Securing Email with Cisco Email Security Appliance (SESA) v3.1 Course

Course Duration: 24 Hours **Course Code: SESA-3101**

1. Course Overview

This course provides comprehensive training on Cisco Email Security Appliance (SESA) v3.1, designed to equip participants with the knowledge and skills to secure email infrastructure effectively. You'll learn how to implement, configure, and manage SESA solutions to protect organizations from spam, phishing, malware, and other email-borne threats. The course also covers policy creation, message tracking, reporting, and troubleshooting techniques to ensure secure and efficient email communication.

2. What You'll Learn:

Understand the architecture and deployment options of Cisco Email Security Appliance (SESA)

Configure inbound and outbound email policies for security and compliance

Implement anti-spam, anti-malware, and data loss prevention (DLP) features

Monitor, report, and troubleshoot email security events

Integrate SESA with other Cisco security solutions for enhanced protection

3. Target Audience:

Network and security engineers

System administrators responsible for email infrastructure

IT professionals interested in email security management

Security analysts focusing on email threat prevention

4. Pre-Requisites:

Basic knowledge of networking and email protocols (SMTP, IMAP, POP3)

Understanding of cybersecurity fundamentals

Familiarity with Cisco devices and security concepts is recommended but not mandatory

5. Course Content (Modules):

Module 1: Introduction to Cisco Email Security Appliance (SESA)

Overview of SESA architecture and deployment

Features and benefits

Module 2: Policy Configuration and Management

Creating and managing inbound and outbound policies

Setting up content filters and security policies

Module 3: Anti-Spam and Anti-Malware Techniques

Configuring anti-spam settings

Implementing anti-malware scanning

Best practices for threat mitigation

Module 4: Data Loss Prevention (DLP)

Overview of DLP functionality

Configuring DLP policies

Monitoring sensitive information

Module 5: Monitoring, Reporting, and Troubleshooting

Message tracking and event logging

Generating reports

Troubleshooting common email security issues

Module 6: Integration and Advanced Features

Integration with other Cisco security products

Advanced configuration and optimization techniques

V25.03.01