中小企业网络选择 LV 是否适合 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/251/2021_2022__E4_B8_AD_E5_B0_8F_E4_BC_81_E4_c101_251111.htm 虚拟专用网（VPN）为远距离工作者们、旅行主管们，以及那些常常将工作带回家里的雇员们提供了一个安全的通道，让他们可以连上公司的本地局域网并存取自己所需的相关资源。现在有许多不同的VPN选项可用，其中一些被内置在流行的操作系统之中，而另一些则需要购买额外的软件或硬件。和绝大多数技术一样，大企业由于充足的费用预算，而在选择正确的VPN解决方案方面拥有更多的灵活性，以及因为拥有专业的IT职员，而拥有对不同种类VPN的选择、部 署以及管理的能力。 对中小企业而言的VPN选项 适合小企业的最流行VPN选项包括：点对点信道协议（PPTP，Point to Point Tunneling Protocol）VPN：PPTP服务内置在Windows Server系统之中，从Windows NT直到Longhorn Server都有，这样你就可以自行建立一个PPTP服务器，而无需购买额外的软件，而PPTP的客户端则已经内置在了近来所有版本的Windows之中。 使用IPsec加密的Layer 2信道协议： L2TP/IPsec VPN服务被内置在Windows 2000 Server以及更高版本之中，而L2TP客户端则被包含在Windows 2000专业版以及之后版本的Windows操作系统之中。 基于IPsec的第三方VPN解决方案：有大批的生产商提供基于IPsec的VPN设备以及集成的防火墙/VPN产品，比如Cisco，SonicWall，Juniper Networks，Symantec，以及很多其他厂商。 基于SSL的VPN解决方案： 基于SSL（Secure Sockets Layer）的VPN设备以及软件可以从多个源头获得。而

即将发布的微软下一版本服务器操作系统（开发代码Longhorn Server）将会提供一个全新的VPN协议SSTP（Secure Socket Tunneling Protocol），同时在Vista Service Pack 1中也将会提供对SSTP协议的支持。这将为中小企业市场提供另一种低成本的VPN解决方案。 对中小企业市场而言，使用SSL VPN的优点 SSL（以及它的继承者，TLS，Transport Layer Security）是相对简单的技术，通过使用公共密钥加密技术（公共/秘密密钥对）来建立一个加密信道，从而对数据进行传输。而它的部署和实施相比起例如IPsec VPN这样的技术而言，也相对没有那么复杂。对中小企业而言，这一点特别的重要，因为它们通常并没有大量的IT职员或IT专家，而且一般也没有对 IPsec VPN进行故障调试所需的专门技术。 SSL VPN常常被吹捧为“ 无需客户端 ”，但是实际上这个说法并不正确；更精确的说法是绝大多数电脑其实都内置了SSL客户端：网页浏览器。因此即使在那些用户根本无权安装任何软件的电脑上，也依然可以建立SSL VPN.显然，这让建立VPN的过程变得更加简单，也让选择到底在何处建立局域网远程连接的过程变得更加富有灵活性。 当用户们试图在饭店里或者其他类似所在地建立VPN连接时，常常会碰到的一个问题是一些网络/防火墙管理员常常会关闭了VPN协议所使用的端口。不过，由于绝大多数网络都会允许进行安全http（HTTPS）通讯，所以这种情况下SSL VPN依旧能够正常工作，而其他的VPN协议可就不行了。 但另一方面，使用SSL VPN，自然也就无法获得使用其他传统VPN技术所能获得的相应存取级别权限。 安全方面 使用VPN的目的是提供一个安全信道，以便远程用户可以存取私有网络。而允许任何类型的远程存

取都会导致一定的风险，包括VPN.比方说，用户口令可能会被“ 破解 ”，从而允许未经授权的人通过VPN服务器存取网络资源。但这种风险可以通过加强口令的复杂度来降低，并通过使用两种以上的认证方式（比如智能卡）来更进一步的削减风险。 而对所有种类的VPN连接来说，另一个风险则是所谓的“ 分裂信道 ”。当远程电脑在连接公司电脑的同时，如果又同时连接到Internet的某个资源上，“ 分裂信道 ”就会发生。如果远程电脑遭受了来自Internet连接的入侵，那么入侵者就可以利用VPN信道来存取公司的网络。VPN客户端可以通过配置来阻止分裂信道的发生。 因为SSL VPN可以在公共电脑上建立，所以可能会为公司网络带来额外的风险，因为这些公共电脑并不一定都打上了最新的系统补丁或者进行了最新的系统更新，所使用的反病毒软件可能也不是最新的病毒库，而且很可能并没有使用防火墙。另外，公共电脑可能不支持两种以上的认证方式，因为它们自身没有智能卡阅读器，或直接被禁用了USB端口。 好的SSL VPN执行过程，会允许你对试图建立VPN连接公司网络的远程电脑自身的“ 健康状况 ”进行检查。这个技术让你可以设定检查标准（比如要求具备反病毒软件，防火墙，以及打上了系统最新补丁包/更新），当远程电脑达不到标准的要求时，就会阻止其向公司网络建立VPN连接。 期待SSTP 微软面向Longhorn Server以及Vista的全新SSTP VPN将有助于解决许多用户在使用PPTP以及L2TP/IPsec连接时遇到的被防火墙、代理服务器以及NAT设备拦截的问题，特别是在那些用户对这些设备没有任何配置控制权的网络上。 就像其他VPN协议一样，SSTP将通过在服务器上的RRAS（路由以及远程存取服务，Routing and

Remote Access Services）进行配置。SSTP通讯使用TCP 443端口。SSTP在IPv6上的信道也将被支持；Vista和Longhorn都已经在系统中安装了IPv6，并默认启用。而多因素认证，比如智能卡或者SecurID令牌，也和RRAS远程存取策略一样，受到支持。而连接系统管理工具包（CMAK，Connection Manager Administration Kit），则可以为SSTP VPN连接建立不同的配置文件。 总结 以前，SSL VPN解决方案一般都很昂贵，因此更多的是被大型级别的企业采用。但是，现在已经出现了低价的SSL VPN设备和软件，而且微软也将在下一版本的Windows服务器以及客户端操作系统中内置SSL信道协议，因此对中小企业来说，SSL VPN已经成为一个切实可行的选择。 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