Cisco职业认证培训系列
CISCO CAREER CERTIFICATIONS

Official Cert Guide

Learn, prepare, and practice for exam success

CCNP安全防火墙642-618认证考试指南

- 掌握CCNP安全防火墙642-618考试主题；
- 使用测试题评估各章知识的掌握情况；
- 通过备考任务复习关键概念；
- 利用CD-ROM中的模拟试题进行练习。

〔美〕 David Hucaby, CCIE #4594
Dave Garneau 著
Anthony Sequeira, CCIE #15626
罗洋, CCIE #25318 译

人民邮电出版社
POSTS & TELECOM PRESS

ciscopress.com

Cisco职业认证培训系列
CISCO CAREER CERTIFICATIONS

CCNP安全防火墙642-618认证考试指南

David Hucaby, CCIE #4594
〔美〕 **Dave Garneau** 著
Anthony Sequeira, CCIE #15626
罗洋, CCIE #25318 译

人民邮电出版社
北京

图书在版编目（CIP）数据

CCNP安全防火墙642-618认证考试指南 / （美）胡卡比（Hucaby,D.），（美）加诺（Garneau,D.），（美）塞凯拉（Sequeira,A.）著；罗洋译. -- 北京：人民邮电出版社，2013.2
ISBN 978-7-115-30797-2

Ⅰ. ①C… Ⅱ. ①胡… ②加… ③塞… ④罗… Ⅲ. ①计算机网络－安全技术－工程技术人员－资格考试－自学参考资料 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2013)第008801号

CCNP 安全防火墙 642-618 认证考试指南

◆ 著 [美] David Hucaby, CCIE #4594 Dave Garneau
Anthony Sequeira, CCIE #15626
译 罗 洋 CCIE #25318
责任编辑 傅道坤

◆ 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 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：46.75
字数：1 098 千字 2013 年 2 月第 1 版
印数：1－3 000 册 2013 年 2 月北京第 1 次印刷
著作权合同登记号 图字：01-2012-7081 号
ISBN 978-7-115-30797-2

定价：118.00 元（附光盘）

读者服务热线：(010)67132692 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

本书是根据 Cisco 最新推出的 CCNP 安全防火墙 642-618 认证考试纲要编写的考试指南。全书分为 17 章和 2 个附录，包括 Cisco ASA 安全设备概述及互操作方式；在 ASA 上配置 IP 路由、设备管理、系统日志；高级安全特性，包括 NAT 地址转换、访问控制、流量检测、代理服务、流量处理、透明防火墙、虚拟防火墙以及高可用性；ASA 设备服务模块介绍和常用流量分析工具。本书包含了大量的配置实例，并对 CLI 命令行和 ASDM 图形化界面分别进行详细阐述，有助于读者掌握配置方式和排错技巧。每章末尾的考试要点总结能够帮助读者快速了解本章内容。

本书深入翔实地讨论了与 CCNP 安全防火墙考试相关的主题，能够帮助读者更好地备考 CCNP 安全认证考试。同时，从事网络安全工作的工程师、网络维护人员也可以从中受益。

关于作者

David Hucaby，CCIE #4594，是肯塔基大学的一名网络架构师，致力于以 Cisco Catalyst 交换机、ASA、FWSM 以及统一无线网络产品线为基础的网络维护。David 持有肯塔基大学电子工程专业的学士和硕士学位，他还为 Cisco Press 撰写过多本图书，其中包括《Cisco ASA，PIX，and FWSM Firewall Handbook，Second Edition》、《Cisco Firewall Video Mentor》、《Cisco LAN Switching Video Mentor》和《CCNP SWITCH Exam Certification Guide》。

David 现在与妻子 Marci 和两个女儿居住在肯塔基。

Dave Garneau，是 Rackspace Hosting 公司网络安全团队的一名高级成员。在此之前，他是 Radix Group 公司的首席顾问和高级技术讲师，曾经在 9 个国家为 3000 多名学生讲授 Cisco 技术，内容主要涉及 Cisco 安全产品线，他还与 Cisco 公司紧密合作，建立了最新的 CCNP 安全课程。Dave 持有丹佛大都会州立学院的数学学士学位。Dave 现在与妻子 Vicki 以及两个刚出生的女儿 Elise 和 Lauren 居住在得克萨斯州的圣安东尼奥市。

Anthony Sequeira，CCIE #15626，是一名 Cisco 认证讲师。Anthony 于 1994 年在佛罗里达州的坦帕市就职于 IBM，由此开始了他的信息技术职业生涯。不久之后，他成立了自己的计算机咨询公司 Computer Solutions，并热衷于 Microsoft 和 Cisco 技术的培训以及技术撰稿。Anthony 在 1996 年加入 Mastering Computers 公司，在全球为大量学生培训最新的计算机技术。Mastering Computers 公司随后成为一家革命性的在线培训公司——KnowledgeNet。Anthony 为该公司服务多年。当前，Anthony 正在准备考取安全方向的 CCIE 认证，他现在还是下一代 KnowledgeNet（即 StormWind Live）的全职讲师。Anthony 还是 VMwave 认证专家。

关于技术审稿人

Doug McKillip，CCIE #1851，是一名独立的咨询师，专注于与 Cisco 培训合作伙伴 Global Knowledge 公司相关的 Cisco 认证培训。他在计算机网络和安全领域有 20 多年的从业经历。在 MCNS（多媒体电缆网络系统）1.0 版本的最初部署期间，McKillip 提供了技术指导和援助。而 MCNS 1.0 版本也是第一个 Cisco 安全培训课程，该课程早在 1998 年上线。从那时起，Doug 逐渐成长为一名安全课程的杰出讲师。Doug 通过为 Global Knowledge 编写大量的安全排错白皮书和安全日志来补充它的培训课程。他持有 MIT 化学工程专业的学士学位和硕士学位，同时还持有特拉华大学计算机和信息科学专业的硕士学位。目前 Doug 居住在特拉华州的威尔明顿市。

Kenny Hackworth，是 Rackspace Hosting 公司的一名网络自动化高级工程师，该公司是云计算服务的翘楚。他当前的专长包括为内容交换产品（Cisco CSS 和 F5 LTM）和安全设备（Cisco 和 Juniper 防火墙）提供支持。他当前的研究重点是自动化技术，尤其是配置更变和设备部署。在加入 Rackspace 公司之前，Kenny 曾经为空军情报局效力，为 NSA（美国国家安全局）提供支持，负责执行数字网络漏洞分析和密码分析等工作。

献辞

一如既往，本书献给我生命中最重要的人：我的妻子 Marci，我的两个女儿 Lauren 和 Kara。她们的关爱、支持和鼓励伴我一路前行。感谢上帝，赋予我忍耐和勇气，才使得我完成本书的编写。

——David Hucaby

我也要将本书献给我生命中最重要的人：我的妻子 Vicki，我的女儿 Elise 和 Lauren，以及我的继子 Ben。没有他们的关爱和支持，就没有我努力地坚持，更不用说完成本书的写作了。此外，我还要将本书献给我的母亲 Marian。40 年以前，她的儿子曾经说过："等我长大，我要编写一本图书"，她对此坚信不疑。如今，我非常高兴终于兑现了我的诺言。

——Dave Garneau

本书献给我过去几十年以来教过的众多学生们。希望通过本书，能传达我对技术和学习的热情，让你们有所感悟。

——Anthony Sequeira

致谢

很荣幸能够再次参与到 Cisco 图书的编写工作中。我热衷于网络领域，而且尤其热爱技术写作。更重要的是，非常感谢上帝带给我的快乐和内在的安宁，让世间万物如此美丽珍贵。

