PassQueen
a.k.a dumpsqueen.com

Administration of Symantec Email Security.cloud - v1

Symantec 250-445

Version Demo

Total Demo Questions: 9

Total Premium Questions: 92

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which two outcomes can result when a user releases a legitimate email from the end-user spam quarantine? (Choose two.)

A. The message is delivered to the user

B. The sender can be added to the user's Approved Senders list

C. Anti-Malware scanning is disabled for the sender

D. The domain's MX record is changed automatically

E. All messages from the sender are released from administrator quarantine

ANSWER: A B

Explanation:

The message is delivered to the user and **the sender can be added to the user's Approved Senders list** are correct. Releasing a message allows the recipient to receive mail that was incorrectly classified as spam. Depending on the available quarantine workflow, the user can also add the sender to the personal Approved Senders list to reduce the likelihood of future legitimate messages from that sender being treated as spam.

Releasing a message does not disable anti-malware scanning for the organization and does not modify the public MX record. Administrators should still use caution when releasing unexpected mail, particularly messages that contain links or attachments. See Broadcom TechDocs: Email Security.cloud.

QUESTION NO: 2

Which two DNS records are commonly used to publish email authentication information for a domain? (Choose two.)

A. SPF

B. DKIM

C. MX

D. PTR

E. SRV

ANSWER: A B

Explanation:

SPF and **DKIM** records are correct. SPF policy information is published in a DNS TXT record and identifies hosts authorized to send mail for a domain. DKIM public keys are also published in DNS, normally as TXT records at a selector-specific name, allowing receiving systems to verify a message signature.

These DNS-published controls can be used with DMARC to improve domain-based email authentication. MX records direct mail delivery, but they do not publish sender authorization or cryptographic verification data. See RFC 7208: SPF and RFC 6376: DKIM.

QUESTION NO: 3

What is the importance of selecting the appropriate content type, when creating a list for Data Protection policy?

A. The content type determines the condition the list resides in.

B. The content type determines whether the list can be used for Policy Based Encryption.

C. The content type determines how often a list can be used.

D. The content type determines what type of policies can be created.

ANSWER: A

Explanation:

The content type determines the condition the list resides in. In Email Security.cloud Data Protection, a list group is designed for use with a particular type of policy condition. Selecting the content type establishes the context in which the values in that list are evaluated, such as the relevant message or content attribute. This association is important because it ensures that the list is made available when configuring the matching condition in a Data Protection policy and that its entries are interpreted appropriately by the policy engine.

Administrators should therefore choose the intended content type before saving the list group. The content type is a defining property of the list group rather than a general label; it connects the group to the applicable condition category used during policy construction. Careful selection at creation time helps ensure the list can support the intended detection logic and policy workflow. Broadcom's Email Data Protection documentation describes creating list groups and selecting their content type for use in the applicable conditions: Creating a list group in Email Data Protection.

QUESTION NO: 4

What are the two characteristics for an email to be considered Spam? (Choose two.)

A. Unsolicited

B. Malicious

C. Unwanted

D. Bulk

ANSWER: A D

Explanation:

Spam is characterized as unsolicited bulk email. "Unsolicited" means the recipient did not request, consent to, or otherwise initiate receipt of the message. This distinguishes spam from mail that a recipient has deliberately subscribed to receive, such as newsletters, service notices, or requested marketing communications. "Bulk" means substantially similar messages are distributed at scale to numerous recipients, rather than being a genuinely individualized one-to-one communication.

These two attributes are used together because a message can be sent to many recipients legitimately when recipients have opted in, while an unsolicited individual message does not necessarily represent a bulk-mail spam campaign. Symantec Email Security.cloud uses layered anti-spam analysis to identify this type of unwanted mass distribution, including message content, sender reputation, and distribution-related signals. The classification of spam should not depend on whether a message contains malware or another malicious payload; spam and malicious email are related but distinct email-security categories.

For Symantec Email Security.cloud product documentation, see Broadcom TechDocs: Email Security.cloud. The widely used industry definition of spam as unsolicited bulk email is also documented by Spamhaus: What is Spam?.

QUESTION NO: 5

Which Email Security.cloud scanning technology is able to be modified by a customer?

A. Traffic Shaping

B. Anti-Spam

C. SMTP Heuristics

D. Anti-Malware

ANSWER: B

Explanation:

Anti-Spam is correct because Email Security.cloud lets customer administrators tailor spam handling to their organization's mail-flow and risk requirements. Through the service's administration portal and policy controls, an administrator can adjust anti-spam settings such as the treatment of messages identified as spam, permitted and blocked sender or domain lists, and end-user spam-management behavior. These controls allow the organization to tune the service for legitimate bulk mail, trusted business partners, and its preferred balance between blocking unwanted mail and allowing potentially suspicious messages for review.

This customer-level configurability is important because spam characteristics and acceptable mail practices vary substantially among organizations. The underlying service continues to apply Symantec's centrally maintained detection intelligence, while the customer modifies how the anti-spam capability is applied and how detected messages are handled within its own account. Broadcom's Email Security.cloud documentation describes the service and its configurable policy-based protection features: Broadcom TechDocs: Email Security.cloud. Additional product information, including email threat-protection capabilities and administrative controls, is available at Broadcom Email Security.cloud.

QUESTION NO: 6

Where can an administrator locate the "Pen Number" for an email quarantined by Anti-Malware?

A. Administrator Quarantine

B. Track and Trace

C. Malware Release

D. End User Quarantine

ANSWER: C

Explanation:

Malware Release is the correct location. In Symantec Email Security.cloud, messages quarantined by the Anti-Malware service are managed through the Malware Release area. This page provides the malware-quarantine records needed to identify a held message and, where authorized, submit it for release. The PEN number is the identifier associated with the quarantined malware event and is displayed with the relevant message information in this workflow. Administrators should use that identifier when they need to reference a specific Anti-Malware quarantine event, such as when investigating a detection, validating the message to be released, or communicating the event details to Broadcom Support. The Malware Release function is specifically designed for handling messages retained because of malware detection, so it exposes the event information that supports controlled release and auditability. Broadcom's Email Security.cloud guidance for locating the PEN number identifies the Malware Release interface as the place to obtain it. See Broadcom Knowledge Base article HOWTO109647 and the Broadcom Security Center support portal for Email Security.cloud documentation and support resources.

QUESTION NO: 7

Which quarantine settings are able to be managed within the Administrator Quarantine for Email Security.cloud?

A. Domain Block Lists

B. End User Block Lists

C. Data Protection Policies

D. Anti-Spam Scanning Settings

ANSWER: D

Explanation:

Anti-Spam Scanning Settings is correct because the Email Security.cloud Administrator Quarantine provides administrators with controls related to how suspected unsolicited email is handled and quarantined. These controls support administration of the anti-spam service, including the treatment of messages identified through spam scanning and the resulting quarantine behavior. Managing these settings from the administrative quarantine helps ensure that the organization's spam-handling approach is applied consistently, while still allowing administrators to review quarantined items and respond to false-positive concerns. This is distinct from managing individual user sender preferences or creating broader data-protection policy rules; the relevant quarantine management function is specifically associated with the anti-spam scanning and quarantine workflow. Broadcom's Email Security.cloud documentation describes the cloud email-security service and its administrative capabilities at Broadcom TechDocs: Email Security.cloud. Additional product and administrator documentation is available through the Broadcom Security Support portal.

QUESTION NO: 8

What is the purpose of Email Security.cloud Click-Time protection?

A. Scan email web links for malware before email is delivered

B. Scan email web links for inappropriate content when the link is accessed by the user

C. Scan email web links for inappropriate content before email is delivered

D. Scan email web links for malware when the link is accessed by the user

ANSWER: D

Explanation:

Email Security.cloud Click-Time protection scans web links for malware at the moment the recipient accesses the link. The service rewrites eligible URLs in inbound messages so that a recipient's click is routed through Symantec's protection service. This timing is important because a URL that appeared safe when the email was initially delivered can later be changed to host malicious content, or its destination can become compromised. By checking the link at click time, Email Security.cloud can evaluate the current risk and block access to known malicious websites, helping protect users from threats such as phishing, drive-by downloads, and malware-hosting pages. This capability complements message-time filtering: it provides an additional layer of protection after delivery, when the linked web content may have changed. Symantec describes Click-Time Protection as URL protection that checks links when recipients click them, rather than relying solely on the state of a link during email processing. See the Broadcom Security Center and the Symantec Email Security.cloud overview.

QUESTION NO: 9

Which two actions should be completed before changing a domain's MX record to route inbound email through Email Security.cloud? (Choose two.)

A. Configure the destination mail server

B. Reduce the MX record TTL in advance

C. Install an endpoint anti-malware agent

D. Create an end-user quarantine account

E. Publish a DKIM private key

ANSWER: A B

Explanation:

Configure the destination mail server and **reduce the MX record TTL in advance** are correct. The destination mail server must be configured in the service so filtered mail has a valid relay target. Reducing the existing MX record TTL before the planned change helps DNS resolvers refresh the new routing information more quickly.

The MX record itself is changed during the cutover. Installing an endpoint anti-malware agent or creating a user quarantine account is not required to establish inbound mail routing through the cloud service. DNS TTL behavior is described in RFC 2181, Section 8. Email Security.cloud documentation is available through Broadcom TechDocs.