Current Technologies
Computer Learning Centers

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Cisco Partner
Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Designing and Implementing Secure Cloud Access for Users and Endpoints

Designing and Implementing Secure Cloud Access for Users and Endpoints

In this Designing and Implementing Secure Cloud Access for Users and Endpoints course delivers a comprehensive, end-to-end view of modern enterprise and cloud security architecture using Cisco's security portfolio and industry-aligned frameworks. The curriculum begins with industry security frameworks and Cisco Security Reference Architectures, including Cisco SAFE, to establish a structured, repeatable approach to designing security across users, devices, networks, applications, and cloud environments. Learners gain a clear understanding of common enterprise and cloud security use cases and how architectural decisions map to real-world operational and risk requirements.

The course then focuses on identity-first and access-based security, covering certificate-based authentication, single sign-on using SAML and OpenID Connect, Cisco Duo multifactor authentication, Cisco ISE endpoint compliance, and secure remote access with AnyConnect. Students learn how identity, posture, and context are enforced consistently across VPNs, applications, and cloud services. Web, DNS, and SaaS security topics are explored in depth through Cisco Umbrella Secure Internet Gateway, content filtering, reverse proxy architectures, and SaaS optimization and monitoring using Cisco ThousandEyes.

Advanced modules address on-premises and cloud threat prevention, including Cisco Secure Firewall, web application firewalls, Cisco Secure Workload for workload segmentation and policy enforcement, and multicloud security policies. Learners gain visibility into cloud threats, attack surface management, cloud assurance, and analytics using Cisco Secure Network Analytics, logging, and Cisco XDR. The course concludes with automation and response, demonstrating how cloud policies, threat detection, and incident response can be automated to reduce risk and response time. A robust lab program reinforces all concepts through hands-on configuration, integration, monitoring, and incident response exercises, preparing learners to design, deploy, and operate secure, zero-trust, cloud-enabled enterprise environments.

This training prepares you for the 300-740 SCAZT v1.0 exam. If passed, you earn the Cisco Certified Specialist – Security Secure Cloud Access certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification. This training also earns you 40 Continuing Education (CE) credits toward recertification.

Course Duration
5 days

Course Price
$4,395.00 or 44 CLCs

Methods of Delivery
- Instructor Led
- Virtual ILT
- On-Site

How you'll benefit

This class will help you:

- Attain skills for designing and implementing cloud security architecture, user and device security, network and cloud security, cloud application and data security, cloud visibility and assurance, and responding to cloud threats
- Gain knowledge for protocols, solutions, and designs to acquire professional-level and expert-level cloud design and implementation roles
- Prepare for the 300-740 SCAZT v1.0 exam
- Earn 40 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The primary audience for this course is as follows:

- Network Engineers
- Network Security Engineers
- Network Architects
- Sales/Presales Engineers

Prerequisites

The knowledge and skills you are expected to have before attending this training are:

- Good understanding of enterprise routing and switching
- Good understanding of WAN networking
- Good understanding of Cisco SD-WAN
- Good understanding of Public Cloud services
- Good understanding of VPN technologies
- Good understanding of Cisco security solutions

OUTLINE

Module 1: Certificate-Based User and Device Authentication

Module 2: Cisco Duo Multifactor Authentication for Application Protection

Module 3: Cisco Duo with AnyConnect VPN for Remote Access

Module 4: Cisco ISE Endpoint Compliance Services

Module 5: SSO using SAML or OpenID Connect

Module 6: Reverse Proxy

Module 7: Cisco SD-WAN Security Content Filtering

Module 8: Cisco SD-WAN to Cisco Umbrella SIG Integration

Module 9: Cisco Umbrella Cloud Access Security Broker

Module 10: Security Policies for Remote Access VPN

Module 11: Cisco Secure Access

Module 12: Cisco Secure Firewall

Module 13: Web Application Firewall

Module 14: Cisco Secure Workload Deployments, Agents, and Connectors

Module 15: Cisco Secure Workload Structure and Policy

Module 16: Multicloud Security Policies

Module 17: Cloud Security Attacks and Mitigations

Module 18: Cloud Visibility and Assurance

Module 19: Cisco Secure Network Analytics and Cisco Secure Analytics and Logging

Module 20: Cisco XDR

Module 21: Cisco Attack Surface Management

Module 22: Cloud Applications and Data Access Verifications

Module 23: Industry Security Frameworks

Module 24: Cisco Security Reference Architecture Fundamentals

Module 25: Cisco Security Reference Architecture Common Use Cases

Module 26: Cisco SAFE Architecture

Module 27: Cisco SD-WAN with ThousandEyes

Module 28: Automation of Cloud Policy

Module 29: Response to Cloud Threats

Module 30: Automation of Cloud Threat Detection and Response

LAB OUTLINE

- Lab 1: Windows Client BYOD Onboarding Interactive Activity
- Lab 2: Use Cisco Duo MFA to Protect the Splunk Application
- Lab 3: Implement Cisco Duo Authentication Proxy MFA for Cisco Remote Access
- Lab 4: Compliance-Based Access
- Lab 5: Implement Web Security
- Lab 6: Deploy DIA Security with Unified Security Policy
- Lab 7: Configure Cisco Umbrella DNS Policies
- Lab 8: Deploy Cisco Umbrella Secure Internet Gateway
- Lab 9: Implement CASB Security
- Lab 10: Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense
- Lab 11: Configure Cisco Secure Firewall Policies
- Lab 12: Explore Cisco Secure Workload
- Lab 13: Explore the ATTACK Matrix Cloud-Based Techniques
- Lab 14: Explore Cisco Secure Network Analytics
- Lab 15: Explore Cisco XDR Incident Response Tasks