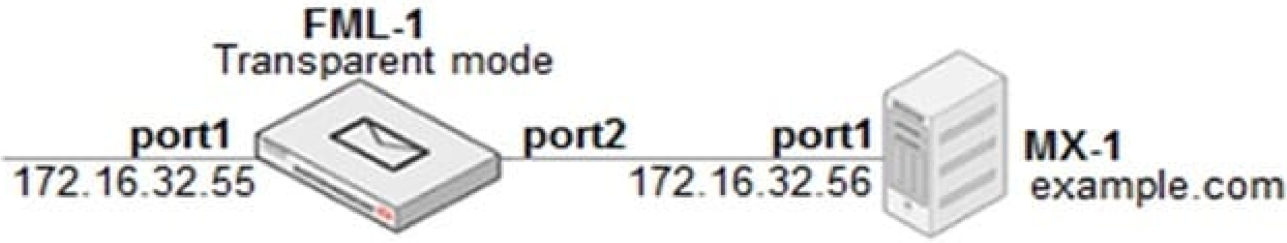
NSE6_FML-6.2$^{Q\&As}$

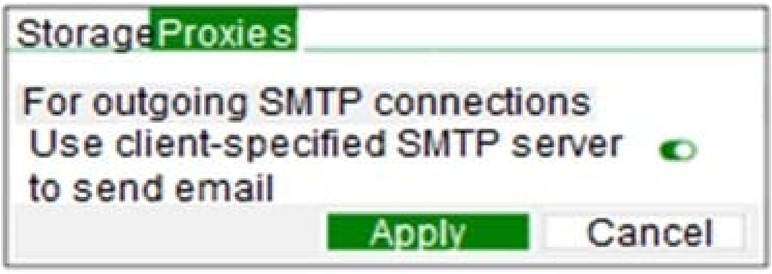
Fortinet NSE 6 - FortiMail 6.2

Pass Fortinet NSE6_FML-6.2 Exam with 100% Guarantee

QUESTION 1

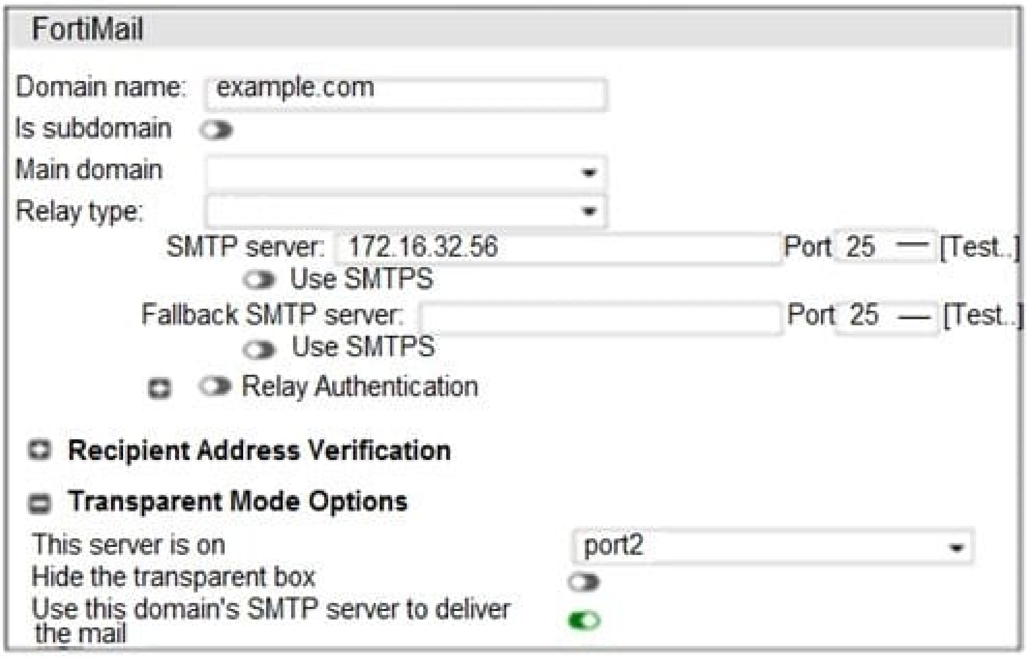
Refer to the exhibit.





For outgoing SMTP connections

Use client-specified SMTP server to send email ●



Domain name: example.com

Is subdomain ○

Main domain

Relay type:

SMTP server: 172.16.32.56 Port 25 [Test..]

