奇固科威 HKW-IDS2000 网络入侵检测系统
用户手册 V1.8.11

杭州奇固科威信息安全技术有限公司

2024 年 8 月

目 录

1 登录界面

默认登录地址为 https://192.168.0.177，进入登录界面。

管理员：用户名 admin，密码 Linkqi@123

本系统分为两种权限：管理员、操作员，审计员

管理员主要系统的配置、管理。

配置项	说明
账号	用户账号
密码	用户密码（由数组大小写字母特殊符号，最少三种以上组合方式，长度为 6-16 位）
选择证书文件	当前用户生成证书并开启证书认证后，该项为比传项

2 主界面

2.1 首页

权限:(管理员，操作员，审计员)

首页主要对系统的信息、系统资源数据、最近告警事件、告警事件风险等级以及网络接口状态数据做一个快速展示。

页面模块	字段	说明
系统信息	产品型号	用户账号
	系统时间	当前系统时间
	软件版本	当前软件版本
	运行时间	当前服务运行时长
	发布时间	当前版本的发布日期
	操作系统	当前的操作系统
	授权截止日期	软件的授权截止日期
	管理口 IP	当前服务管理口 IP（可以在接口管理中管理口接口中配置）
系统资源		主要对系统的内存 CPU 硬盘，实际使用情况做实时展示
入侵告警	事件类型	-
	事件名称	-
	风险等级	风险等级分为高、危、中、低、非攻击
告警事件风险等级		根据最近时间段分析攻击风险进行分析等级划分
网口接口状态		当前所有网口的状态

系统信息

对当前系统的产品型号、版本、发布时间、授权日期等展示

系统资源

实时展示系统的内存、cpu、硬盘的使用情况

入侵告警

入侵告警只对最新的六条数据做展示，如果您期望看到更多，点击更多跳转入侵告警详情即可

告警事件风险等级

根据最近时间段分析攻击风险根据最近时间段分析攻击风险进行分析等级划分，右上角提供

时间选择，详情功能

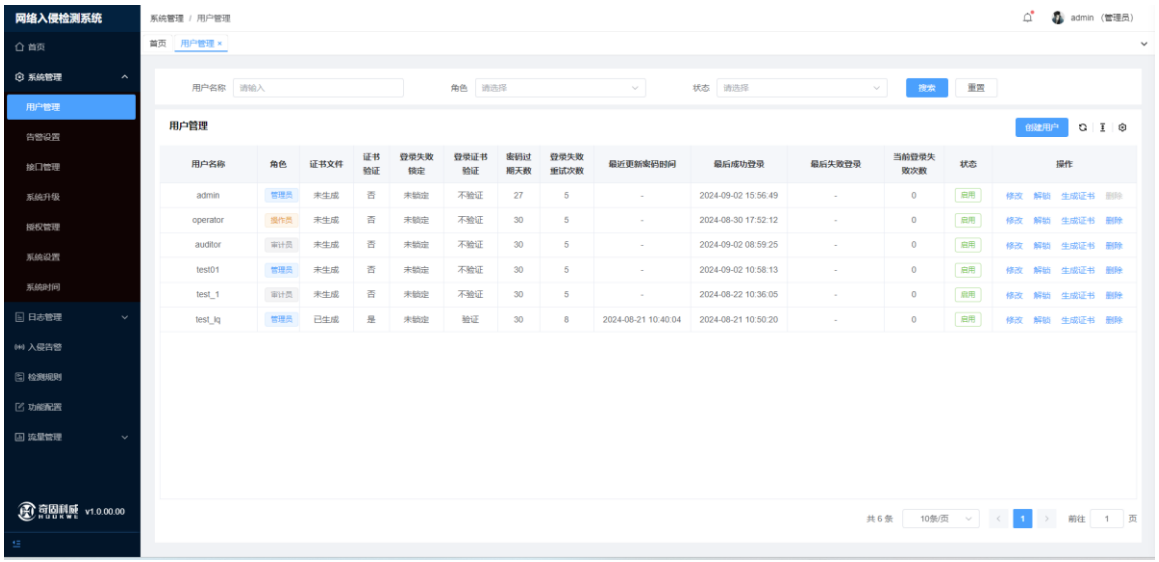
网络接口状态

当前所有网口的状态、右上角提高前往**设置**界面功能

2.2 系统管理

2.2.1 用户管理

权限:(管理员)



管理当前系统下所有的用户，并拥有创建、修改、解锁生产证书、删除功能

功能	说明
创建用户	创建新的用户账号

修改	修改用户信息
解锁	当用户的登录错误上限后，账号就会被锁定
生成证书	我们可以通过生成证书，并在编辑中开启证书认证，从而提升账户的（重复生成证书会覆盖之前的证书）
删除	删除用户

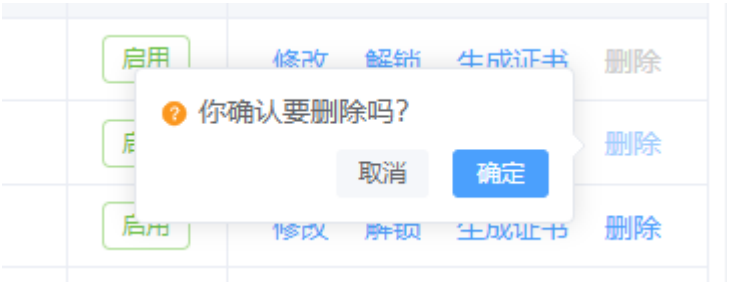
创建用户

配置项	说明
用户名称	新的用户账号（采用数字大小字母特殊符号（_.@）组合），长度为 3-16 位
密码	用户密码（由数组大小写字母特殊符号，最少三种以上组合方式，长度为 6-16 位）
确认密码	当用户的登录错误上限后，账号就会被锁定
角色	管理员，操作员，管理员

编辑用户

配置项	说明
用户名称	**不可修改**
密码过期天数	用户密码（由数组大小写字母特殊符号，最少三种以上组合方式，长度为 6-16 位）
登录失败重试上限	当用户的登录错误上限后，账号就会被锁定
状态	默认开启，关闭后用户无法登录
证书验证	生成证书后，可以更改证书验证是否启动，默认关闭

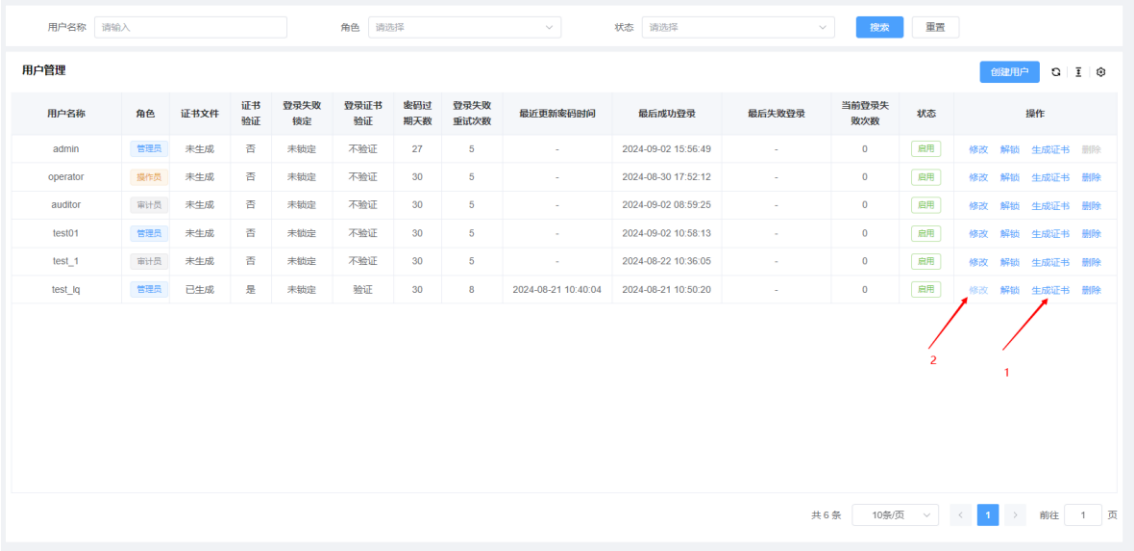
删除用户

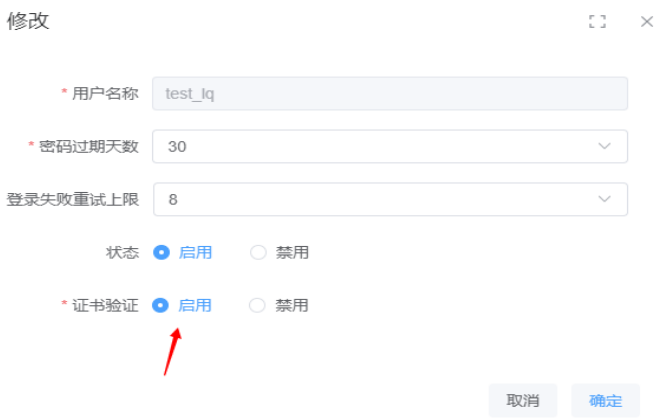


证书

如果希望安全登录使用，可以采取采方式，

1. 生成证书（注：生成证书后会下载一个文件，该文件请妥善保管，后续如修改证书认证，那么则需要上传认证，才可登录）
2. 修改证书验证即可

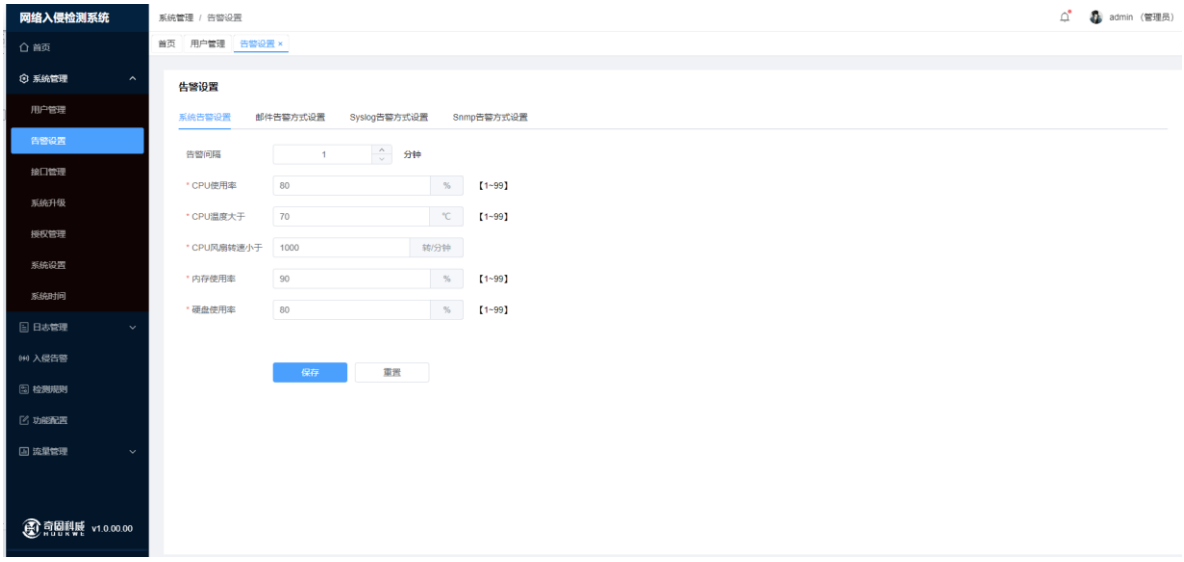




解锁 （如账户多次登录被锁定，则需要登录其他管理账户来解锁才可以继续使用）

2.2.2 告警设置

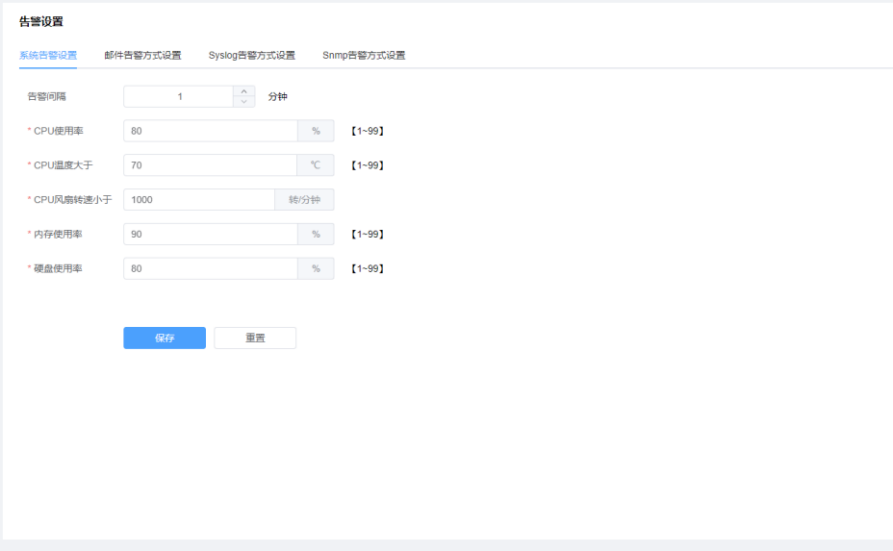
权限:(管理员)



主要对系统的 cpu 使用率，温度，风扇，内存使用率，硬盘使用率，进行配置，如果超出设置上限，则开始告警通知。

功能	说明
系统告警设置	主要对系统的 cpu 使用率，温度，风扇，内存使用率，硬盘使用率，进行配置，如果超出设置上限，则开始告警通知。
邮件告警方式设置	配置后，当出现系统资源告警和入侵告警时，会将通知，推送到对应的邮箱上
syslog 告警方式设置	配置后，当出现系统资源告警和入侵告警时，会将通知，推送到对应的邮箱上
snmp 告警方式设置	配置后，当出现系统资源告警和入侵告警时，会将通知，推送到对应的邮箱上

2.2.2.1 系统告警设置



主要对系统的 cpu 使用率，温度，风扇，内存使用率，硬盘使用率，进行配置，如果超出设置上限，则开始告警通知，设置完成后点击保存

配置项	说明
告警间隔	1-99 分钟
CPU 使用率	1~99
CPU 温度大于	1~99
CPU 风扇转速小于	最小值 1000
内存使用率	1~99
硬盘使用率	1~99

2.2.2.2 邮件告警

配置后，点击保存，当出现系统资源告警和入侵告警时，会将通知推送到对应的邮箱上，

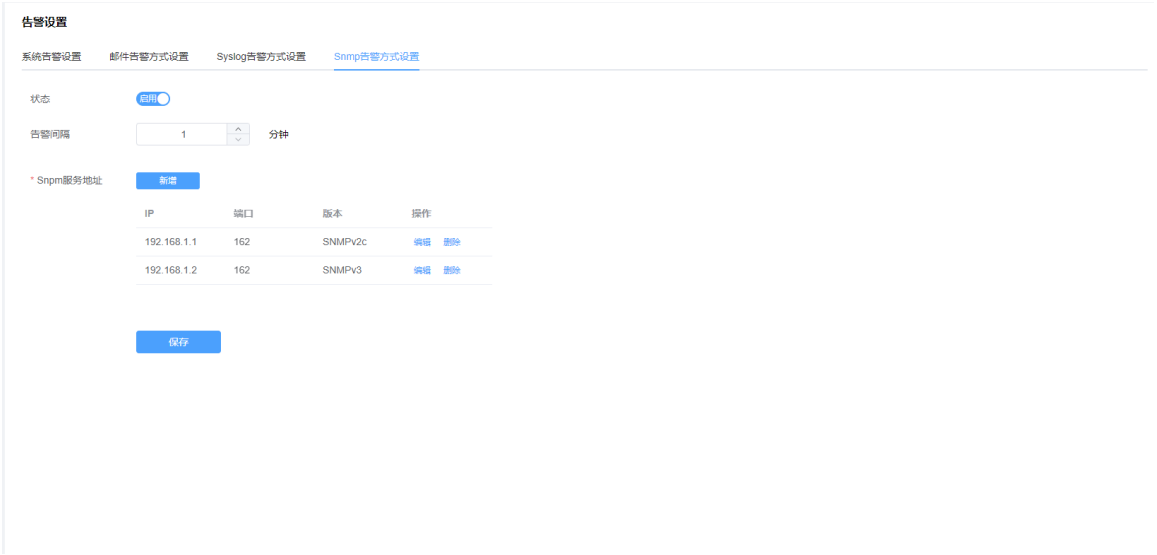
配置项	说明
告警间隔	1-99 分钟
地址	smtp 的服务地址
端口	默认 465
需要身份验证	开启后需要用户名，密码认证
用户名	-
密码	-
发送者	发送人邮箱
邮件标题	邮件的标题
接受者	当出现资源告警，入侵告警后通知的邮箱

2.2.2.3 Syslog 告警方式设置

点击状态为启用，再将其他配置项 完成填写后，点击保存。当出现系统资源告警和入侵告警时，会将通知推送到对应的 Syslog 服务上

配置项	说明
配置文件	
状态	是否使用，默认关闭
告警间隔	1-99
syslog 服务地址	syslog 的服务地址（上限为 5 个，不可重复）

2.2.2.4 Snmp 告警方式设置

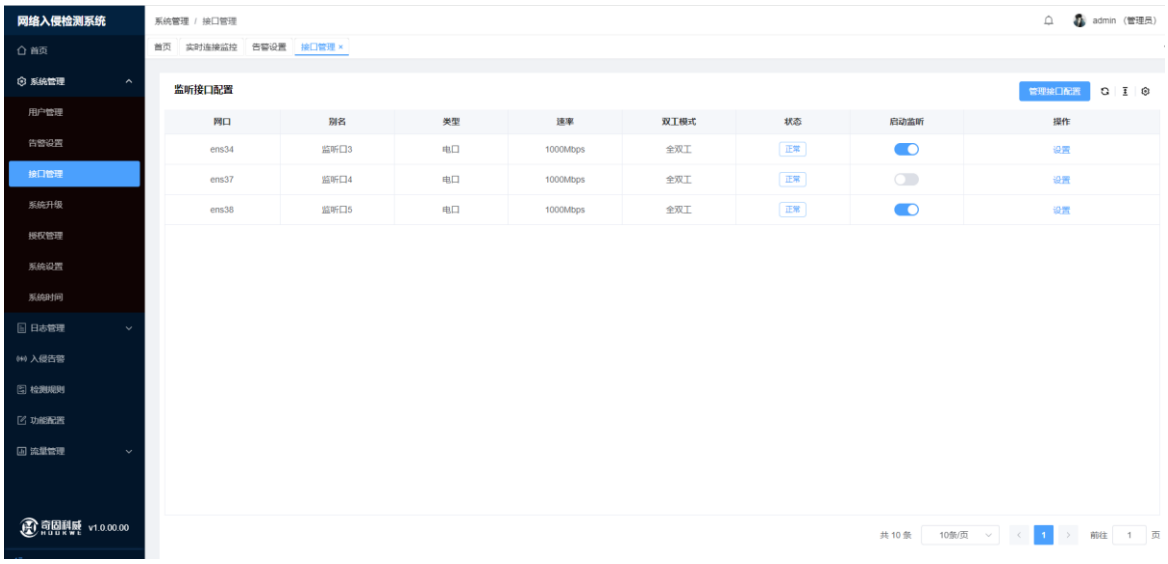


点击状态为启用，再将其他配置项 完成填写后，点击保存。当出现系统资源告警和入侵告警时，会将通知推送到对应的 snmp 服务上

配置项	说明
状态	是否使用，默认关闭
告警间隔	1-99
snmp 服务地址	snmp 的服务地址（上限为 5 个，不可重复）

2.2.3 接口管理

权限:(管理员)



接口管理主要是围绕网口进行管理配置

功能	说明
管理接口配置	通过配置管接口用来配置当前系统的 IP 配置
启动监听	启动后会启动入侵检测和审计检引擎（实际根据功能配置），对当前网口上的所有数据包（实际根据功能配置），进行检测
设置	针对当前网口进行配置

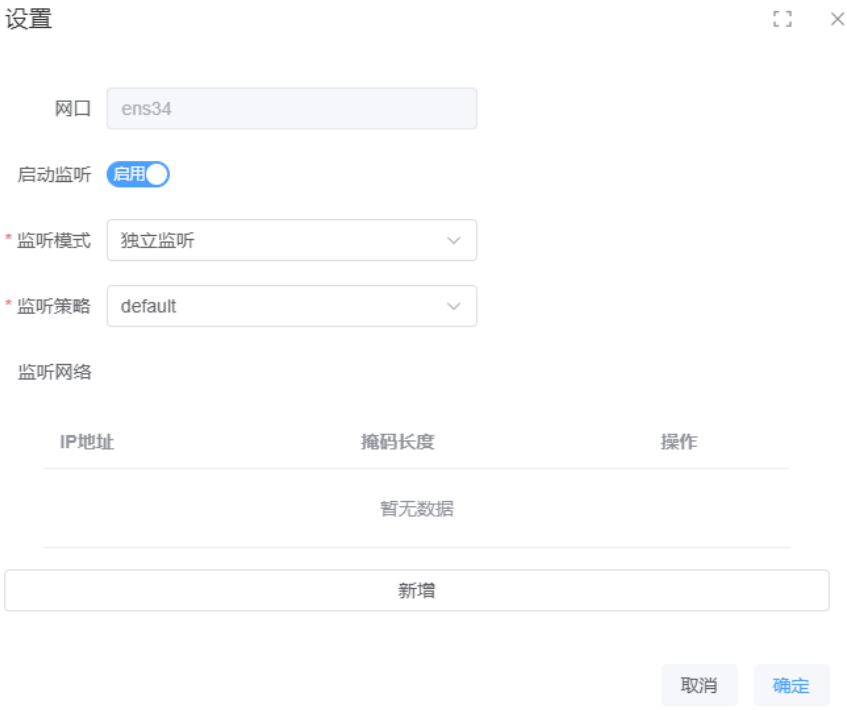
管理接口配置

点击管理接口配置，弹出对话框，填写完成后，点击保存。保存完成后当前配置立即生效，然后通过你配置的新地址打开网页即可

通过配置管接口用来配置当前系统的 IP 配置

设置

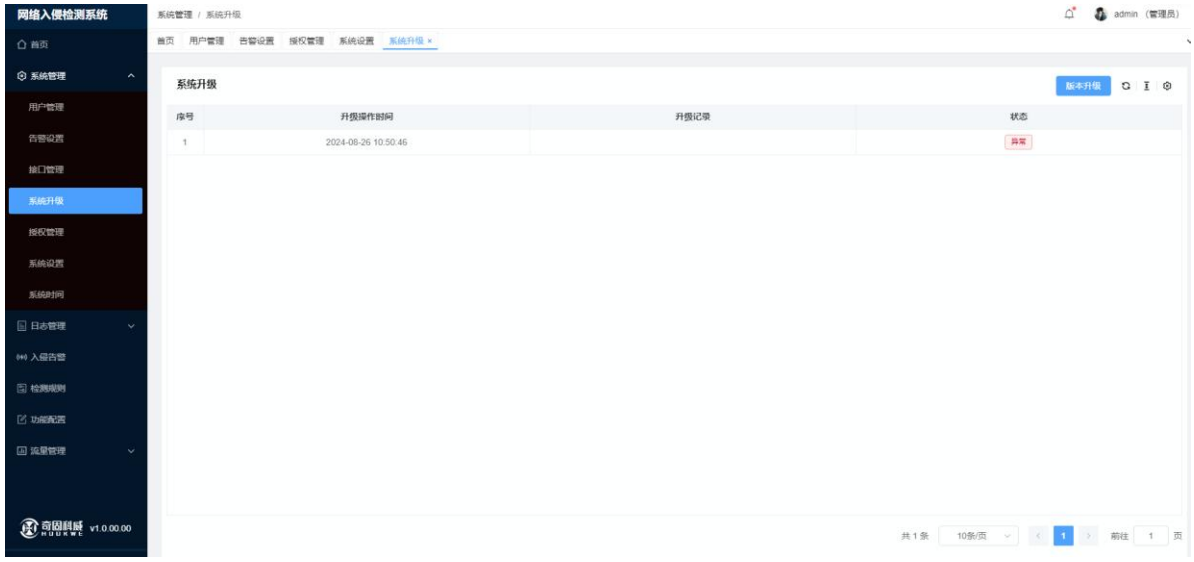
点击列表设置、弹出对话框，即可对当前网口进行配置，配置完成后点击保存（详细请看配置项）



配置项	说明
网口	-
启动监听	启动后会启动入侵检测和审计检引擎（实际根据功能配置），对当前网口上的所有数据包（实际根据功能配置），进行检测
监听模式	可以对当前网口进行独立监听，亦或者和其他网口进绑定桥接
监听策略	主要是对当前网口的入侵检测的规则集进行修改
监听网络	不指定则是所有数据包，如果指定了只会对当前指定的网络进行检测

2.2.4 系统升级

权限:(管理员)



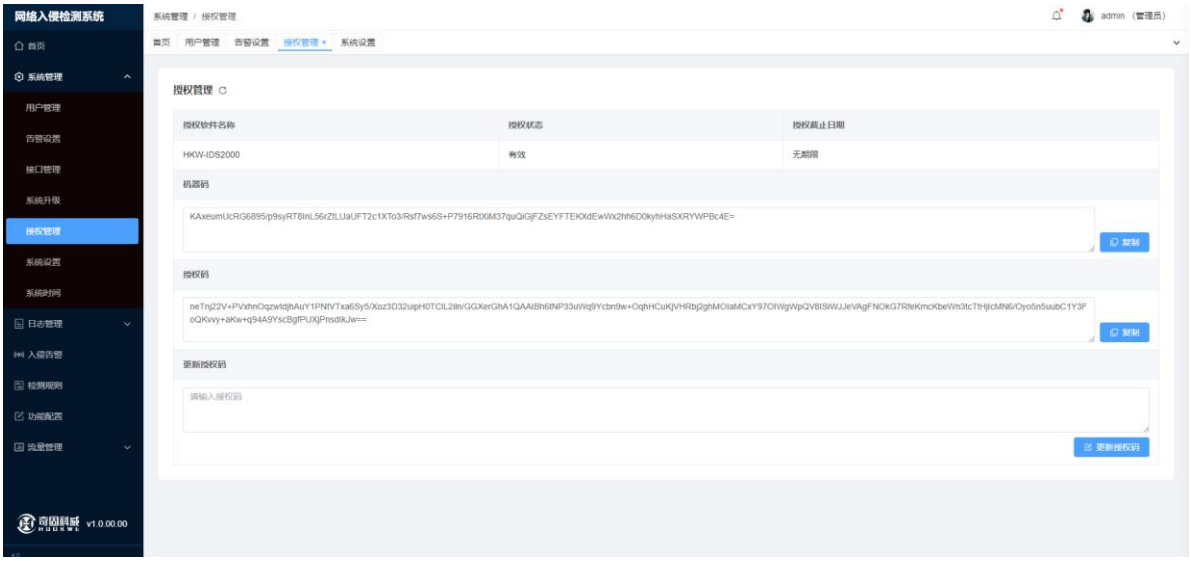
功能	说明
版本升级	上传升级包，成功后等待 30s，后刷新网页即可

版本升级

系统升级可以对历史的升级情况进行查看那，点击版本升级，上传升级包，成功后等待 30s，后刷新网页即可

2.2.5 授权管理

权限: (管理员)

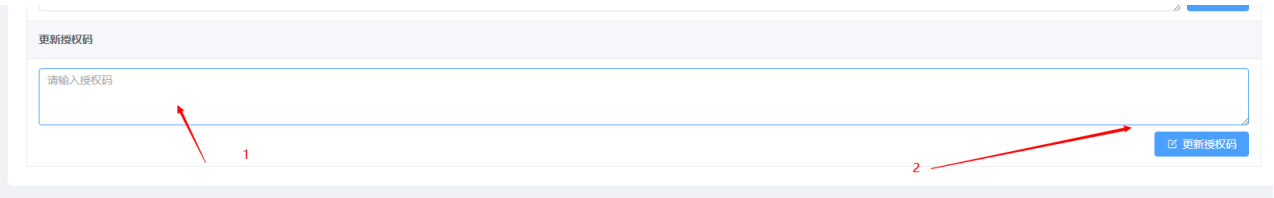


可以对当前的授权状态，授权截止日期等进行查看，

功能	说明
更新授权	首次登录系统需要授权，授权成功后才可以使用所有功能

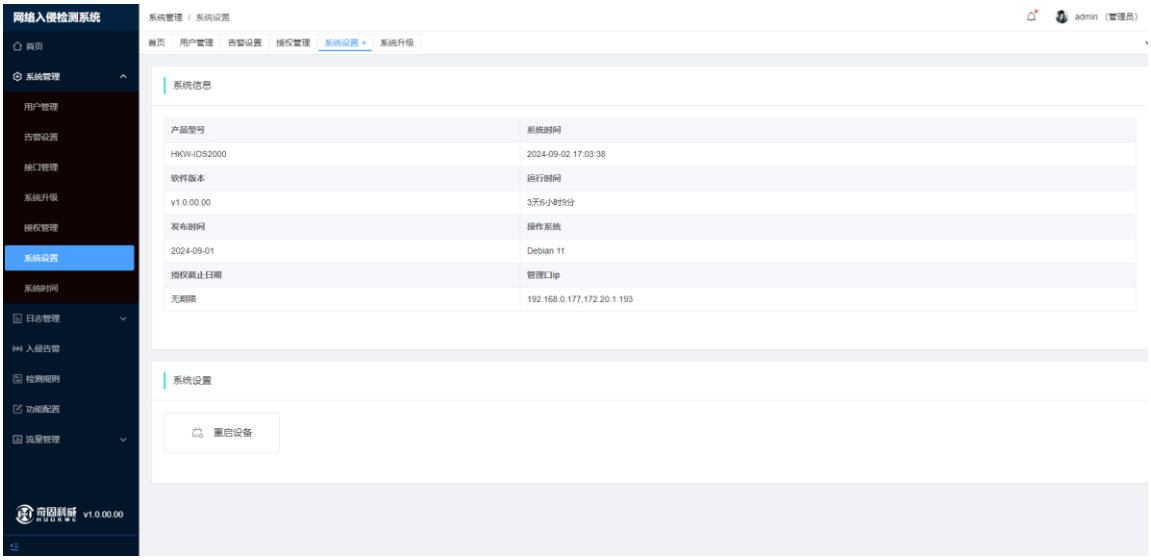
更新授权

将授权码复制到更新授权码中，点击更新授权码，即可完成授权，授权完成后需重新登录



2.2.6 系统设置

权限: (管理员)



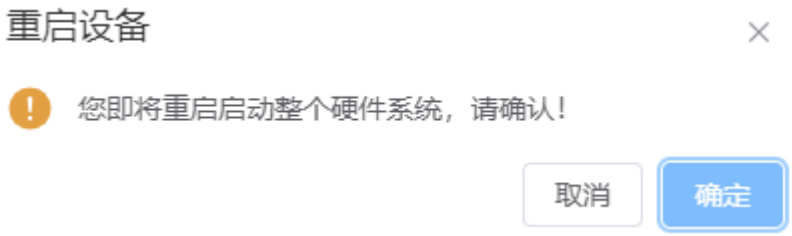
主要是对当前系统信息进行查看，以及重启设备

功能	说明
重启设备	重启设备，成功后等待，后刷新网页即可

页面模块	字段	说明
系统信息	产品型号	用户账号
	系统时间	当前系统时间
	软件版本	当前软件版本
	运行时间	当前服务运行时长
	发布时间	当前版本的发布日期
	操作系统	当前的操作系统
	授权截止日期	软件的授权截止日期
	管理口 IP	当前服务管理口 IP（可以在接口管理中管理口接口中配置）

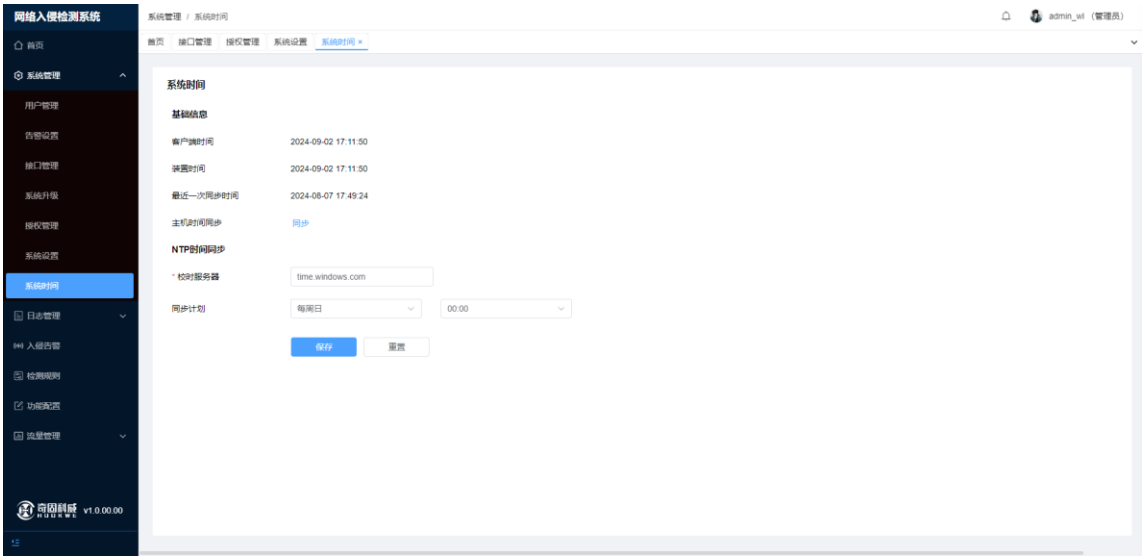
重启设备

点击重启设备，弹出对话框。确认后成功后等待，后刷新网页即可



2.2.7 系统时间

权限: (管理员)



主要对系统时间进行同步

功能	说明
同步	点击主机时间同步，将客户端时间同步到装置
NTP 时间同步	可以通过配置 NTP 时间同步，通过配置校时服务器进行定时同步（推荐）

同步

点击主机时间同步，将客户端时间同步到装置

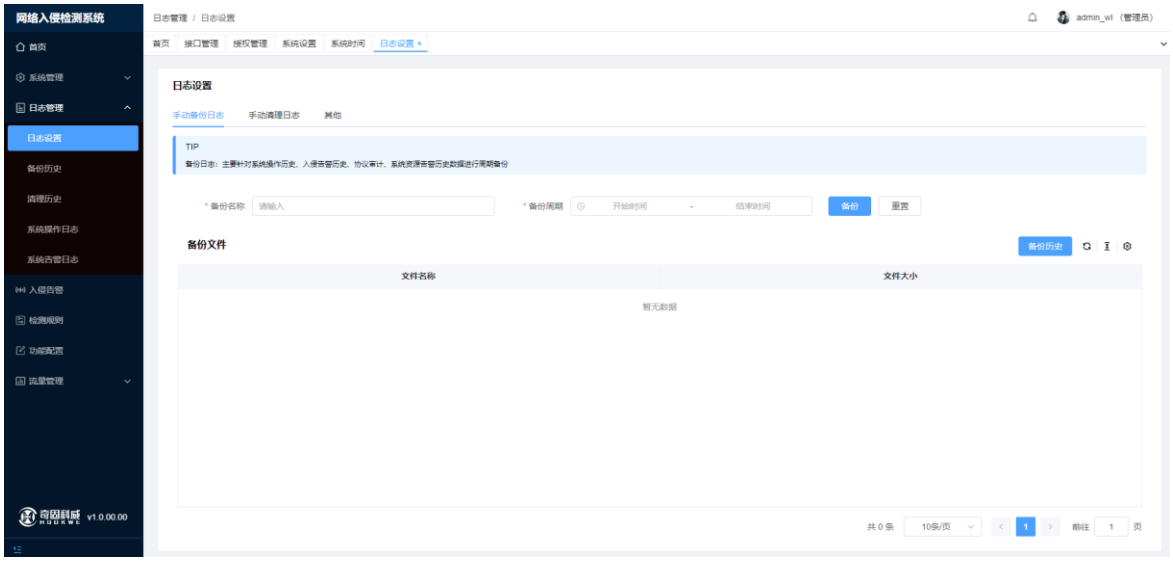
NTP 时间同步

填写校时服务器地址，并设置同步计划，完成后保存

2.3 日志管理

2.3.1 日志设置

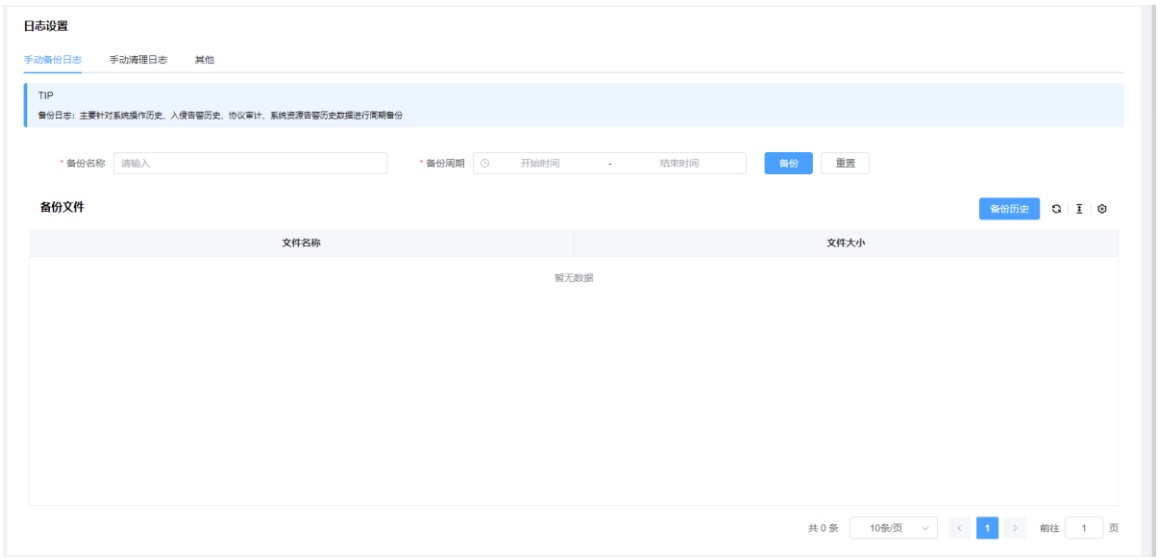
权限:(管理员，操作员)



主要是用于手动备份清理日志以及自动备份清理日志的，

功能	说明
手动备份份日志	对系统操作历史、入侵告警历史、协议审计、系统资源告警历史数据进行周期备份，备份成功后去备份历史下载
手动清理日志	对协议审计数据、资源告警数据、入侵告警数据、备份文件的数据进行周期清理
其他	通过时间自动备份清理日志，也可以将日志备份到远程服务器

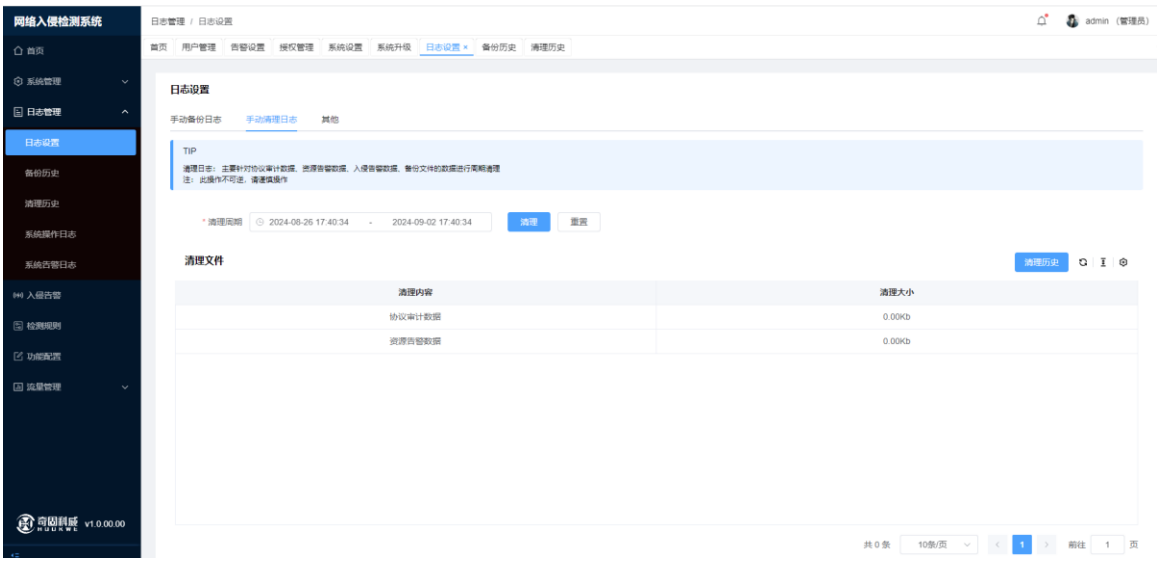
2.3.1.1 手动备份日志



通过配置备份名称以及备份周期，点击**备份**后即可操作成功，操作成功后将您备份的内容展示到列表当中，（备份数据可以通过备份历史去下载）

配置项	说明
备份名称	-
备份周期	通过选择的周期，会对这个时间范围内的操作历史、入侵告警历史、协议审计、系统资源告警历史数据进行周期备份

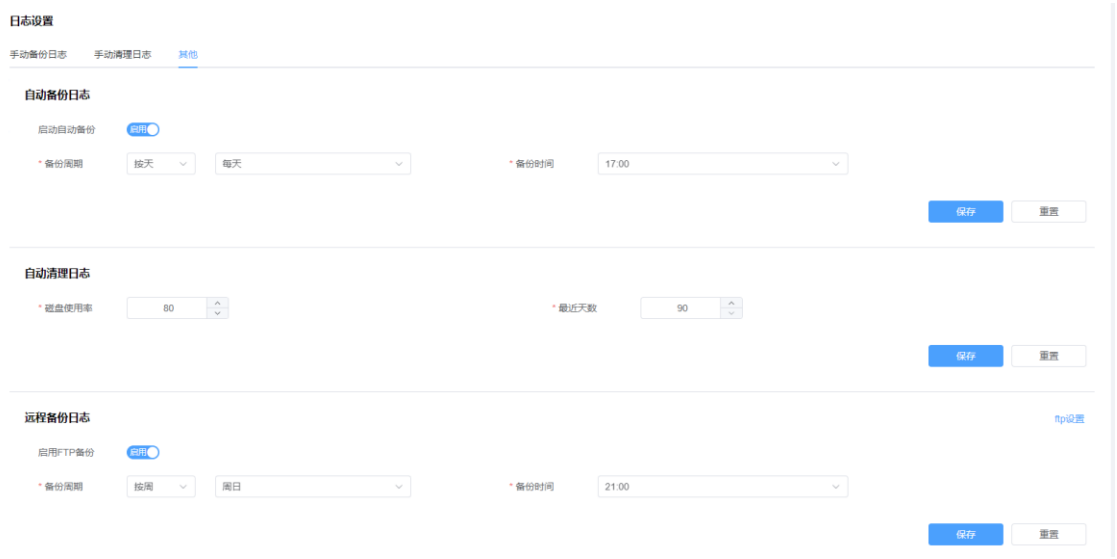
2.3.1.2 手动清理日志



通过配置清理周期，点击**清理**后即可操作成功，操作成功后将您清理的内容展示到列表当中

配置项	说明
清理周期	协议审计数据、资源告警数据、入侵告警数据、备份文件的数据进行周期清理

2.3.1.3 其他



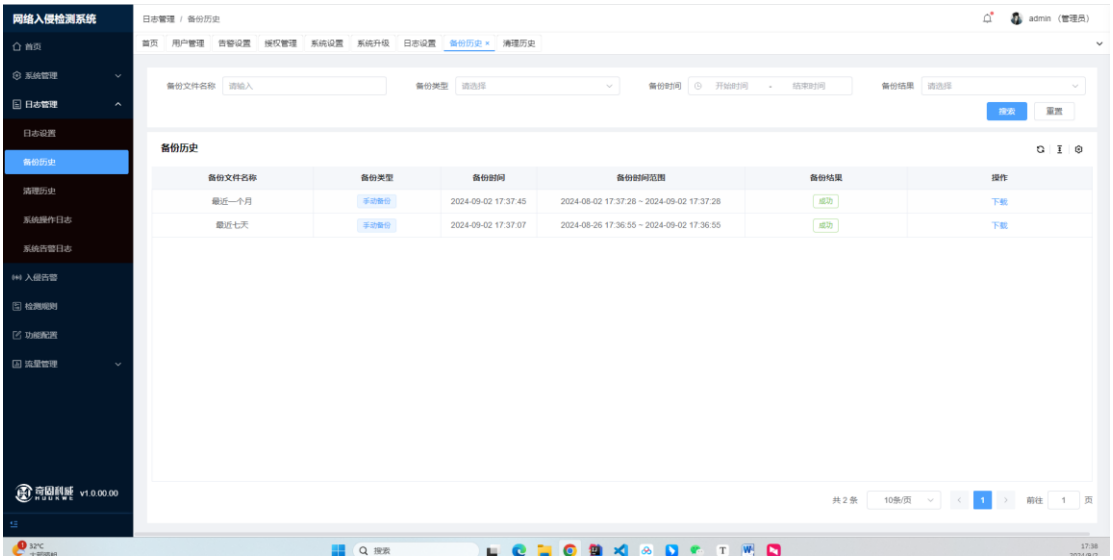
我们还提供了定时操作，通过配置对应的参数，达到清理以及备份的效果 （备份的结果会出现在备份历史，可以通过备份历史去下载对应的内容）

模块	配置项	说明
自动备份日志	启动自动备份	启动后将会按照指定的备份周期时间，定时备份
	备份周期	提供按天、按周、按月的 方式进行备份
	备份时间	-
自动清理日志	磁盘使用率	80-100（%）
	最近天数	90-365（天）
远端备份	启动 FTP 备份	启动通过配置 FTP 会备份到对应的服务器上
	备份周期	提供按天、按周、按月的 方式进行备份
	备份时间	-
	服务器地址	**ftp 的地址**
	端口	-

	用户名	-
	密码	-
	路径	默认路径为当前用户目录（home）

2.3.2 备份历史

权限:(管理员，操作员)



备份类似记录，可以对之前备份内容下载

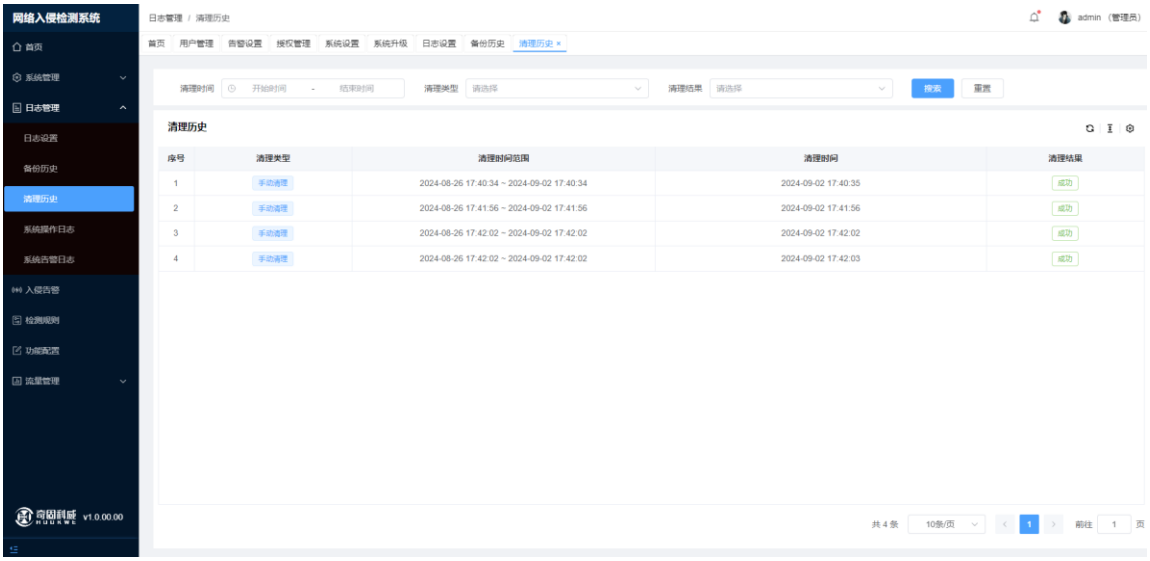
功能	说明
下载	可以下载备份过的内容（注：如果被清理则无法下载）

下载

点击**下载**，弹出对话框确认下载，即可下载，弹出提示框后下载完成

2.3.3 清理历史

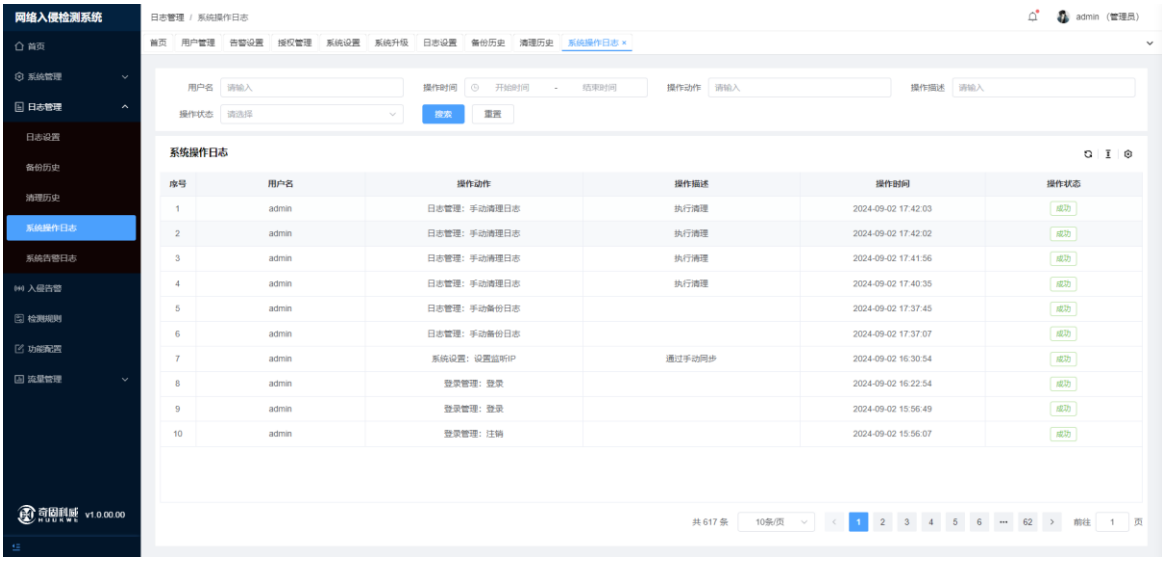
权限:(管理员，操作员)



对对清理历史进行记录

2.3.4 系统操作日志

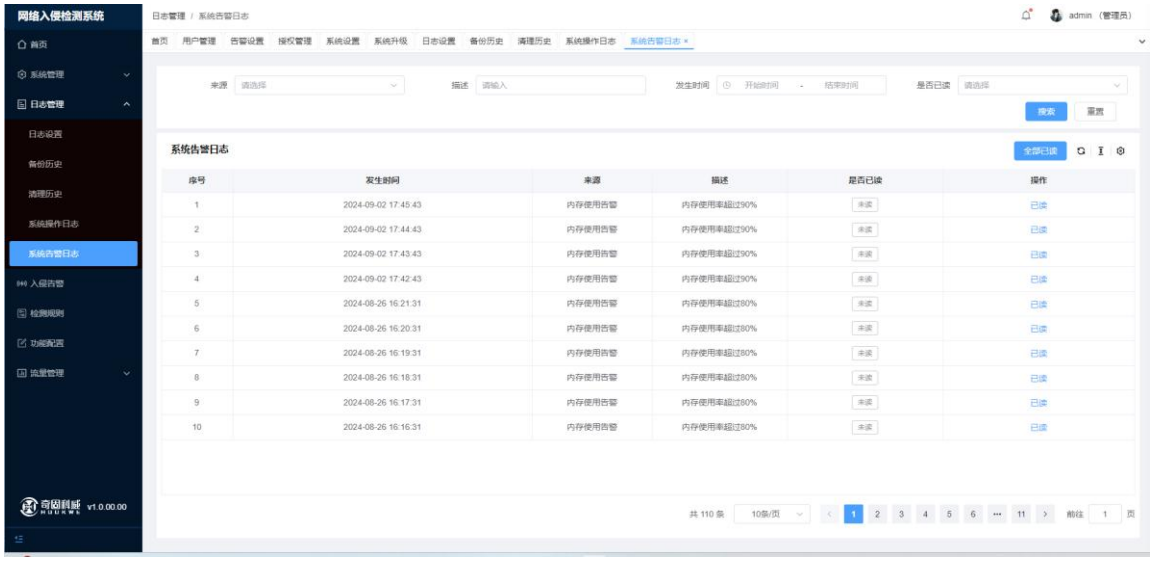
权限:(管理员，操作员)



主要对用户的操作进行记录

2.3.5 系统告警日志

权限:(管理员，操作员)



根据在**系统管理=>告警设置中=》系统告警设置** 的配置来告警， 当超出范围后将告警日志在此片展示

功能	说明
全部已读	读取所有系统告警
已读	读取当前这条系统告警

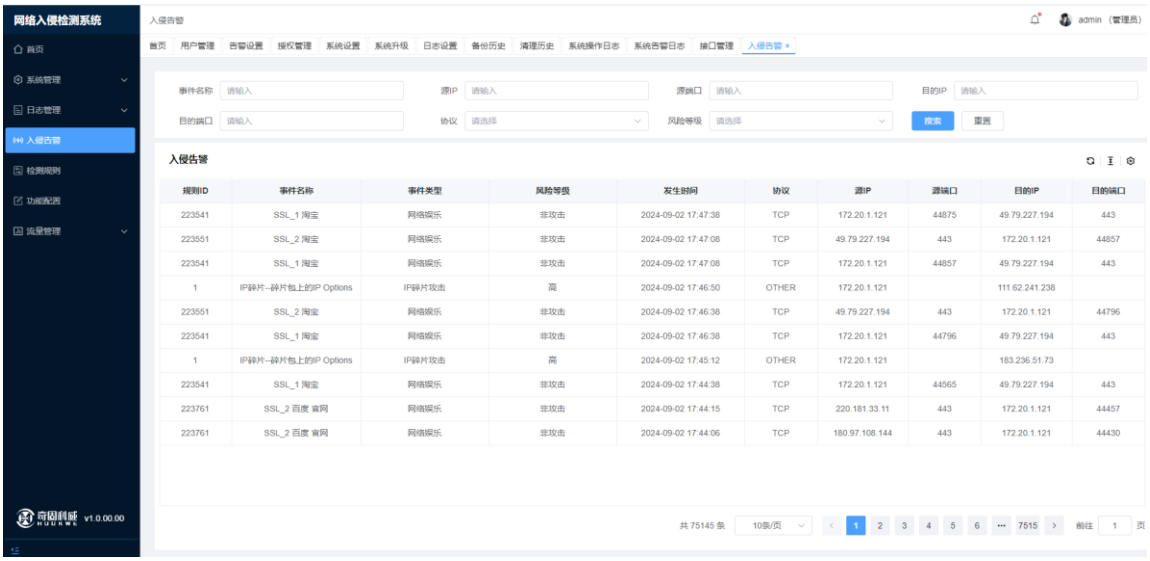
全部已读

点击全部已读后会读取所有的系统告警

点击列表**已读** 读取当前这条系统告警

2.4 入侵告警

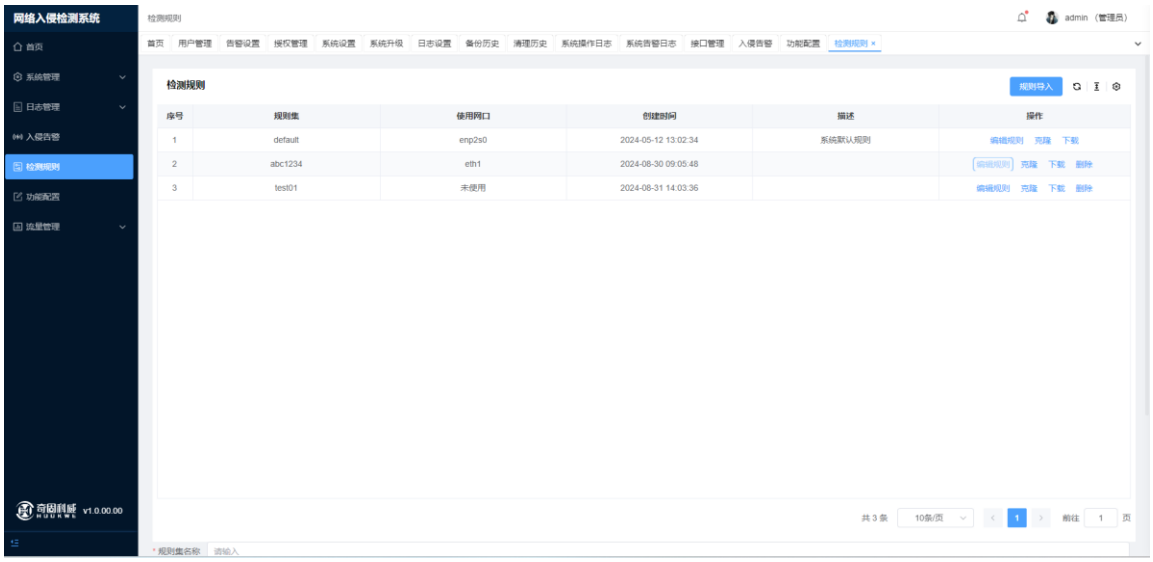
权限:(管理员，操作员，审计员)



当我们给网口配置了对应的检测规则后，会对网口所有数据包做分析，做规则匹配并对风险进行分析评估

2.5 检测规则

权限:(管理员，操作员)

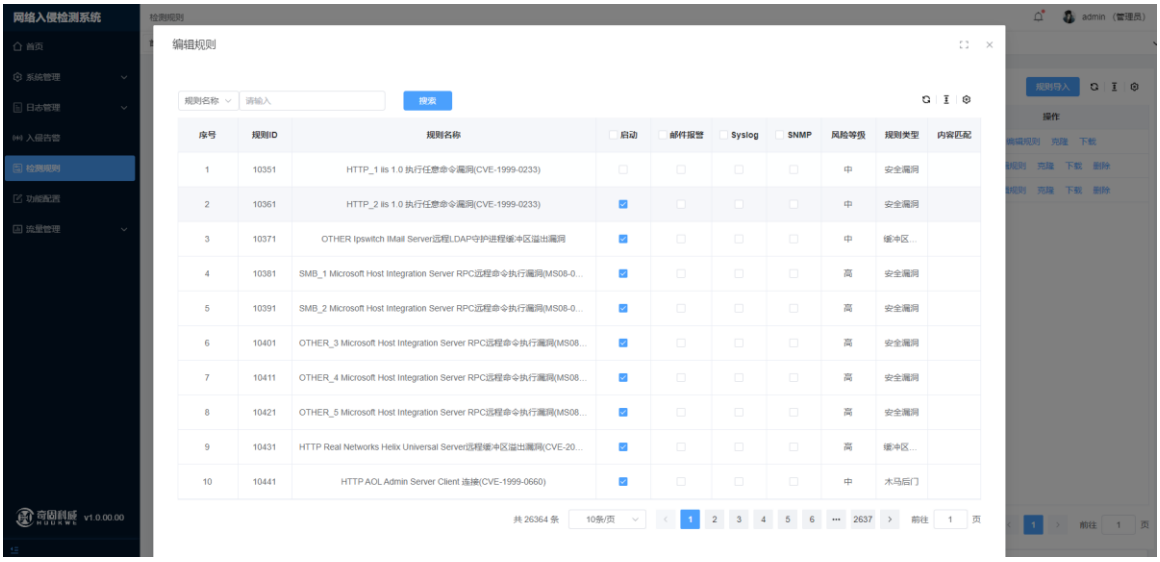


检测规则主要是用来收录我们的规则集的，通过规则来匹配网口的数据，从而做出分析。

功能	说明
编辑规则	修改规则规则集，可以对规则进行启动关闭以及通知
克隆	克隆当前规则集
下载	下载当前规则集文件
删除	删除当前规则集（default 系统默认规则集无法删除）
规则导入	导入新的规则集文件

编辑规则

点击列表**编辑规则**按钮，弹出对话框，你可以对规则是否启用以及通知方式进行修改



克隆

点击列表**克隆**按钮，弹出对话框，我们也自定义规则集内容（基于克隆对象），可以配置不同的规则集

2.6 功能配置

权限:(管理员，操作员)

主要是围绕我们的入侵检测以及审计检测来进行过滤配置

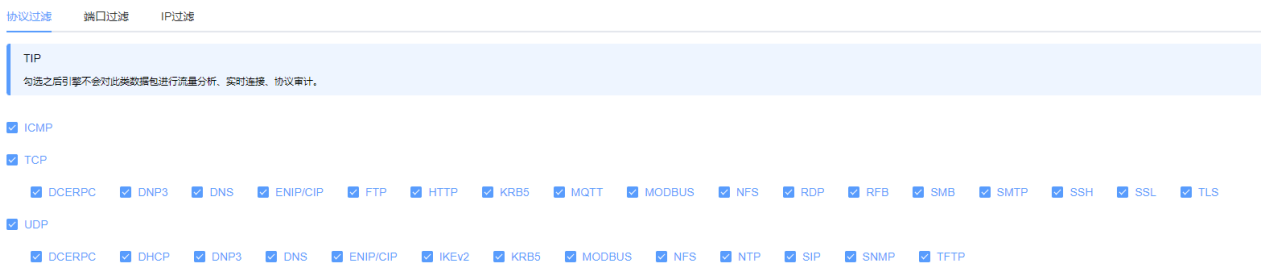
功能	说明
检测配置	控制入侵检测，审计检测是否开启
协议过滤	审计检测时对当前配置的协议进行过滤，影响流量分析、实时连接、协议审计
端口过滤	审计检测时对当前配置的协议进行过滤，影响流量分析、实时连接、协议审计
IP 过滤	审计检测时对当前配置的协议进行过滤，影响流量分析、实时连接、协议审计

检测配置

是否入侵检测： 开启后网口就会对每个数据包进行分析
是否审计检测： 开启后会进行流量统计，协议分析

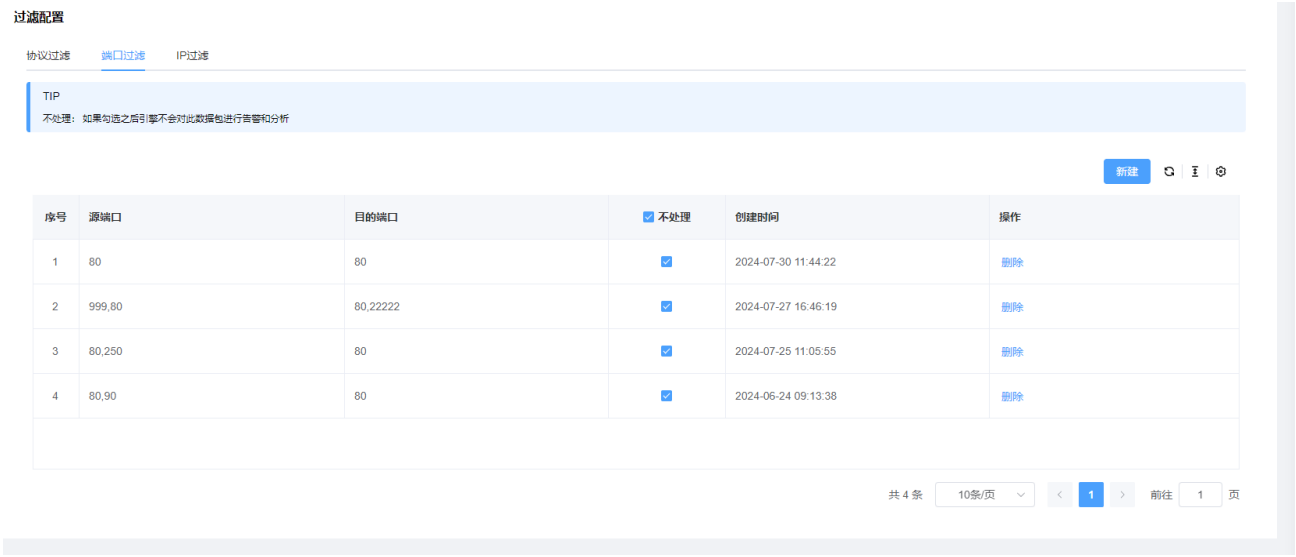
协议过滤

审计检测时对当前配置的协议进行过滤，点击**勾选**后即可生效



端口过滤

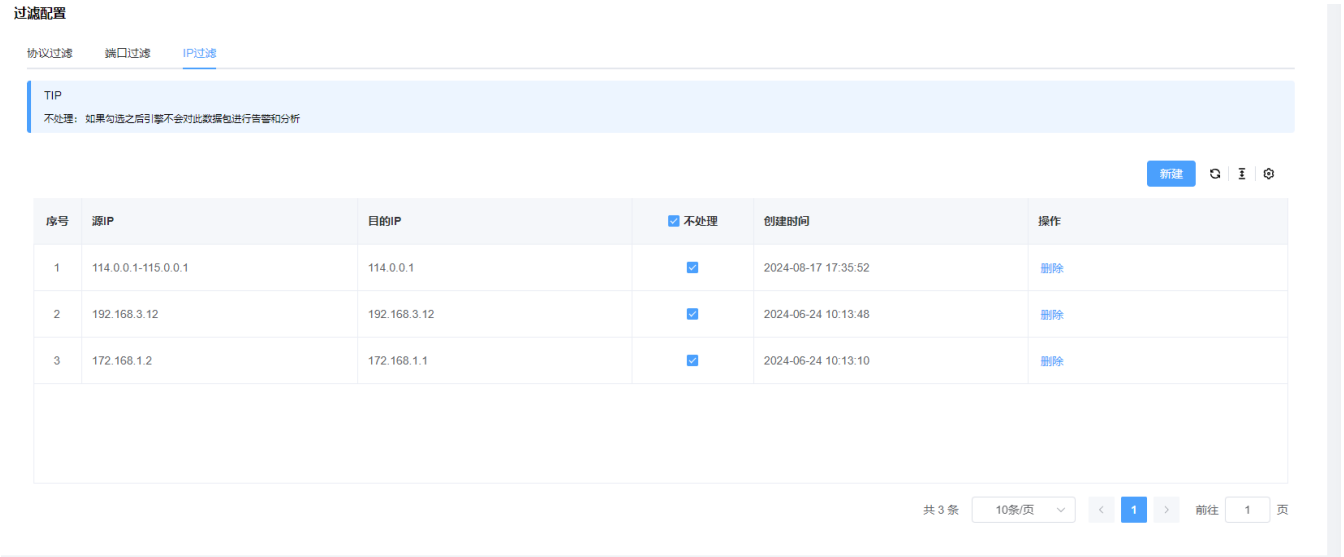
审计检测时对当前配置的端口进行过滤



点击**新增**按钮弹出对话框，对源端口和目的端口进行填写，完成后点击确认后即可生效

2.6.1 IP 过滤

审计检测时对当前配置的 IP 进行过滤

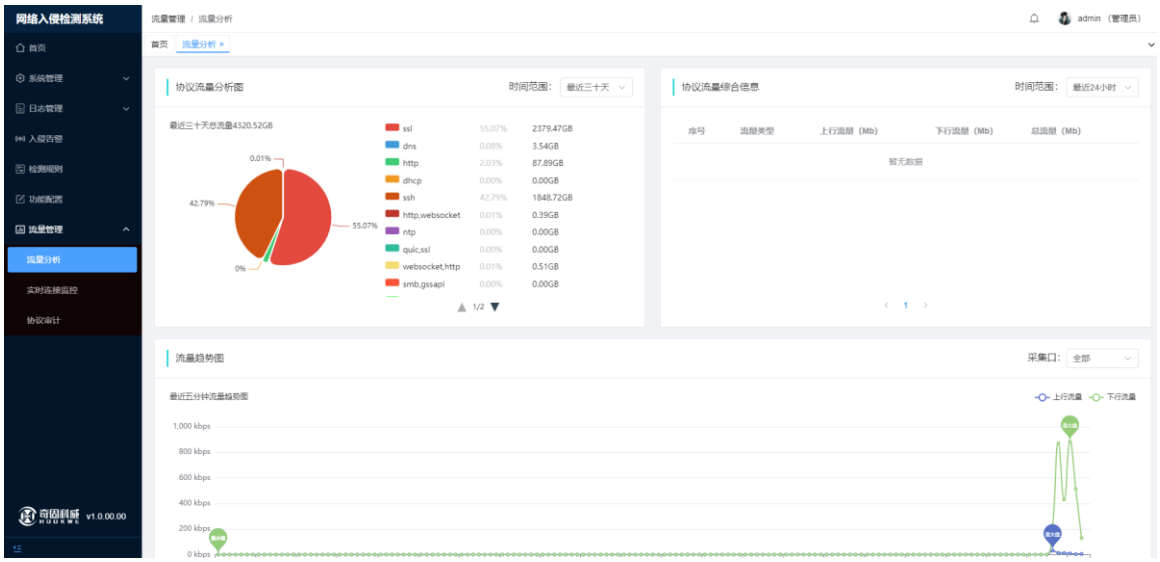


点击**新增**后弹出对话框，对源 IP 和目的 IP 进行填写，完成后确认后即可生效

2.7 流量管理

2.7.1 流量分析

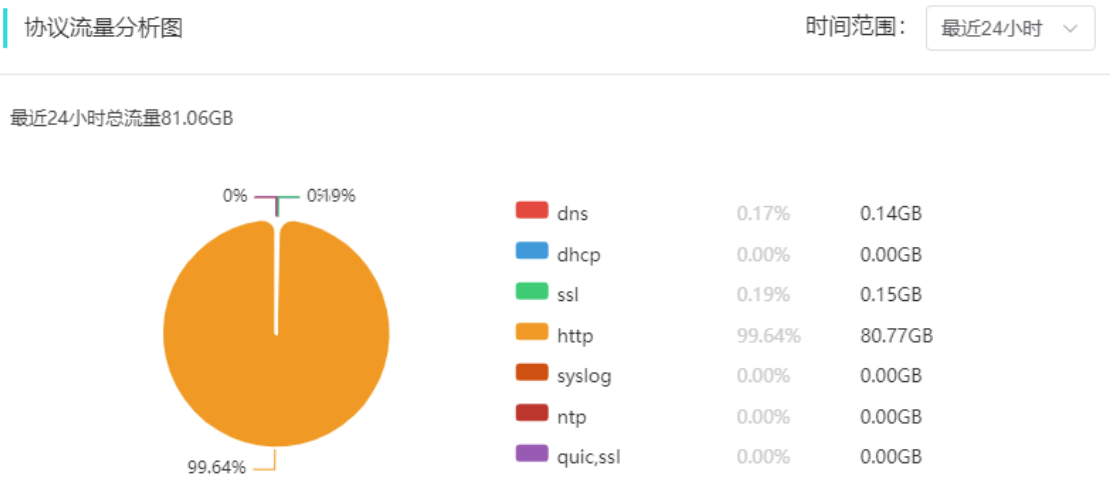
权限:(管理员，操作员，，审计员)



对当前网卡上的流量(实际采集是根据功能配置的过滤配置，来判断是否采集分析)，进行分析和展示。

协议流量分析图

对最近时间段的流量进行分析，点击右上角时间范围可以根据不同的时间段进行分析



协议流量综合信息

对最近时间段的流量进行分析，点击右上角时间范围可以根据不同的时间段进行分析

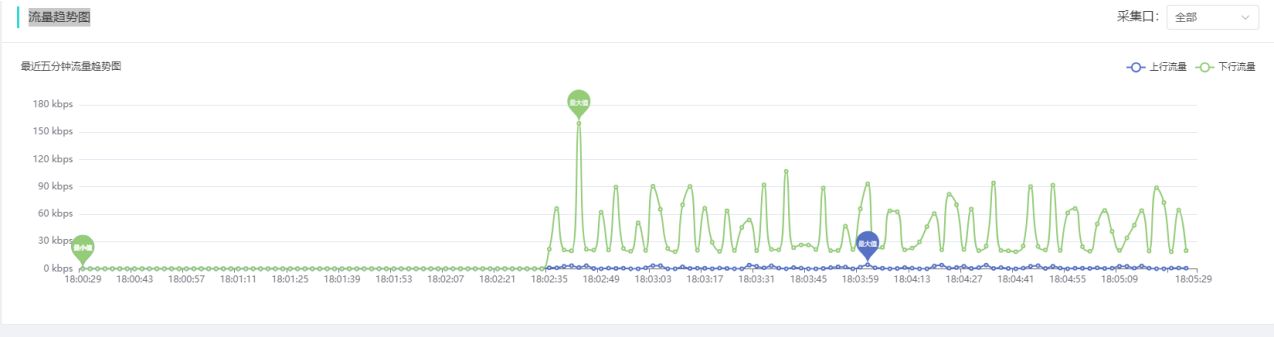
协议流量综合信息　　时间范围：最近24小时

序号	流量类型	上行流量（Mb）	下行流量（Mb）	总流量（Mb）
1	dns	154435245	277292	154712537
2	dhcp	65280	0	65280
3	ssl	33233009	123765156	156998165
4	http	2366264417	84356511499	86722775916
5	syslog	8662	0	8662
6	ntp	76	76	152

1 2

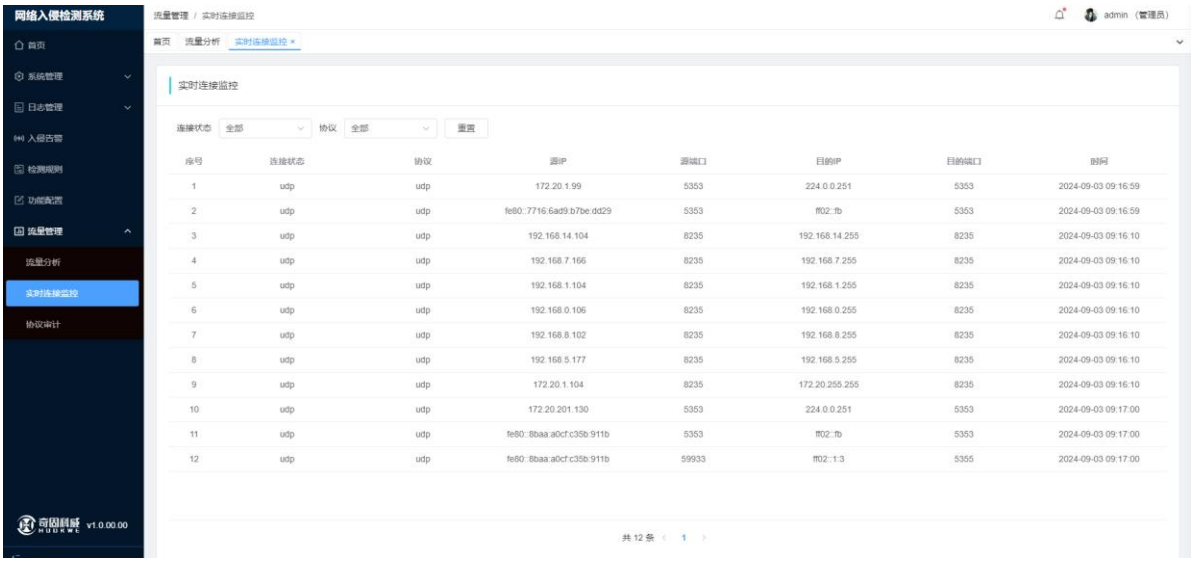
流量趋势图

对会实时的流量进行趋势查看，点击右上角可以对不同的网口进行查看



2.7.2 实时连接监控

权限:(管理员，操作员，，审计员)

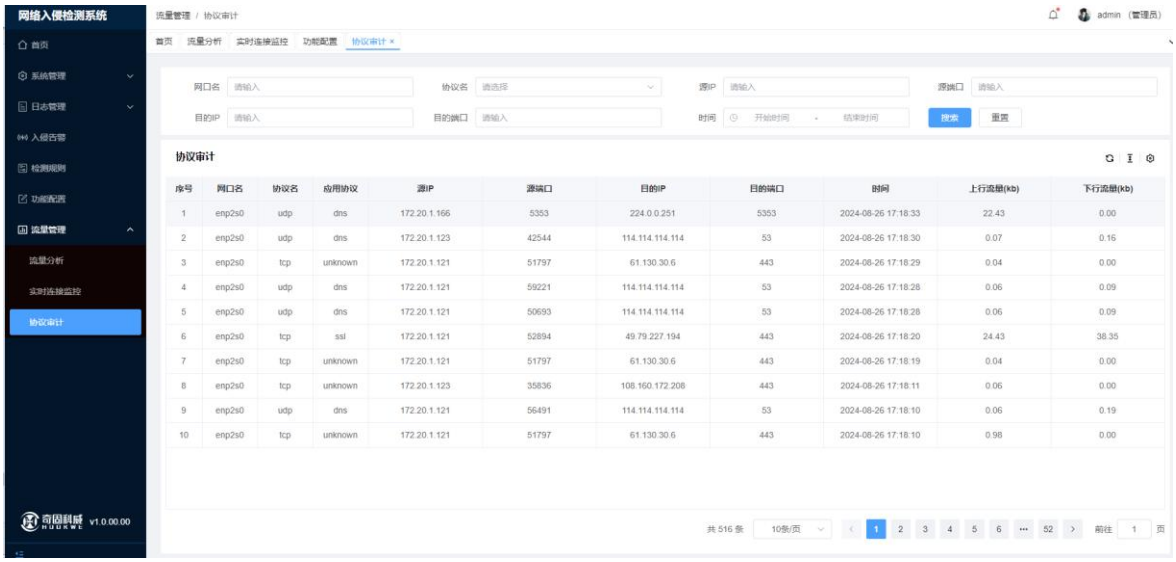


对当前网卡进行实时监听，对所有协议进行实时收集(实际采集是根据功能配置，来判断是否采集分析)，

进行分析和展示

2.7.3 协议审计

权限:(管理员，操作员，审计员)



对当前网卡进行实时监听，,对所有数据包 (实际采集是根据功能配置，来判断是否采集分析)，进行分析和展示。