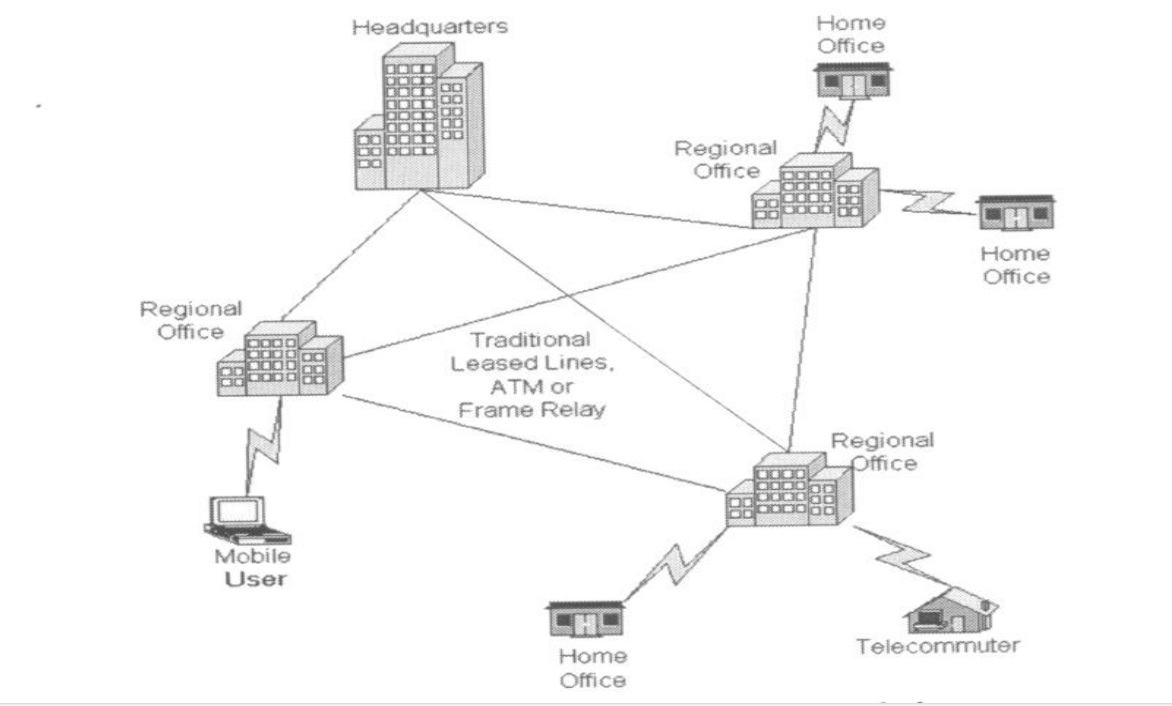
Современные криптографические протоколы

VPN – виртуальные частные сети

История

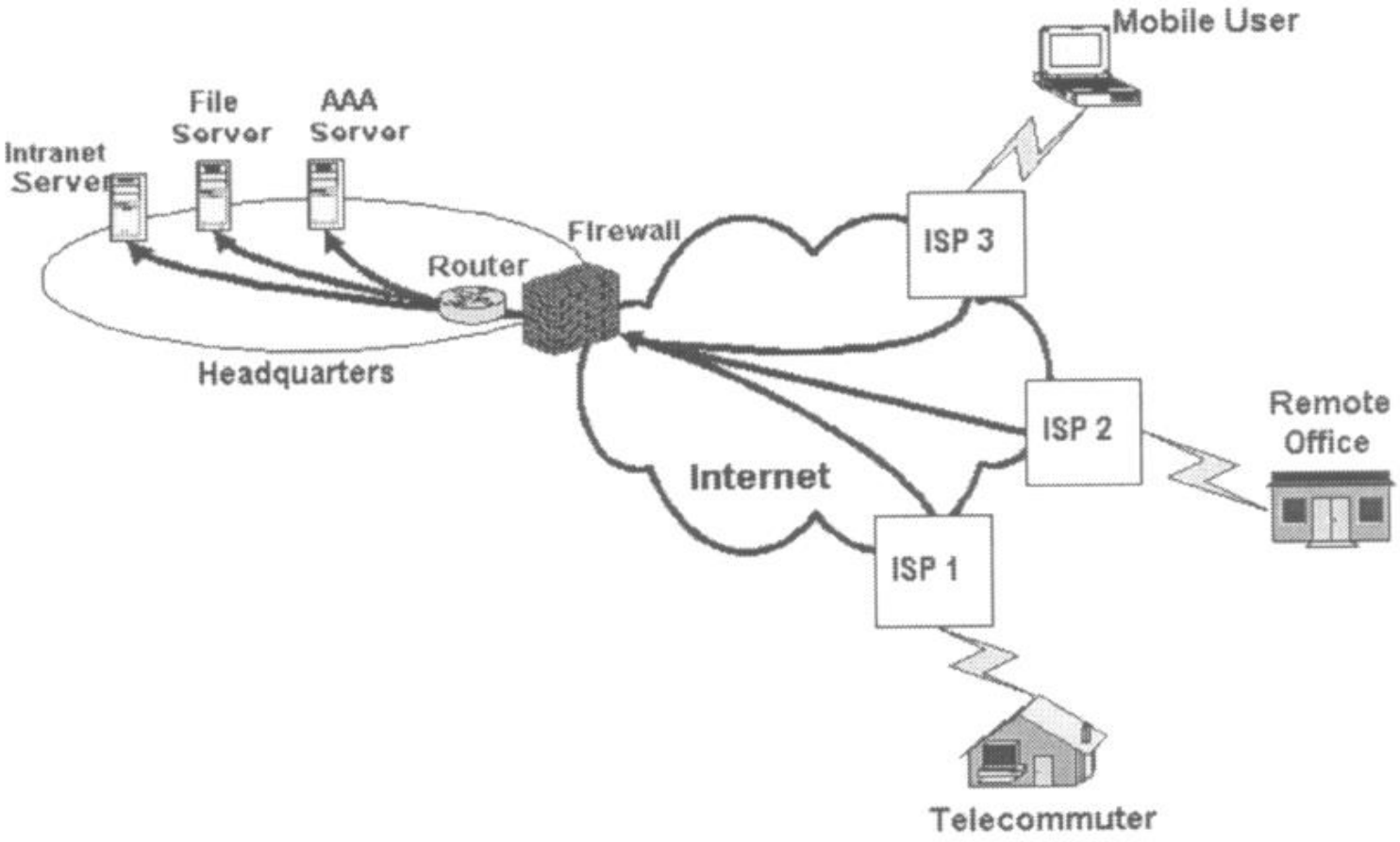
- Частные сети – понятие из «телефонной» эры



Виртуальные частные сети

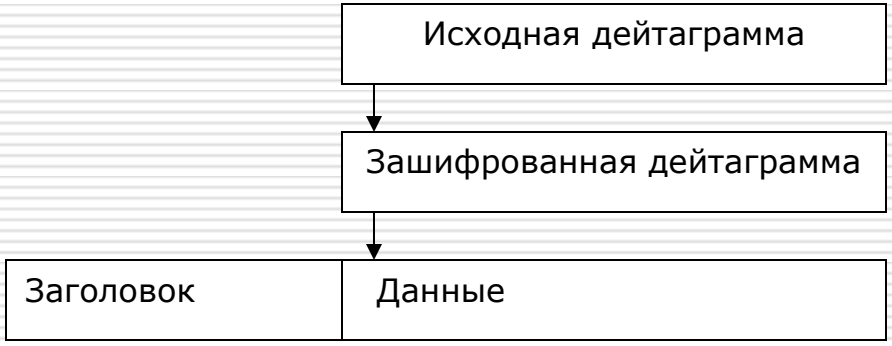
- Типичное определение – частная сеть, которая использует публичные телекоммуникационные сети вместо выделенных линий
- Возможность удалённого доступа
- Шифрование
- Существенно дешевле частной сети в полном смысле этого термина

Виртуальные частные сети



Тунеллирование

- P2P соединение через публичную сеть используется для передачи инкапсулированных дейтаграмм:

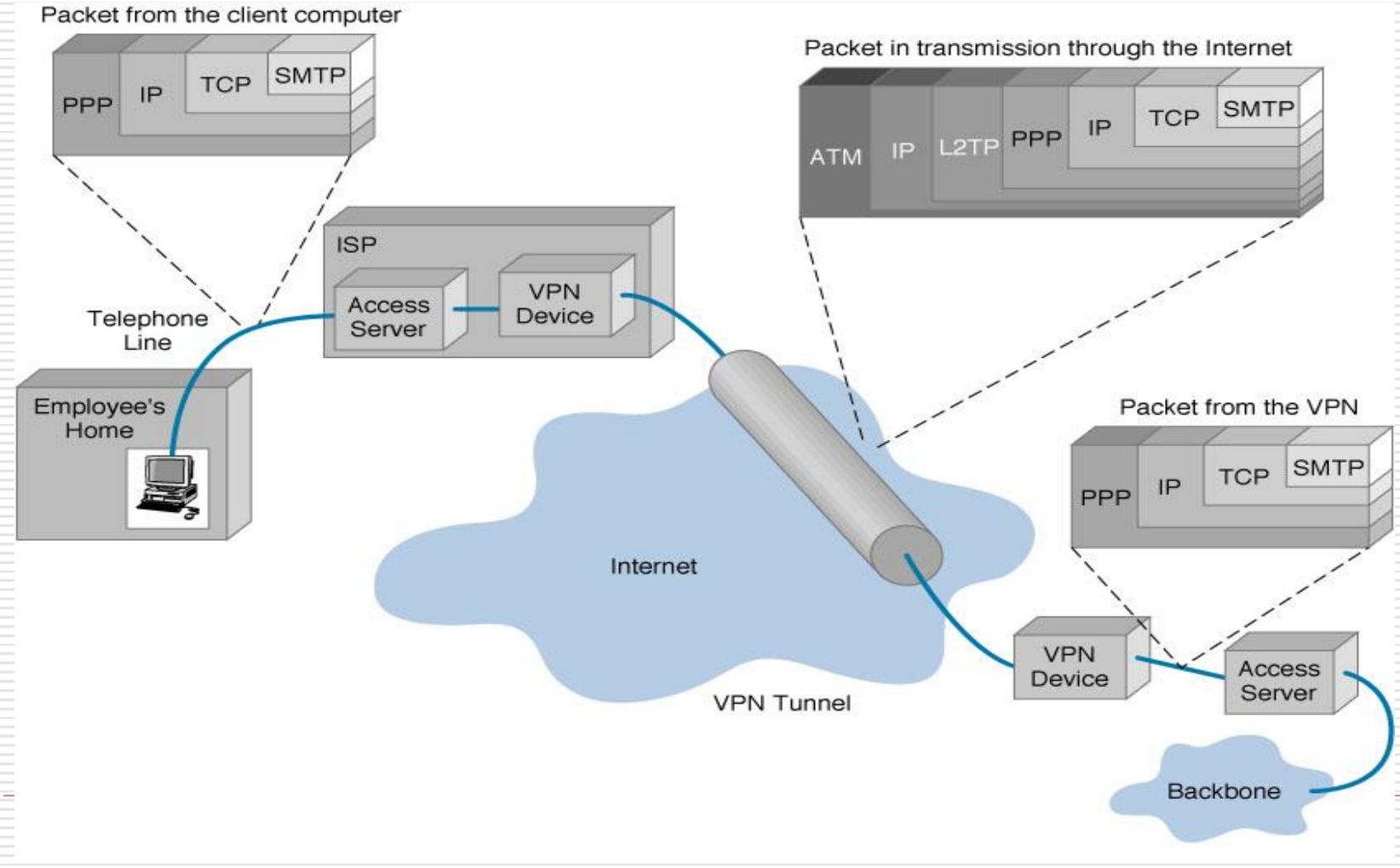


Инкапсуляция данных в VPN

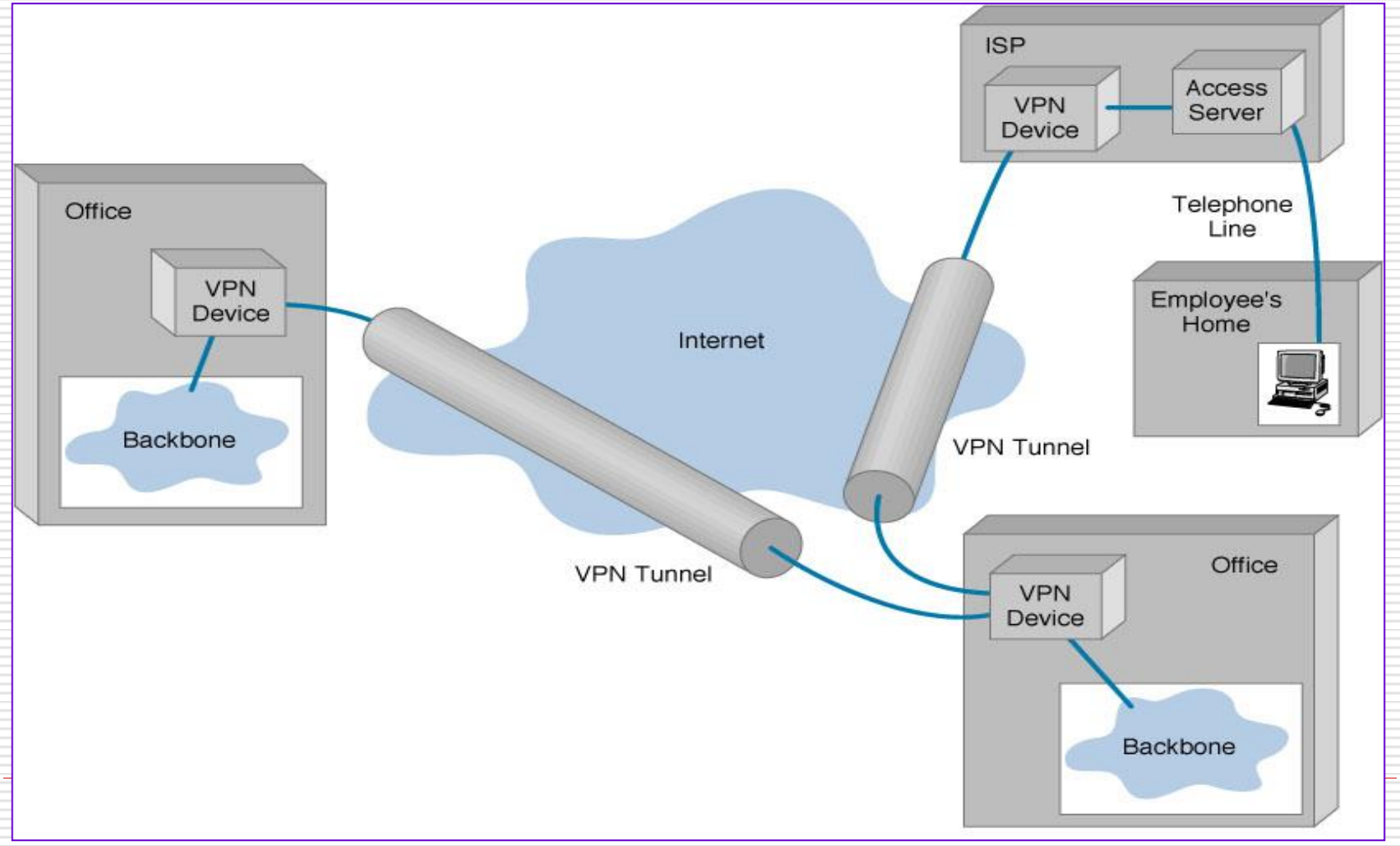
Типы подключений:

