Технологии брандмауэров

13

В этой главе

- *Понятие брандмауэра*
- *Виртуальные сети*
- *Политика брандмауэра*
- *Политика сетевого доступа*
- *Гибкость политики*
- *Политика усиленной аутентификации удаленных пользователей*
- *Политика доступа через модемы*
- *Компоненты брандмауэра*
- *Принципы функционирования брандмауэра*
- *Межсетевые экраны*
- *Защита Web-серверов*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Понятие брандмауэра (020)

Брандмауэром (firewall) называется стена, сделанная из негорючих материалов и препятствующая распространению пожара. В сфере компьютерных сетей брандмауэр (БМ) представляет собой барьер, защищающий от виртуального пожара — попыток злоумышленников вторгнуться в сеть.

Брандмауэр — это подход к безопасности. Он способствует реализации политики безопасности, которая определяет разрешенные службы, типы доступа к ним и является реализацией этой политики в терминах сетевой конфигурации, хостов, маршрутизаторов и других мер защиты.

Брандмауэр — это стена...

Брандмауэр представляет собой систему или комбинацию систем, позволяющих разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Как правило, эта граница проводится между локальной сетью и Internet, хотя ее можно провести и внутри локальной сети предприятия.

Система брандмауэра может быть маршрутизатором, персональным компьютером, хостом или группой хостов, созданной специально для защиты сети или подсети от неправильного использования протоколов и служб хостами, находящимися вне этой подсети.

О***сновная цель системы брандмауэра*** — управление доступом к защищаемой сети. Он реализует политику сетевого доступа, вынуждая проходить все соединения с сетью через брандмауэр, где они могут быть проанализированы, а затем разрешены либо отвергнуты. (См. рис. 13.1).

Брандмауэр:

Определение

- вынуждает все сетевые соединения проходить через шлюз, где они могут быть проанализированы и оценены с точки зрения безопасности, и предоставляет другие средства, такие, как меры усиленной аутентификации вместо паролей.
- может ограничить доступ к тем или иным системам или доступ к Internet от них, блокировать определенные сервисы TCP/IP, или обеспечить другие меры безопасности.
- устанавливается на границе защищаемой сети и фильтрует все входящие и исходящие данные, пропуская только авторизованные пакеты.
- для каждого проходящего пакета на основе установленных правил принимает решение пропускать его или отбросить.
- включает ряд элементов, таких как политика внесения изменений в структуру сети, а также технические средства и организационные меры.

Фирмы, внедряющие Intranet, устанавливают брандмауэры "по периметру" корпоративных Web-серверов, тем самым ограничивая доступ посторонних клиентов.

Брандмауэры первого поколения, известные также как маршрутизаторы с фильтрацией пакетов, проверяют адреса отправителя и получателя в проходящих пакетах TCP/IP. Пакеты проверяются по списку доступа на наличие "дружественного адреса", и если он обнаружен, пакетам разрешается вход в сеть (в противном случае — запрещается). Эти брандмауэры служат больше средством устрашения, чем оплотом безопасности. При их использовании хакеры могут легко имитировать дружественные адреса — этот процесс называется "спуфингом" (spoofing — обман, подлог) — и получить доступ к intranet.

Следующее поколение брандмауэров — "уполномоченные серверы" (proxy servers) было создано именно для решения проблемы с имитацией IP-адресов. Эти брандмауэры могут фильтровать пакеты на уровне приложений, что особенно важно для безопасности в intranet.

Как ...уполномоченные представители... Web-сервера, такие брандмауэры могут связываться с запросом доступа системы. Кроме того, они проверяют законность пользовательского имени, пароля и передаваемых данных, а не только заголовка пакета. Например, уполномоченное приложение HTML "знает", как должны выглядеть "правильные" данные HTML, и способно определить, можно ли разрешить доступ.

Брандмауэры третьего поколения, используют для фильтрации специальные многоуровневые методы анализа состояния пакетов SMLT (Stateful Multi-Layer Technique). В отличие от брандмауэров уровня прило-

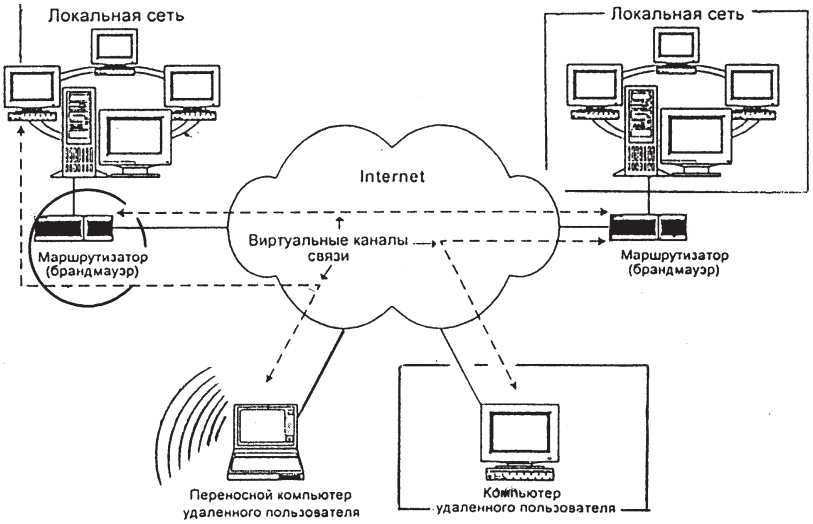


РИС. 13.1

жений, брандмауэры на основе SMLT используют программное обеспечение для анализа данных, способное создавать мгновенную копию целого пакета. Эти брандмауэры быстро сравнивают проходящие пакеты с известным состоянием (state) дружественных пакетов, позволяя значительно сократить время обработки по сравнению с медленными брандмауэрами уровня приложений.

Виртуальные сети (634)

Ряд брандмауэров позволяет также организовывать виртуальные корпоративные сети (Virtual Private Network), т.е. объединить несколько локальных сетей, включенных в Internet в одну виртуальную сеть. ***VPN позволяют организовать прозрачное для пользователей соединение локальных сетей***, сохраняя секретность и целостность передаваемой информации с помощью шифрования. При этом при передаче по INTERNET шифруются не только данные пользователя, но и сетевая информация — сетевые адреса, номера портов и т.д.

Схемы подключения (524)

Для подключения брандмауэров применяются различные схемы. Брандмауэр может использоваться в качестве внешнего роутера. При этом между внешним роутером и брандмауэром имеется только один путь, по которому идет весь трафик. Обычно роутер настраивается таким образом, что брандмауэр является единственной видимой снаружи машиной. Эта схема является наиболее предпочтительной с точки зрения безопасности и надежности защиты.

Существуют решения которые позволяют организовать для серверов, которые должны быть видимы снаружи, третью сеть; это позволяет обеспечить контроль за доступом к ним, сохраняя в то же время необходимый уровень защиты в основной сети.

Администрирование (653)

Легкость администрирования является одним из ключевых аспектов в создании эффективной и надежной системы защиты. Ошибки при определении правил доступа могут образовать брешь, через которую может быть взломана система. Поэтому в большинстве брандмауэров реализованы сервисные утилиты, облегчающие ввод, удаление, просмотр набора правил.

Наличие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе или редактирования правил. Обычно эти утилиты позволяют просматривать информацию, сгруппированную по каким-либо критериям, например все, что относится к конкретному пользователю или сервису.

Системы сбора статистики и предупреждения об атаке (654)

Еще одним важным компонентом брандмауэра является система сбора статистики и предупреждения об атаке. Информация обо всех событиях — отказах, входящих/выходящих соединениях, числе переданных байтов, использованных сервисах, времени соединения — накапливается в файлах статистики.

Многие брандмауэры позволяют гибко определять подлежащие протоколированию события, описывать

действия брандмауэра при атаках или попытках несанкционированного доступа — это может быть сообщение на консоль, почтовое послание администратору системы и т.д.

Немедленный вывод сообщения о попытке взлома...

Немедленный вывод сообщения о попытке взлома на экран консоли или администратора может помочь, если попытка оказалась успешной и атакующий уже проник в систему. В состав многих брандмауэров входят генераторы отчетов, служащие для обработки статистики. Они позволяют собрать статистику по использованию ресурсов конкретными пользователями, по использованию сервисов, по отказам и источникам, с которых проводились попытки несанкционированного доступа и т.д.

Аутентификация (653)

Прежде чем пользователю будет предоставлено право воспользоваться тем или иным сервисом, необходимо убедиться, что он действительно тот, за кого себя выдает. ***Процесс определения, какие сервисы разрешены, называется авторизацией***. Авторизация обычно рассматривается в контексте аутентификации — как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы. При получении запроса на использование сервиса от имени какого-либо пользователя, брандмауэр проверяет, какой способ аутентификации определен для данного пользователя, и передает управление серверу аутентификации. После получения положительного ответа от сервера аутентификации брандмауэр образует запрашиваемое пользователем соединение. Как правило, пользователь знает некое секретное слово, которое посылает серверу аутентификации в ответ на его запрос.

Одной из схем аутентификации является использование стандартных UNIX паролей. Эта схема является наиболее уязвимой с точки зрения безопасности — пароль может быть перехвачен и использован другим лицом.

Чаще всего применяются схемы с использованием одноразовых паролей. Даже будучи перехваченным, этот пароль будет бесполезен при следующей регистрации, а получить следующий пароль из предыдущего — крайне трудная задача.

Для генерации одноразовых паролей используются как программные, так и аппаратные генераторы. Последние представляют собой устройства, вставляемые в слот компьютера. Знание секретного слова необходимо пользователю для приведения этого устройства в действие.

Ряд брандмауэров поддерживают технологию Kerberos — один из наиболее распространенных методов аутентификации. Некоторые схемы требуют изменения клиентского программного обеспечения — шаг, который далеко не всегда приемлем. Как правило, все коммерческие брандмауэры поддерживают несколько различных схем, позволяя администратору выбрать наиболее приемлемую для своих условий.

Брандмауэры – основа СЗИ (554)

Все брандмауэры выполняют одну и ту же задачу — защищают внутренние ресурсы от внешних атак. Но какой тип брандмауэра предпочтительнее?

