Принципы работы компьютерных сетей

Компьютерные сети

10.6.1.4 объяснять назначение частной виртуальной сети

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.

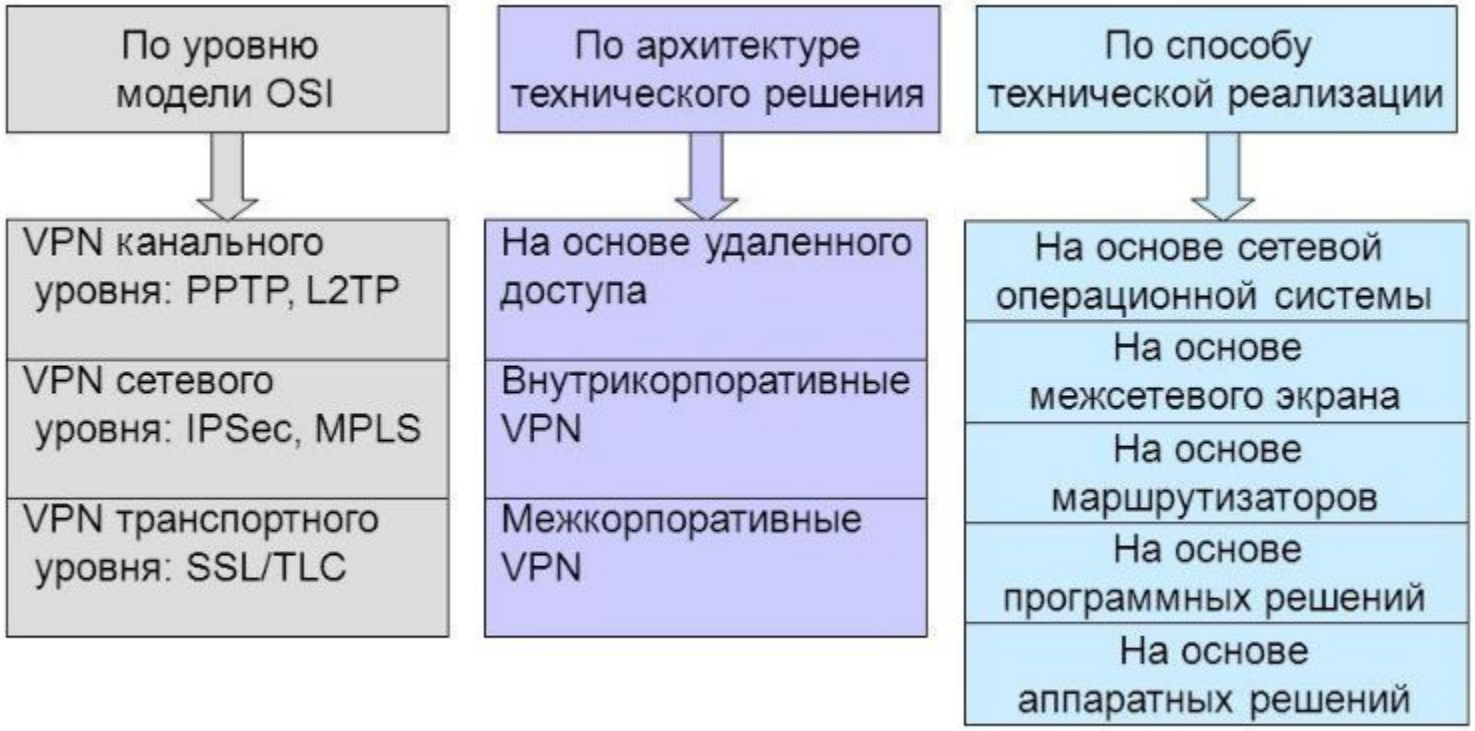
Цель VPN-технологий состоит в максимальной степени обособления потоков данных одного предприятия от потоков данных всех других пользователей сети общего пользования. Обособленность должна быть обеспечена в отношении параметров пропускной способности потоков и в конфиденциальности передаваемых данных.

