

恩创工业防火墙 S2104

用户手册

AVCOMM恩创®

工业防火墙S2104

用户手册

版权声明

©AVCOMM 恩创®版权所有

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工业防火墙。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

一、	登录.....	1
1.1	登录.....	1
1.2	系统设置向导.....	2
1.3	功能区域介绍.....	4
1.4	登录退出.....	6
二、	历史流量.....	6
三、	防护设置.....	7
四、	对象管理.....	8
4.1	地址对象.....	8
4.2	应用对象.....	10
4.3	区域对象.....	14
4.4	时间对象.....	15
五、	策略管理.....	16
5.1	策略配置.....	16
5.2	策略学习.....	19

六、	网络配置	20
6.1	接口管理.....	20
6.1.1	网络接口.....	20
6.1.2	Vlan 管理.....	22
6.1.3	网桥管理.....	23
6.1.4	聚合管理.....	24
6.2	DHCP 服务器.....	25
6.3	路由管理.....	28
6.4	NAT	29
七、	虚拟专网	30
7.1	隧道管理.....	31
7.2	证书管理.....	34
八、	系统管理	35
8.1	基本设置.....	35
8.1.1	管理设置.....	35
8.1.2	警告设置.....	36

8.1.3	日志管理.....	36
8.1.4	双机热备.....	37
8.2	资产管理.....	38
8.2.1	资产安全.....	38
8.2.2	探测.....	40
8.3	诊断工具.....	42
8.4	连接控制数.....	43
8.5	账户设置.....	44
8.5.1	账户设置.....	44
8.5.2	登录安全.....	46
8.5.3	三权分立.....	47
8.5.4	权限分配.....	48
8.6	应用配置.....	49
8.7	系统设置.....	50
8.7.1	常规选择.....	50
8.7.2	系统配置.....	51
九、	集中管理.....	52

9.1 注册列表.....	52
9.2 展示中心.....	55
十、 日志审计	56
10.1 防护日志.....	56
10.2 系统日志.....	57
10.3 管理日志.....	58
十一、 附录 A.....	58
11.1 无法打开 WEB 管理页面怎么办?	59
11.2 打开 WEB 管理界面显示白屏怎么办?	59
11.3 学习到的规则应用后, 业务处理中断怎么办?	59

一、登录

1.1 登录

设备启动完成后，没有配置过任何安全策略的工业防火墙默认工作在学习模式，这种状态下工业防火墙不拦截任何报文。

管理平台将网线插入 MGMT 口，出厂时设备默认的管理口 IP 地址为 192.168.1.254，通过管理地址 https 方式访问工业防火墙，需要使用正确的用户凭据登录 WEB 管理平台，登录界面及说明如图 1 所示：

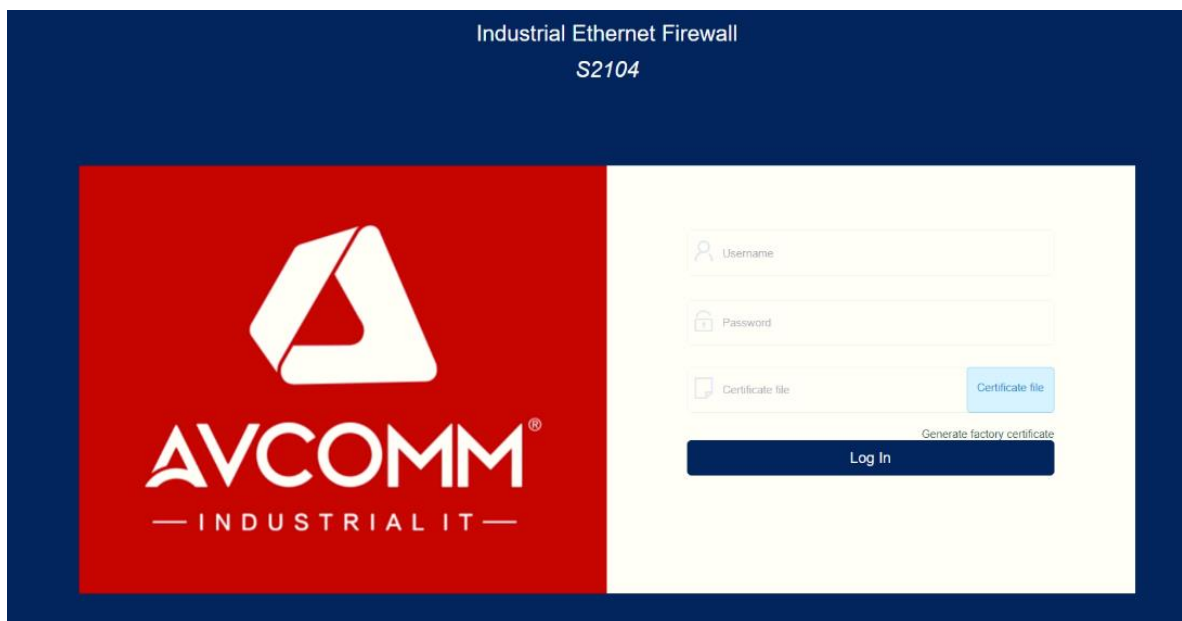


图 1

名称	说明
用户名	用于区分用户身份的唯一标识，由具备用户管理权限的用户（如 sysuser、secuser、loguser）创建并维护。

密码	用户的访问口令，用户在正确登录之后可修改自身用户的口令
语言	用户可根据需求选择中文或英文
证书文件	系统出厂默认的用户需要导入出厂证书文件才可登录
生成出厂证书	点击可生成出厂证书

注：系统出厂默认的用户名、密码如下：

- 系统管理员用户名：sysuser，密码：talent123
- 安全管理员用户名：secuser，密码：talent123
- 审计管理员用户名：loguser，密码：talent123

首次登陆系统使用登录界面的生成出厂证书完成登录，后续登录可使用用户自己的登录证书登录设备，详情参考 8.5。

WEB 管理平台第一次登录成功界面如图 2 所示：



图 2

1.2 系统设置向导

工业防火墙第一次登陆成功界面如图 2 所示，进入系统设置向导，建议及时修改默认的

管理员密码。修改完成后，点击下一页进入设备设置，工作模式分为四种，默认为学习模式，

如图 3 所示：

图 3

名称	说明
学习模式	所有数据包都能通过
警告模式	所有数据包都能通过，但对匹配规则的异常数据包会记录警告日志
防护模式	根据规则匹配进行数据包允许、阻断的处理，没有有规则匹配的都被丢弃
旁路学习模式	对镜像到接口的数据包进行解析

用户在完成设备设置后，请点击下一步进入时间设置，系统时间无误直接点击下一页，

如错误!未找到引用源。所示：

图 4

点击下一页进入系统设置，用户可根据需求，选择启用 syslog 服务器设置，建议用户选择启用，以便随时监测工业防火墙的异常通知等详情。设置完成后点击退出向导按钮完成配置，如图 5 所示：



The screenshot shows a four-step configuration wizard. The steps are: 第一步 管理员 (Step 1: Administrator), 第二步 设备设置 (Step 2: Device Settings), 第三步 设备时间 (Step 3: Device Time), and 第四步 系统设置 (Step 4: System Settings). The current step is Step 4, which is highlighted with a blue circle and the number 4. The configuration fields are: Syslog 服务器 (Syslog Server) with an empty text box, Syslog 端口 (Syslog Port) with the value 514, and 删除多少天以前日志 (Delete logs from how many days ago) with the value 30. There is an unchecked checkbox labeled 启用 (Enable). At the bottom, there are two buttons: 上一步 (Previous Step) and 退出向导 (Exit Wizard).

图 5

1.3 功能区域介绍

工业防火墙所有的业务功能均通过界面的功能列表进行选择，然后在主功能操作区域进行相应的操作。

以 sysuser 账户为例，登入系统后，如图 6 所示：

- 状态栏：点击语言可以改变界面显示语言（简体中文和 English）
- 操作区域：当前所操作的区域模块
- 功能列表：模块导航栏

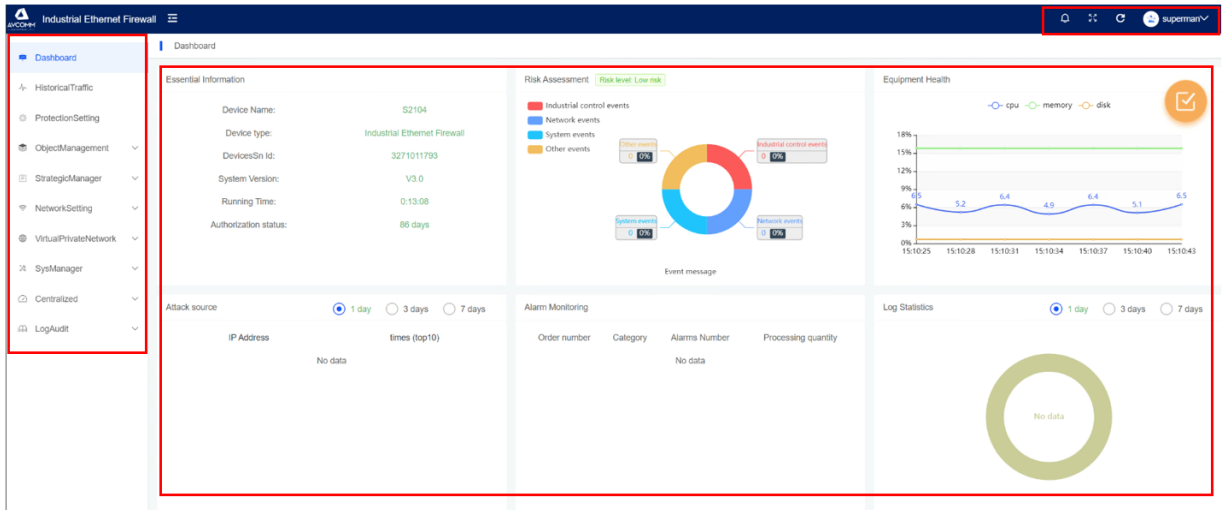


图 6


点击请选择展示模块中的  按钮，可以自定义选择想要展示的模块，勾选相应的选项后点击保存，便可展示出所选项的相应内容。如图 7 所示



图 7

名称	说明
网卡流量	显示通过系统的实时网络数据流量、数据包数和字节数
基本信息	显示设备的名称、型号、序列号、系统版本、运行时间及授权剩余天数
风险评估	显示工控事件、网络事件、系统事件、其他事件的数量和风险等级评估情况
设备健康	显示设备的 CPU、内存和磁盘的使用状态
攻击来源	显示 top10 的被阻断的源 IP 统计结果
告警监控	实时显示系统今日工控事件、今日网络事件、今日其他事件和所有工控事件、所有网络事件、所有其他事件的告警数量和处理数量
日志统计	统计并以饼状图显示系统中产生的警告、提示、错误的信息数量占比情况

