Course Outline

Securing the Web with Cisco Web Security Appliance (SWSA)

Course Summary

Description

Securing the Web with Cisco Web Security Appliance (SWSA) v3.0 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 helps you prepare to take the exam, Securing the Web with Cisco Web Security Appliance (300-725 SWSA), which leads to CCNP Security and the Cisco Certified Specialist - Web Content Security.

Objectives

By the end of the course, students will 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

Topics

- Describing Cisco WSA
- Deploying Proxy Services
- Utilizing Authentication
- Creating Decryption Policies to Control HTTPS Traffic
- Understanding Differentiated Traffic Access Policies and Identification Profiles
- Defending Against Malware
- Enforcing Acceptable Use Control Settings
- Data Security and Data Loss Prevention
- Performing Administration and Troubleshooting
- References
- Lab outline

Audience

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

Course Outline

Securing the Web with Cisco Web Security Appliance (SWSA)

Course Summary (cont.)

Prerequisite

To fully benefit from this course, you should have knowledge of these topics:

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

Duration

Two Days

Course Outline

Securing the Web with Cisco Web Security Appliance (SWSA)

Course Outline

I. Describing Cisco WSA

A. Technology Use Case
B. Cisco WSA Solution
C. Cisco WSA Features
D. Cisco WSA Architecture
E. Proxy Service
F. Integrated Layer 4 Traffic Monitor
G. Data Loss Prevention
H. Cisco Cognitive Intelligence
I. Management Tools
J. Cisco Advanced Web Security Reporting (AWSR) and Third-Party Integration
K. Cisco Content Security Management Appliance (SMA)

II. Deploying Proxy Services

A. Explicit Forward Mode vs. Transparent Mode
B. Transparent Mode Traffic Redirection
C. Web Cache Control Protocol
D. Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
E. Proxy Bypass
F. Proxy Caching
G. Proxy Auto-Config (PAC) Files
H. FTP Proxy
I. Socket Secure (SOCKS) Proxy
J. Proxy Access Log and HTTP Headers
K. Customizing Error Notifications with End User Notification (EUN) Pages

III. Utilizing Authentication

A. Authentication Protocols
B. Authentication Realms
C. Tracking User Credentials
D. Explicit (Forward) and Transparent Proxy Mode
E. Bypassing Authentication with Problematic Agents
F. Reporting and Authentication
G. Re-Authentication
H. FTP Proxy Authentication
I. Troubleshooting Joining Domains and Test Authentication
J. Integration with Cisco Identity Services Engine (ISE)

IV. Creating Decryption Policies to Control HTTPS Traffic

A. Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Inspection Overview
B. Certificate Overview
C. Overview of HTTPS Decryption Policies
D. Activating HTTPS Proxy Function
E. Access Control List (ACL) Tags for HTTPS Inspection
F. Access Log Examples

V. Understanding Differentiated Traffic Access Policies and Identification Profiles

A. Overview of Access Policies
B. Access Policy Groups
C. Overview of Identification Profiles
D. Identification Profiles and Authentication
E. Access Policy and Identification Profiles Processing Order
F. Other Policy Types
G. Access Log Examples
H. ACL Decision Tags and Policy Groups
I. Enforcing Time-Based and Traffic Volume Acceptable Use Policies, and End User Notifications

VI. Defending Against Malware

A. Web Reputation Filters
B. Anti-Malware Scanning
C. Scanning Outbound Traffic
D. Anti-Malware and Reputation in Policies
E. File Reputation Filtering and File Analysis
F. Cisco Advanced Malware Protection
G. File Reputation and Analysis Features
H. Integration with Cisco Cognitive Intelligence

Course Outline

Securing the Web with Cisco Web Security Appliance (SWSA)

Course Outline (cont.)

VII. Enforcing Acceptable Use Control Settings

A. Controlling Web Usage
B. URL Filtering
C. URL Category Solutions
D. Dynamic Content Analysis Engine
E. Web Application Visibility and Control
F. Enforcing Media Bandwidth Limits
G. Software as a Service (SaaS) Access Control
H. Filtering Adult Content

VIII. Data Security and Data Loss Prevention

A. Data Security
B. Cisco Data Security Solution
C. Data Security Policy Definitions
D. Data Security Logs

IX. Performing Administration and Troubleshooting

A. Monitor the Cisco Web Security Appliance
B. Cisco WSA Reports
C. Monitoring System Activity Through Logs
D. System Administration Tasks
E. Troubleshooting
F. Command Line Interface

X. References

A. Comparing Cisco WSA Models
B. Comparing Cisco SMA Models
C. Overview of Connect, Install, and Configure
D. Deploying the Cisco Web Security Appliance Open Virtualization Format (OVF) Template
E. Mapping Cisco Web Security Appliance Virtual Machine (VM) Ports to Correct Networks
F. Connecting to the Cisco Web Security Virtual Appliance
G. Enabling Layer 4 Traffic Monitor (L4TM)
H. Accessing and Running the System Setup Wizard
I. Reconnecting to the Cisco Web Security Appliance
J. High Availability Overview
K. Hardware Redundancy
L. Introducing Common Address Redundancy Protocol (CARP)
M. Configuring Failover Groups for High Availability
N. Feature Comparison Across Traffic Redirection Options
O. Architecture Scenarios When Deploying Cisco AnyConnect Secure Mobility

XI. Lab outline

- 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