# Securing the Web with Cisco Web Security Appliance

Référence : **SWSA**     Durée : **2 jours**     Certification : **300-725**

Code CPF : **RS579**

## CONNAISSANCES PREALABLES

- 1-To fully benefit from this course, you should have one or more of the following basic technical competencies:. • 2-Cisco certification (CCENT certification or higher). • 3-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]. • 4-Cisco Networking Academy letter of completion (CCNA® 1 and CCNA 2). • 5-Windows expertise: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+). • 6-The learner is expected to have the following skills and knowledge before attending this course:. • 7-TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS. • 8-IP routing.

## PROFIL DES STAGIAIRES

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

## OBJECTIFS

- 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.

## CERTIFICATION PREPAREE

- Securing your Email with Cisco Email Security Appliance. This exam will not be available until the 24th of February 2020. Passing the exam will count as one of the concerntrations for the New CCNP Security Certification and will provide the Cisco Certified Specialist - Web Content Security Certification. Pour en savoir plus sur cette certification, cliquez ici et accédez aux informations complètes fournies par France Compétences

## METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

## FORMATEUR

Consultant-Formateur expert Security Cisco

## METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

## CONTENU DU COURS

### 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

## Certification Securing your Email with Cisco Email Security Appliance
- Cette formation prépare au passage de la certification Securing your Email with Cisco Email Security Appliance