Securing Networks with Cisco Firewalls v1.1 (300-710)

Exam Description: Securing Networks with Cisco Firewalls v1.1 (SNCF 300-710) is a 90-minute exam associated with the CCNP Security Certification. This exam tests a candidate's knowledge of Cisco Secure Firewall (formerly Cisco Firepower) and Cisco Secure Firewall Management Center (formerly Cisco Firepower Management Center), including policy configurations, integrations, deployments, management, and troubleshooting.

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.

30% 1.0 Deployment

- 1.1 Implement Secure Firewall modes
  - 1.1.a Routed mode
  - 1.1.b Transparent mode
- 1.2 Implement NGIPS modes
  - 1.2.a Passive
  - 1.2.b Inline
- 1.3 Implement high availability options
  - 1.3.a Port channels
  - 1.3.b Failover
  - 1.3.c Equal-Cost Multipath (ECMP) routing
  - 1.3.d Static route tracking
  - 1.3.e Clustering
- 1.4 Describe virtual appliance on-premises and cloud deployment

30% 2.0 Configuration

- 2.1 Configure system settings in Secure Firewall Management Center
- 2.2 Configure policies in Secure Firewall Management Center
  - 2.2.a Access control
  - 2.2.b Intrusion
  - 2.2.c Malware & File
  - 2.2.d DNS
  - 2.2.e Identity
  - 2.2.f Decryption
  - 2.2.g Prefilter
- 2.3 Configure these features using Secure Firewall Management Center
  - 2.3.a Network discovery

- 2.3.b Application detectors
- 2.3.c Correlation
- 2.3.d Encrypted visibility engine

2.4 Configure objects using Secure Firewall Management Center
- 2.4.a Object management
- 2.4.b Intrusion rules

2.5 Configure devices using Secure Firewall Management Center
- 2.5.a Device management
- 2.5.b NAT
- 2.5.c VPN
- 2.5.d QoS
- 2.5.e Platform settings
- 2.5.f Certificates
- 2.5.g Routing

2.6 Describe the use of Snort within Secure Firewall Threat Defense

25% 3.0 Management and Troubleshooting

3.1 Troubleshoot with Secure Firewall Management Center GUI and device CLI

3.2 Configure dashboards and reporting in Secure Firewall Management Center

3.3 Troubleshoot using:
- 3.3.a packet capture procedures
- 3.3.b Packet Tracer

3.4 Analyze risk and standard reports

3.5 Describe device management tools
- 3.5.a Cisco Defense Orchestrator
- 3.5.b Cloud-delivered Firewall Management Center
- 3.5.c Secure Firewall Device Manager
- 3.5.d Secure Firewall Management Center

15% 4.0 Integration

4.1 Configure Cisco Secure Firewall Malware Defense (formerly AMP for Networks) in Secure Firewall Management Center

4.2 Configure Cisco Secure Endpoint (formerly AMP for Endpoints) integration with Secure Firewall Management Center

4.3 Implement Threat Intelligence Director for third-party security intelligence feeds

4.4 Describe using Cisco SecureX for security investigations

4.5 Describe Secure Firewall Management Center integration using pxGrid

4.6 Describe Rapid Threat Containment (RTC) functionality within Secure Firewall Management Center

4.7 Describe Cisco Security Analytics and Logging