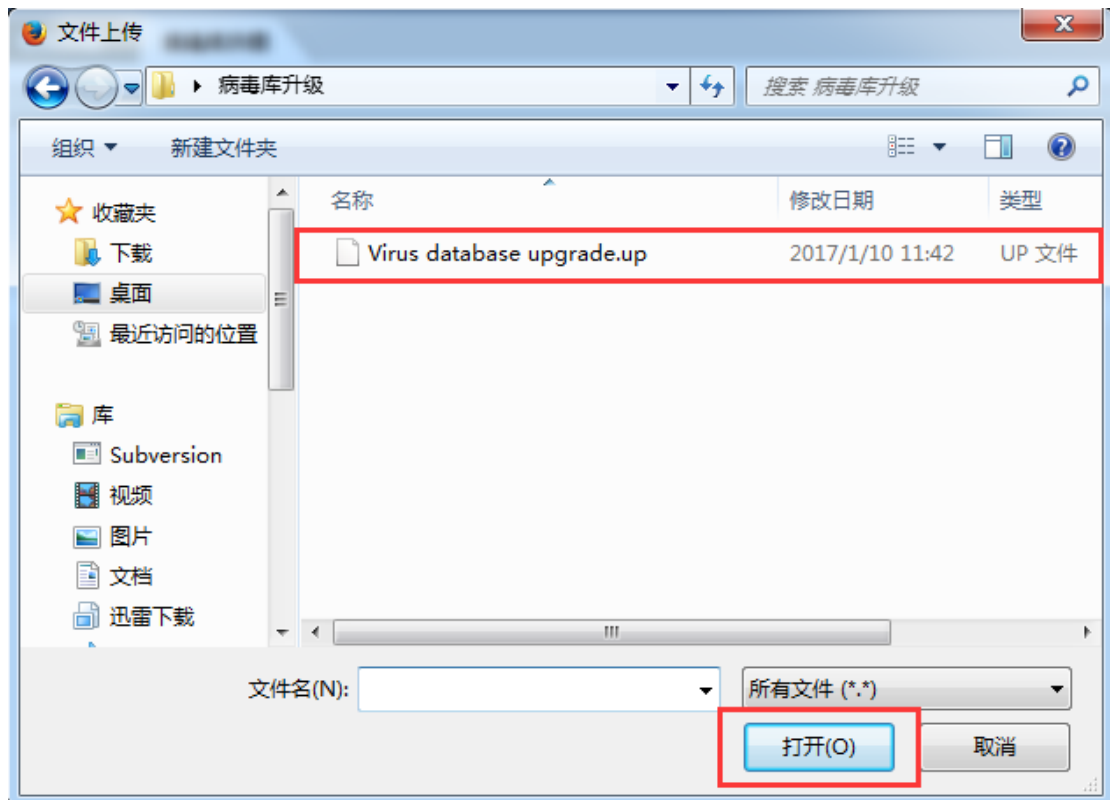
3.2.8.1 模块升级

以具备管理系统升级权限的用户（如 sysuser）登录，在『系统升级』操作区，点击右侧 **浏览**，选择要升级的模块或病毒库或授权，然后点击升级，完成升级模块或病毒库或授权的操作。『模块升级』如下图所示：



3.2.8.2 病毒库升级

『病毒库升级』如下图所示：

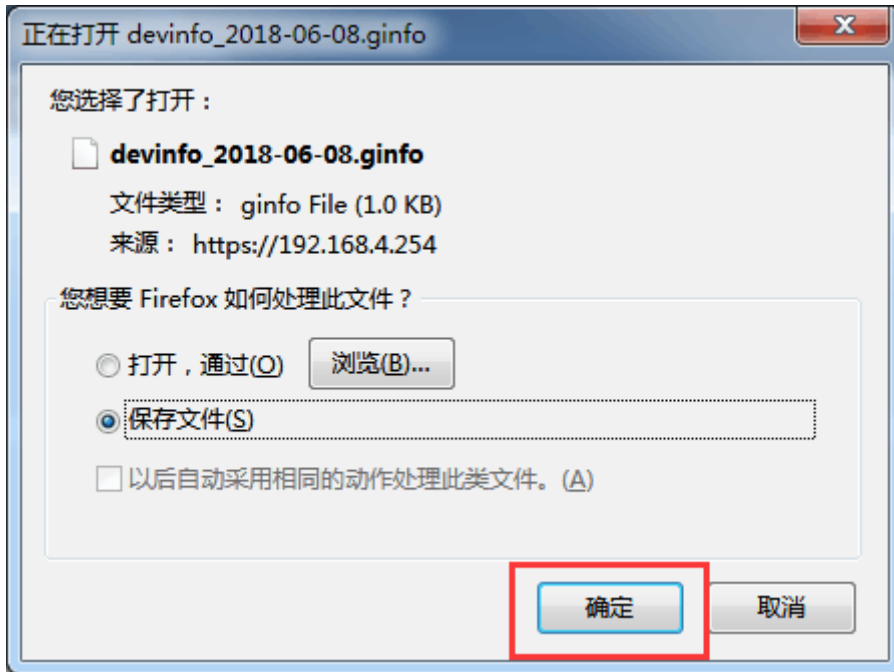


3.2.8.3 授权管理

SANGFOR_FGAP 安全隔离与单向导入系统支持对测试机器来进行管理控制。

导出设备信息: 导出设备的信息来做授权文件。如下图所示:





『授权管理』升级对过期的测试机器授权



3.2.9. 设备状态

3.2.9.1 设备状态信息

以具备查看系统状态权限的用户（如 sysuser）登录，在『设备状态信息』操作区，列出设备别名、设备型号、SN、固件版本、权限许可、硬件唯一码和设备资源信息（包括 CPU、内存，磁盘等使用情况）。

下图中：1 为设备名称、型号、版本、权限许可、SN、硬件唯一码。

2 为 CPU 的占用率。

3 为内存的占用率。

4 为磁盘的使用率。

5 为内部链路状态。



3.2.9.2 设备策略信息

『设备策略信息』用来查看配置的策略状态是否正常，可以以『模块』名称、『IP 地址』、[状态]来[查询]。如下图所示为策略状态正常：如下图所示为策略状态异常：

查看策略总数和发送文件总数信息。



3.3. 策略管理

『访问用户』用来管理通过客户端登录设备的用户信息。

以具备管理访问用户权限的用户（如 secuser）登录，在『访问用户』操作区，选择[添加]，输入『用户名』、『密码』，选择[所属级别]，选择[密码更换周期]，选择[有效日期]，选择[状态]，点击[确定]即完成添加用户操作。

访问客户端用户

添加账户

用户名: root

密码: (*请用8位及以上字母与数字组合字符)

确认密码: 密码过短

所属级别: 第0级(查看自身文件)

密码更换周期: 第0级(查看自身文件)

有效日期: 第1级(查看自身及同属第1级文件)

状态: 第2级(查看所有级别文件)

确定 取消

修改用户则在操作区处，对添加的用户进行编辑。



修改了用户密码，一定要重新生成授权文件，否则会造成访问用户无法登录设备。

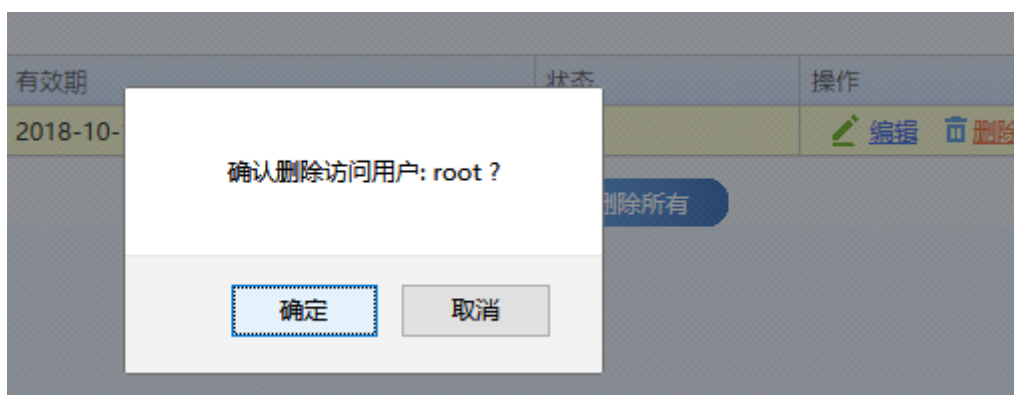
单独删除添加的用户。如下图所示：

访问客户端用户

客户端访问服务端口: 10021 保存设置

用户名	所属级别	有效期	状态	操作
root	第0级	2018-10-17 至 2019-01-17	正常	编辑 删除 生成证书

添加 删除所有 双击进入编辑



创建完访问用户，需生成证书，才能使用添加的用户来进行登陆。

『客户端访问服务端口』：客户端访问设备服务需要的端口号，默认为 10021。可自行修改，点击保存设置将保存修改内容并使设备生效。

主机安全

该设置项用来设置允许或拒绝用户从某 IP 或者某个网段访问设备。

以具备管理主机安全权限的用户（如 secuser）登录，在『主机安全』的操作区，点击添加，然后在『源 IP 地址』输入相应的 IP 或网段，设置[访问行为]“允许”或“拒绝”，

输入『描述（可选）』，点击**确定**完成访问设置。

修改『主机安全』则在操作区处，对添加的主机进行**编辑**。

单独**删除**添加的主机限制。如下图所示：

主机安全			
源主机地址	访问行为	描述	操作
0.0.0.0/0	允许	all	编辑 删除

[添加](#)
[删除所有](#)

3.3.1. 地址绑定

该设置项用来设置客户端『Ip 地址』与『Mac 地址』绑定关系。

以具备设置地址绑定权限的用户（如 secuser）登录，在『地址绑定』选项的操作区，点击**添加**，然后在对话框输入要绑定的『Ip 地址』和『Mac 地址』，输入『描述（可选）』，点击**确定**完成添加。

修改绑定主机则在操作区处，对绑定的主机进行编辑。

单独删除添加的绑定主机。如下图中所示：

地址绑定			
ip地址	Mac地址	描述	操作
192.168.1.30	08:D4:0C:0A:2A		 编辑  删除
		添加	删除所有

确认删除地址绑定对象: 192.168.1.30 ?

