Основы построения VPN

Виртуальные частные сети - VPN

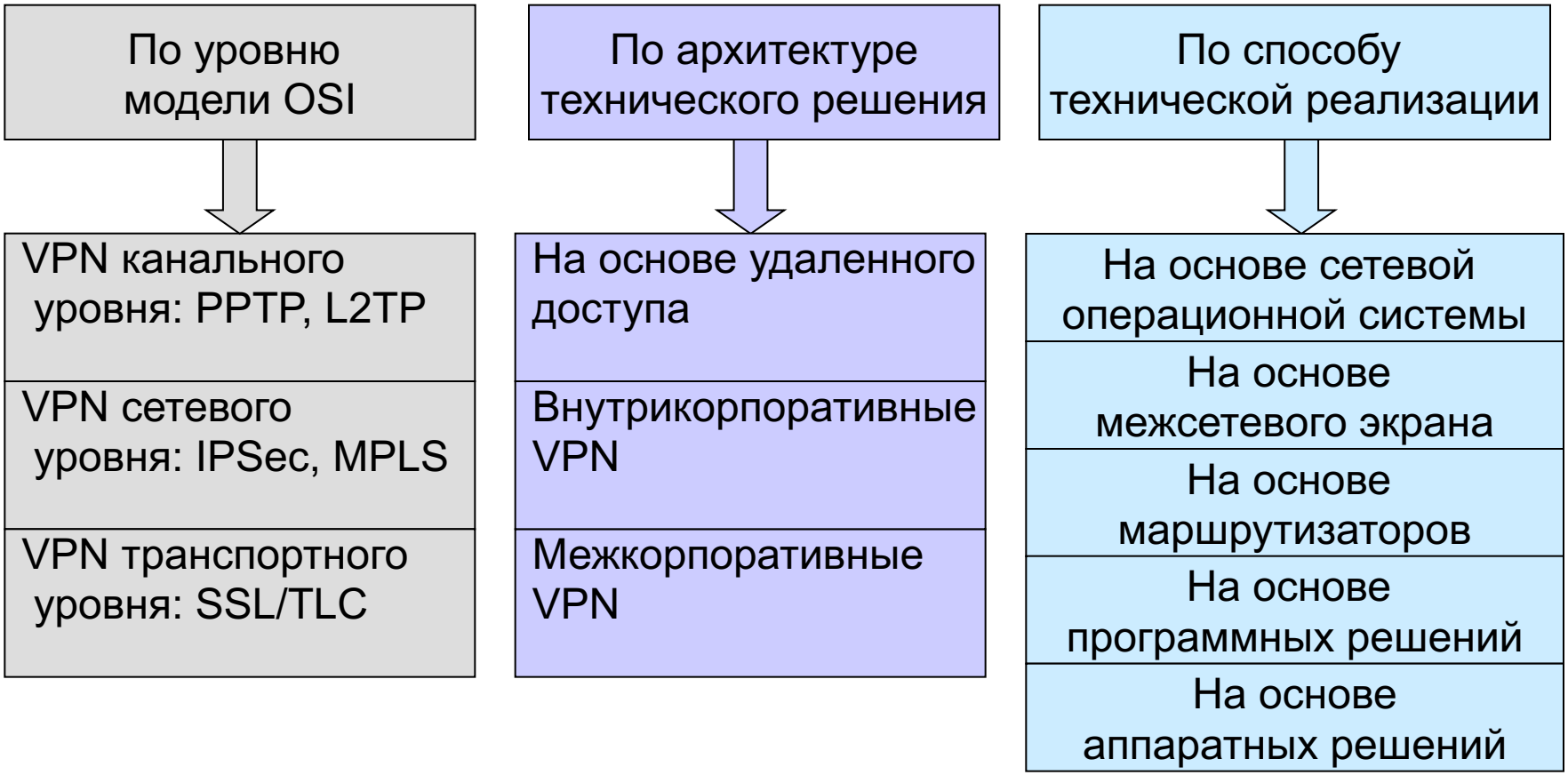
VPN – Virtual Private Network – имитируют возможности частной сети в рамках общедоступной, используя существующую инфраструктуру.

Особенность VPN – формирование логических связей не зависимо от типа физической среды. Позволяют обойтись без использования выделенных каналов.

Задача: обеспечение в общедоступной сети гарантированного качества обслуживания, а также их защита от возможного несанкционированного доступа или повреждения.

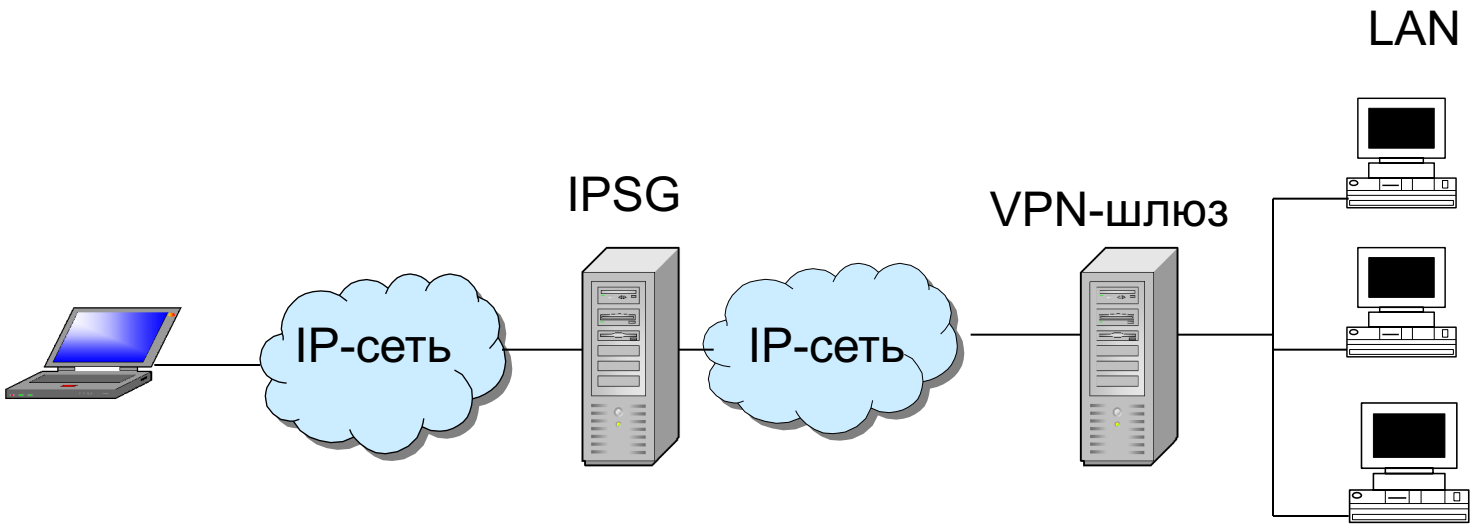
- 1998 год – разработка приложений VPN, позволяющих осуществлять централизованный контроль со стороны пользователей.
- 1999 год – модель аутентификации, дополнительные средства для конфигурирования клиентов
- 2000 год – включение средств VPN в Windows2000
- В настоящее время технология вошла в фазу расцвета. Используются различные технологии и архитектуры с учетом потребностей конкретной сети.
- Использование сети Интернет для предоставления удаленного доступа к информации может являться безопасным.

Классификация VPN



Базовые архитектуры VPN

- Шлюз-шлюз
- Шлюз-хост
- Хост-хост
- Комбинированная – через промежуточный шлюз (IPSG)



Основные компоненты VPN

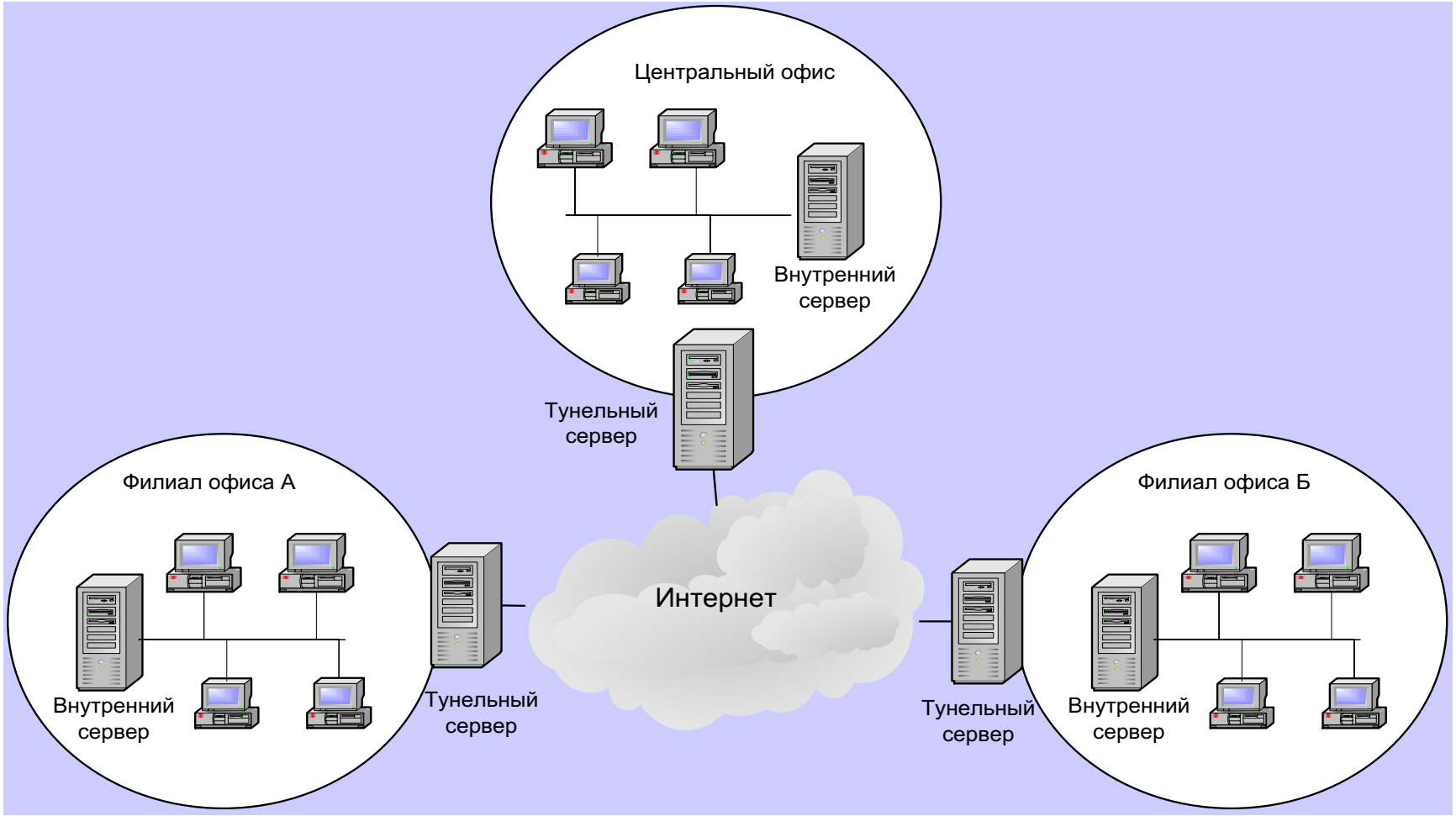
- **VPN-шлюз** – сетевое устройство, подключенное к нескольким сетям, выполняет функции шифрования, идентификации, аутентификации, авторизации и туннелирования. Может быть решен как программно, так и аппаратно.
- **VPN-клиент (хост)** решается программно. Выполняет функции шифрования и аутентификации. Сеть может быть построена без использования VPN-клиентов.

- **Туннель** – логическая связь между клиентом и сервером. В процессе реализации туннеля используются методы защиты информации.
- **Граничный сервер** – это сервер, являющийся внешним для корпоративной сети. В качестве такого сервера может выступать, например, брендмауэр или система NAT.
- **Обеспечение безопасности информации VPN** – ряд мероприятий по защите трафика корпоративной сети при прохождении по туннелю от внешних и внутренних угроз.

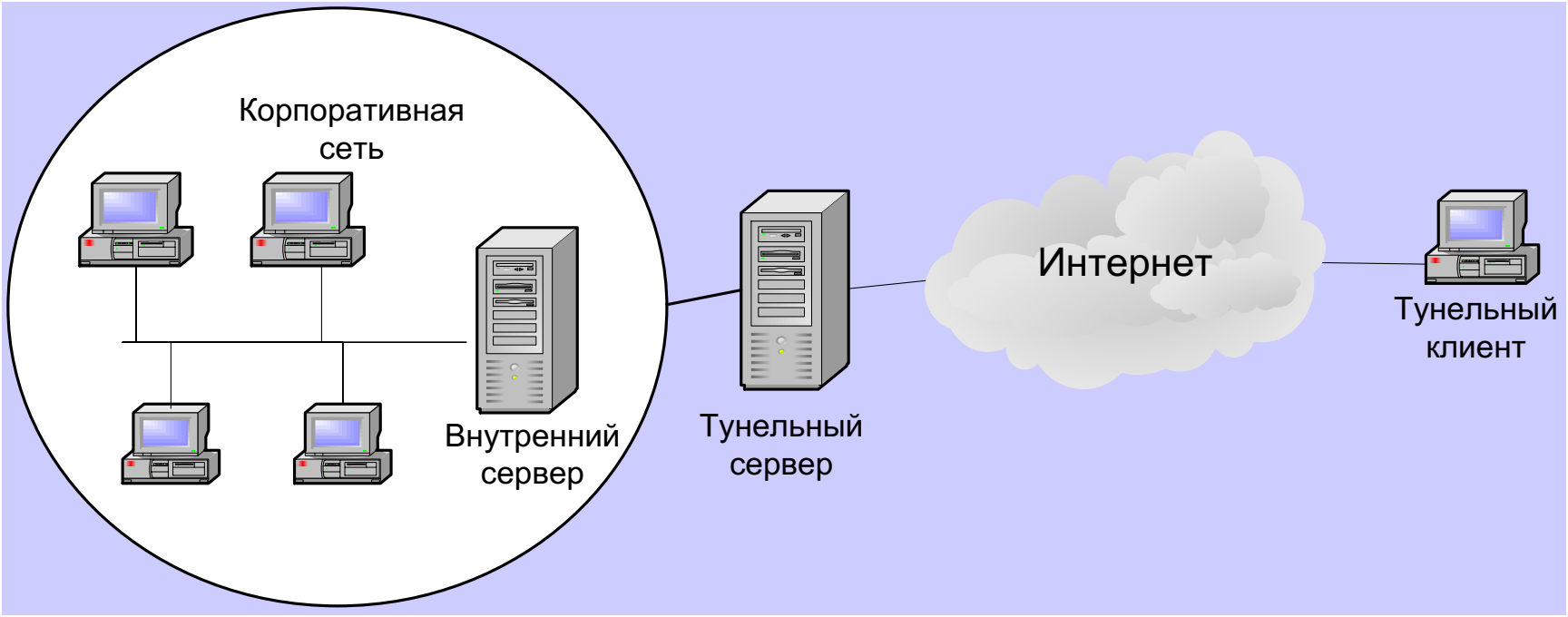
Схемы взаимодействия провайдера и клиента

- **Пользовательская схема** – оборудование размещается на территории клиента, методы защиты информации и обеспечения QoS организуются самостоятельно.
- **Провайдерская схема** – средства VPN размещаются в сети провайдера, методы защиты информации и обеспечения QoS организуются провайдером.
- **Смешанная схема** – используется при взаимодействии клиента с несколькими провайдерами.

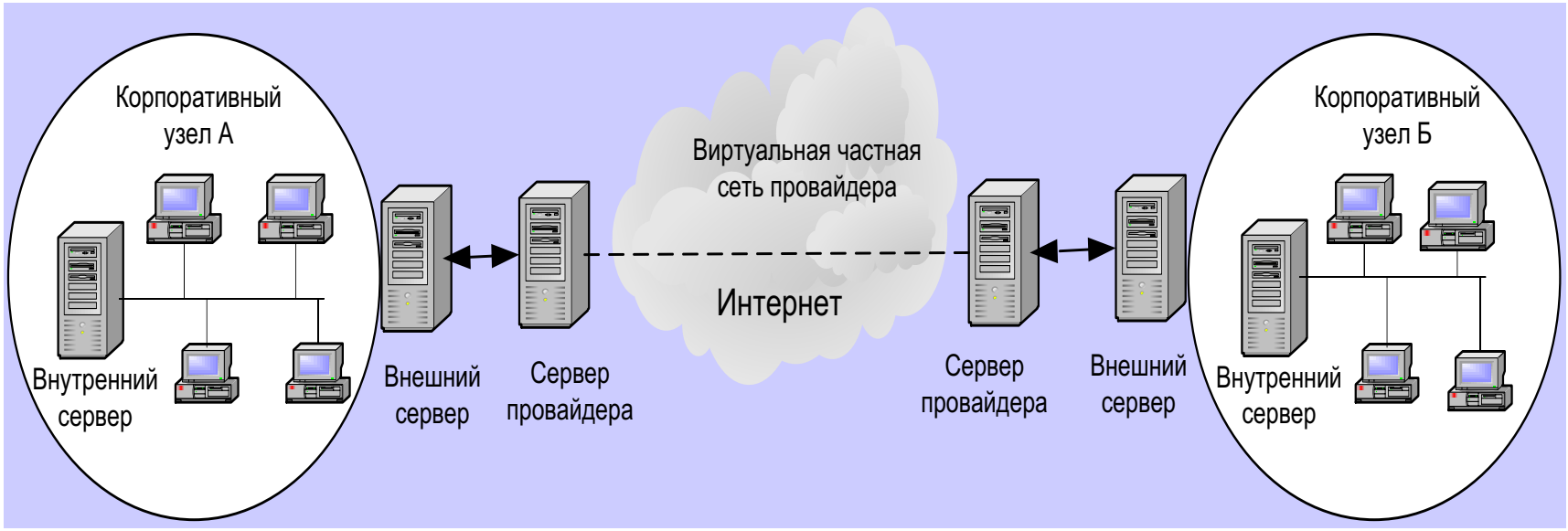
Схема соединения филиалов с центральным офисом



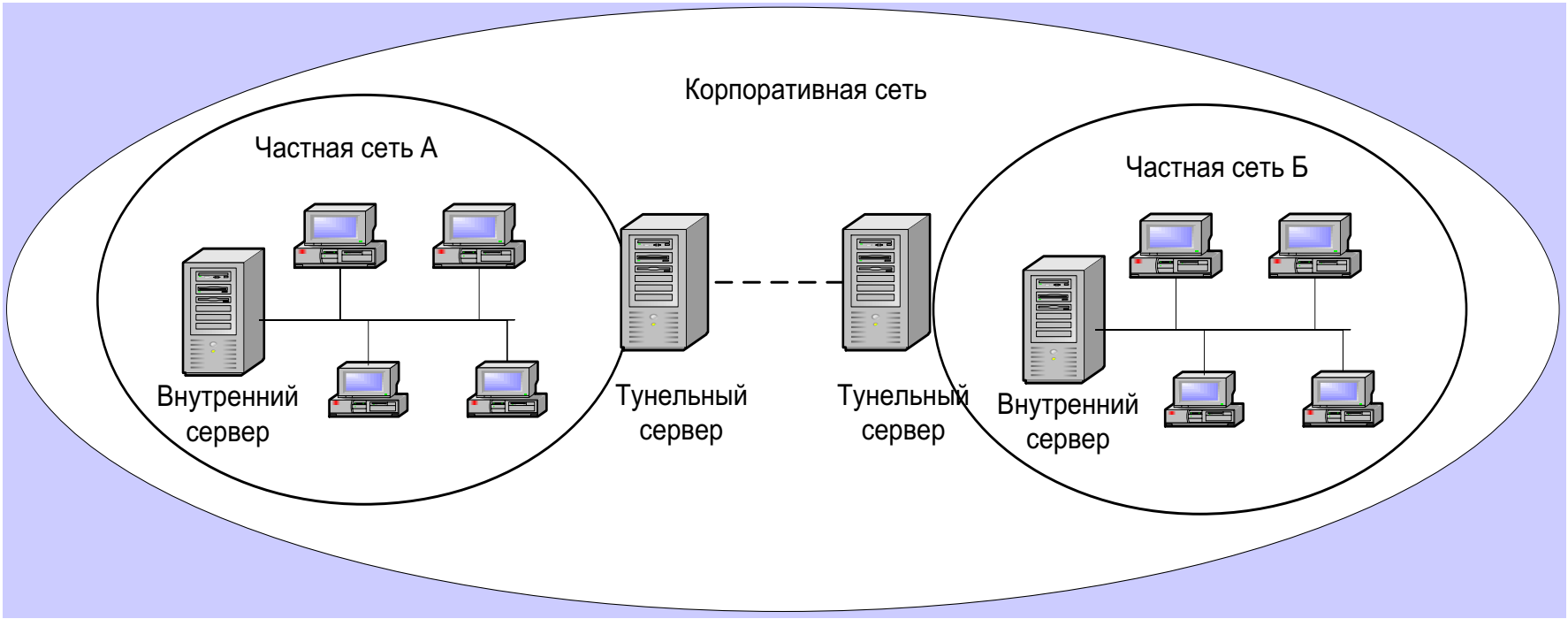
Связь удаленного пользователя с корпоративной сетью



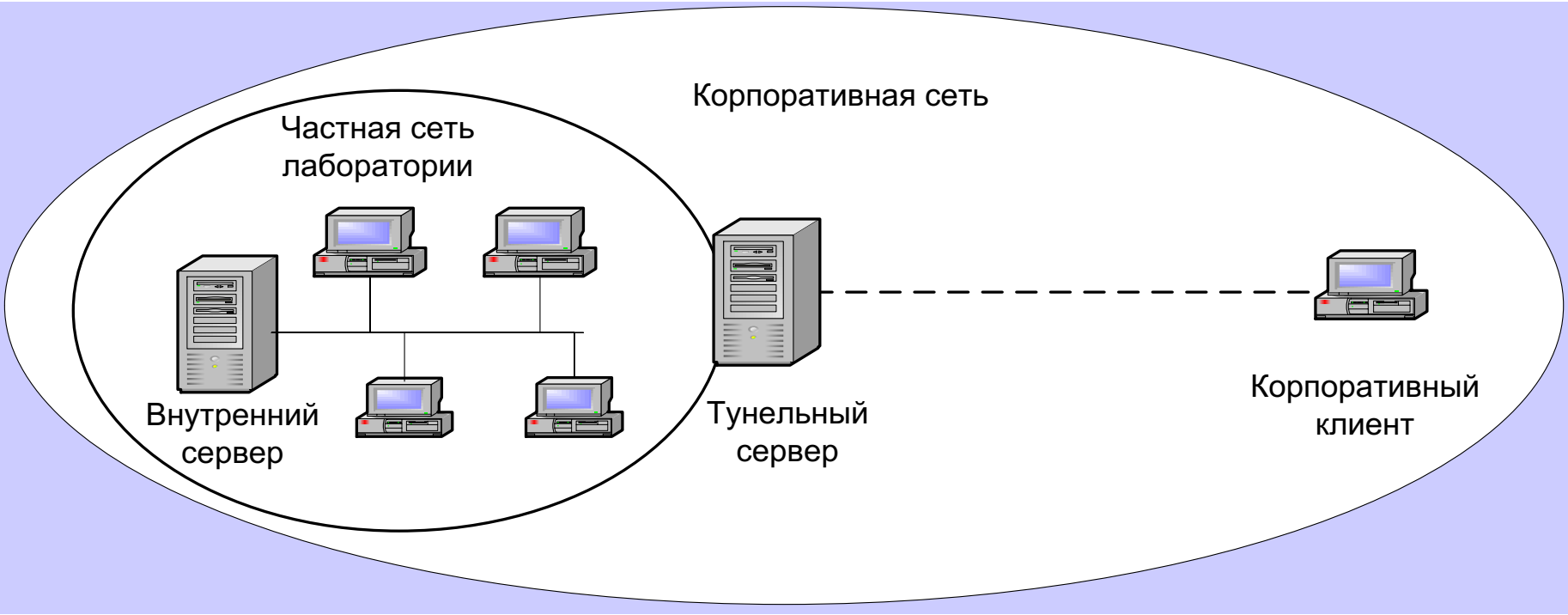
Организация туннеля через провайдера Internet, поддерживающего службу VPN



