Сетевые экраны

БГА, РТФ
Кафедра ИБ

Зензин Александр Степанович, к.т.н.

Обзор

1. Функции сетевых экранов
2. Пример-аналогия сетевого экрана
3. Типы сетевых экранов разных уровней
4. Реализация сетевых экранов
5. Архитектура сетевых экранов
6. Дополнительные материалы

Функции сетевых экранов

Сетевой, или межсетевой, экран — это комплекс программно-аппаратных средств, осуществляющий информационную защиту одной части компьютерной сети от другой путем анализа проходящего между ними трафика.

Для сетевых экранов существуют и другие термины, хорошо отражающие функциональное назначение средств защиты этого типа:

- **Брандмауэр** — это слово много лет назад пришло в русский язык из немецкого. Изначально оно обозначало перегородку в поезде, отделяющую область топки паровоза от пассажирского отделения.
- **Файервол** и другие транслитерации английского слова firewall, хотя официально не приняты, можно встретить в литературе достаточно часто. Исходным значением этого термина является элемент конструкции дома, а именно стена, сделанная из огнеупорного материала и препятствующая распространению огня между частями дома (обычно принадлежащими разным собственникам).

Для сетевого экрана одна часть сети является внутренней, другая — внешней (рис. 1). Сетевой экран защищает внутреннюю сеть (например, локальную сеть предприятия или, как вырожденный случай, отдельный компьютер пользователя) от угроз, исходящих из внешней сети (мы будем, как правило, подразумевать под такой сетью Интернет).

Защиту границ между локальными сетями предприятия и Интернетом обеспечивают **корпоративные сетевые экраны**, те же функции, но на границе между домашним компьютером и Интернетом, выполняют **персональные сетевые экраны**.

Функции сетевых экранов

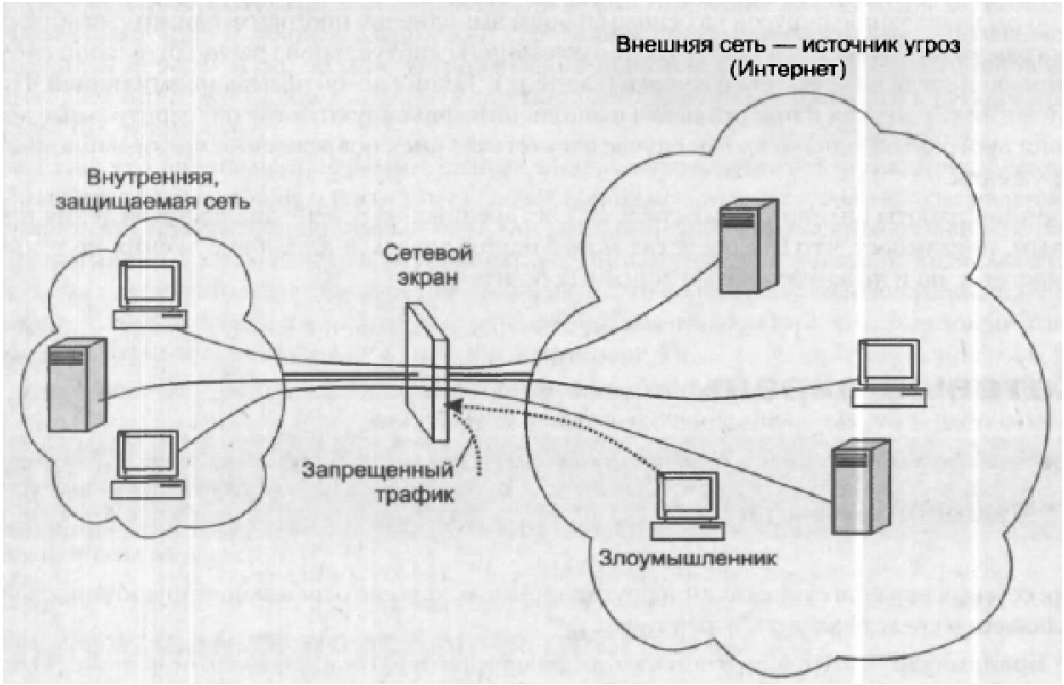

Рис. 1. Сетевой экран защищает внутреннюю сеть от угроз, исходящих из внешней сети.

Для эффективного выполнения сетевым экраном его главной функции — защиты — необходимо, чтобы через него проходил весь трафик, которым обмениваются узлы защищаемой части сети с узлами Интернета.

Такое расположение позволяет сетевому экрану полностью контролировать (запрещать, ограничивать или протоколировать) доступ внешних пользователей к ресурсам внутренней сети. Сетевой экран защищает сеть не только от несанкционированного доступа внешних злоумышленников, но от ошибочных действий пользователей защищаемой сети, например таких, как передача во внешнюю сеть конфиденциальной информации.

Функции сетевых экранов

Чтобы осуществлять контроль доступа, сетевой экран должен уметь выполнять следующие функции:

- анализировать, контролировать и регулировать трафик (функция фильтрации);
- играть роль логического посредника между внутренними клиентами и внешними серверами (функция прокси-сервера);
- фиксировать все события, связанные с безопасностью (функция аудита).

Наряду с этими базовыми функциями на сетевой экран могут быть возложены и другие вспомогательные функции защиты, в частности:

- антивирусная защита;
- шифрование трафика;
- фильтрация сообщений по содержимому, включая типы передаваемых файлов, имена DNS и ключевые слова;
- предупреждение и обнаружение вторжений и сетевых атак;
- функции VPN;
- трансляция сетевых адресов.

Как можно заметить, большинство из перечисленных функций реализуются в виде отдельных продуктов или в составе систем защиты других типов. Так, функции пакетной фильтрации встроены практически во все маршрутизаторы, задача обнаружения вирусов решается множеством разнообразных программ, шифрование трафика — неотъемлемый элемент технологий защищенных каналов и т. д., и т. п.

Функции сетевых экранов

Прокси-серверы часто поставляются в виде приложений, более того, они сами часто **интегрируют** в себе многие функции, свойственные сетевым экранам, такие, например, как аутентификация, трансляция сетевых адресов или фильтрация по содержимому (**контенту**).

Отсюда возникают сложности при определении понятия «сетевой экран». Например, довольно распространено мнение, что сетевой экран — это пограничное устройство, выполняющее пакетную фильтрацию (то есть маршрутизатор), а прокси-сервер — это совершенно отличный от сетевого экрана инструмент защиты. Другие настаивают, что прокси-сервер является непременным и неотъемлемым атрибутом сетевого экрана. Третьи считают, что сетевым экраном может быть названо только такое программное или аппаратное устройство, которое способно отслеживать состояние потока пакетов в рамках соединения.

Мы будем придерживаться широко распространенной точки зрения о том, что сетевой экран — это программно-аппаратный комплекс, выполняющий *разнообразные функции* по защите внутренней сети, набор которых *может меняться в зависимости от типа*, модели и конкретной конфигурации сетевого экрана.

Пример-аналогия сетевого экрана

ПРИМЕР-АНАЛОГИЯ

Функционально сетевой экран можно сравнить с системой безопасности современного аэропорта. Аналогии здесь достаточно очевидные (рис. 24.22) — самолет соответствует защищаемой внутренней сети, а внешняя сеть, из которой приходит потенциально опасный трафик, — внешнему миру, откуда прибывают будущие пассажиры самолета, готовящегося к полету, при этом не все они приезжают с чистыми и ясными намерениями.

В потоке пассажиров, постоянно входящих в здание аэропорта, могут встречаться различные злоумышленники. Наиболее зловещие — террористы — пытаются пронести на борт взрывчатку (в сетевом мире — пакеты, несущие во внутреннюю сеть вирусы, способные «взорвать» серверы и компьютеры пользователей) или оружие для захвата самолета в воздухе (атака по захвату управления удаленным компьютером). Контрабандисты несут с собой незадекларированные ценности (запрещенный контент), а некоторые личности пытаются попасть в самолет по поддельным документам (несанкционированный доступ к внутренним ресурсам сети).

