虚拟专用网络技术及实现

东北财经大学信息系　田青
大连海事大学计算中心　徐薇

VPN技术是近一年来IT业最热门技术。本文简要介绍了VPN工作原理，并就企业如何构建VPN提出了方法和步骤。

引　言

1998年全球信息产业最热的三项技术是IP电话、电子商务和虚拟专用网络(VPN)，1999年VPN技术则成为国际网络市场最热门话题。据国外的预测和调查，到2001年，网络服务提供商（ISP）将通过VPN获益90亿美元，购买VPN产品的企业也可通过它削减建网成本、吸引新客户、节省大量的远程通信费用，广泛利用信息资源并获得高收益（尤其是IT产业）。那么，

到底什么是VPN呢?

虚拟专网即VPN（Virtual Private Network），它是企业跨越公共网络（目前主要是Internet）建立的安全的为企业自用的专用网络，人们称之为“公网私用”的VPN。通过VPN可以使企业的信息在公共网络(Internet)上传输，其效果就像在广域网中为企业建立了一条专线，安全可靠、方便快捷。在VPN技术的支持下，用户要想进入企业网，不论他在何处，只需连入当地的Internet或ISP提供的网络，即可通过公网连入企业内部网，从中获取信息。

VPN工作原理

VPN系统可由分布在不同地方的多个专用网络（主要是企业内部网）构成，这些专用网络之间可以利用公共网络进行安全通信，在公共网络上传输的信息通过复杂的算法加密，保证VPN用户的数据安全传输。图1是企业内部专用网络及远程用户通过公共网络连接起来的示例，图中各个内部网络位于VPN设备后面，并通过路由器接入公共网络。

图中隧道指专网数据加密后在公网中通过的多层虚拟通道。隧道从一个VPN设备开始，通过路由器横跨整个公网到达其他VPN设备。

在VPN系统中，用户要通过公网向其他专网发送数据，一般要经过如下几个过程:

(1) 主机发送明文信息到连接公共网络的VPN设备;

(2) VPN设备根据网络管理员设置的规则，确定是否需要对数据进行加密或让数据直接通过；对需要加密的数据，VPN设备对整个数据包（包括要传送的数据、源IP地址和目标IP地址）进行加密和附上数字签名（鉴别);

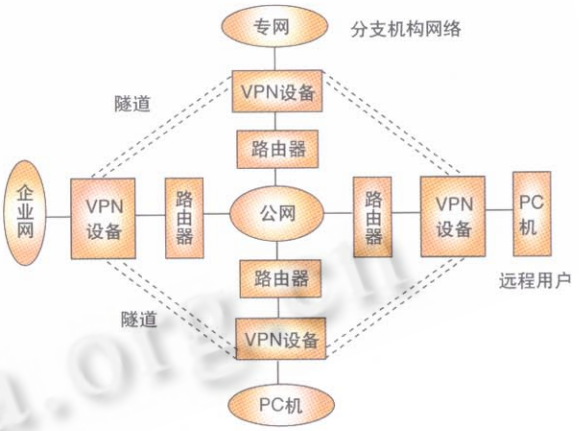

图1　VPN示例

(3) VPN设备加上新的数据报头，其中包括目的地VPN设备需要的安全信息和一些初始化参数;

(4) VPN设备对加密后数据、鉴别包以及源IP地址、目标VPN设备IP地址进行重新封装，重新封装后数据包通过虚拟通道（隧道）在公网上传输;

(5) 当数据包到达目标VPN设备时，数据包被封装，数字签名被核对无误后数据包被解密。

在这种VPN结构中，数据按照严密的算法在公网中通过隧道从一端VPN设备到达另一端。通过数字证书来标记整个隧道，并以此来鉴别属于此VPN的隧道。VPN系统根据系统设置的安全规则表实施数据通信，对用户来

说完全是透明的和自动的。在VPN系统后面的员工照样上网发送电子邮件或下载文件，由VPN系统决定他们的任务哪些需要加密或不加密。

VPN使用的协议

VPN主要采用的隧道技术以及加密、身份认证等方法。其中，隧道是由隧道协议形成的。VPN使用的协议主要有三种，即PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）、L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）、IPSec（IP security，IP安全协议）。

PPTP协议是PPP协议的扩展，在推出之初的是为了拨号VPN，这种协议通过使用户拨号进入本地ISP并利用隧道技术接入企业网络。PPTP支持Windows NT、95和98，在Windows 平台上运行PPTP可以无缝地构建和维护VPN。

L2TP协议包括PPTP和L2F（Layer 2 Forwording）协议，支持多路隧道。基于Layer 2的VPN封装了IP协议IPX、AppleTalk等非IP协议，如图2所示。

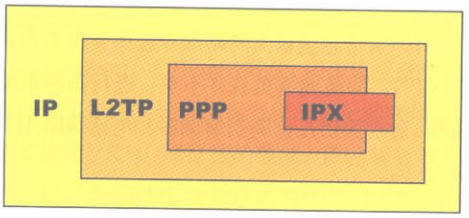

图 2 VPN使用的协议

协议是用来增强VPN安全性的标准协议。IPSec包含了用户身份认证、查验和数据完整性等内容。标准化的IPSec能实现来自不同厂商的产品相互混合及相互匹配。不过，在为远程用户构建VPN时，IPSec需要在使用者的每个桌面系统上加载特殊的客户软件，相对来说，比较繁琐。

VPN选择方案

根据业务类型，VPN业务大致可分为三类，在此我们引用Cisco的定义方式，将三种用户需求定义为：Intranet VPN、Access VPN与Extranet VPN。所谓Intranet VPN即企业的总部与分支机构间通过公网构筑的虚拟网。AccessVPN是指企业员工或企业的小分支机构通过公网远程拨号的方式构筑的虚拟网。Extranet VPN即企业间发生收购、兼并或企业联盟，使不同企业网通过公网来构筑的虚拟网。其中我们通常把Access VPN叫做拨号VPN，即VPDN，将Intranet VPN和Extranet VPN统称为专线VPN或场地到场地的VPN。根据上述分类，作为拥有网络资源的大型网络服务提供商ISP，推广VPN业务的种类也相应分为拨号VPN业务和专线VPN业务两类。

（1）拨号VPN业务。拨号VPN是对ISP最具实际意义的解决方案。拨号VPN的隧道发起又分为由用户发起、ISP拨号服务器（NAS）发起或企业网远程路由器发起三种。真正使用较多的是通过NAS发起的VPDN。VPDN的核心是L2TP协议，通过L2TP开展的VPDN，能为企业用户带来这样的利益：企业员工到ISP的各节点出差或办公时，可通过当地的市话直接拨号上网，并访问企业网。以中国电信169为例，若开通了VPDN业务，公司的员工到各地出差时，只需拨打当地的169，然后输入用户名、口令即可。认证结束后，用户可以直接登录到自己公司的NT域服务器，与其他员工共享信息，企业员工不必在ISP上拥有自己的账号，只要使用自己在企业网中的账号和口令拨号上网即可。企业员工通过上网可以真正得到企业网中的可用信息，而这些企业网信息是通过公网上普通的拨号上网无法得到的。

（2）专线VPN业务。专线VPN为用户提供的是安全可靠，并具有QoS（服务质量）保障的虚拟专网。专线VPN主要服务于三大类客户：第一类是国家政府机构，各大部委；第二类是在国内各地拥有众多办事处的大型企业；第三类是在华经商的外企分支机构。

对于第一类客户，政府机关可以通过ISP分布在全国各地的节点直接上网，并通过IPSEC实现各分支机构的隧道建立和安全通信，使政府或部委的特定机构（如海关，税务等）的通信安全得到保障。

对于第二类用户，ISP可通过批发VPN端口为其提供服务。企业网的各节点通过ISP的VPN设备进行接入，完成企业网内部通信的要求。该项业务可以同VPDN一起，由ISP为企业提供全面的VPN解决方案。

对于第三类用户，客户群较大，但企业的总部设在国外，构建VPN时，要通过国际链路，跨越多个ISP，因此国内的ISP无法保障其应用所需的QoS。这种情况下，企业网的建设者可以不依赖ISP而直接通过公网来实现VPN。

不同的企业用户可根据自身情况选择不同的VPN解决方案。

企业如何构建 VPN

企业构建VPN具有成本低、开销少、灵活度高等优点，在具体实施时，可按照几大步骤进行：

（1）明确远程访问要求。企业首先要明确需要与何种公网连接，用户是通过局域网、广域网还是拨号链路进入企业专用网络，远程用户是否为同一机构的成员等等问题。此外，企业决策者还应解决VPN特有的几个问题，即远程访问的资格、可执行的计算能力、外联网连接的责任以及VPN资源的监管、为出差旅行的员工及远程工作站的员工提供访问步骤等。当然，决策中还应包括一些技术细节，例如加密密钥长度等。如果VPN的加密算法要求公开认证，则还需要法律的支持保护。

