伟思信安 安全隔离与信息交换系统 ViGap V6.5 用户手册

版本	作者	起止日期	备注	审查
V1.0	章学宇	2022/01/15	初次编写	陈功湖
V1.1	章学宇	2022/05/15	功能新增	
V1.2	章学宇	2022/11/01	新增15版本功能	

目 录

第一章 系统概述	1
1.1. 系统简介	1
1.2. 名词解释	2
第二章 运行环境	2
2.1. 硬件运行环境	2
第三章 安装部署	3
3.1. 前置工作	3
3.1.1. 设备清单检查	3
3.1.2. 安装环境要求	3
3.1.3. 温度及湿度要求	3
3.1.4. 环境洁净度要求	3
3.1.5. 静电要求	4
3.1.6. 雷电/电磁要求	4
3.1.7. 安装台面检查	5
3.1.8. 安全注意事项	5
3.1.9. 安装工具准备	6
3.2. 设备上架	6
3.2.1. 安装到水平台面	6
3.2.2. 安装到标准机架	7
3.3. 系统部署检查	7
第四章 业务操作指南	8
4.1. 登录管理	8
4.1.1. 准备工作	8
4.1.2. 管理方式	8
4.1.3. Web 页面管理	
第五章 运维操作	9
5.1. 常见故障	9
5.1.1. CPU 高	9
5.1.2. 内存高	9
5.1.3. 网络异常	9
5.1.4. SYLOG 日志失效	
5.2. 运维指南	10
5.2.1. 日常运维	10
5.2.2. 应急处理	11
5.3. 注意事项	12
第六章 功能介绍	12
6.1. 初始化配置	12
6.2. 系统状态	13
6.2.1. 系统状态	13
6.2.2. 统计分析	14
6.3. 设备管理	15
6.3.1. 设备管理	15

6.3.2. 系统升级	19
6.3.3. 备份/恢复	19
6.3.4. 时间设置	21
6.3.5. 系统规则	22
6.3.6. API 管理	
6.3.7. 授权验证	24
6.4. 网络工具	25
6.4.1. 网络接口	25
6.4.2. 域名解析	
6.4.3. 诊断工具	
6.5. 高可用性	
6.5.1. 多机热备	
6.5.2. 虚拟 IP	
6.5.3. 双击热备状态	
6.6. 策略配置	
6.6.1. 对象	
6.6.2. 隔离映射	
6.6.3. 访问控制	41
6.6.4. 本地服务	
6.6.5. 数据交换	45
6.6.6. 业务代理	54
6.6.7. 工业控制	
6.6.8. 攻击防御	
第七章 用户管理	68
7.1. 初始化配置	
7.2. 用户管理	69
7.3. 证书认证	71
7.4. 安全配置	73
第八章 用户使用安全说明	74
8.1. 使用限制	74
8.2. 安全环境	76
8.3. 用户职责	77
第九章 日记审计	78
9.1. 初始化配置	
9.2. 日志与审计	79
9.2.1. 管理日志	
9.2.2. 访问日志	
9.2.3. 文件交换日志	80
9.2.4. 数据库交换日志	
9.2.5. 应用日志	
9.2.6. 告警日志	
9.2.7. 文件同步状态日志	
9.2.8. 工业代理日志	
9.2.9. 攻击防护日志	
9.2.10. 关键字过滤日志	

9.2.11. SNMP 服务	
9.2.12. 审计管理	
第十章 典型案例	
10.1. 本地文件同步(本地 FTP)	
10.2. 远程文件同步(远程 FTP 为例)	
10.3. 数据库同步(MySQL 为例)	
10.4. 隔离映射(FTP 映射为例)	
10.5. 视频代理	
10.6. Modbus 工业代理	

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 ViGap V6.5(以下简称 ViGap V6.5)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 ViGap V6.5 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。

在核心的 GAP 电子开关隔离芯片上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 FPGA 设计硬件基片,该芯片具有百万门电路以及多路 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

第1页共104页

或单独购买模块。

采用专利技术的应用层安全防御系统,ViGap V6.5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,ViGap V6.5 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,ViGap V6.5 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。

ViGap V6.5 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。

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, ViGap V6.5 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。

参数	参数值
输入	Input:100~240V AC Freq:47~63Hz
温度	0°C∼40 °C
湿度	10%~90%(无冷凝)
电源	220V 交流电

ViGap V6.5 运行环境应满足以下标准:

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: 0°C ~ 40°C
- 2) 湿度: 10%~90%(无冷凝)

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

第3页共104页

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;
- 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;
- 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:

第4页共104页

- 1) 对供电系统采取有效的防电网干扰措施;
- 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;
- 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

第5页共104页

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;

第6页共104页

- 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:

- 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;
- 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;
- 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:



3.3.系统部署检查

1) 连接电源线到 ViGap V6.5 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 ViGap V6.5 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 ViGap V6.5 的可信端接口,连接另一端到内网交换机的网口;
- 连接网线的一端到 ViGap V6.5 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 ViGap V6.5 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 业务操作指南

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

- ▶ ViGap V6.5 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";

第8页共104页

- 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:

 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

第9页共104页

起。如: IPMAC 绑定、连接数限制等;

 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。

5.2. 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。

- 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;
- 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 ViGap V6.5 分为可信端和不可信端,分别连接到内 网和外网;
- 2) ViGap V6.5采用 B/S 模式管理,通过可信端管理口分别对 ViGap V6.5两端进行管理。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;

and a second	
A CARLES AND A CARLES A	
•••••••••••••	ルスッ住田住立
	-victory-idea TIGX
a	
	伟思信安安全隔离与信息交换系统ViGap
	▲ 用户名
	▲ 密码
	验证码 371723
	登录
	© 2008-2022 0 All Rights Reserved.
	为达到最佳体验效果,推荐下载使用谷歌浏览器:Chrome,

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",首次登录需修改密码。在验证栏输入验证码,首次登录系统需 修改登录密码。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。

 ♣ 首页 ▲ 统计分析 ■ 设备管理 	9.3% CPU使用率	58.1% 内存使用率	1% 磁盘使用率	801/700000 并发数	设备型号: ViGap 系统版本: 6.5.9.15		2022年11月04日 星期五 05:35:28	
,國络丁貝	7770070404				文件交换模块版本: 1.0.0.2.12	Ks	(本许可: 正式版	
	个可信端系统状态				数据库交换模块版本: 1.3.2.28	b36 招	权天数: 永久	
目向可用性	7.3%	42.3%	1%	794/700000	开机时长: 4天6时7分48秒	1	控模块: 运行中	
♥策略配置	CPU使用率	□ □	磁盘使用率	开发数				
▲工业控制	•							
☞ 退出		■記計 ▼ 37 05:16:06 05:17:16 57 05:16:06 05:17:16	05:18:30 05:19:41 05 05:18:30 05:19:41 05	52052 052205 052317 52052 052205 052317	052427 052540 052652 052 052427 052540 052652 052	08 05:29:19 05:30 08 05:29:19 05:30	30 05:31:39 05:32:51 30 05:31:39 05:32:51	(法) 不可信調 05:34:01 05:35:1 05:34:01 05:35:1

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 ViGap V6.5 可信端 和不可信端目前的状态。

											🚨 adm	nin 👻 🗙	开启全
「信端系统状态				设备信	18.								
9.3% 58.1% U使用率 内存使用率	1% 磁盘使用率	957/700000 并发数		设备型号: ViGap 系统版本: 65915			2022年11月04日 星期五 05:36:03						
				文件3	24年, 0.5. と換模块版	.9.15 反本: 1.0.0).2.12		版本i	午可: 正元	优版		
可信端系统状态				数据库	1 交换模均	快版本: 1.	3.2.28L b3	6	授权	天数: 永久	L.		
7.3% 42.3%	1%	485/700000		开机时长:4天6时7分48秒			工控制	蕈块:运行	ф				
U使用率 内存使用率	磁盘使用率	开发数											
経済合計量 正行・下行 上行(KB) 40 20 10 	05:19:11 05:20:20 05:2	21:35 05:22:46 (05:23:54 0	05:25:07	05:26:20	05:27:31	05:28:46	05:29:59	05:31:08	05:32:18	05:33:30	信讀 不F	J信講 05:35

实时更新显示 ViGap V6.5 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,可对系统状态进行实时查看

系统监控显示 ViGap V6.5 的可信端和不可信端 CPU、内存、负载的系统实时展示和7天内的历史数据统计,便于查看和分析。

	实时数据 11/04	11/03 11/02 11/01 10/31	10/30 10/29
U	可信論 不可信識	内存	-〇- 可信端 -〇- 不可信端
100		100	
80 -		80-	
60 -		60	· · · · · · · · · · · · · · · · · · ·
40 -		40	
20-1		20 -	
0 -04 05:09:29	0 0 11-04 05:15:42 11-04 05:21:59 11-04 05:28:20 11-04	05:34:39 11-04 05:09:29	11-04 05:15:42 11-04 05:21:59 11-04 05:28:20 11-04 05:34:3
0 1-04 05:09:29 言端负载	11-04 05:15:42 11-04 05:21:59 11-04 05:28:20 11-04 	0 05:34:39 0 不可信端负载	11-04 05:15:42 11-04 05:21:59 11-04 05:28:20 11-04 05:34:3
0 -04 05:09:29 言端负载	11-04 05:15:42 11-04 05:21:59 11-04 05:28:20 11-04 	⁰ ⁰ ⁰ ⁰ ⁰ ⁰ ⁰ ⁰ ¹	11-04 05:1542 11-04 05:21:59 11-04 05:2820 11-04 05:34:3

会话连接基于 IP 会话连接,展示可信端和不可信端的连接资源数据信息和 top

排名,支持实时信息展示和和7天内的历史数据统计

			实时数据 11/04	11/03 11/02 11/0	10/31 10/30	10/29			
				可信講 7	下可信請				
000 800 600 400 200		11		11	1				1
0	11-04 05:12:44	11-04 05:15:16 11-04	05:17:49 11-04	5:20:27 11-04 05:23:0	5 11-04 05:25:40	11-04 05:28:20	11-04 05:30:56	11-04 05:33:30	11-04 05:30
0 1-04 05:10:07 可信端	11-04 05:12:44	11-04 05:15:16 11-04 信端Top 排名 不可	05:17:49 11-04। 信端Top 排名	05:20:27 11-04 05:23:0	5 11-04 05:25:40	11-04 05:28:20	11-04 05:30:56	11-04 05:33:30	11-04 05:30
0 1-04 05:10:07 可信端 网络	11-04 05:12:44 不可信端 可 协议	11-04 05:15:16 11-04 「信識Top 排名 不可 源地址		ງຣະ20:27 11-04 ບໍ່ຣະ23:0	5 11-04 05:25:40 目标地	11-04 05:28:20	11-04 05:30:56	11-04 05:33:30	11-04 05:3
0 04 05:10:07 可信講 阿络	11-04 05:12:44 不可信端 可 协议 udp	11-04 05:15:16 11-04 信識Top 排名 不可 源地址 192.168.5.112:13	05:17:49 11-04 (信端Top 排名 7	95:20:27 11-04 05:23:0	5 11-04 05:25:40 目标地 192.16	11-04 05:28:20	11-04 05:30:56	11-04 05:33:30	11-04 05:3
0 1-04 05:10:07 可信講 阿姆 Ipv4	11-04 05:12:44 不可信端 可 协议 udp tcp	11-04 05:15:16 11-04 (信談Top 排名 不可 避地址 192.168.55.112:12 192.168.15.109:6	05:17:49 11-04+ 信端Top 排名 7 1651	js.20.27 11-04 ojs.23.0	5 11-04 05:25:40 目标地 192.16 192.16	11-04 05:28:20 tht: 86.5.255:137 88.15.187:10000	11-04 05:30:56	11-04 05:33:30	11-04 05:3
0 1-04 05:10:07 可信踌 ipv4 ipv4 ipv4	11-04 05:12-24 不可信講 可 协议 2 1 (14) 1 (14) 1 (14)	11-04 05:15:16 11-04 信識Top 排名 不可 避地址 192.168.5.112:13 192.168.15.109:0 192.168.15.109:0 192.168.15.109:0 192.168.15.109:0	05:17:49 11-04 H 信講Top 排名 7 1651 6172	11-04 05:23:0	5 11-04 05:25:40 目标地 192.16 192.16 192.16	11-04 05:28:20 tht 88.5.255:137 88.15.187:10000 88.15.187:10000	11-04 05:30:56	11-04 05:33:30	11-04 05:

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。

	WERT VERYON NORTHAL VELOCIEDE BELAVIE
当前模式	安全通道
模式选择	○ 应用機式 ⑥ 安全通道
安全通道设置	接 []: 全选 重置 [] T1(enp2s0) [] T2(enp3s0) [] T3(enp4s0) [] T4(enp5s0) [] T5(enp6s0) [] T6(enp7s0) [] T7(eno1) [] T6(eno2) [] C1 [] C2 [] P地址/子网境码: [] 92.11.1/24 stp生成树协议: ④ 原用 ○ 景用
	接口: 全选 重度 NT1(enp2s0) NT2(enp3s0) NT3(enp4s0) NT4(enp5s0) NT5(enp6s0) 2 NT6(enp7s0) NT7(eno1) NT9(eno2) C1 2 C2 P地址/子网编码: 1921.1.2/24 stof+成树协议: 全局用 〇葉用

