Основы безопасности информационных технологий

Технологии межсетевых экранов.

Содержание лекции

- Основные понятия
- Фильтрация пакетов
- Межсетевые экраны уровня соединения
- Межсетевые экраны прикладного уровня
- Межсетевые экраны с динамической фильтрацией пакетов
- Межсетевые экраны инспекции состояний
- Межсетевые экраны уровня ядра
- Обход межсетевых экранов
  - постепенный подход
  - туннелирование

Основные понятия

Межсетевой экран (сетевой экран) — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Задачи:

- защита и изоляция приложений, сервисов и машин во внутренней сети от нежелательного трафика, приходящего из внешней сети интернет
- ограничение или запрещение доступа хостов внутренней сети к сервисам внешней сети интернет
- поддержка преобразования сетевых адресов (network address translation, NAT)

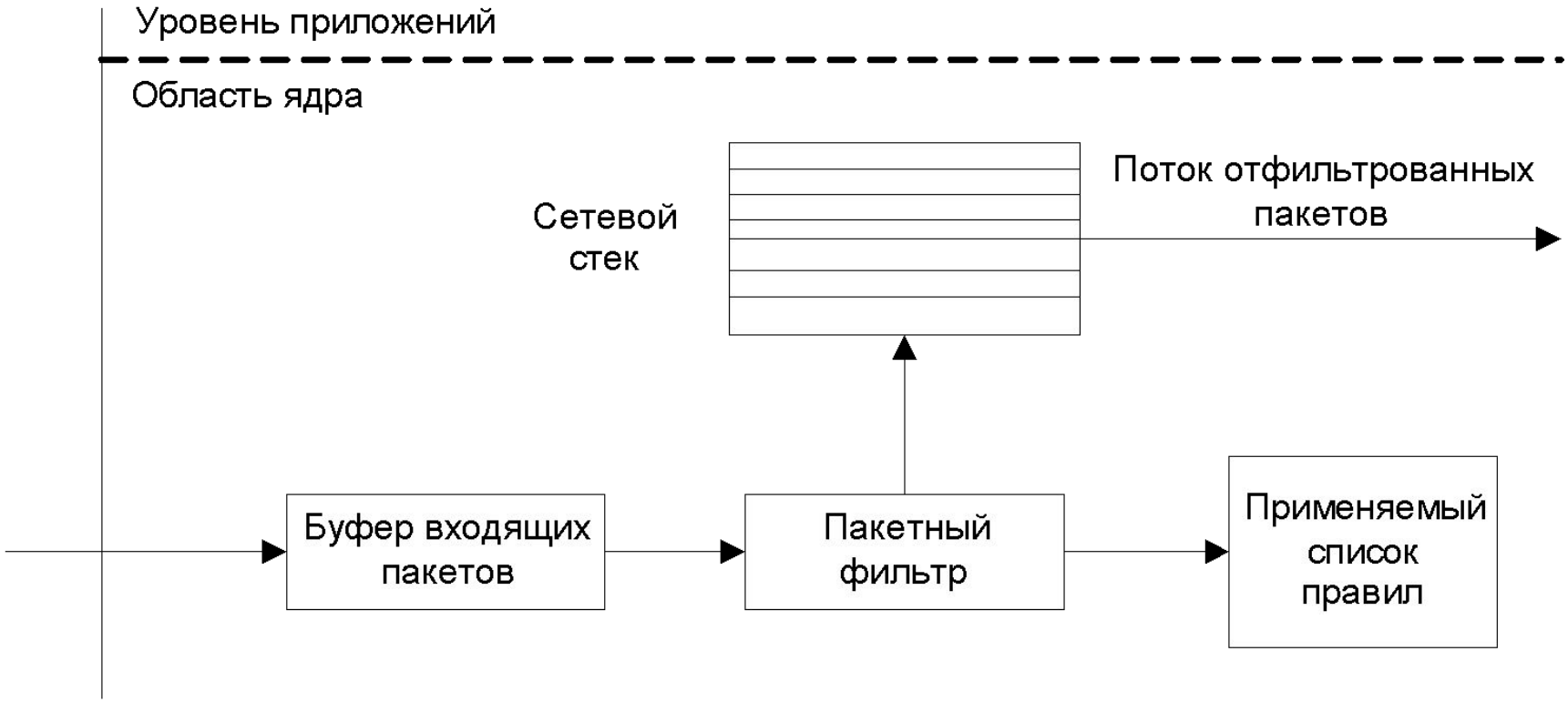
Фильтрация пакетов

Фильтры пакетов контролируют:

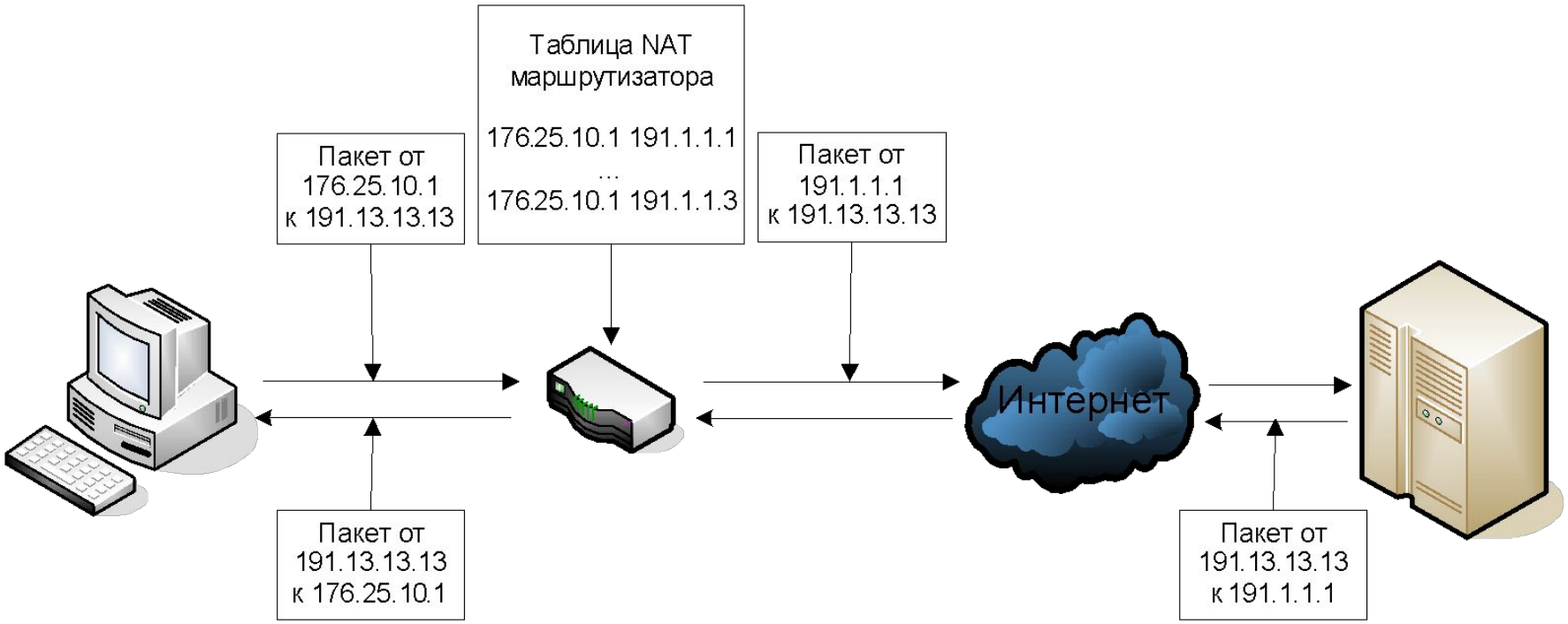
- физический интерфейс, откуда пришел пакет
- IP-адрес источника
- IP-адрес назначения
- тип транспортного уровня (TCP, UDP, ICMP)
- транспортные порты источника и назначения

Фильтрация пакетов

Схема архитектуры фильтра пакетов



Трансляция пакетов

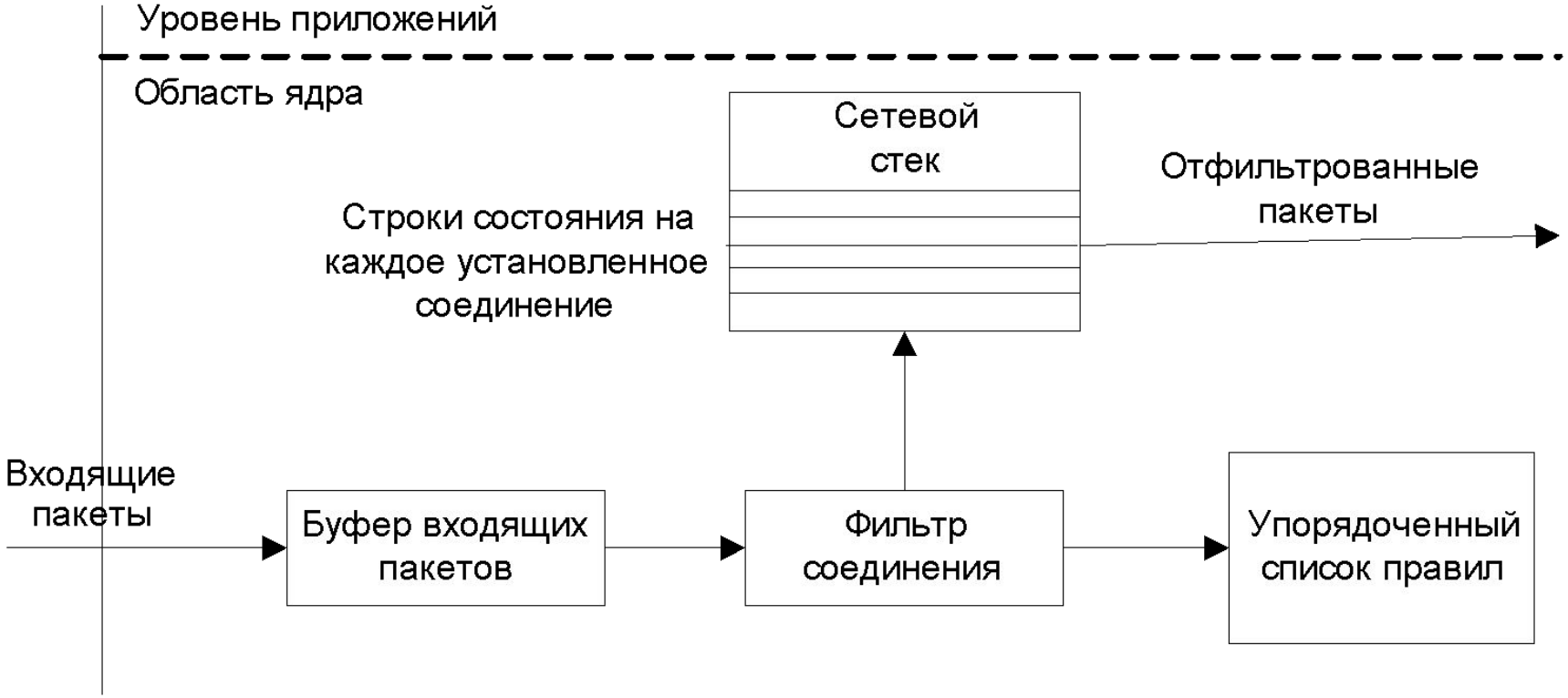


Достоинства и недостатки технологии фильтрации

Преимущества	Недостатки
Быстрота работы (по сравнению с другими технологиями МЭ) МЭ может быть реализован аппаратно Не требуется конфигурирование хостов пользователя Схема NAT «прячет» внутренние IP-адреса	Не «понимает» прикладные протоколы Не может ограничить доступ подмножеству протоколов даже для основных служб Не отслеживает соединения (не содержит информацию о сеансе) Слабые возможности обработки информации внутри пакета Не может ограничить информацию с внутренних компьютеров к службам МЭ сервера Практически не имеет аудита Трудно тестировать правила (из-за сложности внутренних сетей, наличия различных служб)

Межсетевые экраны уровня соединения

Схема функционирования МЭ уровня соединения



Межсетевые экраны уровня соединения

Таблица состояний:

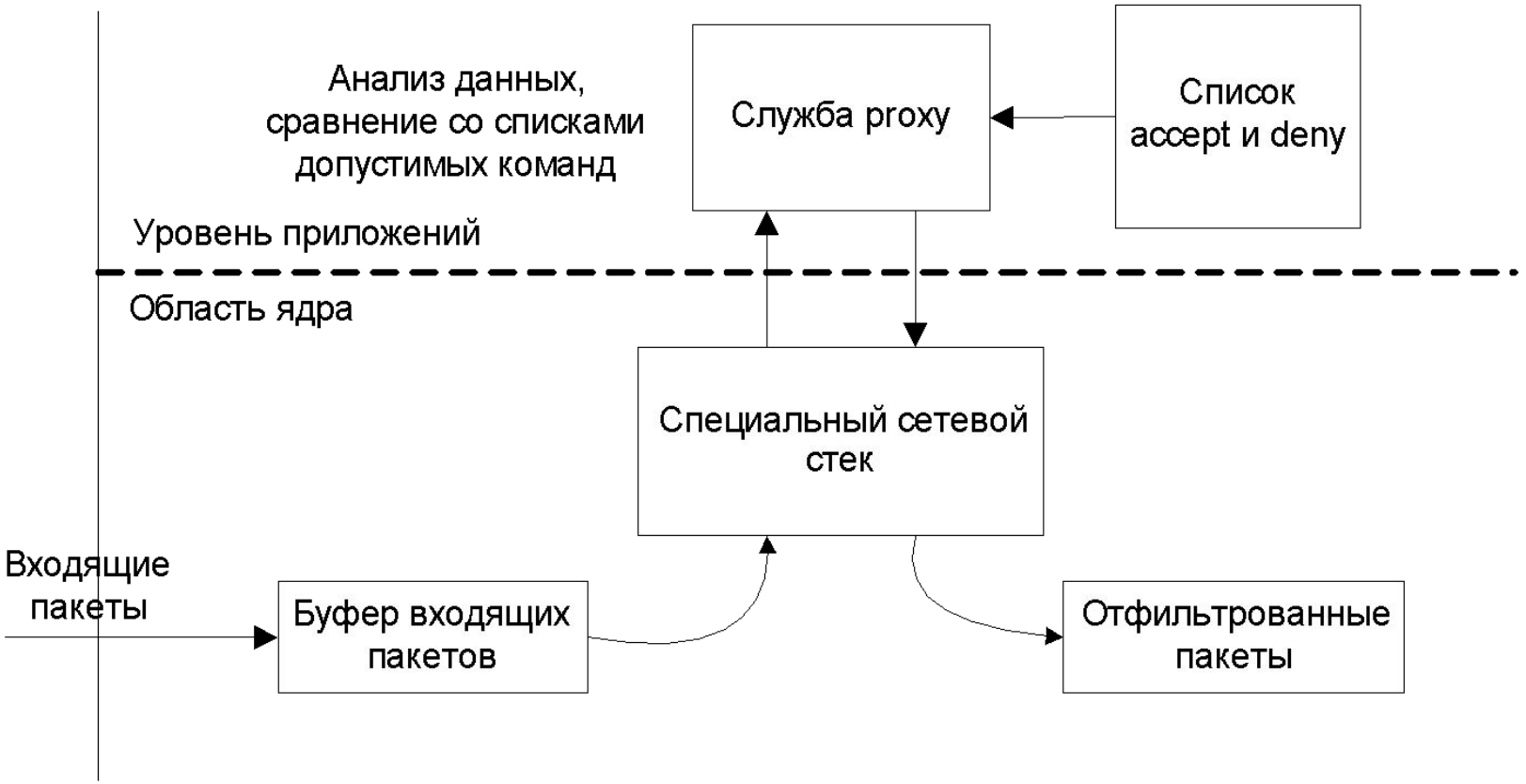
- идентификатор сеанса
- состояние соединения
- последовательная информация
- IP-адрес источника и IP-адрес назначения
- номера портов, участвующих в сеансе
- физический интерфейс, куда прибыл пакет
- физический интерфейс, куда передается пакет
- временные метки начала открытия сеанса и т.д.

Достоинства и недостатки технологии соединений

Достоинства	Недостатки
Возможность запрещения соединений с определенными хостами При использовании NAT — скрытие внутренних IP-адресов	Не могут ограничить доступ протоколов, отличных от TCP Не осуществляют проверки для протоколов высших уровней Ограниченный аудит (слабая связь с высшими уровнями протоколов) Не позволяют дополнения функций — HTTP-кэширования ответов, фильтрации URL, аутентификацию Трудность тестирования правил

Межсетевые экраны прикладного уровня

Схема функционирования МЭ прикладного уровня

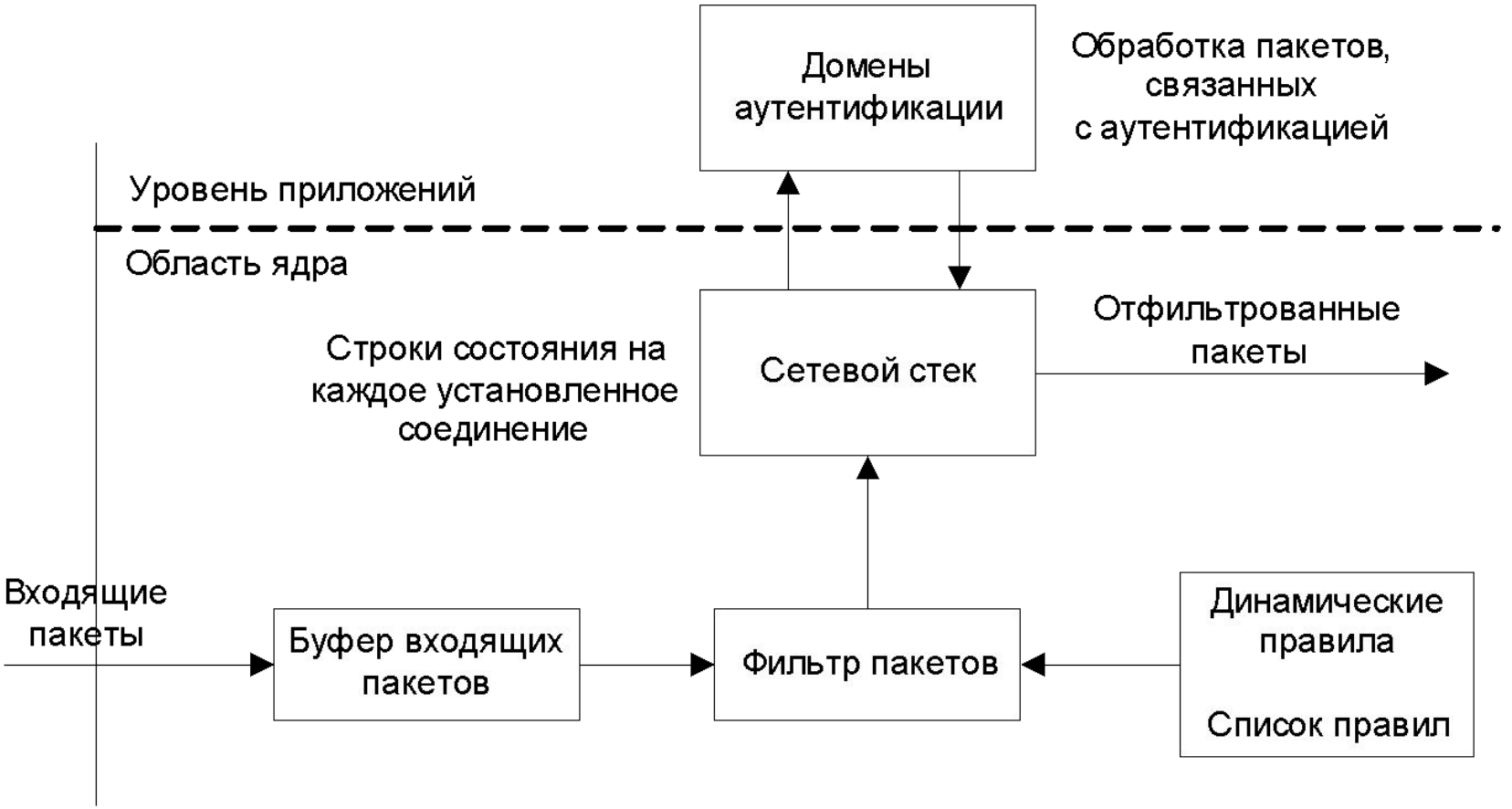


Достоинства и недостатки МЭ прикладного уровня

Достоинства	Недостатки
Работа с протоколами высшего уровня (HTTP, FTP)	Служба proxy требует замены сетевого стека на сервере МЭ
Возможность хранения частичной информации о состоянии, полной информации состояния приложения и частичной информации о сеансе	Служба proxy слушает порт (как сетевой сервер, т.е. МЭ не может его использовать)
Возможность ограничения доступа к определенным сетевым службам	Временная задержка (входной пакет обрабатывается дважды — приложением и proxy)
Возможность оперирования с информацией данных пакета	Новый proxy должен быть добавлен для каждого контролируемого протокола
Запрещение прямого соединения с внешними серверами	Службы proxy обычно требуют модификации процедур клиентов
Прозрачность proxy	Службы proxy уязвимы к ошибкам ОС и ПО прикладного уровня
Возможность реализации дополни тельных свойств (фильтрации URL, аутентификации, кэширования HTTP)	Не осуществляется проверка информации пакета, содержащейся в низших уровнях
Хороший аудит	Служба proxy может требовать дополнительных паролей или процедур аутентификации

