проблемы пакетных фильтров

крис касперски

Пакетные фильтры относятся к самому быстрому типу брандмауэров (программные прокси они же брандмауэры уровня приложений работают на порядок тормознее, поскольку вынуждены полностью пересобирать TCP-пакеты, что значительно увеличивает латентность; с домашними и офисными локалками они еще справляются, но на высокоскоростных каналах оказываются категорически неприменимы).

Тем не менее и у пакетных фильтров тоже есть проблемы. Большинство персональных брандмауэров, посторонних по этой схеме, серьезно тормозят даже на модемных соединениях, не говоря уже о DSL-подключении. На простом веб-серфинге задержка практически не заметна, но при активной работе с несколькими десятками TCP/IP-соединений она может "отъедать" чуть ли не половину пропускной способности нашего канала, а это уже нехорошо. Конечно, разработчики брандмауэров могут возразить, что, мол на персональных компьютерах такое количество соединений никому не нужно, но это будет наглая ложь. Осел требует от трехсот до пятисот соединений, тоже самое относится к другим файлобменным клиентам. К тому же, при организации локальной сети на компьютер, смотрящий в Интернет, ложится довольно таки приличная нагрузка.

Рисунок 1 любой брандмауэр это по сути стена

Для нормальной фильтрации трафика, требуется колоссальное количество памяти и нехилые процессорные ресурсы. Все дело в том, что данные передаются по сети не сплошным потоком, а расщепляются на многоуровневую иерархию пакетов. В грубом приближении ее можно записать так: Ethernet → IP → TCP/UDP. Один TCP/UDP пакет разбивается на большое количество IP пакетов, которые "вываливаются " в сеть настоящей "горстью риса", то есть в разупорядоченном состоянии. Порядок доставки IP-пакетов может не совпадать с порядком их "нарезки" в TCP-пакете, причем, некоторые IP-пакеты могут теряться и тогда отправляющая сторона передает их вновь и вновь… Да и сама установка TCP-соединения представляет собой многостадийную операцию. А это значит, что пакетный фильтр, работающий на IP уровне, будет просто нефункционален! Достаточно сказать, что в IP протоколе нет понятия "порта" и

"закрыть" порт с IP уровня невозможно. В несколько упрощенной схеме это можно изобразить так: отправитель посылает получателю книгу, разрезанную на мелкие куски, произвольным образом перемешанные между собой, а получатель тем или иным образом собирает этот puzzle в исходный вид. Допустим, между ними сидит злой цензор, который внимательно просматривает каждый кусочек на предмет "политкорректности" и либо уничтожает его, либо передает "наверх". Очевидно, если цензор (он же брандмауэр) не будет выполнять полной сборки TCP-пакетов, он не заметит ничего подозрительно. Теоретически, можно посадить брандмауэр на TCP/UDP уровень и фильтровать уже собранные пакеты, но… тогда хакер сможет передать "сырой" IP пакет и брандмауэр будет в шляпе.

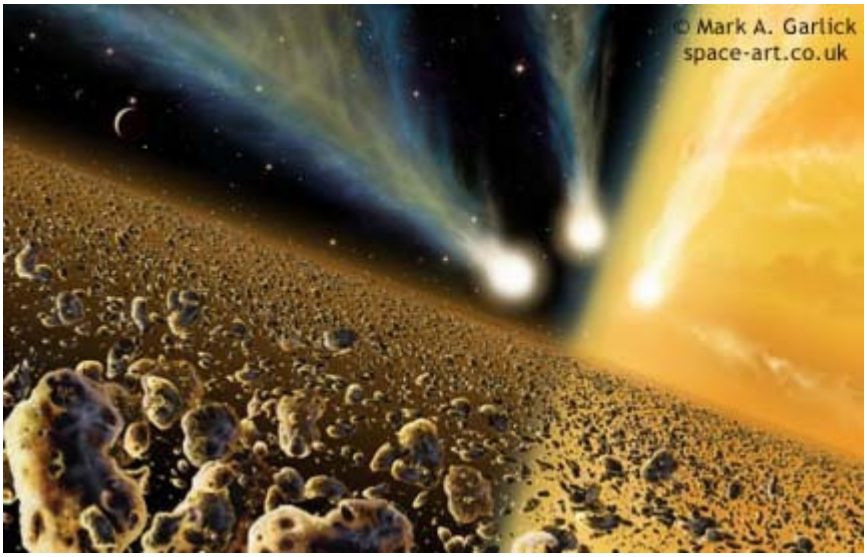

Рисунок 2 хакеры атакуют

Максимальная защита обеспечивается при фильтрации пакетов на Ethernet-уровне. При условии, что брандмауэр сконструирован без ошибок, никакой хакер не сможет его обойти. Большинство разработчиков именно так и поступают. Типичный персональный брандмауэр встраивается в "разрыв" между драйвером сетевой платы и TCPIP.SYS-драйвером, который, как и следует из его названия, реализует протокол TCP/IP. При этом, брандмауэр должен самостоятельно собирать TCP-пакеты, фактически полностью повторяя собой TCPIP.SYS, реализация которого является весьма нетривиальной задачей, но это еще цветочки. Попробуем рассчитать пиковую потребность в оперативной памяти. Возьмем гигабитный Ethernet (а, что? имеем же мы на это право!), тайм-аут в 30 сек. и 100 соединений. Довольно мягкие условия, не правда ли? В грубом приближении получаем: 1.073.741.824 * 30 * 100 / 8 = 402.653.184.000 байт или 375 Гбайт. Какая там оперативная память! Даже винчестеров такого объема в персональных компьютерах еще не встречается! На самом деле, это проблема не брандмауэра, а самого протокола TCP/IP (именно на этом и основана известная SYN-атака), но брандмауэр удваивает потребности TCP/IP-стека в оперативной памяти, что не есть хорошо. Но это еще полбеды! Хуже всего, что брандмауэр не может отдавать IP-пакеты "наверх" до тех пор, пока он не соберет весь TCP-сегмент целиком и не проверит его на "вшивость". Пакетный фильтр вынужден накапливать поступающие данные в своих собственных очередях и либо "прибивать" неправильный TCP, либо отдавать накопленные IP всем скопом. А вот от этого операционной системы может очень сильно поплохеть. Процессор будет просто не успевать обрабатывать такую ораву и возникнут неизбежные тормоза. К тому же, все настойки операционной системы, касающиеся TCP/IP окажутся бесполезны, поскольку такой брандмауэр фактически уподобляется прокси-северу, отрезающую ее от внешнего мира.

В нормальных операционных системах (LINUX, FreeBSD), пакетный фильтр изначально встроен в TCPIP-драйвер и там таких проблем просто не возникает. В Windows, пакетный фильтр впервые появился в 2000 SP2, который был существенно доработан в XP, но до звания брандмауэра ему еще далеко и его очень легко обойти.

