

THOMSON

GUIDE TO
FIREWALLS AND NETWORK SECURITY
INTRUSION DETECTION AND VPNs

防火墙与网络安全
——入侵检测和 VPNs

(美) Greg Holden 著
王斌 孔璐 译



清华大学出版社

防火墙与网络安全

——入侵检测和 VPNs

(美) Greg Holden 著

王斌 孔璐 译

清华大学出版社

北 京

Greg Holden

Guide to Firewalls and Network Security: Intrusion Detection and VPNs

EISBN: 0-619-13039-3

Copyright © 2004 by Course Technology, a division of Thomson Learning.

Original language published by Thomson Learning (a division of Thomson Learning Asia Pte Ltd). All Rights reserved.

本书原版由汤姆森学习出版集团出版。版权所有，盗印必究。

Tsinghua University Press is authorized by Thomson Learning to publish and distribute exclusively this Simplified Chinese edition. This edition is authorized for sale in the People's Republic of China only (excluding Hong Kong, Macao SAR and Taiwan). Unauthorized export of this edition is a violation of the Copyright Act. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

本中文简体字翻译版由汤姆森学习出版集团授权清华大学出版社独家出版发行。此版本仅限在中华人民共和国境内(不包括中国香港、澳门特别行政区及中国台湾地区)销售。未经授权的本书出口将被视为违反版权法的行为。未经出版者预先书面许可，不得以任何方式复制或发行本书的任何部分。

981-254-540-9

北京市版权局著作权合同登记号 图字：01-2003-3438

本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

图书在版编目(CIP)数据

防火墙与网络安全——入侵检测和 VPNs/(美)侯登(Holden, G.)著；王斌，孔璐译.—北京：清华大学出版社，2004
书名原文：Guide to Firewalls and Network Security: Intrusion Detection and VPNs

ISBN 7-302-08572-2

I. 防… II. ①侯…②王…③孔… III. 计算机网络—防火墙 IV. TP393.08

中国版本图书馆 CIP 数据核字(2004)和 039175 号

出版者：清华大学出版社 地 址：北京清华大学学研大厦
http://www.tup.com.cn 邮 编：100084
社总机：010-62770175 客户服务：010-62776969

组稿编辑：曹康

文稿编辑：李阳

封面设计：康博

版式设计：康博

印刷者：北京昌平环球印刷厂

装订者：北京市密云县京文制本装订厂

发行者：新华书店总店北京发行所

开 本：185×260 印张：20.5 字数：524 千字

版 次：2004 年 6 月第 1 版 2004 年 6 月第 1 次印刷

书 号：ISBN 7-302-08572-2/TP·6149

印 数：1~4000

定 价：40.00 元

本书如存在文字不清、漏印以及缺页、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)62770175-3103 或(010)62795704。

前 言

本书旨在介绍防火墙和其他网络安全组件，将它们组合起来可以创建 LAN 周围的深层防御边界。如今，防火墙是使用得最为广泛的安全工具，它们在一般用户及信息技术专家中正日益普及。然而，如果获得安全策略的支持，并能与反病毒软件、入侵检测系统和其他工具结合起来使用，防火墙的作用将得到最大程度的发挥。

同时，本书还将防火墙与有效的边界安全及网络安全性所需要的其他因素结合起来讨论。这些因素包括包过滤、身份验证、代理服务器、加密、堡垒主机、虚拟专用网络(VPN)、日志文件维护和入侵检测系统等。

本书主要内容

让读者无需从头至尾按顺序阅读本书。然而，前三章对防火墙及其适合于网络安全程序之处作了全面介绍，因此强烈建议您从这三章开始阅读。其内容如下所示：

第 1 章“防火墙规划和设计”概述了各种不同的防火墙和它们的主要功能，这样您可选择满足需要的合适的防火墙。

第 2 章“开发安全策略”帮助您协调防火墙目标和组织的整体安全策略的目标。您还会学到如何一步一步地与管理部门一起工作，确保安全策略奏效。

第 3 章“防火墙配置策略”介绍了将一个或多个防火墙定位到网络边界，并协调它们与其他组件(如 DMZ、路由器和 VPN)一起工作的不同方法。

接下来的一些章节讨论了对于防火墙和网络安全来说比较重要的特定主题。您会发现这几章对您有最直接的意义，而不是流于形式。第 4 章“数据包过滤”讨论了最初始的，有时也是最基本的防火墙活动，介绍了无状态和有状态的包过滤，以及如何针对通用的协议(例如 ICMP、TCP 和 UDP)建立规则集。第 5 章“代理服务器和应用级防火墙”讨论了代理服务器如何代表网络上的单台主机工作，以对它们提供保护。第 6 章“用户身份验证”描述了防火墙进行身份验证的原因，它们如何通过用户、客户端和会话验证，以及集中式身份验证和一次性口令系统来确认经过授权的个体。第 7 章“加密和防火墙”重点是防火墙体系结构中的角色加密和为网络建立 PKI。第 8 章“选择堡垒主机”解释了如何保护运行有防火墙、入侵检测软件或是在 DMZ 上提供公共服务的主机的安全。

