Securing Email with Cisco Email Security Appliance

SESA 3.0 | 3 days

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.

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. The exam will be available beginning February 24, 2020.

After you pass 300-720 SESA:

- You earn the **Cisco Certified Specialist - Email Content Security**
- 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** (300-701 SCOR) exam or its equivalent.

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

Outline

- Describing the Cisco Email Security Appliance
- Administering the Cisco Email Security Appliance
- Controlling Sender and Recipient Domains
- Controlling Spam with Talos SenderBase and Anti-Spam
- Using Anti-Virus and Outbreak Filters
- Using Mail Policies
- Using Content Filters
- Using Message Filters to Enforce Email Policies
- Preventing Data Loss
- Using LDAP
- SMTP Session Authentication
- Email Authentication
- Email Encryption
- Using System Quarantines and Delivery Methods
- Centralized Management Using Clusters

- Testing and Troubleshooting
- References

Target Audience

- Security engineers
- Security administrators
- Security architects
- Operations engineers
- Network engineers
- Network administrators
- Network or security technicians
- Network managers
- System designers
- Cisco integrators and partners

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 Servers (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- Experience with IP routing