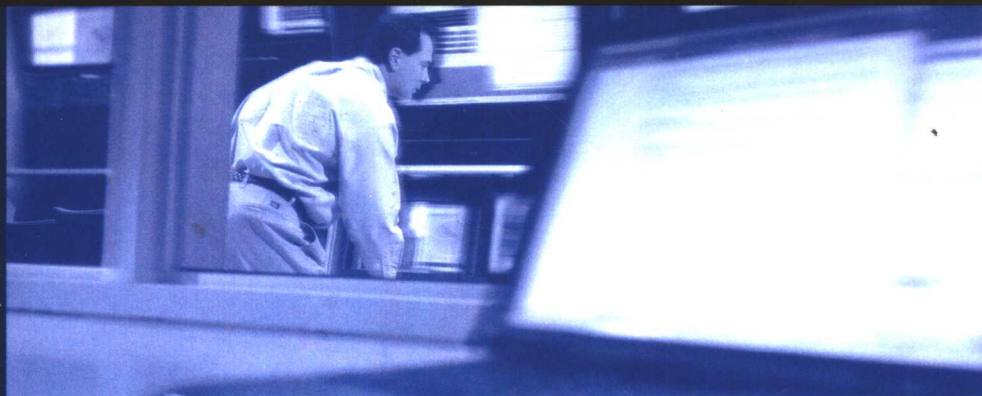




Cisco 职业认证培训系列  
CISCO CAREER CERTIFICATIONS

ciscopress.com



# CCSP 自学指南： Cisco 安全 PIX 防火墙 (CSPFA) (第二版)

**CCSP Self-Study:**  
**Cisco Secure PIX Firewall Advanced (CSPFA)**  
Second Edition

Cisco authorized self-study book for  
CCSP® 642-521 foundation learning

[美] Behzad Behtash 著  
孙国冉, CCIE #12210 译  
王艳奇, CCIE #12283

 人民邮电出版社  
POSTS & TELECOM PRESS

Cisco 职业认证培训系列

**CCSP 自学指南：  
Cisco 安全 PIX 防火墙 ( CSPFA )  
( 第二版 )**

[美] Behzad Behtash 著

孙国冉, CCIE #12210

王艳奇, CCIE #12283

译

人民邮电出版社

## 图书在版编目 (CIP) 数据

CCSP 自学指南. Cisco 安全 PIX 防火墙 (CSPFA): 第 2 版 / (美) 贝塔什 (Behtash, B.) 著; 孙国冉, 王艳奇译. —北京: 人民邮电出版社, 2005.4

(Cisco 职业认证培训系列)

ISBN 7-115-13167-8

I. C... II. ①贝...②孙...③王... III. 计算机网络—安全技术—工程技术人员—资格考核—自学参考资料 IV. TP393.08

中国版本图书馆 CIP 数据核字 (2005) 第 017832 号

## 版 权 声 明

Behzad Behtash: CCSP Self-Study: Cisco Secure PIX Firewall Advanced (CSPFA), Second Edition

ISBN: 1587051494

Copyright © 2004 Cisco Systems, Inc.

Authorized translation from the English language edition published by Cisco Press.

All rights reserved.

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

版权所有, 侵权必究。

Cisco 职业认证培训系列

**CCSP 自学指南:**

**Cisco 安全 PIX 防火墙 (CSPFA) (第二版)**

- 
- ◆ 著 [美] Behzad Behtash
  - 译 孙国冉, CCIE#12210 王艳奇, CCIE#12283
  - 责任编辑 李 际
  
  - ◆ 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 010-67132692
  - 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: 41
  - 字数: 1 000 千字 2005 年 4 月第 1 版
  - 印数: 1 - 3 500 册 2005 年 4 月北京第 1 次印刷
  
  - 著作权合同登记 图字: 01-2004-0564 号
  - ISBN 7-115-13167-8/TP · 4497

定价: 88.00 元

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

# 内容提要

本书分 7 个部分对 Cisco 公司网络安全的拳头产品 PIX 防火墙进行了系统讲述。第 1 部分讲述了网络安全的基础知识、实施安全策略的基本方法、Cisco 公司网络安全方面的产品概况，并对 PIX 防火墙的各种型号和基本特点进行了系统阐述。第 2 部分通过举例的方式讲述了在不同规模和不同复杂程度的环境下部署 PIX 防火墙的具体方法和配置。第 3 部分对 PIX 防火墙的配置进行了详细讲解，包括基本配置、PDM 管理配置、地址和端口转换配置、访问控制列表和内容过滤的配置、为简化配置如何进行对象分组、基本的路由配置。第 4 部分讲述的是高级配置，包括如何配置 PIX 防火墙以支持特殊的上层协议和多媒体协议，如何配置攻击保护、入侵检测和动态阻挡，如何配置认证、授权和记帐，如何配置故障倒换以提高安全系统的可靠性。第 5 部分对 VPN 中的关键技术，如 IPSec 进行了概要的描述，然后讲述了使用 PIX 防火墙构建不同类型的 VPN 时的具体配置方法。第 6 部分讲述的是 PIX 防火墙的维护和管理，特别是在企业网中如何使用防火墙管理中心（MC）和 AUS 以图形化的方式管理和维护防火墙。第 7 部分则以专题的方式分别讲述了专用 Cisco 6500 交换机和 Cisco 7600 路由器上的防火墙服务模块（FWSM）、使用 SOHO 网络的 PIX 防火墙。

