COMPUTER LEARNING CENTRE
EDUCATE | INNOVATE | EMPOWER

CISCO PARTNER Learning

Training overview

Securing the Web with Cisco Web Security Appliance (SWSA)

Description

The **Securing the Web with Cisco Web Security Appliance (SWSA)** training shows you how to implement, use, and maintain Cisco® Web Secure Appliance (WSA) (formally Cisco® Web Security Appliance), powered by Cisco Talos, to provide advanced protection for business email and control against web security threats. Through a combination of expert instruction and hands-on practice, you'll learn how to deploy proxy services, use authentication, implement policies to control HTTPS traffic and access, implement use control settings and policies, use the solution's anti-malware features, implement data security and data loss prevention, perform administration of Cisco WSA solution, and more. This training prepares you for the Securing the Web with Cisco Web Secure Appliance (300-725 SWSA) v1.0 exam. If passed, you earn the Cisco Certified Specialist - Web Content Security certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP®) Security certification. This training earns you 16 Continuing Education (CE) credits toward recertification.

How you'll benefit

Thistraining willhelp you:

- Implement Cisco WSA to secure web gateways, provide malware protection, and use policy controls to address the challenges of securing and controlling web traffic
- Gain valuable hands-on skills focused on web security
- Prepare for the 300-725 SWSA v1.0 exam
- Earn 16 CE credits toward recertification

Who should enroll

- Security Architects
- System Designers
- Network Administrators
- Operations Engineers
- Network Managers, Network or Security Technicians, and Security Engineers and managers responsible for web security

- Cisco Integrators and Partners

Technology areas

- Web Security

Objectives

- Describe Cisco WSA
- Deploy proxy services
- Utilize authentication
- Describe decryption policies to control HTTPS traffic
- Understand differentiated traffic access policies and identification profiles
- Enforce acceptable use control settings
- Defend against malware
- Describe data security and data loss prevention
- Perform administration and troubleshooting

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- IP routing

You are expected to have one or more of the following basic technical competencies or equivalent knowledge:

- Implementing and Administering Cisco Solutions (CCNA) (CCENT certification or higher)
- Relevant industry certification [International Information System Security Certification Consortium ((ISC)2), Computing Technology Industry Association (CompTIA) Security+, International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), ISACA]
- Cisco Networking Academy letter of completion (CCNA 1 and CCNA 2)
- Windows expertise: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+)

Outline

- Cisco WSA Overview
- Proxy Services
- Cisco WSA Authentication
- Administration and Troubleshooting
- Decryption Policies
- Differentiated Traffic Access Policies and Identification Profiles
- Defending Against Malware
- Acceptable Use Control Settings
- Data Security and Data Loss Prevention

Lab Outline

- Configure the Cisco Web Security Appliance
- Deploy Proxy Services
- Configure Proxy Authentication
- Review Reporting Services and Web Tracking
- Perform Centralized Cisco AsyncOS Software Upgrade Using Cisco SMA
- Configure HTTPS Inspection
- Create and Enforce a Time/Date-Based Acceptable Use Policy
- Configure Advanced Malware Protection
- Configure Referrer Header Exceptions
- Utilize Third-Party Security Feeds and MS Office 365 External Feed
- Validate an Intermediate Certificate

What to expect on the exam

Securing theWeb withCisco Web Secure Appliance (300-725 SWSA) v1.0 is a 90-minute exam associated with the Cisco Certified DevNet Specialist – Web Content Security certification and satisfies the concentration exam requirement for the CCNP Security certification.

This exam tests your knowledge of Cisco Secure Web Appliance, including:

- Proxy services
- Authentication
- Decryption policies
- Differentiated traffic access policies
- Identification policies
- Acceptable use control settings
- Malware defense
- Data security
- Data loss prevention