# SWSA (SECURING THE WEB WITH CISCO WEB SECURITY APPLIANCE (SWSA) V3.0) 3.0

## Objetivo

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. Prepare for 300-725 SWSA exam certifies your knowledge of Cisco wEB Security Appliance, including administration, Implement Cisco WSA to secure web gateways, provide malware protection, and use policy controls to address the challenges of securing and controlling web traffic. This 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. After you pass 300-725 SWSA: • You earn the Cisco Certified Specialist - Web Content Security certification; • You will have satisfied the concentration exam requirement for new the CCNP Security certification. To complete CCNP Security, you also need to pass the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam or its equivalent.

## Público Alvo

• Networking and security professionals involved with deployment, configuring and support using Cisco's Web Security Appliances solutions; • Professionals who need to prepare for the Cisco 300-725 certification exam.

## Pré-Requisitos

We recommend that the student has the following prerequisites : • Knowledge of TCP/IP services, including DNS, SSH, FTP, SNMP, HTTP, and HTTPS; • Experience with IP Routing and switching.

## Carga Horária

16 horas (2 dias).

## Conteúdo Programático

**Course Introduction**
Course Outline
Course Goals

**Cisco WSA Basics**
Describe Cisco WSA and its key features.
Describe to manage the safe use of web-based and social networking applications

Describe Cisco WSA can help organizations define and enforce acceptable use policies
Describe the features of the Cisco WSA
Describe the architecture of Cisco WSA products.
Describe the Cisco WSA proxy service.
Describe integrated L4TM service of the Cisco WSA.
Describe the data loss prevention service of the Cisco WSA.
Describe the Cognitive Threat Analytics feature of the Cisco WSA.
Describe the management tools that are available on the Cisco WSA.
Describe the advanced web security reporting application solution
Describe how to integrate Cisco WSA with Splunk.
Describe Cisco Content Security Management Appliance solution.
Practical Use: Configure the Cisco Web Security Appliance

**Deploying Proxy Services**
Describe different proxy modes
Describe how to configure and manage services such as PAC and WCCP, and deploy
This lesson includes these topics:
Describe the difference between explicit forward mode and transparent mode.
Describe transparent mode traffic redirection mechanism.
Describe the Web Cache Communication Protocol.
Describe the WCCP downstream flow.
Describe the proxy bypass upstream and downstream.
Describe how to tune caching behavior for safety or performance.
Describe the functions of a programmable automation controller file (PAC)
Describe the FTP proxy service.
Describe the SOCKS protocol and the SOCKS proxy services.
Describe the proxy access log and the HTTP headers.
Describe customizing Error Notifications with EUN Pages
Describe how to create custom EUN pages.
Practical Uses: Deploy Proxy Services

**Utilizing Authentication**
Configure an NTLM authentication realm and will authenticate a transparent proxied
Describe authentication protocols supported by the Cisco WSA.
Describe an authentication realm that must be created to enable client authentication
Describe Tracking User Credentials
Describe the authentication surrogates supported by the Cisco WSA.
Describe transparent proxy mode and explicit (forward) proxy mode to WSA redirection
Describe how Cisco WSA allows bypassing authentication with problematic agents
Describe how access logs and authentication logs can be used to review accounting
Describe the re-authentication feature of the Cisco WSA.
Describe the FTP proxy authentication.
Troubleshooting Joining Domains and Test Authentication
Describe how to troubleshoot joining domains and testing authentication issues
Integration with Cisco ISE
Describe the Cisco WSA integration with Cisco ISE.
Practical Uses: Configure Proxy Authentication

**Creating Decryption Policies to Control HTTPS Traffic**
Describe how decryption policies are used to control HTTPS traffic
Provide an overview of the SSL and TLS inspection.
Describe types of certificates that should be used for HTTPS decryption using WSA
Overview of HTTPS Decryption Policies
Provide an overview of HTTPS decryption policies
Activating HTTPS Proxy Function
Describe the process of activating HTTPS proxy function
Describe ACL tags for HTTPS inspection
Describe examples of the Cisco WSA access logs.
Practical Uses: Configure HTTPS Inspection

**Understanding Differentiated Traffic Access Policies and Identification Profiles**
Configure Cisco WSA access policies, define and configure authentication exemptions and use the policy tractool to test the Cisco WSA configuration
Overview of Access Policies
Provide an overview of the Cisco WSA access policies.
Describe Cisco WSA access policy groups.
Overview of Identification Profiles
Provide an overview of the Cisco WSA identification profiles.
Identification Profiles and Authentication
Describe Cisco WSA identification profiles and authentication.
Access Policy and Identification Profiles Processing Order
Describe access policies and identification profiles on the Cisco WSA.
Describe multiple policy types uses to manage different aspects of web requests
Access Log Examples
Understand the access log role in the troubleshooting process
ACL Decision Tags and Policy Groups
Describe Cisco WSA ACL decision tags and policy groups
Enforcing Time-Based and Traffic Volume Acceptable Use Policies, and End User Notifications
Describe how Cisco WSA enforces time-based and traffic volume acceptable use policies and end user notifications.
Practical Use: Create and Enforce a Time/Date-Based Acceptable Use Policy

**Defending Against Malware**
Describe anti-malware features on the Cisco WSA, and configure anti-malware and web reputation settings per policy
Web Reputation Filters
Describe Cisco WSA web reputation filters
Anti-Malware Scanning
Describe Cisco WSA anti-malware scanning feature
Scanning Outbound Traffic
Describe how Cisco WSA scans outbound traffic.
Anti-Malware and Reputation in Policies
Describe anti-malware and reputation in Cisco WSA policies
File Reputation Filtering and File Analysis
Describe the file reputation filtering and file analysis feature of the Cisco WSA
Cisco Advanced Malware Protection

Provide an overview of Cisco Advanced Malware Protection.
File Reputation and Analysis Features
Configure file reputation and analysis features of the Cisco WSA
Integration with Cisco Cognitive Intelligence
Describe Cisco WSA integration with Cognitive Threat Analytics
Practical Use: Configure Advanced Malware Protection

**Enforcing Acceptable Use Control Settings**
Configure and enforce acceptable use policies, enable and configure URL filters, and utilize custom URL categories
Controlling Web Usage
Describe Cisco web usage controls that are available on the Cisco WSA
Describe the URL filtering feature on the Cisco WSA
URL Category Solutions
Describe Cisco WSA URL filters
Dynamic Content Analysis Engine
Describe the dynamic content analysis engine feature of the Cisco WSA
Web Application Visibility and Control
Describe the web application visibility and control feature of the Cisco WSA
Enforcing Media Bandwidth Limits
Enforce media bandwidth limits on the Cisco WSA
SaaS Access Control
Overview of the SaaS access control using Cisco WSA
Filtering Adult Content
Configure the Cisco WSA to filter adult content from some web searches and websites
Practical Use: Configure Referrer Header Exceptions
Practical Use: Utilize Third-Party Security Feeds and MS Office 365 External Feed

**Data Security and Data Loss Prevention**
Describe and implement data security and data loss prevention solution using Cisco WSA.
Provide an overview of the data security solution
Cisco Data Security Solution
Describe Cisco data security solution
Data Security Policy Definitions
Describe Cisco WSA data security policy definitions
Data Security Logs
Describe Cisco WSA log file types to troubleshoot data security and external data loss prevention policies.
Practical Use: Validate an Intermediate Certificate

**Performing Administration and Troubleshooting**
Perform administrative and troubleshooting tasks on the Cisco WSA
Monitor the Cisco Web Security Appliance
Describe how the Cisco WSA allows you to monitor your company’s network by using various tools
Cisco WSA Reports
Describe reporting feature of the Cisco WSA
Monitoring System Activity Through Logs
Describe how to monitor Cisco WSA system activity through logs
System Administration Tasks
Describe various Cisco WSA tools used to perform system administration tasks

Troubleshooting
Describe various methods to troubleshoot connectivity over Cisco WSA
Command Line Interface
Describe how the AsyncOS CLI allows you to configure and monitor the Cisco WSA.
Practical Use: Review Reporting Services and Web Tracking
Practical Use: Perform Centralized AsyncOS Software Upgrade Using Cisco SMA

**Cisco WSA References**
Comparing Cisco WSA Models
Describe the various Cisco WSA models
Comparing Cisco SMA Models
Overview of Connect, Install, and Configure
Provide an overview of installing and configuring the Cisco WSA
Deploying the Cisco Web Security Appliance OVF Template
Deploy the Cisco Web Security Appliance OVF template.
Mapping Cisco Web Security Appliance VM Ports to Correct Networks
Map Cisco WSA VM ports to the correct networks.
Connecting to the Cisco Web Security Virtual Appliance
Connect to the Cisco WSA for the first time
Enable L4TM the feature on the Cisco WSA
Accessing and Running the System Setup Wizard
Access and run the Cisco WSA system setup wizard
Reconnecting to the Cisco Web Security Appliance
Describe reconnecting to the Cisco WSA
High Availability Overview
Provide an overview of the Cisco WSA high availability option
Hardware Redundancy
Describe hardware redundancy option for the Cisco WSA.
Introducing CARP Protocol
Provide an overview of the CARP protocol.
Configuring Failover Groups for High Availability
Configure failover groups for high availability on the Cisco WSA.
Architecture Scenarios When Deploying AnyConnect Secure Mobility
Understand 4 architecture scenarios when deploying AnyConnect secure mobility.

**Labs Outline**
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: Review Reporting Services and Web Tracking
Lab 11: Perform Centralized AsyncOS Software Upgrade Using Cisco SMA

TELECON
Avenida Paulista, 171 - 10 andar Bela Vista – São Paulo – SP
Tel.: (11) 3090-7651 – www.telecon.com.br