ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Межсетевое экранирование

Межсетевые экраны

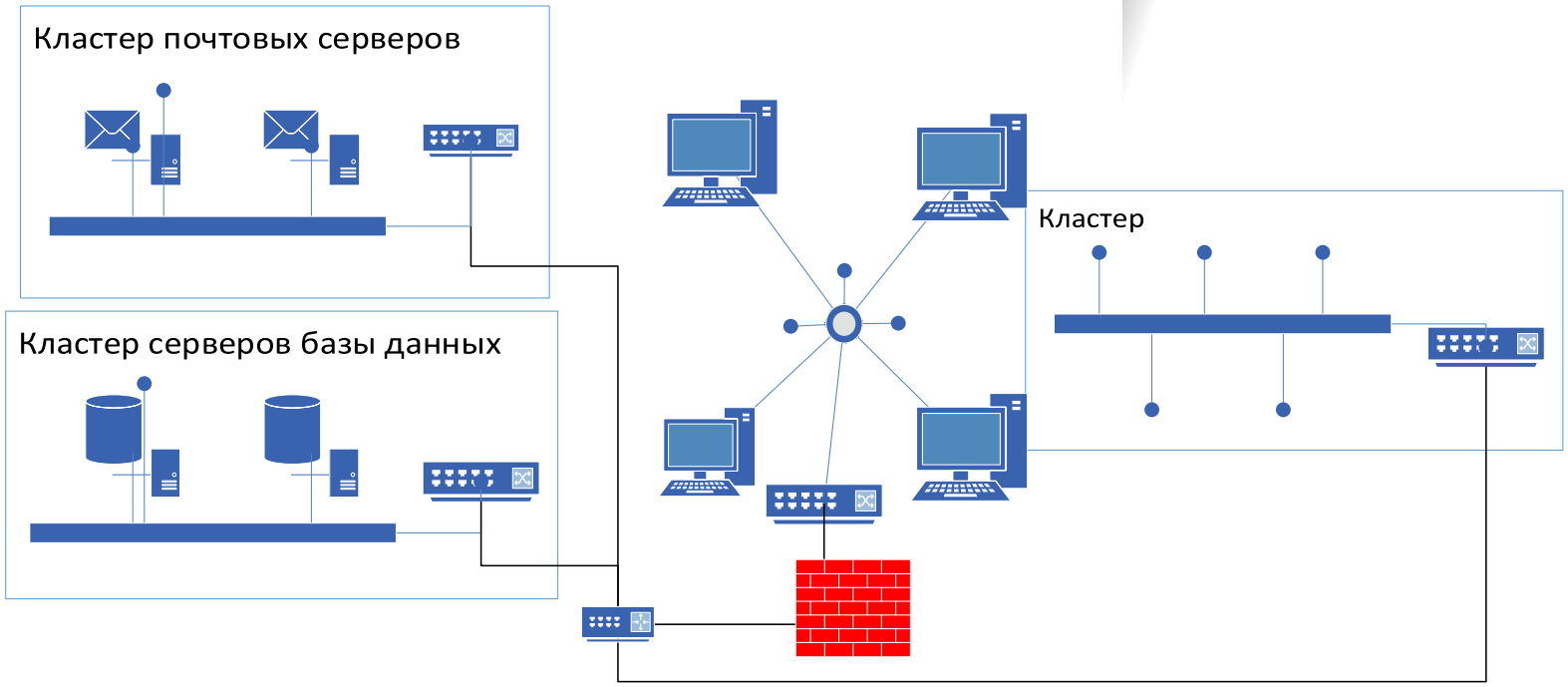
Согласно «Руководящему документу. Межсетевые экраны» Гостехкомиссии

«Межсетевым экраном называется локальное (однокомпонентное) или функционально-распределенное средство (комплекс), которое реализует контроль за информацией, поступающей в автоматизированную систему и/или выходящей из нее, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т. е. анализа по совокупности критериев и принятия решения об ее распространении в (из) автоматизированной системе».

Функции:

- Обеспечивают высокоуровневую поддержку политики безопасности организации по отношению ко всем протоколам семейства TCP/IP.
- Современные межсетевые экраны характеризуются прозрачностью для легальных 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.

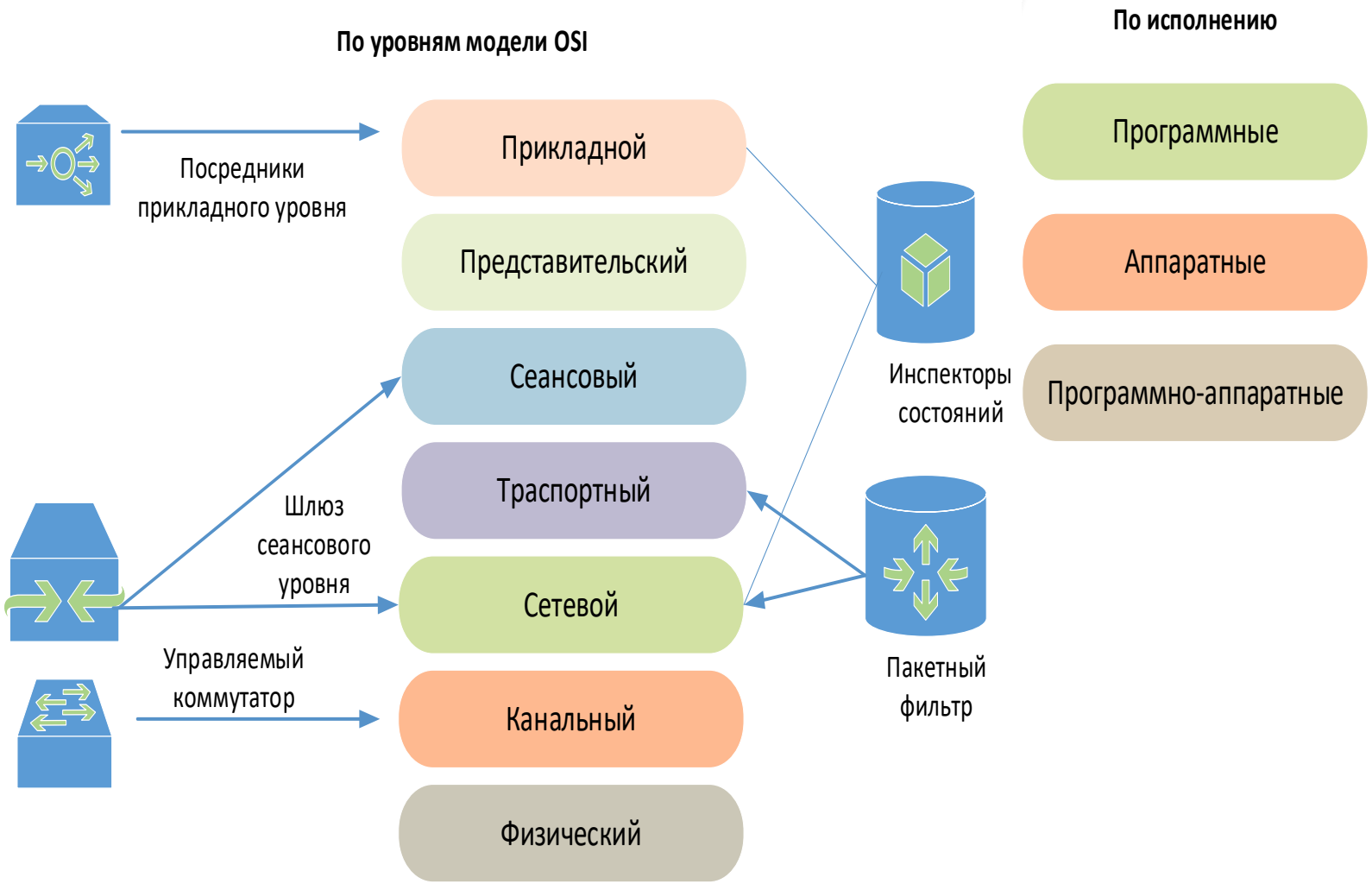
Межсетевые экраны



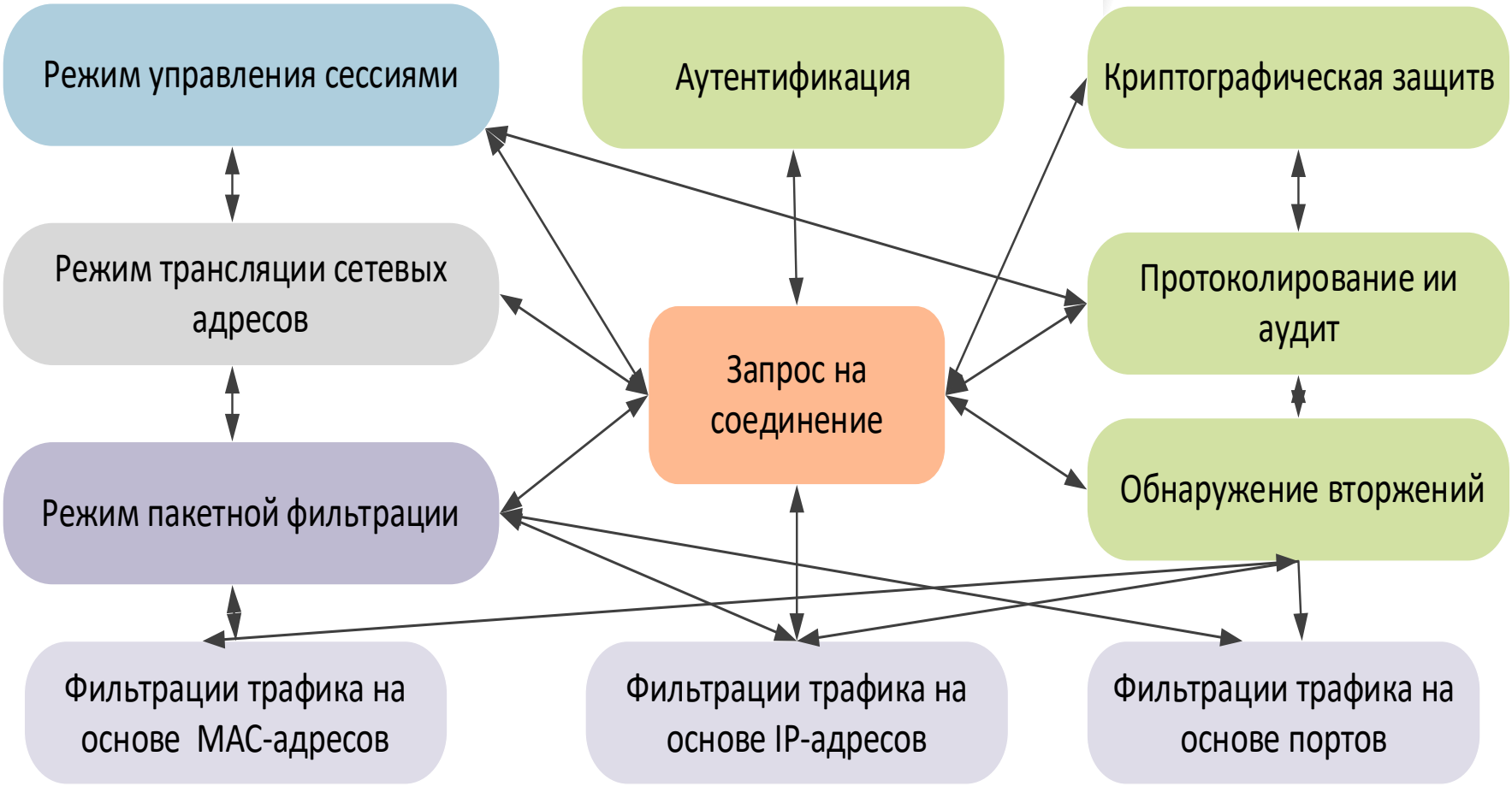
Задачи

1. Защита периметра сети
2. Объединение филиалов организации в виртуальную частную сеть (VPN)
3. Фильтрация трафика
4. Настройка маршрутизации
5. Сегментирование сети
6. Преобразования сетевых адресов
7. Балансировка нагрузки
8. Сбор и мониторинг информации
9. Локальное и удаленное управление

Классификация межсетевых экранов



Архитектура межсетевых экранов



Коммутаторы

Функции:

1. Возможность фильтрации трафика на основе:

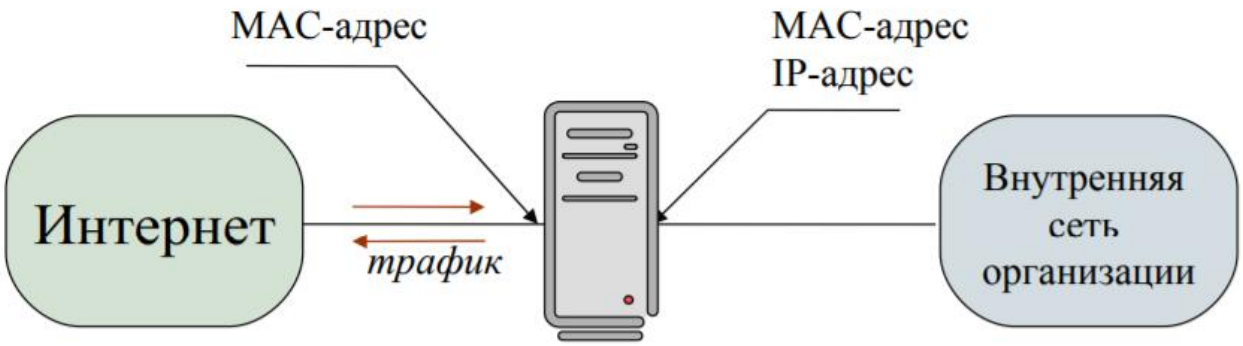
- MAC-адресов, содержащихся в заголовках пакетов.
- IP адресов (маршрутизация L3 уровня).

2. Сегментация сети на рабочие группы, используя сети VLAN.

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

4. Протоколирование.

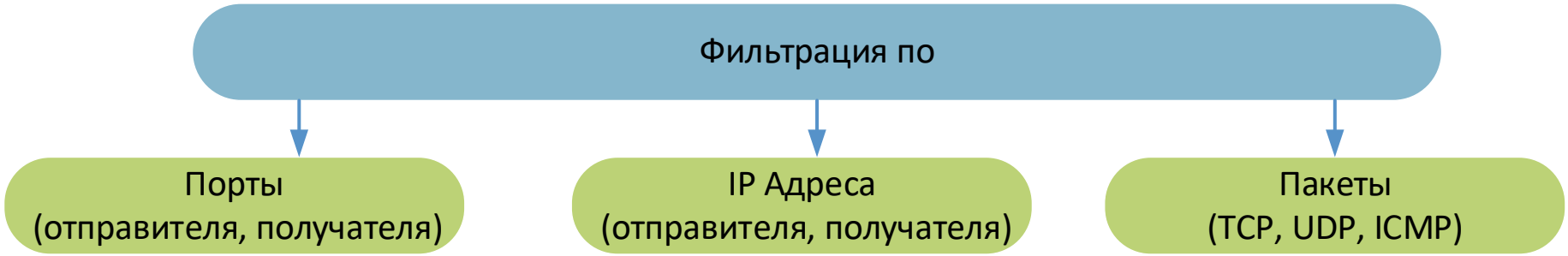
Недостаток: аппаратно установленный в сетевой карте MAC-адрес легко меняется программным путем, поскольку значение, указанное через драйвер, имеет более высокий приоритет, чем зашитое в плату.



