IPTABLES

iptables - управление пакетными фильтрами IP

Синтаксис

iptables -[ADC] спецификация правил цепочки [опции]

iptables -[RI] цепочка номер правила спецификация правила [опции]

iptables -D цепочка номер правила [опции]

iptables -[LFZ] [цепочка] [опции]

iptables -[NX] цепочка

iptables -P цепочка действие [опции]

iptables -E имя старой цепочки имя новой цепочки

Описание

Программа Iptables используется для создания, обслуживания и проверки таблиц с правилами фильтрации пакетов IP в ядре Linux. Можно определить несколько таблиц, каждая из которых будет содержать множество встроенных цепочек и может также включать цепочки, определенные пользователем.

Каждая цепочка представляет собой список правил, которому может соответствовать множество пакетов. Каждое правило указывает действие (target), которое совершается по отношению к пакетам, удовлетворяющим заданным критериям. Действие может быть одной из предопределенных операций или задавать переход к пользовательской цепочке.

Действия

Правила брандмауэра содержат критерии проверки пакетов и указывают выполняемое по отношению к пакету действие. Если пакет не соответствует заданным критериям, происходит переход к следующему правилу в цепочке. При соответствии пакета заданным критериям выполняется заданное для правила действие (предопределенная операция или переход к пользовательской цепочке). Список предопределенных операций включает ACCEPT (принять), DROP (отбросить), QUEUE (поместить в очередь) или RETURN (возвратить управление вызвавшей цепочке).

Операция ACCEPT обеспечивает пропускание (восприятие) пакета, DROP ведет к отказу от дальнейшей обработки пакета (отбрасыванию), QUEUE передает пакет в пользовательскую область, RETURN обеспечивает возврат к следующему правилу предыдущей (вызвавшей данную) цепочки. При достижении конца встроенной цепочки или выполнении правила с операцией RETURN по отношению к пакету выполняется операция, заданная политикой цепочки.

Таблицы

Существуют три предопределенных таблицы (реальное присутствие таблиц определяется опциями компиляции ядра).

-t, --table

Эта опция задает таблицу, которая используется по отношению к пакету при выполнении заданных критериев. Если при компиляции ядра была включена опция автоматической загрузки модулей, будет предпринята попытка загрузить соответствующий таблице модуль (если модуль не был загружен ранее).

Подерживаются следующие таблицы:

filter - принятая по умолчанию таблица, которая содержит встроенные цепочки INPUT (принимаемые пакеты), FORWARD (пересылаемые маршрутизатором пакеты) и OUTPUT (локально сгенерированные пакеты).

nat -эта таблица используется в тех случаях, когда встречается пакет организации нового соединения. Таблица содержит три встроенных цепочки - PREROUTING (изменение пакетов, как будто они являются входящими), OUTPUT (изменение локально сгенерированных пакетов до их маршрутизации) и POSTROUTING (изменение пакетов, как будто они являются исходящими).

mangle - эта таблица служит для специализированного преобразования пакетов. Таблица имеет две встроенных цепочки - PREROUTING (изменение входящих пакетов до их маршрутизации) и OUTPUT (изменение локально сгенерированных пакетов до маршрутизации).

Опции

Опции, распознаваемые iptables можно разделить на несколько групп.

Команды

Эти опции служат для задания выполняемых действий - в каждой строке может быть указана только одна команда, если в данном документе явно не сказано иное. Для всех длинных (полных) вариантов написания команд и опций можно вводить только часть имени, обеспечивающую уникальную идентификацию команды или опции.

-A, --append

Добавляет одно или несколько правил в конец указанной цепочки. Если имя (адрес) отправителя или получателя, заданное командой, может быть преобразовано в несколько адресов, правила создаются для всех возможных комбинаций адресов.

-D, --delete

Удаляет одно или несколько правил из указанной цепочки. Существуют два варианта задания удаляемых правил - по номеру (нумерация начинается с 1) и по соответствию (в команде полностью указывается удаляемое правило).

-R, --replace

Заменяет правило в указанной цепочке. Если имя отправителя или получателя, заданное командой, может быть преобразовано в несколько адресов, выдается сообщение об ошибке. Заменяемое правило задается по его номеру (нумерация с 1).

-I, --insert

Вставляет одно или несколько правил в указанную цепочку, начиная с заданного номера. Если номер не указан, правила всталяются в начало цепочки.

-L, --list

Выводит список всех правил указанной цепочки. Если цепочка не указана, выводятся списки правил для всех цепочек. С этой командой можно использовать опцию -Z (zero - 0) - это приведет к автоматическому сбросу всех счетчиков в результате вывода списка правил. Представление списка зависит также от других аргументов.

