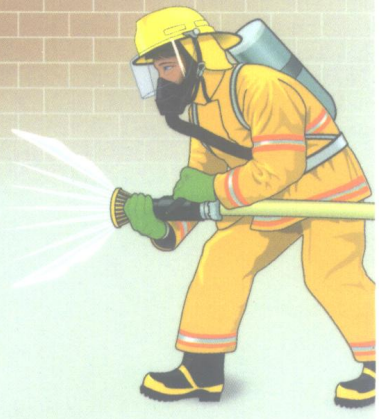
ET PUBLISHING 今日電子

网络安全

- 了解什么是防火墙，防火墙怎样保护商用网络免受攻击
- 了解防火墙的组成，包过滤器的作用，应用代理网关的功能
- 学习虚拟专用网(VPN)怎样保护用户在不安全网络(如因特网)上发送数据，而不用担心被截获

Practical Firewalls

防火墙原理与实施



[美] Terry William Ogletree 著
李之棠 李伟明 陈 琳 等译
李之棠 审校

que

電子工業出版社
Publishing House of Electronics Industry
URL:http://www.phei.com.cn

防火墙原理与实施

Practical Firewalls

[美] Terry William Ogletree 著

李之棠 李伟明 陈 琳 等译

李之棠 审校

電子工業出版社

Publishing House of Electronics Industry

北京 · Beijing

内容简介

CRACK、SATAN是什么？当使用因特网时，如何创建安全的数据传输通道？什么是拒绝服务攻击？包过滤[illegible]的作用是什么？Linux OS中包含了哪些内置的包过滤工具？在哪里能得到免费的软件以构建防火墙等等。这些都是从事网络管理的专业人士必须知道的。

本书针对网络管理员所面临的防火墙问题，通过精心准备和细致研究，提出了最好的解决方案。为了照顾终端用户，作者用通俗易懂的方式深入介绍了复杂的包过滤和代理等技术。同时，还通过一步步介绍常用的工具和命令，引导一般用户进行实践，达到成功使用防火墙的目的。从本书可以学到构建防火墙的基本概念，并了解几个常用的商用防火墙。

本书适用于网络管理人员及对防火墙技术感兴趣的人士。

Authorized translation from the English language edition published by Que Corporation, Copyright©2000.
All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Publisher.
Simplified Chinese language edition published by Publishing House of Electronics Industry, Copyright©2001.

本书中文简体版专有翻译出版权由Pearson教育集团所属的Que Corporation授予电子工业出版社。其原文版权及中文翻译出版权受法律保护。未经许可，不得以任何形式或手段复制或抄袭本书内容。

图书在版编目（CIP）数据

防火墙原理与实施 /（美）奥哥里瑞（Ogletree, T.）著；李之棠等译，北京：电子工业出版社，2001.2
（网络安全）
书名原文：Practical Firewalls
ISBN 7-5053-6525-8
Ⅰ.防… Ⅱ.①奥… ②李… Ⅲ.防火墙－基本知识 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2001）第06562号

书　　名：**防火墙原理与实施**
原 书 名：Practical Firewalls
著　　者：[美] Terry William Ogletree
译　　者：李之棠　李伟明　陈　琳　等
审 校 者：李之棠
责任编辑：赵红燕
排版制作：今日电子公司制作部
印 刷 者：北京东光印刷厂
装 订 者：三河司庄装订厂
出版发行：电子工业出版社　URL：http://www.phei.com.cn
　　北京市海淀区万寿路173信箱　邮编：100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：18　字数：450千字
版　　次：2001年2月第1版　2001年2月第1次印刷
书　　号：ISBN 7-5053-6525-8
　　TP·3594
定　　价：29.00元
版权贸易合同登记号　图字：01-2000-4358

凡购买电子工业出版社的图书，如有缺页、倒页、脱页、所附磁盘或光盘有问题者，请向购买书店调换。若书店售缺，请与本社发行部联系。电话：68279077

译 者 序

因特网——21世纪人类社会的数字神经，正以前所未有的速度在全球各个地方迅猛发展。其规模一天天扩大，带宽一天天提升，服务一天天增加。网上席卷的信息浪潮正铺天盖地地冲向人类生活的各个领域。这一切必将对人类社会的科学、技术、政治、经济、军事乃至文化和生活产生巨大的作用和深远的影响。

