Безопасность сети. Средства обеспечения безопасности сети

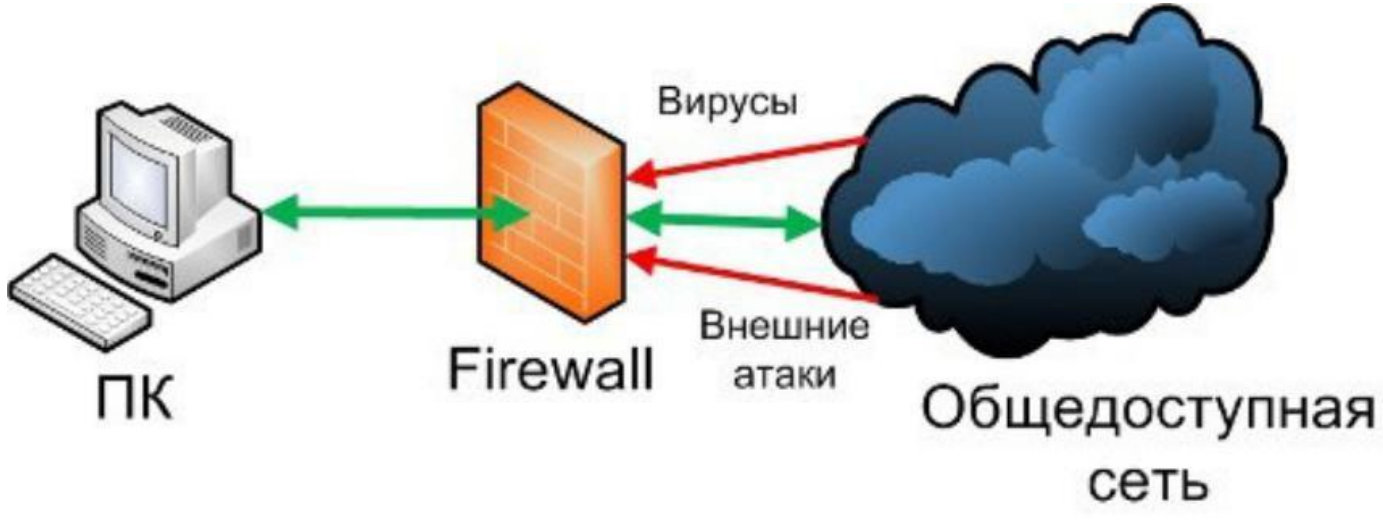
Подготовил: Вусик А.С.

Безопасность сети. Средства обеспечения безопасности сети

- Компьютерная и сетевая безопасность
- Брандмауэр
- Механизм виртуальных частных сетей
- Безопасная информационная система
- Конфиденциальность, доступность, целостность данных. Сервисы сетевой безопасности
- Шифрование информации,Аутентификацию,Идентификация,Авторизацию, Аудит,Технология защищенного канала

Брандмауэр

- Брандмауэр представляет собой межсетевой экран, который контролирует обмен сообщениями, ведущийся по протоколам всех уровней, и не пропускает подозрительный трафик в сеть. Брандмауэр может использоваться и внутри сети, защищая одну подсеть от другой. Помимо брандмауэра аналогичные проблемы призваны решать встроенные средства безопасности операционных систем и приложений, таких как базы данных, а также встроенные аппаратные средства компьютера.



Типы фаерволов

Существует три базовых типа брандмауэров:

- фильтры пакетов сетевого уровня (или stateless),
- с сохранением состояния (или stateful),
- и прикладного уровня.

Пример брандмауэра

Comodo Firewall

ZoneAlarm Free

GlassWire

TinyWall

Функции брандмауэров

Для обеспечения компьютерной безопасности нужно защитить от несанкционированного доступа все ресурсы, находящиеся внутри локальной сети:

- аппаратные ресурсы (серверы, дисковые массивы, маршрутизаторы),
- программные ресурсы (операционные системы, СУБД, почтовые службы и т. п.),
- данные, хранящиеся в файлах и обрабатываемые в оперативной памяти.

Наиболее часто используемым средством защиты этого типа является брандмауэр, устанавливаемый в местах всех соединений внутренней сети с Интернетом.

