УДК 004.056 https://doi.org/10.33619/2414-2948/84/44

IPTABLES ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СЕТЕЙ НА БАЗЕ LINUX

©Лиманова Н. И., *ORCID: 0000-0003-2924-5602, SPIN-код: 9799-8380, д-р техн. наук, Поволжский государственный университет телекоммуникаций и информатики, г. Самара, Россия, nataliya.i.limanova@gmail.com*
©Третьяков Е. Ю., *ORCID: 0000-0002-1591-8100, Поволжский государственный университет телекоммуникаций и информатики, г. Самара, Россия, egor.tretyakov.03@mail.ru*

IPTABLES FOR SECURITY OF LINUX-BASED INFORMATION NETWORKS

©Limanova N., *ORCID: 0000-0003-2924-5602, SPIN-code: 9799–8380, Dr. habil., Povolzhsky State University of Telecommunications and Informatics, Samara, Russia, nataliya.i.limanova@gmail.com*
©Tretyakov E., *ORCID: 0000-0002-1591-8100, Povolzhsky State University of Telecommunications and Informatics, Samara, Russia, egor.tretyakov.03@mail.ru*

Аннотация. В статье рассмотрены основные компоненты информационной безопасности: конфиденциальность, целостность и доступность. Пароли, шифрование, аутентификация и защита от проникновения – это методы, предназначенные для обеспечения конфиденциальности. Целостность означает поддержание данных в исходном состоянии и предотвращение их изменения: случайного или злонамеренного. Под обеспечением доступности информации понимают соответствие сетевых и вычислительных ресурсов ожидаемому объему доступа к данным и реализацию политики резервного копирования для целей аварийного восстановления. Для обеспечения безопасности информационных сетей на базе RedOS наилучшим образом показала себя утилита iptables, используемая для настройки брандмауэра ядра Linux. Несмотря на то, что на первый взгляд реализация IP-маршрутизации в Linux может выглядеть довольно сложной, на практике наиболее распространенные варианты использования (NAT и/или базовый брандмауэр Интернета) значительно проще реализуются. IPTABLES — это пользовательская утилита, позволяющая работать цепочками/правилами. В статье подробно рассмотрены принципы работы iptables, приведено подробное описание таблиц nat, mangle, filter, raw и цепочек. Таблица nat используется для трансляции сетевых адресов, mangle применяется для искажения пакетов, filter дает возможность выполнять фильтрацию пакетов, raw и ее цепочки используются перед любыми другими таблицами в netfilter. Цепочка input применяется для обработки входящих пакетов и подключений, forward – для проходящих пакетов, output – для исходящих пакетов. Показано, что для обеспечения безопасности функционирования компьютерных классов и всей сетевой инфраструктуры в целом, достаточно только двух таблиц: filter и nat. Другие таблицы предназначены для сложных конфигураций, включающих несколько маршрутизаторов и решений по маршрутизации. Приведены результаты использования iptables на основе опыта администрирования информационных сетей на базе RedOS в федеральном государственном бюджетном образовательном учреждении высшего образования «ПГУТИ».

Т. 8. №11. 2022
https://doi.org/10.33619/2414-2948/84

Abstract. The article discusses the main components of information security: confidentiality, integrity and accessibility. Passwords, encryption, authentication, and intrusion protection are methods designed to ensure confidentiality. Integrity means maintaining the data in its original state and preventing its modification: accidental or malicious. Ensuring the availability of information is understood as the compliance of network and computing resources with the expected amount of data access and the implementation of a backup policy for disaster recovery purposes. To ensure the security of information networks based on RedOS, the iptables utility, used to configure the Linux kernel firewall, has proven itself in the best way. Despite the fact that at first glance the implementation of IP routing in Linux may look quite complicated, in practice the most common use cases (NAT and/or basic Internet firewall) are much easier to implement. IPTABLES is a custom utility that allows you to work with chains/rules. The article describes in detail the principles of iptables operation, provides a detailed description of the NAT, mangle, filter, raw tables and chains. The NAT table is used to translate network addresses, mangle is used to distort packets, filter makes it possible to filter packets, raw and its chains are used before any other tables in netfilter. The input chain is used to process incoming packets and connections, forward – for passing packets, output – for outgoing packets. It is shown that to ensure the safety of the functioning of computer classes and the entire network infrastructure as a whole, only two tables are sufficient: filter and nat. Other tables are designed for complex configurations involving multiple routers and routing solutions. The results of using iptables based on the experience of administration of information networks based on RedOS in the federal state budgetary educational institution of higher education PSUTI are presented.

