email : techcenter@trainocate.com.my
contact : +603-2281-1111

UCSEC: Implementing Cisco Unified Communications Security

Course Code: UCSEC
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Implementing Cisco Unified Communications Security (UCSEC) v1.0 is a new five-days ILT class that is designed to provide students with the necessary knowledge and skills to implement security features in a Cisco Unified Communications environment. Cisco Unified Communications support several features and mechanisms to secure voice signaling and communications and to mitigate attacks against Cisco Unified Communications networks. The Implementing Cisco Unified Communications Security (UCSEC) v1.0 course introduces security mechanisms and describes different implementation scenarios that increase the security level of Cisco Unified Communications networks.

SKILLS COVERED

Upon completing this course, the learner will be able to meet these overall objectives:

- Identify vulnerabilities in Cisco Unified Communications networks and describe security strategies, cryptographic services, PKI, and VPN technologies
- Implement network infrastructure security features
- Implement Cisco Unified Communications Manager and Cisco Unified Communications endpoint security features
- Implement network infrastructure security features

WHO SHOULD ATTEND?

- Network Engineers
- Security Engineers

PRE-REQUISITES

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

- Working knowledge of converged voice and data networks
- Working knowledge of Cisco IOS gateways, Cisco Unified SRST gateways, and Cisco Unified Border Element
- Working knowledge of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
- CCNP® Voice certification is recommended

Additional knowledge and skills that will help the learner benefit fully from the course are as follows:

- Knowledge of network security fundamentals
- Knowledge of Cisco IOS Firewall and Cisco ASA adaptive security appliance firewalls
- Knowledge of IPsec and SSL VPNs
- CCNA® Security certification is recommended

Cisco learning offerings:

- Implementing Cisco Voice Communications and QoS (CVOICE) v8.0
- Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) v8.0

- Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) v8.0
- Implementing Cisco IOS Network Security (IINS) v1.0

MODULES

Module 1: Vulnerabilities of Cisco Unified Communications Networks and Security Fundamentals

- Lesson 1-1: Assessing Vulnerabilities of Cisco Unified Communications Networks
- Lesson 1-2: Describing Security Implementation Strategies
- Lesson 1-3: Describing Cryptographic Services and Functions
- Lesson 1-4: Describing Key Management and PKI
- Lesson 1-5: Describing IPsec and Cisco AnyConnect SSL VPN

Module 2: Network Infrastructure Security

- Lesson 2-1: Implementing Network Separation and Packet Filtering
- Lesson 2-2: Implementing Switch Security Features
- Lesson 2-3: Implementing Cisco AnyConnect SSL VPNs in Cisco Unified Communications Networks

Module 3: Cisco Unified Communications Manager and Endpoint Security Features

- Lesson 3-1: Hardening Cisco Unified Communications Endpoints
- Lesson 3-2: Implementing Toll-Fraud Prevention
- Lesson 3-3: Implementing Native Cisco Unified Communications Manager Security Features
- Lesson 3-4: Implementing Cisco Unified Communications Manager Security Features Based on Security Tokens

Module 4: Cisco Unified Communications Integration and Features Secure

- Lesson 4-1: Implementing SRTP to Gateways and Signaling Protection by IPsec
- Lesson 4-2: Implementing Secure Signaling and SRTP in SRST and Cisco Unified Communications Manager Express
- Lesson 4-3: Implementing Trusted Relay Points
- Lesson 4-4: Implementing Proxies for Secure Signaling and SRTP

Lab Details

- Lab 1-1: Identifying Security Weaknesses in a Cisco Unified Communications Network
- Lab 2-1: Implementing Firewalls
- Lab 2-2: Implementing 802.1X
- Lab 2-3: Implementing Cisco AnyConnect SSL VPNs
- Lab 3-1: Implementing Cisco Unified Communications Manager Security Features Based on Security Tokens
- Lab 4-1: Implementing SRTP to Gateways and Signaling Protection by IPsec
- Lab 4-2: Implementing Secure SRST and Secure Cisco Unified Communications Manager Express
- Lab 4-3: Implementing Trusted Relay Points
- Lab 4-4: Implementing Proxies for Signaling and RTP

END OF PAGE