CCIE Security v3.0 Quick Reference

Lancy Lobo
Umesh Lakshman

Cisco Press

CCIE Security v3.0

Quick Reference

Lancy Lobo
Umesh Lakshman

ciscopress.com

Table of Contents

About the Authors

Lancy Lobo, CCIE No. 4690 (Routing and Switching, Service Provider, Security), is a 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. He is currently pursuing a Ph.D. in organizational management at Capella University.

Umesh Lakshman is a systems engineer with the Customer Proof of Concept Labs (CPOC) team at Cisco, where he supports Cisco sales teams by demonstrating advanced technologies, such as Multiprotocol Label Switching (MPLS) and high-end routing with the Cisco CRS-1 and Cisco 12000 series, to customers in a presales environment. Umesh has conducted several customer-training ses-sions for MPLS and service provider architectural designs. Umesh has 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.

 Please see page 131 for more details.

Introduction

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

With this document as your guide, you will review topics on networking theory, security protocols, hash algorithms, data encryp-tion standards, application protocols, security appliances, security applications, and solutions.

 Please see page 131 for more details.

Chapter 3
Application Protocols

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 it 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 use the **ip http authentication** command to allow 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 enables the HTTP server. If a secure HTTP connection is required, **ip http secure-server** needs to 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, the default login method is to enter the hostname as the username and the enable or secret password as the password. If local

 Please see page 131 for more details.

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 provides the ability to connect to a HTTPS server securely. 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, he first authenticates to the server by using the server's digital certificate. The client then negotiates the security protocols it will use 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 use **ip http authentication** to allow 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.

 Please see page 131 for more details.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is a text-based protocol usually used by two mail servers to exchange e-mail. Users can then retrieve e-mail from the servers via mail clients such as Outlook, Eudora, or Pine. Mail clients use 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 purpose.

Table 3-1 SMTP Commands

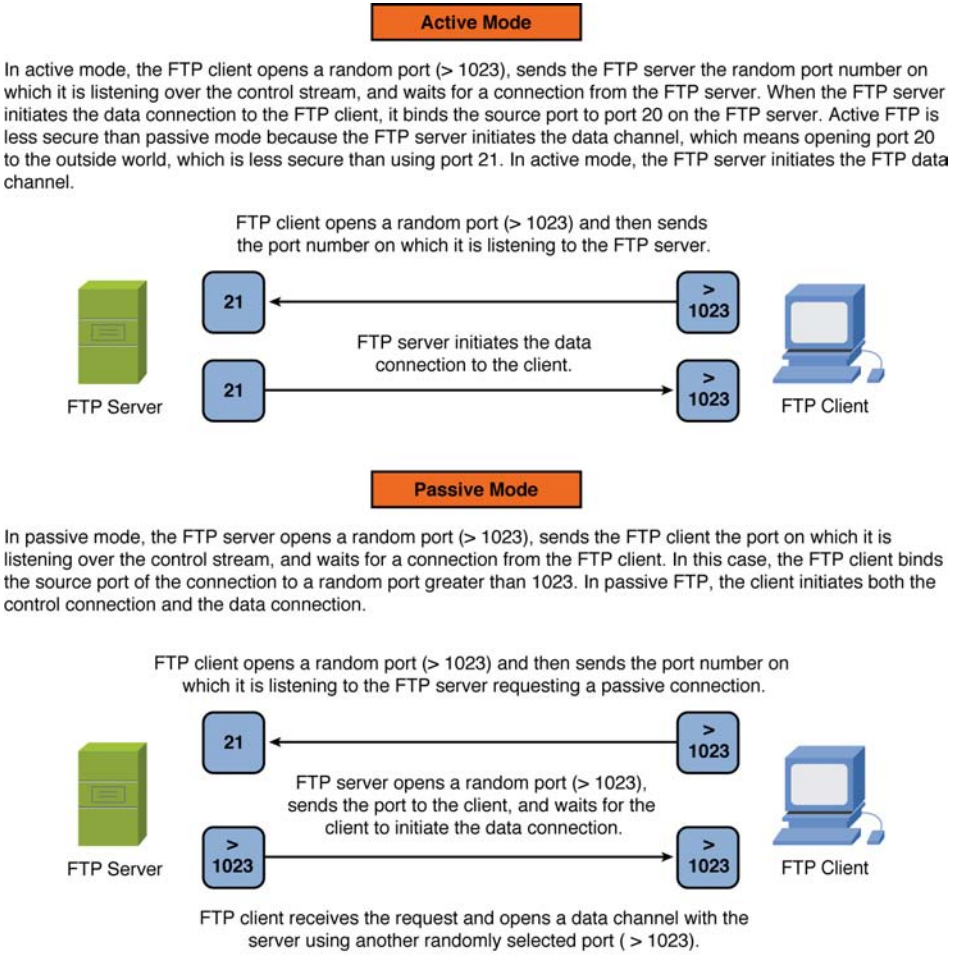
Command	Function
HELLO (HELO)	Identifies the SMTP client to the SMTP server.
MAIL (MAIL)	Initiates a mail transaction in which the mail data is delivered to an SMTP server, which is then either delivered to mailboxes or passed to another system via SMTP.
RECIPIENT (RCPT)	Identifies an individual recipient of the mail data; multiple use of the command is 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.

 Please see page 131 for more details.

File Transfer Protocol

FTP allows users to transfer files from one host to another. FTP is a TCP-based connection-oriented protocol, and it 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.

FIGURE 3-1
Overview of FTP Operation and Operating Modes



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 it is configured to do 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, and 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 different kinds of resource records, each of which stores a different kind of information about the domain and the hosts in the domain. Resource 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 will 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 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 is 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 address 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

 Please see page 131 for more details.

CCIE Security v3.0 Quick Reference

Lancy Lobo
Umesh Lakshman

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

Digital Edition Febrauary 2011

ISBN-10: 0-13-211713-4

ISBN-13: 978-0-13-211713-5

Warning and Disclaimer

This digital Quick Reference is designed to provide information about the CCIE Security v3.0 exam. Every effort has been made to make this digital Quick Reference as complete and 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 digital Quick Reference.

The opinions expressed in this digital Quick Reference belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this digital Quick Reference 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 digital Quick Reference should not be regarded as affecting the validity of any trademark or service mark.

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 of the professional technical community.

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

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this digital Quick Reference when ordered in quantity for bulk purchases or special sales, which may include elec-tronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more informa-tion, please contact: U**.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com.

For sales outside the United States please contact: **International Sales** international@pearsoned.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.**