项目总体设计报告

项目名称：基于内核模块的包过滤防火墙

姓名	陈洋	谷韫名	丁华威	苏世侦	符景乐
学号	**521021911061**	**521021910621**	**521021911053**	**521030910143**	**521021911063**

学院：电子信息与电气工程学院

报告完成日期：2023 年 6 月 23 日

1、系统需求分析

1.1 需求分析

包过滤是在网络层中根据事先设置的安全访问策略(过滤规则) ,检查每一个数据包的源 IP 地址、目的 IP 地址以及 IP 分组头部的其他各种标志信息(如协议、服务类型等) , 确定是否允许该数据包通过。本项目需实现根据特定的规则对数据包进行过滤和检查，从而满足过滤进出网络的数据、管理进出访问网络的行为、记录通过防火墙信息内容和活动、对网络攻击检测和告警等需求。

1.2 总体功能要求

（1）包过滤: 防火墙应具备对网络数据包进行过滤和检查的能力，根据预定义的规则集合决定允许或拒绝传输。

（2）内核模块集成: 防火墙应作为一个内核模块实现，以确保在操作系统内核级别进行网络流量控制和处理。

（3）规则管理: 提供用户友好的界面或命令行工具，用于管理和配置防火墙的规则集合，包括添加、删除和修改规则。

（4）灵活的规则定义: 支持灵活的规则定义，如基于 IP 地址、端口、时间段、网络接口、ICMP 报文的子类型等进行报文的检查和控制。

小组分工：

检查和控制要素的扩展：苏世侦、丁华威

多包过滤规则的扩展：谷韫名、符景乐

图形化界面方便进行的管理：陈洋

1.3 软件开发平台要求

ubuntu-22.04.1

1.4 运行环境要求

Gcc、tkiner 等包

2、计划进度安排

6.19-6.25 熟悉项目需求、代码；小组内部分工，制定计划

6.25-7.9 设计并实现各模块的内容；实现模块的整合与链接；测试软件的功能性

7.10-7.16 代码后期维护与更新

3、系统总体架构

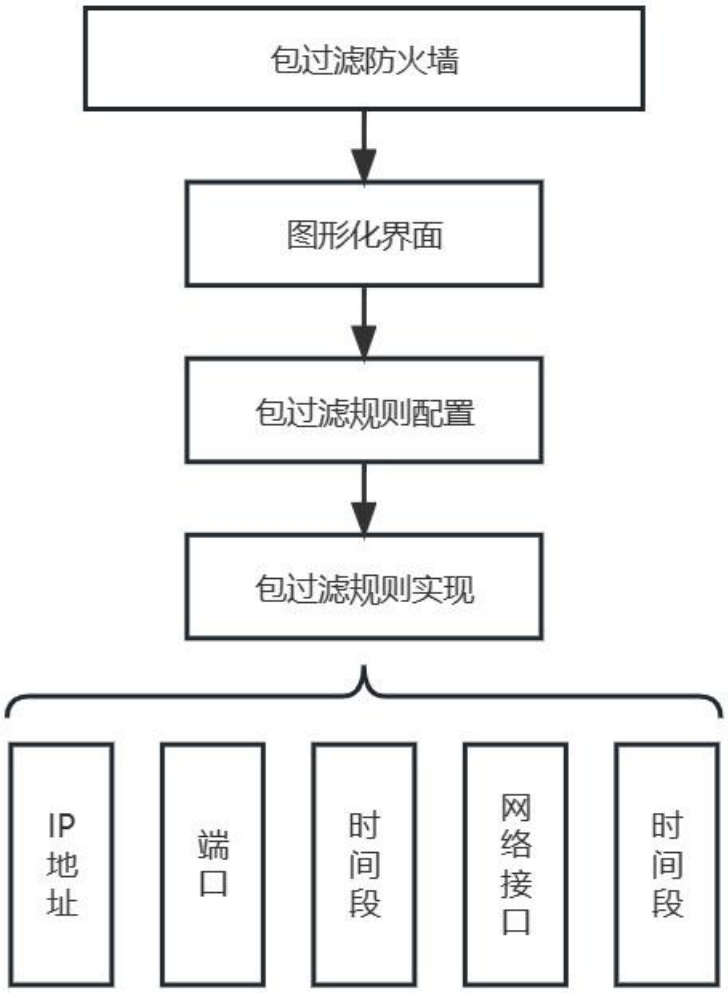
3.1 平台架构

通过编译 linux 的内核模块来实现包过滤防火墙。将准备两个不同的虚拟机，一个用于发出数据包，另一个用于接收数据包。通过两个 linux 平台来测试防火墙的效果实现。

3.2 总体架构

包过滤防火墙首先通过图形化界面模块，允许用户配置多条过滤规则，然后通过一系列模块实现各规则的功能。

逻辑图如图所示：



4、图形化界面模块

4.1 模块结构

当用户在终端打开包过滤防火墙界面时，将调用窗口管理模块和图形绘制模块将窗口展示在显示屏中，并且调用用户界面组件模块产生可供用户操作的按键、输入框。当用户尝试输入或点击按键时，系统将调用事件处理模块与下层包过滤配置功能进行交互，响应用户的请求。

因此四个子模块是并行的，各司其职，并不存在明显的上下级关系。

4.2 窗口管理模块

负责创建和管理窗口，包括窗口的位置、大小、标题等属性。它提供了窗口的显示、隐藏、最小化、最大化等功能，并处理窗口之间的层叠关系。

4.3 用户界面组件模块

负责创建和管理各种用户界面组件，如按钮、文本框、下拉菜单、复选框等。它负责处理用户与组件的交互，包括接收用户输入、响应用户操作，并提供相应的事件处理和状态管理

4.4 图形绘制模块

负责将用户界面的各种图形元素绘制到屏幕上。它通过调用底层的图形

库或图形引擎，将界面组件、图像、文本等绘制为可见的图形对象，并处理图形的渲染、更新和刷新。

4.5 事件处理模块

负责处理用户界面上的各种事件，如鼠标点击、键盘输入、窗口拖动等。它监听并分发事件，将事件传递给相应的事件处理函数或回调函数进行处理，并更新界面状态以响应用户操作。

5、包过滤规则配置模块

5.1 包过滤配置模块需要实现以下功能：1.查看规则 2.删除规则 3.添加并存储规则。

5.2 规则解析模块

解析用户从图形化界面中输入的规则参数值，将其中字符串转化为可供程序操作的整型数。

5.3 规则验证模块

验证用户配置的规则是否合法，如果合法，则向上级传递合法的信号，并调用下级规则存储模块存储该规则；如果非法，则向上级传递非法的信号。

5.4 规则存储模块

负责将规则配置保存到持久化存储中，以便后续的读取和使用。该模块可能会与数据库、文件系统或其他存储系统进行交互，将规则配置以结构化的方式进行存储，并提供读取、更新和删除规则的接口

6、包过滤规则实现模块

按照总体架构中设计，并行设立各个模块。需要应用哪条规则，就调用哪个模块的函数。

7、运行平台

6.1 软件平台

Linux 系统的虚拟机

6.2 硬件平台

笔记本电脑

8、接口设计

接口用图形化界面模块实现，使得用户能以访问应用程序的方法配置包过滤防火墙，而不必在终端配置。

9、系统出错处理设计

9.1 错误的参数

例如 IP 地址格式错误、找不到对应的端口等，此时需将错误信息反馈给用户界面。

9.2 未知的符号

配置规则时输入未知的符号，此时需将具体的符号错误信息反馈给用户界面

9.3 冲突的规则

当添加一条已经被存储的规则时，系统将反馈重复信息，并终止此次添加。

9.4 删除不存在的规则

当删除一条不存在的规则时，系统将反馈此信息。

建议处理办法：定义一个枚举变量 error，不同的值表示不同的错误种类。当上述函数在各自模块运行报错时，系统将为对应的枚举变量赋值并终止函数

的运行，图形化界面模块探测到枚举变量值的变化后，向用户发送相应的报错提示。