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。

安全通道:选择透明模式需要配置桥接口。勾选"安全通道"。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;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、安全通道模式切换需要花费10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

重启系统	切换模式	恢复出厂设置	关闭系统	系统名称	反向远程管理	服务状态
注意:重启系	统将中断当前操	作,请谨慎操作				
					A Tours	
					· 望居系统	

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

设备管理								
重启系统	切换模式	恢复出厂设置	关闭系统	系统名称	反向远程管理	服务状态		
注意:恢复:	出厂设置后:							
1、管理口	[T1) IP为: 192.	168.0.254/24						
3、不可信歸	(NT1) IP为: 1	192.168.10.254/24						
3、所有日记	将被清空							
4、备份在服	务器上的配置文	件和信息将被清空						
5、所有已裔	置项将被重置							
6、设备将自	动重启							
					つ恢复出厂设	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

设备管理							
重启系统	切换模式	恢复出厂设置	关闭系统	系统名称	反向远程管理	服务状态	
注意:关闭系	统将中断当前操	作,请谨慎操作					
						_	
					○ 关闭系统		

点击"设备管理"中的"关闭系统"模块,点击下方按钮,系统关闭。

6.3.1.5. 系统名称

设备管理	
重启系统 切换模式	恢复出厂设置 关闭系统 条编名称 反向远程管理 服务状态
可信端主机名	ViGap-T
不可信端主机名	ViGap-NT
设备型号	ViGap
	☑ 确认修改

点击"设备管理"中的"系统名称"模块,可对系统可信端和不可信端的名称进行修改。

6.3.1.6. 反向远程管理

系统不可信端可连接到一台远程服务器的 SSH 服务,并通过服务器反向连接到系统端的指定端口,实现远程运维功能;

点击"设备管理"中的"反向远程管理"模块,输入服务器的连接参数。并定义 好系统不可信端的连接端口和允许访问时间,点击"保存配置"生效。

重启系	统 切换模式	恢复出厂设置	关闭系统 系统名称	反向远程管理服	务状态			
反 务器均	也址:	€重置搜索条件						O 添
序号	服务器地址	服务器端口	远程管理端口	开始时间	结束时间	状态(时间范围内)	管理	
1	192.168.12.57	22	22225->22224->22 √ 20001->20002->10001 √	2022-06-20 00:00	2022-06-24 00:00	启动	☞编辑	會删除

家号 服务 SSH	服务信息					
						^
192. 服务	吟器地址: 192.168.12.57	服务器端口:	22	密码: •••••••	•••••	11 册除
开始	台时间: 2022-06-20 0	0:00 结束时间:	2022-06-24 00:00	状 态: 🗹 勾选将在持	旨定时间范围内启动	
远程制	管理端口					
序号	号 远程端口	监控端口	本地端口	状态 (勾选启用)	◎添加 會清空	
1	22225	22224	22		會 删除	
2	20001	20002	10001		自 删除	
3	32225	32226	22		☆ 删除	

- ▶ 服务器地址:远程(公网)服务器地址
- ▶ 服务器端口:远程(公网)服务器端口
- ▶ 服务器密码:远程(公网)服务器 SSH 连接密码(默认用户 root)
- ▶ 开始/结束时间:允许管理时间
- ▶ 远程端口:远程(公网)服务器反连端口
- ▶ 监控端口:服务状态监测端口
- ▶ 本地端口:自身 SSH 端口

6.3.1.7. 服务状态

设备管理

点击"设备管理"中的"服务状态"模块,可对系统主要模块状态进行查询

信系统 切换模式	t 恢复出厂设置 关闭系统 系统名称 反向远程管理 <mark>服务状态</mark>
业代理服务	运行中
数据库服务	运行中
文件同步服务	已停止
WEB服务	运行中
SH服务	运行中

6.3.1.8. 注销登录

在系统侧边栏最下方,点击"退出",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。

统升级		
可信端系统升级	不可信益	·····································
应用升级		
	升级包版本:	6.5.9.15
	升级包日期:	2022-10-28 10:09:44
	升级包MD5:	2293738fcdc962b0b637c7938db7c915
	应用升级包:	▲ 上传应用升级包
组件升级		
	组件升级包:	▲ 上传组件升级包

注:

升级失败则提示相关信息,升级成功需要重启才生效。 需区分对应升级包,命名格式为"upgrade.rootfs-xxx_v6.5.9.x"为应用升级包; 命名格式为"upgrade-visec-x""upgrade-usr""upgrade-webapp"为组件升级包。 多个升级包建议升级后统一重启

6.3.3. 备份/恢复

在 ViGap V6.5 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。

备份配置	恢复配置						
	位置:	全部 ~					
	备份区域:	全部 ~)				
	选择目标位置:	●备份到本地 〇备份到服	务器 〇以上两者				
	加密备份:	◎是○否					
				确认			
序号	名称	大小	位置	区域	描述	备份时间	管理

- 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。
- ▶ 加密备份:可选备份是否加密,默认选择"是"。
- 备注:本地加密备份完成会在下载可信端和不可信端各一个加密文件,文件名为 "T/NT-config.backup-当前日期";不加密备份则下载源 json 格式配置

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

名心/桁信

恢复配置可把本地或服务器上已备份的配置上传至 ViGap V6.5,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。

备份面	置 恢复配置							
	位置:	全部 ~						
	恢复区域:	全部						
	本地备份文件上传:	▲ 选择要上传的文件						
			121				1	
序号	名称		大小	位置	区域	描述	备份时间	管理
1	ALL-config-backup-20	210513151602.gz	2970	全部	全部	test	2021-05-13 15:16:02	自删除 ▲下载 つ恢复

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

首份配定	1 秋夏毗直							
	位置: 全部 备份区域: 全部 选择目标位置: ④ 备份到本	✓ ✓ 地 ○ 省份到服务器 ○以	上两者		确认			
序号	名称		大小	位置	区域	描述	备份时间	管理
1	ALL-config-backup-20210513151	602.gz	2970	全部	全部	test	2021-05-13 15:16:02	自制除 山下載 り恢复

- 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. 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。

时间设置	
日期和时间设置时间服务器同步	
可信端当前时间: 2022-01-18 13:48:26 不可信端当前时间: 2022-01-18 13:48:26 系統日期: 2022 年 01 マ 月 18 マ 日 系統时间: 13 マ 时 48 マ 分 26 マ 秒	
管理机时间: 2022-01-18 13:48:28 O 更新管理机时间到设备时间	

时间设置					
日期和时间设置时间服务	器同步				
开启可信端NTP服务: 上一级NTP服务器地址:	☑ 192.168.5.109 ● 添加	會删除			
开启不可信端NTP服务: 上一级NTP服务器地址:	☑ 192.168.6.109 ●添加	自删除			
			保存		

- ▶ 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。

6.3.5. 系统规则

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。

在访问控制列表可以查看绑定列表,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;

注: 在使用该功能前,请将当前管理主机添加到 IP/MAC 绑定列表,否则可能导致 添加其他主机后,当前主机无法访问管理系统。

7 号	名称	IP地址	MAC地址	描述	管理
	test	192 168 5 109	00-50-56-C0-00-08		C 200 0 250

访问控制				编辑	添加IP/MAC绑定
方问控制列	表		名称	test2	
序号	名称	IP地址	IP地址	格式 10.10.10.10	
1	test	192.168.5.1	MAC地址		8 含粉涂
			描述	请输入描述	
				确认	

- ▶ 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. ;
- ▶ 描述:描述不限制,可以填写,也可以不填写。

6.3.6. API 管理

系统的使用状态查询,策略配置等服务支持 API 调用,调用 API 需做认证。进入"设备管理">"API 管理"页面,可创建 API Key 使远程主机认证调用。

命名 Key 名称,选择需要调用的业务模块权限,填入调用的主机 IP 地址,点击"创建"按钮,创建 公钥和私钥密码对。

建API Key	创建成功	×
注		
est	恋匙仅显示次,遗失后不可找问, 请务必妥善保存	E词,策略配置等服务。通过 API文档 查看
限设置(可多选)		
运行状态 🚽 网络 🗌 重启设备 🗌 对象 🗌 规则策略	Access Key	i虑建议为 API key 绑定ip,每个 API key 最
王控自学习	f86b99e1-08a9e57f-ebd3a746-snysq 复制密钥	58.1.1,192,168.1.2
定ip地址(选填)	Sercet Key	
	vy3pera-oenczbf-j9qxau7-ken0f 复制增明	
	权限设置	
	运行状态网络	
创建	温馨提示	
	◎ 请不要泄漏您的 Access Key 和 Secret Key ,以免造成资产损失	

系统提供了 API 接入的操作步骤说明,接口类型支持和示例文档。可在 "API 文 档"模块处查看和下载。

ALIX ALIX	1 101C				
API简介					
 欢迎使用安全隔 此文档是安全隔 您可以通过点击 您可以通过点击 	高商与信息交换系统 API! 高商与信息交换系统API的II 击下方链接下载API接口说明 初文档和示例	ŧ一官方文档,API提供的能力到 到文档	*在此持续更新,请大家及时	XÌÌ.	
接入准备					
接口类型					
签名认证					

注:

1、最多创建 20 组 API key

2、请不要泄漏您的 API key,以免造成资产损失。出于安全考虑,建议为 API key 绑定 ip,每个 API key 最多绑定 20 个 ip 地址。多个 IP 地址用半角逗号分隔,如 192.168.1.1,192.168.1.2

3、每个请求必须使用您的 API Key 进行签名验证

6.3.7. 授权验证

ViGap V6.5 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

第 24 页 共 104 页

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。

进入"设备管理">"授权验证"页面,可进行工业模块的注册文件下载和授权。 对为激活工业模块的系统,点击工控注册的"注册文件下载"按钮,下载序列号文件, 文件名为"icp_license.txt";在系统"点击上传授权文件"按钮,上传工控授权文 件,文件名为"icp.lic",注册工业模块。

	d and a
单位名称	
联系电话	
单位座机	
单位地址	
邮箱地址	
购买日期	
单位联系人	
所在部门	
供应商	
授权信息	设备行册号: 4686042A60613BF28A5494E1265F143C 授权 要 : 試明版 已邮理时间: 0天0-0413分300 授权 天教: 30天
授权文件	▲ 后走上场援权文件
1402100	

6.4. 网络工具

6.4.1. 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。

6.4.1.1. 接口初始化

当需要自定义默认管理 IP 或接口顺序时,可在"网络工具">"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	物理口(可拖拉调换)	类型	ip地址	Link状态 C刷新
C1	enp1s0f0	通道口 ~		UP
C2	enp1s0f1	通道口 ~		UP
T1	enp4s0f0	管理口 ~	192.168.10.254/24	UP
T2	enp4s0f1	业务口 ~		UP
Т3	enp4s0f2	业务口 ~		DOWN
T4	enp4s0f3	业务口 ~		DOWN
T5	enp5s0f0	业务口 ~		DOWN
T6	enp5s0f1	业务口 ~		DOWN
T7	enp5s0f2	业务口 ~		DOWN
Т8	enp5s0f3	业务口 ~		DOWN
Т9	enaphyt4i0	业务口 ~		DOWN
T10	enaphyt4i1	业务口 ~		DOWN
<mark>示:</mark> 、此操作将	把上面配置设为系统默认配置,	恢复出厂设置后	生效	□ 同步为当前配置

- ▶ 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"心跳口""管理口""业务口";其中不可信端只有"心跳 口"和"业务口"。"心跳口"用于双机心跳检测,可配置通讯地址;"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或重启后生效;

6.4.1.2. 网络接口查看

进入"网络工具">"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。

第 26 页 共 104 页

们列表							
接口	物理口	类型	IP地址	是否Link	允许Ping	状态	管理
T1	enp3s0	管理口(允许业务)	192.168.15.37/24 192.168.11.137/24	2	2	启用	☞ IP地址管理
Т2	enp4s0	业务口	192.168.7.37/24	0		启用	C IP地址管理
ГЗ	enp5s0	业务口		0		启用	☞ IP地址管理
Γ4	enp6s0	业务口		0		启用	C IP地址管理
r5	enp7s0	业务口				停用	☞ IP地址管理
Г6	enp8s0	业务口		0		停用	C IP地址管理
7	enp2s0f1	业务口		0		启用	☞ IP地址管理
8	enp2s0f0	业务口		0		启用	C IP地址管理
oond0	T5 T6	聚合口	192.168.5.37/24 2001::37/64			启用	C IP地址管理

