

# PASESA (CHANNEL PARTNER SECURING EMAIL WITH CISCO EMAIL SECURITY APPLIANCE) 2.x

## Objetivo

Channel Partner Securing Email with Cisco Email Security Appliance (PASESA) 2.x é um curso com carga horária de dois dias (16 horas), para capacitar os participantes nas atividades de instalação, configuração, administração e suporte no produto ESA (Email Security Appliance), com aplicação em projetos abrangendo desde redes pequenas (Small-Business) até as de médio porte. Após completar este treinamento o aluno estará apto à:

- Descrever o produto Cisco ESA;
- Instalar o produto Cisco ESA;
- Administrando o produto Cisco ESA;
- Controlar o domínio de remetentes e destinatários;
- Controlar SPAM, com os recursos Cisco SensorBase e AntiSpam;
- Usar os recursos Anti-Vírus e "Outbreak Filters";
- Estabelecer as políticas de email;
- Usar os recursos para filtragem de conteúdos;
- Usar os recursos de DLP (Data Loss Prevention);
- Integração com LDAP;
- Utilizar autenticação e criptografia;
- Descrever uma solução "Clustering".

## Público Alvo

O público primário são os profissionais de canais parceiros Cisco que demandam conhecimentos para instalar, operar, administrar e realizar suporte em uma solução Cisco ESA. Esse curso também é indicado para a preparação dos engenheiro de campo (Field Engineers) de canais parceiros Cisco na realização do exame de certificação (650-153 ESFE).

## Pré-Requisitos

Para maior aproveitamento é recomendado que o aluno tenha conhecimentos básicos do modelo TCP/IP, e desejável experiência em administração e suporte de sistemas de correio eletrônico (email), com o protocolo SMTP e extensões MIME (Multipurpose Internet Mail Extensions) para formatos de mensagens.

## Carga Horária

16 horas (2 dias).

## Conteúdo Programático

- Course Introduction
  - Overview
  - Course Goal and Objectives
  - Course Flow
  - Additional References
  - Your Training Curriculum

Reviewing the Cisco ESA

- Cisco Security Management Appliance (SMA)
- SMTP conversation
- Terms and definitions
- Pipeline
- Licensing

#### Performing and Evaluating

- Various scenarios based on a lab topology design and implement the Cisco ESA.

#### Installing the Cisco ESA

- System architecture
- Concept of the listener
- Various network topologies
- Instructor will demonstrate the installation of both the Cisco ESA and Cisco SMA

#### Administering the Cisco ESA

- Create and customize reports
- Use message tracking
- Administer the Cisco ESA, including the following actions:
  - Shutdown
  - Reboot
  - Suspend
  - Upgrade
  - Rollback
- Manage log files using FTP
- Create and use administrator accounts
- Instructor will demonstrate the Cisco ESA by connecting to the Cisco SMA for centralized tracking and reporting.

#### Controlling Sender and Recipient Domains

- Explain the differences between the Host Access Table (HAT) and the Recipient Access Table (RAT)

#### Controlling Spam with Cisco SensorBase and Antispam

- Discuss Cisco SensorBase and the antispam engine
- Make adjustments to the HAT and the antispam policies
- Manage the spam quarantine both locally or using the Cisco SMA
- Instructor will demonstrate configuring spam quarantine from the Cisco ESA to the Cisco SMA

#### Using Antivirus and Outbreak Filters

- Compare the two signature-based antivirus engines with outbreak filters
- Configure antivirus and outbreak filter policies
- Adjust antivirus and outbreak filter policies

#### Using Mail Policies

- Separate enterprise groups with different filtering requirements.

#### Using Content Filters

- Content filters

- How to apply filters to policies
- The use of filters to match specific words in message bodies and attachments
- Dictionaries, footers, and best practices

#### Preventing Data Loss

- Describe the RSA data loss prevention (DLP) engine
- Prevent the loss of sensitive data in outbound email through the use of the RSA DLP engine

#### Using LDAP

- Configure LDAP to control the flow of email
- Configure LDAP to enforce user access policies

#### Using Authentication and Encryption

- Configure Transport Layer Security (TLS) to encrypt email
- Configure the Cisco ESA to work with Cisco Registered Envelope Service (RES) to encrypt mail
- Use Sender Policy Framework (SPF) to authenticate email

#### Clustering

- Create a clustered environment
- Manage a clustered environment

#### Laboratórios

- Lab 1-1: Access Lab
- Lab 2-1: Plan the Cisco Email Security Appliance
- Lab 3-1: Install Your Cisco Email Security Appliance
- Lab 4-1: Perform Administration
- Lab 5-1: Test Your Listener Settings
- Lab 6-1: Defending Against Spam with SensorBase and Antispam
- Lab 7-1: Defend Against Viruses
- Lab 8-1: Customize Mail Policies for Your End Users
- Lab 9-1: Enforce Your Business Policies in Email Delivery
- Lab 10-1: Configure DLP
- Lab 11-1: Configure LDAP Accept
- Lab 11-2: Configure SMTP Call-Ahead
- Lab 11-3: Accommodate Multiple Domains Using LDAP Accept Bypass and Domain Assignments
- Lab 11-4: Control Mail Policies with LDAP Group Queries
- Lab 12-1: Configure Envelope Encryption
- Lab 12-2: Encrypt Email with TLS
- Lab 13-1: Configure Clusters