-F, --flush

Очищает указанную цепочку, удаляя из нее все правила.

-Z, --zero

Сбрасывает в 0 значения счетчиков для всех цепочек. Эту опция можно использовать совместно с командой -L (--list - список) для просмотра значний счетчиков перед их сбросом.

-N, --new-chain

Создает новую пользовательскую цепочку с заданным именем. Имя содаваемой цепочки не должно использоваться для других цепочек.

-X, --delete-chain

Удаляет указанную пользовательскую цепочку. На удаляемую цепочку не должно быть ссылок в других цепочках (такие цепочки нужно удалить заранее). Если команда не содержит аргументов, будет предпринята попытка удаления всех пользовательских цепочек.

-P,--policy

Задает политику для цепочки (действие, выполняемое после проверки всех правил в цепочке). Политика может указываться только для встроенных цепочек.

-E, --rename-chain

Переименовывает указанную пользоватеьскую цепочку, не оказывая влияния на структуру таблицы.

-h (Help)

Выдает краткую справку о синтаксисе команд.

Параметры

Описанные ниже параметры используются для задания правил фильтрации пакетов.

-p, --protocol [!] протокол

Протокол, для которого задается правило. Опция protocol может принимать значения tcp, udp, icmp, all (все протоколы) или содержать числовое обозначение протокола (см. файл /etc/protocols). Опция ! означает инверсию (все протоколы, кроме указанного). Если протокол не указан, правило применяется для всех протоколов (эквивалентно опции all). Значение all нельзя использовать с командой check.

-s, --source [!] адрес[/маска]

Задает отправителя. Поле address может содержать адрес IP, имя хоста или имя сети. Поле mask может содержать маску подсети в явном виде или указывать число битов в сетевой части адреса (например, значение 24 эквивалентно маске 255.255.255.0). Опция "!" задает инверсию (все адреса, кроме указанных). Флаг --src является удобным сокрашением при задании адреса отправителя.

-d, --destination [!] адрес[/маска]

Задает получателя пакета. Значение остальных полей такое же, как для флага -s (source) . Для сокращенной записи удобно использовать флаг --dst.

-j, --jump действие

Указывает действие, выполняемое при совпадении пакета с заданными правилом условиями, В качестве действия можно указывать пользовательскую цепочку или одну из предопределенных операций (см. EXTENSIONS). Если в правиле не указано действие, программа просто переходит к проверке следующего правила, увеличивая значения связанных с данным правилом счетчиков.

-i, --in-interface [!] [имя]

Необязательное имя интерфейса, через который принимаются пакеты (для цепочек INPUT, FORWARD и PREROUTING). Флаг "!" перед именем интерфейса инвертирует значение (все интерфейсы, кроме указанного). Если имя интерфейса заканчивается знаком "+", правило применяется ко всем интерфейсам, содержащим в своем имени указанный текст (например, eth+ задает все интерфейсы Ethernet).

-o, --out-interface [!] [name]

Необязательное имя интерфейса, через который должны передаваться пакеты (для цепочек FORWARD, OUTPUT и POSTROUTING). С этим параметром могут использоваться описанные выше опции "!" и "+".

[!] -f, --fragment

Этот флаг означает, что правило применимо только к пакетам, являющимся фрагментами (начиная со второго) большого пакета. Поскольку для таких пакетов невозможно определить порт отправителя/получателя (тип ICMP), пакеты не будут соответствовать ни одному из правил, задающих номера портов или тип ICMP. Флаг "!" инвертирует значение аргумента -f (для всех пакетов, кроме фрагментов).

Другие опции

Поддерживаются также дополнительные опции, описанные ниже:

-v, --verbose

Подробный вывод. Эта опция обеспечивает по команде list вывод сведений об адресах интерфейсов, опциях правил и масках TOS. Показываются также значения счетчиков пакетов и байтов с использованием суффиксов K (1000), M (1000000) или G (1000000000) (см. также описание флага -x). При операциях добавления, вставки, замены и удаления эта опция обеспечивает вывод сведений об изменяемых правилах.

-n, --numeric

Для обозначения IP-адресов и портов используются номера взамен имен. По умолчанию программа пытается выводить имена хостов, сетей и служб.

-x, --exact

Выводятся точные значения показаний счетчиков пакетов и байтов взамен сокращенных обозначений с использованием суффиксов K (1000), M (1000K) или G (1000M). Эту опцию можно использовать только с командой -L.

--line-numbers

При просмотре списка правил выводятся их номера в соответствии с положением правил в цепочках.

Расширения правил соответствия

Программа iptables может использовать модули расширенного соответствия пакетов. Перечисленные здесь опции включены в базовый вариант программы; для большинства из этих опций можно использовать флаг инверсии “!”.

tcp

Это расширение загружается при использовании `--protocol tcp' и отсутствии других критериев соответствия. Данное расширение обеспечивает следующие опции:

--source-port [!] [порт[:порт]]

Спецификация порта (или диапазона портов) отправителя. Для указания портов могут использоваться их номера или имена служб. Можно указывать диапазон портов, включающий крайние значения - port:port. Если не указан номер стартового порта, он предполагаеься равным 0; при отсутствии верхней границы принимается значение 65535. Если номер стартового порта превышает номер конечного порта, эти номера меняются местами. В качестве синонима для этой опции можно использовать --sport .

--destination-port [!] [порт[:порт]]

Спецификация порта (или диапазона портов) получателя. В качестве сокращения можно использовать --dport.

--tcp-flags [!] mask comp

Выполняется при наличии указанных флагов TCP . Первый аргумент задает флаги, которые следует проверять, а второй - флаги, которые должны быть установлены. В качестве флагов могут указываться SYN, ACK, FIN, RST, URG, PSH, ALL, NONE. Флаги перечисляются через запятую. Команда iptables -A FORWARD -p tcp --tcp-flags SYN, ACK, FIN, RST SYN отыскивает пакеты с установленным флагом SYN, но без флагов ACK, FIN и RST .

[!] --syn

Этому правилу могут соответствовать только пакеты TCP с установленным битом SYN и битами ACK и FIN, имеющими нулевые значения. Такие пакеты служат для инициирования соединений TCP (например, блокирование таких пакетов на входном интерфейсе не позволит организовать соединения с вашей сетью, но не будет мешать организации соединений по инициативе станций вашей сети). Эта опция эквивалентна --tcp-flags SYN, RST, ACK SYN. Установка флага "!" инвертирует значение правила (все пакеты кроме SYN).

--tcp-option [!] номер

Выполняется при установленной опции TCP .

udp

Это расширение загружается при использовании опции --protocol udp, если не задано иных спецификаций. Расширение поддерживает следующие опции:

--source-port [!] [порт[:порт]]

Порт (или диапазон портов) отправителя (см. описание опции --source-port в параграфе ***TCP***).

--destination-prt [!] [порт[:порт]]

Порт (или диапазон портов) адресата (см. описание опции --desination-port в параграфе ***TCP***).

icmp

Это расширение загружается при использовании опции --protocol icmp, если не задано иных спецификаций. Расширение поддерживает следующие опции:

--icmp-type [!] название типа

Эта опция позволяет задать тип ICMP, который можно указать с помощью номера или имени. Для просмотра списка имен можно использовать команду **iptables -p icmp -h.**

mac

--mac-source [!] адрес

Проверяется соответствие MAC-адресов. Адрес задается в формате XX:XX:XX:XX:XX:XX. Отметим, что эта опция имеет смысл только для пакетов, поступающих в цепочки PREROUTING, FORWARD или INPUT от интерфейсов

Ethernet.

limit

Этот модуль ограничивает скорость соответствия с использованием фильтра token bucket. Модуль может использоваться в комбинации с действием LOG для ограничения частоты записей в протокол. Правило для этого расширения будет выполняться до тех пор, пока не будет превышен заданный предел (если не используется флаг “!”, который обращает правило).

--limit rate

Максимальное значение средней скорости соответствия (average matching rate), задаваемое числом с необязательным суффиксом /second (в секунду), /minute (в минуту), /hour (в час), /day (за сутки). По умолчанию используется значение 3/hour.

--limit-burst number

Максимальное изначальное число пакетов для соответствия – это значение вызывается повторно каждый раз, когда не достигается описанный выше предел. По умолчанию устанавливается изначальное значение 5.

multiport

Этот модуль проверяет соответствие заданному набору портов отправителя или получателя (можно указать до 15 портов). Модуль используется только совместно с опциями ***-p tcp*** или ***-p udp***.

--source-port [порт[,порт]]

Правило выполняется для указанных параметром портов.

--destination-port [порт[,порт]]

Правило выполняется для указанных параметром портов.

--port [порт[,порт#]]

Правило выполняется, если номера портов отправителя и получателя совпадают и входят в число указанных правилом портов.

mark

Этот модуль служит для проверки соответствия поля netfilter mark, связанного с пакетом (поле можно установить с помощью действия **MARK**, описанного ниже).

