Понятие межсетевого экрана (Firewalls)

Обычно у компании есть внутренняя сеть: серверы, компьютеры сотрудников, маршрутизаторы. В этой сети хранится конфиденциальная информация: корпоративная тайна, персональные данные, данные сотрудников. Внутренняя сеть соединяется с глобальным интернетом, и это опасно — злоумышленники могут использовать такое соединение, чтобы похитить данные.

Для защиты устанавливают межсетевые экраны — программы или устройства, которые охраняют границы корпоративной сети.

Межсетевой экран (МЭ, файрвол, брандмауэр) — инструмент, который фильтрует **входящий и исходящий** сетевой трафик. Он анализирует источник трафика, время передачи, IP-адрес, протокол, частоту сообщений и другие параметры, после чего принимает решение: пропустить или заблокировать трафик.

У межсетевых экранов бывают стандартные настройки — например, он может блокировать все входящие подключения или исходящие пакеты от определенных приложений. Для корпоративных целей экраны, как правило, настраивают дополнительно — задают протоколы, порты, разрешения для приложений. Обычно этим занимается системный администратор или специалист по информационной безопасности.

Классический межсетевой экран не изучает передаваемые данные, не ищет вредоносный код, ничего не шифрует и не расшифровывает. Он работает только с сетевыми параметрами соединения, а точнее — с признаками отдельных IP-пакетов, из которых состоит это соединение, такими как IP-адреса соединяющихся компьютеров и некоторые другие параметры.

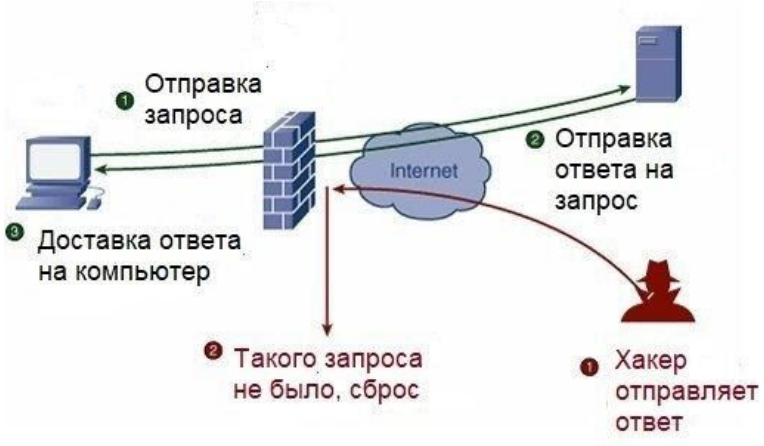

Рис. 1. Упрощенный пример работы Файрвола

Межсетевой экран выступает в качестве барьера между двумя сетями, например, внутренней сетью компании и интернетом. Он защищает от:

−Несанкционированного доступа из интернета в защищенную сеть. Например, если из интернета придет пакет данных от ненадежного адресата, МЭ его не пропустит.

−Неконтролируемых сетевых подключений. Если кто-то попытается устроить DDoS-атаку, чтобы уронить серверы компании, МЭ не пропустит все эти пакеты данных.

−Несанкционированной передачи из защищенной сети в интернет. Например, вирус проник на сервер, собрал данные и пытается отправить их хакеру. МЭ заметит передачу подозрительному адресату и заблокирует ее — данные не утекут в сеть.

Чаще всего межсетевой экран устанавливают на границе корпоративной сети и интернета. Но можно поставить его и внутри корпоративной сети, чтобы создать отдельную, особо защищенную сеть. Например, дополнительно фильтровать трафик к серверам с самыми секретными данными. Кроме того, экран может стоять на отдельном компьютере и защищать только его. В этом случае его иногда называют сетевым (а не межсетевым), однако по классификации ФСТЭК он также будет относиться к межсетевым экранам.

Межсетевые экраны бывают двух видов: аппаратные и программные. Они выполняют одинаковые функции, но работают немного по-разному:

−**Программно-аппаратные комплексы (ПАК), или аппаратные МЭ** — специальные устройства или компоненты роутеров, на которых установлено фильтрующее программное обеспечение. Все железо и ПО внутри этого устройства специализировано на фильтрации трафика и нескольких смежных задачах, дополнительные программы на аппаратный МЭ поставить нельзя. Это снижает уязвимость такого устройства к атакам и позволяет обеспечивать защищенность более высокого класса.

−**Программные МЭ** — программное обеспечение на сервере, которое занимается фильтрацией трафика. По сути, это то же ПО, что установлено в аппаратном МЭ, но оно устанавливается на сам сервер.

Аппаратные МЭ обычно стоят на границе сети, например, там, где внутренняя сеть подключается к интернету. Программные стоят на узлах самой внутренней сети, то есть защищают непосредственно компьютеры и серверы.

Аппаратные МЭ дороже, но надежнее, обеспечивают более серьезную защиту. Программные дешевле, но менее надежны — есть риск, что трафик от злоумышленника успеет навредить сети. Кроме того, программные межсетевые экраны часто настолько нагружают компьютер, на который установлены, что там ничего больше нельзя установить. Из-за этого для них иногда выделяют отдельный сервер — и этот сервер фактически играет роль аппаратного межсетевого экрана.

Межсетевой экран можно развернуть и на облачном сервере. Его можно расположить на границе логической локальной сети в облаке точно так же, как физический МЭ можно расположить на границе физической корпоративной сети. Такой МЭ будет фильтровать соединения на границе виртуальной частной сети.

Если компания хранит персональные данные, то, согласно 152-ФЗ, она обязана обеспечить им защиту. Чтобы защищать данные в соответствии с требованиями закона, компании нужно использовать средства защиты, сертифицированные ФСТЭК. Такой сертификат подтверждает, что программа или устройство действительно надежно защищает данные. ФСТЭК сертифицирует в том числе межсетевые экраны — как программные, так и аппаратные.

То есть, если вы храните в базах данных информацию о своих сотрудниках или клиентах, вы работаете с персональными данными, а значит, обязаны обеспечить им защиту. Иногда это подразумевает, что нужно задействовать сертифицированный ФСТЭК межсетевой экран.

Сертификат ФСТЭК также может подтвердить, что МЭ подходит для защиты государственной тайны. Так что компании, которые хранят такие сведения, тоже обязаны использовать только сертифицированные межсетевые экраны.

Если вы не храните гостайну или персональные данные, необязательно устанавливать именно сертифицированный ФСТЭК межсетевой экран. Но если вы

заботитесь о секретности ваших данных, при выборе экрана имеет смысл обратить внимание на сертификат — он подтвердит, что выбранный МЭ действительно надежный.

ВИДЫ МЕЖСЕТЕВЫХ ЭКРАНОВ ПО КЛАССИФИКАЦИИ ФСТЭК

Для сертификации межсетевого экрана ФСТЭК определяет его профиль защиты. Профиль нужно знать, чтобы понять, в какой конкретно системе, с какими целями и для защиты каких данных можно использовать этот экран.

К каждому профилю есть конкретные технические требования, а сам профиль зависит от двух параметров: типа МЭ и его класса защиты.

Типы межсетевых экранов по ФСТЭК:

−«А» — аппаратные, установленные на физических границах сети. Например, программно-аппаратные комплексы в месте физического подключения сети компании к интернету через кабель.

−«Б» — программные и аппаратные, установленные на логических границах сети, например встроенные в маршрутизатор.

−«В» — программные, установленные на узлы, например компьютеры сотрудников.

−«Г» — аппаратные и программные, работающие с протоколами http и https, то есть с веб-трафиком.

−«Д» — аппаратные и программные, которые работают с промышленными протоколами передачи данных.

