ST0-079
Symantec Brightmail Gateway 8.0 (STS)

Version 13.5

ST0-079

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 10

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

A. spamming
B. renaming

C. phishing
D. spimming

Answer: B

QUESTION NO: 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: A, E

QUESTION NO: 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

QUESTION NO: 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: B, D

QUESTION NO: 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

QUESTION NO: 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: A, C

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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: B, E

QUESTION NO: 19

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

A. 60GB
B. 80GB