Implementing Cisco Secure Mobility Solutions (SIMOS)

Who should attend

The primary audience for this course is as follows:

- Network Security Engineers

Prerequisites

This section lists the skills and knowledge that you must possess to benefit fully from the course. This section includes recommended Cisco learning offerings that you may complete to benefit fully from this course, including the following:

- Cisco Certified Network Associate (CCNA®) certification
- Cisco Certified Network Associate (CCNA®) Security certification
  [*Knowledge of Microsoft Windows operating system

Course Objectives

Upon completing this course, the you will be able to meet these overall 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 Content

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. You 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.

Detailed Course Outline

Module 1: The Role of VPNs in Network Security

- VPN Definition
- Key Threats to WANs and Remote Access
- Cisco Modular Network Architecture and VPNs
- VPN Types
- VPN Components
- Secure Communication and Cryptographic Services
- Cryptographic Algorithms
- Cryptography and Confidentiality
- Cryptography and Integrity
- Cryptography and Authentication
- Cryptography and Nonrepudiation
- Keys in Cryptography
- Public Key Infrastructure
- Next-Generation Encryption
- Dependencies in Cryptographic Services
- Cryptographic Controls Guidelines

Module 2: Deploying Secure Site-to-Site Connectivity Solutions

- Site-to-Site VPN Topologies
- Site-to-Site VPN Technologies
Module 3: Deploying Cisco IOS Site-to-Site FlexVPN Solutions

- FlexVPN Overview
- Public Key Infrastructure (PKI)
- Site-to-Site VPN Topologies
- FlexVPN Architecture
- FlexVPN Configuration Overview
Module 4: Deploying SSL VPNs

- SSL VPN Components
- SSL/TLS
- Overview of group policies and connection profiles
- Basic Cisco Clientless SSL VPN
- Solution Components
- Configure ASA gateway
- Configure basic authentication
- Configure access control (including URL entry and bookmarks)
- Verify basic clientless SSL VPN
- Troubleshoot basic clientless SSL VPN
- Lab 4-1 Objective: Implement Basic Cisco Clientless SSL VPN on Cisco ASA
- Deploying Application Access options (plug-ins, smart tunnels)
- Configure and verify plugins
- Configure and verify smart tunnels
- Troubleshoot plugins and smart tunnel
- Lab 4-2 Objective: Application Access clientless SSL
- Advanced Authentication in Cisco Clientless SSL VPN Solution Components
- Configure and verify Certificate based Authentication
- Configure and Verify External Authentication
- Troubleshoot Advanced Authentication in Clientless SSL VPN
- Lab 4-3 Objective: Advanced AAA Clientless SSL

Module 5: Deploying Cisco AnyConnect VPNs

- IP Address assignment
- Split Tunneling
- Basic Cisco AnyConnect SSL VPN
- Solution Components
- SSL VPN Server Authentication
- SSL VPN Clients Authentication
- SSL VPN Clients IP Address Assignment
- SSL VPN Split Tunneling
- Configure ASA for Basic AnyConnect SSL VPN
- Configure Basic Cisco Authentication
- Configure Access Control
- Verify and Troubleshoot Basic Cisco AnyConnect SSL VPN
- Lab 5-1 Objective: Implement Basic Cisco AnyConnect SSL VPN on Cisco ASA
- DTLS Overview
- Parallel DTLS and TLS Tunnels
- Configure DTLS
- Verify DTLS
- Cisco AnyConnect Client Configuration Management
- Cisco AnyConnect Client Operating System Integration Options
- Cisco AnyConnect Start Before Logon
- Cisco AnyConnect Trusted Network Detection
- Configure, Verify, and Troubleshoot Cisco AnyConnect Start Before Logon and Cisco AnyConnect Trusted Network Detection
- Lab 5-2: Implement Advanced Cisco AnyConnect SSL VPN on Cisco ASA
- AnyConnect Support for IPsec/IKEv2
- Configure a Cisco AnyConnect IPsec/IKEv2 VPNs on a Cisco ASA Adaptive Security Appliance
- Verify and Troubleshoot Cisco AnyConnect IPsec/IKEv2 VPNs on Cisco ASA
- Lab 5-3: Configure Cisco AnyConnect IPsec/IKEv2 VPNs on Cisco ASA
- Cisco AnyConnect Advanced Authentication Scenarios
- External Authentication
- Certificate-Based Server Authentication
- Configure and Verify Certificate-Based Client Authentication
- SCEP Proxy Overview
- SCEP Proxy Connection Flow
- SCEP Proxy Configuration Procedure
- Configure SCEP Proxy
- Verify SCEP Proxy
- Local Authorization Overview
- Local Authorization Scenario
- Local Authorization Configuration Procedure
- Configure Local Authorization
- External Authentication and Authorization Scenario
- Configure External Authentication and Authorization
- Troubleshoot Advanced Authentication and Authorization in Cisco AnyConnect VPNs
- Accounting
- Lab 5-3: Configure Cisco AnyConnect IPsec/IKEv2 VPNs on Cisco ASA
- Lab 5-4: Implement Advanced Cisco AnyConnect SSL VPN on Cisco ASA

Module 6: Endpoint Security and Dynamic Access Policies
Implementing Cisco Secure Mobility Solutions (SIMOS)

- Cisco HostScan Overview
- Cisco HostScan Prelogin Assessment
- Install Cisco HostScan
- Configure Prelogin Criteria and Prelogin Policy
- Configure Host Scan Endpoint Assessment
- Configure Host Scan Advanced Endpoint Assessment
- DAP Overview
- Integrating DAP with Host Scan
- Configuring DAP
- Verifying and Troubleshooting DAP
- Lab 6-1: Configure Hostscan and DAP for AnyConect SSL VPNs
Implementing Cisco Secure Mobility Solutions (SIMOS)