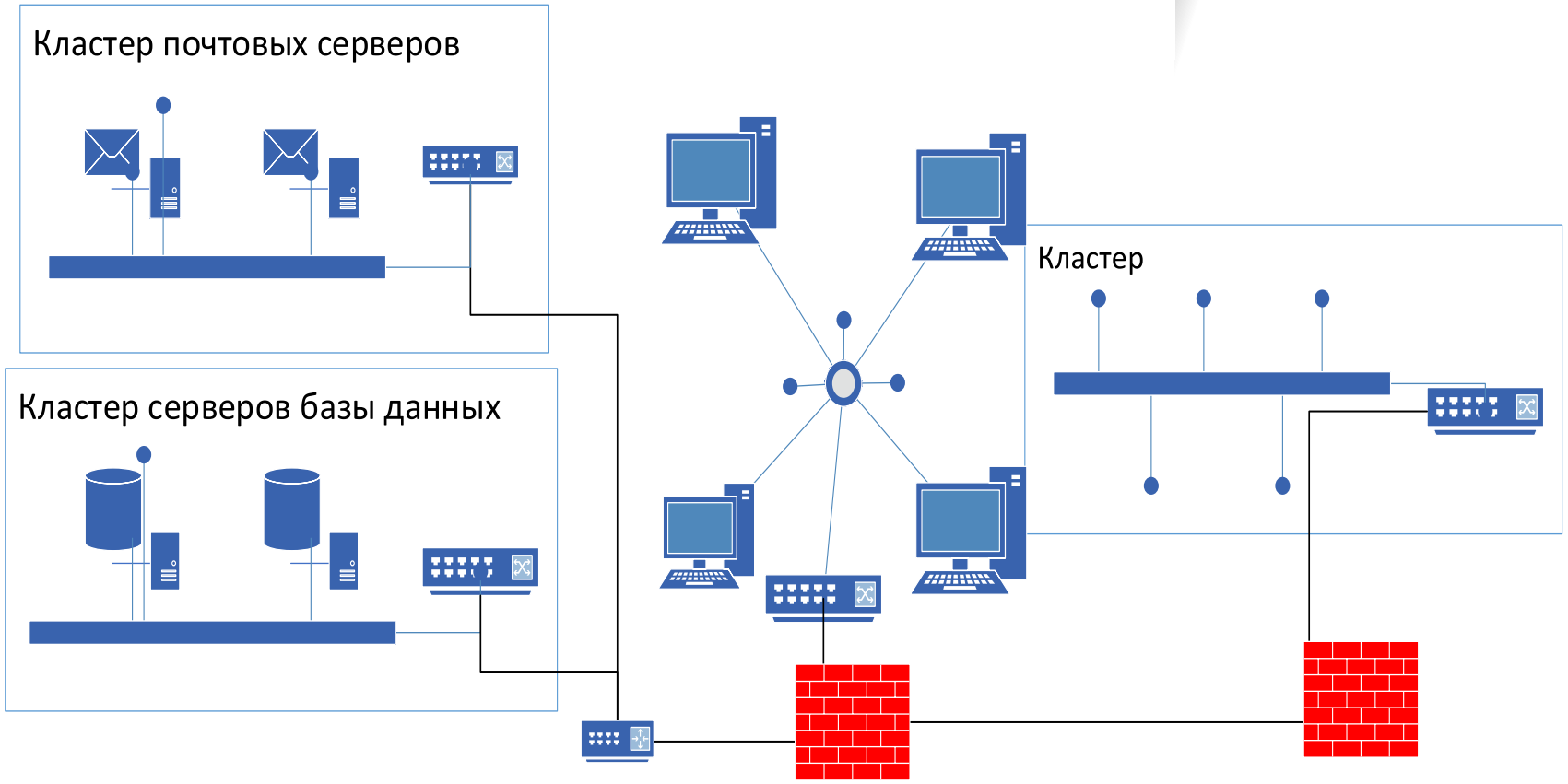
Пакетные фильтры (экранирующий маршрутизатор)

Маршрутизатор, обрабатывающий пакеты (сетей TCP/IP и IPX/SPX) на основании информации, содержащейся в заголовках пакетов:

- Используется статическая фильтрация (заданная администратором для каждого уникального типа пакета, требующего обработки).
- для многоканальных соединений требуется учитывать дуплексность соединений.
- Реализованы в в пограничных маршрутизаторах, операционных системах, персональные межсетевые экраны.



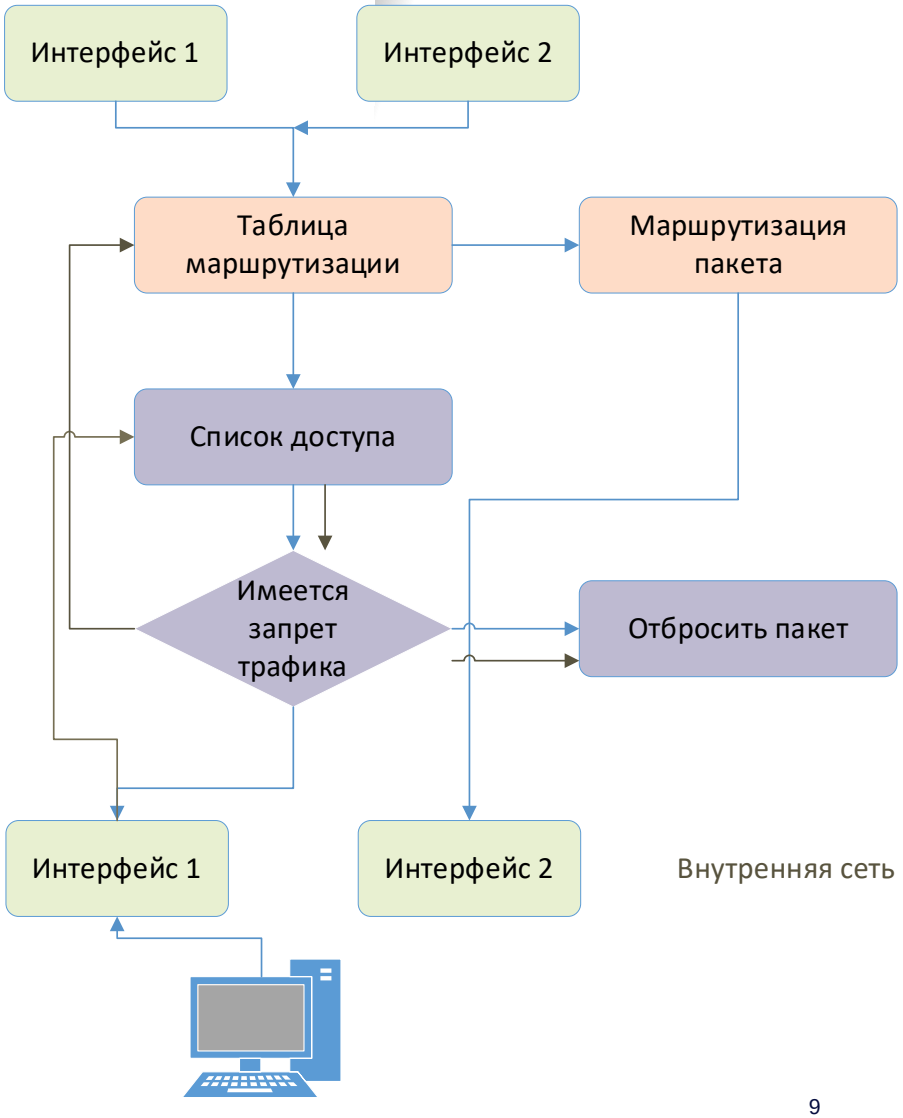
Пакетные фильтры (экранирующий маршрутизатор)



IP-адрес отправителя	Порт отправителя	IP-адрес получателя	Порт получателя	Протокол (TCP, UDP, ICMP)	**Флаги**	**Данные**

Списки доступа

- При поступлении трафика проверка списка доступа:
- 1. Начинается сверху вниз;
- 2. При нахождении совпадения проверка списка прекращается и выполняется действие, указанное в инструкции (заблокировать или пропустить).
- 3. Последним идет неявная инструкция по блокировке всего трафика.
-
- **Виды ACL**
- стандартные списки (позволяют проверять только IP адрес отправителя);
- расширенные списки (позволяют фильтровать пакеты на основе адресов, портов и протоколов получателя и отправителя);
- именованные списки.



