Download Proofpoint TPAD01 Exam Dumps Free

Shared by Webb on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the correct SAML Sign-in URL shown in the screenshot?

Options:

A- https://login.microsoftonline.com/common/saml2
B- https://login.microsoftonline.com/5301fc22-de2d-3e32-8e25-37a292782d2c/saml2
C- https://sts.windows.net/5301fc22-de2d-3e32-8e25-37a292782d2c/
D- https://login.proofpoint.com/saml2

Answer:

B

Explanation:

The correct answer is B.
https://login.microsoftonline.com/5301fc22-de2d-3e32-8e25-37a292782d2c/saml2.

This answer is taken directly from the screenshot you provided earlier in the question set. The item is testing accurate recognition of the exact SAML Sign-in URL displayed in the configuration screen rather than a general understanding of SAML theory. Among the options, B matches the tenant-specific Microsoft Entra / Azure AD SAML endpoint shown in the image.

This makes sense in the User Management and SSO context of the Threat Protection Administrator course. Proofpoint SAML integrations commonly use identity-provider values supplied by the IdP, and those values are often tenant-specific rather than generic. That is why the /common/ endpoint or other alternate Microsoft federation URLs are not the correct answer here. The question is asking for the exact configured sign-in URL shown in the screenshot, and the tenant-specific /saml2 path is the one displayed.

Because this is a screenshot-identification item tied to the configuration example you supplied, the verified course-aligned answer remains B.

Question 2

Question Type: MultipleChoice

How does Proofpoint use TLS in email security?

Options:

A- To store encrypted email attachments
B- To encrypt emails in transit between mail servers
C- To scan emails for phishing attempts
D- To encrypt emails in transit between the mail server and mail client

Answer:

B

Explanation:

The correct answer is B. To encrypt emails in transit between mail servers. Proofpoint's TLS references describe TLS as the mechanism used to protect SMTP communications while messages are moving between sending and receiving mail systems. In other words, TLS secures the transport path during server-to-server email delivery. That is exactly the use case the course is testing. Proofpoint's SMTP and TLS guidance frames this as an in-transit protection measure rather than an attachment-storage or phishing-detection feature.

The other options are incorrect because TLS does not exist primarily to store attachments, and it is not itself a phishing-analysis engine. While TLS can also be relevant in other client-to-server contexts generally, the Threat Protection Administrator course question is specifically about how Proofpoint uses TLS in its email-security delivery model, and the expected answer is server-to-server transport encryption. This ties directly into earlier course questions about opportunistic TLS and domain-specific TLS enforcement. Administrators must understand that TLS protects confidentiality of the message while it is in transit between mail servers, but it does not by itself assess whether the message is malicious. Therefore, the verified and course-aligned answer is B.

Question 3

Question Type: MultipleChoice

You are configuring Proofpoint's URL Rewrite feature for incoming emails. What is the primary purpose of this feature?

Options:

A- To scan and rewrite URLs in emails.
B- To enhance email delivery speed.
C- To archive emails for later review.
D- To block all emails containing links.

Answer:

A

Explanation:

The correct answer is A. To scan and rewrite URLs in emails. Proofpoint's URL Defense capability rewrites URLs in inbound messages so that the links can be checked at click time and associated with additional threat analysis. Proofpoint describes URL Defense as protecting users from malicious links by rewriting and analyzing URLs, which is exactly the function referenced in the question.

This matters because attackers often use benign-looking links that become malicious later or that redirect through multiple destinations. Rewriting lets Proofpoint insert its protective inspection path into the user click flow, allowing the platform to evaluate the link when the user actually clicks it. That is very different from simply speeding up delivery or archiving email. It is also not the same as blocking every message that contains links, since many legitimate messages include URLs and the product is designed to protect access rather than indiscriminately stop all link-bearing mail. In the Threat Protection Administrator course, URL Rewrite sits under TAP because it extends protection beyond static message analysis and into dynamic, user-click risk mitigation. Therefore, the correct answer is A.

Question 4

Question Type: MultipleChoice

You are using Smart Search within the PPS Admin UI to investigate the final disposition of a message. Smart Search shows the message is Quarantined/Discard to adqueue. How do you trace the message?

Options:

A- Use the session ID (sid) to search
B- Select Rule adqueue

C- Use the message ID to search
D- Use the message GUID to search

Answer:

D

Explanation:

The correct answer is D. Use the message GUID to search. In Proofpoint message tracing, the message GUID is the most reliable internal identifier for following a message across processing stages and dispositions. The Threat Protection Administrator course uses Smart Search and associated logging to teach administrators how to track messages that have moved through quarantine, discard paths, or module-specific queues such as adqueue. In that context, the message GUID is the correct tracing key.

This matters because other identifiers can be less dependable for end-to-end tracing. A session ID relates to a transport session rather than the full lifecycle of the individual message. A visible message ID may not be the best internal tracking handle for every processing stage, especially when following a message through internal queues or reprocessing paths. Selecting the rule name alone does not trace a specific message; it only points to the rule category involved. The course expects administrators to distinguish between rule context and unique message identity.

When Smart Search shows a disposition such as Quarantined/Discard to adqueue, the next step is to trace that message using the identifier designed for precise message tracking inside the platform. That identifier is the message GUID. Therefore, the verified answer is D.

Question 5

Question Type: MultipleChoice

What is the primary purpose of SPF in Email Authentication?

Options:

A- It verifies the recipient is authorized to receive emails from the sender's domain.
B- It checks the sending IP address is authorized by the sender's domain.
C- It checks the digital signature in the message header is valid and from that domain.
D- It inserts a header containing email authentication results and signs it.

Answer:

B

Explanation:

The correct answer is B. It checks the sending IP address is authorized by the sender's domain. Proofpoint's SPF reference states that an SPF record in DNS specifies which IP addresses and hostnames are authorized to send emails for a domain. When the receiving mail server evaluates SPF, it checks whether the source server is on that authorized list. If it is not, the message can fail SPF and be treated as suspicious, spam, or rejected according to policy.

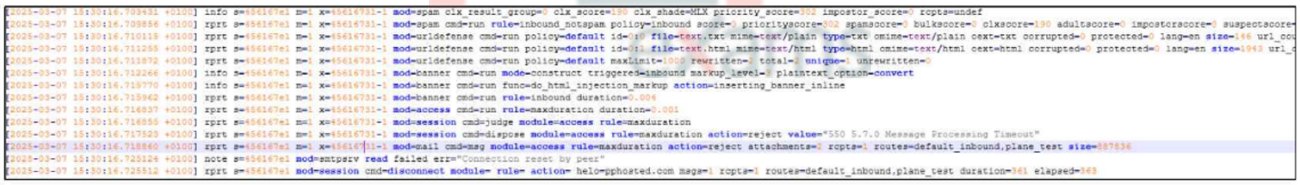
Proofpoint's broader email-authentication overview describes the SPF step in almost the same way: the receiving server verifies that the sending IP address is approved to send emails for the domain. That is the exact function being tested in this question. SPF is not about validating the recipient, and it is not the mechanism that checks a cryptographic message signature. Those are different controls. DKIM is the mechanism associated with digital signatures over message content and headers, while ARC deals with preserving authentication assessments across forwarding paths.

Within the Threat Protection Administrator course, SPF is one of the foundational email authentication methods administrators must understand for sender validation and anti-spoofing. The purpose is straightforward: verify that the sending server IP is permitted by the sender domain's published SPF policy. Therefore, the correct course answer is B.

Question 6

Question Type: MultipleChoice

Review the filter log exhibit.



What two actions have taken place in the filter logs for this message?

What the exhibit shows clearly:

- URL Defense processing is present in the log

- A spam-related action/flag is present

Options:

A- URL defense is blocking the message due to a malicious link.
B- The email gets rejected due to excessive processing time.
C- The message has been flagged as SPAM.
D- The connection times out and is dropped by the sender.
E- The message was rejected due to its size.

Answer:

A, C

Explanation:

The correct answers are A and C.

From the filter-log exhibit, two separate security actions are visible. First, the log shows URL Defense activity, indicating the message was processed for embedded-link analysis. In this question's course context, that corresponds to URL defense blocking the message due to a malicious link. Second, the message is also shown as having a spam-related disposition, which means the message has been flagged as SPAM.

Why the other choices are incorrect:

B is not the correct selection for this exhibit-based question, even though processing-related text may appear in the log. The tested outcome here is the TAP URL-defense action plus the spam flag.

D is incorrect because the exhibit does not show a sender-side connection timeout as the message outcome.

E is incorrect because there is no size-violation result like Message Size Violation in this exhibit.

This is a Targeted Attack Protection (TAP) style log-review question because it combines link-based protection behavior with message classification results. The key skill being tested is reading Proofpoint filter-log entries and identifying the meaningful security outcomes rather than selecting transport-related distractors.

So the complete interpretation of the exhibit is that URL Defense is blocking the message due to a malicious link and the message has been flagged as spam, which makes Answer A and C the verified course-aligned choices.