ST0-097

Symantec Brightmail Gateway 9.0 (STS)

Version 14.30

ST0-097

Topic 1, Volume A

QUESTION NO: 1

In which two situations are multiple group policies useful? (Select two.)

A. when the entire organization wants to delete spam

B. when only the Human Resources department wants to receive spam

C. when only the Engineering department wants to keep message logs

D. when only the Legal department should be allowed to send archive files

E. when all of the departments want to scan outbound messages

Answer: B, D

QUESTION NO: 2

Which two actions must be taken to allow end-users to create personal Good and Bad Senders lists? (Select two.)

A. add "Hold message in Spam Quarantine" action to Local Bad Senders domains

B. check the option "Enable end-user settings for this policy group"

C. configure an LDAP source with Authentication and Recipient Validation functions

D. configure an LDAP source with Authentication and Routing functions

E. configure an LDAP source with Authentication and Address Resolution functions

Answer: B, E

QUESTION NO: 3

ST0-097

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

A. Invalid Senders

B. Sender HELO domains

C. Sender IP connections

D. Invalid Recipients

Answer: D

QUESTION NO: 4

What is the default report data retention period?

A. 7 days

B. 14 days

C. 30 days

D. 60 days

Answer: A

QUESTION NO: 5

What is the maximum number of rows a report can have?

A. 100 rows

B. 1,000 rows

C. 10,000 rows

D. 100,000 rows

Answer: B

QUESTION NO: 6

A company uses multiple control centers. What must be done to ensure legitimate NDRs are recognized by Bounce Attack Prevention across all scanners?

A. configure the same seed value on each control center

B. configure different seed values on each control center

C. configure the same seed value on each scanner

D. configure different seed values on each scanner

Answer: A

QUESTION NO: 7

During which phase of inbound message flow does Symantec Brightmail Gateway 9.0 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

QUESTION NO: 8

ST0-097

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

A. It provides message management services.

B. It downloads spam definitions.

C. It hosts Spam Quarantine.

D. It downloads virus definitions.

E. It runs filters.

Answer: A, C

QUESTION NO: 9

During which phase of outbound message flow does Symantec Brightmail Gateway 9.0 determine whether the number of recipients exceeds the good number of recipients per message?

A. message routing

B. message delivery

C. outbound SMTP session

D. outbound SMTP connection

Answer: C

QUESTION NO: 10

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. flush incoming messages

Answer: C

QUESTION NO: 11

What is the new encryption action introduced in Symantec Brightmail Gateway 9.0?

A. deliver messages with S/MIME encryption

B. deliver messages with content encryption

C. deliver messages with envelope encryption

D. deliver messages with PGP encryption

Answer: B

QUESTION NO: 12

Symantec Brightmail Gateway 9.0 includes a new policy-based encryption feature. How is this new feature licensed?

A. The license is included with Symantec Protection Suite.

B. The license is included with Symantec Brightmail Gateway 9.0.

C. The license is included with Symantec Content Encryption.

D. The license is included with Symantec Endpoint Encryption.

Answer: C

QUESTION NO: 13

Which Symantec Brightmail Gateway 9.0 feature improves responsiveness to new spam threats and increases overall antispam effectiveness?

A. rapid release definitions

B. Fastpass

C. microupdates

D. real time updates

Answer: D

QUESTION NO: 14

An administrator needs to determine whether a sending MTA is being throttled by Symantec Brightmail Gateway 9.0. Where is this information located?

A. Reputation Summary report

B. IP reputation lookup table

C. SMTP server logs

D. message audit logs

Answer: B

QUESTION NO: 15

What are the Symantec Global Bad and Good Sender lists based on?

A. reputation data from Symantec Global Services

B. reputation data from a global Symantec LiveUpdate server

C. reputation data from the Symantec Global Intelligence Network

D. global reputation data from Symantec Protection Center

Answer: C

QUESTION NO: 16

Which feature, when enabled through the directory data sources, allows third party MTAs the ability to relay through Symantec Brightmail Gateway 9.0 and protects it against becoming an open relay?

A. MTA verification

B. address validation

C. TLS certificate authentication

D. SMTP authentication

Answer: D

QUESTION NO: 17

Which Symantec Brightmail Gateway 9.0 feature will change the original domain of an internal user relaying mail outside of an organization?

A. address masquerading

B. address aliasing

C. domain mapping

D. content filtering

Answer: D

QUESTION NO: 18

ST0-097

An organization is receiving spam because of small targeted attacks from unknown senders. Which Symantec Brightmail Gateway 9.0 feature should help slow down these types of attacks?

A. dictionary attack prevention

B. directory harvest attack prevention

C. global reputation analysis

D. connection classification

Answer: D

QUESTION NO: 19

What is required before attempting installation of the Symantec Brightmail Gateway 9.0 appliance?

A. console access to the appliance

B. hostname for default gateway

C. hostname, port, username, and password for proxy

D. two IP addresses for each appliance

Answer: A

QUESTION NO: 20

Which TCP port is used for communication between the Control Center and the scanner(s)?

A. 41001

B. 41002

C. 41004

D. 41008

Answer: B

QUESTION NO: 21

There is a firewall in place between Symantec Brightmail Gateway 9.0 and the Internet at the customer site. An administrator needs to use an external NTP server on the Internet for time synchronization. Which port must be open on the firewall to allow this?

A. 120

B. 121

C. 122

D. 123

Answer: D

QUESTION NO: 22

What happens if a Symantec Brightmail Gateway scanner is behind another internal messaging gateway?

A. Symantec Brightmail Gateway scanners might quarantine all mail from the internal gateway MTA if DKIM is disabled.

B. Symantec Brightmail Gateway scanners might identify the IP address of the internal gateway MTA as a source of spam.

C. Symantec Brightmail Gateway scanners will trust all mail from the internal gateway MTA.

D. Symantec Brightmail Gateway scanners will grant the internal gateway MTA a Fastpass.

Answer: B