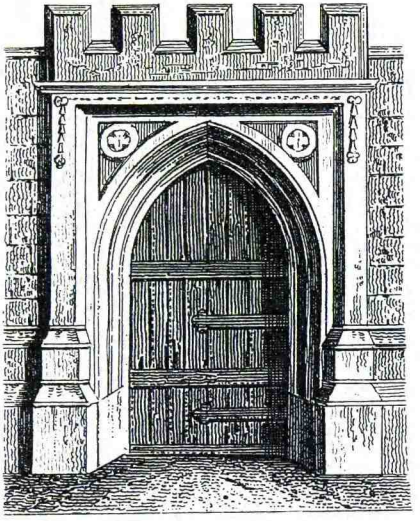
Building Internet Firewalls

构筑因特网防火墙



[美] D. Brent Chapman
Elizabeth D. Zwicky 著

舒若平 朱孝明
郑 宏 胡红宇 译

O'REILLY™

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

构筑因特网防火墙

Building Internet Firewalls

[美] D. Brent Chapman
Elizabeth D. Zwicky 著

舒若平 朱孝明 郑 宏 胡红宇 译

胡红宇 审校

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

联机信息资源

经由匿名 FTP：

ftp://ftp.greatcircle.com/pub/firewalls-book/

万维网上：

http://www.greatcircle.com/firewalls-book/

勘误表网址：

ftp://ftp.greatcircle.com/pub/firewalls-book/Errata

译 者 的 话

今天，谈论因特网已不是计算机界的专利，各行各业的人都在津津乐道。然而，究竟有多少人意识到与因特网相伴而来的巨大风险呢。来自世界各地的形形色色的侵袭者正虎视眈眈，随时都有可能对你的站点发动攻击，破坏你的站点安全。有关美国和欧洲的重要的政府或军事部门的计算机网络系统被"黑客"入侵的报道已屡见不鲜。用不了多久，因特网安全问题就会像计算机病毒一样困扰每一个系统管理员或网络管理者，使我们不得不面对它。

本书全面系统地论述了计算机网络安全问题并且提出了有效地解决这一问题的方法和步骤。我们不揣冒昧地翻译了本书并向业界同行推荐它，希望能为促进国内的计算机安全应用与发展尽绵薄之力。但由于水平有限和时间仓促，书中的缺点错误在所难免，恳请读者批评指正。

在本书翻译过程中，得到了黄永杰、冀春林、高明辉、罗华、朱延洁、周汝华、韩文茜、李海波、陈为林、陈岩、胡朝元、杜团文、范齐、闪瑾雷、李蒨、陈绪、葛丽丽、徐钧等诸多同志的大力支持和帮助；特别是北京联大自动化工程学院的尹传平老师在百忙中对译稿提出了宝贵的意见，在此一并表示衷心的感谢！

译者

1997 年 3 月

序

在任何社会中，只有极少数人是怀有恶意的。据估计，因特网现在大约有 3 千万到 4 千万用户。但是即使恶意用户所占的百分比不到整个社会的百分之一，其绝对数量也非常大，以致于你也将受到来自他们的影响。

向计算机紧急事件响应组织协同中心(CERT－CC)报告的安全事故数量在逐年递增——在 1989 年不到 200 件，在 1991 年大约 400 件，在 1993 年约 1400 件，而在 1994 年达 2,241 件。预计我们将在 1995 年看见多于 3000 件事故的报告。这些事故发生在政府的和军队的站点上，以及《财富》杂志所载的 500 家公司、大学，以及其它一些小规模的网点上。一些事故只涉及单一系统上的单一帐号。另一些(例如，那些与数据包嗅探有关的)可能涉及多达 100,000 个系统。当然，这些数字仅仅是冰山之一角。有许多入侵并没有报告到 CERT 协同中心或者其它计算机安全事故响应组织。事实上，许多完全没报告——在一些情况下，因为受害的机构更愿意避免公开或者草率的指控；在另一些情况下，因为入侵根本没被检测到。