VPN-соединение защищенных сетей внутри корпоративной сети



VPN-соединение корпоративного клиента с защищенной сетью внутри корпоративной сети



Защита данных в VPN

Требования к защищенному каналу:

- Конфиденциальность
- Целостность
- Доступность легальным пользователям (аутентификация)

Методы организации защищенного канала:

- Шифрование.
- Аутентификация – позволяет организовать доступ к сети только легальных пользователей.
- Авторизация – контролирует доступ легальных пользователей к ресурсам в объемах, соответствующих предоставленными им правами.
- Туннелирование – позволяет зашифровать пакет вместе со служебной информацией.

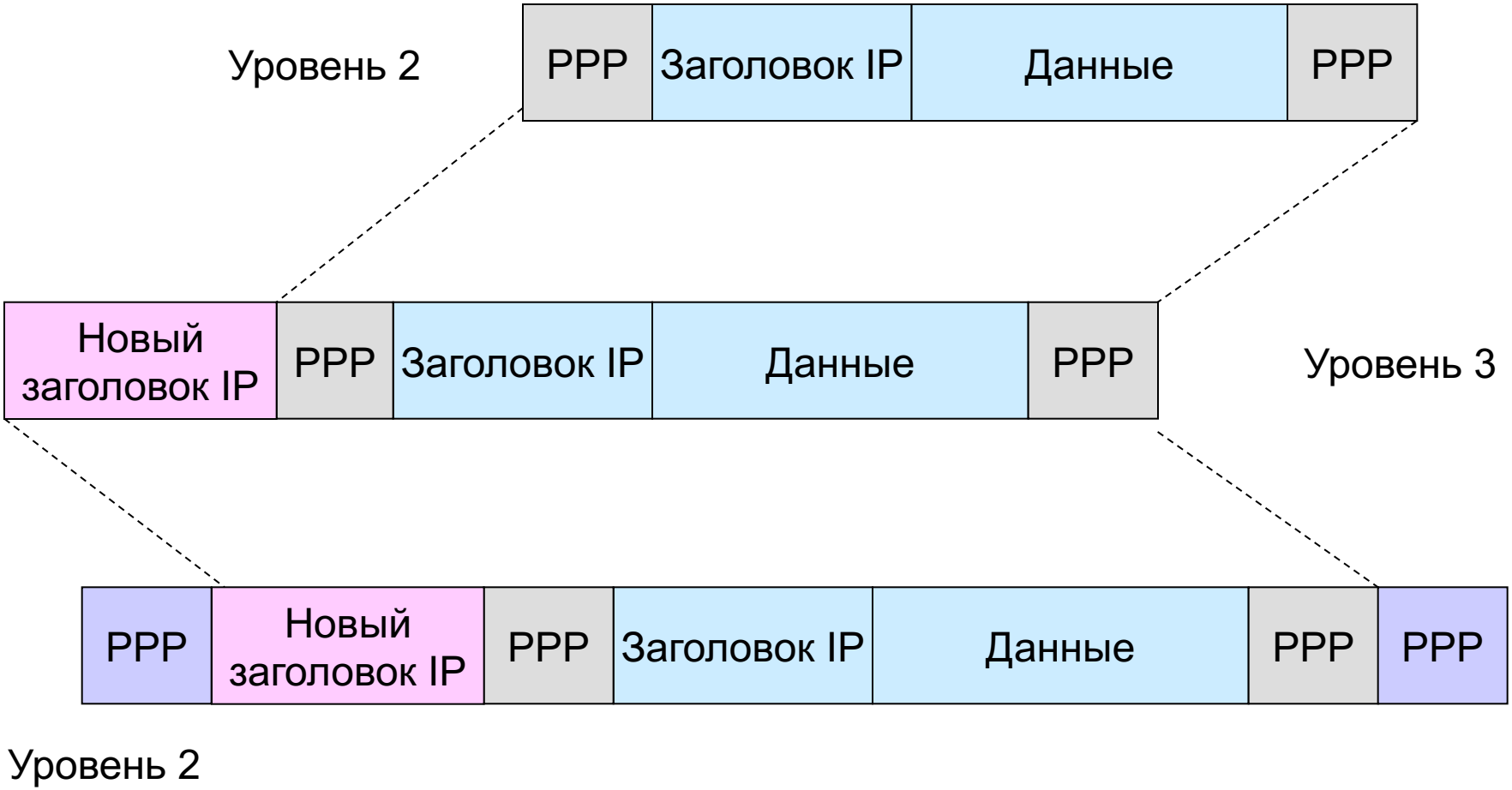
Поддержка VPN на различных уровнях модели OSI

- Канальный уровень:
  - L2TP, PPTP и др. (авторизация и аутентификация)
  - Технология MPLS (установление туннеля)
- Сетевой уровень:
  - IPSec (архитектура «хост-шлюз» и «шлюз-шлюз», поддержка шифрования, авторизации и аутентификации, проблемы с реализацией NAT)
- Транспортный уровень:
  - SSL/TLS (архитектура «хост-хост» соединение из конца в конец, поддержка шифрования и аутентификации, реализован только для поддержки TCP-трафика)

Протоколы канального уровня:

- **PPTP** (Point-to-Point-Tunneling Protocol). Шифрует кадры PPP и инкапсулирует их в IP пакеты (1996 год, разработка Microsoft, Ascend, 3Con и US Robotics)
- **L2F** (Layer to Forwarding). Прототип L2TP (1996 год, разработка Cisco)
- **L2TP** (Layer to Tunneling Protocol). Инкапсулирует кадры PPP в протокол сетевого уровня, предварительно проведя аутентификацию пользователя (1997 год, разработка Cisco и IETF)

