



# NSE6\_FML-6.2<sup>Q&As</sup>

Fortinet NSE 6 - FortiMail 6.2

## Pass Fortinet NSE6\_FML-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

[https://www.geekcert.com/nse6\\_fml-6-2.html](https://www.geekcert.com/nse6_fml-6-2.html)

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

What three configuration steps are required to enable DKIM signing for outbound messages on FortiMail? (Choose three.)

- A. Generate a public/private key pair in the protected domain configuration
- B. Enable DKIM check in a matching session profile
- C. Enable DKIM check in a matching antispam profile
- D. Publish the public key as a TXT record in a public DNS server
- E. Enable DKIM signing for outgoing messages in a matching session profile

Correct Answer: ABD

---

### QUESTION 2

FortiMail is configured with the protected domain example.com.

Which two envelope addresses will require an access receive rule, to relay for unauthenticated senders? (Choose two.)

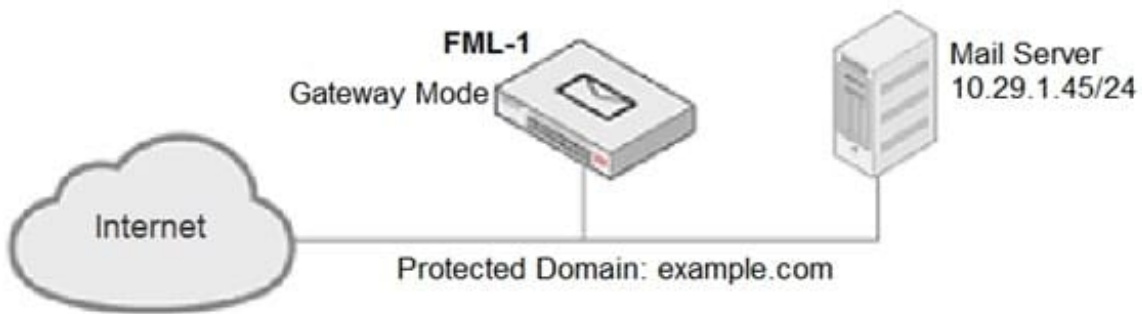
- A. MAIL FROM: accounts@example.com RCPT TO: sales@external.org
- B. MAIL FROM: support@example.com RCPT TO: marketing@example.com
- C. MAIL FROM: training@external.org RCPT TO: students@external.org
- D. MAIL FROM: mis@hosted.net RCPT TO: noc@example.com

Correct Answer: BD

---

### QUESTION 3

Refer to the exhibit.



Access Control Rule

Enabled	<input checked="" type="checkbox"/>
Sender:	User Defined *
Recipient:	User Defined *
Source:	IP/Netmask 0.0.0.0/0
Reverse DNS pattern:	* <input type="checkbox"/> Regular Expression
Authentication status:	Any
TLS profile:	--None-- <input type="button" value="+ New..."/> <input type="button" value="Edit..."/>
Action:	Reject
Comments:	

It is recommended that you configure which three access receive settings to allow outbound email from the example.com domain on FML-1? (Choose three.)

- A. The Sender pattern should be set to \*@example.com
- B. The Action should be set to Relay
- C. The Recipient pattern should be set to 10.29.1.45/24
- D. The Enable check box should be cleared
- E. The Sender IP/netmask should be set to 10.29.1.45/32



Correct Answer: BDE

#### QUESTION 4

Refer to the exhibit.

### IBE Encryption

Enable IBE service	<input checked="" type="checkbox"/>
IBE service name:	<input type="text" value="Example Secure Portal"/>
User registration expiry time (days):	<input type="text" value="30"/>
User inactivity expiry time (days):	<input type="text" value="90"/>
Encrypted email storage expiry time (days):	<input type="text" value="180"/>
Password reset expiry time (hours):	<input type="text" value="24"/>
Allow secure replying	<input checked="" type="checkbox"/>
Allow secure forwarding	<input type="checkbox"/>
Allow secure composing	<input type="checkbox"/>
IBE base URL:	<input type="text"/>
"Help" content URL:	<input type="text"/>
"About" content URL:	<input type="text"/>
Allow custom user control	<input type="checkbox"/>

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

Correct Answer: A

Reference: [https://docs.fortinet.com/document/fortimail/6.4.0/cli-reference/813529/system-encryptionibe#config\\_3733402351\\_2450215](https://docs.fortinet.com/document/fortimail/6.4.0/cli-reference/813529/system-encryptionibe#config_3733402351_2450215)

#### QUESTION 5

Refer to the exhibit.



Sender Reputation	Authentication Reputation	Endpoint Reputation
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

Correct Answer: D

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

[NSE6\\_FML-6.2 PDF Dumps](#) [NSE6\\_FML-6.2 VCE Dumps](#) [NSE6\\_FML-6.2 Braindumps](#)