伟思信安

安全隔离与信息交换系统

V7.0-3000

用户手册

修订历史记录

版本	日期	AMD	修订者	说明
V1.0	2021 年 3 月 20 日	A	章学宇	初次编写
V1.1	2021 年 4 月 1 日	M	张锦灿	规格审核
V1.2	2021 年 9 月 10 日	M	陈功湖	规格审核

（A-添加，M-修改，D-删除）

目 录

第一章 系统概述

1.1. 系统简介

伟思信安安全隔离与信息交换系统 ViGap7.0-3000（以下简称 ViGap7.0）是珠海伟思有限公司采用先进 GAP 技术独立研制生产的新一代网络安全产品。它专用于国产 AK 环境，放置在可信网络和不可信网络之间，连接两个网络并控制网络间的信息交换。ViGap 通过专用硬件在可信网络与不可信网络间实现物理隔断，可以防止各种基于网络层和操作系统层的攻击，并通过基于硬件设计的反射 GAP 系统，实现在线高速实时的数据传输。

伟思信安安全隔离与信息交换系统采用国产化操作系统--银河麒麟（Kylin）。Kylin 是由国防科技大学研制的开源服务器操作系统，凭借其优越的性能及完善的生态建设连续 10 年位列国产操作系统占有率居首。此操作系统是 863 计划重大攻关科研项目，目标是打破国外操作系统的垄断，研发一套中国自主知识产权的服务器操作系统。

伟思信安安全隔离与信息交换系统 ViGap7.0-3000 具有强大的安全特性，能够满足高度可控环境下的安全数据交换需求，主要特点包括：

采用独特的“2＋1”安全体系架构，通过基于 ASIC 芯片技术设计的专用隔离电子开关系统，实现用户关键网络及服务系统与外界的物理隔断，实现链路层与网络层的彻底断开。

采用高性能和多条流水线设计的 ASIC 芯片为基础建立的全新硬件隔离架构，拥有全线速隔离交换性能，满足大型网络应用所面对大用户量、低延时访问的需求。在核心的 GAP 电子开关隔离芯片上采用了含 TRUE LVDS 功能强大的 APXII 系列 EP2A70 作为 FPGA 设计硬件基片，该芯片具有 500 万门电路以及多路 Giga 位的通道，支持内部高达 1060 个硬件 I/Os 通道，使得电子开关具有高速的数据传输能力和并发处理能力。

充分考虑关键应用对可靠性、可用性的要求，采用负载均衡技术以及基于应用协议连接资源保护的 QOS 服务质量控制技术消除单点故障和网络实现对网络服务的高可靠性及可用性保证。

采用无协议的“GAP Reflective”，GAP 隔离反射技术实现开放网络通讯协议的剥离与重组，有效阻断来自网络层及服务器 OS 层的各类已知/未知攻击，弥补其它安全技术对网络未知攻击的防御盲区。

广泛支持各类通用应用协议（HTTP、FTP、SMTP、DNS、SQL 等），包括支持视频会议、流媒体以及 VPN 等特殊应用代理以及用户定制协议，无需再进行二次开发或单独购买模块。

采用专利技术的应用层安全防御系统，ViGap7.0 产品特别针对广泛应用的 WEB、EMAIL 和 FTP 等服务采用专利技术 WebApplication 保护技术™，实现了全面应用层安全防护，可防止 WEB 溢出漏洞、Unicode 漏洞、Inject 攻击、Cookie 中毒、恶意 JaveScript、ActiveX 控件甚至 CGI 脚本等各类应用层安全风险。

智能化攻击识别与过滤，ViGap7.0 采用先进的应用层协议分析技术智能识别并过滤大量基于应用层协议的攻击行为，ViGap7.0 提供目前市场上丰富的协议分析模块，全面防护各类应用系统安全风险，包括：HTTP、FTP、SMTP、POP3、IMAP、DNS 等数十种协议分析模块。

ViGap7.0 系列产品可以部署在任何需要保障内部网络信息安全免受外部黑客攻击的网络出口连接处。适用于政府机构、金融保险、军队警察、电力电讯及企业网络。

1.2. 名词解释

- 后台管理：是一种管理方式，通过采用串口或 SSH 方式连接到设备的命令行界面，用提供的命令查询运行状态。
- 前台管理：使用 WEB 管理的方式，操作简单易懂，不利于批量操作。
- 可信端：一般位于网闸上层，可以连接涉密网络，用来保存文件或推送文件到涉密网络的服务器。
- 不可信端：一般位于网闸下层，可以连接非涉密网络，用来保存或接收来自非涉密网络的文件。
- 隔离映射：将目的网络的服务器地址和端口映射到源端网络的业务接口上，实现跨网访问资源。

第二章 运行环境

2.1. 硬件运行环境

为保证系统能长期稳定的运行，ViGap7.0 应安装在标准的 19 英寸的机柜里，保证电源有良好的接地措施、防尘措施、保持运行环境的空气通畅和室温稳定。

ViGap7.0 运行环境应满足以下标准：

参数	参数值
输入	200V 4A 50Hz
温度	-10℃～50 ℃
湿度	5%～90%
电源	220V 交流电

第三章 安装部署

3.1. 前置工作

3.1.1. 设备清单检查

在确认安装环境符合要求后，打开设备包装箱并对照定货合同及装箱单仔细核对设备及附件是否齐全，如有疑问或差错请与设备销售商取得联系。

3.1.2. 安装环境要求

必须安装非露天的室内环境中，为保证设备的安全运行，系统要求安装环境具备以下条件。

3.1.3. 温度及湿度要求

为保证设备正常工作并延长其使用寿命，安装环境需维持一定的温度和湿度。若安装环境内长期湿度过高，则容易造成绝缘材料绝缘不良，甚至漏电；还会发生材料

性能变化，金属部件锈蚀等现象。若相对湿度过低绝缘垫片会干缩而引起紧固螺丝松动；在干燥的气候环境下还容易产生静电；从而危及设备上的电路。

温度过高危害更大，因为高温会加速绝缘材料的老化过程，使设备的可靠性大大降低并严重影响其使用寿命。

设备对环境的要求如下：

1) 温度：-10℃～50 ℃

2) 湿度：5%～90%（非凝结状态）

3.1.4. 环境洁净度要求

尘埃对设备的安全运行也是一个重要影响因素，因为空气中的灰尘的累积会造成静电吸附；使金属接插件或金属接点接触不良或电路短路；这一因素不但会影响设备的使用寿命，同时也容易造成通信故障。尤其是在室内相对湿度偏低时，更易产生这种静电吸附。

除尘埃外，设备对空气中所含的腐蚀性酸性气体也有严格的要求，因为这些有害气体在一定湿度环境下会加速对金属部分的腐蚀和某些部件的老化。

因此机房内对安装环境的要求为无爆炸性、导电性、导磁性及腐蚀性气体或尘埃。具体要求请参照的相关要求或规定 。

3.1.5. 静电要求

尽管设备在防静电方面作了大量的设计考虑，采取了多种措施来减少静电积累；但当静电积累超过一定限度时仍会对系统电路乃至整机产生巨大的破坏作用。在与设备连接的通信网中静电感应主要来自两个方面：一是高压输电线路、雷电等外界电场；二是环境建筑及装饰材料、整机结构等。

因此系统内部为防止静电损伤应做到：

1) 设备及地板有良好的接地连接；

2) 环境防尘；

3) 保持适当的环境温度与湿度；

4) 接触电路板时应佩戴防静电手腕套或手套，穿防静电工作服；

5) 拆卸下的电路板应板面朝上放置在具有抗静电作用的工作台上或放入防静电袋中；

6) 观察或转移已拆卸了的电路板时，应只接触电路板的外边缘，避免用手直接触摸电路板上的元器件。

3.1.6. 雷电/电磁要求

设备的设计大量考虑了环境电磁及雷电对其的影响，但是在雷击强度超过一定范围时仍然有可能对安全网关造成损害；而使用过程中可能的电磁干扰源，无论是来自设备或应用系统外部，还是来自内部；都是以电容耦合、电感耦合、电磁波辐射、公共阻抗包括接地系统耦合的传导方式等对设备产生影响。为达到更好的防雷和抗干扰效果的要求，用户应做到：

1) 对供电系统采取有效的防电网干扰措施；

2) 设备安装环境最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些；

3) 远离强功率无线电发射台、雷达发射台、高频大电流设备等；

4) 必要时采取电磁屏蔽的方法；

5) 保证机箱的保护接地用保护地线与大地保持良好接触；

6) 保证电源插座的接地点与大地良好接触；

7) 为增强电源的防雷击效果，可以在电源的输入端安装电源避雷器，这样可大大增强电源的抗雷击能力。

3.1.7. 安装台面检查

对设备进行安装前要保证以下安装环境的再确认：

1) 确认设备的入风口及通风口处留有足够的空间，以利于设备散热；

2) 确认安装环境自身有良好的通风散热系统；

3) 确认安装环境足够牢固，能够支撑要安装的设备及其安装附件的重量；

4) 确认安装环境有良好接地连接。

【注】：与墙壁的距离应不小于 15 厘米。

3.1.8. 安全注意事项

基于安装设备的广泛应用及其在数据通信网络中担当的重要作用，再次强调：手册中的如下标志，在阅读过程中请多加注意：

以下安全建议对设备的安装和使用过程中要特别引起重视：

1) 请将设备放置在远离潮湿或远离热源的地方；

2) 请确认设备已经正确接地；

3) 请在安装维护过程中佩戴防静电手腕（套），并确保防静电手腕（套）与皮肤良好接触；

4) 注意不要将手指或其它物件伸入设备的散热风扇中；

5) 建议用户使用 UPS（Uninterrupted Power Supply 不间断电源）系统。

【注】：表明该项操作不正确可能给操作者的人身安全带来极大的危险，操作者必须严格遵守正确的操作规程。

【注】：表示在安装使用中需要注意的操作，该操作不正确可能影响设备的正常使用。

3.1.9. 安装工具准备

包装中不附带安装工具、仪表及相关设备，请准备相应的工具：

6) 十字镙丝刀

7) 一字镙丝刀

8) 防静电手腕套

9) 防静电袋

10) 电源线

11) 可选电缆

3.2. 设备上架

根据用户安装环境，可以安装到两种环境中：

1) 直接放置在稳定的水平平台上；

2) 与其它网络设备一起安装在标准机架上。

3.2.1. 安装到水平台面

这是一种最简便经济的安装方式，但安装操作过程中要注意以下事项：

1) 保证水平平台的牢固性和稳定性，并保证有良好的接地连接；

2) 设备的通风口与形成通风障碍的障碍物之间要留有至少 15 厘米的通风通道；

3) 设备的上表面不要堆放重物。

3.2.2. 安装到标准机架

外形尺寸设计是符合标准 19 英寸机架（以下称机架）上架装配要求的，因此它非常容易安装到机架上。

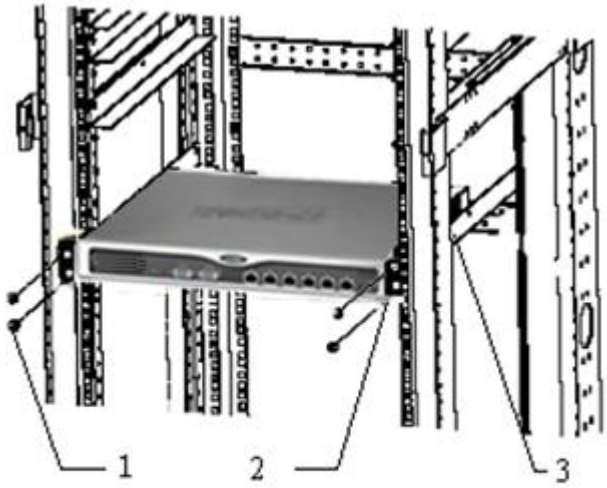
以下安装设备到机架的具体说明：

1) 检查并确认机架的安装是否合格并符合其安装标准；需要注意检查机架是否稳固并且有良好的接地连接；

2) 将挂耳用螺钉安装到设备靠前面板的两侧；

3) 确定设备要安装的位置，将设备安放到预定位置的托盘上（建议由用户提供与该机架配套的设备托盘），并注意设备与机架之间的距离要合适；

4) 用满足机柜安装尺寸要求的盘头螺钉将设备通过固定挂耳固定在机柜上，请保证位置水平并牢固。机柜和设备如图所示：



说明：

1. 镙钉 2. 挂耳 3. 导轨

3.3. 系统部署检查

1) 连接电源线到 ViGap7.0 后面的电源插口，然后插入另一端的电源插头到 220V 电插座；

2) 开启 ViGap7.0 后面的电源开关和前面设备开关；

3) 查看设备液晶屏是否正确显示；

4) 连接网线的一端到 ViGap7.0 的可信端接口，连接另一端到内网交换机的网口；

5) 连接网线的一端到 ViGap7.0 的非可信端接口，连接另一端到外网设备的网口，例如外网交换机、路由器、防火墙等；

6) 用内网管理主机登陆 ViGap7.0 并进行适当的配置；

7) 测试网络的连通性以及是否可以正常访问服务器，例如 ping。

第四章 管理操作指南

4.1. 登录管理

4.1.1. 准备工作

- 接通电源，液晶屏显示序列号后表示启动完毕；
- 选用一带 Windows 系统 PC 作为管理主机；
- 使用交叉线，管理网闸。

4.1.2. 管理方式

- 串口命令行管理 - 常用于恢复工作
- Web 页面管理 ---- 常用于正常管理
- SSH 远程管理 ---- 常用于管理调试

4.1.3. Web 页面管理

- ViGap7.0 上下层板通过上层板管理口进入 Web 页面，进行统一管理。
- 上层板（可信端）登陆入口：在管理主机输入

  https://192.168.0.254:10000，按证书提示点击“确定”；
- 管理员账号：在“用户名”一栏输入用户名 admin，在“密码”一栏输入其对应默认口令“admin*pwd”（管理人员应及时更改系统初始缺省管理员的用户名和口令），在验证栏输入验证码。点击“登录”。
- 下层板（不可信端）系统由可信端页面统一管理

第五章 运维操作

5.1. 常见故障

5.1.1. CPU 高

设备出现 CPU 高通常有两种情况：

- 流量超过设备处理能力导致；
- 某些功能模块消耗 CPU 过高。

解决方法：关闭不必要开启的部分功能模块，查看系统流量是否超过 CPU 处理能力。

5.1.2. 内存高

设备出现内存高主要可能是开启功能模块、大量的连接导致的内存消耗。

解决方法：检查系统当前状态，判断是否是因正常的功能开启或会话连接数量导致的内存消耗。

5.1.3. 网络异常

出现网络慢、丢包、业务不通等现象，原因很多，需要根据现象逐个排除，例如：

- 流量超过设备处理能力导致；
- 设备配置导致（如用户主机被限速）；
- 模块不正常导致；
- 接口协商不正常导致。

解决方法：

1) 判断是否个别用户异常还是所有用户都有问题，如果是所有都有异常，需要判断异常产生的位置；个别用户网络异常，需要考虑是否由 BT 阻断、限速等配置引起。如：IPMAC 绑定、连接数限制等；

2) 观察设备相关接口状态，判断用户流量，以及是否由接口硬件相关问题导致网络异常。

5.1.4. SYLOG 日志失效

在 SYSLOG 服务器上看不到对应模块日志。
解决方法：

1) 是否正确配置 SYLOG 服务器的地址和端口号；

2) 是否指定模块的日志类别和等级到 SYSLOG Server。

5.1.5. 本地 FTP 服务器登入异常

出现无法连接可信端/不可信端的本地 FTP 服务
解决方法：

1) 确认客户端和系统业务口的网络通讯正常；

2) 登入的 FTP 账号、密码输入无误，端口号为固定的 21；

3) 确认系统是否勾选了“启用强制访问控制”，勾选状态下，需要在系统浏览器进行用户认证后，方可连接。上传的文件须先进行打标识的操作；

4) FTP 客户端版本过低，建议采用 FileZilla 3.11.0.1 以上版本。

5.1.6. 远程数据资源连接异常

针对远程同步数据资源连接异常的问题，可通过日志审计员账号登录系统，在“文件同步状态日志”模块进行查询。

5.2. 运维指南

5.2.1. 日常运维

1) 连接数

如当前的连接数达到或接近系统最大值，将导致新会话不能及时建立连接，此时已经建立连接的通讯虽不会造成影响；但仅当现有的连接拆除后，释放出来的资源才可供新建连接使用。

2) 维护建议

当前连接数正常使用至 85％时，需要考虑设备容量限制并及时升级，以避免因设备容量不足影响业务拓展。

3) CPU 检查

正常工作状态下设备 CPU 使用率应保持在 10%以下，如出现 CPU 利用率过高情况需给予足够重视，应检查连接数使用情况和各类告警信息，并检查网络中是否存在攻击流量。通常情况下 CPU 利用率过高往往与攻击有关，可通过正确设置系统参数、攻击防护的对应选项进行防范。

4) 内存检查

设备对内存的使用把握得十分准确，正常情况下，内存的使用率应基本保持稳定，不会出现较大的浮动。如果出现内存使用率过高（>90%）时，可以查看连接数情况，或通过实时监控功能检查网络中是否存在异常流量和攻击流量。

5) 高峰期资源检查

在业务使用高峰时段检查设备关键资源（如：cpu、连接数、内存和接口流量）等使用情况，建立网络中业务流量对设备资源使用的基准指标，为今后确认网络是否处于正常运行状态提供参照依据。当连接数数量超过平常基准指标 20％时，需通过实时监控检查当前网络是否存在异常流量。当 cpu 占用超过平常基准指标 20％时，需查看异常流量、定位异常主机、检查策略是否优化。

5.2.2. 应急处理

当网络出现故障时，应迅速检查设备状态并判断是否存在攻击流量，定位故障是否与设备有关。如果故障与设备有关，可首先检查设备的安全策略、访问控制策略、路由等是否按照实际使用需求配置，检验策略配置是否存在问题。一旦定位设备故障，可通过命令进行双机切换，单机环境下发生故障时利用备份的交换机/路由器配置，快速旁路网闸。在故障明确定位前不要关闭网闸。

1) 检查设备运行状态

网络出现故障时，应快速判断设备运行状态，通过管理器登陆到设备上，快速查看 CPU、内存、连接数以及相应信息，初步排除硬件故障并判断是否存在攻击行为。

2) 跟踪设备对数据包处理情况

如果出现部分网络无法正常访问，顺序检查接口状态、路由和策略配置是否有误，

在确认上述配置无误后，通过 tcpdump 命令检查设备对特定网段数据报处理情况。

3) 检查是否存在攻击流量

通过实时监控确认是否有异常流量，同时在上行交换机中通过端口镜像捕获进出网络的数据包，据此确认异常流量和攻击类型，并在选项设置、入侵防护等项目中启用对应防护措施来屏蔽攻击流量。

4) 检查 HA 工作状态

检查 HA 工作状态，进一步确认引起切换的原因，引起 HA 切换原因通常为链路故障，交换机端口故障，设备断电或重启。设备运行时务请不要断开 HA 心跳线缆。

5) 发生故障时处理方法

如果出现以下情况可初步判断网闸硬件或系统存在故障：无法使用 console 口登陆设备，设备反复启动、无法建立 ARP 表、接口状态始终为 Down、无法进行配置调整等现象。为快速恢复业务，可通过调整上下行设备路由指向，快速将设备旁路，同时联系供应商进行故障诊断。

5.3. 注意事项

故障处理后的总结与改进是进一步巩固网络可靠性的必要环节，有效的总结能够避免很多网络故障再次发生。

1) 在故障解决后，需要进一步总结故障产生原因，并确认该故障已经得到修复，避免故障重复发生；

2) 条件容许的情况下，构建设备业务测试环境，对所有需要调整的配置参数在上线前进行测试评估，避免因配置调整带来新的故障隐患；

3) 分析网络可能存在的薄弱环节和潜在隐患,通过技术论证和测试验证来修复隐患。

第六章 功能介绍

6.1. 初始化配置

1) 伟思信安隔离与信息交换系统 ViGap7.0-3000 分为可信端和不可信端，分别连接

到内网和外网；

2) ViGap7.0 采用 B/S 模式管理，通过可信端管理口分别对 ViGap7.0 两端进行管理。可信端管理口 IP 地址为 192.168.0.254/24，不可信端默认业务口 IP 地址为 192.168.10.254/24；

3) 管理可信端和不可信端机时，选择一台安装有浏览器的客户机，与可信端管理口相连，修改客户机 IP 地址，使其与可信端管理接口（处于同一个网段，可信端管理口初始值为 192.168.0.254/24）；在浏览器地址栏输入：https://192.168.0.254:10000 即出现可信端管理系统登陆界面；

4) 在“用户名”一栏输入用户名 admin，在“密码”一栏输入其对应默认口令“admin*pwd”（管理人员应及时更改系统初始缺省管理员的用户名和口令），在验证栏输入验证码。进入系统可分别对可信端和不可信端进行配置，配置内容基本一致，配置保存后应用会自动生效到可信端和不可信端（部分配置修改后需要重启系统）。管理系统分为：设备管理、高可用性、策略配置、工业控制四大模块。

6.2. 系统状态

6.2.1. 系统状态

登录系统成功后，在主界面显示系统状态页面，这个页面显示 ViGap7.0 可信端和不可信端目前的状态。

实时更新显示 ViGap7.0 两端的系统状态、设备信息、网络吞吐量。

- 系统状态：CPU 使用率、内存使用率、磁盘使用率、并发数。

- 设备信息：设备型号、系统版本、文件交换模块版本、数据库交换模块版本、设备工作模式、版本许可、授权天数、运行时长；
- 网络吞吐量：上行和下行流量；可统计总数和按接口统计。

6.2.2. 统计分析

在统计分析页面显示 ViGap7.0 的可信端和不可信端使用率的曲线图,便于查看和分析，显示系统的 CPU 使用率、内存使用率、磁盘使用率的动态变化。

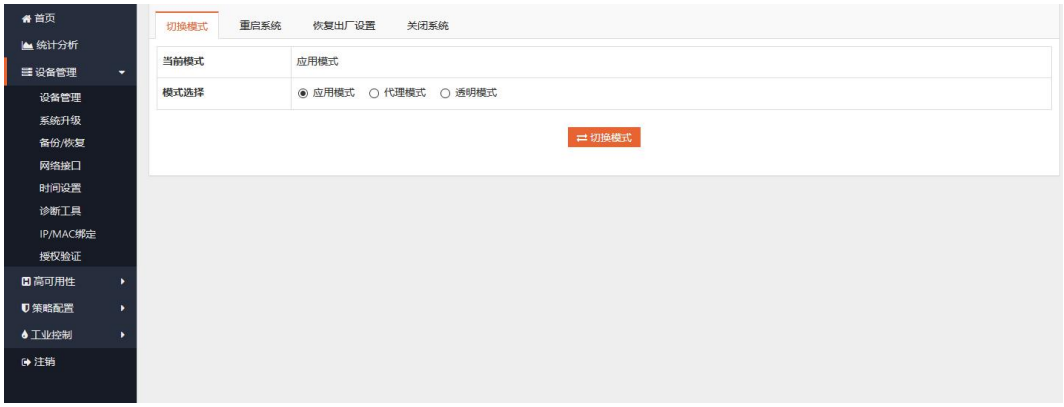
6.3. 设备管理

6.3.1. 设备管理

设备管理页面提供了模式切换、系统重启和关闭、恢复出厂设置的功能，方便对系统进行控制。

6.3.1.1. 模式切换

可根据需要选择对应的模式。



点击“设备管理”中的“切换模式”模块，可以查看系统当前模式。根据需要点击模式前面的单选框，点击“切换模式”，页面提示完成后切换成功。

透明模式：选择透明模式需要配置桥接口。勾选“透明模式”。勾选需要桥接的物理接口（管理口可桥接），填写桥接口 IP 和掩码，选择是否启用 STP 生成树。配置完成后，点击“切换模式”，页面提示完成后切换成功。

- 模式说明：应用模式下，系统提供高性能和高稳定性；代理模式下，系统提供高安全性；透明模式主要提升系统网络传输能力。默认模式下，系统设置为“应用模式”。
- 透明模式参数配置：可信端和不可信端的接口至少勾选一个，页面提供了“全选”和“重置”的便捷操作，IP 地址必填。启用 STP 生成树可以用于在局域网中消除环路，默认勾选。

