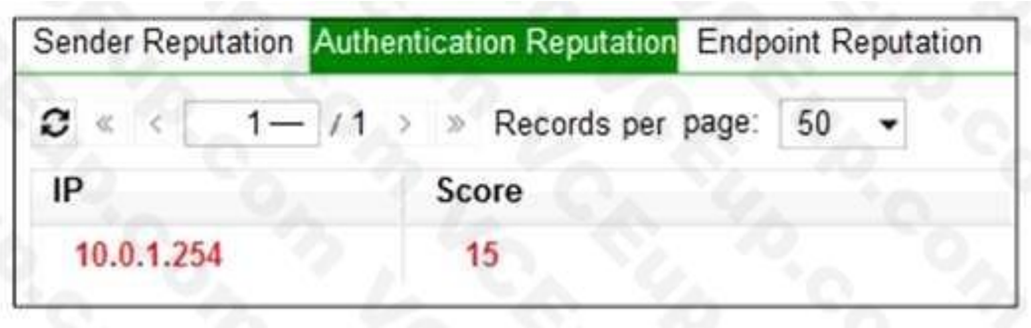
Topic 1, Main Questions Pool

Question 1

Refer to the exhibit.



Records per page: 50

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

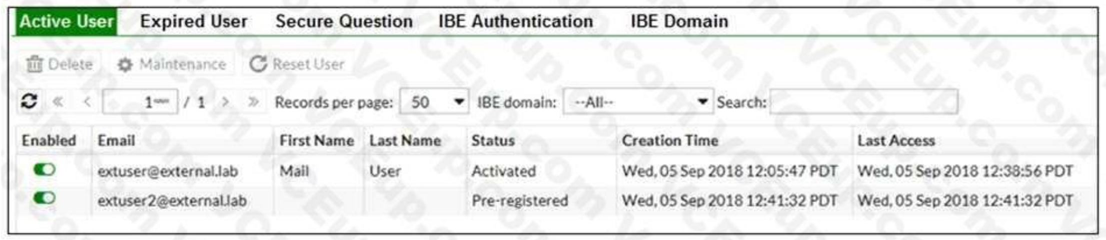
Answer: D

Explanation:

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

Question 2

Refer to the exhibit.



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

Enabled	Email	First Name	Last Name	Status	Creation Time	Last Access
●	extuser@external.lab	Mail	User	Activated	Wed, 05 Sep 2018 12:05:47 PDT	Wed, 05 Sep 2018 12:38:56 PDT
●	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 orattachment 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.

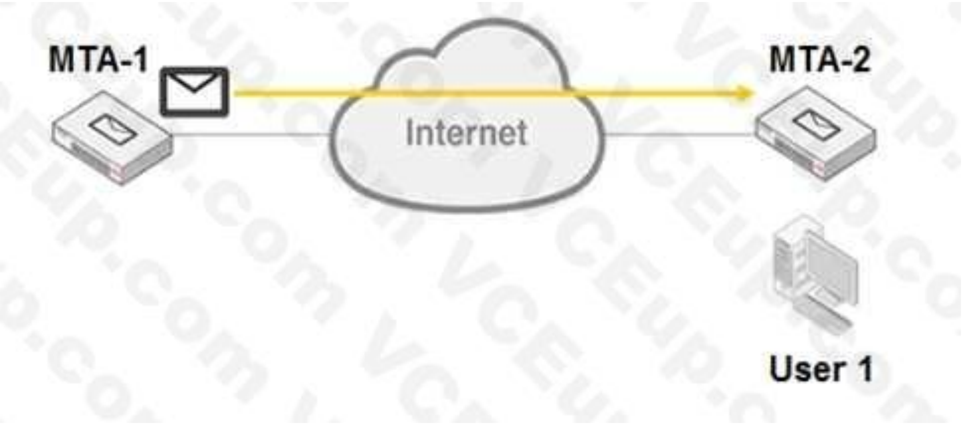
Answer: D

Explanation:

Reference: https://docs.fortinet.com/document/fortimail/6.4.2/administrationguide/470401/configuring-ibe- users

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 logs were generated load 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

Answer: AD

Explanation:

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

Answer: AD

Explanation:

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

Answer: BD

Explanation:

Question 6

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

A. DNSBL

B. SURBL

C. IP reputation

D. URI filter

Answer: AB

Explanation:

Reference: https://docs.fortinet.com/document/fortimail/6.4.0/administrationguide/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

Answer: ABD

Explanation:

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

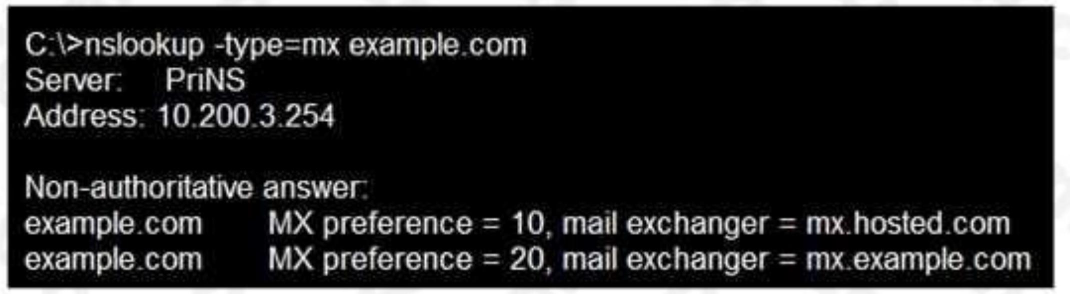
Answer: BCE

Explanation:

Reference: https://docs.fortinet.com/document/fortimail/6.2.0/administrationguide/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

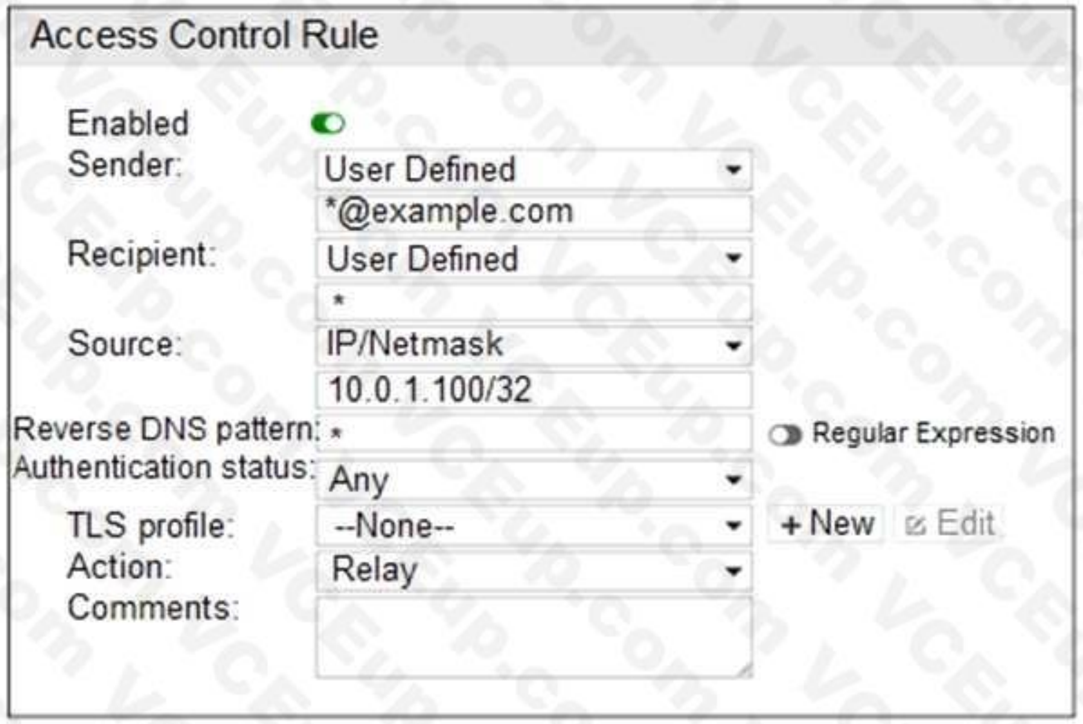
D. The higher preference value is used to load balance more email to the mx.example.com MTA

Answer: AC

Explanation:

Question 10

Refer to the exhibit.



Access Control Rule

Enabled	●
Sender:	User Defined *@example.com
Recipient:	User Defined *
Source:	IP/Netmask 10.0.1.100/32
Reverse DNS pattern:	* ○ Regular Expression
Authentication status:	Any
TLS profile:	--None-- + New Edit
Action:	Relay
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

Explanation:

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

Answer: CD

Explanation:

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

Answer: B

Explanation:

Reference: https://docs.fortinet.com/document/fortimail/6.2.0/administrationguide/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

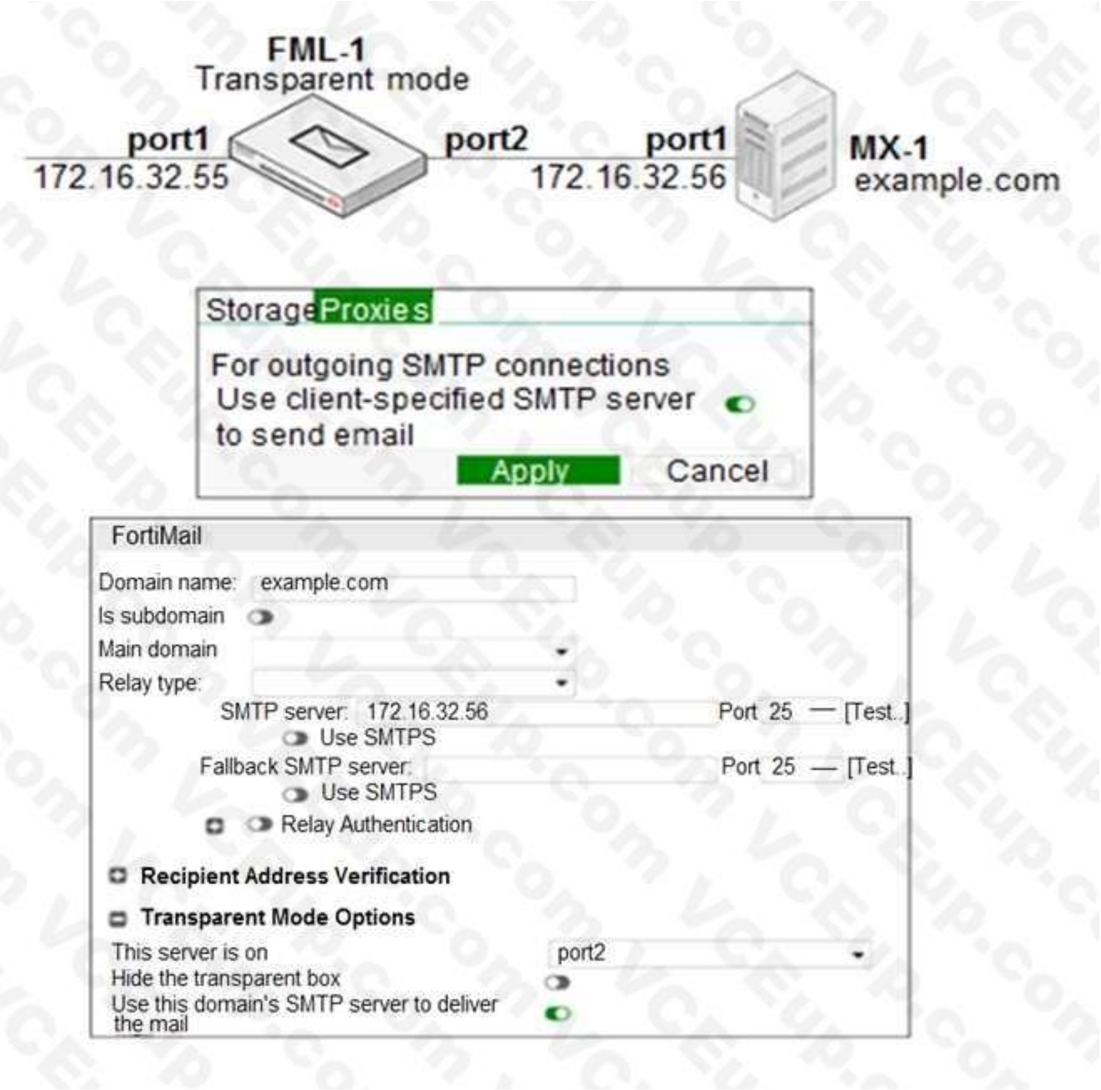
Answer: CD

Explanation:

