**VPN** - обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети

VPN базируется на 3 методах - Тунелирование, Шифрование, Аутентификация.  
В сети должен быть 1 узел, который светится в интернете, и другие узлы могут подключиться к нему. Узел перенаправляет уже хосты куда нужно

* **PPTP (Point-to-Point Tunneling Protocol) (1723 порт)** –не особо секьюрный VPN
* **L2TP (Layer 2 Tunneling Protocol) (1701 порт)** –Главное достоинство L2TP состоит в том, что этот протокол позволяет создавать туннель не только в сетях IP, но и в таких, как ATM, X.25 и Frame Relay
* **SSL**
  + **SSTP (Secure Socket Tunneling Protocol) (443 порт)** –VPN тунель идущий внутри TLS тунеля
* **IPSec (IP Security)** –набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном, применяется для организации VPN-соединений
  + **IKEv2 (**стандартный протокол набора протоколов **IPsec**)

Что бы подключиться к VPN этих типов, можно это сделать напрямую из ОС используемой системы. Так же мы можем использовать сторонние прилаги – OpenVPN, Cisco AnyConnect, …Если VPN настроен через них

Так же для подключения к VPN, нужно что бы на роутере была включена опция passthrough L2TP/PPTP/IPSec, а так же провайдер должен поддерживать эти протоколы

**Что такое Виртуальная частная сеть (VPN)?**

Раньше для осуществления безопасной передачи данных возникала необходимость в выделенной линии, связывающей два пункта. Расходы на организацию таких линий довольно велики.   
Виртуальная частная сеть дает пользователям безопасный способ доступа к ресурсам корпоративной сети через Интернет или другие общественные или частные сети без необходимости выделения линии.

Безопасная частная виртуальная сеть представляет собой совокупность технологий/служб туннелирования, аутентификации, управления доступом и контроля, используемых для защиты данных и передачи трафика через Интернет.

Существует много причин для использования виртуальных частных сетей. Наиболее типичны следующие из них:

**Безопасность** (защита данных).   
С помощью аутентификации получатель сообщения, являющийся пользователем виртуальной частной сети, может отслеживать источник полученных пакетов и обеспечить целостность данных.   
С средств защиты данных в виртуальных частных сетях гарантируется конфиденциальность исходных пользовательских данных.

**Стоимость** (снижение количества линий доступа и уменьшение расходов на междугороднюю телефонную связь).  
Организация виртуальной частной сети позволяет компании передавать данные через линии доступа к Интернету, таким образом уменьшая необходимость в некоторых из существующих линий.   
При организации виртуальной частной сети снижаются расходы на междугороднюю телефонную связь, поскольку пользователь обычно получает услуги от местного Интернет-провайдера, а не совершает междугородний звонок для установления прямой связи с компанией.

Известно, что сети, использующие протокол IP, имеют "слабое место", обусловленное самой структурой протокола IP. Разработчики IP не намеревались обеспечивать каких-либо функций безопасности на уровне IP, а гибкость IP позволяет хитроумно использовать особенности данного протокола в целях преодоления контроля за трафиком, управления доступом и других мер безопасности. Поэтому данные в сети, использующей протокол IP, могут быть легко подделаны или перехвачены.

При туннелировании для передачи по сети протокольных пакетов сети одного типа они вставляются или инкапсулируются в протокольные пакеты другой сети. Это обеспечивает безопасность при передаче данных.

<http://zyxel.by/kb/1638>

Какими средствами можно оганизовать VPN туннель и их основные различия

Средствами Windows и сторонними средствами, например, Cisco VPN Client. Сторонние клиенты отличаются более гибкой настройкой параметров подключения.

**Cisco VPN Client**

Cisco VPN Client - программное обеспечение, устанавливаемое на персональный компьютер и предназначенное для создания IPSec-туннеля с любым сервером Cisco Easy VPN.

Клиент VPN от компании Cisco поддерживает двухфакторную аутентификацию пользователей с помощью USB-токенов или смарткарт Aladdin eToken.

**Основные возможности и характеристики Cisco VPN Client:**

* Cisco VPN Client поддерживает все операционные системы Windows, Linux, Solaris и MacOS;
* поддержка множества протоколов для построения VPN-туннеля
* поддержка токенов (**USB-ключи и смарт-карты eToken – персональное средство аутентификации и защищeнного хранения данных**)
* поддержка разных видов аутентификации
* В Cisco VPN Client отсутствуют конфликты с клиентом Microsoft L2TP/IPSec;
* Cisco VPN Client сжимает передаваемые данные;
* балансировка нагрузки и поддержка резервных VPN-шлюзов;
* централизованное управление с помощью политик (включая списки резервных VPN-шлюзов);

<http://www.lanberry.ru/cisco/nastroika-cisco-vpn-client>

**VPN от Винды**:

Для удаленной сети требуется VPN-компьютер с двумя сетевыми подключениями: одно – к публичной сети и одно – к безопасной. Microsoft обеспечивает эти функции в роли сервера маршрутизации и удаленного доступа, включенной в операционную систему Windows Server.

Клиентский компьютер в Интернете устанавливает подключение к узлу VPN и оба компьютера шифруют все данные, передаваемые между ними. Когда узел VPN получает пакет от клиента, он расшифровывает пакет и ретранслирует его в безопасную сеть. Трафик от узлов безопасной сети к клиенту проходит через компьютер VPN, который зашифровывает данные перед их передачей клиенту по публичной сети.

Можно создать несколько VPN-подключений, копируя их в папке "Сетевые подключения". Затем можно переименовать подключения и изменить их параметры. Это позволяет легко создавать различные подключения с использованием различных узлов, параметров безопасности и других параметров. Дополнительные сведения см. в разделах Создание копии сетевого подключения и Переименование сетевого подключения.