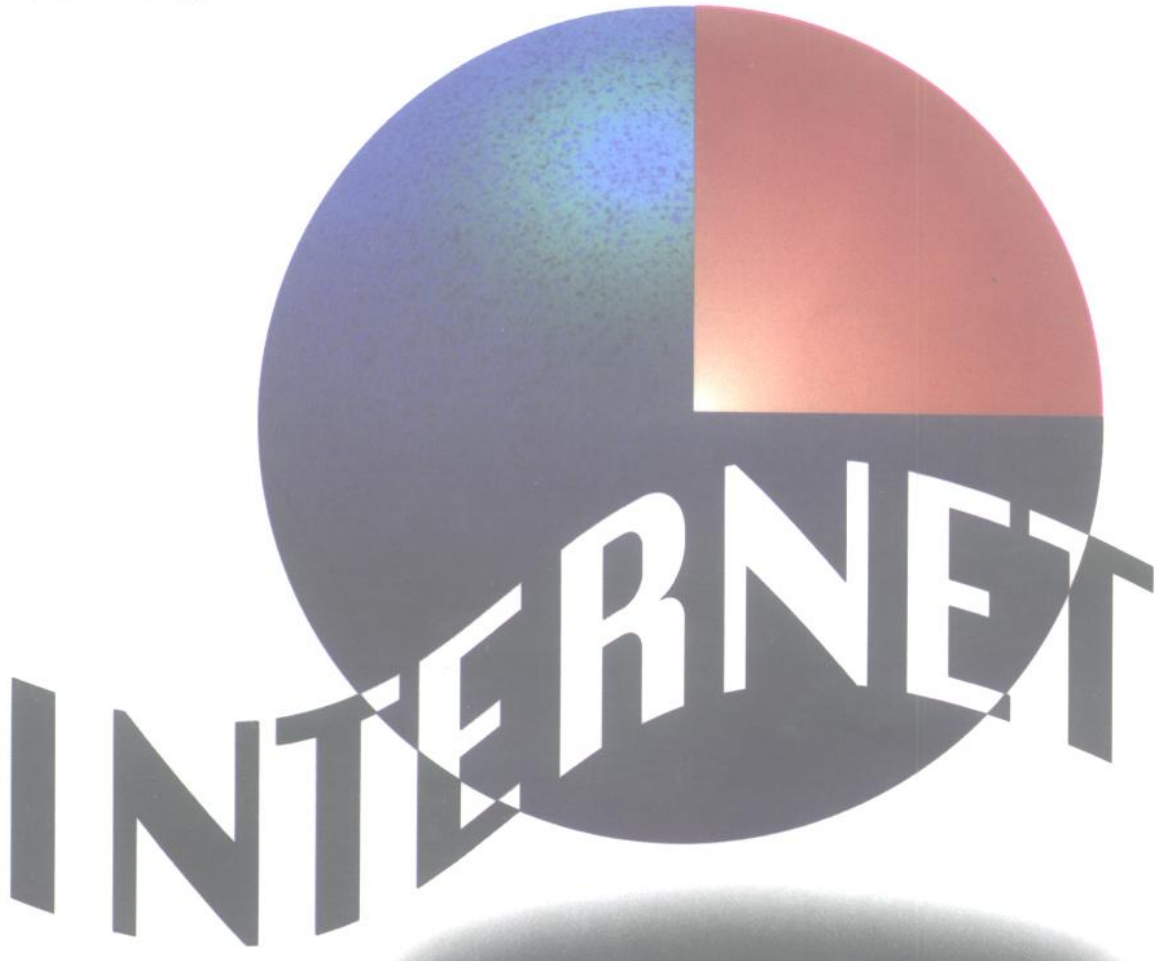
◆ [美] Scott Fuller & Kevin Pagan 著
◆ 董 春 张红雨 刘英杰 译
◆ 王邵平 审校



Intranet 防火墙

FIREWALLS

Intranet FIREWALLS
Intranet 防火墙

[美]Scott Fuller 和 Kevin Pagan 著

董 春 张红雨 刘英杰 译

王邵平 审校

電子工業出版社
Publishing House of Electronics Industry

内 容 提 要

近年来 Internet 以出人意料的速度向前发展。而 Intranet(企业内联网)是由 Internet 引发出来的,它的出现将迎来新一轮技术革命。防火墙是与 Intranet 紧密相联的。

本书从防火墙的概念讲起,介绍了 Internet 和 Intranet 的基本知识,在此基础上讨论了防火墙的理论和实施。另外,还介绍了防火墙的产品及相关信息的 Web 地址。在附录中提供了许多 Intranet 和网络安全等有价值的补充信息。

