新闻之认证、加密两招解除VPN安全隐患 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/63/2021_2022__E6_96_B0_E9_97_BB_E4_B9_8B_E8_c40_63974.htm VPN（Virtual Private Network）虚拟专用网络，是通过在公共的网络环境中建立专用通道进行数据传输的一种技术。虚拟专用网不是真的专用网络，但却能够实现专用网络的功能，在公共网络环境中虚拟通道，可以达到降低成本的目的。据估算，如果企业放弃租用专线而采用VPN，其整个网络的成本可节约21%-45%，至于那些以电话拨号方式连网存取数据的公司，采用VPN则可以节约通讯成本50%-80%。正是基于这一优势，近几年的VPN应用越来越多。但是，由于VPN是在不安全的Internet中进行通信，而通信的内容可能涉及到企业的机密数据，企业必须确保其VPN上传送的数据不被攻击者窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问，因此VPN存在的安全隐患问题就显得非常重要，有没有办法能够解除这个问题，让VPN圆了企业“节约成本”的梦吗？有。 认证技术 认证技术可以区分真实数据与伪造、被篡改过的数据。这对于网络数据传输,特别是电子商务是极其重要的。认证协议一般都要采用一种称为摘要的技术。摘要技术主要是采用HASH函数将一段长的报文通过函数变换，映射为一段短的报文即摘要。由于HASH函数的特性，使得要找到两个不同的报文具有相同的摘要是困难的。该特性使得摘要技术在VPN中有两个用途：1：验证数据的完整性。发送方将数据报文和报文摘要一同发送,接收方通过计算报文摘要,与发来摘要比较,相同则说明报文未经修改。由于在报文摘要的计算

过程中一般是将一个双方共享的秘密信息连接上实际报文一同参与摘要的计算，不知道秘密信息将很难伪造一个匹配的摘要，从而保证了接收方可以辨认出伪造或篡改过的报文。2：用户认证。该功能实际上是上一种功能的延伸。当一方希望验证对方，但又不希望验证秘密在网络上传送，这时一方可以发送一段随机报文，要求对方将秘密信息连接上该报文作摘要后发回，接收方可以通过验证摘要是否正确来确定对方是否拥有秘密信息，从而达到验证对方的目的。 常用的HASH函数有MD5，SHA-1等。 加密技术简介 在VPN中为了保证重要的数据在公共网上传输时不被他人窃取,采用了加密机制。IPSec通过ISAKMP/IKE/Oakley协商确定几种可选的数据加密方法如DES、3DES。在现代密码学中，加密算法被分为对称加密算法和非对称加密算法。 对称加密算法采用同一把密钥进行加密和解密，优点是速度快，但密钥的分发与交换不便于管理。 使用不对称加密加密时，通讯各方使用两个不同的密钥,一个是只有发送方知道的专用密钥d，另一个则是对应的公用密钥e，任何人都可以获得公用密钥e。专用密钥和公用密钥在加密算法上相互关联，一个用于数据加密，另一个用于数据解密。由于不对称加密运算量大，一般用于加密对称加密算法中使用的密钥。不对称加密还有一个重要用途即数字签名。 目前，常用的数据加密算法有： 对称加密算法： 国际数据加密算法（IDEA：International Data Encryption Algorithm）：128位长密钥，把64位的明文块加密成64位的密文块。 DES和3DES加密算法 (The Data Encryption Standard):DES有64位长密钥,实际上只使用56位密钥。 AES：Rijndial加密算法 不对称加密算法： RSA 椭圆曲线制算法

综上所述，在信息化建设如火如荼的今天，企业应用vpn也必然成为一种趋势，那么，怎样才能有效消除vpn潜在的安全隐患也成为了现在企业、厂商共同关心的问题，如果从以上两个方面来做的话，应该是会起到事半功倍的效果的。