

安全隔离与信息交换系统

快速配置手册



江苏深网科技有限公司



修改文档历史记录:

日期	版本	说明	修改人
2021年07月22	1.0.0	初稿	Wangh
B		211.2	
2023年05月24	101	百次王则裁网	Hooy
日	1.0.1	史以于加截含	песу

安全隔离与信息交换系统 -----快速配置手册

欢迎使用

• SWG

深网信安全隔离与信息交换系统(本手册中简称 SWG) 是以 SWOS 为系统平台,以网闸 特有的 2+1 物理结构为基础的网络安全产品。该产品采用开放性的系统架构及模块化的设计, 融合了工业协议(MODBUS、OPC、IEC104) 控制、访问控制等多种安全手段,全面提升隔离能 力。



声明

■ 本文档中所提到的产品规格及资讯仅供参考,有关内容可能会随时更新,江苏深网 不另行通知。

本文档中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而 有所差异,此可能产生的差异为正常现象,产品功能和性能请以产品说明书为准。

■ 本文档中没有任何关于其他同类产品的对比或比较,江苏深网也不对其他同类产品表达意见,如引起相关纠纷应属于自行推测或误会,江苏深网对此没有任何立场。

■ 本文档中提到的信息为正常公开的信息,若因本文档或其所提到的任何信息引起了 他人直接或间接的资料流失、利益损失,江苏深网及其员工不承担任何责任。

二、 系统简介

● 业务能力

SWG 的访问型业务能够支持多种应用协议,包括文件传输,常用的 TCP 协议、UDP 协议, 还包括多种工业控制协议(Modbus、OPC、IEC104)。SWG 可灵活组网,支持多种接入方式, 包括代理、路由,以适应的用户需求;一体化策略配置方式,不同的协议、不同的方向、不 同的接入模式策略统一进行配置管理,给管理员带来了极大的便利。同时还具备强大的安全

策略权限管理、细粒度的审计和日志记录等功能。

物理架构

- SWG 的物理架构由内网处理单元、外网处理单元、隔离与交换控制单元组成。
- 内网处理单元:包括内网接口单元。接口部分负责与内网的连接,并终止内网用户的网络连接,对数据进行访问控制、防护等安全检测后剥离出"纯数据",作好交换的准备,也完成来自内网对用户身份的确认,确保数据的安全。
- 外网处理单元: 与内网处理单元功能相同, 但处理的是外网连接。
- 隔离与交换控制单元:是网闸隔离控制的摆渡控制,控制交换通道的开启与关闭。 控制单元中包含一个数据交换区,就是数据交换中的摆渡船。对交换通道的控制方 式目前有两种技术,摆渡开关与通道控制。摆渡开关是电子倒换开关,让数据交换 区与内外网在任意时刻都不能同时连接,形成空间间隔 GAP,实现物理隔离。通道 方式是在内外网之间改变通讯模式,中断了内外网的直接连接,采用私密的通讯手 段形成内外网的物理隔离。该单元中有一个数据交换区,作为交换数据的中转。

三、系统部署

常见的部署方式是放置在两个不同密级的安全域间,防止高密区数据流向低密区。通常 情况下,内网接高密网络,外网接低密网络,即使外网被入侵,也不会影响内网数据安全。 常见的部署如下拓补图:



快速配置手册



● 映射模式

网闸作为代理服务器接受客户端的访问,客户端访问的是网闸设备,而不是真正的服务

器。网闸接收到新的请求后,作为客户端去访问真正的服务器。



映射模式拓补如下图所示:



● 路由模式

网闸作为网关部署到网络中,客户端访问的是真正的服务器的 IP 地址,只是客户端与服务器不在同一网段,客户端需要将请求的数据包交给下一跳网关,即网闸。网闸根据数据包的目的 IP 地址,通过配置的路由,将数据请求发送到目的服务器。

注:路由模式拓补与映射模式拓补相似。

四、安装



SWG 支持通过 WEBUI 方式远程登录管理,管理员在安装部署 SWG 完成后,登录到 SWG 的 WEB 管理界面对系统进行管理。登录前,先使用专用的串口转换接口,使用串口 查询或配置网闸管理口地址,再通过双绞线将管理主机的 RJ45 接口与 SWG 的管理接口 MGT0 直连,配置内网管理主机的 IP 地址为 192.168.1.X/24 (X 取值范围为: 2-253)。 在管理主机的浏览器上输入 SWG 的管理 URL,例如:<u>https://192.168.1.254:88</u>,弹出如

下的登录页面。



欢迎管理员登录-内网



普通用户登录

外网使用相同的方式配置。

● 管理员账户

账户类型	用户名/密码	
系统管理员	sysadm/SWkj!@34	
网络安全员	admin/SWkj!@34	
安全审计员	auditor/SWkj!@34	
串口管理员(调试用 , 只用于串口或 ssh 访问)	console/console	