没有人知道实际检测到的被侵入站点的准确的统计数字，但是安全组织中多数人认为这仅仅占百分之几。这里我引用一个统计数字：它来自一个向其顾客提供网络入侵服务的事故响应组。经客户同意，他们试图使用入侵者在侵袭过程中所使用的同样工具来突破系统。这个组发现只有 4% 被探测的站点检测到突破企图。更加惊人的估计是：AT&T Bell 实验室的 Bill Cheswick 相信在那些侵袭成功者中，至少 40% 的侵袭者获得引导访问①。

不仅仅事故的数量在日益增长；而且侵袭的方法也日趋复杂化。当 CERT 协同中心在 1988 年的秋天伴随着因特网蠕虫的出现而成立时，我们面对的侵袭可分为两种主要的类别：猜测口令和利用操作系统与系统程序中的安全漏洞。虽然仍有无数的站点变成这种侵袭的受害者，但在新近发生的事故中呈现出日益明显的技术复杂性。某种程度上，这是系统用户和系统管理员意识提高的结果——用户选择更好的口令，同时管理员更迅速地修补系统。遗憾地是，这种安全意识提高的结果没有压制住对安全的侵袭；它只是迫使侵袭者采用新的诡计。今天，许多侵袭手段更为先进。它们包括伪造网际协议(IP)地址(入侵者猜测与网络连接和机器之间认可的相关联顺序号)，利用 UNIX 系统的确定 IP 数据包类型上的源路由选项，以及截获开放的终端或者登录会话。

这不是说所有用户与系统管理员已吸取了过去侵袭的教训。实际上，在用户和系统管理员中间仍然需要进行更多的教育，管理人员也一样(他们也经常不能完成需要的安全训练)。计算机化的世界，是一个危险的世界，而且太少的人认识到这一点。这是 Internet 的增长可能实际上已伤害到我们的一种情形。在因特网的早期，站点连接到网络通常需要权威的硬件和软件工作人员。今天，连接到因特网是如此容易，以至于各站点忽略了应采取先进的技术去实现安全连接和保持安全。

若干年以前，我在欧洲的一个站点工作(该站点曾经被一个自美国的站点发动侵袭的人

① * 防火墙文摘，1995 年 3 月 31 日。

明显地侵入过)。后来,当我在美国站点会晤系统管理员时,她向我保证在他们那儿甚至没有计算机连接到因特网。当我告诉她嫌疑犯系统的完整域名时,她答复,"啊,你指的是Sun"。其结果是,Sun 在站点中没有被任何人认识到的情况下,为在特殊的应用中使用,曾经安装连接到因特网而运行多年。管理员向我保证他们将断开机器。然而,第二天早晨,欧洲管理人员发给我另一条惊人的电子邮件消息——另一次入侵来自同一个美国系统。我打电话给美国的系统管理员。的确,她断开了调制解调器,她断开了显示器。然而,这一切努力并没有使她脱离到的因特网系统的连接。她不知道这一点,但是侵袭者知道,并在继续利用这一事实。

我一直在告诫那些系统管理员,他们被非法侵入搞的焦头烂额,但是仍没有采取可以阻止这些侵入成功的基本措施。一位系统管理员抱怨他曾经多次重装他的系统,而他仍然被侵袭。其结果是,虽然他知道关于 CERT 顾问和代理商安全公报,但他不愿去安装它们,觉得那样太麻烦。例如,CERT 顾问 CA-93:16 在 1993 年的 11 月被邮寄到网上;它就 Sendmail 的大多数版本问题通告 UNIX 团体;代理商也曾经合作提供替代程序,以及用于 sendmail.cf 文件 MProg 的 /bin/sh 替代程序的顾问程序。一年半以后,CERT 仍然收到来自利用这种旧的 Sendmail 的薄弱环节而被侵入的站点的通报。

