почему не фаерволят фаерволы

tagline: ошибки конфигурации персональных брандмауэров

криска ака мыщъх, no-email

> **вот стоит фаервол, неприступный как скала. наивный юзер свято верит, что никакой червь, троян или хакер через этот фаервол не перелезет. фиг там! фаеры блокируют лишь единичные вторжения и шанс подцепить заразу от наличия/отсутствия фаервола не зависит. точнее, _практически_ не зависит, поскольку большинство юзеров даже не пытаются сконфигурировать свой фаерок, а на все его вопросы не задумываясь отвечают "да". возможности фаеров, конечно же, не безграничны, но в умелых руках они превращаются в мощное оружие, отражающее значительный процент атак.**

введение

Фаер (от английского firewall – огненная стена, точнее, огнезащитная стена, разделяющая смежные здания от распространения пожара, ведь в былые времена зачастую выгорали целые города), он же **брандмауэр** (от немецкого brandmauer — brand: пожар, mauer: стена), он же **межсетевой экран**, если говорить совсем по-русски. Но что же это все-таки такое? А ничего… Удачный маркетинговый трюк впарить нам многофункциональный "швейцарский" нож, вместо того, чтобы позволить покупать эти программные продукты по отдельности.

Персональные фаеры берут на себя функции:

- маршрутизаторов, определяя политику перемещений пакетов между узлами;
- proxy-серверов, громко называемых "брандмауэрами уровня приложений";
- систем обнаружения вторжений (они же IDS – Intruder Detection System);
- антивирусов, ищущих в трафике известные сигнатуры;
- ревизоров, контролирующих целостность файлов;
- …и многое-многое другое.

С одной стороны — мы получаем оптовый пакет "услуг", который в розницу обошелся бы намного дороже (ну, представим себе на минуту, что пиратства в России нет), плюс каждый программный пакет потребовал бы индивидуальной настройки. Но если рассмотреть вопрос под другим углом, развернув принцип на 180 градусов ниже нуля, можно быстро прийти к выводу, что комбинированные устройства хорошими не бывают и швейцарским ножом тот же швейцарский сыр не разрежешь.

Популярность персональных фаеров в первую очередь связана с интенсивным рекламным маркетингом и лишь потом с их реальными достоинствами, однако, предлагать читателю устанавливать~~овить~~ набор профессиональных проактивных и реактивных защитных систем никто не собирается, ведь даже персональные фаерволы удается настроить немногим.~~лишь единицам.~~

На самом деле все не так уж и сложно. Фаервол — сравнительно бесхитростная ~~вещь~~штука и конфигурируется с полпинка. Главное — базовыми понятиями владеть, которые мыщъх сейчас и растолкует.

>>> выноска 1

> **Firewall правильно переводится отнюдь не как "огненная стена"/"стена огня", а как огне*защитная* стена.**

обзор персональных брандмауэров

Рынок велик, широк и могуч. Программистов много. И каждый из них, сцука такая, хочет кушать, то есть жрать. Вот они и программируют всякую хрень, засоряющую информационное пространство глобальной сети.

Фаеров куча — какой из них выбрать? Или, быть может, ничего выбирать не нужно и выбор уже сделан за нас? В XP SP2 встроена какая-то пародия на персональный брандмауэр, которая делает вид, что работает и страшно нервничает при всякой попытке ее отключения, популярно объясняя пользователю, что его компьютер находится в ужасной опасности и вот-вот падет жертвой хакерской атаки или другой крупной трагедии.

На сайте http://www.firewallleaktester.com можно найти перечень персональных брандмауэров вместе с результатами тестирования их стойкости к различным видам проникновения. Последнее тестирование состоялось в 2006 году. То есть больше года назад. Для компьютерной индустрии — это огромный срок, но… ядра персональных брандмауэров не переписываются каждый день, да и методики атак совершенствуются довольно медленно, поэтому представленным результатам вполне можно верить.

