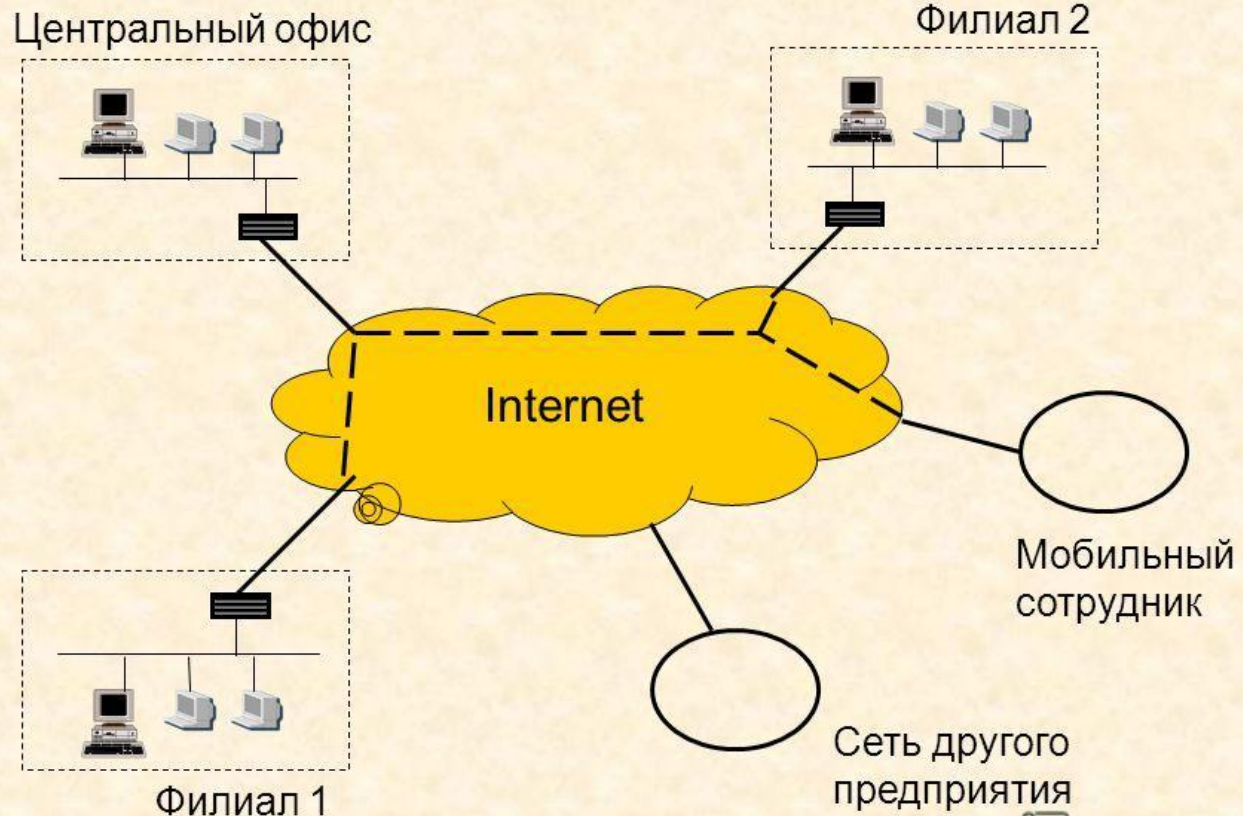


VPN



VPN-соединение корпоративного клиента с защищенной сетью внутри корпоративной сети

