PassQueen
a.k.a dumpsqueen.com

Symantec Messaging Gateway 10.5 Technical Assessment

Symantec ST0-250

Version Demo

Total Demo Questions: 14

Total Premium Questions: 144

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Symantec Messaging Gateway Overview	36
Topic 2, Installation and Configuration	31
Topic 3, Administration	67
Topic 4, Troubleshooting	10
Total	144

QUESTION NO: 1

An administrator requires encrypted SMTP transport to a business partner without changing the normal SMTP port used for mail delivery. Which SMTP extension should the partner mail server advertise and the Symantec Messaging Gateway scanner use?

A. STARTTLS

B. AUTH LOGIN

C. VRFY

D. ETRN

ANSWER: A

Explanation:

STARTTLS is the SMTP extension used to upgrade an existing SMTP session to a TLS-protected session. The SMTP connection is established normally, and the sending server uses the STARTTLS command when the receiving server advertises STARTTLS capability. This permits encrypted transport without requiring a separate SMTP service port for the mail flow.

In Symantec Messaging Gateway, a TLS delivery action can be applied through policy for outbound mail that requires protected server-to-server transmission. Administrators should also validate the partner certificate and TLS requirements before enforcing TLS-only delivery. The SMTP TLS extension is defined in RFC 3207.

QUESTION NO: 2

Which additional Email Reports Data collection must be enabled to track Top Probe Accounts via reports?

A. Spam and Unwanted Mail

B. Submissions

C. Sender IP connections

D. Invalid Recipients

ANSWER: D

Explanation:

Invalid Recipients must be enabled because probe accounts are recipient addresses that are monitored for attempted delivery activity. Symantec Messaging Gateway records the recipient-validation events needed to identify these addresses as invalid-recipient data. When this additional Email Reports Data collection is active, the reporting database retains the relevant recipient information and can aggregate it into the Top Probe Accounts report. This allows an administrator to see which probe addresses receive the highest volume of attempted messages, helping identify directory-harvesting behavior and other unsolicited-mail activity directed at non-deliverable or monitored recipients.

Additional Email Reports Data collections are optional because retaining detailed event data has storage and processing implications. Enabling the collection before relying on the report is important: reports can only use data gathered while the applicable collection was enabled, rather than reconstructing probe-account activity from events that were not retained. The Symantec Messaging Gateway documentation library provides the product administration and reporting references at Broadcom TechDocs: Symantec Messaging Gateway. Product support and knowledge resources are available through the Broadcom Security Support portal.

QUESTION NO: 3

Which two types of end-user feedback can contribute to the Symantec Messaging Gateway custom anti-spam rules process? (Select two.)

A. missed spam submissions

B. false positive submissions

C. invalid-recipient submissions

D. blocked TLS connection submissions

E. directory synchronization submissions

ANSWER: A B

Explanation:

Missed spam submissions provide samples of unwanted mail that was delivered without being identified as spam. These submissions can help Symantec evaluate message patterns that require organization-specific anti-spam detection.

False positive submissions provide samples of legitimate mail that was incorrectly classified as spam. This feedback helps identify cases where a custom rule may need to avoid matching legitimate business mail. Both submission types are useful because they provide evidence of local mail characteristics that may not be represented in global anti-spam rules. See the Symantec Messaging Gateway documentation for anti-spam administration information.

QUESTION NO: 4

During which phase of inbound message flow does Symantec Messaging Gateway 10.5 accept, reject, or defer messages on the basis of the message envelope?

