Лекция №21. Технологии межсетевого экранирования.

Оглавление

[Введение 1](#_Toc509260558)

[1. Фильтрация трафика 5](#_Toc509260559)

[2. Выполнение функций посредничества. 6](#_Toc509260560)

[3. Дополнительные возможности МЭ 8](#_Toc509260561)

[Заключение. 10](#_Toc509260562)

# Введение

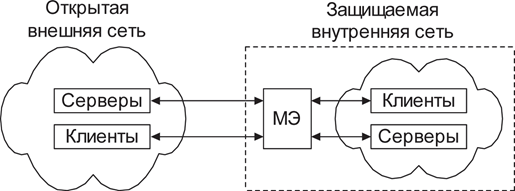
Межсетевое экранирование является одним из основных элементов эшелонированной обороны ЛВС.

*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.

Для противодействия несанкционированному межсетевому доступу межсетевой экран МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 1). При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно межсетевой экран входит в состав защищаемой сети.

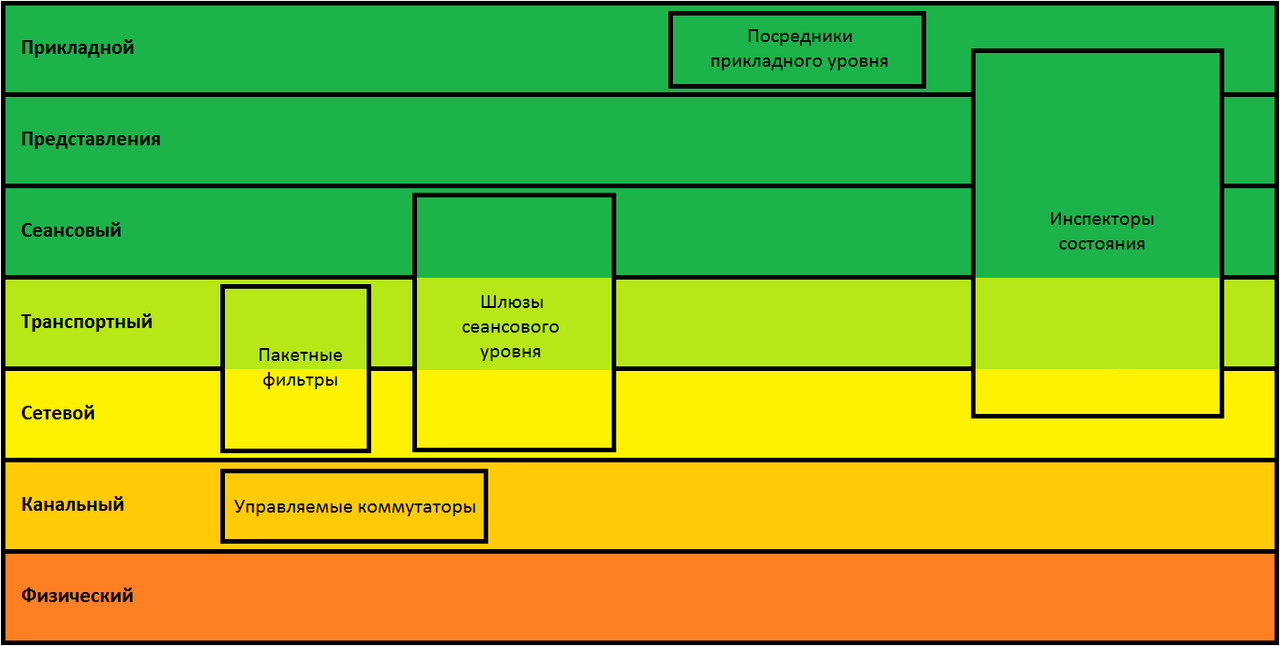
***Рис. 1. Схема подключения межсетевого экрана***

Межсетевой экран, защищающий сразу множество узлов внутренней сети, призван решить две основные задачи:

* + - ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой компании, пытающиеся получить доступ к серверам баз данных, защищаемых межсетевым экраном;
    - разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требуемым для выполнения служебных обязанностей.

До сих пор не существует единой общепризнанной классификации межсетевых экранов. МЭ можно классифицировать по следующим основным признакам.

*Классификация по функционированию на уровнях модели OSI*:

* + - управляемые коммутаторы
    - пакетные фильтры *(*экранирующий маршрутизатор *–* Screening Router);
    - шлюзы сеансового уровня (экранирующий транспорт);
    - прикладные шлюзы, посредники прикладного уровня (Application Gateway);
    - шлюзы экспертного уровня, инспекторы состояния (Stateful Inspection Firewall).

***Управляемые коммутаторы***

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).

Многие производители сетевого оборудования, такие как Cisco, HP, ZyXEL, предоставляют в своих коммутаторах возможность фильтрации трафика на основе MAC-адресов, содержащихся в заголовках фреймов. Например, в коммутаторах семейства Cisco Catalyst эта возможность реализована при помощи механизма Port Security. Однако данный метод фильтрации не является эффективным, так как аппаратно установленный в сетевой карте MAC-адрес легко меняется программным путем, поскольку значение, указанное через драйвер, имеет более высокий приоритет, чем зашитое в плату. Поэтому многие современные коммутаторы позволяют использовать другие параметры в качестве признака фильтрации — например, VLAN ID. Технология виртуальных локальных сетей (англ. Virtual Local Area Network) позволяет создавать группы хостов, трафик которых полностью изолирован от других узлов сети.

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 (Screening Router)***

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 (например, TCP или UDP). 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.

При анализе заголовка сетевого пакета могут использоваться следующие параметры:

* IP-адреса источника и получателя;
* тип транспортного протокола;
* поля служебных заголовков протоколов сетевого и транспортного уровней;
* порт источника и получателя.

Достаточно часто приходится фильтровать фрагментированные пакеты, что затрудняет определение некоторых атак. Многие сетевые атаки используют данную уязвимость межсетевых экранов, выдавая пакеты, содержащие запрещённые данные, за фрагменты другого, доверенного пакета. Одним из способов борьбы с данным типом атак является конфигурирование межсетевого экрана таким образом, чтобы блокировать фрагментированные пакеты. Некоторые межсетевые экраны могут дефрагментировать пакеты перед пересылкой во внутреннюю сеть, но это требует дополнительных ресурсов самого межсетевого экрана, особенно памяти. Дефрагментация должна использоваться очень обоснованно, иначе такой межсетевой экран легко может сам стать жертвой DoS-атаки.

Пакетные фильтры могут быть реализованы в следующих компонентах сетевой инфраструктуры:

* пограничные маршрутизаторы;
* операционные системы;
* персональные межсетевые экраны.

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[19][20].

***Шлюзы сеансового уровня***

Межсетевой экран сеансового уровня исключает прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая в качестве посредника (англ. 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 т. д.). 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: как и у всех вышеперечисленных классов межсетевых экранов, у шлюзов сеансового уровня отсутствует возможность проверки содержания поля данных, что позволяет злоумышленнику передавать «троянских коней» в защищаемую сеть.

***Посредники прикладного уровня***

Межсетевые экраны прикладного уровня, как и шлюзы сеансового 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 (англ. 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. Например, аргумент имени пользователя длиной в 100 символов либо содержащий бинарные данные является, по крайней мере, подозрительным.

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 другие.

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.

***Шлюзы экспертного уровня,*** ***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.

Термин инспектор состояния (англ. stateful inspection), внедрённый компанией Check Point Software, полюбился производителям сетевого оборудования настолько, что сейчас практически каждый межсетевой экран причисляют к этой технологии, даже если он и не реализует её полностью.

*По используемой технологии*:

* + - контроль состояния протокола (Stateful Inspection);
    - на основе модулей посредников (прокси).

*По исполнению*:

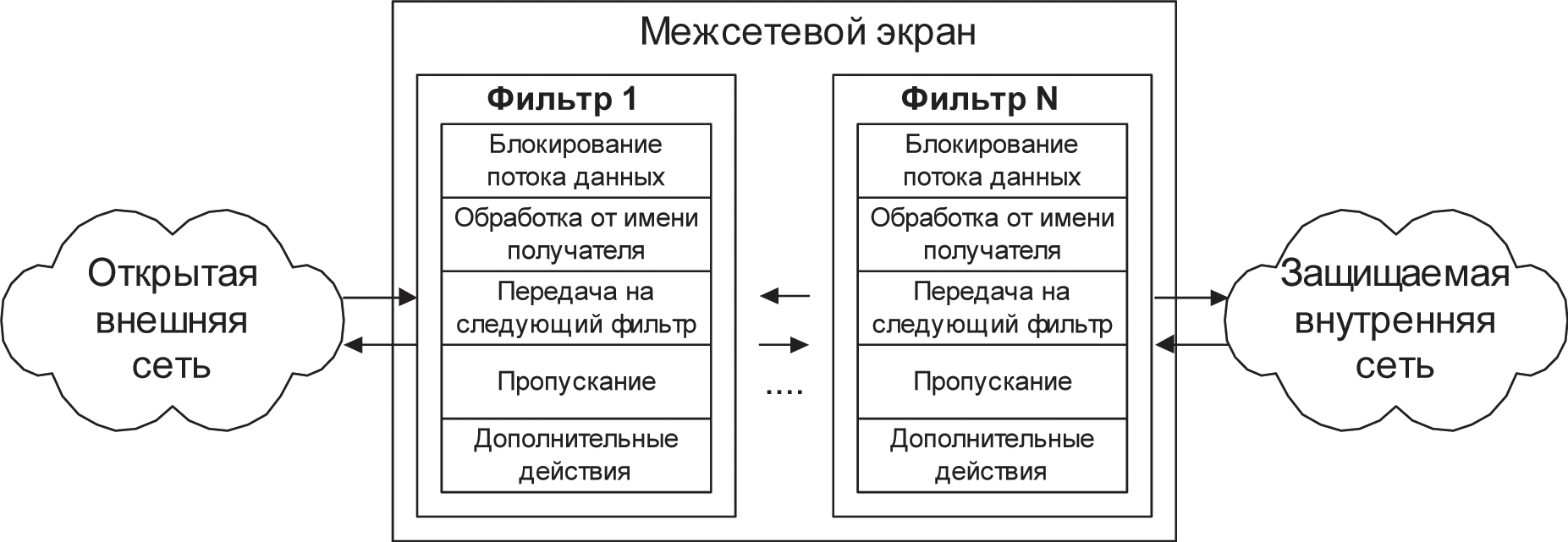
* + - аппаратно-программный;
    - программный.

*По схеме подключения*:

* + - схема единой защиты сети;
    - схема с защищаемым закрытым и незащищаемым открытым сегментами сети;
    - схема с раздельной защитой закрытого и открытого сегментов сети.

# 1. Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований [4, 22]. Фильтрация осуществляется на основе набора предварительно загруженных в межсетевой экран правил, соответствующих принятой политике безопасности. Поэтому межсетевой экран удобно представлять как последовательность фильтров, обрабатывающих информационный поток (рис. 10.2).



***Рис. .2. Структура межсетевого экрана***

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих действий:

Анализ информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена.

Принятие на основе интерпретируемых правил одного из следующих решений:

* + - не пропустить данные;
    - обработать данные от имени получателя и возвратить результат отправителю;
    - передать данные на следующий фильтр для продолжения анализа;
    - пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрацию событий и др. Соответственно, правила фильтрации определяют перечень условий, по которым осуществляется:

* + - разрешение или запрещение дальнейшей передачи данных;
    - выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

* + - служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
    - непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
    - внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т. д.

Используемые критерии анализа зависят от уровней модели ОSI, на которых осуществляется фильтрация. В общем случае чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

# 2. Выполнение функций посредничества.

Функции посредничества МЭ выполняет с помощью специальных программ, называемых *программами-посредниками* или *экранирующими агентами*. Данные программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетями.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере МЭ. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

Следует иметь в виду, что МЭ может выполнять функции фильтрации без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетями. Вместе с тем программные посредники могут и не осуществлять фильтрацию потока сообщений.

В общем случае программы-посредники, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:

* + - проверку подлинности передаваемых данных;
    - фильтрацию и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
    - разграничение доступа к ресурсам внутренней сети;
    - разграничение доступа к ресурсам внешней сети;
    - кэширование данных, запрашиваемых из внешней сети;
    - идентификацию и аутентификацию пользователей;
    - трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
    - регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов [4, 22].

Программы-посредники могут осуществлять *проверку подлинности получаемых и передаваемых данных*. Это актуально для аутентификации не только электронных сообщений, но и мигрирующих программ (Javа, АсtivеХ Соntrols), по отношению к которым может быть выполнен подлог. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей.

Программы-посредники могут выполнять *разграничение доступа к ресурсам внутренней или внешней сети*, используя результаты идентификации и аутентификации пользователей при их обращении к межсетевому экрану.

Способы *разграничения доступа к ресурсам внутренней сети* практически не отличаются от способов разграничения, поддерживаемых на уровне операционной системы.

При *разграничении доступа к ресурсам внешней сети* чаще всего используется один из следующих подходов:

* + - разрешение доступа только по заданным адресам во внешней сети;
    - фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;
    - накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти МЭ и полный запрет доступа во внешнюю сеть.

С помощью специальных посредников поддерживается также *кэширование данных*, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска МЭ, называемого в этом случае прокси-сервером. Поэтому если при очередном запросе нужная информация окажется на прокси-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого прокси-сервера.

Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на прокси-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам прокси-сервера, а непосредственный доступ к ресурсам внешней сети запрещается.

*Фильтрация и преобразование потока сообщений* выполняются посредником на основе заданного набора правил. Здесь следует различать два вида программ-посредников:

* + - экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например, FТР, НТТР, Теlnet;
    - универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных, и если какой-либо объект не соответствует заданным критериям, то посредник либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например обезвреживание обнаруженных компьютерных вирусов. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы.

МЭ с посредниками позволяют также организовывать защищенные виртуальные сети VРN, например, безопасно объединить несколько локальных сетей, подключенных к Интернету, в одну виртуальную сеть.

Помимо выполнения фильтрации трафика и функций посредничества, современные межсетевые экраны позволяют реализовать ряд

других, не менее важных функций, без которых обеспечение защиты периметра внутренней сети было бы неполным. Рассмотрим дополнительные возможности современных межсетевых экранов.

# 3. Дополнительные возможности МЭ

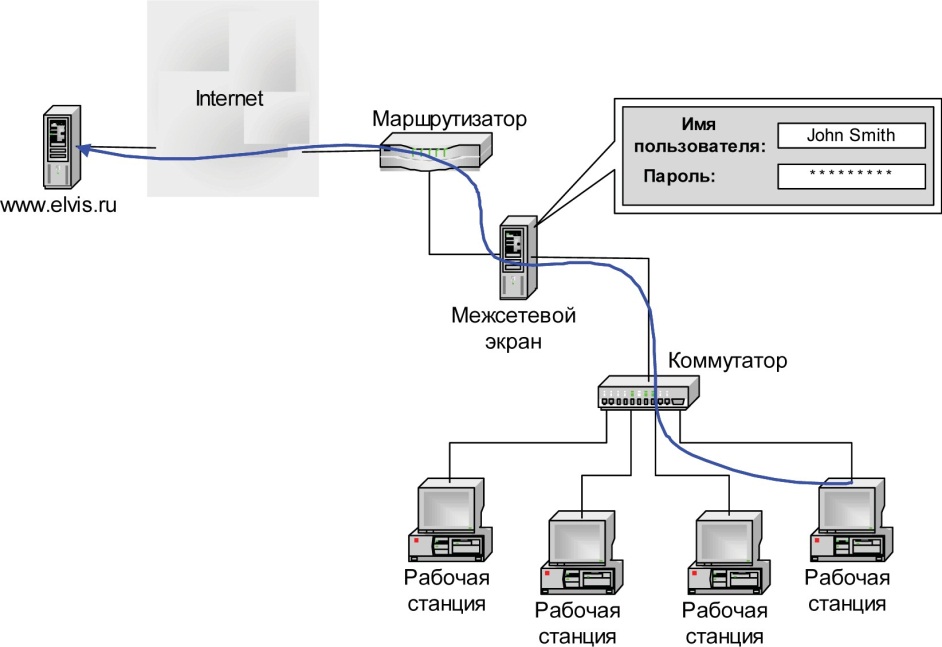
Рассмотрим реализацию межсетевыми экранами таких функций, как идентификация и аутентификация пользователей, трансляция внутренних сетевых адресов для исходящих пакетов сообщений, регистрация событий, реагирование на задаваемые события, анализ зарегистрированной информации и генерация отчетов.