确定

取消

3.3.2. 存储管理

『存储管理』界面下，包含『本地存储』、『网络存储』两个标签页。

3.3.2.1 本地存储

该设置项用来删除设备中旧文件和旧日志。

以具备管理本地存储权限的用户（如 secuser）登录，在『存储管理』的操作区。

空间整理：自动删除“天数”以前的文件。

日志存储：可设置空间不足的大小，删除“天数”前的日志。



空间整理设置为 0 时不删除。

本地存储		网络存储
空间整理：自动删除 1 天以前的文件缓存 (设置为0 时不删除)		
日志存储：空间不足 4000 MB(范围 1000-9999 MB)，自动删除 5 天 (范围： 5~180) 以前的日志		
保存设置		

3.3.2.2 网络存储

该设置项用来把设备的文件存放放置在客户机指定的路径下。

以具备管理『网络存储』权限的用户（如 secuser）登录，在『网络存储』的操作区，勾选[开启使用网络存储]，然后输入『用户名』、『密码』、『网络路径』，点击保存完成设置。



路径格式：//主机 IP/目录路径。

3.3.3. 内容审查

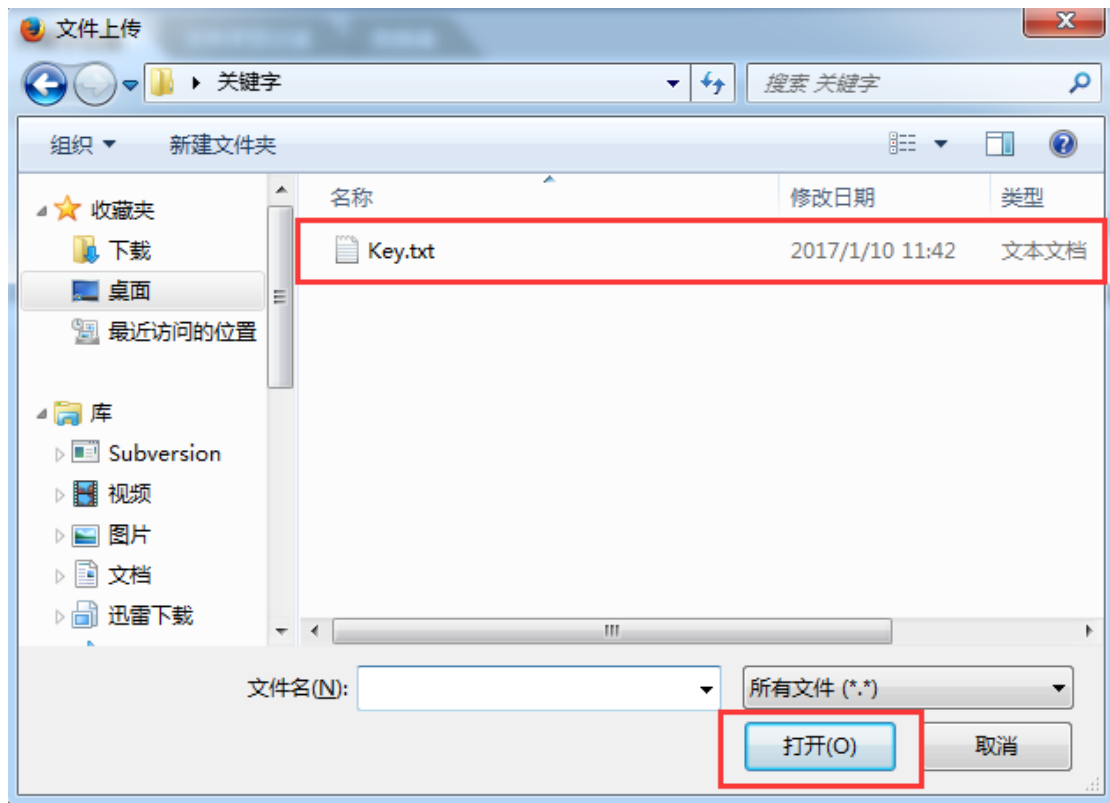
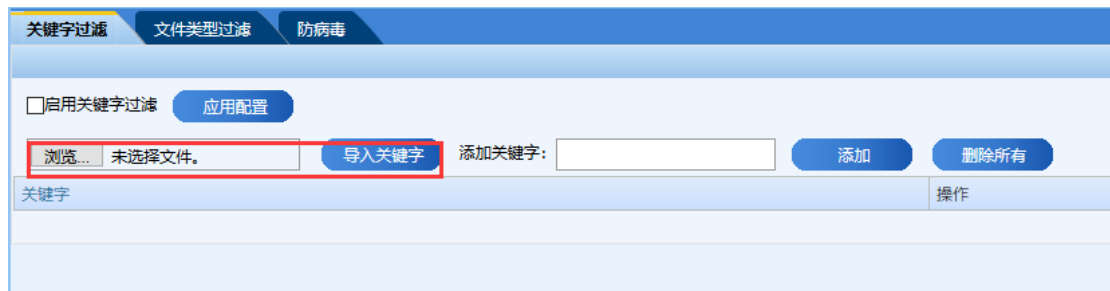
『内容审查』界面下，包含『关键字过滤』、『文件类型过滤』、『防病毒』三个标签页。

3.3.4. 关键字过滤

该设置项用来设置过滤文件内的关键字。

以具备管理关键字过滤权限的用户（如 sysuser）登录，选择『策略管理』下『内容审查』选项，勾选[启用关键字过滤]。

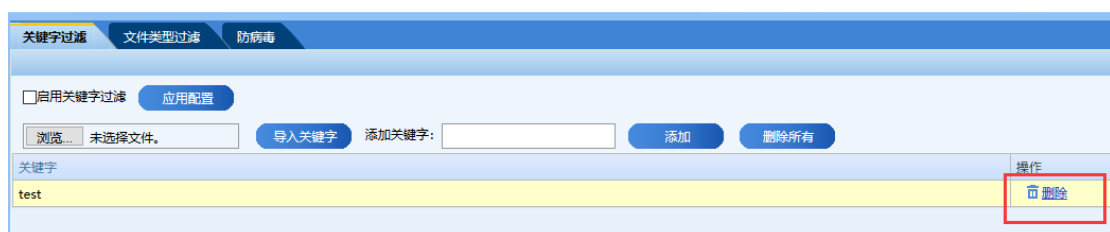
文本，如下图所示：

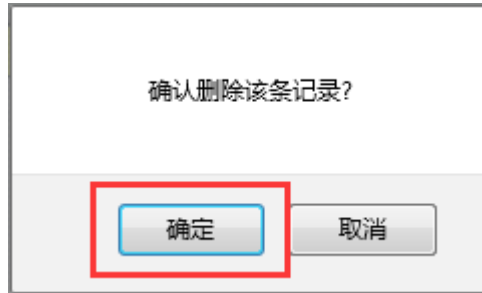


界面添加关键字。



删除添加的关键字。如下图中所示：





3.3.5. 文件类型过滤

该设置项用来设置过滤文件类型。

以具备管理文件类型过滤权限的用户（如 secuser）登录。

可设置启用[常见类型过滤]，DLL、EXE、ZIP、RAR。

支持黑白名单过滤：

不启用：关闭过滤。

白名单：允许通过。

黑名单：不允许通过。

在后缀类型输入常规类型。

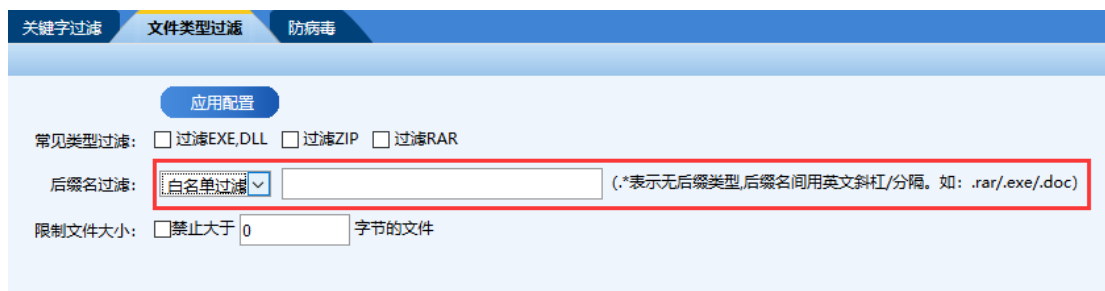


选择黑白名单必须输入后缀类型。

. *表示无后缀类型，后缀类型间用英文/分隔。

不启用过滤类型时，不显示后缀类型输入框。只有选择黑白名单过滤时才显示。

如下图所示：



文件大小过滤，点击开启限制文件大小后的单选框，[禁止大于]多少字节的文件处输入“限制的文件大小”。

3.3.6 防病毒

该设置项用来设置『防病毒』。

以具备管理『防病毒』权限的用户（如 secuser）登录，在『防病毒』操作区，勾选[启用防病毒]，然后再点击应用配置。



3.3.7 数据传输

以具备管理『数据传输』权限的用户（如 secuser）登录，在『数据传输』的操作区，点击添加，然后输入『策略名称』、选择传输[协议类型]、选择[本机 IP 地址]、输入『本机端口』、输入『目的服务器 IP』、输入『目的服务端口』（可与内网应用端口不同），点击确定完成添加操作。

