Designing and Implementing Secure Cloud Access for Users and Endpoints

Duration: 5 Days **Course Code: SCAZT** **Version: 1.1** **Delivery Method: Virtual Learning**

Overview:

Get the skills you need 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.
The Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) course 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 course also 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. This training also earns you 40 Continuing Education (CE) credits toward recertification.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

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

Objectives:

- **By the end of 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)
- 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
- Introduce the Cisco Secure Firewall platforms, use cases, and security capabilities
- Demonstrate a comprehensive 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

- 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
- 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

Prerequisites:

No specific requirement for this course

- CCNA - Implementing and Administering Cisco Solutions
- SDWFND - Cisco Catalyst SD-WAN Operation and Deployment
- SCOR - Implementing and Operating Cisco Security Core Technologies

Testing and Certification

None

Follow-on-Courses:

None recommended

Content:

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

LABS:

- Windows Client BYOD Onboarding Interactive Activity
- Use Cisco Duo MFA to Protect the Splunk Application
- Implement Cisco Duo Authentication Proxy MFA for Cisco Remote Access
- Compliance-Based Access
- Implement Web Security
- Deploy DIA Security with Unified Security Policy
- Configure Cisco Umbrella DNS Policies
- Deploy Cisco Umbrella Secure Internet Gateway
- Implement CASB Security
- Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense
- Configure Cisco Secure Firewall Policies
- Explore Cisco Secure Workload
- Explore the ATTACK Matrix Cloud-Based Techniques
- Explore Cisco Secure Network Analytics
- Explore Cisco XDR Incident Response Tasks

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo