

DUMPSBOSS.COM

Fortinet NSE 6 - FortiMail 6.2

Fortinet NSE6 FML-6.2

Version Demo

Total Demo Questions: 5

Total Premium Questions: 32

Buy Premium PDF

<https://dumpsboss.com>

support@dumpsboss.com

dumpsboss.com

QUESTION NO: 1

Which FortiMail option removes embedded code components in Microsoft Word, while maintaining the original file format?

- A. Behavior analysis
- B. Impersonation analysis
- C. Content disarm and reconstruction
- D. Header analysis

ANSWER: C**Explanation:**

Reference: <https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/8c063dd3-bafe-11e9-a989-00505692583a/fortimail-admin-620.pdf> (435)

QUESTION NO: 2

Refer to the exhibit.

Message Scan Rule

Name:

Description:

☒ Conditions

Match all conditions **Match any condition**

+ New... **Edit...** **Delete**

ID	Condition
1	Body contains sensitive data "Credit_Card_Number"
2	Attachment contains sensitive data "Credit_Card_Number"
3	Subject contains Credit Card

☒ Exceptions

+ New... **Edit...** **Delete**

ID	Condition
1	Sender contains sales@example.com

Which two message types will trigger this DLP scan rule? (Choose two.)

A. An email message with a subject that contains the term "credit card" will trigger this scan rule

- B. An email that contains credit card numbers in the body, attachment, and subject will trigger this scan rule
- C. An email message that contains credit card numbers in the body will trigger this scan rule
- D. An email sent from sales@internal.lab will trigger this scan rule, even without matching any conditions

ANSWER: B C

QUESTION NO: 3

A FortiMail is configured with the protected domain example.com.

On this FortiMail, which two envelope addresses are considered incoming? (Choose two.)

- A. MAIL FROM: accounts@example.com RCPT TO: sales@external.org
- B. MAIL FROM: support@example.com RCPT TO: marketing@example.com
- C. MAIL FROM: training@external.org RCPT TO: students@external.org
- D. MAIL FROM: mis@hosted.net RCPT TO: noc@example.com

ANSWER: C D

Explanation:

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9aa62d26-858d-11ea-9384-00505692583a/FortiMail-6.4.0-Administration_Guide.pdf (30)

QUESTION NO: 4

Refer to the exhibit.



Which statement describes the impact of setting the User inactivity expiry time option to 90 days?

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

ANSWER: A

Explanation:

Reference: https://docs.fortinet.com/document/fortimail/6.4.0/cli-reference/813529/system-encryption-ibe#config_3733402351_2450215

QUESTION NO: 5

Refer to the exhibit.

Sender Reputation		Authentication Reputation		Endpoint Reputation	
⌂		« < 1 — / 1 > »		Records per page: 50 ▼	
IP		Score			
10.0.1.254		15			

Which configuration change must you make to block an offending IP address temporarily?

- A. Add the offending IP address to the system block list
- B. Add the offending IP address to the user block list
- C. Add the offending IP address to the domain block list
- D. Change the authentication reputation setting status to Enable

ANSWER: D

Explanation:

Reference: <https://help.fortinet.com/fweb/550/Content/FortiWeb/fortiweb-admin/blacklisting.htm>