que®

个人防火墙

〔美〕Jerry Lee Ford 著
段云所 王昭 唐礼勇 陈钟 译

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

个人防火墙

[美] Jerry Lee Ford 著

段云所 王昭 唐礼勇 陈钟 译

人民邮电出版社

图书在版编目（CIP）数据

个人防火墙 /（美）福德（Ford,J.L.）著；段云所等译. —北京：人民邮电出版社，2002.8

ISBN 7-115-10408-5

Ⅰ. 个… Ⅱ. ①福…②段… Ⅲ. 计算机网络－安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2002）第 046840 号

个人防火墙

◆ 著 [美] Jerry Lee Ford

译 段云所 王昭 唐礼勇 陈钟

责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子函件 315@ptpress.com.cn

网址 http://www. ptpress.com.cn

读者热线 010-67180876

北京汉魂图文设计有限公司制作

北京顺义向阳胶印厂印刷

新华书店总店北京发行所经销

◆ 开本：787×1092 1/16

印张：13.75

字数：324 千字 2002 年 8 月第 1 版

印数：1-4 000 册 2002 年 8 月北京第 1 次印刷

著作权合同登记 图字：01－2001－4078 号

ISBN 7-115-10408-5/TP・2949

定价：25.00 元

本书如有印装质量问题，请与本社联系 电话：(010)67129223

内容提要

个人防火墙是保护个人计算机接入公共网络（如因特网）的安全有效措施。本书分析了个人和家庭上网面临的安全威胁和风险、Windows 网络的漏洞和问题，并以个人防火墙为安全对策，介绍了个人防火墙的用途、结构、安装和使用等知识，特别给出了几个流行的个人防火墙的具体应用实例，如 McAfee、BlackICE、ZoneAlarm 等。

本书适合于关心个人计算机连网安全的所有读者，通过阅读本书，可以对计算机连网的安全问题和解决措施有良好的了解。本书对网络安全专业人员也有很好的参考价值，可以帮助他们提高对个人防火墙技术和产品的认识。

前　言

你需要这本书吗

个人计算机第一次出现不是很多年前的事，个人计算机的好处和局限是明显的，因为每一台计算机对自己而言是一个孤岛。过去的若干年来，大量的努力倾注于计算机系统互联。从第一个局域网出现，我们进入了因特网时代，世界上成百上千万台计算机共享大量的开放的网络资源和信息。

互连不再是主要的问题。新的焦点是连接的速度有多快。这导致了 56K 调制解调器的出现，以及 Cable 和 DSL 连接。因为 Cable 和 DSL 连接总是在线，没有等待，访问是即时的。然而，所有这些令人惊奇的互连性存在一个缺点——安全。

所有用于用户访问 Internet 信息的工具和资源同样可用于对他们进行攻击。黑客是成长起来的一类入侵计算机系统的个体。

大多数人在个人计算机上保存了很多有价值的信息，例如个人财务记录、电子日记等，他们不想与别人共享这些信息。然而，许多人没有意识到当他们的个人计算机连接到 Internet 时，Internet 也连接到他们的计算机，有一点诀窍的人都可侵入并浏览。

为了对抗这一暴露，你需要竖立一个屏障阻止未经许可的访问者，而不会约束你在 Internet 上冲浪的能力。这就是个人防火墙的作用。在这本书里，你将会知道，当你连接到 Internet 时碰到的安全风险，如何使用防火墙防备外部威胁，你将会学到个人防火墙如何工作、如何安装以及他们如何保护你的计算机。不管你建立一个拨号连接或高速 Cable、DSL 的 Internet 连接，你会发现本书将会帮助你更加安全的冲浪。

开始阅读之前需要的条件

为了有效地使用这本书，你所需要的是一台个人计算机，到 Internet 的连接和一个个人防火墙。你的 Internet 连接可以是拨号连接、Cable modem 或 DSL 连接。如果你不知道使用何种个人防火墙，首先读这本书，它会帮你做决定。这本书覆盖了若干个人防火墙，包括基于软件的和基于硬件的。你将会了解软件和硬件防火墙的优缺点，怎样选择一款适合你的防火墙。你还会得到下载一些比较好用的免费防火墙的地址信息。

