Московский физико-технический институт
(государственный университет)
Факультет радиотехники и кибернетики
Кафедра информатики и вычислительной техники

Фильтрация сетевых пакетов на основе мандатных меток в операционной системе «Эльбрус»

Выпускная квалификационная работа
(бакалаврская работа)

Студент: Имкенов Адьян, 313 группа
Научный руководитель: к.т.н. Морозов Ю.В.

Москва, 2017

Введение

- Межсетевой экран (МЭ) – комплекс программных и аппаратных средств, осуществляющий фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

В ядре ОС «Эльбрус» реализована мандатная модель разграничения доступа в качестве модуля Elmac.

- Всем субъектам (процессам) и объектам (файлам) назначаются уровни доступа (мандатные метки). Мандатная метка состоит из пары значений: уровень и категория доступа.
- Сетевые пакеты, отправляемые процессом, наследуют мандатную метку этого процесса. Метка добавляется в дополнительный заголовок IPv4-пакета по стандарту RFC 1108.
- В целях контроля доступа субъектов к сетевым ресурсам межсетевые экраны должны поддерживать фильтрацию по мандатным меткам.

Цель

Реализовать фильтрацию сетевого трафика с учетом мандатных меток сетевых пакетов в межсетевом экране Netfilter в составе ядра Linux.

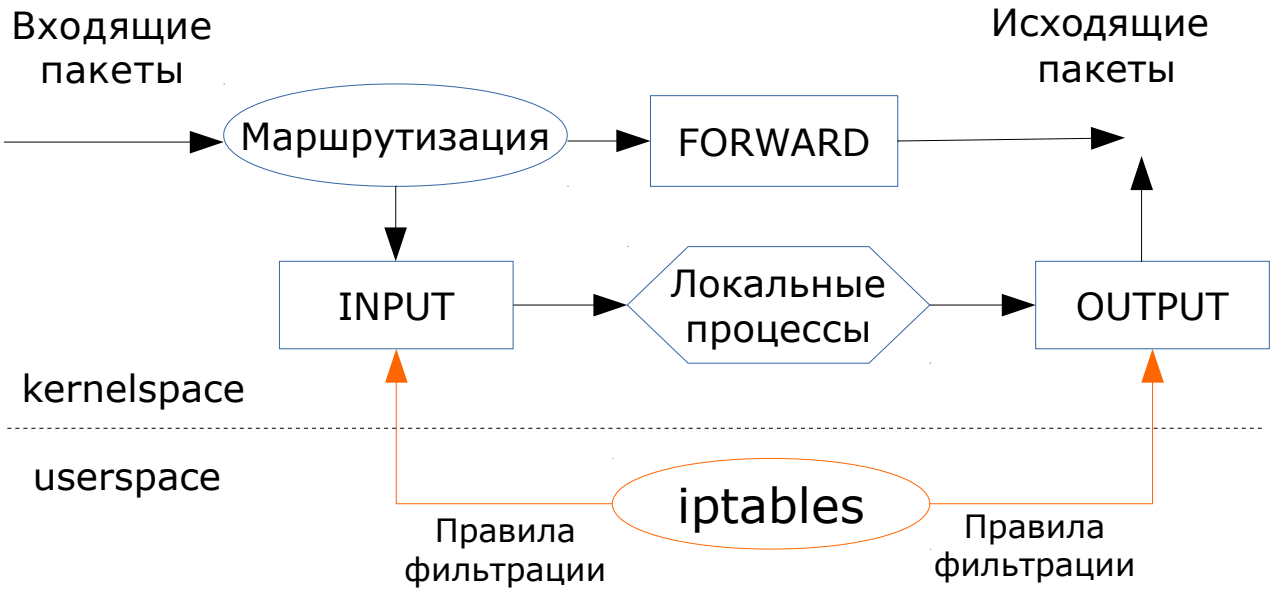
Задачи

- Изучить принцип работы межсетевого экрана Netfilter.
- Разработать расширение для Netfilter, позволяющее пропускать/блокировать сетевые пакеты на основе мандатных меток.
- Разработать расширение для создания правил фильтрации, учитывающих мандатные метки.

