РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

РЕФЕРАТ К ДОКЛАДУ

Тема: «Межсетевые экраны»

дисциплина: Информационная безопасность

Студент: Евсеева Дарья Олеговна

Группа: НФИбд-01-19

МОСКВА

2022 г.

Оглавление

Введение

Проблема обеспечения компьютерной безопасности является очень важной и актуальной в современном мире. Несанкционированный доступ, кража информации, нарушения в работе локальных сетей и т.д. являются серьезными угрозами и требуют эффективных решений. Одним из средств защиты от подобных угроз являются межсетевые экраны.

Что такое межсетевые экраны?

Межсетевой экран (Firewall, брандмауэр) представляет собой программно-аппаратный или программный комплекс, который отслеживает сетевые пакеты и блокирует или разрешает их прохождение. В фильтрации трафика межсетевой экран опирается на установленные параметры, которые задаются администратором. Чаще всего такие параметры называют правилами межсетевого экрана. В качестве параметров могут использоваться, например, IP-адреса, доменные имена, порты или протоколы.

Межсетевые экраны часто называют фильтрами, так как они осуществляют фильтрацию пакетов, не подходящих под критерии, определённые в конфигурации. Основной задачей межсетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа, т.е. обеспечение сетевой безопасности. Примером функций, выполняемых межсетевыми экранами, могут служить: обнаружение подмены трафика, защита корпоративной сети от DDoS-атак или блокировка передачи данных на неизвестный IP-адрес.

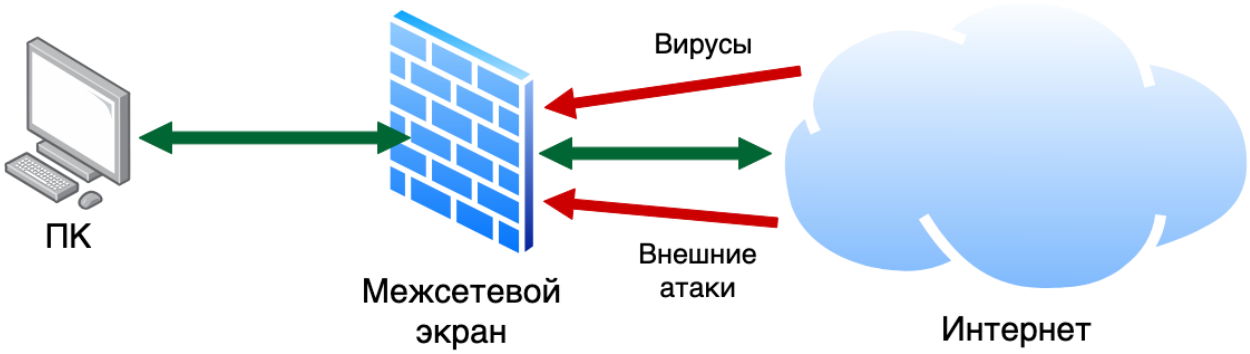

Рис. 1. Принцип работы межсетевого экрана

Классификация межсетевых экранов

Далее рассмотрим различные варианты классификации межсетевых экранов.

По способу реализации

Первый вариант классификации межсетевых экранов – по способу реализации. В данном случае межсетевые экраны подразделяются на программные и программно-аппаратные.

Программные межсетевые экраны представляют собой специальное программное обеспечение, которое устанавливается на компьютер и защищает сеть от внешних угроз. Межсетевой экран может являться отдельной программой, а также быть частью какого-либо приложения (например, антивирусной программы). Данный тип межсетевых экранов является удобным и недорогим решением для частных ПК или небольших локальных сетей.

Для обеспечения защиты сетей крупных компаний и организаций используются аппаратно-программные комплексы. Они представляют собой специальные устройства, функционал которых ограничивается только задачами межсетевого экрана. Такие устройства, как правило, работают на основе операционных систем FreeBSD или Linux. Еще один вариант реализации аппаратно-программных комплексов – в виде специального модуля в штатном сетевом оборудовании (например, коммутаторе или маршрутизаторе).

По применяемой технологии фильтрации трафика

Также, существует классификация межсетевых экранов в зависимости от применяемой технологии фильтрации трафика. В данном случае можно выделить несколько основных типов межсетевых экранов:

- Прокси-сервер

Прокси-сервер выполняет функцию шлюза, он обеспечивает пользователю анонимность и защищает от некоторых сетевых угроз. С помощью прокси-сервера можно создать межсетевой экран на уровне приложения.

Основным достоинством данной технологии является обеспечение полной информации о приложениях. Однако, этот вариант нельзя называть эффективным вариантом реализации межсетевого экрана из-за присутствия таких проблем, как, например, необходимость использования отдельного прокси для каждого сервиса (что существенно ограничивает количество доступных сервисов и возможность масштабирования) и недостаточная производительность межсетевого экрана.

- Межсетевой экран с контролем состояния сеансов

Данный тип межсетевого экрана является одним из самых популярных. В данном случае межсетевой экран принимает решение о пропуске или блокировке трафика на основе анализа состояния порта и протокола. Также, при принятии решения межсетевой экран учитывает не только правила, которые были заданы администратором, но и контекст, что значительно повышает эффективность работы.

- Межсетевой экран UTM

Главное достоинство межсетевых экранов UTM (Unified Threat Management) заключается в эффективном сочетании таких функций, как контент-фильтр, служба IPS (Intrusion Prevention System, система предотвращения вторжений) и антивирусная защита. В данном случае появляется необходимость администрирования только одного

устройства (вместо нескольких), за счет чего повышаются эффективность и удобство управления защитой сети.

- Межсетевой экран нового поколения

Межсетевые экраны нового поколения (NGFW, Next-Generation Firewall) созданы для противостояния современным угрозам. Межсетевые экраны данного типа выполняют все основные функции, характерные для обычных межсетевых экранов, однако они способны выполнять фильтрацию уже не просто на уровне протоколов и портов, а на уровне протоколов приложений и их функций, что позволяет блокировать атаки и вредоносную активность намного более эффективно.

- Межсетевой экран нового поколения с активной защитой от угроз

Данный тип межсетевого экрана является модернизацией обычного межсетевого экрана нового поколения (NGFW). Он предназначен для обеспечения эффективной защиты от угроз с высокой степенью сложности.

Вместе со всеми возможностями обычных межсетевых экранов нового поколения, они поддерживают такие функции, как, например, учет контекста и обнаружение ресурсов, создающих повышенные риски, на его основе, автоматизация функций безопасности (что повышает быстродействие и оперативность отражения сетевых атак), а также применение корреляции событий на ПК и в сети (что позволяет повысить эффективность обнаружения потенциально вредоносной активности).

Ограниченность возможностей

При использовании межсетевых экранов необходимо понимать, что их возможности по анализу трафика ограничены. Любой межсетевой экран может анализировать только такой трафик, который он способен четко идентифицировать и интерпретировать. Если же межсетевой экран не распознает тип трафика, то он теряет свою эффективность, так как не способен принять обоснованное решение насчет действий в отношении такого трафика. Поэтому при задании правил для межсетевого экрана очень важно определить порядок действий в случае приема трафика, который не поддается однозначной интерпретации.

Выводы

Итак, мы рассмотрели понятие межсетевого экрана, различные варианты классификации межсетевых экранов, а также сложности, которые могут возникнуть при их использовании.

Список литературы

1. Межсетевой экран (Firewall) // URL: https://www.tadviser.ru/index.php/Статья:Межсетевой_экран_(Firewall)
2. Межсетевые экраны – виды и особенности // URL: https://www.smart-soft.ru/blog/mezhsetevye-ekrany-vidy/
3. Межсетевой экран: что такое и как работает // URL: https://selectel.ru/blog/firewall/
4. Межсетевой экран: что это такое и как он защищает корпоративные сети и сайты от злоумышленников // URL: https://mcs.mail.ru/blog/mezhsetevoy-ekran-chto-eto-takoe-i-kak-on-zashchishchaet