Designing and Implementing Secure Cloud Access for Users and Endpoints v2.0 (300-740)

Exam Description: Designing and Implementing Secure Cloud Access for Users and Endpoints v2.0 (SCAZT 300-740) is a 90-minute exam associated with the CCNP Security Certification. This exam certifies a candidate's knowledge of zero-trust frameworks, identity management with Cisco Duo, and the deployment of policies through SSE, ZTNA, and microsegmentation. The exam evaluates skills in cloud operations, including viability, telemetry analysis, and the integration of Cisco Secure Access with XDR and Splunk.

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 Concepts

- 1.1 Describe industry cloud security frameworks such as NIST SP 800-207 and CISA Zero Trust Maturity Model v2.0
- 1.2 Select mitigation methods to defend against attacker, tactics, and techniques using the MITRE ATT&CK cloud frameworks (identity providers [IDPs], SaaS, and IaaS)
- 1.3 Describe security requirements for public cloud platforms such as AWS, Azure, and Google Cloud (GCP)
  - 1.3.a Authentication and access control
  - 1.3.b Secure using cloud native constructs such as VPCs, security groups, access lists, or multi-cloud defense
  - 1.3.c Posture and compliance
  - 1.3.d Shared Responsibility Model
- 1.4 Describe operational requirements for public cloud platforms such as AWS, Azure, and Google Cloud (GCP)
  - 1.4.a Visibility and monitoring
  - 1.4.b Infrastructure
  - 1.4.c Consumption model (PaaS, IaaS, SaaS)
- 1.5 Describe private cloud including local hypervisors such as VMware and container orchestration platforms such as Kubernetes
- 1.6 Describe how eBPF-based tools (Cilium, Tetragon) provide runtime security observability and enforcement for containerized workloads

20% 2.0 Identity

- 2.1 Describe the use and function of identity intelligence across IDPs
- 2.2 Implement user and device authentication via identity certificates

2.3 Implement multifactor authentication (including phishing resistant) for users and devices with Cisco Duo
2.4 Implement endpoint posture policies for user access to resources
2.5 Configure user and device trust using SAML authentication for a mobile or web application
2.6 Configure SSO and user provisioning using an IDP connection
2.5.a SCIM
2.5.b SAML

30% 3.0 Policies

3.1 Describe encryption methods for data in transit and at rest in cloud environments such as TLS, IPsec in context, and tunnels
3.2 Describe how features such as IPS, DLP, and malware protection help provide secure private access
3.3 Describe the use, purpose, and characteristics of AI Defense
3.4 Describe AI features in Secure Access such AI Access and AI Guardrails
3.5 Describe how web application firewalls protect against DDoS
3.6 Determine security policies for network security edge to enforce application policy
3.5.a Security services edge (SSE)
3.5.b SDWAN devices such as Cisco Secure Firewall (FTD), Meraki, and Catalyst

3.7 Determine security policies for application enforcement using Cisco Secure Workload and enforcement agents
3.7.a Lateral movement prevention
3.7.b Microsegmentation
3.7.c Vulnerability assessment and response
3.7.d Application discovery and monitoring
3.7.e Policy creation, validation, and analysis

30% 4.0 Access

4.1 Configure DNS security
4.2 Configure Secure Web Gateway
4.3 Configure Data Loss Protection
4.4 Configure CASB
4.5 Configure secure private access for workloads
4.5.a Resource connector or IPsec backhaul
4.5.b Branch connectivity

4.6 Configure secure private access for users
4.6.a VPN as a service with ISE as a RADIUS server using Secure Access and Cisco Secure Client
4.6.b Digital experience monitoring using Thousand Eyes and Secure Access
4.6.c Zero-trust access (clientless and client-based) using Secure Access, Cisco Secure Client, QUIC, and MASQUE

10% 5.0 Operations

5.1 Select the process or tool that provides cloud application (includes workloads and containers) visibility, microsegmentation, traffic analysis, and policy enforcement based on security requirements
5.2 Interpret traffic flow and telemetry reports for baseline and compliance behavior analysis
5.3 Interpret Cisco Secure Access dashboards
5.4 Integrate Cisco Secure Access with Cisco XDR and Splunk Enterprise to enhance SOC operations