



CISCO NETWORKING ACADEMY PROGRAM

ciscopress.com



思科网络技术学院教程 网络安全基础

Cisco Networking Academy Program
**Fundamentals of
Network Security**
Companion Guide

The only authorized textbook for the
Cisco Networking Academy Program

内附光盘



[美]

Cisco Systems 公司
Cisco Networking Academy Program

著

李滌非 欧岩亮 秦华

译

 人民邮电出版社
POSTS & TELECOM PRESS



思科网络技术学院教程

网络安全基础

393.08
115

[美] Cisco Systems 公司 著
Cisco Networking Academy Program
李滌非 欧岩亮 秦华 译

人民邮电出版社

图书在版编目 (CIP) 数据

网络安全基础/美国思科公司, 思科网络技术学院著; 李涤非, 欧岩亮, 秦华译.
—北京: 人民邮电出版社, 2005.4
思科网络技术学院教程

ISBN 7-115-13160-0

I. 网... II. ①美...②思...③李...④欧...⑤秦... III. 计算机网络—安全技术—
高等学校—教材 IV. TP393.08

中国版本图书馆 CIP 数据核字 (2005) 第 020940 号

版权 声 明

Cisco System Inc Cisco Networking Academy Program: Cisco Networking Academy Program Fundamental
of Network Security Companion Guide

Copyright ©2004 by Cisco Systems, Inc.

All rights reserved.

本书中文简体字版由美国 Cisco Press 公司授权人民邮电出版社出版。未经出版者书面许可, 对
本书的任何部分不得以任何方式复制或抄袭。

版权所有, 侵权必究。

思科网络技术学院教程

网络安全基础

-
- ◆ 著 [美] Cisco Systems 公司
Cisco Networking Academy Program
 - 译 李涤非, 欧岩亮, 秦华
 - 责任编辑 陈昇
 - ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 ciscobooks@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
读者热线 010-67132705
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销
 - ◆ 开本: 787×1092 1/16
印张: 38.5
字数: 962 千字 2005 年 4 月第 1 版
印数: 1—4 000 册 2005 年 4 月北京第 1 次印刷

著作权合同登记号 图字: 01-2003-4801 号

ISBN 7-115-13160-0/TP·4490

定价: 80.00 元 (附光盘)

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

内容提要

本书是“思科网络技术学院教程 网络安全基础”课程的官方指定教材，是对该课程的课堂教学的补充。全书共分为 15 章，分别介绍了网络安全概览、基础路由器与交换机安全、路由器 ACL 和 CBAC、路由器 AAA 安全、路由器入侵检测、监测和管理、路由器端到端的 VPN、路由器远程访问 VPN、PIX 防火墙、PIX 防火墙的地址转换和连接、PIX 防火墙的访问控制列表（ACL）、PIX 防火墙的 AAA、PIX 高级协议与入侵检测、PIX 故障切换与系统维护、PIX 防火墙 VPN、PIX 防火墙管理等内容。

本书适合参加思科网络技术学院网络安全基础课程的读者使用，对于参加 CCSP 和 CCIE 安全考试的读者也有较大的帮助。

前 言

*网络安全基础*连同*网络安全基础实验练习*，与相应的思科网络学院在线课程一同为您提供网络安全的全面介绍。

思科网络学院课程能帮您在计算机网络领域中获得职位，或者接受深层次的教育培训。网络安全基础课程重点关注基于安全策略的总体安全过程，主要强调安全边界、安全连接、安全管理、身份验证服务和入侵检测。本书也包括在 Cisco IOS 防火墙和 PIX Security Appliance 上安装、配置、监控和维护使用 Cisco 基于 CLI 和基于 Web 的设备管理器。

*网络安全基础*的设计目的是让用户可随时随地参考查阅。本书补充了课程中的材料，帮助您关注重要的概念并有助于安排好您的备考学习时间。

本书完全符合 Cisco 在课程中所使用的形式和格式。附带的光盘中包括了交叉引用的照片活动、电子实验活动，以及以生动的交互多媒体形式表现出的各种学习参考资料。

本书还介绍了 Cisco 公司 CCSP SECUR 和 CSPFA 考试的全部主题。

本书的目标

本书的目标使您学习基于安全策略的总体安全过程，主要强调的领域是安全边界、安全连接、安全管理、身份验证服务和入侵检测。本书设计与思科网络学院课程结合使用，也可单独作为参考资料。