- Удалённый доступ (Remote Access)
- Равноправное подключение (Site-to-Site)

Инкапсуляция



Типы подключений



Популярные протоколы

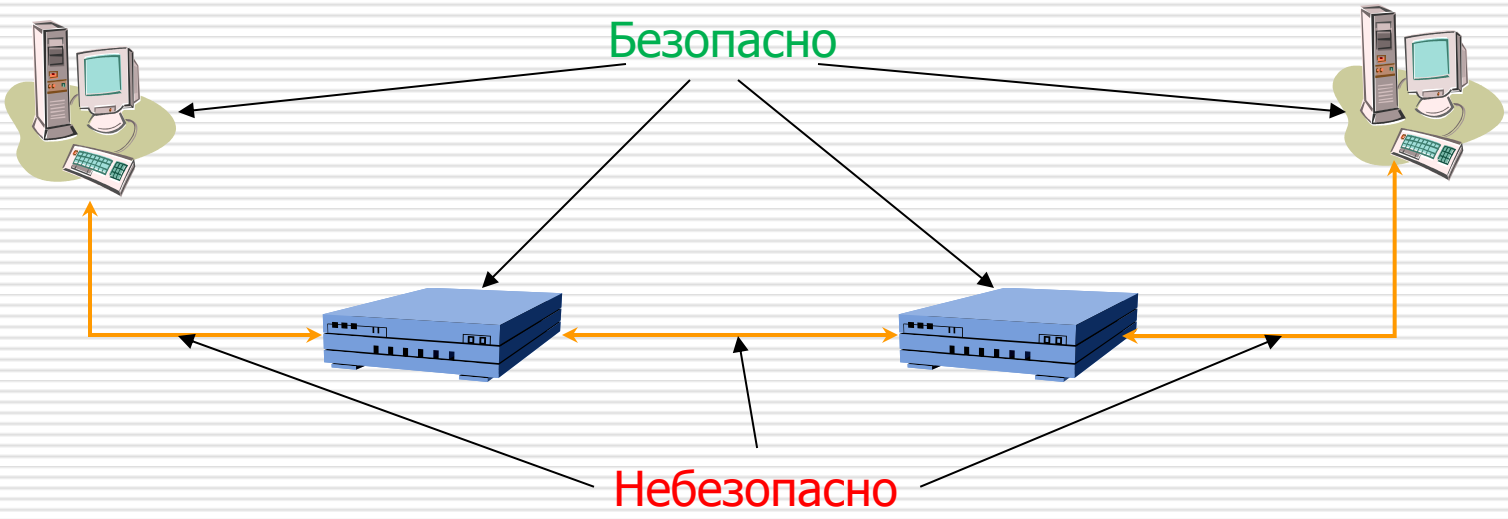
- PPTP - Point-to-Point Tunneling Protocol
- L2TP - Layer 2 Tunneling Protocol
- IPsec - Internet Protocol Security
- OpenVPN – “userspace VPN”

Протокол IPSec

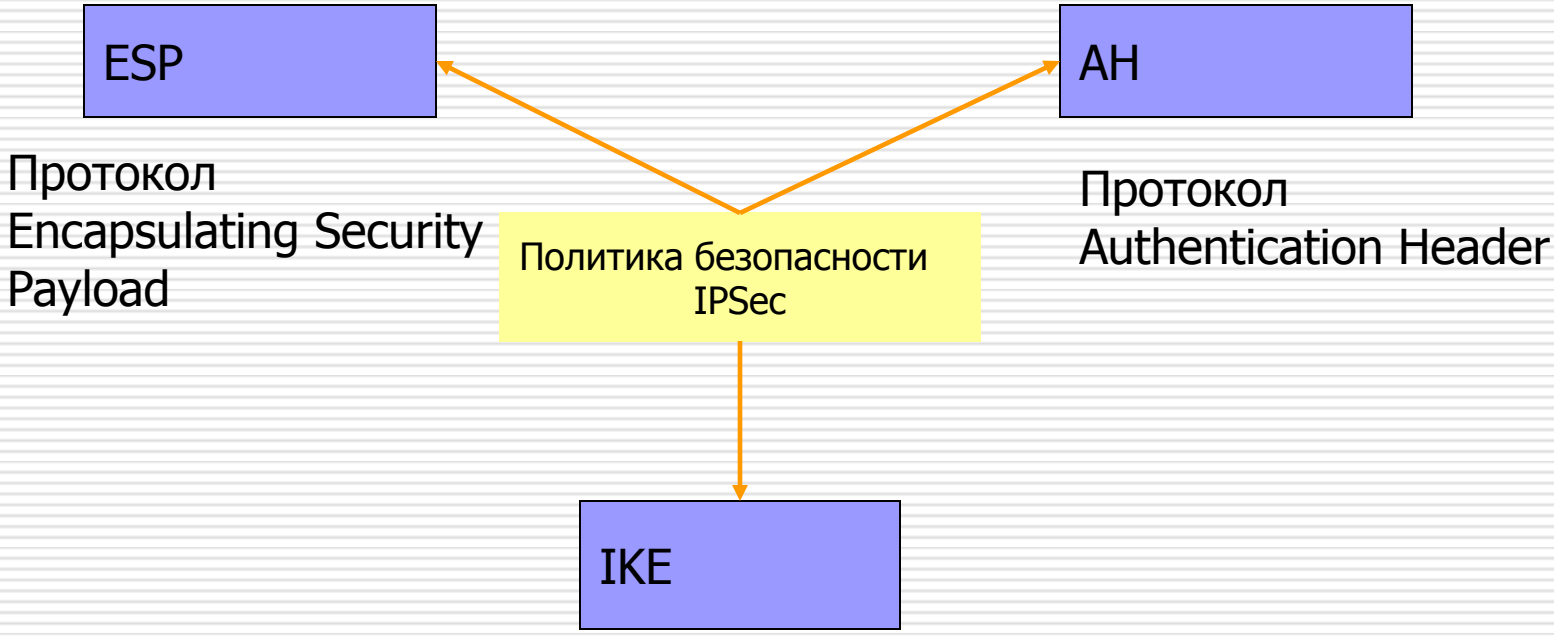
Задачи IPSec

- Удостоверение источника IP пакетов
  - *аутентификация*
- Предотвращение «проигрывания» старых пакетов (дубликатов)
- Обеспечение целостности и конфиденциальности данных
  - *контроль целостности и шифрование*