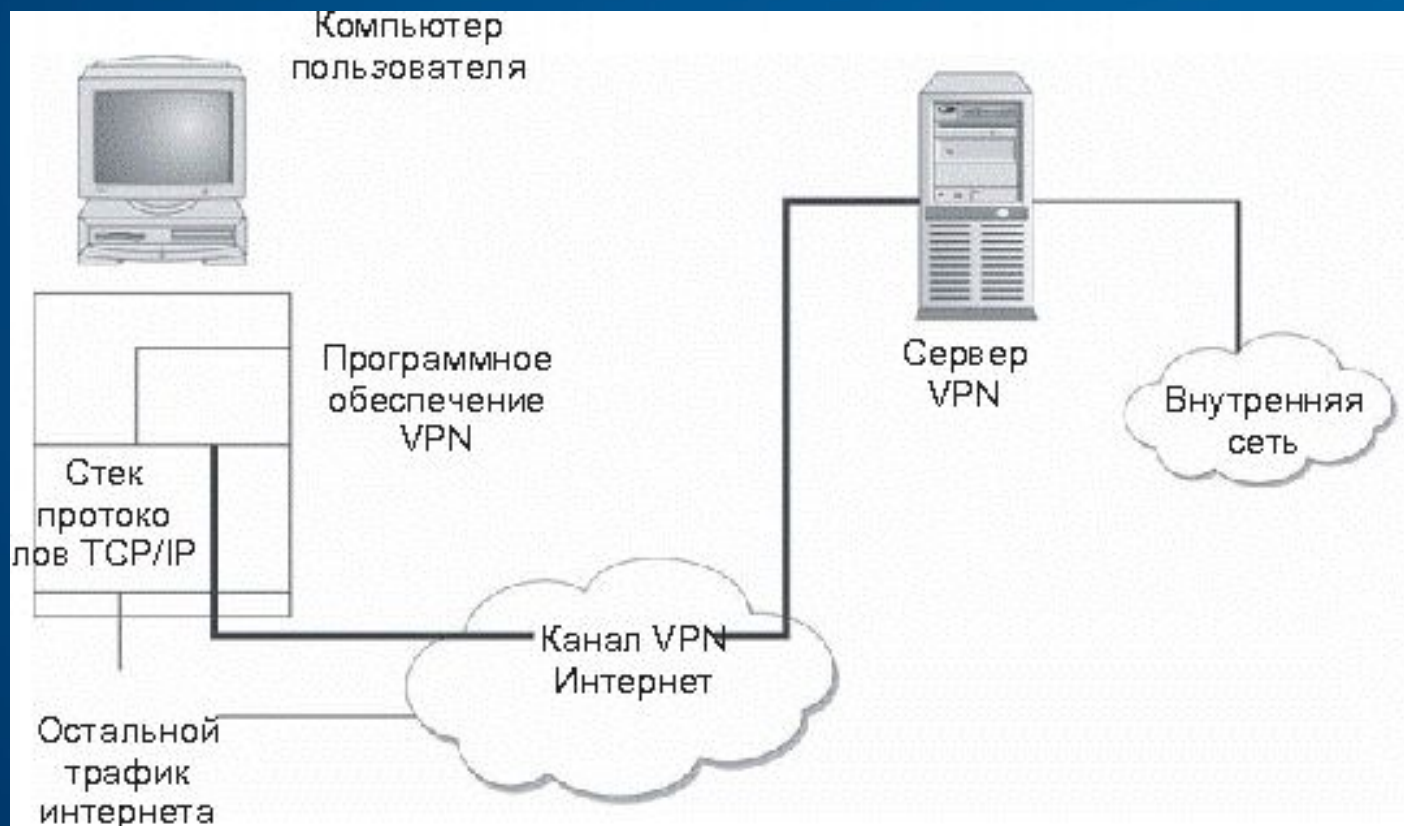
Организация VPN через общую сеть



Виртуальные частные сети (VPN)

- Существуют различные виды реализации VPN - туннелирования:
 - VPN на базе маршрутизаторов;
 - VPN на базе сетевых операционных систем;
 - VPN на базе межсетевых экранов;
 - VPN на базе специализированного программного обеспечения.

Принципиальная схема виртуальной частной сети



Протоколы создания виртуальных частных сетей

Для создания сетей VPN разработано множество протоколов. Каждый из ЭТИХ протоколов обеспечивает определенные возможности VPN:

- Протокол IPSec (IP Security) – представляет собой основанный на стандартах набор протоколов и алгоритмов защиты. IPSec действует на сетевом уровне, обеспечивая защиту и аутентификацию пакетов IP, пересылаемых между устройствами (сторонами) IPSec.
- Протокол GRE (Generic Routing Encapsulation). Разработанный Cisco туннельный протокол, обеспечивающий инкапсуляцию многих типов протокольных пакетов в туннели IP, создает виртуальную двухточечную связь с маршрутизаторами Cisco в удаленных точках IP-сети.
- Протокол L2F (Layer 2 Forwarding). Разработанный Cisco туннельный протокол, который позволяет создать сеть VPDN (Virtual Private Dialup Network), распространяющихся на удаленные домашние офисы, которые кажутся при этом непосредственной частью сети предприятия.

VPN

Туннелирование обеспечивает передачу данных между двумя точками — окончаниями туннеля — таким образом, что для источника и приемника данных оказывается скрытой вся сетевая инфраструктура, лежащая между ними. Транспортная среда туннеля, как паром, подхватывает пакеты используемого сетевого протокола у входа в туннель и без изменений доставляет их к выходу.

Однако нельзя забывать, что на самом деле «паром» с данными проходит через множество промежуточных узлов (маршрутизаторов) открытой публичной сети. В связи с этим возникают две проблемы. Первая заключается в том, что передаваемая через туннель информация может быть перехвачена злоумышленниками. Вторая проблема состоит в том, что злоумышленники имеют возможность модифицировать передаваемые через туннель данные так, что получатель не сможет проверить их достоверность.