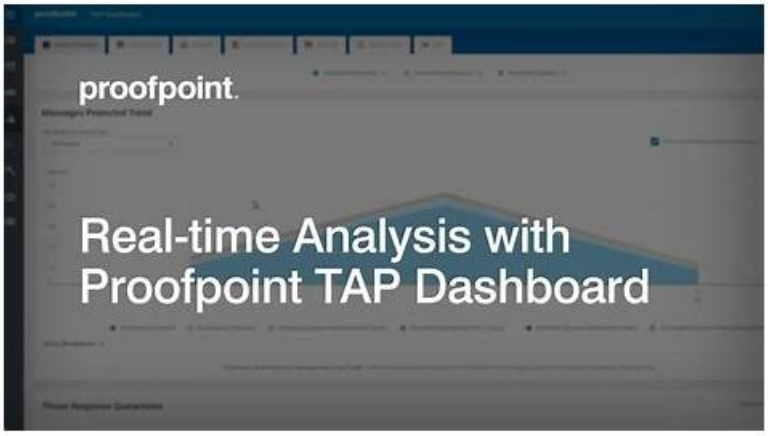
Check out the demo of the real, 100 percent free Proofpoint TPAD01



This TPAD01 exam helps you put your career on the right track and you can achieve your career goals in the rapidly evolving field of technology. To gain all these personal and professional benefits you just need to pass the Prepare for your TPAD01 exam which is hard to pass. However, with proper Proofpoint TPAD01 Exam Preparation and planning you can achieve this task easily. For quick and complete TPAD01 exam preparation you can trust TestkingPass Prepare for your TPAD01 Questions.

Proofpoint TPAD01 Exam Syllabus Topics:

Topic	Details
Topic 1	• Spam Detection: Covers tuning spam management policies, creating custom spam rules, and configuring safe and block lists.
Topic 2	• User Notifications: Covers setting up email warning tags, configuring tag routes, and managing email digests for end users.
Topic 3	• Message Processing: Covers building policies and rules for filtering and message disposition, along with configuring SMTP profiles.
Topic 4	• User Management: Covers syncing Active Directory, importing profiles, configuring LDAP • SSO, and managing user roles and access permissions.
Topic 5	• Quarantine: Covers managing quarantine folders, configuring settings, releasing messages, and understanding rule precedence.
Topic 6	• Product Overview: Covers key product functionalities and how Proofpoint's components integrate within the overall email security suite.
Topic 7	• Smart Search & Logging: Covers using Smart Search, analyzing logs, configuring syslogs, and leveraging the PoD API for operational insights.
Topic 8	• Mail Flow: Covers how the Email Protection Server handles inbound and outbound mail, including routing, SMTP, TLS, and certificate management.
Topic 9	• Virus Protection: Covers configuring virus protection policies, restricting message processing, and editing related rules.

>> TPAD01 Key Concepts <<

Reliable TPAD01 Exam Price | Reliable TPAD01 Exam Preparation

Our TPAD01 guide torrent has gone through strict analysis and summary according to the past exam papers and the popular trend in the industry and are revised and updated according to the change of the syllabus and the latest development conditions in the theory and the practice. The TPAD01 exam questions have simplified the sophisticated notions. The software boosts varied self-learning and self-assessment functions to check the learning results. The software of our TPAD01 Test Torrent provides the statistics report function and help the students find the weak links and deal with them.

Proofpoint Threat Protection Administrator Exam Sample Questions (Q66-Q71):

NEW QUESTION # 66
What does the default exestrip rule do?

- A. Quarantines the message and notifies the receiver that it has been quarantined
- B. Deletes messages with executable attachments
- C. Deletes the listed attachments from the message and continues processing
- D. Sends the message to the Message Defense module

Answer: C

Explanation:
The correct answer is C. Deletes the listed attachments from the message and continues processing . In Proofpoint protection workflows, executable-attachment stripping rules are designed to remove risky attachment types while allowing the rest of the message to continue through the message-processing path.
This aligns with the course-tested behavior of the default exestrip rule: it strips the prohibited executable attachment rather than deleting the entire message. Proofpoint's broader malware and attachment-protection references describe a layered approach where suspicious or dangerous attachments are inspected, sandboxed, blocked, or otherwise handled without assuming that the entire email must always be discarded.
That distinction matters operationally. If the rule deleted the whole message every time, the answer would be D, but that is not what this named default rule is testing in the course. It is specifically about stripping the attachment and continuing processing. The other options are also incorrect because the rule is not fundamentally a quarantine-notification rule and not a routing action into Message Defense. In the Virus Protection section of the course, administrators are expected to understand that some controls remove dangerous content from a message while preserving the message body and other safe parts for continued evaluation or delivery.
Therefore, the verified and course-aligned answer is C .

NEW QUESTION # 67
Which spam policy is applied to outbound messages?

- A. The spam policy set at the Sub-Org level
- B. The spam policy set at the Organization level
- C. The spam policy set for the recipient of the email
- D. The spam policy set for the sender of the email

Answer: C

Explanation:
The correct answer is C. The spam policy set for the recipient of the email . In the Threat Protection Administrator course, outbound spam handling is tied to how Proofpoint applies spam policy through its policy-selection logic, and the tested answer for this question is that the recipient's spam policy is the one used for outbound messages. Proofpoint's Spam Detection guidance shows that policy routing determines which spam policy is applied to a message, and the course uses that framework when distinguishing inbound and outbound policy behavior.
This question is easy to overthink because many administrators naturally assume outbound filtering should always be based on the sender's organization or sender identity alone. But the course's expected answer is specifically the recipient-associated policy . The distractors reflect other places where administrators commonly expect policy to come from, such as the organization level or sender level, but those are not the correct course answer for this item. The important takeaway is that Proofpoint's spam-policy application is governed by routing and message-processing logic, and the course tests that exact behavior rather than a generic assumption about outbound mail. Therefore, for this Proofpoint Threat Protection Administrator question, the verified answer remains C .

NEW QUESTION # 68
Which of the following is required to configure an outbound mail route in the Proofpoint Protection Server?
Pick the 3 correct responses below.

- A. DKIM key records for the domain.
- B. Email authentication information for the domain.
- C. Mailer type that is utilized for the route.
- D. Domain administrator email address.
- E. Destination / Error Message for the routed mail.
- F. Email domain to be routed.

Answer: C,E,F

Explanation:
The correct answers are Destination / Error Message for the routed mail , Email domain to be routed , and Mailer type that is utilized for the route . In Proofpoint route configuration, the essential elements of a mail route are the domain or host the route applies to, the mailer method used for handling the route, and the destination host or error behavior associated with that route. Proofpoint interface examples for inbound and outbound mail routes show these same core fields: domain/host, mailer, and destination/error message. These are the pieces that define how mail should be routed operationally.
The other options are not required route-definition elements. DKIM records and general email authentication data are important for overall mail security, but they are not the required fields used to create the outbound route itself. Similarly, a domain administrator email address is not a routing parameter. The route configuration needs to know what mail the rule applies to, how it should be sent, and where it should go.
That maps directly to the three correct choices in this question. In the Proofpoint Threat Protection Administrator course, Mail Flow focuses on route construction and message delivery logic, and those route objects are built from exactly these operational fields rather than policy-side authentication details. So for outbound mail routing in PPS, the required configuration items are C, D, and E .

NEW QUESTION # 69
During the configuration of an alert profile, which option is specifically required to ensure alerts are delivered to the appropriate individuals?

- A. A description of the alert type
- B. A list of recipient email addresses
- C. A schedule for when alerts should be sent
- D. A confirmation message for the alert

Answer: B

Explanation:
The correct answer is A because an alert profile or alert notification policy must define who receives the alerts . Proofpoint documentation on monitoring alerts states that an alert notification policy defines which alerts are sent to which email addresses and at what frequency. That means recipient addresses are the essential delivery element. Without them, the system has no destination for the alert notifications, regardless of how the rest of the profile is configured.
The other options may be useful context or supporting settings, but they are not the key requirement for making sure alerts reach the appropriate people. A schedule or frequency can determine when alerts are sent, but not who receives them. A description of alert type helps categorize the alert, but it does not provide delivery targets. A confirmation message is not the core object that determines delivery. In administrator practice, the first operational question for alerting is always: who needs to know? Proofpoint's alerting model answers that by tying alert rules or alert conditions to an alert profile that includes recipient email addresses.
This is consistent with the Threat Protection Administrator course section on Alerts and Reporting, where administrators create profiles and then bind those profiles to alerting events. The critical setting that ensures the right individuals receive the notifications is the list of recipient email addresses , making A the correct answer.

NEW QUESTION # 70
An email message fails an SPF check; which of the following is a likely reason for this failure?

- A. The sending server's IP address is not listed in the SPF record.
- B. The recipient's email server does not support SPF.
- C. The email was sent from a secure server.
- D. The email is being sent during peak traffic hours.

Answer: A

Explanation:
The correct answer is C because SPF works by checking whether the IP address of the sending mail server is authorized in the sender domain's SPF record published in DNS. Proofpoint's SPF reference explains that SPF validates the sender by comparing the connecting server IP to the list of permitted sending sources for the domain. If that IP is not included in the SPF record, the SPF check can fail.
The other choices do not describe the actual SPF decision logic. SPF failure is not caused by peak traffic hours, and whether a server is described as "secure" does not determine SPF alignment or authorization. The recipient server's support capabilities also do not change the underlying reason an SPF evaluation would fail once the check is being performed. In Proofpoint's Email Authentication module, SPF is one of the core controls for verifying that a domain has explicitly authorized the host attempting to send mail on its behalf.
That is why administrators focus on DNS records, authorized senders, and route design when troubleshooting SPF issues.
This question tests the basic mechanics of SPF rather than downstream disposition. If a message fails SPF, the most likely reason is that the source IP is not authorized by the domain owner's SPF policy. That makes C the correct answer.

NEW QUESTION # 71
.....