VPN是什么？VPN有什么用？新手入门指南

VPN是什么？它可以保护你上网**隐私安全**，也能用于翻墙突破防火长城的封锁，而在中国大多数人用于后者的用途。随着在线隐私问题以及互联网内容审查日趋严重，越来越多的人开始使用VPN服务。那么VPN怎么用呢？接下来本文将详细介绍。

VPN（或[虚拟专用网络](https://zh.wikipedia.org/zh/%E8%99%9B%E6%93%AC%E7%A7%81%E4%BA%BA%E7%B6%B2%E8%B7%AF)）是保护你的在线隐私，自由上网的终极工具，优质的VPN服务可以为你带来这些好处：

* 通过对你的上网**流量进行加密**，第三方无法读取你的上网内容，从而保护你的个人隐私，并绕过防火长城的封锁，使得你可以自由访问的Google、Facebook、Twitter、YouTube等网站。
* 无论你身在何处，都可以**解锁受限制的内容**，比如因地区版权限制的音视频内容，海外华人可以使用VPN观看国内音视频(网易云、B站、腾讯视频等)，也可以用于观看美区的Netflix。
* 改变你的**地理位置**，当网站或App限制特定地理位置时，这点很有用。
* 保护你的设备免受黑客攻击和公共WiFi**网络的威胁**。

除了安全和隐私问题外，推动VPN使用的另外两个因素是，观看受地区版权限制的音视频内容，和访问被封锁的网站。不仅是中国，越来越多的人使用VPN来获得安全，私密且不受限制的上网体验。

**VPN是什么？**

VPN将你的电脑/手机，与VPN服务器之间创建**加密连接**，此加密连接可以看作是受保护的“虚拟隧道”， 你可以想象成你的上网内容在一根虚拟的管道中传输， 通过它你可以在线访问所有内容，任何人都无法窥视你的内容。这为你提供了高级别的在线匿名性以及安全性，并允许你不受限制地访问网站。

如果没有VPN，则你在线进行的所有操作都可以通过设备的[IP地址](https://zh.wikipedia.org/wiki/IP%E5%9C%B0%E5%9D%80)追溯到你的实际位置和所使用的设备 。从计算机到手机和平板电脑，每个连接到互联网的设备都有一个唯一的IP地址。通过使用VPN将会隐藏你的真实位置和IP地址，这个IP地址将由你正在使用的VPN服务器代替，IP地址就好比你家的门牌号，不知道你家的门牌号，也就无法查到你家的水表。

大多数VPN提供商在**全球都部署**有服务器，这为你提供了许多服务器选择，并可以访问全球任何地方的内容。购买VPN服务并下载该设备的软件之后，你可以立即连接到这些全球服务器中的任何一个，从而改变你实际的IP地址，在互联网的世界里，你就相当于穿越到了世界的另外一个角落，你就绕过了地理限制和防火长城。

如果你有兴趣，可以阅读有关VPN的其他内容：

* [翻墙](https://qiangwaikan.com/gfw/) -关于翻墙和科学上网的详细介绍。
* [中国VPN推荐](https://qiangwaikan.com/best-vpn-china/) -详细测评在中国好用的VPN服务商。

**为什么要使用VPN？**

为什么全世界越来越多的人使用VPN服务？这确实取决于你使用VPN的初衷，使用VPN的原因有很多：

* 防止运营商（[ISP](https://zh.wikipedia.org/wiki/%E4%BA%92%E8%81%94%E7%BD%91%E6%9C%8D%E5%8A%A1%E4%BE%9B%E5%BA%94%E5%95%86)）、第三方、网络管理员窥视你的上网内容，并且**绕过防火长城**的审核机制。
* **隐藏你的真实IP**地址和地理位置，使你能够匿名浏览互联网内容。
* 通过加密你的互联网连接来**增加安全级别**。
* **解锁地区限制**，观看仅限于某些地理位置的网站内容。
* 种子下载，P2P下载和流媒体。
* 更改IP地址（地理位置），获得一些上网便利。
* 随时随地保护自己**免受黑客攻击**，尤其是在咖啡馆、酒店和机场使用公共WiFi时。
* 保护你的私人数据，例如银行密码、信用卡、照片和其他个人信息。