[协议类型]分为 TCP、UDP、DBSYNC、DTCP(双向通讯)、DDBSYNC（双设备 DB 同步）五种。如下图 TCP、UDP、DBSYNC 协议的配置界面。

如下图为 DTCP(双向通讯)的配置界面。

数据传输

添加数据传输策略

策略名称:	test
协议类型:	TCP
本机IP地址:	0.0.0.0
本机端口:	6000
目的服务器IP:	192.168.30.22
目的服务端口:	60000
白名单数据内容:	

支持3种白名单数据格式：
以ASCII:开头的后续字符串格式 (ASCII:HELLO)
以HEX:开头的后续十六进制数据格式 (HEX:0A0B3276AACE)
以PCRE:开头的后续正则式格式 (PCRE:^[0-9])

『策略名称』：给策略设置一个名称，以便于策略的管理。

[协议类型]：传输数据用到的协议类型。

[本机 IP 地址]：设备外网业务通信口的 IP 地址。

『本机端口』：设备外网为传输数据开启的端口号。

『目的服务器 IP』：数据传输到的目的服务器的 IP 地址。

『目的服务端口』：数据传输到的目的服务器的端口号（可与内网应用端口不同）。

数据传输

添加数据传输策略

策略名称:	TEST		
协议类型:	DTCP (双设备TCP)		▼
本机IP地址:	0.0.0.0		▼
本机端口:	60000		
目的服务器IP:	192.168.3.10		
目的服务器端口:	60000		
白名单数据内容:			
支持3种白名单数据格式: 以ASCII:开头的后续字符串格式 (ASCII:HELLO) 以HEX:开头的后续十六进制数据格式 (HEX:0A0B3276AACE) 以PCRE:开头的后续正则式格式 (PCRE:^(0-9))			
本机反馈IP地址:	192.168.10.11		
本机反馈端口:	60001		
目的反馈IP地址:	192.168.11.11		
目的反馈端口:	60001		

确定

取消

『本机反馈 IP 地址』：从另一台设备内网通信口流出的数据到本台设备外网通信口的 IP 地址。

『本机反馈端口』：从另一台设备内网通信口流出的数据到本台设备外网通信口的端口号。

『目的反馈 IP 地址』：从本台设备内网通信口流出的数据到另一台设备外网通信口的 IP 地址。

『目的反馈端口』：从本台设备内网通信口流出的数据到另一台设备外网通信口的端口号。

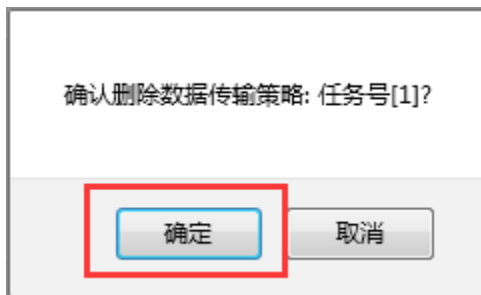


『白名单数据内容』处可填写交换数据的白名单，若要设置内容为 ASCII 数据并且数据以 ABC 开始，应填入以下内容“ASCII:ABC”；十六进制数据和正则表达式同上。

修改『数据传输』则在操作区处，对『数据传输』进行编辑、全选、启用选中策略、停用选中策略、删除所有。

单独删除添加的『数据传输』。如下图所示:

数据上传										
选择	名称	任务号	协议类型	本机IP地址	本机端口	目的服务器	目的端口	数据内容	状态	操作
☐	test	1	TCP	0.0.0.0	6000	192.168.30.22	60000		启用	 编辑 删除
添加 全选 启用选中策略 停用选中策略 删除所有										



3.3.8 文件交换

『文件交换』界面下，包含『FTP 自动交换』、『SMB 自动交换』、『HTTP 交换』三个标签页。

3.3.8.1 FTP 自动交换

该项使设备主动发起连接外网文件服务器，把文件同步传输至内网文件服务器

以具备管理主动交换权限的用户（如 secuser）登录，在『FTP 自动交换』操作区，点击 **添加**，输入交换源和交换目的『FTP 服务器 IP 地址』、『服务端口』号、『用户名』、『密码』、『子路径』等信息。



『子路径』输入为 FTP 根目录下的子路径，以/分隔路径。

『策略名称』：给策略设置一个名称，以便于策略的管理。

[完成后移除源文件]：源端文件传输到设备外网后，删除源文件。

[完成后移除空目录]：（与[完成后移除源文件]冲突，两者只能选一个）

[增量传输]：只传输源端有更改或新添加的文件，对于未发生改变的文件只在策略新建时传输一次，不再重复传输。



[增量传输]时，文件过多应及时删除文件，否则会影响传输速度。

[跳过空目录]：不传输源端空目录到设备外网。

『交换源间隔』：设备每隔多长时间（单位秒）去源端服务器检测新文件。

[文件类型过滤]提供白名单和黑名单的文件名过滤方式。

- ❖ 白名单是指只允许指定的文件类型通过。
- ❖ 黑名单是指不允许指定的文件类型通过。

文件扩展名以/为分割号。如.txt/.xml/.doc 等。

[源 FTP 编码类型]：源端 FTP 的编码类型，默认为 GBK。

设置[优先级]：共分 5 级。

『流量控制』：控制传输文件时的速率。

填写完相应的信息后点击**确定**，如果还需要继续添加新的交换任务，就在任务列表处，点击**添加**，填写完成相应信息后点击**确定**即可。如下图所示：



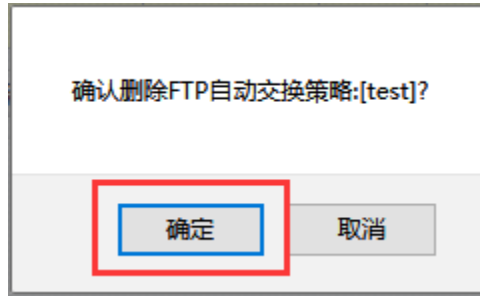
如选择了黑/白名单过滤，必须输入后缀类型。

修改『FTP 自动交换』任务则在操作区处，对『FTP 自动交换』任务进行**编辑**、**全选**、**启用选中策略**、**停用选中策略**、**删除所有**。

单独**删除**添加的『FTP 自动交换』任务。如下图中所示：

选择	名称	源FTP服务器IP	源端口	子路径	目的服务器IP	目的端口	子路径	源文件	循环间隔	过滤类型	级别	状态	操作
☐	test	192.168.1.22	21	/rrr	192.168.2.34	21	/rrr	移除	3	不启用过滤	默认	启用	

添加 全选 启用选中策略 停用选中策略 删除所有



3.3.8.2 SMB 自动交换

该项使设备主动发起连接外网文件服务器，把文件同步传输至内网文件服务器

以具备管理主动交换权限的用户（如 secuser）登录，在『SMB 自动交换』操作区，点击 **添加**，输入交换源和交换目的『IP 地址』、『用户名』、『密码』、『共享名』、『子路径』等信息。

『策略名称』：给策略设置一个名称，以便于策略的管理。

[完成后移除源文件]：源端文件传输到设备外网后，删除源文件。

[完成后移除空目录]：（与[完成后移除源文件]冲突，两者只能选一个）

[增量传输]：只传输源端有更改或新添加的文件，对于未发生改变的文件只在策略新建时传输一次，不再重复传输。



[增量传输]时，文件过多应及时删除文件，否则会影响传输速度。

[跳过空目录]：不传输源端空目录到设备外网。

『交换源间隔』：设备每隔多长时间（单位秒）去源端服务器检测新文件。

[文件类型过滤]提供白名单和黑名单的文件名过滤方式。

- ❖ 白名单是指只允许指定的文件类型

- ❖ 黑名单是指不允许指定的文件类型

文件扩展名以/为分割号。如.txt/.xml/.doc 等。

设置[优先级别]：共分 5 级。

『流量控制』：控制传输文件时的速率。

填写完相应的信息后点击**确定**，如果需要继续添加新的交换任务，就在任务列表处，点击**添加**，填写完成相应信息后点击**确定**即可。如下图所示：

FTP自动交换
添加FTP自动交换策略

源FTP服务器IP地址: 192.168.88.99 目的服务器IP地址: 192.168.30.22

源服务器端口: 21 目的服务器端口: 21

交换源: 用户名: TEST 交换目的: 用户名: ROOT

密码: 密码: *****

子路径: /etc (路径间用斜杠/分隔) 子路径: /HOME (路径间用斜杠/分隔)

