SESA

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.

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

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

Course Objectives

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

Course 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+)

The knowledge and skills you are expected to have before attending this training are:

- Transmission control protocol/internet protocol (TCP/IP) services, including domain name system (DNS), secure shell (SSH), file transfer protocol (FTP), simple network management protocol (SNMP), hypertext transfer protocol (HTTP), and hypertext transfer protocol secure (HTTPS)
- Experience with IP routing

Course Outline

1. Describing the Cisco Email Security Appliance
2. Controlling Sender and Recipient Domains
3. Controlling Spam with Talos SenderBase and Anti-Spam
4. Using Anti-Virus and Outbreak Filters
5. Using Mail Polices
6. Using Content Filters
7. Using Message Filters
8. Preventing Data Loss
9. Using LDAP
10. Describing SMTP Session Authentication
11. Using Email Authentication
12. Using Email Encryption
13. Administering the Cisco Email Security Appliance
14. Using System Quarantines and Delivery Methods
15. Centralizing Management Using Clusters
16. Testing and Troubleshooting

Lab Outline

1. Verify and Test Cisco ESA Configuration
2. Advanced Malware in Attachments (Macro Detection)
3. Protect Against Malicious or Undesirable URLs Beneath Shortened URLs
4. Protect Against Malicious or Undesirable URLs Inside Attachments
5. Intelligently Handle Unscannable Messages
6. Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement
7. Integrate Cisco ESA with AMP Console
8. Prevent Threats with Anti-Virus Protection
9. Applying Outbreak Filters
10. Configure Attachment Scanning
11. Configure Outbound Data Loss Prevention
12. Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query
13. Domain Keys Identified Mail (DKIM)
14. Sender Policy Framework (SPF)
15. Forged Email Detection
16. Perform Basic Administration
17. Configure the Cisco Secure Email and Web Manager for Tracking and Reporting