Cisco职业认证培训系列
CISCO CAREER CERTIFICATIONS

# Official Cert Guide

Learn, prepare, and practice for exam success

- 掌握CCNP安全Secure 642-637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。

# CCNP安全Secure 642-637 认证考试指南

〔美〕 Sean Wilkins 著
Trey Smith
蒋楠 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Secure 642-637 认证考试指南

〔美〕 Sean Wilkins
Trey Smith 著
蒋楠 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Secure 642-637认证考试指南 / （美）威尔金斯（Wilkins,S.），（美）史密斯（Smith,T.）著；蒋楠，罗洋译. -- 北京：人民邮电出版社，2014.8
ISBN 978-7-115-34737-4

Ⅰ. ①C… Ⅱ. ①威… ②史… ③蒋… 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(2014)第035820号




◆ 著 [美] Sean Wilkins Trey Smith
译 蒋 楠 罗 洋 CCIE # 25318
责任编辑 傅道坤
责任印制 彭志环 杨林杰

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路 11 号
邮编 100164 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：36
字数：827 千字 2014 年 8 月第 1 版
印数：1－3 000 册 2014 年 8 月北京第 1 次印刷
著作权合同登记号 图字：01-2011-4678 号

定价：108.00 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

# 内容提要

本书是根据 Cisco 最新推出的 CCNP 安全 Secure 642-637 认证考试纲要编写的考试指南。全书分为 22 章和 2 个附录，包括网络安全基础的概念、组件、Cisco SAFE 模型；对网络及其组件造成威胁的各种手段；网络基础保护（NFP）概述；交换机数据面的攻击手段及应对方案；使用 802.1X 与 Cisco IBNS 框架为网络提供有效的访问授权；802.1X 认证的配置与实施；路由器数据面的攻击手段及应对方案；Cisco IOS 控制面/管理面的攻击手段及应对方案；NAT/ZBPFW/IPS 的配置与实施；站点到站点的安全解决方案；站点到站点 IPSec VPN 的部署/认证；DMVPN 的部署；为基于隧道的 IPSec VPN 部署高可用性；GET VPN 的部署；使用 SSL VPN/EZVPN 部署远程访问的解决方案等。

本书包含了大量的配置实例，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 Secure 642-637 认证考试相关的主题，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

**Sean Wilkins**，是一名来自于 SR-W 咨询公司的资深网络顾问，他拥有近 20 年的 IT 从业经验，曾供职于 Cisco、Lucent、Verizon、AT&T，以及其他一些私营企业。Sean 当前持有 CCNP/CCDP（Cisco）、MCSE（Microsoft）和 A+/Network+（CompTIA）证书，同时他还拥有计算机信息系统应用科学和计算机网络专业的学士学位。另外，他还获得了网络架构与设计、组织管理学以及网络安全这三个研究方向的硕士学位。在工作闲暇，Sean 还是一名技术撰稿人和编辑。

**Trey Smith**，作为一名高级网络安全架构师，他在网络设计与部署、保护大型企业及运营商网络方面拥有超过 15 年的从业经验。另外，他曾是许多企业、数据中心及 SMB 网络的架构级交付工程师。Trey 拥有管理信息系统专业的工商管理学士学位，同时他还持有 CCSP、CCNP、CCDP、MCSE（Microsoft）和 CISSP（ISC2）认证。目前，他致力于为一家世界 50 强的企业提供支付卡行业（PCI）数据安全标准（DSS）方面的战略及技术支持。

# 关于技术审稿人

**Sean Connelly**，CCIE #17085（路由交换及安全），是 TASC 公司的一名高级网络设计工程师，该公司总部坐落于华盛顿特区。他曾经为两家政府机构工作了近 10 年。Sean 目前致力于设计统一的 802.1X 解决方案、设计与实施大型数据中心网络，以及积极帮助政府机构创建网络安全的方案。在加入 TASC 之前，他是一名 ADCom 公司的 IT 服务部主管，该公司主要负责设计各种全球化的 WAN 解决方案。除了持有两个方向的 CCIE 证书以外，Sean 还获得了 CISSP 认证和工商管理专业的学士学位，并拥有 14 年的 IT 从业经验。

**Robert Woods**，是一名在网络信息安全及管理方面拥有 21 年丰富经验的资深信息安全专家。当前，他主要为一些金融服务机构提供满足管理及行业需求的企业网络安全方面的支持，其中包括为支付卡行业数据安全标准（PCI DSS）提供战略上和技术上的帮助。Robert 在全球最大的零售行业龙头中任职合格安全评审，同时他还是美国最大的汽车保险公司的高级技术顾问。他持有 CISSP、MCSE 和 GSEC Gold 认证，并且在南伊利诺伊斯大学获得了电子系统技术（EST）专业的学士学位和诺威治大学信息安全方向（MSIA）的硕士学位。

