СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 9

Межсетевое экранирование

Преподаватель: **Батыргалиев Асхат Болатканович, PhD, ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»**

askhat.b.b@gmail.com

Содержание

1. Понятие межсетевого экранирования
2. Классификация межсетевых экранов
3. Уязвимости межсетевых экранов

По завершению лекции Вы будете знать:

1. Понятие межсетевого экранирования
2. Классификация межсетевых экранов
3. Уязвимости межсетевых экранов

Понятие межсетевого экранирования

Межсетевое экранирование является одним из основных элементов эшелонированной обороны ЛВС.

Межсетевой экран (*МЭ*) – это специализированный комплекс межсетевой защиты, называемый также системой *firewall* или брандмауэром.

Межсетевой экран, сетевой экран - программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

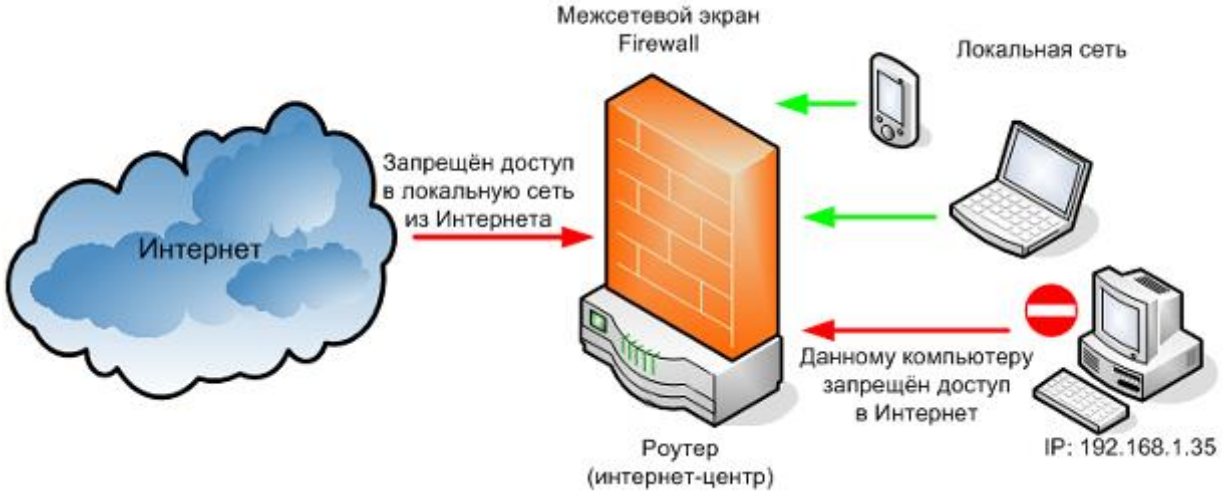
Межсетевой экран позволяет разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Интернет. Обычно межсетевые экраны защищают внутреннюю сеть предприятия от вторжений из глобальной сети Интернет, хотя они могут использоваться и для защиты от нападений из корпоративной интрасети, к которой подключена локальная сеть предприятия. Технология межсетевых экранов стала одной из самых первых технологий защиты корпоративных сетей от внешних угроз.

Для большинства организаций установка межсетевого экрана является необходимым условием обеспечения безопасности внутренней сети.

Понятие межсетевого экранирования

Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

Наиболее распространённое место для установки межсетевых экранов - граница периметра локальной сети для защиты внутренних хостов от атак извне. Однако атаки могут начинаться и с внутренних узлов - в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечёт границу сетевого периметра, и межсетевой экран не будет задействован. Поэтому в настоящее время межсетевые экраны размещают не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности.



Понятие межсетевого экранирования

Межсетевой экран предназначен для защиты от следующих типов киберугроз:

- **Бэкдор-доступа**

Это атаки с использованием уязвимостей в установленном на ПК программном обеспечении: операционной системе, утилитах, прикладных приложениях. Такие бреши могут иметься везде, включая Windows, они позволяют хакеру получить доступ к устройству, посылать и принимать с него с трафик. Брандмауэр блокирует подобные действия.

- **Фишинг**

Мошенническая схема, в ходе которой пользователь попадает на фальшивый (фишинговый) сайт, один в один копирующий известный веб-ресурс. Например, повторяет страницы входа в социальную сеть или оплаты через онлайн-банкинг. Человек вводит личные данные, и они попадают в руки злоумышленника. Файервол запрещает подключения к подозрительным сайтам.

- **Взлом удаленного доступа**

С помощью удаленного рабочего стола пользователь может управлять компьютером через интернет, т. е. дистанционно. Хакеры могут перехватить этот доступ и украсть важные данные. В задачи брандмауэра входит запрет на передачу такого трафика.

- **Переадресация маршрута**

Пакеты данных передаются по сети определенными маршрутами, а этот вид атак предполагает подмену пути следования информации таким образом, чтобы конечное устройство ничего не «заподозрило».

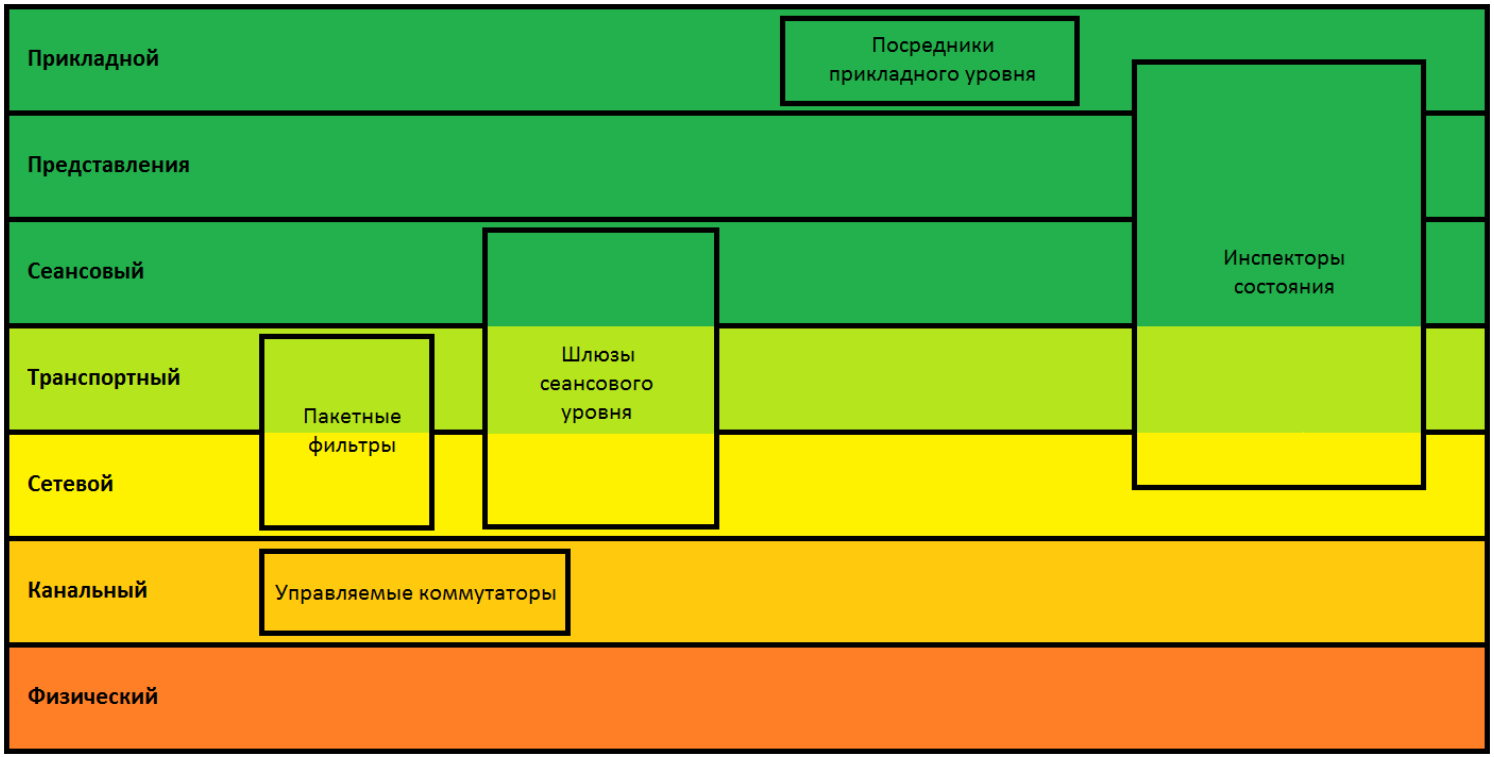
- **DDoS-атаки**

Поскольку главная задача брандмауэра — это фильтрация, он помогает справиться с наплывом огромных объемов трафика. Блокировка работает как на входящие, так и на исходящие пакеты, если ваше устройство попробуют использовать в качестве атакующего.

Классификация межсетевых экранов

Поддерживаемый уровень сетевой модели OSI является основной характеристикой при классификации межсетевых экранов:

1. Управляемые коммутаторы.
2. Пакетные фильтры.
3. Шлюзы сеансового уровня.
4. Посредники прикладного уровня.
5. Инспекторы состояния.



Классификация межсетевых экранов

Управляемые коммутаторы иногда причисляют к классу межсетевых экранов, так как они осуществляют фильтрацию трафика между сетями или узлами сети. Однако они работают на канальном уровне и разделяют трафик в рамках локальной сети, а значит не могут быть использованы для обработки трафика из внешних сетей (например, из Интернета).

При реализации политики безопасности в рамках корпоративной сети, основу которых составляют управляемые коммутаторы, они могут быть мощным и достаточно дешёвым решением. Взаимодействуя только с протоколами канального уровня, такие межсетевые экраны фильтруют трафик с очень высокой скоростью. Основным недостатком такого решения является невозможность анализа протоколов более высоких уровней.

Пакетные фильтры функционируют на сетевом уровне и контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов. Многие межсетевые экраны данного типа могут оперировать заголовками протоколов и более высокого, транспортного, уровня. Пакетные фильтры одними из первых появились на рынке межсетевых экранов и по сей день остаются самым распространённым их типом. Данная технология реализована в подавляющем большинстве маршрутизаторов и даже в некоторых коммутаторах.

Так как пакетные фильтры обычно проверяют данные только в заголовках сетевого и транспортного уровней, они могут выполнять это достаточно быстро. Поэтому пакетные фильтры, встроенные в пограничные маршрутизаторы, идеальны для размещения на границе с сетью с низкой степенью доверия. Однако, в пакетных фильтрах отсутствует возможность анализа протоколов более высоких уровней сетевой модели OSI. Кроме того, пакетные фильтры обычно уязвимы для атак, которые используют подделку сетевого адреса. Такие атаки обычно выполняются для обхода управления доступом, осуществляемого межсетевым экраном.

Классификация межсетевых экранов

Межсетевой экран сеансового уровня исключает прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая в качестве посредника (*proxy*), который реагирует на все входящие пакеты и проверяет их допустимость на основании текущей фазы соединения. **Шлюз сеансового уровня** гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению. Как только приходит запрос на установление соединения, в специальную таблицу помещается соответствующая информация (адреса отправителя и получателя, используемые протоколы сетевого и транспортного уровня, состояние соединения и др.). В случае, если соединение установлено, пакеты, передаваемые в рамках данной сессии, будут просто копироваться в локальную сеть без дополнительной фильтрации. Когда сеанс связи завершается, сведения о нём удаляются из данной таблицы. Поэтому все последующие пакеты, «притворяющиеся» пакетами уже завершённого соединения, отбрасываются.

Так как межсетевой экран данного типа исключает прямое взаимодействие между двумя узлами, шлюз сеансового уровня является единственным связующим элементом между внешней сетью и внутренними ресурсами. Это создаёт видимость того, что на все запросы из внешней сети отвечает шлюз, и делает практически невозможным определение топологии защищаемой сети. Кроме того, так как контакт между узлами устанавливается только при условии его допустимости, шлюз сеансового уровня предотвращает возможность реализации DoS-атаки, присущей пакетным фильтрам.

Несмотря на эффективность этой технологии, она обладает серьёзным недостатком: у шлюзов сеансового уровня отсутствует возможность проверки содержания поля данных, что позволяет злоумышленнику передавать «троянских коней» в защищаемую сеть.

Классификация межсетевых экранов

Межсетевые экраны прикладного уровня исключают прямое взаимодействие двух узлов. Однако, функционируя на прикладном уровне, они способны «понимать» контекст передаваемого трафика. Межсетевые экраны, реализующие эту технологию, содержат несколько приложений-посредников (*application proxy*), каждое из которых обслуживает свой прикладной протокол. Такой межсетевой экран способен выявлять в передаваемых сообщениях и блокировать несуществующие или нежелательные последовательности команд, что зачастую означает DoS-атаку, либо запрещать использование некоторых команд (например, FTP PUT, которая даёт возможность пользователю записывать информацию на FTP сервер).

Посредник прикладного уровня может определять тип передаваемой информации. Например, это позволяет заблокировать почтовое сообщение, содержащее исполняемый файл. Другой возможностью межсетевого экрана данного типа является проверка аргументов входных данных.

Посредники прикладного уровня способны выполнять аутентификацию пользователя, а также проверять, что SSL-сертификаты подписаны конкретным центром. Межсетевые экраны прикладного уровня доступны для многих протоколов, включая HTTP, FTP, почтовые (SMTP, POP, IMAP), Telnet и др.

Недостатками данного типа межсетевых экранов являются большие затраты времени и ресурсов на анализ каждого пакета. По этой причине они обычно не подходят для приложений реального времени. Другим недостатком является невозможность автоматического подключения поддержки новых сетевых приложений и протоколов, так как для каждого из них необходим свой агент.

Классификация межсетевых экранов

Инспекторы состояния

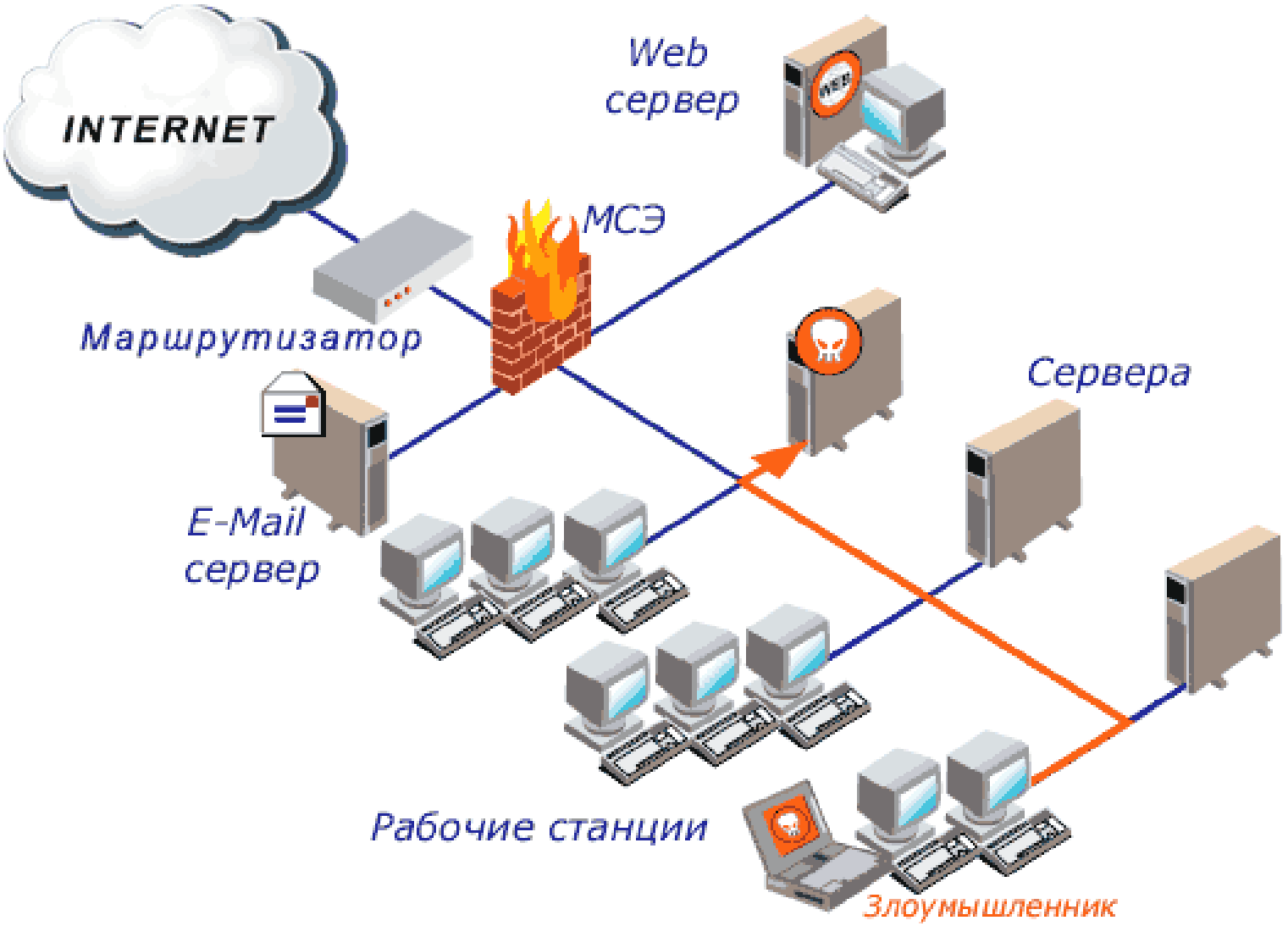
Каждый из вышеперечисленных типов межсетевых экранов используется для защиты корпоративных сетей и обладает рядом преимуществ. Однако, куда эффективней было бы собрать все эти преимущества в одном устройстве и получить межсетевой экран, осуществляющий фильтрацию трафика с сетевого по прикладной уровень. Данная идея была реализована в инспекторах состояний, совмещающих в себе высокую производительность и защищённость. Данный класс межсетевых экранов позволяет контролировать:

- ❑ каждый передаваемый пакет - на основе таблицы правил;
- ❑ каждую сессию - на основе таблицы состояний;
- ❑ каждое приложение - на основе разработанных посредников.

Осуществляя фильтрацию трафика по принципу шлюза сеансового уровня, данный класс межсетевых экранов не вмешивается в процесс установления соединения между узлами. Поэтому производительность инспектора состояний заметно выше, чем у посредника прикладного уровня и шлюза сеансового уровня, и сравнима с производительностью пакетных фильтров. Ещё одно достоинство инспекторов состояния - прозрачность для пользователя: для клиентского программного обеспечения не потребуется дополнительная настройка. Данные межсетевые экраны имеют большие возможности расширения. При появлении новой службы или нового протокола прикладного уровня для его поддержки достаточно добавить несколько шаблонов.

Однако, инспекторам состояний по сравнению с посредниками прикладного уровня свойственна более низкая защищённость.

Уязвимости межсетевых экранов



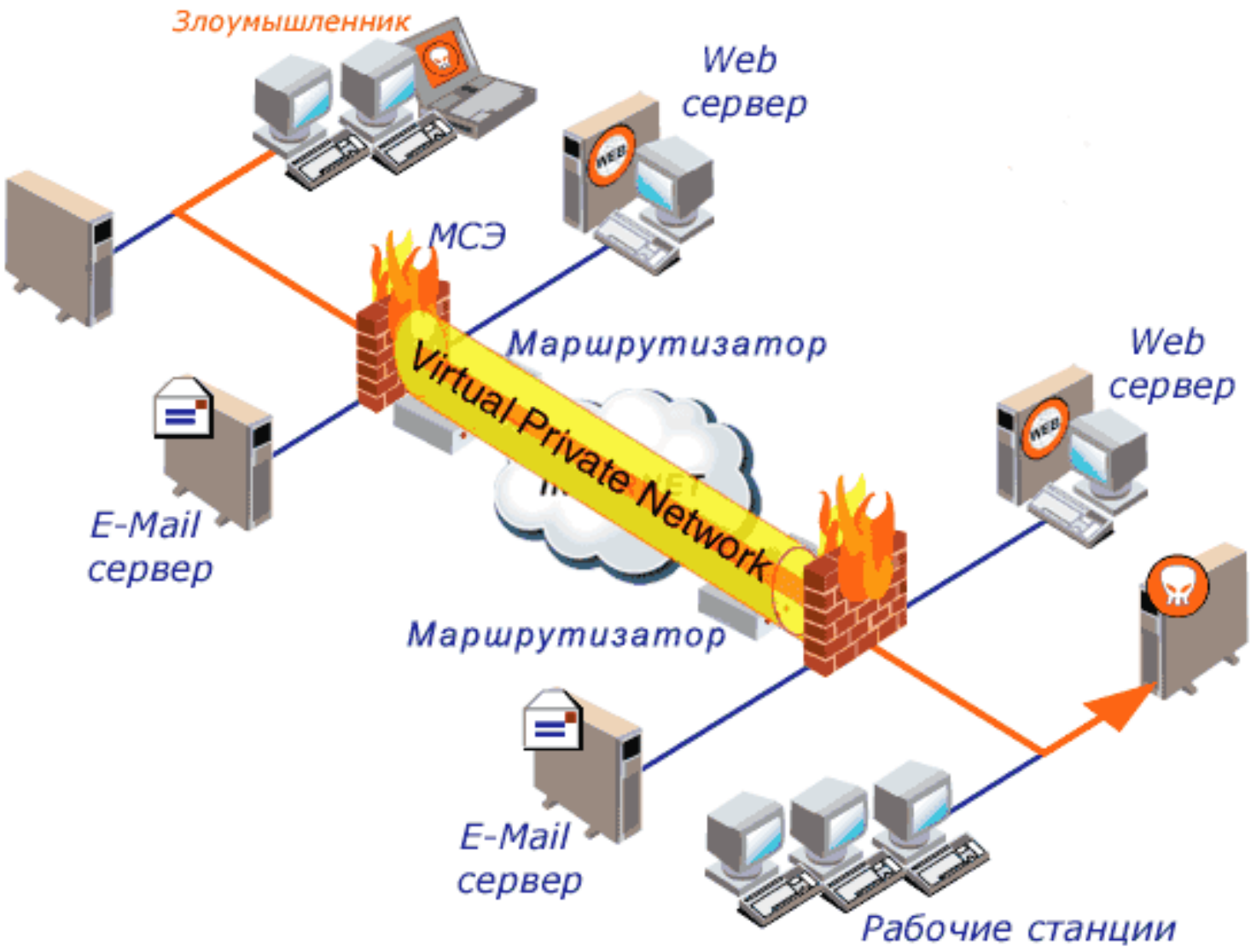
Уязвимости межсетевых экранов

Межсетевой экран фильтрует трафик и принимает решения о пропуске или блокировании сетевых пакетов, опираясь на информацию об используемом протоколе. Как правило, правила предусматривают соответствующую проверку с целью определения того, разрешен или нет конкретный протокол. Например, если на МСЭ разрешен 25 и 80 порты, то тем самым разрешается пропуск во внутреннюю сеть почтового (SMTP) и Web (HTTP) трафика.

Именно этот принцип обработки и используется квалифицированными злоумышленниками. Вся несанкционированная деятельность осуществляется в рамках разрешенного протокола, создавая тем самым в нем туннель, по которому злоумышленник и реализует атаку.

Самый простой пример, демонстрирующий применение туннелей - Internet-черви и макровирусы, заносимые в корпоративную сеть в виде вложений (attachments) в сообщения электронной почты. Если межсетевой экран разрешает прохождение SMTP-трафика, то во внутреннюю сеть может попасть и «вирусная инфекция».

Уязвимости межсетевых экранов



Уязвимости межсетевых экранов

Подмена адреса - это способ сокрытия реального адреса злоумышленника. Однако он может использоваться и для обхода защитных механизмов межсетевого экрана. Такой простейший способ, как замена адреса источника сетевых пакетов на адрес из защищаемой сети, уже не может ввести в заблуждение современные межсетевые экраны. Все они используют различные способы защиты от такой подмены.

Однако, сам принцип подмены адреса остается по-прежнему актуальным. Например, злоумышленник может подменить свой реальный адрес на адрес узла, у которого установлены доверенные отношения с атакуемой системой и реализовать на нее DoS-атаку.

В каждой организации есть пользователи, обладающие практически неограниченными правами в сети - сетевые администраторы. Они никому неподконтрольны и могут делать в сети практически все, что угодно. Как правило, они используют свои неограниченные права для выполнения своих функциональных обязанностей. Но представьте на минуту, что администратор чем-то обижен. Будь-то низкой зарплатой, недооценкой его возможностей, местью и т.п. Известны случаи, когда такие обиженные администраторы «портили кровь» не одной компании и приводили к очень серьезному ущербу.

Уязвимости межсетевых экранов

Абсолютное большинство межсетевых экранов построено на классических моделях разграничения доступа, разработанных в 1970-1980 годах. Согласно этим моделям субъекту (пользователю, программе, процессу или сетевому пакету) разрешается или запрещается доступ к какому-либо объекту (например, файлу или узлу сети) при предъявлении некоторого уникального, присущего только этому субъекту, элемента. В 80% случаев этим элементом является пароль. В других случаях таким уникальным элементом является Touch Memory, Smart или Proximity Card, биометрические характеристики пользователя и т.д. Для сетевого пакета таким элементом являются адреса или флаги, находящиеся в заголовке пакета, а также некоторые другие параметры.

Даже самый мощный и надежный межсетевой экран не защитит от проникновения в корпоративную сеть нарушителя, если последний смог подобрать или украсть пароль авторизованного пользователя. Мало того, межсетевой экран даже не зафиксирует нарушения, так как для него нарушитель, укравший пароль, является авторизованным пользователем.