Ключевые слова: информационная безопасность, IPTABLES, обработка пакетов, конфиденциальность данных, доступность информации, целостность информации.

Keywords: information security, IPTABLES, encryption, data confidentiality, information availability, information integrity.

С развитием информационных систем быстрыми темпами начался процесс информатизации большинства областей деятельности по всему миру. Информатизация затронула все сферы жизни людей. Информационная безопасность стала одной из наиболее важных частей структуры информационного общества.

Информационная безопасность — это набор методов, предназначенных для защиты персональных данных от несанкционированного доступа или их изменения, как при хранении, так и при передаче с одного компьютера на другой. Основные компоненты информационной безопасности чаще всего сводятся к 3 пунктам: конфиденциальность, целостность и доступность. Данные являются конфиденциальными, если они могут быть доступными ограниченному кругу лиц. Для обеспечения конфиденциальности необходимо иметь возможность определять, кто пытается получить доступ к данным, и блокировать попытки тех, кто не авторизован. Пароли, шифрование, аутентификация и защита от проникновения — это методы, предназначенные для обеспечения конфиденциальности [5].

Целостность означает поддержание данных в исходном состоянии и предотвращение их изменения: случайного или злонамеренного. Многие методы, обеспечивающие конфиденциальность, также защищают и целостность данных. Хакер не может изменить данные, к которым у него нет доступа. Существуют и другие инструменты, которые помогают обеспечить глубокую защиту целостности: контрольные суммы позволяют проверить данные, например, программное обеспечение для контроля версий и частое

Т. 8. №11. 2022
https://doi.org/10.33619/2414-2948/84

резервное копирование, могут помочь восстановить данные в исходном состоянии, если это необходимо. Целостность также охватывает концепцию безотказности: необходимо доказать, что исходная целостность данных сохранена, особенно в юридических контекстах.

Доступность — это зеркальное отражение конфиденциальности: хотя необходимо убедиться, что к данным не могут получить доступ неавторизованные пользователи, а также необходимо обеспечить, чтобы к ним могли получить доступ те, у кого есть соответствующие разрешения. Обеспечение доступности данных означает соответствие сетевых и вычислительных ресурсов ожидаемому объему доступа к данным и реализацию политики резервного копирования для целей аварийного восстановления.

Довольно важным пунктом является конфиденциальность. По своему содержанию информация с ограниченным доступом объединяет всю совокупность сведений, составляющих как тайную, так и конфиденциальную информацию, нуждается в защите на законодательном уровне и подлежит охране государством [3]. Согласно действующему законодательству к информации с ограниченным доступом также относится информация, которая не подлежит обнародованию и распространению в средствах массовой информации. Защита конфиденциальной информации сегодня является одним из важнейших факторов создания и обеспечения предпосылок, необходимых для стабильности и дальнейшего развития информационного общества. Она направлена на обеспечение интересов субъектов информационных отношений.

Для обеспечения конфиденциальности в ядре Linux используется утилита iptables. Iptables — это утилита командной строки для настройки брандмауэра ядра Linux, реализованная в рамках проекта Netfilter. Термин iptables также обычно используется для обозначения этого брандмауэра на уровне ядра. Его можно настроить непосредственно с помощью iptables или с помощью одного из множества консольных и графических интерфейсов. Iptables используется для IPv4 , а ip6tables используется для IPv6 . И iptables, и ip6tables имеют одинаковый синтаксис, но некоторые параметры относятся либо к IPv4, либо к IPv6.

Iptables используется для проверки, изменения, пересылки, перенаправления и/или удаления IP–пакетов. Код для фильтрации IP–пакетов уже встроен в ядро и организован в виде набора таблиц, каждая из которых предназначена для определенной цели. Таблицы состоят из набора предопределенных цепочек, а цепочки содержат правила, которые проходятся по порядку. Каждое правило состоит из предиката возможных совпадений и соответствующего действия (называемого целевым), которое выполняется, если предикат истинен; то есть условия совпадают. Если IP–пакет достигает конца встроенной цепочки, включая пустую цепочку, то политика цепочки target определяет конечный пункт назначения IP–пакета. Iptables — это пользовательская утилита, позволяющая работать с этими цепочками/правилами. Большинство новых пользователей находят реализацию IP–маршрутизации в Linux довольно сложной, но на практике наиболее распространенные варианты использования (NAT и/или базовый брандмауэр Интернета) значительно проще.

В фильтре iptables все пакеты делятся на три аналогичные цепочки:

Input — обрабатывает входящие пакеты и подключения. Например, если какой–либо внешний пользователь пытается подключиться к вашему компьютеру по ssh или любой веб–сайт отправит свой контент по запросу браузера, тогда все эти пакеты попадут в эту цепочку;

forward — эта цепочка применяется для проходящих пакетов. Сюда попадают пакеты, которые отправлены на ваш компьютер, но не предназначены ему, они просто пересылаются по сети к своей цели. Такая ситуация наблюдается на маршрутизаторах или, например, если ваш компьютер раздает WiFi;

Т. 8. №11. 2022
https://doi.org/10.33619/2414-2948/84

output — эта цепочка используется для исходящих пакетов и соединений. Сюда попадают пакеты, которые были созданы при попытке выполнить ping losst.ru, или когда вы запускаете браузер и пытаетесь открыть любой сайт.

В компьютерных сетях пакет — это определенным образом оформленный блок данных, передаваемый по сети в пакетном режиме. Ключом к пониманию того, как работает iptables, является эта диаграмма, представленная на Рисунке.

