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!

Configuring and Troubleshooting Cisco SASE v1.0 (Secure Access Service Edge)(SASE) v1.0

Configuring and Troubleshooting Cisco SASE v1.0 (Secure Access Service Edge)(SASE) v1.0

his five-day, hands-on, instructor-led course offers comprehensive training on Configuring and Troubleshooting Cisco Secure Access Service Edge (SASE). It equips students with the skills to implement, manage, and optimize cutting-edge Cisco SASE technologies such as Zero Trust Network Access (ZTNA), Firewall as a Service (FWaaS), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), DNS-Layer Security, Threat Intelligence and Prevention, and Cisco DUO. The goal is to provide participants with the expertise necessary to proficiently configure, manage, and troubleshoot advanced network and security configurations, ensuring they can address contemporary security challenges in Networks effectively. Furthermore, students will delve into the Secure Web Gateway (SWG) for safe internet access and Cloud Access Security Broker (CASB) for Data Loss Prevention (DLP), crucial for protecting sensitive information in the cloud. The program also includes DNS-Layer Security, offering robust protection against online threats at the DNS layer and blocking malicious domain requests. Another critical component is Threat Intelligence and Prevention, where students will learn to utilize advanced threat detection mechanisms and integrate with Cisco Talos for real-time threat intelligence. Lastly, the course covers the Secure Internet Gateway (SIG), providing comprehensive visibility and control over internet traffic. This course is designed to equip students with the knowledge and hands-on experience needed to effectively manage and secure a modern network environment using Cisco's cutting-edge SASE technologies.

How you'll benefit

This class will help you:

- Learn how to Setup and Manage a Network Environment with SASE technologies
- Secure a Network Environment
- Utilize advanced threat detection mechanisms and integrate with Cisco Talos for real-time threat intelligence

Course Duration
5 days

Course Price
$4,595.00 or 45 CLCs

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

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
- System Administrators
- IT Professionals
- Technical Support Staff
- Cisco Certified Professionals

OUTLINE

The course encompasses a wide range of topics, including:

- **Secure Access Service Edge (SASE) Overview:**
  - Students learn how Cisco's Secure Access Service Edge (SASE) is designed to provide a comprehensive understanding of the SASE network architecture, which merges essential networking and security functions into a single, unified cloud service. This approach is increasingly crucial as organizations move towards cloud services and adopt mobile workforces, making the traditional network perimeter obsolete. Cisco's SASE model addresses these modern challenges by seamlessly integrating security and networking functionalities to ensure secure, fast, and reliable access to resources, irrespective of the user's or resource's location. Students gain the knowledge and skills necessary for the effective implementation, management, and use of Cisco's SASE solutions. It covers an introduction to the SASE concept, detailing its importance in today's digital environment and the evolution of network security towards this integrated framework. The curriculum delves into the core components of Cisco SASE, including Cloud-Delivered Security (with Secure Web Gateway, Cloud Access Security Broker, and Firewall as a Service), Zero Trust Network Access, SD-WAN for optimized performance and security, and DNS Security for threat protection at the DNS layer.

- **Zero Trust Network Access (ZTNA):**
  - Students Learn the foundational elements of Zero Trust Network Access (ZTNA) in the Cisco Secure Access Service Edge (SASE) running in the Commercial Cloud. This concept is pivotal in modern cybersecurity strategies, advocating for a 'never trust, always verify' approach to network access. ZTNA operates on the principle that no entity, either inside or outside the network perimeter, should be automatically trusted. Instead, it necessitates continuous verification of the credentials and context of access requests. The course delves deep into the mechanisms and implementations of ZTNA, equipping participants with the knowledge to apply these principles in securing network access. Through practical, hands-on training, attendees learn how to configure, manage, and troubleshoot ZTNA as part of Cisco's comprehensive SASE solutions.