本书的组织

本书共分 11 章和 2 个附录。第 1～4 章给出了本书其余部分需要的基础知识，其余的章节讲述了一些特定的题目。

第 1 章介绍了高速 Internet 接入，以及使用个人防火墙保护个人计算机的需要。另外还介绍了一些黑客和黑客组织。

第 2 章介绍了关于 Cable 或 DSL 连接的附加信息，解释了如何建立和配置你的 Cable 或 DSL 连接以获得最大性能。这一章同样解释了高速连接为什么更不安全，你为什么需要用个人防火墙保护它们。

第 3 章覆盖了硬件和软件个人防火墙的差别，个人防火墙如何操作的额外的介绍。本章还回顾了 TCP/IP 和基本的网络通信。

第 4 章揭露了微软网络的漏洞，讨论了如何锁住它们的方式，除此而外，本章还讨论了升级到一个更安全的 Windows 版本的好处。

第 5 章介绍了 Cable 或 DSL 路由器，解释了它们如何用作个人防火墙。这一章告诉你如何安装和配置这些设备，内容包括 IP 地址拦截和回顾防火墙日志。

第 6 章告诉你如何安装、配置和使用 McAfee 个人防火墙。你将会了解如何配置可信的应用和网络安全设置。本章对这一防火墙的每一个主要特征进行了介绍，包括如何管理报警和日志文件。

第 7 章全面介绍了 BlackICE Defender 防火墙，你将会了解如何安装和配置它，以及如何建立安全配置。本章对这一防火墙的每一个主要特征进行了介绍，包括如何分析安全事件和收集攻击者的信息。

第 8 章全面介绍了 ZoneAlarm 防火墙，告诉你如何安装和配置它，解释了每一个主要的应用特征。你将会学到如何使用 ZoneAlarm 进行安全设置和配置可信应用，你还会了解到如何分析 ZoneAlarm 的日志文件和激活它的自动更新特征。

第 9 章告诉你如何对你的家庭计算机进行免费的 Internet 安全扫描，这样你可以对个人防火墙的有效性进行测试。本章给出了典型扫描的结果，帮助你分析这些结果。

第 10 章提供了一些连接到 Internet 时，如何使你的计算机更安全的措施。此外，你还可以得到好的冲浪习惯和使你的计算机和应用更新的建议。

第 11 章告诉你如何建立家庭网络和如何使用硬件和软件个人防火墙的组合使其更

安全。这一章提供了使家庭网络更安全的一些选择，解释了这些选择之间的一些差别。

附录 A 介绍了一系列附加的防火墙产品，提供了对每一个产品的简单评价。

附录 B 补充了第 9 章的材料，提供了一些可以免费测试你的计算机安全的 Web 站点。

术语表提供了一些你阅读本书可以参考的名词和定义的列表。

如何使用这本书

本书的设计是一章一章进行阅读，然而，根据你的经验和兴趣，你会发现你只需要阅读确定的部分。第 1～4 章提供了阅读本书其余部分的基础，第 5～8 章覆盖了特定的个人防火墙产品，你可能至少需要阅读其中一章。如果你想使你的安全最大化，你最好阅读第 5 章，然后，选择介绍软件防火墙的三章之一。

第 9 章介绍如何运行一个网络扫描来测试防火墙的安全强度，是要阅读的基本内容。第 10 章提供了如何使你的计算机安全的建议，也很有用。如果你有一个家庭网络，第 11 章是很基本的，否则，可以跳过去，最后，附录给出了各章内容的补充。

目　录

第 1 部分　个人防火墙简介 ····· 1

第 1 章　为什么需要个人防火墙 ····· 2

1.1　高速因特网访问的新时代 ····· 3
1.1.1　传统的 56K 因特网访问 ····· 3
1.1.2　高速因特网访问的新纪元 ····· 3
1.2　使用个人防火墙保护你的计算机 ····· 4
1.3　典型的因特网连接 ····· 6
1.4　究竟谁是黑客 ····· 8
1.4.1　黑客组织 ····· 9
1.4.2　黑客从何处获取工具 ····· 11
1.5　他们希望从你那儿得到什么 ····· 12

