

Fortinet

Exam Questions NSE6_FML-6.4

Fortinet NSE 6 - FortiMail 6.4



NEW QUESTION 1

Refer to the exhibit.

Sender Reputation	Authentication Reputation	Endpoint Reputation
<input type="button" value="Refresh"/> <input type="button" value="Previous"/> <input type="text" value="1"/> / 1 <input type="button" value="Next"/> Records per page: <input type="text" value="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> Question 2

NEW QUESTION 2

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"/> Records per page: <input type="text" value="50"/> IBE domain: <input type="text" value="--All--"/> Search: <input type="text"/>						
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

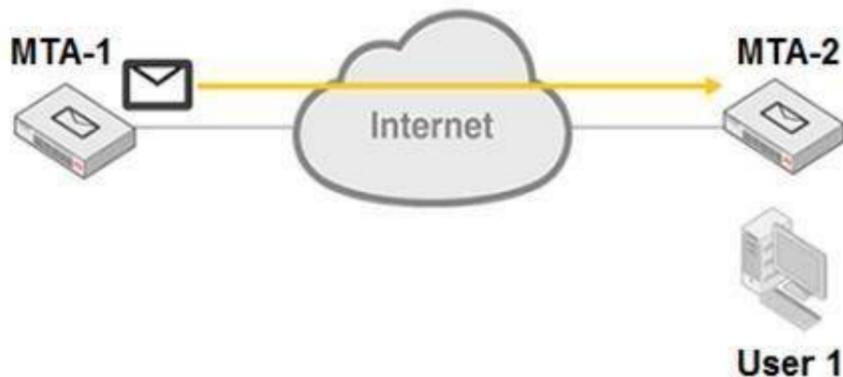
Answer: D

Explanation:

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

NEW QUESTION 3

Refer to the exhibit.



MTA-1 is delivering an email intended for User 1 to MTA-2.

Which two statements about protocol usage between the devices are true? (Choose two.)

- A. User 1 will use logs were generated load the email message from MTA-2
- B. MTA-2 will use IMAP to receive the email message from MTA-1
- C. MTA-1 will use POP3 to deliver the email message to User 1 directly
- D. MTA-1 will use SMTP to deliver the email message to MTA-2

Answer: AD

NEW QUESTION 4

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 (322, 323)

NEW QUESTION 5

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

Answer: ABD

NEW QUESTION 6

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

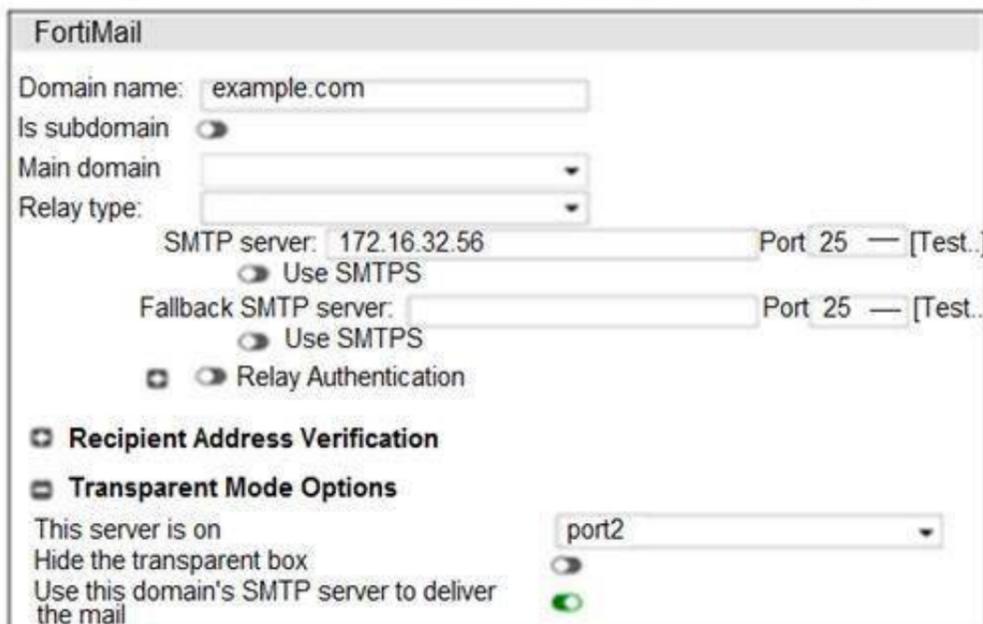
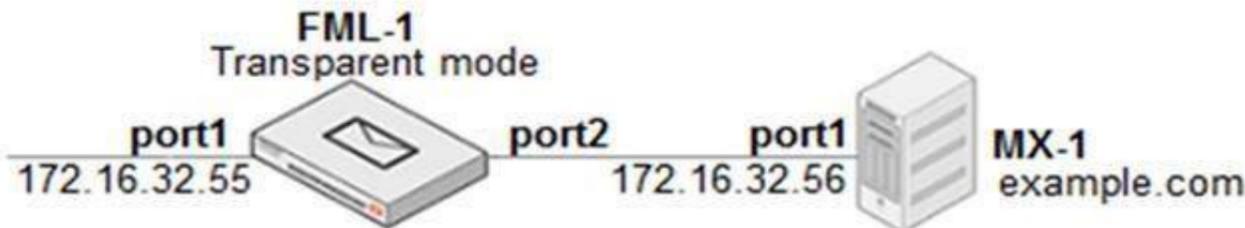
Answer: BCE

