Current Technologies
Computer Learning Centers

cisco Partner
Platinum Learning

Securing Email with Cisco Email Security Appliance (SESA) V3.2

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Securing Email with Cisco Email Security Appliance (SESA) V3.2

Course Duration

4 Days

Course Price

$3,595.00
36 CLCs

Methods of Delivery

In-Person ILT
Virtual ILT
Onsite ILT

About this Class

The Securing Email with Cisco Email Security Appliance (SESA) training 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 training 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 training prepares you for the 300-720 SESA v1.1 exam. If passed, you earn the Cisco Certified Specialist – Email Content Security certification and satisfy the concentration exam requirement for the CCNP Security certification. This training also earns you 24 Continuing Education (CE) credits towards recertification.

Securing Email with Cisco Email Security Appliance (SESA) V3.2

How you will benefit

This class 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
- Prepare for the 300-720 SESA v1.1 exam
- Earn 24 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

- Security Engineers
- Security Administrators
- Security Architects
- Operations Engineers
- Network Engineers
- Network Administrators
- Network or Security Technicians
- Network Managers
- System Designers
- Cisco Integrators and Partners

Securing Email with Cisco Email Security Appliance (SESA) V3.2

Objectives

After taking this course, you should be able to:

- Describe and 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
- Prevent data loss
- Perform lightweight directory access protocol (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

The basic technical competencies you are expected to have before attending this training are:

- Cisco certification, such as Cisco Certified Support Technician (CCST) Cybersecurity 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, such as Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], and CompTIA (A+, Network+, Server+)

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Securing Email with Cisco Email Security Appliance (SESA) V3.2

Course Outline

Module 1: Describing the Cisco Email Security Appliance

Module 2: Controlling Sender and Recipient Domains

Module 3: Controlling Spam with Talos SenderBase and Anti-Spam

Module 4: Using Anti-Virus and Outbreak Filters

Module 5: Using Mail Polices

Module 6: Using Content Filters

Module 7: Using Message Filters

Module 8: Preventing Data Loss

Module 9: Using LDAP

Module 10: Describing SMTP Session Authentication

Module 11: Using Email Authentication

Module 12: Using Email Encryption

Module 13: Administering the Cisco Email Security Appliance

Module 14: Using System Quarantines and Delivery Methods

Module 15: Centralizing Management Using Clusters

Module 16: Testing and Troubleshooting

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Securing Email with Cisco Email Security Appliance (SESA) V3.2

Lab Outline

Lab 1: Verify and Test Cisco ESA Configuration

Lab 2: Advanced Malware in Attachments (Macro Detection)

Lab 3: Protect Against Malicious or Undesirable URLs Beneath Shortened URLs

Lab 4: Protect Against Malicious or Undesirable URLs Inside Attachments

Lab 5: Intelligently Handle Unscannable Messages

Lab 6: Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement

Lab 7: Integrate Cisco ESA with AMP Console

Lab 8: Prevent Threats with Anti-Virus Protection

Lab 9: Applying Outbreak Filters

Lab 10: Configure Attachment Scanning

Lab 11: Configure Outbound Data Loss Prevention

Lab 12: Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query

Lab 13: Domain Keys Identified Mail (DKIM)

Lab 14: Sender Policy Framework (SPF)

Lab 15: Forged Email Detection

Lab 16: Perform Basic Administration

Lab 17: Configure the Cisco Secure Email and Web Manager for Tracking and Reporting