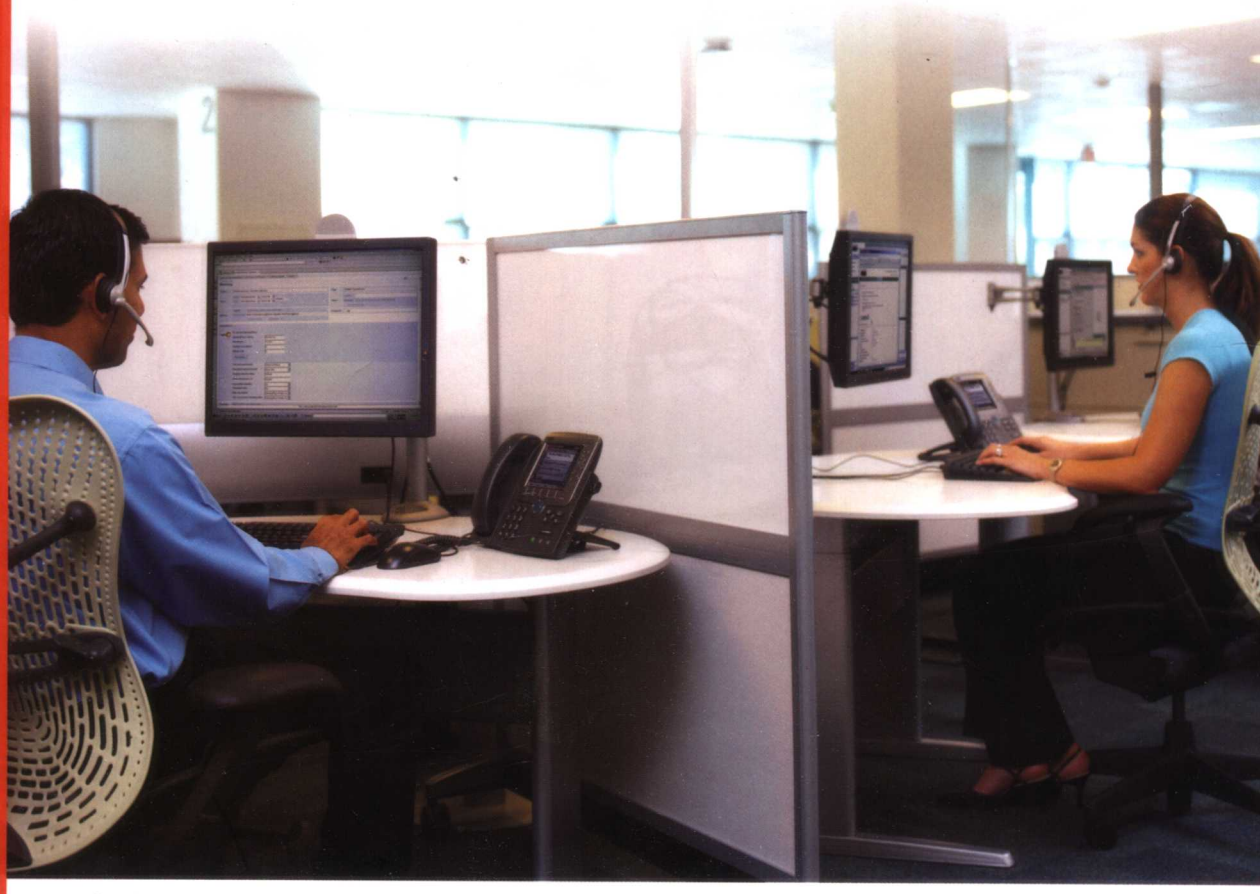
Cisco Systems

ciscopress.com

防火墙基础

Firewall Fundamentals



An introduction to network and computer firewall security

[美] Wes Noonan
Ido Dubrawsky 著

陈麒帆，CCIE #15116 译

人民邮电出版社
POSTS & TELECOM PRESS

防火墙基础

[美] Wes Noonan　Ido Dubrawsky　著

陈麒帆，CCIE #15116　译

人 民 邮 电 出 版 社

北 京

图书在版编目（CIP）数据

防火墙基础 /（美）努南（Noonan, W.），（美）达布斯基（Dubrawsky, I.）著；陈麒帆译. —北京：人民邮电出版社，2007.6
ISBN 978-7-115-15964-9

Ⅰ. 防… Ⅱ. ①达…②陈… Ⅲ. 计算机网络－防火墙 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 034551 号

防火墙基础

◆ 著 [美] Wes Noonan Ido Dubrawsky
译 陈麒帆，CCIE #15116
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
人民邮电出版社河北印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：18.75
字数：462 千字 2007 年 6 月第 1 版
印数：1 - 4 000 册 2007 年 6 月河北第 1 次印刷