虽然使用VPN的好处这么多，当然你可能更感兴趣的，还是使用VPN翻墙，接下来我将介绍一下具体步骤：

**怎么用VPN翻墙？**

使用VPN进行翻墙非常简单，有很多VPN服务商提供了非常好用的VPN软件，你只需要付费购买之后，下载他们提供的软件进行安装即可使用。

接下来我将以[Panda VPN](https://qiangwaikan.com/go/panda)为例，介绍以下具体流程。Panda VPN是一款使用简单的VPN，并且中文支持很好，非常适合入门使用。

第一步：创建账户

首先进入[Panda VPN官网](https://qiangwaikan.com/go/panda)，选择”购买”之后，就会跳转到购买页面。这里首先设置邮箱和密码，注意一定不要把邮箱填写错了，请再三检查，免得后面麻烦。

第二步：选择套餐

接下来可看到Panda VPN提供的几种不同时长的套餐，根据自己的需求进行选择。

第三步：选择支付方式

Panda VPN提供的支付方式有很多，当然肯定使用支付宝最方便。

第四步：下载客户端

注册之后，可以点击顶部的”下载”按钮，可以看到Panda VPN为用户提供不同设备的客户端应用程序，下载之后进行安装，安装过程就是点击”下一步”，没有什么难点。

第五步：开始翻墙

完成以上步骤之后，你就可以开始翻墙上网了，Panda VPN提供了很多服务器节点，首先尝试推荐节点，其他的可以慢慢研究，比如Netflix专用节点、低延迟游戏节点等等。

当然，市面上VPN数不胜数，并不是每款VPN都那么好用。如果你刚接触VPN，可能很难分辨好坏。参考[翻墙软件测评](https://qiangwaikan.com/best-vpn-china/)，获取详细测试结果和排名。

**使用VPN合法吗？**

答案显而易见，使用VPN属于违法行为。当然，我们也**不必惊慌**，因为在国内使用VPN的大有人在，不可能全都进行处罚。如果你使用VPN只是用于工作和学习，而不是在网络上发表反动言论，那么大可不必担忧。

现在国外网站上关于中国的负面言论很多，但我们应该理性的去看带，而不是国外的媒体带偏了节奏，更不要将这些反动言论在网络上发表。这也是防火长城成立的原因，中国人口众多，一旦一些不负责任的负面言论占据了上风，很可能会引起社会的不稳定。

所以，如果大家以后掌握了科学上网的方法之后，请用于工作和学习。

**VPN安全吗？**

通常，只要你使用的是高质量VPN服务，VPN都是安全使用的。

根据我对GooglePlay和App Store的调查发现，当前市场上可能有300多种VPN。不幸的是，大多数VPN服务都不太好用，这些都会威胁到你的安全和隐私，并且无法在中国使用，换句话说，好用的VPN可能并不多。

一项有趣的研究发现，84％的免费安卓VPN应用会泄漏用户数据。尽管大多数人都知道应该避免使用免费的VPN，但仍有很多人使用这些危险的应用程序。正如我在[免费VPN](https://qiangwaikan.com/free-vpn/)使用指南中所介绍的，不建议使用免费VPN的原因有很多：

* 恶意软件植入（在免费VPN应用程序中很常见）
* 收集个人数据（许多流行的VPN提供商在应用程序中隐藏收集你的个人数据）
* 占用带宽流量，降低网络速度
* 浏览器劫持
* 流量泄漏（IP地址泄漏，DNS泄漏）
* 欺诈（身份盗用和财务欺诈）

加密和VPN同样如此。银行，企业和任何处理敏感数据的网站都必须每天使用加密技术，以确保人员（及其数据）的安全。VPN和加密是我们所有人都需要使用的必要工具，即使有些人出于自身原因滥用此技术。

**VPN协议和加密**

VPN协议到底是什么？VPN协议可以理解成是一种规则，用于在设备和VPN服务器之间**交换信息**。这有点像人类交流所用的语言，两个人之间如果使用同一种语言，就能听懂对方的话，对使用其他语言的人来说，他们无法听懂你们的话。这就好比设备和服务器之间，建立了安全且加密的连接以传输数据。