# 献辞

将本书献给我的三个女儿 Stacy、Anij 和 Saliah，而且在本书的创作期间，她们其中一个小天使来到了人间。如果没有你们，一切都将显得苍白无力。

——Sean Wilkins

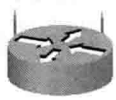
将本书献给我的妻子 Jackie、女儿 Olivia 与 Victoria：是你们给予了我勇气，是你们鼓励我应该“做得更好”，感谢你们对我的支持和理解。

——Franklin H.Smith III

# 致谢

借此机会，我们想要感谢所有对本书的编写及出版给予过帮助的人。正是因为你们的努力，本书才能成功地与读者见面。对于那些我们无法直接致谢的人，我们再一次由衷地感谢你们的付出，并期待与你们下一次共事。

# 本书图标使用说明



无线
路由器

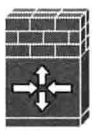
路由器

ATM/ 快速吉比特
以太网交换机

接入点

交换机

安全
交换机



Cisco IOS
防火墙

内容安全
服务模块

入侵
防御系统

SSL VPN
网关

IP 电话

AAA 服务器

Web 服务器

安全
终结点

数据库

PC

文件 / 应用
服务器

笔记本
电脑



无线连接

网络云



以太网连接

# 前言

本书将帮助你准备 Cisco Secure 认证考试。Secure 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 IOS 路由器、交换机和虚拟专用网（VPN）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主题。在开始应用安全策略之前，你应当具备与计算机网络相关的大量且深入的操作经验。Cisco Secure 课程旨在介绍相关的安全产品与 Cisco IOS 软件集成的安全特性，并阐述这些安全产品的应用，以及如何利用安全产品来增强网络的安全。Secure 课程是为网络管理员、网络安全管理员、网络架构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 22 章，章节内容相互关联且循序渐进。其中一些章节还包含了案例分析和练习配置的相关命令及注解。

本书涵盖以下主题。

- **第 1 章，“网络安全基础”**，回顾了基础的网络安全概念和组件，以及 Cisco SAFE 模型。本章所论述的内容是其他章节知识的核心基础。
- **第 2 章，“网络安全威胁”**，介绍可能对网络及其组件造成威胁的各种手段。只有更好地掌握了这些攻击方法，网络安全工程师才能从容面地面对可能出现的安全挑战。
- **第 3 章，“网络基础保护（NFP）概述”**，NFP 详细阐述了一种用于保护运行 Cisco IOS 软件设备的分层级方法。本章还涵盖了对控制、数据和管理层面进行攻击的手段，以及对应的安全技术。
- **第 4 章，“配置与实施交换式数据面安全解决方案”**，回顾了几种针对网络中交换机的数据层面进行攻击的手段，然后介绍用于应对这种攻击的安全技术，以及如何配置它们来为交换式的数据面提供最佳的保护。
- **第 5 章，“802.1X 与 Cisco 基于身份的网络服务（IBNS）”**，论述如何使用 IEEE 802.1X 和 Cisco IBNS 框架来为网络提供有效的访问授权。本章还介绍了 802.1X 的基础，包括各种可扩展的认证协议（EAP），以及各种可被用于保护网络的 IBNS 特性。
- **第 6 章，“配置与实施 802.1X 认证（基础）”**，描述如何在运行 Cisco IOS 软件的设备上配置基础的 802.1X 认证，从而阻止未经授权的客户端获取到网络资源的访问特权。
- **第 7 章，“配置与实施 802.1X 认证（进阶）”**，描述如何在运行 Cisco IOS 软件的设备上配置高级的 802.1X 认证特性，从而阻止未经授权的客户端获取到网络资源的访问特权。

- **第 8 章，“配置与实施 Cisco IOS 路由数据层面的安全”**，介绍了几种针对网络中路由器（或 3 层交换机）的数据层面进行攻击的手段，然后介绍了一些应对这种攻击的安全特性以及它们的配置方法。
- **第 9 章，“配置与实施 Cisco IOS 控制层面的安全“**，涵盖了几种针对网络中设备的控制层面进行攻击的手段，然后介绍了一些应对这种威胁的安全特性以及它们的配置方法。
- **第 10 章，“配置与实施 Cisco IOS 管理层面的安全”**，介绍了几种针对网络中设备的管理层面进行攻击的手段，然后介绍了一些应对这种攻击的安全特性以及它们的配置方法。
- **第 11 章，“配置与实施网络地址转换（NAT）”**，介绍网络地址转换（NAT）特性，以及该特性在网络中的各种用法。几乎每一个人在日常的网络使用过程中都会用到 NAT 特性；由于 IPv4 地址空间的枯竭，理解 NAT 特性的重要性已经不言而喻。
- **第 12 章，“配置与实施基于区域的策略防火墙”**，涵盖基于区域的策略防火墙（ZBPFW）特性，以及如何使用该特性来保护网络的不同部分。在当前的网络环境下，网络和相关设备不得不面对大量的安全威胁。ZBPFW 特性的各种出色功能可以为网络及设备提供有效的保护，避免受到各种攻击的威胁。
- **第 13 章，“配置与实施 IOS 入侵防御系统（IPS）”**，Cisco IOS 入侵防御系统（IPS）特性集被设计用于替代 Cisco IOS 入侵检测系统（IDS）。除了 IDS 常用的特征库匹配方法外，Cisco IPS 产品还使用有状态 pattern 识别、协议分析、流量异常检测和协议异常检测等特性。本章讨论 Cisco IOS IPS 的安全特性。
- **第 14 章，“介绍 Cisco IOS 站点到站点的安全解决方案”**，介绍站点到站点的 VPN 技术，以及与 IPSec VPN 主题相关的各种技术细节。
- **第 15 章，“部署基于 VTI 的站点到站点 IPSec VPN”**，涵盖如何使用 Cisco IOS 软件部署静态和动态的点到点 VTI 隧道。IPSec 虚拟隧道接口（VTI）极大地简化了在创建站点到站点 VPN 隧道时的配置过程。
- **第 16 章，“为站点到站点的 IPSec VPN 部署可扩展的认证”**，Cisco IOS 设备支持 CA 互操作性的特性。该特性允许 IOS 设备在创建 IPSec 连接时与认证权威机构（CA）通信。该功能提供了一种具有可扩展性和可管理性的企业 VPN 解决方案。
- **第 17 章，“部署 DMVPN”**，Cisco IOS 软件所提供的动态多点虚拟专用网（DMVPN）特性适用于简化在大型的中心站点到分支站点、非全互连和全互连环境下的 VPN 部署。本章涵盖如何在运行 Cisco IOS 软件的设备上实施 DMVPN。
- **第 18 章，“为基于隧道的 IPSec VPN 部署高可用性”**，介绍如何为 IPSec VPN 提供高可用性解决方案的机制，从而避免意外的网络中断。
- **第 19 章，“部署 GET VPN”**，涵盖 Cisco 组加密传输虚拟专用网（GET VPN）技术的部署。该技术适用于为复杂的、冗余的和全互连的网络环境提供简单的部署解决方案。
- **第 20 章，“使用 SSL VPN 部署远程访问的解决方案”**，远程访问 VPN 技术允许移动办公人员通过不可信任网络来访问企业内部资源。本章对比两种远程访问 VPN

技术，然后涵盖了在 Cisco ISR 上对基础的基于客户端和无客户端的 SSL VPN 解决方案的配置、验证及故障排除。

- **第 21 章，“使用 EZVPN 部署远程访问的解决方案”**，Cisco Easy VPN 是一种基于客户端/服务器模型的 VPN 解决方案，EZVPN 特性支持服务器向众多的远程设备“推送” VPN 安全参数，从而简化了配置的过程。
- **第 22 章，“最后冲刺”**，在完成了本书之前所有章节的学习后，本章总结了一些对考试有用的工具，并提出了建议的学习计划。
- **附录 A，“摸底测验及填空题答案”**，给出了在每章开头摸底测验的答案，以及每章末尾填空题的答案。
- **附录 B，“CCNP 安全 Secure 642-637 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了少量的更新，那么本附录旨在帮助你获取这些更新内容。如果 Cisco 彻底改革了考试内容，本附录则无法涵盖所有变化的内容。那时，你将需要购买配套的新版认证书籍。更新的考试内容将会以 PDF 文件的形式发布在与本书配套的网站上：www.ciscopress.com/title/9781587142802。
- **附录 C，“助记表”**，你可以在随书附赠的 CD 中找到该附录的 PDF 文件。该附录包括一系列内容不完整的表格，这些表格旨在帮助你牢记每一章的考试要点。你可以根据提示和线索完成表格中缺失的内容，从而测试自己对考试要点的掌握情况。
- **附录 D，“助记表答案”**，你可以在随书附赠的 CD 中找到该附录的 PDF 文件。你可以使用该附录所提供的完整表格来检查自己对附录 C 的完成情况。当然，你也可以把附录 D 作为一种帮助准备考试的独立学习工具。
- **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来帮助你进行自我评估，并强化章节重点。

- **摸底测验**：每章开头的一系列测试题将帮助你测验对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当重点关注的地方。
- **基础知识点**：作为每章的核心小节，基本知识点部分给出了备考所需掌握的协议、概念及技能。
- **备考指南**：在每章的末尾，备考指南罗列了本章的考试要点，同时，还给出了助记表附录和备考所需掌握的关键术语。不推荐为了通过认证考试而只关注本节所给出的考试要点、助记表和关键术语，但本节确实能够在最后备考冲刺阶段为你提供帮助。
- **填空题**：每章末尾都有一系列的复习填空题，用于测试你对本章重点内容的理解情况。这些填空题能够非常有效地帮助你理解重点内容和回忆考试要点。
- **CD 光盘上的考试练习**：本书配套的 CD 光盘上包含了一些免费的交互式考试练习。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被预测。因此，你不能只是简单地着眼于“记住”每个可能的答案，而应当通过扎实地学习来掌握课程重点，从而在考试中应对自如。

# 目录