本书的最后三章深入讨论了一些高级主题，重点考虑了流行的防火墙和 VPN 选项。第 9 章“创建虚拟专用网”讨论了 VPN 的建立，它为公司提供了在公共 Internet 进行安全通信的经济可行的方法。因为 VPN 使用加密和身份验证，在阅读本章之前先阅读第 6 章和第 7 章将很有好处。第 10 章“建立自己的防火墙”向您讲述了两类防火墙，解释了桌面防火墙和企业防火墙

如何工作。第 11 章“防火墙管理”讨论了在管理防火墙时需要定期执行的不同维护任务，包括日志文件轮循和检查。本章还深入介绍了反病毒软件和入侵检测系统与防火墙的整合。

读者还将被指导查看一些在线资源以及本书提到的一些印刷品。

本书特色

为了帮助您全面了解网络概念，本书提供了许多有特色的内容，以便提升其教学价值。

- **本章学习目标：**本书每章的开头都列出了本章中应掌握的一些概念。这一列表可以使您很快地了解到该章的主要内容，可以对学习起到帮助作用。
- **示意图表和截图：**大量的网络配置图解可以帮助您直观地了解防火墙的常规设置和体系结构。另外，大量的列表用理论和实际的数据提供了详细的内容和比较。有些表提供了用于构建防火墙规则集的包过滤规则的具体示例。因为大部分学校实验室使用 Microsoft 操作系统，所以本书的图及实用项目都采用 Microsoft 操作系统的产品。
- **本章小结：**每章的最后都会对这章的内容作个总结。这些小结为重述和回顾每章所讲的内容提供了有用的参考。
- **关键术语：**在本章小结后面，列出了一些新的网络术语和它们的定义，这可以帮助正确理解每章的主要概念，并提供有用的参考。
- **复习题：**每章后面都提供了一组复习题，以巩固每章中的学习要点。这些问题可确保您真正掌握这些概念。
- **实用项目：**尽管理解网络技术背后的原理很重要，但只有通过实践才能得到提高。除了纯理论的东西外，每章还提供了一系列用于给学生们提供实践经验的练习。
- **案例项目：**最后，每章结尾都提供一些特定的与防火墙和与安全相关的建议方案。您被要求评估这些情况，决定该采取的行动来弥补所描述的问题。该部分内容将帮助您提高迅速作出决定和除错的技能——这种技能是防火墙和安全系统管理的一个重要方面。

附录和术语表

除了这些外，本书还包括下列内容：

- **附录 A：安全性资源：**附录提供了一些可在线找到的与安全相关的最新信息的站点。您可以获得一些知名站点提供的信息，关于网络安全及病毒警告的背景知识，并可以测试已有网络配置的端口扫描器，以及可帮助您找到用于网络安全领域的证书的地方。
- **术语表：**这是本书中使用的所有缩略词和技术术语的总目录，包括其定义。

顺应 Web 的改变

总有一天，本书附录提到的所有基于 Web 的资源都会过时，或是被更新的资源所淘汰。在有些情况下，您从本书所了解到的 URL 将把您带到它们的替代品那儿，而另外的情况则是，显

示令人讨厌的 404 错误消息：“File not found。”

如果发生这种情况，请不要放弃！如果您愿意花些时间和精力，通常通过 Web 都可以找到您想要的信息。而许多大型、综合性的 Web 站点都提供了搜索引擎。只要访问这些站点，您就可以使用这一工具帮助您找到所需的。

不要对使用 <http://www.google.com>、<http://www.hotbot.com> 或 <http://www.excite.com> 这样的搜索工具来搜索相关信息感到害怕。一些标准组织可能在线提供了有关他们的标准的、最准确的特定信息，此外还存在大量第三方的关于在这一领域的练习和帮助。如果无法找到书中所指示的内容，可以去别处找找。