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: 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

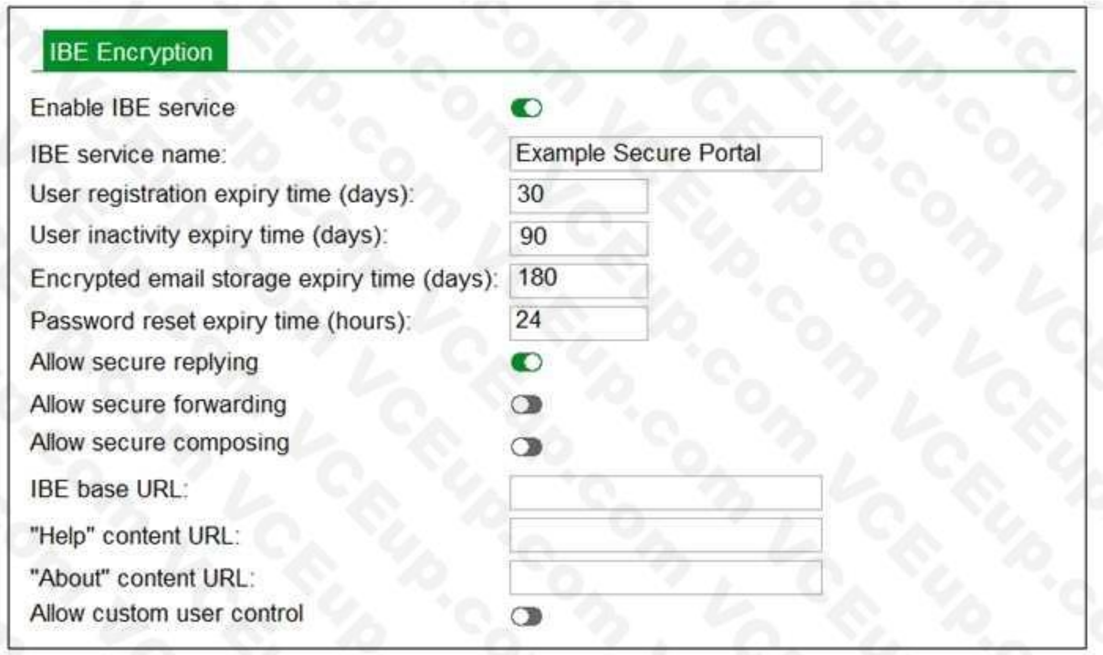
D. FML-1 will use the transparent proxy for incoming sessions

Answer: BD

Explanation:

Question 15

Refer to the exhibit.



IBE Encryption

Enable IBE service	●
IBE service name:	Example Secure Portal
User registration expiry time (days):	30
User inactivity expiry time (days):	90
Encrypted email storage expiry time (days):	180
Password reset expiry time (hours):	24
Allow secure replying	●
Allow secure forwarding	○
Allow secure composing	○
IBE base URL:	
"Help" content URL:	
"About" content URL:	
Allow custom user control	○