本书讲述的重点是如何在实际环境中应用 PIX 防火墙，所以关注的不是某项技术的细节，而是产品应用时的各种配置。本书适合于准备进行 CCSP 认证考试的考生，也适合于想对 PIX 防火墙的应用有深入了解的各类工程技术人员。

## 关于作者

Behzad Behtash, CCNP, CCDP, MCSE, 是一名 IT 顾问, 在组网和安全方面有 9 年多的经验, 拥有威斯康星——麦迪逊大学化学工程专业的学士学位, 居住在加利福尼亚的奥克兰。

## 关于技术审稿人

Nairi Adamian, CCIE Security No.10294, CISSP, 工作在位于澳大利亚的 Cisco 系统公司技术支持中心 (TAC), 是一名负责安全和虚拟专用网 (VPN) 的工程师。她为 Cisco 多种安全产品提供技术支持, 如 PIX 防火墙、VPN 集中器、入侵监测系统以及其他相关的技术, 拥有悉尼理工大学计算机科学专业的学士学位, 目前正在攻读 Macquarie 研究生管理学院的 MBA。

Andy Fox, CCNA, CCDA, CSS-1, 是 Global Knowledge 公司 Cisco 认证的一名讲师。Andy 讲解 Cisco 的认证课程已有 6 年多, 是“管理 Cisco 网络安全”课程方面的主管, 是本书 (《Cisco 安全 PIX 防火墙》) 第一版的作者。Andy 在美国空军时是一名计算机操作员, 从那时起开始从事计算机科学相关工作。

Izak Karmona 是 HP 公司的网络安全顾问, 工作在以色列, 是一名 CCSP, 目前正在努力获取 CCIE 安全证书。Izak 在网络行业工作超过了 15 年。他的工作包括为 HP 公司的客户提供网络设计、安全和实施服务。Izak 拥有以色列海尔法理工学院 (Technion Institute of Technology) 计算机科学专业的学士学位。

## 献 辞

把这本书献给我的女儿 Tiana；我的儿子 Daryan；还有我亲爱的妻子 Anita，她总是我的第一个读者。

另外，我也把这本书献给我的父母，感谢他们对我无私的关爱和支持。同时献给 Ramin、Kaveh 和 Saman，亲爱的哥哥和朋友。

我还要感谢另外两个值得尊敬的人，他们对我的成长帮助甚多：威斯康星——麦迪逊大学的 Glenn Sather 和 Thatcher Root 教授。谢谢他们对我的信任。

## 致 谢

我要感谢 Michelle Grandin, Christopher Cleveland, Tammi Barnett, Kris Simmons, San Dee Phillips, Keith Clien, 以及其他 Cisco Press 的同仁，感谢他们给我写这本书的机会，感谢他们在本书整个写作过程中所给与的支持和指导。特别感谢 Betsey Henkels，一位非常好的合作者。她是一名资深的技术人员，作为本书的开发编辑，她所付出的努力使本书的质量大为提高。

我还要感谢审稿人 Nairi Adamian、Andy Fox 和 Izak Karmona，感谢他们的贡献和建设性的建议。他们的奉献，让我十分感激。

我还要感谢我的大学同学和朋友 Grant Moerschel，是他把我介绍给 Cisco Press，感谢他的友谊和洞察力。

最后，我要感谢在 Cisco 系统公司工作的 Matt Krieg，感谢他提供了有关 PIX 防火墙开发方面的及时信息。

# 序 言

本书是 Cisco Systems 公司认可的学习教材,可以帮助你理解 Cisco 安全防火墙高级 (CSPFA) 考试中所涉及的概念。本书是和 Cisco Internet 学习解决方案小组合作开发的,这个团队在 Cisco Systems 公司负责开发 CSPFA 考试。作为考前辅导教材,本书详细、全面地阐述了一个网络和安全工程师配置、验证和管理 PIX 防火墙系列产品的方方面面。无论你要通过 CCSP 的认证,还是要成为 PIX 专业人士,或者只是想更好地理解产品、服务和策略,以便应用 PIX 防火墙系列中的产品,这本书都能让你从中获益。

Cisco Systems 公司和 Cisco Press 提供本书的印刷版本,旨在让客户和广大用户能够以另一种方式进行学习。虽然出版物不同于教师指导环境和远程学习环境,但毕竟学习方式因人而异。通过 Cisco Press 出版本书,旨在将知识传播给更多的网络专业人员。

