proofpoint. LEVEL UP

LEVEL THREE
PROTECTION SERVER

FORMAT

Offered as Virtual Instructor Led Training (VILT) or Instructor-Led Training (ILT).

DURATION

3 days

INTENDED AUDIENCE

Experienced PPS administrators responsible for ongoing management of Proofpoint Protection Server (PPS) solutions in a large enterprise environment.

PREREQUISITE

- Completion of the Threat Protection- Level 2 course (formerly Protection Server- Level 2), receiving a passing exam score or a minimum of 5 years of experience administering PPS

- Experience using basic Unix at the command line and a Telnet client for SSH

REGISTRATION

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

This course teaches you advanced settings, recommended configuration, and troubleshooting for PPS solutions. You'll get in-depth knowledge of mail processing, PPS logs, TLS, firewall rules and troubleshooting, envelope splitting, and email authentication.

COURSE OUTLINE

Lesson 1: Mail Processing and Filter

Examine how the filter interacts with incoming messages, interfaces with other processes, and ultimately accepts, rejects or discards messages.

Lesson 2: Network Configuration

Explore network interface settings on master and agent servers and make modifications as you attach a mail filter agent to a master configuration server.

Lesson 3: PPS Logs and archive log messages

Lesson 4: System Settings

Configure system settings, such as creating an SMTP profile for digest messages, implementing group-based routing and look-back hops.

Lesson 5: TLS

Configure TLS Fallback and implement TLS Encryption.

Lesson 6: Remote Syslog

Configure remote syslog in on-prem PPS deployment.

Lesson 7: Email Firewall Rules

Build Email Firewall rules to run against conditions from the connection stage through the end of the message, within recommended configurations. Describe potential issues with some configurations.

Lesson 8: Parsing PPS Logs

Use examples from real messages in the filter log to explain both how to read the log files and how the filter process works.

Lesson 9: Email Firewall Troubleshooting

Reinforce understanding of how the filter processes messages and how following best practices helps performance.

Lesson 10: Spam Detection

Review Spam module recommended configurations and walk through how safelists, blocklists and custom spam rules are executed.

Lesson 11: Envelope Splitting

Gain hands-on experience with SMTP message flow by sending messages in which envelope splitting occurs.

Lesson 12: TAP

Describe TAP UD and TAP AD recommended configurations and the results of integrating with Palo Alto WildFire.

Lesson 13: Email Authentication

Explore how PPS processes email authentication using SPF, DKIM and DMARC.

Lesson 14: User Import

Explore issues that occur with user imports and user databases after the initial installation.

Lesson 15: Health Check

Describe and discuss the various recommendations related to the configuration of a PPS Email Protection implementation.

Lesson 16: Sizing

Discuss the parameters needed when using the PPS sizing tool and the kind of output that can be expected.