Санкт-Петербург, ул. Седова, 80, телефон (812) 449-0770, факс (812) 449-0771, E-mail: info@bilim.com

iptables 1.3.0

Краткий обзор изменений

Николай Малых

nmalykh@bilim.com

12 февраля 2005 года была анонсирована новая версия популярной системы фильтрации пакетов и управления трафиком iptables. Вы можете загрузить исходные кода программы с сайта www.netfilter.org. Новая версия программы работает с ядрами версии 2.4.4 и выше (рекомендуется 2.4.18), однако ряд новых функций будет поддерживаться только ядром 2.6.10 и выше или после установки "заплаток" на ядра предыдущих версий. Полный список изменений вы найдете на сайте http://www.netfilter.org/files/changes-iptables-1.3.0.txt.

В новой версии исправлены ошибки, обнаруженные с момента выпуска iptables 1.2.11 и 1.3.0rc1, добавлены новые функции, а также полностью переработана библиотека libiptc, что позволило существенно повысить скорость загрузки таблиц правил. Рассмотрим некоторые изменения более подробно.

libiptc

Harald Welte и Martin Josefsson полностью переписали код libiptc, что привело к ускорению загрузки таблиц в десятки раз. Особенно заметен эффект при загрузке больших таблиц. Например, загрузка файла, содержащего более 15000 строк в версии 1.2.11 занимала 3 - 5 минут, а сейчас увеличившийся дополнительно набор правил загружается за 2 – 3 секунды. Однако такое ускорение не прошло даром и реализованный в новой версии механизм загрузки правил (мы не будем подробно рассматривать его – желающие смогут разобраться по исходным кодам) имеет по крайней мере один побочный эффект. Эффект этот проявляется в том, что некоторые правила после их редактирования и перезагрузки таблицы реально не изменяются, хотя при просмотре с помощью команд iptables -L и itables-save вы увидите в списке измененное правило. У меня пока не было времени разобраться с этим эффектом, хотя его причины достаточно понятны и в данный момент могу лишь сказать, что побочные эффекты возникают при изменении параметров соответствий dstlimit, hashlimit и, возможно, limit. Аналогичный эффект возникает и при использовании соответствия tbf, которое пока еще не включено в официально распространяемый пакет.
Каких-то серьезных проблем этот побочный эффект не вызывает, поскольку вместо команды **/etc/init.d/iptables restart** можно воспользоваться парой команд **/etc/init.d/iptables stop** и **/etc/init.d/iptables start**. Возникающая пауза, когда у вас не будут работать фильтры, достаточно мала (как я уже писал, загрузка таблицы из 15 тысяч правил занимает 2 – 3 секунды) и не может привести с существенному росту риска компрометации системы во время перезапуска правил.

Переменные окружения IPTABLES_LIB_DIR и IP6TABLES_LIB_DIR

Rusty Russell добавил поддержку переменных окружения IPTABLES_LIB_DIR и IP6TABLES_LIB_DIR, которые позволяют использовать несколько вариантов библиотек iptables в одной системе.

Поддержка muilti-call

Bastiaan Bakker добавил опцию компиляции DO_MULTI=1 для поддержки muilti-call.

Поддержка номера версии расширения

Rusty Russel добавил для расширений поддержку номера версии (revision number) для использования которой в ядре должна быть включена поддержка getsockopts.

Процедура инициализации

Повторная инициализация libiptc/libip6t не выполняется пока не будет успешно завершена попытка загрузки модуля ядра с помощью modprobe (Rusty Russell).

Описание таблицы raw

Harald Welte добавил описание (man) для таблицы raw, которая до этого фактически была недокументированной.

Режим ROUTE –tee

Patrick Schaaf добавил в операции ROUTE режим –tee, который позволяет создавать копию пакета, соответствующего условиям и передавать его по заданному маршруту.

`--tee`

Задает копирование пакета и маршрут куда следует передавать копию. Для исходного пакета продолжается обработка в последующих правилах цепочек. Этот режим не может использоваться вместе с опциями –iif или –continue.

Сооответствие physdev для Ipv6

Bart De Schuymer добавил возможность проверки физического устройства для пакетов IPv6.

Опция –log-uid для операции LOG

John Lange реализовал для операции LOG опцию –log-uid, позволяющую записывать в журнальный файл идентификатор пользователя, от имени которого запущена сгенерировавшая пакет программа.

Порязрядные действия для операции MARK

Henrik Nordstrom и Rusty Russell реализовали поддержку поразрядных действий для операции MARK.

Поддержка ipset2 для операции SET

Jozsef Kadlecsik обновил операцию SET для поддержки ipset2.

Система учета трафика

Piotr Gasid'o обновил соответствие account до версии 0.1.16

Новое соответствие comment

Brad Fisher написал модуль comment, позволяющий добавлять комментарии в правила iptables. Модуль поддерживает единственный параметр

```
--comment <Текст комментария>
```

Например, для добавления комментария “Приватный блок адресов” для всех пакетов, принятых из сети 192.168.0.0/24 можно использовать правило

```
-A INPUT -s 192.168.0.0/16 -m comment --comment "Приватный блок адресов"
```

Для использования этого модуля в ядре должна быть включена опция **comment match support**.

Новое соответствие hashlimit

Harald Welte написал модуль hashlimit, позволяющий вводить ограничения, связанные с адресом или парой “адрес-порт” для получателей/отправителей пакетов. С помощью данного условия можно задавать ограничения типа

- не более 1000 пакетов в секунду для каждого хоста в сети 192.168.0.0/16
- не более 100 в секунду для каждого сервиса на хосте 192.168.1.1

одной строкой iptables.

Основная идея заключается в создании хэш-таблицы для каждого адреса получателя и поддержка отдельных счетчиков пакетов и байтов для каждой записи. Таким способом можно, например, вводить ограничения на скорость и число попыток организации соединения с каждым адресом, как это делает **limit** для всех адресов сразу. Более подробное описание модулей hashlimit, limit и tbf вы найдете на сайте.