SESA (SECURING EMAIL WITH CISCO EMAIL SECURITY APPLIANCE (SESA)) 3.1

Objetivo

After taking this course, you should be able to: â¢ Describe and administer the Cisco Email Security Appliance (ESA) â¢ Control sender and recipient domains â¢ Control spam with Talos SenderBase and anti-spam â¢ Use anti-virus and outbreak filters â¢ Use mail policies â¢ Use content filters â¢ Use message filters to enforce email policies â¢ Prevent data loss â¢ Perform LDAP queries â¢ Authenticate Simple Mail Transfer Protocol (SMTP) sessions â¢ Authenticate email â¢ Encrypt email â¢ Use system quarantines and delivery methods â¢ Perform centralized management using clusters â¢ Test and troubleshoot Prepare for 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.

PÃºblico Alvo

â¢ Security or network professionals seeking knowledge to design, install, configure, operate, and support the Cisco Email Security solution. â¢ Professionals who need to prepare for the Cisco 300-720 certification exam.

PrÃ©-Requisitos

To fully benefit from this course, you should have one or more of the following basic technical competencies: â¢ TCP/IP services, including DNS, SSH, FTP, SNMP, HTTP, and HTTPS; â¢ Experience with IP routing.

Carga HorÃ¡ria

32 horas (4 dias).

ConteÃºdo ProgramÃ¡tico

Course Introduction
Course Outline
Course Goals

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

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

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
Email Security Manager Overview
Mail Policies Overview
Handling Incoming and Outgoing Messages Di?erently
Matching Users to a Mail Policy
Message Splintering
Configuring Mail Policies

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
Understanding Text Resources
Text Resource Management
Using Text Resources

Using Message Filters to Enforce Email Policies
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
Overview of the 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

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

Email Authentication
Email Authentication Overview
Configuring DomainKeys and DomainKeys Identified MailDKIM) Signing
Verifying Incoming Messages Using DKIM
Overview of Sender Policy FrameworkSPF) and SIDF Verification
Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
Forged Email Detection

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

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

Project & Design References
Model Specifications for Large Enterprises
Model Specifications for Midsize Enterprises and Small-to-Midsize Enterprises or Branch
Cisco Email Security Appliance Model Specifications for Virtual Appliances
Packages and Licenses

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