第 2 章　高速 Internet 连接日益增长的脆弱性 ····· 14

2.1　选择高速连接：Cable 与 DSL ····· 15
2.1.1　高速 Cable Internet 访问 ····· 15
2.1.2　高速 DSL Internet 访问 ····· 16
2.2　Cable Modem 与 DSL Modem ····· 17
2.3　建立 Cable 或 DSL 连接 ····· 19
2.4　安装前的任务 ····· 20
2.4.1　更新操作系统 ····· 20
2.4.2　加速 Internet 访问 ····· 20

2.5 安装网卡……23
2.6 安装软件驱动程序……23
2.6.1 网络配置……24
2.6.2 安装高速 Modem……24

第 3 章 防火墙释义……29

3.1 理解个人防火墙……30
3.1.1 在个人防火墙中寻找什么……30
3.1.2 硬件防火墙……30
3.1.3 软件防火墙……33
3.1.4 典型的软件防火墙的要求……34
3.2 网络概述……34
3.2.1 数据如何在网络计算机间传送……35
3.2.2 理解计算机如何进行通信……36
3.2.3 ISP 如何使用 MAC 地址……36
3.2.4 TCP/IP……37
3.2.5 TCP/IP 端口……37
3.3 理解防火墙如何进行操作……39
3.4 防火墙的功能……39
3.4.1 入侵检测……40
3.4.2 检测扫描计算机的企图……40
3.4.3 防范特洛伊木马……41
3.4.4 检查所有的网络数据流……42
3.5 防火墙分类……42
3.5.1 应用网关防火墙……42
3.5.2 包过滤防火墙……43
3.5.3 电路级防火墙……43
3.5.4 状态检查防火墙……43

第 2 部分 安全管理……45

第 4 章 锁定 Windows 网络……46

4.1 关于 Microsoft 网络……47
4.1.1 Microsoft 网络简介……47
4.1.2 Microsoft 网络是如何实现的……48
4.1.3 可信的 Microsoft 网络……48
4.1.4 关掉你的 NetBIOS 端口……52

4.1.5　保护打印机和磁盘驱动器不受来自 Internet 的入侵……53
4.1.6　配置家庭网络通信……54
4.2　增强安全性……57
4.2.1　设置用户名和口令……57
4.2.2　NTFS 的安全性……57
4.2.3　加密你的文件……59
4.3　为什么仍然需要个人防火墙……61

第 5 章　硬件防火墙……63

5.1　硬件防火墙……64
5.2　BEFSR41 快速以太网 Cable/DSL 路由器……64
5.3　安装硬件防火墙……65
5.4　通过 Web 浏览器进行配置……68
5.4.1　基本配置……68
5.4.2　更改口令……70
5.4.3　查看路由器状态……70
5.4.4　配置 DHCP 服务……71
5.4.5　设置你的路由器/防火墙日志……72
5.4.6　使用帮助……74
5.5　Cable/DSL 路由器的其他功能……75
5.6　使用 Linksys BEFSR41 快速以太网 Cable/DSL 路由器作为个人防火墙……76
5.7　其他 Cable/DSL 路由器……77

第 6 章　McAfee 个人防火墙……78

6.1　McAfee 概述……79
6.2　系统要求……79
6.3　安装和设置……80
6.4　根据配置向导建立安全策略……82
6.5　常规操作……85
6.5.1　保存配置更改……87
6.5.2　对配置更改加密……87
6.5.3　管理 McAfee 个人防火墙的日志文件……88
6.5.4　系统启动时运行防火墙……88
6.5.5　关闭 McAfee 个人防火墙……89
6.5.6　配置应用程序设置……89
6.5.7　系统设置……89
6.5.8　碎片包……95
6.5.9　最小化到系统程序栏（SysTray）……95

6.5.10 在系统程序栏里启动……95
6.5.11 帮助（Help）……95
6.5.12 阻塞所有通信（Block Everything）……95
6.5.13 过滤通信（Filter Traffic）……96
6.5.14 允许所有通信（Allow Everything）……96
6.5.15 报告应用程序信息摘要（Reporting Summary Application Information）·96
6.5.16 报告应用程序信息细节（Reporting Detailed Application Information）·96
6.6 使用日志……96
6.7 局限……99
6.8 测试 Macfee 个人防火墙……100

第 7 章 BlackICE Defender……101

7.1 综述……102
7.2 系统要求……103
7.3 安装和设置……103
7.4 配置 BlackICE Defender……104
7.4.1 保护设置……105
7.4.2 日志设置……106
7.4.3 证据日志设置……107
7.4.4 搜集攻击者的信息……108
7.4.5 管理指定的 IP 地址……109
7.4.6 ICEcap 属性页……110
7.4.7 建立接口和警报设置……111
7.5 更新 BlackICE Defender 的防护水平……111
7.5.1 自动更新个人防火墙……112
7.5.2 手工更新个人防火墙……113
7.6 正常操作……114
7.6.1 使用 Report Logs……114
7.6.2 高级防火墙设置……118
7.6.3 停止 BlackICE 引擎……120
7.6.4 WWW Network ICE……120
7.6.5 Exit……120
7.7 BlackICE Defender 的局限性……121
7.8 测试 BlackICE Defender 个人防火墙……121

第 8 章 ZoneAlarm……122

8.1 概述……123
8.2 系统需求……123

8.3　安装 ZoneAlarm ····· 124
8.4　开始运行 ZoneAlarm ····· 127
8.5　用 ZoneAlarm 工作 ····· 129
8.5.1　管理 Internet Alerts 和 Firewall Logging ····· 130
8.5.2　Internet Lock Settings ····· 131
8.5.3　配置 Security Settings ····· 132
8.5.4　管理因特网应用程序 ····· 133
8.5.5　ZoneAlarm 的基本配置 ····· 135
8.6　ZoneAlarm Desk Band 工具栏 ····· 136
8.7　ZoneAlarm 警报和日志文件 ····· 137
8.8　ZoneAlarm 警报 ····· 139
8.8.1　程序警报 ····· 139
8.8.2　防火墙警报 ····· 141
8.9　ZoneAlarm 的局限 ····· 142
8.10　测试你的 Zone Labs 个人防火墙 ····· 142

第 9 章　你的计算机有多安全 ····· 144

9.1　针对因特网黑客测试你的弱点 ····· 145
9.1.1　执行一次免费的安全扫描 ····· 145
9.1.2　端口探测 ····· 148
9.2　在运行个人防火墙的条件下测试 ····· 149
9.2.1　再次运行因特网扫描 ····· 150
9.2.2　第二次探测端口 ····· 151
9.3　测试从里到外的安全性 ····· 151
9.4　最后的分析 ····· 154

第 10 章　有安全意识习惯的冲浪者 ····· 155

10.1　更新你的个人防火墙 ····· 156
10.1.1　更新 McAfee 个人防火墙 ····· 156
10.1.2　更新 BlackICE Defender ····· 156
10.1.3　更新 ZoneAlarm ····· 156
10.2　更新你的微软操作系统 ····· 156
10.3　保持你的操作系统被锁定 ····· 159
10.4　使用反病毒软件 ····· 160
10.4.1　反病毒 ····· 160
10.4.2　抗击特洛伊木马 ····· 162
10.4.3　不要成为一个靶机——阻止分布式服务拒绝攻击 ····· 163
10.5　小心小甜饼（cookies） ····· 163

10.6 备份你的数据 164
10.7 警惕并经常测试 165

第 11 章 家庭网络与 Internet 连接共享 166

11.1 什么是家庭网络 167
11.2 把你的网络放在一起 167
11.3 网络软件配置 168
11.4 网络管理 169
11.4.1 建立工作组和计算机名 169
11.4.2 共享网络资源 171
11.5 将你的家庭网络连接到 Internet 175
11.6 使用第二道防火墙加强防御 178
11.7 微软的 Internet 连接共享 180
11.8 使用 NetBEUI 保护你的家庭网络 182

第 3 部分 附录 183

附录 A 其他防火墙产品 184

A.1 Aladdin Knowledge Systems eSafe Desktop 3.0 185
A.2 Norton Personal Firewall 2001 185
A.3 PGP Desktop Security 7.0 186
A.4 Symantec Desktop Firewall 2.0 187
A.5 Sygate Personal Firewall 188
A.6 ConSeal PC Firewall 188
A.7 Tiny Wall Personal Firewall 189

附录 B 其他测试安全性的网站 191

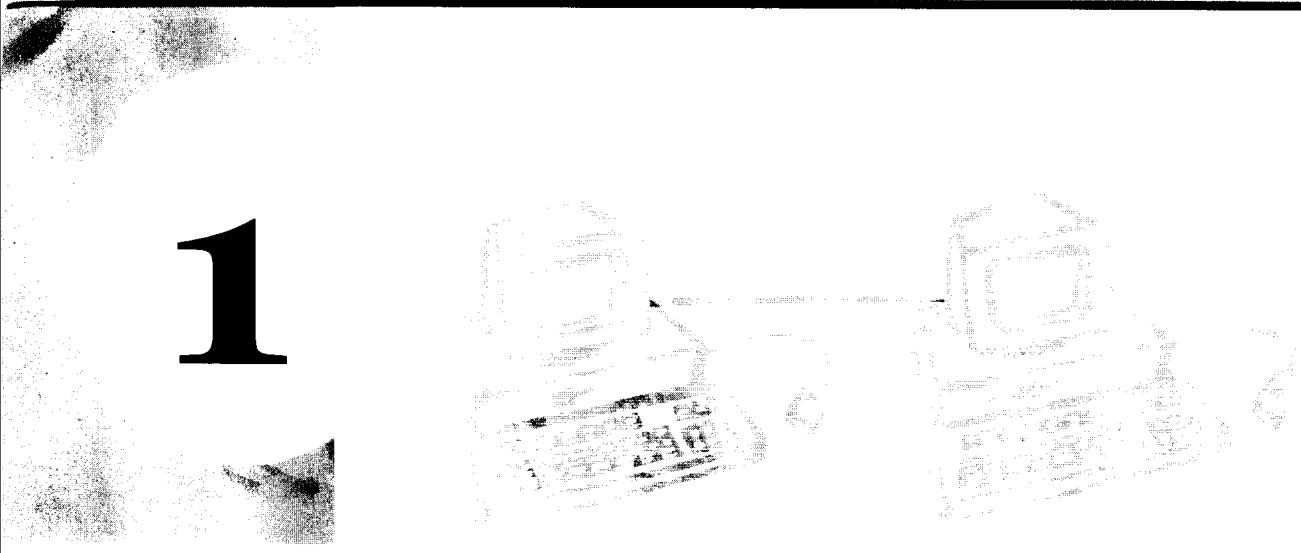
B.1 HackerWhacker 192
B.2 Gibson Research Corporation 192
B.3 Secure Design 193
B.4 Sygate Online Services 194
B.5 Symantec 195
B.6 McAfee 195
B.7 HackYourself.com 196

附录 C 术语表 198

第1部分

个人防火墙简介

1



为什么需要个人防火墙

阅读本章后，你将了解有关因特网的初步知识，并认识到因特网的神奇和危险。因特网是充满信息和机遇的黄金宝地，不幸的是，它也是大胆狂徒的围猎场，他们或者手持工具，入侵计算机并偷走你的个人或财务信息，或者在你的计算机上搞恶作剧，或者干脆破坏你的计算机系统。

在广泛使用的高速因特网的引导下，计算机系统正逐渐成为不法之徒的目标。本书的目的是介绍个人防火墙，以帮助那些在WWW 上冲浪的人们保护他们的数据和隐私。具体而言，应达到以下目的：

- 帮助你认识黑客组织，知道不采取安全措施访问因特网时面临的威胁；
- 帮助你认识高速 Cable modem 和 DSL 接入的危险；
- 让你认识到安装个人防火墙很容易保护你的计算机；
- 帮助你认识软件防火墙和硬件防火墙的区别，并正确选择使用；
- 帮助你了解购置防火墙时应考虑哪些特性。

1.1　高速因特网访问的新时代

无论何时，如果你不使用防火墙，一旦你登录因特网，就意味着将你的计算机电子地链接到一个毫无控制、毫无保护的巨大的网络上。直到最近，除非你在提供高速因特网的公司工作，否则你必须用 56K 的调制解调器通过电话线拨号接入因特网服务提供商才能访问因特网。这种方式不仅很慢，还经常不能真正达到 56K 的速率，实际上，如果能达到 44～49kbit/s，就算很幸运了。

1.1.1　传统的 56K 因特网访问

直到最近，接入因特网还经常很慢，甚至经常掉线，迫使你不停地重拨。当你每次拨号都听到忙音时更是无奈。

当你拨入 ISP 后，ISP 会自动分配给你的计算机一个临时地址，称为 IP 地址。这个 IP 地址是你在网上独一无二的标识。一般情况下，IP 地址的分配是一个动态的过程，这就意味着每次接入可能获得不同的 IP 地址。

