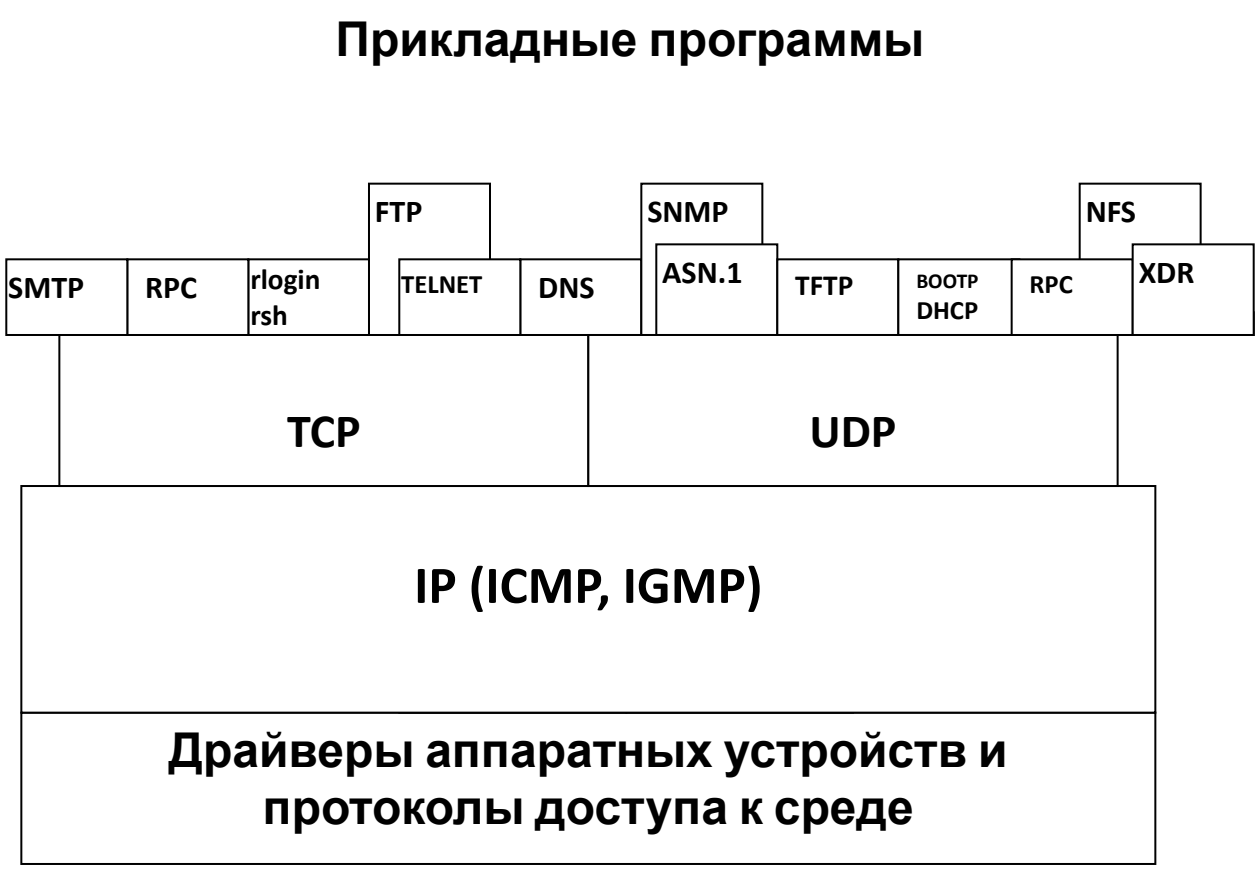
Безопасность транспортного уровня

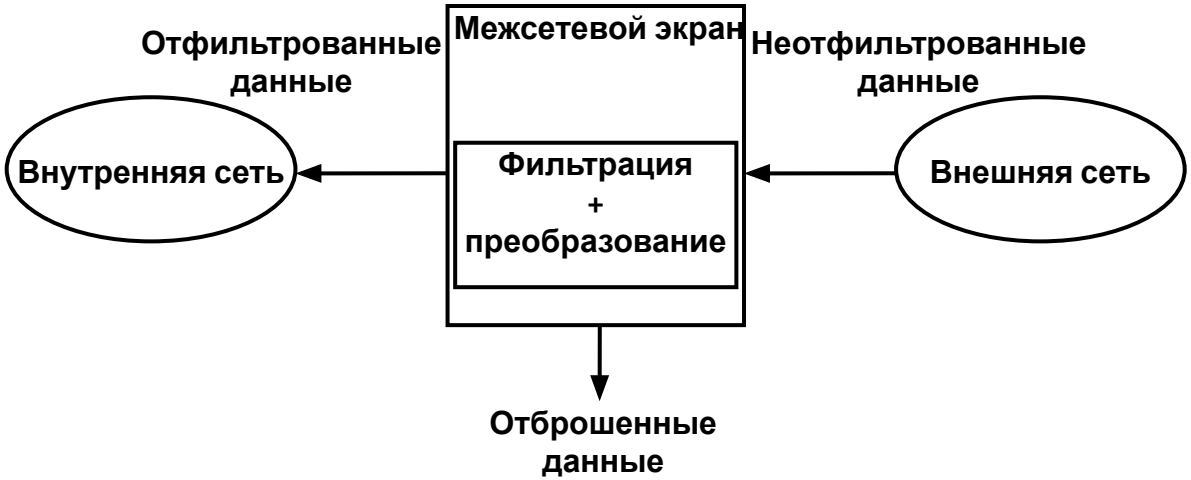
Стек протоколов TCP/IP



Экранирование

Межсетевые экраны:

- экранирующие концентраторы (мосты, коммутаторы) – уровень 2;
- экранирующие маршрутизаторы – уровень 3;
- **транспортное экранирование – уровень 4;**
- **прикладные (прокси) экраны – уровень 7.**



NAT – Network Address Translator

TRANSPORT LAYER SECURITY

История

- Secure Sockets Layer – внутренняя разработка Netscape, 1994 г.
- SSL v 2.0 – Опубликована Netscape в 1995 г.
  - Запрещена для использования в Интернете, 2011
- SSL v 3.0 – Опубликована Netscape в 1999 г.
  - Послужила основой для TLS, не рекомендована для использования
- TLS 1.0 – RFC 2246, 1999 г.
- TLS 1.1 – RFC 4346, 2006 г.
- TLS 1.2 – RFC 5246, 2008 г.

Задачи TLS

- Криптографическая безопасность: обеспечение безопасного соединения между двумя сторонами.
- Совместимость: реализации могут обмениваться параметрами криптографических алгоритмов без знания особенностей реализации друг друга.
- Расширяемость: TLS предоставляет средства для добавления новых методов симметричного и асимметричного шифрования
  - избежать «изобретения велосипеда» – создания новых протоколов защиты с новыми уязвимостями;
  - избежать создания новых библиотек функций защиты.
- Эффективность:
  - кэширование сессий для уменьшения числа вычислительно-сложных операций, таких как операции с открытыми ключами.;
  - снижение объемов трафика.

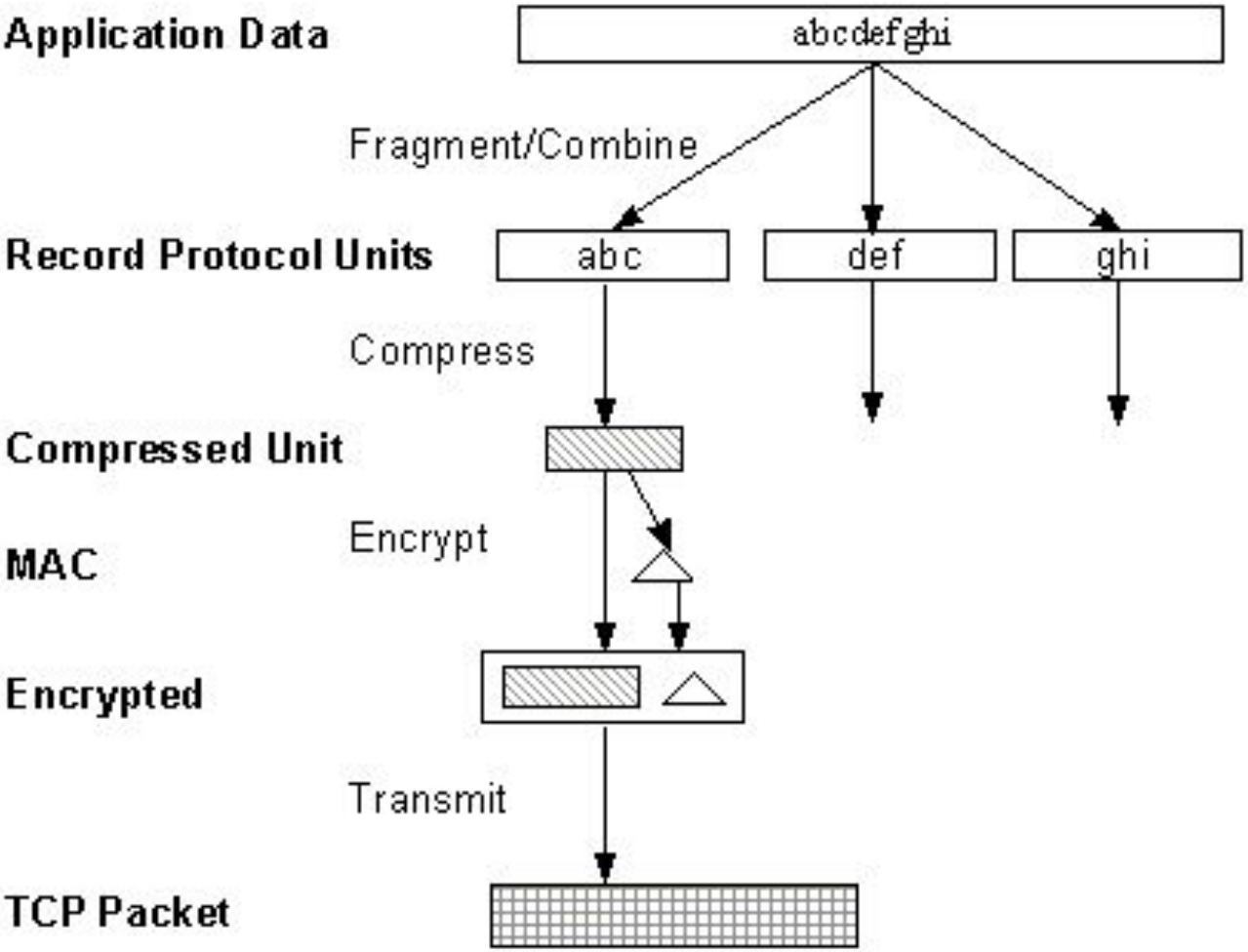
Двухуровневая архитектура TLS

- Протокол записей TLS
  - TLS Records
- Прикладные протоколы TLS
  - Протокол установления соединения (Handshaking)
  - Протокол изменения криптографических параметров (change cipher spec)
  - Протокол оповещений (alert)
  - Протокол прикладных данных

Протокол записей TLS

- Фрагментация
  - Деление потока данных на фрагменты
  - Размер фрагмента не более 16 кбайт
  - Границы сообщений прикладных протоколов не соблюдаются
- Сжатие
  - Стандарт определяет использование DEFLATE (gzip)
- Аутентификация (MAC)
  - MD5, SHA 1, SHA 256/384/512
- Шифрование
  - RC4, 3DES, AES
- Транспорт
  - TCP

Протокол записей TLS



Состояние TLS

- Два набора состояний: текущее и следующее (pending)
- Каждый набор состояний: состояние чтения + состояние записи
- Состояние:
  - Состояние сжатия
  - Состояние шифрования
  - Ключ цифровой подписи (MAC)
  - Номер последовательности
- Начальное состояние: сжатие отсутствует, шифрование отсутствует, без подписи, 0
- Смена текущего состояния на следующее по получению сообщения change cipher spec (1 байт)
- Алгоритм установления соединение конфигурирует **следующее** состояние