本书的读者

本书面向任何要学习网络安全和总体安全过程的读者。主要的读者是社区学院和四年制的大学本科。本书可用作课堂上的教科书，适合于具有 CCNA 证书或具有同等知识的读者使用。读者应该熟练掌握 TCP/IP 和基本的网络概念。

其次面向的读者是企业的教育职员和全体教师。对于要想获得有效安全措施的公司和机构而言，必须在设计和实施安全技术、产品和解决方案方面对每个人进行培训。

最后面向的是一般用户。对于那些想要避开传统技术手册的用户来说，本书是他们的良师益友。

本书的特性

本书的很多特性可帮助读者加快对本书中所介绍的连网和路由选择技术的全面理解。

- **目标**——每章以一个目标列表开始，学习完本章后应掌握这些目标。目标提供了该章中所介绍概念的参考。

- **图、例、表和案例**——本书包含的图、例和表有助于解释各种理论、概念、命令和安装顺序，从而加深对概念的理解并有助于以直观的方式理解章中所介绍的内容。另外，特定的案例也提供了详细描述问题和解决方案的现实生活场景。
- **章节总结**——每章末尾是该章所涉及概念的总结，它提供了章节提要，可帮助学习。
- **关键术语**——多数章包括该章所涉及的关键术语。这些术语可帮助学习。另外，关键术语强化了章中所介绍的概念，并且在您学习新的概念前，有助于理解该章中的材料，在章中实际使用该术语的位置，您可以找到用黑体和斜体字突出显示的关键术语。
- **复习题和答案**——在每章结尾出现的复习题可作为对学习的评估。这些问题强化了每章中的概念，并且在学习其他章节之前，可测试您对本章内容的掌握情况。
- **技能提高活动**——本书中所引用的试验活动可在《思科网络技术学院教程 网络安全基础实验手册与练习册》一书中找到。这些试验可帮助您将理论与实践相结合。

本书的组织方式

本书分为 15 章和 4 个附录。

- **第 1 章“网络安全概述”**——本章提供基本的网络安全概述，包括对攻击和威胁的介绍，其他的主题包括安全框架和策略，最后介绍了安全产品和解决方案。
- **第 2 章“基本的路由器和交换机安全”**——本章首先介绍了一般的路由器和交换机安全，说明了禁用不需要服务的重要性。本章还介绍了边界路由器的概念，并讨论了路由器管理。最后探讨了保护交换机和 LAN 访问安全的主题。
- **第 3 章“路由器 ACL 和 CBAC”**——本章介绍访问控制列表 (ACL)，包括 IP ACL 的类型。还介绍了基于上下文的访问控制 (CBAC)，包括：
 - 任务 1 和 2：配置 CBAC
 - 任务 3：使用端口到应用程序映射 (PAM)
 - 任务 4：定义检查规则
 - 任务 5：应用检查规则和 ACL 到路由器接口
 - 任务 6：测试和检验 CBAC
- **第 4 章“路由器 AAA 安全”**——本章描述了验证、授权和记账 (AAA) 安全网络访问，包括网络访问服务器 (NAS) AAA 验证过程和 Cisco 安全访问控制服务器的实现，本章还介绍了 AAA 服务器的概述和配置，最后介绍了 Cisco IOS 防火墙验证代理。
- **第 5 章“路由器入侵检测、监控和管理”**——本章介绍 IOS 防火墙入侵检测系统 (IDS)，说明了设置 IDS 并用日志记录和系统日志进行监控的过程。本章还讨论了简单网络管理协议 (SNMP)，介绍了管理路由器的方法，最后介绍了安全设备管理器 (SDM)。
- **第 6 章“路由器配置站点到站点 VPN”**——本章介绍了虚拟专用网 (VPN)，然后讨论了 IOS 加密系统。文中解释了 IPSec，包括使用预共享密钥的站点到站点 IPSec VPN 的概念和数字证书。最后讨论了使用数字证书配置站点到站点 IPSec VPN 的方法。
- **第 7 章“路由器远程访问 VPN”**——本章介绍远程访问 VPN，还介绍了 Cisco Easy VPN 和 Cisco VPN 3.5 客户端。最后讨论了 VPN 企业管理。

- **第 8 章“PIX Security Appliance”**——本章介绍防火墙，并概述了各种 PIX Security Appliance 的型号、特点及其性能。本章所讨论的 PIX Security Appliance 主题包括启动、路由选择和多播配置，以及使用动态主机配置协议（DHCP）。
- **第 9 章“PIX Security Appliance 转换和连接”**——本章讨论了传输协议、网络地址转换和配置域名系统（DNS）的支持。介绍完转换后讨论的是连接。另外，本章还解释了如何在 PIX Security Appliance 上使用端口地址转换（PAT）。最后讨论了 PIX Security Appliance 上的多个接口。
- **第 10 章“PIX Security Appliance 访问控制列表”**——本章讨论了 ACL 和 PIX Security Appliance，举例说明如何使用 ACL。其他介绍的内容包括过滤、对象组和嵌套的对象组。
- **第 11 章“PIX 安全应用 AAA”**——本章介绍了如何在 PIX Security Appliance 上使用 AAA，包含验证配置、授权配置和记账配置。最后讨论了 PPPoE 和 PIX Security Appliance。
- **第 12 章“PIX 高级协议和入侵检测”**——本章介绍了使用 PIX Security Appliance 对高级协议的处理。还介绍了对多媒体的支持。另外，文中说明了 PIX Security Appliance 的配置，以提供攻击防护和入侵检测。本章定义了规避方法并提供了多个配置示例。也介绍了 PIX Security Appliance 的系统日志配置。最后讨论了 SNMP 和 PIX Security Appliance。
- **第 13 章“PIX 故障转移与系统维护”**——本章首先讨论了解故障转移概念的内容，还讨论了串行电缆故障转移和基于 LAN 的故障转移。其他的主题包括通过远程访问进行系统维护和命令授权方法，最后介绍了密码恢复和 PIX Security Appliance 的升级。
- **第 14 章“PIX Security Appliance VPN”**——本章主要讨论 PIX Security Appliance 如何启用安全的虚拟专用网（VPN），还介绍了配置 VPN 的任务，包括：
 - 任务 1：有关 VPN 支持准备的配置
 - 任务 2：配置 IKE 参数
 - 任务 3：配置 IPSec 参数
 - 任务 4：测试和验证 VPN 配置

另外，本章还介绍了 Cisco VPN 客户端到 PIX Security Appliance VPN 和扩展 PIX Security Appliance VPN 的方法。

- **第 15 章“PIX Security Appliance 管理”**——本章介绍 PIX Security Appliance 管理工具，包括 Cisco PIX 设备管理器（PDM），讲述了如何准备 PDM、如何使用 PDM 配置 PIX Security Appliance，以及如何用它来创建站点到站点和远程访问 VPN。最后讨论了企业 PIX 管理。
- **附录 A“关键术语”**——该术语表包含本书中使用的所有关键术语。
- **附录 B“复习题的答案”**——本附录包含了每章末的习题答案。
- **附录 C“物理层安全”**——本附录讨论了从最基本到最复杂级别的第 1 层安全。指出了用户和网络所面对的一些威胁。本附录还讨论了在基础级别上管理网络安全的企业所能获得的好处。
- **附录 D“操作系统安全”**——本附录讨论了操作系统安全许多复杂的细节问题，附录的第一部分讨论了 Linux 操作系统的安全，第二部分讨论了 Windows 操作系统的安全。

命令语法约定

本书中使用的命令语法约定与 Cisco IOS 软件命令参考中所用的约定相同。命令参考中描述的约定如下：

- 竖线(|)用来分开可选的互斥参数。
- 方括号([])括出可选的参数。
- 花括号({ })表示必需的选项。
- 方括号套尖括号([{}])表示可选的命令中必要的参数。
- **黑体字**指出指令和关键字。
- *斜体字*表示要提供的参数值。

Cisco 系统网络图标说明

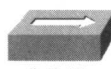
Cisco 公司使用了标准化的图标集来表示网络拓扑结构说明中的各种设备，下面的图标说明中显示了最常见的图标，全书中会经常出现这些图标。



路由器



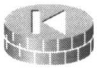
交换机



集线器



网络访问
服务器



PIX Security
Appliance



IOS
防火墙



防火墙
路由器



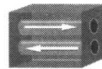
防火墙交换机
模块 (FWSM)



