Forcepoint Email Security Administrator Instructor-Led Training

Datasheet

September 2020

Forcepoint

forcepoint.com

Forcepoint Email Security Administrator Instructor-Led Training

In this two-day course, you will learn the features, components, and key integrations that enable Forcepoint Email Security functionality: how to administer policies, handle incidents, and upgrade, manage and assess the health of the Forcepoint Email Security system. You will develop skills in creating email policies, configuring 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 (Classroom training)

Duration:

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

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 exams

This course prepares you for 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

- Forcepoint solution introduction
- Forcepoint Email Security key features and new features

2. Understanding the deployment solution

- Communicate the Email Security key features.
- 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 the 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 the 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 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 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 usage model for Real-Time Black 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 trusted IP group and Allow Access List.

7. Managing Traffic – Advanced Configurations

Identify supported SMTP Port usage for appliance and hybrid modes.
Configure IP Address Group for Trusted and Allowed systems.
Enable SMTP VRFY command on the test system.
Explain how the System Administrator manages the Message Quarantine.
Describe the differences in permissions between Trusted IP and 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

Understand how Email Policy Flow, Types, and Conditions affect message flow.
Describe the 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 Protection (DLP) Tools with Email Security appliance.
Configure the Global IP and Global Address Permit Lists.
Verify policy behavior with test message generation tool.
Configure Email Security Antivirus and Antispam policy and verify detection.
Configure Email Data Loss Protection (DLP) action and policy rules.
Confirm Email DLP functionality with test message capture and log reviews.

Module 3: PEM & Advanced Configurations & Maintenance

9. Personal Email Manager (PEM) operations

Understand Personal Email Manager (PEM) architecture and use cases.
Configure the PEM portal and complete PEM configurations.
Describe Admin vs end user PEM and Quarantine activities.
Customize 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 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.
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.
Enforced/Mandatory TLS vs opportunistic TLS.
Enable enforced TLS for incoming/outgoing connections.
Enforced 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 Log Server Architecture and Database Partition Rollover and Deployment.

Terms and Conditions

- 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.
- ILT 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.