Модель угроз IPSec



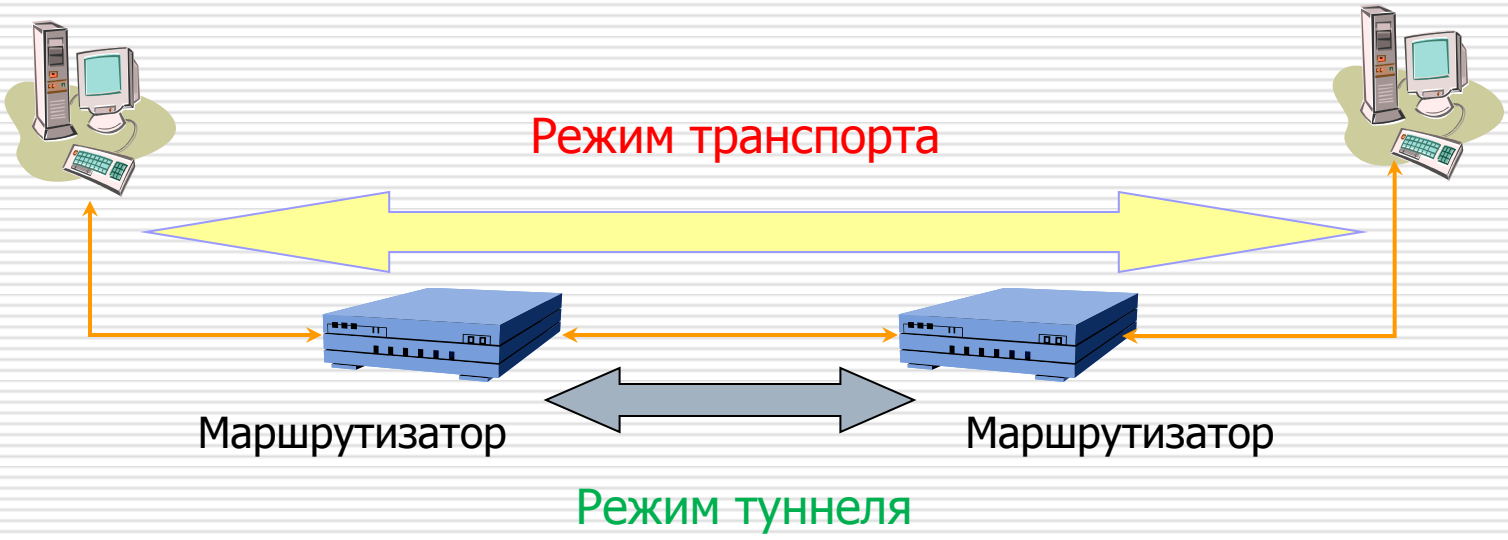
Архитектура IPSec



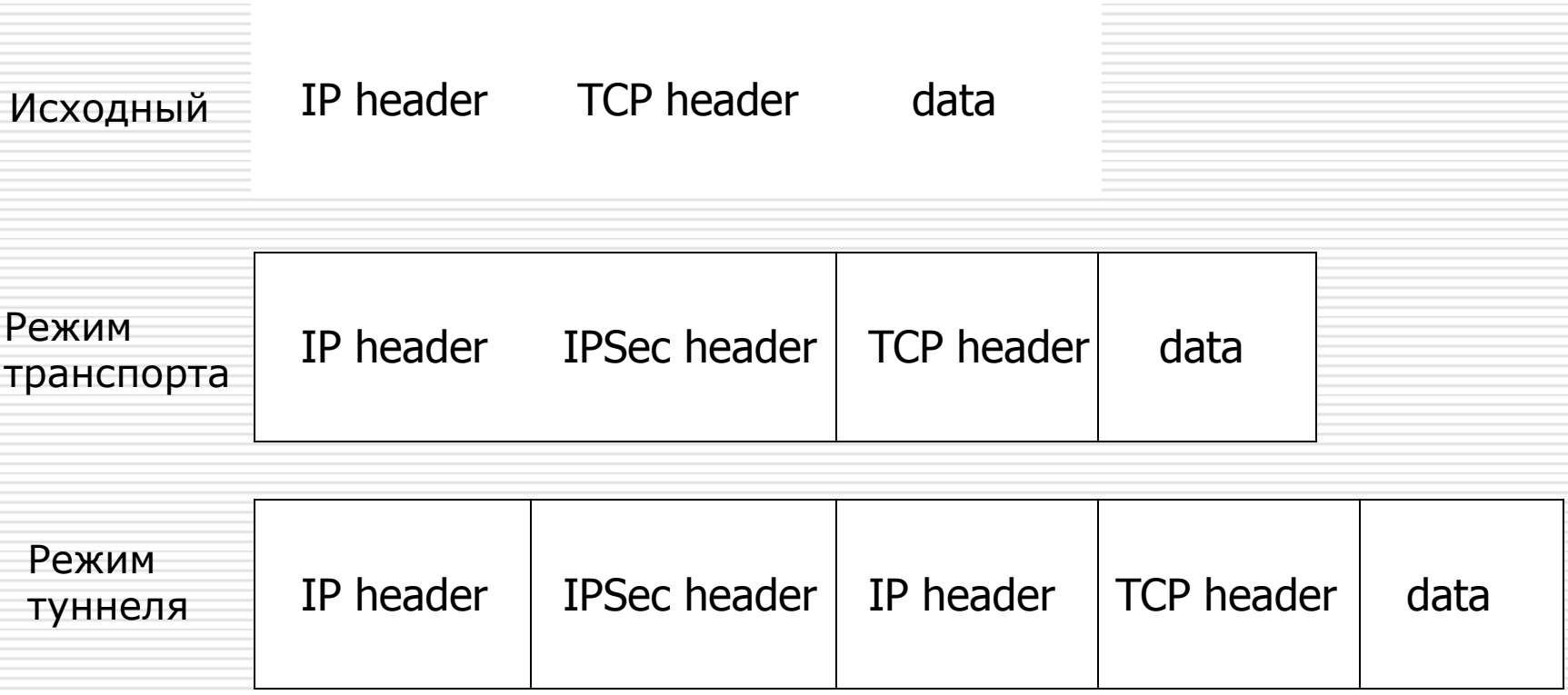
Архитектура IPSec

- Протокол IPSec предназначен для защиты канала в трёх разных ситуациях:
  - Узел-узел, узел-маршрутизатор и маршрутизатор-маршрутизатор
- IPSec работает в двух режимах:
  - *Режим транспорта* (для P2P)
  - *Режим туннеля* (для VPN)

Архитектура IPsec



Виды пакетов



IPSec

- Набор протоколов (RFC 2401)
  - Authentication Header (AH)
    - RFC 2402
  - Encapsulating Security Payload (ESP)
    - RFC 2406
  - Internet Key Exchange (IKE)
    - RFC 2409
  - IP Payload Compression (IPcomp)
    - RFC 3137

