Основы работы брандмауэров

Сенченко Т.В. (aka Boffin)
127.0.0.1@online.com.ua
icq: 865491

Начну с небольшого вступления и расскажу, что вынудило меня собрать достаточно исчерпывающую информацию о брандмауэрах и написать эту статью.
Я уверенна, что многие из вас слышали о таком программном продукте, как Tiny Personal Firewall Engine (у меня одна из первых его версий) для платформ *Win all.
Краткая предыстория… Tiny появился у меня лет 6 назад. В каком году он написан и кто его непосредственный автор, я не знаю - вся информация вырезана. Интерфейс очень простой, имеет минимальный набор функций.
Этот PFW я неоднократно тестировала параллельно с другими популярными коммерческими продуктами. Тестирование проводилось различными средствами и методами, в частности, как мной лично, так и другими сторонами по моей просьбе.
Проводилось также тестирование с использованием бесплатных online-служб, например:
http://www.grc.com/x/IPAgentDiscontinued.htm **(ссылка " ShieldsUP! vulnerability profiling tests")**
// Тест показал 0 открытых портов.
http://scan.sygatetech.com/
https://grc.com/x/ne.dll?bh0bkyd2
http://security.symantec.com/ssc/
http://www.hackerwatch.org/probe/
http://www.pcflank.com/about.htm
Я также протестировала продукты **PC Firewall** компании *ConSeal*, **Personal Firewall** производства *McAfee.com*, **BlackICE Defender**, выпускаемый *Network ICE*, **Secure Desktop** фирмы Sybergen, **Norton Personal Firewall 2000** от *Symantec* и **ZoneAlarm**, разработанный *Zone Labs*. Все эти продукты можно отнести к трем категориям: предназначенные для корпоративных сетей с централизованным управлением; автономные решения для домашнего офиса или небольшой компании; предназначенные для системного администратора (позволяют оперативно и скрупулезно контролировать все аспекты сетевой работы).
Если говорить отдельно о **Tiny Personal Firewall**, то он на 100% показал себя как надежное и устойчивое средство для защиты персонального компьютера (и, как вариант сервера на платформе Windows), потребляющее минимальное количество системных ресурсов. Уже намного позже, я пробовала последние его версии (коммерческие), но увы, мое мнение о них осталось более негативным, чем я предполагала. Хотя, я и сейчас консервативно отдаю предпочтение продукту именно этой компании, если рассматривать его как сетевую защиту для платформ Windows.
Далее события начали развиваться таким образом, что пришло время для подведения итогов. К тому моменту было уже собрано достаточно информации, проведено немало тестов и мое сознание требовало конечного результата, который будет высказан и вынесен на всеобщее обсуждение. Таким образом, появилось желание (возможно, кто-то подкинул идею) написать статью о технологии брандмауэров. Статья не может претендовать на полноту обзора темы, она представляет собой лишь краткий набор ответов на часто задаваемые вопросы (FAQ). Некоторые выдержки и примеры я брала из разных источников, поэтому я буду указывать авторов этих материалов следующей аббревиатурой: ***источник: «Название_книги» (Автор)**

Что такое брандмауэр?

Брандмауэр (*межсетевой экран*) - это система или группа систем, реализующих правила управления обменом данными (доступом) между двумя или несколькими сетями. Фактические средства, с помощью которых это достигается, весьма различны, но в принципе брандмауэр можно рассматривать как пару механизмов: один для блокирования передачи информации, а другой - для пропуска информации. Главное, что нужно знать о брандмауэрах - это то, что они реализуют

правила управления доступом. Если не вполне понятно, какого рода доступ необходимо обеспечить или запретить, тут брандмауэр вам не поможет. Также важно знать, что конфигурация брандмауэра, определяет правила для всех систем, которые он защищает. Поэтому на администраторов брандмауэров, управляющих доступом к большому количеству хостов, возлагается большая ответственность.

В отличие от брандмауэров, реализованных на специализированных аппаратных платформах, персональные (PFW) представляют собой относительно дешевое ПО, которое инсталлируется непосредственно на каждый защищаемый ПК. Такие брандмауэры осуществляют контроль за сетевыми устройствами и выполняют те же основные функции, что и корпоративные брандмауэры: обнаружение попыток вторжения, контроль доступа, выполнение правил безопасности, регистрация событий. Обычно персональный брандмауэр фильтрует весь сетевой трафик, разрешая только санкционированные соединения.

Зачем нужен брандмауэр?

Многие организации подключают свои локальные сети к Интернету. А поскольку сеть Интернет в целом не является безопасной и, как утверждает статистика, незащищенная система в открытой сети «выживает» не более 20 минут, то машины в этих ЛВС подвержены риску несанкционированного использования и внешних атак. Брандмауэр - это средство защиты, которое можно использовать для управления обменом данными между надежной сетью и остальным миром (Интернет).
Основная функция брандмауэра - централизация управления доступом. Если удаленные пользователи могут получить доступ к внутренним сетям в обход брандмауэра, его эффективность близка к нулю. Например, если человек, находящийся в командировке, имеет модем, присоединенный к его ПК в офисе, он может дозвониться до своего компьютера из любого места, а так как этот ПК также находится во внутренней защищенной сети, то атакующий, имеющий возможность установить коммутируемое соединение с этой машиной, может обойти защиту брандмауэра. Если пользователь имеет подключение к Интернету у какого-нибудь провайдера, и часто соединяется с Интернетом со своей рабочей машины с помощью модема, то он устанавливает небезопасное соединение с Интернетом, в обход защиты брандмауэра.

Брандмауэры обеспечивают несколько типов защиты:

- Они могут блокировать нежелательный трафик;
- Они могут направлять входной трафик только к надежным внутренним системам;
- Они могут скрыть уязвимые системы, которые нельзя обезопасить от атак из Интернета другим способом;
- Они могут протоколировать трафик входящий во внутреннюю сеть и выходящий из нее;
- Они могут скрывать информацию (такую, как имена систем, топологию сети, типы сетевых устройств и внутренние идентификаторы пользователей) о внутренней сети от пользователей Интернета;
- Они могут обеспечить более надежную аутентификацию, чем та, которую предоставляют стандартные приложения.

Совокупность большинства мер, рекомендованных для обеспечения безопасности сети, позволяет затормозить действия решительного хакера примерно за 5 сек. За это время он сумеет найти «дыру» в защите и атаковать вас. При наличии в корпоративной сети прямого выхода в Интернет (кабельный модем, DSL, ISDN или линия T1) и отсутствии мощного брандмауэра дверь для злоумышленника открыта. Но даже если вы отгорожены от Всемирной паутины брандмауэром, помните, что около половины всех неприятностей причиняют организациям их недовольные или болезненно любопытные сотрудники.

От чего не может защитить брандмауэр?

Брандмауэр не может защитить от атак, которые выполняются не через него. Многие подключенные к сети Internet корпорации очень опасаются утечки конфиденциальных данных через этот канал. Руководство многих организаций, напуганное подключением к Internet, не вполне представляет, как защищать доступ к модемам по коммутируемым линиям. **Чтобы брандмауэр выполнял свои функции, он должен быть часть согласованной общей системы защиты в организации.** Правила брандмауэра должны быть реалистичными и отражать уровень защиты всей сети в целом.

Брандмауэры не могут защитить от передачи по большинству прикладных протоколов команд подставным ("троянским") или плохо написанным клиентским программам. Брандмауэр -- не панацея и его наличие не отменяет необходимости контролировать программное обеспечение в локальных сетях или обеспечивать защиту хостов и серверов. Передать "плохие" вещи по протоколам HTTP, SMTP и другим очень просто.

Какой брандмауэр выбрать?

Какой брандмауэр вы в конечном итоге выберете, зависит главным образом от принятой в вашей организации политики безопасности. Вообще говоря, чем жестче правила безопасности, тем больше функций контроля брандмауэр должен выполнять.

Проблема выбора брандмауэра в том, что различия между продуктами, производителями и технологиями усложняется. Несколько лет назад, когда брандмауэры производили не более десятка компаний, выбор был намного проще; но теперь, когда многие десятки поставщиков предлагают брандмауэры того или иного типа, путаница среди профессионалов и экспертов в области сетей и защиты вполне объяснима.

Брандмауэры можно разделить на три основные категории: фильтры пакетов, механизмы контекстной проверки и шлюзы уровня приложений (известные так же, как посредники, или proxy). При выборе важно помнить, что, хотя все брандмауэры выполняют по сути одни и те же основные функции, механизмы их выполнения принципиально отличны друг от друга. Но чтобы понять эти различия, вы должны вначале познакомиться с базовыми технологиями фильтрации пакетов и контекстной проверки.

Хороший брандмауэр может обнаружить, что его порты сканируются, зарегистрировать это событие и уведомить вас, если ему это поручено. Например, брандмауэр ZoneAlarm может быть настроен на вывод всплывающего окна с предупреждением каждый раз, когда ваш компьютер сканируется. В этом случае, если ваш жесткий диск внезапно начал вращаться или необъяснимо снизилась скорость работы, вы можете заблокировать нападение с помощью временного прерывания соединения. Брандмауэр BlacklCE Defender идет еще дальше и отслеживает IP-адрес раздражающего компьютера, с которого идет сканирование, а затем докладывает о нем.
Однако не всегда сканирование - это нападение. Например, кто-то, возможно, случайно ввел неправильный IP-адрес при попытке соединиться с HTTP-сервером или открыть сеанс связи с другом через NetMeeting. Также возможно, что ваш провайдер мог запустить какое-либо тестирование. Другая ложная тревога, как известно, возникает от основанных на использовании технологий Интернета телевизионных услуг, которые иногда случайно соединяются с неправильными IP-адресами.

Существует несколько различных реализаций брандмауэров:

Шлюзы с фильтрацией пакетов

Брандмауэры с фильтрацией пакетов используют маршрутизаторы с правилами фильтрации пакетов для предоставления или запрещения доступа на основе адреса отправителя, адреса получателя и порта. Они обеспечивают минимальную безопасность за низкую цену, и это может оказаться приемлемым для среды с низким риском. Они являются быстрыми, гибкими и прозрачными. Правила фильтрации часто нелегко администрировать, но имеется ряд средств для упрощения задачи создания и поддержки набора правил.

Прикладные шлюзы

Прикладной шлюз использует программы (называемые прокси-серверами), запускаемые на брандмауэре. Эти прокси-серверы принимают запросы извне, анализируют их и передают безопасные запросы внутренним хостам, которые предоставляют соответствующие услуги. Прикладные шлюзы могут обеспечивать такие функции, как аутентификация пользователей и протоколирование их действий.

Брандмауэры прикладного уровня должны настраиваться так, чтобы весь выходящий трафик казался исходящим от брандмауэра (то есть, чтобы только брандмауэр был виден внешним сетям). Таким образом будет запрещен прямой доступ во внутренние сети. Все входящие запросы для различных сетевых служб, таких как Telnet, FTP, SSH, RLOGIN, и т.д., независимо от того, какой внутренний хост запрашивается, должны проходить через соответствующий прокси-сервер на брандмауэре.

Гибридные или сложные шлюзы

Гибридные шлюзы объединяют в себе два описанных выше типа брандмауэра и реализуют их последовательно, а не параллельно. Если они соединены последовательно, то общий уровень безопасности повышается, однако при параллельном использовании общий уровень безопасности системы будет соответствовать наименее безопасному из используемых методов. В средах со средним и высоким риском, гибридные шлюзы могут оказаться идеальной реализацией брандмауэра.

Зачастую межсетевые экраны реализуются программными средствами на базе ПК общего назначения. Они устанавливаются на рабочие станции и работают под управлением большинства операционных систем. Автономные межсетевые экраны защищают только одно рабочее место, поэтому их администрированием занимается владелец этого компьютера.

Специализированные межсетевые экраны (их иногда называют аппаратными брандмауэрами) — это программно-аппаратные комплексы, работающие в точке подключения к Internet. Они выполняют функции маршрутизатора, коммутатора и межсетевого экрана. Как правило, на них не требуется устанавливать дополнительное программное обеспечение. Большинство межсетевых экранов данного типа может защищать до 250 хостов, поэтому они часто используются предприятиями для защиты соединений с небольшими удаленными офисами. Владелец такого брандмауэра может сам заниматься его администрированием, но может и доверить эту работу независимой организации, которая будет выполнять администрирование удаленно.

Межсетевые экраны на базе агентов — это программные решения, в основном подобные автономным экранам, за тем исключением, что набор правил обеспечения безопасности для них задается центральным сервером, как правило, установленным в корпоративной сети. Межсетевые экраны на базе агентов выполняют эти правила на хосте, на котором работает удаленный агент.

Какие брандмауэры лучше использовать для платформ Windows?

Для оценки перечисленных ниже персональных межсетевых экранов я установила каждый программный продукт на ПК с последней версией операционной системы, которую он поддерживает. Эти компьютеры с установленными брандмауэрами я подключила к небольшой локальной сети и настроила так, чтобы они обеспечивали ее защиту. Примеры данных межсетевых

экранов не являются показателями качества и не служат каким-либо рекламным целям. Были взяты программы, которые являлись популярными на тот момент (2001-2003 гг.)

Я определяла возможности каждого межсетевого экрана путем выполнения на защищенном хосте стандартных приложений, таких, как браузеры Web и клиенты электронной почты. Кроме того, при помощи имевшихся в моем распоряжении сигнатур атак я имитировала сканирование как портов, так и служб, а также атаку типа “отказ в обслуживании” (Denial of Service, DoS) на защищаемый хост. Таким образом, мне удалось оценить уровень защиты, обеспечиваемой каждым экраном, качество ведения системного журнала и удобство процедуры уведомлений.

Список функций межсетевого экрана Personal Firewall компании McAfee:

Он может запрашивать введение пароля для изменения параметров конфигурации и обеспечивать различные уровни защиты для различных интерфейсов.

Personal Firewall: может выполнять фильтрацию как исходящего, так и входящего трафика. Без такой фильтрации нельзя эффективно защититься от программ-шпионов и «троянских коней», которые, незаметно проникнув на компьютер, пытаются сообщить внедрившей их стороне сведения о его конфигурации (например, как учетные записи, пароли) и информацию об использовании Web.

Как правило, программы-шпионы не наносят системе вреда, но они часто раскрывают информацию о последних загрузках программ, посещаемых сайтах Web и перечне средств, установленных на данном ПК. Антивирусные комплексы не регистрируют эти программы, поскольку они не считаются вредоносными. Для борьбы с такими шпионскими модулями я бы рекомендовала такие утилиты, как **Ad-Aware** и **Spyware-Cop**.

«Троянские кони» могут пересылать пароли и некоторые файлы. Например, один из «троянских коней», BackDoor, позволяет злоумышленнику взять ПК под свой полный контроль. Способность Personal Firewall фильтровать исходящий трафик лишает такие программы возможности связываться с установившими их злоумышленниками, однако для этого необходимо задать несколько не совсем очевидных правил фильтрации.

Personal Firewall предлагает три готовых набора правил обеспечения безопасности: Block Everything (полная блокировка), Filter Traffic (фильтрация трафика) и Allow Everything (отсутствие блокировки). Режим Block Everything полностью оправдывает свое название: реализовать его можно другим способом и совершенно бесплатно — просто отключившись от Internet. С другой стороны, Allow Everything означает, что защита попросту отсутствует. Таким образом, рассмотрения заслуживает только ружим Filter Traffic, поскольку он предоставляет возможность решать, пропускать или нет трафик для тех или иных портов и тех или иных протоколов.

Межсетевой экран **Norton Internet Security**, раньше носивший имя AtGuard Personal Firewall, способен заблокировать рекламу Web, информацию о версии браузера Internet, а также JavaScript и ActiveX. Кроме того, система может фильтровать входящий и исходящий трафик. При большом разнообразии технологий сценариев Web подчас бывает трудно разобраться, страницы с каким содержанием в действительности представляют собой рекламу. Norton Internet Security дает пользователю возможность отправить нераспознанную рекламу в корзину для мусора, предоставляемую межсетевым экраном. В следующий же раз информация такого типа будет заблокирована.

