全国信息化计算机应用技术资格认证指定教材
（考试科目编码 2101）

防火墙技术

标准教程

全国信息化计算机应用技术资格认证管理中心　组编
主 编　曾勋炜　付爱英　盛鸿宇

- 防火墙基础
- TCP/IP
- 网络设计
- 防火墙体系结构
- 防火墙高级功能
- 网络攻击类型和方法
- 常见防火墙的选购和应用

多媒体教学光盘

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

全国信息化计算机应用技术资格认证指定教材

防火墙技术标准教程

全国信息化计算机应用技术资格认证管理中心 组编

主 编 曾勋炜 付爱英 盛鸿宇

副主编 徐知海 鄢志辉 张坚琳 石 力

北京理工大学出版社

BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 提 要

本书是全国信息化计算机应用技术资格认证（CCAT）项目的指定教材，属于工程师级认证体系。CCAT资格认证项目设立的目的除了培养学生掌握相应专业的理论知识，注重学员动手能力、创新能力的训练外，还注重培养和提高学员的企业管理能力，为社会和企业培养既懂技术又懂管理的复合型人才，以改变人才培养中存在的重理论轻实践、重文凭轻能力的缺陷。

本书共分7章。第1章介绍了防火墙的基本概念和功能；第2章介绍了支撑防火墙技术的网络基础知识；第3章介绍了与防火墙实施相关的网络设计技术；第4章根据防火墙的发展过程介绍防火墙自身的几种体系结构；第5章介绍了防火墙的多种高级功能及其相关知识；第6章介绍了常见的网络攻击类型和方法、几种常用的防范网络攻击的类型和方法以及由于防火墙自身漏洞问题而常面临的几种攻击；第7章介绍了目前流行的几家防火墙产品，如Check Point、Ciso PIX、Linux IP Table、Microsoft ISA Server、NetScreen和SonicWALL，详细介绍了这些产品的性能、功能、安装和配置以及产品的管理维护，为防火墙产品的选购和应用提供了参考依据。随书配有多媒体教学光盘，方便读者实际操作，让读者在最短时间内掌握最多的知识和技能。

本书是CCAT项目的指定教材，也可作为高等院校、高等职业院校信息与计算机相关专业数据库技术的教材，亦可作为数据库管理员学习参考。

图书在版编目（CIP）数据

防火墙技术标准教程／曾勋炜，付爱英，盛鸿宇主编；全国信息化计算机应用技术资格认证管理中心组编．—北京：北京理工大学出版社，2007.1（2007.7重印）

全国信息化计算机应用技术资格认证指定教材

ISBN 978-7-5640-0994-6

Ⅰ.防…　Ⅱ.①曾…②付…③盛…④全…　Ⅲ.计算机网络-防火墙-资格考核-教材　Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2006）第165111号

出版发行／北京理工大学出版社
社　　址／北京市海淀区中关村南大街5号
邮　　编／100081
电　　话／（010）68914775（办公室）68944990（批销中心）68911084（读者服务部）
网　　址／http://www.bitpress.com.cn
经　　销／全国各地新华书店
印　　刷／北京圣瑞伦印刷厂
开　　本／787毫米×1092毫米　1/16
印　　张／22.25
字　　数／499千字
版　　次／2007年1月第1版　2007年7月第2次印刷
印　　数／5001～8000册　　责任校对／张　宏
定　　价／35.00元　　责任印制／母长新

全国信息化计算机应用技术资格认证
专家委员会名单

编 委 会

主　任		
李国杰	中国工程院 中国科学院计算技术研究所	院士 所长
副主任		
李增泽	人事部中国高级公务员培训中心远程培训处 人事部中国国家人事人才培训网	处长 总裁
袁开榜	全国高等学校计算机教育研究会 世界教科文卫组织	理事长/教授 专家

执行委员会

杜建京	人事部中国高级公务员培训中心远程培训处	副处长
李大友	全国高等学校计算机教育研究会 北京工业大学	副理事长 课程与教材建设委员会主任教授
陈蜀宇	全国高等学校计算机教育研究会网络分会 重庆大学软件学院	常务副理事长 博导　院长/教授
丁石藤	复旦大学网络教育学院	副院长/教授
胡剑锋	江西蓝天学院	博士/院长助理
（以下按汉语拼音排序）		
丁　新	全国高等学校计算机教育研究会计算机网络教育分会 华南师范大学网络教育学院	副理事长 院长
丁晓明	西南大学计算机学院	博士　院长助理/教授
郝成义	中国人民大学网络教育学院	副院长/副教授
焦金生	《计算机教育》杂志社	主编
焦宝文	清华大学信息科学技术学院	教授
姜令嘉	山东大学网络教育学院	副院长/副教授

林亚平	湖南大学计算机学院	副院长/博导
卢先和	清华大学出版社计算机与信息分社	博士　社长
孟昭鹏	天津大学网络教育学院	硕士　副院长
冉蜀阳	四川大学网络教育学院	博士　常务副院长
盛鸿宇	教育部高职高专电子信息类教学指导委员会 北京联合大学	秘书
王晓军	北京邮电大学网络学院	副院长
徐乃庄	上海交通大学网络教育学院	副院长/教授
印　鉴	中山大学计算机科学系	副主任/副教授
张长利	东北农业大学	副校长
	东北农业大学网络教育学院	院长

秘　书

李顺福	全国高等学校计算机教育研究会网络分会	秘书长/高级工程师
杨志坚	北京理工大学出版社	社长
张文峰	北京理工大学出版社	社长助理

委　员

办公自动化应用模块委员名单

丁建民	全美测评软件系统有限公司	副总裁
丁晓明	西南大学计算机学院	博士　院长助理/教授
刘兴东	深圳职业技术学院	副院长/高级工程师
卢冠忠	华东理工大学	博导　副校长/党委副书记
马希荣	天津师范大学计算机与信息工程学院	博士　院长/教授
司银涛	北京交通大学远程继续教育学院	副院长/高级工程师
冉蜀阳	四川大学网络教育学院	博士　副院长
宋真君	辽宁交通高等专科学校计算机系	硕士　系主任
苏开荣	重庆邮电大学应用技术学院	常务副院长/副教授
吴子文	福建师范大学数学与计算机科学学院	院长/教授
谢咏才	中国农业大学网络学院	常务副院长/教授
闫洪亮	河南平顶山工学院计算机科学与工程系	副主任

张长利	东北农业大学	副校长
	东北农业大学网络教育学院	院长
何履胜	重庆电子职业技术学院	副院长/副教授
	重庆高技能人才开发协会	副理事长

多媒体与平面设计模块委员名单

丁振国	西安电子科技大学计算机应用学院	博士　副院长/教授
常建平	河南公安高等专科学校警察管理系	系主任
迟呈英	鞍山科技大学计算机学院	副院长
丁　新	华南师范大学网络教育学院	院长
符云清	重庆大学网络学院	博士　副院长/教授
龚晓阳	东华大学网络教育学院	副院长/副教授
刘希玉	山东师范大学信息管理学院	博士　院长/教授
刘正岐	陇东学院计算机科学系	主任/教授
马希荣	天津师范大学计算机与信息工程学院	博士　院长/教授
孟昭鹏	天津大学网络教育学院	副院长
苏开荣	重庆邮电大学应用技术学院	常务副院长/副教授
王世伟	中国医科大学网络中心	主任/教授
杨　涛	重庆天极信息发展有限公司	副总裁
印　鉴	中山大学计算机科学系	副主任/副教授
朱巧明	苏州大学计算机科学与技术学院	院长/教授
陈传文	南昌大学艺术设计学院	副院长
梅小清	南昌大学艺术设计学院	副主任

网络设计模块委员名单

鲍有文	北京联合大学信息学院	硕士　副院长/教授
何东建	西北农业科技大学信息工程学院	院长/教授
高占国	重庆通信学院地管部	主任/副教授
郝成义	中国人民大学网络教育学院	副院长/副教授
林亚平	湖南大学计算机学院	博导　副院长
刘革平	西南大学网络教育学院	博士　副院长/副教授
欧朝全	全国高等学校计算机教育研究会网络分会	理事
石　岗	武汉大学网络中心	博士　主任/教授

石　忠	渤海大学信息学院	硕士　院长
王世伦	四川师范大学计算机学院	副院长/副教授
王晓军	北京邮电大学网络学院	副院长
徐贯东	温州师范学院计算机科学与工程学院	博士　院长/副教授
徐乃庄	上海交通大学网络教育学院	副院长/教授
许晓艺	华南师范大学网络教育学院	副院长/高级工程师
杨　涛	重庆天极信息发展有限公司	副总裁
曾　鹏	南京邮电学院计算机系	博士　副主任
崔雅娟	北京语言大学	副教授

网络安全模块委员名单

陈庆章	浙江工业大学信息学院	党委书记/教授
丁振国	西安电子科技大学网络教育学院	博士　副院长/教授
龚晓阳	东华大学网络教育学院	副院长/副教授
何东健	西北农业科技大学信息工程学院	院长/教授
林筑英	贵州师范大学数学与计算机学院	院长/教授
刘革平	西南大学网络教育学院	博士　副院长/副教授
刘建臣	河北建筑工程学院	主任/教授
姜令嘉	山东大学网络教育学院	副院长/副教授
冉蜀阳	四川大学网络教育学院	博士　常务副院长
丘　威	广东梅州市嘉应学院计算机科学与技术系	硕士　主任
司银涛	北京交通大学远程继续教育学院	副院长/高级工程师
苏小兵	华东师范大学网络教育学院	院长助理
万常选	江西财经大学信息管理学院	博士　副院长/教授
王永书	重庆网络安全学会	常务副理事长
王振友	山东理工大学计算机学院	院长/教授
徐乃庄	上海交通大学网络教育学院	副院长/教授
张长利	东北农业大学 东北农业大学网络教育学院	副校长 院长
郑　宁	杭州电子工业学院计算机分院	院长/教授
朱巧明	苏州大学计算机科学与技术学院	院长/教授
姚　华	江西蓝天学院	副教授

总　序

努力造就数以亿计的高素质劳动者以及大批的创新人才，大力提升国家核心竞争力和综合国力，走人才强国之路，是实现中华民族伟大复兴的一项重大而紧迫的任务。

国务院《关于大力推进职业教育改革与发展的决定》和国务院办公厅转发教育部等部门《关于进一步深化普通高校毕业生就业制度改革的有关问题意见的通知》以及劳动和社会保障部、教育部、人事部《关于进一步推动职业学校实施职业资格证书制度的意见》等文件指出：应“在全社会实行学历证书、职业资格证书并重的制度，提高劳动者素质，推动就业准入制度”，“鼓励普通高校毕业生参加职业资格考核鉴定，进一步拓宽毕业生的就业渠道”。中央决定对专业技术人才的评价要由社会、行业直至企业认可，在专业技术人员中实施职业资格认证制度和执业资格制度，打破技术职务终身制，不拘一格选用人才、任用人才，走专业技术人才职业资格与国际接轨的道路，努力实现国际互认。

“全国信息化计算机应用技术资格认证”（CCAT）项目重点是培养学员的学习能力、实践能力，着力提高学员的创新能力和实际动手能力，提升学员的综合素质和就业、创业能力，特别是注重管理能力的培养和提升，改变目前教育体系普遍存在的重理论轻实践、重文凭轻能力、重技术轻管理的传统的教学模式。

“全国信息化计算机应用技术资格认证”（CCAT）考试的推行，为社会各界人士以及在校学生提供了学习最新的与国际接轨的计算机应用技能的机会，也为各类考生搭建了参加全国范围内考试的平台及获得国际性证书的机会，从而为以信息技术为核心的各行各业培养和造就符合《决定》精神的专业技术人才。该项考试一经推出，立即获得了社会的广泛认可和一致好评。

CCAT 系列教程是在全国高等学校计算机教育研究会和国际权威认证机构的指导下，按照国际通行的考试大纲、教学大纲并结合中国国情编写的，由全国信息化计算机应用技术资格认证管理中心组织各级专家、教授承担教程的编写与审定工作，由北京理工大学出版社和清华大学出版社共同出版。CCAT 系列教程不仅适用于社会各界人士以及在校学生参加“全国信息化计算机应用技术资格认证”考试的需求，同样适用于各级院校进行课程置换开展相关内容的教学工作。

加快高等教育的创新，促进高等教育、高等职业技术教育和经济社会发展紧密结合，调

整学科和专业结构，创新人才培养模式，是我们责无旁贷的历史重任。为此，我们呼吁各级高校把认证项目列入教学计划，使学生取得相应模块的认证资格，并计入学分，创立高校教育培养同人才需求结构相适应的有效机制。

全国高等学校计算机教育研究会理事长 袁开榜

前　言

为贯彻中共中央、国务院《关于进一步加强人才工作的决定》，培养高层次、高技能和复合型的社会急需人才，全国信息化计算机应用技术资格认证管理中心受国家人事部中国高级公务员培训中心和教育部全国高等学校计算机教育研究会的委托，组织编写了全国信息化计算机应用技术资格认证（简称“CCAT 资格认证”）项目的指定教材。CCAT 资格认证项目是全国性的 IT 培训认证项目，其主要特色是为社会培养动手能力和管理能力兼备的人才。该培训认证与在国际上享有盛誉的瑞士管理论坛（Swiss Management Forum ，简称“SMF”）已实现了国际互认。本书属于 CCAT 资格认证项目中工程师级认证体系。

随着计算机技术和网络互联技术的飞速发展以及人们对信息资源共享的强烈需求，互联网已经发展成为政府机关、企事业单位和各种团体开展日常工作的平台。通过这个平台，人们充分地共享着数据和信息资源，降低了人力、物力等方面的成本，极大地提高了工作效率。但是，互联网的普及也为一些道德品行不端之人创造了制造麻烦的条件，他们或是为谋取非法经济利益而窃取企业重要数据信息，或是怀着恶作剧心理而干扰网络正常运行。这些不良行为的存在，让网络用户尤其是企事业用户为自己数据的安全感到忧虑。如何保障互联网上重要数据的安全呢？除了加强数据自身的物理安全外，更主要的还是通过采用防火墙技术来保障。

防火墙技术是建立在通信网络技术和信息安全技术基础上的应用性安全技术，防火墙架设在企业内部网络和互联网之间，是保护企业内部网络免受互联网不良入侵的有效屏障，它能够将未被授权的访问阻塞掉从而保障了内部网络数据的安全。防火墙在保护网络安全方面已经发挥出越来越重要的作用。

最早的防火墙是依附于路由器的包过滤功能，即通过在路由器上创建简单的访问控制列表来实现防护功能。但由于传递数据包的网络协议的复杂性，基于路由器的访问控制列表还是不够安全的。随后，防火墙历经发展，先后出现了满足不同需求的应用级网关防火墙、电路级网关防火墙、状态包检测防火墙以及 VPN 技术。其中状态包检测防火墙由于协议的灵活性和很好的性能成为最佳选择。目前，大多数防火墙产品都包含了状态包检测功能和 VPN 技术。

目前也没有哪个防火墙产品能做到十全十美，一般都是在某方面具有优势。因此，最好的网络安全防护方案技术提供多层的访问控制，除了采用防火墙来高效地保护内部网络外，各个应用系统、各个服务器、甚至每台工作站的自身安全防护也不可忽视。所以说，防火墙固然很重要，虽然能很好地保护重要数据信息，但更重要的是人们的安全防护意识。希望大家能够通过本书，了解防火墙技术，了解基本的原理，提高网络安全意识。

本书共分 7 章。第 1 章，介绍了防火墙的基本概念和功能，阐明了采用防火墙的原因，列举了防火墙的几种部署方案。第 2 章，介绍了支撑防火墙技术的网络基础知识，包括 OSI 七层模型以及模型中的各层功能作用、TCP/IP 数据传输的实现过程和实现防火墙技术的应用层的几种常见的应用程序和工具的使用。第 3 章，介绍了与防火墙实施相关的网络设计技术，

包括从网络安全的级别确定、网络拓扑结构的选择、网络安全策略定义等方面来设计网络防火墙的实施方案。第 4 章，根据防火墙的发展过程介绍防火墙自身的几种体系结构，包括双重宿主主机体系结构、被屏蔽主机体系结构和被屏蔽子网体系结构。还介绍了包过滤、应用级网关、电路级网关和状态包检测等防火墙技术的实现机制和各自的优缺点。最后还介绍了基于网络主机等几种防火墙的具体实施。第 5 章，介绍了防火墙的多种高级功能及其相关知识，如与加密相关的密码理论、与访问控制相关的身份验证和授权机制、保护私有网络数据安全的 VPN 技术和 IPSec 协议知识，还有网络地址转换、病毒免役和网络监控等等技术，这些功能的实现使得防火墙在网络安全防护中的作用更加突出。第 6 章，介绍了常见的网络攻击类型和方法、几种常用的防范网络攻击的类型和方法以及由于防火墙自身漏洞问题而常面临的几种攻击。第 7 章，介绍了目前流行的几家防火墙产品，如 Check Point、Ciso PIX、Linux IP Table、Microsoft ISA Server、NetScreen 和 SonicWALL，详细介绍了这些产品的性能、功能、安装和配置以及产品的管理维护，为防火墙产品的选购和应用提供了参考依据。