A. SMTP delivery

B. message filtering

C. SMTP session

D. message routing

ANSWER: C

Explanation:

SMTP session is correct because it is the inbound processing stage in which Symantec Messaging Gateway evaluates the SMTP conversation and its envelope information before it accepts the message body for subsequent processing. The envelope consists primarily of the SMTP sender supplied with `MAIL FROM` and the recipient or recipients supplied with `RCPT TO`. At this point, the gateway can apply connection- and recipient-level controls and return an SMTP response that accepts the transaction, rejects it, or temporarily defers it. This early decision point is important because an SMTP rejection or deferral is communicated directly to the sending server during the active SMTP exchange, rather than occurring after the message has been fully received and queued. The SMTP protocol defines these envelope commands and the use of success, permanent-failure, and temporary-failure responses during a mail transaction. Symantec Messaging Gateway's inbound mail-processing design uses this session-level stage to make envelope-based handling decisions before later content-oriented processing stages. See the Symantec Messaging Gateway documentation portal at Broadcom TechDocs and the SMTP transaction specification in RFC 5321.

QUESTION NO: 5

Which MTA operation is used if queues need to be drained to remove a host from use and continue scanning and delivery of messages?

A. delete the Scanner from the Control Center so that it is no longer used

B. set the Scanner configuration to "Pause message scanning and delivery"

C. set the Scanner configuration to "Do not accept incoming messages"

D. disable the Conduit so that new messages are not accepted

ANSWER: C

Explanation:

The appropriate operation is **set the Scanner configuration to "Do not accept incoming messages"**. This places the Scanner's mail-transfer service into a drain state: it stops accepting new SMTP traffic while allowing messages already held in its queues to continue through the normal scanning and delivery workflow. Administrators use this state when they need to take a Scanner out of service for maintenance, replacement, or decommissioning without abruptly interrupting mail that the host has already received.

Queue draining is important because messages can remain pending while content scanning, routing, retry handling, or downstream delivery is still in progress. Preventing new incoming messages lets the existing queue decrease naturally while the Scanner remains operational for those messages. Once the queued workload has cleared, the host can be safely removed from active use. This controlled process maintains message processing continuity and avoids leaving already accepted mail stranded in the appliance queue. Symantec Messaging Gateway administration documentation describes Scanner and MTA operational controls in its product documentation; see the Broadcom Symantec Messaging Gateway documentation and the Broadcom Support portal for the applicable release guides.

QUESTION NO: 6

What is required before attempting installation of the Symantec Messaging Gateway 10.5 appliance?

A. console access to the appliance

B. DVD-ROM drive listed on hardware compatibility list

C. valid license file

D. machine account created in Active Directory

ANSWER: A

Explanation:

Console access to the appliance is required before installing Symantec Messaging Gateway 10.5 because the installation process must be performed from the appliance's local console. The administrator needs direct keyboard, video, and monitor access, or an equivalent supported remote-console capability supplied by the server hardware, to boot the installation media and interact with the installer. This access is also necessary to enter the initial network settings that allow the appliance to become reachable for subsequent browser-based administration through the Symantec Messaging Gateway Control Center.

The prerequisite is specifically about being able to access and operate the target appliance during its pre-network installation stage. Initial deployment cannot assume that the appliance already has an operational management interface or is reachable on the network. Once the operating system and Messaging Gateway software have been installed and initial configuration is complete, ongoing administration is normally performed through the web-based Control Center. Broadcom's Messaging Gateway documentation and product resources are available through the Symantec Messaging Gateway documentation portal and the Broadcom Symantec Messaging Gateway product page.

QUESTION NO: 7

Which two policy actions are available within Symantec Messaging Gateway version 10.0? (Select two.)

A. create a quarantine incident

B. deliver the message to the Outlook spam folder

C. send notification to the administrator

D. terminate the sender's connection

E. create an informational incident

ANSWER: A E

Explanation:

Symantec Messaging Gateway policy processing can generate incidents as an outcome of a rule match. “create a quarantine incident” is an available action for retaining a message in quarantine for later review and disposition. This supports controlled handling of mail that meets a policy condition while preserving the message and its associated incident details for authorized administrators or reviewers. “create an informational incident

” is also available when the policy should record the event and provide visibility without using quarantine as the handling mechanism. Informational incidents provide an audit and investigation record, allowing policy matches to be tracked through the product’s incident-management workflow.