Требования

- Поддержка протокола IPv4.
- Фильтрация на основе сравнения метки сетевого пакета и метки хоста назначения/отправления.

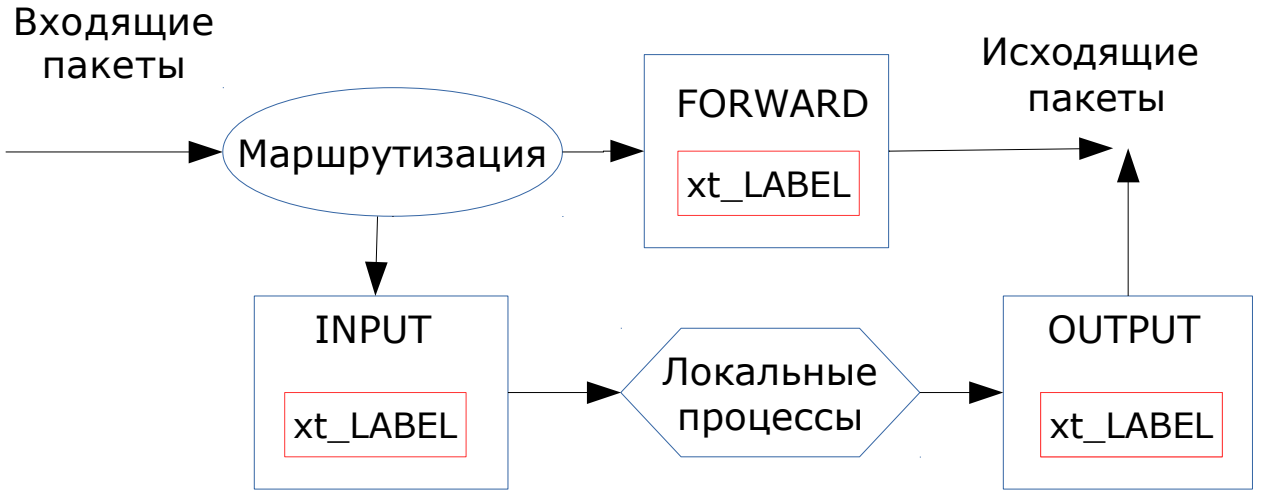
Схема фильтрации сетевых пакетов в системе Netfilter, реализованная в ядре Linux



Основу работы Netfilter составляют цепочки – упорядоченные наборы правил. В данной реализации для фильтрации применяются 3 базовые цепочки: INPUT, FORWARD и OUTPUT.

1. Сетевые пакеты, предназначенные для локальной машины попадают в цепочку INPUT. Проходящие пакеты – в цепочку FORWARD. Исходящие пакеты – в цепочку OUTPUT.
2. Правила фильтрации устанавливаются утилитой iptables. Они состоят из критерия и действия. Когда пакет проходит через цепочку, система netfilter проверяет, соответствует ли пакет всем критериям правила, и если так, то выполняет заданное действие (обычно ACCEPT или DROP).
3. Критериями являются поля заголовков сетевых пакетов: адрес отправителя/получателя, номер сетевого интерфейса, тип транспортного протокола и др.

