

Exam Questions NSE6_FML-6.4

Fortinet NSE 6 - FortiMail 6.4

https://www.2passeasy.com/dumps/NSE6_FML-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="button" 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

Refer to the exhibit.

Access Control Rule

Enabled

Sender:

Recipient:

Source:

Reverse DNS pattern: Regular Expression

Authentication status:

TLS profile:

Action:

Comments:

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 3

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 4

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

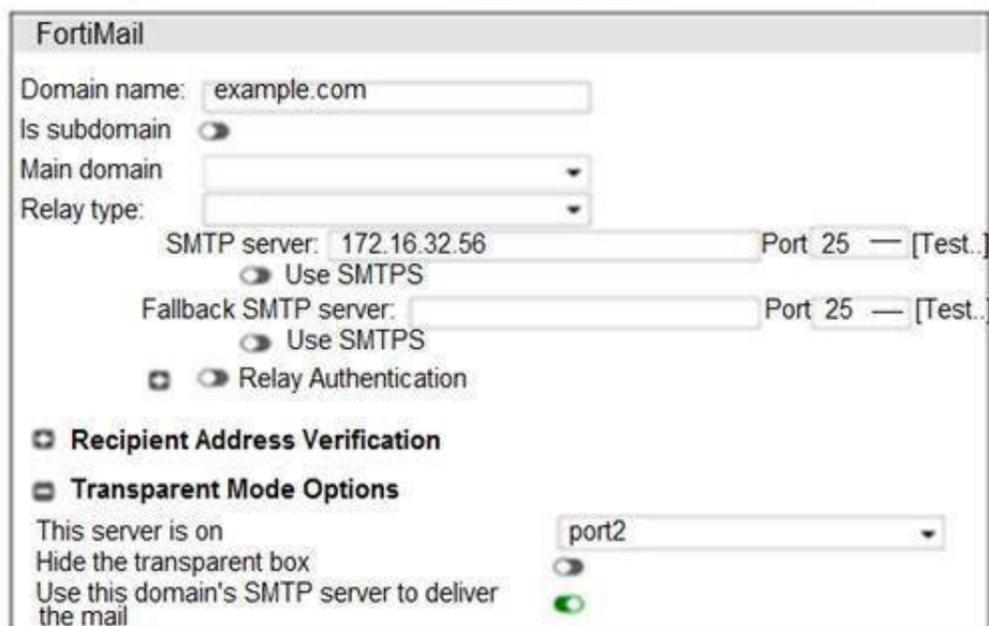
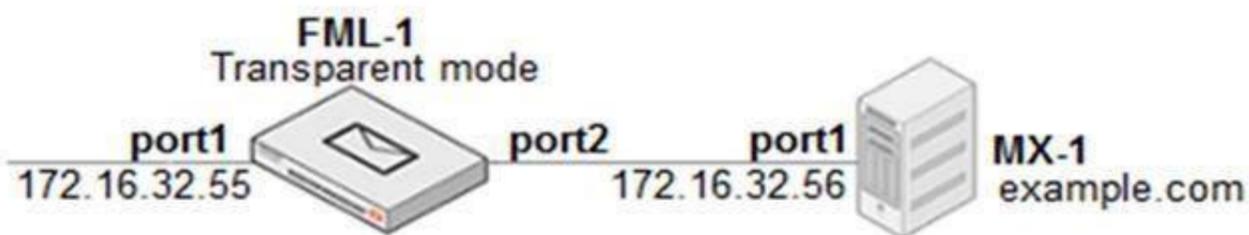
Answer: B

Explanation:

