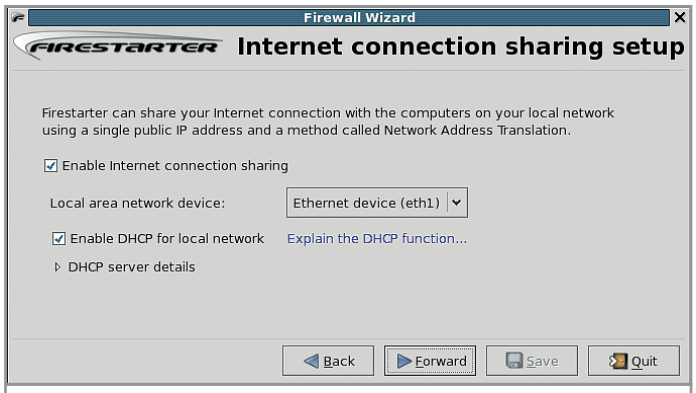
Анатолий Лебедев

# Великая огненная стена

Для того чтобы обеспечить сетевую безопасность в современных пользовательских Linux-системах, совершенно необязательно вручную прописывать все правила iptables. Большую часть рутинной работы может взять на себя Firestarter.

Массовое внедрение широкополосного доступа в Интернет не может не радовать. Как вы сами прекрасно знаете, поставщиков подобных услуг сегодня существует довольно много. К сожалению, далеко не все из них готовы обеспечить безопасность своим пользователям. Почему это происходит — отдельный вопрос. В некоторых сетях проблемами безопасности заниматься просто некому или, что зачастую более верно, никому не хочется. Подобная ситуация свойственна многим только что образовавшимся домашним локальным сетям, организаторы которых ставят перед собой только одну задачу — ничего не делая заработать как можно больше денег. И выполняют они ее с рвением, достойным всяческих похвал.

Пользователям же, которым не посчастливилось оказаться участниками одной из таких сетей, остается только вспомнить известную истину — если хочешь, чтобы что-то было сделано хорошо, то сделай это сам. И, вооружившись свободным пакетом Firestarter, начать стоить собственную крепость, проникнуть в которую злоумышленнику как из локальной, так и из внешней сети будет весьма проблематично. Но перед тем как мы приступим непосредственно к работе, необходимо немного сказать о самой программе. Firestarter — полностью свободное решение, позволяющее, не используя консоль и не изучая достаточно сложный синтаксис системного брандмауэра ядра Linux, задавать политику безопасности для каждого активного сетевого интерфейса.




**Если вы хотите предоставить соединение с Интернетом другим компьютерам, подключенным к вашей сети, воспользуйтесь специальным мастером**

## Установка

Для начала необходимо скачать дистрибутив программы. Последнюю версию продукта можно найти на сайте разработчиков, который располагается по адресу www.fs-security.com, в разделе «Download» .

Как обычно существует несколько вариантов сборки для различных дистрибутивов:

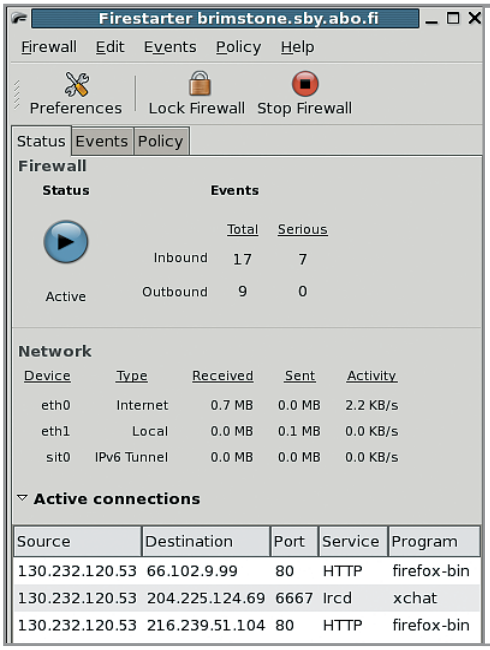
- **Fedora Core**
- **Mandrake**
- **Debian**
- **Slackware**
- **Gentoo**

Ну и, конечно же, в исходных текстах для тех пользователей, которые любят собирать все программы самостоятельно. Так как наиболее удобным и качественным дистрибутивом на сегодня является Fedora Core, скачаем пакет для него. Установка в этом случае происходит следующим образом:

```
rpm -Uvh firestarter-1.0.1-1.i386.rpm
```

После выполнения этой операции в основном меню GNOME или KDE (в зависимости от того, что вы используете) появится иконка Firestarter. Щелкнув по ней, запустите установленное приложение.

