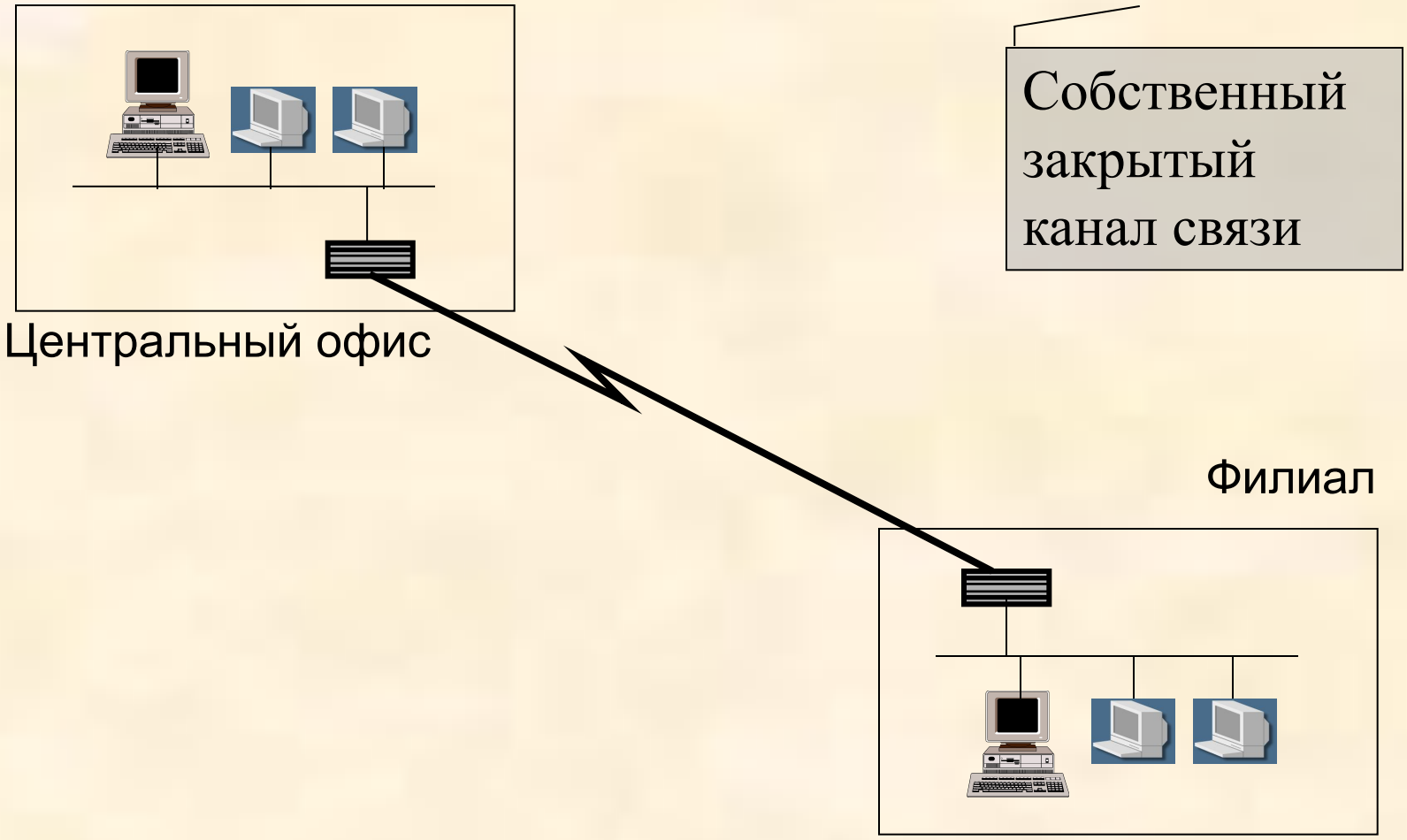
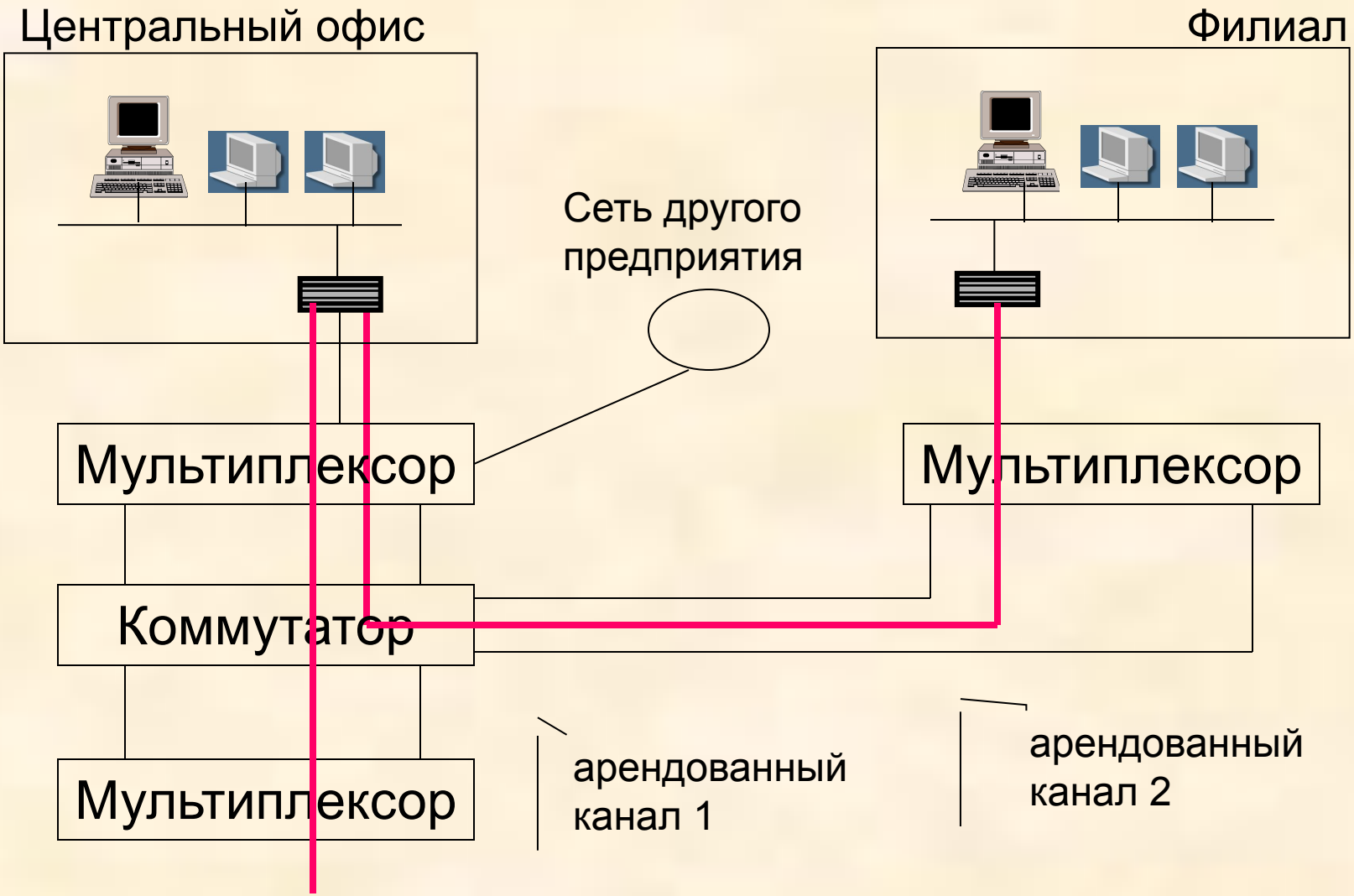
Виртуальные частные сети

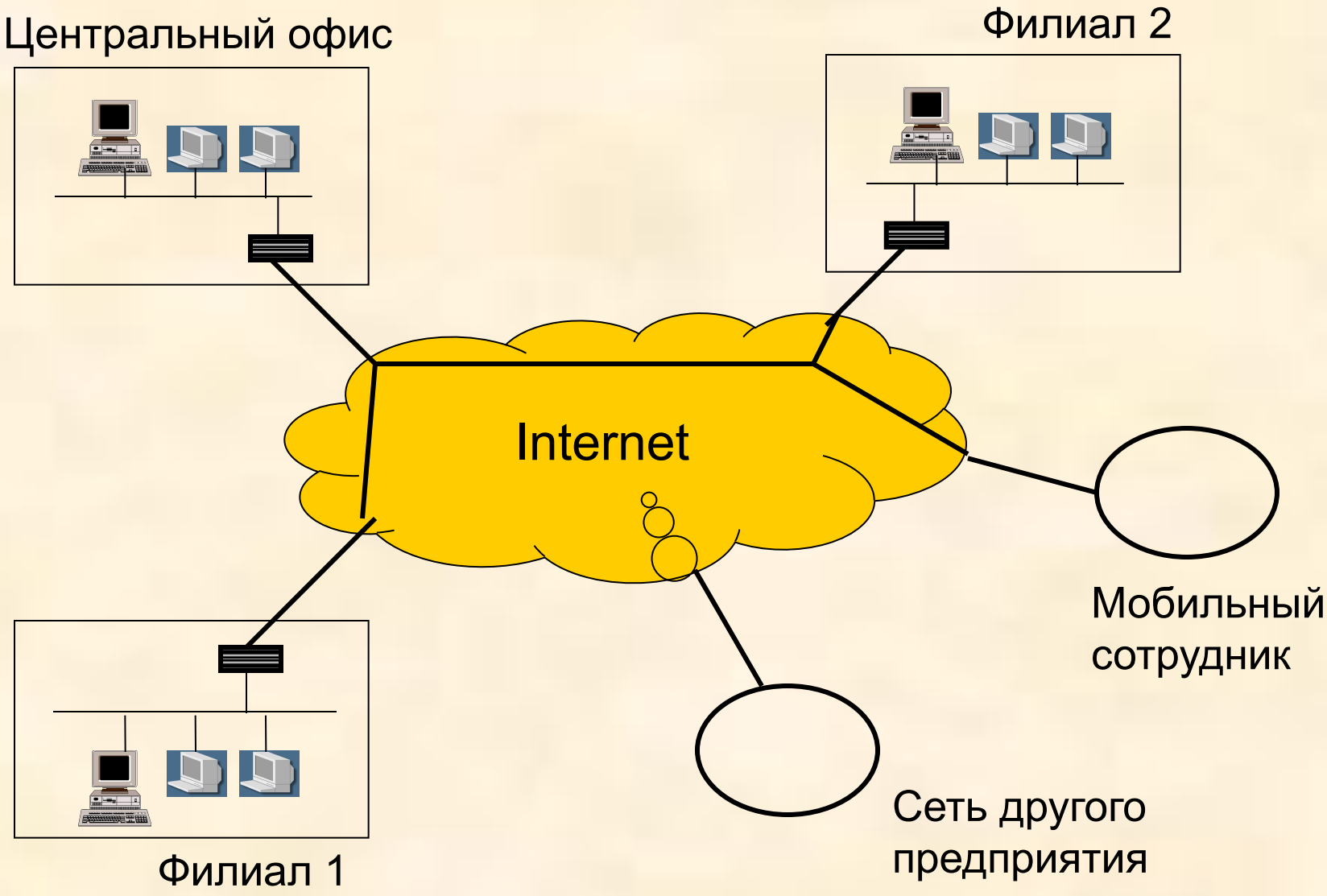
Истинная частная сеть



Частная сеть на арендованных каналах



Организация VPN через общую сеть

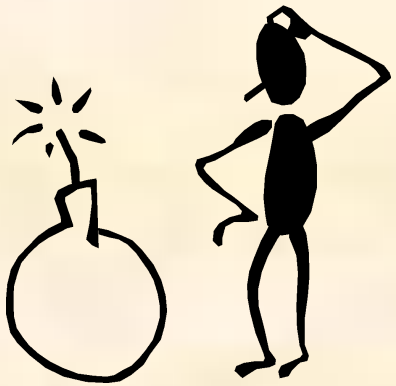


Организация VPN через общую сеть

Преимущества

Простота и доступность реализации

Низкая стоимость



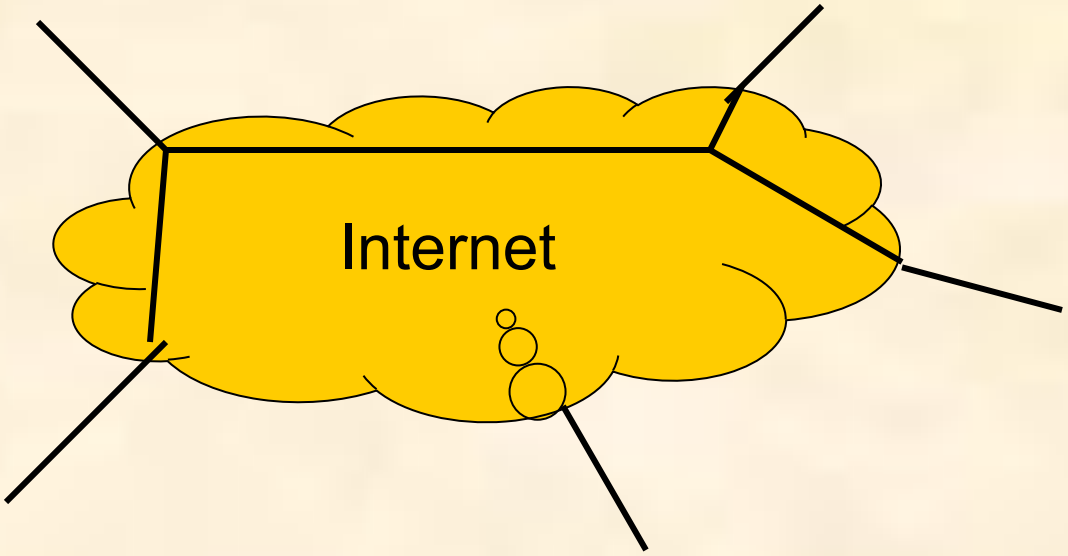
Недостатки

Непредсказуемость пропускной способности

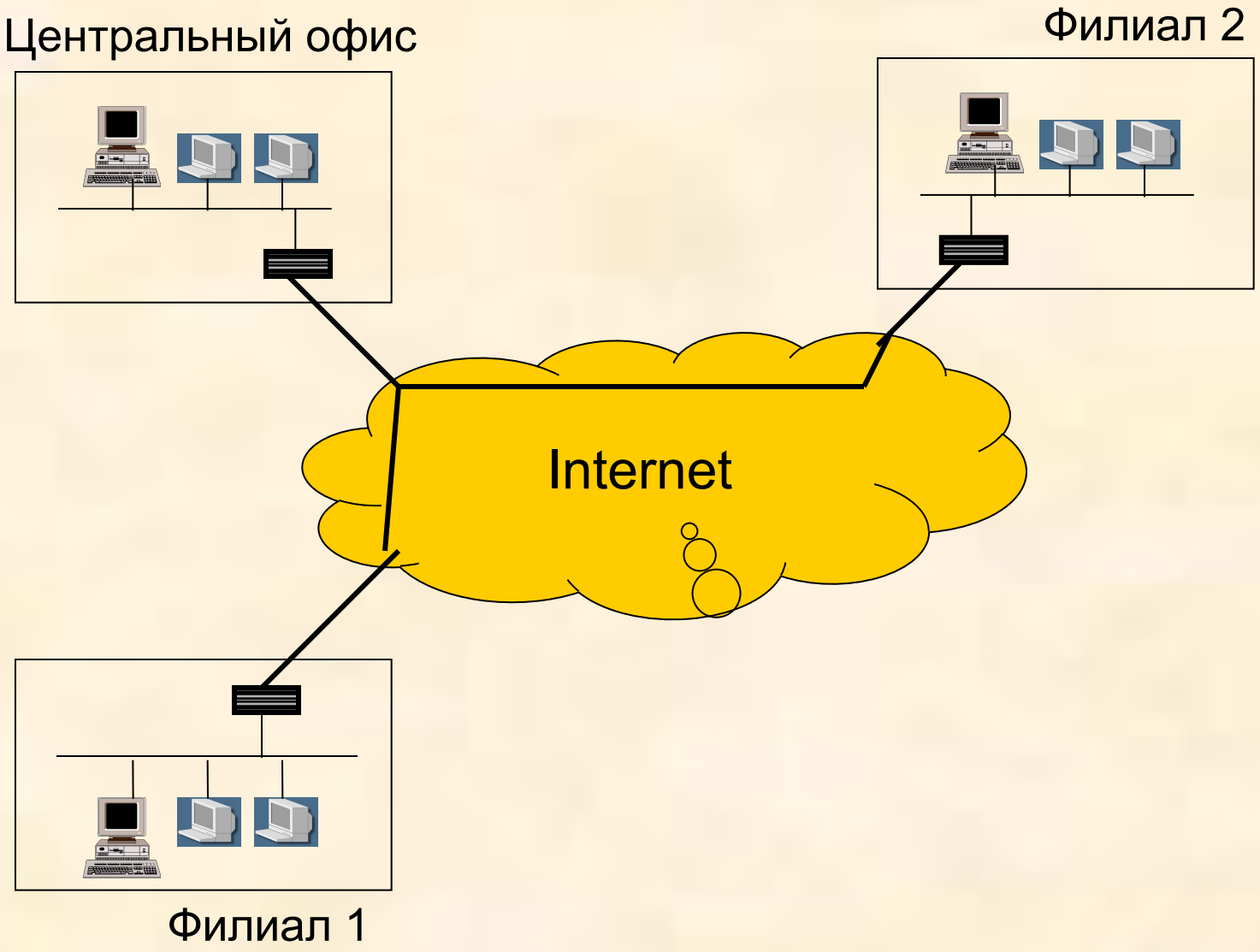
Угроза перехвата информации, передаваемой по открытой сети

Виды VPN

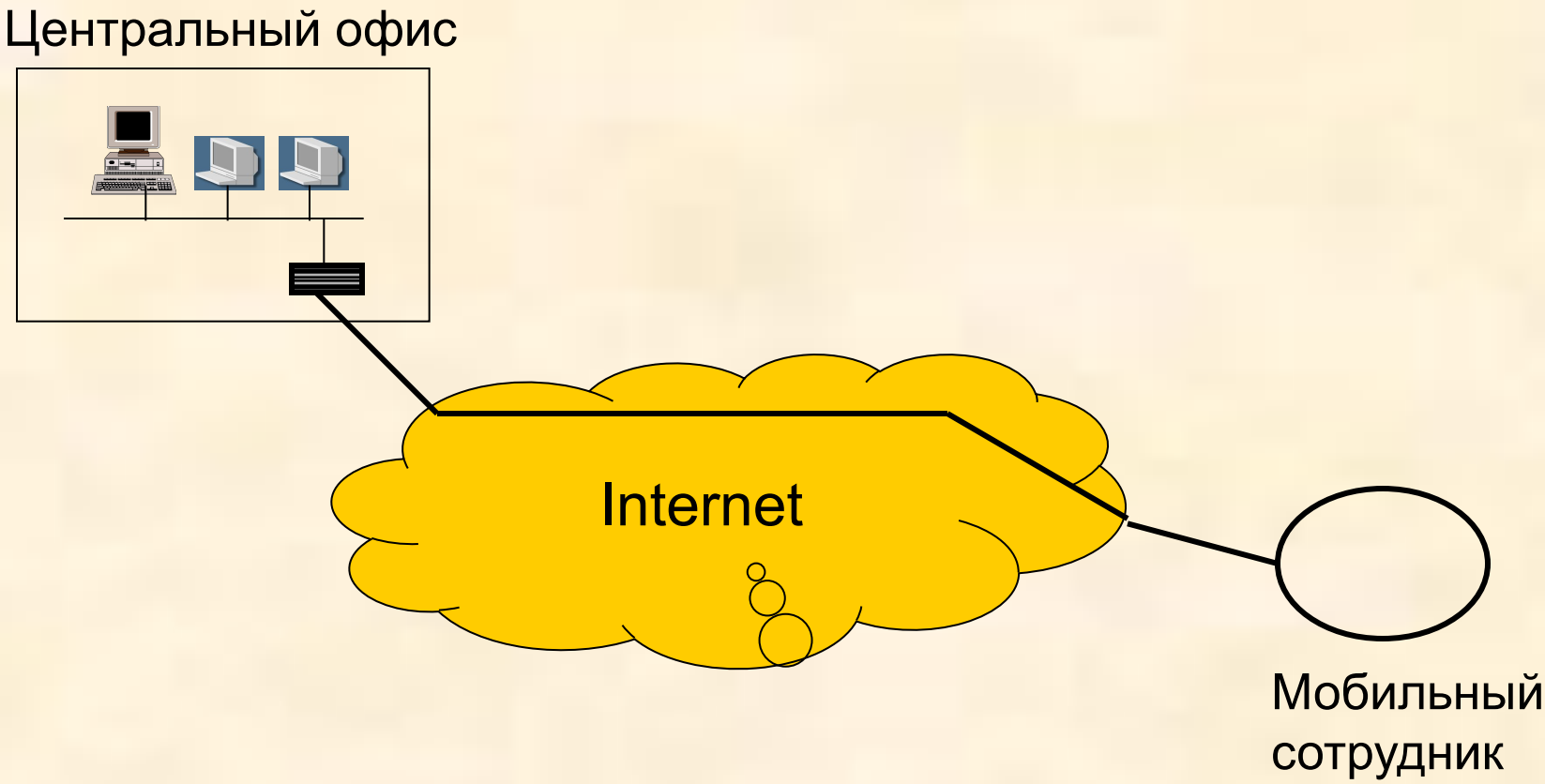
- **Внутрикорпоративные VPN (Intranet VPN)**
- **VPN с удалённым доступом (Remote Access VPN)**
- **Межкорпоративные VPN (Extranet VPN)**



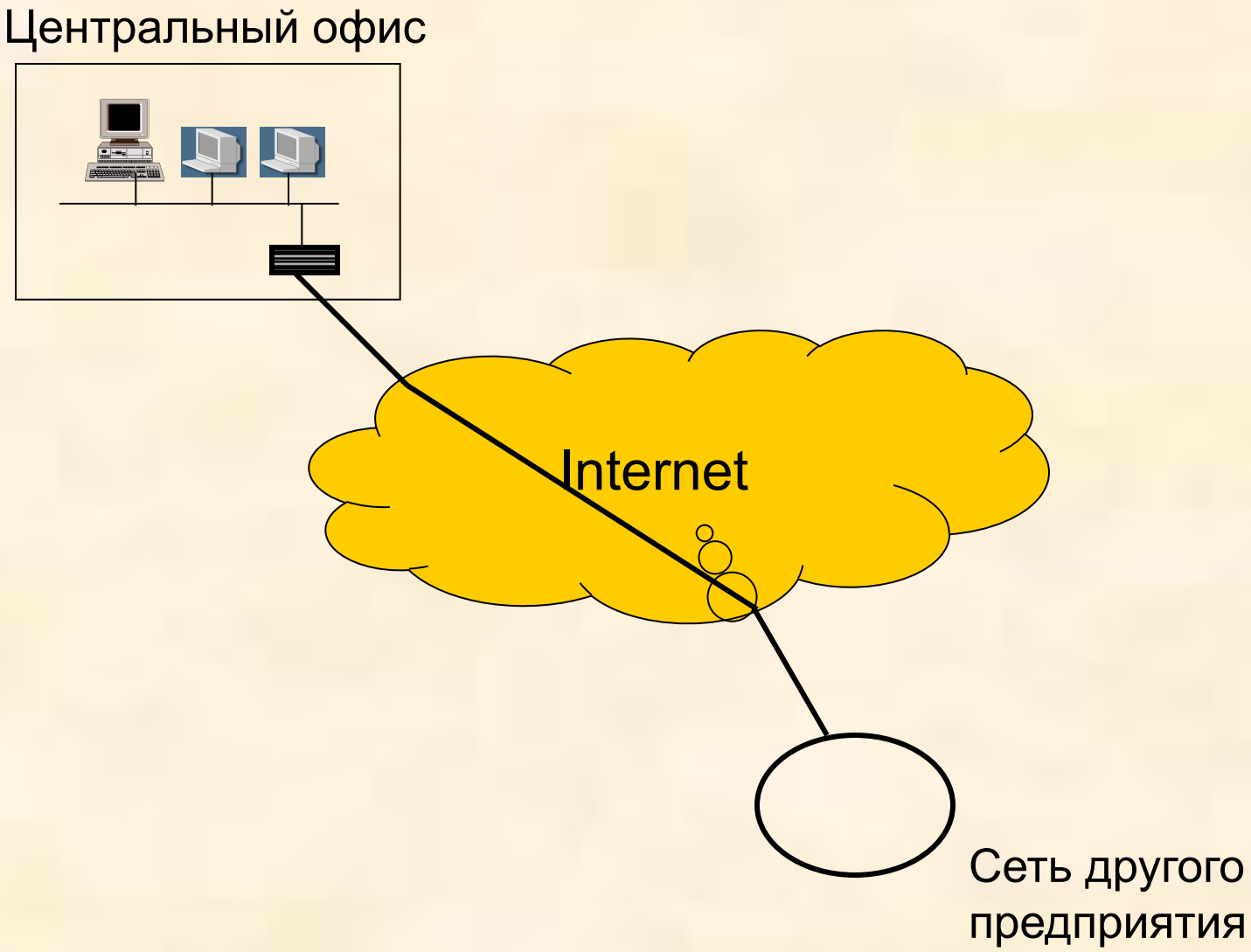
Внутрикорпоративные VPN



VPN с удалённым доступом



Межкорпоративные VPN



Типы VPN-устройств

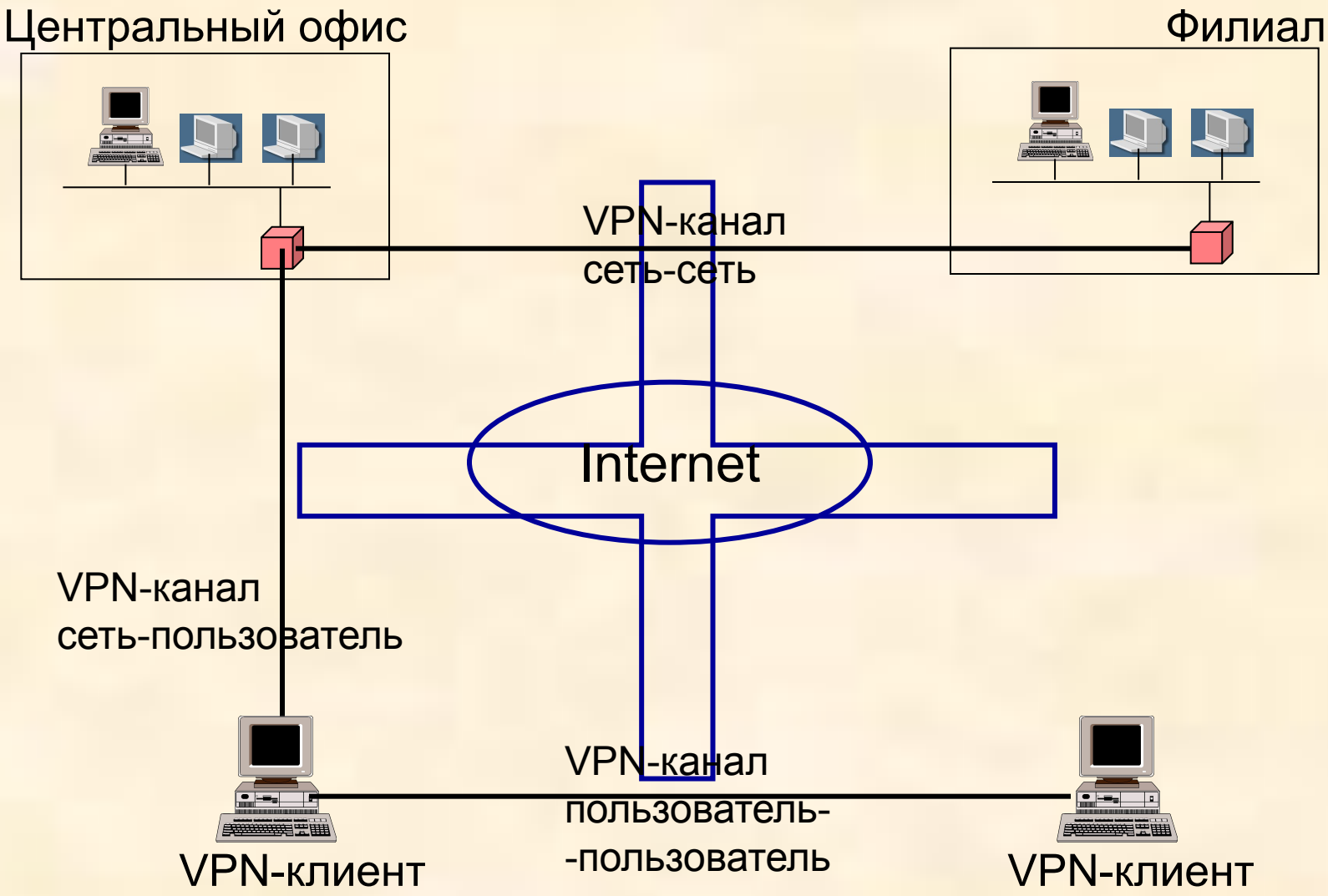
Отдельное аппаратное устройство VPN на основе специализированной ОС реального времени, имеющее 2 или более сетевых интерфейса и аппаратную криптографическую поддержку – так называемый “черный ящик”

Отдельное программное решение, дополняющее стандартную операционную систему функциями VPN

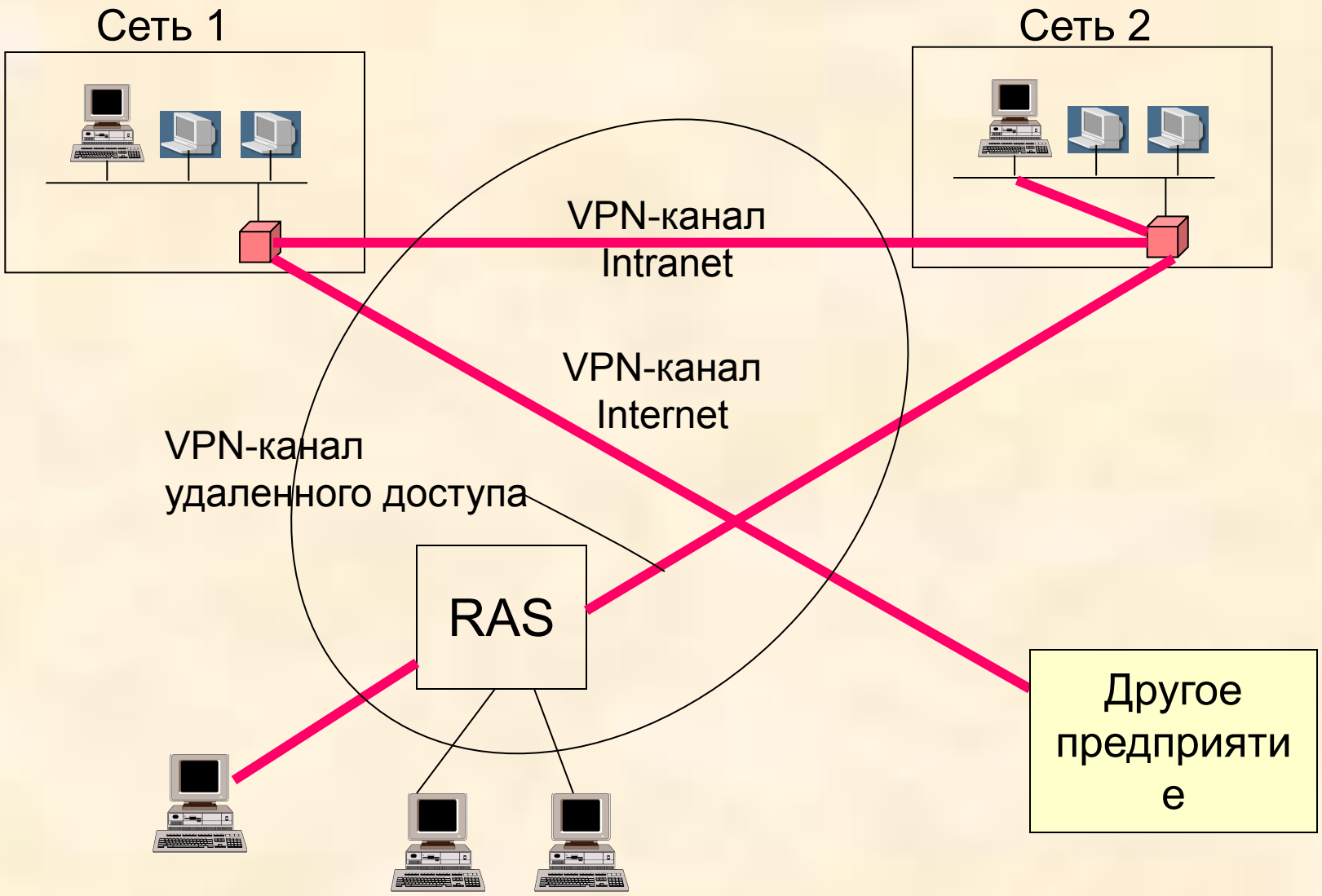
Расширение межсетевого экрана за счет дополнительных функций защищенного канала