Установление соединения

Клиент

- ClientHello

Сервер

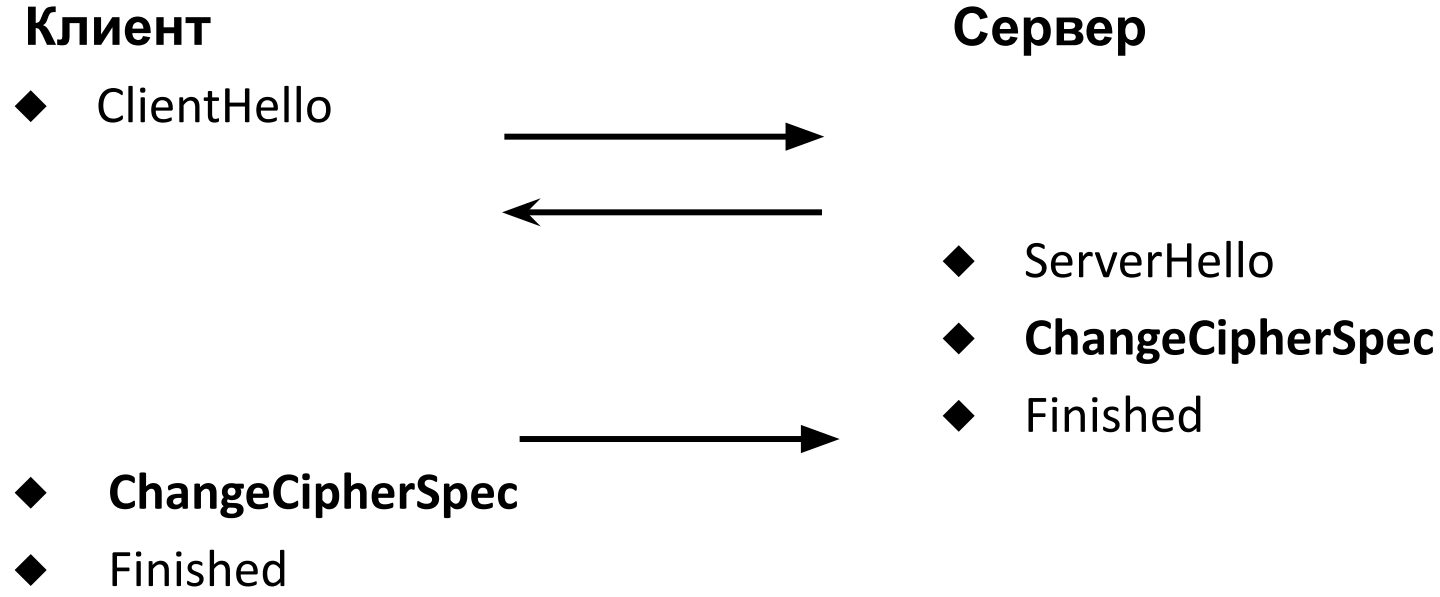
- ServerHello
- *Server Certificate*
- *ServerKeyExchange*
- *CertificateRequest*
- SerververHelloDone

- *Client Certificate*

- ClientKeyExchange
- *CertificateVerify*
- **ChangeCipherSpec**
- Finished

- **ChangeCipherSpec**
- Finished

Возобновление соединения



- Идентификатор сессии в ClientHello != 0
- Идентификатор сессии сохранен в кэше сессий сервера

Протокол оповещений

- Уровень оповещения:
  - Предупреждения (warning)
  - Аварийные (fatal)
- Назначение оповещения
  - Закрытие – отправитель более не будет посылать сообщения
  - Ошибки (не все ошибки аварийные)

Передача прикладных данных

- Прикладные данные сжимаются и шифруются в соответствии с текущим состоянием протокола записей TLS
- Прикладные данные рассматриваются как бинарные последовательности, их семантика или структура не учитываются TLS

Приложения TLS

- HTTPS – HTTP поверх TLS
- SMTP, IMAP, POP – поддерживают режим работы поверх TLS