解析关于 LV 技术原理及其应用全面 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__E8_A7_A3_E6_9E_90_E5_85_B3_E4_c101_461759.htm 随着电子商务、企业信息化、教育信息化等信息化进程的推进，整个社会的信息化程度不断提高。在人们的工作、生活中，信息处理变得越来越重要了。而作为信息处理的一种典型模式，企业等各类社会组织的“ 内部资源处理系统 ”迅速地发展起来，并逐步成为组织的各种业务的基础设施。在这些内部资源系统的服务器和主机上，配置了大量的业务处理应用软件。 随着中国进入WTO和经济全球化的进程，企业为了提高工作效率和竞争能力，远程访问、移动办公已经成了各种社会组织的普遍需要。由于Internet的普及和发展，通过 IPSec VPN技术实现大量数据的远程访问为人们提供了一种低运行成本、高生产效率的远程访问方式。但是，IPSec VPN也有不足，它使用十分复杂，必须安装和维护客户端软件。另外，从远程通过IPSec通道连接到企业内部网络可能会增加局域网受到攻击或被病毒感染的可能。SSL VPN(安全套接层虚拟专网)技术的出现刚好解决的这一问题。 SSL VPN技术帮助用户通过标准的Web浏览器就可以访问重要的企业应用。这使得部门员工出差时不必再携带自己的笔记本电脑，仅仅通过一台接入了Internet的计算机就能访问企业资源，这为企业提高了效率也带来了方便，同时很好的解决了安全性问题。 SSL VPN原理 如果把SSL 和VPN 两个概念分开，大家对他们的含义应该都非常清楚，但是作为一种新技术，它们之间是如何结合起来的大家也许还不是很了解。从学术和商业的角度来讲，因

为他们代表的含义有所不同，因而常常会被曲解。 SSL（安全套接层）协议是一种在Internet上保证发送信息安全的通用协议。它处于应用层。SSL用公钥加密通过SSL连接传输的数据来工作。SSL协议指定了在应用程序协议（如HTTP、Telnet和FTP等）和 TCP/IP协议之间进行数据交换的安全机制，为TCP/IP连接提供数据加密、服务器认证以及可选的客户机认证。SSL协议包括握手协议、记录协议以及警告协议三部分。握手协议负责确定用于客户机和服务器之间的会话加密参数。记录协议用于交换应用数据。 警告协议用于在发生错误时终止两个主机之间的会话。 VPN（虚拟专用网）则主要应用于虚拟连接网络，它可以确保数据的机密性并且具有一定的访问控制功能。VPN是一项非常实用的技术，它可以扩展企业的内部网络，允许企业的员工、客户以及合作伙伴利用Internet访问企业网，而成本远远低于传统的专线接入。过去，VPN 总是和IPSec 联系在一起，因为它是VPN 加密信息实际用到的协议。IPSec 运行于网络层，IPSec VPN 则多用于连接两个网络或点到点之间的连接。 所谓的SSL VPN，其实是VPN设备厂商为了与IPsec VPN区别所创造出来的名词，指的是使用者利用浏览器内建的Secure Socket Layer封包处理功能，用浏览器连回公司内部SSL VPN服务器，然后透过网络封包转向的方式，让使用者可以在远程计算机执行应用程序，读取公司内部服务器数据。它采用标准的安全套接层（SSL）对传输中的数据包进行加密，从而在应用层保护了数据的安全性。高质量的SSL VPN解决方案可保证企业进行安全的全局访问。在不断扩展的互联网Web站点之间、远程办公室、传统交易大厅和客户端间，SSL VPN克服了IPSec VPN的不

足，用户可以轻松实现安全易用、无需客户端安装且配置简单的远程访问，从而降低用户的总成本并增加远程用户的工作效率。而同样在这些地方，设置传统的IPSec VPN非常困难，甚至是不可能的，这是由于必须更改网络地址转换（NAT）和防火墙设置。 通过SSL VPN远程访问企业内部网络的构架 SSL VPN的实现 简单的来讲，SSL VPN一般的实现方式是在企业的防火墙后面放置一个SSL代理服务器。如果用户希望安全地连接到公司网络上，那么当用户在浏览器上输入一个URL后，连接将被SSL代理服务器取得，并验证该用户的身份，然后SSL代理服务器将提供一个远程用户与各种不同的应用服务器之间连接。掌握四个关键术语的含义有助于理解SSL VPN是如何实现的。即：代理、应用转换、端口转发和网络扩展。 SSLVPN网关至少要实现一种功能：代理Web页面。它将来自远端浏览器的页面请求（采用HTTPS协议）转发给Web服务器，然后将服务器的响应回传给终端用户。 对于非Web页面的文件访问，往往要借助于应用转换。SSL VPN网关与企业网内部的微软CIFS或FTP服务器通信，将这些服务器对客户端的响应转化为HTTPS协议和HTML格式发往客户端，终端用户感觉这些服务器就是一些基于Web的应用。 在进行代理和应用转换时，测试者发现，这些产品之间存在着很大的差别。有的产品所能支持的应用转换器和代理的数量非常少。有的则很好地支持了FTP、网络文件系统和微软文件服务器的应用转换。 用户在选择网关时，必须对自己所需要转换的应用有一个很明确的了解，并能够根据它们的重要性给它们排个先后顺序。 而有一些应用，如微软Outlook或MSN，它们的外观会在转化为基于Web界面的过程中丢失

。此时要用到端口转发技术。端口转发用于端口定义明确的应用。它需要在终端系统上运行一个非常小的Java或ActiveX程序作为端口转发器，监听某个端口上的连接。当数据包进入这个端口时，它们通过SSL连接中的隧道被传送到SSL VPN网关，SSL VPN网关解开封装的数据包，将它们转发给目的应用服务器。使用端口转发器，需要终端用户指向他希望运行的本地应用程序，而不必指向真正的应用服务器。 一些SSL VPN网关还可以帮助企业实现网络扩展。它将终端用户系统连接到企业网上，并根据网络层信息（如目的IP地址和端口号）进行接入控制。虽然牺牲了高级别的安全性，却也换来了复杂拓扑结构下网络管理简单的好处。 