FIREFLY

CISCO

CONTACT US

Securing Email with Cisco Email Security Appliance

DURATION: 4 DAYS COURSE CODE: SESA FORMAT: LECTURE/LAB

COURSE DESCRIPTION

The Securing Email with Cisco Email Security Appliance (SESA) v3.1 course shows you how to deploy and use Cisco® Email Security Appliance to establish protection for your email systems against phishing, business email compromise, and ransomware, and to help streamline email security policy management. This hands-on course provides you with the knowledge and skills to implement, troubleshoot, and administer Cisco Email Security Appliance, including key capabilities such as advanced malware protection, spam blocking, anti-virus protection, outbreak filtering, encryption, quarantines, and data loss prevention.

WHO SHOULD ATTEND

Network or security technicians, administrators, engineers or managers responsible for web and email security

Security architects and system designers

Network administrators and operations engineers

Cisco partners, resellers, or employees responsible for supporting Cisco email security solutions

Cisco channel partners who are seeking to maintain, optimize, and troubleshoot a Cisco ESA

Channel partner field engineers who are seeking to be trained and certified on the Email Security for Field Engineer (700-280 ESFE) exam

PREREQUISITES

A student must possess one or more of the following basic technical competencies:

- Cisco certification (Cisco CCENT certification or higher)
- Relevant industry certification, such as (ISC)²
- Cisco Networking Academy letter of completion (CCNA 1 and CCNA 2)
- Windows expertise: Microsoft (Microsoft Specialist, MCSA, MCSE), CompTIA (A+, Network+, Server+)

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

- TCP/IP services, including DNS, SSH, FTP, SNMP, HTTP, and HTTPs, is assumed
- Experience with IP routing is assumed

COURSE OBJECTIVES

Describe the Cisco Email Security Appliance

Administer the Cisco Email Security Appliance

Control sender and recipient domains

Control spam with Talos SenderBase and anti-spam

Use anti-virus and outbreak filters

Use mail policies

Use content filters

Use message filters to enforce email policies

Prevent data loss

Perform LDAP queries

Authenticate SMTP sessions

Authenticate email

Encrypt email

Use system quarantines and delivery methods

Perform centralized management using clusters

Test and troubleshoot

COURSE OUTLINE