

最实用全面
常备参考书

网络完全技术宝典

17 大网络安全内容详解 7 项配置管理操作 105 段视频全程演示

网络安全 = 实用方案提供 + 按步图解指导
完全技术宝典 = 常用技巧说明 + 视听光盘



网络安全 完全技术宝典

史晓红 编著



- 网络安全分析与规划
- 网络设备及其系统安全：服务器系统安全、网络设备系统安全、网络安全设备和路由器安全
- Internet、局域网和虚拟网接入安全：局域网接入安全、无线网络安全、Internet连接共享服务
- 远程访问及其安全：网络访问防护、网络远程接入安全、网络客户端安全
- 网络应用服务：网络应用服务安全
- 数据安全：数据备份与恢复和数据存储与访问安全
- 防病毒技术：系统漏洞扫描和网络病毒防御
- 网络分析工具：网络流量分析工具

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

网络安全 完全技术宝典



藏史晓红 编著



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书主要从网络操作系统及应用服务、网络设备、网络访问与存储 3 个方面出发,全面介绍了网络安全防御系统的规划与部署。操作系统及应用服务安全主要包括 Windows Server 2008 基本安全配置、系统漏洞安全、活动目录安全、Web 网站访问安全、FTP 服务安全、网络防病毒系统以及 Windows Vista 和 Windows XP 客户端的安全部署。网络设备安全主要包括交换机、路由器、网络安全设备以及 IOS 的安全配置。网络访问与存储安全主要包括网络访问防护、远程访问安全、Forefront TMG 安全网关、数据存储与访问安全以及网络流量分析等内容。

本书内容全面、技术新颖、图文并茂、贴近应用、通俗易懂,既可以作为中高级网络安全管理人员的工具用书,也可以作为各类院校相关专业的教材及网络安全培训班教材,还可作为高校毕业生充电的自学参考书。

图书在版编目(CIP)数据

网络安全完全技术宝典/史晓红 编著. —北京:
中国铁道出版社, 2009. 12
ISBN 978-7-113-10924-0
I. ①网… II. ①史… III. ①计算机网络—安全技术
IV. ①TP393. 08
中国版本图书馆 CIP 数据核字 (2009) 第 236634 号

书 名: 网络安全完全技术宝典
作 者: 史晓红 编著

责任编辑: 韩中领
特邀编辑: 孙佳志
封面设计: 王加宝
版式设计: 郑少云

编辑部电话: (010) 63583215
责任校对: 王 宏
封面制作: 白 雪
责任印制: 李 佳

出版发行: 中国铁道出版社(北京市宣武区右安门西街 8 号 邮政编码: 100054)
印 刷: 北京市彩桥印刷有限责任公司
版 次: 2010 年 3 月第 1 版 2010 年 3 月第 1 次印刷
开 本: 787mm×1092mm 1/16 印张: 43 字数: 1037 千
印 数: 3 000 册
书 号: ISBN 978-7-113-10924-0
定 价: 88.00 元(附赠光盘)

版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社计算机图书批销部联系调换。

前言

本书的写作目的

随着 Internet 技术的迅速发展,现代人的工作和生活有了前所未有的改变,工作效率大幅提高,物质文化生活日益丰富。人们在充分享受网络带来的便利的同时,也不得不面对一个非常严峻的问题——网络安全。正是 Internet 应用技术的广泛性,使得安全问题影响到人们的生活和利益。不仅如此,许多企业管理者也越来越重视网络的应用,并开始意识到网络安全问题对企业效益增长和生产效率提高的制约。网络安全已成为网络建设不可或缺的组成部分。

网络安全管理不同于网络应用管理。对于服务器或网络设备应用而言,管理员只需按照相关程序发挥服务器或网络设备的性能即可;而网络安全管理是整个网络的基础,安全管理员必须综合考虑各方面可能的因素。因此,网络安全管理员需要具备的知识量是非常惊人的,知识的学习和积累是至关重要的,只有看得多,学得多,懂得多,才能对各种安全问题应对自如。

本书适合哪些人阅读

- ❖ 大中型网络安全管理员和系统管理员
- ❖ 即将从事网络管理工作的计算机和网络技术爱好者
- ❖ 高校毕业生就业前的自学参考书
- ❖ 高级网络培训班的参考教材
- ❖ 大专院校的实训教程

读者能从本书学到什么

- ❖ 能够熟练掌握 Windows Server 2008 安全功能并运用到网络管理中
- ❖ 能够根据用户需求打造安全的网络服务器,并确保网络服务访问安全
- ❖ 掌握主流 Cisco 网络设备的安全配置与管理技术
- ❖ 能够洞察网络潜在的各种威胁,将安全隐患消灭于无形
- ❖ 借助 NAP、IPSec、Forefront TMG 等安全新技术保护网络安全

本书有哪些特色

第一,面向需求。当今正是网络应用迅速普及的时期,网络安全问题已经成为困扰众多企业发展的难题,以致许多用户不得不面对来自四面八方的网络威胁与攻击。本书正是适应了这些用户的需求,将网络安全技术渗透到每一项网络应用当中,充分确保网络的安全运行。

第二,技术新颖。本书主要以 Microsoft 推出的 Windows Server 2008 网络服务平台为例,介绍网络服务器系统以及应用服务的安全配置。IPSec 防火墙规则、NAP、RODC、AD DS、

IIS 7.0 等都是 Windows Server 2008 系统新增的功能,这些新增的内容均可在本书中找到,同时提供了部署方案实例。

第三,实用为主。本书以应用为本,全面介绍安全局域网的打造。软件方面主要包括服务器系统、客户端系统、局域网访问控制、远程访问安全、网络防病毒、局域网流量分析等内容,它们都是局域网中最常用的应用技术。硬件方面则介绍接入交换机、路由器、安全设备等局域网必备设备的安全配置。

第四,实例教学。本书采用具有实际意义的案例,不仅让广大读者掌握了技术,更是一种实际经验的积累。为了避免一味地阐述深奥的理论知识,本书还采用了大量的图片来加以说明,这在增强了图书的趣味性和可读性的同时,可以让读者轻松地学习到知识。

第五,演示光盘。随书附送一张演示光盘,涵盖了书中所有重要实例的演示,读者只需根据光盘中的实例操作,即可轻松实现相应的功能。

各章节主要内容

本书共分 17 章,每章的具体内容如下表所示。

章	本 章 内 容
第 1 章	概括介绍网络安全包含的主要内容、面临的主要问题以及网络安全的总体规划
第 2、3 章	介绍服务器系统安全,包括 Windows Server 2008 常规安全配置、系统漏洞安全以及借助 WSUS 进行服务器和客户端的系统更新的方法
第 4 章	介绍常用网络服务的安全,包括活动目录服务、WWW 服务、FTP 服务等的安全配置与管理
第 5 章	简要介绍了病毒的定义、特点以及对网络安全的威胁,以 Symantec 网络防病毒系统为例,介绍了局域网防病毒系统的部署与应用
第 6 章~ 第 9 章	主要介绍常用网络设备安全,包括网络设备 IOS 安全、路由器安全配置、交换机安全配置以及网络安全设备的应用与管理
第 10 章	介绍无线局域网的安全配置,常用的安全技术包括传输加密和身份验证
第 11 章	介绍 NAP 技术的应用,NAP 技术是 Microsoft 公司推出的网络访问保护技术,可以用于确保局域网访问与接入的安全
第 12、13 章	介绍如何使用 Forefront TMG 实现局域网共享接入、安全防护以及内网服务器的发布。远程访问安全主要介绍了 VPN 技术的应用与部署
第 14、15 章	介绍局域网数据的安全存储与访问技术,主要包括主流的网络存储方案部署、局域网访问安全控制以及数据的备份与恢复技术等
第 16 章	以 Windows Vista 和 Windows XP Professional 系统为例,介绍如何打造客户端系统安全,以及管理员如何通过 GPMC 快速部署客户端安全策略
第 17 章	介绍常用的网络流量分析工具的应用,以便管理员可以实时掌握局域网运行情况

技术团队及技术支持

本书由史晓红编著，赵卫东、刘淑梅、马倩、杨伏龙、李文俊、王同明、石长征、郭腾、白华、莫展宏、许坦、李海宁、陈志成、田俊乐、刘国增、王延杰、刘红、王淑江、王春海对本书的编写提出了宝贵意见，并且参与了部分的编写工作。

编者长期从事系统维护和网络管理工作，具有较高的理论水平和丰富的实践经验，曾经出版过 30 余部计算机类图书，均以易读、易学、实用的特点，受到众多读者的一致好评。本书是编者的又一呕心之作，希望能对读者的系统维护和网络管理工作有所帮助。

