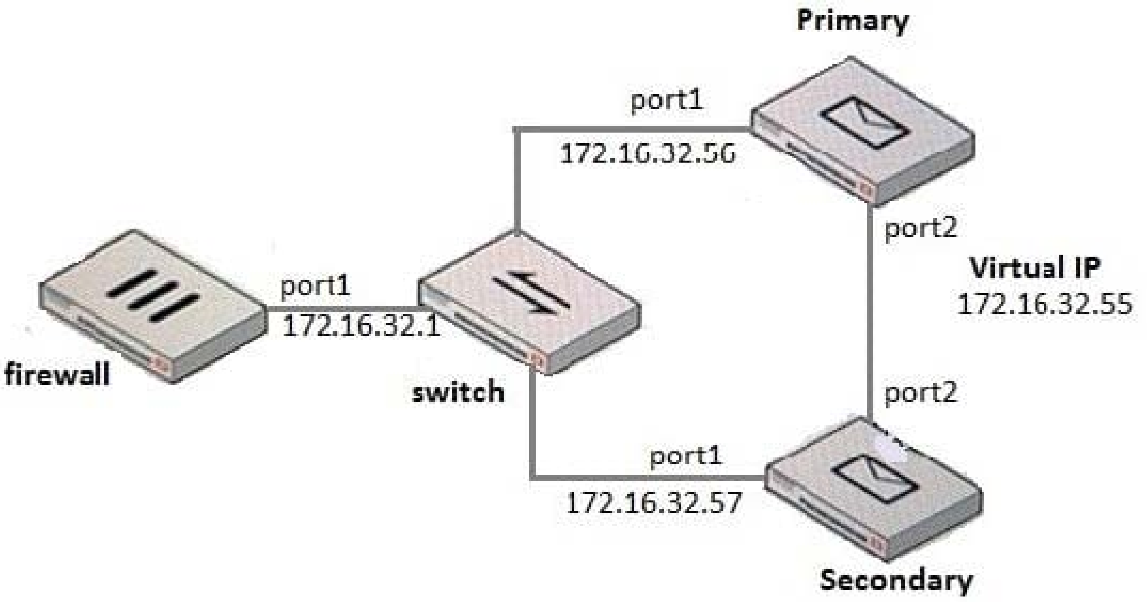
NSE6_FML-6.0 Q&As

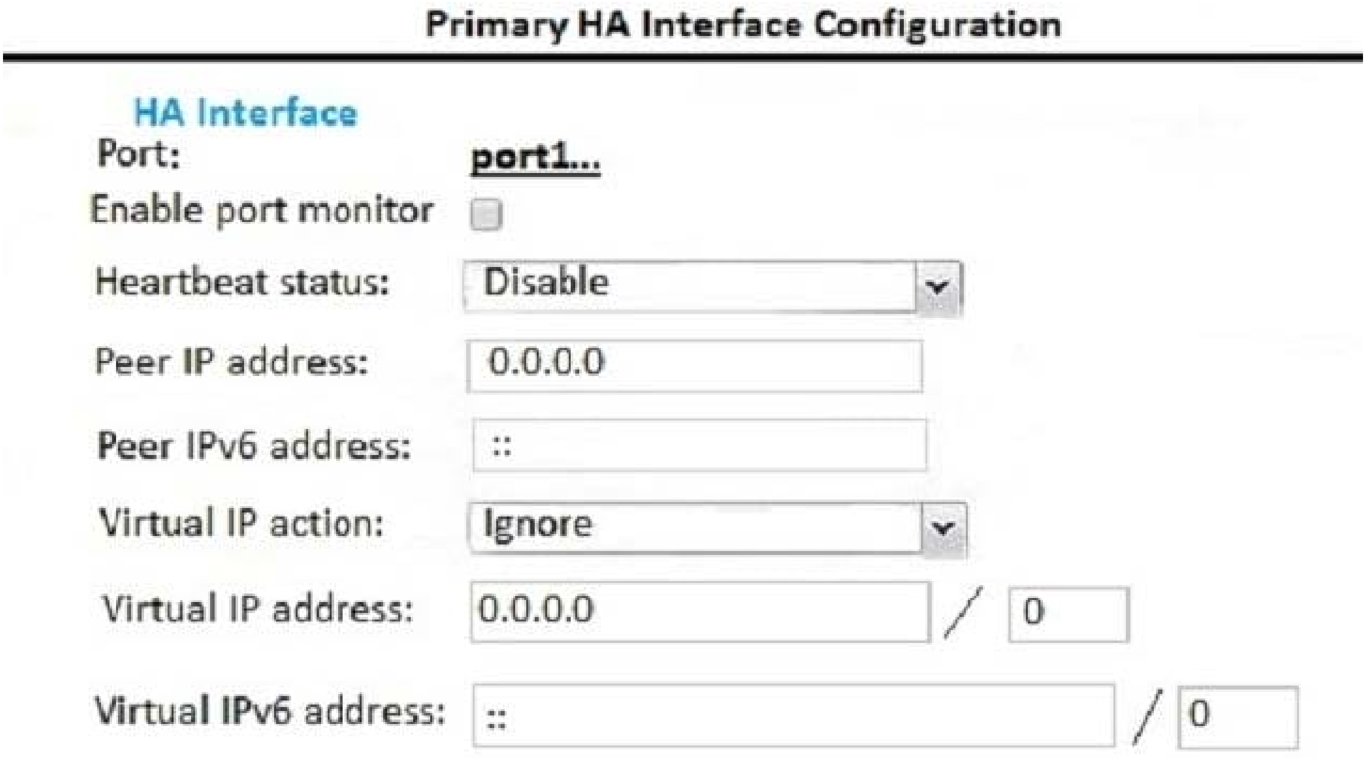
Fortinet NSE 6 - FortiMail 6.0

Pass Fortinet NSE6_FML-6.0 Exam with 100% Guarantee

QUESTION 1

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: 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

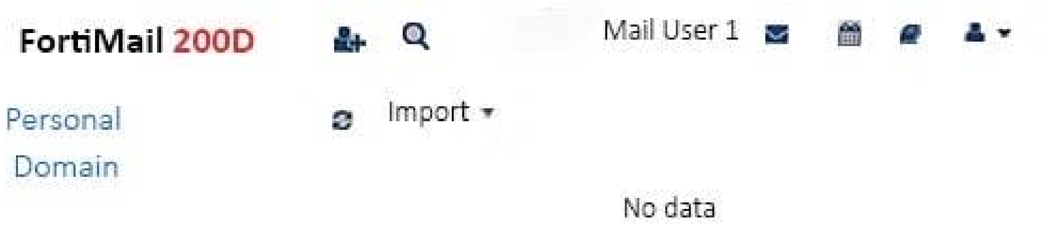
D. Virtual IP address: 172.16.32.55/24

E. Virtual IP action: Use

Correct Answer: CDE

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

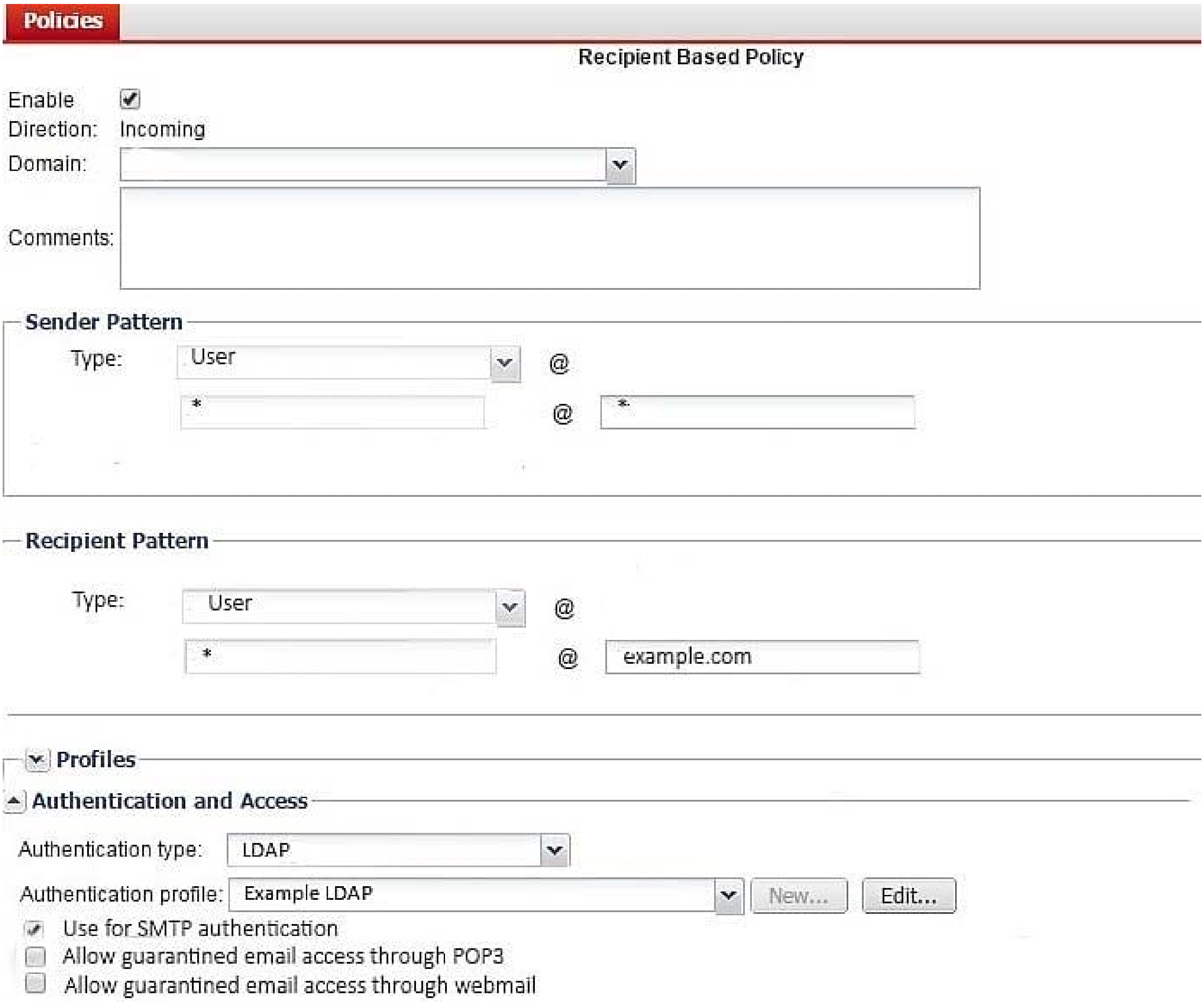
C. The administrator has not made any changes to the default address book access privileges

D. The administrator has configured an inbound recipient policy with a customized resource profile

Correct Answer: A

QUESTION 3

Examine the FortiMail recipient-based policy shown in the exhibit; then answer the question below.



Recipient Based Policy

Enable ☑
Direction: Incoming
Domain:
Comments:

Sender Pattern
Type: User @
* @ *

Recipient Pattern
Type: User @
* @ example.com

Profiles
Authentication and Access
Authentication type: LDAP
Authentication profile: Example LDAP
☑ Use for SMTP authentication
□ Allow guarantined email access through POP3
□ Allow guarantined 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

Correct Answer: A

QUESTION 4

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

A. Upgrade the active unit, which will upgrade the standby unit automatically

B. Upgrade both units at the same time

C. Upgrade the standby unit, and then upgrade the active unit

D. Break the cluster, upgrade the units independently, and then form the cluster again as quickly as possible

Correct Answer: D

QUESTION 5

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