虽然安全事故的数量持续增长,侵袭的方式变得越来越复杂,但仍然有关心安全的那些人的好消息。总的说来,我们已看到对连接到因特网相伴而生的危险的认识在不断加深,并且安全团体为此作了大量的工作。其表现之一是事故响应和安全组论坛(FIRST)的成长壮大,它吸引了各种各样的计算机安全事故响应组(在我写此文时已超过 40 个),它们来自政府,商业,以及学术机构等。同样令人鼓舞的是有越来越多的和更好的免费可用的安全工具。计算机操作,监测,和安全技术组(COAST)在 Purdue 的档案馆是大多数安全工具的测试和征集中心。(这本书的附录 A 告诉你如何会晤这两个组织。)最终,一些优秀的出版物(关于因特网安全的书和报纸等)使其他人可以借鉴旁人那些来之不易的智慧。

在这些危险出现的时候,防火墙是保持你的站点安全的最好方法。虽然可能你已将其它形式的安全合并起来,但如果对于连接到因特网你是认真的,防火墙应该处于你的安全计划的中心。Brent Chapman 作为因特网防火墙技术的最早研究者和权威;他的防火墙邮件清单和指南是对那一点的证明。Elizabeth Zwicky 则通过她在系统管理员协会(SAGE)的工作,起到安全和合理的系统管理的代言人的作用。他们合写的书将就关于因特网安全方面的意识和能力提高到一个新的水平。

Ed DeHart
CERT 技术顾问
CERT 协同中心(CERT-CC)
软件工程学院
Carnegie Mellon 大学
匹兹堡,PA
1995 年 6 月

前　言

本书是构筑防火墙的实用指南。它提供如何在你的站点设计和安装防火墙的具体步骤和方法，并且说明如何配置因特网服务，如电子邮件，FTP，环球网等，来与防火墙一起工作。防火墙是复杂的，并且我们不能把所有内容归结为一些简单的规则。因为它主要取决于你的站点所用的硬件设备、操作系统、联网方式，以及你想要你的用户能做什么、不能做什么。我们试图给你足够的规则、例子和资源，期望你将能够依靠自己来完成防火墙的设置。

防火墙是什么，它能为你做些什么？防火墙是在因特网和你的内部网络之间限制访问的方法。你在最有效的地方——你的网络连接到因特网的地方安装防火墙。在你的站点，防火墙的存在能大大地减少外部侵袭者突破你的内部系统与网络的可能性。防火墙也能禁止你自己的用户发送危险的信息——未加密的口令和敏感数据——到外部世界损害你的系统。

我们看到，对与因特网有关系统的侵袭比过去更为严重而且技术上更复杂。为避免这些侵袭损害我们的系统，我们需要得到各方帮助。防火墙是保护你的站点免受这些侵袭的十分有效的方法。由于这个原因，我们极力推荐将防火墙包括在你的站点的全面的因特网安全计划中。然而，防火墙应该只是那个计划中的一部分。安全策略、强大的主机安全、鉴证和加密、与你安装的防火墙一样，也是至关重要的。这本书在着重论述防火墙的同时将涉及这些问题。

这本书的范围

这本书被划分成四部分：

第一部分，网络的安全性，探讨因特网安全的问题，并且着重研究作为解决这个问题的有效策略的一部分的防火墙问题。

第一章，为什么要构筑因特网防火墙简要介绍当今使用因特网的主要风险；讨论保护什么，和防备什么；讨论各种各样的安全模式；同时简介防火墙能为你的站点安全做些什么和不能做什么。

第二章，因特网服务，概述了用户想要的和需要的因特网服务，并且汇总了由那些服务造成的安全问题。

第三章，安全战略，概述了机构在采取安全策略并且决定为专用安全设施投资之前，需要了解的基本安全原则。

第二部分，构筑防火墙，描述如何构筑防火墙并配置与之一起运行的服务。

第四章，防火墙设计，概述了用于构筑防火墙的基本部件和主要体系结构：双重宿主主机，被屏蔽主机，被屏蔽子网，以及在这些基本的体系结构上的变化。

第五章，堡垒主机，给出了用于许多防火墙配置中的关于设计和构筑堡垒主机的详细指导。

第六章，*数据包过滤*，描述数据包过滤系统如何工作，并且讨论用其构筑的防火墙能完成什么和不能完成什么。

第七章，*代理系统*，描述代理客户和代理服务器如何工作，并且如何利用这些系统构筑防火墙。

第八章，*配置因特网服务*，逐一描述如何配置与防火墙一起运行的各种主要的因特网服务。

第九章，*两个防火墙实例*，给出了防火墙的两个基本配置实例。

第十章，*认证及入站服务*，讨论允许用户从因特网访问你的系统的问题，并且描述各种各样的认证策略与产品。

第三部分，*保持维持站点安全*，描述如何确立你的站点的安全策略，维护你的防火墙，并且处理即使是最有效的防火墙也可能发生的安全问题。

第十一章，*安全策略*，讨论了你的站点具有清晰易懂的安全策略的重要性，及该策略应该包括什么和不应该包括什么。它也讨论使管理人员与用户接受策略的方法。

第十二章，*维护防火墙*，描述如何随时维护你的防火墙安全，及如何使你自己了解到新的因特网安全威胁和技术。

第十三章，*对安全事故作出反应*，描述当侵入发生，或者当你怀疑你的安全正在受到威胁时该做什么。

第四部分，*附录*，由下面三个附录组成：

附录 A，资源部分，包括你能取得有关因特网安全的进一步的信息与帮助的地址清单：环球网页，FTP 站点，邮件清单，新闻组，响应组，图书，论文，和会议等。

附录 B，工具部分，汇集了最好的免费的防火墙工具和如何得到它们的信息。

附录 C，TCP/IP 基本原理，包括对构筑或者管理防火墙的任何人都是十分重要的关于 TCP/IP 的背景信息。

读者对象

谁应该读这本书？

虽然本书旨在那些需要构筑防火墙的人，但是它的大部分内容对关心因特网安全的每个人也是合适的。下面告诉你哪些段落特别适合于你：

如果你是系统管理员：

你应该通读全书。正如我们所述，TCP/IP 的全面知识对了解和构筑防火墙是十分重要的。如果你尚不熟悉 TCP/IP，你现在至少应该立刻读附录 C。[①]

如果你是正考虑连接到因特网的站点的管理人员：

你至少应该阅读本书的第一部分。第一部分的各章将向你简介各种类型的因特网威胁、服务，以及安全方法和策略。还将为你介绍防火墙，描述对实施因特网安全它们能做什

① 这里我们执意推荐你阅读 Craig Hunt 原书的全部内容，《TCP/IP 网络管理》(O'Reilly & Associates, 1992)，与附录相配合。

么和不能做什么。你也应该读第四章，它提供防火墙设计的概述。此外，附录 A 告诉你在何处能取得更多信息与资源。

如果你是已经连接到因特网的站点的管理人员和用户：

你应该阅读为前一类管理人员推荐的全部章节。此外，你还应该读第三部分，它解释在你的站点上可能出现的各种问题，例如，如何发展安全策略，保持最新，以及如果有人侵袭你的站点如何作出反应。

软件平台

在很大程度上，本书是独立于平台的。因为这里提供的大多数信息是由通用型的原则组成的，其中大多数应该适用于你，不论你使用什么硬件设备、软件、和联网方式。大多数与特定平台有关的问题是用什么类型的系统作为堡垒主机。但人们已成功地使用各种计算机构筑堡垒主机（在本书的第五章中描述），包括 UNIX 系统，Windows NT 机器，Macintosh，VMS VAX 及其它系统。

说到这里，我们必须承认本书中的具体例子有明显的 UNIX 倾向。这是有原因的。由于本书是关于构筑防火墙的，而现在，完成这个任务所需的大部分免费使用的工具是在 UNIX 系统环境下。因此，今天构筑的大多数防火墙使用 UNIX 系统作为它们的堡垒主机（当然，虽然许多其它类型的机器可以被包括在全面配置中）。我们期待这种状况会在今后几年内改变，现在，可供多种类型的系统使用的商业化系统正变得越来越多。当然，另一个理由是我们自己的经验也主要集中在 UNIX 方面。