Если вы собираетесь открыть свою сеть для внешнего мира — установив Web-сервер, введя электронную коммерцию или предоставив бизнес-партнерам и заказчикам доступ к сетевым ресурсам, то наверняка знаете, что вам нужен хороший брандмауэр.

Какой брандмауэр в конечном счете выбрать, зависит главным образом от принятой в организации политики безопасности. Чем жестче правила безопасности, тем больше функций контроля брандмауэр должен выполнять. Помните, однако, что производительность и надежность брандмауэра находятся в обратнопропорциональном соотношении.

Брандмауэр располагается на границе сети и регулирует доступ к корпоративным ресурсам. Это устройство анализирует и собирает информацию о внешних по отношению к сети пакетах и сеансах (в зависимости от типа брандмауэра). Соответствующий принятой политике безопасности брандмауэр пропустит или не пропустит конкретный пакет и позволит или не позволит организовать конкретный сеанс в соответствии с принятыми правилами.

Проблема выбора брандмауэра в том, что различия между продуктами, производителями и технологиями стали стираться. Несколько лет назад, когда брандмауэры производили не более десятка компаний, выбор был проще; но теперь, когда множество поставщиков

предлагают брандмауэры различных типов, путаница в умах потребителей вполне объяснима.

Брандмауэры можно разделить на три основные категории:

- фильтры пакетов,
- механизмы контекстной проверки,
- шлюзы уровня приложений (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. Но чтобы понять эти различия, читатель должен вначале ознакомиться с базовыми технологиями фильтрации пакетов, контекстной проверки и посредничества.

Фильтры пакетов (534)

Фильтры пакетов анализируют поля поступающих IP-пакетов и затем пропускают или удаляют их в зависимости от принятых правил. Решение о пропуске или удалении пакета принимается в соответствии с несколькими критериями, в том числе в зависимости от IP-адреса отправителя/получателя, высокоуровневого протокола (например, TCP или UDP), номеров портов отправителя/получателя TCP или UDP.

Фильтр анализирует пакеты на сетевом уровне независимо от приложения. Благодаря этому он обеспечивает высокую производительность, правда, может пропустить атаку на уровне приложения.

Не привязанные к приложениям, фильтры пакетов обеспечивают хорошую производительность. Но поскольку они ничего не знают о приложениях и не в состоянии понять суть конкретного сеанса связи, фильтры пакетов уязвимы для хакеров на уровне приложений.

Фильтр пакетов проверяет только заголовок пакета, но не данные внутри него. Как правило, фильтры пакетов не являются коммерческими продуктами, однако многие из имеющихся на рынке маршрутизаторов выполняют те же функции. Часто фильтры пакетов создаются теми, кто реализует защиту своей сети самостоятельно.

Контекстная проверка (533)

Фильтры обрабатывают пакеты очень быстро, но их вряд ли можно признать идеальным средством защиты, так как они просматривают только некоторые поля в заголовке пакета.

Другим типом технологии брандмауэра является контекстная проверка сеансов между клиентами и серверами. Не ограничиваясь фильтрацией, брандмауэры этого типа перехватывают пакеты на сетевом уровне и принимают решения на основании высокоуровневой информации.

Брандмауэры с контекстной проверкой могут интеллектуально отслеживать пакеты и сеансы между клиентом и сервером. Брандмауэры этого типа просматривают пакеты на сетевом уровне для получения необходимой для принятия решений в области защиты информации. Эта информация сохраняется и используется при последующих попытках соединения.

Данные делятся на "хорошие" (которые правила безопасности разрешают пропустить), "плохие" (которые правила безопасности запрещают пропускать) и "неизвестные" (для которых никаких правил не определено). Брандмауэр с контекстной проверкой обрабатывает их следующим образом: данные, признаваемые хорошими, пропускаются; данные, признаваемые плохими, изымаются, а неизвестные — фильтруются, т.е. по отношению к ним брандмауэр действует как фильтр пакетов.

Пользователи должны помнить, что если они определяют новый сервис, а брандмауэр не имеет соответствующего модуля проверки данных, то по отношению к этому новому сервису брандмауэр будет действовать только как фильтр пакетов.

С совершенствованием технологии данная модель пополняется. Изначально технология имела менее надежную модель безопасности относительно обработки трафика, но с обнаружением новых хаков и модификацией программного обеспечения для защиты от них технология проверки надежно укрепляется.

Совет

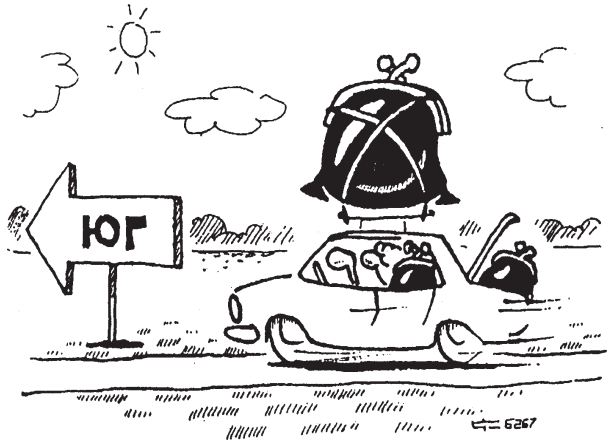
Иногда контекстная проверка может вступить в противоречие с принятой моделью безопасности, в этом случае все зависит от целей бизнеса. Несмотря на то, что эта технология может представляться недостаточной для многих компаний, где приняты жесткие меры информационной защиты, она выполняет поставленные перед ней задачи в ситуациях, когда требования бизнеса, в частности необходимость связи с внешним миром, заставляют отступить от некоторых слишком строгих правил безопасности (ситуация довольно типична).

Одной из функций брандмауэров данного типа является трансляция адресов. Она позволяет организации скрыть внутренние IP-адреса, так что извне виден только один адрес. Другие черты этой технологии — собственно проверка данных с анализом содержимого поля данных, удобство использования и высокая производительность. UDP — один из типов трафика, о котором часто забывают, потому что этот протокол не предусматривает установления соединения и, таким

образом, не учитывается при определении производительности. Кроме того, UDP не имеет контекста.

Еще одной сильной стороной технологии контекстной проверки является реальная пропускная способность. Скептики утверждают, хотя и без успеха, что технологии проверки быстрее, потому что они не анализируют все уровни стека IP. Правда же в том, что при измерении производительности учитывать приходится множество факторов.

Шлюзы уровня приложений и посредники (634)



Нужны дополнительные накладные расходы на обслуживание посредника...

Данная технология основана, как следует из названия, на использовании посредника, принимающего и организующего соединения по поручению клиента. Следствием этого являются дополнительные накладные расходы на обслуживание соединения. Чтобы брандмауэр с посредником мог обслуживать большое количество соединений, операционная система должна быть эффективной.

Шлюзы уровня приложений или посредники выступают в качестве промежуточного звена передачи пакетов между сервером и клиентом. Вначале устанавливается соединение с посредником, а уже затем он решает: создавать соединение с адресатом, или нет.

Брандмауэры с посредником обычно защищают соединения TCP посредством дублирования любого разрешенного соединения. Трафик UDP использовать в среде с посредниками не рекомендуется; при необходимости он обслуживается транслятором UDP.

Кроме того, многие производители брандмауэров предпочитают осуществлять настройку операционной системы в целях увеличения производительности, каковая невозможна без доступа к исходному коду ОС. Это является одной из причин того, что многие эксперты в области брандмауэров рекомендуют их для UNIX, а не для NT.

Хорошо написанный посредник использует подмножество прикладных программ для конкретного протокола. Использование этого подмножества команд является одной из причин высокой надежности данной модели. "Все, что явным образом не разрешено, запрещено" — справедливо не только для политики безопасности в целом, но и для посредника в частности.

Базовые необходимые команды разрешены, тем не менее некоторые отладочные команды, а также команды сбора информации могут оказаться запрещены. Разрешены только команды, необходимые для выполнения обычной транзакции. В противном случае команда блокируется.

Особенностями эффективных посредников являются минимальное кодирование, минимальный набор команд (подмножество прикладных команд) и трансляция адресов, которая вызвана тем, что посредники создают новое соединение каждый раз, когда активизируются. Посредник принимает запрос и затем инициирует новый запрос к серверу; поэтому сервер воспринимает запрос как исходящий от посредника, а не от действительного клиента. Трансляция адреса — это преобразование нескольких адресов в один, так как каждое соединение между клиентом и целевым сервером состоит в действительности из двух соединений.

Решения на базе посредников обеспечивают так называемую защиту по периметру. Вместо того чтобы защищать все хосты, концепция защиты по периметру предусматривает укрепление защиты нескольких из них, так как посредник берет на себя защиту находящихся за ним хостов. И хотя чаще защита нарушается изнутри, защита по периметру поможет на какое-то время предотвратить проникновение посторонних в сеть.

Почему именно брандмауэры? (054)

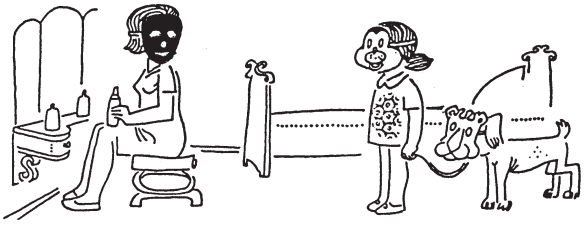
Основной причиной использования брандмауэров является тот факт, что без брандмауэра системы подсети подвергаются опасности использования уязвимых мест служб (NFS и NIS) или сканирования и атак со стороны хостов в Internet. В среде без брандмауэра сетевая безопасность полностью зависит от безопасности хостов, которые должны в этом случае взаимодействовать для достижения одинаково высокого уровня безопасности. Чем больше подсеть, тем труднее поддерживать все хосты на одном уровне безопасности.

