　隧道技术是VPN的基本技术类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到PPP中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有L2F、PPTP、L2TP等。L2TP协议是目前IETF的标准，由IETF融合PPTP与L2F而形成。

　　第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有VTP、IPSec等。IPSec（IP Security）是由一组RFC文档组成，定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在IP层提供安全保障。

**GRE、PPTP、L2TP隧道协议**

|  |
| --- |
| 在IPSec 和Multiprotocol Label Switching (MPLS) VPN出现前，GRE被用来提供Internet上的VPN功能。GRE将用户数据包封装到携带数据包中。因为支持多种协议，多播，点到点或点到多点协议，如今，GRE仍然被使用。 在GRE隧道中，路由器会在封装数据包的IP头部指定要携带的协议，并建立到对端路由器的虚拟点对点连接   * Passenger: 要封装的乘客协议 (IPX, AppleTalk, IP, IPSec, DVMRP, etc.). * Carrier: 封装passenger protocol的GRE协议，插入到transport和passenger包头之间, 在GRE包头中定义了传输的协议 * Transport: IP协议携带了封装的passenger protocol. 这个传输协议通常实施在点对点的GRE连接中(GRE是无连接的).   GRE的特点：   * GRE是一个标准协议 * 支持多种协议和多播 * 能够用来创建弹性的VPN * 支持多点隧道 * 能够实施QOS   GRE的缺点：   * 缺乏加密机制 * 没有标准的控制协议来保持GRE隧道（通常使用协议和keepalive） * 隧道很消耗CPU * 出现问题要进行DEBUG很困难 * MTU和IP分片是一个问题   配置：  这里配置对端的IP地址和tunnel ID (tunnel key 2323)来进行简单的认证。两端配置的tunnel ID必须配置相同。  在Cisco IOS versions 12.2(8)T允许配置keepalive，定期发送报文检测对端是否还活着  GRE隧道 GRE建立的是简单的（不进行加密）VPN隧道，他通过在物理链路中使用ip地址和路由穿越普通网络。 大部分协议都没有内建加密机制，所以携带他们穿越网络的很常见的方法就是使用加密（如使用IPSec）的GRE隧道，这样可以为这些协议提供安全性。（相关配置请参看GRE over IPSec）网状连接（Full-Mesh） 由于GRE是建立点对点的隧道，如果要多个端点的网状互联，则必须采用这种Hub-and-spoke的拓扑形式  但是可以通过使用NHRP（Next-Hop Resolution Protocol）来自动建立全网状拓扑。（相关配置请参看NHRP 配置全网状互联GRE隧道）  VPDN简介 VPDN（Virtual Private Dial Network，虚拟私有拨号网）是指利用公共网络（如ISDN和PSTN）的拨号功能及接入网来实现虚拟专用网，从而为企业、小型ISP、移动办公人员提供接入服务。  VPDN采用专用的网络加密通信协议，在公共网络上为企业建立安全的虚拟专网。企业驻外机构和出差人员可从远程经由公共网络，通过虚拟加密隧道实现和企业总部之间的网络连接，而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。 VPDN有下列两种实现方式：   1. 网络接入服务器（NAS）通过隧道协议，与 VPDN网关建立通道的方式。这种方式将客户的PPP连接直接连到企业的网关上，目前可使用的协议有L2F与L2TP。其好处在于：对用户是透明的，用户 只需要登录一次就可以接入企业网络，由企业网进行用户认证和地址分配，而不占用公共地址，用户可使用各种平台上网。这种方式需要NAS支持VPDN协议， 需要认证系统支持VPDN属性，网关一般使用路由器或VPN专用服务器。 2. 客户机与VPDN网关建立隧道的方式。这种方式由客户机先建立 与Internet的连接，再通过专用的客户软件（如Win2000支持的L2TP客户端）与网关建立通道连接。