Explanation:

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

NEW QUESTION 7

Refer to the exhibit.



Which two statements about how the transparent mode FortiMail device routes email for the example.com domain are true? (Choose two.)

- A. If incoming email messages are undeliverable, FML-1 can queue them to retry later

- B. If outgoing email messages are undeliverable, FM-1 can queue them to retry later
- C. FML-1 will use the built-in MTA for outgoing sessions
- D. FML-1 will use the transparent proxy for incoming sessions

Answer: BD

NEW QUESTION 8

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

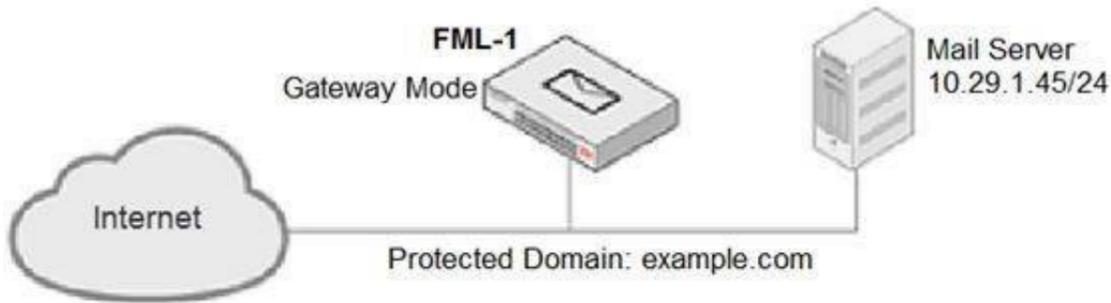
Answer: A

Explanation:

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

NEW QUESTION 9

Refer to the exhibit.



Access Control Rule

Enabled:

Sender: User Defined
*

Recipient: User Defined
*

Source: IP/Netmask
0.0.0.0/0

Reverse DNS pattern: * Regular Expression

Authentication status: Any

TLS profile: --None--

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

Answer: BDE

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 10

A FortiMail administrator is investigating a sudden increase in DSNs being delivered to the protected domain for undeliverable email messages. After searching the logs, the administrator identifies that the DSNs were not generated as a result of any outbound email sent from the protected domain. Which FortiMail antispam technique can the administrator use to prevent this scenario?

- A. Spam outbreak protection
- B. Bounce address tag validation
- C. Spoofed header detection
- D. FortiGuard IP Reputation

Answer: A

Explanation:

Reference: <https://docs.fortinet.com/document/fortimail/6.2.0/administrationguide/769204/managing-the-mail-queue>

NEW QUESTION 12

While reviewing logs, an administrator discovers that an incoming email was processed using policy IDs 0:4:9. Which two scenarios will generate this policy ID? (Choose two.)

