# Администрирование локальных сетей

Лекция 8

Безопасность сетевых соединений

# Обзор лекции

- Описание функций и утилит пакетной фильтрации
- Список известных портов и приложений, которые их используют.
- Список критериев которые вы можете использовать для фильтрации сетевого трафика.
- Описание возможностей пакетной фильтрации в Microsoft Windows Server .
- Список основных уязвимостей сетевых соединений.
- Описание функций IPSec.

# Обзор лекции

- Описание функций и архитектуры протоколов IPSec.
- Список компонентов IPSec в Windows Server .
- Список политик IPSec по умолчанию включенных в Windows Server и их использование.
- Описание функций компонентов политик IPSec.
- Использование оснастки IP Security Policies для управления политиками IPSec.

# Безопасность соединений на основе сетевых фильтров

- Фильтрация пакетов позволяет защитить компьютеры от разрушительного сетевого трафика с помощью блокировки пакетов с определенными параметрами.
- Брандмауэры обычно используют пакетные фильтры для пропуска разрешенного трафика и блокировании неавторизованного трафика.
- Фильтрующие пакеты позволяют защитить против вирусов, подмены данных и других атак хакеров.

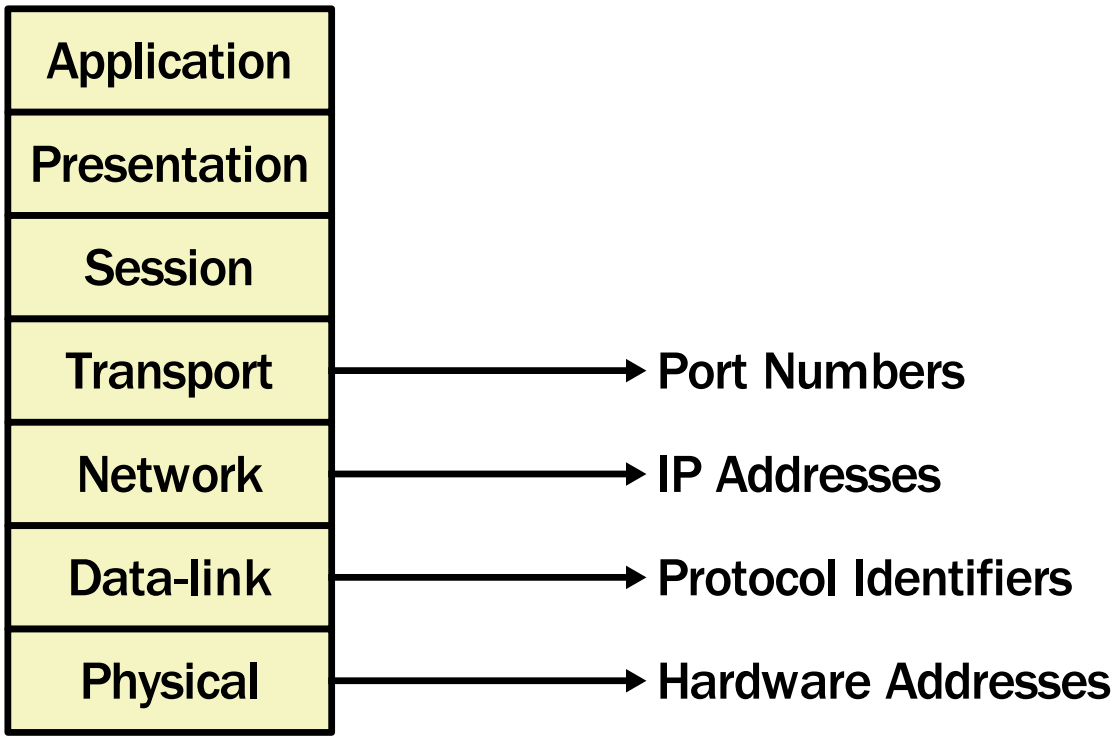
# Назначение номеров порта и протокола

- Адреса IP определяют системы, которые отправляют и получают системы.
- Поле Protocol в IP пакете задает тип протокола транспортного уровня который инкапсулирован в пакет.
- Каждый протокол транспортного уровня имеет поле Port которое определяет приложение, которое получает данные пакета.

# Введение в пакетные фильтры

- Пакетная фильтрация позволяет управлять сетевым трафиком по таким критериям как IP адрес, протоколы и номера портов.
- Пакетные фильтры часто используются на маршрутизаторах для обеспечения доступа в Интернет.