建议和问题

有关这本书的建议和问题请向出版商提出：

O'Reilly & Associates
103 Morris Street, Suite A
Sebastopol, CA 95472
1－800－998－9938（在美国或者加拿大）
1－707－829－0515（国际或者本地）
1－707－829－0104（FAX）

你也能用电子方法把消息发送给我们。见本书中关于 O'Reilly & Associates 的联机服务的所有信息。

有关本书的技术问题或意见，请发送电子邮件到如下地址：

firewalls－book@greatcircl . com

目　　录

序
前言
第一部分：网络的安全性 …… (1)

第一章：为什么要构筑因特网防火墙 …… (3)

你试图保护什么 …… (3)
你试图防备什么 …… (4)
如何保护你的站点 …… (10)
什么是因特网防火墙 …… (13)

第二章：因特网服务 …… (19)

电子函件 …… (20)
文件传输 …… (21)
远程终端访问和命令执行 …… (22)
Usenet 新闻 …… (23)
万维网 …… (24)
其它信息服务 …… (25)
入网成员信息 …… (26)
实时会议服务 …… (27)
名字服务 …… (28)
网络管理服务 …… (29)
时间服务 …… (29)
网络文件系统 …… (30)
窗口系统 …… (31)
打印系统 …… (31)

第三章：安全战略 …… (33)

最小特权 …… (33)
纵深防御 …… (34)
阻塞点 …… (35)
最薄弱链接 …… (35)
失效保护状态 …… (36)
普遍参与 …… (38)
防御多样化 …… (38)

简单化 …… (39)

第二部分:构筑防火墙 …… (41)

第四章:防火墙设计 …… (43)

防火墙定义 …… (43)
防火墙体系结构 …… (48)
防火墙体系结构的不同形式 …… (54)
内部的防火墙 …… (62)
未来趋势 …… (66)

第五章:堡垒主机 …… (69)

总的原则 …… (69)
特殊类的堡垒主机 …… (70)
选择机器 …… (71)
选择物理位置 …… (74)
在网络上定位堡垒主机 …… (74)
选定堡垒主机提供的服务 …… (75)
堡垒主机上不保留用户帐号 …… (77)
构筑堡垒主机 …… (77)
运行堡垒主机 …… (95)
保护机器和备份 …… (96)

第六章:数据包过滤 …… (99)

数据包为什么要过滤 …… (100)
配置数据包过滤路由器 …… (103)
数据包是什么样的 …… (104)
路由器对数据包的作用 …… (116)
数据包过滤规则的约定 …… (118)
按地址过滤 …… (121)
按服务过滤 …… (123)
选择数据包过滤路由器 …… (126)
在哪里进行数据包过滤 …… (135)
总结 …… (136)

第七章:代理系统 …… (143)

为什么要代理 …… (143)
代理是如何工作的 …… (146)
代理服务器术语 …… (148)

将代理用于因特网服务……(149)
没有代理服务器的代理……(150)
将 SOCKS 用于代理 ……(151)
将 TIS 因特网防火墙工具包用于代理 ……(153)
如果不能代理怎么办……(154)

第八章:配置因特网服务 ……(157)

电子函件……(159)
文件传输……(169)
终端访问(Telnet) ……(180)
远程命令执行……(182)
网络新闻传输协议(NNTP) ……(186)
万维网(WWW)和 HTTP ……(190)
其它信息服务……(198)
信息查询服务……(203)
实时会议服务……(205)
域名系统(DNS)……(211)
系统日志 syslog ……(226)
网络管理服务……(227)
网络时间协议(NTP) ……(234)
网络文件系统(NFS)……(236)
网络信息服务/黄页(NIS/YP)……(238)
X11 窗口系统 ……(239)
打印协议(lpr 和 lp) ……(242)
其它协议分析……(243)

第九章:两个防火墙实例 ……(245)

被屏蔽子网体系结构……(245)
被屏蔽主机体系结构……(262)

第十章:认证及入站服务 ……(271)

使用入站服务的风险……(272)
什么是认证……(274)
认证机制……(277)
完整的认证系统……(281)
网络级加密……(285)
终端服务器和调制解调器组……(288)

第三部分:维护站点安全 …… (291)

第十一章:安全策略 …… (293)

你的安全策略 …… (293)
综合考虑安全策略 …… (297)
制定战略与策略 …… (299)
如果你不能得到安全策略怎么办 …… (303)

第十二章:维护防火墙 …… (305)

日常管理 …… (305)
监控你的系统 …… (307)
保持领先 …… (314)
是否费时 …… (316)
何时重建 …… (317)

第十三章:对安全事故作出反应 …… (319)

对事故作出反应 …… (319)
事故发生后做什么 …… (325)
追踪和捕获入侵者 …… (325)
规划你的反应 …… (327)
未雨绸缪 …… (334)

第四部分:附录 …… (343)

附录 A :资源 …… (343)

WWW 页面 …… (343)
FTP 站点 …… (344)
邮件表 …… (345)
新闻组 …… (346)
响应组及其它组织 …… (348)
会议 …… (350)
论文 …… (352)
图书 …… (355)

附录 B :工具 …… (355)

认证工具 …… (355)
分析工具 …… (356)
数据包过滤工具 …… (358)

代理系统工具…… (358)
守护程序…… (359)
实用工具程序…… (360)

附录 C :TCP/IP 基本原理 …… (361)

第一部分

网络的安全性

第一章，为什么要构筑因特网防火墙
第二章，因特网服务
第三章，安全战略

第一部分探索因特网的安全问题并着重介绍解决这一问题的有效策略组成部分的防火墙。

第一章，为什么要构筑因特网防火墙，介绍当今与使用因特网有关的主要风险；讨论保护什么和防备什么；讨论各种各样的安全模式；和介绍为了你的站点安全，防火墙在这方面能做什么和不能做什么。

第二章，因特网服务，概述用户想要的和需要的因特网服务并总结由这些服务带来的安全问题。

第三章，安全战略，概述机构在采纳安全策略和投入专门的安全机制之前需要了解的基本安全原则。

本章内容提要：

- 你试图保护什么
- 你试图防备什么
- 如何保护你的站点
- 什么是因特网防火墙

1 为什么要构筑因特网防火墙

漫步书店、翻开杂志或报纸、收听新闻广播时，你几乎躲不开有关因特网的一些事情。因特网变得如此普及，就连非技术性的出版物在提到它时也不再需要作更多的解释。当非技术性出版物着迷于因特网时，技术性出版物已经领先一步，开始关注因特网的安全问题。这是个合理的进步。当你为街区有了高速公路而带来的第一次兴奋感渐渐消逝时，你会注意到它不仅仅是方便旅行，同时它也向大量的外来者暴露了你所在的位置，这是你所不愿意看到的。

下面两种观点都是对的：因特网以变革的方式，提供了检索信息和发布信息的能力，这是个不可思议的技术进步；但它也以变革的方式带来了信息污染和信息破坏的主要危险。本书将要提出一种权衡其优点和风险的折衷方法——在参与因特网的同时也保护你自己。

本章以下各节中描述的是在因特网上人们已经用来保护其数据和资源的不同的安全模式。本书的重点是讲述网络的安全模式，特别是因特网防火墙的用法。防火墙是一种允许网络连接到因特网，同时保持某一等级的安全性的解决办法。在本章最后一节"什么是因特网防火墙"中，我们描述了防火墙的基础知识，并且概要总结了在帮助你构筑你的站点防火墙时，它们能做些什么和不能做什么。但是，在讨论你能用防火墙做些什么之前，让我们先简短地描述一下你为什么需要它。在你的系统中你要保护的是什么？哪些类型的侵袭和侵袭者是我们今天常见的？哪些类型的安全性措施可用来保护你的站点？

你试图保护什么？

防火墙本质上是一种保护装置。如果你在构筑防火墙，你需要弄清楚的第一个问题是你试图保护什么？当你连接到因特网时，你正把下面这些东西置于风险之中：

- 你的数据：你保存在计算机里的信息
- 你的资源：计算机本身
- 你的声誉

你的数据

需要保护的数据有三个独立的特征：