Cisco Press 将针对已有的和将推出的考试,出版其他认证自学系列丛书,帮助 Cisco Internet 学习解决方案小组实现其首要目标:对 Cisco 网络技术领域的专业人员进行培训,使其能够组建和维护可靠的、易于扩展的网络。Cisco 职业认证和相应的课程通过严谨、循序渐进的培训来实现上述目标。

为通过 Cisco 职业认证并完成 Cisco 认证的专业人员的日常工作,建议结合采用教师指导的培训、实际动手、远程学习、自学等学习方式。Cisco Systems 授权的培训合作伙伴遍布世界各地,他们提供高质量的指导以及宝贵的实验室和模拟环境。有关当地的 Cisco 培训伙伴计划的详细,请访问 <http://www.cisco.com/go/authorizedtraining>。

Cisco Press 和 Cisco Systems 合作出版的书籍符合相应课程和认证的质量要求。希望本书以及后续的认知自学图书对增强读者的网络知识大有裨益。

Thomas M. Kelly

Cisco Systems 公司

Cisco Internet 学习解决方案分部副总裁

2004 年 1 月

# 前 言

过去几年里，网络安全引起了越来越多的关注。当前的环境和对安全的普遍关注增强了人们对网络安全技术和产品的重视。这一点直接反映在对网络安全产品和服务投资的增加上，也反映在对网络安全专业人员和专家的需求不断增加上。

为适应市场对安全的需要，Cisco Systems 公司提供了多种网络安全产品、创新的技术和服务。Cisco PIX 防火墙安全系列产品是占据主导市场份额的防火墙产品，众多的网络工程师和专业的安全人士用它们为各种规模和复杂程度的网络提供保护。

## 读者对象

本书的读者是需要了解有关 PIX 防火墙安装、配置和维护详细信息的网络工程师、安全专业人员和支持工程师。准备参加 CCSP 考试的人员也可以用它作为考前的辅导教材。要充分理解本书的信息，读者应该具有扎实的网络基础知识，熟悉网络安全的基本概念。

## 本书的初衷

Cisco Press 于 2001 年发行了《Cisco 安全 PIX 防火墙》的第一版，书中讲述了 PIX 防火墙的操作和高级特性，满足了当时市场的需求。从出版第一版以后，PIX 防火墙已经进行了重大的改进和提高，引入了几种新的型号，包括针对 Cisco 6500 系列交换机和 Cisco 7600 系列 Internet 路由器的模块。Cisco 系统公司还引入了使用图形化用户界面的 PIX 设备管理器（PDM），改善了对企业网中 PIX 防火墙的维护和管理。



本书包含了 CSPFA 第一版出版以后的更新信息、新引入的 PIX 防火墙型号和技术。其中包括 PIX 防火墙软件版本 6.3 中引入的开放式最短路径优先协议 (OSPF)、802.1Q VLAN 和逻辑接口、网络地址转换 (NAT) 遍历。另外, 更多的重点放在了 PDM 上, 它将是管理和配置 PIX 防火墙最主要的工具。

## 如何使用本书

本书共包括 22 章, 这些章节是按照逻辑顺序进行排列的, 不过你可以按照自己的需要方便地阅读任何章节。第 4 章中举了几个例子, 通过它们你可以了解网络的典型布局并完成 PIX 防火墙的配置。你可以参照这章的内容确定实施中基本的网络布局, 在此基础上学习后续的章节。当然, 你也可以在读过了其他章节以后再回来阅读第 4 章, 你将发现对这一章的内容已经非常熟悉。

各章的内容如下。

第 1 章, “Cisco 网络安全方面的产品”——这一章对网络安全进行了概述, 并简要地描述了 Cisco 语音、视频与集成数据架构 (AVVID) 和企业网安全架构 (SAFE) 的框架。

第 2 章, “Cisco PIX 防火墙技术与特点”——这一章对 PIX 防火墙技术和能力进行了简要描述, 其中介绍了适应性安全算法 (ASA)。

第 3 章, “Cisco PIX 防火墙系列产品介绍”——这一章讲述了 PIX 防火墙安全产品系列, 介绍了各种型号产品的特点和功能。

第 4 章, “在网络中实施 Cisco PIX 防火墙”——这一章举例说明了在不同规模和复杂程度的网络中, 如何实施 PIX 防火墙。

第 5 章, “Cisco PIX 防火墙入门”——这一章讲述了 PDM 的操作, 以及使用 PDM 配置 PIX 防火墙的步骤。

第 6 章, “Cisco PIX 设备管理器”——这一章介绍 PDM 操作以及使用 PDM 配置 PIX 防火墙的过程。

第 7 章, “转换和连接”——这一章详细说明了 PIX 防火墙如何处理入站和出站数据, 还讲述了网络地址转换 (NAT) 和端口地址转换 (PAT) 技术。

第 8 章, “访问控制列表和内容过滤”——这一章讲述了如何使用访问控制列表 (ACL) 来控制穿过 PIX 防火墙的数据流。

第 9 章, “对象分组”——这一章讲述了 PIX 防火墙的对象分组功能, 通过这项功能来简化创建和应用 ACL 的步骤。

第 10 章, “路由选择”——这一章讲述了 PIX 防火墙支持的路由选择功能。

第 11 章, “高级协议处理”——这一章讲述了 PIX 防火墙的协议修正功能以及高级协议处理能力。

第 12 章, “攻击保护、入侵检测和动态阻挡”——这一章讲述了 PIX 防火墙的在线入侵检测和动态阻挡功能, 以及相关的配置步骤。

第 13 章, “认证、授权和记帐”——这一章简要介绍了 PIX 防火墙认证、授权和记帐 (AAA) 的步骤, 还讨论了可下载的 ACL。

第 14 章, “故障倒换”——这一章详细介绍 PIX 防火墙的高可用性和相关的配置步骤。

第 15 章, “虚拟专用网”——这一章简要讲述了 VPN 的基础知识, 以及如何在 PIX 防

火墙中实施 IP 安全 (IPSec) 和 Internet 密钥交换 (IKE)。

第 16 章,“站到站 VPN”——这一章详细讲述了使用 PIX 防火墙构建站到站 VPN 连接的配置步骤。

第 17 章,“客户远程访问 VPN”——这一章详细讲述了使用 PIX 防火墙构建客户远程访问 VPN 连接的步骤。

第 18 章,“系统维护”——这一章详细讲述了 PIX 防火墙的系统维护协议和配置任务,包括映像更新和密码恢复步骤。

第 19 章,“企业网中的 PIX 防火墙管理”——这一章讲述了 Cisco 防火墙管理中心(防火墙 MC)的操作和功能。

第 20 章,“企业网中的 PIX 防火墙维护”——这一章讲述了如何使用防火墙自动升级服务器来维护企业网中 PIX 防火墙的运行。

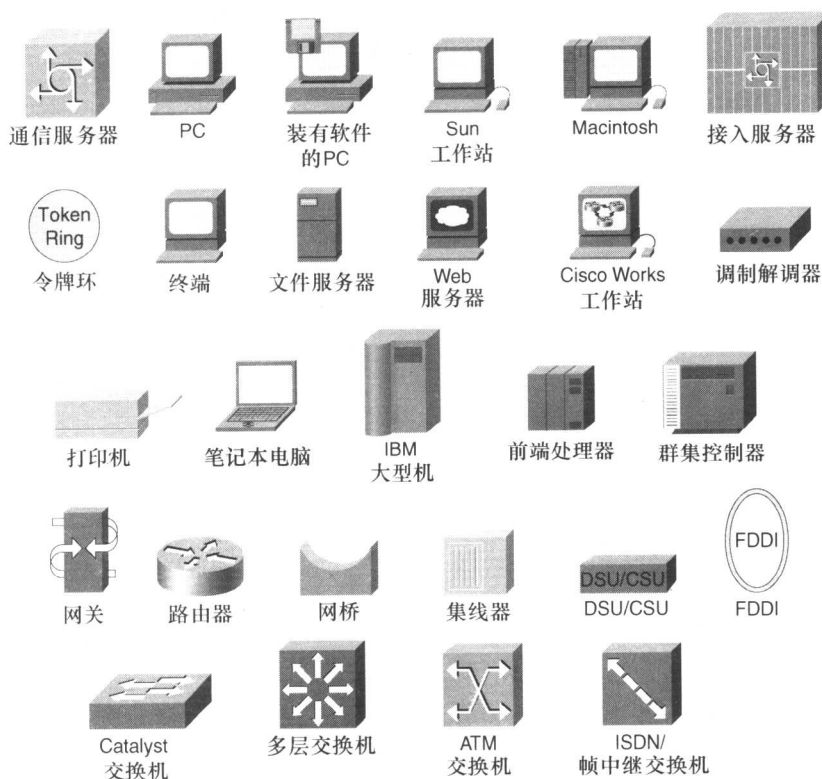
第 21 章,“防火墙服务模块”——这一章详细讲述了用于 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列 Internet 路由器上的 PIX 防火墙服务模块(FWSM)的功能。

第 22 章,“SOHO 网络中的 PIX 防火墙”——这一章重点讲述了 PIX 防火墙针对小办公室/家庭办公室(SOHO)网络的功能和技术。

附录 A,“复习题答案”——这个附录是各章复习题的答案。

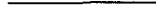
附录 B,“安全资源”——这个附录列举了很多有用的安全资源,包括书籍和 Internet 上的资源。

## 本书使用的图标





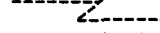
网络云图



实线：以太网



折线：串行电路



虚线：交换式串行连接

## 命令语法规范

本书使用的命令语法规范和 IOS 命令参考中使用的规范是一样的。命令参考中对规范  
的描述如下。

- **粗体**表示要逐个字符键入的命令和关键字。在实际配置举例和输出中（不是在通用命令语法中），**粗体**表示由用户手工输入（比如 **show** 命令）的内容。
- *斜体字*表示的是参数，在实际使用时需要用实际值来替代。
- 垂直线 (|) 把多个选项分隔开，只能选择其中的一个。
- 方括号 [ ] 表示可选元素。
- 大括号 { } 表示必选项。
- 位于方括号中的 ( [{}]) 表示可选元素中的必选项。

# 目 录

## 第一部分 概 述

<b>第 1 章 Cisco 网络安全方面的产品</b> .....	3
1.1 为什么网络安全是必需的 .....	3
1.2 安全威胁的类型 .....	4
1.3 网络攻击 .....	4
1.3.1 侦查攻击 .....	5
1.3.2 访问攻击 .....	5
1.3.3 DoS 攻击 .....	5
1.4 实施网络安全 .....	6
1.4.1 保护 (Securing) 系统 .....	7
1.4.2 监控网络 .....	7
1.4.3 测试安全性 .....	7
1.4.4 改进安全性 .....	7
1.5 Cisco AVVID 与 SAFE .....	8
1.5.1 Cisco AVVID 框架 .....	8
1.5.2 SAFE 计划概述 .....	9
1.5.3 SAFE 的优点 .....	10
1.6 小结 .....	10
1.7 复习题 .....	11
<b>第 2 章 Cisco PIX 防火墙技术与特点</b> .....	13
2.1 防火墙的种类 .....	13
2.1.1 包过滤器 .....	13
2.1.2 代理服务器 .....	14
2.1.3 基于状态的包过滤 .....	15
2.2 PIX 防火墙概述 .....	15
2.2.1 Finesse 操作系统 .....	16
2.2.2 ASA .....	16
2.2.3 直通代理 .....	16
2.2.4 基于状态的包过滤 .....	17
2.2.5 故障倒换 (Failover) .....	17
2.3 小结 .....	18
2.4 复习题 .....	18

**第 3 章 Cisco PIX 防火墙系列**

产品介绍 .....	21
3.1 PIX 防火墙 500 系列产品 .....	21
3.1.1 PIX 防火墙 501 .....	23
3.1.2 PIX 506 E 防火墙 .....	24
3.1.3 PIX 515E 防火墙 .....	25
3.1.4 PIX 525 防火墙 .....	28
3.1.5 PIX 535 防火墙 .....	30
3.2 FWSM .....	33
3.3 PIX 防火墙许可证 .....	35
3.3.1 基本的许可证选项 .....	35
3.3.2 VPN 许可证选项 .....	36
3.4 小结 .....	37
3.5 复习题 .....	37

**第二部分 PIX 防火墙入门****第 4 章 在网络中实施 Cisco PIX**

防火墙 .....	41
4.1 设计考虑 .....	41
4.2 DMZ .....	42
4.3 选择合适的 PIX 防火墙型号 .....	42
4.4 应用举例 .....	44
4.4.1 企业网应用举例 .....	45
4.4.2 大型公司网络应用举例 .....	52
4.4.3 中小型商业网络应用举例 .....	58
4.4.4 SOHO 网络应用举例 .....	62
4.5 小结 .....	66
4.6 复习题 .....	66

**第三部分 防火墙配置****第 5 章 Cisco PIX 防火墙入门**

5.1 CLI .....	71
5.2 配置 PIX 防火墙 .....	73
5.2.1 查看与保存配置 .....	74
5.2.2 命令 write erase 与 tftp-server .....	74
5.2.3 命令 write net 与 configure net .....	75
5.2.4 命令 name .....	76
5.2.5 命令 reload .....	77

5.3 检查 PIX 防火墙的状态 .....	77
5.3.1 命令 show memory .....	77
5.3.2 show version .....	77
5.3.3 命令 show ip address .....	78
5.3.4 命令 show interface .....	78
5.3.5 命令 show cpu usage .....	81
5.3.6 命令 ping .....	81
5.4 时间设置和 NTP 支持 .....	82
5.4.1 设置节约白天时间和时区 .....	83
5.4.2 命令 ntp .....	84
5.5 ASA 安全级别 .....	85
5.6 基本的 PIX 防火墙配置 .....	87
5.6.1 命令 nameif .....	87
5.6.2 命令 interface .....	88
5.6.3 命令 ip address .....	89
5.7 nat 命令 .....	90
5.7.1 global 命令 .....	92
5.7.2 route 命令 .....	92
5.8 Syslog 命令 .....	93
5.9 配置 DHCP 服务器 .....	96
5.9.1 DHCP 基础知识 .....	97
5.9.2 配置一台 PIX 防火墙作为 DHCP 服务器 .....	98
5.9.3 DHCP 中继 .....	102
5.10 PPPoE 和 PIX 防火墙 .....	103
5.10.1 在 PIX 防火墙上配置 PPPoE .....	104
5.10.2 监控 PPPoE 客户端 .....	106
5.11 小结 .....	108
5.12 复习题 .....	108
5.13 实验练习——Cisco PIX 防火墙入门 .....	108
5.13.1 目标 .....	109
5.13.2 实验拓扑结构 .....	109
5.13.3 任务 1——执行常用的 命令 .....	109
5.13.4 任务 2——配置 PIX 防火 墙的接口 .....	112
5.13.5 任务 3——配置用于内部 和外部接口的全局地址、 NAT 和路由选择 .....	114
5.13.6 任务 4——测试内部、 外部接口的连接性 .....	116
5.13.7 任务 5——配置系统	

日志输出 .....	117	7.2.5 标识 NAT .....	165
5.13.8 任务 6——配置将系统		7.2.6 策略 NAT .....	165
日志输出到一台系统日志		7.2.7 转换和连接 .....	166
服务器上 .....	118	7.2.8 静态和管道 .....	168
<b>第 6 章 Cisco PIX 设备管理器</b> .....	121	7.3 配置 DNS 支持 .....	170
6.1 PDM 概述 .....	121	7.3.1 使用 alias 命令实现 DNS	
6.2 PDM 操作要求 .....	123	支持 .....	170
6.2.1 Windows 系统的要求 .....	124	7.3.2 通过扩展的 NAT 和 Static	
6.2.2 Sun Solaris 操作系统要求 .....	124	命令完成 DNS 记录转换 .....	174
6.2.3 Linux 操作系统要求 .....	125	7.4 PAT .....	175
6.2.4 总的指导方针 .....	125	7.4.1 使用外部接口地址实现	
6.3 PDM 的准备工作 .....	125	PAT .....	177
6.4 使用 PDM 来配置 PIX 防火墙 .....	128	7.4.2 将子网映射到 PAT 地址上 .....	177
6.4.1 配置 .....	130	7.4.3 使用多个 PAT 来备份 PAT	
6.4.2 监控 .....	140	地址 .....	178
6.5 小结 .....	142	7.4.4 使用 PAT 扩大一个全局	
6.6 复习题 .....	142	地址池 .....	178
6.7 实验练习——用 PDM 配置		7.5 端口重定向 .....	179
PIX 防火墙 .....	142	7.6 配置多个接口 .....	180
6.7.1 目标 .....	142	7.7 小结 .....	182
6.7.2 实验拓扑结构 .....	143	7.8 复习题 .....	183
6.7.3 任务 1——使用 PDM 安装		7.9 实验练习——配置通过 PIX	
向导 .....	143	防火墙的访问 .....	183
6.7.4 任务 2——使用 PDM 安装		7.9.1 目标 .....	184
向导来配置一个特权模式		7.9.2 实验拓扑结构 .....	185
密码 .....	145	7.9.3 任务 1——配置一个通道	
6.7.5 任务 3——配置出站 NAT .....	145	来允许 ICMP 通过 PIX	
6.7.6 任务 4——通过 PIX 防火		防火墙 .....	185
墙测试连通性 .....	147	7.9.4 任务 2——配置 PIX 防火	
6.7.7 任务 5——配置和测试入		墙来允许处于内部接口上	
站访问 .....	147	的用户可以访问堡垒主机 .....	186
6.7.8 任务 6——配置入侵检测 .....	150	7.9.5 任务 3——配置 PIX 防火	
6.7.9 任务 7——配置 PDM 监控		墙来允许处于外部接口上	
制入侵检测 .....	151	的用户可以访问堡垒主机 .....	187
<b>第 7 章 转换和连接</b> .....	153	7.9.6 任务 4——配置 PIX 防火墙	
7.1 传输协议 .....	153	来允许处于外部接口上的	
7.1.1 TCP .....	153	用户可以访问内部的主机 .....	188
7.1.2 UDP .....	155	<b>第 8 章 访问控制列表和内容过滤</b> .....	191
7.2 NAT .....	156	8.1 访问控制列表 .....	191
7.2.1 动态内部转换 .....	157	8.2 把 conduit 转换成 ACL .....	197
7.2.2 静态内部转换 .....	160	8.3 使用 ACL .....	201
7.2.3 动态外部转换 .....	162	8.4 恶意活动代码过滤 .....	206
7.2.4 静态外部转换 .....	163	8.4.1 Java Applet 过滤 .....	206
		8.4.2 ActiveX 过滤 .....	206

