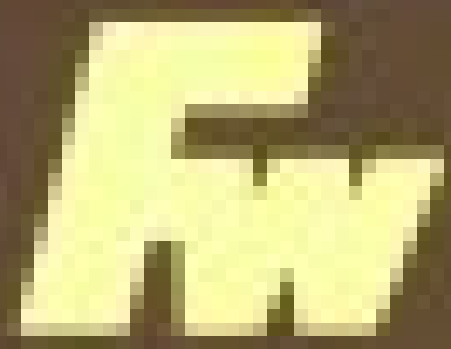
阎 慧 王 伟 宁宇鹏 等编著

防火墙原理与技术

国家信息化安全教育认证(ISEC)系列教材

机械工业出版社
CHINA MACHINE PRESS



防火墙原理与技术

国家信息化安全教育认证(ISEC)系列教材

防火墙原理与技术

阎 慧 王 伟 宁宇鹏 等编著

机械工业出版社

本书是ISEC系列教材中的一本，主要从防火墙核心技术、测试和选购方法、配置、防火墙新技术、和防火墙应用案例等多个方面对防火墙相关技术进行了阐述和分析。

全书在深入浅出对防火墙原理进行分析的基础上，注重防火墙的实际应用和案例分析。

本书适用于负责安全保障的网络管理人员、信息管理人员和对计算机和网络安全管理感兴趣的读者，也可以作为网络安全培训和高等院校的教材。

图书在版编目(CIP)数据

防火墙原理与技术/阎慧等编著. —北京：机械工业出版社，2004.4
(国家信息化安全教育认证(ISEC)系列教材)
ISBN 7-111-14172-5

Ⅰ.防… Ⅱ.阎… 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(2004)第019293号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)
责任编辑：丁 诚
责任印制：李 妍

北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2004年5月第1版·第1次印刷
787mm×1092mm 1/16·12.75印张·314千字
0001—5000册
定价：22.00元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话：(010)68993821、88379646
封面无防伪标均为盗版

国家信息化安全教育认证(ISEC)专家组

卿斯汉　中国科学院信息安全技术工程研究中心主任　研究员
曲成义　中国航天科技集团公司第710研究所总工　研究员
许榕生　中国科学院高能物理研究所计算中心研究员
贾颖禾　国务院信息化工作办公室网络与信息安全组研究员
曹元大　北京理工大学软件学院院长　博士生导师
杨义先　北京邮电大学信息安全中心主任　博士生导师
林　鹏　国家计算机网络应急技术处理协调中心广东分中心副主任
　　教授级高级工程师
祁　金　公安部公共网络信息安全监察局管理监察处副处长
景乾元　公安部公共网络信息安全监察局安全对策处副处长
万平国　国际信息战略研究中心理事　中网通讯网络有限公司董事长
刘宝旭　中国科学院高能物理研究所计算中心副研究员

教材编委会

主　任：宋　玲
副主任：赵小凡　张会生　欧阳满　蔡金荣　沈志工
成　员：洪京一　张宝泰　王　宏　孙论强　彭　澎　张晓伟
　　刘树安　刘　旸　马志谦　胡　铮　宁宇鹏　阎　慧
　　王　伟　薛静锋　辛　阳

出版说明

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时，也面临着日益突出的信息安全问题。党和国家领导人多次强调，必须充分认识到做好信息安全保障工作的重要性，大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用，再到各级网络信息系统信息安全保障体系的建设、运行，需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督，由 ISEC 国家信息化安全教育认证管理中心统一管理与实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同，教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计，课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次，不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下，由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据，坚持面向行业用户的需求和侧重技术应用两个基本原则，全面地介绍了信息安全各种主流技术和管理规范，以帮助读者深入了解信息安全本质，并熟练掌握相应的技能，从而建立完备的信息安全观念。本系列教材包括：《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》，共计 10 本。

在写作过程中，北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

前　言

电子政务和电子商务是信息数字化发展到一定阶段的必然产物。随着电子政务和电子商务的展开，办公、生活、交流和信息共享的数字化，标志着我国已经全面进入信息化社会，但是人们不得不在享受网络带来便利的同时深切关注网络体系结构和网络技术本身所带来的信息安全问题。防火墙便是人们遇到网络安全问题后最先想到的解决方案之一。

