

# Fortinet

## Exam Questions NSE6\_FML-6.4

Fortinet NSE 6 - FortiMail 6.4



**NEW QUESTION 1**

Refer to the exhibit.

Active User						
Expired User						
Secure Question						
IBE Authentication						
IBE Domain						
<input type="button" value="Delete"/> <input type="button" value="Maintenance"/> <input type="button" value="Reset User"/>						
<input type="button" value="Refresh"/> <input type="button" value="Previous"/> <input type="text" value="1 / 1"/> <input type="button" value="Next"/> <input type="button" value="Records per page: 50"/> <input type="text" value="IBE domain: --All--"/> <input type="text" value="Search:"/>						
Enabled	Email	First Name	Last Name	Status	Creation Time	Last Access
<input checked="" type="checkbox"/>	extuser@external.lab	Mail	User	Activated	Wed, 05 Sep 2018 12:05:47 PDT	Wed, 05 Sep 2018 12:38:56 PDT
<input checked="" type="checkbox"/>	extuser2@external.lab			Pre-registered	Wed, 05 Sep 2018 12:41:32 PDT	Wed, 05 Sep 2018 12:41:32 PDT

Which statement describes the pre-registered status of the IBE user extuser2@external.lab?

- A. The user has received an IBE notification email, but has not accessed the HTTPS URL or attachment yet.
- B. The user account has been de-activated, and the user must register again the next time they receive an IBE email.
- C. The user was registered by an administrator in anticipation of IBE participation.
- D. The user has completed the IBE registration process, but has not yet accessed their IBE email.

**Answer:** D

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortimail/6.4.2/administrationguide/470401/configuring-ibe-users>

**NEW QUESTION 2**

An administrator sees that an excessive amount of storage space on a FortiMail device is being used up by quarantine accounts for invalid users. The FortiMail is operating in transparent mode. Which two FortiMail features can the administrator configure to tackle this issue? (Choose two.)

- A. Automatic removal of quarantine accounts
- B. Recipient address verification
- C. Bounce address tag verification
- D. Sender address rate control

**Answer:** AD

**Explanation:**

Reference: [https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9aa62d26-858d-11ea-9384-00505692583a/FortiMail-6.4.0-Administration\\_Guide.pdf](https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9aa62d26-858d-11ea-9384-00505692583a/FortiMail-6.4.0-Administration_Guide.pdf) (322, 323)

**NEW QUESTION 3**

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

**Answer:** BD

**NEW QUESTION 4**

Which two antispam techniques query FortiGuard for rating information? (Choose two.)

- A. DNSBL
- B. SURBL
- C. IP reputation
- D. URI filter

**Answer:** AB

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortimail/6.4.0/administrationguide/352990/configuring-antispam-profiles-and-antispam-action-profiles>

**NEW QUESTION 5**

Which three statements about SMTPS and SMTP over TLS are true? (Choose three.)

- A. SMTP over TLS connections are entirely encrypted and initiated on port 465
- B. SMTPS encrypts the identities of both the sender and receiver
- C. The STARTTLS command is used to initiate SMTP over TLS
- D. SMTPS encrypts only the body of the email message
- E. SMTPS connections are initiated on port 465

**Answer:** BCE

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortimail/6.2.0/administrationguide/807960/fortimail-support-of-tls-ssl>

**NEW QUESTION 6**

Refer to the exhibit.

```
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
```

