

# О пользе файерволов



*Сергей Супрунов*

Среди начинающих системных администраторов зачастую бытует мнение, что файервол способен решить многие (если не все) проблемы безопасности любого компьютера – от настольной машины до выделенного сервера DNS, и потому его использование обязательно. Как следствие – поголовная «файерволизация» всех систем без исключения... На самом деле файервол – это всего лишь специализированная подсистема, решающая строго определённые задачи.

## Узел противоречий, или Замечание о терминах

На российских IT-просторах «имеют хождение» несколько терминов, обозначающих предмет нашего сегодняшнего разговора: файервол (в различ-

ных синтаксических начертаниях), брандмауэр (наивная попытка перевести английский термин firewall на более подходящим «отечественным» словом), пакетный фильтр, межсетевой экран.

Зачастую они используются как синонимы, хотя при дотошном рассмотрении можно найти некоторые тонкости по смыслу между ними. Иногда в эту же плеяду добавляется термин «бастион».

Ну, фаервол и брандмауэр – по сути, одно и то же (см. врезку «Для справки: брандмауэр»), а смысла для русскоговорящих людей они не несут никакого – весь смысл закладывается исключительно разношёрстными определениями. (Можно проследить некоторую тенденцию термином «фаервол» именовать программный пакетный фильтр, а словом «брандмауэр» – аппаратный межсетевой экран или выделенный компьютер-шлюз, выполняющий функции МСЭ. Впрочем, тенденция довольно слабенькая.) А вот словосочетания «пакетный фильтр» и «межсетевой экран» уже обладают и определёнными лексическими значениями, на основе которых можно найти некоторые различия этих терминов.

Очевидно, что межсетевой экран (МСЭ, иногда просто МЭ) – это экран между сетями, ограничивающий доступность одной сети из других. В основном МСЭ применяется для ограничения доступа в локальную сеть предприятия из Интернета (а также в обратную сторону).

Из термина же «пакетный фильтр» (ПФ) следует, что задача одного – фильтрация отдельных пакетов (как правило, речь идёт о пакетах стека TCP/IP). Поскольку межсетевое экранирование частенько ограничивается фильтрацией пакетов на шлюзе между сетями, то термины МСЭ и ПФ нередко используются как синонимы. Но нужно иметь в виду, что фильтровать пакеты можно не только между сетями, а межсетевое экранирование может осуществляться и на основе других принципов (например, с помощью прокси-сервера или технологии NAT). Кроме того, понятие МСЭ в широком смысле охватывает все уровни сетевой модели OSI, в то время как зона действия ПФ обычно ограничивается сетевым и транспортным уровнями (иногда «дотягиваясь» до канального и прикладного).

Ну и, наконец, «бастион». Обычно этим термином определяют выделенный компьютер, располагающийся на границе локальной сети и решающий задачи меж сетевого экранирования (хотя некоторые авторы довольно охотно используют здесь слово «брандмауэр»).

В дальнейшем мы будем говорить в основном о пакетных фильтрах (ис-

## Для справки: брандмауэр

На Руси термином «брандмауэр», позаимствованным из немецкого языка (die Brandmauer, противопожарная стена), в пожарном деле некогда называли огнеупорную стену, разделяющую здание и призванную защитить всё строение в целом в случае возгорания в одной из его частей. Поскольку слово «firewall» означает у пожарных Туманного Альбиона то же самое, то некоторые российские перевод-

чики решили использовать именно термин «брандмауэр» как более интегрированный в русский язык.

Кстати, этимология слова «фаервол» как раз и восходит к этой пожарно-архитектурной конструкции, то есть речь не об «огненной стене», где «сгорают» все зловерные пакеты, а о «стене», защищающей вашу маленькую локальную сеть от «пожара», бушующего на просторах Интернета.

пользуя термин «фаервол» в этом смысле). Некоторые особенности МСЭ укажем отдельно.

## Один в поле не воин?

Итак, зачем же нужен фаервол? Если говорить упрощённо, то его основное назначение – защита сети или отдельного хоста от внешних соединений путём фильтрации нежелательных пакетов, а в некоторых случаях и блокирование внутреннего трафика, пытающегося выйти за пределы локальной сети. Посмотрим, когда же такая защита действительно необходима. Начнём со случая отдельного хоста, не выполняющего роль маршрутизатора между несколькими сетями (например, это может быть рабочая станция пользователя или веб-сервер в «демилитаризованной зоне» (DMZ)).