著作权合同登记号 图字：01-2006-7043 号

ISBN 978-7-115-15964-9/TP

定价：45.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223

内容提要

在病毒和蠕虫等网络威胁泛滥的今天，防火墙已经成为保护网络和计算机的代名词。只有全面理解防火墙的作用、防火墙的部署、防火墙的不同类型等才能完善安全防范手段。本书介绍了防火墙的基本概念；研究了多种主流防火墙类型的特性以及它们之间的异同，帮助读者进行选择；针对每种类型的防火墙提出了基本的实施配置方案，指导管理员快速地将防火墙安装在网络中；最后，在读者对防火墙产品有了一定的了解和辨别能力以后，本书还介绍了一些高级防火墙特性，以使防火墙能够满足更多、更复杂的环境。

书中提供了大量实施案例，指导网络管理员和家庭计算机用户有的放矢地选择恰当的防火墙产品，并通过相应的配置使其发挥最大功效。

本书适合网络管理员、防火墙及其相关技术的初学者和其他对防火墙技术感兴趣的人士阅读。

关于作者

Wes Noonan，CISA，是活跃在 NetIQ 公司安全解决产品线上的一位质量工程师。Wes 拥有超过 12 年的行业经验，尤其在基于视窗系统的网络和网络安全框架设计和实施方面有独到之处。Wes 是 *Hardening Network Infrastructure* 一书的作者，他也是 *CISSP Training Guide*（《CISSP 认证考试指南》，已由人民邮电出版社翻译出版）和 *Hardening Network Security* 的合著者或供稿人之一，同时他还是“黑客解密”系列丛书中 *Cisco Networks* 的技术编辑。Wes 还维护着 Techtarget.com 中的一个 Windows 系统网络安全的“专家解答”版块（http://searchwindowssecurity.techtarget.com/ateAnswers/0,289620,sid45_tax298206,00.html）。Wes 和他的妻子以及两只斗牛犬居住在德克萨斯州的休斯敦市中心。

Ido Dubrawsky，CISSP，是 Microsoft 公司通信部门的一位战略安全顾问。到微软工作之前，Ido 拥有一家网络安全咨询公司——Silicon Security, Inc.（http://www.siliconsec.com）并且担任总裁，同时在 AT&T 公司的 Callisma 分部负责安全咨询工作。在加入 AT&T 公司之前，Ido 曾为 Cisco System 工作 4 年多，在 SAFE 工程组同时担任网络安全工程师和网络安全构架师。

关于技术审校人

Randy Ivener，CCIE #10722，是 Cisco 公司产品安全事件调查组的一名专家。他拥有 CISSP 和 ASQ CSQE 证书。Randy 长期以网络安全顾问的身份帮助多家公司了解并且保护他们的网络。在投身信息安全领域之前，他花了大量的时间在软件开发和培训师的工作上面。Randy 毕业于美国海军学院，并拥有 MBA 学位。

Eric S.Seagren，拥有 CISA、CISSP-ISSAP、SCNP、CCNA、MCP+I、MCSE 和 CNE 证书，有 9 年的计算机领域从业经验。近 7 年的时间中他致力于为一家财富 100 公司提供金融服务。Eric 从接触 Novell 服务器开始他的计算机事业，并且在休斯敦本地的一家小公司进行日常网络诊断和排错的工作。他在金融服务业的主要职责包括服务器管理、灾难恢复、商务持续性协调、千年虫修补和网络弱点评估分析。在过去的几年中，他作为一名 IT 构架师和风险分析师，负责设计和评估高安全、高扩展性、高冗余性能的网络。Eric 居住在德克萨斯州的密苏里。

致　谢

我要感谢我的妻子允许我又一次花那么多的时间写书，没有你，我无法完成这本书。

非常感谢 Brian Ford 给我创造了写作本书的机会我非常庆幸能有机会和 Ido Dubrawsky 合作，希望以后能再有这样的机会。感谢 Brian 和 Ido 给我这样的机会和权利，能够和他们一起共事。对于 Brett Bartow 和 Andrew Cupp，我知道我们一次又一次地让你们疯狂，但我要感谢你们一直以来都不厌其烦地支持着我们，给予我们最大的引导和鼓励，而这些正是我们完成这本著作所必需的。

