

# Дистрибутив для создания межсетевого экрана – pfSense

*Сергей Яремчук*

**В начале января был представлен очередной релиз 1.2-RC4 дистрибутива pfSense, предназначенного для построения межсетевого экрана, с которым мы сегодня и познакомимся.**

Основой проекта pfSense [1] послужил m0n0wall, о котором уже шла речь на страницах журнала [2]. Дистрибутив m0n0wall ориентирован в первую очередь на использование во встроенных устройствах, его характеризуют легкость в настройке и понятность для новичка. Основой обоих дистрибутивов послужил FreeBSD. В pfSense разработчики постарались вложить максимальную функциональность, дополнив его приложениями, при сохранении той же простоты. Платой послужили больший размер дистрибутива и более высокие требования, предъявляемые к аппаратной части, в частности к объему оперативной памяти. Еще одним отличием является использование в pfSense Packet Filter (PF) с интегрированным ALTQ (HFSC) вместо IP Filter в m0n0wall. Дистрибутив содержит основные компоненты m0n0wall и поддерживает все присущие последнему функции: DHCP-сервер и клиент, клиент PPPoE, статические маршруты, 802.1Q VLAN, беспроводные устройства, SNMP, IPsec и PPTP VPN, графики работы, Captive Portal с возможностью аутентификации RADIUS и многое дру-

гое. Разработчики pfSense к этому добавили переработанный веб-интерфейс, сервер PPPoE, DNS-форвардинг, FTP-прокси и др. Возможна работа с несколькими WAN-интерфейсами с распределением нагрузки. Правда, с оговоркой: только одно соединение может быть настроено с использованием PPPoE, PPTP или BigPond, остальные должны получать статический или динамический IP-адрес, например в Ethernet-сети.

Поддержка протокола CARP (Common Address Redundancy Protocol), позволяет организовать балансировку нагрузки и прозрачное резервирование шлюза. Кроме IPsec и PPTP поддерживается и OpenVPN. Используя систему пакетов, можно легко установить еще около 20 приложений или сервисов, среди которых Pure-FTPd, Squid, Spamd, Snort, FreeRADIUS, nmap, nut и другие. Хотя в последней версии дистрибутива нужно меню в настройках почему-то отсутствует, информация на сайте о такой функциональности есть по-прежнему. Возможно, это связано с глубокими переделками интерфейса. Если чего-то в этом списке не хватает, можно, используя команду

pkg\_add, легко установить предварительно пакеты. Интерфейс не локализован, но работа ведется, в чем можно убедиться, обратившись по адресу [5]. Судя по приведенной там информации, на дату написания этих строк было переведено 97%, но в настоящее время опять же нет каких-либо видимых инструментов, позволяющих сменить языки интерфейса. Будем надеяться, что они появятся в окончательном релизе. Хотя базового английского вполне достаточно, чтобы разобраться с настройками.

На форуме проекта можно найти и варианты нестандартных решений для pfSense. Например, по адресу [3] рассказано, как pfSense использован в качестве DHCP-сервера на компьютере с одной сетевой карточкой в сети, которая уже имеет свой firewall. Комментарии по поводу целесообразности такого подхода можно почитать в блоге [4]. В вольном переводе и кратко звучит так: это не лучшее решение, но оно работает. Текущей стабильной версией является 1.0.1, которая датирована октябрём 2006 года. Сейчас активно идет разработка релиза 1.2, построенного на FreeBSD 6.2.

Распространяется pfSense по условиям BSD-подобной лицензии, разрешающей его модификацию и бесплатное использование, но с сохранением информации о разработчиках. Заявлена коммерческая поддержка продукта. Остальные пользователи могут получить информацию на форуме проекта.

## Первый запуск

Для работы pfSense потребуются компьютер с 128 Мб оперативной памяти и диск размером более 2 Гб для установки. Требования к процессору не предъявлено. В документе «Known working configurations» можно найти примеры аппаратных средств рабочих конфигураций. В частности, здесь приводятся данные о работе на Pentium 200. Плюс дополнительную информацию о совместимом оборудовании можно найти в документе «Supported Hardware for pfSense/FreeBSD», который также доступен на сайте проекта. Ядро скомпилировано с поддержкой многопроцессорных систем.

Первоначальная работа с pfSense напоминает m0n0wall. После тестирования устройств предлагается настроить сетевые интерфейсы VLAN, LAN и WAN. Если будет обнаружено только одно сетевое устройство, появится предупреждение о невозможности работы роутера. После их настройки можно ввести имя дополнительных (Optional) интерфейсов, хотя, как мне показалось, удобнее эту часть производить в GUI. По окончании подтверждаем установку и ждем. Если IP-адрес интерфейса WAN назначается статически и в сети нет DHCP-сервера, то ждем долго, очень долго. Дело в том, что, как и в m0n0wall, LAN-интерфейс автоматически получает адрес 192.168.1.1, а WAN при помощи DHCP. Первое время я думал, что после появления «Configuring WAN Interface» система виснет, но тестирование на виртуальных машинах и в других конфигурациях показало, что все нормально, нужно долго ждать. К сожалению, игнорировать настройку WAN, чтобы потом все указать через веб-интерфейс, тоже нельзя. Будем надеяться, что такое поведение к релизу исправят, ведь в том же m0n0wall отсутствие DHCP-сервера определялось быстро.

```
*** Welcome to pfSense 1.2-RC4-cdrom on pfSense ***

LAN*      -> 1e0      -> 192.168.1.1
WAN*      -> 1e1      -> 192.168.1.199 (DHCP)

pfSense console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) Pftop
10) Filter Logs
11) Restart webConfigurator
12) pfSense PHP shell
13) Upgrade from console
99) Install pfSense to a hard drive/memory drive, etc.

Enter an option: █
```

Рисунок 1. Меню pfSense

По окончании инициализации – меню. Пунктов в нем на порядок больше, чем в m0n0wall – 16 (см. **рис. 1**). Полезным является возможность указать другой IP-адрес LAN. Выбираем 2, вводим адрес и маску сети, разрешаем/запрещаем использование DHCP-сервера. Под цифрой 99 находится пункт, позволяющий установить pfSense на жесткий диск.

## Веб-интерфейс

Дальнейшие настройки следует производить через веб-интерфейс. Адрес, который нужно набирать в браузере, будет выведен по окончании настройки. Для регистрации используем логин admin и пароль pfsense.

Первоначальную установку можно произвести при помощи Setup Wizard, кнопка вызова которого находится во вкладке «System». Здесь все просто. На первом шаге указываем имя и домен, к которому принадлежит компьютер, адреса DNS-серверов, часовой пояс и сервер времени. Далее настройки WAN. Выбираем тип получения адреса: DHCP, статический, PPPoE, PPTP, BigPond. Обратите внимание на два флажка внизу – «Block private networks from entering via WAN» и «Block non-Internet routed networks from entering via WAN», которые блокируют подключение к WAN с адресов указанных сетей. Дальше LAN-интерфейс и смена пароля администратора.

После работы мастера пакеты с LAN в WAN будут проходить без проблем, причем все.

Чтобы самостоятельно создавать правила NAT, следует отключить их автоматическое создание в «System →

Advanced», сняв флажок «Disable NAT Reflection».

Настройка PPPoE- или PPTP-соединения мне показалась несколько запутанной по сравнению с тем же m0n0wall. Дело в том, что после установки будут доступны настройки только LAN и WAN. Если с первым все понятно, то что делать с WAN? Если здесь прописать настройки сетевой карты, то тогда возникает вопрос, где же указывать PPPoE, и наоборот. Оказалось, сначала следует зайти в меню «Interfaces → Assign», перейти во вкладку «VLANs», где создать новый интерфейс, и возвратиться в «Interface assignments». После добавления VLAN на этой странице справа появляется неприметная кнопка. Причем эта кнопка служит как для добавления нового интерфейса, если есть свободный VLAN, так и для удаления последнего в списке. Поэтому следует быть внимательным. На других вкладках для удаления и добавления используются разные кнопки. Теперь настройки внешней сетевой карты указываем во VLAN, а в WAN заполняем информацию о PPPoE. Обратите внимание на сообщения системы, выводимые вверх страницы: в них содержатся предупреждения или рекомендации. В некоторых случаях для VLAN требовалась перезагрузка системы.

По умолчанию SSH отключен, включить его можно во вкладке «System → Advanced». Для повышения безопасности опционально можно указать отличный от 22 порт и отключить аутентификацию по паролю, оставив только по ключу. Ключ следует скопировать в поле Authorizedkeys. Во вкладке «Advanced» можно включить первый

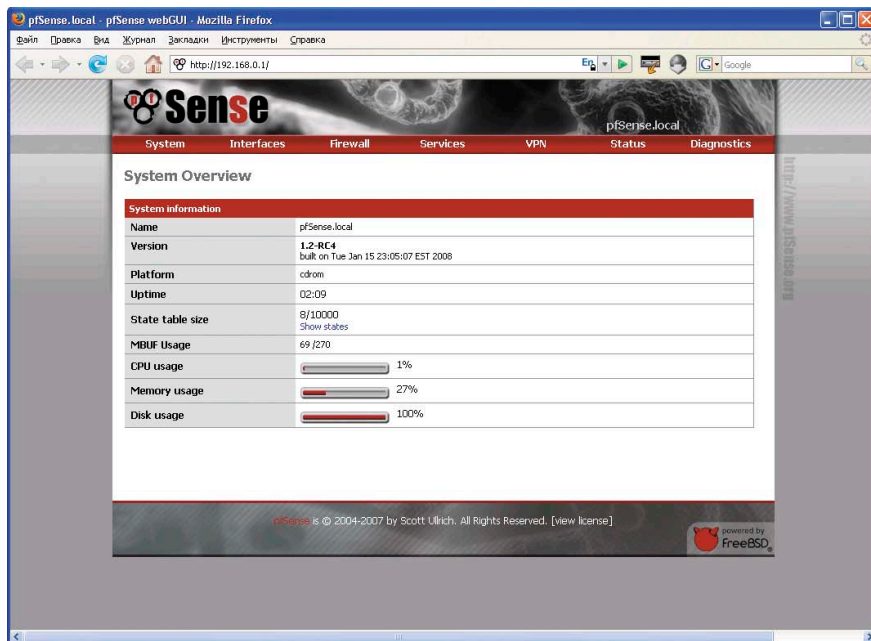


Рисунок 2. Веб-интерфейс pfSense

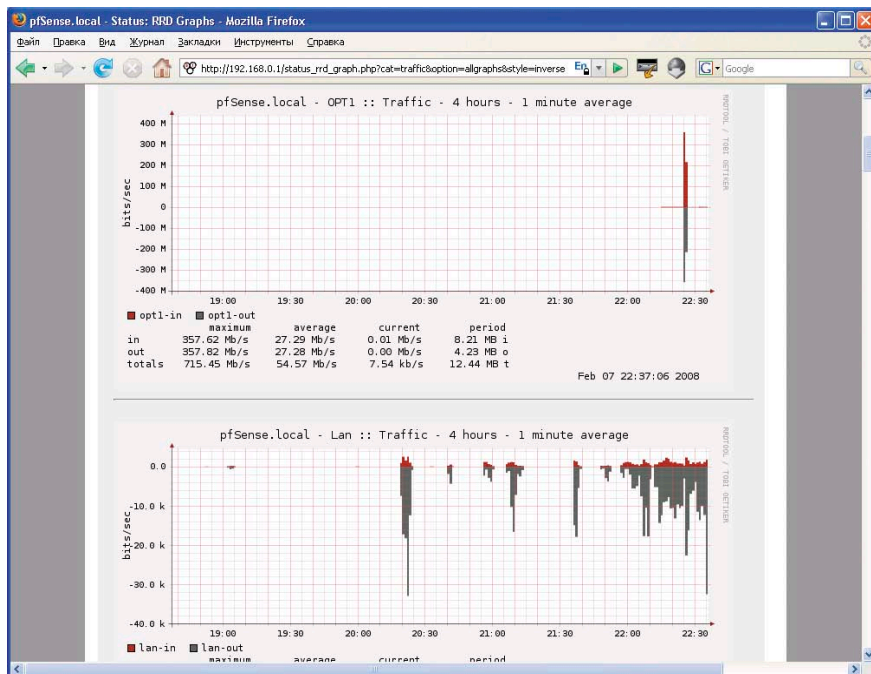


Рисунок 3. Графики pfSense

последовательный порт (это отключит видеокарту и клавиатуру), функцию «Filtering Bridge», указать сертификаты для webGUI, отключить меню в консоли и настроить прочие параметры.

Кроме вкладок, о которых уже говорилось, в интерфейсе pfSense доступны еще четыре. В «Firewall» производится настройка правил межсетевого экрана и NAT. Выбирая пункты меню, можно также задать псевдонимы (aliases), которые позволяют упростить правила и расписание (Schedules). По умолчанию весь тра-

фик разрешен, в LAN стоит правило «Default LAN -> any», а из WAN блокируется доступ только с адресов частных сетей. Правило NAT формируется автоматически (Automatic outbound NAT rule generation). Поэтому сразу после установки pfSense выполняет роль маршрутизатора без фильтрации трафика. Новое правило создается очень просто. Для этого не нужно обладать знаниями PF, достаточно представить конечный результат. Выбирается значение параметра, предложенного конфигуратором (адреса/интерфейс ис-


точника и назначения, протокол, порт или диапазон, расписание и прочие). Ошибиться очень тяжело. Созданные правила можно расставлять по порядку. При выборе пункта «Traffic Shaper» запустится мастер настройки. На первом шаге следует выбрать внешний и внутренний интерфейс и указать скорость Download/Upload, затем устанавливается приоритет для VoIP-сервисов. В «Penalty Box» указываются адреса, трафик с которых будет идти с наименьшим приоритетом. Затем настройки ограничений для P2P-сетей, сетевых игр и остальных протоколов.

Во вкладках «Services» и «VPN» производятся настройки серверов, входящих в состав pfSense. Здесь также ничего сверхсложного, все особенности их работы спрятаны, и с подключением нужной функциональности сможет справиться новичок.

Вкладки «Diagnostics» и «Status» полностью соответствуют своим названиям. Если не нравится внешний вид интерфейса, можно изменить его при помощи скинов.

## Заключение

Впечатление о pfSense только положительное. Несмотря на некоторые шероховатости интерфейса, связанные, очевидно, с тем, что перед нами пока предрилиз, его настройка не должна вызвать особых затруднений даже у неподготовленного человека. Личные впечатления и информация на форумах показывают, что после установки и настройки pfSense без проблем работает как в сетях небольшого размера, так и в больших сетях со сложной структурой.

**P.S.** Пока верстался номер, вышла версия pfSense 1.2. Подробности о внесенных изменениях смотрите на сайте проекта. 

1. Сайт проекта pfSense – <http://www.pfsense.com>.
2. Яремчук С. m0n0wall – дистрибутив для создания межсетевого экрана – //Системный администратор, № 5, 2007 г. – С. 74-77.
3. Форум проекта – <http://forum.pfsense.org/index.php/topic,7052.msg40058.html#msg40058>.
4. Блог проекта – <http://blog.pfsense.org>.
5. Перевод интерфейса pfSense – <http://www.pfsense.com:8080/ru>.