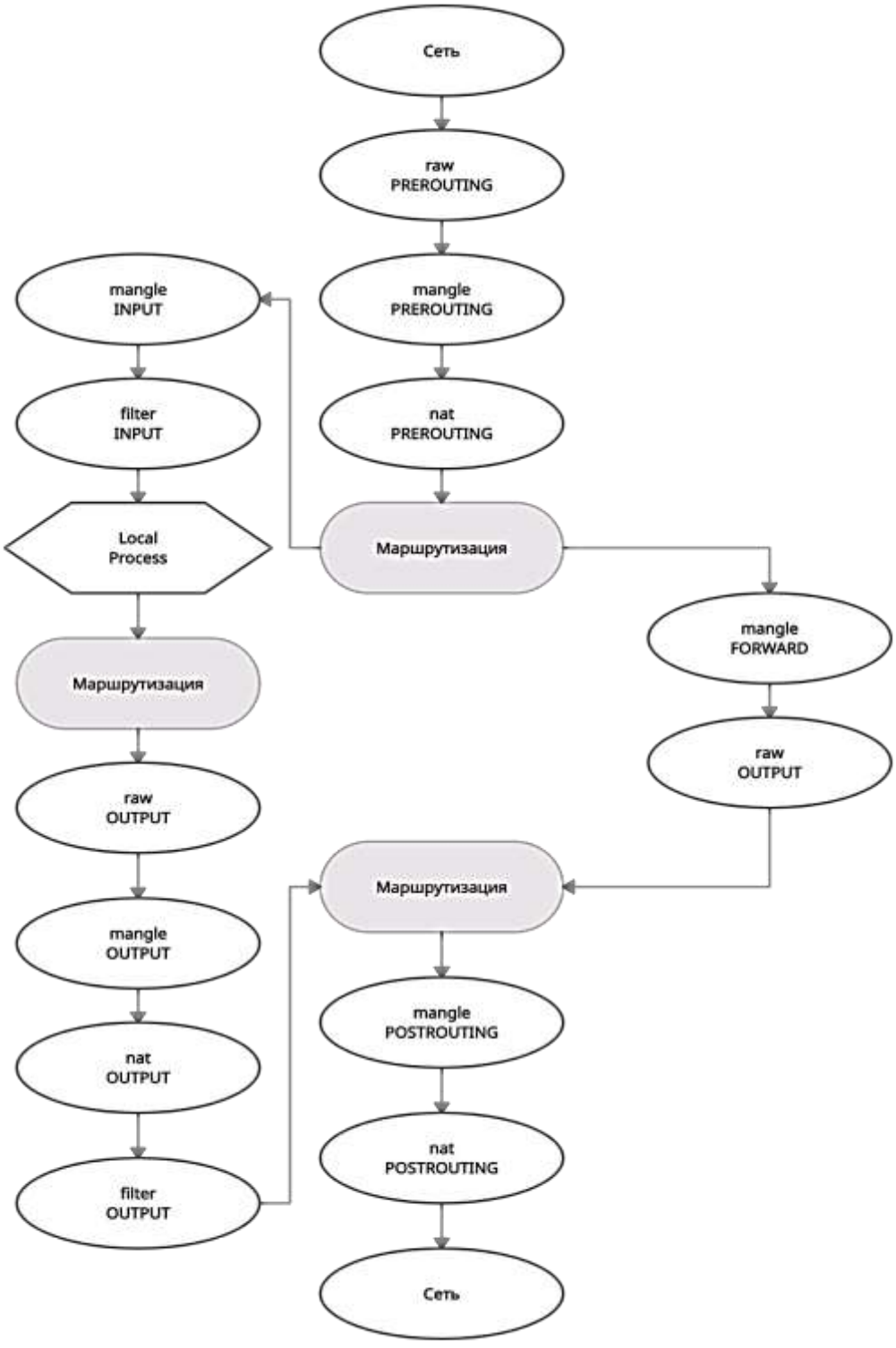

Рисунок. Принципы работы iptables

Т. 8. №11. 2022
https://doi.org/10.33619/2414-2948/84

Слово, записанное буквами в нижнем регистре, расположенное сверху в блоке диаграммы — это таблица, а слово, записанное в верхнем регистре в нижней части блока — цепочка. Каждый IP–пакет, поступающий на любой сетевой интерфейс, проходит через эту блок–схему сверху вниз. Распространенным заблуждением является то, что пакеты, поступающие из внутреннего интерфейса, обрабатываются иначе, чем пакеты из интерфейса, обращенного к Интернету. Все интерфейсы обрабатываются одинаково. Каждый сетевой администратор решает и определяет правила, которые относятся к ним по–разному. Некоторые пакеты предназначены для локальных процессов, поэтому поступают из верхней части диаграммы и останавливаются на <Local Process>, в то время как другие пакеты генерируются локальными процессами; следовательно, нужно с <Local Process> продвигаться вниз по блок–схеме (Таблица).

Таблица

СОДЕРЖАНИЕ IPTABLES

Таблица	*Описание*
nat	Таблица nat используется в основном для трансляции сетевых адресов. Пакеты, прошедшие NAT, изменяют свои IP–адреса в соответствии с нашими правилами. Пакеты в потоке проходят через эту таблицу только один раз. Предполагается, что разрешен первый пакет потока. Остальные пакеты в том же потоке автоматически подвергаются «NAT» или маскарадингу, и к ним будут применяться те же действия, что и к первому пакету. Другими словами, они не будут повторно проходить через эту таблицу, но, тем не менее, будут рассматриваться как первый пакет в потоке. Это основная причина, по которой не следует выполнять какую–либо фильтрацию. Цепочка PREROUTING используется для изменения пакетов, как только они попадают на брандмауэр. Цепочка OUTPUT используется для изменения локально сгенерированных пакетов (т.е. на брандмауэре), прежде чем примется решение о маршрутизации. Наконец, у нас есть цепочка POSTROUTING, которая используется для изменения пакетов, когда они собираются покинуть брандмауэр.
mangle	Эта таблица используется в основном для искажения пакетов. Помимо прочего, можно изменять содержимое разных пакетов и их заголовков. Примерами этого может быть изменение TTL, TOS и т.д. MARK не является изменением пакета, а значение метки для пакета устанавливается в пространстве ядра. Другие правила или программы могут использовать эту отметку дальше в брандмауэре для фильтрации или расширенной маршрутизации. Таблица состоит из пяти встроенных цепочек: PREROUTING, POSTROUTING, OUTPUT, INPUT и FORWARD[4]. PREROUTING используется для изменения пакетов, как только они попадают в брандмауэр и до того, как примется решение о маршрутизации. POSTROUTING используется для изменения пакетов сразу после принятия всех решений о маршрутизации. OUTPUT используется для изменения локально сгенерированных пакетов после того, как примется решение о маршрутизации. INPUT используется для изменения пакетов после того, как они были перенаправлены на сам локальный компьютер, но до того, как приложение пользовательского пространства фактически “увидит” данные. FORWARD используется для искажения пакетов после того, как было принято первое решение о маршрутизации, но до того, как будет принято последнее. Стоит заметить, что mangle нельзя использовать для любого вида преобразования сетевых адресов или маскарадинга, а таблица nat была создана для таких операций.
filter	Таблицу фильтров следует использовать исключительно для фильтрации пакетов. Например, можно эффективно использовать DROP, LOG, ACCEPT или REJECT пакеты, как и в других таблицах. В эту таблицу встроены три цепочки[2]. Первая называется FORWARD и используется для всех не локально сгенерированных пакетов, которые не предназначены для нашего локального хоста. INPUT используется для всех пакетов,