我为 Cisco Press 写作图书已经有 10 年之久，虽然图书写作工作困难耗时，但是我仍然能够从中获得快乐。因此，我非常感谢 Dave Garneau 和 Anthony Sequeira 给予的帮助。此外，能够与 Brett Bartow 和 Chris Cleveland 共事是我的荣幸。感谢你们的耐心，特别是我拖延交稿日期的时候。

我还要衷心感谢本书技术审稿人提出的意见和建议，正是这些宝贵的意见，才让本书更加完善，也让我受益匪浅。

——David Hucaby

本书的编写是一项繁杂困难的工作，最初，我是打算作为本书的技术审稿人参与本书的编写工作，但是由于 David Hucaby 的邀请，我才以作者的身份最终参与到了本书的编写。就在我刚接受这个挑战不久，我就换了份新工作，搬到了新的城市并住进了新家，这一切新改变都让我焦头烂额。但正是 Brett Bartow 和 Christopher Cleveland 让我学会了忍耐，我才得以继续本书的编写工作。在此，向他们两位表示感谢，希望他们的耐心没有全部用尽，我期待着能够和他们在下一次的工作中共事。

我还要感谢技术审稿人，他们对待细节一丝不苟的态度让我钦佩。作为技术审稿人的 Doug McKillip 和 Kenny Hackworth，都是我亲密的挚友，他们给了我很多帮助。正是 Doug 和 Kenny 严谨的作风，才使得本书能够以更好的面貌和读者出现。

——Dave Garneau

感谢我的挚友 Brett Bartow，谢谢他帮助我获得如此珍贵的机会，让我可以参与 Cisco 图书的编写工作。同时，我还要谢谢他邀请我加入他所在的棒球联盟。

能够与 David Hucaby 和 Dave Garneau 共同编写本书，我感到无比荣幸。正是他们的无私，我才获得了编写本书的机会，并成为本书的第 3 位作者。

需要重点提及的是，为了本书的编写工作，David Hucaby 为我提供了访问最新的 Cisco ASA 设备的机会，对此我表示感谢。

最后，谢谢我的家人 Joette 和 Annabella，以及爱犬 Sweetie，谢谢你们对我长期伏案于电脑前不停工作的理解。另外，我还要感谢我的脊椎按摩师 Paton 医生给予的帮助。

——Anthony Sequeira

译者序

非常荣幸能够为人民邮电出版社翻译本书，同时这也是我第一次以译者身份完成一整本书系统的翻译和审校工作。本书作为 Cisco CCNP 安全认证系列书籍中的一本，着力为读者介绍了 Cisco ASA 设备及其所具备的大量安全特性。构建一个网络就如同建设一座城市，但想要使得其次序井然地运行，离不开方方面面的安全规范。现如今，网络安全技术已经越发热门，甚至于可以概括为一句话：存在网络的地方，必然需要安全。如果你仅仅是一名初学者，那么在选择本书之前需要谨慎，因为在尚未掌握基本网络构建技术的前提下去学习网络安全技术是很困难的。译者推荐读者应当在学习过 CCNA、CCNP 之后，再开始网络安全领域的学习，切勿急于求成。掌握和理解防火墙技术，将帮助读者在以后的工作中更好地完成相关的任务。

本书使用了大量篇幅阐述如何在 ASDM 中管理和配置防火墙。相比 CLI 命令行，ASDM 能够为管理员提供更为直观的 GUI 界面。在配置某些特性，特别是对防火墙进行验证和故障排除时，使用 ASDM 将显得非常方便和快捷。

学习防火墙的关键，是掌握防火墙内在的安全视角以及各种安全策略的本质。由于防火墙所涉及的技术内容相对较多，非常容易造成读者思路混乱，最终得不到最好的学习效果。因此，非常有必要对每项技术特性进行分类，并梳理清晰的知识体系。当然这种学习方式不仅限于防火墙，对于其他知识的学习也非常具有帮助。

不得不谈到的是，Cisco 在 2012 年 5 月底升级了 CCNP 安全认证中的防火墙和 VPN 考试。就本书而言，从原本的 642-617 升级到了 642-618，这使得本人需要对已经完成的翻译内容进行核对更新。在新版考试大纲中，更加明确了防火墙考试的内容，对某些特性和技术进行了更新。尤其是本书第 7 章所论述的 NAT 技术，两版认证书籍在内容上存在非常大的不同，望读者予以重视。

本书的翻译及审校工作由本人独立完成，但在此期间，离不开各位关心我的朋友的支持和帮助。翻译一本书是一项耗时耗力的工作，需要经常熬夜，斟字酌句；也需要反复阅读，多次修改。由于原书是由三位作者共同编写完成，导致某些章节的语法使用、描述习惯都存在很大不同。因此本人尽量在翻译中消除这些差异，以更为统一地形式展现书本内容。

翻译此类技术书籍是一项挑战。不仅要求对书中所涉及的技术内容进行准确地描述，还应当符合中文叙述和说明的习惯。因此对比原书，本书在内容和字句上进行了较大的调整。由于本人中文表达能力有限，无法完全中文式地将本书翻译成品，但在描述内容上，力争做到通顺清晰。另外，本书涉及知识面较广，加之本人技术水平有限，译文中难免存在不当之处，敬请读者谅解。如果读者对本书译文存在异议，可以通过邮件与本人交流，以求共同进步。

不管如何，本书最终的面世才未枉费之前付出的所有心血。本人同时也希望谨以本书为载体，向读者传递作者以及译者的初衷，特别是除了技术知识以外的其他东西。

致谢

首先，我要感谢一直关注本书出版的所有朋友，正是你们的支持和鼓励，才使得我有勇气和毅力完成本书的翻译。

感谢 56cto 论坛的代工（红盟过客）对译文的校审。翻译期间，他如同一位亲切的大哥对我给予了很大的帮助。感谢人民邮电出版社的幕后工作人员对我的支持和肯定，特别是傅道坤大哥长期在翻译工作上对我的提醒和敲打，促使我不断进步。感谢我亲爱的同学，是你们在我百忙之中能够友情地帮助我对本书进行试读校对，你们所标注的一笔一划都是友谊的见证。感谢我的父母长期对我生活和工作的关心，儿子已然长大，还请你们放心，保重身体。

最后，我还要感谢一直在我身边支持我的人，感谢你的体谅和关心。若你不蹙眉，便是我所求。

罗洋

feierly@vip.qq.com

2012 年 7 月于成都

本书图标使用说明


Cisco ASA
设备

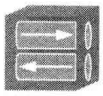

入侵防御系统


内容安全服务模块


AAA 服务器

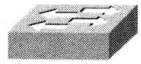

证书管理机构


SSL VPN
网关


IPSec VPN
网关


路由器


三层交换机

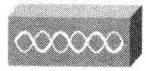

二层交换机


PC


IP 电话


服务器


网络云


接入点


无线连接

以太网连接

前言

本书将帮助你准备 Cisco 防火墙 642-618 认证考试。防火墙考试是获得 CCNP 安全认证必经的一系列考试中的一门。本门考试主要侧重于与 Cisco ASA 设备相关的安全策略的应用。

本书读者对象

网络安全是极其复杂的。在开始应用安全策略之前，你需要对计算机网络具有大量而且深入的操作经验。Cisco 防火墙课程旨在介绍 ASA 安全产品，解释 ASA 设备如何工作，以及阐述如何利用 ASA 设备应对网络中日益增长的安全威胁。防火墙课程是为网络管理员、网络安全管理员、网络构架师以及打算在自己的网络中应用安全策略的网络从业人员准备的。

本书内容结构

本书共包含 17 章，章节内容相互关联且循序渐进。本书每章包含的实例或配置操作都可以在命令行接口（CLI）和 Cisco 自适应安全设备管理器（ASDM）上进行实施。

本书涵盖以下主题。

- **第 1 章，“Cisco ASA 设备概述”**：讨论网络安全和流量过滤策略的基本概念，同时介绍了 Cisco ASA 设备概况，其中包括 ASA 特性集、产品许可，以及如何针对不同网络环境的安全需求选择 ASA 设备型号。
- **第 2 章，“使用 ASA 设备”**：介绍用来与 ASA 设备进行交互，以及控制 ASA 设置基本操作的方法，其中讨论了 CLI 和 ASDM 两种方法。
- **第 3 章，“配置 ASA 设备接口”**：解释如何配置 ASA 设备接口运行于网络时所需的参数。
- **第 4 章，“配置 IP 连通性”**：涵盖 ASA 设备通过 DHCP 获取 IP 地址，以及利用多种动态路由协议来交换路由信息的 ASA 特性。
- **第 5 章，“管理 ASA 设备”**：介绍对 ASA 设备进行本地或远程管理控制所需的配置命令及工具。
- **第 6 章，“记录 ASA 设备行为”**：阐述如何配置 ASA 设备，使之产生可被收集和分析的日志信息。日志信息可提供对网络和安全行为的审计跟踪。
- **第 7 章，“地址转换”**：讨论当数据包穿越 ASA 设备时，如何对数据包内的 IP 地址进行更变或转换，其中涉及各种不同类型的网络地址转换及端口地址转换（PAT）。本章讲解了在防火墙 OS 版本 8.3 之前和之后的地址转换方法，注意，OS 版本 8.3 之后的转换配置已经完全不同于之前。
- **第 8 章，“穿越 ASA 设备的控制访问”**：介绍访问控制列表和主机规避（host shunning），并利用上述特性对穿越 ASA 设备的流量行为进行控制。

- **第 9 章，“流量检测”**：讲解了模块化策略框架（MPF），这是一种用来定义和实施不同类型的流量检测策略的方法。此外还讲解了 ICMP、UDP、TCP 和应用协议检测引擎，以及其他高级检测工具，比如在僵尸网络中的流量过滤和威胁检测等。
- **第 10 章，“使用代理服务来控制访问”**：讨论当用户流量穿越 ASA 设备时，利用认证、授权和审计的管理方式对其进行控制。
- **第 11 章，“流量处理”**：讲解用于处理分段流量、QoS 优先流量、流量限速及流量整形的功能和方法。
- **第 12 章，“透明防火墙模式”**：介绍了透明防火墙模式。当网络中引入了 ASA 设备时，可以使用透明防火墙模式来藏匿 ASA 设备。ASA 设备充当的是透明网桥，在第 2 层进行流量转发。
- **第 13 章，“在 ASA 设备上创建虚拟防火墙”**：讨论在单台物理 ASA 设备上使用 Multiple Context 模式来提供多个虚拟防火墙或者 Security Context。
- **第 14 章，“配置高可用性”**：介绍用来在一对 ASA 之间实施高可用性的两种策略。
- **第 15 章，“整合 ASA 设备服务模块”**：介绍在 ASA 设备上配置 AIP 和 CSC 安全服务模块（SSM）的步骤。上述两种模块分别提供深度入侵防御和内容检测的功能。
- **第 16 章，“流量分析工具”**：介绍了用于测试和分析穿越 ASA 设备的数据包的两种故障排除工具。
- **第 17 章，“最后冲刺”**：在完成了本书之前所有章节的学习后，本章总结了对考试有用的相关工具，并提出了建议的学习计划。
- **附录 A，“‘我已经知道了吗’测试题答案”**：给出在每章开头“我已经知道了吗？”测试题的答案。
- **附录 B，“CCNP 安全防火墙 642-618 考试更新：版本 1.0”**：如果 Cisco 对编写本书所参考的考试大纲进行少量更新，那么本附录旨在帮助你获取这些更新内容。如果 Cisco 对考试内容完全改革，本附录则无法涵盖所有变化内容。那时，你将需要参考配套的新版认证书籍。更新的考试内容将会以 PDF 文件形式发布在与本书相关的网站上：www.ciscopress.com/title/9781587142710。
- **术语表**：定义了出现在每章末尾的术语，能够正确解释这些术语将有助于备考。