- A. Email was processed using IP policy ID 4
- B. Incoming recipient policy ID 9 has the exclusive flag set
- C. FortiMail applies the default behavior for relaying inbound email
- D. FortiMail configuration is missing an access delivery rule

Answer: CD

NEW QUESTION 14

While testing outbound MTA functionality, an administrator discovers that all outbound email is being processed using policy IDs 1:2:0. Which two reasons explain why the last policy ID value is 0? (Choose two.)

- A. Outbound email is being rejected
- B. IP policy ID 2 has the exclusive flag set
- C. There are no outgoing recipient policies configured
- D. There are no access delivery rules configured for outbound email

Answer: CD

NEW QUESTION 19

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 profiles
- B. Domain-level service settings
- C. Access profiles
- D. Address book management options

Answer: A

NEW QUESTION 20

A FortiMail administrator is concerned about cyber criminals attempting to get sensitive information from employees using whaling phishing attacks. What option can the administrator configure to prevent these types of attacks?

- A. Impersonation analysis
- B. Bounce tag verification
- C. Content disarm and reconstruction
- D. Dictionary profile with predefined smart identifiers

Answer: A

NEW QUESTION 24

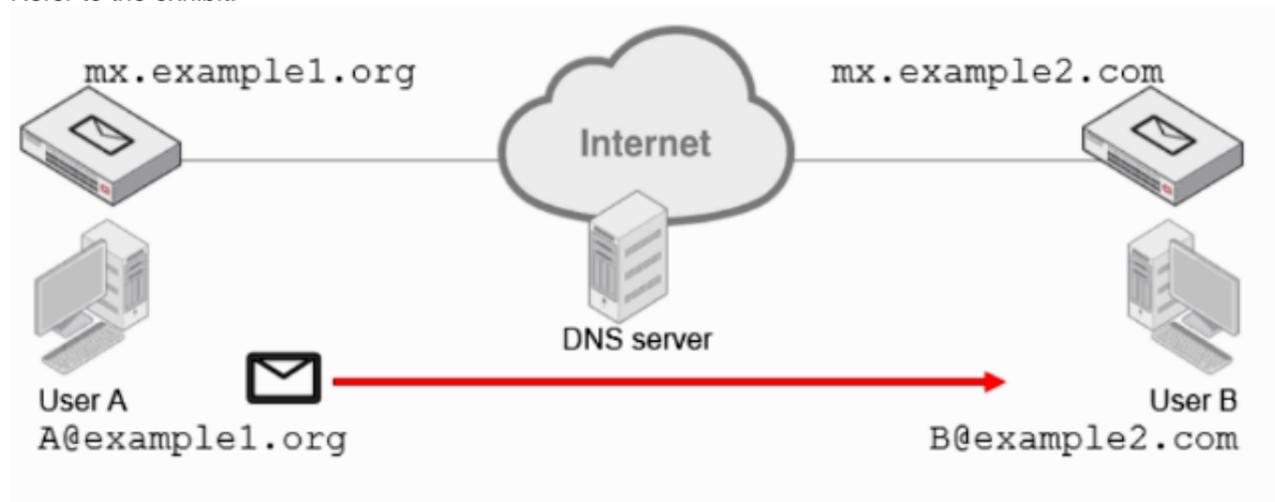
Which two features are available when you enable HA centralized monitoring on FortiMail? (Choose two.)

- 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 28

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 29

Refer to the exhibit.

FortiMail

Domain name:

Is subdomain

Main domain:

Relay type:

SMTP server: Port:

Use SMTPS

Fallback SMTP server: Port:

Use SMTPS

Relay Authentication

Recipient Address Verification

Transparent Mode Options

This server is on

Hide the transparent box

Use this domain's SMTP server to deliver the mail

For the transparent mode FortiMail shown in the exhibit, which two sessions are considered incoming sessions? (Choose two.)

