New Riders

北京科海培训中心

Windows 2000 虚拟专用网络

[美] Thaddeus Fortenberry 著

陆建业 译

- 提供实际规划与真正设计各种隧道解决方案的文档，包括如何为分支机构和总部进行复杂的远程局域网配置
- 分析和 VPN 有关的所有代理、NAT 以及防火墙配置
- 分步骤地配置 L2TP，PPTP 和 IPSec

清华大学出版社

http://www.tup.tsinghua.edu.cn

NRP 北京科海培训中心

Windows 2000 虚拟专用网络

[美] Thaddeus Fortenberry 著

陆建业 译

清华大学出版社

(京)新登字 158 号

著作权合同登记号:01-2001-0379

内 容 提 要

本书从实用的角度出发,全面地介绍了在 Windows 2000 平台上怎样实现 VPN(虚拟专用网络)技术。全书分别介绍了有关隧道的基本概念、隧道技术及其应用、相关协议、相关服务;涵盖了从路由环境到 NAT、DNS 以及活动目录的知识;给出了 VPN 解决方案的向导;附录还提供了一些重要资料。

本书的目的是写给那些想学习如何配置自己的网络的设计者和管理员。作者以自己丰富的经验给出一种直截了当、并可着手进行的实现 VPN 的方法,是一本很有价值的参考书。

书　名:Windows 2000 虚拟专用网络
作　者:Thaddeus Fortenberry
出版者:清华大学出版社(北京清华大学校内,邮编 100084)
印刷者:北京门头沟胶印厂
发行者:新华书店总店北京科技发行所
开　本:787×1092 1/16　印张:16.875　字数:410 千字
版　次:2001 年 8 月第 1 版　　2001 年 8 月第 1 次印刷
印　数:0001～5000
书　号:ISBN 7-302-04763-4/TP・2822
定　价:32.00 元

关于作者

Thaddeus Fortenberry(MCSE,MCT)是虚拟专用网络和 Windows 平台方面的权威专家。作为 Compaq 的虚拟专用网络项目经理,他设计了隧道以及隧道服务器设置的整体实现方案。从 Windows NT 发布之日起,他就一直致力于对 Windows NT 的研究,并且作为微软的 Windows 2000 Rapid Deployment Program 的参与者帮助实现 VPN 和网络设计。Thaddeus 同时也负责对 Compaq 公司的 Qtest Active Directory 进行管理和设置,Qtest Active Directory 是 Windows 2000 Active Directory 正式发布前的第二个最大测试版本。除此之外,他也是 HappyVPN 测试网络的关键构造者,该测试网络是一个完全建立在使用 Windows 2000 隧道技术的 VPN 连接基础上的分布式网络的活动目录设置。

关于技术评论人员

下面这些评论人员为 Windows 2000 虚拟专用网络的整个开发过程提出了大量的专业意见。对于写作这本书,这些做出了重大贡献的专业人士提供了技术、组织以及流程各方面的内容。他们的反馈意见保证了 Windows 2000 的虚拟专用网络能够提供最高质量的技术信息,从而满足读者的需要。

Gary Olsen 是 Compaq 计算机公司客户服务部门的顾问。他从 Brigham Young 大学获得了工业教育专业的理科学士学位以及计算机辅助设计的科学硕士学位。从 1983 年起,他一直在计算机产业界工作。Gary 在 Windows 2000 Rapid Deployment Program(RDP)工作了大约两年,协助测试新闻组,并同微软的工程师一起查找和纠正错误,编写 KB 文档,撰写培训课程,以及测试发布的测试版本。此外,他还负责训练 Compaq 的 Windows 2000 技术支持工程师并且为 Compaq 和微软的顾客提供活动目录方面的顾问。Gary 在许多会议和网络杂志上发表了一些关于活动目录设计和整合的论文,并在过去的两年中担任了 Compaq 的世界范围的 Qtest Windows 2000 域的企业管理员。Gary 还是 New Riders 出版的"Windows 2000 Active Directory Design & Deployment"一书的作者(ISBN:1-57870-242-9)。