8.5 URL 过滤 .....	207	10.2.4 查看 SMR 配置 .....	256
8.6 小结 .....	211	10.3 小结 .....	256
8.7 复习题 .....	211	10.4 复习题 .....	257
8.8 实验练习——在 PIX 防火墙上配置 ACL .....	211	<b>第四部分 高级配置</b>	
8.8.1 目标 .....	213	<b>第 11 章 高级协议处理 .....</b>	
8.8.2 实验拓扑结构 .....	213	261	
8.8.3 任务 1——关闭到一个接口的 ping .....	214	11.1 高级协议 .....	261
8.8.4 任务 2——配置入站 ACL .....	215	11.1.1 修正命令 .....	262
8.8.5 任务 3——测试并验证入站 ACL .....	216	11.1.2 FTP 标准模式 .....	264
8.8.6 任务 4——配置出站 ACL .....	217	11.1.3 FTP 被动模式 .....	265
8.8.7 任务 5——测试并验证出站 ACL .....	218	11.1.4 FTP 修正配置 .....	265
<b>第 9 章 对象分组 .....</b>	<b>221</b>	11.1.5 rsh .....	266
9.1 对象分组入门 .....	221	11.1.6 SQL*Net .....	268
9.2 嵌套式对象分组 .....	227	11.1.7 SIP .....	269
9.3 小结 .....	230	11.1.8 SCCP .....	269
9.4 复习题 .....	230	11.2 多媒体协议支持 .....	270
9.5 实验练习——配置对象组 .....	230	11.2.1 标准的 RTP 模式 .....	271
9.5.1 目标 .....	232	11.2.2 RealNetworks RDT 模式 .....	272
9.5.2 实验拓扑结构 .....	232	11.2.3 RTSP Fixup Configuration .....	272
9.5.3 任务 1——配置服务对象分组 .....	233	11.2.4 H.323 Fixup .....	273
9.5.4 任务 2——配置一个 ICMP 类型对象分组 .....	233	11.3 小结 .....	275
9.5.5 任务 3——配置一个嵌套式服务器对象分组 .....	234	11.4 复习题 .....	275
9.5.6 任务 4——使用对象分组配置一个入站 ACL .....	235	11.5 实验练习——配置并且测试 Cisco PIX 防火墙的高级协议处理 .....	275
9.5.7 任务 5——配置到内部主机的 Web 和 ICMP 访问 .....	236	11.5.1 目标 .....	277
9.5.8 任务 6——测试并检查入站 ACL .....	237	11.5.2 实验拓扑结构 .....	277
<b>第 10 章 路由选择 .....</b>	<b>239</b>	11.5.3 任务 1——显示已配置的修正协议 .....	277
10.1 路由选择选项 .....	239	11.5.4 任务 2——改变已配置的修正协议 .....	278
10.1.1 静态路由选择 .....	239	11.5.5 任务 3——测试出站 FTP 修正协议 .....	278
10.1.2 动态路由 .....	241	11.5.6 任务 4——测试入站 FTP 修正协议 .....	279
10.2 IP 组播协议 .....	251	11.5.7 任务 5——将修正协议恢复成缺省设置 .....	280
10.2.1 允许主机接收组播通信 .....	252	11.5.8 任务部分答案 .....	280
10.2.2 为组播源转发组播通信 .....	254	<b>第 12 章 攻击保护、入侵监测与动态阻挡 .....</b>	
10.2.3 配置其他的 IGMP 选项 .....	255	283	
		12.1 攻击保护 .....	283
		12.1.1 邮件保护 .....	283

