Implementing Security Service Edge with Cisco Secure Access (ICSA)

ID ICSA **Prix** sur demande **Durée** 3 jours

A qui s'adresse cette formation

- Security Engineers
- Security Administrators
- Network Security Engineers
- Cloud Security Engineers
- Security Architects
- Security Consultants
- Systems Engineers
- Infrastructure Engineers
- SOC Analysts
- Zero Trust Security Specialists

Pré-requis

There are no formal prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- 2+ years of experience in network security or security administration
- Basic understanding of enterprise routing and switching
- Basic understanding of WAN networking concepts
- Basic understanding of VPN technologies (IPsec, SSL/TLS)
- Basic understanding of DNS, HTTP/HTTPS, and web security concepts
- Basic understanding of Zero Trust principles
- Familiarity with cloud-based security services

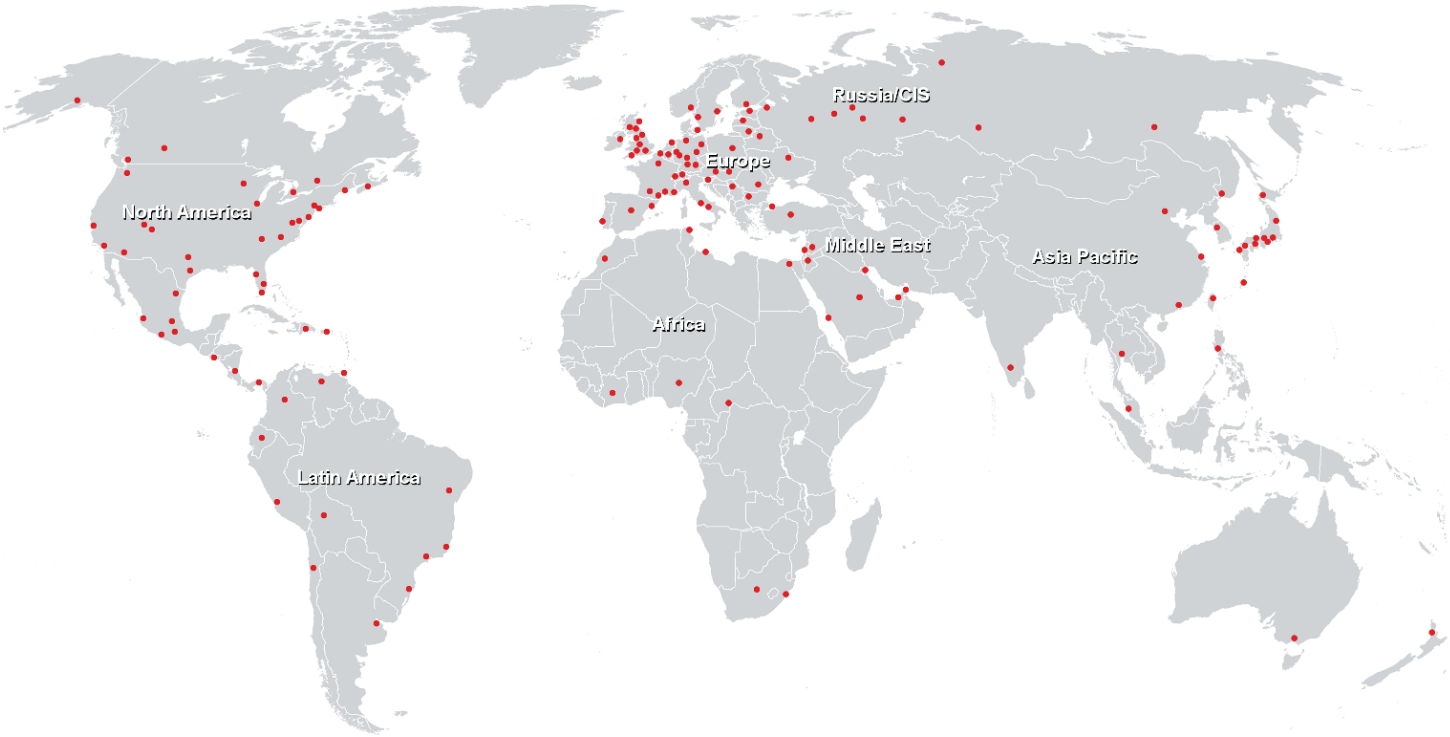
These skills can be found in the following Cisco Learning Offerings:

- Implementing and Operating Cisco Security Core Technologies (SCOR)
- Implementing and Administering Cisco Solutions (CCNA)
- Cisco SDWAN Fundamentals (SDWFND)
- Implementing Cisco SD-WAN Solutions (ENSDWI)

Objectifs

- Describe the SASE frameworks, the SSE cloud-based security services it includes, and the SD-WAN concepts and Cisco SD-WAN edge device on-box security capabilities that complete the SASE architecture
- Describe the Cisco Secure Access platform architecture and primary use cases
- Describe the Cisco Secure Access management options and the Admin Portal
- Describe the building blocks of the Cisco Secure Access initial configuration workflow
- Describe the user-side traffic acquisition methods and private-application backhaul methods available in Cisco Secure Access
- Configure Cisco Secure Access user provisioning and SAML-based SSO authentication
- Configure the common Cisco Secure Access components required for Secure Private Access, including app-side connectivity, private resource definition, and access policy
- Configure Zero Trust Access in Cisco Secure Access using client-based and browser-based methods
- Configure VPNaaS and Branch IPsec in Cisco Secure Access for Secure Private Access
- Configure Endpoint Posture, Security, and IPS Profiles in Cisco Secure Access for Secure Private Access
- Configure the common Cisco Secure Access components required for Secure Internet Access
- Describe the access methods dedicated to Secure Internet Access in Cisco Secure Access
- Configure threat and content defense capabilities in Cisco Secure Access for Secure Internet Access
- Configure Data Loss Prevention in Cisco Secure Access
- Verify Cisco Secure Access user experience using Experience Insights
- Integrate Cisco Secure Access with Cisco XDR and Splunk Enterprise to enhance SOC operations

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch