**项目中期检查报告**

**项目名称：应用层包过滤防火墙的控制功能拓展**

**姓名： 秦瑞泽、王梦奇**

**学号：5130369074、5130369059**

**学院：电子信息与电气工程学院 信息安全工程**

**报告完成日期：2016年11月12日**

1. **项目开发目标**

本项目的目的是基于《信息安全技术解析与开发实践》中已有的包过滤防火墙简单版本，设计一款具有拓展功能的应用层包过滤防火墙。已有的例子中，仅仅实现了单条规则的包过滤防火墙，且只针对源地址、端口以及目的地址、端口进行过滤。我们本次项目的目的主要有以下几方面：

（1）过滤规则拓展。增加对于时间段 、网络接口、ICMP报文子类型的检测。具体而言，可以按时间段开闭防火墙、可以针对不同网络接口设定不同的规则、增添对于ICMP报文子类型的检测。

（2）多过滤规则支持。在本项目中需开发出可同时支持多条规则过滤的防火墙，同时也应设计出对应冲突规则处理方法。

（3）友好的控制界面。即防火墙有有好的UI交互界面，可以进行规则的增删改查，可以进行针对时间段的过滤，可以进行对协议的过滤选择。

1. **项目开发内容**
   1. **面向用户需求模块**
      1. **前端交互子模块**

本模块主要要求为设计合理的UI界面，能够为用户提供舒适的使用体验。可以允许用户在UI界面上进行规则的浏览和控制。本模块主要包含输入模块和阅览模块两大部分。输入模块要求提供IP、端口、协议、时间、网卡的选择，阅览模块要求提供列举规则、选中规则(供删除、修改使用)等功能。

技术实现方面，本模块初步决定采用跨平台C++图形用户界面应用程序开发框架Qt，以方便在Linux内核系统上开发防火墙以及使用Netfilter函数库。（备选Python语言对应的pyqt以及python bindings for libnetfilter\_queue）

逻辑方面，主要需要实现的功能为提供多种规则的输入输出方式:具体而言应包含：

输入：IP、端口的输入框（最好附带有效性检测），可检测协议的选择部件（如下拉条）、时间段选择部件（最好设置标准时间选择部件）、网卡选择部件（下拉条）

输出：预计应使用表格类部件，可查询数据库中所有规则，并提供选中修改或删除的功能。可添加用户提示输出模块，显示程序对用户操作的响应。

* + 1. **指令处理子模块**

本模块主要涉及功能为响应用户的操作指令，并进行校验和执行，以及与数据库进行连接等功能。

本模块主要分为三部分，规则校验模块、规则生成模块以及数据交互模块。三个模块应实现的功能为：

规则校验模块：识别用户输入的参数，并进行有效性校验。若出现问题，按错误类型提升用户修改输出。若符合规则，则发送至规则生成模块进行处理。

规则生成模块：本模块主要功能为，将用户传入的参数，生成合理的对应到的控制规则，并按规定的格式发往数据交互模块。

数据交互模块：本模块的主要功能为处理用户需求处理模块与数据库模块的交互需求。预想的使用场景为：

用户发送查询请求，该模块向数据库请求所有规则数据，并发送至输出模块。

用户需要添加模块，应先校验库中规则与当前规则是否重复，然后向数据库中添加规则。

* 1. **数据库模块**
     1. **数据交互子模块**

本模块主要功能为连接用户需求模块以及数据包裁决模块，为其提供数据查询服务。

预计需要实现的功能包含：

查询所有规则、插入数据、删除数据、修改数据等。

* + 1. **数据存储子模块**

本模块主要完成规则的储存工作，将用户需求处理界面发来的规则，以及对于默认规则和冲突解决原则的处理方法。

储存方法应至少包含每条规则所带有的参数信息。即IP、端口、协议、网卡、允许或者禁止。对于时间段的处理可直接由用户需求模块传至裁决模块，暂决定不进行数据库存储。

* + 1. **默认规则及冲突解决模块**

本模块主要负责设置默认规则以及冲突解决模块，可在用户需求模块中添加前端控件对此模块进行调控。

默认规则即表示对未找到匹配规则的数据包的处理方式，即允许或禁止。

冲突解决可设计为对于所有规则匹配，若对于多条规则均匹配到，若有一条规则禁止则禁止。

* 1. **数据包判决模块**
     1. **解释执行模块**

本模块主要实现两个功能，即IP报文的参数提取以及规则执行。

本项目中，需要抓取的IP参数包括源IP、端口，目的IP、端口、协议类型。

规则执行则主要包括：将报文放行或者阻止。这个功能在例子中已实现。

* + 1. **规则选取模块**

本模块的主要功能为获取参数，向数据库请求所有相关规则，联合冲突解决模块选择正确的报文处理方式。

1. **项目进展情况**
   1. **面向用户需求模块**
      1. **前端交互子模块**

在本模块中，为了配合功能和美观，我们首先设计了UI界面。

主界面：

菜单栏

规则列表（可逐条选中）（可排序）

增添规则

编辑规则

删除规则

开/关

规则编辑弹窗：

源IP地址

源端口

允许/禁止

协议选择

起始时间

结束时间

确认

取消

目的IP地址

源端口

为了代码实现交互界面，我们着重学习了Qt的编程，主要学习了两本教材，《Qt+Creator快速入门》和《Qt及Qt Quick开发实战精解》。

我们主要学习了Qt中，主窗口框架和我们需要使用的部件的使用。由于我们需要使用数据库，我们还学习了QtSql模块，从而连接Qt与数据库。我们这阶段的学习为之后的代码实现铺下了良好的基础。

* + 1. **指令处理子模块**

有关这部分，我们首先设计了规则的输入的检验逻辑。

IP地址应符合IP地址的范围，超出范围或者不规范的输入应该予以提示。

端口的范围应为0至65535的整数。

协议选择，应为下拉框，从预设的协议中选择。

起始时间和结束时间也应该从标准时间选择器中选择。

在本模块中，规则的查询和储存都需要和数据库连接，在本模块中我们利用学习的QtSql与数据库进行连接。

* 1. **数据库模块**
     1. **数据交互子模块**

本模块中，需要完成规则的查询，插入删除功能。使用SQL命令。

* + 1. **数据存储子模块**

在本模块，我们设计了规则储存的表格式。

|  |  |  |
| --- | --- | --- |
| 数据名称 | 类型 | 备注 |
| 标识主键(ID) | Long | 专属标识，自动生成，逐增，不可重复 |
| 创建时间 | Qtime | 创建时间，自动生成 |
| 更新时间 | Qtime | 更新时间，自动生成 |
| 允许/禁止 | BOOL | 本条规则允许或者禁止，非空 |
| 源IP | String | 源IP |
| 源端口 | Int | 源端口 |
| 目的IP | String | 目的IP |
| 目的端口 | Int | 目的端口 |
| 协议选择 | Int | 预设协议 |
| 起始时间 | Qtime |  |
| 终止时间 | Qtime |  |
| 是否删除 | BOOL | 标识是否删除 |

* + 1. **默认规则及冲突解决模块**

在本模块中，我们设计了以下默认规则：

源IP、源端口、目的IP、目的端口，可为空，为空则表示对于全部IP、端口进行匹配。

起始时间、终止时间可为空，为空则表示对于全部时间进行匹配。

冲突规则则采取有一条规则禁止则判决为禁止的规则。

* 1. **数据包判决模块**
     1. **解释执行模块**

单条规则的解释，已经在例子中实现，本模块需要做的是所有规则的匹配和判决。

对于规则选取模块中的选取得到的模块，进行冲突判决之后判决执行。

* + 1. **规则选取模块**

规则选取的过程，我们首先查询并遍历所有规则，将所有符合条件的规则选出，提交至解释执行模块。

1. **目前存在的问题及建议**

（包括存在的问题、困难及意见建议）

1. **下一阶段工作安排**

（以时间为顺序，按条目给出下一阶段需要完成的工作，以及对应的时间安排）