Такое положение дел сложилось в силу ряда причин, а именно:

- **уязвимость сервисов TCP/IP** — ряд сервисов TCP/IP являются небезопасными и могут быть скомпрометированы умными злоумышленниками; сервисы, ис-

пользуемые в ЛВС для улучшения управления сетью, особенно уязвимы;

- **легкость наблюдения за каналами и маскарада** — трафик Internet незашифрован; электронная почта, пароли и передаваемые файлы могут быть перехвачены, используя легкодоступные программы, затем могут быть использованы пароли для проникновения в системы;



Маскарад...

- **отсутствие политики** — многие сети могут быть сконфигурированы по незнанию таким образом, что будут открывать доступ к ним со стороны Internet, не подозревая при этом о возможных злоупотреблениях; многие сети допускают использование большего числа сервисов TCP/IP, чем это требуется для деятельности их организации, и не пытаются ограничить доступ к информации об их компьютерах, которая может способствовать проникновению в сеть;

- **сложность конфигурирования** — средства управления доступом в хостах зачастую являются сложными в настройке и контроле за ними; неправильно сконфигурированные средства часто приводят к неавторизованному доступу.

Ошибки и упущения в безопасности стали распространенными, проникновения происходят не в результате хитроумных атак, а из-за простых ошибок в конфигурировании и угадываемых паролей. Подход с использованием брандмауэра имеет многочисленные преимущества для сетей и помогает повысить безопасность хостов.

Защита от уязвимых мест в службах (024)

Брандмауэр может:

- значительно повысить сетевую безопасность и уменьшить риски для хостов в подсети путем фильтрации небезопасных по своей природе служб. В результате подсеть будет подвергаться гораздо меньшему числу опасностей, так как через брандмауэр смогут пройти только безопасные протоколы.

- запретить использование таких уязвимых служб, как NFS за пределами данной подсети. Это позволит защититься от использования этих служб посторонними атакующими, но продолжать использовать их внутри сети, не подвергаясь особой опасности.

- обеспечить защиту от атак с использованием маршрутизации источника и попыток изменить маршруты передачи данных с помощью команд перенаправления ICMP.

- заблокировать все пакеты с маршрутизацией источника и перенаправить ICMP, а затем информировать администраторов об инцидентах.

Управляемый доступ к системам сети (023)

Сеть может запретить доступ к своим хостам извне, за исключением особых случаев, таких как почтовые или информационные серверы.

Эти свойства брандмауэров требуются при политике управления доступом, построенной по принципу: не предоставлять доступ к хостам или службам, к которым доступ не требуется.

Концентрированная безопасность (023)

Концентрация обеспечивается тем, что большинство или все изменения в программах и дополнительные программы по безопасности установлены на системе брандмауэра, а не распределены по многим хостам. В частности, системы одноразовых паролей и другие дополнительные программы усиленной аутентификации могут быть установлены только на брандмауэре, а не на каждой системе, которой нужно обращаться к Internet.

Повышенная конфиденциальность (023)

Сети могут заблокировать такую информацию о пользователях, как время последнего сеанса, определить, читалась ли почта, как часто используется система, работают ли в данный момент в этой системе пользователи, и может ли быть система атакована, не привлекая при этом внимания. Блокируя эту информацию, они скрывают другую информацию, которая была бы полезна для атакующего.

Протоколирование и статистика использования сети и попыток проникновения (033)

Брандмауэр может протоколировать доступ и предоставить статистику об использовании сети, о подозрительных событиях (alarm), о том, были ли брандмауэр или сеть атакованы либо зондированы. Кроме того, статистика использования сети важна в качестве исходных данных при проведении исследований для формулирования требований к сетевому оборудованию и программам и анализе риска.

Политика брандмауэра (053)

Политика сетевого доступа (023)

Существует два вида политики сетевого доступа, которые влияют на проектирование, установку и использование системы брандмауэра.

Политика верхнего уровня является проблемной концептуальной политикой, которая определяет, к каким сервисам доступ будет разрешен или явно запрещен из защищаемой сети, как эти сервисы будут использованы, и при каких условиях будет сделано исключение и политика не будет соблюдаться.

Политика нижнего уровня описывает, как брандмауэр должен ограничивать доступ и фильтровать сервисы, указанные в политике верхнего уровня.

Некоторые варианты этой политики можно реализовать: запрет доступа извне, неограниченный доступ в Internet или ограниченные входящий и выходящий доступ. ***Политика проектирования*** брандмауэра во многом определяет политику сетевого доступа: чем строже политика проектирования брандмауэра, тем более строгой будет и политика сетевого доступа. Поэтому прежде всего следует определиться с политикой проектирования брандмауэра.

Типовыми политиками проектирования брандмауэра являются:

- запрет всех сервисов, кроме тех, что явно разрешены,
- разрешение на доступ ко всем сервисам, кроме тех, что явно запрещены.

Первый тип более безопасен и поэтому предпочтителен, но он также более строг, в результате чего при нем допускается работа меньшего числа сервисов.

Для того чтобы правильно разработать концептуальную политику, а затем систему брандмауэра, которая реализует эту политику, NIST рекомендует, сначала разработать самый безопасный вариант политики – т.е. запретить все сервисы, кроме тех, что явно разрешены. При этом ***разработчики политики должны разбираться в следующих вопросах:***

- какие сервисы в Internet организация планирует использовать (например, TELNET, WWW, NFS);
- каким образом эти сервисы будут использованы, т.е. локально, через Internet, по модему из дома или из удаленных организаций;
- дополнительные потребности, такие как шифрование и обеспечение работы по модему;
- какие риски связаны с предоставлением этих сервисов;
- какова стоимость средств защиты и каковы изменения в возможностях использования сети при обеспечении защиты;
- приоритеты обеспечения безопасности при использовании тех или иных сервисов по отношению к возможности его использования (будет ли предоставляться сервис, если он слишком рискован, или его слишком дорого защищать).

Политика доступа к сервисам (023)

Политика доступа к сервисам должна фокусироваться на проблемах использования Internet, описанных выше, и, судя по всему, на всем доступе к сети извне (т.е. политика доступа по модемам, соединений SLIP и PPP). Эта политика должна быть уточнением общей политики организации в отношении защиты информационных ресурсов.

Данная политика должна быть реалистичной и согласованной с заинтересованными лицами перед установкой брандмауэра.

Определение

Реалистическая политика – политика, в которой найден баланс между защитой сети от известных рисков, и обеспечен доступ пользователей к сетевым ресурсам. Если система брандмауэра запрещает или ограничивает использование некоторых сервисов, то в политике должна быть описана степень предусмотренной строгости, чтобы можно было предотвратить изменение параметров средств управления доступом немедленно. Только поддерживаемая руководством реалистическая политика может обеспечить это.

Брандмауэр может реализовать ряд политик доступа к сервисам, но типичная политика может запрещать доступ к сети из Internet и разрешать только доступ к Internet из сети. Другой типичной политикой может быть разрешение некоторого доступа из Internet, но лишь к избранным системам, таким, как информационные и почтовые серверы. Брандмауэры часто реализуют политики доступа к сервисам, которые позволяют пользователям сети работать из Internet с некоторыми избранными хостами, но этот доступ предоставляется только в сочетании с усиленной аутентификацией.

Политика проекта брандмауэра (053)

Политика проекта БМ определяет правила реализации политики доступа к сервисам. ***Обычно реализуется одна из двух базовых политик проекта:***

- разрешить доступ для сервиса, если он явно не запрещен;
- запретить доступ для сервиса, если он явно не разрешен.

Брандмауэр, реализующий первую политику, пропускает все сервисы в сеть по умолчанию, если этот

сервис не был явно указан в политике управления доступом как запрещенный. Брандмауэр, реализующий вторую политику, по умолчанию запрещает все сервисы, но пропускает те, которые указаны в списке разрешенных сервисов. Вторая политика следует классической модели доступа, используемой во всех областях информационной безопасности.

Первая политика менее желательна, так как создает больше возможностей обойти брандмауэр; так, пользователи могут получить доступ к новым сервисам, не запрещаемым политикой(или не указанных в политике), или запустить запрещенные сервисы на нестандартных портах TCP/UDP, не запрещенных политикой.

Вторая политика строже и безопаснее, но ее труднее реализовать и она может повлиять на работу пользователей, когда некоторые сервисы, такие, как описанные выше, могут оказаться блокированными или использование их будет ограничено.

Реализация политики доступа к сервисам существенно зависит от возможностей и ограничений системы брандмауэра и уязвимых мест в разрешенных Internet-сервисах. Например, может потребоваться запретить сервисы, разрешенные политикой доступа, если уязвимые места в них не контролируются политикой нижнего уровня и, если безопасность сети составляет приоритет.

Эффективность системы брандмауэра при защите сети зависит от типа его реализации, от правильности выполнения процедур и от политики доступа к сервисам.

Гибкость политики (053)

Любая политика безопасности, связанная с сервисами Internet и доступом к сети должна быть гибкой. Эта гибкость необходима, поскольку Internet постоянно претерпевает изменения и потребности организации могут изменяться по мере появления новых сервисов и новых способов функционирования организации.

Новые протоколы и сервисы предоставляют новые возможности организациям, но могут возникнуть и новые проблемы с безопасностью. Поэтому политика должна иметь возможности учета новых проблем.

Кроме того, риски для организации также не бывают статичными, поскольку могут произойти большие изменения, такие, как новые обязанности, возложенные на организацию, или незначительные — изменения конфигурации сети.

Политика усиленной аутентификации удаленных пользователей (023)

Удаленные пользователи — это те, которые устанавливают соединения с внутренними системами откуда-либо из Internet. Эти соединения могут исходить от любого участка в Internet, от модемных линий, от авторизованных пользователей. В любом случае для всех таких соединений следует использовать меры усиленной аутентификации брандмауэра перед предоставлением доступа к внутренним системам.

В политике должно быть определено, что удаленные пользователи не получают доступ к системам с помощью неавторизованных модемов за брандмауэром. Из этого правила не может быть исключений, так как даже один перехваченный пароль или неконтролируемый модем может открыть "черный вход", минуя брандмауэр.

Такая политика не лишена недостатков: необходимо обучать пользователей пользоваться средствами усиленной аутентификации, расходовать средства на устройства аутентификации пользователей и администрировать удаленный доступ. Но контролировать удаленный доступ — необходимо.

Политика доступа через модемы (033)

Авторизованные пользователи нуждаются также в возможности исходящих звонков для доступа к системам, к которым нет доступа через Internet. Эти пользователи могут создать уязвимые места при небрежном обращении с модемом. Возможность исходящих звонков позволяет организовать и входящие звонки, если не принять соответствующие меры предосторожности.

Эти возможности необходимо учитывать при разработке брандмауэра и включать в него при необходимости. Требование обязательности использования мер усиленной аутентификации при доступе через брандмауэр должно быть отражено в политике. Политика может запрещать использование неавторизованных модемов, присоединенных к системам сети, если дос-

туп по модему обходит средства защиты брандмауэра. Строгая политика может ограничить число используемых модемов в сети, уменьшая таким образом ее уязвимость.

Помимо соединений через модемы, политика должна регламентировать использование соединений с помощью протоколов SLIP и PPP. Пользователи могут использовать их для создания новых сетевых соединений внутри защищенной сети. Такое соединение потенциально является способом обхода брандмауэра и может оказаться даже более опасным, чем коммутируемое соединение.

Реализация ПИБ (653)

Брандмауэр предоставляет средства реализации политики сетевого доступа. Фактически, брандмауэр обеспечивает управление доступом для пользователей и служб.

Брандмауэр является набором компонентов, настроенных на реализацию определенной политики контроля внешнего доступа к сети. Обычно они защищают внутреннюю сеть компании от вторжений из Internet, однако могут использоваться и для защиты от "нападений" из внутренней сети.

Как и в случае реализации любого другого механизма сетевой защиты, организация, вырабатывающая конкретную политику безопасности, кроме всего прочего, должна определить тип трафика TCP/IP, который будет восприниматься брандмауэром как авторизованный. Например, необходимо решить, будет ли ограничен доступ пользователей к определенным службам на базе TCP/IP, и если будет, то до какой степени.

Выработка политики безопасности поможет понять, какие компоненты брандмауэра необходимы и как их сконфигурировать, чтобы обеспечить заданные ограничения доступа.

Компоненты брандмауэра (054)

Основными компонентами брандмауэра являются:

- политика сетевого доступа
- механизмы усиленной аутентификации
- фильтрация пакетов
- прикладные шлюзы

Принципы функционирования брандмауэра

Брандмауэры чаще функционируют на какой-либо UNIX платформе (BSDI, SunOS, AIX, IRIX и т.д.), реже – на DOS, VMS, WNT, Windows NT. Из аппаратных платформ встречаются INTEL, Sun SPARC, RS6000, Alpha, HP PA-RISC, семейство RISC процессоров R4400-R5000.

Помимо Ethernet, многие брандмауэры поддерживают FDDI, Token Ring, 100Base-T, 100VG-AnyLan, различные серийные устройства. Требования к оперативной памяти и объему жесткого диска зависят от количества машин в защищаемом сегменте сети.

Как правило, в операционную систему, под управлением которой работает брандмауэр вносятся изменения, цель которых — повышение защиты самого брандмауэра. Эти изменения затрагивают как ядро ОС, так и соответствующие файлы конфигурации.

Многие брандмауэры имеют систему проверки целостности программных кодов. При этом контрольные суммы программных кодов хранятся в защищенном месте и сравниваются при старте программы во избежание подмены программного обеспечения.

Мерой эффективности брандмауэра служит вовсе не его способность к отказу в предоставлении сервисов, а способность предоставлять сервисы пользователям в эффективной, структурированной и надежной среде. Брандмауэры должны анализировать сетевой трафик и определять, какие транзакции санкционированы без неоправданного замедления работы системы.

Брандмауэры представляют собой лишь инструмент, позволяющий администратору безопасности следить за определенными участками сети и блокировать передачу потенциально опасных данных. Именно поэтому нельзя ограничиваться только постановкой и настройкой БМ, о котором часто впоследствии забывают.

Основу для работы БМ создает надежная аутентификация пользователей. БМ обеспечивает пользователям, имеющим сертификаты, возможность работать с внутренней информацией из любой сети как по одну, так и по другую сторону экрана. Кроме того, брандмауэр может аутентифицировать не только пользователей, но и внешние серверы, блокируя доступ пользователей внутренней сети к "неблагонадежным" внешним компьютерам.

Работа всех брандмауэров основана на использовании информации разных уровней модели OSI (взаимодействия открытых систем), которая определяет семь уровней взаимодействия ИС, — начиная с уровня физической среды передачи данных и заканчивая уровнем прикладных программ, используемых для коммуникаций. Чем выше уровень модели OSI, на котором брандмауэр фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты. (См. рис. 13.2).

Существующие брандмауэры значительно отличаются друг от друга как по уровню защиты, так и по используемым в них способам защиты. ***Большинство брандмауэров, поставляемых как коммерческие продукты, можно условно отнести к одной из четырех категорий:***

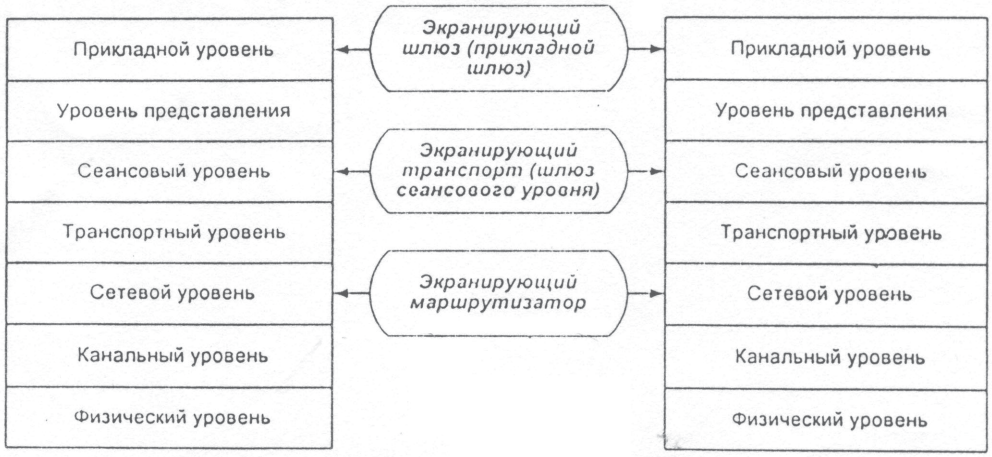
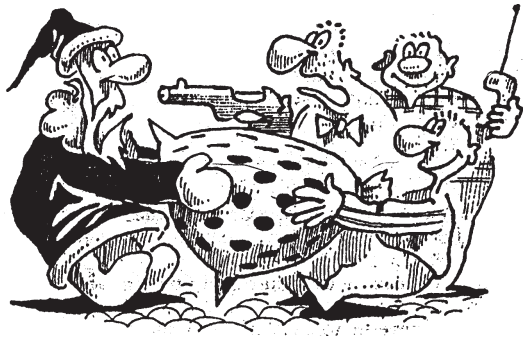


РИС. 13.2

- брандмауэры с фильтрацией пакетов (packet-filtering firewall);
- шлюзы сеансового уровня (circuit-level gateway);
- шлюзы прикладного уровня (application-level gateway);
- брандмауэры экспертного уровня (stateful inspection firewall).

Лишь немногие брандмауэры относятся только к одной из перечисленных категорий, еще меньше — в точности соответствует определениям для каждой из категорий. Тем не менее эти определения отражают ключевые возможности, отличающие один вид брандмауэров от другого.

Усиленная аутентификация (054)



Усиленная аутентификация...

Пользователям рекомендуется выбирать такие пароли, которые было бы трудно угадать и не сообщать их никому, однако тот факт, что злоумышленники могут наблюдать за каналами в Internet и перехватывать передающиеся в них пароли, делает традиционные пароли нецелесообразными.

Разработан ряд мер усиленной аутентификации — смарт-карты, биометрические, и программные механизмы для защиты от уязвимости обычных паролей. Хотя они и имеют различия, все они одинаковы в том, что пароли, генерируемые устройством усиленной аутентификации, не могут быть повторно использованы атакующим, который перехватывает трафик соединения. Поскольку проблема с паролями в Internet постоянна, брандмауэр, который не использует средств усиленной аутентификации – пустая трата времени и средств.

Некоторые устройства усиленной аутентификации, используемые в настоящее время, называются ***системами с одноразовыми паролями***. Смарт-карта, например, генерирует ответ, который хост использует вместо традиционного пароля. Так как смарт-карта работает совместно с программой или оборудованием на хосте, генерируемые ответы уникальны для каждого установления сеанса. Результатом является одноразовый пароль, который в случае перехвата не может быть использован злоумышленником для установления сеанса с хостом под видом пользователя.

Так как брандмауэры могут централизовать управление доступом в сети, то логично именно в их состав включать установки программ или устройств усиленной аутентификации. Если хосты не используют мер усиленной аутентификации, злоумышленник может попытаться взломать пароли или перехватить сетевой трафик с целью найти в нем сеансы, в ходе которых передаются пароли.

Фильтрация пакетов (033)

Брандмауэр с фильтрацией пакетов представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Брандмауэр

пропускает или отбраковывает пакеты в соответствии с информацией, содержащейся в IP-заголовках пакетов. (См. рис. 13_3).

Например, большинство брандмауэров с фильтрацией пакетов может пропускать или отбраковывать пакеты на основе информации, позволяющей ассоциировать данный пакет с конкретными отправителем и получателем

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы из следующих полей пакета:

- IP-адрес отправителя,
- IP-адрес получателя,
- информации о приложении или протоколе,
- TCP/UDP-порт отправителя,
- TCP/UDP-порт получателя.

Не все маршрутизаторы фильтруют по TCP/UDP-порту отправителя, но многие производители предоставляют такую возможность. Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации.

Если брандмауэр может блокировать соединения TCP или UDP к определенным портам или от них, то можно реализовать политику, при которой определенные виды соединений могут быть осуществлены только с конкретными хостами. Например, блокировать все входящие соединения для всех хостов, кроме нескольких систем, входящих в состав брандмауэра. Для этих систем могут быть разрешены только определенные сервисы, такие как SMTP для одной системы и TELNET или FTP — для другой.

