Forcepoint Email Security Administrator Virtual Instructor-Led Training

Datasheet

February 2022

Forcepoint

forcepoint.com

Forcepoint Email Security Administrator Virtual Instructor-Led Training

In this course, you will learn the features, components, and key integrations that enable Forcepoint Email Security functionalities; how to administer policies, handle incidents, upgrade, manage and assess the health of the Forcepoint Email Security system. You will develop skills in creating email policies, configure email encryption, incident management, reporting, and system architecture and maintenance.

Audience

- System administrators, network security administrators, IT staff
- Sales engineers, consultants, implementation specialists
- Forcepoint Channel Partners

Format:

Instructor-led training (Virtual training)

Duration:

3 days (12 hours), typically delivered in 3 sessions (4 hours per session), plus any additional homework each session, if necessary.

Exam Price:

One attempt is included

Course objectives

- Describe the key capabilities of Forcepoint Email Security.
- Understand the required product hardware and add-on components.
- Understand multiple deployment scenarios.
- Perform initial setup functions of Email Security.
- Define connection level controls and secure message controls.
- Configure user account authentication activities.
- Create antispam email policies to control inbound email traffic.
- Configure traffic management with various block/permit lists and manage message quarantines.
- Demonstrate how to configure email DLP policies, rules, and actions.
- Configure and customize PEM portal.
- Activate email and transport layer encryption methods.
- Schedule, run, and interpret reports and configure message logs.
- Describe how to perform appliance system upgrades and disaster recovery procedures

Prerequisites for attendance

- General understanding of system administration and Internet services.
- Basic knowledge of networking and computer security concepts.
- A computer that meets the requirements noted at the end of this document.

Certification exam

This course prepares you to take and pass the Forcepoint Email Security Administrator Certification exam. One exam attempt is included in the price of the course, but the execution of the exam is not accomplished during the course. A minimum score of 80% on the multiple-choice online exam is required to pass.

Course Outline

Module 1: Features & Components

1. Forcepoint solution overview

- Summarize the Forcepoint Email solution including key and new features.

2. Understanding the deployment solution

- Articulate Email Security key benefits and differentiators from other email security products.
- Describe the Email Security hardware platform and virtualization options.
- Identify the appropriate installation method and sizing requirements to follow.
- Describe the components of Email Security and its supported platforms.
- Administer the appliance management tools.

3. Understanding the Product Deployment

- Describe a high-level overview of email delivery with the security appliance.
- Plan for appliance and email server network integration.
- Configure physical and/or virtual appliance settings and plan for network host name and routing.
- Review and configure appliance internal daemons.
- Identify and configure Communication Points with external services.
- Review planned hardware resources and user loads.

4. Getting started with Forcepoint Email Security

- Describe fundamental Email Security concepts and system usage models.
- Setup the Email Security system and review First Boot procedures.
- Customize the Forcepoint Manager Console and integrate the Email module.
- Complete initial V-Series appliance configuration and install the Manager Console.

5. Setting up users and defining email routing

- Configure user directories and customized user groups.
- Describe Domain Group integration with Active Directory server.
- Define user directories for authentication within a domain.
- Define a user directory filter for specific users and groups.
- Direct outbound emails to Email Security via Smart Host.
- Verify outbound email delivery to remote recipients.

Module 2: Traffic & Policies

6. Managing Traffic - Antispam Related Configurations

- Explain the pre-filtering concept and Bulk Email Elimination tools.
- Describe the message processing flow for an SMTP system.
- Create a global IP block list and edit the trusted host list.
- Configure the usage model for the real-time block list and reputation service checks.
- Integrate Reverse DNS Lookup and Sender Policy Framework checks.
- Verify Recipient Validation and implement Directory Harvest Attack prevention.
- Determine whether SMTP authentication is a suitable resource for your organization.
- Compare the trusted IP group and the Allow Access list.

