

Securing Email with Cisco Email Security Appliance (SESAv3.2)

Duration: 32 Hours (4 Days)

Overview

The **Securing Email with Cisco Email Security Appliance (SESA)** 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 course also earns you 24 Continuing Education (CE) credits towards recertification.

Course duration

- 4 Days

How you'll benefit

This training will help you:

- Deploy high-availability email protection against the dynamic, rapidly changing threats affecting your organization
- Gain leading-edge career skills focused on enterprise security
- This course also earns you 24 Continuing Education (CE) credits towards recertification.

This course prepares you to take the exam:

300-720 SESA exam

What to expect in the exam

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.

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.

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

Technology areas

- Security

Training overview

Objectives

After taking this course, you should be able to:

- 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

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

Outline

- 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 SenderBase and Anti-Spam
 - SenderBase 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 DomainKeys and DomainKeys 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 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
- 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 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
- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Forged Email Detection
- Configure the Cisco SMA for Tracking and Reporting