



Document Generated: 07/09/2026

Learning Style: On Demand

Technology: Cisco

Difficulty: Intermediate

Course Duration: 40 Hours

Securing the Web with Cisco Web Security Appliance (SWSA) v3.0 - On Demand



Course Information

About this course:

This course will provide you skills to implement, use, and maintain Cisco® Web Security Appliance (WSA), powered by Cisco Talos. Being a Cisco Web Security Appliance expert you will be able to provide advanced protection for business email,

and full control against web security threats.

Through a combination of instructor video, text, and hands-on practice, you'll learn how to implement policies to control HTTPS traffic and access, implement use control settings and policies, deploy proxy services, implement data security and data loss prevention, perform administration of Cisco WSA solution, use authentication, use the solution's anti-malware features, and more.

Upon completing this course, you will be fully prepared to take the Securing the Web with Cisco Web Security Appliance (300-725 SWSA) exam, passing which will lead to CCNP® Security and the Cisco Certified Specialist - Web Content Security certifications.

Course Objective:

You should be able to do the following once you complete the course:

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

Audience:

- Operations engineers
- Network managers, network or security technicians, and security engineers and managers responsible for web security
- Cisco integrators and partners
- Security architects
- System designers
- Network administrators

Prerequisite:

You should have knowledge of these topics to fully benefit from this course:

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

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

- 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+)
- Cisco certification (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]

Course Outline:

Describing Cisco WSA

Technology Use Case
 Cisco WSA Solution
 Cisco WSA Features
 Cisco WSA Architecture
 Proxy Service
 Integrated Layer 4 Traffic Monitor
 Data Loss Prevention
 Cisco Cognitive Intelligence
 Management Tools
 Cisco Advanced Web Security Reporting (AWSR) and Third-Party Integration
 Cisco Content Security Management Appliance (SMA)

Deploying Proxy Services

Explicit Forward Mode vs. Transparent Mode
 Transparent Mode Traffic Redirection
 Web Cache Control Protocol
 Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
 Proxy Bypass
 Proxy Caching
 Proxy Auto-Config (PAC) Files
 FTP Proxy
 Socket Secure (SOCKS) Proxy
 Proxy Access Log and HTTP Headers
 Customizing Error Notifications with End User Notification (EUN) Pages

Utilizing Authentication

Authentication Protocols
 Authentication Realms
 Tracking User Credentials
 Explicit (Forward) and Transparent Proxy Mode
 Bypassing Authentication with Problematic Agents

- Reporting and Authentication
- Re-Authentication
- FTP Proxy Authentication
- Troubleshooting Joining Domains and Test Authentication
- Integration with Cisco Identity Services Engine (ISE)

Creating Decryption Policies to Control HTTPS Traffic

- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Inspection Overview
- Certificate Overview
- Overview of HTTPS Decryption Policies
- Activating HTTPS Proxy Function
- Access Control List (ACL) Tags for HTTPS Inspection
- Access Log Examples

Understanding Differentiated Traffic Access Policies and Identification Profiles

- Overview of Access Policies
- Access Policy Groups
- Overview of Identification Profiles
- Identification Profiles and Authentication
- Access Policy and Identification Profiles Processing Order
- Other Policy Types
- Access Log Examples
- ACL Decision Tags and Policy Groups
- Enforcing Time-Based and Traffic Volume Acceptable Use Policies, and End User Notifications

Defending Against Malware

- Web Reputation Filters
- Anti-Malware Scanning
- Scanning Outbound Traffic
- Anti-Malware and Reputation in Policies
- File Reputation Filtering and File Analysis
- Cisco Advanced Malware Protection
- File Reputation and Analysis Features
- Integration with Cisco Cognitive Intelligence

Enforcing Acceptable Use Control Settings

- Controlling Web Usage
- URL Filtering
- URL Category Solutions
- Dynamic Content Analysis Engine
- Web Application Visibility and Control
- Enforcing Media Bandwidth Limits
- Software as a Service (SaaS) Access Control

Filtering Adult Content

Data Security and Data Loss Prevention

- Data Security
- Cisco Data Security Solution
- Data Security Policy Definitions
- Data Security Logs

Performing Administration and Troubleshooting

- Monitor the Cisco Web Security Appliance
- Cisco WSA Reports
- Monitoring System Activity Through Logs
- System Administration Tasks
- Troubleshooting
- Command Line Interface

References

- Comparing Cisco WSA Models
- Comparing Cisco SMA Models
- Overview of Connect, Install, and Configure
- Deploying the Cisco Web Security Appliance Open Virtualization Format (OVF) Template
- Mapping Cisco Web Security Appliance Virtual Machine (VM) Ports to Correct Networks
- Connecting to the Cisco Web Security Virtual Appliance
- Enabling Layer 4 Traffic Monitor (L4TM)
- Accessing and Running the System Setup Wizard
- Reconnecting to the Cisco Web Security Appliance
- High Availability Overview
- Hardware Redundancy
- Introducing Common Address Redundancy Protocol (CARP)
- Configuring Failover Groups for High Availability
- Feature Comparison Across Traffic Redirection Options
- Architecture Scenarios When Deploying Cisco AnyConnect® Secure Mobility

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your LinkedIn profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:



- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

[Find Out More](#) or [See List Of Badges](#)