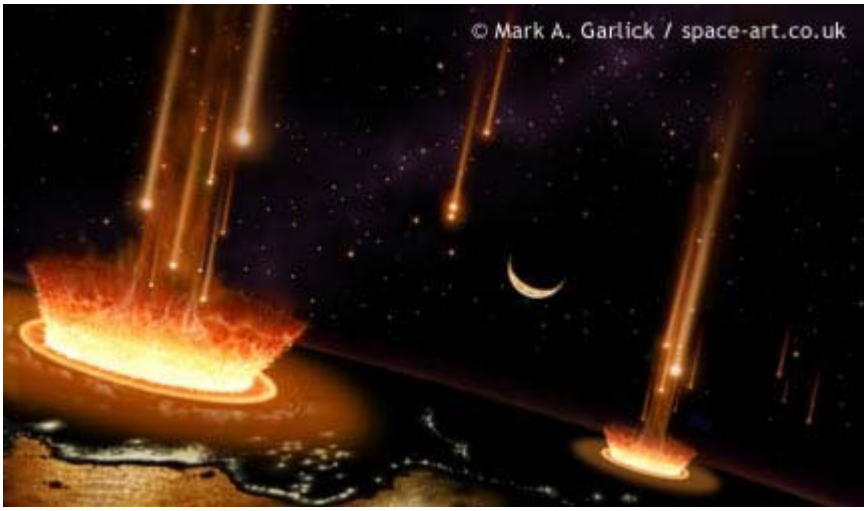

Рисунок 3 хакеры продолжают атаковать

Короче, ситуация прямо как у Ханлайна: "…дочитав инструкцию до конца, я удивился, как человек ухитряется выжить, да еще в скафандре". В общем, мясокомбинат полный. Как же со всем этим справляются персональные брандмауэры? Ведь они же работают! Ну… или делают вид, что работают. Да никак не справляются! Они работаю исключительно на IP-уровне, эмулируя лишь несколько важнейших функций TCP. Сборка пакетов и проверка контрольной суммы в этот перечень, естественно, не входит. При условии, что заголовок TCP пакета полностью помещается в IP-пакет, брандмауэр может определить порт назначения и без сборки, что позволяет ему "закрывать" охраняемые порты, впрочем, эту защиту очень легко обойти, причем как извне так и изнутри (подробности — в статье "обход брандмауэров снаружи и изнутри").

Персональные брандмауэры обеспечивают лишь минимальную защиту от "пионеров", при этом довольно существенно тормозят соединение, поскольку просмотр заголовков пакетов занимает какое-то время. Теоретически, накладные расходы легко свести к нулю. Для этого даже необязательно программировать на ассемблере, хороший пакетный фильтр можно написать и на Си, если, конечно, подойти к делу с головой, однако, достойных продуктов на рынке пока что не наблюдается.

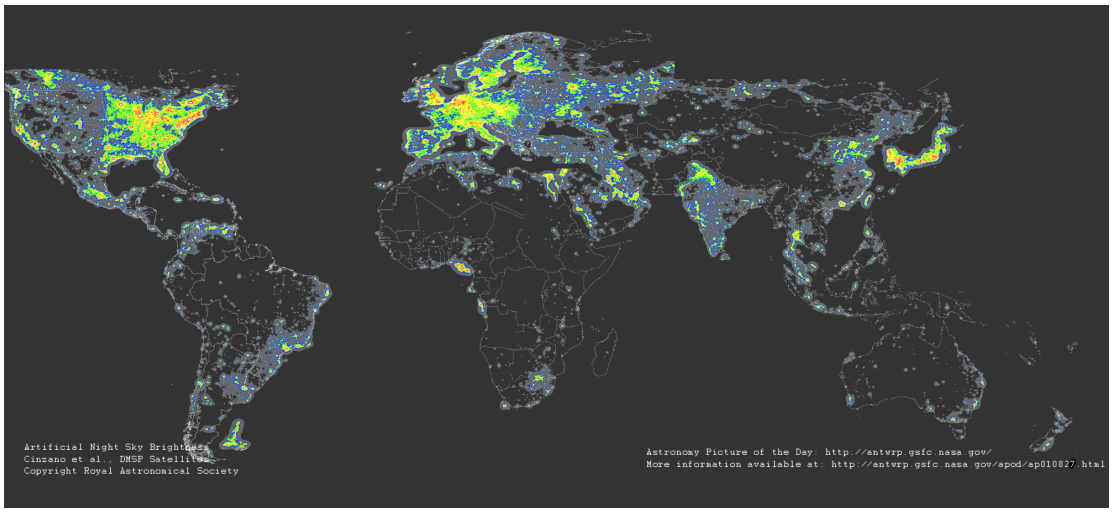

Рисунок 4 плотность брандмауэров на душу населения в разных регионах земли по данным НАСА. шутка. на самом деле, это ночная освещенность городов, но с количеством брандмауэров она довольно таки неплохо корреллирует

Некоторые брандмауэры не просто фильтруют пакеты по критериям портов или IP-адресов, но еще и проверяют их на соответствие стандартам RFC или анализируют содержимое на предмет наличия червей или использования тех или иных уязвимостей клиентских приложений. Для неискушенного пользователя звучит заманчиво, но в действительности все это

полная чушь. Начнем со стандартов. Их много хороших и разных, а разночтений в стандартах еще больше. Поэтому, нельзя с уверенностью сказать, соответствует ли конкретно взятый пакет стандарту или нет. Большинство атак реализуется вполне стандартными TCP/IP пакетами, и задача брандмауэра состоит не в соблюдении стандарта, а его нарушении. Например, при уничтожении пакета с истекшим сроком жизни, каждый узел обязан отправить специальное уведомление, дескать ваша депеша сдохла в дороге, так что не взыщите. Утилита trace route именно так и работает! Она отправляет множество пакетов с различным сроком жизни, а потом собирает уведомления, поступающие ото всех транзитных узлов, что позволяет реконструировать топологию сети. Чтобы воспрепятствовать этому, брандмауэр должен нарушить стандарт и задержать уведомление о смерти!

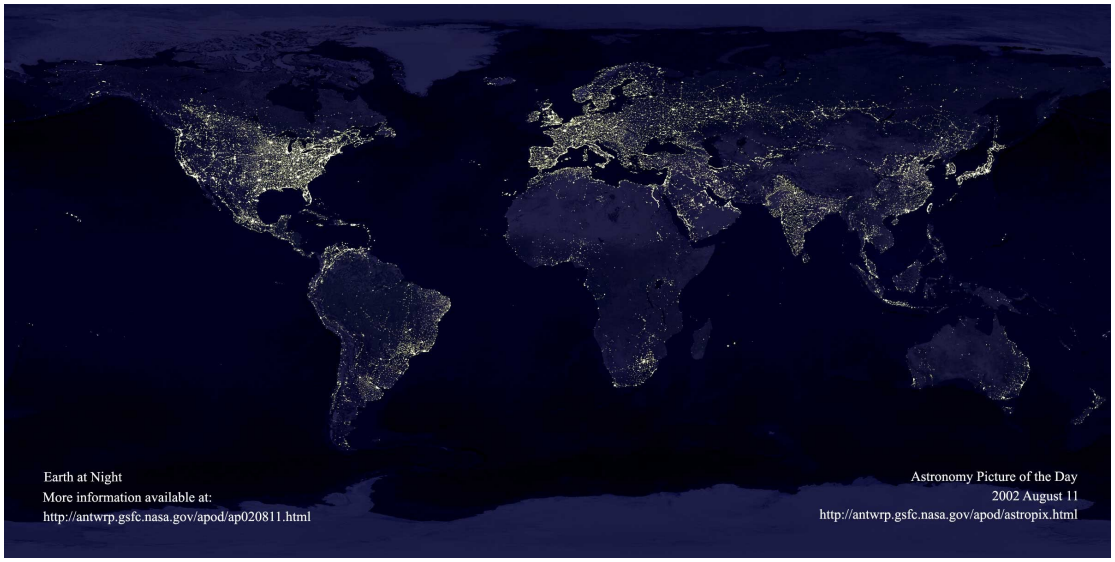

Рисунок 5 приблизительная структура сети Интернет (вид из космоса)

Теперь перейдем к червям и уязвимостям. Очевидно, что предвидеть сигнатуры еще неизвестных червей никакой брандмауэр не в силах, и поэтому его необходимо периодически обновлять. А раз так — то не лучше ли установить заплатку на программное обеспечение и заткнуть дыру, через которую лезут черви? Пользователь либо апдейтится, либо нет. Если он апдейтится, то такой брандмауэр ему не нужен, а если не апдейстится — тут уже ничто не поможет. Короче, получается замкнутый круг.

К тому же, проверку содержимого пакетов невозможно осуществить на IP-уровне и брандмауэру все-таки придется поднапрячься и собрать весь TCP, про сложность которого мы уже говорили. Самое сканирование так же потребует некоторого времени и процессорных ресурсов (особенно, если червь упакован полиморфным упаковщиком), а про эвристические анализаторы мы вообще молчим. На модемном соединении проверять содержимое пакетов еще реально, но на быстрых каналах — это труба.

Сказанное вовсе не повод для отказа от брандмауэров. Они безусловно нужны, но не стоит поручать им те функции, с которыми они справится не в состоянии. Ведь никто же не стремится превратить подводную лодку в вертолет. И даже если такой агрегат все-таки будет создан, его технические характеристики будут явно не на высоте. Ведь подлодка требует большой плотности и прочности (иначе как прикажите опускаться на глубину), а вертолет должен максимально облегчить свой вес. Вот так и брандмауэры. Уязвимые порты затыкаются заплатками. Пакетный фильтр скрывает приватные узлы локальной сети от "внешнего мира". Антивирусы ловят агрессивно настроенные программы. Каждый занят своим делом и никто не пытается залезть в одну штанину двумя ногами.