多层
交换机



通用
防火墙



VPN
集中器



CiscoWorks
工作站



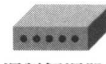
Cisco
安全管理器



Cisco
呼叫管理器



IBM
大型机



调制解调器



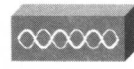
感应器



Cisco
CA



PC



接入点



膝上型电脑



文件服务器



Cisco
目录服务器



IP 电话



Web
服务器



网云



串行线路连接



以太网连接

目 录

第一部分

第 1 章 网络安全概述3
1.1 网络安全的基本原理、趋势和 目标.....3
1.1.1 网络安全的需要.....4
1.1.2 影响网络安全的趋势.....5
1.1.3 网络安全目标.....7
1.1.4 网络安全的关键要素.....8
1.1.5 安全意识.....9
1.2 安全威胁与攻击.....10
1.2.1 网络安全弱点.....11
1.2.2 主要网络威胁.....12
1.2.3 侦查.....13
1.2.4 窃听.....15
1.2.5 系统访问.....16
1.2.6 其他访问攻击.....19
1.2.7 拒绝服务.....20
1.2.8 分布式拒绝服务.....22
1.2.9 弱点: OSI 层次模型.....25
1.3 安全框架与策略.....27
1.3.1 安全车轮.....27
1.3.2 安全策略基础.....30
1.3.3 网络安全情况研究.....33
1.4 安全产品和解决方案.....37
1.4.1 身份.....38
1.4.2 防火墙.....40
1.4.3 虚拟专网.....41
1.4.4 入侵探测.....44
1.5 监控、管理和审计.....46
1.6 SAFE.....49
1.7 小结.....50
1.8 关键术语.....51

1.9 复习题.....52
第 2 章 基本的路由器和交换机安全55
2.1 路由器和交换机安全概要.....55
2.1.1 路由器拓扑.....56
2.1.2 路由器安装与安全.....58
2.1.3 访问控制.....59
2.1.4 使用密码控制路由器 访问.....63
2.1.5 设置优先级.....64
2.1.6 设置用户账号.....65
2.1.7 登录标语.....66
2.2 禁用不需要的服务.....67
2.2.1 路由选择、代理 ARP、 ICMP.....72
2.2.2 NTP、SNMP、路由器名字、 DNS.....74
2.3 边界路由器安全.....77
2.3.1 控制入站和出站流量.....77
2.3.2 网络地址转换.....79
2.3.3 路由协议验证与更新 过滤.....81
2.3.4 流量过滤.....83
2.3.5 过滤 ICMP 消息.....87
2.3.6 Cisco IOS 防火墙.....88
2.4 路由器管理.....89
2.4.1 日志.....90
2.4.2 网络设备间的时间同步.....92
2.4.3 软件和配置的维护.....94
2.4.4 使用 SSH 进行远程管理.....95
2.5 安全交换和局域网访问.....96
2.5.1 第二层攻击以及缓解.....98
2.5.2 端口安全.....99
2.5.3 虚拟局域网.....101
2.6 小结.....102

2.7 关键术语	102	3.3.10 配置一个空接口	147
2.8 复习题	103	3.4 小结	148
第3章 路由器 ACL 和 CBAC	107	3.5 关键术语	148
3.1 访问控制列表	107	3.6 复习题	149
3.1.1 在 ACL 中使用掩码	109	第4章 路由器 AAA 安全	153
3.1.2 ACL 总结	110	4.1 AAA 安全网络访问	153
3.1.3 处理 ACL	111	4.1.1 AAA 安全网络构架	154
3.1.4 应用 ACL	112	4.1.2 验证方法	155
3.1.5 编辑 ACL	113	4.2 网络访问服务器 (NAS) AAA 验证过程	158
3.1.6 排除 ACL 故障	114	4.2.1 远程管理	158
3.2 IP ACL 的类型	115	4.2.2 远程网络访问	158
3.2.1 标准 ACL	116	4.2.3 AAA 安全服务器的 选择	159
3.2.2 扩展 ACL	117	4.2.4 NAS 配置	160
3.2.3 命名 IP ACL	118	4.3 Cisco Secure ACS	160
3.2.4 注释 IP ACL 条目	118	4.3.1 管理 Cisco Secure ACS 3.0 for Windows	161
3.2.5 锁和密钥 (动态) ACL	119	4.3.2 Cisco Secure ACS for Windows 故障排除技术	163
3.2.6 反身 ACL	120	4.3.3 Cisco Secure ACS for UNIX 概述	163
3.2.7 使用时间范围的时基 ACL	122	4.3.4 Cisco Secure ACS 2.3 for UNIX 的特性集	164
3.2.8 验证代理	122	4.3.5 Cisco Secure ACS 解决方案 引擎	165
3.2.9 Turbo ACL	123	4.4 AAA 服务器概述及配置	167
3.3 基于上下文的访问控制	123	4.4.1 TACACS	168
3.3.1 CBAC 是如何工作的	125	4.4.2 XTACACS	168
3.3.2 支持 CBAC 的协议	127	4.4.3 TACACS+	168
3.3.3 配置 CBAC: 第一步 ——设置审计跟踪和 警报	128	4.4.4 介绍 RADIUS	168
3.3.4 配置 CBAC: 第二步 ——设定全局超时和 阈值	129	4.4.5 RADIUS 和 TACACS+ 的 比较	170
3.3.5 配置 CBAC: 第三步 ——定义应用程序端口 映射 (PAM)	132	4.4.6 Kerberos 概述	171
3.3.6 配置 CBAC: 第四步 ——定义检查规则	134	4.5 Cisco IOS 防火墙验证代理	171
3.3.7 配置 CBAC: 第五步 ——在路由器接口上应用 检查规则和 ACL	142	4.5.1 支持的服务器	172
3.3.8 配置 CBAC: 第六步 ——测试和检验	145	4.5.2 验证代理操作	172
3.3.9 移除 CBAC 配置	147	4.5.3 验证代理配置任务	173
		4.5.4 HTTPS 验证代理	175
		4.6 小结	177
		4.7 关键术语	177