本书在编写过程中力求体现下列特点：

1. 本书所涉及的知识点由浅入深，与防火墙技术密切相关，并且与实际产品相结合，所以实用性较强，能为采用防火墙技术实现网络安全防护的网络安全管理员、工程师和技术人员以及对防火墙感兴趣的人员提供切实的指导。

2. 内容阐述循序渐进，图文并茂、条理清楚，便于自学。

3. 配有多媒体教学光盘，使读者能在最短的时间内掌握最多的知识和技能。

4. 配有一套标准题库，该题库中的每个例子都对不同知识点进行了练习，对于读者掌握这些知识点及使用技巧都有很大的帮助。

本书是 CCAT 资格认证指定教材，适用于社会各界人士以及在校学生参加“全国信息化计算机应用技术资格认证”考试的需求，尤其适用于高等院校、大中专学校等进行课程置换，作为相关课程的教材，亦可作为计算机职业技能考试及继续教育的培训教材或自学教材。

由于时间仓促，加之编者水平有限，书中难免有疏漏之处，恳请广大读者批评指正。

编 者

目　录

第 1 章　防火墙基础

随着 Internet 在全世界的迅速发展和广泛应用，Internet 中出现的信息泄密、数据篡改和服务拒绝等网络安全事件频繁发生，网络安全问题越来越严重。为解决这些问题，出现了很多网络安全技术和方法，防火墙是其中最为成功的一种。

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来越多地应用在专用网络与公用网络的互联环境中，特别是接入 Internet 网络。

1.1　什么是防火墙？

“防火墙”这个术语来自应用在建筑结构里的安全技术。在楼宇里用来起分隔作用的墙，用来隔离不同的公司或房间，尽可能地起防火作用。一旦某个单元起火，这种方法就可以保护其他的居住者。然而，多数防火墙里都有一个重要的门，允许人们进入或离开大楼。因此，虽然防火墙保护了人们的安全，但这个门在提供增强安全性的同时也应该允许必要的访问。

在计算机网络中，防火墙是一个保护一个网络免受其他网络攻击的屏障。具体地讲，防火墙是一种用来加强网络之间访问控制的特殊网络设备，它对两个或多个网络之间传输的数据包和连接方式按照一定的安全策略对其进行检查，来决定网络之间的通信是否被允许，其中被保护的网络称为内部网络或私有网络，另一方则被称为外部网络或公用网络。防火墙能有效地控制内部网络与外部网络之间的访问及数据传输，从而达到保护内部网络的信息不受外部非授权用户的访问和过滤不良信息的目的。

从技术角度来讲，防火墙是采用综合的网络技术（包过滤技术等）设置在被保护网络和外部网络（或公用网络）之间的一道屏障，用以分隔被保护网络与外部网络系统防止发生不可预测的、潜在破坏性的入侵。它是不同网络或网络安全域之间信息的唯一出入口，像在两个网络之间设置了一道关卡，能根据企业的安全政策控制出入网络的信息流，防止非法信息流入被保护的网络内，且本身具有较强的抗攻击能力。它是提供信息安全服务、实现网络和信息安全的基础设施。

图 1–1 显示了一个简单的防火墙结构。

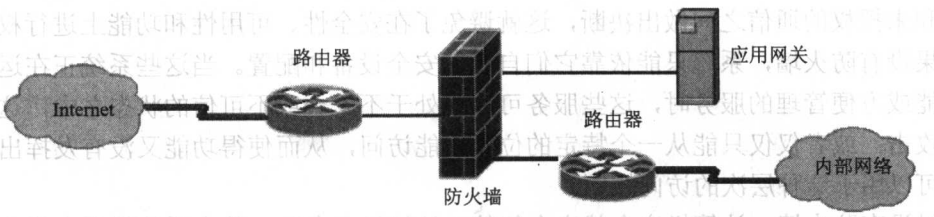

图 1–1　防火墙结构

在防火墙结构中，连接互联网的路由器（外部路由器）强迫所有流入的通信流量经过应