由于时间仓促，加之编者水平有限，并且本书涉及的系统与知识点较多，虽然力求完善，但书中难免有不妥和遗漏之处，欢迎大家与我们联系和交流。

技术支持邮箱：wwb_beijing@163.com

技术支持 QQ：19559955

编 者

2009 年 10 月

配套光盘说明

软硬件需求

硬件:

PIII 500 以上 CPU、256MB 以上内存、200MB 以上可用硬盘空间、支持 1024×768 分辨率的显卡和显示器、CD 或 DVD 光驱、声卡、音箱或耳机。

软件:

Windows 98/2000/Me/2003/XP/Vista 操作系统, 显示器设置为 1024×768 分辨率。

操作指南

步骤 1 关闭所有正在运行的应用程序, 将多媒体演示光盘置入光驱, 光盘将自动运行, 显示光盘名称界面 (见图 1), 当出现鼠标光标时, 在界面上进行单击操作, 进入光盘章节界面 (见图 2)。

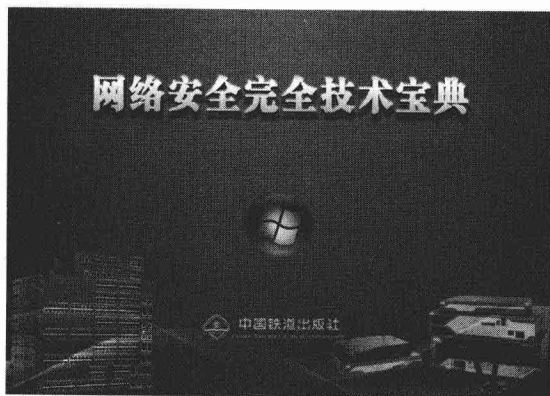


图 1 光盘名称界面



图 2 光盘章节界面

步骤 2 在光盘章节界面中单击^①按钮, 弹出帮助框 (见图 3); 再次单击^②按钮, 关闭帮助框。单击^③按钮, 显示光盘的制作团队信息 (见图 7)。

步骤 3 在光盘章节界面中单击感兴趣的章节对应的按钮, 进入要学习视频内容的播放界面 (见图 4), 视频自动播放, 本光盘默认从第一个视频开始播放。读者可以按照自己的需要调整解说(本光盘没有提供解说)和背景音乐的音量, 并实现视频的播放、暂停、快进、快退, 也可以拖动视频播放滑块进行快速浏览。

步骤 4 单击“上一个视频”或“下一个视频”按钮, 直接跳到下一个视频或返回上一个视频。也可单击“视频选择”按钮, 弹出视频选择界面 (见图 5), 选择感兴趣的视频进行

播放。单击“返回”按钮，返回至光盘章节界面。

步骤 5 单击^②按钮，弹出帮助框（见图 6）；再次单击^③按钮，关闭帮助框。单击^④按钮，显示光盘的制作团队信息。



图 3 光盘章节界面帮助框

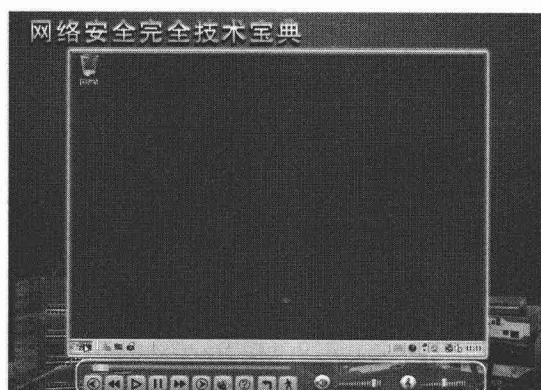


图 4 视频播放界面

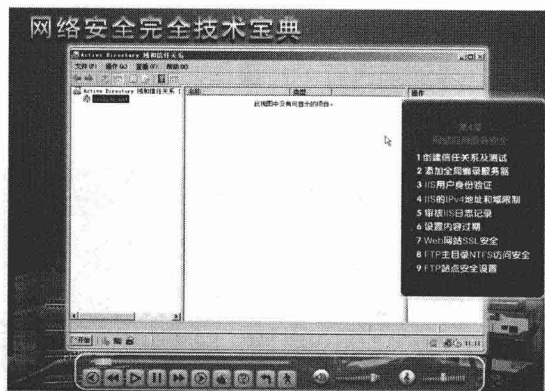


图 5 视频播放界面中的视频选择界面

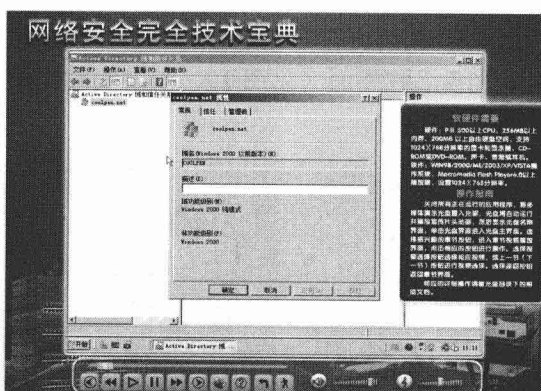


图 6 视频播放界面中的帮助框

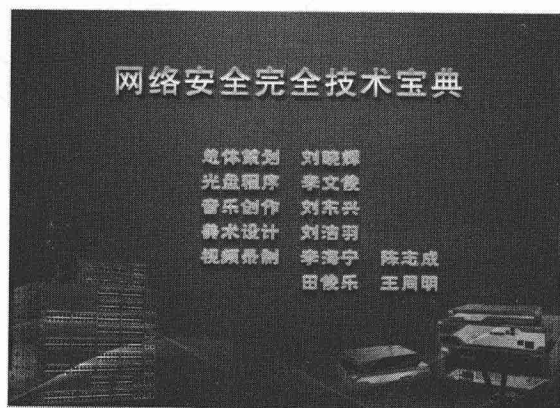


图 7 退出界面

目 录

第 1 章 网络安全分析与规划	1
1.1 安全风险分析	1
1.1.1 资产保护	1
1.1.2 网络攻击	2
1.1.3 风险管理	3
1.2 网络信息安全防御体系	4
1.2.1 网络信息安全防御体系的特性	4
1.2.2 运行机制	5
1.2.3 实现机制	6
1.2.4 网络威胁	7
1.3 网络安全技术	8
1.3.1 防病毒技术	8
1.3.2 防火墙技术	9
1.3.3 入侵检测技术	10
1.3.4 安全扫描技术	10
1.3.5 网络安全紧急响应体系	11
1.4 网络设备系统安全	11
1.4.1 网络设备的脆弱性	11
1.4.2 部署网络安全设备	12
1.4.3 IOS 安全	12
1.5 局域网接入安全	12
1.5.1 常规接入安全措施	13
1.5.2 NAC 技术	13
1.5.3 NAP 技术	13
1.5.4 TNC 技术	14
1.6 服务器系统安全	14
1.6.1 服务器硬件安全	14
1.6.2 操作系统安全	14
1.7 网络应用服务安全	15
1.8 数据安全	15
1.8.1 数据存储安全	15
1.8.2 数据访问安全	16
1.9 Internet 接入安全	17
1.9.1 代理服务器	17

1.9.2 防火墙.....	17
1.10 远程访问安全.....	18
1.10.1 IPSec VPN 远程安全接入.....	18
1.10.2 SSL VPN 远程安全接入.....	18
1.11 数据灾难与数据恢复.....	18
1.12 网络管理安全.....	19
1.12.1 安全管理规范.....	19
1.12.2 网络管理.....	20
1.12.3 安全管理.....	20
1.13 网络安全规划与设计.....	21
1.13.1 网络安全规划原则.....	21
1.13.2 划分 VLAN 和 PVLAN.....	22
1.13.3 客户端安全.....	23
第 2 章 服务器系统安全.....	24
2.1 服务器系统安全概述.....	24
2.1.1 影响服务器系统安全的因素.....	24
2.1.2 系统安装的注意事项.....	25
2.1.3 系统服务配置的注意事项.....	25
2.1.4 补丁安装的注意事项.....	26
2.1.5 Internet 防火墙简介.....	27
2.1.6 服务端口与端口威胁.....	27
2.2 Windows Update 配置及应用.....	28
2.2.1 配置 Windows Update.....	29
2.2.2 安装系统更新.....	30
2.3 系统管理员账户.....	31
2.3.1 默认组权限.....	31
2.3.2 更改 Administrator 账户名称.....	33
2.3.3 系统管理员口令设置.....	35
2.3.4 创建陷阱账户.....	37
2.4 磁盘访问权限.....	38
2.4.1 权限范围.....	38
2.4.2 设置磁盘访问权限.....	39
2.4.3 查看磁盘权限.....	40
2.5 系统账户数据库.....	40
2.5.1 启用加密.....	41
2.5.2 删除系统账户数据库.....	42
2.6 安全配置向导.....	43
2.6.1 配置和应用安全配置向导注意事项.....	43

2.6.2	配置安全服务.....	43
2.6.3	应用安全配置策略.....	49
2.7	配置 Windows 防火墙.....	50
2.8	关闭端口.....	52
2.8.1	查看端口.....	53
2.8.2	启动/关闭服务.....	55
2.9	系统服务安全.....	56
2.9.1	服务账户.....	56
2.9.2	服务权限.....	56
2.9.3	漏洞和应对措施.....	57
2.9.4	配置系统服务安全.....	58
2.10	安全策略.....	59
2.10.1	账户策略.....	59
2.10.2	限制用户登录.....	61
2.10.3	审核策略.....	63
2.10.4	IPSec 安全策略.....	66
第 3 章	系统漏洞扫描.....	73
3.1	漏洞概述.....	73
3.1.1	漏洞的特性.....	73
3.1.2	漏洞生命周期.....	74
3.2	漏洞扫描.....	75
3.2.1	漏洞扫描概述.....	75
3.2.2	MBSA.....	76
3.2.3	360 安全卫士.....	83
3.2.4	X-Scan.....	85
3.2.5	系统补丁部署概述.....	89
3.3	漏洞预警.....	90
3.3.1	安全中心.....	91
3.3.2	中文速递邮件服务.....	91
3.3.3	中文网络广播.....	92
3.4	Windows 系统更新管理.....	93
3.4.1	WSUS 概述.....	93
3.4.2	WSUS 服务器的安装.....	94
3.4.3	配置 WSUS 服务器常规选项.....	97
3.4.4	计算机分组管理.....	100
3.4.5	同步和管理更新.....	102
3.4.6	为客户端审批更新.....	104
3.4.7	WSUS 客户端的安装和设置.....	107

3.4.8 客户端更新部署.....	111
第4章 网络应用服务安全	112
4.1 活动目录安全.....	112
4.1.1 限制用户登录域控制器.....	112
4.1.2 目录访问权限.....	114
4.1.3 只读域控制器.....	114
4.1.4 可以重启的 AD DS.....	119
4.1.5 辅助域控制器.....	120
4.1.6 信任关系类型.....	122
4.1.7 创建信任关系.....	124
4.1.8 SYSVOL 目录概述.....	126
4.1.9 SYSVOL 重定向.....	127
4.1.10 更改 SYSVOL 存储空间.....	130
4.1.11 全局编录概述.....	131
4.1.12 添加全局编录服务器.....	132
4.2 IIS 安全机制.....	133
4.2.1 IIS 访问控制安全.....	133
4.2.2 NTFS 访问安全.....	134
4.2.3 身份验证.....	135
4.2.4 IIS 安装安全.....	136
4.3 Web 网站访问安全.....	136
4.3.1 用户控制安全.....	136
4.3.2 访问权限控制.....	138
4.3.3 IPv4 地址控制.....	141
4.3.4 设置内容过期.....	143
4.3.5 内容分级设置.....	143
4.4 安全 Web 网站.....	145
4.4.1 Web 服务器端设置.....	145
4.4.2 客户端设置.....	147
4.5 FTP 站点访问安全.....	147
4.5.1 设置 TCP 端口.....	148
4.5.2 连接数量限制.....	148
4.5.3 用户访问安全.....	149
4.5.4 文件访问安全.....	151
第5章 网络病毒防御	152
5.1 病毒概述.....	152
5.1.1 计算机病毒.....	152
5.1.2 木马病毒.....	153

