# FireWall (Брандмауэр)

*Основной задачей брандмауэра является защита сетевых коммуникаций от несанкционированного доступа как извне, так и изнутри компьютерной сети. Брандмауэры бывают различных типов и размеров и зачастую представляют собой комплекс, фактически установленный на нескольких разных компьютерах. Здесь брандмаузер (firewall) — это одно или несколько устройств, расположенных между безопасными (trusted) внутренними сетями и небезопасными (untrusted) внешними (такими как Internet), которые исследуют весь протекающий между сетями трафик (см. рис.1).*

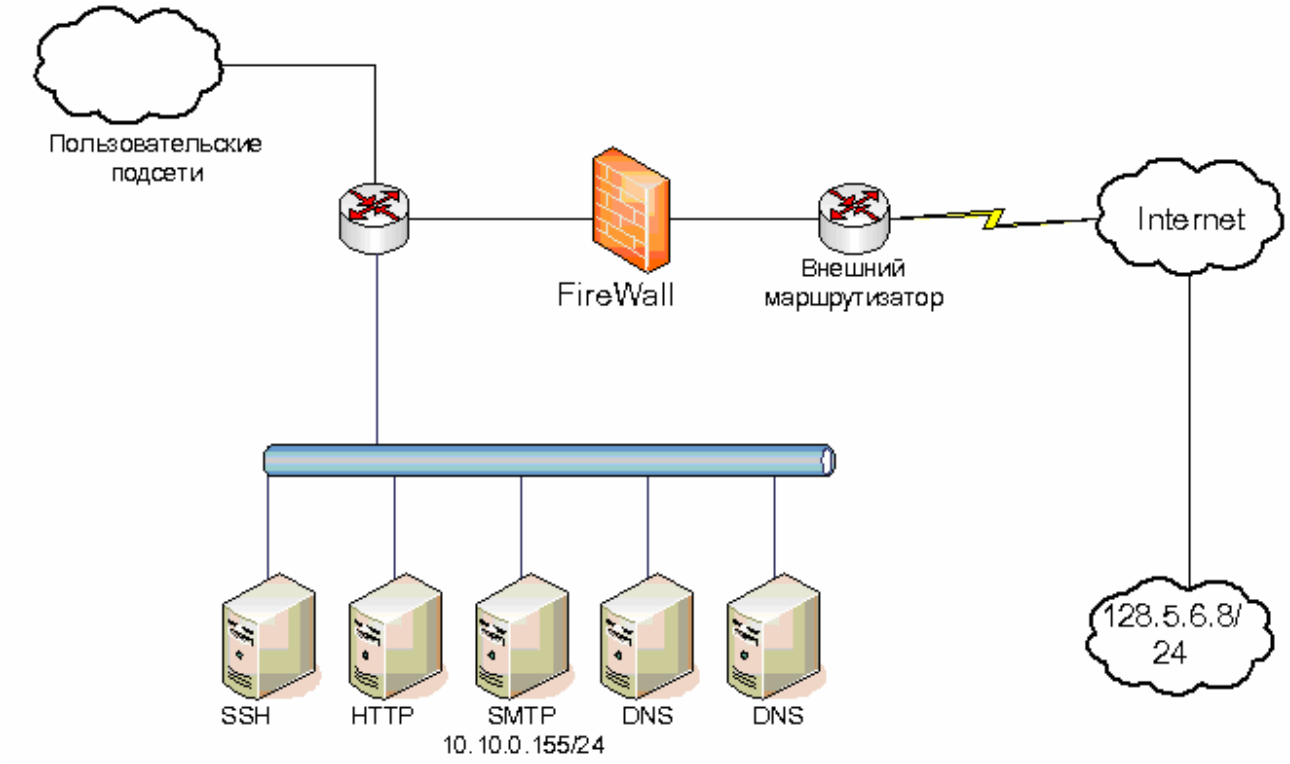


*Рис.1. Брандмауэр в сети*

*Брандмауэры обладают следующими свойствами.*

- *Вся связь проходит через брандмауэр.*
- *Брандмауэр разрешает только санкционированный трафик.*
- *Брандмауэр способен противодействовать атакам на себя.*

*Брандмауэр можно рассматривать как буфер между безопасной и небезопасной сетями. Термин брандмауэр (firewall — огненная стена) происходит от названия строительной технологии, подразумевающей установку огнеупорных перегородок препятствующих распространению огня в случае пожара. По существу это просто барьер. Сетевой брандмауэр — это средство противодействия вторжению из других сетей.*

*В качестве брандмауэра может выступать маршрутизатор, персональный компьютер, хост или совокупность хостов, специально предназначенных для защиты закрытой сети от расположенных на внешних хостах служб, которые могут нанести вред. Обычно система брандмауэра устанавливается на границе внутренней сети, в точке ее подключения к Internet. Однако брандмауэр может быть расположен и внутри сети, обеспечивая дополнительную, специализированную защиту некоторого ограниченного числа хостов.*

*Способ защиты безопасной сети зависит как от конструкции брандмауэра, так и от применяемых им правил. В настоящий момент существует четыре основных категории брандмауэров*

- *Фильтры пакетов.*

- *Шлюзы прикладного уровня.*
- *Шлюзы канального уровня.*
- *Процессоры проверки пакетов с фиксацией состояния.*

*Подобно всем остальным программным технологиям брандмауэр обладает жизненным циклом, на протяжении которого происходит его проектирование, разработка и усовершенствование.*

# Назначение брандмауэров

*Для чего нужны брандмауэры? Почему для противостояния нападению недостаточно настройки самой системы? Ответ очень прост — брандмауэр является специализированным средством решения конкретной задачи — выявления несанкционированного трафика, а его применение избавляет от необходимости искать компромисс между степенью защищенности и функциональными возможностями системы.*

*Без брандмауэра система будет вынуждена полагаться на собственные средства и устройства защиты. Система способна выполнять собственные службы, улучшающие ее функциональные возможности или облегчающие администрирование, однако они обычно не отличаются достаточной степенью безопасности, строгостью проверки прав и ограничены возможностью запуска только из определенного места расположения. Брандмауэры позволяют реализовать именно такой уровень управления доступом.*

*Если среда не обладает брандмауэром, то вся ответственность за обеспечение безопасности целиком и полностью ложится непосредственно на хосты. В этом случае степень защищенности системы в целом будет определена наименее защищенным хостом. Чем больше сеть, тем сложней поддерживать все хосты на одинаково высоком уровне безопасности. Поскольку небольшие оплошности время от времени неизбежны (например, критически важное дополнение к программе обеспечения безопасности было добавлено только к 14 Web-серверам из 15), вторжение (break-in) может произойти из-за самых простых ошибок конфигурации или внесения неадекватных изменений в систему защиты.*

*Поскольку брандмауэр является единственной точкой выхода в небезопасные сети, администратор системы безопасности может сосредоточить свои усилия именно на нем, а не на нескольких разных машинах. Применение брандмауэра вовсе не означает, что о безопасности защищаемой им системы, можно уже не заботиться, ведь это лишь средство защиты, а не панацея.*

*Брандмауэры — превосходные ревизоры (аудиторы). Поскольку через них проходит весь трафик, в случае вторжения или каких либо неприятностей, содержащаяся в их журналах информация позволит восстановить ход событий.*

*В общем случае, брандмауэры позволяют уменьшить риск несанкционированных или непреднамеренных действий в системе (например, деятельности хакеров). От каких же именно рисков брандмауэры защищают системы? Корпоративные системы и данные требуют защиты от следующих возможных неприятностей.*

- *Риск нарушения конфиденциальности.*

*Речь идет о несанкционированном доступе извне к секретным данным, а также о публикации данных, не предназначенных для этого. В мире бизнеса можно легко потерять миллионы долларов из-за нечаянной публикации бизнес-плана, утечки секретов фирмы или финансовой информации.*

- *Риск нарушения целостности данных.*

*Речь идет о несанкционированном изменении данных, например финансовой информации, спецификаций товаров или их цен на Web-сайте. Адекватность деловой информации — обязательное условие в любом бизнесе. Не будучи уверенным в достоверности информации невозможно принять правильное решение. А как насчет деловых партнеров, которые могут увидеть на сайте ложную информацию? Или*

