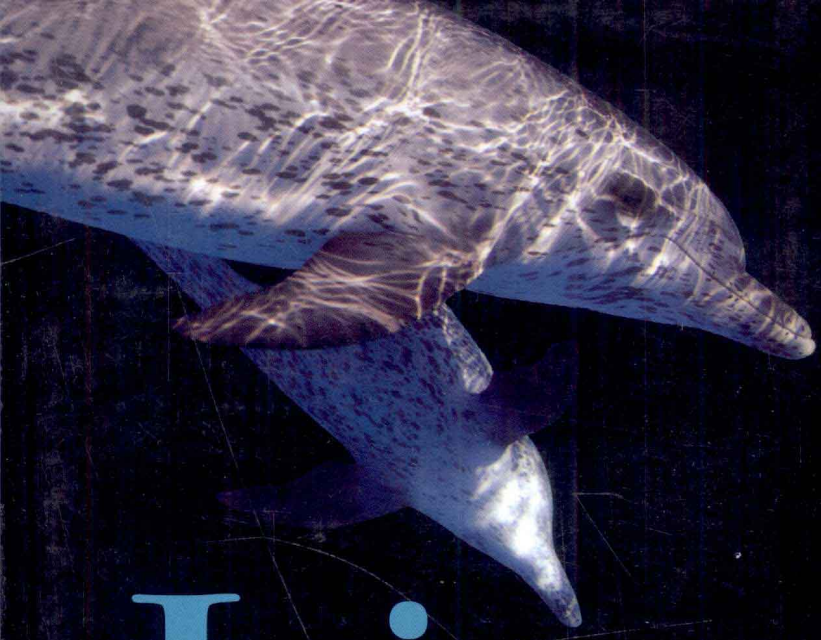


悦知文化
Delight Press

Linux

网络安全技术与实现（第2版）

极其灵活的防火墙使用技巧
全面的带宽合并和管理知识
您必须知晓的透明式防火墙
常见网络攻击以及防御之道
防火墙硬件评估和性能优化

redhat
CERTIFIED
ENGINEER

陈勇勋　著
黄　强　审校

清华大学出版社

Linux 网络安全技术与实现(第 2 版)

陈勇勋　　著

黄　强　　审校

清华大学出版社

北　京

Linux 網路安全技術與實現(第 2 版)
陈勇勋
精誠資訊股份有限公司-悦知文化，2011.07
ISBN: 978-986-6072-14-7

图书在版编目(CIP)数据

Linux 网络安全技术与实现(第 2 版)/陈勇勋 著；黄强 审校. —北京：清华大学出版社，2012.3
ISBN 978-7-302-27886-3

Ⅰ. L…　Ⅱ. ①陈…　②黄…　Ⅲ. Linux 操作系统—安全技术　Ⅳ. TP316.89

中国版本图书馆 CIP 数据核字(2012)第 008395 号

责任编辑：王　军　韩宏志
封面设计：康　博
责任校对：蔡　娟
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：32　　**字　　数**：655 千字
版　　次：2012 年 3 月第 1 版　　**印　　次**：2012 年 3 月第 1 次印刷
印　　数：1～4000
定　　价：68.00 元

产品编号：044541-01

推荐序

现在开源软件日趋丰富，熟悉这个领域的技术人才也越来越多，这对企业，尤其是中小企业来说不啻是一大福音。

企业信息系统包含各种不同用途、不同规模的服务器以及各种应用程序，在规划系统时，规划人员必须谨慎考虑哪些位置上可以使用免费资源；在这方面，那些使用者直接接触不到，但又必不可少服务器可以作为重点考虑对象。本书使用Linux实现网络安全就是一个很好的例子。信息安全极其重要，但如果考虑到成本，每个企业管理者都会犹豫一番，毕竟还没有遇到问题就要先投入一大笔钱，其紧迫性显然不如将钱花在直接与业绩挂钩的事情上。但如果安全成本较低，并且掌握这种技术的人才又容易找到，企业管理者将可以放心地、大刀阔斧地部署安全解决方案。

本书就是要提供这样的解决方案，不管是为自己的公司降低信息系统的成本，或是为别的公司建设新的系统，本书都有极高的参考价值。如果你已经是Linux相关的技术人员，本书会提高你的应用能力；如果你是Windows平台的技术人员，本书会增加你跨领域就业的资本。

作者陈勇勋常年研究Linux的相关技术，教学经验丰富，已经撰写了多本畅销著作。他一直以推广开源软件的应用为己任，在这个领域的技术研究上投入了很多心血，相信由他来编写本书，可以让读者快速掌握Linux安全技术知识并将所学技术得心应手地运用于实际工作中。

张智凯

Richard Chang

精诚资讯知识产品事业部处长

作者序

很多年前我就一直想撰写本书，只是时间上实在不允许，如今总算了结了多年来的一桩心愿，我为此感到十分欣慰。当然这还要感谢屠立刚和唐任威两位老师，他们总是恰逢其时地为我提供理论指导，使我得以突破许多盲点来完成这一著作。

在接触因特网的这16年来，我亲眼目睹Linux系统不断和成长和完善，心中总有一种莫名的感动，因为背后的功臣竟是一群不求回报的、夜以继日默默付出的志愿者，而他们的成果却足以抗衡拥有千亿资产的商业公司，甚至超越了他们的产品。由于缺少市场营销的推动，Linux系统的市场占有率始终不高，当然这样也就埋没了Linux许多令人赞赏的功能，如防火墙(Layer2、3、7)、流量控制(Traffic Control)、基于策略的路由(Advance Routing)、虚拟专用网络(Virtual Private Network)等，这也是激发我撰写本书的动力；我的下一个目标是完成《Linux系统虚拟化技术》一书，请大家拭目以待吧！

本书可分为安全、基于策略路由、流量控制及通信安全四大部分，主要内容如下。

■安全

以Linux内置的Netfilter为主线，介绍Netfilter模块的用法及组合应用上的技巧，再逐步延伸出应用层防火墙(Layer 7 Firewall)及透明式防火墙(Transparent Firewall)的技术原理及应用，还讨论如何结合反向代理机制来确保企业网络的安全。

■基于策略的路由

基于策略的路由一直都是网络管理人员梦寐以求的利器。有了基于策略的路由之后，你可以将网络上所有的数据包玩于股掌，例如，所有http数据包经由第一条ADSL连接因特网，企业中一半的客户端使用第一条ADSL、另一半的客户端使用第二条ADSL，甚至还可以做到让企业对外的网络连接平均分摊到多条ADSL上等高难度的网络管理操作。其实市场上很多负载均衡设备就是使用Linux来搭建的，而且这个功能通常只存在于价格高昂的商用路由器之上。

■ 流量控制

讲述如何使用Linux内置的流量控制功能来管理网络上的流量；除了传统上以IP及端口的方式来限制流量之外，也将介绍如何使用应用层协议来控制流量，以便轻松地管理企业对带宽的使用。

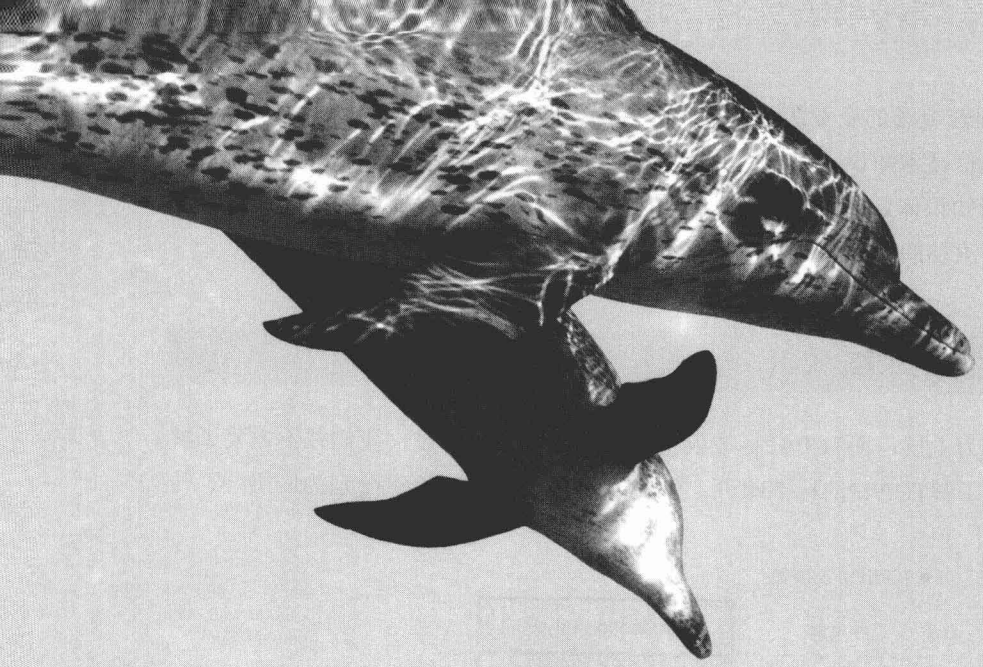
■ 虚拟专用网络

由于企业海外分部的建立及无线上网的普及，使得网络通信安全主题受到人们的重视，VPN硬件设备也因此逐渐流行起来。这样的设备通常价格不菲，但我们只要巧妙使用Linux系统，就可以建立起适于企业使用的VPN系统。

只要你能随着本书的章节循序渐进地学习，一定可以很快将Linux系统应用于企业网络安全的管理上。

陈勇勋

目　录



Linux

第1章 防火墙的基本概念

1