БРАНДМАУЭРЫ

Брандмауэр, фаерволл, межсетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основная задача - защита компьютерных сетей или отдельных узлов от несанкционированного доступа

В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на:

*-традиционный сетевой* (или *межсетевой*)  *экран* — программа (или неотъемлемая часть операционной системы) на шлюзе (сервере, передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями.

*-Персональный сетевой экран* — программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие на:

* *сетевом уровне*, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;
* *сеансовом уровне*  — отслеживающие сеансы между приложениями, не пропускающие пакеты, нарушающие спецификации TCP/IP.
* *уровне приложений -* фильтрация на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Возможности брандмауэра

* фильтрация доступа к заведомо незащищенным службам;
* препятствование получению закрытой информации из защищенной подсети, внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
* контроль доступа к узлам сети;
* регистрация попыток доступа как извне, так и из внутренней сети, что позволяет вести учёт использования доступа в Интернет отдельными узлами сети;
* регламентирование порядка доступа к сети;
* уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран;

Проблемы, не решаемые файрволом

* не защищает узлы сети от проникновения через «люки» или уязвимости ПО;
* не обеспечивает защиту от многих внутренних угроз (утечки данных);
* не защищает от загрузки пользователями вредоносных программ, в том числе вирусов;

Политики проекта брандмауэра

* разрешить доступ для сервиса, если он явно не запрещен
* запретить доступ для сервиса, если он явно не разрешен

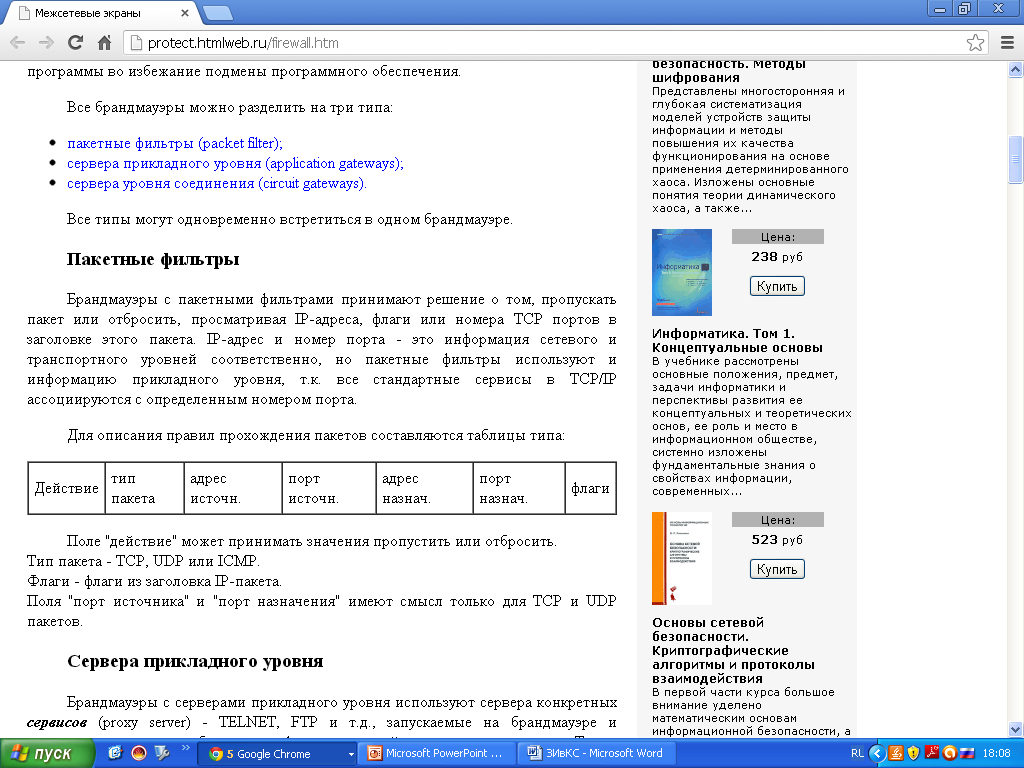
Брандмауэр, который реализует первую политику, пропускает все сервисы в сеть по умолчанию, если только этот сервис не был явно указан в политике управления доступом как запрещенный. Брандмауэр, который реализует вторую политику, по умолчанию запрещает все сервисы, но пропускает те, которые указаны в списке разрешенных сервисов.

Типы брандмауров

* пакетные фильтры (packet filter)
* сервера прикладного уровня (application gateways)
* сервера уровня соединения (circuit gateways)

**Пакетные фильтры**

* принимают решение о том, пропускать пакет или отбросить, просматривая IP-адреса, флаги или номера TCP портов в заголовке этого пакета.
* Для описания правил прохождения пакетов составляются таблицы типа:



**Действие** - может принимать значения пропустить или отбросить. Если подходящее правило не было найдено, использу-ется политика по умолчанию - либо разрешено все, что не запре-щено, либо запрещено все, что не разрешено.   
**Тип пакета** - TCP, UDP или ICMP.   
**Флаги** - флаги из заголовка IP-пакета.   
Поля "**порт источника**" и "**порт назначения**" имеют смысл только для TCP и UDP пакетов.

В качестве данных для анализа могут также использоваться

* длина IP-пакета,
* направление передачи пакета,
* текущее время.

Дополнительной возможностью пакетных фильтров является трансляция сетевых адресов и портов или изменение реальных адресов компьютеров внутренней сети на вымышленные (виртуальные), причем несколько (или все) внутренние адреса могут транслироваться в один сетевой адрес (с изменением номеров портов). Кроме аспектов, связанных с аспектами защиты, это может использоваться в случае, если количество компьютеров, подключенных к сети Интернет, в организации больше, чем количество сетевых адресов, официально выделенных данной организации.

Достоинства и недостатки пакетных фильтров

Достоинства:

1. относительно невысокая стоимость;
2. гибкость в определении правил фильтрации;
3. максимальная пропускная способность.

Недостатки:

· локальная сеть видна из сети Интернет;

· не учитывается содержимое IP-пакетов;

· правила фильтрации пакетов трудны в описании;

· при нарушении работоспособности МЭ все компьютеры за ним становятся незащищенными либо недоступными;

· аутентификацию с использованием IP-адреса (внешней сети) можно обмануть подменой адреса;

· отсутствует аутентификация на пользовательском уровне.

Сервера прикладного уровня

МЭ прикладного уровня существует много - под каждый протокол прикладного (и сеансового) уровня. Каждый МЭ допускает и защищает только тот протокол, который он поддерживает (реализуется политика "запрещено все, что не разрешено").

Наиболее популярные поддерживаемые МЭ протоколы:

· гипертекстовые протоколы - HTTP, SHTTP, HTTPS, Gopher;

· протокол пересылки файлов - FTP;

· почтовые протоколы - SMTP, POP3, IMAP, NNTP;

· протоколы удаленного доступа - Telnet, rlogin, rsh, rexec, RPC, XWindow;

· протокол сетевой файловой системы - NFS, NetBEUI;

· протокол службы имен - DNS;

· "безопасные" протоколы - SSH, SSL, S/MIME, SOCKS.

компьютер-инициатор в начале сеанса связи передает МЭ имя компьютера-адресата и запрашиваемого сервиса. Здесь же может передаваться и имя пользователя, с правами которого будет осуществляться доступ. В схеме передачи данных между двумя соединениями вместо простого копирования используется техника высокоуровневой фильтрации, трансляции и кэширования данных

* Так как МЭ функционирует на прикладном уровне, то у него существуют большие возможности по фильтрации прикладных команд и данных. Например, для протокола FTP возможно запрещение команды "put" - команды записи файла на сервер. Возможна организация разграничения доступа к объектам сервера.
* Если МЭ поддерживает "безопасный" протокол, то возможно поддержание конфиденциальности и целостности передаваемых данных через внешнюю сеть данных путем шифрования данных и вычисления криптографических контрольных сумм. В этом случае компьютер-инициатор тоже должен поддерживать тот же самый "безопасный" протокол либо необходим еще один МЭ прикладного уровня, поддерживающий тот же самый "безопасный" протокол.

Достоинства и недостатки МЭ прикладного уровня

Достоинства:

* возможность усиленной аутентификации компьютера-инициатора и пользователя;
* возможность защиты от подмены во время связи аутентифицированного компьютера-инициатора;
* возможна защита целостности и конфиденциальности передаваемых данных и команд;
* фильтрация пересылаемых команд и данных;
* большая гибкость в протоколировании передаваемых команд и данных.

Недостатки:

необходимость в существовании нескольких МЭ для разных сервисов.