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

NEW QUESTION 5

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 6

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

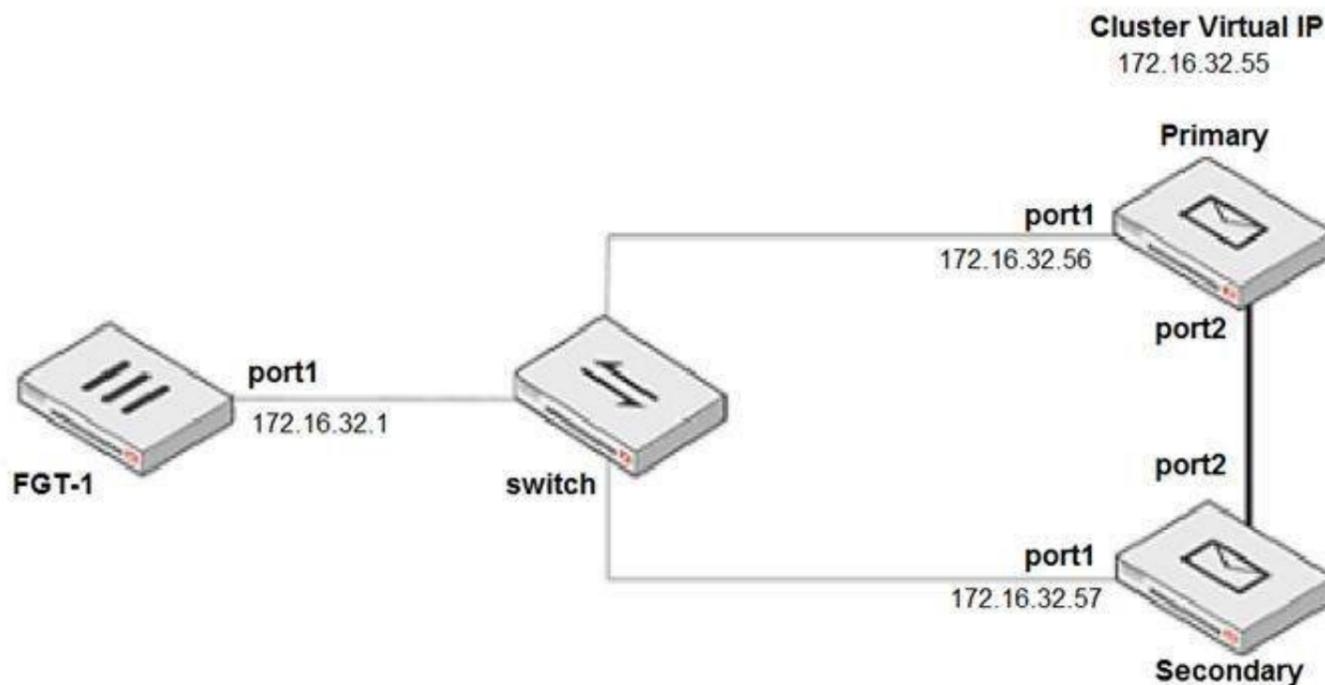
Answer: A

Explanation:

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

NEW QUESTION 7

Refer to the exhibit.



Primary HA Interface Configuration

HA Interface	
Port:	port1
Enable port monitor	<input type="checkbox"/>
Heartbeat status:	Disable
Peer IP address:	0.0.0.0
Peer IPv6 address:	
Virtual IP action:	lphone
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

Answer: ABD

NEW QUESTION 8

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

Answer: CD

Explanation:

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

NEW QUESTION 9

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 10

Refer to the exhibit.

AntiVirus Action Profile

Domain:

Profile name:

Tag subject

Insert header

Insert disclaimer at

Deliver to alternate host

Deliver to original host

BCC

Replace Infected/suspicious body or attachment(s)

Archive to account

Notify with profile

Final action

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

Answer: BC

NEW QUESTION 10

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 15

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 20

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 25

Examine the FortMail mail server settings shown in the exhibit; then answer the question below.

Mail Server Settings	Relay Host List	Disclaimer	Disclaimer Exclusion List
<div style="display: flex; justify-content: space-between;"> Local Host Local Host Setting </div>			
Host name:	<input type="text" value="mx"/>		
Local domain name:	<input type="text" value="example.com"/>		
SMTP server port number:	<input type="text" value="25"/>		
SMTP over SSL/TLS	<input checked="" type="checkbox"/>		
SMTPS server port number:	<input type="text" value="465"/>		
SMTP MSA service	<input checked="" type="checkbox"/>		
SMTP MSA port number:	<input type="text" value="587"/>		
POP3 server port number:	<input type="text" value="110"/>		
Default domain for authentication:	<input type="text" value="--None--"/>		
Webmail access	<input checked="" type="checkbox"/> Redirect HTTP to HTTPS		

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

- A. mx.example.com will enforce SMTPS on all outbound sessions
- B. mx.example.com will display STARTTLS as one of the supported commands in SMTP sessions
- C. mx.example.com will accept SMTPS connections
- D. mx.example.com will drop any inbound plaintext SMTP connection

Answer: BC

NEW QUESTION 26

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 28

Which of the following statements are true regarding FortiMail's behavior when using the built-in MTA to process email in transparent mode? (Choose two.)

