

Securing Email with Cisco Email Security Appliance

Duration: 4 Days **Course Code: SESA** **Version: 3.2** **Delivery Method: Virtual Learning**

Overview:

Learn how to deploy and use Cisco® Email Security Appliance to establish protection for your email systems against phishing, business email compromise and ransomware. 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 is worth 24 Continuing Education (CE) Credits.

Target Audience:

Individuals responsible for the deployment, administration and troubleshooting of a Cisco Email Security Appliance.

Objectives:

- | | |
|--|---|
| <ul style="list-style-type: none"> ■ After completing 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 | <ul style="list-style-type: none"> ■ 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:

Attendees should meet the following prerequisites:

- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
 - Experience with IP routing
- It is recommended that you have one of the following:**
- Cisco certification (Cisco CCNA® 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+)
 - CCNA - Implementing and Administering Cisco Solutions

Testing and Certification

Recommended as preparation for the following exams:

- **300-720 - Securing Email with Cisco Email Security Appliance**
This is one of the concentration exams for the new CCNP Security Certification, to obtain the CCNP Security Certification you will also need to take the 300-701 SCOR exam. Passing the 300-720 exam will also provide you with the Cisco Certified Specialist - Email Content Security Certification.

Content:

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

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

- Cisco Email Security Manager Overview
- Mail Policies Overview
- Handling Incoming and Outgoing Messages Differently
- Configuring Mail Policies
- Matching Users to a Mail Policy
- Message Splintering

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

Using Message Filters

- 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

- 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

Describing 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

Using Email Authentication

- Email Authentication Overview
- Overview of Sender Policy Framework (SPF) and SIDF Verification

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

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

Labs

- Discovery Lab 1: Verify and Test Cisco

- Understanding Text Resources
- Text Resource Management
- Using Text Resources

- Configuring DomainKeys and DomainKeys Identified Mail (DKIM) Signing
- Verifying Incoming Messages Using DKIM
- Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
- Forged Email Detection

Using 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

ESA Configuration

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

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK