Cisco职业认证培训系列
CISCO CAREER CERTIFICATIONS

Official Cert Guide

Learn, prepare, and practice for exam success

CCNA安全640-554认证考试指南

- 掌握CCNA安全640-554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；
- 用CD-ROM中的模拟试题进行练习；
- 通过90分钟的培训视频进行学习。

〔美〕 **Keith Barker,** CCIE #6783 著
Scott Morris, CCIE #4713
YESLAB工作室 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

CCNA安全640-554
认证考试指南

〔美〕**Keith Barker,** CCIE #6783 著
Scott Morris, CCIE #4713
YESLAB工作室 译

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

CCNA安全640-554认证考试指南 /（美）巴克尔(Barker,K.)，（美）莫里斯（Morris,S.）著；YESLAB工作室译. -- 北京：人民邮电出版社，2014.8
ISBN 978-7-115-35935-3

Ⅰ. ①C… Ⅱ. ①巴… ②莫… ③Y… Ⅲ. ①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. ①TP393.08

中国版本图书馆CIP数据核字(2014)第127333号

版 权 声 明

◆ 著 [美] Keith Barker Scott Morris
译 YESLAB 工作室
责任编辑 傅道坤
责任印制 彭志环 焦志炜

◆ 人民邮电出版社出版发行 北京市丰台区成寿市路 11 号
邮编 100064 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
三河市潮河印业有限公司印刷

◆ 开本：800×1000 1/16
印张：33
字数：768 千字 2014 年 8 月第 1 版
印数：1－3 000 册 2014 年 8 月河北第 1 次印刷

著作权合同登记号 图字：01-2013-8476 号

定价：89.00 元（附光盘）

读者服务热线：(010)81055410 印装质量热线：(010)81055316
反盗版热线：(010)81055315

YESLAB 工作室简介

作为执国内高端 IT 培训之牛耳的企业，YESLAB 多年来深感本土图书数量的缺位、引进作品质量的参差。

有鉴于知识分享始终是 YESLAB 不变的追求，YESLAB 甘愿在培训市场之外，通过书作向华语同仁公开自己对 IT 的解读，以鼎精英之智，以传技术之功，以飨万千读者。

YESLAB 工作室应运而生，这是北京鼎智传承科技有限公司服务于技术读者的机构，旨在与人民邮电出版社就 IT 技术类专业图书的翻译和创作工作展开深入合作，践行“鼎智传承”之宗旨。

YESLAB 工作室的译作均由拥有大量译作的业内专家执笔，同时由 YESLAB 高级讲师和学员共同参与和审稿，尽一切可能为读者带来原汁原味的技术阅读体验。

YESLAB 工作室创作的本土化图书，全部是老余、现任明教教主、阿彭等技术精英；孙晨、戴鑫、闫斌等后起之秀的心血结晶，经由专长于写作的业内人士执笔润色，旨在让读者通过阅读，在事业上百尺竿头更进一步。

除了与人民邮电出版社深入合作之外，YESLAB 工作室还会与国内高校合作，陆续推出以校企合作为目标而定制的供高校师生使用的国家高校教材。

YESLAB 工作室期待能够在未来不断与各类高校和企业开展合作，一道创作更多佳品，为华语技术图书贡献力量。我们更加期待着能够参与本土华语技术图书的对外输出工作，让华人在全球技术领域发出自己的声音。

内容提要

本书是 Cisco IINSv2（640-554）认证考试的官方认证指南，主要内容包括网络安全的概念、使用生命周期的方式来理解安全策略、建立安全战略、网络基础保护、使用 Cisco 配置专家（CCP）来保护网络架构、在 Cisco IOS 设备上保护管理层、使用 IOS 和 ACS 服务器实施 AAA、保护二层技术、在 IPv6 环境中保护数据层、规划威胁控制战略、使用访问控制列表来缓解网络威胁；理解防火墙的基础概念、实施 Cisco IOS 基于区域的防火墙、在 Cisco ASA 上配置基本防火墙策略、Cisco IPS/IDS 基础、实施基于 IOS 的 IPS、VPN 技术基础、理解 PKI 基础、IP 安全基础，实施 IPSec 站点到站点 VPN、使用 Cisco ASA 实现 SSL VPN 等，为广大备考人员提供了详实的学习资料。为便于读者深入掌握各章所学的知识，本书提供了大量的案例分析材料，并且在各章提供了测验题和复习题，以加强读者对所学知识的记忆和理解。