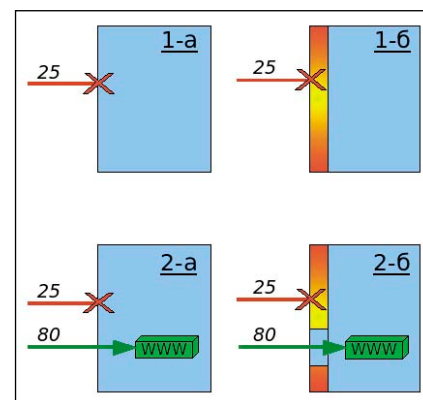
На **рисунке** на схеме 1-а условно изображена операционная система, на которой ни одна из сетевых служб не запущена. Что произойдёт при попытке извне обратиться, скажем, к 25-му порту такой системы? Соединение будет отклонено, поскольку на указанном порту никакая программа, способная это соединение обработать, не функционирует.

По какой-то надобности мы решили защитить эту систему с помощью «закрытого» фаервола (см. **рисунок**, схема 1-б). Теперь при обращении к 25-му порту соединение также будет отклонено (хотя и несколько иначе), но уже не сетевым стеком операционной системы, а пакетным фильтром. Получается, что мы ничего не приобрели в плане функциональности, но зато обзавелись дополнительной подсистемой, которая требует вычислительных ресурсов и внимания со стороны администратора. (Я уже чувствую, как некоторых читателей начинает переполнять

праведный гнев от такой неслыханной некомпетентности. Прошу у них некоторого терпения – чуть позже будут раскрыты и отличия первого и второго случаев. Сейчас же нам важен общий принцип без излишних деталей.)

Теперь предположим, что нам нужно запустить на данном хосте публичный веб-сервер. В первом случае мы просто запускаем Apache (или кому что больше нравится), который приступает к обслуживанию запросов на 80-м порту TCP. Любые соединения на другие порты по-прежнему будут отклоняться операционной системой (см. **рисунок**, схема 2-а). При использовании ПФ мы будем вынуждены открывать в нём «дырку» для доступа к 80-му порту (см. **рисунок**, схема 2-б). То есть опять получается, что в обоих случаях мы приобретаем одинаковую функциональность – доступ возможен только на 80-й порт, и если работающий там Apache содержит уязвимость, то ПФ никакой защиты от взлома не обеспечивает (хотя, как будет показано ниже, может в ряде случаев усложнить дальнейшее развитие атаки).

Кто-то наверняка уже подумал, что схема 2-б более гибка, поскольку ПФ позволяет пропускать не все



«Незащищённая» система и система с пакетным фильтром

соединения, а лишь с тех IP-адресов, с которых нужно. В общем случае это действительно так (более того, есть и другие «сопутствующие» функции ПФ, о которых будет сказано далее). Но с учётом того, что и Apache прекрасно справляется с ограничением доступа, используя правила Allow и Deny (да ещё и на уровне отдельных каталогов и даже файлов, а не только всего сайта в целом), в данном конкретном примере особой пользы от ПФ тоже не видно. Тем более, что речь мы сейчас ведём о «публичном» веб-сервере, то есть службе, которая должна быть доступна всем желающим.

Таким образом то, что во многих настольных дистрибутивах Linux, во FreeBSD и ряде других систем файрвол по умолчанию не запускается, — вполне нормально, и вовсе не подрывает общую защищённость системы. Если внимательно следить за тем, какие сервисы на каких портах работают, то потребность в фильтрации трафика обычно не возникает — в любом случае мы должны пропускать трафик к работающим службам, а блокирование остальных портов не требуется, поскольку там и так никакая программа не работает.

## Граница на замке

А вот если рассматриваемый узел выполняет роль маршрутизатора, будучи включённым несколькими своими интерфейсами в различные сети, то здесь файрвол уже приобретает действительную ценность. Безусловно, можно по-прежнему обойтись и без него — за счёт грамотного администрирования сетевых служб на всех хостах сети. Но что проще — закрыть доступ к 69-му порту в правилах ПФ на шлюзе, или же на каждой машине сети, использующей TFTP, прописывать, с каких IP-адресов на этот порт доступ открыт, а с каких должен блокироваться, и затем отслеживать добавление/удаление машин, смену их IP-адресов и так далее?

Так что в полезности файрвола в его функции межсетевого экрана сомнений, думаю, ни у кого не возникает, и это применение подробно описано в самой различной документации и литературе.

Однако здесь нужно заметить, что указанная польза от файрвола на

шлюзе имеет место быть лишь в том случае, когда внутри локальной сети используются реальные IP-адреса (то есть к которым возможен непосредственный доступ из Интернета). Если же вы используете «частные» адреса, описанные в RFC1918 (а именно так в большинстве случаев и бывает, по крайней мере, в России, не избалованной избытком свободных IP-адресов), то ваша локальная сеть уже отделена от Глобальной сети, и для решения проблем контроля за транзитом трафика через шлюз может оказаться достаточно таких средств как NAT- или прокси-серверы.

## Долой дискриминацию файрволов!

Справедливости ради, вернёмся к первому случаю — использованию файрвола на хосте, не являющемся маршрутизатором (да и к варианту с маршрутизатором многое из сказанного ниже тоже относится). Раньше мы пришли к выводу, что файрвол в обычной ситуации на такой системе бесполезен. Однако в ряде случаев его использование может принести определённые преимущества (а порой становится необходимым).

Во-первых, если в реализации сетевого протокола операционной системы есть уязвимости, то файрвол позволит минимизировать последствия некоторых атак (зато, если уязвимости есть в самом файрволе...).

Во-вторых, в некоторых «закрытых» операционных системах администратору довольно сложно контролировать, какие сетевые службы запущены, для чего они предназначены, какими программами обслуживаются и т. д. В таком случае бывает проще «отгородить» операционную систему от остального мира пакетным фильтром, чтобы получить некоторый уровень контроля над её сетевой активностью. Здесь же заметим, что и на всех остальных системах нельзя быть на 100% уверенным в том, какие программы и на каких портах работают, если система будет взломана — в этом случае файрвол, делающий невозможным работу программ на произвольных сетевых портах, может существенно усложнить жизнь злоумышленнику (правда, лишь в случае, если в результате взлома не получены

права суперпользователя; иначе любые правила фильтрации можно легко изменить).

В-третьих, современные пакетные фильтры, помимо собственно фильтрации по адресам, портам и прочим признакам, могут предоставлять развитые средства нормализации пакетов, защиту от подмены IP-адресов (полезную, впрочем, только при наличии нескольких сетевых интерфейсов), способны ограничивать интенсивность входящих и/или исходящих соединений, управлять доступной полосой пропускания сетевого канала, позволяют контролировать способ блокирования нежелательного трафика (скажем, с выдачей RST-пакета или без таковой) и так далее.

Кстати, а чем, как не пакетным фильтром, мы обычно перенаправляем трафик на прозрачный прокси-сервер или выполняем NAT-трансляцию? Наконец, пакетные фильтры превосходно умеют этот трафик считать! Таким образом, для решения подобных специфических задач программа-файрвол может оказаться весьма полезной даже на машине с одним сетевым интерфейсом.

## Быть или не быть?

Таким образом, использование файрвола весьма желательно, но всё же не является таким уж бесспорным вопросом. Фильтрация трафика не всегда имеет смысл, и уж тем более не является панацеей от любых проблем безопасности. Хотя всегда можно сказать, что хуже от использования файрвола не будет (и это по большому счёту действительно так), лучше всё же более взвешенно оценивать необходимость в нём, чтобы избежать дополнительной работы (как для себя, так и для своих коллег).

Ну и напоследок хочется опять вернуться к терминологии. С учётом вышесказанного, наиболее предпочтительными терминами мне видятся всё-таки «межсетевой экран» и «пакетный фильтр», как дающие лучшее представление о функциях и целях конкретной подсистемы. Впрочем, учитывая бездонное море уже написанной и переведённой документации, можно смело предсказывать термину «файрвол», несмотря на его неоднозначность, безоблачное будущее. 