本书通俗易懂,语言流畅,既适合专业人员参考,又适合对 Intranet 感兴趣的非专业人员阅读,有助于读者全面深入了解 Intranet 及安全性问题。

书　　名:Intranet 防火墙

著　　者:[美]Scott Fuller 和 Kevin Pagan

译　　者:董　春　张红雨　刘英杰

审 校 者:王邵平

责任编辑:王明君　刘娜

特约编辑:那青

印 刷 者:北京市大中印刷厂

出版发行:电子工业出版社出版、发行　URL:http://www.phei.co.cn

北京市海淀区万寿路 173 信箱　邮编 100036　发行部电话:68214070

经　　销:各地新华书店经销

开　　本:787×1092 1/16　印张:11.5　字数:294.4 千字

版　　次:1997 年 7 月第 1 版　1997 年 7 月第 1 次印刷

书　　号:ISBN 7-5053-4097-2 / TP·1800

定　　价:19.00 元

著作权合同登记号 图字:01-97-0820 号

作 者 简 介

Kevin D. Pagan

Kevin D. Pagan 先生是专门从事民事诉讼法的律师，是地方政府的代表，现在担任德克萨斯州麦卡伦市的助理城市律师。Pagan 先生在阿肯色州立大学获会计学学士学位，在南 Methodist 大学获法律学学士学位。Pagan 先生是德克萨斯州律师协会和美国律师协会的会员。在 11 年的律师生涯中，Pagan 先生为两家法律公司做过网络系统管理员，并帮助这些公司和其他客户开发研制普通业务和其他法律方面的网络解决方案。Pagan 先生与他人合著了许多关于计算机方面的书籍。

Scott Fuller

Scott Fuller 先生是 IDEAS 公司的总裁，曾经在 EDS 公司就职。IDEAS 是美国全国性的提供计算机解决方案的公司，咨询与 MIS 有关的各方面的问题。Fuller 先生在计算机操作、软件工程、及终端用户培训方面有广泛的经验。Fuller 先生与 Pagan 先生合作出版了 6 本与计算机有关的书籍。您可以给 Fuller 先生发 E-Mail，地址是：ScottFuller@msn. com.

Dennis Lone

Dennis Lone 先生名片上印的是："多数时间是一个作家"。Lone 先生自上大学以来，写作占去了他的大部分时间（当他赶一份新闻稿件时，自称为"打字机"）。在他成为企业家时，有几年他在加州的硅谷创建并运作一个高技术广告媒体机构。后来，他移居太平洋西北海岸，在那里作为自由作家生活和工作至今。虽然他写的书籍多数与技术有关，但他仍认为自己是一个对用户具有同情心的非技术人员。为一切会使我们的生活变得更轻松的事情而奋斗。

致　谢

与其它有关前沿技术的书籍一样，本书是由许多人组成的一支队伍完成的，而不仅仅是几名作者。在此向他们全体表示衷心的感谢，并特别感谢以下几个人。

Ventana 的职员们，特别是 Lynn、Judy 和 Neweleen，是他们将这项工程由一个好的想法变成了一本真正的书。这不是一项轻松的任务，尤其是在飓风期间。即使在最困难的时刻，他们也始终与我们站在一起。

感谢书中涉及到的许多软件和硬件公司，他们允许我们访问有关安全性产品的敏感信息。

最后，感谢我们的文学上的代理人 Lisa Swayne 和 Bill Adler，他们为我们而冒险，并且始终没有放弃。特别是 Lisa，在本书的写作期间始终把握着它的方向，确保本书不走入歧途。

译 者 序

现在 Internet(国际互联网)的发展已成燎原之势,随着 WWW 上商业活动的激增,Intranet(企业互联网)也应运而生。Intranet 是以 Web 浏览器、服务器和基于网络的协议(如 TCP/IP 和超文本传输协议 HTTP)作为企业内部应用的标准平台,将 Internet 中 TCP/IP、SMTP、HTML、Java、URML、WWW 等技术和标准融入企业的信息结构之中,并使企业互联网(Intranet)与国际互联网(Internet)无缝地连接起来,为企业经营带来巨大的好处。Intranet 正在成为 Internet 发展的新热点,据估计在未来几年,Internet 软件开发市场的百分之七十将属于 Intranet。目前网络世界的迅速崛起,对各种组织机构以及所有的人乃至社会本身将带来深刻的影响,人们和企业所关心的是所有这一切连接性的价值是什么?我们大家聚集一堂的用意又是什么?从何处去赚钱?这就是为什么越来越多的人开始对网络感兴趣。一个真正的 Intranet 应用程序可使员工更轻松地完成实际工作、重新设计产品、客户的服务项目或者改变决策过程。如果一家企业内部通过 Intranet 来改变他们的工作过程的话,那么这家企业就得改变管理方式,这些改变由网络专家来作出决定吗?当然不是,应该由企业主管、政府官员、董事会、市场开发部门、工程部门、客户服务部门、人事部门等来作出决策,因此本书也将适合他们阅读。如果您是掌握企业核心的管理者,Intranet 将助您重新部署企业战略。为了交易和信息流动,内部系统还将需要与世界上其他网络进行广泛的连接,另外,被辞职的雇员是否会报复式地破坏您的网络?通过 Intranet 处理的机密信息是否会被非法截获?您的 Web 服务器能保证安全处理在线业务吗?Intranet 要能更好地服务于企业的经营和管理,这些安全问题将要优先考虑的。在本书中讨论的防火墙(firewall)解决方案,将帮助企业网络免受未授权用户、网络"黑客"和工业间谍的攻击。在安全策略中除了有效的防火墙之外,可能还要有身份验证、数字密码、数据加密等安全机制,从而保证在 Internet/Intranet 环境中,用户的通信和企业内部资源的安全。

什么是防火墙?对这个新近出现的名词可能有些耳熟,但其概念不是人人都知道的。防火墙是为实现企业的安全策略所须的计算机软件及硬件设备的组合,简而言之是一个保护网络的安全措施。为帮助读者完全理解防火墙,在第一部分中,本书作者使用了"搭积木"的方式,例如,本书后面章节所讨论的如何建造 Intranet 防火墙,是基于您从前面章节中所获知识的基础上,如一般防火墙技术等章节。这种方法将使读者对掌握这一迅速发展的技术打下一个良好的基础。先从计算机安全的重要性讲起,然后用较多篇幅介绍了 Intranet 技术,在此基础上讨论了防火墙的理论和实施。在第二部分针对第一部分,选择了 5 种能够帮助我们说明各种技术的防火墙产品,并提供了为数众多的防火墙产品的制造者、简单介绍和联络信息,包括 Web 地址,您可以通过 Web 地址来得到更多的有关防火墙产品的信息。第三部分是"附录",提供了许多 Intranet 和网络安全的有价值的补充信息。

下一个问题则是本书所面对的读者群。从我着手翻译本书起,一方面被本书作者的编排结构和通俗的语言技巧所吸引,另一方面一直在考虑谁将关心这本书?等译稿初步完成时,这个答案自然就有了,本书适合于对计算机感兴趣的所有人。也许您还是认为安全问题离我们太远,其实不然。如果您或您的公司有了一个计算机网络,并且访问您的计算机的用户不限于您

的家里或公司内部，那么您就需要掌握安全性知识。如果您的网络使用 Internet 方式连接，或者您正在考虑用 Internet 技术改进您的内部网络，那么您就需要了解防火墙。本书不但给计算机行业的人员（如系统管理员和系统操作员）提供了有用的信息，而且给非计算机人员（如管理决策者）提供了有关计算机安全和 Intranet 操作的基本知识。正如本书作者所宣称的："无论您的企业大小如何，也不管您使用什么样的计算机平台，本书所含的信息都将对您有所帮助"，因此只要您有兴趣获取新的知识，在案头增添这本好书是很值得的。

在本书的翻译过程中，得到了航天工业总公司七一〇研究所黄祖蔚研究员的指导，并得到了北京航天四创高技术开发中心资深网络专家宋国光先生和美国 SUN 公司的马荣增先生的热情帮助，王式佳小姐帮助录入书稿，在此一并致谢。

由于时间紧迫，加之译者水平所限，如有疏漏和不当之处，敬请广大读者批评指正。

译者：董春

1997 年初

序　言

在日益拥挤的“信息高速公路”上，随着计算机、网络、Web 站点、服务器及其它各种以硅为灵魂的产品的激增，已经引起人们对这样一个问题的关注：即公司的计算机系统上的信息是否存在不安全因素？这种担心是有理由的，因为曾经一度被认为无害的“黑客”已成为成熟的间谍，加之在 Internet 及最近出现的企业 Intranet 上，访问各种系统的用户，正按指数级增加。

随着企业系统中有价值数据的不断增加，各企业现在必须在其系统的以下 3 个主要入口处设防：内部访问、外部访问（如通过 Internet）和最近出现的混血儿——Intranet。本书集中论述了 Intranet 和用来保护这些系统安全的防火墙。