本书主要面向备考 Cisco IINSv2（640-554）的考生，全书紧密围绕考试主题，在内容的组织和编写上切实凸显了认证考试需求。此外，本书也非常适合从事网络安全的工程技术人员及网络管理员参考。

关于作者

Keith Barker，CCIE #6783（路由交换和安全），在网络互联领域拥有 27 年资深工作经验。目前，他就职于 Copper River IT 公司，担任网络工程师和培训师的职务；他曾经就职于 EDS、Blue Cross、Paramount Pictures 和 KnowledgeNet，并在过去的几年中教授过 CCIE 级别的培训课程。作为 Cisco Learning Network 最早的 Cisco VIP，他目前仍在以多种方式为其提供服务。他拥有 CISSP 和 CCSI 证书，热衷于授课和分享教学视频。读者可以在网站 http://www.youtube.com/keith6783 观看到许多他录制的视频；也可以通过邮箱 Keith.Barker@CopperRiverIT.com，或通过访问 http://www.CopperRiverIT.com 来与他取得联系。

Scott Morris，CCIE #4713（路由交换、ISP/拨号、安全和 SP），在网络互联领域拥有 25 年的丰富经验。他还拥有 CCDE 及众多其他认证，其中包括四大主要厂商的 9 项专家级认证。他曾旅居世界各地，为不同企业和运营商提供咨询；目前，Scott 是 Copper River IT 公司的首席技术专家。他也为 Cisco 公司和其他技术厂商提供 CCIE 级别的培训和技术培训课程。他的“前半生”（事业起步期）是一名摄影记者，从一个完全不同的领域跨入 IT 行业使他产生出了许多有趣的观点。作为 Cisco Learning Network 最早的 Cisco VIP，他目前仍在以多种方式为其提供服务。读者可以通过邮箱 smorris@CopperRiverIT.com，或通过访问 http://www.CopperRiverIT.com 与他取得联系。

关于合著者

Kevin Wallace，CCIE #7945，Cisco 认证讲师，拥有多项 Cisco 认证，其中包括 CCSP、CCVP、CCNP 和 CCDP。他于 1989 年开始接触 Cisco 技术，曾作为网络设计专家就职于迪斯尼世界渡假村，作为高级技术讲师就职于 SkillSoft、Thomson NETg 和 KnowledgeNet，作为网络管理员就职于东肯塔基大学。Kevin 拥有肯塔基大学的电子工程理学学士学位，他还是 Cisco Press 出版的多本书籍的作者和合著者，其中包括：*CCNP TSHOOT 642-832 Cert Kit*、*CCNP TSHOOT 642-832 Official Certification Guide*、*CCNP ROUTE 642-902 Cert Kit* 和 *CCNP Routing and Switching Official Certification Library*，所有这些书籍都是面向当前的 CCNP 认证考试。

Michael Watkins，CCNA/CCNP/CCVP/CCSP，就职于 SkillSoft 的全职高级技术讲师，拥有 12 年网络管理、培训和咨询经验。Michael 曾就职于卡夫食品、强生公司、雷神公司和美国空军，帮助这些机构实施并学习最新的网络技术。除了拥有网络互联和编程技术领域的 20 多项认证之外，他还拥有瓦巴什学院的文学学士学位。

关于技术审稿人

Brandon Anastasoff，自 2007 年 10 月以来一直在 Cisco 公司担任系统工程师。此前，他的工作是在一家知名的报纸出版公司担任首席网络架构师。他在网络技术领域拥有 20 年以上的工作经验。最近 10 年，他一直专注于安全领域，并在 Cisco 内部以及 Cisco 之外获得了许多认证证书，其中包括 CISSP 和 CCSP，以及刚刚考取的 CCIE 安全认证证书。在英国学习期间，Brandon 曾休学一年前往沙特阿拉伯，希望能够在继续学业之前看一看真正的工作环境。在赴沙特阿拉伯期间，他没有经受住高薪的诱惑，自此进入了职场，再也没有继续他的学业。Brandon 在他职业生涯的早期面临一项艰难的抉择：是继续从事电脑动画美术行业，还是转而投身于炙手可热的 PC 网络大潮当中。对于选择进入网络技术领域，他从未感到后悔。他的工作领域从早期的 Windows 和苹果操作系统，转变为 Novell 的 NetWare，而后又开始转入网络设备（主要是 Cisco 的 LAN/WAN 设备）的配置。进入 21 世纪后，Brandon 的工作领域又逐渐转变为网络安全方向，因此他也开始对病毒、特洛伊木马以及法证调查等内容变得越来越熟悉。目前，Brandon 对他的现状非常满意，并会不失时机地向别人介绍网络安全技术。

David Burns，对路由交换技术、网络安全技术及移动技术有深入的了解。目前，他在 Cisco 公司担任系统工程经理，业务遍及美国多家服务提供商企业。2008 年 7 月，David 作为一名高级系统工程师加入了 Cisco 公司，它的工作内容包括为一家在美国的移动服务提供商建立飞蜂窝（Femtocell）、数据中心、MTSO 及安全网络架构等。他此前任职于一家总部位于美国的大型线缆公司，并在那里担任高级网络工程师和高级安全设计工程师。David 拥有 10 年以上的工作经验，在加盟 Cisco 之前，他曾经担任过多项工作，包括 SP 的实施、管理和设计，管理美国军方情报通信系统等。他拥有多项销售和工程/Cisco 技术认证，包括 CISSP、CCSP、CCDP，以及两项助理级的认证。David 刚刚通过了 CCIE 安全的笔试考试，目前正在备考 CCIE 安全实验考试。David 是知识分享的大力倡导者，也是网络技术（特别是网络安全技术）的热衷者。他曾在 Cisco Live 发表过关于飞蜂窝（移动技术）和 IPS（安全技术）等技术的演讲。Dave 在佐治亚州的南方理工州立大学获得了电信工程技术领域的理学学士学位。目前，他在这所高校的计算机与电子工程技术学院担任行业咨询委员会的委员。

献辞

我愿将本书献给赐予了我生命的父母，献给延续了我生命的儿女，献给我的爱妻Jennifer，因为她让我的人生变得如此美好。Jennifer，我爱你。

——Keith

那些会影响人们一生的灵感和思索总是不断变化，但它们都会通过不同的方式塑造着我们，让我们最终成为了此时此刻的自己。我对这些将我塑造为（或转变为）今日之我的所有影响心怀感恩。愿将本书献给我的朋友兼合著者Keith，感谢你让我相信创作这样一本图书是一个好点子，而且其中乐趣颇多（并在创作的过程中不断提醒我这一点）。愿将本书献给我的挚友Amy（你比我要明智得多），感谢你不断告诫我应该把更多注意力放到我的CCIE语音考试中，并不断敦促我、鼓励我前行。愿将本书献给我的挚友Angela，是你让我变得理智而又谦和，是你不断找出我计划中的漏洞，让我把一切变得更加完善，是你让我至今仍保持了这份幽默。最后，愿将本书献给我的两个小公主，是你们让我在看待这个世界时，拥有了一个更加积极的视角。

