统一安全管理平台

用户手册

AVCOMM 恩创®

统一安全管理平台

用户手册

关于此用户手册

此用户手册旨在指导专业安装人员安装和配置统一安全管理平台。包括帮助避免意外发生问题的步骤。

注意:

只有合格且经过培训的人员才能对此产品进行安装、检查和维修。

免责声明

AVCOMM保留随时更改本手册或产品硬件的权利，恕不另行通知。此处提供的信息目的是为了保证其准确可靠。但是可能不会涵盖所有的细节和更改，也并未提供在安装、操作或维护过程中遇到的所有可能的意外情况。如需更多信息，或出现未完全包含在此手册中的特定问题，应将此提交给AVCOMM。用户有责任确定手册是否有任何针对添加的新信息和/或纠正可能的无意造成的技术或印刷错误进行的不定期更新和修订。AVCOMM对其被第三方使用不承担任何责任

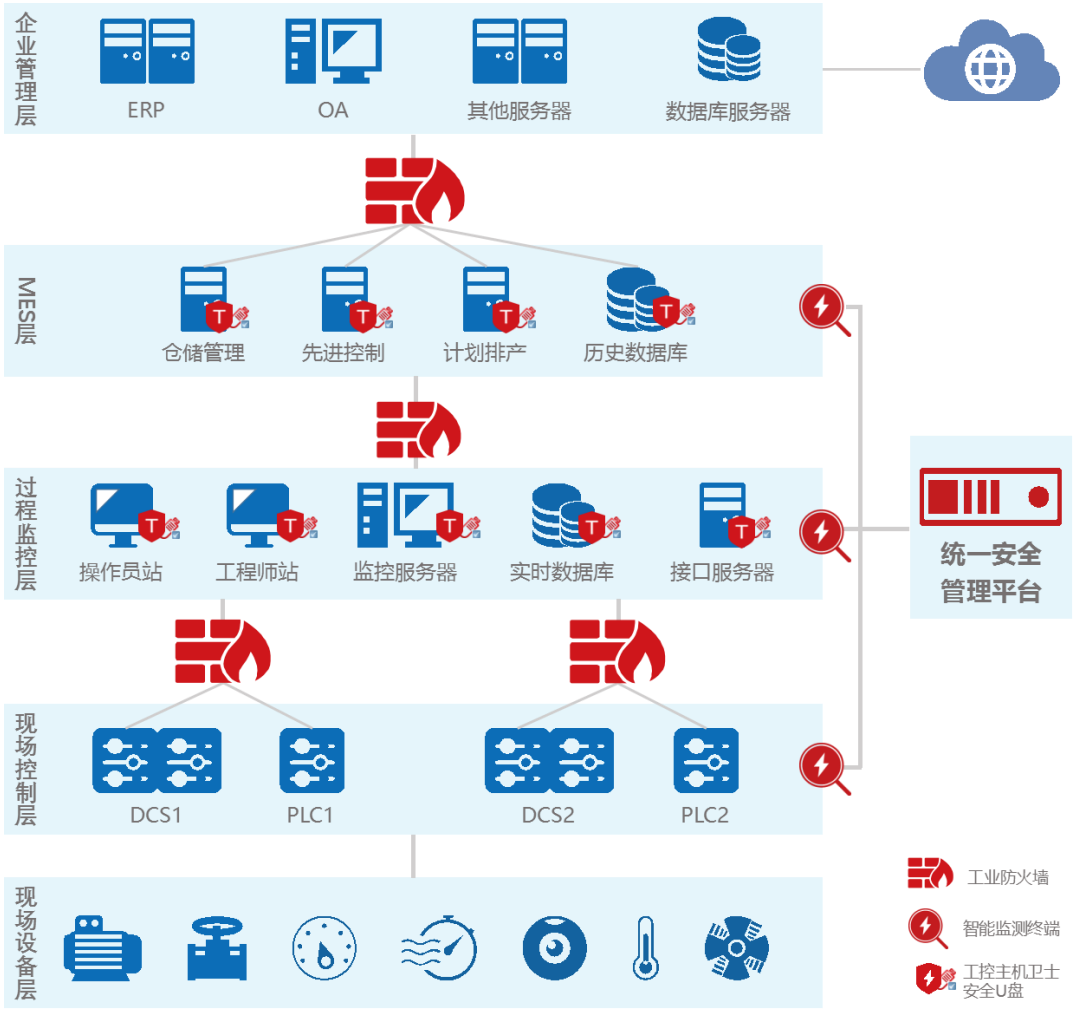
AVCOMM 在线技术服务

在 AVCOMM，您可以使用在线服务表来请求支持。提交的服务表保存在服务器上，供 AVCOMM 团队成员分配任务并监控您的服务状态。如遇任何困难，请随时发邮件至 sales@n-tron.com.cn

目录

1. 统一安全管理概述

1.1 统一安全管理组网图



1.2 产品说明

恩创统一安全管理平台可以对恩创公司生产的工业防火墙、智能监测终端和被主机卫士加固过的工作站进行集中管理，并对外提供 Web 管理能力。

管理员通过 Web 管理界面即可对系统内已经安装过恩创公司的产品进行统一管理，这包括：

- 查看已经安装的工业防火墙、智能监测终端和主机卫士当前的工作状态；
- 查看已经部署或者配置新的工业防火墙的防火墙策略、白名单策略以及查看和处理已经产生的告警日志和非法报文的拦截记录；
- 查看已经部署或者配置新的智能监测终端的工业协议白名单监测策略、违反协议规约策略、无流量策略、异常流量基线配置等及查看和处理相关的日志告警；
- 查看已经部署或者配置新的主机卫士相关的安全策略和查看处理日志报警；

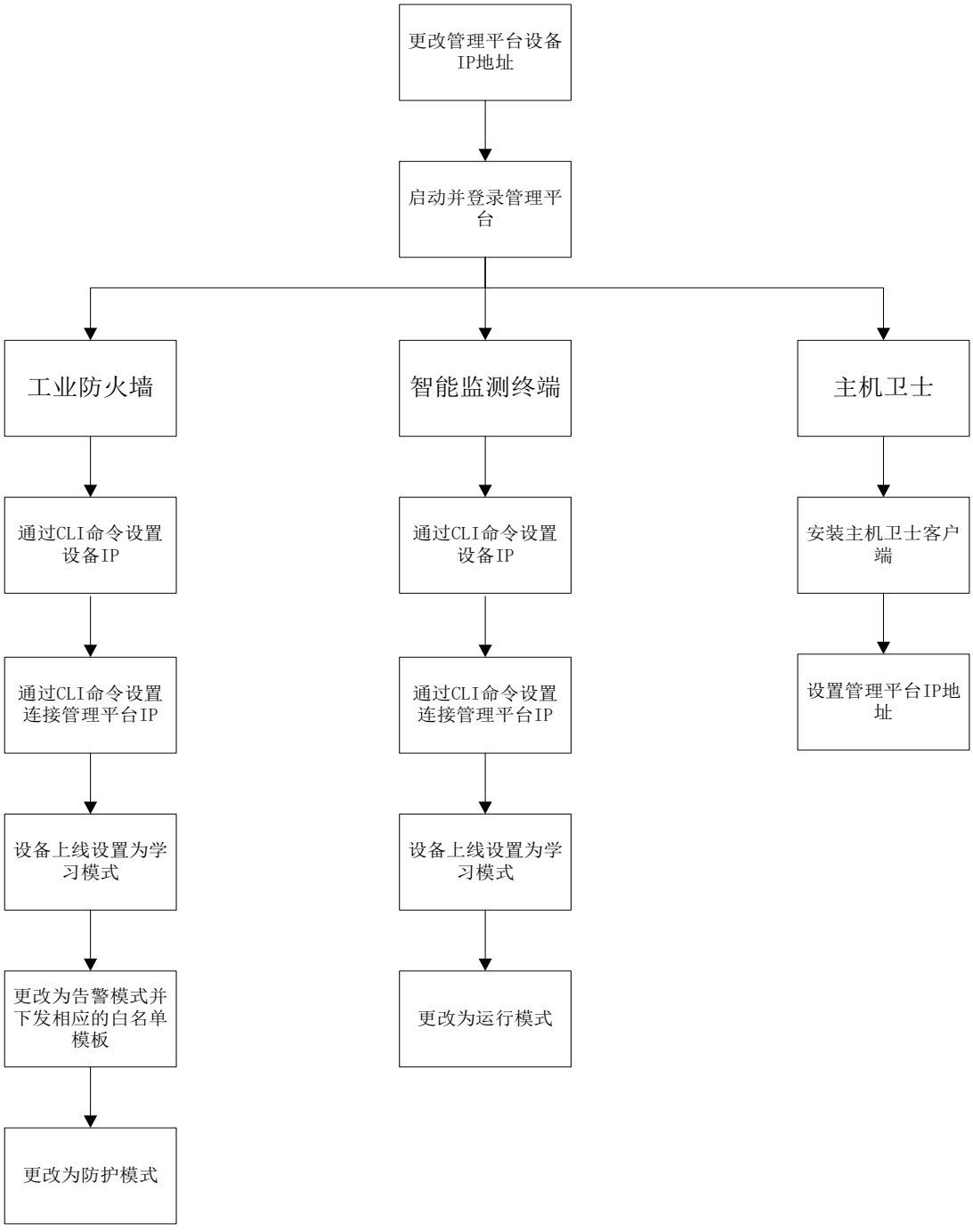
➢ 配置系统相关的数据库备份策略、可信主机和管理用户；

其中工业防火墙和监控审计的智能监测终端通过自身专有的管理网口接入与统一安全管理平台相通的网络，被主机卫士加固过的工作站通过已有的物理连接接入与管理平台相通的网络。

工业防火墙、监控审计的智能监测终端和统一安全管理平台出厂时有默认 IP，需要通过指定的方式更改成客户可以使用的 IP 地址，具体更改方法见下文。

1.3 操作步骤

统一安全管理操作步骤流程图，简单介绍统一安全管理平台控制工业防火墙、智能监测终端和主机卫士的基本步骤，详细操作请参考相关章节。（统一安全管理平台以下简称管理平台）



1.4 关于本手册

本手册主要面向客户公司的网络安全系统的超级管理员、管理员和审计员，介绍如何配置和管理工业防火墙、主机加固、监控审计和系统配置。在配置时，也可以通过在线帮助，查看各个细节。阅读本手册需要具备以下的基础知识：

- ✓ 信息系统管理
- ✓ 常用浏览器操作
- ✓ 基本的网络知识

如果要精通工业防火墙、主机加固、监控审计和系统配置的配置与管理，请仔细阅读本手册。

1.5 如何使用本手册

本手册主要对工业防火墙、主机加固、监控审计和系统配置进行尽可能的详细介绍。关于更多的信息，请查看主页：www.n-tron.com.cn

1.6 图形界面格式约定

格　式	意　义
<>	带尖括号“<>”表示按钮名，如“单击<保存>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[防火墙管理]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

2. 统一安全管理平台登录

2.1 统一安全管理平台的启动

管理平台要先于其被管理的设备启动。按照安装手册的说明，检查管理平台硬件已经正确配置完毕后，将电源线接通，将管理平台的电源按钮置于“on”档，管理平台将开始启动。正常情况下管理平台会自动完成整个启动过程。旧版本的管理平台（含有 6 个网口的设备）默认请将网线与 ETH4 连接，新版本的管理平台（只含有 2 个网口的设备）默认请将网线与 1 号网口连接，无论是旧的还是新的管理平台，可使用的 **IP 地址默认是 192.168.8.8**（此为管理平台默认 IP 地址，后续可根据需要自行修改）。

管理平台启动完成后，在网络可达管理平台的主机上开启谷歌游览器（推荐使用谷歌游览器），并输入 https://192.168.8.8:8440/如下类似的网址：

https://192.168.8.8:8440(新版本) 或

http://192.168.8.8:8080(老版本)

即可以访问管理平台，进行后续的登录和配置。

📖 **说明：**

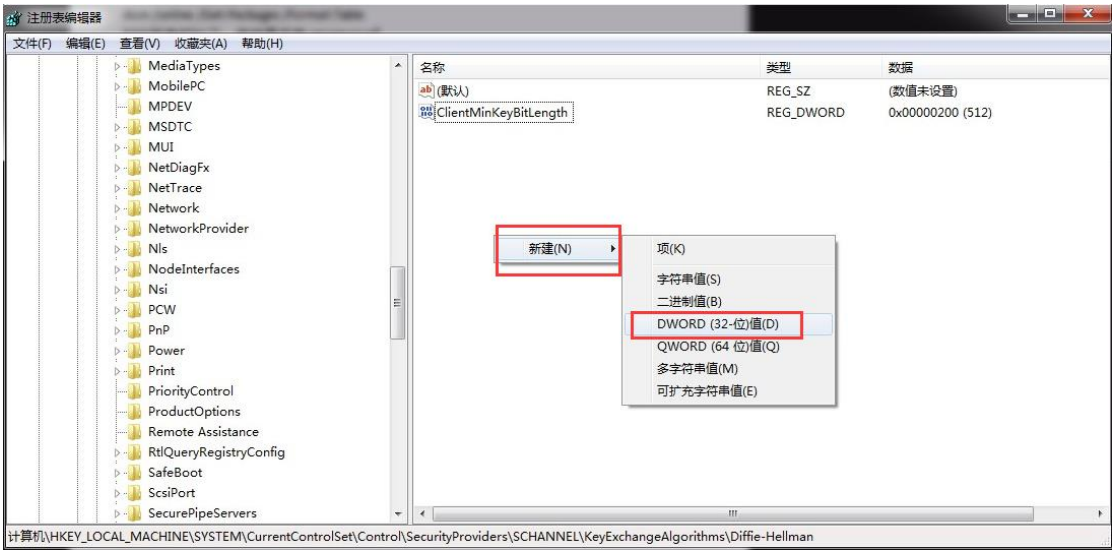
如果浏览器报如下图的错误，您只需要点击浏览器页面下面的“高级”，然后再选择“继续前往192.168.[redacted]（不安全）”即可。

📖 **说明：**

如果 IE 浏览器无法访问，请打开注册表，找到如下注册表路径：

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

鼠标右键选择新建，选择 DWDRD（32 位），修改名称为 ClientMinKeyBitLength，修改数据为 00000200。



2.2 管理平台的登录

管理平台启动后，在浏览器中输入正确的管理平台所在的管理页面的地址，在弹出如图 2-1 所示的

登录对话框后，输入正确的用户名和密码，点击<登录>，将进入系统的配置页面。

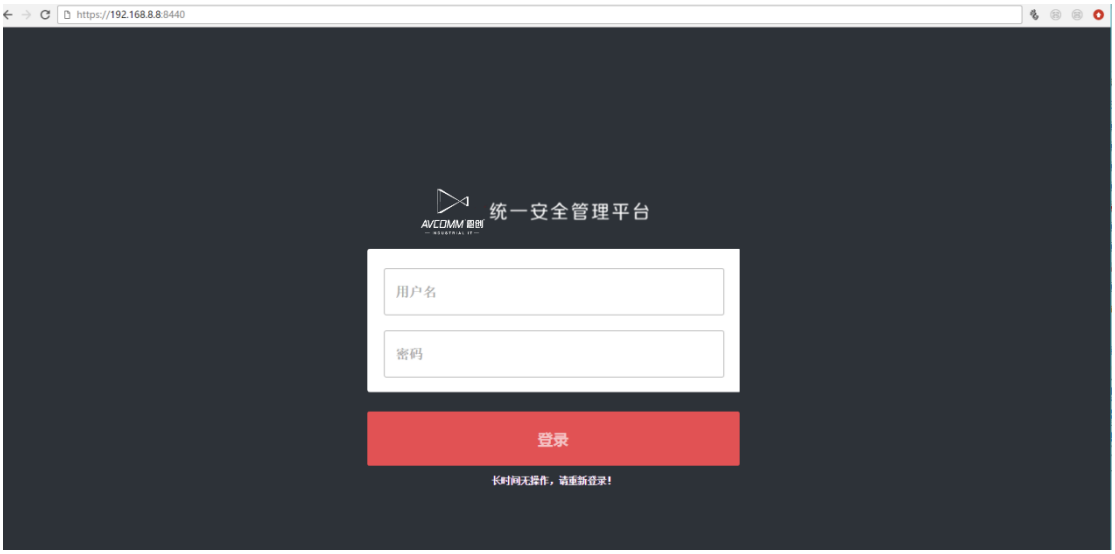


图 2-1 管理平台启动后的页面

目前管理平台支持四种角色的用户，如果是首次登录管理系统，将以默认的用户“admin”和默认密码“Admin@123”进行登录操作，进入系统后，不同角色的用户拥有不同的权限。可以创建其它角色的用户为系统操作员，但创建后需经过系统审核员批准后才会真正的生效。

系统包括的角色有：系统操作员、系统审核员、配置管理员、审计管理员。如果配置了自定义的用户，后续可以使用这些用户进行分权管理。

2.3 查看管理平台版本

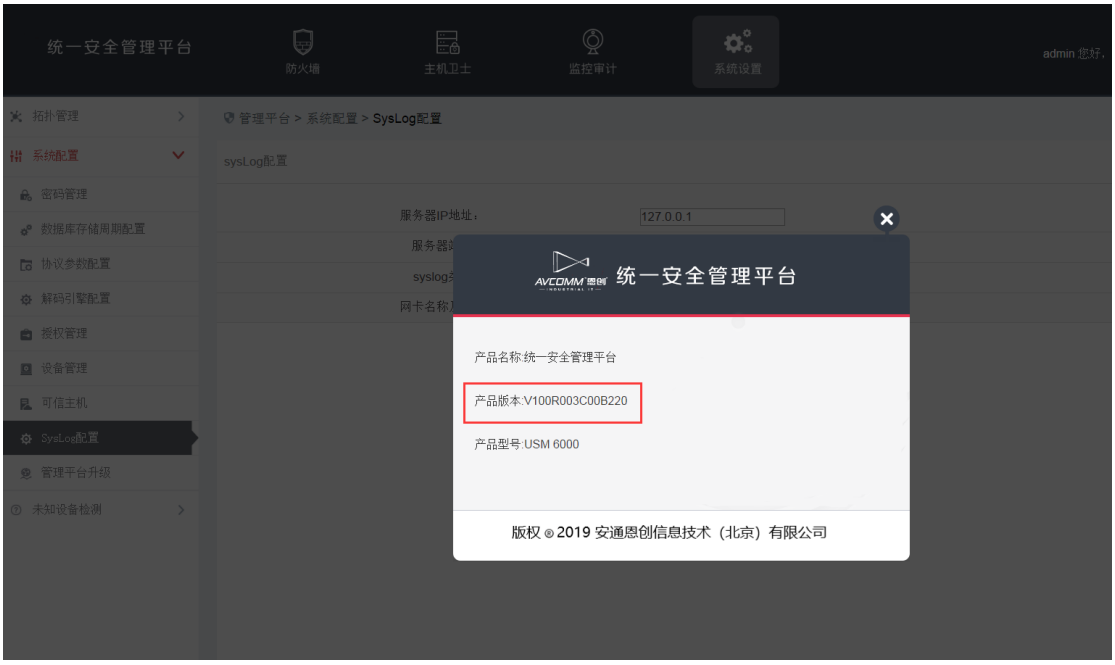
登录管理平台后点击<关于>按钮，查看管理平台版本信息。（如图 2-2 所示）

图 2-2 管理平台版本信息

2.4 管理平台退出

点击<退出>按钮，退出管理平台。（如图 2-3 所示）

图 2-3 管理平台退出



3. 工业防火墙

3.1. 产品介绍

3.1.1 产品概述

工业防火墙（又可叫做可信网关、网关）是安通恩创信息技术（北京）有限公司完全自主研发的一系列工业防火墙产品的总称，本系列产品目前有 S1100/S2100/S3100 三个型号，产品的硬件与软件均拥有完全自主知识产权，坚决杜绝后门的隐患，本产品拥有多种网络接入模式(同时支持电口和光口)，管理形式上采用集中管理分散部署的方式。对工业防火墙进行配置管理的统一安全管理平台是产品不可分割的一部分，该平台采用 B/S 架构，管理员可在任意连通到管理平台的机器上便捷的访问和管理，大幅提高运维效率，有效降低维护成本。产品硬件采用完全符合工业标准的自主设计，可以部署和应用到各种复杂的工业生产环境，硬件经过 CE，CC 和 FCC 等业内顶级标准认证，可以稳定长期不间断运行，大幅减少客户的系统停车时间。工业防火墙软件采用完全自主可控的架构设计，各主要功能模块互相配合，对流通在客户工控网络中的所有数据进行全方位的解析、判断和控制，有效保障客户正常生产数据的传输，完全杜绝非法数据和病毒在客户工控网络中的分散和传播，最大程度上保证了客户生产的长期稳定运行。

3.1.2 外观与说明

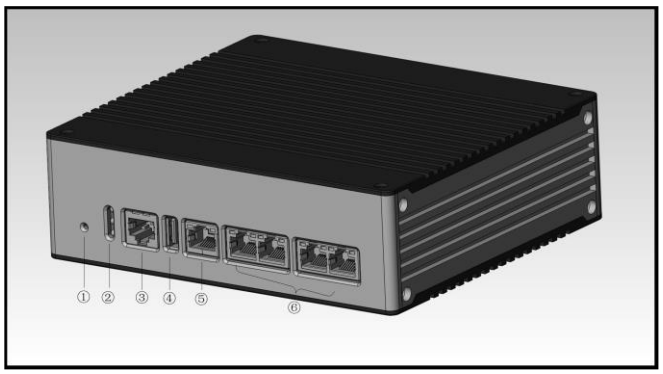


图 3-1 产品系列中 S2100 的外观

①Reset 复位按键
②LED 指示灯
③Console 串口，RS232
④USB 2.0接口
⑤管理网口，10/100/1000BASE-T 自适应以太网电口
⑥业务网口，10/100/1000BASE-T 自适应以太网电口；共分 2 对，紧连在一起的为一对，一对中的任意一个可以做为入口，另外一个作为出口；两对之间不可交叉。

3.1.3 指示灯说明

设备上有 3 个指示灯，分别为 PWR、RUN、BP 指示灯

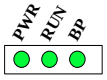


图 3-2 指示灯

表格 1 工业防火墙指示灯说明

指示灯	面板丝印	状态	说明
电源指示灯	PWR	长灭	没有上电或主机电源故障
		绿色常亮	电源正常，主机正常上电
运行指示灯	RUN	长灭	设备未上电或者故障
		绿闪	设备正常运行
		红闪	设备故障或者受到网络攻击
旁路指示灯	BP	长灭	未启动 BPYASS 功能
		常亮	启动 BYPASS 功能
以太网电接口指示灯	MGMT ETH1/ETH2/ETH	常灭	对应接口处于未连接状态
		指示灯颜色	绿色表示当前工作在千兆速率下

	3/ETH4		橙色表示当前工作在百兆速率下
		指示灯常亮	接口已经建立连接
		指示灯闪烁	接口正在收发数据

3.1.4 技术规格

表格 2 工业防火墙技术规格

型号	S1100	S2100	S3100
功能特性			
防火墙功能	状态检测包过滤防火墙功能		
深度报文解析	OPC、Siemens S7、Modbus-TCP/Modbus-RTU、Ethernet/IP（CIP）、MMS、IEC104、DNP3、FINS、PROFINET 等协议的深度报文解析，支持 OPC 的动态端口，OPC、Siemens S7、Modbus-TCP、Ethernet/IP（CIP）、MMS、IEC104、DNP3 只读，报文格式检查，完整性检查，支持 OPC 基金会发布的 OPC 3.0 规范。		
白名单功能	基于白名单的访问控制策略		
智能学习规则	可通过智能协议检测来辅助生成规则		
规则测试模式	提供测试模式验证安全规则的正确性和业务适用性		
三级权限管理	管理员权限分为审批管理员，配置管理员，审计管理员类型		
日志本地缓存	安全日志可以发给日志服务器或本地缓存		
IP/MAC 地址绑定	支持手动或者学习建立 IP、MAC 绑定关系，防止地址欺骗		
用户自定义白名单应用	根据客户现场实际业务来识别工控协议，方便准备无误报		
未知设备检测	快速发现非法接入的设备		
会话管理	可实时查询正在进行的会话和个性设置会话老化时间		
性能特性			
数采点数	100000 点以上		
数据包时延	满配策略条件下小于 100us		
并发连接	300000	300000	300000
用户数量限制	无限制		

Bypass 功能	断电或系统异常时自动 bypass		
硬件规格			
处理器	专用多核网络处理器	专用多核网络处理器	专用多核网络处理器
内存	DDR3 1G	DDR3 1G	DDR3 2G
日志存储	4G	4G	4G
业务端口	2 端口 RJ45 10/100/1000Mbps 自适应 2 端口 SPF 10/100/1000Mbps	4 端口 RJ45 10/100/1000Mbps 自适应	6 端口 RJ45 10/100/1000Mbps 自适应 6 端口 SFP 10/100/1000Mbps 自适应
Bypass	1 对	2 对	3 对
管理端口	1 端口 10/100/1000Mbps 自适应	1 端口 10/100/1000Mbps 自适应	1 端口 10/100/1000Mbps 自适应
串行接口	RJ45 调试端口	RJ45 调试端口	RJ45 调试端口
USB 接口	1 端口 USB 2.0	1 端口 USB 2.0	1 端口 USB 2.0
尺寸/电源/运行环境			
工作环境	温度：-40～75℃ 湿度：5%-95% 无凝结	温度：-40～75℃ 湿度：5%-95% 无凝结	温度：0～40℃ 湿度：20%-80% 无凝结
存储环境	温度：-40～85℃ 湿度：5%-95% 无凝结	温度：-40～85℃ 湿度：5%-95% 无凝结	温度：0～40℃ 湿度：20%-80% 无凝结
MTBF	25 万小时	25 万小时	25 万小时
电源	12-36V DC 1+1 冗余供电	12-36V DC 1+1 冗余供电	90-265V/AC 1+1 冗余供电
最高功率	<7W	<7W	<250W
尺寸（WxDxH）mm	168 x 118 x 58	168 x 118 x 58	482 x 434 x 30
安装方式	35mm 标准 DIN 导轨卡接	35mm 标准 DIN 导轨卡接	标准 19 寸机架安装
防护等级	IP40	IP40	IP40
认证	CE、CB	CE、CB	CE、CB

3.2. 启动和登录

3.2.1 工业防火墙的启动

根据工业防火墙的硬件安装手册将工业防火墙安装到指定位置后，确保工业防火墙的电源接头正常，将其与要求的电源接通后，工业防火墙将开始正常启动，可以根据安装手册的说明来使用 console 口对工业防火墙的启动过程进行监控。

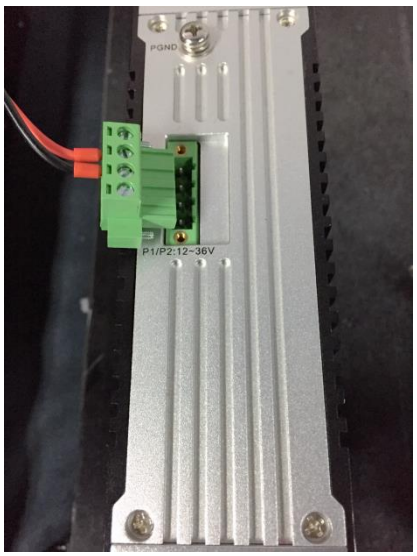


图 3-3 使用提供的电源线给工业防火墙接通电源

工业防火墙启动完成后，没有配置过任何安全策略的新工业防火墙将默认工作在“初始状态”的工作模式下，这种状态下工业防火墙透明存在，不拦截任何报文。如果是已经配置过安全策略，此时启动后工业防火墙将使用上次关闭前的安全配置。

工业防火墙需要连接到管理平台正常上线后方能配置，连接管理平台请将网线插入到 MGMT 口，出厂时所有工业防火墙的默认 IP 地址被设置为 192.168.8.6，在接入到管理平台所在的网络前后都可以更改工业防火墙 MGMT 口的地址。在管理平台能够正常管理工业防火墙前，可通过工业防火墙的命令行接口配置管理口的地址和设置要连接到的管理平台的地址。工业防火墙的命令行使用在下一小节介绍，设置工业防火墙 MGMT 口的地址请参考 3.2.2.4 更改管理口的 IP 地址，设置连接到的管理平台的地址请参考 3.2.2.5 设置管理平台的地址

3.2.2 CLI 的使用

CLI（Command Line Interface，命令行接口）是用户与设备之间的文本类指令交互界面。用户输入文本类命令，通过输入回车键提交设备执行相应命令，从而对设备进行配置和管理，并可以通过查看输出信息确认配置结果。

由于设备的一些操作需要在此界面下完成，所以工业防火墙设备启动后，需要使用 CLI 命令进行一些必要的配置，比如设置连接到的管理平台的地址。

工业防火墙设备支持多种方式进入命令行接口界面，比如通过 Console 口直接连接或者通过 Telnet/SSH 登录设备后进入命令行接口界面等。无论哪种方式，登录设备时默认使用的用户名为：admin，默认密码为：admin。设备的命令行接口界面下图所示。

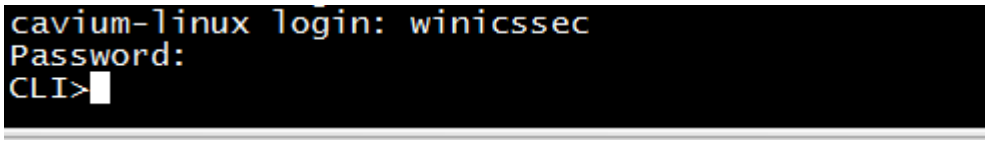


图 3-4 命令行界面

常用命令简介：

3.2.2.1 帮助

CLI>help 显示帮助信息。

3.2.2.2 系统统计信息相关

CLI>show pkt stat 查看各层次报文统计信息
CLI>show mgmtip 查看管理口 IP 地址信息
CLI>show fpa 查看 FPA 信息，主要为各种内存统计信息
CLI>show mem pool 查看 mem pool 内存信息

3.2.2.3 进入系统配置视图

CLI> config 进入系统配置视图，可进行下面的配置。

3.2.2.4 更改管理口的 IP 地址

注意：如果进行配置，需先使用 config 命令进入系统视图 CLI#set mgmtip <ip> [netmask] 更改设备管理口的 IP 地址
例如：将工业防火墙 A 管理口的 IP 地址更改为 192.168.8.6，掩码 255.255.255.0 的完整命令如下：
CLI# set mgmtip 192.168.8.6 255.255.255.0

3.2.2.5 设置管理平台的地址

CLI>show serverip 查看工业防火墙上配置的统一安全管理平台的 IP 地址
CLI#set serverip <IPV4ADDR:serverip> 设置工业防火墙需要连接到的统一安全管理平台的 IP 地址
例如：管理平台的地址为 192.168.8.8，那么完整命令如下：CLI> set serverip 192.168.8.8
CLI>config 设置工业防火墙网关命令
例如：需要增加网关地址为 192.168.1.1，那么完整命令如下：CLI# set mgmtgw 192.168.1.1

3.3. 防火墙管理

3.3.1 功能介绍

工业防火墙是管理平台的管理对象，所有策略配置都是针对具体的工业防火墙，如防火墙的安全策略规则都要下发到具体的工业防火墙才能发挥作用。为了方便的对含有相同业务的多个工业防火墙进行管理，系统还引入了防火墙分组的概念。

防火墙分组是对同一业务的工业防火墙进行配置的统一下发和控制，当操作分组时，将影响到该分组下的所有在线工业防火墙，以使同一分组的工业防火墙进行统一的配置。如果工业防火墙有个性化的配置，需要先将其从自己所在的分组中解除。

3.3.2 防火墙管理

在浏览器成功打开并登录管理平台的 Web 管理界面后，在上方菜单栏中找到[工业防火墙]，点击按钮(如图 3-5 所示)，然后在左侧导航栏找到[防火墙管理/防火墙管理]，点击菜单左侧[防火墙管理](如图 3-6 所示)，将在右侧的展示页面中看到防火墙管理的页面（如图 3-7 所示

图 3-5 上方菜单栏中的工业防火墙

图 3-6 导航栏中的防火墙管理

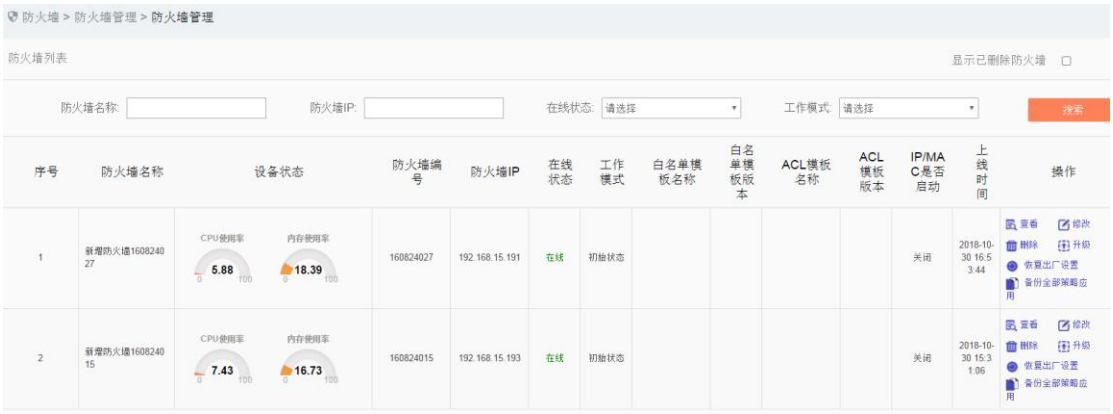


图 3-7 防火墙管理展示页面

此处可以查看到工业防火墙当前的运行状态，含义如下：

表格 3 防火墙管理列表显示说明

列名称	说明	
防火墙名称	系统或用户对每个工业防火墙的一个称呼，如“生产车间 1 控制室工业防火墙”	
设备状态	工业防火墙当前的运行状况，包括 CPU 和内存使用率。如果某项数值 1min 内一直处于超负荷状态，将产生相应的告警。	
防火墙编号	由系统自动分配的工业防火墙的唯一标识号，一个标识号代表唯一一个工业防火墙	
防火墙 IP	工业防火墙管理网口的 IP 地址	
在线状态	当前工业防火墙是处于与管理平台连通的状态（即在线）还是未连通（即离线）的状态	
工作模式	工业防火墙当前工作在哪种工作模式下，新工业防火墙默认是“初始状态”	
白名单模板名称	工业防火墙运用的白名单规则模板的名称，如果为空则表示工业防火墙当前没有设置白名单规则	
白名单模板版本	工业防火墙运用的白名单规则模板的版本，版本与模板的 ID 唯一确定一组白名单规则，每次编辑白名单并保存后，版本号会自动+1	
上线时间	工业防火墙最新一次上线时的时间	
操作	查看 查看	查看工业防火墙的更多详细信息，每个工业防火墙已经授权的功能在此子页面下进行查看
	修改 修改	对工业防火墙的信息、工作模式、白名单模板、安全策略规则等等进行修改和设置

	删除 删除	删除离线的工业防火墙，无法删除在线的工业防火墙。删除后的工业防火墙可以点击“显示已删除”进行信息查看和恢复
	升级 升级	在线升级工业防火墙上运行的软件，只有工业防火墙在线时才可以进行此操作，参照 3.3.4 防火墙升级章节
	恢复出厂设置 恢复出厂设置	一键还原防火墙设备出厂设置
	备份全部策略应用 备份全部策略应用	将源设备上正在应用的全部策略拷贝到一台或多台其他在线且非学习模式下的设备上进行下发应用

3.3.2.1 信息查看

点击[工业防火墙管理]中“操作”属性列中的<查看>按钮，将显示(如图 3-8 所示)工业防火墙的详细信息：

图 3-8 工业防火墙信息查看页

此页面除了有设备的更详细信息外，最重要的就是授权信息，点击<查看授权信息>将打开授权信息页面，更具体的授权信息相关操作参照 3.3.3 授权管理章节。

点击本页面的<返回>按钮，将返回到[防火墙列表显示]页面。

3.3.2.2 修改防火墙

点击[防火墙列表]中操作列下的<修改>按钮（如图 3-9 所示），将打开工业防火墙信息修改页面，可以分别修改“工业防火墙基本信息”、“工作模式信息”、“应用的白名单模板设置”、“防火墙安全策略模板”、“IP/MAC 地址绑定”（如图 3-10 所示）

图 3-9 修改按钮

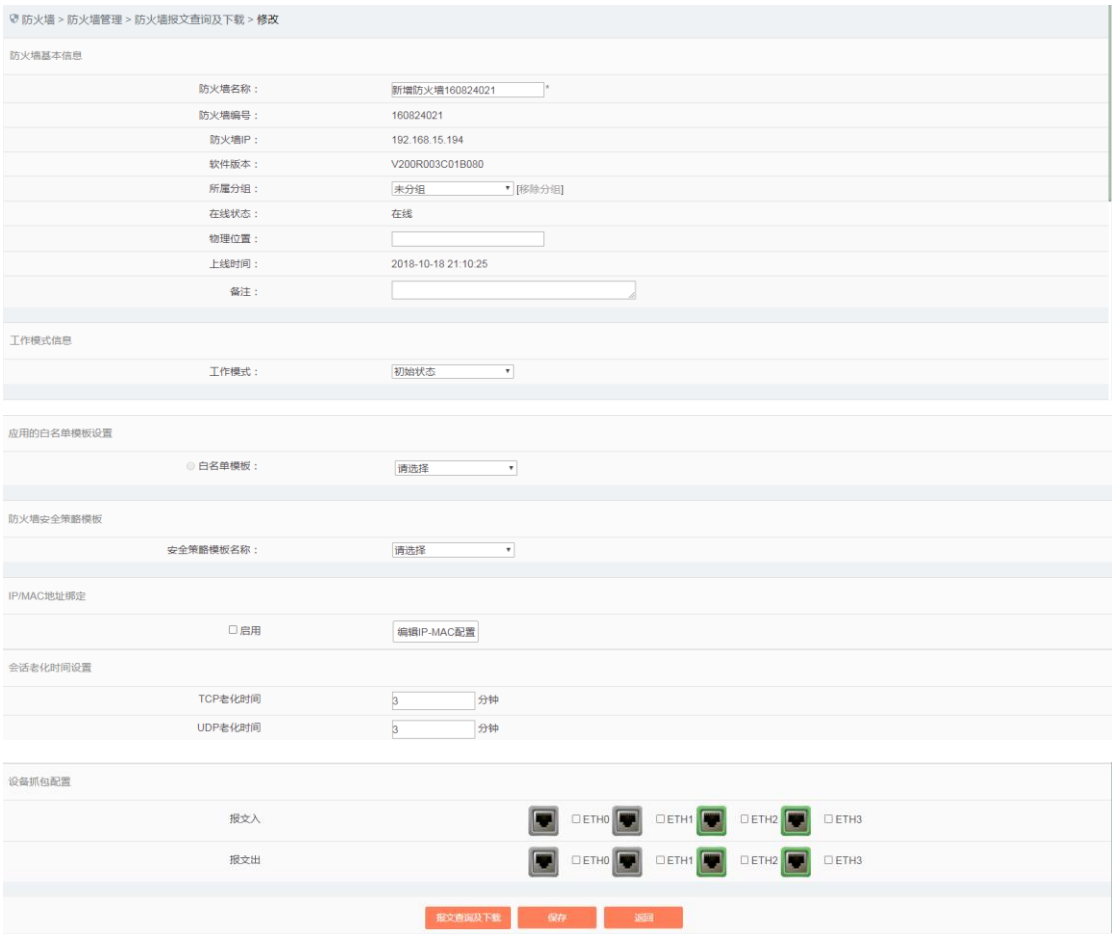


图 3-10 工业防火墙修改页面

表格 4 工业防火墙修改信息说明

列名称	说明
防火墙名称	给工业防火墙定义一个容易理解、记忆且有含义的名称，建议配置工业防火墙时修改此项
物理位置	工业防火墙所属的部门或者所在的物理位置，如生产车间 1 控制室，可选填
备注	可选填，附加说明信息
工作模式	1.如果当前模式为学习模式，工业防火墙模式下拉列表项只有学习完成和学习模式 2.如果当前为学习完成状态，工业防火墙模式下拉列表项有学习模式、告警模式和防护模式 3.如果当前模式为告警模式，工业防火墙模式下拉列表项有学习模式和防护模式 4.如果当前模式为防护模式，工业防火墙模式下拉列表项有学习模式和

	告警模式 5.如果用户更改模式为学习模式时，下面的白名单模板设置项将被灰掉，不可操作 6.如果用户由学习模式更改为学习完成，此时会有白名单模板生成编辑框出现，让用户命名学习生成的白名单模板 7.工业防火墙如果有分组,则此时用户无法更改工作模式和白名单模板，需要退出分组后才可操作。	
白名单模板	工业防火墙当前运用的白名单规则模板，只有工业防火墙更改为告警模式或防护模式时编辑框被点亮，此时必须选择一个白名单模板才能够保存。	
安全策略模板名称	工业防火墙当前运用的安全策略模板，可选填	
IP/MAC 地址绑定	配置 IP/MAC 地址绑定规则	
会话老化时间设置 设备抓包配置	设置 TCP、UDP 连接的会话老化时间 勾选抓包网口，支持抓取 eht0、eth1、eth2、eth3、eth4 和 eth5 任意一个或者多个端口的报文，可以指定抓取每个端口进、出或者双向报文。管理平台对抓取到的报文按设备端口分类存储，可以查询和下载报文。 报文查询及下载　查看网口抓包抓取到的全部报文，可下载	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到工业防火墙信息列表显示页面
	返回	忽略所有的修改，返回到工业防火墙信息列表显示页面

3.3.2.3 删除防火墙

点击[防火墙列表]中操作列下的<删除>按钮，可以把不再使用的离线工业防火墙进行删除。(如图 3-11 所示)：

图 3-11 工业防火墙删除按钮

但注意在线的工业防火墙无法执行删除操作，如点击“删除”会有相应的提示。

3.3.2.4 检索防火墙

在[防火墙列表]页面中，可以根据条件对工业防火墙进行检索，(如图 3-12 所示)：

图 3-12 检索工业防火墙

3.3.3 授权管理

License 即许可证，是设备供应商对产品特性的使用范围、期限等进行授权的一种合约形式，License 可以动态控制产品的某些特性是否可用。当需要时，用户可以通过购买 License 激活产品的某些特性和功能特性。对于本产品，每个工业防火墙设备中只能存在一个处于激活状态的 License 文件，激活新的 License 将会使旧的 License 失效。

目前设备支持以下方法激活 License：

通过统一安全管理平台手动激活

当购买或续购 License，获得 License 授权证书后，通过登录统一安全管理平台指定页面，对所管理的设备进行授权和授权的更新。

工业防火墙授权管理包含授权工具、工业防火墙和统一安全管理平台三大组件。授权工具属于恩创公司，只允许在公司内指定用户使用。

3.3.3.1. 查看授权

点击左侧导航栏[防火墙管理]，打开后的页面选择要查看授权的工业防火墙，点击操作列下的<查看>按钮，在打开的页面中，有(如图 3-13 所示)的按钮：

图 3-13 查看工业防火墙的授权信息

- 查看授权信息

  点击<查看授权信息>打开后，将弹出具体的授权信息页面，(如图 3-14 所示)

