СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Межсетевое экранирование

СПбГЭТУ «ЛЭТИ», 2021 г.

4. МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

4.1 Общие положения

Межсетевой экран (брандмауэр или firewall, МСЭ)- специализированный комплекс защиты, позволяющий разделить среду передачи на 2 и более части и реализовать набор правил, определяющих условия прохождения пакетов с данными из одной части в другую.

Первоначально термин МСЭ описывал аппаратное устройство, которое блокировало нежелательный трафик и пропуская полезный. Затем появились высоконадежные программные средства, которые относительно просто инсталлируются и эффективно используются.

Первые МСЭ появились в начале 90 гг. и представляли собой программные или программно-аппаратные устройства, осуществляющие IP-маршрутизации с установленными правилами фильтрации. Недостаток этих МСЭ заключался в том, что трудно было сформулировать приемлемые правила фильтрации и ограничивать сервисы прикладного уровня (Telnet, FTP, SMTP). В 1994 году компания Check Point ввела графический интерфейс конфигурирования и управления. В 1996 г. Вышел межсетевой экран для ОС Windows NT, с помощью которого администраторы могли сконфигурировать надежную защиту без знания UNIX.

К основным функциям межсетевого экрана можно отнести:

ограничение доступа внешних пользователей к серверам защищаемым межсетевым экраном;

разграничение доступа внутренних пользователей к внешним ресурсам;

фильтрация трафика;

сигнализация и аудит.

Современные МСЭ обеспечивают высокоуровневую поддержку политики безопасности организации по отношению ко всем протоколам семейства TCP/IP и характеризуются прозрачностью для пользователей, большим быстродействием и высокой эффективностью.

Основной тенденцией развития средств сетевой защиты является интеграция, в частности, межсетевых экранов с криптографическими и антивирусными средствами, а также средствами анализа уровня обеспечения безопасности.

4.2 Классификация межсетевых экранов

По функционированию на уровнях модели OSI (рис 4.1):

- пакетный фильтр (экранирующий маршрутизатор-screening router);
- шлюз сеансового уровня (экранирующий транспорт);
- прикладной шлюз (application gateway);
- шлюз экспертного уровня (stateful inspection), инспектор состояний.

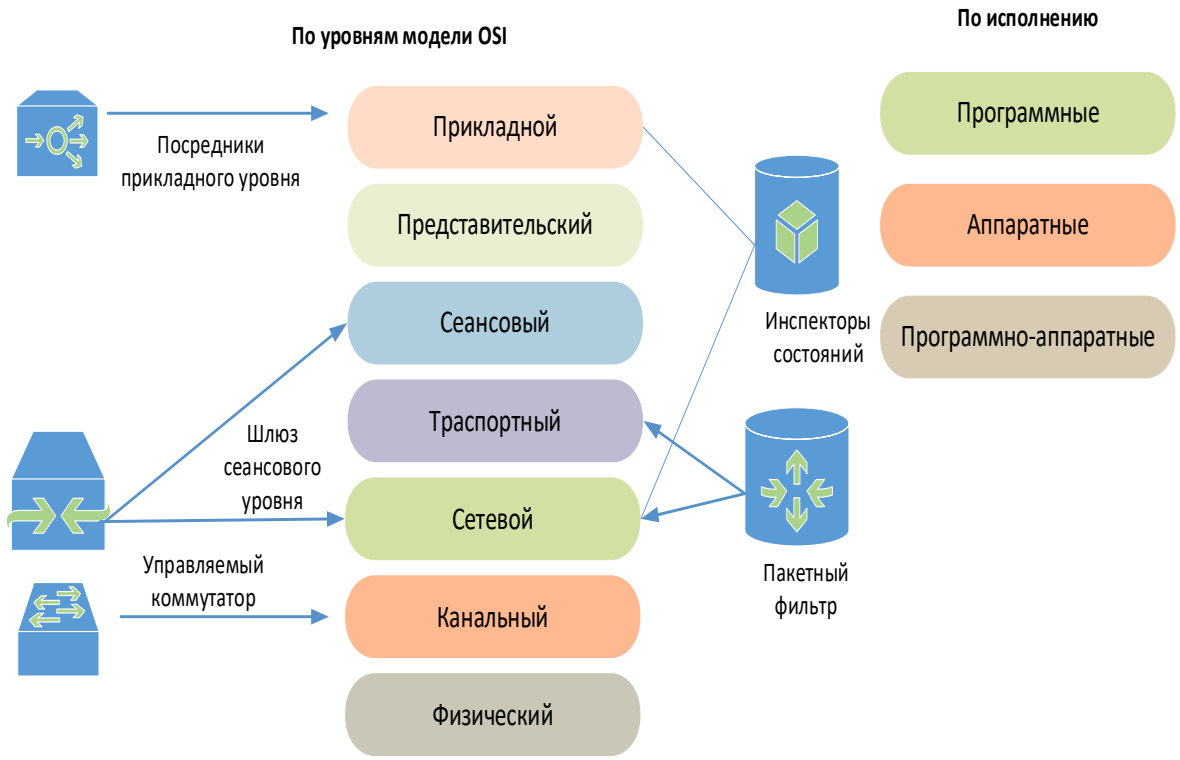


Рис. 4.1

По используемой технологии:

-контроль состояния протокола (stateful inspection-экспертный уровень);

- на основе модулей посредников (proxy);

По исполнению (рис 4.1):

- аппаратный (в виде специализированного устройства, достоинством данного исполнения является простота ввода в эксплуатацию, за счет наличия типовых шаблонов настройки, а к недостаткам можно отнести меньшую по сравнению с программными аналогами масштабируемость и трудность обеспечения взаимодействия с программными продуктами сторонних фирм);

- программно-аппаратный (в виде модуля к маршрутизатору или коммутатору, или специально выделенного сервера);

- программный (в виде программного приложения или усеченной ОС, недостатком программного исполнение, является потребления ресурсов, а также уязвимость самих ОС).

По схеме подключения:

- схема единой защиты сети;

- схема с защищаемым закрытым и не защищаемым открытым сегментами сети;

- схема с раздельной защитой закрытого и открытого сегментов сети.

По расположению в сети:

- традиционные межсетевые экраны используются для защиты корпоративных сетей;

- персональные межсетевые экраны контролирует весь входящий и исходящий трафик независимо от прочих системных защитных средств на персональном компьютере. При этом поддерживается доступность сетевых сервисов, уменьшается нагрузка, индуцированная внешней активностью.

4.3 Основные компоненты межсетевых экранов и особенности их функционирования

Компоненты межсетевого экрана зависят от уровня функционирования, согласно уровню эталонной модели. В современных МСЭ имеет место комбинирование технологий, реализованных в различные архитектуры МСЭ (рис 4.2).

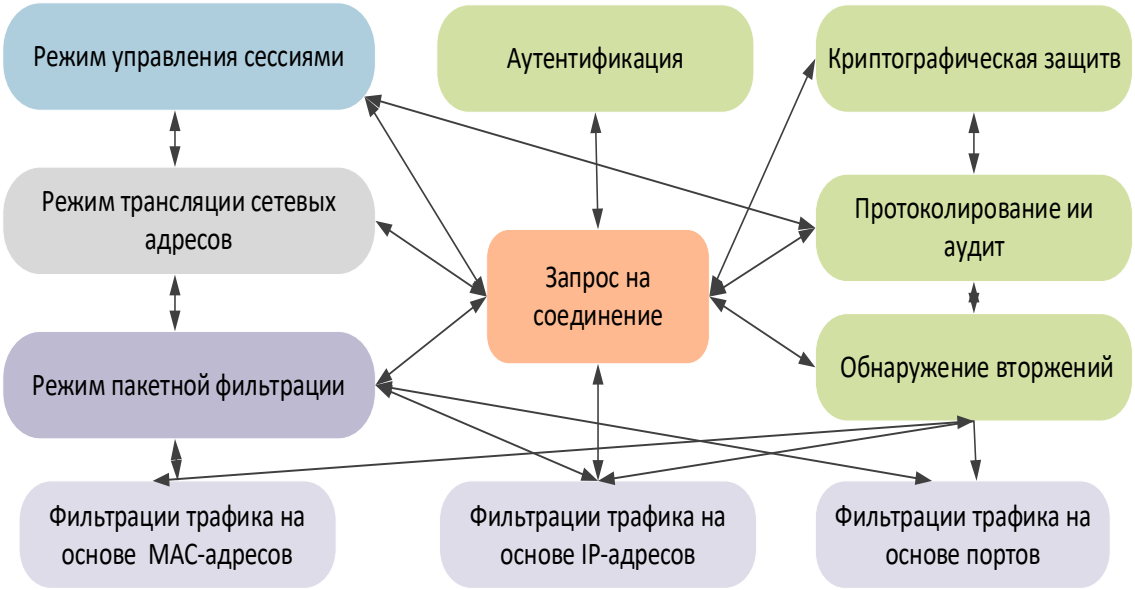


Рис. 4.2

4.4 Управляемые коммутаторы

Коммутаторы позволяют осуществлять фильтрацию пакетов, однако наряду со стандартными условиями фильтрации, многие коммутаторы позволяют создавать дополнительные барьеры и ограничивать доступ

пользователей к некоторым службам за счет использования запрета доступа некоторых MAC-адресов к ресурсам другого сегмента.

К функциям фильтрации трафика на уроне коммутатора можно отнести:

1. Возможность фильтрации трафика на основе MAC-адресов, содержащихся в заголовках пакетов или IP адресов, при использовании маршрутизации на L3 уровне.

2. Сегментацию сети на рабочие группы, используя технологию разделения сети на VLANы.

3. Аутентификацию конечных точек по протоколу 802.1x (в некоторых случаях с ограничением списка контроля доступа).

4. Протоколирование.

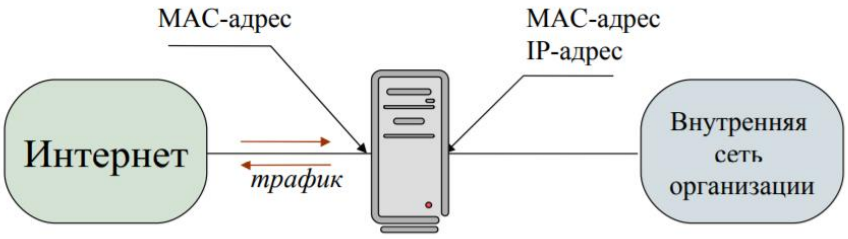


Рис. 4.3 [1]

К *недостаткам* данной технологии можно отнести, то, что аппаратно установленный в сетевой карте MAC-адрес легко меняется программным путем, поскольку значение, указанное через драйвер, имеет более высокий приоритет, чем указанное в сетевой плате.

4.5 Пакетные фильтры

Пакетный фильтр- маршрутизатор, обрабатывающий пакеты (сетей TCP/IP и IPX/SPX) на основании информации, содержащейся в заголовках пакетов, для этого:

- используется статическая фильтрация (заданная администратором для каждого уникального типа пакета, требующего обработки).
- для многоканальных соединений требуется учитывать дуплексность соединений.

Технология реализована в пограничных маршрутизаторах, операционных системах, персональные межсетевые экраны. МСЭ предназначен для фильтрации трафика, на основе набора предварительно загруженных в экран правил, соответствующих политике безопасности. Для описания правил прохождения пакетов составляются правила фильтрации с основными параметрами (рис. 4.4).

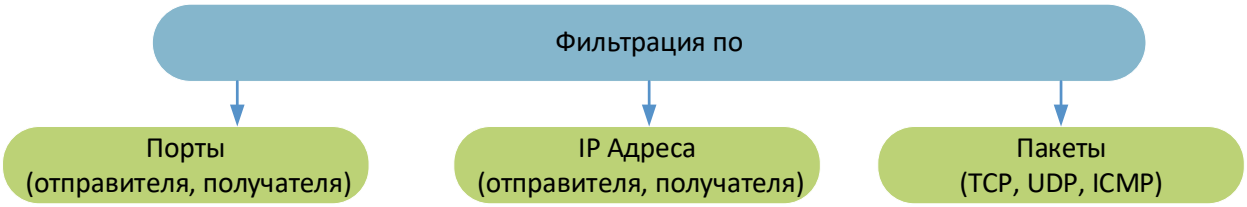


Рис. 4.4

При этом сетевой трафик может проходит не через один фильтр, а через ряд фильтров, следующих друг за другом. Для этого анализируются заголовки IP, TCP и UDP пакетов (адрес получателя, отправителя, порт и др.) и осуществляется поиск правилах фильтрации, с которым согласуются все проверяемые поля

Для функционирования правил фильтрации формируются списки доступа, которые могут быть:

- стандартными (позволяют проверять только IP адрес отправителя);
- расширенными (позволяют фильтровать пакеты на основе адресов, портов и протоколов получателя и отправителя);
- именованными.

При поступлении сетевого трафика проверка списка доступа (рис. 4.5):

- начинается сверху вниз;
- при совпадения, проверка списка прекращается и выполняется действие, указанное в инструкции (заблокировать или пропустить).

Последним идет неявная инструкция по блокировке всего трафика. На основании правила принимается решение:

- не пропустить пакет;
- обработать пакет от имени получателя и возвратить результат отправителю;
- передать данные на следующий фильтр, для продолжения анализа;
- пропустить данные, игнорируя следующие фильтры;
- использовать правило по умолчанию (отбрасывание пакетов).

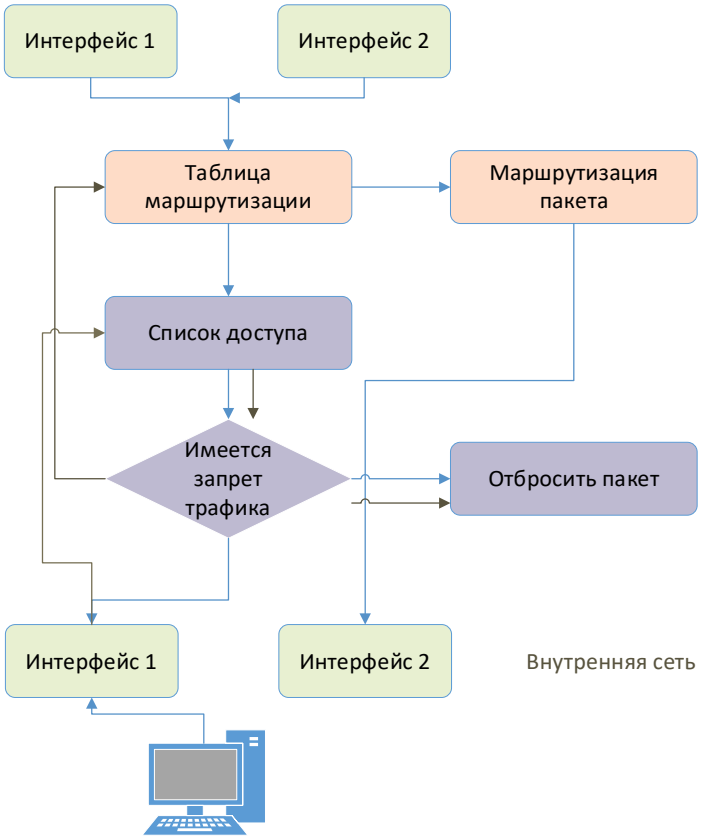


Рис. 4.5

Стандартные списки доступа. Инструкция для стандартного списку доступа задается следующей командой:

Router(config)# access-list номер permit | deny IP_адрес_отправителя инвертированная_маска (wildcard mask)

Номер списка принимает значения от 1 до 99. Цифры не означают приоритет или упорядоченность (рис 4.6). Алгоритм работы стандартного списка доступа представлен на рис. 4.7.

```
Router(config)# access-list 1 deny 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit 10.1.0.0  0.0.255.255
Router(config)# access-list 1 deny any
```

Рис. 4.6

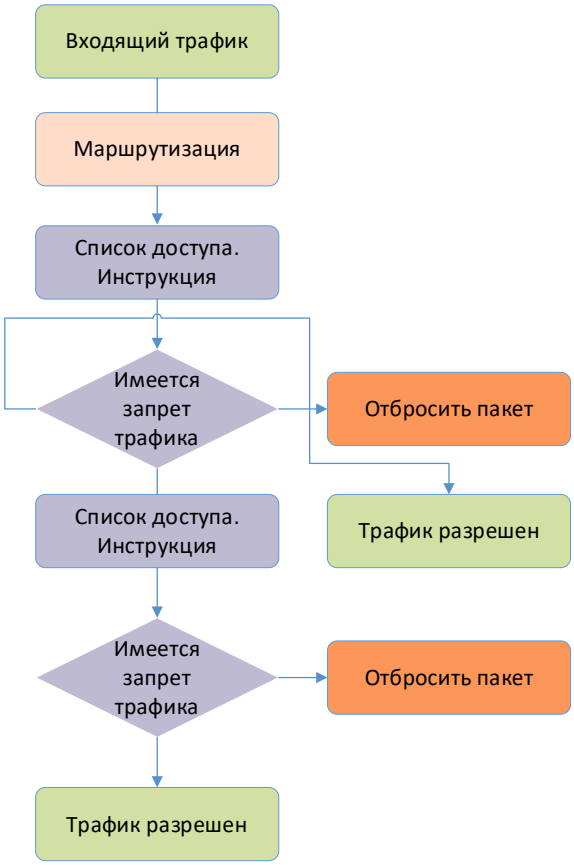


Рис. 4.7

Расширенные списки доступа имеют номера от 100 до 199. Общий пример команды (рис 4.8, рис. 4.9):

Router(config)#access-list номер permit | deny протокол IP_адрес_отправителя инвертированная_маска порт_отправителя IP_адрес_получателя инвертированная_маска порт_получателя

Router(config)#access-list 100 permit tcp 192.168.1.0 0.0.0.255 eq 80 10.1.1.0 0.0.0.255 eq 443

Рис. 4.8

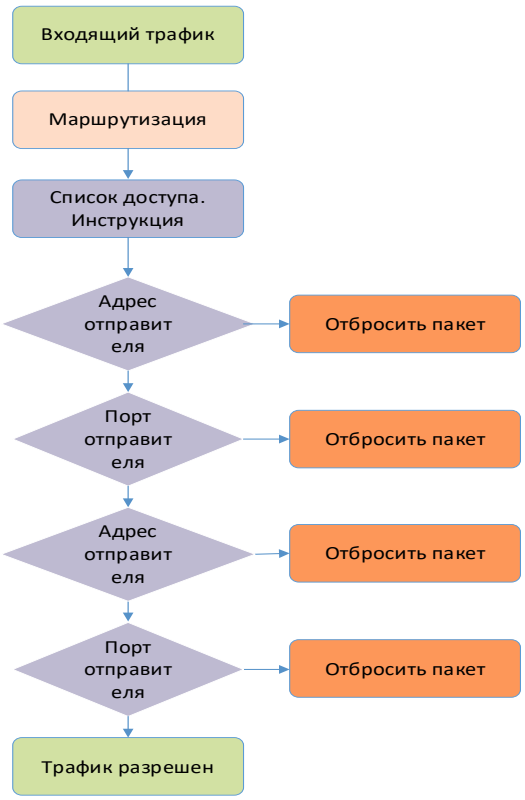


Рис. 4.9

Именованные списки доступа. В отличие от стандартных и расширенных списков можно редактировать. Именованный список позволяет использовать названия списков вместо их номеров. Синтаксис команд для стандартных списков:

Router(config)# ip access-list standard название

Router(config-std-nacl)# permit host IP_адрес_отправителя

Router(config-std-nacl)# deny IP_адрес_отправителя инвертированная_маска

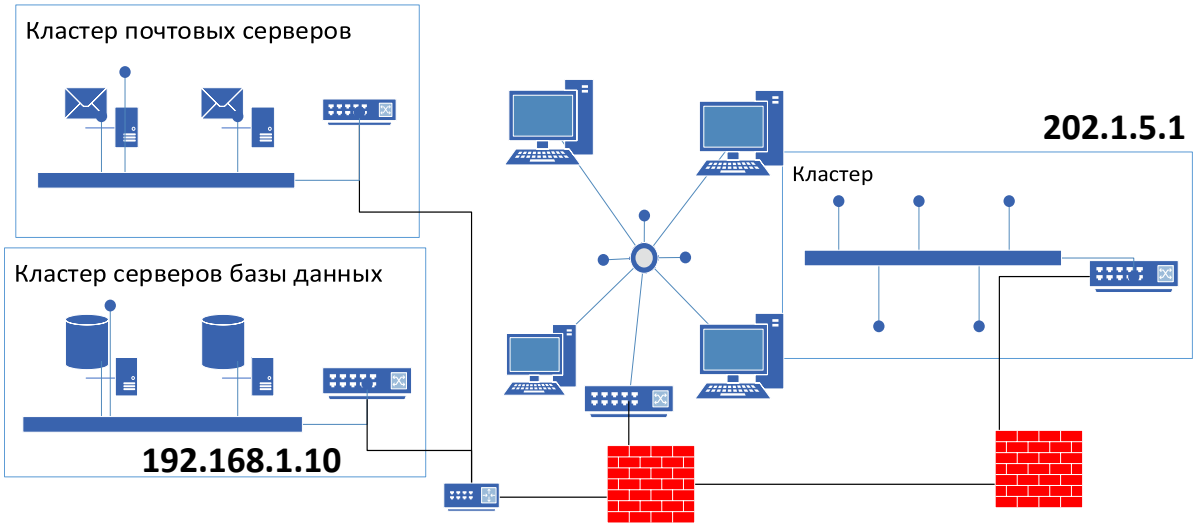
Для расширенных списков:

Router(config)# ip access-list extended название

Router(config-ext-nacl)# permit ip IP_адрес_отправителя инвертированная_маска IP_адрес_получателя инвертированная_маска

Router(config-ext-nacl)# deny tcp IP_адрес_отправителя инвертированная_маска порт_отправителя IP_адрес_получателя инвертированная_маска порт_получателя

В качестве примера рассмотрим доступ от хоста с адресом 192.168.1.10 к серверу 202.1.5.1 через маршрутизатор R, но не без доступа к другим частям сети. Для этого используются списки доступа, где в качестве имени указывается либо символьное имя либо номер. В первой строчке acl number 3001 указывается номер правила, это позволяет в случае необходимости вставить между ними еще дополнительные правила.



Пример списка доступа
acl number 3001
rule permit tcp source 192.168.1.0 0.0.0.255
destination 202.1.5.1 source-port any
destination port 80
Rule 20 deny ip source any destination

Рис. 4.10

Пакетные фильтры реализованы как аппаратно (может быть использован обычный маршрутизатор) так и в виде программного обеспечения установленного на сервере.

Достоинства: простота реализации, высокая производительность, прозрачность для программных приложений, малая цена.

Недостатки:

- проверяя только заголовки пакетов, пакетный фильтр не обеспечивает ряд важных функций (аутентификация, проверка подлинности, целостности и др.). Отсутствует возможность анализа пакетов прикладного уровня;
- отсутствует защита от подмены адреса;
- сложность настройки и администрирования;
- при увеличении числа правил возможно снижение производительности;
- требуется детальное знание сетевых услуг и протоколов;
- нет контроля состояния соединения;
- трудность функционирования в сетях с динамическим распределением адресов.

4.5 Шлюзы сеансового уровня. Технология NAT. Правила фильтрации сетевого контента и способы ограничения доступа к сетевой инфраструктуре

Шлюзы сеансового уровня, оперируют на сеансовом уровне иерархии OSI. К функциям шлюза сеансового уровня относят:

1. динамическую фильтрацию в сетевых фильтрах;
2. фильтрацию фрагментированных пакетов;
3. трансляция IP- адресов.

Рассмотрим процедуру фильтрации фрагментированных пакетов, с функцией защиты от Ddos атак, которая состоит из следующих этапов (рис 4.11):

1. МСЭ получает пакет SYN от компьютера А.
2. МСЭ передает полученный пакет на сервер В.
3. Сервер В передает пакет SYN/ACK на компьютер А, но МСЭ его перехватывает.
4. МСЭ пересылает полученный пакет на компьютер А, кроме того, МСЭ от имени компьютера А посылает пакет ACK на сервер В
5. Если же МСЭ не получит пакета ACK или кончится тайм-аут на установление соединения, то он вышлет в адрес сервера В пакет RST, отменяющий соединение.

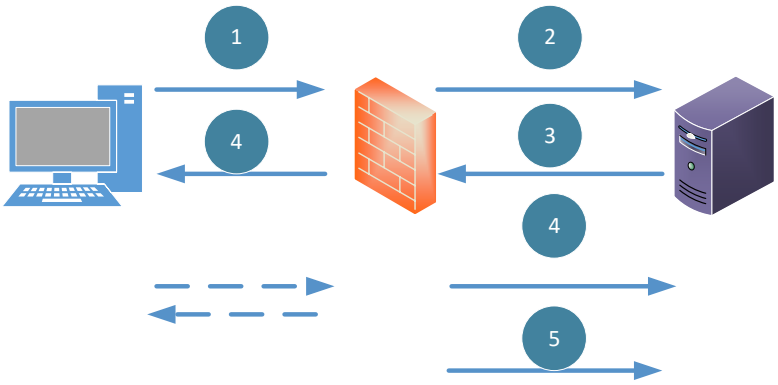


Рис. 4.11

Экранирующий транспорт осуществляет контроль виртуальных соединений и трансляцию IP-адресов при взаимодействии с внешней средой.

Для установки виртуального соединения принимая запрос от рабочей станции на связь с внешней сетью, шлюз (рис 4.12):

1. Проверяет, удовлетворяет ли он базовым критериям фильтрации.