注： 1、代理模式切换需要花费 20 秒左右。

2、切换模式成功后，刷新页面，页面数据会刷新。

6.3.1.2. 重启系统

点击“设备管理”>“重启系统”模块，点击下方按钮，系统重启。重启系统一般为 30 秒左右。

6.3.1.3. 恢复出厂设置

点击“设备管理”中的“恢复出厂设置”模块，点击下方按钮，系统恢复出厂设置。

注：恢复出厂设置后：

1、T1（管理口）和 NT1（第一个业务口）IP 会还原为用户自定义的默认 IP(具体看网络配置-网口初始化)

2、所有日记被清空，备份在服务器上的配置文件和信息将被清空

3、所有已配置项将被重置

4、设备自动重启

6.3.1.4. 关闭系统

点击“设备管理”中的“恢复出厂设置”模块，点击下方按钮，系统关闭。

6.3.1.5. 注销登录

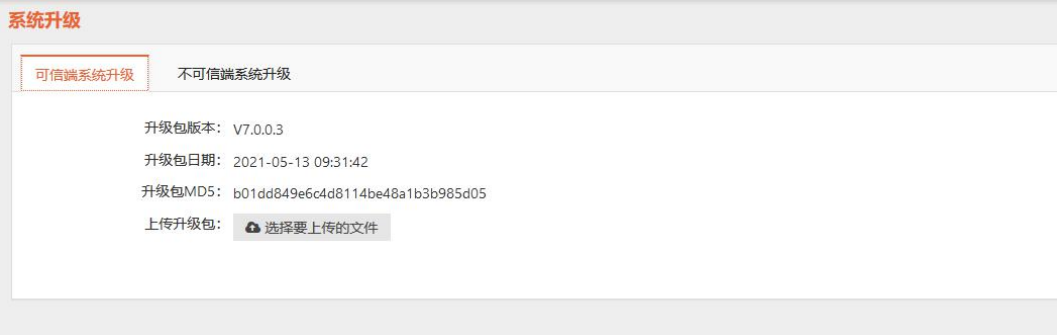
在系统侧边栏最下方，点击“注销”，系统退出当前账号，跳转至登录页面。

6.3.2. 系统升级

在系统升级页面，可以对系统固件和程序升级到指定版本。

在“设备管理”>“系统升级”，进入升级页面。把升级包下载到本地，选择可信

端或不可信端，点击“选择要上传的文件”按钮，上传升级包，等到系统提示升级成功后，重启系统，即可升级成功。



注：

升级失败则提示相关信息，升级成功需要重启才生效。

6.3.3. 备份/恢复

在 ViGap7.0 中备份与恢复配置文件，配置文件为加密的文件。

6.3.3.1. 备份配置

备份配置可把两端机上的配置下载到本地或者服务器，并在下方列表查看备份的配置信息。

在“设备管理”>“备份/恢复”，选择“备份配置”标签，进入备份配置页面。

- 位置：选择备份位置，可选项：全部、可信端、不可信端，默认选择备份位置是“全部”；
- 备份区域：选择备份区域，可选项：全部、数据资源、数据同步策略、策略配置（数据库除外）、系统配置。默认选择备份区域是“全部”；
- 选择目标位置：可选项：备份到本地、备份到服务器、以上两者。

点击“确认”，即可把系统现有配置下载到本机

6.3.3.2. 恢复配置

恢复配置可把本地或服务器上已备份的配置上传至 ViGap7.0，将系统恢复为备份的配置。

在“设备管理”>“备份/恢复”，选择“恢复配置”标签，进入恢复配置页面。点击“选择要上传的文件”可把本地备份恢复到系统配置

点击下方服务器备份列表中备份文件右侧的“恢复”可把服务器备份恢复到系统配置

- 位置：选择备份位置，可选项：全部、可信端、不可信端，默认选择备份位置是“全部”；
- 恢复区域：选择恢复区域，可选项：全部、数据资源、数据同步策略、策略配置（数据库除外）、系统配置。默认选择备份区域是“全部”；

恢复完配置后，需要重启才能生效配置。

6.3.4. 网络接口

在网络接口页面，可对两端的接口信息和网络信息进行查看和配置。

6.3.4.1. 接口初始化

首次使用或要自定义默认管理 IP 时，可在“设备管理”>“网络接口”点击“网口初始化”，对系统接口位置和名称进行重定义；根据接口的实际位置，把物理口列排列为正确顺序，再自定义默认值 IP（一般配置管理口 IP）；点击“确认”保存为初始化配置，在系统恢复出厂设置时，该配置会生效。

- 接口：显示接口的名称；
- 物理口：显示系统真实的物理接口名称，可通过拖拽调整位置顺序；
- 类型：接口类型有“通道口”“管理口”“业务口”；其中不可信端只有“通道口”和“业务口”。“通道口”用于配置可信和不可信端通讯，不可配置 IP；“管理口”为可信端管理入口，仅可配置一个；“业务口”是用于业务传输的接口。
- IP 地址：配置初始值 IP 地址；
- Link 状态：网线连接状态判断；有助于判断设备该口是否接入网络；Link 状态对应的是“物理口”列的接口状态；
- 同步为当前配置：勾选该项后，网口初始化的配置会同步到当前的配置，需要重启后生效。

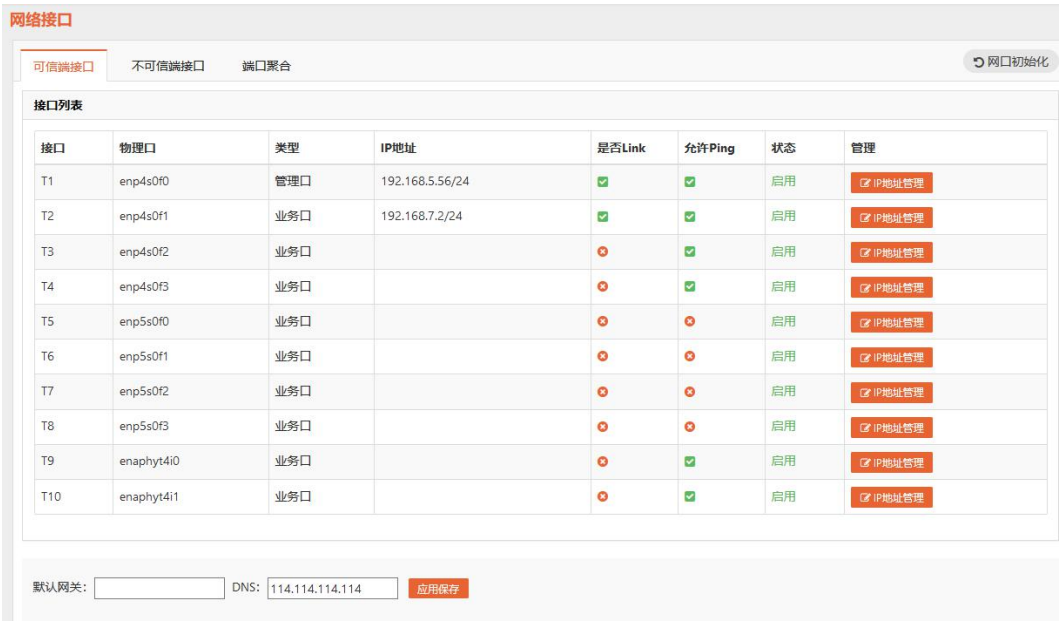
注：

1、若处于配置状态时有网线连接状态变动。需重复点击 LINK 状态旁边的‘刷新’按钮更新；

2、可信端和不可信端的网口初始化配置需要恢复出厂后生效；

6.3.4.2. 网络接口查看

进入“设备管理”>“网络接口”，可查看当前网络接口的信息，并进行接口 IP、网关和路由信息的配置。



- IP 地址管理：新增接口 IP 地址、修改接口常规配置，支持接口多个 IP 配置；支持 IPV4 和 IPV6 类型地址添加；
- 默认网关：填写接口默认网关，点击“应用保存”按钮保存配置；
- DNS：填写接口 DNS，点击“应用保存”按钮保存配置；
- 添加路由：点击添加路由。可添加多个。添加路由可选择目的网络、接口、网关，并在下方列表查看和启停。

6.3.4.3. IP 地址管理

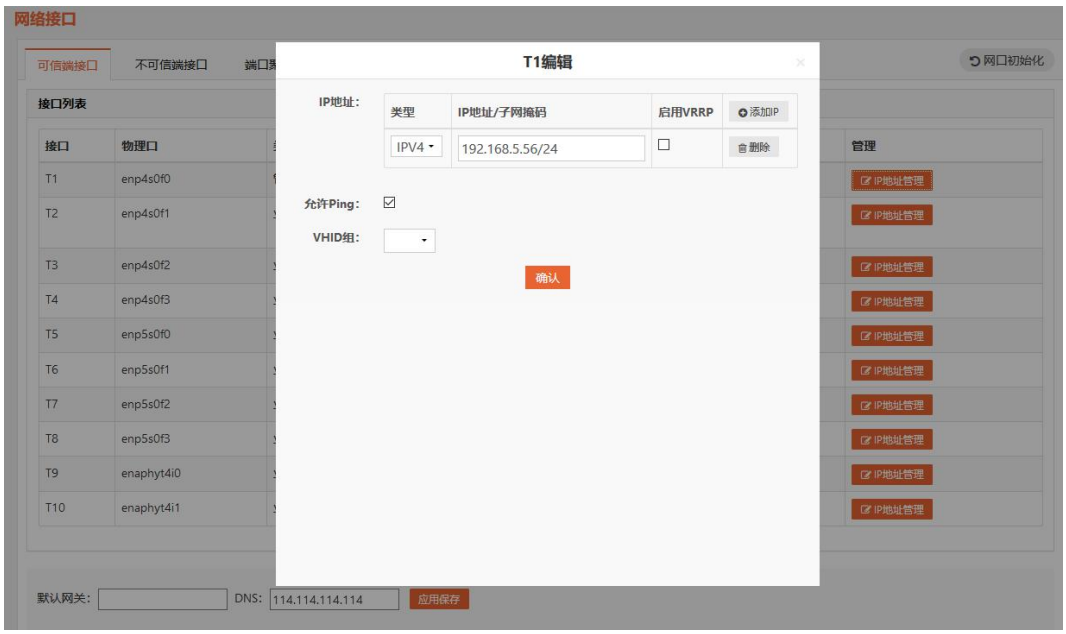
进入“设备管理”>“网络接口”页面，选择要修改的网络接口，点击“IP 地址管理”按钮，进行 IP 的添加、修改、删除；

点击“添加 IP”，为该接口添加一个新的 IP 地址，选择 IP 类型为“IPV4”或“IPV6”，地址格式为“xxx.xxx.xxx.xxx/24”；默认不勾选“启用 VRRP”（VRRP 用于多机热备功能）

点击“清除 IP”，清除接口的所选 IP 信息；

点击输入框，可编辑接口修改当前的 IP 信息；

点击“保存”按钮生效。



- IP 地址：新增、修改和删除 IP 地址。
- 类型：可选项：IPV4、IPV6；
- 启用 VRRP：启用或禁用 VRRP，用于双机热备的虚拟 IP 管理。默认不勾选；
- 允许 Ping：允许或禁止接口可 Ping；默认勾选；
- VHID 组：选择接口所属 VHID 组，和配置多机热备有关，可选值为 1~255，默认空。

注：不同接口不可配同个网段的 IP 地址。

不可信端配置同理。

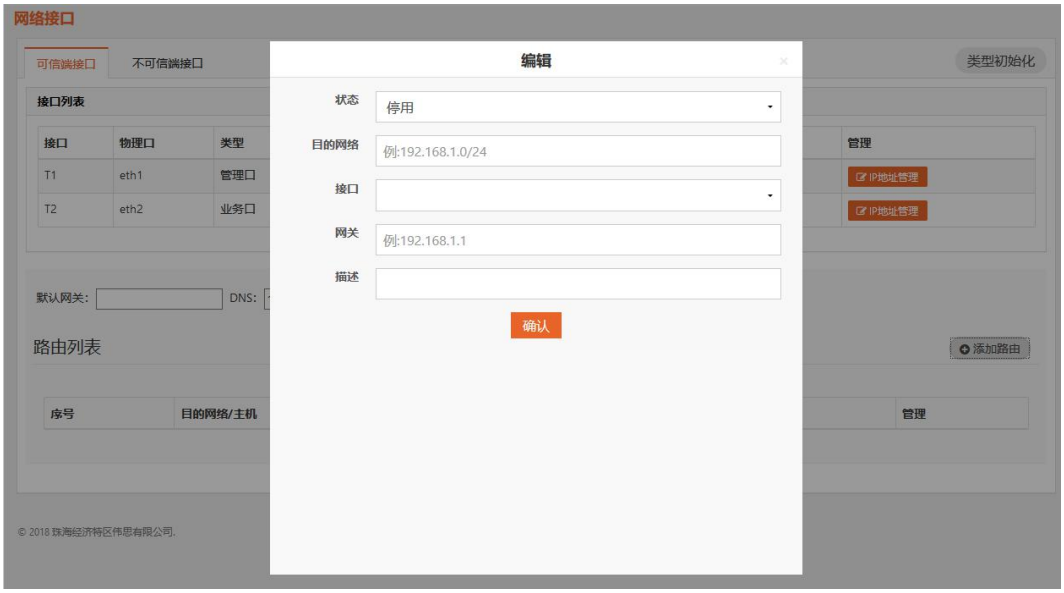
6.3.4.4. 路由管理

在静态路由页面可以对路由进行管理，路由用于访问默认网关无法到达的网络，在两个相邻的不同子网的网络之间经常需要设置路由使两个网络之间能进行通讯。

进入“设备管理”>“网络接口”页面，点击“添加路由”按钮，进行路由配置。

配置路由的目的网络（格式为“xxx.xxx.xxx.xxx/24”）、接口、网关，并可选描述。点击“确认按钮”保存路由配置，并可在页面下方查看路由列表。

配置完成的路由可在路由列表查看，并做“编辑”和“删除”操作。



- 状态：启用或停用路由，默认选中“停用”；
- 目的网络：填写所对应的 IP 地址段和对应的子网掩码。
- 接口：在下拉菜单选择对应的接口。
- 网关：填写所对应的网关 IP 地址。
- 描述：描述不限制，可以填写，也可以不填写。

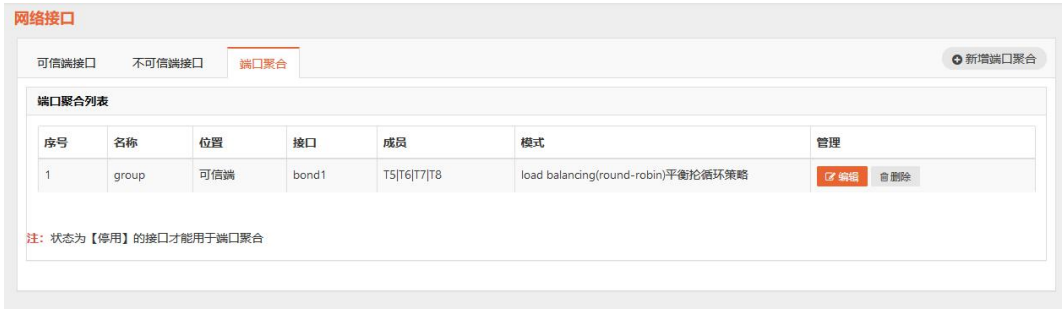
6.3.4.5. 端口聚合

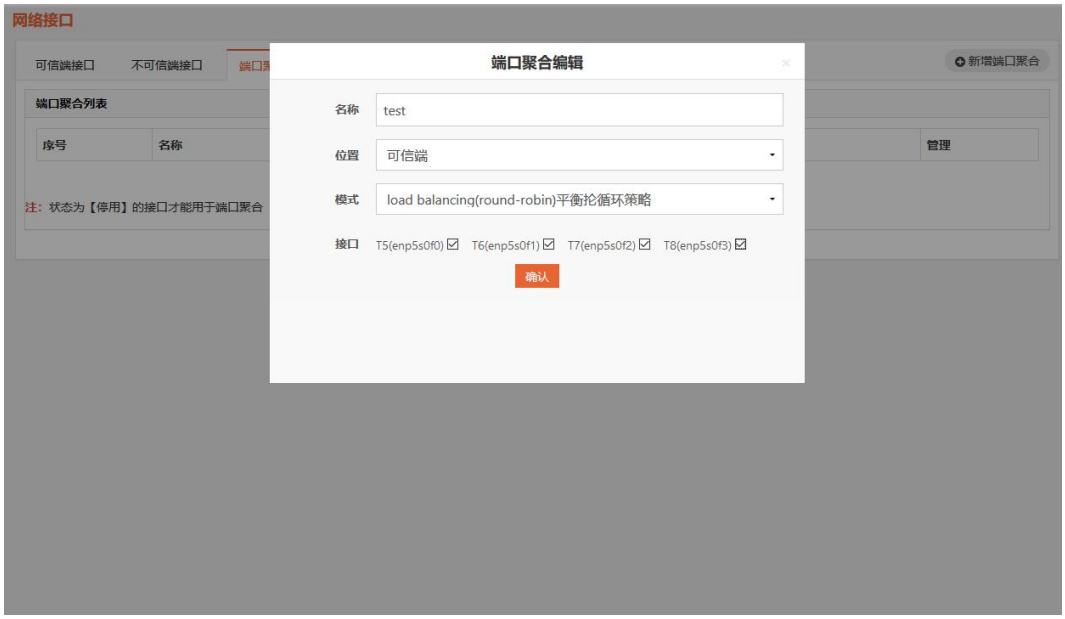
当系统需要与交换机连接提供集中访问，可用端口聚合功能做多网卡的聚合，以实现负荷在各成员端口的分担，即路径冗余，提供更高的连接可靠性。

进入“设备管理”>“网络接口”页面，点击“端口聚合”模块，进行配置。

点击右上方“新增端口聚合”按钮，填写聚合名称，选择可信端或不可信端要聚合的模式和接口，接口可多选；点击“保存”生效。

配置完成的聚合端口可在端口聚合列表查看，并做“编辑”和“删除”操作。





- 名称：自定义端口聚合的名称；
- 位置：可选位置为“可信端”或“不可信端”。
- 模式：提供七种常用的聚合模式可选，默认选中“load-balancing”。
- 接口：选中的为聚合成员接口，至少选中一个。

注：状态为【停用】的接口才能用于端口聚合。

6.3.5. 时间设置

在时间设置页面可以对系统时间进行调整，支持手动设置、同步管理机设置、时间服务器同步三种设置方式。在时间修改后，日志与审计显示时间，也将按照修改后的时间显示。

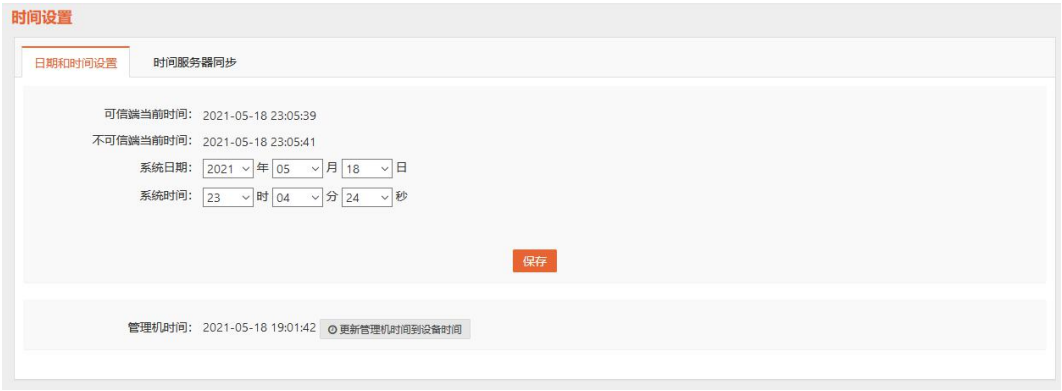
进入“设备管理”>“日期和时间设置”页面，系统会展示系统可信端和不可信端的当前日期和时间，可信和不可信时间独立管理，手动设置和管理机同步支持两端同时同步，时间服务器同步支持两端分开同步。

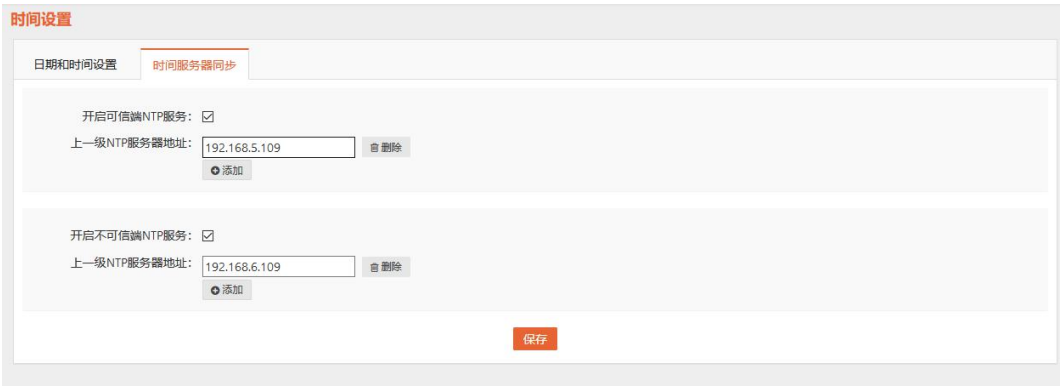
手动设置：在日期时间下拉框可手动选择时间，点击“保存”按钮可将时间同步

为和手动设置一致。

管理机同步：在时间展示下方可查看管理机（即当前操作系统的 PC 端）当前时间，点击“更新管理机时间到设备时间”按钮可将系统时间同步到和管理机一致。

时间服务器同步：点击“时间服务器同步”标签可跳转到时间服务器配置模块。勾选可信端或不可信端开启系统 NTP 服务，并填写上级的 NTP 时间服务器地址，点击“保存”按钮，提示同步成功后，刷新页面，时间即同步至 NTP 服务器一致。





- 可信端当前时间：显示系统可信端的当前时间；
- 不可信端当前时间：显示系统不可信端的当前时间；
- 系统日期/系统时间;手动设置系统两端当前时间，点击“保存”按钮；
- 管理机时间：查看管理机当前时间，点击“更新管理机时间到设备时间”按钮从管理机更新时间到系统；
- 开启可信端 NTP 服务：勾选开启 NTP 服务，从 NTP 服务器更新时间到系统。存在上一级 NTP 服务器时以上级服务器作为 NTP 服务器，不存在上一级 NTP 服务器地址则以本身服务器作为 NTP 服务器；
- 上一级 NTP 服务器地址：点击“添加”按钮添加上级 NTP 服务器地址，点击“删除”按钮删除 NTP 服务器 IP。

不可信端 NTP 服务配置同可信端一致。

6.3.6. 诊断工具

ViGap7.0 提供了一些常用的诊断工具便于用户定位网络故障。

6.3.6.1. Ping 工具

进入“设备管理”>“诊断工具”页面，点击“Ping 工具”标签，通过 Ping 目标主机并根据返回的结果，来判断可信端网络或不可信网络的主机是否可达。

- 位置：默认为可信端，可在下拉列菜单选择可信端或不可信端；
- 目标主机：填写目标主机 IP；
- 次数：默认为 3 次，可在下拉列菜单选择 Ping 1 至 5 次；

点击“确认”按钮进行测试；

6.3.6.2. Traceroute

进入“设备管理”>“诊断工具”页面，点击“Traceroute 工具”标签，通过路由跟踪，返回系统到达目的 IP 途径的路由数量。

- 位置：默认为可信端，可在下拉列菜单选择可信端或不可信端；
- 目标主机：填写目标主机 IP；
- 最大跳数：默认为 3 次，可在下拉列菜单选择 Ping 1 至 5 次；
- 确认：点击“确认”按钮进行测试；

6.3.6.3. TCP 服务检查

进入“设备管理”>“诊断工具”页面，点击“TCP 服务检查”标签，该工具可用于检测服务器的地址和端口，通过发送和返回 TCP 报文，返回一个是否成功的结果。

- 位置：默认为可信端，可在下拉列菜单选择可信端或不可信端；
- 目标主机：填写目标主机 IP；
- 端口：填写目标主机 TCP 端口；
- 确定：点击确定进行 TCP 通讯；

6.3.6.4. 抓包工具

进入“设备管理”>“诊断工具”页面，点击“抓包工具”标签，选择要抓包的位置、协议类型和接口（只可选择启用中切 Link 的接口），点击“启动抓包”即可开始抓取接口数据包，可以手动停止抓包，若不停止，系统将在五分钟后自动停止抓包，此时系统会生成一个 pcap 文件可供下载。

- 位置：默认为可信端，可在下拉列菜单选择可信端或不可信端；
- 接口：选择主机要进行抓包的接口，可在下拉列菜单选择其他已有接口；
- 协议类型：默认为 all，可在下拉列菜单选择 ip、arp、tcp、udp；
- 启动抓包：点击启动进行对应协议的抓包；
- 停止抓包下载数据：点击停止抓包并下载数据文件；

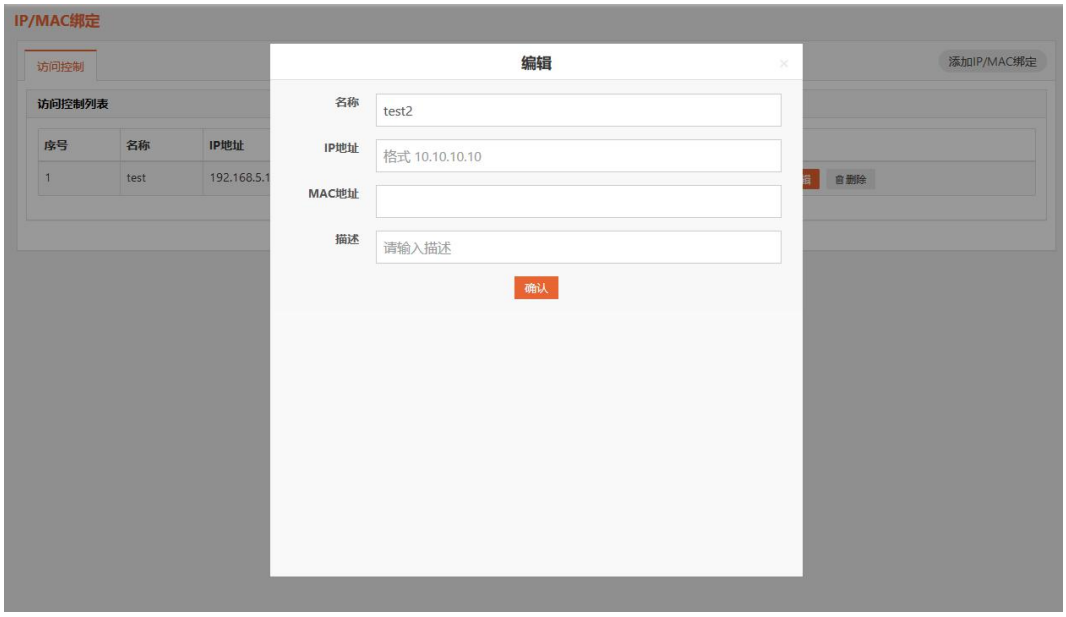
6.3.7. IP/MAC 绑定

进入“设备管理”>“IP/MAC 绑定”页面，可为系统添加 IP/MAC 绑定，点击“添加”，新增一个 IP 和 MAC 匹配对，填写 IP 地址和 MAC 地址，并为该对添加名称和相关描述，点击“保存”生效。

绑定过的 IP 地址可以在访问控制列表查看，系统会对绑定的 IP 进行匹配，只有与 IP 对应 MAC 地址的主机访问，才能打开系统页面。

点击“删除”，清除该 IP 和 MAC 匹配对；

点击编辑，可编辑修改；



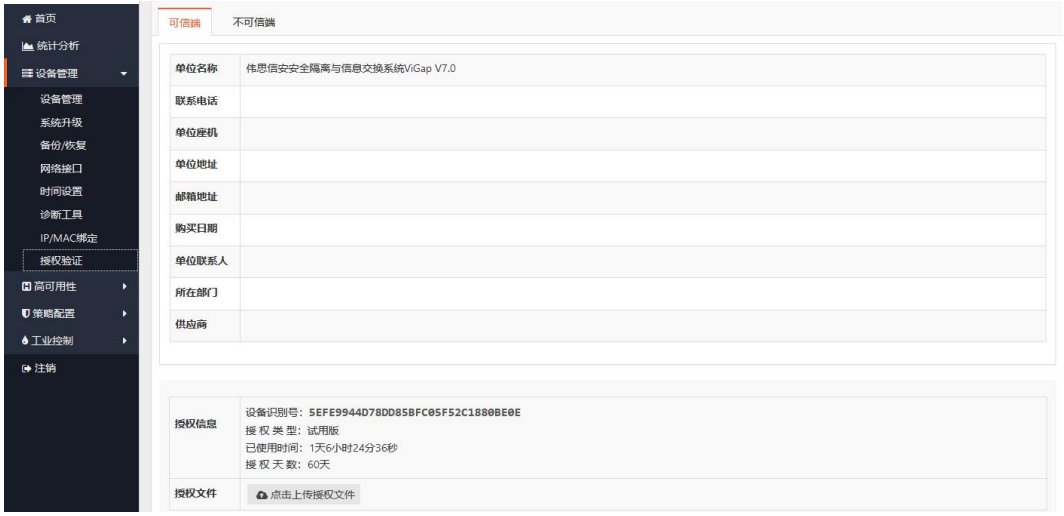
- 名称：可以是字母、数字、下划线、中文任意组合，最大长度 32 个字符；
- IP 地址：绑定主机的 IP 地址，格式为“xxx.xxx.xxx.xxx”；
- MAC 地址：绑定主机的 MAC 地址，格式为“xx.xx.xx.xx.xx.xx”；
- 描述：描述不限制，可以填写，也可以不填写。

6.3.8. 授权验证

ViGap V7.0 设备具有唯一识别号，在系统首页或授权验证页面可进行两端授权相关信息的查看，系统的授权版本分为试用版和正式版。

试用版有限制使用天数，当系统试用期剩余天数不足七天时，打开页面会有弹出框提示，当系统为试用版且过期时，页面登录后会停留在授权验证页面，无法正常使用功能，请联系相关人员进行授权和注册。

进入“设备管理”>“授权验证”页面，系统用于试用版的注册文件命名为“tmp.dat”，正式版的注册文件命名为“license.dat”，可在系统“点击上传授权文件”按钮，上传注册文件，注册后，无需重启，刷新页面即可更新注册状态。



6.4. 高可用性

6.4.1. 多机热备

配置多机热备的目的是为了当主机出现故障，不能正常工作时，其余备机会根据优先级主动接管主机服务，以保证数据链路不会中断。主机修复正常后，又会接管任务。配置 ViGap7.0 的多机热备，我们需要两套以上单独的、完全相同的 ViGap7.0 设备。

进入“高可用性”〉“多机热备”页面，勾选启用多机热备，为热备池添加一台以上的设备：填写设备 IP（主机之间需要网络可达）并选择该设备的优先级，优先级高的为主机。点击“保存”按钮。配置生效，系统会自主同步，将当前双机配置同步到热备池内的其他主机，优先级高的为主机。

多个设备之间，通过优先级来判断当前哪台设备作为主机。在系统配置了虚拟 IP 后，多台设备可统一对外提供一个 IP 作为业务配置接口。详见下一章节。

- 是否启用多机热备：勾选之后启用；

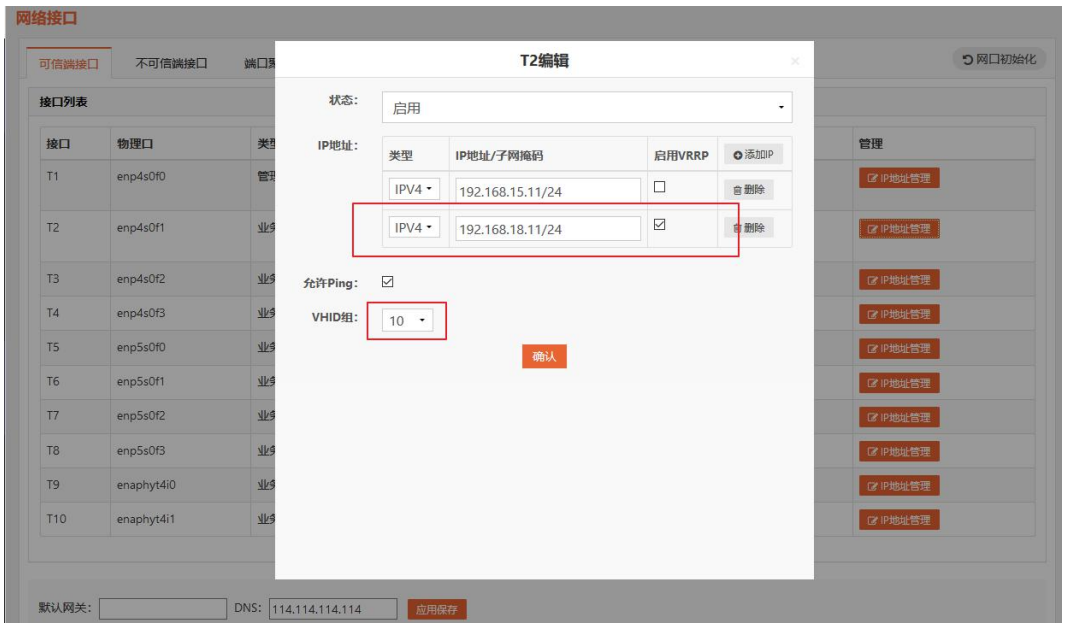
- 设备 IP：查看当前设备 IP；
- 热备地址池：配置双机的主备机地址和优先级；

注：一般把主机的管理口 IP 添加到热备池，也可以添加其他业务口 IP，该接口 IP 对于多机热备的作用是：当该主机 IP 处于断开状态，主机将会自动切换到下一优先级主机。

6.4.2. 虚拟 IP

在配置高可用双机热备时，需要为主备设备配置一套虚拟 IP；虚拟 IP 只在主设备上激活，也就是说，通过虚拟 IP 访问到的都是主设备，其作用主要在业务运行时出现主设备异常，系统能自主切换到备机，业务不会断开。

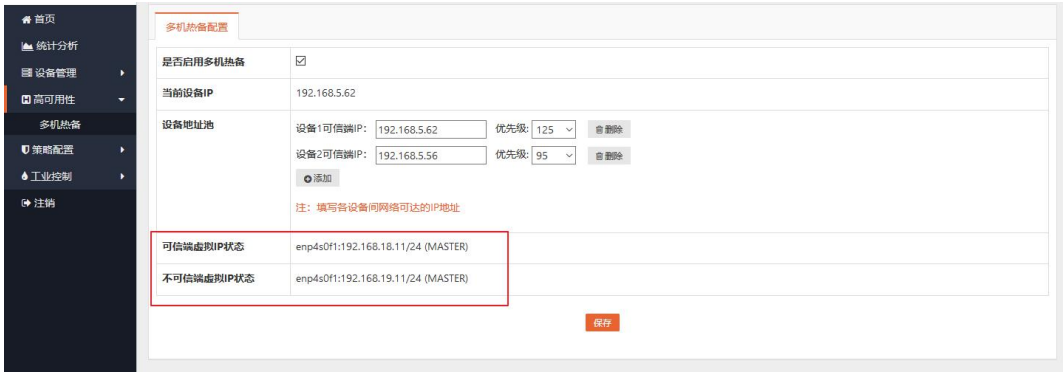
选择设备（热备池中的任一设备），进入“设备管理”>“网络接口”页面（或在多机热备配置页面点击“添加 VRRP 虚拟 IP”标签），选择要作为虚拟 IP 的接口地址，例如“192.168.18.11/24”，勾选“启用 VRRP”选项，在下方下拉框选择“VHID 组”，例如“10”，点击“保存”；在不可信端也需要选择一个接口地址作为虚拟 IP，进行如上配置 IP 和勾选“启用 VRRP”选项，并在下方下拉款选择一个新的 VHID 组，例如“11”；可信端和不可信端不可选择一样的 VHID 组，点击“保存”；



刷新页面，进入“高可用性”>“多机热备”页面。查看下方“可信端虚拟 IP 状态”和“不可信端虚拟 IP 状态”，虚拟 IP 已经生效，且根据设备优先级，将当前设备切换为 MASTER 状态（主机状态）或 BACKUP 状态（备机状态）。

在热备池任意设备配置双机和虚拟 IP 后，配置会自动到池内其他设备，无需反复

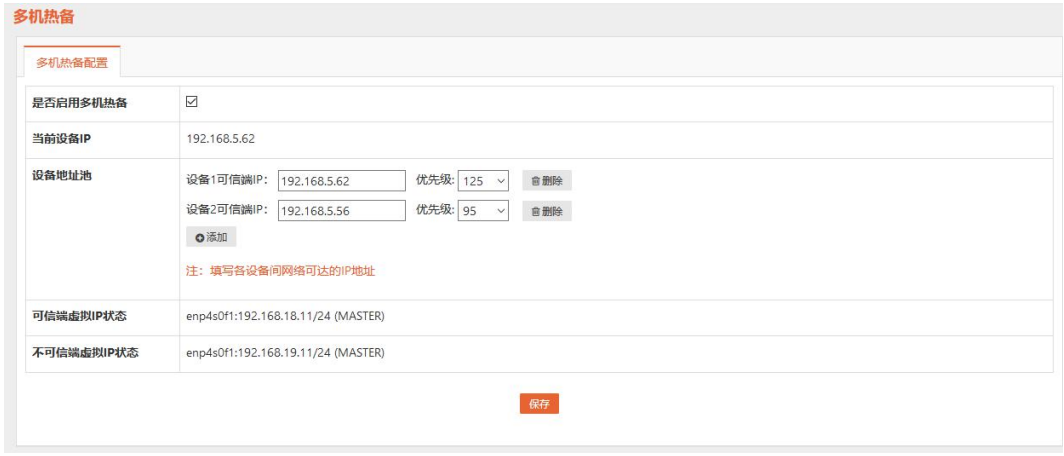
配置。



6.4.3. 双击热备状态

当优先级第一的不可信端或可信端主机出现故障，不能正常工作时，会通知另一端端主机，然后可信端主机跟不可信端主机的双机热备状态一同变为备机状态；优先级第二不可信端备机跟可信端备机的双机热备状态变为主机状态，以此类推。

状态显示在“高可用性”->“多机热备”中。



注意：在配置双击热备前必须清掉所有的任务配置（最好是恢复默认值），否则同步可能异常。

6.5. 策略配置

6.5.1. 对象

对象：

在 ViGap7.0 的对象服务页面，可以创建 IPV4、IPV6、时间计划或文本的对象，用于策略的添加使用。一次添加，多处复用。

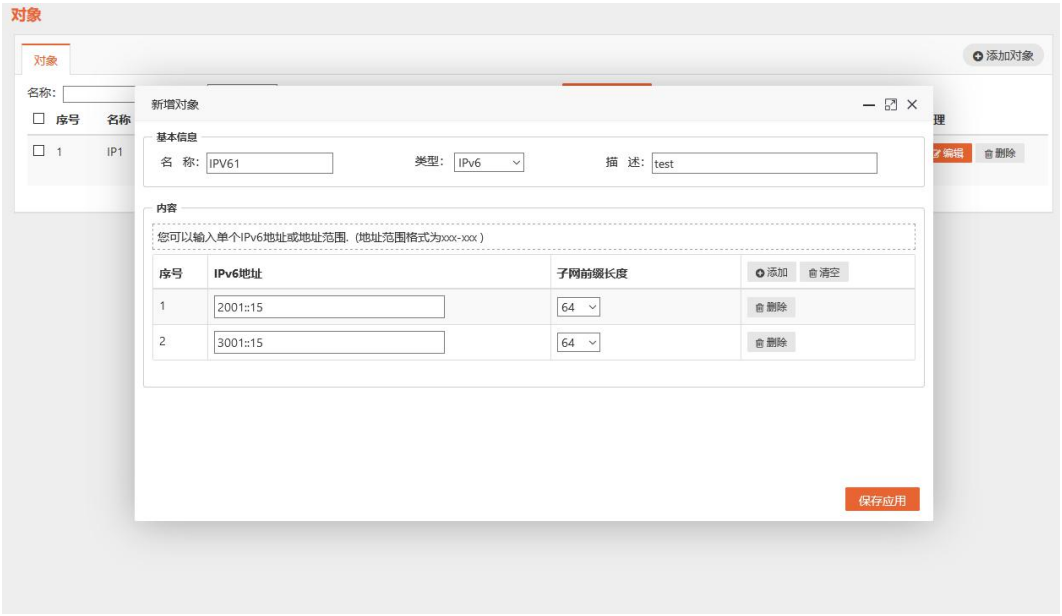
进入“策略配置”>“对象”页面，点击“添加对象”按钮添加一个类型对象。输入对象名称和描述，选择需要的对象类型，在下方点击“添加”对象，点击“清除 IP”，清除接口的所选 IP 信息；

再次点击“添加”，可添加多个同类型对象；

点击“删除”，删除当前对象；

点击“清空”，清空对象内容列表；

点击“保存应用”保存对象配置；



- 名称：可以是字母、数字、下划线、中文任意组合，最大长度 32 个字符；
- 类型：下拉框选择文件对象类型，可以选择 IPv4、IPv6、计划表、文本对象；
- 描述：描述不限制，可以填写，也可以不填写。
- 内容：IPv4 类型内容：至少添加一个 IPv4 地址和子网掩码长度；

  IPv6 类型内容：至少添加一个 IPv6 地址和子网掩码长度；

  计划表内容：在计划类型下拉框选择为每天、每周、每月或自定义日期范

围，日期范围在弹出日历选择一段连续日期范围。时间范围在弹出时间框选择开启时间和结束时间。

注：1、除了计划时间，网络和文本类型一个对象里可以添加多个数据，称为对象组。

添加完成的对象可以在对象列表里面查看相关信息，并可用关键字检索对象。

点击“编辑”，修改当前对象；

点击“删除”，删除当前行对象；

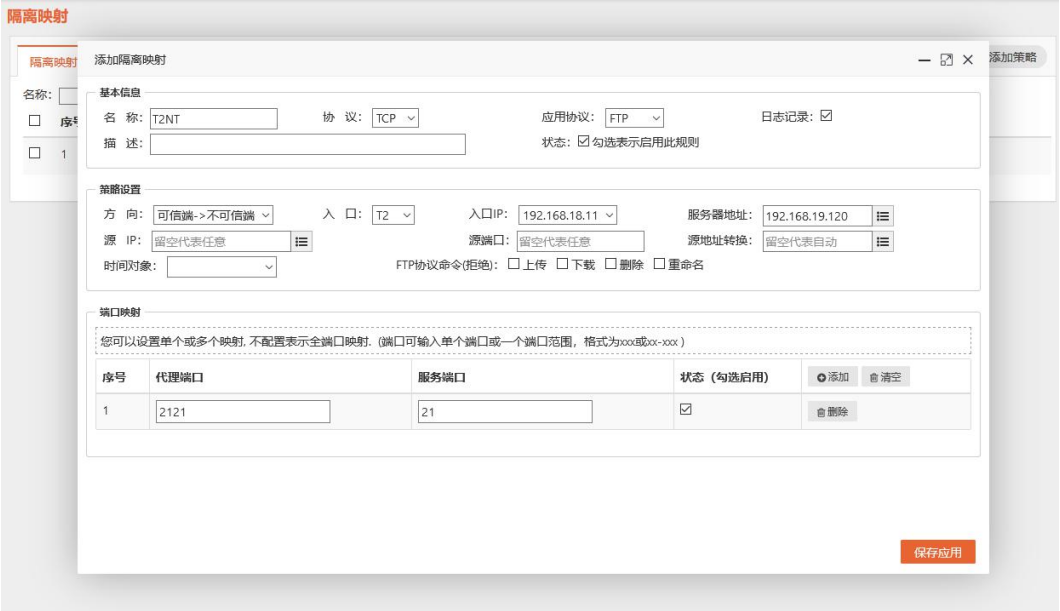
在实际业务操作的时候可以调用对象，可以在对应位置点击查看对象详情。

正在使用中的对象支持修改，业务会对应更新修改后的对象参数。

6.5.2. 隔离映射

当一个网络主机需要跟另一网络主机进行关联时可使用隔离映射，使得指向网闸的某个地址和端口的数据转发到另一网络的一台主机上。

进入“策略配置”>“隔离映射”页面，点击“添加策略”按钮添加一个新的隔离映射。系统必填项为映射名称、相关描述，选择协议和数据方向、数据入口 IP 地址和目的服务器地址以及需要映射的端口。勾选启用此规则后，点击“保存应用”，规则生效。



- 名称：可以是字母、数字、下划线、中文任意组合，最大长度 32 个字符；
- 状态：选择启用或禁用，默认选中启用；
- 协议：默认选择 TCP 协议，可在下拉菜单中选择 TCP 或 UDP 协议；
- 处理模块：默认不定义，可在下拉菜单中选择 HTTP、FTP、SMTP、POP3、MYSQL、SIP 和 RTSP；
- 日志记录：默认不勾选，勾选日志记录后，可使用日志审计员账号登录，在“访问日志”模块查看通过该映射的相关日志；
- 描述：描述不限制，可以填写，也可以不填写；
- 状态：默认勾选启用规则；
- 方向：选择映射方向从可信端到不可信端或不可信端到可信端，默认选中从可信端到不可信端；
- 入口：在需要通讯的一端，选择一个已启用的接口，作为入口的接口；
- 入口 IP：在上述入口接口中选择一个 IP，该 IP 和需要和源主机能正常通讯；
- 服务器地址：填写需要到达的目的主机的 IP 地址，可手动输入 IP 地址或选择 IPv4/IPv6 类型对象，目的主机需要和一端能正常通讯；
- 源 IP/源端口：限制访问系统入口的 IP 地址，只有填写的 IP 地址的端口才可访问可信网络，可以留空代表任意地址可接入，可以选择 IP 对象/对象组；
- 源地址转换：可填写 IP 地址/IP 对象，用于展示给外部的源 IP 地址，方便把源端真实地址进行隐藏；
- 时间对象：可在此处选择一个启用中的计划表对象，映射业务只会在计划的时间

内开启；

- 端口映射：可添加一个或多个端口，代理端口填写系统内部转发端口，服务端口填写服务器真实访问端口。

注：1、端口映射配置时，不配置表示全端口映射。

2、选择应用协议默认为不定义，也可根据应用层实际使用情况选择对应的协议，选择的协议可以进行对应的条件过滤（如选择 HTTP 应用协议，可以对访问请求方式进行过滤，如 GET、POST、PUT 过滤等）

添加完成的策略可以在隔离映射列表里面查看相关信息，并可用关键字进行检索。

点击“点击启用/禁用”按钮手动对策略进行启停；

点击“编辑”按钮进入隔离映射修改页面；

点击“删除”按钮删除该条映射；

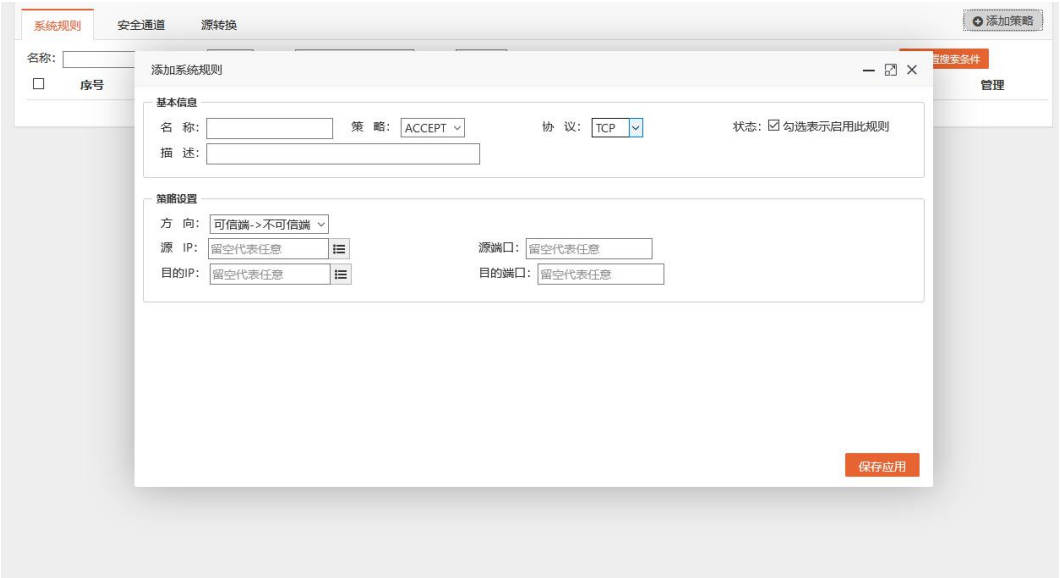
勾选列表左边的复选框可以批量删除策略。

6.5.3. 访问控制

6.5.3.1. 系统规则

在 ViGap7.0 的访问控制页面可以新增系统规则，对指定访问地址、端口、策略类型和协议进行阻断和放行。

进入“策略配置”>“访问控制”页面，切换到“系统规则”标签，点击“添加策略”按钮添加一个新的规则。



- 名称：可以是字母、数字、下划线、中文任意组合，最大长度 32 个字符；
- 策略：默认选择“ACCEPT”，可在下拉框选择“DROP”或“REJECT”
- 协议：默认选择“TCP”，可在下拉框选择“UDP”或“ICMP”
- 状态：新增时默认选中“启用”，保存配置后，可以在列表页面点击禁用；
- 描述：描述不限制，可以填写，也可以不填写；
- 方向：默认选中可信端->不可信端，可选不可信端->可信端；
- 源 IP/端口：限制访问源的地址和端口；
- 目的 IP/端口：限制到达的目的地址和端口。

添加完成的服务可以在系统规则列表里面查看相关信息。

点击“点击启用/禁用”按钮手动对策略进行启停；

点击“编辑”按钮进入策略修改页面；

点击“删除”按钮删除该条策略（可批量删除）。

6.5.4. 本地服务

6.5.4.1. 本地 FTP

在 ViGap7.0 的本地服务页面可以创建可信端和不可信端的本地 FTP 服务，FTP 服务可对系统数据上传和下载，以及文件同步业务。

进入“策略配置”>“本地服务”页面，选择本地 FTP 模块的可信端或不可信端标签，点击“添加 FTP”按钮添加一个新的本地 FTP 服务。

- 状态：新增时默认选中“禁用”，保存配置后，可以在列表页面点击启用；
- 位置：可选择可信端或不可信端，默认选中当前所在端；
- 用户名：3-8 位数字、字母或组合；
- 密码：不能使用中文字符，只能单纯英文或数字（或者英文数字组合）；
- 强制访问控制等级：配置强制访问等级后，在下拉菜单中选择等级。

添加完成的服务可以在本地 FTP 列表里面查看相关信息。

点击“点击启用/禁用”按钮手动对服务进行启停；

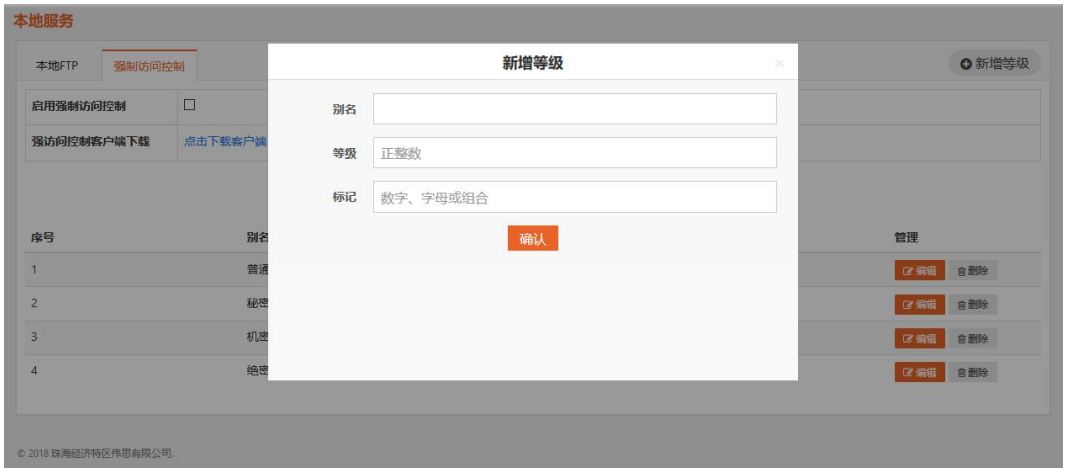
点击“编辑”按钮进入本地 FTP 修改页面；

点击“删除”按钮删除该条服务。

6.5.4.2. 强制访问控制

ViGap7.0 可对上传至本地的文件进行限制，保证系统安全。

进入“策略配置”>“本地服务”页面，选择强制访问控制模块，勾选启用强制访问控制等级，点击“添加等级”按钮，添加等级。



- 别名：可以是字母、数字、下划线、中文任意组合，最大长度 32 个字符；
- 等级：正整数；
- 标记：标记：数字、字母或组合。

等级用于区分 FTP 账户的权限，选择了强制访问控制等级的账户可以访问等于或低于自身等级的文件。

下载页面上的强制访问客户端，可用于对文件打上或解除等级标识。

启动标识客户端，填写可信端或不可信端的 IP 地址、FTP 账号名和密码后（端口号默认 5566），点击“连接”按钮，连接成功后，即可对本地的文件夹或文件进行打标识或除标识操作；

6.5.5. 数据交换

6.5.5.1. 文件交换

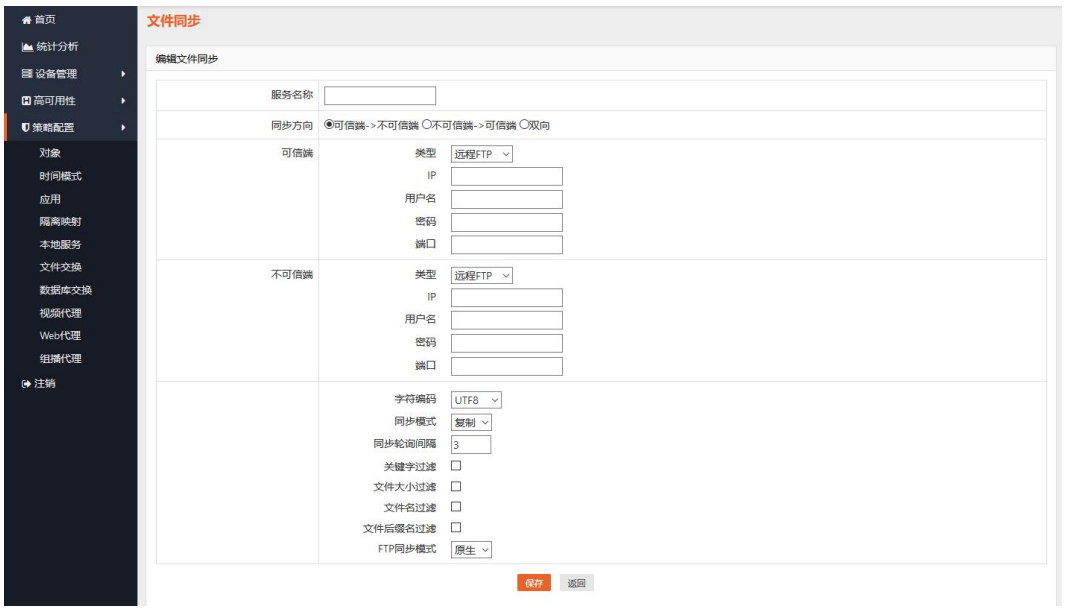
ViGap V7.0 可对可信端网络和不可信端网络进行文件交换。进入“策略配置”>“文件交换”页面，点击“添加策略”按钮，添加一个文件交换任务。

创建非结构化数据同步任务时：

a. 如果是配置本地任务，必须要先在可信端和不可信端创建本地 FTP。

b. 如若创建远程同步任务，则必须要在可信端和不可信端分别准备一台服务器，该服务器上装对应服务器，然后在文件同步业务中进行任务配置。

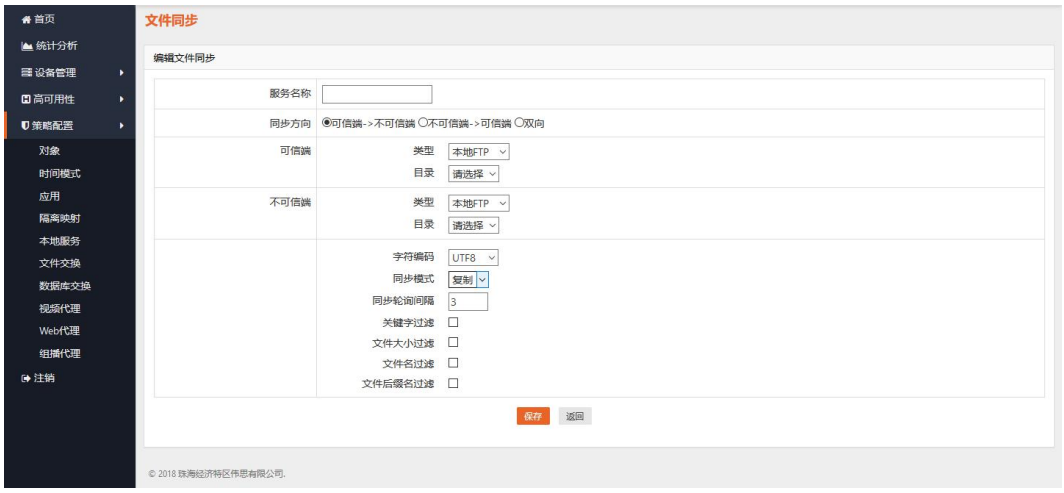
远程 FTP：



- 类型：远程 FTP；
- IP：填写远程 FTP 服务器的 IP 地址；
- 用户名：填写远程 FTP 服务器的登录用户名；
- 密码：填写远程 FTP 服务器的登录密码；
- 端口：填写远程 FTP 服务器的 FTP 服务端口号；
- FTP 同步模式：默认选中“专用”，可在下拉菜单中选择“原生”。

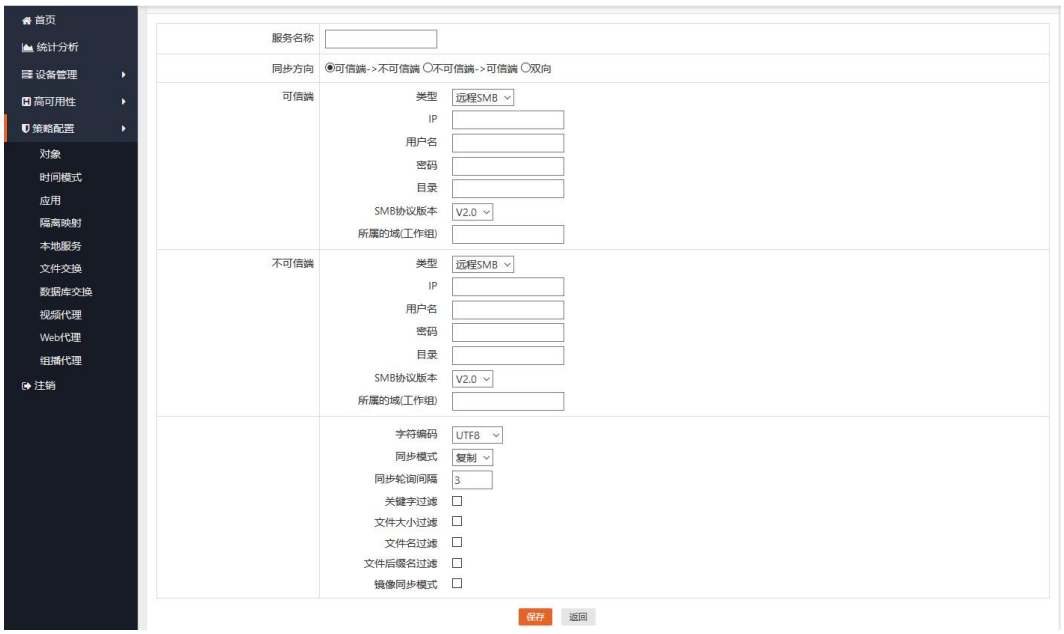
注：同步模式差异：专用模式性能高，原生模式稳定性高

本地 FTP：



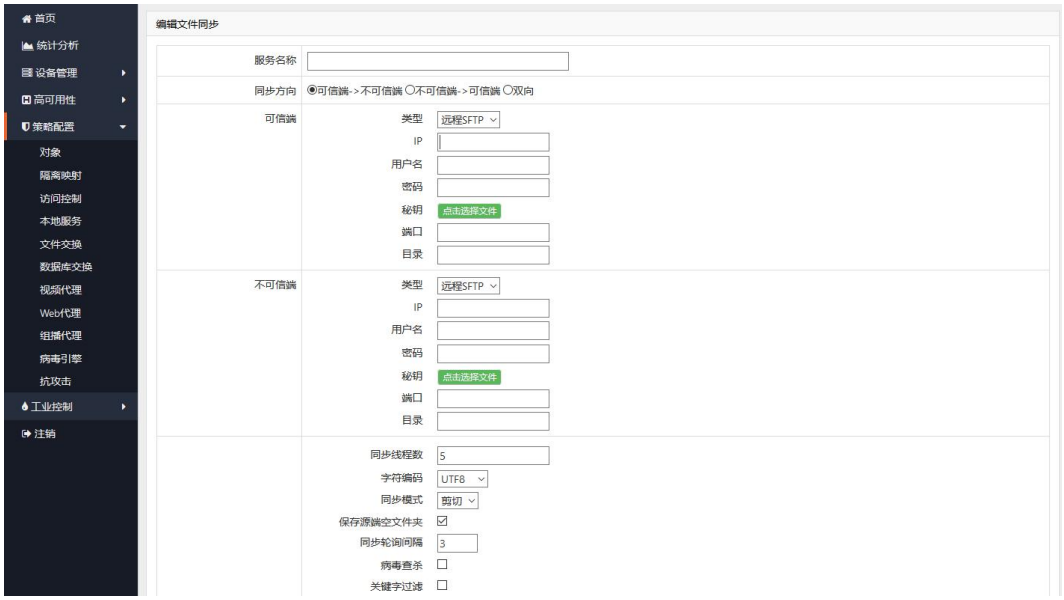
- 类型：本地 FTP；
- 目录：选择 FTP 目录（账户），下拉框中选择本地服务页面中，处于启用状态的本地 FTP；

远程 SMB：



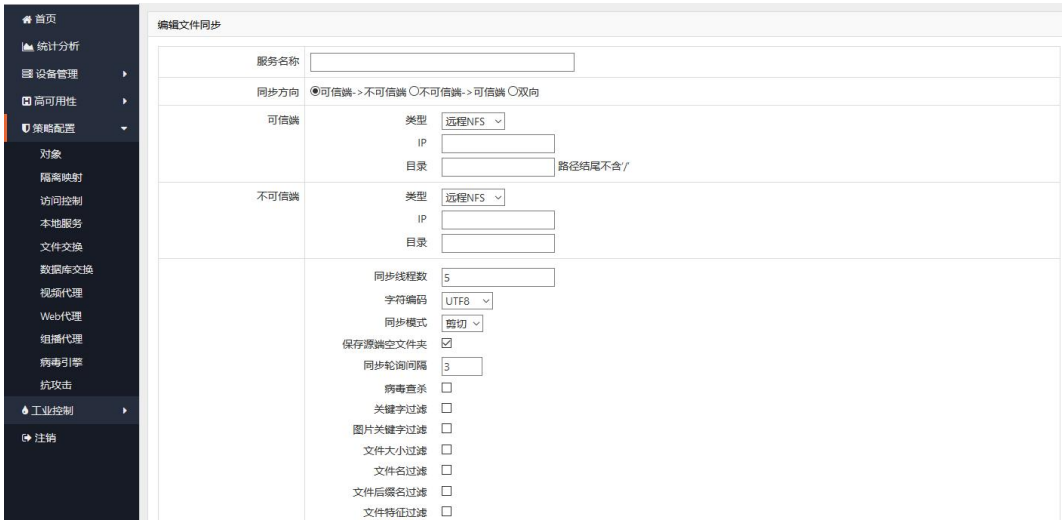
- 类型：远程 SMB；
- IP：填写远程 SMB 服务器的 IP 地址；
- 用户名：填写远程 SMB 服务器的登录用户名；
- 密码：填写远程 SMB 服务器的登录密码；
- 目录：填写远程 SMB 服务器的共享目录，目录格式为“\smb”
- SMB 协议版本：默认选中 V2.0（稳定），可在下拉菜单选择 V1.0 或 V3.0；
- 所属的域（工作组）：填写 SMB 服务所属工作组。

远程 SFTP：



- 类型：远程 SFTP；
- IP：填写远程 SFTP 服务器的 IP 地址；
- 用户名：填写远程 SFTP 服务器的登录用户名；
- 密码：填写远程 SFTP 服务器的登录密码；
- 端口：填写远程 SFTP 服务器的服务端口；
- 目录：填写远程 SFTP 服务器的共享目录；
- 密钥：上传连接 SFTP 服务器的密钥；

远程 NFS：



- 类型：远程 NFS；
- IP：填写远程 NFS 服务器的 IP 地址；
- 目录：填写远程 NFS 服务器的共享目录，需填写绝对路径，结尾不含‘/’；

通用设置：

- 服务名称：可以是字母、数字、下划线、中文任意组合，最大长度 32 个字符；
- 同步方向：默认选中“可信端->不可信端”，还有“不可信端->可信端”、“双向”可选；
- 字符编码：默认为 UTF8，可在下拉菜单中选择 CP936；
- 同步模式：默认为剪切，可在下拉菜单中选择剪切或复制（注意：若选择双向文件同步，则该值只能为复制）；
- 同步轮循间隔：填入数字，默认为“3”；
- 关键字过滤：勾选关键字过滤则开启关键字过滤，并配置需要过滤的关键字，不勾选关键字过滤则不开启关键字过滤；
- 文件大小过滤：勾选文件大小过滤则开启文件大小过滤，并配置过滤的最大、最小值以及单位，不勾选文件大小过滤则不开启文件大小过滤；
- 文件名过滤：勾选文件名过滤则开启文件名过滤，并配置需要过滤的文件名关键字，不勾选文件名过滤则不开启文件名过滤；
- 文件后缀名过滤：勾选文件后缀过滤则开启文件后缀过滤，并在后缀过滤类型下拉菜单中选择后缀过滤的类型和配置需要过滤的文件后缀，不勾选文件后缀过滤则不开启文件后缀过滤；
- 保存：点击“保存”按钮，完成该同步任务的创建；
- 返回：点击“返回”按钮，取消该同步任务的创建；

6.5.5.2. 数据库交换

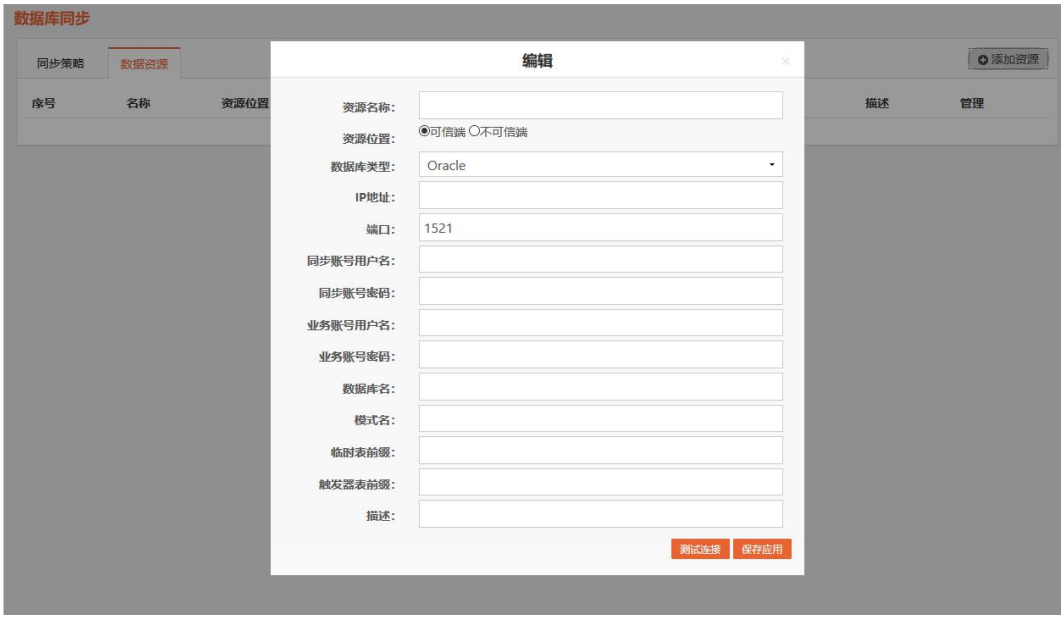
ViGap V7.0 可对可信端网络和不可信端网络进行数据库表数据交换。进入“策略配置”>“数据库交换”页面。

数据库管理页面主要包括：同步策略配置和数据资源配置两部分。

创建数据库同步策略时，必须要创建好可信端和不可信端的数据库资源。

数据资源：

在 ViGap7.0 的可信端的数据库交换页面可以进行可信端和不可信端的数据库资源配置，完成配置，测试连接成功后，可以用于数据库交换使用。



- 资源名称：可以是字母、数字、下划线、中文任意组合。
- 资源类型：默认选中 Oracle，可在下拉菜单中选择 SQLServer、MySQL、DB2；SYBase、DM、OSCRA、KingbaseES 的数据库类型；
- IP 地址：该数据库所在服务器的 IP 地址；
- 端口：数据库使用的端口号；
- 同步帐号用户名：数据库同步账户用户名；
- 同步帐号密码：数据库同步账户密码；，
- 业务帐号用户名：数据库业务帐号用户名；
- 业务帐号密码：数据库业务帐号密码；
- 数据库名：该资源所在的数据库名称；
- 模式名：自定义模式名；

- 临时表前缀/触发器表前缀：使用触发器同步方式时生成的临时表前缀名。自定义，一般采用“xxx_”格式；
- 描述：描述不限制，可以填写，也可以不填写。

然后点击“连接测试”按钮，连接成功后方可保存。

同步策略：

配置好可信端和不可信端的数据资源后，可以在同步策略页面添加策略，进行数据库数据交换。

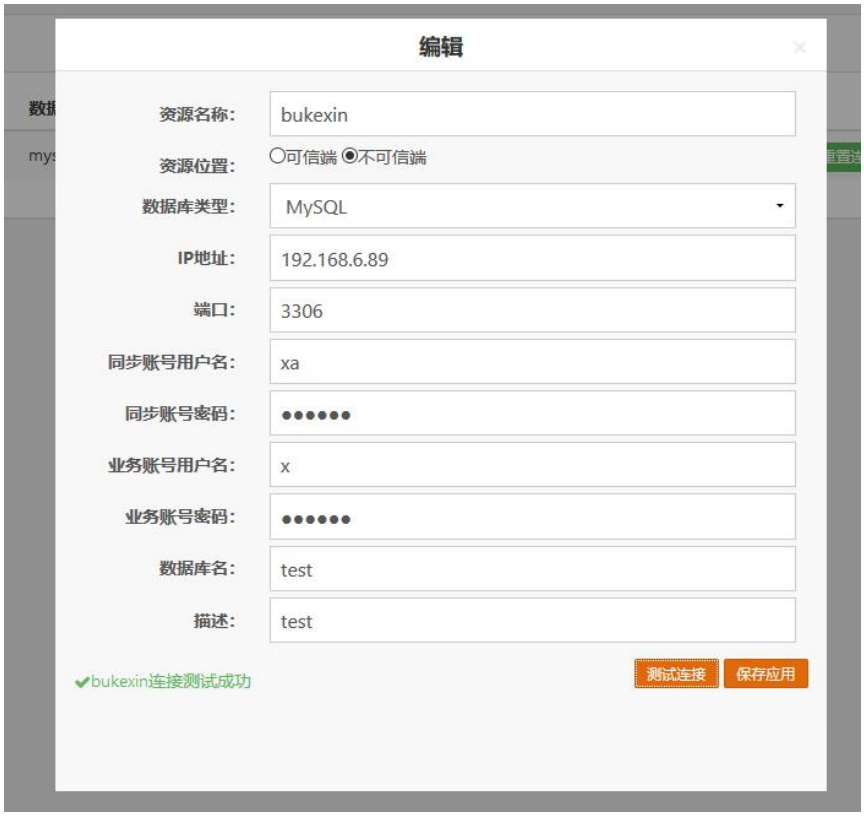
以 MySQL 数据库同步为例：

1) 配置可信端数据资源；

- 资源名称：可以是字母、数字、下划线、中文任意组合，如：kexin；
- 资源类型：可以是 Oracle、SQLServer、MySQL、DB2 等数据库类型，如：MySQL；
- IP 地址：可信端数据库所在服务器的 IP 地址，如：192.168.5.88；
- 端口：可信端数据库使用的端口号，如：3306；
- 同步帐号用户名：数据库同步账户用户名，如：xa；
- 同步帐号密码：数据库同步账户密码，如：123456；
- 业务帐号用户名：数据库业务帐号用户名，如：x；
- 业务帐号密码：数据库业务帐号密码，如：123456；

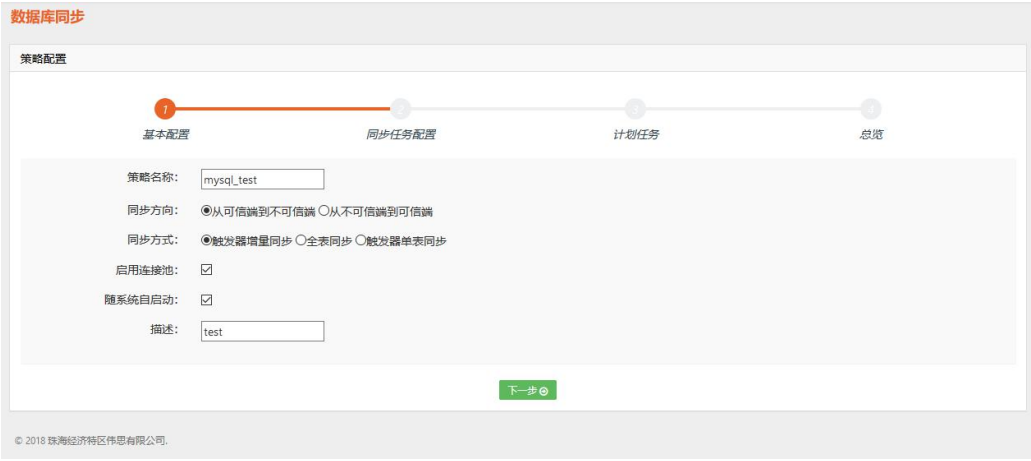
- 数据库：可信端资源所在的数据库名称，如：test；
- 临时表前缀：使用触发器同步方式时生成的临时表前缀名，如“yewu_”
- 触发器表前缀：自定义，如“tongbu_”
- 描述：描述不限制，可以填写，也可以不填写。

2) 配置不可信端数据资源；



- 资源名称：可以是字母、数字、下划线、中文任意组合，如：bukexin；
- 资源类型：可以是 Oracle、SQLServer、MySQL、DB2 等数据库类型，如：MySQL；
- IP 地址：可信端数据库所在服务器的 IP 地址，如：192.168.6.89；
- 端口：可信端数据库使用的端口号，如：3306；
- 同步帐号用户名：数据库同步账户用户名，如：xa；
- 同步帐号密码：数据库同步账户密码，如：123456；
- 业务帐号用户名：数据库业务帐号用户名，如：x；
- 业务帐号密码：数据库业务帐号密码，如：123456；
- 数据库：可信端资源所在的数据库名称，如：test；
- 描述不限制，可以填写，也可以不填写。

3) 添加同步策略



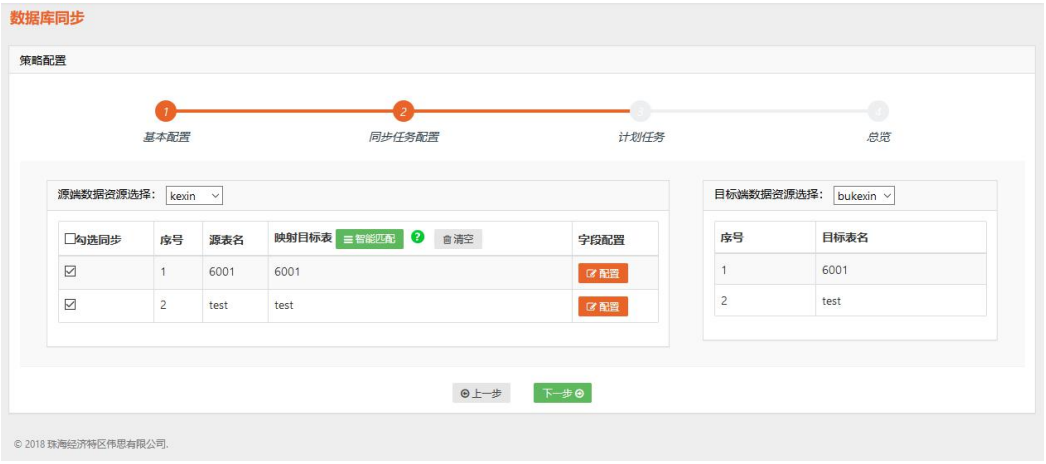
- 策略名称：可以是字母、数字、下划线、中文任意组合，如：mysql_test；
- 同步方向：可选项：从可信端到不可信端、从不可信端到可信端；
- 同步方式：

a. 触发器方式：是指发送端数据库同步表中插入、删除、更新若干条数据后，接收端数据库同步表中也自动同步插入、删除、更新了同样的数据。

b.普通全表同步方式：是指把整张表的数据都进行同步。

c. 触发器单表同步：是指发送端数据库同步表中插入、删除、更新若干条数据后，接收端数据库同步表按表接受数据的插入、删除和更新数据。

- 启用连接池：勾选启用连接池，用于更新数据库数据；
- 跟随系统自启动：勾选，系统启动时自动启动策略服务；
- 描述：描述不限制，可以填写，也可以不填写。



- 资源选择：选择已配置保存的可信端资源和不可信端资源。如：源端数据资源选择“kexin”，目标端数据资源选择“bukexin”；
- 映射目标表：

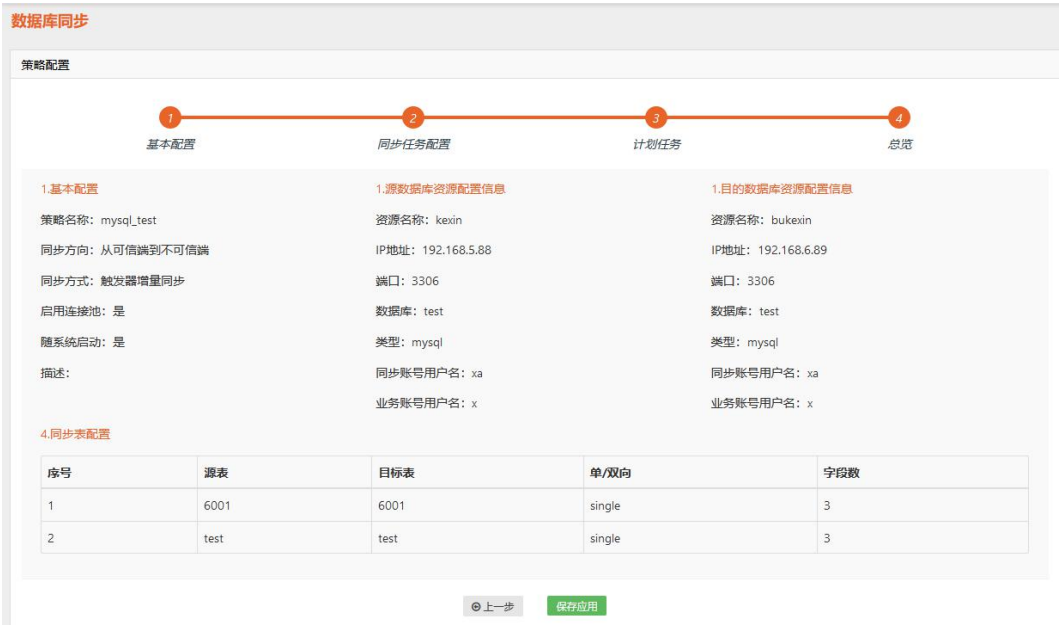
使用智能匹配，源表和目标表名称一致的将自动映射；

使用拖拽的方式，把【目标表名】的列拖拽到【映射目标表】的表格中

点击“清空”按钮删除已匹配的目标表

- 勾选同步：勾选的表会进行同步，不勾选则不进行同步；
- 配置：进入配置可以修改同步源端表的标识列，同步方向。

- 时间间隔：系统默认是 3 秒，也可以自己根据需要填写其他整形数。



确认策略配置，确认无误后点击“保存应用”按钮，如还需修改点击“上一步”按钮。

至此，数据库同步策略配置完成，

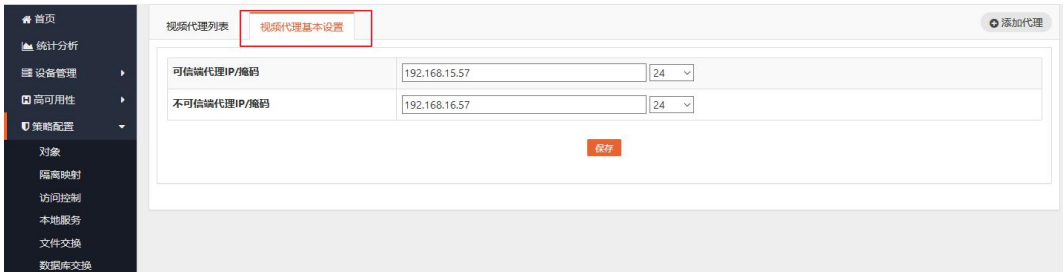
6.5.6. 业务代理

6.5.6.1. 视频代理

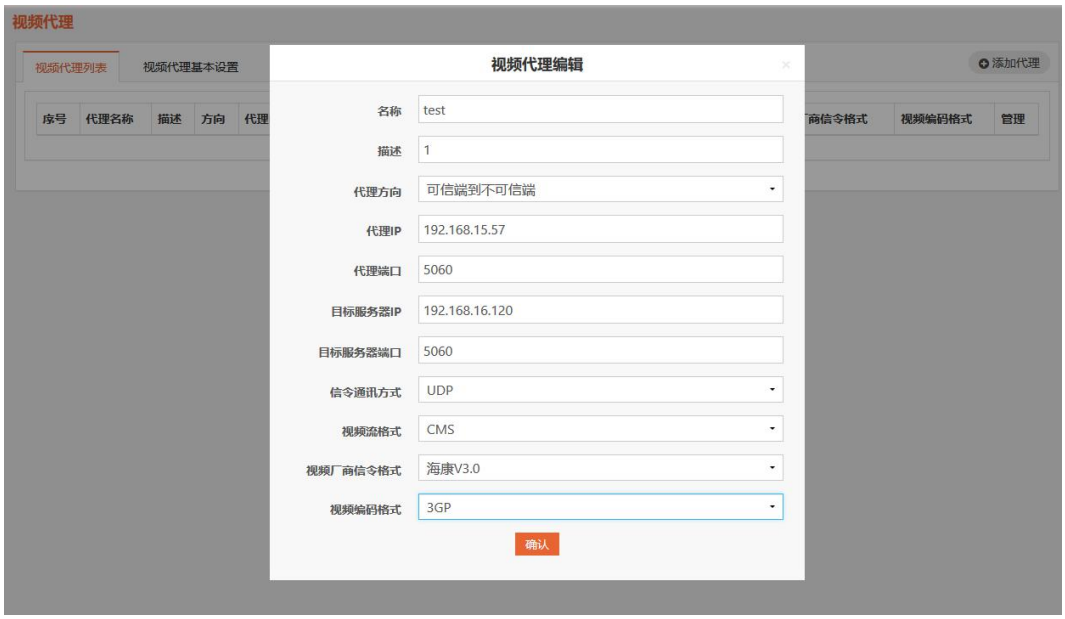
ViGap V7.0 可把一端网络的视频流安全传输到另一端，支持大多数主流厂商信令和视频流格式的注册和传输。

进入“策略配置”>“视频代理”页面，需要先配置代理 IP（视频接入接口 IP）

后，才可添加视频代理策略，点击“视频代理基本设置”标签，配置可信端和不可信端的代理地址，点击“保存”生效；



点击“视频代理列表”标签，进入视频代理列表页面。点击“添加代理”新增一条视频代理。



- 代理名称：设置该策略的名称；
- 代理 IP： 系统映射的 IP 地址；
- 代理端口：系统映射的端口号；
- 服务器 IP： 真实的服务器 IP 地址；
- 服务器端口：真实的端口号；
- 信令通信方式：在下拉框中有可选项。支持 UDP；
- 视频流格式：在下拉框中有可选项；
- 厂商信令格式：在下拉框中有可选项；
- 视频编码：在下拉框中有可选项；
- 描述：可对该设置做详细描述

添加完成的视频代理策略立刻生效，可以在列表里面查看相关信息。

点击“编辑”按钮进入修改页面；

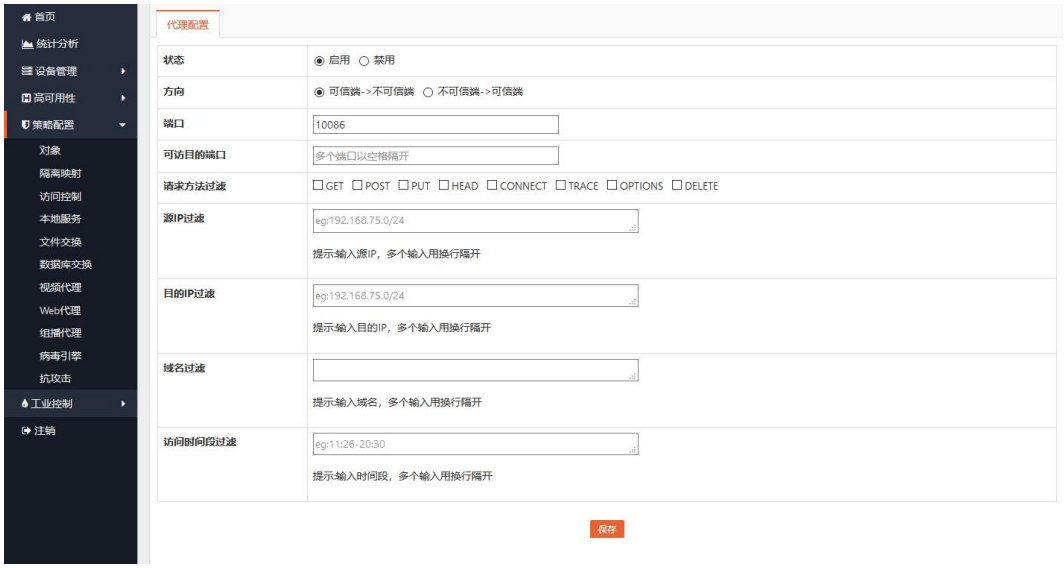
点击“删除”按钮删除该条代理；

6.5.6.2. Web 代理

ViGap V7.0 可对 http 服务器做浏览器代理，并对访问做相关限制。

进入“策略配置”>“Web 代理”页面，勾选启用代理，配置代理端口和方向，并可做相关访问限制，点击“保存”后生效。

在源端的浏览器设置 HTTP 代理，代理选项填写系统可信端的业务 IP 地址和配置的端口，点击“保存”。浏览器即可访问到不可信端网络的 Web 页面。



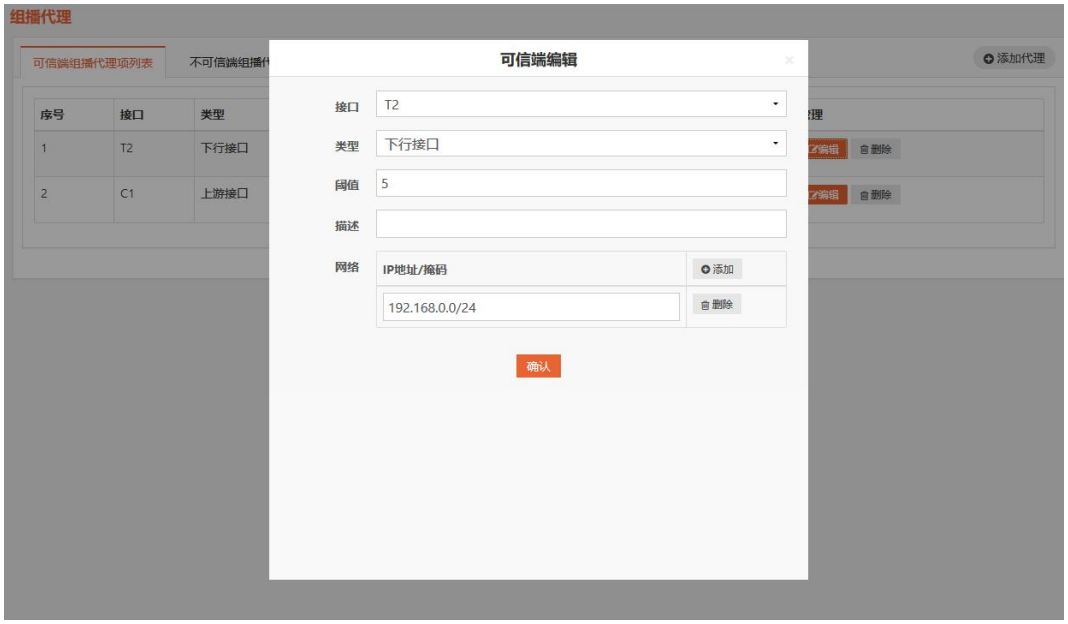
- 状态：默认不启用；
- 方向：可选择“可信端->不可信端”或“不可信端->可信端”；
- 端口：自定义网络端口；
- 可访问的端口：可填写目的服务器可访问的端口，可多填。留空代表不做限制；
- 请求方发过滤：可选 HTTP 请求方式过滤，可选 GET、POST、PUT、HEAD、CONNECT、TRACE、OPTIONS、DELETE 黑名单过滤；

- 源 IP 过滤:对发起请求的 Web 端做黑名单限制,填写格式如“xxx.xxx.xxx.xxx/24”多个输入用换行隔开;
- 目的 IP 过滤:对访问的目的 IP 做黑名单限制,填写格式如“xxx.xxx.xxx.xxx/24”多个输入用换行隔开;
- 域名过滤：对访问的目的地址做域名限制;
- 访问时间段过滤：对代理可用时间段做限制，填写格式如“11:20-12:20”多个用换行隔开。

6.5.6.3. 组播代理

ViGap V7.0 支持对可信网络端的主机发送的数据通过代理，复制到不可信网络多个加入此组播的主机，是一种一对多的通讯方式，组播方式解决了单播情况下数据的重复拷贝及带宽的重复占用，也解决了广播方式下带宽资源的浪费。

进入“策略配置”>“组播代理”页面，点击“添加代理”，配置可信端和不可信端的上游和下行的代理接口地址和 TLL，点击“保存”后生效。



- 上游接口：即组播服务器所在的首位 IP 地址，可以是网段
- 下游接口：即客户端所在的首位 IP 地址，可以是网段
- TTL 值：即跳过多少个路由器

注：一般来说，可信端和不可信端的组播代理配置除指定接口外，其它配置一样，上游都是组播服务器地址，下游都是客户端地址

添加完成的组播代理策略立刻生效，可以在列表里面查看相关信息。

点击“编辑”按钮进入修改页面；

点击“删除”按钮删除该条代理；

6.5.7. 攻击防御

ViGap V7.0 在可信端和不可信端都配备了一个病毒库引擎可抗攻击引擎，可把病毒文件阻挡在网闸外部或内部病毒隔离区，防止病毒文件入侵。

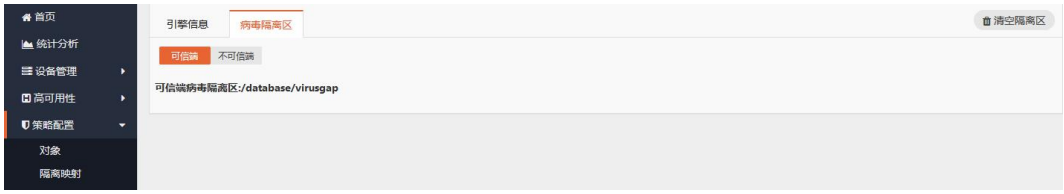
6.5.7.1. 病毒引擎

进入“策略配置”>“组病毒引擎”页面，勾选启用可信端病毒引擎和不可信端病毒引擎，点击“保存”生效。

在引擎信息页面可以查看病毒库版本和最后更新日期。点击“升级病毒库”可以把本地病毒库上传到 ViGapV7.0 上。

系统在业务运行中对过滤的病毒文件可选删除或保留的操作。选择保留的数据会存储到系统内部的病毒隔离区。

点击“病毒隔离区”标签，可以查看可信端和不可信端的保留病毒文件。点击右上角“清空隔离区”可以对病毒文件进行清空。



6.5.7.2. 抗攻击

系统可设置抗攻击。在配置抗攻击时，进入“策略配置”>“组病毒引擎”页面，勾选启用对应的抗攻击协议，并设置阈值，点击“保存”。

- TCP Flood：勾选启用，并设置阈值，默认阈值为 150；
- UDP Flood：勾选启用，并设置阈值，默认阈值为 150；
- ICMP Flood：勾选启用，并设置阈值，默认阈值为 150；

第七章 用户管理

7.1. 初始化配置

用户管理员可以通过管理员账号登录系统，对系统管理员、日志审计员和用户管理员进行设置，并进行一些相关的安全配置，可信端和不可信端使用统一账户管理。

系统提供了默认用户管理员 adminuser，管理人员应及时更改系统初始用户管理员的用户名和口令。选择一台安装有浏览器的客户机，与可信端管理口相连，修改客户机 IP 地址，使其与可信端管理接口（处于同一个网段，可信端管理口初始值为 192.168.0.254/24）；在浏览器地址栏输入：https://192.168.0.254:10000 即出现可信端管理系统登陆界面；

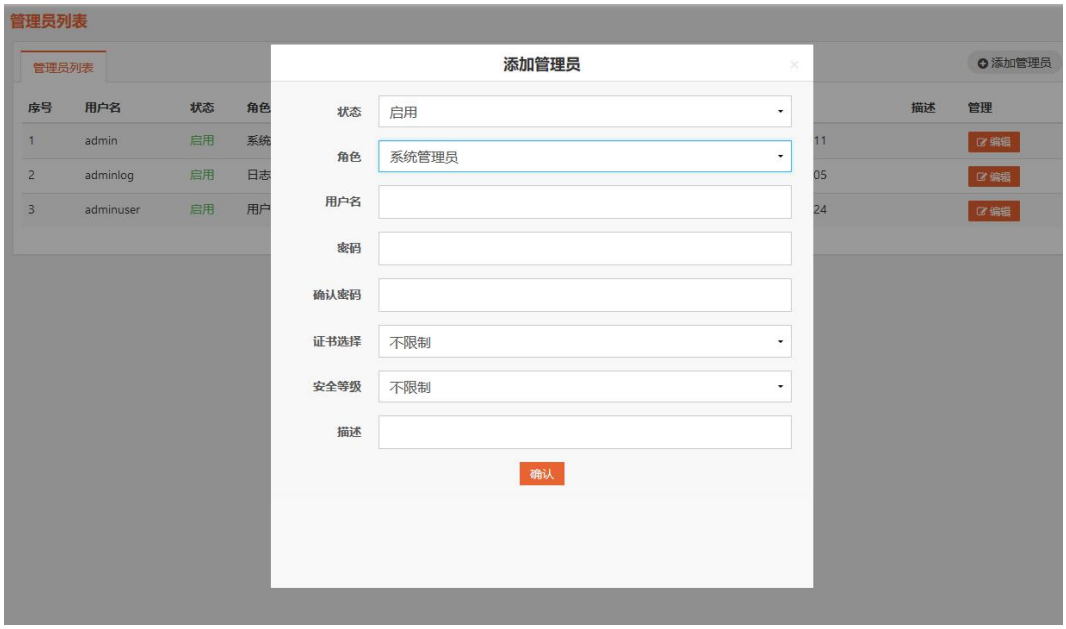
在“用户名”一栏输入用户名 adminuser，在“密码”一栏输入其对应默认口令“admin*pwd”，在验证栏输入验证码。即可进入系统的用户管理模块。系统用户管理分为：管理员列表和用户配置两大模块，并提供了角色定义和安全等级说明。

7.2. 用户管理

管理员列表显示了系统的用户以及角色等相关信息，并提供了用户新增、修改和删除的功能。

添加和修改管理员：

进入“用户管理”>“管理员列表”页面，点击“添加管理员”按钮进行新增。建议管理人员在登录系统后新增自己的角色用户，并删除系统默认用户。



- 状态：默认启用，可在下拉菜单中选择“启用”或“禁用”；
- 角色：默认为系统管理员，可在下拉菜单中选择“系统管理员”、“用户管理员”、“日志审计员”；
- 用户名：包含英文字母、数字、下划线、或破折号；
- 密码：不少于 8 位；
- 证书选择：默认不限制，可以在下拉菜单中选择 visec_01、visec_02;
- 安全等级：默认不限制，可在下拉菜单中选择等级 1、2、3；
- 描述：描述不限制，可以填写，也可以不填写。

角色定义：

定义了三个角色并添加了相关描述。

admins（系统管理员）：能查看和操作除日记审计员和用户管理以外的所有页面；

logauditor（日志审计员）：只能查看和操作日志审计相关的页面；

manager（用户管理员）：能查看和操作用户管理相关的页面。

安全等级：

定义了 1~3 三个等级，并规定了不同等级的对应权限。

级别 1：所有权限；

级别 2：设备管理、高可用性、对象、时间模式、应用、隔离映射；

级别 3：设备管理、高可用性、本地服务、文件交换、数据库交换、视频代理、Web 代理、组播代理。

7.3. 证书认证

在用户登录时可以启用证书认证，开启证书认证后，用于登录系统的 Web 浏览器必须导入至少一个证书，才可访问登录管理页面。用户也可以设置登录使用的证书，则登录时要导入对应证书才可正常登录该账号。

进入“用户管理”>“安全配置”页面，进行以下操作导入证书和登录。

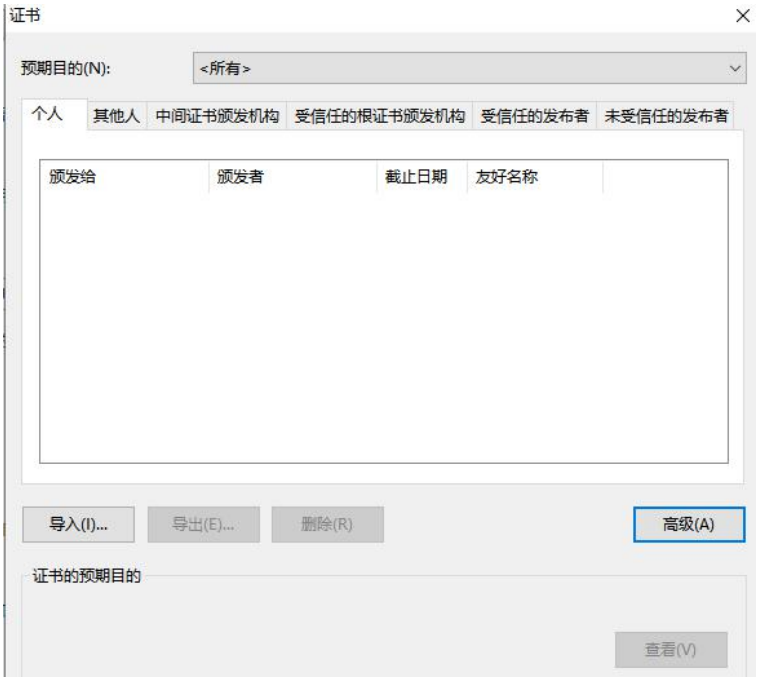
1) 下拉框选择“启用证书认证”，点击保存。

2) 在安全配置页面下载客户端证书 visec_01 或 visec_02 到本地；

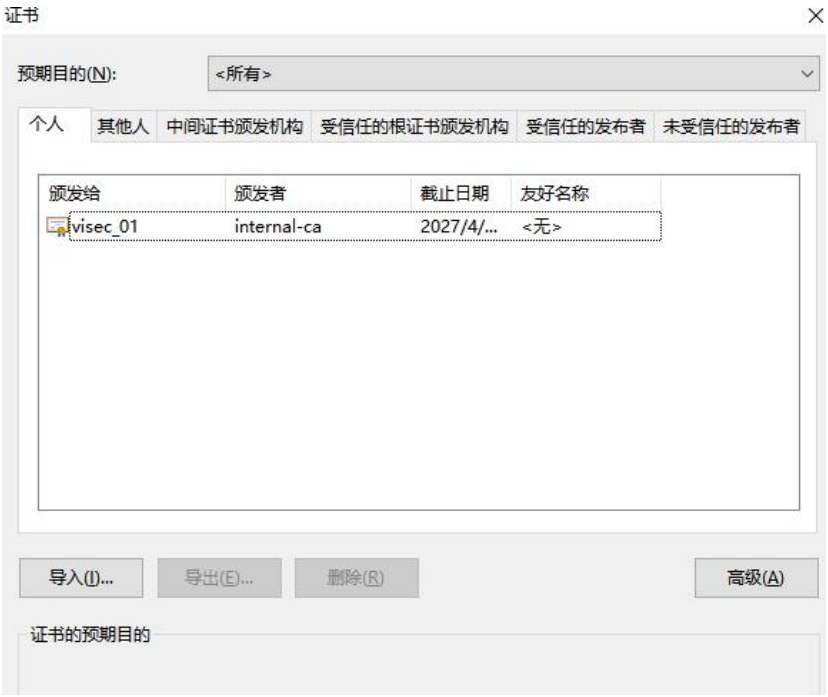
3) 在客户端机浏览器登录前上传证书；

以 Chrome 浏览器为例：

设置->高级-》HTTPS/SSL->管理证书：



点击“导入”按钮，选择本地证书，点击“下一步”，输入密码（两个证书的密码都为空），点击“确定”导入证书。



4) 导入证书后，清除浏览器缓存，在浏览器地址栏输入：https://192.168.0.254:10000 即出现可信端管理系统登陆界面，用对应证书认证的账号登录，即可登录成功。

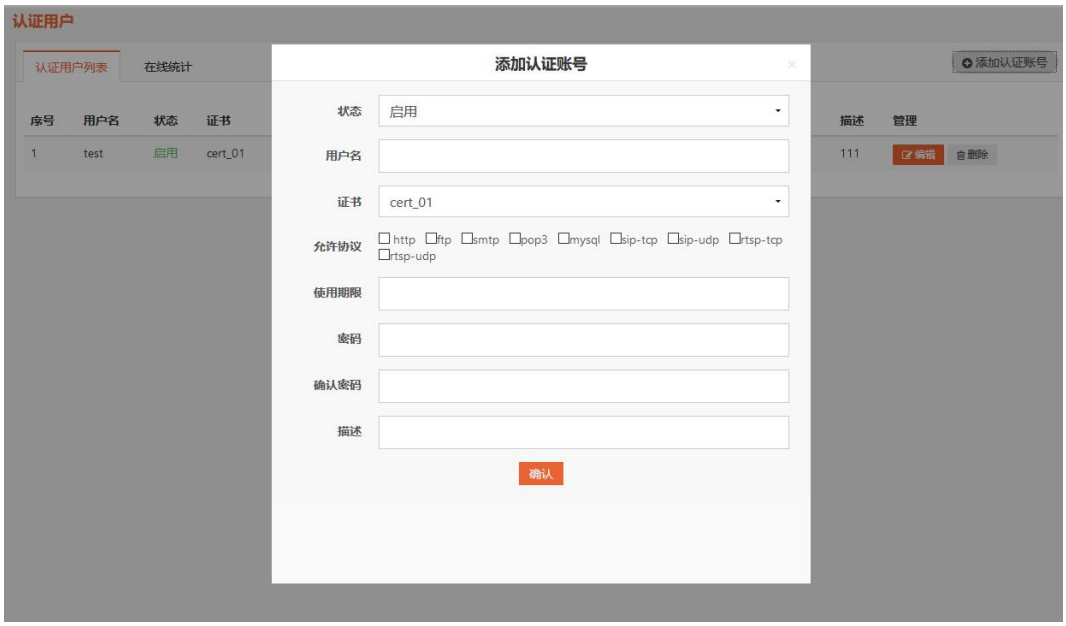
5) 用户在配置时默认不限制证书（即导入任意一本证书都可通过认证）。也可指定证书认证，此时就需要用特定证书才可进行登录，否则提示证书不匹配。

7.4. 用户认证

ViGapV7.0 的强制访问控制功能、代理模式下的隔离映射功能、数据同步功能和代理功能，必须先进行用户认证，才可正常使用。

进入“用户管理”>“认证用户”页面，点击“添加认证账号”按钮进行新增。

配置用户登录口令，选择证书和使用期限，并勾选允许通过的协议，点击“保存”生效。



- 状态：选择启用或禁用；
- 用户名/密码：设置认证用户的登录口令；
- 允许协议：勾选选择允许使用的业务协议，可选项有：http、ftp、smtp、pop3、mysql、sip-tcp、sip-udp、rtsp-tcp、rtsp-udp。其中前五种主要用于映射的协议过滤，后四种用于代理的协议过滤；
- 使用期限：允许账号使用的最后期限日期；
- 描述：填写相关说明。

点击“确认”认证用户配置完成。

点击“编辑”，可修改用户相关配置；

点击“删除”删除用户。

配置完成认证用户后，在运行上述业务前，需要：

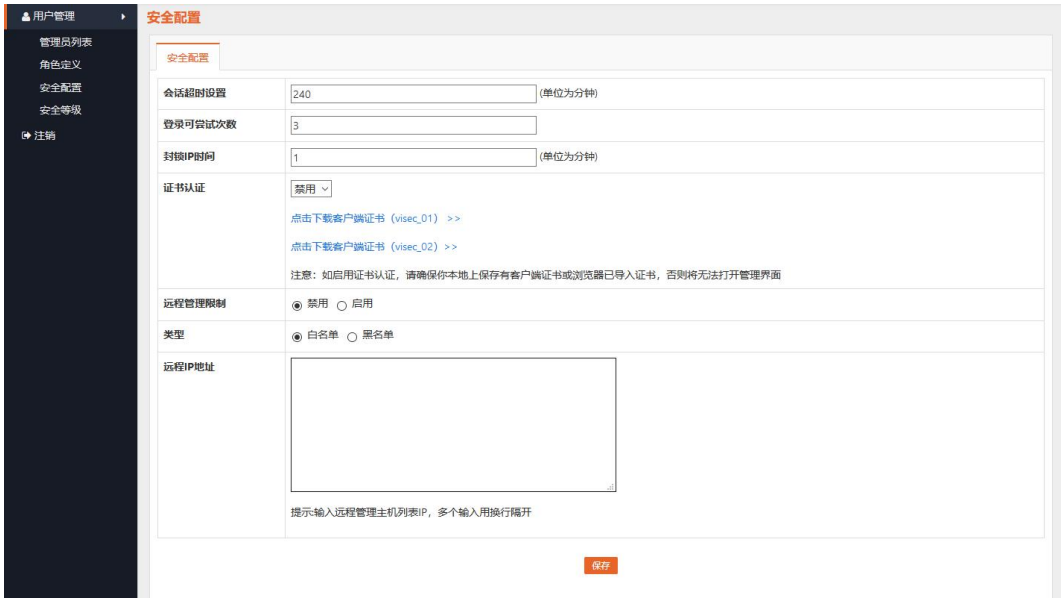
1) 在浏览器导入用户选择的证书（详见 7.3 证书认证）；
2) 使用运行业务的接口 IP 地址（非管理口）登陆认证页面，登陆端口为 8443（格式如 https：//192.168.15.57:8443）；
3) 输入用户名密码，登陆成功；
4) 登陆完成，页面显示该认证用户允许使用的协议；

5) 业务操作结束使用后，退出认证。

7.5. 安全配置

用户管理员可以在安全配置页修改登录选项，并在此页面下载登录证书（开启证书认证后使用）。

进入“用户管理”>“安全配置”页面，进行相关设置。



- 会话超时设置：默认为 240 分钟，也可以自定义超时时间，单位为分钟；
- 登录可尝试次数：默认为 3 次，可以填写其他整数来自定义次数，
- 封锁 IP 时间：超出登录可尝试次数后封锁登录，默认为 1 分钟，也可以自定义封锁时间，单位为分钟；
- 证书认证：选择“启用”来启用证书认证，把证书导入到本地用于登录时认证；
- 远程管理限制：选中“启用”来启用远程管理限制后，允许特定 IP 地址的客户端机登录系统；
- 类型：定义远程管理限制采用黑名单或白名单；
- 远程 IP 地址：输入限制的客户端机 IP 地址，多个 IP 用换行隔开。

点击“保存”保存安全配置设置。

第八章 用户使用安全说明

8.1. 使用限制

ViGapV7.0 支持用户使用主要业务功能，但对于系统安全及部分运维需要超级管理员才可操作。

用户限制功能：

- 设备升级（管理员提供升级包）

系统对升级包的完整性和安全性做校验，不支持用户自定义的升级包，在系统升级时联系管理员采用对应权限进行升级

- 授权注册（license 注册）

用户无权对系统进行二次转让，注册和授权。设备具有唯一识别号，由伟思公司统一管理，当系统为试用版且过期时，请联系相关人员进行授权和注册

- 用户配置

用户管理员可新增、删除、修改用户

- 系统证书下载

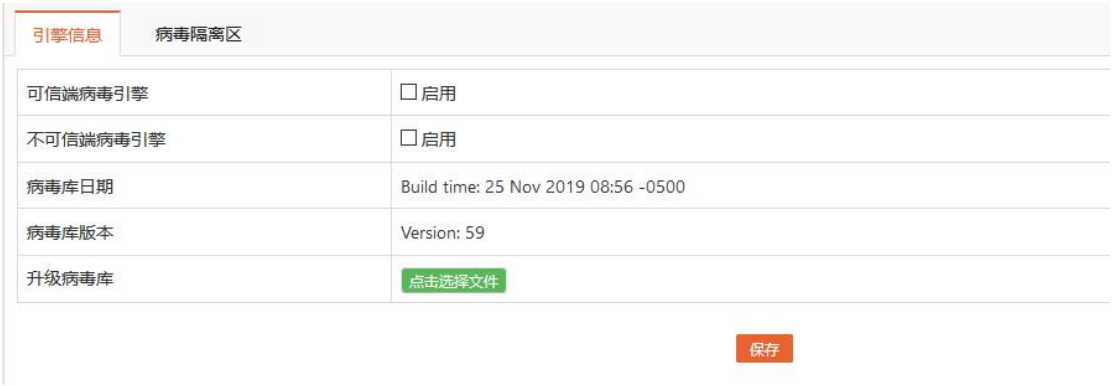
系统默认提供 cert_01 和 cert_02 证书，用于登录时认证导入，开启证书认证的用户需要在浏览器导入证书口方可访问登录页面。

- 安全配置：登录口令、用户权限设置、证书设置、安全等级

仅有超级权限管理员可对系统的登录时长、登录 IP 限制、证书使用、登录可尝试次数和封锁时间做配置。当用户需要对该配置做更改时请联系管理员。

- 病毒库升级

ViGap 提供系统病毒过滤和隔离，请联系管理员进行病毒库定时升级



支持用户直接使用的功能：

- 设备控制（关机、重启、恢复出厂）；
- 接口配置；
- 时间配置；
- 网络诊断工具；
- 业务配置（业务同步、隔离映射）；
- 日志查看和检索；
- 日志设置和同步；
- 后台基础命令使用（admin 账号）

8.2. 安全环境

ViGapV7.0 提供以下接口供用户管理和配置：

接口功能	访问端口	登入限制
Web 页面管理	10000	用户口令、证书
SSH 后台管理	6422	用户口令，提供部分功能
FTP 文件上传	21	用户口令，指定文件位置，启用本地服务
客户端管理	无	无

以下端口为系统常用程序端口，用户不可接入：

端口功能	访问端口	备注

python	16161	不可占用
mysqld	3306	不可占用
java	9527	不可占用
内外端通讯进程	38381	不可占用
视频代理程序	9999	配置业务后开启，不可占用
工业代理程序	12345	配置业务后开启，不可占用
用户认证程序	8443	不可占用

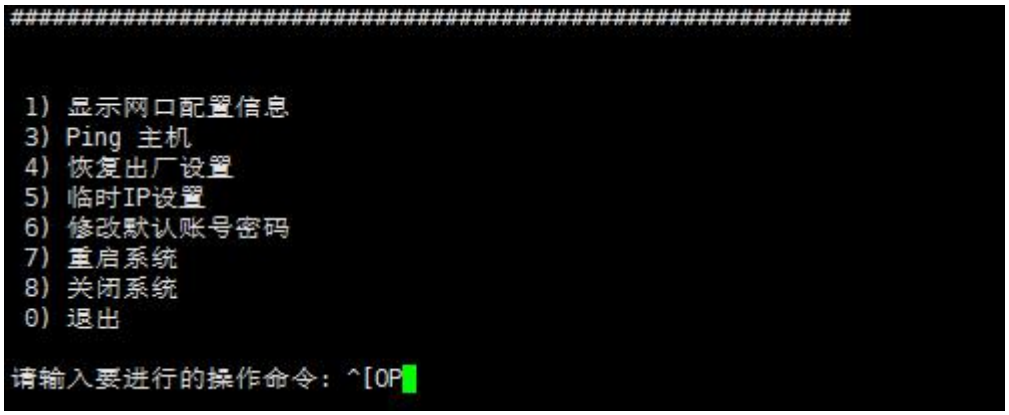
ViGap 提供用户登入系统页面和后台的接口，并提供常用功能

页面登录：

在浏览器地址栏输入：https://192.168.0.254:10000 即出现可信端管理系统登陆界面，输入默认用户名：admin，密码：admin*pwd，点击“登录”。

后台登录：

ViGap 后台配置界面，先启动 SSH 工具，通过 6422 端口登入，输入命令：SSH 192.168.0.254 6422，然后按下 Enter 键，跳转到 ViGap 登录界面，输入用户名：admin，密码：admin*pwd，按下 Enter 键，即可登入系统后台。



系统仅在后台开放以下命令：

- 显示网口配置信息
- Ping 主机
- 恢复出厂设置
- 临时 IP 设置
- 修改默认账号密码
- 重启系统

- 关闭系统
- 退出

8.3. 用户职责

- 路由模式下，系统可能被流量攻击、重要数据被转发到不可信网络、系统部分功能不支持（数据同步功能）；可能导致系统资源被占用，甚至导致瘫痪；
  用户可自行配置路由模式。
- 不开通安全合规性检查引发的安全事件：

1、未开启证书认证：仅通过用户名口令校验登录，可能导致系统登录时被恶意 CSRF 攻击；

2、未做证书认证：开启了页面登录证书认证后，必须把证书（系统页面提供下载链接）下载到本地，再导入用于登录的浏览器，否则会导致系统登录页面打开失败，用户无法登入系统，此时需要联系管理员索要证书或关闭认证；

3、未做用户认证：系统支持用户业务权限限制（如允许用户使用 FTP 协议、http 协议、snmp 协议等）；操作业务的用户必须拥有对应的权限，并在访问的业务口上做登录认证；否则会导致业务不通；此时需要开启用户的业务权限，并在浏览器上登录认证；

4、地址配置错误：系统 IP、网关或 DNS 配置错误，可能导致网络不通，访问系统页面失败；此时需要联系管理员。采用串口进入系统后台修改系统 IP 地址

第九章 日记审计

9.1. 初始化配置

日志审计员可以通过日志账号登录系统，可以对系统产生的工作日志进行查看和管理，包括：管理日志、系统日志、访问日志、文件交换日志、数据库交换日志、告警日志，并进行一些相关的审计管理，可信端和不可信端使用统一账户管理。

系统提供了默认用户管理员 adminlog，管理人员应及时更改系统初始日志审计员的用户名和口令。选择一台安装有浏览器的客户机，与可信端管理口相连，修改客户机 IP 地址，使其与可信端管理接口（处于同一个网段，可信端管理口初始值为

192.168.0.254/24）；在浏览器地址栏输入：https://192.168.0.254:10000 即出现可信端管理系统登陆界面；

在“用户名”一栏输入用户名 adminlog，在“密码”一栏输入其对应默认口令“admin*pwd”，在验证栏输入验证码。即可进入系统的日志审计模块。

9.2. 日志与审计

9.2.1. 管理日志

管理行为日志中记录了管理员的所有操作，可以根据查询条件来查看管理员对系统的操作。审计员还可以导出，清空日志。

点击“日志与审计”>“管理日志”，进入管理日志页面。

可根据查询条件搜索（包括管理员、IP、时间、消息、角色、级别、时间范围），查看管理日志的相关信息，

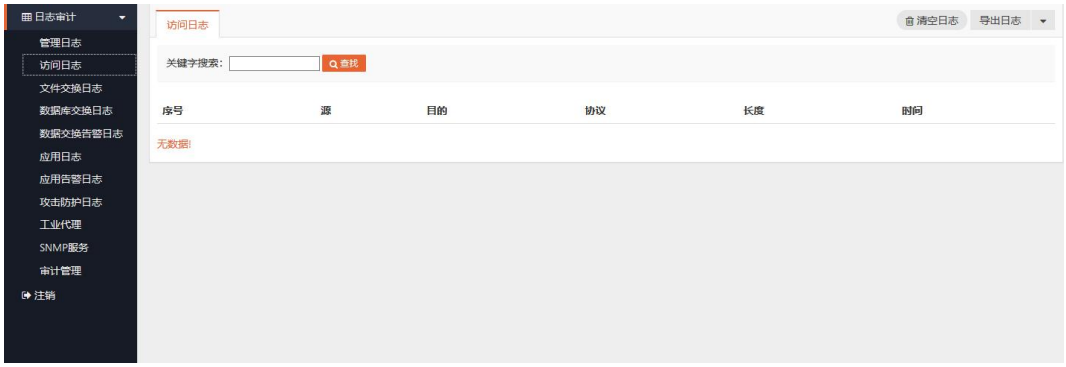
点击“清空日志”按钮，即可清空管理模块日志。

点击“导出日志”按钮，导出管理日志，可在下拉菜单中选择导出为 csv 格式、xls 格式、pdf 格式或 html 格式。

9.2.2. 访问日志

在代理模式下，系统提供访问日志查看，访问日志可查看了用户配置的代理类业务，可信端和不可信端的访问的访问记录。

用户切换到代理模式，登录到日志审计模块，点击“日志与审计”，然后点击“访问日志”，进入访问日志页面。



可根据关键字搜索，查看访问日志的相关信息，

点击“清空日志”按钮，即可清空访问日志。

点击“导出日志”按钮，导出访问日志，可在下拉菜单中选择导出为 csv 格式、xls 格式、pdf 格式或 html 格式。

9.2.3. 文件交换日志

文件同步日志记录了所有文件同步产生的日志，可以根据查询条件（外端业务 ID、目录、文件名、操作状态）来查询，查看文件同步同步多少文件，文件同步是否成功。

点击“日志与审计”>“文件交换日志”，进入日志页面。

可根据查询条件搜索（服务名称、源服务器 IP、目的服务器 IP、文件路径、文件名），查看文件交换日志的相关信息，可切换“可信端->不可信端”“不可信端->可信端”筛选同步方向的日志。