5.1.3	蠕虫病毒.....	154
5.1.4	网页病毒.....	154
5.1.5	恶意软件.....	155
5.1.6	中毒症状.....	156
5.1.7	传播途径.....	157
5.1.8	计算机病毒的危害.....	158
5.2	网络防病毒软件.....	159
5.2.1	网络防病毒系统.....	159
5.2.2	服务器端与客户端.....	159
5.3	McAfee 防病毒产品.....	160
5.3.1	McAfee 防病毒产品的特点.....	160
5.3.2	McAfee ePolicy Orchestrator.....	161
5.4	Symantec AntiVirus.....	163
5.4.1	Symantec Endpoint Protection 的功能与特点.....	163
5.4.2	Symantec Network Access Control 概述.....	164
5.4.3	Symantec Endpoint Protection Manager 概述.....	165
5.4.4	可选组件.....	165
5.4.5	Symantec Endpoint Protection Manager 的工作方式.....	165
5.4.6	Symantec Endpoint Protection Manager 的功能.....	166
5.5	瑞星杀毒软件网络版.....	166
5.5.1	版本分类.....	167
5.5.2	瑞星网络防病毒系统的构成.....	167
5.6	Symantec Endpoint Protection 企业版的安装.....	168
5.6.1	安装要求.....	169
5.6.2	安装 Symantec Endpoint Protection Manager.....	170
5.6.3	配置 Symantec Endpoint Protection Manager.....	171
5.6.4	迁移和部署向导.....	174
5.6.5	安装 Symantec Endpoint Protection Manager Web 控制台.....	177
5.7	安装 Endpoint Protection Manager 客户端.....	177
5.7.1	安装受管理客户端.....	178
5.7.2	部署非受管客户端.....	182
5.8	升级病毒库.....	184
5.8.1	安装 LiveUpdate 管理工具.....	184
5.8.2	登录 Symantec LiveUpdate Administrator.....	185
5.8.3	配置 LiveUpdate.....	186
5.8.4	下载和分发.....	187
5.8.5	配置 LiveUpdate 策略.....	190

第6章 网络设备系统安全	193
6.1 网络设备系统安全概述	193
6.1.1 登录密码安全简介	193
6.1.2 配置命令级别安全简介	194
6.1.3 SNMP 安全简介	195
6.1.4 终端访问限制安全简介	195
6.1.5 HTTP 服务安全简介	195
6.1.6 系统安全日志	196
6.1.7 IOS 系统版本升级	198
6.2 登录密码安全详解	199
6.2.1 配置 Enable 密码	199
6.2.2 配置 Telnet 密码	199
6.2.3 配置管理用户	200
6.3 配置命令级别安全详解	200
6.3.1 配置多个用户级别	200
6.3.2 登录和离开授权级别	201
6.4 终端访问限制安全详解	201
6.4.1 控制虚拟终端访问	201
6.4.2 控制会话超时	202
6.5 SNMP 安全详解	202
6.5.1 配置 SNMP 字符串	202
6.5.2 配置 SNMP 组和用户	203
6.5.3 SNMP 配置实例	204
6.6 HTTP 服务安全	205
6.6.1 关闭 HTTP 服务	205
6.6.2 配置安全 HTTP 服务	206
6.6.3 配置安全 HTTP 客户端	207
6.7 系统安全日志	207
6.7.1 启用系统日志信息	207
6.7.2 设置日志信息目的设备	208
6.7.3 配置日志消息的时间戳	209
6.7.4 配置日志序列号	209
6.7.5 定义消息严重等级	210
6.7.6 限制日志发送到历史表和 SNMP	210
6.7.7 配置 UNIX 系统日志服务器	211
6.8 IOS 系统版本升级	212
6.8.1 备份系统软件映像	212
6.8.2 恢复或升级系统软件映像	214

第 7 章 局域网接入安全.....	216
7.1 局域网接入安全概述.....	216
7.1.1 基于端口的传输控制简介.....	216
7.1.2 动态 ARP 检测简介.....	217
7.1.3 基于端口的认证安全简介.....	217
7.1.4 VLAN 安全简介.....	218
7.1.5 PVLAN 安全简介.....	219
7.1.6 MAC 和 VLAN 访问列表简介.....	221
7.2 基于端口的传输控制详解.....	222
7.2.1 风暴控制.....	222
7.2.2 流量控制.....	224
7.2.3 保护端口.....	224
7.2.4 端口阻塞.....	225
7.2.5 端口安全.....	225
7.2.6 传输速率限制.....	227
7.2.7 MAC 地址更新通知.....	228
7.2.8 绑定 IP 和 MAC 地址.....	231
7.3 动态 ARP 检测详解.....	231
7.3.1 动态 ARP 检测的配置方针.....	232
7.3.2 在 DHCP 环境下配置动态 ARP 检测.....	232
7.3.3 在无 DHCP 环境下配置 ARP ACL.....	233
7.3.4 限制 ARP 数据包的速率.....	234
7.3.5 运行有效检测.....	235
7.3.6 配置日志缓冲.....	235
7.3.7 显示动态 ARP 检测信息.....	236
7.4 基于端口的认证安全详解.....	236
7.4.1 配置 IEEE 802.1x 认证.....	237
7.4.2 配置交换机到 radius 服务器的通信.....	237
7.4.3 配置重新认证周期.....	238
7.4.4 修改安静周期.....	239
7.5 VLAN 安全详解.....	239
7.5.1 划分 VLAN.....	239
7.5.2 设置 VLAN trunk 过滤.....	243
7.6 PVLAN 安全详解.....	245
7.6.1 配置 PVLAN.....	245
7.6.2 将 VLAN 配置为 PVLAN.....	245
7.6.3 关联主 VLAN 与辅 VLAN.....	246
7.6.4 配置 PVLAN 混杂端口.....	246
7.6.5 配置 PVLAN host 端口.....	247

7.6.6	配置 PVLAN Trunk 端口	247
7.6.7	将辅 VLAN 映射为主 VLAN 三层 VLAN 接口	248
7.7	使用 Cisco CNA 配置安全	249
7.7.1	CNA 可管理的设备	249
7.7.2	Cisco CNA 安全导向	249
7.7.3	配置端口安全	254
7.7.4	配置 ACL	258
7.7.5	创建 IP 访问列表	259
7.7.6	MAC 扩展访问列表	265
7.7.7	应用 ACL	266
7.7.8	时间访问列表	267
第 8 章	路由器安全	269
8.1	路由器连接策略	269
8.2	路由器面板	270
8.3	路由器连接	272
8.3.1	与局域网设备之间的连接	272
8.3.2	与 Internet 接入设备的连接	273
8.4	访问控制列表	275
8.4.1	访问列表的类型	275
8.4.2	配置访问列表注意事项	276
8.4.3	访问列表配置步骤	278
8.5	IP 访问列表	278
8.5.1	创建标准访问列表	278
8.5.2	创建扩展访问列表	279
8.5.3	创建 IP 访问列表名称	280
8.6	时间访问列表	282
8.6.1	基于时间的访问列表	282
8.6.2	相关配置命令	284
8.6.3	将 IP 访问列表应用到接口	284
8.7	MAC 访问列表	285
8.7.1	创建端口扩展访问列表名称	285
8.7.2	将端口访问列表应用到二层接口	285
8.8	网络地址转换	286
8.8.1	NAT 概述	286
8.8.2	静态地址转换	287
8.8.3	动态地址转换	288
8.8.4	端口复用地址转换	289

8.9 使用 SDM 配置路由器	290
8.9.1 Cisco SDM 简介	291
8.9.2 SDM 配置路由器——防火墙和 ACL	292
8.9.3 SDM 配置路由器——安全审计	293
8.9.4 SDM 配置路由器——NAT	296
8.10 创建并应用 VLAN 访问列表	298
8.11 网络攻击安全防范	300
8.11.1 IP 欺骗防范	300
8.11.2 SYN 淹没防范	301
8.11.3 Ping 攻击防范	302
8.11.4 DoS 和 DDoS 攻击防范	303
第 9 章 网络安全设备	304
9.1 网络防火墙	304
9.1.1 网络防火墙简介	304
9.1.2 防火墙的主要功能	306
9.1.3 防火墙的局限性	307
9.1.4 防火墙的脆弱性	307
9.2 入侵检测系统	308
9.2.1 IDS 概述	308
9.2.2 IDS 的优势	308
9.2.3 IDS 的缺陷	309
9.3 入侵防御系统	310
9.3.1 IPS 概述	310
9.3.2 IPS 的技术特征	311
9.3.3 IPS 的分类	312
9.3.4 IPS 的技术优势	313
9.3.5 IPS 的缺陷	314
9.4 漏洞扫描系统	315
9.4.1 计算机漏洞的概念	315
9.4.2 存在系统漏洞的原因	315
9.4.3 漏洞扫描概述	316
9.4.4 常用漏洞扫描工具	316
9.5 Cisco ASDM 概述	317
9.5.1 Cisco ASDM 特点	317
9.5.2 Cisco 安全设备准备	319
9.5.3 Cisco ASDM 安装配置	319
9.6 安全设备的端口	321
9.6.1 安全设备的物理端口	321