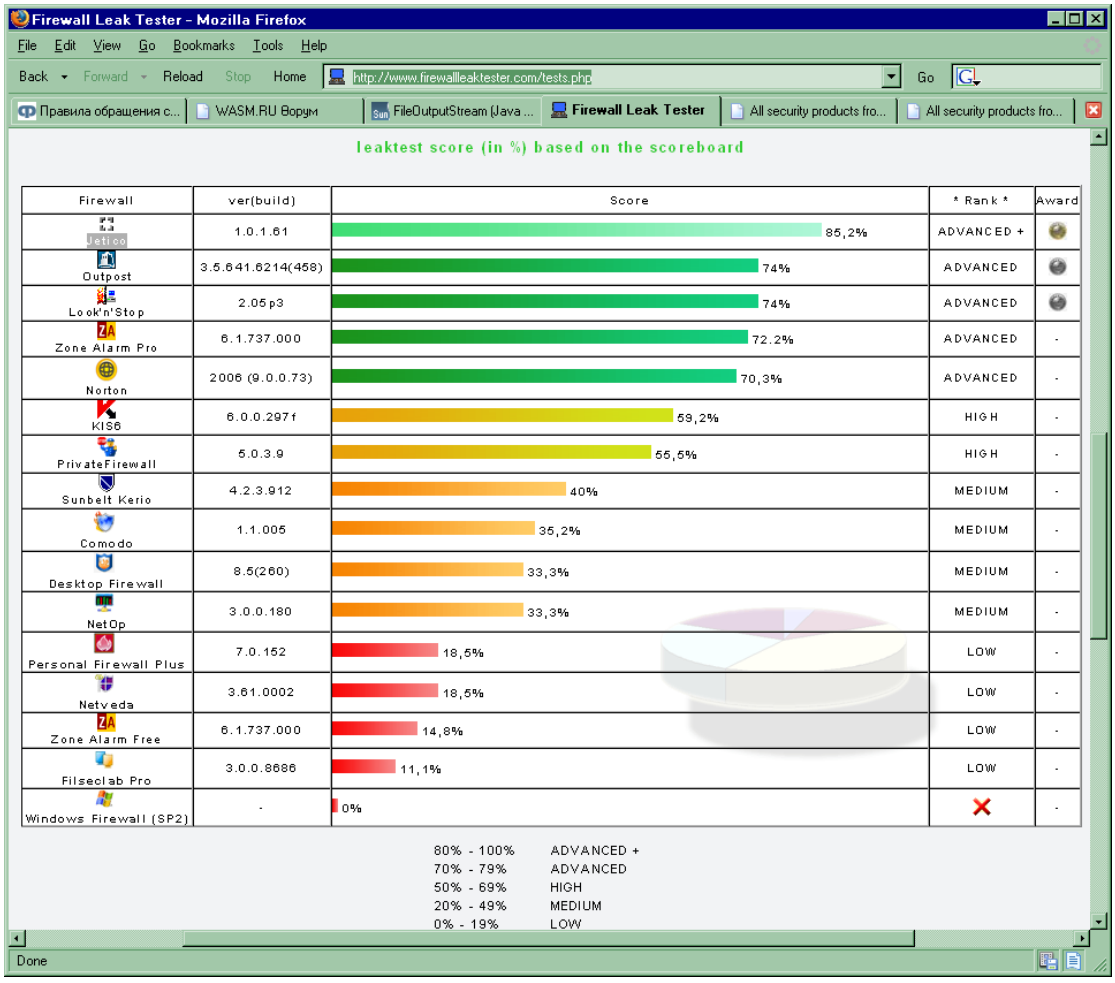

Рисунок 1 результат тестирования персональных брандмауэров по данным http://www.firewallleaktester.com

Первое место занял компактный и к тому же бесплатный фаервал **Jetico Personal Firewall**, созданный одноименной компанией (http://www.jetico.com/jpfirewall.htm). На втором месте оказался популярный отечественный брандмауэр **Outpost Firewall Pro** от компании Agnitum, ожидающей 40 убитых енотов за каждый компьютер на котором он будет установлен. Возможно, Outpost действительно хороший персональный брандмауэр (лично меня как разработчика прельщает возможность создания подключаемых модулей и наличие SDK, но отпугивает откровенно кривая реализация перехвата системных функций), однако, отдавать свои кровные не каждый захочет. Windows Firewall вообще провалил тестирование и вместо награды получил жирный красный крест. А чего еще можно ожидать от Microsoft?!

