Securing Email with Cisco Email Security Appliance (SESA v3.1)

Price	Duration	Delivery Methods
$1,750.00	4 Daytime Classes or 8 Evening Classes	Virtual, Private Group,

CAREER SKILLS+™

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

Security engineers
Security administrators
Security architects
Operations engineers
Network engineers
Network administrators
Network or security technicians
Network managers
System designers

Cisco integrators and partners

Course Prerequisites

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

Course Objectives

Describe and administer the Cisco Email Security Appliance (ESA)
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 Simple Mail Transfer Protocol (SMTP) sessions
Authenticate email
Encrypt email
Use system quarantines and delivery methods
Perform centralized management using clusters
Test and troubleshoot

Agenda

1 - 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
2 - 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
3 - 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
4 - Controlling Spam with Talos SenderBase and Anti-Spam
SenderBase Overview
Anti-Spam
Managing Graymail
Protecting Against Malicious or Undesirable URLs
File Reputation Filtering and File Analysis
Bounce Verification
5 - 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
6 - 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
7 - Using Content Filters
Content Filters Overview

Overview of Sender Policy FrameworkSPF) and SIDF Verification
Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
Forged Email Detection
13 - 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
14 - Using System Quarantines and Delivery Methods
Describing Quarantines
Spam Quarantine
Setting Up the Centralized Spam Quarantine
Using Safelists and Blocklists 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
15 - 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
16 - 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
17 - 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
18 - 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 Unscannable 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
DomainKeys Identified Mail (DKIM)
Sender Policy Framework (SPF)
Forged Email Detection
Configure the Cisco SMA for Tracking and Reporting