谁需要这本书？

本书为计算机行业中的每一位成员提供了有用的信息，包括网络的运行和实施人员（如系统管理员和系统操作员）、购置计算机相关设备的决策人员、甚至每天使用该系统的用户，因为以上人员需要了解计算机安全和 Intranet 操作的基本知识。

无论您的企业大小如何，也不管您使用什么样的计算机平台，本书所含信息都将对您有所帮助。

虽然我们假设您对基本的计算机概念和操作系统有所了解，但使用本书并不需要具有 Intranet、Internet 协议、或防火墙的知识。

如果您或您的公司有了一个计算机网络，并且访问您的计算机的用户不限于您的家里或公司内部，那么您就需要掌握安全性知识。如果您的网络使用 Internet 方式连接，或者您正在考虑用 Internet 技术改进您的内部网络，那么您就需要了解防火墙（在第一章中将介绍传统的网络安全和 Intranet 防火墙的区别）。

防火墙是为实现企业的安全策略所需的软件及硬件设备的组合，通常是为保护网络免受来自外部的非授权用户的访问。例如，与 Internet 连接的一个计算机网络，必须保护其不被 Internet 上非授权用户所访问。类似的，一个企业 Intranet（即使用 Internet 技术的内部网络），可能有某些部分不允许另一些部分访问，防火墙系统将提供这种保护。

无论您对外部访问进行设计、管理，或简单的使用计算机，本书都将在计算机安全方面使您和您的企业避免付出昂贵的错误代价。

本书讲些什么？

本书解释如何使用防火墙来保护您企业的 Intranet 安全区域。为此，书中还介绍了计算机、Intranet 和网络安全的基本知识，在此之后，探讨了更复杂的防火墙概念，并为您建立和管理您自己的防火墙系统提供了实用信息。

本书分为三部分：第一部分是“防火墙概念”、第二部分是“防火墙产品”、第三部分是“附录”。选择了 5 种能够帮助我们说明各种方法的防火墙产品。在第一部分中，我们提到这些产

品，以帮助解释如何实现一个 Intranet 防火墙。第二部分提供了这些产品更详细的信息，还列出了其它一些防火墙产品及销售商。您最好还是查一下第三部分的附录，提供了许多 Intranet 和网络安全的有价值的补充信息。

下面是本书的内容概要：

第一部分：防火墙概念

第一章，“基础知识”中提出所有您所需要的普通知识，来回答为什么您的企业会从 Intranet 技术中获益，为什么您需要防火墙、安全如何重要以及其它与 Intranet 防火墙有关的基本概念。

第二章，“Intranet 概念”中囊括 Intranet 设计和实现的理论。

第三章，“将防火墙集成到总的网络安全中”，讨论实现将防火墙纳入您已有的网络安全计划中的概念和设计策略。

第四章，“防火墙的概念和技术”中提出防火墙理论和建设的实用信息。

第五章，“实际防火墙的实现”中用一个典型的商业为例，给出在您的企业中如何使用 Intranet 防火墙的实用信息。

第二部分：防火墙产品

第六章至第十一章给出我们在第一部分提到的产品的更详细的背景信息。

- BorderWare Firewall Server（第七章）
- LT Auditor +（第八章）
- Modem Security Enforcer（第九章）
- Internet Scanner（第十章）
- CyberSafe Challenger（第十一章）

第十二章，“其它防火墙产品”中列举了为数众多的其它防火墙产品及制造者、简单介绍和联络信息，包括 Web 地址，您可以通过 Web 地址来得到更多的有关防火墙产品的信息。

第三部分：附录

附录 A：“电子邮件的保密性和安全性”是关于 E-Mail 安全问题的绝妙的讨论，作者是 Sean Carton 和 Gareth Branwyn，摘自他们的 Internet Power Toolkit（Ventana 1996）。

附录 B：“关于防火墙的其它有用的注释”是选自最近出版的《全国计算机安全联盟防火墙购买者指南》，感谢全国计算机安全联盟（NCSA）允许我们引用这些短文，它为策划协议和测试您的防火墙提供了有价值的提示，并给出 Internet Protocol 第六版关于安全影响的一些想法。

附录 C：“其它资料丰富的防火墙资源”中列举了与安全有关的 Usenet 新闻组、邮件表、经常被问的问题（FAQS）和组织。

附录 D：“Intranet 重新定义企业信息系统”是 Netscape 通信有限公司的白皮书，在此是得到 Netscape 的许可引用的。

开始学习如何保护你的计算机系统免于内部和外部的入侵者的危害，请翻到第一章。

目　录

第一部分　防火墙概念

第二部分 防火墙产品

第三部分 附 录

第一部分　防火墙概念