Расширение Netfilter для пропуска/блокировки сетевых пакетов на основе мандатных меток

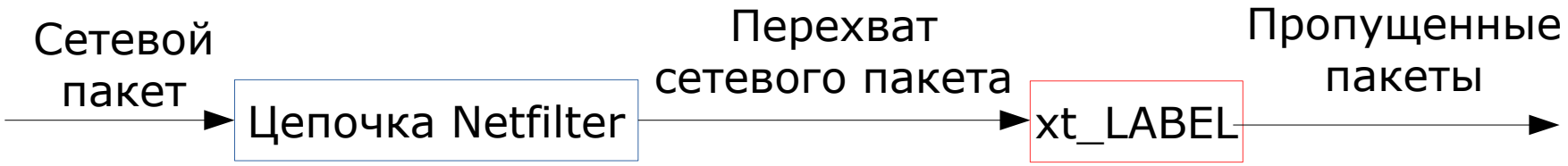


Механизм xtables-addons позволяет создавать пользовательские модули ядра и встраивать их в цепочки Netfilter.

Для фильтрации сетевого трафика по мандатным меткам разработан модуль ядра xt_LABEL, перехватывающий входящие и исходящие сетевые пакеты и выполняющий следующие функции:

- Разбор заголовков сетевых пакетов для выделения мандатной метки
- Передача метки пакета в монитор мандатного разграничения доступа для сравнения с меткой хоста/порта назначения
- Принятие решения о пропуске/блокировке пакета по результатам сравнения

Функциональность модуля xt_LABEL



label_tg (struct sk_buff *skb, struct xt_action_param *par) – функция фильтрации пакетов

- skbuff_getattr(skb) — Выделяет метку из сетевого пакета
- par->host_label — Получает метку хоста из iptables
- mac_access() — Сравнивает метки

sk_buff *skb — структура сетевого пакета

xt_action_param *par – параметры, полученные из правила iptables

xt_register_targets() – функция регистрации в цепочках Netfilter

Заполнение структуры

struct label_tg_reg

Поля структуры
- name = «LABEL» — Название расширения
- target = label_tg — Вызываемая функция
- hooks = NF_INET_LOCAL_IN | NF_INET_LOCAL_OUT | NF_INET_FORWARD — Цепочки, в которые встраивается расширение

Расширение iptables для создания правил фильтрации на основе мандатных меток

Для утилиты iptables разработано расширение libxt_LABEL, которое позволяет применять к сетевым пакетам действие LABEL для их фильтрации по мандатным меткам.

Общий синтаксис правил:

iptables -A [цепочка] [критерии] -j LABEL --level [уровень] --cat [категория]

С помощью набора базовых критериев фильтрации можно назначить определенному хосту/порту мандатную метку, с которой будут сравниваться метки сетевых пакетов.

