



CCNA Security

Portable Command Guide

All the CCNA Security 210-260 commands
in one compact, portable resource

ciscopress.com

Bob Vachon

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



What Do You Want to Do?

I want to:	Chapter	Page
Apply the quantitative risk analysis formula	2	17
Configure a client-based SSL VPN using ASDM	21	275
Configure a clientless SSL VPN using ASDM	21	286
Configure 802.1X port-based authentication	6	65
Configure AAA access control on an ASA 5505	20	260
Configure AAA accounting	6	65
Configure AAA authorization	6	64
Configure ACLs on an ASA 5505	20	243
Configure an ASA to ISR site-to-site IPsec VPN	21	294
Configure an IOS site-to-site IPsec VPN	16	183
Configure an IOS zone-based firewall	11	129
Configure basic settings on an ASA 5505	19	206
Configure DHCP settings on an ASA 5505	20	230
Configure device management access using ASDM	19	205
Configure interfaces on an ASA 5505	19	208
Configure IOS IPS	12	142
Configure IP ACLs	10	110
Configure IP ACLs with object groups	10	117
Configure IPv6 ACLs	10	121
Configure local AAA authentication	6	58
Configure NAT services on an ASA 5505	20	250
Configure NTP	5	51
Configure objects and object groups on an ASA 5505	20	235
Configure port security on a switch	7	72
Configure role-based access control	5	47
Configure server-based AAA authentication	6	61
Configure SNMPv3	5	51
Configure SSH access	5	42
Configure storm control on a switch	7	87
Configure STP Enhancement on a switch	7	84
Configure syslog	5	51
Configure the control plane on an ASA 5505	19	212

CCNA Security Portable Command Guide

Bob Vachon

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

CCNA Security Portable Command Guide

Bob Vachon

Copyright © 2016 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 March 2016

Library of Congress Control Number: 2016931906

ISBN-13: 978-1-58720-575-0

ISBN-10: 1-58720-575-0

Warning and Disclaimer

This book is designed to provide information about CCNA Security (210-260 IINS) exam and the commands needed at this level of network administration. Every effort has been made to make this book as complete and as 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 author 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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.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 from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager, Cisco Press: Jan Cornelssen

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Development Editor: Chris Cleveland

Project Editor: Mandie Frank

Copy Editor: Geneil Breeze

Technical Editor: Dave Garneau

Editorial Assistant: Vanessa Evans

Designer: Mark Shirar

Composition: codeMantra

Indexer: Tim Wright

Proofreader: Paula Lowell



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco Logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCDP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems Logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort Logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Crime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanel, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx Logo 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. (08129)

About the Author

Bob Vachon is a professor in the Computer Systems Technology program at Cambrian College in Sudbury, Ontario, Canada, where he teaches networking infrastructure courses. He has worked and taught in the computer networking and information technology field since 1984. He has collaborated on various CCNA, CCNA Security, and CCNP projects for the Cisco Networking Academy as team lead, lead author, and subject matter expert. He enjoys playing the guitar and being outdoors.

About the Technical Reviewers

Dave Garneau is a customer support engineer on the High Touch Technical Support (HTTS) Security team at Cisco Systems. He has also worked at Rackspace Hosting on its Network Security team. Before that, he was the principal consultant and senior technical instructor at The Radix Group, Ltd. In that role, Dave trained more than 3,000 students in nine countries on Cisco technologies, mostly focusing on the Cisco security products line, and worked closely with Cisco in establishing the new Cisco Certified Network Professional Security (CCNP Security) curriculum. Dave has a bachelor of science degree in mathematics from Metropolitan State University of Denver. Dave lives in McKinney, Texas, with his wife, Vicki, and their twin girls, Elise and Lauren.

Dedications

This book is dedicated to my students. Thanks for reminding me why I do this stuff.

I also dedicate this book to my beautiful wife, Judy, and daughters, Lee-Anne, Joëlle, and Brigitte. Without their support and encouragement, I would not have been involved in this project.

Acknowledgments

I would like to start off with a big thanks to my friend Scott Empson for involving me with this project. Your *Portable Command Guide* series was a great idea and kudos to you for making it happen.

Thanks to the team at Cisco Press. Thanks to Mary Beth for believing in me and to Chris for making sure I got things done right and on time.

Special thanks to my Cisco Networking Academy family. A big thanks to Jeremy and everyone else for involving me in these very cool projects. You guys keep me young.

Finally, a great big thanks to the folks at Cambrian College for letting me have fun and do what I love to do ... teach!

Contents at a Glance

Introduction xxi

Part I: Networking Security Fundamentals

- CHAPTER 1 Networking Security Concepts 1
- CHAPTER 2 Implementing Security Policies 15
- CHAPTER 3 Building a Security Strategy 27

Part II: Protecting the Network Infrastructure

- CHAPTER 4 Network Foundation Protection 35
- CHAPTER 5 Securing the Management Plane 41
- CHAPTER 6 Securing Management Access with AAA 57
- CHAPTER 7 Securing the Data Plane on Catalyst Switches 69
- CHAPTER 8 Securing the Data Plane in IPv6 Environments 91

Part III: Threat Control and Containment

- CHAPTER 9 Endpoint and Content Protection 99
- CHAPTER 10 Configuring ACLs for Threat Mitigation 107
- CHAPTER 11 Configuring Zone-Based Firewalls 125
- CHAPTER 12 Configuring Cisco IOS IPS 135

Part IV: Secure Connectivity

- CHAPTER 13 VPNs and Cryptology 149
- CHAPTER 14 Asymmetric Encryption and PKI 161
- CHAPTER 15 IPsec VPNs 167
- CHAPTER 16 Configuring Site-to-Site VPNs 177

Part V: Securing the Network Using the ASA

- CHAPTER 17 Introduction to the ASA 187
- CHAPTER 18 Introduction to ASDM 195
- CHAPTER 19 Configuring Cisco ASA Basic Settings 205
- CHAPTER 20 Configuring Cisco ASA Advanced Settings 229
- CHAPTER 21 Configuring Cisco ASA VPNs 273
- APPENDIX A Create Your Own Journal Here 303

Index 309

Reader Services

Register your copy at www.ciscopress.com/title/9781587205750 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9781587205750 and click Submit. Once the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Table of Contents

Introduction xxi

Part I: Networking Security Fundamentals

CHAPTER 1	Networking Security Concepts	1
	Basic Security Concepts	2
	Security Terminology	2
	Confidentiality, Integrity, and Availability (CIA)	2
	Data Classification Criteria	2
	Data Classification Levels	3
	Classification Roles	3
	Threat Classification	3
	Trends in Information Security Threats	4
	Preventive, Detective, and Corrective Controls	4
	Risk Avoidance, Transfer, and Retention	4
	Drivers for Network Security	5
	Evolution of Threats	5
	Data Loss and Exfiltration	5
	Tracking Threats	6
	Malware	6
	Anatomy of a Worm	7
	Mitigating Malware and Worms	7
	Threats in Borderless Networks	8
	Hacker Titles	8
	Thinking Like a Hacker	9
	Reconnaissance Attacks	9
	Access Attacks	10
	Password Cracking	11
	Denial-of-Service Attacks	11
	Distributed Denial-of-Service Attacks	12
	Tools Used by Attackers	13
	Principles of Secure Network Design	13
	Defense in Depth	14

CHAPTER 2 Implementing Security Policies 15

- Managing Risk 15
 - Quantitative Risk Analysis Formula 16
 - Quantitative Risk Analysis Example 17
 - Regulatory Compliance 17
- Security Policy 19
 - Standards, Guidelines, and Procedures 20
 - Security Policy Audience Responsibilities 21
 - Security Awareness 21
- Secure Network Lifecycle Management 22
 - Models and Frameworks 23
 - Assessing and Monitoring the Network Security Posture 23
 - Testing the Security Architecture 24
- Incident Response 24
 - Incident Response Phases 24
 - Computer Crime Investigation 25
 - Collection of Evidence and Forensics 25
 - Law Enforcement and Liability 25
 - Ethics 25
- Disaster-Recovery and Business-Continuity Planning 26

CHAPTER 3 Building a Security Strategy 27

- Cisco Borderless Network Architecture 27
 - Borderless Security Products 28
- Cisco SecureX Architecture and Context-Aware Security 28
 - Cisco TrustSec 30
 - TrustSec Confidentiality 30
 - Cisco AnyConnect 31
 - Cisco Talos 31
- Threat Control and Containment 31
- Cloud Security and Data-Loss Prevention 32
- Secure Connectivity Through VPNs 32
- Security Management 33

Part II: Protecting the Network Infrastructure

CHAPTER 4 Network Foundation Protection 35

- Threats Against the Network Infrastructure 35
- Cisco Network Foundation Protection Framework 36