**Идентификация и аутентификация пользователей.** Кроме разрешения или запрещения допуска различных приложений в сеть, межсетевые экраны могут также выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам, разделяемым межсетевым экраном.

Прежде чем пользователю будет предоставлено право применять какой-либо сервис, необходимо убедиться, что пользователь – действительно тот, за кого себя выдает. Идентификация и аутентификация пользователей являются важными компонентами концепции межсетевых экранов. Авторизация пользователя обычно рассматривается в контексте аутентификации – как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы.

Идентификация и аутентификация пользователя иногда осуществляются при предъявлении обычного идентификатора (имени) и пароля. Однако эта схема уязвима с точки зрения безопасности – пароль может быть перехвачен и использован другим лицом. Многие инциденты в сети Интернет произошли отчасти из-за уязвимости традиционных многоразовых паролей. Злоумышленники могут наблюдать за каналами в сети Интернет и перехватывать передающиеся в них открытым текстом пароли, поэтому такая схема аутентификации считается неэффективной. Пароль следует передавать через общедоступные коммуникации в зашифрованном виде (рис. 3). Это позволяет предотвратить получение несанкционированного доступа путем перехвата сетевых пакетов.

Более надежным методом аутентификации является использование одноразовых паролей. Широкое распространение получила технология аутентификации на основе одноразовых паролей SecurID, разработанная компанией Security Dynamics и реализованная в коммуникационных серверах ряда компаний, в частности в серверах компании Cisco Systems и др.

***Рис. 3. Схема аутентификации пользователя по предъявляемому паролю***

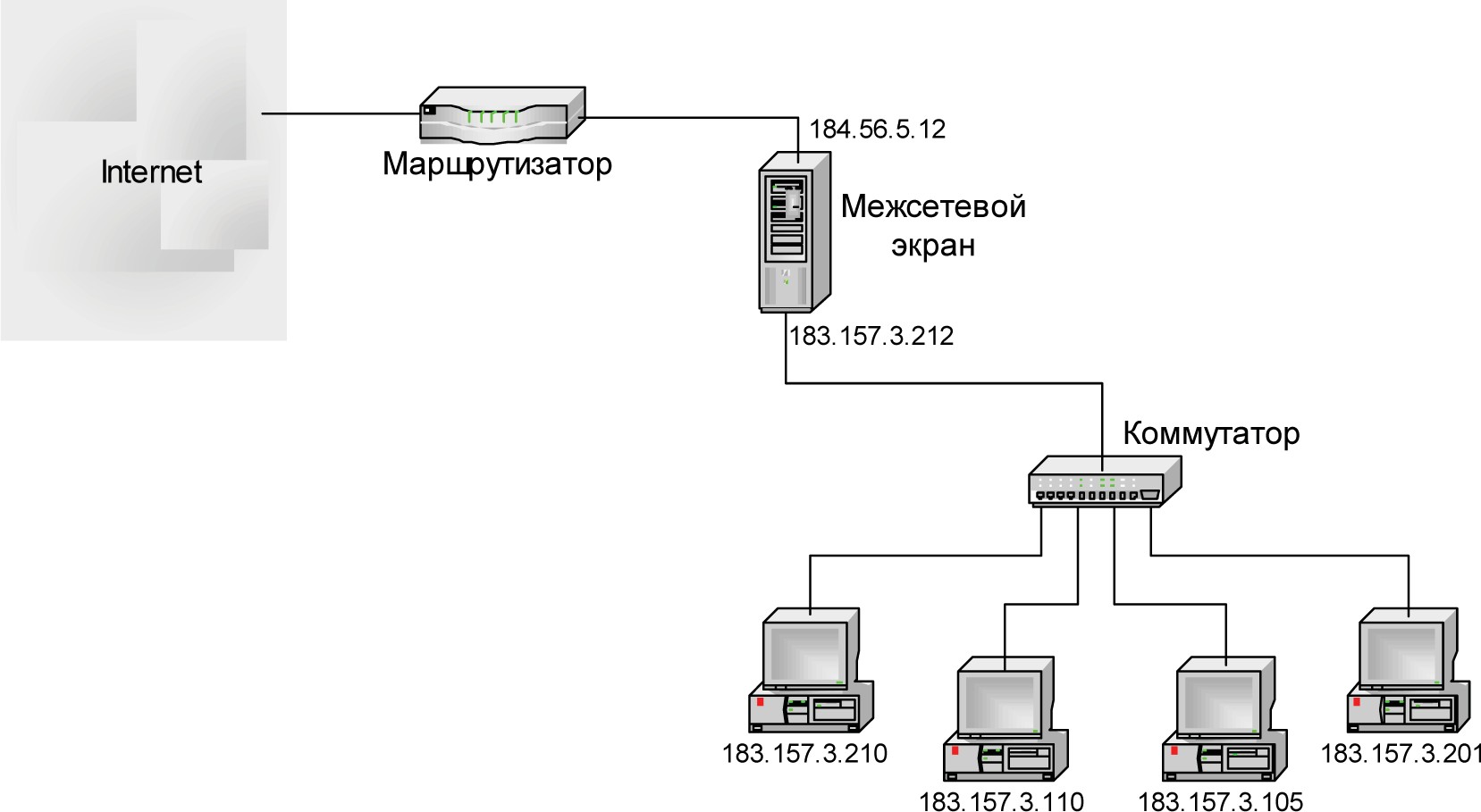
Удобно и надежно также применение цифровых сертификатов, выдаваемых доверенными органами, например центром распределения ключей. Большинство программ-посредников разрабатывается таким образом, чтобы пользователь аутентифицировался только в начале сеанса работы с межсетевым экраном. После этого от него не требуется дополнительная аутентификация в течение времени, определяемого администратором.