Функции брандмауэров

Идеальный персональный брандмауэр должен выполнять шесть функций:

- **1. Блокировка внешних атак.**

В идеале брандмауэр должен блокировать все известные типы атак, включая сканирование портов, IP-спуффинг, DoS и DDoS, подбор паролей и пр.

- **2. Блокировка утечки информации.**

Даже если вредоносный код проник в компьютер (не обязательно через сеть, а, например, в виде вируса на купленном пиратском CD), брандмауэр должен предотвратить утечку информации, заблокировав вирусу выход в сеть.

- **3. Контроль приложений.**

Неизбежное наличие открытых дверей (то есть открытых портов) является одним из самых узких мест в блокировке утечки информации, а один из самых надежных способов воспрепятствовать проникновению вирусов через эти двери — контроль приложений, запрашивающих разрешение на доступ. Кроме банальной проверки по имени файла, весьма желательна проверка аутентичности приложения.

Функции брандмауэров

- **4. Поддержка зональной защиты.**

Работа в локальной сети часто подразумевает практически полное доверие к локальному контенту, что открывает уникальные возможности по использованию новейших (как правило, потенциально опасных) технологий. В то же время уровень доверия к Интернет-контенту значительно ниже, а значит, необходим дифференцированный подход к анализу опасности того или иного содержания.

- **5. Протоколирование и предупреждение.**

Брандмауэр должен собирать лишь необходимый объем информации — избыток (равно как и недостаток) сведений недопустим. Возможность настройки файлов регистрации и указания причин для привлечения внимания пользователя весьма приветствуются.

- **6. Максимально прозрачная работа.**

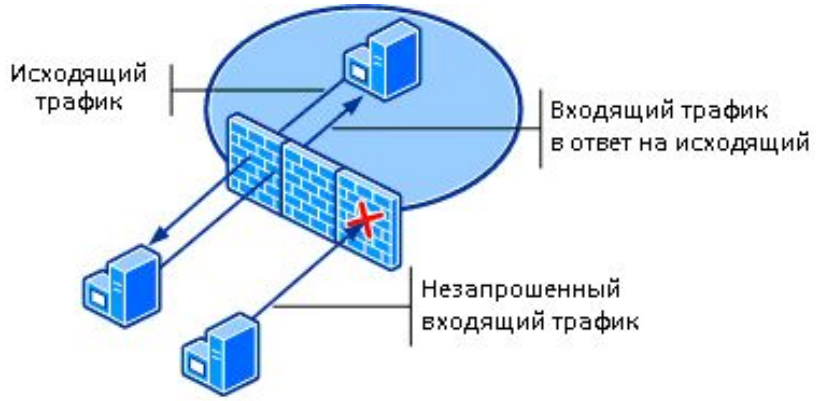
Эффективность и применяемость системы часто обратно пропорциональны сложности ее настройки, администрирования и сопровождения. Несмотря на традиционный скепсис в отношении мастеров (wizards) по настройке и прочих «буржуйских штучек», даже опытные администраторы не пренебрегают ими просто в целях экономии времени.

Входящий и исходящий трафик

Сетевой трафик, с точки зрения сервера, может быть либо входящим, либо исходящим; брандмауэр поддерживает отдельный набор правил для каждого вида трафика.

Трафик, который происходит из любой точки сети называется входящим трафиком. Он воспринимается не так, как исходящий трафик, который отправляется сервером. Как правило, сервер разрешает исходящий трафик, потому что считает себя заслуживающим доверия. Однако набор правил для исходящего трафика может использоваться для предотвращения нежелательной коммуникации в случае, если сервер взломан злоумышленником или вредоносным исполняемым файлом.

Чтобы использовать преимущества безопасности брандмауэра по максимуму, нужно определить все способы взаимодействия других систем с вашим сервером, создать правила, которые явно позволяют такое взаимодействие, а затем сбросить весь оставшийся трафик. Имейте в виду, что также нужно создать соответствующие правила для исходящего трафика, чтобы сервер мог отправлять подтверждения для разрешенных входящих соединений. Кроме того следует учитывать, что серверу, как правило, нужно инициировать свой исходящий трафик (например, для загрузки обновлений или подключения к базе данных), а потому важно продумать эти случаи и создать для них набор правил.



Правила фаерволов

Сетевой трафик проходит список правил брандмауэра в определённой последовательности, которая называется цепочкой правил. Как только фаервол обнаруживает правило, которому отвечает трафик, он выполняет соответствующее действие для этого трафика.

Пример работы фаервола

Предположим, у вас есть сервер со списком правил для входящего трафика:

Принимать (accept) новый и ранее установленный трафик на сетевой интерфейс через порт 80 и 443 (веб-трафик HTTP и HTTPS).

Сбрасывать (drop) входящий трафик от IP-адресов нетехнических сотрудников офиса на порт 22 (SSH).

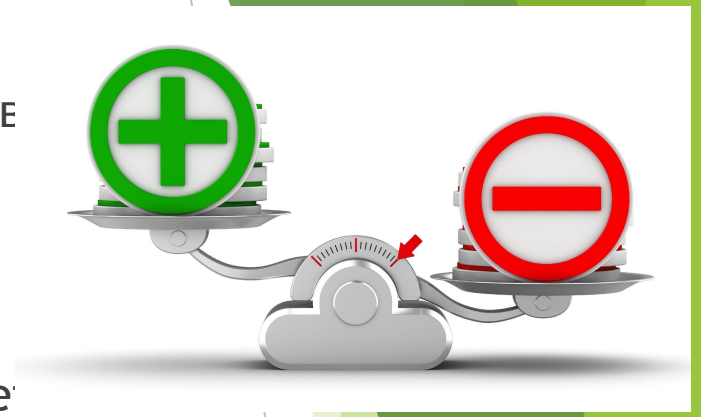
Принимать новый и существующий входящий трафик IP-диапазона офиса на частный сетевой интерфейс через порт 22 (SSH).

Обратите внимание на слова «accept» и «drop» в этих примерах. С их помощью задаётся действие, которое фаервол должен выполнить в случае, если трафик отвечает правилу.

- Accept значит разрешить трафик;
- Reject – заблокировать трафик и вернуть ошибку «unreachable»;
- Drop – заблокировать трафик и не возвращать ничего.

Далее правило должно содержать условия, с которыми сопоставляется каждый пакет трафика.

Недостатки брандмауэров



Нельзя забывать и об обратной стороне медали — о недостатках брандмауэров, причем не отдельных решений, а всей технологии в целом.

Разрозненность систем защиты

Это одна из самых важных проблем, решить которую пытаются немало поставщиков, но пока без особого успеха. Во многих брандмауэрах отсутствует защита от саботажа со стороны авторизованных пользователей. Этот вопрос можно рассматривать с этической, социальной или любой другой точки зрения, но сути дела это не меняет: брандмауэры не способны запретить авторизованному пользователю украсть (передать, уничтожить, модифицировать) важную информацию. И хотя уже давно существуют другие решения (например, разграничение доступа и пр.), проблема заключается в разрозненности всех подобных систем, которые, по сути, должны выполнять одну и ту же функцию. Пока антивирусные программы, системы обнаружения вторжений, разграничения доступа и др. не получат единого центра управления, эффективность каждой из них можно смело делить на два.

Недостатки брандмауэров

- Снижение производительности

К счастью, подобные вопросы возникают все реже и реже, особенно у индивидуальных пользователей, стремящихся защитить свой ПК или небольшую локальную сеть. В то же время крупные локальные сети по-прежнему генерируют столь емкий трафик, что обычными программными (дешевыми или бесплатными) решениями сеть не прикроешь. Аппаратные решения демонстрируют отличную производительность и масштабируемость, но вот цена (порой исчисляемая десятками тысяч долларов) переводит вопросы их применения в совершенно иную плоскость, так что порой максимум возможного — это выделение специального сервера, заточенного исключительно под обслуживание брандмауэра. Естественно, подобное универсальное решение автоматически сказывается на уменьшении скорости доступа.

- Отсутствие защиты для нестандартных или новых сетевых сервисов

Решением здесь в какой-то мере могут служить шлюзы на уровне соединения или пакетные фильтры, но, как уже говорилось, им недостает гибкости. Конечно, существуют определенные возможности по туннелированию нестандартного трафика, например в HTTP, но этот вариант нельзя назвать удобным сразу по нескольким причинам. Есть множество унаследованных систем, код которых переписать невозможно, однако оставлять их беззащитными тоже нельзя.

Спасибо за внимание!