Control Plane Security	37
Control Plane Policing	37
Management Plane Security	38
Role-Based Access Control	39
Secure Management and Reporting	39
Data Plane Security	39
ACLs	40
Antispoofing	40
Layer 2 Data Plane Protection	40
CHAPTER 5 Securing the Management Plane	41
Planning a Secure Management and Reporting Strategy	42
Securing the Management Plane	42
Securing Passwords	43
Securing the Console Line and Disabling the Auxiliary Line	43
Securing VTY Access with SSH	44
Securing VTY Access with SSH Example	45
Securing Configuration and IOS Files	46
Restoring Bootset Files	47
Implementing Role-Based Access Control on Cisco Routers	47
Configuring Privilege Levels	47
Configuring Privilege Levels Example	47
Configuring RBAC	48
Configuring RBAC via the CLI Example	49
Configuring Superviews	49
Configuring a Superview Example	50
Network Monitoring	51
Configuring a Network Time Protocol Master Clock	51
Configuring an NTP Client	52
Configuring an NTP Master and Client Example	52
Configuring Syslog	53
Configuring Syslog Example	54
Configuring SNMPv3	54
Configuring SNMPv3 Example	55
CHAPTER 6 Securing Management Access with AAA	57
Authenticating Administrative Access	57
Local Authentication	57

- Server-Based Authentication 58
- Authentication, Authorization, and Accounting Framework 58
- Local AAA Authentication 58
 - Configuring Local AAA Authentication Example 60
- Server-Based AAA Authentication 61
 - TACACS+ Versus RADIUS 61
 - Configuring Server-Based AAA Authentication 62
 - Configuring Server-Based AAA Authentication Example 63
- AAA Authorization 64
 - Configuring AAA Authorization Example 64
- AAA Accounting 65
 - Configuring AAA Accounting Example 65
- 802.1X Port-Based Authentication 65
 - Configuring 802.1X Port-Based Authentication 66
 - Configuring 802.1X Port-Based Authentication Example 68

CHAPTER 7 Securing the Data Plane on Catalyst Switches 69

- Common Threats to the Switching Infrastructure 70
 - Layer 2 Attacks 70
 - Layer 2 Security Guidelines 71
- MAC Address Attacks 72
 - Configuring Port Security 72
 - Fine-Tuning Port Security 73
 - Configuring Optional Port Security Settings 74
 - Configuring Port Security Example 75
- VLAN Hopping Attacks 76
 - Mitigating VLAN Attacks 76
 - Mitigating VLAN Attacks Example 77
- DHCP Attacks 78
 - Mitigating DHCP Attacks 78
 - Mitigating DHCP Attacks Example 80
- ARP Attacks 80
 - Mitigating ARP Attacks 80
 - Mitigating ARP Attacks Example 82
- Address Spoofing Attacks 83
 - Mitigating Address Spoofing Attacks 83
 - Mitigating Address Spoofing Attacks Example 83
- Spanning Tree Protocol Attacks 84
 - STP Stability Mechanisms 84

Configuring STP Stability Mechanisms	85
Configuring STP Stability Mechanisms Example	86
LAN Storm Attacks	87
Configuring Storm Control	88
Configuring Storm Control Example	88
Advanced Layer 2 Security Features	88
ACLs and Private VLANs	89
Secure the Switch Management Plane	89
CHAPTER 8 Securing the Data Plane in IPv6 Environments	91
Overview of IPv6	91
Comparison Between IPv4 and IPv6	91
The IPv6 Header	92
ICMPv6	93
Stateless Autoconfiguration	94
IPv4-to-IPv6 Transition Solutions	94
IPv6 Routing Solutions	94
IPv6 Threats	95
IPv6 Vulnerabilities	96
IPv6 Security Strategy	96
Configuring Ingress Filtering	96
Secure Transition Mechanisms	97
Future Security Enhancements	97
 Part III: Threat Control and Containment	
CHAPTER 9 Endpoint and Content Protection	99
Protecting Endpoints	99
Endpoint Security	99
Data Loss Prevention	100
Endpoint Posture Assessment	100
Cisco Advanced Malware Protection (AMP)	101
Cisco AMP Elements	101
Cisco AMP for Endpoint	102
Cisco AMP for Endpoint Products	102
Content Security	103
Email Threats	103
Cisco Email Security Appliance (ESA)	103
Cisco Email Security Virtual Appliance (ESAV)	104

Cisco Web Security Appliance (WSA)	104
Cisco Web Security Virtual Appliance (WSAV)	105
Cisco Cloud Web Security (CWS)	105

CHAPTER 10 Configuring ACLs for Threat Mitigation 107

Access Control List	108
Mitigating Threats Using ACLs	108
ACL Design Guidelines	108
ACL Operation	108
Configuring ACLs	110
ACL Configuration Guidelines	110
Filtering with Numbered Extended ACLs	110
Configuring a Numbered Extended ACL Example	111
Filtering with Named Extended ACLs	111
Configuring a Named Extended ACL Example	112
Mitigating Attacks with ACLs	112
Antispoofing ACLs Example	112
Permitting Necessary Traffic through a Firewall Example	114
Mitigating ICMP Abuse Example	115
Enhancing ACL Protection with Object Groups	117
Network Object Groups	117
Service Object Groups	118
Using Object Groups in Extended ACLs	119
Configuring Object Groups in ACLs Example	119
ACLs in IPv6	121
Mitigating IPv6 Attacks Using ACLs	121
IPv6 ACLs Implicit Entries	122
Filtering with IPv6 ACLs	122
Configuring an IPv6 ACL Example	123

CHAPTER 11 Configuring Zone-Based Firewalls 125

Firewall Fundamentals	125
Types of Firewalls	125
Firewall Design	126
Security Architectures	127
Firewall Policies	127
Firewall Rule Design Guidelines	128
Cisco IOS Firewall Evolution	128
Cisco IOS Zone-Based Policy Firewall	129

	Cisco Common Classification Policy Language	129
	ZPF Design Considerations	129
	Default Policies, Traffic Flows, and Zone Interaction	130
	Configuring an IOS ZPF	131
	Configuring an IOS ZPF Example	132
CHAPTER 12	Configuring Cisco IOS IPS	135
	IDS and IPS Fundamentals	135
	Types of IPS Sensors	136
	Types of Signatures	136
	Types of Alarms	136
	Intrusion Prevention Technologies	137
	IPS Attack Responses	137
	IPS Anti-Evasion Techniques	138
	Managing Signatures	140
	Cisco IOS IPS Signature Files	140
	Implementing Alarms in Signatures	140
	IOS IPS Severity Levels	141
	Event Monitoring and Management	141
	IPS Recommended Practices	142
	Configuring IOS IPS	142
	Creating an IOS IPS Rule and Specifying the IPS Signature File Location	143
	Tuning Signatures per Category	144
	Configuring IOS IPS Example	147
 Part IV: Secure Connectivity		
CHAPTER 13	VPNs and Cryptology	149
	Virtual Private Networks	149
	VPN Deployment Modes	150
	Cryptology = Cryptography + Cryptanalysis	151
	Historical Cryptographic Ciphers	151
	Modern Substitution Ciphers	152
	Encryption Algorithms	152
	Cryptanalysis	153
	Cryptographic Processes in VPNs	154
	Classes of Encryption Algorithms	155
	Symmetric Encryption Algorithms	155

- Asymmetric Encryption Algorithm 156
- Choosing an Encryption Algorithm 157
- Choosing an Adequate Keyspace 157
- Cryptographic Hashes 157
 - Well-Known Hashing Algorithms 158
 - Hash-Based Message Authentication Codes 158
- Digital Signatures 159

CHAPTER 14 Asymmetric Encryption and PKI 161

- Asymmetric Encryption 161
 - Public Key Confidentiality and Authentication 161
 - RSA Functions 162
- Public Key Infrastructure 162
 - PKI Terminology 163
 - PKI Standards 163
 - PKI Topologies 164
 - PKI Characteristics 165

CHAPTER 15 IPsec VPNs 167

- IPsec Protocol 167
 - IPsec Protocol Framework 168
 - Encapsulating IPsec Packets 169
 - Transport Versus Tunnel Mode 169
 - Confidentiality Using Encryption Algorithms 170
 - Data Integrity Using Hashing Algorithms 170
 - Peer Authentication Methods 171
 - Key Exchange Algorithms 172
 - NSA Suite B Standard 172
- Internet Key Exchange 172
 - IKE Negotiation Phases 173
 - IKEv1 Phase 1 (Main Mode and Aggressive Mode) 173
 - IKEv1 Phase 2 (Quick Mode) 174
 - IKEv2 Phase 1 and 2 174
 - IKEv1 Versus IKEv2 175
- IPv6 VPNs 175

