



丛书
累计印数
80万册

100%

内容丰富、权威

在OSI多层协议上开发和实现有效的安全策略

抵制对公司网络和VPN的攻击

配置Cisco网络安全产品，获得最高安全性



[美] Rajesh Kumar Sharma, NIIT 等著

赵刚 方兰 林瑶 等译

Cisco 网络安全 宝典

防火墙
AAA安全
入侵检测

• • • • •



WILEY



電子工業出版社

Publishing House of Electronics Industry
www.phei.com.cn

美国计算机“宝典”丛书

Cisco 网络安全宝典

Cisco Security Bible

[美] Rajesh Kumar Sharma, NIIT 等著

赵 刚 方 兰 林 瑶 等译

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书讲述有关如何提高网络安全的问题,并非仅仅讲述一般性的原理、原则和方法,而是在介绍基础理论、给出安全体系结构的同时,结合 Cisco 产品,将一般性的原理、原则和方法,体现在 Cisco 产品的安全功能特性以及它们的实现和配置上,并配有应用案例加以说明。全书有 7 部分,共 18 章。第 1 部分介绍网络安全,概述了网络安全有关的基本概念,如威胁、防范措施、安全策略、体系结构以及相应的 Cisco 软硬件产品;第 2 部分研究保护网络基础设施安全的方法;第 3 部分介绍通过防火墙提高安全性,探讨了在保护网络安全中防火墙所扮演的角色;第 4 部分的内容为理解和实现 AAA,描述了鉴别、授权和记账方法;第 5 部分介绍虚拟专用网,阐述 VPN 的作用、基本技术和相应产品;第 6 部分介绍 Cisco 技术和安全产品,详细描述了 Cisco IOS IPSec 以及如何对其进行配置,还简要介绍了一些 Cisco 安全产品;第 7 部分介绍网络基础知识,回顾了基本的网络概念。书中还附有相关习题和答案,帮助读者掌握和巩固有关知识。

本书案例丰富、实用性强,是学习网络安全技术、熟悉和掌握 Cisco 产品安全特性的优秀读物,也可供网络安全方面的研究和开发人员参考。



Copyright ©2002 by Publishing House of Electronics Industry. Original English language edition copyright ©2002 by Wiley Publishing, Inc. All rights reserved including the right of reproduction in whole or in part in any form. This translation published by arrangement with Wiley Publishing, Inc.

本书中文简体专有翻译出版权由美国 Wiley Publishing, Inc. 授予电子工业出版社及其所属今日电子杂志社。未经许可,不得以任何手段和形式复制或抄袭本书内容。该专有出版权受法律保护,侵权必究。

著作权合同登记号 图字: 01-2002-2302

图书在版编目 (CIP) 数据

Cisco 网络安全宝典 / (美) 沙尔马 (Sharma, R. K.) 著; 赵刚等译. — 北京: 电子工业出版社, 2002.11
(美国计算机“宝典”丛书)

书名原文: Cisco Security Bible

ISBN 7-5053-8176-8

I. C... II. ①沙... ②赵... 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 (2002) 第 085828 号

责任编辑: 牛 勇

排版制作: 今日电子公司制作部

印 刷: 北京东光印刷厂

出版发行: 电子工业出版社 www.phei.com.cn

北京市海淀区万寿路 173 信箱 邮编: 100036

经 销: 各地新华书店

开 本: 787 × 1092 1/16 印张: 37 字数: 947 千字

版 次: 2002 年 11 月第 1 版 2002 年 11 月第 1 次印刷

定 价: 59.00 元

凡购买电子工业出版社的图书, 如有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系。
联系电话: (010) 88211980 68279077

出版说明

21 世纪是一个崭新的世纪，是催人奋进的世纪。在新世纪的第一乐章中，我们热忱地向广大读者、IT 人士推荐这套全新改版的美国计算机“宝典”丛书。

丛书的出版宗旨

本着提高广大读者计算机专业技能的宗旨，我社从美国 Wiley 出版公司引入了这套“宝典”丛书。美国的 Wiley 出版公司始创于 1807 年，是美国最著名的出版公司之一，该公司出版了许多经典的作品。本套丛书秉承了 Wiley 图书一贯的水准，内容全面、权威。在世界各地 51 个国家被译为 31 种文字，拥有几百万读者。自 1994 年将这套丛书引入中国市场以来，累计销量已近百万册。得到了广大读者的认同，成为电子工业出版社的著名品牌之一。

