

配置监控系统（CMS） 用户手册

四川电科智造科技有限公司

电子科技大学自动化研究所（技术支持）

声明

服务指南

四川电科智造科技有限公司

www.imia-uestc.com

TEL: 028-61831819

技术支持


电子科技大学自动化研究所

www.ia.uestc.edu.cn

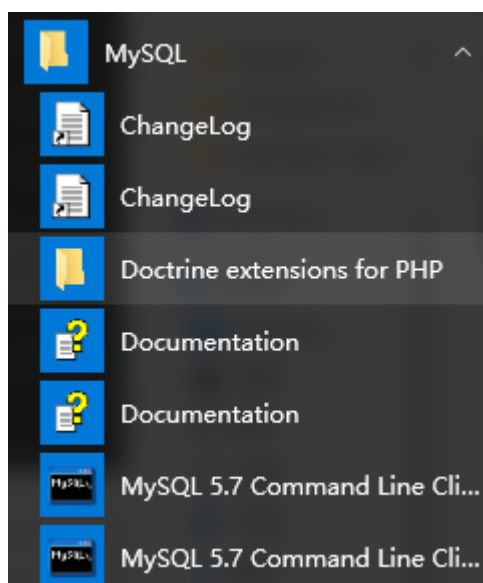
目录

声明	II
使用须知.....	1
1. 概述.....	5
2. 工业防火墙配置监控系统（CMS）概述	9
2.1 CMS 基本信息	9
2.2 CMS 窗体按钮	9
2.2.1 主页窗口.....	10
2.2.2 实时数据窗口.....	12
2.2.3 日志窗口.....	12
2.2.4 统计窗口.....	13
2.2.5 用户管理窗口.....	14
2.2.6 系统设置窗口.....	14
3. 使用配置管理平台（CMS）	15
3.1 防火墙配置概述.....	15
3.2 配置管理防护墙基本信息.....	16
3.2.1 属性标签.....	16
3.2.2 NAT 标签	17
3.2.3 白名单标签.....	20
3.2.4 深度包过滤标签.....	21
3.2.5 应用层协议控制标签.....	23
3.2.6 连接数据控制标签.....	24
3.2.7 策略路由标签.....	25
3.2.8 状态检测标签.....	28

使用须知

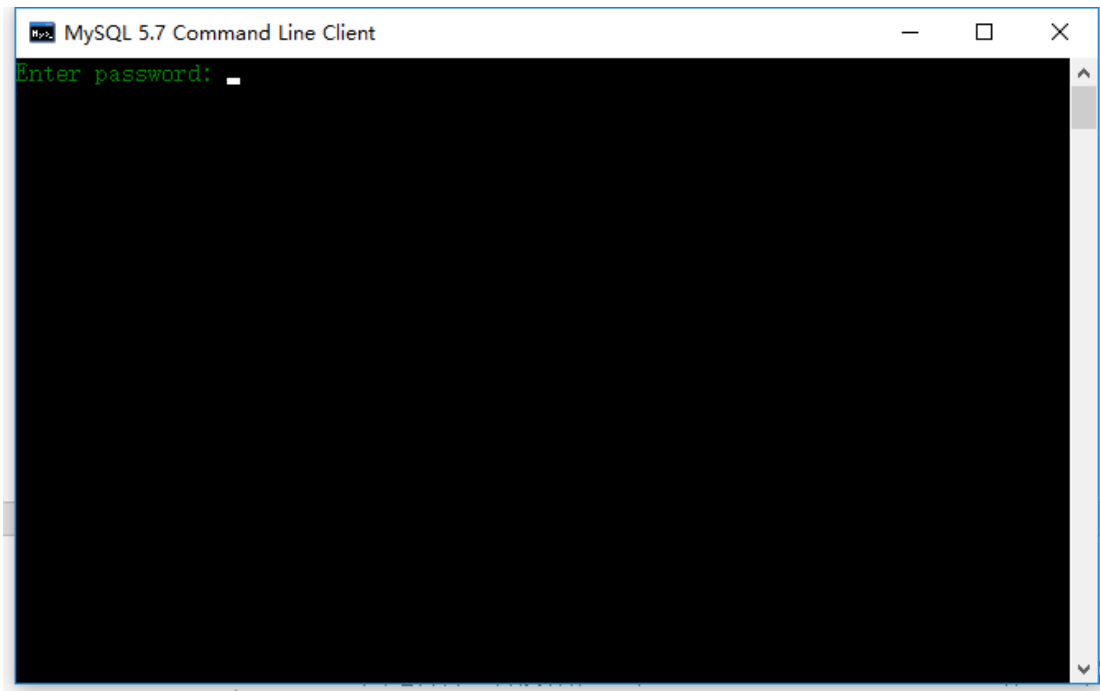
- 1、 从安装包中找到  mysql-connector-odbc-3.51.30-winx64.msi 安装 mysql 数据库，安装期间会设置数据库的用户名和密码，请牢记！

- 2、 Mysql 安装完成后，从已安装应用中找到

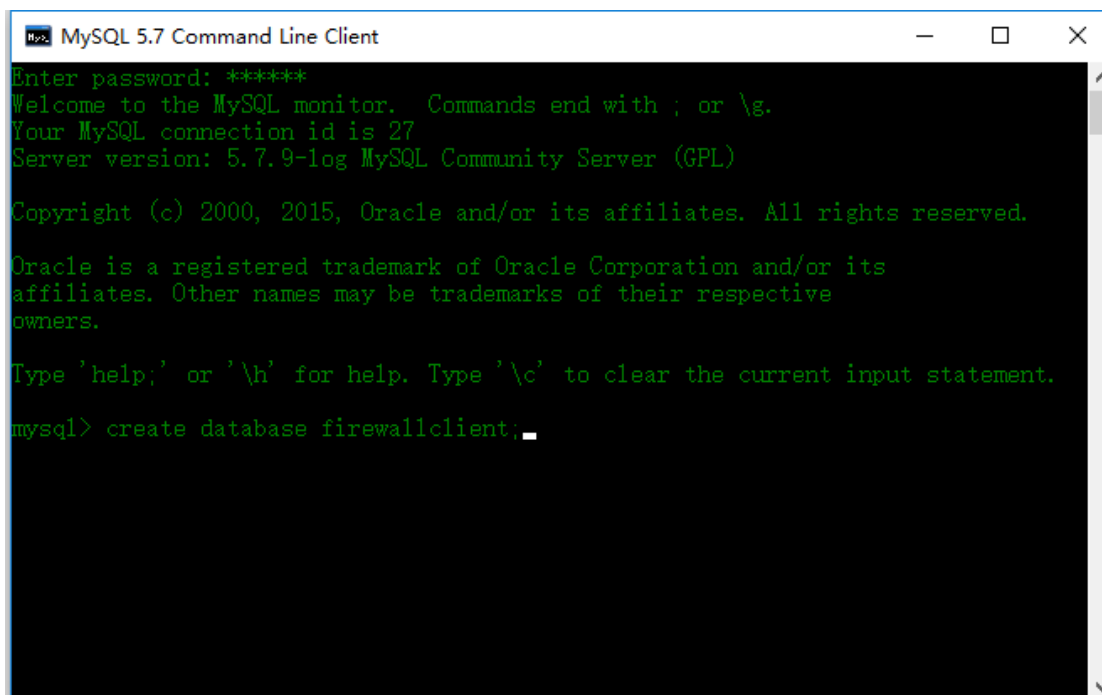


，右键选择以管理员身份运行 MySQL 5.7 Command Line Client。

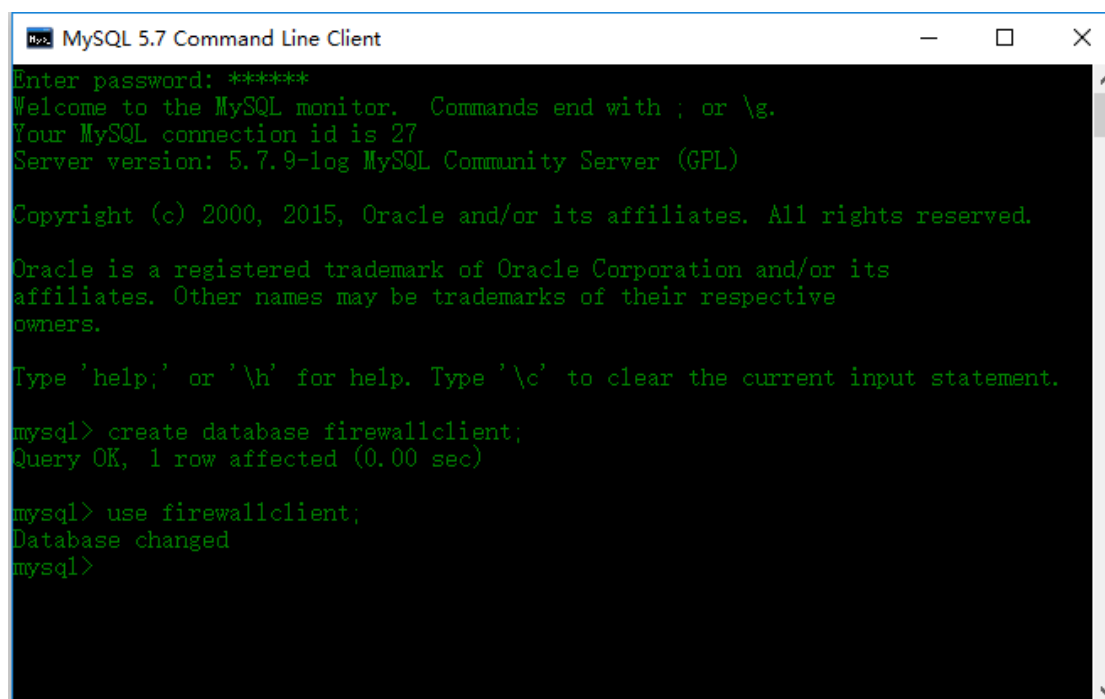
- 3、 输入安装 mysql 时的用户密码然后执行以下操作：



- (1) create database firewallclient;
(firewallclient 为数据库名称, 可更改)



- (2) use firewallclient;



```
MySQL 5.7 Command Line Client
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 27
Server version: 5.7.9-log MySQL Community Server (GPL)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

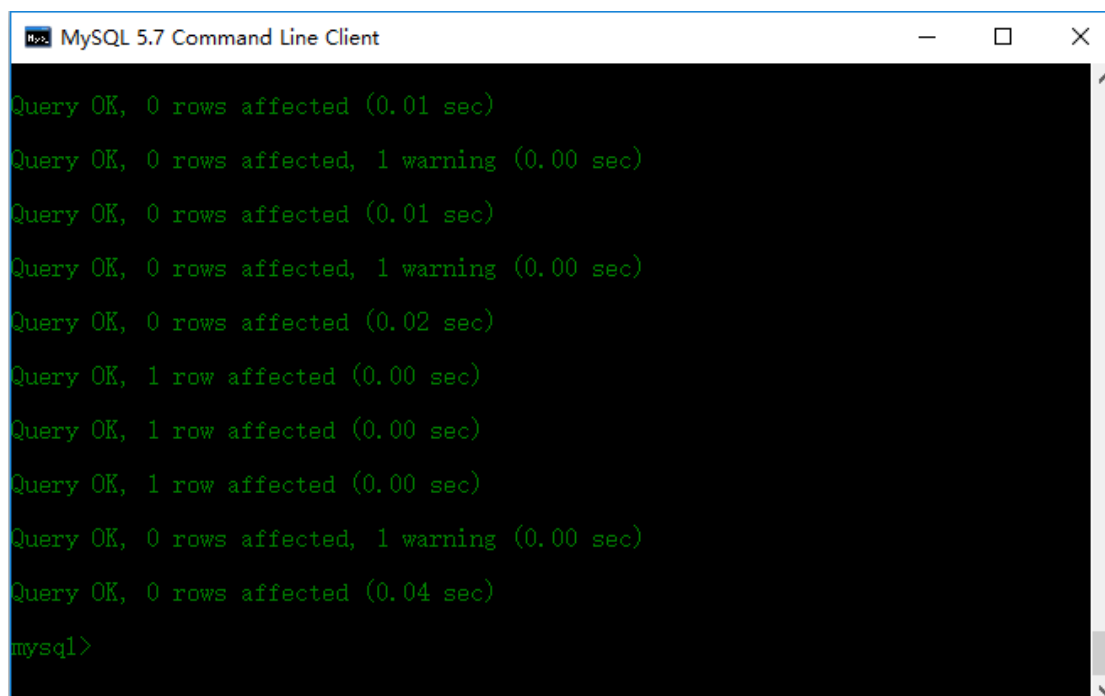
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database firewallclient;
Query OK, 1 row affected (0.00 sec)

mysql> use firewallclient;
Database changed
mysql>
```

(3) `source E:/firewallclient.sql;`

(E:/firewallclient.sql 为.sql 文件所在地址, 请根据实际文件所在地址输入, 回车后等待执行完毕即可。)



```
MySQL 5.7 Command Line Client

Query OK, 0 rows affected (0.01 sec)
Query OK, 0 rows affected, 1 warning (0.00 sec)
Query OK, 0 rows affected (0.01 sec)
Query OK, 0 rows affected, 1 warning (0.00 sec)
Query OK, 0 rows affected (0.02 sec)
Query OK, 1 row affected (0.00 sec)
Query OK, 1 row affected (0.00 sec)
Query OK, 1 row affected (0.00 sec)
Query OK, 0 rows affected, 1 warning (0.00 sec)
Query OK, 0 rows affected (0.04 sec)

mysql>
```

4、 启动 CMS 客户端,

(1)、提示第一次使用 CMS 客户端需要配置数据库信息。

提示

由于你是第一次使用，请首先配置数据库信息！

确 定

(2)、填写数据库信息（根据步骤 2、3 的数据库信息填写）。

数据库信息

数据库名称	<input type="text" value="firewallclient"/>
主机名或IP地址	<input type="text" value="localhost"/>
用户名	<input type="text" value="root"/>
密码	<input type="password" value="*****"/>

清 空 保 存

数据库信息可在主界面的系统设置中更改。

(3)、数据库配置成功后，准备完成，可正常启用智盾工业安全解决方案！

1. 概述

智盾工业网络安全解决方案是电科智造联合电子科技大学自动化研究所推出的一套针对工业控制网络安全的完整解决方案。涵盖数据采集、传输、处理、可视化的全过程，该方案根据不同工业现场的实际情况，在不改变原有拓扑结构的情况下实现对 DCS、PLC 的安全防护。

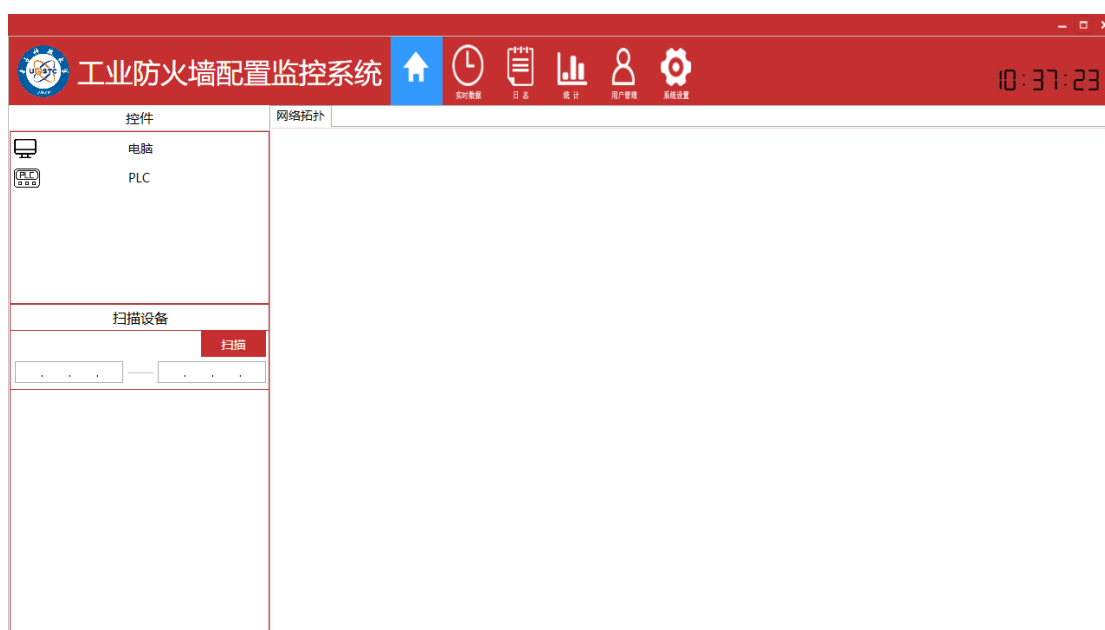
核心产品主要包括智盾工业防火墙（IMIF-1000 或 IMIF-500）、远程数据采集系统、工业网络智能分析系统等。

仅需 8 步即可轻松启用智盾工业网络安全方案，并显著改善工业控制系统的安全性：

1. 将工业防火墙安装在需要保护的设备和外设网络之间。并记录需要保护的设备 IP 地址。
2. 使用默认的超级用户名 “admin” 和密码 “admin” 登录工业防火墙配置管理系统。



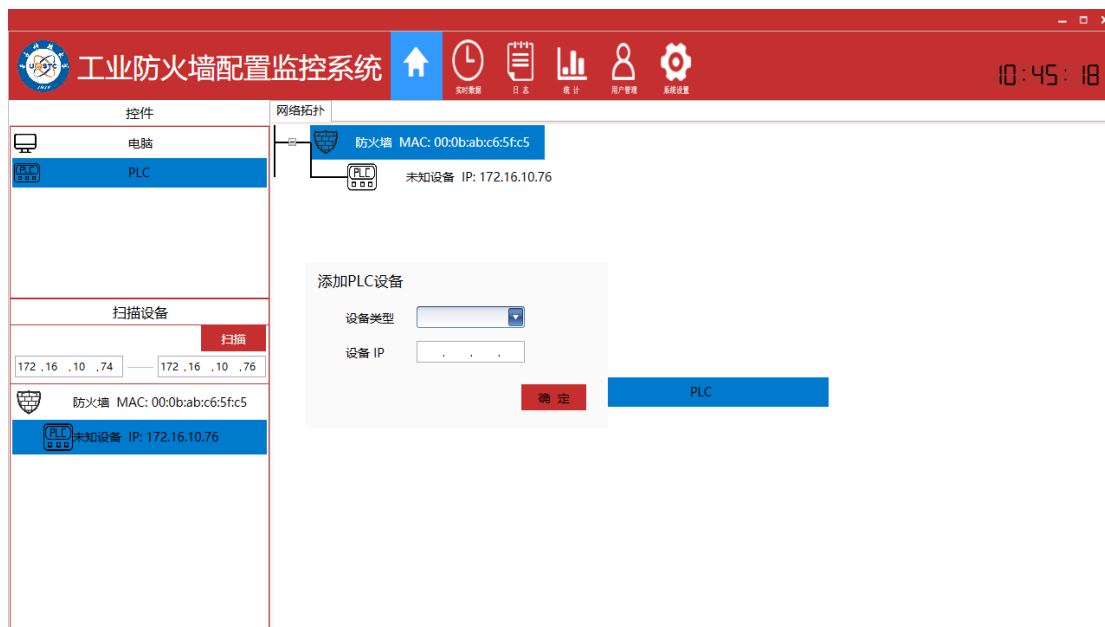
3. 登录成功后进入工业防火墙配置监控系统的主页界面。



4. 在主页界面左下方的扫描设备窗口输入要扫描设备的 IP 地址范围，即可扫描出该 IP 地址范围下的设备（参照第一步记录的被保护设备 IP）。



5. 通过从控件视图及扫描设备视图选择需要的设备并拖放至网络拓扑界面中，构建完整的网络拓扑图。



6. 对每个拖入网络拓扑图中的受保护 PLC 设备添加设备信息。

添加PLC设备

设备类型

设备 IP

确定

7. 双击网络拓扑图中的防火墙图标，即可弹出防火墙基本属性和设备信息窗口，通过切换选项卡按钮，可对防火墙进行规则配置。

The screenshot displays the '工业防火墙配置监控系统' (Industrial Firewall Configuration Monitoring System) interface. The main window is titled '网络拓扑' (Network Topology) and shows a list of devices on the left, including '电脑' (Computer) and 'PLC'. The 'PLC' device is selected, and its configuration window is open. The window has two tabs: '属性' (Properties) and 'NAT'. The '属性' tab is active, showing the following fields:

- 名称 (Name): IMIF-1000
- 防火墙 ID (Firewall ID): 00:0b:abc6:5fc5
- 防火墙 IP (Firewall IP): 172.16.10.19
- 描述 (Description): 智盾工业防火墙IMIF-1000配置监控管理平台
- 设备信息 (Device Information):
 - IP 地址 (IP Address): 172.16.10.76
 - MAC 地址 (MAC Address): 2c:4d:54:ed:dd:0a
 - 设备类型 (Device Type): 未知设备 (Unknown Device)

Buttons for '启用无IP模式' (Enable No IP Mode), '重设IP' (Reset IP), and '保存' (Save) are visible.

8. 规则配置完成后，智盾工业网络安全解决方案将成功应用在控制系统。

2. 工业防火墙配置监控系统（CMS）概述

2.1 CMS 基本信息

以 CMS 软件为中心的智盾工业网络安全解决方案共包含如下几个核心模块：

IMIF：智盾 IMIF-1000 工业安全防火墙，其实现对工业设备和控制系统的安全控制，并对工业网络提供防护功能；

CMS：配置监控系统，是基于 Windows 的中央管理控制平台系统，用于监控、管理和配置远程部署的防火墙安全设备。

2.2 CMS 窗体按钮



CMS 有六个顶层窗体按钮。分别是：

1. 主 页：由控件、扫描设备和网络拓扑三个窗口组成，允许用户将控件窗口和扫描设备窗口中的设备拖入网络拓扑窗口，构建系统的网络拓扑图。
2. 实时数据：实时监控设备的状态，方便用户查看设备处理信息时的各项信息和状态。
3. 日 志：通过操作该窗口，用户可在合理时间段内查询设备历史处理信息并可将所需信息导出备份。
4. 统 计：通过操作该窗口，用户可根据需要，查看指定时间

段内设备处理信息的统计分类结果。

5. 用户管理：用户可以通过此窗口查看用户的基本信息，并且可以根据监控系统的实际需求，添加用户、删除用户，修改密码和修改用户的权限。
6. 系统设置：查看数据库的基本信息，并且修改数据库的基本信息。

2.2.1 主页窗口

主页窗口可以划分以下三个区域：

控件区域：主页窗口的左上方区域，用户可以直接将控件下方的电脑和 PLC 控件直接拖到网络拓扑区域，能够方便用户创建网络拓扑。



扫描设备区域：主页窗口的左下方区域，用户根据监控系统的实际需求，输入需要扫描设备的 IP 地址范围，即可扫描出该 IP 地址范围下的设备。

扫描设备

扫描

172 . 16 . 10 . 74

—

172 . 16 . 10 . 80

 防火墙 MAC: 00:0b:ab:c6:60:12



未知设备 IP: 172.16.10.80

 防火墙 MAC: 00:0b:ab:c6:5f:c5



未知设备 IP: 172.16.10.76

网络拓扑区域：用户可以通过绘制网络拓扑图，反应工业防火墙配置监控系统整体的网络拓扑关系。



2.2.2 实时数据窗口

用户可通过实时数据窗口来实时监控设备的状态，及时处理设备异常。实时数据库为用户提供了快捷、高效的工厂信息。



时间	主机名称	源IP地址	目标IP地址	IP数据包标示	传输层协议类型	源端口号	目标端口号	处
2017-07-21-15:40:42	hehe-FWA-1330	172.16.10.167	172.16.10.76	29751	modbus	5912	502	
2017-07-21-15:40:42	hehe-FWA-1330	172.16.10.167	172.16.10.76	29750	modbus	5912	502	
2017-07-21-15:40:47	hehe-FWA-1330	172.16.10.167	172.16.10.76	29756	modbus	5914	502	
2017-07-21-15:40:47	hehe-FWA-1330	172.16.10.167	172.16.10.76	29755	modbus	5914	502	
2017-07-21-15:40:47	hehe-FWA-1330	172.16.10.167	172.16.10.76	29754	modbus	5912	502	
2017-07-21-15:40:47	hehe-FWA-1330	172.16.10.167	172.16.10.76	29753	modbus	5912	502	
2017-07-21-15:40:49	hehe-FWA-1330	172.16.10.167	172.16.10.76	29761	modbus	5915	502	
2017-07-21-15:40:49	hehe-FWA-1330	172.16.10.167	172.16.10.76	29760	modbus	5915	502	
2017-07-21-15:40:49	hehe-FWA-1330	172.16.10.167	172.16.10.76	29759	modbus	5914	502	
2017-07-21-15:40:49	hehe-FWA-1330	172.16.10.167	172.16.10.76	29758	modbus	5914	502	
2017-07-21-15:40:51	hehe-FWA-1330	172.16.10.167	172.16.10.76	29766	modbus	5916	502	
2017-07-21-15:40:51	hehe-FWA-1330	172.16.10.167	172.16.10.76	29765	modbus	5916	502	
2017-07-21-15:40:51	hehe-FWA-1330	172.16.10.167	172.16.10.76	29764	modbus	5915	502	
2017-07-21-15:40:51	hehe-FWA-1330	172.16.10.167	172.16.10.76	29763	modbus	5915	502	
2017-07-21-15:40:52	hehe-FWA-1330	172.16.10.167	172.16.10.76	29771	modbus	5917	502	
2017-07-21-15:40:52	hehe-FWA-1330	172.16.10.167	172.16.10.76	29770	modbus	5917	502	
2017-07-21-15:40:52	hehe-FWA-1330	172.16.10.167	172.16.10.76	29769	modbus	5916	502	
2017-07-21-15:40:52	hehe-FWA-1330	172.16.10.167	172.16.10.76	29768	modbus	5916	502	

2.2.3 日志窗口

用户可以通过操作该窗口界面上方的五个下拉框，查看被防火墙保护的设备在相应时间段内，各项数据信息和数据处理状态。有效防止丢失所需信息，用户也可以根据自己的实际需求，导出日志信息。



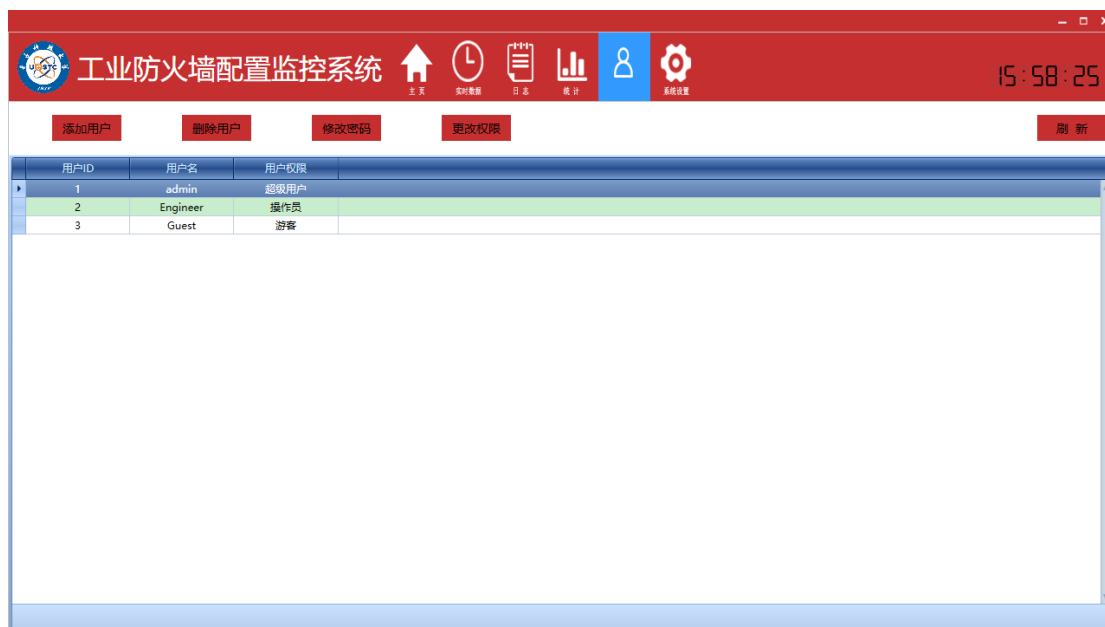
2.2.4 统计窗口

用户通过操作该窗口上方的四个下拉框，根据需要选择不同的参数，查看处理日志统计信息。用户可根据统计结果相应修改安全解决方案，以使控制系统更加安全。



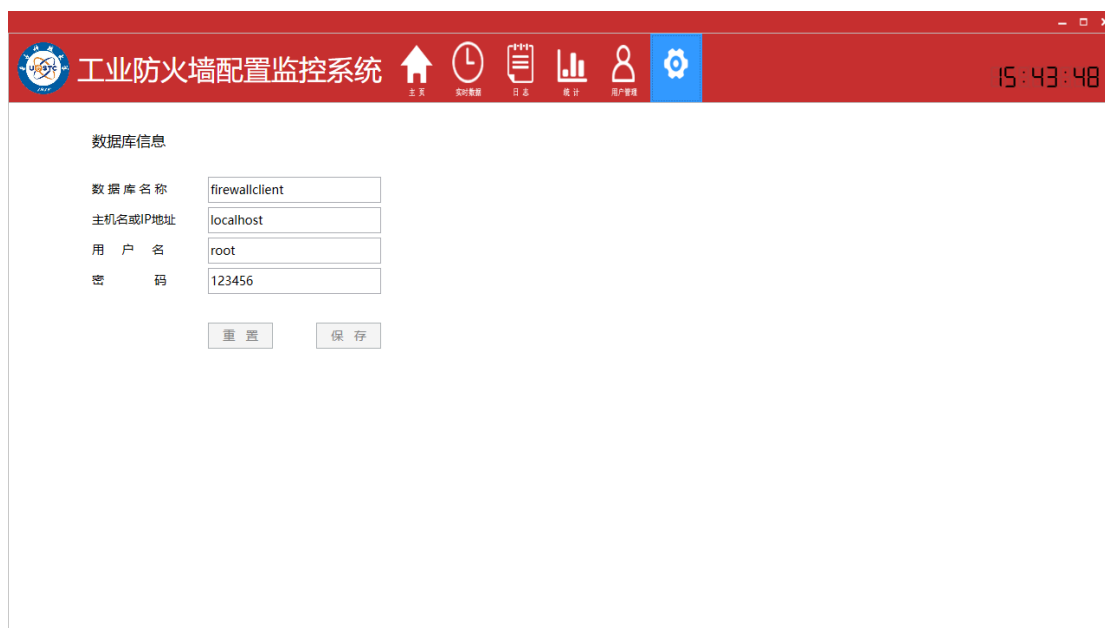
2.2.5 用户管理窗口

用户可在此窗口查看用户的基本信息，并且可根据监控系统的实际需求，添加用户、删除用户，修改密码和修改用户的权限。



2.2.6 系统设置窗口

用户可通过此窗口查看数据库的基本信息，并可修改或重置数据库的基本信息。



工业防火墙配置监控系统

15:43:48

数据库信息

数据库名称: firewallclient

主机名或IP地址: localhost

用户名: root

密码: 123456

重置 保存

3. 使用配置管理平台（CMS）

3.1 防火墙配置概述

用户可通过使用鼠标左键双击主页窗体网络拓扑图界面中的防火墙图标进入防火墙属性和规则配置窗口。



网络拓扑 00:10:f3:5f:f3:59

属性 NAT 白名单 深度包过滤DPI 应用层协议控制A 连接数控制CNC 策略路由PRT 状态检测STD

设置

名称: 00:10:f3:5f:f3:59

防火墙 ID: 00:10:f3:5f:f3:59

防火墙 IP: 172.16.10.117 启用无IP模式 重设IP

描述:

设备信息

IP 地址: 172.16.10.251

MAC 地址: d8:cb:8a:f1:e3:dc

设备类型: 未知设备

确定 应用 关闭

用户可通过点击选择窗口中不同的选项卡查看防火墙和被保护设备信息或者配置并启用防火墙规则。

3.2 配置管理防护墙基本信息

3.2.1 属性标签

网络拓扑 00:0b:ab:c6:5f:c5

属性 NAT 白名单 深度包过滤DPI 应用层协议控制A 连接数控制CNC 策略路由PRT 状态检测STD

设置

名称 : 00:0b:ab:c6:5f:c5

防火墙 ID : 00:0b:ab:c6:5f:c5

防火墙 IP : 172.16.10.19

启用无IP模式 重设IP

描述 :

设备信息

IP 地址 : 172.16.10.76

MAC 地址 : 2c:4d:54:ed:dd:0a

设备类型 : 未知设备

保存

平台属性窗口可以划分以下两个个区域：

防火墙设置区域：用户可以修改防火墙名称和添加防火墙描述方便管理，同时可以启用防火墙的透明模式，修改防火墙的IP地址。点击启用无IP模式按钮后，防火墙将全透明隐形并显著降低被攻击几率，重设IP操作可根据用户的实际需求重新设置防火墙IP地址。

名称：输入一个名称或者标识符作为防火墙的独特标识。这一点操作人员非常重要，每个防火墙需要独一无二的名称避免

混淆。

防火墙 ID：防火墙的硬件地址，当名称混淆时可作为唯一标识防火墙的标志，不可更改。

防火墙 IP：防火墙的 IP 地址，可通过操作进行修改。

重设防火墙IP

IP地址：

应用

取消

设备信息区域：用户可通过该区域查看被当前防火墙所保护设备的 IP 地址、MAC 地址和设备类型等设备的基本信息。

3.2.2 NAT 标签

NAT 的配置步骤如下：

1. 启用 NAT 映射

网络拓扑

00:10:f3:5f:f3:59

属性

NAT

白名单

深度包过滤DPI

应用层协议控制A

连接数控制CNC

策略路由PRT

状态检测STD

防火墙 MAC: 00:10:f3:5f:f3:59
IP: 172.16.10.117

添加NAT

NAT类型 :

DNAT

源IP地址	源端口	映射IP地址	映射端口	是否记录日志	操作
-------	-----	--------	------	--------	----

操作：可修改或者删除制定 NAT 规则。

2. NAT 配置

通过单击该页面上添加 NAT 红色按钮即可进行 NAT 配置，可切换 NAT 类型。

NAT配置

映射类型：☒ 记录日志目的 IP：映射目的 IP：目的端口：映射目的端口：

添 加

返 回

DNT 配置：

防火墙 MAC: 00:0b:ab:c6:5f:c5

IP: 172.16.10.19

添加NAT

应用

NAT类型：

源IP地址	源端口	映射IP地址	映射端口	是否记录日志	操作
172.16.10.55	22	192.168.1.1	22	<input type="checkbox"/>	 

关闭

SNT 配置：

防火墙 MAC: 00:0b:ab:c6:5f:c5

IP: 172.16.10.19

添加NAT

应用

NAT类型 : SNAT

	源设备IP地址	网口	网口IP地址	映射IP地址	是否记录日志	操作
1	192.16.10.22	eth0	192.16.10.2	172.16.10.19	<input type="checkbox"/>	

关闭

源地址映射中的网口 IP 即为设备的网关 IP 地址。点击应用按钮后即可启用 NAT。

3.2.3 白名单标签

将工业防火墙放置到工业监控系统环境中, 用户可通过点击该窗口添加名单的红色按钮添加白名单。

The screenshot shows the 'Industrial Firewall Configuration Monitoring System' (工业防火墙配置监控系统) interface. The main window displays the 'Whitelist' (白名单) configuration for a firewall with MAC 00:0b:ab:c6:5f:c5 and IP 172.16.10.19. The 'Whitelist' tab is selected, showing a form to add a new entry. The form includes fields for 'Source IP' (源 IP), 'Destination IP' (目的 IP), 'Source Port' (源端口), and 'Destination Port' (目的端口). The 'Log' (记录日志) checkbox is checked. The 'Add' (添加) button is highlighted in red.

工业防火墙配置监控系统

网络拓扑 00:0b:ab:c6:5f:c5

属性 NAT 白名单 深度包过滤DPI 应用层协议控制A 连接数控制CNC 策略路由PRT 状态检测STD

防火墙 MAC: 00:0b:ab:c6:5f:c5
IP: 172.16.10.19

白名单

源 IP : 172 . 16 . 10 . 254
目的 IP : 172 . 16 . 10 . 76
源端口 : 22
目的端口 : 22
☒ 记录日志

添加 返回

用户通过弹出的白名单窗口, 输入要添加白名单的源 IP、目的 IP、源端口、目的端口进行添加白名单操作。

3.2.4 深度包过滤标签

该窗口主要功能是实现各个协议的应用层的深度解析, 用户通过点击该窗口上面添加规则的红色按钮, 点击协议类型的下拉按钮即可添加不同类型的协议, 从而实现不同的规则配置, 该工业防火墙配置监控系统规则配置有三种协议类型可以配置, 分别是 Modbus/TCP、OPC、DNP3。

1. 基于 Modbus/TCP 协议的规则配置

该协议主要针对 Modbus/TCP 协议实现入侵检测, 主要将功能码和双向通信作为检测特征, 通过匹配请求数据包和响应数据包功能码的匹配情况实现基于 Modbus/TCP 协议的入侵检测。

规则配置

协议类型

modbusTcp

☒ 记录日志

主机IP地址

☒ All

从机IP地址

☒ All

线圈地址范围

12292

12292

最小转速

700

最大转速

700

允许通过的功能码

06

1

确定

返回

2. 基于 OPC 协议的规则配置

该协议通过通用统一标识符和数据包类型的匹配关系, 也就是特定的通用统一标识符对应特定的数据包类型。

规则配置

协议类型

OPC

☒ 记录日志

IP地址规则

主机IP地址

☐ All

从机IP地址

☐ All

确定

返回

3. 基于 DNP3 协议的规则配置

该协议针对 DNP3 协议的入侵检测，以功能码段序列为检测特征，由于工业环境下的周期性特点，所以特定的功能码序列也具有特性，利用这个特征进行基于 DNP3 协议的入侵检测模块。

规则配置

协议类型

DNP3

☒ 记录日志

IP地址规则

主机IP地址

☐ All

从机IP地址

☐ All

确定

返回

3.2.5 应用层协议控制标签

用户通过操作该窗口，防火墙可识别并控制各种应用类型，支持 HTTP、FTP、SMTP、POP3、TELNET、SSH 等常见应用层协议。



用户通过该界面可以在应用层协议控制规则列表中查看 HTTP、FTP、SMTP、POP3、TELNET、SSH 等常见应用层协议的基本信息，由于各应用层协议的初始状态均设置为 allow，用户想要修改应用层协议的状态，即可单击各应用层协议控制列表中操作栏的铅笔按钮，此时界面会弹出一个应用层协议控制规则列表的窗口，点击该界面操作栏的铅笔按钮，即可切换应用层控制协议的状态。

防火墙 MAC: 00:0b:ab:c6:5f:c5

IP: 172.16.10.19

应用层协议控制规则列表			
	应用层协议	状态	是否记录日志
1	http	allow	<input type="checkbox"/>
2	ftp	allow	<input type="checkbox"/>
3	smtp	allow	<input type="checkbox"/>
4	pop3	allow	<input type="checkbox"/>
5	telnet	allow	<input checked="" type="checkbox"/>
6	ssh	allow	<input type="checkbox"/>

关闭

应用层协议默认状态为允许通过,可通过配置修改禁用相应协议。

3.2.6 连接数据控制标签

用户通过操作该窗口, 防火墙能够设置单 IP 的最大并发会话数, 防止大量非法连接产生时影响网络的性能。用户通过点击该页面上添加规则按钮实现 IP 连接数控制通过该弹出的窗口, 可设置最大连接数和选择是否记录日志。

IP连接数控制

源 IP :	<input type="text" value="172 . 16 . 10 . 222"/>
目的 IP :	<input type="text" value="172 . 16 . 10 . 123"/>
源端口 :	<input type="text" value="2585"/>
目的端口 :	<input type="text" value="502"/>
最大连接数 :	<input type="text" value="0"/> <input checked="" type="checkbox"/> 记录日志

添加

返回


用户添加的连接数控制规则会显示在 IP 连接数控制规则列表中，用户可通过该列表操作栏来修改控制规则和删除规则。

防火墙 MAC: 00:10:f3:5f:f3:59

IP: 172.16.10.117

添加规则

IP连接数控制规则列表

	源IP地址	源端口	目的IP地址	目的端口	最大并发会话数	是否记录日志	操作
1	172.16.10.222	11	172.16.10.253	22	3	<input checked="" type="checkbox"/>	 
2	172.16.10.11	12	172.16.10.13	23	4	<input checked="" type="checkbox"/>	 

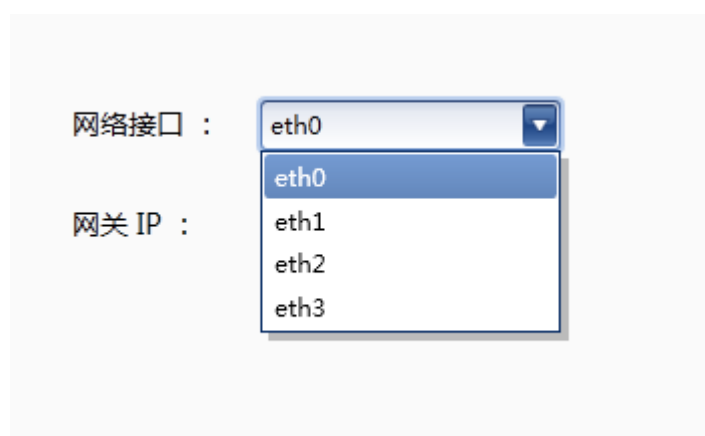
3.2.7 策略路由标签

用户可通过点击该页面上的添加路由按钮对系统进行路由配置，通过弹出来的路由配置窗口，用户根据实际需要，点击路由类型的下拉框可选择默认路由、主机路由、网络路由三种不同的路由类型。



1. 配置默认路由

用户选择默认路由类型时，通过选择不同的网络接口（该系统提供了四中不同的网络接口，分别为 eth0、eth1、eth2、eth3）和输入网关 IP，点击下方的添加按钮，可实现默认路由类型的路由配置。



路由配置

路由类型：

默认路由

☒ 记录日志

网络接口：

eth0

网关 IP：

172 . 16 . 10 . 254

添加

返回

2. 配置主机路由

通过弹出的主机路由配置界面，用户通过选择不同的网络接口和输入相应的网关 IP 和目的主机 IP，可实现主机路由配置。

路由配置

路由类型：

主机路由

☒ 记录日志

网络接口：

eth3

网关 IP：

172 . 16 . 10 . 254

目的主机 IP：

172 . 16 . 10 . 231

添加

返回

3. 配置网络路由

通过弹出的网络路由配置界面，用户通过选择不同的网络接

口和输入相应的网关 IP、网络主机 IP 和网络掩码，可实现网络路由配置。



路由配置

路由类型：网络路由

☒ 记录日志

网络接口：eth0

网关 IP：. . .

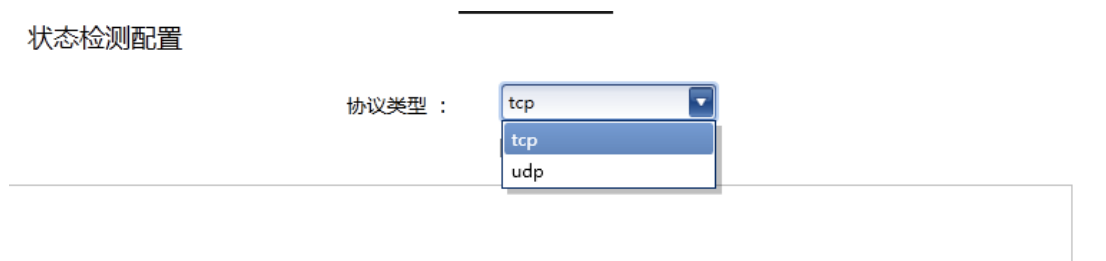
网络主机IP：. . . 网络掩码：. . .

添加 返回

该策略路由 PRT 界面还提供了路由规则列表，方便用户直接查看路由类型、主机 IP、规则网络 IP、目的地址网络掩码、网络接口、网关地址、是否记录日志和操作等路由规则的基本信息。

3.2.8 状态检测标签

用户可通过点击该页面上的添加规则按钮对系统进行状态检测配置，通过弹出来的状态检测配置窗口，用户根据实际需要，点击协议类型的下拉框可选择 tcp、udp 两种不同的协议类型。



状态检测配置

协议类型：tcp
tcp
udp

用户通过选择不同的协议类型（tcp、udp），输入相应的源 IP、目的 IP、源端口和目的端口添加不同的状态检测配置规则。该状态检测 STD 界面还提供了状态检测规则列表，方便用户直接查看路由协议、源 IP 地址、源端口和目的端口等状态检测规则的基本信息。

状态检测配置

协议类型：

tcp

▼

☒ 记录日志

源 IP：

.

.

.

目的 IP：

.

.

.

源端口：

目的端口：

添加

返回