

Securing the Web with Cisco Web Security Appliance

Duration: 2 Days Course Code: SWSA Version: 3.1

Overview:

The **Securing the Web with Cisco Web Security Appliance (SWSA)** course shows you how to 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, 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 is worth 16 Continuing Education (CE) Credits

Target Audience:

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

Objectives:

- **After completing 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

Prerequisites:

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
- CCNA - Implementing and Administering Cisco Solutions
- G013 - CompTIA Security+

Testing and Certification

Recommended preparation for exam(s) :

- **300-725** - Securing the Web with Cisco Web Security Appliance

Follow-on-Courses:

Delegates looking for training on Cisco's Email Security Appliance should consider:

- **SESA** - Securing your Email with Cisco Email Security Appliance

Content:

Cisco WSA Overview

- 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)

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

Cisco WSA 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)

Administration and Troubleshooting

- Monitor the Cisco Web Security Appliance
- Cisco WSA Reports
- Monitoring System Activity Through Logs
- System Administration Tasks
- Troubleshooting
- Command Line Interface

Decryption Policies

- 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

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

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

Labs:

- Discovery Lab 1: Configure the Cisco Web Security Appliance
- Discovery Lab 2: Configure Proxy Authentication
- Discovery Lab 3: Configure Reporting Services and Web Tracking
- Discovery Lab 4: Configure the Cisco Secure Email and Web Manager for Tracking and Reporting
- Discovery Lab 5: Configure HTTPS Inspection
- Discovery Lab 6: Create and Enforce a Time/Date-Based Acceptable Use Policy
- Discovery Lab 7: Configure Advanced Malware Protection
- Discovery Lab 8: Configure Referrer Header Exceptions
- Discovery Lab 9: Utilize Third-Party Security Feeds and MS Office 365 External Feed
- Discovery Lab 10: Validate an Intermediate Certificate

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK