Designing and Implementing Cloud Connectivity v1.0 (300-440)

Exam Description: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300-440) is a 90-minute exam associated with the CCNP Enterprise Certification. This exam certifies a candidate's knowledge of designing and implementing cloud connectivity, including architecture models, IPsec, SD-WAN, operation, and design.

The following topics are general guidelines for the content likely to be included in the exam. However, other related topics may also appear on any specific exam delivery. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

15% 1.0 Architecture Models

1.1 Describe internet-based connectivity to cloud providers (AWS, Azure, and Google Cloud)
- 1.1.a Native IPsec
- 1.1.b Cisco SD-WAN internet connectivity

1.2 Describe private connectivity to cloud providers (AWS, Azure, and Google Cloud)
- 1.2.a MPLS provider
- 1.2.b Colocation provider
- 1.2.c SDCI regional cross-connect

1.3 Describe connectivity to SaaS cloud providers (AWS, Azure, and Google Cloud)
- 1.3.a Direct internet access models into SaaS
- 1.3.b Indirect access models via a Cloud Security Provider
- 1.3.c SaaS connectivity via a centralized internet gateway
- 1.3.d Dedicated connectivity to a SaaS provider

15% 2.0 Design

2.1 Recommend the connectivity model to provide high availability, resiliency, SLAs, and reliability based on business and technical requirements

2.2 Recommend the connectivity model based on network architecture requirements such as bandwidth, QoS, dedicated vs shared, multi-homing, and routing needs based on business and technical requirements

2.3 Recommend a connectivity model to meet regulatory compliance (NIST, FEDRAMP, ISO) based on business and technical requirements

2.4 Describe cloud-native security policies for AWS, Azure, and Google Cloud, such as east/west traffic within the cloud provider, backhaul internet traffic, inbound connectivity to the internet

25% 3.0 IPsec Cloud Connectivity

3.1 Configure IPsec internet-based secure cloud connectivity between an on-premises Cisco IOS XE router to a native AWS, Azure, and Google Cloud endpoint

3.2 Configure IPsec internet-based secure cloud connectivity between an on-premises Cisco IOS XE router and an AWS, Azure, or Google cloud-hosted Cisco IOS XE router

3.3 Configure routing on Cisco IOS XE to integrate with cloud networks using BGP and OSPF, including redistribution and static routing

25% 4.0 SD-WAN Cloud Connectivity

4.1 Configure Cisco SD-WAN internet-based secure cloud connectivity for AWS, Azure, and Google Cloud

4.2 Configure Cisco SD-WAN OnRamp to a SaaS cloud provider

4.3 Configure Cisco SD-WAN policies (north/south and east/west)

- 4.3.a Security
- 4.3.b Routing
- 4.3.c Application

20% 5.0 Operation

5.1 Diagnose IPsec internet-based secure cloud connectivity between an on-premises Cisco IOS XE router to a native AWS, Azure, and Google Cloud endpoint

5.2 Diagnose routing issues on Cisco IOS XE to integrate with cloud networks using BGP and OSPF, including redistribution and static routing

5.3 Diagnose Cisco SD-WAN internet-based secure cloud connectivity for AWS, Azure, and Google Cloud

5.4 Diagnose Cisco SD-WAN policy issues (north/south and east/west)

- 5.4.a Security
- 5.4.b Routing
- 5.4.c Application