

Fortinet NSE6_FML-5.3.8 Exam

Volume: 30 Questions

Question: 1

Examine the nslookup output shown in the exhibit; then answer the question below.

```
C:\>nslookup -type=mx example.com
Server: PriNS
Address: 10.200.3.254

Non-authoritative answer:
example.com      MX preference = 10, mail exchanger = mx.hosted.com
example.com      MX preference = 20, mail exchanger = mx.example.com
```

Identify which of the following statements is true regarding the example.com domain's MTAs. (Choose two.)

- A. External MTAs will send email tomx.example.com only if mx.hosted.com is unreachable.
- B. The primary MTA for the example.com domain is mx.hosted.com.
- C. The PriNS server should receive all email for the example.com domain.
- D. The higher preference value is used to load balance more email to the mx.example.com MTA.

Answer: C,D

Question: 2

Which of the following CLI commands, if executed, will erase all data on the log disk partition? (Choose two.)

- A. execute formatmaildisk
- B. execute formatmaildisk_backup
- C. execute formatlogdisk
- D. execute partitionlogdisk 40

Answer: D

Question: 3

Which of the following statements regarding SMTPS and SMTP over TLS are true? (Choose three.)

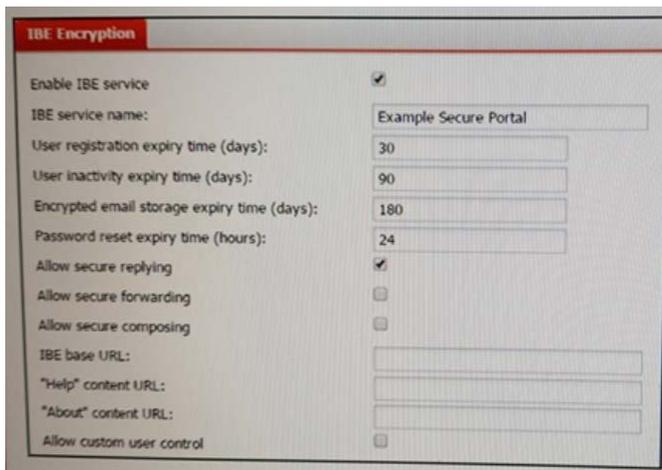
Fortinet NSE6 FML-5.3.8 Exam

- A. In an SMTPS session, the identities of both sender and receiver are encrypted.
- B. SMTPS connections are initiated on port 465.
- C. SMTP over TLS connections are entirely encrypted and initiated on port 465.
- D. The STARTTLS command is used to initiate SMTP over TLS.
- E. SMTPS encrypts the body of the email message, where the most sensitive content exists.

Answer: A,B,D

Question: 4

Examine the FortiMail IBE service configuration shown in the exhibit; then answer the question below.



The screenshot shows the 'IBE Encryption' configuration page. The 'Enable IBE service' checkbox is checked. The 'IBE service name' is 'Example Secure Portal'. The 'User registration expiry time (days)' is 30, 'User inactivity expiry time (days)' is 90, 'Encrypted email storage expiry time (days)' is 180, and 'Password reset expiry time (hours)' is 24. The 'Allow secure replying' checkbox is checked, while 'Allow secure forwarding', 'Allow secure composing', and 'Allow custom user control' are unchecked. There are also fields for 'IBE base URL', 'Help content URL', and 'About content URL'.

Which of the following statements describes the User inactivity expiry time of 90 days?

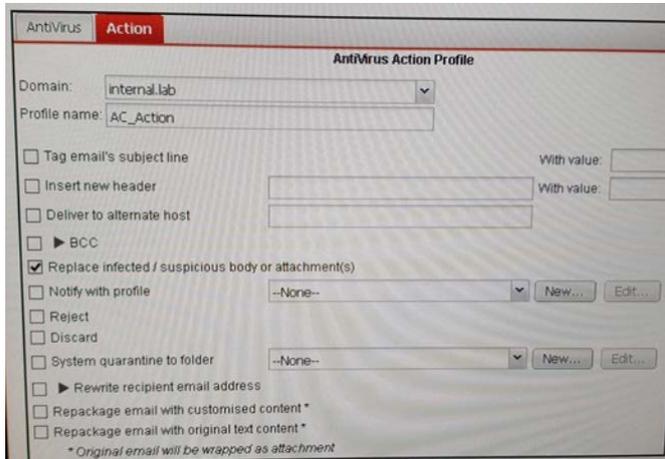
- A. First time IBE users must register to access their email within 90 days of receiving the notification mail message.
- B. After initial registration, IBE users can access the secure portal without authenticating again for 90 days.
- C. Registration IBE users have 90 days from the time they receive a notification email message to access their IBE email.
- D. IBE user accounts will expire after 90 days of inactivity, and must register again to access new IBE email message.

Answer: D

Fortinet NSE6 FML-5.3.8 Exam

Question: 5

Examine the FortiMail antivirus action profile shown in the exhibit; then answer the question below.



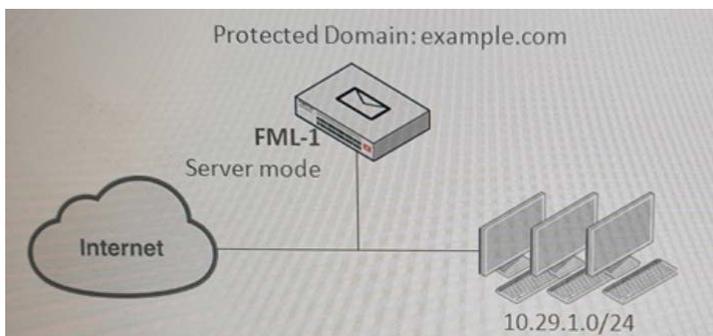
What is the expected outcome if FortiMail applies this action profile to an email? (Choose two.)

- A. The sanitized email will be sent to the recipient's personal quarantine.
- B. A replacement message will be added to the email.
- C. Virus content will be removed from the email.
- D. The administrator will be notified of the virus detection.

Answer: B,C

Question: 6

Examine the FortiMail topology and access receive rule shown in the exhibit; then answer the question below.



Fortinet NSE6_FML-5.3.8 Exam

The screenshot shows the 'Access Control Rule' configuration window in FortiMail. The 'Enabled' checkbox is checked. The 'Sender pattern' is set to 'User Defined' with a dropdown menu and a text box containing '*'. There are 'Regular expression' checkboxes for both 'Sender pattern' and 'Recipient pattern', both of which are unchecked. The 'Recipient pattern' is also set to 'User Defined' with a dropdown menu and a text box containing '*'. The 'Sender IP/netmask' is set to 'User Defined' with a dropdown menu and a text box containing '0.0.0.0 / 0'. The 'Reverse DNS pattern' is set to 'User Defined' with a dropdown menu and a text box containing '*'. There are 'Regular expression' checkboxes for both 'Sender IP/netmask' and 'Reverse DNS pattern', both of which are unchecked. The 'Authentication status' is set to 'Any' with a dropdown menu. The 'TLS profile' is set to '--None--' with a dropdown menu and 'New...' and 'Edit...' buttons. The 'Action' is set to 'Reject' with a dropdown menu. There is a 'Comments' text area at the bottom. 'Create' and 'Cancel' buttons are at the bottom left.

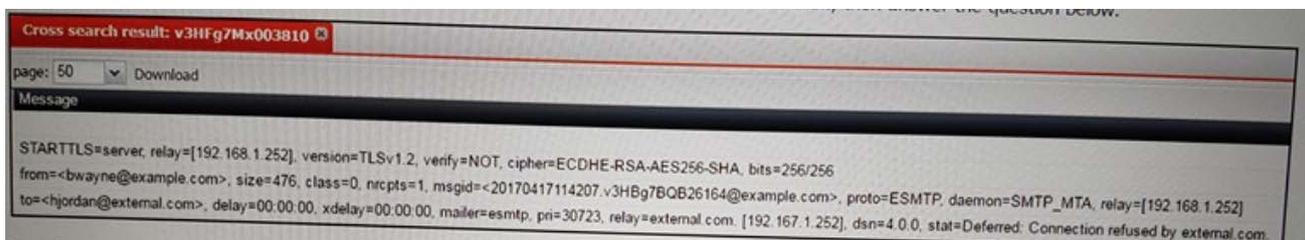
An administrator must enforce authentication on FML-1 for all outbound email from the example.com domain. Which of the following settings should be used to configure the access receive rule? (Choose two.)

- A. The Sender IP/netmask should be set to 10.29.1.0/24.
- B. The Authentication status should be set to Authenticated.
- C. The Recipient pattern should be set to *@example.com.
- D. The Action should be set to Reject.

Answer: C,D

Question: 7

Examine the message column of a log cross search result of an inbound email shown in the exhibit; then answer the question below:



Based on the logs, which of the following statements are true? (Choose two.)

- A. The FortiMail is experiencing issues delivering the email to the back-end mail server.
- B. The logs were generated by a sever mode FortiMail.

Fortinet NSE6 FML-5.3.8 Exam

C. The logs were generated by a gateway or transparent mode FortiMail.

D. The FortiMail is experiencing issues accepting the connection from the remote sender.

Answer: D

Question: 8

An organization has different groups of users with different needs in email functionality, such as address book access, mobile device access, email retention periods, and disk quotas. Which FortiMail feature specific to server mode can be used to accomplish this?

A. Resource profile.

B. Address Book Management options

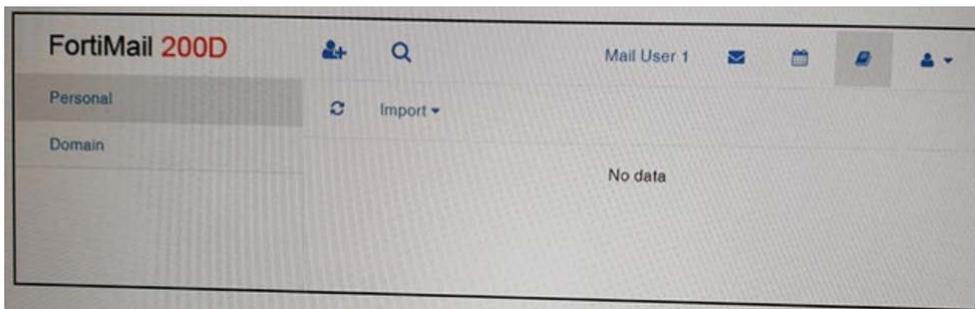
C. Access profile

D. Domain-level service settings.

Answer: D

Question: 9

Examine the FortiMail user webmail interface shown in the exhibit; then answer the question below.



Which one of the following statements is true regarding this server mode FortiMail's configuration?

A. The protected domain-level service settings have been modified to allow access to the domain address book.

B. This user's account has a customized access profile applied that allows access to the personal address book.