Cisco Systems

Cisco 职业认证培训系列
CISCO CAREER CERTIFICATIONS

ciscopress.com

CCIE Security 实验指南

CCIE® Self-Study
CCIE Practical Studies: Security

Hands-on preparation for the CCIE Security lab exam

内附光盘

[美] Dmitry Bokotey，CCIE #4460
[英] Andrew Mason，CCIE #7144 著
[美] Raymond Morrow，CCIE #4146
陈晓筹，CCIE #10552
邝卫国，CCIE #3415 译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco 职业认证培训系列

CCIE Security 实验指南

[美] Dmitry Bokotey, CCIE#4460
[英] Andrew Mason, CCIE#7144 著
[美] Raymond Morrow, CCIE#4146

陈晓筹，CCIE#10552
邝卫国，CCIE#3415 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

CCIE Security 实验指南 /（美）博克泰（Bokotey, D.）等著；陈晓筹，邝卫国译.
—北京：人民邮电出版社，2005.8
（Cisco 职业认证培训系列）
ISBN 7-115-13528-2

Ⅰ. C... Ⅱ. ①博...②陈...③邝... Ⅲ. 计算机网络－工程技术人员－资格考核－自学参考资料 Ⅳ. TP393

中国版本图书馆 CIP 数据核字（2005）第 064294 号

版 权 声 明

Dmitry Bokotey, Andrew Mason, Raymond Morrow: CCIE Practical Studies: Security
(ISBN: 1587051109)
Copyright © 2003 Cisco Press
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

CCIE Security 实验指南

◆ 著 [美] Dmitry Bokotey, CCIE#4460
[英] Andrew Mason, CCIE#7144
[美] Raymond Morrow, CCIE#4146
译 陈晓筹，CCIE#10552 邝卫国，CCIE#3415
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
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：53
字数：1301 千字 2005 年 8 月第 1 版
印数：1－2 500 册 2005 年 8 月北京第 1 次印刷

著作权合同登记号 图字：01-2004-0566 号
ISBN 7-115-13528-2/TP・4722
定价：148.00 元（附光盘）

读者服务热线：(010) 67132705 印装质量热线：(010) 67129223

内容提要

和所有的CCIE实验室考试一样，CCIE Security的实验室考试力图模拟现实环境中业内专家和 TAC 工程师最经常开展的网络安全实践，并通过一定的形式变化，以检验考生的实际技能水平。准备实验室考试时，如果没有动手实践，就无法充分证明已经准确地理解了安全问题和安全概念。考生接触的案例越多，就越容易理解实验室中的问题，越有可能高效地成功实施解决方案和排除故障。

按照这样的理念，本书给出了一个完整的实验室环境的有条理的逐步扩建过程，带领读者从开始的网络基础知识到后面深入的网络安全知识、专门的网络安全设施，循序渐进地学习。在每一章中，都有课程和案例分析。案例分析用于帮助读者强化相关的概念、算法过程等理论知识，同时包含所有需要的配置，为读者提供最直接的指导。最后的实验室结果就是一个完整的网络安全解决方案。通过完成情况，读者可以评估参加和通过CCIE Security实验室考试所要求的技术能力。由于包含了这些大量的操作实验，本书可以帮助正在准备 CCIE 安全实验室考试的考生以及业界的其他技术人员，提高专业技能，迈向设定的职业发展目标。

关于作者

Dmitry Bokotey，CCIE No.4460，持有路由与交换（Routing & Switching）、ISP 拨号（ISP Dial）和安全（Security）领域 3 张 CCIE 证书，现就职于 Cisco Systems 公司美国高级技术服务 IP/MPLS 核心技术部，担任网络顾问工程师。在过去 10 年中，他为许多大企业和服务提供商设计并实现过各种各样的网络。在其职业生涯中，他多次进行过高级网络技术主题的演讲。目前 Bokotey 先生正为 Cisco Press 编写另一本书，即 *CCNP Practical Studies: Remote Access*。

Andrew G. Mason，CCIE No. 7144，CCDP，CSS1，CCNP:Security。是 Boxing Orange 公司（www.boxingorange.com）的技术主管。Boxing Orange 公司是一家英国公司，Cisco 的 VPN/Security 合作伙伴，专注于 Cisco 安全解决方案的设计与实施。Mason 先生在网络界有 12 年的从业经验，曾为全球很多大型组织提供服务。

Raymond Morrow，CCIE No. 4146，CSS1，Cisco IP 电话设计专家，现就职于 Northrop Grumman 公司。此前，Morrow 先生是德克萨斯圣安东尼奥 Computer Solutions 公司的首席顾问，这家公司是 Cisco 的银牌合作伙伴，并获得了 Security/VPN 合作伙伴专业认证。他在网络行业有 16 年的工作经验，为大量的客户设计、实施过很多网络项目。目前他已通过了 CCIE Security 笔试，正在潜心准备 CCIE Security 的实验室考试，同时还在参加 Cisco Press *CCNP Practical Studies: Remote Access* 编写项目的工作。

此为试读，需要完整PDF请访问：www.ertongbook.com

关于技术审校人

Maurilio Gorito，CCIE No. 3807，持有路由与交换（Routing & Switching，1998）、广域网交换（WAN Switching，2001）和安全（Security，2003）3 张 CCIE 证书。Maurilio 有长达 16 年的 Cisco 网络和 SNA 网络环境的工作经历，包括运行 IGRP、EIGRP、BGP、OSPF、QoS 和 SNA 的大型 IP 网络的规划、设计、实施和故障诊断，网络范围覆盖全球，其中包括巴西和美国。Maurilio 还有 7 年多在学校和公司讲述技术课程的经验。目前他是 Cisco Systems 公司 CCIE 团队中的内容工程师（content engineer），负责协助 CCIE 实验室考试的内容开发，完成实验室考试的内容技术性评价，联系考生（CCIE 客户服务一部分），并在美国加州圣何塞的 CCIE 实验室，监考 CCIE 路由与交换以及安全实验室考试。Maurilio 持有数学和教育学的学位。

Randy Ivener，CCIE No. 10722，Cisco Systems 公司高级服务的安全专家，持有认证的信息系统安全专业人员证书（CISSP，Certified Information Systems Security Professional）和 ASQ 认证的软件质量工程师证书。在作为网络安全顾问的几年中，他帮助公司理解网络安全和实施安全保护，采用的产品和技术包括防火墙、VPN、入侵检测、验证系统等。在投身安全领域之前，他曾从事过软件开发、当过培训讲师。他毕业于美国海军研究院（US Naval Academy），获得商业管理硕士学位。

Martin Walshaw，CCIE No. 5629，CISSP，CCNP，CCDP，是 Cisco Systems 公司南非企业销售部系统工程师。其专业领域包括收敛（convergence）、安全、内容传递连网等，这使得他没日没夜地都在忙于工作。在过去的 15 年中，Martin 涉足从 RPG III、COBOL 编程到 PC 销售等 IT 业的很多方面。在空闲时，Martin 喜欢与他的妻子 Val、儿子 Joshua 和 Callum 一起共度欢乐时光。没有他们的耐心、理解和支持，完成编写本书这样的计划是不可能实现的。

献　辞

Dmitry Bokotey：

献给我的妻子 Alina，感谢她对我的耐心与支持、自始至终陪伴着我，并且毫不怀疑我的“愚蠢”想法。

献给我的女儿 Alyssa，感谢她每天为我的生活带来了阳光和意义。

Andrew Mason：

我想把这本书献给我的家庭。Helen，我美丽的妻子，再次忍受了无数个不眠之夜和忙碌的周末，给予我支持和信赖，毫无怨言。Rosie 和 Jack，我的两个孩子，棒极了，他们让我坚持不懈，让我觉得我是多么的幸运。

Raymond Morrow：

我想把这本书献给那个女人，她是我的整个世界，她的笑容一直照亮着我的每一天；也献给我的孩子们，他们是父母能期盼得到的最好的孩子。

致　谢

Dmitry Bokotey：

本书是集体努力的产物。我想感谢我的合著者，Andrew Mason 和 Raymond Morrow，他们把我带入出版业，感谢他们愿意与我保持同步并让步于我，他们的职业水准和知识使我受益匪浅。我永远感激我的妻子，Alina，她帮助我写作并编辑了我的那些章节。

感谢 Cisco Press 的团队，特别是 Brett Bartow，不但信任我，并与我们配合默契；感谢所有技术审稿人，还有 Dayna Isley，他们的富有价值的建议让本书得以完善。

非常感谢 Cisco Systems 公司 CCIE 部门，特别是 Kathe Saccenti，帮助我成为了一名更好的工程师。

此外，感谢我在 Cisco Systems 公司的同事和经理 Rosa Elena Lorenzana 和 Sanjay Pal 对我的支持和关心。

最后，我要感谢我的父母，他们让我把大量的时间花在了计算机上，尽管他们认为那么做毫无意义。

Andrew Mason：

这本书是由我和其他两位素未谋面、居住在世界的另一边的人合作写成的。我们很快组成团队投入到这个合作项目中。我想感谢他们，Dmitry 和 Raymond，在本书的写作过程中保持了完美与专业的工作态度。那是一种快乐。

我想感谢 Cisco Press 的 Brett Bartow 和 Dayna Isley 对我的帮助和指导，他们提升了整个过程的价值，并减轻了我们的写作的负担。

还要感谢 Max Leitch 以及 Boxing Orange 公司所有职员一直以来的支持和帮助。

Raymond Morrow：

写作本书是一个人生梦想的实现。如果没有家庭、朋友、合著者和 Cisco Press 相关工作人员的支持，我永远不能将这个梦想变成现实。没有我妻子 Liz 的鼓励，没有孩子们对我

将时间长期花在计算机上的理解，这本书可能还只完成了一半。

这种类别以及该主题的图书，实际上是不可能由一个人来完成的，所以我要感谢我的合著者 Dmitry Bokotey 和 Andrew Mason 的乐于妥协和合作的精神，因此促成了我们都引以为自豪的该项目的完成。当然，还要有人帮助我们保持一致性以及正确的方向，所以这里要特别感谢 Brett Bartow，知道何时可以让步，何时不让步。另外还要感谢 Dayna Isley 诚恳的建议，否则这本书可能只是我们 3 个人写的一堆无序的文字。

序

我们已经超越了称之为“网络”的革命。大多数雇员已经非常熟悉网络环境下的应用，人们逐渐把“i”和“e”与各种行为组成的词汇，认为就是结合某种 Internt 功能的工具。在这股潮流中，那些乘浪前进的网络专家，正面临着在安全方面投入更多的精力，以调整、有时甚至是重整网络资源。随着网络活动获得空前的普及，我们意识到安全缺口将潜在地影响无数的用户。在网络效能考虑中，保护网络安全的努力已经大大超出了其他任何因素。对安全实施方面具有深入全面的知识和专门技能的网络人才，世界需求非常旺盛。

因此，CCIE 计划适应这种需求，增加了一个 CCIE 级别的认证，帮助雇主鉴定和证实这方面的专门技能，这是很有意义的。不过，设置 CCIE 的安全系列（Security Track）并不是一种新想法，CCIE 部门认为，这方面已经大大地滞后了。我要感谢在 Cisco Systems 公司内外的许多人，帮助我们把这个系列的认证变成了现实。

大约 3 年前，在引入 CCIE 安全的笔试时，已萌发了 CCIE 安全系列的构思。参加这门考试的人数逐步上升，达到受欢迎程度仅次于路由与交换考试。和所有的 CCIE 实验室一样，我们花费了很长一段时间来仔细地检查、鉴定和改写，以确定实验室吸收了业内专家和 TAC 工程师最常开展的实验，并且对原来广受欢迎的笔试，成为实践性的补充。重要的是要记住，尽管获得 CCIE 实验室考生资格要求通过笔试，但实验室测试的是：在部署更特定的安全功能之前，建立一个实验室基础结构所需的技能。因为 CCIE 计划总是尽每一分力以满足雇主对“互连网络专家”的期望，因此正在寻求 CCIE 安全认证的那些人，在准备 CCIE 安全系列考试时，应该记住这一点。