*покупатели, как это скажется на уровне сбыта? И наконец, является ли достоверной финансовая отчетность?*

- *Риск нарушения доступа. Система должна быть доступна всём заинтересованным пользователям в любой момент. Недоступность системы может стоить корпорации потери прибыли, снижения производительности труда сотрудников, а также трудно поддающейся оценке потери доверия потребителей и отрицательной рекламы.*

# Основные типы атак

*В предыдущем разделе было изложено, зачем корпорации и отдельные пользователи применяют брандмауэры. Теперь ответим на вопрос, как именно хакеры получают несанкционированный доступ в систему? Мотивы для таких атак могут быть самыми разными: от любопытства, "а можно ли это сделать вообще", до желания частыми вторжениями скомпрометировать саму систему безопасности, украсть чужие секреты или из хулиганских побуждений повредить или уничтожить систему.*

*Существует множество различных способов, позволяющих злоумышленнику получить доступ в систему. Вот краткий список наиболее часто употребляемых способов атак.*

- **Человеческий фактор** *(social engineering).*

*Подразумевает завладение нападающим пароля либо сертификата администратора или другого пользователя, обладающего в системе правами, достаточными для доступа к необходимым ресурсам или для выполнения системных операций.*

- **Ошибки программного обеспечения** *(software bug).*

*Нападающий, используя дефект программного обеспечения, заставляет приложение или службу выполнить несанкционированные либо непредусмотренные команды. Такие атаки особенно опасны, когда приложение выполняется с расширенными или административными правами. Подобные атаки возможны в случае переполнения буфера (butter overflow) и ошибки формата строки (format string vulnerabilities).*

- **Вирусы и/или троянские кони** *(Viruses and/or Trojan code).*

*Подразумевает запуск вредоносной программы на выполнение законным пользователем. Обычно программу для такой атаки маскируют невинным посланием электронной почты или распространяют при помощи вируса. Будучи запущенной на выполнение, такая программа способна на многое, она может не только открыть доступ чужаку, похитить файлы и/или сертификаты, но и удалить файлы системы.*

- **Плохая настройка системы** *(poor system configuration).*

*Нападавший использует ошибки в настройке системы: доступные службы и/или учетные записи. Начинающие администраторы достаточно часто забывают (или не умеют) изменить заданные по умолчанию пароли и учетные записи (как в системе, так и на прикладном уровне), а также не ограничивают доступ к административным приложениям и не отключают посторонние и неиспользуемые службы.*

*Кроме несанкционированного доступа к системе, злонамеренная личность может попытаться просто уничтожить ее. Вывод из строя достаточно важного, высокопроизводительного коммерческого приложения может привести к серьезным финансовым потерям. К подобному типу атак относится отказ в обслуживании (DoS — Denial of Service). При атаке DoS пользователи, сеть или организация лишаются жизненно важной службы либо ресурса. Обычно потеря службы вызвана дисфункцией отдельной сетевой службы, например электронной почты или Web, частичной или полной потерей подключения к сети или недоступностью какой-либо службы.*

# Размещение брандмауэра

*Брандмауэры следует устанавливать во всех точках соединения сетей с разными требованиями безопасности. Чаще всего брандмауэры используют на стыке Internet и локальной сети. Еще одной областью применения брандмауэра является защита подключения*

*к внешнему партнеру (например, поставщику платных данных), а также защита особо важных областей внутренней сети.*
*Достаточно часто используется понятие периметра сети (network perimeter), означающее границы локальной сети. Когда локальная Сеть подключается к другой сети, например Internet, формируются точки входа (ingress point) и выхода (egress point). Эти точки подключения почти всегда защищают брандмауэры.*
*На первый взгляд определение периметра сети кажется простым. Однако с появлением виртуальных закрытых сетей определить фактический периметр стало достаточно трудно. Технология виртуальной закрытой сети (virtual private network), называемой также виртуальной частной сетью, позволяет удаленным пользователям подключаться через брандмауэр так, будто они находятся в локальной сети. Подобное расширение позволило создать корпоративные сети, но сами хосты остались вне периметра защиты, обеспечиваемой корпоративными брандмауэрами. Злонамеренные личности могут использовать этих пользователей как проводников через корпоративный брандмауэр. Для обеспечения одинакового уровня безопасности в пределах периметра сети администратор должен позаботиться об установке на этих хостах локальных персональных брандмауэров.*

# Достоинства и недостатки брандмауэров

*Брандмауэр — это всего лишь один из фрагментов архитектуры системы безопасности, и, как любой фрагмент архитектуры, он обладает сильными и слабыми сторонами.*

## Достоинства

■ *Брандмауэры превосходны в реализации корпоративной политики безопасности.*
*Они должны быть настроены так, чтобы ограничить доступ к средствам управления, а к общедоступным ресурсам — нет.*

■ *Брандмауэры позволяют ограничить доступ к определенным службам.*
*Например, брандмауэр разрешает свободный доступ к Web-серверу, но запрещает доступ к Telnet и другим демонам, не предназначенным для общего использования. При помощи функций аутентификации большинство брандмауэров способно обеспечить выборочный доступ.*

■ *Брандмауэры являются специализированным средством.*
*Следовательно, не придется искать компромисс между степенью защищенности и функциональными возможностями.*

■ *Брандмауэры — превосходные ревизоры.*
*Обладая достаточным пространством на диске или возможностью удалённого хранения журналов регистрации, брандмауэр способен регистрировать весь проходящий через него трафик (или только указанный).*

■ *Брандмауэры способны оповестить пользователей о соответствующих событиях.*

## Недостатки

■ *Брандмауэры не могут защитить от разрешенного содержимого.*
*Брандмауэры защищают приложения и разрешают обычный обмен информацией с этими приложениями (в противном случае от брандмауэров было бы больше вреда, чем пользы). Но если сами приложения обладают дефектами, то брандмауэры их не исправят и не смогут предотвратить атаку, поскольку для брандмауэра вся передаваемая информация вполне допустима.*

■ *Брандмауэры эффективны настолько, насколько эффективны правила, которые они призваны выполнять.*
*Набор чрезмерно вольготных правил уменьшит эффективность брандмауэра.*

■ *Брандмауэры бессильны перед человеческим фактором*

*Также как и перед уполномоченным пользователем, преднамеренно использующим свои права в злонамеренных целях.*

■ *Брандмауэры не могут ни устранить просчеты администратора, ни заменить плохо разработанную политику безопасности.*

■ *Брандмауэры не противодействуют атакам, трафик которых через них не проходит.*

# Правила успешной защиты

*По умолчанию, за исключением очень редких случаев, системы и приложения устанавливаются конфигурациях не самого высокого уровня защищенности. Кроме того, по умолчанию в системе устанавливается и активизируется ряд служб и приложений, функциональные возможности которых могут понадобиться лишь потенциально, но на самом деле не используются. Хорошей привычкой является установка лишь минимально допустимого набора служб и учетных записей, необходимого для функционирования системы. Большинство вторжений происходит именно потому, что нападающий воспользовался неиспользуемой службой или системной учетной записью. Практику отключения неиспользуемых служб и перенастройку остальных в целях обеспечения большей безопасности и зачастую называют укреплением хоста (host hardening).*

*Ниже приведен небольшой перечень действий, осуществляемых обычно при укреплении хоста:*

■ *Отключите ненужные и неиспользуемые службы..*

■ *Удалите ненужные учетные записи и группы. Измените заданные по умолчанию пароли системных приложений и учетных записей или удалите их. Отключите учетные записи не требующие интерактивной регистрации (login).*

■ *Перенастройте оставшиеся службы, увеличив их уровень безопасности.*

■ *Защитите все средства администрирования.*

■ *Используйте сложные пароли. Сложными считаются пароли состоящие более чем из семи символов как в верхнем так и в нижнем регистре, содержащие цифры и символы.*

