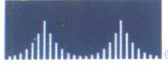


CISCO SYSTEMS



Cisco Press

Cisco 职业认证培训系列  
CISCO CAREER CERTIFICATIONS

CQS



# Cisco 安全 PIX 防火墙

Cisco Secure  
PIX Firewalls

Reduce the threat of network attacks with the  
official CSPFA Coursebook

[美] David W. Chapman Jr.  
Andy Fox

著

刘兴初 李逢天

译

李逢天

审校

人民邮电出版社

POSTS & TELECOMMUNICATIONS PRESS

Cisco 职业认证培训系列

# Cisco 安全 PIX 防火墙

[美] David W. Chapman Jr. Andy Fox 著

刘兴初 李逢天 译

李逢天 审校

人民邮电出版社

---

## 图书在版编目 (CIP) 数据

Cisco 安全 PIX 防火墙 / (美) 查普曼 (Chapman, D. W.), (美) 福克斯 (Fox, J. A.) 著; 刘兴初, 李逢天译. —北京: 人民邮电出版社, 2002.8

ISBN 7-115-10388-7

I. C... II. ①查...②福...③刘...④李... III. 计算机网络—防火墙 IV. TP393.08  
中国版本图书馆 CIP 数据核字 (2002) 第 043130 号

## 版权声明

David W. Chapman Jr. Andy Fox: Cisco Secure PIX Firewalls

Authorized translation from English language edition published by Cisco Press.

Copyright ©2002 by Cisco Press.

All rights reserved.

本书中文简体字版由美国 **Cisco Press** 出版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。

Cisco 职业认证培训系列

### Cisco 安全 PIX 防火墙

◆ 著 [美] David W. Chapman Jr. Andy Fox  
译 刘兴初 李逢天  
审 校 李逢天  
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 315@ptpress.com.cn  
网址 <http://www.ptpress.com.cn>  
读者热线 010-67180876  
北京汉魂图文设计有限公司制作  
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: 19  
字数: 454 千字 2002 年 8 月第 1 版  
印数: 1-4 000 册 2002 年 8 月北京第 1 次印刷

著作权合同登记 图字: 01-2002-0395 号

ISBN 7-115-10388-7/TP · 2939

定价: 40.00 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

本书详细介绍了配置、验证并管理 PIX 防火墙产品系列的相关知识，内容包括黑客的常见攻击手段，网络内部和外部的安全威胁；不同型号 PIX 防火墙的特点，升级所需要完成的任务；基本的安装细节，以及如何启用更高级的特性和访问控制；采用 PIX 系统日志服务和 PIX AAA 子系统的管理和监测；配置 PIX 故障切换机制，PIX 上的 IPSec，以及 Cisco IOS 防火墙特性集。附录提供了一些很有帮助的参考，包括配置 PIX 入侵检测特性、SNMP 管理支持、DHCP 客户端和服务端、安全 Shell 协议（SSH）连接，以及许多与安全相关的资源。

本书适合那些准备参加 Cisco Security Specialist 1 认证考试的人员。本书还适合那些想理解并更有效地使用 PIX 防火墙的网络管理人员。

## 关于作者

David W. Chapman Jr., CCSI, CCNP, CCDP, CSS-1, 是 Global Knowledge 公司的 Cisco 安全讲师。David 是“Cisco 安全 PIX 防火墙”课程的主管，他负责保证课程的完整性和质量，并向刚接触这门课程的讲师提供指导。自从 1994 年，David 就开始在企业网络中使用 Cisco 公司的产品。在来到 Global Knowledge 公司之前，他在波特兰的一家 Cisco 金牌认证伙伴公司工作，去年他在那里帮助 Cisco 的 SmartStart Customers 计划建立原型、测试并建立安全的电子商务基础平台。最近，David 已经通过了 CCIE 安全资格考试，正准备参加实验室考试。

Andy Fox, CCSI, CCNA, CCDA, CSS-1, 是 Global Knowledge 公司的一名 CCSI(认证 Cisco 认证的讲师)。Andy 已经讲授了 5 年多的 Cisco 认证课程，目前是“管理 Cisco 网络安全 (MCNS)”课程的主管。Andy 在 1980 年从 Purdue 大学毕业后，从事了计算机科学方面的职业，在空军担任计算机操作员。Andy 在他的 5 年军旅生涯中从事过不同的工作。其中一个工作是在德国的 Ramstein 空军基地的 BBN C70 MINET 主机的系统管理员。那份工作帮助他得到了下一份工作：在 Massachusetts Cambridge 的 Bolt Beranck 和 Newman 的网络运行控制员。在网络运行中心工作期间，Andy 帮助维护许多广域网络，包括 ARPANET、MILNET 和 MINET。他随后的工作是在 New York City 的 TYMNET (英国电信) 的系统工程师和在 Pennsylvania Collegeville 的 RPR 药厂的系统工程师，在这些工作之后，他于 1996 年成为了一名讲师。

## 关于技术审稿人

Randy Ivener 是 Cisco 公司的高级工程服务组的安全和 VPN 专家。他是一名 CCNP、Cisco 安全专家-1 (CSS-1) 和 ASQ 认证的软件质量工程师。作为一名网络安全顾问，他用了几年的时间，帮助公司理解并保护他们的网络安全。他熟悉许多安全产品和技术，包括防火墙、VPN、入侵检测和认证系统。在从事安全工作之前，他将很多时间用于软件开发并担任培训讲师。Randy 毕业于美国海军学院，拥有 MBA 学位。

Doug McKillip, P.E., CCIE #1851, 是一名独立顾问，从事与 Global Knowledge 公司相关的 Cisco 认证培训方面的咨询。他在计算机网络方面超过 13 年的工作经验，在过去的 9 年中，他主要从事安全和防火墙工作。在最初采用 MCNS 第一版培训课程的时候，Doug 提供了许多指导性的和技术性的帮助，他一直是 Global Knowledge 公司 (Cisco 公司的培训伙伴) 的首席讲师和课程主管。Doug 拥有 MIT 的化学工程学士与硕士学位，Delaware 大学的计算机科学硕士学位。他现在居住在 Delaware Wilmington。

David Ofsevit 是 Cisco 公司的技术市场工程师。现在，他在 Cisco 的企业解决方案工程组工作，侧重于网络设计的安全部分。这个工作得益于他先前从事的销售技术支持的工作经验，当时他也是从事网络安全工作。他是 Cisco 安全领域解决方案设计组的成员，也是安全与 VPN 顾问组的成员。

在 1996 年，Cisco 公司收购了 TGV 软件公司，David 自从那时起就加入了 Cisco 公司。在 TGV 公司工作之前，David 工作过的公司有 DEC 公司、Mitre Corporation 公司和美国运输部。他拥有 MIT 的电子工程 S.B-S.M 组合学位。

Gilles Piche, CCSI, 是一名安全顾问，在过去 5 年中，他在加拿大一直工作于网络安全领域。在此之前，他供职于

加拿大政府，从事网络工程工作。Gilles 也是一名 Cisco 认证的安全讲师，在最近的一年半时间里，他为 Global Knowledge Network（加拿大）公司讲授 Cisco 安全课程。

# 前

# 言

本书的目的是为了帮助网络工程师深刻理解 PIX 防火墙，以及如何使用防火墙来减轻对他们网络的巨大威胁。读者需要具备基本的 IP 操作和安全概念，这样才能更好地利用本书的内容。对于刚刚接触网络安全和 PIX 防火墙的读者，我们建议先阅读《管理 Cisco 网络安全 (MCNS)》(Michael Wenstrom 著，中文版由人民邮电出版社出版)。就像 MCNS 课程是“Cisco 安全 PIX 防火墙”课程的前期必要课程一样，MCNS 一书提供了本书所需的许多基本知识。

不仅网络工程师将从本书中受益，网络设计者也将发现书中的案例学习对于设计安全网络基础结构是非常有价值的。而且，信息系统审计员也将获得所需的知识，以正确评估复杂的配置，判断是否符合保密要求。本书所提供的案例学习将用来对常用的配置进行讨论。

## 本书的创作动机

本书面向的读者是那些想要更新他们的基本 PIX 操作知识并想钻研高级配置的网络工程师。我们发现在书店里目前还没有其他的书讲述 PIX 的高级特性。

## 本书目标

本书的目标是将那些具备基本 PIX 知识的读者引领到一个更高的水平，使他们掌握高级 PIX 防火墙技能。通过向读者提供通用的实际案例学习，本书帮助读者在设计并实施他们自己的 PIX 安全方案时，理解各种配置方案的优点和不足。

