网络工程师系列丛书

虚拟专用网（VPN）精解

- VPN技术世界领先
- 解决方案全面细致
- 内容讲解深入浅出
- 轻松组建虚拟专用网

王达　等编著

清华大学出版社
http://www.tup.tsinghua.edu.cn

网络工程师系列丛书

虚拟专用网(VPN)精解

王 达 等 编著

清华大学出版社

北 京

内 容 简 介

本书主要针对微软的 Windows 系统，特别是对 Windows 2000 系统中的虚拟专用网（VPN）方案做了详细而又准确的介绍，有许多安全配置方案是作者率先进行了书面系统阐述。在最后 3 章中主要介绍各种硬件 VPN 方案的主要特点，以及 3Com 和 Cisco 两个网络设备商的硬件 VPN 方案。读者阅读本书后即可全面掌握基于 Windows NT 4.0 及 Windows 2000 系统中的 VPN 方案配置方法，并且对主要网络硬件设备商 3Com 和 Cisco 的 VPN 方案有一个基本的了解，对从事实际 VPN 网络组建有所裨益。

本书特点是非常系统地对各方案的配置方法都采用了 Step-by-Step 的方式，一步步地进行实际的配置介绍，图表丰富，便于读者的理解。本书非常适用于网络工程人员或网络爱好者自学，也可作为网络培训机构的培训教材。

图书在版编目（CIP）数据

虚拟专用网（VPN）精解/王达等编著. —北京：清华大学出版社，2004.1
（网络工程师系列丛书）
ISBN 7-302-07688-X

I. 虚… II. 王… III. 虚拟网络 IV. TP393.01

中国版本图书馆 CIP 数据核字（2003）第 106046 号

出 版 者：清华大学出版社　　地　　址：北京清华大学学研大厦
http://www.tup.com.cn　　邮　　编：100084
社总机：010-62770175　　客户服务：010-62776969

组稿编辑：丁　岭
文稿编辑：陶萃渊
封面设计：王　永
印 装 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　印张：34.25　字数：852 千字
版　　次：2004 年 1 月第 1 版　2004 年 1 月第 1 次印刷
书　　号：ISBN 7-302-07688-X / TP・5633
印　　数：1~4000
定　　价：48.00 元

前　言

VPN（虚拟专用网）网络技术早在几年前就出现，并得到许多网络设备商、软件系统商的支持。如 Microsoft 公司从 Windows 95 开始就提供支持，在 Windows 98 系统中得到了初步完善。在服务器版本的 Windows NT Server 4.0 系统中，通过后来开发的补丁程序也可以实现 VPN 服务器和客户端的双重支持。许多企业用户也声称将采用这一新技术，于是在 1999 年 VPN 出现了它的第一鼎盛时期，成为当时业界的焦点。但由于 VPN 在当时还算是新生技术，在许多方面，特别是安全性方面都还相当不完善，使得有些企业用户在应用过程中受到了网络安全的威胁。于是 VPN 网络技术在得到短暂应用后即受到巨大的阻力，一度出现了停滞状态，甚至有人认为 VPN 技术也像当时的.com 一样属泡沫技术。

但是随着各网络设备商和软件系统商的努力，VPN 网络不仅在安全性方面得到了相当大的改进，在其他技术方面也全面得到扩充。特别是随着 2000 年 Windows 2000 系统的正式发布，原来一直对 VPN 网络技术支持不够全面、彻底的不良局面得到了改善。自 Windows 2000 系统开始对传统的 IPSec VPN 方案提供了全面支持，不仅可以提供原来 PPTP 隧道协议 VPN 的方案支持，而且还提出了新的 L2TP 隧道协议 VPN 方案，VPN 的应用得到前所未有的推进。在 2003 年 4 月份 Microsoft 推出了其最新操作系统 Windows 2003，在这个操作系统对 VPN 技术的支持更是前所未有。在硬件方面，各网络设备商也投入了极大的热情，开发了不同方案的 VPN 设备，目前主要包括集中器、交换机、路由器、防火墙等，使 VPN 设备得以推广，由于技术的成熟和激烈的竞争，也使各种 VPN 设备价格得到大幅下调。由此我们完全可以预料，有了 Windows 2000/Windows 2003 的全面支持，VPN 网络技术正在迎来它的第二个春天。

说到 VPN 网络的优势，许多人都有一个基本的概念，那就是可大大节省网络构建和通信费用。以前采用数据专线方式构建企业之间网络的互联，所花的成本仅少数大公司才敢过问，就拿一条 64KB 的 DDN 专线来讲吧，一个月下来的专线通信费就近 2 万元（不同地区或许有所不同），绝大多数的中小型企业就不可能接受。如果采用传统拨号方式，那通信费更是不敢想象，如果两个企业网络之间分属于不同的地区，则需要承担昂贵的长途通信费。但使用 VPN 网络技术，企业网络间根本不需要构建专门的物理连接，也不需要拨长途，而是通过公用网，如因特网进行逻辑连接。这样用户就不必花费巨额的资金来构建专门的物理连接网络，也不再需要拨长途进行通信了，只需要在本地与 ISP 连接，大大节省了通信费用。当然，VPN 网络的优势其实远不止以上所说的这些，我们都将在书中详细介绍。

本书主要介绍了目前主流的服务器操作系统 Windows 2000 Server 系统中的各种 VPN 方案应用、配置方法，以及主要网络设备商的 VPN 方案。本书所介绍的内容非常系统地、全面地、条理清楚地采取 Step-by-Step 的方式，一步步向读者介绍各种 VPN 方案的配置方法，图文并茂，并且所有图形界面都是从实际的网络环境所得，非常便于读者自学，并可作为培训机构的培训教材。

本书由王达主笔统稿，何艳辉、王珂、王志军、何江林、沈春奇、温武、刘冬青、周建辉、苏国强、沈芝兰、高林、李玉卿、周刚、肖强、沈倩等同志参与了编写、录入及排版工作，作者所在单位许多同事给予了大力支持，在此对他们表示感谢。由于水平有限，尽管力争完善，但仍可能无法完全避免不正确和疏漏之处，恳请读者批评指正。

作　者

2003 年 12 月

目　录

第 1 章　计算机网络 VPN 基础

VPN 是一种新型的远程网络访问技术，它的出现已有好几年的历史，但在近两年内得到了企业用户的广泛关注。越来越多的网络设备开发、生产商投入到 VPN 设备的开发和技术支持，微软自 Windows 2000 系统以来也对 VPN 技术提供了全面的支持。本章将从纯技术角度对 VPN 技术做一个综合介绍。

1.1　VPN 的产生及前景

随着企业的收购和合并愈演愈烈，再加上企业自身的发展壮大与国际化，每家企业的分支机构不仅越来越多，而且它们的网络基础设施互不兼容也更为突出。以前各分支机构互访所采用的常规方法是租用专线，这样的连接方式一则要支付昂贵的通信费用，再则缺乏灵活性，对于企业地理位置的改变不能很好地适应。随着企业业务和自身应用需求的发展，企业之间的合作及企业与客户之间的联系也日趋紧密，且这些合作和联系都是动态的，总是处于变化和发展之中，这种关系也需要靠网络来维持和加强。这样不但带来了网络的复杂性，还带来网络的管理和安全性问题。如果仅通过公用的因特网（Internet）是很难保证其安全性的，因为因特网是一个全球性和开放性的、基于 TCP/IP 技术的、不可管理的国际互联网络，基于因特网的商务活动就面临信息威胁和安全隐患。如果采用传统的租用专线，虽然在安全性方面有足够的保证，但是仍不能从根本上解决企业用户的实际困难。在这样的背景下，一种基于公用网络的动态、安全的连接解决方案就成为时代之需，VPN 技术就是这样一种网络连接技术。VPN 技术的成功引入可以从根本上满足企业用户的低通信费和高灵活性的双重需求，更重要的是它可以提供与专用线路相媲美的通信安全保障，是一种非常廉价、安全、灵活自如的远程网络接入解决方案。

VPN（Virtual Private Network）中文名为“虚拟专用网”。它并不是一个新的名词，因为在电信服务中，早在电话网络中就提出了 VPN 的概念，而本书所讲的全是关于计算机网络中的 VPN 技术，它是专指基于数据网络为企业联网访问提供的虚拟专用网技术（若在本书中没有特别指明，都是指计算机网络中的 VPN，而不是指电信中的 VPN）。同时，VPN 技术既可以在 IP 网络中实现，也可以在诸如 ATM 等非 IP 网络中进行，但在本书中仅对 IP 网络服务中的 VPN 技术进行介绍。

近几年来，许多企业已经利用经济有效的 VPN 来传送话音业务，并从中受益。使这一切成为可能的基础是大量已经建成的网络基础设施。只有在互联网和 Web 飞速发展的前提条件下，可用于数据网络的共享资源才有可能以同样的速度增长。在当今话音、视频和数据汇聚的时代，对网络的需求正在以惊人的速度增加。

VPN 代表了当今网络发展演化的最高形式，它综合了传统数据网络的性能优点——安

全和 QoS(Quality of Service,服务质量)，和共享数据网络结构的优点(简单和低成本)，必将成为未来传输完全汇聚业务的主要工具。拥有新一代技术优势的企业已经开始着手进行此项工程。

