# Designing and Implementing Secure Cloud Access for Users and Endpoints Training

BILGINÇ
IT Academy
info@bilginc.com
bilginc.com

Duration: **5 Day**

The **Designing and Implementing Secure Cloud Access for Users and Endpoints** training teaches you the 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.

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 Security (CCNP SECURITY).

**How You'll Benefit**

This training 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

**What to Expect in the Exam**

300-740 SCAZT v1.0: Designing and Implementing Secure Cloud Access for Users and Endpoints is a 90-minute exam associated with the Cisco Certified Specialist – Secure Cloud Access certification and satisfies the concentration exam requirement for the Cisco Certified Network Professional Security (CCNP SECURITY).

The exam tests your knowledge of designing and implementing:

- Cloud security architecture
- User and device security
- Network and cloud security
- Application and data security
- Visibility and assurance
- Threat response

## Prerequisites

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

- Basic understanding of enterprise routing
- Basic understanding of WAN networking
- Basic understanding of Cisco SD-WAN
- Basic understanding of Public Cloud services

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

- Implementing and Administering Cisco Solutions (CCNA)
- Implementing Cisco SD-WAN Solutions (ENSDWI)
- Cisco SDWAN Fundamentals (SDWFND)

# Designing and Implementing Secure Cloud Access for Users and Endpoints Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## What You Will Learn

- 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

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

specific scenarios
- Demonstrate the comprehensive knowledge required to use automation for cloud threat detection and response

## Training 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