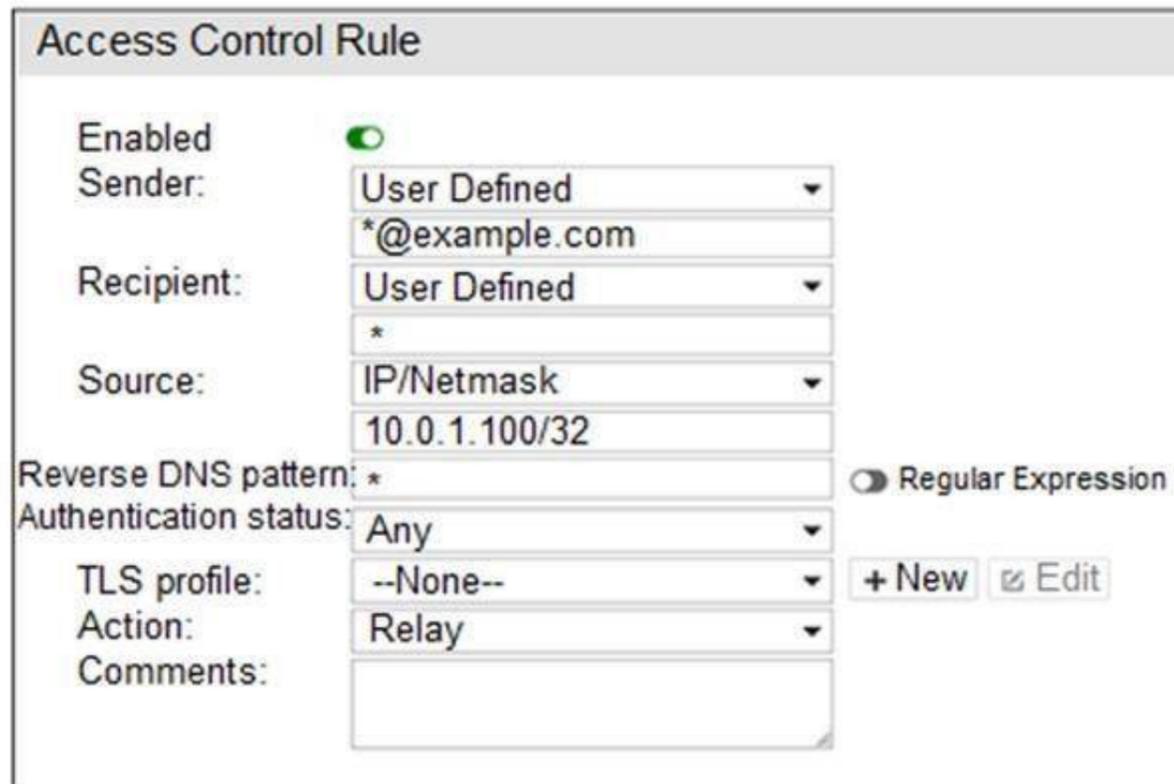
Which two statements about the MTAs of the domain example.com are true? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 7**

Refer to the exhibit.



Which two statements about the access receive rule are true? (Choose two.)

- A. Email matching this rule will be relayed
- B. Email must originate from an example.com email address to match this rule
- C. Senders must be authenticated to match this rule
- D. Email from any host in the 10.0.1.0/24 subnet can match this rule

**Answer:** AB

**NEW QUESTION 8**

If you are using the built-in MTA to process email in transparent mode, which two statements about FortiMail behavior are true? (Choose two.)

- A. MUAs need to be configured to connect to the built-in MTA to send email
- B. If you disable the built-in MTA, FortiMail will use its transparent proxies to deliver email
- C. FortiMail can queue undeliverable messages and generate DSNs
- D. FortiMail ignores the destination set by the sender, and uses its own MX record lookup to deliver email

**Answer:** CD

**NEW QUESTION 9**

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:** CD

**Explanation:**

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

**NEW QUESTION 10**

Refer to the exhibit.

**IBE Encryption**

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 10**

Refer to the exhibit.

**Session Profile**

Profile name:

**SMTP Limits**

Restrict number of EHLO/HELOs per session to:

Restrict number of email per session to:

Restrict number of recipients per email to:

Cap message size (KB) at:

Cap header size (KB) at:

Maximum number of NOOPs allowed for each connection:

Maximum number of RSETs allowed for each connection:

**FortiMail**

Domain name:

Relay type:

SMTP server:  Port:  [Test...]

Use SMTPS

Fallback SMTP server:  Port:  [Test...]

Use SMTPS

Relay Authentication

**Other**

Webmail theme:

Webmail language:

Maximum message size (KB):

SMTP greeting (EHLO/HELO) name (as client):

IP pool:  Direction:

Remove received header of outgoing email

Use global bayesian database

Bypass bounce verification

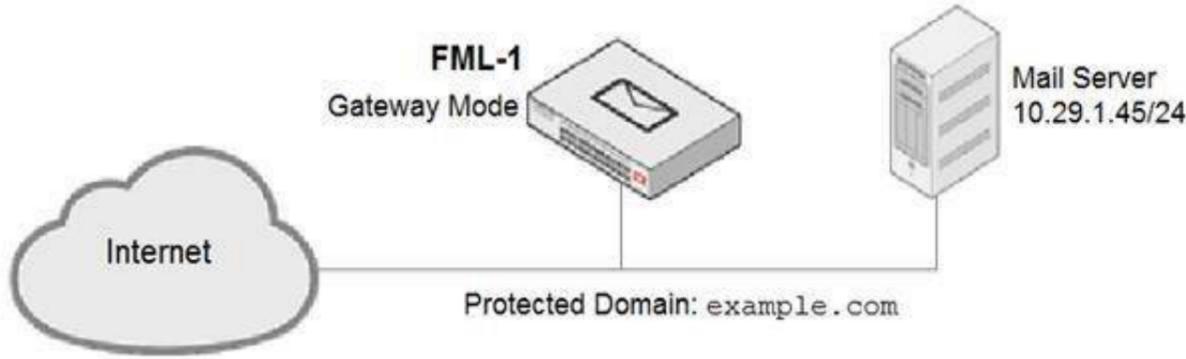
Which message size limit will FortiMail apply to the outbound email?

- A. 204800
- B. 1024
- C. 51200
- D. 10240

**Answer:** A

**NEW QUESTION 13**

Refer to the exhibit.



IP Policy											
Enabled	ID	Source	Destinati...	Session	AntiSpam	AntiVirus	Content	DLP	IP Pool	Authentication	Exclu...
<input checked="" type="checkbox"/>	1	0.0.0.0/0	0.0.0.0/0	Example Session							<input checked="" type="checkbox"/>

An administrator has enabled the sender reputation feature in the Example\_Session profile on FML- 1. After a few hours, the deferred queue on the mail server starts filling up with undeliverable email. What two changes must the administrator make to fix this issue? (Choose two.)

- A. Apply a session profile with sender reputation disabled on a separate IP policy for outbound sessions
- B. Clear the sender reputation database using the CLI
- C. Create an outbound recipient policy to bypass outbound email from session profile inspections
- D. Disable the exclusive flag in IP policy ID 1

**Answer: AD**

**NEW QUESTION 17**

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)

**NEW QUESTION 22**

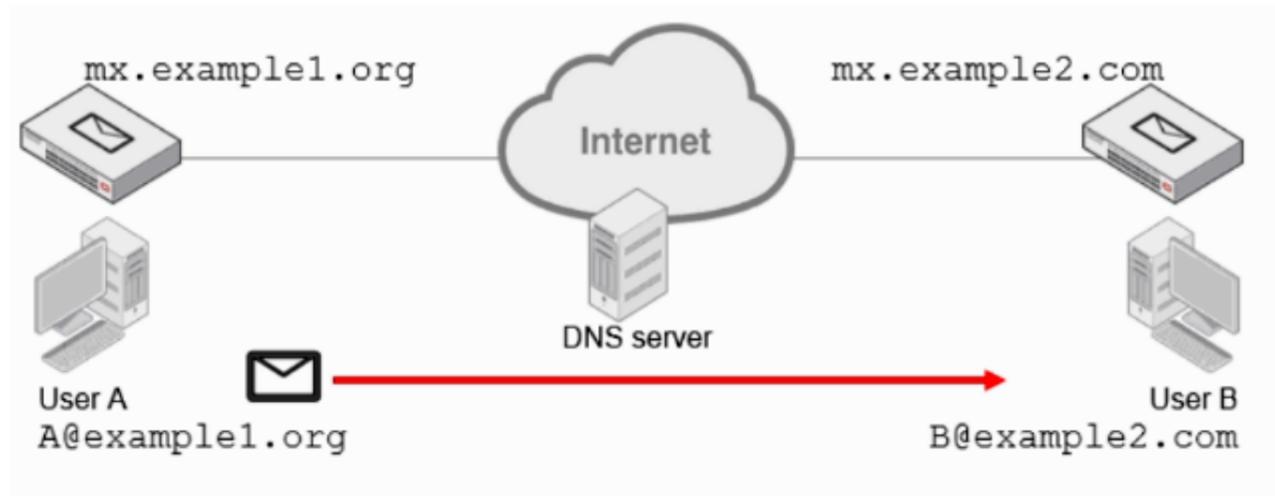
Which two features are available when you enable HA centralized monitoring on FortiMail? (Choose two.)

- A. Policy configuration changes of all cluster members from the primary device.
- B. Firmware update of all cluster members from the primary device.
- C. Cross-device log searches across all cluster members from the primary device.
- D. Mail statistics of all cluster members on the primary device

**Answer: CD**

**NEW QUESTION 26**

Refer to the exhibit.



Which two statements about email messages sent from User A to User B are correct? (Choose two.)

- A. User A's MUA will perform a DNS MX record lookup to send the email message.
- B. mx.example1.org will forward the email message to the MX record that has the lowest preference.
- C. The DNS server will act as an intermediary MTA.

D. User B will retrieve the email message using either POP3 or IMA

**Answer:** AC

**NEW QUESTION 27**

Which statement about how impersonation analysis identifies spoofed email addresses is correct?

- A. It uses behavior analysis to detect spoofed addresses.
- B. It maps the display name to the correct recipient email address.
- C. It uses DMARC validation to detect spoofed addresses.
- D. It uses SPF validation to detect spoofed addresses.

**Answer:** A

**NEW QUESTION 32**

Examine the FortiMail session profile and protected domain configuration shown in the exhibit; then answer the question below.

Which size limit will FortiMail apply to outbound email?

- A. 204800
- B. 51200
- C. 1024
- D. 10240

**Answer:** B

**Explanation:**

domain only applies to inbound. <https://kb.fortinet.com/kb/viewContent.do?externalId=FD31006&sliceId=1>

**NEW QUESTION 34**

Examine the FortiMail recipient-based policy shown in the exhibit; then answer the question below.

**Policies**

**Recipient Based Policy**

Enable

Direction: Incoming

Domain:

Comments:

---

**Sender Pattern**

Type:  @

---

**Recipient Pattern**

Type:  @

---

**Profiles**

**Authentication and Access**

Authentication type:

Authentication profile:

Use for SMTP authentication

Allow guaranteed email access through POP3

Allow guaranteed email access through webmail

After creating the policy, an administrator discovered that clients are able to send unauthenticated email using SMTP. What must be done to ensure clients cannot send unauthenticated email?

- A. Configure a matching IP policy with SMTP authentication and exclusive flag enabled
- B. Move the recipient policy to the top of the list
- C. Configure an access receive rule to verify authentication status
- D. Configure an access delivery rule to enforce authentication

