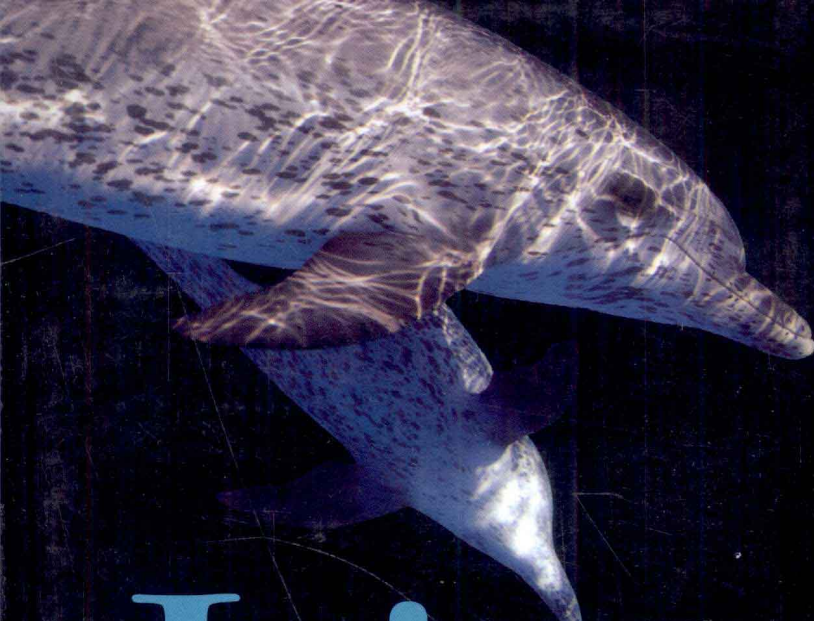




Linux

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



陈勇勋
黄强

著
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

本书为精诚资讯股份有限公司-悦知文化授权清华大学出版社于中国大陆(台港澳除外)地区之中文简体版本。本著作物之专有出版权为精诚资讯股份有限公司-悦知文化所有。该专有出版权受法律保护, 任何人不得侵害之。

本书封面贴有清华大学出版社防伪标签, 无标签者不得销售。

版权所有, 侵权必究。侵权举报电话: 010-62782989 13701121933

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系统不断成长和不断完善，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

第 1 章 防火墙的基本概念	1
1.1 TCP/IP的基本概念	2
1.1.1 应用层	2
1.1.2 传输层	3
1.1.3 网络层	4
1.1.4 链路层	4
1.2 数据包传输	4
1.3 TCP、UDP及Socket的关系	9
1.4 何谓防火墙	12
1.5 防火墙的判断依据	14
1.5.1 各层数据包包头内的信息	14
1.5.2 数据包所承载的数据内容	16
1.5.3 连接状态	16
1.6 防火墙的分类	17
1.6.1 数据包过滤防火墙	17
1.6.2 应用层防火墙	18
1.7 常见的防火墙结构	19
1.7.1 单机防火墙	19
1.7.2 网关式防火墙	20
1.7.3 透明防火墙	24
1.8 小结	24
第 2 章 Netfilter/iptables	25
2.1 何谓内核	26
2.2 何谓Netfilter	27
2.3 Netfilter与Linux的关系	27
2.4 Netfilter工作的位置	28
2.5 Netfilter的命令结构	30
2.6 Netfilter的filter机制	31

2.7	规则的匹配方式	35
2.8	Netfilter与iptables的关系	36
2.9	iptables工具的使用方法	38
2.9.1	iptables命令参数	38
2.9.2	iptables规则语法	48
2.9.3	学以致用: iptables的规则语法	56
2.10	使用iptables机制来构建简单的单机防火墙	57
2.10.1	如何测试防火墙规则正确与否	59
2.10.2	解决无法在防火墙主机上对外建立连接的问题	62
2.10.3	管理防火墙规则数据库的办法	68
2.11	使用filter机制来构建网关式防火墙	71
2.12	Netfilter的NAT机制	73
2.12.1	IP网段的划分	73
2.12.2	私有IP	74
2.12.3	NAT	74
2.12.4	数据包传输方向与SNAT及DNAT的关系	76
2.12.5	NAT的分类	79
2.12.6	NAT并非无所不能	86
2.13	Netfilter的Mangle机制	86
2.14	Netfilter的raw机制	89
2.15	小结	91
第3章	Netfilter的匹配方式及处理方法	93
3.1	匹配方式	94
3.1.1	内置的匹配方式	94
3.1.2	从模块扩展而来的匹配方式	98
3.2	处理方法	139
3.2.1	内置的处理方法	139
3.2.2	由模块扩展的处理方法	142
3.3	小结	153
第4章	Netfilter/Iptables的高级技巧	155
4.1	防火墙性能的最优化	156

4.1.1	调整防火墙规则顺序	156
4.1.2	巧妙使用multiport及iprange模块	158
4.1.3	巧妙使用用户定义的链	158
4.2	Netfilter连接处理能力与内存消耗	159
4.2.1	计算最大连接数	160
4.2.2	调整连接跟踪数	160
4.2.3	连接跟踪数量与内存消耗	161
4.3	使用raw 表	162
4.4	简单及复杂通信协议的处理	163
4.4.1	简单通信协议	163
4.4.2	复杂通信协议	164
4.4.3	ICMP数据包的处理原则	171
4.4.4	在DMZ上使用NAT将面临的问题及解决方案	172
4.4.5	常见的网络攻击手段及防御方法	175
4.5	小结	191
第 5 章	代理服务器的应用	193
5.1	何谓代理服务器	194
5.2	代理服务器支持的通信协议	195
5.3	代理服务器的分类	195
5.3.1	何谓缓存代理	195
5.3.2	何谓反向代理	196
5.4	代理服务器的硬件要求	197
5.5	安装Squid代理	198
5.6	使用Squid构建缓存代理	199
5.6.1	缓存代理的基本配置	199
5.6.2	缓存代理客户端的配置	204
5.6.3	缓存代理的高级配置	205
5.6.4	缓存代理连接访问控制	209
5.6.5	缓存对象的管理	210
5.6.6	Squid代理的工作日志	214
5.6.7	Squid代理的名称解析	216
5.7	透明代理	217

5.7.1	透明代理的工作原理	217
5.7.2	透明代理的配置	218
5.8	反向代理	219
5.8.1	Web 服务器的分类	219
5.8.2	构建反向代理	221
5.9	小结	226
第 6 章	使用Netfilter/Iptables保护企业网络	227
6.1	防火墙结构的选择	228
6.2	防火墙本机的安全	230
6.2.1	网络攻击	230
6.2.2	系统入侵	231
6.2.3	入站/出站的考虑事项	231
6.2.4	远程管理的安全考虑事项	232
6.3	防火墙的规则定义	232
6.3.1	企业内部与因特网	232
6.3.2	DMZ与因特网	234
6.3.3	企业内部与DMZ	238
6.4	入侵与防御的其他注意事项	238
6.4.1	更新系统软件	238
6.4.2	Syn Flooding攻击防御	238
6.4.3	IP欺骗防御	241
6.5	小结	242
第 7 章	Linux内核编译	243
7.1	为何需要重新编译内核	245
7.2	内核编译	246
7.2.1	安装软件开发环境	246
7.2.2	获取内核源代码	247
7.2.3	整合源代码	248
7.2.4	设置编译完成后的内核版本号	249
7.2.5	清理内核源代码以外的临时文件	249
7.2.6	设置内核编译参数	250

7.2.7	执行编译操作	252
7.2.8	安装模块及结构中心	253
7.2.9	修改开机管理程序	255
7.3	如何安装内核补丁	257
7.3.1	下载补丁文件及内核源代码	257
7.3.2	准备内核及补丁的源代码	258
7.3.3	运行内核补丁	259
7.3.4	设置内核编译参数	259
7.3.5	内核编译完毕后的检查	260
7.4	小结	260
第 8 章	应用层防火墙	261
8.1	如何为iptables安装补丁	263
8.2	Layer7模块识别应用层协议的原理	264
8.3	安装Layer7模块的模式	265
8.4	如何使用Layer7模块	267
8.5	Layer7模块使用示例说明	268
8.6	结合使用包过滤器与Layer7模块	271
8.7	小结	273
第 9 章	透明式防火墙	275
9.1	何谓桥接模式	278
9.2	何谓透明式防火墙	279
9.3	构建透明式防火墙	279
9.3.1	使用Linux构建网桥	280
9.3.2	Netfilter在Layer3及Layer2的工作逻辑	284
9.3.3	另一种透明式防火墙	290
9.3.4	配置代理ARP	290
9.4	小结	292
第 10 章	基于策略的路由及多路带宽合并	293
10.1	何谓基于策略的路由	294

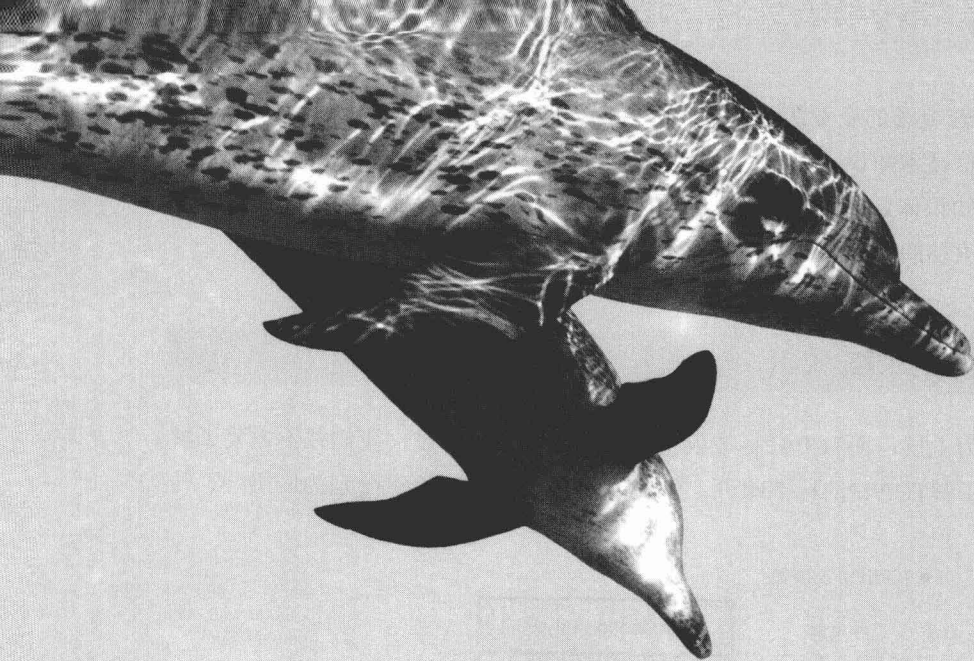
10.2	了解Linux的路由机制	296
10.3	路由策略数据库与路由表的管理	298
10.3.1	管理策略数据库	298
10.3.2	管理路由表	302
10.4	带宽合并	305
10.4.1	何谓带宽合并	306
10.4.2	企业内的带宽合并	307
10.5	小结	319
第 11 章	Linux的带宽管理	321
11.1	队列	322
11.1.1	不可分类的队列算法	323
11.1.2	可分类的队列算法	323
11.2	Linux带宽管理	324
11.3	过滤器	325
11.3.1	FW过滤器	326
11.3.2	U32过滤器	326
11.4	带宽管理部署示例	326
11.4.1	带宽划分	327
11.4.2	设置队列算法	327
11.4.3	设置队列规则	328
11.4.4	设置过滤器	329
11.4.5	测试	330
11.5	带宽借用	332
11.6	类别中的队列	334
11.7	Linux带宽管理的限制	335
11.8	网桥模式中的带宽管理	338
11.9	多接口的带宽管理	339
11.9.1	为内核及iptables安装补丁	340
11.9.2	多接口带宽管理	341
11.10	实际案例	343
11.11	小结	348

