Forcepoint Email Security Administration

Duration: 2 Days

Description

During the two days, 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.

Participants

End-User/Customers: System administrators, network security administrators, IT staff

- Channel Partners: Sales Engineers, consultants, implementation specialists

Objectives

Describe the key capabilities of Forcepoint Email Security

- Understand the required and add-on components of Forcepoint Email Security
- Understand multiple deployment scenarios
- Perform initial setup configurations
- Configure connection level controls and message properties
- Create policies to fulfill various organization needs
- Understand the difference between various block/permit lists
- Configure email DLP policies
- Configure and customize PEM portal
- Understand email encryption methods
- Run and interpret reports and configure logs
- Understand how to upgrade the system and disaster recovery procedures

Certification requirements

- Completion of all course sessions
- Configured lab exercises
- Certification exam (multiple choice)

Programme

Topic 1: Features & Components

1) Forcepoint solution overview
a) Forcepoint solution introduction

2) Forcepoint Email Security features and new features
a) Key features
b) What’s new

3) Understanding the deployment
a) Forcepoint Email Security appliances
b) V-Series appliance interfaces
c) Network without Forcepoint Email Security
d) Network with Forcepoint Email Security
e) Required components
f) Internal daemons
g) Communications with external services
h) Supported V-Series and X-Series models and total resources
i) Hardware allocation

4) Getting started with Forcepoint Email Security
a) Fundamental email security concepts: protected domain and email relay
b) Setting up Forcepoint Email Security

5) Setting up users
a) Domain group
b) User directory

6) Defining email routing
a) Domain-based route
b) Directory-based route

Topic 2: Traffic & Policies

1) Traffic
a) Message processing flow
b) Setting connection properties (simultaneous connection per IP)
c) Configuring message properties (size, volume)
d) RBL & Reputation service
e) SMTP greeting delay
f) Recipient validation
g) DHA prevention
h) SPF check
i) SMTP authentication
j) Global IP block list
k) IP address group
l) Compare trusted IP group and Allow Access List

2) Quarantine system
a) Quarantine system overview
b) Queue monitor
c) Message queues

3) Policy
a) Policy flow
b) Policy type
c) Policy condition
d) Rules, filters, actions
e) Action options merge

f) Global IP and address permit list
g) Dynamic permit list
h) Built-in DLP
I. DLP integration
II. Registered with data security server

Topic 3: PEM & advanced configurations & Maintenance
1) Personal Email Manager (PEM)
a) PEM architecture
b) Enabling PEM
c) End user block/permit list

2) Threat Projection Cloud
a) Threat Protection Cloud introduction
b) Configure Threat Protection Cloud

3) Traffic shaping
a) 5 parameters
b) How traffic shaping works

4) Transfer Layer Security (TLS)
a) Enforced/Mandatory TLS vs opportunistic TLS
b) Enable enforced TLS for incoming/outgoing connections
c) Enforced TLS security level & encryption strength
d) CA issued or self-signed TLS certification process
e) Enable mandatory TLS
f) Enable opportunistic TLS

5) Secure Message Delivery
a) Secure Message Delivery scenario 1
b) Secure Message Delivery scenario 2
c) Enable Secure Message Delivery
d) Secure encryption queue
e) Secure Message Delivery end user experiences

6) Maintenance
a) Reporting
I. Log and reporting system overview
II. Log server and database deployment
III. Dashboard & alert & logs
IV. Presentation reports
V. Real-time monitor
VI. Log database partition & rollover & maintenance
b) System administration & maintenance
I. Manage appliances
II. Delegated administration
III. Backup and restore