--mark значение[/маска]

Правилу соответствуют пакеты с указанным (беззнаковым) значением маркера (если задана маска, используется логическая операция AND по отношению к маркеру перед сравнением).

owner

Этот модуль пытается проверить соответствие различных характеристик создателя пакета для сгенерированных локально пакетов. Правило применимо только для цепочки OUTPUT, но даже в этом случае некоторые пакеты (например отклики ICMP) могут не иметь владельца и правило никогда не будет выполняться для них.

--uid-owner идентификатор пользователя

Правило выполняется для пакетов, созданных процессом, которым владеет указанный пользователь.

--gid-owner идентификатор группы

Правило выполняется для пакетов, созданных процессом, которым владеет указанная группа.

--pid-owner идентификатор процесса

Правило выполняется для пакетов, созданных указанным процессом.

--sid-owner идентификатор сеанса

Правило выполняется для пакетов, созданных процессом в указанном сеансе.

state

Этот модуль в комбинации со средствами контроля соединений позволяет проверить состояние соединения для данного пакета.

--state состояние

Состояние – список разделенных запятыми состояний, соответствие которым проверяется правилом. Возможны состояния INVALID (пакет не связан с известным соединением), ESTABLISHED (пакет связан с соединением, по которому пакеты передаются в обе стороны), NEW (пакет является началом нового соединения или связан с соединением, по которому пакеты передаются только в одном направлении) и RELATED (пакет является началом нового соединения, но связан с существующим соединением – например, передача данных FTP или ошибка ICMP).

unclean

Этот модуль не поддерживает опций, но пытается проверить пакеты на необычность или некорреткность. Данный модуль является экспериментальным.

tos

Этот модуль проверяет соответствие 8 битов типа обслуживания (Type of Service) в заголовке IP (включая биты старшинства - precedence).

--tos tos

Этот аргумент может содержать стандартное имя (используйте **iptables -m tos -h** для просмотра) или числовое значение.

Действия

Программа iptables может использовать модули расширения для действий, описанные ниже.

LOG

Включает протоколирование фактов соответствия пакетов правилу. При установке этой опции для правила ядро Linux будет протоколировать информацию о пакетах, соответствующих правилу с использованием printk().

--log-level уровень

Задает уровень протоколирования (см. руководство syslog.conf(5)).

--log-prefix префикс

Записывает указанный префикс (до 14 символов) в каждой строке протокола. Использование префиксов упрощает работу с файлами протокола.

--log-tcp-sequence

Протоколирование порядковых номеров TCP. При наличии доступа сторонних пользователей к файлу протокола использование этой опции может помочь злоумышленникам при взломе вашей системы.

--logtcp-options

Протоколируются опции из заголовка пакета TCP.

--log-ip-options

Протоколируются опции из заголовка пакета IP.

MARK

Это действие служит для установки значения маркера фильтрации (netfilter mark), связанного с пакетом. Особенно эффективно использовать маркеры с таблицей mangle. .

--set-mark маркер

REJECT

Это действие ведет к отбрасыванию пакета с передачей отправителю уведомления о недоступности адресата.

Данное действие применимо только для цепочек *INPUT*, *FORWARD* и *OUTPUT*, а также пользовательских цепочек,

которые вызываются только из трех перечисленных встроенных цепочек. Для контроля за передаваемыми отправителю сообщениями используются перечисленные ниже опции:

--reject-with тип

Задает тип передаваемого отклика (icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unreachable, icmp-net-prohibited, icmp-host-prohibited), возвращаемый вместе с сообщением об ошибке ICMP (по умолчанию используется тип port-unreachable – порт недоступен). Можно использовать также опцию echo-reply (только для правил, которые применяются к пакетам ICMP ping и обеспечивают генерацию откликов ping). Кроме того, можно задавать тип tcp-reset для правил входной цепочки (или вызываемых лишь из нее правил), которым могут соответствовать только пакеты TCP – использование этой опции будет приводить к передаче отправителю пакета TCP RST.

TOS

Это действие служит для установки 8-битового поля типа обслуживания (Type of Service) в заголовке IP. Данное действие можно использовать только в таблице *mangle*.

--set-tos тип обслуживания

Вы можете использовать числовые значения или имена опций TOS (для просмотра списка имен используйте команду **iptables -j TOS -h**).

MIRROR

Это действие пока находится в экспериментальной стадии и обеспечивает обращение адресов отправителя и получателя пакета в заголовке IP с последующей повторной передачей пакета. Это действие можно использовать только в цепочках *INPUT, FORWARD* или *OUTPUT* и пользовательских цепочках, вызываемых лишь из перечисленных цепочек.

