



Free Questions for [NSE6_FML-7.2](#) by [certsdeals](#)

Shared by [Riley](#) on [03-08-2023](#)

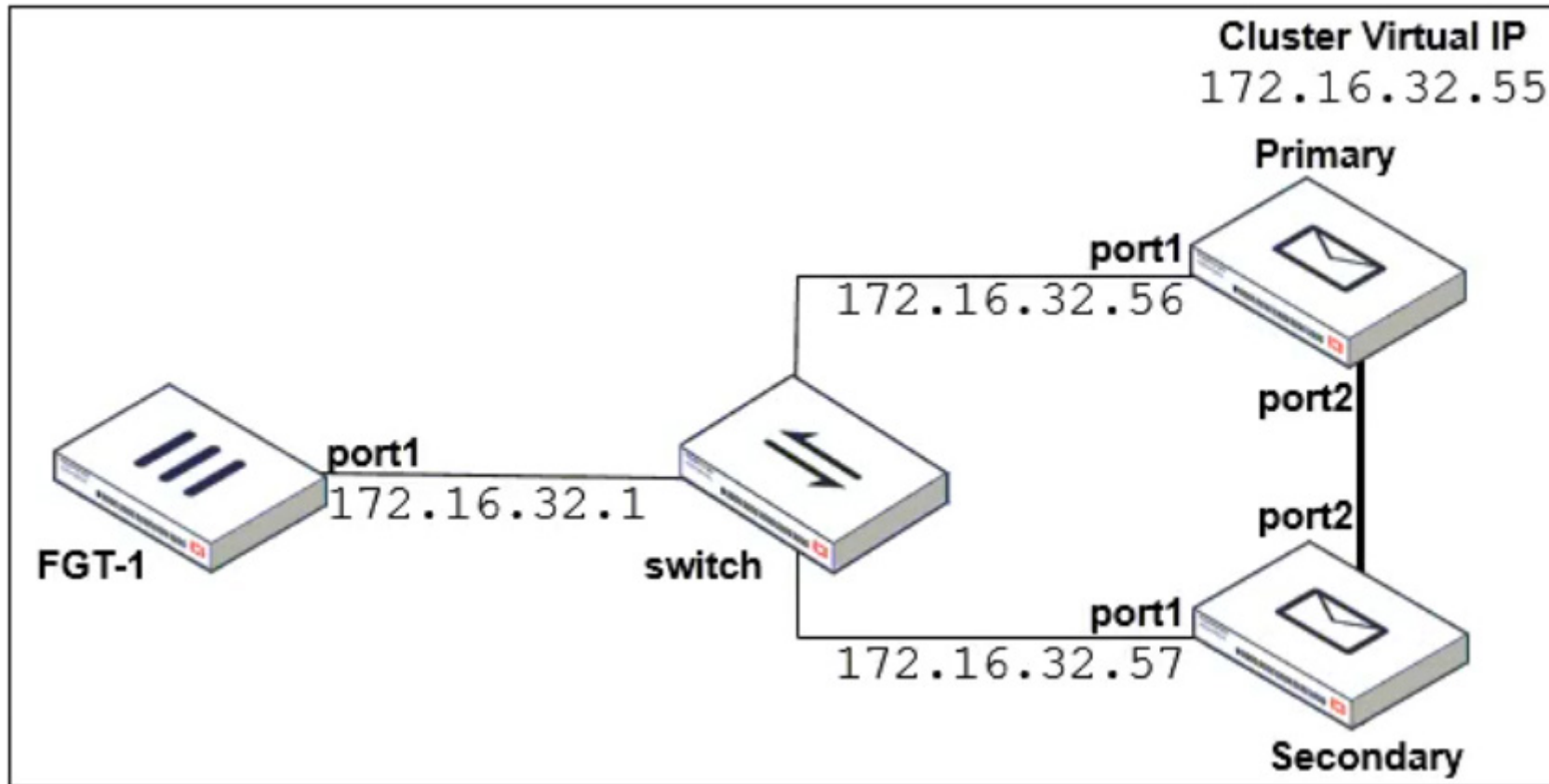
For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

Refer to the exhibit which shows a topology diagram of a FortiMail cluster deployment.