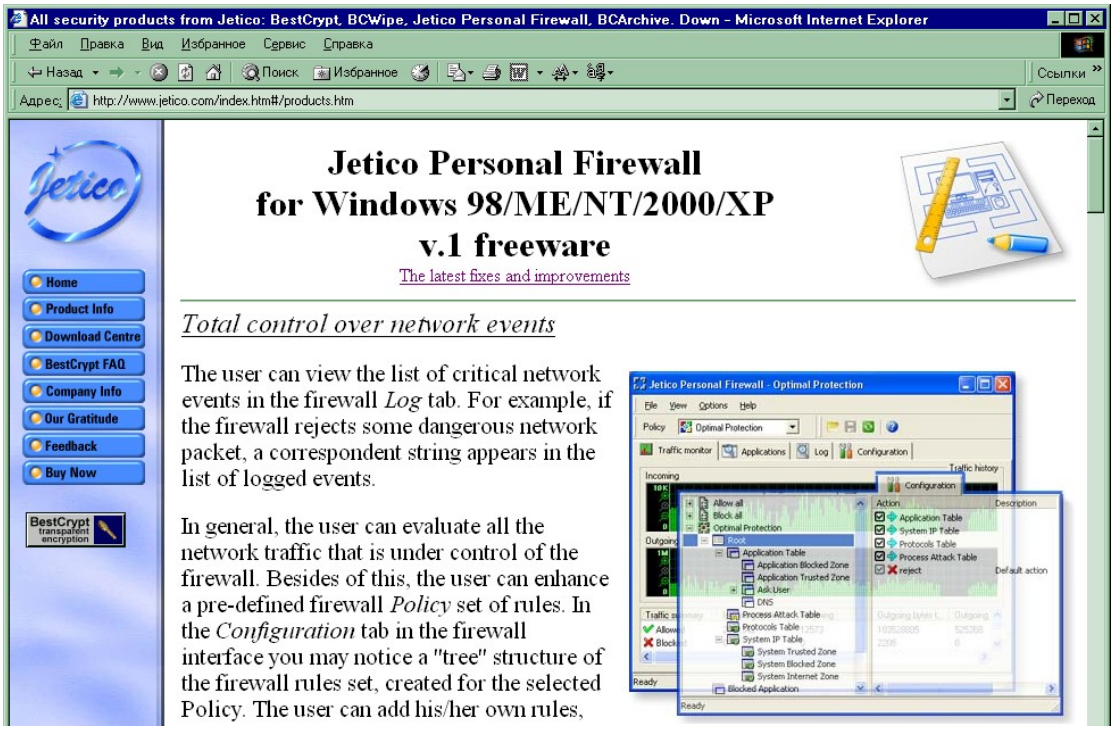

Рисунок 2 отсюда можно скачать лучший бесплатный брандмауэр — Jetico Personal Firewall

По другим данным (см. "*Personal Firewall Software Reviews 2007*" http://personal-firewall-software-review.toptenreviews.com), самым лучшим фаером признан **ZoneAlarm Pro** (золото), Outpost занимает свое "законное" второе место (серебро), а вот **SyGate Personal Firewall**, которым пользуется мыщъх, не получил даже бронзы, попав на восьмое место.

Какой из этого напрашивается вывод? Качество персонального брандмауэра весьма относительная величина, слагающаяся из множества критериев, каждому из которых присваивается свой "вес", но… чтобы получить объективную оценку (или претендующую на роль таковой), необходимо поставить всех пользователей раком, навязав им свои понятия, что такое "хорошо" и что такое "плохо". Например, лично мне плевать на удобство интерфейса, гибкую систему формирования отчетов, etc. Достаточно, чтобы брандмауэр вел мониторинг сетевой активности, писал логи и позволял открывать/закрывать доступ к определенным портам с указанных IP-адресов, что умеет практически любой персональный брандмауэр, исключая разве что недоразумение под названием Windows Firewall.

Короче, братва, кончай дрочить над обзорами. Берем любой фаер и начинаем его настраивать.

Рисунок 3 результат тестирования персональных брандмауэров по данным http://personal-firewall-software-review.toptenreviews.com

В данной статье в качестве подопытной крысы использован SyGate Personal Firewall 4.2. Это — бесплатная версия, остальные уже распространялись как shareware (либо с деньгами и полным функционалом, либо без денег и возможности ведения логов).

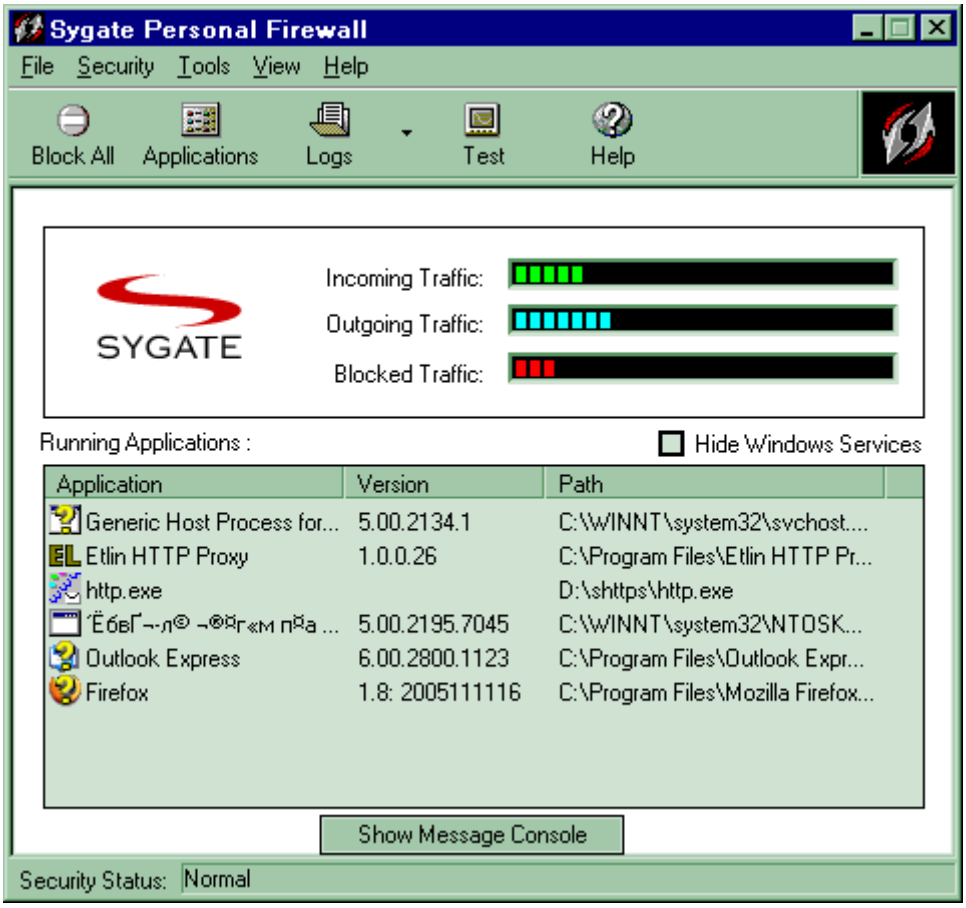

Рисунок 4 внешний вид брандмауэра SyGate Personal Firewall

>>> выноска 2

Не важно какой у тебя брандмауэр. Важно — как он настроен!

