SECURING THE WEB WITH CISCO WEB SECURITY APPLIANCE

DURATION: 2 DAYS

COURSE OVERVIEW

This course has been designed to help learners understand how to install, configure, manage, and troubleshoot a Cisco Web Security Appliance (WSA). Students will learn how to design, configure, administer, monitor, and troubleshoot the Cisco Web Security Appliance (WSA) in small to medium-sized business and enterprise installations. Extensive lab exercises provide attendees with critical hands-on product experience, providing a safe environment to experiment with malware etc.

TARGET AUDIENCE

Individuals involved with the deployment and installation of the Cisco's Web Security Appliances, or Channel Partner's looking to achieve accreditation.

COURSE OBJECTIVES

After you complete this course you should be able to:

1. Describe the Cisco WSA
2. Install and verify the WSA
3. Deploy proxy services for the WSA
4. Utilize authentication with the WSA
5. Configure various policies for the WSA
6. Enforce acceptable use using the WSA
7. Defend against malware
8. Configure data security
9. Describe Cisco Cloud Web Security
10. Use Cisco AnyConnect Secure Mobility Client
11. Perform Administration and Troubleshooting of WSA's

COURSE CONTENT

Reviewing the System

Customer Use Cases

Cisco Web Security Appliance Models and Architecture

Installing and Verifying the Cisco Web Security Appliance

Review the Cisco Security Management Appliance

Install and Verify Cisco Web Security Appliance Hardware

Install and Verify the Cisco Web Security Virtual Appliance for VMware

Run the system set-up Wizard

Configure L4TM

Configuring Virtual Web Security Appliance Connector to Cisco Cloud Web Security

Review Cisco Cloud Web Security

Connect to Cisco Cloud Web Security Using the Cloud Web Security Connector

Deploying Proxy Services

Contrast Proxy Modes

Review PAC Files

Configure and Manage Proxy Services

Deploy Native FTP Proxy

Read Proxy Access Log and HTTP Headers

Utilizing Authentication

Configure NTLM and Proxy Authentication

Identify Authentication Settings and Realms

Describe LDAP Authentication and Authorization

Troubleshoot Joining Domains and Test Authentication

Configuring Policies

Configure Access Policies and Identities

Configure Authentication Exemptions

Review Access Log Tags

Enforcing Acceptable Use

Enable URL Categories and Filters

Configure Application Visibility and Control

Describe SaaS Access Control

Use HTTPS Inspection

Configure HTTPS Proxy Settings

Enforcing Acceptable Use - Advanced Topics

Configure Application Visibility and Control - Advanced Topics

Describe SaaS Access Control - Advanced Topics

Configure Web Usage Controls and URL Categories

View Logging and Reporting

Defending Against Malware

Describe and Configure WBRS

Describe and Configure Anti-Malware Scanning

Describe and Configure Advanced Malware Protection

Interpret ACL Tags Relevant to Anti-Malware

Configuring Data Security

Configure Data Security

Configure Data Loss Prevention(DLP)

Describe Access and Data Security Logs

Describing Cisco Cloud Web Security

Cisco Cloud Web Security Features and Benefits

Explain Cisco Cloud Attach Model

Using Cisco Any Connect Secure Mobility Client

Describe Cisco AnyConnect Web Security

Integrate the Cisco AnyConnect Secure Mobility Client

Performing Administration and Troubleshooting

Describe Report Administration

Monitor the Cisco Web Security Appliance

Configure W3C Logging

Perform Other Administrative Tasks

Describe Hardware Redundancy

Troubleshooting the Cisco Web Security Appliance

Labs

Hardware Challenge Lab 1: Access the Cisco Remote Lab

Hardware Challenge Lab 2: Installing and Verifying the Cisco Web Security Appliance

Hardware Challenge Lab 3: Deploying Proxy Services

Hardware Challenge Lab 4: Utilizing Authentication

Hardware Challenge Lab 5: Configuring Cisco WSA Policies

Hardware Challenge Lab 6: Enforcing Acceptable Use

Hardware Challenge Lab 7: Enforcing Acceptable Use—Advanced Topics

Hardware Challenge Lab 8: Defending Against Malware

Hardware Challenge Lab 9: Configuring Data Security

Hardware Challenge Lab 10: Describing Cisco Cloud Web Security

Hardware Challenge Lab 11: Performing Administration and Troubleshooting

COURSE PREREQUISITES

Delegates should meet the following prerequisites:

Knowledge of TCP/IP services, including Domain Name Server (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS is assumed. - **ICND2** Recommended

Experience with IP Routing

TEST CERTIFICATION

Recommended preparation for exam(s) :

WSFE - 700-281 - This exam is only required for Field engineers looking to meet the Cisco Channel Partner requirements for Express Security - Web. .

FOLLOW ON COURSES

Delegates looking for training on Cisco's Email Security Appliance should consider:

SESA - Securing your Email with Cisco Email Security Appliance

PASESA - Securing Email with Cisco Email Security Appliance - Channel Partners Only.