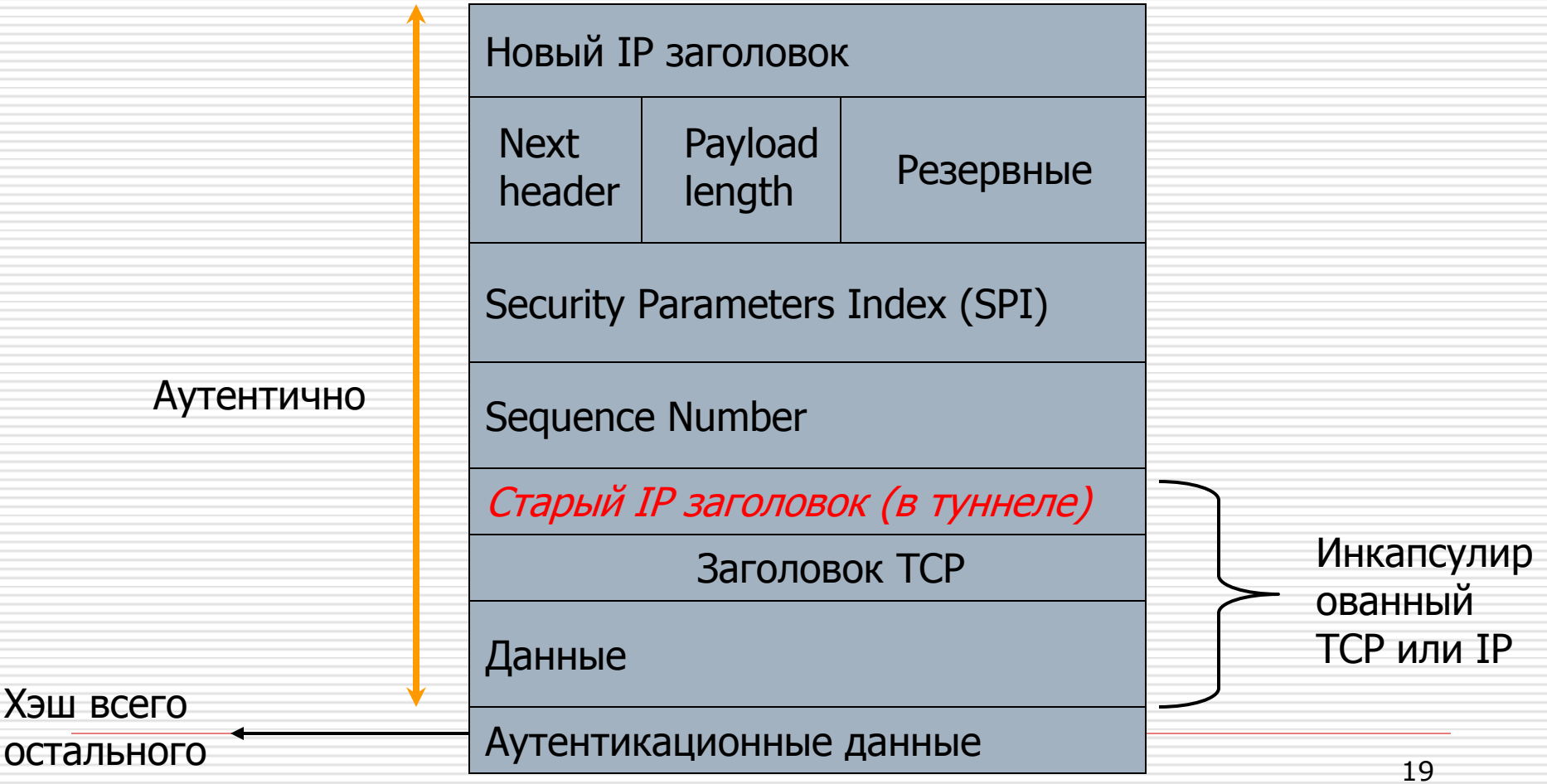
Аутентификационный заголовок - Authentication Header (AH)

- Предназначен для аутентификации источника
  - Предотвращает спуфинг
- Обеспечивает целостность
- Защищает от атак воспроизведения (replay)
  - Использует монотонно возрастающие счетчики последовательности
  - Защищает от атак на отказ в обслуживании
- НЕ обеспечивает конфиденциальность

Детали AH

- Использует 32-битный счетчик последовательности для защиты от атак воспроизведения
- Использует «сильные» хэши для защиты целостности (96-bit)
  - Симметричный шифр
  - HMAC-SHA-96, HMAC-MD5-96

Структура пакета AH



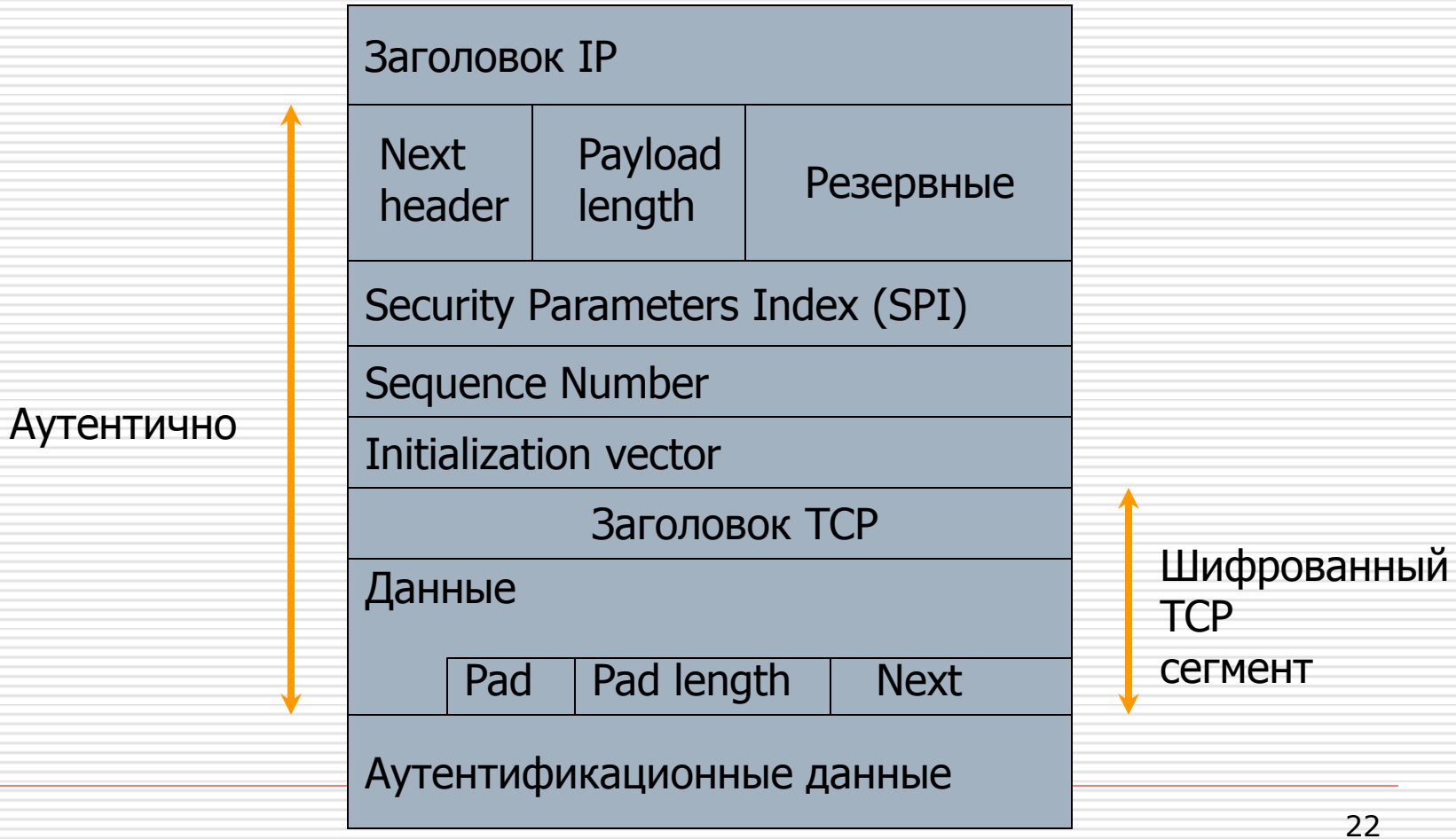
Шифрование данных – Encapsulating Security Payload (ESP)