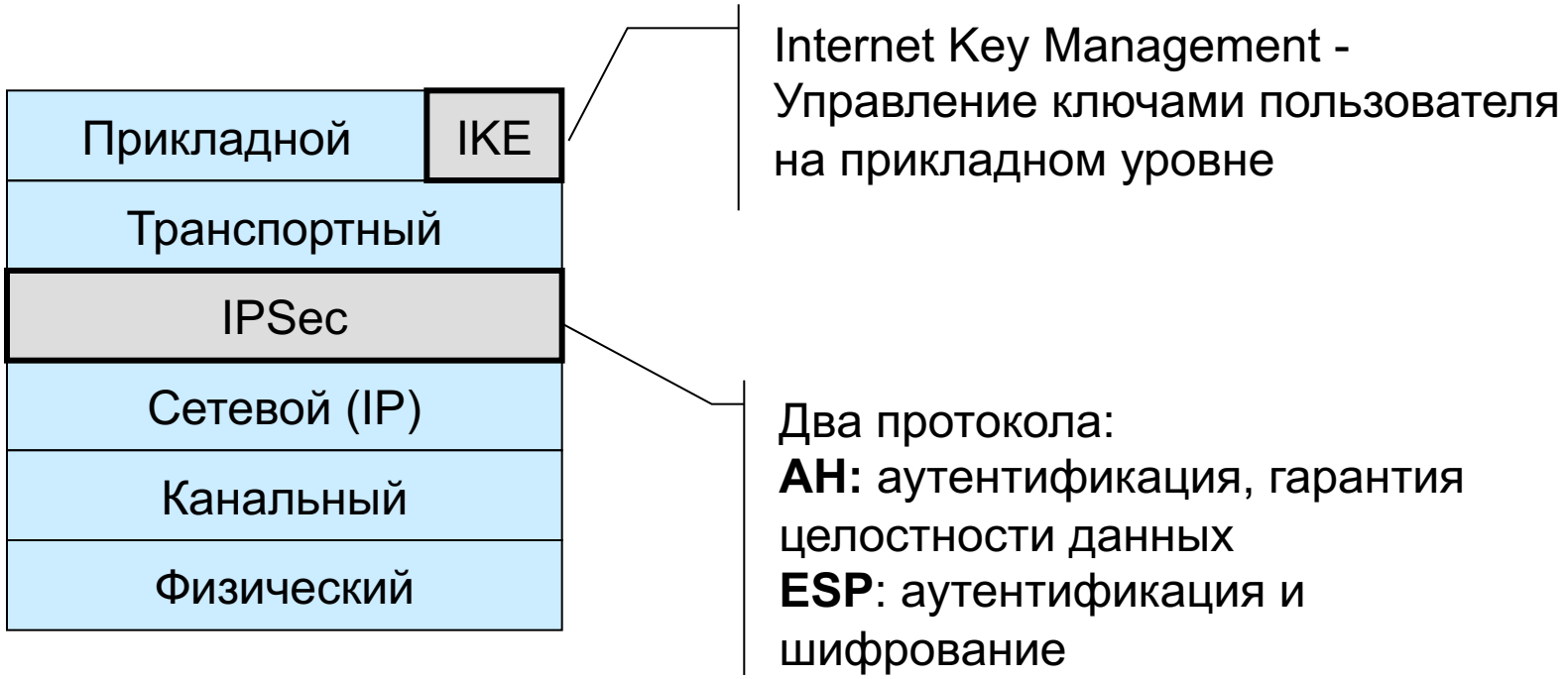
Инкапсуляция кадров PPP в IP



Протоколы сетевого уровня

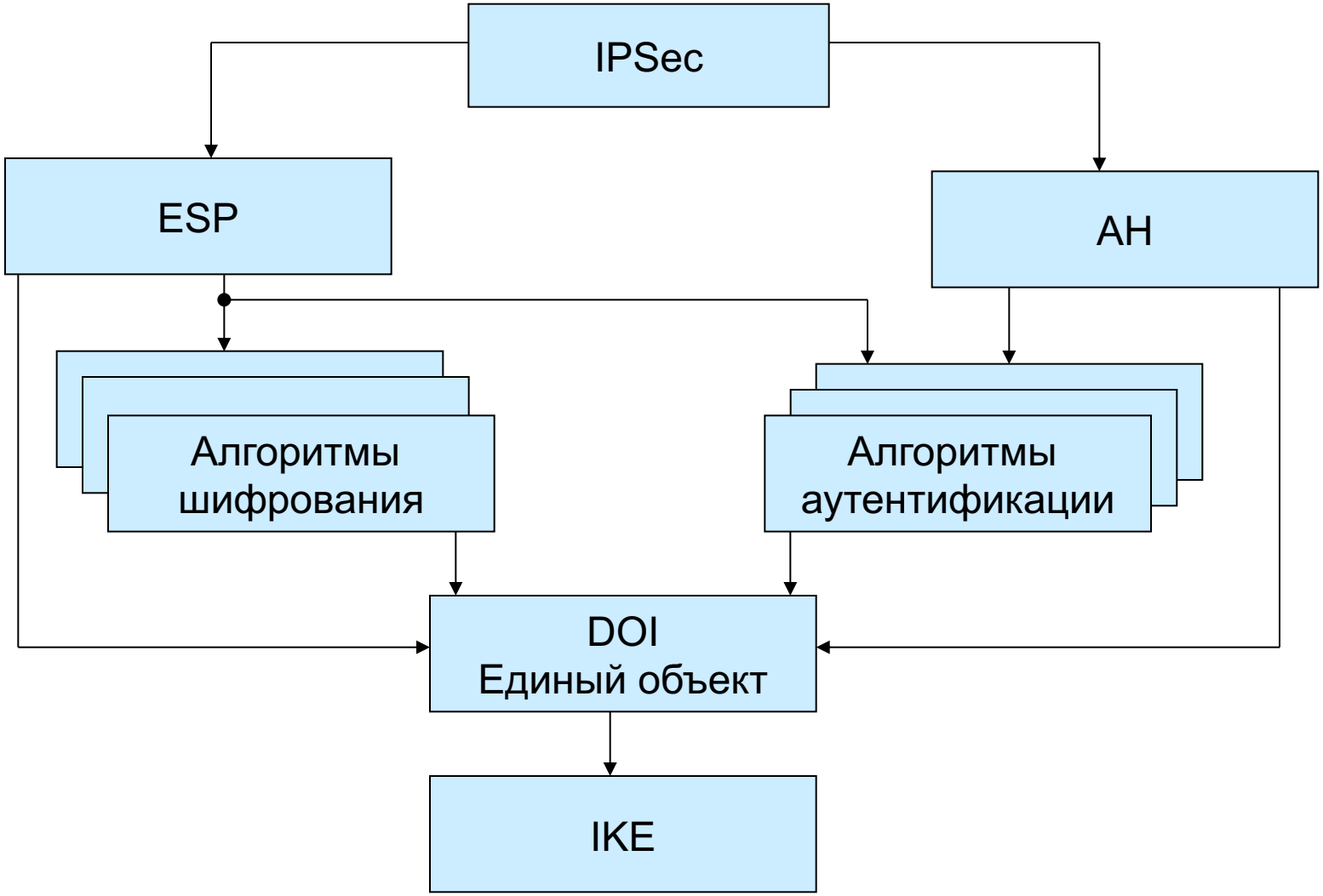
- **IPSec** (IP Security) – набор протоколов. Организует аутентификацию, шифрование и автоматическое снабжение конечных точек канала секретными ключами (1997 год, разработка IETF). Определен для IPv4 и IPv6.
- Поддерживает два режима:
  - Транспортный (защита данных в пакете)
  - Туннельный (защита всего пакета, включая заголовок)
- Каждый из участников соединения должен иметь соответствующее программное обеспечение и сконфигурировать параметры туннеля.

