IMPLEMENTING CISCO SECURE MOBILITY SOLUTIONS (CI-SIMOS)

This subtopic provides an overview of how the course is organized. The course contains these components:

Fundamentals of VPN Technologies and Cryptography

Deploying Secure Site-to-Site Connectivity Solutions

Deploying Cisco IOS Site-to-Site FlexVPN Solutions

Deploying Clientless SSL VPNs

Deploying Cisco AnyConnect VPNs

Endpoint Security and Dynamic Access Policies

Lab 2-1: Implement Site-to-Site Secure Connectivity on the Cisco ASA

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

Lab 2-3: Implement DMVPN

Lab 3-1: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN

Lab 3-2: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN

Lab 3-3: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN

Lab 4-1: Implement ASA Basic Clientless SSL VPN

Lab 4-2: Configure Application Access for Cisco ASA Clientless SSL VPN

Lab 4-3: Implement Local and External AAA for Clientless SSL VPNs

Lab 5-1: Implement ASA Basic AnyConnect SSL VPN

Lab 5-2: Configure Advanced Authentication for Cisco AnyConnect SSL VPN

Lab 5-3: Implement AnyConnect IPSec/IKEv2

Lab 6-1: Implement Host Scan and DAP

Detailed Course Outline

This in-depth outline of the course structure lists each module, lesson, and topic.

Module 1: Fundamentals of VPN Technologies and Cryptography

Module Objective: Introduce VPNs and implement advanced threat controls

Lesson 1: The Role of VPNs in Network Security

Lesson Objective: Describe the role of VPNs in network security

This lesson includes these topics:

VPN Definition

Key Threats to WANs and Remote Access

Cisco Modular Network Architecture and VPNs

VPN Types

VPN Components

Summary

Lesson 2: VPNs and Cryptography

Lesson Objective: Describe cryptography solutions, algorithms, and protocols

This lesson includes these topics:

Secure Communication and Cryptographic Services

Cryptographic Algorithms

Confidentiality Using Cryptographic Controls

Integrity Using Cryptographic Controls

Authentication Using Cryptographic Controls

Nonrepudiation Using Cryptographic Controls

Keys in Cryptography

Public Key Infrastructure

Next-Generation Encryption

Dependencies in Cryptographic Services

Cryptographic Controls Guidelines

Summary

Lesson 3: Module Summary

This lesson includes these topics:

References

Lesson 4: Module Self-Check

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

Module Objective: Deploy secure site-to-site connectivity solutions

Lesson 1: Introducing Cisco Secure Site-to-Site Connectivity Solutions

Lesson Objective: Describe Cisco secure site-to-site connectivity solutions

This lesson includes these topics:

Site-to-Site VPN Topologies

Site-to-Site VPN Technologies

IPsec VPN Overview

Internet Key Exchange v1 and v2

Encapsulating Security Payload

IPsec Virtual Tunnel Interface

Dynamic Multipoint VPN

Cisco IOS FlexVPN

Summary

Lesson 2: Deploying Point-to-Point IPsec VPNs on the Cisco ASA

Lesson Objective: Deploy point-to-point IPsec VPNs on the Cisco ASA

This lesson includes these topics:

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

Configuring Site-to-Site VPN with Connection Profiles Menu

Verify and Troubleshoot Basic Point-to-Point Tunnels on the Cisco ASA

Summary

Lab 2-1: Implement Site-to-Site Secure Connectivity on the Cisco ASA

Lab Objective: Implement an IPsec VPN tunnel on the Cisco ASA

This lab includes these tasks:

Task 1: Configuring the Cisco ASA for Site-to-Site VPN
Task 2: Disabling NAT for Testing
Task 3: Verifying the Site-to-Site VPN

Lesson 3: Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs

Lesson Objective: Deploy Cisco IOS VTI-based point-to-point IPsec VPNs

This lesson includes these topics:

Overview of Cisco IOS VTIs

Configuring Basic IKE Peering

Verify IKE Peering

Configure Static VTI Point-to-Point Tunnels

Verify Static VTI Point-to-Point Tunnels

Configure Dynamic VTI Point-to-Point Tunnels

Verify Dynamic VTI Point-to-Point Tunnels

Summary

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

Lab Objective: Implement a Cisco IOS static VTI point-to-point tunnel

This lab includes these tasks:

Task 1 Configure Static VTI Point-to-Point Tunnel
Task 2: Verify Static VTI Point-to-Point Tunnel

Lesson 4: Deploying Cisco IOS DMVPNs

Lesson Objective: Deploy Cisco IOS DMVPNs

This lesson includes these topics:

