Channel Partner Securing Email with Cisco Email Security Appliance

DURATION: 2 DAYS

COURSE OVERVIEW

This course is designed to help learners understand how to install, configure, and manage the Cisco Email Security Appliance in a small to medium-sized business and enterprise installation. Knowledge application and basic troubleshooting skills are reinforced with the use of hands-on-labs.

This course is for Cisco Channel Partners only, end users and partners not looking for Channel Partner accreditation should attend the SESA course

TARGET AUDIENCE

This course is for Channel Partners seeking to acquire knowledge about how to maintain, optimize, and troubleshoot a Cisco Email Security Appliance as well as those Partner's preparing for the Cisco Email Security Field Engineer (#700-280 ESFE) exam

COURSE OBJECTIVES

After you complete this course you should be able to:

1. Install and Administer the Cisco Email Security Appliance
2. Define domain-based Message Authentication
3. Describe the function of web reputation-based filters
4. Understand and configure outbreak filters
5. Control Sender and Recipient Domains
6. Control Spam with Cisco Sensor Base and antispam
7. Understand and configure Cisco Source Fire Advanced Malware Protection integration using file reputation and analysis services
8. Explain how Advanced Malware Protection results may be applied to content filtering
9. Using Mail Policies
10. Using Content Filters
11. Describe URL filtering

12. Configure message filtering to detect high-volume mail attacks
13. Prevent Data Loss
14. Use LDAP
15. Use Authentication and Encryption
16. Create a Clustered Environment

COURSE CONTENT

Reviewing the Cisco ESA

1. Reviewing the Cisco Security Management Appliance
2. Defining an SMTP Conversation
3. Identifying Terms and Definitions
4. Examining the Pipeline
5. Describing Cisco Email Security Appliance Models and Licensing
6. Installing and Verifying the Cisco Email Security Appliance

Performing an Evaluation

1. Describing Cisco Async OS
2. Describing the Listener

Administering the Cisco Email Security Appliance

1. Configuring Localized Message Tracking and Reporting
2. Configuring Centralized Tracking and Reporting
3. Tracking and Reporting Messages
4. Administering the Cisco Email Security Appliance
5. Managing Log Files
6. Creating and Using Administrator Accounts

Controlling Sender and Recipient Domains

1. Configure Public and Private Listeners
2. Describing the Host Access Table (HAT)
3. Describing the Recipient Access Table (RAT)
4. Describing Email Authentication Methods
5. Defining Domain-Based Message Authentication
6. Troubleshooting with Mail Logs

Controlling Spam with Cisco Sensor Base and Antispam

1. Describing Sensor Base

2. Configure Antispam
3. Quarantining Spam on the Cisco Email Security Appliance
4. Describing Safelist and Block list
5. Quarantining Spam on the Cisco Security Management Appliance
6. Configuring Bounce Verification
7. Describing Web Reputation Filters
8. Defining Outbreak Filters

Using Antivirus, Advanced Malware Protection and Virus Outbreak Filters.

1. Enabling Antivirus Engines
2. Using Outbreak Filters
3. Using Advanced Malware Protection

Using Mail Policies

1. Describing Email Security Manager
2. Creating User-Based Mail Policies
3. Using Message Splintering

Using Content Filters

1. Describing Content Filtering
2. Configuring Basic Content Filtering
3. Applying Content Filter Applications
4. Describing and Configuring Message Filtering

Preventing Data Loss

1. Identifying the Data Loss Problem
2. Choosing a Cisco DLP Solution
3. Implementing DLP Configuration
4. Describing the RSA Engine

Using LDAP

1. Describing LDAP Features
2. Describing Query Tokens and Operators
3. Configuring LDAP Profiles
4. Configuring SMTP Call-Ahead
5. Reviewing Case Studies
6. Using LDAP Group Queries

Using Authentication and Encryption

1. Configuring Cisco Registered Envelope Service
2. Describing TLS
3. Authenticating Email with SPF

Clustering

1. Creating a Clustered Environment
2. Joining an Existing Cluster
3. Managing a Clustered Environment
4. Administering a Cluster from the GUI

Labs

1. Hardware Challenge Lab 1: Access the Cisco Remote Lab
2. Hardware Challenge Lab 2: Install Your Cisco Email Security Appliance
3. Hardware Challenge Lab 3: Plan the Cisco Email Security Appliance
4. Hardware Challenge Lab 4: Perform Administration
5. Hardware Challenge Lab 5: Test Your Listener Settings
6. Hardware Challenge Lab 6: Prevent Domain Spoofing with DMARC
7. Hardware Challenge Lab 7: Defend Against Spam with Sensor Base and Antispam
8. Hardware Challenge Lab 8: Defend Against Viruses
9. Hardware Challenge Lab 9: Prevent Advanced Persistent Threats with Advanced Malware Protection
10. Hardware Challenge Lab 10: Customize Mail Policies for Your End Users
11. Hardware Challenge Lab 11: Enforce Your Business Policies in Email Delivery
12. Hardware Challenge Lab 12: Manage High-Volume Mail Flow
13. Hardware Challenge Lab 13: Configure DLP
14. Hardware Challenge Lab 14: Configure LDAP Accept
15. Hardware Challenge Lab 15: Configure SMTP Call-Ahead
16. Hardware Challenge Lab 16: Accommodate Multiple Domains Using LDAP Accept Bypass and Domain Assignments
17. Hardware Challenge Lab 17: Control Mail Policies with LDAP Group Queries
18. Hardware Challenge Lab 18: Configure Envelope Encryption
19. Hardware Challenge Lab 19: Encrypt Email with TLS
20. Hardware Challenge Lab 20: Configure Clusters

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

TCP/IP Fundamentals

Experience with Internet-based messaging, including Simple Mail Transfer Protocol (SMTP), Internet message formats, and Multipurpose Internet Mail Extensions (MIME) **ICND2** Recommended

TEST CERTIFICATION

Recommended Preparation for exam(s):

Cisco Email Security Field Engineer (ESFE) - 700-280

This exam is required for Channel Partners looking to achieve the Express Security - Email Specialization.