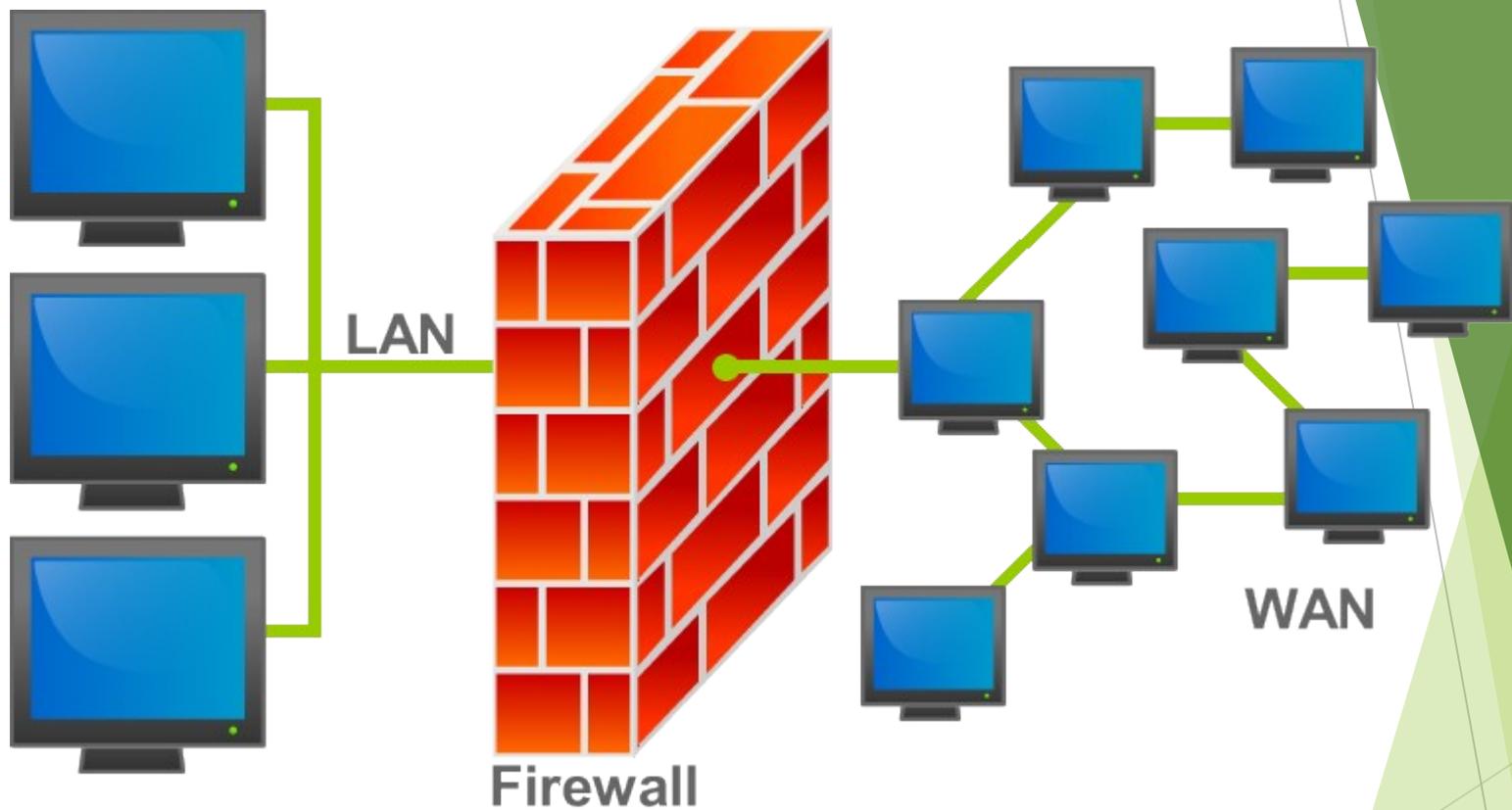


Межсетевой экран и его
функции. Основные
компоненты
брандмауэра.

Межсетевой экран или **сетевой экран** — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов — динамическую замену внутрисетевых (серых) адресов или портов на внешние, используемые за пределами ЛВС.



Расположение сетевого экрана (Firewall) в сети.