Overview of Cisco IOS DMVPN

DMVPN Solution Components

GRE

NHRP

DMVPN Operations

Types of Authentication

Configure DMVPN on Hub

Configure DMVPN on Spoke

Configure Routing in DMVPN

Verify DMVPN

Summary

Lab 2-3: Implement DMVPN

Lab Objective: Configure DMVPN spoke

This lab includes these tasks:

Task 1: Configure a DMVPN Hub
Task 2: Configure a DMVPN Spokes
Task 3: Configure OSPF Routing in DMVPN
Task 4: Verify DMVPN Hub and Spoke Operation
Task 5: Configure a DMVPN Spoke to Spoke Communication
Task 6: Verify DMVPN Spoke-to-Spoke Communication

Lesson 5: Module Summary

This lesson includes these topics:

References

Lesson 6: Module Self-Check

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

Module Objective: Deploy Cisco IOS site-to-site FlexVPN solutions

Lesson 1: Introducing Cisco FlexVPN Solution

Lesson Objective: Evaluate site-to-site VPN technologies

This lesson includes these topics:

FlexVPN Overview

Public Key Infrastructure

FlexVPN Architecture

FlexVPN Configuration Overview

FlexVPN Capabilities

IKEv2 vs. IKEv1 Overview

IKEv2 Message Exchange

IKEv2 DoS Prevention

IKEv1 and IKEv2 Comparison

FlexVPN Use Cases

Summary

Lesson 2: Deploying Point-to-Point IPsec VPNs Using Cisco IOS FlexVPN

Lesson Objective: Describe the use of FlexVPN in point-to-point IPsec VPNs

This lesson includes these topics:

Point-to-Point FlexVPN

FlexVPN Configuration Blocks

IKEv2 Smart Defaults

Basic FlexVPN Scenario 1

Configure Basic FlexVPN: Scenario 1

Basic FlexVPN Scenario 2

Configure Basic FlexVPN: Scenario 2

Advanced FlexVPN Scenario

Configure Advanced FlexVPN

Verify FlexVPN Configurations

Summary

Lab 3-1: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN

Lab Objective: Implement point-to-point FlexVPN using smart defaults and minimal configuration

This lab includes these tasks:

Task 1: Implement Point-to-Point FlexVPN Using Smart Defaults And Minimal Configuration
Task 2: Modify Smart Defaults to Increase Protection Strength
Task 3: Implement Point-to-Point FlexVPN Without Smart Defaults
Task 4: Prepare PKI
Task 5: Configure One Side for Certificate-Based Authentication

Lesson 3: Deploying Hub-and-Spoke IPsec VPNs Using Cisco IOS FlexVPN

Lesson Objective: Describe the hub-and-spoke connectivity scenario that can be implemented using the FlexVPN framework

This lesson includes these topics:

Cisco IOS Hub-and-Spoke 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

Summary

Lab 3-2: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN

Lab Objective: Implement hub-to-spoke secure connectivity using Cisco IOS Flex VPN

This lab includes these tasks:

Task 1: Configure Hub and Spoke for Virtual Access Connections
Task 2: Configure Certificate-Based Authentication on Spoke
Task 3: Configure Locally Managed Mode Config
Task 4: Add a Second Flex VPN Spoke

Lesson 4: Deploying Spoke-to-Spoke IPsec VPNs Using Cisco IOS FlexVPN

Lesson Objective: Describe the spoke-to-spoke connectivity scenario that can be implemented using the FlexVPN framework

This lesson includes these topics:

FlexVPN Spoke-to-Spoke Shortcut Deployments

NHRP in FlexVPN

Configure a Spoke in a Spoke-to-Spoke Shortcut Scenario

Configure a Hub in a Spoke-to-Spoke Shortcut Scenario

Verify and Troubleshoot Spoke-to-Spoke Shortcut Switching

Summary

Lab 3-3: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN

Lab Objective: Configure BGP in the Hub-and-Spoke Topology

This lab includes these tasks:

Task 1: Configure BGP
Task 2: Configure Spoke-to-Spoke Shortcut Switching

Lesson 5: Module Summary

This lesson includes these topics:

References

Lesson 6: Module Self-Check

Module 4: Deploying Clientless SSL VPNs

Module Objective: Deploy clientless SSL VPN

Lesson 1: Clientless SSL VPN Overview

Lesson Objective: Describe clientless SSL VPN and provide a general description of the SSL/TLS protocol

This lesson includes these topics:

Cisco Clientless SSL VPN

Cisco Clientless SSL VPN Use Cases

Cisco Clientless SSL VPN Application Access Methods

Secure Sockets Layer and Transport Layer Security

SSL Session Setup and Key Management

SSL Server Authentication

SSL Client Authentication

SSL Transmission Protection

Cisco ASA Remote Access Configuration Concept

Cisco ASA Connection Profiles

Cisco ASA Group Policies

Summary

Lesson 2: Deploying Basic Cisco Clientless SSL VPN on Cisco ASA

Lesson Objective: Configure and verify baseline clientless SSL VPN remote access features of the Cisco ASA security appliance