1.4 登录退出

点击状态栏用户名，选择登出即可注销登录。

二、历史流量

系统管理员（sysuser）可以查看一天内的接口流量统计情况、一天内的会话数统计情况、一天内的协议流量占比统计情况和一天内的设备总流量统计情况，如图 8 所示：

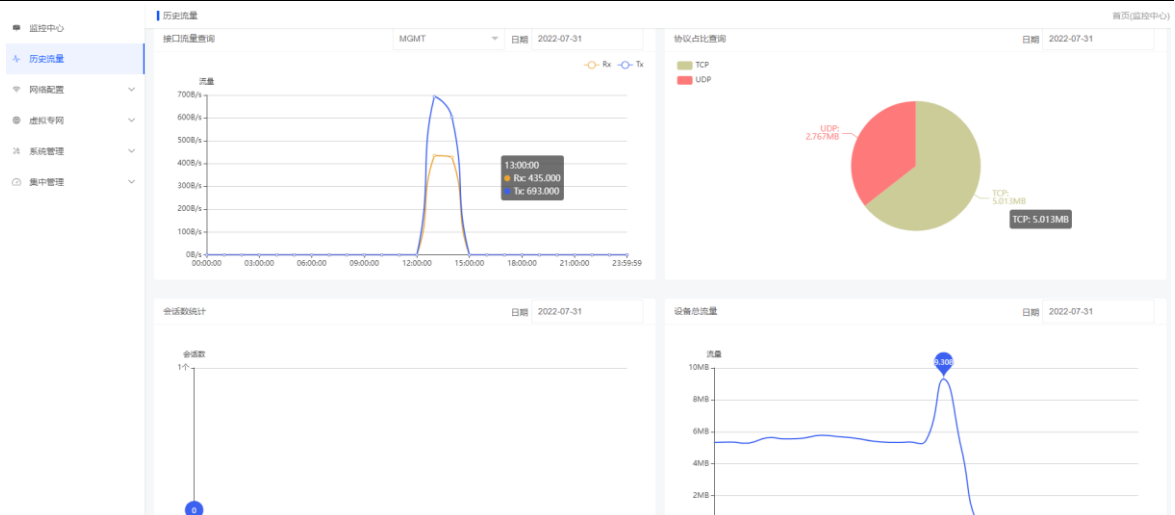


图 8

名称	说明
接口流量查询	统计一天内各个接口的流量数据，并可查询历史日期的统计结果
协议流量占比查询	统计一天内协议流量占比，以饼状图展示，并可查询历史日期的统计结果
会话数统计	统计一天内系统产生的会话数量，并可查询历史日期的统计结果
设备总流量	统计一天内设备所有接口的总流量和，并可查询历史日期的统计结果

三、防护设置

防护设置分为三部分，Dos/DDos 攻击防护、异常数据包攻击防护和扫描防护。默认开启

状态，如图 9 所示：



图 9

名称	说明
Dos/DDos 攻击防护	支持 SYN Flood、UDP Flood、ICMP Flood 攻击防护，并支持设置阈值
异常数据包攻击防护	支持 Ping of Death 攻击防护，可设置包长阈值；支持 TearDrop 攻击、LAND 攻击防护
扫描防护	支持端口扫描防护，可设置阈值

四、对象管理

对象管理包含地址对象、应用对象、区域对象、时间对象，可被策略引用，当对象被工业防火墙策略引用时，不支持删除，支持编辑。

4.1 地址对象

安全管理员（secuser）对地址资源进行管理，地址资源支持配置地址对象和地址组，地址对象支持输入的格式是主机地址、地址段、地址范围或者组合形式，页面可进行添加、编

辑、删除及批量删除等操作，如图 10 所示：



图 10

点击添加按钮，可增加地址资源，输入地址名称，地址对象系可同时输入多个 IP 地址、IP 地址段，或者是组合形式，如图 11 所示：

添加地址资源

* 名称

* 类型

* IP地址

MAC地址

注意 1. IP地址支持散列、范围和组合，散列“,”隔开，范围“-”隔开
2. MAC参考格式：12:23:AB:55:55:AF

描述

图 11

同时，管理员也可以进行地址组的管理，在地址组配置界面，点击添加，可把多个地址

资源合到一个地址组内，如图 12 所示：

添加地址组

* 名称

描述

* 地址组列表

地址列表

关键词搜索

暂无数据

>>

<<

选中地址列表

关键词搜索

132

123

取消 保存

图 12

4.2 应用对象

应用对象支持预定义应用、自定义应用及应用组的配置，安全管理员（secuser）可在预定义应用中查看系统的预定义应用资源（不可编辑、删除），支持自定义应用、应用组的添加、编辑，删除等操作，如图 13 所示：

应用 首页(监控中心) / 对象管理

预定义应用 自定义应用 应用组

名称:

名称	内容	描述
DNP3	tcp目的端口:20000,源端口:1-65535	DNP3
HTTP	tcp目的端口:80,源端口:1-65535	HTTP
FTP	tcp目的端口:21,源端口:1-65535	FTP
IEC104	tcp目的端口:2404,源端口:1-65535	IEC104
MMS	tcp目的端口:102,源端口:1-65535	MMS
MODBUS	tcp目的端口:502,源端口:1-65535	MODBUS
OPCDA	tcp目的端口:135,源端口:1-65535	OPCDA
POP3	tcp目的端口:110,源端口:1-65535	POP3
S7COMM	tcp目的端口:102,源端口:1-65535	S7COMM
SMTP	tcp目的端口:25,源端口:1-65535	SMTP
TELNET	tcp目的端口:23,源端口:1-65535	TELNET
RTSP	tcp目的端口:554,源端口:1-65535	RTSP
OPCUA	tcp目的端口:4840,源端口:1-65535	OPCUA
PROFINET	udp目的端口:34962-34964,49152,49153,49155,源端口:1-65535	PROFINET
CIP	tcp/udp目的端口:44818,源端口:1-65535	CIP

图 13

点击自定义应用，可显示自定义应用列表，点击添加按钮，可添加自定义应用资源，如

图 14 所示：

添加应用资源 ×

1 第一步 基本设置 2 第二步 高级设置 3 第三步 配置结果

* 名称

* 协议

* 端口

* 通讯类型

描述

图 14

名称	说明
名称	自定义应用的名称
协议	协议类型，支持 MODBUS、DNP3、OPCDA 等协议
端口	支持自定义端口，取值范围 1-65535
通讯类型	支持 TCP、UDP 两种
描述	自定义应用的描述信息，1-32 个字符长度

对 MODBUS 应用进行配置时，完成上一步配置点击下一步按钮，进入高级设置，可对 MODBUS 应用进行深度解析控制的配置，支持对功能码、地址、数据类型、解析方式、值域进行控制，如图 15 所示：

添加应用资源

第一步 基本设置 第二步 高级设置 第三步 配置结果

功能码	地址	数据类型	解析方式	阈值控制	动作	操作
Read_Coils		BOOL	0&1	1 - 1	接受	

< 1 > 到第 1 页 确定 共 1 条 10 条/页

上一步 提交

图 15

当需要配置自定义端口的服务时，添加自定义应用，协议选择“自定义服务”，点击下一

步可进行源目端口的配置，如图 16 所示：



The screenshot shows a dialog box titled "添加应用资源" (Add Application Resource) with a close button (X) in the top right corner. It features a progress indicator with three steps: 1. 第一步 基本设置 (Step 1: Basic Settings), 2. 第二步 高级设置 (Step 2: Advanced Settings), and 3. 第三步 配置结果 (Step 3: Configuration Results). Step 1 is currently active. The form includes the following fields:

- * 名称 (Name): A text input field.
- * 协议 (Protocol): A dropdown menu currently set to "自定义服务" (Custom Service).
- 描述 (Description): A text input field.
- 下一步 (Next Step): A blue button.

图 16

可自定义 TCP、UDP 端口及配置 ICMP 协议，端口号支持散列输入、范围输入或者组合格式输入，如图 17 所示



The screenshot shows the same dialog box, now at Step 2: 第二步 高级设置 (Advanced Settings). The progress indicator shows Step 1 as completed and Step 2 as active. The form includes the following elements:

- 类型 (Type): Radio buttons for TCP (selected), UDP, and ICMP.
- 源端口 (Source Port): A text input field.
- * 目的端口 (Destination Port): A text input field.
- 注意 (Note): A red note with three points:
 1. 端口支持散列端口，端口范围和两者组合
 2. 散列端口支持格式，例如：135,80,502
 3. 端口范围支持格式，例如：520-1314
- 上一步 (Previous Step): A button.
- 提交 (Submit): A blue button.