● 接口 IP

接口	IP 地址	
内网 MGT0	192.168.1.254/24	
外网 MGT0	192.168.100.254/24	

● 访问服务

|--|



SSH	开放
WEBUI	开放
PING	开放

● 串口参数

参数	值
波特率	9600
数据位	8
奇偶校验	无
停止位	1
数据流控制	无

● 配置物理接口

步骤 1 以内网配置为例,使用 系统管理员 登录,选择 系统配置>>基本配置>>内网接口配置,选择某接口进行配置,编辑完成后点击【保存】按钮:

📶 深岡岡闸-内岡	≡ 8.6	蒋	🋔 sysadm
 ● 状态监视 			
4-用户管理 <	內阿倫口亂置 系統时间 機式即換 走阿配置		
0: 系统配置 *	1900年 第日: INT4 ビ 1900年 第日: INT3 ビ 1900年 第日: INT3 ビ 1900年 第日: INT3		
基本配置	P: 100.00.135		
功能开关			
抗攻击	IP: 192.168.4.254		
入侵防御			
餐 权用管理	海加度如周卡		
Q. 系统维护 《			
♥ 安全审计 〈			

步骤2点击右上角的【配置生效】按钮。

五、配置案例

5.1 文件摆渡

● 基本需求

如下拓补所示,网闸两侧各有一台文件传输客户端,外端机侧网络文件传输客户端(发送端)与网闸外端机相连,内端机侧网络传输客户端(接收端)与网闸内端机相连;现需要



将内端机侧网络文件传输客户端所在主机的文件同步到外端机侧网络文件传输客户端的主机 上。

● 配置要点



注:本着内外端分离管理的原则,网闸的内、外端均需新建用户,即内网侧新建 的用户,外网侧也要新建同样的用户。

■ 步骤 2 激活普通用户并修改密码

- ① admin 用户登录网闸内外两侧的 webUI
- ② 进入权限管理->普通用户



③ 激活用户

④ 新建的普通用户需在 webUI 普通用户登录界面修改密码

📶 深网网闸-内网	=								酉 保存	🛔 sysadm
 秋志监视 () () 		普通用户								
组管理		账号	等级	所属组	IP	MAC	账户状态	添加用户		
普通用户		ceshi	不涉密	test	192.168.10.100	00:00:00:00:00:00	未激活	删除(修改	
0。" 系统配置 〈		nvrclient	不渗密	test	10.0.0.33	00:00:00:00:00	激活	删除(修改	
管 权限管理 く		dahua	不渗密	test	10.0.0.35	00:00:00:00:00	溆 (活	删除(修改	
Q. 系统维护 〈		Imtserver	不涉密	test	192.168.100.201	00:00:00:00:00	激活	删除(修改	
♥ 安全审计 <		xlserver	不涉密	test	192.168.100.200	00:00:00:00:00	激活	删除(修改	
		sxtclient	不涉密	test	10.0.0.34	00:00:00:00:00	激活	删除(隆改	
		Imtserver1	不涉麼	test	192.168.100.202	00:00:00:00:00:00	激活	删除(修改	
		bijiben	不涉密	test	10.0.0.226	00:00:00:00:00:00	激活		修改	

步骤 3 使用 admin 用户登录 webUI,点击 规则管理>>文件摆渡>>传输路径,点击【添加】 按钮,添加规则界面如下:

源IP地址*		
ip		
目的IP地址*		
ip		
发送/接收路径*		
发送路径		
接收路径		
发送者*	▼ 接收者*	

源地址: 即为 PC1 的 IP 地址目的地

址: 即为 PC2 的 IP 地址

发送/接收路径:可自定义,如:A,B,甲,乙等

发送者、接受者:即是 sysadm 新建的普通用户,用于登录文件传输客户端。

网闸内外两侧均需配置,提交完成后,生效规则。

■ **步骤 4** 安装文件传输客户端安装无特别注意,只需一步一步往下执行即可,安装 成功后,图标为





■ **步骤 5** 文件客户端 配置

(Q) 网间1P	
8 用户名	
會 密码	
□ 自动登录 □ 记住密码	

- ① 双击图标,打开客户端
- ② 网闸内侧, PC1 机: 网闸 ip, 为网闸内侧 IN 端的 ip, 用户名、密码即为 sysadm 新建的普通用户。 网闸外侧, 同理, 填写的网闸 OUT 端的 ip
- ③ 配置发送/接收目录,进入客户端,点击客户端左侧的发送目录/接收目录, 文件目录:选择一个文件目录作为发送/接收目录。
 - 隔离器 IP,发送者/接收者,发送路径/接收路径,根据规则的设置,下拉选择,无法手工录入。
 - 即, 网闸内侧 PC1 配置发送相关参数, 网闸外侧 PC2 配置接收相关参数。
- 步骤 6 文件传输
 - ① 将待发送的文件放入发送目录后,并启动发送即可。



📶 文件传输客户端	i					⊚ – □ ×
😂 网闸地址	序号	文件路径	隔离器地址	发送路径	发送状态	接收人
🕑 启动发送	1	C:/Users/86180/ Desktop/1	10.0.0.133	1-2	发送未启动	xlserver
📈 发送目录						
★ 发送状态						
🗾 接收目录						
📥 接收状态						
🥎 恢复配置						
🖳 保存配置						
(1) 关 于						
		添加		修改	冊修余	

5.2 工控代理

● 基本需求

如下拓补所示,网闸内网有一个 modbus 客户端,外端有一个 modbus 服务器;外端机 侧 modbus 服务器与网闸外端机相连,内端机侧 modbus 客户端与网闸内端机相连;现需使 用将内端机侧 客户端访问外端侧的服务端。



- 配置要点
 - 配置 modbus 客户端与服务,记录 IP 和 MAC 地址
 - 配置网闸的映射规则
 - 激活网闸的用户
- 配置步骤



	步骤	1	创建	用户组
--	----	---	----	-----

- ① 用 sysadm 用户登录系统
- ② 进入'工控配置→组管理',执行新增用户组
- ③ 提交后,执行配置生效

	添加普通	用户组				×	
	普通用户	·组名称 *					
	普通用	户组名称	7				
	描述*						
	描述						
_							
					关闭	提交	
L 创趸	書用户						
\bigcirc	用 sysadm	n用户登录	录系统				
\bigcirc	创建田户	提交后,	执行配备	胃生効 激	·活田户		
					111111		
3	用 admin ;	贫求系统					
4	用户管理	,执行激	活用户				
📶 深岡岡闸-内岡	=						图保存 🌲 🏜 sysadm
 ● 状态监视 ◆ ▲ 用户管理 	普通用户						
组管理	账号	等级	所履组	IP	MAC	账户状态 添加!	₩À
普通用户	ceshi	不涉密	test	192.168.10.100	00:00:00:00:00	未激活 删除	修改
 ♥\$ 系統配置 	nvrclient	不涉密	test	10.0.0.33	00:00:00:00:00		修改
Q. Skitter	Imtserver	不涉密	test	10.0.0.35	00:00:00:00:00		修改 (83)
♥ 安全审计 〈	xlserver	不涉密	test	192.168.100.200	00:00:00:00:00:00		revix 修改
	sxtclient	不涉密	test	10.0.0.34	00:00:00:00:00	10074 Hillion	修改
	İmtserver1	不涉密	test	192.168.100.202	00:00:00:00:00	2007年 前時余	修改
	bijiben	不涉密	test	10.0.0.226	00:00:00:00:00	款活	修改

步骤 2 添加 IP 组

- ① 用 admin 用户登录系统
- ② 点击 对象管理,执行添加 IP 组
- ③ 提交并执行配置生效



	添加IP组			×
	IP组名*			
	用户名			
	IP组*			
			+	
	描述			
	描述			
	等级* ◎绝密	◎机密 ◎秘密 ◎フ	~涉密	
			关闭	提交
注:新建用户		E网闸内外两(则执行。	
■ 步骤 3 添加即	央射规则			
① 用 admin 用户	1登录系统			
 进入(工物配) 	置_\吐射横式	, 执行沃加		
⊻ 近八 工注癿_	■. / 吹加快八	, 17(1) PN/JH	A/L 从J	
	添加吠別惧丸			<u>^</u>
	名称*	映射规则名称		
				·
	协议*	OPC	T	
	协议* 源对象*	OPC		
	协议* 源对象* 目的对象*	OPC IPG1 IPG1	× ×	
	协议* 源对象* 目的对象* 目的端口*	OPC IPG1 IPG1	v v	
	协议* 源对象* 目的对象* 目的端口*	OPC IPG1 IPG1 IAN2		
	协议* 源对象* 目的对象* 目的端口* 入口接口*	OPC IPG1 IPG1 LAN3		
Æ	协议* 源对象* 目的对象* 目的端口* 入口接口* 入口设备IP*	OPC IPG1 IPG1 LAN3 192.160.10.10	× ×	
-6	协议* 源对象* 目的对象* 目的端口* 入口按口* 入口设备IP* 入口端口*	OPC IPG1 IPG1 LAN3 192.160.10.10	× × ×	
-5	 协议* 源对象* 目的对象* 目的端口* 入口按口* 入口设备IP* 入口端口* 	OPC IPG1 IPG1 LAN3 192.160.10.10		
-5	 协议* 源对象* 目的对象* 目的端口* 入口按口* 入口设备IP* 入口端口* 	OPC IPG1 IPG1 LAN3 192.160.10.10	、 、 、 、	提交