2. Если условия фильтрации приемлемы, то шлюз от имени рабочей станции отправляет пакет, помеченный флагом SYN (запрос на соединение) и ISN (начальный порядковый номер) компьютеру внешней среды.
3. Компьютер- получатель откликается посылкой пакета с установленным флагом ASK, подтверждающем прием пакета, а также флагами SYN, ISN, обозначающих возможность передачи данных к шлюзу.
4. Шлюз в свою очередь подтверждает запрос на соединение отсылкой пакета с установленным флагом ASK и номером очередного пакета ISN.

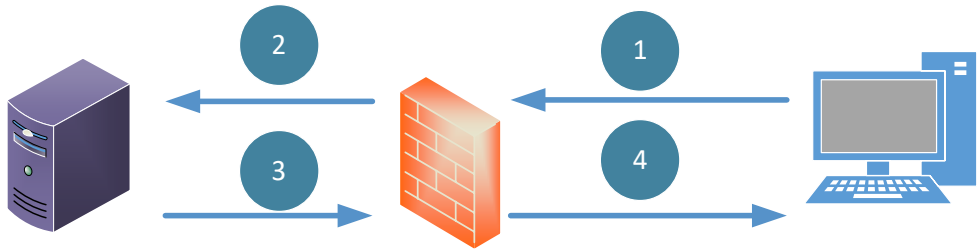


Рис. 4.12

5. Для передачи данных между рабочей станцией и компьютером внешней среды шлюз помещает в специальную таблицу данные о соединении (адрес получателя, отправителя, состояния соединения и т.д.), на основании которых шлюз передает пакеты из внешней среды рабочей станции (табл. 4.1).

Таблица 4.1

Внутренний IP	*Внутренний порт*	*Внешний IP*	*Внешний порт*
192.168.1.3	52001	184.86.48.128	49128
192.168.1.2	49238	184.86.48.128	49129

В случае закрытия сессии шлюз удаляет соответствующую строку из таблицы и разрывает цепь, использовавшуюся в данном соединении.

Шлюзы NAT могут работать в одном из **четырех режимов**:

- *Динамическом* (PAT)- шлюз имеет один-единственный внешний IP-адрес. Все обращения в сеть Internet со стороны клиентов внутренней сети осуществляются с использованием этого внешнего адреса, при этом шлюз оперирует лишь портами внешнего интерфейса, т.е. при обращении клиента шлюз выделяет ему уникальный программный порт транспортного протокола (UDP, TCP) для внешнего IP-адреса;

- *Статическом*- внешнему интерфейсу шлюза назначается столько зарегистрированных IP-адресов, сколько серверов имеется во внутренней сети, в соответствие уникальный внешний IP-адрес шлюза.
- *Статическом с динамической выборкой*, когда IP адреса резервируются динамически из пула внешних IP-адресов;
- Комбинированном-использование сразу нескольких вышеперечисленных режимов и предназначен для сетей, где имеются как клиенты, так и серверы Internet.

Преимущества:

- Позволяет преодолеть нехватку адресов IPv4 и осуществить сокрытие внутренней структуры сети.
- Применение технологии позволяет динамически задавать правила фильтрации трафика.
- Учет, ограничение и разграничение работы пользователей с ресурсами с помощью механизмов аутентификации, а также механизм трансляции внутренних адресов позволяют ограничить доступ к информации как внутренних, так и внешних пользователей.

Недостатки:

- Отсутствие единого стандарта NAT.
- Отсутствие возможности проверки содержания поля данных.
- Невозможность регулирования передачи информации на прикладном уровне.
- Использование ненадежной системы идентификации и аутентификации, основанную на IP-адресах отправителя/получателя.

4.6 Посредники прикладного уровня

Функционирует на прикладном и представительском уровнях эталонной модели OSI. К функция прикладного шлюза относят:

-установку виртуального соединения между рабочей станцией и внешней сетью;

-проверку подлинности передаваемых данных (контроль цифровых подписей);

-фильтрацию (по названию сервиса, допустимому временному диапазону, ограничению на содержимое сообщений);

-преобразование потока сообщений (например, прозрачное шифрование);

-разграничение доступа к внешней/внутренней средам (аутентификация и идентификация при обращении к межсетевому экрану, разрешение доступа только заданным адресам, блокировка поиска информации по нежелательным ключевым словам ит.д.);

-кэширование данных, запрашиваемых из внешней среды;

-администрирование, регистрация событий и генерация отчетов.

Прикладной шлюз осуществляет контроль виртуальных соединений, однако в отличие от шлюза сеансового уровня, для каждого прикладного протокола TCP/IP функционируют свои программы посредники (например, для протокола FTP- посредник FTP, который пропускает только ftp-пакеты).

Достоинства:

- Анализ на прикладном ровне и возможность реализации дополнительных механизмов защиты (например, анализ содержимого).
- Исключение прямого взаимодействия между двумя узлами.
- Высокий уровень защищенности.
- Контроль состояния соединения. Осуществляя фильтрацию пакетов на прикладном уровне, то есть производя проверку содержимого пакета, обеспечивают высокий уровень защиты внутренней среды.

Недостатки:

- высокая стоимость;
- большие затраты времени и ресурсов на анализ каждого пакета
- невозможность автоматического подключения поддержки новых сетевых приложений и протоколов, так как для каждого из них необходим свой агент.

4.7 Инспекторы состояния

Термин «инспектор состояния» был введен компанией Check Point.

Осуществляют фильтрацию пакетов с контролем состояния соединения, сочетая в себе элементы экранирующих маршрутизаторов и прикладных шлюзов. На сетевом и транспортном уровнях обеспечивают фильтрацию

пакетов по содержимому их заголовков, на прикладном уровне осуществляют фильтрацию пакетов в соответствии с заданной политикой безопасности. Инспекторы состояния оперируют на трех уровнях: прикладном, сеансовом и сетевом и позволяют контролировать:

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

При получении пакета данных содержимое этого пакета сравнивается с некими шаблонами, специфическими для соответствующего протокола прикладного уровня. Осуществляется выполнение следующих действий:

- пропуск пакета;
- удаление пакета и сессии;
- регистрация пакета и сессии и передача на механизмы фильтрации (рис 4.12).

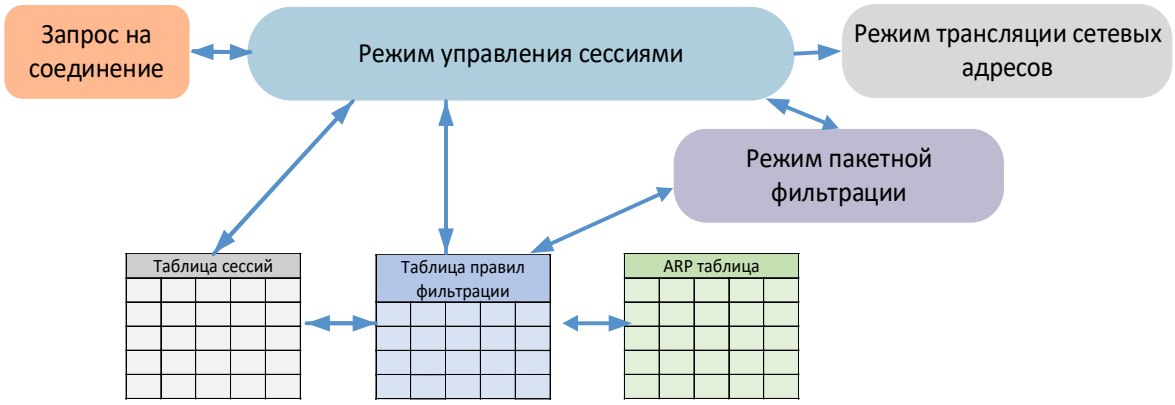


Рис. 4.12

Преимущества механизма управления сессиями:

- контроль хода TCP-соединения. Автоматическое открытие клиентских портов, необходимых для текущего соединения;
- контроль данных прикладных протоколов;
- блокировка атак, связанных с некорректной установкой флагов TCP;

Основные параметры сессии, хранящаяся в таблице сессий:

- интерфейсы, MAC-, IP-адреса и порты взаимодействующих сторон;
- номера родительской и дочерней сессий;
- текущее состояние сессии;
- протокол транспортного и прикладного уровней;

- информация о контексте прикладного протокола;
- номера TCP-последовательностей для последнего принятого пакета;
- имя пользователя, которому принадлежит данная сессия;
- время начала, время последней активности и значение таймаута неактивности сессии;
- количество пакетов и байт, прошедших от клиента к серверу и обратно;
- параметры подсчета интенсивности пакетов в сессии;
- номер порта трансляции при использовании режима NAT.

Механизм фильтрации пакетов позволяет осуществлять идентификацию основных пакетов прикладных протоколов независимо от порта сервиса. Например, для протокола HTTP:

- фильтрацию по адресам WEB-серверов;
- фильтрацию по именам (фрагментам) файлов;
- фильтрацию по методу запроса.

Для протокола SMTP фильтрацию по почтовым адресам отправителя и получателя. Для протокола FTP:

- фильтрацию по командам put, get;
- фильтрацию по именам (фрагментам) файлов;
- фильтрацию по имени/паролю пользователя;

В реализации инспектора состояний могут быть встроены дополнительные функции:

- трансляция сетевых адресов;
- аутентификация пользователей;
- регистрация событий.

Преимущества:

- Прозрачность для конечного пользователя, не требующая дополнительной настройки или изменения конфигурации клиентского программного обеспечения.
- Высокая скорость обработки информационных потоков.
- Не изменяют IP-адресов проходящих через них пакетов (любой протокол прикладного уровня, использующий IP-адреса, будет корректно работать с этими МЭ без каких-либо изменений или специального программами).

К недостаткам можно отнести прямое соединение между авторизованным клиентом и компьютером внешней сети.

4.8 Правила функционирования межсетевых экранов

Для правильного функционирования межсетевых экранов необходимо выполнения следующих этапов:

- разработка политики межсетевого взаимодействия;
- определение схемы подключения межсетевого экрана;
- настройка параметров функционирования.

Политика межсетевого взаимодействия определяет требования к безопасности информационного обмена с внешним миром и нормативно-правовыми документами [2-11] и отражает два аспекта:

- политику доступа к сетевым сервисам, где определяется определяет правила предоставления и использования всех возможных сервисов защищаемой компьютерной сети (сервисы, предоставляемые через сетевой экран, допустимые адреса IP клиентов, правила по которым пользователи могут воспользоваться сервисом, правила аутентификации пользователей и компьютеров, а также условия работы пользователей вне локальной сети организации);
- политику работы межсетевого экрана, отражающую принцип управления межсетевым взаимодействием, положенный в основу функционирования МСЭ.

Существует 2 принципа:

-запрещено все, что явно не разрешено–блокируются любые явно не разрешенные межсетевые взаимодействия. Данный подход позволяет реализовать принцип минимизации привилегий, и с точки зрения безопасности, является лучшим.

-разрешено все, что явно не запрещено. – блокируются только явно запрещенные межсетевые взаимодействия. При этом повышается удобство, но снижается безопасность межсетевого взаимодействия.

4.9 Определение схемы подключения межсетевого экрана

Демилитаризованная зона (DMZ - Demilitarized Zone) - сеть, которая добавляется между защищенной сетью и сетью, которая имеет меньший уровень безопасности, для создания дополнительного уровня безопасности.

В зависимости от условий функционирования, а также количества сетевых интерфейсов межсетевых экранов существуют различные схемы подключения к внешней сети:

- схема единой защиты локальной сети (Без выделения DMZ);

- схема с одной DMZ (с защищаемой закрытой и не защищаемой открытой подсетями);
- схема с Service-log DMZ (с раздельной защитой закрытой и открытой подсетей для одного МЭ с 3 сетевыми интерфейсами);
- схема с двумя DMZ (с раздельной защитой закрытой и открытой подсетей для двух МЭ с двумя сетевыми интерфейсами).

Межсетевые экраны с одним сетевым интерфейсом недостаточно эффективны как с точки зрения безопасности, так и с позиций удобства конфигурирования. Они физически не разграничивают внутреннюю и внешнюю сети, а соответственно не могут обеспечивать надежную защиту межсетевых взаимодействий. В связи с этим рационально рассмотреть схемы подключения межсетевых экранов с двумя и тремя сетевыми интерфейсами:

- единая защита локальной сети;
- с защищаемой закрытой и не защищаемой открытой подсетями;
- с раздельной защитой закрытой и открытой подсетей.

Наиболее простым решением является схема единой защиты локальной сети (рис.4.13), при котором локальная сеть целиком экранируется от потенциально враждебной внешней сети.

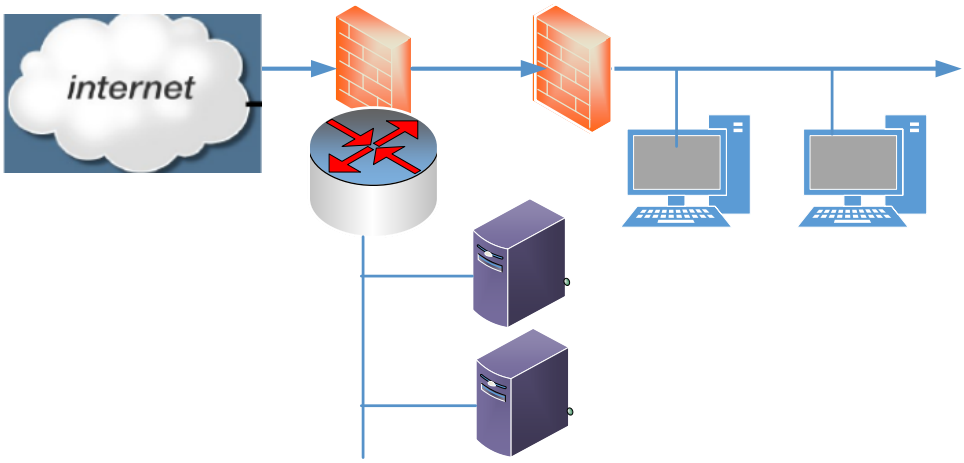


Рис. 4.13

Между пограничным маршрутизатором и брандмауэром имеется только один путь движения трафика. Маршрутизатор настраивается таким образом, что брандмауэр является единственной видимой снаружи машиной. Но объединение открытых серверов, доступных из внешней сети, вместе с другими ресурсами защищаемой локальной сети существенно снижает безопасность межсетевых взаимодействий, поэтому данное подключение

используется в случае отсутствия в локальной сети открытых серверов или возможности доступа к ним из внешней сети только ограниченного числа пользователей.

Схема с защищаемой закрытой и не защищаемой открытой подсетями используется при наличии в составе локальной сети общедоступных открытых серверов (рис. 4.14) и закрытой частью локальной сети. Данный способ обладает защищенностью закрытой части локальной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до межсетевого экрана.

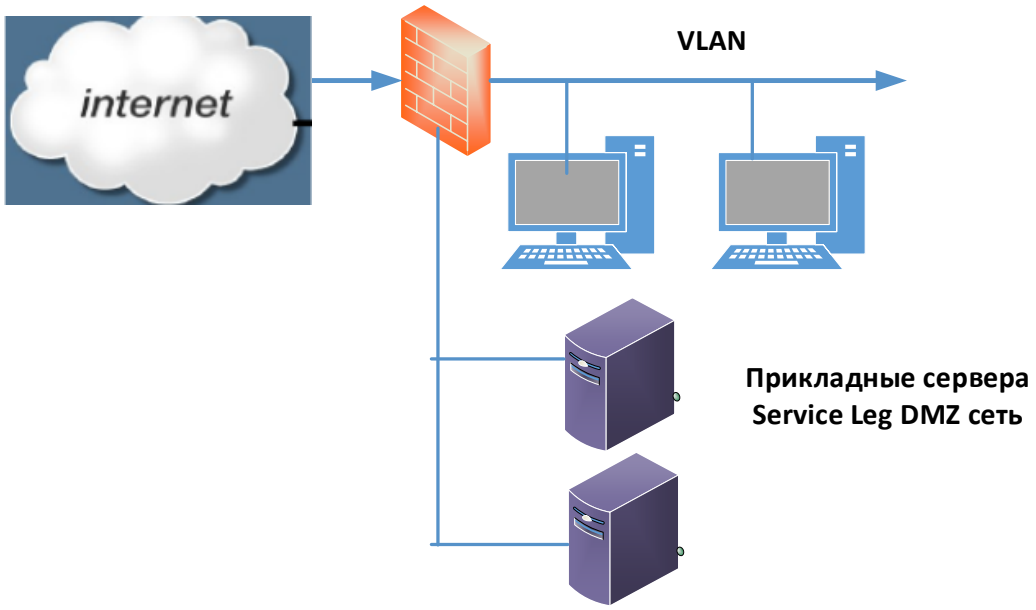


Рис. 4.14

Данную схему целесообразно использовать лишь при невысоких требованиях по безопасности к открытой подсети.

Использование схемы с раздельной защитой закрытой и открытой подсетей, повышает безопасность локальной сети. Такая схема строится на основе межсетевого экрана с тремя сетевыми интерфейсами (рис 4.15) или на основе двух межсетевых экранов с двумя и более сетевыми интерфейсами.

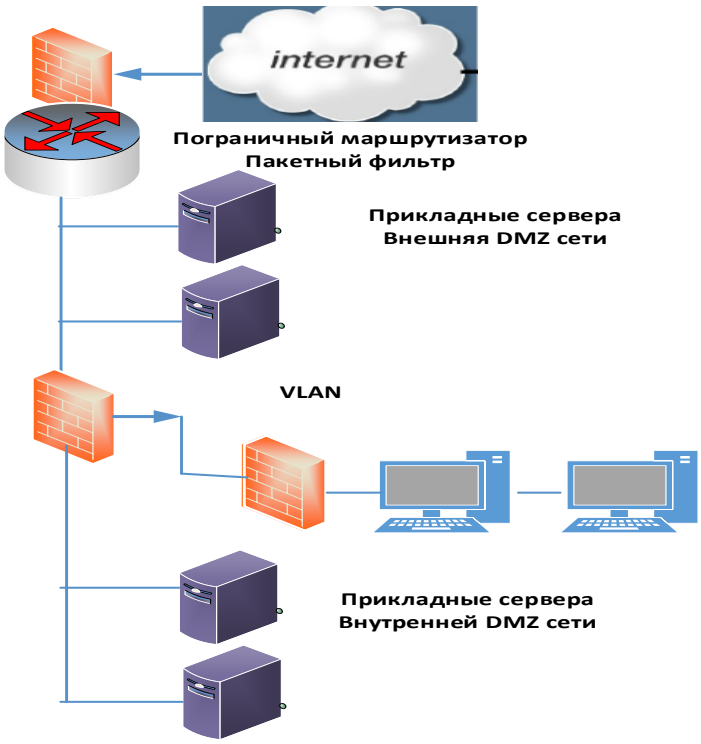


Рис. 4.15

Схема на основе двух межсетевых экранов с двумя и более сетевыми интерфейсами обеспечивает большую степень безопасности, так как защищаемая открытая подсеть выступает в качестве экранирующей подсети. Внутренняя локальная сеть конфигурируется таким образом, что прямой обмен информационными пакетами между внешней сетью и закрытой подсетью невозможен. Для осуществления атаки необходимо преодолеть, две независимые линии защиты, что является весьма сложной задачей.