This lesson includes these topics:

Basic Cisco Clientless SSL VPN

Cisco ASA SSL Server Authentication

SSL VPN Clients Authentication

Clientless SSL VPN URL Entry and Bookmarks

Configuration Scenario

Configuration Tasks

Configure Basic Cisco Clientless SSL VPN

Verify Basic Cisco Clientless SSL VPN

Summary

Lab 4-1: Implement ASA Basic Clientless SSL VPN

Lab Objective: Enable basic clientless SSL VPN connections on the Cisco ASA

This lab includes these tasks:

Task 1: Enable Clientless SSL VPN Connections
Task 2: Enroll ASA in PKI
Task 3: Configure a Bookmark

Lesson 3: Deploying Application Access in Cisco ASA Clientless SSL VPN

Lesson Objective: Deploy and manage advanced application-access features of a clientless Cisco SSL VPN

This lesson includes these topics:

Cisco Clientless SSL VPN Application Access Methods

Cisco Clientless SSL VPN Application Access Solution Components

Application Plug-Ins

Application Plug-Ins Available on Cisco ASA Security Appliances

Plug-In Configuration Scenario

Configure Clientless SSL VPN Plug-Ins

Verify Clientless SSL VPN Plug-Ins

Smart Tunnels

Smart Tunnel Configuration Options and Scenario

Configure Smart Tunnels

Verify Smart Tunnels

Troubleshoot Clientless SSL VPN

Summary

Lab 4-2: Configure Application Access for Cisco ASA Clientless SSL VPN

Lab Objective: Deploy application plugins in the clientless SSL VPNs

This lab includes these tasks:

Task 1: Configure Application Access Using Plugins
Task 2: Configure Application Access Using Smart Tunnels

Lesson 4: Deploying Advanced Authentication and Authorization in Clientless SSL VPN

Lesson Objective: Deploy and manage advanced authentication and authorization features of a clientless Cisco SSL VPN

This lesson includes these topics:

User Authentication and Access Privilege Management

Client Authentication Scenario Using Local CA

Configure Local CA Client Authentication

Verify Client Authentication Using Local CA

Client Authentication Using External CA

Client Authentication and Authorization Using AAA Server

Configure Client Authentication and Authorization Using AAA Server

Verify Client Authentication and Authorization Using AAA Server

Multiple Client Authentication Scenario

Configure Multiple Client Authentication

Verify Multiple Client Authentication

Summary

Lab 4-3: Implement Local and External AAA for Clientless SSL VPNs

Lab Objective: Implement local authorization of clientless SSL VPNs

This lab includes these tasks:

Task 1: Configure Local Authorization
Task 2: Enable RADIUS-Based Authentication and Authorization
Task 3: Test External Authentication and Authorization

Lesson 5: Module Summary

This lesson includes these topics:

References

Lesson 6: Module Self-Check

Module 5: Deploying Cisco AnyConnect VPNs

Module Objective: Implement and maintain Cisco AnyConnect client-based remote access SSL and IPsec VPNs on the Cisco ASA security appliance VPN gateway, according to policies and environmental requirements

Lesson 1: Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA

Lesson Objective: Configure, verify, and troubleshoot a basic Cisco AnyConnect SSL VPN on a Cisco ASA security appliance

This lesson includes these topics:

Basic Cisco AnyConnect SSL VPN

SSL VPN Server Authentication

SSL VPN Clients Authentication

SSL VPN Clients IP Address Assignment

SSL VPN Split Tunneling

Configuration Scenario

Configuration Tasks

Enable AnyConnect SSL VPN

Define IP Address Pool

Configure Identity NAT

Configure Group Policy

Configure Group Policy: Split Tunneling

Configure Connection Profile

Monitor AnyConnect VPN on Client

Monitor AnyConnect VPN on Server

Summary

Lab 5-1: Implement ASA Basic AnyConnect SSL VPN

Lab Objective: Install user certificate on the client machine.