点击“清空日志”按钮，即可清空管理模块日志。

点击“导出日志”按钮，导出管理日志，可在下拉菜单中选择导出为 csv 格式、xls 格式、pdf 格式或 html 格式。

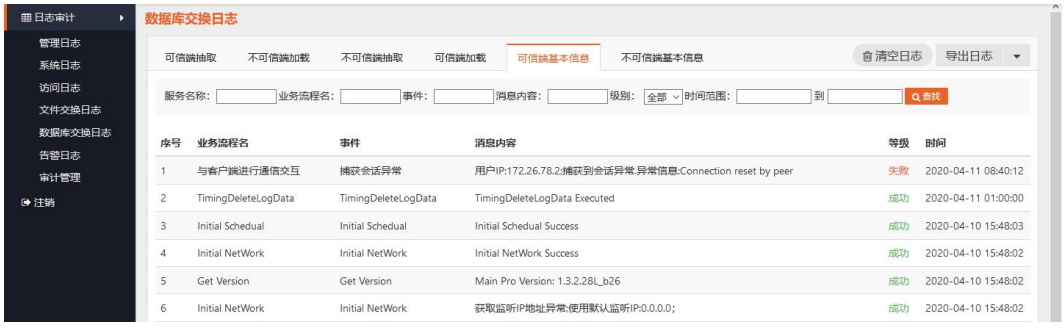
9.2.4. 数据库交换日志

数据库交换日志提供了数据库的抽取记录、加载记录和基本信息记录日志的查看。可切换“可信端->不可信端”“不可信端->可信端”筛选同步方向的日志。

数据库抽取日志记录了管理员对数据库的操作，可以根据查询条件（服务名称、数据流向、抽取表名、加载表名、时间范围）来查询数据库抽取日志。

数据库加载日志用于记录数据库同步服务的数据内容，可以根据查询条件（服务名称、数据流向、抽取表名、加载表名、时间范围）才查询同步记录。

数据库基本信息日志可以根据查询条件（服务名称、业务流程名、事件、消息内容、级别、时间范围）来查询，查看数据库状态是否正常。



9.2.5. 告警日志

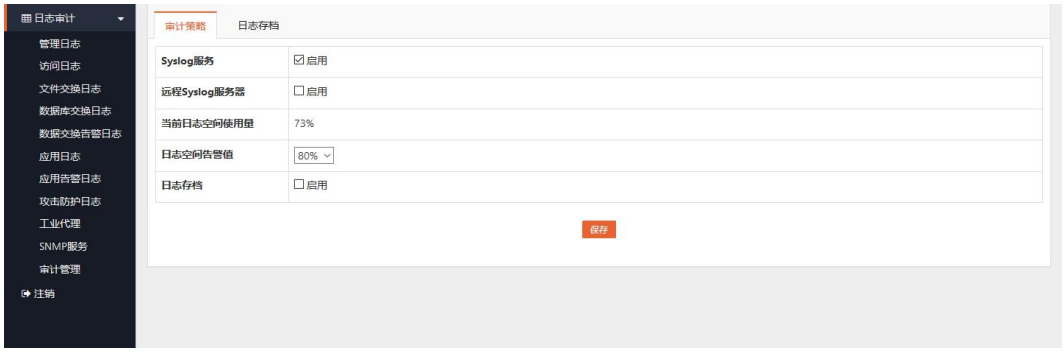
告警日志中记录了包括不能同步的文件、管道连接失败、资源配置失败等异常日志，可以根据查询条件（服务名称、方向、告警模块、消息、级别、时间范围）来对报警日志进行查询。

9.2.6. 日志设置

在日志设置页面中可以设置远程 syslog 服务器。syslog 是一个记录所有类型日志信息的标准系统，在各种主流操作系统上都可以安装 syslog 客户端和服务器。

日志模块可以查看当前日志空间使用率，并在过高时提供告警提示，对于超过预留空间大小的日志，系统会自动删除部分日志，或可手动存档到系统。

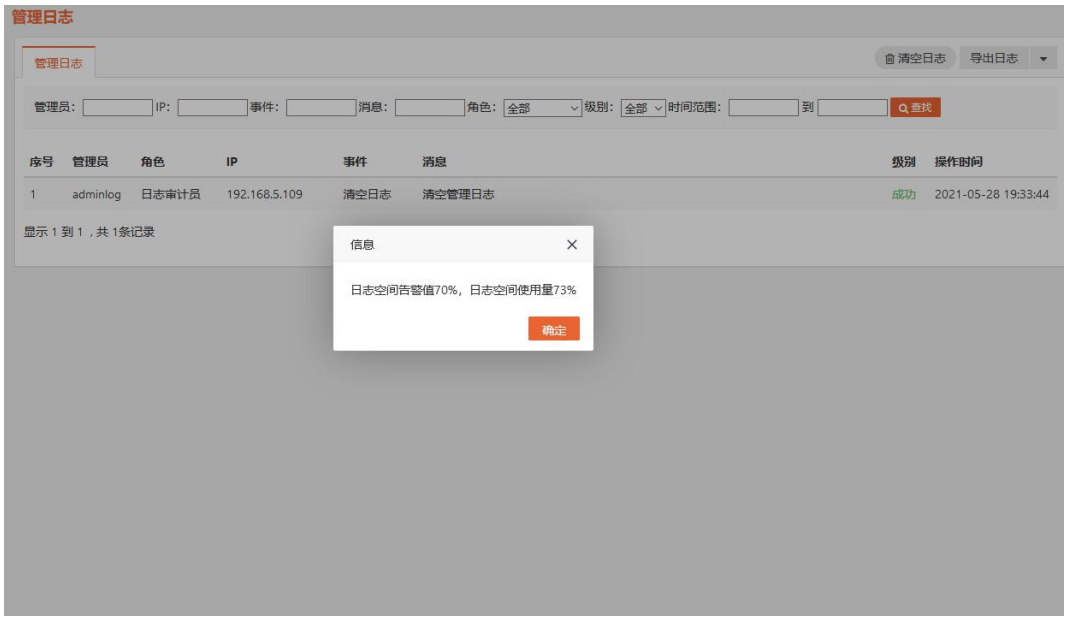
点击“日志与审计”>“日志设置”，进入日志设置。



勾选“启用 syslog 服务”开启可信端和不可信端 syslog 服务。输入远程 syslog 服务器的 IP 地址和端口。点击“保存”，修改配置。

通过把日志输出到外部 syslog 服务器，我们已经把一个重要的负担从 ViGap7.0 设备中分离出来，很大程度上减轻了设备的内存使用率和硬盘存储空间。

设置日志空间告警值，点击“保存”。当日志使用量超过告警提示值时，在使用日志审计员账号登录系统首页时，页面会弹出提示。

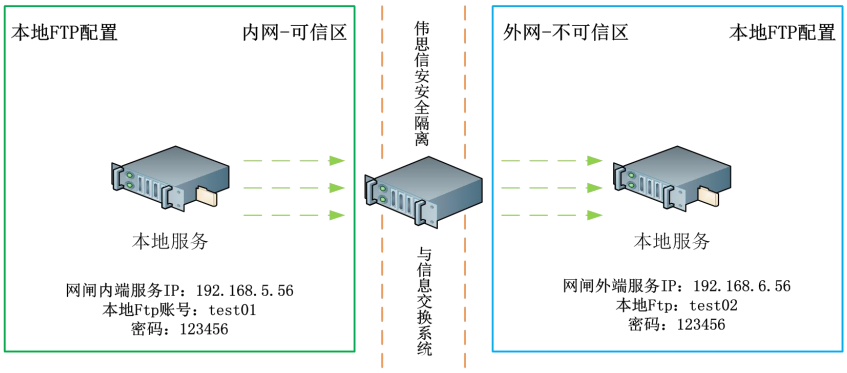


勾选启用日志存档，并设置周期性存档时间。系统会定时存档日志数据。进入“日志与审计”>“日志设置”，切换“日志存档”标签可查看。

第十章 典型案例

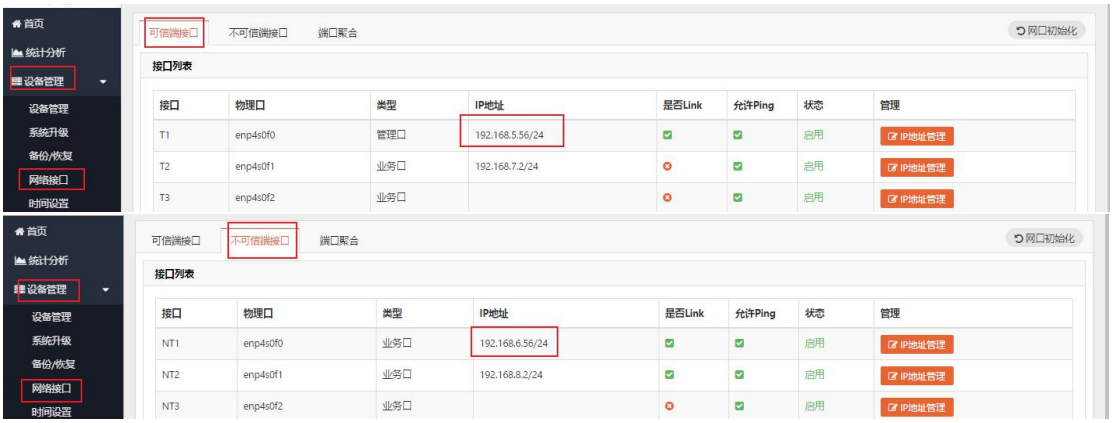
10.1. 本地文件同步（本地 FTP）

- **案例拓扑**



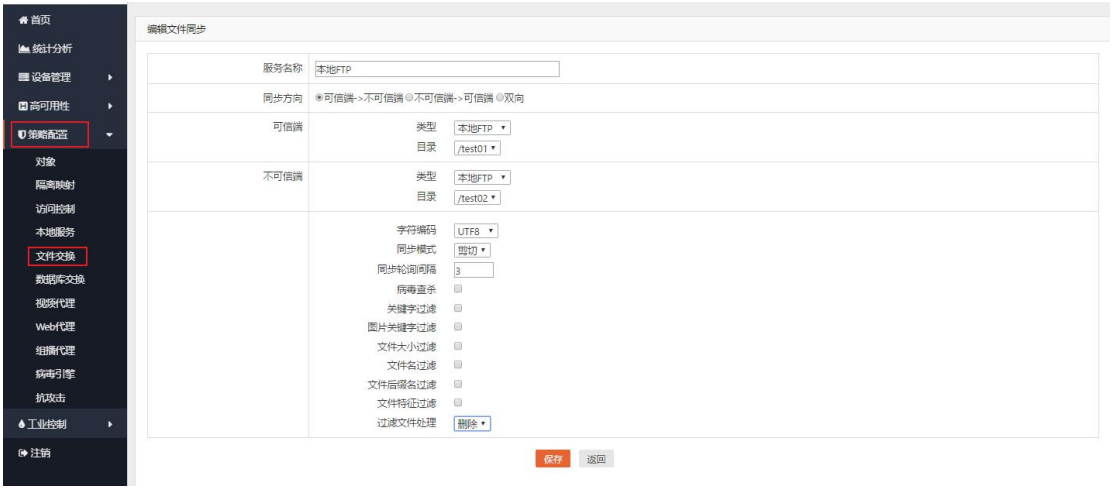
- **操作流程**

1、登陆页面选择“设备管理”>“网络接口”，配置可信端接口和不可信端接口 IP 并启用；这里配置可信端 IP 为 192.168.5.56，不可信端 IP 为 192.168.6.56；



2、登陆页面选择“策略配置”>“本地服务”，为可信端和不可信端添加 FTP，用户名：test01 密码：123456 并开启 FTP 服务

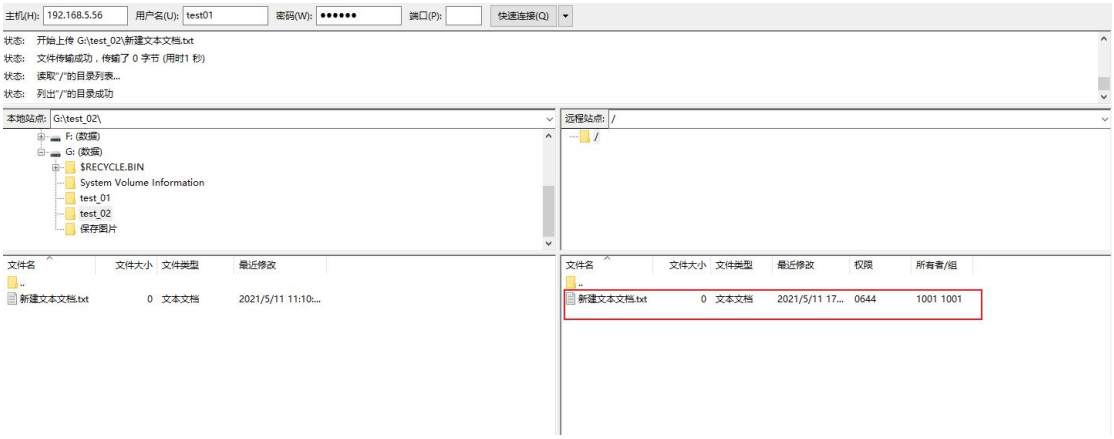
3、选择“策略配置”>“文件交换”，点击添加策略，按步骤填写好可信端和不可信端信息，点击保存；



- 类型：本地 FTP
- 同步模式：默认剪切
- 可信端目录：/test01
- 不信端目录：/test02
- 服务名称：自定义填写
- 同步方向：默认可信端—>不可信端

4、点击“点击启用”按钮，开启本地 FTP。

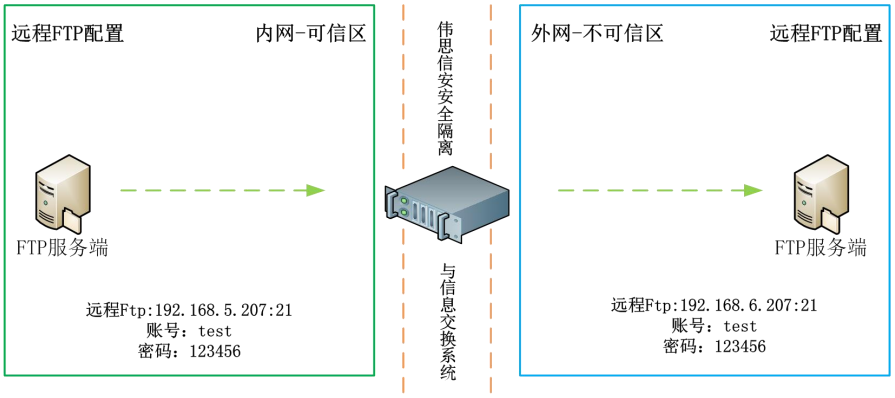
5、连接可信端服务器上传文件。输入 FTP 服务器 IP 地址：192.168.5.56，用户名：test01，密码：123456，点击“快速连接”成功后，点击本地文件，看到上传到可信端成功；



6、连接不可信端服务器查看文件传输。输入 FTP 服务器 IP 地址：192.168.6.56，用户名：test02，密码：123456，点击“快速连接”成功后，查看到文件已经同步到不可信端，点击文件可以从不可信端下载到本地。

10.2. 远程文件同步（远程 FTP 为例）

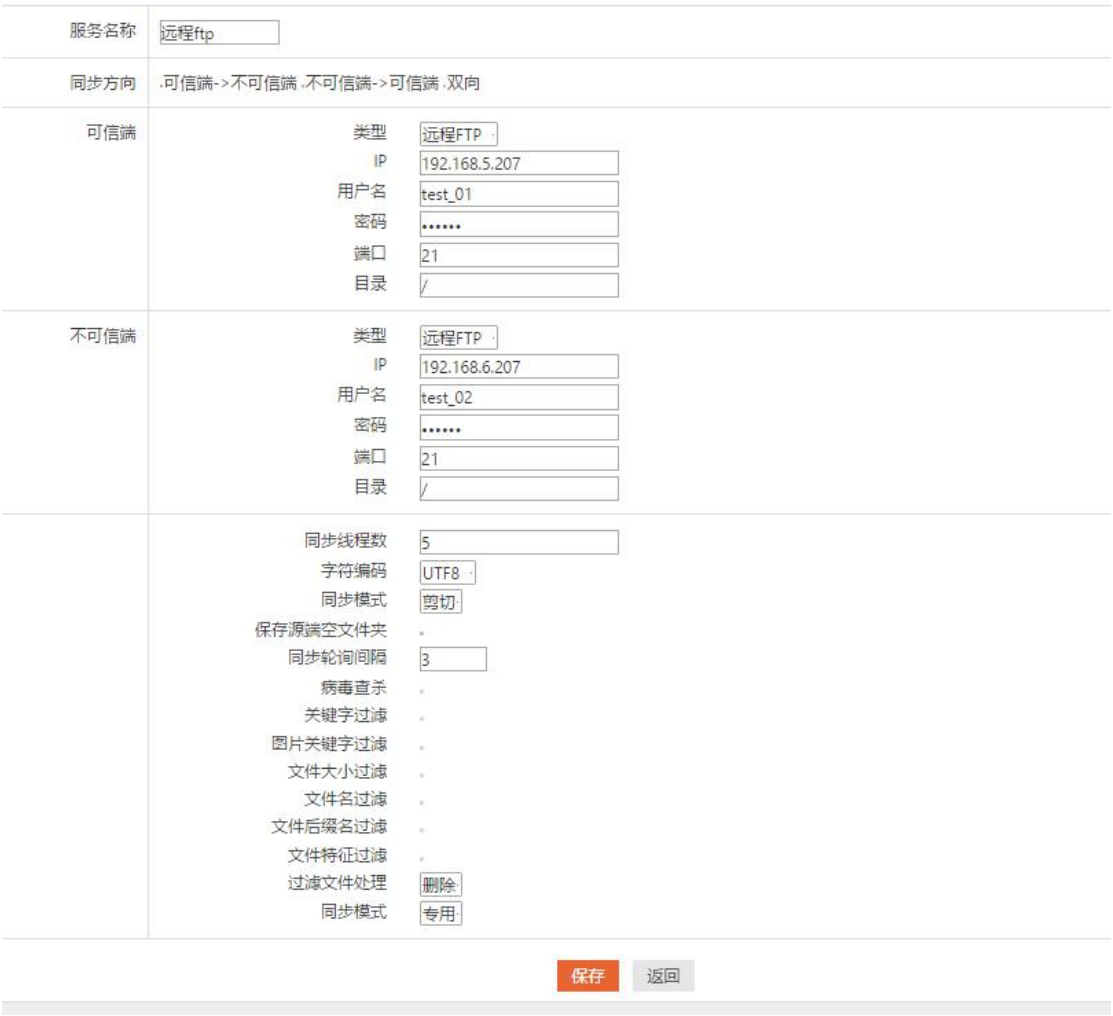
- **案例拓扑**



- **操作流程**

1、在内网 ip 地址为 192.168.5.207 的 FTP 服务器上建立用户：test_01 密码：123456，在外网 ip 地址为 192.168.6.207 的 FTP 服务器上建立用户：test_02 密码：123456；

2、登录界面，选择“策略配置”>“文件交换”，点击添加策略，添加一个远程 FTP 任务。按步骤填写好可信端和不可信端信息，点击保存；

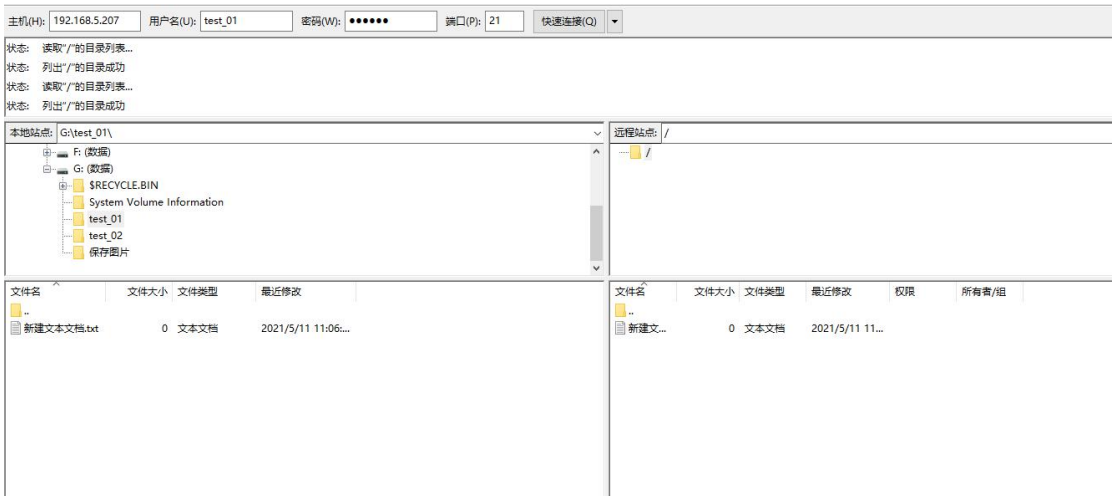


- 类型：远程 FTP
- 端口：21
- 同步模式：默认填“专用”
- 目录：默认都填“/”（即 FTP 根目录）
- 服务名称：自定义填写
- 同步方向：默认 可信端—>不可信端
- 可信端 ip：内网 ip 192.168.5.207
- 可信端用户名：test_01
- 不可信端 ip：外网 ip 192.168.6.207
- 不可信端用户名：test_02
- 过滤条件：默认不做过滤

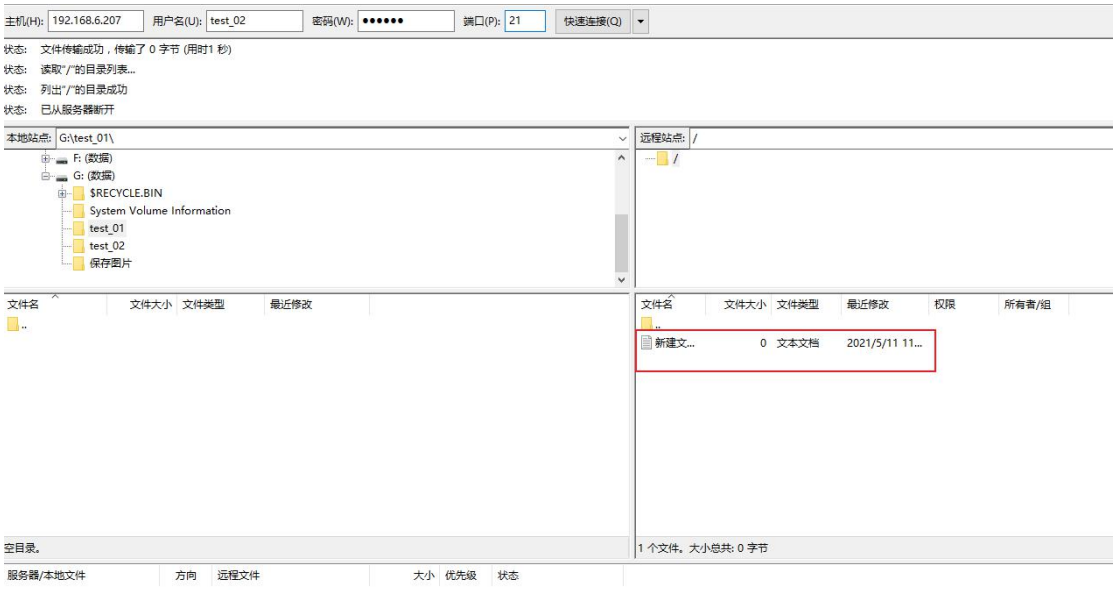
3、点击“点击启用”按钮，开启本地 FTP

4、连接可信端服务器上传文件。输入 FTP 服务器 IP 地址：192.168.5.207，用户名：test_01，密码：123456，点击“快速连接”成功后，点击本地文件上传，看到上

传到可信端成功；

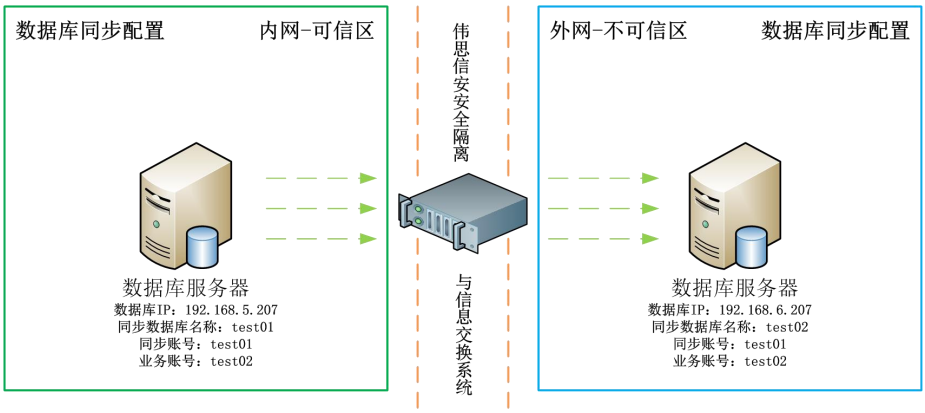


5、连接不可信端服务器查看文件传输。输入 FTP 服务器 IP 地址：192.168.6.207，用户名：test_02，密码：123456，点击“快速连接”成功后，查看到文件已经同步到不可信端，点击文件可以从不可信端下载到本地。