Which IP address must the DNS MX record for this organization resolve to?

Options:

A- 1172 16 32 57

B- 172.16.32.56

C- 172.16.32.55

D- 172.16.32.1

Answer:

C

Question 2

Question Type: MultipleChoice

While reviewing logs, an administrator discovers that an incoming email was processed using policy IDs 0:4:9:INTERNAL.

Which two statements describe what this policy ID means? (Choose two.)

Options:

- A- Access control policy number 9 was used.
- B- The FortiMail configuration is missing an access delivery rule.
- C- The email was processed using IP-based policy ID 4.
- D- FortiMail is applying the default behavior for relaying inbound email.

Answer:

A, C

Question 3

Question Type: MultipleChoice

Refer to the exhibit which shows an nslookup output of MX records of the example.com domain.

```
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 MTA selection behaviors for the example.com domain are correct? (Choose two.)

Options:

- A-** mx.example.com will receive approximately twice the number of email as mx.hosted.com because of its preference value.
- B-** The primary MTA for the example.com domain is mx.hosted.com.
- C-** The external MTAs will send email to mx.example.com only if mx.hosted.com is unreachable.
- D-** The PriNS server should receive all email for the example.com domain.

Answer:

B, C

Question 4

Question Type: MultipleChoice

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

Options:

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

Answer:

B

Question 5

Question Type: MultipleChoice

Which two FortiMail antispam techniques can you use to combat zero-day spam? (Choose two.)

Options:

- A- IP reputation
- B- Spam outbreak protection
- C- DNSBL
- D- Behavior analysis

Answer:

A, B

Question 6

Question Type: MultipleChoice

Refer to the exhibit which displays a history log entry.

History								System Event	Mail Event	AntiVirus	AntiSpam	Encryption
List View Search Export								2022-06-24 13:27:38 -> Current				
Refresh << < <input type="text" value="1"/> / 1 > >>								Records per page: <input type="text" value="100"/> ▼ Go to line: <input type="text"/>				
#	Date	Time	Classifier	Disposition	From	To	Subject					
1	2022-06-24	14:27:...	Not Spam	Accept	extuser@ext...	user1@intern...	Meeting minutes 24-Jun-22					

Why does the last field show SYSTEM in the Policy ID column?

Options:

- A- The email was dropped by a system blocklist.
- B- It is an inbound email.
- C- The email matched a system-level authentication policy.
- D- The email did not match a recipient-based policy.

Answer:

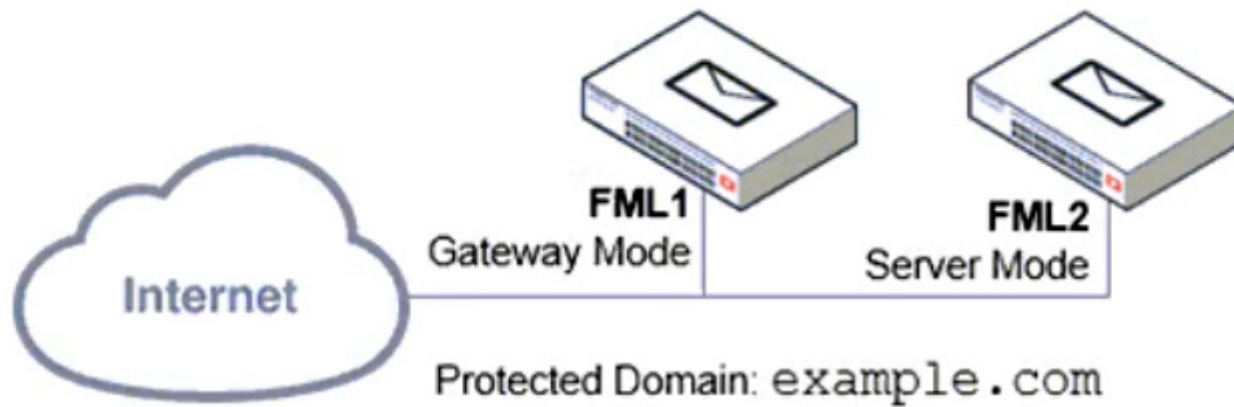
D

Question 7

Question Type: MultipleChoice

Refer to the exhibits, which display a topology diagram (Topology) and two FortiMail device configurations (FML1 Configuration and FML2 Configuration).



Topology



FML1 Configuration

FortiMail	