Neil Ruston 为一家大型的瑞士银行在英国伦敦的办公室设置 Perot 系统。他在信息产业界工作了大约 10 年,最初是设计并设置 NetWare 2/3/4 网络。目前他已经获得了 CNE 4 资格。近来,他一直致力于设计基于 NT 的网络,并且获得了微软系统工程师认证资格。他参加了微软的"Joint Development Program(JDP)"项目,并且设计和设置了一个活动目录和域名服务器的体系,以作为 JDP 项目的一部分。从 Windows 2000 的第二个测试版后,他一直使用 Windows 2000。

Jan De Clercq 是 Compaq 的技术领导小组(TLG)的高级顾问。最初他的研究重点是电

子商务以及微软平台的安全问题。Jan 已经撰写了若干本 Compaq 白皮书，并在杂志上发表这些方面的 Windows 2000 文章。此外，他还在微软会议，RSA 实验室会议以及 EMA 会议上宣讲了论文。Jan 参与了若干个和 Windows、安全以及 PKI 有关的大型 Compaq 账户项目。在过去的一年中，他为若干个大型的 Windows 2000 设计和设置提供了大量值得信赖的有关安全方面的建议。

Warren Barkley 在技术部门工作了十多年。他获得了若干个学术学位以及工业方面的资格认证。Barkley 先生为很多小型或大型的机构担任了网络基础结构的顾问工作。此外，他还编写了几本有关网络和网络安全的技术白皮书。Warren 和他的妻子以及两个儿子一起生活在西雅图地区。

Patrick“Swissman”Ramseier(CCNA，GSEC，CISSP)是 Exodus 通信设备有限公司的高级安全顾问小组的安全专家。Exodus 为企业提供带有关键的 Internet 操作的复杂 Internet 主机，并在供应商中处于领导地位。Patrick 开始是 UNIX 的系统管理员。在过去的 12 年中，他参与了公司安全结构审查，脆弱性评估，虚拟专用网络支持，网络和操作系统安全支持(UNIX-Solaris，Linux，BSD 以及 Windows NT)等方面的培训、研究以及开发。他获得了商业的文学学士学位，并同时攻读计算机科学专业的硕士和博士学位。

前 言

在 Windows 2000 开发阶段的早期，微软就为大多数用户定义了一种方式，使得他们在确保产品与现实世界中的应用能够很好的吻合方面，能扮演更为积极主动的角色。他们通过创建“快速应用程序(Rapid Deployment Program，RDP)”，以及后来的“联合应用程序(Joint Deployment Program，JDP)”做到了这一点。其中每种程序都包括了两个独立的阶段。第一阶段就是找到大约 250 名用户，让他们在一个“近产品环境(near production environment)”下，统一使用上百台的工作站和服务器，当出现问题的时候，他们可以和微软密切协作。另一个阶段就是从不同的微软的合作伙伴中找一些代表，让他们在支持这些早期应用时，就真正地生活并工作在微软。这种工作持续了 22 个月，只有大约 20 名非微软雇员进行这项工作，我就是这 20 名工作人员之一。

在这一项目中，最令人激动的是：虽然我们来自于相互竞争的公司，但我们却像一个紧密团结的团队，与微软的雇员们一起工作，大家都有一个共同的目标：学习并支持 RDP/JDP 用户。无论我们是谁的雇员，这个团队的所有成员都明白，我们可以彼此依赖，互相帮助，以完成我们的任务。针对 Windows 2000 中不同的主要技术问题，我们被分成小组。我虽然是“专攻虚拟专用网络的网络组”的成员，但我仍然经常和其他的专门项目和研究小组一起工作。我们的职责的一部分包括参加每周例会，例会是由 Windows 2000 的不同的开发小组召开的。这使得我们所有人都可以作为 RDP/JDP 用户的代表，对我们所关心的以及所遇到的问题，提出看法。同样，这也使得我们能够清楚地看到微软的应用程序的开发过程。

我相信，给我印象最深的，莫过于使我认识到，在这样一种具有大规模和复杂度的产品上进行协作，需要付出无法想像的努力。作为一个网络管理员，在前期工作中应用微软的产品时，对于我在应用中发现的包含有“缺陷”的产品，我时常会感到沮丧。在我参加到这一过程的工作中以前，我确实对于开发一个操作系统的规模没有正确的概念。在某一特定的技术领域钻研下去是相当容易的，但是请设想一下，要开发代码来完成某一任务，同时还要保证它对操作系统的其他任何部分都不会产生不良影响，该有多么困难，更不必说如何去应用这些技术了。从某种程度上说，协作不能从技术上进行划分，相反，应该将它看作是一个完整的产品。因此，测试就不能太一般化了。其最终结果就是测试要做的事情太多了。让用户参与这一测试绝对是一个奇特的策略。

有时，要保证一个产品能与其他公司的产品相兼容是十分困难的。微软发起并主办了很多技术活动，在这些活动中，他们邀请了竞争对手参加，共同进行互操作的测试。但是，由于技术发展和改进得如此迅猛，使得要保证所有产品在任何类型的环境下都运行良好是十分困难的。同样，我相信 RDP/JDP 对此是有帮助的，因为我们已经在大量不同的环境中应用了 Windows 2000，而且，在开发阶段的早期发现的许多问题都已经得到了解决。

我相信，早期应用策略是一个巨大的成功。Windows 2000，在很多方面来说，都是一个全新的产品，它需要持续不断地努力学习和测试。在应用 Windows 2000 时，透彻地理解该项目可能的范围，诸如在 VPN 链路上设计一个活动目录(Active Directory)，等等，是十分重

要的。RDP/JDP 程序有助于揭示这些可能性。而你，作为 VPN 的实现者，应该在应用之前，将这一程序作为一个模型来考虑。我相信通过这一过程，就可以设计一个测试网络，并建立起一个样板环境，来进行精确的文件管理和测试。

我有机会能和现实生活中的用户一起参加如此大规模的 RDP/JDP 程序，在其中定位 VPN 问题，这对于我在这本书中所阐述的论点和策略来说是无价的。

Thaddeus Fortenberry

本书介绍

首先，我要强调的是，我并不想写一本只是给读者介绍虚拟专用网络（Virtual Private Network，VPN）概念和理论的书。本书的目的就是要解释如何通过配置 Windows 2000 来使用 VPN，并且说明，为什么使用 VPN 是很有意义的。为了达到这个目的，在本书中我加入了许多关于各种配置的优缺点分析，以及各个配置过程。所以，在你读完此书后，你就应该可以在你自己的网络环境中设计并实现有关技术了。

我将介绍在 Windows 2000 中关于 VPN 技术的功能，不过本书的目的并不是解释 RFC。相反，本书是写给那些想学习如何配置他们的网络的网络设计者和网络管理员的。如果你对每个数据包的详细内容，以及所有这一切是如何工作的详细分析感兴趣的话，那么除了这本书，你还得阅读那些以及讨论有关 ITEF 标准的资料。以我的经验，无论如何，大多数网络管理员对技术的细节都不太感兴趣，远不如对如何应用这些技术、如何保证安全以及如何维护网络感兴趣。根据我的经验，我将给出一种直截了当的、可以着手进行的、在工作场地实现 VPN 的方法。

本书的范围

Windows 2000 引进了很多新的技术，这些新技术都是网络管理必须面对的。Windows NT 4.0 的 VPN 连接性是本身所固有的。而在 Windows 2000 中，VPN 环境必须与大量的其他服务共存，以确保应用的灵活性和持续性。本书不仅仅向读者介绍了所有这些其他服务，还讨论了与这些服务应用相关的问题。

和大多数 VPN 书籍不同的是，我不仅仅局限于讨论客户端访问一个公众网络，我还讨论了大量的其他问题，诸如在基于隧道的链路上应用活动目录（Active Directory）——经过历时两年的大量测试证明，在完全基于 VPN 的基础上配置一个功能完善并且可靠的目录环境是可能的。

不管你实现的是哪一种 VPN 环境，你必须记住，一个 VPN 网络要求较强的灵活性，这是因为不断变化的公众需求和不断变化的技术造成的。事实上，任何设计在技术上都是可能的，但是，在设计网络配置时，你必须解决整个这一项目的所有问题，以确保它满足客户的需求。本书致力于涵盖足够范围的技术和策略，使你能够完成上述任务。

本书的组织形式

《Windows 2000 虚拟专用网络》的各个章节是彼此相关联的，开始是最基本的背景知识，后来逐渐过渡到关于在 Windows 2000 平台上应用 VPN 的更为复杂和特殊的问题。不过，你并不需要逐章阅读，因为本书的每一章都针对的是与 VPN 有关的、非常特殊的一组问题，而且每一章都可以作为独立的参考手册来使用。本书的章节是按照以下方式组织的：

- 第 1 章和第 2 章向读者介绍了关于隧道的基本概念，这对于那些不熟悉隧道技术的管理员来说是十分重要的。
- 第 3 章到第 7 章覆盖了包含在 Windows 2000 中的所有隧道技术问题，这些章节不仅包含有关那些实际的协议的内容，诸如 PPTP、IPSec 和 L2TP，还包含了与应用这些隧道技术相关的服务的有关内容。
- 第 8 章到第 12 章详细讨论了在主局域网/分支办公室环境中应用隧道技术的问题。它们涵盖了从路由环境(包括 RRAS 和 IAS)到 NAT、DNS 以及活动目录的知识，从而表明分支机构的设计可以包括分布式的域控制器。
- 附录则涉及到其他的一些资料，范围从关于 VPN 的相关信息，诸如 OSI 参考模型以及相关的 RFC；将一台 Cisco 路由器配置为一个 Windows 2000 隧道服务器的隧道客户机；对你的隧道配置进行基本的故障查找，以及 VPN 未来的诸多方面内容。

我的目标就是，通过本书来解释在 Windows 2000 网络环境中，你应该怎样实现 VPN 技术，以及为什么要这么做。我把我的经验拿出来与你分享，就是希望你对这一技术能获得全面的理解。

目 录

第 1 章　什么是虚拟专用网络

近年来，随着越来越多的公司纷纷要求与总部中心进行网络连接，对于与远程用户和办公室进行价格便宜、安全的通信的需求增加了。虽然大家都知道，专用线路可靠又安全，但是对于大多数公司来说，它们在经济上是不切实际的。而一个虚拟专用网络(Virtual Private Network，VPN)则是通过利用已有的公共网络基础结构，通常就是 Internet，来仿真一个专用网络。这种网络之所以被冠以“虚拟”二字，是因为它使用的是建立在物理连接基础上的逻辑连接。客户端应用程序并不能意识到实际的物理连接，而且在穿越 Internet 进行路由时，其安全性与在专用网络中进行安全路由的安全性是基本上相当的。当 VPN 被配置好并初始化好之后，应用程序将不能分辨出虚拟适配器和物理适配器的差别。

在一个虚拟专用网络被正确地建立起来之后，它就将公共网络(如 Internet)、帧中继以及异步传输模式(ATM)连接成一个广域网(WAN)，而拨号链路则被看作是一个专用网络。一旦定义并配置了 VPN 的基础结构，它就提供了一种无缝集成，使得网络可以被看作是一个专用网络。

1.1　虚拟专用网络的历史

那么，VPN 是怎样走到今天这一步的呢？就在几年前，VPN 还不存在。最近，在一个相当短的时间周期内，随着与用户保持联系的共同需求的增长，VPN 经历了大量的变化和发展。

有一些厂商，如 IBM、微软以及 Cisco 公司，在 90 年代中期就开始开发隧道技术。虽然诸如基于 IP 隧道的 IPX 和 SNA 等产品在几年前就已上市，但是它们对于它们所处的环境来说是十分特殊的，对于整个产业来说，其应用也是有限的。产业需要一种能够对所有类型的通信来说都是标准的隧道解决方案。这种朝着标准化方向发展的推动力，大部分源于对 TCP/IP 的认可和标准化。

到 1996 年，有些厂商意识到了 VPN 的重要性，并开始一起研究制定隧道协议。这些协议推动了两种主要的 VPN 解决方案：“点对点隧道协议(Point-to-Point Tunneling Protocol，PPTP)”，这是由微软、Ascend、3Com、以及 US Robotics 创建的；“第二层转发(Layer 2 Forwarding，L2F)”，这是由 Cisco 创建的。由于这两种解决方案都是由特定厂商制定的，因此支持厂商的产品在采用这两个协议时不能很好地解决协议互操作的问题。