Другие названия

Брандмауэр (нем. *Brandmauer*) – заимствованный из немецкого языка термин, являющийся аналогом английского *firewall* в его оригинальном значении (стена, которая разделяет смежные здания, предохраняя от распространения пожара).

Интересно, что в области компьютерных технологий в немецком языке употребляется слово «Firewall».

Файрвóлл, файрвóл, файервóл, фаервóл – образовано транслитерацией английского термина *firewall*.

Разновидности сетевых экранов

Сетевые экраны подразделяются на различные типы в зависимости от следующих характеристик:

- ▶ обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями;
- ▶ на уровне каких сетевых протоколов происходит контроль потока данных;
- ▶ отслеживаются ли состояния активных соединений или нет.

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, контролирующее 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.

Вырожденный случай – использование традиционного сетевого экрана сервером, для ограничения доступа к собственным ресурсам.

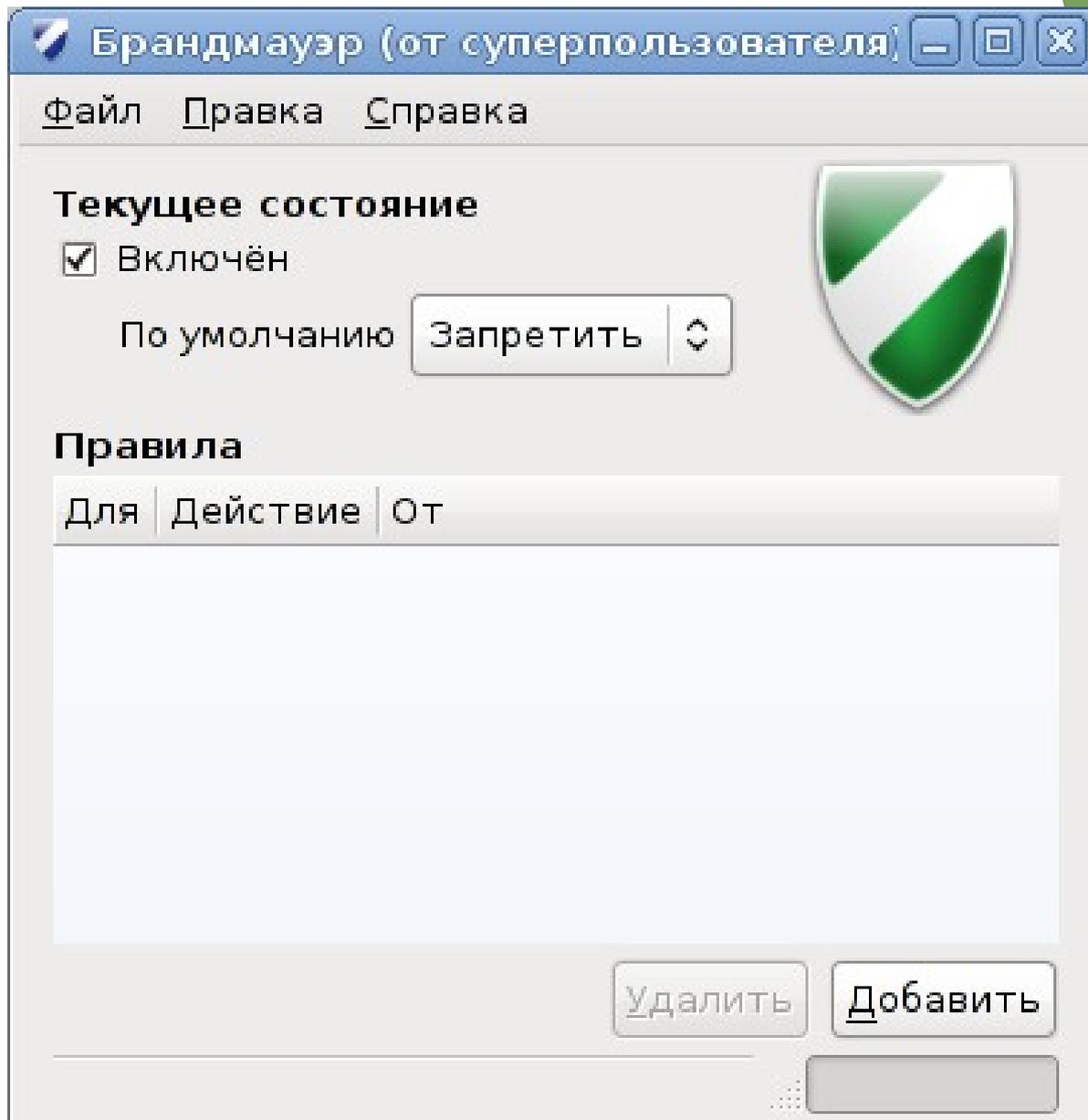
В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие на:

- ▶ *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* (также известные как stateful) – отслеживающие сеансы между приложениями, не пропускающие пакеты нарушающих спецификации TCP/IP, часто используемых в злонамеренных операциях – сканировании ресурсов, взломах через неправильные реализации TCP/IP, обрыв/замедление соединений, инъекция данных.
- ▶ *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.

Некоторые решения, относимые к сетевым экранам уровня приложения, представляют собой прокси-серверы с некоторыми возможностями сетевого экрана, реализуя прозрачные прокси-серверы, со специализацией по протоколам. Возможности прокси-сервера и многопротокольная специализация делают фильтрацию значительно более гибкой, чем на классических сетевых экранах, но такие приложения имеют все недостатки прокси-серверов (например, анонимизация трафика).

В зависимости от отслеживания активных соединений сетевые экраны бывают:

- ▶ *Stateless* (простая фильтрация), которые не отслеживают текущие соединения (например, TCP), а фильтруют поток данных исключительно на основе статических правил;
- ▶ *Stateful*, stateful packet inspection (SPI) (фильтрация с учётом контекста), с отслеживанием текущих соединений и пропуском только таких пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений. Такие типы сетевых экранов позволяют эффективнее бороться с различными видами DoS-атак и уязвимостями некоторых сетевых протоколов. Кроме того, они обеспечивают функционирование таких протоколов, как H.323, SIP, FTP и т. п., которые используют сложные схемы передачи данных между адресатами, плохо поддающиеся описанию статическими правилами, и, зачастую, несовместимых со стандартными, *stateless* сетевыми экранами.



Пример пользовательского интерфейса на платформе Debian GUN/Linux.

Типичные возможности

- ▶ Фильтрация доступа к заведомо незащищенным службам;
- ▶ Препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
- ▶ Контроль доступа к узлам сети;
- ▶ Может регистрировать все попытки 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;

Вследствие защитных ограничений могут быть заблокированы некоторые необходимые пользователю службы, такие как [Telnet](#), [FTP](#), [SMB](#), [NFS](#), и так далее. Поэтому настройка файрвола требует участия специалиста по сетевой безопасности. В противном случае вред от неправильного конфигурирования может превысить пользу.

Также следует отметить, что использование файрвола увеличивает время отклика и снижает пропускную способность, поскольку фильтрация происходит не мгновенно.

Вследствие защитных ограничений могут быть заблокированы некоторые необходимые пользователю службы, такие как Telnet, FTP, SMB, NFS, и так далее. Поэтому настройка файрвола требует участия специалиста по сетевой безопасности. В противном случае вред от неправильного конфигурирования может превысить пользу.

Также следует отметить, что использование файрвола увеличивает время отклика и снижает пропускную способность, поскольку фильтрация происходит не мгновенно.

Проблемы, не решаемые файрволом

Межсетевой экран сам по себе не панацея от всех угроз для сети. В частности, он:

- ▶ Не защищает узлы сети от проникновения через «люки» (англ. *back doors*) или уязвимости ПО;
- ▶ Не обеспечивает защиту от многих внутренних угроз, в первую очередь – утечки данных;
- ▶ Не защищает от загрузки пользователями вредоносных программ, в том числе вирусов;

Для решения последних двух проблем используются соответствующие дополнительные средства, в частности, антивирусы. Обычно они подключаются к файрволу и пропускают через себя соответствующую часть сетевого трафика, работая как прозрачный для прочих сетевых узлов прокси, или же получают с файрвола копию всех пересылаемых данных. Однако такой анализ требует значительных аппаратных ресурсов, поэтому обычно проводится на каждом узле сети самостоятельно.