

NSE6_FML-6.2.VCEplus.premium.exam.30q

Number: NSE6_FML-6.2

Passing Score: 800

Time Limit: 120 min

File Version: 1.0



Website: <https://vceplus.com>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

NSE6_FML-6.2

Fortinet NSE 6 - FortiMail 6.2



Version 1.0

Exam A

QUESTION 1

Refer to the exhibit.

Sender Reputation	Authentication Reputation	Endpoint Reputation
<div> <div> <div>1</div> <div>1</div> </div> <div>Records per page: 50</div> </div>		
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

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 2

Refer to the exhibit.

Active User Expired User Secure Question IBE Authentication IBE Domain

Delete Maintenance Reset User

1 / 1

Records per page: 50 IBE domain: --All-- 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.

Correct Answer: D

Section: (none)

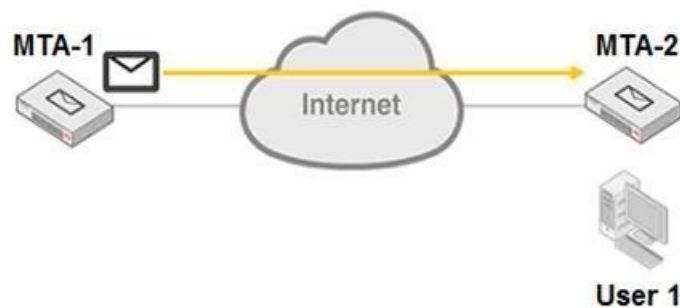
Explanation

Explanation/Reference:

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

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 IMAP to download 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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

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)

QUESTION 5 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6 Which two antispam techniques query FortiGuard for rating information?
(Choose two.)

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 7 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8 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

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 9

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

Correct Answer: AC

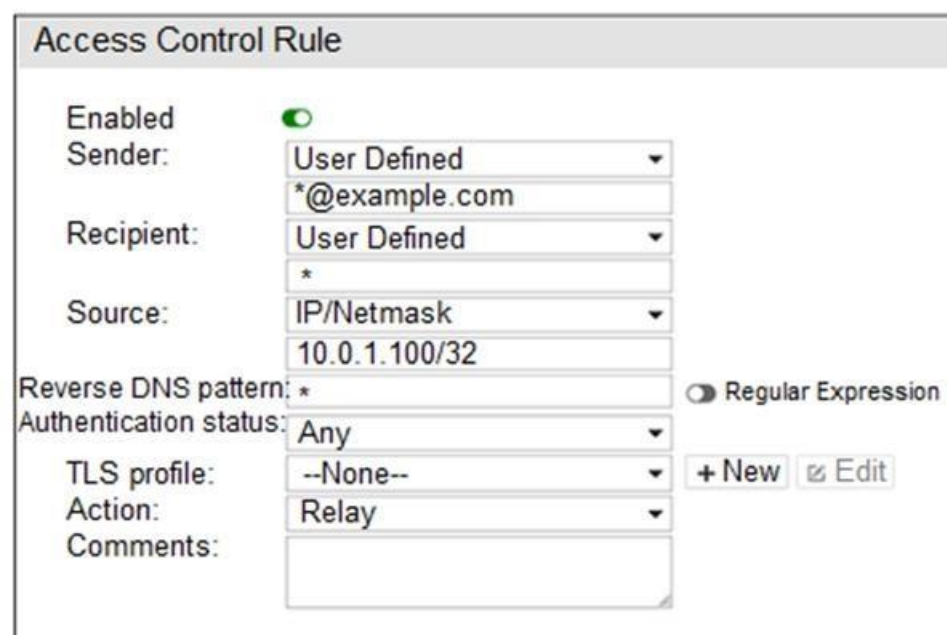
Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Which firmware upgrade method for an active-passive HA cluster ensures service outage is minimal, and there are no unnecessary failovers?

- A. Break the cluster, upgrade the units independently, and then form the cluster
- B. Upgrade both units at the same time
- C. Upgrade the standby unit, and then upgrade the active unit
- D. Upgrade the active unit, which will upgrade the standby unit automatically

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortimail/6.2.0/administration-guide/725928/upgrading-firmware-on-ha-units>

QUESTION 13 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



Correct Answer: CD

Section: (none)

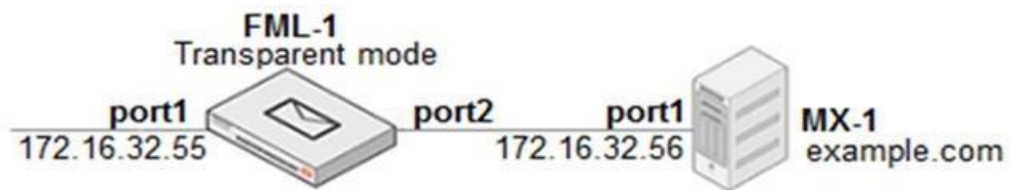
Explanation

Explanation/Reference:

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 14

Refer to the exhibit.



Storage Proxies

For outgoing SMTP connections
Use client-specified SMTP server to send email ☒

Apply **Cancel**

FortiMail

Domain name:

Is subdomain ☐

Main domain

Relay type:

SMTP server: Port [Test..]

☐ Use SMTPS

Fallback SMTP server: Port [Test..]

☐ 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 ☒

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

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

Section: (none)

Explanation

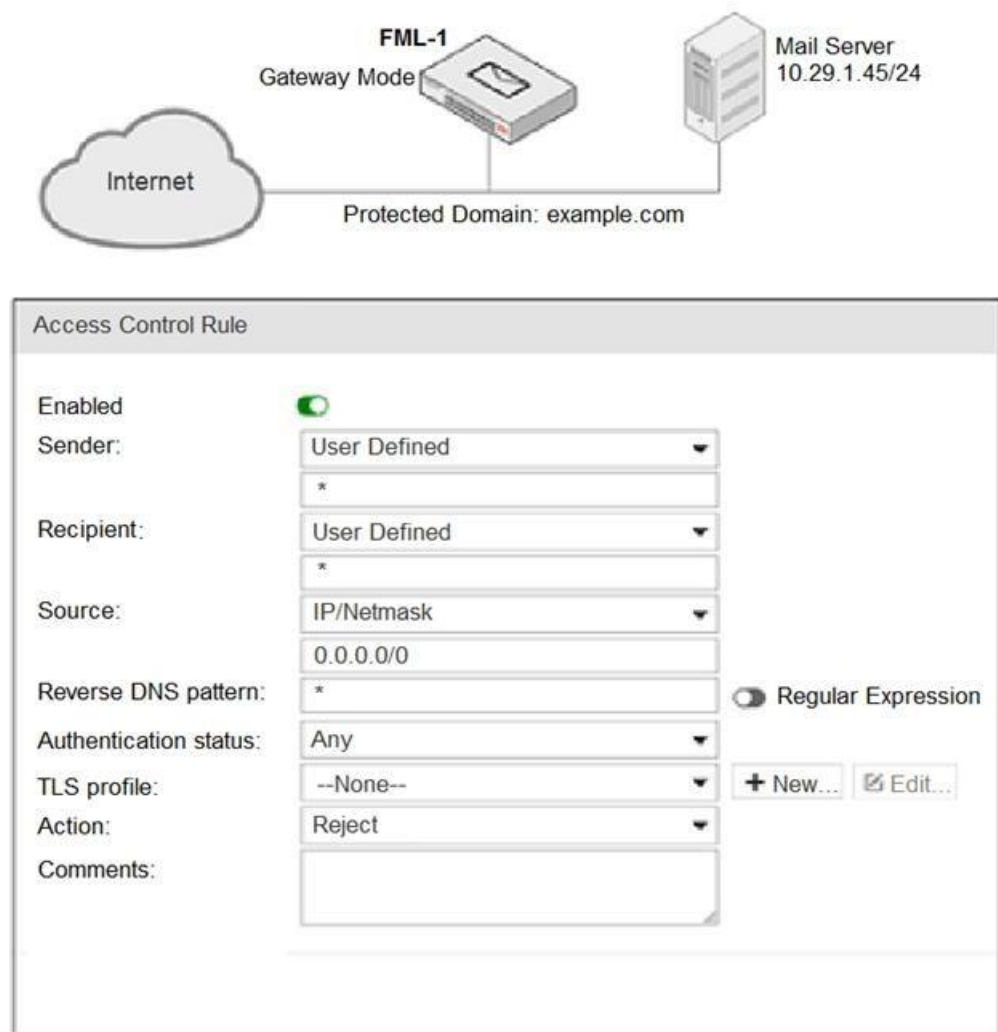


Explanation/Reference:

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

QUESTION 16

Refer to the exhibit.



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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Refer to the exhibit.

Mail Server Settings	Relay Host List	Disclaimer	Disclaimer Exclusion List	Storage
Local Host:				
Host name:	mx			
Local domain name:	example.com			
SMTP server port number:	25			
SMTP over SSL/TLS	<input checked="" type="checkbox"/>			
SMTPS server port number:	465			
SMTP MSA service	<input type="checkbox"/>			
SMTP MSA port number:	587			
POP3 server port number:	110			
Default domain for authentication:	--None--			
Redirect HTTP to HTTPS	<input checked="" type="checkbox"/>			

Which two statements about the mail server settings are true? (Choose two.)

- A. FortiMail will support the STARTTLS extension
- B. FortiMail will accept SMTPS connections
- C. FortiMail will drop any inbound plaintext SMTP connection
- D. FortiMail will enforce SMTPS on all outbound sessions

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

Refer to the exhibit.

Email Archiving Exempt Policy

Policy status:

☒

Account:

journal

+ New...

Edit...

Policy type:

Spam email

Pattern:

Create

Cancel

Email Archiving Policy

Policy status:

☒

Account:

journal

+ New...

Edit...

Policy type:

Recipient Address

Pattern:

marketing@example.com

Create

Cancel



What two archiving actions will FortiMail take when email messages match these archive policies? (Choose two.)

- A. FortiMail will save archived email in the journal account
- B. FortiMail will allow only the `marketing@example.com` account to access the archived email
- C. FortiMail will exempt spam email from archiving
- D. FortiMail will archive email sent from `marketing@example.com`

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 21 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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

Refer to the exhibit.



Message Scan Rule

Name:

DLPOut

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 cotains 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

Correct Answer: BC

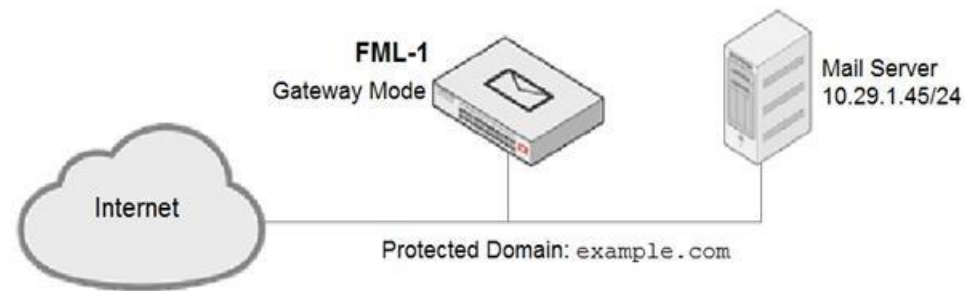
Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

Refer to the exhibit.



IP Policy											
<div> + New.. Edit.. Delete.. Move ▾ </div> <div> 1 / 1 Records per page: 50 ▾ </div>											
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

Correct Answer: AD

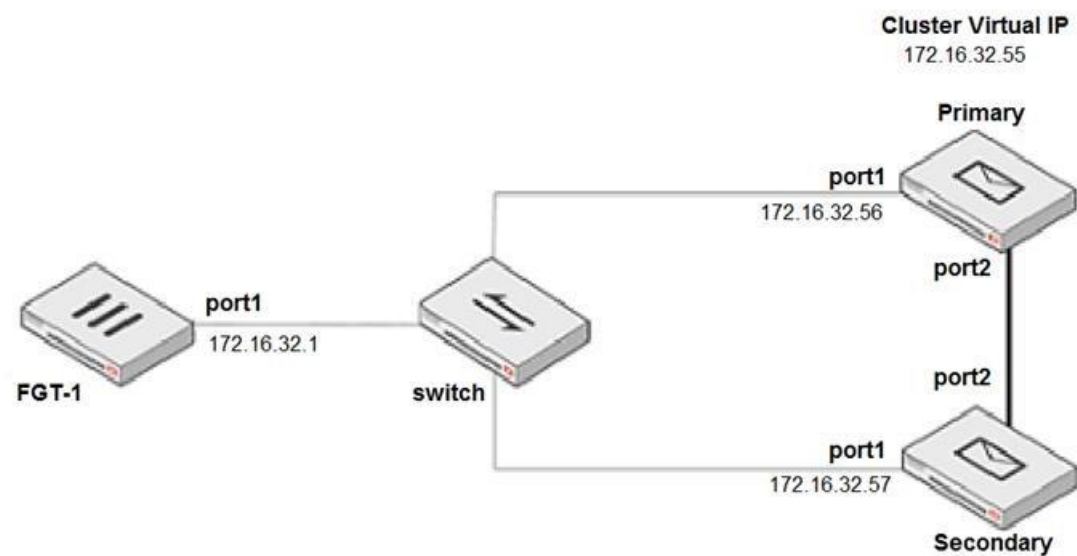
Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Refer to the exhibit.



Primary HA Interface Configuration

HA Interface	
Port:	port1
Enable port monitor	<input type="radio"/>
Heartbeat status:	Disable
Peer IP address:	0.0.0.0
Peer IPv6 address:	
Virtual IP action:	Ipnone
Virtual IP address:	0.0.0.0 / 0
Virtual IPv6 address:	/ 0
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

The exhibit shows a FortiMail active-passive setup.

Which three actions are recommended when configuring the primary FortiMail HA interface? (Choose three.)

- A. Disable **Enable port monitor**
- B. In the **Heartbeat status** drop-down list, select **Primary**
- C. In the **Peer IP address** field, type 172.16.32.57
- D. In the **Virtual IP action** drop-down list, select **Use**
- E. In the **Virtual IP address** field, type 172.16.32.55/24

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25 Which two CLI commands, if executed, will erase all data on the log disk partition?
(Choose two.)

- A. execute formatmaildisk
- B. execute formatmaildisk_backup
- C. execute formatlogdisk
- D. execute partitionlogdisk 40

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortimail/6.2.0/cli-reference/588825/formatlogdisk>

QUESTION 26 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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 27 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



Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

Refer to the exhibit.

AntiVirus Action Profile

Domain: example.com

Profile name: AV_Action

☐ Tag subject

☐ Insert header

☐ Insert disclaimer default at Start of message

☐ Deliver to alternate host

☐ Deliver to original host

☐ BCC

☒ Replace Infected/suspicious body or attachment(s)

☐ Archive to account archive + New... Edit...

☐ Notify with profile --None-- + New... Edit...

☐ Final action Discard

What are two expected outcomes if FortiMail applies this antivirus action profile to an email? (Choose two.)

- A. Virus content will be removed from the email
- B. A replacement message will be added to the email
- C. The sanitized email will be sent to the recipient's personal quarantine
- D. The administrator will be notified of the virus detection

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

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

Correct Answer: C

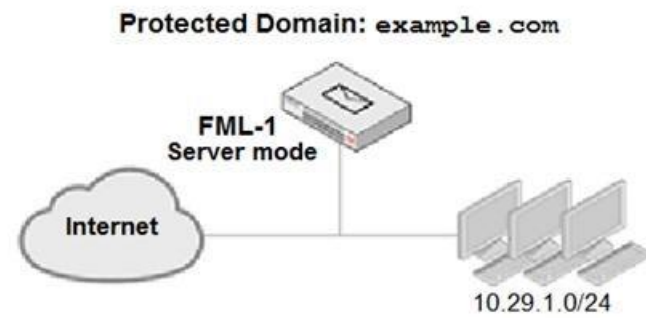
Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

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--
Action:	Relay
Comments:	

An administrator must enforce authentication on FML-1 for all outbound email from the example.com domain.

Which two settings should be used to configure the access receive rule? (Choose two.)

- A. The **Recipient pattern** should be set to *@example.com
- B. The **Authentication status** should be set to **Authenticated**
- C. The **Sender IP/netmask** should be set to 10.29.1.0/24
- D. The **Action** should be set to **Reject**

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference: