



CCNA Security

Portable Command Guide

All the CCNA Security 640-554 commands
in one compact, portable resource

ciscopress.com

Bob Vachon

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

CCNA Security Portable Command Guide

Bob Vachon

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

CCNA Security Portable Command Guide

Bob Vachon

Copyright © 2012 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.

ISBN-10: 1-58720-448-7

ISBN-13: 978-1-58720-448-7

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing May 2012 with corrections March 2014

Library of Congress Cataloging-in-Publication Data will be inserted once available.

Warning and Disclaimer

This book is designed to provide information about the CCNA Security (640-554 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, fitness is implied.

The information is provided on an “as is” basis. The author, 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.

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.

Publisher

Paul Boger

Associate Publisher

David Dusthimer

Executive Editor

Mary Beth Ray

Manager Global

Certification

Erik Ullanderson

Business Operation

Manager,

Cisco Press

Anand Sundaram

Managing Editor

Sandra Schroeder

Development Editor

Andrew Cupp

Project Editor

Mandie Frank

Copy Editor

Keith Cline

Proofreader

Megan Wade

Technical Editor

Jim Lorenz

Book and

Cover Designer

Gary Adair

Publishing

Coordinator

Vanessa Evans

Composition

Mark Shirar

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.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales.

For more information please contact: U.S. Corporate and Government Sales

1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the U.S. please contact: International Sales international@pearsontech.com



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, CCIP, 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, Gigaset, HomeLink, Internet Quotient, IOS, iPhone, iQuickStudy, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chrome Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, 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. (0812R)

Contents at a Glance

Introduction xvii

Part I: Networking Security Fundamentals

- CHAPTER 1** Networking Security Concepts 1
- CHAPTER 2** Implementing Security Policies Using a Lifecycle Approach 13
- CHAPTER 3** Building a Security Strategy for Borderless Networks 25

Part II: Protecting the Network Infrastructure

- CHAPTER 4** Network Foundation Protection 33
- CHAPTER 5** Protecting the Network Infrastructure Using CCP 39
- CHAPTER 6** Securing the Management Plane 53
- CHAPTER 7** Securing Management Access with AAA 77
- CHAPTER 8** Securing the Data Plane on Catalyst Switches 103
- CHAPTER 9** Securing the Data Plane in IPv6 Environments 119

Part III: Threat Control and Containment

- CHAPTER 10** Planning a Threat Control Strategy 127
- CHAPTER 11** Configuring ACLs for Threat Mitigation 131
- CHAPTER 12** Configuring Zone-Based Firewalls 153
- CHAPTER 13** Configuring Cisco IOS IPS 171

Part IV: Secure Connectivity

- CHAPTER 14** VPNs and Cryptology 195
- CHAPTER 15** Asymmetric Encryption and PKI 207
- CHAPTER 16** IPsec VPNs 213
- CHAPTER 17** Configuring Site-to-Site VPNs 223

Part V: Securing the Network Using the ASA

- CHAPTER 18** Introduction to the ASA 247
- CHAPTER 19** Introduction to ASDM 257
- CHAPTER 20** Configuring Cisco ASA Basic Settings 267
- CHAPTER 21** Configuring Cisco ASA Advanced Settings 283
- CHAPTER 22** Configuring Cisco ASA SSL VPNs 319
- APPENDIX A** Create Your Own Journal Here 335

Contents

Introduction xvii

Part I: Networking Security Fundamentals

CHAPTER 1 Networking Security Concepts 1

Basic Security Concepts	2
Assets, Vulnerabilities, Threats, and Countermeasures	2
Confidentiality, Integrity, and Availability	2
Data Classification Criteria	2
Data Classification Levels	2
Classification Roles	3
Threat Classification	3
Preventive, Detective, and Corrective Controls	3
Risk Avoidance, Transfer, and Retention	4
Drivers for Network Security	4
Evolution of Threats	4
Tracking Threats	5
Malicious Code: Viruses, Worms, and Trojan Horses	5
Anatomy of a Worm	6
Mitigating Malware and Worms	6
Threats in Borderless Networks	7
Hacker Titles	7
Thinking Like a Hacker	8
Reconnaissance Attacks	8
Access Attacks	9
Password Cracking	10
Denial-of-Service Attacks	10
Principles of Secure Network Design	11
Defense in Depth	11

CHAPTER 2 Implementing Security Policies Using a Lifecycle Approach 13

Risk Analysis	13
Quantitative Risk Analysis Formula	14
Quantitative Risk Analysis Example	15
Regulatory Compliance	15

Security Policy	17
Standards, Guidelines, and Procedures	18
Security Policy Audience Responsibilities	19
Security Awareness	19
Secure Network Lifecycle Management	19
Models and Frameworks	21
Assessing and Monitoring the Network Security Posture	21
Testing the Security Architecture	22
Incident Response	22
Incident Response Phases	22
Computer Crime Investigation	23
Collection of Evidence and Forensics	23
Law Enforcement and Liability	23
Ethics	23
Disaster-Recovery and Business-Continuity Planning	23

CHAPTER 3 Building a Security Strategy for Borderless Networks 25

Cisco Borderless Network Architecture	25
Borderless Security Products	26
Cisco SecureX Architecture and Context-Aware Security	26
Cisco TrustSec	28
TrustSec Confidentiality	28
Cisco AnyConnect	29
Cisco Security Intelligence Operations	29
Threat Control and Containment	29
Cloud Security and Data-Loss Prevention	30
Secure Connectivity Through VPNs	31
Security Management	31

Part II: Protecting the Network Infrastructure

CHAPTER 4 Network Foundation Protection 33

Threats Against the Network Infrastructure	33
Cisco Network Foundation Protection Framework	34
Control Plane Security	35
Control Plane Policing	36
Management Plane Security	36
Role-Based Access Control	37
Secure Management and Reporting	37

Data Plane Security	37
ACLs	37
Antispoofing	38
Layer 2 Data Plane Protection	38

CHAPTER 5 Protecting the Network Infrastructure Using CCP 39

Cisco Configuration Professional	39
Cisco Configuration Professional Express	40
Connecting to Cisco CP Express Using the GUI	41
Cisco Configuration Professional	44
Configuring an ISR for CCP Support	44
Installing CCP on a Windows PC	45
Connecting to an ISR Using CCP	45
CCP Features and User Interface	47
Application Menu Options	48
Toolbar Menu Options	48
Toolbar Configure Options	49
Toolbar Monitor Options	49
Using CCP to Configure IOS Device-Hardening Features	49
CCP Security Audit	49
CCP One-Step Lockdown	50
Using the Cisco IOS AutoSecure CLI Feature	51
Configuring AutoSecure via the CLI	51

CHAPTER 6 Securing the Management Plane 53

Planning a Secure Management and Reporting Strategy	54
Securing the Management Plane	54
Securing Passwords	55
Securing the Console Line and Disabling the Auxiliary Line	55
Securing VTY Access with SSH	56
Securing VTY Access with SSH Example	57
Securing VTY Access with SSH Using CCP Example	58
Securing Configuration and IOS Files	60
Restoring Bootset Files	61
Implementing Role-Based Access Control on Cisco Routers	62
Configuring Privilege Levels	62
Configuring Privilege Levels Example	62
Configuring RBAC via the CLI	62
Configuring RBAC via the CLI Example	63

Configuring Superviews	63
Configuring a Superview Example	64
Configuring RBAC Using CCP Example	64
Network Monitoring	67
Configuring a Network Time Protocol Master Clock	67
Configuring an NTP Client	67
Configuring an NTP Master and Client Example	67
Configuring an NTP Client Using CCP Example	68
Configuring Syslog	69
Configuring Syslog Example	71
Configuring Syslog Using CCP Example	71
Configuring SNMP	74
Configuring SNMP Using CCP	74

CHAPTER 7 Securing Management Access with AAA 77

Authenticating Administrative Access	78
Local Authentication	78
Server-Based Authentication	78
Authentication, Authorization, and Accounting Framework	79
Local AAA Authentication	79
Configuring Local AAA Authentication Example	80
Configuring Local AAA Authentication Using CCP Example	81
Server-Based AAA Authentication	86
TACACS+ Versus RADIUS	86
Configuring Server-Based AAA Authentication	87
Configuring Server-Based AAA Authentication Example	88
Configuring Server-Based AAA Authentication Using CCP Example	89
AAA Authorization	94
Configuring AAA Authorization Example	94
Configuring AAA Authorization Using CCP	94
AAA Accounting	98
Configuring AAA Accounting Example	98
Cisco Secure ACS	98
Adding a Router as a AAA Client	99
Configuring Identity Groups and an Identity Store	99
Configuring Access Service to Process Requests	100
Creating Identity and Authorization Policies	101