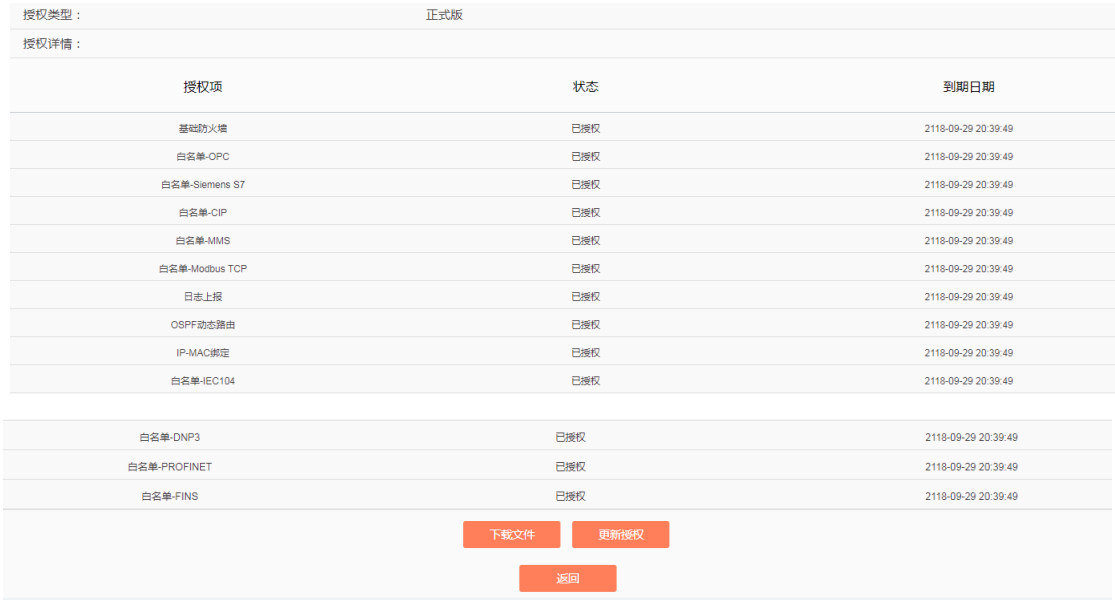


图 3-14 授权详情查看页

此页面显示当前工业防火墙的授权详情。

- 下载文件

  得到工业防火墙的授权文件，可以将此文件发给生产商，用来后续更新授权信息

- 更新授权

  更新当前工业防火墙的授权信息

- 返回

  关闭当前页，返回到工业防火墙查看页面

3.3.3.2. 获取授权文件

在打开的工业防火墙授权详情页上，点击<下载文件>按钮，可以将授权文件下载下来，发给生产商，后续生产商将以此文件为依据，更新新的授权给用户。

3.3.3.3. 更新防火墙授权信息

在打开的工业防火墙授权详情页上，点击<更新授权>按钮，将弹出授权文件选择对话框，以把用户从厂商获取到的最新的授权文件更新到指定的工业防火墙中，(如图 3-15 所示)

图 3-15 选择要更新到工业防火墙的新授权文件

- 浏览

点击浏览后，将弹出文件选择对话框。

找到新的授权文件后(如：以设备 ID 为名字，后缀为“.dat”的文件)，双击文件或选择<打开>，之后再点击<上传>按钮，浏览器将此文件首先上传到管理平台所在的服务器，然后通知给工业防火墙，工业防火墙将执行更新授权动作，更新成功，用户将可以在查看页面看到新的授权信息。

- 返回

点击<返回>将不执行任何操作，直接返回到工业防火墙授权详情页。

3.3.4 防火墙升级

当工业防火墙有新的功能更强大、运行更稳定的版本推出后，用户可以通过统一安全管理平台，对工业防火墙设备进行远程升级操作。

打开[防火墙管理]页面后，点击[防火墙信息显示列表]中操作列下的<升级>按钮，将弹出[选择升级文件]对话框，(如图 3-16 所示)

图 3-16 工业防火墙升级文件选择

- 选择文件

点击“选择文件”后，将弹出文件选择对话框。找到新的升级文件后(如：sys-fw.tar.gz)，双击文件或选择<打开>

- 开始升级

点击此按钮，浏览器将此升级文件首先上传到统一安全管理平台所在的服务器，然后通知并下发升

级文件给工业防火墙，工业防火墙将执行具体的升级动作。

- 关闭

  点击<关闭>将不执行任何操作，直接返回到[防火墙信息显示列表]页。

3.3.5 IP/MAC 地址绑定

在左侧导航栏找到[防火墙管理/防火墙管理]，点击<修改>，将打开工业防火墙的修改页面。(如图 3-17 所示)

图 3-17 工业防火墙管理修改页面中的 IP/MAC 配置

3.3.5.1. 规则配置

可以针对单个工业防火墙或者某个工业防火墙分组“启用”此功能。只有功能启用后，方可编辑相关配置。如果启用了 “IP/MAC 地址绑定”，点击<编辑 IP/MAC 配置>按钮，跳转到 IP/MAC 配置页面，(如图 3-18 所示)

图 3-18 规则配置页面

点击<添加>按钮增加规则，点击 删除，删除当前规则，点击<保存>按钮，保存规则。

3.3.5.2. 学习数据

点击<学习数据>按钮，跳转到学习数据页面，(如图 3-19 所示)

图 3-19 学习数据页面

根据 IP 地址与 MAC 地址条件搜索学习到的学习数据，点击<删除>按钮，删除选中数据，(如图 3-20 所示)

图 3-20 删除学习数据

点击<添加选中规则>按钮，添加选中规则到规则配置列表，(如图 3-21 所示)

图 3-21 添加学习数据

3.3.6 分组管理

在左侧导航栏找到[防火墙管理/分组管理]，单击打开， (如图 3-22 所示)，将在右侧的展示页面中看到分组列表信息显示页面（如图 3-23 所示）。

图 3-22 导航栏中的分组管理

图 3-23 分组列表显示页面

此处可以查看到系统内所有工业防火墙分组的信息，含义如下：

表格 5 分组管理列表显示说明

列名称	说明	
防火墙分组名称	方便记忆的工业防火墙分组的名称，如“6#DCS 工业防火墙组”	
工作模式	分组下所有工业防火墙当前所处于的工作模式，没有添加即为初始状态	
白名单模板名称	分组下所有工业防火墙运用的白名单规则模板的名称，如果为空则表示分组当前没有设置白名单规则	
白名单模板版本	分组下所有工业防火墙运用的白名单规则模板的版本	
包含的防火墙	分组所包含的工业防火墙	
操作	查看	查看分组的更多详细信息

	修改	对分组的信息、工作模式、白名单模板、防火墙规则，包含的工业防火墙等等进行修改和设置
	删除	删除工业防火墙分组，无法删除含有工业防火墙的分组。

3.3.6.1. 添加分组

点击[分组管理]防火墙分组列表标签右侧的<添加>按钮（如图 3-24 所示），将弹出防火墙分组添加页面(如图 3-25 所示)

图 3-24 防火墙分组添加按钮

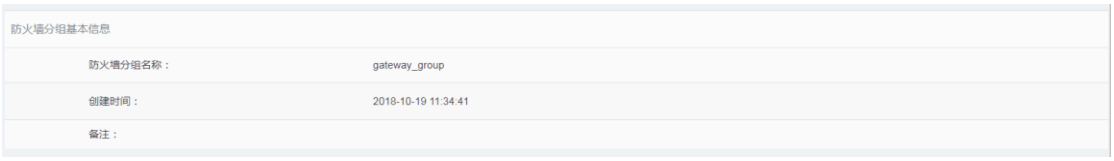


图 3-25 防火墙分组添加页

表格 6 防火墙分组添加信息说明

列名称	说明
防火墙分组名称	给分组定义一个容易理解、记忆且有含义的名称
备注	可选填，附加说明信息

添加时输入工业防火墙分组的名称和其它需要备注的信息，点击<保存>分组将添加完成，在工业防火墙分组列表中将可查看到新添加的分组。

3.3.6.2. 信息查看

点击[防火墙分组列表]中操作列下的<查看>按钮，将显示(如图 3-26 所示)的分组的详细信息：

图 3-26 分组信息查看页

点击<返回>按钮，将返回到[分组列表显示]页面。

3.3.6.3. 修改分组

点击[防火墙分组列表]中操作列下的<修改>按钮（如图 3-27 所示），将打开[分组信息修改]页面，可以分别修改分组的基本信息，分组的运行模式、分组当前应用的白名单模板和 IP/MAC 地址绑定配置（如图 3-28 所示）

图 3-27 修改按钮

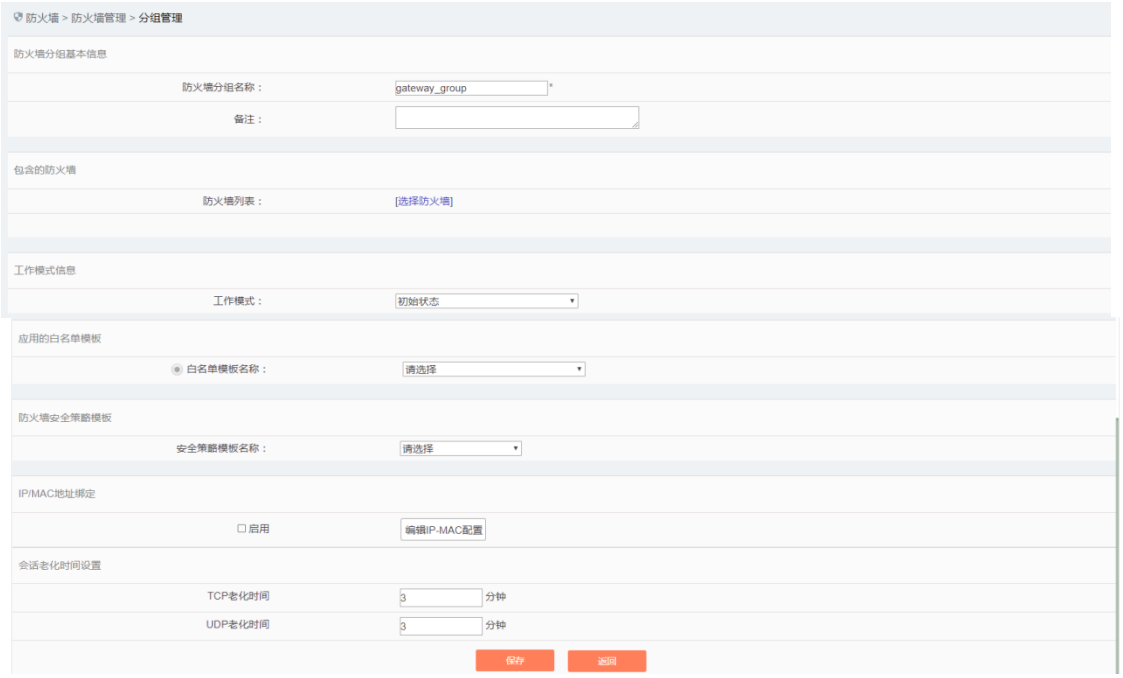


图 3-28 分组信息修改

表格 7 防火墙分组修改信息说明

列名称	说明
防火墙分组名称	给分组定义一个容易理解、记忆且有含义的名称
备注	可选填，附加说明信息
防火墙列表	当前分组下所有的工业防火墙，可以通过点击<选择防火墙>来进行编辑
工作模式	1.如果当前模式为学习模式，工作模式下拉列表项只有学习完成和学习模式 2.如果当前为学习完成状态，工作模式下拉列表项有学习模式、告警模

	式和防护模式 3.如果当前模式为告警模式，工作模式下拉列表项有学习模式和防护模式 4.如果当前模式为防护模式，工作模式下拉列表项有学习模式和告警模式 5.如果用户更改模式为学习模式时，下面的白名单模板设置项将被灰掉，不可操作 6.如果用户由学习模式更改为学习完成，此时会有白名单模板生成编辑框出现，让用户命名学习生成的白名单模板 7.更改分组的工作模式,分组下的所有工业防火墙都将被更改工作模式。	
白名单模板名称	分组运用的白名单规则模板的名称，只有工作模式更改为告警模式或防护模式时编辑框被点亮，此时必须选择一个白名单模板才能够保存。更改将影响到分组下的所有工业防火墙。	
安全策略模板名称	分组运用的安全策略模板的名称，更改将影响到分组下的所有工业防火墙。	
IP/MAC 地址绑定	启用、编辑 IP/MAC 地址绑定	
会话老化时间设置	设置 TCP、UDP 连接的会话老化时间	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到[分组信息显示]列表页面
	返回	忽略所有的修改，返回到[分组信息显示]列表页面

3.3.6.3.1. 添加防火墙到分组

在打开的[分组信息修改]页面下，点击<选择防火墙>将打开[防火墙选择]页面，(如图 3-29 所示)

图 3-29 分组中防火墙选择页

在打开的页面中选择需要的工业防火墙，并在最后一列“操作”点击选择；如想取消则将该列的“√”选掉即可。操作完成后点击<确定>按钮将完成操作

3.3.6.4. 删除分组

点击[防火墙分组列表]<操作>列下的<删除>按钮，可以把不再使用的分组进行删除。(如图 3-30 所示)

图 3-30 分组删除按钮

如果分组下包含有防火墙，则无法删除，需要先将分组下的工业防火墙都解除后再删除。

3.3.6.5. 检索分组

在[防火墙分组列表]页面中，可以根据条件对分组进行检索，(如图 3-31 所示)

图 3-31 检索分组

3.4. 白名单管理

3.4.1 功能介绍

工业控制系统的安全问题有别于传统 IT 网络安全问题，更注重的是可用性、可靠性，因此在技术理

念和产品实现上也完全不同。

工业控制系统强调的是确定性，所以什么样的流量应该在网络中传输是必须要明确和可控的，而传统的“黑名单”思想更注重的是威胁的识别和阻拦，这种思想一是需要频繁更新产品的“黑名单特征库”；二是对于新威胁往往事故发生了才能够提取特征和识别；三是这种产品经常出现漏报和误报。为了解决这些问题，恩创工业防火墙利用工业协议深度包解析技术，实现强大的工业协议白名单功能，通过智能学习引擎，帮助客户识别、定义和控制流通在工业现场中的合法指令，而对于未知的，无论是否对工业现场造成伤害，都不允许其“穿墙而过”，防护从“被动”受到伤害后增加黑名单特征转变为“主动”定义合法流量，防止未知威胁攻击，与工业现场要求的确定性和可控性完全吻合。

工业防火墙防护思想从“黑”到“白”，从“被动防御”到“主动防护”，完全并特别适用于各种工业生产网络系统现场。因此，工业防火墙重要的一个创新就是白名单管理功能。

管理平台的白名单管理功能就是方便用户查看、编辑和使用白名单。

3.4.2 模板管理

点击左侧导航栏的[白名单管理/模板管理](如图 3-32 所示)，进入[白名单模板管理]的页面（如图 3-33 所示）。

图 3-32 选择白名单模板管理

图 3-33 白名单模板管理

此处可以查看到系统内所有白名单模板的信息，含义如下：

表格 8 白名单模板列表显示说明

列名称	说明	
白名单模板名称	方便记忆的白名单模板的名称，如“从数采系统 1 学习到的白名单”	
版本号	白名单规则模板的版本，版本与模板的 ID 唯一确定一组白名单规则，每次编辑白名单并保存后，版本号会自动+1	
应用此模板的防火墙分组	正在使用此白名单模板的所有防火墙分组	
应用此模板的防火墙	正在使用此白名单模板的所有独立的工业防火墙	
白名单编辑	编辑	点击后将进入每个工业协议具体的白名单项编辑页面
	导出	点击后，会导出 Excel 格式的当前白名单规则
	导入	点击后，会将 Excel 格式的白名单规则导入到当前白名单中
操作	查看	查看白名单模板的更多详细信息
	修改	对白名单模板的信息进行修改和设置，系统内置的白名单模板无此按钮
	删除	删除白名单模板，无法删除正在使用的白名单模板，系统内置的白名单模板无此按钮

3.4.2.1 添加白名单模板

打开左侧导航栏的[模板管理]，点击模板管理列表标签右侧的<添加>按钮（如图 3-34 所示），将弹出白名单模板添加页面(如图 3-35 所示)

图 3-34 白名单模板添加按钮

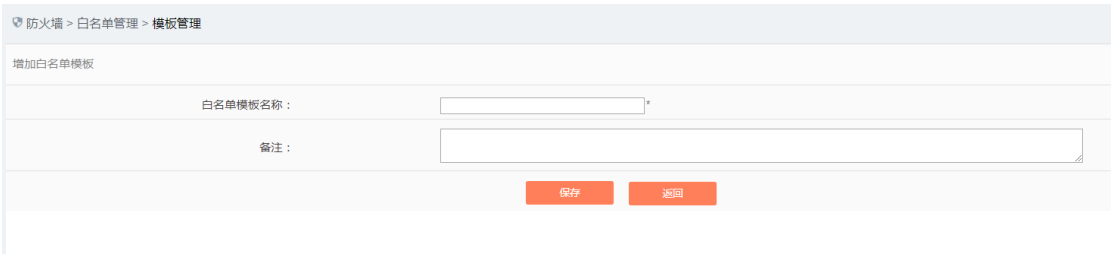


图 3-35 白名单模板添加页

表格 9 白名单模板添加信息说明

列名称	说明
白名单模板名称	给白名单模板定义一个容易理解、记忆且有含义的名字
备注	可选填，附加说明信息

3.4.2.2 信息查看

打开白名单的[模板管理列表]，点击显示列表中操作列下的<查看>按钮，将显示(如图 3-36 所示)的白名单模板的详细信息：

图 3-36 白名单模板信息查看页

点击<返回>按钮，将返回到[白名单模板列表显示]页面。

3.4.2.3 修改白名单模板

打开白名单的[模板管理]，点击显示列表中操作列下的<修改>按钮（如图 3-37 所示），将打开[白名单模板信息修改]页面，可以分别修改白名单模板的基本信息（如图 3-38 所示）

图 3-37 白名单模板修改按钮

图 3-38 白名单模板修改页

表格 10 白名单模板修改信息说明

列名称	说明	
白名单模板名称	给白名单模板定义一个容易理解、记忆且有含义的名字	
备注	可选填，附加说明信息	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到白名单模板信息列表显示页面
	白名单编辑	点击将进入每个工业协议具体的白名单项编辑页面
	返回	忽略所有的修改，返回到白名单模板信息列表显示页面

3.4.2.4 删除白名单模板

点击白名单的[模板管理]信息显示列表中操作列下的<删除>按钮，可以把不再使用的白名单模板进行删除。(如图 3-39 所示)

图 3-39 白名单模板删除按钮

3.4.2.5 检索白名单模板

在白名单的[模板管理]信息显示列表面中，可以根据条件对白名单模板进行检索，(如图 3-40 所示)

图 3-40 检索白名单模板

3.4.3 白名单模板规则管理

白名单模板规则项是指某个白名单模板中具体的某个工业协议的一条条规则，对它的管理是白名单模板管理的核心，所有模板都依赖于具体的每个白名单项。目前工业防火墙支持以下几种标准工业协议的白名单：

OPC Classic 3.0、Siemens S7、Modbus TCP、Ethernet/IP（CIP）、MMS、IEC 104、DNP3、FINS、PROFINET，

工业防火墙计划在不久的将来支持所有通用工业协议的白名单。

进入[白名单模板规则管理]页面的方式有：

第一个路径是：[白名单管理]-[模板管理]-[白名单编辑]列中，点击<编辑>；

第二个路径是：[白名单管理]-[模板管理]-[操作]列中，点击<修改>(如图 3-41 所示)，在打开的[白名单模板修改]页面中，点击<白名单编辑>按钮(如图 3-42 所示)

图 3-41 编辑按钮

图 3-42 白名单编辑按钮

下面将以 OPC 和 Modbus 协议为例，指导如何管理白名单项，其它协议类似，只是具体的字段不同，在这里就不一一赘述了。

3.4.3.1 添加 OPC 白名单项

打开白名单[模板管理]页面后，点击“操作”列下的<编辑>按钮进入具体的规则编辑页面，在此页面点击右侧的<添加>按钮（如图 3-43 所示），将在 OPC 白名单项列表的最下方自动添加一行新的白名单项(如图 3-44 所示)

图 3-43 白名单模板添加按钮

图 3-44 白名单模板添加成功

表格 11 OPC 白名单项字段说明

列名称	说明	
源 IP	发起 OPC 数据请求的 IP 地址，点分十进制格式	
目的 IP	请求 OPC 数据的目的 IP 地址，点分十进制格式	
源 IP 掩码	源 IP 的掩码，一般取值为 0～32	
目的 IP 掩码	目的 IP 的掩码，一般取值为 0～32	
接口名	OPC 协议规范中的某个接口名称，下拉框选取。	
方法名	OPC 协议规范中规定的某个接口下面的某个方法，下拉框选取。	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到白名单模板信息列表显示页面
	返回	忽略所有的修改，返回到白名单模板信息列表显示页面

3.4.3.2 查看 OPC 白名单项

进入[白名单模板规则管理]页面后，默认显示的是 OPC 白名单项，点击不同的 tab 页标签，将显示对应标签的白名单项，(如图 3-45 所示)

图 3-45 OPC 白名单项信息查看页

点击<返回>按钮，将返回到[白名单模板列表显示]页面。

3.4.3.3 修改 OPC 白名单项

进入[白名单模板规则管理]页面后，直接点击某个白名单项下的编辑框，就可以更改某个白名单项的源 IP、目的 IP、源 IP 掩码、目的 IP 掩码、接口名和方法名，修改后点击<保存>按钮即可。

3.4.3.4 修改 OPC 值域

进入[白名单模板规则管理]页面后，直接点击某个白名单项下的编辑框，就可以更改某个白名单项的点别名，源 IP、目的 IP、源 IP 掩码、目的 IP 掩码、接口名和方法名，ItemID,数据类型，最小值，最大值，修改后点击<保存>按钮即可。

3.4.3.5 删除 OPC 白名单项

进入[白名单模板规则管理]页面后，直接点击某个白名单项最右侧的<删除>按钮，可以删除对应的白名单项。(如图 3-46 所示)

图 3-46 白名单模板删除按钮

3.4.3.6 Modbus 协议白名单配置

Modbus 协议的解析深度与其它工业协议不同，工业防火墙可以解析到 Modbus 协议传输的具体的值，所以白名单模板中关于 Modbus 协议的规则配置主要有三部分内容，分别为：协议通配参数、基础白名单和值域控制。

其中协议通配参数主要有如下图中的三个勾选项：

图 3-47Modbus 协议通配参数配置项

- 语法检查

使能此项后，默认情况下，在防护模式时如果报文不符合协议语法，报文将被丢弃并告警。其它工作模式不丢包，但在告警模式下会有相应的告警信息

- Reset

使能此项后，如果有报文被丢弃，工业防火墙会向 Modbus 通信双方发送 Reset 报文，以释放连接资源。

- 连接跟踪检查

使能此项后，默认情况下，在防护模式时如果连接状态不正常，报文将被丢弃并告警。其它工作模式不丢包，但在告警模式下会有相应的告警信息

3.4.3.7 Modbus 基础白名单项

此处配置类似于 OPC 协议，请参考 OPC 协议相关参数配置方法。

3.4.3.8 Modbus 值域控制

使用 Modbus 值域控制功能首先要勾选全局使能选，如图 3-48 所示

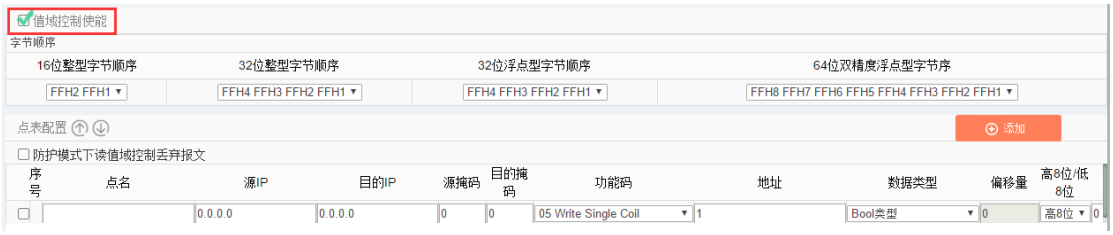


图 3-48 Modbus 值域使能项

使能值域控制功能后，下面的字节顺序就可以编辑了，推荐使用默认配置，如果默认配置与现场不符时，再进行相应的调节。

值域功能最重要的就是“点表配置”，下面把点表配置中的各个字段含义解释在下面表格中

表格 12 Modbus 点击字段说明

列名称	说明
点名	具有含义的代表 Modbus 某个地址的别名
源 IP	发起 OPC 数据请求的 IP 地址，点分十进制格式
目的 IP	请求 OPC 数据的目的 IP 地址，点分十进制格式
源 IP 掩码	源 IP 的掩码，一般取值为 0～32
目的 IP 掩码	目的 IP 的掩码，一般取值为 0～32
功能码	Modbus 协议功能码
地址	Modbus 协议操作的某个点的起始地址
数据类型	点的数据类型
偏移量	某些功能码下操作某种类型的数据在地址中的偏移，如 06 功能码操作的数据类型为 BOOL 型时需要指定地址中哪一位表示此 BOOL 值，默认情况下填 0
高 8 位/低 8 位	某些功能码下操作某种类型的数据在地址中的使用的哪个字节，如 06 功能码(可操作 2 个字节的地址)操作的数据类型为 Byte 型(1 个字节)时需要指定操作的地址中的哪个字节(8 位)，默认情况下为高 8 位
最小值	允许操作的最小值
最大值	允许操作的最大值

值域规则项的添加、修改、编辑、删除请参考 Modbus 基础项操作。

3.4.3.9 白名单规则项学习追加

无论是学习到的还是用户自己手动创建的白名单模板，都可以在学习完成时追加新的学习到的规则。首先把需要再次学习的工业防火墙切换到学习模式，具体操作请参考 3.3.2.2 修改。然后经过适当的学习过程之后，将工业防火墙切换到学习完成，此时在[防火墙信息修改] 页面的工作模式处会提供系统内已有的白名单模板，如图 3-49 所示：

图 3-49 学习完成时选择已有的白名单模板

如果此时选择其中的一个模板，之后点击<保存>按钮，新学习的白名单规则项将自动去重后加入到选择的白名单模板中。此时如果该模板中全部工业协议的规则超过 3000 条，在[模板管理]页面将被标红显示，如图 3-50 所示，并且不能下发给工业防火墙。标红的模板用户需要手工合并到低于 3000 条后才可以下发给工业防火墙使用。

图 3-50 模板中其中一个协议规则数量超过 3000 条

3.5. ACL 管理

3.5.1 功能介绍

工业防火墙作为防火墙类的产品，内置的防火墙管理功能是其基础功能之一，目前工业防火墙采用状态检测防火墙的机制实现相应的安全控制。

简单介绍一下状态检测防火墙。它采用了状态检测包过滤的技术，是传统包过滤上的功能扩展。状态检测防火墙在网络层有一个检查引擎截获数据包并抽取出与应用层状态有关的信息，并以此为依据决定对该连接是接受还是拒绝。这种技术提供了高度安全的解决方案，同时具有较好的适应性和扩展性。状态检测防火墙一般也包括一些代理级的服务，它们提供附加的对特定应用程序数据内容的支持。状态检测技术最适合提供对 UDP 协议的有限支持。它将所有通过防火墙的 UDP 分组均视为一个虚连接，当反向应答分组送达时，就认为一个虚拟连接已经建立。状态检测防火墙克服了包过滤防火墙和应用代理服务器的局限性，不仅仅检测“to”和“from”的地址，而且不要求每个访问的应用都有代理。

3.5.2 安全策略模板管理

点击左侧导航栏的[防火墙管理/安全策略管理](如图 3-51 所示)，进入[安全策略管理]的页面（如图 3-52 所示）。

图 3-51 选择安全策略管理

图 3-52 安全策略管理

此处可以查看到系统内所有安全策略模板的信息，含义如下：

表格 13 安全策略模板列表显示说明

列名称	说明
安全策略模板名称	方便记忆的安全策略模板的名称，如“6#DCS 入站安全策略模板”
版本号	安全策略模板的版本，版本与模板的 ID 唯一确定一组安全策略规则，每次编辑安全策略并保存后，版本号会自动+1
应用此模板的防火墙	正在使用此安全策略模板的所有独立的工业防火墙

安全策略规则维护	编辑	点击后将进入具体的安全策略规则项编辑页面
	导出	点击后，会以 xls 格式，导出当前安全策略规则
	导入	点击后，会将 xls 格式的安全策略规则导入到当前安全策略规则中
操作	查看	查看安全策略模板的更多详细信息
	修改	对安全策略模板的信息进行修改和设置
	删除	删除安全策略模板，无法删除正在使用的安全策略模板

3.5.2.1 添加安全策略模板

打开[防火墙管理/安全策略管理]，在[安全策略模板列表]中找到右侧的<添加>按钮，点击后将弹出安全策略模板添加页面(如图 3-53 所示)

图 3-53 安全策略模板添加页

表格 14 安全策略模板添加信息说明

列名称	说明
安全策略模板名称	给安全策略模板定义一个容易理解、记忆且有含义的名字
备注	可选填，附加说明信息

3.5.2.2 信息查看

点击[防火墙管理/安全策略管理]模板显示列表中操作列下的<查看>按钮，将显示(如图 3-54 所示)的安全策略模板的详细信息：

图 3-54 安全策略模板信息查看页

点击<返回>按钮，将返回到[安全策略管理]页面。

3.5.2.3 修改安全策略模板

点击[安全策略管理]安全策略模板列表中操作列下的<修改>按钮，将打开[安全策略模板信息]修改页面，可以修改安全策略模板的基本信息（如图 3-55 所示）

图 3-55 安全策略模板修改页

表格 15 安全策略模板修改信息说明

列名称	说明	
安全策略模板名称	修改安全策略模板的名字	
备注	可选填，附加说明信息	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到[安全策略管理]页面
	规则编辑	点击将进入具体的安全策略规则项编辑页面
	返回	忽略所有的修改，返回到[安全策略管理]页面

3.5.2.4 删除安全策略模板

点击[安全策略管理]安全策略模板列表操作列下的<删除>按钮，可以把不再使用的安全策略模板进行删除。

注意：如果模板正在被某个工业防火墙或者工业防火墙分组使用，则无法删除。

3.5.2.5 检索安全策略模板

在[安全策略管理]显示列表页面中，可以根据条件对安全策略模板进行检索。(如图 3-56 所示)

图 3-56 检索安全策略模板

3.5.3 安全策略模板规则项管理

安全策略规则项的管理是安全策略管理的核心，所有模板都依赖于具体的每个安全策略规则项。

进入[安全策略规则项管理]页面的入口一个是点击[安全策略管理]显示列表中安全策略规则维护列下的<编辑>按钮，另外一个是进入[安全策略模板信息] 修改页面后，点击<规则编辑>按钮(如图 3-57 所示)

图 3-57 安全策略规则编辑按钮

3.5.3.1 添加安全策略规则

进入[策略模板规则信息]页面后，点击右侧的<添加>按钮（如图 3-58 所示），将在安全策略规则列表的最下方自动添加一行新的规则 (如图 3-59 所示)

图 3-58 安全策略规则添加按钮

图 3-59 新的安全策略规则

表格 16 安全策略规则字段说明

列名称	说明
源安全域	发起数据请求的安全区域，以“any”表示全匹配
目的安全域	数据请求的目的安全区域，以“any”表示全匹配
源 MAC	发起数据请求的 MAC 地址，以“00:00:00:00:00:00”格式
目的 MAC	请求数据的目的 MAC 地址，以“00:00:00:00:00:00”格式
源 IP	发起数据请求的 IP 地址，点分十进制格式
目的 IP	请求数据的目的 IP 地址，点分十进制格式
源 IP 掩码	源 IP 的掩码，一般取值为 0～32
目的 IP 掩码	目的 IP 的掩码，一般取值为 0～32
开始时间	规则生效的起始时间点
结束时间	规则失效的最后时间点
执行动作	命中该规则时防火墙对包的处理，通过、阻断或通过并记录日志
服务	规则所支持的服务类型

操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到安全策略管理模板列表显示页面
	返回	忽略所有的修改，返回到安全策略管理模板信息列表显示页面

3.5.3.2 查看安全策略规则项

进入[策略模板规则信息]页面后，即可查看到当前策略模板下的具体安全策略规则项。(如图 3-60 所示)

图 3-60 安全策略规则项信息查看页

如果模板是新模板，则查看时规则项为空，需要按下面章节完成相应的添加操作即可看到规则。点击<返回>按钮，将返回到[安全策略管理]模板列表显示页面。

3.5.3.3 修改安全策略规则

进入[策略模板规则信息]页面后，直接点击某个安全策略规则下的编辑框，就可以更改某个安全策略规则的源安全域、目的安全域、源 MAC、目的 MAC、源 IP、目的 IP，源 IP 掩码，目的 IP 掩码，开始时间，结束时间，执行动作和服务，修改后点击<保存>按钮即可。

3.5.3.4 删除安全策略规则

进入[策略模板规则信息]页面后，直接点击某个安全策略规则最右侧的<删除>按钮，可以删除对应的安全策略规则。(如图 3-61 所示)

图 3-61 安全策略规则删除按钮

删除后点击<保存>按钮即可。

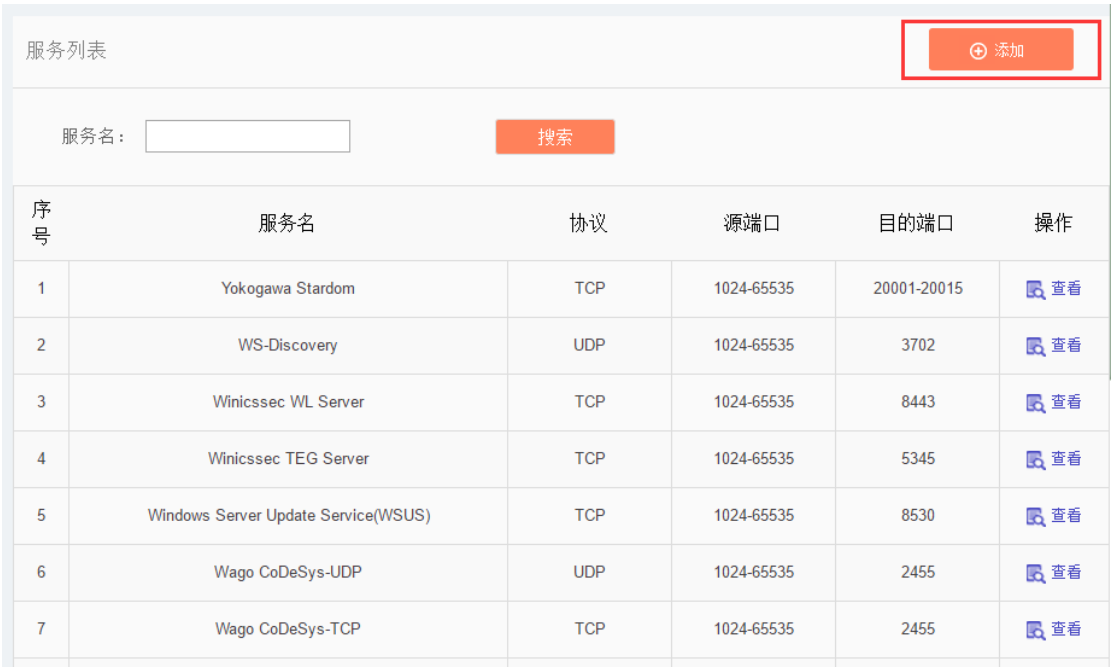
3.5.4 自定义服务

除了可以使用管理平台预先定义好的服务外，用户还可以自己定义网络中其它服务器提供的服务。点击左侧导航栏的[防火墙管理/自定义服务](如图 3-62 所示)，打开[自定义服务]的页面。

图 3-62 选择自定义服务

3.5.4.1 添加自定义服务

进入[自定义服务]页面后，点击右侧的<添加>按钮（如图 3-63 所示），将弹出自定义服务添加页面(如图 3-64 所示)



序号	服务名	协议	源端口	目的端口	操作
1	Yokogawa Stardom	TCP	1024-65535	20001-20015	查看
2	WS-Discovery	UDP	1024-65535	3702	查看
3	Winicssec WL Server	TCP	1024-65535	8443	查看
4	Winicssec TEG Server	TCP	1024-65535	5345	查看
5	Windows Server Update Service(WSUS)	TCP	1024-65535	8530	查看
6	Wago CoDeSys-UDP	UDP	1024-65535	2455	查看
7	Wago CoDeSys-TCP	TCP	1024-65535	2455	查看

图 3-63 自定义服务添加按钮

图 3-64 自定义服务添加页面

表格 17 自定义服务添加字段说明

列名称	说明	
服务名	自定义的服务名称，不能与现有的冲突	
协议	下拉选择该服务所依赖的传输层协议	
源起始端口	服务所使用的源起始端口，从 1 到 65535，没有则输入 1	
源结束端口	服务所使用的源结束端口，从 1 到 65535，没有则输入 65535	
目的起始端口	服务所使用的目的起始端口，从 1 到 65535	
目的结束端口	服务所使用的目的结束端口，从 1 到 65535，只有一个端口则与目的起始端口相同	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到自定义服务列表显示页面
	返回	忽略所有的修改，返回到自定义服务列表显示页面

3.5.4.2 查看自定义服务

进入[自定义服务]页面后，即可查看到当前系统内置和已经自定义过的服务。(如图 3-65 所示)

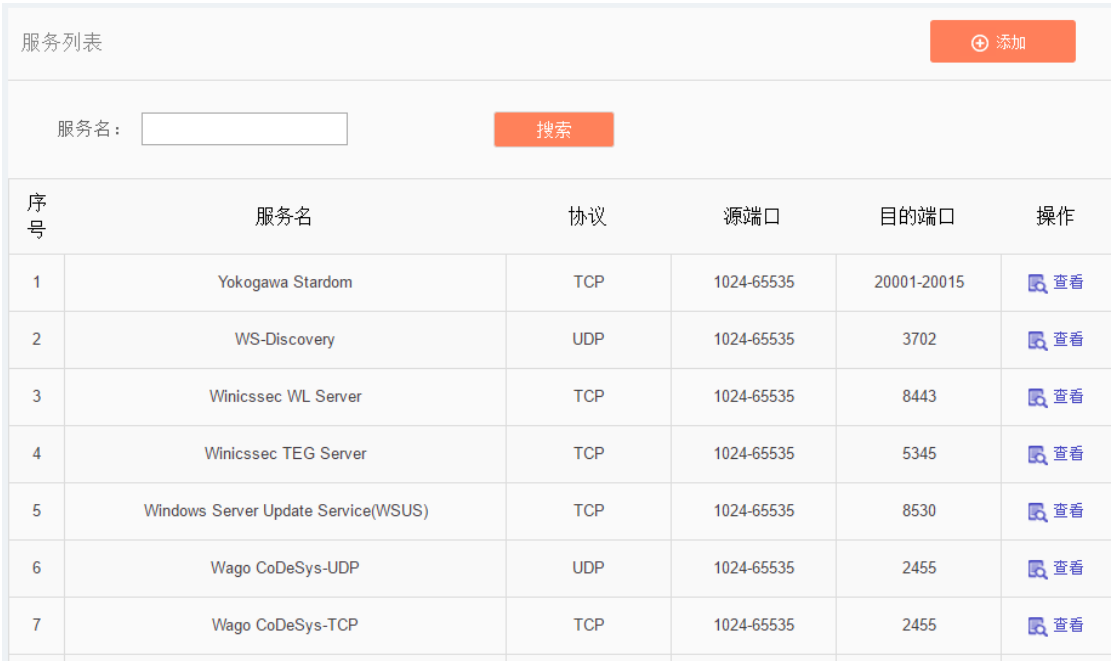


图 3-65 自定义服务信息查看页

3.5.4.3 修改自定义服务

进入[自定义服务]页面后，点击操作列下的<修改>按钮，即可以修改自定义服务，修改页面(如图 3-66 所示)

图 3-66 自定义服务修改页面

每个字段的含义请参考 3.5.4.1 添加自定义服务。

3.5.4.4 删除自定义服务

进入[自定义服务]页面后，直接点击某个自定义服务最右侧的<删除>按钮，可以删除对应的自定义服务。(如图 3-67 所示)

图 3-67 自定义服务删除按钮

注：无法删除正在被某个安全策略使用的自定义服务

3.5.5 自定义白名单应用

在某些特定的工业现场，运行在应用层的协议可能与协议默认运行的端口发生了变化，这个时候如果只是简单的在防火墙安全策略规则中放开协议默认端口或者使用传统的 DPI 技术可能并不能精确识别出来工业协议，所以安通恩创工业防火墙增加一个用户可以自定义白名单应用的功能，以解决上面的问题。

点击左侧导航栏的[防火墙管理/自定义白名单应用](如图 3-68 所示)，打开[自定义白名单应用]的页面(如图 3-69 所示)。

图 3-68 选择自定义白名单应用

图 3-69 选择自定义白名单应用

3.5.5.1. 添加自定义白名单应用

进入[自定义白名单应用]页面后，点击右侧的<添加>按钮（如图 3-70 所示），将弹出自定义白名单应用添加页面(如图 3-71 所示)

图 3-70 自定义白名单应用添加按钮

图 3-71 自定义白名单应用添加页面

表格 18 自定义白名单应用添加字段说明

列名称	说明	
应用名称	自定义的白名单应用的名称，不能与现有的冲突	
应用协议名	下拉选择要自定义应用层的工业协议	
传输层协议	下拉选择该服务所依赖的传输层协议	
目的 IP	提供工业协议服务端的设备 IP 地址	
目的端口	替换此工业协议默认端口的新的端口	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到自定义白名单应用列表显示页面
	返回	忽略所有的修改，返回到自定义白名单应用列表显示页面

3.5.5.2. 查看自定义白名单应用

进入[自定义白名单应用]页面后，即可查看到当前已经自定义过的白名单应用。(如图 3-72 所示)

图 3-72 自定义白名单应用信息查看页

3.5.5.3. 修改自定义白名单应用

进入[自定义白名单应用]页面后，点击操作列下的<修改>按钮，即可以修改自定义白名单应用，修改页面(如图 3-73 所示)

图 3-73 自定义白名单应用修改页面

每个字段的含义请参考 3.5.5.1 添加自定义白名单应用。

3.5.5.4. 删除自定义白名单应用

进入[自定义白名单应用]页面后，直接点击某个自定义白名单应用最右侧的<删除>按钮，可以删除对应的自定义白名单应用。(如图 3-74 所示)

序号	应用名称	应用层协议	传输层协议	目的IP	目的端口	操作
1	自定义CIP	CIP	TCP	192.168.3.56	44819	修改 删除
2	自定义Modbus	MODBUS	TCP	192.168.61.85	503	修改 删除
3	自定义S7	S7	TCP	192.168.67.3	103	修改 删除

图 3-74 自定义白名单应用删除按钮

注：无法删除正在被某个安全策略使用的自定义白名单应用

3.6. 安全域管理

3.6.1. 功能介绍

传统基于接口的策略配置方式需要为每一个接口配置安全策略，给网络管理员带来了极大的负担，安全策略的维护工作量成倍增加，从而也增加了因为配置引入安全风险的概率。和传统防火墙基于接口的策略配置方式不同，业界主流防火墙通过围绕安全域（Security Zone）来配置安全策略的方式解决上述问题。

所谓安全域，是一个抽象的概念，它有两种划分方式：

➢ 按照接口划分。

安全域可以包含三层普通物理接口和逻辑接口，也可以包括二层物理 Trunk 接口+VLAN，划分到同一个安全域中的接口通常在安全策略控制中具有一致的安全需求。

➢ 按照IP 地址划分。

根据 IP 地址划分不同的安全域，以实现按业务报文的源 IP 地址或目的 IP 地址进行安全策略控制。

引入安全域的概念之后，安全管理员将安全需求相同的接口或 IP 地址进行分类（划分到不同的域），能够实现策略的分层管理。通过引入安全域的概念，不但简化了策略的维护复杂度，同时也实现了网络业务和安全业务的分离。

管理平台采用接口划分的方式，实现安全域的管理。

3.6.2. 添加安全域

点击 [安全域管理]安全域列表标签右侧的<添加>按钮(如图 3-75 所示)，将弹出安全域添加页面。(如图 3-75 所示)

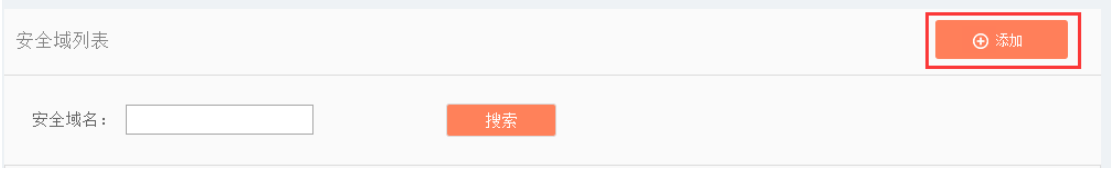


图 3-75 安全域添加按钮

图 3-76 安全域添加页

表格 19 安全域添加信息说明

列名称	说明
安全域名	便于记忆的安全域的名称
优先级	设置安全域的优先级，缺省情况下，允许从高优先级安全域到低优先级安全域方向的报文通过

3.6.3. 查看安全域

点击左侧导航栏的[安全域管理/安全域管理]，进入[安全域管理]的页面（如图 3-77 所示）。

图 3-77 安全域管理页

安全域有两种基本类型，一种是由**系统内置**的安全域，一种是**用户自己创建**的安全域。前者只允许修改优先级，包含的防火墙这两种属性；后者除 ID 外，可以修改其它所有属性。此处可以查看到系统内所有安全域的信息，含义如下：

表格 20 安全域列表显示说明

列名称	说明	
安全域 ID	安全域的唯一标识号，由系统自动分配	
安全域名	便于记忆的安全域的名称	
优先级	设置安全域的优先级	
包含的接口	安全域包含的所有工业防火墙接口	
操作	修改	对安全域的信息进行修改和设置
	删除	删除安全域

点击[安全域管理]显示列表中操作列下的<查看>按钮，将显示安全域的详细信息。
点击<返回>按钮，将返回到[安全域管理]页面。

3.6.4. 修改安全域

点击[安全域管理]安全域列表中操作列下的<修改>按钮，将打开[安全域基本信息]修改页面（如图 3-78 所示），可以修改安全域的基本信息。

图 3-78 修改安全域的信息

这里最主要的是修改安全域所对应的接口。点击[安全域修改]页上的<选择>按钮，将弹出安全域包含接口的选择页面，如图 3-79 所示。

图 3-79 选择安全域包含的防火墙接口

安全域包含了哪个工业防火墙的哪个接口，此接口所连接的网络就属于此安全域。

例如：如果安全域 Trusted 包含了“生产大区 1 工业防火墙”的接口 ETH1，而某个安全策略包含了一条从 Trusted 到 any 安全域的通过策略，则意味着从 ETH1 发起的会话都会通过。

3.6.5. 删除安全域

点击[安全域管理]安全域列表操作列下的<删除>按钮，可以把不再使用的安全域进行删除。

注意：无法删除系统内置的安全域，正在被安全策略规则使用的安全域也无法删除。

3.6.6. 检索安全域

在[安全域管理]安全域显示列表页面中，可以根据条件对安全域进行检索。(如图 3-80 所示)

图 3-80 检索安全域

3.7. 日志管理

3.7.1. 功能介绍

日志管理能够将系统发生的事件或包过滤的动作产生的日志等存入缓冲区或定向发送到日志接收服务器上。通过对日志内容的分析和归档，管理员能够检查工业防火墙发现的网络中的安全漏洞，了解什么时候有什么人试图违背安全策略规则、白名单模板规则违规访问网络。此外，实时的日志记录还可以用来检测正在进行的入侵，并且进行阻止。

🕮 **注意：**

只有审计管理员才有权限进行日志管理

3.7.2. 白名单告警日志

白名单告警日志是流经工业防火墙的报文违反了工业防火墙上的白名单规则产生的，只有工业防火墙处于告警模式或防护模式时才有可能产生此日志。

3.7.2.1. 日志列表

点击左侧导航栏的[日志管理/白名单告警日志](如图 3-81 所示)，进入[白名单告警日志]的列表页面（如图 3-82 所示）。

图 3-81 白名单告警日志菜单

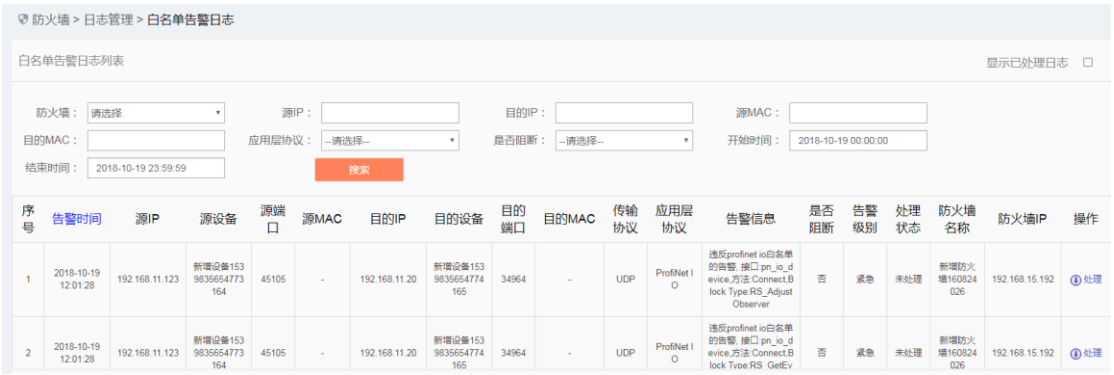


图 3-82 白名单告警日志列表页

此处可以查看到白名单告警所有日志的信息，含义如下：

表格 21 白名单告警日志显示说明

列名称	说明
防火墙名称	由系统生成或用户命名的便于记忆的防火墙的名字
防火墙 IP	工业防火墙分配到的 IP 地址，点分十进制格式
源 IP	发起数据请求的 IP 地址，点分十进制格式
源设备	无设备名称时显示为“-”，否则显示源设备的名称
源端口	发起数据请求的机器所使用的端口
目的 IP	请求数据的目的 IP 地址，点分十进制格式
目的设备	无设备名称时显示为“-”，否则显示目的设备的名称
目的端口	请求的目标机器所使用的端口
传输层协议	报文使用的传输层的协议类型

应用层协议	具体的应用类型	
告警信息	告警的描述信息	
是否阻断	对报文的处理动作是放行还是阻断	
告警级别	告警可能造成的损害级别，级别说明请参考 5.6.2 告警级别说明	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。
勾选[白名单告警日志]白名单告警日志列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。(如图 3-83 所示)

图 3-83 显示已处理的白名单告警日志列表页

3.7.2.2. 处理日志

点击[白名单告警日志]显示列表中操作列下的<处理>按钮，将显示如下图所示[白名单告警日志信息]的处理页面。(如图 3-84 所示)

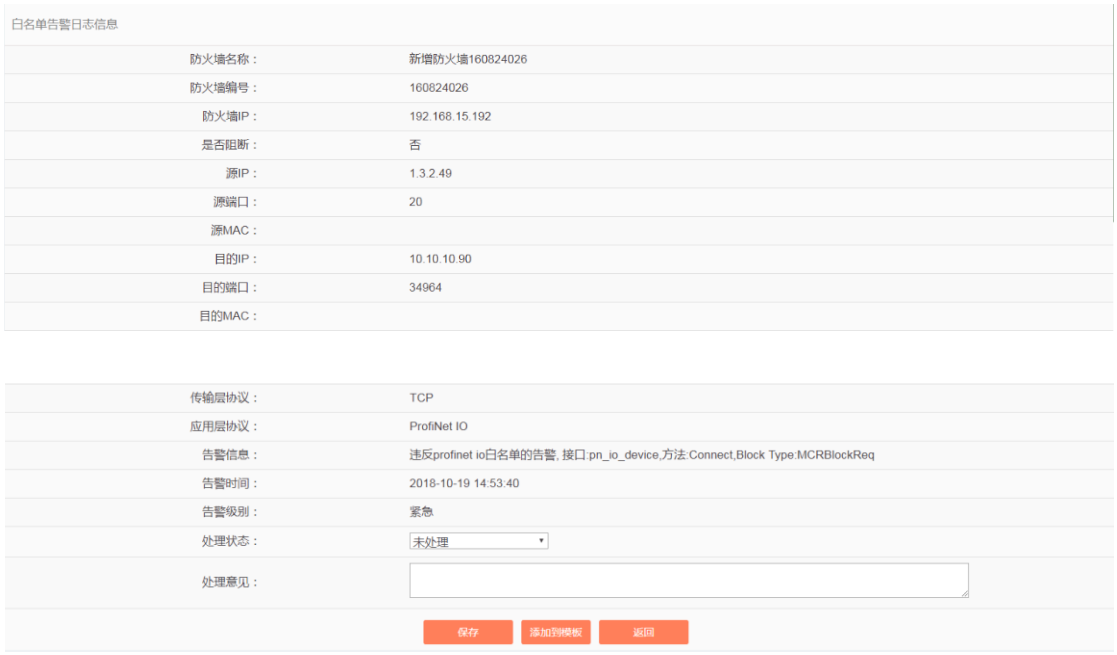


图 3-84 白名单告警处理页

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[白名单告警日志]页的列表中默认将不再看到此条日志。

也可以不选择“关闭”，只填写处理意见。

3.7.2.3. 清空日志

管理平台支持对日志的批量删除功能。

用户可以批量删除无用的日志。在[白名单告警日志]的列表页面中，点击下方的<清空>按钮，即可完成对应日志的批量删除。(如图 3-85 所示)

图 3-85 白名单告警的清空

3.7.2.4. 检索日志

在[白名单告警日志]的列表页面中，可以根据条件对日志进行检索。(如图 3-86 所示)

图 3-86 检索白名单告警日志

3.7.3. 防火墙告警日志

防火墙告警日志是流经工业防火墙的报文违反了工业防火墙上的安全策略规则产生的，无论工业防火墙处于哪种工作模式下，只要报文违反了安全策略规则，都将产生此类型的告警。

3.7.3.1. 日志列表

点击左侧导航栏的[日志管理/防火墙告警日志](如图 3-87 所示)，进入[防火墙告警日志]的列表页面（如图 3-88 所示）。

图 3-87 防火墙告警日志菜单

图 3-88 防火墙告警日志列表页

此处可以查看到防火墙告警所有日志的信息，含义如下：

表格 22 防火墙告警日志显示说明

列名称	说明
防火墙名称	由系统生成或用户命名的便于记忆的工业防火墙的名字
防火墙 IP	工业防火墙分配到的 IP 地址，点分十进制格式
源 IP	发起数据请求的 IP 地址，点分十进制格式
目的 IP	请求数据的目的 IP 地址，点分十进制格式

目的设备	无设备名称时显示为“-”，否则显示目的设备的名称	
目的端口	请求的目标机器所使用的端口	
传输层协议	报文使用的传输层的协议类型	
应用层协议	具体的应用类型	
告警信息	告警的描述信息	
是否阻断	对报文的处理动作是放行还是阻断	
告警级别	告警可能造成的损害级别	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。
勾选[防火墙告警日志]防火墙告警日志列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。(如图 3-89 所示)

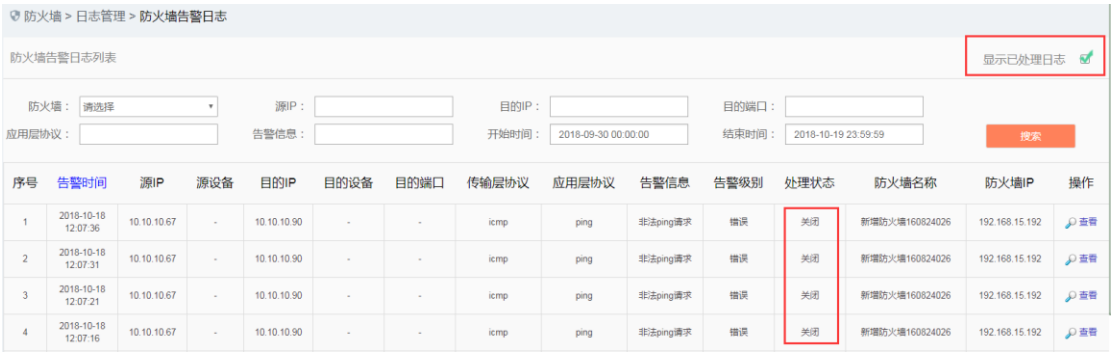


图 3-89 显示已处理的防火墙告警日志列表页

3.7.3.2. 处理日志

点击[防火墙告警日志]显示列表中操作列下的<处理>按钮，将显示如下图所示[防火墙告警日志信息]的处理页面。(如图 3-90 所示)

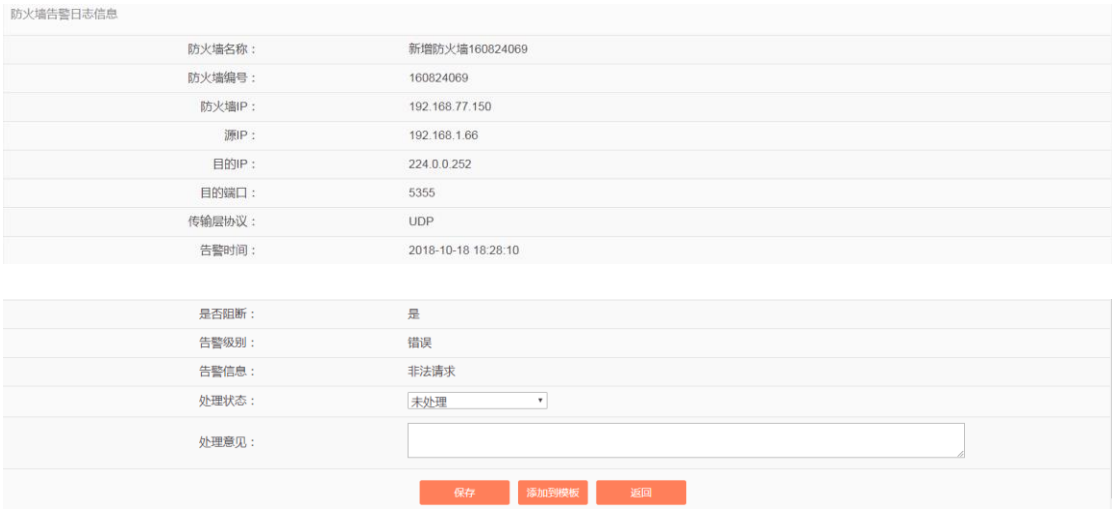


图 3-90 防火墙告警处理页

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[防火墙告警日志]页的列表中默认将不再看到此条日志。也可以不选择“关闭”，只填写处理意见。

3.7.3.3. 清空日志

管理平台支持对日志的批量删除功能。

用户可以选择清空日志。在[防火墙告警日志]的列表页面中，点击下方的<清空>按钮，即可完成对应日志的清空。(如图 3-91 所示)

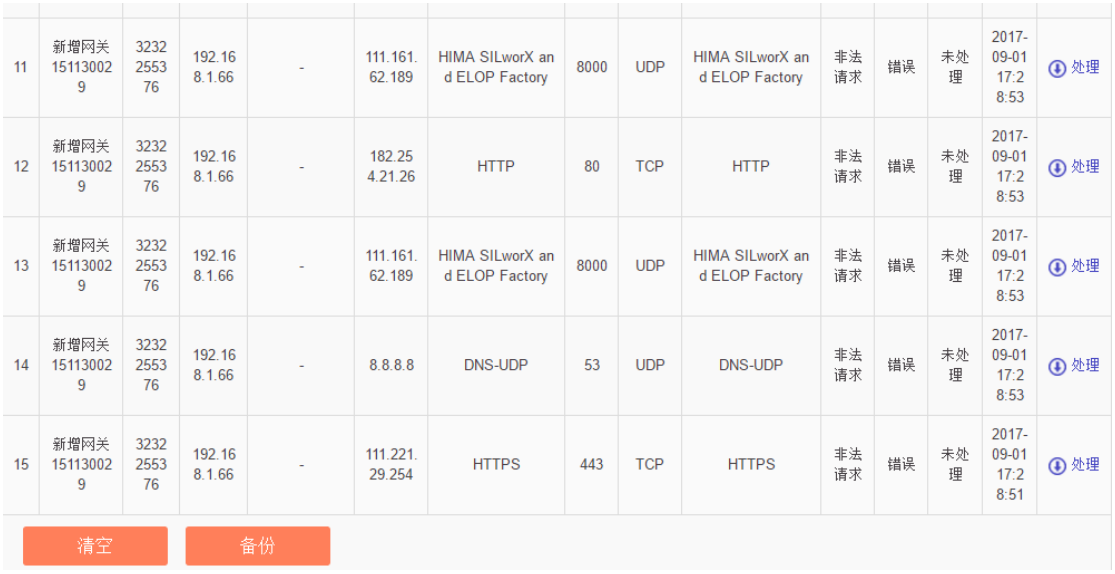


图 3-91 防火墙告警的清空

3.7.3.4. 检索日志

在[防火墙告警日志]的列表页面中，可以根据条件对日志进行检索。(如图 3-92 所示)

图 3-92 检索防火墙告警日志

3.7.4. 防火墙运行日志

防火墙运行日志是记录工业防火墙运行状态的日志。

3.7.4.1. 日志列表

点击左侧导航栏的[日志管理/防火墙运行日志](如图 3-93 所示)，进入[防火墙运行日志]的列表页面（如图 3-94 所示）。

图 3-93 防火墙运行日志菜单

图 3-94 防火墙运行日志列表页

此处可以查看到所有工业防火墙运行日志的信息，含义如下：

表格 23 防火墙运行日志显示说明

列名称	说明
防火墙名称	由系统生成或用户命名的便于记忆的工业防火墙的名字

防火墙 IP	工业防火墙分配到的 IP 地址，点分十进制格式
内容	产生日志后工业防火墙的后续运行状态
操作时间	日志产生时的时间

3.7.4.2. 清空日志

管理平台支持对日志的批量删除功能。

用户可以选择清空日志。在[防火墙运行日志]的列表页面中，点击下方的<清空>按钮，即可完成对应日志的清空。(如图 3-95 所示)

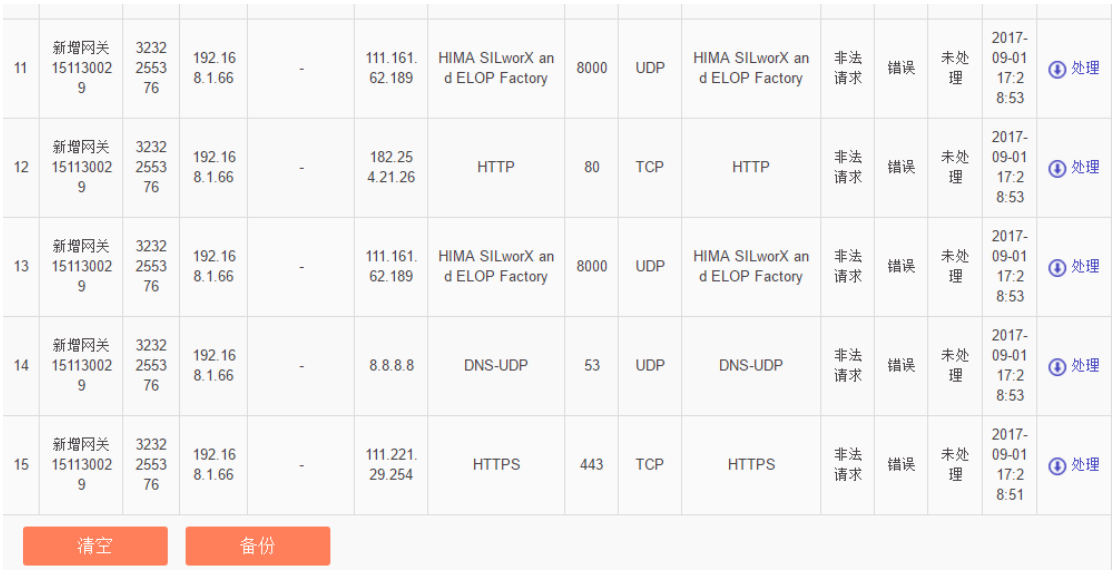


图 3-95 防火墙运行日志的清空

3.7.4.3. 检索日志

在[防火墙运行日志]的列表页面中，可以根据条件对日志进行检索。(如图 3-96 所示)

图 3-96 检索防火墙运行日志

3.7.5. 状态监测日志

相关操作可以参考 3.7.4 防火墙运行日志的介绍

3.7.6. 地址欺骗日志

地址欺骗日志是流经工业防火墙的报文违反了工业防火墙上的 IP/MAC 规则产生的，只有工业防火

墙处于告警模式或防护模式时才有可能产生此日志。

3.7.6.1. 日志列表

点击左侧导航栏的[日志管理/地址欺骗日志](如图 3-97 所示)，进入[地址欺骗日志]的列表页面（如图 3-98 所示）。

图 3-97 白名单告警日志菜单

图 3-98 地址欺骗日志列表页

此处可以查看到地址欺骗所有日志的信息，含义如下：

表格 24 地址欺骗日志显示说明

列名称	说明
防火墙名称	由系统生成或用户命名的便于记忆的工业防火墙的名字
防火墙 IP	工业防火墙分配到的 IP 地址，点分十进制格式
告警信息	告警的描述信息

是否阻断	对报文的处理动作是放行还是阻断	
告警级别	告警可能造成的损害级别	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。
勾选[地址欺骗日志]地址欺骗日志列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。(如图 3-99 所示)

图 3-99 显示已处理的地址欺骗日志列表页

3.7.6.2. 处理日志

请参考其它日志处理方式。

3.7.6.3. 清空日志

请参考其它日志处理方式。

3.7.6.4. 检索日志

请参考其它日志处理方式。

3.7.7. 日志统计

日志统计分为两种模式，一种为统计全部工业防火墙设备四种告警日志数量，另一种为单独一台工业防火墙设备四种告警日志数量。

3.7.7.1. 显示

点击左侧导航栏的[日志管理/日志统计](如图 3-100 所示)，进入[日志统计]的列表页面（如图 3-101 所示）。

图 3-100 日志统计菜单

图 3-101 日志统计页面

3.7.7.2. 检索统计

在[日志统计]的页面中，可以根据条件对统计数据进行检索。(如图 3-102 所示)

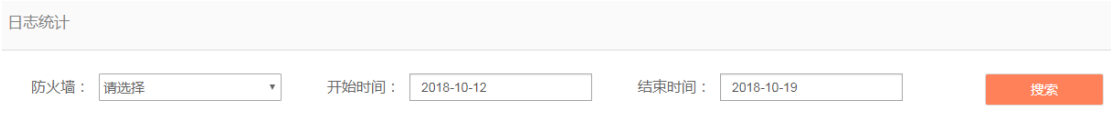


图 3-102 检索日志统计数据

4. 工控主机卫士

4.1 产品介绍

工控主机卫士模块是用来管理，监控工控主机卫士的管理模块，工控主机卫士是本公司针对传统防病毒软件的不足，结合工业控制系统工作站安全防护的特点，基于恩创自有知识产权的“软可信”技术，设计研发的一款主机安全软件产品。

本主机安全软件创新性的将应用程序白名单管理技术引入工控网络安全防护。只有在白名单列表中的应用程序是被允许在系统中运行，白名单列表之外的任何程序都不被允许运行。

本软件可通过统一安全管理平台进行多台工控主机的管理和配置工作，工控主机在运行中产生的各种报警信息和日志会汇总到管理平台，进行数据采集和分析。

4.2 系统权限

统一管理管理平台的系统操作员、系统审核员、管理员和审计员（分别为 sysoperator、sysaudit、admin 和 audit），对于工控主机卫士模块来说，在安装工控主机卫士客户端时会同步和使用管理员和审计员，其使用权限如下：

- 管理员：拥有所有配置管理权限。
- 审计员：拥有日志审计相关的权限

4.3 实时报警

当用户成功登录统一管理管理平台后，点选“主机卫士”标签进入。上部分主要显示系统信息，左侧为系统模块的菜单列表，右侧为当日实时及最近报警信息界面，(如图 4-1 所示)。

图 4-1 实时报警页面

实时报警界面是管理平台成功登录后的默认显示界面，主要包括当日 TOP10 报警程序统计、当日 TOP 10 报警客户端统计、报警数量趋势、当日报警总、终端概况和最近报警 6 部分。

- 当日 TOP 10 程序报警统计：以饼状图的形式显示当天所有程序报警按程序路径分类统计，报警次数最多的前 10 项纪录。当不足 10 项时，仅显示已有的记录。
- 当日 TOP 10 程序报警客户端统计：以柱状图的形式显示当天所有程序报警按 IP 分类统计，报

警次数最多的前 10 项纪录。当不足 10 项时，仅显示已有的记录。

- 报警数量趋势：以折线图的形式显示程序报警和外设报警近 7 天的报警数量趋势，两者间可以相互切换，默认显示程序报警数量趋势。
- 当日报警数：以列表的形式显示当天程序报警和外设报警次数，点击次数，可跳转至程序报警或外设报警界面。
- 终端概况：以列表的形式显示已部署和在线的客户端数量，以及在线率。点击已部署（或在线）的客户端数量值，可跳转至客户端监测界面。
- 最近报警（最多显示 25 条记录）：以列表的形式显示程序报警和外设报警的最近的 25 条报警记录，两者间可以相互切换，默认显示程序报警。

4.4 日志管理

4.4.1 日志分类

通过日志管理模块，审计管理员可以查询和导出程序报警、外设报警、防火墙报警日志、操作系统日志、访问控制告警、非法外联告警。

- 程序报警：客户端向管理平台上报生成的程序报警日志，程序报警界面列表中默认显示当天的所有程序报警。管理员可通过设置条件查询相关日志。界面(如图 4-2 所示)。
- 外设报警：客户端向管理平台上报生成的外设报警日志，外设报警界面列表中默认显示当天的所有外设报警。管理员可通过设置条件查询相关日志。界面(如图 4-3 所示)。
- 防火墙报警日志：客户端向管理平台上报生成的防火墙报警日志，防火墙报警日志界面列表中默认显示当天的所有主机防火墙报警。管理员可通过设置条件查询相关日志。界面(如图 4-4 所示)。
- 操作系统日志：客户端向管理平台上报生成的操作系统日志，操作系统日志界面列表中默认显示当天的所有操作系统日志。管理员可通过设置条件查询相关日志。界面(如图 4-5 所示)。
- 访问控制告警：客户端向管理平台上报生成的主机加固报警日志，访问控制告警界面列表中默认显示当天的所有访问控制告警。管理员可通过设置条件查询相关日志。界面(如图 4-6 所示)。
- 非法外联告警：客户端向管理平台上报生成的非法外联报警日志，非法外联告警界面列表中默认显示当天的所有非法外联告警。管理员可通过设置条件查询相关日志。界面(如图 4-7 所示)。

图 4-2 程序报警

图 4-3 外设报警

图 4-4 防火墙报警日志

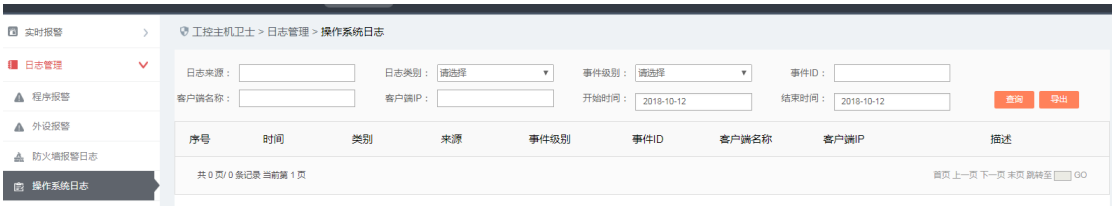


图 4-5 操作系统日志

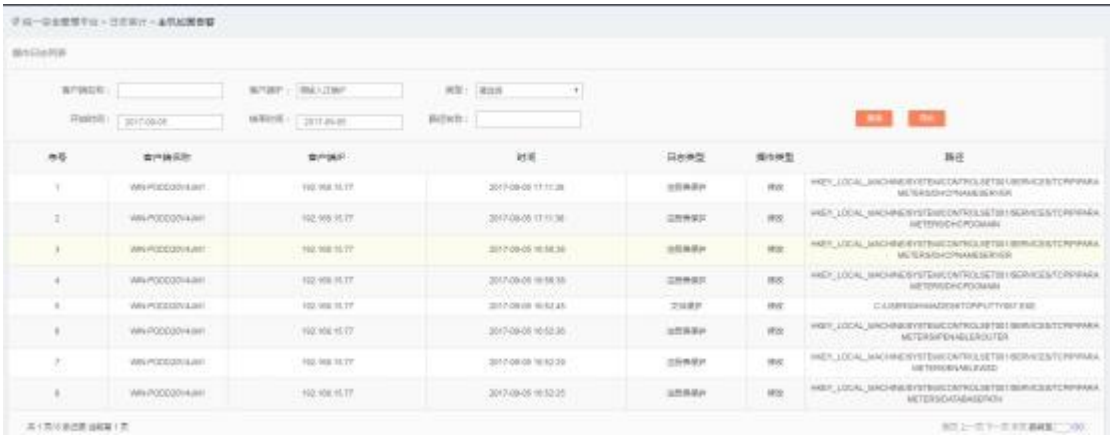


图 4-6 访问控制告警

图 4-7 非法外联告警

4.4.2 日志查询与导出

上述程序报警、外设报警、防火墙报警日志、操作系统日志、访问控制告警、非法外联告警均提供查询、导出功能。

- 查询功能：输入合法的查询条件关键字，点击“查询”按钮查询相关日志。
- 导出功能：单击“导出”按钮，管理员可以根据查询条件将结果导出到 EXCEL 文件。

4.5 主机卫士管理

通过主机卫士管理模块，管理员可以进行客户端状态监测、分组管理、管理客户端分组、卸载或者强制卸载客户端。

4.5.1. 客户端监测

客户端监测：根据分组树[客户端列表]所列查询关键字查询客户端的状态，且客户端的各项状态 10 秒钟刷新一次。管理员可点击<设置别名>为客户端设置别名，及点击<刷新>手动刷新客户端状态。界面默认分页显示所有客户端的当前状态，还可以根据查询条件过滤显示客户端的策略概况信息，操作功能提供“更多”、“查看开机系统加载文件”、“设置别名”和“刷新”功能。(如图 4-8 所示)。

图 4-8 客户端监测

4.5.2. 分组管理

添加、删除、修改系统组织。界面(如图 4-9 所示)，红色框内为新添加的组织结构。当通过组织管理界面添加组织后，管理员可将客户端划分到不同的组织内。

图 4-9 分组管理

4.5.3. 客户端分组

客户端分组：提供查询组织节点中的客户端、向管理员在组织管理界面中创建的基层组织节点中添加客户端、从组织节点中删除或批量删除已添加的客户端功能。界面(如图 4-10 所示)。

图 4-10 客户端分组

4.5.4. 客户端卸载

客户端卸载：提供卸载、强制卸载客户端和实时显示指令动作日志功能。执行强制卸载客户端，管理平台将立刻不再监测该客户端；执行卸载客户端，当客户端返回卸载成功消息后，管理平台将不再监测该客户端。可根据查询关键字精确快速查找指定客户端。界面默认显示当天最新的指令动作日志。可点击<删除>按钮，一键删除全部指令动作日志。界面(如图 4-11 所示)。

图 4-11 客户端卸载

4.6 程序白名单

通过程序白名单模块，管理员可以控制客户端程序白名单相关的各项功能的开启或关闭，程序白名单相关的功能包括：扫描例外模板、进程审计模板、系统完整性检查、白名单管理、程序控制、报警处理、进程审计。可以通过创建的模板快速完成操作。可依据关键字查询快速准确查找指定客户端。界面默认显示当天最新的指令动作日志。可点击<清空消息日志>按钮，一键删除全部指令动作日志。

4.6.1. 策略模板

通过扫描例外模板、进程审计模板功能，包括添加，删除，修改等操作，管理员可以控制客户端各项功能的开启或关闭，可创建的模板包括：扫描例外模板，进程审计模板。

4.6.1.1 扫描例外模板

扫描例外模板：添加、删除、修改、查询扫描例外模板。添加扫描例外模板后，可以点击<规则配

置>，添加不被扫描的例外路径。

模板操作界面，目前仅支持 windows 客户端，(如图 4-12 所示)：

图 4-12 扫描例外模板

模板配置界面，(如图 4-13 所示)：：

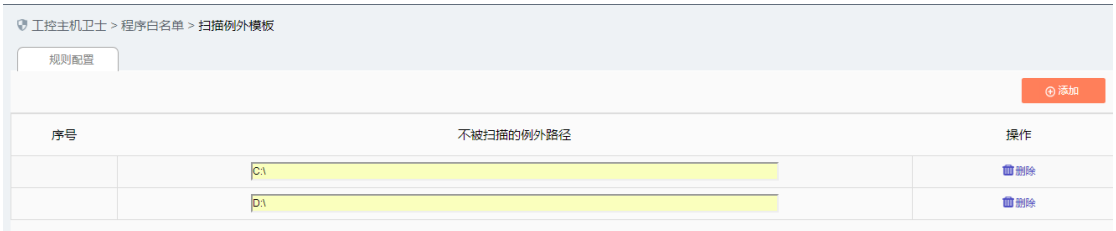


图 4-13 模板配置界面

4.6.1.2 进程审计模板

进程审计模板：添加、删除、修改、查询进程审计模板。添加进程审计模板后，可以点击<规则配置>，添加需要被审计的进程名字。

模板操作界面，包括 windows 和 linux 模板，(如图 4-14 所示)：

图 4-14 进程审计模板

模板配置界面，(如图 4-15 所示)：

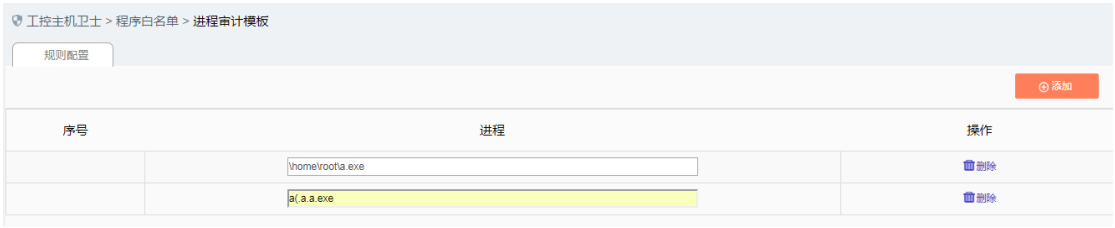


图 4-15 模板配置界面

4.6.2. 系统完整性检查

可以对客户端下发系统完整性检查“开启”和“关闭”指令。客户端执行成功后，界面自动刷新，界面

(如图 4-16 所示)：

图 4-16 系统完整性检查界面

4.6.3. 白名单管理

白名单管理包括设置扫描例外路径，通过设置扫描例外路径，可以在生成白名单时，指定不扫描的路径。设置扫描例外路径需要用到扫描例外模板，扫描例外模板在[扫描例外模板]中配置。用户通过添加扫描例外模板可以给指定的客户端下发扫描例外路径。界面(如图 4-17 所示)。

图 4-17 不扫描路径界面

白名单例外路径配置完成之后，可以通过白名单管理页面向指定的主机卫士下发扫描指令并且可以查看扫描状态，完成后可以查看白名单列表和数量，并且支持导出白名单列表为 csv 的功能。界面(如图 4-18 所示)。

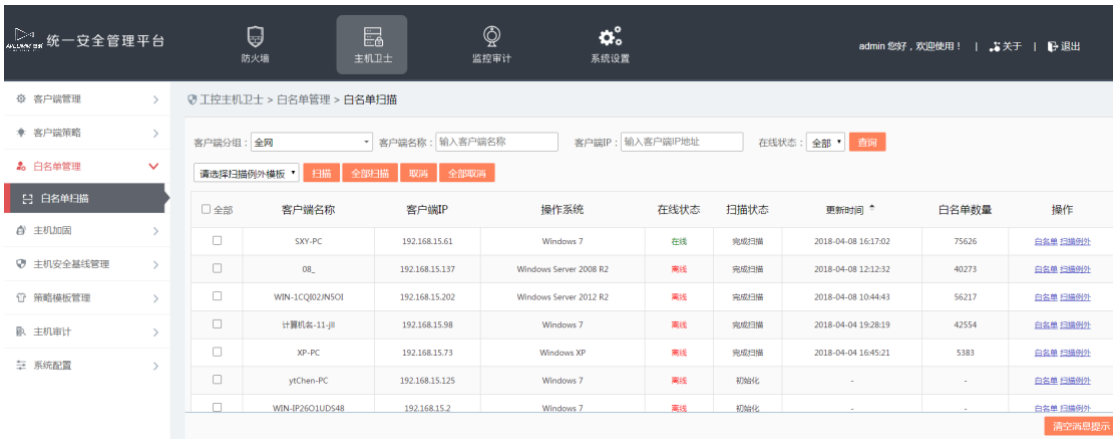


图 4-18 白名单管理界面

查看白名单界面，(如图 4-19 所示)：

图 4-19 查看白名单界面

4.6.4. 程序控制

开启或关闭客户端程序控制。客户端执行成功后，界面自动刷新，(如图 4-20 所示)：

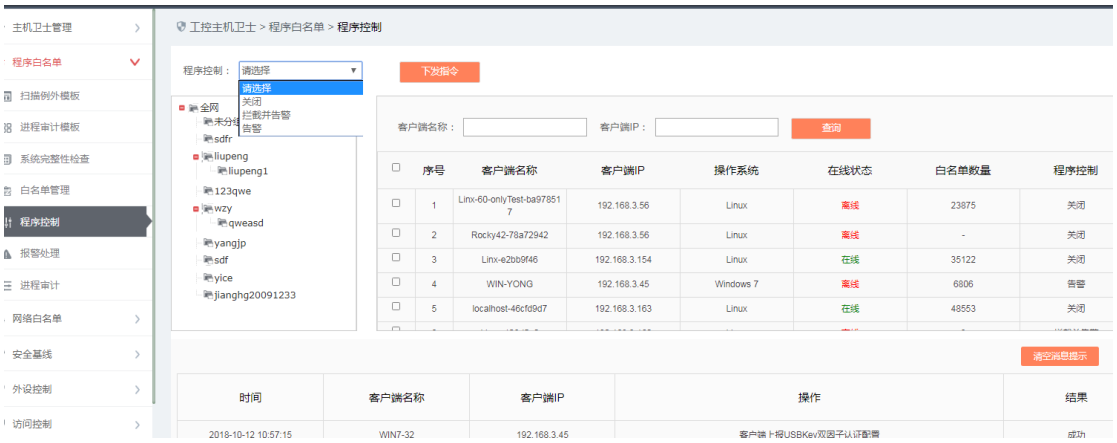


图 4-20 程序控制界面

- 关闭：此项关闭时，不在白名单内的可执行文件允许执行，同时生成报警日志。
- 拦截并告警：此项开启时，自动扫描计算机生成程序白名单数据库，并开启安全防护。不在白名单内的可执行文件不允许执行，同时生成报警日志；
- 告警：此项开启时，自动扫描计算机生成程序白名单数据库，并开启安全防护。不在白名单内的可执行文件允许执行，同时生成报警日志；

4.6.5. 报警处理

可以对白名单拦截的报警日志信息进行加入白名单处理，提供按条件检索及导出功能，界面(如图 4-21 所示)：

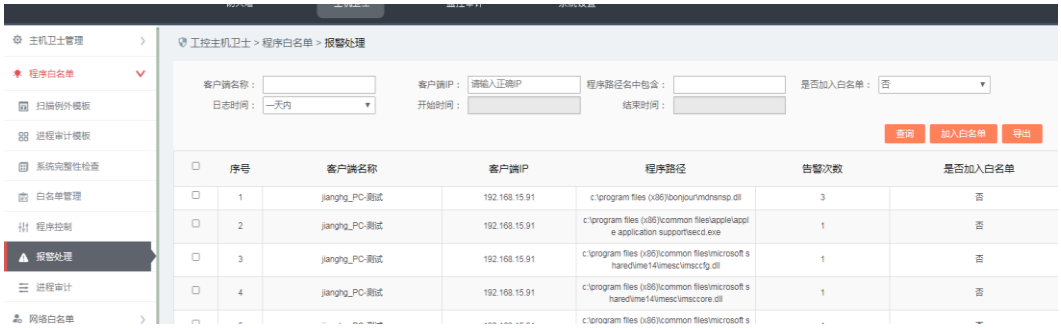


图 4-21 报警处理界面

4.6.6. 进程审计

使用此功能需要先添加进程审计模板，进程审计模板在[进程审计模板]中设置。可以对客户端下发“关闭”、“开启（具体模板）”进程审计策略，待客户端执行成功后，界面自动刷新，(如图 4-22 所示)：。

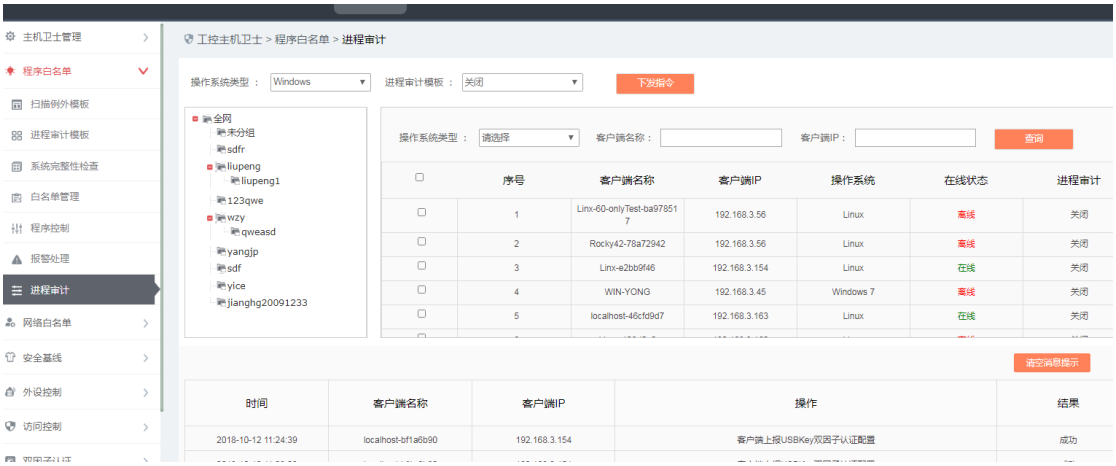


图 4-22 进程审计界面

4.7 网络白名单

网络白名单为 windows 客户端专有功能，可以对 windows 的可执行文件（exe 文件和端口）进行开启和关闭。

4.7.1Windows 防火墙模板

防火墙模板配置，可以配置 windows 系统相关的可执行文件和端口，界面(如图 4-23 所示)：

图 4-23Windows 防火墙模板

Windows 防护墙模板配置界面，(如图 4-24 所示)：

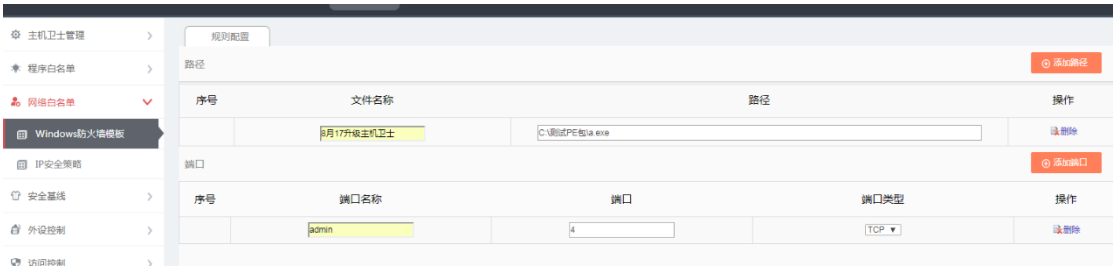


图 4-24 模板配置界面

4.7.2IP 安全策略

IP 安全策略，可以对 SYN 攻击保护和 windows 防火墙模板进行下发，可以进行开启和关闭策略配置。待客户端执行成功后，界面自动刷新，界面(如图 4-25 所示)：

图 4-25IP 安全策略界面

4.8 外设控制

安全 U 盘：内置安全加密芯片，与工控主机卫士软件配套使用，在没有安装工控主机卫士的主机上，安全 U 盘不能被操作。

普通 U 盘：在任何主机上可自动加载识别的 usb 存储设备。

控制客户端普通 U 盘、安全 U 盘操作权限。当授权功能列表中不包含普通 U 盘控制和安全 U 盘控制，本配置页面不可见。如授权功能列表只包含普通 U 盘控制（或安全 U 盘），则管理员只能控制客户端的普通 U 盘（或安全 U 盘）操作权限。

普通 U 盘控制：控制普通 U 盘的使用权限，包括禁止使用、只读使用、不控制。

安全 U 盘控制：控制安全 U 盘的使用权限，包括禁止使用、只读使用、不控制。
策略下发待客户端执行成功后，界面自动刷新，外设控制界面(如图 4-29 所示):

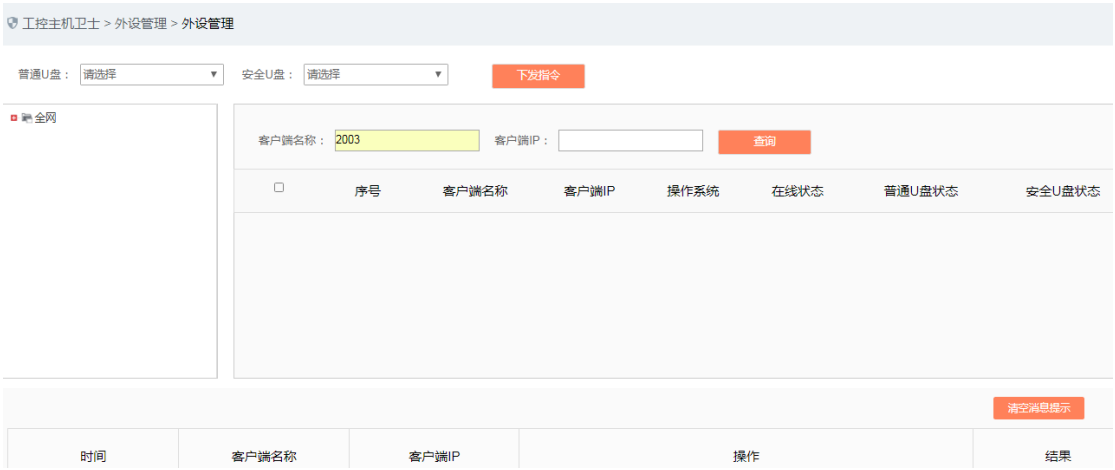


图 4-26 外设控制界面

4.9 非法外联

4.9.1 非法外联模板

1) 、系统默认内置一个通用模板，模板中包含 www.baidu.com、www.sina.com.cn

2) 、管理平台：用户可以自定义模板信息，针对默认模板进行非法地址配置，每个模板最多配置 10 条地址。

3) 、自定义模板中，网址和 IP 地址最多可配置 10 条，如果超过，请重新定义模板。

4) 非法外联模板配置界面(如图 4-44 所示)：

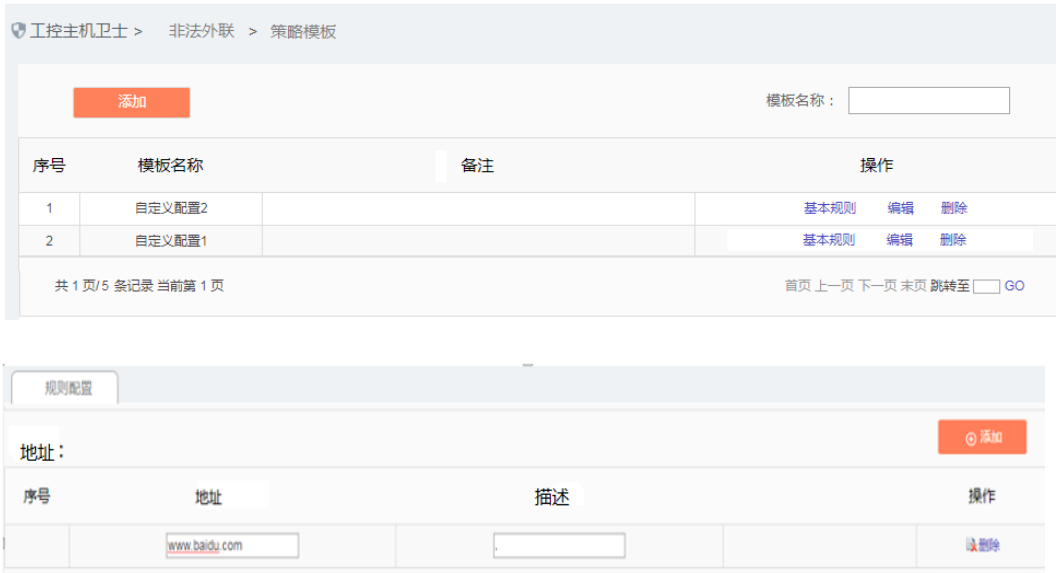


图 4-27 非法外联模板配置界面

4.9.2 策略配置

用户可以向某个主机卫士客户端下发非法外联使能策略同时下发禁用和非法外联检测模板，策略执行成功后，客户端可以查看策略，界面(如图 4-45 所示)：

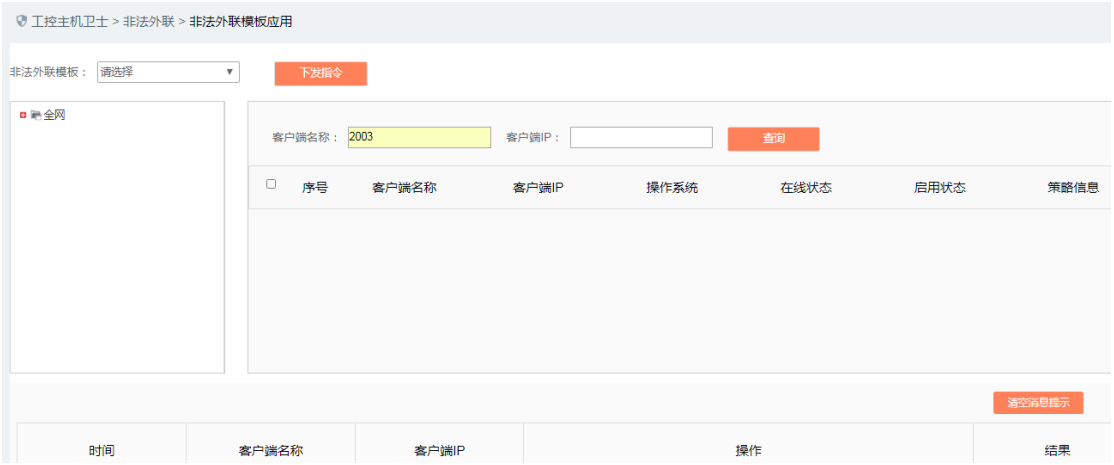


图 4-28 非法外联模板应用界面

查看策略信息，界面(如图 4-46 所示)：

图 4-29 策略信息界面

4.10 基础配置

通过基础配置模块，管理员可以进行系统基础配置、系统操作日志审计、授权和上传非白名单文件的配置。

4.10.1 基础配置

该功能控制客户端（包括 windows 和 linux 客户端）开启或关闭客户端自身保护、报警提示。
自身保护：此项开启时，本产品正常工作所需的所有文件、注册表项、进程均不允许被修改；此项关闭时，上述各项允许被修改。
报警提示：此项开启时，生成实时报警的同时操作系统任务栏会弹气泡提示报警信息；此项关闭时，不再弹气泡提示报警信息。
备注：linux 客户端没有报警提示功能。

功能界面(如图 4-47 所示)：

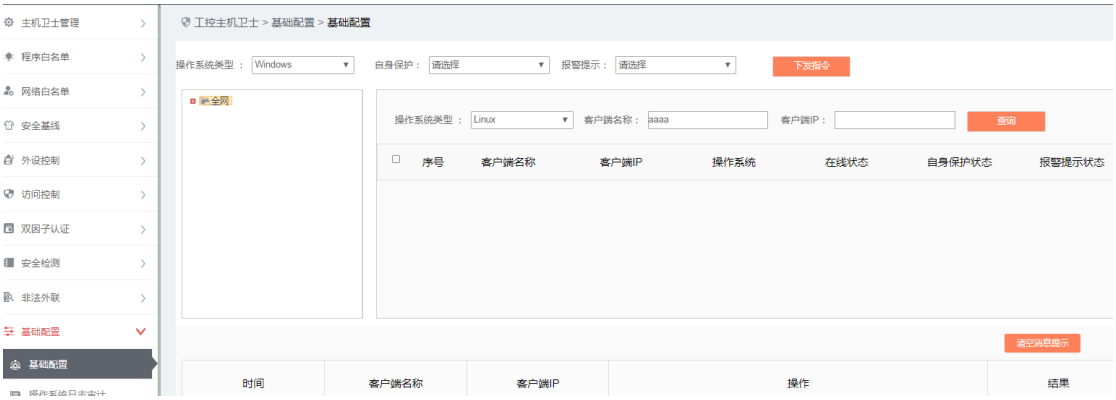


图 4-30 基础配置界面

4.10.2 操作系统日志审计

客户可以通过此界面设置操作系统日志审计的时间。并下发到指定的客户端，界面(如图 4-48 所示)：

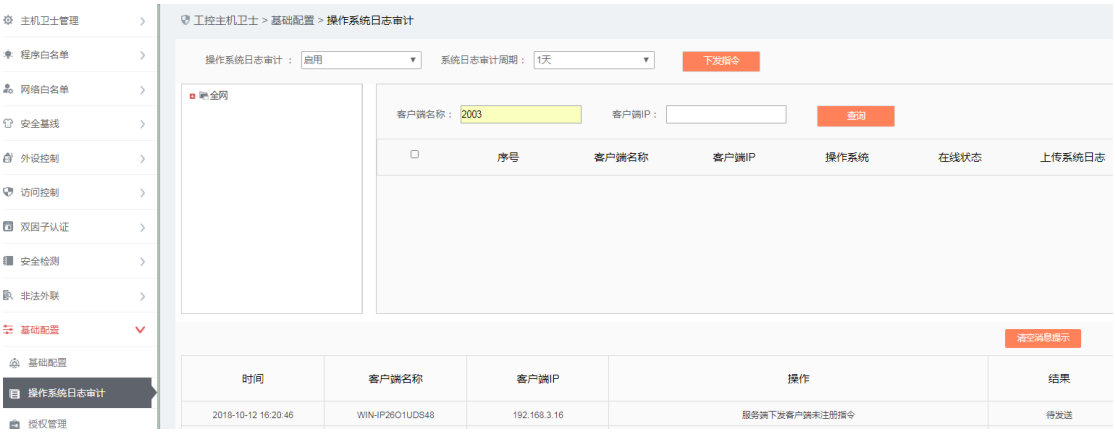


图 4-31 操作系统日志审计界面

4.10.3 授权管理

管理员可通过该界面查看当前的授权信息，如图 4-49 所示。当授权到期或管理员需追加授权节点时，可执行更新授权操作。在工控主机卫士服务器版安装之前，统一管理平台必须首先导入授权文件。点击<请选择授权文件>，弹出选择窗口，如图 4-50 所示，选择正确.lcs 文件，点击<打开>按钮。点击[授权管理]界面的<开始上传>，把选择的 license 文件上传到统一安全管理平台。

图 4-32 授权管理

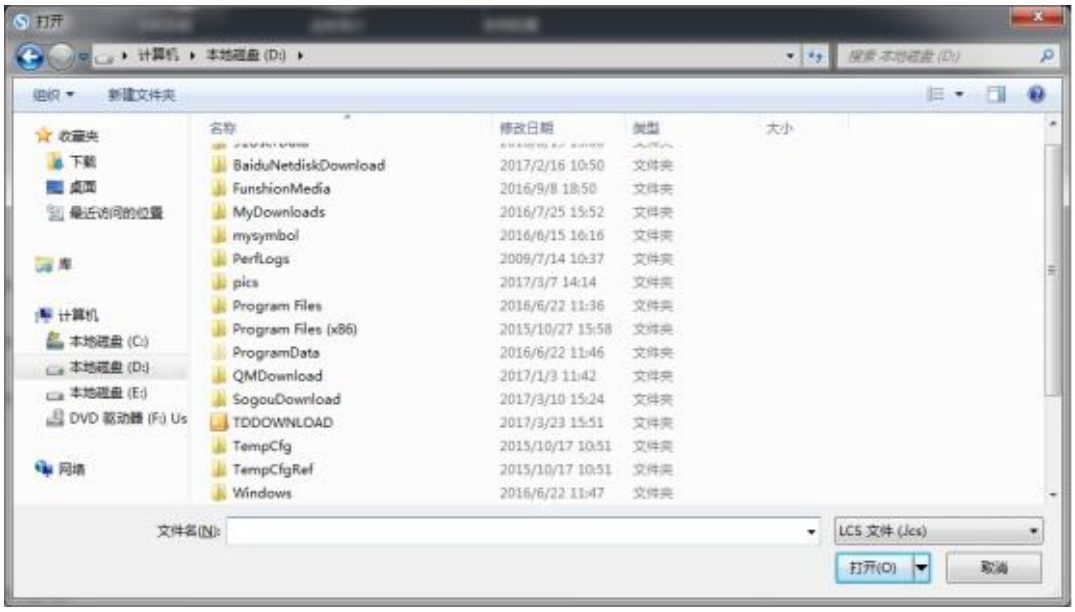


图 4-33 选择 license 文件

4.10.4 上传非白名单文件

开启此功能时，如果已注册的工控主机卫士客户端系统执行了非白名中的可执行程序，且可行执行程序小于 5M，会把此可执行程序上传到统一安全管理平台，以备日后审计。

功能界面(如图 4-51 所示)：

图 4-34 上传非白名单文件界面

5. 监控审计

5.1 产品介绍

5.1.1 产品概述

恩创监控审计是业内领先的工控行业的审计产品，其创新的采用先进的自主研发的硬件，性能优良，功耗低，适用于各种复杂的工业生产现场环境。软件完全自主研发，与自研的硬件相结合，充分发挥硬件的优势，支持网络连接状态检测、工业协议深度解析、工业协议规约检测、全网流量历史数据审计、网络异常检测、工业关键事件检测、用户自定义规则告警、工业协议无流量检测。

恩创监控审计，是专门针对工业控制网络的信息安全审计系统。它采用旁路部署，对工业生产过程“零风险”，基于对工业控制协议（如 IEC104、S7、DNP3、Modbus TCP、OPC）的通信报文进行深度解析（DPI，Deep Packet Inspection），能够实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意软件的传播并实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，为工业控制系统的安全事故调查提供坚实的基础。

恩创控审计，广泛应用于电力、石油、石化、轨道交通、烟草、煤炭、钢铁及先进制造等各个行业。

恩创监控审计一般采用分散部署集中管理的方式，产品包含两大组件**统一安全管理平台**和**智能监测终端**，其中智能监测终端硬件设备分散部署在客户的网络交换机的镜像口处或者串入指定的网络，接受管理平台的集中管理。

5.1.2 外观与说明

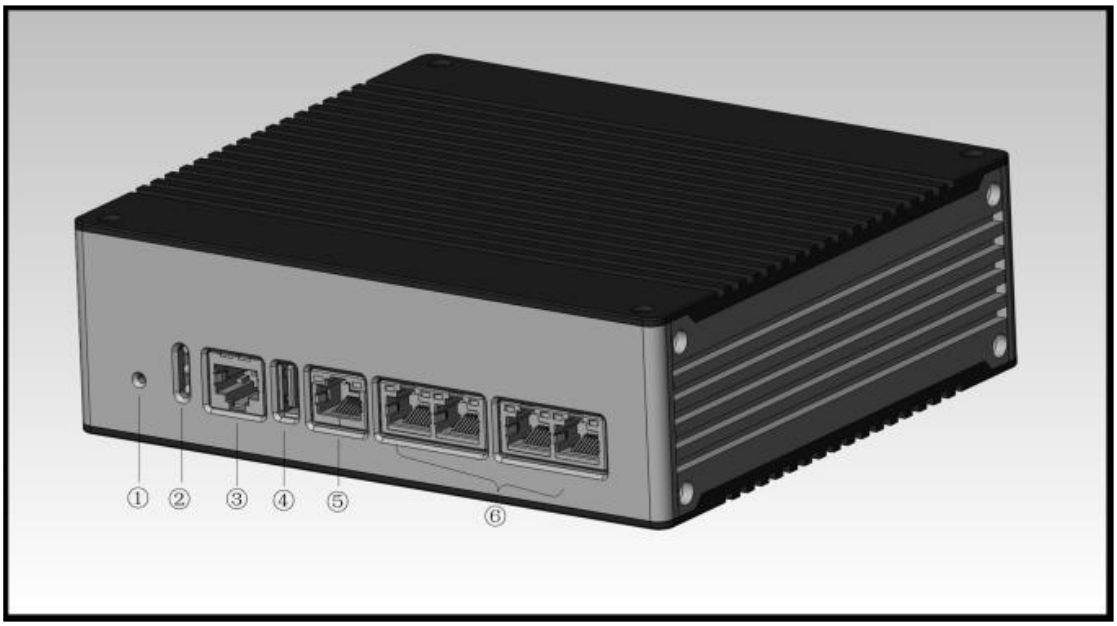


图 5-1 智能监测终端型号 SMA5020 的外观

①Reset 复位按键
②LED 指示灯
③Console 串口，RS232

④USB 2.0接口
⑤管理网口，10/100/1000BASE-T 自适应以太网电口
⑥业务网口，10/100/1000BASE-T 自适应以太网电口

5.1.3 指示灯说明(对应型号 SMA5020)

设备上有 3 个指示灯，分别为 PWR、RUN、BP 指示灯

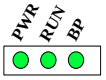


图 5-2 指示灯

表格 25 智能监测终端指示说明

指示灯	面板丝印	状态	说明
电源指示灯	PWR	长灭	没有上电或主机电源故障
		绿色常亮	电源正常，主机正常上电
运行指示灯	RUN	长灭	设备未上电或者故障
		绿闪	设备正常运行
		红闪	设备故障或者受到网络攻击
旁路指示灯	BP	长灭	未启动 BYPASS 功能
		常亮	启动 BYPASS 功能
以太网电接口指示灯	MGMT ETH1/ETH2/ETH3/ETH4	常灭	对应接口处于未连接状态
		指示灯颜色	绿色表示当前工作在千兆速率下 橙色表示当前工作在百兆速率下
		指示灯常亮	接口已经建立连接
		指示灯闪烁	接口正在收发数据

5.1.4 技术规格

表格 26 智能监测终端技术规格

一级需求分类	标题	描述	规格项	具体参数或指标
网络异常检测	协议通信记录	对工控协议的通信报文进行深度解析，记录工控协议的通信日志。 对非工控协议或工控协	记录的工业协议包括	OPC DA、HAD、A&E、DX
				Modbus TCP
				Siemens S7
				DNP3

		议，记录网络连接信息。记录内容包括：时间（开始、结束）、源 MAC、源 IP 地址、源端口、目的 MAC、目的 IP 地址、目的端口、协议、报文数（上行、下行）、字节数（上行、下行）。		IEC104
				CIP
				MMS
				PROFINET
				FINS
			在终端的命令行中配置是否记录工控协议会话信息	支持
			每种工控协议记录 1 个月单表最大支持	1000 万条
			默认情况下记录所有的网络会话信息	支持
			可以设置规则是否记录某些会话信息	支持
			设置规则时，规则的配置项包括	源 IP、目的 IP、源 IP 掩码、目的 IP 掩码、协议、开始源端口、结束源端口、开始目的端口、结束目的端口和执行动作
			此规则包含在某个模板中，每个模板的规格数最大支持	1000 条
			非工控协议 1 个月记录最大支持	1000 万条
	正常通信行为建模	基于工控协议通信记录，自学习建立工控通信模型白名单，即对正常通信行为建模。 支持管理员对建立的工控通信模型白名单进行人工调校。	可以建立白名单的工业协议包括	OPC DA、HAD、A&E、DX，OPC 协议支持动态端口跟踪
				Modbus TCP
				Siemens S7
				DNP3
				IEC104
				CIP
				MMS
				PROFINET
				FINS
			每个白名单模板包含的规则总数最大支持	3000 条(无论是学习还是手动添加)
	异常通信行为检测	对当前工控协议通信行为与白名单进行对比，对偏离白名单的行为进行告警。	对告警事件一键加入白名单	支持，但违反 Modbus TCP 值域、OPC DA 值域、Siemens S7 值域的告警不支持一键添加到白名单。

			此类告警 1 个月最大支持	1000 万条
	异常流量	监测设备的流入流出流量并设置基线值，超出基线值进行报警	异常流量图形化展示	支持
			异常流量统计周期	5 分钟
			异常流量告警确认与告警状态联动	支持
			异常流量基线手动配置	支持
网络攻击检测	工控协议攻击检测	对工控协议报文不符合其规约规定的格式进行检测并告警	可以检测的工业协议包括	OPC DA、HAD、A&E、DX
				Modbus TCP
				Siemens S7
				DNP3
				IEC104
				CIP
				MMS
				PROFINET
				FINS
			支持对某些 IP 的某个协议不进行检测，可以配置的不检测规则的最大条数	1000 条
			1 个月内系统支持的最大告警条数为	1000 万条
	用户自定义告警规则	允许管理员自定义工控协议通信告警规则，对符合告警规则的通信行为进行告警。	支持自定义告警设置的工控协议包括	OPC DA、HAD、A&E、DX
				Modbus TCP
				Siemens S7
				DNP3
				IEC104
				CIP
				MMS
				PROFINET
				FINS
			每种协议最多支持规则	1000 条
			1 个月内告警最大支持	100 万条
	基于参数阈值的检测	对特定过程状态参数、控制信号设定检测阈值，对超阈值的事件进行告警。	支持值域控制的协议包括	Modbus TCP，OPC DA，Siemens S7
			此规则最多支持	和白名单规则合一起上限为 3000 条

			1 个月内告警最大支持	和 Modbus 白名单告警合一起上限为 1000 万条
关键事件检测	无流量检测	在设定的时间内，单 IP 某服务（如 Modbus）的接收报文为零，需要告警。	指定终端上此功能可以开启和关闭	支持
			无流量的时间范围	5-86400 秒
			此规则最多支持	1000 条
			1 个月内最大告警条数支持	10 万条
	关键事件检测	对工程师站组态变更、操控指令变更、PLC 下装、负载变更等关键事件告警。	关键事件定义	系统内置
			用户自定义关键事件	不支持
			关键事件包括	写操作
				S7 协议的 26 请求下载、27 开始下载、28 下载完成、29 请求上载、30 开始上载、31 上载完成、40CPU 启动、41CPU 停止
			此规则最多支持	1000 条
			1 个月内最大告警条数支持	100 万条
网络连接统计	网络连接视图	网络连接实时视图，实时图形化显示监控范围内的所有网络连接，并对异常的网络连接标红显示。 网络连接历史视图，图形化显示一定时间段监控范围内的所有网络连接，并对异常的网络连接标红显示。 双击某个 IP，可以详细展示与此 IP 相连的每个连接的详细信息。 支持基于源、目的 IP 地址过滤，仅显示与某个 IP 地址有关的连接视图。 支持基于源、目的端口过滤，仅显示与某个端口有关的连接视图。 支持基于源、目的 MAC 地址过滤，仅显示与某	提供配置界面配置正常的连接	支持
			对异常连接从建立开始到结束都需要在数据库中存储，在历史视图中使用	最多保存 3 个月的历史连接数据
			连接的详细信息包括：时间（开始、结束）、源 MAC、源 IP 地址、源端口、目的 MAC、目的 IP 地址、目的端口、协议、报文数（上行、下行）、字节数（上行、下行）	实时显示条数不设上限
			实时视图时显示包括：每个 IP 点连接的节点数；有多少个端口打开；多少上行报文数和下行报文数	支持
			连接图中的 IP 配置显示或不显示	支持

		个 MAC 地址有关的连接视图。	连接基线中的配置项包括：源 IP、目的 IP、目的端口	最大支持 1000 条
			网络流量基线配置项包括：源 IP、目的 IP、上行字节数、下行字节数	最大支持 1000 条
	流量统计	提供网络流量及报文数量的实时、历史分时、历史分天（可自定义范围）等的统计情况。	实时流量显示按三种规格实现	过去 60 分钟，横轴坐标每 5 分钟为 1 个点
				过去 24 小时
				过去 30 天
			历史视图可以自定义统计对象(选择统计哪个主机的)，流量、报文在同一个视图中同时体现	支持
	排序统计	给出一定时间范围内按照流出、流入、汇总流量排序的主机、网络设备，以柱状图显示，并提供跳转详细报文功能； 给出一定时间范围内按照流出、流入、汇总报文数排序的主机、网络设备，以柱状图显示，并提供跳转详细报文功能； 给出一定时间范围内按照流出、流入、汇总连接端口排序的主机、网络设备，以柱状图显示，并提供跳转详细报文功能； 给出一定时间范围内按照连接端口排序的主机、网络设备，以柱状图显示，并提供跳转详细报文；	流量 TOP N 可设置	N 的范围：1-50
			流量统计的类型可供下拉选择	下拉选择包括：全部、发送和接收
			报文数 TOP N 可设置	N 的范围：1-50
			报文数统计的类型可供下拉选择	下拉选择包括：全部、发送和接收
			端口统计 TOP N 可设置	N 的范围：1-50
			端口统计的类型可供下拉选择	下拉选择包括：全部、源端口和目的端口
			所有统计可配置时间范围	支持
工作模式支持	系统可以工作在多种模式下	学习模式：系统在此模式下收集学习数据，辅助生成白名单规则，此模式下白名单无告警，其它告警正常产生	切换模式的生效时间	<3s

		运行模式：对违反白名单规则、协议规约的报文，命中用户自定义规则、无流量规则、关键事件的报文进行告警，这些告警可以在管理中心查看		
部署模式支持	终端设备可以以多种方式部署	根据网络的实际要求，终端支持多种部署方式	旁路部署	支持
			串路部署	支持
			旁路转发部署	支持
性能	时间精度	通信记录的时间精度	时间精度要求	<1ms
	终端数量	根据服务器的配置不同，每种服务器支持的终端同时在线数不同	低端服务器最大支持	10 个
会话管理	会话表查询	最大超时时间	最大查询时间，超出此时间将停止查询	30s
		最大会话数	单个智能监测终端支持最大会话数	120000
	会话老化时间	TCP 默认时间	出厂时默认的 TCP 会话老化时间	3 分钟
		TCP 会话老化时间设置	可设置的会话老化时间范围	1-120 分钟
		UDP 默认时间	出厂时默认的 UDP 会话老化时间	3 分钟
		UDP 会话老化时间设置	可设置的会话老化时间范围	1-120 分钟
管理功能	策略管理	提供友好的用户管理界面对策略进行管理	工业协议白名单模板管理	支持
			协议参数配置	支持
			协议规约检测例外模板管理	支持
			无流量检测模板管理	支持
			关键事件检测模板管理	支持
			用户自定义规则	支持

			网络会话审计模板管理	支持
	告警统计信息	对系统内的所有告警信息进行统计汇总	支持的告警包括	工业协议白名单告警
				工业协议协议规约告警
				无流量告警
				用户自定义告警
			图形化展示	支持，包括直方图、饼图和趋势图
			统计结果导出	支持 PNG、JPG、SVG 和 PDF 格式导出
	授权控制	智能监测终端经过授权才能起到监控和审计的作用	专用工具对指定设备进行授权	支持
			管理平台可以查看、下载和更新授权，更新时有结果提示	支持
			授权小于 1 个月到期时黄色底色、已到期的授权项红色底色	支持
	终端设备状态查看	在管理界面可以实时查看设备的状态信息	信息刷新时间	<5s
			可以查看的状态包括	CPU 使用率
				内存使用率
				硬盘使用率
	升级管理	可以对系统内的所有组件进行无缝升级	管理平台自动升级	不支持
			管理平台手动升级	支持
			智能监测终端自动升级	不支持
			智能监测终端手动本地升级	支持
			管理平台升级智能监测终端	支持
	远程管理	可以远程对系统内的策略进行配置管理	通过 web 方式管理系统	支持
	权限验证	身份验证	需要验证用户身份	支持
			用户三权分立	支持，包括系统操作员，系统审核员、配置管理员，审计管理员
			口令强度	长度 8-16，大小写字母，数字，特殊字符(#@!~%^&*)组合
		可信主机	IP 验证	支持
			MAC 验证	支持，可选

存储管理	系统产生的所有告警和日志数据将保存到服务器进行集中管理	日志存储方式	数据库	支持，MySQL
		日志存储周期	最大支持	3 个月
		可以对系统内的日志进行查询	有专门的工具提供查询	支持
			对告警事件进行处理	支持
			可以按指定的条件检索日志	支持
		性能	定时备份	支持，最大 3 个月
			每种日志的最大支持数目	参考各功能指标
			每种告警的最大支持数目	参考各功能指标
	数据库备份	审计管理平台支持自动备份数据到指定的服务器。自动备份支持两种检查策略：磁盘空间达到使用限制和实时数据达到指定限制。备份时还可以指定备份到哪个服务器	磁盘使用限制范围	50%-90%
			存储周期使用限制	1-99，单位:天
			可设置备份到的服务器地址	支持
			匿名用户备份	支持
系统配置	解码引擎配置	解码引擎加载	统一安全管理平台同时加载的解码引擎协议个数	<16

5.2 启动和登录

5.2.1 智能监测终端的启动

根据智能监测终端的硬件安装手册将智能监测终端安装到指定位置后，确保智能监测终端的电源接头正常，将其与要求的电源接通后，智能监测终端将开始正常启动，可以根据安装手册的说明来使用 console 口对智能监测终端的启动过程进行监控。

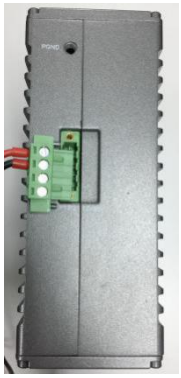


图 5-3 使用提供的电源线给智能监测终端接通电源

智能监测终端正常启动后，对于新智能监测终端，首先需要授权才能工作，将默认工作在工作模式“初始状态”的状态下，此时智能监测终端未有任何监测策略，对于流经智能监测终端的所有报文将不做任何记录，如果需要开始监测，请在管理平台的“策略管理”功能配置页面进行相应的配置，然后选择需要启用监测功能的智能监测终端，将配置的策略应用给终端。

如果智能监测终端已经注册到管理平台，此时启动后智能监测终端将使用上次启动前的策略配置。

5.2.2 CLI 的使用

CLI（Command Line Interface，命令行接口）是用户与设备之间的文本类指令交互界面。用户输入文本类命令，通过输入回车键提交设备执行相应命令，从而对设备进行配置和管理，并可以通过查看输出信息确认配置结果。

由于设备的一些操作需要在此界面下完成，所以设备启动完成后，需要使用 CLI 命令进行一些必要的配置，比如设置连接到的管理平台的地址。

智能监测终端支持多种方式进入命令行接口界面，比如通过 Console 口直接连接或者通过 Telnet/SSH 登录设备后进入命令行接口界面等。无论哪种方式，登录设备时默认使用的用户名为：n-tron.com.cn，默认密码为：n-tron.com.cn。设备的命令行接口界面。(如图 5-4 所示)

```
cavium-linux login: winicssec
Password:

Entering character mode
Escape character is '^]'.

=== WELCOME TO WNT CLI ===

CLI>
```

图 5-4 命令行界面-普通视图

5.2.2.1 帮助

CLI>help 显示帮助信息。

5.2.2.2 系统统计信息相关

CLI>show pkt stat
查看各层次报文统计信息
CLI>show fpa
查看 FPA 信息，主要为各种内存统计信息
CLI>show mem pool
查看 mem pool 内存信息
CLI>config
进入系统视图

5.2.2.3 业务相关

CLI# show log level
Level: TRACE(5)
查看日志级别
CLI# show log plane
查看某个模块日志的开启情况
CLI# set log level <level>
设置日志级别
CLI# set log plane <module_id> [dp|mp|ap|cl]
设置/关闭某个模块的日志

5.2.2.4 设置管理平台的 IP 地址

CLI>show serverip
查看智能监测终端上配置的管理平台的 IP 地址
CLI#set serverip 192.168.8.8
设置智能监测终端需要连接到的管理平台的 IP 地址
CLI>config
设置工业防火墙网关命令，
例如：需要增加网关地址为 192.168.1.1，那么完整命令如下：
CLI# set mgmtgw 192.168.1.1

5.2.2.5 设置智能监测终端的接入方式

CLI#set sma deploy mode access
设置智能监测终端的接入方式为串路部署
CLI#set sma deploy mode port-mirror
设置智能监测终端的接入方式为镜像部署
CLI# set sma deploy mode mirror-forward
设置智能监测终端的接入方式为旁路转发部署

5.2.2.6 更改智能监测终端的 IP 地址

CLI#set mgmtip 192.168.8.6

更改智能监测终端的 IP 地址

5.3 智能监测终端管理

5.3.1 功能介绍

智能监测终端是管理平台的管理对象，所有配置都是针对具体的智能监测终端，如智能监测终端的白名单策略规则都要下发到具体的智能监测终端才能发挥作用。

5.3.2 智能监测终端管理

成功登录管理平台后，在上方菜单栏中找到[监控审计]，点击按钮，然后在左侧导航栏找到[智能监测终端管理/智能监测终端管理]，点击菜单(如图 5-5 所示)，将在右侧的展示页面中看到智能监测终端管理的页面（如图 5-6 所示）。

图 5-5 导航栏中的智能监测终端管理

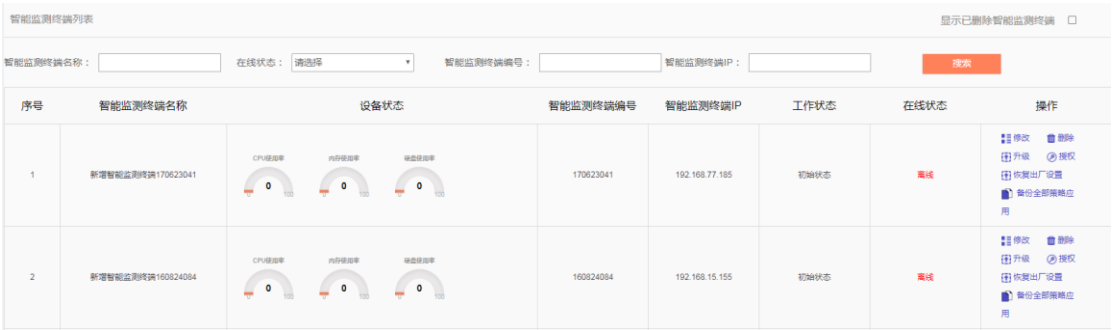
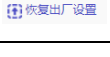


图 5-6 智能监测终端管理展示页面

此处可以查看到智能监测终端当前的运行状态，含义如下：

表格 27 智能监测终端管理列表显示说明

列名称	说明	
智能监测终端名称	系统或用户对每个智能监测终端的一个称呼，如“生产车间 1 控制室智能监测终端”	
设备状态	智能监测终端当前的运行状况，包括 CPU 使用率、内存使用率与硬盘空间利用率。如果某项数值 1min 内一直处于超负荷状态，将产生相应的告警。	
智能监测终端 ID	由系统自动分配的智能监测终端的唯一标识号，一个号代表唯一一个智能监测终端	
智能监测终端 IP	智能监测终端管理网口的 IP 地址	
工作状态	智能监测终端当前工作在哪种工作模式下，新智能监测终端默认是“初始状态”	
在线状态	当前智能监测终端是处于与管理平台连通的状态（即在线）还是未连通（即离线）的状态	
操作	详情 	查看智能监测终端的更多详细信息，更改终端的工作模式、调整策略都在此详情页面
	删除 	删除离线的智能监测终端，在线的智能监测终端不允许删除操作。删除后的智能监测终端可以点击“显示已删除智能监测终端”进行信息查看和恢复
	升级 	在线升级智能监测终端上运行的软件，只有智能监测终端在线时才可以进行此操作，参照 5.3.2.3 智能监测终端升级章节
	授权 	查看和改变智能监测终端的授权项
	恢复出厂设置 	恢复指定智能监测终端到出厂状态，该智能监测终端的除授权以外的所有配置将被清除
	备份全部策略应用 	将源设备上正在应用的全部策略拷贝到一台或多台其他在线且非学习模式下的设备上进行下发应用

5.3.2.1 信息查看

点击[智能监测终端列表]中操作列下的<详情>按钮，将显示(如图 5-7 所示)的智能监测终端的详细信息：

图 5-7 智能监测终端信息查看页

此页面包含了所选设备的更详细信息。

点击本页面的<返回>按钮，将返回到[智能监测终端列表显示]页面。

通过<详情>按钮可以直接修改智能监测终端的配置，包括智能监测终端的基本信息、智能监测终端的运行模式、智能监测终端当前应用的白名单模板、工业协议规约检测模板、无流量检测模板、关键事件检测模板、网络会话审计模板和告警报文保存配置。

表格 28 智能监测终端详细信息说明

列名称	说明
智能监测终端名称	给智能监测终端定义一个容易理解、记忆且有含义的名称
智能监测终端编号	智能监测终端出厂时赋予的编号
智能监测终端 IP	智能监测终端管理网口的 IP 地址
软件版本	智能监测终端当前使用的软件版本
在线状态	智能监测终端与管理平台的连接状态
上线时间	智能监测终端上线时间
工作模式	1.如果当前模式为学习模式，工作模式下拉列表项只有“学习完成”和“学习模式” 2.如果当前为学习完成状态，工作模式下拉列表项有“学习模式”和“运行模式” 3.如果当前模式为运行模式，工作模式下拉列表项有“学习模式” 4.如果用户更改模式为学习模式时，下面的白名单模板设置项将被置灰，不允许操作 5.如果用户由学习模式更改为学习完成，此时会有白名单模板生成编辑框出现，让用户命名学习生成的白名单模板
白名单模板名称	智能监测终端运用的白名单规则模板的名称，只有智能监测终端更改为“运行模式”时编辑框被点亮，此时必须选择一个白名单模板才能够保存。
白名单模板版本	智能监测终端运用的白名单模板的版本号
规约检测例外模板	智能监测终端运用的规约检测例外模板名称
规约检测例外模板版本	智能监测终端运用的规约检测例外模板版本号
无流量检测模板	智能监测终端运用的无流量检测模板名称
无流量检测模板版本	智能监测终端运用的无流量检测模板版本号
关键事件检测模板	智能监测终端运用的关键事件检测模板名称
关键时间检测模板版本	智能监测终端运用的关键事件检测模板版本号

网络会话审计模板	智能监测终端运用的网络会话审计模板名称	
网络会话审计模板版本	智能监测终端运用的网络会话审计模板版本号	
TCP 老化时间	智能监测终端 TCP 会话老化时间	
UDP 老化时间	智能监测终端 UDP 会话老化时间	
部署模式	智能监测终端的部署模式	
工业协议审计日志	智能监测终端是否发送工业协议审计日志	
告警报文保存	白名单告警	智能监测终端是否保存产生白名单告警的报文
	用户自定义告警	智能监测终端是否保存产生自定义告警的报文
	协议规约告警	智能监测终端是否保存违反协议规约的报文
	留存全部报文	智能监测终端是否保存全部原始报文
网口抓包	勾选抓包网口，支持抓取 eth0、eth1、eth2、eth3、eth4 和 eth5 任意一个或者多个端口的报文，可以指定抓取每个端口进、出或者双向报文。管理平台对抓取到的报文按设备端口分类存储，可以查询和下载报文。	
操作	保存	所有的修改信息将被保存并生效，同时返回到智能监测终端信息列表显示页面
	返回	忽略所有的修改，返回到智能监测终端信息列表显示页面
	查询会话表	查看智能监测终端上的会话表
	报文查询及下载	查看网口抓包抓取到的全部报文，可下载

5.3.2.2 删除智能监测终端

点击智能监测终端列表中操作列下的<删除>按钮，可以把不再使用的离线智能监测终端删除。(如图 5-8 所示)

图 5-8 智能监测终端删除

5.3.2.3 智能监测终端升级

当智能监测终端有新的功能更强大、运行更稳定的版本推出后，用户可以通过管理平台，对智能监测终端设备进行远程升级操作。

打开[智能监测终端管理]页面后，点击智能监测终端列表中操作列下的<升级>按钮，将弹出[请选择升级文件]对话框。(如图 5-9 所示)

图 5-9 智能监测终端升级文件选择

- 请选择升级文件

点击请选择升级文件后，将弹出文件选择对话框。找到新的升级文件后(如：sys-sensor.tar.gz)，双击文件或选择<打开>

- 开始上传

点击此按钮，浏览器将此升级文件首先上传到管理平台所在的服务器，然后通知给智能监测终端，智能监测终端将执行具体的升级动作。

- 关闭

点击<关闭>将不执行任何操作，直接返回到智能监测终端列表页。

5.3.2.4 授权管理

License 即许可证，是设备供应商对产品特性的使用范围、期限等进行授权的一种合约形式，License 可以动态控制产品的某些特性是否可用。当需要时，用户可以通过购买 License 激活产品的某些特性和功能特性。对于本产品，每个智能监测终端设备中只能存在一个处于激活状态的 License 文件，激活新的 License 将会使旧的 License 失效。

目前设备支持以下方法激活 License：

通过管理平台手动激活

当购买或续购 License，获得 License 授权证书后，通过登录管理平台指定页面，对所管理的设备进行授权和授权的更新。

智能监测终端授权管理包含授权工具、智能监测终端和管理平台三大组件。授权工具属于恩创公司，只允许在公司内指定用户使用。

5.3.2.4.1 查看授权

打开[智能监测终端管理]页面后，点击智能监测终端列表中操作列下的<授权>按钮，进入详细授权信息页面。(如图 5-10 所示)

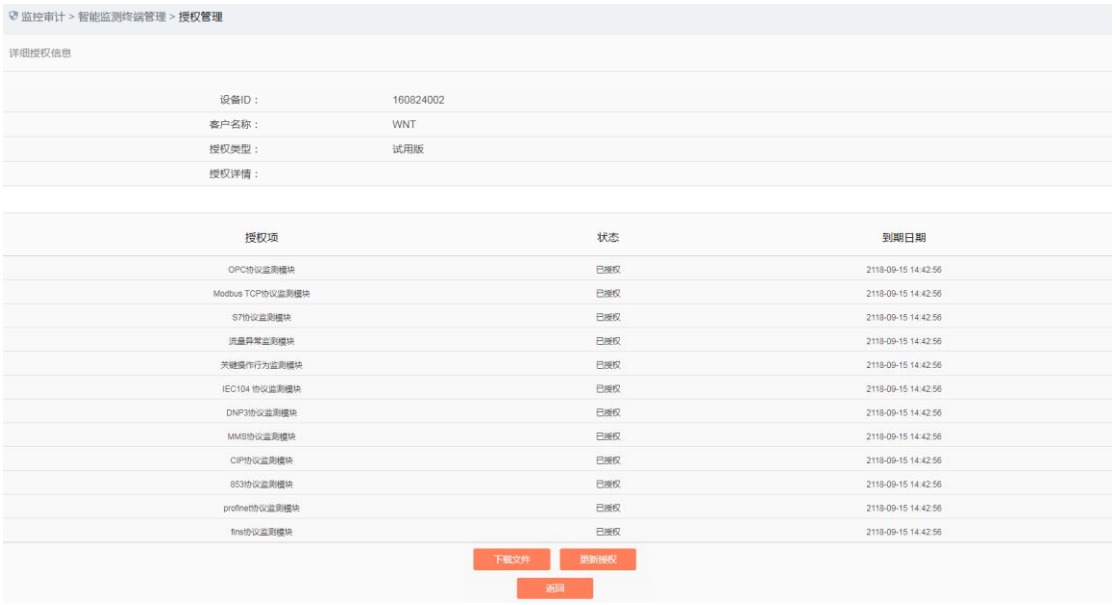


图 5-10 授权详情查看页

此页面显示当前智能监测终端的授权详情。

- 更新授权
  更新当前智能监测终端的授权信息
- 下载文件
  下载当前智能监测终端的授权文件
- 返回
  关闭当前页，返回到智能监测终端管理页面

5.3.2.4.2 更新智能监测终端授权信息

在打开的智能监测终端授权页上，点击<更新授权>按钮，将弹出授权文件选择对话框，以把用户从厂商获取到的最新的授权文件更新到指定的智能监测终端中。(如图 5-11 所示)

图 5-11 选择要更新到智能监测终端的新授权文件

➢ 选择文件

点击选择文件后，将弹出文件选择对话框。

找到新的授权文件后(如：以设备 ID 为名字，后缀为“.dat”的文件)，双击文件或选择<打开>，之后再点击<上传>按钮，浏览器将此文件首先上传到管理平台所在的服务器，然后通知给智能监测终端，智能监测终端将执行更新授权动作，更新成功，用户将可以在授权页面看到新的授权信息。

➢ 返回

点击<返回>将不执行任何操作，直接返回到智能监测终端授权详情页。

5.3.2.5 检索智能监测终端

在[智能监测终端列表]页面中，可以根据条件对智能监测终端进行检索。(如图 5-12 所示)

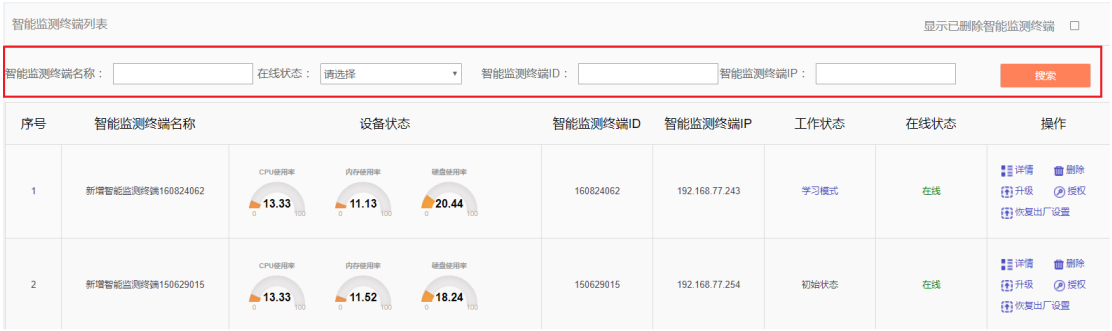


图 5-12 检索智能监测终端

5.4 策略管理

策略管理可以管理智能监测终端使用的所有监测模板，包括工业协议白名单模板、协议参数配置、规约检测例外模板、关键事件检测模板、用户自定义规则、网络会话审计模板和无流量检测模板。

5.4.1 工业协议白名单模板

5.4.1.1 功能介绍

智能监测终端重要的一个创新就是白名单形式的安全策略审计。由于工控网络自身稳定性的特征，使用白名单的方式进行安全审计是解决其安全问题的一个重要且有效的方式。

管理平台的白名单管理功能就是方便用户查看、编辑和使用白名单。

5.4.1.2 模板管理

点击左侧导航栏的[策略管理/工业协议白名单模板](如图 5-13 所示)，进入[工业协议白名单模板]的页面（如图 5-14 所示）。

图 5-13 选择工业协议白名单模板

图 5-14 白名单模板管理

此处可以查看到系统内所有工业协议白名单模板的信息，含义如下：

表格 29 白名单模板列表显示说明

列名称	说明	
模板名称	方便记忆的白名单模板的名称，如“从数采系统 1 学习到的白名单”	
版本号	白名单规则模板的版本，版本与模板的 ID 唯一确定一组白名单规则，每次编辑白名单并保存后，版本号会自动加 1	
应用此模板的智能监测终端	正在使用此白名单模板的所有智能监测终端	
编辑	导入	导入 excel 表格的工业协议白名单规则
	导出	将模板中的工业协议白名单规则导出为 excel 表格
操作	基本配置	查看白名单模板的基本信息，系统内置的白名单模板无此按钮

	规则配置	查看和修改白名单模板规则配置，系统内置的白名单模板无此按钮
	删除	删除白名单模板，不允许删除正在使用的白名单模板，系统内置的白名单模板无此按钮

5.4.1.3 添加白名单模板

点击策略管理的[工业协议白名单模板]模板管理列表标签右侧的<添加>按钮（如图 5-15 所示），将弹出白名单模板添加页面(如图 5-16 所示)

图 5-15 白名单模板添加按钮

图 5-16 白名单模板添加页

表格 30 白名单模板添加信息说明

列名称	说明
模板名称	给工业协议白名单模板定义一个容易理解、记忆且有含义的名字
备注	可选填，附加说明信息

5.4.1.4 导出白名单模板

点击策略管理的[工业协议白名单模板]显示列表中操作列下的<导出>按钮（如图 5-17 所示），将以 excel 表格导出白名单模板中的规则（如图 5-18 所示）。

图 5-17 工业协议白名单模板导出按钮

点击<导出>按钮，将导出一个命名为“白名单模板_{模板名称}_{日期}.xls”的文件，例如在 2015 年 11 月 18 日导出的模板名称为“测试”的规则文件名称为“白名单模板_测试_20151118.xls”。导出的 excel 表格包含该模板的所有规则。(如图 5-18 所示)

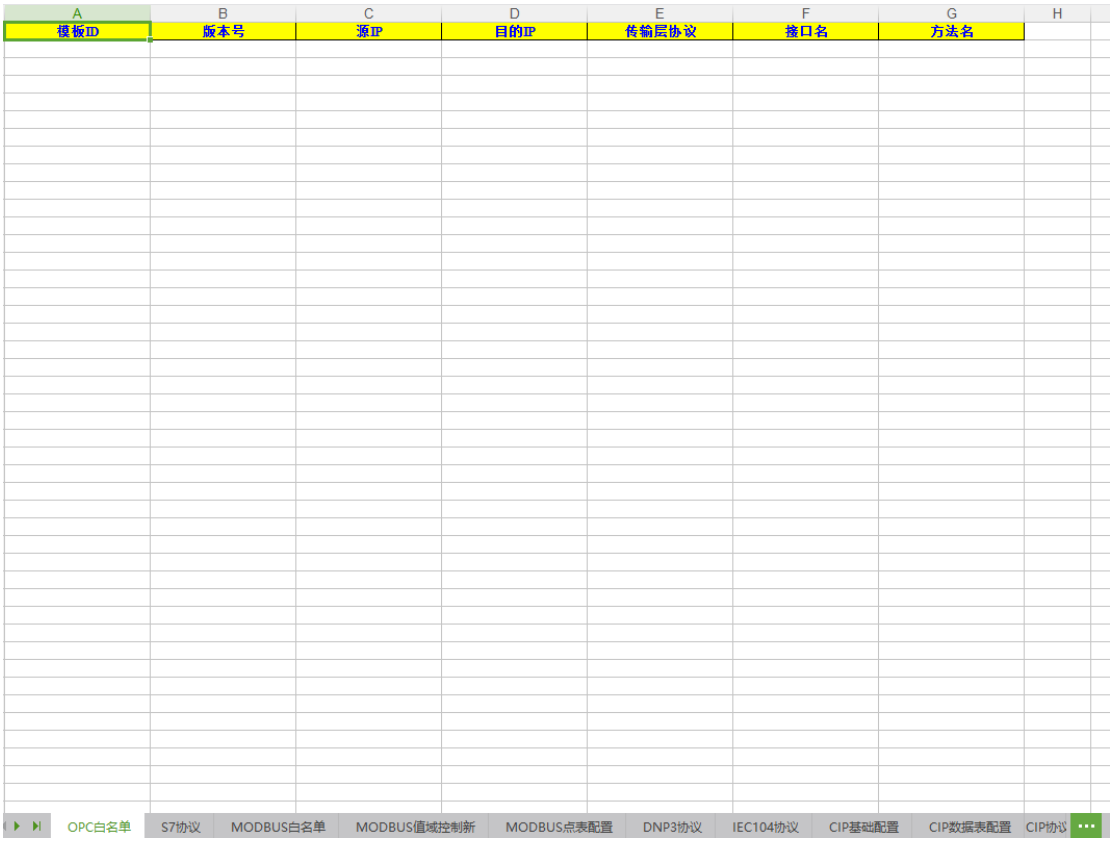


图 5-18 导出 excel 文件示例

5.4.1.5 导入白名单模板

点击策略管理的[工业协议白名单模板]显示列表中操作列下的<导入>按钮（如图 5-19 所示），将以 excel 表格保存的白名单模板中的规则导入到模板（如图 5-20 所示）。

图 5-19 工业协议白名单模板导入规则按钮

点击<导入>按钮，在选择 excel 文件对话框中选择需要导入的文件，点击<导入 Excel>即可导入规则。(如图 5-20 所示)

图 5-20 导入 Excel 选择文件对话框

5.4.1.6 工业协议白名单模板基本配置

点击策略管理的[工业协议白名单模板]显示列表中操作列下的<基本配置>按钮（如图 5-21 所示），将打开[白名单模板信息]页面，可以查看白名单模板的基本信息（如图 5-22 所示）

图 5-21 白名单模板基本配置

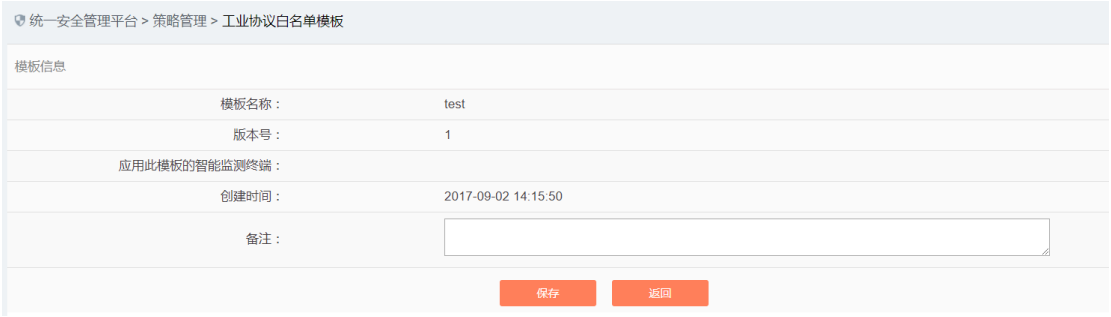


图 5-22 白名单模板基本配置查看页

表格 31 白名单模板基本配置信息说明

列名称	说明
模板名称	白名单模板的名字
版本号	白名单模板的版本号，每修改一次规则自动加 1
应用此模板的智能监测终端	应用此模板的智能监测终端列表
创建时间	白名单模板的创建时间
备注	备注附加信息，可以选填

5.4.1.7 工业协议白名单模板规则配置

工业协议白名单项的管理是白名单模板管理的核心，所有模板都依赖于具体的每个白名单项。目前智能监测终端支持八种标准工业协议的白名单：OPC、Siemens S7、Modbus、DNP3、IEC104、CIP、MMS、FINS、PROFINET，未来将支持所有通用工业协议的白名单。

下面将以 OPC 和 Modbus 协议为例，指导如何管理白名单项，其它协议类似，只是具体的字段不同。

5.4.1.7.1 查看 OPC 白名单项

进入[规则配置]页面后，默认显示的是 OPC 白名单项，点击不同的 tab 页标签，将显示对应标签的白名单项。(如图 5-23 所示)

图 5-23 OPC 白名单项信息查看页

点击<返回>按钮，将返回到[工业协议白名单模板列表显示]页面。

5.4.1.7.2 添加 OPC 白名单项

进入[规则配置]页面后，点击右侧的<添加>按钮（如图 5-24 所示），将在 OPC 白名单项列表的最下方自动添加一行新的白名单项(如图 5-25 所示)

图 5-24 工业协议白名单模板添加按钮

图 5-25 工业协议白名单模板添加页

表格 32 OPC 白名单项字段说明

列名称	说明
源 IP	发起 OPC 数据请求的 IP 地址，点分十进制格式
目的 IP	请求 OPC 数据的目的 IP 地址，点分十进制格式
传输层协议	传输层协议为 TCP
接口名	OPC 协议规范中的某个接口名称，内置在数据字典中
方法名	OPC 协议规范中规定的某个接口下面的某个方法，内置在数据字典中

表格 33 OPC 值域白名单项字段说明

列名称	说明	
源 IP	发起 OPC 数据请求的 IP 地址，点分十进制格式	
目的 IP	请求 OPC 数据的目的 IP 地址，点分十进制格式	
传输层协议	传输层协议为 TCP	
接口名	OPC 协议规范中的某个接口名称，内置在数据字典中	
方法名	OPC 协议规范中规定的某个接口下面的某个方法，内置在数据字典中	
ItemID	点唯一标识符	
数据类型	值类型	
最小值	值类型最小值	
最大值	值类型最大值	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到白名单模板信息列表显示页面
	返回	忽略所有的修改，返回到白名单模板信息列表显示页面

5.4.1.7.3 修改 OPC 白名单项

进入[工业协议白名单模板]规则配置页面，就可以更改某个白名单项的源 IP、目的 IP，接口名和方法名，修改后点击<保存>按钮即可。

5.4.1.7.4 删除 OPC 白名单项

进入[工业协议白名单模板]规则配置页面后，直接点击某个白名单项最右侧的<删除>按钮，可以删除对应的白名单项。(如图 5-26 所示)

图 5-26 工业协议白名单模板删除按钮

此时只是临时删除，如果需要删除生效，此时需要点击保存。
其它协议采用类似的操作即可完成工业协议白名单项的添加、修改和删除。

5.4.1.7.5 Modbus 协议白名单配置

Modbus 协议的解析深度与其它工业协议不同，工业防火墙可以解析到 Modbus 协议传输的具体的值，所以白名单模板中关于 Modbus 协议的规则配置主要有两部分内容，分别为：基础白名单和值域控制。

5.4.1.7.6 Modbus 基础白名单项

此处配置类似于 OPC 协议，请参考 OPC 协议相关参数配置方法。

5.4.1.7.7 Modbus 值域控制

使用 Modbus 值域控制功能首先要勾选全局使能选，如图 5-27 所示

图 5-27Modbus 协议值域使能

使能值域控制功能后，下面的字节顺序就可以编辑了，推荐使用默认配置，如果默认配置与现场不符时，再进行相应的调节。

值域功能最重要的就是“点表配置”，下面把点表配置中的各个字段含义解释在下面表格中

表格 34 Modbus 点击字段说明

列名称	说明
点名	具有含义的代表 Modbus 某个地址的别名
源 IP	发起 Modbus 数据请求的 IP 地址，点分十进制格式
目的 IP	请求 Modbus 数据的目的 IP 地址，点分十进制格式
源掩码	源 IP 掩码
目的掩码	目的 IP 掩码
功能码	Modbus 协议功能码
地址	Modbus 协议操作的某个点的起始地址
数据类型	点的数据类型
偏移量	某些功能码下操作某种类型的数据在地址中的偏移，如 06 功能码操作的数据类型为 BOOL 型时需要指定地址中哪一位表示此 BOOL 值，默认情况下填 0
高 8 位/低 8 位	某些功能码下操作某种类型的数据在地址中的使用的哪个字节，如 06 功能码(可操作 2 个字节的地址)操作的数据类型为 Byte 型(1 个字节)时需要指定操作的地址中的哪个字节(8 位)，默认情况下为高 8 位
最小值	允许操作的最小值
最大值	允许操作的最大值

值域规则项的添加、修改、编辑、删除请参考 Modbus 基础项操作。

5.4.1.8 删除白名单模板

点击策略管理的[工业协议白名单模板]信息显示列表中操作列下的<删除>按钮，可以把不再使用的白名单模板进行删除。正在被使用的白名单模板不允许删除。(如图 5-28 所示)

图 5-28 工业协议白名单模板删除按钮

5.4.1.9 检索白名单模板

在策略管理的[工业协议白名单模板]信息显示列表面中，可以根据条件对白名单模板进行检索。(如图 5-29 所示)

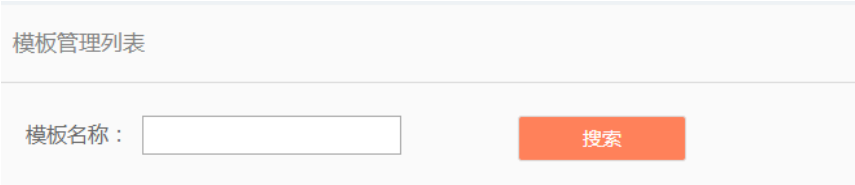


图 5-29 检索白名单模板

5.4.2 规约检测例外模板

5.4.2.1 功能介绍

智能监测终端将依据工业协议规约对报文进行检测，当检测到不符合规约规定的报文时，智能监测终端将报警。如果客户不希望智能监测终端对某些数据连接进行规约检测时，可以通过配置规约检测例外模板禁用智能监测终端的规约检测功能。

5.4.2.2 模板管理

点击左侧导航栏的[策略管理/规约检测例外模板](如图 5-30 所示)，进入[规约检测例外模板]的页面（如图 5-31 所示）。

图 5-30 选择规约检测例外模板

图 5-31 规约检测例外模板管理

此处可以查看到系统内所有规约检测例外模板的信息，含义如下：

表格 35 规约检测例外模板列表显示说明

列名称	说明	
模板名称	方便记忆的规约检测例外模板的名称，如“数采系统 1 的规约例外”	
版本号	规约例外模板的版本，版本与模板的 ID 唯一确定一组规约例外检测规则，每次编辑规约检测例外规则并保存后，版本号会自动加 1	
应用此模板的智能监测终端	正在使用此模板的所有智能监测终端	
编辑	导入	导入 excel 表格的规约检测例外规则
	导出	将模板中的规约检测例外规则导出为 excel 表格
操作	基本配置	查看规约检测例外模板的基本信息
	规则配置	查看和修改规约检测例外模板规则配置
	删除	删除模板，无法删除正在使用的模板

5.4.2.3 添加规约检测例外模板

点击策略管理的[规约检测例外模板]模板管理列表标签右侧的<添加>按钮（如图 5-32 所示），将弹出规约检测例外模板添加页面(如图 5-33 所示)

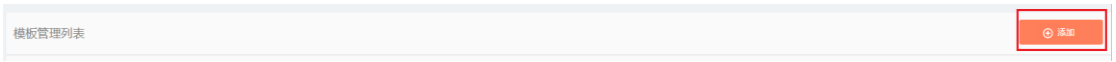


图 5-32 规约检测例外模板添加按钮

图 5-33 规约检测例外模板添加页

表格 36 规约检测例外模板添加信息说明

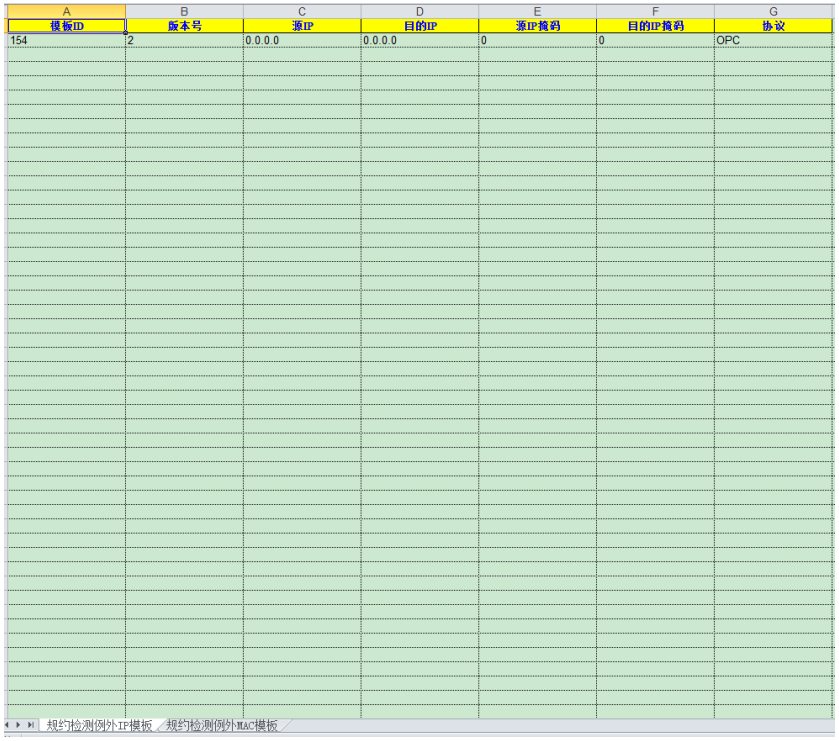
列名称	说明
模板名称	给规约检测例外模板定义一个容易理解、记忆且有含义的名字
备注	可选填，附加说明信息

5.4.2.4 导出规约检测例外模板

点击策略管理的[规约检测例外模板]显示列表中操作列下的<导出>按钮（如图 5-34 所示），将以 excel 表格导出规约检测例外模板中的规则（如图 5-35 所示）。

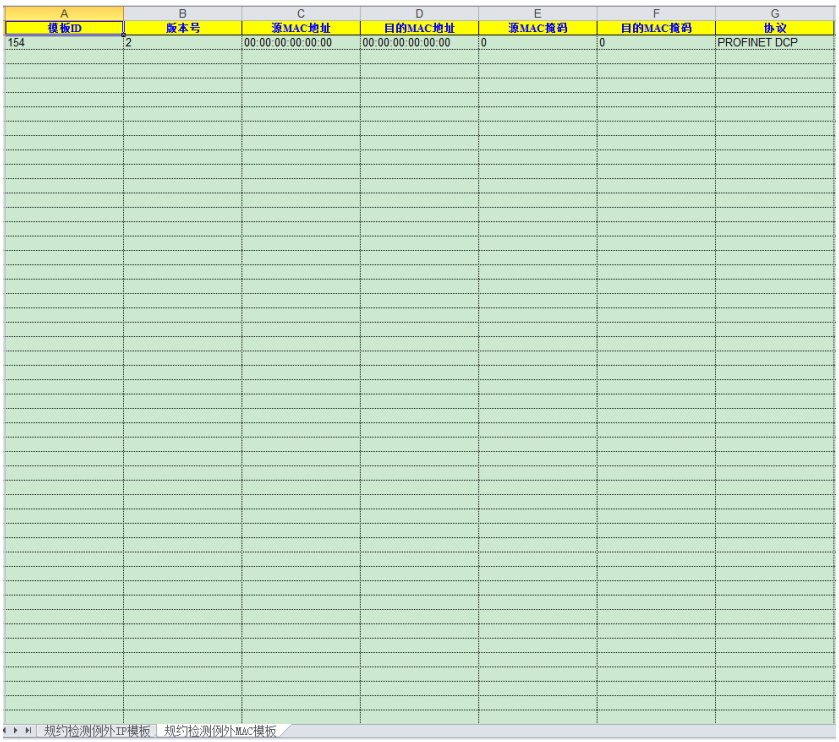
图 5-34 规约检测例外模板导出按钮

点击<导出>按钮，将导出一个命名为“规约检测例外模板_{模板名称}_{日期}.xls”的文件，例如在 2015 年 11 月 18 日导出的模板名称为“测试”的规则文件名称为“规约检测例外模板_测试_20151118.xls”。导出的 excel 表格包含该模板的所有规则。



模板ID	版本号	源IP	目的IP	源IP掩码	目的IP掩码	协议
154	2	0.0.0.0	0.0.0.0	0	0	OPC

规约检测例外IP模板 规约检测例外MAC模板



模板ID	版本号	源MAC地址	目的MAC地址	源MAC掩码	目的MAC掩码	协议
154	2	00:00:00:00:00:00	00:00:00:00:00:00	0	0	PROFINET DCP

规约检测例外IP模板 规约检测例外MAC模板

图 5-35 导出 excel 文件示例

5.4.2.5 导入规约检测例外模板

点击策略管理的[规约检测例外模板]显示列表中操作列下的<导入>按钮（如图 5-36 所示），将以 excel 表格保存的规约检测例外模板中的规则导入到模板（如图 5-37 所示）。

图 5-36 规约检测例外模板导入规则按钮

点击<导入>按钮，在选择 excel 文件对话框中选择需要导入的文件，点击<导入 Excel>即可导入规则。

图 5-37 导入 Excel 选择文件对话框

5.4.2.6 规约检测例外模板基本配置

点击策略管理的[规约检测例外模板]显示列表中操作列下的<基本配置>按钮（如图 5-38 所示），将打开[规约检测例外模板]基本配置页面，可以查看规约检测例外模板的基本信息（如图 5-39 所示）

图 5-38 规约例外检测模板基本配置

图 5-39 规约检测例外模板基本配置查看页

表格 37 白名单模板基本配置信息说明

列名称	说明
模板名称	模板的名字
版本号	模板的版本号，每修改一次规则自动加 1
应用此模板的智能监测终端	应用此模板的智能监测终端列表
创建时间	模板的创建时间
备注	备注附加信息，可以选填

5.4.2.7 规约检测例外模板规则配置

规约检测例外规则的管理是规约检测例外模板管理的核心，所有模板都依赖于具体的每条规则。

5.4.2.7.1 查看规约检测例外规则

进入[规则配置]页面后，显示的是规约检测例外项。包含 IP 规则和 MAC 规则配置(如图 5-40 所示)

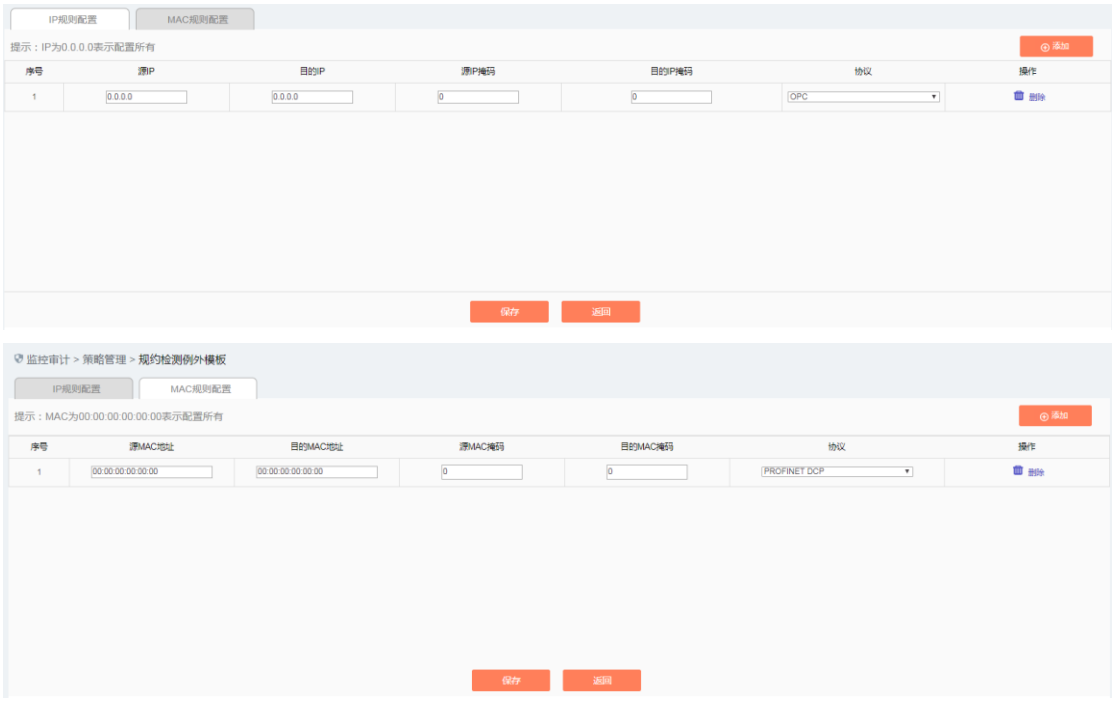


图 5-40 规约检测例外项信息查看页

点击<返回>按钮，将返回到[规约检测例外模板列表显示]页面。

5.4.2.7.2 添加规约检测例外规则

进入[规则配置]页面后，点击右侧的<添加>按钮（如图 5-41 所示），将在规则的最下方自动添加一行新的规约检测例外规则(如图 5-42 所示)

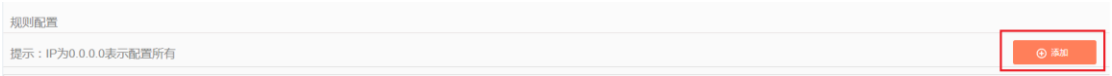


图 5-41 规约检测例外模板添加按钮

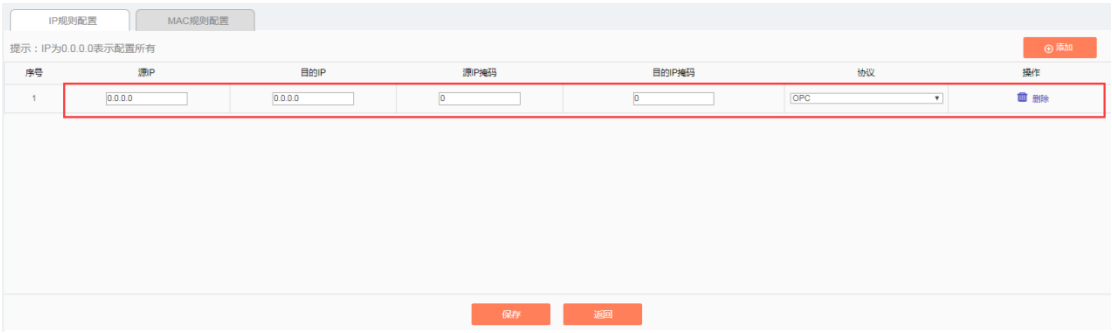


图 5-42 规约检测例外模板添加页

表格 38 规约检测例外 IP 规则字段说明

列名称	说明	
源 IP	规约检测例外连接发起请求的 IP 地址，点分十进制格式	
目的 IP	规约检测例外连接的目的 IP 地址，点分十进制格式	
源 IP 掩码	源 IP 地址的掩码，范围为 0 到 32	
目的 IP 掩码	目的 IP 地址的掩码，范围为 0 到 32	
协议	规约检测例外的工业协议，选项包括 OPC、Modbus、S7、DNP3、IEC104、CIP、MMS 和 853	
操作	删除	删除指定的某条规则，点击《保存》按钮提交删除请求，删除后的数据会重新提交数据库修改信息保存到数据库并生效，同时返回到规约检测例外模板信息列表显示页面
	保存	所有的修改信息将被保存到数据库并生效，同时返回到规约检测例外模板信息列表显示页面
	返回	忽略所有的修改，返回到规约检测例外模板信息列表显示页面

表格 39 规约检测例外 MAC 规则字段说明

列名称	说明
源 MAC 地址	规约检测例外连接发起请求的 MAC 地址
目的 MAC 地址	规约检测例外连接的目的 MAC 地址，
源 MAC 掩码	源 MAC 地址的掩码，范围为 0 到 48
目的 MAC 掩码	目的 MAC 地址的掩码，范围为 0 到 48

协议	规约检测例外的工业协议，选项包括 PROFINET DCP，PROFINET IO RE	
操作	删除	删除指定的某条规则，点击《保存》按钮提交删除请求，删除后的数据会重新提交数据库修改信息保存到数据库并生效，同时返回到规约检测例外模板信息列表显示页面
	保存	所有的修改信息将被保存到数据库并生效，同时返回到规约检测例外模板信息列表显示页面
	返回	忽略所有的修改，返回到规约检测例外模板信息列表显示页面

5.4.2.7.3 修改规约检测例外规则

进入[规约检测例外规则配置]页面，就可以更改某条规则的源 IP、目的 IP，源 IP 掩码、目的 IP 掩码和协议，修改后点击<保存>按钮即可。

5.4.2.7.4 删除规约检测例外规则

进入[规约检测例外规则配置]页面后，直接点击某条规则最右侧的<删除>按钮，可以删除对应的规则。(如图 5-43 所示)

图 5-43 规约检测例外规则删除按钮

5.4.2.8 删除规约检测例外模板

点击策略管理的[规约检测例外模板]信息显示列表中操作列下的<删除>按钮，可以把不再使用的规约检测例外模板删除。正在被使用的规约检测例外模板无法删除。(如图 5-44 所示)

图 5-44 规约检测例外模板删除按钮

5.4.2.9 检索规约检测例外模板

在策略管理的[规约检测例外模板]信息显示列表面中，可以根据条件对规约检测例外模板进行检索。(如图 5-45 所示)

图 5-45 检索规约检测例外模板

5.4.3 关键事件检测模板

5.4.3.1 功能介绍

智能监测终端内置部分关键操作，如对工程师站组态变更、操控指令变更、PLC 下装、负载变更等。用户可以通过配置关键事件检测模板来检测指定连接上发生的关键事件。

5.4.3.2 模板管理

点击左侧导航栏的[策略管理/关键事件检测模板](如图 5-46 所示)，进入[关键事件检测模板]的页面（如图 5-47 所示）。

图 5-46 选择关键事件检测模板

图 5-47 关键事件检测模板管理

此处可以查看到系统内所有关键事件检测模板的信息，含义如下：

表格 39 规约检测例外模板列表显示说明

列名称	说明	
模板名称	方便记忆的关键事件检测模板的名称，如“数采系统 1 的关键事件”	
版本号	关键事件检测模板的版本，版本与模板的 ID 唯一确定一组关键事件检测规则，每次编辑关键事件检测规则并保存后，版本号会自动加 1	
应用此模板的智能监测终端	正在使用此模板的所有智能监测终端	
编辑	导入	导入 excel 表格的关键事件检测规则
	导出	将模板中的关键事件检测规则导出为 excel 表格
操作	基本配置	查看关键事件检测模板的基本信息
	规则配置	查看和修改关键事件检测模板规则配置
	删除	删除模板，无法删除正在使用的模板

5.4.3.3 添加关键事件检测模板

点击策略管理的[关键事件检测模板]模板管理列表标签右侧的<添加>按钮（如图 5-48 所示），将弹出关键事件检测模板添加页面(如图 5-49 所示)

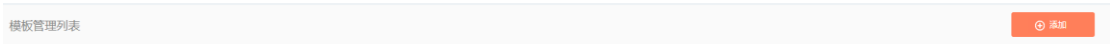


图 5-48 规约检测例外模板添加按

图 5-49 规约检测例外模板添加页

表格 40 关键事件检测模板添加信息说明

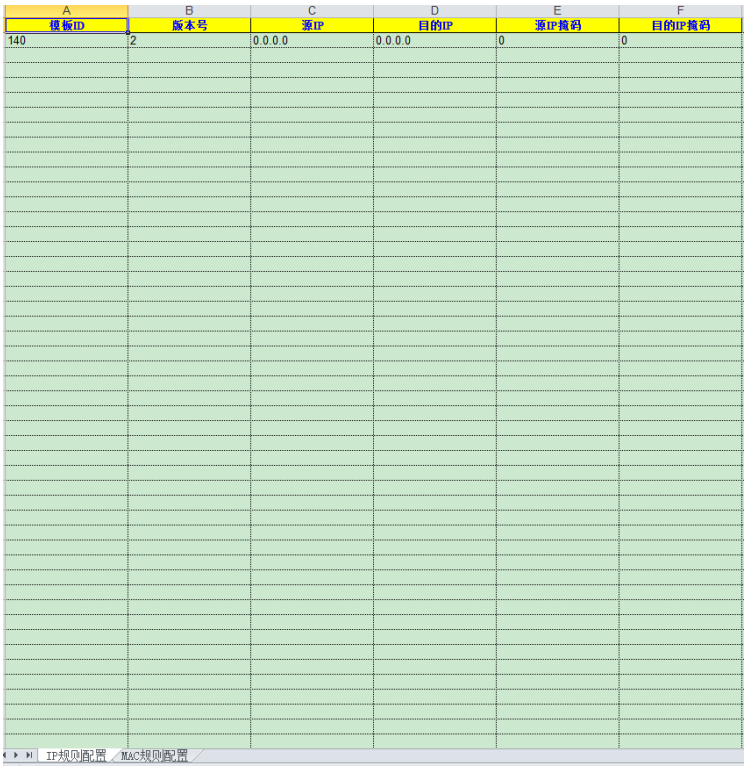
列名称	说明
模板名称	给关键事件检测模板定义一个容易理解、记忆且有含义的名字
备注	可选填，附加说明信息

5.4.3.4 导出关键事件检测模板

点击策略管理的[关键事件检测模板]显示列表中操作列下的<导出>按钮(如图 5-50 所示),将以 excel 表格导出规约检测例外模板中的规则（如图 5-51 所示）。

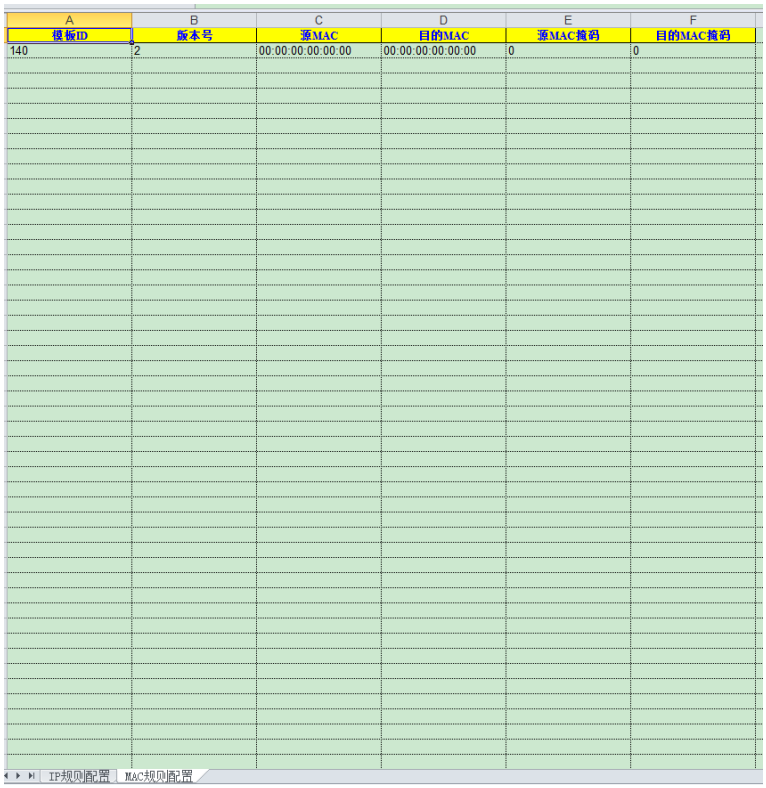
图 5-50 关键事件检测模板导出按钮

点击<导出>按钮，将导出一个命名为“关键事件检测模板_{模板名称}_{日期}.xls”的文件，例如在 2015 年 11 月 18 日导出的模板名称为“测试”的规则文件名称为“关键事件检测模板_测试_20151118.xls”。导出的 excel 表格包含该模板的所有规则。



A	B	C	D	E	F
模板ID	版本号	源IP	目的IP	源IP掩码	目的IP掩码
140	2	0.0.0.0	0.0.0.0	0	0

IP规则配置 MAC规则配置



A	B	C	D	E	F
模板ID	版本号	源MAC	目的MAC	源MAC掩码	目的MAC掩码
140	2	00:00:00:00:00:00	00:00:00:00:00:00	0	0

IP规则配置 MAC规则配置

图 5-51 导出 excel 文件示例

5.4.3.5 导入关键事件检测模板

点击策略管理的[关键事件检测模板]显示列表中操作列下的<导入>按钮（如图 5-52 所示），将以 excel 表格保存的关键事件检测模板中的规则导入到模板（如图 5-53 所示）。

图 5-52 关键事件检测模板导入规则按钮

点击<导入>按钮，在选择 excel 文件对话框中选择需要导入的文件，点击<导入 Excel>即可导入规则。

图 5-53 导入 Excel 选择文件对话框

5.4.3.6 关键事件检测模板基本配置

点击策略管理的[关键事件检测模板]显示列表中操作列下的<基本配置>按钮（如图 5-54 所示），将打开[关键事件检测模板基本配置]页面，可以查看关键事件检测模板的基本信息（如图 5-55 所示）

图 5-54 关键事件检测模板基本配置

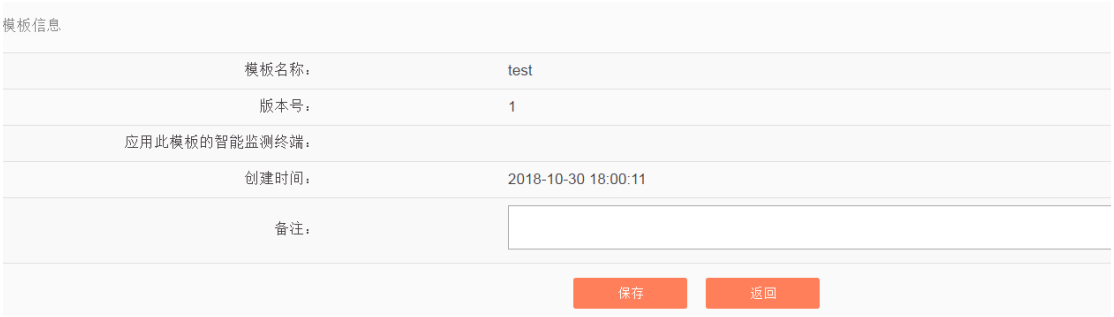


图 5-55 关键事件检测模板基本配置查看页

表格 41 关键事件检测基本配置信息说明

列名称	说明
模板名称	模板的名字
版本号	模板的版本号，每修改一次规则自动加 1
应用此模板的智能监测终端	应用此模板的智能监测终端列表
创建时间	模板的创建时间
备注	备注附加信息，可以选填

5.4.3.7 关键事件检测模板规则配置

关键事件检测规则的管理是关键事件检测模板管理的核心，所有模板都依赖于具体的每条规则。

5.4.3.7.1 查看关键事件检测规则

进入[规则配置]页面后，显示的是关键事件检测规则。(如图 5-56 所示)

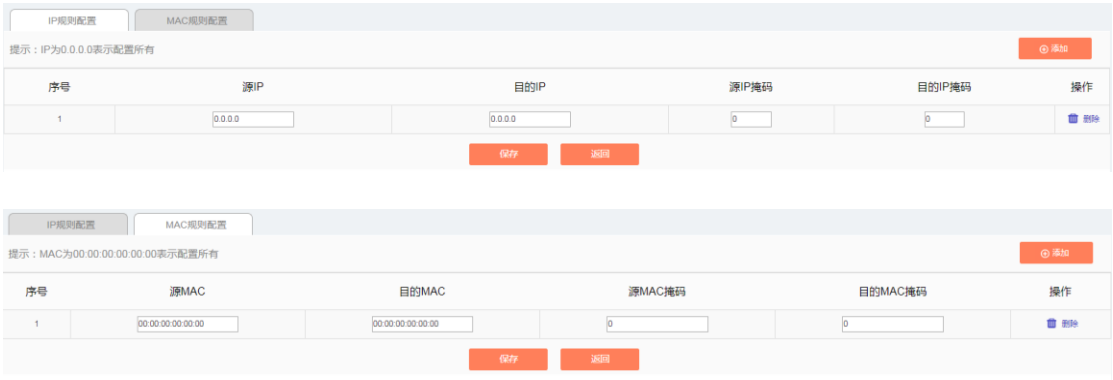


图 5-56 关键事件检测规则查看页

点击<返回>按钮，将返回到[关键事件检测模板列表显示]页面。

5.4.3.7.2 添加关键事件检测规则

进入[规则配置]页面后，点击右侧的<添加>按钮（如图 5-57 所示），将在规则的最下方自动添加一行新的关键事件检测规则(如图 5-58 所示)

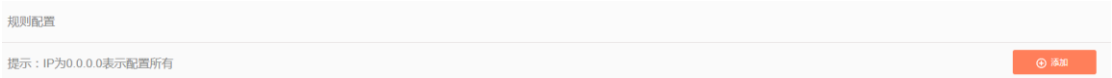


图 5-57 关键事件检测模板添加按钮

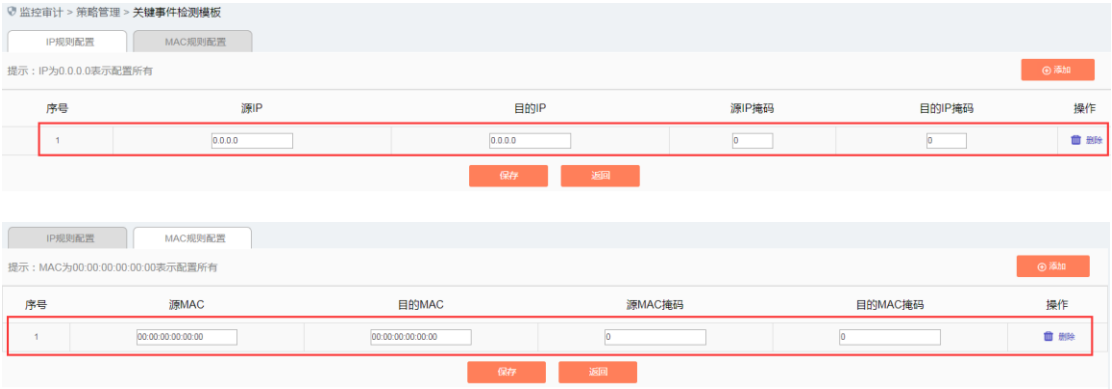


图 5-58 关键事件检测模板添加页

表格 40 关键事件检测 IP 规则字段说明

列名称	说明	
源 IP	关键事件检测连接发起请求的 IP 地址，点分十进制格式	
目的 IP	关键事件检测连接的目的 IP 地址，点分十进制格式	
源 IP 掩码	源 IP 地址的掩码，范围为 0 到 32	
目的 IP 掩码	目的 IP 地址的掩码，范围为 0 到 32	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到模板信息列表显示页面
	返回	忽略所有的修改，返回到模板信息列表显示页面

表格 41 关键事件检测 MAC 规则字段说明

列名称	说明
源 MAC	关键事件检测连接发起请求的 MAC 地址
目的 MAC	关键事件检测连接的目的 MAC 地址
源 IP 掩码	源 MAC 地址的掩码，范围为 0 到 48
目的 IP 掩码	目的 MAC 地址的掩码，范围为 0 到 48

操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到模板信息列表显示页面
	返回	忽略所有的修改，返回到模板信息列表显示页面

5.4.3.7.3 修改关键事件检测规则

进入[关键事件检测模板规则配置]页面，就可以更改某条规则的源 IP、目的 IP，源 IP 掩码和目的 IP 掩码，修改后点击<保存>按钮即可。

5.4.3.7.4 删除关键事件检测规则

进入[关键事件检测模板规则配置]页面后，直接点击某条规则最右侧的<删除>按钮，可以删除对应的规则。(如图 5-59 所示)

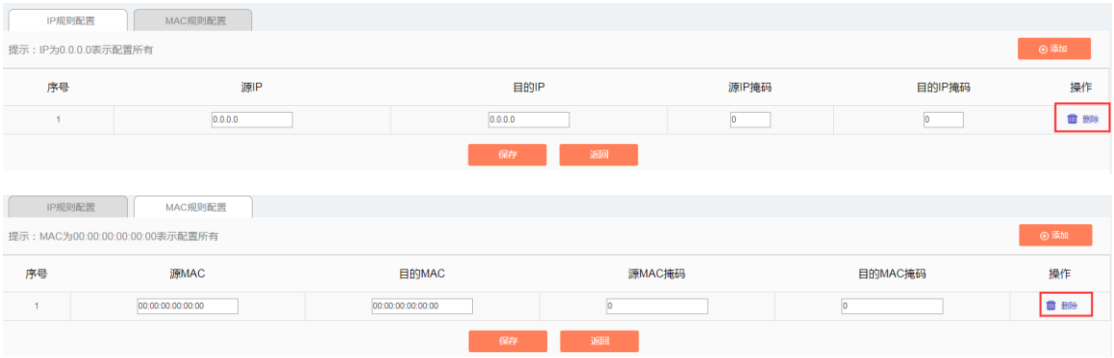


图 5-59 关键事件检测规则删除按钮

5.4.3.8 删除关键事件检测模板

点击策略管理的[关键事件检测模板]信息显示列表中操作列下的<删除>按钮，可以把不再使用的关键事件检测模板删除。正在被使用的模板无法删除。(如图 5-60 所示)

图 5-60 关键事件检测模板删除按钮

5.4.3.9 检索关键事件检测模板

在策略管理的[关键事件检测模板]信息显示列表面中，可以根据条件对关键事件检测模板进行检索。(如图 5-61 所示)

图 5-61 检索关键事件检测模板

5.4.4 用户自定义规则

5.4.4.1 功能介绍

除了智能监测终端内置的关键操作外，智能监测终端允许用户配置其关心的操作。当检测到用户定义的操作后，智能监测终端进行报警。

5.4.4.2 规则配置

点击左侧导航栏的[策略管理/用户自定义规则](如图 5-62 所示)，进入[用户自定义规则]的页面（如图 5-63 所示）。

图 5-62 选择用户自定义规则

图 5-63 用户自定义规则

目前智能监测终端支持五种标准工业协议的用户自定义规则：OPC、Siemens S7、Modbus、DNP3、IEC104、CIP、MMS 和 PROFINET，FINS，未来将支持所有通用工业协议的自定义规则。下面将以 OPC 协议为例，指导如何管理用户自定义规则，其它协议类似，只是具体的字段不同。

5.4.4.3 OPC 自定义规则配置

5.4.4.3.1 查看 OPC 用户自定义规则

进入[用户自定义规则]页面后，默认显示的是 OPC 协议项，点击不同的 tab 页标签，将显示对应标签的用户自定义规则项。(如图 5-64 所示)

图 5-64 OPC 用户自定义规则信息查看页

5.4.4.3.2 添加 OPC 用户自定义规则

进入[用户自定义规则]页面后，点击右侧的<添加>按钮（如图 5-65 所示），将在 OPC 白名单项列表的最下方自动添加一行新的 OPC 用户自定义规则(如图 5-66 所示)

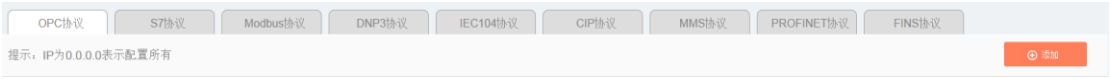


图 5-65 OPC 自定义规则添加按钮

图 5-66 OPC 自定义规则添加页

表格 42 OPC 自定义规则字段说明

列名称	说明
源 IP	发起 OPC 数据请求的 IP 地址，点分十进制格式
源 IP 掩码	源 IP 地址掩码，范围为 0 到 32

目的 IP	请求 OPC 数据的目的 IP 地址，点分十进制格式
目的 IP 掩码	目的 IP 地址掩码，范围为 0 到 32
传输层协议	传输层协议
接口名	OPC 协议规范中的某个接口名称，内置在数据字典中
方法名	OPC 协议规范中规定的某个接口下面的某个方法，内置在数据字典中
删除	删除所选 OPC 自定义规则
保存	所有的修改信息将被保存到数据库并生效

5.4.4.3.3 修改 OPC 用户自定义规则

进入[用户自定义规则]页面，就可以更改某个自定义规则的源 IP、源 IP 掩码、目的 IP、目的 IP 掩码、接口名和方法名，修改后点击<保存>按钮即可。

5.4.4.3.4 删除 OPC 自定义规则

进入[用户自定义规则]页面后，直接点击某条规则最右侧的<删除>按钮，可以删除对应的规则。(如图 5-67 所示)

图 5-67 OPC 用户自定义规则删除按钮

其它协议采用类似的操作即可完成自定义规则的添加、修改和删除。

5.4.5 网络会话审计模板

5.4.5.1 功能介绍

智能监测终端默认将所有流经它的流量记录。当用户不希望记录所有流量时，他可以通过网络会话审计模板配置关心的流量，其他流量将不被智能监测终端记录。

5.4.5.2 模板管理

点击左侧导航栏的[策略管理/网络会话审计模板](如图 5-68 所示)，进入[网络会话审计模板]的页面（如图 5-69 所示）。

图 5-68 选择网络会话审计模板

图 5-69 网络会话审计模板管理

此处可以查看到系统内所有网络会话审计模板的信息，含义如下：

表格 43 网络会话审计模板列表显示说明

列名称	说明	
模板名称	方便记忆的网络会话审计模板的名称，如“数采系统 1 的审计模板”	
版本号	网络会话审计模板的版本，版本与模板的 ID 唯一确定一组网络会话审计规则，每次编辑网络会话审计规则并保存后，版本号会自动加 1	
应用此模板的智能监测终端	正在使用此模板的所有智能监测终端	
编辑	导入	导入 excel 表格的网络会话审计规则
	导出	将模板中的网络会话审计规则导出为 excel 表格
操作	基本配置	查看网络会话审计模板的基本信息
	规则配置	查看和修改网络会话审计模板规则配置
	删除	删除模板，无法删除正在使用的模板

5.4.5.3 添加网络会话审计模板

点击策略管理的[网络会话审计模板]模板管理列表标签右侧的<添加>按钮（如图 5-70 所示），将弹出网络会话审计模板添加页面(如图 5-71 所示)

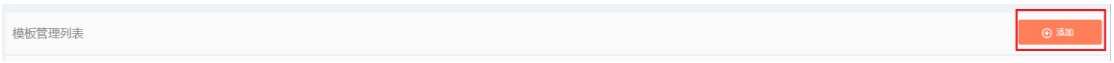


图 5-70 网络会话审计模板

图 5-71 网络会话审计模板添加页

表格 44 网络会话审计模板添加信息说明

列名称	说明
模板名称	给网络会话审计模板定义一个容易理解、记忆且有含义的名字
备注	可选填，附加说明信息

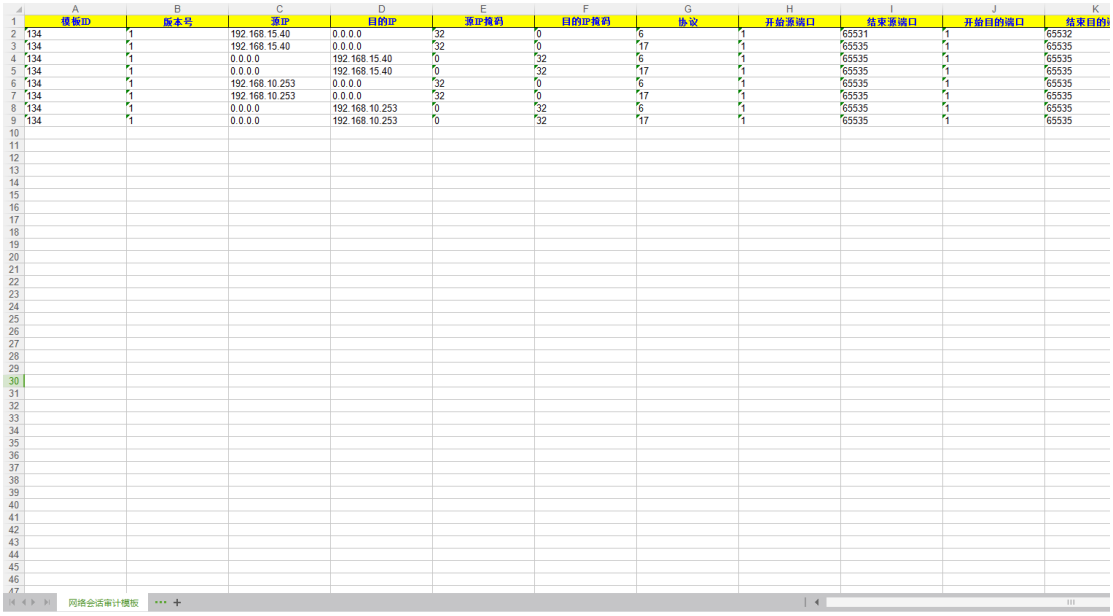
5.4.5.4 导出网络会话审计模板

点击策略管理的[网络会话审计模板]显示列表中操作列下的<导出>按钮(如图 5-72 所示),将以 excel 表格导出网络会话审计模板中的规则（如图 5-73 所示）。

图 5-72 网络会话审计模板导出按钮

点击<导出>按钮，将导出一个命名为“网络会话审计模板_{模板名称}_{日期}.xls”的文件，例如在

2015 年 11 月 18 日导出的模板名称为“测试”的规则文件名称为“网络会话审计模板_测试_20151118.xls”。导出的 excel 表格包含该模板的所有规则。



模板ID	版本号	源IP	目的IP	源IP掩码	目的IP掩码	协议	开始源端口	结束源端口	开始目的端口	结束目的
134	1	192.168.15.40	0.0.0.0	32	0	6	1	65531	1	65532
134	1	192.168.15.40	0.0.0.0	32	0	17	1	65535	1	65535
134	1	0.0.0.0	192.168.15.40	0	32	6	1	65535	1	65535
134	1	0.0.0.0	192.168.15.40	0	32	17	1	65535	1	65535
134	1	192.168.10.253	0.0.0.0	32	0	6	1	65535	1	65535
134	1	192.168.10.253	0.0.0.0	32	0	17	1	65535	1	65535
134	1	0.0.0.0	192.168.10.253	0	32	6	1	65535	1	65535
134	1	0.0.0.0	192.168.10.253	0	32	17	1	65535	1	65535

网络会话审计模板

图 5-73 导出 excel 文件示例

5.4.5.5 导入网络会话审计模板

点击策略管理的[网络会话审计模板]显示列表中操作列下的<导入>按钮（如图 5-74 所示），将以 excel 表格保存的网络会话审计模板中的规则导入到模板（如图 5-75 所示）。

图 5-74 网络会话审计模板导入规则按钮

点击<导入>按钮，在选择 excel 文件对话框中选择需要导入的文件，点击<导入 Excel>即可导入规则。

图 5-75 导入 Excel 选择文件对话框

5.4.5.6 网络会话审计模板基本配置

点击策略管理的[网络会话审计模板]显示列表中操作列下的<基本配置>按钮（如图 5-76 所示），将打开[网络会话审计模板]基本配置页面，可以查看网络会话审计模板的基本信息（如图 5-77 所示）

图 5-76 网络会话审计模板基本配置

图 5-77 网络会话审计模板基本配置查看页

表格 45 网络会话审计模板基本配置信息说明

列名称	说明
模板名称	模板的名字
版本号	模板的版本号，每修改一次规则自动加 1
应用此模板的智能监测终端	应用此模板的智能监测终端列表
创建时间	模板的创建时间
备注	备注附加信息，可以选填

5.4.5.7 网络会话审计模板规则配置

网络会话审计规则的管理是网络会话审计模板管理的核心，所有模板都依赖于具体的每条规则。

5.4.5.7.1 查看网络会话审计规则

进入[规则配置]页面后，显示的是网络会话审计规则。(如图 5-78 所示)

图 5-78 网络会话审计规则查看页

点击<返回>按钮，将返回到[网络会话审计模板列表显示]页面。

5.4.5.7.2 添加网络会话审计规则

进入[规则配置]页面后，点击右侧的<添加>按钮（如图 5-79 所示），将在规则的最下方自动添加一行新的网络会话审计规则(如图 5-80 所示)

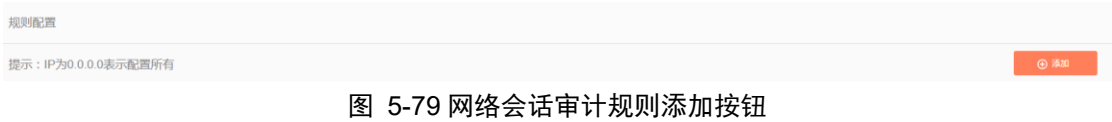


图 5-79 网络会话审计规则添加按钮

图 5-80 网络会话审计规则添加项

表格 46 网络会话审计规则字段说明

列名称	说明
源 IP	网络连接发起请求的 IP 地址，点分十进制格式
目的 IP	网络连接的目的 IP 地址，点分十进制格式
源 IP 掩码	源 IP 地址的掩码，范围为 0 到 32
目的 IP 掩码	目的 IP 地址的掩码，范围为 0 到 32
协议	传输层协议，可选 TCP 或 UDP
开始源端口	源端口的起始数值，范围为 0 到 65535
结束源端口	源端口的结束数值，范围为 0 到 65535，结束源端口必须大于开始源端口
开始目的端口	目的端口的起始数值，范围为 0 到 65535
结束目的端口	目的端口的结束数值，范围为 0 到 65535，结束目的端口必须大于开始目的端口
删除	删除指定规则

操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到模板信息列表显示页面
	返回	忽略所有的修改，返回到模板信息列表显示页面

5.4.5.7.3 修改网络会话审计规则

进入[网络会话审计规则配置]页面，就可以更改某条规则的源 IP、目的 IP，源 IP 掩码、目的 IP 掩码、协议、开始源端口、结束源端口、开始目的端口和结束目的端口，修改后点击<保存>按钮即可。

5.4.5.7.4 删除网络会话审计规则

进入[网络会话审计规则配置]页面后，直接点击某条规则最右侧的<删除>按钮，可以删除对应的规则。(如图 5-81 所示)

图 5-81 网络会话审计规则删除按钮

5.4.5.8 删除网络会话审计模板

点击策略管理的[网络会话审计模板]信息显示列表中操作列下的<删除>按钮，可以把不再使用的网络会话审计模板删除。正在被使用的模板无法删除。(如图 5-82 所示)

图 5-82 网络会话审计模板删除按钮

5.4.5.9 检索网络会话审计模板

在策略管理的[网络会话审计模板]信息显示列表面中，可以根据条件对网络会话审计模板进行检索。(如图 5-83 所示)

图 5-83 检索网络会话审计模板

5.4.6 无流量检测模板

5.4.6.1 功能介绍

智能监测终端可以探测某个用户关心的网络连接由于某种原因没有流量的情况并发出告警。用户可以通过无流量模板配置其关系的流量。

5.4.6.2 模板管理

点击左侧导航栏的[策略管理/无流量检测模板](如图 5-84 所示)，进入[无流量检测模板]的页面（如图 5-85 所示）。

图 5-84 选择无流量检测模板

图 5-85 无流量检测模板管理

此处可以查看到系统内所有无流量检测模板的信息，含义如下：

表格 47 网络会话审计模板列表显示说明

列名称	说明	
模板名称	方便记忆的无流量检测模板的名称，如“数采系统 1 的无流量检测模板”	
版本号	无流量检测模板的版本，版本与模板的 ID 唯一确定一组无流量检测规则，每次编辑无流量检测规则并保存后，版本号会自动加 1	
应用此模板的智能监测终端	正在使用此模板的所有智能监测终端	
编辑	导入	导入 excel 表格的无流量检测规则
	导出	将模板中的无流量检测规则导出为 excel 表格
操作	基本配置	查看无流量检测模板的基本信息
	规则配置	查看和修改无流量检测模板规则配置
	删除	删除模板，无法删除正在使用的模板

5.4.6.3 添加无流量检测模板

点击策略管理的[无流量检测模板]模板管理列表标签右侧的<添加>按钮（如图 5-86 所示），将弹出无流量检测模板添加页面(如图 5-87 所示)

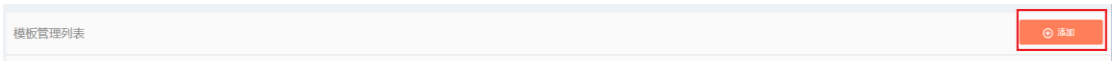


图 5-86 无流量检测模板添加按钮

图 5-87 无流量检测模板添加页

表格 48 无流量检测模板添加信息说明

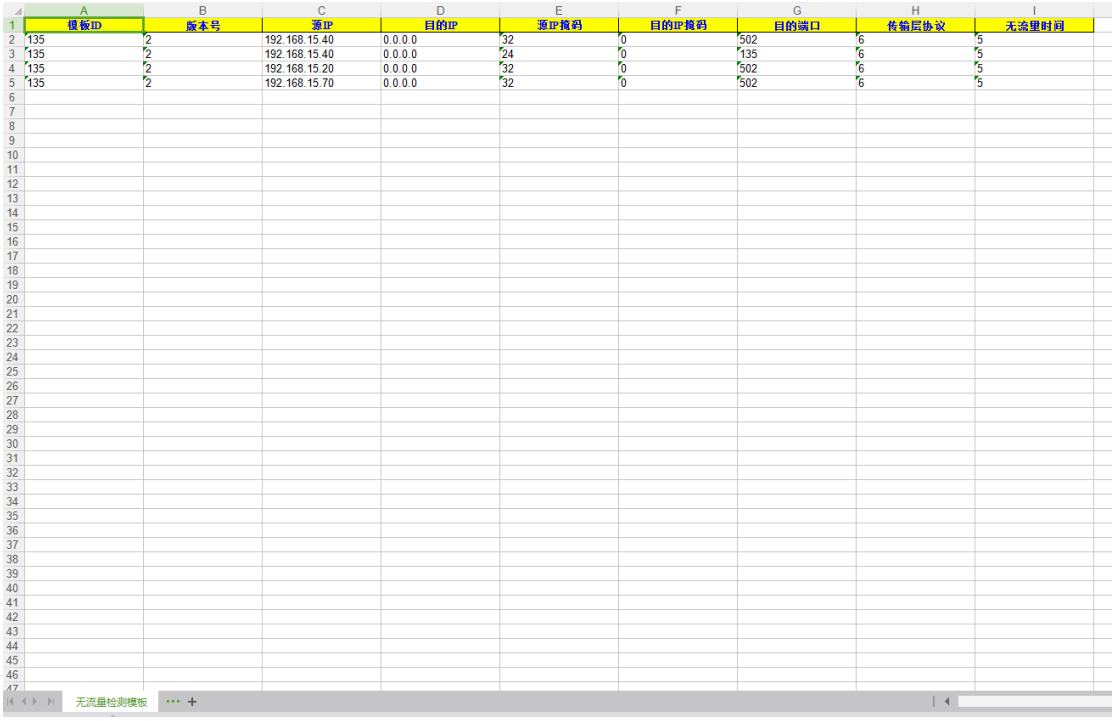
列名称	说明
模板名称	给无流量检测模板定义一个容易理解、记忆且有含义的名字
备注	可选填，附加说明信息

5.4.6.4 导出无流量检测模板

点击策略管理的[无流量检测模板]显示列表中操作列下的<导出>按钮（如图 5-88 所示），将以 excel 表格导出无流量检测模板中的规则（如图 5-89 所示）。

图 5-88 无流量检测模板导出按钮

点击<导出>按钮，将导出一个命名为“无流量检测模板_{模板名称}_{日期}.xls”的文件，例如在 2015 年 11 月 18 日导出的模板名称为“测试”的规则文件名称为“无流量检测模板_测试_20151118.xls”。导出的 excel 表格包含该模板的所有规则。



模板ID	版本号	源IP	目的IP	源IP掩码	目的IP掩码	目的端口	传输层协议	无流量时间
135	2	192.168.15.40	0.0.0.0	32	0	502	6	5
135	2	192.168.15.40	0.0.0.0	24	0	135	6	5
135	2	192.168.15.20	0.0.0.0	32	0	502	6	5
135	2	192.168.15.70	0.0.0.0	32	0	502	6	5

图 5-89 导出 excel 文件示例

5.4.6.5 导入无流量检测模板

点击策略管理的[无流量检测模板]显示列表中操作列下的<导入>按钮（如图 5-90 所示），将以 excel 表格保存的无流量检测模板中的规则导入到模板（如图 5-91 所示）。

图 5-90 无流量检测模板导入规则按钮

点击<导入>按钮，在选择 excel 文件对话框中选择需要导入的文件，点击<导入 Excel>即可导入规则。

图 5-91 导入 Excel 选择文件对话框

5.4.6.6 无流量检测模板基本配置

点击策略管理的[无流量检测模板]显示列表中操作列下的<基本配置>按钮（如图 5-92 所示），将打开[无流量检测模板]基本配置页面，可以查看无流量检测模板的基本信息（如图 5-93 所示）

图 5-92 无流量检测模板基本配置

图 5-93 无流量检测模板基本配置查看页

表格 49 无流量检测模板基本配置信息说明

列名称	说明
模板名称	模板的名字
版本号	模板的版本号，每修改一次规则自动加 1
应用此模板的智能监测终端	应用此模板的智能监测终端列表
创建时间	模板的创建时间
备注	备注附加信息，可以选填

5.4.6.7 无流量检测模板规则配置

无流量检测规则的管理是无流量检测模板管理的核心，所有模板都依赖于具体的每条规则。

5.4.6.7.1 查看无流量检测规则

进入[规则配置]页面后，显示的是无流量检测规则。(如图 5-94 所示)

图 5-94 无流量检测规则查看页

点击<返回>按钮，将返回到[无流量检测模板列表显示]页面。

5.4.6.7.2 添加无流量检测规则

进入[规则配置]页面后，点击右侧的<添加>按钮（如图 5-95 所示），将在规则的最下方自动添加一行新的无流量检测规则(如图 5-96 所示)

图 5-95 无流量检测规则添加按钮

图 5-96 无流量检测规则添加项

表格 50 无流量检测规则字段说明

列名称	说明	
源 IP	网络连接发起请求的 IP 地址，点分十进制格式	
目的 IP	网络连接的目的 IP 地址，点分十进制格式	
目的端口	服务器监听的端口，范围为 0 到 65535	
传输层协议	传输层协议，可选 TCP 或者 UDP	
无流量时间	检测配置规则的无流量时间，范围为 5 秒到 86400 秒	
删除	删除指定规则	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到模板信息列表显示页面
	返回	忽略所有的修改，返回到模板信息列表显示页面

5.4.6.7.3 修改无流量检测规则

进入[无流量检测规则配置]页面，就可以更改某条规则的源 IP、目的 IP、目的端口、传输层协议和无流量时间，修改后点击<保存>按钮即可。

5.4.6.7.4 删除无流量检测规则

进入[无流量检测规则配置]页面后，直接点击某条规则最右侧的<删除>按钮，可以删除对应的规则。(如图 5-97 所示)

图 5-97 无流量检测规则删除按钮

5.4.6.8 删除无流量检测模板

点击策略管理的[无流量检测模板]信息显示列表中操作列下的<删除>按钮，可以把不再使用的无流量检测模板删除。正在被使用的模板无法删除。(如图 5-98 所示)

图 5-98 无流量检测模板删除按钮

5.4.6.9 检索无流量检测模板

在策略管理的[无流量检测模板]信息显示列表面中，可以根据条件对无流量检测模板进行检索。(如图 5-99 所示)

图 5-99 检索无流量检测模板

5.5 日志管理

5.5.1 功能介绍

日志管理能够将系统发生的事件或报文审计产生的日志等存入缓冲区或定向发送到日志接收服务器上。通过对日志内容的分析和归档，管理员能够检查网络的安全漏洞，了解什么时候有什么人试图违背安全策略的行为。此外，实时的日志记录还可以用来检测正在进行的入侵。

5.5.2 工业协议白名单告警

工业协议白名单告警是流经智能监测终端的报文违反了智能监测终端上的工业协议白名单规则产生的，只有智能监测终端处于运行模式时才有可能产生此日志。

5.5.2.1 日志列表

点击左侧导航栏的[日志管理/工业协议白名单告警](如图 5-100 所示)，进入[工业协议白名单告警]的列表页面（如图 5-101 所示）。

图 5-100 工业协议白名单告警菜单

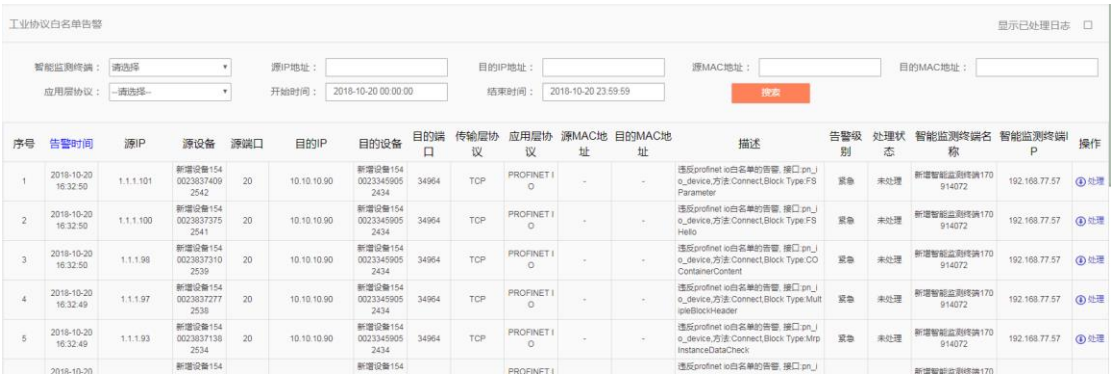


图 5-101 工业协议白名单告警列表页

此处可以查看到白名单告警所有日志的信息，含义如下：

表格 51 白名单告警日志显示说明

列名称	说明
告警时间	发生告警的时间
源 IP	发起数据请求的 IP 地址，点分十进制格式
源设备	系统根据源 IP 自动生成一个源设备名称，支持自定义源设备名称
源端口	发起数据请求的机器所使用的端口
目的 IP	请求数据的目的 IP 地址，点分十进制格式

目的设备	系统根据目的 IP 自动生成一个目的设备名称，支持自定义目的设备名称	
目的端口	请求的目的机器所使用的端口	
传输层协议	报文使用的传输层的协议类型	
应用层协议	具体的应用协议类型	
源 MAC 地址	发起数据请求的 MAC 地址	
目的 MAC 地址	请求数据的目的 MAC 地址	
描述	告警的描述信息	
告警级别	告警可能造成的损害级别，级别说明请参考 5.6.2 告警级别说明	
智能监测终端名称	由系统生成或用户命名的便于记忆的智能监测终端的名字	
智能监测终端 IP	智能监测终端分配到的 IP 地址，点分十进制格式	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选[工业协议白名单告警]白名单告警列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。(如图 5-102 所示)

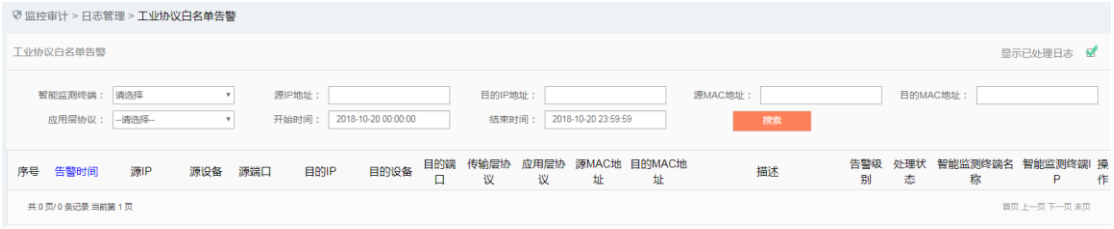


图 5-102 显示已处理的白名单告警列表页

5.5.2.2 处理日志

点击[工业协议白名单告警]显示列表中操作列下的<处理>按钮，将显示(如图 5-103 所示) [工业协议白名单告警信息]的处理页面。

图 5-103 工业协议白名单告警处理页

5.5.2.2.1 关闭日志

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[工业协议白名单告警日志]页的列表中默认将不再看到此条日志。

也可以不选择“关闭”，只填写处理意见。

5.5.2.2.2 加入基线

对于误报的工业协议白名单告警，可以点击<加入基线>，将告警信息一键加入产生该告警的白名单模板中，一键加入白名单后，类似的告警将不再产生。

5.5.2.2.3 导出报文

当智能监测终端配置中勾选了保存告警报文的白名单告警时，该智能监测终端产生的白名单告警报文将可以被下载。点击<导出报文>将自动将报文保存到执行操作的电脑中。

5.5.2.3 检索日志

在[工业协议白名单告警]的列表页面中，可以根据条件对告警进行检索。(如图 5-104 所示)

图 5-104 检索白名单告警

5.5.3 工业协议规约检测告警

工业协议规约检测告警是流经智能监测终端的报文违反了工业协议规约产生的。

5.5.3.1 日志列表

点击左侧导航栏的[日志管理/工业协议规约检测告警](如图 5-105 所示)，进入[工业协议规约检测告警]的列表页面（如图 5-106 所示）。

图 5-105 工业协议规约检测告警菜单

图 5-106 工业协议规约检测告警列表页

此处可以查看到工业协议规约告警所有日志的信息，含义如下：

表格 52 工业协议规约检测告警显示说明

列名称	说明	
告警时间	发生告警的时间	
源 IP	发起数据请求的 IP 地址，点分十进制格式	
源设备	系统根据源 IP 自动生成一个源设备名称，支持自定义源设备名称	
源端口	发起数据请求的机器所使用的端口	
目的 IP	请求数据的目的 IP 地址，点分十进制格式	
目的设备	系统根据目的 IP 自动生成一个目的设备名称，支持自定义目的设备名称	
目的端口	请求的目的机器所使用的端口	
源 MAC 地址	发起数据请求的 MAC 地址	
目的 MAC 地址	请求数据的目的 MAC 地址	
传输层协议	报文使用的传输层的协议类型	
应用层协议	具体的应用协议类型	
告警级别	告警可能造成的损害级别	
智能监测终端名称	由系统生成或用户命名的便于记忆的智能监测终端的名字	
智能监测终端 IP	智能监测终端分配到的 IP 地址，点分十进制格式	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选[工业协议规约检测告警]规约检测告警列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。(如图 5-107 所示)

图 5-107 显示已处理的规约告警列表页

5.5.3.2 处理日志

点击[工业协议规约检测告警]显示列表中操作列下的<处理>按钮，将显示(如图 5-108 所示) [工业协议规约检测告警信息]的处理页面：

图 5-108 工业协议规约告警处理页

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[工业协议规约检测告警]页的列表中默认将不再看到此条日志。

也可以不选择“关闭”，只填写处理意见。

5.5.3.3 检索日志

在[工业协议规约检测告警]的列表页面中，可以根据条件对告警进行检索。(如图 5-109 所示)

图 5-109 检索工业协议规约检测告警

5.5.4 无流量告警

当某些用户指定的流量从某个时刻开始不再产生流量时，智能监测终端将产生无流量报警。

5.5.4.1 日志列表

点击左侧导航栏的[日志管理/无流量告警](如图 5-110 所示)，进入[无流量告警]的列表页面（如图 5-111 所示）。

图 5-110 无流量告警菜单

图 5-111 无流量告警列表页

此处可以查看到无流量告警所有日志的信息，含义如下：

表格 53 无流量告警日志显示说明

列名称	说明	
源 IP	发起数据请求的 IP 地址，点分十进制格式	
目的 IP	请求数据的目的 IP 地址，点分十进制格式	
目的端口	请求的目的机器所使用的端口	
协议	报文使用的传输层的协议类型	
告警级别	告警可能造成的损害级别	
无流量开始时间	从该时刻起，指定的规则无流量	
无流量结束时间	从该时刻起，指定的规则重新开始流量，当没有结束时间时，显示为“-”	
智能监测终端名称	由系统生成或用户命名的便于记忆的智能监测终端的名字	
智能监测终端 IP	智能监测终端分配到的 IP 地址，点分十进制格式	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选[无流量告警]白名单告警列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。(如图 5-112 所示)

图 5-112 显示已处理的无流量告警列表页

5.5.4.2 处理日志

点击[无流量告警]显示列表中操作列下的<处理>按钮，将显示(如图 5-113 所示) [无流量告警信息]的处理页面：

图 5-113 无流量告警处理页

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[无流量告警]页的列表中默认将不再看到此条日志。

也可以不选择“关闭”，只填写处理意见。

5.5.4.3 检索日志

在[无流量告警]的列表页面中，可以根据条件对告警进行检索。(如图 5-114 所示)

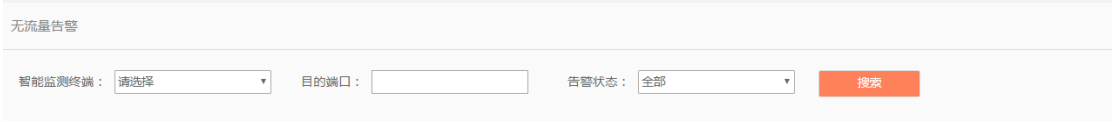


图 5-114 检索无流量告警

5.5.5 关键事件告警

当流经智能监测终端的流量产生关键事件时，智能监测终端将产生告警。

系统内的关键事件定义如下：

1.所有工业协议的写操作；

2.S7 协议的请求下载、开始下载、下载完成、请求上载、开始上载、上载完成、CPU 启动、CPU 停止。

5.5.5.1 日志列表

点击左侧导航栏的[日志管理/关键事件告警](如图 5-115 所示)，进入[关键事件告警]的列表页面（如图 5-116 所示）。

图 5-115 关键事件告警菜单

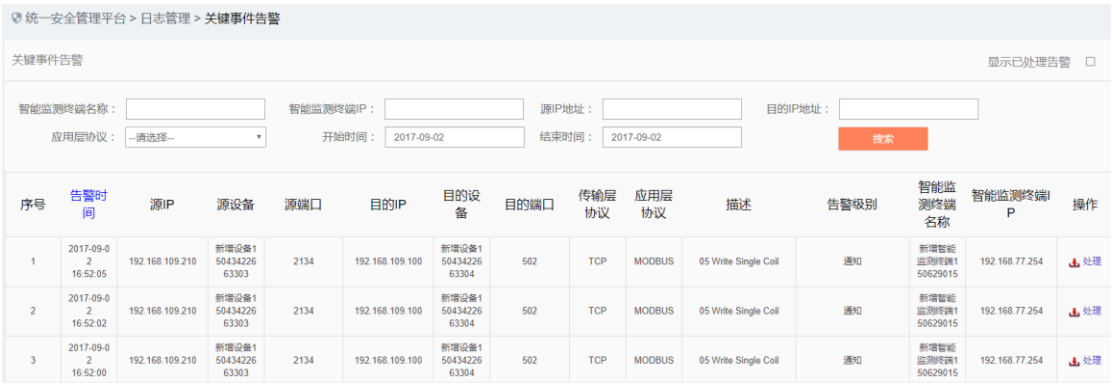


图 5-116 关键事件告警列表页

此处可以查看到关键事件告警所有日志的信息，含义如下：

表格 54 关键事件告警日志显示说明

列名称	说明	
告警时间	产生告警的时间	
源 IP	发起数据请求的 IP 地址，点分十进制格式	
源端口	发起数据请求的端口	
源设备	系统根据源 IP 自动生成一个源设备名称，支持自定义源设备名称	
目的 IP	请求数据的目的 IP 地址，点分十进制格式	
目的设备	系统根据目的 IP 自动生成一个目的设备名称，支持自定义目的设备名称	
目的端口	请求的目的机器所使用的端口	
传输层协议	报文使用的传输层的协议类型	
应用层协议	应用层使用的协议	
描述	对于告警的描述	
源 MAC 地址	发起数据请求的 MAC 地址	
目的 MAC 地址	请求数据的目的 MAC 地址	
告警级别	告警可能造成的损害级别	
智能监测终端名称	由系统生成或用户命名的便于记忆的智能监测终端的名字	
智能监测终端 IP	智能监测终端分配到的 IP 地址，点分十进制格式	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选[关键事件告警]关键事件告警列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。(如图 5-117 所示)

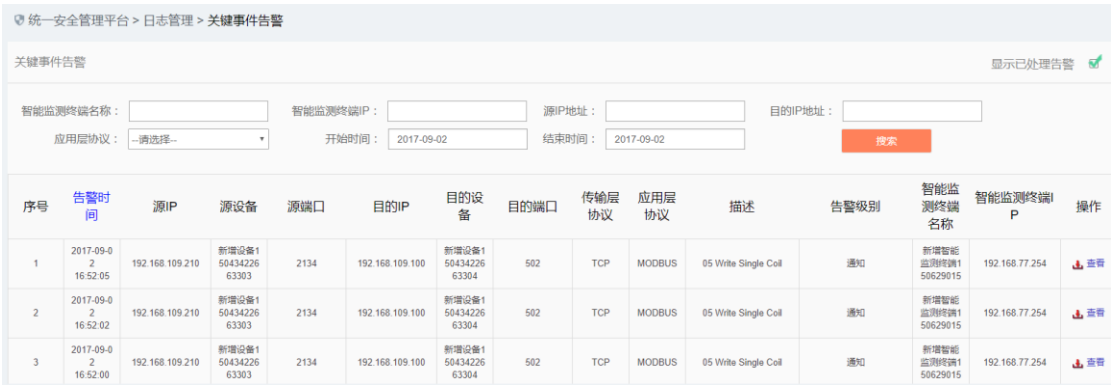


图 5-117 显示已处理的关键事件告警列表页

5.5.5.2 处理日志

点击[关键事件告警]显示列表中操作列下的<处理>按钮，将显示(如图 5-118 所示) [关键事件告警信息]的处理页面：

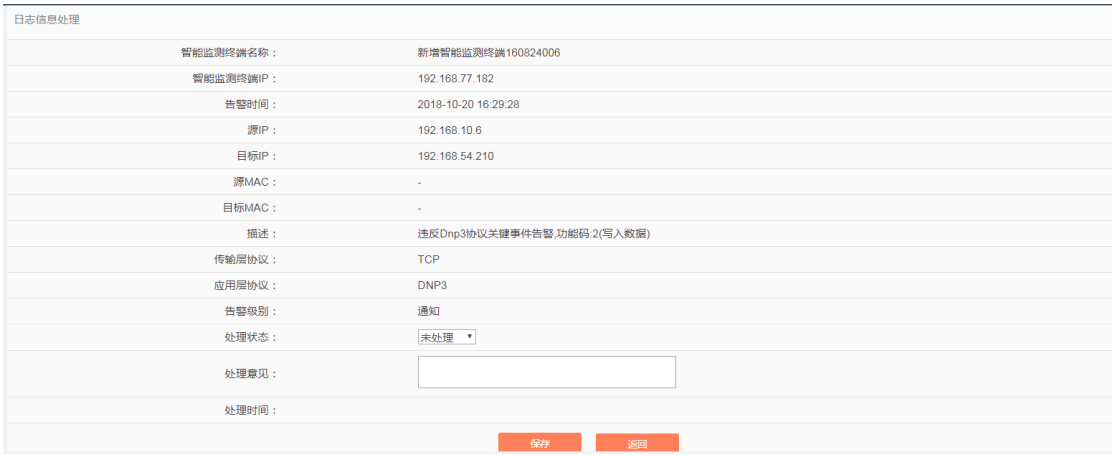


图 5-118 关键事件告警处理页

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[关键事件告警]页的列表中默认将不再看到此条日志。

也可以不选择“关闭”，只填写处理意见。

5.5.5.3 检索日志

在[关键事件告警]的列表页面中，可以根据条件对告警进行检索。(如图 5-119 所示)

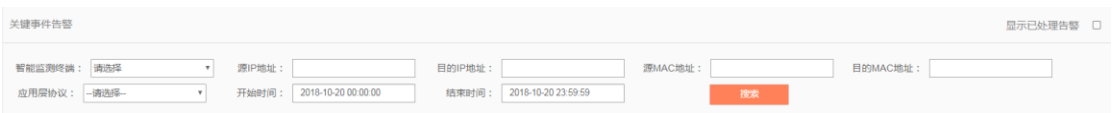


图 5-119 检索关键事件告警

5.5.6 用户自定义告警

用户自定义告警是流经智能监测终端的报文符合用户配置的规则产生的。

5.5.6.1 日志列表

点击左侧导航栏的[日志管理/用户自定义告警](如图 5-120 所示)，进入[用户自定义告警]的列表页面（如图 5-121 所示）。

图 5-120 用户自定义菜单

图 5-121 用户自定义告警列表页

此处可以查看到用户自定义告警所有日志的信息，含义如下：

表格 55 用户自定义告警日志显示说明

列名称	说明
告警时间	发生告警的时间
源 IP	发起数据请求的 IP 地址，点分十进制格式
源端口	发起数据请求的机器所使用的端口
源设备	系统根据源 IP 自动生成一个源设备名称，支持自定义源设备名称

目的 IP	请求数据的目的 IP 地址，点分十进制格式	
目的设备	系统根据目的 IP 自动生成一个目的设备名称，支持自定义目的设备名称	
目的端口	请求的目的机器所使用的端口	
传输层协议	报文使用的传输层的协议类型	
应用层协议	具体的应用类型	
源 MAC 地址	请求数据的目的 MAC 地址	
目的 MAC 地址	请求数据的目的 MAC 地址	
告警级别	告警可能造成的损害级别	
智能监测终端名称	由系统生成或用户命名的便于记忆的智能监测终端的名字	
智能监测终端 IP	智能监测终端分配到的 IP 地址，点分十进制格式	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选[用户自定义告警]用户自定义告警列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。(如图 5-122 所示)

图 5-122 显示已处理的用户自定义告警列表页

5.5.6.2 处理日志

点击[用户自定义告警]显示列表中操作列下的<处理>按钮，将显示(如图 5-123 所示) [用户自定义告

警信息]的处理页面：

图 5-123 用户自定义告警处理页

5.5.6.2.1 关闭日志

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[用户自定义告警日志]页的列表中默认将不再看到此条日志。

也可以不选择“关闭”，只填写处理意见。

5.5.6.2.2 导出报文

当智能监测终端配置中勾选了保存告警报文的用户自定义告警时，该智能监测终端产生的用户自定义告警报文将可以被下载。点击<导出报文>将自动将报文保存到执行操作的电脑中。

5.5.6.3 检索日志

在[用户自定义告警]的列表页面中，可以根据条件对告警进行检索。(如图 5-124 所示)

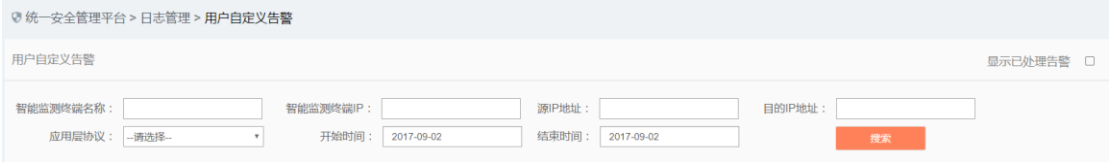


图 5-124 检索用户自定义告警

5.5.7 工业协议审计日志

所有流经智能监测终端的工业协议都将产生工业协议审计日志。

5.5.7.1 日志列表

点击左侧导航栏的[日志管理/工业协议审计日志](如图 5-125 所示)，进入[工业协议审计日志]的列表页面（如图 5-126 所示）。

图 5-125 工业协议审计日志菜单

图 5-126 工业协议审计日志列表页

工业协议审计日志分 OPC 协议，Modbus 协议，S7 协议，DNP3 协议和 IEC104 协议，本文以 OPC 为例，其他两个协议类似。可以查看到 OPC 的工业协议审计日志所有日志的信息，含义如下：

表格 56 工业协议审计日志显示说明

列名称	说明
告警时间	产生日志的时间
源 IP	发起数据请求的 IP 地址，点分十进制格式
源端口	发起数据请求的端口
源设备	系统根据源 IP 自动生成一个源设备名称，支持自定义源设备名称
目的 IP	请求数据的目的 IP 地址，点分十进制格式

目的设备	系统根据目的 IP 自动生成一个目的设备名称，支持自定义目的设备名称	
目的端口	请求的目的机器所使用的端口	
协议	报文使用的传输层的协议类型	
操作接口	OPC 使用的操作接口	
操作方法	OPC 使用的操作方法	
智能监测终端名称	由系统生成或用户命名的便于记忆的智能监测终端的名字	
智能监测终端 IP	智能监测终端分配到的 IP 地址，点分十进制格式	
操作	仅显示当前流	对日志进行过滤，只显示该日志所属的流的所有日志
	导出日志	将日志导出到本地电脑中

5.5.7.2 检索日志

在[工业协议审计日志]的列表页面中，可以根据条件对日志进行检索。(如图 5-127 所示)

图 5-127 检索工业协议审计日志

5.5.8 网络会话审计日志

所有流经智能监测终端的流量都将产生网络会话审计日志。

5.5.8.1 日志列表

点击左侧导航栏的[日志管理/网络会话审计日志](如图 5-128 所示)，进入[网络会话审计日志]的列表页面（如图 5-129 所示）。

图 5-128 网络会话审计日志菜单

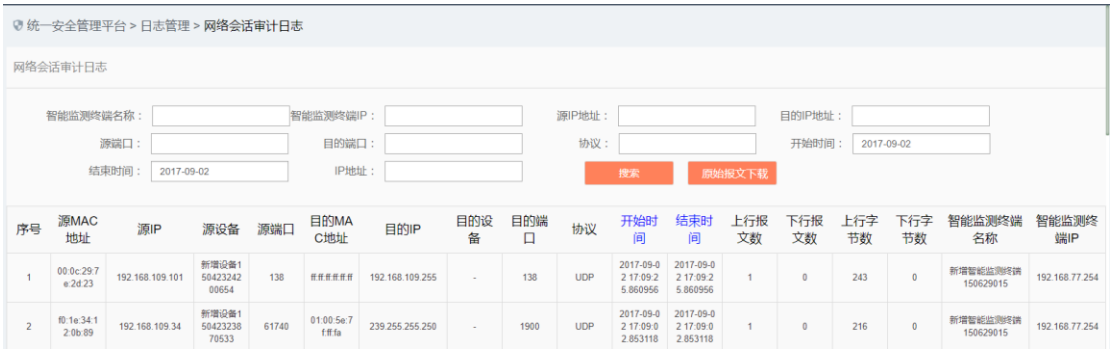


图 5-129 网络会话审计日志列表页

可以查看到网络会话审计日志所有日志的信息，含义如下：

表格 57 工业协议审计日志显示说明

列名称	说明
源 MAC 地址	发起数据请求的 MAC 地址，以“:”分隔符格式
源 IP	发起数据请求的 IP 地址，点分十进制格式
源设备	系统根据源 IP 自动生成一个源设备名称，支持自定义源设备名称
源端口	发起数据请求的端口
目的 MAC 地址	请求数据的目的 MAC 地址，以“:”分隔符格式
目的 IP	请求数据的目的 IP 地址，点分十进制格式
目的设备	系统根据目的 IP 自动生成一个目的设备名称，支持自定义目的设备名称
目的端口	请求的目的机器所使用的端口

协议	报文使用的传输层的协议类型	
开始时间	产生网络会话的起始时间	
结束时间	网络会话终止时的时间	
上行报文数	从客户端到服务器的传输的报文数	
下行报文数	从服务器到客户端的传输的报文数	
上行字节数	从客户端到服务器的传输的字节数	
下行字节数	从服务器到客户端的传输的字节数	
智能监测终端名称	由系统生成或用户命名的便于记忆的智能监测终端的名字	
智能监测终端 IP	智能监测终端分配到的 IP 地址，点分十进制格式	
操作	导出日志	将日志导出到本地电脑

5.5.8.2 检索日志

在[网络会话审计日志]的列表页面中，可以根据条件对日志进行检索。(如图 5-130 所示)

图 5-130 检索网络会话审计日志

5.5.8.3 原始报文下载

在[网络会话审计日志]的列表页面中，可以下载智能终端留存的流经它的报文。（如图）

图 5-131 原始报文下载按钮

点击<原始报文下载>按钮，将进入报文下载页面，如图 5-132 所示。点击<下载>按钮，则对应的报文将被下载到本地电脑。

图 5-132 原始报文下载页面

5.5.9 智能监测终端运行日志

智能监测终端运行日志是记录智能监测终端运行状态的日志。

5.5.9.1 日志列表

点击左侧导航栏的[日志管理/智能监测终端运行日志](如图 5-133 所示)，进入[智能监测终端运行日志]的列表页面（如图 5-134 所示）。

图 5-133 智能监测终端运行日志菜单

图 5-134 智能监测终端运行日志列表页

此处可以查看到所有智能监测终端运行日志的信息，含义如下：

表格 58 智能监测终端运行日志显示说明

列名称	说明
智能监测终端名称	由系统生成或用户命名的便于记忆的智能监测终端的名字
智能监测终端 ID	有系统生成的智能监测终端 ID
智能监测终端 IP	智能监测终端分配到的 IP 地址，点分十进制格式
内容	日志详细描述信息
操作时间	日志产生时的时间

5.5.9.2 检索日志

在[智能监测终端运行日志]的列表页面中，可以根据条件对日志进行检索。(如图 5-135 所示)

图 5-135 检索智能监测终端运行日志

5.5.10 异常流量日志

每次异常流量产生时都要产生一条异常流量日志。

5. 5. 10. 1 日志列表

点击[日志管理/异常流量日志]，(如图 5-136 所示)将打开异常流量日志页面。(如图 5-137 所示)

图 5-136 异常流量日志菜单

图 5-137 异常流量日志页面

此处可以查看到异常流量所有日志的信息，含义如下：

表格 59 白名单告警日志显示说明

列名称	说明	
设备名称	发生异常流量的设备名称	
设备 IP	发生异常流量的设备 IP	
异常类型	为流出流量或者流入流量	
上行基线值	异常流量基线配置中的上行流量数	
上行实际值	实际设备产生上行的流量数	
下行基线值	异常流量基线配置中的下行流量数	
下行实际值	实际设备产生下行的流量数	
异常时间段	产生异常流量的时间	
已确认	异常流量是否已被处理确认	
操作	处理	对异常流量做进一步处理

5.5.10.2 处理日志

点击[异常流量]显示列表中操作列下的<处理>按钮，将显示(如图 5-138 所示) [异常流量]的处理页面：

图 5-138 异常流量处理

勾选进行确认右侧勾选框，来进行确认日志操作。(如图 5-139 所示)

图 5-139 确认异常流量

5.6 系统配置

5.6.1 告警级别设置

登录管理平台后，点击[系统设置/告警级别设置]，(如图 5-140 所示)将打开告警级别设置页面。(如图 5-141 所示)

图 5-140 选择告警级别设置

图 5-141 选择要设置的告警级别

5.6.2 告警级别说明

表格 60 告警级别表

序号	级别	级别说明
1	紧急	已造成系统不可用
2	警示	需要管理员立刻注意的信息
3	关键	可能已经影响到设备功能使用的信息
4	错误	已经造成设备功能不可使用的信息，如非法操作失败
5	警告	可能会影响到设备功能正常使用的信息
6	通知	设备正常产生的事件信息，包括由管理员触发的配置改变等信息
7	信息	关于系统操作的普通信息
8	调试	用于系统调试目的的详细信息

5.7 网络连接

5.7.1 功能介绍

实时与历史显示经过终端设备的网络流量。

5.7.2 网络连接基线配置

5.7.2.1 功能介绍

经过终端设备的网络连接，符合配置网络连接基线规则，网络连接图画绿线，不符合则画红线。

5.7.2.2 规则配置

点击[网络连接/网络连接基线配置]，(如图 5-142 所示)将打开网络连接基线配置页面。(如图 5-143 所示)

图 5-142 网络连接基线配置菜单

图 5-143 网络连接基线配置页面

进入[网络连接基线配置]页面后，点击右侧的<添加>按钮（如图 5-144 所示），将在列表的最下方自动添加一行新的规则(如图 5-145 所示)

图 5-144 规则添加按钮

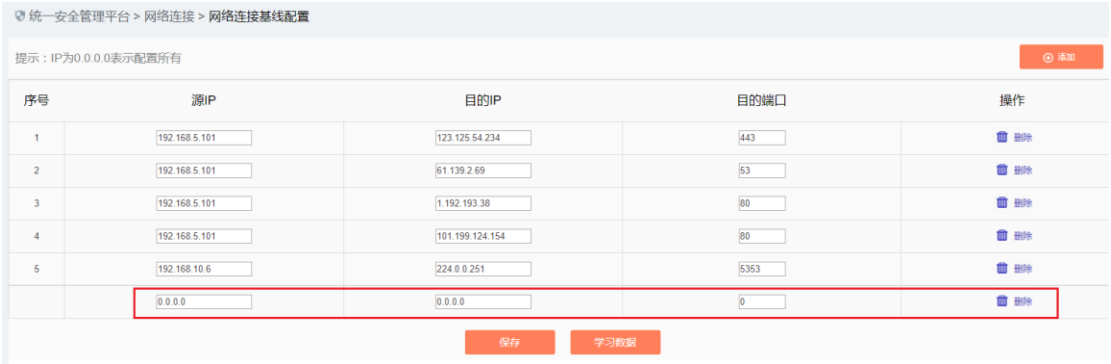


图 5-145 规则添加页

表格 61 规则字段说明

列名称	说明
源 IP	发起数据请求的 IP 地址，点分十进制格式
目的 IP	请求数据的目的 IP 地址，点分十进制格式
目的端口	目的端口，范围为 0 到 65535
删除	删除所选规则
保存	所有的修改信息将被保存到数据库并生效

5.7.2.3 学习数据

进入[网络连接基线配置]页面后，(如图 5-146 所示)点击<学习数据>按钮，跳转到学习数据页面。(如图 5-147 所示)

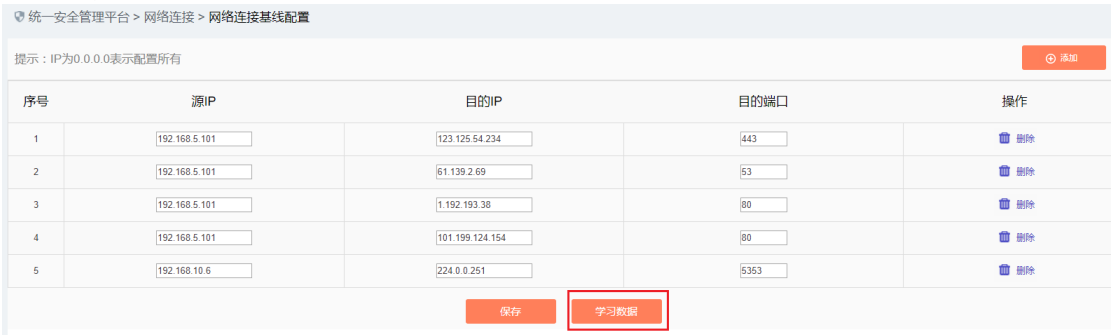


图 5-146 学习数据按钮

图 5-147 学习数据页面

通过查询条件过滤学习数据。(如图 5-148 所示)

图 5-148 学习数据搜索

选中数据后，点击<添加到网络基线>按钮，将学习数据添加到规则配置页面。(如图 5-149 所示)

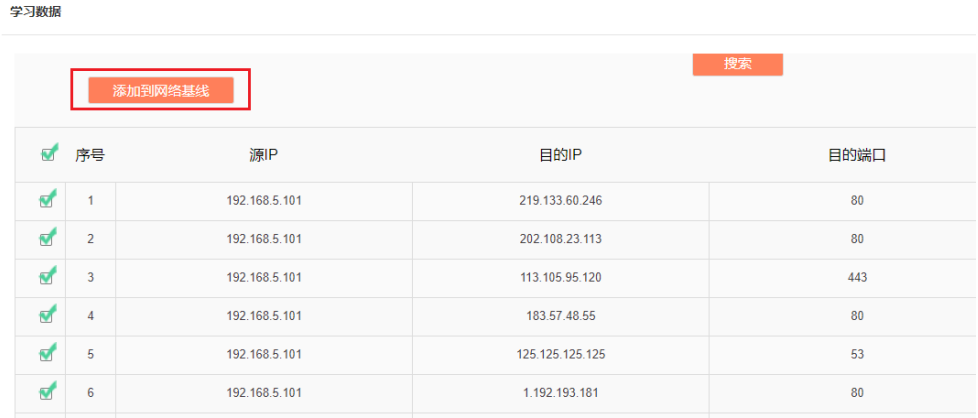


图 5-149 学习数据添加

选中数据后，点击<删除>按钮，将学习数据删除。(如图 5-150 所示)

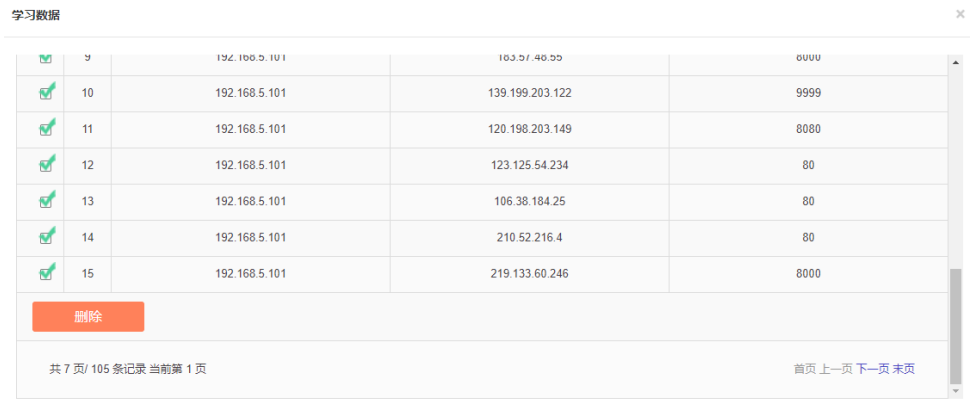


图 5-150 删除学习数据

5.7.3 网络流量基线配置

5.7.3.1 功能介绍

经过终端设备的网络连接流量，符合配置网络流量基线规则，网络连接图画绿线，不符合则画红线。

5.7.3.2 规则配置

点击[网络连接/网络流量基线配置]，(如图 5-151 所示)将打开网络流量基线配置页面。(如图 5-152 所示)

图 5-151 网络流量基线配置菜单

图 5-152 网络流量基线配置页面

进入[网络连流量线配置]页面后，点击右侧的<添加>按钮（如图 5-153 所示），将在列表的最下方自动添加一行新的规则(如图 5-154 所示)

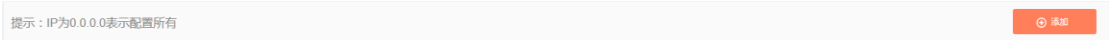


图 5-153 规则添加按钮

图 5-154 规则添加页

表格 62 规则字段说明

列名称	说明
源 IP	发起数据请求的 IP 地址，点分十进制格式
目的 IP	请求数据的目的 IP 地址，点分十进制格式
上行字节数	经过终端设备的流量上行数量。
下行字节数	经过终端设备的流量下行数量。
删除	删除所选规则
保存	所有的修改信息将被保存到数据库并生效

5.7.4 网络连接图

5.7.4.1 功能介绍

实时画出所有经过终端设备的网络连接，符合规则配置的数据画绿线，不符合的画红线。查询历史网络连接。规则与实时相同。

5.7.4.2 实时网络连接图

点击[网络连接/网络连接图]，(如图 5-155 所示)将打开网络连接图页面。(如图 5-156 所示)

图 5-155 网络连接图菜单

图 5-156 网络连接图页面

当开始时间与结束时间为空时，此时画出的网络连接图为实时连接图，可以通过其他条件进行过滤搜索。(如图 5-157 所示)

图 5-157 实时网络连接图

5.7.4.3 历史网络连接图

当开始时间与结束时间不为空时，显示的网络连接图为历史网络连接，可以通过其他条件进行过滤。(如图 5-158 所示)

图 5-158 网络历史连接图

5.8 异常流量

5.8.1 功能介绍

图形化展示所有设备的网络流量是否正常，有三种状态：(如图 5-159 所示)
1.正常状态：设备当前检查周期内流量未有异常并且已经产生的异常流量报警已全部确认
2.红色闪烁：设备当前检查周期内流量有异常，无论有没有未确认的异常流量报警
3.红色外框：设备当前检查周期内流量未有异常但已经产生的异常流量报警未全部确认

图 5-159 三种图形显示

5.8.2 基线配置

5.8.2.1 功能介绍

配置设备 5 分钟内经过的流量大小超过多少为异常流量。

5.8.2.2 规则配置

点击[异常流量/基线配置]，(图 5-160 如所示)将打开基线配置页面。(如图 5-161 所示)

图 5-160 基线配置菜单

图 5-161 基线配置页面

进入[基线配置]页面后，点击右侧的<添加>按钮（如图 5-162 所示），将在列表的最下方自动添加一行新的规则(如图 5-163 所示)

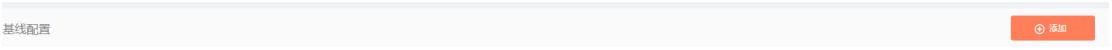


图 5-162 规则添加按钮

图 5-163 规则添加页

表格 63 规则字段说明

列名称	说明
设备	通过输入的设备 IP 自动显示对应设备名称
设备 IP	设备 IP 地址
上行字节数	经过终端设备的流量上行数量
下行字节数	经过终端设备的流量下行数量
删除	删除所选规则
保存	所有的修改信息将被保存到数据库并生效

5.8.3 异常流量监控

5.8.3.1 功能介绍

用户可以选择需要显示的设备，拖动到主界面上的设备则显示状态信息，不在主界面上的设备，不检查流量异常情况。

5.8.3.2 流量监控

点击[异常流量/异常流量监控]，(如图 5-164 所示)将打开异常流量监控页面。(如图 5-165 所示)

图 5-164 异常流量监控菜单

图 5-165 异常流量监控页面

通过设备名称或 IP 地址过滤设备列表。(如图 5-166 所示)

图 5-166 过滤功能

拖拽设备到画布，开始监控设备流量。(如图 5-167 所示)

图 5-167 监控页面

5.9 统计分析

5.9.1 网络流量报文历史统计

5.9.1.1 功能介绍

按小时与天分别对比两个设备的网络流量与报文数量。

5.9.1.2 统计查询

点击[统计分析/网络流量报文历史统计]，(如图 5-168 所示)将打开网络流量报文历史统计页面。(如图 5-169 所示)

图 5-168 网络流量报文历史统计菜单

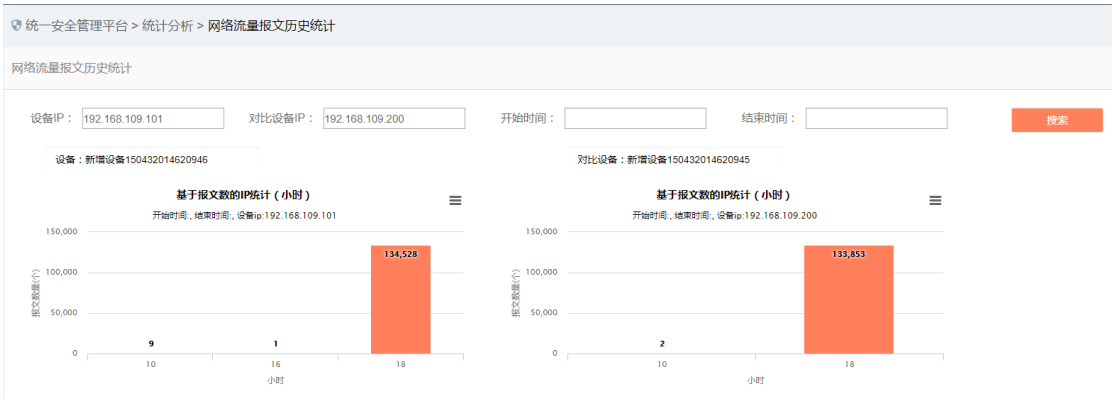


图 5-169 网络流量报文历史统计页面

输入设备 IP 与对比设备 IP，点击搜索查询结果为按小时统计当天数据，(如图 5-170 所示)输入开始时间与结束时间后，会按天统计选择时间段中的数据。(如图 5-171 所示)

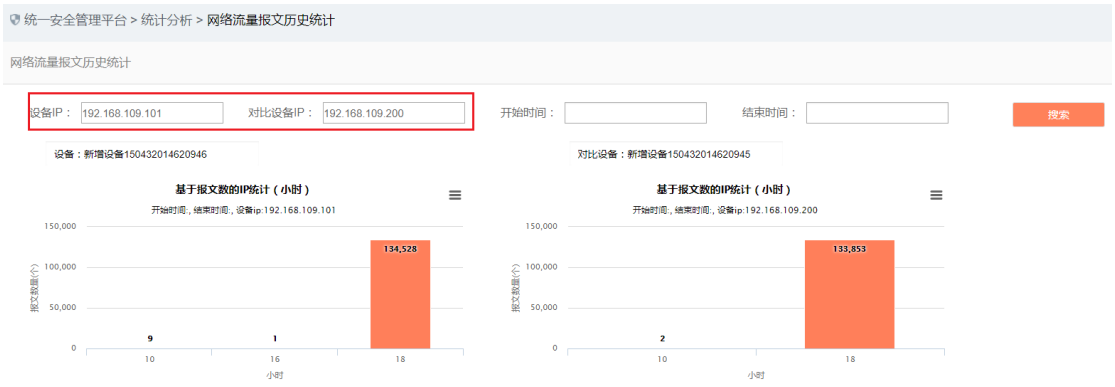


图 5-170 当天数据统计

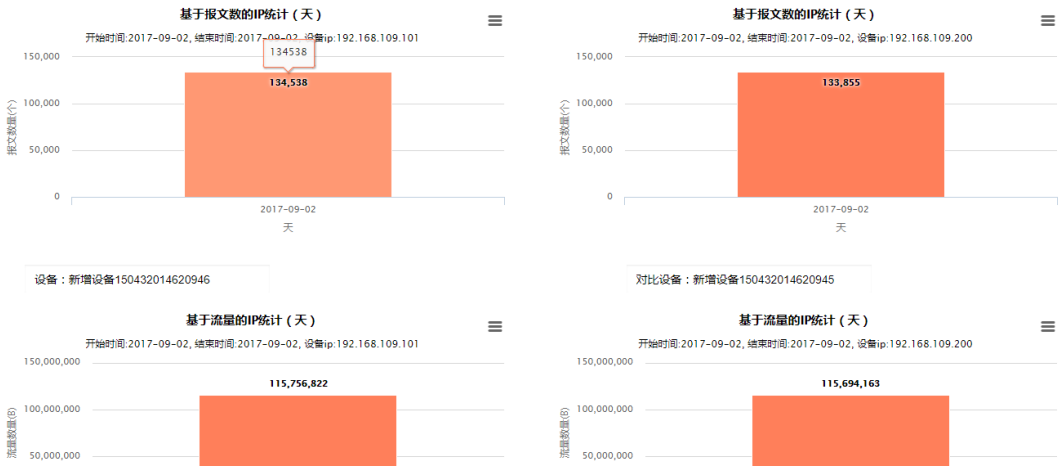


图 5-171 分天数据统计

5.9.1.3 导出统计图

点击导出 图标，导出当前统计图（如图 5-172 所示），点击<全部导出>按钮，导出页面全部统计图。（如图 5-173 所示）

图 5-172 导出单个统计图

图 5-173 导出全部统计图

5.9.2 网络实时流量

5.9.2.1 功能介绍

按 5 分钟，2 小时，每天为节点实时显示当前经过系统的实时流量。

5.9.2.2 实时流量

点击[统计分析/网络实时流量]，(如图 5-174 所示)将打开网络实时流量页面。(如图 5-175 所示)

图 5-174 网络实时流量菜单

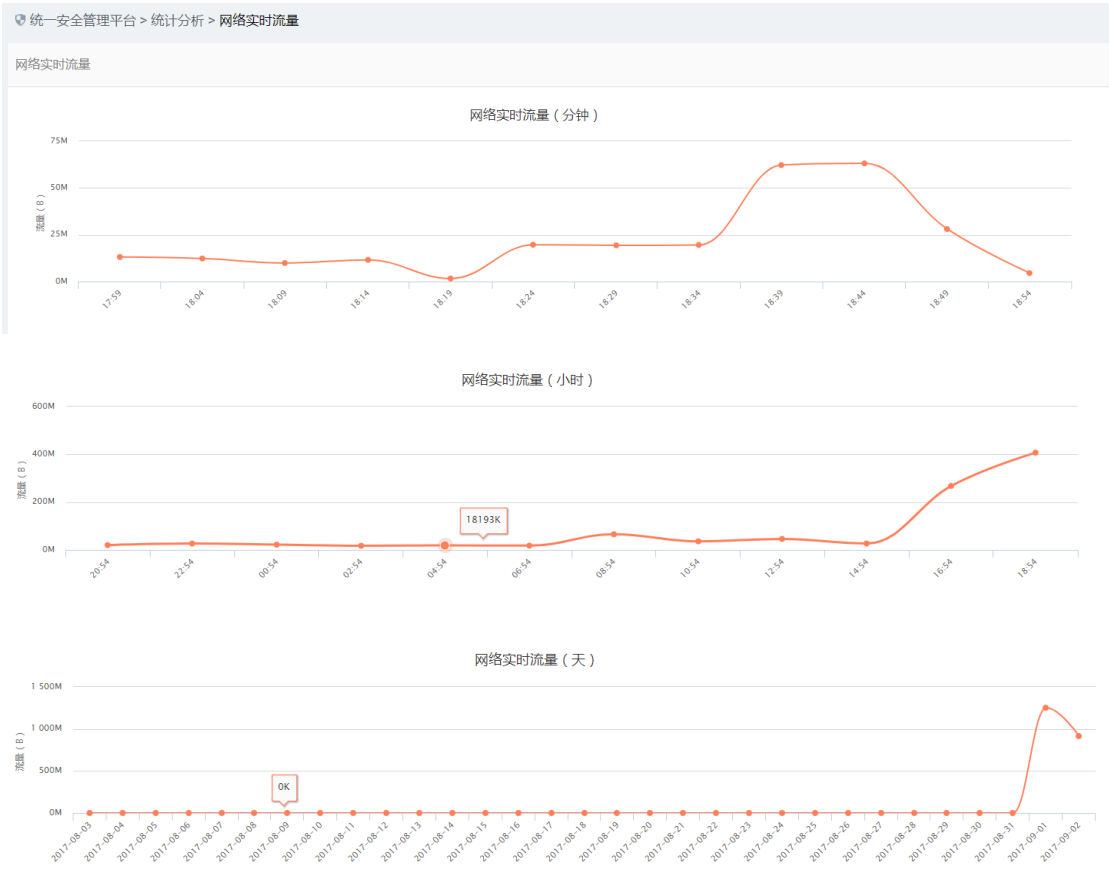


图 5-175 网络实时流量页面

进入页面后，分钟图为 5 分钟刷新一次，小时图为 2 小时刷新一次，天图为 24 小时刷新一次。

5.9.3 报文数统计

5.9.3.1 功能介绍

基于 IP 统计对应经过的报文数。

5.9.3.2 查询报文数

点击[统计分析/报文数统计]，(如图 5-176 所示)将打开报文数统计页面。(如图 5-177 所示)

图 5-176 报文数统计菜单

图 5-177 报文数统计页面

通过查询条件查询指定时间内的报文数，可以通过接收与发送进行过滤。(如图 5-178 所示)

图 5-178 查询报文数

5.9.3.3 导出统计图

点击导出 图标，导出当前统计图。（如图 5-179 所示）

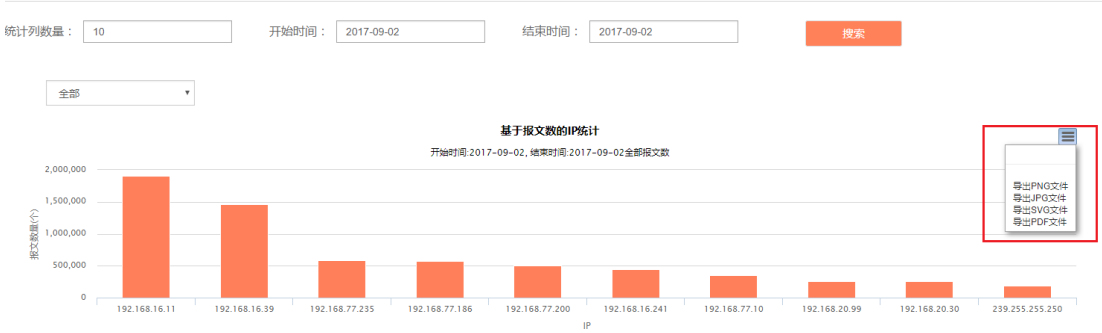


图 5-179 导出统计图

5.9.4 流量统计

5.9.4.1 功能介绍

基于 IP 统计对应经过的流量。

5.9.4.2 查询流量

点击[统计分析/流量统计]，(如图 5-180 所示)将打开流量统计页面。(如图 5-181 所示)

图 5-180 流量统计菜单

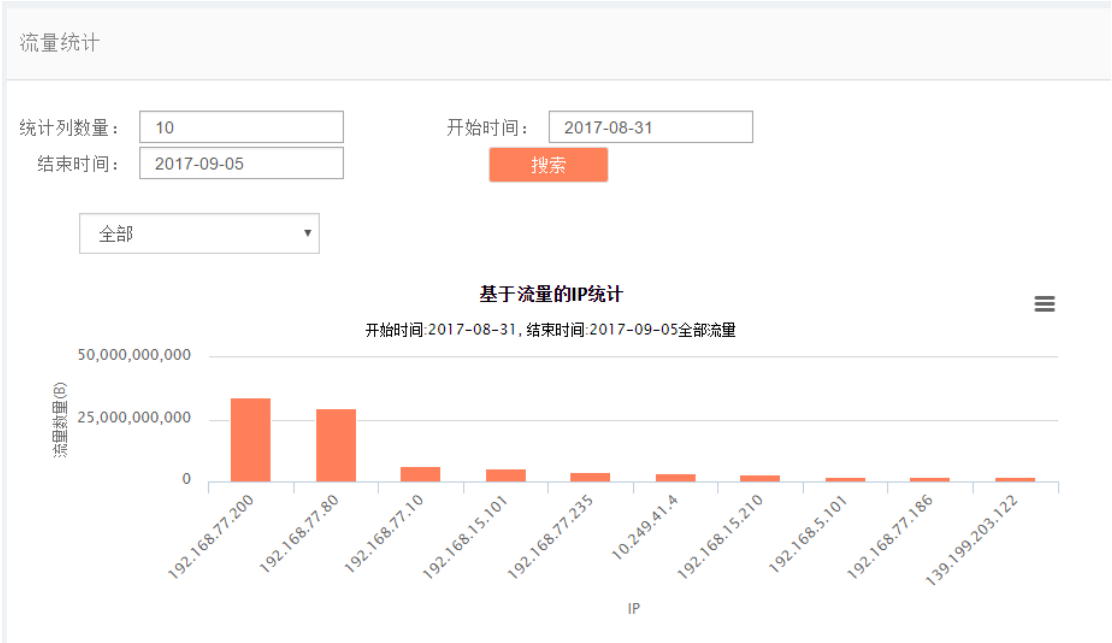


图 5-181 流量统计页面

通过查询条件查询指定时间内的流量，可以通过接收与发送进行过滤。(如图 5-182 所示)

图 5-182 查询流量

5.9.4.3 导出统计图

点击导出 图标，导出当前统计图。（如图 5-183 所示）

图 5-183 导出当前统计图

5.9.5 端口统计

5.9.5.1 功能介绍

基于 IP 统计对应经过的流量，基于端口统计对应经过的流量。

5.9.5.2 查询端口

点击[统计分析/端口统计]，(如图 5-184 所示)将打开端口统计页面，如下图：(如图 5-185 所示)

图 5-184 端口统计菜单

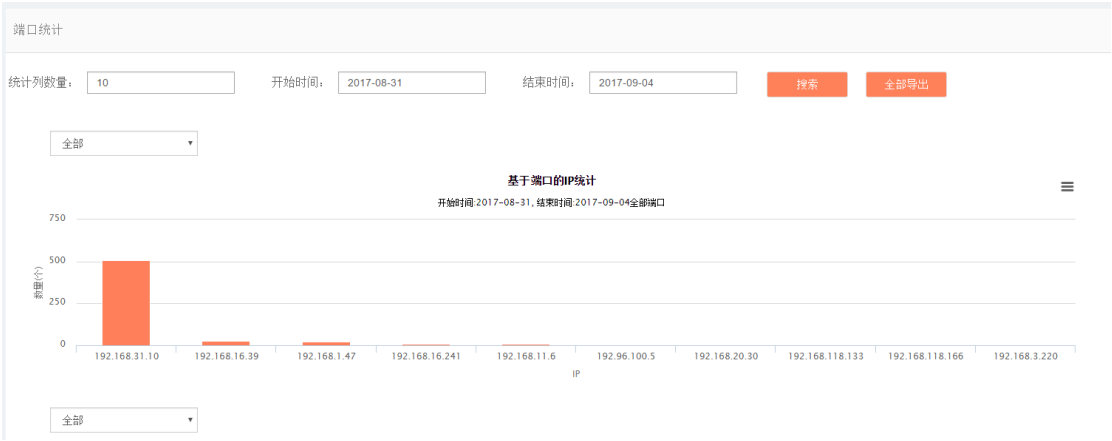


图 5-185 端口统计页面

通过查询条件查询指定时间内的流量，可以通过接收与发送进行过滤。(如图 5-186 所示)

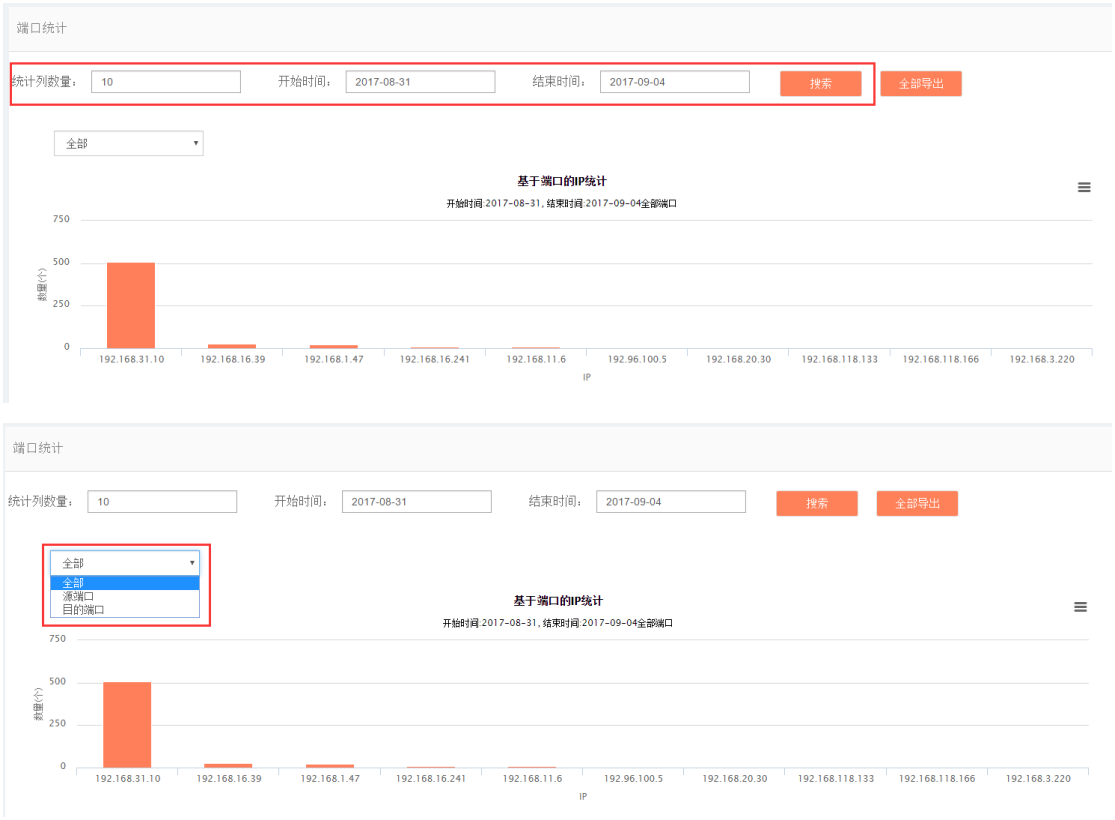


图 5-186 查询流量

5.9.5.3 导出统计图

点击导出 ☰ 图标，导出当前统计图（如图 5-187 所示），点击<全部导出>按钮，导出页面全部统计图。（如图 5-188 所示）

图 5-187 导出统计图

图 5-188 导出全部统计图

5.9.6 告警事件统计

5.9.6.1. 功能介绍

根据告警事件的数量生成直观的图像，供审计人员进行分析。(如图 5-189 所示)

图 5-189 菜单

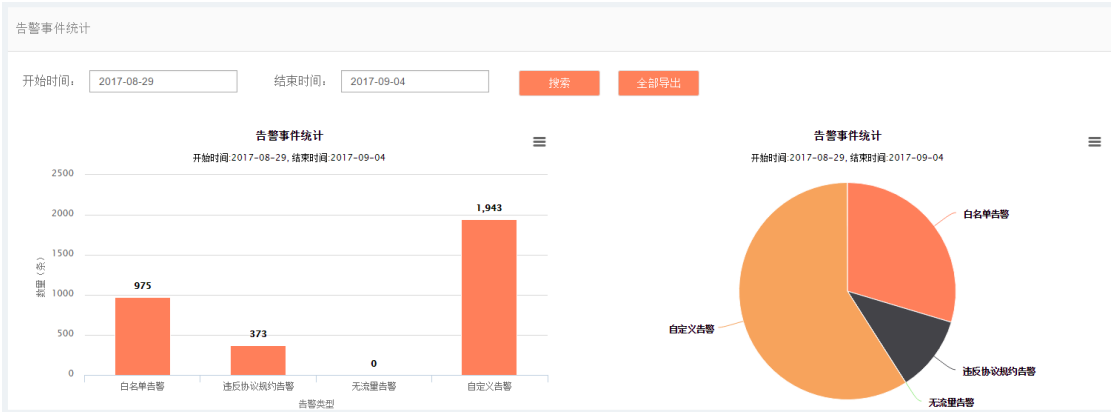


图 5-190 统计页面

5.9.6.2. 查询数据

通过查询条件查询指定时间内的数据。（如图 5-191 所示）

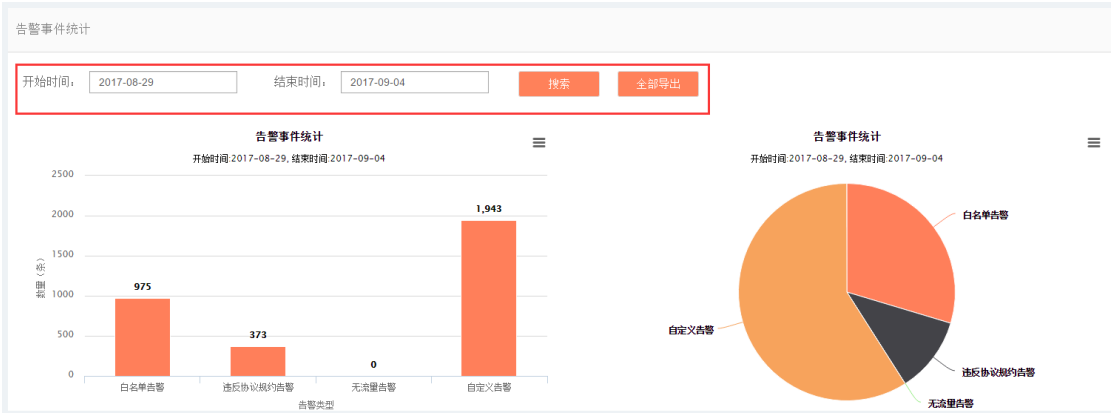


图 5-191 查询数据

5.9.6.3. 导出统计图

点击导出 图标，导出当前统计图（如图 5-192 所示），点击<全部导出>按钮，导出页面全部统计图。（如图 5-193 所示）

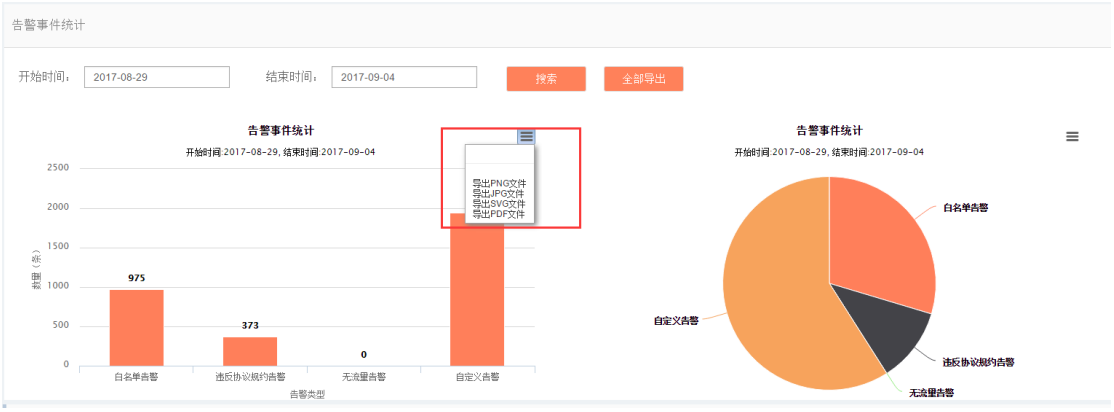


图 5-192 导出统计图

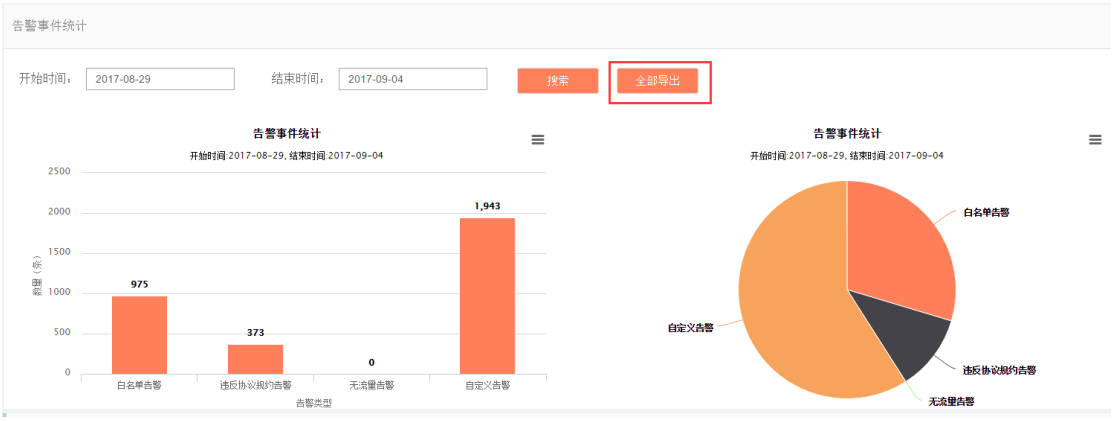


图 5-193 导出全部统计图

6. 系统配置

6.1 系统总览

使用审计管理员成功登录管理平台后，在上方菜单栏中找到[系统设置]，点击按钮，然后在左侧导航栏找到[系统总览/系统总览]，点击菜单(如图 6-1 所示)，将在右侧的展示页面中看到系统操作日志的页面（如图 6-2 所示）。

图 6-1 系统总览菜单栏

图 6- 2 系统总览页面

6. 1. 1 系统总览展示

系统总览可以实时查看工业防火墙，主机卫士客户端，监控审计终端设备在线状态(如图 6- 3 所示)，告警数量(如图 6- 4 所示)与告警趋势(如图 6- 5 所示)。

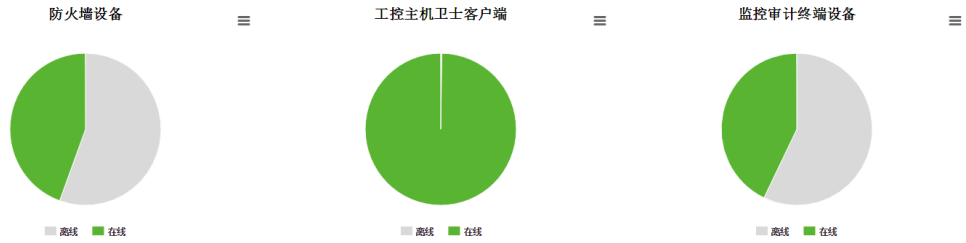


图 6- 3 设备在线状态

图 6- 4 管理平台性能监控

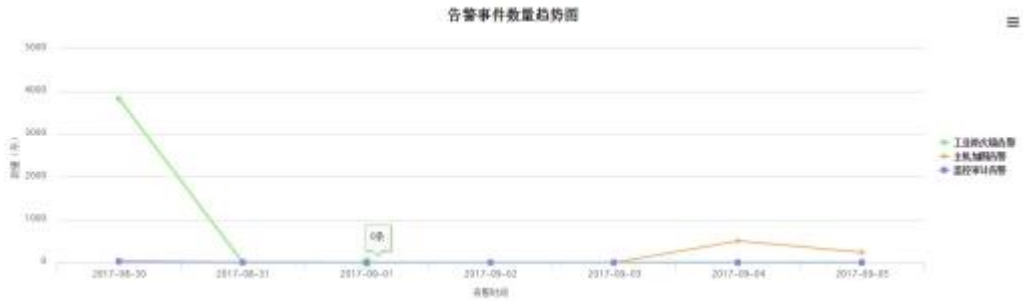


图 6- 5 告警趋势

6.2 系统操作日志

使用审计管理员成功登录管理平台后，在上方菜单栏中找到[系统设置]，点击按钮，然后在左侧导航栏找到[系统操作日志/系统操作日志]，点击菜单(如图 6- 6 所示)，将在右侧的展示页面中看到系统操作日志的页面（如图 6- 7 所示）。

图 6- 6 系统操作日志菜单栏

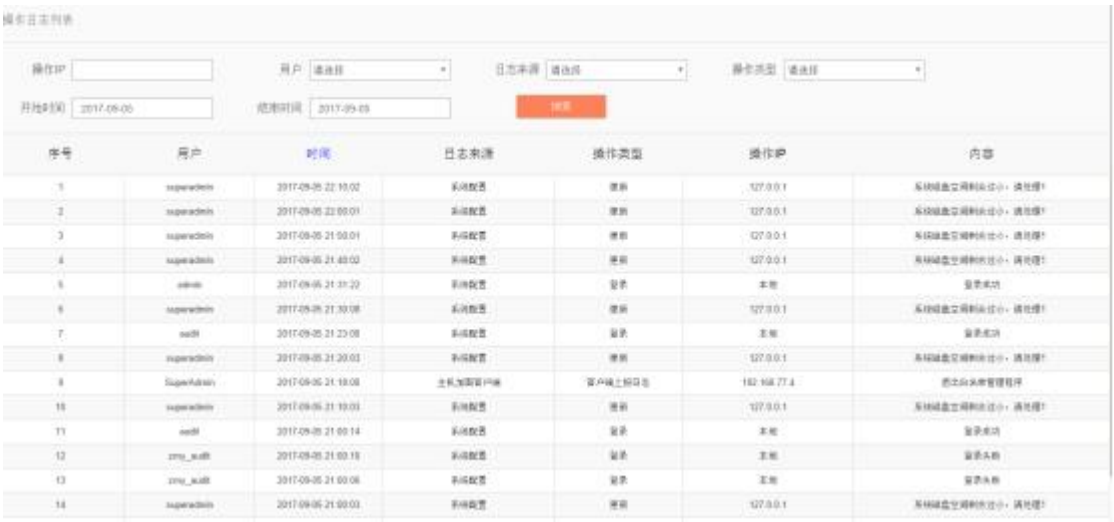


图 6- 7 系统操作日志页面

6.2.1检索日志

在[系统操作日志]的列表页面中，可以根据条件对日志进行检索。(如图 6- 8 所示)

图 6- 8 检索条件

6.3 硬盘容量日志

使用审计管理员成功登录管理平台后，在上方菜单栏中找到[系统设置]，点击按钮，然后在左侧导航栏找到[硬盘容量日志/硬盘容量日志]，点击菜单(如图 6- 9 所示)，将在右侧的展示页面中看到硬盘容量日志的页面（如图 6- 10 所示）。

图 6- 9 硬盘容量日志菜单栏

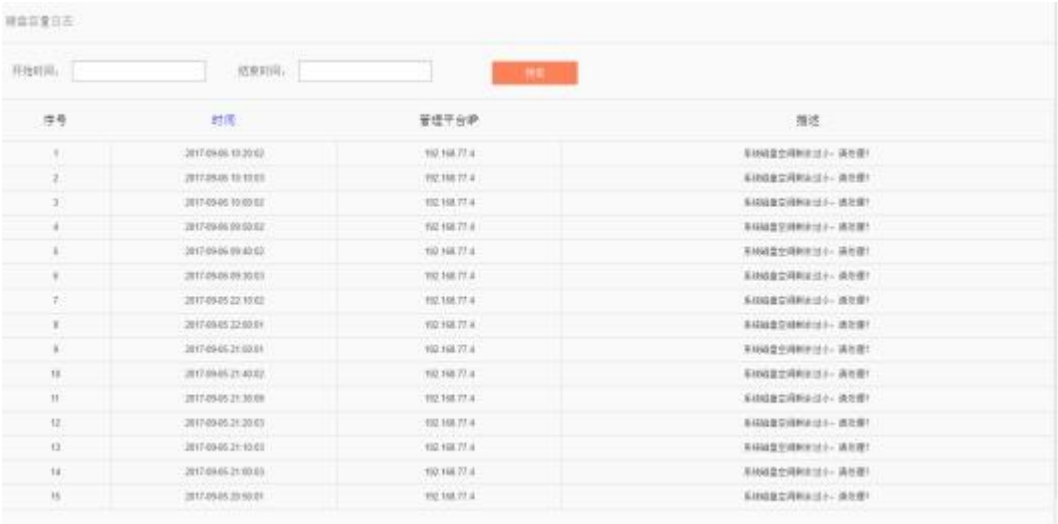


图 6- 10 硬盘容量日志页面

6.3.1检索日志

在[硬盘容量日志]的列表页面中，可以根据条件对日志进行检索。(如图 6- 11 所示)

图 6- 11 检索条件

6.4 系统重启日志

使用审计管理员成功登录管理平台后，在上方菜单栏中找到[系统设置]，点击按钮，然后在左侧导航栏找到[系统重启日志/硬盘容量日志]，点击菜单(如图 6- 12 所示)，将在右侧的展示页面中看到系统重启日志的页面（如图 6- 13 所示）。

图 6- 12 系统重启日志菜单栏

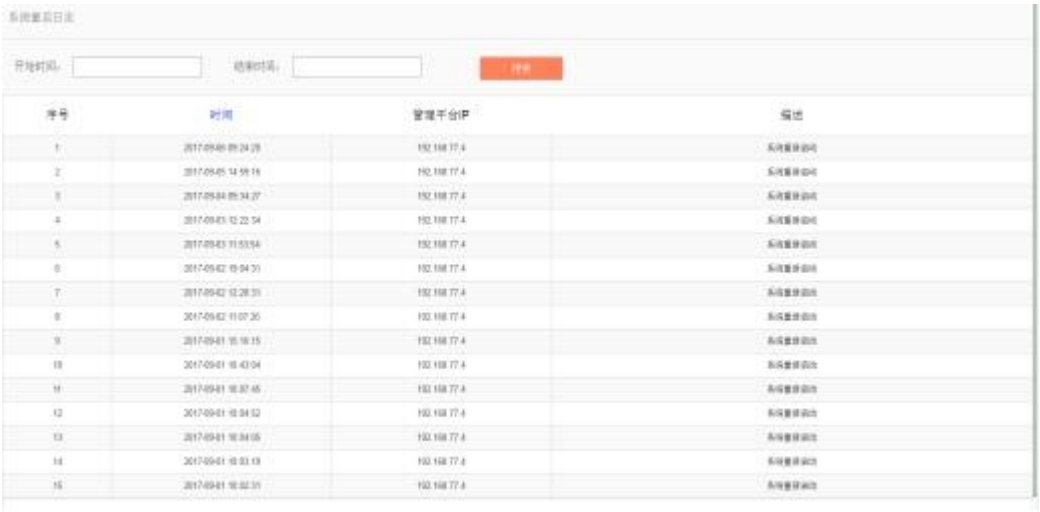


图 6- 13 系统重启日志页面

6.4.1检索日志

在[系统重启日志]的列表页面中，可以根据条件对日志进行检索。(如图 6- 14 所示)

图 6- 14 检索条件

6.5 数据库备份日志

使用审计管理员成功登录管理平台后，在上方菜单栏中找到[系统设置]，点击按钮，然后在左侧导航栏找到[数据库备份日志/数据库备份日志]，点击菜单(如图 6- 15 所示)，将在右侧的展示页面中看到数据库备份日志的页面（如图 6- 16 所示）。

图 6- 15 数据库备份日志菜单栏

图 6- 16 数据库备份日志页面

6.5.1 检索日志

在[数据库备份日志]的列表页面中，可以根据条件对日志进行检索。(如图 6- 17 所示)

图 6- 17 检索条件

6.6 系统配置

6.6.1 密码管理

配置管理员登录，在左侧导航栏找到[系统配置/密码管理] (如图 6- 18 所示)。

图 6- 18 密码管理菜单栏

审计管理员登录，在左侧导航栏找到[系统配置/密码管理] (如图 6- 19 所示)。

图 6- 19 密码管理菜单栏

系统操作员登录，在左侧导航栏找到[系统配置/密码管理] (如图 6- 20 所示)。

图 6- 20 密码管理菜单栏

系统审核员登录，在左侧导航栏找到[系统配置/密码管理] (如图 6- 21 所示)。

图 6- 21 密码管理菜单栏

点击菜单，将在右侧的展示页面中看到密码管理的页面（如图 6- 22 所示）。

图 6- 22 密码管理页面

6.6.1.1 重置密码

重置当前登录用户密码，填写密码后点击<保存>按钮。

6.6.2用户管理

管理平台支持分权分级管理，目前支持 4 种级别的用户：系统操作员、配置管理员和审计管理员，系统审核员。系统操作员可以创建不同的用户，分配不同的角色，配置管理员可以进行配置的管理，审计管理员可以查看所有日志，系统审核员审核系统操作员创建的用户。

6.6.2.1 信息查看

系统操作员登录，点击左侧导航栏的[系统配置/用户管理](如图 6- 23 所示)，进入[用户管理]的页面（如图 6- 24 所示）。

图 6- 23 用户管理菜单

图 6- 24 用户管理列表页

6.6.2.2 添加用户

系统操作员登录，点击 [系统配置/用户管理] 用户列表标签右侧的<添加>按钮，(如图 6- 25 所示)将弹出用户添加页面(如图 6- 26 所示)，添加用户后需要系统审核员审核通过，用户才会生效。

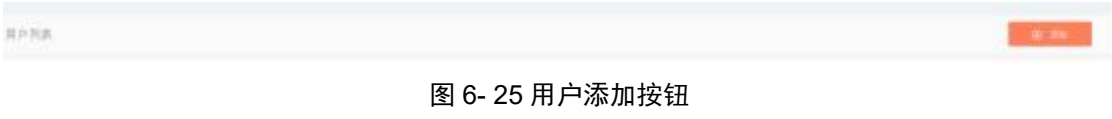


图 6- 25 用户添加按钮

图 6- 26 用户添加页

表格 64 用户添加信息说明

列名称	说明
用户名	给用户定义一个容易理解、记忆且有含义的名字

用户密码	用户的登录密码，密码必须是大小写字母，数字，特殊字符(#@!~%^&*)组合，且长度不小于 8 位，不大于 16 位	
确认密码	再次输入用户的登录密码	
用户权限	用户访问级别；配置管理员和审计管理员中选一种	
备注	可选填，附加说明信息	
操作	保存	所有的信息提交给系统审核员，同时返回到用户列表显示页面
	返回	忽略所有的修改，返回到用户列表显示页面

6.6.2.3 修改密码

系统操作员登录，点击[用户管理]用户列表中操作列下的<修改密码>按钮，将打开[用户管理]用户基本信息修改页面，可以修改用户的基本信息（如图 6- 27 所示）

图 6- 27 修改密码页

6.6.2.4 修改备注

系统操作员登录，点击[用户管理]用户列表中操作列下的<修改备注>按钮，将打开[用户管理]用户基本信息修改页面，可以修改用户的基本信息（如图 6- 28 所示）

图 6- 28 修改备注页

6.6.2.5 删除用户

系统操作员登录，点击[用户管理]用户列表操作列下的<删除>按钮，然后点击<保存>按钮可以把不再使用的用户进行删除。

6.6.3用户审核

系统操作员添加用户后，可以在用户审核查看用户审核进度，系统审核员可以审核用户。

6.6.3.1 信息查看

系统操作员登录，点击左侧导航栏的[系统配置/用户审核](如图 6- 29 所示)，进入[用户审核]的页面（如图 6- 30 所示）。

图 6- 29 用户审核菜单

图 6- 30 用户审核列表页

系统审核员登录，点击左侧导航栏的[系统配置/用户审核](如图 6- 31 所示)，进入[用户审核]的页面（如图 6- 32 所示）。

图 6- 31 用户审核菜单

图 6- 32 用户审核列表页

6.6.3.2 处理用户

系统审核员登录，点击<处理>按钮，跳转到处理页面(如图 6- 33 所示)，选择审核是否通过，点击<保存>，保存处理结果。

图 6- 33 用户审核处理页

6.6.4数据库存储周期配置

用于配置管理平台数据库存储与备份周期，配置管理员登录，点击左侧导航栏的[系统配置/数据库存储周期配置](如图 6- 34 所示)，进入[数据库存储周期配置]的页面（如图 6- 35 所示）。

图 6- 34 数据库存储周期配置

图 6- 35 数据库存储周期配置页面

6.6.4.1 保存操作

按照提示填写信息，先点击<修改>按钮，然后点击<保存>按钮，下发配置。(如图 6- 36 所示)

图 6- 36 保存配置

6.6.5协议参数配置

6.6.5.1 功能介绍

白名单配置模板中往往需要使用自定义功能码等可添加字段，目前 CIP 下拉菜单中通过自定义项进行添加，只支持添加功能。在工业防火墙学习过程中可能学习到用户使用的新的自定义字段，这时需要重新修改字段描述，同时用户自定义的字段也有删除的需求。为此，工业防火墙通过专门的协议参数配置页面，方便用户管理某些工业协议特有的功能特性。

6.6.5.2 协议参数配置

配置管理员登录，点击左侧导航栏的[白名单管理/协议参数配置](如图 6- 37 所示)，进入[协议参数配置]的页面（如图 6- 38 所示）。

图 6- 37 选择协议参数配置

图 6- 38 协议参数配置页面

此处用户可以针对 CIP 协议进行如下三种参数的配置：

- 对象配置
- 服务配置
- PCCC 配置

下面分别说明这三种配置每个字段的含义。

表格 65CIP 协议对象配置字段说明

列名称	说明	
对象号	CIP 协议定义的标准对象以及在工业现场用户自定义的对象，以十六进制值显示	
描述	对象所代表的具体意义	
操作	修改	修改用户自定义对象的描述信息，CIP 标准对象的描述信息无法修改
	删除	删除用户自定义的对象，CIP 标准对象无法删除

表格 66CIP 协议服务配置字段说明

列名称	说明	
服务号	CIP 协议中提供的标准服务以及在工业现场用户自定义的服务，以十六进制值显示	
描述	服务的具体意义	
操作	修改	修改用户自定义的 CIP 服务的描述信息，CIP 标准服务的描述信息无法修改
	删除	删除用户自定义的 CIP 服务，CIP 标准服务无法删除

表格 67CIP 协议 PCCC 配置字段说明

列名称	说明	
CMD	CIP 协议内嵌的 PCCC 格式的报文中的 CMD 号，以十六进制值显示	
FNC	CIP 协议内嵌的 PCCC 格式的报文中的 FNC 号，以十六进制值显示	
描述	PCCC 中的 CMD 和 FNC 的组合唯一确定的方法描述	
操作	修改	重新定义 CMD 和 FNC 的组合唯一确定的方法，PCCC 定义的标准方法无法修改
	删除	删除用户自定义的由 CMD 和 FNC 的组合唯一确定的方法，PCCC 定义的标准方法无法删除

6.6.5.3 CIP 配置添加

点击每个配置列表右侧的<添加>按钮，（如图 6-39 所示）的对象配置中的<添加>按钮，将打开对象配置添加页，（如图 6-40 所示）。

图 6- 39 CIP 协议对象配置添加按钮

图 6- 40 CIP 协议对象配置添加页面

对象号及描述的含义请参考 6.6.5.2 协议参数配置。

点击<保存>将把增加的自定义对象保存到后台，然后跳转到协议参数配置页面。

点击<返回>将不保存编辑的自定义对象，直接返回到协议参数配置页面。

6.6.5.4 CIP 配置修改

请参考 6.6.5.2 协议参数配置操作列下的修改说明。

6.6.5.5 CIP 配置删除

请参考 6.6.5.2 协议参数配置操作列下的修改说明。

6.6.5.6 CIP EPATH 配置添加

点击 tab 页标签跳转到 CIP EPATH 配置页面，（如图 6-41）点<添加>按钮添加一条规则。

图 6-41 CIP EPATH 配置页面

6.6.5.7 CIP EPATH 配置删除

点击<删除>按钮删除一条规则，（如图 6-42）。

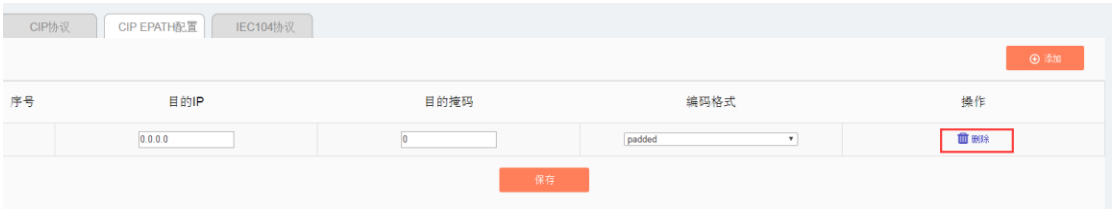


图 6-42 CIP EPATH 删除操作

6.6.5.8 CIP EPATH 配置保存

点击<保存>按钮保存所有规则并下发到设备，（如图 6-43）。

图 6-43 CIP EPATH 保存操作

6.6.5.9 IEC104 配置

点击 tab 页标签跳转到 IEC104 配置页面(如图 6-44)。

图 6-44 IEC104 配置页面

6.6.5.10 IEC104 配置保存

点击<保存>按钮，保存页面配置并下发(如图 6- 45)。

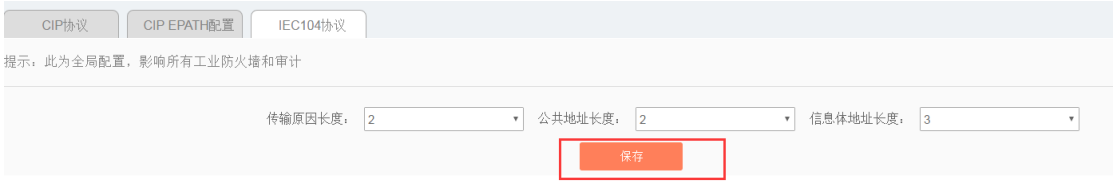


图 6- 45 IEC104 保存

6.6.6解码引擎配置

解码引擎的配置可以让用户方便快捷的定义支持的私有协议，通过上传引擎配置文件实现协议深度解析，并自动生成规则配置界面，自动产生告警。

点击左侧导航栏的[系统配置/解码引擎配置](如图 6- 46 所示)，进入[解码引擎配置]的页面（如图 6- 47 所示）。

图 6- 46 解码引擎配置菜单

图 6- 47 解码引擎配置页面

6.6.6.1 上传解码引擎配置文件

点击“选择文件”选择预置好的解码引擎配置文件，点击“上传”，即可完成对私有协议的配置，（如图 6- 48 所示）。

图 6- 48 协议解码引擎上传配置文件

6.6.6.2 协议解析信息展示

解析成功后，管平台对解析到的私有协议信息进行展示，（如图 6- 49 所示）。展示字段，包括协议 ID，协议名称，版本号，上传时间，和使用状态。

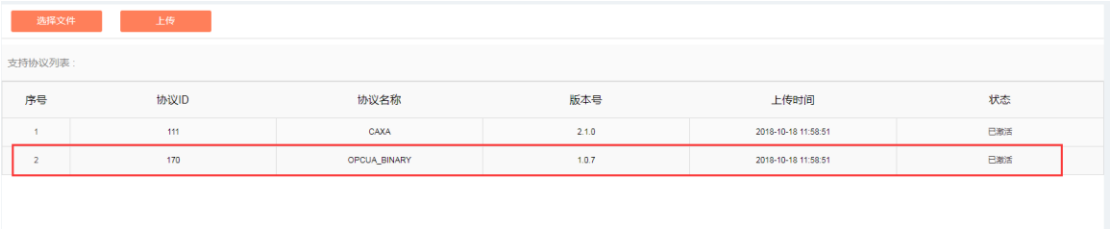


图 6- 49 协议解析信息展示

6.6.7 授权管理

用于授权[工业防火墙]，[主机加固]，[监控审计]功能，点击左侧导航栏的[系统配置/授权管理](如图 6- 50 所示)，进入[授权管理]的页面（如图 6- 51 所示）。

图 6- 50 授权管理菜单栏

图 6- 51 授权管理页面

6.6.7.1 开始上传

点击<请选择授权文件>按钮，选择授权文件，点击<开始上传>，执行授权。

6.6.8 设备管理

设备管理是管理平台重要的功能之一，它提供了友好的界面来帮助用户进行设备的管理。

配置管理员登录，点击左侧导航栏的[系统配置/设备管理](如图 6- 52 所示)，进入[设备管理]的页面（如图 6- 53 所示）。

图 6- 52 设备管理菜单

图 6- 53 设备管理页

此处可以查看到系统内所有设备的信息，含义如下：

表格 68 设备列表显示说明

列名称	说明	
设备名称	便于记忆的设备的名称	
IP 地址 MAC 地址 CPU（%） 内存（%） 流量	设备分配到的 IP 地址，点分十进制格式 设备分配到的 MAC 地址 SNMP 协议获取当前 IP 地址的设备 cpu 使用率信息 SNMP 协议获取当前 IP 地址的设备内存使用率信息 SNMP 协议获取当前 IP 地址的设备产生的总流量	
设备类型	设备的用途分类，如工作站、控制器等 SNMP 配置　　配置 SNMP 协议信息	
操作	查看	查看设备的更多详细信息
	修改	对设备的信息进行修改和设置
	删除	删除设备

6.6.8.1 SNMP 配置

点击[设备管理]显示列表中操作列下的<SNMP 配置>按钮，将显示如下图所示的 SNMP 配置详细信息。(如图 6- 54 所示)

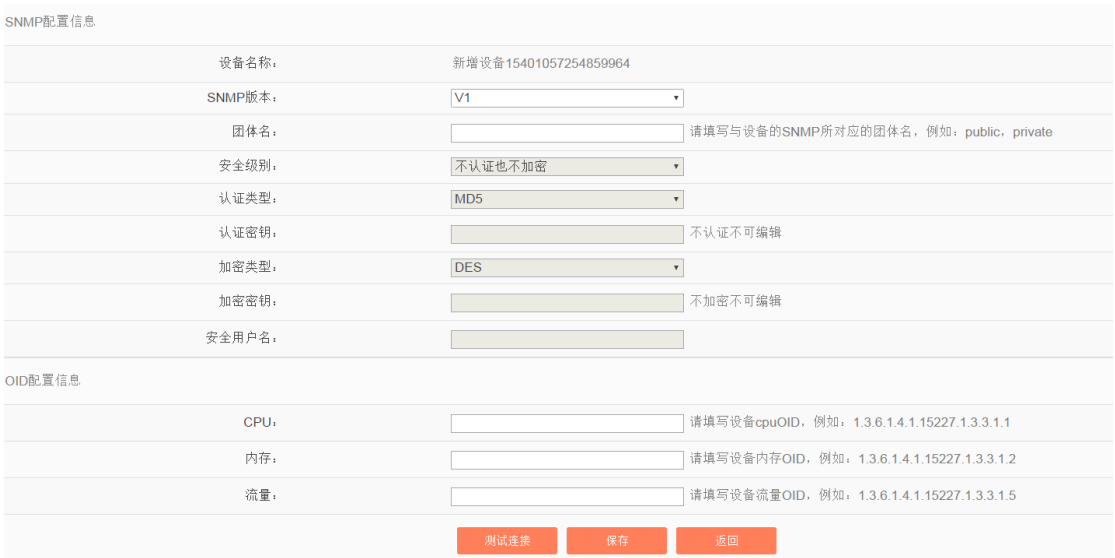


图 6- 54 SNMP 配置

6.6.8.2 查看设备

点击[设备管理]显示列表中操作列下的<查看>按钮，将显示如下图所示的设备的详细信息。(如图 6-55 所示)

图 6- 55 设备信息查看页

点击<返回>按钮，将返回到[设备管理]页面。

6.6.8.3 添加设备

点击 [设备管理]设备列表标签右侧的<添加>按钮，将弹出设备添加页面。(如图 6- 56 所示)

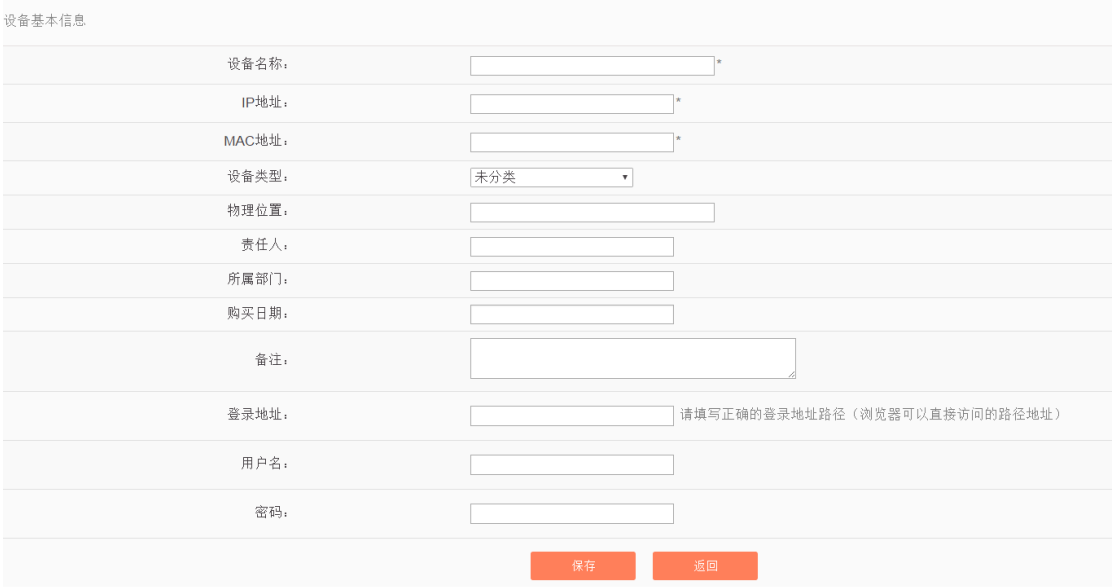


图 6- 56 设备添加页

表格 69 设备添加信息说明

列名称	说明
设备名称	便于记忆的设备的名称
IP 地址	设备分配到的 IP 地址，点分十进制格式
设备类型	设备的用途分类，如工作站、控制器
备注	可选填，附加说明信息

6.6.8.4 修改设备

点击[设备管理]设备列表中操作列下的<修改>按钮，将打开[设备基本信息]修改页面，可以修改设备的基本信息（如图 6- 57 所示）

图 6- 57 设备基本信息修改页

6.6.8.5 删除设备

点击[设备管理] 设备列表操作列下的<删除>按钮，把不再使用的设备进行删除。

6.6.8.6 检索设备

在[设备管理]设备显示列表页面中，可以根据条件对设备进行检索。(如图 6- 58 所示)

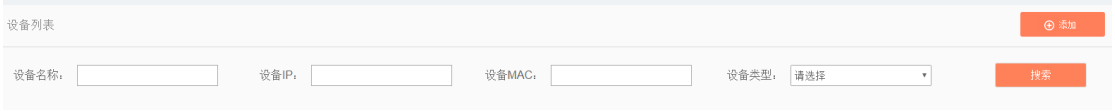


图 6- 58 检索设备

6.6.9 可信主机

访问管理平台的主机是有限制的。在初始情况下，任意一台机器只要可以连接到管理平台服务器都可以访问管理平台。如果一旦配置了可信主机，那么将只有被加入可信主机的机器才可以访问管理平台。管理平台服务器所在的主机，无论何种情况下都可以访问管理平台。

6.6.9.1 信息查看

配置管理员登录，点击左侧导航栏的[系统配置/可信主机](如图 6- 59 所示)，进入[可信主机]的页面（如图 6- 60 所示）。

图 6- 59 可信主机菜单

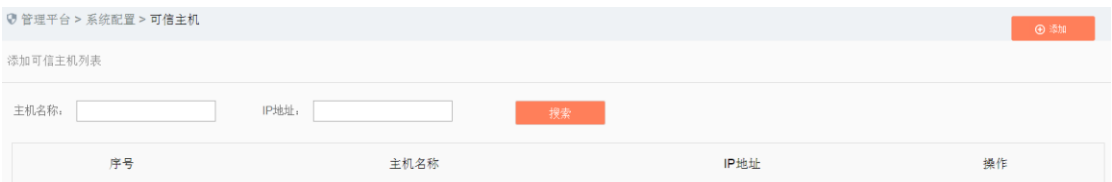


图 6- 60 可信主机列表页

此处可以查看到系统所有可信主机的信息，含义如下：

表格 70 可信主机列表显示说明

列名称	说明	
主机名称	添加时用户命名的便于记忆的名字	
IP 地址	被信任的主机的 IP 地址，点分十进制格式	
操作	查看	查看可信主机的更多详细信息
	修改	修改或重新设置可信主机的信息
	删除	删除可信主机

在此页面上点击操作列下的<查看>按钮，将显示如下图所示的可信主机的详细信息。(如图 6- 61 所示)

图 6- 61 可信主机信息查看页

点击<返回>按钮，将返回到[可信主机]页面。

6.6.9.2 添加主机

点击 [系统设置/可信主机]可信主机列表标签右侧的<添加>按钮，(如图 6- 62 所示)将弹出可信主机添加页面(如图 6- 63 所示)

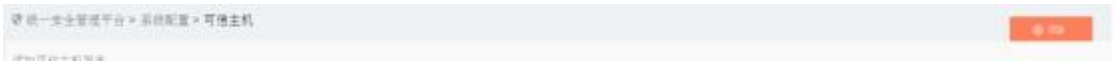


图 6- 62 可信主机添加按钮

图 6- 63 可信主机添加页

表格 71 可信主机添加信息说明

列名称	说明	
主机名称	给可信主机定义一个容易理解、记忆且有含义的名字	
IP 地址	可信主机分配到的 IP 地址，点分十进制格式	
备注	可选填，附加说明信息	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到可信主机列表显示页面
	返回	忽略所有的修改，返回到可信主机列表显示页面

6.6.9.3 修改可信主机信息

点击[可信主机]可信主机列表中操作列下的<修改>按钮，将打开[可信主机基本信息]修改页面，可以修改可信主机的基本信息（如图 6- 64 所示）

图 6- 64 可信主机基本信息修改页

6.6.9.4 删除主机

点击[可信主机]可信主机列表操作列下的<删除>按钮，把不再使用的可信主机进行删除。

6.6.9.5 检索主机

在[可信主机]可信主机列表页面中，可以根据条件对可信主机进行检索。(如图 6- 65 所示)

图 6- 65 检索可信主机

6. 6. 10 SysLog 配置

6.6.10.1 功能介绍

配置 sysLog 服务器 IP 地址与端口，发送工业防火墙设备产生的防火墙告警日志与白名单告警日志到 sysLog 服务器，分为普通类型与电网类型。

6.6.10.2 保存开启 sysLog 服务

配置管理员登录，点击 [系统设置/sysLog 配置]，(如图 6- 66 所示)进入 sysLog 配置页面。(如图 6-67 所示)

图 6- 66 菜单

图 6- 67 sysLog 配置页面

填写 IP 地址与端口号，点击<保存>按钮，保存并开启 sysLog 服务。(如图 6- 68 所示)

图 6- 68 保存 sysLog 配置

6.6.10.3 保存开启电网类型 sysLog 服务

通过 syslog 类型选择电网类型，选择电网类型需要指定网卡，选择网卡，点击<保存>按钮，保存并开启 sysLog 服务。(如图 6- 69 所示)

图 6- 69 电网类型

6. 6. 11 管理平台升级

管理平台升级新版本管理平台功能，跳转到升级服务器进行升级操作。

6.6.11.1 管理平台升级

配置管理员登录，点击 [系统设置/管理平台升级]，(如图 6- 70 所示)进入管理平台升级页面。(如图 6- 71 所示)

图 6- 70 管理平台升级菜单栏

图 6- 71 管理平台升级页面

6.6.11.2 开始升级

选择升级文件后，点击<开始上传>按钮，进度条查看进度，升级成功后访问管理平台。(如图 6- 72 所示)

图 6- 72 开始升级

6.7 拓扑管理

6.7.1 功能介绍

网络拓扑的管理是对目标系统进行安全管理的一个基础，理清客户系统的网络拓扑，不仅可以发现客户系统现有的安全问题和隐患，对后续的安全防护也有非常积极而重要的意义。

管理平台提供了比较专业的设备管理工具和网络拓扑管理工具，可以帮助客户对现有的设备进行数字化的管理，也可以让客户对系统当前的网络拓扑进行非常方便的创建和修改。

6.7.2 拓扑图

管理平台提供了网络拓扑管理工具，可以根据用户系统的现状，方便的形成网络拓扑图。配置管理员登录管理平台后，默认情况下将显示用户系统的网络拓扑，点击左侧导航栏的[拓扑管理/拓扑管理](如图 6- 73 所示)，进入[拓扑管理]的页面（如图 6- 74 所示）。

图 6- 73 设备管理菜单

图 6- 74 设备管理页

审计管理员登录管理平台后，默认情况下将显示用户系统的网络拓扑，点击左侧导航栏的[拓扑管理/拓扑管理](如图 6- 75 所示)，进入[拓扑管理]的页面（如图 6- 76 所示）。

图 6- 75 设备管理菜单

图 6- 76 设备管理页

6.7.2.1 网络拓扑的组成

管理平台的网络拓扑主要有设备和连线组成，其中设备分为如下几种：

- 工业防火墙
- 智能监测终端
- 工作站（包含主机卫士）
- 控制器
- 网络设备
- 服务器
- 未分类

(如图 6- 77 所示)

图 6- 77 拓扑图设备列表

6.7.2.2 网络拓扑设备查询

按照条件查询符合要求的设备，点击<搜索全部>按钮执行查询，（如所示）。

图 6- 78 查询结果

6.7.2.3 编辑网络拓扑

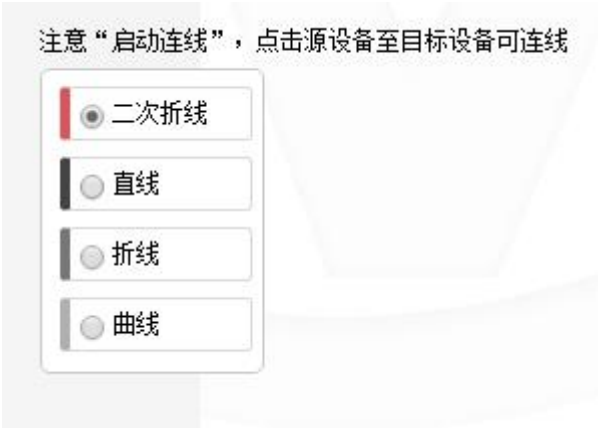
网络拓扑的编辑非常方便。

- **对于设备**

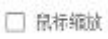
用户只需要在右侧设备树上面找到要添加进拓扑图的设备，点击设备左侧的小图标并将其拖拽进画布，即可完成设备的添加。

- **对于连接线**

用户首先选择连线的类型，目前共有下面几种类型的连接线：



选择连接线的类型后，再点击拓扑图上方的<启动连线>按钮，如图：  ，然后移动到画布，在需要连线的两个设备上依次单击鼠标左键即可完成线的添加。

拓扑图还支持放大和缩小功能，不仅支持点击缩放，如图：  ，还支持鼠标滚轮进行缩放功能，如图：  。

编辑完拓扑图之后，用户点击<保存拓扑图>，如图  ，就完成拓扑图的保存，下次登录时拓扑图信息可以正常查看得到。

6.7.2.4 拓扑联动

拓扑管理不仅可以看到用户系统的网络拓扑情况，在工业防火墙上也可以看到该工业防火墙上目前产生的告警数目。右键点击后，在弹出的菜单中选择查看，就可以看到设备的详细信息。

在拓扑图上任意一个设备点击右键，在弹出的菜单中点击<删除>，就可以将设备从拓扑图上删除掉，同时删除掉对应的连接线。也可以在连接线上直接点击右键，选择<删除>将对应的连接线删除掉。

6.8 未知设备检测

6.8.1 未知设备检测配置

配置管理员登录，点击左侧导航栏的[未知设备检测/未知设备检测配置](如图 6- 79 所示)，进入[未知设备检测配置]的页面（如图 6- 80 所示）。

图 6- 79 未知设备检测配置菜单栏

图 6- 80 未知设备检测配置页面

6.8.1.1 下发配置

未知设备检测功能可以开启或者关闭，开启后必须要选择工作状态，工作状态有：学习中，检测中。

选择学习中，点击<下发配置>按钮，会产生学习数据，可以点击<刷新列表>来查看学习到的学习数据。（如图 6- 81 所示）

图 6- 81 学习中

学习中切换到检测中，点击<下发配置>按钮，学习到的数据会加载到规则表中。（如图 6- 82 所示）

图 6- 82 检测中

规则编辑

点击<编辑规则>按钮，跳转到规则编辑页面。（如图 6- 83 所示）

图 6- 83 规则编辑

规则页面可以编辑规则，点击<保存>按钮，保存编辑结果。（如图 6- 84 所示）

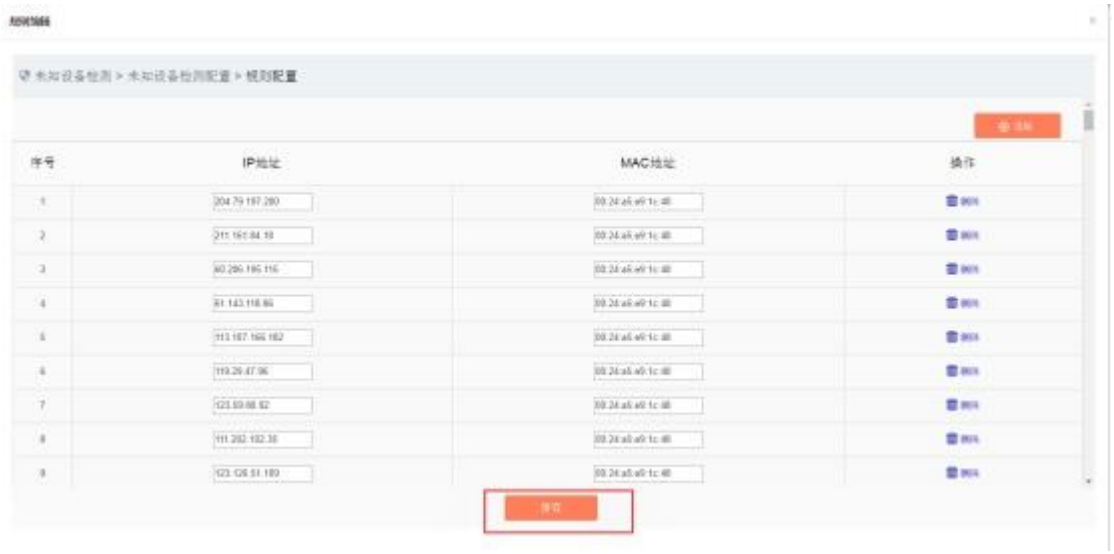


图 6- 84 保存规则

未知设备检测日志

审计管理员登录，点击左侧导航栏的[未知设备检测/未知设备检测日志](如图 6- 85 所示)，进入[未知设备检测日志]的页面（如图 6- 86 所示）。

图 6- 85 未知设备检测日志菜单栏

图 6- 86 未知设备检测日志页面

日志列表

此处可以查看到**未知设备检测日志**所有日志的信息，含义如下：

表格 72 工业协议规约检测告警显示说明

列名称	说明	
IP	发生告警设备的 IP 地址	
MAC	发生告警设备的 MAC 地址	
告警信息	告警的详细信息	
处理状态	告警是否处理	
非法接入时间	日志产生时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选[**未知设备检测日志**]规约检测告警列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。(如图 6- 87 所示)

图 6- 87 显示已处理的未知设备检测日志列表页

6.8.2.1 处理日志

点击[**未知设备检测日志**]显示列表中操作列下的<处理>按钮，将显示(如图 6- 88 所示) [**未知设备检测日志**]的处理页面：

图 6- 88 未知设备检测日志处理页

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[未知设备检测日志]页的列表中默认将不再看到此条日志。

也可以不选择“关闭”，只填写处理意见。

6.8.2.2 检索日志

在[未知设备检测日志]的列表页面中，可以根据条件对告警进行检索。(如图 6- 89 所示)

图 6- 89 检索未知设备检测日志

6.9 SysLog 日志

接收其它设备上报的 syslog 日志，审计管理员登录，点击左侧导航栏的[SysLog 日志/SysLog 日志](如图 6- 90 所示)，进入[SysLog 日志]的页面（如图 6- 91 所示）。

图 6- 90 syslog 日志菜单

图 6- 91 syslog 日志

6.9.1 检索日志

在[SysLog 日志]的列表页面中，可以根据条件对日志进行检索。(如图 6- 92 所示)

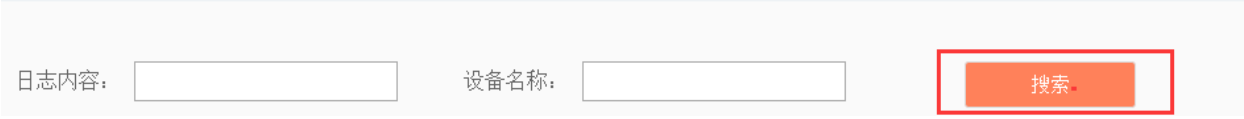


图 6- 92 日志查询