Все маршрутизаторы (даже те, которые не сконфигурированы для фильтрации пакетов), обычно проверяют полную ассоциацию пакета, чтобы определить, куда его нужно направить. Брандмауэр с фильтрацией пакетов, кроме того, перед отправкой пакета получателю сравнивает его полную ассоциацию с таблицей правил, в соответствии с которыми он должен пропустить или отбраковать данный пакет.

Брандмауэр продолжает проверку до тех пор, пока не найдет правила, с которым согласуется полная ассоциация пакета. Если брандмауэр получил пакет, не соответствующий ни одному из табличных правил, он применяет правило, заданное по умолчанию, которое также должно быть четко определено в таблице брандмауэра. Из соображений безопасности это правило обычно указывает на необходимость отбраковки всех пакетов, не удовлетворяющих ни одному из других правил.

Настройка правил (033)

Можно задать правила фильтрации пакетов, которые будут указывать брандмауэру, какие пакеты должны быть пропущены, а какие отбракованы. Например, можно определить правила таким образом, чтобы брандмауэр отбраковывал пакеты, поступающие от внешних серверов (Internet-хостов), IP-адреса которых даны в таблице. Можно также задать правило, в соответствии с которым будет разрешено пропускать только входящие сообщения электронной почты, адресованные почтовому серверу, или правило блокировки всех почтовых сообщений, поступающих от внешнего хоста, который когда-то переполнил сеть гигабайтами ненужных данных.

Кроме того, можно сконфигурировать брандмауэр для фильтрации пакетов на основе номеров портов, задаваемых в заголовках пакетов TCP и UDP (User Datagram Protocol). В этом случае можно будет пропускать отдельные виды пакетов (например, Telnet или FTP), только если они направляются к определенным серверам (соответственно к Telnet или FTP). Однако успешное выполнение подобного правила зависит от того, какие соглашения приняты в сети, функционирующей на основе TCP/IP: для работы приложений TCP/IP серверы и клиенты обычно используют конкретные порты, однако это не является обязательным условием.

Конечно, реальные правила создавать намного сложнее, чем описано выше. Более сложные примеры можно найти в правилах конфигурирования маршрутизаторов компании Cisco, доступных через Internet.

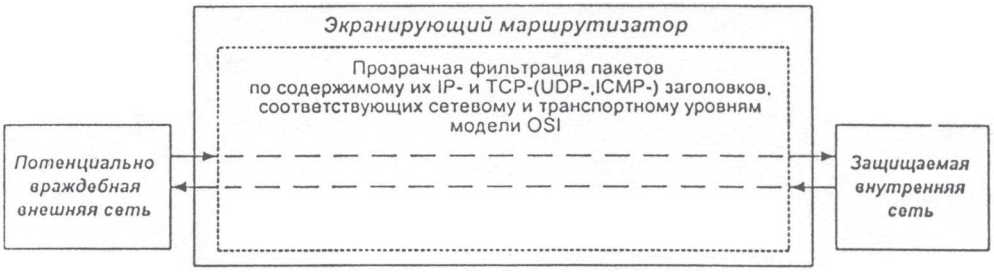
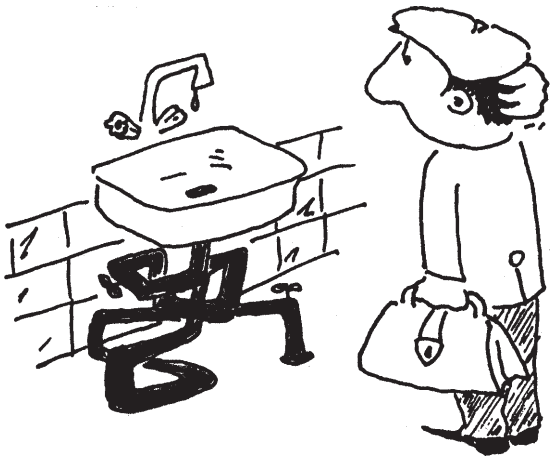


РИС. 13.3

Проблемы маршрутизаторов с фильтрацией пакетов (520)

Часто приходится делать исключения из правил, чтобы разрешить определенные виды доступа, которые обычно блокируются. Но исключения из правил фильтрации могут усложнить их до такой степени, что они станут неконтролируемыми. Добавление определенных правил может усложнить всю схему фильтрации. Как было отмечено, тестирование сложного набора правил на корректность может оказаться очень трудным.



Маршрутизатор...

Некоторые маршрутизаторы с фильтрацией пакетов не фильтруют по порту TCP/UDP отправителя, что может сделать набор правил фильтрации очень сложным и создать пробелы в схеме фильтрации.

Другой проблемой является то, что ряд служб RPC трудно заблокировать потому, что сервера для этих служб слушают порты, случайно выбираемые в процессе загрузки системы. Служба ***portmapper*** отображает первоначальные вызовы служб RPC в назначенные им номера служб, но для маршрутизатора с фильтрацией пакетов ее эквивалента не существует.

Так как нет возможности сообщить маршрутизатору, с каким портом работает служба, нельзя полностью заблокировать эти службы, разве что заблокировать полностью все пакеты UDP (RPC-службы в основном используют UDP). Блокирование всех пакетов UDP приведет к блокированию ряда других полезных служб, например DNS.

Маршрутизаторы с фильтрацией пакетов с более чем двумя интерфейсами не имеют возможностей по фильтрации пакетов в зависимости от того, с какого интерфейса приняты пакеты, и куда должны быть направлены. Фильтрация входящих и исходящих пакетов упрощает правила фильтрации пакетов и позволяет маршрутизатору легко определить, какой IP-адрес подлинный, а какой — фальшивый. Маршрутизаторы без такой возможности затрудняют реализацию стратегий фильтрации.

Низкая стоимость – слабая защита? (624)

Главное преимущество использования брандмауэров с фильтрацией пакетов состоит в невысокой стоимости их реализации и минимальном влиянии на производительность сети. Если в сети уже установлен аппаратный или программный IP-маршрутизатор, обеспечивающий возможность фильтрации пакетов (например, производства Cisco Systems, Bay Networks или Novell), настройка брандмауэра обойдется даром (не считая времени на создание правил фильтрации пакетов).

Несмотря на привлекательность таких брандмауэров с точки зрения минимизации затрат, они, как правило, не могут обеспечить адекватную защиту от хакеров. Корректная настройка правил фильтрации пакетов может оказаться достаточно сложной процедурой, однако даже при создании достаточно эффективных правил, их возможности остаются ограниченными.

Допустим, создано правило, в соответствии с которым брандмауэр будет отбраковывать пакеты с неизвестным адресом отправителя. Однако хакер может использовать в качестве адреса отправителя в своем пакете реальный адрес доверенного (авторизованного) клиента. В этом случае брандмауэр не сумеет отличить поддельный пакет от подлинного и пропустит его, "предполагая", что остальная информация в полной ассоциации пакета соответствует разрешающему правилу. Подобный вид нападений, называемый "address-spoofing" (подмена адреса), довольно широко распространен в Internet и, к сожалению, достаточно эффективен.

Интересно

Поскольку брандмауэр с фильтрацией пакетов, работающий только на сетевом уровне модели OSI, обычно проверяет только информацию, содержащуюся в IP-заголовках пакетов, то "обмануть" его не составляет труда: хакер просто создает заголовок, который удовлетворяет разрешающим правилам брандмауэра. Кроме заголовка пакета, иная содержащаяся в нем информация брандмауэрами данной категории не проверяется.

Шлюзы сеансового уровня (730)

Шлюз сеансового уровня следит за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем брандмауэр с фильтрацией пакетов.

Контроль квитирования связи (624)

Чтобы определить, является ли запрос на сеанс связи допустимым, шлюз сеансового уровня выполняет примерно следующую процедуру. Когда авторизованный клиент запрашивает некую услугу, шлюз принимает запрос, проверяя, удовлетворяет ли клиент базовым критериям фильтрации (например, может ли DNS-сервер определить IP-адрес клиента и ассоциированное с ним имя). Затем, действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за выполнением процедуры квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, например 1000, является запросом клиента на открытие сеанса. Внешний хост, получивший этот пакет, посылает в ответ пакет, помеченный флагом ACK и содержащий число, на единицу большее, чем в принятом пакете (в нашем случае 1001), подтверждая, таким образом, прием пакета SYN от клиента. После этого осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом (например, 2000), а клиент подтверждает его получение передачей пакета ACK, содержащего число 2001. На этом процесс квитирования связи завершается.

Шлюз сеансового уровня воспринимает запрошенный сеанс как допустимый только в том случае, если при выполнении процедуры квитирования связи флаги SYN и ACK, а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными.

Канальные посредники (730)

После того как шлюз "определил", что доверенный клиент и внешний шлюз являются авторизованными участниками сеанса TCP, и проверил допустимость данного сеанса, он устанавливает соединение. Начиная с этого момента шлюз копирует и перенаправляет пакеты в оба направления, не проводя фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, относящиеся к одному из сеансов связи, которые зафиксированы в этой таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает использованную цепь.

Посредник...

Для копирования и перенаправления пакетов в шлюзах сеансового уровня используются специальные приложения, которые иногда называют канальными посредниками (pipe proxies), поскольку они устанавливают между двумя сетями виртуальную цепь, или канал, а затем разрешают пакетам (которые генерируются приложениями TCP/IP) проходить по этому каналу.

Канальные посредники поддерживают несколько служб TCP/IP, поэтому шлюзы сеансового уровня могут использоваться для расширения возможностей шлюзов прикладного уровня, работа которых основывается на программах-посредниках конкретных приложений. В действительности большинство шлюзов сеансового уровня не являются самостоятельными продуктами, а поставляются в комплекте со шлюзами прикладного уровня.

Серверы-посредники (750)

Шлюз сеансового уровня выполняет еще одну важную функцию защиты: он используется в качестве сервера-посредника (proxy server). И хотя этот термин предполагает наличие сервера, на котором работают программы-посредники (что справедливо для шлюза сеансового уровня), в данном случае он означает несколько другое. Сервером-посредником может быть брандмауэр, использующий процедуру трансляции адресов (address translation), при которой происходит преобразование внутренних IP-адресов в один надежный адрес. Этот адрес ассоциируется с брандмауэром, из которого передаются все исходящие пакеты.

В результате в сети со шлюзом сеансового уровня все исходящие пакеты оказываются отправленными из

этого шлюза, что исключает прямой контакт между внутренней (авторизованной) и потенциально опасной внешней сетью. IP-адрес шлюза сеансового уровня становится единственным активным IP-адресом, который попадает во внешнюю сеть. Таким образом, шлюз сеансового уровня и другие серверы-посредники защищают внутренние сети от нападений типа spoofing (имитация адресов), описанных выше.

Однако после установления связи такие шлюзы фильтруют пакеты только на сеансовом уровне модели OSI, т.е. не могут проверять содержимое пакетов, передаваемых между внутренней и внешней сетью на уровне прикладных программ. И поскольку осуществляется эта передача вслепую, хакер, находящийся во внешней сети, может провести свои пакеты через шлюз. После этого хакер обратится непосредственно к внутреннему Web-серверу, который может не обеспечивать функции брандмауэра.

Иными словами, если процедура квитирования связи успешно завершена, шлюз сеансового уровня установит соединение и будет механически копировать и перенаправлять все последующие пакеты независимо от их содержимого. Чтобы фильтровать пакеты, генерируемые определенными сетевыми службами в соответствии с их содержимым, необходим шлюз прикладного уровня.

Добавление proxy-сервера к шлюзу (720)

На одном уровне proxy-сервер скрывает внутренние IP-адреса и обеспечивает централизацию управления и защиты исходящего трафика IP. При передаче всего трафика через proxy-сервер внутренние IP-адреса остаются скрытыми от внешнего мира. Кроме того, компании могут избавиться от необходимости иметь отдельное Internet-соединение для каждой настольной системы.

Некоторые из брандмауэров, представленных на рынке, имеют функцию разделяемого шлюза, но многие брандмауэры, главным образом, фильтры пакетов такой функции не имеют. В этих случаях добавление proxy-сервера к шлюзу позволит компании выступать перед внешним миром под единственным IP-адресом.

Данная стратегия имеет несколько преимуществ. Одно из них в том, что хакеры не могут получать действительные внутренние IP-адреса и использовать их против компании (метод, известный как подделка IP-адресов – IP-spoofing). Компаниям также не придется регистрировать каждый внутренний IP-адрес, что стоит довольно дорого.

Proxy-сервер кэширует информационное наполнение (720)

Помимо действия в интересах клиентов, желающих получить доступ к услугам Internet, proxy-серверы, в отличие от брандмауэров, могут кэшировать информационное наполнение Internet. Многие компании имеют множество конечных пользователей, каждый из которых работает с Internet. Когда хотя бы часть этих пользователей обращается в Internet одновременно, многие сети испытывают нехватку пропускной способности.

Установив proxy-сервер на отдельной машине, можно полностью использовать дисковое пространство этого сервера для сохранения "под рукой" наиболее популярных страниц Web или URL. Предложенный Netscape-продукт применяет модель, которая обеспечивает тиражирование как по требованию, так и по команде.

Тиражирование по требованию типично для большинства операций кэширования. Когда пользователь обращается к удаленному серверу Web-серверу, страница кэшируется на локальном proxy-сервере. Если любой другой пользователь снова обращается к этой странице, кэшированная копия сравнивается с текущей версией, вносятся необходимые изменения и кэшированная версия пересылается клиенту. Это сокращает как время отклика для клиента, так и сетевой трафик.

При тиражировании по команде proxy-сервер автоматически обновляет информацию, хранящуюся в кэш-памяти. Для того чтобы сократить Internet-трафик, приведение определенной страницы в соответствие с последней ее версией может осуществляться в нерабочее время.

Возможности кэширования proxy-сервера пригодны и для использования в иных целях. Помимо предоставления страниц внутренним пользователям для ускорения и сокращения трафика proxy-сервер может также кэшировать страницы принадлежащего компании Web-сервера, к которым чаще всего обращаются внешние пользователи.

Когда сотни внешних пользователей ежедневно обращаются к Web-серверу компании, proxy-сервер может разместить наиболее часто используемые страницы перед Web-сервером и предоставлять их, не обращаясь к серверу. Это позволяет снизить рабочую нагрузку на сервер Web.

Кэширование также предполагает сохранение информации об URL, к которым обращаются чаще всего, и определение срока обновления копии. Помимо сохранения информации об URL proxy-серверы могут быть интегрированы с продуктами независимых про-

изводителей для контроля и фильтрации трафика Internet, как попадающего в сеть компании, так и исходящего из нее.

Руководство компании может, например, запретить сотрудникам во время рабочего дня бесплатный доступ к службам Internet, не связанным с их служебными обязанностями во избежание злоупотреблений.

Серверы уровня соединения (730)

Сервер уровня соединения представляет собой транслятор TCP соединения. Пользователь образует соединение с определенным портом на брандмауэре, после чего последний производит соединение с местом назначения по другую сторону от брандмауэра. Во время сеанса этот транслятор копирует байты в обоих направлениях, действуя как провод.

Транслятор...

Как правило, пункт назначения задается заранее, в то время как источников может быть много. Используя различные порты, можно создавать различные конфигурации. Такой тип сервера позволяет создавать транслятор для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису, сбор статистики по его использованию.

Сравнительные характеристики (520)

Приведем основные преимущества и недостатки пакетных фильтров и серверов прикладного уровня.

Положительные качества пакетных фильтров следующие:

- относительно невысокая стоимость,
- гибкость в определении правил фильтрации,
- небольшая задержка при прохождении пакетов.

Недостатки данного типа следующие:

- локальная сеть видна (маршрутизируется) из Internet,
- правила фильтрации пакетов трудны в описании и требуют очень глубоких знаний технологий TCP и UDP,
- при нарушении работоспособности брандмауэра все компьютеры за ним становятся полностью незащищенными либо недоступными,
- аутентификацию с использованием IP-адреса можно обмануть использованием IP-спуфинга (атакующая система выдает себя за другую, используя ее IP-адрес),
- отсутствует аутентификация на пользовательском уровне.

Преимущества серверов прикладного уровня следующие:

- локальная сеть невидима из Internet,
- при нарушении работоспособности брандмауэра пакеты перестают проходить через него, что снимает угрозы для защищаемых им машин,
- защита на уровне приложений позволяет осуществлять дополнительные проверки, снижая тем самым вероятность взлома с использованием дыр в программном обеспечении,
- аутентификация на пользовательском уровне может быть реализована система немедленного предупреждения о попытке взлома.

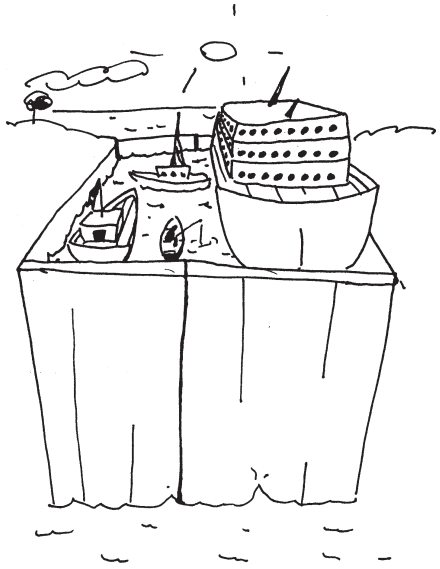
Недостатки этого типа:

- более высокая, чем для пакетных фильтров стоимость;
- невозможность использования протоколов RPC и UDP;
- более низкая производительность, чем для пакетных фильтров.

Шлюзы прикладного уровня (520)

Чтобы защититься от угроз, связанных с маршрутизаторами с фильтрацией пакетов, в брандмауэрах нужно использовать прикладные программы для перенаправления и фильтрации соединений с такими службами, как TELNET и FTP. Такое приложение называется ***proxy-службой***, а хост, на котором оно работает, ***шлюзом прикладного уровня***.

Шлюз прикладного уровня, как и шлюз сеансового уровня, перехватывает входящие и исходящие пакеты, использует программы-посредники, копирующие и перенаправляющие информацию через шлюз, а также функционирует в качестве сервера-посредника, исключая прямые соединения между доверенным сервером или клиентом и внешним хостом.



Шлюз прикладного уровня...

Однако посредники, используемые шлюзом прикладного уровня, имеют существенные отличия от канальных посредников шлюзов сеансового уровня: во-первых, они связаны с приложениями, а во-вторых, могут фильтровать пакеты на прикладном уровне модели OSI.

Прикладные шлюзы и маршрутизаторы с фильтрацией пакетов могут быть объединены для достижения более высокой безопасности и гибкости, чем была бы достигнута, при использовании их отдельно. ***Пользователь, желающий соединиться снаружи с системой в сети, должен сначала соединиться с прикладным шлюзом, а затем — с нужным хостом:***

- сначала пользователь устанавливает telnet-соединение с прикладным шлюзом и вводит имя внутреннего хоста,
- шлюз проверяет IP-адрес пользователя и разрешает или запрещает соединение в соответствии с тем или иным критерием доступа,
- может понадобиться аутентификация пользователя (возможно с помощью одноразовых паролей),
- прокси-сервер создает telnet-соединение между шлюзом и внутренним хостом,
- прокси-сервер передает данные между этими двумя соединениями,
- прикладной шлюз протоколирует соединение.

