Pass2Certify.com
Prepare, Practice, & Pass.

Proofpoint

TPAD01

ExamName: Threat Protection Administrator Exam

Exam Version: 6.0

Questions & Answers Sample PDF

(Preview content before you buy)

Check the full version using the link below.

https://pass2certify.com/exam/tpad01

Unlock Full Features:

Stay Updated: 90 days of free exam updates
Zero Risk: 30-day money-back policy
Instant Access: Download right after purchase
Always Here: 24/7 customer support team

Question 1. (Single Select)

In the context of spam detection, what is the primary function of Proofpoint Dynamic Reputation (PDR)?

A: To provide training for users on how to identify spam.
B: To filter emails based on user-defined rules.
C: To assess the sending MTA's reputation based on its IP address.
D: To analyze email content for spam keywords.

Answer: C

Explanation:
Proofpoint Dynamic Reputation (PDR) is designed to evaluate the reputation of the sending host at the connection level, using the sender's IP address as the core signal. In Proofpoint's own public description of PDR, the technology uses many features to determine the reputation of a particular IP and delays or blocks mail when that IP shows indications of spam activity. That means PDR is not primarily a user training feature, not a user-defined inbox rule engine, and not a simple keyword scanner of message body text. Its job is to assess the sending MTA before full message acceptance and use that reputation to influence how the system handles the connection. This is exactly why PDR is valuable in early-stage filtering: it helps reduce unwanted traffic before deeper content analysis takes place. Proofpoint's spam architecture also describes a multilayered defense where connection-level analysis includes Dynamic Reputation alongside SPF, recipient verification, and other connection checks. In practical administrator terms, PDR is part of the front-line evaluation of the source system's trustworthiness, helping the platform identify suspicious or compromised senders quickly and efficiently. That makes the correct answer the option focused on assessing the sending MTA's reputation by IP address.

Question 2. (Multi Select)

Which Email Firewall features should be used together to mitigate directory harvest attacks?

A: Outbound Throttle
B: SMTP Rate Control
C: Dictionaries
D: Bounce Management

E: Recipient Verification

Answer: B, E

Explanation:

Directory harvest attacks try to discover valid recipient addresses by sending large numbers of SMTP recipient attempts and observing which addresses are accepted or rejected. In Proofpoint's layered connection-level defenses, Recipient Verification and SMTP Rate Control are the two features that work together most directly against this problem. Recipient Verification checks whether the addressed mailbox is valid, while SMTP Rate Control helps detect and automatically block or throttle abusive SMTP connection behavior. Proofpoint's published spam detection material describes connection-level analysis that includes recipient verification and Dynamic Reputation, and then states that based on this analysis, SMTP rate control is used to automatically block or throttle malicious connections, providing strong protection against directory harvest and denial-of-service attacks. That pairing is exactly what makes these two options the correct answer. Outbound Throttle is aimed at controlling excessive outbound mail from accounts, not inbound recipient enumeration. Dictionaries are content and pattern controls, not recipient-existence validation controls. Bounce Management deals with BATV-style handling of backscatter, which is a different problem space. The Threat Protection Administrator course topic list also places SMTP Rate Control and Recipient Verification together under the same operational area, reinforcing that they are complementary controls for this class of attack. For a directory harvest scenario, these are the right two protections to deploy together.

Question 3. (Single Select)

As an administrator, you need to research why an email was sent instead of being blocked; where would you go in Cloud Admin to find which rule triggered the final disposition?

A: Audit Logs
B: Email Firewall
C: MTA Logs
D: Smart Search

Answer: D

Explanation:

The correct answer is Smart Search because Smart Search is the administrative investigation tool used to review message handling, trace processing outcomes, and identify the final rule that determined disposition. In Proofpoint administration workflows, when a message is delivered, quarantined, rejected, or otherwise handled in an unexpected way, Smart Search is the place where administrators review that message record and determine which processing rule was ultimately responsible. Proofpoint training and support materials consistently position Smart Search as the message-forensics interface rather than Audit Logs or general configuration screens. Audit Logs show administrative changes, not the mail-processing rule that handled an individual message.

This distinction matters because the question asks specifically where to find which rule triggered the final disposition. That is message-level evidence, not system-change evidence. MTA logs contain transport details and delivery events, but they are not the primary Cloud Admin interface for understanding final rule disposition in the way Smart Search is. Email Firewall is where you configure rules, but not where you investigate a completed message to see which final rule actually fired. In the Threat Protection Administrator course, Smart Search and logging are grouped as the place to troubleshoot message outcomes, correlate events, and confirm final actions. Therefore, when researching why an email was sent instead of blocked, the correct interface is Smart Search.

Question 4. (Single Select)

When setting up an Import/Authentication Profile in PPS, which of the following is a required piece of information to connect to an LDAP server?

A: POP3 server username
B: LDAP server hostname or IP address
C: SMTP server address
D: IMAP server port number

Answer: B

Explanation:

The correct answer is LDAP server hostname or IP address because an Import/Authentication Profile that connects to LDAP must first know where the LDAP directory service is located. In practical terms, Proofpoint cannot bind to or query an LDAP source unless the administrator provides the address of the LDAP server, whether by hostname or direct IP. This is foundational connection information. By contrast,

POP3, SMTP, and IMAP settings are not what PPS uses to connect to an LDAP directory for authentication or user import. Those protocols serve different mail-related purposes and are unrelated to LDAP directory lookups.

Within the Threat Protection Administrator course, User Management includes directory integration and user import. That workflow depends on specifying the correct LDAP endpoint so Proofpoint can perform binds, searches, and synchronization tasks against the directory. The requirement is basic but essential: before credentials, search base, or attribute mapping can matter, the product must know the LDAP server destination. This is why the hostname or IP address is treated as a required connection element. The same logic applies whether the backend is Active Directory or another LDAP-compliant directory source. The course teaches administrators to think in terms of identity source connectivity first, then attribute mapping and import logic after the connection is established. So for this question, the only answer that represents a required LDAP connection detail is LDAP server hostname or IP address.

Question 5. (Single Select)

What option will release a quarantined message without further filtering?

A: Redirect

B: Release Without Scan

C: Release Encrypted With Scan

D: Release With Scan

Answer: B

Explanation:

The correct answer is Release Without Scan because that option releases the quarantined message directly without resubmitting it through additional filtering stages. In Proofpoint quarantine operations, the wording of the release action matters. “With Scan” indicates the message is being released only after being scanned or reprocessed again by relevant protection layers, while “Without Scan” means the message is sent onward without further filtering. This terminology is also reflected in the release menu design shown in Proofpoint Protection Server training interfaces, where administrators are offered choices that distinguish direct release from release after rescan.

This question is testing quarantine-handling behavior rather than encryption or redirection workflows. “Redirect” changes the destination and does not answer the question about bypassing further filtering. “Release Encrypted With Scan” still includes scan behavior, so it does not meet the condition of no further

filtering. “Release With Scan” explicitly sends the message back through filtering logic before final release. In the Threat Protection Administrator course, Quarantine is taught as an area where administrators must understand the operational difference between resubmitting a message for inspection and simply releasing it. That distinction is important because one action preserves protection checks and the other bypasses them. Therefore, if the goal is to release a quarantined message without further filtering, the correct action is Release Without Scan.

Need more info? Check the link below:

https://pass2certify.com/exam/tpad01

Thanks for Being a Valued Pass2Certify User!

Guaranteed Success Pass Every Exam with Pass2Certify.

Save $15 instantly with promo code

SAVEFAST

Sales: sales@pass2certify.com

Support: support@pass2certify.com