UCSEC (IMPLEMENTING CISCO UNIFIED COMMUNICATIONS SECURITY) 1.0

Objetivo

Implementing Cisco Unified Communications Security (UCSEC) v1.0 is a new 5-day ILT class 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. After completing this course, students will be able to: - Identify vulnerabilities in Cisco Unified Communications networks, describe security implementation strategies, cryptographic services, PKI, and VPN technologies - Implement network infrastructure security features such as network separation and firewalling, 802.1X in phone VLANs, and the IP Phone VPN Client - Harden Cisco Unified Communications endpoints and implement toll-fraud prevention features and Cisco Unified Communications Manager cryptographic security features - Implement secure Cisco Unified Communications Manager integration with external devices, such as gateways, firewalls, and application proxies The software applications covered in this course include: - Cisco Unified Communications Manager version 8.5 - Cisco IOS Software Release v15.1(3)T at routers, Cisco IOS Software Release 2.2.55(SE1) at switches - Cisco ASA adaptive security appliance Release 8.3 - Cisco Secure Cisco Secure Access Control Server (ACS) version 5.2. To provide learners with the necessary knowledge and skills that are common in all Cisco Unified Communications Manager deployments and additionally, those that are required to fully implement a single site solution.

Público Alvo

Channel Partner / Reseller Customer Employee

Pré-Requisitos

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. Additional beneficial knowledge and skills: CCNP Voice certification is recommended. Knowledge of network security fundamentals. Knowledge of Cisco IOS Firewall and Cisco ASA adaptive security appliance firewalls. Knowledge of IPsec and / or SSL VPNs. CCNA Security certification is recommended by attending the following 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)

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Module 1 - Vulnerabilities of Cisco Unified Communications Networks and Security Fundamentals
Module 2 - Network Infrastructure Security
Module 3 - Cisco Unified Communications Manager and Endpoint Security Features
Module 4 - Secure Cisco Unified Communications Integration and Features