

专注讨论网络基础设施的安全性并提供防护措施
全球知名网络安全专家 Wesley J. Noonan 权威力作

全球畅销

"黑客大曝光"系列
图书之姊妹篇



HARDENING

Network Infrastructure 中文版

具体的实施步骤 + 特定的配置实例

为你的系统构筑坚固的安全堡垒

[美] Wesley J. Noonan 著

张辉 石华耀 唐红亮 译

Series Editor: Martha Bragg, CISSP, MCSE, Security Security+

Mc
Graw
Hill

Osborne

Mc
Graw
Hill

清华大学出版社

Hardening Network Infrastructure

中文版

[美] Wesley J. Noonan 著

张 辉 石华耀 唐红亮 译

清华大学出版社

北 京

Wesley J. Noonan
Hardening Network Infrastructure
EISBN 0-07-225502-1
Copyright © 2004 by The McGraw-Hill Companies.

Original language published by the McGraw-Hill Companies, Inc. All Rights reserved. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Simplified Chinese translation edition is published and distributed exclusively by Tsinghua University Press under the authorization by McGraw-Hill Education (Asia) Co., within the territory of the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan. Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书中文简体字翻译版由美国麦格劳-希尔教育出版(亚洲)公司授权清华大学出版社在中华人民共和国境内(不包括中国香港、澳门特别行政区和中国台湾)独家出版发行。未经许可之出口,视为违反著作权法,将受法律之制裁。未经出版者预先书面许可,不得以任何方式复制或抄袭本书的任何部分。

北京市版权局著作权合同登记号 图字 01-2006-0343 号

版权所有, 翻印必究。举报电话: 010-62782989 13501256678 13801310933

本书封面贴有 McGraw-Hill 公司防伪标签, 无标签者不得销售。

图书在版编目(CIP)数据

Hardening Network Infrastructure 中文版/(美)努南(Noonan, W.J.)著;
张辉等译. —北京: 清华大学出版社, 2007.8
书名原文: Hardening Network Infrastructure
ISBN 978-7-302-16006-9

I. H... II. ①努... ②张... III. 计算机网络—安全技术
IV. TP393.08

中国版本图书馆 CIP 数据核字(2007)第 133527 号

责任编辑: 刘秀青

责任校对: 刘雪莲

责任印制: 科海

出版发行: 清华大学出版社

<http://www.tup.com.cn>

c-service@tup.tsinghua.edu.cn

社总机: 010-62770175

投稿咨询: 010-62772015

印装者: 北京市鑫山源印刷有限公司

经销: 全国新华书店

开本: 185×230 印张: 31.00

版次: 2007年9月第1版

印数: 1-3000

定价: 59.00元

地址: 北京清华大学学研大厦 A 座

邮编: 100084

邮购热线: 010-62786544

客户服务: 010-62776969

字数: 677千字

印次: 2007年9月第1次印刷

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题, 请与清华大学出版社出版部联系调换。联系电话: 82896445 产品编号: 021194-01

献给我的妻子 Norma，感谢她给予的支持。

献给我的小狗 Loki 和 Odin，在撰写本书漫长的日日夜夜里，它们一直陪伴在我的左右。

献给不是父亲胜似父亲的 Dwaine。

内 容 提 要

“Hardening”系列是美国 McGraw-Hill 公司新近推出的又一套信息安全系列丛书，与久负盛名的“黑客大曝光”系列携手，为信息安全界奉献了一道饕餮大餐。

本书是“Hardening”系列成员之一，由资深安全专家 Wesley 执笔，通过四段式系统强化教学法，从技术和管理制度两方面，详细介绍了网络基础设施的安全防护工作，对系统管理员容易疏忽或犯错的细节进行深入探讨，旨在帮助读者把网络系统建设成信息安全堡垒。

全书共分 4 大部分 17 章。第 1 部分给出降低系统威胁的 6 个关键措施，是系统阻止入侵的必要手段；第 2 部分则是本书的重中之重，系统讲述强化网络基础设施安全的具体方法和措施；第 3 部分告诫人们：不能一劳永逸，需要利用各种监控技术持续监控系统，教会读者执行安全复查、管理环境变更；第 4 部分对加强网络基础设施防护的成本、员工培训、响应计划进行讨论，同类书中少见。