Параметры конфигурации экрана Norton разделяются на следующие категории: Security (защита), Privacy (конфиденциальность), Parental Control (контроль происхождения) и Advertisement Blocking (блокировка рекламных объявлений). В категории Security поддерживаются функции защиты с использованием правил и возможностью интерактивного обучения, чего нет во многих конкурирующих продуктах. При попытке какого-либо приложения начать взаимодействие через Internet, функция автоматической генерации правил спрашивает у пользователя разрешения на это, после чего межсетевой экран запоминает сделанные пользователем установки и применяет их при последующих повторных запросах доступа. Так как эти правила доступа программ применяются как ко входящему, так и к исходящему трафику, то пользователю придется потрудиться и при первом использовании ответить на все подобные вопросы, иначе не будут работать даже традиционные приложения, такие, как Outlook и IExplorer.

Несмотря на всю свою полезность, функция автоматической генерации правил может стать утомительно навязчивой в ситуации, когда компьютер начинает сканироваться атакующим. Вместо выдачи одного сообщения об атаке (например, «Сканирование портов» или «Атака отказ в обслуживании») Norton будет бомбардировать пользователя многочисленными запросами системы генерации правил о разрешении соединения по каждому сканируемому порту. Решить проблему можно только одним путем — отключить эту функцию, что само по себе не так-то просто, и остаться без механизма автоматизации. Иными словами, редактирование правил фильтрации придется выполнять вручную.

Кроме того, межсетевой экран Norton предлагает выявление вирусов и защиту от них, а также выявление и защиту от многих «троянских коней». Norton Internet Security подойдет тем пользователям, которым нужно единое решение, предоставляющее полный набор возможностей.

Название **BlackICE Defender** (продукт компании Network ICE) имел, вероятно, наибольшую известность на рынке персональных межсетевых экранов в США, по крайней мере, пару лет назад. BlackICE Defender прост в установке и конфигурации, кроме того, он предоставляет широкие возможности выбора политики безопасности, среди которых имеются Trusting (доверительный), Cautious (умеренная предосторожность), Nervous (преувеличенная предосторожность) и Paranoid (мания преследования). Режим по умолчанию, Cautious, хорошо защищает хост, хотя оставляет открытыми для атак некоторые уязвимости с низким уровнем опасности. Два наиболее жестких набора правил, Nervous и Paranoid, оставляют открытым доступ только для ICMP и traceroute, однако, возможно, они делают это для того, чтобы позволить нормально работать системе выявления вторжений.

BlackICE может блокировать злоумышленников, используя их IP-адреса и имена хостов, либо в течение определенного времени, либо неопределенно долго. Defender автоматически выполняет операции обратного отслеживания для определения IP-адреса, имени хоста и даже идентификатора логического входа NetBIOS злоумышленника, если они доступны. Однако средства выявления вторжений иногда некорректно определяют некоторые виды активности в сети, не несущие никакого вреда, квалифицируя их как разновидность атаки. Хочется еще добавить и то, что при попытке отразить атаку, BlackICE иногда отдавал злоумышленнику некий UDP пакет, который может стать небезопасным при определенных ситуациях. Эти выводы я делаю на основании того, что параллельно с Defender тестировался Tiny Personal Firewall, который и заявил об этом.

Наиболее существенным недостатком межсетевого экрана Defender является его неспособность ограничивать исходящий трафик при любых установках правил безопасности. Это означает, что практически невозможно лишить программы-шпионы или «троянских коней» способа сообщать информацию о конфигурации ПК, истории посещений Web-сайтов и даже о последовательности нажатия на клавиши. Видимо, пользователь даже не сможет распознать, что в его системе

разместилась такая программа. В любое время в Сети можно обнаружить не менее десятка «троянских коней», сигнатуры которых еще не занесены в антивирусные реестры. Единственным надежным способом защититься от вредоносного воздействия программ этого типа может служить разрешение исходящего трафика только для известных приложений.

Система **ZoneAlarm** компании Zone Labs является самой простой (IMHO). Ее несложно устанавливать и конфигурировать. Но к серьезным брандмауэрам я бы не стала его относить, скорее к категории «Предупреждение, опасность».

ZoneAlarm поддерживает два интерфейса — один для домашней локальной сети, а другой для соединения с Internet и может фильтровать как входящий, так и исходящий трафик. Для клиентов электронной почты, таких, как Outlook, необходимо вручную указать удаленный почтовый сервер. При выборе соответствующей опции обновление ZoneAlarm может выполняться автоматически. При использовании режима Medium (средний уровень защиты) ZoneAlarm оставляет открытыми шесть уязвимостей, представляющих небольшую опасность. Когда я повысила режим до High (высокий уровень защиты), эти «дыры» исчезли. Но система стала работать существенно медленней.

Какие брандмауэры лучше использовать для платформ *nix?

В большинстве дистрибутивов UNIX есть встроенные брандмауэры. Например для Linux - ipchains, iptables, для FreeBSD - ipwf. По-моему, одним из самых простых и распространенных брандмауэров UNIX является пакет TCP Wrappers. Он читает файлы hosts.deny (запрет) и hosts.allow (разрешение) при попытке доступа к службам, указанным в inetd.conf (если пакет уже установлен, в inetd.conf возникает, например in.telnetd - значит telnet работает под защитой TCP Wrapper). TCP Wrapper поддерживает ведение системного журнала событий (лог). Так же в него входит несколько дополнительных утилит: tcpdchk -проверка конфигурационных файлов, tcpdmatch - проверка правил (например, что произойдет, если что-либо изменить). Но это довольно урезанный брандмауэр, который вряд ли можно рассматривать даже как полнофункциональный пакетный фильтр. Более весомыми утилитами являются iptables и ipwf. IPWF представляет собой "обычный" пакетный фильтр, позволяющий обрабатывать как входящие, так и исходящие пакеты.

Процесс пересылки данных между компьютерами в сети

Взаимодействие через Интернет в конечном счете осуществляется между двумя компьютерами, отправителем и получателем, или, более точно, между сетевой платой на одном компьютере и сетевой платой на другом. Во время сеанса связи, который организуется между двумя компьютерами, они часто меняются ролями. Когда данные посылаются с одного компьютера на другой, они должны пройти по Интернету. Поскольку Интернет - это разнообразие хостов и адресов, данные на самом деле проходят сквозь ряд других компьютеров на пути к указанному удаленному компьютеру. TCP/IP - это набор протоколов, который делает все это возможным. Для того, чтобы компьютеры, находящиеся в Интернете, знали, куда отправить данные, эти данные должны быть соответствующим образом адресованы.
Важно понимать, что когда вы посылаете что-либо, например, электронное письмо, кому-то в сети Интернет, письмо не передается как единый документ. В действительности TCP/IP разбивает его на более управляемые части, называемые пакетами. Отдельные пакеты затем посылаются по Интернету на указанный удаленный компьютер. Не каждый пакет пойдет одним и тем же путем. На самом деле пакеты, составляющие ваше электронное письмо, могут проходить по многим различным маршрутам по дороге к указанному удаленному хосту, где они в конце концов будут получены и вновь собраны стеком TCP/IP. В итоге, письмо поступит в программу работы с электронной почтой получателя для просмотра.
Каждому компьютеру, соединяющемуся с Интернетом, присваивается уникальный IP-адрес. Такой адрес определяет положение исходного компьютера в Интернете. Указание адресов места

отправления и назначения каждого пакета необходимо для осуществления доставки каждого пакета.
Когда прибывает пакет данных, удаленный компьютер внимательно изучает его. Если пакет адресован этому компьютеру, он принимается и обрабатывается, в противном случае он игнорируется.
Присвоение IP-адресов незаметно для большинства пользователей, поскольку большинство провайдеров использует протокол, известный как DHCP, или протокол динамической установки параметров хоста. DHCP автоматически присваивает IP-адрес вашему компьютеру каждый раз, когда вы включаете в сеть ваш компьютер, подключенный к сети Интернет. Если вы используете коммутируемое соединение, ваш IP-адрес присваивается каждый раз в процессе организации такого соединения.

Еще о TCP/IP
TCP/IP - это на самом деле набор многих протоколов, которые работают вместе для обеспечения взаимодействия в больших и малых сетях. TCP и IP – это два протокола в общем наборе TCP/IP. TCP/IP является используемым по умолчанию протоколом для Windows 98, Me, 2000 и XP и автоматически устанавливается, когда стандарт plug-and-play обнаружит на компьютере сетевую карту или модем.
Сети TCP/IP, такие, как Интернет, находят компьютеры с помощью комбинации IP-адреса и MAC-адреса удаленного компьютера. Как и MAC-адрес, каждый IP должен быть уникален.
IP-адрес - это 32-битный адрес, состоящий из комбинации нулей и единиц. Однако, поскольку люди испытывают затруднения при запоминании 32-битовых номеров, IP-адреса преобразуются в десятичное представление с разделительными точками, состоящее из четырех десятичных чисел, каждое из которых отделяется точкой. Например, IP-адрес 10000011 01101111 равнозначен адресу 131.111.7.27.
IP-адреса могут присваиваться компьютеру статически или динамически. Статический адрес специально присваивается компьютеру и никогда не изменяется. Статические IP-адреса достаточно редко используются для соединений с Интернетом. Обычно поставщики услуг доступа в Интернет используют присвоение динамических IP-адресов.

Администрирование брандмауэра

Брандмауэр, как и любое другое сетевое устройство, должен кем-то управляться. Политика безопасности должна определять, кто отвечает за управление брандмауэром. Должны быть назначены два администратора брандмауэра (основной и заместитель) ответственным за информационную безопасность (или кем-либо из руководства) и эти администраторы должны отвечать за работоспособность брандмауэра и защиту сети. Основной администратор должен производить изменения в конфигурации брандмауэра, а его заместитель должен производить любые действия только в отсутствие основного, чтобы не возникало противоречивых установок. Каждый администратор брандмауэра должен сообщить свой домашний телефонный номер, номер сотового телефона и другую информацию, необходимую для того, чтобы связаться с ним в любое время.

Как защититься от вирусов?

Брандмауэры не могут обеспечить хорошую защиту от вирусов и им подобных программ. Имеется слишком много способов кодирования двоичных файлов для передачи по сетям, а также слишком много различных аппаратных архитектур и вирусов, чтобы можно было пытаться выявить их все. Другими словами, брандмауэр не может заменить соблюдение принципов защиты вашими пользователями. В общем случае, брандмауэр не может защитить от атаки, когда программа в виде данных посылается или копируется на внутренний хост, где затем выполняется. Такого рода атаки в прошлом выполнялись на различные версии программ **sendmail**, **ghostscript** и почтовых агентов, типа OutLook, поддерживающих языки сценариев.