История зарождения VPN

История зарождения VPN уходит своими корнями далеко в 60-е годы прошлого столетия, когда специалисты инженерно-технического отдела нью-йоркской телефонной компании разработали систему автоматического установления соединений абонентов АТС – Centrex (Central Exchange). Другими словами это не что иное, как виртуальная частная телефонная сеть, т.к. арендовались уже созданные каналы связи, т.е. создавались виртуальные каналы передачи голосовой информации. В настоящее время данная услуга заменяется более продвинутым ее аналогом – IP-Centrex.

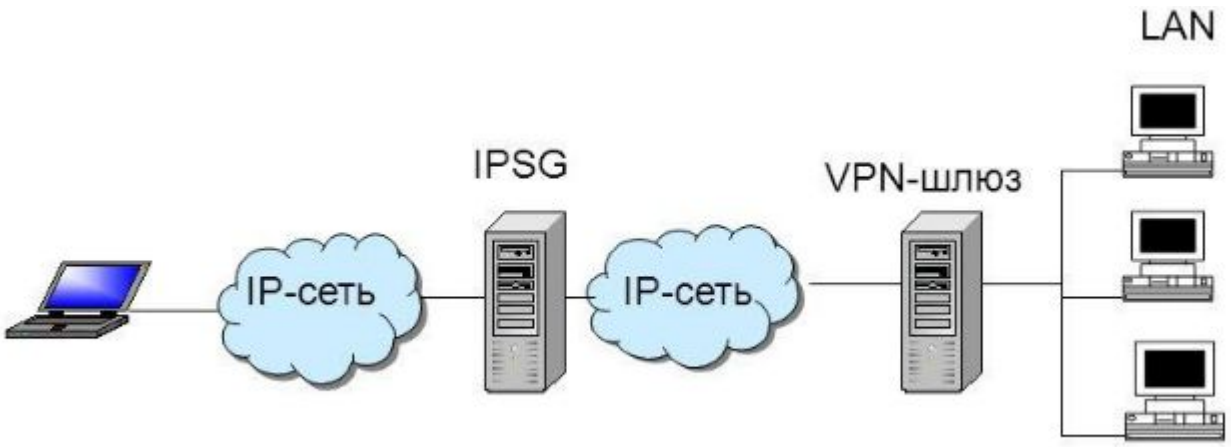
a) 1998 год – разработка приложений VPN, позволяющих осуществлять централизованный контроль со стороны пользователей
b) 1999 год – модель аутентификации, дополнительные средства для конфигурирования клиентов
c) 2000 год – включение средств VPN в Windows2000
d) В настоящее время технология вошла в фазу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

Классификация VPN



Базовые архитектуры VPN

a) Шлюз-шлюз
b) Шлюз-хост
c) Хост-хост
d) 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, брандмауэр или система NAT.

Обеспечение безопасности информации VPN – ряд мероприятий по защите трафика корпоративной сети при прохождении по туннелю от внешних и внутренних угроз.

