



CCNA Security Exam Preparation



# CCNA Security

## Official Exam Certification Guide

- ✓ Master the **IINS 640-553** exam with this official study guide
- ✓ Assess your knowledge with **chapter-opening quizzes**
- ✓ Review key concepts with **Exam Preparation Tasks**
- ✓ Practice with **realistic exam questions** on the CD-ROM

[ciscopress.com](http://ciscopress.com)

Michael Watkins  
Kevin Wallace, CCIE® No. 7945

# **CCNA Security**

## **Official Exam Certification Guide**

---

**Michael Watkins**  
**Kevin Wallace, CCIE No. 7945**

**Cisco Press**

800 East 96th Street  
Indianapolis, IN 46240 USA

## **CCNA Security Official Exam Certification Guide**

Michael Watkins

Kevin Wallace, CCIE No. 7945

Copyright© 2008 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing June 2008

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58720-220-9

ISBN-10: 1-58720-220-4

### **Warning and Disclaimer**

This book is designed to provide the information necessary to be successful on the Cisco IINS (640-553) exam. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

### **Trademark Acknowledgments**

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

## Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact:

**U.S. Corporate and Government Sales**  
1-800-382-3419 [corpsales@pearsontechgroup.com](mailto:corpsales@pearsontechgroup.com)

For sales outside of the U.S. please contact:

**International Sales**  
[international@pearsontechgroup.com](mailto:international@pearsontechgroup.com)

## Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments about how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at [feedback@ciscopress.com](mailto:feedback@ciscopress.com). Please be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

**Publisher:** Paul Boger

**Cisco Press Program Manager:** Jeff Brady

**Associate Publisher:** Dave Dusthimer

**Copy Editor:** Gayle Johnson

**Executive Editor:** Brett Bartow

**Technical Editors:** Ryan Lindfield and Anthony Sequeira

**Managing Editor:** Patrick Kanouse

**Development Editor:** Andrew Cupp

**Senior Project Editor:** Tonya Simpson

**Editorial Assistant:** Vanessa Evans

**Book and Cover Designer:** Louisa Adair

**Composition:** Mark Shirar

**Indexers:** Tim Wright and Heather McNeil

**Proofreader:** Debbie Williams



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
165 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 20 20 020 0791  
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

## About the Authors

**Michael Watkins**, CCNA/CCNP/CCVP/CCSP, is a full-time senior technical instructor with SkillSoft Corporation. With 13 years of network management, training, and consulting experience, he has worked with organizations such as Kraft Foods, Johnson and Johnson, Raytheon, and the U.S. Air Force to help them implement and learn about the latest network technologies. In addition to holding more than 20 industry certifications in the areas of networking and programming technologies, he holds a bachelor of arts degree from Wabash College.

**Kevin Wallace**, CCIE No. 7945, is a certified Cisco instructor working full time for SkillSoft, where he teaches courses in the Cisco CCSP, CCVP, and CCNP tracks. With 19 years of Cisco networking experience, he has been a network design specialist for the Walt Disney World Resort and a network manager for Eastern Kentucky University. He holds a bachelor of science degree in electrical engineering from the University of Kentucky. He is also a CCVP, CCSP, CCNP, and CCDP, with multiple Cisco security and IP communications specializations.

## About the Technical Reviewers

**Ryan Lindfield** is an instructor and network administrator with Boson. He has more than ten years of network administration experience. He has taught many courses designed for CCNA, CCNP, and CCSP preparation, among others. He has written many practice exams and study guides for various networking technologies. He also works as a consultant, where among his tasks are installing and configuring Cisco routers, switches, VPNs, IDSs, and firewalls.

**Anthony Sequeira**, CCIE No. 15626, completed the CCIE in Routing and Switching in January 2006. He is currently pursuing the CCIE in Security. For the past 15 years, he has written and lectured to massive audiences about the latest in networking technologies. He is currently a senior technical instructor and certified Cisco Systems instructor for SkillSoft. He lives with his wife and daughter in Florida. When he is not reading about the latest Cisco innovations, he is exploring the Florida skies in a Cessna.

## Dedications

For their support and encouragement throughout this process, I dedicate my contribution to this book to my family.

—Michael

I dedicate my contribution to this book to my best friend (and wife of 14 years), Vivian.

—Kevin

## Acknowledgments

From Michael Watkins:

I want to thank the team at Cisco Press for their direction and support throughout the writing process. For their support and encouragement throughout this process, I wish to thank and acknowledge Tom Warrick and the instructor team at SkillSoft. I also wish to thank Kevin Wallace, who brought his talent and experience to this project and was an enormous help each step of the way.

Finally, I want to thank my family for their continued support through this project, especially my children, Abigail, Matthew, and Addison, who are always an inspiration in all that I do.

From Kevin Wallace:

I wish to express my sincere thanks to the team at Cisco Press. You guys are a class act, and I'm honored to be associated with you. Also, I give a huge thank-you to Michael Watkins for inviting me to participate in writing this book.

On a personal note, I know all the good things in my life come from above, and I thank God for those blessings. Also, my wife, Vivian, and my daughters, Sabrina and Stacie, have become accustomed to seeing me attached to my laptop over the past few months. Thank you for your love and support throughout this process.



# Contents at a Glance

Foreword xxvi

Introduction xxvii

## **Part I Network Security Concepts 3**

Chapter 1 Understanding Network Security Principles 5

Chapter 2 Developing a Secure Network 45

Chapter 3 Defending the Perimeter 77

Chapter 4 Configuring AAA 111

Chapter 5 Securing the Router 155

## **Part II Constructing a Secure Infrastructure 205**

Chapter 6 Securing Layer 2 Devices 207

Chapter 7 Implementing Endpoint Security 251

Chapter 8 Providing SAN Security 279

Chapter 9 Exploring Secure Voice Solutions 297

Chapter 10 Using Cisco IOS Firewalls to Defend the Network 319

Chapter 11 Using Cisco IOS IPS to Secure the Network 385

## **Part III Extending Security and Availability with Cryptography and VPNs 427**

Chapter 12 Designing a Cryptographic Solution 429

Chapter 13 Implementing Digital Signatures 463

Chapter 14 Exploring PKI and Asymmetric Encryption 491

Chapter 15 Building a Site-to-Site IPsec VPN Solution 523

## **Part IV Final Preparation 589**

Chapter 16 Final Preparation 577

## **Part V Appendixes 583**

Appendix A Answers to “Do I Know This Already?” Questions 585

Appendix B Glossary 595

Appendix C CCNA Security Exam Updates: Version 1.0 617

Appendix D Memory Tables (CD only)

Appendix E Memory Tables Answer Key (CD only)

Index 620



# Contents

Foreword xxvi

Introduction xxvii

## Part I Network Security Concepts 3

### Chapter 1 Understanding Network Security Principles 5

“Do I Know This Already?” Quiz 5

Foundation Topics 9

Exploring Security Fundamentals 9

*Why Network Security Is a Necessity 9*

*Types of Threats 9*

*Scope of the Challenge 10*

*Nonsecured Custom Applications 11*

*The Three Primary Goals of Network Security 12*

*Confidentiality 12*

*Integrity 12*

*Availability 13*

*Categorizing Data 13*

*Classification Models 13*

*Classification Roles 15*

*Controls in a Security Solution 16*

*Responding to a Security Incident 17*

*Legal and Ethical Ramifications 18*

*Legal Issues to Consider 19*

Understanding the Methods of Network Attacks 20

*Vulnerabilities 20*

*Potential Attackers 21*

*The Mind-set of a Hacker 23*

*Defense in Depth 24*

*Understanding IP Spoofing 27*

*Launching a Remote IP Spoofing Attack with IP Source Routing 28*

*Launching a Local IP Spoofing Attack Using a Man-in-the-Middle Attack 29*

*Protecting Against an IP Spoofing Attack 30*

*Understanding Confidentiality Attacks 31*

*Understanding Integrity Attacks 33*

*Understanding Availability Attacks 36*

*Best-Practice Recommendations 40*

Exam Preparation Tasks 41

Review All the Key Topics 41

Complete the Tables and Lists from Memory 42

Definition of Key Terms 42

Chapter 2	Developing a Secure Network	45
	“Do I Know This Already?” Quiz	45
	Foundation Topics	49
	Increasing Operations Security	49
	<i>System Development Life Cycle</i>	49
	<i>Initiation</i>	49
	<i>Acquisition and Development</i>	49
	<i>Implementation</i>	50
	<i>Operations and Maintenance</i>	50
	<i>Disposition</i>	51
	<i>Operations Security Overview</i>	51
	<i>Evaluating Network Security</i>	52
	<i>Nmap</i>	54
	<i>Disaster Recovery Considerations</i>	55
	<i>Types of Disruptions</i>	56
	<i>Types of Backup Sites</i>	56
	Constructing a Comprehensive Network Security Policy	57
	<i>Security Policy Fundamentals</i>	57
	<i>Security Policy Components</i>	58
	<i>Governing Policy</i>	58
	<i>Technical Policies</i>	58
	<i>End-User Policies</i>	59
	<i>More-Detailed Documents</i>	59
	<i>Security Policy Responsibilities</i>	59
	<i>Risk Analysis, Management, and Avoidance</i>	60
	<i>Quantitative Analysis</i>	60
	<i>Qualitative Analysis</i>	61
	<i>Risk Analysis Benefits</i>	61
	<i>Risk Analysis Example: Threat Identification</i>	61
	<i>Managing and Avoiding Risk</i>	62
	<i>Factors Contributing to a Secure Network Design</i>	62
	<i>Design Assumptions</i>	63
	<i>Minimizing Privileges</i>	63
	<i>Simplicity Versus Complexity</i>	64
	<i>User Awareness and Training</i>	64
	Creating a Cisco Self-Defending Network	66
	<i>Evolving Security Threats</i>	66
	<i>Constructing a Cisco Self-Defending Network</i>	67
	<i>Cisco Security Management Suite</i>	69
	<i>Cisco Integrated Security Products</i>	70
	Exam Preparation Tasks	74
	Review All the Key Topics	74