This lab includes these tasks:

Task 1: Install Client Certificate on Employee-PC and Move Employee-PC to SP Subnet
Task 2: Enable AnyConnect SSL VPN Connections and Create a Local VPN User
Task 3: Configure VPN IP Address Pool and Identity NAT
Task 4: Configure Connection Profile
Task 5: Configure Group Policy: IP Pool, DNS and Split Tunneling
Task 6: Test AnyConnect SSL VPNs

Lesson 2: Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA

Lesson Objective: Configure, verify, and troubleshoot advanced features of Cisco AnyConnect SSL VPNs

This lesson includes these topics:

Cisco AnyConnect SSL VPN Solution Components

DTLS Overview

Parallel DTLS and TLS Tunnels

Configure DTLS

Verify DTLS

Cisco AnyConnect Client Configuration Management

Managing Cisco AnyConnect Software from Cisco ASA

Cisco AnyConnect Client Operating System Integration Options

Deploying Cisco AnyConnect Trusted Network Detection

Cisco AnyConnect Start Before Logon

Deploying Cisco AnyConnect Start Before Logon

Summary

Lesson 3: Deploying Advanced Authentication and Authorization in Cisco AnyConnect VPNs

Lesson Objective: Configure, verify, and troubleshoot advanced authentication and authorization in Cisco AnyConnect VPNs

This lesson includes these topics:

Cisco AnyConnect Advanced Authentication Scenarios

Certificate-Based Server Authentication

Certificate-Based Client Authentication

Client Enrollment Methods

Methods for Revoking Credentials

Enable Certificate-Based Authentication

Enable Two-Factor Authentication

Two-Factor Authentication with Name Pre-Fill

Local Authorization Overview

Local Authorization Configuration Procedure

Configure Local Authorization

Verify Local Authorization

External Authorization Scenario

Configure Authorization Profile on Cisco ISE

Verify External Authorization

Troubleshooting Cisco AnyConnect VPN

Summary

Lab 5-2: Configure Advanced Authentication for Cisco AnyConnect SSL VPN

Lab Objective: Implement Cisco AnyConnect SSL VPN access with RADIUS-based user authentication.

This lab includes these tasks:

Task 1: Join the ISE to Active Directory
Task 2: Deploy Certificate-Based Client Authentication
Task 3: Deploy Two-Factor Client Authentication
Task 4: Deploy Local Authorization for Local VPN Users
Task 5: Deploy External Authorization
Task 6: Deploy AnyConnect Profile To Allow AnyConnect VPNs from Remote Desktop
Task 7: Deploy Standalone AnyConnect Client on Guest-PC

Lesson 4: Deploying Cisco AnyConnect IPSec/IKEv2 VPNs

Lesson Objective: Configure, verify, and troubleshoot a Cisco AnyConnect IPsec/IKEv2 VPN on Cisco ASA security appliances

This lesson includes these topics:

Supported Cisco Remote Access IPsec VPN Clients

AnyConnect Support for IKEv2

Making IPsec the Primary Protocol for a Host Entry

IKEv2 Configuration Procedure

Configure a Cisco AnyConnect IPsec VPN on a Cisco ASA

Verify and Troubleshoot Cisco AnyConnect IPsec VPN on Cisco ASA

Summary

Lab 5-3: Implement AnyConnect IPSec/IKEv2

Lab Objective: Implement Cisco AnyConnect IPsec VPN using the WebLaunch method

This lab includes these tasks:

Task 1: Deploy AnyConnect IPsec VPN Using WebLaunch
Task 2: Deploy AnyConnect IPsec VPN Using Standalone AnyConnect Mobility Client (Optional)

Lesson 5: Module Summary

This lesson includes these topics:

References

Lesson 6: Module Self-Check

Module 6: Endpoint Security and Dynamic Access Policies

Module Objective: Deploy Cisco HostScan and DAP features of the Cisco ASA security appliance

Lesson 1: Implementing Host Scan

Lesson Objective: Describe AnyConnect Posture Module and HostScan

This lesson includes these topics:

Overview of AnyConnect Posture Module and HostScan

Security Posture Components

HostScan Functionality

Host Scan Workflow

VPN Posture Deployments

Host Scan Configuration Procedure

Enable Host Scan

Configure Basic Host Scan and Extensions

Configure Advanced Endpoint Assessment

Summary

Lesson 2: Implementing DAP for SSL VPNs

Lesson Objective: Describe the Dynamic Access Policy (DAP) feature of the Cisco ASA security appliance

This lesson includes these topics:

DAP Overview

DAP Solution Components

DAP Hierarchy

DAP Operations

Factors Affecting DAP

Integrating DAP with Host Scan

DAP with Host Scan Integration Scenario

Modify Default DAP

Configure DAP to Match Compliant AntiSpyware Software

Configure DAP to Match Compliant AntiVirus Software

Verify DAP Operation

Summary

Lab 6-1: Implement Host Scan and DAP

Lab Objective: Deploy the ASA's Dynamic Access Policy (DAP) and evaluate endpoint attributes

This lab includes these tasks:

Task 1: Enable Host Scan and Examine AntiSpyware Software on Employee-PC
Task 2: Deploy DAP to Evaluate Endpoint Posture Status
Task 3: Deploy Automatic Endpoint Remediation
Task 4: Deploy AntiVirus Posture (Optional)

Lesson 3: Module Summary

This lesson includes these topics:

References

Lesson 4: Module Self-Check