- ➢ 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。

6.4.1.3. IP 地址管理

进入"网络工具">"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。

伟思信安安全隔离与信息交换系统 V6.5-用户手册

可信端接口	不可信端接口	端口景			T2编辑			0	网口初始
接口列表			状态:	启用					
接口	物理口	类型	IP地址:	类型	IP地址/子网掩码	启用VRRP	⊙添加IP	管理	
T1	enp1s0	管理口		IPV4 -	192 168 5 100/24		自删除	☞ IP地址管理	
T2	enp2s0	业务口			1021100101100/21			@ IP地址管理	
T3	enp5s0	业务口	允许Ping:					I IP地址管理	
Т4	enp6s0	业务口	带外管理:					C2 IP地址管理	
Т5	enp7s0	业务口	VHID组:					☑ IP地址管理	
T6	enp8s0	业务口			确认			☑"IP地址管理	
油列表								0	添加路由
席号	目的	网络/主机						管理	

- ▶ 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;
- ▶ 带外管理(业务口):运行业务口进行系统管理,默认不勾选;
- ▶ VHID 组:选择接口所属 VHID 组,和配置多机热备有关,可选值为1²⁵⁵,默认空。
- 注: 同端不同接口不可配同个网段的 IP 地址。 不可信端配置同理。

6.4.1.4. 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"网络工具">"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。

路由列表						⊙ 添加路由
序号	目的网络/主机	网关	接口	状态	管理	
1	192.168.104.0/24	192.168.104.254	T2	停用	2%编辑 會删除	

第 28 页 共 104 页

可信端接口	不可信端	安口		编辑	× 类型初始
妾口列表			状态	停用	· ·
接口	物理口	类型	目的网络	例:192.168.1.0/24	营理
Т1	eth1	管理口	接口		C? IP地址管理
Т2	eth2	业务口			· CPIP地址管理
			网关	例:192.168.1.1	
			描述		
tt认网关:		DNS:		7651	
各由列表	ŧ			HEN	◎ 添加路日
+0					
13-5		日的四强/土化			Elf

- ▶ 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。

6.4.1.5. 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"网络工具">"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。

号	名称	位置	接口	成员	模式	管理
	Т	可信端	bond0	T5 T6	IEEE 802.3ad动态链接聚合	び 編編 自動除
	NT	不可信端	bond0	NT5 NT6	IEEE 802.3ad动态链接聚合	び 编辑 自删除

伟思信安安全隔离与信息交换系统 V6.5-用户手册

可信端接口不可信端接口 端口第	端口聚合编辑	◎ 新增端口聚
端口聚合列表	名称 test	
序号 名称	位置 可信端 •	管理
L: 状态为【停用】的接口才能用于端口聚合	模式 load balancing(round-robin)平衡抡循环策略 •	
	接口 T5(enp5s0f0) 2 T6(enp5s0f1) 2 T7(enp5s0f2) 2 T8(enp5s0f3) 2	
	输认	

- ▶ 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。

6.4.1.6. 拨号配置

系统支持可信端或不可信端拨号上网(需配备 4G 模块)

网络接口	
可信端接口 不可信	端按口 端口聚合 <mark>拨号配置</mark>
拨号选择	□信講 ∨ ○ 电信/移动 ④ 联通
	● 拔号设置

注:新增 4G 模块后,需要重新进行接口初始化,将 4G 模块接口新增到网络接口使用

6.4.2. 域名解析

系统支持将域名指向系统内部 IP 地址,并映射到外部指定域名,此功能主要搭配 域名映射功能共同使用。

							析	S解
●添加解	0 %						解析	城名
	管理	描述	域名	IP地址	位置	名称	序号	
編 自刑	☞ 編輯		www.qcc.com	192.168.5.37	可信端	test	1	
								_

6.4.3. 诊断工具

ViGap V6.5 提供了一些常用的诊断工具便于用户定位网络故障。

6.4.3.1. Ping 工具

进入"网络工具">"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。

Į	Traceroute	TCP服务检查	抓包工具	Arp	Route show	Free	Ifconfig
	位置: 可	信端 🔻					
E	目标主机:						

- ▶ 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;

6.4.3.2. Traceroute

进入"网络工具">"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。

诊断上具								
Ping工具	Traceroute	TCP服务检查	抓包工具	Arp	Route show	Free	Ifconfig	
	位置: 可	信端 ▼						
I	目标主机:]					
ł	最大跳数: 3	•						
				确认				

- ▶ 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;

6.4.3.3. TCP 服务检查

进入"网路工具">"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。

诊断工具	l								
PingI	具 T	raceroute	TCP服务检查	抓包工具	Arp	Route show	Free	Ifconfig	
	ť	立置:	可信端 ▼						
	目标目	主机:]					
	ģ	端口 <mark>:</mark>]					
					确认				

- ▶ 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;

6.4.3.4. 抓包工具

进入"网路工具">"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。

Ping工具	Traceroute	TCP服务检查	抓包工具	Arp	Route show	Free	Ifconfig
	位置: 可	信端 🔻					
	接口: T1						
	协议类型: all	•					
			_	_			

- ▶ 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;
6.4.3.5. ARP

进入"网路工具">"诊断工具"页面,点击"ARP"标签,该功能可查看系统 Arp 表数据。

诊断工具								
Ping工具	Traceroute	TCP服务检查	抓包工具	Arp	Route show	Free	Ifconfig	
	位置:	可信端 >						
结果:								
? (192.168.	5.84) at 1c:b7:2c:ad: 5.129) at b4:2e:99:2	a0:2f [ether] on en 8:d1:a0 [ether] on	o2s0 enp2s0					
? (192.168.	5.109) at 1c:87:2c:	56:2e:8d [ether] on	enp1s0					
? (192.168.	5.177) at ec:06:8a:94 15.129) at b4:2e:99:	4:78:50 [ether] on e :28:d1:a0 [ether] or	np2s0 enp1s0					
					a a	畒		

6.4.3.6. Route Show

进入"网路工具">"诊断工具"页面,点击"Route Show"标签,该功能可查看系统路由表数据。

新工具						
Ping工具	Traceroute	TCP服务检查	抓包工	具	Arp	Route show Free Ifconfig
	位置:	可信端 >				
结果:						
Kernel IP rou	tin <mark>g ta</mark> ble					
Destination	Gateway	Genmask	Flag	s Metri	c Ref	Use Iface
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0 lo
192.168.5.0	0.0.0.0	255.255.255.0	U	0	0	0 enp2s0
192.168.15.0	0.0.0.0	255.255.255.0	U	0	0	0 enpls0
						确认

6.4.3.7. Free

进入"网路工具">"诊断工具"页面,点击"Free"标签,该功能可查看系统资源占用。

DITH								
Ping工具	Traceroute	e TCPB	务检查	抓包工具	Arp	Route show	Free	Ifconfig
	位	置: 可信	鍴 >					
结果:								
	total	used	free	shared	buff/cache	available		
Mem:	3917284	1838728	183672	530212	1894884	1311460		
Swap:	8191996	73708	8118288					
							确认	

6.4.3.8. Ifconfig

进入"网路工具">"诊断工具"页面,点击"Ifconfig"标签,该功能可查看系统接口配置信息。

诊断工具	
Ping工具	Traceroute TCP服务检查 抓包工具 Arp Route show Free Ifconfig
	位置: 可信端 >
结果:	
enp1s0	Link encap:Ethernet HWaddr EC:D6:8A:56:60:60
	inet addr:192.168.15.77 Bcast:0.0.0.0 Mask:255.255.255.0
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
	RX packets:2269646 errors:0 dropped:17847 overruns:0 frame:0
	TX packets:95214 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:1000
	RX bytes:319245592 (304.4 MiB) TX bytes:55909783 (53.3 MiB)
	Memory:c8c00000-c8c1fff
enp2s0	Link encap:Ethernet HWaddr EC:D6:8A:56:60:6E
	inet addr:192.168.5.77 Bcast:0.0.0.0 Mask:255.255.0

6.5. 高可用性

6.5.1. 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 ViGap V6.5 的多机热备,我们需要两套以上单独的、完全相同的 ViGap V6.5 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	
当前设备IP	192.168.5.56
设备地址油	设备1可信旗岬: 192.168.5.62 优先级: 125 ∨ 自動除 设备2可信旗闸: 192.168.5.56 优先级: 95 ∨ 自動除 ● 添加 注: 填写备设备间网络可达的PP地址
可信端虚拟IP状态	未启用多机热备或未配置虚拟IP 添加VRRP虚拟IP
不可信端虚拟IP状态	未启用多机热备或未配需虚拟IP 添加VRRP虚拟IP

▶ 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。

6.5.2. 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";

```
伟思信安安全隔离与信息交换系统 V6.5-用户手册
```

可信端接口	不可信端接口	第口题			T2编辑		×.	う网口初始
接口列表			状态:	启用			•	
接口	物理口	类型	IP地址:	类型	IP地址/子网掩码	启用VRRP	⊙添加IP	管理
T1	enp4s0f0	管理		IPV4 •	192.168.15.11/24		會删除	Ø IP地址管理
T2	enp4s0f1	水		IPV4 -	192.168.18.11/24		會删除	C/ P地址管理
T3	enp4s0f2	水	允许Ping:				-	☞ P地址管理
т4	enp4s0f3	₹¥Fè	VHID组:	10 •	1			[♂IP地址管理
T5	enp5s0f0	业长多	l		确认			CFIP地址管理
T6	enp5s0f1	业长多						CF IP地址管理
τ7	enp5s0f2	业内省						C IP地址管理
T8	enp5s0f3	AF8						CF IP地址管理
	enaphyt4i0	水下						C》中地址管理
Т9								and the second se

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。

是否启用多机热备	
当前设备IP	192.168.5.62
设备地址池	设备1可信牌IP: 192.168.5.62 优先限: 125 ∨ 自動除 设备2可信牌IP: 192.168.5.56 优先限: 95 ∨ 自動除 ●添加 注: 填写省设备何网络可达的P地址
可信端虚拟IP状态	enp4s0f1:192.168.18.11/24 (MASTER)

6.5.3. 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。

机热音	
多机热备配置	
是否启用多机热备	
当前设备IP	192.168.5.62
设备地址池	公备1可信端IP: 192.168.5.62
可信端虚拟IP状态	enp4s0f1:192.168.18.11/24 (MASTER)
不可信端虚拟IP状态	enp4s0f1:192.168.19.11/24 (MASTER)
	<u>Rtr</u>

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。

6.6. 策略配置

6.6.1. 对象

对象:

在 ViGap V6.5 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;

3称:					-						
序号 名称	新增对象				· L2 × 理						
] 1 IP1	基本信息 名称: □PV61 类型: □Pv6 ∨ 描述: test										
	内容										
	您可以转	俞入单个IPv6地址或地址范围.(地址范围格于	式为xxx-xxx)								
	序号	IPv6地址	子网前缀长度	○添加 會清空							
	1	2001::15	64 ~	會 删除							
	2	3001::15	64 ~	會 删除							
				(保r	字应用 · · · · · · · · · · · · · · · · · · ·						

- ▶ 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;

对象						●添加对象
名称:	类型: 全部	~ 内容:	描述: ○ 里香檀茶条件			
□ 序号	名称	类型	内容	描述	管理	
□ 1	IP1	IPv4	192.168.15.120/24 192.168.16.120/30	test	化编辑	會删除
2	IPV61	IPv6	2001:15/64 3001:15/64	test	2 编辑	會删除

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。

隔离映	射												
隔离	映射												◎添加策略
名称:				全部 ~ 方向	句: 全部	~)		服务器:		描述:		€重置搜索条	(4
	序号	名称	状态	ЛП	ХПІР	源	服务器	端口映射	协议	描述	日志记录	管理	
	1	http1	运行中	T2	192.168.18.11		IP1	8888->8888 √	TCP		禁用	☑ 编辑 ③ 点击	禁用 會删除

6.6.2. 隔离映射

100000000

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 描 述	: T2NT 协士	以: TCP → 应用 状态	№2: FTP > 日 2 勾选表示启用此规则	志记录: 🗹		8
第略设置 方向 源 IP 时间对 文件类 上传下 端口映图	I □信讃->不可信讃 → 入 □ □信讃->不可信讃 → 入 □ □空代表任意 □ 遼文:	□: T2 マ 入口IP: 192.168. 源端口: 留空代表 FPP协议命令(沟选想 d □ tif □ png □.doc/.et/.ppt/.wps □ K8	18.11 ✓ 服务器地址: 1 王章 游地址转换: 示方许): ☑上传 ☑ 下载 ☑ 删除 docx/.pptx/.xisx □ exe □ rar □ pr	92.168.19.120 함空代表目动 ^[1] 重命名 · [2] 列录 df [1] txt	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
^{您可以} 序号	设置单个或多个映射, 不配置表示主演口 代理端口	观别。()满口可输入单个)满口或一个)满口泡围 服务端口	, 值式/为20038/200-2002) 状态 (勾选启用)	⊙添加	自清空	1
I 10000 100						

- > 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)

3、在配置映射代理端口时,系统自用端口不可用于业务配置,以下为限制使用端口:777,3306,9997,38381,4402,21,22,888,999,776,38383,10000,4401,38386,9527,8443,9999,12345,5355,514,53。