Стек протоколов IPSec



В случае использования IPSec в заголовке IP в поле «протокол верхнего уровня» (IPv4) или «следующий заголовок» (IPv6) помечается «IPSec»

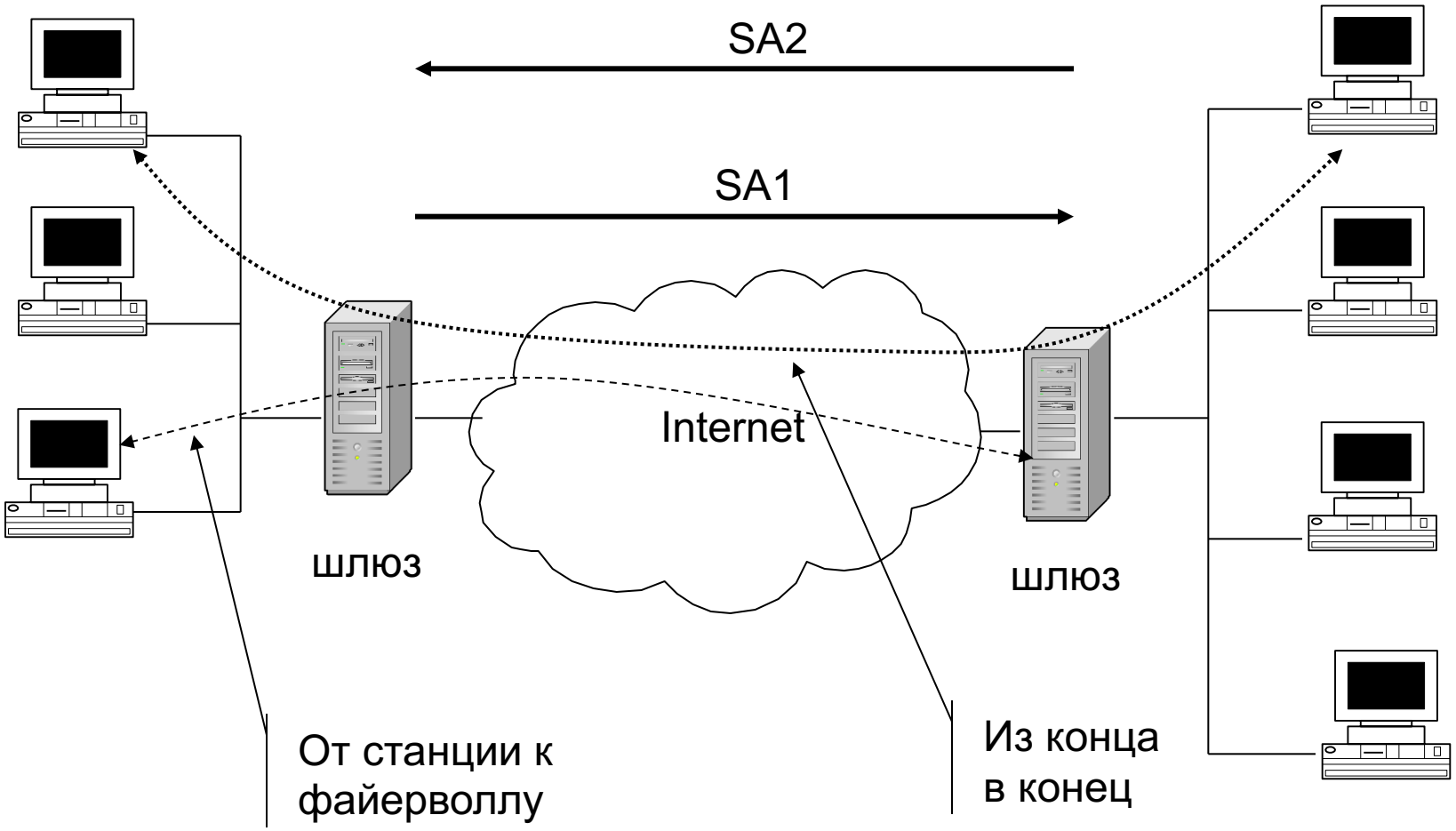
Архитектура IPSec



Ассоциация IPSec – SA (Security Association)

- Параметры SA:
  - Индекс параметра безопасности SPI
  - Адрес приемника
  - Идентификатор протокола безопасности (AH или ESP)
  - Используемый алгоритм обеспечения безопасности
  - Метод обмена ключами
  - Метод аутентификации
  - Метод шифрования
  - Время активности SA
  - Режим протокола (транспортный или туннельный)
  - Время жизни туннеля
  - И.т.п.

