Автор:
05.04.12 16:54 - Последнее обновление 05.04.12 17:12

Виртуальный сетевой экран (Виртуальный файрвол).
или установка PfSense на VirtualBox

Мы уже говорили о виртуализации, о необходимости защиты своего сетевого трафика экранами, о дырявости встроенных экранов в Windows XP, о уязвимости любой Windows просто потому, что множество ловких парней и девчат день и ночь ищут и находят эти уязвимости. А теперь поговорим о возможности пристроить на Windows машине OpenBSD-ный файрвол с помощью виртуальной машины.

Прелюдия.

Однажды широко известный в узких кругах никсоидных параноиков Лёха Монтанов в статье журнала BSD 3/2010 на странице 14 обнаружил нечто, сильно взбудоражившее его воспаленное воображение, несмотря на английский язык изложения. Сначала он хотел просто сделать перевод, потом затеять переписку с настолько (как оказалось) близкими по духу людьми по ту сторону океана, но в итоге получилось что-то в очень вольном изложении. Авторы посоветовали в VMware сервере на Windows XP хосте поднять OpenBSD, в которой есть встроенный сетевой экран (файрвол), через который и пустить весь трафик.

Мы целиком и полностью согласны с такой реализацией идеи, но для подтверждения универсальности принципа выбрали Windows 7, в которой в VirtualBox поселим FreeBSD с тем же самым PF. В дополнение всего эта машина будет стартовать из автостарта втемную и втихую.

Intro (от Л. Монтанова).

Все прелести использование виртуального файрвола изначально были изложены еще в 2005 году Василисом Превалакисом, профессором забугорного университета (Drexel University, Philadelphia). Наш бывший соотечественник предлагал использовать в качестве виртуального файрвола PF и OpenBSD 3.7, работающей при помощи бесплатного VMPlayer. Много времени прошло с тех пор. Pf был портирован и удачно работает во FreeBSD, а на горизонтах виртуализации стабильно развивается проект от Sun Microsystems под названием VirtualBox. Их как раз и будем использовать. Чтобы не

разочаровывать пользователей длинной и нудной работой (для кого это и праздник в принципе:) в консоли FreeBSD, был взят дистрибутив PfSense, включающий в себя непосредственно FreeBSD и уже минимально настроенный файрвол. Плюс ко всему возможность настройки маршрутизатора через веб-интерфейс, что несомненно облегчит жизнь 95% пользователей.

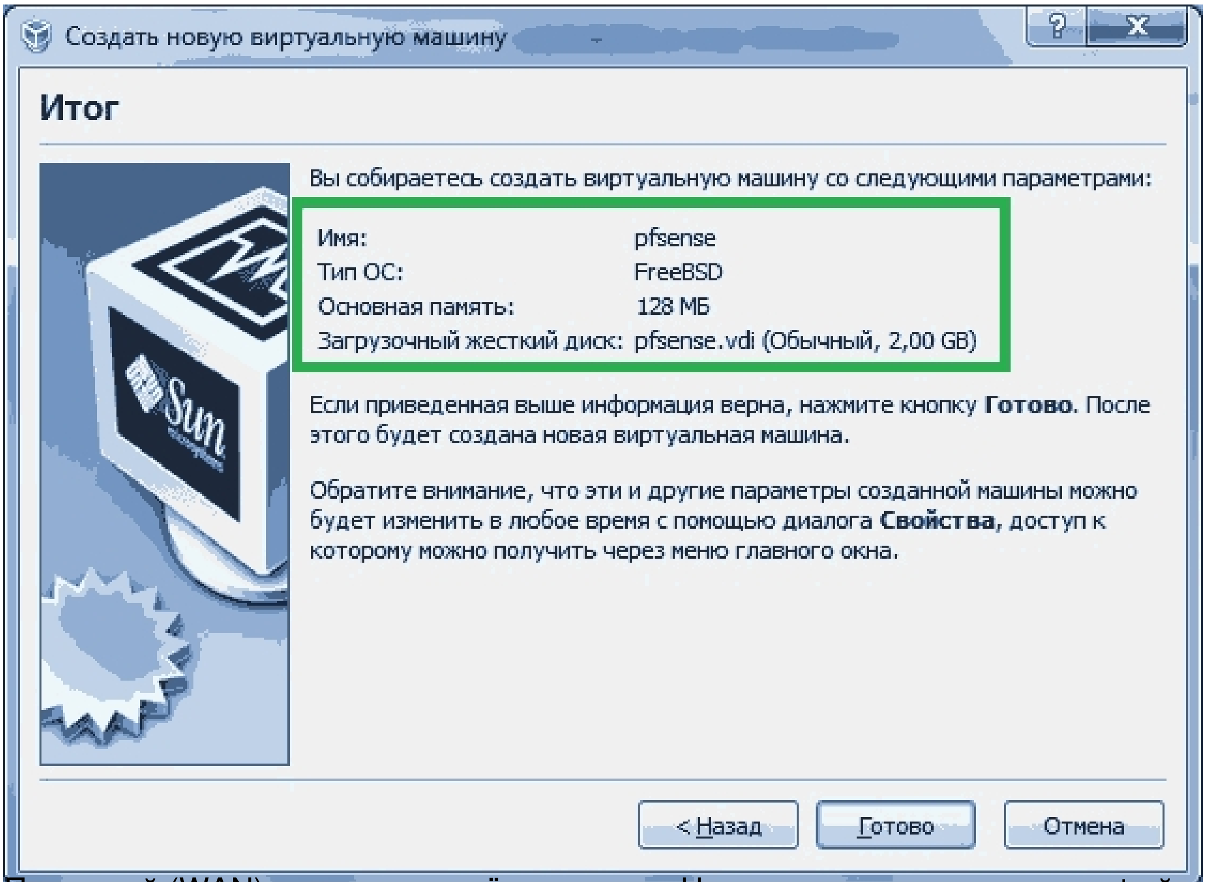
Вопрос из зала: "А зачем это все надо-то? Мой штатный брандмауэр Windows итак прекрасно справляется со всеми задачами!" Ответим на данный вопрос. О том как сломать и обойти Ваш брандмауэр сидит и думает ежедневно не одна тысяча человек, в виде упомянутых выше ловких парней и девчат иностранного (китайского в основном) и российского происхождения. И они постоянно успешно справляются с поставленной задачей, всячески помогая вредоносному программному обеспечению (читай вирусам, троянам, червям и прочему) беспрепятственно проникать в Вашу операционную систему. И это лишь один из многих его недостатков. Если злоумышленник проводит атаку на Windows-машину, значит он обязательно ищет пути обхода штатного файрвола. Ситуацию усугубляет уязвимость стека TCP/IP в Windows.

