Designing and Implementing Secure Cloud Access for Users and Endpoints

Duration: 5 Days **Course Code: SCAZT** **Version: 1.0**

Overview:

The Designing and Implementing Secure Cloud Access for Users and Endpoints course will provide you with the skills to design and implement cloud security architectures, user and device security, network and cloud security, application and data security, visibility and assurance, and threat response.
Some of the Cisco solutions covered in this course include Cisco SecureX, Cisco XDR, Cisco Duo, Cisco ISE, Cisco Catalyst SD-WAN, Cisco Umbrella, Cisco Secure Firewall, Cisco Secure Workload, Cisco Secure Analytics, and more.

This course prepares you for the 300-740 SCAZT exam. If passed, you will satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification as well the Secure Cloud Access Specialist Certification.

This course is worth 40 Continuing Education (CE) Credits

Target Audience:

Anyone involved in the Design and Implementation of a Cisco Secure Cloud Access Solution.

Objectives:

- After completing 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)
- 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

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
- 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:

Attendees should meet the following prerequisites:

- Basic understanding of Enterprise Routing
- Basic understanding of WAN Networking
- Basic understanding of Cisco SD-WAN
- Basic understanding of Public Cloud services
- CCNA - Implementing and Administering Cisco Solutions
- SDWFND - Cisco SD-WAN Operation and Deployment
- SCOR - Implementing and Operating Cisco Security Core Technologies

Testing and Certification

Recommended as preparation for the following exam:

- 300-740 - SCAZT - Designing and Implementing Secure Cloud Access for Users and Endpoints

This exam is one of the Cisco CCNP Security concentration exams as well as one of the Cisco Multicloud Specialist Certifications. Passing this exam will give you the Secure Cloud Access Specialist Certification.

Content:

Certificate-Based User and Device Authentication

- PKI Overview
- PKI Operations
- User versus Machine or Device-Based Certificates
- 802.1X and EAP Methods
- Cisco ISE Certificate Services
- Cisco ISE BYOD Client Certificate Configuration

Cisco Duo Multifactor Authentication for Application Protection

- Zero Trust Security Using MFA
- About Duo MFA and Splunk

Cisco Duo with AnyConnect VPN for Remote Access

- Use Cisco Duo Authentication
- About Cisco Duo MFA and Remote Access VPN

Introducing Cisco ISE Endpoint Compliance Services

- Endpoint Compliance Services Overview

SSO using SAML or OpenID Connect

- SSO using Security Assertion Markup Language
- Using SAML or OpenID Connect
- Single Sign-On with Cisco Duo

Reverse Proxy

- Reverse Proxy
- Reverse Proxy Implementation to Protect Applications

Cisco SD-WAN Security Content Filtering

- Cisco SD-WAN Content Filtering
- Secure Direct Internet Access
- Impelmenting Unified Security Polices

Cisco SD-WAN to Cisco Umbrella SIG Integration

- SIG Overview
- Integrating SIG and Cisco SD-WAN
- Cisco Umbrella DNS Deep Dive
- Cisco Umbrella CDFW and IPS
- Cisco Umbrella Secure Web Gateway

Cisco Umbrella Cloud Access Security Broker

- Cloud Application Security Overview
- Implementing Cisco Umbrella CASB

Cisco Secure Workload Deployments, Agents, and Connectors

- Cisco Secure Workload Capabilities and Deployments
- Cisco Secure Workload Deployments, Agents and Connectors

Cisco Secure Workload Structure and Policy

- Cisco Secure Workload Inventory and Scopes
- Cisco Secure Workload Workspaces
- Cisco Secure Workload Policy Discovery

Multicloud Security Policies

- Multicloud Security Policies Benefits and Requirements
- Multicloud Security Architecture
- Cisco Multicloud Defense

Cloud Security Attacks and Mitigations

- Cloud Security Models
- MITRE ATT;CK® Framework
- MITRE ATT;CK® Matrix for Enterprise Cloud-Based Techniques
- Practical Application of MITRE ATT;CK®
- MITRE ATT;CK® Navigator

Cloud Visibility and Assurance

- Cloud Visibility and Assurance Requirements
- Cloud Visibility and Assurance Tools
- Cloud Visibility and Assurance Automation

Cisco Secure Network Analytics and Cisco Secure Analytics and Logging

- Cisco Secure Network Analytics
- Cisco Secure Network Analytics Components
- Secure Network Analytics Use Cases
- Cisco Security Analytics and Logging (SAL)

Cisco XDR

- Cisco XDR Overview
- Cisco XDR Components
- Cisco Secure Cloud Analytics

Cisco Attack Surface Management

- Cisco Attack Surface Management Introduction
- Cisco XDR Integration
- Cisco Attack Suface Management Use Cases

Exploring Cisco SD-WAN ThousandEyes

- Cisco ThousandEyes Overview
- Deploying Cisco ThousandEyes with Cisco SD-WAN

Automation of Cloud Policy

- Automation of Cloud Policy
- Tools for Automation of Cloud Policy and Troubleshooting

Response to Cloud Threats

- Threat Response Fundamentals
- Response to Data Breaches and User or Application Compromises
- Regulartory Changes and Security Audit Responses

Automation of Cloud Threat Detection and Response

- Cloud Threat Detection and Respnse Automation
- Automation of Cloud Threat Detection and Response Tools
- Cisco XDR Response Tasks and MITRE ATT;CK® Mappings

Labs:

- Discovery Lab 1: Windows Client BYOD Onboarding Interactive Activity
- Discovery Lab 2: Use Cisco Duo MFA to Protect the Splunk Application
- Discovery Lab 3: Integrate the Cisco Duo Authentication Proxy to Implement MFA for Cisco Security Secure Firewall AnyConnect Remote Access VPN
- Discovery Lab 4: Test and Monitor Compliance - Based Access
- Discovery Lab 5 : Implement Web Security
- Discovery Lab 6: Deploy DIA Security with Unified Security Policy
- Discovery Lab 7: Configure Cisco Umbrella DNS Policies
- Discovery Lab 8 : Deploy Cisco Umbrella Secure Internet Gateway
- Discovery Lab 9: Implement CASB Security
- Discovery Lab 10:: Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense
- Discovery Lab 11: Configure Cisco Secure Firewall Policies
- Discovery Lab 12: Explore Cisco Secure Workload
- Discovery Lab 13: Explore the ATT;CK Matrix Cloud-Based Techniques
- Discovery Lab 14: Explore Cisco Secure Network Analytics
- Discovery Lab 15: Explore Cisco XDR

Security Policies for Remote Access VPN

- Cisco Secure Firewall Remote Access VPN Security
- Cisco IOS XE SD-WAN Remote Access VPN Security

Cisco Secure Access

- Cisco Secure Access: SSE Reimagined
- Cisco Secure Client New Capabilities
- QUIC and MASQUE Protocol Benefits
- Cisco Secure Access Use Cases

Cisco Secure Firewall

- Cisco Secure Firewall Platforms
- Cisco Secure Firewall Use Cases
- Cisco Secure Firewall Policies Configuration

Web Application Firewall

- Introduction to WAFs
- Cisco Secure WAF Best Practices

Cloud Applications and Data Access Verifications

- User Cloud Access Verification
- User Cloud Access Verification Using Cisco Duo
- User Cloud Access Verification Using Cisco Cloud Analytics
- User Cloud Access Verification Usng Cisco Secure Workload
- User Cloud Access Verification Usng Cisco Umbrella
- User Cloud Access Verification Usng Cisco Secure Firewall

Industry Security Frameworks

- Introduction to Security Frameworks
- National Institute of Standards and Technologies Cybersecurity Framework
- Cybersecurity and Infrastructure Security Agency Framework
- Defense Information System Agency Framework
- Comparison of Security Frameworks

Cisco Security Reference Architecture Fundamentals

- Talos Threat Intelligence
- XDR Security Operations Toolset
- User/Device Security
- Network Security: Cloud Edge and On-Premises
- Workload, Application and Data Security

Cisco Security Reference Architecture Common Use Cases

- Common Identity
- Converged Multicloud Policy
- SASE Integration
- ZeroTrust Network Access
- XDR Telemetry and Orchestration

Cisco SAFE Architecture

- Cisco SAFE Framework
- Key Components of Cisco SAFE
- Cisco SAFE Phases

Control Center and Investigate

- Discovery Lab 16: Explore Cisco XDR Incident Response Tasks

Additional Information:

Gain the skills to design and implement cloud security architecture, user and device security,network and cloud security, cloud application and data security,cloud visability and Assurance, and responding to cloud Threats. Book Today.

Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278

training@globalknowledge.com.sa

www.globalknowledge.com/en-sa/

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Worood, Riyadh 3140, Saudi Arabia