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。

3称:			状态:	全部 ~	方向: 全部		→入口IP:	服务器:	描述:		○重置搜索条件	
	序号	名称	状态	λП	λПIP	源	服务器	端口映射	协议 描述	日志记录	管理	
	1	http1	运行中	T2	192.168.18.11		IP1	8888->8888 √	TCP	禁用	2 編輯 ◎ 点击禁用	會删除
	2	T2NT	已停用	T2	192.168.18.11		192.168.19.120	2121->21 √	TCP	启用	2 编辑 □点击启用	會删除

6.6.3. 访问控制

6.6.3.1. 安全通道

在 ViGap V6.5 的访问控制页面可以新增通道规则,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">"安全通道"页面,切换到"安全通道"标签,点击"添加策略"按钮添加一个新的规则。

称:	添加安全通道		
」	基本信息		
	名 称: 策 略: ACCEPT	✓ 协议: TCP ✓	状态: 🗹 勾选表示启用此规则
	描述:	优先级: 留空表示追加到最后 ?	日志记录: 🗌
	茶路设置		
	方向: 可信端->不可信端 >		
	源 IP: 留空代表任意 I■	源端口: 留空代表任意	
	目的IP: 留空代表任意	目的端口:留空代表任意	
	关键字过滤: 多个请用 分隔开		
			保存应用

▶ 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。

▶ 关键字过滤:针对关键字对数据包进行阻断

第 41 页 共 104 页

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)。

6.6.3.2. 源转换

在 ViGap V6.5 的访问控制页面可以新增通道规则,对指定源 IP 地址转换为内部 指定地址。

:1	状态: 全部	∨ 方向: 全部	✓ 协议	: 全部 v 源IP:	目的	IP:	描述:		℃重置搜索	条件
序号	名称 状态	方向协议	源IP源	端口 目的IP	目的端口	接口	转换IP	转换端口	描述	管理
全诵道 源	转换									⊙添加
人源转换: □ 勾;	⁶ 添加源转换							- 23	×	
尔:	基本信息			_					重管搜索	经条件
序写	名称:		协议: TCP ,	•			状态: 🔽 勾选	表示启用此规则	加水	Et
	描述:			优先级: 留空	表示追加到最后	0	B	志记录: 🗌		
	44.00 VL 94								-	
	策略设直 方向: 可信	·送~>不可信送 >			~					
	源 IP: 留空	代表任意		源端口: 留空	代表任意					
	目的IP: 留空	代表任意		目的端口: 留	空代表任意					
	转换IP: 192.	.168.16.187 🗸		转换端口: 留	空代表任意					
									_	

- ▶ 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;
- ▶ 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;

第 42 页 共 104 页

- ▶ 优先级:可自定义生效顺序,插入指定策略前
- ▶ 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。
- ▶ 出口:指定数据出口网口。
- ▶ 转换 IP/端口:指定内部转换 IP 和端口。

6.6.4. 本地服务

6.6.4.1. 本地 FTP/SFTP

在ViGap V6.5的本地服务页面可以创建可信端和不可信端的本地FTP 或本地SFTP 服务,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。

本地FTP	强制访问控制 本地SFTP		添加FTP		O 添加FTF
可信端	不可信端	状态	◎禁用 ○启用		
序号	用户名	位置	可信端		管理
1	admin	用户名	test		(2)编辑 □ 点击启用 自删除
2	ftp1	蜜码	•••••		☞ 编辑 ◎ 点击禁用 會 删除
		强制访问控制等级	请选择	•	
			确认		

- ▶ 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;

第 43 页 共 104 页

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。

本地FTP	强制访问控制 本地SFTP				● 添加!
可信義 7	不可信端 用户名	等级	FTP目录	状态	管理
	admin		/admin	禁用	☞ 編編 ■ 点击启用 自 删除
	ftp1		/ftp1	启用	☞ 编辑 ◎ 点击禁用 會 删除

本地 SFTP 服务的创建和使用和 FTP 类似,不做赘述。

6.6.4.2. 强制访问控制

ViGap V6.5 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。

本地FTP 强制访问控制			新增等级	● 新增等级
启用强制访问控制		别名		
访问控制客户端下载 点击下载客户端		等级	正整数	
		标记	数字、字母或组合	
家号	别名		确认	管理
Í	普递			は、病境の自動除
2	秘密			☞ 網續 ● 删除
3	机塑			2 病機 自動除
4	绝密			び編組 自動除
4	绝密			び編組 自動除

▶ 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。

伟思信安安全隔离与信息交换系统 V6.5-用户手册

本地FTP 强制访问	控制			◎ 添加等
自用强制访问控制				
最访问控制客户端下载	点击下载客户端(Windows) 注:国产Kylin系统客户端使用命令 打标识: cryptdient - u ftp用户名 - p 除标识: cryptdient - u ftp用户名 - p	点击下载奏户端(Kylin) 2 密码 - f 需要打标的文件 - g 1 业务口IP 5: 9 密码 - f 需要称标识的文件 - g 0 业务口IP	566	
2 -1	Piter	保存	17:2	86 JH
	普通	च±x	88	27 編編 自制除
	私密	2	bb	(2) 編輯 音劃除
1	机密	3	cc	(2)编辑 自删除
	绝密	4	dd	CF 編載 音劃除

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;

🔒 标识客户端			<u> </u>	×
地址: 92.168.10.254 :	5566 用户名: 🕅	密码: *****		
文件夹/文件名:			打标识 除林	示识
操作文件:	等级 标识:	文件个数: 0	清除	

6.6.5. 数据交换

6.6.5.1. 文件交换

ViGap V6.5 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:

同步		
服务名称		
同步方向	◉可信端->不可信端 〇不可信端->可信端 〇双向	
可信端	关型 本地FTP ~ 目录 ~	
不可信端	类型 本地FTP ~ 目录 ~	
	・ 831U 時間等 1000 1000 1000 美書等者 二 美書等者 二 美書学校 二 美書学校 二 美書学校 二 美書学校 二 三 大健寺以は、 二 文件行びは、 二 文件指示型は、 二 近辺な空砂理 画録 ~	
	过滤文件处理 删除 ~	

- ▶ 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:

服务名称	
同步方向	◉可催講→不可催講○不可催講→可催講 ○双向
可信請	2013年12月1日 1921日 1931 1931
	田田 日田 「
不可佳識	型型 提望SM8 √ IP
	学務報码 UTF6 ~ 同か地式 第0 ~ 周か地式 3 ~ の考慮系示 - 文林大い江道 - 文林大い江道 - 文林市国区は - 文林市国区は - 武道文林地理 - 電動同少検式 -

- ▶ 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:

编辑文件同步 服务名名		
服务文化		
服务名和	2 p	
1003 H 11	7	
同步方向	●可信論→不可信論○不可信論	>可信請 〇双向
可信算	理美 91 泰日	
不可信望	堕类 通 91 录目	
	間防後編数 字符編码 同名之姓子第 同名之世子第 原本是三百八年 (各部運調立之件天 同志之居子入年 同志之居子入年 同志之学子入中 同志 文件本 文件本 文件本 文件本 近 近 文件本 代 近 篇 文件本 代 近 篇 》 代 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 名 二 四 二 四	S UTF8 → 開切 → 慶選 → ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○

▶ 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;

第 48 页 共 104 页

- 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;
- 文件特征过滤:勾选文件特征过滤则开启文件特征过滤,可根据需要选择黑名单 或白名单,可选择勾选系统预置的常见文件类型,或手动上传需要过滤的特征文件;
- ▶ 同名文件策略(远程 FTP):同步的同名文件可以选覆盖原有文件或更名;
- 关键字替换(远程 FTP):可对文本类型文件的内容关键字镜像替换;替换的关键字和目标关键字用"/#/"隔开;
- ▶ 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;

6.6.5.2. 数据库交换

ViGap V6.5 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ViGap V6.5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。

伟思信安安全隔离与信息交换系统 V6.5-用户手册

同步策略	数据资源			编辑	×-		0 添加资源
索号	名称	资源位置	资源名称:			描述	管理
			资源位置:	◉可信端 ○不可信端			
			数据库类型:	Oracle	-		
			IP地址:				
			端口:	1521			
			同步账号用户名:				
			同步账号密码:				
			业务账号用户名:				
			业务账号密码:				
			数据库名:				
			模式名:				
			临时表前缀:				
			触发器表前缀:				
			描述:				
					测试连接 保存应用		

- ▶ 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;

	蒲相
资源名称:	kexin
资源位置:	●可信端 ○不可信端
数据库类型:	MySQL
IP地址:	192.168.5.88
端口:	3306
同步账号用户名:	ха
同步账号密码:	*****
业务账号用户名:	x
业务账号密码:	•••••
数据库名:	test
描述:	test
elegyin)左体测出于成Th	测试连接保存应用

- ▶ 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;

	30344
资源名称	bukexin
资源位置:	○可信端 ◉不可信端
数据库类型	MySQL -
IP地址:	192.168.6.89
端口:	3306
同步账号用户名:	ха
同步账号密码:	•••••
业务账号用户名:	x
业务账号密码:	•••••
数据库名:	test
描述	test
✓bukexin连接测试成	功

- ▷ 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

数据库同步			
策略配置			
0-	0		
基本配置	同步任务配置	计划任务	总览
策略名称:	mysql_test		
同步方向:	●从可信端到不可信端 ○从不可信端到可信端		
同步方式:	●触发器增量同步 ○全表同步 ○触发器单表同步		
启用连接池:			
随系统自启动:			
描述:	test		
		€ ⊕ ٹ –⊤	
© 2018 珠海经济特区伟思有限公司.			

▶ 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:

教挥库同步

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。

	基本配置		同步任务配置	计划任务		总增
原端数据资源选	择: kexir	1 ~			目标端数据资	源选择: bukexin ~
口勾选同步	序号	源表名	映射目标表 言智能匹配 ? 會清空	字段配置	序号	目标表名
	1	6001	6001	(7 配置	1	6001
	2	test	test		2	test

- 资源选择:选择己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"按钮删除己匹配的目标表

- > 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。

数据库同步					
策略配置					
0		2		3	0
基本配置		同步任务配置		计划任务	总览
时间间隔:	3 秒				
				_	
			Θ±-# 下=	₩ Θ	
© 2018 珠海经济特区伟思有限公司.					
时间间隔:	3₽		@上─# 下	≝ ⊚	

▶ 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。

配置						
	0	0				
	基本配置	同步任务配置	计划任务		总览	
1.基本配置		1.源数据库资源配置信息		1.目的数据库资源配	置信息	
策略名称: mysql	_test	资源名称: kexin		资源名称: bukexin		
司步方向:从可信	言端到不可信端	IP地址: 192.168.5.88		IP地址: 192.168.6.8	IP地址: 192.168.6.89	
同步方式: 触发器增量同步		端口: 3306		端口: 3306		
启用连接池:是		数据库: test	数据库: test		数据库: test	
随系统启动:是		类型: mysql	类型: mysql		类型: mysql	
苗述:		同步账号用户名: xa	同步账号用户名: xa		同步账号用户名: xa	
		业务账号用户名: x		业务账号用户名: x		
4.同步表配置						
序号	源表	目标表	单/双向		字段数	
1	6001	6001	single		3	
2	test	test	single		3	

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,

6.6.6. 业务代理

6.6.6.1. 视频代理

ViGap V6.5 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)

第 54 页 共 104 页

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;

颂代理列表	视频代理基本设置		⊙添加代
可信端代理IP			
不可信端代理IP	•		
可信端端口			
不可信端端口			
超时时间			
内容过滤关键字	2	0	

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。

105代理列表 视频代理基本设置		视频代理编辑	×		0)	委加代:
序号 代理名称 描述 方向 代理IP	名称	test		视频厂商信令格式	视频编码格式	管理
	描述	测试				
	代理方向	可信端->不可信端	•			
	代理IP	192.168.15.77				
	代理端口	5060				
	目标服务器IP	192.168.16.100				
	目标服务器端口	5060				
	可信端网络协议	UDP				
	不可信端网络协议	UDP				
	视频流格式	CMS	÷			
	视频厂商信令格式	海康V3.0	-			
	视频编码格式	H264				

- ▶ 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;
- ➢ 网络协议:支持 UDP 和 TCP
- ▶ 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;

65	代理名称	描述	方向	代理IP	代理端口	目标服务器IP	目标服务器端口	信令通讯方式	视频流格式	視頻厂商信令格式	视频编码格式	管理
	test	1	t2nt	192.168.15.57	5060	192.168.16.120	5060	udp	cms	海康V3.0	3gp	

6.6.6.2. Web 代理

ViGap V6.5 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。

Web代理	
(CERE	
状态	○ 歳現 ○ 第明
方向	● 可描述→不可描述。○不可描述,可信述
端口	10066
可访目的端口	●-14日以色物語并
过渡类型	E名単少 此选现订下面的所有过速争数创生效
请求方法过渡	GET POST PUT HAD CONNECT TRACE OPTIONS DELETE
道IP过渡	ng:192168.750/74
	提示输入圈户,多个输入围始打爆开
目的IP过滤	ag-142.168.75.0/24
	提示输入目的P,多个输入预测订展开
域名过渡	
	提示输入域名,多个输入用的行 隔 开
访问时间段过渡	eg:1126-2030
	提示输入gin段。多个输入网络门旗开
MIME类型过滤	(ant/tan) (ant/cas (tant/cas (tant/cas (tant/case) (ta