CHAPTER 16 Configuring Site-to-Site VPNs 177

- Site-to-Site IPsec VPNs 177

IPsec VPN Negotiation Steps	177
Planning an IPsec VPN	178
Cipher Suite Options	178
Configuring IOS Site-to-Site VPNs	179
Verifying the VPN Tunnel	183
Configuring a Site-to-Site IPsec VPN	183

Part V: Securing the Network Using the ASA

CHAPTER 17 Introduction to the ASA 187

Adaptive Security Appliance	187
ASA Models	188
Routed and Transparent Firewall Modes	189
ASA Licensing	190
Basic ASA Configuration	191
ASA 5505 Front and Back Panel	191
ASA Security Levels	193
ASA 5505 Port Configuration	194
ASA 5505 Deployment Scenarios	194
ASA 5505 Configuration Options	194

CHAPTER 18 Introduction to ASDM 195

Adaptive Security Device Manager	195
Accessing ASDM	195
Factory Default Settings	196
Resetting the ASA 5505 to Factory Default Settings	197
Erasing the Factory Default Settings	197
Setup Initialization Wizard	197
Installing and Running ASDM	198
Running ASDM	200
ASDM Wizards	202
The Startup Wizard	202
VPN Wizards	203
Advanced Wizards	204

CHAPTER 19 Configuring Cisco ASA Basic Settings 205

ASA Command-Line Interface	205
Differences Between IOS and ASA OS	206
Configuring Basic Settings	206

Configuring Basic Management Settings	207
Enabling the Master Passphrase	208
Configuring Interfaces	208
Configuring the Inside and Outside SVIs	208
Assigning Layer 2 Ports to VLANs	209
Configuring a Third SVI	209
Configuring the Management Plane	210
Enabling Telnet, SSH, and HTTPS Access	210
Configuring Time Services	211
Configuring the Control Plane	212
Configuring a Default Route	212
Basic Settings Example	212
Configuring Basic Settings Example Using the CLI	213
Configuring Basic Settings Example Using ASDM	215
Configuring Interfaces Using ASDM	217
Configuring the System Time Using ASDM	221
Configuring Static Routing Using ASDM	223
Configuring Device Management Access Using ASDM	226
CHAPTER 20 Configuring Cisco ASA Advanced Settings	229
ASA DHCP Services	230
DHCP Client	230
DHCP Server Services	230
Configuring DHCP Server Example Using the CLI	231
Configuring DHCP Server Example Using ASDM	232
ASA Objects and Object Groups	235
Network and Service Objects	236
Network, Protocol, ICMP, and Service Object Groups	237
Configuring Objects and Object Groups Example Using ASDM	239
ASA ACLs	243
ACL Syntax	244
Configuring ACLs Example Using the CLI	245
Configuring ACLs with Object Groups Example Using the CLI	246
Configuring ACLs with Object Groups Example Using ASDM	247
ASA NAT Services	250
Auto-NAT	251
Dynamic NAT, Dynamic PAT, and Static NAT	251

Configuring Dynamic and Static NAT Example Using the CLI	253
Configuring Dynamic NAT Example Using ASDM	254
Configuring Dynamic PAT Example Using ASDM	257
Configuring Static NAT Example Using ASDM	258
AAA Access Control	260
Local AAA Authentication	260
Server-Based AAA Authentication	261
Configuring AAA Server-Based Authentication Example Using the CLI	261
Configuring AAA Server-Based Authentication Example Using ASDM	262
Modular Policy Framework Service Policies	266
Class Maps, Policy Maps, and Service Policies	267
Default Global Policies	269
Configure Service Policy Example Using ASDM	271
CHAPTER 21 Configuring Cisco ASA VPNs	273
Remote-Access VPNs	273
Types of Remote-Access VPNs	273
ASA SSL VPN	274
Client-Based SSL VPN Example Using ASDM	275
Clientless SSL VPN Example Using ASDM	286
ASA Site-to-Site IPsec VPN	294
ISR IPsec VPN Configuration	294
ASA Initial Configuration	296
ASA VPN Configuration Using ASDM	297
APPENDIX A Create Your Own Journal Here	303
Index	309

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

Welcome to CCNA Security! Scott Empson had an idea to provide a summary of his engineering journal in a portable quick reference guide. The result is the *Portable Command Guide* series. These small books have proven to be valuable for anyone studying for Cisco certifications or as a handy quick reference resource for anyone tasked with managing Cisco infrastructure devices.

The *CCNA Security Portable Command Guide* covers the security commands and GUI steps needed to pass the 210-260 Implementing Cisco Network Security certification exam. The guide begins by summarizing the required fundamental security concepts. It then provides the CLI commands required to secure an ISR. Examples are included to help demonstrate the security-related configuration.

The last part of the book focuses on securing a network using an Adaptive Security Appliance (ASA). It provides the CLI commands and the ASA Security Device Manager (ASDM) GUI screenshots required to secure an ASA 5505. Again, examples are included to help demonstrate the security-related configuration.

I hope that you learn as much from reading this guide as I did when I wrote it.

Networking Devices Used in the Preparation of This Book

To verify the commands in this book, I had to try them out on a few different devices. The following is a list of the equipment I used in the writing of this book:

- Cisco 1941 ISR running Cisco IOS release 15.4(3)M2
- Cisco 2960 switches running Cisco IOS release 15.0(2)SE7
- Cisco ASA 5505 running Cisco ASA IOS software version 9.2(3) with a Base License and the ASA Security Device Manager (ASDM) GUI version 7.4 (1)

Who Should Read This Book

This book is for people preparing for the CCNA Security (210-260 IINS) exam, whether through self-study, on-the-job training and practice, study within the Cisco Academy Program, or study through the use of a Cisco Training Partner. There are also some handy hints and tips along the way to make life a bit easier for you in this endeavor. The book is small enough that you can easily carry it around with you. Big, heavy textbooks might look impressive on the bookshelf in your office, but can you really carry them all around with you when working in some server room or equipment closet?

Organization of This Book

The parts of this book cover the following topics:

- **Part I, “Networking Security Fundamentals”**—Introduces network security-related concepts and summarizes how security policies are implemented using a lifecycle approach. It also summarizes how to build a security strategy for borderless networks.
- **Part II, “Protecting the Network Infrastructure”**—Describes how to secure the management and data planes using the IOS CLI configuration commands.
- **Part III, “Threat Control and Containment”**—Describes how to secure an ISR against network threats by configuring ACLs, a zoned-based firewall, and IOS IPS.
- **Part IV, “Secure Connectivity”**—Describes how to secure data as it traverses insecure networks using cryptology and virtual private networks (VPNs). Specifically, site-to-site IPsec VPNs are enabled using the IOS CLI configuration commands.
- **Part V, “Securing the Network Using the ASA”**—Describes how to secure a network using ASA data as it traverses insecure networks using cryptology and virtual private networks (VPNs). Specifically, remote access SSL VPNs are enabled using the IOS CLI configuration commands and ASDM.

Building a Security Strategy

The chapter covers the following topics:

Cisco Borderless Network Architecture

- Borderless Security Products

Cisco SecureX Architecture and Context-Aware Security

- Cisco TrustSec
- TrustSec Confidentiality
- Cisco AnyConnect
- Cisco Talos

Threat Control and Containment

Cloud Security and Data-Loss Prevention

Secure Connectivity Through VPNs

Security Management

Cisco Borderless Network Architecture

Traditional approaches to network security used well-defined borders to protect inside networks from outside threats and malware. Employees used corporate computers secured with antivirus and personal firewalls. Perimeter-based networks were protected using network-scanning devices (firewalls, web proxies, and email gateways).

Today, network borders are dissolving as users want to access to resources from any location, on any type of endpoint device, using various connectivity methods. Cisco has addressed this with the Borderless Network Architecture, which integrates the following components:

Borderless end zone	The zone offers deployment flexibility and strong security services in multiple dimensions as users connect to the network. End-user access is based on the security posture of the connecting endpoint using the Cisco AnyConnect SSL VPN Client. Infrastructure protection is provided using firewalls, intrusion prevention systems (IPSs), web security, and email security.
Borderless Internet	Implemented by performing Layer 2 through Layer 7 scanning engines managed by enterprises and cloud providers. Scanning engines assume the role of firewalls, intrusion detection/prevention systems (IDSs/IPSs), network proxies, and web gateways.

Borderless data center	Layers virtualized components on top of existing infrastructure components to provide security solutions for the cloud.
Policy management layer	The security policy is managed in central locations and then enforced throughout the network based on context-specific variables. It provides the following: <ul style="list-style-type: none">■ Access policy (who, what, when, where, and how)■ Dynamic containment policy■ Policy for on and off premise

Borderless Security Products

The architectural approach to security found in the Borderless Network Architecture results in distinct categories of Cisco products, technologies, and solutions:

- SecureX and context-aware security
- Threat control and containment
- Cloud security and data-loss prevention
- Secure connectivity through VPNs
- Security management

Cisco SecureX Architecture and Context-Aware Security

To respond to the evolving security needs of today's borderless network environments, Cisco developed the SecureX architecture. It is a new context-aware security architecture that enforces security policies across the entire distributed network, not just at a single point in the data stream.