These incident actions are part of the policy-action model documented for Symantec Messaging Gateway and are selected according to whether the matched message requires quarantine-based handling or informational tracking. Broadcom’s Symantec Messaging Gateway documentation portal provides the product administration and policy configuration references: Symantec Messaging Gateway documentation. Product support resources, including documentation access and lifecycle information, are available from Broadcom Symantec Messaging Gateway Support.

QUESTION NO: 8

Which two actions are valid for a content compliance policy? (Select two.)

A. Edit the message to delete the offensive content

B. Add a header to the message

C. Drop the connection to the offending mail server

D. Forward the message

E. Flag the message for further scanning

ANSWER: B D

Explanation:

Content compliance policies in Symantec Messaging Gateway evaluate messages against administrator-defined content rules, such as keyword, pattern, attachment, or data-leakage criteria. Once a message matches a policy, the policy can apply mail-processing actions that preserve the message for controlled delivery or route it to an alternate recipient for review. “Add a header to the message” is a valid action because it stamps the message with administrator-selected header information. This enables downstream mail systems, compliance workflows, or mail clients to identify the message as having matched a particular compliance condition and handle it accordingly.

“Forward the message” is also a valid content-compliance action. It sends a copy of a matched message to a designated recipient, such as a compliance officer, supervisor, archive mailbox, or incident-review address. This supports oversight and investigation while the gateway processes the original message according to the configured policy behavior. These actions are configured as responses to a content compliance rule match, rather than as connection-level controls. Symantec Messaging Gateway documentation organizes these settings under content compliance policy and message-action configuration. See the Symantec Messaging Gateway documentation and Broadcom’s Messaging Security product information.

QUESTION NO: 9

When an administrator creates a scheduled report in Symantec Messaging Gateway 10.5, which two settings can be configured for the report job? (Select two.)

A. the report recurrence

B. report delivery recipients

C. the Scanner operating system version

D. the LDAP directory schema

E. the DKIM private key

ANSWER: A B

Explanation:

A scheduled report job can be configured with a **recurrence**, such as a daily, weekly, or monthly schedule. This allows the Control Center to generate the selected report automatically at the defined interval.

The administrator can also configure **report delivery recipients** for the scheduled job. This allows completed reports to be sent to designated administrators, managers, or other stakeholders without requiring manual report generation and distribution. Scheduling supports routine operational monitoring and management reporting. See the Symantec Messaging Gateway documentation for reporting administration guidance.

QUESTION NO: 10

How does enabling and configuring sender authentication options in Symantec Messaging Gateway 10.5 help to protect against spam?

A. by protecting against messages sent from trusted partners

B. by protecting against messages sent using a Sendmail MTA

C. by protecting against messages with a forged message ID

D. by protecting against messages with forged sender domains

ANSWER: D

Explanation:

Sender authentication helps protect against spam by protecting against messages with forged sender domains. These controls evaluate whether a sending host is authorized to use the domain presented in the message's envelope sender or other sender identity. Symantec Messaging Gateway can use sender-authentication technologies such as SPF and DomainKeys Identified Mail to validate domain-related assertions. This makes it substantially harder for spammers and phishers to impersonate a legitimate organization's domain, a common tactic used to make unsolicited or malicious email appear trustworthy. Based on the authentication result, administrators can configure policy actions such as accepting, tagging, quarantining, or rejecting a message. Sender authentication is therefore a domain anti-spoofing control: it helps establish whether the claimed sender domain is authentic and provides a reliable signal for spam-filtering policy decisions. It is most effective when combined with the gateway's reputation, content-filtering, and anti-malware protections. For background on SPF domain authorization, see RFC 7208. For the DKIM validation model used to verify signed domain identity, see RFC 6376.

QUESTION NO: 11

An administrator must determine why a particular message generated a content incident and which policy action was applied. Which two sources should the administrator review? (Select two.)