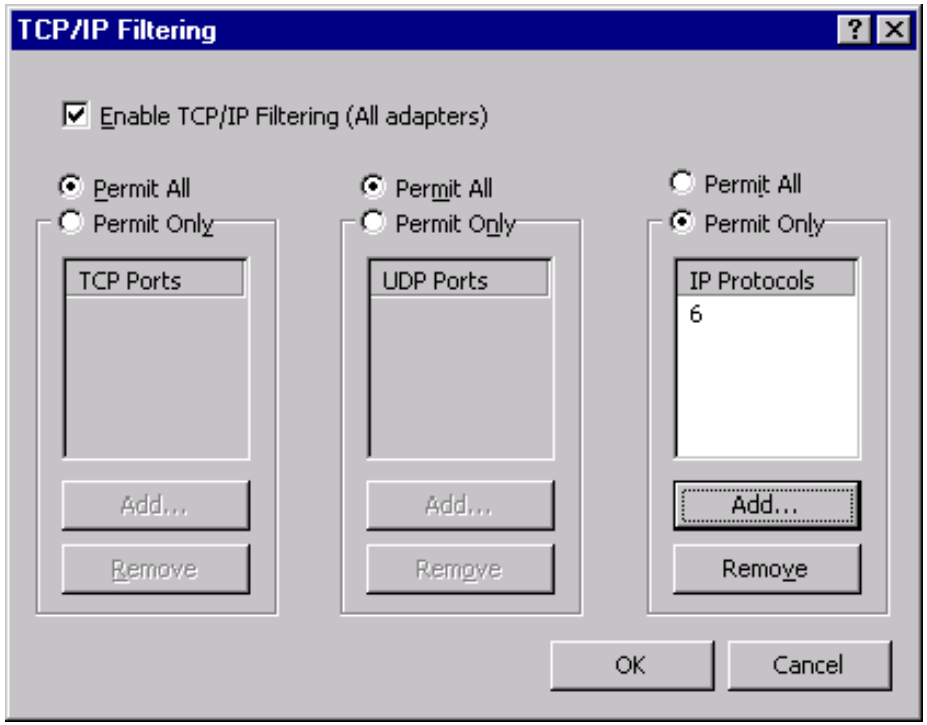
# Критерии пакетных фильтров



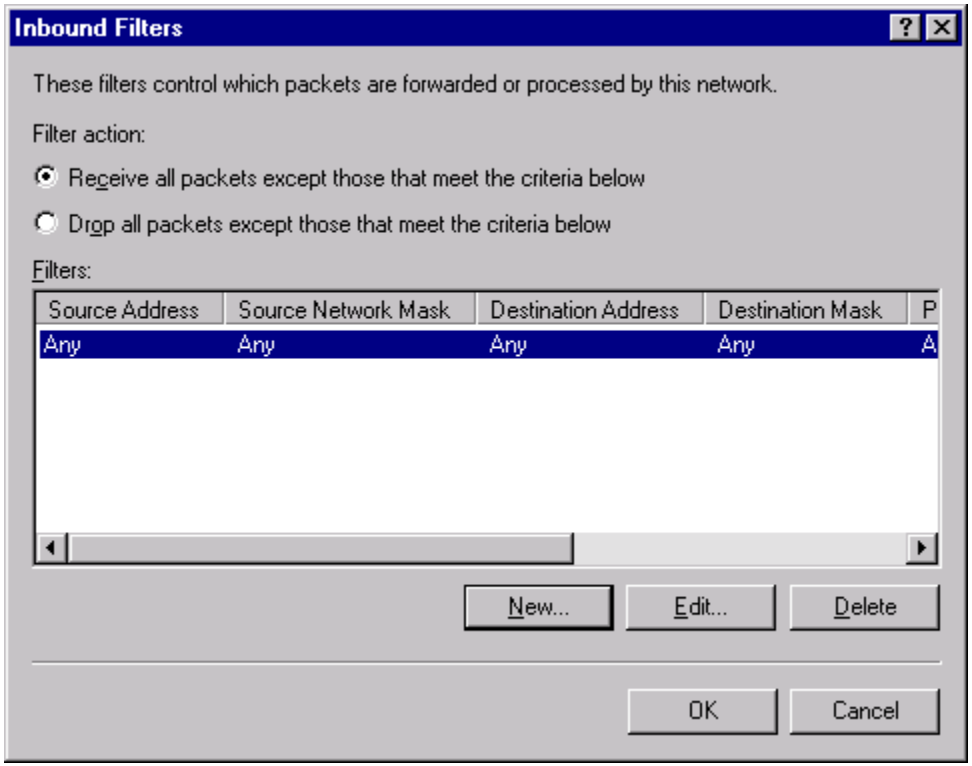
# Реализация пакетной фильтрация в WINDOWS SERVER