Для работы программе необходимо иметь административные полномочия, поэтому сразу после запуска Firestarter перед вами появится окно с предложением ввести пароль для пользователя root. В случае если пароль верен, запустится специальный мастер, который поможет произвести первоначальное конфигурирование программы. После того как она завершит опрос всех установленных в компьютере сетевых интерфейсов, вам потребуется указать, какой из них для чего используется (внешняя сеть, внутренняя). В этом же диалоговом окне можно настроить NAT (Network Address Translations) для работы всех присутствующих в квартире машин через установленное соединение с сетью, а также раздачу IP-адресов через DHCP-сервер.



Окно статуса покажет все активные сессии

## Интерфейс

После окончания работы мастера пользователь попадает в главное окно программы. Его содержимое разбито на три основные группы, в каждой из которых располагаются те или иные компоненты.

## Статус

Первая группа называется «Статус» — в ней отображается список интерфейсов и статистика по ним. Если развернуть скрытые поля под списком интерфейсов, можно будет увидеть все текущие соединения.

## События

Вторая группа носит название «События» и представляет собой таблицу, в которой отмечены все соединения. События отображаются и обновляются в таблице в режиме реального времени, и по ним доступна вся необходимая информация. Все соединения разделены на три типа, и каждый из них отмечается в таблице отдельным цветом. Черным отмечены текущие соединения, серым — заблокированные пакеты. Красным цветом выделены те события, которые могут трактоваться как попытка проникновения к внутренним службам системы и которые требуют к себе особого внимания пользователя.

Если щелкнуть правой клавишей мыши по какому-либо событию, появится контекстное меню, в котором будут предложены действия в зависимости от выбранной политики:

- разрешить соединения с внешнего адреса;
- разрешить использовать эту службу для всех;
- разрешить использовать этот сервис с этого внешнего адреса.

Или же:

- разрешить соединения с этим внешним адресом;
- разрешить исходящие соединения на внешний адрес для этого сервиса;
- разрешить соединения с этого адреса внутренней сети.

**iptables**

## Создание правил вручную

**iptables — пакетный фильтр, встроенный в ядра ОС Linux начиная с версии 2.4. Это серьезная система анализа пакетов, позволяющая реализовать все, что может потребоваться от брандмауэра:**

- **строить firewall, фильтруя пакеты по адресам;**
- **использовать NAT для обеспечения общего доступа в Интернет;**
- **использовать NAT для создания прозрачного прокси-сервера;**
- **строить систему маршрутизации на основе правил QoS.**

**Вся работа с правилами обычно выполняется одноименной утилитой iptables. Так, например, для того чтобы посмотреть список правил, участвующих в обработке пакетов, потребуется ввести следующую команду:**

***iptables -L***

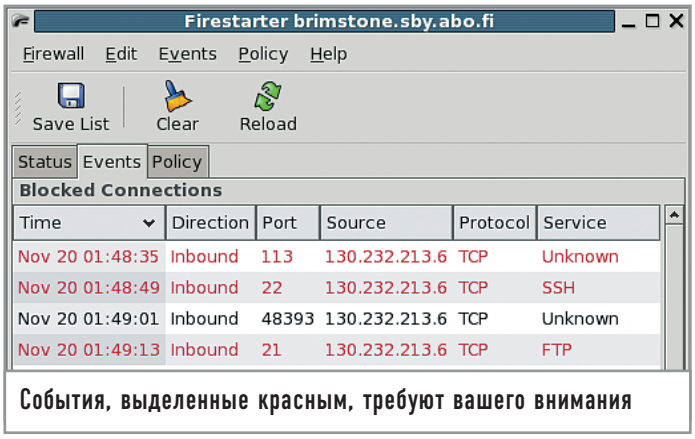
**Для просмотра правил при работе с NAT необходимо явно указать таблицу:**

***iptables -t nat -L***

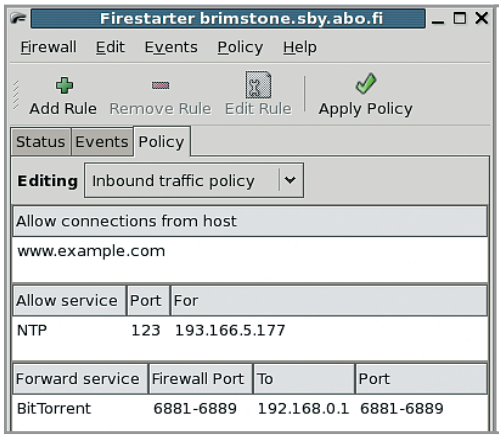
**Для добавления нового правила используется параметр -A:**

***iptables -A INPUT -s 10.11.12.13 -j DROP***

**Данная команда добавляет правило для обработки входящих пакетов с адреса 10.11.12.13 — все пакеты с него будут выкидываться из обработки и не дойдут до получателя. Если вы захотите получить более подробную информацию о работе утилиты iptables, то сможете найти ее в интерактивном справочном руководстве man. Кроме того, в Интернете имеется перевод детальной инструкции по построению брандмауэров с использованием iptables. В ней вы найдете примеры конфигурационных файлов для решения самого различного рода задач, а также сможете познакомиться со всеми параметрами командной строки. Найти ее можно в Интернете по адресу www.opennet.ru/docs/RUS/iptables/index.html.**




**События, выделенные красным, требуют вашего внимания**




**Вы можете задавать правила для входящего и исходящего трафика**

### Политики

Третья группа позволяет редактировать правила обработки входящего и исходящего трафика. Чуть ниже — список адресов, для которых разрешено прохождение данных. Последняя часть управляет трафиком, проходящим во внутреннюю сеть.

## Работа

По своей сути Firestarter — программа для управления firewall, встроенным в ядро Linux, в отличие от большинства решений для ОС Windows, которые полностью выполняют функции фильтра пакетов. Таким образом, при работе с программой мы задаем правила, по которым брандмауэр принимает или отклоняет пакеты. Пакеты в терминологии Firestarter делятся на те, что приходят из внешней сети (Интернет) и из внутренней (LAN). То есть, выбирая ту или иную строку в списке на вкладке «Политика», мы управляем политикой доступа к ресурсам нашей сети из Интернета или же политикой, по которой принимается решение о передаче информации из локальной сети в Интернет.

Для любопытных пользователей разработчиками пакета реализована возможность детально рассмотреть, что же именно создал Firestarter и откуда появляются все эти правила работы с пакетами. В директории /etc/firestarter можно найти скрипты, которые вызываются при запуске программы и которые, собственно, создают правила. При желании в эти скрипты можно добавлять дополнительные правила. Например, если в вашей домашней сети гуляет большое количество широковещательных пакетов от Windows-компьютеров на порты 135–139, можно добавить правило, блокирующее их. Это избавит вас от большого количества мусорных сообщений в журнале программы.

При работе в сетях, в которых провайдер не заботится о вашей безопасности, стоит закрыть для доступа все типовые сервисы, которыми вы не пользуетесь. К ним можно отнести SMTP, HTTP, FTP, TELNET, RPC и прочие — они могут быть включены по умолчанию и использоваться другими пользователями сети в своих целях. Кроме того, стоит быть очень внимательным при работе с сервисами, обеспечивающими проксирование трафика. Так, например, открытый на весь мир HTTP-Proxy запросто может вас разорить, но если это средство использовать с умом, можно сэкономить некоторую сумму денег за счет кеширования. Подобные примеры можно привести в отношении многих других служб. Если для вас это не совсем очевидно, в этом случае лучше довериться мастеру, который предложит использовать общую политику для обеспечения безопасности среднестатистической системы, причем применяемые в ней правила можно считать оптимальными.

## Заключение

Использование подобных программ весьма неоднозначно оценивается критиками. Опытные системные администраторы просто не понимают, зачем они нужны. Они привыкли работать в консоли и хорошо себе представляют, как настраивать подобные службы вручную.

Другие говорят, что базовая настройка безопасности должна производиться дистрибьютором операционной системы. Позиция авторов описанной сегодня программы не всегда пользуется поддержкой, но, судя по популярности подобных средств для Windows, она обязательно найдет своих поклонников. Можно лишь пожелать несколько достойных конкурентов этому продукту, так как грамотная конкуренция поможет улучшать и совершенствовать его.

**СТРИМ**

## Обход системы фильтрации

**За прошлый год проект компании «МТУ Интел» охватил более ста тысяч домашних пользователей. Подключая клиентов посредством ADSL-канала, компания выдает всем реальные адреса. Это весьма удобно, так как всегда можно добраться до своего домашнего компьютера, находясь, например, на работе. Но при этом стоит учесть, что они, проявляя заботу о пользователе, не пропускают пакеты на порты, являющиеся базовыми для большинства сервисов. Так, например, установив FTP-сервер на стандартный порт, вы не сможете получить к нему доступ. Тот же принцип относится к HTTP и многим другим службам. Полный список фильтруемых портов можно получить на странице http://stream.ru/s-filter. Если вам необходимы «смотрящие» во внешнюю сеть те или иные службы, почти всегда можно настроить их через нефильтруемый порт. Тот же HTTP-сервер Apache можно заставить работать на порту 8008, используя директиву Listen 8008 в файле настройки сервера httpd.conf.**