Implementing Cisco Secure Mobility Solutions (SIMOS)

ID CI-SIMOS  Price US$ 3,795  Duration 5 days

Who should attend
- Network Security Engineers
- Network Engineers
- Network Designers and Administrators
- Network Managers
- System Engineers

Access policies (DAP)

Certifications
This course is part of the following Certification:
- Cisco Certified Network Professional Security (CCNP Security)

Prerequisites
Cisco Certified Network Associate (CCNA®) Security certification

OR
Any CCIE certification can act as a prerequisite

Course Objectives
By the end of this course, you will 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
- Deploy Cisco FlexVPN in point-to-point, hub-and-spoke and spoke-to-spoke IPsec VPNs
- Implement Cisco clientless SSL VPNs
- Implement and maintain Cisco AnyConnect SSL and IPsec VPNs
- Deploy endpoint security and dynamic access policies (DAP)

Course Content
Implementing Cisco Secure Mobility Solutions (SIMOS) v1.0 is a new course that is part of the recommended training for the Cisco Certified Network Professional Security (CCNP® Security) certification. This course will prepare you with the knowledge and skills needed 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
DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment.

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

Module 2: Secure Site-to-Site Connectivity Solutions

- Site-to-Site VPN Topologies and Technologies
- IPSec VPN Overview
- Internet Key Exchange v1 and v2
- Security Payload Encapsulation
- IPSec Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN
- Overview of Point-to-Point IPSec VPNs on the Cisco ASA
- Configuration Tasks for Basic Point-to-Point Tunnels on the Cisco ASA
- Enable IKE on an Interface
- Configure IKE Policy
- Configure PSKs
- Choose Transform Set and VPN Peer
- Choose Traffic for VPN
- Configure Site-to-Site VPN with Connection Profiles Menu
- Verify and Troubleshoot Basic Point-to-Point Tunnels on the Cisco ASA
- Overview of Cisco IOS VTIs
- Configure Static VTI Point-to-Point Tunnels
- Verify Static VTI Point-to-Point Tunnels
- Configure Dynamic VTI Point-to-Point Tunnels

Module 3: Cisco IOS Site-to-Site FlexVPN Solutions

- FlexVPN Overview
- Public Key Infrastructure (PKI)
- Site-to-Site VPN Topologies
- FlexVPN Architecture
- FlexVPN Configuration Overview
- FlexVPN Capabilities
- IKEv2 vs. IKEv1 Overview
- IKEv2 Message Exchange
- IKEv2 DoS Prevention
- IKEv1 and IKEv2 Comparison
- FlexVPN Use Cases
- Point-to-Point FlexVPN
- FlexVPN Configuration Blocks
- IKEv2 Profile
- Smart Defaults
- Manipulating Default Values
- Negotiating IKEv2 Proposals
- Point-to-Point VPN Scenario with IPv4 Static Routes
- Configure and Verify Point-to-Point VPN with IPv4 Static Routes
- Point-to-Point VPN Scenario with OSPFv3
- Configure and Verify Point-to-Point VPN with OSPFv3
- Enroll Devices to ECDSA PKI
- Configure Router for ECDSA
- Configure ASA for ECDSA
- Verify EC Key Pairs and Certificates
- Verify IKEv2 SA
- Verify IPSec SA
DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment.

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

Module 4: SSL VPNs

- 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
- Deploying Application Access options (plugins, smart tunnels)
- Configure and verify plugins
- Configure and verify smart tunnels
- Troubleshoot plugins and smart tunnel
- Advanced Authentication in Cisco Clientless SSL VPN Solution Components

Module 5: 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 AnyConnect Authentication
- Configure Access Control
- Configure and Verify Basic Cisco AnyConnect SSL VPN
- 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
- Cisco AnyConnect Trusted Network Detection
- 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
- Cisco AnyConnect Advanced Authentication

Verify Point-to-Point FlexVPN (just flowchart and important show/debug command output)
Cisco IOS FlexVPN
IKEv2 Configuration Payload
Locally Managed Hub-and-Spoke Scenario
Configure a Spoke in a Hub-and-Spoke Scenario
Configure a Hub in a Hub-and-Spoke Scenario
Configuration Exchange
Verify and Troubleshoot Hub-and-Spoke FlexVPN
Spoke-to-Spoke Shortcut Scenario
NHRP in FlexVPN
Configure and Verify a Spoke in a Spoke-to-Spoke Shortcut Scenario
Configure and Verify a Hub in a Spoke-to-Spoke Shortcut Scenario
RADIUS-Managed FlexVPN Scenario
Verify Spoke-to-Spoke Shortcut Switching
Troubleshoot Spoke-to-Spoke Shortcut Switching (just flowchart and important show/debug command output)

Configure and verify Certificate based Authentication
Configure and Verify External Authentication
Troubleshoot Advanced Authentication in Clientless SSL VPN
Scenarios
- External Authentication
- Certificate-Based Server Authentication
- Configure and Verify Certificate-Based Client Authentication
- SCEP Proxy
  - Connection Flow
  - Configuration Procedure
- Local Authorization
- External Authentication and Authorization Scenario
- Configure External Authentication and Authorization
- Troubleshoot Advanced Authentication and Authorization in Cisco AnyConnect VPNs
- Accounting

Module 6: Endpoint Security and Dynamic Access Policies
- 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
  - Integrate with Host Scan
  - Configure
  - Verifying and Troubleshooting

Labs
- Site to Site Secure Connectivity on Cisco ASA
- Implement a Cisco IOS static VTI point-to-point tunnel
- Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN
- Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN
- Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN
- Cisco Clientless SSL VPN on Cisco ASA
- Application Access clientless SSL
- Advanced AAA Clientless SSL
- Implement Basic AnyConnect SSL VPN on Cisco ASA
- Advanced AnyConnect SSL VPN on Cisco ASA
- AnyConnect IPSec/IKEv2 VPNs on Cisco ASA
- Hostscan and DAP for AnyConnect SSL VPNs