和其他网络安全技术相比，防火墙技术相对成熟，应用也最为广泛。它通过监测、限制和更改跨越防火墙的数据流等多种技术，尽可能地对外部网络屏蔽有关被保护网络的结构信息，实现对公司内部网络的安全保护。虽然面对复杂的网络安全问题，防火墙并不是唯一有效的解决方案，但是有一点是得到实践证明和肯定的：直到今天，人们依然把没有防火墙保护而通过服务器或其它设备在网络上提供网络服务的行为认为是自杀性的。所以，网络安全的维护离不开防火墙。

本书以国家信息化安全教育认证（ISEC）考试大纲为依据，从防火墙技术原理起笔，介绍了防火墙测试和选购的方法，侧重于防火墙在实际网络安全防护中的应用。针对配置不完善的防火墙可能存在大量安全漏洞等问题，详细讲解了典型防火墙产品的配置方法，精选了防火墙在政府、企业中实现网络安全解决方案的真实案例，最后通过对防火墙新技术的分析和未来发展的展望来帮助读者建立和完善多层次的防火墙相关知识体系。本书共包含四个部分：

第一部分防火墙基础技术篇，包括第1、2、3章，主要从防火墙的核心技术出发，阐述防火墙各项核心技术的工作原理，帮助读者建立起防火墙基本概念和技术基础。

第1章　防火墙基础：本章介绍了防火墙基本功能、结构、分类和最新发展方向，旨在帮助读者建立起防火墙概念，了解防火墙基本知识。

第2章　防火墙技术：防火墙技术是由多种技术组合而成的，本章介绍了防火墙的三大核心技术：包过滤技术、网络地址翻译技术和代理技术。通过对防火墙核心技术深入浅出的分析，为读者实现防火墙配置和排错打下理论基础。

第3章　虚拟专用网络：虚拟专用网络是独立的网络安全技术，但是在实际应用中其功能大多集成在防火墙中实现，本章通过对IPSEC虚拟专用网络技术的讲解和分析，帮助读者建立起相对完善的防火墙知识体系。

第二部分防火墙测试选购篇，包括第四、五、六章，针对网络安全设备选购者编写，为读者阐述了防火墙测试技术、主流防火墙产品和防火墙的选购方法：

第4章　防火墙标准与测试：本章介绍防火墙相关标准和测试方法。

第5章　防火墙产品：本章收集了大量国内外主流防火墙的信息，并对各种防火墙的特点进行了分析和比较。

第6章　防火墙产品的选购：本章撰述了防火墙选购的原则和需要注意的问题。

第三部分防火墙配置实例篇，包括第7、8、9章，通过对基于路由器的Cisco IOS防火墙特征集，基于Linux的IPTables防火墙和商业防火墙的配置实例讲解，引领读者掌握防火墙实际

操作技能：

第 7 章　Cisco IOS 防火墙特征集：本章介绍了基于路由器实现的 Cisco IOS 防火墙特征集的配置方法，并给出了大量配置实例分析。

第 8 章　Linux IPTables 防火墙配置：本章介绍了最为流行的基于 Linux 操作系统的 IPTables 防火墙的配置方法。

第 9 章　商业防火墙配置示例：本章以方正方通防火墙为实例，为读者描述了基于硬件的防火墙常见的配置方法。

第四部分防火墙深入应用篇，包括第 10、11 章，主要针对防火墙网络安全解决方案的投标与竞标者编写，介绍了防火墙发展中的新兴技术和发展趋势，并给出了企业中防火墙的实际应用案例和方案，有利于用户在实际解决问题时借鉴，增强了本书的完整性和实用性：

第 10 章　防火墙新技术：本章对近年来国内外防火墙中出现的新技术进行了分析和讲解，为读者勾勒出了防火墙技术发展现状和趋势的蓝图。

第 11 章　防火墙指标说明与解决方案：本章给出了详细的防火墙技术指标说明和防火墙在企业中应用的真实案例。

本书主要由阎慧、王伟和宁宇鹏执笔完成，其中第 1、4、5、6、10 章主要由阎慧完成，第 2、3、7、8 章主要由王伟完成，第 9、11 章主要由宁宇鹏完成。另外北京正阳天马信息技术有限公司刘旸先生、马志谦先生也参与了本书的部分编写工作。

