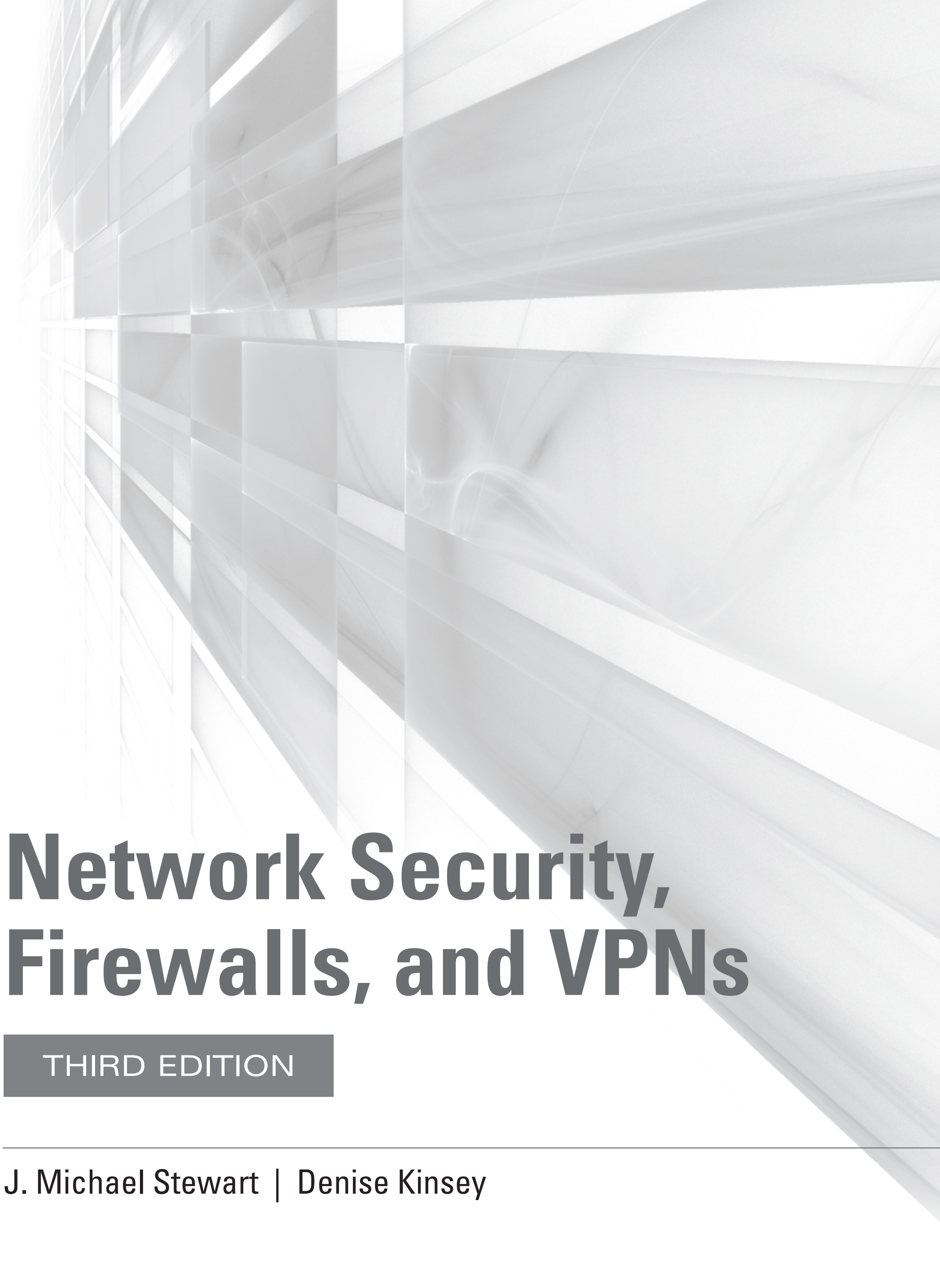
INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA



Network Security, Firewalls, and VPNs

THIRD EDITION

J. Michael Stewart | Denise Kinsey

JONES & BARTLETT
LEARNING

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

World Headquarters
Jones & Bartlett Learning
5 Wall Street
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

Copyright © 2021 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

The content, statements, views, and opinions herein are the sole expression of the respective authors and not that of Jones & Bartlett Learning, LLC. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement or recommendation by Jones & Bartlett Learning, LLC and such reference shall not be used for advertising or product endorsement purposes. All trademarks displayed are the trademarks of the parties noted herein. *Network Security, Firewalls, and VPNs, Third Edition* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product.

There may be images in this book that feature models; these models do not necessarily endorse, represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious, but are used for instructional purposes only.

18365-8

Production Credits
VP, Product Management: Amanda Martin
Director of Product Management: Laura Pagluica
Product Manager: Ned Hinman
Content Strategist: Melissa Duffy
Development Editor: Kim Lindros
Technical Editor: Jeff Parker
Content Coordinator: Paula-Yuan Gregory
Project Manager: Kristen Rogers
Project Specialist: John Fuller
Senior Digital Project Specialist: Angela Dooley
Marketing Manager: Michael Sullivan
Product Fulfillment Manager: Wendy Kilborn
Composition: Exela Technologies
Cover Design: Timothy Dziewit
Text Design: Kristin E. Parker
Media Development Editor: Faith Brosnan
Rights Specialist: James Fortney
Cover Image (Title Page, Part Opener, Chapter Opener): © Digital_Art/Shutterstock
Printing and Binding: LSC Communications

Library of Congress Cataloging-in-Publication Data
Names: Stewart, James Michael, author. | Kinsey, Denise, author.
Title: Network security, firewalls, and VPNs / J. Michael Stewart, Denise Kinsey.
Description: Third edition. | Burlington, MA : Jones & Bartlett Learning, [2021] | Includes bibliographical references and index. | Summary: “Network Security, Firewalls, and VPNs is written for a course on Network Security and Perimeter Defense, with special emphasis placed on Firewalls and VPNs - two key tools for securing networks. It is currently divided into three parts - Part 1 : Foundations of Network Security, Part 2 : Technical Overview of Network Security, Firewalls, and VPNs, and Part 3 : Implementation, Resources, and the Future”—Provided by publisher.
Identifiers: LCCN 2020022142 | ISBN 9781284183658 (paperback)
Subjects: LCSH: Firewalls (Computer security) | Computer networks—Security measures.
Classification: LCC TK5105.59 .S7585 2020 | DDC 005.8–dc23
LC record available at https://lccn.loc.gov/2020022142

6048

Printed in the United States of America

24 23 22 21 20 10 9 8 7 6 5 4 3 2 1

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

This book is dedicated to all who desire to learn more about network security, firewalls, and VPNs. May you gain foundational knowledge with this resource.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Digital_Art/Shutterstock

Brief Contents

Preface xix
Acknowledgments xxi
About the Authors xxiii

PART 1 **Foundations of Network Security** **1**

CHAPTER 1 Fundamentals of Network Security 3

CHAPTER 2 Network Security Threats 31

CHAPTER 3 Common Network Topologies and Infrastructures 67

CHAPTER 4 Network Design Considerations 97

PART 2 **Securing the Perimeter with Firewalls** **131**

CHAPTER 5 Firewall Fundamentals 133

CHAPTER 6 Firewall Implementation 173

CHAPTER 7 Firewall Deployment Considerations 191

CHAPTER 8 Configuring Firewalls 223

PART 3 **Establishing Remote Access with VPNs** **251**

CHAPTER 9 VPN Fundamentals 253

CHAPTER 10 VPN Management 283

CHAPTER 11 VPN Technologies 309

CHAPTER 12 VPN Implementation 327

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

PART 4 **Implementing Network Security 351**

CHAPTER 13 Firewall Security Management 353

CHAPTER 14 Best Practices for Network Security Management 373

CHAPTER 15 Emerging Technology and Regulatory Considerations 405

APPENDIX A Answer Key 427

APPENDIX B Standard Acronyms 429

Glossary of Key Terms 435

References 463

Index 469

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Digital_Art/Shutterstock

Contents

Preface xix

Acknowledgments xxi

About the Authors xxiii

PART 1 **Foundations of Network Security** 1

CHAPTER 1 **Fundamentals of Network Security** 3

What Is Network Security? 4

What Is Trust? 5
Who—or What—Is Trustworthy? 6
What Are Security Objectives? 6

What Are You Trying to Protect? 7

Seven Domains of a Typical IT Infrastructure 8

Goals of Network Security 11

How Can You Measure the Success of Network Security? 11

Why Are Written Network Security Policies Important? 12

Planning for the Worst 12

Who Is Responsible for Network Security? 12

Enhancing the Security of Wired Versus Wireless LAN Infrastructures 13

Internal and External Network Issues 14

Common Network Security Components Used to Mitigate Threats 17

Hosts and Nodes 17
Firewalls 17
Virtual Private Networks 18
Proxy Servers 18
Network Address Translation 19
The Domain Name System 22
Directory Services 22
Intrusion Detection Systems and Intrusion Prevention Systems 23
Network Access Control 24

TCP/IP Basics 24

OSI Reference Model 24
Sub-Protocols 26

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Headers and Payloads 27
Filtering on Addresses 27
CHAPTER SUMMARY 28
KEY CONCEPTS AND TERMS 29
CHAPTER 1 ASSESSMENT 30

CHAPTER 2 Network Security Threats 31

Hackers and Their Motivation 32

Favorite Targets of Hackers 36

Threats from Internal Personnel and External Entities 36

The Hacking Process 38
Reconnaissance 39
Scanning 39
Enumeration 41
Attacking 43
Post-Attack Activities 43

Common IT Infrastructure Threats 44
Hardware Failures and Other Physical Threats 44
Natural Disasters 45
Accidents 45

Malicious Code (Malware) 46
Advanced Persistent Threat 48

Fast Growth and Overuse 49

Wireless Versus Wired 50

Eavesdropping 50

Hijack and Replay Attacks 51

Insertion Attacks 52

Fragmentation Attacks 53

Buffer Overflows 53

Session Hijacking, Spoofing, and Man-in-the-Middle Attacks 54
Session Hijacking 54
Spoofing Attacks 55
Man-in-the-Middle Attacks 56

Covert Channels 57

Network and Resource Availability Threats 59
Denial of Service (DoS) 59
Distributed Denial of Service (DDoS) 60

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Hacker Tools 62

Social Engineering 62

CHAPTER SUMMARY 63

KEY CONCEPTS AND TERMS 64

CHAPTER 2 ASSESSMENT 65

CHAPTER 3 **Common Network Topologies and Infrastructures 67**

What Is a Network Topology? 68

Types of Network Devices 68

What Differentiates Logical and Physical Topologies? 76

Types of Physical Topologies 77
Logical Topology 81
Creating Logical Topologies 83

Differences Between Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) 84

IPSec and IPv6 86

Examples of Network Infrastructures and Related Security Concerns 87

Workgroups 87
SOHO Networks 89
Client/Server Networks 89
LAN Versus WAN 90
Thin Clients and Terminal Services 91
Remote Control, Remote Access, and VPN 91
Boundary Networks 93

CHAPTER SUMMARY 95

KEY CONCEPTS AND TERMS 95

CHAPTER 3 ASSESSMENT 96

CHAPTER 4 **Network Design Considerations 97**

Network Design and Defense in Depth 98

Achieving Defense in Depth through Layering 99
Planning for Scalability 101
Working with Senior Management 102

Protocols 102

Common Types of Addressing 104

IPv6 106

Controlling Communication Pathways 106

Router Configuration 107
Encrypted Protocols 107

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Physical Access Management 107
Filtering 108

Intrusion Detection Systems and Intrusion Prevention Systems 110

Hardening Systems 113

Equipment Selection 114

Authentication, Authorization, and Accounting 115

Communication Encryption 118

Hosts: Local-Only or Remote and Mobile 118

Redundancy 120

Endpoint Security 121

Clients 121
Servers 122
Routers 123
Switches 124
Firewalls and Proxies 124

Risk Assessment and Management 125

What Are Zones of Risk? 126

CHAPTER SUMMARY 128

KEY CONCEPTS AND TERMS 128

CHAPTER 4 ASSESSMENT 129

PART 2 Securing the Perimeter with Firewalls 131

CHAPTER 5 Firewall Fundamentals 133

What Is a Firewall? 134

What Firewalls Cannot Do 138

Why Do You Need a Firewall? 141

How Firewalls Work and What Firewalls Do 143

Types of Firewalls 148

Individual and SOHO Firewall Options 150

Managing the Firewall on an ISP Connection Device 152
Converting a Home Router into a Firewall 153

Uses for Host Software Firewalls 157

Examples of Software Firewall Products 157
Using Windows 10's Host Software Firewall 158
Using a Linux Host Software Firewall 160

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Uses for Commercial Software Network Firewalls 160

Uses for Hardware/Appliance Firewalls 161

Next-Generation Firewalls 162

What Are Virtual Firewalls? 162

Dual-Homed and Triple-Homed Firewalls 163

Ingress and Egress Filtering 164

Types of Filtering 164

Static Packet Filtering 164
Stateful Inspection and Dynamic Packet Filtering 165
Network Address Translation 166
Application Proxy 166
Circuit Proxy 167
Content Filtering 167

Selecting the Right Firewall for Your Needs 167

The Difference Between Buying and Building a Firewall 169

CHAPTER SUMMARY 170

KEY CONCEPTS AND TERMS 170

CHAPTER 5 ASSESSMENT 171

CHAPTER 6 **Firewall Implementation 173**

Examining Your Network and Its Security Needs 174

What to Protect and Why 174
Preserving Privacy 175

Proper Firewall Implementation Procedure 177

Constructing, Configuring, and Managing a Firewall 180

pfSense 180

pfSense Requirements 181

Planning a Firewall Implementation with pfSense 182

Firewalling a Small Organization: Packet Filtering or Application-Level Firewall, a Proxy Implementation 182
Firewalling Medium and Large Organizations: Application-Level Firewall and Packet Filtering, a Hybrid System 182
Firewalling in a Subnet Architecture 183

Installing the pfSense Firewall 183

Configuring a Firewall with pfSense 186

Elements of Firewall Deployment 186

Testing and Troubleshooting 187

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

CHAPTER SUMMARY 188

KEY CONCEPTS AND TERMS 189

CHAPTER 6 ASSESSMENT 189

CHAPTER 7 **Firewall Deployment Considerations** 191

Common Security Strategies for Firewall Deployments 192

Security Through Obscurity 192
Least Privilege 194
Simplicity 195
Defense in Depth 195
Diversity of Defense 196
Chokepoint 199
Weakest Link 199
Fail-Safe 200
Forced Universal Participation 200

Authentication, Authorization, and Accounting 202

Placement of Network Hardware Firewalls 204

Benefit and Purpose of Reverse Proxy 205

Use and Benefit of Port Forwarding 206

Considerations for Selecting a Bastion Host OS 207

Monitoring and Logging 208

Understanding and Interpreting Firewall Logs and Alerts 210

Intrusion Detection Systems and Intrusion Prevention Systems 214

Security Event and Information Management 215

Evaluating Needs and Solutions in Designing Security 216

What Happens When Security Gets in the Way of Doing Business? 218

CHAPTER SUMMARY 219

KEY CONCEPTS AND TERMS 220

CHAPTER 7 ASSESSMENT 220

CHAPTER 8 **Configuring Firewalls** 223

Firewall Rules 224

Inbound and Outbound Communications 226
Access Control Lists 227

Composing Firewall Rules 227

Ordering Firewall Rules 232

What Should You Allow and What Should You Block? 234

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Essential Elements of a Firewall Policy 236

Limitations of Firewalls 238

Improving Performance 240

The Downside of Encryption with Firewalls 242

Firewall Enhancements 244

Management Interfaces 245

CHAPTER SUMMARY 248

KEY CONCEPTS AND TERMS 248

CHAPTER 8 ASSESSMENT 249

PART 3 Establishing Remote Access with VPNs 251

CHAPTER 9 VPN Fundamentals 253

What Is a Virtual Private Network? 254

What Are the Benefits of Deploying a VPN? 259

What Are the Limitations of a VPN? 261

What Are Effective VPN Policies? 263

VPN Deployment Models and Architecture 263

VPN Deployment Models 263
VPN Architectures 265

Tunnel Versus Transport Mode 267

The Relationship Between Encryption and VPNs 268

Symmetric Cryptography 269
Asymmetric Cryptography 270
Hashing 274
Establishing VPN Connections with Cryptography 275
Digital Certificates 278

What Is VPN Authentication? 278

What Is VPN Authorization? 279

CHAPTER SUMMARY 280

KEY CONCEPTS AND TERMS 281

CHAPTER 9 ASSESSMENT 281

CHAPTER 10 VPN Management 283

VPN Management Best Practices 284

Build in Redundancy 285

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Choose the Right VPN Product for Your Environment 285
Develop a VPN Policy 286
Prohibit Split Tunneling 286
Ensure Client Security 286
Practice Vulnerability Management 287
Use Multifactor Authentication 288
Document Your Implementation Plan 288
Monitor VPN Availability 288
Perform Regular Reviews, Backups, and Updates 289

Developing a VPN Policy 290

Developing a VPN Deployment Plan 291

Bypass Deployment 292
Internally Connected Deployment 293
DMZ-Based Implementation 294

VPN Threats and Exploits 296

Commercial Versus Open-Source VPNs 300

Differences Between Personal and Enterprise VPNs 301

Balancing Anonymity and Privacy 301

Protecting VPN Security to Support Availability 301

The Importance of User Training 302

VPN Troubleshooting 303

CHAPTER SUMMARY 307

KEY CONCEPTS AND TERMS 308

CHAPTER 10 ASSESSMENT 308

CHAPTER 11 **VPN Technologies 309**

Differences Between Software and Hardware Solutions 310

Software VPNs 310
Hardware VPNs 311

Differences Between Layer 2 and Layer 3 VPNs 312

Internet Protocol Security (IPSec) 312

Layer 2 Tunneling Protocol (L2TP) 314

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) 315

SSL/TLS and VPNs 317

Secure Shell (SSH) Protocol 318

Establishing Performance and Stability for VPNs 320

Performance 320
Stability 321

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Using VPNs with Network Address Translation (NAT) 322

Types of Virtualization 323

Desktop Virtualization 323
SSL VPN Virtualization 324

CHAPTER SUMMARY 325

KEY CONCEPTS AND TERMS 325

CHAPTER 11 ASSESSMENT 325

CHAPTER 12 **VPN Implementation 327**

Operating System–Based VPNs 328

VPN Appliances 330

Configuring a Typical VPN Appliance 331
Client-Side Configuration 331

Remote Desktop Protocol 331

Using Remote Control Tools 333

Using Remote Access 333

The Technology for Remote Use 334
Choosing Between IPSec and SSL/TLS Remote Access VPNs 335

Remote Desktop Services 335

RD RemoteApp 335
RD Web Access 335
RDS and Hosted Services 336

Microsoft DirectAccess 336

DMZ, Extranet, and Intranet VPN Solutions 337

Intranet VPNs 337
Extranet VPNs 338

Internet Café VPNs 339

Online Remote VPN Options 339

Security 339
Wake-on-LAN Support 339
File Sharing 340
Remote Printing 340
Mac and Mobile Device Support 340

The Tor Application 340

Planning a VPN Implementation 341

Download and Verify Installation Files 342
Installation Tips 342
Configuring OpenVPN 342

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Running OpenVPN 344
Testing and Troubleshooting 344
OpenVPN Private Tunnel 346

VPN Implementation Best Practices 347

CHAPTER SUMMARY 348

KEY CONCEPTS AND TERMS 348

CHAPTER 12 ASSESSMENT 348

PART 4 Implementing Network Security 351

CHAPTER 13 Firewall Security Management 353

Best Practices for Firewall Management 354

Security Measures in Addition to a Firewall 357

Mitigating Firewall Threats and Exploits 358

Concerns Related to Tunneling Through or Across a Firewall 361

Testing Firewall Security 363

Important Tools for Managing and Monitoring a Firewall 364

Troubleshooting Firewalls 366

Detecting Firewall Threats and Responding to Incidents 369

CHAPTER SUMMARY 370

KEY CONCEPTS AND TERMS 370

CHAPTER 13 ASSESSMENT 370

CHAPTER 14 Best Practices for Network Security Management 373

Essentials of Network Security Management 374

Network Security Management Tools 378

Security Plan and Security Policy 379
Security Checklist 380

Limiting Network Access and Implementing Encryption 381

Physical Security 382

Techniques for Preventing and Deterring Incidents 383

Imposing Compartmentalization 384
Using Honeypots, Honeynets, and Padded Cells 384
Antivirus, Monitoring, and Other Host Security Controls 386
Backup and Recovery 387
User Training, Security Awareness, and Ongoing Education 388

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Incident Response 391

Preparation 392
Detection and Analysis 393
Containment 393
Eradication 393
Recovery 393
Post-Incident Follow-Up 393

Fail-Secure, Fail-Open, and Fail-Close Options 394

Network Security Assessments and Testing 395

Security Assessment 396
Configuration Scans 396
Vulnerability Scanning 396
Penetration Testing 397
Post-Mortem Assessment Review 398

Change Management 398

Compliance Auditing 399

Network Security Troubleshooting 400

CHAPTER SUMMARY 402
KEY CONCEPTS AND TERMS 403
CHAPTER 14 ASSESSMENT 403

CHAPTER 15 Emerging Technology and Regulatory Considerations 405

What the Future Holds for Network Security, Firewalls, and VPNs 406

Threats 407
Firewall Capabilities 407
Encryption 407
Authentication 408
Metrics 409
Focus 409
Securing the Cloud 410
Securing Mobile Devices 410
Internet of Things 410
Mobile IP 411
Bring Your Own Device (BYOD) 411

Resource Sites for Network Security, Firewalls, and VPNs 411

Firewall Vendors 411
Virtual Private Network Vendors 411
Network Security Websites 412
Network Security Magazine Websites 412

Tools for Network Security, Firewalls, and VPNs 412

Commercial Off-the-Shelf (COTS) Software 412
Open-Source Applications and Tools 413

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

The Vanishing Network Perimeter **413**
The Impact of Ubiquitous Wireless and Mobile Connectivity 414
Making Wireless and Mobile Connectivity More Secure 415
Potential Uses of Security Technologies **415**
Regulations and Compliance **417**
Specialized Firewalls Available **419**
Emerging Network Security Technologies **421**
Data Leakage Prevention 421
Biometrics 421
Virtualization Security 421
IP Version 6 422
VPNs, Firewalls, and Virtualization 422
CHAPTER SUMMARY **423**
KEY CONCEPTS AND TERMS **424**
CHAPTER 15 ASSESSMENT **424**

APPENDIX A **Answer Key** **427**
APPENDIX B **Standard Acronyms** **429**
Glossary of Key Terms **435**
References **463**
Index **469**

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Digital_Art/Shutterstock

Preface

Purpose of This Text

This text is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (*www.jblearning.com*). Designed for courses and curricula in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current research and trends in this critical subject area. These titles deliver fundamental information security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these texts are not just current, but forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow as well.

The first part of this text focuses on common network security topics and the business challenges and threats that you face as soon as you physically connect your organization's network to the public Internet. It presents key concepts and terms and reveals what hackers do when trying to access your network, thus providing you with the necessary foundation in network security for the discussions that follow.

Part 2 defines firewalls, providing you with an understanding of how to use these tools as security countermeasures to solve business challenges. It discusses how to select and deploy firewalls and the tools for managing and monitoring them. It focuses on the practical, giving concrete, step-by-step examples of how to implement a firewall.

