Implementing Cisco SD-WAN Security and Cloud Solutions (SDWSCS) v1.1

What you'll learn

The Implementing Cisco SD-WAN Security and Cloud Solutions (SDWSCS) v1.1 training is an advanced training focused on Cisco SD-WAN security and cloud services. Through a series of labs and lectures you will learn about on-box security services, including application-aware enterprise firewall, intrusion prevention, URL filtering, malware protection, and Transport Layer Security (TLS) or Secure Socket Layer (SSL) decryption. You will also learn about cloud integration with multiple cloud service providers across multiple use cases.

Additionally, the training labs will allow you to configure and deploy local security services and cloud security services with the Cisco Umbrella Secure Internet Gateway (SIG), as well as integrate the Cisco SD-WAN fabric with a cloud service provider using the Cisco vManage automated workflows.

The training will allow you to earn 24 Continuing Education (CE) credits toward recertification.

How you'll benefit

This training will:

Introduce you to the security and cloud services available in Cisco SD-WAN

Expand your knowledge of integrated security services, such as the application aware firewall and intrusion prevention and cloud and collocated security services in on-premises and private or public cloud environments.

Help you understand drivers, benefits, available features, and the architecture of Cisco SD-WAN integrated and distributed security and cloud networking services

Who should enroll

This training is designed for the following roles:

Network engineers

Network security engineers

Network architects

Sales/presales engineers

Technology areas

Enterprise networking

Network security

Cisco SD-WAN

Cloud services

Training overview

Prerequisites

Before taking this training, you should have a:

Basic understanding of enterprise routing

Basic understanding of WAN networking

Basic understanding of Cisco SD-WAN

Basic understanding of Public Cloud services

These recommended Cisco learning offerings may help students meet these prerequisites:

Implementing and Administering Cisco Solutions (CCNA®)

Implementing Cisco SD-WAN Solutions (ENSDWI)

Cisco SD-WAN Operation and Deployment (SDWFND)

Objectives

After completing this training, you should be able to:

Describe Cisco SD-WAN security functions and deployment options

Understand how to deploy on-premises threat prevention

Describe content filtering options

Implement secure Direct Internet Access (DIA)

Explain and implement service chaining

Explore Secure Access Service Edge (SASE) and identify use cases

Describe Cisco Umbrella Secure Internet Gateway (SIG) and deployment options

Implement Cisco Umbrella SIG and Domain Name System (DNS) policies

Explore and implement Cloud Access Security Broker (CASB) and identify use cases (including Microsoft 365)

Describe how to use Cisco ThousandEyes to monitor cloud services

Configure Cisco ThousandEyes to monitor Microsoft 365 applications

Examine how to protect and optimize access to the Software as a Service (SaaS) application with Cisco SD-WAN Cloud OnRamp

Describe and deploy Cloud OnRamp for multi-cloud, including interconnect and colocation use cases

Examine Cisco SD-WAN monitoring capabilities and features with vManage and vAnalytics.

Lab Outline

Configure Threat Prevention

Implement Web Security

Deploy DIA Security with Unified Security Policy

Deploy Service Chaining

Configure Cisco Umbrella DNS Policies

Deploy Cisco Umbrella Secure Internet Gateway

Implement CASB Security

Microsoft 365 SaaS Testing by Using Cisco ThousandEyes

Configure Cisco OnRamp for SaaS

Deploy Cisco SD-WAN Multicloud Gateways

Cisco vAnalytics Overview