

KillTest

Higher Quality, Better Service!



Q&A

<http://www.killtest.com>

We offer free update service for one year.

Exam : **ST0-079**

Title : Symantec Brightmail
Gateway 8.0 (STS)

Version : DEMO

1. In addition to storing messages for Spam Quarantine and Suspect Virus Quarantine, which type of messages can the Control Center store?

- A.notification messages
- B.compliance triggered messages
- C.delivered messages
- D.deleted messages

ANSWER: B

2. To reach Message Audit logs, which tab should be selected in the Brightmail Control Center?

- A.Status
- B.Administration
- C.Reports
- D.Compliance

ANSWER: A

3. Which feature requires Invalid Recipient Handling to be enabled?

- A.Bounce Attack Prevention
- B.Directory Harvest Attack recognition
- C.Reputation Lookup
- D.Fastpass

ANSWER: B

4. An administrator has navigated through Status -> LDAP Synchronization.
Which tab will display details about an LDAP Synchronization?

- A.LDAP to Scanners
- B.LDAP to CC
- C.LDAP Status
- D.CC to LDAP

ANSWER: B

5. A client needs to import structured customer data.
Which resource is used for this requirement?

- A.records
- B.dictionaries
- C.regular expressions
- D.patterns

ANSWER: A

6. What does the Fastpass feature do?

- A.skips virus scanning for known viruses
- B.skips resource intensive spam scanning steps
- C.passes incoming mail directly to the downstream MTA
- D.bypasses scanning on outgoing mail

ANSWER: B

7. Which feature of Symantec Brightmail Gateway 8.0 detects Non-Delivery Reports (NDR) created by an attacker?

- A.Directory Harvest Attack
- B.Anti-Phishing Filter
- C.Bounce Attack Prevention
- D.Symantec Probe Network

ANSWER: C

8. What is the Heuristic Detection (Bloodhound) feature designed to detect?

- A.unknown viruses
- B.fuzzy matches against compliance rules
- C.regex matches
- D.Denial of Service (DoS) attacks

ANSWER: B

9. What happens to a message that is forwarded to the Suspect Virus Quarantine?

- A.It is automatically deleted after one week.
- B.It is rescanned when the configured hold time has elapsed.
- C.It is placed in the administrator's queue for review.
- D.It is forwarded to Symantec Security Response.

ANSWER: B

10. True file typing is a feature used to combat which behavior?

- A.spamming
- B.renaming
- C.phishing
- D.spimming

ANSWER: B

11. Which two email authentication technologies are included in Symantec Brightmail Gateway 8.0? (Select two.)

- A.Sender ID
- B.POP before SMTP
- C.Domain Keys Identified Mail (DKIM)
- D.Certified Email
- E.Sender Policy Framework (SPF)

ANSWER: AE

12. Spam Rule sets are automatically downloaded from Symantec on a regular basis.

How often are these rule sets refreshed?

- A.every 5 to 10 minutes
- B.every 30 to 60 minutes
- C.every 3 to 5 hours

D.every day

ANSWER: A

13. Which two tasks are performed by the SMTP session component of the MTA? (Select two.)

- A.It verifies the IP address reputation with the BMServer.
- B.It performs aliasing/masquerading for messages.
- C.It reports the message as spam.
- D.It applies the specified queue thresholds.
- E.It interacts with the BMServer to access the filtering modules.

ANSWER: BD

14. Which service retrieves new and updated email filters from Symantec Security Response through HTTPS file transfer?

- A.LiveUpdate
- B.Conduit
- C.Brightmail Engine
- D.MTA

ANSWER: B

15. What are two functions of the Control Center? (Select two.)

- A.It provides message management services.
- B.It routes messages for delivery.
- C.It hosts Spam Quarantine.
- D.It downloads virus definitions.
- E.It runs filters.

ANSWER: AC

16. 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.Accept but do not scan incoming messages

ANSWER: B

17. 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.Accept and deliver messages normally
- B.Pause message scanning and delivery
- C.Do not accept incoming messages
- D.Accept but do not scan incoming messages

ANSWER: C

18. What are two parts of the Control Center? (Select two.)

- A.Message Store

- B.LDAP Sync Service
- C.Brightmail Engine
- D.LiveUpdate Conduit
- E.Suspect Virus Quarantine

ANSWER: BE

19. What is the recommended hard-drive size for a scanner-only virtual machine?

- A.60GB
- B.80GB
- C.100GB
- D.160GB

ANSWER: A

20. What is the minimum required memory size for virtual machine deployments?

- A.1GB
- B.2GB
- C.4GB
- D.6GB

ANSWER: B