CCIE Security v4.0 Quick Reference

Lancy Lobo
Umesh Lakshman

Cisco Press

CCIE Security v4.0 Quick Reference

Third Edition

Lancy Lobo
Umesh Lakshman

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

CCIE Security v4.0 Quick Reference, Third Edition

Lancy Lobo
Umesh Lakshman

Published by:

Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

ISBN-13: 978-0-13-385508-1

ISBN-10: 0-13-385508-2

Warning and Disclaimer

This book is designed to provide information about networking and provide some assistive guidelines and topics to prepare for the CCIE Security written exam. 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 international@pearsoned.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: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Marianne Bartow

Senior Project Editor: Tonya Simpson

Technical Editor(s): Shankar N. Satyanarayanan

Editorial Assistant: Vanessa Evans

Composition: TnT Design, Inc.

Proofreader: Kathy Ruiz

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(s)

Lancy Lobo, CCIE No. 4690 (Routing and Switching, Service Provider, Security), is a senior systems engineer in the Cisco Systems Sales organization that supports a large service provider. Previously, he was a network consulting engineer in the Cisco Systems Advanced Services organization, which supports Cisco strategic service provider and enterprise customers. He has more than 14 years of experience with data-communication technologies and protocols. He has supported several Cisco strategic service provider customers to design and implement large-scale routed networks. Lancy holds a Bachelor's degree in electronics and telecommunication engineering from Bombay University and a dual management degree from Jones International University.

Umesh Lakshman is a systems engineer within the public sector organization and is currently supporting the higher education accounts in the Bay Area. Prior to taking on this role, he was the technical lead at the Customer Proof of Concept Labs (CPOC) team at Cisco, where he supported Cisco sales teams by demonstrating advanced technologies, such as Multiprotocol Label Switching (MPLS) and high-end routing with the Cisco CRS-1 and ASR 9000, to customers in a presales environment. Umesh has conducted several customer-training sessions for MPLS and service-provider architectural designs. He holds a Bachelor's degree in electrical and electronics engineering from Madras University and a Master's degree in electrical and computer engineering from Wichita State University.

About the Technical Reviewers

Shankar N. Satyanarayanan is a systems engineer with the Service Provider organization at Cisco Systems. Shankar has 14 years of service provider networking experience in various roles within Cisco. Prior to his current role, Shankar worked on the software development team and has designed and developed software code on Cisco IOS and Cisco IOS-XR for Cisco high-end routing platforms, such as CRS, C12K, and MGX products. In this role, he designed and developed complex software modules for security, routing, and infrastructure areas such as lawful intercept, control plane policing, port mirroring, link aggregation, IP header compression, and system infrastructure. Shankar joined the service provider account team in 2010 and supports one of the largest service provider accounts at Cisco. In this role, he has been responsible for designing and developing a large business VPN network. As lead systems engineer he was responsible for dealing with the network and security designs for large VPN implementations such as scalable and secure route reflectors, perimeter ACLs, and secure option B interfaces. Shankar's primary focus today is the design and architecture of the mobility backhaul network for the same customer. Shankar holds a Master's degree in Computer Sciences (Networking) from the University of Missouri, Kansas City, and has completed courses in management sciences and engineering from Stanford University. Shankar lives in Edison, New Jersey with his wife, Smita, and two children, Pranav and Akshara.

Dedications

This book is dedicated to Natasha and my two daughters, Elena and Keira. Without their support, this endeavor wouldn’t have been possible.

—Lancy

I would like to dedicate my work on this book to my wife, Malathy. You have been everything a man can ask for in a wife and more. Everything I have achieved would not have been possible without your support.

—Umesh

Acknowledgments

We would like to thank Shankar Satyanarayanan for providing his technical knowledge in editing this book. He has been very diligent in providing his feedback to help improve *CCIE Security v4.0 Quick Reference*.

Contents at a Glance

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).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

CCIE Security v4.0 Quick Reference is an exam preparation tool that provides a quick and concise review of all the key topics on the CCIE Security written exam.

This document reviews topics on networking theory, security protocols, hash algorithms, data encryption standards, application protocols, security appliances, security applications, and solutions.

This page intentionally left blank

This page intentionally left blank

Chapter 3

Application and Infrastructure Security

HTTP

HTTP is a request/response protocol between clients (user agents) and servers (origin servers) that is used to access web-related services and pages. An HTTP client initiates a request by establishing a TCP connection to a particular port on a remote host (port 80 by default). Resources to be accessed by HTTP are identified using uniform resource identifiers (URI or URL) using the http: or https: URI schemes.

HTTP supports authentication between clients and servers, which involves sending a clear-text password (not secure). HTTP is disabled by default on Cisco routers, but can be enabled for remote monitoring and configuration.

Configuring HTTP

Use the **ip http access-class** command to restrict access to specific IP addresses, and employ the **ip http authentication** command to enable only certain users to access the Cisco router via HTTP.

If you choose to use HTTP for management, issue the **ip http access-class** *access-list-number* command to restrict access to specific IP addresses. As with interactive logins, the best choice for HTTP authentication is a TACACS+ or RADIUS server. Avoid using the enable password as an HTTP password.

The **ip http-server** command supports the HTTP server. If a secure HTTP connection is required, **ip http secure-server** must be configured on the router. The default HTTP port 80 can be changed by using the command **ip http port** *port-number*. Varying forms of authentication for login can be set using the **ip http authentication** [**enable** | **local** | **tacacs** | **aaa**] command. However, to initiate the default login method you must enter the hostname as the username and the enable or secret password as the password. If local authentication is specified by using **username** *username* **privilege** [**0-15**] **password** *password*, the access level on the Cisco router is determined by the privilege level assigned to that user.

HTTPS

Secure HTTP, or HTTPS, offers a secure connection to an HTTPS server. It uses SSL and TLS (transport layer security) to provide authentication and data encryption.

An HTTPS client initiates a request by establishing a TCP connection to a particular port on a remote host (port 443 by default). Resources to be accessed by HTTPS are identified using URIs or URLs using the HTTPS URI schemes.

When a client connects to the secure HTTPS port, it first authenticates to the server by using the server's digital certificate. The client then negotiates the security protocols to be used for the connection with the server and generates session keys for encryption and decryption purposes. If the authentication fails, the client cannot establish a secure encrypted session and the security protocol negotiation does not proceed.

Configuring HTTPS

Use the **ip http access-class** command to restrict access-specific IP addresses, and employ **ip http authentication** to enable only certain users to access the Cisco router via HTTP.

If you choose to use HTTP for management, issue the **ip http access-class** *access-list-number* command to restrict access to appropriate IP addresses. As with interactive logins, the best choice for HTTP authentication is a TACACS+ or RADIUS server. Avoid using the enable password as an HTTP password.

The **ip http secure-server** command enables the HTTPS server. HTTP authentication for login can be set using the **ip http authentication** [**enable** | **local** | **tacacs** | **aaa**] command. All default login methods and local authentication methods supported are the same as mentioned in the section, "HTTP."

The **ip http secure-port** command can set the HTTPS port number from the default value of 443, if required.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is a text-based method commonly used by two mail servers to exchange email. Users can then retrieve email from the servers via mail clients such as Outlook, Eudora, or Pine. Mail clients employ various protocols, such as Post Office Protocol 3 (POP3), to connect to the server.

SMTP uses well-known ports TCP port 25 and UDP port 25. The client and SMTP server send various commands when communicating. Table 3-1 lists some SMTP commands and their purposes.

Table 3-1 *SMTP Commands*

Command	Function
HELLO (HELO)	Identifies the SMTP client to the SMTP server.
MAIL (MAIL)	Initiates a mail transaction in which the mail data is delivered to an SMTP server, that is either transported to mailboxes or passed to another system via SMTP.
RECIPIENT (RCPT)	Identifies an individual recipient of the mail data. Various methods of the command are needed for multiple users.
DATA (DATA)	Identifies the lines following the command (such as the MAIL command) as the mail data in ASCII character codes.
SEND (SEND)	Initiates a mail transaction in which the mail data is delivered to one or more terminals.
SEND OR MAIL (SOML)	Initiates a mail transaction in which the mail data is delivered to one or more terminals OR mailboxes.
SEND AND MAIL (SAML)	Initiates a mail transaction in which the mail data is delivered to one or more terminals AND mailboxes.
RESET (RSET)	Aborts the current mail transaction. Any stored sender, recipients, and mail data must be discarded, and all buffers and state tables must be cleared. The receiver must send an OK reply.
VERIFY (VRFY)	Verifies whether a user exists. A fully specified mailbox and name are returned.
NOOP (NOOP)	Specifies no action other than that the receiver sent an OK reply.
QUIT (QUIT)	Closes the transmission channel. The receiver must send an OK reply.

File Transfer Protocol

File Transfer Protocol (FTP) enables users to transfer files from one host to another. FTP is a TCP-based connection-oriented protocol and uses port 21 to open the connection and port 20 to transfer data. FTP uses clear-text authentication. FTP clients can be configured for two modes of operation: PORT (active) mode and PASV (passive) mode. Figure 3-1 shows FTP modes of operation between an FTP client and FTP server for both the active and passive mode.