我要感谢我在 Collective Technologies 和 NetIQ 的同事们给了我完善自我的机会，让我成长成一名真正的工程师。对于 Jeff Pollard，非常感谢你给了我足够的时间让我能完成这本书，每一位能够为你这样的老板工作的员工都是非常幸运的。我同样也要感谢 Geri Williams 在我写这本书的那些深夜里在技术上给予我非常专业的意见。如果我不感谢技术编辑以及文字编辑的话，那就是我的失误，因为你们不仅仅保证了我所写的内容在技术上的精确性，而且让我在对英语的掌握以及写作用词的挑选上比以前更加准确，理解更加彻底。

最后，要感谢我的家人和朋友给予了我倾力的支持和鼓励。

——Wes Noonan

首先，最重要的是我要感谢我的妻子，我深爱并珍爱着的妻子，没有她就没有今天的我。其次，我希望把我的谢意转达给我天真可爱的孩子们，他们真的是我生命的明灯。我离开家很长时间去写这本书，我多希望能够有一点点时间和我的家人在一起，但是抽不出来。我整颗心都充满了对你们的爱意。

我同样也要感谢 Wes Noonan 愿意与我合作此书，感谢 Brett Bartow，你是如此有耐心的编辑。这个计划是对我，也是对他们俩的一次考验。我还要感谢 Brian Ford 把我领进这个项目中来，并且在我失落的时候不厌其烦地做我的听众。

我的朋友 Ben Bazian 是我的开心果，在我需要的时候能给我很好的建议，所以我想把最真诚的感谢送给他。同样真诚的谢意我也想带给 AT&T 公司安全咨询实践部门最杰出的地区主管 Nigel Willson。我还想要感谢在国会图书馆的海岸无线电台和我一起共事的 Ricardo Farraj-Ruiz，Charles Outlaw 和 Karl Weaver，他们都很优秀。最后，同样真诚的谢意要送给在 AT&T/Callisma 工作的 David Barak 和 Peter Griffin。David 在服务提供商（Service Provider）网络路由方面知识的博大精深让我惊讶。

——Ido Dubrawsky

前　言

防火墙是今天在因特网上的安全网络的重要组成部分。本书面对在核心网络和终端用户工作的网络管理员，他们正需要一个机会去学习现代防火墙的性能。本书并不是针对所有可能的防火墙的详尽参考手册，也不是针对防火墙的完全文档，而是提供了坚实的基本原理，让读者可以去构建他们在防火墙管理和实施方面的知识库和技能（包括一般的安全领域）。

写作动机

本书的意图在于提供基本防火墙工作原理的信息，倾向于介绍个别防火墙设备，如 Linksys 和 Cisco PIX 501E，同时还包括个人防火墙，如 Windows 防火墙。尽管市面上的防火墙产品非常多，但是因为技术的规范，基本的工作原理都大同小异。本书希望能够让读者了解这些基本原理。

目的和目标

本书的目的是给读者提供一份现成的防火墙技术方面的参考手册，特别是什么地方适合使用个人或桌面的防火墙。读者可以从本书中获得足够的知识，进而有能力从本书末尾所提供的其他的参考手册中去学习更多、更广泛的关于这一类在网络安全方面非常重要的设备的知识。

目标读者

本书的目标读者是网络管理的初学者、家庭用户和那些希望使用防火墙来保护他们网络的远程办公的公司雇员。本书的目的不是介绍所有防火墙以及其所用性能，而是重点介绍一小部分防火墙，如 Cisco PIX 501E、Linksys，以及个人防火墙（如 Windows 防火墙和趋势科技防火墙）。本书假设读者已经掌握了一些基本的网络知识和计算机操作

系统的知识。

本书是如何组织的

本书采用积木（building-block）方式来组织材料。最初着重防火墙基础以及 TCP/IP 回顾。尽管本书应该按照章节阅读，但是也可以根据不同的产品和概念针对性地阅读。第 1 章到第 3 章介绍了与防火墙相关的必要的背景知识和 TCP/IP 概念。核心内容是第 2 部分和第 3 部分，这部分重点介绍不同的防火墙是如何工作的，以及如何管理防火墙。

以下是各章节的主要内容：

第 1 章，“防火墙简介”——本章介绍了什么是防火墙，讨论了防火墙最适合用来做什么。重点是在什么是防火墙，有些什么样的安全威胁的存在，什么是防火墙的安全策略和怎样用防火墙来保护面临的威胁。

第 2 章，“防火墙基础”——本章覆盖了不同的防火墙技术。重点在于解释软件防火墙，综合的防火墙和应用类防火墙。更进一步地把防火墙分成多种实施模式，比如个人、网络、NAT、代理、电路和透明模式防火墙，同时也介绍了它们是如何工作的。

第 3 章，“防火墙中的 TCP/IP”——本章简单介绍了 TCP/IP，并且从防火墙管理的角度介绍了 TCP/IP 的作用。对 TCP/IP 领域不同的协议、应用和服务都作了回顾，特别着重介绍 IP、TCP、UDP 和 ICMP（介绍了如何配置防火墙去控制它们）。

第 4 章，“个人防火墙：Windows 防火墙和趋势科技 PC-cillin 软件”——本章包括了那些能够被找到并且能被安装在膝上电脑和桌面电脑系统中的个人防火墙。两种在本章中介绍的实例系统是 Windows 防火墙（在 Windows XP 的 SP2 版本和 Windows 2003 服务器版系统中存在）和趋势科技防火墙（因特网安全组建中的一部分）。

第 5 章，“宽带路由器和防火墙”——本章介绍了什么是宽带路由器 / 防火墙，它是如何工作的，应该在什么地方去实施它以及如何去实施。本章的重点是 Linksys 宽带路由器，并且讨论了其基本特性和提供了必要的功能去实施完成一个初始化配置。

第 6 章，“思科 PIX 防火墙和 ASA 安全应用”——本章介绍了思科低端的防火墙 PIX 501E 和 PIX 506E。这些设备被定位在终端用户 / 小型办公室和远程办公室市场。本章简单介绍了一部分 PIX 的功能，同时也介绍了如何去进行一个初始化配置。

第 7 章，“基于 Linux 的防火墙”——本章介绍了基于 Linux 防火墙的演化过程，从 ipfwadm 到 ipchains，再到最新的成品 NetFilter。另外，本章也提供了针对基于 Linux 防火墙的简单配置。

第 8 章，“应用代理防火墙”——本章介绍了什么是应用代理，它是如何工作的，它应该实施在什么地方以及如何实施。本章重点介绍微软 ISA Server 2004 防火墙，讨论了其基本特性和实施完成一个基本配置的必要功能。

第 9 章，“防火墙在网络上的位置”——本章重点在于设计和构建防火墙的实施，讨论了不同的防火墙设计结构，包括双重防火墙和不同类型的非军事化区域（DMZ）实施。本章还研究了不同种类的防火墙，以及每种类型的防火墙在网络中最合适的安放位置。

第 10 章，“防火墙安全策略”——所有防火墙的功能都是通过如何配置防火墙安全策略来实现的。本章涉及了不同种类的防火墙存在于入口和出口的安全策略和规则，同样也提供了如何进行安全的管理性接入。

第 11 章，“管理防火墙”——防火墙的管理是一个至关重要的话题。防火墙变得越来越复杂，对于一般水平的用户和初级管理员来说，防火墙的配置和管理也变得越来越难。本章介绍了一些用来管理个人和小型防火墙的管理工具。

第 12 章，“防火墙能告诉我们什么”——一些非常重要的信息可以从防火墙的日志文件中获得。本章阐述了大部分防火墙支持的一些日志种类以及从这些日志中分别能获得哪些信息。本章解释了如何从提供的日志中去读出信息，如何用这些获得的信息去做辩论分析。本章同样也指明了在日志文件中查找信息时最关键的 10 件事。

第 13 章，“防火墙排错”——无论多么完美地实施防火墙，迟早需要对防火墙进行错误排查。本章说明了如何创建故障排查清单以用来对穿越防火墙的数据流进行排错（同样包括防火墙本身）。

第 14 章，“防火墙高级特性”——本章研究了防火墙所能提供的很多高级特性，同时阐明了在防火墙运用这些高级特性时的限制。

附录 A，“防火墙和安全工具”——本附录列出了防火墙和安全工具的清单，并且简要地讨论了每一种工具的作用和适用的环境。

附录 B，“防火墙和安全资源”——本附录列出了用于额外学习的在线或早期出版的资源。这些资源能够在读者通过本书的学习已经掌握基础知识和基本原理的基础上进一步提供更坚实、更具体的技术信息资源。

本书使用的图标

命令语法约定

本书中用于表示命令的语法约定与 IOS 命令参考手册中使用的一样。命令参考手册描述的约定如下：

- 用**粗体字**表示按字面显示输入的命令和关键字。在实际的配置范例和输出中（不

是通用命令语法中），粗体字表示用户手工输入的命令（比如 **show** 命令）。

- 用*斜体*字表示必须提供的实际值或参数。
- 用竖线（|）隔开互斥的元素。
- 用方括号（[]）表示可选元素。
- 用大括号（{}）表示必不可少的选项。
- 用（[{}]）表示可选元素中必不可少的选项。

目　录

第一部分　认识防火墙

第二部分　防火墙如何工作

第三部分 管理和维护防火墙