普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

防火墙、入侵检测与VPN

Fanghuoqiang Ruqin Jiance Yu VPN

马春光　郭方方　编著

北京邮电大学出版社
www.buptpress.com

普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

防火墙、入侵检测与 VPN

马春光　郭方方　编著

北京邮电大学出版社
·北京·

内 容 简 介

本书以安全防御为中心，全面系统地讲述了网络安全的3种主要技术——防火墙、入侵检测和VPN，以及围绕这3项技术构建安全防御体系的方法。本书分为3部分，共15章，内容包括防火墙基础知识、防火墙的关键技术、主流防火墙的部署与实现、防火墙厂商及产品介绍、防火墙技术的发展趋势、入侵检测技术概述、主流入侵检测产品介绍、入侵检测技术的发展趋势、VPN基础知识、VPN的隧道技术、VPN的加解密技术、VPN的密钥管理技术、VPN的身份认证技术、VPN厂商及产品介绍、VPN技术的发展趋势等。

本书语言表达简洁流畅，内容安排由浅入深，在前后内容上相互呼应，充分阐述了防火墙、入侵检测与VPN这3种防御手段在技术上的互补性。本书内容系统、全面，特别注重知识的实用性，将理论和实际相结合。在对原理进行深入浅出的描述的基础上，对如何部署、配置等实际操作进行了详细说明，对复杂的密码算法通过实例加以形象化说明。通过介绍不同厂商的产品及其技术指标，可以加深读者对每一种技术的理解。在每一部分的最后分别介绍了防火墙、入侵检测与VPN技术的发展趋势，力图对有志于网络安全的研究者有所启示。

本书可作为高等院校信息安全相关专业的本科生、研究生的教材或参考资料，也可供从事计算机科学与技术、网络工程、信息与通信工程等与信息安全有关的科研人员、工程技术人员和技术管理人员参考。

图书在版编目(CIP)数据

防火墙、入侵检测与VPN/马春光，郭方方编著. —北京：北京邮电大学出版社，2008

ISBN 978-7-5635-1662-9

Ⅰ.防… Ⅱ.①马…②郭… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2008)第124811号

书　　名：防火墙、入侵检测与VPN
作　　者：马春光　郭方方
责任编辑：艾莉莎
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京忠信诚胶印厂
开　　本：787 mm×960 mm　1/16
印　　张：17
字　　数：366千字
印　　数：1—5 000册
版　　次：2008年8月第1版　2008年8月第1次印刷

ISBN 978-7-5635-1662-9　　定　价：29.00元

内 容 简 介

本书以安全防御为中心，全面系统地讲述了网络安全的3种主要技术——防火墙、入侵检测和VPN，以及围绕这3项技术构建安全防御体系的方法。本书分为3部分，共15章，内容包括防火墙基础知识、防火墙的关键技术、主流防火墙的部署与实现、防火墙厂商及产品介绍、防火墙技术的发展趋势、入侵检测技术概述、主流入侵检测产品介绍、入侵检测技术的发展趋势、VPN基础知识、VPN的隧道技术、VPN的加解密技术、VPN的密钥管理技术、VPN的身份认证技术、VPN厂商及产品介绍、VPN技术的发展趋势等。

本书语言表达简洁流畅，内容安排由浅入深，在前后内容上相互呼应，充分阐述了防火墙、入侵检测与VPN这3种防御手段在技术上的互补性。本书内容系统、全面，特别注重知识的实用性，将理论和实际相结合。在对原理进行深入浅出的描述的基础上，对如何部署、配置等实际操作进行了详细说明，对复杂的密码算法通过实例加以形象化说明。通过介绍不同厂商的产品及其技术指标，可以加深读者对每一种技术的理解。在每一部分的最后分别介绍了防火墙、入侵检测与VPN技术的发展趋势，力图对有志于网络安全的研究者有所启示。

本书可作为高等院校信息安全相关专业的本科生、研究生的教材或参考资料，也可供从事计算机科学与技术、网络工程、信息与通信工程等与信息安全有关的科研人员、工程技术人员和技术管理人员参考。

图书在版编目(CIP)数据

防火墙、入侵检测与VPN/马春光，郭方方编著. —北京：北京邮电大学出版社，2008

ISBN 978-7-5635-1662-9

Ⅰ.防… Ⅱ.①马…②郭… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2008)第124811号

书　　名：防火墙、入侵检测与VPN
作　　者：马春光　郭方方
责任编辑：艾莉莎
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京忠信诚胶印厂
开　　本：787 mm×960 mm　1/16
印　　张：17
字　　数：366千字
印　　数：1—5 000册
版　　次：2008年8月第1版　2008年8月第1次印刷

ISBN 978-7-5635-1662-9　　定　价：29.00元

信息安全专业系列教材（第2版）

编 委 会

第 2 版总序

发展 21 世纪中国信息安全要靠教育，而搞好信息安全教育就需要好的教材。2004 年，灵创团队北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材，该套教材被教育部列入了“普通高等教育‘十五’国家级规划教材”。至今，三年多的时间过去了，这套教材在信息安全专业的教学中发挥了重要的作用，起到了较好的教学效果，受到教师和学生的好评。

在这三年中，我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设和校企就业（创业）平台建设等在内的信息安全本科专业的全面建设。2005 年，作为组长单位我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题；召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”。我们完成的国内第一次制定的信息安全专业规范，从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系；由通识教育内容、专业教育内容和综合教育内容三大部分，构建课程参考体系；采用顶层设计的方法构建了带有实践性环节的教学体系。我们在国内第一次较全面地提出信息安全学科专业教学改革与创新的研究以及发展思路和政策建议；这些成果已提交教育部相关教学指导委员会，对于引导高等学校信息安全学科专业教学改革与建设，指导信息安全学科专业评估，促进信息安全学科专业教学规范建设与管理，提高专业教育质量和水平起到了重要的作用。多所举办信息安全专业的高校都参照该课题成果调整了自己的教学计划、课程体系和实验方案。

我们积极搭建信息安全专业校际交流平台，组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”和“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地 40 亩的全国信息安全专业本科生实习实训基地，接受了来自全国近 30 所高校的本科生进入该基地参加丰富多彩的实训。

我们努力建设精品课程，主办了“全国高校信息安全专业精品课程建设经验交流会议”，来自全国各地高校的专家齐聚北京邮电大学，介绍了精品课程建设的经验。我们组织建设了全国第一批信息安全实验室，并且编写出版了实验教材《信息安全实验指导》，我们的《现代密码学》课程已经被评为北京市精品课程，并在 2007 年度被评为“国家精品课程”。

经过灵创团队全体人员的共同努力，北京邮电大学信息安全本科专业被教育部评为

第二类优势特色专业。

三年多的时间过去了，无论信息安全的教育和产业都取得了丰硕的成果，随着信息安全向更高层次的发展，其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要，积极探索培养创新型高素质人才，我们按照制定的学科发展战略和专业规范的精神，结合近几年的教学实践，我们对这套信息安全专业本科系列教材进行了全面修订，并及时成立了灵创团队北京邮电大学数字内容研究中心。这次修订不仅对原来的系列教材在第1版的基础上进行修改和完善，还补充了信息安全最新的研究成果，使教材的内容更加翔实和新颖。同时，在原有的教材上又增加了一些新的课程教材，在新修订的系列教材中，目前有《信息安全概论》(第2版)、《现代密码学及其应用》、《网络安全》(第2版)、《信息安全管理》、《计算机病毒原理及防治》(第2版)、《数字版权管理》、《计算机系统安全》，《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与VPN》、《对称密码学及其应用》、《信息安全导论》、《数字图像取证技术》等13本教材，今后随着信息安全专业教学的需要，还将不断地有新的教材补充到这个系列中来，使之更加完善和系统。目前，计划列入的相关教材还有：《入侵检测》(第2版)、《信息内容安全》、《信息安全工程》、《软件安全》及《信息安全标准与法律法规》等。

我们组织了强大的师资队伍，广泛吸收了有着丰富教学科研经验并多次讲授该系列教材的教师充实到这次修订工作中。作者队伍中不但包括北京邮电大学的教师，还包括哈尔滨工程大学、北京交通大学等重点院校的教师。经过反复研讨，本着理论与实际相结合的原则，对原来的系列教材进行了较大的修改和扩充，我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向专业的不同需求。

这次修订我们对内容进行了精心的组织和安排，希望能促进信息安全课程的建设，涌现出更多的信息安全精品课程。虽然我们在这次修订中投入了很大精力，但是由于水平有限，时间仓促，且信息安全专业的发展速度非常快，书中的不足之处和错误在所难免，我们衷心期望使用和关心该系列教材的师生，继续对新的系列教材提出宝贵的意见和建议。

本套系列教材也是国家重点基础研究发展计划(973)(课题编号：2007CB310704和2007CB311203)资助的成果，并被教育部增补为“普通高等教育‘十一五’国家级规划教材”的选题。

在本系列教材的修订过程中，得到了北京邮电大学出版社的大力支持，同时也得到了灵创团队的骨干机构(北京邮电大学信息安全中心和北京邮电大学数字内容研究中心)三百余位成员的支持与配合，在此一并表示感谢。

教授、博导、长江学者特聘教授

杨义先

2007年7月

前　言

当前，信息化已深入到了社会政治、经济、文化、生产、生活的各个领域。由于Internet开放性的设计理念，加之设计之初对安全问题考虑甚少，使得其安全问题十分严重。因此，如何在安全性不尽人意的 Internet 上构建一个相对安全的环境十分重要。本教材以安全防御为中心，全面系统地讲述了信息系统安全防御的 3 项技术——防火墙、入侵检测和 VPN，以及围绕这 3 项技术构建安全防御体系的方法。

本教材包括 3 部分内容，分别介绍防火墙、入侵检测、VPN。在各部分的内容组织上，均按“基础知识、关键技术、系统构建、主流产品、发展趋势”的递进顺序展开，既注重技术细节，又强调系统集成，既讲述当前应用，也兼顾技术发展，力求使不同读者群各得所需。另外，本教材的 3 部分内容既互相联系又自成体系，教师可以根据需要择其部分或全部进行讲授，读者也可以根据需要有选择地进行自学或参考。

第 1～5 章为防火墙部分。防火墙是本地计算机或内部网络与外部网络之间设置的一道屏障，用于阻挡来自外部网络的威胁和入侵。第 1 章是防火墙的基础知识，包括防火墙的定义、分类、规则、功能和特点等；第 2 章是防火墙的关键技术，包括 TCP/IP 协议简介、包过滤技术、状态检测技术、代理技术；第 3 章是主流防火墙的部署与实现，第 4 章是防火墙厂商及产品介绍，这两章详细地讲述了防火墙系统的构建和防火墙设备的选型，以便与实际应用接轨；第 5 章是防火墙技术的发展趋势，提出了进一步研究和学习的若干方向。

第 6～8 章为入侵检测部分。网络探测与攻击技术日新月异，这使得以单纯性阻挡为目的的防火墙捉襟见肘。入侵检测技术可以通过对系统负载的深入分析，发现和处理更加隐蔽的网络探测与攻击行为，为系统提供更强大、更可靠的主动安全策略和解决方案，弥补了防火墙的不足。第 6 章是入侵检测技术概述，从介绍计算机系统面临的威胁入手，依次讲述了入侵检测的概念、分类、作用、过程和特点等基础知识；第 7 章是主流入侵检测产品介绍，讲述了入侵检测系统的性能指标和主流入侵检测产品；第 8 章是入侵检测技术的发展趋势。

第 9～15 章为 VPN 部分。防火墙和入侵检测通过“御敌于门外”构建了一个相对安

全的内部网络，VPN 技术则为在地理位置上分散的多个内部网络间实现安全通信提供了保障。通过特殊的加密通信协议，VPN 在位于 Internet 不同位置的两个或多个企业内部网络之间建立专有的通信线路，实现了在公开网络中虚拟出企业内部专线。第 9 章是 VPN 基础知识，包括 VPN 的定义、VPN 的原理及配置、VPN 的类型、VPN 的特点以及 VPN 的安全机制等内容；第 10 章是 VPN 的隧道技术，包括 VPN 使用的隧道协议、MPLS VPN、IPSec VPN、SSL VPN 等内容；第 11 章是 VPN 的加、解密技术，包括 AES 算法、Diffie-Hellman 算法、SA 机制等内容；第 12 章是 VPN 的密钥管理技术，包括 ISAKMP 协议、IKE 协议和 SKIP 协议；第 13 章是 VPN 的身份认证技术，包括安全口令、PPP 认证协议、使用认证机制的协议、数字签名技术等内容；第 14 章是 VPN 厂商及产品介绍，包括 VPN 产品的功能、VPN 产品的技术指标和知名 VPN 厂商及产品等；第 15 章总结了 VPN 在市场、技术等方面的发展趋势。

哈尔滨工程大学计算机科学与技术学院的马春光副教授和郭方方副教授负责本书的编写工作，硕士研究生于洪君、林相君、徐海利、陆子海等为本书的编写进行了资料收集和整理工作。感谢北京邮电大学罗群副教授、北京邮电大学出版社周明总编对编写本书所给予的帮助和支持，特别感谢我的导师杨义先教授多年来的培养、鼓励和支持。

由于时间仓促以及知识水平所限，书中难免存在不妥和错误之处，真诚希望读者不吝指教，以期再版修订。

本书得到了国家自然科学基金项目(90718003)、国家 863 计划课题(2007AA01Z401)、国家博士后科学基金(20070410896)、黑龙江省博士后基金(LBH-Z06027)、哈尔滨工程大学基础研究基金(HEUFT05067)和黑龙江省新世纪高等教育教学改革工程项目(具有计算机学科特色的信息安全课程体系改革与实践)的支持。

作　者

2008 年 5 月于哈尔滨

目　录

防火墙篇

第1章　防火墙基础知识

第 2 章 防火墙的关键技术

入侵检测篇

VPN 篇