Designing and Implementing Secure Cloud Connectivity (CPLL-ENCC)

Duration: 180 Days

The Designing and Implementing Secure Cloud Connectivity (ENCC) Learning Path helps you develop the skills required to design and implement enterprise cloud connectivity solutions. You will learn how to leverage both private and public internet-based connectivity to extend the enterprise network to cloud providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). You will explore the basic concepts surrounding public cloud infrastructure and how services like Software as a Service (SaaS), Direct Internet Access (DIA), and Cisco Umbrella can be integrated. You will practice how to analyze and recommend connectivity models that are scalable, resilient, secure, and provide the best quality of experience for users. You will learn to implement both Internet Protocol Security (IPsec) and Software-Defined Wide-Area Network (SD-WAN) cloud connectivity, as well as build overlay routing with Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP). You will also implement control and data policies across the SD-WAN fabric and integrate Cisco Umbrella cloud security. Finally, you will practice troubleshooting cloud connectivity issues relating to IPsec, SD-WAN, routing, application performance, and policy application.

This Learning Path prepares you for the 300-440 ENCC v1.0 exam. If passed, you earn the Cisco Certified Specialist–Enterprise Cloud Connectivity certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Enterprise certification.

Skills You'll Learn:

- Develop the expertise to design and implement scalable, resilient, and secure connectivity solutions that extend enterprise networks to major cloud providers, including AWS, Microsoft Azure, and GCP
- Explore the application of virtual private network (VPN) technologies and Cisco Catalyst SD-WAN, including Cloud OnRamp, to manage both private and internet-based cloud connectivity
- Gain the ability to implement robust security measures, including the integration of Cisco Umbrella and native SD-WAN security policies, to protect cloud-based traffic and meet regulatory compliance requirements
- Learn to optimize user experience and application performance for SaaS providers through the implementation of Application Quality of Experience (AppQoE) and efficient routing workflows

- Acquire the diagnostic skills necessary to troubleshoot complex cloud connectivity issues, including underlay and overlay routing, including OSPF and BGP, IPsec tunnels, and SD-WAN policy application

Learning Path Objectives:

1. Describe Public Cloud Connectivity Architecture Models: Explore the basic concepts and terminology of public cloud deployments, services, computing, and providers, as well as connectivity options.
2. Describe Public Cloud Connectivity Design Best Practices: Design secure, scalable, and resilient enterprise cloud connectivity solutions and learn about network redundancy and security policies.
3. Implement Internet-based Public Cloud Connectivity: Learn how you can use IPsec VPNs to implement internet-based cloud connectivity.
4. Implement Cisco SD-WAN Public Cloud Connectivity: Integrate internet-based cloud connectivity with your Cisco SD-WAN fabric and explore cloud security and control policy options.
5. Diagnose Public Cloud Connectivity: Practice and develop your cloud connectivity diagnostic and troubleshooting skills.