○ Use SMTPS

Fallback SMTP server: Port 25 [Test..]

○ Use SMTPS

○ Relay Authentication

Recipient Address Verification

Transparent Mode Options

This server is on port2

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

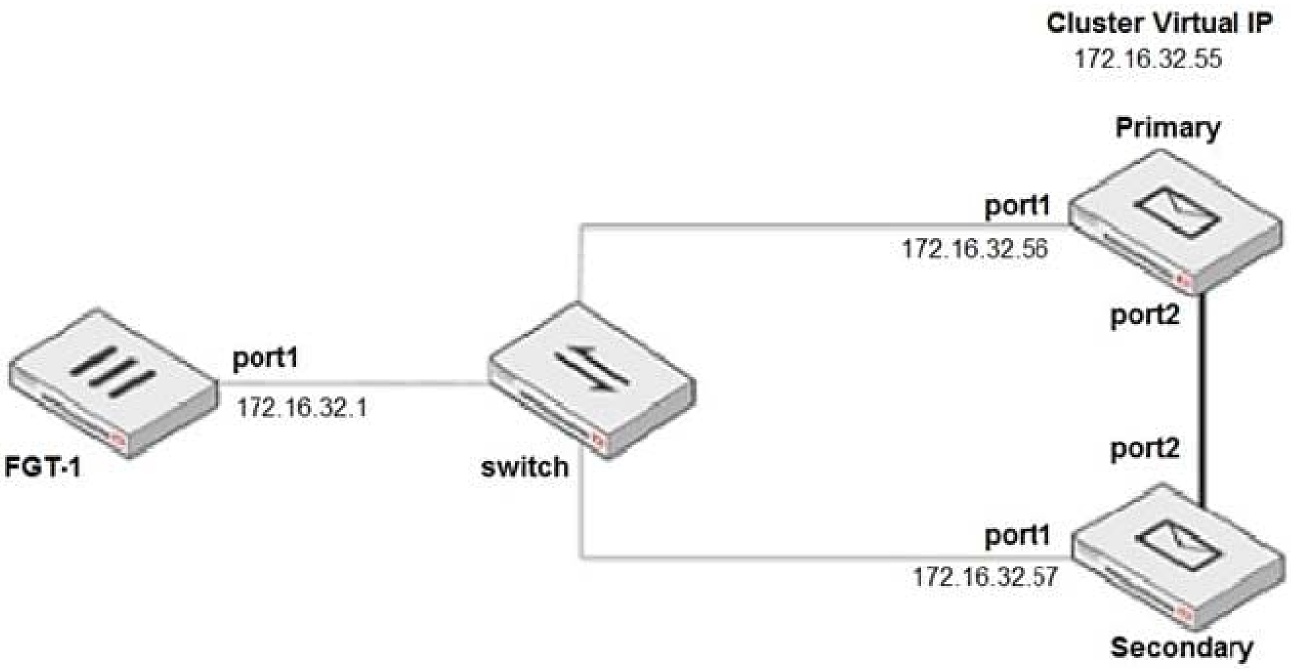
C. FML-1 will use the built-in MTA for outgoing sessions

D. FML-1 will use the transparent proxy for incoming sessions

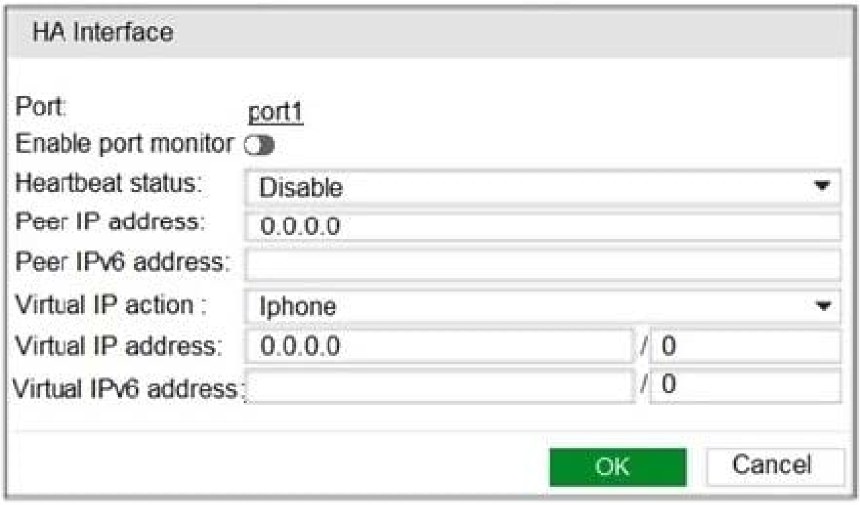
Correct Answer: BD

QUESTION 2

Refer to the exhibit.



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 : Iphone

Virtual IP address: 0.0.0.0 / 0

Virtual IPv6 address: / 0

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

QUESTION 3

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

A. DNSBL

B. SURBL

C. IP reputation

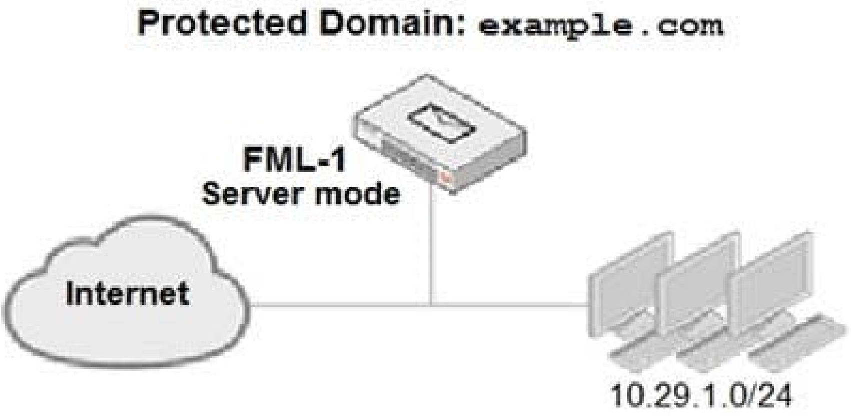
D. URI filter

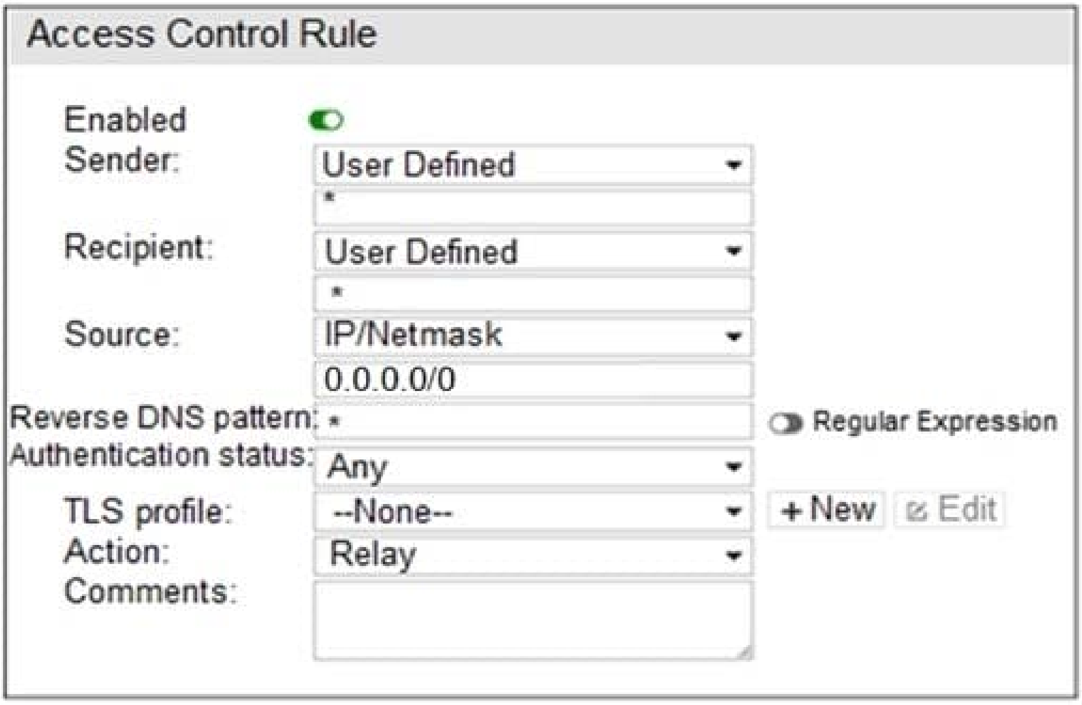
Correct Answer: AB

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

QUESTION 4

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-- + New Edit

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

QUESTION 5

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