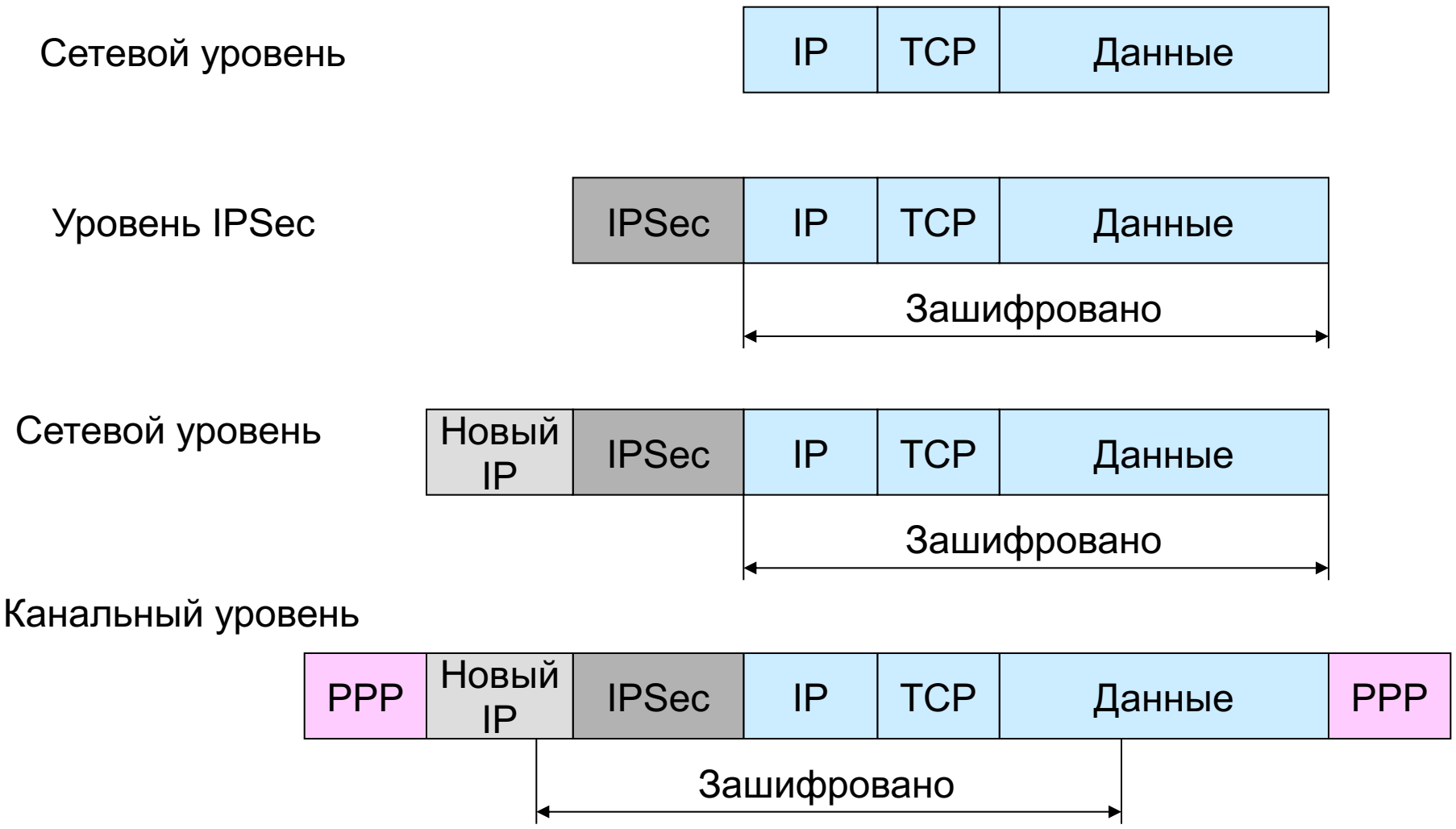
Определение SA



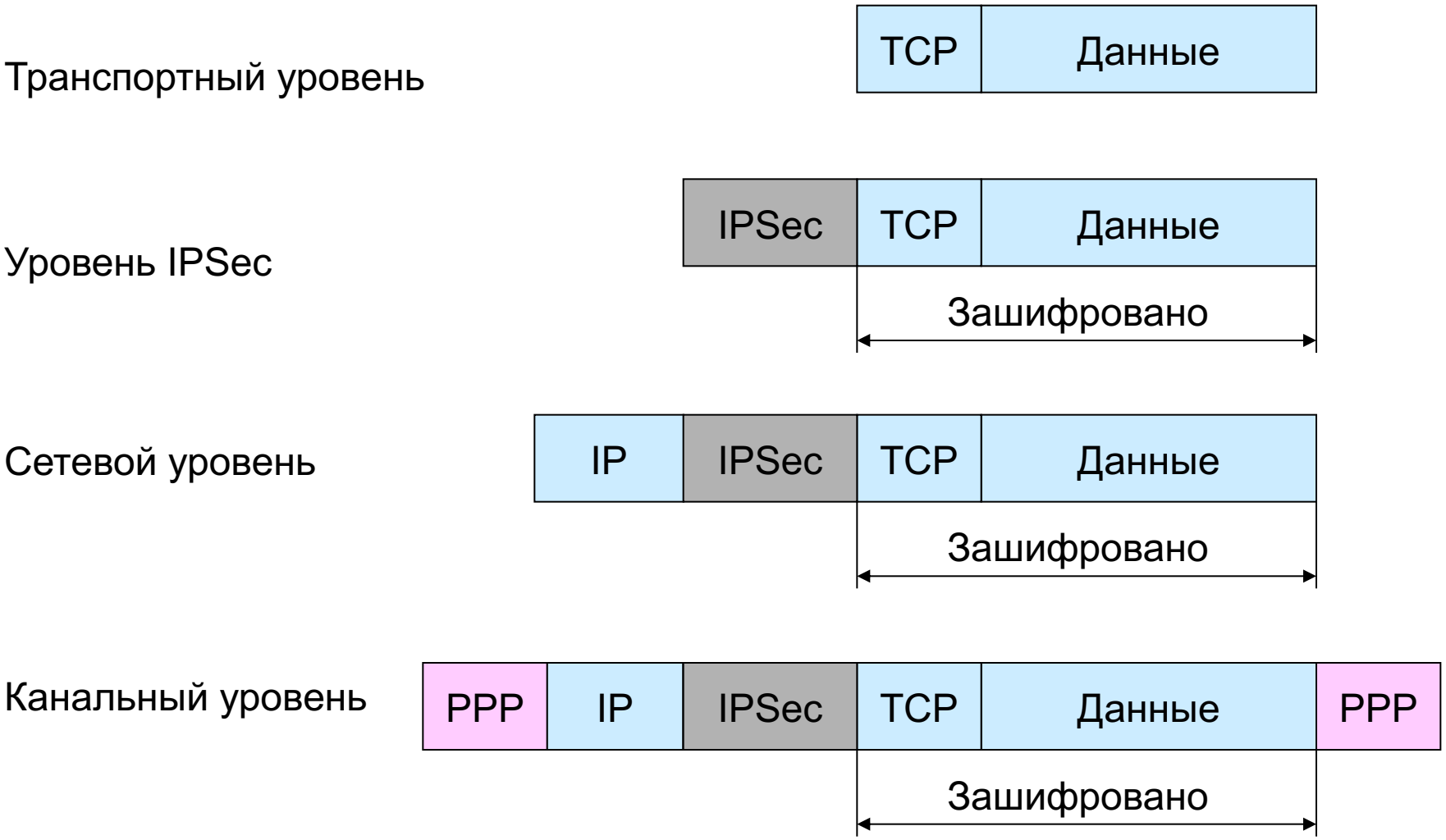
Режимы IPSec

- Туннельный режим:
  - Добавляется новый IP-заголовок
  - Исходный IP-заголовок инкапсулируется (предварительно шифруется).
  - Адрес приемника и передатчика может изменяться на адрес граничного шлюза
  - Инкапсуляция может производиться оконечной станцией или шлюзом VPN
- Транспортный режим:
  - Использует исходный IP-заголовок
  - Адреса оконечных устройств остаются без изменения
  - Инкапсуляция производится оконечными устройствами

Инкапсуляция IPSec для туннельного режима

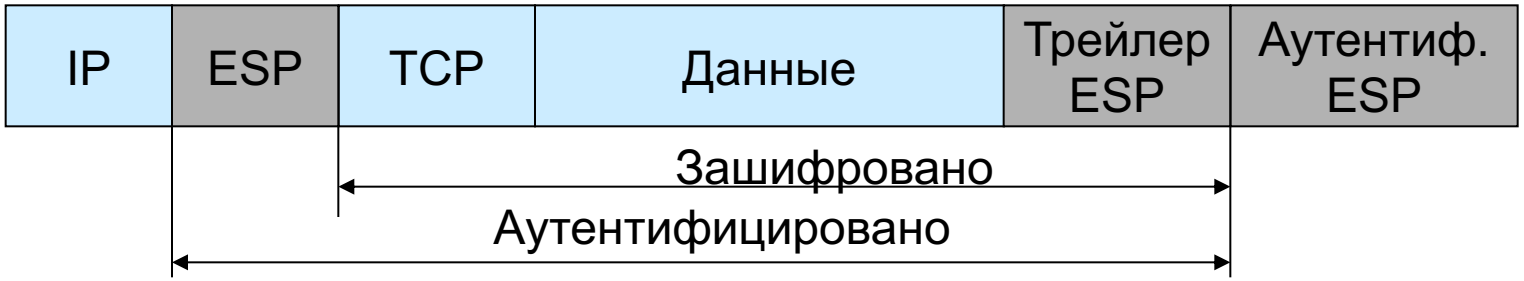


Инкапсуляция IPSec для транспортного режима



Инкапсуляция с аутентификацией (ESP)

Транспортный режим (AH аутентификация):



Туннельный режим (AH аутентификация):

Управление ключом IKE

- Функции IKE:
  - Установление SA (Security Association)
  - Определение параметров безопасности
  - Обмен ключами (UDP, порт 500)
- Фазы работы IKE:
  - Фаза I:
    - Аутентификация (из конца в конец, из конца к файерволлу)
    - Определение параметров безопасности для Фазы II
  - Фаза II:
    - Установление параметров безопасности для соединения
    - Выбор аутентификации (HMAC-MD5, HMAC-SHA)
    - Выбор алгоритма шифрования (DES, RC5, IDEA, Blowfish, CAST-128)

