Для цитирования: Имкенов А. А., Морозов Ю. В., Межуев Ю. В. Фильтрация сетевых пакетов на основе мандатных меток в операционной системе «Эльбрус» // Вопросы радиоэлектроники. 2018. № 2. С. 65–68.
УДК 004.056.53

А. А. Имкенов[1, 2], Ю. В. Морозов[1], Ю. В. Межуев[1]

[1] АО «МЦСТ», [2] МФТИ (ГУ)

ФИЛЬТРАЦИЯ СЕТЕВЫХ ПАКЕТОВ НА ОСНОВЕ МАНДАТНЫХ МЕТОК В ОПЕРАЦИОННОЙ СИСТЕМЕ «ЭЛЬБРУС»

Для защиты сегментов сети или отдельных узлов от несанкционированного доступа применяются средства межсетевого экранирования. Межсетевой экран – комплекс программных и/или аппаратных средств, осуществляющих фильтрацию сетевых пакетов на основе заданных правил. В операционной системе «Эльбрус» всем сетевым пакетам назначаются мандатные атрибуты (метки) безопасности, обеспечивающие разграничение доступа локальных процессов к ресурсам операционной системы. Для повышения степени защищенности при межсетевом взаимодействии необходимо обеспечить поддержку мандатных атрибутов при создании правил фильтрации. В статье подробно рассмотрено устройство межсетевого экрана Netfilter, применяемого в операционной системе «Эльбрус». Описана реализованная схема фильтрации входящих, исходящих и транзитных сетевых пакетов на основе их мандатных атрибутов безопасности. Приведен пример построения правил фильтрации.

Ключевые слова: *межсетевое экранирование, защита от несанкционированного доступа, операционная система «Эльбрус», Netfilter.*

Введение

В составе средств ОС «Эльбрус», обеспечивающих защиту информации, реализован механизм мандатного разграничения доступа в виде модуля ядра Elmac (Elbrus mandatory access control). В рамках мандатной модели всем субъектам и объектам назначаются метки (уровни) доступа. В операционной системе под субъектами понимаются процессы, а в качестве объектов выступают файлы или другие процессы. При обращении субъекта к объекту происходит сравнение их меток, и на его основе принимается решение о предоставлении доступа. Мандатная метка состоит из мандатного уровня и категории.

Кроме объектов файловой системы модуль Elmac контролирует трафик сообщений, пересылаемых в рамках локального многопроцессорного взаимодействия. В контексте Internet фильтрация сетевых пакетов на основе мандатных меток выполняется с использованием описанных в данной статье средств сетевого экранирования. В данный момент эти средства реализованы применительно к версии v4 протокола IP.

Межсетевой экран Netfilter

Состав и функционирование

Межсетевой экран (Firewall) – комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. В ядре ОС «Эльбрус» межсетевой экран реализован в качестве подсистемы Netfilter.

Основу работы Netfilter составляют цепочки – упорядоченные наборы правил, задающих критерии их применения и действия. Определено пять основных цепочек Netfilter (рис. 1):

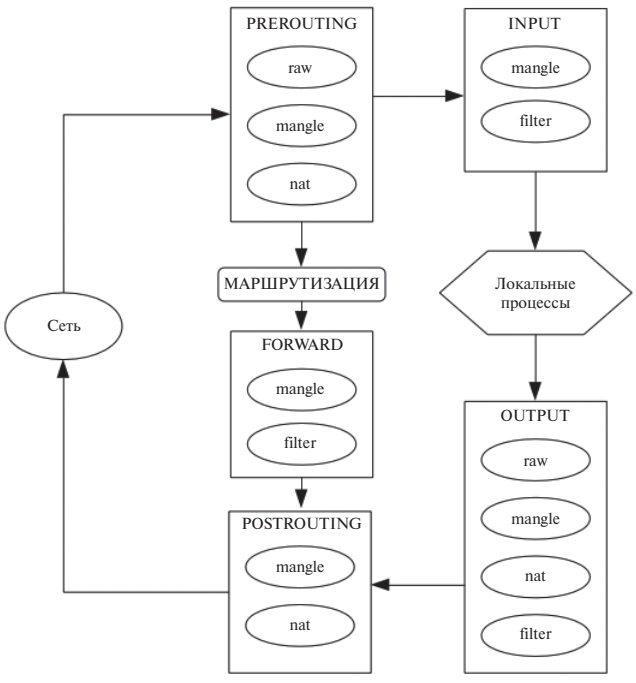

Рисунок 1. Цепочки межсетевого экрана Netfilter

- PREROUTING – для предварительной обработки входящих пакетов;
- INPUT – для входящих пакетов, адресованных локальной машине;
- FORWARD – для проходящих (маршрутизируемых) пакетов;
- OUTPUT – для исходящих пакетов;
- POSTROUTING – для окончательной обработки исходящих пакетов.