что может и не может брандмауэр

Ага, вот! Порты закрыть он может!!! Брандмауэрами закрывают порты — это все знают! Но далеко не каждый догадывается, что… у него нет тех портов, которые следовало бы закрыть. Перефразируя кота Мурзика можно сказать: "чтобы закрыть какой-то порт, его прежде нужно открыть, а чтобы открыть порт у нас денег нет". В прямом смысле. В смысле денег. Вот, допустим, у кого-то имеется локальная сеть с SQL-сервером, который должен быть "виден" только изнутри и недоступен снаружи. В таких случаях умные администраторы просто объясняют маршрутизатору, что SQL не вправе получать пакеты, приходящие из внешнего мира, равно как и отправлять их. Аналогичным образом порты SQL-сервера закрываются и на брандмауэре.

Ах! У нас нет SQL-сервера! Какая жалость!!! А что у нас еще есть?! Ну… если хорошо поискать… Вот черт, ничего не находится!!! Ну, это на Linux ничего не находится, а вот коварная Windows открывает ряд портов для своих служебных целей, даже если нам эти цели без надобности (см. рис. 5)

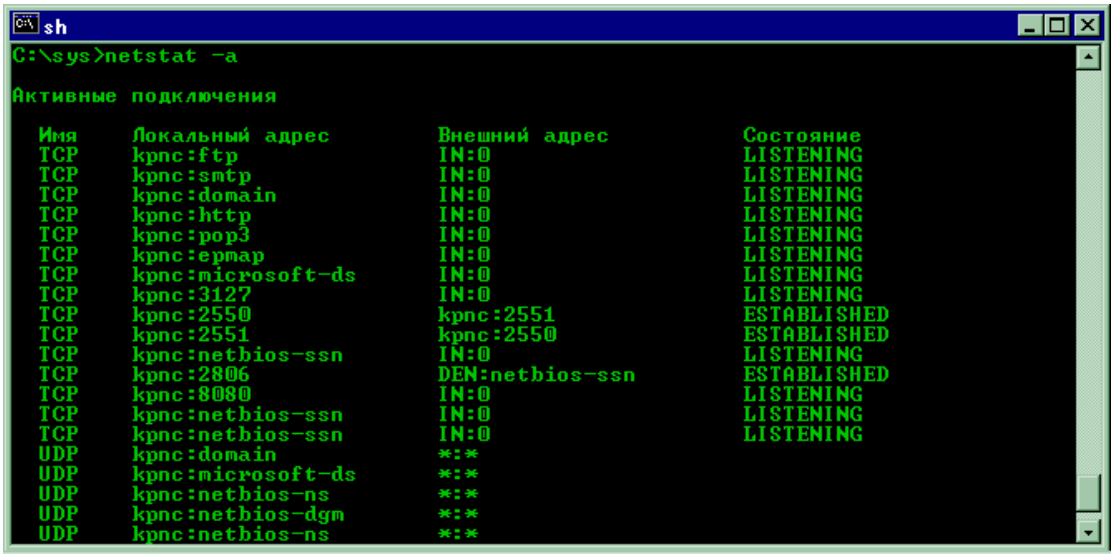

Рисунок 5 штатная утилита netstat, запущенная с ключом -a показывает все порты, открытые системой (строка LISTENING)

В частности, известный червь MSBlast распространялся через дыру в службу DCOM RPC, а точнее через открытый ей 135 gopт. Что такое DCOM RPC? Ну… если у нас намного больше одного компьютера и проснувшись с бодуна мы решили разбить их на домены, то… ну, то есть на фиг этот DCOM RPC, если короче.

Существовало три пути, чтобы предотвратить вторжение червя. Первое — установить заплатку, которая, если мне не изменяет память, вышла за год или полгода до эпидемии. Второе — отключить саму службу DCOM RPC, благо 99,9% пользователям она нужна как мыщъху панталоны. Штатными средствами этого было не сделать, но в сети тут же появились "выключалки" от сторонних разработчиков. Наконец, третий путь: закрыть этот зловредный 135 порт на брандмауэре, что в свое время и сделал мыщъх, которому было лень качать заплатку (см. рис. 6).