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

Answer: AC

NEW QUESTION 31

Examine the FortiMail user webmail interface shown in the exhibit; then answer the question below.



Which one of the following statements is true regarding this server mode FortiMail's configuration?

- A. The protected domain-level service settings have been modified to allow access to the domain address book
- B. This user's account has a customized access profile applied that allows access to the personaladdress book
- C. The administrator has not made any changes to the default address book access privileges
- D. The administrator has configured an inbound recipient policy with a customized resource profile

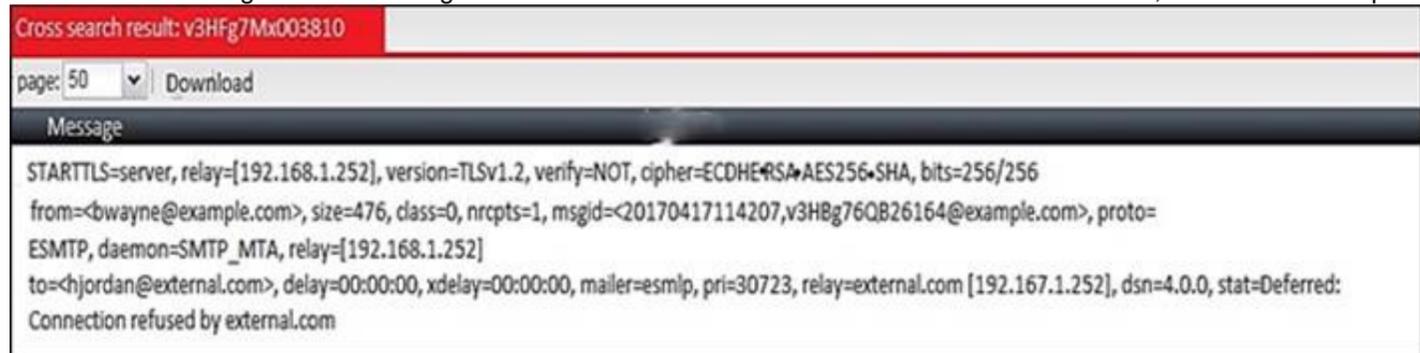
Answer: D

Explanation:

domain address book can be enabled under resource profile which is applied to inbound recipient policy

NEW QUESTION 33

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



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 36

Examine the FortiMail DLP scan rule shown in the exhibit; then answer the question below.

Profile Rule

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 contains Credit Card

Exceptions

New... | Edit... | Delete |

ID	Condition
1	Sender contains sales@internal.lab

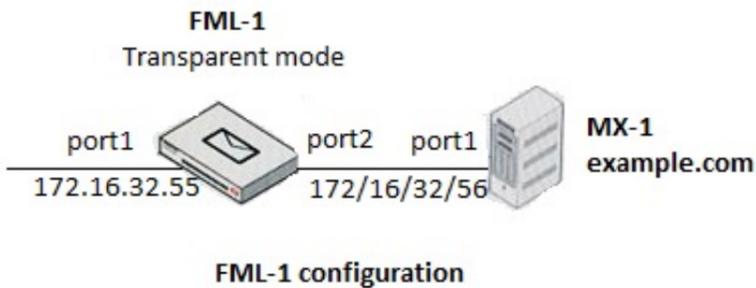
Which of the following statements is true regarding this configuration? (Choose two.)

- A. An email message containing the words "Credit Card" in the subject will trigger this scan rule
- B. If an email is sent from sales@internal.lab the action will be applied without matching any conditions
- C. An email message containing credit card numbers in the body will trigger this scan rule
- D. An email must contain credit card numbers in the body, attachment, and subject to trigger this scan rule

Answer: AC

NEW QUESTION 37

Refer to the exhibit.



Proxies

For outgoing SMTP connections

Use client-specified SMTP server to send email

Apply Cancel

Domains

Domain name:

Relay type:

SMTP server: Port: Use SMTPS

Fallback SMTP server: Port: Use SMTPS

Relay Authentication

Is subdomain

Main domain:

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 of the following statements are true regarding the transparent mode FortiMail's email routing for the example.com domain? (Choose two.)

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

Answer: BC

NEW QUESTION 38

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 40

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE6_FML-6.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE6_FML-6.4 Product From:

https://www.2passeasy.com/dumps/NSE6_FML-6.4/

Money Back Guarantee

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 FirstTry
- * NSE6_FML-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year