## 工业防火墙配置监控系统功能需求分析

1. 功能概述

工业防火墙配置监控系统有用户登录窗口，登陆时需要验证账户名和密码。身份验证通过的用户都有一个权限，他们只能在权限允许的范围内操作。

工业防火墙配置监控系统有6个顶层目录，它们是：

1. 主页：显示拓扑结构和配置防火墙；
2. 实时数据：显示数据的实时处理情况；
3. 日志与统计：时间段内数据的统计情况；
4. 操作日志：操作人员进行的操作记录；
5. 用户管理；增加删除用户，修改用户密码和权限；
6. 系统配置：修改软件的一些配置信息。

本系统的主要功能是发现设备，并给防火墙设备配置一定的规则，监测数据包的处理状态，并提供日志与统计信息。

1. 用户登录

第一次登录时，由于未配置数据库，将只能使用写入在xml中的超级用户admin，登陆成功后，需要首先设置数据库的连接，会在正常连接的数据库中生成一些操作必须的表，同时会在useraccount表中增加超级用户帐号，以后可修改密码。

以后登录时，会在数据库中验证帐号和密码，并读取权限。用户只能在权限允许的范围内操作。

用户输入错误用户名和密码会得到用户名不存在或者密码错误的提示。

第一次登录时，需要输入数据库database，datasource，userid，password信息。通过验证datasource，userid，password即证明可用Mysql服务，创建数据库database，生成必须的表。

1. 主页

主页完成的主要功能就是显示拓扑结构和配置防火墙。

1. 显示拓扑结构

拓扑结构的显示主要有扫描设备和拖拽控件完成拓扑结构两个部分。

1. 扫描设备

输入待扫描的IP地址范围（如172.16.10.60——172.16.10.70），前三个字段自动补齐，不需要重复输入。返回结果是防火墙和对应处于待扫描范围内的被保护设备（多对多的形式）。

1. 完成拓扑结构

根据扫描结果，拖拽主页中的控件图标和扫描结果里的控件图标完成拓扑结构。

1. 手动添加

对于未扫描到的设备，可以进行手动添加。即拖拽相应的设备控件，自己可以设置名称。

1. 配置防火墙

配置防火墙主要是设置防火墙的IP和防火墙的规则。

防火墙现有的规则用一个列表直观的显示。超级用户和操作员用户可以增加新规则，或者修改已有的规则，删除现有的规则。一旦修改后的规则与现有的规则不一致时，会出现一个应用按钮，应用之后，修改后的规则才会被应用到防火墙设备。

1. 设置防火墙IP

将有IP的防火墙设置成无IP模式（0.0.0.0），也可将无IP的防火墙设置成有IP的模式。

1. 配置ModbusTcp规则

在规则列表中加入规则即可。需要输入源IP地址,目标IP地址，线圈地址范围（1-65535）和禁止通过的功能码（21个）。可选择是否生成日志。

1. 配置OPC规则

在规则列表中加入规则即可。需要输入源IP地址,目标IP地址。可选择是否生成日志。

1. 配置DNP3规则

在规则列表中加入规则即可。需要输入源IP地址,目标IP地址。可选择是否生成日志。

1. 配置IEC104规则（待定）

在规则列表中加入规则即可。可选择是否生成日志。

1. 配置自定义规则

在规则列表中加入规则即可。需要输入源IP地址,目标IP地址，端口号，处理结果（通过或者拒绝）。可选择是否生成日志。

1. 实时数据

显示数据包的处理状态：正常和警告。

可在系统设置中设置显示的最多条数。同时可以选择防火墙，处理状态等信息。根据数据包的处理状态，显示不同的颜色。

1. 日志与统计

可以选择防火墙和数据包处理状态和时间段查询对应的日志信息。

日志的分类：正常和警告。

1. 告警事件统计、数量趋势：统计一定时间范围内，TOP N告警事件类型；统计告警事件数量随时间变化的趋势，默认是所有类型告警事件的数量，也可以选择某个特定的事件类型。
2. 对网络连接进行多维度的统计，例如：
3. 基于连接数TOP IP地址：统计某个协议（如Modbus）或全部协议网络连接数最多的IP地址：
4. 基于报文数TOP IP地址：统计某个协议（如Modbus）或全部协议网络报文数最多的IP地址；
5. 基于流量TOP IP地址：统计某个协议（如Modbus）或全部协议网络流量最多的IP地址；
6. 基于连接数TOP协议：统计某个IP或全部IP，网络连接数最多的协议（如Modbus）；
7. 基于报文数TOP协议：统计某个IP或全部IP，网络报文数最多的协议（如Modbus）；
8. 基于流量TOP协议：统计某个IP或全部IP，网络流量最多的协议（如Modbus）。
9. 操作日志

用户的一些操作会生成日志。以下情况会生成记录日志：

1. 用户的登录退出操作；
2. 对防火墙IP地址的设置操作；
3. 对防火墙规则的增加删除修改；
4. 对系统配置的修改。

可以选择用户名和时间范围，查询相应的操作日志。

备注：超级用户可以查看所有的人的操作日志，低等级用户只能查看自己的和比自己等级更低的用户的操作日志。

可以导出操作日志。支持的格式有txt，xls，csv，html。

操作日志显示格式：用户名，时间，操作，操作设备MAC地址。（有没有其余的字段？）

1. 用户管理

用户管理即增加用户，删除用户，修改用户密码，修改用户权限。

有三级用户：超级用户，工程师，游客。

超级用户权限：可以进行一切操作。包括增加删除工程师游客账户，修改权限和密码，配置防火墙规则，修改系统配置，查看日志和实时数据。

工程师权限：只能增加删除游客账号，修改当前用户或者游客的密码，配置防火墙规则，修改系统配置，查看日志和实时数据。

游客权限：仅能查看日志和实时数据。

用户在用户管理界面只能查看到比自己级别低的用户和自己，并且只能操作这些用户。

1. 增加用户

超级用户可以增加工程师帐号和游客帐号，工程师只能增加游客帐号，游客并不能增加帐号。增加帐号时，需要输入用户名和两次密码，只有当用户名不存在且两次密码输入相同时才能成功添加用户。

1. 删除用户

超级用户可以删除工程师帐号和游客帐号，工程师只能删除游客帐号，游客并不能删除帐号。删除帐号时，会弹出确认窗口，只有确认删除用户时才能成功删除选定的帐号。

1. 修改用户密码

超级用户可以修改工程师帐号、游客帐号和自己的密码，工程师能修改游客帐号和自己的密码，游客只能修改自己的密码。修改密码时，需要重复输入两次相同的密码即可。

1. 修改用户权限

超级用户能够将工程师帐号修改成游客帐号，游客账号修改成工程师帐号。工程师和游客均不能修改权限。

1. 系统配置

数据库配置，用户可以自己选择将数据保存在任何地方。需要输入database，datasource，userid，password数据库连接的信息，保存时会验证datasource，userid，password连接情况，如果异常则会提示，并且不能保存，需要重新输入。通过时是否清空原来数据库名database数据？？？

实时数据最大显示条数，默认为200条。