A. Message Audit log

B. Incident Match log

C. Admin Audit log

D. Conduit log

E. Fastpass log

ANSWER: A B

Explanation:

The **Message Audit log** provides message-specific processing information, including the final verdict and actions taken. It helps the administrator identify the resulting disposition of the message.

The **Incident Match log** provides filtering-policy match detail for an incident. It is useful for determining which policy matched the message and for investigating policy precedence or unexpected policy actions.

QUESTION NO: 12

Which two statements describe the use of keys in DKIM processing for Symantec Messaging Gateway 10.5? (Select two.)

A. A private key is used to sign eligible outbound messages.

B. A public key is published in DNS for signature validation.

C. A public key is stored only in the Scanner local message queue.

D. A private key is supplied by the recipient's SMTP server.

E. A private key is included in the DKIM-Signature message header.

ANSWER: A B

Explanation:

DKIM signing uses a **private key** that is controlled by the signing organization. Symantec Messaging Gateway uses that private key to generate a cryptographic signature for an outbound message. The receiving system can then evaluate whether the message content and signed headers remain valid.

The corresponding **public key** is published by the signing domain in DNS. A receiving gateway retrieves this public key through DNS and uses it to validate the DKIM signature. The private key must not be published, while the public key is intentionally available for receiving systems to perform validation. See RFC 6376 and the Symantec Messaging Gateway documentation.

QUESTION NO: 13

What is the default time period that a suspect virus can reside in the Suspect Virus Quarantine?

A. 6 hours

B. 12 hours

C. 24 hours

D. 48 hours

ANSWER: A

Explanation:

The default retention period is **6 hours**. Symantec Messaging Gateway uses the Suspect Virus Quarantine as a temporary holding area for messages that are suspected of containing a virus but require additional scanning or updated virus-definition information before final processing can occur. The six-hour default provides time for the appliance to obtain and apply current protection updates and reassess the message, while also limiting unnecessary delivery delays and preventing the quarantine from retaining unresolved mail indefinitely. This is a configurable quarantine behavior, but the question asks

specifically for the factory default used by the product. Administrators can review and adjust virus-protection and quarantine settings in the Messaging Gateway administration interface when their organization's mail-flow, update schedule, or risk requirements call for a different retention period. Symantec's Messaging Gateway documentation describes the product's virus scanning and quarantine administration features; see the Broadcom Symantec Messaging Gateway documentation portal and the Broadcom Knowledge Base for product documentation and support guidance.

QUESTION NO: 14

A Symantec Messaging Gateway 10.5 administrator is creating a new spam policy and needs to choose a message condition. Which two are valid message conditions? (Select two.)

A. a message that contains a header from DLP

B. a message that is spam or suspected spam

C. a message that contains prepended notation

D. a message that is unscannable

E. a message that fails bounce attack validation

ANSWER: B E

Explanation:

For a Symantec Messaging Gateway spam policy, valid conditions include *a message that is spam or suspected spam* and *a message that fails bounce attack validation*. The spam or suspected-spam condition lets an administrator apply a policy action after the gateway's antispam scanning classifies a message at the configured spam confidence level. This supports policy handling such as quarantining, tagging, deleting, or otherwise processing messages identified by the antispam engine.

Bounce attack validation is also available as a message condition because Messaging Gateway can identify invalid non-delivery reports and other bounce-related abuse. A message that fails this validation can be handled through a spam policy, allowing the administrator to apply a targeted action to messages that do not satisfy the gateway's bounce-validation checks. These conditions are evaluated as message characteristics within the policy framework, enabling antispam and bounce-attack protections to be enforced consistently for the policy's selected recipients or groups. Broadcom's Symantec Messaging Gateway documentation includes the policy-management and antispam configuration guidance relevant to these message-processing controls. See the Symantec Messaging Gateway 10.5 documentation and the Broadcom Support portal for product documentation and knowledge-base resources.