Цепочки состоят из набора таблиц, которые представляют собой упорядоченный список правил со схожим функциональным назначением [1, 2]. Определены следующие таблицы:

- raw – используется в основном для маркировки пакетов, которые не должны обрабатываться системой определения состояний, содержащейся в цепочках PREROUTING и OUTPUT;
- mangle – включает правила модификации IP-пакетов (обычно полей заголовка), содержится во всех пяти стандартных цепочках;
- nat – предназначена для подмены адреса отправителя или получателя в головных пакетах потока – во всех последующих пакетах подмена осуществляется автоматически; содержится в цепочках PREROUTING, OUTPUT и POSTROUTING;
- filter – предназначена для фильтрации сетевых пакетов, содержится в цепочках INPUT, FORWARD и OUTPUT.

При входе в вычислительную систему сетевые пакеты поступают в интерфейс операционной системы, настроенный на стек TCP/IP, и после простых проверок ядром (например, по контрольной сумме) проходят последовательность цепочек, первой из которых является PREROUTING. После этой цепочки в соответствии с таблицей маршрутизации проверяется назначение пакета и в зависимости от результата определяется его дальнейший маршрут. Если пакет не адресован локальной системе, то он направляется в цепочку FORWARD, иначе – в цепочку INPUT, пройдя которую, передается локальным процессам. В итоге обработки локальной программой при необходимости формируется ответ. Пакеты, исходящие от локальной системы, попадают в цепочку OUTPUT. После цепочки OUTPUT (или цепочки FORWARD, если пакет был проходящим) пакеты отправляются в цепочку POSTROUTING для окончательной обработки. Проходя через цепочки, пакет в каждой таблице последовательно сверяется с набором критериев правил, и если он соответствует какому-либо критерию, то выполняется заданное в правиле действие над пакетом [1, 2].

Управление межсетевым экраном

Межсетевой экран Netfilter управляется через интерфейс, предоставляемый утилитой iptables, которая позволяет редактировать правила таблиц, таблицы и цепочки. Правило – это запись/строка, включающая в себя критерии отбора сетевых пакетов и действие над ними, которые соответствуют заданному правилу. Задача утилиты iptables состоит в передаче критериев и действия правил в цепочки Netfilter, где на их основе производится фильтрация сетевых пакетов [3].

Формат команд iptables:

iptables -t [*таблица*] *команда* [*критерии*] [*действие*].

По умолчанию для создания правил используется таблица filter, для создания правил в другой таблице необходимо указать ее название с ключом -t. После имени таблицы указывается команда, определяющая действие с правилом: вставить правило, добавить правило в конец цепочки, удалить правило. Критерии задают параметры отбора пакетов, действие указывает, какое действие необходимо выполнить над пакетом при условии совпадения критериев отбора в правиле [3].

Реализация

В данной реализации для фильтрации сетевых пакетов используются три базовые цепочки – INPUT,

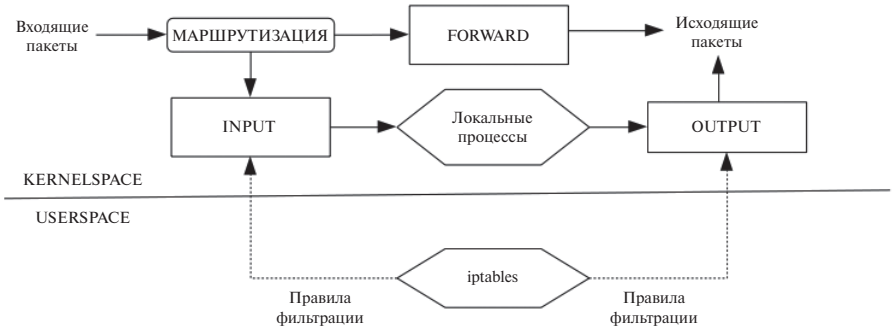

Рисунок 2. Схема фильтрации межсетевого экрана Netfilter

OUTPUT и FORWARD (рис. 2), проходя через которые, пакет последовательно сверяется с каждым набором критериев, заданных во всех правилах, и если пакет соответствует какому-либо критерию, то выполняется заданное действие. Обычно используются два основных действия: ACCEPT – «принять пакет» и DROP – «отбросить пакет». Правила фильтрации задаются в пространстве пользователя и передаются в соответствующие цепочки ядра системы.

