Designing and Implementing Secure Cloud Connectivity

What you'll learn in this course

The Designing and Implementing Secure Cloud Connectivity (ENCC) training 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 training 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. This training also earns you 32 Continuing Education (CE) credits toward recertification.

Course Duration

- Instructor-led training: 4 days with hands-on lab practice
- Virtual instructor-led training: 4 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 4 days of instruction with hands-on lab practice

How you'll benefit

This training will help you:

- Develop the skills required to design and implement enterprise cloud connectivity solutions
- Learn how to apply the virtual private network (VPN) and overlay networking technology, including Cisco Catalyst SD-WAN to extend the enterprise network to cloud providers, such as AWS, Microsoft Azure, and GCP using both private connectivity services and public internet as an underlay
- Examine the solutions for optimizing access to SaaS cloud providers and the workflows for diagnosing and troubleshooting cloud connectivity issues
- Gain knowledge for protocols, solutions, and designs to acquire professional-level and expert-level enterprise roles
- Prepare for the 300-440 ENCC v1.0 exam
- Earn 32 CE credits toward recertification

Who should enroll

- Cloud Architects
- Cloud Administrators
- Cloud Engineers
- Cloud Network Engineers
- Cloud Automation Engineers
- Cloud Systems Engineers
- Cloud Security Managers
- Cloud Consultants
- Cloud Application Developers
- Systems Engineers
- Technical Solutions Architects

Course details

Objectives

- Describe the fundamental components and concepts of cloud computing, including deployment models, cloud services, and cloud providers, to provide learners with a comprehensive overview of the subject
- Describe the options available for establishing connectivity to public cloud services, including point-to-point IPsec VPN and various Cisco Catalyst SD-WAN Cloud OnRamp deployment options
- Describe private connectivity options to public cloud provider infrastructure
- Describe the available options for connectivity to SaaS applications from a geographically distributed organization's premises
- Describe various cloud connectivity options and explore high availability, resiliency, and scalability capabilities with Cisco cloud connectivity
- Describe and explore public cloud security and its components comprehensively
- Describe regulatory compliance requirements
- Explain the available options and describe the procedures for implementing IPsec-driven internet-based public cloud connectivity
- Introduce overlay routing
- Introduce the Cisco Catalyst SD-WAN capabilities for internet-based public cloud connectivity
- Describe Cisco SD-WAN native and cloud security capabilities
- Introduce the Cloud OnRamp for SaaS
- Introduce the Catalyst Cisco SD-WAN Policies
- Introduce AppQoE
- Describe how to diagnose and troubleshoot common issues for connectivity to public cloud environments using internet-based connectivity
- Troubleshoot OSPF, BGP, route redistribution, and static routes deployed in cloud environments
- Describe Cisco SD-WAN and connectivity to public cloud providers

Course Outline

- Public Cloud Fundamentals
- Internet-Based Connectivity to Public Cloud
- Private Connectivity to Public Cloud
- SaaS Connectivity
- Resilient and Scalable Public Cloud Connectivity
- Cloud-Native Security Policies
- Regulatory Compliance Requirements
- Internet-Based Public Cloud Connectivity
- Overlay Routing Deployment
- Cisco SD-WAN Internet-Based Cloud Connectivity
- Cisco SD-WAN Cloud Security
- Cloud OnRamp for Saas
- Cisco SD-WAN Policies
- Application Quality of Experience
- Internet-Based Public Cloud Connectivity Diagnostics
- Overlay Routing Diagnostics
- Cisco SD-WAN Public Cloud Connectivity Diagnostics

Lab outline

- Initial Lab Network Exploration
- Implement IPsec Connectivity to Public Cloud Gateways
- Implement IPsec Connectivity to Cloud-Hosted Cisco IOS-XE Routers
- Implement Overlay Routing
- Deploy Cloud OnRamp for Multicloud
- Deploy Umbrella Cloud Security
- Implement Cloud OnRamp for SaaS with AppQoE
- Troubleshoot Underlay Connectivity
- Troubleshoot Overlay Routing
  Diagnose Cloud OnRamp for Multicloud