# Архитектура брандмауэров

*По мере насыщения рынка брандмауэров, вырабатывались соответствующие методики защиты трафика, передаваемого через контрольные точки сети. В зависимости от конкретной реализации, эти методики существенно отличаются: от простой проверки сетевых пакетов и транспортных уровней модели OSI до исследования содержимого каждого пакета на прикладном уровне. Здесь рассматриваются различия, преимущества и недостатки каждой из основных методик, используемых в брандмауэрах. Обратите внимание: хотя большинство производители брандмауэров реализуют только один из методов описанных здесь, некоторые реализуют несколько. Как правило, это делается для более детализированной выборочной защиты уязвимых протоколов, без потери производительности, неизбежны при реализации такой защиты для всего сетевого трафика.*

*Способ, которым брандмауэр защищает безопасную сеть, зависит от самом брандмауэра, а также политики и правил, которые он реализует. В настоящий моменя существует четыре технологи брандмауэров.*

■ *Фильтры пакетов.*

■ *Шлюзы прикладного уровня.*

■ *Шлюзы канального уровня.*

■ *Проверка пакетов с фиксацией состояния.*

*Подобно всем техническим решениям, брандмауэры проходят обычный жизненный цикл. Следующие разделы описывают каждую из этих технологий более подробно.*

## Фильтры пакетов

*Фильтры пакетов (packet filter) выполняют самые простые действия. Фильтрующая система устанавливается поверх существующей архитектуры передачи данных, использующей пакеты, заголовки протокола Internet (IP) которых содержат адреса и номера портов протоколов, позволяющих передать их по сети получателю. Фильтр пакетов исследует заголовок каждого проходящего через него пакета, а затем принимай решение стоит ли передавать его следующему транзитному участку сетевого пути или его следует отбросить (отправителя об этом можно.уведомить). Принятие решения осуществляется на основании правил, установленных администратором брандмауэра Правила могут быть заданны на основании информации следующего типа:*

- *IP-адрес или диапазон IP-адресов отправителей пакета.*
- *IP-адрес или диапазон IP-адресов получателей пакета.*
- *Сетевой протокол (например, TCP, UDP или ICMP).*
- *Используемый номер порта. Обычно он идентифицирует и тип трафика (порт 80, например, применяемый для протокола HTTP, передает трафик Web).*

## Работа фильтра пакетов

*Фильтр пакетов имеет входной, или "грязный" порт (dirty port), набор правил и выходной, или "чистый" порт. Входной порт подключен к Internet и принимает весь входящий трафик. Трафик, принимаемый входным портом, обрабатывается согласно набору правил или политике, установленной для брандмауэра. На основании набора правил, установленного для брандмауэра, принимается решение о предпринимаемом действии: пакету либо позволяется пройти через выходной порт в защищаемую сеть либо нет.*

*В приведенном ниже примере сети содержится два сервера DNS, сервер HTTP, сервер защищенного удаленного соединения (SSH — Secure Shell) и сервер SMTP. На рис.2 показано взаимное расположение безопасных и небезопасных сетей относительно брандмауэра*

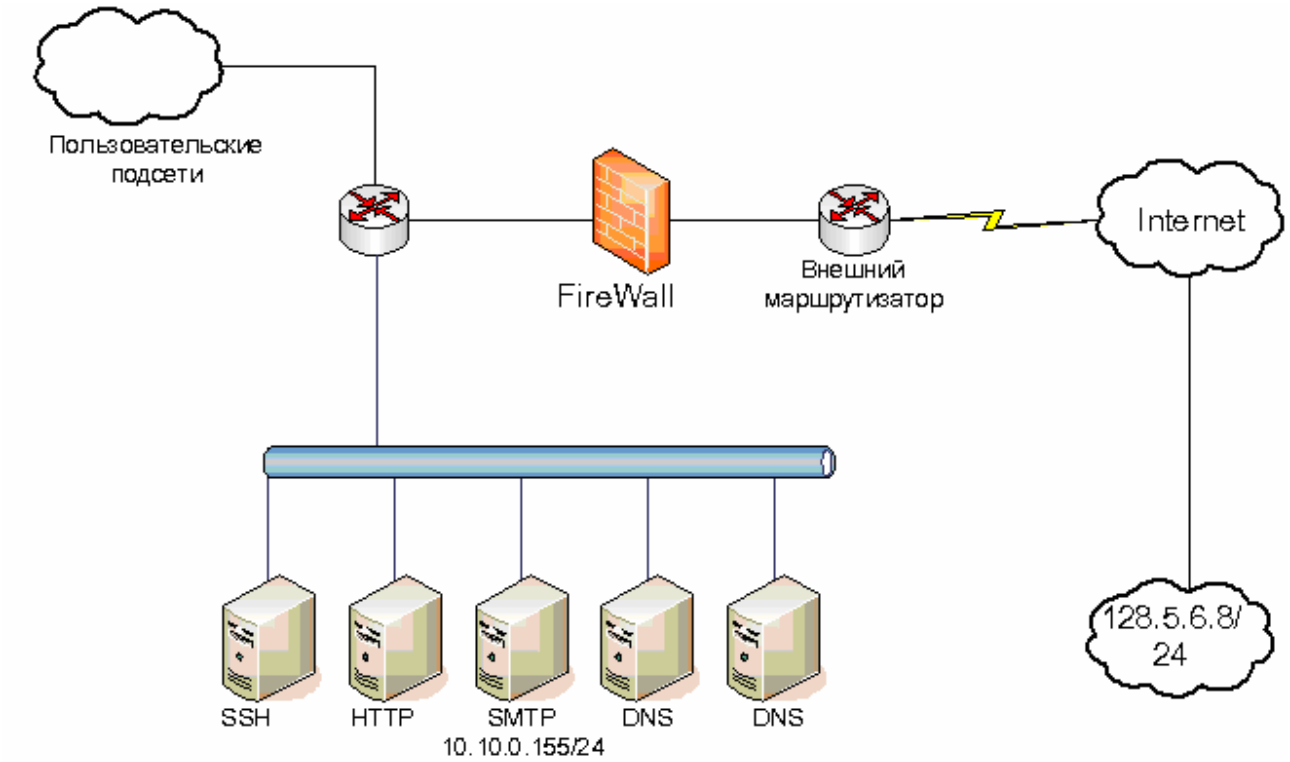


*рис.2. Взаимное расположение безопасных и небезопасных сетей относительно брандмауэра*

# Создание набора правил

*Чтобы рассмотреть пример фильтрации пакета, создадим набор правил по таким критериям:*

- *тип протокола;*
- *адрес отправителя;*
- *адрес получателя;*
- *порт отправителя;*
- *порт получателя;*
- *действие, которое брандмауэр должен предпринять обнаружив соответствие критерию*

*Обратите внимание: порт отправителя не всегда является перенастраиваемы паметром конфигурации, но в большинстве случаев он таковым является.*
*Табл.1 содержит набор правил, представляющий собой политику брандмаузера, предназначенную для принятия решения о допустимости передачи пакета в защищаемую сеть.*

**Таблица 1. Типичный набор правил фильтра пакетов**

| *Правило* | *Тип протокола* | *Адрес отправителя* | *Адрес получателя* | *Порт отправителя* | *Порт получателя* | *Действие* |
|---|---|---|---|---|---|---|
| *1* | *TCP* | *128.5.6.0/24* | *10.10.0.155* | *1023* | *22* | *Разрешить* |
| *2* | *TCP* | *Любой* | *10.10.0.154* | *1023* | *80* | *Разрешить* |
| *3* | *TCP* | *Любой* | *10.10.0.150* | *1023* | *25* | *Разрешить* |
| *4* | *UDP* | *Любой* | *10.10.0.152* | *1023* | *53* | *Разрешить* |
| *5* | *UDP* | *Любой* | *10.10.0.153* | *1023* | *53* | *Разрешить* |
| *6* | *Любой* | *Любой* | *Любой* | *Любой* | *Любой* | *Запретить* |

*Данный набор состоит из шести простых правил брандмауэра. Их простота обусловлена демонстрационными целями, чтобы лучше объяснить саму концепцию использования набора правил фильтра пакетов. В реальной реализации набора, каждое правило дополняется строкой примечания, кратко описывающей его. Обратите также внимание на то, что этот набор правил не является рекомендуемым решением; как будет указано далее, в большинстве реальных систем он неприменим.*
*При фильтрации пакетов применяется правило "полного соответствия". То есть входящий пакет должен соответствовать всем критериям правила; в противном случае оно не будет применено. Это не означает, что пакет будет обязательно он брошен или пропущен, просто данное правило применено не будет. Обычна фильтры пакетов располагают в последовательном порядке, сверху вниз. Хотя для их реализации разработано множество разных стратегий, лидируют среди них следующие две:*

- *Правила располагаются с порядке от более специфических к более общим чтобы общее правило не "поглотило" более специфическое правило, подпадающее под общее правило.*
- *Правила нужно упорядочить так, чтобы используемые наиболее часто распологались в начале (вверху) списка. Это повышает производительность, поскольку найдя соответствие критерию, средство защиты прекратит дальнейший поиск в списке.*

**Правило 1**

*Это правило разрешает передачу входящих пакетов одной из IP-подсетей Internet на один хост сети для осуществления защищенного удаленного соединения (SSH). Протокол SSH считается более безопасным, чем такой открытый текстовый (clear-text) протокол, как Telnet, но он ни в коем случае не является единственно возможным решением для удаленного доступа к локальным ресурсам. В этом примере, доступ разрешен лишь малой части*

*адресов подсети отправителя. Протокол SSH передает пакеты из случайного порта с большим номером (RHP — Random High Port) порту получателя TCP 22. Применение RHP позволяет оптимизировать ресурсы передающей системы и обеспечить ее способом уникальной идентификации каждого подключения. Это особенно ценно, когда посылающий хост должен открыть несколько соединений с одним получателем и на том же самом порту получателя (в данном примере передающий хост открывает несколько защищенных удаленных соединений с одним хостом получателя). Поскольку соединение в этом примере должен установить только один хост, именно он и указан в качестве единственного хоста в перечне адресов получателя.*

**Правило 2**

*Это правило разрешает передачу входящих пакетов порту 80, который обычно используется для трафика HTTP. Хост 10.10.0.154 представляет собой Web-сервер домена. Поскольку невозможно заранее предсказывать, кто именно захочет получить доступ к Web-сайту организации, никаких ограничений на IP-адреса отправителей нет.*

**Правило 3**

*Это правило разрешает входящий трафик протокола SMTP. В системе доменных имен (DNS — Domain Name System) организации может быть зарегистрирована одна или несколько записей, указывающих на почтовые серверы SMTP. Эти записи называются записями MX. В данном примере DNS организации указывает на запись MX внутри периметра сети с IP-адресом 10.10.0.150. Любой хост в Internet, которому понадобится послать электронную почту хосту в этом домене, будет пытаться подключиться к серверу SMTP именно по этому IP-адресу. Поскольку попытку подключения к SMTP может сделать любой хост в Internet, IP-адрес отправителя здесь указан как «любой». Если бы здесь было перечислено подмножество IP-адресов, то некоторые сети в Internet не смогли бы послать почту пользователям этого домена.*

**Правила 4 и 5**

*Два сервера с IP-адресами 10.10.0.152 и 10.10.0.153 являются серверами службы доменных имен этого домена. Фактически для правильной работы службы DNS, достаточно лишь протокола пользовательских дейтаграмм (UDP — User [Datagram Protocol). Протокол TCP необходим в двух случаях, когда следует обеспечить передачу (transfer) зоны DNS, а также когда ответ получается настолько большим, что просто не помещается внутри одного пакета UDP. Взлом серверов DNS осуществляется как правило по протоколу TCP, поэтому специалисты в области безопасности рекомендуют системным администраторам по возможности оградить эти серверы от сединений по протоколу TCP.*

**Правило 6**

*Это правило явно запрещает передачу всех пакетов, которые не соответствуют ни одному из критериев предыдущих правил. Большинство средств защиты выполняет это правило по умолчанию, но для очистки совести его можно включить и в явном виде. Включив это правило в список, задайте необходимость регистрации соответствующих ему пакетов, как это делают по умолчанию жесткие политики. Это может оказаться полезным как по административным причинам, так и по судебным. Набор правил, описанный в табл.1, обладает рядом существенных моментов, на которые стоит обратить внимание. Прежде всего это относится к пакетам, поступающим на устройство безопасности со стороны внешнего интерфейса (например, Internet). Поскольку подключение TCP поддерживает двухсторонний диалог, для трафика поступающего в интерфейс, защищаемый данным устройством, должен был бы быть составлен соответвующий набор правил. В некоторых случаях можно позволить передачу всего исходящего трафика. Если дело обстоит так, то в наборе правил нет необходимости. Но большинство организаций, желающих*

*предотвратить утечку информации в неконтролируемую и небезопасную сеть, ограничивают исходящий трафик. Когда эти фильтры оказываются реализованы, инженер службы безопасности должен удостовериться что, если внешнему пакету TCP разрешен проход сквозь устройство защиты внутрь, то и ответу из внутренней сети также позволен выход во внешнюю.*

*Большинство устройств безопасности, работающих по принципу фильтрации пакетов, реализует сводную политику (summary policy), разрешающую передачу пакетов всех "установленных" ("established") соединений. Для этого они просматривают пакеты TCP и выясняют, являются ли они частью уже существующего диалога (проверяется наличие бита SYN заголовка TCP). Если бит SYN сброшен, то пакет принимается, поскольку он может быть только частью уже установленного диалога TCP. Обратите внимание, устройство безопасности не исследует содержимое самих диалогов, оно передает их исключительно на основании состояния бита SYN. Кроме того, описанные в табл.1 правила не учитывают возврат пакетов по каналам связи инициализированным системами изнутри сети.*

## Преимущества и недостатки устройств фильтрации пакетов

*Как следует из приведенных выше простых наблюдений, установка корректных правил фильтрации пакетов может оказаться занятием достаточно сложным. При рассмотрении возможности применения устройств фильтрации пакетов необходимо учесть их преимущества и недостатки.*

## Преимущества:

■ *Дополнительная нагрузка минимальна, поэтому общая производительность от таких устройств практически не страдает.*

■ *Относительная дешевизна.*

■ *Надежность контроля трафика.*

## Недостатки:

■ *Возможность непосредственного подключения внешних клиентов к внутренним хостам.*

■ *Относительно большое количество брешей в периметре сети. Это связано с тем, что фильтр исследует трафик только на транспортном уровне (протоколы TCP или UDP) или на сетевом уровне (протоколы ICMP или IP). Фильтр пакетов неспособен проверить проходящую через него высокоуровневую информацию. Например, второе правило в табл.1. Хотя устройство фильтрации пакетов способно определить, что входящий запрос HTTP должен быть пропущен, оно не может выяснить, является ли отправивший его пользователь вполне допустимым или злоумышленником и является ли запрос HTTP вполне допустимым или попыткой воспользоваться брешью системы буферизации, унаследованной многими реализациями Web-серверов.*

■ *Затруднено управление и масштабируемость в сложных системах. В многоуровневых системах безопасности (известных также под названием глубоко эшелонированной обороны (Defense in Depth)), все фильтры пакетов для обоих направлений сетевого трафика должны быть синхронизированы.*

■ *Уязвимость к таким атакам, как подмена адресов (spoofing), когда IP-адрес внешнего отправителя заменяется IP-адресом внутренней сети, если предотвращение этой проблемы не предусмотрено заранее. Существует и другой, более сложный тип атаки, когда все пакеты подделываются так, чтобы устройству защиты они казались частью уже установленного подключения. Для этого достаточно сбросить в атакующих пакетах бит SYN. Устройства безопасности, настроенные так, чтобы пропускать пакеты, у которых этот бит не установлен, окажутся бессильны.*

