Securing the Web with Cisco Web Security Appliance

Course Code SWSA
Duration 2 days

Overview

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 is worth 16 Credits in the Continuing Education Program.

Audience

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

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing Cisco WSA.
- Deploying proxy services.
- Utilizing authentication.
- Describing decryption policies to control HTTPS traffic.
- Understanding differentiated traffic access policies and identification profiles.
- Enforcing acceptable use control settings.
- Defending against malware.
- Describing data security and data loss prevention.
- Performing administration and troubleshooting.

Pre-Requisites

- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- IP routing

Recommended qualifications (1 of the following):

- 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+)

Recommended courses:

- G013 - CompTIA Security+
- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

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

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

Exam Details

There is no exam currently aligned to this course.

Further Information

For more information or to book this course, please contact our Course Enquiries Team on **01752 227330** (Option 2) or email us at **enquiries@skilltec.co.uk**.