

Implementing Security Service Edge with Cisco Secure Access (CPLL-ICSA)

Duration: 180 days

The Implementing Security Service Edge with Cisco Secure Access (ICSA) Learning Path explores how to deploy, configure, and operate a Security Service Edge (SSE) solution using the Cisco Secure Access platform, highlighting key concepts, configurations, and verification procedures. You will learn about Secure Access Service Edge (SASE) and SSE architecture and the Cisco Secure Access platform, how to configure Secure Private Access (SPA) and Secure Internet Access (SIA) with zero-trust access, threat and content defense, and data loss prevention (DLP), and how to verify enforcement and monitor user experience.

This is a product Learning Path and does not map to a Cisco certification or exam. Cisco Secure Access is also covered in Implementing and Operating Cisco Security Core Technologies (SCOR) and Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) trainings.

Skills You'll Learn

- Design and deploy cloud-native security frameworks by applying SASE and SSE architectural principles within the organization
- Implement effective zero-trust access controls by configuring Secure Private Access and Secure Internet Access components
- Protect critical data from cyber threats using advanced threat defense and DLP configurations
- Optimize user experience and traffic enforcement through integrated Experience Insights tools and monitoring techniques
- Streamline security operations by integrating Cisco Secure Access with visibility platforms like Cisco XDR and Splunk

Learning Path Objectives:

1. SASE and CSA Overview: Learn how SASE converges network security and wide-area networking into a unified, cloud-based service. Examine the Cisco Secure Access architecture, primary use cases, management options, and the Admin Portal components.
2. CSA Foundation and Identity: Explore the "Get Started with Cisco Secure Access" workflow and user-side and application-side connectivity methods, configure user and group provisioning, and implement SAML-based Single Sign-On (SSO).

3. CSA Secure Private Access: Discover how to configure Secure Private Access using Resource Connectors and IPSec backhaul tunnels. You'll also learn to implement security controls, private access policy rules, and various user-side access methods, including client-based/browser-based ZTA, VPN as a Service, and Branch IPSec tunnels.
4. CSA Secure Internet Access: Learn how to configure Secure Internet Access using various user-side access methods, security controls, and internet access policy rules for accessing the internet and SaaS applications, as well as how to implement DLP and AI Guardrails.
5. CSA Visibility and SOC Integration: Figure out how Experience Insights provides visibility into endpoints, applications, and network performance, and how to integrate Cisco Secure Access with Cisco XDR and Splunk to support Security Operations Center (SOC) operations.