——Scott

致谢

我们想要感谢帮助我们完成了本书的所有同仁。

Cisco Press小组：责任编辑Brett Bartow是这个项目的催化剂，他协调了整个团队的工作，确保我们拥有充足的资源来完成此书的创作。项目编辑Andrew Cupp为本书创作了高质量的珍贵手稿。他为本书提供了大量宝贵的建议，纠正了多项技术错误，并切实地提高了本书的水准。还必须感谢Tonya Simpson以及本书的产品团队，感谢你们在编辑环节对本书提供的帮助，同时感谢你们不断跟进本书的进展。尤其需要感谢Keith Cline在审稿阶段付出的艰辛。

技术审稿人：我们想要感谢本书的技术稿人Brandon Anastasoff和David Burns，感谢你们为本书所作的深入、细致的审校工作，以及你们为本书补充的宝贵内容。

我们的家人：如果没有家庭成员持之以恒的支持，本书当然不可能得以问世。在创作本书的无数个日日夜夜中，是你们不断在我们身边，激励着我们，敦促着我们，鼓舞着我们，给予我们创作的灵感。感谢你们。

彼此：最后，本书是由两个人共同创作完成的。虽然我们在过去的5年间曾分别在三家不同的企业任职，但是我们的友情从未因此而间断。正是因为这份友情，才让创作本书的过程变得妙趣横生。

前言

如果你正在阅读本书，恭喜你，你手中的这本强大的工具书可以帮助你：

- 提升对于网络安全领域的了解和认识；
- 提高实施安全技术的技能；
- 备考 CCNA 安全认证考试。

本书在创作的过程中，无时无刻不把读者放心中。本书会引导读者学习组成安全网络的重要因素，并通过示例向读者演示如何实施这些特性。本书不仅以 CCNA 安全考试作为重点内容，还将理论与实践进行了结合。Scott Morris 和我创作本书的目的，是希望这本书能够作为读者的导游，带领读者在网络安全的世界中尽情遨游。

要想获得 CCNA 安全认证，就必须通过 640-554 *实施 Cisco IOS 网络安全*（*IINSv2*）这项考试。参加 CCNA 安全考试的先决条件是通过 CCNA 路由/交换考试认证（或任何一项 CCIE 认证）。CCNA 安全考试旨在考查读者是否具备了保护 Cisco 路由器、交换机以及相关网络方面的知识。本书包含了 Cisco 考试提纲中的所有主题，其中每章都涵盖了可以帮助读者了解相关信息的考试要点和备考任务。本书附赠的 CD 中，也同样包含了可以帮助读者考取安全 CCNA 认证的视频。当然，本书的 CD 中也提供了许多可以帮助读者备考的测试题目。

关于 640-554 实施 Cisco IOS 网络安全（IINSv2）考试

Cisco CCNA 安全考试的目的是为了考察考生，是否能够理解、实施和验证 Cisco 硬件和软件系统上的最佳做法。这项考试包含如下考点。

- **Cisco 路由器和交换机：**
  - 常见的威胁，包括混合的威胁，以及缓解这些威胁的方法；
  - 安全策略的生命周期法；
  - 理解和实施针对控制层、数据层和管理层的网络基础保护措施；
  - 理解、实施和验证 AAA 服务（认证、授权和审计），包括 TACACS+和 RADIUS 的具体内容；
  - 理解和实施 Cisco 访问控制服务器（Access Control Server，ACS）5.x 版中的基本规则，包括如何配置 ACS 和路由器，使它们能够相互通信；
  - 用来执行数据包过滤和流量分类的标准、扩展和命名的访问控制列表；
  - 理解和实施针对二层攻击（包括 CAM 表溢出攻击和 VLAN 跳转攻击）的保护措施。
- **Cisco 防火墙技术：**
  - 理解和描述防火墙实施过滤的各种方式（包括状态化过滤），比较各类防火墙技术的优劣；
  - 理解防火墙实现网络地址转换（NAT）和端口地址转换（PAT）的方法；

- 理解、实施和解释通过 Cisco 配置专家（CCP）实现基于区域的防火墙策略；
- 理解和描述自适应安全设备（ASA）上的接口特性和默认值、接口安全级别，以及 ASA 上的流量；
- 实施和解释如何通过名为 ASA 安全设备管理器（ASDM）的 GUI 工具在 ASA 上部署防火墙策略。

- **入侵防御系统（IPS）：**
  - 比较入侵防御系统（IPS）和入侵检测系统（IDS），包括这些系统区分恶意流量时所采用的各项方法的利与弊；
  - 描述 IPS 所包含的概念，包括漏报、误报等；
  - 使用 CCP 配置和验证基于 IOS 的 IPS。
- **VPN 技术：**
  - 理解和描述当今虚拟专用网络（VPN）中的各项组成部分，包括对称、非对称、加密、散列函数、Internet 密钥交换（IKE）、公钥基础设施（PKI）、认证、DH 算法、证书管理机构（CA）等概念；
  - 使用 CCP 和命令行界面（CLI）在 IOS 上实施和验证 IPSec VPN；
  - 使用 ASDM 在 ASA 上实施和验证 SSL VPN。

恰如读者所见，这个列表的内容十分庞杂，而本书的目的不仅是与读者一道解决和学习这些内容，而且还希望能够起到寓教于乐的效果。

640-554 IINSv2 考试

表 I-1 列举了 640-554 IINSv2 考试的考点，并指出了该内容位于本书中的哪一个部分。

表 I-1　　640-554 CCNA 安全（IINSv2）考点

考点	部分
常见安全威胁	
描述常见的安全威胁	第 1、2、3 部分
安全与 Cisco 路由器	
在 Cisco 路由器上实施安全	第 2、3 部分
描述保护控制层、数据层和管理层的方法	第 2 部分
描述 Cisco 安全管理器（CSM）	第 2、3 部分
描述 IPv4 到 IPv6 的过渡	第 2 部分
Cisco 设备上的 AAA	
实施 AAA（认证、授权和审计）	第 2 部分
描述 TACACS+	第 2 部分
描述 RADIUS	第 2 部分

续表

考点	部分
验证 AAA 功能	第 2 部分
IOS ACL	
描述用以过滤数据包的标准、扩展和命名的 IP IPS 访问控制列表（ACL）	第 3 部分
描述创建 ACL 时需要考虑的因素	第 3 部分
在网络中实施 IP ACL 以缓解威胁	第 3 部分
保护网络管理和报告系统	
描述保护网络管理	第 2 部分
实施保护网络管理	第 2 部分
常见的二层攻击	
描述使用 Cisco 交换机保护二层安全	第 2 部分
描述 VLAN 安全	第 2 部分
实施 VLAN 和 trunking	第 2 部分
（安全地）实施生成树协议	第 2 部分
Cisco 防火墙技术	
描述不同防火墙技术在操作上的优劣	第 3 部分
描述状态化防火墙	第 3 部分
描述用于防火墙技术中的各类 NAT	第 2 部分
使用 CCP 实施基于区域的策略防火墙	第 3 部分
实施 Cisco 自适应安全设备（ASA）	第 3 部分
实施网络地址转换（NAT）和端口地址转换（PAT）	第 3 部分
Cisco IPS	
描述部署 Cisco 入侵防御系统时需要考虑的因素	第 3 部分
描述 IPS 技术	第 3 部分
使用 CCP 配置 Cisco IOS IPS	第 3 部分
VPN 技术	
描述加密中使用的不同技术	第 4 部分
描述 VPN 技术	第 4 部分
描述 IPSec 的组成	第 4 部分
通过预共享密钥认证的方式实施 IOS IPSec 站点到站点 VPN	第 4 部分
验证 VPN 的工作	第 4 部分
使用 ASA 设备管理器实施 SSL VPN	第 4 部分

关于实施 Cisco IOS 网络安全（IINSv2）640-554 的认证考试指南

本书对应于 640-554 考试中的内容，使用大量的特性来帮助读者理解其中的内容，帮助读者准备相应的考试。

目标与方法

本书采用了多种不同的方法以帮助读者了解考试的内容，读者通过复习，可以完全掌握并记住这些内容，并且有把握认为自己已经学会了这些考点。因此，本书的目的不是为了让读者通过死记硬背来通过考试，而是真正学会并且理解相关的知识。本书会通过下列方法帮助读者通过考试。

- 采用与读者对话的口吻，像一位朋友一样，将本书的内容分门别类，娓娓道来，让读者感觉到这是一本量身定制的图书。
- 帮助读者了解需要掌握的考点，并通过深入的学习来真正“把握”这些内容。
- 通过解释来弥补读者在知识上的欠缺。
- （在 CD 上）提供三份视频文件，来加深读者通过本书所学到概念和技术。
- 通过问题检验读者对于这些内容的掌握程度。

本书特色

为了帮助读者有选择地使用本书，我们将各章的内容分为了几个部分，以帮助读者节省自己的学习时间。

- **“我已经知道了吗？”测试题**：在各章的开篇均备有一份测试题，这可以帮助读者确定自己需要花费多长时间来学习这一章中的知识。
- **基础主题**：这些内容是每章的核心。它们的作用是对这章中各个主题的概念进行解释。
- **备考任务**：在每章的“基础主题”部分之后是“备考任务”的环节，这一部分会向读者罗列出在阅读完这一章之后，读者需要完成哪些任务。每章都包括了读者要想掌握这一章内容，所需要执行的任务。
  - **复习所有考试要点**：在各章的“基础主题”中，最重要的内容旁边均打有“考试要点”的图标。所有这些“考试要点”都会罗列在这个表格中的考试要点一列中。虽然整个一章的内容都有可能出现在考试当中，但读者尤其必须掌握各个考试要点中的内容，因此这些内容需要进行复习。
  - **通过记忆补全表格**：这个环节是为了帮助读者记住一些重要的内容，本书附赠的 CD 中包含了许多这一章更加重要的列表。这些文件列表都只完成了一半，需要读者去把它们补全。
  - **定义关键术语**：虽然 640-554 考试不太可能出现让读者给专业术语下定义这

类的问题，但 CCNA 考试确实要求考生掌握大量的网络专业术语。这个环节会罗列出这一章中最为重要的术语，要求读者对这个术语进行简单的定义，然后读者可以将自己的定义与本书末尾的词汇表进行对比。

- **需要回忆的命令行参考信息**：回顾这一章中介绍的重要命令。

- **CD 上的模拟考试**：本书附赠的 CD 包含了一个考试软件，可以让读者对实际考试中可能出现的问题进行复习。读者可以通过这些问题来对自己进行模拟考试，以找出自己的薄弱环节。

本书组织结构

本书包含 21 个核心章节。第 22 章则为读者介绍了一些准备考试的方法，以及一些关于这项考试的建议。其中每个核心章节中都包含了 CCNA 安全考试的一部分考点。

第 1 部分：网络安全基础

- **第 1 章，“网络安全的概念”**，本章涵盖了网络和信息安全的需求与组成、当今网络的威胁，以及保护网络设计的基本原则。
- **第 2 章，“使用生命周期的方式来理解安全策略”**，本章介绍了风险分析、风险管理和安全策略的概念。
- **第 3 章，“建立安全战略”**，本章介绍了保护无边界网络的方式，以及控制和遏制数据丢失的方式。

第 2 部分：保护网络架构

- **第 4 章，“网络的基础保护”**，本章介绍了使用 NFP（网络基础保护）方式保护网络的方法，以及管理层、控制层和数据层的概念。
- **第 5 章，“使用 Cisco 配置专家（CCP）来保护网络架构”**，本章涵盖了 Cisco 配置专家（CCP）、CCP 特性和 GUI、建立新的设备、CCP 的组成、CCP 审计特性等内容。
- **第 6 章，“在 Cisco IOS 设备上保护管理层”**，本章对管理流量进行了介绍，同时也介绍了如何保护管理流量，并实施安全措施来保护管理层。
- **第 7 章，“使用 IOS 和 ACS 服务器实施 AAA”**，本章介绍了 Cisco ACS 的作用，以及与其一起使用的两大主要协议，即 RADIUS 和 TACACS，本章还涵盖了如何配置路由器，让它与 ACS 服务器实现互操作，以及如何配置 ACS 服务器让它与路由器实现互操作。此外，本章也介绍了如何对路由器和 ACS 服务器之间的互动进行验证和排错。
- **第 8 章，“保护二层技术”**，本章包含了 VLAN 和 trunking 的基础，生成树的基础、常见二层威胁以及缓解这些威胁的方法。
- **第 9 章，“在 IPv6 环境中保护数据层”**，本章包含了 IPv6 的相关内容（如 IPv6 的

基础、IPv6 的配置，以及针对 IPv6 的安全规划）。

第 3 部分：缓解和控制网络威胁

- **第 10 章，“规划威胁控制战略”**，本章中涵盖了缓解和遏制威胁的设计考虑因素，以及用来实现安全网络的硬件、软件和服务。
- **第 11 章，“使用访问控制列表来缓解网络威胁”**，本章包含了访问控制列表（ACL）的优势和基础，以及实施 IPv4 ACL、IPv6 ACL 来过滤数据包的方法。
- **第 12 章，“理解防火墙基础”**，本章涵盖了防火墙所使用的概念和技术、网络地址转换（NAT）的功能（包括 NAT 的组成），以及创建和部署防火墙的指导方针及考虑因素。
- **第 13 章，“实施 Cisco IOS 基于区域的防火墙”**，本章介绍了 IOS 基于区域的防火墙的操作组件和功能组件，以及配置和验证这种技术的方式。
- **第 14 章，“在 Cisco ASA 上配置基本的防火墙策略”**，本章包含了自适应安全设备（ASA）的产品和特性、ASA 防火墙的基础概念，以及配置 ASA 的方法。
- **第 15 章，“Cisco IPS/IDS 基础”**，本章将入侵防御系统（IPS）和入侵检测系统（IDS）进行了比较，同时也介绍了如何识别网络中的恶意流量，如何管理特征，如何监测和管理警告/告警信息。
- **第 16 章，“实施基于 IOS 的 IPS”**，本章涵盖了 IOS IPS 中包含的特性，以及如何安装 IPS 特性，如何使用 IOS IPS 中的特征，以及如何管理和监测 IPS 的警告消息。

第 4 部分：使用 VPN 建立安全连接

- **第 17 章，“VPN 技术基础”**，本章介绍了 VPN 的概念、使用 VPN 的理由，以及密码学的基本构成。
- **第 18 章，“公共密钥架构基础”**，本章包含了公共密钥架构（PKI）的概念、组成以及工作方式，同时也包含了让 PKI 正常工作的案例。
- **第 19 章，“IP 安全基础”**，本章涵盖了 IPSec 的概念、组成和工作方式，以及配置和验证 IPSec 的方式。
- **第 20 章，“实现 IPSec 站点到站点 VPN”**，本章包含了实施 IPSec 站点到站点 VPN 时的设计和准备工作，以及如何实施和验证 IPSec 站点到站点 VPN。
- **第 21 章，“使用 Cisco ASA 实现 SSL VPN”**，本章包含了（用于 VPN 的）SSL 的功能和用法、在 ASA 上配置 SSL 无客户端 VPN 的方法，以及在 ASA 上配置完全 SSL AnyConnect VPN 的方式。
- **第 22 章，“最终准备”**，本章介绍了可以用于准备最终考试的工具，并且可以帮助读者制定出一个高效的学习计划。

附录

- **附录 A，“我已经知道了吗？”测试题答案**，包含了第 1 章到第 21 章所有测试题的答案。
- **附录 B，CCNA 安全 640-554（IINSv2）考试更新**，本附录的作用是告诉读者当考试和本书进行了更新时，如何找到相应的更新信息。

这一部分包含 CCNA 安全考试中的如下主题：

- 描述常见的安全威胁。