
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.

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

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

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

1. Describing the Cisco Email Security Appliance

Discovery 1: Verify and Test Cisco ESA Configuration

2. Administering the Cisco Email Security Appliance

Discovery 2: Perform Basic Administration

3. Controlling Sender and Recipient Domains

4. Controlling Spam with Talos SenderBase and Anti-Spam

Discovery 3: Advanced Malware in Attachments
(Macro Detection)

Discovery 4: Protect against Malicious or Undesirable URLs
Beneath Shortened URLs

Discovery 5: Protect Against Malicious or Undesirable URLs
Inside Attachments

Discovery 6: Intelligently Handle Unscannable Messages

Discovery 7: Leverage AMP Cloud Intelligence Via Pre-
Classification Enhancement

Discovery 8: Integrate Cisco ESA with AMP Console

5. Using Anti-Virus and Outbreak Filters

Discovery 9: Prevent Threats with Anti-Virus Filters

Discovery 10: Applying Content and Outbreak Filters

6. Using Mail Policies

7. Using Content Filters

Discovery 11: Configure attachment Scanning

8. Using Message Filters

9. Preventing Data Loss

Discovery 12: Configure Outbound Data Loss Prevention

10. Using LDAP

Discovery 13: Integrate Cisco ESA with LDAP and Enable the
LDAP Accept Query

11. SMTP Session Authentication

12. Email Authentication

Discovery 14: DomainKeys Identified Mail (DKIM)

Discovery 15: Sender Policy Framework (SPF)

Discovery 16: Forged Email Detection

13. Email Encryption

14. Using System Quarantines and Delivery Methods

15. Centralized Management Using Clusters

Discovery 17: Configure the Cisco SMA for Tracking and
Reporting

16. Testing and Troubleshooting

17. References