- Пакетная фильтрация TCP/IP
- Пакетная фильтрация Routing and Remote Access Service (RRAS)

# Использование пакетной фильтрации TCP/IP



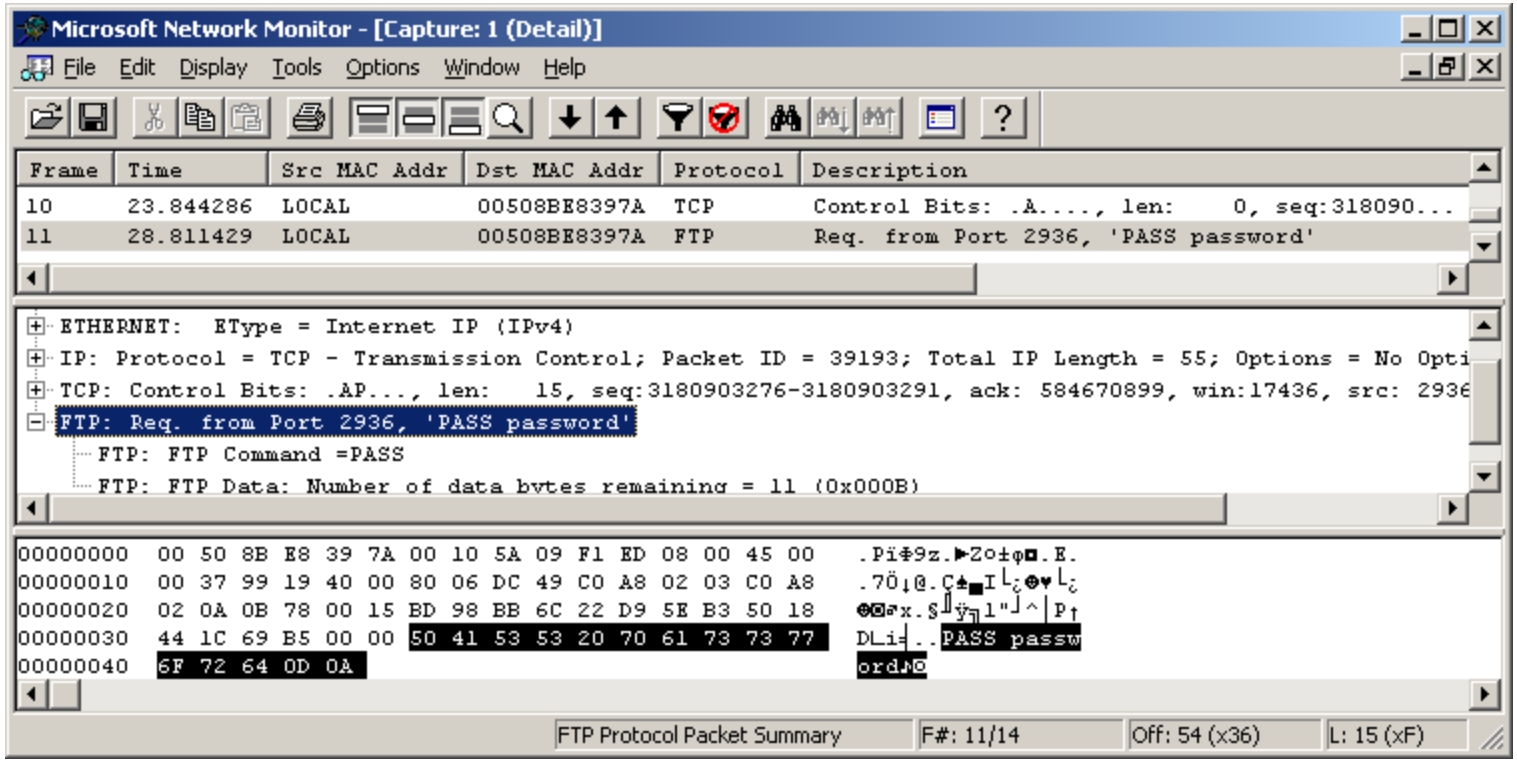
# Использование пакетной фильтрации RRAS



# Защищенная передача в сети

- При необходимости обеспечить защиту конфиденциальных данных в сети Windows Server поддерживает IPSec, что может быть использовано для защиты данных при передаче.

# Демонстрация необходимости защиты



# Введение в IPSec

- Расширения IP Security (IPSec) обеспечивают защиту трафика в IP-сетях.
- IPSec защищает данные средствами цифровой подписи и их шифрования перед передачей данных.
- IPSec – протокол сетевого уровня и может быть передан через любую сетевую среду или устройства поддерживающий протокол IP.

# Функции IPSec

Шифрование IPSec использует алгоритмы Data Encryption Standard (DES) или Triple Data Encryption Standard (3DES).

IPSec позволяет несколько функций безопасности:

- генерация ключей,
- использование криптографических контрольных сумм,
- множественную аутентификацию, предотвращение повторного использования,
- фильтрацию IP пакетов

Использование IPSec предотвращает просмотр, изменение и удаление данных в пакетах, а также IP спуфинг.

# Стандарты IPSec

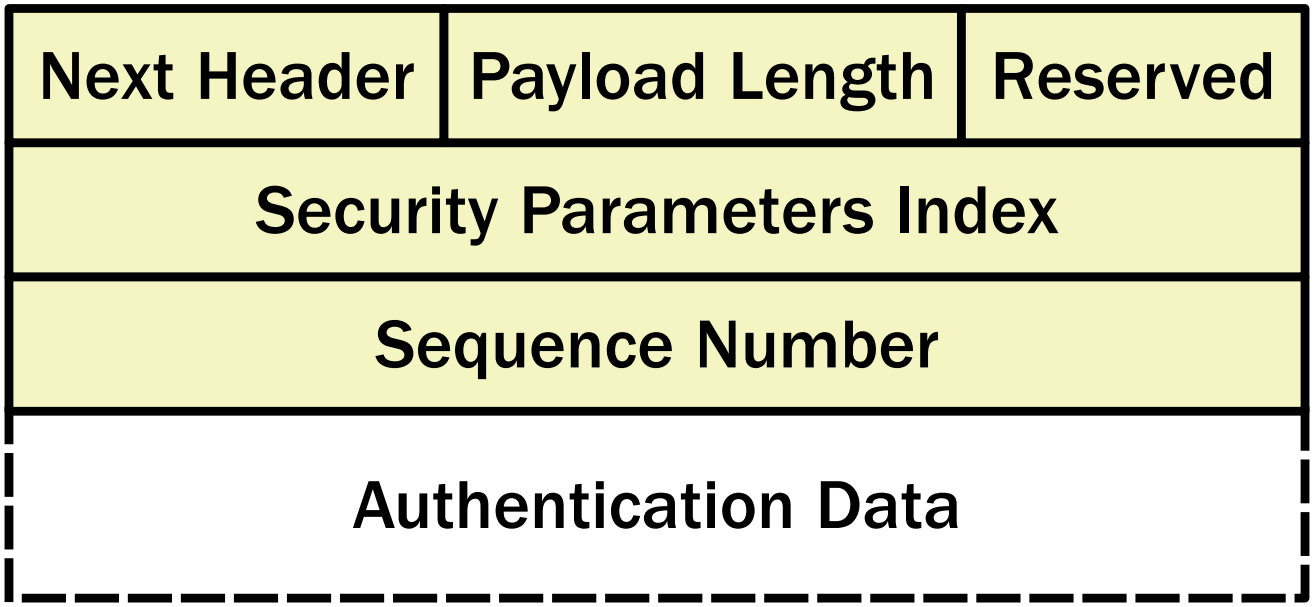
- IPSec основываются на стандартах одобренных Internet Engineering Task Force (IETF).
- Документ RFC 2411, “IP Security Document Roadmap,” описывает работу стандартов.

# Протоколы IPSec

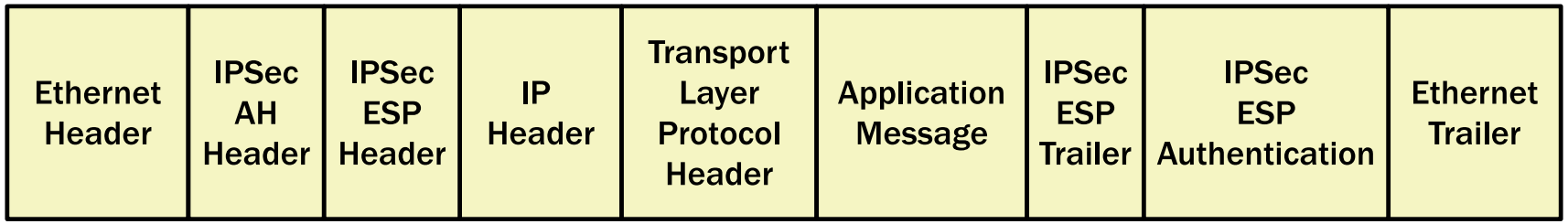
Стандарт IPSec определяет два протокола:

- IP Authentication Header (AH)
- IP Encapsulating Security Payload (ESP)

# Структура кадра
# IP AUTHENTICATION HEADERS (AH)



# Структура кадра
# IP ENCAPSULATING SECURITY PAYLOAD (ESP)

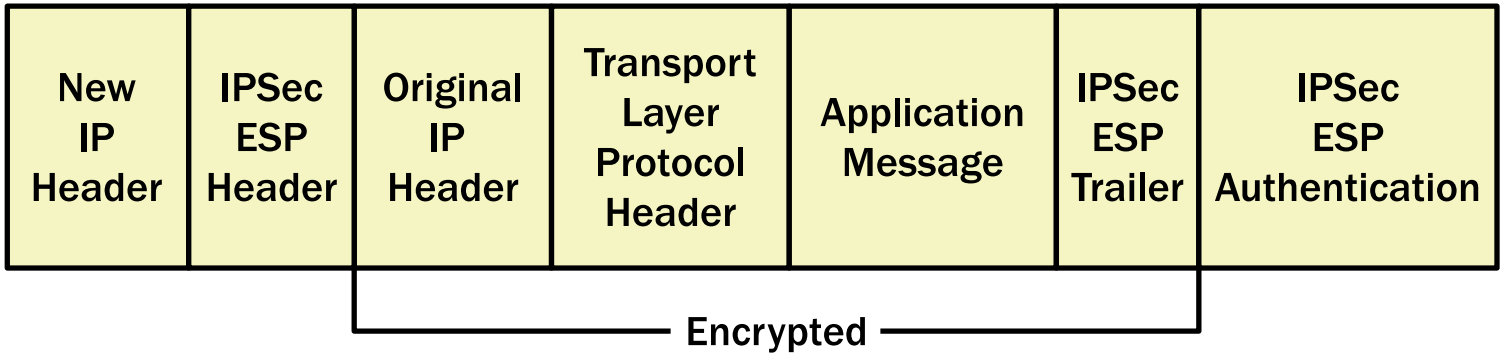


# Транспортный и туннельный режимы

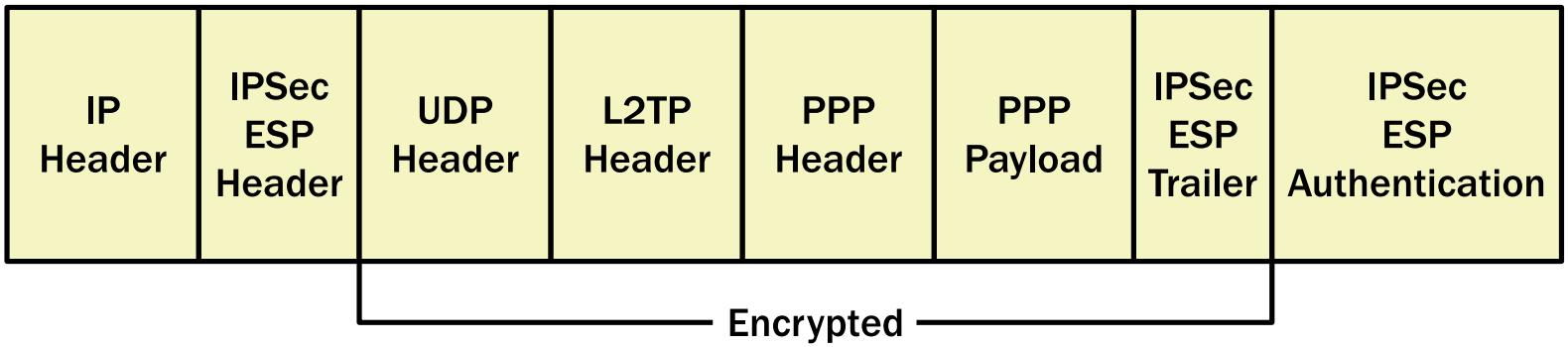
IPSec позволяет работать в двух режимах: транспортном и туннельном.

- **Транспортный режим** используется между компьютерами поддерживающими IPSec.
- **Туннельный режим** используется между маршрутизаторами поддерживающими IPSec.

# Структура пакета в туннельном режиме



# Туннель в протоколе L2TP



# Развертывание IPSec в сети

- Все версии Windows (с версии Windows 2000) поддерживают протоколы IPSec.
- **Политики IPSec** определяют когда и как используется IPSec.
- IPSec реализации в Windows Server совместимы с IPSec реализациями других операционных систем соответствующих стандартам IETF.

# Компоненты IPSec

IPSec в Windows Server включает следующие компоненты:

- Агент IPSec политик
- Internet Key Exchange (IKE)
- IPSec драйвер

# Планирование развертывание IPSec

- Использование IPSec создает дополнительный сетевой трафик и увеличивает нагрузку на процессор, связанную с обработкой трафика.
- IPSec реализации могут быть сконфигурированы для каждого сетевого соединения, используя пакетные фильтры.

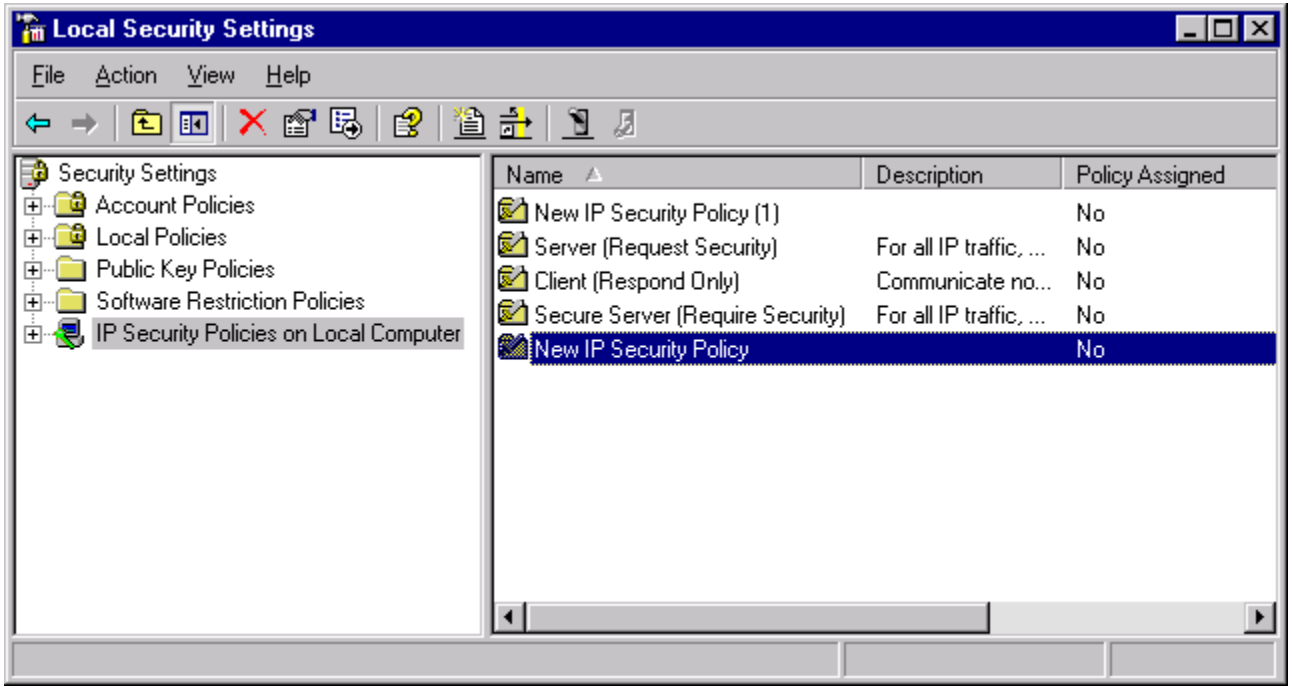
# Работа с политиками IPSec

IPSec политики управляются через оснастку MMC IP Security Policies.

