从应用看V 如何实现企业网络安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E4_BB_8E_E5_BA_94_E7_94_A8_E7_c101_461758.htm 如果你是一名大中型公司精明的管理者你一定考虑过VPN技术；如果你是一名资深网络管理员也一定向公司经理推荐过使用VPN. 关于VPN的好处很多文章都已经介绍过，这里就不再一一罗列了。好处归纳下来就是——降低了费用，增强了安全性。 本文主要讲解VPN对企业安全实现的帮助，为各位读者介绍企业使用VPN后会在安全方面有哪些提升。 一，传统内网连接的缺点： 对于传统内网连接来说如果出现跨区域的情况，例如公司在北京和上海各有一个分部，当这两个分部网络互相分享文件信息时只能通过internet解决，由于所有跨部门的数据包都是在internet公共网络上传输，所以即使数据经过简单加密仍然很容易被黑客监听和破解，这点缺陷为企业内网安全带来了巨大的隐患，特别是金融行业和企业机密信息比较多的公司。如何提高数据的安全呢？这时VPN的优势就大大体现了。 二，VPN适用环境： 并不是所有情况对于VPN都是合适的，例如公司只在北京有一个分部，而且网络都在一个内网中，这时候就不需要使用VPN了。内网中数据的传输躲开了internet公网，从而避免了机密信息被黑客监听的概率。 那么VPN适用于什么网络环境呢？他主要用于互连两个局域网，当然也有连接远程单个用户和公司局域网的，不过用的最多的还是前者。比较常见的就是上面提到的那种情况——公司在北京和上海各有一个分部，这两个分部网络需要互相分享文件信息。 小提示： 如果公司在北京而员工出差到上海，

员工想在上海连接北京公司内网怎么办？这种情况也是可以用VPN来解决的，异地的单个网络节点通过VPN连接北京公司的内网从而顺利完成工作。 三，直接提高企业网络安全：首先我们来看看VPN的安全机理，他和简单的将数据包加密是不同的。 VPN使用三个方面的技术保证了通信的安全性：通道协议、身份验证和数据加密。客户机向VPN服务器发出请求，VPN服务器响应请求并向客户机发出身份质询，客户机将加密的响应信息发送到VPN服务端，VPN服务器根据用户数据库检查该响应，如果账户有效，VPN服务器将检查该用户是否具有远程访问的权限，如果该用户拥有远程访问的权限，VPN服务器接受此连接。在身份验证过程中产生的客户机和服务器公有密钥将用来对数据进行加密。 通俗的讲当VPN客户端和VPN服务器建立连接成功后，所有的数据信息都是在一个专门独立出来的隧道中传输的，这个隧道是电信提供给我们的，在电信方面进行了必要的安全措施，隧道很难被黑客发现。即使黑客能够监视到隧道也无法看到在隧道中传输的信息的真面目。因为VPN数据在Internet中传输时，Internet上的用户只看到公共的IP地址，看不到数据包内包含的专用网络地址。VPN的加密方式使得网络信息传输的安全性大大提高。 另外VPN支持最常用的网络协议，例如IP、IPX和NetBUI协议的网络中的客户机都能很容易地使用VPN.这点使得他的应用范围更广。 小提示： VPN的种类很多，有租用电信的VPN，最常见的是MPLS VPN他是将安全措施都交给电信，所有安全都由电信来保障；还有的VPN是自己搭建VPN，这样在费用上比前者开销小。当然如果自己建立VPN的经验足够丰富，网络管理员技术足够强的话安

全性和租用电信VPN没有什么区别。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com