NSE6_FML-6.0^{Q&As}

Fortinet NSE 6 - FortiMail 6.0

Pass Fortinet NSE6_FML-6.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/nse6_fml-6-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which of the following statements regarding SMTPS and SMTP over TLS are true? (Choose three.)

A. In an SMTPS session, the identities of both sender and receiver are encrypted

B. SMTPS connections are initiated on port 465

C. SMTP over TLS connections are entirely encrypted and initiated on port 465

D. The STARTTLS command is used to initiate SMTP over TLS

E. SMTPS encrypts the body of the email message, where the most sensitive content exists

Correct Answer: ABD

QUESTION 2

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 personal address 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

Correct Answer: A

QUESTION 3

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

A. execute formatmaildisk
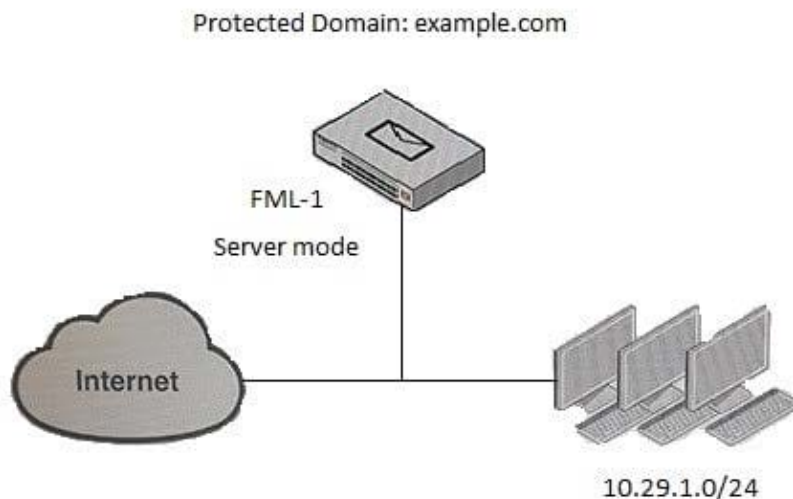
B. execute formatmaildisk_backup

C. execute formatlogdisk

D. execute partitionlogdisk 40

Correct Answer: CD

QUESTION 4

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

Protected Domain: example.com

FML-1
Server mode

Internet

10.29.1.0/24

FortiMail

Access Control Rule

Enabled ☑
Sender pattern: [User Defined ▾]
[*] ☐ Regular expression

Recipient pattern: [User Defined ▾]
[*] ☐ Regular expression

Sender
IP/netmask: [User Defined ▾]
[0.0.0.0] / [0]

Reverse DNS
pattern: [*] ☐ Regular expression

Authentication
status: [Any ▾]

TLS profile: [--None-- ▾] [New...] [Edit..]

Action: [Reject ▾]

Comments: [   ]

[Create] [Cancel]

An administrator must enforce authentication on FML-1 for all outbound email from the example.com domain. Which of the following settings should be used to configure the access receive rule? (Choose two.)

A. The Sender IP/netmask should be set to 10.29.1.0/24

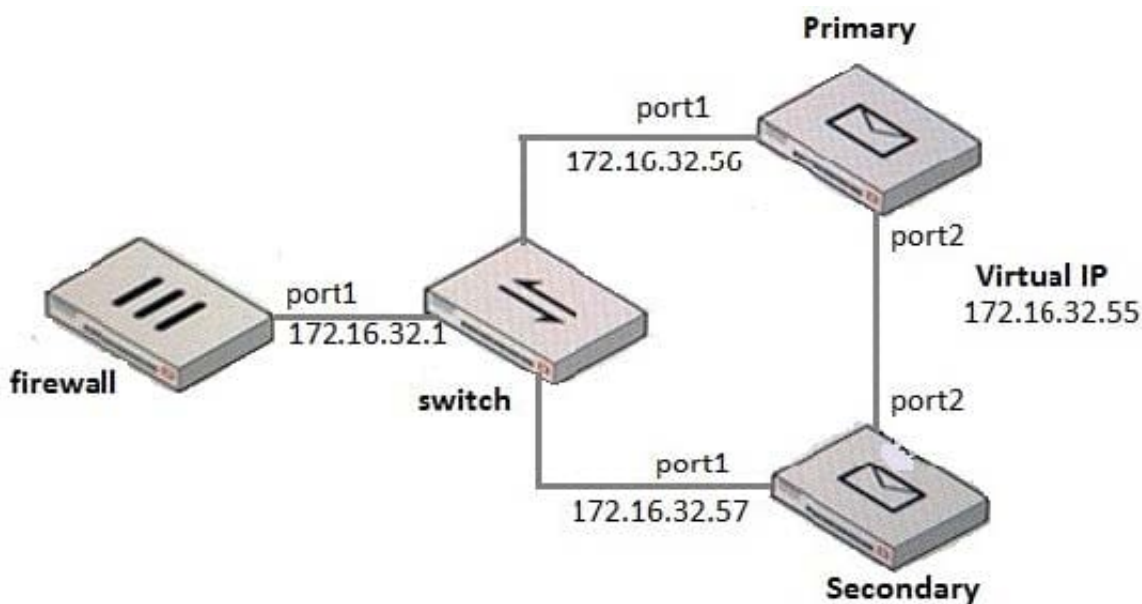B. The Authentication status should be set to Authenticated

C. The Recipient pattern should be set o *@example.com

D. The Action should be set to Reject

Correct Answer: CD

QUESTION 5

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

Primary

port1
172.16.32.56

port2

Virtual IP
172.16.32.55

port1
172.16.32.1

firewall

switch

port2

port1
172.16.32.57

Secondary

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

Correct Answer: CDE

NSE6_FML-6.0 VCE Dumps   NSE6_FML-6.0 Practice Test   NSE6_FML-6.0 Study Guide