**Сервера уровня соединения**

Сервер уровня соединения - транслятор TCP соединения. Пользователь образует соединение с определенным портом на брандмауэре, после чего последний производит соединение с местом назначения по другую сторону от брандмауэра. Во время сеанса этот транслятор копирует байты в обоих направлениях, действуя как посредник. Посредничество заключается в том, что связь между двумя компьютерами физически осуществляется через систему-посредника и реально состоит из двух TCP-соединений.

* компьютер-инициатор не передает МЭ имя компьютера-адресата - его IP-адрес и номер TCP-порта фиксированы для конкретного МЭ и известны. МЭ уровня соединения используются только для организации безопасного соединения от внешних компьютеров (удаленных рабочих станций) к внутреннему компьютеру (серверу поддержки локальной сети или информационному серверу).
* после установления связи факт ее существования уже запротоколирован и проведена аутентификация компьютера-инициатора связи.

Достоинства и недостаткиМЭ уровня соединений

Достоинства:

· локальная сеть может быть невидимой из глобальной сети;

· наличие аутентификации компьютера-инициатора по его символьному имени;

· использование политики "запрещено все, что не разрешено";

· способность гибкого регулирования (ограничения) пропускной способности;

· возможность эффективного противостояния атакам с неправильной фрагментацией пакетов соединения;

· возможность использования статистической информации о соединениях для определения попыток соединения злоумышленником и автоматического блокирования его действий.

Недостатки:

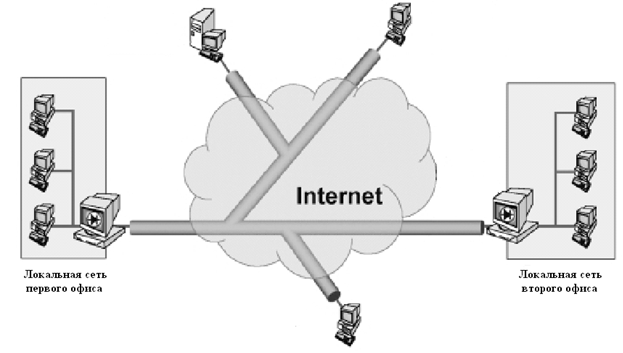
· отсутствие аутентификации пользователя;

· нет защиты целостности и конфиденциальности данных;

· возможность подмены злоумышленником IP-адреса компьютера-инициатора;

Виртуальные частные сети

* *Виртуальной частной сетью (VPN)* называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную сеть, обеспечивающую безопасность циркулирующих данных.
* Защита информации при ее передаче по открытому каналу основана на построении *криптозащищенных туннелей* (*туннелей VPN*). Каждый из таких туннелей представляет собой виртуальное соединение, созданное в открытой сети, по которому передаются криптографически защищенные сообщения виртуальной сети. Пример возможной организации виртуальной частной сети



Основные задачи

* Аутентификация взаимодействующих сторон.
* Криптографическая защита передаваемой информации.
* Подтверждение подлинности и целостности доставленной информации.
* Защита от повтора, задержки и удаления сообщений.
* Защита от отрицания фактов отправления и приема сообщений.

наиболее часто используемые способы

* Конечные точки защищенного туннеля совпадают с конечными точками защищаемого потока сообщений. Данный вариант является наилучшим с точки зрения безопасности. В этом случае обеспечивается полная защищенность канала вдоль всего пути следования пакетов сообщений. Однако, такой вариант ведет к децентрализации управления и избыточности ресурсных затрат.
* Конечные точки защищенного туннеля совпадают с МЭ или пограничным маршрутизатором локальной сети. В данном случае поток сообщений внутри локальной сети оказывается незащищенным, а все сообщения, выходящие из локальной сети, передаются по криптозащищенному туннелю.
* Конечные точки – провайдеры INTERNET. В этом случае не защищаются каналы локальной сети и выделенные каналы связи, защищаются только каналы INTERNET.
* Протоколы поддержки виртуальных частных сетей создаются на одном из трех уровней модели OSI – канальном, сетевом или сеансовом.
* Канальному уровню соответствуют такие протоколы реализации VPN, как PPTP, L2F, L2TP. Сетевому уровню соответствуют протоколы IPSec, SKIP. Сеансовому уровню – SSL, SOCKS. Чем ниже уровень эталонной модели OSI, на котором реализуется защита, тем она прозрачнее для приложений и незаметнее для пользователей. Однако при снижении этого уровня уменьшается набор реализуемых услуг безопасности и становится труднее организация управления. Оптимальное соотношение между прозрачностью и качеством защиты достигается при формировании защищенных виртуальных каналов на сетевом уровне модели OSI.