IPSec политики определяют какой трафик должен быть защищен и какие действия выполняются с трафиком удовлетворяющим заданным критериям.

Три IPSec политики задаются по умолчанию.

# Использование политик IPSec по умолчанию



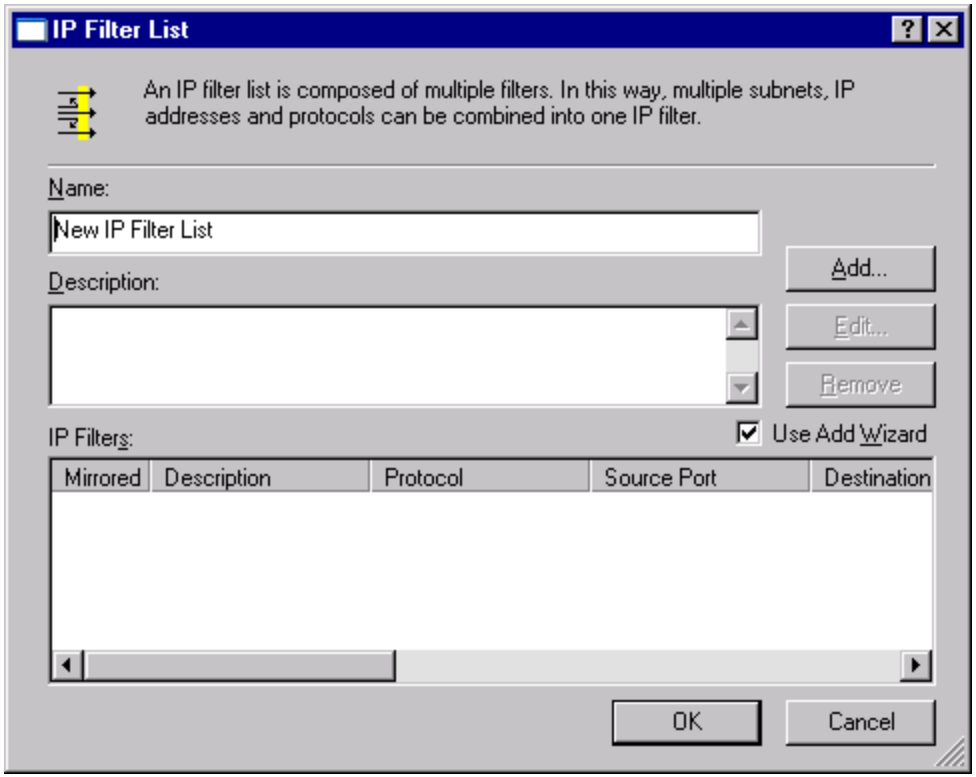
# Содержание политики IPSec

Политики IPSec включают в себя три элемента:

- Правила
- Списки фильтров IP
- Действия фильтров

# Создание правил IPSec

# Создание списка IP фильтров



# Создание Действия фильтров

- Действия фильтров позволяют администраторам определять, что выполняется если трафик удовлетворяет выбранному списку фильтров.
- Действия фильтров доступные по умолчанию:
  - Разрешить
  - Блокировать
  - Согласовать безопасные

# Основное содержание лекции

- Фильтрация пакетов – метод для регулирования TCP/IP трафика, основанный на таких параметрах как IP и физический адрес, протокол и номер порта.
- Сервис - ориентированные фильтры используют номер порта позволяют ограничить трафик связанный с работой приложения.

# Основное содержание лекции

- IPSec – это набор Интернет протоколов обеспечивающих защиту данных во время их передачи в сети.
- IP Authentication Header протокол обеспечивает аутентификацию и целостность данных, но не шифрование.

# Основное содержание лекции

- IP Encapsulating Security Payload протокол шифрует данные в IP датаграммах и обеспечивает аутентификацию и целостность данных.
- IPSec может оперировать в двух режимах: транспортный режим защиты соединений между пользовательскими приложениями и туннельный режим защиты WAN соединений между маршрутизаторами.
- Реализации IPSec Windows Server включают агента политик IPSec, Internet Key Exchange (IKE) и драйверы IPSec.

# Основное содержание лекции

- IPSec в Windows Server по умолчанию имеет три политики: Client (Respond Only), Secure Server (Require Security), and Server (Request Security).
- IPSec политики включают правила, список IP фильтров и действия фильтров.
- Правила являются комбинацией действий IP filter фильтров и списков фильтров.