Securing the Web with Cisco Web Security Appliance v1.0 (300-725)

Exam Description: Securing the Web with Cisco Web Security Appliance v1.0 (SWSA 300-725) is a 90-minute exam associated with the CCNP Security Certification. This exam tests a candidate's knowledge of Cisco Web Security Appliance, including proxy services, authentication, decryption policies differentiated traffic access policies and identification policies, acceptable use control settings, malware defense, and data security and data loss prevention. The course, Securing Web with Cisco Email Security Appliance, helps candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

10% 1.0 Cisco WSA Features

1.1 Describe Cisco WSA features and functionality
- 1.1.a Proxy service
- 1.1.b Cognitive Threat Analytics
- 1.1.c Data loss prevention service
- 1.1.d Integrated L4TM service
- 1.1.e Management tools

1.2 Describe WSA solutions
- 1.2.a Cisco Advanced Web Security Reporting
- 1.2.b Cisco Content Security Management Appliance

1.3 Integrate Cisco WSA with Splunk

1.4 Integrate Cisco WSA with Cisco ISE

1.5 Troubleshoot data security and external data loss using log files

20% 2.0 Configuration

2.1 Perform initial configuration tasks on Cisco WSA

2.2 Configure an Acceptable Use Policy

2.3 Configure and verify web proxy features
- 2.3.a Explicit proxy functionality
- 2.3.b Proxy access logs using CLI
- 2.3.c Active directory proxy authentication

2.4 Configure a referrer header to filter web categories

10% 3.0 Proxy Services

3.1 Compare proxy terms
- 3.1.a Explicit proxy vs. transparent proxy
- 3.1.b Upstream proxy vs. downstream proxy

3.2 Describe tune caching behavior for safety or performance

3.3 Describe the functions of a Proxy Auto-Configuration (PAC) file

3.4 Describe the SOCKS protocol and the SOCKS proxy services

10% 4.0 Authentication

4.1 Describe authentication features
- 4.1.a Supported authentication protocols
- 4.1.b Authentication realms
- 4.1.c Supported authentication surrogates supported
- 4.1.d Bypassing authentication of problematic agents
- 4.1.e Authentication logs for accounting records
- 4.1.f Re-authentication

4.2 Configure traffic redirection to Cisco WSA using explicit forward proxy mode

4.3 Describe the FTP proxy authentication

4.4 Troubleshoot authentication issues

10% 5.0 Decryption Policies to Control HTTPS Traffic

5.1 Describe SSL and TLS inspection

5.2 Configure HTTPS capabilities
- 5.2.a HTTPS decryption policies
- 5.2.b HTTPS proxy function
- 5.2.c ACL tags for HTTPS inspection
- 5.2.d HTTPS proxy and verify TLS/SSL decryption
- 5.2.e Certificate types used for HTTPS decryption

5.3 Configure self-signed and intermediate certificates within SSL/TLS transactions

10% 6.0 Differentiated Traffic Access Policies and Identification Profiles

6.1 Describe access policies

6.2 Describe identification profiles and authentication

6.3 Troubleshoot using access logs

10% 7.0 Acceptable Use Control

7.1 Configure URL filtering

7.2 Configure the dynamic content analysis engine

7.3 Configure time-based & traffic volume acceptable use policies and end user notifications

7.4 Configure web application visibility and control (Office 365, third-party feeds)

7.5 Create a corporate global acceptable use policy

7.6 Implement policy trace tool to verify corporate global acceptable use policy
7.7 Configure WSA to inspect archive file types

10% 8.0 Malware Defense
8.1 Describe anti-malware scanning
8.2 Configure file reputation filtering and file analysis
8.3 Describe Advanced Malware Protection (AMP)
8.4 Describe integration with Cognitive Threat Analytics

10% 9.0 Reporting and Tracking Web Transactions
9.1 Configure and analyze web tracking reports
9.2 Configure Cisco Advanced Web Security Reporting (AWSR)
9.2.a Basic web usage
9.2.b Custom filters

9.3 Troubleshoot connectivity issues