10.3. 数据库同步（MySQL 为例）

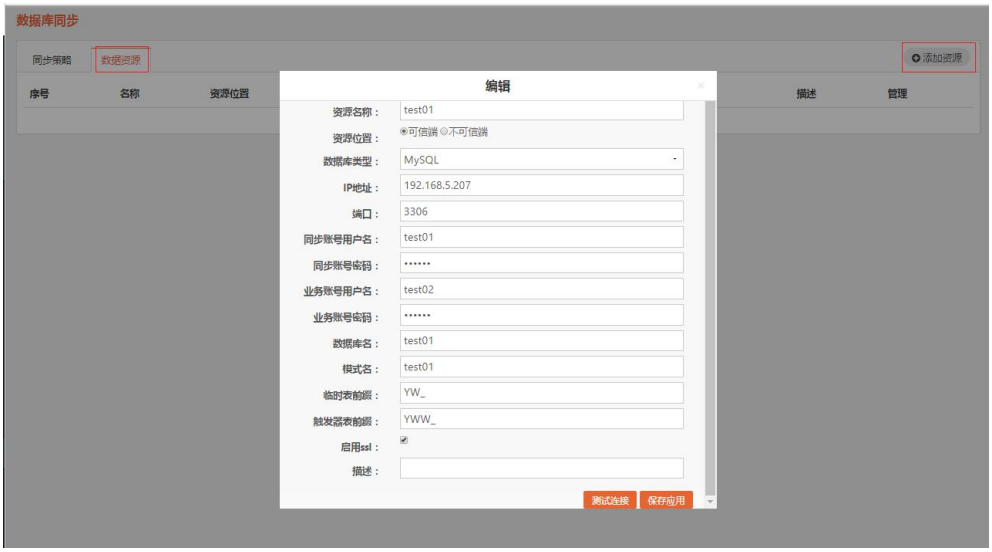
- **案例拓扑**



- **操作流程**

1、在 ip 为 192.168.5.207 的可信端服务器创建 mysql 数据库：test01，创建用户：test01　密码：123456，在 ip 为 192.168.6.207 的不可信端服务器创建 mysql 数据库：test02，创建用户：test02 密码：123456；

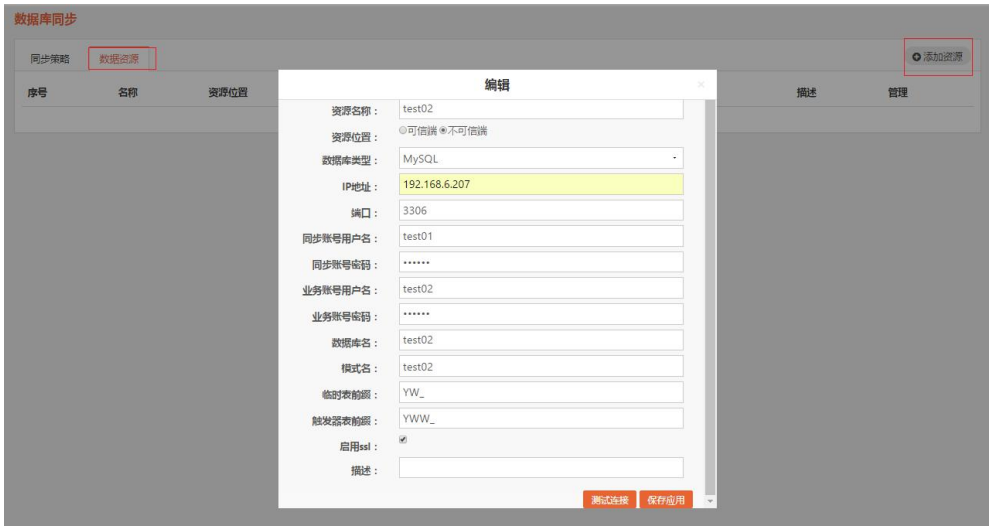
2、添加可信端资源 test01：选择“策略配置”>“数据库交换”，点击“数据资源”标签，添加资源，然后点击测试链接，最后点击保存应用；



- 资源名称：test01 自定义
- 资源位置：可信端
- 数据库类型：mysql
- Ip 地址：192.168.5.207
- 端口：mysql 数据库默认端口为 3306

- 同步账号用户名：test01
- 业务账号用户名：test02
- 数据库名：test01
- 模式名：test01 自定义
- 临时表前缀：在 test01 数据库中临时生成的表，可自定义，不能留空
- 触发器表前缀：在 test_02 数据库中临时生成的表，可自定义，不能留空

3、添加不可信端资源 test02：选择策略配置—>数据库交换—>数据资源，添加资源，然后点测试链接，再点击保存应用；

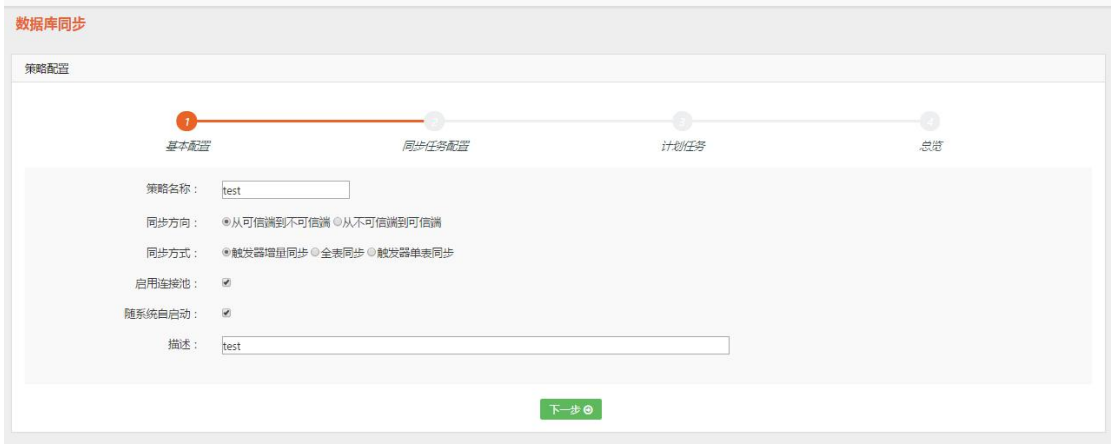


- 资源名称：test02 自定义
- 资源位置：不可信端
- 数据库类型：mysql
- Ip 地址：192.168.6.207
- 端口：mysql 数据库默认端口为 3306
- 同步账号用户名：test01
- 业务账号用户名：test02
- 数据库名：test02
- 模式名：test02 自定义
- 临时表前缀：在 test01 数据库中临时生成的表，可自定义，不能留空
- 触发器表前缀：在 test_02 数据库中临时生成的表，可自定义，不能留空

4、可信端与不可信端数据资源配置完成页面。

5、选择“策略配置”>“数据库交换”，在“同步策略”标签，点击“添加策略”按钮，添加一个数据库同步业务。

6、填写基本配置，包括名称、方向、方式、是否启用连接池和自启动，点击下一步；

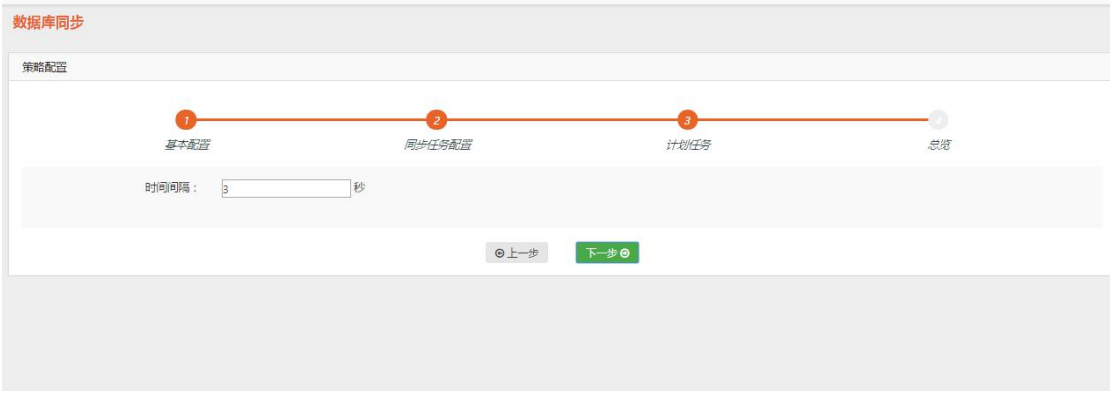


- 策略名称：test 可自定义
- 同步方向：从可信端到不可信端
- 同步方式：触发增量同步
- 描述：test 可自定义

7、填写同步任务配置，这一步主要是选择需要同步的数据，点击下一步；

- 源端数据资源选择：test01
- 目标端数据资源选择：test02
- 勾选需要同步到表或直接点击“智能匹配”按钮，点击“配置”按钮，可以选择双向同步，Where 过滤，操作白名单等等，这里采用默认配置；

8、填写计划任务，填写任务时间，点击下一步；



- 时间间隔：默认间隔 3 秒数据资源同步一次

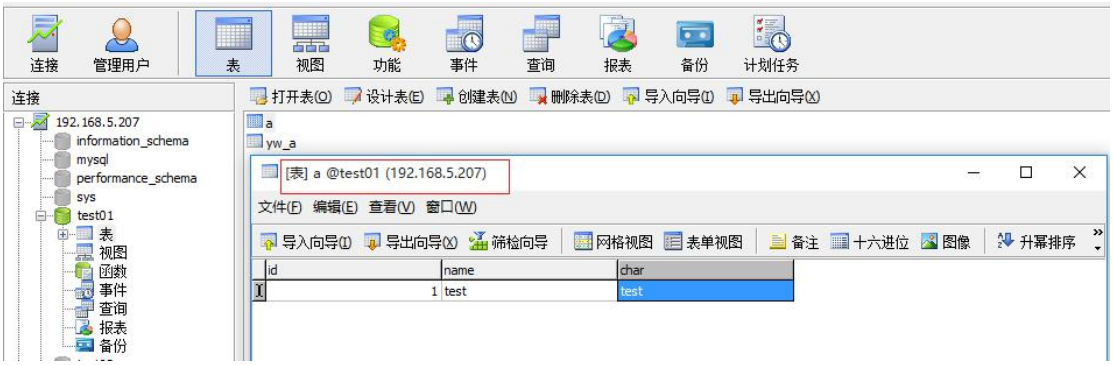
9、查看总览，确认无误后点击“保存应用”；

➢ 同步表配置：数据库 test01 的 a 表同步到数据库 test02 的 b 表

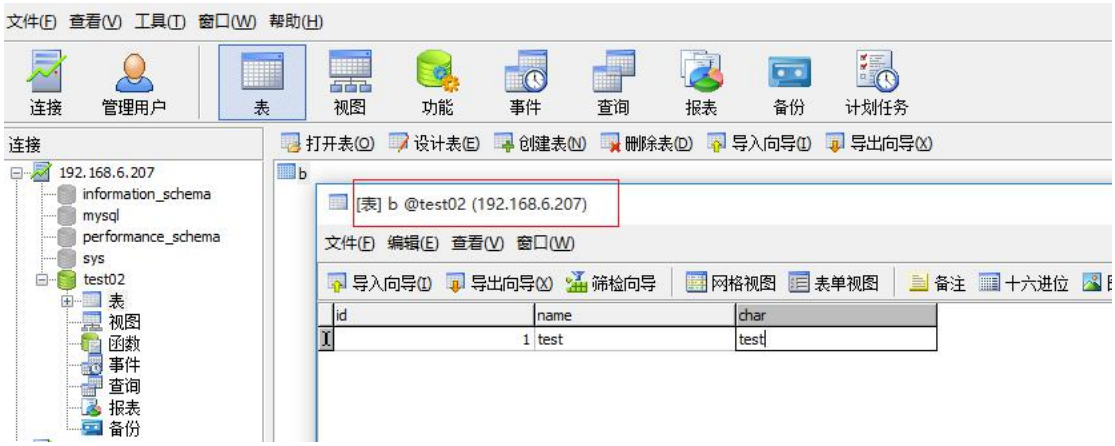
至此，任务配置结束

10、“点击启用”开启数据库资源同步；

11、可信端数据库 test01 的 a 表同步数据

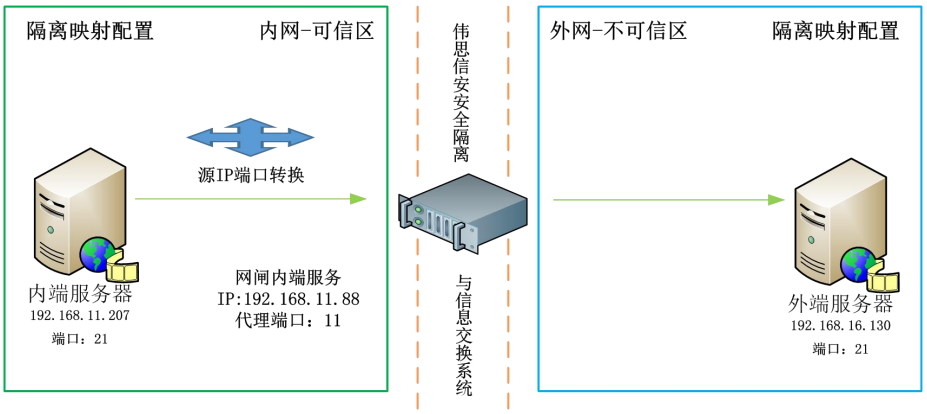


12、成功同步到不可信端数据库 test02 的 b 表



10.4. 隔离映射（FTP 映射为例）

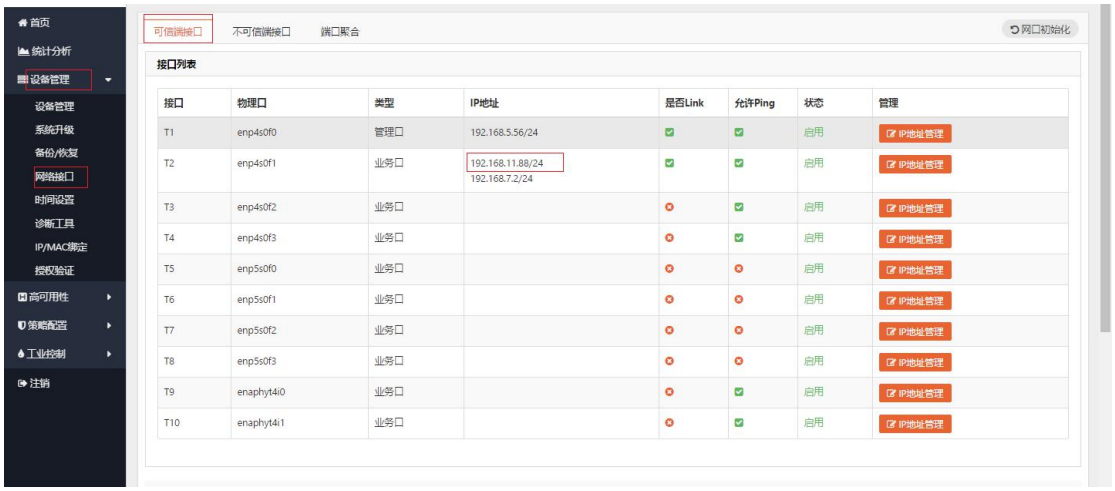
- **案例拓扑**



- **操作流程**

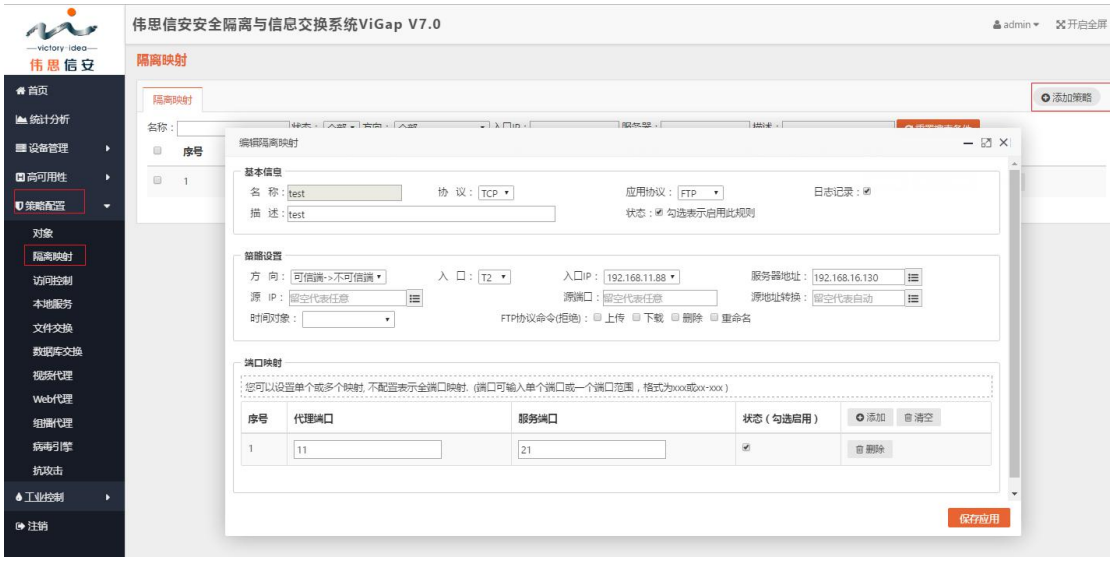
1、在外网准备一个 FTP 服务器 192.168.16.130，建立 FTP 账户 test_01 密码：123456；

2、在可信端业务口配置一个内网可达的 IP，登陆页面，选择“设备管理”>“网络接口”，配置可信端业务口（非管理口）ip：192.168.11.88，并启用；不可信端同理，在业务口配置一个外网 FTP 服务器可达的 IP：192.168.16.56，并启用；



3、登陆页面选择“策略配置”>“隔离映射”，点击“添加策略”按钮；

4、填写 FTP 隔离映射，点击保存应用；

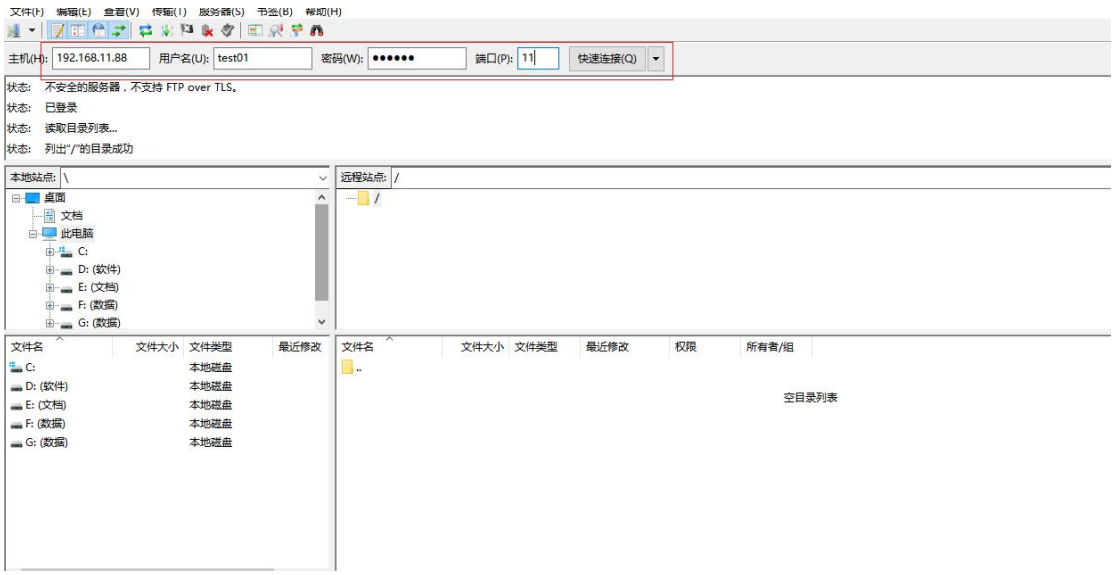


- 名称：test 可自定义
- 协议：tcp
- 应用协议：FTP
- 日志记录：勾选可开启应用记录
- 描述：test 可自定义
- 状态：勾选表示启用 FTP 应用协议
- 方向：可信端到不可信端
- 入口/入口 ip：选择配置好的可信端 ip 192.168.11.88
- 服务器地址：不可信端 ip：192.168.16.130
- 代理端口：11，可自定义，采用不常用端口
- 服务端口：21，填写 FTP 服务器真实端口

状态：勾选启用代理端口

5、“点击启用”按钮，开启 FTP 隔离映射

6、访问可信端业务接口地址，能连接到真实服务器地址，并可用成功上传和下载，表示 FTP 隔离映射连接成功。



10.5. 视频代理

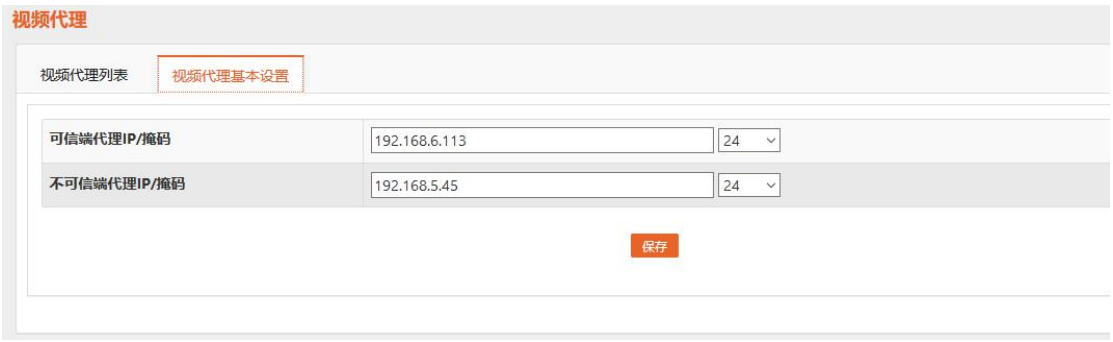
- **案例拓扑**

- **操作流程**

1、配置网闸可信端和不可信端的业务口：

可信端接摄像头或其他视频流服务器、不可信端接上报平台或播放客户端；例：可信端 eth2:192.168.6.113、不可信端 eth2：192.168.5.45；

2、配置网闸视频代理，进入“策略配置”>“视频代理”，切换到“视频代理基本设置”标签，填写上一步配置的可信端和不可信端 IP 做为代理视频 IP；例：可信端代理 IP：192.168.6.113；不可信端代理 IP：192.168.5.45；



3、视频代理配置：切换到“视频代理列表”标签，点击“添加代理”按钮：

- 代理名称、描述
- 代理方向：选择可信端到不可信端；
- 代理 IP：填写网闸的可信端视频代理 IP（上一步配置的可信端 IP）；例：192.168.6.113
- 代理端口：默认填写 5060 来做视频代理端口；例：5060
- 目标服务器 IP：填写上报平台（播放端）IP 地址；例：192.168.5.104
- 目标服务器端口：填写上报平台（播放端）端口；例：5060
- 信令通讯方式：选择“UDP”；
- 视频流格式：选择“CMS”；
- 视频厂商信令格式：选择“陆丰”；
- 视频编码格式：选择“3GP”

配置完成，点击保存；

4、回到摄像头配置页面，修改 SIP 服务器地址为网闸可信端地址；如：192.168.6.113

重新点击保存，返回观察上报平台，观察到上报平台出现摄像头注册信息和视频流信息，再点击“实时点播”是否有视频流传输，可以看到有数据接收进来，证明通过网闸代理成功；

注：上报平台这里采用 LiveCMS 监控流媒体服务器，这里不做描述；摄像头采用海康摄像头。