Web 资源

可从网络上找到特别为本书设计的一些附加资源。请访问 www.course.com，定期搜索本书主题，可获得详细的内容。

阅读准备

本书包括了 70 多个实用项目，其中大部分都要求您安装和使用不同的与安全性相关的软件。您需要一台与 Internet 相连的计算机，在该计算机上应可以运行这些程序。推荐使用的硬件如下所示。

● 硬件要求

计算机的 CPU 必须至少为奔腾 II，运行速度为 300MHz 或更快。要能够同时运行 Web 浏览器、字处理程序以及其他程序，至少需要 192MB 的 RAM(理想的大小是 256MB 或是更高)和最少 75MB 的可用磁盘空间。

● 软件要求

本书中的大部分项目可使用运行 Windows 2000/XP 或 Red Hat Linux 7.3 或更高版本的计算机完成。

实用项目中使用的大部分程序要求您下载和安装相关软件。至少，您的计算机需要安装 Web 浏览器和压缩程序 WinZip(可从 www.winzip.com 中获得)。还需要一个字处理程序或文本编辑器，用以记录从实用项目中获得的结果。在有些项目中，还需要用到电子邮件程序，例如 Outlook Express 或 Netscape Messenger。

● 特殊要求

在本书中，您将找到一些关于 Check Point NG 的参考。如果您有此软件，您的系统将需要至少 128MB 的 RAM 来运行它。注意，Check Point NG 运行于 Windows 2000 上；如果在 Windows XP 上运行，其功能将受到限制。

各章需要的可免费下载软件如下：

第 3 章：Syagte 个人防火墙，www.sygate.com

第 4 章：Tiny 个人防火墙，www.tinysoftware.com

第 5 章: NetProxy, www.grok.co.uk; SOCKS, www.socks.nec.com

第 7 章: PGP(Pretty Good Privacy), <http://web.mit.edu/network/pgp.html>

第 8 章: NetScan Tool 4, www.netscantools.com; IP Sentry, www.ipsentry.com

第 9 章: Symantec Enterprise Virtual Private Network 7.0, www.symantec.com/downloads

第 10 章: ZoneAlarm Pro, www.zonelabs.com

注意:

在第 10 章, 您将学习到 Linksys(www.linksys.com), 它提供了大量路由器、集线器、无线接入点、防火墙和其他硬件。该章中关于 Linksys 产品的引用和描述已经过 Linksys 允许。

目 录

第 1 章 防火墙规划与设计	1
1.1 关于防火墙的误解.....	1
1.2 什么是安全策略.....	2
1.3 什么是防火墙.....	3
1.3.1 类比：安全警卫 Sam.....	3
1.3.2 防火墙提供安全性.....	4
1.3.3 防火墙为个人用户提供保护.....	4
1.3.4 防火墙为网络边界提供安全.....	4
1.3.5 防火墙由多个组件组成.....	6
1.3.6 防火墙面临诸多威胁并且执行各种安全防护任务.....	6
1.4 防火墙保护的类型.....	11
1.4.1 多层防火墙保护.....	11
1.4.2 包过滤器.....	11
1.4.3 NAT.....	14
1.4.4 应用层网关.....	15
1.5 防火墙的局限.....	16
1.6 评估防火墙设备.....	16
1.6.1 防火墙硬件.....	17
1.6.2 纯软件的防火墙组件.....	17
1.7 本章小结.....	19
1.8 关键术语.....	20
1.9 复习题.....	22
1.10 实用项目.....	24
1.11 案例项目.....	27
第 2 章 开发安全策略	28
2.1 什么是安全策略.....	28
2.2 安全策略的重要性.....	29
2.3 确定有效的安全策略所需达到的目标.....	30
2.4 构建安全策略的 7 个步骤.....	30
2.4.1 组建一个工作团队.....	30
2.4.2 制定公司的整体安全策略.....	31
2.4.3 确定被保护的资产.....	32