策略名称:

源目录文件处理: ☒ 完成后移除源文件 ☐ 完成后移除空目录 ☐ 增量传输 ☐ 跳过空目录

交换间隔: 3 秒循环检查新文件

文件类型过滤: 不启用过滤

源FTP编码类型: GBK

优先级: 默认 (4级为最高优先级)

流量控制: 0 KB/s (0为不限制, 范围: 0~20000)

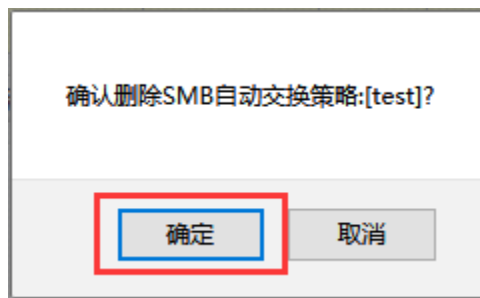
确定 取消

修改『SMB 自动交换』任务则在操作区处，对『SMB 自动交换』任务进行**编辑**、**全选**、**启用选中策略**、**停用选中策略**、**删除所有**。

单独**删除**添加的『SMB 自动交换』任务。如下图中所示：

选择	名称	源服务器ip	共享名	子路径	目的服务器ip	共享名	子路径	源文件	循环间隔	过滤类型	级别	状态	操作
☐	test	192.168.1.22	root	/	192.168.2.34	test	/	移除	3	不启用过滤	默认	启用	

添加 全选 启用选中策略 停用选中策略 删除所有



3.3.9 邮件转发

产品提供『邮件转发』功能，外部邮件发往内网邮件服务器。

以具备管理主动交换权限的用户（如 secuser）登录，在『邮件转发』点击**添加**，输入交换源和换目的服务器『IP 地址』、『端口』、『用户名』、『密码』等信息。



用户名为发送邮箱的地址或接收邮箱的地址。

『策略名称』：给策略设置一个名称，以便于策略的管理。

[协议类型]：协议支持 SMTP、POP3、IMAP 协议，默认为 SMTP 协议。

支持发件人地址黑白名单过滤。

支持收件人地址黑白名单过滤。



地址间用英文斜杠/为分割。如：abc@SANGFOR 光闸.com/123@SANGFOR 光闸.cn。

支持附件黑白名单过滤。如需要携带附件，附件类型不填写，代表可以携带任何类型扩展名的附件。

邮件大小限制。

邮件内容过滤包括主题、正文（每行为一个关键字列）。

邮件转发

添加策略

本机IP地址: 192.168.11.254 目的服务器IP地址: 192.168.1.22

本机端口: 25 目的端口: 25

本机配置: 用户名: sysuser 目的配置: 用户名: ROOT

密码: 密码:

策略名称: test

协议类型: SMTP

发件人地址过滤: 不启用 (地址间用英文斜杠/分隔。如: abc@xxx.com/123@xxx.cn)

收件人地址过滤: 不启用 (地址间用英文斜杠/分隔。如: abc@xxx.com/123@xxx.cn)

附件类型过滤: 禁止带附件 (.* 表示无后缀类型, 后缀名间用英文斜杠/分隔。如: .rar/.exe/.doc)

☐ 禁止大于 [] 字节的邮件

黑名单内容过滤: ☐ 过滤邮件主题 ☐ 过滤邮件正文

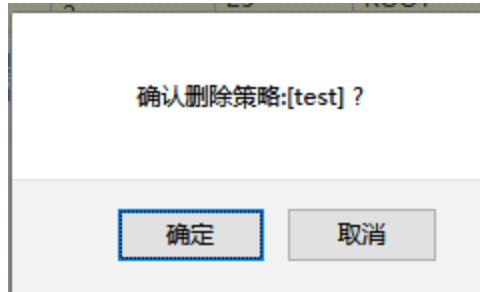
(每行为一个关键字列)

修改『邮件转发』任务则在操作区处，对『邮件转发』任务进行编辑、全选、启用选中策略、停用选中策略、删除所有。

单独删除添加的『邮件转发』任务。如下图中所示：

邮件转发

选择	名称	协议类型	本机IP	本机端口	本地用户	目的服务器	目的端口	目的用户	地址过滤	过滤主题	过滤正文	附件	状态	操作
☐	test	SMTP	192.168.11.254	25	sysuser	192.168.1.22	25	ROOT	不过滤	不过滤	不过滤	禁止带附件	启用	
添加 全选 启用选中策略 停用选中策略 删除所有														



3.3.10 组播策略

以具备管理『组播策略』权限的用户（如 secuser）登录，在『组播策略』操作区，点击 **添加**，输入『策略名称』、『源端组播 IP』、『源端组播端口』、『源接收 IP』、『目的组播 IP』、『目的组播端口』、『目的发送 IP』。

支持 ASM（任意信源）、SSM（指定信源）、FSM（过滤信源）三种[组播类型]。

『信源 IP 地址列表』（按行分隔，不重复 IP 最多 20 个）

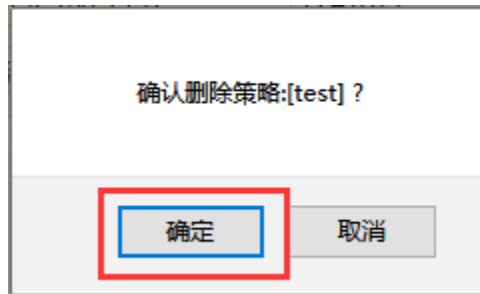
组播策略	
添加策略	
策略名称:	
源端组播IP:	224.0.0.1
源端组播端口:	4000
源接收IP:	0.0.0.0
目的组播IP:	224.0.0.1
目的组播端口:	4000
目的发送IP:	
组播类型:	ASM(任意信源) ASM(任意信源) SSM(指定信源) FSM(过滤信源)
确定 取消	

修改『组播策略』则在操作区处，对『组播策略』进行 **编辑**、**全选**、**启用选中策略**、**停用选中策略**、**删除所有**。

单独删除添加的『组播策略』。如下图中所示：

组播策略									
选择	名称	源组播IP	源组播端口	源接收IP	目的组播IP	目的端口	目的发送IP	状态	操作
☐	test	224.0.0.1	4000	0.0.0.0	224.0.0.1	4000		启用	编辑 删除

[添加](#)
[全选](#)
[启用选中策略](#)
[停用选中策略](#)
[删除所有](#)



3.3.12 数据库同步

以具备管理『数据库同步』权限的用户（如 secuser）登录，在『数据库同步』操作区，点击添加，输入『策略名称』，选择源端和目的端[DB 类型]、『数据库 IP』、『DB 端口』、『DB 名称』、『用户 ID』、『用户密码』等信息，如下图所示：

数据库同步策略	
添加策略	
策略名称: test	目的DB服务器配置
源端DB类型: Oracle	目的端DB类型: MySQL
源端数据库IP: 192.168.4.22	目的端数据库IP: 192.168.50.2
源端DB端口: 3306	目的端DB端口: 3306
源端DB名称: test	目的端DB名称: test
源端用户ID: test	目的端用户ID: test
源端用户密码:	目的端用户密码:
字符集 (可留空):	对象别名前缀 (可留空):
确定 取消	

『字符集（可留空）』：数据库源端的字符集编码类型。

『添加同步表策略』则在操作区处，对『数据库同步』进行编辑，进入后如下图：

数据库同步策略

编辑策略

策略名称: test

源端DB服务器配置

源端DB类型: Oracle

源端数据库IP: 192.168.4.22

源端DB端口: 3306

源端DB名称: test

源端用户ID: test

源端用户密码:

字符集 (可留空):

目的端DB服务器配置

目的端DB类型: MySQL

目的端数据库IP: 192.168.50.2

目的端DB端口: 3306

目的端DB名称: test

目的端用户ID: test

目的端用户密码:

对象别名前缀 (可留空):

确定 取消

包含策略列表

序号	源端表	目的端表	源端表字段	目的端表字段	源端表主键	目的端表主键
添加同步表策略 清除所有表同步策略						

点击[添加同步表策略](#)，输入源和目的『表名称』、『表字段列表』（每个字段要以逗号分隔；所有字段可以*来表示）、『表主键』、选择[表拷贝]、[重建临时表]、[重建触发器]。

自动[读源端表字段](#)（读取到同步的源表的所有字段）。

如下图（『源表字段列表』为使用自动读取表字段读取到的；『目的表字段列表』为所有字段）



自动读取源表字段，需要发送端可以远端登陆源数据库。

数据库同步策略

添加同步表策略

源端同步表配置

源表名称: *

源表字段列表 (逗号分隔):

源表主键:

同步过滤条件:

同步动作: ☒ 同步插入 ☒ 同步更新 ☒ 同步删除

目的端同步表配置

目的表名称: *

目的表字段列表 (逗号分隔):

目的表主键:

特殊选项: ☐ 表拷贝 ☐ 重建临时表 ☐ 重建触发器 ☐ 双向 (需双设备配合)

确定 取消 [读源端表字段](#)



oracle 数据库表面前加用户名/sqlserver 数据库表面前加 dbo, MySQL 数据库字符集必须填入正确。

单独[删除](#)添加的同步表策略。如下图中所示:

数据库同步策略

编辑策略

策略名称: test

源端DB类型: Oracle

源端数据库IP: 192.168.4.22

源端DB端口: 3306

源端DB名称: test

源端用户ID: test

源端用户密码:

字符集 (可留空):

目的端DB类型: MySQL

目的端数据库IP: 192.168.50.2

目的端DB端口: 3306

目的端DB名称: test

目的端用户ID: test

目的端用户密码:

对象别名前缀 (可留空):

包含表策略列表 + 添加同步表策略 - 清除所有表同步策略

序号	源端表	目的端表	源端表字段	目的端表字段	源端表主键	目的端表主键	操作
1	test	hadoop	*	*			编辑 删除

确认删除该条命令？

修改『数据库同步』则在操作区处，对『数据库同步』进行编辑、全选、启用选中策略、停用选中策略、删除所有。

单独删除添加的『数据库同步』。如下图中所示：

数据库同步策略

连续同步间隔: 0 (0-9999) 毫秒 ☐ 开启定时同步 每天同步开始时间: (格式: 08:30) 持续同步时长: 15 (3-1000) 分钟

选择	名称	源端数据库	源端数据库IP	目的端数据库	目的端数据库IP	表策略数	状态	操作
☐	test	[Oracle] test	192.168.4.22	[MySQL] test	192.168.50.2	1	停用	编辑 删除

确认删除策略:[test]？



数据库类型支持 Oracle、SQLServer (2008 以上、2005、2000)、MYSQL、Sybase、PostgreSQL、DB2、达梦 DM、金仓 Kingbase 等。

『连续同步间隔』：发送端强制等待时间（单位为毫秒）。

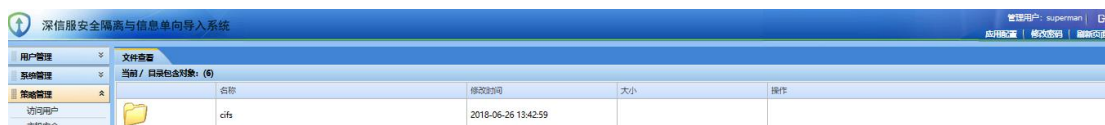
『开启定时同步』：每天同步开始时间（格式：08:30），持续同步时长（3-1000）分钟。

修改完数据库同步限制条件后，点击保存设置将保存修改内容并使设备生效

3.3.13 文件查看



查看、删除（可删除文件或删除文件夹）、传输文件，下图所示：

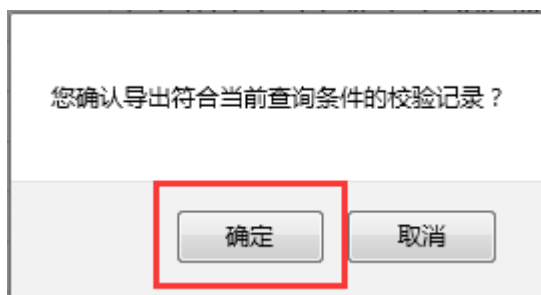
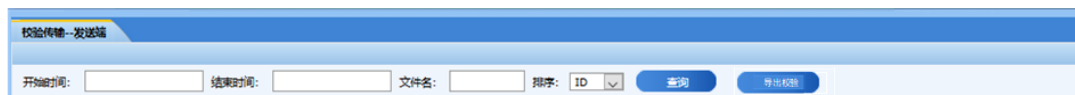


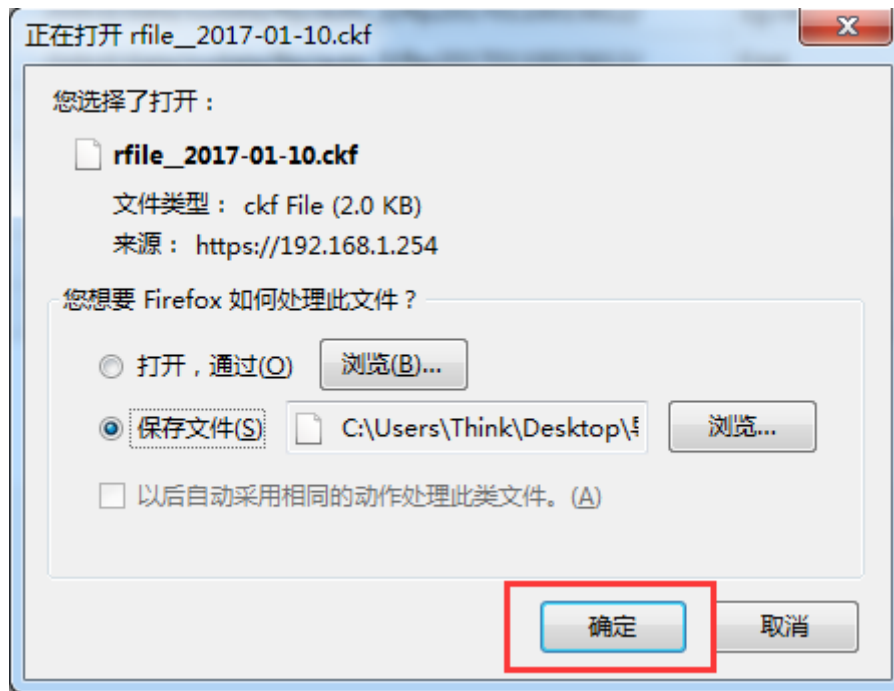
3.3.14 校验传输

『校验传输』功能可以检测从设备发送端到接收端传输是否出错，并可以重传出错文件。

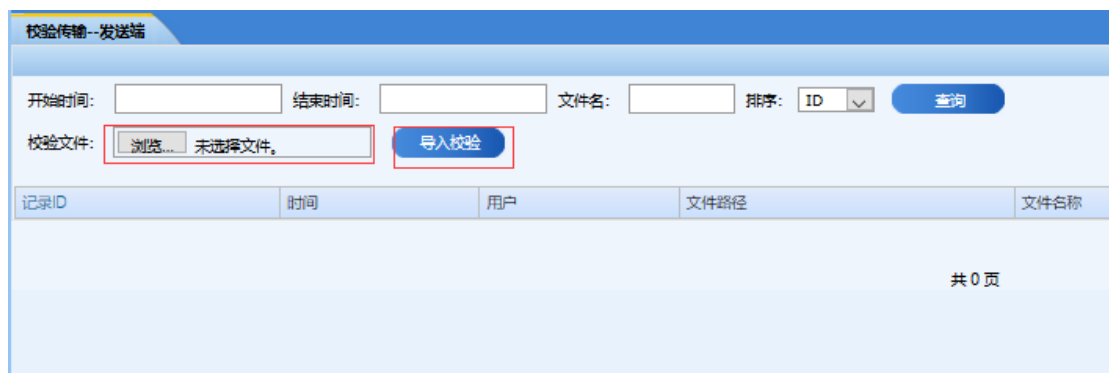
以具备『校验传输』权限的用户（如 secuser）登录。

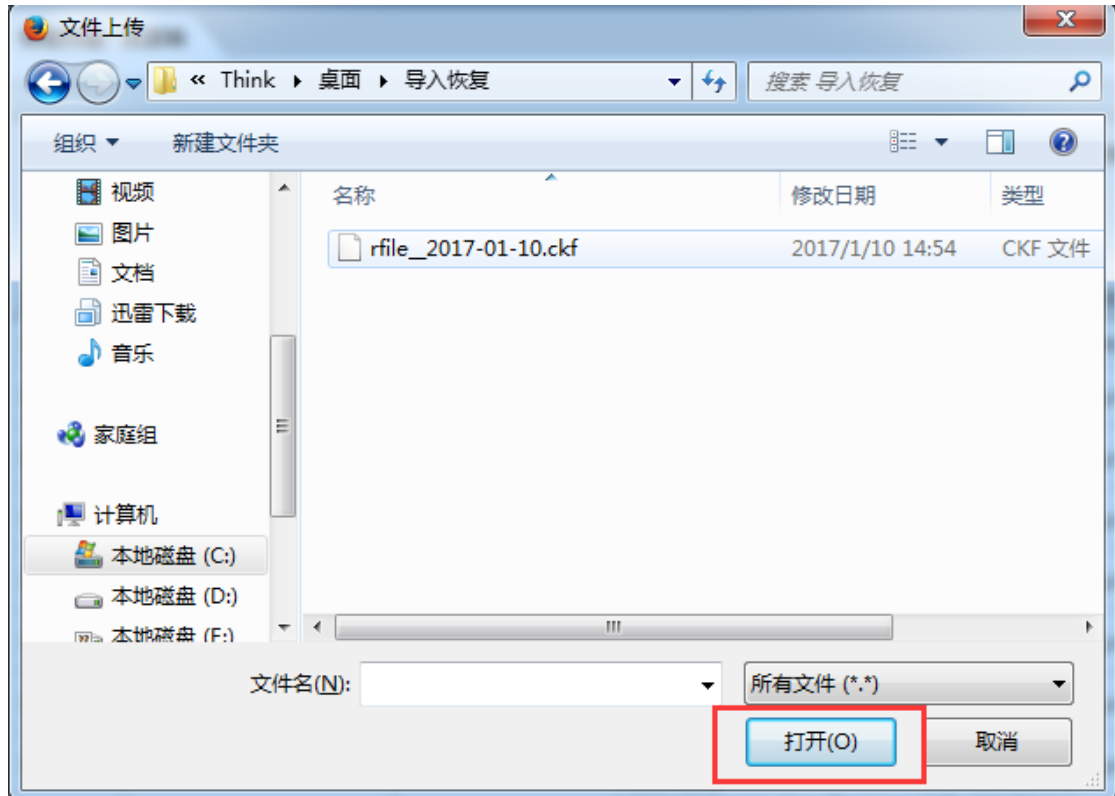
在内网端导出校验，生成文件。如下图中所示：





使用此文件在外网端导入校验。如下图所示：





使用『时间』、『文件名』名来查询文件传输记录。

使用 ID、时间、用户、文件名、大小来[排序]。

3.4. 日志审计

3.4.1. 管理日志

该项为查询、导出、删除系统管理员管理设备的日志。

以具备管理『管理日志』权限的用户（如 loguser）登录。

使用『时间』、『用户』名来查询日志。

使用 ID、内容、时间、用户名、结果来[日志排序]。

管理操作日志					
开始时间: 结束时间: 用户: 日志排序: ID 查询 导出日志 删除日志					
记录ID	时间	用户	管理 IP	操作内容	结果
42	2018-10-15 10:27:12	admin		登录成功!	成功
41	2018-10-11 20:35:26	admin		用户操作超时自动退出!	成功
40	2018-10-11 20:17:06	admin		登录成功!	成功
39	2018-10-11 20:14:32	admin		用户操作超时自动退出!	成功
38	2018-10-11 19:54:25	admin		数据库同步策略[test] 添加表: [test.table]	成功
37	2018-10-11 19:53:57	admin		添加数据库同步策略[test] 操作	成功
36	2018-10-11 19:51:51	admin		登录成功!	成功
35	2018-10-11 19:49:28	admin		用户操作超时自动退出!	成功
34	2018-10-11 19:39:23	admin		登录成功!	成功
33	2018-10-11 18:32:00	admin		用户操作超时自动退出!	成功

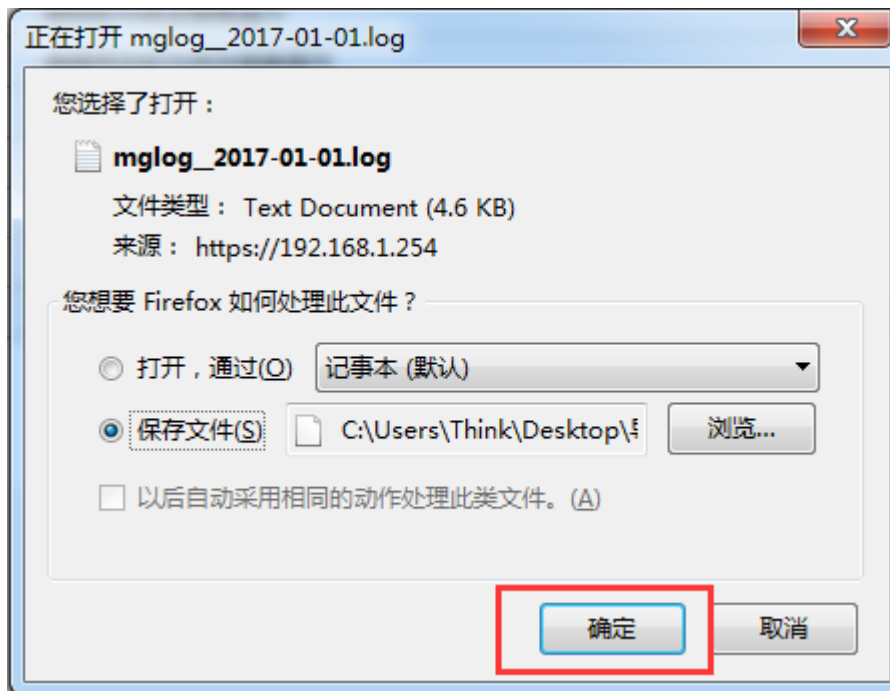
共 5 页 1 2 3 4 > 最后一页

用户导出管理日志供以后查阅。如下图中所示：

管理操作日志					
开始时间: 结束时间: 用户: 日志排序: ID 查询 导出日志 删除日志					
记录ID	时间	用户	管理 IP	操作内容	结果
42	2018-10-15 10:27:12	admin		登录成功!	成功
41	2018-10-11 20:35:26	admin		用户操作超时自动退出!	成功
40	2018-10-11 20:17:06	admin		登录成功!	成功
39	2018-10-11 20:14:32	admin		用户操作超时自动退出!	成功
38	2018-10-11 19:54:25	admin		数据库同步策略[test] 添加表: [test.table]	成功
37	2018-10-11 19:53:57	admin		添加数据库同步策略[test] 操作	成功
36	2018-10-11 19:51:51	admin		登录成功!	成功
35	2018-10-11 19:49:28	admin		用户操作超时自动退出!	成功
34	2018-10-11 19:39:23	admin		登录成功!	成功
33	2018-10-11 18:32:00	admin		用户操作超时自动退出!	成功

共 5 页 1 2 3 4 > 最后一页

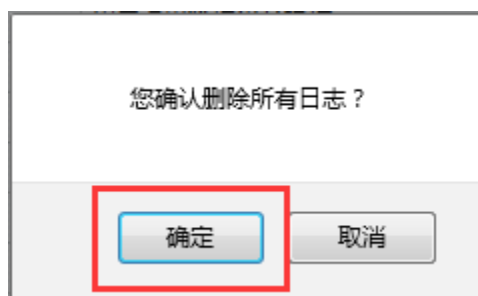
您确认导出符合当前查询条件的所有日志？



用户删除管理日志。如下图所示：

管理操作日志					
开始时间:		结束时间:		用户:	
日志排序:	ID	查询	导出日志	删除日志	
记录ID	时间	用户	管理 IP	操作内容	结果
42	2018-10-15 10:27:12	admin		登录成功!	成功
41	2018-10-11 20:35:26	admin		用户操作超时自动退出!	成功
40	2018-10-11 20:17:06	admin		登录成功!	成功
39	2018-10-11 20:14:32	admin		用户操作超时自动退出!	成功
38	2018-10-11 19:54:25	admin		数据库同步策略[test] 添加表: [test.table]	成功
37	2018-10-11 19:53:57	admin		添加数据库同步策略[test] 操作	成功
36	2018-10-11 19:51:51	admin		登录成功!	成功
35	2018-10-11 19:49:28	admin		用户操作超时自动退出!	成功
34	2018-10-11 19:39:23	admin		登录成功!	成功
33	2018-10-11 18:32:00	admin		用户操作超时自动退出!	成功

共 5 页 1 2 3 4 > 最后一页



3.4.2. 审计员日志

该项用来记录日志管理员操作日志。

以具备管理『审计员日志』权限的用户（如 secuser）登录。

使用『时间』、『用户』名来[查询]日志。

使用内容、时间、用户名、结果来[日志排序]。

导出『审计员日志』供以后查阅。

删除『审计员日志』。

审计员操作日志				
开始时间:		结束时间:		用户:
日志排序:	时间	查询	导出日志	删除日志
记录ID	时间	用户	操作内容	结果
6	2018-10-18 12:02:39	loguser	用户退出管理平台操作	成功
5	2018-10-18 12:01:42	loguser	登录成功!	成功
4	2018-10-18 12:01:27	loguser	用户退出管理平台操作	成功
3	2018-10-18 12:01:20	loguser	修改登录密码操作	成功
1	2018-10-18 12:01:05	loguser	登录成功!	成功
2	2018-10-18 12:01:05	loguser	密码使用超过设定更新期限!	警告
共 1 页				