PPTP 和 L2F 是“开放系统互连(OSI)”的第二层隧道协议，它们被设计成传输第三层协议，如 Apple Talk，IP 以及 IPX，以穿越 Internet。为此，PPTP 和 L2F 利用了已有的第二层 PPP 标准，来传输不同的第三层协议穿越串行链路。第三层的包封装在 PPP 帧中，然后，为了穿越基于 IP 的网络，再将它嵌在 IP 包内进行传输。因为没有一个协议提供数据加密、认证或完整性功能，而这些功能对于 VPN 的私密性来说都是非常关键的，所以这些功能就必须作为独立的过程添加进去。PPTP 将在第 4 章“点对点隧道协议”中详细介绍。

受现存一些隧道协议的缺点所驱使，在 1997 年开始了一些标准化工作和计划性工作。这些工作是伴随着 Internet 工程任务组(Internet Engineering Task Force，IETF)所提出的第二层传输协议(Layer 2 Transport Protocol，L2TP)和 IP 安全协议(Internet Protocol Security，IPSec)而展开的。由于 L2TP 和 IPSec 是多数厂商共同研究和开发的，所以，它们并不像它们的前身那样有太多的互操作性问题。

作为一个第二层协议，L2TP 允许在一个基于 IP 的网络上提供多协议支持。这意味着，它不仅仅局限于某一特殊的协议，而是可以用来传输几种不同的协议。L2TP 规范没有内置的数据安全功能，需要在传输模型中用 IPSec 保证数据安全。L2TP 将在第 7 章“第二层隧道协议”中讨论。

因为隧道技术已经很成熟了，管理员已在实际使用它，所以隧道客户的应用变得更为广泛。除此之外，Windows NT 给管理员提供了基本的网络管理功能，如统计、审计以及报警，这些功能实现起来都很容易，也很容易进行监控。

到 1998 年，VPN 继续发展，有了集中化的用户管理、更好的网络管理以及增强的身份认证和加密机制。微软公司致力于 Windows NT 4.0 的隧道解决方案，升级了有关协议和与安全相关的过程，很多客户机都被升级为包含有隧道客户软件，以使配置更为流畅。

到 1999 年，高效的 VPN 又有了新的特性，如基于标准的认证模型，一个更为简单的接口用于服务器配置，以及其他客户机配置工具。有了新的身份认证模型，可用于客户访问的智能卡增加了将 VPN 集成到消费设备中的安全性和集成性。所以，有越来越多的远程办公者使用 VPN，同时越来越多的公司都使用 VPN 作为分支机构的链路。

Windows 2000 具有成熟的 VPN 选项，它可以提供安全的、可管理的隧道解决方案，这些功能比硬件解决方案或者是租用线路要廉价得多。微软公司承诺在 Windows 2000 中实现 VPN 技术，因为他们预测 VPN 将会在不远的将来成为公共网络中一个重要的因素。Windows 2000 不仅带有内置的对 IPSec、L2TP 和 PPTP 的支持，而且还传递一整套与安全相关的服务，这些服务的范围从对远程认证拨入用户服务(Remote Authentication Dial-In User Service，RADIUS)的完全支持到可扩展的认证协议(Extensible Authentication Protocol，EAP)。Windows 2000 的 VPN 服务将在第 3 章“Windows 2000 中的 VPN 特性”中进行更为详细的讨论。

1.2 虚拟专用网络是如何工作的

正如前面所讲到的，虚拟专用网络实质上就是在一个公共基础结构上的“专用隧道”。为了仿真一条专用网络链路，VPN 给数据封装一个报头，报头中提供有路由信息，这样可以使数据穿越公共网络(通常是指 Internet)，从源地址到达目的地址。为了仿真一条专用链路，VPN 加密所封装的数据，使它的发送具有保密性、真实性和绝对的完整性。如果没有密钥，那么在公共网络上所截取的包是不可读的。在一条链路上，数据是封装好的，而且是被加密的，那么这条链路就被称为 VPN 连接或隧道连接。

VPN 可以由不同的设备构成。现在，用一台 Windows 2000 服务器通过一条加密隧道连接到一台路由器，或者另一台 Windows 2000 设备，或者防火墙，或者其他使用标准协议并支持该加密机制的设备，就可以构成 VPN。