图 17

同时，管理员也可以进行应用组添加、编辑、删除等操作。点击添加按钮，可把多个应

用资源合到一个应用组内，一个应用组最多可添加 10 个应用，如图 18 所示：

图 18

4.3 区域对象

安全管理员（secuser）对区域资源进行管理，可进行编辑修改、删除、添加等操作。为便于操作，设备出厂默认将除管理口外的其他接口都加入到区域中，一个区域一个接口。如图 19 所示：

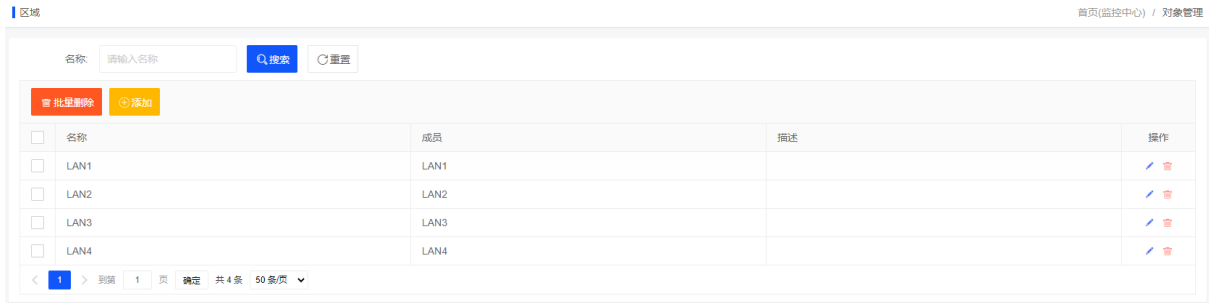


图 19

注：策略引用区域时，源目区域对象不允许配置一致

4.4 时间对象

安全管理员（secuser）可对时间资源进行管理，支持添加、编辑、删除、添加等操作。

设备出厂默认有两个时间对象，一个任意时间对象“always”，一个每周的周期时间“weekly”，

不支持编辑删除。如图 20 所示：



图 20

点击添加按钮，弹出添加页面，可添加自定义时间资源，输入时可选择时间类型，时间

类型有固定时间和周期时间两种，周期时间可按照每天、每周、每月进行配置，如图 21 所

示：



添加时间资源

* 名称

类型 固定时间

日期 固定时间

时间 每天

注意 每周

每月

取消 保存

图 21

五、策略管理

5.1 策略配置

安全管理员（secuser）可进行策略配置管理，可进行添加、编辑、删除、移动等操作。

配置的策略只在设备工作模式为“防护模式”时有效。

防护模式下数据包按照可按照应用、源目地址、源目区域、时间对象进行策略匹配，当策略动作为阻断时，数据包被丢弃；当策略动作为允许时，数据包接受转发。

点击添加按钮，弹出添加策略界面，编辑策略的名称、应用、动作等配置项，配置完成后点击保存。如图 22 所示：

添加规则
✕

* 名称

动作 禁用 ▼

* 应用 请选择应用 ▼

源端区域 请选择 ▼

源端地址 请选择地址 ▼

目的区域 请选择 ▼

目的地址 请选择地址 ▼

作用时间 请选择 ▼

描述

保证带宽(Mb)

限制带宽(Mb)

带宽优先级 0 ▼

图 22

名称	说明
名称	策略名称，必填项
动作	策略动作，包括接受、丢弃、禁用

应用	策略匹配的应用对象，支持配置预定义应用、自定义应用、应用组，必填项
源端区域	策略匹配的源区域对象
源端地址	策略匹配的源端地址对象，可选择地址对象或地址组
目的区域	策略匹配的目的地区域对象
目的地址	策略匹配的目的地地址对象，可选择地址对象或地址组
时间	策略匹配的时间对象
描述	策略的描述信息
保证带宽	策略的最低保证带宽
限制带宽	策略的限制带宽
带宽优先级	策略的优先级，0-7 可选
记录日志	匹配策略是否记录日志的开关
未定义动作	未配置策略或者策略不匹配时执行未定义动作

策略匹配有优先级，位于上方的优先级高于下方的优先级，即优先级号大的优先级高。


可通过  拖拽策略，移动规则的上下位置，以确定规则优先级。如图 23 所示：



图 23

配置的策略支持导出、导入。点击 **策略导出**，直接导出策略。

点击 **策略导入**，可弹出策略导入界面(如图 26 所示)，点击 **策略导入** 选择要导入的策略，点击 **导入策略**，

便已导入策略成功，如图 24 所示：



图 24

5.2 策略学习

策略管理员（secuser）登录工业防火墙后，可以通过“系统管理—工作模式”模块中选择进入学习模式，即从网络环境数据流中自主智能学习到具体的协议类型以及详细协议数据，同时自动生成协议规则。

选择开始时间，学习时长，学习的协议类型，点击开始，便可开始学习，如图 25 所

示：



图 25

学习到的规则，点击应用规则 [应用规则](#)，会在策略配置中查看应用生效的学习规则，如图

26 所示：



图 26

六、网络配置

6.1 接口管理

接口管理支持配置的接口类型有物理接口、桥接口、VLAN 接口、聚合接口。

6.1.1 网络接口

系统管理员（sysuser）对设备接口进行管理，可查看接口连接状态，并可进行设备接口

IP 地址、子网掩码等的添加、编辑、删除和查看操作，如图 27 所示：



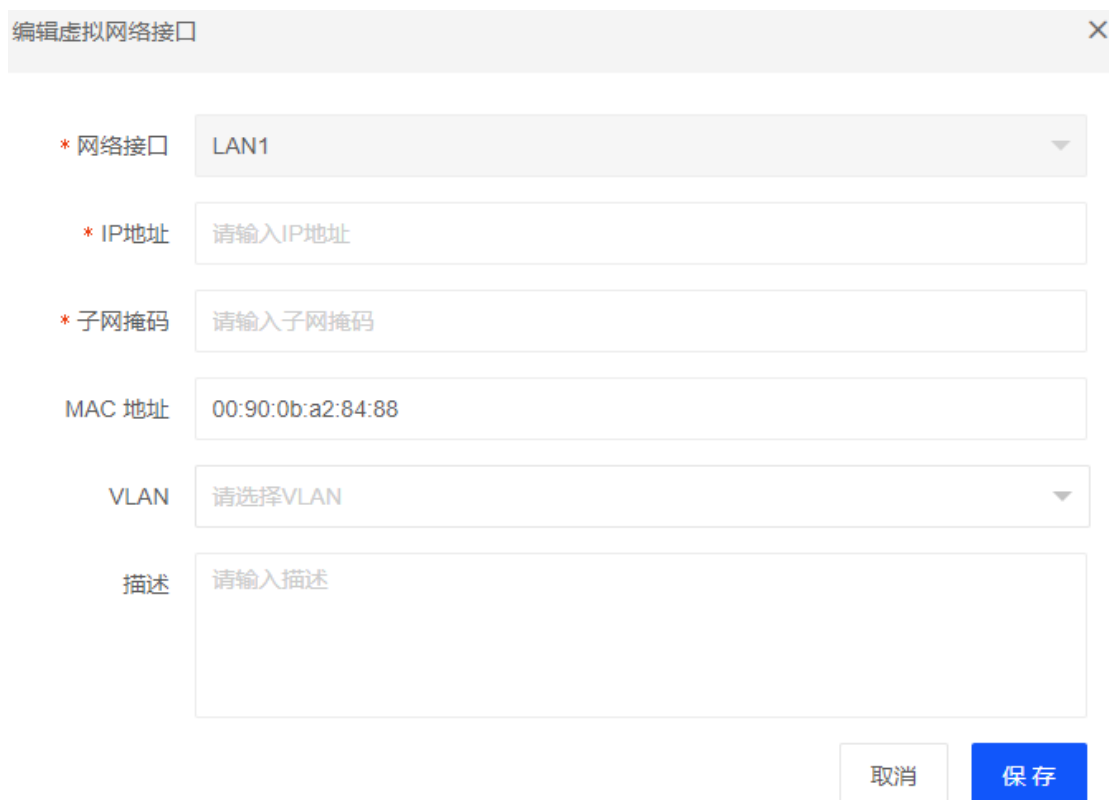
The screenshot shows a web interface for managing network interfaces. At the top, there are tabs for '网络接口' (Network Interface), '网桥管理' (Bridge Management), 'Vlan管理' (Vlan Management), and '聚合管理' (Aggregation Management). Below the tabs, there are search and filter fields for '接口名称' (Interface Name), 'IP地址' (IP Address), and '状态' (Status). A table lists four interfaces:

ID	接口名称	网络适配器名称	IP地址	子网掩码	VLAN	模式	通信状态	描述	操作
1	LAN1	eth0					在线		编辑 删除
2	LAN2	eth1					在线		编辑 删除
3	LAN3	eth2					离线		编辑 删除
4	LAN4	eth3					离线		编辑 删除

图 27

单击 [编辑](#)，进入编辑网络接口，根据实际环境可配置接口的 IP 地址、掩码及 VLAN 标签，

如图 28 所示：



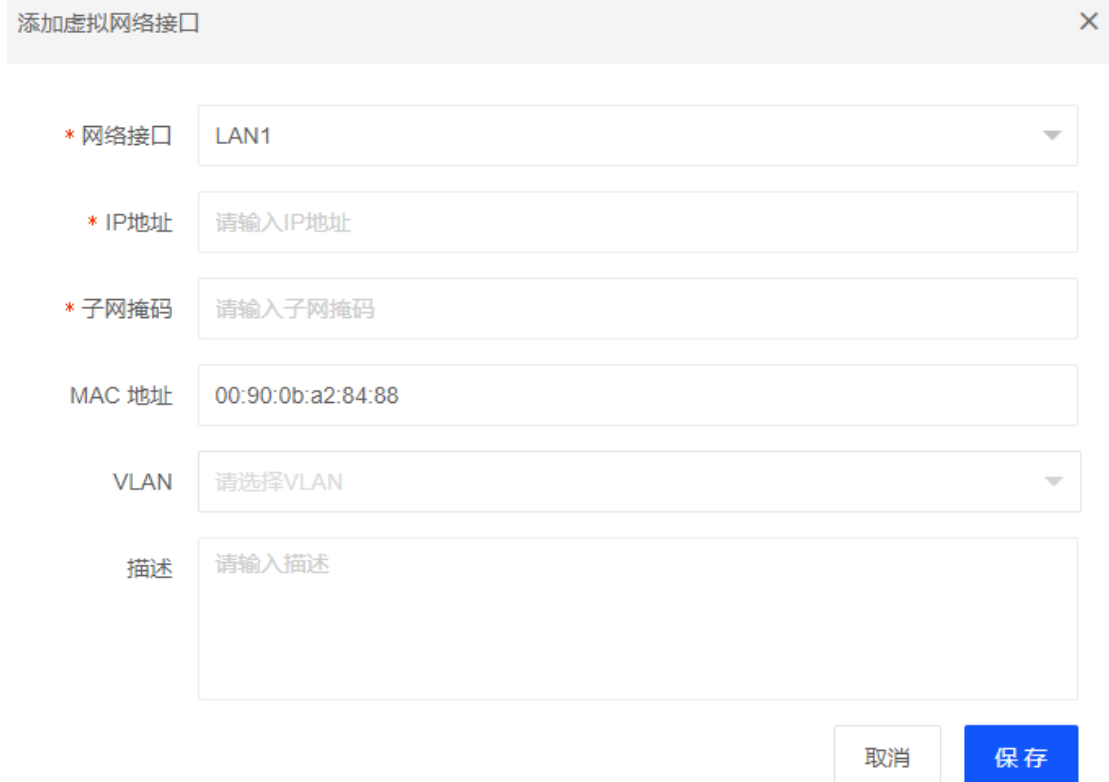
The screenshot shows a dialog box titled '编辑虚拟网络接口' (Edit Virtual Network Interface). It contains the following fields:

- * 网络接口: LAN1 (dropdown menu)
- * IP地址: 请输入IP地址 (text input)
- * 子网掩码: 请输入子网掩码 (text input)
- MAC 地址: 00:90:0b:a2:84:88 (text input)
- VLAN: 请选择VLAN (dropdown menu)
- 描述: 请输入描述 (text input)

At the bottom right, there are two buttons: '取消' (Cancel) and '保存' (Save).

