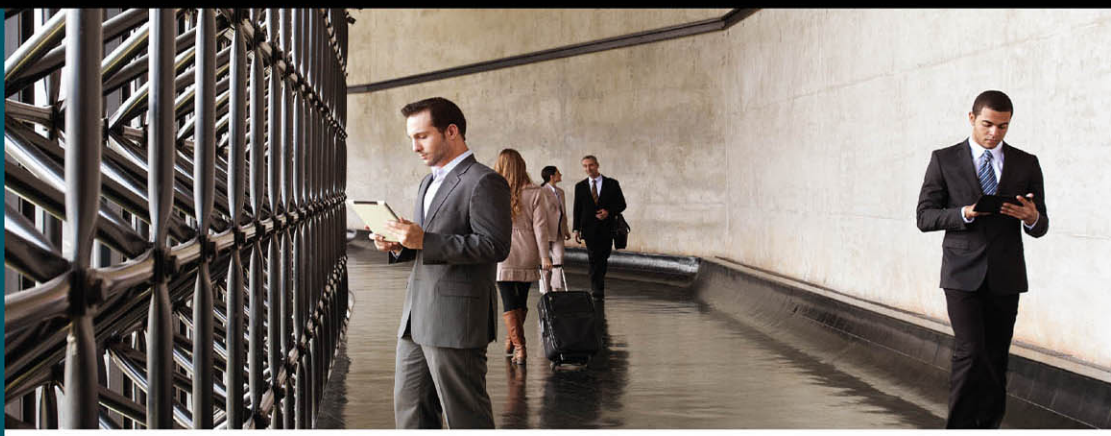

CCNA Security
Portable Command Guide

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

ciscopress.com

Bob Vachon

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

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

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.**

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

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

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.

CHAPTER 3

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: ■ 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.

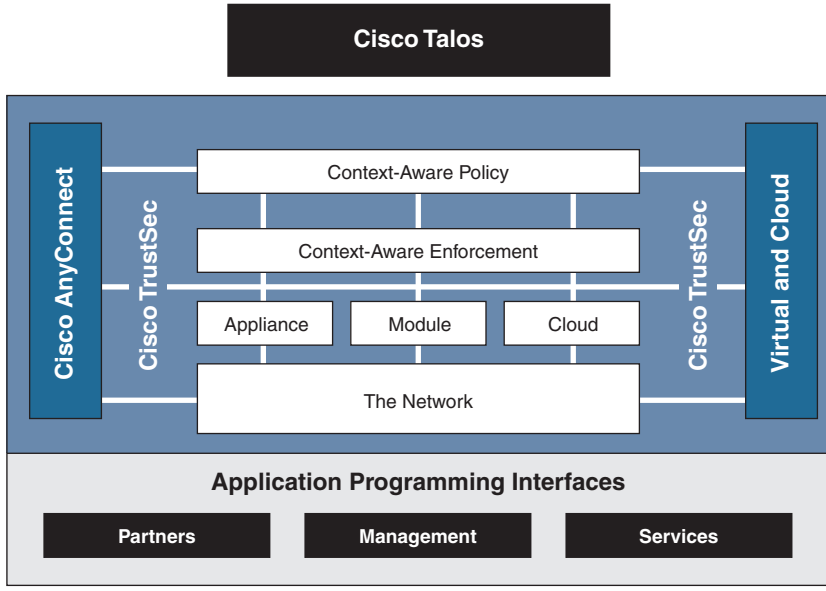

Figure 3-1 Cisco SecureX Components

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

Index

Numerics

A

B

C

D

E

F

G

H

I

J-K

L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z

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