Средства VPN, встроенные в маршрутизатор

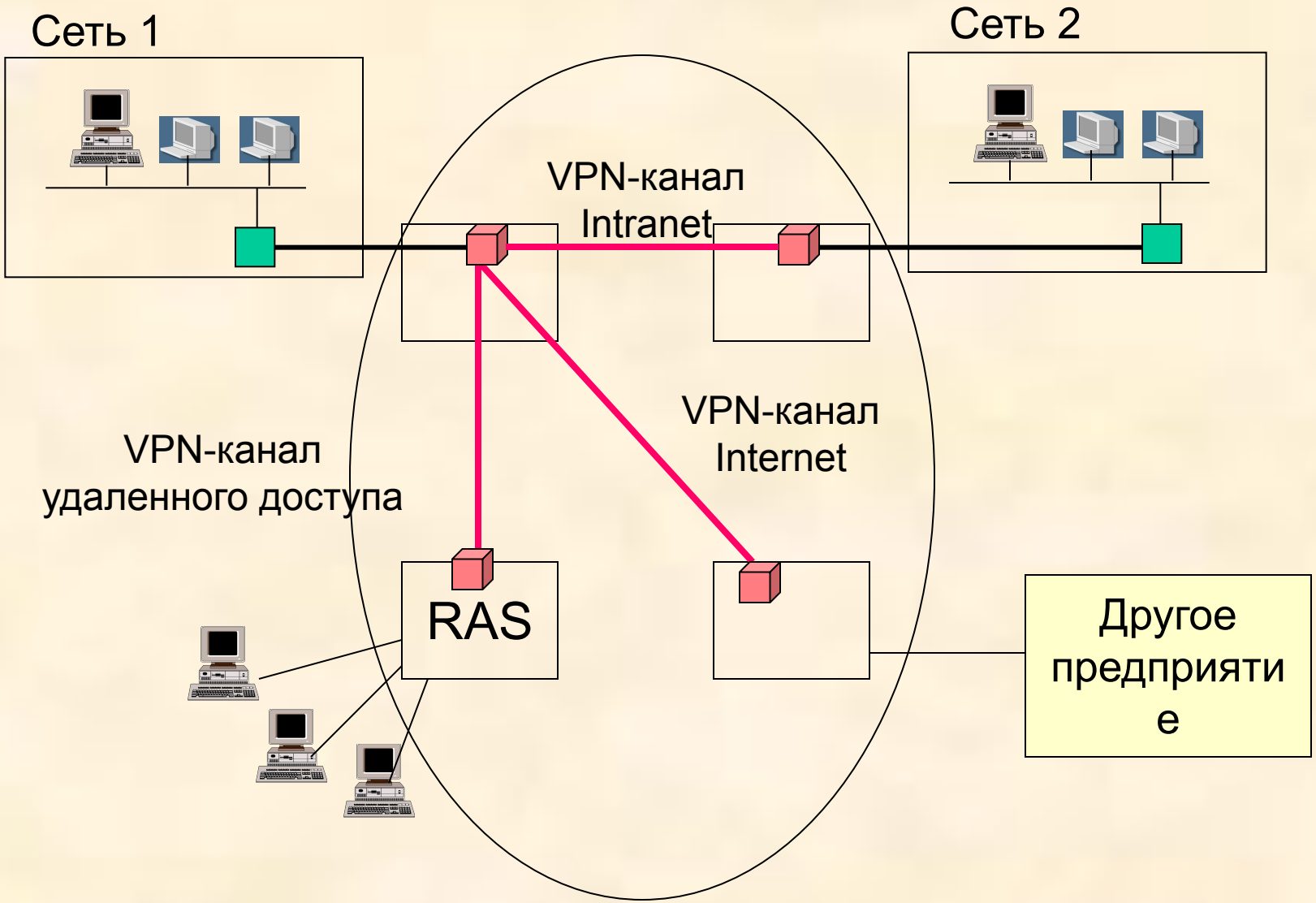
Шлюзы и клиенты VPN



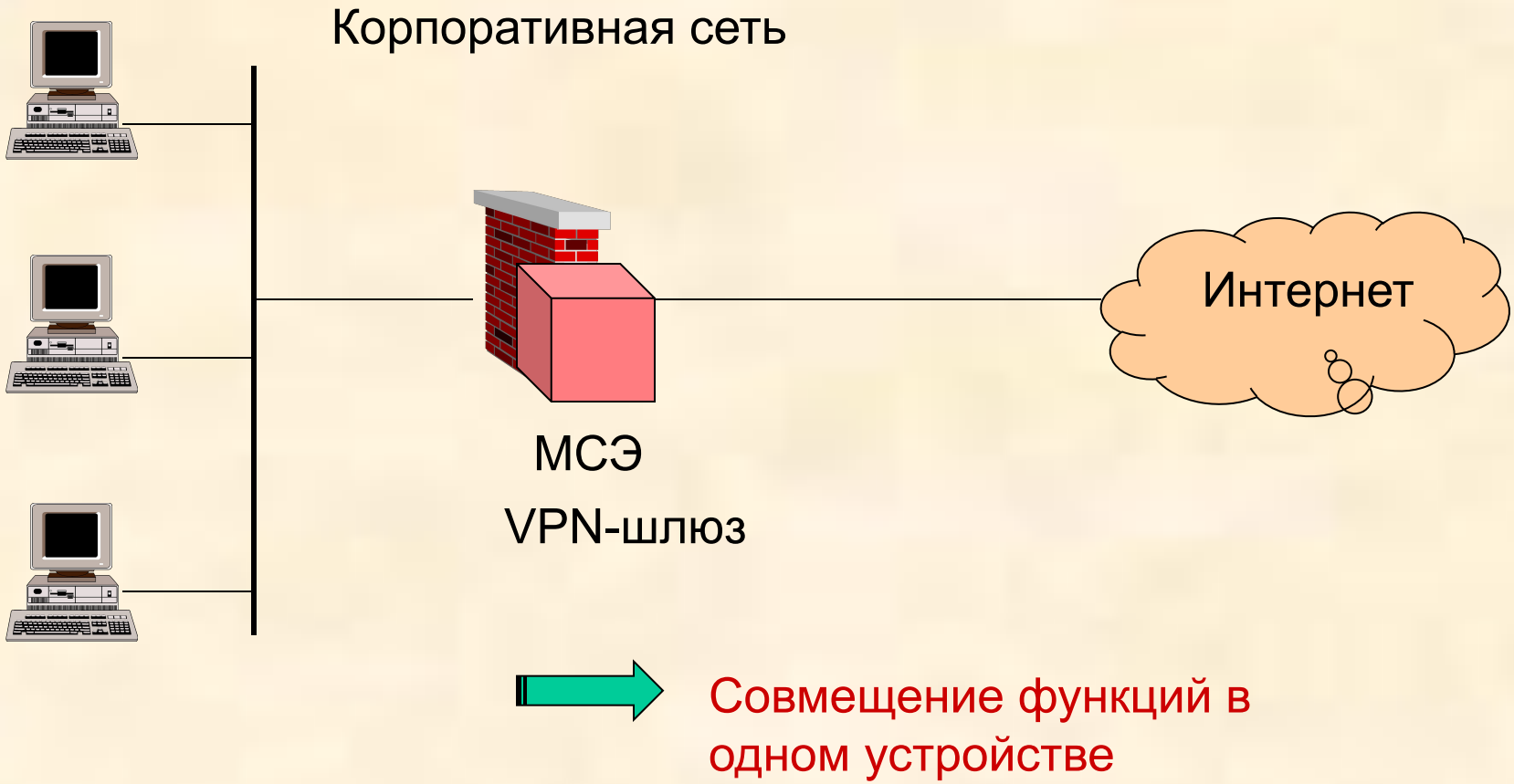
Организация VPN (пользовательская схема)