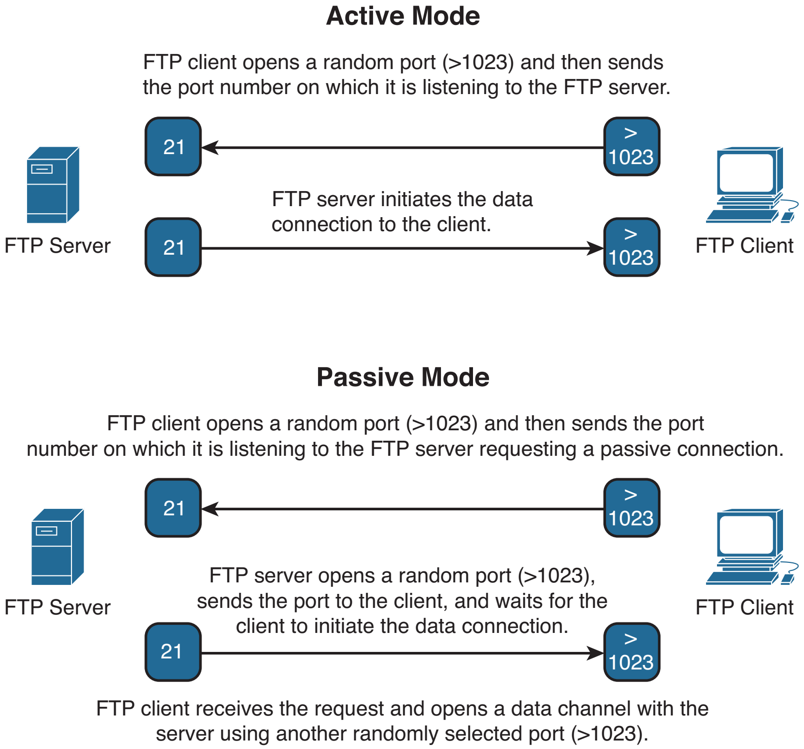
Active Mode
FTP client opens a random port (>1023) and then sends the port number on which it is listening to the FTP server.
21
> 1023
FTP Server
FTP server initiates the data connection to the client.
21
> 1023
FTP Client
Passive Mode
FTP client opens a random port (>1023) and then sends the port number on which it is listening to the FTP server requesting a passive connection.
21
> 1023
FTP Server
FTP server opens a random port (>1023), sends the port to the client, and waits for the client to initiate the data connection.
21
> 1023
FTP Client
FTP client receives the request and opens a data channel with the server using another randomly selected port (>1023).

Figure 3-1 *Overview of FTP Operation and Operating Modes*

In active mode, the FTP client opens a random port (greater than 1023), sends the FTP server the random port number on which it is listening over the control stream, and waits for a connection from the FTP server. When the FTP server initiates the data connection to the FTP client, it binds the source port to port 20 on the FTP server. Active FTP is less secure than passive mode because the FTP server initiates the data channel, which means opening port 20 to the outside world, which is less secure than using port 21. In active mode, the FTP server initiates the FTP data channel.

In passive mode, the FTP server opens a random port (greater than 1023), sends the FTP client the port on which it is listening over the control stream, and waits for a connection from the FTP client. In this case, the FTP client binds the source port of the connection to a random port greater than 1023. In passive FTP the client initiated both the control connection and the data connection.

Domain Name System

Domain Name System (DNS) is a name resolution protocol that translates hostnames to IP addresses and vice versa. A DNS server is a host that runs the DNS service and is configured to process the translation for the user transparently by using TCP/UDP port 53. TCP port 53 is also used for DNS zone transfers. UDP 53 is used for DNS lookups and browsing.

DNS is a hierarchical database where the data is structured in a tree, with the root domain (.) at the top. Various subdomains branch out from the root, much like the directory structure of a UNIX or Windows file system. Cisco routers can be configured for DNS lookups so that users can simply type a hostname versus an IP address. Local names can also be statically configured for devices. A name server stores information about its domain in the form of several kinds of resource records, each of which stores a different kind of information about the domain and the hosts in the domain. These records are traditionally text entries stored in different files on the domain name server. The Cisco DNM browser is a graphical utility that enables you to edit these records via a graphical interface, which reduces the chance of errors in text files. A router does not provide DNS server responses to client devices such as PCs or UNIX hosts. Table 3-2 describes the different record types.

Table 3-2 *Different DNS Record Types*

Record Type	Function
Start of Authority (SOA)	Required for every domain. Stores information about the DNS itself for the domain
Name Server (NS)	Stores information used to identify the name servers in the domain that store information for that domain
Address (A)	Stores the hostname and IP address of individual hosts and translates hostnames to IP addresses
Canonical Name (CNAME)	Stores additional hostnames, or aliases, for hosts in the domain
Mail Exchange (MX)	Stores information about where mail for the domain should be delivered
Pointer (PTR)	Stores the IP address and hostname of individual hosts and translates IP addresses to hostnames in a reverse DNS lookup
Host Information (HINFO)	Stores information about the hardware for specific hosts
Well Known Services (WKS)	Stores information about the various network services available from hosts in the domain
Text Information (TXT)	Stores up to 256 characters of text per line
Responsible Person (RP)	Stores information about the person responsible for the domain

Trivial File Transfer Protocol

Trivial File Transfer Protocol (TFTP) uses UDP port 69 to transfer files between devices. Data transfer occurs between two UDP ports, where one is the source and the other the destination. TFTP is considered to possess weak security because the TFTP packet has no fields to authenticate with a username and password. Therefore, security is enabled by predefinition of the directories and filenames of files to be transferred to the TFTP server. This enables the remote hosts to TFTP the file from the remote TFTP client or