- Предоставляет всё, что AH
- Дополнительно обеспечивает конфиденциальность данных
  - Использует симметричное шифрование

Детали ESP

- Как и AH:
  - Использует 32-битный счетчик последовательности для защиты от атак воспроизведения
  - Использует алгоритмы проверки целостности
- Только ESP:
  - Конфиденциальность:
    - Использует симметричный шифр для шифрования данных

Пакет ESP


Заголовок IP
Next header
Payload length
Резервные
Security Parameters Index (SPI)
Sequence Number
Initialization vector
Заголовок TCP
Данные
Pad
Pad length
Next
Аутентификационные данные
Аутентично
Шифрованный TCP сегмент

Зачем?

1. Зачем одновременно AH и ESP?
2. И AH, и ESP используют симметричные алгоритмы
   - Почему не на открытых ключах?
   - Как происходит обмен ключами?
   - Какие алгоритмы надо выбирать?
   - Похоже на согласование наборов криптопримитивов в SSL

Протокол обмена ключами - Internet Key Exchange (IKE)

- Обмен и согласование политик безопасности
- Установление сессий безопасности
  - Называются *Security Associations*
- Обмен ключами
- Управление ключами
- Можно использовать не только в IPsec

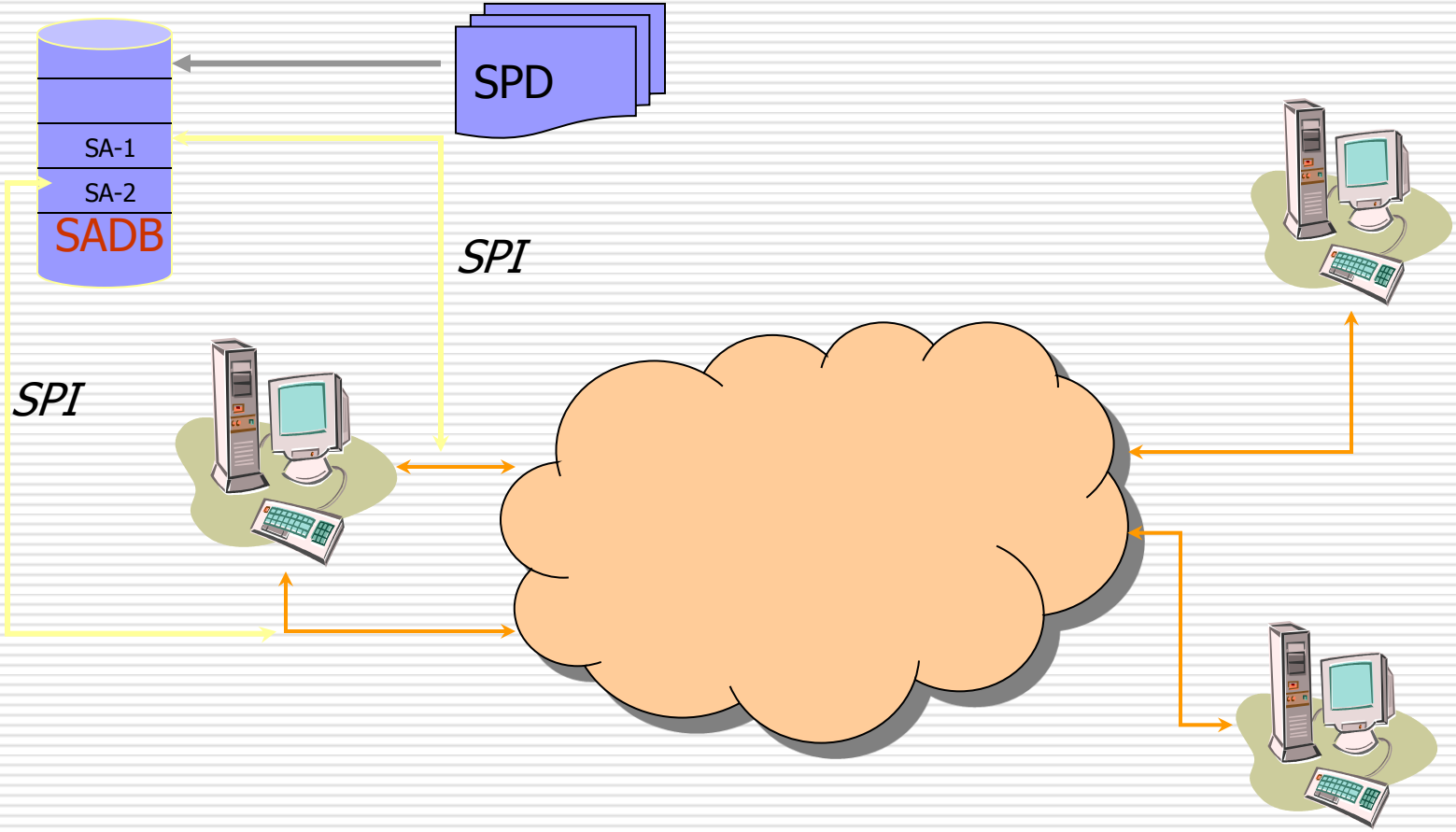
Аббревиатурки IPsec/IKE

- Security Association (SA)
  - Набор атрибутов соединения
  - Набор *асимметричен!*
    - Отдельный SA для входящего трафика, другой SA для исходящего трафика
    - Похоже на набор примитивов в SSL
- Security Association Database (SADB)
  - База таких SA

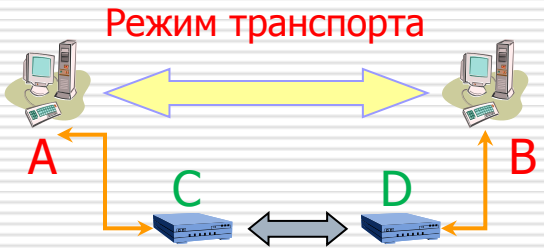
Аббревиатурки IPsec/IKE 2.0

- Security Parameter Index (SPI)
  - Уникальный индекс каждой записи в SADB
  - Обозначает ассоциированную с текущим пакетом SA
- Security Policy Database (SPD)
  - Хранение политик для установки SA

Что с чем связано



Пример SPD и SADB



A: SADB

A: SPD

From	To	Protocol	Port	Policy
A	B	Any	Any	AH[HMAC-MD5]

From	To	Protocol	SPI	SA Record
A	B	AH	12	HMAC-MD5 key

From	To	Protocol	Port	Policy	Tunnel Dest
A_{sub}	B_{sub}	Any	Any	ESP[3DES]	D

C: SPD

From	To	Protocol	SPI	SA Record
A_{sub}	B_{sub}	ESP	14	3DES key

C: SADB

Как это работает

- IKE состоит из двух фаз
  - Фаза 1: установление вспомогательного безопасного соединения из конца в конец
    - Используется также внутри фазы 2
    - Устанавливается только между двумя точками
  - Фаза 2: установление специальных безопасных соединений
    - Происходит много раз
  - Обе фазы используют алгоритм Диффи-Хеллмана выработки общего ключа