其好处在于：用户上网的方式和地点没有限 制，不需ISP介入。缺点是：用户需要安装专用的软件（一般都是Win2000平台），限制了用户使用的平台。   VPDN隧道协议可分为PPTP、L2F和L2TP三种Point to Point Tunneling Protocol（PPTP） 点对点隧道协议（PPTP）是一种支持多协议虚拟专用网络的网络技术, 它工作在第二层。通过该协议，远程用户能够通过Microsoft Windows NT工作站、Windows 95和Windows 98操作系统以及其它装有点对点协议的系统安全访问公司网络，并能拨号连入本地ISP，通过Internet安全链接到公司网络。 PPTP协议假定在PPTP客户机和PPTP服务器之间有连通并且可用的IP网络。因此如果PPTP客户机本身已经是IP网络的组成部分，那么即可通过该 IP网络与PPTP服务器取得连接；而如果PPTP客户机尚未连入网络，譬如在Internet拨号用户的情形下，PPTP客户机必须首先拨打NAS以建 立IP连接。这里所说的PPTP客户机也就是使用PPTP协议的VPN客户机，而PPTP服务器亦即使用PPTP协议的VPN服务器。   * PPTP Access Concentrator (PAC)： 接入服务商，允许拨号接入连接（通常是由ISP担任，而且不需要ISP的协助来建立隧道） * PPTP Network Server (PNS)：通常是PPTP服务器或者路由器用来建立PPTP隧道 * Microsoft Point-to-Point Encryption (MPPE) ：和IPSec一样，是一种数据加密协议，用来为PPP拨号连接传输的数据进行加密。MPPE使用RSA算法来进行加密，支持40-bit和128-bit的会话密钥   PPTP只能通过PAC和PNS来实施，其它系统没有必要知道PPTP。拨号网络可与PAC相连接而无需知道PPTP。标准的PPP客户机软件可继续在隧道PPP链接上操作。  PPTP VPN 协商过程：   1. 客户端（笔记本）通过PPP建立到ISP NAS的连接 2. 客户端建立到PNS（在这里是CISCO路由器）的PPTP连接 3. 客户端和PNS之间建立了一个2层的隧道。多种协议能够在这个隧道上传输 4. 使用MPPE加密PPP数据包，这些数据包接下来通过enhanced GRE封装，并在IP网络上传输 5. 在客户端和PPTP服务器之间建立第二个PPP over GRE会话 6. 数据能够在这个IP/GRE/PPP上传输 7. PPTP隧道使用不同的TCP连接来控制会话   PPTP使用GRE的扩展版本来传输用户PPP包。这些增强允许为在PAC和PNS之间传输用户数据的隧道提供低层拥塞控制和流控制。这种机制允许高效使 用隧道可用带宽并且避免了不必要的重发和缓冲区溢出。PPTP没有规定特定的算法用于低层控制，但它确实定义了一些通信参数来支持这样的算法工作。 PPTP缺点：   * 不支持QOS * 每个用户一个隧道 * 认证和加密比较脆弱   相关的配置请参照PPTP 配置Layer 2 Tunneling Protocol （L2TP） L2TP协议提供了对PPP链路层数据包的通道（Tunnel）传输支持，允许二层链路端点和PPP会话点驻留在不同设备上并且采用包交换网络技术进行信 息交互，从而扩展了PPP模型。L2TP协议结合了L2F协议和PPTP协议的各自优点，成为IETF有关二层隧道协议的工业标准。   * L2TP Access Concentrator (LAC) ：表示L2TP访问集中器，类似于PPTP中的PAC，是附属在交换网络上的具有PPP端系统和L2TP协议处理能力的设备。LAC一般是一个网络接入服 务器NAS，主要用于通过PSTN/ISDN网络为用户提供接入服务。 * L2TP Network Server (LNS) ：表示L2TP网络服务器，也叫做“home gateway”，类似于PPTP中的PNS，是PPP端系统上用于处理L2TP协议服务器端部分的设备。   L2TP隧道建立过程：   1. 用户使用PPP拨号到ISP，并获得一个IP地址。客户端和ISP之间建立邻接，客户端能够接入到Internet。这个步骤是用来作为普通的Internet连接 2. 客户端决定建立一个端到端的L2TP隧道到home gateway，并在下面建立一个新的PPP会话之前前会使用控制会话建立一个隧道 3. 在L2TP隧道里建立一个新的PPP隧道，并分配给客户端一个IP地址。客户端和home gateway之间会使用virtual point-to-point，通过PPP封装进L2TP隧道，建立一个新的IP邻接关系。   建立IPSec保护的L2TP VPN：   1. 客户端使用PPP拨入ISP，ISP分配IP地址给客户端 2. 客户端使用L2TP通过一个VPN端口连接到home gateway 3. home gateway使用AAA服务器对隧道进行认证，并分配一个隧道内部IP地址给客户端 4. 在客户端和gateway之间建立IPSec，来提供L2TP会话的加密。   VPDN拨号用户与总部路由服务器建立连接的过程如下：   1. 拨号用户拨打一个初始化呼叫有VPDN访问接入服务器（NAS） 2. NAS 接收此呼叫，并将启动一个到总部路由服务器（Home Gateway）的L2TP Tunnel 协商：Home Gateway 利用总部的Radius服务器来鉴定NAS 的Tunnel ID，认证通过以后，向NAS发起CHAP Challenge 信号；NAS对来自Home Gateway的Tunnel 进行认证，认证通过之后，就建立了NAS和Home Gateway之间的Tunnel连接。此时，Home Gateway就可以利用其Radius服务器对VPDN用户进行用户级的认证，如果认证通过将建立Home Gateway和用户间的端到端的PPP连接。如果在NAS和Home Gateway之间建立了Tunnel连接之后，又有另一VPDN用户拨打同一NAS，此时将不会重复上述建立Tunnel的过程，而是直接进行用户级的 认证。 3. 从拨号用户发出的帧被NAS接收到以后，被封装在L2TP中，通过IP隧道被转发到总部路由服务器。这样，用户就可以对总部的信息进行访问，实现信息共享。   两种典型的L2TP隧道模式   1. 由远程拨号用户发起： 远程系统拨入LAC，由LAC通过Internet向LNS发起建立通道连接请求。拨号用户地址由LNS分配；对远程拨号用户的验证与计费既可由LAC侧的代理完成，也可在LNS侧完成。 2. 直接由LAC客户（指可在本地支持L2TP协议的用户）发起： 此时LAC客户可直接向LNS发起通道连接请求，无需再经过一个单独的LAC设备。此时，LAC客户地址的分配由LNS来完成。   L2TP的优势   * 灵活的身份验证机制以及高度的安全性： L2TP协议本身并不提供连接的安全性，但它可依赖于PPP提供的认证（比如CHAP、PAP等），因此具有PPP所具有的所有安全特性。L2TP也可与 IPSec结合起来实现数据安全，这使得通过L2TP所传输的数据更难被攻击。L2TP还可根据特定的网络安全要求在L2TP之上采用通道加密技术、端对 端数据加密或应用层数据加密等方案来提高数据的安全性。 * 多协议传输： L2TP传输PPP数据包，这样就可以在PPP数据包内封装多种协议。 * 支持RADIUS服务器的验证： LAC端将用户名和密码发往RADIUS服务器进行验证申请，RADIUS服务器负责接收用户的验证请求，完成验证。 * 支持内部地址分配： LNS可放置于企业网的防火墙之后，它可以对远端用户的地址进行动态的分配和管理，可支持私有地址应用（RFC1918）。为远端用户所分配的地址不是Internet地址而是企业内部的私有地址，这样方便了地址的管理并可以增加安全性。 * 网络计费的灵活性： 可在LAC和LNS两处同时计费，即ISP处（用于产生帐单）及企业网关（用于付费及审计）。L2TP能够提供数据传输的出入包数、字节数以及连接的起始、结束时间等计费数据，可根据这些数据方便地进行网络计费。 * 可靠性： L2TP协议支持备份LNS，当一个主LNS不可达之后，LAC可以重新与备份LNS建立连接，这样增加了VPN服务的可靠性和容错性。   该协议是一种工业标准的Internet隧道协议，功能大致和PPTP协议类似，比如同样可以对网络数据流进行加密。不过也有不同之处，比如PPTP要求 网络为IP网络，L2TP要求面向数据包的点对点连接；PPTP使用单一隧道，L2TP使用多隧道；L2TP提供包头压缩、隧道验证，而PPTP不支持。 L2TP协议是由IETF起草，微软、Ascend、Cisco、3COM等公司参予制定的二层隧道协议，它结合了PPTP和L2F两种二层隧道协议的优 点，为众多公司所接受，已经成为IETF有关2层通道协议的工业标准，基于微软的点对点隧道协议 (PPTP)和思科2层转发协议(L2F)之上的，被一个因特网服务提供商和公司使用使这个虚拟私有网络的操作能够通过因特网。 |