
Implementing Cisco Secure Mobility

Duration: 5 Days Course Code: SIMOS

Overview:

This course is designed to prepare network security engineers with the knowledge and skills they need to protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions. Students of this course will gain hands-on experience with configuring and troubleshooting remote access and site-to-site VPN solutions, using Cisco ASA adaptive Security Appliances and Cisco IOS routers.

Target Audience:

This course will be of benefit to security engineers involved in the support and deployment of Cisco VPN Solutions and individuals looking to obtain the Cisco Certified Network Professional for Security Certification.

Objectives:

- **After attending this course you should be able to :**
 - Describe the various VPN technologies and deployments as well as the cryptographic algorithms and protocols that provide VPN security.
 - Implement and maintain Cisco site-to-site VPN solutions.
 - Implement and maintain Cisco FlexVPN in point-to-point, hub-and-spoke, and spoke-to-spoke IPsec VPNs.
 - Implement and maintain Cisco clientless SSL VPNs.
 - Implement and maintain Cisco AnyConnect SSL and IPsec VPNs.
 - Implement and maintain endpoint security and dynamic access policies (DAP).
-

Prerequisites:

Attendees should meet the following prerequisites:

- Cisco Certified Network Associate (CCNA®) certification
- Cisco Certified Network Associate (CCNA®) Security certification
- Knowledge of Microsoft Windows Operating System

Testing and Certification

Recommended preparation for exam(s):

- **300-209** - Implementing Cisco Edge Network Security Solutions
-

Follow-on-Courses:

Delegates looking to achieve the Cisco Certified Network Professional Certification for Security should also attend the following courses.

- SITCS - Implementing Cisco Threat Control Solutions
 - SISAS - Implementing Cisco Secure Access Solutions
 - SENSS - Implementing Cisco Edge Network Security Solutions
-

Content:

Fundamentals of VPN Technologies and Cryptography

- The Role of VPNs in Network Security
- VPNs and Cryptography

Deploying Secure Site-to-Site Connectivity Solutions

- Introducing Cisco Secure Site-to-Site Connectivity Solutions
- Deploying Point-to-Point IPsec VPNs on the Cisco ASA
- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
- Deploying Cisco IOS DMVPNs

Deploying Cisco IOS Site-to-Site FlexVPN Solutions

- Introducing Cisco FlexVPN Solution
- Deploying Point-to-Point IPsec VPNs Using Cisco IOS FlexVPN
- Deploying Hub-and-Spoke IPsec VPNs Using Cisco IOS FlexVPN
- Deploying Spoke-to-Spoke IPsec VPNs Using Cisco IOS FlexVPN

Deploying Clientless SSL VPN

- Clientless SSL VPN Overview
- Deploying Basic Cisco Clientless SSL VPN
- Deploying Application Access in Clientless SSL VPN

Deploying Advanced Authentication in Clientless SSL VPN

Deploying Cisco AnyConnect VPNs

- Overview of Cisco AnyConnect VPNs
- Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA
- Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA
- Deploying Cisco AnyConnect IPsec/IKEv2 VPNs
- Deploying Advanced Authentication, Authorization, and Accounting in Cisco AnyConnect VPNs

Deploying Endpoint Security and Dynamic Access Policies

- Implementing Host Scan
- Implementing DAP for SSL VPNs

Labs

- Lab 1: Implement Site-to-Site Secure Connectivity on the Cisco ASA
- Lab 2: Implement Cisco IOS Static VTI Point-to-Point Tunnel
- Lab 3: Implement DMVPN
- Lab 4: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN
- Lab 5: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN
- Lab 6: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN
- Lab 7: Implement ASA Basic Clientless SSL VPN
- Lab 8: Application Access clientless SSL
- Lab 9: Advanced AAA clientless SSL
- Lab 10: Lab: Implement ASA Basic AnyConnect SSL VPN
- Lab 11: Configure Advanced Cisco AnyConnect SSL VPN on Cisco ASA
- Lab12: Configure Cisco AnyConnect IPsec/IKEv2 VPNs on Cisco ASA
- Lab13: Configure Advanced Authentication for Cisco AnyConnect VPN on Cisco ASA
- Lab 14: Configure Hostscan and DAP for AnyConnect SSL VPNs

Further Information:

For More information, or to book your course, please call us on +254 713 027 191

training@clclearningafrica.com

www.clclearningafrica.com

Computer Learning Centre 2nd Floor Museum Hill Centre, Muthithi Road, Westlands, Nairobi, Kenya