**Answer: D**

**NEW QUESTION 36**

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
```

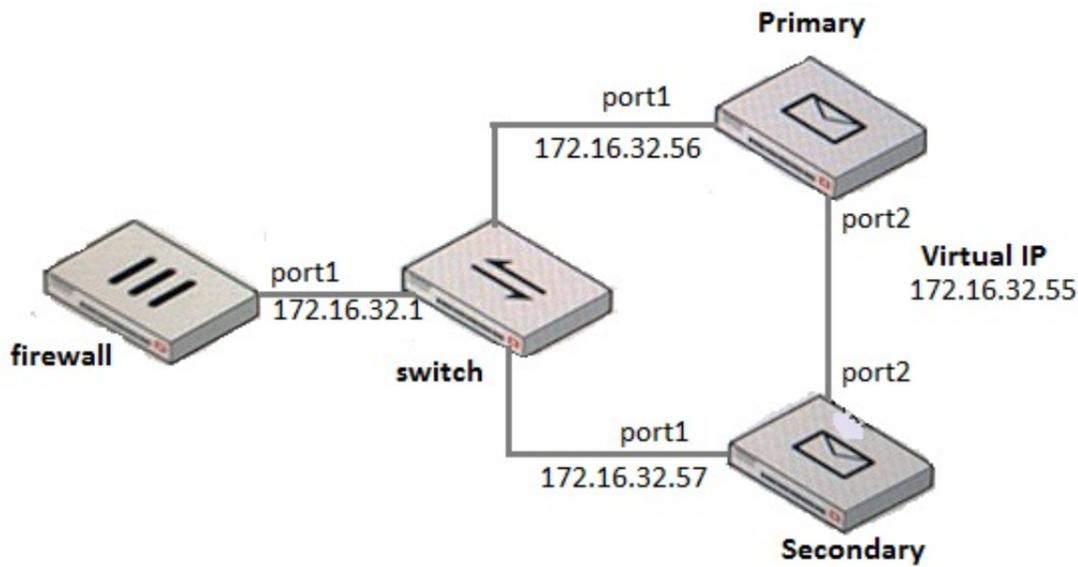
Identify which of the following statements is true regarding the example.com domain's MTAs. (Choose two.)

- A. External MTAs will send email to mx.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: AB**

**NEW QUESTION 37**

Examine the FortiMail active-passive cluster shown in the exhibit; then answer the question below.



Primary HA Interface Configuration

**HA Interface**

Port: **port1...**

Enable port monitor

Heartbeat status: **Disable**

Peer IP address: **0.0.0.0**

Peer IPv6 address: **::**

Virtual IP action: **Ignore**

Virtual IP address: **0.0.0.0** / **0**

Virtual IPv6 address: **::** / **0**

Which of the following parameters are recommended for the Primary FortiMail's HA interface configuration? (Choose three.)

- A. Enable port monitor: disable
- B. Peer IP address: 172.16.32.57
- C. Heartbeat status: Primary
- D. Virtual IP address: 172.16.32.55/24
- E. Virtual IP action: Use

Answer: CDE

**NEW QUESTION 42**

Examine the FortiMail IBE users shown in the exhibit; then answer the question below

Active User	Expired User	Secure Question	IBE Authentication	IBE Domain
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Enabled	Email	First Name	Last Name	Status	Creation Time	Last Access
<input checked="" type="checkbox"/>	njordan@external.com	Hal	Jordan	Activated	Wed, 12 Apr 2017 13:00:28 EDT	Wed, 12 Apr 2017 13:01:25 EDT
<input checked="" type="checkbox"/>	krayner@external.com			Pre-registered	Wed, 12 Apr 2017 13:02:13 EDT	Wed, 12 Apr 2017 13:02:13 EDT

Which one of the following statements describes the Pre-registered status of the IBE user krayner@external.com?

- A. The user was registered by an administrator in anticipation of IBE participation
- B. The user has completed the IBE registration process but has not yet accessed their IBE email
- C. The user has received an IBE notification email, but has not accessed the HTTPS URL or attachment yet
- D. The user account has been de-activated, and the user must register again the next time they receive an IBE email

Answer: C

**NEW QUESTION 47**

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

**FortiMail**

**Access Control Rule**

Enabled

Sender pattern:    Regular expression

Recipient pattern:    Regular expression

Sender IP/netmask:   /

Reverse DNS pattern:   Regular expression

Authentication status:

TLS profile:

Action:

Comments:

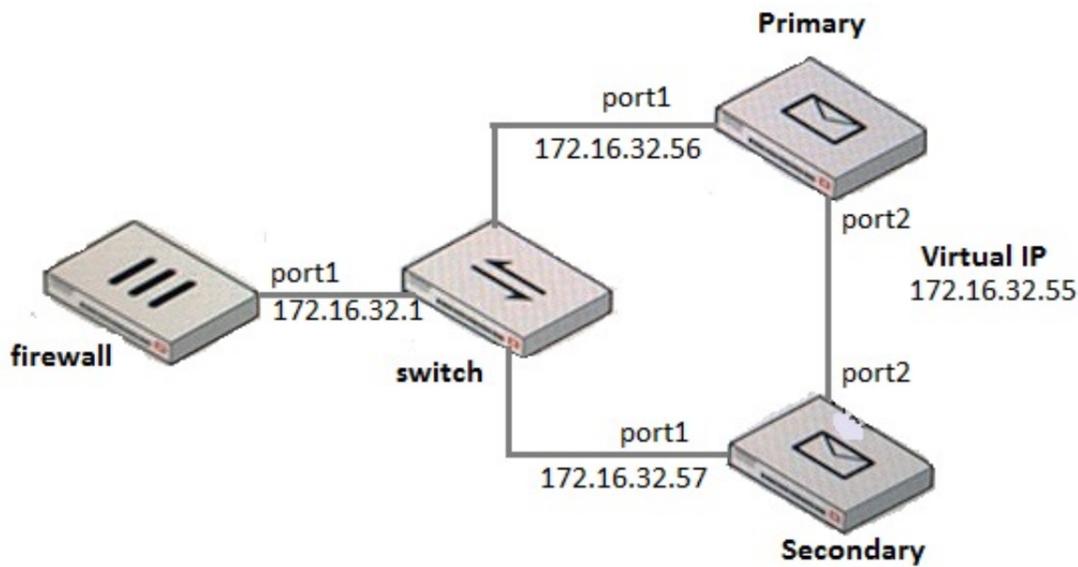
Which of the following statements are true? (Choose two.)

- A. Email from any host in the 10.0.1.0/24 subnet can match this rule
- B. Senders must be authenticated to match this rule
- C. Email matching this rule will be relayed
- D. Email must originate from an example.com email address to match this rule

**Answer: CD**

**NEW QUESTION 52**

Refer to the exhibit.



What IP address should the DNS MX record for this deployment resolve to?

- A. 172.16.32.1
- B. 172.16.32.57
- C. 172.16.32.55
- D. 172.16.32.56

**Answer: C**

**NEW QUESTION 56**

Which of the following antispam techniques queries FortiGuard for rating information? (Choose two.)

- A. URI filter
- B. IP reputation
- C. SURBL
- D. DNSBL

**Answer: AB**

**NEW QUESTION 61**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **NSE6\_FML-6.4 Practice Exam Features:**

- \* NSE6\_FML-6.4 Questions and Answers Updated Frequently
- \* NSE6\_FML-6.4 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE6\_FML-6.4 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* NSE6\_FML-6.4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE6\\_FML-6.4 Practice Test Here](#)**