Securing the Web with Cisco Secure Web Appliance v1.1 (300-725)

Exam Description: Securing the Web with Cisco Secure Web Appliance v1.1 (SWSA 300-725) is a 90-minute exam associated with the CCNP Security Certification. This exam tests a candidate's knowledge of Cisco Secure Web Appliance (formerly 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 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 Features

- 1.1 Describe Cisco Secure Web Appliance features and functionality
  - 1.1.a Proxy service
  - 1.1.b Cognitive Intelligence (formerly Cognitive Threat Analytics)
  - 1.1.c Data loss prevention service
  - 1.1.d Integrated L4TM service
  - 1.1.e Management tools
- 1.2 Describe Secure Web Appliance solutions
  - 1.2.a Cisco Advanced Web Security Reporting
  - 1.2.b Cisco Secure Email and Web Manager
- 1.3 Integrate Cisco Secure Web Appliance with Advanced Web Security Reporting
- 1.4 Integrate Cisco Secure Web Appliance 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 Secure Web Appliance
- 2.2 Configure an access 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 Describe deployment options
- 3.1.a Explicit proxy
- 3.1.b Transparent proxy
- 3.1.c Upstream proxy
- 3.1.d High availability

3.2 Describe these features:
- 3.2.a Tune caching
- 3.2.b IP spoofing
- 3.2.c Web proxy ports
- 3.2.d Range requests

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 methods
- 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 Secure Web Appliance using transparent proxy with WCCP, PBR, or an L4 switch

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 time-based and traffic volume acceptable use policies and end user notifications
- 7.3 Configure web application visibility and control (Office 365, third-party feeds)
- 7.4 Create a corporate global acceptable use policy
- 7.5 Implement policy trace tool to verify corporate global acceptable use policy
- 7.6 Configure Secure Web Appliance to inspect archive file types

10% 8.0 Malware Defense

- 8.1 Describe scanning engines
- 8.2 Configure file reputation filtering and file analysis
- 8.3 Describe Cisco Secure Endpoint
- 8.4 Describe integration with Cognitive Intelligence

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
- 9.4 Interpret system health using the System Health Dashboard
- 9.5 Describe REST API support