IKE Фаза 1

- Цель: установление безопасного соединения между двумя оконечными узлами
  - Этот канал обеспечивает базовые свойства безопасности:
    - Аутентификация источника
    - Конфиденциальность и целостность данных
    - Защита от атак воспроизведения

IKE фаза 1

- Смысл: у каждого приложения свои требования к безопасности
- Но им всем надо согласовывать политики и обмениваться ключами
- Поэтому тут предоставляются базовые примитивы для согласования защищенных сессий между приложениями

Примеры

- Все пакеты, отправляемые на сайт mybank.ru, должны быть зашифрованы с использованием 3DES и HMAC-MD5
- Все пакеты, отправляемые на www.antichat.ru, должны защищаться HMAC-SHA1 (но без шифрования)

Обмен в фазе 1

- Два режима:
  - Главный режим
    - Шесть сообщений в три цикла обмена
    - Больше опций
  - Быстрый режим
    - Четыре сообщения в два цикла обмена
    - Меньше опций

Фаза 1 (Главный режим)

Инициатор

Приёмник

[Header, SA_1]

Фаза 1 (Главный режим)

Инициатор

Приёмник

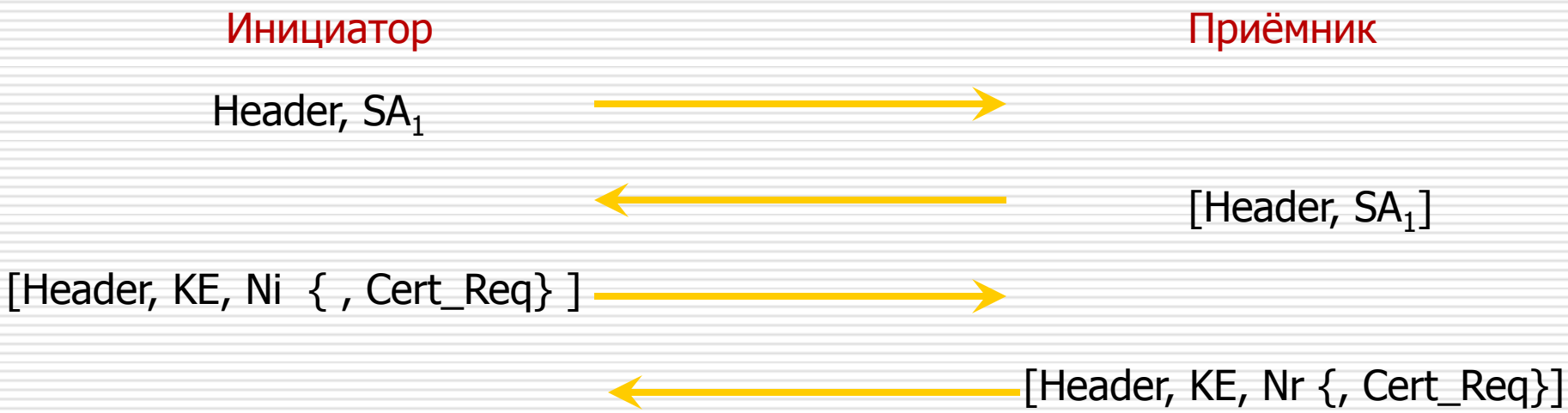
[Header, SA_1]

[Header, SA_2]

Согласование «алфавита»

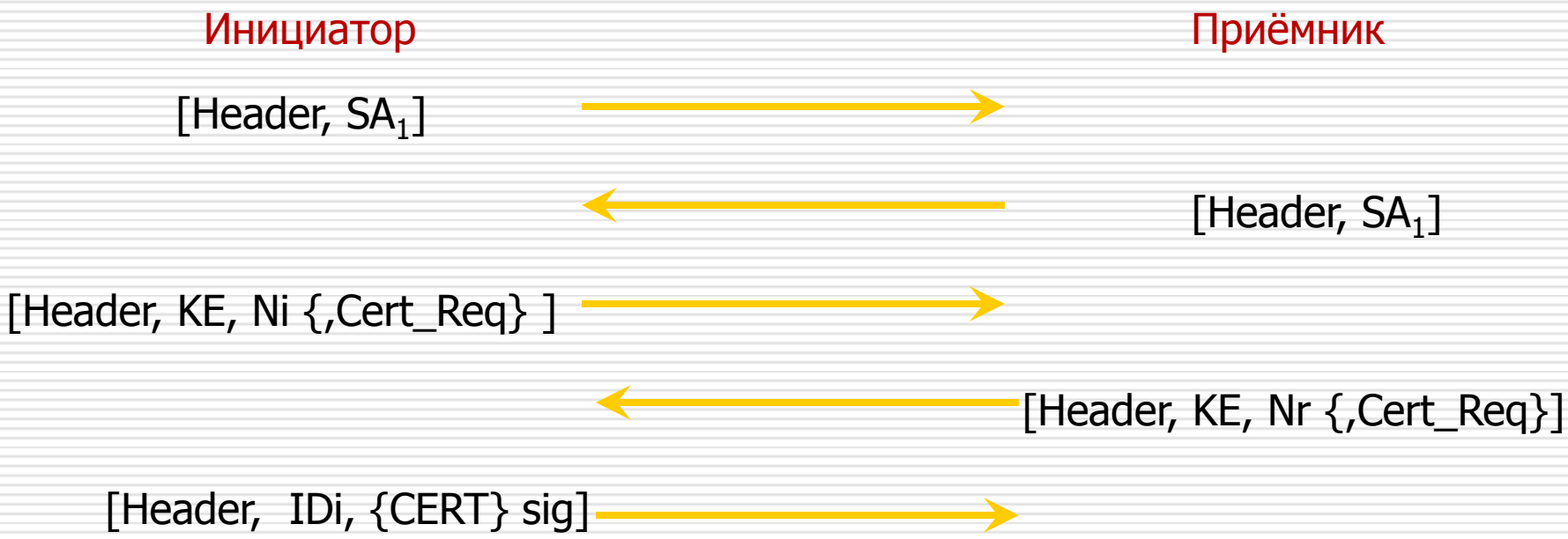
Фаза 1 (Главный режим)

Фаза 1 (Главный режим)