编　者

2004 年 3 月

目　录

第三部分 防火墙配置实例篇

第四部分 防火墙深入应用篇

第一部分　防火墙基础技术篇

第1章　防火墙基础

本章导读：

作为本书的第一章，本章主要介绍了防火墙的基本概念。首先引入了防火墙的定义，然后详细介绍了防火墙的优缺点、基本结构、模型和分类。接着分析了一些常见的攻击方法和防火墙的防御方法以及针对防火墙的攻击手段。最后探讨了防火墙的发展历程和趋势。通过本章的介绍，读者可对防火墙有一个基本的认识，从而奠定深入学习后续内容的基础。

1.1　防火墙概论

TCP/IP协议在互联网中的迅速崛起，造成了Internet的风行全球。然而，最初主要应用于学术研究的Internet以及运行的通信协议是为比目前良好得多的环境而设计的。那时用户和主机之间互相信任，可以进行自由开放的信息交换。而如今Internet上的每一个人都可能遇到安全风险。以各种非法手段企图深入计算机网络的黑客，随着网络覆盖范围的扩大而增加。从而使网络安全成为任何一个计算机系统正常运行并发挥作用的必然选择和必须要考虑的因素。Internet的安全问题成了关注的焦点。早在1994年，在IAB(Internet体系结构理事会)的一次研讨会上，扩充与安全就被当作最重要的两个问题被讨论了。

网络安全从其本质上来讲就是网络上的信息安全。网络信息安全一般是指网络信息的机密性(Confidentiality)、完整性(Integrity)、可用性(Availability)、真实性(Authenticity)、实用性(Utility)和占有性(Possession)。

- 机密性：网络信息的内容不会被未授权的第三方所知。
- 完整性：信息在存储或传输时不被修改、破坏。
- 可用性：可被授权实体访问并按需要使用的特性。
- 真实性：是指信息的可信度，主要是指对信息所有者或发送者的身份的确认。
- 实用性：指信息加密的密钥不可丢失，丢失密钥的信息也就丢失了信息的实用性。
- 占有性：指存储信息的主机，磁盘等信息载体不能被盗用，否则就丧失了信息的占有性。

为了从上述几个方面保障计算机系统的安全，尤其在Internet的环境中，网络安全体系结构的考虑和选择显得尤为重要。采用传统的防火墙网络安全体系结构不失为一种简单有效的选择方案。

1.1.1　防火墙定义

古时候，当人们在构筑和使用木制结构房屋的时侯，为防止火灾的发生和蔓延，往往将坚固的石块堆砌在房屋周围作为屏障，这种防护构筑物被称为“防火墙”。在今日的电子信息世

界里，往往借用了这个概念，使用防火墙来保护敏感的数据不被窃取和篡改，不过这些防火墙是由先进的计算机系统构成的。

防火墙尤如一道护栏隔在被保护的内部网与不安全的非信任网络之间，这道屏障的作用是阻断来自外部的对本网络的威胁和入侵，保护本网络的安全。这种中介系统也叫作“防火墙”，或“防火墙系统”。

一般说来，防火墙是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全策略控制（允许、拒绝、监测）出入网络的信息流，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。

防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域（即 Internet 或有一定风险的网络）与安全区域（局域网）的连接，同时不会妨碍人们对风险区域的访问。防火墙可以监控进出网络的通信量，仅让安全、核准了的信息进入，同时又抵制对企业构成威胁的数据。随着安全问题上的失误和缺陷越来越普遍，对网络的入侵不仅来自高超的攻击手段，也有可能来自配置上的低级错误或不合适的口令选择。而防火墙的作用就是防止不希望的、未授权的信息进出被保护的网络。因此，而防火墙正在成为控制对网络系统访问的非常流行的方法。作为第一道安全防线，防火墙已经成为世界上用得最多的网络安全产品之一（如图 1-1）。

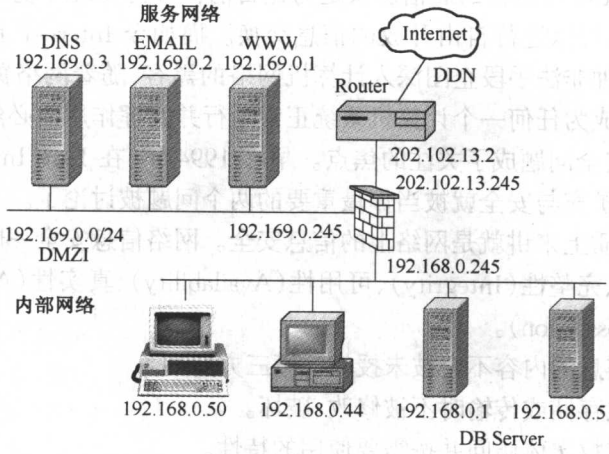


图 1-1 基本的防火墙系统模型

在逻辑上，防火墙既是一个分离器，一个限制器，它也是一个分析器，它有效地监控了内部网和 Internet 之间的任何活动，保证了内部网络的安全。从具体实现上来看，防火墙是一个独立的进程或一组紧密联系的进程，运行于路由器或服务器上，控制经过它们的网络应用服务及传输的数据。安全、管理、速度是防火墙的三大要素。

1.1.2 防火墙的优点

防火墙能提高了主机整体的安全性，因而给站点带来了众多的好处。它主要有以下几方面的优点。

1. 防火墙是网络安全的屏障

一个防火墙(作为阻塞点、控制点)能极大地提高一个内部网络的安全性,并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙,所以网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护网络,这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击,如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 控制对主机系统的访问

防火墙有能力控制对主机系统的访问。例如,某些主机系统可以由外部网络访问,而其他主机系统则能被有效地封闭起来,防止有害的访问。通过配置防火墙,允许外部主机访问 WWW 服务器和 FTP 服务器的服务,而禁止外部主机对内部网络上其他系统的访问。

3. 监控和审计网络访问

如果所有的访问都经过防火墙,那么,防火墙就能记录下这些访问并作出日志记录,同时也能提供网络使用情况的统计数据。当发生可疑动作时,防火墙能进行适当的报警,并提供网络是否受到监测和攻击的详细信息。另外,收集一个网络的使用和误用情况也是非常重要的,可以清楚防火墙是否能够抵挡攻击者的探测和攻击,并且清楚防火墙的控制是否充足。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分,可实现内部网重点网段的隔离,从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。另外,使用防火墙可以隐蔽那些会泄漏内部细节的服务如 Finger,DNS 等。

5. 部署 NAT 机制

防火墙可以部署 NAT 机制,用来缓解地址空间短缺的问题,也可以隐藏内部网络的结构。

1.1.3　防火墙的弱点

虽然防火墙是网络安全体系中极为重要的一环,但并不是惟一的一环,也不能因为有了防火墙就认为可以高枕无忧了。信息安全专家发现他们经常需要和人们的错误观念作斗争,这种错误观念来源于人们的美好愿望,而不是实际的情况。例如,人们可能认为只要有一个防火墙,所有的安全问题都解决了。但事实上,尽管防火墙应当受到人们的充分重视,但仍有一些危险是防火墙解决不了的。

1. 防火墙不能防范来自内部网络的攻击

目前防火墙只提供对外部网络用户攻击的防护。对来自内部网络用户的攻击只能依靠内部网络主机系统的安全性。

2. 防火墙不能防范不经由防火墙的攻击

如果允许从受保护网内部不受限制的向外拨号,一些用户可以形成与 Internet 的直接的连接,从而绕过防火墙,造成一个潜在的后门攻击渠道。例如,在一个被保护的网络上有一个没有限制的拨出存在,内部网络上的用户就可以直接通过 SLIP 或 PPP 连接进入 Internet。这就为从后门攻击创造了极大的可能(见图 1-2)。要使防火墙发挥作用,防火墙就必须成为整