# SECURING EMAIL WITH CISCO EMAIL SECURITY APPLIANCE

### DURATION: 3 DAYS

## COURSE OVERVIEW

The **Securing Email with Cisco Email Security Appliance** (SESA) v3.0 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.

This course helps you prepare to take the exam, **Securing Email with Cisco Email Security Appliance** (300-720 SESA), which leads to **CCNP® Security** and the **Certified Specialist - Email Content Security** certifications.

This class will help you deploy high-availability email protection against the dynamic, rapidly changing threats affecting your organization, and gain leading-edge career skills focused on enterprise security.

## COURSE OBJECTIVES

**After taking this course, you should be able to:**

1. Describe and administer the Cisco Email Security Appliance (ESA)
2. Control sender and recipient domains
3. Control spam with Talos Sender Base and anti-spam
4. Use anti-virus and outbreak filters
5. Use mail policies
6. Use content filters
7. Use message filters to enforce email policies
8. Prevent data loss
9. Perform LDAP queries
10. Authenticate Simple Mail Transfer Protocol (SMTP) sessions

11. Authenticate email
12. Encrypt email
13. Use system quarantines and delivery methods
14. Perform centralized management using clusters
15. Test and troubleshoot

## COURSE CONTENT

### Describing the Cisco Email Security Appliance

Cisco Email Security Appliance Overview

Technology Use Case

Cisco Email Security Appliance Data Sheet

SMTP Overview

Email Pipeline Overview

Installation Scenarios

Initial Cisco Email Security Appliance Configuration

Centralizing Services on a Cisco Content Security Management Appliance (SMA)

Release Notes for AsyncOS 11.x

### Administering the Cisco Email Security Appliance

Distributing Administrative Tasks

System Administration

Managing and Monitoring Using the Command Line Interface (CLI)

Other Tasks in the GUI

Advanced Network Configuration

Using Email Security Monitor

Tracking Messages

Logging

### Controlling Sender and Recipient Domains

Public and Private Listeners

Configuring the Gateway to Receive Email

Host Access Table Overview

Recipient Access Table Overview

Configuring Routing and Delivery Features

## Controlling Spam with Talos Sender Base and Anti-Spam

Sender Base Overview

Anti-Spam

Managing Graymail

Protecting Against Malicious or Undesirable URLs

File Reputation Filtering and File Analysis

Bounce Verification

## Using Anti-Virus and Outbreak Filters

Anti-Virus Scanning Overview

Sophos Anti-Virus Filtering

McAfee Anti-Virus Filtering

Configuring the Appliance to Scan for Viruses

Outbreak Filters

How the Outbreak Filters Feature Works

Managing Outbreak Filters

## Using Mail Policies

Email Security Manager Overview

Mail Policies Overview

Handling Incoming and Outgoing Messages Differently

Matching Users to a Mail Policy

Message Splintering

Configuring Mail Policies

## Using Content Filters

Content Filters Overview

Content Filter Conditions

Content Filter Actions

Filter Messages Based on Content

Text Resources Overview

Using and Testing the Content Dictionaries Filter Rules

Understanding Text Resources

Text Resource Management

Using Text Resources

## Using Message Filters to Enforce Email Policies

Message Filters Overview

Components of a Message Filter

Message Filter Processing

Message Filter Rules

Message Filter Actions

Attachment Scanning

Examples of Attachment Scanning Message Filters

Using the CLI to Manage Message Filters

Message Filter Examples

Configuring Scan Behavior

## Preventing Data Loss

Overview of the Data Loss Prevention (DLP) Scanning Process

Setting Up Data Loss Prevention

Policies for Data Loss Prevention

Message Actions

Updating the DLP Engine and Content Matching Classifiers

## Using LDAP

Overview of LDAP

Working with LDAP

Using LDAP Queries

Authenticating End-Users of the Spam Quarantine

Configuring External LDAP Authentication for Users

Testing Servers and Queries

Using LDAP for Directory Harvest Attack Prevention

Spam Quarantine Alias Consolidation Queries

Validating Recipients Using an SMTP Server

## SMTP Session Authentication

Configuring AsyncOS for SMTP Authentication

Authenticating SMTP Sessions Using Client Certificates

Checking the Validity of a Client Certificate

Authenticating User Using LDAP Directory

Authenticating SMTP Connection Over Transport Layer Security (TLS) Using a Client Certificate

Establishing a TLS Connection from the Appliance

Updating a List of Revoked Certificates

### Email Authentication

Email Authentication Overview

Configuring Domain Keys and Domain Keys Identified Mail DKIM) Signing

Verifying Incoming Messages Using DKIM

Overview of Sender Policy Framework SPF) and SIDF Verification

Domain-based Message Authentication Reporting and Conformance (DMARC) Verification

Forged Email Detection

### Email Encryption

Overview of Cisco Email Encryption

Encrypting Messages

Determining Which Messages to Encrypt

Inserting Encryption Headers into Messages

Encrypting Communication with Other Message Transfer Agents (MTAs)

Working with Certificates

Managing Lists of Certificate Authorities

Enabling TLS on a Listener's Host Access Table (HAT)

Enabling TLS and Certificate Verification on Delivery

Secure/Multipurpose Internet Mail Extensions (S/MIME) Security Services

### Using System Quarantines and Delivery Methods

Describing Quarantines

Spam Quarantine

Setting Up the Centralized Spam Quarantine

Using Safe lists and Block lists to Control Email Delivery Based on Sender

Configuring Spam Management Features for End Users

Managing Messages in the Spam Quarantine

Policy, Virus, and Outbreak Quarantines

Managing Policy, Virus, and Outbreak Quarantines

Working with Messages in Policy, Virus, or Outbreak Quarantines

Delivery Methods

### Centralized Management Using Clusters

Overview of Centralized Management Using Clusters

Cluster Organization

Creating and Joining a Cluster

Managing Clusters

Cluster Communication

Loading a Configuration in Clustered Appliances

Best Practices

**Testing and Troubleshooting**

Debugging Mail Flow Using Test Messages: Trace

Using the Listener to Test the Appliance

Troubleshooting the Network

Troubleshooting the Listener

Troubleshooting Email Delivery

Troubleshooting Performance

Web Interface Appearance and Rendering Issues

Responding to Alerts

Troubleshooting Hardware Issues

Working with Technical Support

**References**

Model Specifications for Large Enterprises

Model Specifications for Midsize Enterprises and Small-to-Midsize Enterprises or Branch Offices

Cisco Email Security Appliance Model Specifications for Virtual Appliances

Packages and Licenses

**Lab Outline:**

Verify and Test Cisco ESA Configuration

Perform Basic Administration

Advanced Malware in Attachments (Macro Detection)

Protect Against Malicious or Undesirable URLs Beneath Shortened URLs

Protect Against Malicious or Undesirable URLs Inside Attachments

Intelligently Handle Un scan able Messages

Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement

Integrate Cisco ESA with AMP Console

Prevent Threats with Anti-Virus Protection

Applying Content and Outbreak Filters

Configure Attachment Scanning

Configure Outbound Data Loss Prevention

Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query

Domain Keys Identified Mail (DKIM)

Sender Policy Framework (SPF)

Forged Email Detection

Configure the Cisco SMA for Tracking and Reporting

**Too much information**

## COURSE PREREQUISITES

TOP

**To fully benefit from this course, you should have one or more of the following basic technical competencies:**

Cisco certification (Cisco CCENT® 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: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], CompTIA (A+, Network+, Server+)

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

TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS

Experience with IP routing

**Cisco learning offerings that contribute to recommended skills and knowledge:**

# TEST CERTIFICATION

**Recommended as preparation for the following exams:**

The 300-720 SESA exam certifies your knowledge of Cisco Email Security Appliance, including administration, spam control and anti-spam, message filters, data loss prevention, Lightweight Directory Access Protocol (LDAP), email authentication and encryption, and system quarantines and delivery methods. The exam will be available beginning February 24, 2020.

After you pass 300-720 SESA:

You earn the Cisco Certified Specialist - Email Content Security certification.

You will have satisfied the concentration exam requirement for the new CCNP Security certification. To complete your CCNP Security certification, pass the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam or its equivalent.