HZ BOOKS

Linux防火墙

Linux Firewalls

(原书第3版)

Third Edition

(美) Steve Suehring
Robert L. Ziegler 著
何泾沙 等译

Novell PRESS™

Novell

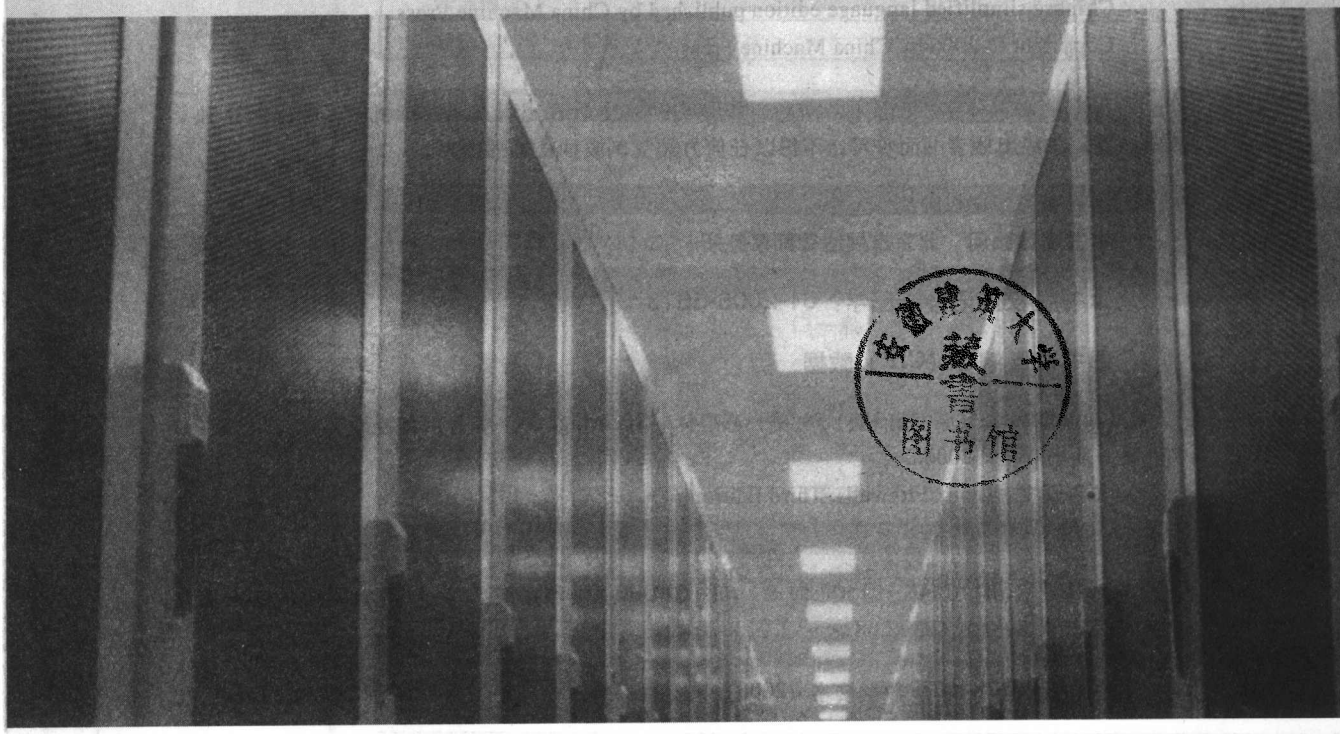
机械工业出版社
China Machine Press

Linux防火墙

(原书第3版)

Linux Firewalls

Third Edition



(美) Steve Suehring
Robert L. Ziegler 著
何泾沙 等译

机械工业出版社
China Machine Press

本书详细介绍Linux操作系统中构建防火墙的方法，以及入侵检测和系统安全的技术。主要内容包括：防火墙的基础知识，Linux防火墙管理程序iptable，构建防火墙的方法，防火墙的优化，数据包的转发，网络监控和攻击检测，内核强化等。本书独立于Linux某个发行版本，涉及常驻于Linux内核的Netfilter核心软件。可帮助读者掌握Linux系统与网络安全技术。

本书条理清晰，图示丰富，可供各类计算机专业技术人员参考。

本书版权登记号：图字：01-2005-5613

图书在版编目（CIP）数据

Linux防火墙（原书第3版）/（美）苏哈林（Suehring, S.）等著；何泾沙等译. －北京：机械工业出版社，2006.6

书名原文：Linux Firewalls, Third Edition

ISBN 7-111-19023-8

Ⅰ. L…　Ⅱ. ① 苏…　② 何…　Ⅲ. ① Linux操作系统　② 计算机网络－防火墙　Ⅳ. ① TP316.89　② TP393.08

中国版本图书馆CIP数据核字（2006）第039597号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码 100037）

责任编辑：乔翠梅　李红玉

北京牛山世兴印刷厂印刷·新华书店北京发行所发行

2006年6月第1版第1次印刷

186mm×240mm · 23印张

定价：46.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

译 者 序

随着计算机和互联网技术的快速发展以及在越来越多的应用领域中的迅速普及，人类对计算机和互联网的依赖程度越来越高，因此增强计算机系统以及互联网络的安全性能也变得越来越重要。然而，实现计算机系统的安全，尤其是实现对采用分布式方式进行运行和管理的互联网络的安全是一个复杂而且技术难度较高的工作，充满了挑战性，近年来也是一个极具活力的研究和开发领域。

防火墙作为互联网络中使用最广泛的安全措施之一，伴随着近年来互联网的快速发展而得到广泛的应用，同时也被实践证明是至今为数不多的成功的网络安全应用实例。然而，防火墙的技术开发以及准确的系统配置和管理对于正确地发挥其在安全方面的功能至关重要。因此，专用的防火墙设备价格昂贵，对技术和管理人员的要求也很高。另一方面，Linux作为目前唯一在全球范围内得到广泛接受和应用的开源操作系统，所提供的灵活性和可操作性为开发和配置防火墙以及按照特定网络环境的要求构建防火墙提供了一个价格低廉、性能优良的平台，日益获得了众多企业和个人用户的广泛接受。

本书是最新的第3版，着重介绍了如何使用Linux操作系统提供的各种机制构建有效的软件防火墙。本书还介绍了互联网环境中防火墙技术的相关内容，如入侵检测、系统安全等。因此，本书适合希望对防火墙的基本概念和知识进行系统了解的人士，也适合对Linux操作系统及其安全已经有了一定程度的了解，但是希望在此基础上对此领域中的技术和应用进行更进一步学习和了解的人士。本书从防火墙的基本概念入手，重点介绍了如何基于Linux操作系统中提供的各种机制和手段构建、配置和管理防火墙，并且讨论了在此基础上如何实现更加完善的网络安全功能并对其进行有效管理的方法，如数据包转发、网络地址变换、入侵检测、网络监控等。因此，本书是一部浅入深出、含量丰富的技术书籍，适合在企业中从事系统安全方面的广大技术和管理工作人员以及家庭用户阅读和学习。

本书由北京工业大学教授、博士生导师、软件学院副院长、北京市特聘教授何泾沙博士负责翻译。北京工业大学软件学院研究生刘辉、王海兰、吴丽和李波参与了部分章节的翻译和校对工作。全书由何泾沙进行统稿及审校。由于译者的水平有限，加上时间上的限制，本书的翻译中难免存在不妥之处，敬请广大读者批评指正，译者在此深表谢意。

前　言

本书主要介绍如何在Linux操作系统中使用Netfilter和iptables构建一个基于软件的防火墙。除了介绍防火墙的基础知识，本书还进一步在网络计算的环境中对防火墙进行更加深入的阐述。最后，我们还将探讨入侵检测和系统安全等主题。

计算机安全是一个不断发展的研究领域。目前已经有很多关于这方面的书籍，并且这方面的书籍还会持续增加。计算机安全始终围绕着如何保护数据这一主题，主要涉及以下三个原则：保密性、完整性、有效性。保密性是指保证数据只能够被得到授权的人访问，而不允许被其他人访问。完整性是指确认数据完好并且没有被损坏。有效性是指当需要访问数据时，就能够正常地访问。这三个原则指导着计算机安全领域中的讨论，并为本书提供了框架。

除了保密性、完整性、有效性这三个原则，我还赞成深入的、基于风险评估的计算机安全方法。虽然防火墙和杀毒软件在保护数据方面起着巨大的作用，但是我并不认为存在着一劳永逸的解决方案。然而，每种安全措施都有一定的成本。因此，每种附加的安全措施或安全层必须要被评估，以保证使用该层所付出的成本不会超过使用该层所带来的好处。

让我们看一下以下示例：我的家庭网络使用了两个防火墙，一个隔断防火墙和一个网关（参阅第6章，“数据包的转发”）。我认为使用两个防火墙带来的好处远大于配置和维护防火墙带来的开销。而有些人只使用单一的防火墙或者根本不使用防火墙。他们认为使用两个或者一个防火墙的成本要高于数据安全所带来的好处。我们还可以找出很多利用“成本收益比”（cost/benefit）进行评估的例子。不幸的是，这种分析在很多安全领域中常常被忽视，而不仅仅是计算机安全领域。如果想要获取关于进行这种分析的更多信息并熟练掌握，请参考Bruce Schneier的著作《*Secrets and Lies*》和《*Beyond Fear*》。

撰写本书的目的

撰写本书的目的首先是给读者提供足够的信息，使其可以利用Linux中的iptables来配置防火墙。本书的另外一个目的是让读者对系统与网络安全有所了解。然而，由于本书并不是系统与网络安全的专著，虽然对系统与网络安全的介绍占据了书中的很大篇幅，但这终究不是本书的主题。同时，本书中涉及的一些话题，我还未看到其他文献有所提及。

本书是第3版，也是新作者Steve Suehring参与修订的第1版。Bob Ziegler撰写了本书的原始材料，并且在2001年修订并完成了第2版。Bob在前两版中的工作非常出色，在他打下的坚实基础上，我编撰出（本书的）第3版。此外，本书以前的版本中有一些内容是由Carl B. Constantine撰稿。Carl修订过的撰稿在本版的附录C中可见。

从1995年开始，在为一家ISP（Internet Service Provider，网络服务提供商）工作的时候，我学到了自己关于Linux安全方面的大部分知识。那时我主要学到的是安全意识。安全意识是网络服务提供商必不可少的，因为对网络服务提供商的基本要求是它必须提供7×24小时的公共接

入服务。这就意味着网络服务提供商所提供的公共服务，时时刻刻都会面临外界袭击网络或侵犯系统的风险。如果不将安全视为运营的核心，那么提供的服务就很难达到客户要求的可靠性，同时我们也不能保证所掌握的数据的完整性。在1995年的时候，尽管安全工具、软件普遍缺乏，也没有书籍像本书一样涉及网络系统安全的问题，但我们仍需提供安全的保障。

以上这个背景也可以帮助解释“为什么选择Linux？”无论过去还是现在，答案都很简单：当面临以及要解决这类问题的时候，Linux和开源工具是当时唯一的解决途径。没有其他的方法能够提供Linux和开源软件所能提供的可靠性。与Linux相比，当时没有其他的操作系统能够在保持总体拥有成本（Total Cost of Ownership，TCO）较低的同时还保证运行的安全性和稳定性。这个状况在今天依然没有太大的变化。单从技术的角度来评价的话，Linux是最出色的。抛去那些有偿研究所取得的成果，考虑总体拥有成本，Linux和开源软件就显得更加优越。为什么选择Linux？因为它是有效的。

本书的读者对象

我在一些书中经常看到近乎无用的“本书的读者对象”部分，这样说是因为那些书的该部分总是试图让你觉得你应该阅读该书。因此，为使出版社满意，我也要告诉你每个人都应该阅读本书。事实上，每个人都应该反复地阅读本书，并且每读一次都应该买一本新书。

然而严肃地说，我无法告诉你是不是应该读这本书，我只想介绍一下这本书。

在读本书之前，你应该已经选择了一个Linux的版本并已将其安装完毕。另外，我还必须假设你现在想要得到的并不是简单地想要了解Linux或Unix操作系统方面简介性的知识，比如chmod命令。那方面的资料很多，你可以在网上找到大量相关信息，但是本书所要讲授的重点和它们相去甚远。然而，本书还是覆盖了大量的基础性内容，如网络安全、数据包过滤以及OSI模型中的层（假如你不太了解OSI模型，本书也会有相应的介绍）。

假如你对防火墙一无所知，或是你对Linux和Linux安全只有很浅的了解，而想在这方面提高一个层次，那么，希望本书对你会有所帮助。本书无论对家庭用户还是对企业中的系统安全管理员都有一定的帮助。

如果想从本书得到最大的收获，你应该基本熟悉、至少不惧怕Linux命令或shell命令。你应该知道如何在文件系统中移动文件以及如何使用基本的shell命令。

Linux的发布

有关Linux和开源方面的书籍应该更加中立于任何发行版或者覆盖多种发行版，本书在这两方面都做到了。建立在常驻于Linux内核的Netfilter核心软件之上，Linux防火墙通过使用iptables防火墙管理程序来构成。因此，它与各种Linux发行版在很大程度上是没有关系的。然而，本书的确包含了一些来自SUSE、Red Hat/Fedora和Debian的命令和观点。我们承认，也有别的Linux发行版，它们中的一些也是很棒的。选择以上这三种发行版并不意味着放弃其他的发行版。

在本书的第2版中只使用了Red Hat。因此，在此修订版中我尽力去除那些只与此发行版有关的内容和写法。这样做并不是为了偏向某一发行版而排斥其他的发行版，而是一种务实的决定，是为了给更多的读者提供实际的应用和防止当读者与作者所使用的发行版不一致时所产生的有

关文件和命令位置的混乱。

本书中的错误

尽管花了很多精力去核对论据、数据、文件和语法，一些错误还是不可避免地会流过拼写检查、技术性编辑、印刷排版和复审的整个过程。我首先对书中还可能存在的错误感到抱歉。我在此也邀请本书的读者访问我的网站，即下面的配套网站，以获得与本书相关的更新以及其他信息。同时有任何反馈信息请发到我的邮箱：steve.suehring@braingia.com。尽管我不能保证会有正确的答案，但我肯定会尽力回答和并且指出一个正确的方向。

配套网站

请访问http://www.braingia.org/，了解有关本书的更新信息以及相关的安全类文章的链接。网站上还包括书中所提供脚本的最新更新。

致谢

首先感谢我的家庭在我每天写作的时候给予我的支持。同样感谢我的代理Studio B的Laura Levin，她做了很多工作并且给予了我不断的支持。还要感谢A. J. Prowant为本项目所做的技术编辑。

Chris和Nikie Tuescher同样值得感谢，他们是最好的朋友并且对我们后来没有去明尼阿波利丝表示理解——因为本书花费了我们大量的时间！感谢Aaron和Jodi Deering请我们到家里吃饭，并感谢Aaron使我在篮球场上十分放松。感谢Duff Damos这么多年来的友谊。感谢Pat Dunn时常在更新密码却很快又忘记它，感谢他的耐心以及不断的帮助。

下面是被感谢人名字的罗列，然而它没有按照一个特定的顺序。虽然他们所提供的帮助并没有能够清楚、准确地表达出来，他们以各种不同的形式（正面或负面的）对本书的撰写做出了贡献。Andy Hale（请让我知道您准备何时能够修复您家的地板）、Dan Noah、Jim & Amy Leu、Kent & Amy Laabs、Michael Mittelstadt、Denise Sandell、Pflugers夫妇、AWRC、Jake Buchholz、Richard Dean Anderson、Aaron Schrab、Beez、Rysch、HFB & #JBS、Guthries夫妇、Heins夫妇、Tim McKeown、Pearl & Moff、Rob Konkol、Erin Thomas、Paul、Darrick、Jeff Sanner、Edward Van Halen、Peter DeLuise、DBAs及数据构架小组、Sarah Hagerman、Jay & Deb Schrank、Brian Page、（还有人在继续往下阅读吗）、Mark Little、Nightmare Squad、Jim Oliva、John Eckendorf、90fm、Scott & Karla Kluck、Amanda Tapping、Steffen夫妇、Eliot Irons、Keith Imlach及数据安全小组、（不，还有人在认真地往下阅读吗）、Sue Crawford、Erich Hartman（顿号是我最好的朋友）、Ron Mackay、Chasteen夫妇、Darrin Davisson、（如果到此时您还没有看到您的名字，就请等到我出版的下一本书吧）、Justin Hoerter、John Hein、Andy Berkvam、互联网络、Mike Wrzinski、、（因为我太喜欢顿号，所以在这里额外多加了一个顿号）、Chris Judge、Tony Falduto、Steve Hannan（我在这里感谢了一位项目经理）、Greg Rubey、Ryan Anderson、Suzi Limberg、Kevin Blake、Dave Dahlke（我感谢的人越多，得到的报酬就越多）、Michael Shanks、Tom Lindley、（这个位置出租）、Kevin Bedell、James Turner、

DeeAnn LeBlanc、Neil Peart、Music Quest的Norm & Crew。

这个名单会很长，就像上一次一样，我确信我会忘掉某些人。我必须在规定的时间内将本书的终稿提交给出版社。如果您的名字没有出现在以上的名单里，请在这里接受我诚挚的谢意，虽然在我写这一部分时忘记了您。

我们希望得到您的反馈

作为本书的读者，你们是最重要的评论家。我们希望您能让我们知道哪些方面是做的好的，哪些方面应该做的更好，任何富有智慧的建议都是受欢迎的。

您可以给我发电子邮件或者直接给我写信，让我知道您是否喜欢此书——这样做可以让本书更加出色。

请注意我不能帮你们解决关于本书的技术问题。同时，因为邮件的数量过于庞大，所以有时候不能回复所有的邮件。

当您写信时，请包含本书的书名以及作者的名字，当然还要写上您的名字、邮件地址以及电话号码。我会认真阅读您的评论并与作者和编辑来分享它们。

邮件地址：feedback@novellpress.com

邮寄地址：Mark Taber
Associate Publisher
Novell Press/Pearson Education
800 East 96th Street
Indianapolis，IN 46240 USA

读者服务

要想从Novell出版社获取本书更多的信息，请访问我们的网站：www.novellpress.com。键入ISBN或者书名就可以搜索到您想要找的页面。

目　录

第二部分 高级议题、多个防火墙和网络防护带

第三部分 超越iptables

附 录

第一部分 数据包过滤及基本安全措施

第1章 防火墙的基本概念

小型站点可以通过T1线路、电缆调制解调器、DSL、IDSN、无线网络或使用电话线建立PPP连接的拨号账号来访问Internet。直接连到Internet上的计算机是安全问题的焦点。无论是一台计算机还是由连接起来的计算机组成的一个局域网（Local Area Network，LAN），小型站点关心的焦点是与Internet直接相连的机器，这台机器就是防火墙。

防火墙（firewall）根据其实现和目的的不同有许多含义。在本书开头部分，防火墙是指与Internet相连的机器，这里是你实施安全策略的地方。防火墙的外部接口卡是与Internet的连接点或网关。防火墙的任务是保护这个网关在你这一边的东西，防范来自另一边的东西。

一个简单的防火墙设置有时被称为堡垒（bastion）防火墙，因为它是对抗来自外界攻击的主要防线。所有安全措施都安装在领域内的这个防御者上。这样，防火墙尽其所能来保护系统。

在这条防线之后是单台计算机或计算机组。防火墙的任务也许只是简单地作为LAN上其他机器到Internet的连接点。你可以在这台防火墙后面运行本地的私有服务，诸如共享打印机或共享文件系统，或者你也许想要所有计算机都能访问WWW，但其中一台机器可能保存着个人财政记录。你也许想从这台机器上访问Internet，但并不想任何人访问这台主机。在某种情况下，你也许想要向Internet提供服务，其中一台机器也许可以成为Internet的Web站点，也许还要提供邮件服务器或网关的功能。你的设置和目标将决定你的安全策略。

防火墙的任务是执行你定义的安全策略。这些策略反映了哪项服务是你想让你的计算机能够被访问的，哪项服务是你想提供给外界的，哪项服务是你想提供给特定的远程用户或站点的，哪项服务或程序是你个人在本地机器上运行的。安全策略是所有关于计算机上私有的或受保护的服务、程序和文件的访问控制和授权使用。

家庭和小型商业系统没有大企业站点所面临的所有安全问题，但基本的想法和步骤是一样的。只是不需要考虑太多的因素，并且安全策略不像大型商业站点那样严格。重点是保护你的站点不受来自Internet的不受欢迎的访问。数据包过滤防火墙是常见的一种方法，是网络安全的一部分，它控制内部和外部的访问。

当然，拥有防火墙并不意味着完全的保护。安全是一个过程，而不仅仅是一个硬件。例如，即使防火墙正常工作，下载间谍软件或者单击了一封精心掩饰的恶意电子邮件也是有可能的。于是打开电脑，网络就会遭到攻击。采取正确的措施来减少成功的入侵带来的危害和在防火墙硬件方面投入大量资金同样重要。将最好的安全经验应用于局域网将有助于减少成功入侵的影响，并且能提高网络的弹性。

需要记住的是Internet应用的前提是基于端与端之间相互透明的连接。两台正在通信的机器之间的网络对于它们是不可见的。实际上，如果网络中某台设备无法正常工作，那么这两台计算机之间的数据将会被重新路由，而两端的计算机并不知道。

理想情况下，防火墙应该是透明的。否则，哪怕两台端点计算机之间的网络出现了一丁点失误，都会阻止Internet应用。另外，并不是每个网络应用都使用容易从简单的数据包过滤防火墙通过的通信协议。使特定数据流通过没有额外应用支持和技术更加复杂的防火墙是不可能的。

更复杂的问题是网络地址转换（Network Address Translation，NAT）的引入。NAT使一台计算机可以通过翻译其他计算机的请求并把它们转发到目的地来为其他机器工作。伴随RFC 1918私有IP地址出现的NAT已经有效地预防了IPv4地址过于虚幻的缺点。NAT和RFC 1918地址空间的结合使某些类型的网络传输变得困难、不可能、复杂或昂贵。

注意　许多路由设备（特别是服务于DSL、电缆调制解调器和无线网络的），被当做防火墙出售，而它们却只不过是支持NAT的路由器而已。它们无法实现真正的防火墙所具有的众多功能，但确实将网络内部与外部分开。当购买声称能作为防火墙使用的路由器时，应该知道它只不过是提供了NAT功能而已。尽管部分产品有很好的特性，但更高级配置有时根本不可能达到。

最复杂的一直是多媒体和用于实时通信软件和流行网络游戏的点对点（peer-to-peer，P2P）协议的使用。这些协议不利于当今的防火墙技术。现在对于不同的应用协议需要开发和使用专门的软件。能够轻松并且经济地处理不同协议的防火墙体系正在标准委员会工作小组的研究之中。

需要注意的是防火墙、DHCP、NAT的结合增加了网络的复杂性，从而使网站为了提供用户期望的服务不得不加强系统的安全性能。小企业常常不得不使用多个LAN和复杂的网络配置来满足本地服务器的不同的安全需要。

在讲解开发防火墙的细节之前，先介绍一下数据包过滤防火墙所基于的基本概念和机制。这些概念涉及一个大体的框架，包括什么是网络通信，基于网络的服务是如何被定义的，什么是数据包，消息和网络中计算机之间传输的信息的类型。

1.1　OSI网络参考模型

OSI（Open System Interconnection）模型表示一种层次型的网络架构。OSI模型中的每一层都提供了相关于其他层的独特功能。OSI模型包括七层，如图1-1所示。

有时用数字来表示各层，如最低层（物理层）为1层，最高层（应用层）为7层。若有人说3层交换机，就是指OSI模型的第三层。如果对安全和入侵检测感兴趣，那么必须知道OSI模型的各层才能清楚各种可能危及你的系统的攻击方式。

OSI中每一层都很重要。每天使用的各种协议，例如IP、TCP、ARP、NFS等，都是基于模型中的各层的。每一层在通

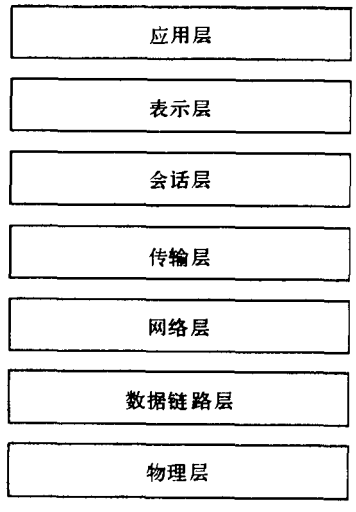


图1-1　OSI模型的七层

信过程中都有它独特的功能和角色。

物理层被介质本身所使用，像电报和相关的信号发送协议，换句话说，即传输数据位。一般物理层较少关心网络入侵分析，而关注于保证设备和电缆的安全。因为本书并没有打算谈论物理性的安全问题（门锁是多么的有趣？），所以也不会在物理层上花很多时间。当然，加强物理线路的安全性不同于保护无线设备。

物理层的上一层是数据链路层。数据链路层在给定的物理介质上传送数据，并负责传输中的检查和错误恢复之类的工作。数据链路层亦定义硬件的物理地址，像以太网卡的MAC（Media Access Control）地址。

数据链路层之上的网络层是IP网络中的第三层，也是最重要的一层，它负责逻辑地址和数据的路由。IP是网络层协议，就是说网络层使用IP地址和子网掩码。路由器和部分交换机工作在第三层，用来在逻辑和物理上分开的网络间传送数据。

网络可靠性主要建立在第四层（即传输层）上。传输层上的协议包括TCP和UDP。第五层是会话层，在这一层上端点之间的会话被建立。第六层即（表示层）主要同它上面的应用层进行通信，同时也定义一些像加密之类的服务供使用。最后，应用层负责向用户或应用程序显示数据。

除了OSI模型，还有一个模型是DARPA模型，有时也被称为TCP/IP参考模型，它只有四层。OSI模型已经成为传统或事实上的模型，大多数的讨论都在这个模型上进行。

当数据从应用层传送到OSI模型的各层时，下一层的协议可能会在数据中加一些自己的信息。本层的数据通常包含由上层协议加在数据上的数据头，有时也会有数据尾。这个过程（被称为封装）持续到数据从物理介质传送完毕。当以太帧到达目的地时，开始在OSI模型中自底向上传送，每一层都会读取来自发送方相应层的头部（或可能的尾部）信息。这个过程被称为多路分解（demultiplexing）。

1.1.1 面向无连接协议和面向连接协议

在OSI模型的一些层中，协议根据层的某种特性来定义，如无连接还是面向连接。这种定义涉及协议包括的一些方法，例如错误控制、流控制、数据分段和数据重组。

把面向连接的协议想像成打电话。通常有一个合适的协议来生成和维持通话。拨号方即通话的发起者，通过拨号来开始。另一端的接收者（或机器，这种情况越来越多）接受请求并开始通话。用于初始化电话交谈的请求通常通过接收端的电话铃声来指示。接收方拿起电话说“Hello”或其他的问候语。拨号方随后通过对问候的回应来确认通话。这时，可以说通话被安全地建立起来了。之后，交谈便继续。通话期间如果出现问题，如通话有噪音，一方便会让另一方重复刚才的话。通常当通话完成时，双方会说“Good-bye”来告诉对方通话结束。随后，通话便结束了。

刚才的例子给出了一个并不十分完整的面向连接协议（如TCP）的场景。规则都有例外，TCP协议也有例外或出现错误的情况。例如，由于不受发送方和接收方控制的技术原因也许导致呼叫的初始化失败。

另一方面，无连接协议更像邮局投递的明信片。发送方在明信片上写下信息投到邮箱，便失去了对信息的控制。明信片投递成功后，发送方不会收到直接的确认通知。UDP和IP本身都是无连接的例子。

1.1.2 下一步

从这里将对IP（Internet Protocol）协议进行更细节的探讨。但我还是强烈要求读者多花些时间来学习OSI模型和协议本身。协议和模型的知识对安全专家是必需的。极力推荐W. Richard Stevens的《*TCP/IP Illustrated*》第一卷，这是一本每个计算机专家的桌子上都不会缺少的好书。

1.2 IP协议

IP协议是Internet运行的基础。IP协议和其他层的协议为无数的应用提供通信。IP是提供第三层上的路由功能的无连接协议。

1.2.1 IP地址分类和子网划分

也许读者已经很清楚了，但还是不得不介绍一下，IPv4的IP地址由被多个点分开的32比特位组成，称做“点分”标记法。同样，尽管大家都理解或至少见过IP地址，但越来越少的人能理解子网划分和子网掩码，它们是IP地址分类方案的重要部分。本节将简单介绍一下IP地址分类和子网划分。

IP地址被分类而不是作为完全一样的地址空间。IP地址的分类如表1-1所示。

表1-1　Internet地址

类　型	地址范围
A	0.0.0.0～127.255.255.255
B	128.0.0.0～191.255.255.255
C	192.0.0.0～223.255.255.255
D	224.0.0.0～239.255.255.255
E（未分配）	240.0.0.0～255.255.255.255

在实际应用中，只有A～C类地址经常被使用。读者可能也使用过D类地址，它们通常是用于广播。E类地址未分配使用。

特殊的IP地址

主要有三类特殊的IP地址：

- **网络地址0**：在A类地址中，网络地址0不是可路由的地址部分。当作为源地址时，唯一合法的使用是在初始化时主机用来动态地得到由服务器分配给自己的IP地址。当用做目的地址时，只有地址0.0.0.0有意义，并且只能用于本地机器标识自己或作为惯例指示默认的路由。
- **回环网络地址127**：A类地址中，网络地址127不是可路由的地址部分。回环地址是操作系统支持的专用网络接口。它用于本地网络服务的地址分配机制。换句话说，本地用户用它来标识本地服务器。回环流量完全保持在操作系统内，而不会被送到物理的网络接口。代表性地，127.0.0.1作为唯一的回环接口指向本地主机。
- **广播地址**：广播地址应用于网络内所有主机。广播地址主要有两类，有限广播不被路由但会被送到相同物理网络段上的所有主机。IP地址的网络字段和主机字段全为1就是地址255.255.255.255。直接网络广播会被路由，并被送到专门网络上的每台主机，IP地址的网