## 本书所用的表示习惯

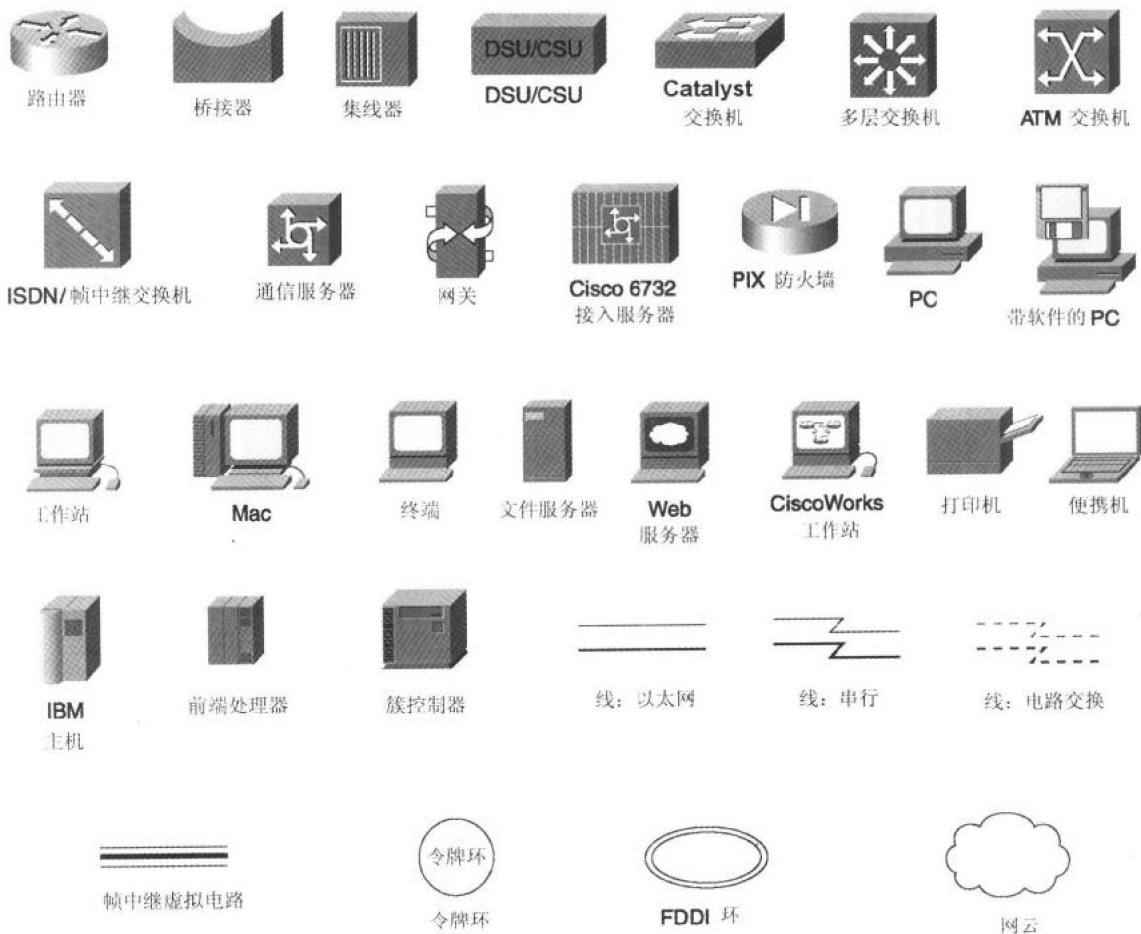
本书中采用的命令语法的表示习惯与 Cisco IOS 软件命令参考中的习惯相同。命令参考的表示习惯如下：

- 竖条(|)用于分开互斥的选项。
- 方括号[ ]表示任选的关键字或参数。
- 大括号{ }表示必选项。



- 大括号位于方括号内[{} ]表示任选项中的必选项。
- 命令和关键字用粗体字表示。在配置实例和输出显示中（不是指一般的命令语法），粗体字表示命令需要用户手工输入（例如 **show** 命令）。
- 斜体字表示用户应输入具体值的参数。

### 本书所用的图标



# 序

2001年1月, Cisco Systems 公司宣布了一套新的职业认证系列, 称为 Cisco 认证专家 (Cisco Qualified Specialist, CQS)。最先发布的 CQS 是 Cisco 安全专家 1 (Cisco Security Specialist 1, CSS-1)。CSS1 是设计用于认证技术人员的通用网络安全技能和知识, 它侧重于入侵检测系统、防火墙和虚拟专用网络。最近, 对于合格的网络安全专业人员的需求量越来越大。每天, 企业都在进行着一场永无终止的战争: 保证他们网络的安全, 使他们的网络免受那些蓄意破坏系统或企图获取非授权访问权限的黑客的威胁。对于那些负责确保访问安全并控制网络内部活动的网络安全专业人员来讲, 控制防火墙被认为是一项很关键的技能。

《Cisco 安全 PIX 防火墙》采用书本的形式, 所讲授的知识与有导师辅导的实验室课程和远程教学的同名课程是一样的。尽管以书本的形式来推广这些知识与参加由 Cisco 教学伙伴提供的 Cisco 认证培训中获得的动手经验不能相提并论, 但它是满足全球对 Cisco 培训需求的一个极具价值的构成部分。本书使读者能够描述、配置、验证并管理 PIX 防火墙产品系列以及 Cisco 路由器中的 Cisco IOS 防火墙特性集。CSPFA 教材和 Cisco Press 出版社的其他书籍都具有较高的质量标准, 保证了高质量的知识传授。无论读者是为了准备 CSS-1 认证考试, 还是对安装、配置并操作 Cisco PIX 防火墙感兴趣, 这本书都将增强读者对防火墙的理解。

其他 CSS-1 认证教材包括《管理 Cisco 网络安全》、《Cisco 安全虚拟专用网络》和《Cisco 安全入侵检测系统》。

Rick Stiffler  
Cisco Systems 公司  
VPN 和安全培训部经理  
2001年9月

# 目 录

<b>第 1 章 网络安全介绍</b> .....	2
1.1 为什么网络安全是必需的 .....	3
1.2 定义安全的网络设计 .....	4
1.3 网络安全威胁分类 .....	6
1.4 网络安全是如何被破坏的 .....	7
1.4.1 侦察攻击 .....	7
1.4.2 访问攻击 .....	7
1.4.3 DoS 攻击 .....	8
1.5 网络安全策略和安全轮图 .....	9
1.6 小结 .....	10
1.7 复习题 .....	11
<b>第 2 章 Cisco PIX 防火墙软件和硬件</b> .....	12
2.1 防火墙的类型 .....	13
2.1.1 数据包过滤器 .....	14
2.1.2 代理过滤器 .....	15
2.1.3 状态型数据包过滤器 .....	16
2.2 PIX 防火墙逻辑 .....	16
2.3 PIX 防火墙的型号 .....	17
2.4 复习题 .....	23
<b>第 3 章 使用并升级 Cisco PIX 防火墙软件映像</b> .....	26
3.1 PIX 命令行接口 .....	28
3.2 维护并测试 PIX 防火墙 .....	29
3.3 在 PIX 防火墙上安装一个新的 OS .....	36
3.3.1 升级到 PIX 防火墙的一个不同版本 .....	36
3.3.2 使用监视模式升级到一个不同的 PIX OS .....	37
3.3.3 安装 PIX OS 5.0 和更早的版本 .....	38
3.3.4 安装 PIX OS 5.1 和更新的版本 .....	38

3.3.5 用 Windows PC 创建一张启动帮助 (Boothelper) 磁盘 .....	39
3.3.6 用 UNIX、Solaris 或 Linux 工作站创建一张启动帮助磁盘 .....	39
3.3.7 为具有软盘驱动器的 PIX 防火墙安装并使用启动帮助程序 .....	40
3.4 口令恢复 .....	41
3.4.1 对于 PIX Classic、PIX 10000、510 和 520 的软盘口令恢复 .....	41
3.4.2 对于 PIX 506、515、525 和 535 的 TFTP 口令恢复 .....	42
3.5 复习题 .....	43
<b>第 4 章 配置 Cisco PIX 防火墙 .....</b>	<b>44</b>
4.1 ASA 安全级别 .....	45
4.2 配置 Cisco PIX 防火墙的 6 个基本命令 .....	47
4.2.1 nameif 命令 .....	47
4.2.2 interface 命令 .....	48
4.2.3 ip address 命令 .....	49
4.2.4 nat 命令 .....	50
4.2.5 global 命令 .....	50
4.2.6 route 命令 .....	52
4.3 复习题 .....	54
<b>第 5 章 Cisco PIX 防火墙翻译 .....</b>	<b>56</b>
5.1 传输协议 .....	58
5.1.1 传输控制协议 .....	58
5.1.2 用户数据报协议 .....	60
5.2 PIX 防火墙翻译 .....	61
5.2.1 静态地址翻译 .....	61
5.2.2 动态地址翻译 .....	63
5.2.3 翻译和连接 .....	65
5.3 复习题 .....	67
<b>第 6 章 配置通过 Cisco PIX 防火墙的访问 .....</b>	<b>68</b>
6.1 配置通过 PIX 防火墙的访问 .....	69
6.2 理解静态翻译和管道命令 .....	70
6.2.1 static 命令 .....	71
6.2.2 conduit 命令 .....	71
6.3 穿过 PIX 进行访问的其他方法 .....	76
6.3.1 配置 PAT .....	77
6.3.2 配置 nat 0 .....	78
6.3.3 配置 FIXUP 协议 .....	79
6.3.4 多媒体支持 .....	80
6.4 配置多个接口 .....	81