Domain name	<input type="text" value="example.com"/>
Is subdomain	<input type="checkbox"/>
Main domain	<input type="text"/>
Relay type	<input type="text" value="Host"/>
SMTP server	<input type="text" value="fml2.example.com"/> Port <input type="text" value="465"/> [Test...]
	<input checked="" type="checkbox"/> Use SMTPS
Fallback SMTP server	<input type="text"/> Port <input type="text" value="25"/> [Test...]
	<input type="checkbox"/> Use SMTPS

FML2 Configuration

 Local Host	
Host name	<input type="text" value="FML2"/>
Local domain name	<input type="text" value="example.com"/>
Default domain for authentication	<input type="text" value="--None--"/>
 SMTP Service <input checked="" type="checkbox"/>	
SMTP server port number	<input type="text" value="25"/>
SMTPS server port number	<input type="text" value="465"/>
SMTP over SSL/TLS	<input type="checkbox"/>
SMTP MSA service	<input checked="" type="checkbox"/>
SMTP MSA port number	<input type="text" value="587"/>
Authentication	SMTP <input type="checkbox"/> SMTPS <input checked="" type="checkbox"/> SMTP over TLS <input checked="" type="checkbox"/>

What is the expected outcome of SMTP sessions sourced from FML1 and destined for FML2?

Options:

- A- FML1 will fail to establish any connection with FML2.
- B- FML1 will attempt to establish an SMTPS session with FML2. but fail and revert to standard SMTP.
- C- FML1 will send the STARTTLS command in the SMTP session, which will be rejected by FML2.
- D- FML1 will successfully establish an SMTPS session with FML2.

Answer:

D

Question 8

Question Type: MultipleChoice

Refer to the exhibit which displays a history log entry.

History								System Event	Mail Event	AntiVirus	AntiSpam	Encryption
List		View	Search	Export				2022-06-24 13:27:38 -> Current				
Refresh	«	<	1 / 1	>	»	Records per page:	100	Go to line:				
#	Date	Time	Classifier	Disposition	From	To	Subject					
1	2022-06-24	14:27:...	Not Spam	Accept	extuser@ext...	user1@intern...	Meeting minutes 24-Jun-22					

Why does the last field show SYSTEM in the Policy ID column?

Options:

- A- The email was dropped by a system blocklist.
- B- It is an inbound email.
- C- The email matched a system-level authentication policy.
- D- The email did not match a recipient-based policy.

Answer:

D

Question 9

Question Type: MultipleChoice

Refer to the exhibit which shows an nslookup output of MX records of the example.com domain.

```
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 MTA selection behaviors for the example.com domain are correct? (Choose two.)

Options:

- A- mx.example.com will receive approximately twice the number of email as mx.hosted.com because of its preference value.
- B- The primary MTA for the example.com domain is mx.hosted.com.
- C- The external MTAs will send email to mx.example.com only if mx.hosted.com is unreachable.
- D- The PriNS server should receive all email for the example.com domain.

Answer:

B, C

Question 10

Question Type: MultipleChoice

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

Options:

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

Answer:

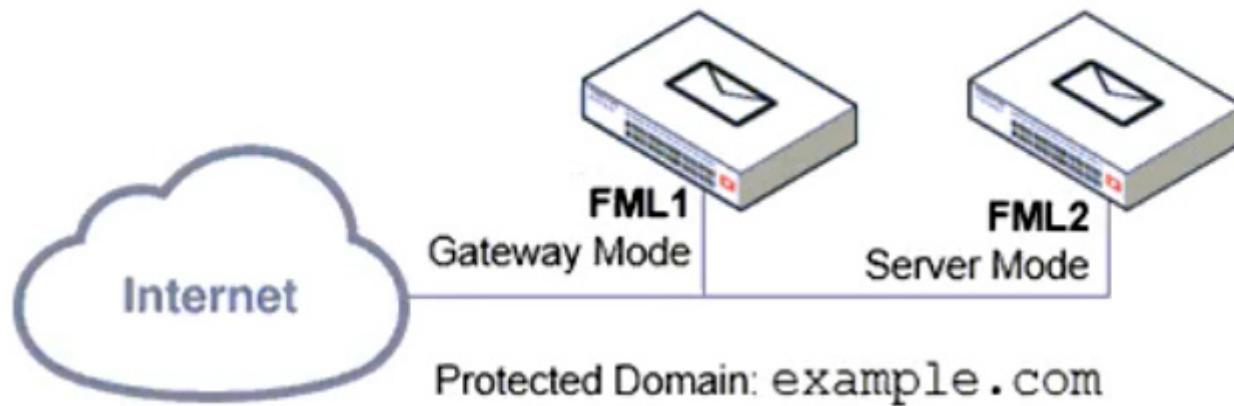
B

Question 11

Question Type: MultipleChoice

Refer to the exhibits, which display a topology diagram (Topology) and two FortiMail device configurations (FML1 Configuration and FML2 Configuration).



Topology



FML1 Configuration

FortiMail	
Domain name	<input type="text" value="example.com"/>
Is subdomain	<input type="checkbox"/>
Main domain	<input type="text"/>
Relay type	<input type="text" value="Host"/>
SMTP server	<input type="text" value="fml2.example.com"/> Port <input type="text" value="465"/> [Test...]
	<input checked="" type="checkbox"/> Use SMTPS
Fallback SMTP server	<input type="text"/> Port <input type="text" value="25"/> [Test...]
	<input type="checkbox"/> Use SMTPS

FML2 Configuration

 Local Host	
Host name	<input type="text" value="FML2"/>
Local domain name	<input type="text" value="example.com"/>
Default domain for authentication	<input type="text" value="--None--"/>
 SMTP Service <input checked="" type="checkbox"/>	
SMTP server port number	<input type="text" value="25"/>
SMTPS server port number	<input type="text" value="465"/>
SMTP over SSL/TLS	<input type="checkbox"/>
SMTP MSA service	<input checked="" type="checkbox"/>
SMTP MSA port number	<input type="text" value="587"/>
Authentication	SMTP <input type="checkbox"/> SMTPS <input checked="" type="checkbox"/> SMTP over TLS <input checked="" type="checkbox"/>

What is the expected outcome of SMTP sessions sourced from FML1 and destined for FML2?

Options:

- A- FML1 will fail to establish any connection with FML2.
- B- FML1 will attempt to establish an SMTPS session with FML2. but fail and revert to standard SMTP.
- C- FML1 will send the STARTTLS command in the SMTP session, which will be rejected by FML2.
- D- FML1 will successfully establish an SMTPS session with FML2.

Answer:

D

Question 12

Question Type: MultipleChoice

While reviewing logs, an administrator discovers that an incoming email was processed using policy IDs 0:4:9:INTERNAL.

Which two statements describe what this policy ID means? (Choose two.)

Options:

- A- Access control policy number 9 was used.
- B- The FortiMail configuration is missing an access delivery rule.
- C- The email was processed using IP-based policy ID 4.
- D- FortiMail is applying the default behavior for relaying inbound email.

Answer:

A, C

To Get Premium Files for NSE6_FML-7.2 Visit

https://www.p2pexams.com/products/nse6_fml-7.2

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/nse6-fml-7.2>

