

SESA ((SECURING EMAIL WITH CISCO EMAIL SECURITY APPLIANCE PART 1 AND 2)) 2.0

Objetivo

Securing Email with Cisco Email Security Appliance (SESA) é um curso com carga horária de três dias, que proporciona aos alunos os conhecimentos necessários para instalar, configurar, gerenciar e realizar atividades de suporte ao produto. É curso desenvolvido para capacitação operacional do produto, aliando apresentação do conteúdo teórico, sempre reforçado e associado pela realização de atividades práticas associadas. Após completar este treinamento o aluno estará apto à:

- Descrevendo o Cisco ESA;
- Instalação do Cisco ESA;
- Administrar o Cisco ESA;
- Controlar domínios de remetentes e destinatários;
- Controlar SPAM utilizando as ferramentas Anti-Spam (Incluí SensorBase);
- Utilizar as características Anti-Vírus e “Outbreak Filters”;
- Utilizar Política para controle dos e-mails (Mail Policies);
- Utilizar filtros de conteúdos (Content Filters);
- Utilizar DLP (Data Loss Preventing);
- Integrar com LDAP;
- Utilizar mecanismos de autenticação e criptografia;
- Utilizar filtros de mensagens (Message Filters);
- Utilizar sistema de quarentena e métodos de entrega;
- Entender o mecanismo “Clustering”;
- Realizar processos de suporte.

Público Alvo

O público primário inclui os indivíduos os profissionais que demandam conhecimentos para instalar, operar, prestar suporte e otimizar o produto Cisco ESA.

Pré-Requisitos

Para maior aproveitamento é recomendado que o aluno possua conhecimentos fundamentais no protocolo TCP/IP e experiências na configuração, operação e manutenção de sistemas de correio (email) corporativo (SMTP e MIME).

Carga Horária

24 horas (3 dias).

Conteúdo Programático

- Course Introduction
 - Overview
 - Curso Goal and Objectives
 - Additional References
 - Cisco Glossary of Terms

Module 1: Reviewing the Cisco Email Security Appliance
Reviewing the Cisco Security Management Appliance

- The Cisco Security Management Appliance
- Features and Benefits of the Cisco Security Management Appliance
- Centralized Reporting
- Advanced Message Tracking
- Cisco Security Management Appliance Benefits
- Model Specifications
- Cisco Security Management Appliance Deployment

Defining an SMTP Conversation

- SMTP Conversation Overview
- Example: SMTP Conversation

Identifying Terms and Definitions

- Terms and Definitions

Examining the Pipeline

- Processing Incoming Mail
- Process Outgoing Mail
- The Email Pipeline
- Cisco Email Pipeline

Describing Cisco Email Security Appliance Models and Licensing

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

Installing and Verifying the Cisco Email Security Appliance

- AsyncOS Architecture
- Describing the Listener
- One-Armed Deployment with Private Address
- Multiple Listeners
- Initial Cisco Email Security Appliance Configuration
- NIC Pairing
- Describing VLANs
- Cisco Email Security Appliance Management

Module 2: Administering the Cisco Email Security Appliance

Configuring Localized Message Tracking and Reporting

- Localized Message Tracking and Reporting
- Local Message Tracking
- Using Local Message Tracking
- Search for Email with Message Tracking
- Message Tracking
- Localized Reporting
- Scheduling CSV or PDF Reports via Email
- Change Locale for Web GUI

- Choose Language for Generated Report

Configuring Centralized Tracking and Reporting

- Addressing the Need for Multiple Cisco Email Security Appliances
- Centralizing Reporting and Tracking Data
- Place the Cisco Security Management Appliance in Your Network
- Access Centralized Reporting Data
- DLP Incident Summary
- Report Details on Large Enterprises: Domain-Based Overview Report
- Domain-Based Executive Summary
- Reporting Traffic in a Global Enterprise: Reporting by Appliance Groups
- Report by Appliance Groups
- Message Tracking with Cisco Security Management Appliance

Tracking and Reporting Messages

- Configuring the Cisco Security Management Appliance for Email Applications

Administering the Cisco Email Security Appliance

- System Administration Overview
- Upgrading the System
- Configuring Upgrade Settings
- Suspend and Resume Listeners
- Suspending and Resuming Listeners Using the GUI
- Display System Status over the Web
- Monitor System Status with SNMP
- Monitor System Status with the Web User Interface