The architecture starts with a solid network technology foundation that ensures the network infrastructure is not compromised in any way. It has security enforcement elements in the form of appliances, modules, or cloud services built on top. This architecture can deal with the full spectrum of devices, ranging from the traditional corporate PC or Mac, all the way to next-generation mobile devices such as iPads and Androids. With Cisco AnyConnect, security is enforced in the network by tethering these myriad devices into the security infrastructure at the most optimal point and attaching seamlessly.

The components of the SecureX strategy include the following:

- Context awareness
- Cisco TrustSec
- Cisco AnyConnect
- Cisco Talos

Figure 3-1 illustrates the components of the SecureX strategy.

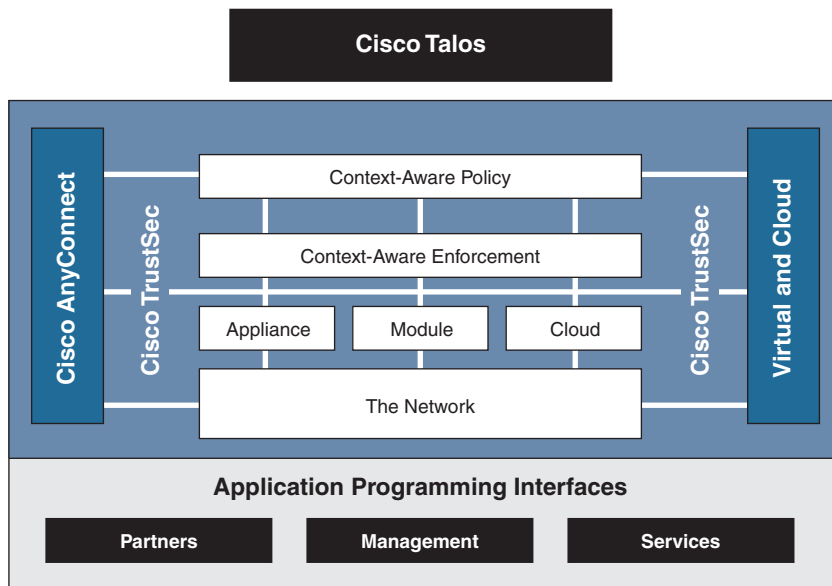


Figure 3-1 Cisco SecureX Components

Components of the Cisco SecureX strategy include the following:

Context-aware policies	Allows enforcement elements such as infrastructure devices to use user information (for example, user identity, security posture of the connecting device, and the point of access to the network) to define the access policy.
Cisco TrustSec	TrustSec is an intelligent and scalable access control solution that mitigates security access risks across the entire network to provide access to anyone, anywhere, anytime.
Cisco AnyConnect Client	AnyConnect Client provides for secure connectivity across a broad set of PC- and smartphone-based mobile devices. The enforcement devices provide posture assessment, access control services, and policy enforcement.
Cisco Talos	Cisco Talos Security Intelligence and Research Group (Talos) correlates data of almost a million live data feeds from deployed Cisco email, web, firewall, and IPS solutions to detect, analyze, and protect against both known and emerging threats. Information is shared with Cisco customers and devices on demand.

Cisco TrustSec

TrustSec is an umbrella term that encompasses the Cisco next-generation Network Access Control (NAC) framework, including the following:

- Policy-based access control
- Identity-aware networking based on roles
- Data confidentiality
- Data integrity

It does so by incorporating the following technologies:

- IEEE 802.1x (Dot1x)
- Cisco NAC Appliance
- Profiling technologies
- Guest services
- Security group tags (SGTs) and security group ACLs (SGACLs)
- MACSec (802.1AE)
- Access Control Server (ACS)
- Identity Services Engine (ISE)

When user TrustSec identities are not based on IP addresses or usernames, they are role based. When users authenticate, their privileges are based on their SGT and SGACL.

Cisco ISE combines the functionality of other Cisco products—such as the Cisco Secure Access Control Server (ACS) for authentication, authorization, and accounting (AAA) services, and Network Admission Control (NAC)—into this next-generation policy server.

TrustSec Confidentiality

TrustSec implementation follows this process:

1. A user connects to a switch using 802.1X. The switch relays the authentication credentials to an ISE. The ISE authenticates the user and assigns the user an SGT.
2. Traffic from the authenticated user is tagged with its specific SGT. Network devices along the data path read this tag and enforce its associated policy by restricting access to predetermined network destinations and resources. The devices do so by using SGACLs.
3. TrustSec can also provide data confidentiality by using MACSec. For example, if a policy requires that data should be secured, Cisco TrustSec understands this policy and dynamically encrypts the user data.

Cisco AnyConnect

Cisco AnyConnect protects mobile employees on PC-based or smartphone platforms using an SSL or IP Security (IPsec) virtual private network (VPN) to deliver a more seamless, always-on, and always-protected experience to end users, while enabling IT administrators to enforce policies and block malware with cloud-based or hybrid web security.

Cisco AnyConnect provides the following:

- Device support regardless of device type (for example, PC, laptop, smartphone, tablet, or PDA)
- Multifunctional security by combining multiple security controls in one client application
- Consistent experience by providing an always-on intelligent connection for seamless experience and performance

Cisco Talos

Cisco Talos combines the Cisco Security Intelligence Operations (SIO) and Sourcefire VRT to provide collective security intelligence. Talos baselines the current global state of threats and provides the network with valuable information to detect, prevent, and react to threats. It operates as an early-warning system by correlating threat information from the SensorBase, analyzed by the Threat Operations Center. This information is then provided to enforcement devices such as the Cisco Adaptive Security Appliance (ASA), Integrated Services Router (ISR), and IPS device for real-time threat prevention.

Threat Control and Containment

The Cisco threat control and containment solution regulates network access, isolates infected systems, prevents intrusions, and protects critical business assets. This solution counteracts malicious traffic before it affects a business.

Threat prevention products include the following:

Cisco ASAs	The Adaptive Security Appliance devices provide proven firewall services and integration of VPN and IPS technologies.
Cisco ISRs	Integrated Services Routers provide network security controls using zone-based policy firewall (ZPF), IOS IPS, and VPN technologies.
Cisco IPS	Intrusion prevention is provided using dedicated appliances or is integrated into ASA and ISR devices. These IPS sensors support a variety of IPS technologies, including signature-based, anomaly-based, policy-based, and reputation-based techniques.

Cloud Security and Data-Loss Prevention

Adding to the complexity of securing a network is the fact that many modern network designs now incorporate cloud computing. Threats in cloud computing include the following:

- Abuse of cloud computing
- Account or service hijacking
- Data loss in the cloud
- Unsecure interfaces and application programming interfaces (APIs)
- Malicious insiders

Administrators, because they are ultimately responsible for data residing on networks over which they have no control, must also consider the consequences if the cloud environment is not properly secured.

Two following traditional key services must now be secured in the cloud:

Securing web access	Cisco Cloud Web Security (CWS), formerly known as Cisco ScanSafe, is a cloud-based solution that provides comprehensive web security as a service (SaaS). Cisco CWS provides enhanced security for all endpoints while they access Internet websites using publicly available wireless networks including hotspots and mobile cellular networks. With Cisco CWS, administrators can set and enforce specific web use policies to control access to websites and specific content in web pages and applications as well as SaaS applications.
	Cisco Web Security Appliance (WSA) is a type of firewall and threat monitoring appliance that provides secure web access, content security, and threat mitigation for web services. It also provides advanced malware protection, application visibility and control, insightful reporting, and secure mobility.
Securing email access	Cisco Email Security Appliance (ESA) is a type of firewall and threat monitoring appliance for email traffic. It provides the capability to quickly block new email-based blended attacks, to control or encrypt sensitive outbound email, control spam, and more.

Secure Connectivity Through VPNs

There are two VPN-based solutions to implement secure connectivity:

Secure communications for remote access	Provides secure customizable access to corporate networks and applications by establishing an SSL or IPsec VPN tunnel between the remote host and central site
Secure communications for site-to-site connections	Provides secure site-to-site IPsec VPN access between two or more sites

Security Management

Cisco network management systems help automate, simplify, and integrate a network to reduce operational costs; improve productivity; and achieve critical functions such as availability, responsiveness, resilience, and security.

The hierarchy of tools available for security management is as follows:

Device managers	Web interface tool that simplifies the configuration and monitoring of a single device.
Cisco ASA Security Device Manager (ASDM)	A GUI-based device management tool for ASAs.
Cisco Security Manager	An enterprise-level application solution to configure and manage thousands of firewalls, routers, switches, IPS sensors, and other security solutions. Scalability is provided using intelligent policy-based management techniques that simplify administration.

This page intentionally left blank

Numerics

- 3DES (Triple Data Encryption Standard), 155
- 802.1X authentication, 65-68
 - configuring, 66-68

A

- AAA (authentication, authorization, and accounting), 58
 - accounting, 65
 - authentication, configuring server-based authentication, 61-64
 - authorization, 64
 - local authentication, 260
 - local authentication, configuring, 58-60
 - server-based authentication, 261-266
- aaa command, 59-60
- access attacks, 10-11
- access rules, 127-128
- access-class command, 45
- access-list command, 116
- accountability, 14
- accounting, 65
- ACLs (access control lists), 40
 - antispoofing, 112-117
 - ASA ACLs, 243-249
 - configuring, 245-249
 - syntax, 244-245
 - configuring, 110-112
 - design guidelines, 108
 - in IPv6, 121-124
- IPv6
 - configuring, 123-124
 - filtering, 122-123
 - implicit entries, 122
 - mitigating ICMP abuse, 115-116
 - mitigating threats with, 108
 - named extended ACLs, 111-112
 - numbered extended ACLs, 110-111
 - object groups
 - configuring, 119-121
 - in extended ACLs, 119
 - network object groups, 117-118
 - service object groups, 118-119
 - permitting traffic, 114
 - statements, 108-109
- address spoofing attacks, 83-84
- administrative threats, 3
- advanced wizards (ASDM), 204
- adware, 6
- AES (Advanced Encryption Standard), 155
- alarms, 136
- ALE (annualized loss expectancy), 17
- alert-severity command, 145
- amplification attacks, 12
- anomaly-based IPS, 137
- anti-evasion techniques, 138-139
- antispoofing, 40, 112-117
- AnyConnect, 31
- ARO (annualized rate of occurrence), 17
- ARP attacks, 71, 80-82
- asymmetric encryption algorithms, 156, 161-162
 - PKI, 162-165
 - characteristics, 165
 - standards, 163-164
 - topologies, 164

- private keys, 161-162

- public keys, 161-162

- RSA functions, 162

- ATOMIC-IP engine, 140

- attacks

- access attacks, 10-11

- address spoofing attacks, 83-84

- alarms, 136

- ARP attacks, 80-82

- denial-of-service, 11

- DHCP attacks, 78-80

- distributed denial-of-service, 12

- LAN storms, 87-88

- Layer 2, 70-71

- password cracking, 11

- reconnaissance attacks, 9-10

- responses, 137-138

- STP attacks, 84-87

- timing attacks, 139

- tools used for, 13

- VLAN attacks, 76-78

- mitigating, 76-78

- authentication

- 802.1X, 65-68

- configuring, 66-68

- local authentication, 57-58, 260

- configuring, 58-60

- routing protocols, 37

- server-based authentication, 58,

- 261-266

- configuring, 61-64

- RADIUS, 62

- TACACS+ 62

- authorization, 64

- Auto-NAT, 251

- AV (asset value), 16

B

- Basel II, 19

- basic settings, configuring on Cisco ASA,
212-227

- black hats, 8

- blended threats, 10

- block ciphers, 152

- blue hats, 8

- bootset files, restoring, 47

- Borderless Network Architecture, 27-28

- components, 27-28

- products, 28

- botnets, 12

- bots, 12

- BPDU guard, 84

- brute force attacks, 11

- buffer overflow attacks, 11

- business continuity planning, 26

C

- C3PL (Cisco Common Classification
Policy Language), 129

- CAPEC (Common Attack Pattern
Enumeration and Classification), 6

- CAs (certificate authorities), 163

- category command, 144

- certificates, 163

- CIA (confidentiality, integrity, and
availability), 2

- ciphers, 151

- Cisco AMP (Advanced Malware
Protection), 101-103

- elements, 101-102

- Cisco ASA (Adaptive Security Appliance),
31, 187-191

- AAA

- local authentication, 260

- server-based authentication,

- 261-266

- ACLs, 243-249

- configuring, 245-249

- syntax, 244-245

- Auto-NAT, 251

- basic settings, configuring, 206-208,
212-227

- CLI, 205-206

- configuring, 191-194

- control plane, configuring, 212

- DHCP services, configuring, 230-235

- Dynamic NAT, configuring, 251-257

- Dynamic PAT, 251-253

- features, 187-188

- interfaces, configuring, 208-210

- licensing, 190-191
- management plane, configuring, 210-212
- models, 188-189
- MPF, 266-271
 - class maps, 267-268
 - default global policies, 269-270
 - policy maps, 268-269
 - service policies, 269-271
- network objects, 236-237
- object groups, 237-239
 - configuring, 239-242
- routed mode, 189
- service objects, 236-237
- site-to-site VPNs
 - ASA initial configuration, 296-297
 - configuring, 297-301
 - ISR IPsec VPN configuration, 294-296
 - transparent mode, 189
- Cisco ASDM (ASA Security Device Manager), 33, 195-198
 - accessing, 195-196
 - advanced wizards, 204
 - factory default settings, 196-197
 - installing, 198-199
 - running, 200-202
 - Setup Initialization Wizard, 197-198
 - Startup Wizard, 202-203
 - VPN wizards, 203
- Cisco AutoSecure, 37
- Cisco Collective Security Intelligence Cloud, 101
- Cisco ESA (Email Security Appliance), 103-104
- Cisco ESAV (Email Security Virtual Appliance), 104
- Cisco IOS IPS, 135
- Cisco ISE (Identity Services Engine), 58
- Cisco ISR (Integrated Services Routers), 31
- Cisco NFP (Network Foundation Protection), 36
- Cisco Talos, 31
- Cisco TrustSec, 30
 - AnyConnect, 31
 - confidentiality, 30
 - Talos, 31
- class maps, 267-268
- class-map command, 131
- CLI (command-line interface), Cisco ASA, 205-206
- client-based SSL VPNs, 275-286
- clientless SSL VPNs, 286-294
- cloud security, 32
 - CWS, 105
- COBIT (Control Objectives for Information and Related Technology), 23
- command and control servers, 12
- commands
 - aaa, 59-60
 - access-list, 116
 - alert-severity, 145
 - ASA and IOS, comparing, 206
 - category, 144
 - class-map, 131
 - commands parser mode, 49
 - copy, 143
 - crypto isakmp policy, 179
 - description, 131
 - dot1x, 67
 - enable algorithm-type, 47
 - enable level, 47
 - enable view, 49
 - errdisable recovery, 74
 - event-action, 145
 - exec-timeout, 44
 - exit, 133
 - fidelity-rating, 145
 - hostname, 44-45
 - inspect, 133
 - ip access-group, 116
 - ip access-list, 55
 - ip arp inspection, 81
 - ip dhcp snooping, 79-80
 - ip domain name, 44
 - ip ips, 143-146
 - ip ssh, 44-45
 - ipv6 access-list, 122
 - key, 67
 - line aux 0, 44
 - line console 0, 44

- line vty 0, 45
 - logging, 54
 - login, 44
 - login local, 44
 - match, 131
 - no exec, 44
 - ntp, 51-52
 - object-group network, 117-118
 - object-group service, 118-119
 - parser view, 49
 - permit protocol, 122
 - policy-map, 132
 - privilege mode, 47
 - radius server, 67
 - reload, 47
 - retired, 145
 - secret password, 49
 - secure boot-image, 46
 - security passwords min-length, 43
 - service password-encryption, 43
 - service timestamps, 54
 - show ip ips, 146
 - show secure bootset, 46
 - snmp-server, 55
 - spanning-tree, 85-87
 - storm-control, 88
 - switchport, 72-73
 - transport input ssh, 45
 - username, 43-44
 - view, 51
 - zone security, 131-133
 - zone-pair, 132
- commands parser mode command, 49
- comparing
- ASA and IOS commands, 206
 - IPv4 and IPv6, 91-92
 - RADIUS and TACACS+, 61
- compartmentalization, 13
- computer crime investigation, 25
- confidential data, 3
- configuration files, securing, 46
- configuring
- 802.1X authentication, 66-68
 - AAA
 - local authentication, 58-60
 - server-based authentication, 61-64
 - ACLs, 110-112
 - IPv6, 123-124
 - object groups, 119-121
 - ASA site-to-site VPNs, 297-301
 - Cisco ASA, 191-194
 - ACLs, 245-249
 - basic settings, 212-227
 - basic settings, configuring, 206-208
 - control plane, configuring, 212
 - DHCP services, 230-235
 - Dynamic NAT, 251-257
 - Dynamic PAT, 251-253
 - interfaces, 208-210
 - management plane, 210-212
 - MPF, 266-271
 - server-based authentication, 261-266
 - Static NAT, 251-254
 - ingress filtering, 96-97
 - IOS IPS, 142-148
 - NTP
 - clients, 52
 - master clock, 51-52
 - object groups, 239-242
 - port security, 72-76
 - RBAC, 48-49
 - privilege levels, 47-48
 - site-to-site VPNs, 179-185
 - SNMPv3, 54-55
 - storm control, 88
 - STP stability mechanisms, 84-87
 - superviews, 49-51
 - syslog, 53-54
 - ZPF, 131-134
- console line security, 43-44
- containing threats, 31
- content security, 103-105
- Cisco ESA, 103-104
 - Cisco ESAV, 104
 - CWS, 105
 - email threats, 103
 - WSA, 104-105
- control plane, 36-38
- configuring on Cisco ASA, 212
- Control Plane Logging, 38
- controlling threats, 31

