Securing Email with Cisco Email Security Appliance (SESA) v3.2

What you'll learn in this course

The Securing Email with Cisco Email Security Appliance (SESA) training 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 training 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.

This training prepares you for the 300-720 SESA v1.1 exam. If passed, you earn the Cisco Certified Specialist – Email Content Security certification and satisfy the concentration exam requirement for the CCNP Security certification. This training also earns you 24 Continuing Education (CE) credits towards recertification.

Course duration

- Instructor-led training: 4 days in the classroom with hands-on lab practice
- Virtual instructor-led training: 4 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 4 days of video instruction with hands-on lab practice

Who should enroll

- Security Engineers
- Security Administrators
- Security Architects
- Operations Engineers
- Network Engineers
- Network Administrators
- Network or Security Technicians
- Network Managers
- System Designers
- Cisco Integrators and Partners

How to Enroll

To enroll in the SESA course or explore our larger catalog of courses on Cisco Digital Learning, contact us at <training@fastlane-mea.com>

Course details

Outline

1. Describing the Cisco Email Security Appliance
2. Controlling Sender and Recipient Domains
3. Controlling Spam with Talos SenderBase and Anti-Spam
4. Using Anti-Virus and Outbreak Filters
5. Using Mail Polices
6. Using Content Filters
7. Using Message Filters
8. Preventing Data Loss
9. Using LDAP
10. Describing SMTP Session Authentication
11. Using Email Authentication
12. Using Email Encryption
13. Administering the Cisco Email Security Appliance
14. Using System Quarantines and Delivery Methods
15. Centralizing Management Using Clusters
16. Testing and Troubleshooting

Prerequisites

The basic technical competencies you are expected to have before attending this training are:

- Cisco certification, such as Cisco Certified Support Technician (CCST) Cybersecurity certification or higher
- Relevant industry certification, such as (ISC)2, CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC), and ISACA
- Cisco Networking Academy letter of completion (CCNA® 1 and CCNA 2)
- Windows expertise, such as Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], and CompTIA (A+, Network+, Server+)

The knowledge and skills you are expected to have before attending this training are:

- Transmission control protocol/internet protocol (TCP/IP) services, including domain name system (DNS), secure shell (SSH), file transfer protocol (FTP), simple network management protocol (SNMP), hypertext transfer protocol (HTTP), and hypertext transfer protocol secure (HTTPS)
- Experience with IP routing