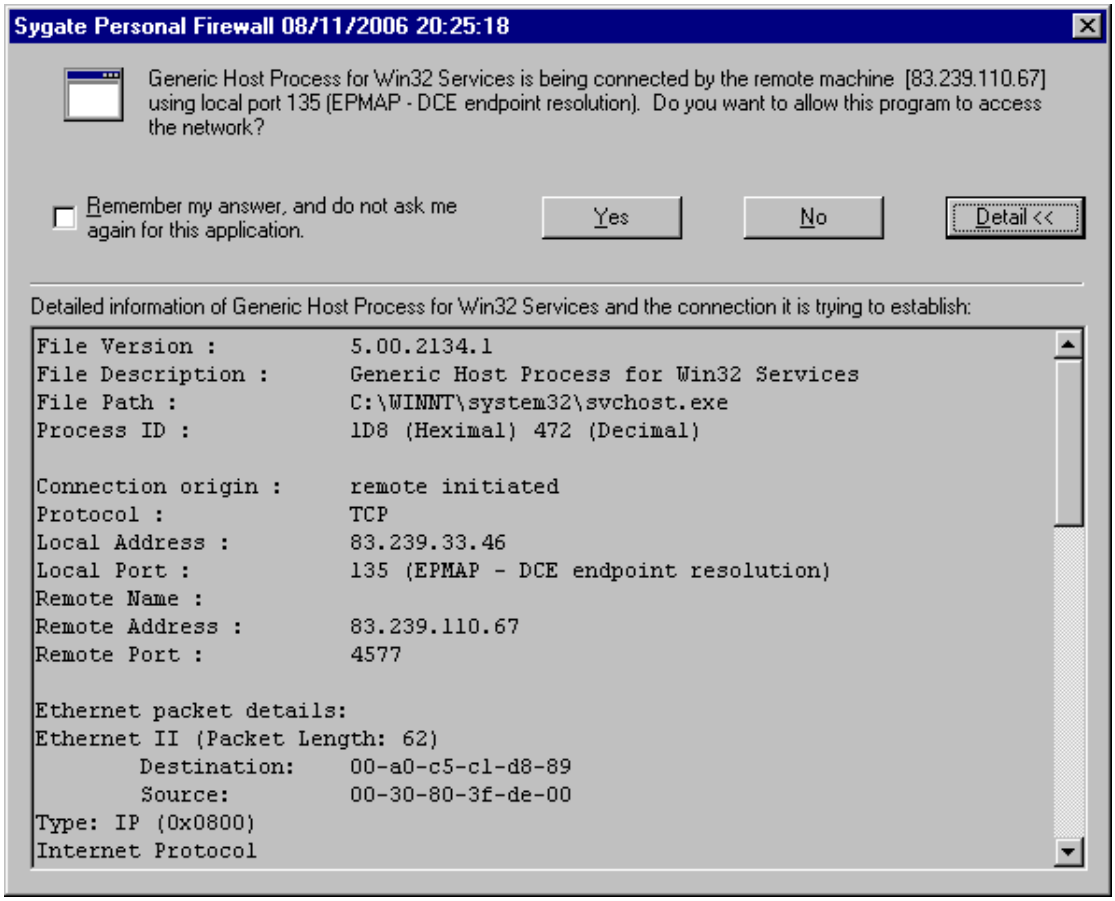

Рисунок 6 червь MSBlast ломиться на уязвимый 135 порт, закрытый на брандмауэре

Однако, данное решение не является универсальным. Огромное количество дыр находится в прикладных приложениях типа IE. Отрубить дырявый IE от сети брандмауэр сможет. Только тогда легче просто выключить модем и пойти топиться, потому что без Интернета нам уже не жить. В качестве альтернативы предлагается установить заплатку, а лучше сменить IE на Оперу, за всю историю существования которой в ней обнаружилась всего лишь пара дыр, да и то некритичных.

Брандмауэр тут не нужен. То есть очень даже нужен!!! Например, давайте занесем все баннерно-обменные сети в "черный список", чтобы с них ничего не загружалось. Тужа же добавить адреса всех "счетчиков" (тип "рамблеровского"), чтобы никакая информация от нас не отправлялась (хоть никакого секрета она и не представляет, но все-таки, лично мне неприятно быть частью чьей-то статистической базы данных). Только… специально для этой цели существуют "банерорезалки" с уже готовыми "черными листами", причем постоянно пополняемыми. Зачем дрочить вручную, если можно снять телку (причем бесплатно) и она (в смысле баннерорезака) все сделает сама?!

Основное назначение персонального брандмауэра — это разделение интра и итетернет, то есть возведение защитной стены между локальной сетью (как правило, домашней) и враждебным интернетом. Допустим, у нас имеются "расшаренные" файлы/папки и принтеры, доступные без всякий паролей (ведь пароли — это такой геморрой), и чтобы нас не поимели как молодых, брандмауэр позволяет заблокировать всякие попытки обращения к "расшаренным" ресурсам извне, ну или открыть к ним доступ только с определенных адресов (например, из корпоративной сети той организации, где вы работаете). У большинства брандмауэров это делается одним взмахом мыши: просто сбрасываем/устанавливаем галочку напротив пункта "…. shared flies/folders/printers".