- A. DESTINATION IP: 172.16.32.56 MAIL FROM: support@example.com RCPT TO: marketing@example.com
- B. DESTINATION IP: 192.168.54.10 MAIL FROM: accounts@example.com RCPT TO: sales@example.com
- C. DESTINATION IP: 10.25.32.15 MAIL FROM: training@example.com RCPT TO: students@external.com
- D. DESTINATION IP: 172.16.32.56 MAIL FROM: mis@hosted.net RCPT TO: noc@example.com

Answer: AC

NEW QUESTION 30

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

Session

Session Profile

Profile name:

Connection Settings

Sender Reputation

Endpoint Reputation

Sender Validation

Session Settings

Unauthenticated Session Settings

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:



Domains

Domain name:

Is subdomain:

Main domain:

LDAP User Profile:

Advanced Settings

Mail Routing LDAP profile:

Remove received header of outgoing email

Webmail theme:

Webmail language:

Maximum message size(KB):

Automatically add new users to address book:

Which size limit will FortiMail apply to outbound email?

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

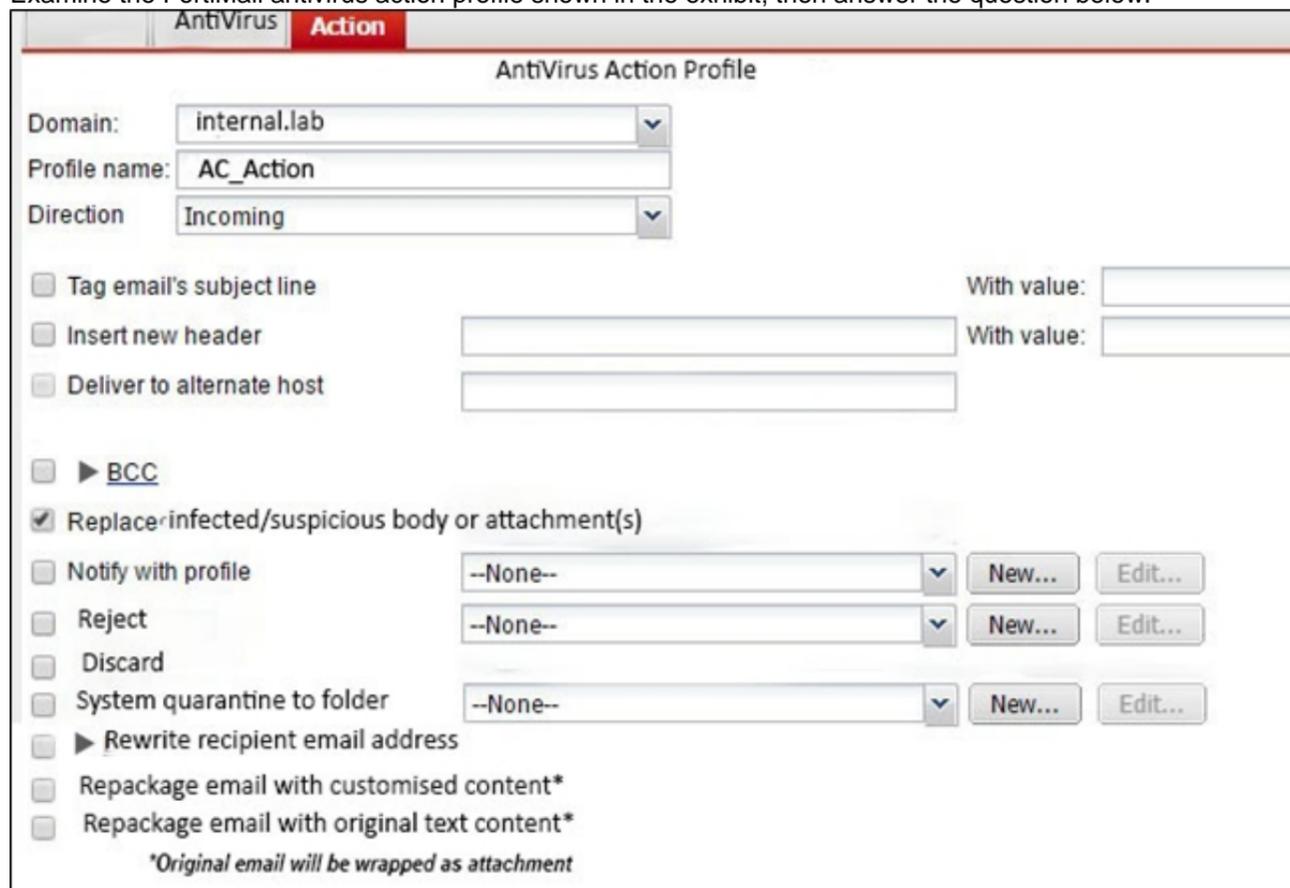
Answer: B

Explanation:

