

# **SWSA (SECURING WEB WITH CISCO WEB SECURITY APPLIANCE)**

## **Objetivo**

Securing Web with Cisco Web Security Appliance (SWSA) é um curso com carga horário de dois dias, que proporciona aos alunos os conhecimentos necessários para instalar, configurar, gerenciar e realizar atividades de suporte ao produto. É curso desenvolvido para capacitação operacional do produto, aliando apresentação do conteúdo teórico, sempre reforçado e associado pela realização de atividades práticas associadas. Após completar este treinamento o aluno estará apto à:

- Descrevendo o Cisco WSA;
- Instalação do Cisco WSA;
- Administrar o Cisco WSA;
- Implantar serviço de “Proxy” utilizando o WSA;
- Utilizar processo de autenticação com o WSA;
- Utilizar serviço de uso responsável ( Enforce Acceptable Use );
- Proteção com ameaças do tipo “Malware”;
- Configuração para segurança de dados;
- Descrever o serviço Cisco Cloud Web Security;
- Utilização do Cisco Anyconnect secure Mobility Client;
- Realizar atividades administrativas e de suporte ao WSA.

## **Público Alvo**

O público primário inclui os indivíduos os profissionais que demandam conhecimentos para instalar, operar, prestar suporte e otimizar o produto Cisco WSA.

## **Pré-Requisitos**

Para maior aproveitamento é recomendado que o aluno possua conhecimentos fundamentais no protocolo TCP/IP, incluindo DNS, SSH, FTP, SNMP, HTTP e HTTPS e experiência com roteamento IP.

## **Carga Horária**

16 horas (2 dias).

## **Conteúdo Programático**

Course Introduction

- Overview
- Course Goal and Objectives
- Course Flow
- Additional References
- Your Training Curriculum

Module 1: Reviewing the System

Customer Use Cases

- Enforcing Acceptable Use
- Acceptable Usage Policies
- Malware Detection and Protection
- Mobile Users Bypassing Corporate Controls
- AnyConnect Secure Mobility Client

## Cisco Web Security Appliance Models and Architecture

- Cisco Web Security Appliance Models
- Architecture Overview
- AsyncOS Overview
- Proxy Service Overview
- Integrated L4TM
- Cisco Cloud Web Security Provides SaaS Delivery of Security
- Management Tools
- Splunk Application for Cisco Web Security Appliance

## Module 2: Installing and Verifying the Cisco Web Security Appliance

### Review the Cisco Security Management Appliance

- The Cisco Security Management Appliance
- Features and Benefits of the Cisco Security Management Appliance
- Centralized Reporting and Configuration Management
- Model Specifications
- Cisco Security Management Appliance Deployment

### Install and Verify Cisco Web Security Appliance Hardware

- Installing and Cabling Cisco Web Security Appliance Hardware
- Sample Interface Deployments
- Connecting to the Cisco Web Security Appliance for the First Time

### Install and Verify the Cisco Web Security Virtual Appliance for VMware

- Preparing for the Cisco Web Security Virtual Appliance Installation on VMware
- Deploying the Cisco Web Security Appliance OVF Template
- Additional VM Settings
- Map Cisco Web Security Appliance VM Ports to Correct Networks
- Connecting to the Cisco Web Security Virtual Appliance for the First Time

### Run the System Setup Wizard

- Accessing the System Setup Wizard
- Running the System Setup Wizard
- Reconnecting to the Cisco Web Security Appliance

### Configure L4TM

- Enable L4TM

## Module 3: Configuring Virtual Web Security Appliance Connector to Cisco Cloud Web Security

### Review Cisco Cloud Web Security

- Cisco Cloud Web Security
- Supported and Unsupported Functionality Features

## Connect to Cisco Cloud Web Security Using the Cloud Web Security Connector

- Configuring the Cloud Connector
- Cloud Web Security Connector Option
- Network Interfaces and Wiring
- Routes for Management and Data Traffic
- Configure Transparent Connection Settings
- Directory Group Policies in the Cloud
- Cloud Connector Logs

## Module 4: Deploying Proxy Services

### Contrast Proxy Modes

Objective: Contrast proxy modes

This lesson includes these topics:

- Explicit Forward Mode vs. Transparent Mode
- Explicit Forward Mode Configuration
- Transparent Mode Traffic Redirection
- Web Cache Control Protocol
- WCCP Upstream Flow
- WCCP Downstream Flow
- Proxy Bypass
- Defining Cisco WSA WCCP Service Group
- Enabling Cisco WSA Transparent Redirection
- Enabling WCCP Redirection on a Cisco ASA

### Review PAC Files

- PAC File Troubleshooting
- PAC File Deployment Options
- PAC File Examples: Single and Failover
- PAC File Hosting

### Configure and Manage Proxy Services

- Configuring and Managing Proxy Caching
- Tune Caching Behavior for Safety or Performance
- The Proxy Settings GUI Page
- Customizing Error Notifications with EUN Pages
- EUN Localization Directories

### Deploy Native FTP Proxy

- FTP Proxy Supports Both Active and Passive Mode
- FTP Forward Mode vs. Transparent Mode
- FTP Proxy Configuration
- FTP Client Example: FileZilla

### Read Proxy Access Log and HTTP Headers

- Cisco Web Security Appliance Access Log: Squid Component
- Squid Access Log Format
- Common Response Codes
- HTTP Headers
- Access Log Examples
- Customizing the Access Log
- MIME Types

## Utilizing Authentication

### Configure NTLM and Proxy Authentication

- Cisco Web Security Appliance Proxy Authentication
- Authentication Protocols and Proxy Modes
- Explicit Forward Mode
- Transparent Mode
- Reporting and Authentication
- Reauthentication
- FTP Proxy Authentication

### Identify Authentication Settings and Realms

- Global Authentication Settings
- Creating Realms and Realm Sequences
- Creating an NTLM Realm for Active Directory
- Joining a Cisco WSA to the Active Directory Domain
- Configuring an Identity to Require Transparent User Identification

### Describe LDAP Authentication and Authorization

- Creating LDAP Realms for Other Directories
- Defining How Users Are Stored
- Binding to the Directory
- LDAP Group Authorization

### Troubleshoot Joining Domains and Test Authentication

- Trouble Joining the Domain
- Common Errors When Joining the Domain
- Test Authentication: NTLM or LDAP
- Authentication Always Starts with an Access Log Error

## Module 6: Configuring Policies

### Configure Access Policies and Identities

- Access Policies
- Access Policy Groups
- Policy Trace
- Identities
- Authentication
- Other Policy Types

## Configure Authentication Exemptions

- Configure Access Policy Membership
- Configure an Identity to Avoid Authentication

## Review Access Log Tags

- Access Log Decision Tags Reflect Policy Controls
- Access Log Examples
- ACL Decision Tags and Policy Groups

## Module 7: Enforcing Acceptable Use

### Enable URL Categories and Filters

- URL Filtering
- URL Category Solutions

### Configure Application Visibility and Control

- Web Usage Controls
- Dynamic Content Analysis Engine
- Configuring the URL Filtering Engine

### Describe SaaS Access Control

- Enforcing Time-Based Acceptable Use Policies
- URL Warning Page

### Use HTTPS Inspection

- HTTPS Inspection and Decryption Policies
- Active HTTPS Proxy
- ACL Tags for HTTPS Inspection
- Access Log Examples

### Configure HTTPS Proxy Settings

- Relevant Licenses
- Enabling the HTTPS Proxy
- Invalid Certificate Management for HTTPS Proxy
- HTTPS Inspection Pipeline
- HTTPS Inspection Policy

## Module 8: Enforcing Acceptable Use: Advanced Topics

### Configure Application Visibility and Control: Advanced Topics

- Web Application Visibility and Control
- Streaming Media Bandwidth Control

### Describe SaaS Access Control: Advanced Topics

- SaaS Access Control
- How SaaS Access Control Works

### Configure Web Usage Controls and URL Categories

- Relevant Licenses
- Web Usage Control Engines
- Custom URL Categories
- Creating Time Ranges to Use in Policies
- Predefined URL Category Control Settings
- Custom URL Category Control Settings
- Enabling Safe Search and Site Content Ratings
- Configuring Application Visibility Controls
- Configuring Media Bandwidth Limits
- SaaS Access Control Configuration

#### View Logging and Reporting

- ACL Tags Associated with URL Filtering
- Access Log Examples
- URL Categories Reports
- Client Web Activity Report
- Client Detail Report
- AVC Report

#### Module 9: Defending Against Malware

##### Describe and Configure WBRS

- WBRS Actions
- WBRS Parameters
- Cisco DVS Engine
- Webroot vs. McAfee or Sophos

##### Describe and Configure Antimalware Scanning

- Outbound Malware Scanning
- Relevant Licenses
- WBRS Configuration
- Antimalware: Global Configuration
- Antimalware: Per-Policy Configuration
- Destination Settings

##### Describe and Configure Advanced Malware Protection

- Cisco Advanced Malware Protection
- Cisco Advanced Malware Protection Integration: Decision Flow
- Cisco Advanced Malware Protection File Analysis
- Relevant Cisco Advanced Malware Protection Licensing
- Cisco Advanced Malware Protection Global Configuration
- Cisco Advanced Malware Protection Architecture
- Cisco Advanced Malware Protection Per-Policy Configuration
- Cisco Advanced Malware Protection Reporting

##### Interpret ACL Tags Relevant to Antimalware

- ACL Tags for WBRS and Cisco DVS
- Access Log Entries

- Access Log Examples
- WBRs Reports
- Antimalware Reports
- Client Malware Risk Reports

## Module 10: Configuring Data Security

### Configure Data Security

- Data Security
- Multiple Data Security Policies
- Data Security URL Filter Controls
- Data Security Reputation Filters
- Data Security Content Filters

### Configure DLP

- Data Loss Prevention
- Add an ICAP Server
- Create Multiple DLP Policies
- Requests Sent to External DLP

### Describe Access and Data Security Logs

- ACL Tags for Data Security
- Access and Data Security Logs

## Module 11: Describing Cisco Cloud Web Security

### Describe Cisco Cloud Web Security Features and Benefits

- Cisco Cloud Web Security
- Global Data Center Footprint
- Cloud Proxy
- IPv6 Readiness

### Explain Cisco Cloud Attach Model

- Cisco Cloud Attach Model
- Cisco Web Security Appliance Connector
- Cisco Web Security Appliance Connector Features
- Cisco Web Security Appliance Connector Definitions
- Managing the Web with Cisco Cloud Web Security
- URL Filtering
- Application Visibility and Control
- Web Intelligence Reporting
- Flexible Report Output (Grid)
- Flexible Report Output (Pie Chart)
- Time Analysis Trending
- User Audits
- Loss of Productivity

## Module 12: Using Cisco AnyConnect Secure Mobility Client

## Describe Cisco AnyConnect Web Security

- Cisco AnyConnect Web Security Main Features
- Cisco AnyConnect Web Security
- VPN Client

## Integrate the Cisco AnyConnect Secure Mobility Client

- Configuration and Deployment of Cisco AnyConnect Web Security
- Creating the Profile—Proxies
- Creating the Profile—Exceptions
- Creating the Profile—Preferences
- Creating the Profile—Authentication
- Creating the Profile—Advanced
- Dynamic Updates to Cisco AnyConnect Configuration
- Cisco AnyConnect GUI
- Cisco AnyConnect Web Security Messages
- Cisco AnyConnect Web Security Debugging

## Module 13: Performing Administration and Troubleshooting

### Describe Report Administration

- Reports for Email Delivery
- On-Demand Reports
- Report Archiving and Exporting

### Monitor the Cisco Web Security Appliance

- Comprehensive System Monitoring Tools
- System Capacity Report
- Log Subscriptions
- Alert Center
- Monitor the Cisco WSA with the CLI
- SNMP Configuration

### Configure W3C Logging

- W3C Logging
- W3C Logging Configuration Method 1
- W3C Logging Configuration Method 2

### Perform Other Administrative Tasks

- Restricting Administrative Access
- Creating Users
- Configuring File Management and Disaster Recovery
- Updates and Upgrades
- Upgrade Process
- Feature Keys

### Describe Hardware Redundancy

- Hardware RAID on All Models
- Redundant Power Supply on Higher Models



## Troubleshoot the Cisco Web Security Appliance

- Troubleshooting with CLI Commands
- Authentication Troubleshooting
- Policy Trace Tool
- Open a Support Case
- Remote Access
- Packet Capture Tool
- Cisco Web Security Appliance Access Log Format

## Laboratórios

- Lab 1: Access the Cisco Remote Lab
- Lab 2: Installing and Verifying the Cisco Web Security Appliance
- Lab 3: Deploying Proxy Services
- Lab 4: Utilizing Authentication
- Lab 5: Configuring Cisco WSA Policies
- Lab 6: Enforcing Acceptable Use
- Lab 7: Enforcing Acceptable Use—Advanced Topics
- Lab 8: Defending Against Malware
- Lab 9: Configuring Data Security
- Lab 10: Describing Cisco Cloud Web Security
- Lab 11: Performing Administration and Troubleshooting