以下是目前使用的最多并且最受欢迎的VPN协议，这部分内容可能非常枯燥，非战斗人员请迅速跳过，继续往下看：

VPN协议

* **OpenVPN** – OpenVPN仍然是最流行，最安全的[VPN协议](https://qiangwaikan.com/vpn-protocol/)，可以在所有类型的不同设备上使用。OpenVPN是为多种身份验证方法开发的开源项目，它是一种非常通用的协议，可以在具有不同功能的许多不同设备上使用，并可以通过UDP或TCP在任何端口上使用。OpenVPN使用[OpenSSL](https://zh.wikipedia.org/zh-hans/OpenSSL)库和TLS协议提供出色的性能和强大的加密。
* **IKEv2/IPSec** – IKEv2/IPSec是一种快速且 安全的VPN协议。它已在许多操作系统（例如Windows，Mac OS和iOS）中自动进行了预配置。它对于重新建立连接非常有效，特别是与移动设备建立连接时。缺点是IKEv2是由Cisco和Microsoft开发的，不是像OpenVPN这样的开源项目。IKEv2 / IPSec是轻量级VPN，在暂时中断时可以安全的快速重新连接，对移动用户来说是绝佳选择。
* **L2TP/IPSec**–L2TP/IPSec协议也是一个不错的选择。该协议比PPTP更安全，但是由于数据包是双重封装的，因此它加密速度可能会较慢。它通常与移动设备一起使用，并内置在许多操作系统中。
* PPTP –点对点隧道协议是一种基础的VPN协议，内置在许多操作系统中。不幸的是，PPTP具有已知的安全漏洞，并且出于隐私和安全原因，不再被认为是安全协议。
* **WireGuard** – [WireGuard](https://www.wireguard.com/)是一种新型的实验性协议，与现有的VPN协议相比，旨在提供更高的安全性和更好的性能。尽管它仍在积极开发中，并且尚未经过审核，但仍有一些VPN提供商仅出于测试目的支持它，可以参考我对[WireGuard的测评](https://qiangwaikan.com/wireguard/)。

每个VPN协议都有自己的优缺点。OpenVPN目前是最流行的，因为它是安全的，开源的，并且还具有良好的性能，但这也需要使用第三方VPN服务商的应用程序。L2TP/ IKEv2也是一种安全的协议，具有出色的性能，可以在大多数操作系统上本地使用，但它不是开源的。

VPN加密

AES（[高级加密标准](https://zh.wikipedia.org/wiki/%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86)）是当今使用的最常见的加密密码之一，大多数VPN使用密钥长度为128位或256位的AES加密。即使在量子计算方面取得了进步，AES-128也被认为是非常安全的。想要破解这些加密数据，可能要以年为单位，而这些相关密钥其实是有过期时间的，即便破解出来也没用。

VPN日志

当你在使用VPN服务的时候，你所有的传输数据都会经过VPN服务器，理论上来说，他们可以知道并储存你的数据，这些数据也可以叫做日志。

对于一些一线VPN商家来说，他们都有严格的日志策略，很多都具有”无日志”策略，意思就是不记录你的任何日志。

以下是不同类型的VPN日志：

* **浏览日志** –这些日志基本上包括你在线进行的所有操作：浏览历史记录，时间，IP地址等。除非你使用的是免费VPN，否则正规的VPN服务商基本不会记录这些日志。
* **连接日志** –连接日志通常包括日期，时间，连接数据，有时还包括IP地址。通常，此数据用于优化VPN网络，并可能处理用户使用问题，这些日志可能不是那么重要。
* **无日志** –尽管有许多VPN声称是“无日志”，但 在实际测试中只有少数经验证为，真正的无日志VPN服务。

**如何选择VPN?**

拥有良好的速度

当你使用VPN时，背后其实发生了很多事情。你的计算机正在加密和解密通过远程VPN服务器转发的数据包。这些加解密操作都会花费计算机更多的时间，从而直接表现为你的网络速度。