Тем не менее, все больше поставщиков брандмауэров предлагают брандмауэры "выявляющие вирусы". Они будут полезны только наивным пользователям, обменивающимся выполняемыми программами для платформы Windows или документами с потенциально разрушительными макросами. Есть много решений на базе брандмауэра для проблем типа червя "ILOVEYOU" и других подобных атак, но они реализуют слишком упрощенные подходы, пытаясь ограничить ущерб от действий настолько глупых, что они вообще не должны выполняться. Не полагайтесь на то, что эти средства защитят вас хоть сколько-нибудь от атакующих.

Критические ресурсы для служб брандмауэра

Критичными для брандмауэра могут быть разные ресурсы, в зависимости от типов информации, передаваемых через систему. Некоторые думают, что смогут автоматически увеличивать пропускную способность брандмауэра, перенося его на компьютер с более быстрым процессором или процессором другой архитектуры, что не всегда верно. Потенциально это может привести к значительным денежным затратам, абсолютно не решающим проблему или не дающим ожидаемой масштабируемости решения. В загруженной системе особенно важен объем ОЗУ. Необходимо иметь достаточно оперативной памяти, чтобы вместить каждый экземпляр той или иной программы, необходимой для решения возложенных на машину задач. В противном случае начнется откачка страниц и производительность не будет расти. Незначительное использование области подкачки обычно не вызывает проблем, но если область подкачки системы быстро заполняется, пришло время расширять оперативную память. Систему с интенсивной подкачкой страниц часто достаточно просто заблокировать с помощью атаки на службы или сильно затормозить простой перегрузкой обращениями.

Какие основные правила фильтрации необходимо задавать для экранирования пакетов на базе ядра?

***источник:** «Брандмауэры в Internet» **(**Matt Curtin & Marcus J. Ranum**)**

Мы рассмотрим пример для пакета *ipfwadm* на Linux, но принципы (и даже большая часть командных строк) подойдут и для других интерфейсов экранирования пакетов на уровне ядра на системах Unix с "открытым кодом".

Правила пакета *ipfwadm* делятся на четыре основных категории:

-A
: Учет пакетов

-I
: Входной брандмауэр

-O
: Выходной брандмауэр

-F
: Брандмауэр для пересылки

Пакет *ipfwadm* поддерживает также возможности маскирования (`-M`). Подробнее о ключах и опциях пакета **ipfwadm** см. на соответствующей странице справочного руководства.

Реализация

Пусть в организации используется приватная сеть класса C (см. RFC 1918) с адресом 192.168.1.0. Поставщик услуг Internet выделил адрес 201.123.102.32 для внешнего интерфейса шлюза и адрес 201.123.102.33 для внешнего почтового сервера. В организации приняты следующие правила:

- Разрешаются все исходящие подключения по TCP
- Разрешаются обращения извне по протоколам SMTP и DNS к внешнему почтовому серверу
- Передача любой другой информации блокируется

Следующий блок команд можно поместить в файл загрузки системы (например, `rc.local` во многих Unix-системах).

```
ipfwadm -F -f
ipfwadm -F -p deny
ipfwadm -F -i m -b -P tcp -S 0.0.0.0/0 1024:65535 -D 201.123.102.33 25
ipfwadm -F -i m -b -P tcp -S 0.0.0.0/0 1024:65535 -D 201.123.102.33 53
ipfwadm -F -i m -b -P udp -S 0.0.0.0/0 1024:65535 -D 201.123.102.33 53
ipfwadm -F -a m -S 192.168.1.0/24 -D 0.0.0.0/0 -W eth0

/sbin/route add -host 201.123.102.33 gw 192.168.1.2
```

Объяснение

- Первая строка сбрасывает (`-f`) все правила пересылки (`-F`).
- Вторая строка устанавливает отказ от передачи в качестве стандартного правила (`-p`).
- Строки с третьей по пятую задают правила для входящей информации (`-i`) в следующем формате:

  ipfwadm **-F** (forward - пересылка) **-i** (входящая) **m** (маскирование) **-b** (двунаправленное) **-P** (протокол)[протокол] **-S** (источник)[подсеть/маска] [исходные порты] **-D** (цель) [подсеть/маска][порт]

- Шестая строка добавляет (`-a`) правило, разрешающее обращаться с внутренних IP-адресов к любым портам по любым внешним адресам.
- Восьмая строка добавляет маршрут, так что информация, посылаемая по адресу 201.123.102.33 будет передаваться на внутренний адрес 192.168.1.2.

Что такое DMZ (демилитаризованная зона) и зачем она нужна?

DMZ (ДМЗ) - сокращение от "demilitarized zone" (демилитаризованная зона). В контексте брандмауэров этот термин означает часть сети, не входящую непосредственно ни во внутреннюю сеть, ни в Internet. Обычно это область между маршрутизатором, обеспечивающим доступ в Internet, и бастионным хостом, хотя так можно называть область между любыми двумя компонентами архитектуры защиты, обеспечивающими выполнение правил доступа.

ДМЗ можно создать, установив списки контроля доступа на маршрутизаторе, обеспечивающем выход в Internet. Это позволяет минимально открыть хосты локальной сети, разрешая доступ из Internet только к определенным и контролируемым службам на этих хостах. Многие коммерческие брандмауэры просто создают на бастионном хосте третий сетевой интерфейс и называют его DMZ. Суть в том, что соответствующая сеть не является ни "внешней", ни "внутренней".

Например, Web-сервер, работающий на платформе NT, может быть уязвим для многих атак на службы RPC, NetBIOS и SMB. Эти службы не нужны для работы Web-сервера, поэтому блокирование подключений по протоколу TCP к портам 135, 137, 138 и 139 на этом хосте уменьшит его уязвимость для атаки на службы. Фактически, если заблокировать передачу на этот хост информации по любым протоколам, кроме HTTP, атакующему останется для атаки только одна служба.