2.4.4	决定安全策略审核的内容	33
2.4.5	确定安全风险	35
2.4.6	定义可接受的使用策略	35
2.4.7	提供远程访问	35
2.5	考虑防火墙的不足	36
2.6	其他的安全策略主题	37
2.7	定义针对违反安全规则的响应	37
2.8	克服管理的障碍	38
2.8.1	雇员的培训	38
2.8.2	呈交并回顾制定过程	39
2.8.3	改进安全策略	39
2.9	本章小结	39
2.10	关键术语	40
2.11	复习题	40
2.12	实用项目	42
2.13	案例项目	45
第 3 章	防火墙配置策略	47
3.1	对防火墙建立规则和约束	47
3.1.1	规则的作用	48
3.1.2	限制性的防火墙	48
3.1.3	侧重连通性的防火墙	49
3.2	防火墙配置策略：总的观点	49
3.2.1	可伸缩性	50
3.2.2	生产效率	50
3.2.3	处理 IP 地址问题	51
3.3	不同的防火墙配置策略	51
3.3.1	屏蔽路由器	52
3.3.2	双宿主主机	54
3.3.3	屏蔽式主机	54
3.3.4	两个路由器共用一个防火墙	55
3.3.5	DMZ 屏蔽子网	56
3.3.6	多重防火墙 DMZ	58
3.3.7	反向防火墙	63
3.3.8	专用防火墙	63
3.4	为防火墙添加新功能的方法	63
3.4.1	NAT	63
3.4.2	加密	64

3.4.3	应用程序代理	65
3.4.4	VPN	66
3.4.5	入侵检测系统(IDS)	66
3.5	本章小结	68
3.6	关键术语	69
3.7	复习题	70
3.8	实用项目	72
3.9	案例项目	75
第 4 章	数据包过滤	77
4.1	理解数据包和数据包过滤	77
4.1.1	执行数据包过滤的装置	78
4.1.2	数据包的剖析	78
4.1.3	关于数据包过滤的快速指南	80
4.1.4	规则的使用	80
4.2	数据包过滤的方法	82
4.2.1	无状态数据包过滤	82
4.2.2	有状态数据包过滤	87
4.2.3	根据数据包内容过滤	89
4.3	设立专用的数据包过滤器规则	89
4.3.1	适应多种变化的数据包过滤器规则	89
4.3.2	适用于 ICMP 的数据包过滤器规则	90
4.3.3	阻断 ping 包的数据包过滤器规则	90
4.3.4	启用 Web 访问的数据包过滤器规则	91
4.3.5	启用 DNS 的数据包过滤器规则	92
4.3.6	启用 FTP 的数据包过滤器规则	92
4.3.7	使用电子邮件的数据包过滤器规则	93
4.4	本章小结	93
4.5	关键术语	94
4.6	复习题	95
4.7	实用项目	97
4.8	案例项目	100
第 5 章	代理服务器和应用级防火墙	102
5.1	代理服务器概述	102
5.1.1	“代理服务器”的比喻说明	102
5.1.2	代理服务器是如何工作的	103
5.1.3	代理服务器和数据包过滤器的不同	104
5.1.4	代理服务器配置示例	104

5.2	代理服务器的目标	106
5.2.1	隐藏内部客户机的身份	106
5.2.2	阻断 URL	107
5.2.3	阻断和过滤内容	107
5.2.4	电子邮件的代理保护	108
5.2.5	提高性能	109
5.2.6	保障安全	109
5.2.7	提供用户身份验证	110
5.2.8	重定向 URL	110
5.3	代理服务器配置的注意事项	110
5.3.1	提供可伸缩性	110
5.3.2	客户端配置	111
5.3.3	服务配置	112
5.3.4	创建过滤规则	113
5.3.5	确认单个故障点	113
5.3.6	确认缓冲区溢出弱点	113
5.4	选择代理服务器	113
5.4.1	透明代理	114
5.4.2	非透明代理	114
5.4.3	基于 SOCKS 的代理	114
5.5	基于代理服务器的防火墙的比较	115
5.5.1	开放源代码的 T.REX 防火墙	116
5.5.2	Squid	116
5.5.3	WinGate	116
5.5.4	Symantec 企业防火墙	117
5.5.5	ISA	117
5.6	反向代理	117
5.7	代理服务器何时不适用	119
5.8	本章小结	119
5.9	关键术语	120
5.10	复习题	121
5.11	实用项目	123
5.12	案例项目	128
第 6 章	用户身份验证	130
6.1	常规身份验证过程	130
6.2	防火墙实现身份验证过程的方式	131
6.3	防火墙身份验证的类型	132

6.3.1	用户身份验证	132
6.3.2	客户端身份验证	133
6.3.3	会话身份验证	134
6.4	集中式身份验证	135
6.4.1	Kerberos 身份验证	135
6.4.2	TACACS+	137
6.4.3	远程身份验证拨号用户服务(RADIUS)	137
6.4.4	TACACS+和 RADIUS 的比较	137
6.5	口令安全性问题	139
6.5.1	可能被破解的口令	139
6.5.2	用户使用口令的误区	139
6.5.3	马虎的安全习惯	139
6.6	口令安全工具	140
6.6.1	一次性口令软件	140
6.6.2	屏蔽口令系统	140
6.7	其他的身份验证系统	140
6.7.1	单口令系统	141
6.7.2	一次性口令系统	141
6.7.3	基于证书的身份验证	142
6.7.4	802.1x Wi-Fi 身份验证	142
6.8	本章小结	143
6.9	关键术语	143
6.10	复习题	145
6.11	实用项目	146
6.12	案例项目	152
第 7 章	加密和防火墙	153
7.1	为何防火墙需要使用加密技术	153
7.1.1	黑客们对未加密防火墙的利用	154
7.1.2	加密的代价	154
7.1.3	保证数据完整性	155
7.1.4	维持机密性	155
7.1.5	对网络客户端进行身份验证	155
7.1.6	启用 VPN	156
7.2	数字证书、公钥和私钥	156
7.2.1	数字证书	156
7.2.2	密钥	158
7.3	分析流行的加密方案	162

7.3.1	对称加密和非对称加密	163
7.3.2	PGP	164
7.3.3	X.509	165
7.3.4	X.509 和 PGP 的比较	165
7.3.5	SSL	166
7.4	使用 IPSec 加密	167
7.4.1	理解 IPSec	167
7.4.2	IPSec 的模式	167
7.4.3	IPSec 协议	168
7.4.4	IPSec 组件	169
7.4.5	启用 IPSec	170
7.4.6	IPSec 的局限	171
7.5	本章小结	171
7.6	关键术语	172
7.7	复习题	174
7.8	实用项目	175
7.9	案例项目	181
第 8 章	选择堡垒主机	183
8.1	安装堡垒主机：常规需求	183
8.2	选择主机计算机	184
8.2.1	是否需要多台主机	184
8.2.2	内存考虑	185
8.2.3	处理器速度	185
8.2.4	选择操作系统	186
8.3	放置堡垒主机	187
8.3.1	物理位置	187
8.3.2	网络位置	188
8.3.3	保证主机本身的安全性	189
8.4	配置堡垒主机	191
8.4.1	让主机自行防卫	191
8.4.2	选择要提供的服务	192
8.4.3	有关 UNIX 系统的考虑事项	192
8.4.4	有关 Windows 系统的考虑事项	193
8.4.5	禁用账户	193
8.4.6	禁用不需要的服务	194
8.4.7	限制端口	195
8.5	进行备份	196

8.6	对堡垒主机进行审核	196
8.7	连接堡垒主机	196
8.8	本章小结	197
8.9	关键术语	198
8.10	复习题	199
8.11	实用项目	200
8.12	案例项目	207
第 9 章	创建虚拟专用网	208
9.1	VPN 的组件和操作	208
9.1.1	VPN 内部组件	209
9.1.2	VPN 的核心活动	211
9.1.3	VPN 的优点和缺点	213
9.1.4	VPN 扩展了网络边界	213
9.2	VPN 的类型	214
9.2.1	VPN 器件	214
9.2.2	软件 VPN 系统	215
9.2.3	组合了硬件和软件的 VPN	216
9.2.4	结合使用不同供应商产品的 VPN	217
9.3	VPN 设置	217
9.3.1	mesh 配置	217
9.3.2	hub-and-spoke 配置	218
9.3.3	混合配置	219
9.3.4	配置和企业内外网的访问	219
9.4	VPN 使用的隧道协议	220
9.4.1	IPSec/IKE	220
9.4.2	PPTP	221
9.4.3	L2TP	221
9.4.4	工作在 SSL/PPP 和 SSH 上的 PPP	221
9.5	在 VPN 内启用远程接入连接	222
9.5.1	配置服务器	222
9.5.2	配置客户端	224
9.6	使用 VPN 的良好习惯	224
9.6.1	采用 VPN 策略的必要性	224
9.6.2	VPN 和包过滤	224
9.6.3	PPTP 过滤器	226
9.6.4	L2TP 和 IPSec 包过滤规则	226
9.6.5	对 VPN 进行审核和测试	227

9.7	本章小结	228
9.8	关键术语	229
9.9	复习题	230
9.10	实用项目	232
9.11	案例项目	238
第 10 章	建立自己的防火墙	240
10.1	企业防火墙和桌面防火墙	240
10.2	桌面防火墙	242
10.2.1	Tiny Personal Firewall	242
10.2.2	Sygate Firewalls	246
10.2.3	ZoneAlarm 防火墙	249
10.3	企业防火墙	253
10.3.1	Linksys	253
10.3.2	Microsoft 的 Internet Security and Acceleration Server 2000	254
10.4	本章小结	256
10.5	关键术语	257
10.6	复习题	258
10.7	实用项目	260
10.8	案例项目	267
第 11 章	防火墙管理	269
11.1	使防火墙满足新的需求	269
11.1.1	确定防火墙需要的资源	270
11.1.2	识别新的危险	271
11.1.3	增加软件升级和补丁	271
11.1.4	添加硬件	273
11.1.5	处理网络的复杂性	273
11.2	遵守一些已证明行之有效的安全规则	274
11.2.1	环境管理	274
11.2.2	BOIS、启动和屏保锁	275
11.3	使用远程管理接口	276
11.3.1	为什么远程管理工具很重要	276
11.3.2	远程管理工具的安全性事项	276
11.3.3	远程管理工具的基本特征	277
11.4	追踪日志文件的内容	277
11.4.1	准备使用报告	277
11.4.2	监视可疑事件	278
11.4.3	自动化安全检查	280

11.5 安全漏洞总是会发生	281
11.5.1 使用入侵检测系统(IDS)	281
11.5.2 接受安全报警	282
11.5.3 发生入侵时	282
11.5.4 入侵发生过程中和之后的应对	283
11.6 配置高级防火墙功能	283
11.6.1 数据缓存	283
11.6.2 热备用冗余系统	284
11.6.3 负载均衡	285
11.6.4 过滤内容	286
11.7 本章小结	287
11.8 关键术语	288
11.9 复习题	289
11.10 实用项目	291
11.11 案例项目	294
附录 A 安全资源	296
A.1 与安全性相关的网站	296
A.2 反病毒站点	297
A.3 免费在线安全性扫描网站	297
A.4 事故响应站点	298
A.5 安全证书站点	298
A.6 安全专题的背景信息	299
A.7 时事通讯、新闻组和邮件列表	299
术语表	301

第1章 防火墙规划与设计

本章学习目标：

- 了解关于防火墙的一些误解
- 认识到防火墙基于一个有效的安全策略
- 理解防火墙的作用
- 描述防火墙提供的各种类型的保护
- 了解防火墙的各种限制
- 确定对防火墙硬件和软件的最优化配置

网络安全性由一系列不断发展的技术组成，特别应用在与通信或者商务服务的 Internet 相连接的网络中。网络安全性中近来最重要的一个发展就是，防火墙已作为了一个重要角色。由于黑客与恐怖分子的公开攻击、病毒和其他入侵软件的蔓延，防火墙已经成为一个基本的安全工具。防火墙现在实质上已不是每个网络以及许多个人计算机可有可无的部分，而是必需的产口。

没有一个安全系统能绝对保证它的信息一直都受到了保护。但是由于防火墙与安全策略配合使用，根据其保护的业务的需求进行开发，经常进行维护和升级，所以它是网络管理员可以部署的最有效的安全工具之一。

本章向您提供了在规划和设计防火墙方面所涉及诸多问题的大致介绍。首先，介绍一些关于防火墙的错误理解——“防火墙 101”，以便于您一开始就可以对防火墙的概念有一个更加清晰的认识。接下来学习用以控制防火墙工作的一些安全策略、标准以及程序。然后学习防火墙保护的类型、防火墙的限制以及如何利用硬件创建防火墙。本章最后对防火墙软件包进行了评价。

注意：

在本书中，“防火墙”这一术语并不一定表示防火墙只是一个路由器、计算机、VPN 网关或者软件程序。任何单独的防火墙程序实际上是由若干软件和硬件组件组合而成的。

在本章中，我们假定您对 TCP/IP 和网络基础设施的有基础的了解。同时假定您了解 IP 地址和域系统等内容，并熟悉 Internet 和基于 Web 的软件。如果在阅读完本章后，您对 TCP/IP 或网络基础设施其他方面的基础知识有些不解的话，可以通过访问 www.course.com 来提高您的技能。

1.1 关于防火墙的误解

许多人都曾听说过“防火墙”这个术语，但是并没有把它与 Internet 联系起来。他们可能曾经听过他们的汽车技工提到过在汽车内部和发动机之间存在着一道防火屏障，或许将之理解成