（2）选择VPN设备。可选择的VPN产品很多，但产品基本上可分成三大类，即基于硬件的VPN、基于软件的VPN和基于防火墙VPN。

硬件VPN产品是典型的加密路由器，其优点是速度快，且由于在设备中存储了加密密钥，较之相应的软件产品更不易被破坏。

基于软件的VPN则可能提供更多的灵活性。例如它们允许根据地址或协议打开通道，根据流量类型的不同在远程站点遇到混合信息流时分优先级等。

基于防火墙的VPN则利用了防火墙安全机制的优势，对内部网络访问进行限制。此外，它们能执行地址翻译、满足严格的认证功能要求、提供实时报警、并具备广泛的登录能力。大多数商业防火墙还能通过剔除危险或不必要的服务加固主机操作系统内核。此外它还能提供操作系统保护。

对于这三种VPN产品各有其优缺点，选择时要结合具体情况加以考虑。

（3）选择VPN服务器位置及配置网络设备。构建VPN系统可以利用企业原有的资源（局域网），构造VPN首先要确定VPN服务器的位置，其次，要配置网络地址翻译器等其他网络设备。

VPN服务器放置的位置应考虑不同的情况。对于期望通过远程访问复制办事处工作环境的员工来说，VPN服务器最好直接放在专用网络中，但这种方法容易成为攻击者的攻击目标。而对于一个企业中绝大多数远程用户属于外部机构的情况，将VPN设备放在DMZ（“非军事区”）网络上意义更大，这种放置使屏蔽DMZ的防火墙更有助于保护其间的设备，使之免于内部和外部的威胁。

（4）安装和配置VPN。不同的VPN产品安装的方法不同，要注意的是基于软件的VPN和基于防火墙的VPN产品在安装前，首先要从服务器中取消所有不必要的服务、应用程序和用户帐户，确保安装最新的、安全的产品，确保VPN系统的安全。在对VPN进行配置时，通常网管员要为一系列因素设定参数，例如密钥长度、主要与次要认证服务器及相关的共享秘密资源、连接和超时设置、证书生成、密钥生成和分布机制等。

（5）监控和管理VPN。这一步是要建立监控Internet连接的机制，它可以测定VPN对网络的利用和吞吐量，而且也是培训服务台员工操作VPN设备及认识认证服务器和防火墙互相间的影响的重要一步。

另外，机构中的所有网管员都应该了解VPN的基本操作，认识到管理VPN的人不应该只是那些安装和配置VPN的人，最终用户也需要接受Internet连接及VPN软件工作原理的基本培训。而且，让最终用户接受一些基本故障排除方法的培训，从而使他们能自己解决一些小故障。

（6）进行备份。随着用户对VPN的进一步熟悉，企业可能会涉及到一些由任务决定的应用程序，例如公司要为客户建立一个电子商店。在这样的情况下，备份连接是必须的，因此，网管员在设计网络阶段就应为冗余链路和设备制定计划。信息流量大的站点应选择支持多设备负载均衡的VPN。即使网络负载并不重，进行备份也能尽量避免麻烦。通常保留几台调制解调器和电话线路用于紧急情况就够了。

结束语

VPN技术的直接受益者是ISP和企业，首先ISP将VPN作为网络服务的一项增值业务推向企业，企业要向ISP付费从而使ISP从企业得到回报。此外，VPN技术最终目的是服务于企业，为现代企业的信息共享提供安全可靠的途径，企业因而从中获得可观的经济效益（尤其是在以知识经济为背景的未来社会）。

由于VPN能真正为ISP和企业带来利益，VPN在国外已形成产业，各大IT厂商都在积极推进VPN技术，开发新产品，很多企业也构建了自己的虚拟专网，并从中获益。随着我国信息化建设的进一步发展，相信未来几年我国企业也将逐步认识到VPN的价值并更多地利用它。■

参考文献

(1) 杨心强，数据通信与计算机网络，北京：电子工业出版社，1996

(2) 张涛，公网私用的VPN技术，软件世界，1999，(5)

(3) 王高华，怎样选择VPN方案，计算机世界，1999，(3.22)