Для того чтобы отфильтровать трафик пассажиров, система безопасности аэропорта пропускает всех пассажиров и их багаж через единственно возможный путь — зону контроля. Также поступают при защите сети, направляя весь входящий трафик через сетевой экран. В зоне контроля аэропорта применяются разнообразные средства проверки пассажиров и их багажа: сличение паспортов с компьютерной базой данных, а лиц пассажиров — с фотографиями в паспортах; просвечивание сумок и чемоданов; проход пассажиров через металлодетекторы, а при первом подозрении — вытряхивание всех вещей; дотошная ручная проверка сумок и прощупывание пассажиров. Между злоумышленниками и службой безопасности постоянно происходит состязание в коварстве, с одной стороны, и находчивости — с другой. Новые трюки вызывают появление новых способов проверки. Например, пронос взрывчатки в подошве ботинка вызвал к жизни не очень приятную обязательную процедуру прохождения металлоискателя в носках, а использование террористами флаконов для маскировки жидких компонентов бомбы лишило пассажиров возможности брать с собой в кабину шампуни и другие любимые жидкости в больших объемах.

Сетевые экраны тоже пытаются использовать все возможные средства и методы для противостояния разнообразным угрозам. С помощью паролей и цифровых сертификатов они проверяют аутентичность внешних узлов, пытающихся установить соединения с внутренними; отслеживают логику обмена пакетами для того, чтобы отразить атаки, основанные на искажении этой логики;

Пример-аналогия сетевого экрана

«просвечивают» содержимое электронных писем и загружаемых документов, пытаясь блокировать запрещенный контент; сканируют загружаемые программы, проверяя их на наличие известных вирусов. Так же как и в зоне контроля аэропорта, здесь постоянно идет соревнование между хакерами, все время изобретающими новые методы атак, и разработчиками сетевых экранов, старающихся эти атаки обнаружить и пресечь.

Рис. 24.22. Зона контроля аэропорта как аналогия сетевого экрана

Типы сетевых экранов разных уровней

Одной из принятых классификаций сетевых экранов является разделение их на типы в зависимости от уровня модели OSI, на котором они работают.

Сетевые экраны сетевого уровня, называемые также **экранами с фильтрацией пакетов** (packet filtering firewall), в полном соответствии со своим названием решают задачу фильтрации пакетов по IP-адресам и портам приложений на основании списков доступа. Фильтрация на основе статических правил, при которой не отслеживаются состояния соединений, называется **простой фильтрацией** (stateless packet inspection). Этому типу сетевых экранов соответствуют маршрутизаторы. Опытный администратор может задать достаточно изощренные правила фильтрации, учитывающие многие требования, касающиеся защиты ресурсов внутренней сети, тем не менее этот тип сетевых экранов уступает по степени защиты другим типам. Преимуществами брандмауэров сетевого уровня являются простота, невысокая стоимость и минимальное влияние на производительность сети.

Сетевые экраны сеансового уровня отслеживают состояние соединений. Они фиксирует подозрительную активность, направленную на сканирование портов и сбор другой информации о сети. *Отслеживание состояний соединений* заключается в том, что сетевой экран проверяет, насколько соответствует последовательность обмена сообщениями контролируемому протоколу.

Типы сетевых экранов разных уровней

То есть, например, если клиент посылает TCP-сообщение SYN, запрашивающее TCP-соединение, сервер должен отвечать TCP-сообщением ЛСК SYN, а не посылать в ответ, например, свой TCP-запрос SYN. После того как сетевой экран установил допустимость TCP-соединения, он начинает работать простым передаточным звеном между клиентом и сервером. Для того чтобы контролировать процесс установления соединения, сетевой экран должен фиксировать для себя текущее состояние соединения, то есть запоминать, какое последнее сообщение отправил клиент и какое сообщение он ожидает получить. Такой подход, когда пропускаются только те пакеты, которые удовлетворяют логике работы соответствующего протокола, называют **фильтрацией с учетом контекста** (stateful packet inspection). Благодаря такой способности брандмауэры сетевого уровня могут защищать серверы внутренней сети от различных видов атак, использующих уязвимости протоколов, в частности от DoS-атак.

Сетевые экраны прикладного уровня способны интерпретировать, анализировать и контролировать содержимое сообщений, которыми обмениваются приложения. К этому уровню относят прокси-серверы, о которых мы будем говорить подробнее далее. Прокси-сервер перехватывает запросы клиентов к внешним серверам с тем, чтобы потом отправить их от своего имени. Этот тип сетевых экранов обеспечивает самый высокий уровень защиты, хотя и имеет свои недостатки, например требует больших вычислительных затрат. Кроме того, прокси-серверы могут скрывать адрес «доверившегося» ему клиента, что снижает эффективность других средств защиты.

Реализация сетевых экранов

Реализация сетевого экрана так же многовариантна, как и его функциональность. В качестве аппаратной составляющей сетевого экрана может выступать маршрутизатор или комбинация маршрутизаторов, компьютер или комбинация компьютеров, комбинация маршрутизаторов и компьютеров, наконец, это может быть специализированное устройство. Таким же разнообразием отличается и программная составляющая сетевого экрана, имеющая гибкую структуру и включающая в себя различные модули, функции которых могут широко варьироваться.

Сложная структура аппаратных и программных средств сетевого экрана, разнообразие настраиваемых параметров, наборы правил, регламентирующих работу фильтров разного уровня, списки паролей и другой информации для проведения аутентификации, списки прав доступа пользователей к внутренним и внешним ресурсам сети — все это требует от администратора значительной дополнительной работы по конфигурированию. Только в случае качественной настройки аппаратуры и программных модулей сетевой экран действительно может стать краеугольным камнем системы защиты сети предприятия. «Умные» сетевые экраны позволяют администратору упростить эту работу, потому что они требуют только задания высокоуровневых правил политики безопасности сети, которые затем автоматически транслируются в низкоуровневые операции по конфигурированию отдельных функциональных подсистем сетевого экрана.

Архитектура сетевых экранов

Простейшей архитектурой сети с сетевым экраном является вариант, когда все функции сетевого экрана реализуются одним программно-аппаратным устройством, например маршрутизатором или, как показано на рис. 2, универсальным компьютером. Такой способ построения защиты логически самый простой, однако он имеет очевидный недостаток, заключающийся в полной зависимости системы защиты от работоспособности одного звена, в данном случае — компьютера-брандмауэра.

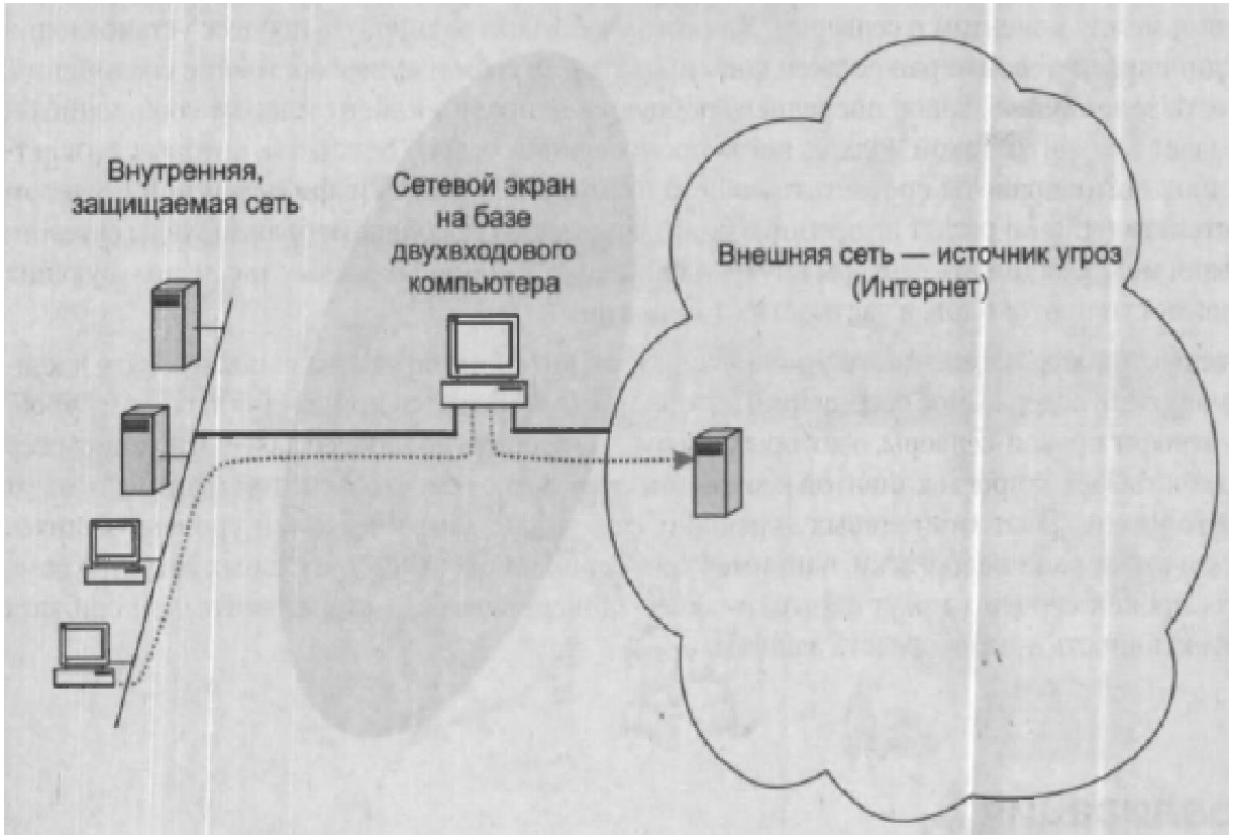

Рис. 2. Сетевой экран на базе двухвходового компьютера

Архитектура сетевых экранов

Компьютер, играющий роль сетевого экрана, должен иметь, по крайней мере, два сетевых интерфейса, к одному из которых подключается внутренняя, к другому — внешняя сеть. Двухвходовой компьютер выполняет функции программного маршрутизатора, а также те функции сетевого экрана, конкретный перечень которых определяется установленным на данном компьютере программным обеспечением.

Более надежные схемы сетевых экранов включают несколько элементов. В сети, показанной на рис. 3, на рубеже защиты установлено два маршрутизатора, между которыми располагается так называемая сеть периметра.

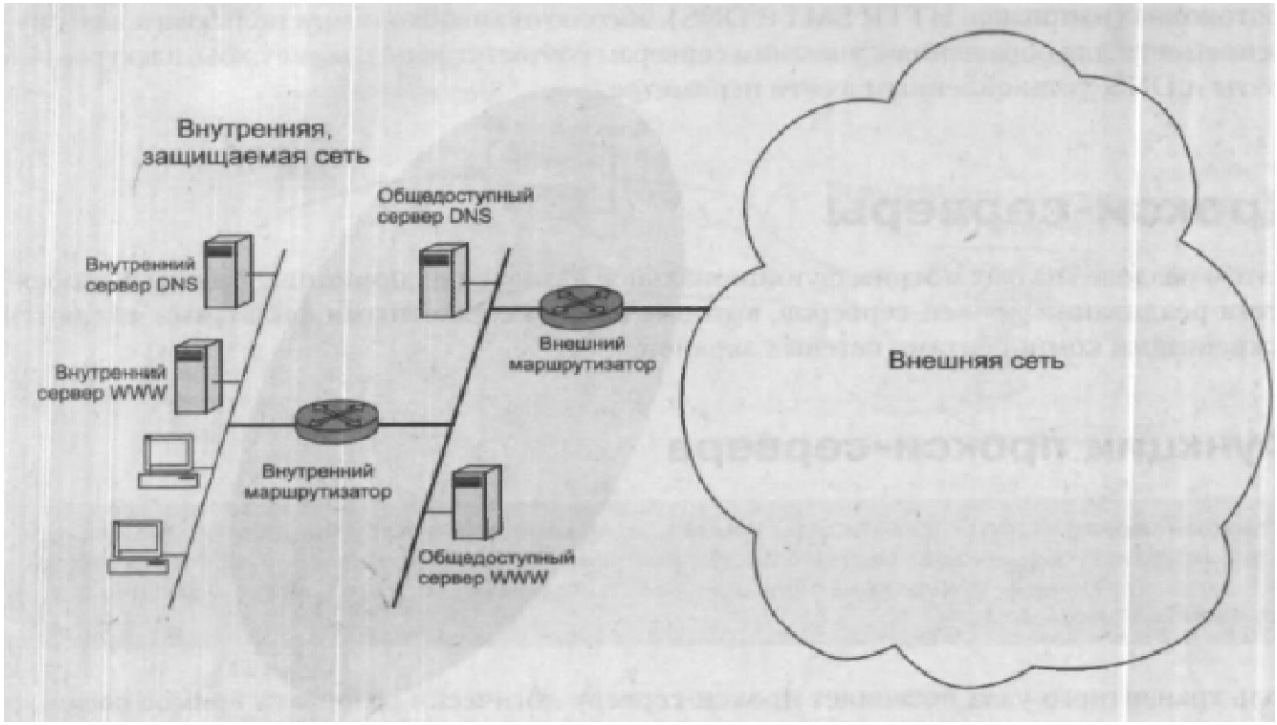

Рис. 3. Сетевой экран на базе двух маршрутизаторов

Архитектура сетевых экранов

Сеть периметра, *или* **сеть демилитаризованной зоны** *(DMZ), — это сеть, которую для добавления еще одного уровня защиты внутренней сети размещают между внутренней и внешней сетями в качестве буфера.*

В сети периметра обычно располагаются компьютеры, которые предоставляют общедоступные сервисы, например почтовый сервер, внешний сервер DNS или внешний веб-сервер предприятия. В этой зоне могут быть размещены также прокси-серверы. Учитывая, что само назначение этих компьютеров предполагает практически никак не ограничиваемый доступ к ним внешних пользователей (а значит, и злоумышленников), их необходимо защищать особенно тщательно. Главными задачами при защите этих компьютеров (называемых иногда **компьютерами-бастионами**) является обеспечение целостности и доступности размещенных на них данных для пользователей внешней сети. Эту задачу решают «индивидуальные» средства защиты, устанавливаемые на компьютерах-бастионах, такие, например, как антивирусные программы или фильтры спама.

Чтобы пояснить, каким образом сеть периметра усиливает защиту внутренней сети, давайте посмотрим, что произойдет, если какой-либо злоумышленник сможет «взломать» первый рубеж защиты — внешний маршрутизатор — и начнет прослушивать трафик подключенной к нему сети периметра. Очевидно, что он получит доступ только к трафику общедоступных серверов, который не является секретным.

Архитектура сетевых экранов

Внешний маршрутизатор призван фильтровать трафик с целью защиты сети периметра и внутренней сети. Однако строгая фильтрация в этом случае оказывается невостребованной. Общедоступные серверы по своей сути предназначены для практически неограниченного доступа. Что касается защиты внутренней сети, правила фильтрации для доступа к ее узлам и сервисам являются одними и теми же для обоих маршрутизаторов, поэтому внешний маршрутизатор может просто положиться в этом деле на внутренний маршрутизатор.

Обычно внешний маршрутизатор находится в зоне ведения провайдера, и администраторы корпоративной сети ограничены в возможностях его оперативного реконфигурирования. Это является еще одной причиной, по которой функциональная нагрузка на внешний маршрутизатор обычно невелика.

Основная работа по обеспечению безопасности локальной сети возлагается на *внутренний маршрутизатор*, который защищает ее как от внешней сети, так и от сети периметра. Правила, определенные для узлов сети периметра по доступу к ресурсам внутренней сети, часто бывают более строгими, чем правила, регламентирующие доступ к этим ресурсам внешних пользователей. Это делается для того, чтобы в случае взлома какого-либо компьютера-бастиона уменьшить число узлов и сервисов, которые впоследствии могут быть атакованы с этого компьютера. Именно поэтому внутренний маршрутизатор должен отбрасывать все пакеты, следующие во внутреннюю сеть из сети периметра, исключая пакеты нескольких протоколов (например, HTTP, SMTP, DNS), абсолютно необходимых пользователям внутренней сети для обращения к внешним серверам соответственно веб-службы, электронной почты и DNS, установленным в сети периметра.

