Securing Email with Cisco Secure Email Gateway v1.1 (300-720)

Exam Description: Securing Email with Cisco Secure Email Gateway v1.1 (SESA 300-720) is a 90-minute exam associated with the CCNP Security Certification. This exam certifies a candidate's knowledge of Cisco Secure Email Gateway (formerly Cisco Email Security Appliance), including administration, spam control and antispam, message filters, data loss prevention, LDAP, email authentication and encryption, and system quarantines and delivery methods.

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.

15% 1.0 Administration

- 1.1 Configure Cisco Secure Email Gateway features
  - 1.1.a Hardware and virtual machine performance specifications
  - 1.1.b Initial configuration process
  - 1.1.c Routing and delivery features
  - 1.1.d GUI
  - 1.1.e Manage certificate authorities
  - 1.1.f Logging
- 1.2 Describe centralized services on a Cisco Secure Email and Web Manager
- 1.3 Configure mail policies
  - 1.3.a Incoming and outgoing messages
  - 1.3.b User matching
  - 1.3.c Message splintering
- 1.4 Integrate Cisco Secure Email Gateway with SecureX
- 1.5 Configure Cisco Secure Email Threat Defense

15% 2.0 Spam Control with Talos SenderBase and Antispam

- 2.1 Control spam with Talos SenderBase and Antispam
- 2.2 Describe graymail management solution
- 2.3 Configure file reputation filtering and file analysis features
- 2.4 Implement malicious or undesirable URLs protection
- 2.5 Describe the bounce verification feature

20% 3.0 Content and Message Filters

- 3.1 Describe the functions and capabilities of content filters
- 3.2 Create text resources such as content dictionaries, disclaimers, and templates
  - 3.2.a Dictionary filter rules

3.2.b Text resources management

3.3 Configure message filters components, rules, processing order, and attachment scanning

3.4 Configure scan behavior

3.5 Configure the Cisco Secure Email Gateway to scan for viruses using Sophos and McAfee scanning engines

3.6 Configure outbreak filters

3.7 Configure Data Loss Prevention (DLP)

15% 4.0 LDAP and SMTP Sessions

4.1 Configure and verify LDAP servers and queries (Queries and Directory Harvest Attack)

4.2 Understand spam quarantine functions

4.2.a Authentication for end users of spam quarantine

4.2.b Use spam quarantine alias to consolidate queries

4.3 Understand SMTP functionality

4.3.a Email pipeline

4.3.b Sender and recipient domains

4.3.c SMTP session authentication using client certificates

4.3.d SMTP TLS authentication

4.3.e TLS email encryption

20% 5.0 Email Authentication and Encryption

5.1 Configure Domain Keys and DKIM signing

5.2 Configure SPF and SIDF

5.3 Configure DMARC verification

5.4 Configure forged email detection

5.5 Configure email encryption

5.6 Describe S/MIME security services and communication encryption with other MTAs

5.7 Configure Cisco Secure Email

15% 6.0 System Quarantines and Delivery Methods

6.1 Configure quarantine (spam, policy, virus, and outbreak)

6.2 Use safelists and blocklists to control email delivery

6.3 Manage messages in local or external spam quarantines

6.4 Configure virtual gateways