12.1.2 DNS 保护 .....	284	Windows 2000 服务器的 机器上安装 CSACS .....	337
12.1.3 分段保护和虚拟重组 .....	286	13.11.4 任务 2——向 CSACS 数据库中添加用户 .....	337
12.1.4 AAA 洪泛保护 .....	288	13.11.5 任务 3——标识 AAA 服务器和协议 .....	338
12.1.5 SYN 洪泛保护 .....	288	13.11.6 任务 4——配置并测试 入站访问的认证 .....	338
12.1.6 反欺骗 .....	291	13.11.7 任务 5——配置并测试 出站访问的认证 .....	339
12.2 入侵检测 .....	292	13.11.8 任务 6——配置并测试 控制台访问的认证 .....	340
12.3 动态阻挡 .....	296	13.11.9 任务 7——配置并测试 虚拟 Telnet 认证 .....	341
12.4 小结 .....	297	13.11.10 任务 8——改变并测试 认证超时时间和提示 信息 .....	341
12.5 复习题 .....	298	13.11.11 任务 9——配置 ACS, 在认证的时候写入可 下载的 ACL .....	343
12.6 实验练习——配置入侵检测 .....	298	13.11.12 任务 10——使用入站 访问认证, 验证可下载 ACL 的功能 .....	343
12.6.1 目标 .....	300	13.11.13 任务 11——配置并测试 记帐 .....	345
12.6.2 实验拓扑结构 .....	300		
12.6.3 任务 1——配置启用 Cisco IDS 信息特征码, 发送 Cisco IDS 系统日 志到系统日志服务器 .....	300		
12.6.4 任务 2——配置启用 Cisco IDS 攻击特征码, 发送 Cisco IDS 系统日 志到系统日志服务器 .....	301		
<b>第 13 章 认证、授权与记帐 .....</b>	<b>305</b>	<b>第 14 章 故障倒换 .....</b>	<b>347</b>
13.1 AAA 基础知识 .....	305	14.1 理解故障倒换 .....	347
13.2 直通代理操作过程 .....	307	14.1.1 故障倒换的 IP 地址 .....	348
13.3 支持的 AAA 服务器 .....	308	14.1.2 配置复制 .....	348
13.4 在 Windows NT 上安装 CSACS .....	308	14.1.3 状态故障倒换 .....	349
13.5 认证配置 .....	315	14.1.4 故障倒换接口测试 .....	349
13.5.1 其他服务的认证 .....	318	14.2 硬件要求 .....	350
13.5.2 控制台访问的认证 .....	321	14.3 基于电缆的故障倒换配置 .....	351
13.6 授权配置 .....	324	14.4 基于 LAN 的故障倒换配置 .....	356
13.6.1 添加授权规则 .....	325	14.5 小结 .....	360
13.6.2 可下载的 ACL .....	326	14.6 复习题 .....	360
13.7 记帐配置 .....	330	14.7 实验练习——配置基于 LAN 的故障倒换 .....	360
13.7.1 <b>match acl_name</b> 选项 .....	331	14.7.1 目标 .....	361
13.7.2 查看 CSACS 中的记帐 信息 .....	331	14.7.2 实验拓扑结构 .....	361
13.8 查找 AAA 配置故障 .....	332	14.7.3 任务 1——将主 PIX 防 火墙配置成基于 LAN 的 状态故障倒换模式的备用	
13.9 小结 .....	334		
13.10 复习题 .....	334		
13.11 实验练习——在 PIX 防火墙 上配置 AAA .....	334		
13.11.1 目标 .....	336		
13.11.2 实验拓扑结构 .....	336		
13.11.3 任务 1——在运行			



PIX 防火墙	361	16.3.2 创建变换集	408
14.7.4 任务 2——配置基于 LAN 故障倒换的备用 PIX 防火墙	365	16.4 创建加密图	408
14.7.5 任务 3——测试基于 LAN 状态的故障倒换	366	16.4.1 创建一个 IPSec 规则	409
14.7.6 任务 4——让主 PIX 防火墙处于活动状态	367	16.4.2 VPN 助手	410
		16.4.3 简易 VPN	413
<b>第五部分 VPN 配置</b>		16.5 案例研究：使用预先共享 密钥的三站点全网状 IPSec 隧道	414
<b>第 15 章 虚拟专用网</b>	371	16.5.1 网络安全策略	415
15.1 利用 PIX 防火墙提供安全的 VPN	371	16.5.2 波特兰、西雅图和圣何塞 防火墙上的配置举例	415
15.2 IPSec 概述	372	16.6 小结	418
15.2.1 支持的 IPSec 标准	374	16.7 复习题	418
15.2.2 IKE	374	16.8 实验练习——配置站到站 VPN	418
15.2.3 DES	374	16.8.1 目标	419
15.2.4 3DES	375	16.8.2 实验拓扑结构	419
15.2.5 AES	375	16.8.3 任务 1——配置 IKE 参数	419
15.2.6 D-H	375	16.8.4 任务 2——配置 IPSec 参数	420
15.2.7 MD5	375	16.8.5 任务 3——IPSec 配置的 测试和验证	421
15.2.8 SHA-1	375	16.8.6 任务 4——使用 PDM (可选)	423
15.2.9 RSA 签名	375	16.8.7 任务 5——使用 PDM VPN 助手 (可选)	423
15.2.10 CA	376	<b>第 17 章 客户端远程访问 VPN</b>	425
15.2.11 NAT-T	376	17.1 Cisco VPN 客户端	425
15.2.12 SA	376	17.2 配置远程访问 VPN	428
15.3 IKE 概述	376	17.3 使用 PDM 配置远程访问 VPN	437
15.4 CA 概述	377	17.4 小结	443
15.5 小结	380	17.5 复习题	443
15.6 复习题	380	17.6 实验练习——远程访问 VPN	443
<b>第 16 章 站到站 VPN</b>	383	17.6.1 目标	444
16.1 IPSec 配置任务	383	17.6.2 实验拓扑结构	445
16.1.1 任务 1——准备配置 VPN	384	17.6.3 任务 1——配置 PIX 防火墙	445
16.1.2 任务 2——配置 IKE 参数	387	17.6.4 任务 2——在 CSACS 中 创建用户	447
16.1.3 任务 3——配置 IPSec 参数	390	17.6.5 任务 3——验证配置	447
16.1.4 任务 4——VPN 配置的 测试与验证	400	17.6.6 任务 4——在主机 1 上 安装 Cisco VPN 客户端	449
16.2 简易 VPN 操作	400		
16.3 使用 PDM 配置 VPN	405		
16.3.1 系统选项	405		