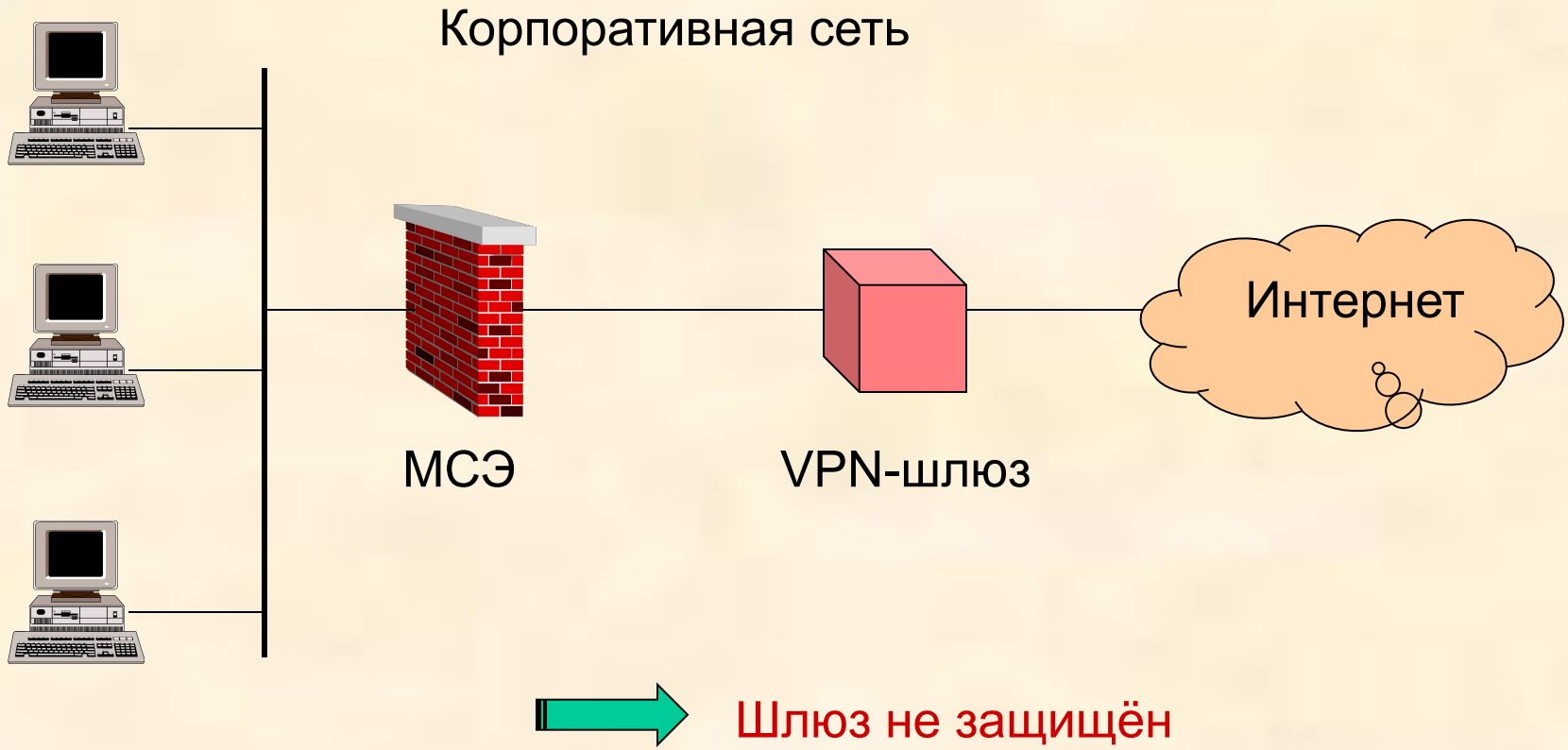
Организация VPN (провайдерская схема)



