# Securing Email with Cisco Email Security Appliance (SESA) 1.0

## Course Overview:

Securing Email with Cisco Email Security Appliance (SESA) combines Parts 1 and 2 (SESA1, SESA2) into a single, three-day course. Students who take this SESA training learn to use Cisco Email Security Appliances (ESAs) to manage and troubleshoot email in their networks. Attendees of this SESA course receive in-depth instruction on popular features, emphasizing topics listed below, learn advanced Internet email concepts and receive an overview of how to customize configurations. SESA also teaches advanced configuration and operation of the Cisco ESA (Formerly Cisco IronPort Email Security Appliance). Extensive lab exercises provide critical hands-on experience with advanced features of the ESA.

## Who Should Attend:

- Enterprise messaging managers and system administrators
- Email system designers and architects
- Network managers responsible for messaging implementation of the sender

## Prerequisites:

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

- A moderate knowledge of TCP / IP fundamentals, including IP addressing and subnetting, static IP routing and DNS.
- Experience with Internet based messaging, including SMTP, Internet message formats, and MIME message format.
- Familiarity with command line interface (CLI) and graphical user interface (GUI).
- Previous experience with email security would be helpful.

## Course Objectives:

Upon completing this course, the learner will be able to meet these overall objectives:

- Creating and apply Data Loss Prevention (DLP) polices to outgoing email
- Configuring Email Security Appliances to detect and handle unwanted spam and viruses
- Using Message Tracking and Reporting to document email traffic trends

- Managing spam quarantines
- Using Cisco reputation-based services, Sensor Base and Virus Outbreak Filters, to increase the security of an email network
- Integrating an ESA with a directory server via LDAP
- Debugging LDAP integration issues
- Using message filters to redirect and modify messages
- Performing safe deployment and debugging of message filters
- Configuring TLS and Guaranteed Secure Delivery
- Configuring Email Authentication with DKIM and SPF

## Course Outline:

**Module 1: Introduction & System Overview**

- List IronPort Email Security Appliances
- Describe the ESA Hardware Options
- Describe the Email Pipeline Filters
- List the ESA Feature Key Options
- Describe the Operation of a Listener

**Module 2: Tracking and Reporting Messages**

- Perform a system installation of an M Series
- Integrate the M Series into the existing C Series lab.
- Use local and Centralized Message Tracking
- Use Local and Centralized Reporting

**Module 3: Controlling Sender & Recipient Domains**

- Configure public and private listeners
- Configure SMTP Routes
- Use Senderbase Reputation Scores (SBRS) to manage mail
- Use Mail Debugging Tools

**Module 4: Controlling Spam with SenderBase & Anti**

- Spam
- Adjust SBRS Configure Anti-Spam Settings
- Configure the IronPort Spam Quarantine
- Use the Security Management Appliance for Off Box Quarantining

**Module 5: Using Anti**

- Virus & Virus Outbreak Filters
- Enable one or both Anti-Virus Engines
- Use one or both AV Engines in Mail Policies
- Use Virus Outbreak Filters to preemptively drop traffic and provide zero-hour protection
- Identify best practices for managing IronPort Anti-Virus

**Module 6: Using Mail Policies to Direct Business Email**

- Use Email Security Manager Create a User Based Mail Policies
- Use Message Tracking to monitor message splintering

**Module 7: Using System Quarantines and Delivery Methods**

- Describe, create and manage quarantines
- Perform searches quarantine contents
- Assign Bounce Profiles
- Create Virtual Gateways

**Module 8: Using Content Filters for Specific Business Needs**

- Describe content scanning
- Detect password protected / non-protected attachments
- Create weighted content matching
- Use Smart Identifiers
- Implement Matched Content Visibility
- Execute best practices when staging new filters

**Module 9: Encrypting Outbound Email**

- Provision with the Cisco Registered Envelope Service
- Associate a content filtering rule with an "Encrypt" action
- Register a CRES Envelope Recipient

**Module 10: Troubleshooting**

- Identify Issues
- Diagnose and Isolate Problems
- Troubleshooting tools and best practices
- Log file contents and log administration

**Module 11: System Administration**

- Safely upgrade software on your IronPort
- Manage users and control alerting behavior
- Manage configurations and prepare for disaster recovery Access Customer Support

**Module 12: Configuring LDAP Queries**

- This module focuses directly on common LDAP configurations and issues. A brief overview of the Lightweight Directory Access Protocol is provided to give those new to LDAP some familiarity, but the bulk of the module assumes a basic understanding of LDAP terms and concepts. Active Directory is emphasized in a number of case studies to highlight the various installation choices. These include addressing the use of the ESA against multiple directories in a heterogeneous enterprise.

**Module 13: Message Filters (Advanced Policy)**

- This module focuses on advanced filter options with specific emphasis on creating, troubleshooting, simplification/streamlining and regular expressions. Helpful tips and tricks for both Message and Content filters are covered. Extensive hands on exercises are designed to give the students practice working with the Command Line Interface (CLI), as well as practical experience troubleshooting and examining logs.

**Module 14: Email Authentication**

## Lab Outline:

**Part I**

- Lab 1-1: Installing Your Email Security Appliance
- Lab 2-1: Configuring the M-Series for Tracking and Reporting
- Lab 3-1: Testing Your Listener Settings
- Lab 4-1: Defending Against Spam with SenderBase and Anti-Spam
- Lab 4-2: Configuring Off-Box Quarantining to the M-Series
- Lab 5-1: Defending Against Viruses
- Lab 5-2: Defending Against Virus Outbreaks and Targeted Attacks
- Lab 6-1: Customizing Mail Policies for Your End Users
- Lab 7-1: Configuring Bounce Profiles
- Lab 7-2: Configuring Virtual Gateways
- Lab 8-1: Enforcing Your Business Policies in Email Delivery
- Lab 9-1: Configuring DLP

- Lab 10-1: Configuring Envelope Encryption
- Lab 11-1: Troubleshooting
- Lab 12-1: Delegated Administrator
- Lab 12-2: Configuring Clusters

**Part II**

- Lab 1-1: Configuring LDAP Accept
- Lab 1-2: Configuring SMTP Call-Ahead
- Lab 1-3: Accommodating Multiple Domains Using LDAP Accept Bypass and Domain
- Lab 1-4: Controlling Mail Policies with LDAP Group Queries
- Lab 2-1: Redirecting Your Mail With Message Filters
- Lab 2-2: Removing Header Information From Outbound Email with Message Filters
- Lab 2-3: Removing File Attachments with Message Filters
- Lab 3-1: Encrypting with TLS
- Lab 4-1: Domain Keys Identified Mail
- Lab 4-2: SIDF and SPF Verification