Стандартные списки доступа

Инструкция задается следующей командой:

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

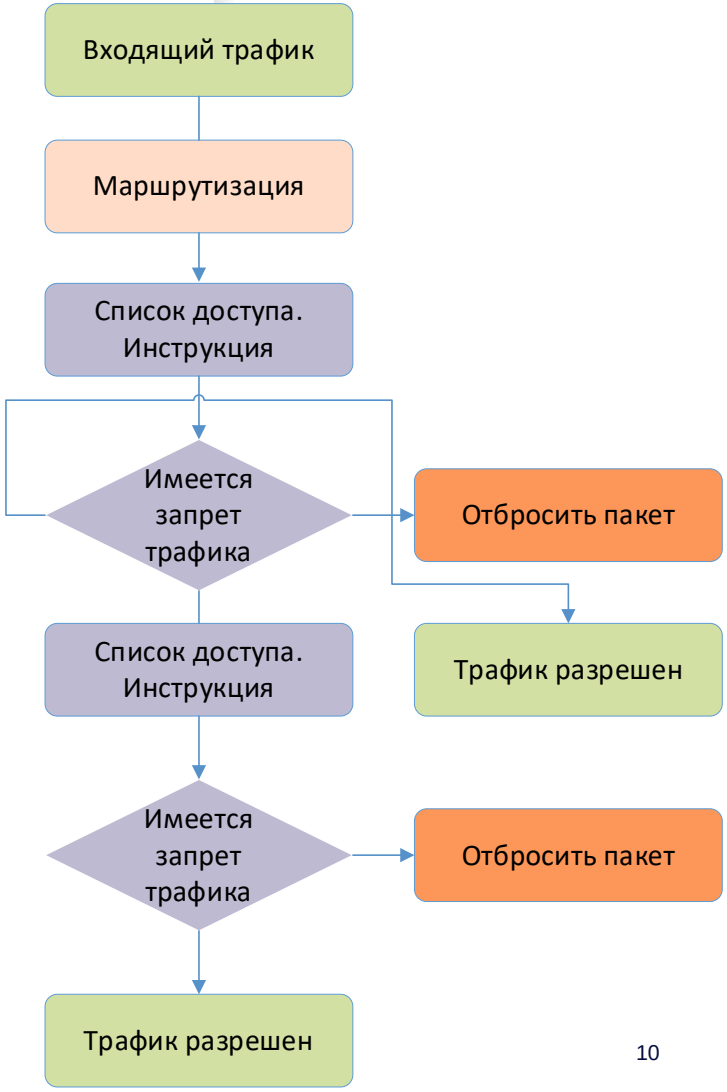
Номер списка принимает значения от 1 до 99. Цифры не означают приоритет или упорядоченность.

- команда *permit*(разрешить)
- *deny* (запретить)
- инвертированная маска (wildcard mask) определяет диапазон адресов, на которые будет распространяться запрет/разрешение.

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



Расширенные списки доступа

Расширенные списки доступа имеют номера от 100 до 199.

Общий пример команды:

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

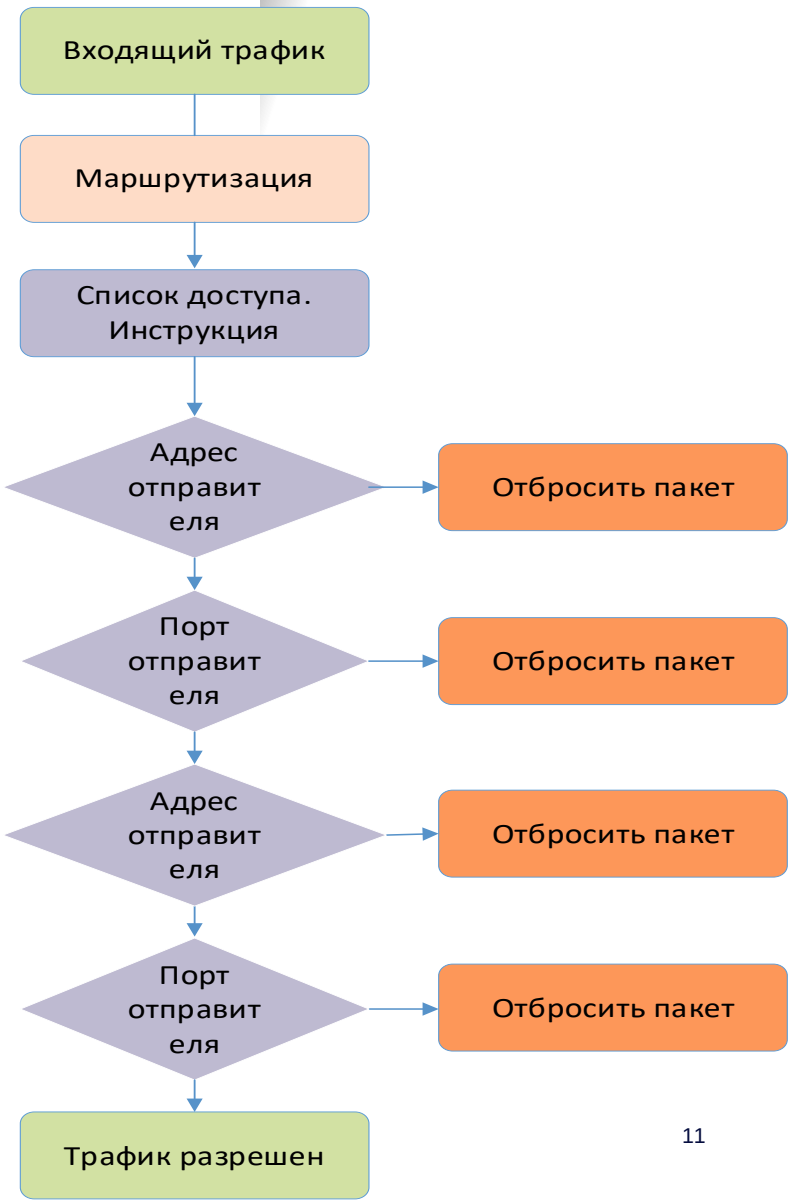
Например:

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

Данная команда разрешает TCP трафик от хостов с диапазоном 192.168.1.0/24 на хосты с диапазоном 10.1.1.0/24 (порт отправителя 80, а порт получателя – 443)

Router(config)#access-list 100 deny tcp any host 172.16.1.5 gt 5000

Команда запрещает весь TCP трафик от любого хоста на конкретный хост с адресом 172.16.1.5 на порт от 5001 и выше



Именованные списки доступа

1. В отличие от стандартных и расширенных списков можно редактировать.

2. 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

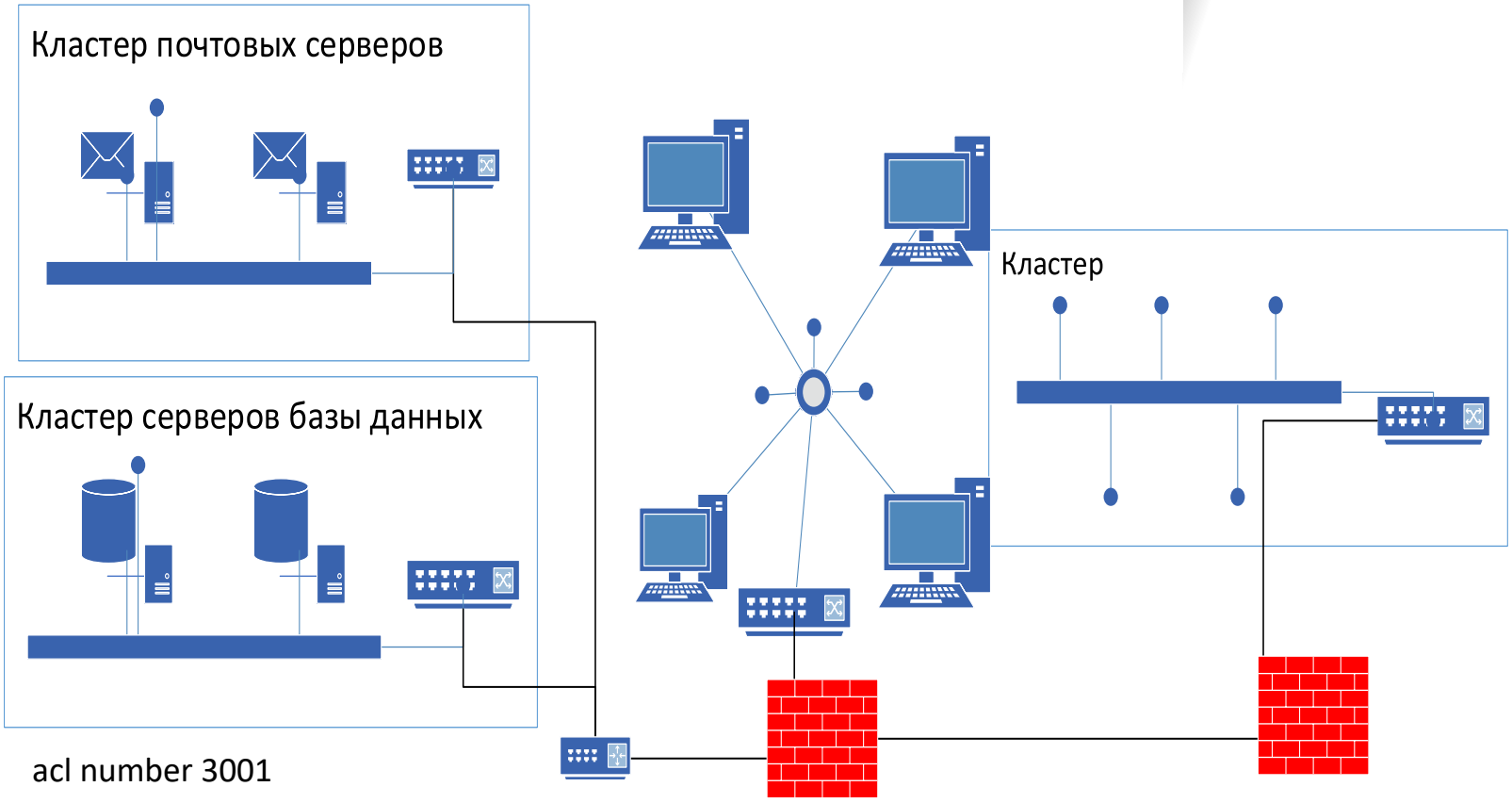
Для расширенных списков:

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

Списки доступа



acl number 3001

rule permit tcp source 192.168.1.0 0.0.0.255

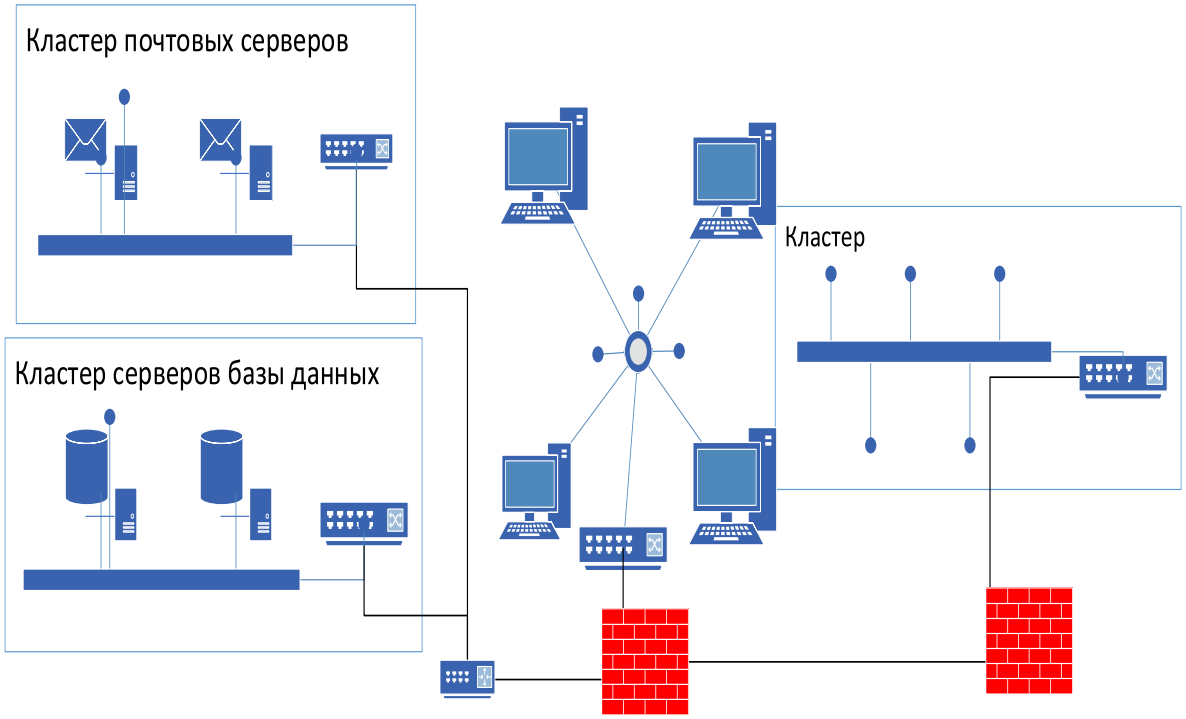
destination 202.1.5.1 source-port any

destination port 80

Rule 20 deny ip source any destination

Списки доступа

Пакетные фильтры, целесообразно встраивать в пограничные маршрутизаторы для передачи трафик другим межсетевым экранам с целью проверки данных на более высоких уровнях стека протоколов.



Достоинства: высокая скорость работы, простота реализации.

Недостатки

- Отсутствует возможность анализа пакетов прикладного уровня.
- Нет защиты 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.

Шлюзы сеансового уровня

Шлюзы сеансового уровня, оперируют на сеансовом уровне иерархии OSI.

