Securing Email with Cisco Email Security Appliance (SESA) – e-Learning

Cisco

- **Nível:** Avançado
- **Duração:** h

Sobre o curso

This course shows you how to deploy and use Cisco Email Security Appliance to establish protection for your email systems against phishing, business email compromise, and ransomware, and to help streamline email security policy management.

This hands-on course provides you with the knowledge and skills to implement, troubleshoot, and administer Cisco Email Security Appliance, including key capabilities such as advanced malware protection, spam blocking, anti-virus protection, outbreak filtering, encryption, quarantines, and data loss prevention.

This course helps prepare you for the Securing Email with Cisco Email Security Appliance (300-720 SESA) exam, which leads to CCNP Security and the Certified Specialist – Email Content Security certifications.

Certification

- Associated Certification: CCNP Security
- Associated Exam:300-720 SESA

This course includes

- Access duration: 180 days
- Labs
- Self-paced training
- Video training
- Continuing Education Credits: 24

This course is also available in an Instructor-Led Training (ILT) format. For more information, select this link: Securing Email with Cisco Email Security Appliance (SESA)

Destinatários

- Security engineers
- Security administrators
- Security architects
- Operations engineers
- Network engineers
- Network administrators
- Network or security technicians
- Network managers
- System designers
- Cisco integrators and partners

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 Cisco 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 Lightweight Directory Access Protocol (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

Pré-requisitos

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

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

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 [International Information System Security Certification Consortium ((ISC)^2), Computing Technology Industry Association (CompTIA) Security+, International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), 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+)