Межсетевые экраны с динамической фильтрацией пакетов

Схема функционирования МЭ с динамической фильтрацией



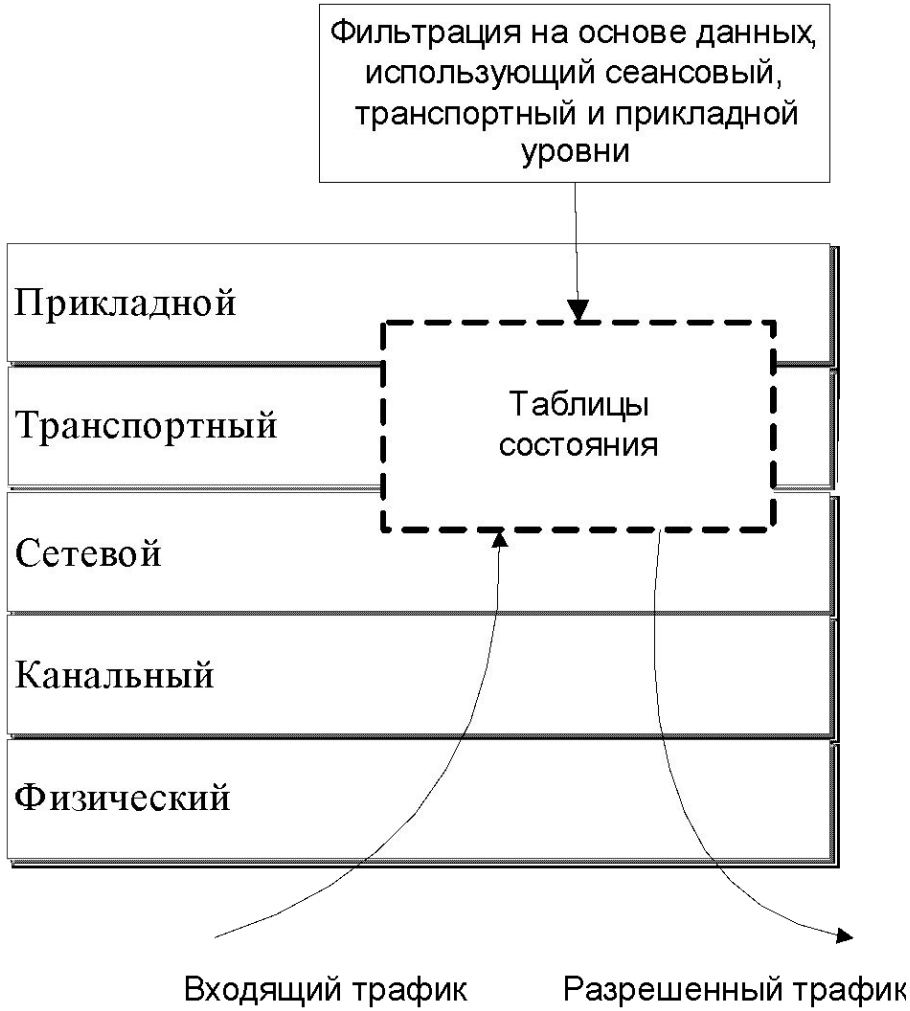
Достоинства и недостатки МЭ с динамической фильтрацией

Достоинства	Недостатки
Не позволяет непрошеным пакетам UDP войти во внутреннюю сеть Если запрос пакета UDP приходит из внутренней сети и направлен на не доверенный хост, то сервер МЭ позволяет появление ответного пакета, доставляемого хосту — инициатору запроса. Пакет ответа должен содержать IPн (соответствующий запросу) и номер порта (соответствующий запросу) и иметь соответствующий тип протокола транспортного уровня Динамический фильтр может использоваться для поддержки ограниченного множества команд ICMP	Не «понимает» прикладные протоколы Не может ограничить доступ подмножеству протоколов даже для основных служб Не отслеживает соединения Слабые возможности обработки информации внутри пакета Не может ограничить информацию с внутренних компьютеров к службам МЭ сервера Практически не имеет аудита Трудно тестировать правила (из-за сложности внутренних сетей, наличия различных служб)

Межсетевые экраны инспекции состояний

Таблица состояний:

- протокол, используемый для соединения
- IP-адреса источника и назначения
- номера портов источника и назначения
- листинг с обращенными адресами и номерами портов
- время, по истечению которого соединение будет удалено
- состояние TCP-соединения
- состояние отслеживаемого соединения



Пример записи в таблице состояний для IPtables

- *tcp 6 93 SYN_SENT src=192.168.1.1 dst=192.168.200.200 sport=1054 dport=21 [UNREPLIED] src=192.168.200.200 dst = 192.1 68.1.1 sport=21 dport=1054 use=1*

- *tcp 6 41294 ESTABLISHED src=192.168.1.1 dst=192.168.200.200 sport=1054 dport = 21 src=192.168.200.200 dst=192.168.1.1 [ASSURED] use=1*

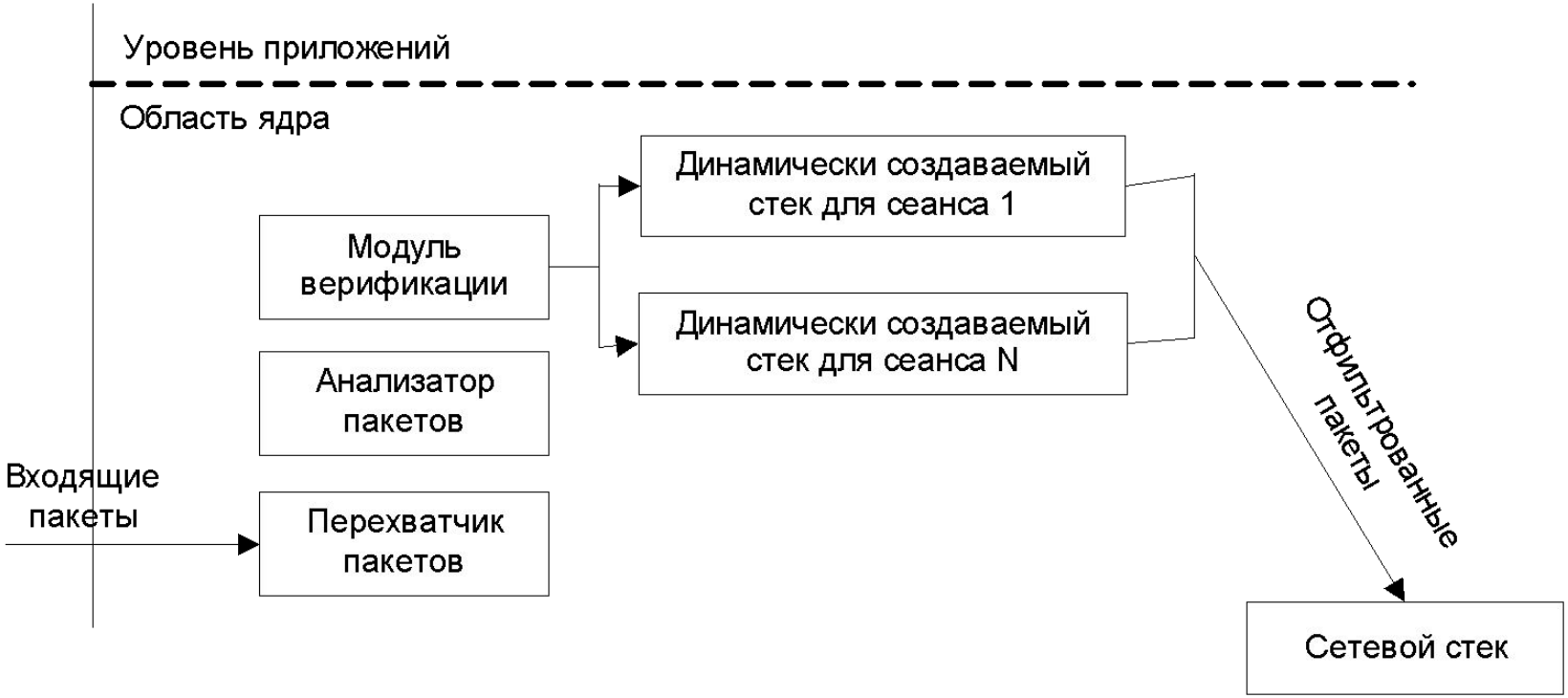
Межсетевые экраны уровня ядра

Подсистема МЭ включает следующие модули:

- ядро безопасности
- модуль управления хостом
- модуль управления каналами связи МЭ
- агент регистрации входов
- агент аутентификации

Межсетевые экраны уровня ядра

Схема функционирования МЭ уровня ядра



Виды Proxy

- для IP
- для ICMP
- для TCP
- для UDP
- для HTTP
- для FTP
- для Telnet
- для SMTP

Обход межсетевых экранов: постепенный подход

Под *постепенным подходом* (firewalking) понимается методика сбора информации об удаленной сети, защищенной МЭ используя трассировкочно-подобные методы для посылки и анализа ответов на IP-пакетов

Обход межсетевых экранов: туннелирование

В процессе инкапсуляции применяются три типа протоколов:

- несущий протокол
- протокол-пассажир
- протокол инкапсуляции

Необходимо решить следующие задачи:

- разработать несущий протокол, протокол-пассажир и протокол инкапсуляции
- проанализировать методы обнаружения туннеля и снизить влияние демаскирующих факторов