本书是负责安全保障工作的网络管理员和系统管理员的必读之书，也可作为信息管理员以及对计算机和网络安全感兴趣的人员的参考书。

序 言

毫无疑问，当今的 IT 专业人员必须能够处理好各种安全事件——从蠕虫和病毒到无赖用户，再到老套的黑衣入侵者。本书的内容不仅包括理论，还介绍了颇有价值的实际操作方法，对于必须处理实际问题的系统管理员来说，使用起来非常方便。书中的例子都便于在命令行上直接运用。

在建立安全机制上越具有前瞻性，那么以后被迫去打补丁、进行更新，以及从安全事件中恢复的机会也越少。从降低风险而不是加强安全的角度去考虑问题，是有助于促进向前瞻性安全机制转变的一种思维方式。经常提提类似于“我怎样才能最大限度地降低风险？”这样的问题，获得的回报将是更为可靠的安全性。牢记一点：“完美”是“够用”的大敌。“不要老想着投入完美的解决方案，而应该集中着眼于最实用的方案。”

说到底，没有网络用户的协助，就不可能实现有效而持久的安全策略。解决管理和资源问题往往要比解决 IPsec 的配置问题更富挑战性。很幸运，Wesley 先生已经在本书里介绍了这两方面的问题。

最后记住一点，并不只有您一个人单打独斗。如果要在网络、用户和数据的安全性上面更有作为，那么我们这些网络安全的捍卫者们就必须联手合作。有了 Firewall-Wizards Mailing List（防火墙向导邮递列表）这类论坛，就能让本书作者这样的高手帮助人们解决特定问题。安全机制建立得不正确、有人做了不该做的事，或者有人攻击了我们的系统，这些可能都不是我们的错。但是尽我们所能保障网络的安全，并且帮助其他人保障安全，就是我们义不容辞的责任了。

Paul D. Robertson

TruSecure®公司风险评估部主管

Firewall-Wizards®安全邮递列表主席

Paul Robertson 在 IT 和安全领域有 20 多年的从业经验：他参加美国陆军时曾在白宫供职，还在 Internet 上创办了 USA Today 网站。Paul 目前在 TruSecure®公司帮助数百家企业客户进行风险管理，他还参与了计算机取证领域的工作，是 www.personalfirewallday.org 发起人和 Firewall-Wizards Mailing List（防火墙向导邮递列表）的主席。

前言

知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼不知己，每战必败。
故善攻者，敌不知其所守；善守者，敌不知其所攻。

——孙武，《孙子兵法》

为什么一本介绍网络基础设施安全防护的书，一开始却要引用《孙子兵法》上的两段话呢？这个问题的答案是，如今的网络总处在攻击之下，这无异于一场数字战争。

战争中的一方是黑客(hacker)、骇客(cracker)和脚本小子(script kiddie)，他们企图攫取信息，侵入受到保护的资源之中。他们是敌人，您需要知道他们是何许人也，他们意欲何为。您还需要了解他们使用的攻击方法和入侵形式。McGraw-Hill/Osborne 出版的 *Hacking Exposed* (中译本名为《黑客大曝光》，由清华大学出版社出版) 系列图书是了解现有安全威胁的很好资源。这些图书列举并解释了黑客所采用的各种攻击手段。但是做到知彼，仅仅只是了解了战争的一个方面。

这场数字战争的另一方则是计算机安全领域内的专业人士。

我们是努力防止黑客、骇客和脚本小子入侵我们系统的人。只知道针对您的网络存在哪些威胁还远远不够，您不但要了解敌人，还要了解您自己和您的网络（从防火墙到路由器再到交换机，以及在这之间的所有东西）。您一旦熟悉了这些内容，接下来就要了解如何加强对这些网络资源的防护。例如，如果您知道黑客会利用冒充欺骗的伎俩来窃取资源的访问权，那么，应该怎样配置防火墙和路由器来抵御这样的威胁呢？本书详细地说明了在加强网络资源的防护时所能实施的特定方法和步骤，它给 *Hacking Exposed* 系列图书补充了很多颇富价值的内容。笔者将会让您展示如何进行防御，从而让您的敌人所发动的攻击付诸东流。

在看过许多技术书籍和白皮书之后，我倍感沮丧，因为这些资料很少能举例说明该怎么做。它们只是在概念上深入地进行了解释和说明，看过之后我们仍旧会问：“行，那既然我搞懂了这个问题，我该对此怎么办呢？”当出版社找到我来撰写本书的时候，给我触动

最大的就是出版社也想回答这个问题：“我该对此怎么办呢？”我决定从一个顾问的角度来编写本书。在书中，我没有去细抠各种入侵的原理，然后告诉读者说需要修正这类问题；而是告诉读者，如何才能加强对资源的防护以抵御攻击，并且尽我所能给出特定的配置实例。我希望读者能够把这本书当作一本参考手册或者行动手册，指导自己完成加强网络基础设施防护的各个步骤和过程。

读者在本书里将会看到加强网络基础设施防护所涉及到的所有方面的内容，这些内容分成4个独立的部分进行介绍。在第1部分“立即行动”里，我们先从六件事谈起，如果您还没有做这些事的话，应该马上就去做。

第2部分“从全局出发——系统级的加强防护过程”，我们首先考察一个安全策略，然后提出指导原则，读者可以按照这些指导原则制定一个良好的安全策略。只有您已经清晰地定义了网络设备一贯的安全防护状态是怎样的，才能让自己所有的网络设备都处于这样的一种状态，这也是为什么加强网络防护的第一步必须是制定一份安全策略的原因。接下来，我们将会研究特定的网络基础设施硬件，加强对它们的安全保护。我们不仅要考察我们能为保护这些硬件做什么，而且还要考察怎样可以用这些硬件去保护网络。例如，我们不仅会考察保护防火墙自身免遭入侵的步骤，还会考察使用防火墙来保护网络基础设施所需的步骤。作为第2部分的总结，我们会介绍各种技术和概念，并且探讨在设计一个得到系统级安全防护的网络基础设施时，如何将这些技术融入其中。

第3部分“绝不能一劳永逸”探讨如何处理好网络基础设施上发生的变化。我们会介绍从安全策略的调整到打补丁和进行更新的各方面内容，说明如何有效地解决这些必然会出现的变化，同时又不会使网络处于易受攻击的状态。

最后，我们在第4部分“如何成功地加强网络基础设施的防护”里，将会阐述加强网络基础设施防护的软性技巧。这方面涉及到的问题包括：如何评价成本翻番、以及配备和培训人员时牵扯到的事项。我们在这部分结束前探讨了网络安全的严峻现实：在您竭尽全力网络仍被入侵的情况下，该怎么办。

我真诚地希望，在阅读本书并且实践了书中给出的建议之后，读者朋友不仅能对敌人做到“知彼”，而且对自己和自己的网络能做到“知己”，此外，读者也能懂得要去防御什么，如何进行防御。

说明：在本书里的一些代码行末尾（如下面这个例子），读者会看到一个右箭头（→）。该符号表明这是一条单行的命令，它实际应该放在一行里，因为印刷页宽的限制而必须折行。

```
iptables -A INPUT -I eth0 -p tcp -m tcp -s 192.168.1.100 -d →  
192.168.1.1 --dport 443 --syn -j ACCEPT
```

作者简介

Wesley J. Noonan (得克萨斯州休斯顿) 已经在计算机这个行业内工作了 14 年之多, 他的专长是设计和实现基于 Windows 的网络和网络基础设施。他是 Collective Technologies, LLC 公司 (www.colltech.com) 的资深网络顾问, 这是一家涉及到存储、服务器和网络设计、体系结构、实现和安全的专业公司。Wesley 早年在美国海军的 Banyan VINES 网上开始了他的计算机职业生涯。他曾设计和构建过从 25 到 25 000 用户的各种规模的网络。Wesley 最近完成的工作有: 设计和实现有 100 个结点的安全 VPN 互连网络、实现一个全球性的安全 Citrix 部署任务, 以及为 Collective Technologies, LLC 公司的客户提供安全审计和安全设计方面的大量咨询。Wesley 以前曾在 BMC 软件公司的研发部工作, 从事 PATROL 管理解决方案的研发, 负责该公司网络和应用管理产品的结构设计和测试。他在一家公司设计过一个安全网络基础设施, 可全天候提供飞机的状态和信息; 他还配合休斯顿本地的金融和石化公司, 设计和实现了这些公司的安全和网络基础设施。Wesley 也是一位活跃的培训师, 他为自己的客户开设了基于 Cisco 路由和交换技术的课程。他还多次在技术会议 (如 MCTCON2002) 和用户研讨会 (如 Associate of IT Professionals-Houston) 上发言, 发言的主题是网络安全和保护企业网络基础设施免于被攻破和入侵的方法。他是 SecurityFocus 和 Firewall-Wizards Mailing List (防火墙向导邮递列表) 的积极参与者, 持有的专业资格证书包括 MCSE、CCNA、CCDA、NNCSS 和 Security+, 在这些领域里他都是专家。Wesley 是 QUE 出版的 CISSP Training Guide 一书的作者, 而本书是他写的第二本书。从一个人能志趣结合的角度来看, Wesley 的确是个幸运的人。他还会继续享受网络设计和安全的各个方面带给他的快乐。

主编简介

Roberta Bragg (密苏里州的大峡谷市) 拥有的头衔有 CISSP、MCSE:Security、MVP、Security+、ETI-Client Server、Certified Technical Trainer、IBM Certified Trainer、DB2-UGDB 和 Citrix Certified Administrator。她已经当了六年 MCP 杂志的 Security Advisor (安全顾问) 专栏作家, 她是 searchWin2000.com 的 Security Expert (安全专家)。她还为拥有 55 000 订户的 Security Watch 时事通讯撰文。2002 年, Roberta 在华盛顿州西雅图市设计、规划、召开并且参加了第一届 Windows Security Summit (Windows 安全峰会)。Roberta 是 Windows Security Academy (Windows 安全学院) 的创办人和发言人, 这是一个为期三天的网络安全

建设研讨会。她还教 SANS 和 MIS 方面的课程。微软公司推选她在其 2004 年安全峰会上讲授 IT 职业人高级课程。Roberta 是一位安全技术的布道者,她巡游世界,在网络和 Windows 安全问题上提供咨询、评估和培训。她还成为了 Ceel Pasternak 和 Linda Thornburg 所写的 Cool Careers for Girls (女生的酷职业) 系列图书的主角之一。Roberta 在 Seattle Pacific University (西雅图太平洋大学) 和 Johnson County Community College (约翰逊郡社区学院) 任教,讲授 Windows 2000 安全设计和网络安全设计的课程。Roberta 是 *MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network* 一书的作者,是 McGraw-Hill/Osborne 出版的 *Network Security: The Complete Reference* 一书的第一作者。她为 QUE 和 New Riders 出版社撰写了有关 SQL Server 2000、CISSP 和 Windows 安全等方面的图书。

技术审稿人

Eric S. Seagren (得克萨斯州的密苏里城) 的头衔有 CISSP、SCNP、CCNA、CNE、MCP+i、MCSE, 他在计算机业内有八年的工作经验。而在最近的五年里, 他一直负责一家“财富 100 强”公司的金融安全工作。Eric 的计算机职业生涯是从一家休斯顿的小公司开始的, 他当时在那家公司里负责有线网络的运行, 并且从事一般性的网络和服务器的故障检修工作。他在金融安全方面的工作经历包括: Novell 和微软的服务器管理、灾难恢复和 Y2K 问题的修复。他在近两年里担任 IT 结构设计师, 负责设计安全的、可扩展的和冗余的网络, 这些工作包括扩展 DMZ 设计, 评估和审计各种网络设计和产品 (包括路由器、交换机、防火墙, 以及入侵检测和防护系统) 的安全性。

目 录

第 1 部分 立即行动!

第 1 章 开门六件事	3
1.1 复查网络设计	5
1.2 安装防火墙	8
1.2.1 应用代理	9
1.2.2 有状态的数据包检测/过滤网关	9
1.2.3 混合防火墙	9
1.2.4 应该实现哪种防火墙	10
1.3 实现访问控制列表	10
1.4 关闭不必要的功能和服务	11
1.5 实施病毒防护	12
1.6 保护无线连接的安全	13
1.7 小结	13

第 2 部分 从全局出发——系统级的加强防护过程

第 2 章 制定安全策略	17
2.1 安全策略的作用	18
2.2 安全策略的组成	21
2.2.1 从何处开始	21
2.2.2 良好安全策略的特征	24
2.3 安全策略建议	26
2.3.1 加密策略	27
2.3.2 模拟/ISDN 策略	27
2.3.3 防病毒策略	27

2.3.4 审计、安全漏洞评估和风险评估策略	27
2.3.5 拨号策略	27
2.3.6 DMZ 策略	28
2.3.7 外网策略	28
2.3.8 无线通信策略	28
2.3.9 VPN 策略	28
2.3.10 防火墙安全策略	29
2.3.11 路由器和交换机安全策略	29
2.3.12 远程访问策略	29
2.3.13 口令策略	29
2.3.14 入侵检测/保护系统策略	30
2.3.15 内容过滤/Internet 策略	30
2.3.16 企业级监视策略	30
2.3.17 AUP 策略	30
2.3.18 网络连接策略	31
2.3.19 网络文档策略	31
2.4 为什么安全策略会失效, 如何避免失效	31
2.4.1 将安全当作前进的障碍	32
2.4.2 安全是后天学会的行为	32
2.4.3 安全不乏意外事件和情况	32
2.4.4 安全策略始终没有尽头	32
2.4.5 防止失败	32
2.5 小结	33
第 3 章 强化防火墙	34
3.1 基于硬件和基于软件的防火墙	35
3.1.1 强化远程管理	36
3.1.2 实现身份验证和授权	42
3.1.3 强化操作系统	44
3.1.4 强化防火墙的服务和协议	45
3.1.5 利用冗余强化防火墙	56
3.1.6 强化路由协议	58
3.2 小结	62

第 4 章 用 IDS/IPS 强化网络安全	63
4.1 IDS/IPS 技术.....	64
4.1.1 基于主机的入侵检测/保护	65
4.1.2 基于网络的入侵检测/保护	66
4.2 IDS/IPS 的组成.....	67
4.3 IDS/IPS 设备的强化.....	68
4.3.1 强化 Windows 上的 PureSecure	68
4.3.2 强化 Cisco IDS.....	71
4.4 IDS/IPS 的部署.....	73
4.4.1 检测和保护的对比	74
4.4.2 放置检测器	74
4.4.3 在交换式网络中放置检测器的位置.....	75
4.5 IDS/IPS 的调优.....	76
4.5.1 调整 PureSecure 的检测器	77
4.5.2 调整 Cisco IDS 的检测器.....	79
4.6 IDS/IPS 的日志、报警和阻断.....	83
4.6.1 PureSecure 的日志功能	83
4.6.2 Cisco IDS 的日志功能.....	85
4.6.3 PureSecure 的报警	86
4.6.4 Cisco IDS 的报警.....	87
4.6.5 使用 Cisco IDS 和 Cisco PIX 防火墙阻断流量.....	90
4.7 小结.....	91
第 5 章 强化 VPN 和远程拨号访问.....	92
5.1 强化 VPN 连接	93
5.1.1 不同的 VPN 连接类型和 VPN 技术.....	94
5.1.2 强化 VPN 设备安全的方法.....	96
5.1.3 强化基于 IPsec 的 VPN.....	118
5.1.4 强化 VPN 客户机的安全.....	132
5.2 强化拨号远程访问	133
5.3 小结.....	134

第 6 章 强化路由器和交换机.....	136
6.1 强化管理访问.....	137
6.1.1 保护控制台访问.....	138
6.1.2 保护 VTY 访问.....	139
6.1.3 保护基于 Web 的管理访问.....	141
6.1.4 保护辅助端口的访问.....	142
6.1.5 保护特权模式的访问.....	142
6.1.6 实现多用户名和 AAA.....	143
6.1.7 提供提示.....	144
6.2 强化服务和功能.....	145
6.2.1 CDP 协议.....	145
6.2.2 TCP 和 UDP 小服务器.....	146
6.2.3 finger.....	146
6.2.4 NTP 协议.....	146
6.2.5 bootp 服务器.....	148
6.2.6 DHCP 协议.....	148
6.2.7 配置自动加载.....	148
6.2.8 名字解析.....	149
6.2.9 代理 ARP.....	149
6.2.10 重定向广播.....	150
6.2.11 IP 源路由.....	150
6.2.12 ICMP 重定向、不可达和地址掩码应答.....	150
6.2.13 syslog.....	150
6.2.14 SNMP 协议.....	151
6.2.15 实现环回地址.....	154
6.2.16 禁用未用的接口.....	154
6.2.17 配置内存转储.....	155
6.3 强化路由器的技术.....	155
6.3.1 实现冗余.....	156
6.3.2 强化路由协议.....	156
6.3.3 实现流量管理.....	161
6.3.4 实现 IPsec.....	172
6.4 强化交换机的技术.....	174