Managing Log Files

- Access Logs
- Review Commit Comments in the System Log
- Sample Error Logs

Creating and Using Administrator Accounts

- Predefined Administrative Users
- Administrator Password Controls
- Local User Account and Password Settings Page
- Account Locking
- The Basics of Custom User Roles
- User Role Creation
- Assigning a User to a Role

Module 3: Controlling Sender and Recipient Domains

Configuring Public and Private Listeners

- Public and Private Listeners

Describing the HAT

Objective: Describe the HAT

This lesson includes these topics:

- Classifying Senders in the HAT
- Controlling the SMTP Connection (Two Listeners)
- Controlling the SMTP Connection (One Listener)
- Define Mail Flow Policies for Each Listener
- Sample Mail Flow Policies
- Edit the HAT
- Edit the HAT on the Public Listener
- Edit the HAT on the Private Listener

Describing the RAT

Objective: Describe RAT

This lesson includes these topics:

- Adding New Domains in the RAT
- Adding Internal Domains to the RAT
- SMTP Routes Overview
- Configuring SMTP Routes
- Configure Prioritized SMTP Routes
- Configuring IP Routes

Describing Email Authentication Methods

- DomainKeys and DKIM

- Email Authentication with DomainKeys and DKIM
- Configuring DomainKeys and DKIM
- Enabling DKIM for Mail Flow Policies
- SPF and SIDF Verification
- Enabling SPF and SDIF for Mail Flow Policies
- SPF and SDIF Results in Message and Content Filters

Defining Domain-Based Message Authentication

- What Is DMARC?
- DMARC Verification
- DMARC Resource Records
- DMARC Verification Profiles
- Configuring DMARC Verification Profiles
- Applying DMARC Profiles to Mail Flows
- Configuring DMARC Global Settings
- DMARC Reporting Options
- DMARC Reporting

Troubleshooting with Mail Logs

- Using Debugging Tools
- Troubleshoot with Log Files
- Using Mail Logs

- Tracking Mail Messages with the tail mail_logs Command
- Use the findevent Command
- Use the grep Command

Module 4: Controlling Spam with Cisco SensorBase and Antispam

Describing SensorBase

- Antispam Overview
- SensorBase Network
- Interpret SensorBase Scores
- Reputation Score Ranges per Sender Group (Default)
- Assigning SBRS Ranges per Sender Group

Configuring Antispam

- Controlling Antispam Behavior in the Pipeline
- Spam Analysis by CASE
- Best Practices for Managing Spam
- Configure Mail Policy Spam Settings
- Marketing Message Detection: The Problem
- Detecting and Reporting Marketing Messages
- Detecting and Reporting Spam
- Microsoft Outlook
- Lotus Notes
- Outlook Express 6
- Entourage (Apple Mac)
- Apple Mail.app
- Mozilla Thunderbird
- Netscape Messenger
- Windows Live Mail
- Antispam Best Practices

Quarantining Spam on the Cisco Email Security Appliance

- Configure Spam Quarantine
- Accessing Quarantined Spam on the Cisco Email Security Appliance
- Configuring End-User Authentication
- Configuring Spam Notification Messages

Describing Safelist and Blocklist

- Overview of Safelists and Blocklists
- Configuring Safelists and Blocklists
- End-User List Management
- Safelist and Blocklist Deployment Details
- Use Headers to Track and Test Spam

Quarantining Spam on the Cisco Security Management Appliance

- External Spam Quarantine
- Configure the Spam Quarantine on the Cisco Security Management Appliance
- Accessing the Spam Quarantine

- Configuring the Cisco Security Management Appliance External Spam Quarantine

Configuring Bounce Verification

- Bounce Verification
- Configuring Bounce Verification Address Tagging

Describing Web Reputation Filters

- Web Reputation Applications
- Web Reputation in the Mail Flow
- Antispam Configuration
- Web Reputation Content Filter Conditions
- Web Reputation Content Filter Actions
- Web Reputation Message Filters

Defining Outbreak Filters

- Outbreak Filters
- Configure Outbreak Filters
- Outbreak Filters Applied to Mail Policies
- Outbreak Filter Features
- Customize Outbreak Filters
- Monitor Outbreak Filters
- Monitor Outbreak Quarantines

Module 5: Using Antivirus, Virus Outbreak Filters, and Advanced Malware Protection

Enabling Antivirus Engines

- Antivirus Overview
- Configuring Global Antivirus Settings (Enabling Sophos or McAfee)
- Dual Antivirus Scanning
- Recommended Antivirus Practices
- Configuring Antivirus Behavior on a Mail Policy
- Configuring the Antivirus Settings Page
- Track Virus Activity in the Mail Logs
- Check Logs for Virus Updates
- Control Antivirus Behavior in the Pipeline
- Virus Type Reports

Using Outbreak Filters

- Outbreak Filters Overview
- Outbreak Rules vs. Adaptive Rules
- Taking Action with Outbreak Filters
- Working with Outbreak Filter Updates
- Listing and Updating Outbreak Filter Rules
- Configuring Outbreak Filters for a Mail Policy
- Managing an Outbreak Quarantine
- Creating Outbreak Reports

Using Advanced Malware Protection

- Cisco SourceFire Advanced Malware Protection
- Advanced Malware Protection Enhances Cisco Email Security
- Cisco Zero-Hour Malware Protection
- File Reputation and Analysis
- File Processing Overview
- Enabling Advanced Malware Protection
- File Reputation and Analysis Settings
- Advanced Malware Protection Mail Policy
- File Analysis and Reputation Results as Conditions
- Monitor Advanced Malware Protection

Module 6: Using Mail Policies

Describing Email Security Manager

- Email Security Manager Overview
- Email Security Manager
- Mail Policies Overview
- Separate Incoming and Outgoing Mail Policies
- Match on Different Users with Mail Policies

Creating User-Based Mail Policies :

- Define User-Based Policies
- Mail Policies Determine What Happens to Mail Messages
- Use Email Security Manager to Maintain Mail Policies
- Matching Users to a Policy
- Build Mail Policies by Changing Defaults

Using Message Splintering

- Message Splintering Concepts
- Track Splintered Messages
- Finding Messages in Policy, Virus, and Outbreak Quarantines
- Mail Policy Matching Exercise
- Order of Mail Policies Make a Difference

Module 7: Using Content Filters

Describing Content Filtering

- Use Content Filters
- Planning Your Content Filter Deployment

Configuring Basic Content Filtering

- Looking for Confidential Content in Outgoing Mail
- Creating a Content Filter
- Choosing Conditions and Actions
- Applying the Content Filter to a Mail Policy
- Testing with the Trace Tool

Applying Content Filter Applications

- Match on File Analysis by Advanced Malware Protection
- Match on File Attachments
- Detect Password-Protected Attachments
- Using Image Analysis
- Apply Content Dictionaries
- Give Weights to Dictionary Terms
- Import a Dictionary
- Editing the Imported Dictionary
- Apply the Dictionary with a Filter
- Track Matched Content
- Applying Content Dictionaries
- Remove Attachments with Keywords
- Detect High-Volume Mail Attacks

Describing and Configuring Message Filtering

- URL Filtering Applications
- URL Filtering Using Content Conditions
- Content Filter Actions
- URL Filtering Used with Message Filters

Module 8: Preventing Data Loss

Identifying the Data Loss Problem

- Intellectual Property Leakage
- Protect Sensitive Data

Choosing a Cisco DLP Solution

- DLP Is Applied in Outgoing Mail Policies
- Identify DLP Violations
- List of International ID Numbers Covered in DLP

Implementing DLP Configuration

- Enable the DLP Feature
- Enabling DLP Policies
- Add a DLP Template from the Category
- Configure DLP Actions
- Configuring DLP Policy Customization
- Configuring Secondary Actions of DLP Policy
- Enable DLP in Outgoing Mail Policies
- DLP Is Tracked in the Mail Logs
- Troubleshoot with Trace

Describing the RSA Engine

- In-Depth Analysis
- Weighted Scores

- Accurate Classifiers
- DLP Message Scanning Flow
- Severity Ratings

Module 9: Using LDAP

Describing LDAP Features

- LDAP Overview
- Attributes of LDAP Directories
- LDAP Uses a Hierarchical Namespace
- Using LDAP to Check Recipients
- LDAP and the Pipeline

Describing Query Tokens and Operators

- Using Query Tokens and Operators
- Running the Active Directory Wizard
- Configuring Active Directory and Other LDAP Profiles

Configuring LDAP Profiles

- Configuring an LDAP Server Profile
- Complete Server Setup
- Enabling the Accept Query on a Listener
- Preventing Harvest Attacks

Configuring SMTP Call-Ahead

- SMTP Call-Ahead
- Order of Recipient Validation
- SMTP Call-Ahead Profiles
- SMTP Call-Ahead Configuration
- Assign a Call-Ahead Profile to a Listener
- CLI Test

Reviewing Case Studies

- University Case Study: ABC University
- ABC University: Single Directory
- Accommodating Domains Not in the Directory
- Accommodating for Multiple Directories
- Option A: Separate Listeners
- Option B: Single Listener with Domain Assignments
- Configuring Domain Assignments
- Accommodating Multiple Directories in One Domain
- Configuring a Chained Query
- Review: What to Configure If...
- Routing (Aliasing)
- Masquerading

Using LDAP Group Queries

- Using Group Queries for Routing
- Using LDAP Group Queries
- LDAP and the Pipeline
- Using Group Queries for Routing: Example
- Configuring LDAP Group Queries
- Configuring Group Queries for Routing
- Review Questions

Module 10: Using Authentication and Encryption

Configuring Cisco Registered Envelope Service

- Overview of Cisco Registered Envelope Service
- Registering a Recipient with Cisco Registered Envelope Service
- Recipient Receives a Notification Message with Encrypted HTML File
- Setting Up Email Encryption
- Enabling Email Encryption
- Configuring the Encryption Profile: Key Server Settings
- Configuring the Encryption Profile: Envelope Settings
- Configuring the Encryption Profile: Message and Notification
- Committing Your Changes
- Provisioning the Profile with Cisco Registered Envelope Service
- Initiating Encryption with Content Filters
- Defining the Encrypt Condition
- Defining the Encrypt Action
- No Auth Envelope: Encryption
- Multiple Cisco Registered Envelope Service Profiles
- Encrypt on Quarantine Exit
- Controlling Encryption Settings with SMTP Headers
- Guaranteed Secure Delivery
- Guaranteed Secure Delivery When Used with Secure Envelopes
- Outgoing Content Filter Controls Use of TLS
- Verifying TLS Failover in mail_logs

Describing TLS

- TLS Overview
- Certificate Management Overview
- Configuring TLS on Your Appliance
- Certificate Management
- Certificate Profile Creation
- Certificate Profile Management
- Creating a New Certificate Profile via CLI
- Certificate Profile Usage
- Certificate Authority Management
- CA Usage

- Updating a List of Revoked Certificates
- Choosing TLS Server Settings in the HAT
- Enabling Server TLS in Mail Flow Policies
- Choosing TLS Client Settings
- Enabling Client TLS in Destination Controls
- Outbound TLS Troubleshooting
- Verifying the TLS Connection in mail_logs
- Viewing Reports on TLS Connections

Authenticating Email with SPF

- Authentication Problems
- SPF and SIDF Authentication Features
- Email Fields that Are Checked by SPF and SIDF
- SPF Record Example
- SPF and SIDF Verification
- Implementing SPF
- Enabling SPF and SIDF in the HAT
- Checking Verified Mail with Content Filters
- Testing SPF and SIDF Results

Module 11: Using Message Filters

Identifying Message Filters

- Message Filters Overview
- How Message Filters Work
- Message Filter Benefits
- Create Filters with the CLI

Describing Regular Expression Basics

- Filter Basics: Label
- Filter Basics: Rule
- Filter Basics: Action
- Example: Using the Filter Rule
- Example: Using the Filter Action
- Final Actions
- Message Filters at Work
- Message Filters at Work Redux
- Using Regular Expressions for Filtering
- Regular Expressions with Operators
- Regular Expression Basics
- Regular Expression Resources
- Common Filters: Frequent Things to Match
- Common Filters: Frequent Things to Do
- Common Filters: Selective Actions

Applying Message Filters

- Removing Encryption Tags
- Removing the Encryption Tag with Message Filters

- Changing Your Content Filter to Encrypt on an X-Header
- Using Encryption Configuration Options
- Action Variable Quick Reference
- Common Filters: More Examples
- Attachment Scanning in Action
- Attachment Filtering Variables
- Filters for Everyday Use: Attachment Checking and Blocking
- Using the scanconfig Command to Control Attachment Type Options
- Debugging Filters: Use Quarantines to Verify Filters
- Inactive and Invalid Filters
- Managing Filters: Order
- Managing Filters: Import and Export

Module 12: Using System Quarantines and Delivery Methods

Describing Quarantines

- Types of Quarantines
- AsyncOS Features that Quarantine
- System Quarantine Defaults
- Maximum Space, Rights, and Defaults Table
- Describing System Quarantines as One
- Creating Custom System Quarantines (Space Reallocation)
- Accessing System Quarantined Contents

Describing Policy, Virus, and Outbreak Quarantines

- Benefits of Centralized Policy, Virus, and Outbreak Quarantines
- Migration of Policy, Virus, and Outbreak Quarantines

Setting Delivery Limits

- Listeners (SMTP Receivers) Are Not SMTP Delivery Clients
- Configuring Destination Controls

Creating Virtual Gateways

- Configuring Multiple SMTP Identities
- Configuring Virtual Gateways
- Configuring Virtual Gateways: altsrchoost Command
- Configuring Virtual Gateways: Content Filters
- Verifying Virtual Gateway Operation

Configuring Bounce Profiles

- Default Bounce Profile
- Applying the Bounce Profile to a Listener

Module 13: Understanding Clustering

Creating a Clustered Environment

- Cluster Topology
- Setting Up Clustering

- Checking Required Features
- Creating a New Cluster

Joining an Existing Cluster

- Joining an Existing Cluster
- Joining an Existing Cluster over SSH

Managing a Clustered Environment

- Centralized Management Overview
- Managing the Cluster from Any Machine

Administering a Cluster from the GUI

- Centralized Management Feature in the GUI
- Creating New Settings
- Centralized Management Best Practices

Module 14: Troubleshooting

Identifying Appliance-Related Problems

- Troubleshooting Overview
- Types of Troubleshooting Methods
- Categories of Appliance Faults

Lesson 2: Monitoring the System

- Monitoring Overview
- Configuring Alerts in the User Interface
- Subscribing to Alerts
- Examples of DNS and FTP Alerts
- Configuring TLS Alerts
- Backup Log Files

Diagnosing Problems

- Debugging DNS Problems
- diagnostic Command
- CLI Troubleshooting Tools
- Isolating the Problem
- Diagnosing Network Problems
- Diagnosing Listener Problems
- Diagnosing Work Queue Problems
- Diagnosing Delivery Problems

Locating Common Problems and Solutions

- Observing System Status
- Monitoring Outbound Connections
- Displaying Real-Time Activity
- Troubleshooting TCP/IP Packets

- Problem: Sender Outside.com Cannot Send Mail to You; Use the findevent Command
- Problem: Connection from Sender Outside.com Is Unexpectedly Closed
- Problem: Connection from Sender Is Unexpectedly Closed; Use Injection Debug
- Problem: Incoming Mail Fails; Check Injection Debug Log
- Problem: Example.org Is Not Receiving Your Mail; Check Counters and Gauges
- Problem: Example.com Is Not Receiving Your Mail; Check mail_logs
- Cisco Support

Laboratórios

- Lab 1: Access the Cisco Remote Lab
- Lab 2: Install Your Cisco Email Security Appliance
- Lab 3: Perform Administration
- Lab 4: Test Your Listener Settings
- Lab 5: Prevent Domain Spoofing with DMARC
- Lab 6: Defend Against Spam with SensorBase and Antispam
- Lab 7: Defend Against Viruses
- Lab 8: Prevent Advanced Persistent Threats with Advanced Malware Protection
- Lab 9: Customize Mail Policies for Your End Users
- Lab 10: Enforce Your Business Policies in Email Delivery
- Lab 11: Manage High-Volume Mail Flow
- Lab 12: Configure DLP
- Lab 13: Configure LDAP Accept
- Lab 14: Configure SMTP Call-Ahead
- Lab 15: Accommodate Multiple Domains Using LDAP Accept Bypass and Domain Assignments
- Lab 16: Control Mail Policies with LDAP Group Queries
- Lab 17: Configure Envelope Encryption
- Lab 18: Encrypt Email with TLS
- Lab 19: Verify SIDF and SPF
- Lab 20: Redirect Mail with Message Filters
- Lab 21: Configure Virtual Gateways
- Lab 22: Configure Clusters
- Lab 23: Troubleshoot