CoPP (Control Plane Policing), 37-38
 copy command, 143
 corrective controls, 4
 countermeasures, 2-4
 CPPr (Control Plane Protection), 38
 crackers, 8
 criteria for data classification, 2
 cryptanalysis, 153-154
 crypto isakmp policy command, 179
 cryptography
 ciphers, 151
 digital signatures, 159
 encryption algorithms, 152-153
 hashing algorithms, 158
 HMAC, 158
 modern substitution ciphers, 152
 cryptology, 151
 custodians of data, 3
 CWS (Cisco Cloud Web Security), 32, 105

D

data classification
 criteria for, 2
 levels, 3
 data plane, 36, 39-40
 ACLs, 40
 address spoofing attacks, 83-84
 antispoofing, 40
 ARP attacks, 80-82
 DHCP attacks, 78-80
 LAN storms, 87-88
 Layer 2 attacks, 70-72
 Layer 2 security tools, 40
 port security, configuring, 72-76
 STP attacks, 84-87
 VLAN attacks, 76-78
 decrypting ciphertext, 153-154
 default global policies, 269-270
 defense in depth, 14
 denial-of-service attacks, 11
 deployment modes (VPN), 150
 DES (Data Encryption Standard), 155
 description command, 131
 detective controls, 4
 DHCP attacks, 70, 78-80

DHCP services, configuring
 on Cisco ASA, 230-235
 dictionary lists, 11
 digital signatures, 159
 disaster recovery, 26
 distributed denial-of-service attacks, 12
 DLP (data loss prevention), 32, 100
 DMCA (Digital Millennium Copyright Act), 18
 dot1x command, 67
 drivers for network security, 5
 dual stack, 94
 Dynamic NAT, configuring, 251-257
 Dynamic PAT, 251-253, 257-258

E

EAPOL (Extensible Authentication Protocol over LAN), 65
 EF (exposure factor), 16
 email threats, 103
 enable algorithm-type command, 47
 enable level command, 47
 enable view command, 49
 encryption algorithms, 152-155
 asymmetric, 156, 161-162
 private keys, 161-162
 public keys, 161-162
 RSA functions, 162
 asymmetric encryption algorithms,
 PKI, 162-165
 choosing, 157
 IPsec, 170
 keyspace, choosing, 157
 symmetric, 155-156
 endpoint security, 99-100
 Cisco AMP for Endpoints, 102-103
 posture assessment, 100-101
 errdisable recovery command, 74
 ESA (Email Security Appliance), 32
 ethics, 25
 EU Data Protection Directive, 18
 event monitoring, 141-142
 event-action command, 145
 evidence collection, 25
 evolution of threats, 5

exec-timeout command, 44
exfiltration, 5
exit command, 133
exploits, 2
extended ACLs, object groups, 119
external assessments, 24

F

factory default settings for Cisco
ASDM, 196-197
false negatives, 136
fidelity-rating command, 145
firewalls
architectures, 127
Cisco ASA, 187-191
ACLs, 243-249
Auto-NAT, 251
basic settings, configuring,
206-208, 212-227
CLI, 205-206
configuring, 191-194
control plane, configuring, 212
DHCP services, configuring,
230-235
features, 187-188
interfaces, configuring, 208-210
licensing, 190-191
local authentication, 260
management plane, configuring,
210-212
models, 188-189
MPF, 266-271
network objects, 236-237
object groups, 237-239-242
routed mode, 189
server-based authentication,
261-266
service objects, 236-237
transparent mode, 189
design guidelines, 126
evolution of technology, 128
permitting traffic through, 114
policies, 127-128
rule design guidelines, 128
types of, 125-126

ZPF, 129-134
C3PL, 129
configuring, 131-134
design guidelines, 129
rules, 130

first generation threats, 5
FISMA (Federal Information Security
Management Act), 18
forensics, 25

G

GLB (Gramm-Leach-Bliley) Act, 18
gray hats, 8
guidelines, 20

H

hackers
thinking like, 9
titles, 8
hacktivists, 8
hashing algorithms, 158, 170-171
HIPAA (Health Insurance Portability and
Accountability Act), 18
HMAC (Hash-based Message
Authentication Codes), 158
hostname command, 44-45
hybrid cracking, 11

I

ICMP flooding, 12
ICMP object groups, 237-239
ICMPv6, 93-94
IDS (intrusion detection system), 135
IKE (Internet Key Exchange), 172-175
negotiation phases, 173
Phase 1, 173-174
Phase 2, 174-175
image files (IOS), securing, 46
implicit entries (ACLs), 122
in-band network security management, 42
incident response, 24-25
computer crime investigation, 25
ethics, 25

- evidence collection, 25
 - forensics, 25
 - law enforcement, 25
 - phases, 24-25
 - ingress filtering, configuring, 96-97
 - inspect command, 133
 - installing Cisco ASDM, 198-199
 - interfaces, configuring on Cisco ASA, 208-210
 - internal assessments, 23
 - Internet information queries, 10
 - IOS image files, securing, 46
 - IOS IPS
 - configuring, 142-148
 - rules, creating, 143-144
 - severity levels, 141
 - signatures, tuning, 144-147
 - ip access-group command, 116
 - ip access-list command, 55
 - ip arp inspection command, 81
 - ip dhcp snooping command, 79-80
 - ip domain name command, 44-45
 - ip ips command, 143-146
 - IP spoofing, 10
 - ip ssh command, 44-45
 - IPS (intrusion prevention system), 31, 135
 - alarms, 136
 - anomaly-based, 137
 - anti-evasion techniques, 138-139
 - attack responses, 137-138
 - event monitoring, 141-142
 - IOS IPS
 - configuring, 142-148
 - rules, creating, 143-144
 - severity levels, 141
 - policy-based, 137
 - recommended practices, 142
 - reputation-based, 137
 - sensors, 136
 - signature-based, 137
 - signatures, 136, 140-141
 - managing, 140
 - tuning, 144-147
 - IPsec, 167-172
 - confidentiality, 170
 - encryption algorithms, 170
 - hashing algorithms, 170-171
 - IKE, 172-175
 - negotiation phases, 173-175
 - key exchange algorithms, 172
 - NSA Suite B Standard, 172
 - packet encapsulation, 169
 - peer authentication methods, 171
 - site-to-site VPNs
 - cipher suite options, 178
 - planning, 178
 - verifying configuration, 183
 - transport versus tunnel mode, 169
 - IPv6
 - ACLs, 121-124
 - configuring, 123-124
 - filtering, 122-123
 - implicit entries, 122
 - comparing with IPv4, 91-92
 - header, 92-93
 - ICMPv6, 93-94
 - ingress filtering, configuring, 96-97
 - routing solutions, 94
 - stateless autoconfiguration, 94
 - threats, 95
 - transition mechanisms, 94, 97
 - VPNs, 175
 - vulnerabilities, 96
 - ipv6 access-list command, 122
 - ISC (Internet Storm Center), 6
 - ISE (Cisco Identity Services Engine), 58
 - ITIL (Information Technology Infrastructure Library), 23
- ## J-K
- Kali Linux, 13
 - key command, 67
 - key exchange algorithms, 172
- ## L
- LAN storms, 71, 87-88
 - law enforcement, 25
 - Layer 2
 - advanced security features, 88-89
 - attacks, 70-71

- security guidelines, 71-72
- security tools, 40
- least privilege, 13
- levels, for data classification, 3
- licensing, Cisco ASA, 190-191
- line aux 0 command, 44
- line console 0 command, 44
- line vty 0 command, 45
- local authentication, 57-58, 260
- local authentication, configuring, 58-60
- logging command, 54
- login command, 44-45
- login local command, 44
- loop guard, 84

M

- MAC address spoofing, 10, 70
- MAEC (Malware Attribute Enumeration and Characterization), 6
- malware, 6
 - adware, 6
 - Cisco AMP, 101-103
 - elements, 101-102
 - Cisco AMP for Endpoints, 102-103
 - mitigating, 7-8
 - scareware, 6
 - spyware, 6
 - Trojan horses, 6
 - viruses, 6
 - worms, 6
 - anatomy of, 7
- man-in-the-middle attacks, 10
- management plane, 36-39
 - bootset files, restoring, 47
 - configuring on Cisco ASA, 210-212
 - console line security, 43-44
 - IOS image files, securing, 46
 - password security, 43
 - RBAC, 39
 - securing, 89
 - VTY access, 44-46
- managing
 - risk, quantitative risk analysis, 16-19

- security, 33
 - in-band management, 42
 - OOB management, 42
 - signatures, 140
- master NTP clock, configuring, 51-52
- match command, 131
- MD5 (Message Digest algorithm 5), 158
- mediated access, 14
- Metasploit, 13
- mitigating
 - address spoofing attacks, 83-84
 - ARP attacks, 82
 - DHCP attacks, 78-80
 - malware, 7-8
 - VLAN attacks, 76-78
- modern substitution ciphers, 152
- MPF (Modular Policy Framework), 266-271
 - class maps, 267-268
 - default global policies, 269-270
 - policy maps, 268-269
 - service policies, 269, 271
- MTD (maximum tolerable downtime), 26
- MULTI-STRING engine, 140

N

- NAC (Network Access Control)
 - Cisco TrustSec, 30
- named extended ACLs, 111-112
- NAT (Network Address Translation)
 - Auto-NAT, 251
 - Dynamic NAT, 251-257
 - Dynamic PAT, 251-253
 - Static NAT, 251-254
- NAT firewalls, 125
- NERC (North American Electric Reliability Corporation), 18
- network monitoring, 51-55
 - NTP, 52-53
 - clients, configuring, 52
 - master clock, configuring, 51-52
 - SNMPv3, configuring, 54-55
 - syslog, configuring, 53-54
- network object groups, 117-118, 237-239
- network security
 - advanced Layer 2 features, 88-89

- control plane, 37-38
 - data plane, 39-40
 - ACLs, 40
 - address spoofing attacks, 83-84
 - antispoofing, 40
 - ARP attacks, 80-82
 - DHCP attacks, 78-80
 - LAN storms, 87-88
 - Layer 2 attacks, 70-72
 - Layer 2 security tools, 40
 - port security, configuring, 72-76
 - VLAN attacks, 76-78
 - defense in depth, 14
 - design principles, 13-14
 - drivers for, 5
 - endpoint security, 99-100
 - Cisco AMP for Endpoints, 102-103
 - posture assessment, 100-101
 - in-band management, 42
 - IPsec
 - confidentiality, 170
 - hashing algorithms, 170-171
 - IKE, 172-175
 - key exchange algorithms, 172
 - NSA Suite B Standard, 172
 - packet encapsulation, 169
 - peer authentication methods, 171
 - transport versus tunnel mode, 169
 - management plane, 38-39
 - bootset files, restoring, 47
 - console line security, 43-44
 - IOS image files, securing, 46
 - password security, 43
 - RBAC, 39
 - securing, 89
 - OOB management, 42
 - posture assessment, 23-24
 - secure network lifecycle management, 22-24
 - SecureX, 28-29
 - Cisco TrustSec, 30
 - testing techniques, 24
 - VPNs, 32, 149-150
 - classifying, 149-150
 - deployment modes, 150
 - encryption algorithms, 155
 - IPsec, 167-172
 - remote-access, 150, 273-274
 - site-to-site, 150
 - Next Generation firewalls, 126
 - next generation threats, 5
 - NFP (Cisco Network Foundation Protection), 36
 - NIST (National Institute of Standards and Technology), 23
 - no exec command, 44
 - NSA Suite B Standard, 172
 - NTP (Network Time Protocol), 52-53
 - clients, configuring, 52
 - master clock, configuring, 51-52
 - ntp command, 51-52
 - numbered extended ACLs, 110-111
- ## O
- object-group network command, 117-118
 - object-group service command, 118-119
 - object groups, 237-239
 - configuring, 119-121, 239-242
 - in extended ACLs, 119
 - network object groups, 117-118
 - service object groups, 118-119
 - one-time pads, 151
 - OOB (out-of-band) network security management, 42
 - OWASP (Open Web Application Security Project), 6
 - owners of data, 3
- ## P
- packet sniffers, 10
 - packet-filtering firewalls, 126
 - parser view command, 49
 - passwords
 - cracking, 11
 - securing, 43
 - PCI DSS (Payment Card Industry Data Security Standard), 18
 - peer authentication methods, 171
 - permit protocol command, 122
 - permitting traffic through firewalls, 114

- pharming, 10
- phishing, 10, 103
- phreakers, 8
- physical threats, 3
- ping of death attacks, 11
- ping sweeps, 10
- PIPEDA (Personal Information Protection and Electronic Documents Act), 18
- pivoting attacks, 96
- PKI (public key infrastructure), 162-165
 - characteristics, 165
 - standards, 163-164
 - topologies, 164
- plaintext, 152
- planning IPsec VPNs, 178
- policy maps, 268-269
- policy-based IPS, 137
- policy-map command, 132
- polyalphabetic ciphers, 151
- port scanners, 10
- port security, configuring, 72-76
- PortFast, 84
- preventive controls, 4
- private data, 3
- private keys, 161-162
- private VLANs, 89
- privilege levels (RBAC), configuring, 47-48
- privilege mode command, 47
- procedures, 20
- protocol object groups, 237-239
- proxy firewalls, 126
- public data, 3
- public keys, 161-162

Q

- qualitative risk analysis, 16
- quantitative risk analysis, 16-19
 - example of, 17
 - regulatory compliance, 17-19

R

- RA-Guard, 97
- RADIUS, 61

- radius server command, 67
- RAs (registration authorities), 163
- RBAC (Role-Based Access Control), 39
 - configuring, 48-49
 - privilege levels, configuring, 47-48
- reconnaissance attacks, 9-10
- reflection attacks, 12
- regulations, quantitative risk analysis, 17-19
- reload command, 47
- remote-access VPNs, 150, 273-274
 - client-based SSL VPNs, 275-286
 - clientless SSL VPNs, 286-294
- reputation-based IPS, 137
- restoring bootset files, 47
- retired command, 145
- risk, 2
 - countermeasures, 4
 - quantitative risk analysis, 16-19
 - example of, 17
 - regulatory compliance, 17-19
- Rivest ciphers, 156
- rogue switches, 76
- root guard, 84
- rotation of duties, 13
- routing protocols, authentication, 37
- RPO (recovery point objective), 26
- RSA (Rivest, Shamir, and Adleman)
 - algorithm, 162
- RSA crypto keys, creating, 143
- RTO (recovery time objective), 26
- rule design guidelines, 128
- rules, creating, 143-144
- running Cisco ASDM, 200-202

S

- Safe Harbour Act, 19
- SBU (sensitive but unclassified) data, 3
- scareware, 6
- script kiddies, 8
- SEAL (Software-optimized Encryption Algorithm), 155
- SEAP (Signature Event Action Processor), 146
- second generation threats, 5
- secret data, 3

- secret password command, 49
- sectools.org, 13
- secure boot-image command, 46
- SecureX, 28-29
 - Cisco TrustSec, 30
 - AnyConnect, 31
 - confidentiality, 30
- security. *See also* network security
 - AAA, 58
 - accounting, 65
 - authorization, 64
 - ACLs
 - antispoofing, 112-117
 - configuring, 110-112
 - design guidelines, 108
 - in IPv6, 121-124
 - mitigating ICMP abuse, 115-116
 - mitigating threats with, 108
 - named extended ACLs, 111-112
 - numbered extended ACLs, 110-111
 - permitting traffic, 114
 - statements, 108-109
 - attacks
 - access attacks, 10-11
 - address spoofing attacks, 83-84
 - ARP attacks, 80-82
 - denial-of-service, 11
 - DHCP attacks, 78-80
 - distributed denial-of-service, 12
 - LAN storms, 87-88
 - password cracking, 11
 - reconnaissance attacks, 9-10
 - STP attacks, 84-87
 - VLAN attacks, 76-78
 - authentication
 - 802.1X, 65-68
 - local authentication, 57-58
 - routing protocols, 37
 - server-based authentication, 58
 - business continuity planning, 26
 - Cisco IOS IPS, 135
 - cloud security, 32
 - CWS, 105
 - content security, 103-105
 - Cisco ESA, 103-104
 - Cisco ESAV, 104
 - email threats, 103
 - WSA, 104-105
 - countermeasures, 2
 - cryptanalysis, 153-154
 - cryptography
 - ciphers, 151
 - digital signatures, 159
 - encryption algorithms, 152-153
 - hashing algorithms, 158
 - HMAC, 158
 - modern substitution ciphers, 152
 - data loss, 5
 - disaster recovery, 26
 - DLP, 100
 - endpoint security, 99-100
 - posture assessment, 100-101
 - exploits, 2
 - firewalls
 - architectures, 127
 - design guidelines, 126
 - evolution of technology, 128
 - policies, 127-128
 - rule design guidelines, 128
 - ZPF, 129-134
 - IDS, 135
 - incident response, 24-25
 - ethics, 25
 - evidence collection, 25
 - forensics, 25
 - law enforcement, 25
 - phases, 24-25
 - IPS, 135
 - alarms, 136
 - anomaly-based, 137
 - anti-evasion techniques, 138-139
 - attack responses, 137-138
 - event monitoring, 141-142
 - policy-based, 137
 - recommended practices, 142
 - reputation-based, 137
 - sensors, 136
 - signature-based, 137
 - signatures, 136, 140-141
 - IPsec, 167-172
 - confidentiality, 170