4.10 Недостатки межсетевых экранов

К общим недостаткам межсетевых экранов можно отнести сложность администрирования. К наиболее частым атакам и уязвимостям, которым подвергаются межсетевые экраны целесообразно отнести:

1. Обход защиты межсетевого экранирования. Межсетевые экраны не могут защитить ресурсы внутренней сети в случае неконтролируемого использования в ней модемов. Доступ в сеть через модем по протоколам SLIP или PPP в обход межсетевого экрана делает сеть практически незащищенной. Поэтому необходимо контролировать все имеющиеся в сети точки удаленного доступа. Для этих целей возможно применение как организационных, так и технических мер.

Рис. 4.16

2. Использование злоумышленником или персоналом разрешенных портов. Правила предусматривают соответствующую проверку с целью определения того, разрешен или нет конкретный протокол (например, если открыты порты 25 и 80, то тем самым разрешается пропуск во внутреннюю сеть почтового (SMTP) и Web (HTTP) трафика). Вся несанкционированная деятельность осуществляется в рамках разрешенного протокола, создавая тем самым в нем туннель, по которому злоумышленник и реализует атаку. Самый простой пример, применения туннелей - Internet-черви и макровирусы, заносимые в корпоративную сеть в виде вложений.

3. Наиболее очевидный недостаток межсетевых экранов - невозможность защиты от авторизованных пользователей, выполняющих несанкционированные действия. Для устранения этого недостатка возможно использование систем обнаружения атак (intrusion detection systems). Данные средства, обнаруживают и блокируют несанкционированную деятельность в сети независимо от того, кто ее реализует - авторизованный пользователь (в т.ч. и администратор) или злоумышленник. Такие средства могут работать как самостоятельно, так и совместно с межсетевым экраном. Например, система RealSecure обладает возможностью автоматической реконфигурации межсетевого экрана CheckPoint Firewall-1 путем изменения правил, запрещая тем самым доступ к ресурсам корпоративной сети с атакуемого узла.

4. Отсутствие встроенных механизмов защиты от вирусов, апплетов и др.

5. Подмена IP адреса.

6. Подбор пароля.

7. Отсутствие защиты новых сетевых сервисов. Межсетевые экраны разграничивают доступ по широко распространенным протоколам, таким как HTTP, Telnet, SMTP, FTP и ряд других. При появлении нового протокола или сервиса встает вопрос о создании нового посредника.

Для эффективной защиты межсетевого взаимодействия необходимо использовать все возможные методы– пакетная фильтрация, технология посредничества, а также фильтрация экспертного уровня. Использование одной из перечисленных технологий по отдельности приводит к специфическим недостаткам межсетевых экранов:

пакетная фильтрация, основанная на анализе служебных полей IP, ICMP, UDP и TCP-пакетов уязвима из-за возможности подмены IP-адресов.

- Программы-посредники без использования пакетных фильтров подвержены атакам «отказ в обслуживании», а без фильтрации экспертного уровня характеризуются более высокими затратами компьютерных ресурсов.
- Фильтрация экспертного уровня, без использования программ-посредников не обеспечивает аутентификацию взаимодействующих сторон, трансляцию сетевых адресов и ряд других важных функций защиты, например криптографическое преобразование трафика и антивирусную защиту.

Поэтому межсетевые экраны, поддерживающие все ранее перечисленные методы защиты, обеспечивают наиболее высокую безопасность корпоративной сети при ее подключении к Internet.

4.11 Настройка параметров функционирования межсетевого экрана

Для построения защищенной компьютерной сети, с использование межсетевого экранирования, необходимо определить все требования, которые накладывает законодательство и внешнее окружение на функционирование межсетевого экрана [2-6]. Для этого целесообразно:

1.1 Определить топологию защищаемой сети и специфику защищаемых сервисов.

1.2 Оценить класс защиты. На практике подавляющему большинству государственных организаций достаточно межсетевого экрана 4-го и 5-го классов защиты с сертификатом ФСТЭК.

1.3 Определить типы технологий межсетевых экранов, которые наиболее эффективны в данном случае (с учетом производительности и интеграции межсетевого экрана в физическое окружение, стоимости). Наиболее подходящий для большинства государственных заведений — типы «А» и «Б», то есть межсетевые экраны, применяемые на физической и, соответственно, логической границе локальной сети. Межсетевые экраны типа «Б» могут иметь как программную, так и программно-аппаратную реализацию, в отличие от них тип тип «А» может быть только программно-аппаратным.

1.4 Выбрать тип оборудования и проверить наличие сертификатов согласно классу защищенности.

1.5. Создать политику межсетевого экрана, в которой определено, как следует обрабатывать входящий и исходящий трафик.

2.1 Выполнить анализ рисков и определить при каких условиях какому типу трафика разрешено проходить через межсетевой экран.

2.2 Сформировать правила фильтрации трафика и управления сессиями, где быть определено, как МСЭ обрабатывает входящий и исходящий трафик для конкретных IP-адресов, диапазонов адресов, протоколов, приложений и типов содержимого.

2.3 Осуществить проверку заданных правил на непротиворечивость.

2.4 Проанализировать производительность МСЭ на заданном наборе правил.

3. Осуществить испытания для оценки защищенности и на соответствие классу защищенности.

4. Управление архитектурой, политиками, ПО и другими компонентами межсетевого экрана осуществлять в случае:

4.1 Динамичного изменения организации межсетевого экранирования при изменении требований законодательства, в случае возникновении и фиксации атаки, а также организационно- административных условий в организации.

4.2 Нарушения балансировки компонент межсетевого экрана. В этой ситуации потенциальные проблемы с доступом к ресурсам должны быть своевременно устранены.

4.3 Изменении динамики мониторинга сетевого окружения и журналов событий вследствие угроз, как осуществленных, так и не осуществленных.

СПИСОК ЛИТЕРАТУРЫ

1. Межсетевой экран ССПТ-2. Электронный ресурс https://www.lektorium.tv/sites/lektorium.tv/files/additional_files/1331667948_13623_29_02_2012_firewall_sspt-2_funct_novopashenniy.pdf. По состоянию на 02.12.2021
2. Приказ ФСТЭК № 17 от 11 февраля 2013 года
3. Приказ ФСТЭК № 21 от 18 февраля 2013 года
4. Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утверждёнными Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119
5. Приказ ФСТЭК России от 9 февраля 2016 г. №9 Требования к межсетевым экранам
6. Информационное сообщение ФСТЭК «Об утверждении требований к межсетевым экранам» от 28 апреля 2016 г. N 240/24/1986
7. Лапонина О.Р. Л24 Основы сетевой безопасности. Часть 1. Межсетевые экраны: Учебное пособие / О.Р. Лапонина — М.: Национальный Открытый Университет «ИНТУИТ», 2014. — 378 с., ил., табл.— (Серия «Основы информационных технологий»).