为了确保使用VPN时最快的速度，最好优先考虑最适合你需求的VPN服务器。举个例子，如果你在中国，并且想要浏览被墙的网站，那么肯定有限选择香港的服务器，其次时美国服务器，至于欧洲服务器可以在特殊时期备用。

一般来说，良好的VPN服务不会严重影响你的网络速度，并且会对中国线路进行优化，使得运营商转发你的数据时，不会绕路而是直接走最短路线，这将进一步缩短往返时间。但，某些质量不高的VPN服务可能会大大降低你的网络速度，通常表现为连上VPN后无法上网，或者速度缓慢，所以在选择VPN的时候，应该考虑这些因素。

以下是一些使你的VPN速度最大化的建议：

* 1.选择具有良好性能的优质VPN服务。
* 2.连接到附近的服务器，并且该服务器负载不高(其他用户也会选择此节点，从而会增加负载)。
* 3.如果前两个选项不起作用，请尝试更改VPN协议。 VPN速度也可能受到你所使用的设备，网络或互联网提供商对VPN连接的限制。

支持解锁流媒体

优质的VPN除了在线隐私和安全性之外，还被全球成千上万的人用于解锁流媒体资源，这些音视频资源因版权或地区限制不能直接观看。但由于VPN使你能够改变的IP地址，并且可以切换到世界各地的任何VPN服务器位置，因此VPN也是用于在线观看音视频的不错工具。

以下是VPN的一些流媒体用途：

* 利用VPN观看Netflix – 无论你身在何处，都可以使用[优质的Netflix VPN](https://qiangwaikan.com/unblock-netflix/)享受无限制的视频播放体验。这意味着世界上任何地方的人们都可以访问拥有最多优质视频资源库的美国Netflix。
* 体育视频–一些体育赛事/比赛受到某些地理限制的限制，可以使用VPN破解。

VPN还可用于解锁其他[视频网站](https://qiangwaikan.com/video/)，例如Hulu，Amazon Prime和BBC iPlayer。同样，在国外工作生活的海外华人，他们都无法直接直接使用国内的音视频应用，因为很多资源都受到地区版权保护，因为很多人都使用[回国VPN](https://qiangwaikan.com/into-china/)来观看视频和听音乐。

支持种子下载

VPN的另一个非常流行的用途是种子下载和P2P下载。当你使用VPN[下载种子文件](https://qiangwaikan.com/torrent-site/)时，你的真实身份和IP地址将对第三方隐藏。

种子下载和P2P文件共享在某种程度上是灰色地带，可能会被归类为侵犯版权，具体取决于你要共享/下载的内容以及居住地。目前，世界各地的国家都在打击种子下载，如果没有VPN的情况下种子下载会存在风险。

尽管我们在“恢复隐私”中不支持任何非法活动或侵犯版权，但显而易见的是，没有VPN的种子下载可能会有风险。

媒体公司通常会运行监视节点网络，这些网络将加入种子下载监视组，并收集所有侵权方的连接数据。然后，媒体公司可以去找拥有相关的互联网服务提供商，并将让他们提供相关用户资料以及连接时间。然后，将代表版权所有者对用户进行侵犯版权的罚款或起诉。

支持常见设备

可以说大多数VPN都支持常见设备，比如：Windows、Mac、iOS和安卓。基本上来说，这几种设备已经可以满足我们的日常上网需求，并且这些VPN服务商大多支持3种设备同时在线，这意味着你可以和你的好友一起共享此账号，只要不在同一种设备登陆即可。

当然，也有一些比较大牌的VPN商家，比如[ExpressVPN](https://qiangwaikan.com/express-review/)，它支持多达22设备，可以说只有你想不到没有ExpressVPN不支持的设备，并且ExpressVPN也是我认为最好用的VPN。

在说说在路由器上安装VPN，由于国内的环境所以，你不可能在路由器上直接安装VPN，通常想要先刷机，然后安装一些固件。虽然在路由器使用VPN，可以绕过在线设备的限制，但是整个过程可能不那么简单，个人也不建议花费如此多的时间，除非你对此很有兴趣。

**VPN隐私保护**

VPN和Tor

VPN和Tor都是提供在线匿名的隐私工具，但是它们彼此之间有很大的不同。

Tor意思是The Onion Router（[洋葱路由器](https://www.torproject.org/zh-CN/download/)），既是浏览器又是利用多次“IP跳跃”来保护用户隐私的网络。Tor由美国政府于2002年创立，至今仍主要依靠美国政府机构提供资金。除了这个令人不安的事实，Tor还有其他一些问题：

* 有些人认为Tor网络已经受到威胁
* 微软的DRM可以轻松暴露Windows-on-Tor用户
* 使用Tor时查看PDF文档也会泄漏你的身份
* Tor用户容易受到端到端的定时攻击
* Tor对于日常使用来说太慢了

对于许多人来说，Tor最大的隐患是由于这是美国政府的一个项目，如今仍由美国政府资助。另外，恶意的Tor节点也存在许多问题，许多人还怀疑政府机构出于监视目的而运行Tor节点。

尽管存在Tor带来的风险，但仍有一些人喜欢将Tor和VPN服务一起使用。

为什么VPN可以提供隐私保护？

好的VPN可以为你提供在线隐私和安全性。如果没有VPN，你的网络服务提供商（ISP）可以轻松监视和记录你的在线活动：你访问的网站，你发表的评论，社交媒体互动，偏好等。许多国家现在要求网络提供商记录用户数据和浏览活动。VPN是保护自己免受这些隐私监视的最佳解决方案。

使用VPN时，你的互联网提供商只能看到你在线且已连接到VPN服务器。你的信息经过加密和安全保护，因此第三方无法读取。借助VPN，也可以放心使用公共WiFi热点，这要归功于保护你数据的安全加密。在没有VPN的情况下使用公共WiFi是有风险的，因为黑客可以利用公共Wi-Fi来窃取你的身份、信用卡、银行帐户和密码等信息，而VPN可以加密并保护这些数据免受第三方和黑客的攻击。

VPN能够让我100％匿名？

很遗憾，不能。考虑到可能暴露匿名的各种不同方式（特别是通过浏览器指纹识别），仅用VPN是不能保证你100％的匿名性。实际上，借助NSA等监视机构的大量资源，实现100％的在线匿名性可能非常困难。

当然，使用VPN已经可以保证大多数时候的隐私安全。另外，你可以采取一些简单的步骤来进一步提高在线匿名性，而不仅仅是使用VPN：

* 使用安全的浏览器，防止浏览器出现指纹 （你的浏览器可以向第三方泄露很多信息）。
* 使用良好的广告拦截器(很多VPN现在自带了此功能)。广告基本上是在变相中进行跟踪，在线收集信息，对你进行概要分析，然后使用这些数据为你定位更好的广告。

VPN的泄漏和断线切换

困扰许多VPN服务的一个严重问题是数据泄漏问题。以下是几种不同类型的泄漏，它们会在使用VPN时破坏你的隐私和安全性：

* DNS泄漏 –当你的[DNS请求](https://zh.wikipedia.org/zh-hans/%E5%9F%9F%E5%90%8D%E7%B3%BB%E7%BB%9F)泄漏出VPN隧道并由网络运营商处理时，就会发生这种情况。这将会暴露你的浏览历史记录（DNS请求），互联网提供商的IP地址以及你的真实位置。
* IP地址泄漏 – IP地址泄漏只是当你的IP地址从VPN隧道泄漏出去时。这可能是短暂的暂时性泄漏，也可能是连续性泄漏。这通常发生在，对于带有不支持或无法正确阻止IPv6的VPN。
* WebRTC泄漏 –这主要发生在Firefox、Chrome、Brave，以及任何其他使用WebRTC API的基于Chromium的浏览器。WebRTC泄漏会通过浏览器泄露你的IP地址，即使你使用的是良好的VPN。

**关于VPN的总结**

使用VPN可以让我们享受真正自由的上网体验，解锁地区限制的视频资源，浏览被屏蔽的网站等。当然自由有时候是把双刃剑，当你掌握了翻墙技术之后，请不要用于非法途径，而是将VPN用于对自己工作和学习都有益的事情上，希望你在翻墙之后，学习到更多有趣的知识。