IP网络构建VPN网络的若干种技术 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/237/2021_2022_IP_E7_BD_91_E7_BB_9C_E6_9E_c101_237153.htm 当一种资源开始稀缺时，人们总会创造更多的资源或者寻找更好的替代资源，当资源开始丰富的时候，人们又会开始浪费资源，最终导致资源再次稀缺。网络带宽就是这样，带宽和应用需求在不断赛跑，尽管带宽越来越宽，但是人们总是有越来越多的带宽需求。所以解决带宽稀缺的方法不仅包括寻找更高的带宽，同时也需要充分地利用现有带宽。 构建VPN网络的基础网络平台可以是IP网络，也可以是ATM网络或者FR网络等。基于ATM/FR等网络构建的虚拟专用网络都属于传统数据专网的范畴，本文重点讨论基于IP网络构建虚拟专用网络的若干种技术。 根据构建VPN的基础网络平台的层次不同，可以将VPN划分为二层VPN，比如利用VLAN在以太网络上实现多个虚拟网络；三层VPN，比如利用 IPSec 实现VPN等；四层VPN，比如利用SSL技术构建VPN.至于在国内应用较多的基于TDM技术实现数据网络，比如DDN等，则一般将其称为数据专网，而不再将其纳入VPN的概念，尽管数据专网也是在电信运营商提供的统一的数据网络平台上利用时分复用等技术构建的虚拟的用户专用网络。 链路加密机实现VPN 链路加密机指的是针对具体的链路层协议提供数据加密功能的设备，比如ATM加密机、帧中继加密机、DDN加密机等。加密机的特点是必须在链路两端配对使用，比如一个企业租用一条64K的链路，那么必须在链路两端分别部署加密机。利用链路加密机可以实现链路两端的网络之间通信的保密性，但是

其组网方式也因此受到限制，不能实现任意两点之间灵活的加密保护。 随着Internet和宽带网络的发展，链路加密机已经不适合在 Internet和宽带网络环境下应用了，因为企业利用Internet构建Intranet时，企业两个分支机构之间网络连接可能会跨越很多种链路，比如一方接入利用ADSL，然后通过运营商的骨干ATM网络达到另外一段城域网，在这样的网络环境下利用链路加密机实现端到端的网络保护是不可能的。 基于IPSec 的VPN 基于IPSec的VPN主要目的是解决网络通信的安全性和利用开放的Internet实现异地的局域网络之间的虚拟连接，IPSec VPN既可以在IPv4网络也可以在IPv6网络中部署。图1是典型的基于IPSec的VPN组网模式，其中体现了移动用户接入VPN（Access VPN）、企业分支机构同总部之间构建的Intranet VPN，以及企业同合作伙伴之间构建的Extranet VPN. 基于IPSec的VPN不依赖于网络接入方式，它可以在任意基础网络上部署，而且可以实现端到端的安全保护，即两个异地局域网络的出口上只要部署了基于IPSec 的网关设备，那么不管采用何种广域网络都能够保证两个局域网络安全地互联在一起。 基于SSL的VPN SSL （Secure Socket Layer，安全套接字层）是Netscape公司开发的协议软件，目的是保护HTTP协议，但是这个协议本身可以保护任何一种基于TCP协议的应用。 基于SSL也可以构建VPN，因为SSL在Socket层上实施安全措施，因此它可以针对具体的应用实施安全保护，目前应用最多的就是利用SSL实现对Web应用的保护。 在应用服务器前面需要部署一台SSL服务器，它负责接入各个分布的SSL客户端。这种应用模式也是SSL主要的应用模式，类似于IPSec VPN中的Access VPN模式，如果企业分布的网络环境下只有

这种基于C/S或B/S架构的应用，不要求各分支机构之间的计算机能够相互访问，则可以选择利用SSL构建简单的VPN.具备这种应用模式的企业有：证券公司为股民提供的网上炒股，金融系统的网上银行，中小企业的ERP等。 基于SSL的VPN部署起来非常简单，只需要一台服务器和若干客户端软件。