清华大学计算机安全译丛

PEARSON
Prentice
Hall

防火墙与VPN

原理与实践 Firewalls and VPNs

Principles and Practices

Richard Tibbs Edward Oakes 著
李展 刑博特 等 译

PEARSON
Education

清华大学出版社

清华大学计算机安全译丛

PEARSON Prentice Hall

防火墙与VPN

原理与实践 Principles and Practices Firewalls and VPNs

Richard Tibbs Edward Oakes 著
李展 刑博特 等 译

清华大学出版社
北京

图书在版编目(CIP)数据

防火墙与 VPN——原理与实践/(美)迪波斯(Tibbs, R.),(美)奥克斯(Oakes, E.)著;李展等译. —北京: 清华大学出版社, 2008.12
书名原文: Firewalls and VPNs Principles and Practices
ISBN 978-7-302-18651-9

Ⅰ. 防… Ⅱ. ①迪… ②奥… ③李… Ⅲ. 计算机网络—防火墙 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 149762 号

责任编辑: 龙啟铭 李玮琪
责任校对: 徐俊伟
责任印制: 王秀菊

出版发行: 清华大学出版社 **地 址**: 北京清华大学学研大厦 A 座
http://www.tup.com.cn **邮 编**: 100084
社 总 机: 010-62770175 **邮 购**: 010-62786544
投稿与读者服务: 010-62776969, c-service@tup.tsinghua.edu.cn
质 量 反 馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者: 北京市昌平环球印刷厂
装 订 者: 三河市李旗庄少明装订厂
经 销: 全国新华书店
开 本: 185×230 **印 张**: 23.5 **字 数**: 566 千字
版 次: 2008 年 12 月第 1 版 **印 次**: 2008 年 12 月第 1 次印刷
印 数: 1～3000
定 价: 46.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。
联系电话: 010-62770177 转 3103 产品编号: 026832-01

安全系列丛书

安全系列丛书是为将要从事信息技术安全职业的学员准备的一套丛书。这套丛书提供了来自业界专家的实践箴言，和对你手把手的培训。该丛书中的每本书，都列举了现实生活中大量的例子。这些例子能帮助你将所学到的知识应用到你的工作中去。以下是本书的几个关键元素，这些元素的目的是帮助学员解决学习过程中的一些问题。

本章目标：这些扼要、可行的目标概括了该章将涵盖哪些内容。

本章导论：每章开始先阐释一下每个主题的重要性，以及这些主题在整本书篇章结构中的地位。

实例：从书中提取出概念，而且展示这些概念是如何用在实际场所中的。

提示：和主题相关、但是超出了本书讨论范围的额外信息。

注意：不可忽视的、关键的信息。这些信息和上下文直接相关。

技能测试：每章末都附有习题，这些习题呼应该章目标，巩固相关的知识点。每章有四种题型：

- **多项选择题**：测验读者对该章内容的理解程度。
- **练习题**：围绕章节中出现的个别概念设计的简要、引导性的课程项目。
- **项目题**：综合一章内若干知识点的较长、引导性的课程项目。
- **案例研究**：运用该章中的知识点来解决问题的实际场景。

本系列丛书包括：

- 计算机安全基础
- 信息安全：原理与实践
- 防火墙与 VPN：原理与实践
- 安全策略与规程：原理与实践
- 网络防御与安全对策：原理与实践

“计算机安全”类图书还有：

书　名	书　号	定　价
密码学与网络安全	978-7-302-11490-1(翻译版)	43.00 元
	978-7-302-09967-3(影印版)	48.00 元
网络安全基础：应用与标准(第 3 版)	978-7-302-15435-8(翻译版)	39.00 元
	978-7-302-15451-8(影印版)	39.00 元
经典密码学与现代密码学	978-7-302-10740-8(翻译版)	35.00 元
	978-7-302-11156-6(影印版)	23.00 元
网络安全：加密原理、算法与协议	978-7-302-15259-0	39.00 元

译者序

本书采用教科书形式、以理论基础与实际应用结合的方法，全面介绍了与网络安全相关的各种内容，覆盖了防御对策、攻击形式以及与计算机安全相关的策略，填补了其他一些安全图书某些内容缺失的空白。

本书以平易近人的语言详细阐述了防火墙、入侵检测系统、加密基础、操作系统加固、抵御病毒/木马/间谍软件攻击以及安全策略和安全标准的实际应用。为了巩固学习的知识，在本书每一章的末尾，都给出了多项选择题、练习题、项目题和一个案例研究，为学生提供了动手实践和深入理解本章内容的机会。

本书适合于作为学习网络安全的教材，也是网络管理员、安全专业人员以及安全审计专业人员日常工作的手边手册。

参加本书翻译工作的人员包括：张长富、蔡建章、李匀、张建安、邓铁洪、徐君、杨莹、李强、李勇、蒋恩骏、杨文保、苏辛、周成兴、魏敬安、朱建波、徐志平、赵杰辉、傅祎、郭碧莲、郭洵、洪晓煜、黄宣达、江松波、柯渝、赖曲芳、廖阳、刘文红、贺军等，张福林先生对本书中的一些关键段落和疑难之处作出了详细的解释和指导，在此深表感谢。限于译者水平，错误和遗漏之处，敬请读者批评指导。

前言

随着越来越多的人们要求将办公室、家庭与远程工作空间的计算机相连接，网络安全已经成为一个日益重要的课题。美国联邦调查局（Federal Bureau of Investigation，FBI）报告显示，危害性网络安全攻击数量在逐年上升。计算机攻击的扩散以及对网络和对远程访问依赖程度的不断增长，促成了对诸如防火墙和虚拟专用网（VPN）等保护组织和个人免受威胁的系统需求的增长。同样，各种组织也需要适当配备能够统筹掌握安全软件与硬件的专业人员。本书的目的就是为学生（未来的专业人士）储备安装、使用和操纵防火墙与虚拟专用网的知识。

本书首先讲解基本网络与计算机安全概念，专门着重于网络和数据链路层以及 TCP 和 UDP 传输协议。基础一旦打牢，图书内容就转向了保护网络以及安装和操作防火墙的细节。本书涉及有关计算机网络威胁的内容，并且详尽解释每一项威胁对一个系统的意图，及其完成其任务的计划。读者将通过阅读和使用特定的防火墙技术、工具和技巧来学习保护系统安全，并且有一章篇幅全部用于防火墙安装和配置实践。之后本书转向虚拟专用网的主题，演示了虚拟专用网技术如何跨越 Internet 提供安全的通信——当前对不同位置之间安全通信问题的最廉价解决方案。最后，会通过对日志记录的介绍学习有关日常防火墙维护的思想。

在书中的实例、练习以及工程题中，均使用了低成本、易获得的硬件来创建小型网络，并帮助读者理解和学习防火墙和虚拟专用网。所有用到的软件均将在光盘或软盘上运行，而无须在硬盘驱动器上安装。因此，日常使用的电脑就可以用来做练习。本书中使用了四种开放源码方案：一种专门用于防火墙；两种用于虚拟专用网；还有一种方案中集成了其余所有设备。虽然在开放源码的网站中有这些方案的文档，但这类网站均假定读者已经具有很扎实的网络基础，并且具有丰富的 Linux 经验。在我们看来，将没有经验和经验很少的学生以及小规模企业主排除在外不尽合理。本书中所应用的工具和技术均可满足这些经验较少的用户。

除了我们对开放源码方案以及面向 Linux 应用程序的偏爱，我们还提供了使用商用操作系统和软件防火墙的一定数量的练习。而且，我们还提供了专门的参考书，用于复习商用和开放源码虚拟专用网解决方案。无可避免，

Windows-Linux集成在多年内将会是主流趋势。所以贯穿于本书始末，我们指出，Windows 应用程序能够用于访问开放源代码技术、初级 Linux 技术、防火墙技术和虚拟专用网技术。

由于很多经济上的原因，各院校和大学有预算限制的羁绊，而且免费的开放源码解决方案对于学生的价值，被唯一一件事情所阻碍：缺乏基本网络安全原理的例子，并为实验室提供完整实践练习的教科书。我们希望这本书能够满足这些需求。

本书读者对象

本书适合四年制大学生和对 TCP/IP 网络具有基本了解的人士。本书重点讲解了一类基于 Linux 的防火墙(LEAF)以及几类基于 Linux 的工具，但完成练习和方案并不需要具备 Linux 的预备知识。本书可以整体用于一门有关防火墙和虚拟专用网的课程中；或者，本书的第二部分以及第三部分可以与一篇入门介绍的文档联合用于提供对网络深入理解的课程中。为了完全利用本书，上述课程应包含能够进行广泛实践练习、实现方案和进行案例研究的实验室。

本书主要内容

第 1 部分：网络概念与 TCP/IP 族(第 1 章和第 2 章)

第 1 部分的章节对网络安全进行了复习，并介绍了 TCP/IP 协议族的网络覆盖范围。这部分是对 TCP/IP 的复习和对基本网络安全概念的介绍。讨论或者在与有关网络的基本文档同时使用时，可以完全跳过本部分。

第 1 章提供了对 TCP/IP 协议栈的一般理解。其范围包括了对 MAC 地址以及 IP 协议和 IP 报头的过滤及细节。实践方案将要求使用子网和超网(supernetting)来指定和聚合 IP 地址阻塞，以及使用嗅探器和其他工具来镜像/捕获网络流量。第 2 章介绍了 TCP 协议和 TCP 有限状态机。由于对 TCP 协议报头的状态过滤在防火墙技术中是一个重要概念，所以，读者应学会在 TCP 会话中追踪数据包流量。由于虚拟专用网频繁在 UDP 中嵌入它们的数据包，在第 2 章中详尽揭示了 UDP 报头和使用 UDP 的基本应用程序。为了巩固第 2 章中的概念，读者将会使用 ping 以及 traceroute 功能完成一些基本的网络诊断。

第 2 部分：防火墙基础(第 3 章～第 7 章)

第 2 部分介绍了几种类型的防火墙，并且详尽讲解了：防火墙的安装；创建防火墙策略；以及防火墙规则和策略如何影响网络流量。

第 3 章的内容覆盖了一系列免费和商用防火墙，包括 Windows XP 防火墙以及 Mac OS X 操作系统防火墙。本章还介绍了路由器访问控制表以及 Linux 内核中的 iptables 工具。Nmap 工具用于讲解端口扫描器，并作为决定网络中开放端口的工具。

第 4 章首先概括了来自 Internet 和内网的众多威胁。数据包过滤是防火墙的主要工作，并且有主要方法——无状态以及状态方式——来决定是允许还是拒绝数据包。第 4 章

还完整地概括了 IP 路由，及其影响路由器或防火墙应作出的决定。Nessus 在本章中作为一种高级网络扫描工具而被引入。

第 5 章是有意安排的第一次防火墙类练习，其中包含了安装方案。第 5 章解释了个人配置文件以及嵌入式 Linux 防火墙(LEAF)特性。

防火墙保护内网计算机免受外部攻击，并且控制内网计算机访问 Internet。第 6 章提供了有关允许通过防火墙的服务和应用的信息。本章有助于通过建立防火墙策略的步骤为网络管理员提供指引。本章探究了防火墙所提供的服务或必须允许防火墙通过的服务，例如端口转发。本章还继续进行了在第 3 章中开始的对路由器访问控制列表的讨论。

第 7 章继续了在第 3 章中开始的对 iptable 的讨论，将 iptable 与 LEAF Shorewall 设备进行比较。本章还继续了在第 4 章中开始的对威胁的讨论。第 7 章以一些配置实例更深入探究了防火墙如何为内网提供服务。

第 3 部分：VPN 和日志(第 8 章和第 9 章)

第 3 部分覆盖了有关虚拟专用网与及使用日志文件完成网络事件回顾分析的内容。要理解本部分中的概念，需要理解第 2 部分中的主题，这里是第 2 部分的延伸。但即便是第 2 部分没有包含在课程中，第 3 部分中的某些章节还是会涉及到相关内容。

第 8 章覆盖了 IPSec、传输层安全(TLS，也叫做套接层安全(SSL))以及虚拟专用网的细节内容，并为每项内容配备了几个项目练习题。本章还概括了点对点隧道协议，讨论了在医疗网络中如何保证有线和无线连接的安全，符合 HIPPA。第 8 章进一步继续讨论了在虚拟专用网环境下密钥交换的威胁。它还描述了如何使用开放源码软件设置个人证书授权，以方便学生完成实验室的工程练习。

第 9 章讲解了几个主题，包括系统、防火墙以及路由器日志同时被“提取”时发生的日志服务器和“数据融合”问题。本章的目的是在发现安全漏洞时减轻系统管理员和网络管理员的负担。在这种环境中，毁坏评估和对破坏者评估尤为重要。章节主题包含了对 Linux 中 syslog 守护进程、Microsoft Windows 日志记录的介绍，以及守护进程工具(daemontl)和其他在 LEAF 中可见的日志配置范围的讲解。

章节末的练习、项目和案例研究均随本书的进展而增加难度。案例研究均取自实际环境。

本书约定

为了帮助读者从本书中获取更多知识，我们在书中使用如下约定：

练习：有关练习

这些内容说明如何理解书中介绍的概念，并在工作中加以应用。

提示：有关提示

这里提供超出本书范围的相关主题信息。

这里说明如何将书中学到的概念在实践中运用它们。

注意一般出现在正文的边栏。它们表示关键的、需要牢记的信息,这些信息直接与正文有关。

源代码段以及代码块均被框起并以数字标注,并且均能在 www. prenhall. com/security 中下载。

新出现的关键术语以斜体字出现。

此图标表示能在相应网站 www. prenhall. com/security 上找到更多信息。

教师和学生资源

教师资源仅提供给教师,需要这些资料的老师请与 longqm@tup. tsinghua. edu. cn 联系。它含包:

- 教师手册:提供教学提示、每章导言、教学目标、教学建议以及章末习题的答案。
- PowerPoint 幻灯片演示:每章课件,用于教学。
- 题库:用 Prentice Hall 的 TestGen 软件可以使用这个 TestGen 兼容的题库文件。该软件在 www. prenhall. com/testgen 网站上可以免费下载。TestGen 是试题生成器,可以以适合不同教学情形的各种形式打印。该程序提供许多选项,可以组织和显示题库和测验。它具有内置的随机数字以及文本生成器,通过计算可以创建试题的多个版本,所提供的测试题可能比题库问题更多。强大的搜索和排序功能,使用户能够轻松找到试题,以需要的方式安排它们。

本书配套网站

www. prehall. com/security 是本书配套网站,这是一个 Pearson 学习工具,可以为学生和教师提供在线支持。其内容主要包括如下几方面。

- 交互式学习指南。这是基于 Web 的交互式测试,学生可以在这里方便地进行在线测试,自行检测是否掌握了本书的相关知识。
- 附加的 Web 工程和资源,练习每章所学的基本概念。
- 防火墙和 SLAX 的 ISO 光盘镜像,提供项目和练习的平台。

作者简介

Richard W. Tibbs

Tibbs 博士获得了美国乔治梅森大学(George Mason)系统与信息技术工程学院的哲学博士学位,专门从事运营研究。他还在科罗拉多大学波尔得分校(University of Colorado, Boulder)获得了计算机科学硕士学位以及应用数学学士学位。

他主要研究网络安全、网络和计算机、网络和计算机容量规划、队列理论和仿真、流量监控和分析,以及远程通信网络中的自适应路由。他是 ACM、IEEE 和 INFORMS 的成员。

Tibbs 博士曾在工业部门、政府机关和学术研究单位工作 20 多年,后来在瑞德福大学(Radford University)任全职教师。他的行业背景包括宇航、电讯和软件开发。他在政府机关工作的单位是美国地质调查局和 MITRE 公司,他还在联邦基金研究和开发中心的运输工程部工作过。

Edward B. Oakes

Edward B. Oakes 在瑞德福大学(Radford University)获得了计算机科学学士学位,现在正在理工大学(Technology)硕士在读。2004 年,他由于教学开发的贡献获得了安娜李斯图尔特奖(Anna Lee Stewart)。

他现在是瑞德福大学理论计算方面的学术带头人,在网络和安全方面有超过 14 年的实践经验。除了其他角色之外,他还担任瑞德福大学信息安全主管有 5 年的时间。他喜欢的领域包括网络安全、无线计算,以及在教室中理论联系实际授课。

质量保证

感谢质量保证团队，他们关注细节，努力工作，确保本书的正确性。

技术编辑

Erich Titl
Charles Steinkuehler

审核者

Charles R. Esparza
Glendate Community College

Jeff Dorsz

Saddleback College

致谢

感谢开放源码用户名单中的用户：leaf 用户，shorewall 用户，openvpn 用户。特别感谢 Tom Eastep、Charles Steinkuehler、Erich Tile 和 James Yonan，感谢他们的鼎力帮助。感谢我的合作者——Ed Oakes，如果没有他的帮助，本书的完成是不可能的。

——Richard Tibbs

感谢 Tomas Matejicek，感谢他创建和继续改进 SLAX Linux Live 版本，感谢对 SLAX 项目做出贡献的所有人。感谢我的合作者——Rick Tibbs，在他的勤奋努力下，本书才得以成功。特别感谢 Nicole Sulgit 和 Megan Smith-Creed，感谢他们编辑本书的耐心细致。最后，感谢 Janie Hensdell、Kathy Harris 和我的父母，感谢他们在过去的几个月中对我的支持和帮助。

——Edward Oaks

目录

第 1 部分　网络概念与 TCP/IP 族