# VPN在互联网中的应用现状与前景分析

随着网络科技的发展,互联网的安全问题日益显著。而VPN技术利用Internet或其他公共互联网络的基础设施为用户创建隧道,采用高强度的认证、加密算法保证传输数据的完整性和私密性,提供了与专用网络一样的安全和功能保障。VPN的主要特点就是安全、费用低、灵活性大,它可以在远程用户、商业伙伴、公司内部网等建立可靠的安全链接,并保护数据传输的安全性,目前VPN技术已经成为网络技术中的一个热点。

VPN的英文全称是Virtual Private Network，中文翻译过来就是虚拟专用网。指的是依靠ISP和其他NSP，在公有网络中建立专用的数据通信网络。所谓虚拟，是指于用户不再需要真正的去铺设实际的物理线路，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的。所谓专用网络，是指用户可以按照自己的实际需求建立一条专有的通讯线路，就好比是架设了一条专线一样。在企业运行中，不用支付线路费用，也不用购买路由器等硬件设备。所付出的仅仅是购买VPN设备，向企业所在地的ISP支付一定的上网费用，这就是为什么VPN节省成本的原因。

虚拟专用网络的基本用途有两个，首先是保证通过Internet能够实现远程用户的相互连接。在企业中，公司内部员工可以和各分支办事处，商业合作伙伴，远程用户之间相互访问。其次是如何保证在通过公共互联网远程访问企业资源的安全性。例如企业中的一些重要的商业机密信息是不能泄露的。VPN用户对数据的安全性都比较关心，目前VPN主要采用隧道技术来保证安全。类似于点对点的连接技术，它是在公共网络上建立一条数据通道称隧道，让数据包通过这条隧道传输。即首先对数据包进行加密，而不是公开的在网上传输，然后由VPN封装成IP包的形式，通过隧道在网上传输。

创建隧道的过程类似于在两个人之间建立会话的过程，首先隧道的两个端点必须同意创建隧道并对加密方案达成一致，协商隧道的各种配置，如地址分配或压缩等参数。然后发送端将数据包加密并封装成IP包，接收端收到后对数据包进行解密，发给远程接入服务器或本地路由器。

目前VPN主要采用隧道技术、加密解密技术、密钥管理技术及使用者与设备身份认证技术这四项技术来保证安全。

隧道技术主要解决了公用网与专用网的兼容问题，隐藏发送者、接受者的IP地址以及一些其它协议信息。向用户提供了端到端的、安全的连接服务。

隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议如IP封装到PPP中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层（数据链路层）协议进行传输。第二层隧道协议主要有L2F、 PPTP、L2TP等。第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层（网络层）协议进行传输。第三层隧道协议有VTP、IPSec等。IPSec ( IP Security )即IP安全协议定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在IP层提供安全保障。

加解密技术是数据通信中一项比较成熟的技术，即在数据传输之前，发送方利用算法对数据进行加密，加密后的数据我们称为密文，接收方收到密文后，利用同样的算法进行解密，以还原成相应的明文。以保证数据在传输过程中不会被其它非法用户窃取或篡改。VPN可直接利用现有的加解密技术。

密钥管理的主要任务是如何保证在公用数据网上安全地传递密钥而不被窃取。现行密钥管理协议又分为ISAKMP和SKIP两种。在密钥管理协议ISAKMP中，双方都有两把密钥，即公有密钥和私有密钥。SKIP主要是利用Diffie-Hellman的演算法则，在网络上传输密钥。