CHAPTER 8 Securing the Data Plane on Catalyst Switches 103

Common Threats to the Switching Infrastructure	104
Layer 2 Attacks	104
Layer 2 Security Guidelines	104
MAC Address Attacks	105
Configuring Port Security	105
Fine-Tuning Port Security	106
Configuring Optional Port Security Settings	107
Configuring Port Security Example	108
Spanning Tree Protocol Attacks	109
STP Enhancement Features	109
Configuring STP Enhancement Features	110
Configuring STP Enhancements Example	111
LAN Storm Attacks	112
Configuring Storm Control	112
Configuring Storm Control Example	113
VLAN Hopping Attacks	113
Mitigating VLAN Attacks	114
Mitigating VLAN Attacks Example	114
Advanced Layer 2 Security Features	115
ACLs and Private VLANs	116
Cisco Integrated Security Features	116
Secure the Switch Management Plane	117

CHAPTER 9 Securing the Data Plane in IPv6 Environments 119

Overview of IPv6	119
Comparison Between IPv4 and IPv6	119
The IPv6 Header	120
ICMPv6	121
Stateless Autoconfiguration	122
IPv4-to-IPv6 Transition Solutions	122
IPv6 Routing Solutions	122
IPv6 Threats	123
IPv6 Vulnerabilities	124
IPv6 Security Strategy	124
Configuring Ingress Filtering	124
Secure Transition Mechanisms	125
Future Security Enhancements	125

Part III: Threat Control and Containment**CHAPTER 10 Planning a Threat Control Strategy 127**

- Threats 127
 - Trends in Information Security Threats 127
- Threat Control Guidelines 128
 - Threat Control Design Guidelines 128
- Integrated Threat Control Strategy 129
 - Cisco Security Intelligence Operations 130

CHAPTER 11 Configuring ACLs for Threat Mitigation 131

- Access Control List 131
 - Mitigating Threats Using ACLs 132
 - ACL Design Guidelines 132
 - ACL Operation 132
- Configuring ACLs 134
 - ACL Configuration Guidelines 134
 - Filtering with Numbered Extended ACLs 134
 - Configuring a Numbered Extended ACL Example 135
 - Filtering with Named Extended ACLs 135
 - Configuring a Named Extended ACL Example 136
 - Configuring an Extended ACL Using CCP Example 136
- Enhancing ACL Protection with Object Groups 140
 - Network Object Groups 140
 - Service Object Groups 140
 - Using Object Groups in Extended ACLs 141
 - Configuring Object Groups in ACLs Example 142
 - Configuring Object Groups in ACLs Using CCP Example 144
- ACLs in IPv6 149
 - Mitigating IPv6 Attacks Using ACLs 149
 - IPv6 ACLs Implicit Entries 149
 - Filtering with IPv6 ACLs 149
 - Configuring an IPv6 ACL Example 151

CHAPTER 12 Configuring Zone-Based Firewalls 153

- Firewall Fundamentals 153
 - Types of Firewalls 154

Firewall Design	154
Firewall Policies	154
Firewall Rule Design Guidelines	155
Cisco IOS Firewall Evolution	155
Cisco IOS Zone-Based Policy Firewall	156
Cisco Common Classification Policy Language	156
ZFW Design Considerations	156
Default Policies, Traffic Flows, and Zone Interaction	157
Configuring an IOS ZFW	157
Configuring an IOS ZFW Using the CLI Example	160
Configuring an IOS ZFW Using CCP Example	161
Configuring NAT Services for ZFWs Using CCP Example	167

CHAPTER 13 Configuring Cisco IOS IPS 171

IDS and IPS Fundamentals	171
Types of IPS Sensors	172
Types of Signatures	172
Types of Alarms	172
Intrusion Prevention Technologies	173
IPS Attack Responses	174
IPS Anti-Evasion Techniques	175
Managing Signatures	175
Cisco IOS IPS Signature Files	176
Implementing Alarms in Signatures	176
IOS IPS Severity Levels	177
Event Monitoring and Management	177
IPS Recommended Practices	178
Configuring IOS IPS	178
Creating an IOS IPS Rule and Specifying the IPS Signature File Location	179
Tuning Signatures per Category	180
Configuring IOS IPS Example	183
Configuring IOS IPS Using CCP Example	185
Signature Tuning Using CCP	193