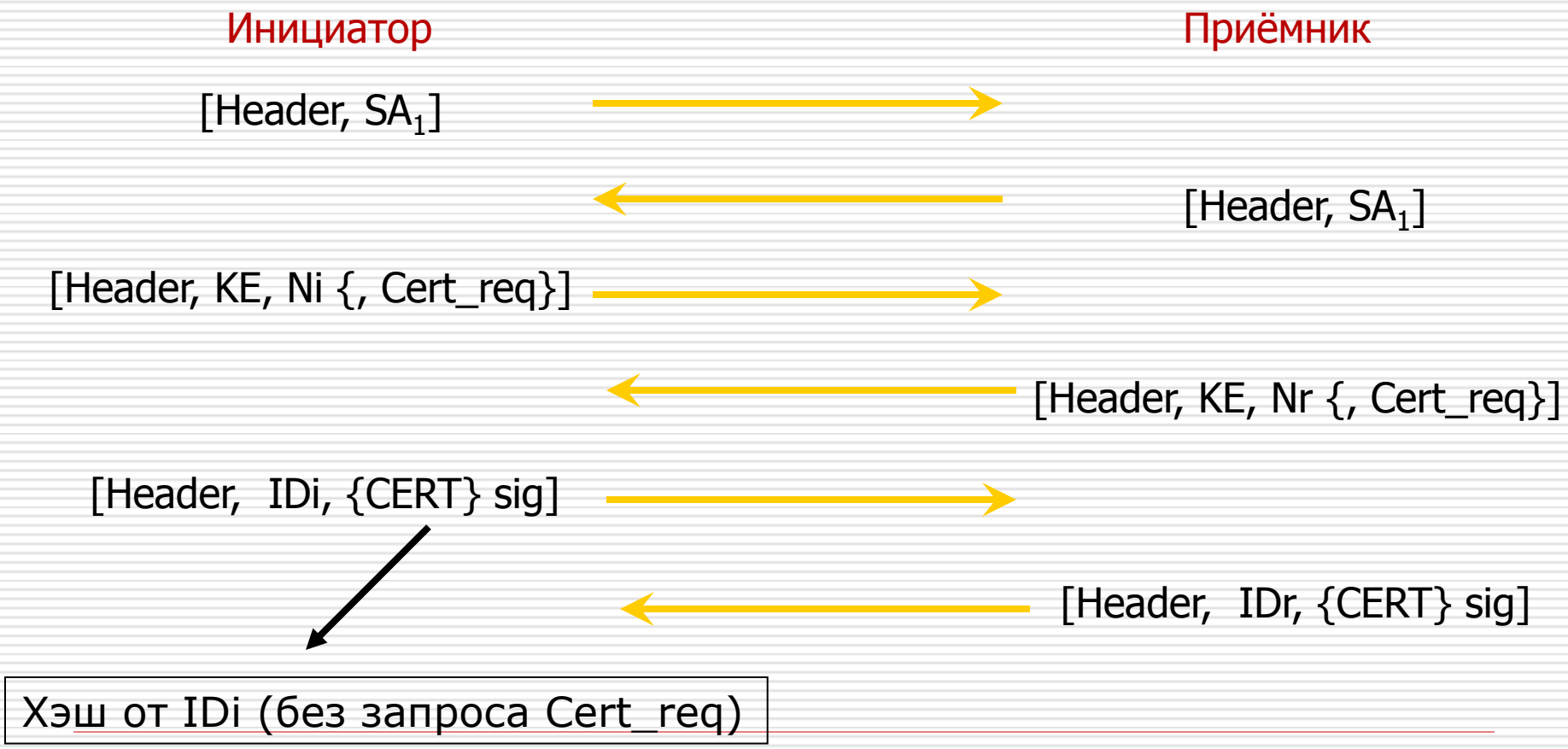


Согласование общего секрета с помощью Диффи-Хеллмана
Использование nonces для предотвращения атак воспроизведения

Фаза 1 (Главный режим)



Фаза 1 (Главный режим)



Фаза 1 (Быстрый режим)

Инициатор

Приёмник

[Header, SA_1, KE, Ni, IDi]

Фаза 1 (Быстрый режим)

Первые два сообщения объединяются в одно (объединение Hello и выработки секрета по DH)

IPSec (Фаза 1)

- Четыре способа аутентификации
  - Цифровая подпись
  - Два варианта с публичными ключами
  - Pre-shared key
- Замечание: IKE использует ассиметричные шифры для шифрования

IPSec (Фаза 2)

- Цель: установление специальных безопасных каналов между двумя точками
  - Точки идентифицируются парами <IP, port>:
    - т.е. <www.mybank.ru, 8000>
  - или пакетами:
    - т.е. все пакеты на 128.124.100.0/24
  - Использует для взаимодействия канал, установленный на фазе 1

IPSec (фаза 2)

- Единственный режим: быстрый режим
- Несколько обменов в быстром режиме можно объединять в один
- Генерация SA для оконечных точек
- Может использовать для взаимодействия канал, установленный на фазе 1

Протокол сжатия IP

- Предназначен для... сжатия
- Можно задать как часть политики IPSec

Политики IPsec

- Политки фазы 1 определяются в терминах *наборов защиты*
- Каждый набор...
  - Должен содержать:
    - Алгоритм шифрования
    - Алгоритм хэширования
    - Метод аутентификации
    - Группу для алгоритма Диффи-Хеллмана
  - Опционально содержит:
    - Время жизни
    - …

Политики IPSec

- Политики фазы 2 описываются в терминах *предложений*
- Каждое предложение:
  - Может содержать одно из -
    - AH предложения
    - ESP предложения
    - IPComp предложения
    - А также необходимые атрибуты, такие как
      - Длина ключа, время жизни, и т.д.

Пример политики IPSec

- По-русски:
  - Весь трафик на 128.104.120.0/24 должен:
    - Использовать pre-shared ключ
    - Группа DH это MODP (http://tools.ietf.org/html/rfc3526) с 1024-битным модулем
    - HMAC это HMAC-SHA (128 битный ключ)
    - Шифровать 3DES
- В терминах IPSec:
  - [Auth=Pre-Hash;
    DH=MODP(1024-bit);
    HASH=HMAC-SHA;
    ENC=3DES]

Пример политики IPsec

- По-русски:
  - Весь трафик на 128.104.120.0/24 должен:
    - Использовать AH с HMAC-SHA или ESP с 3DES для шифрования
    - HMAC-MD5 или HMAC-SHA для аутентификации сообщений
- В терминах IPsec:
  - [AH: HMAC-SHA] or,
  - [ESP: (3DES and HMAC-MD5) or (3DES and HMAC-SHA)]

Обсуждение

- IPSec далеко не единственный вариант
  - Безопасность может быть надстройкой над IP
    - T.e. SSL/TLS, Kerberos…
- Сложность
  - Протоколы IPSec очень сложны!
    - Два режима, три подпротокола
  - Сложность – враг безопасности

Обсуждение

- Он используется
  - Да — прежде всего некоторыми вендорами VPN решений
    - Но не все маршрутизаторы его поддерживают
  - Но нет — на самом деле это не очевидное для использования между двумя точками решение
    - Слишком простая аутентификация (аутентифицируются узлы)
    - Алгоритм шифрования по-умолчанию слишком слабый (DES)
    - Слишком сложен для использования приложениями

Материалы по IPSec

- IP, IPsec and related RFCs:
  - http://www.ietf.org/html.charters/ipsec-charter.html
  - IPsec: RFC 2401, IKE: RFC 2409
  - www.freeswan.org
- Google ☺

OpenVPN

- https://openvpn.net/index.php/open-source/documentation/security-overview.html
- Инкапсулирует в UDP или TCP
- Два вида виртуальных сетевых устройств в Linux – tun, tap
- Использует SSL/TLS для взаимной аутентификации участников
- Формат пакета:
  - HMAC(explicit IV, encrypted envelope)
  - Explicit IV
  - Encrypted Envelope

Задание

- Настроить OpenVPN сервер в двух вариантах – tun, tap
  - Клиентские сертификаты – с помощью easy-rsa
- Прочитать описание протокола PPTP и разобрать атаку на MS-CHAP v2
  - А также возможности cloudcracker по взлому сессий PPTP
  - DEFCON 20 Talk by Moxie Marlinspike: http://www.youtube.com/watch?v=sIidzPntdCM

(Defeating PPTP VPNs and WPA2 Enterprise with MS-CHAPv2)