Current Technologies
Computer Learning Centers

CISCO Partner
Platinum Learning

Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (SCAZT)

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (SCAZT)

Course Duration

5 Days

Course Price

$4,395.00
44 CLCs

Methods of Delivery

In-Person ILT
Virtual ILT
Onsite ILT

About this Class

The Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 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 (CCNP) Security certification.

Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (SCAZT)

How you will benefit

This class 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

Why Attend with Current Technologies CLC

- Our Instructors are 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 job roles best suited to the material in this course are:

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

Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (SCAZT)

Objectives

After taking this course, you should be able to:

- 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

Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (SCAZT)

Cont. Objectives

After taking this course, you should be able to:

- 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

Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (SCAZT)

Course Outline

Module 1: Industry Security Frameworks

Module 2: Cisco Security Reference Architecture Fundamentals

Module 3: Cisco Security Reference Architecture Common Use Cases

Module 4: Cisco SAFE Architecture

Module 5: Certificate-Based User and Device Authentication

Module 6: Cisco Duo Multifactor Authentication for Application Protection

Module 7: Cisco Duo with AnyConnect VPN for Remote Access

Module 8: Introducing Cisco ISE Endpoint Compliance Services

Module 9: SSO using SAML or OpenID Connect

Module 10: Deploying On-Premises Threat Prevention

Module 11: Examining Content Filtering

Module 12: Exploring Cisco Umbrella SIG

Module 13: Reverse Proxy

Module 14: Securing Cloud Application with Cisco Umbrella SIG

Module 15: Exploring Cisco SD-WAN ThousandEyes

Module 16: Optimizing SaaS Applications

Module 17: Security Policies for Remote Access VPN

Module 18: Cisco Secure Access

Module 19: Cisco Secure Firewall

Module 20: Web Application Firewall

Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (SCAZT)

Course Outline

Module 21: Cisco Secure Workload Deployments, Agents, and Connectors

Module 22: Cisco Secure Workload Structure and Policy

Module 23: Cloud Security Attacks and Mitigations

Module 24: Multicloud Security Policies

Module 25: Cloud Visibility and Assurance

Module 26: Cisco Secure Network Analytics and Cisco Secure Analytics and Logging

Module 27: Cisco XDR

Module 28: Cisco Attack Surface Management

Module 29: Cloud Applications and Data Access Verifications

Module 30: Automation of Cloud Policy

Module 31: Response to Cloud Threats

Module 32: Automation of Cloud Threat Detection and Response

Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 (SCAZT)

Lab Outline

- **Lab 1: Explore Cisco SecureX**
- **Lab 2: Windows Client BYOD Onboarding Interactive Activity**
- **Lab 3: Use Cisco Duo MFA to Protect the Splunk Application**
- **Lab 4: Integrate the Cisco Duo Authentication Proxy to Implement MFA for Cisco Security Secure Firewall AnyConnect Remote Access VPN**
- **Lab 5: Configure Cisco ISE Compliance Services**
- **Lab 6: Configure Threat Prevention**
- **Lab 7: Implement Web Security**
- **Lab 8: Deploy DIA Security with Unified Security Policy**
- **Lab 9: Configure Cisco Umbrella DNS Policies**
- **Lab 10: Deploy Cisco Umbrella Secure Internet Gateway**
- **Lab 11: Implement CASB Security**
- **Lab 12: Microsoft 365 SaaS Testing by Using Cisco ThousandEyes**
- **Lab 13: Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense**
- **Lab 14: Configure Cisco Secure Firewall Policies**
- **Lab 15: Explore Cisco Secure Workload**
- **Lab 16: Explore the ATT&CK Matrix Cloud-Based Techniques**
- **Lab 17: Explore Cisco Secure Network Analytics**
- **Lab 18: Explore Cisco XDR Incident Response Tasks**