

LEVEL TWO

THREAT PROTECTION

FORMAT

Instructor Led Training (ILT)
Virtual Instructor Led Training (VILT)
Onsite training at a customer's facilities (OS)

DURATION

VILT- 4 days
ILT- 3 days

INTENDED AUDIENCE

- Customers
- Partners
- Messaging Administrators
- Security Analysts

RECOMMENDED LEARNING

Threat Protection Level 1 for Administrators and Analysts Learning Path

REGISTRATION

Contact your account representative or training@proofpoint.com for registration information.

This course provides detailed information about the services running on Proofpoint Protection Server (PPS) and the features found in the Email Protection module. This course also provides a classroom lab environment for configuring these services and features.

PROTECTION SERVER SERVICES

Lesson 1: Threat Landscape and SMTP

Discuss how email threats fit into the overall threat landscape and review how email flows from senders to recipients. Review SMTP commands and configure an inbound mail routes.

Lesson 2: Email Protection Infrastructure

Describe PPS deployment scenarios, such as the on-premises standard cluster and PoD. Become familiar with the PPS management interface and software components.

Lesson 3: Message Processing

Describe how PPS filters email messages to protect email users and organizations. Describe the purpose and components of policy routes and email firewall rules. Configure and implement policy routes and email firewall rules.

Lesson 4: Quarantine

Describe the purpose of the quarantine and how to configure quarantine settings. Search for quarantined messages. Discuss how the quarantine impacts message filtering. Configure rules that quarantine messages.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.

Lesson 5: Smart Search and Log Viewer

Describe the settings for log viewer, reporting, alerts, and Smart Search. View entries recorded in the filter and MTA logs using log viewer and Smart Search.

Lesson 6: Encryption

Configure TLS encryption. Describe the purpose and function of certificates. Import a signed certificate.

Lesson 7: User Management and End User Services

Describe how PPS manages users and organizes sub-orgs and groups. Import and manage users. Describe the function of the End User Digest. Create custom branding of the end user interface. Make modifications to the end user web application.

EMAIL PROTECTION

Lesson 8: Email Firewall

Describe the unique components and features of the email firewall module. Configure and implement these features in the module: recipient verification, SMTP rate control, and bounce management.

Lesson 9: Impostor Email

Identify the various types of impostor email threats and describe how to mitigate them. Configure the anti-spoof rule.

Lesson 10: Email Authentication

Describe the purpose and function of these email authentication methods: SPF, DKIM, and DMARC. Configure DMARC policies and rules.

Lesson 11: Spam Detection

Describe how Proofpoint Dynamic Reputation and spam detection work. Configure spam detection features and spam policies. Configure safelists, blocklists, and custom spam rules.

Lesson 12: Virus Protection

Explain how the virus protection module works. Describe the virus protection module's general settings, virus definitions, policies and rules.

Lesson 13: Email Warning Tags

Use Email Warning Tags to warn or inform users that an incoming message may be dangerous.

Lesson 14: Targeted Attack Protection (TAP)

Explain how TAP protects users from malicious attachments and URLs. Configure settings in URL defense and in attachment defense, and then test the results. Describe how to access and use the TAP Threat Dashboard.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.