### УДК 004.42

**Е.В. БОРИСОВА**

**E.V. BORISOVA**

**РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ ДЛЯ УПРОЩЕННОЙ НАСТРОЙКИ СЕТЕВОГО ФИЛЬТРА** NETFILTER С ПОМОЩЬЮ **УПРАВЛЯЮЩЕЙ УТИЛИТЫ IPTABLES**

**DEVELOPMENT OF SOFTWARE MODULE FOR SIMPLIFIED SETUP NETWORK FILTER NETFILTER USING THE IPTABLES UTILITY MANAGEMENT**

*В данной статье рассматривается возможность упрощенной настройки сетевого фильтра netfilter с помощью управляющей утилиты iptables , используемого в операционной системе Linux. Для этого разработан программный модуль, который позволяет использовать вместо существующего консольного интерфейса более наглядный и интуитивно понятный графический.*

*Ключевые слова: сетевой фильтр netfilter, утилита iptables, операционная система Linux, программный модуль.*

*This article discusses the possibility of a simplified configuration of network filter netfilter using the management utility iptables is used in Linux operating system. To do this, a software module that allows you to use instead of the existing console interface more intuitive and intuitive graphics.*

*Keywords: netfilter network filter, iptables utility, Linux operating system, software module*

Каждый компьютер, подключенный к сети, находится в потенциальной опасности. В сети много угроз начиная от программ, которые будут пытаться любым способом проникнуть в систему и, заканчивая злоумышленниками, которые хотят получить доступ к нужному им узлу сети. А программное обеспечение, установленное на компьютере, может содержать еще не известные и неисправленные уязвимости, которые и могут стать проблемами в безопасности.

Если для домашних компьютеров это не достаточно актуально, так как они подключены к сети через роутеры и NAT, которые скрывают их от внешней сети, то для серверов это актуально как никогда. Операционная система Linux удобно сочетает в себе высокую производительность работы системы и возможность точной настройки элементов системы под нужды конкретного пользователя. В этой системе в ядро встроен гибкий и надежный firewall netfilter. С помощью утилиты iptables выполняется защита системы от внешних вторжений, перенаправление портов, а также еще очень много действий с трафиком.

Iptables – название пользовательской утилиты (запускаемой из командной строки), предназначенной для управления системой netfilter. С её помощью администраторы систем могут создавать и изменять правила, управляющие фильтрацией и перенаправлением пакетов. Для работы с семейством протоколов IPv6 существует отдельная версия утилиты iptables – ip6tables.

Некоторые авторы под словом netfilter имеют в виду только те элементы межсетевого экрана, которые непосредственно являются частью стека протоколов ядра, а всё прочее (систему таблиц и цепочек) называют iptables. Из-за не совсем ясной терминологии, иногда весь проект (внутриядерный межсетевой экран вместе с пользовательской утилитой) просто именуется netfilter/iptables. [1]

На рисунке 1 схематично отображена работа межсетевого экрана netfilter и его настройка посредством утилиты iptables.

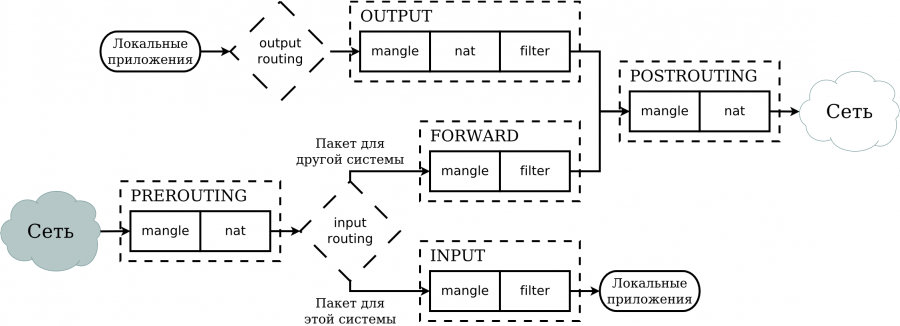


Рисунок 1 - Работа межсетевого экрана netfilter и его настройка посредством утилиты iptables

Ключевыми понятиями iptables являются:

1. Правило –­ состоит из критерия, действия и счетчика.
2. Цепочка – упорядоченная последовательность правил.
3. Таблица – совокупность базовых и пользовательских цепочек, объединенных общим функциональным назначением. [1]

На рисунке 2 представлена диаграмма прохождения таблиц и цепочек.

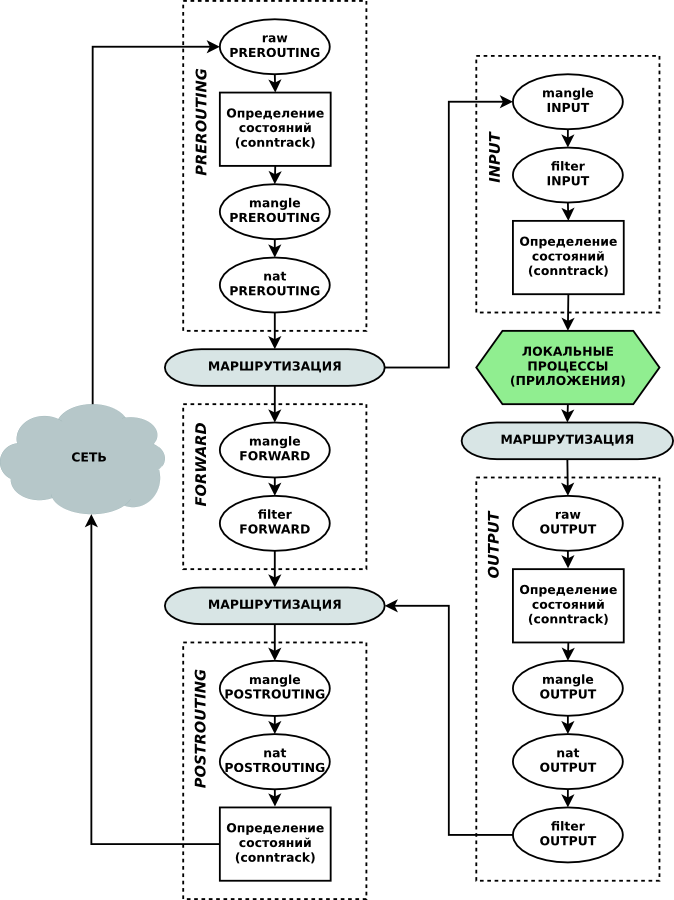


Рисунок 2 – Диаграмма прохождения таблиц и цепочек

Целью разработки программного модуля для упрощённой настройки сетевого фильтра iptables является создание удобного графического интерфейса для настройки и управления межсетевым экраном netfilter. На данный момент существовал только консольный режим, с которым не всем пользователям удобно работать.

Основной функцией разработанного программного модуля является создание Bash скрипта, который будет задавать настройки сетевого экрана iptables.

В предлагаемом продукте реализована возможность создания, удаления и сохранения правил, используемых для настройки межсетевого экрана iptables.

Программа была написана на языке С++ с использованием фреймворка Qt.

На рисунке 3 представлен снимок экрана, отображающий процесс написания программы.

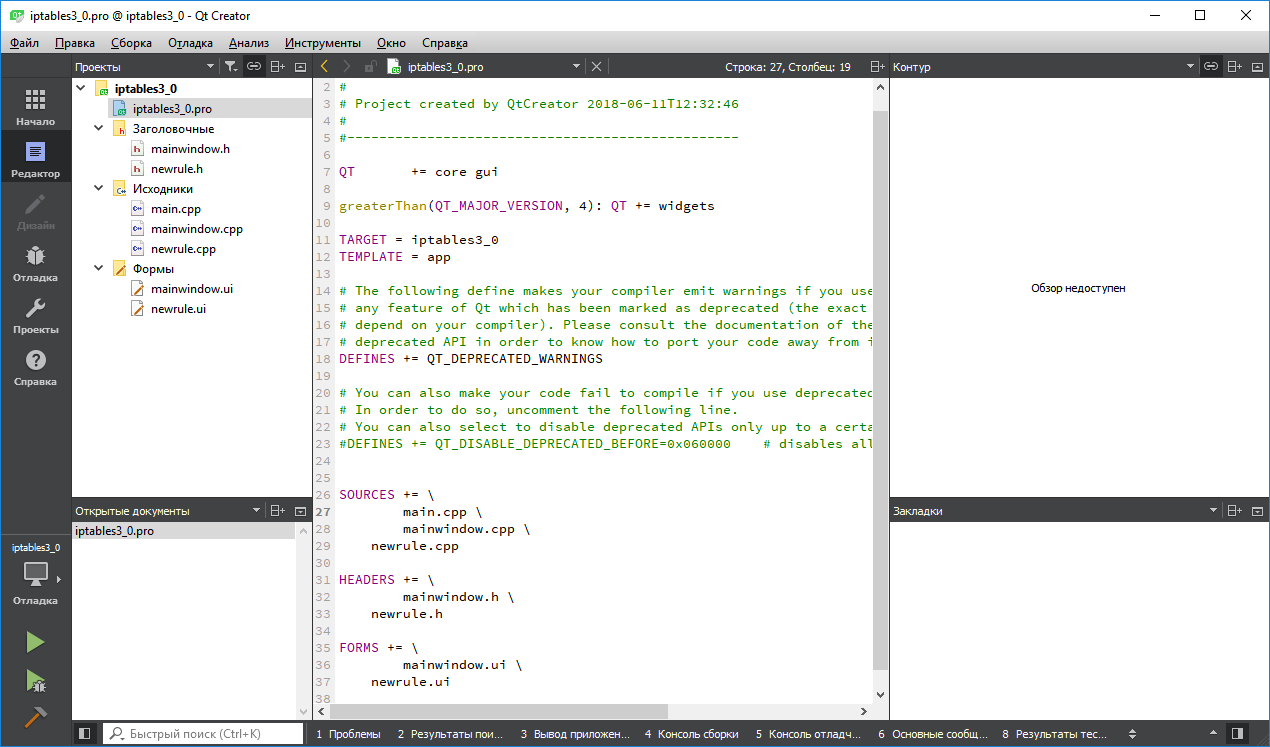


Рисунок 3 – Фрагмент кода программы

В программном модуле предусмотрена реализация возможности создания, удаления и сохранения правил, используемых для настройки МЭ iptables. Рисунок 4 демонстрирует предлагаемый графический интерфейс главного меню программного модуля.

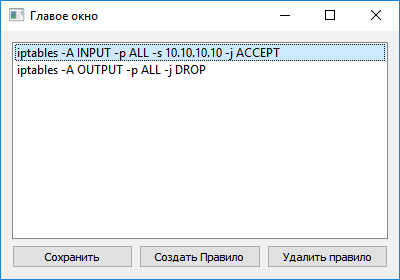


Рисунок 4 - Главное меню программного модуля

Сначала пользователю предлагается выбрать таблицу, для которой будет создаваться правило.

Далее, в зависимости от выбора таблицы необходимо выбрать цепочку, в которой будет создаваться правило.

Существует 5 типов стандартных цепочек, встроенных в систему:

1. PREROUTING – для изначальной обработки входящих пакетов.
2. INPUT – для входящих пакетов, адресованных непосредственно локальному процессу (клиенту или серверу).
3. FORWARD – для входящих пакетов, перенаправленных на выход (можно заметить, что перенаправляемые пакеты проходят сначала цепь PREROUTING, затем FORWARD и POSTROUTING).
4. OUTPUT – для пакетов, генерируемых локальными процессами.
5. POSTROUTING – для окончательной обработки исходящих пакетов.

Также можно создавать и уничтожать собственные цепочки при помощи утилиты iptables.

Цепочки организованны в 4 таблицы:

1. Raw – просматривается до передачи пакета системе определения состояний. Используется редко, например, для маркировки пакетов, которые не должны обрабатываться системой определения состояний. Для этого в правиле указывается действие NOTRACK. Содержит цепочки PREROUTING и OUTPUT.
2. Mangle – содержит правила модификации (обычно заголовка) IP‐пакетов. Среди прочего, поддерживает действия TTL (Time to live), TOS (Type of Service), и MARK (для изменения полей TTL и TOS, и для изменения маркеров пакета). Содержит все пять стандартных цепочек.
3. Nat – просматривает только пакеты, создающие новое соединение (согласно системе определения состояний). Поддерживает действия DNAT, SNAT, MASQUERADE, REDIRECT. Содержит цепочки PREROUTING, OUTPUT, и POSTROUTING.
4. Filter – основная таблица, используется по умолчанию если название таблицы не указано. Содержит цепочки INPUT, FORWARD, и OUTPUT.