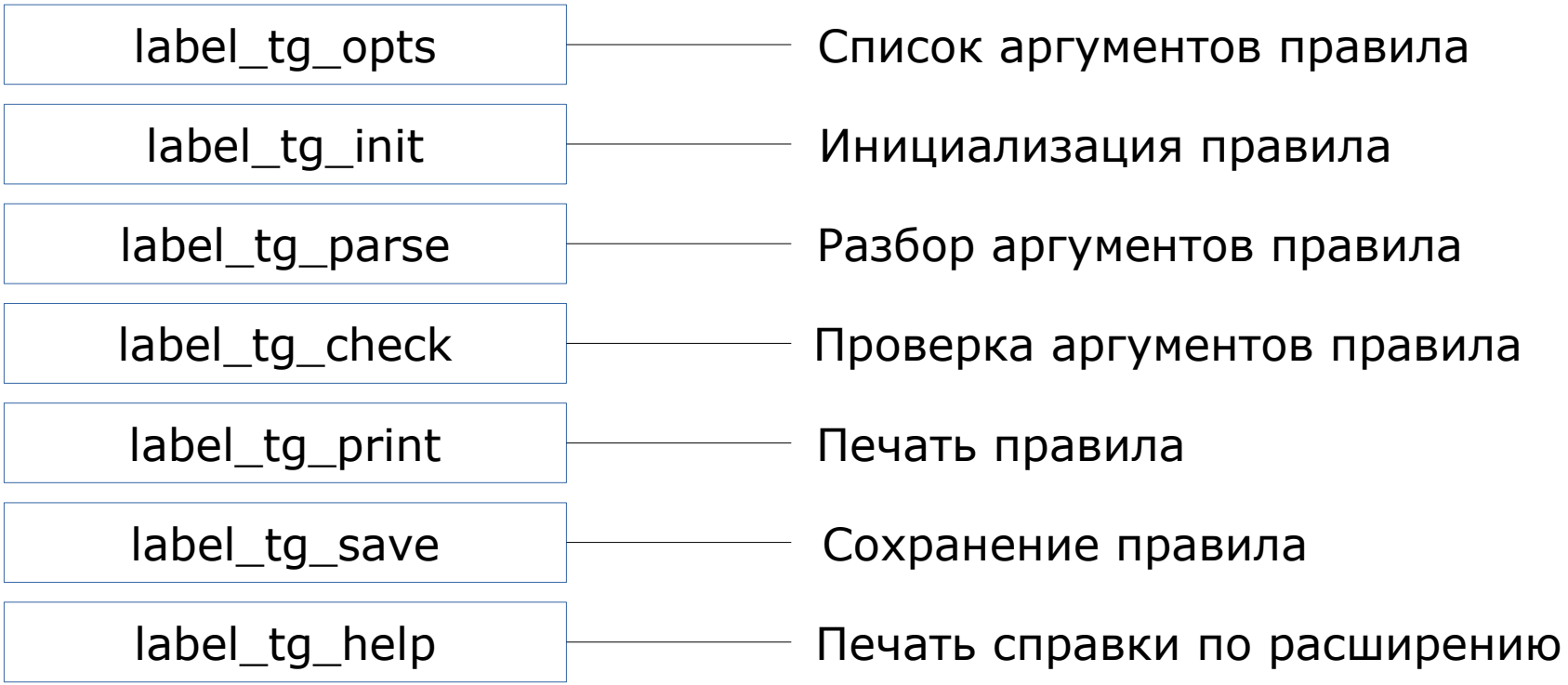
Пример: Фильтрация входящего ssh-соединения.

iptables -P INPUT DROP
iptables -A INPUT -p tcp --dport 22 -j LABEL --level 1 --cat 1

Первое правило задает политику по умолчанию отклонять все входящие пакеты. Второе правило разрешает доступ по протоколу ssh (порт 22) сетевым пакетам с мандатной меткой 1:1.

Функциональность libxt_LABEL

В рамках создания расширения разработаны следующие функции:



Пример тестирования

Команда ping выполняется с различными мандатными метками к машине, на которой заданы правила фильтрации:

iptables -P INPUT DROP
iptables -A INPUT -p icmp -j LABEL —level 3 – cat 1

Результаты тестирования

```
elbrus-1 ~ # elmacexec --level 1 --cat 1 -- ping -c2 192.168.0.4
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.

--- 192.168.0.4 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 999ms

elbrus-1 ~ # elmacexec --level 2 --cat 1 -- ping -c2 192.168.0.4
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.

--- 192.168.0.4 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 999ms

elbrus-1 ~ # elmacexec --level 3 --cat 1 -- ping -c2 192.168.0.4
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.
64 bytes from 192.168.0.4: icmp_seq=1 ttl=64 time=0.403 ms
64 bytes from 192.168.0.4: icmp_seq=2 ttl=64 time=0.310 ms

--- 192.168.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.310/0.356/0.403/0.050 ms
```

Результаты

- Реализован модуль ядра xt_LABEL, фильтрующий сетевые пакеты на основе их мандатных меток
- Модуль xt_LABEL встроен в цепочки INPUT, OUTPUT и FORWARD межсетевого экрана netfilter
- Разработано расширение libxt_LABEL для утилиты iptables, позволяющее создавать правила фильтрации, учитывающие мандатные метки
- Проведено тестирование
- Разработка готовится к внедрению в рамках ОКР «Малахит»