第 12 章 流量统计	349
12.1 安装及测试SNMP服务器	350
12.1.1 安装SNMP服务器	350
12.1.2 测试SNMP服务器	351
12.2 安装及设置MRTG	352
12.2.1 安装MRTG	352
12.2.2 设置MRTG	352
12.2.3 使用cfgmaker工具编写MRTG针对网卡的配置文件	353
12.3 另一种网络流量监测方式	357
12.3.1 结合使用Netfilter/Iptables和MRTG来监测网络流量	357
12.3.2 手动编写MRTG的配置文件	359
12.4 外部程序及MRTG配置文件的示例	360
12.5 小结	362
第 13 章 弱点扫描、入侵检测及主动防御系统	363
13.1 何谓弱点扫描	364
13.1.1 OpenVAS弱点扫描工具	364
13.1.2 OpenVAS弱点扫描工具的工作架构	365
13.1.3 下载及安装OpenVAS弱点扫描工具	365
13.1.4 进行弱点扫描	368
13.2 入侵检测系统	374
13.2.1 网络设备的限制	374
13.2.2 入侵检测系统的分类	375
13.2.3 入侵检测系统的部署	375
13.2.4 Snort入侵检测系统介绍	376
13.2.5 下载及安装Snort入侵检测系统	377
13.2.6 下载及安装Snort的规则数据库	378
13.2.7 配置Snort	381
13.2.8 Snort的启停	382
13.2.9 Snort的警告	382
13.3 主动防御系统	383
13.3.1 下载Guardian	384
13.3.2 安装Guardian	384

13.3.3	设置Guardian	385
13.3.4	Guardian的启停	386
13.4	小结	387
第 14 章	VPN基础篇	389
14.1	何谓VPN	390
14.1.1	VPN的原理	392
14.1.2	常见的VPN架构	393
14.1.3	VPN的安全问题	393
14.1.4	VPN机制的优缺点	393
14.2	数据加解密	394
14.2.1	何谓“明文”	394
14.2.2	何谓“密文”	395
14.3	数据加密类型	396
14.3.1	对称加密	396
14.3.2	非对称加密	397
14.4	哈希算法	398
14.4.1	常见的哈希算法	399
14.4.2	哈希算法的特性	399
14.5	基于IPSec的VPN	400
14.5.1	IPSec的工作模式	400
14.5.2	IPSec的组成要素	401
14.5.3	AH及ESP协议运行时需要设置的参数	409
14.5.4	安装IPSec参数的管理工具	411
14.5.5	配置传输模式IPSec VPN	411
14.6	Linux中的IPSec架构	420
14.6.1	IPSec机制的SPD	421
14.6.2	IPSec机制的SAD	422
14.7	小结	425
第 15 章	VPN实战篇	427
15.1	IKE	428
15.2	Preshared Keys验证模式下的传输模式VPN	433

15.2.1	数据库服务器的设置	434
15.2.2	客户端主机的设置	435
15.2.3	启动VPN	436
15.3	Preshared Keys验证模式下的隧道模式VPN	437
15.3.1	VPN 服务器(A)主机上的设置	438
15.3.2	VPN 服务器(B)主机上的设置	439
15.4	何谓数字证书	440
15.4.1	数字证书的必要性	440
15.4.2	证书管理中心	441
15.4.3	将Linux系统作为企业的CA	447
15.5	数字证书验证模式下的传输模式VPN	453
15.5.1	证书的生成及保存	453
15.5.2	客户端VPN主机的设置	454
15.6	数字证书验证模式下的隧道模式VPN	457
15.6.1	证书的生成及保存	457
15.6.2	设置VPN 服务器(A)	457
15.6.3	设置VPN 服务器(B)	458
15.6.4	启动IPSec	459
15.7	小结	459
第 16 章	VPN: L2TP Over IPSec	461
16.1	何谓PPP	462
16.2	何谓L2TP协议	462
16.2.1	L2TP协议的原理	463
16.2.2	L2TP协议的安全问题	465
16.2.3	L2TP协议安全问题的解决方案	465
16.2.4	Client to Site的L2TP VPN结构探讨	466
16.2.5	L2TP 客户端及服务器之间网段的选择	467
16.2.6	Proxy ARP的工作原理	467
16.3	构建L2TP VPN	470
16.3.1	配置L2TP服务器	470
16.3.2	配置PPP服务器	472
16.3.3	建立VPN的拨号帐户	472

16.3.4	证书的生成及保存	473
16.3.5	配置安全策略	473
16.3.6	IKE配置文件	474
16.3.7	启动L2TP服务器	475
16.4	配置L2TP客户端	475
16.4.1	生成L2TP客户端证书	475
16.4.2	将证书导入Windows XP/7系统前的准备工作	476
16.4.3	设置Windows XP系统上的L2TP客户端	476
16.4.4	设置Windows 7系统中的L2TP客户端	484
16.5	IPSec连接穿透NAT的问题	492
16.6	小结	494



Linux

|第1章| 防火墙的基本概念

1