FIREFLY

CONTACT US

Implementing Cisco Secure Mobility Solutions

DURATION: 5 DAYS COURSE CODE: SIMOS FORMAT: LECTURE/LAB

COURSE DESCRIPTION

Implementing Cisco Secure Mobility Solutions (SIMOS) v1.0 is a newly created five-day instructor-led training (vILT) course that is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification.

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.

WHO SHOULD ATTEND

Network Security Engineers

PREREQUISITES

The knowledge and skills that a learner must have before attending this course are as follows:

- CCNA Security or valid CCSP or any CCIE certification can act as a prerequisite

LEARNING OBJECTIVES

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)

COURSE OUTLINE

1. Fundamentals of VPN Technologies and Cryptography
   - The Role of VPNs in Network Security
   - VPNs and Cryptography
2. 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
3. Deploying Cisco IOS Site-to-Site Flex-VPN 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
4. Deploying Clientless SSL VPNs
   - Clientless SSL VPN Overview
   - Deploying Basic Cisco Clientless SSL VPN on Cisco ASA
   - Deploying Application Access in Cisco ASA Clientless SSL
   - VPN Deploying Advanced Authentication and Authorization in Clientless SSL VPN
5. Deploying Cisco AnyConnect VPNs
   - Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA
   - Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA
   - Deploying Advanced Authentication and Authorization in Cisco AnyConnect VPNs
   - Deploying Cisco AnyConnect IPSec/IKEv2 VPNs
6. Endpoint Security and Dynamic Access Policies
   - Implementing Host Scan
   - Implementing DAP for SSL VPNs

DISCOVERY LABS

1: Implement Site-to-Site Secure Connectivity on the Cisco ASA

2: Implement Cisco IOS Static VTI Point-to-Point Tunnel

3: Implement DMVPN

4: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN

5: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN

6: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS FlexVPN

7: Implement ASA Basic Clientless SSL VPN

8: Configure Application Access for Cisco ASA Clientless SSL VPN

9: Implement Local and External AAA for Clientless SSL VPNs

10: Implement ASA Basic AnyConnect SSL VPN

11: Configure Advanced Authentication for Cisco AnyConnect SSL VPN

12: Implement AnyConnect IPSec/IKEv2

13: Implement Host Scan and DAP