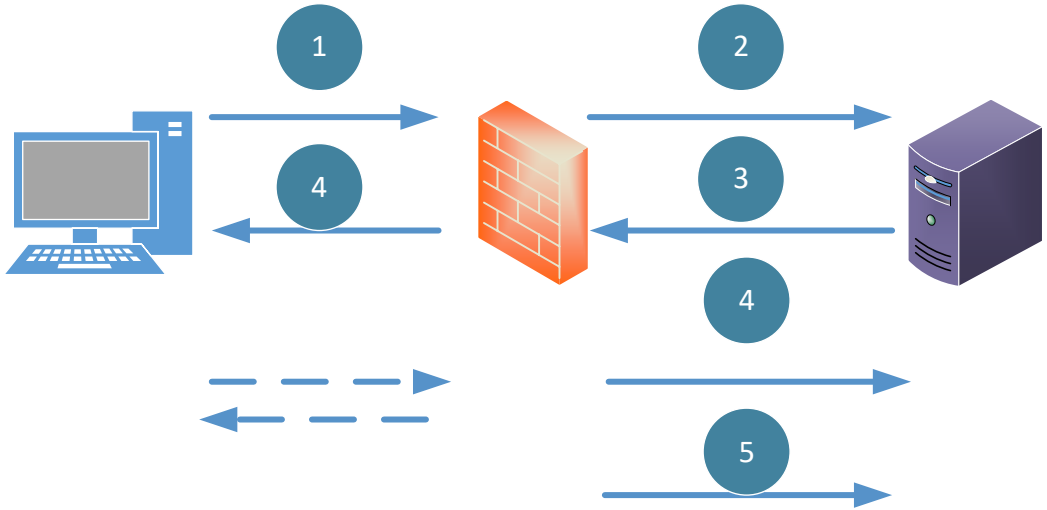
- **Функции:**

1. Динамическая фильтрация в сетевых фильтрах.
2. Фильтрация фрагментированных пакетов.
3. Трансляция IP- адресов.

Шлюзы сеансового уровня

Пример многоступенчатого порядка установления соединения. Процедура установления соединения состоит из следующих этапов:

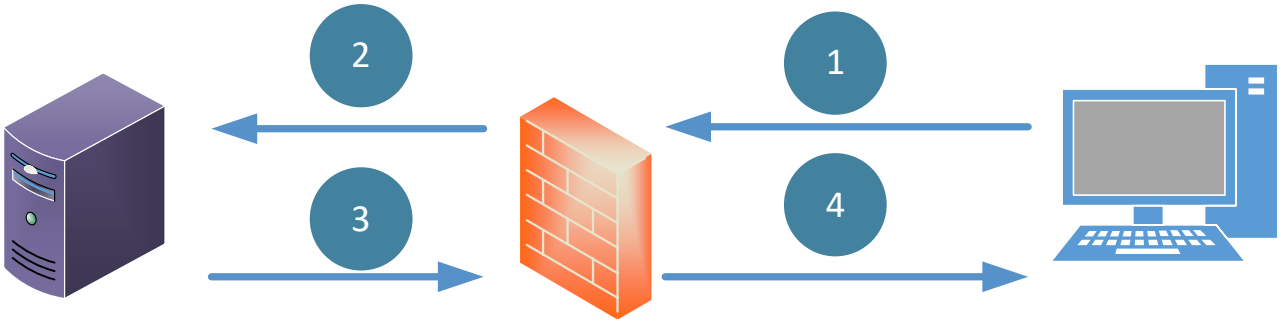
1. МСЭ получает пакет SYN от компьютера A
2. МСЭ передает полученный пакет на сервер B
3. Сервер B передает пакет SYN/ACK на компьютер A, но МСЭ его перехватывает.
4. МСЭ пересылает полученный пакет на компьютер A, кроме того, МСЭ от имени компьютера A посылает пакет ACK на сервер B
5. Если же МСЭ не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



Шлюзы сеансового уровня

Преобразованием IP-адресов (Network Address Translation, NAT), при которых внутренняя сеть имеет адреса, невидимые в общедоступной сети.

1. При обращении компьютера из внутренней сети наружу шлюз перехватывает этот запрос и заносить его в специальную таблицу.
2. Выступает от имени клиента, используя свой внешний (зарегистрированный) IP-адрес.
3. На полученный ответ шлюз идентифицирует получателя по таблице.
4. Передает ответ получателю.



Внутренний IP	Внутренний порт	Внешний IP	Внешний порт
192.168.1.2	50300	184.86.48.128	49127
192.168.1.3	52001	184.86.48.128	49128
192.168.1.2	49238	184.86.48.128	49129

Шлюзы сеансового уровня

- 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.

Шлюзы сеансового уровня

Преимущества:

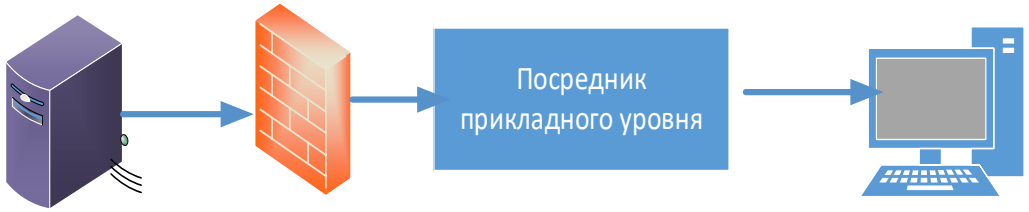
- Позволяет преодолеть нехватку адресов IPv4 и осуществить сокрытие внутренней структуры сети
- Позволяют динамически задавать правила фильтрации трафика

Недостатки:

- Некоторые прикладные протоколы работают неправильно (FTP)
- Нет единого стандарта NAT
- Отсутствует возможность проверки содержания поля данных
- Невозможность регулирования передачи информации на прикладном уровне
- Используют ненадежную систему идентификации и аутентификации, основанную на IP-адресах отправителя/получателя.

Посредники прикладного уровня

Содержат несколько приложений-посредников, каждое из которых обслуживает свой прикладной протокол и позволяют:



Задачи

1. Определение типа сообщения
2. выявление в передаваемых сообщениях несуществующие или нежелательные последовательности команд
3. осуществление проверки аргументов входных данных
4. Аутентификация пользователя
5. Проверка сертификатов
6. Кеширование данных
9. Сбор и мониторинг информации

Посредники прикладного уровня

Кэширование информации с использованием посредника Web на границе внутренней сети, позволяет снизить нагрузку на каналы связи Internet и запускать дополнительные сетевые службы.

Режимы:

- Прямой
- Обратный

Посредники прикладного уровня

Преимущества:

- 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.

Недостатки:

- 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

Инспекторы состояния

Термин «инспектор состояния» был введен компанией Check Point. 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.

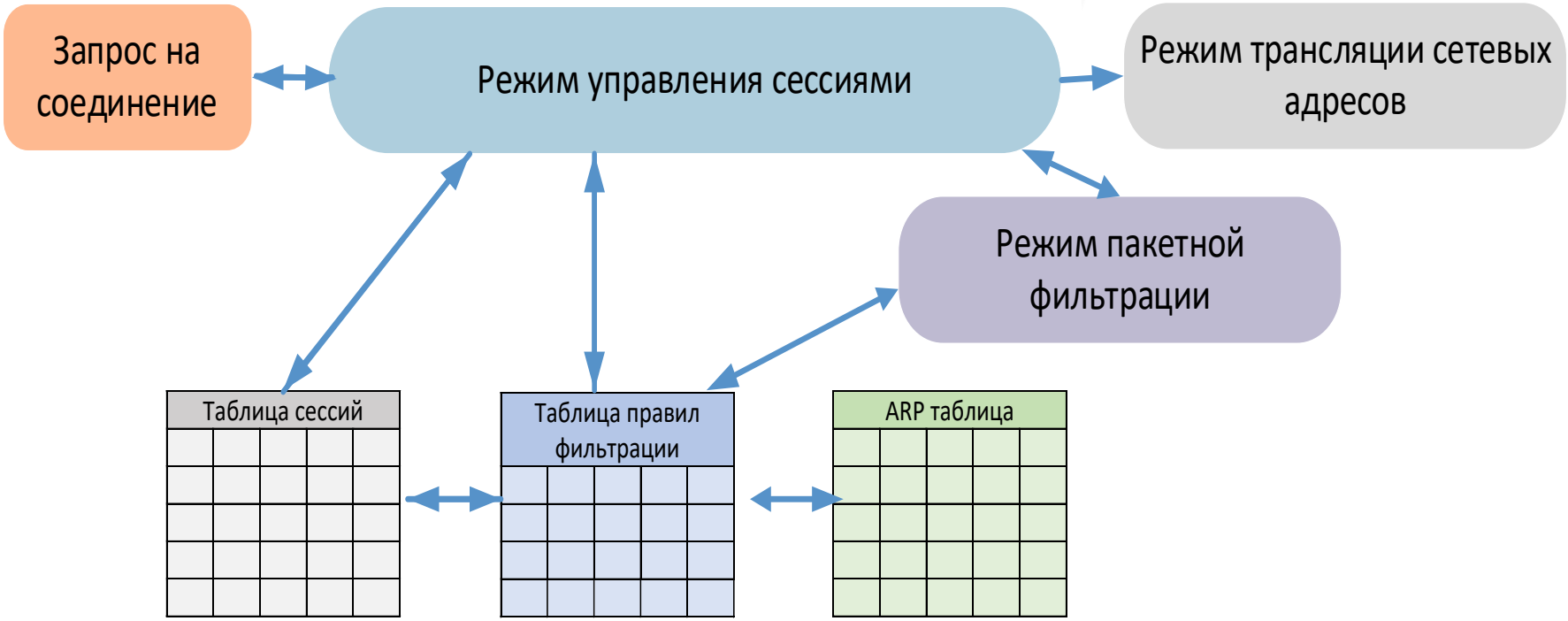
При получении пакета данных содержимое этого пакета сравнивается с некими шаблонами, специфическими для соответствующего протокола прикладного уровня. Осуществляется выполнение следующих действий:

- пропуск пакета;
- удаление пакета и сессии;
- регистрация пакета и сессии.

Дополнительные функции:

- Трансляция сетевых адресов
- Аутентификация пользователей
- Регистрация событий

Инспекторы состояния. Управление сессиями



Инспекторы состояния

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

Инспекторы состояния. Фильтрация прикладных протоколов

Идентификация основных прикладных протоколов независимо от порта сервиса

Протокол HTTP:

фильтрация по адресам WEB-серверов

фильтрация по именам (фрагментам) файлов

фильтрация по методу запроса

Протокол SMTP:

фильтрация по почтовым адресам отправителя и получателя

Протокол FTP:

фильтрация по командам put, get

фильтрация по именам (фрагментам) файлов

фильтрация по имени/паролю пользователя

Сервисы SQL:

фильтрация по SQL-запросам

Инспекторы состояния. Фильтрация прикладных протоколов

Дополнительные функции

- Проверка подлинности (**аутентификация**) пользователя может осуществляться как при предъявлении обычного идентификатора (имени) и пароля, так и с помощью цифровых сертификатов.
- **Протоколирование и аудит.** Межсетевой экран имеет возможность регистрации всех действий: пропуск или блокирование сетевых пакетов, изменение правил разграничения доступа администратором безопасности.

Инспекторы состояния. Фильтрация прикладных протоколов

Преимущества:

- Прозрачность для конечного пользователя, не требующая дополнительной настройки пли 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).

Недостатки:

Допускают прямое соединение между авторизованным клиентом и компьютером внешней сети.

- .

Демилитаризованная зона

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

Архитектура DMZ:

- 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).

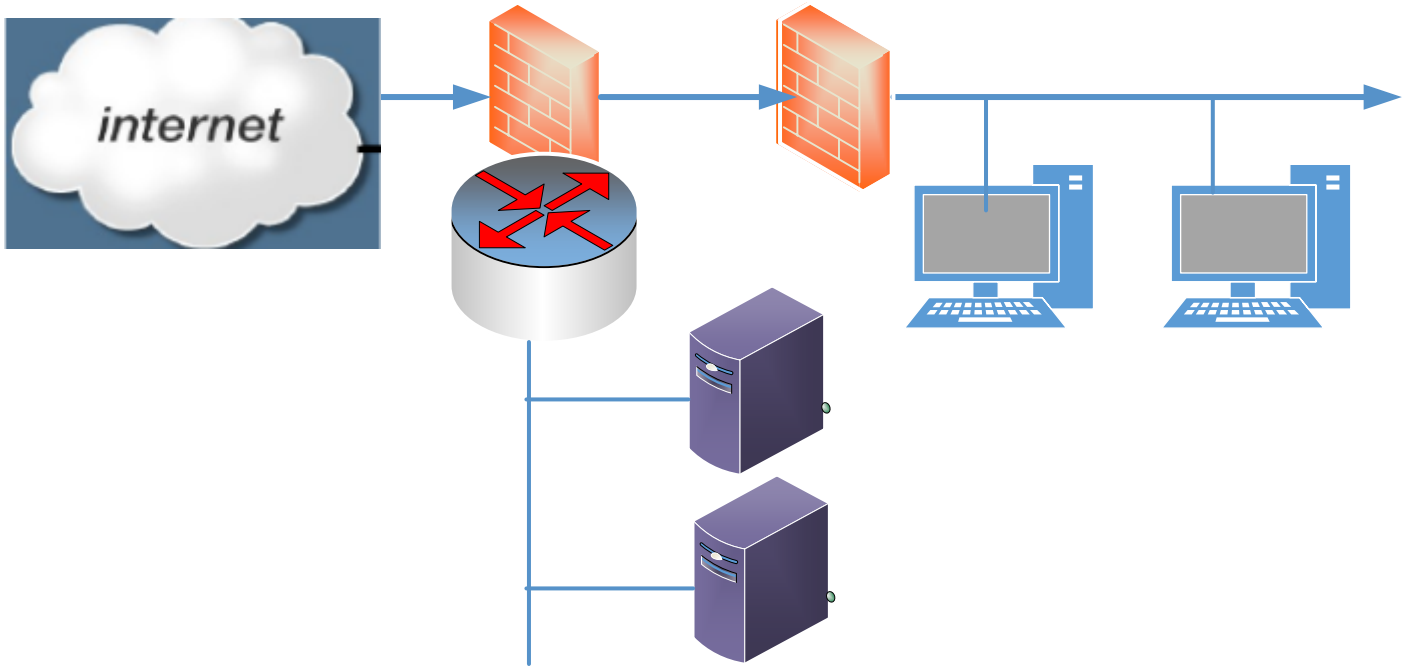
Демилитаризованная зона

Политика:

- Прохождение пакетов от более безопасного интерфейса к менее безопасному разрешено , если не запрещено.
- Прохождение пакетов от менее безопасного интерфейса к более безопасному запрещено, если не разрешено.
- Прохождение пакетов на интерфейсах с одинаковым уровнем безопасности запрещено.
- Размещение межсетевого экрана в том месте, где происходит разветвление маршрута.

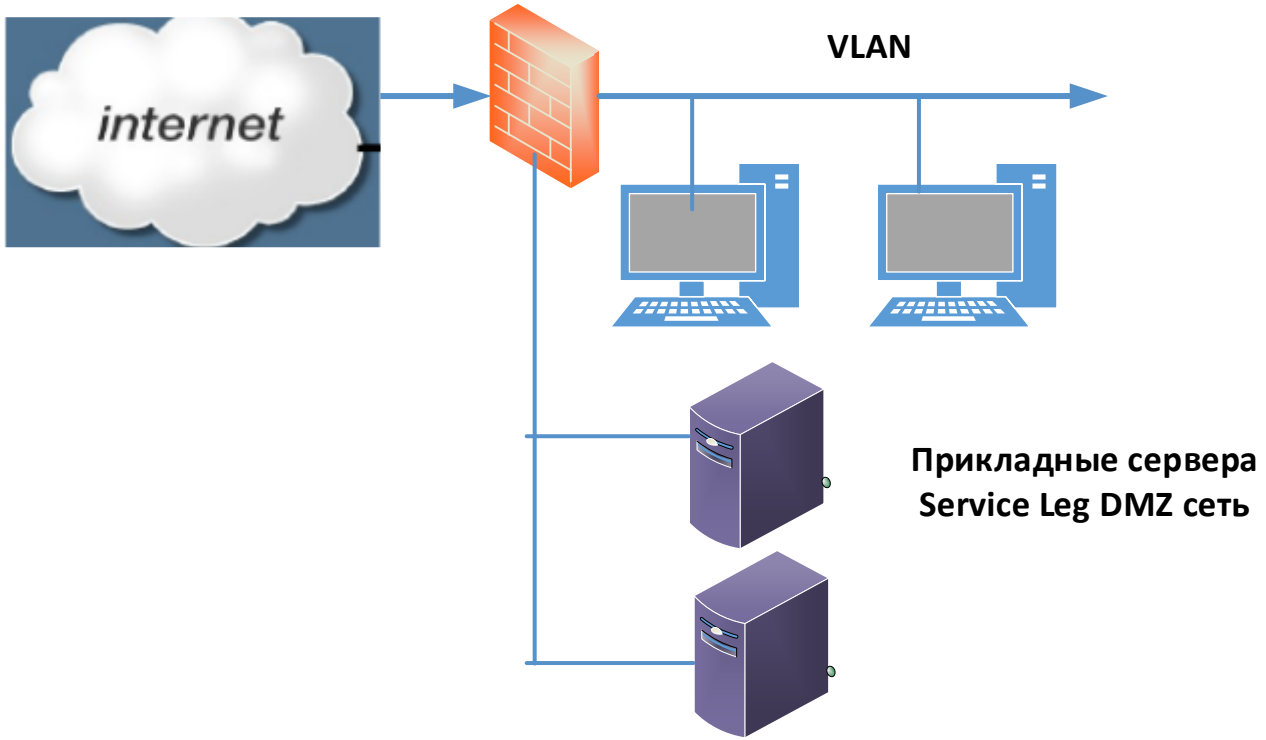
Конфигурация с одной DMZ-сетью

В DMZ располагают публично доступные сервера, такие как веб-сервер или почтовый сервер, которые не должны быть размещены во внутренних защищенных сетях, но к которым необходим доступ либо только извне, либо только изнутри, либо и извне, и изнутри. Причина в том, что никогда нельзя гарантировать, что эти системы и ресурсы не могут быть взломаны. Но взлом этих систем не должен автоматически означать доступ ко всем внутренним системам



Service Leg конфигурация

Сетевые интерфейсы МСЭ соединяются с Интернетом, внутренней сетью, отдельным сетевым интерфейсом формируется DMZ-сеть.



Недостаток: возрастание риска DoS-атаки на межсетевой экран, при интересе со стороны злоумышленника к сервисам, расположенные в DMZ-сети.

Конфигурация с двумя DMZ-сетями

Архитектура:

Пограничный маршрутизатор- осуществляет фильтрацию пакетов и обеспечивает защиту серверов.

Основной межсетевой экран управляет доступом для внутренних серверов, и служит защитой для межсетевых экранов как от внешних, так и от внутренних атак.

Межсетевой экран внутренней DMZ обеспечивает управление доступом и защиту серверов, если внешние сервера атакованы.

Нарушения безопасности

1. Обход МСЭ через модем
2. Обход правил фильтрации персоналом из внутренней сети
3. Использование механизмов туннелирования
4. Атака на МСЭ
5. Подмена IP адреса
6. Перехват, подбор пароля

Межсетевые экраны. Нормативно-правовое обеспечение

- Приказ ФСТЭК № 17 от 11 февраля 2013 года
- Приказ ФСТЭК № 21 от 18 февраля 2013 года
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утверждёнными Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119
- Приказ ФСТЭК России от 9 февраля 2016 г. №9 Требования к межсетевым экранам
- Информационное сообщение ФСТЭК «Об утверждении требований к межсетевым экранам» от 28 апреля 2016 г. N 240/24/1986

Межсетевые экраны. Нормативно-правовое обеспечение

Типы межсетевых экранов согласно Информационному сообщению ФСТЭК «Об утверждении требований к межсетевым экранам» от 28 апреля 2016 г. N 240/24/1986:

- тип «А»: межсетевой экран, применяемый на физической границе или между физическими границами сегментов локальной инфраструктуры организации;
- тип «Б»: межсетевой экран, применяемый на логической границе или между логическими границами сегментов локальной инфраструктуры организации;
- тип «В»: межсетевой экран, применяемый на узле (хосте) информационной системы;
- тип «Г»: межсетевой экран, применяемый на сервере или на физической границе сегмента серверов;
- тип «Д»: межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами.

Межсетевые экраны. Нормативно-правовое обеспечение

Приказ ФСТЭК России от 9 февраля 2016 г. №9 Требования к межсетевым экранам

Для дифференциации требований к функциям безопасности межсетевых экранов выделяются шесть классов защиты межсетевых экранов. Самый низкий класс – шестой, самый высокий – первый.

Класс защищённости	**Применение**		
	ГИС	АСОИУ	ИСПДн
Межсетевые экраны, соответствующие 6 классу защиты	3 и 4 классы защищенности	3 класс защищенности	3 и 4 уровни защищенности персональных данных
Межсетевые экраны, соответствующие 5 классу защиты	2 класс защищенности	2 класс защищенности	2 уровень защищенности персональных данных
Межсетевые экраны, соответствующие 4 классу защиты	1 класс защищенности	1 класс защищенности	1 уровень защищенности персональных данных
Межсетевые экраны, соответствующие 3, 2 и 1 классам защиты	Гос тайна		

Межсетевые экраны. Алгоритм выбора

1. **Определить все требования, которые накладывает законодательство и внешнее окружение на функционирование межсетевого экрана**.

   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 «А» может быть только программно-аппаратным.

   1.4 Проверить наличие сертификатов.

Межсетевые экраны. Алгоритм выбора

2. 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 Проанализировать производительность МСЭ на заданном наборе правил.

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

Межсетевые экраны. Алгоритм выбора

4. **Управление архитектурой, политиками, ПО и другими компонентами межсетевого экрана.**

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

   4.2 Балансировка компонент межсетевого экрана, чтобы потенциальные проблемы с доступом к ресурсам были своевременно устранена.

   4.3 Динамический мониторинг сетевого окружения и журналов событий для определения угроз, как осуществленных, так и не осуществленных.

Литература

1. Приказ ФСТЭК № 17 от 11 февраля 2013 года
2. Приказ ФСТЭК № 21 от 18 февраля 2013 года
3. Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утверждёнными Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119
4. Приказ ФСТЭК России от 9 февраля 2016 г. №9 Требования к межсетевым экранам
5. Информационное сообщение ФСТЭК «Об утверждении требований к межсетевым экранам» от 28 апреля 2016 г. N 240/24/1986
6. 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»).