Цепочки с одинаковым названием, но в разных таблицах — совершенно независимые объекты. Например, raw PREROUTING и mangle PREROUTING обычно содержат разный набор правил. Пакеты сначала проходят через цепочку raw PREROUTING, а потом через mangle PREROUTING. [1]

На рисунке 5 представлен разработанный графический интерфейс меню выбора цепочки.

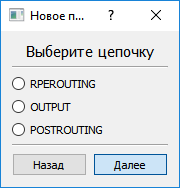
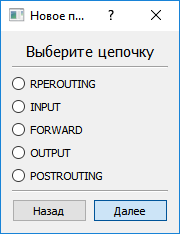
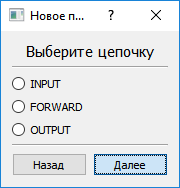


Рисунок 5 - Меню выбора цепочки

После выбора цепочки можно пропустить или выбрать дополнительные условия для фильтрации пакета.

В системе netfilter, каждый пакет, проходящий через механизм определения состояний, может иметь одно из четырёх возможных состояний:

1. NEW – пакет открывает новый сеанс. Классический пример – пакет TCP с флагом SYN.
2. ESTABLISHED – пакет является частью уже существующего сеанса.
3. RELATED – пакет открывает новый сеанс, связанный с уже открытым сеансом. Например, во время сеанса пассивного FTP, клиент подсоединяется к порту 21 сервера, сервер сообщает клиенту номер второго, случайным образом выбранного порта, после чего клиент подсоединяется ко второму порту для передачи файлов. В этом случае второй сеанс (передача файлов по второму порту) связан с уже существующим сеансом (изначальное подсоединение к порту 21).
4. INVALID – все прочие пакеты. [1]

В случае, например, если выбрана цепочка FORWARD – предлагается выбрать для каких типов пакетов (источника или назначения), будет создаваться правило. На рисунке 6 отображен разработанный графический интерфейс меню выбора условия.

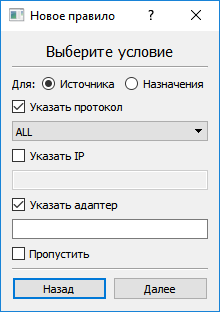
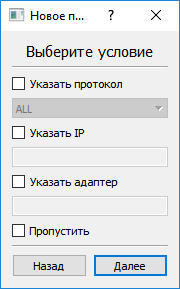


Рисунок 6 - Меню выбора условия

Далее следует выбрать действие, которое будет совершаться с пакетом. На рисунке 7 представлено как отображается меню выбора действия.

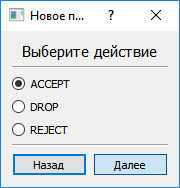


Рисунок 7 - Меню выбора действия

В конце необходимо подтвердить добавление правила в массив. На рисунке 6 показан разработанный графический интерфейс меню подтверждения.

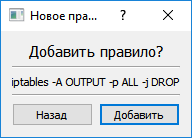
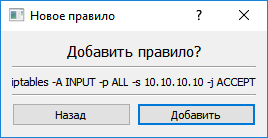


Рисунок 8 - Меню подтверждения

В качестве практического применения программный модуль целесообразно использовать как инструмент для более быстрой и наглядной настройки iptables в дистрибутивах OC Linux с графической оболочкой.

**СПИСОК ЛИТЕРАТУРЫ**

* 1. Войтов Н.М. Администрирование Red Hat Enterprise Linux. – М.: ДМК Пресс, 2011. – 192 с.

**Борисова Екатерина Владимировна**

ОГБПОУ "Рязанский колледж электроники"

Тел.: +7(920)632-13-33

E-mail: ekaterina21333@yandex.ru