本书适用于那些希望在 CCIE 安全考试的学习中包含实践内容的网络专业人士。从我多年从事监考官的经验来看，有一点怎么强调都不过分，那就是在任何网络中实现各种功能时，精通其背后的概念的重要性。准备实验室考试时，如果

没有动手实践帮助你深入钻研并达到那个层次的理解，是远不够充分的。考生接触的案例越多，他就越容易理解实验室中的问题。完成实验室活动和实际使用 **show/debug** 命令，能更好地让考生准备高效地成功实现和排除故障的方案。

任何人，如果能将阅读与动手实验相结合，都有很高的获得 CCIE 证书的几率。但重要的是要记住，获得 CCIE 证书并不是终极目标。CCIE 计划致力于确立一个网络界公认的专门技能级别，但获得专门技能的能力并不是仅由 Cisco 的一枚徽章所标记的。最根本地，它是技术知识与通过进行更高级别的准备获得技巧而实现成功的、安全的网络的能力。那才是准备 CCIE 安全实验室考试的最终奖赏。

Kathe Sacccenti，CCIE #2099
CCIE 路由与交换考试生命周期经理，CCIE 安全考试合作开发者
Cisco System 公司

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

在网络技术不断变化的今天，随着我们对采用这一技术来完成日常工作的依赖程度的提高，保护网络安全也达到了前所未有的重要。通过采用硬件和软件，诸如防火墙、虚拟专网（Virtual Private Network，VPN）和入侵检测系统（Intrusion Detection System，IDS）等，很多公司逐步接近脚本小子（script kiddie）和黑帽黑客（black hat hacker）们在今天电子世界提出的挑战，并且寻找他们相信的人员来保护他们的电子环境。

Cisco Systems 公司在它广受欢迎的 CCIE 计划中，已经开发了满足安全专业人士需要的专业化系列——CCIE 安全系列。CCIE 安全系列是声望很高的一项认证，是为把那些在连续变化的网络安全领域中展示他们独特能力的人士认可为安全专家而专门设计的。CCIE 安全系列的考生有两项测试，一项是对常见的以及不引人注意的安全最优方法的书面资格考试，另一项是一天艰难的实验室动手考试，要求他们展示将安全理论应用于网络环境的能力。

本书的目的是通过提供大量的操作实验，帮助那些准备一天实验室考试的 CCIE 安全考试考生。这些操作实验也能帮助安全专业人士满足他们日常工作的需要。因为 CCIE 安全考试包括了路由与交换的内容以及安全的概念和实践，所以本书在开始复习了网络基础知识，而主体部分是更高级的最新技术需求。

本书面向的读者

本书面向的是正在准备 CCIE 安全实验室考试的网络与安全的管理员和工程师。

本书的第二类读者是业界的其他技术人员，比如，有兴趣学习如何配置某项特定安全技术的以及正在寻找如何实现某项安全技术的清晰准确的实例的那些技术人员。

本书有意帮助你评估参加和通过 CCIE 安全实验室考试所要求的技术能力。本书的内容假设你已通过了 CCIE 安全的笔

试，正在准备 CCIE 安全的实验室考试。如果在准备笔试，那么建议你参考有关 CCNA、CCSP 认证的书籍，以掌握更基本的技术概念。

本书的特点

本书主要是为帮助准备 CCIE 安全实验室考试的 CCIE 考生而设计的，给出了一个完整的实验室环境的有条理地逐步扩建过程，在这个环境中，你可以按自己的步调完成最后一章。在每一章都有“案例分析”和“课程”，可在其中实践用于完成最后安全实验室所需的技术与方法。案例分析通常涉及多于一台设备所含的技术。尽管案例分析是设计用于强化一章的主题，但也包含了所有需要的配置，比如 IP 地址分配、路由选择协议，以使案例可运行于网络环境中。在不必要或者不可能采用案例分析时，则采用课程达到同样的目的。这些案例分析和课程的展开形式，是在给出答案之前测试你找出办法和完成解决过程的能力。因为每步都建立在前一步之上，因此强烈建议做完所有案例分析和课程。最后的实验结果就是一个完整的网络安全解决方案。

本书将着重于配置网络和安全所必需的、其级别与在 CCIE 安全实验室考试中见到的相似的配置技能。本书简要地回顾每种技术背后的理论，但本书不应该代替针对每项技术的详细参考书。

每章最后的一节是复习题，帮助你预测是否准备好学习下一章。每章都有一节常见问题解答，简要地说明本章的资料可能适用于网络环境中哪些地方。

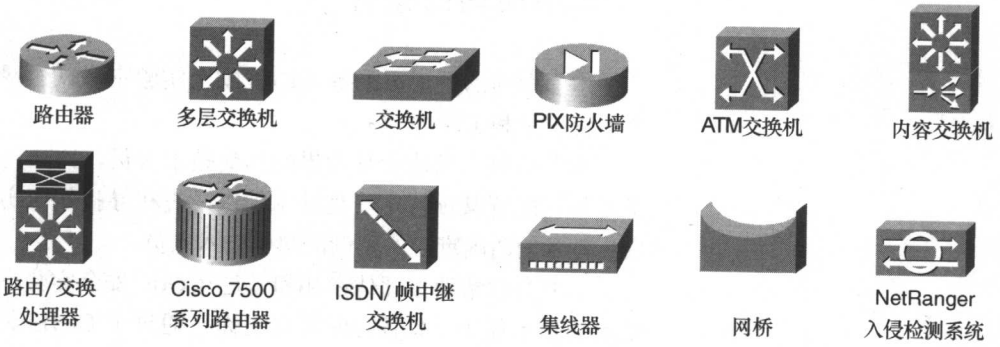
命令语法约定

本书中用于表示命令的语法约定与 IOS 命令参考手册中使用的一样。命令参考手册描述的约定如下：

- 对于互斥的元素用竖线（|）隔开。
- 方括号（[ ]）表示可选元素。
- 必不可少的选项用大括号（{}）括起。
- 对于可选元素中必不可少的选项用（[{}]）括起。
- **粗体**字表示按字面显示输入的命令和关键字。在配置范例和输出中（不是通用命令语法中），粗体字表示用户手工输入的命令。
- 对于你必须提供实际值的参数，用*斜体*表示。

图中使用的设备图标

Cisco 使用下面的标准图标表示不同的网络设备，在本书中可能会见到其中的一些。



本书包含的内容

本书组织成 26 章和 6 个附录。

第 1 章，“CCIE 安全认证计划”——这章概述 CCIE 认证计划，着重介绍安全系列的认证。

第 2 章，“培养 CCIE 观念”——这章介绍开始 CCIE 学习时所持的态度与心理准备，包括学习动机以及结构化学习计划的重要性。这是些在其他图书中常被忽略、但发人深省的内容。

第 3 章，“建立测试实验室”——这章介绍 CCIE 安全考试需要的实验室设备，包括必要的路由器、交换机和安全设备。本章还概述了将要使用的最佳设备和降低实验室开支的方法。建立的这个实验室从此贯穿全书使用。

第 4 章，“第 2 层和第 3 层交换与局域网连接”——本章说明了 Catalyst 3550 交换机的配置。此外，还包括分配虚拟局域网（VLAN）地址，以及将正确的 IP 地址应用到实验室路由器局域网端口上。

第 5 章，“帧中继连接”——本章讲述帧中继的配置及其与 CCIE 安全实验室有关的知识。

第 6 章，“ISDN 连接”——本章讲述 ISDN 的配置，包括基本配置，然后将重点放在诸如身份验证和回叫这些安全方面的说明上。

第 7 章，“ATM 连接”——这章讲述 ATM 的配置。包括 ATM 的概念以及配置 classical IP over ATM 所需的配置步骤。

第 8 章，“RIP”——这章简要地总结 RIP，并将实施一些 RIP 基本配置范例，然后增加相关的安全特征，比如验证。

第 9 章，“EIGRP”——这章简要总结 EIGRP，并介绍配置简单的 EIGRP、EIGRP 选项以及排除 EIGRP 配置中的故障。

第 10 章，“OSPF”——这章简要总结 OSPF，并将实施一些 OSPF 基本配置范例，然后增加相关的安全特征。

第 11 章，“IS-IS”——这章简要总结 IS-IS，并给出配置、监测和调试 IS-IS 的一些例子。

第 12 章，“BGP”——这章简要总结 BGP。本章还包含几个说明 BGP 基本配置和相关安全性的例子。

第 13 章，“重分布”——这章概述重分布，并给出一些基于场景的不同形式的重分布任务范

例。

第 14 章，“安全入门”——这章概要说明安全技术，包括 Cisco IOS 安全以及诸如 VPN、AAA、IDS 等技术的概述。

第 15 章，“Cisco IOS 软件与 Catalyst 3550 系列的基本安全”——这章讲述基本的安全，如密码管理、访问列表和安全外壳（SSH）等。

第 16 章，“访问控制列表”——这章介绍控制列表的选项，包括锁与密钥、反身 ACL 和扩展 ACL 等。

第 17 章，“IP 服务”——这章介绍 IP 协议定义的服务，如配置指示器响应协议（Director Response Protocol，DRP）服务器代理、日志、热备份路由器协议（Hot Standby Router Protocol，HSRP）以及 IP 计账。

第 18 章，“AAA 服务”——这章包含 AAA 服务的配置，以及 RADIUS 与 TACACS+协议的配置。

第 19 章，“虚拟专网”——这章介绍虚拟专网（VPN），着重介绍 IPSec，并给出了 PIX 防火墙和 IOS 路由器上的例子。

第 20 章，“高级虚拟专网”——本章介绍动态多点 VPN（DM VPN），包括多点 GRE、IPSec profile、动态地址的周边路由器以及中心和周边路由器的动态隧道创建。

第 21 章，“虚拟私有拨号专网”——本章包括 VPDN 的基本知识和配置，包括配置带验证的 VPDN 和配置默认的 VPDN 组模板。

第 22 章，“Cisco IOS 防火墙”——本章讲述 Cisco IOS 防火墙，同时还讲述了配置 TCP 拦截、基于上下文访问控制（Context-Based Access Control，CBAC），以及端口到应用的映射（Port-to-Application Mapping，PAM）。

第 23 章，“Cisco PIX 防火墙”——本章讲述配置和监控 Cisco PIX 防火墙。

第 24 章，“Cisco PIX 防火墙和 IOS 软件上的 IDS”——本章考察 PIX 和 IOS 的 IDS，什么时候使用他们以及其缺点。

第 25 章，“Internet 服务提供商的安全服务”——本章内容包含为服务提供商行业所固有的安全事项，包括防止 DoS 攻击的技巧和配置 L2VPN 等。

第 26 章，“实验方案举例”——本章提供 8 个实验室场景的例子。这些场景都基于贯穿本书使用的技术。这些场景模拟了你在 CCIE 安全实验考试中将遇到的一些场景类型。

附录 A，“基本的 UNIX 安全”——这个附录包括基本的 UNIX 安全和在 CCIE 安全实验考试中可能需要的命令。

附录 B，“Windows 的基本安全”——此附录包括基本的 Windows 安全和准备 CCIE 安全实验考试可能需要的技术。

附录 C，“ISDN 错误代码和调试指南”——此信息性的附录给出在排除 ISDN 故障时可作为参考的 ISDN 错误代码。

附录 D，“Cisco IOS、Catalyst OS 和 PIX 上的密码恢复”——密码恢复是必须具备的重要技巧。此附录包括用在 Cisco IOS，Catalyst OS 和 PIX 防火墙上的各种密码恢复方法。

附录 E，“安全相关的 RFC 和出版物”——此附录覆盖了与安全相关的 RFC 和出版物，帮助你学习和成为完全合格的安全 CCIE 的抱负。

附录 F，“复习题答案”——此附录包括各章结束后的复习题的答案。

目　录

第一部分　CCIE 计划与你的实验室环境

第二部分　网络连接

此为试读，需要完整PDF请访问：www.ertongbook.com