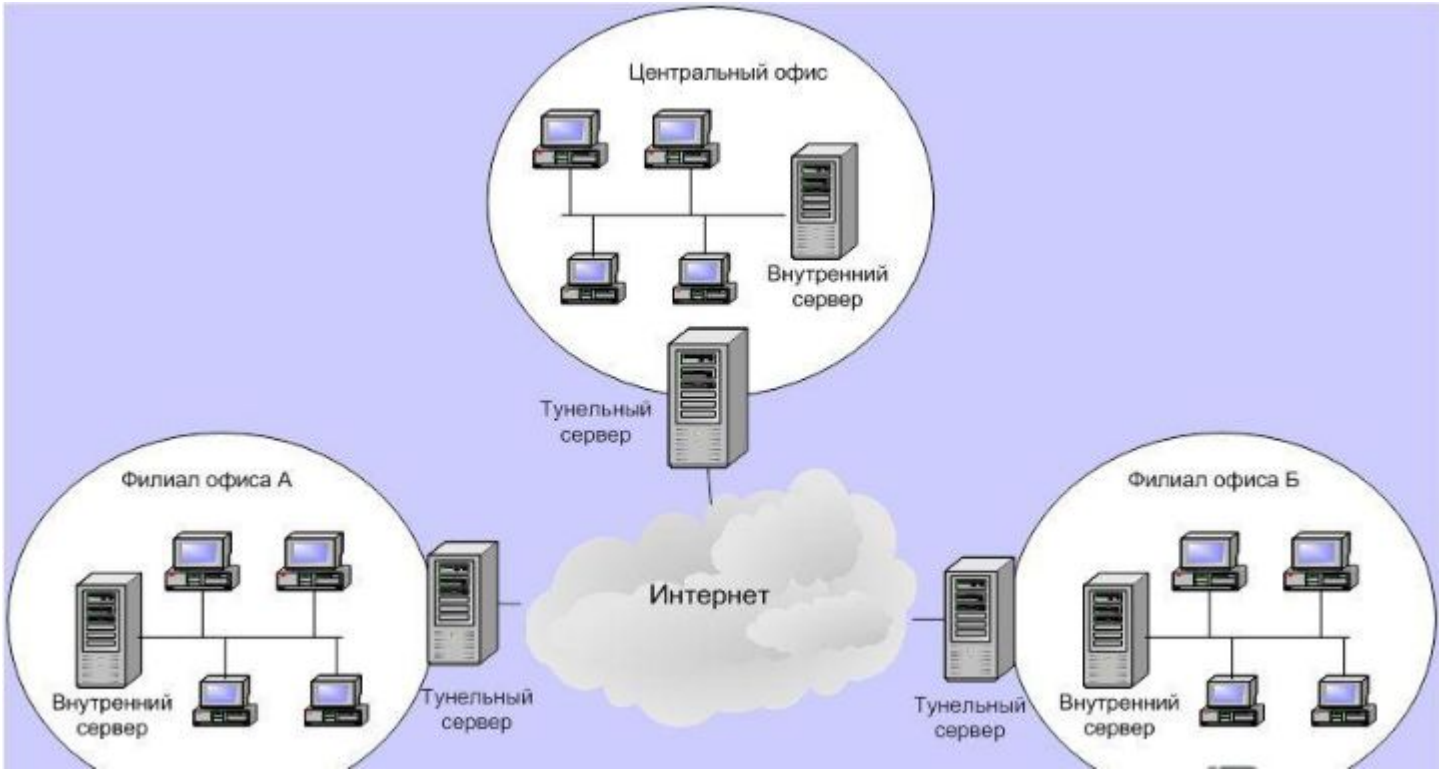
Схемы взаимодействия провайдера и клиента

Пользовательская схема – оборудование размещается на территории клиента, методы защиты информации и обеспечения QoS организуются самостоятельно.

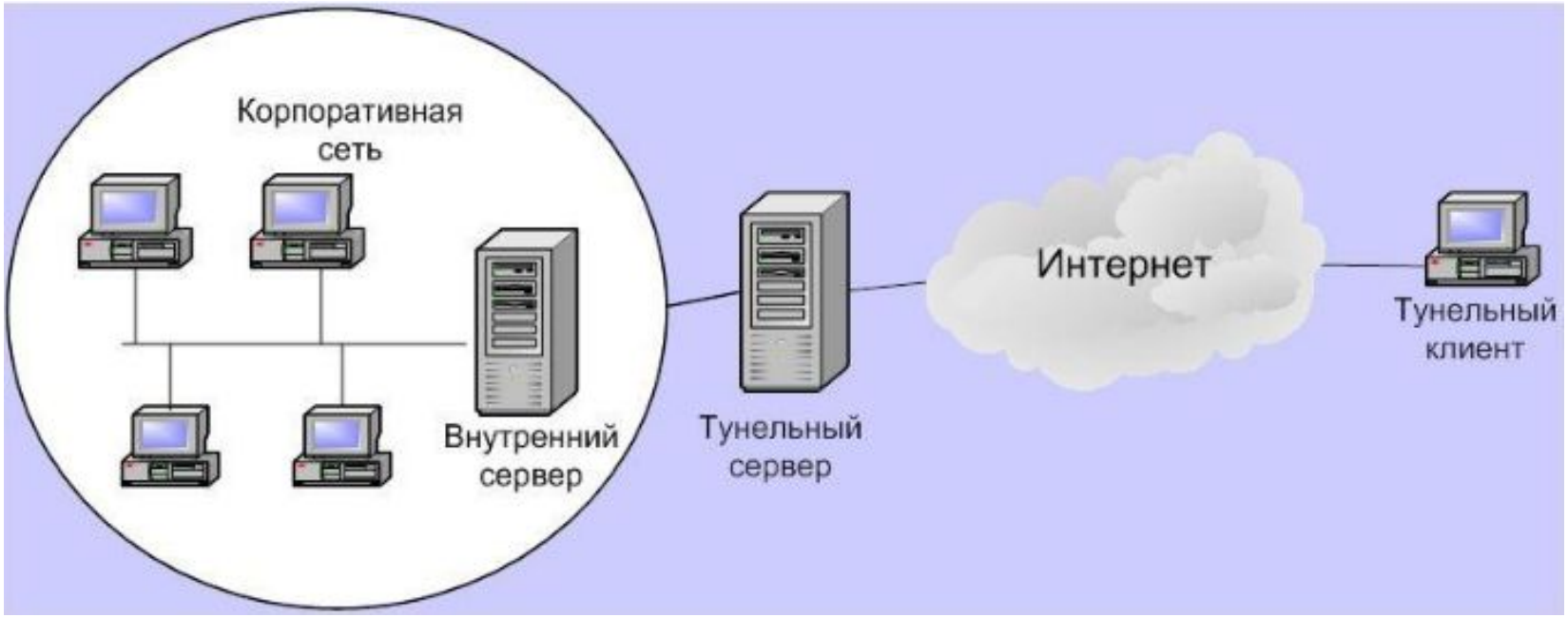
Провайдерская схема – средства VPN размещаются в сети провайдера, методы защиты информации и обеспечения QoS организуются провайдером.