Таблица	*Описание*
	предназначенных для нашего локального хоста, а OUTPUT используется для всех локально сгенерированных пакетов.
raw	Таблица raw и ее цепочки используются перед любыми другими таблицами в netfilter. Было введено использование цепи NOTRACK[1]. Эта таблица довольно новая и доступна только в случае компиляции с ядрами поздней версии 2.6 и выше. Таблица raw содержит две цепочки. Цепочка PREROUTING и OUTPUT, где они будут обрабатывать пакеты до того, как они попадут в любую из других подсистем сетевого фильтра. Цепочка PREROUTING может использоваться для всех входящих пакетов на эту машину или пересылаемых, в то время как цепочка OUTPUT может использоваться для изменения локально сгенерированных пакетов до того, как они попадут в любую из других подсистем сетевого фильтра.

Опыт администрирования информационных сетей на базе RedOS в ФГБОУ ВО «ПГУТИ» показал, что для обеспечения безопасности функционирования компьютерных классов и всей инфраструктуры в целом, достаточно только двух таблиц: filter и nat. Другие таблицы предназначены для сложных конфигураций, включающих несколько маршрутизаторов и решений по маршрутизации.

Обеспечение информационной безопасности стало важнейшей задачей в жизни современного общества. Для обеспечения безопасности сети Linux, была разработана утилита iptables. Она позволяет обрабатывать входящие подключения, просматривать, изменять, удалять, принимать, отклонять, перенаправлять пакеты, а также записывать их данные в логи. Благодаря данной утилите выполняется защита системы от внешних вторжений, перенаправление портов и множество других действий, выполняемых с трафиком. Однако, ее недостаток состоит в том, что она сложна в настройке.

Источники:

1. IPTABLES. https://ipset.netfilter.org/iptables.man.html
2. Настройка netfilter с помощью iptables. https://clck.ru/32dahU
3. Конфиденциальная информация. https://dostup.media/confidentiality
4. Linux: IPTABLES – руководство: ч. 1. основы IPTABLES. https://goo.su/205MyZ7
5. Information Security: The Ultimate Guide. https://goo.su/6NfM5G

Работа поступила
в редакцию 01.10.2022 г.

Принята к публикации
12.10.2022 г.

Ссылка для цитирования:

Лиманова Н. И., Третьяков Е. Ю. IPTABLES для обеспечения безопасности информационных сетей на базе LINUX // Бюллетень науки и практики. 2022. Т. 8. №11. С. 366-371. https://doi.org/10.33619/2414-2948/84/44

Cite as (APA):

Limanova, N., & Tretyakov, E. (2022). IPTABLES for Security of LINUX-based Information Networks. *Bulletin of Science and Practice, 8*(11), 366-371. (in Russian). https://doi.org/10.33619/2414-2948/84/44