丛书的涉及范围

“宝典”丛书的涉及范围甚广，既包括众多的流行软件、编程语言、图形图像，也包括数据库、网络等高端技术等方面的书籍。对于某些软件，我们还进行了本地化处理，按相应的中文版软件进行了调整，进一步贴近中国读者的需求。

每一本“宝典”共同贯彻的一项宗旨就是，全面、系统地介绍相应的主题，力求该软件或系统能做到的，读者通过本书的学习也能做到。

丛书的创作队伍

“宝典”丛书的作者都是某个计算机专业领域的专家、教授，有些还是某软件的特约测试者。比如 Deke McClelland、Alan Simpson 和 Ellen Finkelstein 等知名畅销计算机图书作家，在相关领域都具有很高的声望。他们拥有丰富的实践经验，所介绍的内容都是在工作中得到千锤百炼，具有一定的权威性。在他们所撰写的书籍当中，会介绍一些技巧，同时也会为读者提出某些忠告，以免犯同样的错误。

在中文版“宝典”中我们也本着同样的原则，译者均经过严格筛选，他们大都是来自于高等院校的教授、学者，计算机领域的高手，不但具有高深的专业知识，同时也具备英语方面的深厚底蕴。我们的编辑队伍，同样是来自于计算机专业的高素质人才。通过这种严格的层层把关，相信最终奉献给读者的将是一部部精品。

丛书的新特性

新的世纪，“宝典”以全新的面貌呈现在广大读者面前。无论是版式、用纸还是印刷质量，相关人员都颇费一番苦心，进行了很大改善。同时我们对于丛书的选题也进行了调整，使其更适合我国的计算机发展水平。对于原书中某些不适合中国国情以及过于调侃的内容进行了删减。我们将秉承“宝典”丛书一贯的“权威、全面、精益求精”的风格，力争每一本书能成为您探索计算机领域奥秘的“宝典”。

译 者 序

随着计算机网络的应用范围不断扩大，网络安全越来越受到人们的关注。众多厂商都推出了自己的安全产品。其中，Cisco 的联网产品可谓家喻户晓，但谈到 Cisco 的安全产品或产品所具有的安全特性，就未必有很多人清楚了。实际上，在网络安全方面，Cisco 也做了很多工作，尤其是通过与其联网产品相结合，使它具有了一定的特色和优势。

本书的重点是结合 Cisco 产品讲述如何提高网络安全性。本书讲述的是如何提高网络安全的问题，但并非仅仅讲述一般性的原理、原则和方法，而是在介绍基础理论、给出安全体系结构的同时，结合 Cisco 产品，将一般性的原理、原则和方法，体现在 Cisco 产品的安全功能特性以及它们的实现和配置上，并配有应用案例加以说明，这是本书的突出特点。本书的具体内容覆盖路由器、加密机制、AAA 机制、防火墙、VPN、安全和网络管理等与网络安全有关的各个领域。由于目前 Cisco 联网和安全产品在实际应用和市场上都占有很大份额，因此，本书具有很强的实用性。

本书覆盖内容广泛，并包含了不少新技术、新名词、新产品，有许多还没有标准译法，这对翻译造成了不少困难。对于英文的产品名或程序中的菜单、提示等，除非有公认译法，或大家已约定俗成，我们一般不予翻译，或者只是在适当的地方，在括号中给出中文意思，而不是作为正式的译名。这样做的原因是，一方面有些内容确实很难译成符合汉语习惯的语句，我们也只好不译；另一方面，我们觉得，保留英文原名可以方便读者进一步在因特网或手册中查阅相关资料，以免因为译名不统一，使读者不知道看到的到底是何物。还需要提到的一个词是“packet”，在翻译过程中，除在个别讲述交换技术（第三层以下）等的地方，我们将其翻译为“分组”，如把“packet switch”翻译为“分组交换”，在其他场合，我们一般根据上下文，把这个词译为“数据包”或“包”。这主要是出于尊重专用术语和习惯的考虑。

参加本书翻译的有赵刚、方兰、林瑶、杨宏、康平军、谭荣、韩锋、钱卫、董韶君、蒋晓红、肖斌等。限于水平，错误和不妥之处在所难免，敬请广大读者批评指正。

目 录

前言	1
第 1 部分 理解网络安全	5
第 1 章 认识网络安全的威胁	7
1.1 安全威胁背后的动机	7
1.1.1 攻击背后的动机	7
1.1.2 攻击行为对网络的影响	8
1.2 网络安全的需求	8
1.3 网络安全上的弱点	9
1.3.1 技术	10
1.3.2 实现	11
1.3.3 策略框架的脆弱性	12
1.4 安全威胁的种类	13
1.4.1 谁是入侵者	13
1.4.2 安全威胁的分类	14
1.5 制定和评估安全策略	21
1.5.1 风险分析	22
1.5.2 网络安全策略的构成	24
1.5.3 准备安全策略	26
1.5.4 一个安全策略的模板	27
1.5.5 网络安全监视	29
1.6 案例研究	31
1.6.1 范围和权限的定义	32
1.6.2 关于计算机使用的策略	33
1.6.3 鉴别和识别用户的策略	33
1.6.4 远程访问的策略	33
1.6.5 访问因特网的策略	34
1.7 小结	34
第 2 章 互联网协议的网络安全	35
2.1 保护网站	35
2.1.1 保护敏感数据	36
2.1.2 按可信程度划分网络	37
2.1.3 建立安全边界	38
2.1.4 边界网络	38

2.1.5	保护网站	39
2.2	网络的完整性	41
2.2.1	MD5 标准	41
2.2.2	PGP 标准	42
2.3	理解运输层的安全	42
2.3.1	安全外壳协议	43
2.3.2	安全套接层协议	44
2.3.3	PCT 协议	46
2.3.4	TLS 协议	47
2.4	理解网络层的安全	48
2.4.1	IPSec 协议	48
2.4.2	IPv6 协议	50
2.5	理解数据链路层的安全	50
2.5.1	点对点协议	51
2.5.2	虚拟局域网	52
2.5.3	虚拟专用网	54
2.6	关于 IP 安全的 Cisco 软硬件产品	55
2.6.1	Cisco Secure PIX Firewall	56
2.6.2	Cisco IOS Firewall	56
2.6.3	Cisco Secure Scanner	57
2.6.4	Cisco Secure Policy Manager	57
2.6.5	Cisco Secure Intrusion-Detection System	57
2.6.6	Cisco Secure Access Control Server	58
2.6.7	Cisco IOS 软件	58
2.6.8	Cisco Security Posture Assessment	59
2.7	小结	59
第 3 章	入侵检测	61
3.1	理解入侵检测的概念	61
3.1.1	基于网络的入侵检测系统	61
3.1.2	基于主机的入侵检测系统	64
3.1.3	比较两种入侵检测系统	66
3.2	网络攻击和入侵的原因	67
3.2.1	错误的配置	67
3.2.2	无效的安全策略	67
3.2.3	技术上的缺陷	68
3.3	TCP/IP 协议组的缺陷	68
3.3.1	物理层和数据链路层	69
3.3.2	网络层	69
3.3.3	运输层	70
3.3.4	应用层	70
3.3.5	ICMP 的缺陷	70

3.3.6 RIP 的缺陷	71
3.4 Cisco 安全策略	71
3.4.1 防火墙	71
3.4.2 加密	75
3.4.3 鉴别	77
3.4.4 访问控制表	78
3.5 Cisco IOS 入侵检测系统	79
3.5.1 Cisco IOS 入侵检测系统的特性	79
3.5.2 管理防火墙	81
3.5.3 配合使用 Cisco IOS 软件和 Cisco IOS 防火墙	81
3.5.4 Cisco IOS 防火墙的用户	81
3.5.5 Cisco IOS 入侵检测系统特征信号列表	81
3.5.6 Cisco 安全入侵检测系列产品	82
3.6 小结	83
第 2 部分 提高网络安全性	85
第 4 章 提高网络基础设施的安全性	87
4.1 园区网的安全问题	88
4.2 管理接口的安全化	88
4.2.1 保护控制台访问	89
4.2.2 加密口令	92
4.2.3 管理会话超时	93
4.2.4 使用标志消息作为欢迎和指示信息	93
4.2.5 控制 Telnet 访问	94
4.2.6 管理 HTTP 访问	96
4.2.7 控制 SNMP 访问	97
4.3 保护物理设备	99
4.4 提高路由器到路由器通信的安全性	100
4.4.1 配置文件安全	100
4.4.2 鉴别选路协议	100
4.4.3 通过过滤器进行流量控制	101
4.5 提高以太网交换机的安全性	103
4.5.1 以太网交换机的控制访问	103
4.5.2 端口安全	104
4.5.3 访问安全	104
4.6 案例研究	105
4.6.1 方案说明	105
4.6.2 配置举例	106
4.7 小结	108
第 5 章 通过 ACL 提高网络安全性	109
5.1 基于策略的选路	109

5.1.1	match 命令	110
5.1.2	set 命令	110
5.2	访问表概述	110
5.2.1	访问表的操作过程	112
5.2.2	如何实现访问表	114
5.2.3	配置访问表的基本命令	114
5.3	TCP/IP 访问表	116
5.3.1	IP 地址	116
5.3.2	子网划分	118
5.3.3	子网掩码	118
5.3.4	通配符掩码	120
5.3.5	标准 IP 访问表	122
5.3.6	扩展 IP 访问表	125
5.3.7	如何放置访问表	129
5.3.8	命名 IP 访问表	130
5.4	动态访问表	131
5.4.1	锁和键的运做过程	131
5.4.2	配置动态访问表	132
5.4.3	动态访问表的配置技巧	134
5.5	反访问表	135
5.5.1	用基本访问表和反访问表进行会话过滤	135
5.5.2	反访问表的运作过程	136
5.5.3	FTP 问题	136
5.5.4	配置反访问表	137
5.5.5	反访问表配置实例	139
5.6	监视访问表	140
5.7	案例研究	141
5.7.1	方案说明	141
5.7.2	配置举例	141
5.8	小结	142
第 6 章	通过 Cisco 边界路由器保护网络	143
6.1	边界路由器	143
6.1.1	DMZ 区域	144
6.1.2	堡垒主机	144
6.1.3	Cisco 边界路由器的特性	146
6.1.4	边界路由器所执行的任务	147
6.1.5	Cisco 路由器和 Cisco IOS 软件	149
6.2	NAT 概述	149
6.3	使用 NAT	150
6.3.1	NAT 实现	151
6.3.2	地址转换类型	151
5.4	NAT 操作	152

6.4.1	内部本地地址转换	152
6.4.2	超载内部全局地址	153
6.4.3	TCP 负载分发	154
6.4.4	网络重叠	154
6.5	配置 NAT	156
6.5.1	静态 NAT 映射	156
6.5.2	动态 NAT 配置	157
6.5.3	配置内部全局地址超载	158
6.5.4	配置 TCP 负载分发	159
6.5.5	配置 NAT 映射重叠地址	160
6.6	NAT 的验证和故障定位	161
6.7	NAT 的优点和缺点	162
6.7.1	NAT 的优点	163
6.7.2	NAT 的缺点	163
6.8	案例研究	163
6.8.1	方案说明	163
6.8.2	配置举例	163
6.9	小结	164
第 7 章	Cisco 加密技术	165
7.1	Cisco 加密技术概述	165
7.1.1	常见的网络安全攻击	165
7.1.2	理解加密和解密	166
7.1.3	实现加密	168
7.1.4	使用加密的应用	171
7.1.5	在哪里实现加密	171
7.1.6	AIM 模块	173
7.1.7	Cisco IOS 加密系统概述	173
7.2	配置 Cisco 加密	177
7.2.1	用 DSS 创建公钥和私钥	178
7.2.2	交换 DSS 公共密钥	178
7.2.3	使用 DES 加密算法	179
7.2.4	分类加密图并将其应用于接口	179
7.2.5	用 GRE 隧道配置加密	181
7.2.6	加密的测试和验证	181
7.2.7	Cisco 加密技术的故障定位	183
7.2.8	用于定制加密的选项	183
7.3	小结	184
第 3 部分	通过防火墙提高安全性	185
第 8 章	Cisco IOS 防火墙	187
8.1	Cisco IOS 防火墙概述	187

8.1.1	Cisco IOS 软件的特点	188
8.1.2	Cisco IOS 的脆弱性	189
8.1.3	Cisco IOS 防火墙的优点	189
8.2	Cisco IOS 防火墙组件	190
8.3	基于上下文的访问控制	192
8.3.1	CBAC 功能	192
8.3.2	CBAC 的运做	193
8.3.3	CBAC 的处理过程	194
8.3.4	配置 CBAC	195
8.3.5	验证 CBAC	203
8.3.6	调试 CBAC	203
8.3.7	关闭 CBAC	204
8.3.8	解释 CBAC 所产生的消息	205
8.3.9	CBAC 的优点	206
8.3.10	CBAC 的缺点	206
8.3.11	兼容性问题	207
8.3.12	Cisco IOS 防火墙管理	207
8.3.13	CBAC 配置	208
8.4	案例研究	208
8.4.1	方案说明	208
8.4.2	配置举例	209
8.5	小结	209
第 9 章	Cisco PIX 防火墙	211
9.1	Cisco PIX 简介	211
9.1.1	PIX ASA	212
9.1.2	直通式代理鉴别	214
9.1.3	管道和静态转换	214
9.2	各型号 PIX 防火墙的比较	215
9.2.1	Cisco Secure PIX 535 防火墙	217
9.2.2	Cisco Secure PIX 525 防火墙	217
9.2.3	Cisco Secure PIX 515 防火墙	218
9.2.4	Cisco Secure PIX 506 防火墙	219
9.2.5	Cisco Secure PIX 501 防火墙	220
9.3	PIX 防火墙的故障切换	220
9.4	配置 PIX 防火墙	221
9.4.1	非特权模式	222
9.4.2	特权模式	222
9.4.3	配置模式	223
9.4.4	在接口上实施安全	223
9.4.5	配置防火墙	224
9.4.6	保存配置	225

9.5	高级PIX 防火墙功能	225
9.5.1	控制穿过防火墙的出站访问	226
9.5.2	控制穿过防火墙的入站访问	231
9.6	监视PIX 防火墙配置	237
9.7	案例研究	239
9.8	小结	241
第 4 部分 理解和实现 AAA		243
第 10 章 Cisco AAA 安全技术		245
10.1	通过 AAA 提高网络访问的安全性	245
10.1.1	AAA 安全服务	245
10.1.2	AAA 和访问通信流	247
10.1.3	AAA 安全服务器	247
10.1.4	Cisco 安全访问控制服务器	254
10.2	鉴别方法	256
10.2.1	用户名 / 口令鉴别	256
10.2.2	S/Key 鉴别	258
10.2.3	安全卡	259
10.2.4	PPP 上的 PAP 和 CHAP 鉴别	261
10.2.5	TACACS+ 鉴别	264
10.2.6	RADIUS 鉴别	264
10.2.7	Kerberos 鉴别	265
10.3	授权方法	267
10.3.1	TACACS+ 授权	268
10.3.2	RADIUS 授权	269
10.4	记账方法	269
10.4.1	TACACS+ 记账	270
10.4.2	RADIUS 记账	271
10.5	理解代理鉴别	272
10.5.1	关于鉴别代理的讨论	272
10.5.2	配置鉴别代理	273
10.6	小结	274
第 11 章 配置网络接入服务器使用 AAA 安全功能		275
11.1	AAA 安全服务器	275
11.1.1	AAA 与本地安全数据库的关系	275
11.1.2	AAA 与远程安全数据库的关系	276
11.1.3	Cisco 支持的远程安全数据库标准	277
11.1.4	保护远程访问安全所面临的挑战	278
11.1.5	在 NAS 上配置 AAA	278
11.2	保护特权 EXEC 和配置模式的安全	279
11.3	配置 AAA 鉴别概貌文件	280

11.4	允许 AAA 授权	282
11.5	配置 AAA 记账	282
11.6	案例研究	283
11.6.1	方案说明	283
11.6.2	配置举例	283
11.7	小结	285
第 5 部分 虚拟专用网		287
第 12 章 虚拟专用网基础		289
12.1	VPN 简介	289
12.1.1	实现 VPN 的方法	291
12.1.2	完整 VPN 解决方案的特性	292
12.2	为什么要实现 VPN	293
12.2.1	VPN 关注的问题	293
12.2.2	用户机构获得的好处	294
12.2.3	ISP 获得的好处	294
12.2.4	部署 VPN 应考虑的事项	297
12.3	在 VPN 中传输数据	299
12.4	VPN 的类型	301
12.4.1	内联网 VPN	301
12.4.2	外联网 VPN	302
12.4.3	远程访问 VPN	303
12.5	隧道协议	304
12.5.1	自愿隧道	304
12.5.2	强制隧道	305
12.5.3	PPTP	305
12.5.4	第 2 层转发协议	312
12.5.5	第 2 层隧道协议	317
12.5.6	PPTP, L2F 和 L2TP 的比较	323
12.6	VPN 案例	324
12.6.1	连接分部办公室的网络	324
12.6.2	连接商业伙伴和供应商的网络	324
12.6.3	远程访问网络	324
12.7	小结	325
第 13 章 提高虚拟专用网的安全性		327
13.1	基本 VPN 技术	327
13.1.1	点到点隧道协议	327
13.1.2	第 2 层转发	328
13.1.3	第 2 层隧道协议	328
13.1.4	IPSec	329

13.2	IPSec 概述	329
13.2.1	创建鉴别首部	330
13.2.2	封装安全净载	331
13.2.3	因特网密钥交换	331
13.2.4	IPSec 的工作过程	333
13.3	实现 IPSec	335
13.3.1	为 IPSec 做规划	335
13.3.2	配置 IKE	335
13.3.3	配置 IPSec	336
13.3.4	验证 IPSec	338
13.4	Cisco Secure VPN 客户软件	338
13.4.1	Cisco Secure VPN 客户软件完成的任务	338
13.4.2	Cisco Secure VPN 客户软件的功能特点	339
13.4.3	安装 Cisco Secure VPN 客户软件的系统需求	339
13.5	小结	342
第 6 部分 Cisco 技术和安全产品		343
第 14 章 Cisco IOS IPSec		345
14.1	利用预共享密钥配置 Cisco IPSec	345
14.1.1	为实施 IPSec 制定规划	345
14.1.2	配置 IKE	346
14.1.3	在配置 IPSec 时使用变换集	348
14.1.4	验证 IPSec 配置	351
14.2	利用 RSA 加密随机数配置 Cisco IOS IPSec	353
14.2.1	为 IPSec 做准备	353
14.2.2	配置 RSA 加密	354
14.2.3	为 RSA 加密随机数配置 IKE	355
14.3	扩展 Cisco VPN 的范围	355
14.3.1	使用动态加密图	355
14.3.2	实施 IKE 模式配置	356
14.3.3	PIX 防火墙上的 IPSec 扩展鉴别	357
14.3.4	配置隧道端点发现	358
14.4	小结	358
第 15 章 Cisco 的网络安全管理产品		361
15.1	CiscoWorks2000 ACL Manager	361
15.1.1	ACL Manager 的功能特性	362
15.1.2	ACL Manager 的工具	363
15.1.3	ACL Manager 带来的好处	365
15.1.4	ACL Manager 完成的任务	365
15.1.5	安装 ACL Manager 的配置需求	366