图 28

点击添加按钮，可添加虚拟网络接口，即子接口，如图 29 所示：



添加虚拟网络接口

* 网络接口 LAN1

* IP地址 请输入IP地址

* 子网掩码 请输入子网掩码

MAC 地址 00:90:0b:a2:84:88

VLAN 请选择VLAN

描述 请输入描述

取消 保存

图 29

注意：

- 删除只可以删除添加的虚拟网络接口，真实的网络接口只会清理 IP 地址和 VLAN 的相关信息
- 每个接口只能添加到一个接口属性；

例：eth0 接口添加到 VLAN，就不能再添加到网桥或聚合

6.1.2 Vlan 管理

系统管理员（sysuser）对 VLAN 进行管理，可执行添加、编辑、删除等操作，新建 VLAN 标

签，点击添加，进入添加界面，VLAN 标签填写范围为 1-4094，如图 30 所示：

添加Vlan
✕

* 标签

IP地址

子网掩码

描述

图 30

配置好 VLAN 标签后，配置 VLAN 接口，在网络接口界面点击编辑按钮，给接口选择 VLAN 标签，当配置单个 VLAN 标签时，接口模式为 access；配置两个及以上的 VLAN 标签时，接口模式为 trunk。如图 31 所示：

接口管理
首页(监控中心) / 网络配置

网络接口 网桥管理 Vlan管理 聚合管理

接口名称: IP地址: 状态:

批量删除
添加

<input type="checkbox"/>	ID	接口名称	网络适配器名称	IP地址	子网掩码	VLAN	模式	通道状态	描述	操作
<input type="checkbox"/>	1	LAN1	eth0					在线		编辑 删除
<input type="checkbox"/>	2	LAN2	eth1					在线		编辑 删除
<input type="checkbox"/>	3	LAN3	eth2			100	access	离线		编辑 删除
<input type="checkbox"/>	4	LAN4	eth3			100	access	离线		编辑 删除

< 1 > 到第 1 页 确定 共 4 条 50 条页

图 31

6.1.3 网桥管理

系统管理员（sysuser）对网桥进行管理，可进行添加、编辑、删除等操作，点击添加按

钮，进入添加网桥的界面，编辑桥接口名称、选择网络接口等信息，网桥的接口 IP 地址用来做桥接口管理。如图 32 所示：



The image shows a dialog box titled "添加桥" (Add Bridge) with a close button (X) in the top right corner. The dialog contains the following fields:

- * 桥名称** (Bridge Name): A text input field with the placeholder "请输入桥名称" (Please enter bridge name).
- 网络接口** (Network Interface): A dropdown menu with the placeholder "请选择网络接口" (Please select network interface).
- IP地址** (IP Address): A text input field with the placeholder "请输入IP地址" (Please enter IP address).
- 子网掩码** (Subnet Mask): A text input field with the placeholder "请输入子网掩码" (Please enter subnet mask).
- 描述** (Description): A larger text input field with the placeholder "请输入描述" (Please enter description).

At the bottom right of the dialog, there are two buttons: "取消" (Cancel) and "保存" (Save).

图 32

注：接口只能被加入一个桥接口中，不能被再次加入到其他桥接口

6.1.4 聚合管理

系统管理员（sysuser）对聚合进行管理，可进行添加、编辑、删除等操作。聚合接口支持的模式有五种，常用的模式有 1 主备份策略和 4 动态链路聚合模式。点击添加聚合接口，进入添加界面，如图 33 所示：

添加网口聚合

* 名称

* 网络接口 请选择网络接口

* 模式 请选择 模式

IP地址 请选择 模式

子网掩码 0 (平衡轮循环策略)

Miiimon 1 (主-备份策略)

2 (平衡策略)

3 (广播策略)

状态 4 (IEEE802.3ad 动态链接聚合)

描述 请输入描述

取消 保存

图 33

6.2 DHCP 服务器

系统管理员（sysuser）对 DHCP 服务器进行管理，支持启用 DHCP 服务的接口有物理接口、VLAN 接口、桥接口。支持 DHCP 服务器的添加、编辑、删除等操作，同时还支持配置 IP 地址静态绑定，给指定的客户端分配固定的 IP 地址。

新建 DHCP 服务器，点击添加按钮，弹出添加 DHCP 域界面，选择启用 DHCP 服务的接口，配置网络地址/掩码，地址范围、租期等，配置完成后点击保存，如图 34 所示：

添加DHCP域
×

* 网络接口

* 网络地址

* 网络掩码

网关

域名

DNS服务器

* 地址范围 -

* 默认租约时间(分钟)

* 最大租约时间(分钟)

描述

图 34

名称	说明
网络接口	启用 DHCP 服务的接口
网络地址	指定的网络，和掩码一起配合生效，必填项
掩码	指定的网络地址的掩码，必填项
网关	为客户端设置默认网关

域名	为 DHCP 客户端设置 DNS 域名
DNS 服务器	为客户端设置 DNS 服务器 IP 地址
地址范围	DHCP 客户端可分配的地址范围，属于网络地址/掩码范围内有效，必填项
默认租约时间	客户端获取地址后的租约时间，默认 1 天
最大租约时间	最大租约时间，当客户端超时租约时间但尚未更新 IP 地址时，最长可使用该 IP 的地址的时间，默认 3 天

DHCP 静态绑定，进入 DHCP 静态 IP 配置界面，点击添加，可为某个主机分配指定的 IP 地址，如图 35 所示：

添加DHCP静态IP ×

* 主机名称

* IP地址

* MAC地址

描述

注意： 建议静态绑定的IP地址在地址池外

图 35

6.3 路由管理

系统管理员（sysuser）对静态路由进行管理，可进行添加、编辑、删除等操作。点击

添加路由，如图 36 所示：



图 36

名称	说明
目的 IP 地址	静态路由的目的 IP 地址
子网掩码	静态路由的网络掩码
下一跳	下一跳的 IP 地址
网络接口	静态路由的出接口，可与下一跳地址二选一进行配置

权重	在多下一跳负载均衡时，权重越大，命中的概率就越大
描述	静态路由的描述信息，1-32 个字符长度

6.4 NAT

系统管理员（sysuser）对 NAT 进行管理，NAT 分为 SNAT 和 DNAT。NAT 配置可针对特定的应用进行地址转换。SNAT 对源地址转换，可编辑、删除、添加、搜索等操作。

新建 SNAT，点击添加，可进入 SNAT 添加界面，添加设备的源 IP 地址、目的 IP 地址和转换后的 IP 地址等，并启用该策略，如图 37 所示：

图 37

DNAT 对目的地址进行、目的端口进行转换，支持添加、编辑、删除、搜索等操作。

新建 DNAT 策略，点击添加，可进入添加目的 NAT 界面，添加设备的源 IP 地址、目的 IP 地址和转换后的 IP 地址等，并启用该策略，如图 38 所示：



添加DNAT

入接口 请选择网络接口

应用 请选择应用

源IP 请选择地址

* 目的IP 请选择地址

* 转换后 IP 请输入转换后的IP地址

转换后的端口 请输入转换后的端口

描述 请输入描述

状态 启用

取消 保存

图 38

七、虚拟专网

策略管理员（secuser）对 VPN 进行配置，对传输的数据进行加密，保证数据传输的安全性。VPN 配置支持两种认证方式，包括预共享密钥和国密证书认证两种方式。国密证书认证需要授权，授权文件需要向相关人员获取。

7.1 隧道管理

1) 策略管理

安全管理员（secuser）对策略管理进行操作，支持添加、编辑、删除和查看等操作。

创建 VPN 策略，先点击添加策略配置,添加界面如图 39 所示：

图 39

名称	说明
组名	策略管理的组名
验证方法	预共享密钥和证书认证两种，两端需配置一致
密码	预共享密钥，两端需配置一致

IKE	第一次交换协商 IKE SA 的参数，包括加密算法、认证算法、DH 算法，协商时两端必须配置一致才可以协商成功
ESP	为报文使用的安全协议，防火墙目前只支持 ESP 方式，也需要协商加密算法及认证算法等，同理两端需要配置一致才可以协商成功

2) 隧道策略

安全管理员（secuser）对隧道策略进行操作，支持添加、编辑、删除和查看等操作。

配置完认证策略，添加隧道策略，引用配置好的认证组，配置 VPN 两端的网关及要保护的流量（感兴趣流），勾选自动启动，如图 40 所示：

添加隧道策略

* 源地址 MGMT (eth4,10.0.14.11)

* 源子网

* 认证组 当前没有可用的身份验证组

* 目的地址

* 目标子网

自动启动 启用

直通 启用

取消 保存

图 40

名称	说明
源地址	VPN 隧道两端的源地址
源子网	VPN 隧道保护的流量的源子网
认证组	VPN 使用的认证组（策略管理）
目的地地址	VPN 隧道两端的目的地地址
目标子网	VPN 隧道保护的流量的目标子网
自动启动	勾选启动，会主动建立 VPN 连接
直通	启用直通，VPN 协商成功后，会下发运行保护流量通过的策略

3) 国密 VPN 授权

使用国密证书认证方式时，需要先获取 VPN 授权，授权成功后配置国密证书，才可进行 VPN 设置。先配置认证策略，再进行隧道策略。策略管理支持添加、编辑及删除。

当认证方式为国密认证时，需要先获取授权，点击 VPN>隧道管理>国密 VPN 授权，导出国密 VPN 信息，获取授权文件后，点击导入授权文件，VPN 的授权状态会同步更新，如图 41 所示：



图 41

7.2 证书管理

获取到相关证书后，点击添加 CA 证书，如图 42 所示：



添加CA证书

* 证书名

* CA 证书

取消 保存

图 42

添加 IPSEC 证书，点击添加，包括签名证书及加密证书等相关信息，都为必填项，如图

43 所示：



添加Ipsec证书

* 证书名

* 签名证书

* 加密证书

* 证书类型 软证书

* 签名私钥

* 加密私钥

取消 保存

图 43

八、系统管理

8.1 基本设置

8.1.1 管理设置

系统管理员（sysuser）在基本设置中可进行管理设置，主要包含管理口配置、SNMP 设置、SSH 设置、访问安全设置。如图 44 所示：

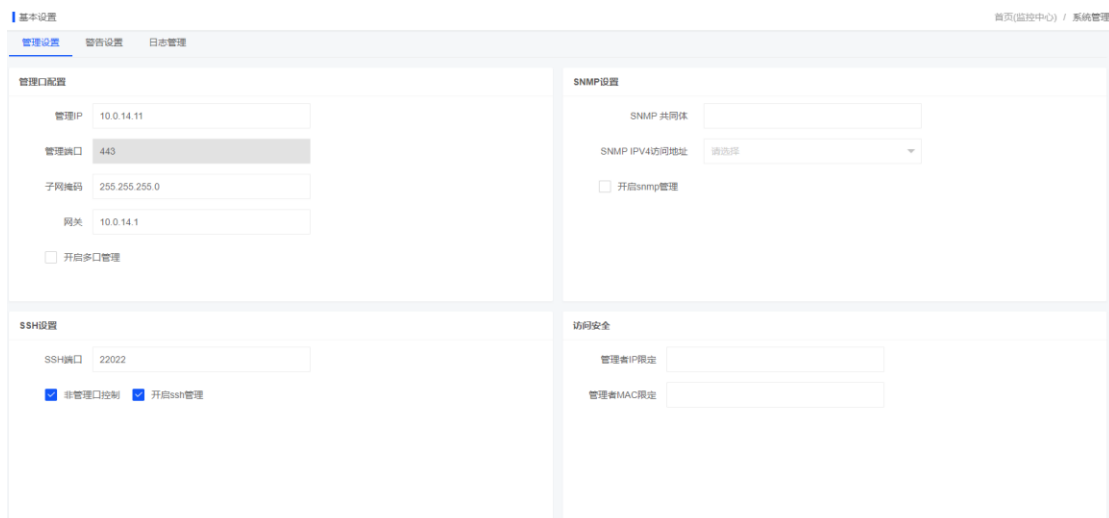


图 44

名称	说明
管理口设置	设备管理口配置，支持配置多口管理，默认网关
SNMP 设置	SNMP 服务启用禁用及配置
SSH 设置	SSH 服务启用、禁用，支持开启管理口及业务口的 SSH 服务
访问安全	支持配置管理者访问安全绑定

8.1.2 警告设置

系统管理员（sysuser）在基本设置中可进行警告设置，即工业防火墙 CPU 使用率、内存使用率、硬盘使用率、网络使用率警告标准。当设备状况达到警告值时，配合“邮箱设置”发送警告邮件到管理员邮箱以通知管理员。如图 45 所示：

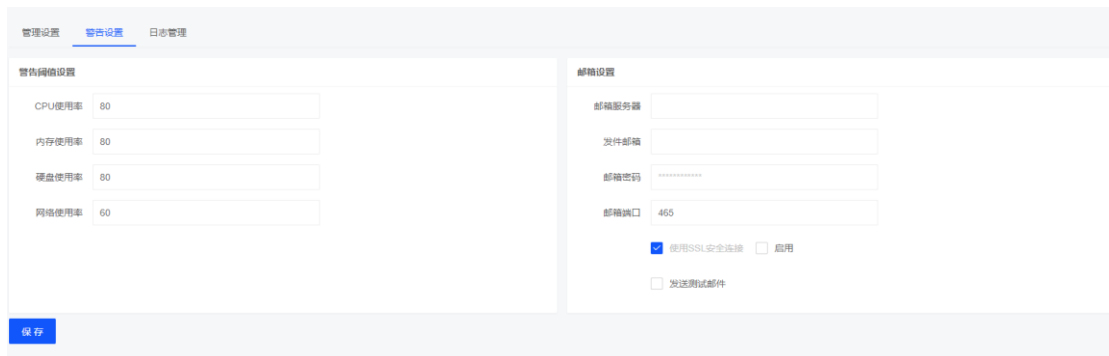


图 45

8.1.3 日志管理

系统管理员（sysuser）在基本设置中可进行日志管理，主要包含日志存储时间管理和 Syslog 设置。启用 Syslog 服务器后，日志信息会同步备份到 Syslog 服务器。如图 46 所示：

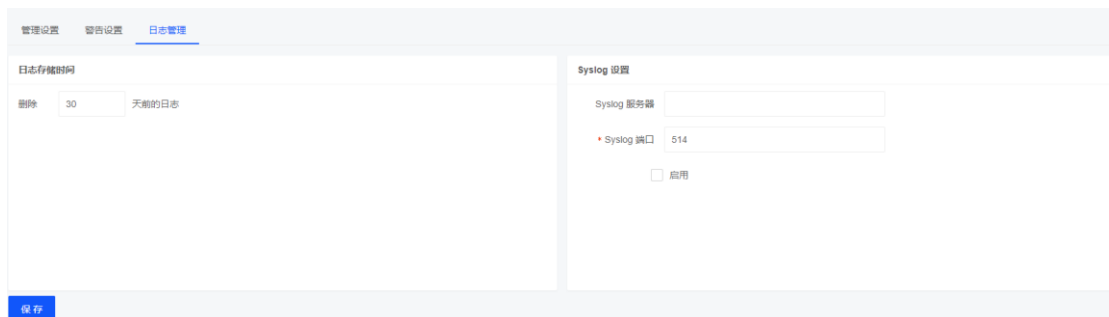


图 46

8.1.4 双机热备

系统管理员（sysuser）在基本设置中可进行双机热备管理，当主机设备发生故障时业务可切换到备机以达到保护链路正常通信的目的。主要包含双机热备配置和双机热备状态。

配置双机热备需两台设备，一台作为主机，一台作为备机，配置界面如图 47 所示：



图 47

名称	说明
设备主从模式	分为主设备和从设备两种
抢占模式	有抢占和非抢占两种，只有主设备支持配置
心跳频率	主从设备之间用来互相通告设备工作状态，心跳频率支持配置的范围为 1-3s，两端配置不一致时，已协商的最小值生效，默认为 1s
策略同步间隔	支持配置的时间范围为 1-10 分钟，主设备按照策略同步间隔将本机的配置同步到备机，两端配置不一致时，以协商的最小值生效，默认为 1 分钟

本端 IP 地址	本设备 HA 接口的 IP 地址，必填项
对端 IP 地址	对端设备的 HA 接口 IP 地址，用于心跳包交互，必填项
刷新网络	用于同步主设备需要监控的网络接口
双机热备状态	开启双机热备后，会同步显示本机的 HA 状态信息及对端设备的 HA 状态信息

8.2 资产管理

8.2.1 资产安全

资产安全分为三个部分，资产汇总信息，资产清单，资产导入，如图 48 所示：

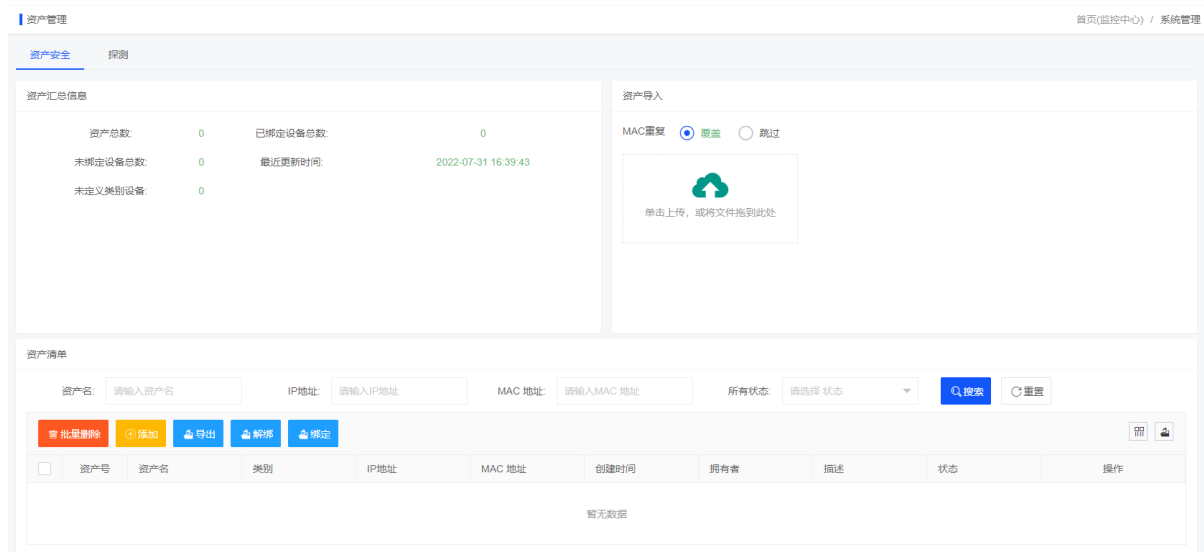


图 48

策略管理员（secuser）对资产清单进行管理，可编辑、删除、添加，解绑和绑定等操作，如图 49 所示为解绑和绑定：

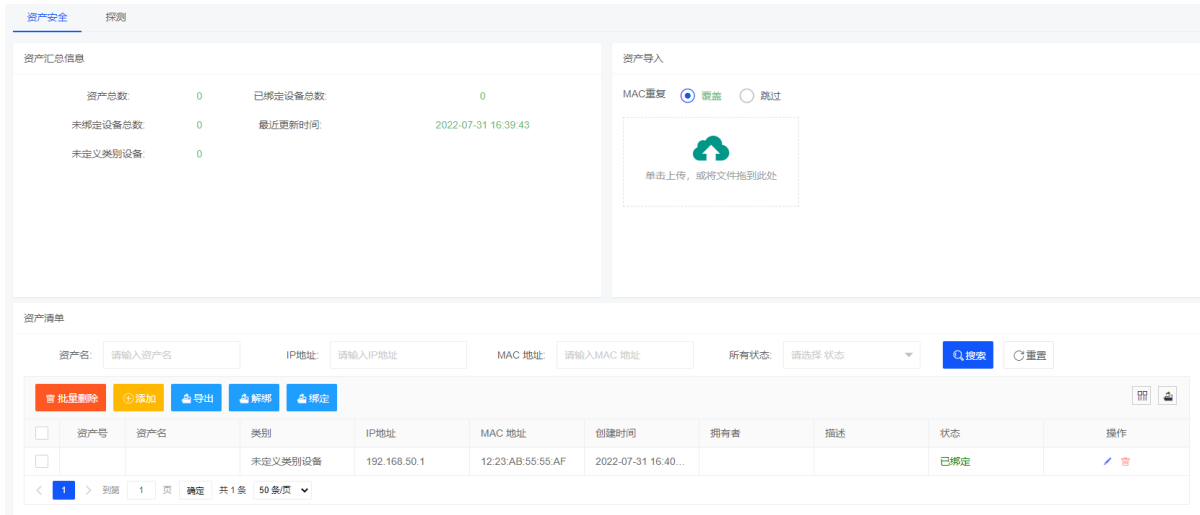


图 49

添加资产清单，类别有多种选项，也可以手动设置类别，如图 50 所示：



图 50

资产导入只支持 csv 格式的文本导入，如图 51 所示：



图 51

名称	说明
覆盖	资产清单存在的一条资产与导入的资产重复，去掉资产清单的资产，添加导入的资产。
跳过	资产清单存在的一条资产与导入的资产重复，资产清单的资产不做处理，导入的资产不添加。

8.2.2 探测

探测可以通过设备接口来进行探测，可以对探测出的 IP 和 MAC 进行绑定，

1. **探测：**每次探测时间为 2 分钟，选中接口点击探测就会进入探测界面，如图 52 所示：

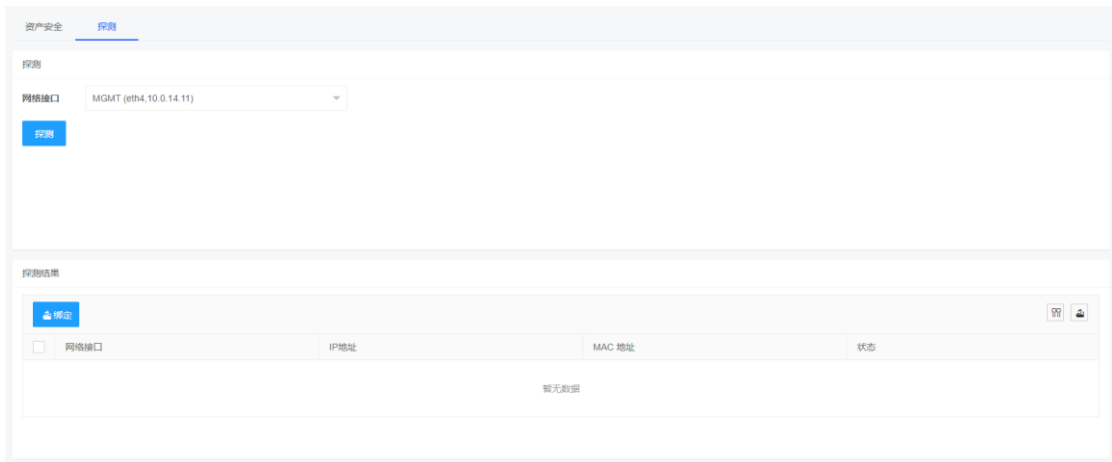


图 52

注：如在两分钟内探测出所有结果，不会再探测；如探测不出结果会等待 2 分钟超时退出。

2. **绑定：**将探测出的 IP 地址和 MAC 地址进行绑定，如不想绑定不需要对探测的结果进行操作，选中要绑定的结果，点击绑定即可。如图 53 所示：

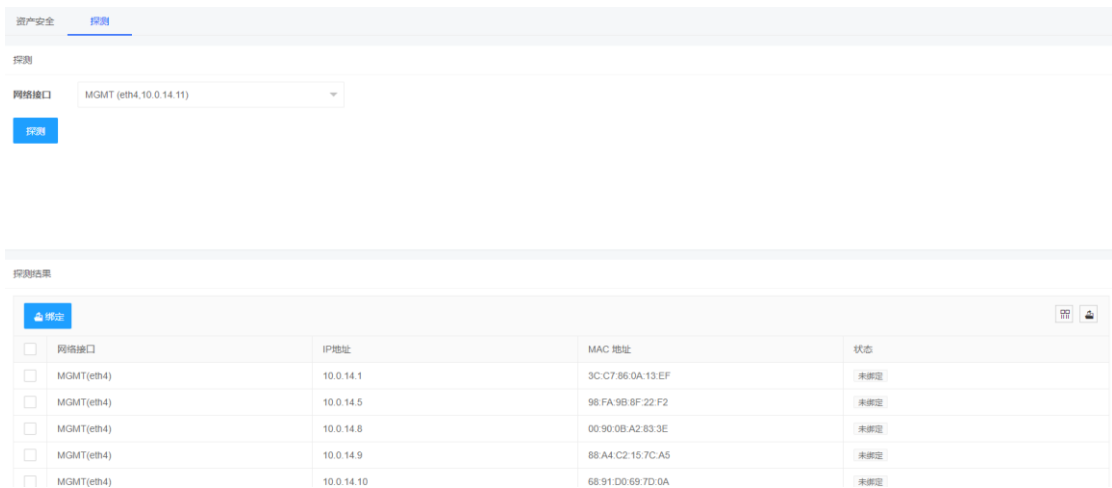


图 53

查看资产安全存在绑定结果，如图 54 所示：

资产清单

资产名: IP地址: MAC地址: 所有状态:

<input type="checkbox"/>	资产号	资产名	类别	IP地址	MAC地址	创建时间	拥有者	描述	状态	操作
<input type="checkbox"/>			未定义类别设备	10.0.14.1	3C:C7:86:0A:13:EF	2022-07-31 16:47...			已绑定	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/>			未定义类别设备	10.0.14.5	98:FA:9B:8F:22:F2	2022-07-31 16:47...			已绑定	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/>			未定义类别设备	10.0.14.8	00:90:0B:A2:83:3E	2022-07-31 16:47...			已绑定	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/>			未定义类别设备	10.0.14.9	88:A4:C2:15:7C:A5	2022-07-31 16:47...			已绑定	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/>			未定义类别设备	10.0.14.10	68:91:D0:69:7D:0A	2022-07-31 16:47...			已绑定	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/>			未定义类别设备	10.0.14.14	00:16:31:D4:AE:82	2022-07-31 16:47...			已绑定	<input type="button" value="编辑"/> <input type="button" value="删除"/>

< 1 > 到第 1 页 确定 共 6 条 50 条/页

图 54

8.3 诊断工具

诊断工具分为诊断和抓包两部分：

1. **诊断工具**：用来检测网络通信，支持 PING，TELNET，TRACEROUTE，如图 55 所示：



图 55

2.抓包：抓包可以通过设备，网络接口，协议，源 IP 地址，目的 IP 地址和目的端口来进行筛选抓包条件，并可以配置抓包的数量。抓包文件可以删除和下载，。

可使用状态，状态对抓包记录进行筛选。如图 56 所示：

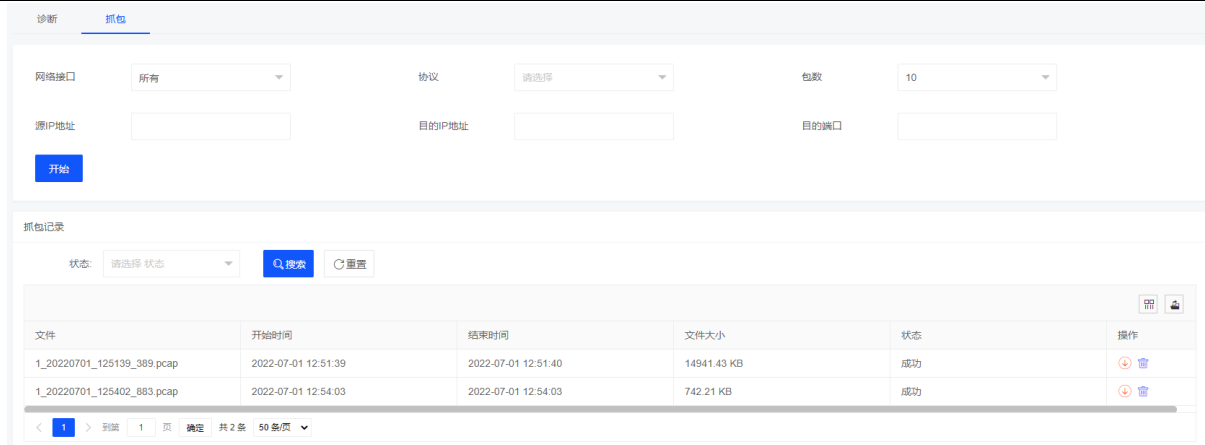


图 56

8.4 连接控制数

策略管理员（secuser）可配置某个 IP 地址的最大连接数及控制连接速率。支持添加、编辑、删除操作。

新建最大连接数控制，点击添加按钮，进入添加界面，最大连接数的设置范围为 100—65535，每秒连接数的设置范围为 10-10000。如图 57 所示：

添加连接数

* IP地址

* 最大连接数

* 每秒连接数

描述

状态 启用

图 57

8.5 账户设置

8.5.1 账户设置

工业防火墙系统是多用户系统。具备用户管理权限的管理员(sysuser, secuser, loguser)可完成对用户的维护工作。如图 58 所示：



图 58

管理员用户(以 sysuser 系统管理员为例)可以删除子用户，但不能自己删除自己及其他管理员用户(secuser 安全管理员和 loguser 审计管理员)。如图 59 所示：

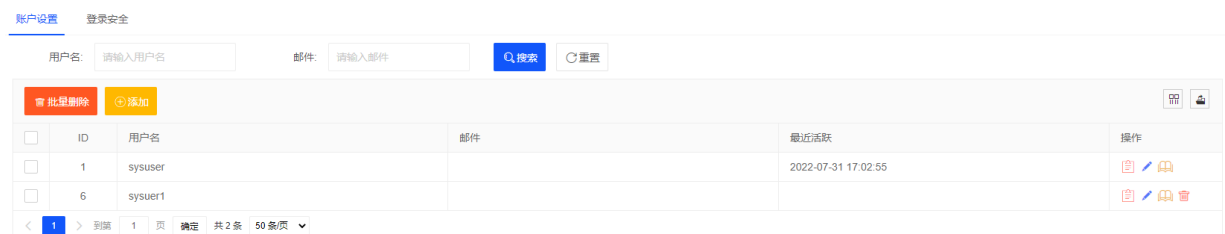


图 59

点击详细可以查看用户的详细信息，并添加用户权限，以 sysuser 为例，如图 60 所示：



图 60

点击添加，可添加子用户并给子用户添加权限，子用户的权限小于等于父用户，如图 61

所示：

添加用户 ✕

* 角色

* 登入名

* 密码


* 确认密码

收件邮箱

用户权限

- 监控中心
- 历史流量
- 网络配置
- 虚拟专网
- 系统管理
- 集中管理

图 61

用户登录需要证书文件, 点击 , 可生成证书文件, 在登录界面导入证书文件进行登录。

8.5.2 登录安全

策略管理员 (secuser) 可通过安全设置进行密码格式设置及密码有效期等设置。如图 62 所

示:

图 62

名称	说明
密码设置	可设置密码限制，包含密码长度
密码有效期时间	用户密码每隔一段时间必须修改，即密码有效期时间
登入超时时间	用户登录 WEB 管理界面后，如果超过一定时间不对界面进行操作，需要重新登录，即登入超时时间
最大重试次数	登录用户名或密码输入错误允许重试次数，超过该次数则登入系统会被禁止（锁定 10 分钟）

注：密码复杂程度不可更改。

8.5.3 三权分立

工业防火墙采用权限分立的用户管理方法，划分了 3 个角色的管理员：

sysuser/secuser/loguser，分别对应着系统管理员、安全管理员、审计管理员三个角色。

系统管理员(sysuser)主要负责对整体工业防火墙运行的维护。

安全管理员(secuser)主要负责对工业防火墙的规则设置和策略管理。

审计管理员(loguser)主要负责对工业防火墙行为进行审计以及分析系统状态。

不同管理员只能添加或编辑自身角色用户信息，而不能修改其他类别的角色用户信息。

使用管理员登录，可创建本权限下的子管理员，并为子管理员分配工业防火墙设备，子管理员仅能查看或者修改其分配的设备。

8.5.4 权限分配

系统管理员(sysuser)及其子管理员可操作的功能模块为：

- ❖ 监控中心
- ❖ 历史流量
- ❖ 网络配置
- ❖ 虚拟专网
- ❖ 系统管理
- ❖ 集中管理

安全管理员(secuser)及其子管理员可操作的功能模块为：

- ❖ 监控中心
- ❖ 历史流量
- ❖ 对象管理
- ❖ 策略管理
- ❖ 防护设置

- ❖ 系统管理
- ❖ 集中管理
- ❖ 日志审计


审计管理员(loguser)及其子管理员可操作的功能模块为:


- ❖ 监控中心
- ❖ 历史流量
- ❖ 系统管理
- ❖ 集中管理
- ❖ 日志审计

注：子管理员在用户功能模块仅能修改自身信息。

8.6 应用配置

添加或者修改规则后，规则不会自动应用到对应工业防火墙设备，而需要手动点击页面

右上角 “等待确认” 查看所有等待处理的事件，如图 63 所示：



事件类型	事件状态	搜索	重置	下发
请选择	等待	Q 搜索	重置	下发
用户名	事件	创建时间	结束时间	状态
<input checked="" type="checkbox"/> superman	系统配置更新	2022-07-31 17:09:23		等待
<input checked="" type="checkbox"/> superman	IP-MAC改变	2022-07-31 16:48:04		等待
<input checked="" type="checkbox"/> superman	网络更新	2022-07-31 15:51:50		等待
<input checked="" type="checkbox"/> superman	VLAN改变	2022-07-31 15:51:50		等待
<input checked="" type="checkbox"/> superman	规则更新	2022-07-31 15:32:58		等待

< 1 > 到第 1 页 确定 共 5 条 50 条/页

图 63

勾选需要提交的事件，点击“下发”按钮，等待显示“配置成功”，即表示此次操作应用成功，如图 64 所示：



图 64

8.7 系统设置

8.7.1 常规选择

系统管理员（sysuser）可对授权信息、设备信息、工作模式进行编辑修改，支持系统升级、整机备份操作。如图 65 所示：

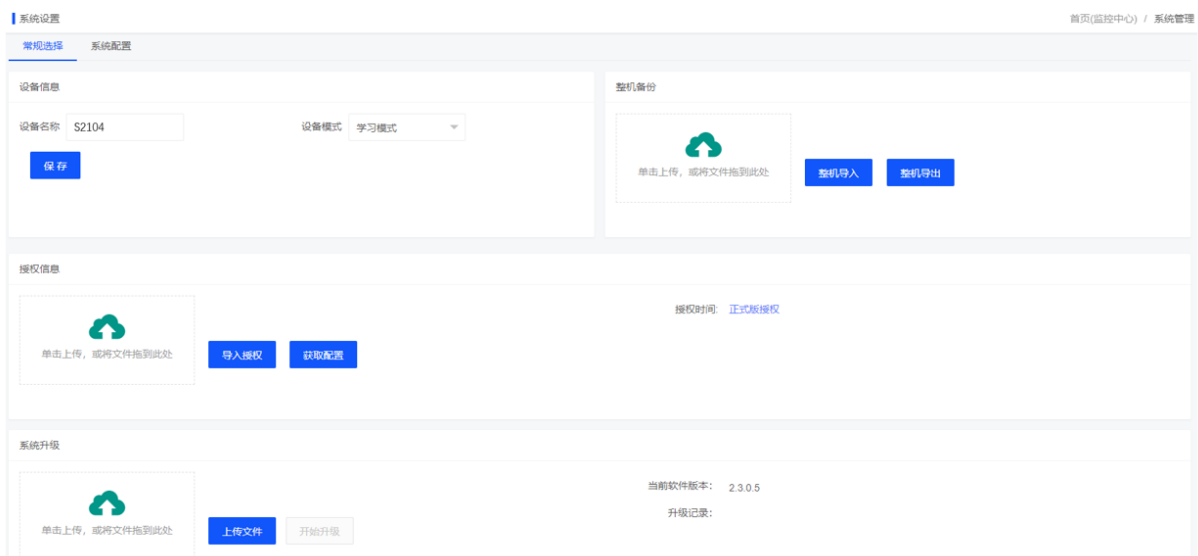


图 65

名称	说明
授权信息	可获取授权配置，并导入授权。同时可查看授权剩余天数
设备信息	可设置设备名称，选择系统语言
工作模式	设备工作模式，支持防护模式、警告模式、学习模式和旁路学习模式四种模式选择
系统升级	可查看当前系统版本、升级记录，并进行版本升级
整机备份	可整机导出备份文件，并整机导入备份文件

8.7.2 系统配置

系统管理员（sysuser）可进行系统配置，配置 Bypass、时间服务器、重启、关机、恢复出厂

和设置向导。如图 66 所示：

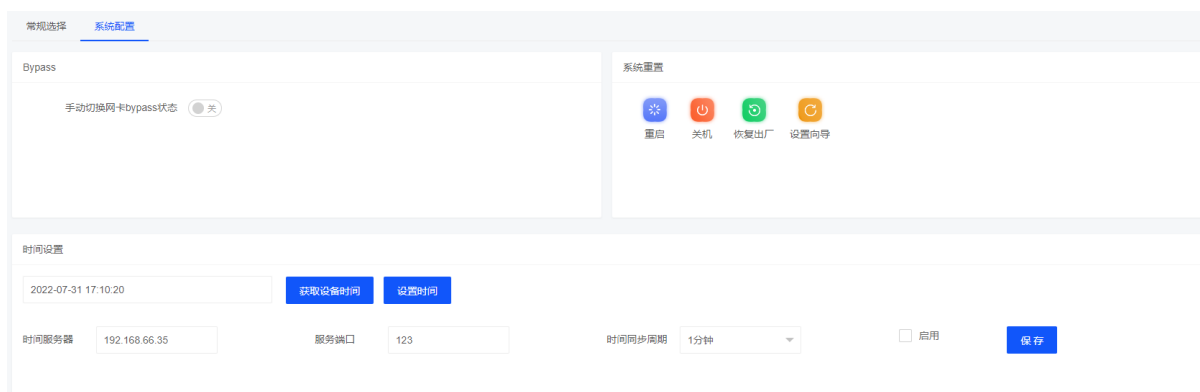


图 66

名称	说明
Bypass	可通过设置手动切换 Bypass 状态, 并选择开启或关闭 Bypass, 关闭 bypass 时不可以进行手动切换
时间设置	可设置时间和获取设备时间, 配置时间服务器、服务端口、时间同步周期和是否启用
重启	点击后可重启工业防火墙系统
关机	点击后可关闭工业防火墙系统
恢复出厂	点击后设备可进行恢复出厂, 除管理口地址其余配置都恢复到出厂状态
设置向导	点击后即进入初始化向导

九、集中管理

9.1 注册列表

工业防火墙集中管理功能是指工业防火墙可作为集中管控端, 部署在其他区域的设备都可以注册集中管理平台, 从而实现集中管理平台对下属设备的管控。

集中管理平台可以实现的功能如下:

1. 查看客户端设备基本信息

注册成功后, 集中管理平台可以查看绑定的客户端设备的基本信息, 包括设备的 IP 地址、设备名称、序列号、授权状态、工作模式、bypass 状态等。

2. 对客户端设备进行基本操作

成功注册的设备，集中管控端可以手动切换 bypass 模式，对设备进行授权及解除注册等操作。在集中管控端的设备资产列表中，还可以实现免密登录访问客户端设备，在展示中心告警列表中，可以通过统计的未处理告警数直接跳转到客户端设备此数据统计页面。

3. 监视客户端设备运行情况及事件信息

成功注册的设备，集中管控端在展示中心可以实时查看 top5 的设备流量情况，告警事件及 top5 的攻击信息，还有设备在线离线情况，设备离线将会有掉线提醒并发出掉线提示音。