- **Firewall as a Service (FWaaS):**
  - Students learn to Configure and Troubleshoot Cisco's firewall as a service (FWaaS) running in the Commercial Cloud. FWaaS represents a transformative shift in firewall deployment, moving from traditional hardware-based solutions to a more flexible, cloud-based model. This innovative approach enables scalable, location-independent security measures that can adapt to the dynamic needs of modern networks. Within the course framework, participants delve into the architecture, configuration, and management of FWaaS, gaining hands-on experience in implementing these solutions within Cisco's SASE framework. The training highlights how FWaaS integrates seamlessly with other SASE components to provide comprehensive security coverage, including threat prevention, intrusion detection, and traffic inspection across all network traffic. This segment ensures that attendees are well-versed in leveraging FWaaS to enhance their organization's network security posture, enabling robust protection against evolving cyber threats while maintaining high levels of performance and accessibility.

- **Secure Web Gateway (SWG):**
    - Students learn how to configure the Secure Web Gateway (SWG) and how SWG serves as a critical defense mechanism, acting as a checkpoint that all outbound web traffic must pass through, ensuring that only safe and compliant traffic can access the web. This technology is vital in preventing threats from reaching an organization's network by enforcing corporate and regulatory policy compliance, blocking access to malicious websites, and scanning for and stopping the spread of malware. The course meticulously covers the configuration, management, and optimization of SWG within the Cisco SASE framework, providing participants with practical, hands-on experience. Learners will understand how SWG functions as an integral part of a layered security strategy, complementing other SASE components to offer a robust, unified security posture. By the end of this segment, attendees will be equipped with the skills necessary to deploy and manage SWG solutions effectively, enhancing their organization's ability to safeguard against web-based threats while facilitating secure, productive internet access.

- **Cloud Access Security Broker (CASB):**
    - Students Learn how Cloud Access Security Broker (CASB) addresses the growing need for advanced cloud security measures. CASB acts as a mediator between users and cloud service providers, offering visibility, compliance, data security, and threat protection for cloud applications. It enables organizations to extend their security policies beyond traditional boundaries to the cloud, ensuring safe cloud usage across all services and devices. During the course, participants are introduced to the fundamentals of CASB, including its deployment models and key functionalities. The curriculum is designed to provide hands-on experience in integrating CASB solutions within the Cisco SASE framework, focusing on how to manage and secure cloud applications effectively. Attendees will learn to configure CASB to monitor and control cloud activities, prevent unauthorized data sharing, and protect against cloud-based threats. This segment empowers participants with the knowledge and practical skills to implement CASB solutions, enhancing their capability to navigate the complexities of cloud security and ensure comprehensive protection across their digital environments.

- **DNS-Layer Security:**
    - Students learn how DNS-Layer Security acts as the first line of defense by leveraging the Domain Name System (DNS) to block malicious internet destinations before a connection is established. By filtering traffic at the DNS layer, organizations can effectively prevent threats from reaching their network or endpoints, significantly reducing the risk of malware infections and data breaches.
    - Students also learn how it intercepts DNS queries to identify and block requests to known malicious sites or those that violate organizational policies. Participants gain practical experience in configuring and managing DNS-Layer Security within the Cisco SASE framework, learning to leverage this technology to enhance their overall security posture. Through hands-on training, attendees will understand how DNS-Layer Security integrates with other SASE components to provide a comprehensive, multi-layered security strategy. This segment ensures that personnel are equipped with the skills to deploy DNS-Layer Security effectively, enabling them to safeguard their organizations against a wide array of cyber threats from the very first point of internet access.

- **Threat Intelligence and Prevention:**
    - Students are equipped with the knowledge and skills to leverage intelligence about emerging threats and vulnerabilities to prevent attacks before they occur. Threat Intelligence involves the

collection, analysis, and dissemination of information about threats and their indicators, helping organizations to understand and anticipate potential security risks. Students learn how to integrate Threat Intelligence into the Cisco SASE framework, enabling real-time detection and prevention of threats across the network. Participants learn how to apply Threat Intelligence feeds to enhance the efficacy of security solutions such as FWaaS, SWG, and DNS-Layer Security, ensuring these systems can identify and block sophisticated attacks based on the latest intelligence. Moreover, the training delves into the implementation of advanced threat prevention techniques, such as sandboxing and behavior analysis, which are crucial for identifying and mitigating zero-day exploits and advanced persistent threats (APTs).