Пару слов о том, как все это работает. Виртуальная машина выступает в роли маршрутизатора и файрвола для Вашего основного компьютера. Попадая на физический сетевой интерфейс, пакет сразу передается в виртуальное окружение, проходит обработку на "пригодность" и в случае положительного заключения передается через виртуальный интерфейс Вам. Для Вас это делается абсолютно прозрачно и Вы не видите разницы.

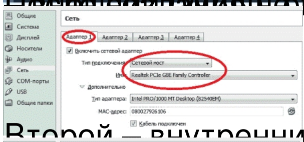
Собсно, сабж.

Имеем Windows 7, интернет. Необходимо скачать последний **VirtualBox** и **PFsense** – дистрибутив FreeBSD в виде LiveCD , в который включен портированный из OpenBSD сетевой экран pf.

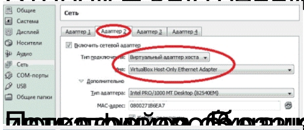
Качаем, ставим VirtualBox. Запускаем его, создаем новую машину pfsense с динамическим диском 2 Гб, 128 Мб памяти, как на картинке.



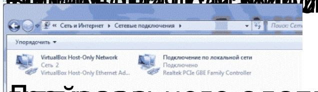
фейсы. Первый



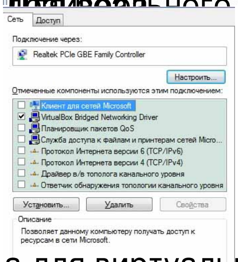
Второй – внутренний (LAN), направлен на виртуальный адаптер хоста.



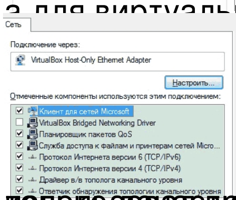
го сетевого



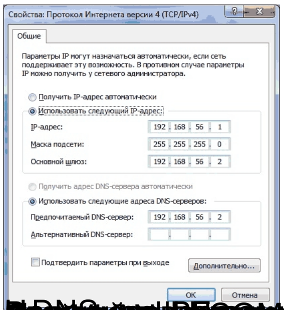
адаптера (в моем случае – это Realtek) отключаем все, кроме VirtualBox

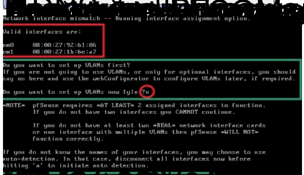


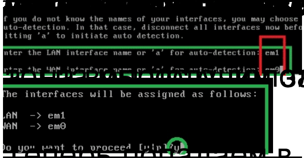
а для виртуального адаптера (VirtualBox Host-Only Network) оставляем все,



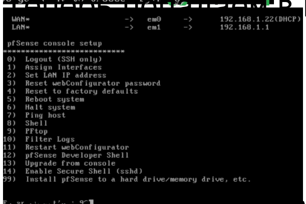
для выхода в сеть



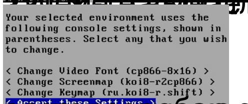




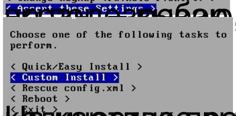
...меню, где выбираем 99 – установка на жесткий диск.



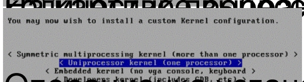
...окне спрашивается про локализацию шрифтов, я



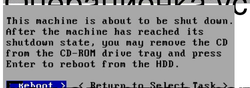
...ных установках результат будет тот же. Следующий

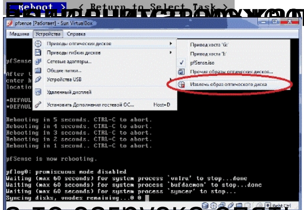


...“Quick/Easy Install”. Далее

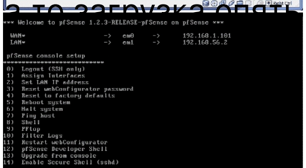


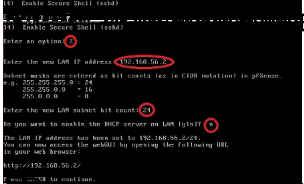
Операционка установится, потом скажет приготовьтесь и перезагрузите компьютер.





...начнется с него. После загрузки получаем такое меню.





Следующий экран – настройка WAN.