● 集中管理端设备手工添加注册

在注册列表界面，可手工添加注册资产，如图 67 所示：

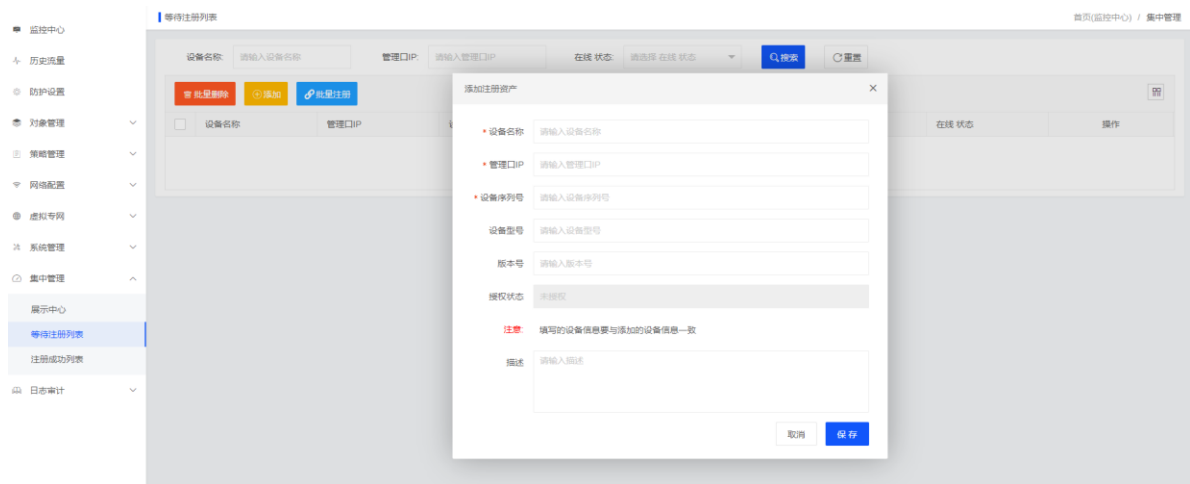


图 67

名称	说明
设备名称	请求注册的设备名称

管理口 IP 地址	请求注册的设备管理口 IP 地址
设备序列号	设备出厂的序列号，设备的唯一标识
设备型号	设备出厂时的型号
版本号	请求注册的设备版本号信息
授权状态	请求注册的设备授权信息，可通过此信息获知设备剩余授权天数
在线状态	请求注册的设备在线状态，即客户端设备是否还在发注册请求，若客户端设备不再向此管理平台发送请求，则状态为离线
操作	可以对请求注册的设备执行接受注册，接受注册则设备添加到注册成功列表

说明：此处手动添加设备资产信息，设备名称、管理口 IP、设备序列号为必填项，其余为选填项，设备序列号作为设备的唯一标识，当有序列号匹配的设备请求注册时，会同步刷新此设备信息。

在等待注册列表界面可以通过设备名称、管理口 IP 和在线状态进行查询，如图 68 所示：

设备名称: 管理口IP: 在线 状态:

图 68

通过注册之后，在注册成功列表中便可看到注册成功的设备情况，并可进行解绑操作和查看基本设置操作。如图 69 所示：



图 69

9.2 展示中心

设备添加到注册成功列表后，展示中心会显示此设备的统计信息。设备资产中

会显示此设备的图标，告警信息统计表中会显示此设备的告警情况。当前风险评估和设

备总流量会统计所有设备的告警 top5 汇总情况及设备总流量排名前 TOP5 的值。如图 70 所

示：



图 70

名称	说明
告警信息	统计所有成功注册设备的告警信息，包括设备名称、IP 地址及告警数，点击对应设备的未告警处理数，可以成功跳转到此设备的告警统计页面
风险评估	当前风险评估汇总所有设备的工业防护警告、网络流量警告、系统防护警告、其他消息的占比情况，当前攻击来源和目的的 TOP5 值是对所有成功注册设备的攻击数量的 TOP5 值汇总情况
设备总流量 TOP5	所有成功注册设备的总流量排名前 5 的汇总情况，可按照近一天、近三天、近 7 天展示流量信息
设备资产	设备成功注册后，设备信息添加到此统计框中，设备图标显示绿色则设备在线，黄色则设备离线，当鼠标点击此设备图标，会成功登录到设备的 web 界面，可对客户端设备进行操作。
掉线提醒	成功注册的设备离线后，会弹出掉线提醒并发出报警声音，可以手动关闭声音最小化此弹窗，设备重新上线后此提醒关闭。

十、 日志审计

10.1 防护日志

防护日志显示设备记录的防护日志信息分类(分为警告和错误和提示)及当天防护日志分布情况（分为工控事件、网络事件、放行正常协议、其他事件）。查看防护日志信息，可根据

源目 IP、端口及协议类型、时间段、日志级别等来筛选要查看的信息。并可标记所选项为已读或当前页为已读状态。支持防护日志的删除及情况操作。如图 71 所示：

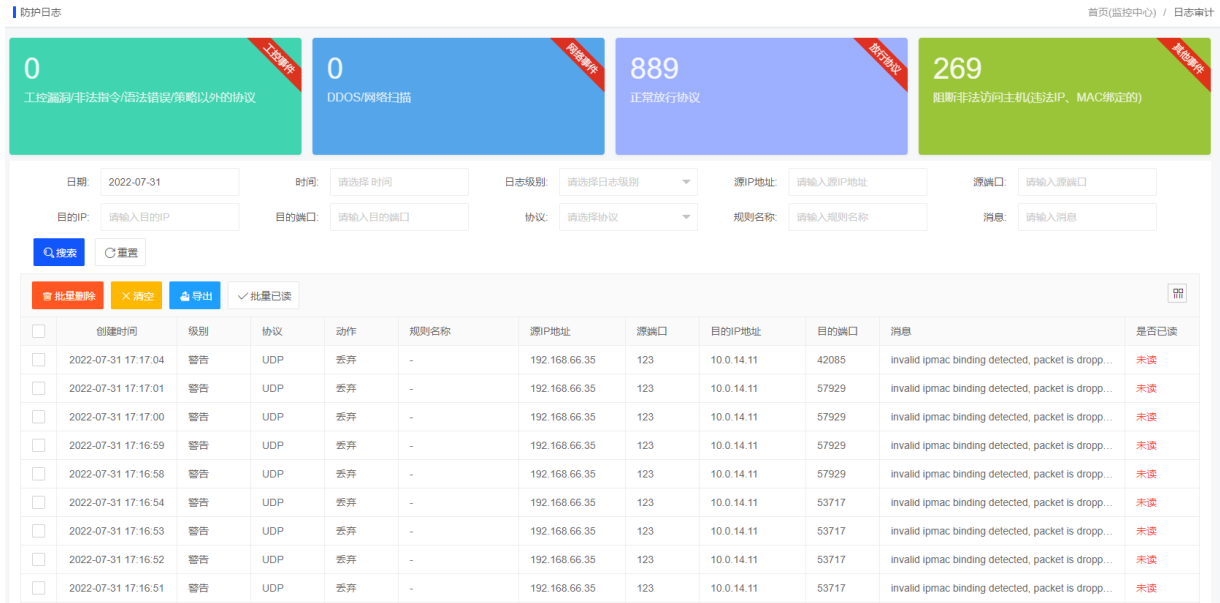


图 71

10.2 系统日志

系统日志包括所有工业防火墙设备的系统日志信息分类(分为警告和错误和提示)查询。可通过查询时间、日志级别、分类信息、消息查询系统日志情况，支持系统日志的删除及清空操作。如图 72 所示：

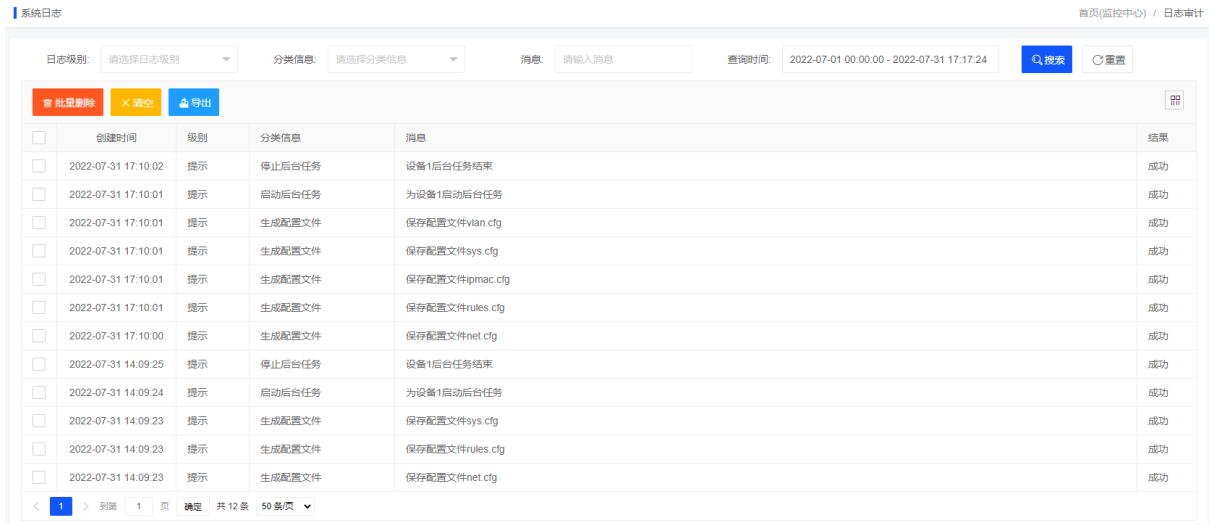


图 72

10.3 管理日志

管理日志包括所有工业防火墙设备的管理日志信息分类(分为警告和错误和提示)查询。可通过用户类别、登录 IP 地址、日志信息级别、时间条件、消息等筛选查看管理日志信息，支持管理日志的删除及清空操作。如图 73 所示：



图 73

十一、 附录 A

恩创工业防火墙常见问题解答：

11.1 无法打开 WEB 管理页面怎么办？

答：检查工业防火墙设备与客户机通信是否通过 MAN 口来连接。

设备默认管理地址为 192.168.1.254，请确认登陆 PC 的 IP 地址是否在同一网段

客户端电脑 Ping 测试 WEB 管理界面的 IP 地址是否 Ping 通。

如还是无法打开 WEB 管理界面，请随时发邮件至 sales@n-tron.com.cn 或者拨打 24 小时

客服热线：010-82859971。

11.2 打开 WEB 管理界面显示白屏怎么办？

答：更换使用的浏览器（最好使用 Chrome 或 Firefox）。

如还是白屏请随时发邮件至 sales@n-tron.com.cn 或者拨打 24 小时客服热线：010-

82859971。

11.3 学习到的规则应用后，业务处理中断怎么办？

答：检查应用的规则的详情，确保包含通信的命令，还可以手动添加规则确保业务正常通信。

如还是出现异常请随时发邮件至 sales@n-tron.com.cn 或者拨打 24 小时客服热线：010-

82859971。