Этот пример иллюстрирует важный принцип: никогда не давайте атакующим больше точек доступа, чем абсолютно необходимо для поддержки служб, предлагаемых для общего доступа.

Продолжу опять от себя… Следующий, часто задаваемый вопрос:

Насколько брандмауэры совместимы с другим ПО?

Совместимость с программами, обращающимися к Internet, очень важна: неудачно спроектированный брандмауэр может истолковать вполне законное действие (скажем, открытие порта для осуществления Internet-коммуникации) как попытку взлома, а вполне обычную программу принять за вредоносную. Одни брандмауэры спрашивают у пользователя разрешения на запуск программ, другие самостоятельно разрешают или блокируют их выполнение. По совместимости в целом почти безупречные результаты показал BlackICE Defender, а McAfee.com отстал от него лишь ненамного. Norton и ZoneAlarm в большинстве случаев сработали хорошо; Secure Desktop и ESafe выступили слабо. Ну и устойчивее всех, мне показался Tiny Personal Firewall Engine.

Что можно разрешать в правилах брандмауэра, а что нет?

Лучший способ – это установить сетевой экран на заново инсталлированную «чистую» систему, пока нет другого ПО, которое может препятствовать четкой спецификации правил вашего сетевого экрана.

Хороший брандмауэр в состоянии отличить сетевой трафик, принадлежащий «честным» программам, от злонамеренного, происходящего от «троянского коня» или злоумышленника. Это можно сделать, анализируя либо сами программы, либо трафик данных. Примером первого подхода может служить брандмауэр, который проверяет каждый запускаемый на выполнение файл по готовой таблице программ, дозволенных к применению. Пример второго, который не выясняет, какие программы запущены, но исследует все данные, поступающие на компьютер и отправляемые с него, на подозрительное поведение или наличие определенных сигнатур.

И, несомненно, самый оптимальный способ – это определение IP-адреса к которому подключается та или иная программа. Например, если вы приобрели модем для выхода в Интернет и используете web-браузер Internet Explorer, то ему нужно позволить выход один раз. Это означает, что в правилах вашего брандмауэра необходимо разрешить этот запрос, но только на **исходящий** трафик. Если вы пользуетесь каким либо почтовым клиентом, то ему также необходимо разрешить исходящий запрос.

А теперь представим (как вариант), что мы пробрели «пиратский» программный продукт для работы с графикой. Для примера возьмем Adobe PhotoShop. Перед инсталляцией запустили брандмауэр. Что же дальше? Мы вышли в Интернет и вдруг наш PFW выдает предупреждение, что PhotoShop «просится» в сеть. Первым делом, нужно отследить на какой ip-адрес был сделан запрос, а потом анализировать ситуацию, разрешить соединение или нет. Я могу однозначно сказать – НЕТ. Причин может быть множество, одна из которых – программа пытается передать «хозяину» информацию о лицензионном соглашении, но т. к. такового у нас нет, мы можем (разрешив) получить в ответ предупреждение: «Продукт не имеет лицензионного соглашения, а потому срок его использования истек».

Или возьмем другой пример. Вы используете для передачи IM сообщений в сети icq-клиента. После установки, программа icq попросит вас о соединении с Интернет и мы должны ей это разрешить, но при этом, опять таки, внимательно анализируя трафик. Естественным будет то, что icq попросится на свой сервер icq.com, но никак не будет естественным то, что клиент icq выдаст запрос на неизвестный домен. Тут мы вправе думать, что угодно, потому как неизвестно, какого рода информацию о нашей системе хочет отдать эта программа.

Далее опять немного теории и терминологии…

***источник: «Брандмауэры в Internet» (Matt Curtin & Marcus J. Ranum)**

Анатомия подключения по протоколу TCP

Протокол TCP поддерживает 6 "флагов", которые могут быть установлены (ON) или сброшены (OFF). Вот эти флаги:

FIN
: "Управляемое" соединение закрыто

SYN
: Открывается новое соединение

RST
: "Непосредственное" соединение закрыто

PSH
: Указывает получающему хосту передать данные приложению, а не просто поставить их в очередь

ACK

"Подтверждает" предыдущий пакет

URG

"Срочные" ("Urgent") данные, требующие немедленной обработки

Рассмотрим пример, когда клиент работает на хосте 5.6.7.8 и получил динамический порт 1049. Сервер работает на порту 80 хоста 1.2.3.4.

Клиент начинает попытку подключения:

```
5.6.7.8:1049 -> 1.2.3.4:80 SYN=ON
```

Сервер получает этот пакет и понимает, что кто-то хочет организовать новое подключение. Посылается ответ:

```
1.2.3.4:80 -> 5.6.7.8:1049 SYN=ON ACK=ON
```

Клиент получает ответ и информирует сервер, что ответ получен:

```
5.6.7.8:1049 -> 1.2.3.4:80 ACK=ON
```

Теперь подключение открыто. Это называется трехэтапным согласованием (three-way handshake). Его назначение - удостоверить ОБА хоста, что между ними установлено действующее соединение.

В сети Internet, ненадежной и переполненной, необходимы средства, компенсирующие потерю пакетов.

Если клиент посылает начальный пакет SYN и не получает пакет с флагами SYN+ACK в течение нескольких секунд, он посылает пакет SYN повторно.

