中国科学出版集团
新世纪书局

国内资深网络工程师多年修订的经典图书
政府和企业实施VPN网络的完整解决方案

# VPN
# 网络组建案例实录
（第2版）

## 国内最权威的VPN组网技术指南

王春海 宋涛 编著

■ **多种组建技术**

集作者多年的网络工程经验，介绍使用Windows Server 2003、ISA Server 2006、Windows Server 2008、Forefront TMG、智能卡等多种技术组建VPN网络的方法

■ **完整解决方案**

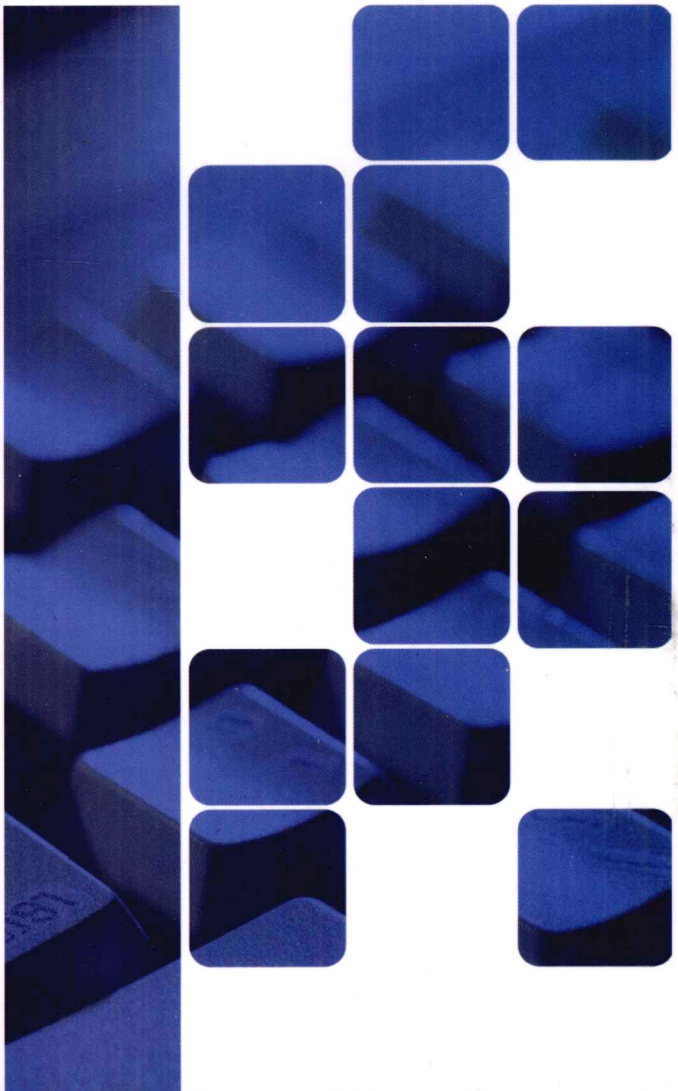
从基础VPN服务器到大型网络，提供9种组建案例，全部来自一线工程实践，极具参考价值

■ **提供实验环境的搭建**

讲解使用VMWare Workstation的Team功能组建书中实验环境的方法，让您边学边练，掌握实际工作中的配置方法

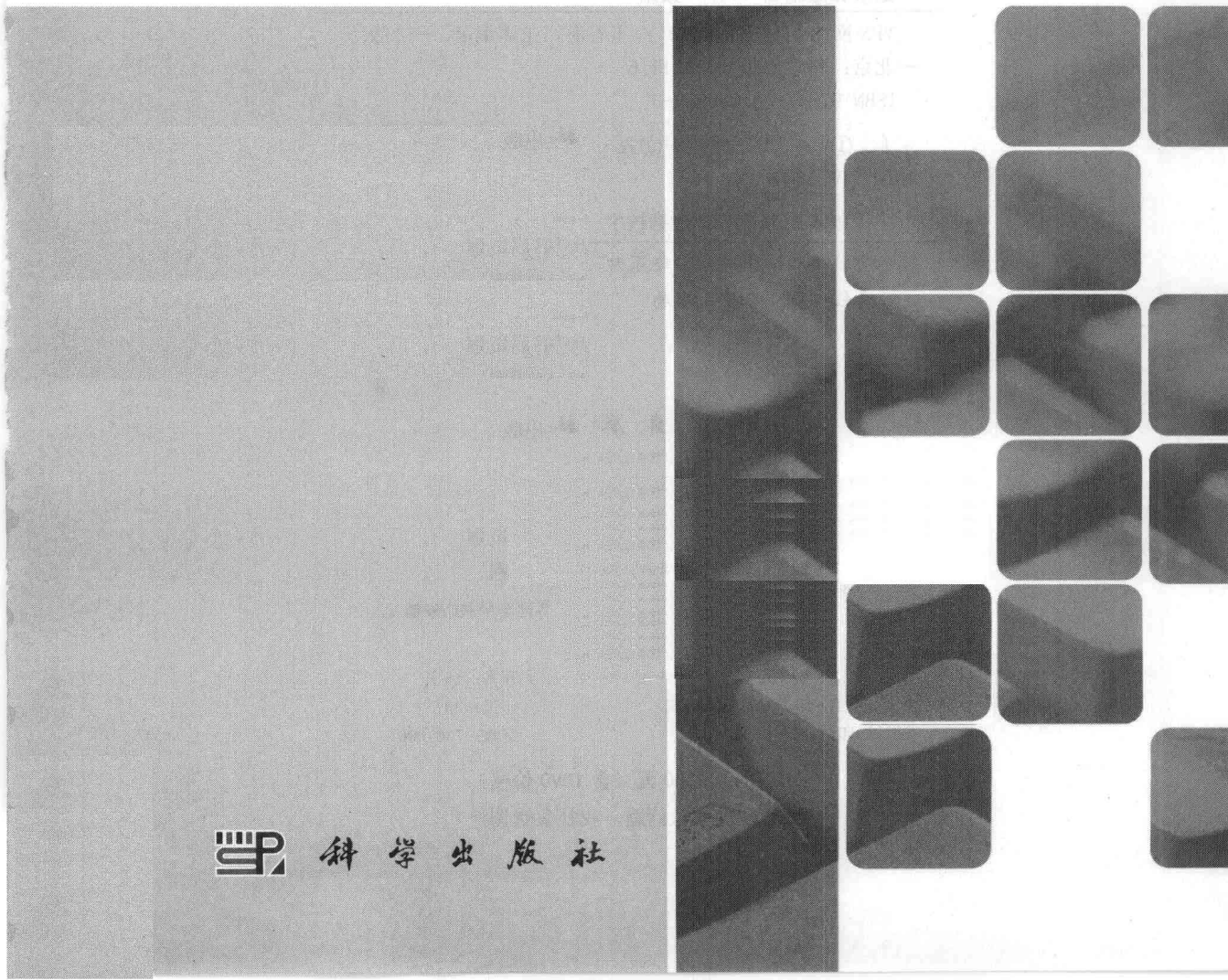
**1DVD多媒体教学课程**
**帮您直观了解VPN组建和管理的全过程**

科学出版社



# VPN
# 网络组建案例实录
（第2版）

王春海 宋涛 编著



科学出版社

## 内 容 简 介

本书主要介绍使用Windows Server 2003、Windows Server 2008、ISA Server 2006与Forefront TMG 2010组建“软件”VPN服务器与VPN网络的知识。本书介绍的VPN服务器具有低成本、高性能、高安全、可扩展的特点，而客户端采用Windows XP、Windows Server 2003、Windows Vista、Windows 7、Windows Server 2008内置的VPN客户端，对终端用户的要求低。

本书内容全面，配置步骤详细，具有完整的使用案例，并且本书的VPN解决方案已通过生产环境的检验，是可以实际使用的。全书主要分为三部分，第一部分（第1～6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，这一部分使用Windows Server 2003与ISA Server 2006；第二部分（第7～10章）介绍基于Windows Server 2008、Windows Server 2008 R2与Forefront TMG 2010组建VPN网络的内容；第三部分（第11章、第12章）介绍Windows Server 2003、Windows Server 2008与ISA Server 2006、Forefront TMG 2010使用中的注意事项、经典案例、典型故障及解决方法。

本书适合作为网络培训机构的专业培训教材，也适合读者自学使用。另外，本书对于正从事VPN网络组建的工作人员提高技术水平、增加组网经验有极大帮助。

**图书在版编目（CIP）数据**

VPN网络组建案例实录 / 王春海，宋涛编著. —2版.
—北京：科学出版社，2011.6
ISBN 978-7-03-030972-3

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

中国版本图书馆CIP数据核字（2011）第080859号

责任编辑：王海霞 赵东升 / 责任校对：刘雪连
责任印刷：新世纪书局 / 封面设计：彭琳君

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

中国科学出版集团新世纪书局策划
北京市艺辉印刷有限公司印刷
中国科学出版集团新世纪书局发行 各地新华书店经销
*

| | |
|---|---|
| 2011年7月 第 二 版 | 开本：16开 |
| 2011年7月第一次印刷 | 印张：30 |
| 印数：1—3 000 | 字数：730 000 |

**定价：59.80元（含1DVD价格）**

（如有印装质量问题，我社负责调换）

# 前 言

传统的 VPN 服务器大多采用“硬件”方式，但这种方式存在以下缺点。

- 使用的 VPN 服务器有容量限制，易造成用户原有投资的浪费。
- 硬件 VPN 组网简单、配置固定。
- 兼容性差。一般硬件 VPN 服务器采用自己的标准或者协议，没有采用工业标准。
- 维护困难。一般硬件 VPN 服务器只能由服务器生产公司的技术人员调试。
- 硬件 VPN 服务器不适合由网络管理员自己组建，也不适合网络管理员管理。

在当今时代组建的 VPN 服务器应该由管理员完全控制或者“一手”组建，这样管理员很容易上手，再加上现在 PC 服务器硬件性能的不断提高与成本的不断下降，无论从成本、性能、可靠性，还是安全性、可扩展性上分析，软件 VPN 服务器都有无可比拟的优势，而且软件 VPN 服务器也非常适合一些网络系统集成公司用于部署与学习。

## 本书内容

本书共有 12 章以及附录 A、附录 B、附录 C，具体内容安排如下。

第 1 章介绍网络基础、VPN 网络基础。

第 2 章介绍基本 VPN 服务器的组建，只需要一台服务器即可组建适合于企业生产环境使用的 VPN 服务器，并且可以稳定运行。

第 3 章是本书的重点章节之一，全面详细地介绍了用于机关、企业、事业单位的两种 VPN 服务器的网络拓扑及 VPN 服务器的安装、配置及客户端使用的完整步骤，还介绍了使用标准证书服务器为客户端颁发证书并且让客户端使用 L2TP 方式拨叫 VPN 服务器的方式。截至本书出版之时，本书是第一本介绍客户端使用 L2TP 方式登录 VPN 服务器的图书。

第 4 章是对第 3 章内容的改进与扩展，以大学组建校园 VPN 服务器为例，介绍了具有多出口网络的 VPN 服务器的组建与系统策略的配置方法。

第 5 章是本书的重点章节，介绍了联合使用企业证书、Active Directory、ISA Server 组建用“智能卡”进行身份验证的 VPN 网络的详细步骤。有关使用智能卡验证 VPN 服务器的组建方法，是许多专业公司的“不传之秘”，本书第一次“公开”了这些内容。

第 6 章介绍了一个真实的案例——某市市政府网络 VPN 改造方案，使“内网用户”、“政府大院外各乡镇、局”能使用 VPN 的方式安全访问省、市、国务院“政务内网”的相关内容，包括交换机的重新规划、防火墙的设置、使用智能卡进行身份验证、使用脚本自动安装驱动程序、创建 VPN 连接、自动导入证书文件，以及客户在使用过程中碰到的各类问题及解决的办法。

第 7 章介绍基于 Windows Server 2008、Windows Server 2008 R2 的 VPN 网络的组建。

第 8 章介绍使用 Forefront TMG 2010 组建并配置 VPN 网络的内容。

第 9 章介绍使用 Windows Server 2008、Windows Server 2008 R2 的 Active Directory、证书服务、Forefront TMG 2010 组建基于智能卡身份验证的 VPN 网络的内容。

第 10 章介绍使用 Forefront TMG 2010 企业版组建 VPN 阵列的内容。

第 11 章介绍 Windows Server 2003、Windows Server 2008 的一些“关键”操作，如修改 SID、添加授权数量、修改关机菜单等。

第 12 章介绍 ISA Server 2006、Forefront TMG 2010 的经典应用，以及一些疑难故障的排除、分析与解决方法。

附录 A 介绍 VMware Workstation 的基础知识与基本使用，包括 VMware Workstation 的安装、配置，虚拟机模板的创建方法，VMware Tools 的安装与使用，以及 Team 功能的使用。

附录 B 介绍使用 VMware Workstation 的 Team 功能组建本书第 2～10 章的实验环境的方法。

附录 C 总结了 VPN 客户端拨叫 VPN 服务器时出现的故障代码及其说明。

## 本书的学习原则

- 照做实验。
- 自己“修改”关键数据，再自己做实验。
- 对实验环境进行改造，用于实际工作环境。
- 使用注意事项、备份策略、做记录等。

## 本书的读者对象

- 计算机网络专业学生。
- 系统集成公司。
- 单位信息中心技术主管。
- 网络爱好者。

## 本书的适用范围

- 基于 Windows Server 2003、Windows Server 2008、Windows Server 2008 R2 以及 ISA Server 2006、TMG 2010 组建的“偏软件”的 VPN 网络解决方案。
- 需要组建的 VPN 网络规模在 100～1000 连接个的单台 VPN 服务器的 VPN 网络解决方案；以及 1000～15 000 个甚至 15 000×1000 个并发的 VPN 连接的特大型 VPN 网络。

注：一般情况下，单台 Windows Server 2003+ISA Server 2006（或 Windows Server 2008+ForeFront TMG 2010）可以实现并发 500～1000 个连接；而在 ForeFront TMG 2010 企业版中，可以组建更多。

- 单位需要有固定的、可用公网 IP 地址，至少 VPN 服务器一端需要有固定的公网地址（可以是双 WAN 口路由器、路由器转发 VPN 服务端口）。
- 需要高可靠性、高安全性、高稳定性的软件/硬件进行身份验证的 VPN 网络。
- 需要自由定义 VPN 客户端各种行为和各种能力的要求苛刻的用户。

## 本书读者需要的基础知识

- 必须熟悉 TCP/IP 协议、熟悉 TCP/IP 地址、子网掩码、网关、DNS，会划分子网，熟悉路由、交换、NAT 的区别。
- 具有一定的防火墙或路由器的调试基础，至少自己组建过网络。
- 具有一定的自学能力。

## 本书案例

本书主要介绍了适合以下 3 种应用环境的 VPN 案例。

- 中小企业单台 VPN 服务器的解决方案。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校。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 网络的解决方案。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 网络的解决方案。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 Forefront TMG 或 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，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。使用本方案，可以组建 100 000 万路并发连接的 VPN 网络。

本书提供的方案，均来源于作者近几年来给一些学校、政府、机关与事业单位做的 VPN 网络方案，它们都经受住了实际使用环境的检验。

## 本书约定

- 一般情况下，只要具有 Pentium 4 2.0 GHz CPU、1GB 内存、10GB 可用硬盘空间的计算机，具有双网卡和 Internet 环境，就可以满足本书第 2～6 章介绍的 VPN 服务器的需求；具有 Core 2 6300 CPU、4GB 内存、双网卡并具有 Internet 环境，可以满足本书第 7～10 章的 VPN 服务器的需求。

- 本书第 2～6 章所采用的服务器端操作系统是 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；本书第 7～10 章采用的是 Windows Server 2008 R2 与 Forefront TMG 2010。只是在采用“智能卡”进行身份验证时，需要 Windows XP 及其以上的 Windows 操作系统。

## 作者简介

王春海，在网络应用、网络组建、网络安全、虚拟机技术等多个方面都有很深的研究，精通 Microsoft 公司的 ISA Server、Forefront TMG、Windows Server 2003、Windows Server 2008、SharePoint、Exchange 等多个方面的产品，是 2009～2011 年度 MVP（微软最有价值专家），是 Microsoft Forefront 方面的 MVP，为政府及多家企事业单位组建并维护包括 VPN 网络在内的多种网络，在长期的工作中积累了大量的经验并解决了各种各样的网络问题。

编著者

2011 年 5 月

# 目 录