

# Securing the Web with Cisco Web Security Appliance (SWSA)

- **Formato do curso:** Presencial e Live Training
- **Preço:** 1495€
- **Duração:** 14 horas

In this Cisco Web Security Appliance training you learn how to implement, use, and maintain a 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, 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 course helps you prepare to take the exam, **Securing the Web with Cisco Web Security Appliance** (300-725 SWSA), which leads to **CCNP® Security** and the **Cisco Certified Specialist - Web Content Security**.

## This course will help 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 for high-demand responsibilities focused on web security

## Destinatários

Individuals involved in the deployment, installation and administration of a Cisco Web Security Appliance:

- 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

## Pré-requisitos

### **Attendees should meet the following prerequisites :**

- 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 or higher) -ICND1 Recommended
  - Relevant industry certification (ISC)2, (CompTIA) Security+, EC-Council, GIAC, ISACA
  - Cisco Net 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+)
- 

## Objetivos

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
- 

## Metodologia

- Instructor-led training: 2 days in the classroom with hands-on lab practice
- 

## Programa

### **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

**Labs:**

- Lab 1: Configure the Cisco Web Security Appliance
  - Lab 2: Deploy Proxy Services
  - Lab 3: Configure Proxy Authentication
  - Lab 4: Configure HTTPS Inspection
  - Lab 5: Create and Enforce a Time/Date-Based Acceptable Use Policy
  - Lab 6: Configure Advanced Malware Protection
  - Lab 7: Configure Referrer Header Exceptions
  - Lab 8: Utilize Third-Party Security Feeds and MS Office 365 External Feed
  - Lab 9: Validate an Intermediate Certificate
  - Lab 10: View Reporting Services and Web Tracking
  - Lab 11: Perform Centralized Cisco AsyncOS Software Upgrade Using Cisco SMA
- 

**Prossiga na sua certificação Cisco!**

**Este curso confere 16 créditos no programa Continuing Education da Cisco.**

[Se procura revalidar a sua certificação Cisco, conheça o programa Continuing Education.](#) Como forma de incentivar os candidatos a manter, aumentar e a diversificar o seu conjunto de skills, a Cisco desenvolveu este Programa de Recertificação que oferece caminhos flexíveis para revalidar competências e certificações existentes.