科海图书
25年·IT技术出版专家

VPN网络组建完全解决方案

王春海　张晓莉　田　浩　编著

VPN

网络组建案例实录

技术要点：

- 基本VPN服务器的组建
- 企事业单位VPN网络的组建
- 具有多出口的校园VPN网络的组建
- 使用智能卡组建VPN网络
- 某市政府VPN网络解决方案
- 证书服务
- 路由和远程访问服务
- ISA Server 2006代理服务器与防火墙
- 常见问题的解决方法
- 实验环境的搭建

集作者多年网络工程经验，提供实施VPN网络的完整解决方案

5个大型VPN网络案例，全部来自一线工程实践，极具实用价值

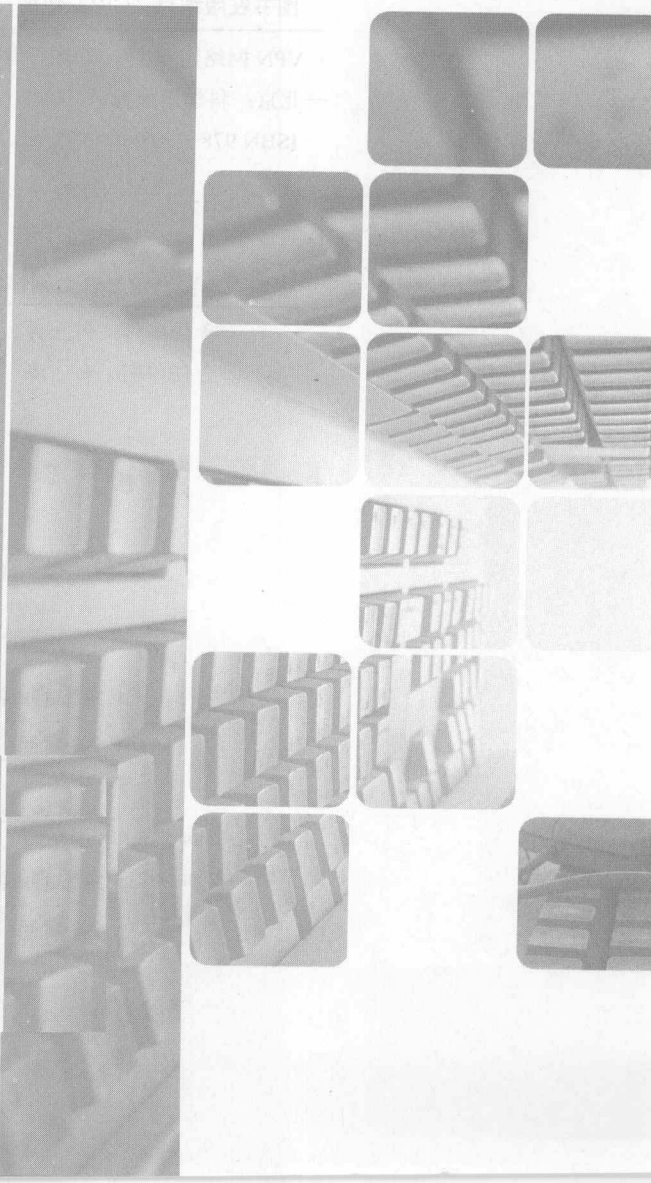
科学出版社

TP393.01/15
2008

VPN

网络组建案例实录

王春海　张晓莉　田 浩　编著



科学出版社

内 容 简 介

本书通过实际工程案例，介绍了使用 Windows Server 2003、ISA Server 2006 组建“软件”VPN 服务器与 VPN 网络的解决方案。

全书技术先进，所介绍的案例都是实际 VPN 网络的完整方案，并且都经过实际工作环境的检验，具有较高的实用价值。全书主要分三部分，第一部分（第 1 章~第 6 章）是实际 VPN 案例的真实记录，旨在让读者快速掌握 VPN 网络的组建，提高动手能力，增加 VPN 组网经验；第二部分（第 7 章~第 9 章）主要介绍 VPN 网络的理论知识，包括证书服务、Windows Server 2003 路由和远程访问服务及 ISA Server 2006 代理服务器和防火墙；第三部分（第 10 章及附录）主要介绍 VPN 网络中常见问题的解决方法及本书试验环境的搭建。

本书适合网络工程技术人员、网络技术爱好者、网络管理员和维护人员阅读，也很适合作为网络技术培训机构的教学用书。

图书在版编目（CIP）数据

VPN 网络组建案例实录/王春海，张晓莉，田浩编著.
—北京：科学出版社，2008
ISBN 978-7-03-021793-6

I. V… II. ①王… ②张… ③田… III. 虚拟网络—基本知识
IV. TP393.01

中国版本图书馆 CIP 数据核字（2008）第 060455 号

责任编辑：何立兵 / 责任校对：李玉茹
责任印刷：科 海 / 封面设计：王 嵩

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京市鑫山源印刷有限公司

科学出版社发行 各地新华书店经销

*

2008 年 7 月 第 一 版 开本：16 开
2008 年 7 月第一次印刷 印张：23.25
印数：000 1-4 000 字数：565 千字

定价：45.00 元

（如有印装质量问题，我社负责调换）

前言

全书通过5个实际工程案例，详尽地讲解了使用Windows Server 2003与ISA Server 2006组建安全VPN网络的具体方法，所提供的案例都是来自笔者亲自参与的实际工程，并经过实际工作环境的检验，具有较高的实用价值，读者完全可以将这些案例应用于自己的组网工程中。

与传统的硬件VPN组网方案相比，随着PC服务器硬件性能的不断提高与成本的不断下降，软件VPN服务器在成本、性能、可靠性、安全性、可扩展性等方面已体现出无可比拟的优势。因此软件VPN服务器成为了VPN网络解决方案的首选。本书只介绍软件VPN组网方案。

本书内容

本书共分3部分，各部分内容安排如下：

第一部分（第1章~第6章）：实际工程案例的真实记录，包括：组建基本的VPN服务器、企事业单位VPN网络的组建、具有多出口的校园VPN网络的组建、使用智能卡验证的VPN网络的组建、某市政府VPN网络解决方案。

第二部分（第7章~第9章）：介绍VPN网络的理论知识，包括：证书服务、Windows Server 2003路由和远程访问服务、ISA Server 2006代理服务器与防火墙。

第三部分（第10章、附录A、附录B）：介绍Windows Server 2003 VPN网络中常见问题的解决方法、VMware Workstation 6.0 的使用以及本书中试验环境的搭建。

本书案例

本书主要介绍了适合以下三种应用环境的VPN案例。

- 中小企业单VPN服务器解决方案：基本VPN服务器的组建，适合预算较小、维护与使用经费有限的中小企业或者中小学，使用一台Windows Server 2003服务器，通过Internet

为不超过1000个用户、最大并发300~500个用户的网络提供VPN接入服务。

- 大中专院校、中型企业VPN解决方案：单台或者两台服务器（一台低配置的证书服务器、一台VPN服务器），适合对安全性要求比较高、有一定经费的企业，通过Internet为出差用户、家庭办公用户、远程分公司或办事处，提供到公司总部指定网络的、安全的VPN接入服务。在访问时，使用“证书”进行身份验证与数据加密。
- 政府、机关与事业单位、大学VPN解决方案：多台服务器（一台证书服务器、一台Active Directory服务器、至少一台使用ISA Server标准版或企业版的VPN服务器），为单位内部、分公司、各下级部门提供到单位内网、政府内网（或其他网络，例如教育网）的访问。在访问时，使用硬件的“智能卡”进行身份验证与数据加密，智能卡具有唯一性，并且每隔一段时间需要进行认证。

本书约定

- 一般情况下，本书采用的VPN服务器，只要配置Pentium 4 2.0 GHz CPU、1GB内存、双网卡、10GB剩余硬盘空间的计算机、具有Internet环境，都可以满足其硬件要求。
- 本书所采用的操作系统是Windows Server 2003 R2（带SP2），ISA Server 2006简体中文标准版、客户端操作系统支持Windows 98及其以上的Windows操作系统。但当使用“智能卡”进行身份验证时，需要Windows XP及其以上的Windows操作系统。

读者对象

- 网络工程技术人员
- 网络技术爱好者
- 网络管理员和网络维护人员
- 网络技术培训机构

本书由王春海、张晓莉、田浩编著，樊玉芳、任文霞、马卫华、乔龙、龚威、白凤涛、陈永川、王冠雄、李海川、潘宁、李荣秀、李琳、王利峰、张新彦、盖伟东、彭静、赵艳也参与了编写工作。另外，感谢王金柱的大力支持与协助。

由于编者水平有限，并且本书涉及的系统与知识点很多，尽管笔者力求完善，但难免有不妥和错误之处，诚恳地期望广大读者和各位专家不吝指教。有关本书的意见反馈和更新消息以及在学习中遇到的问题，您都可以通过下列方式与作者联系。

作者个人网站：http://www.wangchunhai.cn
51cto专家博客：http://wangchunhai.blog.51cto.com
电子邮件：wangchunhai@heuet.edu.cn

作者
2008年5月

试读结束：需要全本请在线购买：www.ertongbook.com

目 录

试读结束：需要全本请在线购买： www.ertongbook.com

1 CHAPTER

VPN 网络概述

本章首先简要介绍虚拟专用网络（Virtual Private Network，VPN）的概念，然后介绍VPN网络的连接方式、连接属性以及商用VPN服务器的系统需求和网络架构。

技术要点：

（1）VPN网络的概念。
（2）VPN网络的拓扑结构。
（3）VPN网络的基础理论知识。
（4）软、硬件VPN网络各自的特点与优缺点。

学习目标：

（1）理解网络的“物理连接”、“逻辑连接”。
（2）掌握VPN网络的网络拓扑、组成与架构。

1.1 VPN网络的概念

使用通信介质将网络设备与计算机设备连接之后，网络在“物理”上已经连通，但必须让“计算机设备”通过“通信介质”与“网络设备”进行“逻辑连通”，才可能进行网络的应用。

所谓“逻辑连通”，是指在网络应用范围内的网络中，两个想要通信的“计算机设备”（假设这两个计算机设备之间没有网络防火墙或者防火墙未生效，而防火墙问题暂时不考虑）是可以互相ping通的。在TCP/IP网络中，两个设备（或多个设备）可以互相ping通，包括以下几种情况（物理网络已经连通）。

- 两个设备在同一个子网之中，即子网掩码相同，网络号相同，只有主机号不同。例

如，IP 地址分别为 192.168.1.1 和 192.168.1.23，子网掩码都是 255.255.255.0。

- 两个设备不在同一个子网之中，但这两个设备之间有路由器或网关，由路由器或网关转发数据，使这两个设备之间可以通信。

所以，只要交换机或路由器中的路由参数（路由表）正确，计算机设置正确（正确设置IP地址、子网掩码、网关地址），网络物理连通，就可以互相访问、ping通（不考虑防火墙屏蔽网络之间互访信息）。

网络物理连通、网络逻辑连通之后，网络设备就可以通信了。当然，如果在网络中处于“关键位置”的设备上设置了规则“阻止”某些设备通信，则网络也可能无法通信。图1-1中的“三层交换机”、“防火墙”和“路由器”都处于关键位置。

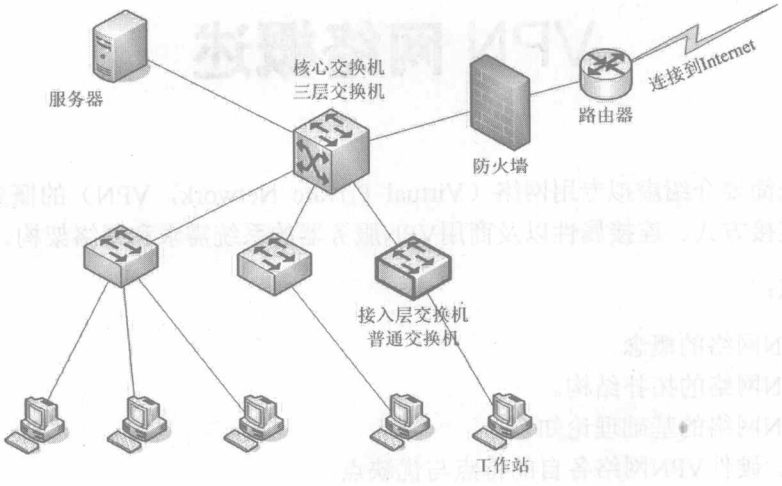


图 1-1　一个有防火墙、交换机、路由器、服务器和工作站的网络拓扑

根据网络“物理连通”的规模，网络可以分为局域网、城域网和广域网。许多的广域网与局域网互联后组成了Internet。

局域网，是指物理位置相近的、一个单位内的所有计算机组成的网络，或者个人的几台计算机组成的网络。局域网可以大到覆盖整个单位的所有楼层，小到只包含两台计算机。局域网主要使用交换机进行设备之间的互联，局域网如果要访问Internet，一般通过中心机房的“出口”连接到Internet。局域网是高速互联的，网络中的每台计算机都可以高速访问其他计算机或者服务器，通常情况下，局域网中的计算机可以用100Mbit/s的速度连接到交换机，局域网中的服务器通常以1Gbit/s甚至10Gbit/s的速度连接到中心交换机。

城域网，是指在局域网的基础上，将分布在同一个城区或一定范围内的一些局域网、单机连接在一起组成的网络。城域网的物理范围要大于局域网，它通常是多个单位或者一个单位的不同部门（物理上分散）通过无线或者租用网通或电信线路组建的网络。例如，某个城市的市政府、法院、医院、农业局等单位组建的政府内网就是城域网的典型案例。一般来说，城域网互联的接口速度要远远低于局域网的速度，一般为几Mbit/s到几十Mbit/s。

