Securing Networks with Cisco Firewalls v1.2 (300-710)

Exam Description: Securing Networks with Cisco Firewalls v1.2 (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 and Cisco Secure Firewall 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 management

30% 2.0 Configuration

- 2.1 Configure system settings in Secure Firewall Management Center
- 2.2 Configure security policies such as access control, DNS, identity, and network analysis policy in Secure Firewall Management Center
- 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 such as certificates, platform setting, and health policy
- 2.5.b Network settings such as NAT, QoS, and routing
- 2.5.c Secure access such as zero trust network access, and VPN

2.6 Describe 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 Firewall Threat Defense using tools:
- 3.3.a Packet capture procedures
- 3.3.b Packet Tracer
- 3.3.c Firewall engine debug
- 3.3.d System Support Trace

3.4 Analyze risk and standard reports such as events (connection, discovery, intrusion, malware, and unified) and network map

3.5 Describe device management tools
- 3.5.a Cisco Security Cloud Control Firewall Management (formerly Cloud-delivered Firewall Management Center)
- 3.5.b Secure Firewall Device Manager
- 3.5.c Secure Firewall Management Center

15% 4.0 Integration

4.1 Configure Cisco Secure Firewall Malware Defense in Secure Firewall Management Center

4.2 Configure Cisco Secure Endpoint integration with Secure Firewall Management Center

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

4.4 Describe using Cisco XDR 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

4.8 Describe Splunk integration and AI-driven threat intelligence