- 4.8 复习题.....178
- 第 5 章 路由器入侵探测、监控和管理**.....181
- 5.1 IOS 防火墙 IDS.....181
- 5.1.1 实现签名.....183
- 5.1.2 响应选项.....183
- 5.2 安装 Cisco IOS 防火墙 IDS.....183
- 5.2.1 步骤 1: 初始化路由器上的 IOS Firewall IDS——设置通告的类型.....184
- 5.2.2 步骤 2: 初始化路由器上的 IOS Firewall IDS——设置通告队列的尺寸.....184
- 5.2.3 步骤 3: 配置、禁用或删除签名.....185
- 5.2.4 步骤 4: 创建和应用审计规则.....186
- 5.2.5 步骤 5: 检验配置.....187
- 5.2.6 步骤 6: 添加 IOS 防火墙 IDS 到 IDS Director 的映射图.....189
- 5.3 使用日志和 Syslog 监控.....189
- 5.3.1 日志的价值.....189
- 5.3.2 配置日志.....190
- 5.3.3 配置日志消息的同步.....191
- 5.3.4 限制错误消息的严重程度.....192
- 5.3.5 系统日志 (Syslog).....193
- 5.4 SNMP.....196
- 5.4.1 SNMP 的安全.....198
- 5.4.2 SNMP 版本 3 (SNMPv3).....199
- 5.4.3 如何配置 SNMP.....201
- 5.4.4 SNMP 管理应用程序.....201
- 5.5 管理路由器.....202
- 5.5.1 管理员的访问机制.....202
- 5.5.2 升级路由器.....203
- 5.5.3 测试和安全确认.....204
- 5.5.4 企业监控.....204
- 5.6 安全设备管理器 (SDM).....205
- 5.6.1 访问 SDM.....207
- 5.6.2 下载安装 SDM.....209
- 5.6.3 修改现有的配置文件.....209
- 5.6.4 使用默认的配置文件.....210
- 5.7 小结.....210
- 5.8 关键术语.....211
- 5.9 复习题.....211
- 第 6 章 路由器配置 Site-to-Site VPN**.....215
- 6.1 VPN.....215
- 6.1.1 Site-to-Site VPN.....215
- 6.1.2 VPN 技术选项.....216
- 6.1.3 隧道协议.....217
- 6.1.4 隧道接口.....218
- 6.2 IOS 密码系统.....219
- 6.2.1 对称加密.....220
- 6.2.2 非对称加密.....221
- 6.2.3 Diffie-Hellman 算法.....222
- 6.2.4 数据完整性.....223
- 6.2.5 HMAC.....224
- 6.2.6 来源验证.....225
- 6.3 IPsec.....226
- 6.3.1 验证头.....228
- 6.3.2 ESP 协议.....229
- 6.3.3 IPsec 传输模式.....230
- 6.3.4 安全关联.....231
- 6.3.5 IPsec 的 5 个步骤.....233
- 6.3.6 IKE.....233
- 6.3.7 IPsec 和 IKE 的逻辑流程.....235
- 6.4 使用预共享密钥的 Site-to-Site IPsec VPN.....236
- 6.4.1 任务 1: 为 IKE 和 IPsec 做准备.....236
- 6.4.2 任务 2: 配置 IKE.....237
- 6.4.3 任务 3: 配置 IPsec.....237
- 6.4.4 任务 4: 测试和校验 IKE.....240
- 6.5 数字证书.....240
- 6.5.1 SCEP.....241
- 6.5.2 CA 服务器.....242
- 6.5.3 用一个 CA 注册设备.....243
- 6.6 使用数字证书配置 Site-to-Site IPsec VPN.....244
- 6.6.1 任务 1: 为 IKE 和 IPsec

9.4 连接.....	330	合作伙伴 Web 访问	
9.4.1 穿过 PIX 安全设备的两种方法.....	330	DMZ	353
9.4.2 静态通道.....	331	10.2.4 ACL 的常规用法: 允许 DMZ 访问内部邮件	354
9.5 端口地址转换.....	331	10.2.5 VPN 解决方案: 双 DMZ 和 VPN 集中器	355
9.5.1 PIX 安全设备的 PAT.....	332	10.2.6 用 ACL 禁用 Ping.....	356
9.5.2 使用外部地址转换的 PAT.....	333	10.3 过滤.....	357
9.5.3 映射子网到 PAT 地址.....	334	10.3.1 过滤恶意小程序	357
9.5.4 使用多 PAT 地址提供后备 PAT 地址.....	334	10.3.2 URL 过滤	358
9.5.5 使用 PAT 增加全局地址以支持更多主机.....	335	10.4 对象组.....	359
9.5.6 端口重定向.....	335	10.4.1 在 ACL 中使用对象组	360
9.6 PIX 安全设备的多接口	337	10.4.2 配置对象组	362
9.6.1 通过 PIX 安全设备进行访问.....	337	10.4.3 在对象组上应用 ACL	362
9.6.2 在 PIX 安全设备上配置三个接口.....	338	10.5 嵌套的对象组	363
9.6.3 配置 PIX 安全设备的四个接口.....	339	10.5.1 配置嵌套的对象组	364
9.7 小结.....	340	10.5.2 嵌套对象组例子	364
9.8 关键术语.....	341	10.5.3 ACL 中多个对象组的例子	365
9.9 复习题.....	341	10.5.4 验证和管理对象组	366
第 10 章 PIX 安全设备访问控制列表	345	10.6 小结.....	367
10.1 ACL 和 PIX 安全设备	345	10.7 关键术语.....	367
10.1.1 ACL 使用原则.....	345	10.8 复习题.....	367
10.1.2 实现 ACL.....	346	第 11 章 PIX 安全应用 AAA	371
10.1.3 Turbo ACL.....	346	11.1 AAA.....	371
10.1.4 ACL 与管道技术的比较.....	347	11.1.1 用户在验证和授权中看到了什么	372
10.1.5 ACL 案例研究: 管道和 ACL 行为的差异.....	348	11.1.2 切入型代理操作	373
10.1.6 ACL 的验证和故障排除.....	351	11.1.3 TACACS+和 RADIUS.....	374
10.2 使用 ACL.....	351	11.1.4 CSACS 和 PIX	375
10.2.1 使用 ACL 拒绝内网用户的 Web 访问.....	352	11.2 PIX 上的验证配置.....	376
10.2.2 使用 ACL 来允许 Web 访问 DMZ.....	352	11.2.1 aaa-server 命令.....	376
10.2.3 ACL 的通常用法: 允许		11.2.2 aaa authentication 命令	377
		11.2.3 AAA 验证实例.....	378
		11.2.4 验证非 Telnet、非 FTP 或非 HTTP 流量	378
		11.2.5 虚拟 Telnet	379
		11.2.6 虚拟 HTTP	380
		11.2.7 控制台访问验证	381
		11.2.8 更改验证超时和验证提示	382

11.3	PIX 安全应用上的授权配置	383	12.1.4	SQL*Net Fixup 配置	406
11.3.1	aaa authorization 命令	383	12.1.5	SIP Fixup 配置	407
11.3.2	使用可下载的 ACL 提供授权	384	12.1.6	小客户 Fixup 配置	407
11.4	在 PIX 安全应用上配置记账	385	12.2	多媒体支持和 PIX 安全应用	408
11.5	使用 AAA 服务定义流量	386	12.2.1	实时流协议	409
11.6	监控 AAA 配置	386	12.2.2	H.323	412
11.7	PPPoE 和 PIX 安全应用	387	12.2.3	IP 电话和 PIX 安全应用 DHCP 服务器	413
11.7.1	PIX 如何与 PPPoE 交互工作	387	12.3	攻击防护	414
11.7.2	配置 PIX 支持 PPPoE	388	12.3.1	邮件防护	414
11.7.3	监控和故障排除 PPPoE 客户端	389	12.3.2	DNS 防护	415
11.8	附录 11-A: 如何向 CSACS-NT 添加用户	390	12.3.3	分片防护和虚拟重组	416
11.8.1	附加用户信息	391	12.3.4	AAA 泛洪防护	416
11.8.2	用户设置	391	12.3.5	SYN 泛洪攻击	417
11.8.3	账号禁用	392	12.3.6	TCP 拦截	418
11.9	附录 11-B: CSACS 和授权	393	12.4	入侵检测和 PIX 安全应用	418
11.9.1	如何在 CSACS 上建立一个允许指定服务的授权规则	393	12.4.1	信息和攻击入侵检测特征	419
11.9.2	如何创建仅对 CSACS 上指定主机提供服务的授权规则	393	12.4.2	PIX 安全应用中的入侵检测	420
11.9.3	如何在 CSACS 上为非 telnet、非 FTP 和非 HTTP 的流量授权	394	12.5	规避	421
11.10	附录 11-C: CSACS 和 ACL	395	12.6	PIX 安全应用系统日志记录	422
11.11	附录 11-D: 如何在 CSACS 中查看记账信息	397	12.7	SNMP	424
11.12	小结	397	12.7.1	SNMP 实例	425
11.13	关键术语	398	12.7.2	MIB 支持	425
11.14	复习题	398	12.7.3	示例: SNMP 通过 PIX 安全应用	426
第 12 章	PIX 高级协议和入侵检测	401	12.8	小结	428
12.1	高级协议处理	401	12.9	关键术语	428
12.1.1	fixup 命令	402	12.10	复习题	429
12.1.2	FTP Fixup 配置	403	第 13 章	PIX 故障转移与系统维护	433
12.1.3	远程 Shell (rsh) Fixup 配置	405	13.1	了解 PIX Security Appliance 故障转移	433
			13.1.1	故障转移的 IP 地址	435
			13.1.2	配置文件复制	435
			13.1.3	故障转移和有状态故障转移	436
			13.1.4	故障转移接口测试	437
			13.2	串行电缆故障转移配置	438
			13.2.1	步骤 1: 连接防火墙	438

13.2.2	步骤 2: 连接故障转移 电缆	439	14.2	配置 VPN 任务	461
13.2.3	步骤 3: 配置主 PIX	440	14.2.1	任务 1: 准备配置 VPN 支持	462
13.2.4	步骤 4: 从防火墙接电	440	14.2.2	任务 2: 配置 IKE 参数	465
13.2.5	验证故障转移配置 文件	442	14.2.3	任务 3: 配置 IPSec 参数	467
13.3	基于 LAN 的故障转移配置	443	14.2.4	任务 4: 测试和校验 VPN 配置	470
13.3.1	步骤 1~4: 配置主 PIX	444	14.3	Cisco VPN 客户端	473
13.3.2	步骤 5~10: 配置从 PIX	445	14.3.1	Cisco VPN 客户端拓扑 结构	474
13.4	通过远程访问维护系统	447	14.3.2	PIX Security Appliance 分配 IP 地址到 VPN 客户端	475
13.4.1	为 PIX Security Appliance 控制台配置 Telnet 访问	447	14.3.3	配置 PIX Security Appliance 的 PIX 到 VPN 客户端隧道	476
13.4.2	SSH 连接到 PIX Security Appliance	448	14.3.4	为 PIX 到 PIX 客户端 隧道配置 VPN 客户端	478
13.4.3	用 SSH 客户端连接到 PIX Security Appliance	448	14.4	使用 CA 扩展 PIX VPN	479
13.5	命令授权	449	14.5	小结	481
13.5.1	方法 1: 启用级别命令 授权	450	14.6	关键术语	481
13.5.2	方法 2: 本地命令授权	450	14.7	复习题	482
13.5.3	方法 3: ACS 命令 授权	451			
13.6	PIX Security Appliance 密码 恢复	452	第 15 章	PIX 安全管理	485
13.7	升级 PIX Security Appliance 映像及激活密钥	452	15.1	PIX 管理工具	485
13.8	小结	453	15.1.1	PIX 设备管理器	486
13.9	关键术语	453	15.1.2	Cisco 安全策略管理器	486
13.10	复习题	454	15.1.3	PIX 管理中心	487
			15.2	Cisco PIX 设备管理器	488
第 14 章	PIX Security Appliance VPN	457	15.2.1	PDM 运行要求	489
14.1	PIX Security Appliance 实现 安全的 VPN	457	15.2.2	PDM 浏览器要求	489
14.1.1	PIX VPN 性能	457	15.2.3	PDM 的准备	491
14.1.2	PIX VPN 拓扑结构	458	15.2.4	运用 PDM 配置 PIX	493
14.1.3	IPSec 实现 PIX VPN 特性	459	15.2.5	使用 PDM 创建站点到 站点 VPN	501
14.1.4	IPSec 概述	459	15.2.6	使用 PDM 创建远程 访问 VPN	506
14.1.5	PIX Security Appliance 支持 IPSec 标准	459	15.3	企业 PIX 管理	509
			15.3.1	PIX MC	509
			15.3.2	PIX MC 的主要概念	510