Механизм xtables-addons представляет собой фреймворк для создания пользовательских модулей в целях расширения функционала Netfilter. Основным преимуществом xtables-addons является отсутствие необходимости налагать патчи на ядро и iptables, что значительно упрощает процесс разработки и сопровождения. Расширения создаются в виде модулей ядра и могут быть загружены по желанию пользователя [4].

В рамках данной работы разработан модуль ядра xt_LABEL, предназначенный для работы с сетевыми пакетами, имеющими мандатную метку по стандарту RFC1108. С использованием механизма xtables-addons модуль был встроен в цепочки межсетевого экрана INPUT, OUTPUT и FORWARD, предназначенные для фильтрации сетевых пакетов (рис. 3). Модуль перехватывает входящие и исходящие сетевые пакеты и производит разбор заголовков пакетов для выделения мандатной метки. Далее происходит сравнение мандатной метки пакета и хоста, которому он предназначается, и принимается решение о пропуске или блокировке пакета. Для сравнения меток используется функция mac_access, реализованная в рамках монитора мандатной защиты Elmac.

С целью назначения мандатной метки хостам разработано расширение libxt_LABEL для утилиты iptables. Оно позволяет применять действие LABEL при построении правил фильтрации сетевых пакетов. В правиле необходимо указать название действия опцией –j, мандатный уровень хоста опцией –level и мандатную категорию хоста опцией –cat.

Синтаксис правил:

iptables –A [*цепочка*] [*критерии*] *–j LABEL –level* [*уровень*] *–cat [категория*].

Действие LABEL применяется к входящим, исходящим и транзитным сетевым пакетам, проходящим через цепочки INPUT, FORWARD и OUTPUT. С помощью набора базовых критериев фильтрации можно назначить определенному порту/хосту мандатную метку, с которой будут сравниваться метки сетевых пакетов.

Пример

Одной из самых популярных задач, решаемых с помощью межсетевого экрана, является ограничение входящих соединений. На сервере развернут сервер печати CUPS (tcp-протокол, порт 631). Необходимо запретить доступ к сетевому принтеру всем пользователям, кроме пользователей с мандатной меткой 1:1. Для решения такой задачи необходимо задать на сервере следующие правила фильтрации:

iptables –A INPUT –P DROP #По умолчанию отклоняем все входящие пакеты.
iptables –A INPUT –p tcp –dport 22 –j LABEL –level 1 –cat 1 #Пропускаем только сетевые пакеты с меткой 1:1.

Заключение

В статье описана реализация фильтрации сетевых пакетов на основе мандатных меток, реализованная в ОС «Эльбрус». Было проведено исследование функциональности встроенного межсетевого экрана Netfilter, разработаны модуль ядра xt_LABEL для разбора заголовков пакетов и расширение для утилиты iptables, позволяющее создавать правила фильтрации на основе мандатной политики. Описанное решение позволяет обеспечить надежную защиту вычислительного комплекса от несанкционированного доступа на уровне межсетевого взаимодействия.

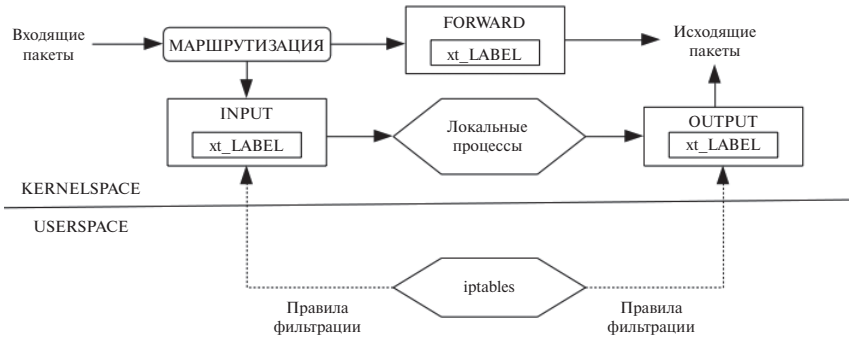

Рисунок 3. Разработанная схема фильтрации с использованием модуля xt_LABEL

СПИСОК ЛИТЕРАТУРЫ

1. Russel R. Packet Filtering HowTo. Netfilter Core Team, 2012. Available at: https://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html (accessed 15.11.2017)
2. Russel R., Welte H. Linux Netfilter hacking. Netfilter Core Team, 2012. Available at: https://www.netfilter.org/documentation/HOWTO/netfilter-hacking-HOWTO.html (accessed 15.11.2017)
3. Andreasson O. Iptables Tutorial 1.2.2. Available at: https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html (accessed 15.11.2017)
4. Engelhardt J., Bouliane N. Writing Netfilter modules. Netfilter Core Team, 2012, pp. 5–35. Available at: http://inai.de/documents/Netfilter_Modules.pdf (accessed 15.11.2017)

ИНФОРМАЦИЯ ОБ АВТОРАХ

Имкенов Адьян Арсланович, студент, МФТИ (ГУ); инженер-программист, АО «МЦСТ», 119334, Москва, ул. Вавилова, д. 24, тел.: 8 (495) 135-955-52, e-mail: adjan.a.imkenov@mcst.ru.
Морозов Юрий Владимирович, начальник отдела, АО «МЦСТ», 119334, Москва, ул. Вавилова, д. 24, тел.: 8 (495) 135-955-52, e-mail: muvlad@mcst.ru.
Межуев Юрий Васильевич, ведущий инженер-программист, АО «МЦСТ», 119334, Москва, ул. Вавилова, д. 24, тел.: 8 (495) 135-955-52, e-mail: yury.v.mezhuev@mcst.ru.

For citation: Imkenov A. A., Morozov Yu. V., Mezhuev Yu. V. Packet filtering based on mandatory labels in the Elbrus operating system. Voprosy radioelektroniki, 2018, no. 2, pp. 65–68.

A. A. Imkenov, Yu. V. Morozov, Yu. V. Mezhuev

PACKET FILTERING BASED ON MANDATORY LABELS IN THE ELBRUS OPERATING SYSTEM

Firewall is used in order to protect network segments or individual hosts from unauthorized access. It is a set of software and hardware designed to filter network connections based on predefined rules. In the operating system Elbrus all network packets are assigned to the mandatory secure attributes (labels), providing access control for local processes to operating system resources. To increase the degree of protection during the network interaction it is necessary to support the mandatory attributes for creating filtering rules. The article describes in detail the arrangement of Netfilter firewall which is used in operating system Elbrus. Described the implemented filtering scheme of incoming, outgoing and transit network packets based on their mandatory secure attributes. Given an example of creation of filter rules.

Keywords: firewall, information security, Elbrus operating system, Netfilter.

REFERENCES

1. Russel R. [Packet Filtering HowTo]. Netfilter Core Team, 2012. Available at: https://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html (accessed 15.11.2017)
2. Russel R., Welte H. [Linux Netfilter hacking]. Netfilter Core Team, 2012. Available at: https://www.netfilter.org/documentation/HOWTO/netfilter-hacking-HOWTO.html (accessed 15.11.2017)
3. Andreasson O. [Iptables Tutorial 1.2.2]. Available at: https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html (accessed 15.11.2017)
4. Engelhardt J., Bouliane N. [Writing Netfilter modules]. Netfilter Core Team, 2012, pp. 5–35. Available at: http://inai.de/documents/Netfilter_Modules.pdf (accessed 15.11.2017)

AUTHORS

Imkenov Adyan, student, MIPT; engineer-programmer, JSC MCST, 24, ulitsa Vavilova, Moscow, 119334, Russian Federation, tel.: +7 (495) 135-955-52, e-mail: adjan.a.imkenov@mcst.ru.
Morozov Yuriy, head of Department, JSC MCST, 24, ulitsa Vavilova, Moscow, 119334, Russian Federation, tel.: +7 (495) 135-955-52, e-mail: muvlad@mcst.ru.
Mezhuev Yuriy, leading engineer-programmer, JSC MCST, 24, ulitsa Vavilova, Moscow, 119334, Russian Federation, tel.: +7 (495) 135-955-52, e-mail: yury.v.mezhuev@mcst.ru.