3.4.3. 系统日志

该项用来[查询]、导出、删除『系统日志』。

以具备管理『系统日志』权限的用户（如 loguser）登录。

使用『时间』、『日志类型』来[查询]日志。

使用 ID、时间、类型、结果、备注来[日志排序]。

导出『系统日志』供以后查阅。

删除『系统日志』。

系统日志				
开始时间:		结束时间:		日志类型:
日志排序:	ID	查询	导出日志	删除日志
记录ID	时间	类型	结果	备注
共 0 页				

3.4.4. 交换日志

该选项用来查看用户与 IP 地址的某个时间段内自动交换任务内容的日志。

以具备管理『交换日志』权限的用户（如 loguser）登录。

使用『时间』、『用户』名、『IP』、『端口』来[查询](#)日志。

使用 ID、用户、时间、访问者 IP、目的 IP、端口、信息、结果来[\[日志排序\]](#)。

导出『交换日志』供以后查阅。

删除『交换日志』。



3.4.5. 邮件日志

该选项用来查看基于用户与 IP 地址的某个时间段内发送邮件转发任务内容的日志。

以具备管理『邮件日志』权限的用户（如 loguser）登录。

使用『时间』、『对象地址』来[查询](#)日志。

使用 ID、时间、对象地址、发件人、收件人、结果来[\[日志排序\]](#)。

导出『邮件日志』供以后查阅。

删除『邮件日志』。



3.4.6. 连接日志

该项用来管理『连接日志』。

以具备管理『连接日志』权限的用户（如 loguser）登录。

使用『时间』、『IP』、『端口』来[查询](#)日志。

使用 ID、时间、源 IP、目的 IP、端口、告警信息来[\[日志排序\]](#)。

导出『连接日志』供以后查阅。

删除『连接日志』。



3.4.7. 内容过滤

该项用来查看设备传输『内容过滤』日志。

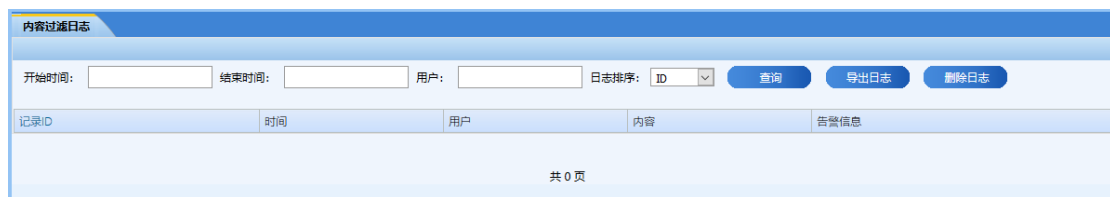
以具备管理『内容过滤』日志权限的用户（如 loguser）登录。

使用『时间』、『用户』来[查询](#)日志。

使用 ID、时间、内容、用户、告警信息来[\[日志排序\]](#)。

导出『内容过滤』日志供以后查阅。

删除『内容过滤』日志。



3.4.8. 数据库同步日志

该项用来查看设备『数据库同步日志』。

以具备管理『数据库同步日志』权限的用户（如 loguser）登录。

使用『时间』、『策略名』、『数据库 IP』、『同步表名』来[查询](#)日志。

使用 ID、时间、策略名、源数据库名、源数据库 IP、目的数据库名、目的数据库 IP、源同步表、目的同步表来[\[日志排序\]](#)。

导出『数据库同步日志』供以后查阅。

删除『数据库同步日志』。



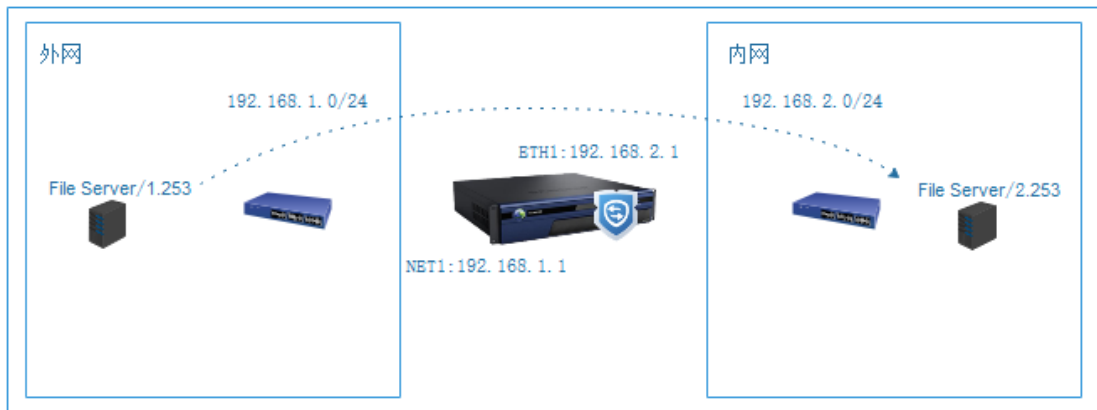
ID	时间	策略名	源数据库名	源数据库IP	目的数据库名	目的数据库IP	源同步表	目的同步表	结果
共 0 页									

第4章 SANGFOR_FGAP 安全隔离与信息单向导入系统产品部署案例

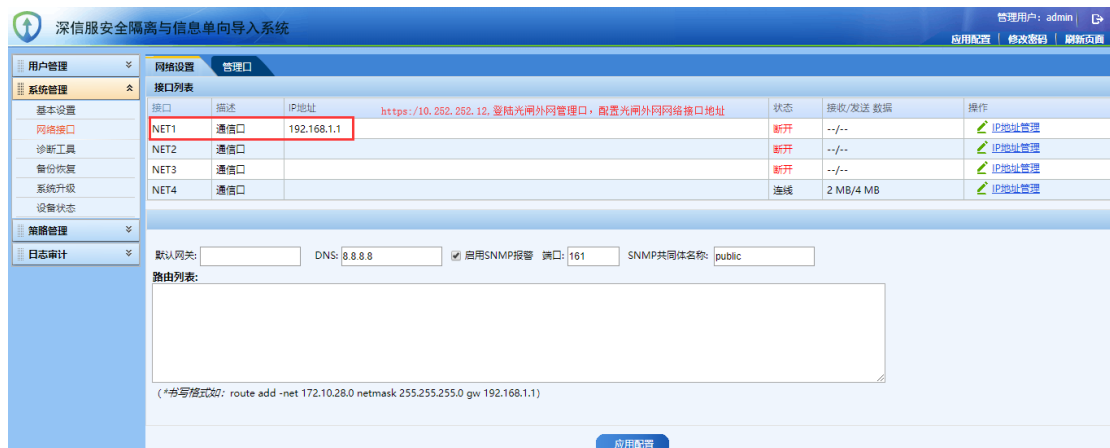
4.1.FTP 自动交换

需求：外网文件服务器 192.168.1.253（账号：admin，密码：admin，端口 21），向内网 192.168.2.253（账号：admin，密码：admin，端口 21）同步文件。

原理：内外端服务器均为 FTP 服务器，不在同一个子网，需要通过单向光闸从外端服务器将文件搬运至内端服务器，其中光闸采取主动工作模式，主动抓取、主动推送。



第一步：分别登录内外网面板「系统管理 -> 网络接口」配置对应内外网接口地址。



第二步：在外端机「策略管理 -> 文件交换」中定义源 FTP、目标 FTP 的传输路径，子路径是指该用户名下的路径，尽量勾选删除源文件，否则会每次都轮询到该文件。注：增量传输会对源文件和目的服务器文件做校验，将大大影响设备性能，如不是特殊需求不建议开启

系统管理

策略管理

访问用户

主机安全

地址绑定

存储管理

内容审查

数据传输

文件交换

邮件转发

组播策略

视频点播

数据库同步

文件查看

校验传输

日志审计

添加FTP自动交换策略

源FTP服务器IP地址: 192.168.1.253

源服务器端口: 21

交换源端: 用户名: andy 密码: **** 子路径: /andy (路径间用斜杠/分隔)

目的服务器IP地址: 192.168.2.253

目的服务器端口: 21

交换目的端: 用户名: andy 密码: **** 子路径: /andy (路径间用斜杠/分隔)

策略名称: FTP

源目录文件处理: ☒ 完成后删除源文件 ☐ 完成后删除空目录 ☐ 增量传输 ☐ 跳过空目录

交换源间隔: 3 秒循环检查新文件

文件类型过滤: 不启用过滤 (*表示无后缀类型, 后缀名间用英文斜杠/分隔, 如: .rar/.exe/.doc)

源FTP编码类型: UTF8

优先级: 默认 (4级为最高优先级)

流量控制: 0 KB/s (0为不限制, 范围: 0~20000)

确定 取消

第三步：在外端机应用策略。

深信服安全隔离与信息单向导入系统

管理用户: admin

应用配置 修改密码 刷新页面

用户管理

系统管理

策略管理

访问用户

主机安全

地址绑定

存储管理

内容审查

数据传输

文件交换

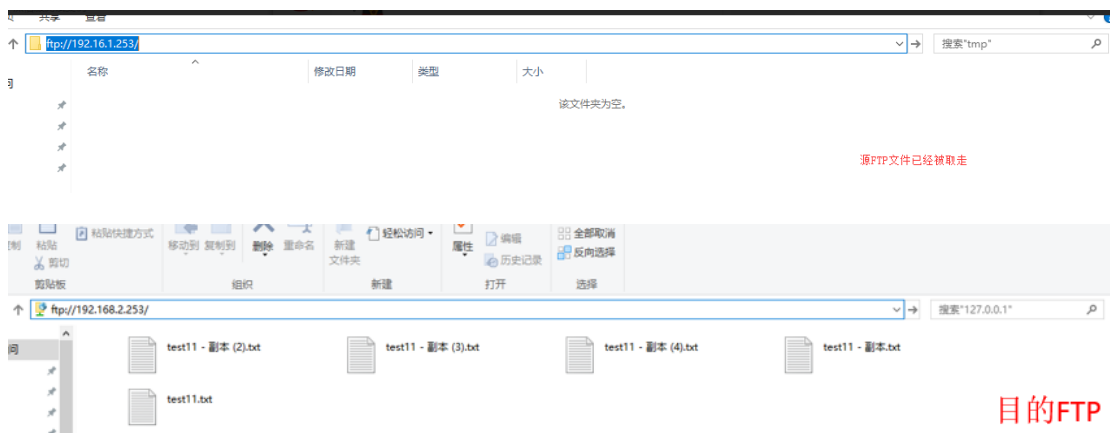
邮件转发

FTP自动交换 SMB自动交换

名称	源FTP服务器IP	源端口	子路径	目的服务器IP	目的端口	子路径	源文件	循环间隔	过滤类型	级别	状态	操作
FTP	192.168.1.253	21	/andy	192.168.2.253	21	/andy	删除	3	不启用过滤	默认	应用	应用 删除