Part 3 focuses on virtual private networks (VPNs) and reviews implementing a VPN, the technologies involved, and VPN-management best practices. It also discusses what challenges the future holds for information security professionals involved in network security. It covers the tools and resources available to the professional and scans the horizon of emerging technologies.

Learning Features

The writing style of this text is practical and conversational. Step-by-step examples of information security concepts and procedures are presented throughout. Each chapter begins with a statement of learning objectives. Illustrations are used both to clarify the material and to vary the presentation. The text is sprinkled with Notes, Tips, FYIs, Warnings, and sidebars to alert the reader to additional and helpful information related to the subject under discussion.

Chapter Assessments appear at the end of each chapter, with solutions provided in the back of the text. Chapter summaries are included in the text to provide a rapid review or

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

preview of the material and to help students understand the relative importance of the concepts presented.

Audience

The material is suitable for undergraduate or graduate students in computer science majors, information science majors, cybersecurity majors, students at a two-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT principles and want to expand their knowledge.

New to this Edition

This edition provides an improved format, where each major topic (network security, firewalls, VPNs) is examined from introduction through advanced topics before moving to a different topic and includes better integration among the topics. This edition also reflects the latest software versions and technology. The final chapters introduce encompassing best practices for network security and consider the future of technology, regulatory considerations, and people and process management.

Cloud Labs

This text is accompanied by Cybersecurity Cloud Labs. These hands-on virtual labs provide immersive mock IT infrastructures where students can learn and practice foundational cybersecurity skills as an extension of the lessons in this text. For more information or to purchase the labs, visit go.jblearning.com/stewart3e.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Digital_Art/Shutterstock

Acknowledgments

Dr. Denise Kinsey would like to thank Rob and M.C. for your undying support and encouragement; the development team and everyone at JBL with special thanks to Ned, Melissa, and Kim. I appreciate all of your comments and ideas in building this edition.

Jones & Bartlett Learning thanks all of the people who reviewed the second edition of this text. Your feedback helped to shape this revision.

Georgia Brown
American Military University
ECPI
EC Council University
Western Governors University
Tidewater Community College

Shana Bumpas
John Tyler Community College

Colin T. Carlile
Our Lady of the Lake University

Casimer DeCusatis
Marist College

Charles DeSassure
Tarrant County College

M. Lamine Diop
Blue Ridge Community College

Perry Hood
Wiregrass Georgia Technical College

Richard McKinney
Nashville State Community College

Teresa Nash
Lewis-Clark State College

Nicholas Peirce
Thomas Nelson Community College

Richard S. Riddle Jr.
Danville Community College

Jianhua Yang
Columbus State University

Tatyana Zidarov
Hagerstown Community College

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Digital_Art/Shutterstock

About the Authors

James Michael Stewart has been working with computers and technology for more than 25 years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job-skill and certification courses such as CISSP, CEH, and Security+. He is the primary author of the *CISSP Study Guide, 4th Edition* and the *Security+ 2008 Review Guide*. In addition, Michael has written numerous texts on other security and Microsoft certification and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom. Michael holds the following certifications: CISSP, ISSAP, SSCP, MCT, CEI, CEH, TICSA, CIW SA, Security+, MCSE+Security: Windows 2000, MCSA Windows Server 2003, MCDST, MCSE NT & W2K, MCP+I, Network+, iNet+. He graduated in 1992 from the University of Texas at Austin with a bachelor's degree in philosophy.

Denise Kinsey, Ph.D has worked in computer networking and cybersecurity for over 20 years. She has designed, implemented, and managed IT and OT projects for government and the private sector. Denise is the author of several IT and cybersecurity texts meant to educate and empower readers to learn more about technology and implement secure systems for their employers and their homes. When not solving cybersecurity problems she loves to work with her students to improve the networks and cybersecurity of non-profits and local businesses. Denise holds numerous certifications, including CISSP. C|CISO, Security+, and many others. Dr. Kinsey is an Associate Professor.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.