广域网，是指在局域网的基础上，将一个单位的不同分公司、分部门的局域网，通过租用网络服务提供商（ISP）的线路连接起来组成的网络。像公安、税务、银行、电力等部

门，一般都组成省、市、县、镇四级的网络结构，如图1-2所示。

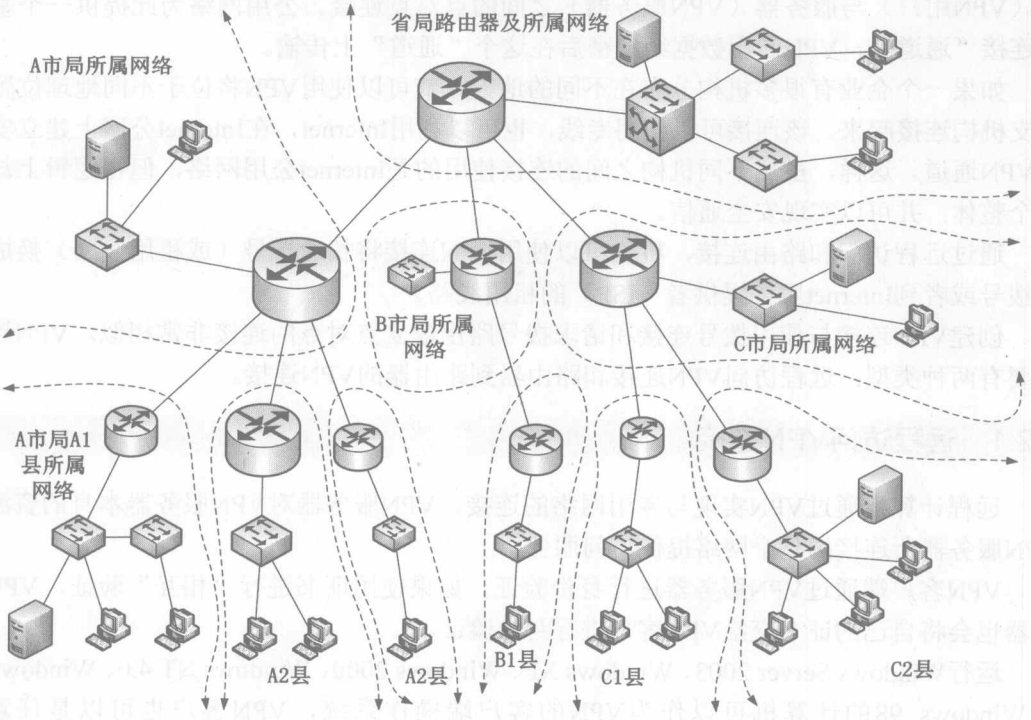


图 1-2　省、市、县、镇四级广域网结构拓扑图

在图1-2的网络拓扑中，省局到市局速度最快，市局到县局其次，县局到乡镇速度最慢。每个节点可以通过其上级节点与相邻节点互通。

在城域网与广域网中，都需要租用ISP的线路，通常情况下需要按月或者按年向ISP交纳专线租用费，而且费用比较高。

VPN网络是在“城域网”与“广域网”基础上，利用ISP提供的Internet接入线路，在公网（指Internet）上组建自己私有网络的一种技术与方法。通过Internet组建VPN网络，可以极大地节省组建成本与使用费用（与组建广域网相比）。

1.2　VPN的连接方式

通过VPN能以模拟点对点专用链路的方式，通过共享或公用网络在两台计算机之间交换数据。虚拟专用联网是创建和配置虚拟专用网的行为。

要模拟点对点链路，应压缩或包装数据，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其终点。为保密起见，如果要模拟专用链路，则应加密数据。一旦加密，若不知道密钥，即使从共享或者公用网络截取到数据包，也是很难解密的。封装和加密专用数据之外的连接是VPN连接。

在家里或者旅途中工作的用户可以使用VPN连接建立到企业内网的服务器的远程访问

连接，方法是使用公用网络提供的基础结构。从用户的角度来讲，VPN连接是一种在计算机（VPN用户）与服务器（VPN服务器）之间的点对点连接。公用网络为此提供一个基础的连接“通道”，VPN专用数据经加密后在这个“通道”上传输。

如果一个企业有很多机构分布在不同的地方，就可以使用VPN将位于不同地理位置的分支机构连接起来。该连接可以使用专线，也可以利用Internet，在Internet公网上建立安全的VPN通道。这样，虽然不同机构之间的连接使用的是Internet公用网络，但在逻辑上却是一个整体，并可以实现安全通信。

通过远程访问和路由连接，机构可以使用VPN连接将长途拨号（或租用线路）换成本地拨号或者到Internet服务提供者（ISP）的租用线路。

创建VPN连接与使用拨号连接和请求拨号路由建立点对点的连接非常相似。VPN连接主要有两种类型：远程访问VPN连接和路由器到路由器的VPN连接。

1.2.1 远程访问VPN连接

远程计算机通过VPN实现与专用网络的连接。VPN服务器对VPN服务器本身的资源及VPN服务器所连接的整个网络提供访问服务。

VPN客户端通过VPN服务器进行身份验证，如果使用证书进行“相互”验证，VPN服务器也会将自己的证书交给VPN客户进行身份验证。

运行Windows Server 2003、Windows XP、Windows 2000、Windows NT 4.0、Windows 95和Windows 98的计算机可以作为VPN的客户端操作系统，VPN客户也可以是任意非Microsoft点对点隧道协议（PPTP）的客户端，或是有IPSec的第二层隧道协议（L2TP）客户端。

1.2.2 路由器到路由器的VPN连接

路由器可以通过建立路由器到路由器的VPN连接将专用网络的两个部分连接起来。VPN服务器可以提供与网络的路由连接，以使此网络与VPN服务器连接。在路由器到路由器的VPN连接上，当两个路由器之间建立VPN连接时，路由器只负责数据包的发送和接收，但在发送之后和接收之前都要通过VPN进行数据包的处理。

1.3 基于Internet或Intranet的VPN连接

在需要安全的点对点连接来连接用户或网络时，可以使用VPN连接。典型的VPN连接可分为基于Internet的VPN连接和基于Intranet的VPN连接两种类型。

1.3.1 基于Internet的VPN连接

使用基于Internet的VPN连接，可以充分利用覆盖全球的Internet，费用较低。它一般也有以下两种方式。

- Internet 上的远程访问。远程访问客户通过 Internet 来初始化 VPN，连接到专用网

试读结束：需要全本请在线购买：www.ertongbook.com