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

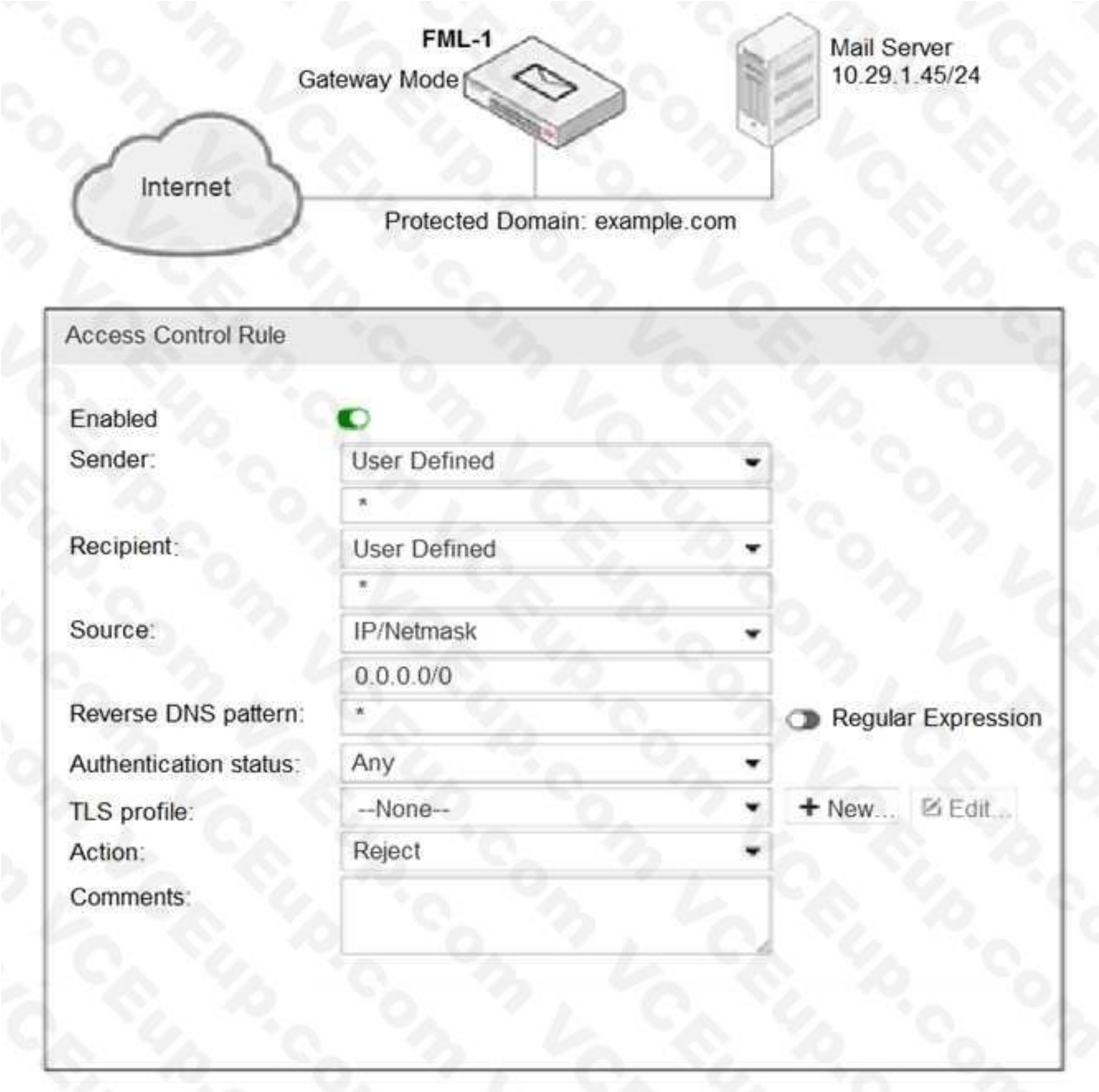
Answer: A

Explanation:

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

Question 16

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:	Reject ▾
Comments:	