在因特网上，你的计算机与其他计算机通信时，所有接收或发送的数据都来自你的 IP 地址。因此，你的 IP 地址会在因特网上暴露你的计算机。一旦你的 IP 地址被入侵者盯上，他就可以访问你的计算机。幸好，临时拨号连接和动态 IP 地址分配大大增加了入侵者跟踪你的计算机的难度。

注意：IP 地址很像家庭住址，它提供了一种在因特网上识别你的计算机的方法，并且通过给分配的 IP 地址收发数据包，可以与其他计算机建立通信。要想知道更多关于 IP 地址的内容，可参考人民邮电出版社出版的《TCP/IP Primer Plus 中文版》，书号为 ISBN 7-115-10303。

概括地说，传统的因特网连接方式有以下特点：

- 采用 56K 慢速率连接；
- 拨号时临时建立连接；
- IP 地址每次都不同；
- 拨入时间长，可能经常掉线。

1.1.2　高速因特网访问的新纪元

采用高速连接，因 56K 拨号连接带来的诸多问题将迎刃而解。高速因特网连接可以保持网络连接持续通畅。通常可采用两种方式：

- 有线电缆（Cable）——这种方式是指采用有线电视同轴电缆连接；
- DSL——这是一种专用连接方式，它通过当地电信公司的电话电缆连接（当然，不是直接接到电话线上）。

这两种接入技术都能提供比 56K 快 20 倍的速率，而且能保持稳定连接，因而不会浪费你不断拨号的时间，也不会让你遭受长时间听到忙音的痛苦。同时，由于你的计算机是稳定连接的，因此 IP 地址也总是保持不变。

高速连接确实不错。但是，任何事情都有两面性，高速连接也不例外。有讽刺意味的是，高速连接的优势也正是其劣势所在。多数情况下，高速连接就像将未上锁的前门向外敞开着一样。这是由高速连接的下列特性决定的：

- IP 地址固定——使得入侵者容易一次又一次地跟踪你的计算机；
- 高速访问——使入侵者可以更快的速度闯入你的计算机；
- 主动连接——意味着你的计算机更容易受到攻击。

由于高速因特网连接仅仅是另一种简单网络连接方式，只要计算机没有关机，它就一直连在网上，保持活动状态。由于高速因特网访问方式，因特网服务提供商配置他们的 DHCP 服务器，使你的计算机 IP 地址保持不变。事实上，如果你每几周至少上网一次，那么你的计算机会刷新地址分配，从而保持 IP 地址不变。但如果你上网的时间间隔超过一定的周期，IP 地址可能会改变。

注意：ISP 维持一个 IP 地址池，用于动态分配或租赁给接入的计算机。租赁周期长度由 ISP 设定。当你首次登录时，ISP 从 IP 地址池中分配一个地址给你的计算机。只要你不断地登录刷新租赁周期，你的地址将保持不变。然而，如果你超过设定的周期长度没有接入，ISP 将收回分配给你的地址。下次连接时，ISP 将另外分配一个新的 IP 地址给你。这一过程对终端用户来说是透明的。

注意：DHCP 代表动态主机配置协议。ISP 用 DHCP 服务器管理 IP 地址分配过程。

由于 IP 地址就像家庭地址一样保持不变，网络上的入侵者（骇客或黑客）很容易闯入你的计算机。一旦你的计算机被他们闯入，他们就可以一次次进出，因为你的 IP 地址不变。

高速连接是一把双刃剑，它在让你高速访问因特网的同时，也使得他人可以高速访问你的计算机。

最后，持续的连接也使得你的计算机或网络成为充满诱惑的目标，因为一旦你的计算机被选定为目标，持续的连接可以让入侵者随时找到你。

如果你喜欢随大流，你就会选择微软的操作系统。很不幸，你可以在第 9 章“你的计算机有多安全”中看到，微软的操作系统虽然易用，但不够安全。事实上，用微软的操作系统高速接入，将使得因特网面临着访问的隐患无穷。

1.2　使用个人防火墙保护你的计算机

至此，你已对高速 Internet 连接如何比普通 56K 连接不安全有了大致了解。现在应该知道的是如何在高速接入时保护你的计算机免受威胁。