Objetivos

After taking 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 to enforce email policies
- 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

_____

Pre-requisitos

To fully benefit from this course, you should have one or more of the following basic technical competencies:

- Cisco certification (Cisco CCENT® 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+)

The knowledge and skills that a student must have before attending this course are:

Centro de Transferencia de Tecnología
2700215 / 591-79671047
eriveros@cttbolivia.com

P á g. 1 | 7

- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- Experience with IP routing

_____

Contenido

- Describing the Cisco Email Security Appliance
    - o Cisco Email Security Appliance Overview
    - o Technology Use Case
    - o Cisco Email Security Appliance Data Sheet
    - o SMTP Overview
    - o Email Pipeline Overview
    - o Installation Scenarios
    - o Initial Cisco Email Security Appliance Configuration
    - o Centralizing Services on a Cisco Content Security Management Appliance (SMA)
    - o Release Notes for AsyncOS 11.x
- Administering the Cisco Email Security Appliance
    - o Distributing Administrative Tasks
    - o System Administration
    - o Managing and Monitoring Using the Command Line Interface (CLI)
    - o Other Tasks in the GUI
    - o Advanced Network Configuration
    - o Using Email Security Monitor
    - o Tracking Messages
    - o Logging
- Controlling Sender and Recipient Domains
    - o Public and Private Listeners
    - o Configuring the Gateway to Receive Email
    - o Host Access Table Overview
    - o Recipient Access Table Overview
    - o Configuring Routing and Delivery Features
- Controlling Spam with Talos SenderBase and Anti-Spam
    - o SenderBase Overview

Centro de Transferencia de Tecnología
2700215 / 591-79671047
eriveros@cttbolivia.com

CTT

Pág. 2 | 7

- o Anti-Spam

- o Managing Graymail

- o Protecting Against Malicious or Undesirable URLs

- o File Reputation Filtering and File Analysis

- o Bounce Verification

- Using Anti-Virus and Outbreak Filters

  - o Anti-Virus Scanning Overview

  - o Sophos Anti-Virus Filtering

  - o McAfee Anti-Virus Filtering

  - o Configuring the Appliance to Scan for Viruses

  - o Outbreak Filters

  - o How the Outbreak Filters Feature Works

  - o Managing Outbreak Filters

- Using Mail Policies

  - o Email Security Manager Overview

  - o Mail Policies Overview

  - o Handling Incoming and Outgoing Messages Differently

  - o Matching Users to a Mail Policy

  - o Message Splintering

  - o Configuring Mail Policies

- Using Content Filters

  - o Content Filters Overview

  - o Content Filter Conditions

  - o Content Filter Actions

  - o Filter Messages Based on Content

  - o Text Resources Overview

  - o Using and Testing the Content Dictionaries Filter Rules

  - o Understanding Text Resources

  - o Text Resource Management

  - o Using Text Resources

- Using Message Filters to Enforce Email Policies

  - o Message Filters Overview

  - o Components of a Message Filter

  - o Message Filter Processing

Centro de Transferencia de Tecnología
2700215 / 591-79671047
eriveros@cttbolivia.com

CTE

CTT

Pág. 3 | 7

- o Message Filter Rules
- o Message Filter Actions
- o Attachment Scanning
- o Examples of Attachment Scanning Message Filters
- o Using the CLI to Manage Message Filters
- o Message Filter Examples
- o Configuring Scan Behavior

- Preventing Data Loss
  - o Overview of the Data Loss Prevention (DLP) Scanning Process
  - o Setting Up Data Loss Prevention
  - o Policies for Data Loss Prevention
  - o Message Actions
  - o Updating the DLP Engine and Content Matching Classifiers

- Using LDAP
  - o Overview of LDAP
  - o Working with LDAP
  - o Using LDAP Queries
  - o Authenticating End-Users of the Spam Quarantine
  - o Configuring External LDAP Authentication for Users
  - o Testing Servers and Queries
  - o Using LDAP for Directory Harvest Attack Prevention
  - o Spam Quarantine Alias Consolidation Queries
  - o Validating Recipients Using an SMTP Server

- SMTP Session Authentication
  - o Configuring AsyncOS for SMTP Authentication
  - o Authenticating SMTP Sessions Using Client Certificates
  - o Checking the Validity of a Client Certificate
  - o Authenticating User Using LDAP Directory
  - o Authenticating SMTP Connection Over Transport Layer Security (TLS) Using a Client Certificate
  - o Establishing a TLS Connection from the Appliance
  - o Updating a List of Revoked Certificates

- Email Authentication
  - o Email Authentication Overview
  - o Configuring DomainKeys and DomainKeys Identified Mail (DKIM) Signing

Centro de Transferencia de Tecnología
2700215 / 591-79671047
eriveros@cttbolivia.com

CTT

P á g . 4 | 7

- o Verifying Incoming Messages Using DKIM
- o Overview of Sender Policy Framework (SPF) and SIDF Verification
- o Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
- o Forged Email Detection
- Email Encryption
  - o Overview of Cisco Email Encryption
  - o Encrypting Messages
  - o Determining Which Messages to Encrypt
  - o Inserting Encryption Headers into Messages
  - o Encrypting Communication with Other Message Transfer Agents (MTAs)
  - o Working with Certificates
  - o Managing Lists of Certificate Authorities
  - o Enabling TLS on a Listener's Host Access Table (HAT)
  - o Enabling TLS and Certificate Verification on Delivery
  - o Secure/Multipurpose Internet Mail Extensions (S/MIME) Security Services
- Using System Quarantines and Delivery Methods
  - o Describing Quarantines
  - o Spam Quarantine
  - o Setting Up the Centralized Spam Quarantine
  - o Using Safelists and Blocklists to Control Email Delivery Based on Sender
  - o Configuring Spam Management Features for End Users
  - o Managing Messages in the Spam Quarantine
  - o Policy, Virus, and Outbreak Quarantines
  - o Managing Policy, Virus, and Outbreak Quarantines
  - o Working with Messages in Policy, Virus, or Outbreak Quarantines
  - o Delivery Methods
- Centralized Management Using Clusters
  - o Overview of Centralized Management Using Clusters
  - o Cluster Organization
  - o Creating and Joining a Cluster
  - o Managing Clusters
  - o Cluster Communication
  - o Loading a Configuration in Clustered Appliances
  - o Best Practices

Centro de Transferencia de Tecnología
2700215 / 591-79671047
eriveros@cttbolivia.com

CTT

P á g . 5 | 7

- Testing and Troubleshooting
  - o Debugging Mail Flow Using Test Messages: Trace
  - o Using the Listener to Test the Appliance
  - o Troubleshooting the Network
  - o Troubleshooting the Listener
  - o Troubleshooting Email Delivery
  - o Troubleshooting Performance
  - o Web Interface Appearance and Rendering Issues
  - o Responding to Alerts
  - o Troubleshooting Hardware Issues
  - o Working with Technical Support
- References
  - o Model Specifications for Large Enterprises
  - o Model Specifications for Midsize Enterprises and Small-to-Midsize Enterprises or Branch Offices
  - o Cisco Email Security Appliance Model Specifications for Virtual Appliances
  - o Packages and Licenses

Laboratorio

- Verify and Test Cisco ESA Configuration
- Perform Basic Administration
- Advanced Malware in Attachments (Macro Detection)
- Protect Against Malicious or Undesirable URLs Beneath Shortened URLs
- Protect Against Malicious or Undesirable URLs Inside Attachments
- Intelligently Handle Unscannable Messages
- Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement
- Integrate Cisco ESA with AMP Console
- Prevent Threats with Anti-Virus Protection
- Applying Content and Outbreak Filters
- Configure Attachment Scanning
- Configure Outbound Data Loss Prevention
- Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query
- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)

Centro de Transferencia de Tecnología
2700215 / 591-79671047
eriveros@cttbolivia.com

CTT

Pág. 6 | 7

- Forged Email Detection
- Configure the Cisco SMA for Tracking and Reporting

_____

Centro de Transferencia de Tecnología
2700215 / 591-79671047
eriveros@cttbolivia.com

P á g . 7 | 7