Так как межсетевые экраны могут централизовать управление доступом в сети, они являются подходящим местом для установки программ или устройств усиленной аутентификации. Хотя средства усиленной аутентификации могут использоваться на каждом хосте, более практично их размещение на межсетевом экране. При отсутствии межсетевого экрана, использующего меры усиленной аутентификации, неаутентифицированный трафик таких приложений, как TELNET или FTP, может напрямую проходить к внутренним системам в сети.

Ряд межсетевых экранов поддерживают Kerberos – один из распространенных методов аутентификации. Как правило, большинство коммерческих межсетевых экранов поддерживает несколько

различных схем аутентификации, позволяя администратору сетевой безопасности сделать выбор наиболее приемлемой схемы для своих условий.

**Трансляция сетевых адресов.** Для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, межсетевые экраны выполняют очень важную функцию – трансляцию внутренних сетевых адресов (Network Address Translation) – рис. 4.

***Рис. 4. Трансляция сетевых адресов***

Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов выполняется автоматическое преобразование IР-адресов компьютеров отправителей в один «надежный» IР-адрес.

Трансляция внутренних сетевых адресов может осуществляться двумя способами: динамически и статически. В первом случае адрес выделяется узлу в момент обращения к МЭ. После завершения соединения адрес освобождается и может быть использован любым другим узлом корпоративной сети. Во втором случае адрес узла всегда привязывается к одному адресу МЭ, из которого передаются все исходящие пакеты. IР-адрес МЭ становится единственным активным IР-адресом, который попадает во внешнюю сеть. В результате все исходящие из внутренней сети пакеты оказываются отправленными МЭ, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности, трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например в сети Интернет. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

**Администрирование, регистрация событий и генерация отчетов.** Простота и удобство администрирования являются одним из ключевых аспектов в создании эффективной и надежной системы защиты. Ошибки при определении правил доступа могут образовать дыру, через которую может быть взломана система. Поэтому в большинстве межсетевых экранов реализованы сервисные утилиты, облегчающие ввод, удаление, просмотр набора правил. Наличие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе или редактировании правил. Как правило, эти утилиты позволяют просматривать информацию, сгруппированную по каким-либо критериям, – например, все, что относится к конкретному пользователю или сервису.

Важными функциями межсетевых экранов являются *регистрация событий*, *реагирование на задаваемые события*, а также *анализ зарегистрированной информации* и *составление отчетов*. Являясь критическим элементом системы защиты корпоративной сети, межсетевой экран имеет возможность регистрации всех действий, им фиксируемых. К таким действиям относятся не только пропуск или блокирование сетевых пакетов, но и изменение правил разграничения доступа администратором безопасности и другие действия. Подобная регистрация позволяет обращаться к создаваемым журналам по мере необходимости – в случае возникновения инцидента безопасности или сбора доказательств для предоставления их в судебные инстанции либо для внутреннего расследования.

При правильно настроенной системе фиксации сигналов о подозрительных событиях (alarm) межсетевой экран может дать детальную информацию о том, были ли межсетевой экран или сеть атакованы либо зондированы. Собирать статистику использования сети и доказательства ее зондирования важно по ряду причин. Прежде всего нужно знать наверняка, что межсетевой экран устойчив к зондированию и атакам, и определить, адекватны ли меры защиты межсетевого экрана. Кроме того, статистика использования сети важна в качестве исходных данных при проведении исследований и анализе

риска для формулирования требований к сетевому оборудованию и программам.

Многие МЭ содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей. Системы учета позволяют произвести анализ статистики и предоставляют администраторам подробные отчеты. За счет использования специальных протоколов МЭ могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, то есть выдача предупредительных сигналов. Любой МЭ, который не способен посылать предупредительные сигналы при обнаружении нападения, нельзя считать эффективным средством межсетевой защиты.

# Заключение.

Современные межсетевые экраны существенно отличаются от классических прототипов начала 1990-х годов. Если раньше МЭ был предназначен только для разграничения доступа между Интернетом и внутренней сетью, то сегодня появились новые области его применения:

* сегментация сети с различными требованиями по безопасности;
* защита центров обработки данных;
* защита серверов приложений и т. д.

Тенденции дальнейшего развития межсетевых экранов можно увидеть в некоторых продвинутых решениях современных МЭ.

Применение в межсетевых экранах технологии Deep Packet Inspection позволило проводить более глубокий анализ пропускаемого через МЭ трафика на предмет обнаружения различных нарушений и атак. Технология Deep Packet Inspection позволила вывести межсетевые экраны на качественно новый уровень и защитить приложения и сервисы, ранее считавшиеся незащищенными, например технологию IP-телефонии.

Параллельно с МЭ с функцией Deep Packet Inspection стали появляться межсетевые экраны приложений (Application Firewall) – узкоспециализированные решения, которые ориентировались на защиту отдельных приложений или сервисов на прикладном уровне эталонной модели OSI.

Современные межсетевые экраны могут выполнять не только разграничение доступа между Интернетом и внутренней сетью, но и осуществлять глубокий анализ содержимого трафика, подключая ряд дополнительных подсистем предотвращения атак IPS (Intrusion Prevention), антивирусной защиты, контроля содержимого и др. Существуют межсетевые экраны со встроенной системой построения межофисных VPN.

Неотъемлемыми свойствами современных корпоративных межсетевых экранов стали централизованное управление, инспекция разных сетевых и прикладных протоколов, поддержка NAT, интеграция с различными серверами аутентификации, фильтрация URL и т. д.

Изменилась платформа, на которой реализуется межсетевой экран. Если раньше это было преимущественно программное решение, то постепенно произошел сдвиг в сторону аппаратной фильтрации трафика, что позволяет реализовать более скоростную и надежную обработку информационных потоков.

Аппаратные межсетевые экраны могут быть выполнены как в программно-аппаратном варианте, так и в виде специальных модулей, интегрируемых в маршрутизаторы и коммутаторы.

Появляются межсетевые экраны, ориентированные на защиту широко распространяющихся приложений для электронной коммерции на базе веб-сервисов. В существующих продуктах обеспечивается поддержка IP-телефонии, видеоконференц-связи, систем Telepresence. Поэтому в ближайшие годы можно ожидать развития межсетевых экранов, поднявшихся с уровня сети на прикладной.

Важной тенденцией, влияющей на развитие межсетевых экранов, является их более тесная интеграция с другими решениями по информационной безопасности. Пользователи предпочитают иметь одно устройство, решающее весь комплекс задач по защите сети и при этом объединяющее в себе решения производителей-лидеров по каждому из направлений сетевой безопасности.

Если интегрировать в одном устройстве сразу несколько защитных решений, то можно получить многофункциональное защитное устройство UTM (Unified Threat Management), которое позволяет сократить издержки и при этом обеспечить высокий уровень защиты за счет тесной интеграции таких защитных технологий, как межсетевой экран, система предотвращения атак, VPN, антивирус, антиспам, защита от шпионского ПО, контроль URL и т.п.