以TCP/IP为代表的开放式体系结构是因特网成功发展的关键原因之一，但这同时也给网络安全带来了深刻的危机和严重的挑战。全球每年因网络安全漏洞和黑客入侵造成的经济损失不计其数。各国政府和相关部门在推进网络化、信息化的同时也都十分关注网络安全的防范和处理。随着我国加入WTO进程脚步的日渐加快，这一问题将更为严峻和紧迫。我国的网络信息安全应该主要靠我们自己来解决。

当前，有关网络安全、特别是防火墙方面实用的书太少，本书正好满足这方面的需求。本书有以下三个特点：第一是内容新颖，如虚拟专用网、分布式拒绝服务攻击（DDOS）及Linux下的防火墙等技术和工具都是在同类书中尚未见到的。第二是基础扎实，为了让初学者了解防火墙的工作原理，作者从TCP/IP协议的机制及其固有的安全脆弱性到包过滤、应用代理的工作原理都进行了详细的论述。第三是注重实践，作者用了很大篇幅来介绍防火墙安全体系的构造、安全策略和安全规则的制定以及各种流行商用防火墙的实际使用等。尤其注重面向任务的解决方案和便于实现的技巧。它不仅对需要了解和使用防火墙的广大用户是一本有益的启蒙和指导书，而且对那些从事防火墙和网络安全研究的大专院校师生及专门研究人员也是一本难得的实用参考书。

本书由李之棠、李伟明、陈琳、尹恒、隋诚、舒承春等翻译，最后由李之棠审稿。在翻译过程中，曾得到华中科技大学天华网络安全研究所的研究生、武汉天融信网络安全技术有限公司的有关同志以及电子工业出版社吴源等同志的帮助，在此一并表示感谢。

由于我们水平有限，不妥之处在所难免，诚望读者批评指正。

译者

2000年11月于武汉

关于作者

Terry Ogletree 现在是新泽西的咨询顾问。他从 1980 年开始研究网络计算机系统，其研究对象是数字设备 PDP 计算机和基于开放 VMS 的 VAX 和 Alpha 服务器系统。从 1985 年开始，他从事 UNIX 和 TCP/IP 方面的工作，并且在 Windows NT 刚出现时，就着手研究它了。他编写了《Upgrading and Repairing Networks, Second Edition》(由 Que 出版公司出版)、《Windows NT Server 4.0 Networking》(由 Sams 出版公司出版)，该书是 Sams 的《Windows NT Server 4 Resource Library》的第四卷。另外，他还撰写了很多由 Macmillan 公司出版的书籍的部分章节，包括《Windows NT Server Unleashed》和 Que 出版公司出版的《Special Edition Using UNIX, Third Edition》。

可以通过其 Email 信箱 ogletree@bellsouth.net 写信给他，也可以访问他的主页 www.twoinc.com。

致　　谢

再一次感谢在编写本书的过程中 Macmillan 的编辑——资深编辑 Jenny Watson 和 Todd Brakke 的帮助。他们对本书提出了许多有用的建议。值得指出的是团队协调者 Vicki Harding，他一直关注我写书的进度。另外我在 Bristol-Myers Squibb 的老板 Robert Venard 和 Tom Crayner 对我的支持，是令人鼓舞并且非常值得感谢的。

我还要感谢几个人的帮助，虽然他们与编写本书没有直接的关系。特别感谢 Jo Chamblee、James Garrett 和 Steve McGuire，感谢他们对我写书的鼓励和支持。在 Raleigh，NC 的 Michael D. Parrot 及其同事的经济支持免去了我的后顾之忧，在此表示感谢。最后，感谢我的父母 Gordon Ogletree 和 Billie Jean Ogletree 对我的一贯支持。

告诉我们您的想法

作为本书的读者，您是我们最重要的批评家和评论员。我们很想知道您的观点，并且想知道我们所做的哪些是对的，哪些需要改进，您希望我们出版哪些方面的书籍以及其他的建议。

作为本书的出版者，我欢迎您的评论。您可以传真，发 Email 或者直接写信给我，告诉我关于本书您喜欢以及不喜欢的部分，以及怎样将本书写得更好。

我恐怕不能帮您解决关于本书所讨论一些技术问题，Terry W. Ogletree 欢迎您的技术咨询。跟他最好的联系方式是通过他的 Email: ogletree@bellsouth.net。

当您写信时，请一定要包含本书的书名，作者以及您的名字和电话或者传真号。我将会仔细地分析您的评论，并将它与本书的其他作者和编辑共享。

Fax: 317-581-4666

Email: hardware@mcp.com

Mail: Macmillan USA
201 West 103rd Street
Indianapolis, IN 46290 USA

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

在短短的几年之内，因特网已经渗透到人们生活的各个方面。可以预料，未来的几年里，对大多数人来说，连上因特网，就和使用电话一样普遍。随着技术的发展，出现了一个新的领地——赛百空间。然而在这个新的领域，使用传统的方法来保护网络上的数据和资源越来越显得力不从心。

要保证与因特网相连的网络的安全，需要使用防火墙。防火墙是指一个大系列的产品，用于在网络和因特网之间限制网络数据流，从而保护网络不受外部网络的威胁。建立防火墙的两种基本技术是包过滤和应用程序代理网关。如果理解了这两种技术的工作原理，那么就可以更好地为网络建立或购买防火墙产品。本书主要涉及这些方面，并且讲述了防火墙的其他重要特征，例如，日志、报警和认证等特征。

虽然现在很多厂家都销售称为“防火墙装置”的产品，但是还是需要时间仔细地做出购买的方案。如果不使用商业产品，而是从因特网上下载软件，例如TIS因特网防火墙，或者TCP Wrapper来构建防火墙，也可以建立更加安全的环境。

关于防火墙内容的书很少，而其中在过去几年内出版的又更少。一些书涉及防火墙的每一个可能的主题，还有一些只是讨论某一种特定的防火墙产品。本书将给读者介绍所有建立防火墙的重要概念，以及这些概念在一些产品（免费和商业产品）中的实现。

本书内容

本书的内容从易到难，从简单的介绍到复杂的主题，一一叙述。如果已经对一些主题很熟悉，可以跳过这些主题的章节。文中的交叉参考信息使得更容易找到其他信息，返回前面的章节以更全面理解概念。

第1章介绍防火墙的有关知识。很好地讨论了为什么需要防火墙，以及防火墙可以保护和不可以保护的安全类型。

第2章专门针对没有深刻把握TCP/IP以及提供网络服务工具的用户。如果对地址类型或者划分子网不熟悉，可以参考本章。

第3章讨论了在简单网络和更大的网络，例如连接了因特网的网络安全实现之间的差别。还讨论普通黑客使用的一些攻击方法，例如拒绝服务攻击和IP地址欺骗。

第4章讨论建立防火墙的不同体系结构。涉及DMZ（非军事区域）和双宿主机的作用，介绍包过滤以及应用程序代理技术。还介绍网络安全策略的选择以及怎样使用防火墙实现这些策略。

第5章讨论防火墙的早期类型。介绍监视路由器使用的技术，禁止不需要的数据流通过防火墙，从而不能进入网络内部。

第6章包含了当选择用于提供防火墙服务的计算机时，所需考虑的有关配置的重要问题。由于暴露于因特网之中，它们是网络中最脆弱的主机，所以，为了抵御入侵者，它们尤其需要配置得很好。

第7章分析了一种更新的技术。包过滤器可以允许或阻止网络和外部世界之间的IP包数据流，而代理服务器则不需要在客户和服务器之间有直接的IP流就能提供网络服务。

第8章介绍了在UNIX和Windows NT中常见的设置审计的方法。

第9章讨论加密技术。如果没有基本的密码学概念，那么需要阅读这一章。可以了解到私有密钥和公开密钥的区别以及二者更适合用在哪些场合。

第10章继续介绍了如何用加密技术在因特网上建立安全隧道连接。

第11章讲述在出于个人安全需要，例如传送已用数字签名签过的邮件时，如何迅速安装并使用PGP。对在UNIX和Windows NT下安装PGP都作了介绍。

第12章简要叙述了可以从因特网上下载的常用的工具，大多数情况下，可以免费使用它们构造防火墙。

第13章更为详细地介绍了如何安装和配置这些免费工具。在UNIX主机上使用TCP软件包有助于实现安全访问，并对诸如Telnet和FTP这样重要的网络服务提供日志功能。

第14章更详细地介绍了一个可以免费下载的产品。如果对UNIX系统管理不熟悉，那么要配置FWTK就比较困难，但这一章使读者以正确的方向起步，它介绍了重要的概念，并说明了配置文件是如何工作的。

第15章是关于SOCKS安全协议的。这种产品在Internet Explorer这样的商业产品中被广泛地实现。在许多库中也提供了这个协议，它们可以使现存的应用程序SOCK化（SOCKSify）。

第16章介绍了可从因特网上免费获得的有用工具。SQUID是一个可用于访问控制和管理网络带宽的缓冲代理服务器。它在本地缓存中存储频繁地对Web对象访问的事件。

第17章讨论了已被加入到Linux内核中的包过滤能力，以及如何使用ipfwadm和ipchains这两个工具来管理这些函数。

第18章讨论了如何在防火墙产品中安装Microsoft项目。还简要介绍了如何用服务器的图形用户接口来配置服务。

第19章讨论了另一个用于Windows NT服务器的商业产品。分析了防火墙和基本的配置问题。

第20章瞄准了新出现的一种防火墙产品，它尽可能地做到即插即用，并希望防火墙的配置过程对于端用户更为容易。

在第21章中，将会看到因特网安全性发展的一些可能性，例如新一代IP协议IPv6，还有关于保护商业网络，以及保护用于访问网络的主机的讨论。

附录A简要介绍了TCP和UDP端口，列出了常用端口和它们的用途。

附录B收集了可使网络上主机更安全的有用的工具，并告诉在哪里下载像SATAN和COPS这样的工具。

最后，附录C列出了可以跟踪因特网安全和防火墙技术的有用资源。由于因特网上的威胁在迅速变化，所以必须对于当前的威胁十分熟悉。

目　　录

第一部分　了解防火墙和因特网安全

第三部分　防火墙的安装与配置

此为试读，需要完整PDF请访问：www.ertongbook.com

第四部分　附　　录

第一部分
了解防火墙和因特网安全

第1章　防火墙基础知识

本章要点

- 为什么需要防火墙
- 使用站点的安全策略设计防火墙
- 防火墙技术
- 硬件防火墙还是软件防火墙？开发还是购买
- 防火墙能做什么
- 防火墙不能防范什么

1.1　为什么需要防火墙

当我们把公司的网络连接到因特网时，需要考虑许多事情，例如需要何种连接来提供足够的带宽以满足所希望的流量以及使用何种ISP。在任务书中的某处，将毋庸置疑地包括“需要防火墙”的字眼。重要的是要懂得不应该把这种特别字眼作为一般的任务，而应该作为任务书中的首要任务。当与因特网连接时，在自己的网络和现代网络世界之间安装一个防火墙是重要的任务之一。

1.1.1　什么是防火墙

5年前，在网络领域可能还没有人听过防火墙这个术语。在安全专家采用它来描述防止讨厌的入侵者闯进已连接到较大网络的网络之前，这一术语通常在建筑行业使用。例如，防火墙可能是共管大楼内各个单位之间的一个防火屏障。如果在某个单位突发火灾，防火墙有助于把火隔离开，阻止火蔓延到其他单位。实际上，防火墙有助于包容上面的问题。

防火墙用在网络中时也以上述方式运行：它有助于防止来自其他网络的问题进入局域网（LAN）并危及系统或数据。在局域网和因特网之间，防火墙仅允许某些信息流通过而阻止其他信息流。大楼里的防火墙通常是由水泥构件或其他坚固的防火材料构成的，而网络中防火墙的结构则更复杂。

用来允许或阻止信息流的机制可以是简单的包过滤，它基于包头的内容来抉择；或者可以是更复杂的应用代理，它位于客户和外部世界之间，作为一个中间人提供某些网络服务。

参见：什么是应用代理？可在第7章找到这种防火墙技术。

由于其名字的原因，人们容易认为防火墙是一个单一的设备或软件产品。然而，即使在最简单的情况下，也应把防火墙看作为一个系统。该系统基于网站的安全规则，在内部网络和外部网络之间实行访问控制。由于网络防火墙提供了类似大楼防火墙防止火灾蔓延的屏蔽功能，所以采用术语“防火墙”来描述内部网络和外部世界之间的那些组件。

防火墙厂商之间互相竞争，各厂商都努力使自己的产品比别人高出一筹，结果是给防火墙开发了许多新的功能。由于防火墙位于内部网络的周边，是到外部世界的一种关口，显然它要做许多与安全相关的事情，例如，现代防火墙可能包括下列新的功能：

- 高速缓存　对拥有 Web 服务器向因特网上用户提供大量内容服务的网络来说，这一点特别有用。高速缓存服务器通过存储频繁读取的局部数据来提高用户访问的响应时间并节省有用的因特网带宽，否则会因相同数据的重复存取而消耗这些带宽。
- 地址转换　一个配置好了的防火墙仅把自己的网络地址暴露给外部世界，使我们能在内部网中使用任意想要的 IP 地址空间。
- 内容限制　通过限制访问已知的包含讨厌内容的 URL，或通过对流入数据包进行关键字检查等方法，大量防火墙产品允许我们限制用户在因特网上存取某些信息。
- 地址导航　这一功能使防火墙可以修改请求，如 HTTP 请求，并用与请求包中不同的地址把它们发送到主机。这样当在因特网上出现单个主机对许多用户时，就可把负载分布到几个服务器上去。

这些特点虽然提供了许多安全方面的好处，但大多是用来解决性能问题的。例如，地址转换和导航可有助于对潜在的黑客隐藏内部网的IP地址空间，这是很明显的安全好处。潜在的黑客知道的信息越少，实现其目标就将越困难。这些特点还可以帮助管理员在多个机器之间实现性能平衡。使用地址转换就意味着不用获得很大的IP地址子网来覆盖网络上的每个工作站和服务器。

1.1.2　这是难解的麻烦

因特网是一个很迷人的、但并不一定很友好的地方。随着时间的推移，新标准和新技术会不断向前发展，这种情况可能会变得好一些。然而现实总是这样，随着因特网继续快速地增长，当我们探索到新的前沿时，又会出现许多技术和人的问题。在因特网上碰到的人并不都具有良好的意图，所以在把网络连接到因特网以后，需要同时考虑安全问题。

参见：关于因特网上新近发生的各种不同安全威胁问题的详细情况，见第 3 章。

你可能已经碰到许多问题，例如计算机病毒，当连上因特网后这些问题还将变得更为复杂。现在不是担心通过软盘拷贝感染病毒，而是担心通过 Email 的附件和下载的演示软件或共享软件带进病毒。不是担心职员用公司的 Email 系统去不断侵扰其他员工，而是要担心他（她）们使用可以漫游到世界任何地方的电子邮件达到同样的目的。如果在管理公司的工作站或服务器时，曾为阻止诸如滑稽的文本文件、色情文学或其他类似的讨厌材料而碰到过许多问题的话，那么在连接到因特网之前，请稍等！

1.2　使用站点的安全策略设计防火墙

在设计防火墙策略之前，要坐下来仔细考虑应防范什么和准备怎样做的问题。如果工作范围不只是非常小的公司，就应该有公司的安全策略。可用这些策略开始处理问题。在和用户（或他们的管理者）交谈以后，就可对什么服务能通过防火墙做出决定。

参见：在第4章可找到更多关于怎样创建安全策略的信息。
在第2章可得到更多关于应用TCP/IP的基本服务。

在考察了这些服务及其潜在的缺陷之后，就可决定在你的环境中需要哪些服务了。

1.2.1 应考虑的新的安全威胁

当连接到因特网时，如果未采取适当的防范措施，就面临着一个可能会时常受到困扰的全新的与安全相关的世界。过去仅仅考虑和处理那些由未受培训员工所造成的一些错误或由心怀不满的员工所撕开的一些安全缺口，而现在要担心的是那些潜在的世界范围内的黑客。

每隔几个月，我们可能会在晚间新闻中听到关于新病毒的故事，如特洛伊木马或已在因特网上引起严重危害的蠕虫病毒等。人们可能会想到那些黑客是世界上一群非常聪明的程序员，他（她）们为了开发十分恶毒的新程序，或闯进一个敏感数据站点而耗费几个月甚至几年时间来进行“黑”的尝试。然而，实际上这并不需要很深的专业知识。所听到的许多恐怖事件也并非如此，因为许多非常聪明的编程技巧只是利用了目前可用操作系统和应用软件中某些已知的安全漏洞和程序错误而已。

几年前，Dan Farmer 和 Wietse Venema 写了一篇题为“通过攻击来改善站点的安全”的文章。在该文中，作者通过一些例子让读者了解黑客是怎样利用普通系统例程和程序来得到网络和计算机上的信息的。文中还告诉读者某些程序，如已经开发并使用的Sendmail的特点。尽管文中提到的某些漏洞和程序错误已经通过补丁和更新得以解决，但读一读这篇文章，将让们我懂得，许多从未想过的事情已经发生了。当今正在使用的许多主要操作系统的初始开发及其使用都是基于单机或小网络的，其网络功能是后来附加和提升的，所以仍然留有许多不是专为今天互联网环境设计的特点。

从什么地方可找到这篇文章

这篇文章由Farmer和Venema撰写，题为“通过攻击来改善站点的安全”。可通过因特网上许多不同的网站下载得到。如果用作者姓名作为关键字搜索，将返回许多地址，由此可以找到拷贝。我们推荐在任何网络安全领域工作的人都阅读一下这篇文章。

1.2.2 决定将为用户提供哪些服务

当准备创建一个好的网络安全策略时，从哪里开始呢？首先要决定将为用户群提供何种可用的服务。正在建立因特网连接的事实指明有必要对用户群进行分类。这些需求到底是些什么？这些需求将带来哪些商业利益？在试图给用户提供其所需服务中又存在哪些风险？

公司需要连接到因特网时，通常源于如下的理由：

- Email　允许员工同厂商和用户保持联系。
- 远程访问　允许移动员工访问本地LAN资源。
- 研究　给技术人员同其他公司或协会的同事保持联系的能力。
- 客户支持　允许客户查看产品文档和其他资料，以减轻支持人员的工作负担。
- 厂商支持　允许客户访问供货商已经放在网上的支持文档资料。
- 市场展示　建立电子商务业务，允许公司在因特网上开拓其产品市场。

根据上面的应用，可对下面的各种服务进行部分或完全的组合，以满足用户的需求。

- FTP　研究人员使用FTP同其他网站交换数据文件。使用匿名FTP来允许客户访问文件或文档资料。
- Telnet　如果客户服务支持小组需要登录到客户的计算机进行问题诊断，用这个服务建立远程登录会话是很有帮助的。当在远程站点或出席远地会议时，可用Telnet来检查自己的网络。
- 万维网（WWW）　WWW服务器能让公司在因特网上进行市场展示。也可通过Web站点来更新产品信息或服务来吸引客户。
- Email　使用简单邮件传输协议（SMTP）可以在桌面和几乎世界任何地方之间传输电子邮件。Email还是公司员工和客户之间快速通信的便捷通道。考虑到今天邮资的代价，随着更多的消费者连接到因特网，在未来几年内大多数商务将开始通过 Email 传输票据。

参见：读者将在第 2 章中找到大量的服务列表。

这些基本的服务并不是在因特网上可用服务的全部列表。这里提及这些只是让你能开始考虑怎样去使用因特网。当提出对公司有利的服务列表时，需要考虑每个服务并问几个问题。有和这些服务需要的客户或服务器程序相关的安全制度吗？使用该服务的方式在LAN中可能会暴露安全漏洞吗？

参见：由于大多数服务都是基于TCP或UDP协议，并用不同的端口号区别它们的会话的，所以当考虑到底把哪种服务提供给用户时，请见附录 A 中熟知的端口表。

例如，安全策略可能允许用户建立可通过防火墙流出的Telnet会话，而又决不允许外边的Telnet会话流入。这就意味着允许用户和客户系统建立远程会话，而不允许外人登录到内部网络。还可为其他重要的网络服务，如FTP和SMTP建立类似的规则，这取决于具体的需要。安全策略同几乎任何一种规则一样，不论它是否贴近安全，总存在一些例外。

参见：在第 4 章中可得到更多关于安全策略帮助设计防火墙的信息。

1.2.3　防火墙策略

在审视所包含的安全问题后，就能设计一个防火墙策略。防火墙可以使用两种基本的方法实现安全策略：

- 允许任何访问，除非被规则特别拒绝。
- 拒绝任何访问，除非被规则特别允许。

我们应该采用上述第2个策略。这是因为从逻辑的观点看，更容易指定一个较小的列表使之允许通过防火墙访问，而不是指定一个较大的列表使之不允许通过防火墙访问。还有，随着因特网持续地增长，新的协议和服务将频繁地开发出来，我们将不得不继续加进新规则以阻挡随之而来的新问题。这样，在有时间审查新开发中的安全问题并决定是否允许那些新协议和服务通过防火墙之前，网络仍然是安全的。

参见：在第 4 章中可得到更多关于创建防火墙的信息。

此为试读，需要完整PDF请访问：www.ertongbook.com