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

NEW QUESTION 32

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



AntiVirus Action Profile

Domain:

Profile name:

Direction:

Tag email's subject line With value:

Insert new header With value:

Deliver to alternate host

► BCC

Replace infected/suspicious body or attachment(s)

Notify with profile

Reject

Discard

System quarantine to folder

► Rewrite recipient email address

Repackage email with customised content*

Repackage email with original text content*

**Original email will be wrapped as attachment*

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: BC

NEW QUESTION 36

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

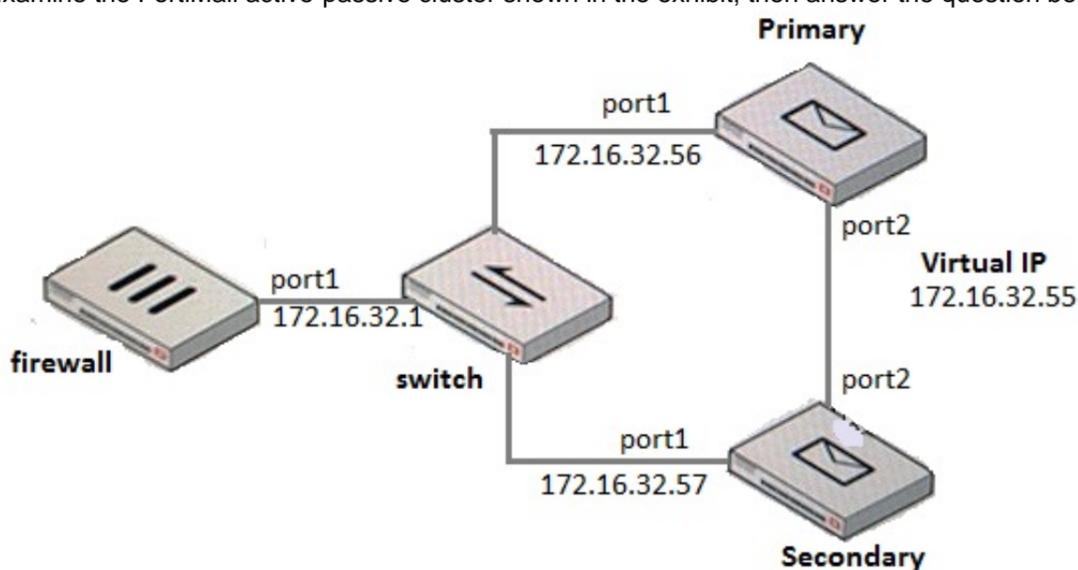
After creating the policy, an administrator discovered that clients are able to send unauthenticated email using SMTP. What must be done to ensure clients cannot send unauthenticated email?

- 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 40

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:
Peer IPv6 address:
Virtual IP action: Ignore
Virtual IP address: /
Virtual IPv6 address: /

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 43

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

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 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 email message
- B. After initial registration, IBE users can access the secure portal without authenticating again for 90 days
- C. Registered 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

NEW QUESTION 45

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

```
Cross search result: v3Hfg7Mx003810
page: 50 | Download
Message
STARTTLS=server, relay=[192.168.1.252], version=TLSv1.2, verify=NOT, cipher=ECDHE-RSA-AES256-SHA, bits=256/256
from=<bwayne@example.com>, size=476, class=0, nrpts=1, msgid=<20170417114207.v3Hfg76QB26164@example.com>, proto=
ESMTP, daemon=SMTP_MTA, relay=[192.168.1.252]
to=<hjordan@external.com>, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=30723, relay=external.com [192.167.1.252], dsn=4.0.0, stat=Deferred:
Connection refused by external.com
```

Based on 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 server mode FortiMail
- 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: AC

NEW QUESTION 49

.....

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](#)