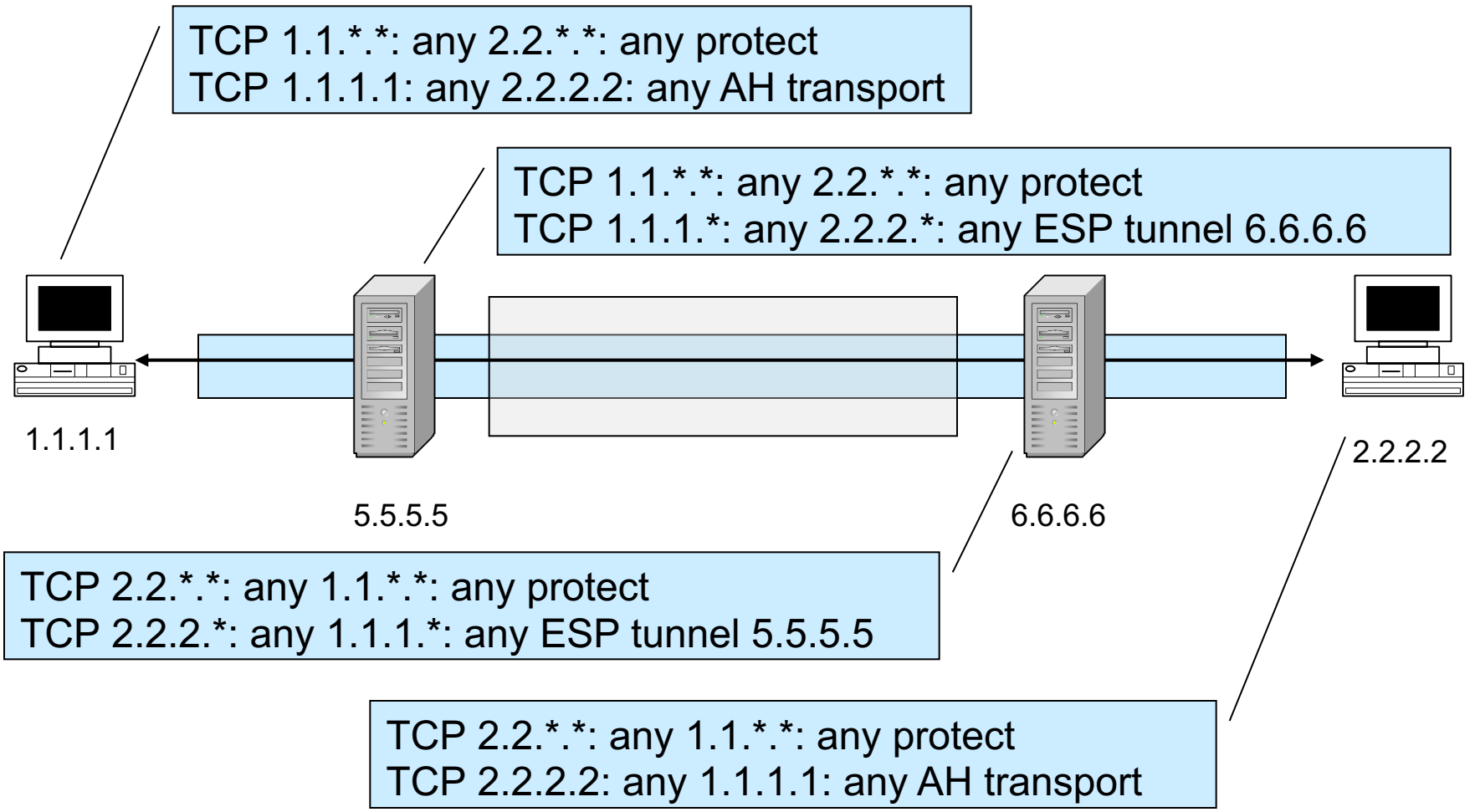
Общая процедура IPSec

- Фаза I для узла A, аутентификация
- Фаза II для узлов A и B, обмен ключами
- Установление туннеля
- Контроль состояния туннеля минимум каждые 10 с.

Правила безопасности

- Правила безопасности определяют способы защиты, пропуска и сброса трафика.
- Основным условием работы правил безопасности является зеркальность трафика в соединении
- В случае ошибочного прописывания правил безопасности могут возникать конфликты, приводящие к потере трафика:
  - Скрывание
  - Конфликт в типе туннелей
  - Зацикливание
  - Асимметрия

Пример реализации правил безопасности

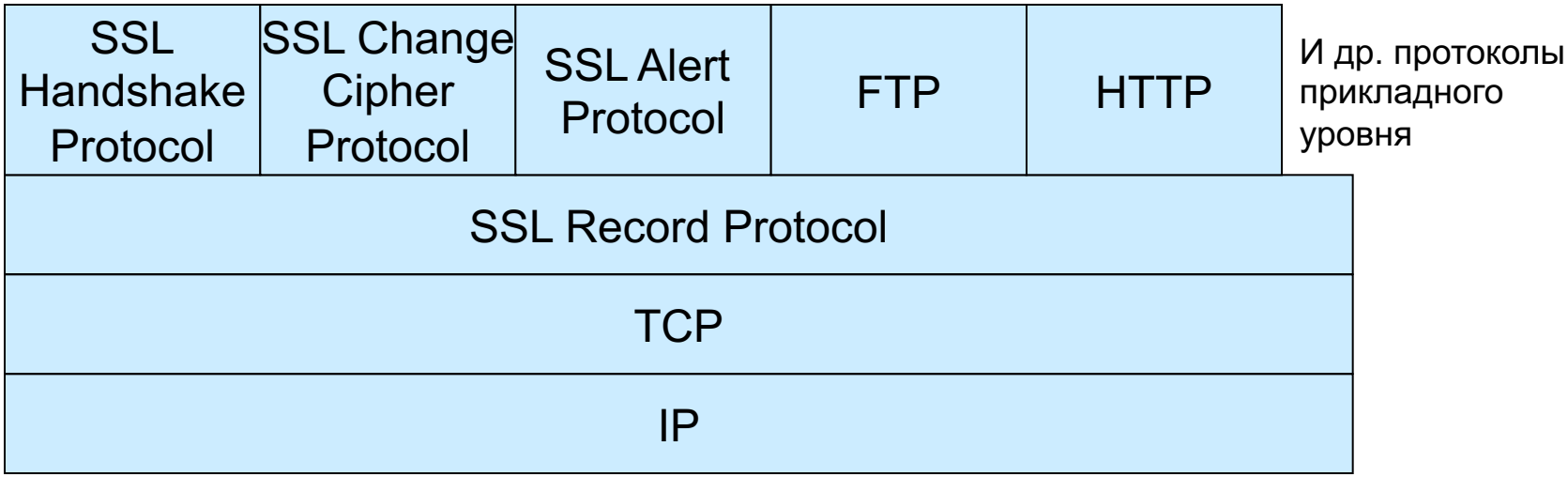


Протоколы транспортного уровня

- SSL – Secure Sockets Layer. SSLv3, 1996 год.
- TLS – Transport Layer Security. Стандарт IETF, RFC 2246.

  В настоящее время объединены в общий стек протоколов SSL/TLS

Стек протоколов SSL/TLS



- Все браузеры поддерживают SSL/TLS.
- SSL/TLS реализован поверх TCP (надежность доставки, квитирование), между транспортным и прикладным уровнем. Не поддерживает приложения UDP (отсутствует квитирование)
- Стек протоколов SSL/TLS:
  - SSL Record Protocol: защита передаваемых данных
  - SSL Handshake Protocol: установление сессии (соглашение о используемых алгоритмах, параметры безопасности)
  - SSL Change Cipher Protocol (смена шифра)
  - SSL Alert Protocol (сообщения об ошибках)

Критерии выбора протокола VPN

- Тип подключения:
  - Постоянное: IPSec
  - Временное: SSL/TLS
- Тип доступа:
  - Пользователь (сотрудник компании): IPSec
  - Гость: SSL/TLS
- Уровень безопасности корпоративной сети:
  - Высокий: IPSec
  - Средний: SSL/TLS
  - В зависимости от предоставляемой услуги: IPSec +SSL/TLS
- Уровень безопасности данных:
  - Высокий: IPSec
  - Средний: SSL/TLS
  - В зависимости от предоставляемой услуги: IPSec +SSL/TLS
- Масштабируемость решения:
  - Масштабируемость: IPSec
  - Быстрое развертывание: SSL/TLS

Сравнительные характеристики протоколов VPN

Критерии	Протоколы			
	L2F	L2TP	IPSec	SSL/TLS
Многопротокольное туннелирование	Да	Да	Да	Нет
Поддержка аутентификации и шифрования	Нет	Слабая	Да	Очень надежная
Управление потоком данных в туннеле	Нет	Нет	Да	Да
Управление правами пользователей	Нет	Нет	Нет	Да
Сфера применения	Удаленный доступ через провайдера	Удаленный доступ через провайдера	Для реализации собственного решения	Для реализации собственного решения
Перспективы развития	Слабые	Существуют	Радужные	Радужные