- **Cisco DUO:**
    - Student Learn how Cisco DUO provides a multifactor authentication (MFA) solution that strengthens access security by requiring two or more verification factors to validate a user's identity before granting access to network resources. This approach is integral to implementing a Zero Trust security model, ensuring that only authenticated and authorized users and devices can access an organization's critical systems and data. Within the course, participants receive comprehensive training on deploying, configuring, and managing Cisco DUO within the context of the Cisco SASE framework. The module covers how to integrate DUO with various applications and services to enforce MFA, thereby significantly reducing the risk of unauthorized access and potential security breaches. Learners will explore DUO's user-friendly authentication mechanisms, such as push notifications, SMS passcodes, and phone callbacks, which enhance security without compromising user convenience.
    - The hands-on sessions provide practical experience in setting up policy enforcement, user and device management, and reporting and analytics within DUO, offering insights into monitoring and responding to authentication attempts. By incorporating Cisco DUO into their cybersecurity arsenal, course attendees will be better equipped to protect sensitive data against threats arising from compromised credentials, ensuring robust access security across their organizations. This training ensures that personnel understand the critical importance of multifactor authentication and are prepared to implement and manage it effectively as part of their overall security strategy.

SD-WAN (Software-Defined Wide Area Network) Integrations:

- **Meraki SD-WAN Connectivity:**
    - Meraki SD-WAN SASE Secure Connect represents an innovative approach to integrating the flexibility and efficiency of SD-WAN with the comprehensive security framework provided by Cisco's Secure Access Service Edge (SASE) architecture. This integration is designed to address the needs of organizations looking to simplify their network connectivity and security management while ensuring robust protection against evolving cyber threats.
    - The Meraki SD-WAN SASE Secure Connect solution offers a streamlined way to connect branch offices, remote locations, and the workforce to applications and services, regardless of where they are hosted—be it in the cloud, on-premises, or in a hybrid environment. This is achieved by leveraging Meraki's SD-WAN capabilities for intelligent path selection and optimized application performance, combined with Cisco's SASE solutions for secure, policy-based access control and threat protection.
    - For organizations, particularly those within the Commercial sectors, Meraki SD-WAN SASE Secure Connect presents a robust solution. It enables them to adapt to the demands of digital transformation while maintaining a strong security posture. The course provides detailed guidance

on deploying, configuring, and managing this integrated solution, ensuring that participants are equipped with the necessary skills to leverage the benefits of SD-WAN and SASE in a unified, effective manner.

- **Cisco Catalyst SD-WAN Connectivity:**
  - Students learn how to use Catalyst SD-WAN SASE Secure Connect, which facilitates seamless, secure connectivity between various entities within an organization, including branch offices, remote workers, and cloud services. It combines the reliability and advanced features of Cisco's Catalyst SD-WAN solutions with the comprehensive security capabilities inherent in the SASE model, such as Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), and Firewall as a Service (FWaaS). This integration ensures that security is not just an overlay but is deeply integrated into the network architecture, providing end-to-end protection and visibility.
  - Enhanced Network Performance: Leveraging the Catalyst SD-WAN's ability to intelligently route traffic across the most efficient paths ensures optimal application performance and user experience.
  - Embedded Security: Direct integration of SASE components into the SD-WAN infrastructure means that security policies and protections are applied consistently, regardless of where connections originate or where resources are located.
- Hands-on labs showing students how to implement SASE on Cisco Catalyst SD-WAN, Meraki SD-WAN, Umbrella, and DUO