Дополнительные материалы для изучения
Система Firewall

Учитывая важность проблемы защиты, разработана специальная система **firewall** ("огненная стена" или брандмауэр). Первые Firewall появились в конце 80-х годов, в 1991 году фирма DEC предложила устройство **SEAL** (Secure External Access Link), устройства же современного типа появились в 1993 году (**TIS** – Trusted Information System – защищенные ИС). Система **firewall** заменяет маршрутизатор или внешний порт сети (gateway). Защищенная часть сети размещается за ним. Пакеты, адресованные Firewall, обрабатываются локально, а не просто переадресуются. Пакеты же, которые адресованы объектам, расположенным за Firewall, не доставляются. По этой причине хакер вынужден иметь дело с системой защиты ЭВМ Firewall. Схема взаимодействия Firewall с локальной сетью и внешним Интернет показана на рис. 4.

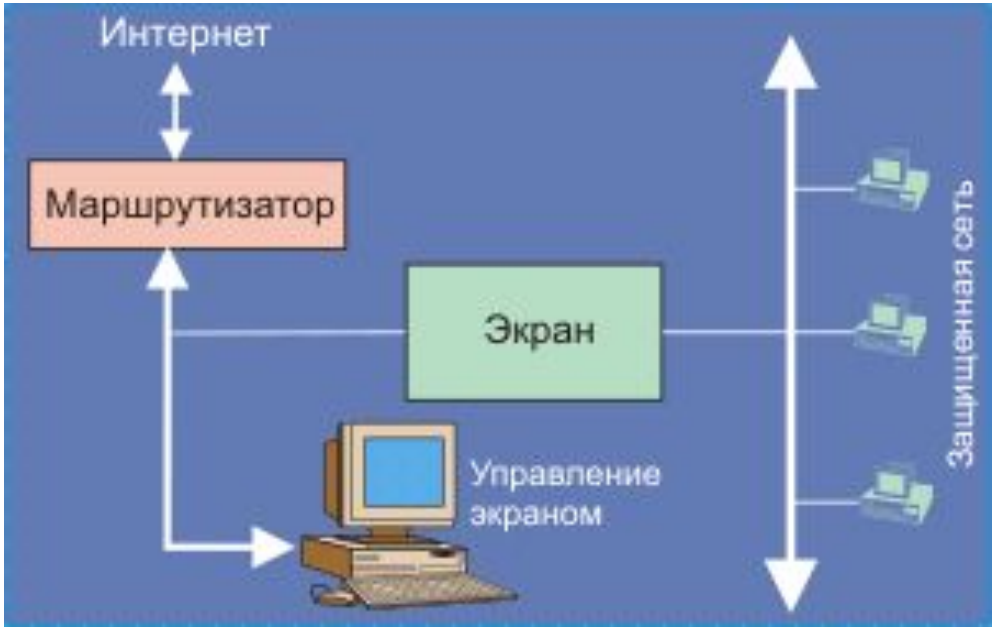

Рис. 4. Схема Firewall

Такая схема проще и надежнее, так как следует заботиться о защите одной машины, а не многих. Экран, маршрутизатор и ЭВМ управления экраном объединены небольшой, незащищенной локальной сетью. Основные операции по защите осуществляются здесь на IP-уровне. Эту схему можно реализовать и на одной ЭВМ, снабженной двумя интерфейсами. При этом через один интерфейс осуществляется связь с Интернет, а через второй - с защищенной сетью. Такая ЭВМ совмещает функции маршрутизатора-шлюза, экрана и управления экраном. Возможна реализация Firewall, показанная на рис 5. Здесь функция экрана выполняется маршрутизатором, но и прокси может выполнять некоторые защитные функции. Возможен вариант прокси-сервера и с одним сетевым интерфейсом. Эту схему можно реализовать и на одной ЭВМ, снабженной двумя интерфейсами. При этом через один интерфейс осуществляется связь с Интернет, а через второй - с защищенной сетью.

Рис. 5. Схема Firewall, где функцию экрана выполняет маршрутизатор

В этой схеме доступ из Интернет возможен только к прокси-серверу, ЭВМ из защищенной сети могут получить доступ к Интернет тоже только через прокси-сервер. Ни один пакет посланный из защищенной ЭВМ не может попасть в Интернет и, аналогично, ни один пакет из Интернет не может попасть непосредственно защищенной ЭВМ. Возможны и другие более изощренные схемы, например со вторым "внутренним" Firewall для защиты от внутренних угроз.

Вне зависимости от того, насколько надежен ваш сетевой экран, не следует снижать требования к безопасному конфигурированию рабочих станций и серверов.
Следует также помнить, что сетевой экран не способен защитить от вирусов, сетевых червей, троянских коней, **атак из локальной сети** и различных мошеннических трюков ("социальная инженерия"). Но самой серьезной угрозой являются "новые" неизвестные доселе атаки. Существует несколько разновидностей Firewall.

Фильтрующие Firewall

Фильтрующая разновидность сетевых экранов производит отбор пакетов по содержимому заголовков (адреса и номера портов). Но такие экраны не могут различить команду get от put, так как для этого надо просматривать поле данных. Функции таких сетевых экранов могут быть реализованы практически любым маршрутизатором.

Прокси Firewall

Сетевые экраны на основе прокси-серверов способны анализировать не только заголовки, но и пересылаемые данные. Такие серверы исключают прямое соединение клиента и удаленного сервера. От имени клиента запрос посылает сетевой экран. Для большой сети целесообразно иметь отдельные машины для прокси-серверов, обеспечивающих разные виды услуг (WWW, FTP и пр.), см. рис. 6 и 6А.

Рис. 6. Размещение WEB-сервера в демилитаризованной зоне

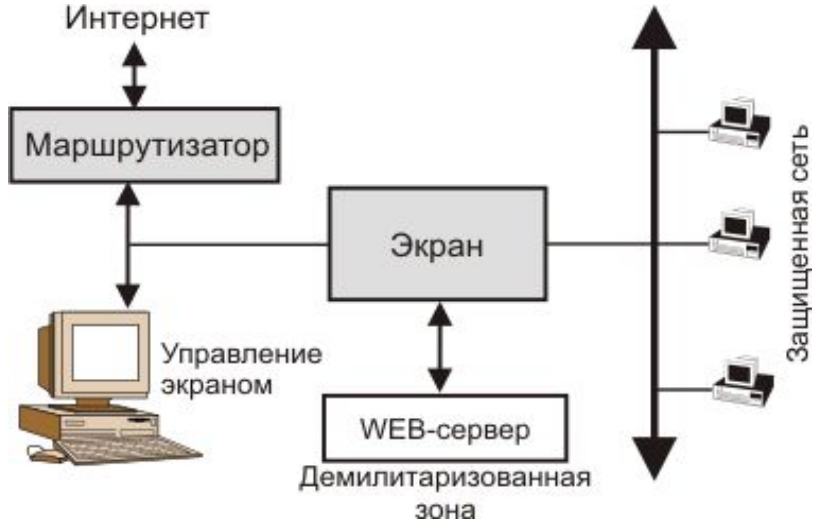

Рис. 6а. Вариант построения демилитаризованной зоны с помощью сетевого экрана с 3-мя интерфейсами

Разные серверы для разных услуг помимо безопасности пропорционально увеличивают быстродействие системы в целом.

На рисунках показаны два (но не единственных) варианта защиты сети с помощью сетевого экрана, построенного на основе прокси-сервера и имеющего “демилитаризованную” зону. В такой зоне обычно размещаются серверы, доступные из Интернет непосредственно (вне защищаемого контура). Такие серверы бывают нужны для рекламирования изделий фирмы, обслуживания клиентов или для демонстрации достижений учреждения или научного центра. Такие схемы сохраняют доступность вашего WEB-сервера со стороны поисковых систем, что позволит узнать о вашей компании или учреждении большему количеству людей. Вариант на рис. 6А несколько гибче, но требует трех сетевых интерфейсов для прокси-сервера. Существуют аппаратные решения, совмещающие многие из описанных здесь возможностей.

Следует помнить, что подключение через модем должно производиться через специальный защищенный сервер с поддержкой протоколов типа Radius. Наилучшее для него место размещения - демилитаризованная зона, ведь безопасность сети определяется ее самым уязвимым элементом.

При выборе политики и правил отбора пакетов важно ответить на следующие вопросы:

- Какие сетевые услуги вы желаете реализовать и для каких направлений (изнутри и снаружи)?
- Следует ли ограничивать “внутренних” клиентов в части подключения к серверам в Интернет?
- Имеются ли узлы в Интернет, для которых вы бы хотели создать особые условия доступа (например, филиалы вашего учреждения)?

Обычно сетевым экраном реализуется одна из двух политик безопасности:

- разрешено все, что не запрещено правилами;
- запрещено все, что не разрешено правилами.

На первый взгляд может показаться, что эти две политики неотличимы, но это совсем не так. В первом варианте при появлении нового приложения или протокола придется вводить новые ограничительные правила. Второй вариант политики консервативнее и здесь реже приходится менять правила.

Прокси-сервер обычно привязан к конкретному типу приложений и способен разрешать или запрещать выполнение определенных операций. Рассмотрим, как внутренним клиентом через такого рода сервер может быть загружена определенная WEB-страница с сервера в Интернет.

Дополнительные материалы для изучения
Система Firewall

Прямое соединение внутреннего клиента с внешним сервером через сетевой экран невозможно. Прокси-сервер посылает HTTP-запрос внешнему серверу от своего имени с IP-адреса своего внешнего интерфейса, подключенного к Интернет. Понятно, что и отклик от внешнего WEB-сервера придет через указанный интерфейс в прокси-сервер. После получения запрошенной WEB-страницы прокси-сервер производит определенные администратором проверки, после чего открывает сессию передачи полученных данных через свой интерфейс LAN клиенту-заказчику. На фазе проверок возможна сортировка данных и блокировка доступа клиента к определенному типу данных, например, порнографического вида.

Вообще фильтрация данных стала в последнее время широко обсуждаемой проблемой. Отбор может производиться по URL, хотя этот способ селекции мало эффективен, во-первых, потому что URL часто меняются, во-вторых, из-за того, что клиент может всегда заменить URL на IP-адрес. Надежда на то, что в ограничительный список можно включить и IP-адреса, напрасна, так как некоторые программы могут воспринимать IP-адрес в десятичном (а не в десятично-точечном) представлении. Существуют и более изощренные фильтры, где содержимое анализируется по ключевым словам или по характеру вложений (Java или ActiveX).

Выбирая правила фильтрации, нужно сначала сформулировать общую стратегию:

- какие сервисы в сети нужно обеспечить и в каком направлении (изнутри вовне или извне внутрь);
- какие ограничения на выход в Интернет для внутренних машин вы готовы установить;
- имеются ли внешние машины, для которых вы готовы предоставить какие-то формы доступа в вашу сеть.

Дополнительные материалы для изучения
Система Firewall

В разных системах межсетевых экранов правила фильтрации формулируются различным образом, но, как правило, требуются следующие данные:

- в каком направлении и через какой интерфейс передаются пакеты;
- IP-адреса отправителя и получателя;
- допустимые опции IP;
- используемые протоколы высокого уровня (UDP, TCP, ICMP);
- допустимые типы ICMP-сообщений;
- номера портов отправителя и получателя (для протоколов (UDP и TCP).

Некоторые протоколы желательно отфильтровывать из-за их потенциальной опасности. Работа с ними допускается лишь на специально выделенных машинах.

1. Порт 23 (Telnet), не должен использоваться вообще или использоваться для исследовательских целей на одной ЭВМ.
2. Порты 20 и 21 (FTP) лучше закрыть везде, но, в крайнем случае, их можно открыть при необходимости на одном FTP-сервере.
3. Порт 25 (SMTP) обычно разрешается только на центральном почтовом сервере.
4. Порт 53 (DNS) открывается только для серверов имен (первичного и вторичного).
5. Порт 520 (RIP) может быть использован для перенаправления потока данных. Если можно обойтись без протокола маршрутизации RIP, это следует сделать.
6. Порты 70 (Gopher) и 80 (WWW) должны быть открыты только для шлюзов соответствующих приложений.
7. Порт 119 (NNTP -служба новостей) должен использоваться только сервером новостей.
8. Порт 79 (Finger) желательно закрыть, так как через него может быть получена полезная для хакера персональная информация.

9. Порт 69 (TFTP) безоговорочно должен быть закрыт для любых внешних пользователей. Открытие для внутренних пользователей должно осуществляться в случае крайней необходимости для выбранных IP-адресов.
0. Порт 540 (UUCP) лучше заблокировать из-за его уязвимости (сама услуга устарела).

В принципе, прокси-серверы могут работать в обоих направлениях, т.е. обеспечивать внешним клиентам доступ к внутренним серверам. Обеспечивая сокрытие данных о клиентах и структуре внутренней сети, прокси-серверы становятся критической точкой системы в целом. Взлом или выход из строя такого устройства может парализовать работу большого числа людей.

Существуют так называемые прозрачные прокси-серверы. Такие серверы создают больший комфорт клиентам, ведь не нужно авторизоваться сначала в прокси или как-то адаптировать свое программное обеспечение. Для клиента создается впечатление, что он работает непосредственно с внешним сетевым объектом, он может даже не знать о существовании прокси. Запросы внутреннего клиента к внешнему серверу перехватываются прокси-сервером и после анализа блокируются или передаются во внешнюю сеть. Пользователь авторизуется на внешнем сервере, а не в прокси. Но у прокси остается возможность блокировки некоторых операций, например, GET или PUT. Прокси может вести журнал операций или предоставлять различные права разным клиентам. Следует заметить, что прозрачный сервер не скрывает IP-адреса внутренних клиентов. Если прокси организует подключение внешнего клиента к внутреннему серверу, для внутреннего сервера клиентом является прокси, а не внешний объект. Но внешний объект знает IP-адрес внутреннего сервера.

Ситуацию можно несколько улучшить, если поместить все внутренние серверы в демилитаризованную зону, тогда хакер не получит никаких данных об остальных объектах внутренней сети. Внутренние серверы в этом случае должны быть дополнительно защищены, например, локальными программами типа Firewall.

В случае классического прокси клиенту нужно знать имя прокси и ЭВМ, с которой он хочет взаимодействовать. Имя прокси клиент должен преобразовать в его IP-адрес, послав запрос в DNS, а имя ЭВМ передать прокси-серверу в качестве параметра запроса. DNS в этом случае сообщает внутренние IP-адреса только внутренним сетевым объектам. Для работы с внешними IP-адресами служит другой DNS-сервер. В случае же прозрачного прокси схема взаимодействия с DNS идентична той, которая существует при отсутствии сетевого экрана.

Для прокси-серверов достаточно типично использование трансляции сетевых адресов **NAT** (Network Address Translation). Такая схема, среди прочего, позволяет обойтись меньшим числом реальных IP-адресов. При реализации запросов во внешнюю сеть программа NAT подставляет в поле адрес отправителя IP сервера NAT. При получении отклика программа NAT заносит в поле адреса получателя адрес клиента источника запроса.

Существуют сетевые услуги, которые следует блокировать сетевым экраном:

- **NFS (Network File System)**. В случае разрешения доступа к этой услуге через сетевой экран, на удаленной машине можно будет смонтировать файловую систему вашей сети и делать с ней все что угодно…
- **NIS** (Network Information System - сетевая информационная система). Эта система позволяет хакерам узнать нужные им имена узлов и пользователей в вашей сети.
- **X-windows**. По уязвимости эта услуга сравнима с Telnet, допускает удаленный запуск процессов.

