Administration of Symantec™ Messaging Gateway 10.5
Sample Exam

Contents

Sample Questions

1. Which default action is taken by the system when a message is unscannable for malware and content filtering?

    a. quarantine message
    b. delete message
    c. prepend subject
    d. deliver normally

2. Which feature is automatically enabled when enabling Control Center authentication?

    a. spam quarantine address resolution
    b. message sender validation
    c. invalid recipient handling
    d. suspect virus quarantine address resolution

3. What are two reasons for an administrator to create a content filtering rule using informational incidents instead of quarantine incidents? (Select two.)

    a. to monitor access to a specific policy violation without affecting mail flow
    b. to track policy violations without affecting mail flow
    c. to track policy violation remediation activity
    d. to monitor for policy violation false positives without affecting mail flow
    e. to reduce the number of policy violation alerts sent to the administrator

4. How may the size of incident folders be limited?

    a. globally
    b. by group
    c. by user
    d. by folder

5. A Symantec Messaging Gateway administrator needs to configure compliance violations so the sender's manager makes the final decision as to whether the content is sent.

    Which action should the administrator configure for content violations?

    a. add bcc recipient
    b. hold for review
    c. send notification
    d. create a quarantine incident

6. Which feature of Symantec Messaging Gateway is designed to identify the IP address of senders of virus infected emails?

    a. Email Virus Attacks
    b. Connection Classification
    c. Email Suspect Virus Quarantine
    d. Local Bad Sender IPs

7. Which two sender authentication technologies are included in Symantec Messaging Gateway? (Select two.)

    a. Domain Keys Identified Mail (DKIM)
    b. email greylisting
    c. sender reputation analysis
    d. Author Domain Signing Practices (ADSP)
    e. Sender Policy Framework (SPF)

8. Which service retrieves new and updated spam definitions from Symantec Security Response?

    a. LiveUpdate
    b. Conduit
    c. Brightmail Engine
    d. Directory Data Service

9. Which MTA operation is used if incoming messages need to be stopped while waiting for new virus definitions?

    a. accept and deliver messages normally
    b. pause message scanning and delivery
    c. do not accept incoming messages
    d. delay incoming messages

10. What is the minimum number of Ethernet interfaces that must be configured in order to complete the Bootstrap process?

    a. 0
    b. 1
    c. 2
    d. 3

11. During the site setup wizard, why must Symantec Messaging Gateway be allowed outbound network access?

    a. to enable outgoing email
    b. to complete the licensing process
    c. to connect to an NTP server
    d. to connect to LiveUpdate

12. An IP address is defined in the Local Good Sender IPs group and the action for that group is to deliver messages normally. An administrator wants to verify that the sender policy is working correctly and uses the IP Reputation Lookup tool to search for an IP from the Local Good Sender IPs group.

    Which action does the Symantec Messaging Gateway display under the Local Status within the IP search results?

    a. Skip AV Filtering
    b. Skip AS Filtering
    c. Filter Partially
    d. Filter Normally

13. A partner company emails a daily report containing the latest spam threats to the IT manager. The report is identified as spam based on the content and is blocked.

    How can the IT manager use Adaptive Reputation Management to ensure the reports will be delivered successfully?

    a. enable Fastpass
    b. add an entry to Third Party Good Senders
    c. lower Suspect Spam Threshold
    d. add an entry to Local Good Sender Domains

14. Outgoing messages need to be checked for specific words and phrases. Any messages containing the listed words should be held for review.

    Which content filtering resource is used for this requirement?

    a. Directories
    b. Dictionaries
    c. Notifications
    d. Annotations

15. An administrator configures the Symantec DLP Connect feature in Symantec Messaging Gateway. All outbound messages must be processed by Symantec Data Loss Prevention (DLP) so the bypass setting was disabled.

    What will happen to outbound messages if Symantec DLP Network Prevent servers are temporarily unavailable?

    a. Messages will be deferred until a DLP server is available.
    b. Messages will be held in the delivery queue until a DLP server is available.
    c. Messages will be held as informational incidents until a DLP server is available.
    d. Messages will be held as quarantine incidents until a DLP server is available.

16. Before performing a software update of Symantec Messaging Gateway, which option is used to view thedetails of the software update?

    a. View Manifest
    b. View Description
    c. View Metadata
    d. View Notes

17. Which feature of Symantec Messaging Gateway detects Non-Delivery Reports (NDR) created by an attacker?

    a. directory harvest attack prevention
    b. bot attack prevention
    c. bounce attack prevention
    d. denial of service attack prevention

18. Which log will help identify problems with downloading antivirus filters?

    a. Conduit log
    b. Java LiveUpdate (JLU) controller log
    c. Java LiveUpdate (JLU) server log
    d. Brightmail server log

19. An administrator learns that a user is receiving spam while other user's spam is being quarantined. After using the Message Audit logs to review the missed spam, the administrator finds that the user is opted out of antispam protection.

    Which section of the Message Audit Log detail page would provide this information?

    a. Verdict
    b. Tracker
    c. Actions Taken
    d. Untested Verdicts

20. After Symantec Messaging Gateway checks a message for its reputation, what is the next filtering phase?

    a. spam filtering
    b. virus filtering
    c. content filtering
    d. regex filtering

Answers

1-b, 2-a, 3-b&d, 4-d, 5-d, 6-a, 7-a&e, 8-b, 9-b, 10-b, 11-b, 12-b, 13-d, 14-b, 15-b, 16-b, 17-c, 18-b, 19-d, 20-b

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com