Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (300-740)

Exam Description: Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (SCAZT 300-740) is a 90-minute exam associated with the CCNP Security Certification. This exam certifies a candidate's knowledge of designing and implementing cloud security architecture, user and device security, network and cloud security, application and data security, visibility and assurance, and threat response.

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 Cloud Security Architecture

1.1 Describe the components of the Cisco Security Reference Architecture
- 1.1.a Threat intelligence
- 1.1.b Security operations toolset
- 1.1.c User/device security
- 1.1.d Network security: cloud edge and on-premises
- 1.1.e Workload, application, and data security

1.2 Describe use cases and the recommended capabilities within an integrated architecture
- 1.2.a Common identity
- 1.2.b Converged multicloud policy
- 1.2.c SASE integrations
- 1.2.d Zero-trust network access

1.3 Describe industry security frameworks such as NIST, CISA, and DISA

1.4 Describe the SAFE architectural framework

1.5 Describe the SAFE Key structure
- 1.5.a Places in the Network
- 1.5.b Secure Domains

20% 2.0 User and Device Security

2.1 Implement user and device authentication via identity certificates

2.2 Implement multifactor authentication for users and devices

2.3 Implement endpoint posture policies for user access to resources

2.4 Configure SAML/SSO and OIDC using an identity provider connection

2.5 Configure user and device trust using SAML authentication for a mobile or web application

20% 3.0 Network and Cloud Security

3.1 Determine security policies for endpoints to control access to cloud applications
- 3.1.a URL filtering (web layer and DNS layer)
- 3.1.b Advanced app control
- 3.1.c Network protocol blocking such as FTP and bit torrent
- 3.1.d Direct-internet-access for trusted business applications
- 3.1.e Web application firewall
- 3.1.f Reverse proxy

3.2 Determine security policies for endpoints to control access to SaaS applications such as Office 365, Workday, and Salesforce

3.3 Determine security policies for remote users using VPN or application-based

3.4 Determine security policies for network security edge to enforce application policy
- 3.4.a Security services edge
- 3.4.b Cisco Secure Firewall (FTD and ASA)

25% 4.0 Application and Data Security

4.1 Describe the MITRE ATT&CK framework and attacker defense mitigation techniques

4.2 Describe cloud security attack tactics and mitigation strategies

4.3 Describe how web application firewalls protect against DDoS attacks

4.4 Determine security policies for application enforcement using Cisco Secure Workload and enforcement agents
- 4.4.a Lateral movement prevention
- 4.4.b Microsegmentation

4.5 Determine cloud (hybrid and multicloud) platform security policies based on application connectivity requirements (third- party providers such as AWS, Azure, and Google Cloud)

15% 5.0 Visibility and Assurance

5.1 Describe the Cisco XDR solution

5.2 Describe use cases for visibility and assurance automation

5.3 Describe benefits and capabilities of visibility and logging tools such as SIEM, Open Telemetry, and Cisco Secure Network Analytics

5.4 Validate traffic flow and telemetry reports for baseline and compliance behavior analysis

5.5 Diagnose issues with user application and workload access
- 5.5.a Cisco Secure Network Analytics
- 5.5.b Cisco Secure Cloud Analytics
- 5.5.c Cisco Secure Cloud Insights
- 5.5.d Cisco Secure Analytics and Logging

5.6 Verify user access to applications and data using tools (firewall logs, Duo, Umbrella, and Cisco Secure Workload)

5.7 Analyze application dependencies using tools such as firewall logs and Cisco Secure Workload

10% 6.0 Threat Response

6.1 Describe use cases for response automation
6.2 Determine actions based on telemetry reports
6.3 Determine policies based on security audit reports
6.4 Determine action based on user or application compromise
- 6.4.a Contain
- 6.4.b Report
- 6.4.c Remediate
- 6.4.d Reinstantiate