VPN 是一个极有前途的技术，它能使你的企业脱颖而出。随着企业全球化进程的不断深入和移动办公队伍的不断增长，网络主管们越来越认识到 VPN 的巨大优势，这种网络技术也正在越来越多地被加以采用。VPN 代表了当今网络发展的最新趋势，能够提供远程访问、外部网和内部网的连接，价格比专线或者帧中继网络要低得多。而且 VPN 在降低成本的同时满足了对网络带宽、接入和服务不断增加的需求，迎合了用户对安全性和网络性能的追求，并且可以较以前的产品提供更为丰富的特性和功能。因此，VPN 必将成为未来企业传输业务的主要工具。根据 Infonet Research 公司（为美国的一家比较有名的互联网市场调研公司，其网址为：www.infonetresearch.com）的 2002 年所做统计报告发现：VPN 产品、系统集成和服务的市场在过去的几年中都以每处超过 100%的增长率发展，从 1997 年的 2.05 亿美元到 2001 年的 119 亿美元。而据 Infonetics Research 公司（是一家 1997 年成立的美国互联网市场调研公司，它在全球都非常有名，它的业务覆盖北美、欧洲、亚洲以网络数据和通信工业，它的网址为：www.infonetics.com）最近研究表明，欧洲的 VPN 产品及服务将在 2002 年—2006 年间得到 150%以上的发展，业务量从 2002 年的 5.4 亿美元增长到 2006 年的 13.2 亿美元。而对全球的预测中，在 2003 年—2007 年中，VPN 服务及产品市场增长率也都在 42%以上，市场量从 25.3 亿美元增长到 35.8 亿美元。另还据 Infonetics Research 公司的最新调查显示，2003 年上半年全球虚拟专用网（VPN）和防火墙硬件与软件的销售收入为 7.05 亿美元，增长率为 1%，今年第二季度将达到 8.74 亿美元。

使用 VPN 网络，无论采用哪种协议，计算设备（PC、笔记本电脑、数字助理等）都可通过服务提供商的本地访问点协商连接，创建通道。一般来说，在目的地 LAN（局域网）的 RADIUS（远程验证拨入用户服务）服务器验证用户，建立恰当的网络授权，当然服务提供商也可以提供验证和授权，作为连接服务的一部分。然后，发送者在服务提供商的网络上向目的地 LAN 发送加密数据。

1.2 VPN 基础

VPN 是利用公网（如因特网或网络服务提供商的 IP 骨干网）或专网（局域网）来构建的虚拟专用网络，是通过特殊设计的硬件和软件，直接通过共享的 IP 网所建立的隧道来完成的。通过 VPN 可以实现远程网络之间安全、点对点的连接。VPN 是专用网络的延伸，它包含了类似因特网的共享或公共网络连接。它的基本点就是化公为私，使每个企业可以临时从公用网中挖走一部分地盘供自己专用。于是，企业网络想连接到哪里都可以，保密性、安全性、可管理性的问题也容易解决了，而且还可以降低网络的使用成本。

VPN 以其更低的网络运营成本实现更加灵活、更加自由的局域网延伸，它与租用专线网络方式相比，无论是从运营成本上，还是从其性能上来说都具有无可替代的优势，更值得一提的就是人们普遍关心的网络数据通信安全方面，随着 VPN 技术的日益完善，目前

VPN 网络的安全性能也完全可以与物理专线网络方式相媲美，因此赢得了越来越多企业用户的青睐。

1.2.1　VPN 的组成

VPN 是一门新型的网络技术，它为我们提供了一种通过公用网络（如最大的因特网）安全地对企业内部专用网络进行远程访问的连接方式。我们知道一个网络连接通常由三个部分组成：客户机、传输介质和服务器。VPN 网络同样也需要这三部分，不同的是 VPN 连接不是采用物理的传输介质，而是使用一种称之为“隧道”的技术来作为传输介质的，这个隧道是建立在公共网络或专用网络基础之上的，如因特网或专用 Intranet 等。同时要实现 VPN 连接，企业内部网络中必须配置有一台基于 Windows NT 或 Windows 2000 Server（目前 Windows 系统是最为普及，也是对 VPN 技术支持最为全面的一种操作系统）的 VPN 服务器。VPN 服务器一方面连接企业内部专用网络，另一方面要连接到因特网或其他专用网络，这就要 VPN 服务器必须拥有一个公用的 IP 地址，也就是说企业必须先拥有一个合法的因特网或专用网域名。当客户机通过 VPN 连接与专用网络中的计算机进行通信时，先由 NSP（网络服务提供商）将所有的数据传送到 VPN 服务器，然后再由 VPN 服务器将所有的数据传送到目标计算机。因为在 VPN 隧道中通信能确保通信通道的专用性，并且传输的数据是经过压缩、加密的，所以 VPN 通信同样具有专用网络的通信安全性。整个 VPN 通信过程可以简化为以下 4 个通用步骤：

（1）客户机向 VPN 服务器发出请求。

（2）VPN 服务器响应请求并向客户机发出身份质询，客户机将加密的用户身份验证响应信息发送到 VPN 服务器。

（3）VPN 服务器根据用户数据库检查该响应，如果账户有效，VPN 服务器将检查该用户是否具有远程访问权限；如果该用户拥有远程访问的权限，VPN 服务器接受此连接。

（4）最后 VPN 服务器将在身份验证过程中产生的客户机和服务器公有密钥将用来对数据进行加密，然后通过 VPN 隧道技术进行封装、加密、传输到目的内部网络。

典型的 VPN 网络连接简化示意图如图 1.1 所示。

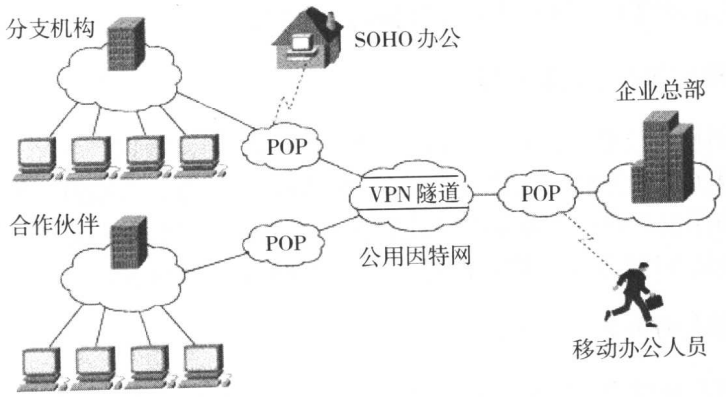

图　1.1

注意：在实际的 VPN 网络中要比图 1.1 所示结构复杂许多，主要体现在加入了许多 VPN 专用设备，如 VPN 路由器、交换机或者防火墙，这些专用设备的加入可以大大加强网络的数据交换或者网络安全性能，就像我们常见的 LAN 一样，在较完善的 LAN 中通常不仅包括工作站、传输介质（如双绞线）和服务器，实际上也可能包括集中器、交换机、路由器或者防火墙等。有关 Windows 系统中 VPN 构建和配置将在后面的章节中详细介绍。

1.2.2 VPN 网络与专线网络的区别

在 VPN 技术真正得到应用之前，企业用户要与远程网络进行连接，通常所采用的是租用专用线路，如帧中继、DDN、ATM 等，这个代价不是一般企业可以接受的。而且在电信部门租用的帧中继（Frame Relay）与异步传输模式网（ATM）等数据网络提供永久虚拟线路（PVC-Permanent Virtual Circuit）来连接需要通信的单位，所有的权限掌握在别人（服务提供商 NSP）的手中。如果用户需要一些别的服务，需要填写许多的单据，再等上相当一段时间，得到服务商的验证后，才能享受到新的服务。更为重要的是两端的终端设备不但价格昂贵，而且需要一定的专业技术人员管理，无疑增加了成本。还有，帧中继、ATM 数据网络也不会像因特网那样，可立即与世界上任何一个使用因特网的单位连接，不具有交换功能。而本书所介绍的 VPN 技术是通过因特网来进行远程网络连接的，用户完全可以控制自己与其他使用者的联系，同时支持拨号的用户，并且在投资成本上具有绝对的优势。

下面具体介绍 VPN 网络与传统的专线网络相比所具有的明显特点，主要体现在以下几个方面。

1．采用传输媒体不一样

整个 VPN 网络的任意两个节点之间的连接没有传统专网建设所需的点对点的物理链路，而是架构在公用网络 VPN 服务提供商 ISP 所提供的网络平台之上的逻辑网络。用户的数据是通过 ISP 在公共网络（如因特网）中建立的逻辑隧道（Tunnel），即点对点的虚拟专线进行传输的。然后通过相应的数据加密和身份认证技术来保证用户内部网络数据在公网上安全传输，真正实现在公网传输网络数据的安全性。

2．数据传输和加密方式不一样

VPN 在公用网上要模拟点对点链路，需重新压缩或封装数据，并加上一个提供路由信息的报头，该报头使数据能够通过共享或公用网络到达终点。要模拟专用链路，为保密应加密数据，以确保没有密钥不能从共享或者公共网络截取的数据包解密。封装和加密专用数据之处的链接是 VPN 连接。数据封装和加密过程如图 1.2 所示。

3．网络连接的呼叫方式不一样

VPN 网络客户机使用特定的、基于 TCP/IP 的协议的“隧道协议”，来对虚拟专用网络服务器的虚拟端口进行依次虚拟呼叫。VPN 网络的最常见应用是，虚拟网络客户机使用 VPN 连接到与因特网相连的远程访问服务器上，目前在各大企业网络互联中得到广泛应用。远