15.1.6	安装 ACL Manager	366
15.1.7	ACL Manager 支持的设备	367
15.2	Cisco 安全策略管理器	367
15.2.1	CSPM 的功能特性集	367
15.2.2	CSPM 的版本	368
15.2.3	CSPM 的许可证选项	369
15.2.4	CSPM 的功能特性	369
15.2.5	CSPM 的优点	370
15.2.6	配置任务	370
15.2.7	安装 CSPM 的配置需求	371
15.2.8	安装 CSPM	371
15.2.9	登录到 CSPM	373
15.2.10	CSPM 的实现	373
15.2.11	CSPM 支持的设备	373
15.3	Cisco Secure ACS	374
15.3.1	基于 Windows NT 的 Cisco Secure ACS	374
15.3.2	ACS 的功能	376
15.3.3	CSNT 的模块	378
15.3.4	安装 CSNT 的系统需求	381
15.3.5	配置 CSNT	382
15.3.6	管理 CSNT	383
15.3.7	配置 CSNT 管理员账号	383
15.3.8	查找 CSNT 故障	384
15.3.9	基于 UNIX 的 Cisco Secure ACS	384
15.4	小结	385
第 16 章	Cisco 防火墙和 VPN 管理产品	387
16.1	Cisco PIX 防火墙管理器	387
16.1.1	PIX 防火墙管理器的组件	387
16.1.2	PIX 防火墙管理器的优点	388
16.1.3	安装 PIX 防火墙管理器	388
16.1.4	SYSLOG 报告	392
16.1.5	PIX 管理器的局限性	392
16.2	VPN/安全管理解决方案	393
16.2.1	VMS 带来的好处	393
16.2.2	VMS 的组件	393
16.2.3	安装和更新 CiscoWorks2000 VMS	395
16.2.4	在清单中加入设备	398
16.2.5	更新清单中的设备	398
16.2.6	检验安装	398
16.3	小结	398

第7部分 网络基础知识	399
第17章 网络基础	401
17.1 网络基础入门	401
17.2 网络模型	402
17.2.1 客户/服务器模型	402
17.2.2 对等网络模型	403
17.3 网络的分类	404
17.3.1 局域网	404
17.3.2 广域网	404
17.3.3 公用网	406
17.3.4 内联网	407
17.3.5 外联网	410
17.4 网络拓扑结构	411
17.4.1 总线型拓扑结构	411
17.4.2 环形拓扑结构	412
17.4.3 星型拓扑结构	413
17.4.4 星型总线型拓扑结构	413
17.4.5 星型环型拓扑结构	414
17.5 网络传输媒体	415
17.5.1 同轴电缆	415
17.5.2 双绞线	417
17.5.3 光纤	418
17.5.4 IBM 电缆系统	419
17.6 专线	420
17.6.1 常规专线	420
17.6.2 T1 链路	420
17.6.3 T2 链路	420
17.6.4 T3 链路	421
17.6.5 T4 链路	421
17.7 局域网的网络体系结构	421
17.7.1 以太网	421
17.7.2 令牌环	423
17.7.3 光纤分布式数据接口	424
17.7.4 异步传输模式	425
17.8 网络设备	425
17.8.1 中继器	426
17.8.2 集线器	426
17.8.3 网桥	426
17.8.4 路由器	427
17.8.5 桥式路由器	427
17.8.6 网关	428

17.8.7 调制解调器	428
17.8.8 交换机	428
17.9 网络管理	429
17.9.1 网络管理系统	429
17.9.2 网络管理系统的选择	430
17.9.3 网络管理体系结构	431
17.9.4 网络管理功能域	432
17.10 网络管理协议	436
17.10.1 SNMP 模型	437
17.10.2 SNMPv2	441
17.10.3 CMIP	442
17.10.4 RMON	443
17.11 小结	446
第 18 章 OSI 模型	447
18.1 标准化组织	447
18.2 OSI 网络模型	448
18.2.1 物理层	448
18.2.2 数据链路层	449
18.2.3 网络层	456
18.2.4 运输层	457
18.2.5 会话层	458
18.2.6 表示层	459
18.2.7 应用层	459
18.3 OSI 的数据传输	459
18.3.1 帧	460
18.3.2 数据传输	460
18.4 协议	461
18.4.1 数据链路层协议	461
18.4.2 网络层协议	463
18.4.3 运输层协议	466
18.5 小结	467
附录 A 习题与参考答案	469
附录 B 实验练习	539
词汇表	543