Не следует оставлять без внимания безобидный на первый взгляд протокол ICMP, так как он позволяет получить много разнообразной и полезной для хакера информации. По этой причине целесообразно блокировать прохождение ICMP-пакетов следующих типов:

- Входящие *echo request* и исходящие *echo replay*. Это сохранит возможность для внутренних клиентов тестировать доступность узлов Интернет, но не даст зондировать ваши внутренние сетевые объекты.
- Входящие сообщения redirect. Такие сообщения позволяют модифицировать таблицу маршрутизации.
- Входящие сообщения service unavailable и исходящие destination unreachable. Это препятствует хакеру зондирование вашей сети. Если хакер может узнать, доступны ли нужные ему узлы или службы, это существенно упростит его задачу.

Дополнительные материалы для изучения
Система Firewall

Если вы поставили и сконфигурировали Firewall, не следует расслабляться. Во-первых, ваш сетевой экран защитит вашу сеть не от всех потенциальных угроз (например, вирусы, сетевые черви, троянские кони, доставляемые по почте, не в его сфере возможностей). Во-вторых, если за экраном не вы один, то вас могут обслужить по части сетевых проблем ваши соседи по локальной сети. По этой причине нужно позаботиться об уязвимости ваших внутренних серверов и рабочих станций.

Расстаньтесь с услугами rlogin, rcp, rexec, telnet (замените на ssh), так как с ними работать удобно не только вам, но и хакерам. По возможности замените услуги FTP на SFTP или scp. Загляните в конфигурационный файл /etc/inetd.conf, а также в /etc/rc.* и удалите все ненужные и потенциально опасные услуги и приложения, например, finger. Не оставляйте без внимания и такие файлы как */etc/networks, /etc/protocols, /etc/services, /etc/hosts*.

Если сетевой экран работает на ЭВМ с ОС Windows, там не должно быть файловой системы FAT, так как она не обеспечивает защиты.

В последнее время появился новый вид услуг - MFWS (Managed Firewall Service). Компании, предоставляющие такую услугу, берутся за настройку и управление сетевыми экранами клиента. Сами сетевые экраны могут располагаться у клиента или сервис-провайдера. О настройке межсетевых экранов смотри firewallbyhand.txt.

Недостатки системы Firewall происходят от ее преимуществ, осложняя доступ извне, система делает трудным и доступ наружу. По этой причине система Firewall должна выполнять функции DNS (сервера имен) для внешнего мира, не выдавая никакой информации об именах или адресах внутренних объектов, функции почтового сервера, поддерживая систему псевдонимов для своих клиентов. Псевдонимы не раскрываются при посылке почтовых сообщений во внешний мир.

Система Firewall

Служба FTP в системе может и отсутствовать, но если она есть, доступ возможен только в сервер Firewall и из него. Внутренние ЭВМ не могут установить прямую FTP-связь ни с какой ЭВМ из внешнего мира. Процедуры telnet и rlogin возможны только путем входа в сервер Firewall. Ни одна из ЭВМ в защищенной сети не может быть обнаружена с помощью PING (ICMP) извне. И даже внутри сети будут возможны только определенные виды трафика между строго определенными машинами.

Понятно, что в целях безопасности защищенная сеть не может иметь выходов во внешний мир помимо системы экран, в том числе и через модемы. Экран конфигурируется так, чтобы маршрут по умолчанию указывал на защищенную сеть. Экран не принимает и не обрабатывает пакеты внутренних протоколов маршрутизации (например, RIP). ЭВМ из защищенной сети может адресоваться к экрану, но при попытке направить пакет с адресом из внешней сети будет выдан сигнал ошибки, так как маршрут по умолчанию указывает назад в защищенную сеть.

Для пользователей защищенной сети создаются специальные входы для FTP/scp, telnet/ssh и других услуг. При этом не вводится каких-либо ограничений по транспортировке файлов в защищенную сеть и блокируется передача любых файлов из этой сети, даже в случае, когда инициатором FTP-сессии является клиент защищенной сети. Единственные протоколы, которым всегда позволен доступ к ЭВМ Firewall являются SMTP (электронная почта) и NNTP (служба новостей).

Внешние клиенты Интернет не могут получить доступа ни к одной из защищенных ЭВМ ни через один из протоколов. Если нужно обеспечить доступ внешним пользователям к каким-то данным или услугам, для этого можно использовать сервер, подключенный к незащищенной части сети (или воспользоваться услугами ЭВМ управления экраном, что нежелательно, так как снижает безопасность).

Дополнительные материалы для изучения
Система Firewall

ЭВМ управления экраном может быть сконфигурирована так, чтобы не воспринимать внешние (приходящие не из защищенной сети) запросы типа FTP/scp, telnet/ssh и пр., это дополнительно повысит безопасность.

Стандартная система защиты здесь часто дополняется программой wrapper. Немалую пользу может оказать и хорошая система регистрации всех сетевых запросов.

Системы Firewall часто используются и в корпоративных сетях, где отдельные части сети удалены друг от друга. В этом случае в качестве дополнительной меры безопасности применяется шифрование пакетов. Система Firewall требует специального программного обеспечения.

Следует иметь в виду, что сложная и дорогостоящая система Firewall не защитит от “внутренних” злоумышленников. Нужно тщательно продумать систему защиты модемных каналов (сама система Firewall на них не распространяется, так как это не внешняя часть сети, а просто удаленный терминал). Хороший результат можно получить, совместно обрабатывая журнальные файлы IDS и Firewall.

Если требуется дополнительная степень защиты, при авторизации пользователей в защищенной части сети могут использоваться **аппаратные средства идентификации**, а также шифрование имен и паролей.

В последнее время появилось большое число аппаратных решений для межсетевых экранов. Это, прежде всего CISCO PIX Firewall.

Но крайне интересное предложение поступило от компании 3COM (см. www.3com.com/products), где Firewall встроен в сетевой интерфейс и снабжен программным обеспечением, позволяющим мониторировать состояние группы таких интерфейсов.

Дополнительные материалы для изучения
Система Firewall

При выборе той или иной системы Firewall следует учитывать ряд обстоятельств.

1. **Операционная система**. Существуют версии Firewall, работающие с UNIX и Windows NT. Некоторые производители модифицируют ОС с целью усиления безопасности. Выбирать следует ту ОС, которую вы знаете лучше.
2. **Рабочие протоколы**. Все Firewall могут работать с FTP (порт 21), e-mail (порт 25), HTTP (порт 80), NNTP (порт 119), Telnet/ssh (порт 23/22), Gopher (порт 70), SSL (порт 443) и некоторыми другими известными протоколами. Как правило, они не поддерживают SNMP.
3. **Типы фильтров**. Сетевые фильтры, работающие на прикладном уровне прокси-сервера, предоставляют администратору сети возможность контролировать информационные потоки, проходящие через Firewall, но они обладают не слишком высоким быстродействием. Аппаратные решения могут пропускать большие потоки, но они менее гибки. Существует также “схемный” уровень прокси, который рассматривает сетевые пакеты, как черные ящики и определяет, пропускать их или нет. Отбор при этом осуществляется по адресам отправителя, получателя, номерам портов, типам интерфейсов и некоторым полям заголовка пакета.
4. **Система регистрации операций**. Практически все системы Firewall имеют встроенную систему регистрации всех операций. Но здесь бывает важно также наличие средств для обработки файлов с такого рода записями.
5. **Администрирование**. Некоторые системы Firewall снабжены графическими интерфейсами пользователя. Другие используют текстовые конфигурационные файлы. Большинство из них допускают удаленное управление.
6. **Простота**. Хорошая система Firewall должна быть простой. Прокси-сервер (экран) должен иметь понятную структуру и удобную систему проверки. Желательно иметь тексты программ этой части, так как это прибавит ей доверия.

Дополнительные материалы для изучения
Система Firewall

К средствам мониторинга сетевых атак относятся такие программные продукты, как SNORT (IDS), для предотвращения атак используются различные системы типа Firewall.