添加 全选 应用选中策略 停用选中策略 删除所有

第四步，测试，在外端 FTP 服务器上放置新文件，查看外端机是否取走了该文件，查看内端机是否收到了该文件，查看内端机是否将文件发送给了内网 FTP 服务器。



第五步，分别登陆内外端机在日志审计-交换日志可以查看获取到的文件信息。

深信服安全隔离与信息单向导入系统

管理用户: admin

应用配置 修改密码 刷新页面

用户管理

系统管理

策略管理

访问用户

主机安全

地址绑定

存储管理

内容审查

数据传输

文件交换

邮件转发

日志审计

管理日志

审计类日志

系统日志

交换日志

邮件日志

连接日志

内容过滤

数据库同步日志

交换日志

开始时间: 结束时间: 用户: IP: 端口: 日志类型: ID

查询 导出日志 删除日志

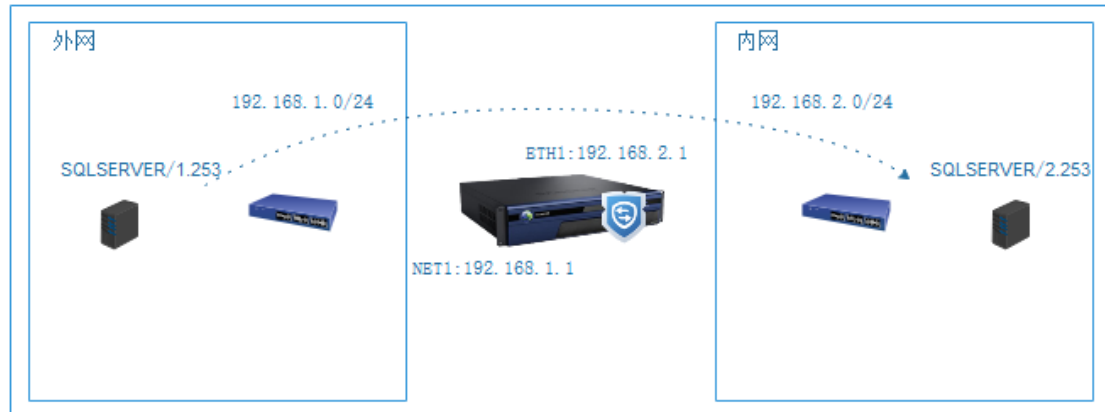
记录ID	时间	用户	访问者IP	目的IP	端口	信息	结果
------	----	----	-------	------	----	----	----

共 0 页

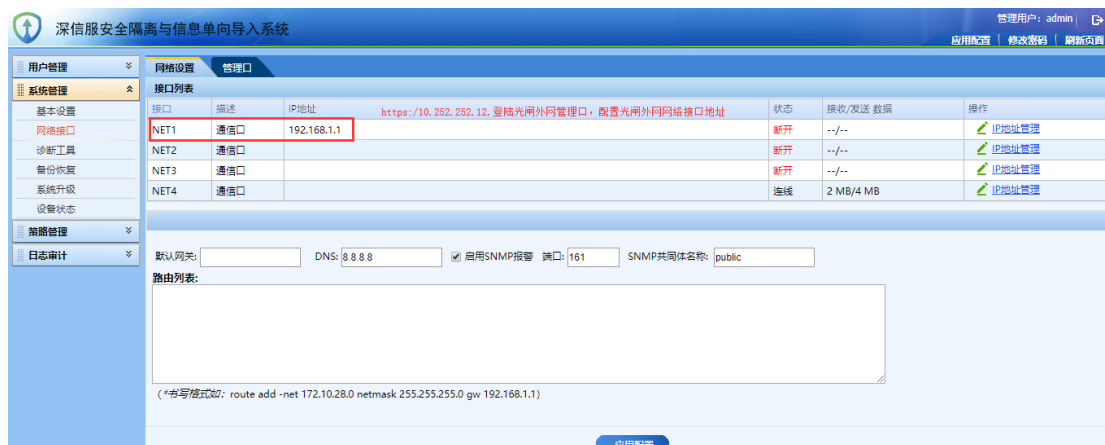
4.2.数据库同步

需求：外网 SQLSERVER 数据库 192.168.1.253 「TDB」表「Table1」中的变更内容需实时同步至内网 SQLSERVER 数据库 192.168.2.253 「TDB」表「Pracs」中。

原理：两端数据库服务器不在同一个子网，也不可能不主动发起同步。光闸需要通过触发器记录外网数据库表中的数据变化，并将变动同步至内网的数据库对应的表中。



第一步：分别登录内外网面板「系统管理 -> 网络接口」配置对应内外网接口地址。



第二步：在外网「策略管理 -> 数据库同步」中添加策略。



第三步：输入策略名称，选择数据库类型，并输入数据库 IP、端口、名称、用户名称、用户密码等信息。



同步用户由于需要创建触发器、系列、表等操作，因此最好给予其 DBA 权限。

建议 DB 两边字符集一致否则容易出现同步数据乱码的情况，如果不是 MySQL, Sybase DB

的同步字符集可以不用填写。如果目的 DB 为 MySQL 或 Sybase DB 填写目标数据库对应字符集。

第四步：点击「编辑」，并在下级界面点击「添加同步表策略」。



内网表名称配置：SqlServer：“dbo.需同步表名”；

Mysql：“数据库名称.需同步表名”；Oracle：“表属主.需同步表名”

第五步：点击确定后返回至「数据库同步」页，勾选设置的策略并启用。



第五步：测试

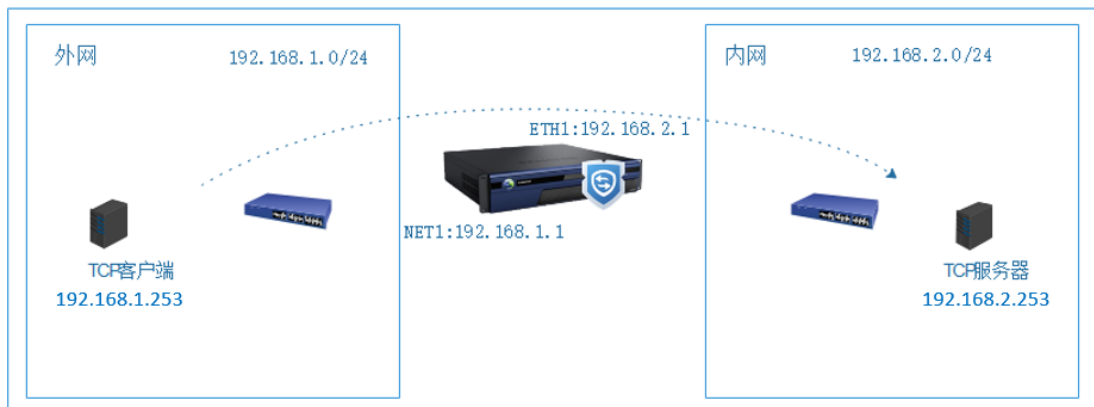
在源数据库插入数据，观察「日志审计 -> 数据库同步日志」中的记录，查看是否能正常同步数据。



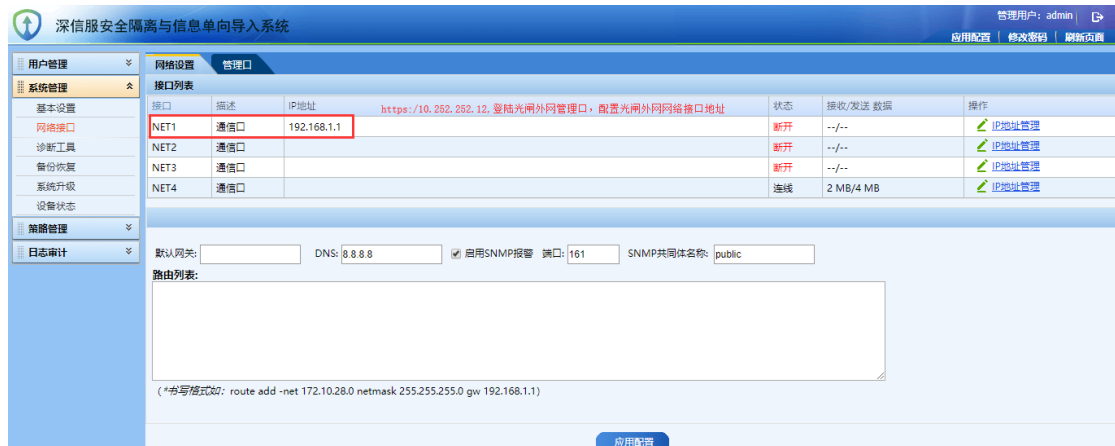
4.3.数据传输

需求：外网服务器需要采用 TCP 方式发送实时数据流到内网服务器中。

原理：单向光闸的外端机、内端机分别与客户的外网服务器、内网服务器建立会话，只单向传输应用层数据，传输层及以下的数据均不是。



第一步：在「系统管理 -> 网络接口」配置对应内外网接口地址。



第二步：在「策略管理 -> 数据传输」添加本地 IP（光闸对外接口地址），本地端口（光闸对外开放端口），目的服务器 IP，目的服务器端口。



第五步：应用策略。



第六步：测试业务是否有数据（实测业务）