Part IV: Secure Connectivity

CHAPTER 14 VPNs and Cryptology 195

Virtual Private Networks	195
VPN Deployment Modes	196

Cryptology = Cryptography + Cryptanalysis	197
Historical Cryptographic Ciphers	197
Modern Substitution Ciphers	198
Encryption Algorithms	198
Cryptanalysis	199
Cryptographic Processes in VPNs	200
Classes of Encryption Algorithms	201
Symmetric Encryption Algorithms	201
Asymmetric Encryption Algorithm	202
Choosing an Encryption Algorithm	202
Choosing an Adequate Keyspace	202
Cryptographic Hashes	203
Well-Known Hashing Algorithms	203
Hash-Based Message Authentication Codes	203
Digital Signatures	204

CHAPTER 15 Asymmetric Encryption and PKI 207

Asymmetric Encryption	207
Public Key Confidentiality and Authentication	207
RSA Functions	208
Public Key Infrastructure	208
PKI Terminology	209
PKI Standards	209
PKI Topologies	210
PKI Characteristics	211

CHAPTER 16 IPsec VPNs 213

IPsec Protocol	213
IPsec Protocol Framework	214
Encapsulating IPsec Packets	215
Transport Versus Tunnel Mode	215
Confidentiality Using Encryption Algorithms	216
Data Integrity Using Hashing Algorithms	216
Peer Authentication Methods	217
Key Exchange Algorithms	217
NSA Suite B Standard	218
Internet Key Exchange	218
IKE Negotiation Phases	219
IKEv1 Phase 1 (Main Mode and Aggressive Mode)	219

IKEv1 Phase 2 (Quick Mode)	220
IKEv2 Phase 1 and 2	220
IKEv1 Versus IKEv2	221
IPv6 VPNs	221

CHAPTER 17 Configuring Site-to-Site VPNs 223

Site-to-Site IPsec VPNs	223
IPsec VPN Negotiation Steps	223
Planning an IPsec VPN	224
Cipher Suite Options	225
Configuring IOS Site-to-Site VPNs	225
Verifying the VPN Tunnel	229
Configuring a Site-to-Site IPsec VPN Using IOS Example	230
Configuring a Site-to-Site IPsec VPN Using CCP Example	232
Generating a Mirror Configuration Using CCP	241
Testing and Monitoring IPsec VPNs	242
Monitoring Established IPsec VPN Connections Using CCP	244

Part V: Securing the Network Using the ASA

CHAPTER 18 Introduction to the ASA 247

Adaptive Security Appliance	247
ASA Models	248
Routed and Transparent Firewall Modes	249
ASA Licensing	249
Basic ASA Configuration	251
ASA 5505 Front and Back Panel	251
ASA 5510 Front and Back Panel	252
ASA Security Levels	253
ASA 5505 Port Configuration	255
ASA 5505 Deployment Scenarios	255
ASA 5505 Configuration Options	255

CHAPTER 19 Introduction to ASDM 257

Adaptive Security Device Manager	257
Accessing ASDM	258
Factory Default Settings	258
Resetting the ASA 5505 to Factory Default Settings	259
Erasing the Factory Default Settings	259
Setup Initialization Wizard	259

Installing and Running ASDM 260

 Running ASDM 262

ASDM Wizards 264

 The Startup Wizard 264

 VPN Wizards 265

 Advanced Wizards 266

CHAPTER 20 Configuring Cisco ASA Basic Settings 267

ASA Command-Line Interface 267

 Differences Between IOS and ASA OS 268

Configuring Basic Settings 268

 Configuring Basic Management Settings 269

 Enabling the Master Passphrase 269

Configuring Interfaces 270

 Configuring the Inside and Outside SVIs 270

 Assigning Layer 2 Ports to VLANs 271

 Configuring a Third SVI 272

Configuring the Management Plane 272

 Enabling Telnet, SSH, and HTTPS Access 272

 Configuring Time Services 274

Configuring the Control Plane 274

 Configuring a Default Route 274

Basic Settings Example 274

 Configuring Basic Settings Example Using the CLI 275

 Configuring Basic Settings Example Using ASDM 277

CHAPTER 21 Configuring Cisco ASA Advanced Settings 283

ASA DHCP Services 284

 DHCP Client 284

 DHCP Server Services 284

 Configuring DHCP Server Example Using the CLI 285

 Configuring DHCP Server Example Using ASDM 287

ASA Objects and Object Groups 289

 Network and Service Objects 289

 Network, Protocol, ICMP, and Service Object Groups 291

 Configuring Objects and Object Groups Example Using
 ASDM 293

ASA ACLs	295
ACL Syntax	296
Configuring ACLs Example Using the CLI	297
Configuring ACLs with Object Groups Example Using the CLI	299
Configuring ACLs with Object Groups Example Using ASDM	300
ASA NAT Services	301
Auto-NAT	302
Dynamic NAT, Dynamic PAT, and Static NAT	302
Configuring Dynamic and Static NAT Example Using the CLI	304
Configuring Dynamic NAT Example Using ASDM	306
AAA Access Control	308
Local AAA Authentication	308
Server-Based AAA Authentication	309
Configuring AAA Server-Based Authentication Example Using the CLI	309
Configuring AAA Server-Based Authentication Example Using ASDM	310
Modular Policy Framework Service Policies	313
Class Maps, Policy Maps, and Service Policies	314
Default Global Policies	317
Configure Service Policy Example Using ASDM	318
CHAPTER 22 Configuring Cisco ASA SSL VPNs	319
Remote-Access VPNs	319
Types of Remote-Access VPNs	319
ASA SSL VPN	320
Client-Based SSL VPN Example Using ASDM	321
Clientless SSL VPN Example Using ASDM	328
APPENDIX Create Your Own Journal Here	335

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, either working in his gardens or white-water canoe tripping.

About the Technical Reviewer

Jim Lorenz is an instructor and a senior training developer for the Cisco Networking Academy Program. He holds a bachelor's degree in computer information systems and has over 20 years of experience in networking and IT. Jim has developed course materials, including content, labs, and textbooks for the CCNA and CCNP curricula. Most recently he coordinated lab development for the CCNA Security course.

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 who, 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. Thank you Mary Beth for believing in me and to Drew and Mandie for making sure I got things done right and on time. Also thanks to my friend Jim for keeping me in check.

Special thanks to my Cisco Networking Academy family. A big thanks to Jeremy and Rob 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!

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 very 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 640-554 IINS (Implementing Cisco IOS Network Security) certification exam. The guide begins by summarizing the required fundamental security concepts. It then provides the CLI commands and the Cisco Configuration Professional GUI screenshots required to secure an ISR. Examples are included to help demonstrate the security-related configuration.

The last section 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 1841 ISR running Cisco IOS advanced IP services software release 12.4(20)T1 and the Cisco Configuration Professional GUI version 2.6
- Cisco ASA 5505 running Cisco Adaptive Security Appliance software version 8.4(2) with a Base License and the ASA Security Device Manager (ASDM) GUI version 6.4(5)

Who Should Read This Book

This book is for those people preparing for the CCNA Security (640-554 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. It is small enough that you will find it easy to carry around with you. Big, heavy textbooks might look impressive on your bookshelf in your office, but can you really carry them all around with you when you are working in some server room or equipment closet somewhere?

Organization of This Book

The parts of this book cover the following topics:

- **Part I, “Network 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 and CCP.
- **Part III, “Threat Control and Containment”**—Describes how to secure an ISR against network threats using the IOS CLI configuration commands and CCP to configure ACLs, 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 and CCP.
- **Part V, “Securing the Network Using the ASA”**—Describes how to secure a network using an 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 CCP.

This page intentionally left blank

Network Foundation Protection

The chapter covers the following topics:

Threats Against the Network Infrastructure

Cisco Network Foundation Protection Framework

Control Plane Security

- Control Plane Policing

Management Plane Security

- Role-Based Access Control
- Secure Management and Reporting

Data Plane Security

- ACLs
- Antispoofing
- Layer 2 Data Plane Protection

Threats Against the Network Infrastructure

Common vulnerabilities and threats against a network infrastructure include the following:

Vulnerabilities	<ul style="list-style-type: none"> ▪ Design errors ▪ Protocol weaknesses ▪ Software vulnerabilities ▪ Device misconfiguration
Threats	<ul style="list-style-type: none"> ▪ Trust exploitation ▪ Login, authentication, and password attacks ▪ Routing protocol exploits ▪ Spoofing ▪ Denial of service (DoS) ▪ Confidentiality and integrity attacks

The impact of those threats and vulnerabilities includes the following:

Impact	<ul style="list-style-type: none"> ■ Exposed management credentials ■ High CPU usage ■ Loss of protocol keepalives and updates ■ Route flaps and major network transitions ■ Slow or unresponsive management sessions ■ Indiscriminate packet drops
---------------	---

Cisco Network Foundation Protection Framework

The Cisco Network Foundation Protection (NFP) framework provides an umbrella strategy for infrastructure protection forming the foundation for continuous service delivery.

NFP logically divides a router and Catalyst switches into three functional areas:

Control plane	Provides the ability to route data correctly. Traffic consists of device-generated packets required for the operation of the network itself, such as Address Resolution Protocol (ARP) message exchanges or Open Shortest Path First (OSPF) protocol routing advertisements.
Management plane	Provides the ability to manage network elements. Traffic is generated either by network devices or network management stations using tools such as Telnet, Secure Shell (SSH), Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Network Time Protocol (NTP), or Simple Network Management Protocol (SNMP).
Data plane (forwarding plane)	Provides the ability to forward data. Typically consists of user-generated packets being forwarded to another end station. Most traffic travels through the router via the data plane. Data plane packets are typically processed in fast-switching cache.

Figure 4-1 provides a conceptual view of the NFP framework.

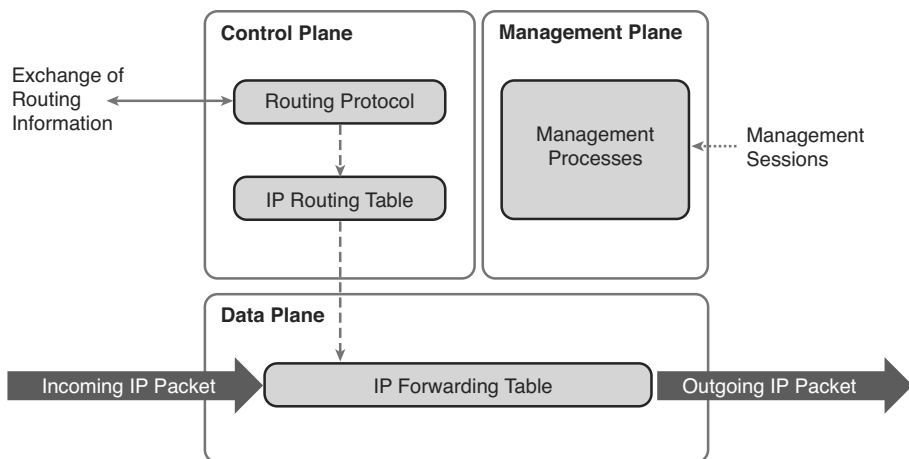


Figure 4-1 NFP Planes

Each of these planes must be protected to provide network availability and ensure continuous service delivery. The Cisco NFP framework provides the tools and techniques to secure each of these planes.

Control Plane Security

Control plane security can be implemented using the following features:

Cisco AutoSecure	Cisco AutoSecure provides a one-step device lockdown feature to protect the control plane and the management and data planes. It is a script that is initiated from the command-line interface (CLI) to configure the security posture of routers and disables nonessential system processes and services. It first makes recommendations to address security vulnerabilities and then modifies the router configuration.
Routing protocol authentication	Neighbor authentication prevents a router from accepting fraudulent routing updates. Most routing protocols support neighbor authentication.
CoPP	Control Plane Policing (CoPP) is used on higher-end Cisco devices with route processors. It is a Cisco IOS feature designed to enable users to manage the flow of traffic managed by the route processor of their network devices.

Control Plane Policing

CoPP is designed to prevent unnecessary traffic from overwhelming the route processor. The CoPP feature treats the control plane as a separate entity with its own ingress (input) and egress (output) ports. Because the CoPP feature treats the control plane as a separate entity, a set of rules can be established and associated with the ingress and egress ports of the control plane.

CoPP consists of the following features:

CoPP	Control Plane Policing lets users configure a QoS filter that manages the traffic flow of control plane packets. This protects the control plane against reconnaissance and DoS attacks.
CPPr	Control Plane Protection is an extension of CoPP but allows a finer policing granularity. For example, CPPr can filter and rate-limit the packets that are going to the control plane of the router and discard malicious and error packets (or both).
Control Plane Logging	The Control Plane Logging feature enables logging of the packets that CoPP or CPPr drop or permit. It provides the logging mechanism that is needed to deploy, monitor, and troubleshoot CoPP features efficiently.

Management Plane Security

Management plane security can be implemented using the following features:

Login and password policy	Restrict device accessibility. Limit the accessible ports and restrict the “who” and “how” methods of access.
Role-based access control	Ensure access is only granted to authenticated users, groups, and services. Role-based access control (RBAC) and authentication, authorization, and accounting (AAA) services provide mechanisms to effectively authenticate access.
Authorize actions	Restrict the actions and views that are permitted by any particular user, group, or service.
Secure management access and reporting	Log and account for all access. Record who accessed the device, what occurred, and when it occurred.
Ensure the confidentiality of data	Protect locally stored sensitive data from being viewed or copied. Use management protocols with strong authentication to mitigate confidentiality attacks aimed at exposing passwords and device configurations.
Present legal notification	Display legal notice developed with legal counsel.

Role-Based Access Control

RBAC restricts user access based on the role of the user. Roles are created for job or task functions and assigned access permissions to specific assets. Users are then assigned to roles and acquire the permissions that are defined for the role.

In Cisco IOS, the role-based CLI access feature implements RBAC for router management access. The feature creates different “views” that define which commands are accepted and what configuration information is visible. For scalability, users, permissions, and roles are usually created and maintained in a central repository server. This makes the access control policy available to multiple devices using it.

The central repository server can be a AAA server such as the Cisco Secure Access Control System (ACS) to provide AAA services to a network for management purposes.

Secure Management and Reporting

The management network is a very attractive target to hackers. For this reason, the management module has been built with several technologies designed to mitigate such risks.

The information flow between management hosts and the managed devices can be out-of-band (OOB) (information flows within a network on which no production traffic resides) or in-band (information flows across the enterprise production network, the Internet, or both).

Data Plane Security

Data plane security can be implemented using the following features:

Access control lists	Access control lists (ACLs) perform packet filtering to control which packets move through the network and where.
Antispoofing	ACLs can be used as an antispoofing mechanism that discards traffic that has an invalid source address.
Layer 2 security features	Cisco Catalyst switches have integrated features to help secure the Layer 2 infrastructure.

ACLs

ACLs are used to secure the data plane in a variety of ways, including the following:

Block unwanted traffic or users	ACLs can filter incoming or outgoing packets on an interface, controlling access based on source addresses, destination addresses, or user authentication.
Reduce the chance of DoS attacks	ACLs can be used to specify whether traffic from hosts, networks, or users can access the network. The TCP intercept feature can also be configured to prevent servers from being flooded with requests for a connection.

Mitigate spoofing attacks	ACLs enable security practitioners to implement recommended practices to mitigate spoofing attacks.
Provide bandwidth control	ACLs on a slow link can prevent excess traffic.
Classify traffic to protect other planes	ACLs can be applied on vty lines (management plane). ACLs can control routing updates being sent, received, or redistributed (control plane).

Antispoofing

Implementing the IETF best current practice 38 (BCP38) and RFC 2827 ingress traffic filtering renders the use of invalid source IP addresses ineffective, forcing attacks to be initiated from valid, reachable IP addresses which could be traced to the originator of an attack.

Features such as Unicast Reverse Path Forwarding (uRPF) can be used to complement the antispoofing strategy.

Layer 2 Data Plane Protection

The following are Layer 2 security tools integrated into the Cisco Catalyst switches:

Port security	Prevents MAC address spoofing and MAC address flooding attacks
DHCP snooping	Prevents client attacks on the Dynamic Host Configuration Protocol (DHCP) server and switch
Dynamic ARP inspection (DAI)	Adds security to ARP by using the DHCP snooping table to minimize the impact of ARP poisoning and spoofing attacks
IP source guard	Prevents IP spoofing addresses by using the DHCP snooping table