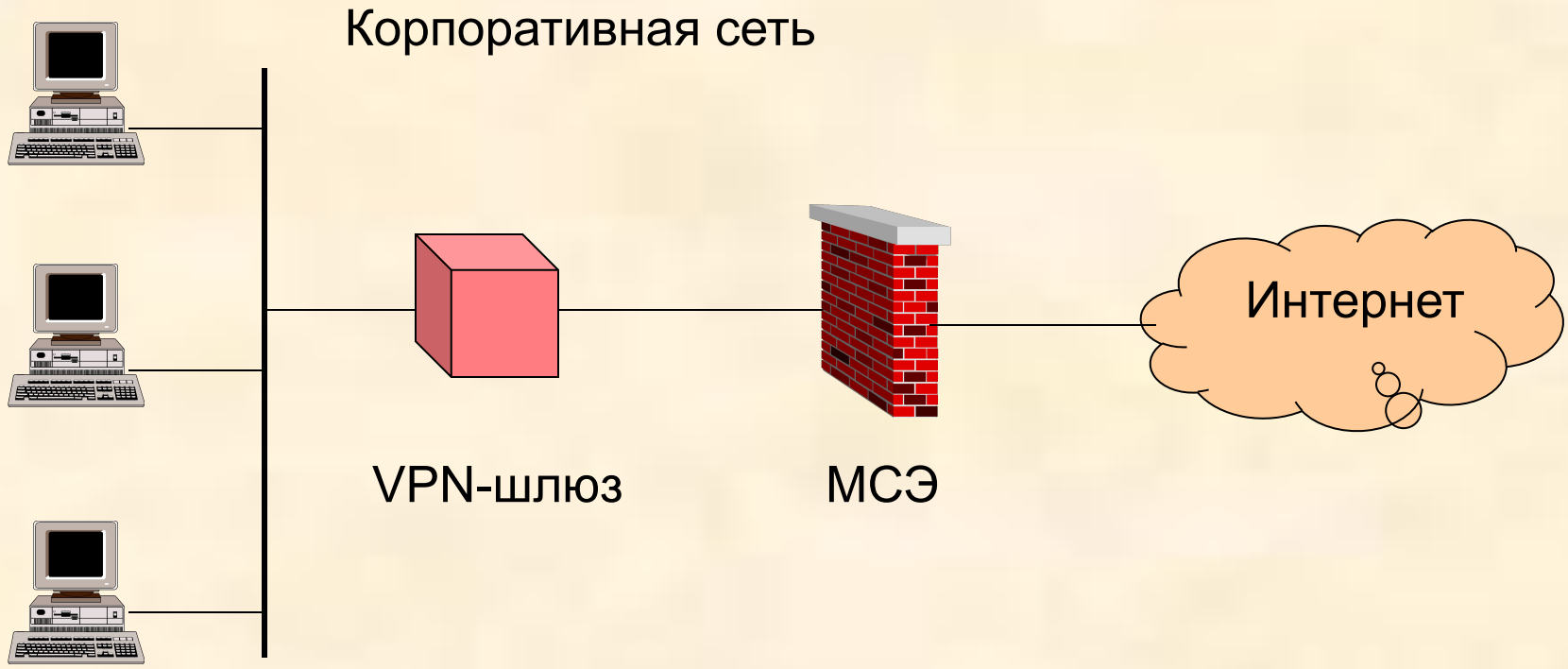
Взаимное расположение VPN-шлюза и МСЭ



Взаимное расположение VPN-шлюза и МСЭ

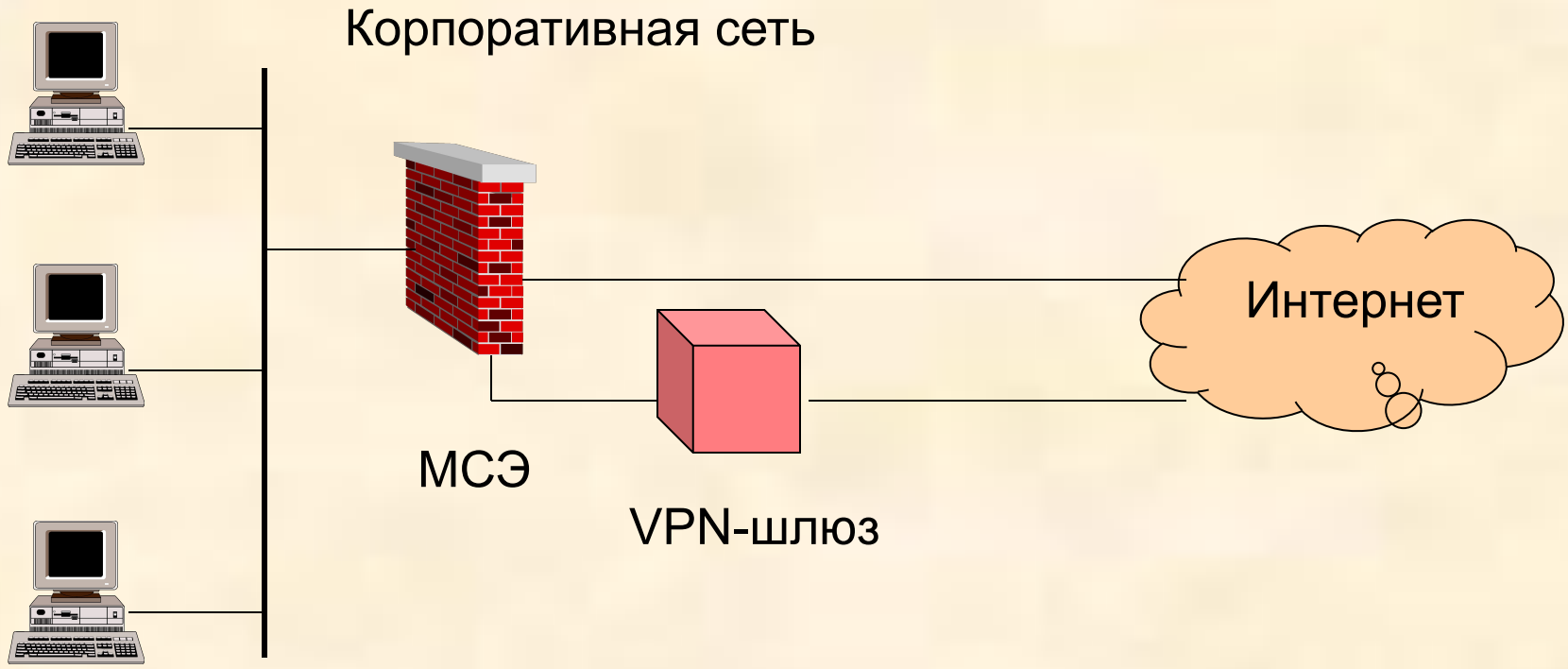


Взаимное расположение VPN-шлюза и МСЭ

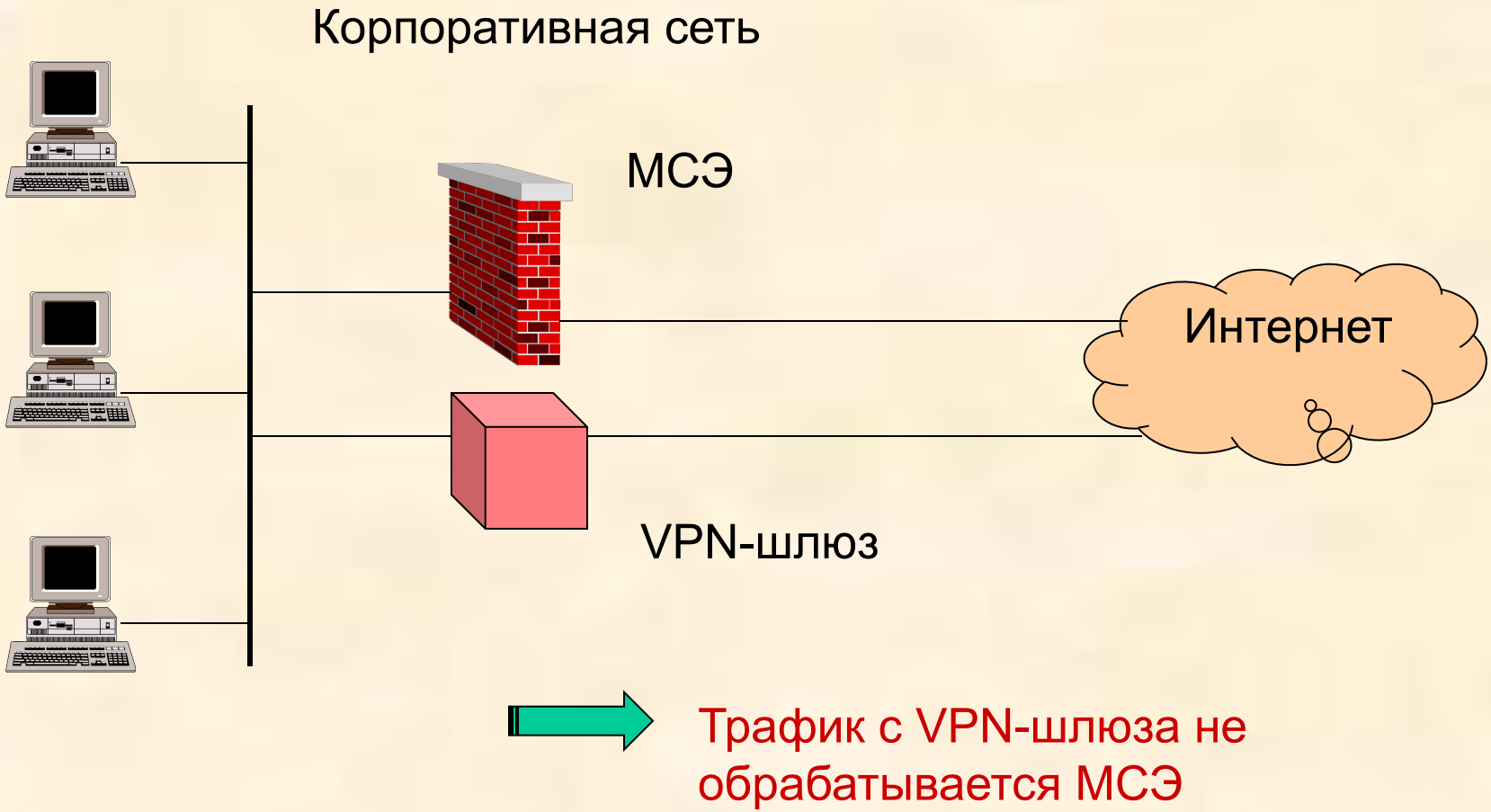


Требуется настройка МСЭ для пропуска зашифрованного трафика

Взаимное расположение VPN-шлюза и МСЭ

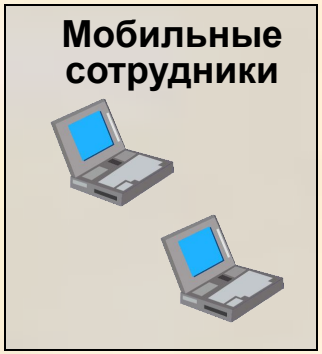


Взаимное расположение VPN-шлюза и МСЭ



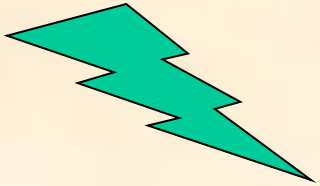
Дополнительный материал: Удаленный доступ по протоколу L2TP (RFC 2888)

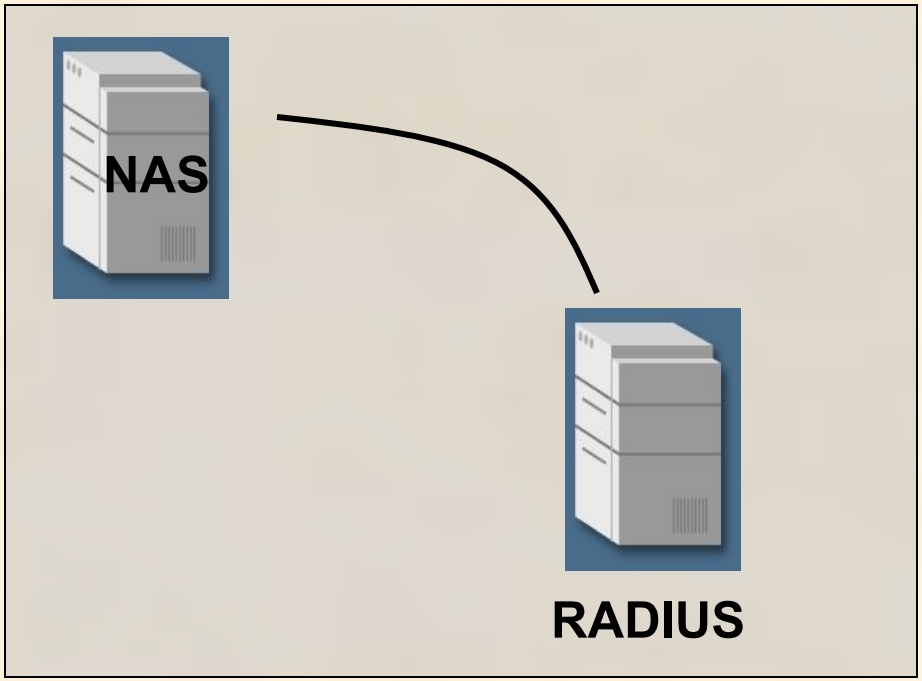
Удаленный доступ: общая схема



PPP

IP

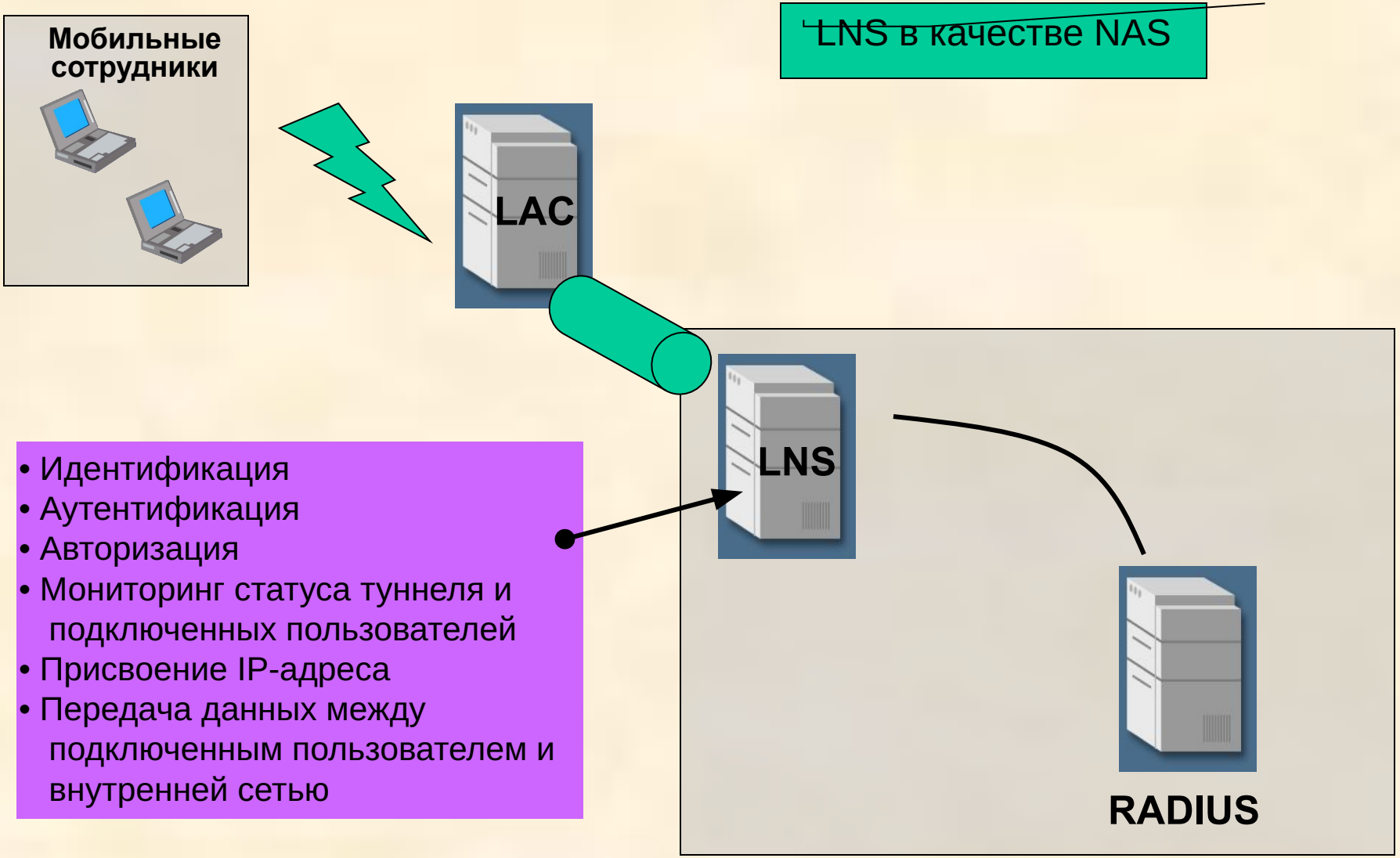




Network Access Server

- Идентификация
- Аутентификация
- Авторизация
- Мониторинг статуса подключенных пользователей