Прикладные шлюзы имеют серьезные **преимущества** перед обычным режимом, при котором прикладной трафик пропускается напрямую к внутренним хостам. Они включают в себя:

- **скрытие информации**, при котором имена внутренних систем необязательно будут известны внешним системам с помощью DNS, так как прикладной шлюз может быть единственным хостом, чье имя должно быть известно внешним системам;
- **надежная аутентификация и протоколирование**, при котором прикладной трафик может быть предварительно аутентифицирован до того, как он достигнет внутренних хостов, и может быть запротоколирован более эффективно, чем стандартные средства протоколирования хоста;
- **оптимальное соотношение между ценой и эффективностью**, поскольку дополнительные программы или оборудование для аутентификации или протоколирования нужно устанавливать только на прикладном шлюзе;
- **простые правила фильтрации**, так как правила на маршрутизаторе с фильтрацией пакетов будут менее сложными, чем они были бы, если бы маршрутизатор сам фильтровал прикладной трафик и отправлял его большому числу внутренних систем. Маршрутизатор должен только пропускать прикладной трафик к прикладному шлюзу и блокировать весь остальной трафик.

Недостаток прикладного шлюза заключается в том, что при использовании клиент-серверных протоколов, таких, как TELNET, требуется двухшаговая процедура для вхождения или выхода.

Некоторые прикладные шлюзы требуют модифицированных клиентов, что может рассматриваться либо как недостаток, либо как преимущество, в зависимости от того, облегчают ли модифицированные клиенты использование брандмауэра. Прикладной шлюз TELNET необязательно требует модифицированного клиента TELNET, тем не менее он требует другой логики действий от пользователя: пользователь должен установить соединение(но не сеанс) с брандмауэром, а не напрямую установить сеанс с хостом. Но модифицированный клиент TELNET делает брандмауэр прозрачным, позволяя пользователю указать конечную систему(а не брандмауэр) в команде TELNET.

Брандмауэр является как бы дорогой к конечной системе и поэтому перехватывает соединение, а затем выполняет дополнительные шаги, такие, как запрос одноразового пароля. Пользователю не нужно в этом случае ничего предпринимать, но на каждой системе должен быть установлен модифицированный клиент.

Прикладной шлюз для электронной почты служит для централизованного сбора электронной почты и распространения ее по внутренним хостам и пользователям. Шлюз должен принимать почту от внешних пользователей, а затем переправлять ее на другие внутренние системы. Пользователи, посылающие электронные

письма с внутренних систем, могут посылать их с внутренних систем, или, если внутренние имена систем неизвестны снаружи сети, письмо должно быть послано на прикладной шлюз, который затем переправит его к хосту назначения.

В отличие от канальных посредников, посредники прикладного уровня пропускают только пакеты, сгенерированные теми приложениями, которые им поручено обслуживать. Например, программа-посредник службы Telnet может копировать, перенаправлять и фильтровать лишь трафик, генерируемый этой службой. Если в сети работает только шлюз прикладного уровня, то входящие и исходящие пакеты могут передаваться лишь для тех служб, для которых имеются соответствующие посредники. Так, если шлюз прикладного уровня использует только программы-посредники FTP и Telnet, то он будет пропускать пакеты этих служб, блокируя при этом пакеты всех остальных.

Фильтрация на прикладном уровне (520)

В отличие от шлюзов сеансового уровня, которые копируют и механически перенаправляют все поступающие пакеты, посредники прикладного уровня (самого высокого в модели OSI) проверяют содержимое каждого проходящего через шлюз пакета. Эти посредники могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Утилиты этих шлюзов позволяют фильтровать определенные команды, используемые этими службами. Например, можно сконфигурировать шлюз таким образом, чтобы он предотвращал использование клиентами команды FTP Put, которая дает возможность пользователю, подключенному к FTP-серверу, записывать на него информацию. Многие сетевые администраторы предпочитают запретить использование этой команды, чтобы уменьшить риск случайного повреждения хранящейся на FTP-сервере информации и вероятность заполнения его гигабайтами хакерских данных, пересылаемых на сервер для заполнения его дисковой памяти и блокирования работы.

В дополнение к фильтрации пакетов многие шлюзы прикладного уровня регистрируют все выполняемые сервером действия и предупреждают сетевого администратора о возможных нарушениях защиты, что наиболее важно. Например, при попытках проникновения в систему извне BorderWare Firewall Server компании Secure Computing позволяет фиксировать адреса отправителя и получателя пакетов, время, когда эти попытки были предприняты, и используемый протокол. Продукт Black Hole компании Milkyway Networks также регистрирует все действия сервера и предупреждает администратора о возможных нарушениях, посылая ему сообщение по электронной почте или на пейджер. Аналогичные функции обеспечивают и продукты Eagle и Sidewinder Security Server.

Необходимо фиксировать адрес отправителя и получателя...

Шлюзы прикладного уровня обеспечивают один из самых высоких на сегодня уровней защиты, однако существует мнение, что такая высокая степень защиты имеет и оборотную сторону, а именно — отсутствие "прозрачности" работы шлюза для пользователей. В идеале все брандмауэры должны быть "прозрачными", т.е. их работа должна оставаться незаметной для пользователей, обращающихся из своей внутренней сети в Internet. В реальной жизни брандмауэры вносят задержки в процесс передачи данных или требуют от пользователей выполнения нескольких процедур регистрации при подключении к Internet или корпоративной интрасети.

Пример

Многие поставщики утверждают, что их шлюзы прикладного уровня "прозрачны", однако рекомендуют конфигурировать их таким образом, чтобы они выполняли аутентификацию пользователей при их обращении к внешней сети (т.е. процедуру, которая нарушает "прозрачность" работы шлюза).Так, шлюз Black Hole компании Milkyway Networks можно сконфигурировать так, что пользователи будут выходить во внешнюю сеть, не регистрируясь на этом шлюзе. Но Milkyway Networks рекомендует такую конфигурацию шлюза, при которой пользователи должны будут регистрироваться на нем либо один раз в течение установленного периода, либо при каждом запросе на установление сеанса связи. Аналогичным образом может быть настроен шлюз Gauntlet Internet Firewall компании Trusted Information Systems.

При работе шлюза в "непрозрачном" режиме пользователь подключается к посреднику соответству-

ющей службы (например, Telnet) и сообщает ему имя хоста, к которому он собирается подключиться. После этого пользователь получает и отправляет информацию так, как если бы было установлено прямое соединение клиента с внешним хостом. В "прозрачном" режиме подключение пользователя к удаленному хосту выполняется без предварительного взаимодействия со шлюзом, однако затем шлюз перехватывает все запросы пользователя.

Серверы прикладного уровня (620)

Брандмауэры с серверами прикладного уровня используют серверы конкретных сервисов, запускаемых на брандмауэре и пропускающих через себя весь трафик, относящийся к данному сервису. Таким образом, между клиентом и сервером образуются два соединения: от клиента до брандмауэра и от брандмауэра до места назначения.

Полный набор поддерживаемых серверов различается для каждого конкретного брандмауэра, однако ***чаще всего встречаются серверы для следующих сервисов:***

- терминалы (Telnet, Rlogin),
- передача файлов (Ftp),
- электронная почта (SMTP, POP3),
- WWW (HTTP),
- Gopher,
- Wais,
- X Window System (X11),
- Принтер,
- Rsh,
- Finger,
- новости (NNTP) и т.д.

Использование серверов прикладного уровня позволяет решить важную задачу — скрыть от внешних пользователей структуру локальной сети, включая информацию в заголовках почтовых пакетов или службы доменных имен (DNS).

Другим положительным свойством является возможность аутентификации на пользовательском уровне (аутентификация — процесс подтверждения идентичности чего-либо; в данном случае это процесс подтверждения, действительно ли пользователь является тем, за кого себя выдает).

При описании правил доступа используются такие параметры, как название сервиса, имя пользователя, допустимый временной диапазон использования сервиса, компьютеры, с которых можно пользоваться сервисом, схемы аутентификации.

Серверы протоколов прикладного уровня позволяют обеспечить наиболее высокий уровень защиты — взаимодействие с внешним миров реализуется через небольшое число прикладных программ, полностью контролирующих весь входящий и выходящий трафик.

Комбинация брандмауэра и proxy-сервера (624)

Доступ к Internet расширил возможности проникновения посторонних в хранилища важной для компании информации. Но при наличии упреждающей политики защиты сохранить ресурсы в безопасности существенно легче.

Хотя большинство экспертов по безопасности рекомендуют многоуровневый подход к защите сетевых ресурсов, включая шифрование и аутентификацию, ключевым компонентом любой такой системы является брандмауэр.

Брандмауэр размещается на шлюзе между локальной сетью и Internet. Помимо других функций, брандмауэр может просматривать IP-пакеты и, в зависимости от адресов отправителя и получателя, пропускать (не пропускать) пакеты, пытающиеся проникнуть в систему.

Брандмауэры также могут контролировать сеансы связи с Internet на уровне приложений, а это более надежное средство защиты, нежели простой просмотр IP-адресов приходящих пакетов. Кроме того, шлюз уровня приложений можно точно настроить для контроля определенных типов трафика.

Организация посреднических сеансов для предотвращения прямого доступа внешнего трафика к внутренним ресурсам — еще одна возможность шлюза уровня приложений. Когда брандмауэр опознает входящий трафик Internet, он инициирует уполномоченное приложение для организации отдельного сеанса с внутренними ресурсами по поручению внешнего пользователя.

Хотя многие брандмауэры справляются с этими посредническими услугами, на рынке систем защиты стали появляться продукты относительно нового типа, называемые proxy-серверами.

Поскольку множество брандмауэров выполняет функции proxy-серверов, некоторые пользователи считают установку proxy-сервера излишеством. В действительности proxy-сервер может ощутимо укрепить брандмауэр и даже обеспечить возможности, которые тот предложить не может.

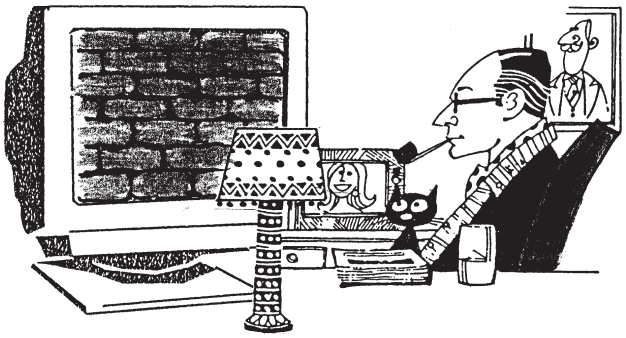
Компания, имеющая выход в Internet, должна обратить внимание на брандмауэры с тем, чтобы только законные пользователи могли войти в сеть извне и чтобы только законные сеансы были открыты. Тем временем многие компании начинают проявлять интерес

и к тому, чем заняты в Internet сотрудники самой компании.

В общем, proxy-сервер управляет и контролирует трафик Internet между сетью компании и внешним миром; кроме того, он направляет весь исходящий трафик через одну точку, кэширует страницы Web и осуществляет контроль за разрешенными сервисами Internet внутри и вне сети.

Proxy-сервер может размещаться на той же машине, что и брандмауэр, или устанавливается за ним (в зависимости от имеющегося на диске места). И поскольку настольные системы в компании размещаются часто в нескольких сетевых сегментах, установка proxy-серверов в различных местах, в том числе в удаленных офисах, может снизить рабочую нагрузку на одну машину.

Вполне вероятно, что абсолютно надежных сетей не существует; как только разрешена передача данных в/из Internet, автоматически возникает потенциальная возможность нарушения защиты. В то время как брандмауэр охраняет сеть от атак извне, proxy-сервер контролирует деятельность внутренних пользователей, а значит, при регулировании трафика Internet можно "поймать сразу двух зайцев". Поэтому многие эксперты по безопасности рекомендуют комбинацию брандмауэра и proxy-сервера.



Брандмауэр экспертного уровня...

Брандмауэры экспертного уровня (750)

Эти брандмауэры сочетают в себе элементы всех трех описанных выше категорий. Как и брандмауэры ***с фильтрацией пакетов***, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Брандмауэры экспертного уровня также выполняют функции ***шлюза сеансового уровня***, определяя, относятся ли пакеты к соответствующему сеансу. И наконец, брандмауэры экспертного уровня берут на себя функции ***шлюза прикладного уровня***, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Мой дом — моя крепость

Совет

Брандмауэры экспертного уровня обеспечивают один из самых высоких на сегодня уровней защиты корпоративных сетей, и, по утверждению специалистов, обмануть их не просто. Тем не менее, не стоит забывать, что даже эти надежные брандмауэры не обеспечивают 100%-й безопасности. Тогда целесообразно ли вообще устанавливать брандмауэр? Это нужно делать по той же причине, по которой устанавливается замок на входную дверь, несмотря на то, что ни один замок не может гарантировать полной защиты. Оставив сеть без брандмауэра, вы просто оставляете дверь открытой. Так что "думайте сами, решайте сами...".

Как и шлюз прикладного уровня, брандмауэр экспертного уровня может быть сконфигурирован для отбраковки пакетов, содержащих определенные команды, например команды Put и Get службы FTP. Однако, в отличие от шлюзов прикладного уровня, при анализе данных прикладного уровня такой брандмауэр не нарушает клиент-серверной модели взаимодействия в сети.

Шлюз прикладного уровня устанавливает два соединения: одно — между авторизованным клиентом и шлюзом, второе — между шлюзом и внешним хостом. После этого он пересылает информацию между этими двумя соединениями. Несмотря на высокий уровень защиты, обеспечиваемый подобными шлюзами, такая схема может сказаться на производительности работы.

В противоположность этому б***рандмауэры экспертного уровня допускают прямые соединения между клиентами и внешними хостами***. Для обеспечения защиты такие брандмауэры перехватывают и анализируют каждый пакет на прикладном уровне модели OSI. Вместо применения связанных с приложениями программ-посредников, брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработки данных на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что, теоретически, должно обеспечить более эффективную фильтрацию пакетов.

Поскольку брандмауэры экспертного уровня допускают прямое соединение между авторизованным клиентом и внешним хостом, некоторые утверждают, что брандмауэры этой категории обеспечивают менее высокий уровень защиты, чем шлюзы прикладного уровня.

Рекомендации специалистов

Это важно

Американская Национальная ассоциация по компьютерной безопасности (NCSA) рекомендует политику сетевой защиты каждой компании создавать из двух компонентов: политики доступа к сетевым сервисам и политики реализации брандмауэров.

В соответствии с политикой доступа к сетевым сервисам определяется список сервисов Internet, к которым доступ ограничен. Также определяются ограничения на использование протоколов SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Ограничения методов доступа необходимы для того, чтобы пользователи не могли обращаться к "запрещенным" сервисам Internet обходными путями.

Политика доступа к сетевым сервисам должна основываться на одном из следующих принципов:

- Запретить доступ из Internet во внутреннюю сеть, но разрешить его из внутренней сети в Internet.
- Разрешить ограниченный доступ во внутреннюю сеть из Internet, обеспечивая работу только отдельных, "авторизованных", систем, например почтовых серверов.
- Запрещать все, что не разрешено в явной форме.
- Разрешать все, что не запрещено в явной форме.

Межсетевой экран...

Межсетевые экраны (750)

Межсетевой экран (МЭ) — это полупроницаемая мембрана, расположенная между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). МЭ контролирует все информационные потоки во внутреннюю сеть и из нее. (См. рис. 13_4).

Контроль информационных потоков заключается в их фильтрации, т.е. в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.

Целесообразно разграничить случаи, когда экран устанавливается на границе с внешней (обычно общедоступной) сетью или на границе между сегментами одной корпоративной сети. Соответственно, следует говорить о внешнем и внутреннем межсетевых экранах.

Как правило, при общении с внешними сетями используется исключительно семейство протоколов TCP/IP. Поэтому внешний межсетевой экран должен учитывать специфику этих протоколов. Для внутренних экранов ситуация сложнее: здесь следует принимать во внимание помимо TCP/IP по крайней мере протоколы SPX/IPX, применяемые в сетях Novell NetWare. Иными словами, от внутренних экранов нередко требуется многопротокольность.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, является, скорее, исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования. В этом случае каждое подключение должно защищаться собственным экраном.

Межсетевые экраны целесообразно классифицировать по тому, на каком уровне модели OSI производится фильтрация — канальном, сетевом, транспортном или прикладном. Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

Возможности межсетевого экрана непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Чем выше уровень в модели OSI, на котором функционирует экран, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее экран может быть сконфигурирован.

В то же время фильтрация на каждом из перечисленных уровней обладает своими достоинствами, такими, как дешевизна, высокая эффективность или прозрачность для пользователей. В силу этой, а также других причин, в большинстве случаев используются смешанные конфигурации, в которых объединены разнотипные экраны.

Качество межсетевого экрана определяется еще двумя очень важными характеристиками — простотой применения и собственной защищенностью. В плане простоты использования первостепенное значение имеют наглядный интерфейс при задании правил фильтрации и возможность централизованного администрирования составных конфигураций.

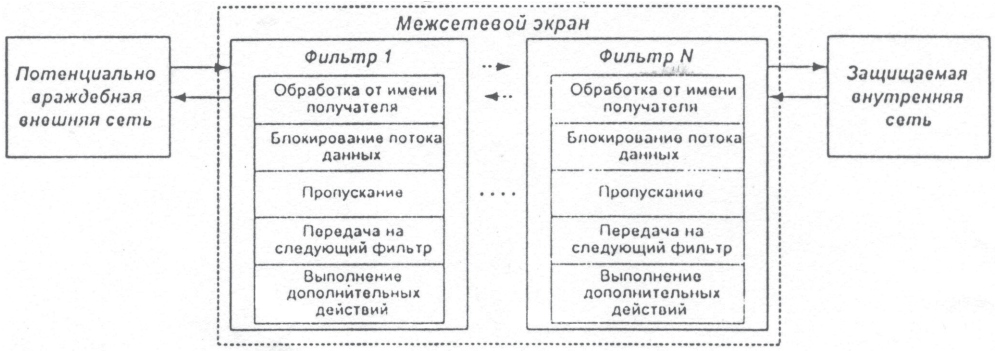


РИС. 13.4.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. При выполнении централизованного администрирования следует также позаботиться о защите информации от пассивного и активного прослушивания сети, т.е. обеспечить ее (информации) целостность и конфиденциальность.

Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Так, прикладной экран может осуществлять действия от имени субъектов внутренней сети, в результате чего из внешней сети кажется, что имеет место взаимодействие исключительно с межсетевым экраном. При таком подходе топология внутренней сети скрыта от внешних пользователей, поэтому задача злоумышленника существенно усложняется.

Резюме

Брандмауэр — это подход к безопасности; он помогает реализовать политику безопасности, которая определяет разрешенные службы и типы доступа к ним, и является реализацией этой политики в терминах сетевой конфигурации, нескольких хостов и маршрутизаторов, и других мер защиты, таких как усиленная аутентификация вместо статических паролей.

Брандмауэр это система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Как правило, эта граница проводится между локальной сетью предприятия и Internet, хотя ее можно провести и внутри локальной сети предприятия.

Система брандмауэра может быть маршрутизатором, персональным компьютером, хостом, или группой хостов, созданной специально для защиты сети или подсети от неправильного использования протоколов и служб хостами, находящимися вне этой подсети.

Основной причиной использования брандмауэров является тот факт, что без брандмауэра системы подсети подвергаются опасности использования уязвимых мест служб, таких NFS и NIS, или сканирования и атак со стороны хостов в Internet. В среде без брандмауэра сетевая безопасность целиком зависит от безопасности хостов, которые должны в этом случае взаимодействовать для достижения одинаково высокого уровня безопасности. Чем больше подсеть, тем труднее поддерживать все хосты на одном уровне безопасности.

Удаленные пользователи — это те пользователи, которые устанавливают соединения с внутренними системами откуда-либо из Internet. Эти соединения могут исходить от любого места в Internet, от модемных линий, от авторизованных пользователей, работающих из дома. В любом случае для всех таких соединения должны использоваться меры усиленной аутентификации брандмауэра перед предоставлением доступа к внутренним системам.

Межсетевой экран — это полупроницаемая мембрана, которая располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети) и контролирует все информационные потоки во внутреннюю сеть и из нее.

Контроль информационных потоков состоит в их фильтрации, то есть в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.