Классы защиты межсетевых экранов по ФСТЭК:

−6 класс — самый низший, подходит для работы с персональными данными 3 и 4 уровня защищенности. Про уровни защищенности персональных данных описано в методике определения актуальных угроз ПДн при их обработке в ИСПДн.

−5 класс — подходит для работы с данными 2 уровня защищенности.

−4 класс — подходит для работы с данными 1 уровня защищенности.

−1, 2 и 3 класс — необходим для работы с гостайной.

Класс защиты Тип межсетевого экрана	6	5	4	3	2	1
Межсетевой экран типа "А"	ИТ.МЭ. А6.ПЗ	ИТ.МЭ. А5.ПЗ	ИТ.МЭ. А4.ПЗ	ИТ.МЭ. А3.ПЗ	ИТ.МЭ. А2.ПЗ	ИТ.МЭ. А1.ПЗ
Межсетевой экран типа "Б"	ИТ.МЭ. Б6.ПЗ	ИТ.МЭ. Б5.ПЗ	ИТ.МЭ. Б4.ПЗ	ИТ.МЭ. Б3.ПЗ	ИТ.МЭ. Б2.ПЗ	ИТ.МЭ. Б1.ПЗ
Межсетевой экран типа "В"	ИТ.МЭ. В6.ПЗ	ИТ.МЭ. В5.ПЗ	ИТ.МЭ. В4.ПЗ	ИТ.МЭ. В3.ПЗ	ИТ.МЭ. В2.ПЗ	ИТ.МЭ. В1.ПЗ
Межсетевой экран типа "Г"	ИТ.МЭ. Г6.ПЗ	ИТ.МЭ. Г5.ПЗ	ИТ.МЭ. Г4.ПЗ	-	-	-
Межсетевой экран типа "Д"	ИТ.МЭ. Д6.ПЗ	ИТ.МЭ. Д5.ПЗ	ИТ.МЭ. Д4.ПЗ	-	-	-

Типы и классы защиты не зависят друг от друга напрямую. Например, может существовать экран типа «А» с 6 классом защищенности или экран типа «В» с 1 классом.

Комбинация типа и класса защиты определяет профиль защиты каждого конкретного межсетевого экрана. И именно от профиля зависят технические требования к МЭ.

Таблица определения профиля защиты межсетевого экрана. Для некоторых профилей нет 1, 2 и 3 уровней защиты — такие экраны не используют для хранения гостайны.

Получается, что профилей защиты всего 24. На сайте ФСТЭК выложены требования к 15 профилям — ко всем, кроме тех, что требуют 1, 2 и 3 уровня защиты. Эти профили — закрытая информация, так как они используются для хранения гостайны.

***Пример**: представим, что компании нужно установить межсетевой экран на компьютер сотрудника. Сотрудник работает с персональными данными 3 уровня защищенности — значит, ей нужен межсетевой экран 6 уровня защиты и типа «В», для установки на узел сети. Это экран с профилем ИТ.МЭ. В6.ПЗ. Получается, нужно искать межсетевой экран с сертификатом, соответствующим выбранному профилю. Профили более высокого уровня тоже подойдут — например, можно поставить и экран ИТ.МЭ. В4.ПЗ.*

Если этой же компании понадобится межсетевой экран на границе сети, это будет уже экран типа «А» и того же 6 уровня защищенности — экран профиля ИТ.МЭ. А6.ПЗ.

Общепринято делят файрволы на традиционные, файрволы UTM и файрволы NGFW. Традиционный файрвол относится к «родителям» современного сетевого экрана. На рынке он еще встречается, но уже не так актуален, как его более новые сородичи. По сути, он только контролирует доступ к вашей сети, то есть разрешает или запрещает проходить какому-либо интернет-трафику в вашу сеть.

Файрвол NGFW или, по-другому, файрвол следующего/нового поколения - ультрасовременный межсетевой экран с функциями обнаружения и предотвращения угроз, VPN и полного контроля интернет-приложений.