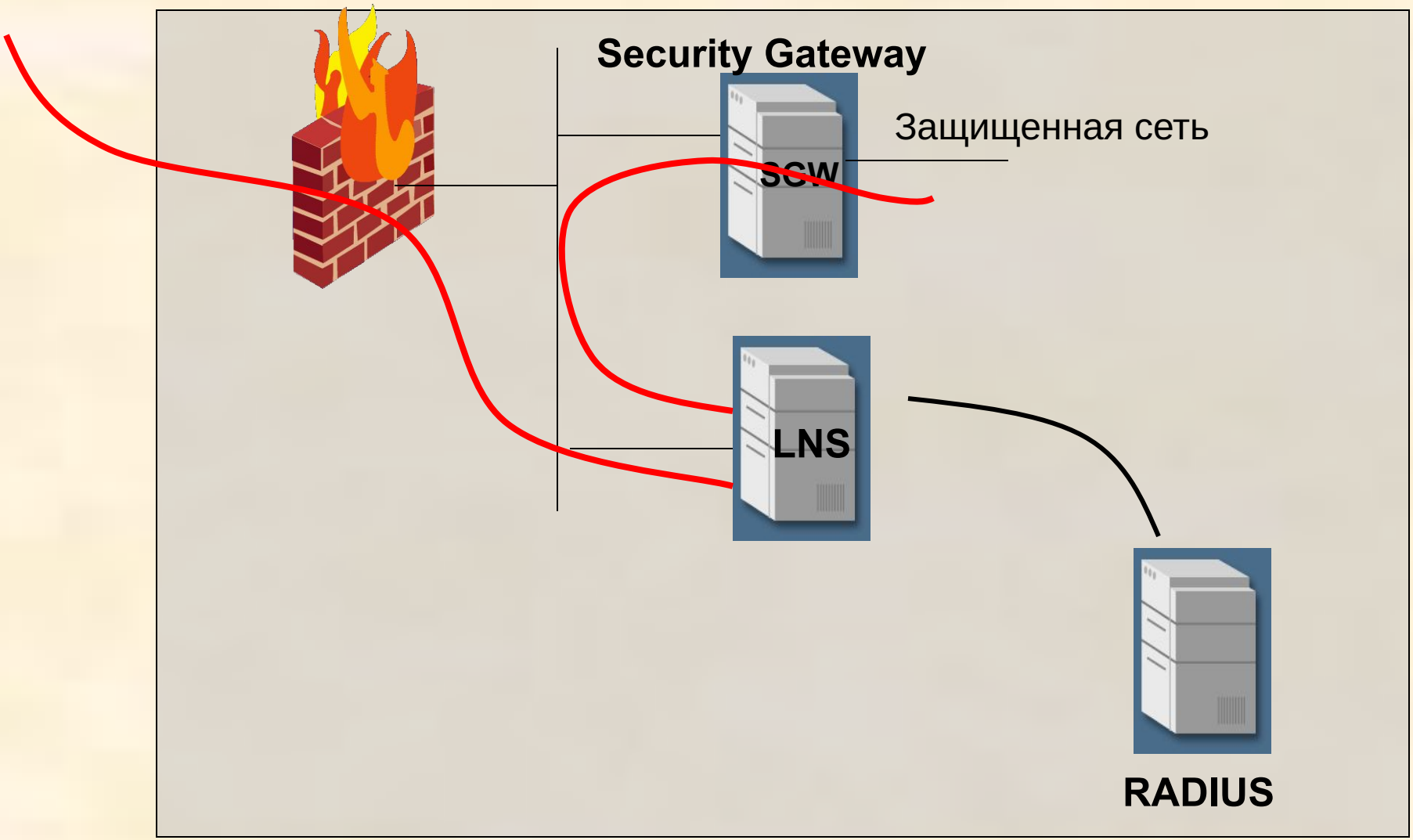
Удаленный доступ: L2TP



LNS в качестве NAS

- Идентификация
- Аутентификация
- Авторизация
- Мониторинг статуса туннеля и подключенных пользователей
- Присвоение IP-адреса
- Передача данных между подключенным пользователем и внутренней сетью

Если в сети используется IPSec



Недостатки предложенной схемы

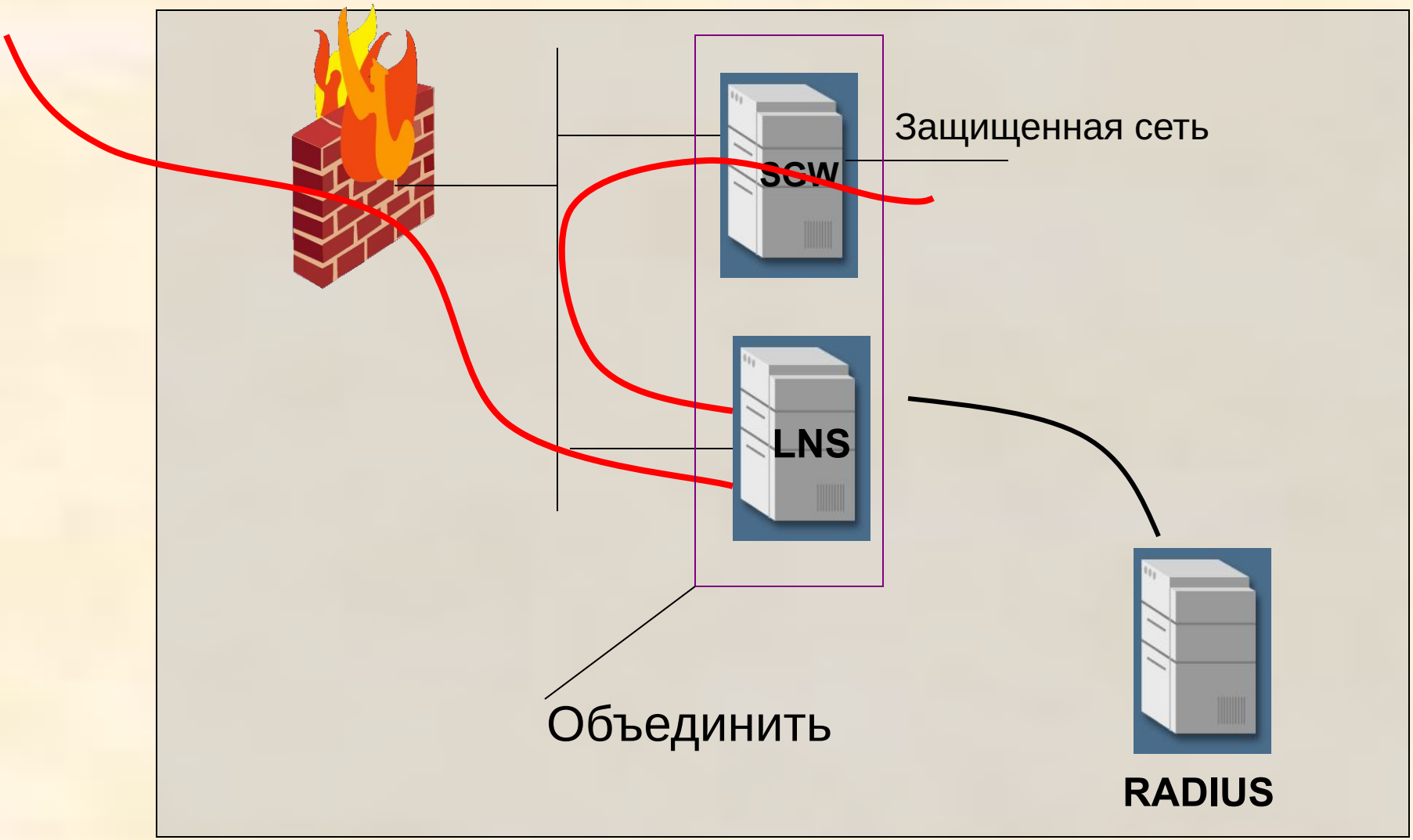
Независимые базы пользовательских бюджетов для SGW и LNS

Необходимость настройки маршрутизации на участке:

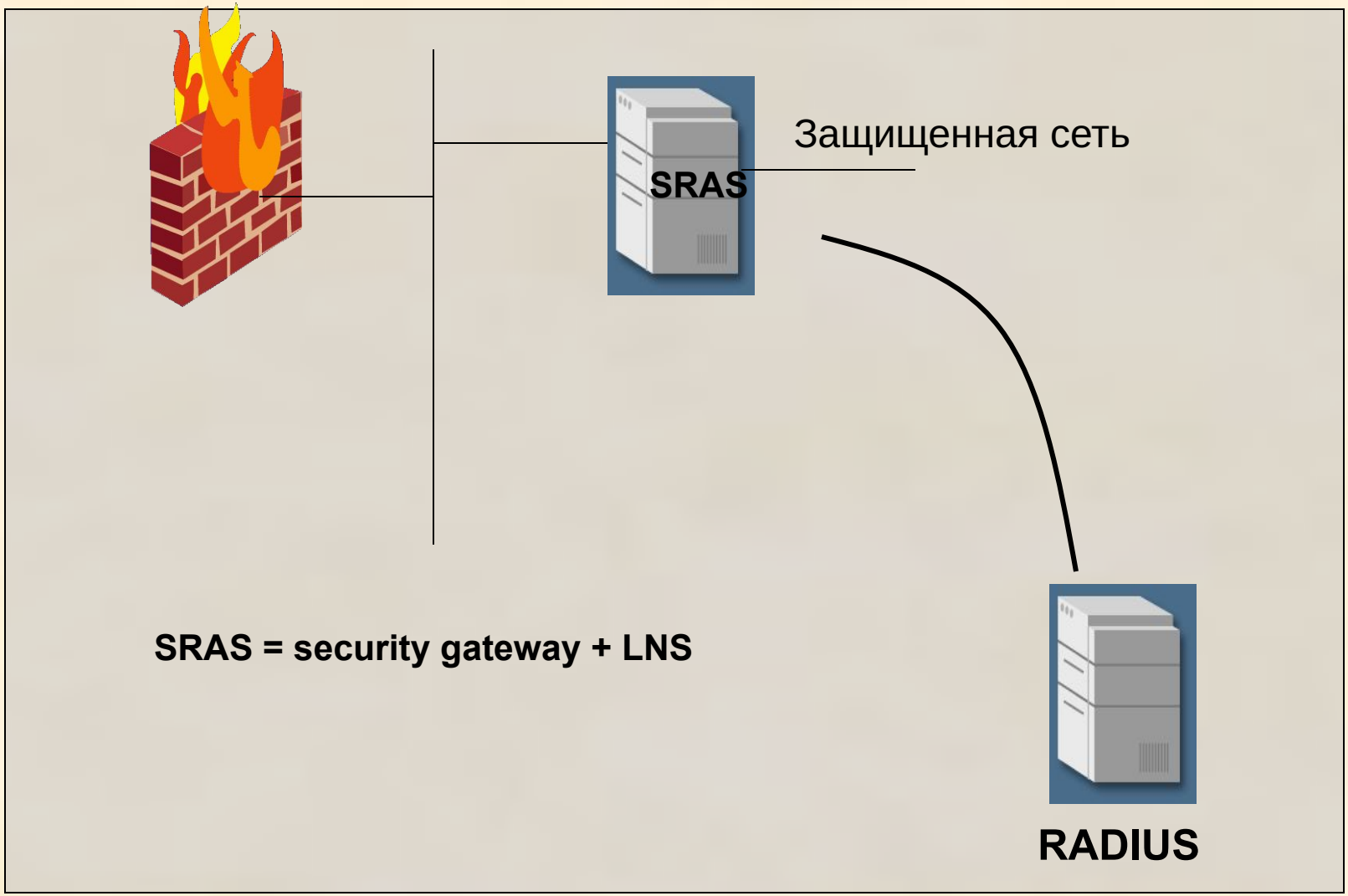
SGW – LNS – Удаленный пользователь

SGW не может контролировать статус туннеля и статус подключившихся пользователей

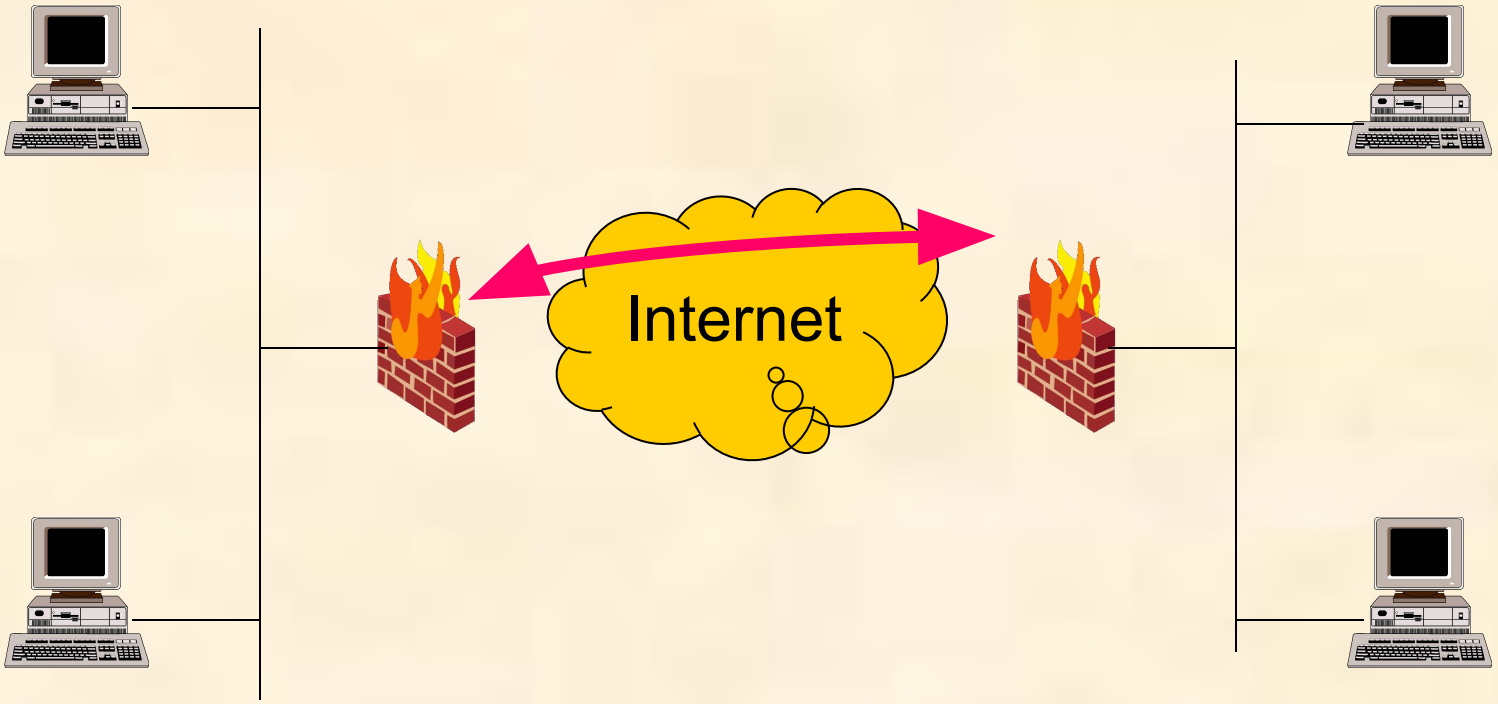
Решение



Secure Remote Access Server

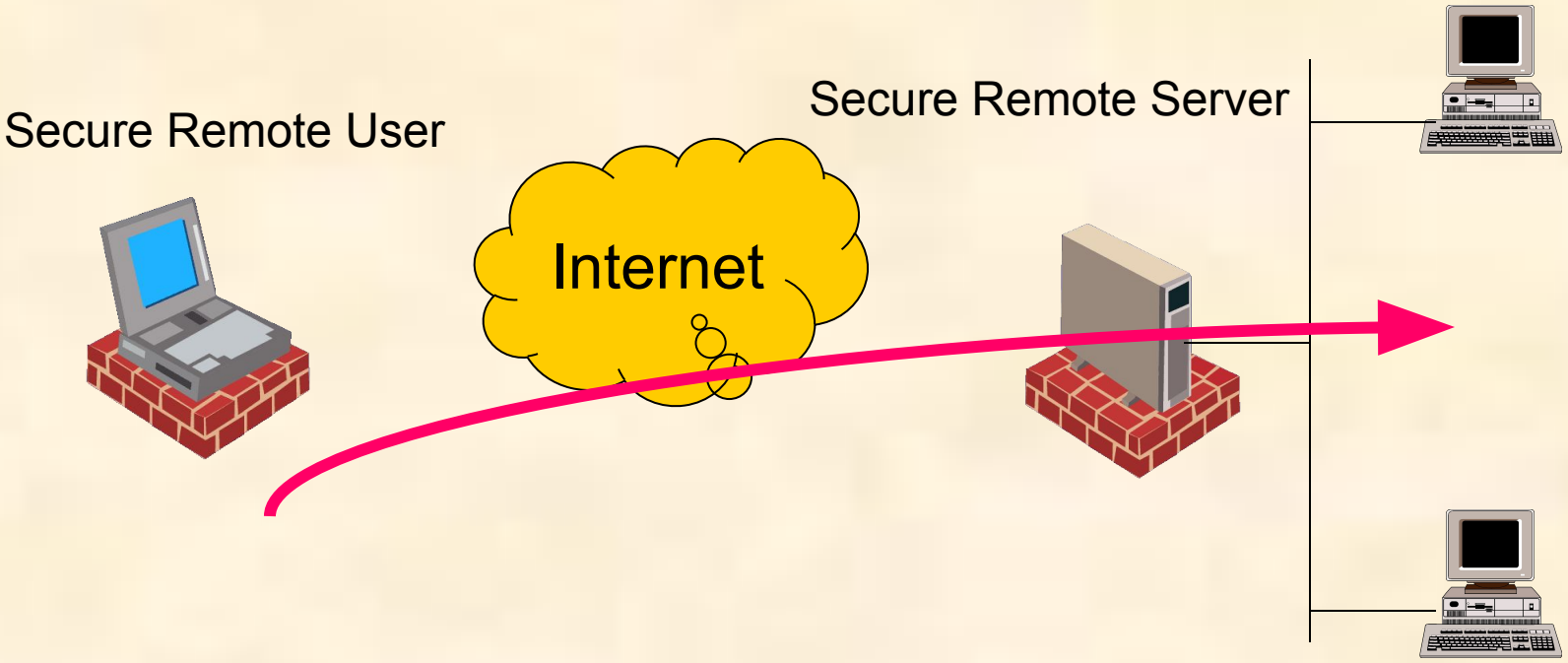


Решения на базе МЭ CheckPoint



Шлюз – шлюз (Site-to-site)

Решения на базе МЭ CheckPoint



Пользователь – шлюз (Client-to-site VPN)

Решения на базе МЭ CheckPoint

- **IKE (с поддержкой PKI)**

Схемы управления ключами

Решения на базе МЭ CheckPoint

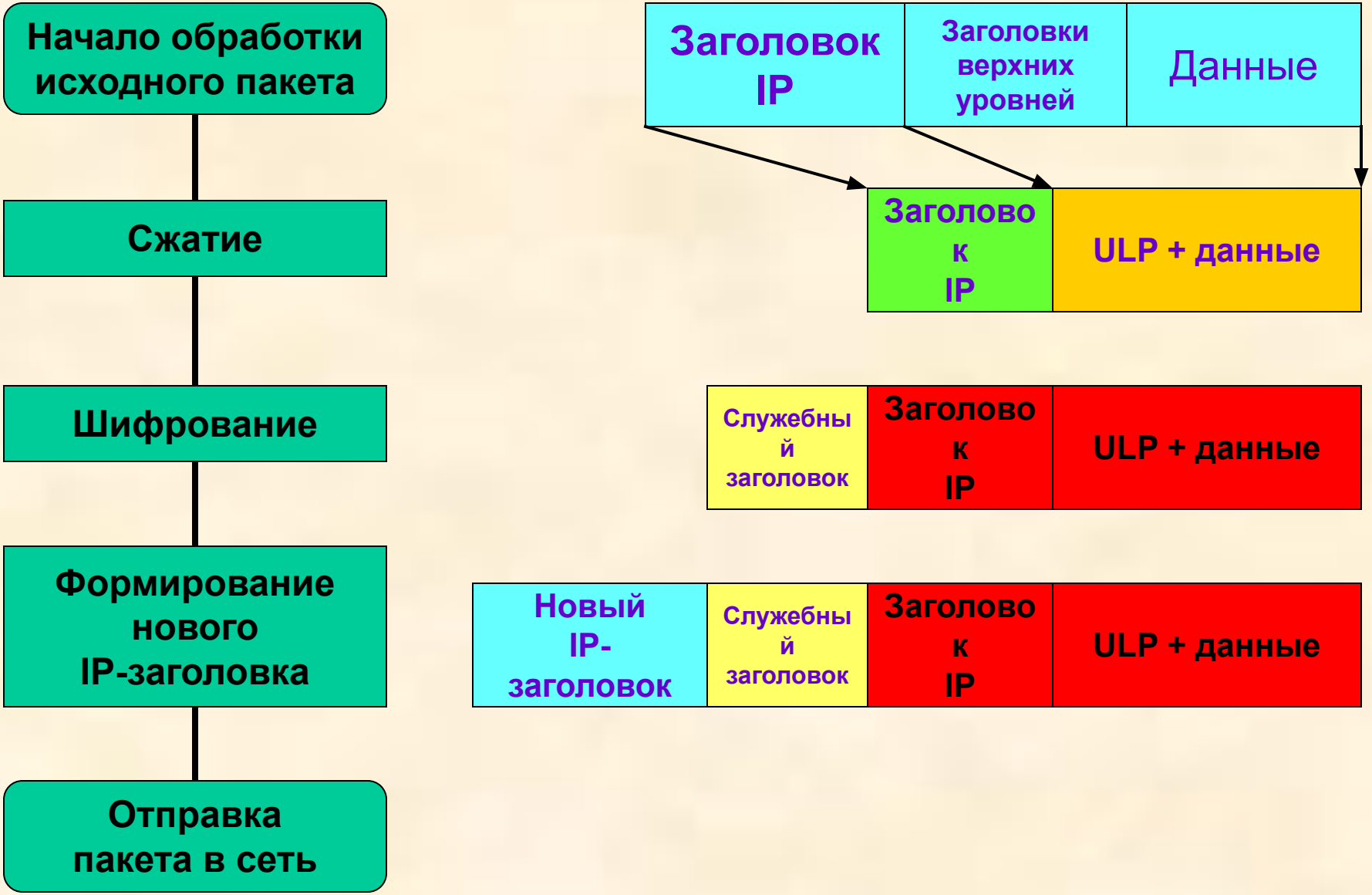
- **DES**
- **Triple DES**
- **CAST**
- **AES (128/256)**

Алгоритмы шифрования

Решения на базе МЭ CheckPoint

Вид VPN	Тип VPN в CheckPoint
Intranet VPN	Site-to-site
Extranet VPN	Site-to-site
Remote Access VPN	Client-to-site VPN

Решение на базе «Континент-К»



Решение на базе «Континент-К»