本书每章都包含如下内容帮助你进行自我评估，并强化章节重点。

- **“我已经知道了吗？”测试题**：每章开头的一系列测试题将帮助你测试对于本章内容的熟悉程度。这些测试题根据章节重点进行划分，有助于你了解在学习本章时应该重点关注的地方。
- **基本主题**：作为每章的核心小节，基本主题部分给出了备考所需要掌握的协议、概念及技能。
- **备考任务**：在每章末尾，备考任务罗列了本章的关键主题。同时，还给出了备考所需掌握的关键术语。不推荐为了认证考试而只关注本节所给出的关键主题和关

键术语，但本节确实能够在最后备考冲刺阶段为你提供帮助。

- **测试对命令的记忆情况**：每章末尾使用表格总结了该章涉及的相关命令。当进行配置时，请注意给出的命令、语法、顺序及参数的使用方式。
- **CD 光盘上的考试练习**：本书配套的 CD 光盘上包含了一些交互式的考试练习。推荐使用这些练习进行考试前的自我测试。利用这些测试，你将熟悉最终的考试形式并提高技能熟练程度。需要提醒的是，真正考试中的问题可能无法预测。因此，你不能只是简单地着眼于“记得”每个可能的答案，而应该通过扎实地学习来掌握课程重点，从而在考试中能够应对自如。

认证考试和备考指南

认证考试的考试试题都是保密的，即使你提前获知了考试内容并因此通过考试，那么当你在工作中遇到需要使用考试中必须掌握的技巧时，你将会一筹莫展。因此，应该把注意力集中到努力掌握重要的知识点，而不是一心只为了通过考试。

通过查阅发布在 Cisco Learning Network 上的“642-618 Deploying Cisco ASA Firewall Solutions Exam Topics (Blueprint)”可以获知想要通过考试必须掌握的内容。表 I-1 罗列出了防火墙 v2.0 考试要点，并且指出了相关内容位于书本的何处。在真实环境下，当你配置 Cisco ASA 设备时，以下要点也是必须掌握的。

表 I-1　　FIREWALL v2.0 考试要点和所在的章节

考试要点	所在的章节
ASA 基本配置	
熟悉 ASA 产品系列	第 1、15 章
操作 ASA 许可	第 1 章
管理 ASA 启动过程	第 2 章
操作 ASA 接口设置	第 3、8 章
实施 ASA 管理特性	第 2、4、5、6、16 章
实施 ASA 访问控制特性	第 8、10 章
在 ASA 上执行 NAT	第 7 章
实施 ASDM 公共服务器特性	第 2 章
操作 ASA QoS 设置	第 11 章
实施 ASA 透明防火墙	第 12 章
ASA 路由特性	
配置 ASA 静态路由	第 4 章
配置 ASA 动态路由	第 4 章
ASA 检测策略	
实施 ASA 检测特性	第 9 章

续表

考试要点	所在的章节
ASA 高级网络保护	
实施 ASA 僵尸网络流量过滤	第 9 章
ASA 高可用性	
实施 ASA 接口冗余和负载共享特性	第 3 章
实施 ASA 虚拟化特性	第 13 章
实施 ASA 有状态故障倒换	第 14 章

注意，并非所有的章节都会与特定的考试主题相关联。每一版的认证考试所强调的功能和特性并不相同，而有一些考试主题则显得比较宽泛。本书旨在帮助读者准确地抓住考试要点，因此，本书包含了不同版本的考试（新版和旧版）中所有可能出现的考试要点。虽然某些章节并不涉及考试主题，但却有助于读者更好地理解网络安全的相关概念。当然，你可能只是想要通过考试，但将来，你可能会为了成为合格的网络安全工程师而努力。

同样重要的是，本书提供的参考相对而言只是“静态”的，而考试主题却是动态变化的，原因是 Cisco 经常对认证考试的内容进行更新。

在准备认证考试时，除了将本书用作参考资料之外，读者还可以在 Cisco.com 上找到大量的与考试主题相关的详细资料。由于本书的目的是尽可能地帮助读者备考防火墙考试，因此对于某些主题的内容，将原本近 600 页的配置指南浓缩到 30 页的章节内容中，以便于读者掌握。如果读者需要查阅关于某些主题的详细信息，则应该阅读与这些主题相关的 Cisco 文档。

注意，由于安全威胁和防护措施的不断发展，Cisco 将保留更改考试主题而无需提前声明的权力。尽管上文中的表 I-1 给出了相应的考试主题，但一定确保在考试前通过 Cisco.com 获取了最新的考试主题。通过访问 Cisco.com 站点，在 Training & Events 下选择认证列表，能够查阅到目前 Cisco 认证考试体系中的所有考试主题。另外，Cisco Press 可能会针对本书发布更新的参考内容，具体请浏览 www.ciscopress.com/title/9781587142710。建议在考前定期检查更新内容。

认证准备

目前，网络安全方向缺乏大量的优秀工程师。因此，许多工程师考虑将学习方向从路由/交换调整到网络安全。要知道，“网络安全”仅仅只是关注“网络”上的“安全”，这听起来毋庸置疑。但实际上，在你准备 CCNP 安全认证，部署网络安全特性之前，必须具备基本的网络路由与交换知识。所以，建议在学习网络安全之前，首先达到 CCNA 或 CCNP 的相关技能要求。

参加防火墙认证考试

和其他 Cisco 认证考试一样，你需要在考前全身心地投入。由于无法准确获知考题，因此最佳的方式便是能够掌握考试相关的所有主题。安排好你的时间表，在考前好好休息，保证以充足的精力参加最后的考试。

关于 Cisco 培训和认证的最新信息，可以查阅 Cisco.com 站点上的 Training & Events 页面。

追踪认证状态

通过登录 www.cisco.com/go/certifications/，可以查询到自己的认证状态。如果你是第一次登录，则需要创建一个账号。

如何准备考试

准备任何认证考试的最佳方法是，尽量将备考资料和实际动手操作相结合。本书中给出了一些练习测试及实例情景，有助于读者更好地备考。如果可能，尽可能在 Cisco ASA 设备上进行实际操作，以获得真实的操作经验。如果通过真实的 ASA 设备进行实验操作，对于命令和概念的理解将会事半功倍。

Cisco.com 提供了大量与 ASA 设备及其软件和特性相关的宝贵信息，但任何单一的信息源都不足以完全应付防火墙考试，除非你对 Cisco 产品已经拥有大量的操作经验，并且具有网络或网络安全背景。但是在最低程度上，你可以使用本书并结合 Support and Download 页面提供的资源（www.cisco.com/cisco/web/support/index.html）来准备考试。

评估考前准备

备考人员往往在考试真正开始后才发觉自己准备得不够充分，但这为时已晚。因此，建议使用每章开头的“我已经知道了吗？”测试题，浏览了解每章的考试要点，并复习每章最后的命令来评估自己的准备状态。你需要循序渐进地耐心学习，除非你能够轻松完成上述要求。

真正的 Cisco 安全专家

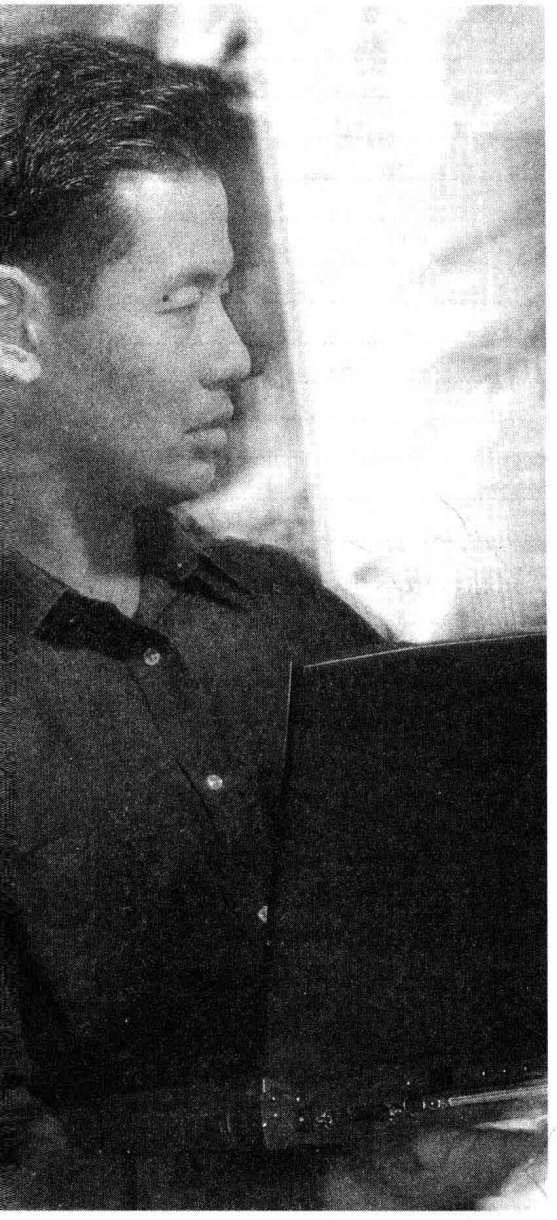
Cisco 公司在 Internet 领域具有很高的权威性。真正的 Cisco 认证安全专家需要掌握大量的知识，因为他们对于网络和网络安全具有相当深刻的理解。所以，Cisco 认证体系赢得了广泛的尊重。Cisco 认证体系对认证人员的专业技能及态度提出了很高的要求，因此 Cisco 认证具备很高的含金量。

考试注册

防火墙考试使用上机考试形式，需要完成 60~70 个题目，其中题型可能包括多选题、填空题、排序题或仿真模拟题。你可以选择在任何 Pearson VUE（www.personvue.com）考试中心进行考试。考试时间大约是 90 分钟，但当读者进行考试注册时，可能会被告之考试时间能够被适当延长，这主要是为了确保你能够适应考试环境以及学会如何正确使用考试设备。

书本内容更新

Cisco 可能会对考试主题进行更新，且不进行提前通知。因此，Cisco Press 将会在本书相关站点上发布更新的内容，读者可以访问 www.ciscopress.com/title/9781587142710 进行查阅。建议读者养成考前定期查阅上述站点的好习惯，从而及时发现更新的内容。同时建议读者定期查阅 Cisco Press 发布的本书勘误表或其他支持文件。



本章涵盖以下主题：

- **防火墙概述**：概述如何通过构建安全域和部署防火墙来保护网络。
- **防火墙技术**：阐述各种防火墙防护形式及网络安全工具。
- **Cisco ASA 特性**：涵盖 Cisco ASA 设备提供的大量安全特性。
- **选择 ASA 设备型号**：介绍各种 ASA 产品型号的规格特性，通过这些信息来对设备型号做出正确的选择。
- **选择 ASA 设备许可**：具备许可文件的 ASA 设备才能有效地保证网络安全。本节介绍各种特性许可及如何基于不同 ASA 平台进行许可选择。