15.3.3 AUS	511
15.4 小结	511
15.5 复习题	512

第三部分

附录 A 关键术语	517
-----------	-----

附录 B 复习题答案	525
------------	-----

附录 C 物理层安全	531
------------	-----

C.1 什么是物理安全?	531
C.2 第 1 层安全的开销是什么?	533
C.3 第 1 层安全保护了什么?	534
C.4 物理安全同样能够防御其他威胁	534
C.5 物理层安全的基础	534
C.6 ANSI/TIA/EIA	535
C.7 安全培训	537
C.7.1 建立安全意识	537
C.7.2 需要进行验证	538
C.7.3 登录访问及操作	538
C.7.4 提出适当有礼的质疑	538
C.7.5 知道向哪些人寻求援助	539
C.8 高级通行证及 Biometric 验证	539
C.9 威慑因素	539
C.10 工作区安全	540
C.10.1 闲置插座	540
C.10.2 抗干扰插座	540
C.10.3 抗干扰路径	541
C.10.4 电信间	541
C.11 入侵者怎样截取信息并解码	542
C.11.1 入侵者是怎样截取资料的	543
C.11.2 入侵者怎样对资料解码	543
C.12 光纤入侵	543
C.12.1 直接物理入侵	544
C.12.2 管道	545

C.13 无线侦听	545
C.13.1 竞争驾驶	545
C.13.2 竞争拨号和竞争行走	546
C.14 安全自动控制	546
C.15 物理安全中的人员因素	547
C.16 小结	549

附录 D 操作系统安全	553
-------------	-----

D.1 Linux 操作系统级安全	553
D.1.1 保护正在运行的进程	554
D.1.2 文件系统和目录安全	556
D.1.3 验证安全	560
D.2 Linux 基础设施级安全	562
D.2.1 保护 Samba	562
D.2.2 保护 NFS	564
D.2.3 保护 xinetd 守护进程	566
D.3 保护 Linux 网络服务	568
D.3.1 保护 Linux FTP 服务器	568
D.3.2 保护 Linux Web 服务器	569
D.3.3 保护 Linux 邮件服务器	571
D.4 Linux 网络安全和过滤方法	573
D.4.1 TCP 包装程序	573
D.4.2 网络地址转换	574
D.4.3 防火墙和代理服务	574
D.5 Windows 2000 验证安全	576
D.5.1 识别安全架构	576
D.5.2 在 Windows 2000 中验证用户	577
D.6 Windows 2000 操作系统级安全	578
D.6.1 保护文件和打印资源	578
D.6.2 加密文件系统	580
D.6.3 审核对资源的访问	583
D.7 Windows 2000 基础结构级安全	584
D.7.1 保护活动目录	584
D.7.2 用组策略辅助安全管理	585
D.7.3 安全模版、安全配置和分析工具的使用	586
D.7.4 安全地对 DNS 记录进行更新	586