▶ 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;
- ▶ 过滤类型:可下拉选择黑名单或白名单过滤;
- ▶ 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。

6.6.7. 工业控制

6.6.7.1. 工业内容策略

工业内容策略包括 Modbus TCP、S7、OPC 等工业协议,每种工业协议都需要通过 license 进行激活使用,对数据进行过滤需要基于工业协议代理上,过滤产生的日志 可在系统工具中的日志与审计下的 Sproxy 日志中记录。

Modbus TCP:

点击工业内容策略会跳转到 Modbus TCP 策略页面,在 Modbus TCP 中通过配置从站地址、功能码、寄存器地址、读寄存器长度限制、寄存器写值过滤等对通过 ViGap V6.5 的工业协议代理通信进行阻断或放行,已达到安全应用的目的;

全局配置由应用模式,名单机制组成,默认为测试模式,黑名单机制,介绍如下: 全局配置:

全通模式:允许所有数据通过,不产生日志,黑白名单设置无效。

工作模式:允许匹配的策略通过,并产生日志。

测试模式:允许所有数据通过,并产生日志。

第 57 页 共 104 页

名单机制:

黑名单机制:对匹配相应的策略进行拦截。

白名单机制:对匹配相应的策略进行放行。

在"工业控制"中,点击"工业内容策略",进入工业内容策略设置页面,鼠标 滑动到 i 标记即可查看功能介绍。

MC	DBUS	ТСР	S7					◎ 添加
局	设 <mark>置</mark> :	应用模式	工作模式	▼ 白名单机制 ▼	设置 ①			
)	序号	规则ID	从站地址	功能码	寄存器地址	读寄存器长度限制	寄存器写值过滤	操作
1	1	11	111 🖸	05 WRITE SINGLE COIL D	11 🖸		地址:11 值:1 🖪	2 编辑 前册

点击"添加策略"按钮,进入编辑工业内容策略 Modbus TCP 页面。

工业内容策略-> MODBUS TCP			
编辑			
规则ID	1-1024 必填		
从站地址	any: 🗹 📑		
功能码	any: 🗹 🕞 🖉		
		咏 存 取消	

填写规则 ID、从站地址、功能码、寄存器地址、读寄存器长度大于、寄存器写值 过滤等信息后,点击"保存",生成规则。

- ▶ 规则 ID: 必填, 数字, 1-1024, 不能重复。
- 从站地址:选填,数字,0-99999,默认停用,点击"加号",添加一条从站 地址填写栏与是否启用的复选框,不能添加超过五个从站地址;点击"删除", 删除当前行的从站地址栏;存在 any 复选框,点击勾选,则包含所有的从站地址。
- ▶ 功能码:选填(下拉框形式),默认停用选填,点击"加号" ,添加一条功能

码下拉框选项栏与是否启用的复选框,点击"笔" ,添加一条功能码输入框 与是否启用的复选框,输入框只能输入现有功能码和自定义范围内的功能码,不 能添加超过五个功能码地址;点击"删除" ,删除当前行的功能码栏目;存在 any复选框,点击勾选,则包含所有的功能码。

注意:读功能码与写功能码不能一起使用在一条策略上,读功能码可编辑项为 读寄存器长度限制,写功能码可编辑项为寄存器地址与寄存器写值过滤。

规则ID	1
从站地址	any:□ @
功能码	any: □ 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
读寄存器长度大于	any:□ 10 启用Z

读寄存器长度限制(大于):为读功能码可编辑项,选填,0-99999,正整数,读寄存器功能码读取长度大于某个值的匹配;存在 any 复选框,默认勾选启用,匹配 所有的读寄存器长度(勾选 any,黑白名单都放行)。

编辑	
规则ID	1
从站地址	any:□
功能码	any: □
寄存器地址	any: □
寄存器写值过滤	any: □

寄存器地址:为写功能码可编辑项,选填,0-99999,正整数,支持地址段(0-3)、
 多个地址(2,4,5)、单个地址(6)选填(下拉框形式),默认停用选填,点击
 "加号" ,添加一条寄存器地址栏与是否启用的复选框,不能添加超过五个寄存器地址;点击"删除" ,删除当前行的寄存器地址栏目;存在 any 复选框,

点击勾选,则包含所有的寄存器地址。

寄存器写值过滤:为写功能码可编辑项,选填,包含地址和对应值,地址:正整数,0-99999;值:0-99999,正整数。默认停用,点击"加号" ,添加一条寄存器写值过滤地址与值、是否启用的复选框,不能添加超过五个寄存器写值过滤; 点击"删除" ,删除当前行的寄存器写值过滤栏目;存在 any 复选框,点击勾选,则包含所有的寄存器值。

对于自定义

功能码,读寄存器长度限制,寄存器地址,寄存器写值过滤,均可自定义配置。

● MODBUS TCP 配置注意事项:

所配置的整条规则为与的关系,所设置的各个项必须都符合才匹配,若在一条策 略中配置了多个功能码,则各个功能码之间为或关系。

S7 协议:

支持 S7-200、S7-200-smart、S7-300、S7-400 。

点击 S7 标签页即可跳转到 S7 规则页面,其中的全局设置功能与 Modbus TCP 类似。

工业内容	策略						
MODBU	JS TCP	<mark>\$</mark> 7					◎ 添加策略
全局设置	: 应用模式 法 写控制	测试模式 🔻	黑名单机制 ▼	设置 🛈	提示:黑名单下,PUD类型为07-用户	数据,设置子功能码无效	
	_	i e contra co					
	序号	规则ID	PDU类型		功能码 功能号	操作	
	1	23	01 - 工作模式	0	any 🖸	「日本語」の「「「「」」」で、「「」」の「「」」で、「「」」を見ていていた。」。	

点击"添加策略"钮,进入编辑工业内容策略S7页面。

编辑	
规则ID	1-1024 必填
PDU类型	01 - 工作模式 🔹 启用 🗹
力能码	any: 🗹 📑

图 6.40 工业内容策略 S7 编辑页面

填写规则 ID,选择 IP 对象、PDU 类型、功能码或者功能号等,点击"保存",生成规则。

- ▶ 规则 ID: 必填, 数字, 1-1024, 不能重复。
- ➢ PDU 类型:下拉框(0x01-工作模式; 0x02-消息确认; 0x03-数据确认; 0x07-用 户数据),必填,默认 01,若 PDU 类型选择 0x01、0x02、0x03:则允许选择功能 码,必填,下拉框;
- ▶ 功能码:选填(下拉框形式),默认停用,选填,点击"加号" ,添加一条功能码下拉框选项栏与是否启用的复选框,点击"删除" ,删除当前行的功能码栏目;存在 any 复选框,点击勾选,则包含所有的功能码。
- 功能号:选填(下拉框形式),默认停用,选填,点击"加号",添加一条主功能号和子功能号的下拉框选项栏与是否启用的复选框,主功能号下可以有多个子功能号,点击"删除", , 删除当前行的功能号栏目;存在 any 复选框,点击勾选,则包含所有的功能号。

注意: 在黑名单下, PUD 类型为 07-用户数据, 设置子功能码无效。

● S7 配置注意事项:

所配置的整条规则为与的关系,所设置的各个项必须都符合才匹配,若在一条策 略中配置了多个相同的功能码或者功能号,则各个功能码之间为或关系。

6.6.7.2. 工业协议代理

T db4th 201712 TB

工业协议代理包括 Modbus TCP 和 S7 两种协议,每种工业协议都需要通过 license 进行激活使用,所代理的映射可在工业内容策略中进行过滤处理。

通过配置协议、源端口、目标地址、目标端口等对通过 ViGap V6.5 的通信进行映射转发,下面创建一条代理规则。

在"工业控制"中,点击"工业协议代理",进入工业协议代理设置页面。

1.11										
●添加作									0添加代理	
全局设置: 最大连接客户端数量 [55535 [设置]										
	ID	名称	方向	协议	网间地址/主站串口	网间端口/波特率	服务器地址/从站串口	服务器端口/网络转发端口	操作	
0	ID	名称 modbus	方向 可信端->不可信端	协议 Modbus TCP	阿问地址/主站串口 192.168.5.187	网间端口/波特率	服务器地址/从站串口 192.168.6.135	服务器端口/网络转发端口 502	操作 了《編編 ◎ 点击禁用	自删除

在当前页面可以对最大连接客户端数量进行设置,默认值为65535,范围1-65536, 应用于所有协议;

点击"添加代理"按钮,进入编辑工业协议代理页面。

工业协议代理	
代理配置	
名称	
代理方向	可信端到不可信端 >
协议	Modbus TCP 👻
网间地址	
网间端口	
服务器地址	
服务器端口	提示:目标端口建议选择502
是否启用代理	
	66 存 1003档

选择协议,填写网闸地址、网闸端口、目标地址、目标端口等信息后,点击"保 存",生成代理规则。

- ▶ 协议: 下拉框, 默认 MODBUS TCP, 选项包括: MODBUS TCP、S7。
- ▶ 网闸地址: IP 地址, 必填, 可填写网闸接口 IP 或者虚拟 IP。
- 网闸端口:必填,正整数,0-65535,形式为下拉框与输入框,只需填写一个,已 代理过的端口不可再重复。
- ▶ 目标地址: IP 地址,必填,所要代理转发的 IP 地址。
- 目标端口:必填,正整数,0-65535,形式为下拉框与输入框,只需填写一个,建 议填写默认值 502。
- ▶ 是否启用过滤:单个复选框,默认不勾选。

注意事项

所生成的代理会根据源端口在可信端与不可信端规则列表中生成对应的过滤规则,使得工业协议可以正常访问。

6.6.7.3. 自学习策略

自学习策略支持工业协议数据的识别和控制,可识别的工业协议包括: Modbus TCP、DNP3、OPC DA、RSSP、IEC104、S7、OPC UA、IEC61850、BACNET 的工业数据流。 启动自学习策略时,网闸需配置成透明模式。

ViGap V6.5 会记录经过网闸的工业数据流量(需先启用工控日志记录),用户可

根据这些历史数据配置生成自学习模板,下面创建一条自学习。

在"工业控制"中,点击"工控自学习",进入策略设置页面。

工控自学习			
策略			●添加策略
名称	注释	学习结果	
		当前无配置信息	

点击"添加策略"钮,进入编辑自学习模板添加页面。

第編 第2日年2000 名称 (最多63个字符) 近史数据展示 天・ 历史数据 日期 名称 日期 19 数量	自学习策略			
名称 注释 (@多63个字符) 历史数据展示 天・ 历史数据 ● 名称 日期 IP 数量	编辑			清空自学习数据
注释 @##653个字符) 历史数据展示 天・ 历史数据 <	名称			
历史数据展示 天 历史数据 名称 日期 IP 数量	注释		最多63个字符)	
历史数据 日周 IP 数量	历史数据展示	天		
名称 日期 IP 数量	历史数据			
	□ 名称	日期	IP	数量

选择历史数据,填写策略名称、注释,点击"保存",生成自学习策略。

- ▶ 名称:可填写英文、数字和组合,长度不大于24;
- ▶ 注释:可填写中文、英文、数字和组合,长度不大于 63;
- ▶ 历史数据选择:可在下拉框选择历史数据展示的单位,可选按天展示或按小时;
- ▶ 历史数据:根据需求选择需要生成自学习模板的数据

生成自学习策略后,会自动跳转掉策略配置界面,也可在自学习策略展示列表点 击行修改按钮进行配置。

界面右侧展示服务器-客户端连接树,左侧列表是根据用户勾选的历史数据生成的 工业策略,不同协议生成的策略有差异,但都包括数据类型、注释、值等基本参数。

odbus DNP3 OPC RSSP IEC	C104 S7 OPCUA IEC61850 B	ACNET		◆新增设备单元◆添加规则
き型	注释	值	操作	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
nb_func	读输入寄存器	func_id:4	2 1	└─ 0 % 192.168.5.153 : 11
mb_input_register			C	
mb_input_register			20	
mb_input_register			88	
mb_input_register			8° 🖞	
mb_input_register			C 🖞	
nb_input_register			20	
mb_input_register			C2 🗇	
mb_input_register			C° 🖬	
nb_input_register			C 🖞	
mb_input_register			C° û	

点击策略行右侧编辑按钮,可查看策略详情,并对该策略类型的数据流做控制和 审计。

- > 范围内:可在下拉框选择对该类型数据进行的操作,可选通过、丢弃或重置;
- 日志:对匹配该策略的数据进行日志审计,可在下拉框选:不记录、紧急、告警、 严重、错误、警示、通知、信息或调试。

* 7 J	注题	1	値	場作		192.100.5.155
mb_func	编辑规则		144	J#1F	- 🛛 ×	\$ 192.168.5.153 : 1
mb_input_register		编	辑规则(modbus)			
nb_input_register	类型	mb func				
nb_input_register						
nb_input_register	功能号	4				
mb_input_register	注释	读输入寄存器				
nb_input_register	影響の					
nb_input_register	监控设置					
mb_input_register	范围内	通过 ·		日志不记录		-
mb_input_register						
mb_input_register						

可在右侧按钮点击"新增设备单元"选择工业服务器和客户端后,手动添加策略。

5	新增设备单元(modbus)	
服务器IP	0.0.0.0	
客户端IP	0.0.0.0	
设备单元	设备单元id 1-255	
	确认	

注释		值	操作		192 🖵 1
新增规则				— 🛛 ×	¢
		新增规则(modbus)			
类型	mb_func				
功能号					
 注释					
 监控设置					
范围内	通过	•	日志不记录	•	
				保存规则	

6.6.7.4. 工控日志模板

用户需配置工控日志模板后, ViGap V6.5 才会根据用户勾选,记录对应协议的工业数据,否则默认不记录。

在"工业控制"中,点击"工控日志模板",进入日志设置页面。

電	
名称	
启用	● 全选 modbus dnp3 opc rssp iec104 iec61850 s7 opcua bacnet
日志记录截止时间	2027-11-08 00:55:30
注释	(最多63个字符)

根据需要记录的数据,勾选对应协议,点击"保存"生效。

6.6.8. 攻击防御

ViGap V6.5 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。

6.6.8.1. 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 ViGapV6.5 上。

引擎信息病毒隔离区	
可信端病毒引擎	区局用
不可信端病毒引擎 团启用	
病毒库日期	Build time: 25 Nov 2019 08:56 -0500
病毒库版本	Version: 59
升级病毒库	点击选择文件
	(CT)

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。

引擎信息	● 清空隔商区
可倍端 不可倍端	
可信端病毒隔离区:/database/virusgap	

6.6.8.2. 抗攻击

系统可设置抗攻击。在配置抗攻击时,进入"策略配置">"抗攻击"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	□ 阈值:150
UDP Flood	國值:150
ICMP Flood	□ 阈值:150
TearDrop攻击检测	0
LAND攻击检测	

▶ 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,首次登录需修改密码。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。
管理员	列表								● 添加管理员
序号	用户名	状态	角色	证书	安全等级	创建时间	最后编辑时间	描述	管理
1	admin	启用	系统管理员			2017-02-14 10:14:14	2017-02-14 10:14:14		12 编辑
2	adminlog	启用	日志审计员			2017-02-16 15:41:05	2017-02-16 15:41:05		CF 编辑
3	adminuser	启用	用户管理员			2017-02-16 15:12:24	2017-02-16 15:12:24		18 總雄

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。

管理员列	表							
管理员	列表				添加管理员	×		◎ 添加管理员
序号	用户名	状态	角色	状态	启用	-	描述	医 管理
1	admin	启用	系统	84	老姑藤田日		11	2 编辑
2	adminlog	启用	日志	用巴	於坑邑理页		05	☞編編
3	adminuser	启用	用户	用户名			24	☞ 编辑
				密码			_	
				确认密码				
				证书选择	不限制	•		
				安全等级	不限制	•		
				描述				
					确认			

▶ 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对应证书;

▶ 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(系统审计员):只能查看和操作日志审计相关的页面;

manager (系统操作员):能查看和操作用户管理相关的页面。

角色定义	
角色定义	
角色	描述
admins	系统管理员-能查看和操作除日志审计和用户管理以外的所有页面
logauditor	系统审计员-只能直看和操作日志审计相关的页面
manager	系统操作员-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。

安全等级	
安全等级	
级别	权限
1	x
2	设备管理局可用性对象时间模式应用隔离映射
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
注:此功能)	期于系统管理员

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:

入	其他人	中间证书颁发机构	受信任的相	正书颁发机构	受信任的发布者	未受信任的发表
颁发		颁发者	- Self (2001)	截止日期	友好名称	
	45	Buture	mattA ens	1		
- 导入 正书的:	(I)	导出(E)	/////////////////////////////////////			高级(A

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。

	(<u>IN</u>):	<所有>				
人	其他人	中间证书颁发机构	受信任的根	证书颁发机构	受信任的发布者	未受信任的发布
颁发	给	颁发者		截止日期	友好名称	
v	isec_01	internal-o	a	2027/4/	<无>]
			TRATI A Long			

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。

and a second sec		
0		
0 · 0 / 0 0 0 / 0 / 0 / 0 / 0 / 0 / 0 /		
· · · · · · · · · · · · · · · · · · ·		
/ · · · · · · · · · · · · · · · · · · ·		
	伟思信安安全隔离与信息交换系统ViGap	
	▲ 用户名	
	▲ 密码	
	BANTAR B7 200 10	
	登录	
	© 2008-2022 0 All Rights Reserved.	
	为达到最佳体验效果,推荐下载使用谷歌浏览器:Chrome。	

 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。

++000+++++++		

A CONTRACTOR OF		
	小小 住田信 幕	
A . LA CARDON AND A CONTRACT OF A CONTRACT. CONTRACT OF A CONTRACT. CONTRACT OF A CONTRACT. CONTRACT OF A CONTRACT. CONTRACT OF A CONTRACT OF A CONTRACT OF A CONTRACT. CONTRACT OF A CONTRACT OF A CONTRACT. CONTRACT OF A CONTRACT OF A CONTRACT	-victory-idea-	
		2
0		
	伟思信安安全隔离与信息交换系统ViGap	
and the second	* admin	
	- damin	
	A	
	30 165 5 5 5 × 2	
	1 4 91	
	登录	
	▲证书不匹配	
X		
	# 2009 2022 At Diable Descript	
	为达到最佳体验效果,推荐下载使用谷歌演选器:Chrome。	TITI
	© 2008-2022 All Rights Reserved. 为达到最佳体验效果,推荐下载使用谷歌词武器:Chrome。	

7.4. 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)。

▲用户管理 >	安全配置		
管理员列表 角色定义	安全配置		
安全配置	会话超时设置	240 (单位为分钟)	
女王寺 坂 ▶ 注销	登录可尝试次数	3	
	封锁IP时间	1 (单位为分钟)	
	证书认证	第用 √ 点击下载案户端证书(visec_01)>> 点击下载案户端证书(visec_02)>> 注意:如启用证书以证,请确保你本地上保存有备户编证书或浏览器已导入证书,否则将无法打开管理界面	
	远程管理限制	● 禁用 ○ 启用	
	类型	● 白名単 ○ 黒名単	
	远程IP地址		
		80	

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

ViGap V6.5 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

授权信息	设备识别号: 5EFE9944D78DD85BFC05F52C1880BE0E 授权类型: 试用版 已使用时间: 4天7小时9分37秒 授权天数: probation is empty.天	
授权文件	▲ 点击上传授权文件	

● 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。

安全配置		
会话超时设置	240	(单位为分钟 范围1-240)
登录可尝试次数	3	(范围3-10)
封锁IP时间	1	(单位为分钟 范围1-30)
密码过期时间	7	(单位为天 范围1-30)
证书认证	 禁用 √ 点击下载客户端证书(cert_01)>> 点击下载客户端证书(cert_02)>> 注意:如启用证书认证,请确保你将 	\$地上保存有客户端证书或浏览器已导入证书,否则将无法打开管理界面

● 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

可信端病毒引擎	
不可信端病毒引擎	□启用
病毒库日期	Build time: 25 Nov 2019 08:56 -0500
病毒库版本	Version: 59
升级病毒库	点击选择文件

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

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	22	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	

ViGapV6.5提供以下接口供用户管理和配置:

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	4401、38383、38386	配置业务后开启,不可占用		
内外端通讯进程	38382	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		

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 22 端口登入,输入命令:
SSH 192.168.0.254 22,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。

1) 显示网口配置信息 3) Ping 主机 4) 恢复出厂设置 5) 临时IP设置 6) 修改默认账号密码 7) 重启系统 8) 关闭系统 0) 退出

请输入要进行的操作命令: ^[0P

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

第77页共104页

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;

-victory-idea	
住田信空空合原南与信白六语系统ViCon	
中心后女女王丽离马后心又厌余尔VIGdP	
▲ 用户名	
● 密码	
37 St 4	
短距的 イイマンズ	
8.8	
±.,*	
	A second s
e 2008 2022 0 All Diskle Dessented	
w zuud-zuuzz u All Rights Reserved.	
为匹到最佳体验效果,推荐下载使用谷歌浏览器:Chrome。	

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,首次登录需修改密码。即可进入系统的日志审 计模块。

伟思信安安全隔离与信息交换系统 V6.5-用户手册

3	管理员:	IP:	事件:	消息: 角色: 全部 v 级:	别: 全部 > 时间范围:	創 Q 蒼	e
F	号 管理员	角色	IP	事件	消息	级别	操作时间
1	adminlog	日志审计员	192.168.15.109	登录	登录管理界面	成功	2022-01-18 15:10:25
2	adminlog	日志审计员	192.168.15.109	退出	退出管理界面	成功	2022-01-18 15:10:21
	adminlog	日志审计员	192.168.15.109	清空日志	清空管理日志	成功	2022-01-18 15:10:18

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。

家号	管理员	角色	IP	事件	消息	级别	操作时间
	adminlog	日志审计员	192.168.5.109	登录	登录管理界面	成功	2021-05-28 17:13
	adminlog	日志审计员	192.168.5.109	退出	退出管理界面	成功	2021-05-28 17:13
	adminlog	日志审计员	192.168.5.109	清空日志	清空管理日志	成功	2021-05-28 17:13
3 显示 1 到	adminlog 町3,共3祭	日志审计员	192.168.5.109	清空日志	清空管理日志	成功	2021-05-

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。

访问日志					會 清空日志 导出日志 ▼
关键字搜索:	Q查找				
序号	源	目的	协议	长度	时间
无数据!					

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。

可信端->不可信端	不可信端->可信端				會 清空日志	导出日志 🔻
服务名称:	源服务器IP:	目的服务器IP:	文件路径:	文件名: 时间范	图: 到	Q查找
序号 服务	各名称	源服务器IP	目的服务器IP	文件路径	文件名	时间
无数据!						

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。

服务名称:		数据流向:	抽取表名:	加载表名	3: 时间范围:	到[]到[]	Q查找
号	服务名称	数据流向	抽取表名	加载表名	抽取成功 (条)	抽取失败 (条)	时间
(据)							

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。

可信端抽取	不可信端加载	不可信端抽取	可信端加载	可信端基本信息 7	不可信端基本信息	會清空日志	导出日志
践务名称:	数	屠流向:	抽取表名:	加載表名:	时间范围:	到到	丸査找
号	服务名称	数据流向	抽取表名	加载表名	加载成功 (条)	加载失败(条)	时间
तानः							

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。

可信	需抽取 不可信端加载	不可信端抽取 可信詞	端加载 可信端基本信息 不可信端基本信息	@ 清空日和	5 导出日志 -
服务	名称: 业务流程名	:事件:	消息内容: 级别: 全部 > 时间范围: 到		2 查找
家号	业务流程名	事件	消息内容	等级	时间
1	与客户端进行通信交互	捕获会话异常	用户IP:172.26.78.2捕获到会话异常.异常信息:Connection reset by peer	失败	2020-04-11 08:40:1
8	TimingDeleteLogData	TimingDeleteLogData	TimingDeleteLogData Executed	成功	2020-04-11 01:00:0
	Initial Schedual	Initial Schedual	Initial Schedual Success	成功	2020-04-10 15:48:0
	Initial NetWork	Initial NetWork	Initial NetWork Success	成功	2020-04-10 15:48:0
	Get Version	Get Version	Main Pro Version: 1.3.2.28L_b26	成功	2020-04-10 15:48:0
5	Initial NetWork	Initial NetWork	获取监听IP地址异常;使用默认监听IP:0.0.0.0;	成功	2020-04-10 15:48:0

9.2.5. 应用日志

应用日志记录了代理数据的日志,可查看数据文件经系统代理的相关信息,并可 针对地址、应用类型等进行查看。

点击"日志与审计">"应用日志",进入日志页面。

应用	日志							@清空日志 导出日志 ▼
位应用的	置: 全部 类型: 全部	✓ 源IP: ✓ 内容:		源湖 时间范围:	<u>الم</u> انية المانية الم	E	abilP:目的端口: 핏Q_查找	
序号	位置	源IP	源端口	目的IP	目的端口	应用类型	内容	时间
序号 1	位置	源IP 192.168.11.22	源端口 3943	目的IP 192.168.12.56	目的端口 81	应用类型 HTTP	内容 192.168.11.22通过GET方式访问/a1.zip	时问 2022-06-17 14:46:13
序号 1 2	位置 可信端 可信端	源IP 192.168.11.22 192.168.11.22	源端口 3943 3942	目的IP 192.168.12.56 192.168.12.56	目的端口 81 81	应用类型 HTTP HTTP	内容 192.168.11.22通过GET方式访问/a1.zip 192.168.11.22通过GET方式访问/a1.zip	时间 2022-06-17 14:46:13 2022-06-17 14:46:09