- *Отсутствие аутентификации пользователей.*

*В связи с удобством применения, а также совместимостью с устаревшими версиями, статическая фильтрация пакетов все еще используется некоторыми организациями в качестве средства защиты. Но в настоящий момент статическая фильтрация пакетов обеспечивает лишь минимальную защиту.*
*В связи с большим количеством и серьезным характером недостатков фильтров пакетов первого поколения они не пользовались спросом и быстро покинули рынок. Огромное количество уязвимых мест сделали статические фильтры пакетов мишенью для многочисленных типов атак, а также доступной мишенью для желающих поохотиться на хосты во внутренних сетях. Однако небольшие организации все еще применяют их как дополнительное средство защиты.*

## Шлюзы прикладного уровня

*В области информационных технологий одну и туже вещь нередко называют по-разному. Это в полной мере относится к шлюзами прикладного уровня. Термин шлюз прикладного уровня (application gateway) практически является синонимом терминов бастионный хост (bastion host), прокси-шлюз (proxy gateway) и прокси-сервер (proxy server), поскольку все они описывают тот же самый метод защиты периметра.*
*Шлюз прикладного уровня выполняет те же функции, что и операторы на заре первых телефонных систем. В те времена телефонный вызов поступал оператору, который затем переключал телефонные линии так, чтобы соединить абонентов. Ни вызывающая, ни вызываемая сторона не могли узнать, прослушивает их оператор или нет. Поскольку операторы часто подслушивали переговоры, они были зачастую наиболее информированными людьми в обществе и рассказывали потом самые интересные истории (в лучшем случае).*
*Шлюз прикладного уровня обеспечивает более высокий уровень защиты чем фильтр пакетов, но достигается это за счет потери "прозрачности" для приложений. Всем поддерживаемым брандмауэром приложениям должна быть назначена индивидуальная программа, принимающая данные клиентского приложения и передающая их серверу получателя. Bed трафик, который проходит через шлюз прикладного уровня, передается дальше или отвергается. Шлюз прикладного уровня выступает в роли посредника для таких приложений, как электронная почта, FTP, Telnet и WWW. Таким образом, для клиентов шлюз прикладного уровня является сервером, а для серверов получателей — клиентом. Обработка информации, осуществляемая шлюзом прикладного уровня, происходит на» самом верхнем уровне модели OSI, что налагает дополнительные требования.*
*Брандмауэр проверяет формат приложений. Он может даже осуществлять дополнительную аутентификацию и регистрацию информации, а также выполнять в случае необходимости преобразование данных. Еще одним преимуществом использования прокси-серверов является возможность фильтраций трафика в зависимости от протокола. Некоторые брандмауэры, например, способны фильтровать трафик соединений FTP и запрещать использование команды FTP put, что позволяет исключить возможность записи пользователями информации, например, на анонимный сервер FTP. Кроме защиты данных, подключение через прокси-сервер предотвращает возможность использования внутренних служб. В результате защищенность служб, выполняющихся на шлюзе прикладного уровня; существенно увеличивается.*

## Работа шлюза прикладного уровня

*О сеансе связи между пользовательской системой и Шлюзом прикладного уровня известно только ей. Шлюз прикладного уровня регистрирует информацию о подключении, включая инициатора подключения, адреса, назначение, время и продолжительность сеанса связи, а*

*кроме того обрабатывает трафик проходящий между хостами. На рис.3 представлены потоки информации сквозного (end-to-end) подключения между клиентом и сервером Telnet. Предположим, что вымышленная компания решает разместить сервер Telnet так, чтобы удаленные администраторы могли выполнять действия на определенном хосте. Чтобы замаскировать реальное имя хоста сервера от просмотра из небезопасных сетей, компания анонсируют шлюз Telnet, а не фактический сервер. Процесс подключения к хосту проходит следующим образом.*

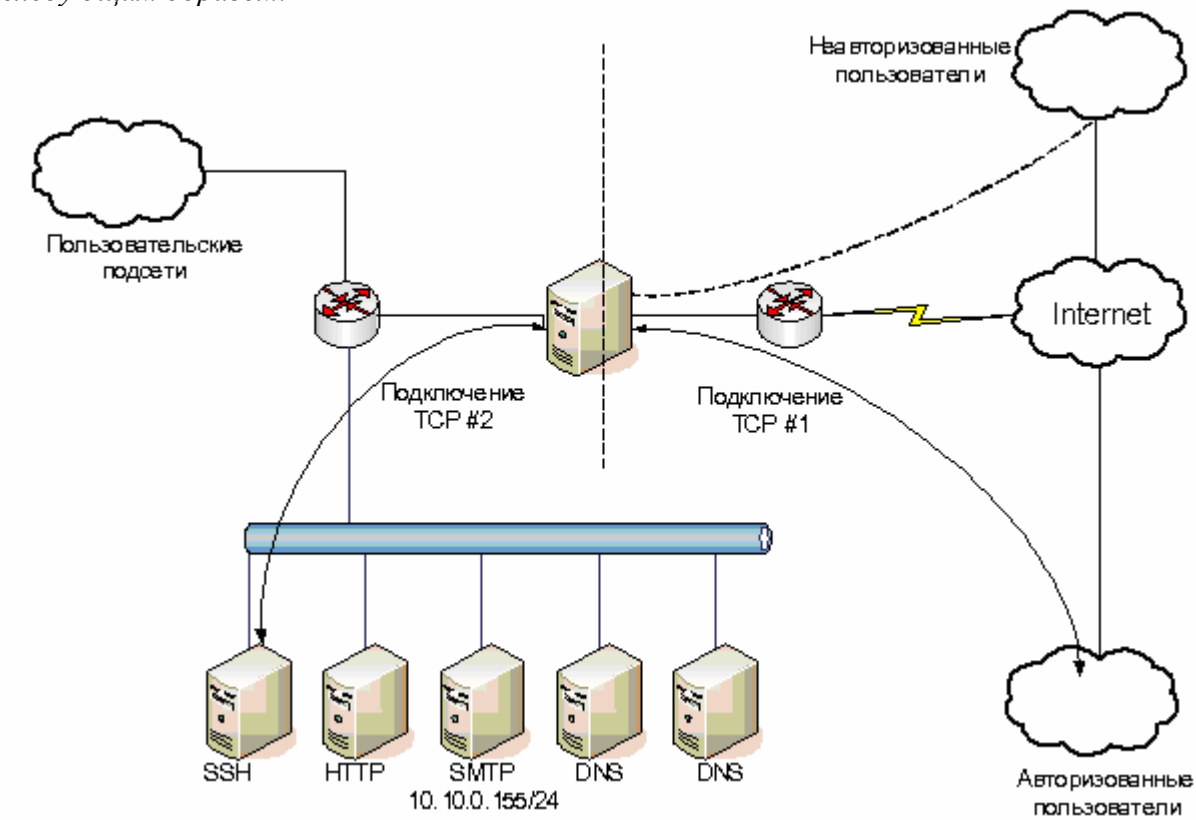


*Рис.3 потоки информации сквозного (end-to-end) подключения между клиентом и сервером Telnet.*

*1. При помощи Telnet пользователь обращается к шлюзу прикладного уровня через порт 23. Устройство защиты проверяет IP-адрес отправителя а списке допустимых отправителей. Если IP-адрес допустим, то процесс переходит к следующему этапу подключения, в противном случае прекращается. Выполняющийся на шлюзе прикладного уровня прикладной демон (application daemon), Представляет собой укрепляющее защиту приложение, существенно затрудняющий ее преодоление; кроме того, это единственный элемент, который необходимо модифицировать при обнаружении новых брешей системы безопасности.*

*2. Пользователь запрашивает аутентификацию. Аутентификация пользователей на уровне устройства шлюза имеет несколько преимуществ. Это позволяет централизовать процесс аутентификации, уменьшить затраты на администрирование и хранение учетных записей пользователей, а также облегчить корреляцию событий при попытке отследить подозрительные действия пользователей по их учетным записям. Кроме того, управление процессом регистрации и его обслуживание существенно проще, когда все происходит на единой платформе.*

*3. Пройдя проверку, пользователь получает приглашение ко вводу команд или системное меню, необходимое для подключения к требуемой системе. IP-адреса хостов недоступны из Internet непосредственно; соединение осуществляется только со шлюзом. Фильтрующие устройства блокируют прямой доступ к IP-адресам хостов*

*4. Пользователь выбирает систему для подключения. При этом инициализируется новое соединение TCP между хостом получателя и шлюзом прикладного уровня.*

*5. У пользователя запрашивают дополнительную аутентификационную информацию, если это необходимо.*

## Недостатки шлюзов прикладного уровня

*Недостатком использования шлюза прикладного уровня является непрозрачность для конечного пользователя. В то время как наблюдается тенденция повышение удобства пользовательских интерфейсов и архитектур, шлюзы прикладного уровня добавляют в процесс подключения "неудобный" этап. Кроме того, приложение конечного пользователя, вероятно, придется перенастроить, чтобы оно осуществляло эти промежуточные действия. Хоть в большинстве известных приложении эта возможность предусмотрена, пользователям все-таки придется запускать отдельное приложение только для того, чтобы установить соединение с одной организацией. В некоторых системах это может оказаться крайне непрактичным.*

*Как правило, шлюзы прикладного уровня обладают двойным или многоадресным характером, т.е. они обладают несколькими платами сетевого интерфейса (NIC). Если шлюз прикладного уровня обладает двумя сетевыми платами, одна из них будет подключена к защищаемой сети, а другая — к Internet или небезопасной сети.*

*Шлюзы прикладного уровня укрепляют защиту, но могут оказаться уязвимыми в случае описанных ниже обычных атак на средства безопасности.*

■ **Переполнение запросами на синхронизацию** *(SYN flooding). Переполнение запросами на синхронизацию заключается в передаче непрерывного потока поддельных запросов на определенный компьютер, который постоянно занят их обработкой и не может взаимодействовать с законными пользователями. Этот тип атаки эксплуатирует необходимость синхронизации протокола управления передачей (TCP). В ходе атаки переполнения SYN нападающий посылает адресату череду поддельных сообщений. Он постоянно изменяет адрес отправителя пакета, но остальная часть пакета TCP SYN остается вполне допустимой. Поскольку сообщения являются поддельными, они не содержат реального обратного адреса компьютера, которому следует передать ответ. По мере поступления на атакуемый компьютер подделанных запросов, на которые не удается ответить, его таблицы сетевых соединений заполняются, поскольку вначале он пытается завершать соединения корректно. Пытаясь справиться с проблемой затора (congestion problem), сервер достаточно быстро прекращает отвечать на поступающие запросы об установлении соединений, передаваемые в том числе и законными пользователями.*

■ **Переполнение тестовыми пакетами** *(ping flooding). Тестовый опрос (pinging) заключается в передаче одним компьютером тестового пакета (ping) другому компьютеру и ожидании ответа от него. Переполнение тестрвыми пакетами подразумевает передачу миллионов тестовых пакетов в секунду с одного или нескольких (обычно одного).поддельного адреса отправителя на один или несколько (обычно несколько) реальных адресов получателей. Переполнение наступает, когда получатель пытается отвечать на подделанные тестовые запросы отправителя. Общая пропускная способность, необходимая для передачи всех ответов, может очень быстро превысить доступную пропускную способность сети или подсети получателя. Переполнение тестовыми пакетами может существенно снизить производительность системы либо даже полностью заблокировать работу всей сети или подсети. Обратите внимание, использование в ходе подобной атаки нескольких скоординированных систем в Internet (называемой распределенным отказом в обслуживании (DDoS — Distributed Denial of Service)) увеличивает сложность ее отражения.*

■ **Злонамеренный аплет** *(malicious applet). Аплет (applet)— это небольшая прикладная программа, способная загружается и выполняется автоматически, изменяя при этом стандартное функционирование системы. Он обладает потенциальной возможностью установки и выполнения функций, запрещенных на данном компьютере, что*

*может привести к непредсказуемым последствиям, включая удаление системных файлов или критических важных данных.*

## Шлюзы канального уровня

*По принципу действия шлюз канального уровня (circuit-level gateway) подобен шлюзу прикладного уровня, но ориентирован скорее на неинтерактивные (noninteractive) приложения. После начального этапа аутентификации, позволяющего удостовериться в том, что пользователь имеет право доступа к службе через шлюз, он просто передает подключение по назначению. Прокси-серверы и серверы SOCKS — это типичные представители шлюзов канального уровня. Шлюзы канального уровня передают подключения TCP из безопасной сети в небезопасную. В процессе передачи IP-адрес отправителя преобразуется так, чтобы извне казалось, что подключение инициировал шлюз. Применение большинства прокси-серверов прикладного уровня требует модификации клиентских приложений. Одним из наиболее ярких примеров является прокси-сервер Web. Хотя при подключении через прокси-сервер не нужно устанавливать нового программного обеспечения, клиентское приложение (Web-браузер) приходится перенастраивать на работу через прокси-сервер. Это подразумевает указание IP-адреса внутреннего интерфейса (trusted interface) прокси-сервера, а также порта TCP — прослушивающей службы. Указываемый для протокола TCP порт не обязан соответствовать стандартному порту TCP, на котором эта служба выполняется обычно. С точки зрения пользовательского подключения прокси-сервер совершенно "прозрачен" (если не учитывать аутентификацию).*

## Работа шлюза канального уровня

*Ниже приведена последовательность действий, осуществляемых в процессе подключения через шлюз канального уровня (как уже было сказано, при использовании шлюза канального уровня приходится изменять конфигурацию или устанавливать специальное .Программное обеспечение).*

*1. Пользователь пытается подключения к определенному URL (http://www.названиекомпании. com).*

*2. Вместо передачи запроса URL серверу DNS клиентское приложение посылает его по указанному адресу внутреннего интерфейса прокси-сервера.*

*3. При необходимости аутентификации у пользователя запрашивают его имя и пароль*

*4. Если пользователь проходит аутентификацию, то прокси-сервер выполняет все необходимые дополнительные действия (например, сравнивает URL со списком разрешенных или запрещенных URL), посылает запрос URL серверу DNS, а затем устанавливает соединение с обладателем полученного IP-адреса, передав в качестве IP-адреса отправителя свой адрес, т.е. адрес прокси-сервера.*

*5. Прокси-сервер передает клиенту ответ Web-сервера.*

## Недостатки шлюзов канального уровня

*Большинство шлюзов канального уровня обладает перестраиваемой конфигурацией порта TCP. В этом кроется определенный недостаток. Поскольку шлюз канального уровня не может исследовать каждый пакет на прикладном уровне, это позволяет чужим при- - ложениям использовать порты TCP, открытые для другого, законного приложения. Несколько равнозначных (peer-to-peer) приложений могут быть настроены так, чтобы выполниться на произвольных портах, например на порту TCP 80 и TCP 443 (обычно открываемом для просмотра Web). Таким образом, возникает потенциальная опасность для приложений.*

*У шлюза канального уровня есть и другие недостатки, поэтому не рекомендуется использовать его как единственные средство защиты сети. Вводящие подключения вообще невозможны, если шлюз не оснащен специальным приложением, реализующим эту функциональную возможность. Некоторые клиентские приложения не предусматривают перенастройку на использование SOCKS или прокси-серверов, а это лишает их внешнего доступа. Кроме того, установка дополнительных приложений, реализующих возможность доступа извне, зачастую сопряжена со значительный расходами, что ограничивает либо количество приложений, использующих эту возможность, либо область внешних ресурсов, к которым они могут обращаться.*

# Проверка пакетов с фиксацией состояния (SPI)

*Основное внимание уделено брандмауэрам, реализующим процесс проверки пакетов с фиксацией состояния (SPI — Stateful Packet Inspection). Реализующие SPI брандмауэры сочетают скорость и гибкость фильтров пакетов с высокой степенью защиты средств прикладного уровня и прокси-серверов. Компромисс, как всегда, приводит к промежуточному результату: брандмауэр SPI не обладает такой скоростью, как фильтр пакетов, и не обеспечивает такой же степени безопасности, как прикладной протокол (application protocol). Но это компромиссное решение весьма эффективно в реализации жесткой политики безопасности периметра сети.*

*Принцип действия брандмауэра, реализующего проверку пакетов с фиксацией состояния, основан на исследовании каждого поступившего на него пакета (будь это даже часть уже установленного диалога) и разрешает или запрещает его передачу на основании набора правил, очень похожих на правила фильтрации пакетов. На первый взгляд это очень похоже на брандмауэр фильтрации пакетов. Различие заключается в способе исследования пакета. Схема процесса проверки пакетов с фиксацией состояния приведена на рис.4*

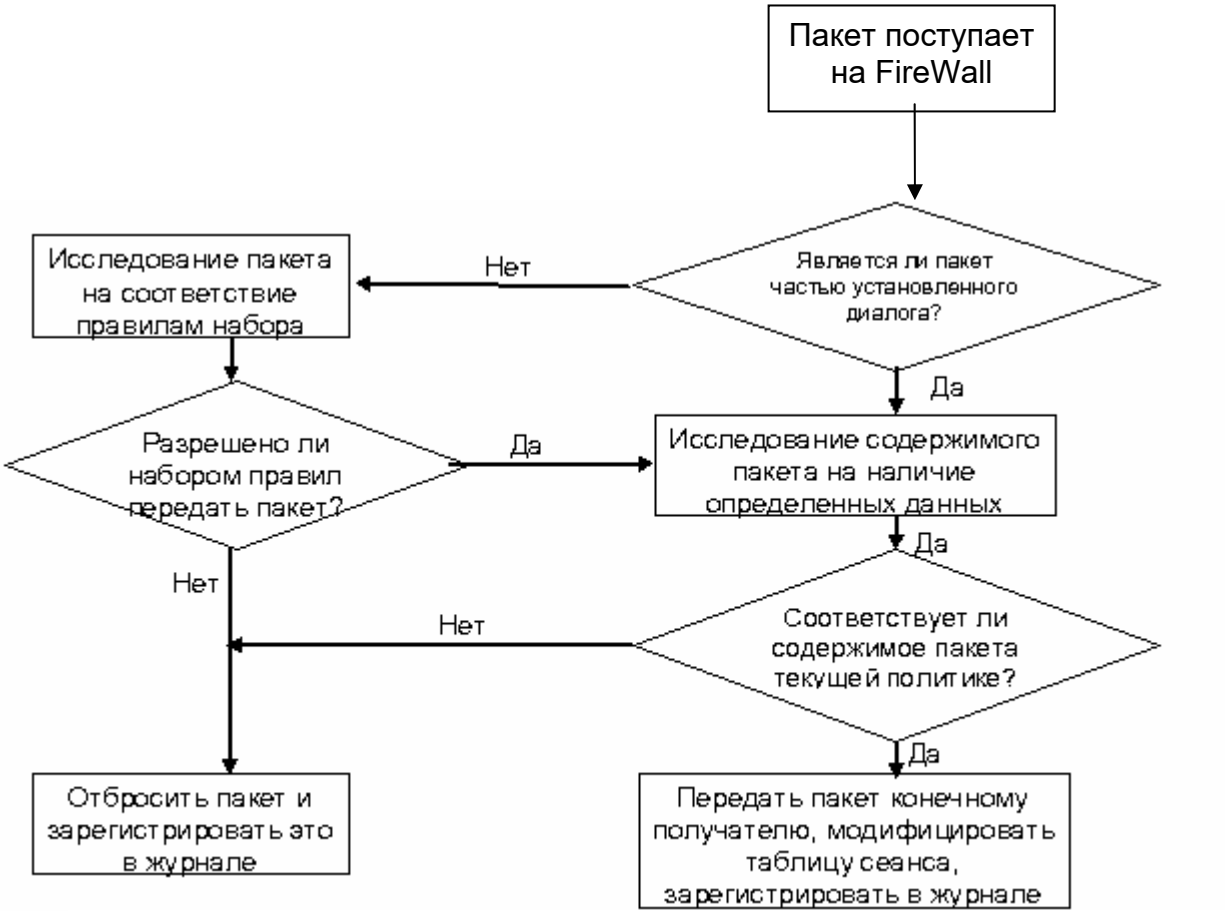


*Рис.4 Схема проверки пакетов с фиксацией состояния*

## Работа брандмауэра проверки пакетов с фиксацией состояния

*Когда пакет поступает на брандмауэр, его проверка осуществляется следующим образом.*

*1. Поступившей пакет исследуется на предмет принадлежности к уже установленному сеансу связи. Фильтр пакетов способен распознать пакет существующего диалога TCP только по признакам, выяснив состояние бита SYN (установлен или сброшен). Брандмауэр SPI, чтобы выяснить принадлежность пакета, сравнивает его характеристики с Таблицей существующих подключений, а также допустимых подключений. Для этого брандмауэр хранит таблицу подключений, содержащую IP-адреса отправителя и получателя, информацию о транспортном протоколе и порте получателя. Фактически, может сохраняться и любая другая информация, включая последовательные номера TCP, которые помогают брандмауэру точней идентифицировать пакет как часть существующего диалога.*
*2. В зависимости от протокола, пакет может быть исследован далее. Некоторые популярные протоколы имеют множество широко известных дефектов. Производители брандмауэров предусмотрели функциональные возможности, позволяющие улучшить способность брандмауэра защитить хосты от злонамеренной деятельности. Если брандмауэр обладает такими возможностями для протокола пакета, то он сможет прочитать и часть данных пакета. Впоследствии это будет использовано в ходе принятия решения о возможности передачи пакета на основании его содержимого.*
*3. Если в таблице подключений нет элемента соответствующего рассматриваемому пакету, то брандмауэр исследует его на соответствие правилам. Набор правил для большинства брандмауэров SPI подобен набору правил фильтров пакетов: IP-адрес и порт отправителя, IP-адрес и порт получателя, используемый протокол. Соответствующий набору правил пакет может быть впоследствии (но не обязательно) подвергнут дополнительному исследованию данных, как было описано ранее.*
*4. Если на основании данных отправителя, получателя, протокола и содержимого пакет будет признан допустимым, брандмауэр передаст его конечному получателю, а также создаст или модифицирует соответствующую запись о данном диалоге в своей таблице подключений. Впоследствии он использует эту запись при проверке ответного пакета.*
*5. Чтобы выяснить, когда именно удалять запись из таблицы подключений, брандмауэры используют таймер или ожидают пакет TCP с установленным битом FIN.*

# Преимущества SPI

*Описанные процессы имеют перед технологией фильтрации пакетов два существенных преимущества. Таблица подключений значительно уменьшает вероятность подделки IP-адреса отправителя на соответствующий схеме внутренних IP-адресов атакуемой сети (spoofing) и предотвратить маскировку пакетов под часть уже установленного соединения. Поскольку фильтрующие пакеты брандмауэры не регистрируют установленные сеансы связи, они вынуждены полагаться лишь на формат пакета (а именно на состояние бита SYN заголовка пакета TCP), чтобы выяснить, не является ли пакет частью уже проверенного и установленного диалога. Это допускает возможность подделки пакетов TCP и не обеспечивает никаких способов проверки состояния пакетов UDP или ICMP. Хранение таблицы подключений предоставляет брандмауэру намного больше информации, используемой в процессе принятия решения о допустимости пакета.Еще одним преимуществом брандмауэров SPI перед брандмауэрами фильтрации пакетов является их способность исследовать содержимое пакетов некоторых типов. В связи с широкой известностью ряда дефектов общепринятых протоколов, эта возможность является очень ценной. Например протоколы SMTP и FTP. Оба, и сервер и клиент FTP уязвимы при получении неправильно оформленного запроса или команды. Способность брандмауэра SPI контролировать содержимое пакета, позволяет организовать проверку правильности передаваемых команд.*
*Обратите внимание, это возможно только для тех протоколов, которые передают команды в незашифрованном и незакодированном виде. Протокол FTP, например, допускает просмотр команд и даже определение направления их передачи. Просматривая информацию*

*порта TCP, брандмауэр способен определить, какая из сторон диалога является клиентом, а какая сервером. Впоследствии он может идентифицировать команды, передаваемые с обеих сторон, и проверять, не посылает ли сервер клиенту недопустимые команды, и наоборот. На подобном принципе основана и защита протокола SMTP. Протокол SMTP обладает рядом команд, передача которых может оказаться нежелательной. Эти команды могут спровоцировать утечку информации, которую организация не желает публиковать. Брандмауэр с возможностью защиты трафика протокола SMTP пропустит на сервер SMTP только те команды, передача которых разрешена явно. Остальные команды, в том числе и злонамеренные, будут просто отброшены.*

*Но поскольку брандмауэры с фиксацией состояния ищут в содержимом пакета лишь соответствие указанным строкам, обеспечиваемая ими степень зашиты внутренних хостов оказывается несколько ниже, чем у брандмауэров прикладного уровня. Кроме того, они не выступают в роли прокси-сервера и не устанавливают соединения от имени индивидуального отправителя. Этот подход обеспечивает намного более выт сокую производительность (как с точки зрения общей пропускной способности, так и количества подключений), а также более быструю обработку каждого пакета. Быстродействие процессоров SPI превышает возможности быстрого Ethernet (FastEthernet), открывая, таким образом, новый рынок для средств защиты таких высокоскоростных каналов связи, как OC-12 и Gigabit Ethernet. Хотя на настоящий момент спрос на рынке средств защиты каналов связи с Internet на таких скоростях не очень велик, подобные брандмауэры все чаще устанавливают внутри корпоративных сетей, для обеспечения безопасности между сегментами одной сети.*

# Методы реализации

*В этом разделе описаны типы брандмауэров, устанавливаемых на различных платформах. Здесь нет подробного анализа всех их преимуществ и недостатков для каждой платформы, а лишь приведен обзор, позволяющий продемонстрировать различные механизмы, используемые для защиты периметра сети.*

## Хост-ориентированные брандмауэры

*Производители брандмауэров используют два способа развертывания программного обеспечения брандмауэров на аппаратных средствах серверов. Первый — сугубо как приложение. Этот метод развертывания брандмауэров основан на знании особенностей существующих платформ. Как правило, брандмауэр устанавливается и выполняется как отдельное приложение, поверх коммерческой операционной системы. Хотя большинство операционных систем обладает как минимум одним собственным приложением брандмауэра, такие наиболее популярные операционные системы, как.Windows NT/2000, Sun Solaris и HPUX способны сами выполнять функции брандмауэров. Они поддерживают фильтрацию пакетов, шлюзы прикладного уровня, шлюзы канального уровня и брандмауэры проверки пакетов с фиксацией состояния.*

*Предпосылкой к установке брандмауэра на операционной системе является защищенность самой операционной системы. Этот прием известен под названием укрепления (hardening) операционной системы и должен осуществляться на любой системе, подключенной к небезопасной сети. Как уже было сказано ранее, хост-ориентированный брандмауэр всегда должен жестко придерживаться стандартов и политик безопасности, принятых в организации. В этих документах (стандарты и политика) должны быть отображены принципы обеспечения безопасности для каждого ресурса (концепция минимального набора прав, например).*

*Применение большинства брандмауэров-приложений, выполняющихся поверх сурествующих операционных систем, не исключает ряда дополнительных мер по улучшению безопасности хоста, включая замену некоторых из сетевых демонов операционной системы на более*

*надежные, замену или изменения стека TCP/IP, изменение файлов запуска, файлов конфигурации, записей в системном реестре и добавление новых процессов.*
*Второй способ подразумевает интеграцию с операционной системой, а не установку поверх нее. В этом случае базовая операционная система (обычно Unix), настраивается и укрепляется, а затем в нее жестко интегрируется приложение брандмауэра. Обычно такой способ применяется для операционных систем, не обладающих функциональными возможностями полной коммерческой версии, поскольку производители в этом случае удаляют все необязательные функциональные возможности. Обычно в результате получается платформа, даже более защищенная, чем коммерческая версия операционной системы, и без необходимости приспосабливать организацию к изменившимся возможностям новой операционной системы.*

## Брандмауэры, ориентированные на маршрутизаторы

*Маршрутизаторы достаточно часто используют в качестве первой линии обороны комплексной архитектуры безопасности, а иногда (особенно в малых сетях) их используют вместо брандмауэров. Причина в стоимости: небольшие организации просто не могут позволить себе приобретение относительно дорогостоящих автономных устройств защиты сети, а также связанных с ними затрат на администрирование и поддержку.*
*За последние годы функциональные возможности ориентированных на маршрутизаторы брандмауэров фильтрации пакетов существенно улучшились, они легки в эксплуатации и недороги. Некоторые реализации пошли даже дальше фильтрации пакетов. Функциональные возможности средств защиты, применяемых на маршрутизаторах, продолжают совершенствоваться, наряду с дополнениями, не имеющими отношения к безопасности.*
*В общей архитектуре безопасности, реализация маршрутизатора в качестве устройства защиты весьма популярна. Маршрутизатор, выполняющий предварительную фильтрацию пакетов, снижает нагрузку на брандмауэры SPI и брандмауэры прикладного уровня. Это оптимизирует архитектуру брандмауэров и маршрутизаторов: маршрутизатор выполняет предварительную проверку пакетов, а брандмауэр, обладающий большими функциональными возможностями, исследует только те из них, которые проходят через первый набор фильтров.*

## Интегрированные хост-ориентированные брандмауэры

*Интегрированный хост-ориентированный брандмауэр является, как правило, составной частью программного обеспечения, установленного на одиночной системе для защиты только ее. Если к таким небезопасным сетям, как Internet, подключена только одна или две машины, то хост-ориентированные брандмауэры являются наиболее экономичным решением. Интегрированные хост-ориентированные брандмауэры обычно устанавливают в небольших офисах, насчитывающих от одного до пяти компьютеров.*
*В корпоративной среде, где защиты требуют сотни или тысячи машин, подключенных в корпоративную сеть, интегрированный хост-ориентированный брандмауэр не обеспечивает ни централизованного управления, ни достаточной масштабируемости. Корпорации все чаще стандартизуют и устанавливают хост-ориентированные брандмауэры своим конечным пользователям для использования в домашних сетях. Это становится особенно актуально по мере увеличения популярности "не выключающихся" (always-on) широкополосных подключений.*

## Брандмауэры-устройства

*Брандмауэры-устройства — это специальные устройства (состоящие из аппаратных средств и программного обеспечения), предназначенные для контроля поступающего на них*

*трафика и принятия решения о необходимости его передачи. Свою операционную систему, программное обеспечение и необходимые данные брандмауэры-устройства хранят не на жестком диске, а на флэш-карте (flash card) или микросхеме (chip). Микросхема подобна микросхемам запоминающих устройств, используемых в персональных компьютерах, но при выключении питания информация на ней не теряется, а сохраняется подобно микросхемам BIOS (постоянное запоминающее устройство). Диапазон брандмауэров-устройств весьма широк: от самых дешевых с низкой производительностью и очень простыми возможностями (применяемых в небольших офисах и индивидуальными пользователями дома), до самых дорогих специализированных устройств, способных обслуживать несколько интерфейсов Gigabit Ethernet. Такие брандмауэры обладают чрезвычайно высокой производительностью, т.к. они не обременены множеством дополнительных функций операционной системы. Размер операционных систем этих устройств очень мал, лишь несколько мегабайт (вплоть до недавних времен они умещались на 3.5" гибком диске). Устройства обычно настраивают при помощи интерфейса командной строки, их собственных утилит или Web-ориентированных интерфейсов, предоставляющих доступ по протоколу HTTP.*

# СПИСОК ЛИТЕРАТУРЫ

1. *Страссберг К. Е. «Полный справочник по брандмауэрам»*
2. *Шоберг А. Г. Курс лекций по предмету «Сети ЭВМ и Телекоммуникации»*
3. *Польман Н., Кразерс Т. «Архитектура брандмауэров для сетей предприятия: Пер. с англ.»*