SCAZT

Designing and Implementing Secure Cloud Access for Users and Endpoints

The training provides you with the skills to design and implement cloud security architecture, user and device security, network and cloud security, cloud application and data security, cloud visibility and security, and cloud threat response. You will gain knowledge of protocols, solutions and designs to take a professional and expert role in the development and implementation of cloud solutions.

Course Contents

- Compare and contrast the National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), and Defense Information Systems Agency (DISA) security frameworks, and understand the importance of adopting standardized frameworks for cybersecurity in enhancing an organization's security posture
- Describe the Cisco Security Reference Architecture and its five main components
- Describe commonly deployed use cases and recommend the necessary capabilities within an integrated security architecture to address them effectively
- Describe the Cisco Secure Architecture for Everyone (SAFE) architecture
- Review the benefits, components, and process of certificate-based authentication for both users and devices
- Enable Duo multi-factor authentication (MFA) to protect an application from the Duo Administration Portal, and then configure the application to use Duo MFA for user login authentication
- Install Cisco Duo and implement its multifactor authentication on remote access virtual private network (VPN)
- Configure endpoint compliance
- Review and demonstrate the ability to understand Stateful Switchover (SSO) using security assertion markup language (SAML) or OpenID Connect together with Cisco Duo
- Describe Cisco software-defined wide-area network (SD-WAN) on-box and integrated threat prevention security services
- Describe SD-WAN on-box and integrated content filtering security services
- Describe the features and capabilities of Cisco Umbrella Secure Internet Gateway (SIG), such as DNS Security, Cloud-Delivered Firewall (CDFW), intrusion prevention systems (IPS), and interaction with Cisco SD-WAN
- Introduce the reverse proxy for internet-facing applications protections
- Explore the Cisco Umbrella SIG use case to secure cloud application access, the limitations and benefits of the solution, and the features available to discover and control access to cloud delivered applications
- Explore the Cisco ThousandEyes capabilities for monitoring the Cisco SD-WAN deployment
- Describe the challenges of accessing SaaS applications in modern business environments and explore the Cisco SD-WAN Cloud OnRamp for SaaS solution with direct or centralized internet access
- Introduce the Cisco Secure Firewall platforms, use cases, and security capabilities
- Demonstrate a comprehesive understanding of web application firewalls
- Demonstrate a comprehensive understanding of Cisco Secure Workload capabilities, deployment options, agents, and connectors
- Demonstrate a comprehensive understanding of Cisco Secure Workload application dependency mapping and policy discovery
- Demonstrate a comprehensive understanding of common cloud attack tactics and mitigation strategies
- Demonstrate a comprehensive understanding of multicloud security requirements and policy capabilities
- Introduce the security issues with the adoption of public clouds and common capabilities of cloud visibility and assurance tools to mitigate these issues
- Introduce Cisco Secure Network Analytics and Cisco Security Analytics and Logging
- Describe Cisco Attack Surface Management
- Describe how Application Program Interfaces (APIs) and automation can help in troubleshooting cloud policy, especially in the context of misconfigurations
- Demonstrate a comprehensive knowledge of the appropriate responses to cloud threats in specific scenarios
- Demonstrate the comprehensive knowledge required to use automation for cloud threat detection and response

E-Book You will receive the original course documentation from Cisco in English language as a Cisco E-Book. In the Cisco Digital Learning Version, the content of the courseware is integrated into the learning interface instead.

Target Group

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

Prerequisites

You should have the following knowledge and skills before attending this training course:

- Basic understanding of enterprise routing
- Basic understanding of WAN networks
- Basic understanding of Cisco SD-WAN
- Basic understanding of public cloud services

This knowledge can be found in the following Cisco learning offerings:

- CCNA - Implementing and Administering Cisco Solutions
- ENSDWI - Implementing Cisco SD-WAN Solutions
- SDWFND - Cisco SD-WAN Operation and Deployment

Course Target

The course prepares you for the SCAZT exam. Validate your knowledge in the areas of cloud security architecture design and implementation, user and device security, network and cloud security, application and data security, visibility and security, and threat response. If you pass, you will receive the Cisco Certified Specialist - Secure Cloud Access certification. If you combine this Multicloud Specialist exam with the Cisco Core Professional exam SCOR, you will also fulfill the CCNP Security certification requirements.

Processing time

approx. 30 hours

Status 04/25/2025

This Course in the Web

You can find the up-to-date information and options for ordering under the following link: www.experteach-training.com/go/**SCAZ**

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Cisco Digital Learning

This course is available in the Cisco Digital Learning Library. These recently developed, multi-modal training events include HD videos moderated by lecturers with stored searchable text and subtitles, as well as a exercises, labs, and explanatory text and graphics. We provide this offer to you via our myExperTeach learning portal. Effective of the activation of the account, access to the courses will be granted for a duration of 6 months. In the case of packet solutions (Cisco Digital Learning Subscriptions), this time period will amount to 12 months.

Cisco Digital Learning	Prices, excl. of V.A.T.
6 months activation	**€ 900**

Training		Prices, excl. of V.A.T.
Classes in Germany	**5 Days**	**€ 3,595**
Online Training	**5 Days**	**€ 3,595**

Date/course venue Course language German

19/05-23/05/25	HY Düsseldorf	01/09-05/09/25	HY Online
19/05-23/05/25	HY Online	08/12-12/12/25	HY Düsseldorf
01/09-05/09/25	HY Düsseldorf	08/12-12/12/25	HY Online

Table of Contents

SCAZT – Designing and Implementing Secure Cloud Access for Users and Endpoints

Outline
Industry Security Frameworks*
Cisco Security Reference Architecture Fundamentals*
Cisco Security Reference Architecture Common Use Cases*
Cisco SAFE Architecture*
Certificate-Based User and Device Authentication
Cisco Duo Multifactor Authentication for Application Protection
Cisco Duo with AnyConnect VPN for Remote Access
Introducing Cisco ISE Endpoint Compliance Services
SSO using SAML or OpenID Connect
Deploying On-Premises Threat Prevention
Examining Content Filtering
Exploring Cisco Umbrella SIG
Reverse Proxy
Securing Cloud Application with Cisco Umbrella SIG
Exploring Cisco SD-WAN ThousandEyes*
Optimizing SaaS Applications
Security Policies for Remote Access VPN
Cisco Secure Access
Cisco Secure Firewall
Web Application Firewall
Cisco Secure Workload Deployments, Agents, and Connectors
Cisco Secure Workload Structure and Policy
Cloud Security Attacks and Mitigations
Multicloud Security Policies
Cloud Visibility and Assurance
Cisco Secure Network Analytics and Cisco Secure Analytics and Logging
Cisco XDR
Cisco Attack Surface Management
Cloud Applications and Data Access Verifications
Automation of Cloud Policy*
Response to Cloud Threats*
Automation of Cloud Threat Detection and Response*
* This section is self-study material that can be done at your own pace if you are taking the instructor-led version of this course.

Lab outline
Explore Cisco SecureX
Windows Client BYOD Onboarding Interactive Activity
Use Cisco Duo MFA to Protect the Splunk Application
Integrate the Cisco Duo Authentication Proxy to Implement MFA for Cisco Security Secure Firewall
AnyConnect Remote Access VPN
Configure Cisco ISE Compliance Services
Configure Threat Prevention
Implement Web Security
Deploy DIA Security with Unified Security Policy
Configure Cisco Umbrella DNS Policies
Deploy Cisco Umbrella Secure Internet Gateway
Implement CASB Security
Microsoft 365 SaaS Testing by Using Cisco ThousandEyes
Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense
Configure Cisco Secure Firewall Policies
Explore Cisco Secure Workload
Explore the ATT&CK Matrix Cloud-Based Techniques
Explore Cisco Secure Network Analytics
Explore Cisco XDR Incident Response Tasks