Межсетевой экран UTM – это «универсальный солдат», который включает в себя абсолютно все: антиспам, антивирус, тот же NGFW и другие функции. Он предназначен для комплексной сетевой защиты. Такое сочетание «всего в одном» - главный козырь UTM устройств, т.к. это получается значительно дешевле чем покупать отдельно службу предотвращения вторжений, фильтр, антивирус и др., а еще гораздо проще осуществляется процесс настройки и управление межсетевым экраном, чем отдельно каждым устройством, выполняющим только одну функцию.

Что важно знать о межсетевых экранах, сертифицированных ФСТЭК

−Межсетевой экран фильтрует трафик — не пропускает подозрительный трафик внутрь защищенной сети и не выпускает его из нее.

−Межсетевые экраны бывают аппаратные и программные. Аппаратные — отдельные устройства, которые заняты только фильтрацией трафика. Программные — специальное ПО, которое устанавливают на компьютеры и серверы.

−Если вы храните персональные данные или государственную тайну, то обязаны обеспечить им защиту. Межсетевой экран — одна из таких защитных мер.

−Для гарантии надежности межсетевого экрана производители получают сертификат ФСТЭК. Только МЭ, сертифицированный ФСТЭК, можно использовать для защиты персональных данных.

−ФСТЭК делит межсетевые экраны на профили, в зависимости от назначения и уровня защиты, который они обеспечивают. Чем секретнее данные, которые вы храните, тем более защищенный МЭ нужно выбирать.

Межсетевые экраны (МЭ) с фильтрацией пакетов

МЭ с фильтрацией пакетов обеспечивают защиту сети путем фильтрации сетевых сообщений на основе информации, содержащейся в заголовках TCP/IP каждого пакета.

Фильтры пакетов принимают решение исходя из следующих данных заголовка:

−IP-адрес источника;

−IP-адрес отправителя;

−применяемый сетевой протокол (TCP, UDP, ICMP);

−порт источника TCP или UDP;

−порт назначения TCP или UDP;

−тип сообщения ICMP (Internet Control Message Protocol – протокол управляющих сообщений в сети Интернет), если применяется протокол ICMP.

Существуют различные стратегии реализации фильтров пакетов. Наиболее популярными являются следующие две.

1. Построение правил – от наиболее конкретных к наиболее общим.
2. Правила упорядочиваются таким образом, чтобы наиболее часто используемые из них находились во главе списка. Это сделано для повышения эффективности.

Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола и поэтому могут использоваться с любым протоколом, работающим через IP. Некоторые протоколы требуют распознавания межсетевым экраном выполняемых ими действий. Например, FTP будет использовать одно соединение для начального входа и команд, а другое - для передачи файлов. Соединения, используемые для передачи файлов, устанавливаются как часть соединения FTP, и поэтому межсетевой экран должен уметь считывать трафик и определять порты, которые будут использоваться новым соединением. Если межсетевой экран не поддерживает эту функцию, передача файлов невозможна.

Достоинства МЭ с фильтрацией пакетов:

−производительность – фильтрация происходит на скорости, близкой к скорости передачи данных;

−хороший способ управления трафиком;

−прозрачность.

Недостатки МЭ с фильтрацией пакетов:

−низкий уровень масштабируемости. По мере роста наборов правил становится все труднее избегать «ненужных» соединений;

−возможность открытия больших диапазонов портов;

−подверженность атаки с подменой данных. Атаки с подменой данных, как правило, подразумевают присоединение ложной информации в заголовок TCP/IP.

Межсетевые экраны, работающие только посредством фильтрации пакетов, не используют модули доступа, и поэтому трафик передается от клиента непосредственно на сервер. Если сервер будет атакован через открытую службу, разрешенную правилами политики межсетевого экрана, межсетевой экран никак не отреагирует на атаку. Межсетевые экраны с пакетной фильтрацией также позволяют видеть извне внутреннюю структуру адресации. Внутренние адреса скрывать не требуется, так как соединения не прерываются на межсетевом экране.