- hashing algorithms, 170-171
- IKE, 172-175
- key exchange algorithms, 172
- NSA Suite B Standard, 172
- packet encapsulation, 169
- peer authentication methods, 171
- transport versus tunnel mode, 169
- management plane, VTY access, 44-46
- managing, 33
- risk, 2
 - countermeasures, 4
 - quantitative risk analysis, 16-19
- roles, 21
- SSH, commands, 44-46
- threats, 2, 35
 - in borderless networks, 8
 - categories of, 3
 - controlling, 31
 - corrective controls, 4
 - detective controls, 4
 - to email, 103
 - evolution of, 5
 - impact of, 36
 - to IPv6, 95
 - preventive controls, 4
 - to switching, 70-71
 - tracking, 6
 - trends, 4
- VPNs, 32
 - vulnerability, 2, 35
- security passwords min-length command, 43
- security policies, 19-22
 - awareness and training programs, 21-22
 - structure, 19
 - technical policies, 20
- SeND (Secure Neighbor Discovery), 97
- sensitive data, 3
- sensors, 136
- separation of duties, 13
- server-based authentication, 58, 261-266
 - configuring, 61-64
 - RADIUS, 62
 - TACACS+, 62
 - service engines, 140
 - service object groups, 118-119, 237-239
 - service password-encryption command, 43
 - service policies, 269-271
 - service timestamps command, 54
 - Setup Initialization Wizard (ASDM), 197-198
 - SHA-1 (Secure Hash Algorithm), 158
 - show ip ips command, 146
 - show secure bootset command, 46
 - SIEM, 51
 - signature-based IPS, 137
 - signatures, 136, 140-141
 - managing, 140
 - tuning, 144-147
 - site-to-site VPNs, 150
 - ASA initial configuration, 296-297
 - cipher suite options, 178
 - configuring, 179-185, 297-301
 - ISR IPsec VPN configuration, 294-296
 - negotiation steps, 177-178
 - planning, 178
 - verifying configuration, 183
 - SLE (single loss expectancy), 17
 - snmp-server command, 55
 - SNMPv3, configuring, 54-55
 - social engineering, 4, 11
 - SOX (Sarbanes-Oxley Act of 1992), 18
 - spam, 103
 - spanning-tree command, 85-87
 - spyware, 6
 - SSH (Secure Shell) commands, 44-46
 - SSL (Secure Sockets Layer), remote-access VPNs, 273-274
 - client-based SSL VPNs, 275-286
 - clientless SSL VPNs, 286-294
 - standards, 20
 - Startup Wizard (Cisco ASDM), 202-203
 - stateful firewalls, 126
 - stateless autoconfiguration, 94
 - statements (ACLs), 108-109
 - Static NAT, 258-259
 - Static NAT, configuring, 251-254
 - storm control, configuring, 88
 - storm-control command, 88

STP (Spanning Tree Protocol)
 manipulating, 71
 stability mechanisms, configuring,
 84-87

STRING engines, 140

structure of security policies, 19

substitution ciphers, 151

Suite B, 172

supervisors, configuring, 49-51

switching
 rogue switches, 76
 threats to, 70-71

switchport command, 72-73

symmetric encryption algorithms,
 155-156

syntax
 ASA ACL syntax, 244-245

syslog, configuring, 53-54

tracking, 6
 trends, 4

timing attacks, 139

titles of hackers, 8

top secret data, 3

traceability, 14

tracking threats, 6

transition mechanisms, 97

transport input ssh command, 45

transport mode (IPsec), 169

Trojan horses, 6

true positives, 136

trust exploitation, 11

trusted ports, 78

tuning signatures, 144-147

tunnel mode (IPsec), 169

tunneling, 94

types of firewalls, 125-126

T

TACACS+, 61

Talos, 31

TCP SYN flooding, 12

technical policies, 20

technical threats, 3

testing network security, 24

thinking like a hacker, 9

third generation threats, 5

threats, 2, 35
 blended, 10
 in borderless networks, 8
 categories of, 3
 controlling, 31
 corrective controls, 4
 detective controls, 4
 to email, 103
 evolution of, 5
 hackers
 thinking like, 9
 titles, 8
 impact of, 36
 to IPv6, 95
 preventive controls, 4
 to switching
 Layer 2 attacks, 70-71

U

UDP flooding, 12

unclassified data, 3

untrusted ports, 78

username command, 43-44

users of data, 3

V

verifying site-to-site VPN configuration, 183

view command, 51

views, configuring supervisors, 49-51

viruses, 6

VLAN attacks, 76-78
 mitigating, 76-78

VPNs, 32, 149-150
 classifying, 149-150
 cryptographic processes, 154-157
 deployment modes, 150
 encryption algorithms, 155
 asymmetric, 156
 choosing, 157
 keyspace, choosing, 157
 symmetric, 155-156

IPsec, 167-172
 confidentiality, 170

- hashing algorithms, 170-171
- IKE, 172-175
- key exchange algorithms, 172
- NSA Suite B Standard, 172
- peer authentication methods, 171
- transport versus tunnel
 - mode, 169

- IPv6, 175

- remote-access, 150, 273-274
 - client-based SSL VPNs, 275-286
 - clientless SSL VPNs, 286-294
- site-to-site, 150

- ASA initial configuration,
 - 296-297
- cipher suite options, 178
- configuring, 179-185, 297-301
- ISR IPsec VPN configuration,
 - 294-296
- negotiation steps, 177-178
- planning, 178
- verifying configuration, 183

- VTY access security, 44-46

- vulnerabilities, 2, 35

- IPv6, 96

W

- WASC TC (Web Application Security Consortium Threat Classification), 6
- weakest link architecture, 13

- websites
 - CAPEC, 6
 - ISC, 6
 - MAEC, 6
 - OWASP, 6
 - WASC TC, 6

- white hats, 8
- worms, 6
 - anatomy of, 7
 - mitigating, 7-8

- WSA (Cisco Web Security Appliance),
 - 104-105

X-Y-Z

- zombies, 12
- zone security command, 131-133
- zone-pair command, 132
- zones, 127
- ZPF (Cisco IOS Zone-Based Policy Firewall), 128-134
 - C3PL, 129
 - configuring, 131-134
 - design guidelines, 129
 - rules, 130

This page intentionally left blank

I want to:	Chapter	Page
Configure the management plane on an ASA 5505	19	210
Explain asymmetric encryption	14	161
Explain Cisco Advanced Malware Protection (AMP)	9	101
Explain data loss and exfiltration	1	3
Explain endpoint security, data loss prevention, and endpoint posture assessment	9	99
Explain how to mitigate email threats	9	103
Explain incidence response	2	24
Explain IPv6 security strategy	8	96
Explain MPF service policies	20	266
Explain public key infrastructure	14	162
Explain the basic configuration of an ASA 5505	17	191
Explain the Cisco NFP Framework	4	36
Explain the differences between IPv4 and IPv6	8	91
Explain the Internet Key Exchange protocol	15	172
Explain the IPsec protocol	15	167
Explain threat classification, malicious code, and general security concepts	1	3
Explain threat control guidelines	3	31
Explain VPNs and cryptology	13	154
Identify and explain Layer 2 attacks	7	70
Identify IPv6 threats, vulnerabilities, and mitigating security strategy	8	95-96
Install and run ASDM	18	198
Mitigate ARP attacks	7	80
Mitigate DHCP attacks	7	78
Mitigate network attacks with ACLs	10	112
Mitigate VLAN attacks	7	76
Mitigate address spoofing attacks	7	83
Provide an overview of the ASA	19	205
Provide an overview the different ASDM wizards	18	202
Secure IOS and configuration files	5	42
Secure passwords	5	43
Secure the control plane, management plane, and data plane	4	37-39
Use the AutoSecure feature	4	37