可根据查询条件搜索,查看日志的相关信息

点击"清空日志"按钮,即可清空应用模块日志。

点击"导出日志"按钮,导出应用日志,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。

9.2.6. 告警日志

告警日志分为数据交换告警日志、应用告警日志。记录了包括不能同步的文件、 管道连接失败、资源配置失败、代理数据过滤等异常日志,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。

告警日	志							
告警	日志							@清空日志 导出日志 ▼
位告警	置: 全部 模块: 全部	ß v 源IP: ß v 內容:		Bji	源端口:]范围:		目的)時口: 目的)端口: 到 Q:雪找	
序号	位置	源IP	源端口	目的IP	目的端口	告警模块	内容	时间
1	不可信端	192.168.11.22	3943	192.168.12.56	81	HTTP	a1.zip中发现病毒Malware.AnkeHuber,禁止传输	2022-06-17 14:46:17
2	不可信端	192.168.11.22	3942	192.168.12.56	81	HTTP	a1.zip中发现病毒Malware.AnkeHuber.禁止传输	2022-06-17 14:46:13
3	不可信端	192.168.11.22	3940	192.168.12.56	81	HTTP	a1.zip中发现病毒Malware.AnkeHuber,禁止传输	2022-06-17 14:46:04
4	不可信端	192.168.11.22	3933	192.168.12.56	81	HTTP	a1.zip中发现病毒Malware.AnkeHuber.禁止传输	2022-06-17 14:46:00

9.2.7. 文件同步状态日志

文件同步状态日志记录了数据资源服务器连接的网络相关日志,并在出现异常时 提供审计。

文件同	步状态日志					
文件	同步状态日志					四志 导出日志 ▼
日志	内容: 操作項: 操作结果: 全部 > 日志美型: 全部 > 来源:	全部 >时间范	围:]到[Q查找	
序号	日志内容	操作项	操作结果	日志类型	来源	创建时间
1	SFTP连接异常	fileSync sftp	失败	告警	可信端	2022-06-17 16:49:25
2	服务: fileSyndsftp.SFTP连接异常,请检查SFTP服务是否可连接!	fileSync sftp	失败	告警	可信端	2022-06-17 16:49:25
3	服务: fileSyndsftp,SFTP连接异常,请检查SFTP服务是否可连接!	fileSync sftp	失败	告警	可信端	2022-06-17 16:48:48
4	SFTP连接异常	fileSync sftp	失败	告警	可信端	2022-06-17 16:48:48
-		0.0 1.0	24-11A-	21-214	27/2224	

可根据查询条件搜索,查看日志的相关信息

点击"清空日志"按钮,即可清空日志。

点击"导出日志"按钮,导出日志,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。

9.2.8. 工业代理日志

工业代理日志记录了数据资源服务器连接的网络相关日志,并在出现异常时提供审计。

业代理	里						
可信封	# 不可信端	自学习					會清空日志 导出日志
关键	字查询		Q查找告答	日志 连接日志			
序号	协议	源地址	源MAC	目标地址	目的MAC	详细消息	操作时间
1	MODBUS TCP	192.168.11.22:19864	70:88:CD:A5:DD:F3	172.26.78.2:502	68:91:D0:61:1A:AB	不符合规则 empty rules, deny	2022-06-16 13:57:51

可根据查询条件搜索,查看日志的相关信息

点击"清空日志"按钮,即可清空日志。

点击"导出日志"按钮,导出日志,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。

9.2.9. 攻击防护日志

攻击防护日志记录了系统抗攻击记录的日志

攻击防护日志							
攻击防护日志						會 清空日志 导出日志	•
关键字搜索:	Q查找						
序号	源	目的	协议	长度	说明	时间	
无数据!							

可根据关键字条件搜索,查看日志的相关信息

点击"清空日志"按钮,即可清空日志。

点击"导出日志"按钮,导出日志,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。

9.2.10. 关键字过滤日志

关键字过滤日志记录了代理(FTP、HTTP、POP3、STMP)拦截的日志

关键字过滤日志								
关键字过滤日志						俞 清空日志		
关键字搜索:	Q直找							
序号	ip地址	端口	协议	长度	关键字	时间		
无数据!								

可根据关键字条件搜索,查看日志的相关信息

点击"清空日志"按钮,即可清空日志。

点击"导出日志"按钮,导出日志,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。

9.2.11. SNMP 服务

系统支持信息上报至 SNMP 服务器,支持 V1-V3 版本。

填写服务器连接参数,并选择对应版本,实现连接。

SNMP服务器					
SNMP服务器					
启动SNMP服务器					
监听端口	161				
设备位置					
共同体					
SNMPv3					
	既存				

9.2.12. 审计管理

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"日志审计">"审计管理",进入日志设置。

审计管理	
审计策略 日志存相	皆
Syslog服务	☑ 倉用
远程Syslog服务器	□启用
当前日志空间使用量	7%
日志空间告警值	80% ~
日志存档	□启用
FTP服务器	用户名 密码
	服务器地址
	服务器端口

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 ViGap V6.5 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。

管理员:	IP:	事件:	消息:	角色: 全部	阝 ~ 级别:	全部 > 时间范围:	到	Q童	2
劳号 管理员	角色	IP	事件	消息				级别	操作时间
1 adminlog	日志审计员	192.168.5.109	清空日志	清空管理日志				成功	2021-05-28 19:33:4
55 1 到 1 , 共 1条记录		信息		×					
			日志空间曾	言警值70%,日志空间使	5用量73%				

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。

审计管理	同计管理								
审计策略	日志存档	邮件通知							
提示: 系统	默认保留最近180)天的存档,超时后将会	自动从服务器中删除, 如需长时间存	档请下载到本地!					
序号		名称	大小	存档时间	管理				

系统还支持通过邮件或 FTP 方式上传日志数据到服务器

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;

₩首页	可信端接口	不可信満接口 端口	聚合					つ阿口初始化
L	接口列表							
设备管理	接口	物理口	类型	IP地址	是否Link	允许Ping	状态	管理
系统开级	T1	enp4s0f0	管理口	192.168.5.56/24	•		启用	⑦ IP地址管理
备份/恢复	T2	enp4s0f1	业务口	192.168.7.2/24	0		启用	CF IP地址管理
网络报口 时间设置	тз	enp4s0f2	业务口		0		启用	(》IP地址管理
脅前页	可信講接口	不可信満接口 講口	聚合					つ网口初始化
▶ 统计分析	接口列表							
■设备管理 -								
设备管理	接口	物理口	类型	IP地址	是否Link	允许Ping	状态	管理
系統升级	NT1	enp4s0f0	业务口	192.168.6.56/24			启用	C P地址管理
备份/恢复	NT2	enp4s0f1	业务口	192.168.8.2/24	•	2	启用	C IP地址管理

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

♣ 首页	本地FTP 强制防闭控制		O 添加FTP
▶ 统计分析		添加FTP	
目 设备管理	・ 可信識 不可信識	una e*用 ob用	
■ 高可用性	序号 用户名		管理
□策略配置	•	位置 り 信 病 ・	
对象		用户名 test01	
隔离映射		密码	
访问控制		强制访问控制等级 请选择	
文件交换		御込	
数据库交换		_	
视频代理			
Web代理			

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

第 87 页 共 104 页

可信端信	息.	点击保存:
月1日4月1日	応り	总山 你 什;

● 首页	编辑文件同步		
🕍 统计分析			
■设备管理 >	服务名称	本地FTP	
■ 高可用性 →	同步方向	◎可信講->不可信講◎不可信講	黃->可信讃 ◎双向
	可信端	类型 目录	本36FTP ・ / rest01 *
对象 隔离映射	不可信講	类型 目录	[#±857D • //set02 •
·切回控制 本地服务		字符编码	
文件交换 数据库交换		同步模式 同步轮询问隔	
视质代理		病毒查杀 关键字过滤	
Web代理		图片关键字过滤	
组播代理		文件大小过滤	
病時]擘		文件名过速	
抗攻击		文件特征过速	
♦工业控制		过滤文件处理	翻時、
● 注销			9279 182m

- ▶ 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:默认可信端一>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;

5 读取"7的日录列表 列出"701日录成功	
站点: G:\test_02\	▽ 远程站点: //
G (双部) G SRECYCLE.BIN G System Volume Information test_01 ↓ test_02 G 保存到片	
A 文件大小 文件类型 最近修改	文件名 文件大小 文件类型 最近惨改 权限 所有者/组
新建文本文档.txt 0 文本文档 2021/5/11 11:10:	

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。

主机(H): 192.168.6.56 用户名(U): test02 密	④(W): ●●●●●●	
状态: 读取目录列表 状态: 列出"/"的目录成功 状态: 读取"/"的目录列表		^
状态: 列出"/"的目录成功		~
本語記念記。(Skipet, O2)、 ・ (法語) ・ (法) ・ ((法) ・ ((法)) ・ ((法)) ・ ((())) ・ (()) ・ (过程整点 / / Z	×
文件名 文件大小 文件类型 最近修改	文件名 文件大小 文件类型 最近修改 权限 所有費/組	_
	≧新建文本文档.txt 0 文本文档 2021/5/1117 0644 10011001	

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;

		The start of the s
同步万向	、可信端->不可信端、不可信端->可	1信端,以向
可信端	类型	远程FTP
	IP	192.168.5.207
	用户名	test 01
	密码	
	端口	21
	日录	
	HA	
不可信端	类型	远程FTP
	IP	192.168.6.207
	用户名	test_02
	密码	
	端口	21
	目录	
	同步线程数	5
	字符编码	UTF8 ·
	同步模式	剪切·
	保存源端空文件夹	
	同步轮询间隔	3
	病毒查杀	
	关键字过滤	6
	图片关键字过滤	5. C
	文件大小过滤	
	文件名过滤	5.
	文件后缀名过滤	
	文件特征过滤	*
	过減文件处理	删除
	同步模式	专用

伟思信安安全隔离与信息交换系统 V6.5-用户手册

- ▶ 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 可信端一>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

第 90 页 共 104 页

传到可信端成功;

主机(H); 192.168.5.207 用户名(U): test_01 密码(W): ●●●●●● 第日(P): 21 快速连接(Q) ●	
状态: 读敬 / 你自录列表	
ixta: 列出"/"的目录成功	
状态: 读取"/"的目录列表	
状态: 列出""的目录成功	
本地站点: Gi(test_01) / 适便站点: /	
⊕F(数据) ∧ → ↓ /	
è G: 徽强)	
B \$RECYCLE.BIN	
est_01	
test_02	
v	
文件名 文件大小 文件类型 最近修改 权限 所有:	1/组
■新建文本文档stat 0 文本文档 2021/5/11 11:06: ◎新建文 0 文本文档 2021/5/11 11:06:	
I II	

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。

3: 文件传输成功,传输了 0 字节 (用时1 秒) 5. 法即**/****/*****************************	
· 例示 / 的目录成功	
S: 已从服务器断开	
的结点: G:\test 01\	✓ 远程站点: /
名	✓ 文件名 文件大小 文件类型 最近修改 权限 所有書/組
	■新建文 0 文本文档 2021/5/11 11

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;

步策略	数据资源						◎添加的
ę	名称	资源位置		编辑	×	描述	管理
			资源名称:	test01	- 100		
			资源位置:	◎可信講◎不可信講			
			数据库类型:	MySQL	•		
			IP地址:	192.168.5.207			
			端口:	3306			
			同步账号用户名:	test01			
			同步账号密码:				
			业务账号用户名:	test02			
			业务账号密码:				
			数据库名:	test01			
			模式名:	test01			
			临时表前缀:	YW_			
			944597-54592 -	YWW	- 10		
					- 18		
			10111551 :				
			加速:				

- ▶ 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: mysq1 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:选择策略配置一>数据库交换一>数据资源,添加资源,然后点测试链接,再点击保存应用;

数据库同步							
同步策略	数据资源						◎添加资源
序号	名称	资源位置		编辑	×	描述	 锂
			资源名称:	test02			
			资源位置:	◎可信端 ◉不可信端	- 18		
			数据库类型:	MySQL	•		
			IP地址:	192.168.6.207			
			端口:	3306			
			同步账号用户名:	test01			
			同步账号密码:				
			业务账号用户名:	test02			
			业务账号密码:				
			数据库名:	test02			
			模式名:	test02			
			临时表前缀:	YW_			
			触发器表前缀:	YWW_			
			启用ssl:	8	- 18		
			描述:				
				测试连接 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: mysq1 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。

伟思信安安全隔离与信息交换系统 V6.5-用户手册

骨首 页		同步策略	数据资源							⊙添加资源
▲ 统计分析		成号	名称	资源位置	数据库类型	IP/端口	使用数量	描述	管理	
■ 设备管理	•									
目高可用性		1	test01	可信調	mysql	192.168.5.207 : 3306	0		◎ 编辑 ● 里音连接池 ● 删除	
♥策略配置	-	2	test02	不可信端	mysql	192.168.6.207 : 3306	0		☞ 编辑 ● 重查注接池 會 删除	
对象										
隔离映射										
访问控制										
本地服务										
文件交换										
把相關在心中的										

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;

数据库同步			
策略配置			
ा - <u>स</u> र्वता	·····································	计划任务	3 表版
策略名称: 同步方向: 同步方式: 一同並按池: 随系统自启动: 描述:	test ●从可信講到不可信講 ◎从不可信講到可信講 ●触发器增固同步 ◎全表同步 ◎触发器单表同步 Ø test		
		下	

- ▶ 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;

	0-			0		
	基本配当	Ϊ.	同步任务配置	计划任务		記憶
<u> </u>	¥: test01	•			目标满数据资料	勤选择: test02 ▼
■勾选同步	序号	源表名	映射目标表 三智能匹配 2 映射配置方法:	段配置	序号	目标表名
	1	а	1、使用智能匹配, ; b 表名称一致的将自动	原表和目标 映射; ≥ 配置	1	b
			2、使用拖拽的方式 表名】的列拖拽到[表1 的声格中	, 把【目标 映射目标		
			261 192010			

- ▶ 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;

数据库同步					
策略配置					
	0			0	
	基本配置	同步任务和置	计划任务	总管	
	时间间隔: 3	秒			
		©上───────────────────────	下─步❷		

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";

以据库同步								
節略配置								
		•	•		•			
基本	和智	同步任务配置	计划任务		急度			
1.基本配置		1.源数据库资源配置信息	1.源数据库资源配置信息		至信息			
策略名称:test		资源名称:test01		资源名称:test02				
同步方向:从可信端到不可信	言述	IP地址: 192.168.5.207		IP地址: 192.168.6.207				
同步方式:触发器增量同步)洲口:3306		端口:3306				
启用连接池:是		数据库:test01		数据库:test02				
随系统启动:是		类型:mysql	类型:mysql					
描述:		同步账号用户名:test01	同步账号用户名:test01		st01			
		业务账号用户名:test02	业务账号用户名:test02		st02			
4.同步表配置								
序号	源表	目标表	单/双向		字段数			
1 a		b	b single		3			
		● ⊢—歩	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;

数据库同	步					启动test成功					
同步策	略数	据资源									⊙添加策略
序号	名称	状态	源资源	目标资源	方向	启动时间	停止时间	描述	管理		
1	test	运行中	test01	test02	可信端->不可信端	2021-05-12 13:56:30			☞编辑 ◎点	法停止 會删除	

11、可信端数据库 test01 的 a 表同步数据

	■ ■ ■ ■ ■ ■ ■ ■ ■ ■	 事件 査询 	报表 备份 书	计划任务	
注接 192.168.5.207 information_schema wysql performance_schema	◎ 打开表(2) ♀ 设计表(2) □ a yw_a (辰) a @test01 (192.166)	□ ● 创建表(L) □ 및 删除表 3.5.207)	60 🖓 导入向导口 😱	导出向导创	×
ettol1 ettol1 ettol1 意 表 初路 雪面 振 電面 振 電面 振 電 電 電 電 電 電 電 電 電 電 電 電 電	文件(D)编辑(D) 查看(V) 密 · 导入向导(D) · 导出向导 · d · 1	口W) 後) 🍶 筛检向导 🌆 name test	网格视图 目 表単视图 char test	▲ 备注 ■ 十六进位	📓 图像 │ 🎶 升幂排序 🐥

12、成功同步到不可信端数据库 test02 的 b 表

文件(E) 3	きる(U) 工具(I) 窗[コ(<u>W)</u> 報則	ש <mark>(H)</mark>									
戸 注接	2 管理用户	表	视图	」 功能	事件	查询	退	(三) 备份				
连接		10	打开表(2)	7 设计表 🗉	📪 创建表(Ŋ 📑 🖬除	表回 🐺 导	入向导(I)	🔋 导出向导	(X)		
	<pre>information_schema mysql performance_schema sys sys test022</pre>		10 (表) 文件(D) マ(中(D) マ(中(D))	b @test02 (1 編輯(E) 查看 词导(I) 🏹 导	92.168.6.20 (V) 窗口(W 出向导(X) 。	7)) <mark>通</mark> 筛检向导		视图 🔳 表		副备注	11111111111111111111111111111111111111	E
	·····································		id		name 1 test	8	d	har estl		_		
	 □ 函数 ■ 事件 ● 查询 ▲ 报表 ■ 备份 											

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;

伟思信安安全隔离与信息交换系统 V6.5-用户手册

	接口列表							
] - [
	接口	物理口	类型	IP地址	是否Link	允许Ping	状态	管理
	т1	enp4s0f0	管理口	192.168.5.56/24			启用	☞ IP地址管理
1	T2	enp4s0f1	业务口	192.168.11.88/24			启用	⑦ IP地址管理
				192.168.7.2/24				
	тз	enp4s0f2	业务口		0		启用	G* IP地址管理
	T4	enp4s0f3	业务口		0		启用	CB IP地址管理
	T5	enp5s0f0	业务口		0	0	启用	CP IP地址管理
•	T6	enp5s0f1	业务口		0	0	启用	CP IP地址管理
•	Т7	enp5s0f2	业务口		0	0	启用	CP IP地址管理
•	Т8	enp5s0f3	业务口		0	0	启用	C ⅠP地址管理
	Т9	enaphyt4i0	业务口		0		启用	☑ ⅠP地址管理
	T10	enaphyt4i1	小客口		0		启用	C≥ 10+6519 9579

- 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;

骨 首页		隔离	映射									◎添加策略
▲ 统计分析		名称:			· 华杰· 人动。 古向 · 人动	-] » L	חוד - מו	服体型。	1254 ·		O TRACTOR	
■ 设备管理	2		序号	编辑隔离明	触						- 🖾 ×	
日高可用性			1	基本信息		102 103 <u>-</u>					î	
♥策略配置	-			名称: 描述:	test	协议: TCP ·	•	应用协议: [FTP •] 状态: ☑ 勾选表示启用	日初 此规则	記录: ≥		
对象												
隔离映射				爺略设置								
访问控制				方向:	可信端->不可信端 •	入口: 12 •		92.168.11.88 •	服务器地址: 192	.168.16.130	=	
本地服务				ातः १२: इन्होंग्रेज्		F	ぷぁ⊔: 〒协议命令(拒绝): ■ ト	空代表任意 6 日下载 日期除 日期	游地址转换: (883) B命名	代表目动		
文件交换												
数据库交换				端口映射								
视频代理				您可以设	"置单个或多个映射,不配置表示。"	全端口映射. (端口可)	输入单个端口或一个端口	范围,格式为xxx或xx-xxx)			
webl C建 组播代理				序号	代理端口		服务端口		状态 (勾选启用)	◎添加	自清空	
病毒引擎				1	11		21			會删除		
抗攻击												
	•											
●注销											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

	C														
₩ 首页	陽調	明映射													◎ 添加策略
🖿 统计分析	名称	:		状态:	全部・フ	方向: 全部	• \	.□IP :	服务器:		描述:	:	○ 重管搜索条件		
■ 设备管理	۵	序号	名称	状态	ЛП	λ□IP	源	服务器	端口映射	协议	描述	日志记录	管理		
■ 高可用性		1	test	运行中	T2	192.168.11.88		192.168.16.130	11->21 √	TCP	test	启用	☞ 编辑 ● 点击禁用	會删除	
♥策略配置															
对象	_														
隔离映射															
访问控制															
本地服务															
文件交换															
数据库交换															
视频代理															
Web代理															
組織代理															
病毒引擎															
抗攻击															
♦工业控制															
● 注销															

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。

又件(F) 編編(E) 参看(V) 传输(I) 服务醑(S) 予签(B) 報切(H)	
M - V - A - X + A - X - A - X - M		
主机(H): 192.168.11.88 用户名(U): test01 毫	(₩): ••••• 端口(P): 11 快速连接(Q) ▼	
状态: 不安全的服务器,不支持 FTP over TLS。 状态: 日登录 状态: 读取目录列表 状态: 列出//的目录成功	,,	
本域認識。\ \		
文件名 文件大小 文件类型 最近停改 ** C: 本均磁盘	文件名 [^] 文件大小 文件类型 最近修改 权限	所有者/组 空目录列表

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;

=\#/护理ID/I奋网	1021000110	24
高3m1 ULE1F/1略址J	192.168.6.113	
可信端代理IP/掩码	192.168.5.45	24 ~

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:

家号	代理名称	描述	方向	代理IP	代理端口	目标服务器IP	目标服务器端口	信令通讯方式	视频流格式	视频厂商信令格式	视频编码格式	管理	
1	test1		t2nt	192.168.6.113	5060	192.168.5.104	5060	udp	cms	陆丰	3gp	ぽ编辑	自删除

	视频代理编辑	
名称	test1	
描述		
代理方向	可信端到不可信端	•
代理IP	192.168.6.113	
代理端口	5060	
目标服务器IP	192.168.5.104	
目标服务器端口	5060	
信令通讯方式	UDP	•
视频流格式	CMS	•
视频厂商信令格式	陆丰	
视频编码格式	3GP	-

- ▶ 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

平台1		
☑ 启用		
协议版本	GB/T28181-2011	~
SIP服务器ID	3702120200200000121	0
SIP服务器域	3702120200	0
SIP服务器地址	192.168.6.113	
SIP服务器端口	5060	0
SIP用户名	3402000001111111111	0
SIP用户认证ID	3402000001111111111	0
密码	*****	0
密码确认	•••••	0
注册有效期	3600	⊘秒
注册状态	在线	$\mathbf{\vee}$
心跳周期	60	⊘秒

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。

10.6. Modbus 工业代理

● 案例拓扑



▶ 操作流程

1、这里分别使用 Modbus Slave 和 Modbus Poll 仿真软件来搭建 Modbus 测试环境;

2、在内网打开一个 Modbus Slave 服务器,设置主站地址为1、功能码为3、寄存器地址位设置为0-10,设置 TCP 连接端口为502,开启连接;

3、在不可信端业务口配置一个外网可达的 IP,登陆页面,选择"设备管理">"网络接口",配置不可信端业务口 ip: 192.168.5.87,并启用;可信端同理,在业务口配置一内网 Modbus 服务器可达的 IP: 192.168.12.87,并启用;

4、登陆页面,选择"工业控制">"工业协议代理",点击"添加代理"按钮;

5、填写工业协议代理,点击保存应用;

名称	test
代理方向	不可信端到可信端 >
协议	Modbus TCP 🗸
网间地址	192.168.5.87
网甸端口	502
服务器地址	192.168.12.120
服务器端口	502 提示: 目标端口建议选择502
是否启用代理	

- ▶ 代理名称、描述可自定义
- ▶ 代理方向:选择不可信端到可信端;
- ➢ 协议:选择 Modbus TCP
- 网闸地址:填写网闸的不可信端工业代理 IP(上文配置的不可信端 IP);例: 192.168.5.87
- ▶ 网闸端口:默认填写 502 来做 Modbus 代理端口;例: 502
- ▶ 服务器地址: Modbus 服务器地址,填入上文的 192.168.12.120
- ▶ 服务器端口:填入上文的 502
- ▶ 是否启用代理:勾选启用

配置完成,点击保存。

全局	司设置	: 最大	连接客户端数量 6	5535	设置									
	ID	名称	方向	协议	网间地址/主站串口	网间端口/波特率	服务器地址/从站串口	服务器端口/网络转发端口	操	ľF				
	1	test	不可信端->可信端	Modbus TCP	192.168.5.87	502	192.168.12.120	502	۵	点击禁用	修改	删除		

6、点击进入工业内容策略页面,应用模式设置工作模式,选择白名单机制后点击 设置;

7、点击新增工业内容策略,策略 ID 输入 1,功能码取消勾选 ANY 选择 03 功能 码,勾选启用后保存;

从站地址	any: □
功能码	any: □
读寄存器长度大于	any: 🗹 0-99999的正整数 启用

按照该配置, 允许了从站地址 1、功能码 03、寄存器长度不做限制的工业数据通行;

8、在内网打开一个 Modbus Poll,设置主站地址为1、功能码为3、寄存器地址位 设置为 0-10;设置连接方式为 Modbus TCP,连接 IP 填写不可信端工业代理 IP 192.168.5.87、连接端口为 502,点击连接;

ile	Edit	Conr	nectio	n	Setup	FL	unctio	ons	Dis	play	V	iew	W	indo	W	Help			
D	🗳 日	8	×	-	빌	ė	Л	05	06	15	16	17	22	23	ТС	· []	P	12	Ī

		Read/Write Definition X
Alias	00000	Slave ID:
	0	
	0	Function: 03 Read Holding Registers (4x) V Cancel
	0	Address: 0 Protocol address. E.g. 40011 -> 10
	0	Quantity: 10
	-1647	Scan Rate: 1000 [ms] Apply
	8	Disable
	0	Read/Write Disabled Disable on error Read/Write Once
	7	
	0	New
	0	● 10 ○ 20 ○ 50 ○ 100 ○ Fit to Quantity
		Hide Alias Columns DPLC Addresses (Base 1)
	0	View Rows 10 0 20 0 50 0 100 Fit to Quantity Hide Alias Columns PLC Addresses (Base 1)

Modbus Poll 客户端连接成功,数据读写功能正常。