2006电子商务理解IPsec验证和认证选项 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/62/2021_2022_2006_E7_94_B5_E5_AD_90_c40_62354.htm IPsec VPNs通过将个人的主机与整个网络连接起来扩大网络的安全周长。一个安全的VPN从认证这些传输隧道终端的身份开始，但是薄弱的验证选项会引起互用性问题或网络妥协问题。本文将探究普通IPsec VPN身份验证和认证选项、他们的安全性以及配置涵义问题。 标准IPsec VPN特性 IPsec VPN传输隧道能够被静态配置(“钉住”)或建立Internet Key Exchange (IKE)标准中定义的动态使用信息。IKE使两个VPN网关(或两个VPN主机，或一个网关和一个主机)彼此验证，商议安全参数，进而生成数据加密、保证数据完整性的密匙。 验证最主要是为了避免与未经过验证的用户建立传输隧道连接。在一个点对点的VPN中，验证使我们及时发现伪装为VPN网关的攻击者。在远程访问VPN中，验证使我们及时禁止伪装为合法用户的入侵者访问。为了通过认证，IKE 待接入的终端设备使用标准验证类型进行认证:一IPv4 或 IPv6地址，一主机名(完全合格域名(FQDN))，一电子邮件地址(User FQDN)或一X.500识别名(Distinguished Name (DN))。IKE待接入的终端设备能使用不同的ID类型.例如，user@mycorp.com (User FQDN)能与vpn.mycorp.com (FQDN)建立传输隧道。 为了防止ID欺骗，我们主张使用IKE标准认证方法:一个预共享密钥(Pre-Shared Key，PSK)，一RSA 或 DSS数字签名，或一个加密的公匙。要使用预共享密钥，需要在两端待接入的终端设备彼此验证前，赋予他们相同的秘密值。要使用数字签名，用户端必须持有认证中

心(Certificate Authority，CA)发放的认证证书。要使用加密的公匙，每个用户必须生成一对他们自己的RSA密匙，之后将公匙配置到每一个将要通信IKE待接入的终端设备中。IKE 待接入的终端设备必须使用相同的认证方法:例如，user@mycorp.com和vpn.mycorp.com可能都使用共享的PSK“芝麻开门(opensesame)”。或者他们可能都使用RSA签名，每个都生成发送人自己的证书。 因为这些信息要通过可能发生偷听的不可信任的网络，IKE使用加密方法来保护信息。例如IKE PSK从不传输.待接入的终端设备仅仅传输双方都知道相同的PSK的加密过的杂乱信号。但是这不适用于IKE ID。IKE以两种模式操作:5-信息主模式(5-message Main Mode)，该模式阻止ID欺骗(ID sniffing).或3-信息挑战模式(3-message Aggressive Mode)，该模式能用普通文字发送发送者的ID。两种模式都支持所有的IKE标准ID类型和认证方法，除了，如果主模式与PSK一起使用，ID必须是一个IP地址。这使主模式/PSK不能远程登陆VPN，因为移动用户很少连接静态IP地址。 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