Designing Cisco Security Infrastructure v1.0 (300-745)

Exam Description: Designing Cisco Security Infrastructure v1.0 (SDSI 300- 745) is a 90-minute exam associated with the CCNP Security Certification. This exam tests a candidate's knowledge of security architecture design, including secure infrastructure, applications, risk, events, requirements, artificial intelligence, automation, and DevSecOps. The course, Designing Cisco Security Infrastructure, helps candidates to prepare for this exam.

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 Secure Infrastructure

1.1 Select the security approaches to protect against threats

1.1.a Endpoint and client devices (on-network, off-network, and remote)

1.1.b Identity such as MFA, passwordless, continuous trust, and identity intelligence

1.1.c Email (phishing, ransomware, business email compromise, malware, and spoofing)

1.2 Modify the security architecture to address technical requirements

1.2.a Hybrid workers

1.2.b IoT

1.2.c SaaS

1.2.d Applications across data center and multi-cloud

1.3 Select a VPN and tunneling solution such as SD-WAN, IPsec, MPLS, GRE, DMVPN, and public cloud tunnel options based on business and technical requirements

1.4 Select the approach to secure the infrastructure management and control planes

1.5 Select the firewall feature or architecture such as traditional firewall, Nextgen firewall, Web Application Firewall, IPS/IDS, distributed firewall, eBPF, and host-based firewall given business and technical requirements

25% 2.0 Applications

2.1 Select the security solution such as firewalls, SSL offloading, SSL decryption, DLP, and endpoint based on application and flow data, to protect an application

2.2 Select the design for cloud-native applications, microservices, containers, and serverless architectures to ensure segmentation/microsegmentation

2.3 Describe the design policies to address the impacts of emerging technologies such as generative AI, machine learning, and quantum computing

30% 3.0 Risk, Events, and Requirements

3.1 Describe how the SOC leverages incident handling and incident response tools

3.2 Modify a design to mitigate risk

3.3 Modify a security design following an incident

3.4 Describe the use of frameworks such as MITRE CAPEC, NIST SP 800-37, and SAFE in the lifecycle of a security design

3.5 Match the regulatory and industry compliance document to a given business or technical scenario

15% 4.0 Artificial Intelligence, Automation, and DevSecOps

4.1 Describe the functions, uses, and role of AI in securing network infrastructure

4.2 Select the feature or element required to support automated security architecture/infrastructure such as API tooling, Infrastructure as Code, monitoring, container scanning, security telemetry, alerting, and SOAR

4.3 Select the next step in workflows and pipelines to be implemented by DevSecOps engineers to minimize risk from automated deployments