Securing Email with Cisco Email Security Appliance (SESA)

Seminar	Zurzeit keine Termine	Teilnahmebescheinigung
Präsenz	24 Unterrichtseinheiten	

Seminarnummer: 25277 | Herstellernummer: CI-SESA

Stand: 09.05.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/25277

Dieser Kurs bereitet Sie auf die Installation, Konfiguration, den Betrieb, die Wartung und die grundlegende Fehlerbehebung der Cisco Email Security Appliance (ESA) vor.

Nutzen

Securing Email with Cisco Email Security Appliance (SESA) combines Parts 1 and 2 (SESA1, SESA2) into a single three-day course. Students learn to use Cisco Email Security Appliances (ESA's) to manage and troubleshoot email in their networks. Attendees receive in-depth instruction on popular features, emphasizing topics listed below, learn advanced Internet email concepts and receive an of how to customize configurations. SESA also teaches advanced configuration and operation of the Cisco ESA (Formerly Cisco IronPort Email Security Appliance). Extensive lab exercises provide critical hands-on experience with advanced features of the ESA. This course prepares students for successful configuration and operation of an Email Security Appliance. Exploring specific features, mail administrators will receive training with emphasis on:

- Administering with best practices for configuration and operation.
- Managing, monitoring, and troubleshooting email flowing through an ESA.
- Configuring access control policies, eliminating threats at the perimeter, based on the identity and trustworthiness of the sender.
- Creating and apply Data Loss Prevention (DLP) polices to outgoing email.
- Configuring Email Security Appliances to detect and handle unwanted spam and viruses.
- Using Message Tracking and Reporting to document email traffic trends.
- Managing spam quarantines.
- Using Cisco reputation-based services, SensorBase and Virus Outbreak Filters, to increase the security of an email network.
- Integrating an ESA with a directory server via LDAP
- Debugging LDAP integration issues
- Using message filters to redirect and modify messages
- Performing safe deployment and debugging of message filters

- Configuring TLS and Guaranteed Secure Delivery

Configuring Email Authentication with DKIM and SPF

Zielgruppe

Enterprise messaging managers and system administrators Email system designers and architects Network managers responsible for messaging implementation

Voraussetzungen

It is assumed that attendees possess the following background knowledge and skills:

- A moderate knowledge of TCP / IP fundamentals, including IP addressing and sub-netting, static IP routing and DNS.
- Experience with Internet-based messaging, including SMTP, Internet message formats, and MIME message format.
- Familiarity with command line interface (CLI) and graphical user interface (GUI).
- Previous experience with email security would be helpful.

Inhalte des Seminars

- Day One Agenda

Module 1 Introduction & System Overview

Module 2 Tracking and Reporting Messages

Module 3 Controlling Sender & Recipient Domains

Module 4 Controlling Spam with SensorBase & Anti-Spam

Module 5 Using Anti-Virus & Virus Outbreak Filters

- Day Two Agenda

Module 6 Using Mail Policies to Direct Business Email

Module 7 Using System Quarantines and Delivery Methods

Module 8 Using Content Filters for Specific Business Needs

Module 9 Preventing Data Loss

Module 10 Encrypting Outbound Email

Module 11 Troubleshooting

Module 12 System Administration
- Day Three Agenda

Module 13: Configuring LDAP Queries

Module 14: Configuring Message Filters

Module 15: Configuring TLS

Module 16: Authenticating Email

Appendix: Routing and Masquerading

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/25277 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.