SNAT

Это действие можно использовать только в таблице трансляции адресов (цепочка *POSTROUTING*). Данное действие обеспечивает изменение адреса отправителя данного пакета (и всех последующих пакетов в этом соединении), а проверка правил приостанавливается. Действие может использоваться с опцией:

--to-source <ip-адрес>[-<ip-адрес>][:порт-порт]

которая может указывать один новый IP-адрес отправителя или диапазон IP-адресов и портов (необязательно и может использоваться только совместно с -p tcp или -p udp). Если диапазон портов не задан, порты отправителя с номерами ниже 512 будут отображаться в другие порты с номерами меньше 512, порты с номерами до 1024 также будут отображаться в порты с номерами меньше 1024, а остальные порты будут отображаться в порты с номерами 1024 и выше. По возможности при отображении портов их номера сохраняются.

DNAT

Это действие можно использовать только в таблице трансляции адресов (цепочка *PREROUTNG* или *OUTPUT* и пользовательские цепочки, которые могут вызываться только из перечисленных цепочек). Действие обеспечивает изменение адреса получателя данного пакета (и всех последующих пакетов в данном соединении). Правило может использовать опцию:

--to-destination <ip-адрес>[-<ip-адрес>][:порт-порт]

которая может указывать один новый IP-адрес получателя или диапазон IP-адресов и портов (необязательно и может использоваться только совместно с -p tcp или -p udp). Если диапазон портов не указан, номера портов не изменяются.

MASQUERADE

Это действие можно использовать только в таблице трансляции адресов (цепочка *POSTROUTING*). Действие можно использовать только для динамических адресов (выделяемых при коммутируемых соединениях). Для статических адресов следует использовать действие SNAT. Маскирование адресов эквивалентно заданию отображения адресов IP при передаче пакетов интерфейсом. При отключении интерфейса (down) информация об отображении сохраняется. Это действие может использовать опцию:

--to-ports <порт>[-<порт>]

Задает диапазон портов отправителя для использования. Эта опция имеет более высокий приоритет по сравнению с указанием портов в действии SNAT. Порты можно задавать только при использовании опции -p tcp или -p udp.

REDIRECT

Это действие можно использовать только в таблице трансляции адресов (цепочка *PREROUTNG* или *OUTPUT* и пользовательские цепочки, которые могут вызываться только из перечисленных цепочек). Действие обеспечивает изменение IP-адреса получателя пакета (локально генерируемые пакеты отображаются на адрес 127.0.0.1). Действие может использовать опцию:

--to-ports <порт>[-<порт>]

которая задает диапазон используемых портов получателя. Если порты не заданы, сохраняется исходный номер порта. Задание портов поддерживается только при использовании опции -p tcp или -p udp.

Диагностика

При использовании программы на стандартный вывод могут передаваться различные сообщения об ошибках. Сообщения с кодом 2 говорят о некорректном использовании параметров, при остальных ошибках используется код 1.

Ошибки

Пока неизвестны.

Совместимость с IPCHAINS

Программа iptables очень похожа на ipchains Расти Рассела (Rusty Russell). Основная разница заключается в том, что цепочки *INPUT* и *OUTPUT* используются только для пакетов принимаемых и передаваемых (соответственно) локальным хостом. Следовательно, каждый пакет проходит только через одну из предопределенных цепочек. В ipchains транзитные пакеты пропускались через три цепочки.

Вторым важным отличием является то, что -i указывает входной интерфейс, -o - выходной и оба эти флага можно использовать для пакетов, передаваемых в цепочку *FORWARD*.

Iptables представляет собой чистый фильтр пакетов, использующий по умолчанию таблицу фильтрации с необязательными модулями расширения. Такое решение позволяет избавиться от путаницы при совместном использовании фильтров и маскарадинга IP. Перечисленные ниже опции обрабатываются по другому:

-j MASQ

-M -S

-M -L

Есть и другие отличия между программами.

Дополнительная информация

Детальную информацию можно найти в документах iptables-HOWTO и netfilter-hacking-HOWTO.

Авторы

Rusty Russell написал iptables, используя на ранних этапах консультации Michael Neuling.

Marc Boucher убедил отказаться от ipnatctl и написал модули трансляции адресов.

James Morris написал политику TOS и проверку флагов качества обслуживания. Jozsef Kadlecsik написал политику REJECT. Ядро команды Netfilter составляют Marc Boucher и Rusty Russell.

Перевод на русский язык

Николай Малых (nmalykh@bilim.com)