Смешанная схема – используется при взаимодействии клиента с несколькими провайдерами.

Схема соединения филиалов с центральным офисом

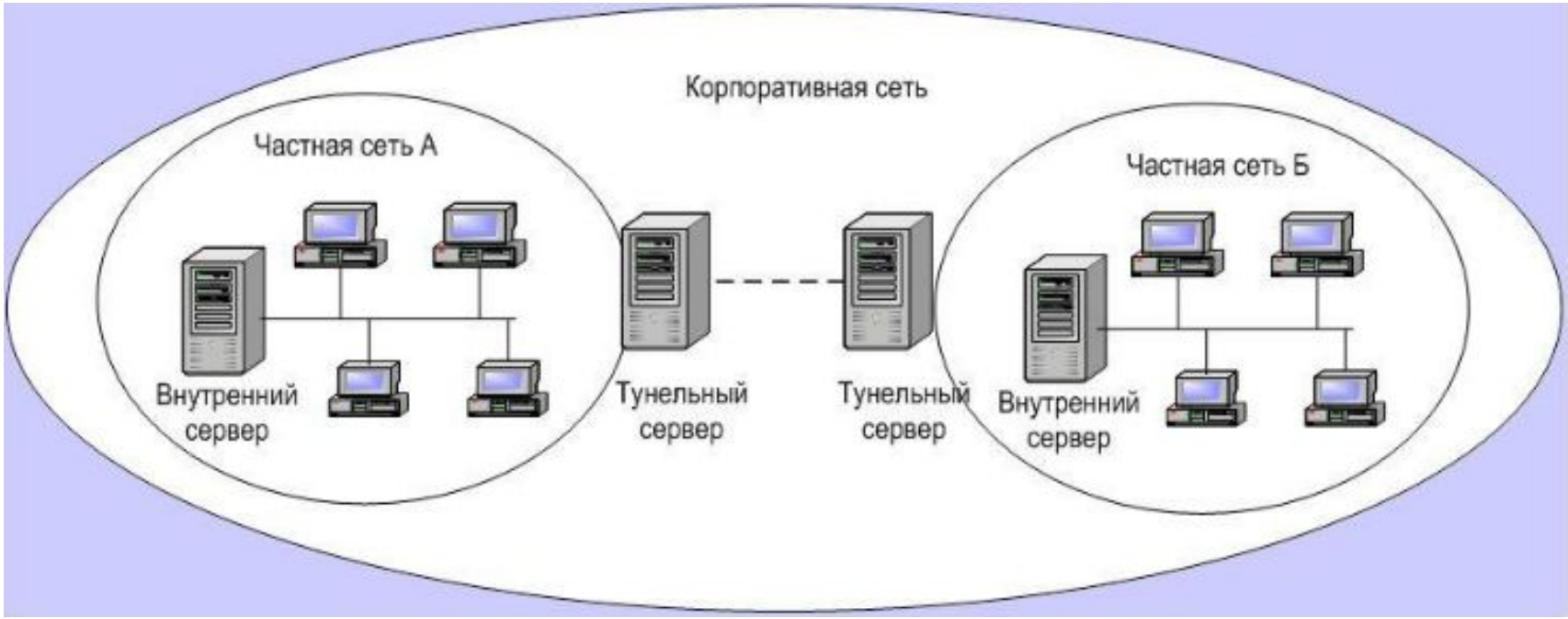


Связь удаленного пользователя с корпоративной сетью

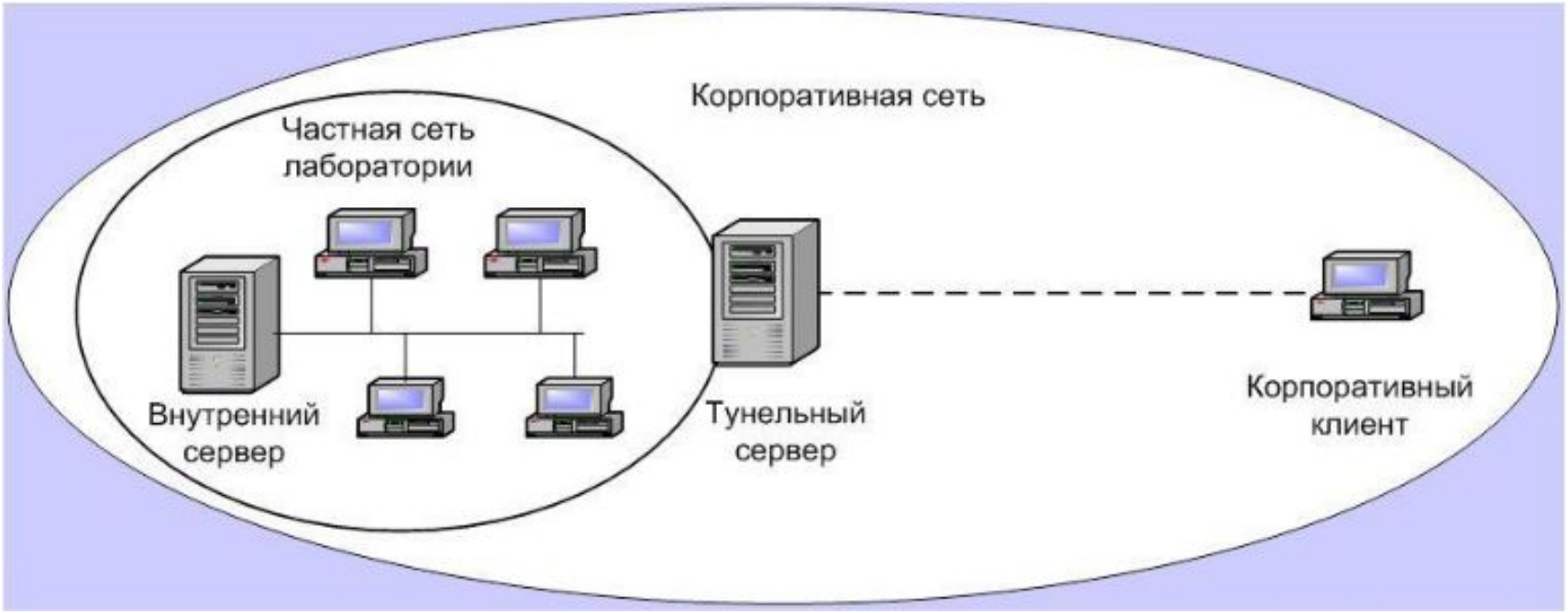


Организация туннеля через провайдера Internet, поддерживающего службу VPN

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:

a) Конфиденциальность
b) Целостность
c) Доступность легальным пользователям (аутентификация)

Методы организации защищенного канала:

a) Шифрование.
b) Аутентификация – позволяет организовать доступ к сети только легальных пользователей.
c) Авторизация – контролирует доступ легальных пользователей к ресурсам в объемах, соответствующих предоставленными им правами.
d) 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)

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