Интересные возможности предоставляет программный пакет **TCP Wrapper**, который использует демон tcpd, запускаемый вместо сетевых служб, указанных в файле inetd.conf. TCP wrapper позволяет разрешить доступ только с определенных узлов, находящихся в вашей сети. Кроме того, эта программа регистрирует запросы к сервисам и имена (адреса) узлов, откуда они поступили. Это ее свойство может быть крайне полезной при анализе, который нужно проводить при подозрении вторжения.

Хорошего результата можно достичь, грамотно конфигурируя программное обеспечение ЭВМ и контролируя качество паролей. Пример фрагмента журнального файла ZoneAlarm (разновидность Firewall) представлен ниже:

FWIN,2005/08/19,14:25:04 +4:00 MT,61.235.154.103:44666,194.85.70.31:1027,UDP
FWIN,2005/08/19,14:39:36 +4:00 GMT,220.168.156.70:37740,194.85.70.31:1026,UDP
FWIN,2005/08/19,14:39:36 +4:00 GMT,220.168.156.70:37740,194.85.70.31:1027,UDP
FWIN,2005/08/19,14:44:34 +4:00 GMT,222.241.95.69:32875,194.85.70.31:1027,UDP

Эта распечатка демонстрирует попытки прощупывания ЭВМ с IP-адресом 194.85.70.31 на предмет откликов со стороны портов 1026 и 1027 (протоколы cap и exosee). Зондирование производится с нескольких разных адресов (61.235.154.103, 220.168.156.70 и 222.241.95.69). Объектом атаки в данном случае является рабочая станция, которая не поддерживает эти протоколы.

После проникновения хакер старается ликвидировать следы своей работы и в то же время оставить для себя “калитку”. Сделать это он может, заведя новую учетную запись или загрузив троянского коня. По этой причине нужно регулярно проверять список учетных записей и сканировать машину на предмет наличия троянских коней и spyware.

В последнее время возникли новые угрозы - вторжения через приложения, когда для распознавания атаки нужно просматривать не только заголовки пакета (уровни L3-L4), но и поле данных. Для борьбы с такими попытками вторжений создаются Firewall нового типа для распознавания *атак на прикладном уровне*. Кроме того, современные Firewall при фильтрации URL используют их репутацию, это же касается и IP-адресов.

В Интернет можно найти утверждения, что Firewall можно легко обойти. Отчасти это верно. Но не следует из этого делать вывод, что можно обойтись без этого средства защиты. Во-первых, нужно стремиться максимально осложнять жизнь хакерам, во-вторых, хакер всегда предпочтет найти более легкую мишень для атаки, взломав, например, незащищенный сервер соседа (☻).

Дополнительные материалы для изучения
Система Firewall

Информацию по системам Firewall можно найти по следующим адресам.

URL	Содержание
http://search.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html	Автоматическая конфигурация прокси для Netscape и Microsoft броузеров
http://www.software.digital.com	Alta Vista Firewall
http://www.cyberguardcorp.com/	CyberGuard Firewall
http://www.raptor.com/	Eagle Firewall
http://www.checkpoint.com/	Firewall-1
http://www.tis.com/	Gauntlet Firewall
http://www.on.com/	ON Guard Firewall
http://www.sctc.com	BorderWare Firewall
ftp://ftp.nec.com/pub/socks/	SOCKS прокси
ftp://ftp.tis.com/pub/firewalls/toolkit	Средства для работы с Firewall
majordomo@greatcircle.com	Подписной лист по проблематике Firewall. Для подписки в тело сообщения следует поместить subscribe firewall. Там же имеется архив: http://www.greatcircle.com/firewalls

Прикладные Firewall

Сегодня 75% успешных Интернет атак (данные Gartner Inc.) использует уязвимости приложений. WEB-приложения также часто являются объектами сетевых атак. Безопасность таких приложений обеспечивается специальными программами - "прикладными Firewall". Смотри Application Firewalls.

Несмотря на то что 98% компаний имеют традиционные Firewall, а 69% - оснащены системами IDS/IPS, они становятся мишенями атак. Названные средства в основном анализируют заголовки пакетов (IP-адреса и номера портов), а прикладные порты, например, порт=80 для WEB-приложений всегда открыт. Для обеспечения безопасности нужно достаточно глубоко анализировать поле данных. Существуют специальные программы для сканирования уязвимости приложений. При этом анализируются десятки параметров и в конечном итоге блокируются тысячи уязвимостей.

Но реально на рынке пока достаточно мало средств противодействия атакам против приложений.

Прикладными Firewall [4, 6] используют знания о специфических особенностях приложения для блокировки вредоносных запросов, обеспечивая защиту не на сетевом, а на прикладном уровне. Такие программы пригодны для защиты WEB-, SOA и XML-приложений. Хакер при таких атаках входит в систему как легальный пользователь, затем меняет свой уровень привилегий и получает доступ в зоны, куда доступ обычным пользователям запрещен. Эти средства защиты предполагают контроль не только входного трафика, но и выходного. С учетом того, что большинство видов электронного бизнеса мигрирует в область WEB-технологий, прикладные Firewall будут весьма востребованы. Разумеется, это не исключает применения всех других средств сетевой защиты.

Особую разновидность прикладных Firewall составляют **WAF** (WEB-application Firewall), которые имеют целью защиту на прикладном уровне.

Следует иметь в виду, что со многих точек зрения IPS (система предотвращения вторжения) эффективнее Firewall. Современные Firewall и IPS могут работать с входными потоками до 10 Гбит/с. Эти системы для распознавания атак используют как сигнатуры, так детектирование аномального поведения.

К 2009 году сложилась технология FireWall нового поколения, базирующаяся на **UTM** (Unified Threat Management). Эта технология объединяет в себе традиционные методы и IPS. Анализ трафика производится не только на уровнях L3-L4, но и на прикладном уровне. На текущий момент такие приборы составляют не более 1%, но ожидается, что к 2018 году их число достигнет 45% от общего числа Firewall.

На практике число Firewall, используемых в одной сети, зависит от поставленной задачи. Помимо главного Firewall, отделяющего сеть от Интернет, могут существовать Firewall, защищающие отдельные серверы (DNS, NTP, SMTP) или даже отдельные рабочие станции. В последнем случае речь идет об установленных там программах. Поставив Firewall на входе, например, вашего почтового сервера, вы можете в несколько раз сократить объем приходящего SPAM.

Система Firewall

Схема защиты с несколькими Firewall показана на рис. 7. См. The Essential Guide for Upgrading your Network.

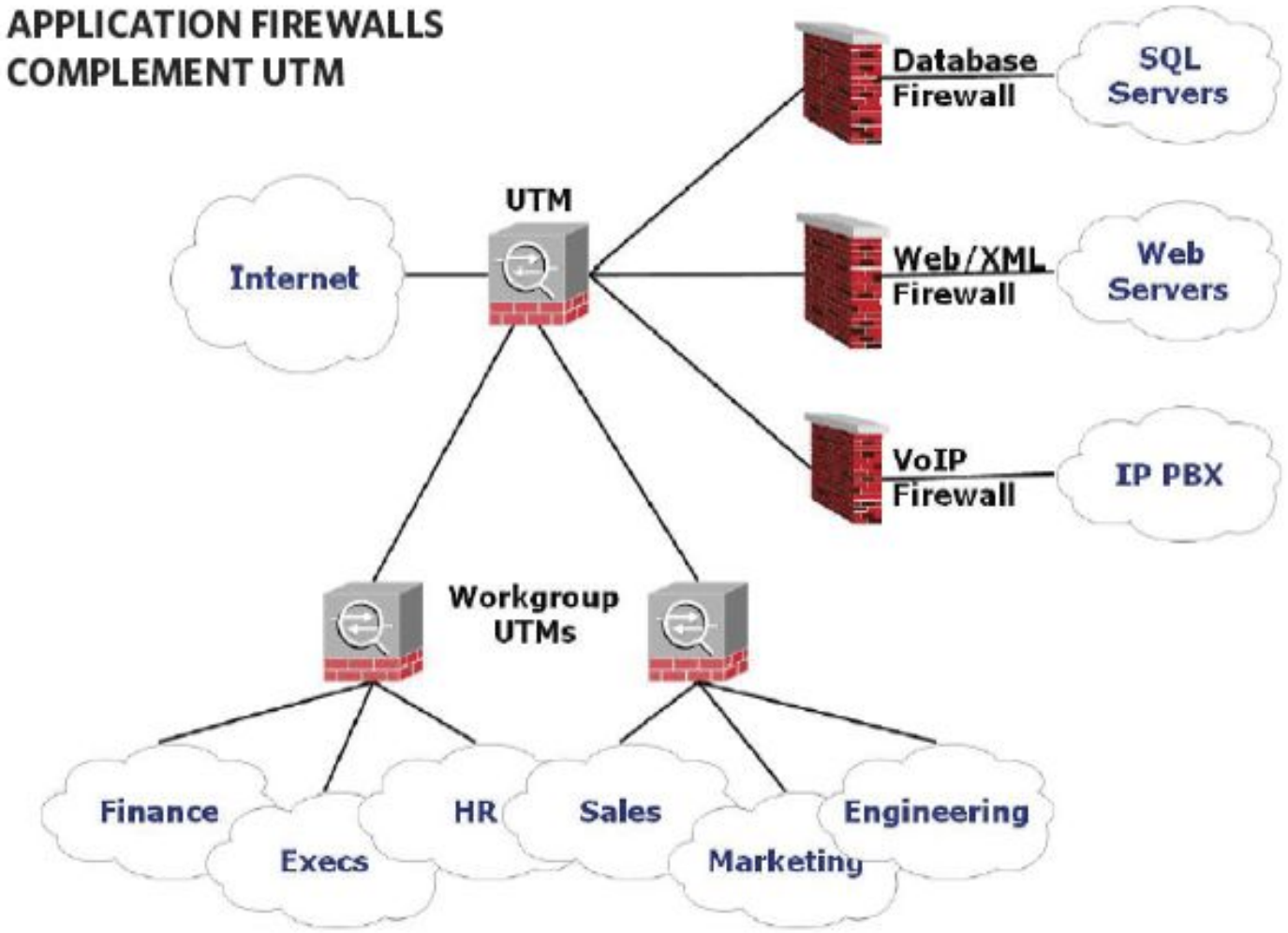

Рис. 7. Вариант системы Firewall, настроенных на разные задачи

Дополнительные материалы для изучения
Система Firewall

Firewall почтового сервера должен контролировать не только входящий трафик, но и исходящий. Так можно выявлять взлом машин локальной сети и превращение их в зомби для рассылки SPAM. При этом в сети нужно запретить посылку почты непосредственно из рабочей станции, минуя почтовый сервер.

Цена Firewall зависит от полосы канала и в 2009 году составляла 5000$ за гигабит в секунду [3].

Ниже в таблице перечислены опции современных Firewall и их функции [5].

Технология	**Решаемая проблема**
Анализ состояния	Блокировка всех нежелательных протоколов
Firewall рабочей станции	Защищает от DoS-атак
Глубокий анализ пакетов (DPI)	Выявляет опасное содержимое пакетов в случае разрешенных протоколов
Фильтрация уязвимостей	Блокирует влияние известных уязвимостей
Экранирование уязвимостей	Блокирует уязвимость пока она не удалена. Блокурует уязвимости, которые не могут быть удалены.
Интеллектуальные фильтры	Защищают от атак нулевого дня. Усиливают политику безопасности.
Обычные фильтры	Защита приложений

Firewall нового поколения

В последнее время появились новые опции Firewall:

- встраивание системы IPS;
- управление доступом для пользователей и групп;
- возможность фильтрации на уровне L3 и L3 и т.д.;
- эти устройства могут работать в каналах с быстродействием до 10 Гбит/с.

Пример Firewall нового поколения представлен на рис. 8. Новые возможности в этой сфере предоставляет пользователям техника SDN (Software Defined Network).

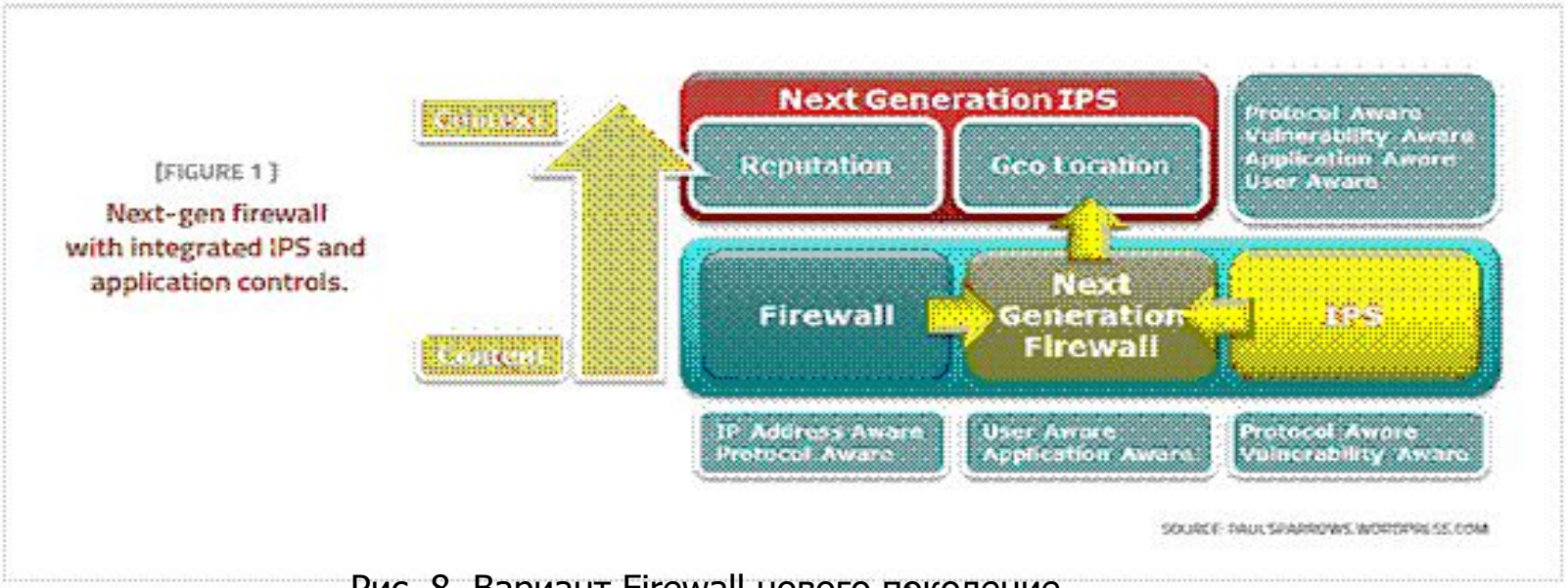

Рис. 8. Вариант Firewall нового поколение

Firewall нового поколения могут помочь решить проблемы безопасного применения мобильного оборудования.

Firewall inbound и outbound типов

Большинство Firewall относятся к inbound-типу, т.е. к блокирующим вредоносный внешний трафик, включая DDoS-атаки. Но существуют также и outbound Firewall, которые блокируют вредоносный трафик, исходящий из локальной сети, включая SPAM (см. "**Comparing firewalls: Differences between an inbound & outbound firewall**", Kevin Beaver, Network Security). Некоторые Firewall могут решать обе эти задачи.

Полезные ссылки

1. Understanding Firewalls (CERT)
2. Debunking Some Common Myths (Некоторые мифы сетевой безопасности)
3. Greg Young, John Pescatore. Magic Quadrant for Enterprise Network Firewalls (Gartner)
4. Next Generation Web Application Firewalls: NG-WAF
5. Intrusion Defense Firewall (Trend Micro)
6. The Technical Guide on WEB application Firewall
7. Proactive Security through Firewall Log Analysis

Широкое использование мобильных устройств **(laptop с Wi-Fi, iPAD, iPhone и т.д.) размывает периметр сети и делает Firewall неэффективным.**