7. Managing Traffic – Advanced Configurations

- Identify supported SMTP port usage for appliance and hybrid modes.
- Configure the IP Address Group for trusted and allowed systems.
- Enable SMTP VRFY command on the test system.
- Explain how a system administrator manages the Message Quarantine.
- Describe the differences in permissions between Trusted IP and the Allow Access List.
- Enable and monitor the Appliance Quarantine system.
- Enable the Archive queue and move it to a remote SAMBA share.

8. Configuring Email Security Policies

- Explain how email policy flow, types, and conditions affect message flow.
- Describe how policies combine rules, filters, and actions in the Email Security appliance.
- Configure default action types and options.
- Configure the integration and merging of Message Action options.
- Integrate Data Loss Prevention (DLP) tools with the Email Security appliance.
- Configure the Global IP and Global Address permit lists.
- Verify policy behavior with the test message generation tool.
- Configure the Email Security Antivirus and Antispam policy and verify detection.
- Configure the Email Data Loss Prevention (DLP) action and policy rules.
- Confirm Email DLP functionality with a test message capture and log reviews.

Module 3: PEM & Advanced Configurations & Maintenance

9. Personal Email Manager (PEM) operations

- Describe Personal Email Manager (PEM) architecture and use cases.
- Configure the PEM portal and complete PEM configurations.
- Describe administrator vs. end user PEM and quarantine activities.
- Customize the PEM notification message and schedule.
- Differentiate between personal and global address block/permit lists.
- Perform advanced PEM configuration for key user accounts.
- Manage multiple mailboxes within the PEM portal.

10. Traffic shaping and threat protection

- Configure the Email sandbox module and test its performance on test messages.
- Analyze how Secure Message Delivery and Transport Layer Security increase message security.
- Identify traffic shaping parameters and customize URL Sandbox solutions.
- Configure Threat Protection Cloud.
- Identify the five parameters of traffic shaping and how they function.

11. Transfer Layer Security (TLS)

- Configure Secure Message Delivery for Email and DLP modules.
- Verify Secure Message Delivery via Secure Portal message pickup.
- Describe the Secure Message Delivery end user experience for an external recipient.
- Differentiate enforced/mandatory TLS from opportunistic TLS.
- Enable enforced TLS for incoming/outgoing connections.
- Enforce TLS security level and encryption strength.
- Describe the TLS certification process.
- Enable mandatory TLS and opportunistic TLS.

12. Email Security Reporting and Maintenance

- Describe the overall requirements for Log Database rollover and maintenance.
- Identify how dashboard tools, health alerts, and logs indicate appliance performance.
- Activate and customize the Email Security real-time monitor.
- Manage the Presentation reports and the Reporting Engine tools.
- Explore the Log Server architecture and the Database Partition rollover and deployment.

To attend this virtual online course, you must have a computer with:

- *A high-speed internet connection (minimum of 1 MB connection required)*
- *An up-to-date web browser (Google Chrome recommended)*
- *PDF viewer*
- *Zoom client*
- *Speakers and microphone or headset (headset recommended)*

A separate monitor, tablet, or ebook reader is also recommended for the course to view the lab guide while conducting the lab scenarios.

Terms and Conditions

- Virtual Instructor Led Trainings (VILTs) are delivered as live instructor-led training in an online classroom with no on-site delivery element.
- This course is limited to the topics described in this data sheet and may not address all of your unique requirements.
- Forcepoint trainings are standard and non-negotiable.
- Forcepoint provides the training “AS IS” and makes no warranties of any kind, express or implied.
- VILT courses must be completed within six months from purchase or the course may be forfeited.
- The training services in this course are provided pursuant to the Subscription Agreement.
- Assent to the Subscription Agreement constitutes acceptance of the above terms and conditions.

For more information about this course or other Forcepoint training offerings, please visit https://www.forcepoint.com/services/training-and-technical-certification or contact Forcepoint Technical Learning Services at learn@forcepoint.com.

Forcepoint