SWSA - SECURING THE WEB WITH CISCO WEB SECURITY APPLIANCE V3.1

Course Code: 100496

Implement, use, and maintain Cisco Web Security Appliance (WSA), 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, the *SWSA - Securing the Web with Cisco Web Security Appliance v3.1* course teaches 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 course helps you prepare to take the exam, Securing the Web with Cisco Web Security Appliance (300-725 SWSA), which leads to the CCNP Security and Cisco Certified Specialist - Web Content Security certifications. The 300-725 SWSA exam certifies your knowledge of Cisco Web Security Appliance including proxy services, authentication, decryption policies, differentiated traffic access policies and identification policies, acceptable use control settings, malware defense, and data security and data loss prevention.

This course is eligible for 16 Continuing Education Credits (ILT & ELT Modality).

What You'll Learn

After taking this course, you should be able to:

- 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

Who Needs to Attend

- 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

Prerequisites

To fully benefit from this course, you should have knowledge of these topics:

- 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:

- 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]
- 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+)

SWSA - SECURING THE WEB WITH CISCO WEB SECURITY APPLIANCE V3.1

Course Code: 100496

CLASSROOM LIVE	$1,995 USD	2 Day

SWSA - SECURING THE WEB WITH CISCO WEB SECURITY APPLIANCE V3.1

Course Code: 100496

VIRTUAL CLASSROOM LIVE	$1,995 USD	2 Day

Virtual Classroom Live 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

Virtual Classroom Live Labs

- Configure the Cisco Web Security Appliance
- Deploy Proxy Services
- Configure Proxy Authentication
- 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

- View Reporting Services and Web Tracking
- Perform Centralized Cisco AsyncOS Software Upgrade Using Cisco SMA

Jan 26 - 27, 2026 | 8:30 AM - 4:30 PM EST

SWSA - SECURING THE WEB WITH CISCO WEB SECURITY APPLIANCE V3.1

Course Code: 100496

ON-DEMAND	$500 USD

SWSA - SECURING THE WEB WITH CISCO WEB SECURITY APPLIANCE V3.1

Course Code: 100496

PRIVATE GROUP TRAINING	2 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 12/9/2025 11:53:41 PM