---

6.5 复习题 .....	84
<b>第 7 章 系统日志 .....</b>	<b>86</b>
7.1 系统日志消息 .....	87
7.2 系统日志配置 .....	88
7.2.1 logging host 命令 .....	90
7.2.2 logging trap 命令 .....	91
7.2.3 logging buffered 命令 .....	91
7.2.4 logging console 命令 .....	91
7.2.5 logging facility 命令 .....	91
7.2.6 logging monitor 命令 .....	92
7.2.7 logging standby 命令 .....	92
7.2.8 logging timestamps 命令 .....	92
7.2.9 (no) logging message 命令 .....	93
7.2.10 show logging 命令 .....	93
7.2.11 clear logging 命令 .....	94
7.3 依据不同版本的、新的系统日志消息 .....	94
7.4 复习题 .....	94
<b>第 8 章 Cisco PIX 防火墙上的 AAA 配置 .....</b>	<b>96</b>
8.1 定义 AAA .....	97
8.2 直通式代理的操作运行 .....	100
8.3 支持的 AAA 服务器 .....	101
8.4 安装用于 Windows NT 的 CSACS .....	101
8.5 配置认证 .....	106
8.5.1 其他服务的认证 .....	109
8.5.2 虚拟 Telnet .....	109
8.5.3 虚拟 HTTP .....	111
8.5.4 控制台访问的认证 .....	112
8.5.5 改变认证超时时间 .....	113
8.5.6 改变认证提示 .....	115
8.6 配置授权 .....	115
8.6.1 为 CSACS-NT 增加授权规则 .....	117
8.6.2 其他服务的授权 .....	119
8.7 配置审计 .....	120
8.7.1 用 CSACS-NT 查看审计记录 .....	121
8.7.2 其他服务的审计 .....	122
8.8 检验配置 .....	123
8.9 复习题 .....	124
<b>第 9 章 Cisco PIX 防火墙高级协议处理和攻击防卫 .....</b>	<b>126</b>

9.1 对高级协议处理的需求	128
9.1.1 标准模式的 FTP	128
9.1.2 被动模式的 FTP	130
9.1.3 fixup protocol FTP 命令	131
9.1.4 远程命令解释程序 (rsh)	132
9.1.5 SQL*Net	133
9.2 多媒体支持	135
9.2.1 实时流协议 (RTSP)	136
9.2.2 H.323	139
9.3 攻击防卫	140
9.3.1 邮件防卫	140
9.3.2 DNS 防卫	141
9.3.3 碎片攻击防卫	142
9.3.4 AAA 风暴攻击防卫	143
9.3.5 SYN 风暴攻击防卫	144
9.4 总结	147
9.5 复习题	147
<b>第 10 章 Cisco PIX 防火墙故障切换</b>	<b>148</b>
10.1 故障切换操作	150
10.1.1 故障切换电缆	151
10.1.2 配置复制	151
10.1.3 故障切换监视	152
10.1.4 故障恢复	155
10.2 配置故障切换	155
10.3 实验练习	158
10.3.1 任务 1: 配置主 PIX 防火墙, 使它可以在发生故障时切换到 PIX 防火墙	159
10.3.2 任务 2: 强制让主 PIX 防火墙再次回到活跃状态	161
10.3.3 任务 3: 为主 PIX 防火墙配置状态型故障切换	161
10.4 复习题	163
<b>第 11 章 为 Cisco PIX 防火墙配置 IPSec</b>	<b>164</b>
11.1 Cisco 安全 PIX 防火墙支持安全的 VPN	165
11.1.1 PIX、VPN 和 IPSec	167
11.1.2 IPSec	168
11.1.3 IKE	168
11.1.4 SA	168
11.1.5 DES	168
11.1.6 3DES	169
11.1.7 D-H	169

11.1.8 MD5 .....	169
11.1.9 SHA-1 .....	169
11.1.10 RSA 签名 .....	169
11.1.11 CA .....	169
11.2 配置 PIX 防火墙的 IPSec 支持 .....	170
11.2.1 任务 1: 为 IPSec 做准备 .....	171
11.2.2 任务 2: 为预共享密钥配置 IKE .....	171
11.2.3 任务 3: 配置 IPSec .....	175
11.2.4 任务 4: 测试并检验 IPSec 的总体配置 .....	187
11.3 扩展 PIX 防火墙 VPN .....	188
11.3.1 PIX 防火墙的 CA 注册 .....	188
11.4 案例学习 1: 使用预共享密钥为点对点主机配置 PIX 防火墙 IPSec .....	189
11.4.1 网络安全策略 .....	189
11.4.2 PIX 1 防火墙的配置实例 .....	189
11.4.3 PIX 2 防火墙的配置实例 .....	191
11.5 案例学习 2: 使用预共享密钥的三个站点完全网状连接 IPSec 隧道 .....	192
11.5.1 网络安全策略 .....	193
11.5.2 Portland、Seattle 和 San Jose PIX 防火墙的配置实例 .....	193
11.6 总结 .....	196
11.7 复习题 .....	196
11.8 参考文献 .....	197
<b>第 12 章 Cisco IOS 防火墙基于上下文的访问控制 .....</b>	<b>198</b>
12.1 Cisco IOS 防火墙简介 .....	199
12.1.1 基于上下文的访问控制 .....	200
12.1.2 认证代理 .....	200
12.1.3 入侵检测 .....	201
12.2 基于上下文的访问控制的操作运行 .....	205
12.2.1 配置 CBAC .....	208
12.2.2 配置 CBAC .....	214
12.2.3 将检查规则和 ACL 应用到路由器接口上 .....	218
12.2.4 测试、检验并监视 CBAC .....	222
12.3 复习题 .....	223
<b>第 13 章 Cisco IOS 防火墙认证代理配置 .....</b>	<b>224</b>
13.1 IOS 认证代理简介 .....	225
13.2 认证代理配置任务 .....	227
13.2.1 AAA 服务器配置 .....	228
13.2.2 AAA 配置 .....	231
13.2.3 认证代理配置 .....	233

13.2.4 测试并检验配置 .....	234
13.2.5 认证代理服务配置实例 .....	235
13.3 复习题 .....	237
<b>附录 A 为入侵检测配置 PIX .....</b>	<b>238</b>
A.1 PIX 入侵检测简介 .....	239
A.2 入侵检测配置要素 .....	240
A.2.1 以接口为单位配置审计策略 .....	240
A.2.2 从审计策略中选择性地禁用 IDS 特征 .....	242
A.3 PIX IDS 配置实例 .....	242
A.4 PIX IDS 特征 .....	244
A.5 常见问题的问答 .....	244
A.6 推荐读物列表 .....	245
<b>附录 B 在 PIX 防火墙上配置 SNMP 协议 .....</b>	<b>246</b>
B.1 理解 PIX 对 SNMP 的支持 .....	247
B.2 从 PIX 上检索 SNMP 数据 .....	248
B.2.1 MIB 浏览 .....	248
B.2.2 SNMP 陷阱 .....	248
B.2.3 配置 PIX 来允许浏览 MIB 并发送系统日志陷阱 .....	248
B.3 SNMP v1 MIB-II 目录 .....	249
B.4 网络上的 SNMP 资源 .....	250
<b>附录 C 在 PIX 防火墙上配置动态主机配置协议 (DHCP) .....</b>	<b>252</b>
C.1 DHCP 基础 .....	253
C.2 DHCP 服务器 .....	254
C.3 DHCP 客户端 .....	254
C.4 配置实例 .....	255
C.4.1 PIX 506 作为 DHCP 服务器: 静态外部地址 .....	255
C.4.2 PIX 506 作为 DHCP 客户端: 动态获取的外部地址 .....	256
C.5 互联网上的 DHCP 资源 .....	256
<b>附录 D 在 PIX 防火墙上配置安全 Shell (SSH) .....</b>	<b>258</b>
D.1 安全 Shell (SSH) 简介 .....	259
D.2 为 SSH 访问配置 PIX .....	260
D.2.1 配置 PIX 来接受 SSH 连接 .....	260
D.2.2 配置 SSH 客户端来连接到 PIX .....	261
D.3 SSH 客户端连接的故障诊断 .....	265
D.4 为我们的平台获取一个 SSH 客户端软件 .....	267
<b>附录 E 安全资源 .....</b>	<b>270</b>
<b>附录 F 复习题答案 .....</b>	<b>276</b>



# 原书空白页