Насколько надежна такая защита? Может ли хакер "пробить" брандмауэр?! Независимо от конструктивных особенностей реализации брандмауэра непосредственный обмен данными с закрытым портом "извне" невозможен. И хотя имеется ряд "узких" мест (например, при сильной фрагментации TCP-пакета, порт назначения не вмещается в TCP-заголовок и некоторые брандмауэры спокойно пропускают такие пакеты), мы можем не заморачиваясь и не выседая на

измену чувствовать себя как у Христа за пазухой, ибо вероятностью быть атакованным через скаченный варез несравненно выше.

Еще брандмауэр может (и должен) следить за сетевой активностью _честных_ приложений, показывая кто из них ломиться в сеть, на какой порт и по каким адресам. Например, если мы запускаем Горящего Лиса и он ломится на Home Page, ранее прописанную нами, то это — нормально. Если же Лис лезет на fxfeeds.mozilla.org, то это тоже нормально, только очень сильно подозрительно, но в принципе, программа подобного уровня вправе обращаться к своему сайту и никакого криминала здесь нет. А вот если игра типа "Тетриса" пытается открыть какой-то порт (например, порт 666), то с вероятностью близкой к единице в ней запрятана закладка и от такой программы можно ожидать всего, чего угодно, так что лучше стереть ее на хрен или ограничиться тем, что на вопрос брандмауэра ответить "нет".

Вообще говоря, пробить брандмауэр "изнутри" очень просто. То есть, зловредная программа имеет в своем арсенале массу способов как установить канал связи с удаленным узлом и брандмауэр ей не помеха. Тем не менее, основная масса малвари написана пионерами, которые ни хрена не шарят в теме и потому попытки открытия back-door портов (через которые хакеры и рулят захаченными компьютерами) отлавливаются брандмауэрами со свистом навозной пули. Более грамотная малварь внедряется в процессы доверенных приложений (например, в IE, Горящего Лиса, Outlook Express, The Bat, etc), осуществляя обмен данными от их имени. Большинство брандмауэров отлавливают факт внедрения (хотя и не обязаны это делать), однако, если малварь _уже_ находится на компьютере, то у нее есть все шансы обломать брандмауэр каким бы крутым он ни был. Впрочем, учитывая качество нынешней малвари, брандмауэры побеждают чаще.

>>> выноска 3

Наличие персонального брандмауэра не освобождает от необходимости установки заплаток и _в_ _общем_ _случае_ не останавливает малварь, лезущую в не залатанные дыры.

приступаем к настройке брандмауэра

Курить надо. Документацию. Пыхать потом будем. В смысле устанавливать. Брандмауэр. И хотя мне еще не встречалась документация которая торкает, курить все равно надо. Конфигурировать брандмауэр методом тыка — занятие для экстремалов. Мыщъх бы и рад дать пошаговое руководство по настройке _всех_ брандмауэров, но не может этого сделать, поскольку брандмауэров слишком много, но принципы их конфигурации довольно схожи и все различия упираются в интерфейс.

Начнем с портов. Вернее сказать, вернемся к нем. Ох уж эти порты… развелось их тут. Некоторые руководства предлагают сразу и навсегда закрыть порты, используемые троянскими лошадьми, устанавливающими back-door'ы. Списки таких портов выглядят довольно внушительно. Троянцев сейчас много и все они используют различные порты. Ну, положим, закроем мы их. Что это нам даст?! А ничего! Эти порты и так закрыты по умолчанию. Проникнуть сквозь них малварь не сможет и чтобы установить back-door ей придется либо прикинуться полезным варезом, который установит на компьютер сам пользователь, либо же заюзать какую-нибудь не залатанную дыру. Естественно, после того как малварь обоснуется на компьютере, она попытается открыть порт, ожидая поступления дальнейших инструкций от хакера. И, если этот порт закрыт на брандмауэре, малварь обломается, а брандмауэр выдаст предупреждение. Дескать, вот такая тут зараза…

Интернет буквально кишит подобными статьями, от непроходимой тупости которых мыщъх уже устал. Короче. Внятно, доступно и на пальцах. Мальварь уже давно не использует фиксированные порты, а выбирает их случайным (или псевдослучайным образом). Это раз. А теперь два: при установке _любого_ TCP/IP соединения на самом деле используется не один, а _два_ порта: заранее известный фиксированный порт удаленного узла (например, в случае WWW это порт 80), и локальный порт, автоматически открываемой операционной системой на нашей машине и выбираемый произвольным образом (естественно, из числа свободных). Существует вероятность (причем, весьма значительная), что при установке легального TCP/IP соединения нормальной программой, операционная система назначит "троянский" локальный порт, который закрыт брандмауэром!!! Это означает, что: а) соединение не будет установлено; б) брандмауэр поднимет визг, а пользователь, соответственно, хватаясь за сердце, начнет искать несуществующего трояна, скачивая самые последние версии антивирусов, но так и не найдет его, поскольку… тревога оказалась ложной.

По той же причине нельзя закрыть _все_ неиспользуемые порты, как советуют некоторые авторы, т.к. при этом мы не сможем вообще установить ни одного TCP/IP соединения!!!

Так какие же порты нужно закрывать?! Ответ: если (допустим) у вас домашняя локальная сеть и proxy-сервер на 8080 порте, через который выходят в Интернет остальные домочадцы, то точно таким же образом через него могут выходить в сеть и все остальные обитатели Интернет. Зачем? Ну мало ли… Даже если proxy не анонимный (то есть не подходит для атак от чужого имени), то внутрисетевой трафик у большинства провайдеров обычно значительно дешевле или вовсе бесплатен. Вот юные хакеры и рыщут в поисках домашних proxy. Вообще-то, большинство proxy позволяет установить пароль на вход, но… далеко не все программы, работающие через proxy поддерживают такой режим.

ОК. Другой ход. В настойках proxy должен быть список разрешенных интерфейсов, с которыми он может работать. Обмен пакетами со всеми остальными интерфейсами запрещен. Интерфейс в данном случае это (в грубом приближении) идентификатор сетевого устройства. Сетевая карта, модем — все они имеют свои интерфейсы. Короче, выбираем интерфейс сетевой карты, подключенной к домашней локальной сети и запрещаем все остальные. Красота! Ну да… красота. Местами. А местами безобразие сплошное. Если DSL модем имеет Ethernet порт, воткнутый в свич (вполне типичная конфигурация домашней локальной сети), то у нас имеется всего один интерфейс как для интернета, так и для локальной сети.

Или вот, мыщъх использует Etlin HTTP Proxy, позволяющий выбрать всего один интерфейс для работы. А мыщъх'у необходимо выбрать два: интерфейс локальной домашней сети и интерфейс виртуальной сети VM Ware, которой тоже нужен доступ в Интернет. Можно, конечно, выбрать другой Proxy сервер, но проще в настройках брандмауэра указать список IP адресов домашней локальной сети (и виртуальной сети), с которых разрешен доступ к порту Proxy-сервера (в данном случае это 8080 порт). Если же у вас нет proxy-сервера, то просто не заморачивайтесь с этим вопросом (примечание: модемы с Ethernet-портами обычно имеют встроенный брандмауэр, позволяющий разграничить доступ к локальной сети — по поводу его настройки курите прилагающиеся к модему мануалы).

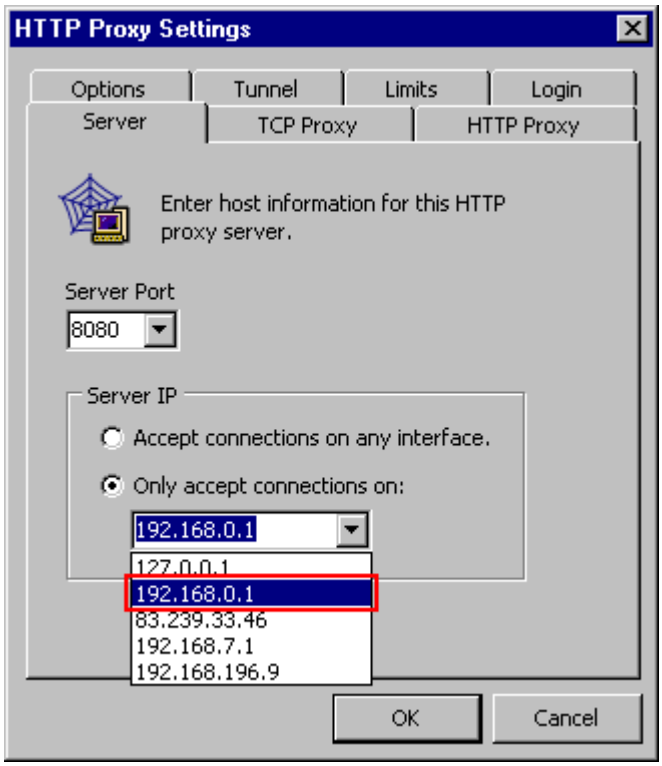

Рисунок 7 proxy-сервер "Etlin HTTP Proxy" позволяет выбрать интерфейс с которым он будет работать, но только один…

Теперь перейдем к зашаренным ресурсам, про которые мы уже говори. Брандмауэры в своей массе не блокируют к ним доступ из Интернета по умолчанию, "благодаря" чему атаки следуют ударными темпами и компьютеры ложатся стройными могильными рядами. Лучше

вообще не иметь никаких расшаренных ресурсов, используя персональные ftp сервера, которые как раз и предназначены для обмена файлами, но… объяснить среднестатистическому пользователю типа "жена" что такое ftp намного сложнее, чем найти копию Windows без багов. Так что приходится шарить. Ну и шарьте себе на здоровье, только в настройках брандмауэра найдите пункт, касающийся доступа шары из интернета и распорядитесь с ним по обстоятельствам.

И последнее (но самое важное). Практически все брандмауэры поддерживают список "доверенных приложений", а при выводе запроса на подтверждение имеют галочку "не показывать это сообщение в дальнейшем". Так вот! Настоятельно рекомендуется сию галочку не трогать!!! Конечно, частые запросы на подтверждения очень аноят, но зато позволяют держать ситуацию под контролем. Тоже самое относиться и к списку доверенных приложений. Допустим, заносим туда IE, чтобы брандмауэр не задалбливал нас дурацкими вопросами. Теперь запускаем какое-нибудь приложение, которое неожиданно вызывает браузер по умолчанию (в данном случае IE) и передает через него некоторую информацию на удаленный узел, например, серийный номер для подтверждения его (не)валидности. А вот если при _каждом_ запуске IE будет выпрыгивать запрос от брандмауэра, этот фокус уже не пройдет!!!

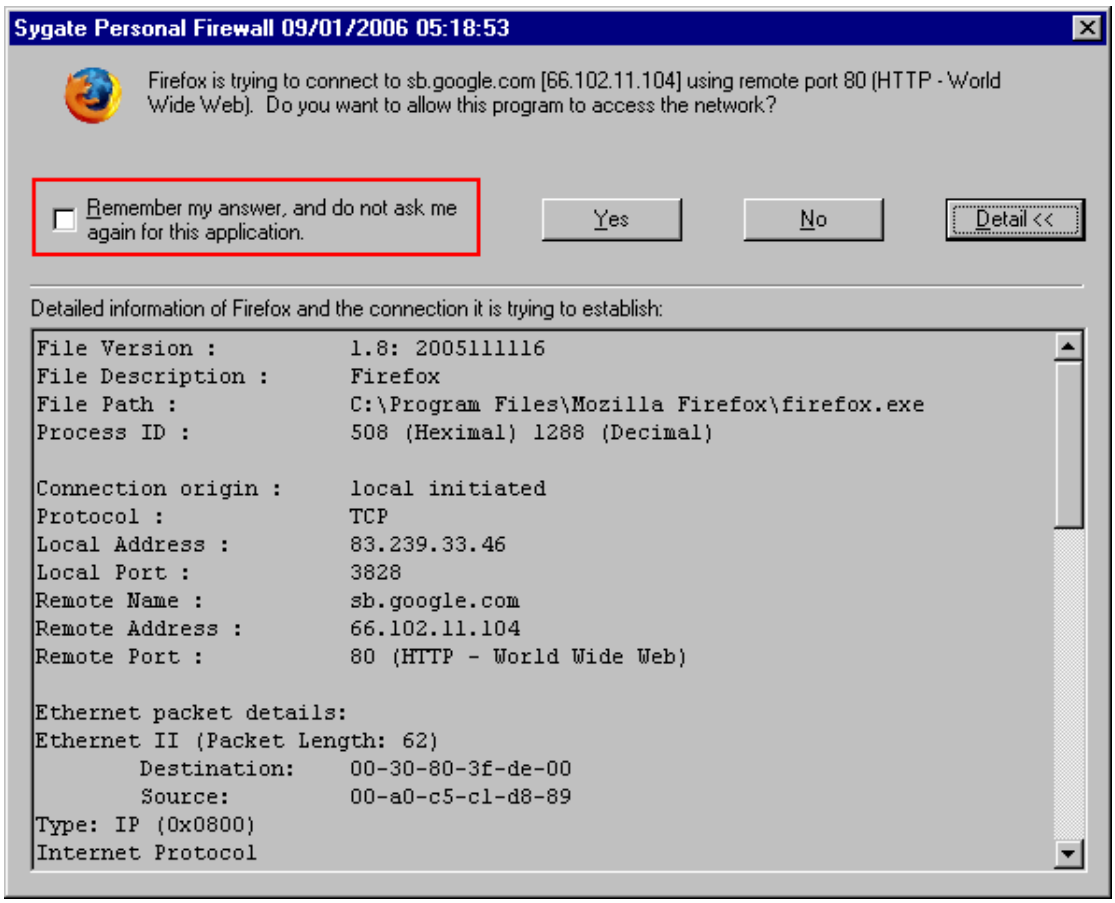

Рисунок 8 галочка, предлагающая не выводить это сообщение в дальнейшем (чтобы не надоедать), к услугам которой лучше не прибегать

Попутно: запретите своему компьютеру посылать эхо ответы (опция ICMP ECHO в брандмауэре), чтобы неприятели не запинговали вас до смерти, за короткое время сгенерировав до фига мегабайт трафика, не только затормозив работу компьютера, но еще и посадив на бабки, ведь трафик — он на большинстве тарифов денег стоит!

заключение

Брандмауэр (даже персональный) это все-таки не IE и даже не Горящий Лис, а программный пакет совсем другого порядка, требующий знания и _понимания_ протоколов, на которых держится Интернет. В противном случае, навряд ли можно ожидать осмысленного ответа на вопрос, заданный пользователю брандмауэром. Человеческий фактор — самое слабое

звено и никакими техническими ухищрениями эту проблему не исправишь. Банальность, конечно, но с каждым годом она все обостряется и обостряется.