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

Category: Networking & Security | **Vendor:** Cisco

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Cisco Certified Specialist – Security Secure Cloud Access, Cisco Certified Network Professional Security, CCNP SECURITY, Cisco Certified Specialist – Secure Cloud Access
Related Exam:	300-740

Course Overview

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 SecurityCCNP 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 SecurityCCNP 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

About This Course

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 SecurityCCNP 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 SecurityCCNP 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

Who Should Attend

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

Prerequisites & Entry Requirements

General 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)

Learning Outcomes

Upon successful completion of this course, participants will 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
- 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

Detailed Course Outline

- Certificate-Based User and Device Authentication
- Cisco Duo Multifactor Authentication for Application Protection
- Cisco Duo with AnyConnect VPN for Remote Access
- Cisco ISE Endpoint Compliance Services
- SSO using SAML or OpenID Connect
- Reverse Proxy
- Cisco SD-WAN Security Content Filtering
- Cisco SD-WAN to Cisco Umbrella SIG Integration
- Cisco Umbrella Cloud Access Security Broker
- 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
- Multicloud Security Policies
- Cloud Security Attacks and Mitigations
- 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 Verification
- Industry Security Frameworks
- Cisco Security Reference Architecture Fundamentals
- Cisco Security Reference Architecture Common Use Cases
- Cisco SAFE Architecture
- Cisco SD-WAN with ThousandEyes
- Automation of Cloud Policy
- Response to Cloud Threats
- Automation of Cloud Threat Detection and Response

□□ Certification Path

Cisco Certified Specialist – Security Secure Cloud Access, Cisco Certified Network Professional Security, CCNP SECURITY, Cisco Certified Specialist – Secure Cloud Access

Exam: 300-740

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

Frequently Asked Questions

Q: What delivery options are available for Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) course helps prepare you for the Cisco Certified Specialist – Security Secure Cloud Access, Cisco Certified Network Professional Security, CCNP SECURITY, Cisco Certified Specialist – Secure Cloud Access certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the 300-740 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 5-day Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)?

Yes, we provide corporate training, dedicated training, and closed classes for Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Designing and Implementing Secure Cloud Access for Users and Endpoints, Cisco Professional Level Security - CCNP, SCAZT

Q: Why choose Nexus Human for Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)