Если сервер посылает пакет SYN+ACK и не получает пакет с флагом ACK в течение нескольких секунд, он посылает пакет SYN+ACK повторно.

Именно последнее является причиной, по которой атаки путем переполнения SYN-пакетами так хорошо работают. Если посылать пакеты SYN от множества различных портов, это потребует существенных ресурсов сервера. Если также отказаться отвечать на полученные в ответ пакеты SYN+ACK, сервер будет долго СОХРАНЯТЬ эти подключения, повторно посылая пакеты SYN+ACK. Некоторые серверы перестают принимать новые подключения при наличии достаточного количества формирующихся, вот почему атаки путем переполнения SYN-пакетами (SYN flooding) работают.

Все пакеты, передаваемые в обоих направлениях после трехходового согласования, будут иметь установленный бит ACK. Фильтры пакетов, не поддерживающие информацию о состоянии, используют эту особенность в так называемых фильтрах "установленных подключений". Они будут пропускать только пакеты с установленным битом ACK. При этом в определенном направлении не смогут проходить пакеты, способные организовать новое подключение. Обычно не разрешают открывать новые подключения с внешних хостов на внутренние, требуя установленного бита ACK во входящих пакетах.

Когда приходит время закрывать подключение, это можно сделать двумя способами. С помощью флага FIN или с помощью флага RST. При использовании флагов FIN обе стороны подключения должны послать пакеты с установленными флагами FIN, чтобы показать, что они собираются закрыть подключение, а затем послать подтверждения на эти FIN-пакеты, показывающие, что они поняли намерение противоположной стороны подключения закрыть его. При посылке пакетов RST подключение закрывается принудительно и вы не получаете информации о том, поняла ли противоположная сторона ваше требование о закрытии подключения и получила ли она на самом деле все посланные ей данные.

Закрытие подключения с помощью FIN-пакетов также может привести к ситуации отказа служб, поскольку стек TCP должен сравнительно надолго запоминать закрытые подключения на случай, когда другая сторона не получила одного из FIN-пакетов.

Если открыть и закрыть достаточно много подключений, в конечном итоге можно получить "закрытые" подключения во всех имеющихся слотах, описывающих подключения. В этом случае вы не сможете динамически выделять новые подключения, ибо все возможные уже использованы. Различные операционные системы по-разному реагируют на эту ситуацию.

Ссылки

1. Стивен Бэлловин (Steven M. Bellovin).
   Реализация протокола FTP для поддержки брандмауэров (Firewall-friendly FTP).
   Рабочий документ RFC 1579.

2. Р. Финлейсон (R. Finlayson).
   Многоадресная IP-передача и брандмауэры (Ip multicast and firewalls).
   Рабочий документ RFC 2588, май 1999.

3. Я. Рехтер (Y. Rekhter), Б. Московиц (B. Moskowitz), Д. Карренберг (D. Karrenberg), Г. де Грут (G. J. de Groot) и Е. Лир (E. Lear).
   Распределение адресов для приватных IP-сетей (Address allocation for private internets).
   Рабочий документ RFC 1918, февраль 1996.

4. Р. Сайер (R. Thayer), Н. Дорасвами (N. Doraswamy) и Р. Гленн (R. Glenn).
   Принципы создания стандарта защиты IP (IP Security Document Roadmap).
   Рабочий документ RFC 2411, ноябрь 1998.

ДРУГИЕ ПРЕПЯТСТВИЯ

Возможность безопасного администрирования межсетевых экранов в удаленных офисах из центральной сети предоставляет в распоряжение корпораций функциональность, которой им давно недоставало. Так как в удаленных офисах часто нет специалистов по обслуживанию такой техники, требуется полное управление из центра. Но даже в этом случае перед поставкой новинок в удаленный офис необходимо выполнить их конфигурацию. Помимо этого, такие устройства нужно правильно подключить. Большинство из них имеет несколько интерфейсов, каждый со своими

параметрами защиты, поэтому правильное подключение имеет решающее значение для их корректной работы.

Те пользователи, которые справились с этими основополагающими требованиями, могут приступать к решению более сложных задач, таких, как применение наборов правил и управление событиями защиты. Нужно ли в каждом удаленном офисе реализовывать одни и те же наборы правил или они могут несколько различаться? Или, например, как обрабатывать события, фиксируемые персональным межсетевым экраном, в центральном офисе? Будут ли данные об этих событиях «путешествовать» по Internet в текстовом виде, открытые для перехвата и возможного искажения, или они будут заключены в туннели VPN? Кроме того, придется решить, что делать с данными о подобных событиях, когда они достигнут центрального офиса — интегрировать ли их в существующую систему сетевого управления так, чтобы служба технической поддержки была уведомлена о получении сообщения о событии высоким приоритетом. Помимо технических аспектов решений, это лишь некоторые из процедурных сложностей, возникающих при внедрении персональных межсетевых экранов.

Занимаетесь ли вы администрированием удаленных офисов или просто работаете на ПК дома, в любом случае вы, скорее всего, вложили немало труда и средств в свои компьютеры. Если же вы хотите должным образом защитить эти вложения, то персональные межсетевые экраны заслуживают самого пристального изучения.

Итак, каково же решение проблемы? Начните с создания собственной оборонительной системы. Это означает усиление и затем тестирование защиты всей сети — начиная с ОС и кончая внешними брандмауэрами и маршрутизаторами. «Тренируйте» сетевые службы на противодействие распределенным атакам, вирусам и прочим безобразиям, пока они не «научаться улаживать» такие проблемы.