6.4.1 强化 VLAN	175
6.4.2 强化服务和功能	178
6.5 小结	184
第 7 章 用内容过滤保护网络安全	186
7.1 Internet 内容过滤的体系结构	188
7.1.1 基于客户机的内容过滤	188
7.1.2 基于服务器的内容过滤	188
7.1.3 基于网关的内容过滤	191
7.2 Internet 内容过滤技术	192
7.2.1 滥用资源	192
7.2.2 保留网络带宽	192
7.2.3 不健康的工作环境	192
7.2.4 不健康的 Web 代码 (Java/ActiveX Applet)	193
7.2.5 实施内容过滤	193
7.3 电子邮件的内容过滤	213
7.3.1 实施病毒保护	213
7.3.2 过滤附件	214
7.3.3 实施内容过滤	215
7.3.4 实施垃圾邮件控制	216
7.4 小结	217
第 8 章 加强 WLAN 网络连接的安全	218
8.1 未获 IT/管理部门批准禁用 WLAN	219
8.1.1 防止非法 AP	219
8.1.2 实施 WLAN 探测	221
8.1.3 拆除非法 WAP	224
8.2 加强 WAP 的安全	224
8.2.1 加强远程管理的安全	225
8.2.2 安全地配置 SSID	227
8.2.3 配置日志	229
8.2.4 加强服务的安全	230
8.2.5 限制无线模式	233

8.2.6 使用 MAC 地址过滤	234
8.3 加强 WLAN 连接的安全	237
8.3.1 加强 WEP 的安全	237
8.3.2 加强 WPA 的安全	240
8.3.3 用 VPN 加强 WLAN 的安全	245
8.4 加强 Windows XP 无线客户的安全	245
8.4.1 加强 WEP 的安全	246
8.4.2 加强预共享密钥 WPA 的安全	247
8.4.3 用 WPA 加强 RADIUS/802.1x 的安全	248
8.5 小结	250
第 9 章 实现 AAA	252
9.1 AAA 机制	253
9.1.1 RADIUS	253
9.1.2 TACACS+	254
9.2 认证和访问控制	254
9.2.1 基于 IOS 设备的 AAA 认证	255
9.2.2 PIX 防火墙上的 AAA 认证	263
9.3 授权和网络安全	266
9.3.1 在 IOS 设备上的授权	266
9.3.2 PIX 防火墙上的授权	267
9.4 记账和网络安全	270
9.4.1 基于 IOS 环境下的 AAA 记账	271
9.4.2 PIX 防火墙上的 AAA 记账	272
9.5 802.1x 基于端口的认证	272
9.5.1 802.1x 网络设备的功能	273
9.5.2 在 IOS 交换机上配置 802.1x 认证	274
9.6 小结	280
第 10 章 通过网络管理加强网络安全	281
10.1 实现一个网络管理系统 (NMS)	282
10.1.1 故障管理	283
10.1.2 配置管理	298

10.1.3 性能管理	301
10.1.4 记账或者资产管理	303
10.1.5 安全管理	303
10.2 加强网络管理协议的安全	303
10.3 小结	311
第 11 章 实施一个安全的边界	312
11.1 DMZ 实施方法	313
11.1.1 在 DMZ 中使用一个多宿防火墙	313
11.1.2 在 DMZ 中使用一个双重防火墙	316
11.1.3 VLAN 和 DMZ	318
11.2 Internet 访问模块	318
11.2.1 通过 Internet 模块的流量 flow	320
11.2.2 防火墙实施	320
11.3 VPN/远程访问模块	324
11.3.1 远程访问 VPN 终止网段	325
11.3.2 站点到站点 VPN 终止网段	326
11.3.3 拨号远程用户终止网段	326
11.3.4 NIDS/NIPS 部署	326
11.4 WAN 访问模块	327
11.5 外联网访问模块	328
11.6 无线访问模块	329
11.7 电子商务访问模块	330
11.7.1 Web 服务 DMZ 网段	331
11.7.2 应用程序服务 DMZ 网段	331
11.7.3 数据库服务 DMZ 网段	331
11.8 小结	332
第 12 章 实施一个安全的内部网络	334
12.1 使用虚拟局域网 (VLAN) 分隔网络	335
12.1.1 执行信任模型	335
12.1.2 使用 VLAN 隔离系统	337
12.2 设计企业园区	338