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

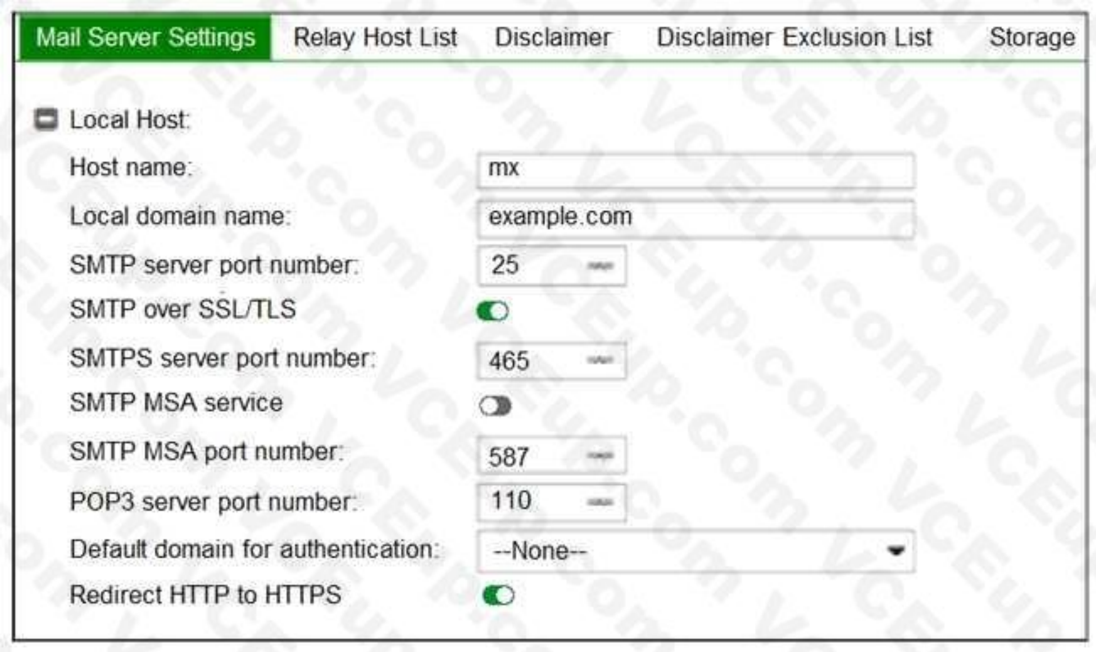
E. The Sender IP/netmask should be set to 10.29.1.45/32

Answer: BDE

Explanation:

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	●
SMTPS server port number:	465
SMTP MSA service	○
SMTP MSA port number:	587
POP3 server port number:	110
Default domain for authentication:	--None--
Redirect HTTP to HTTPS	●

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

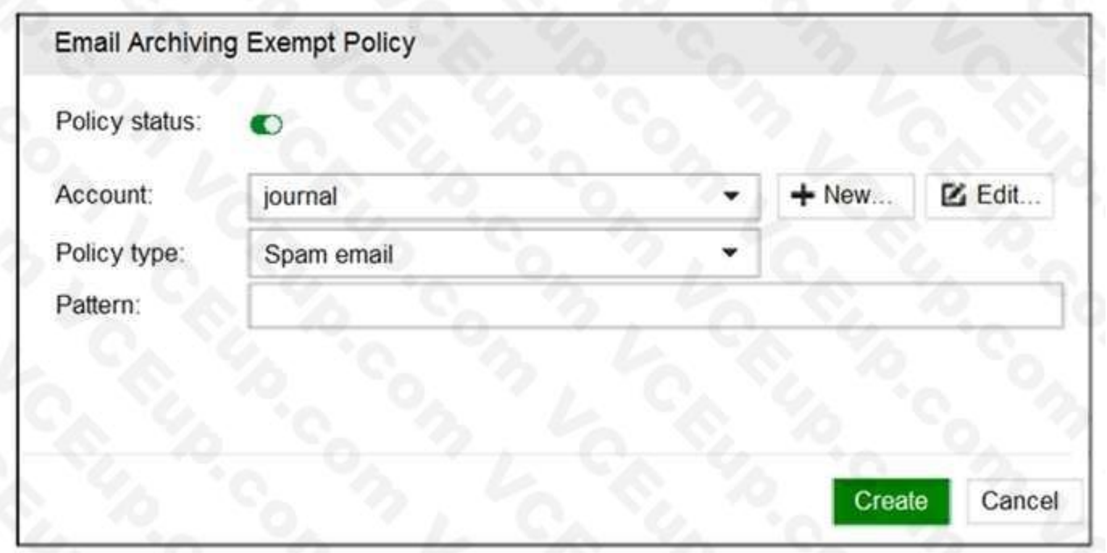
D. FortiMail will enforce SMTPS on all outbound sessions

Answer: BC

Explanation:

Question 18

Refer to the exhibit.



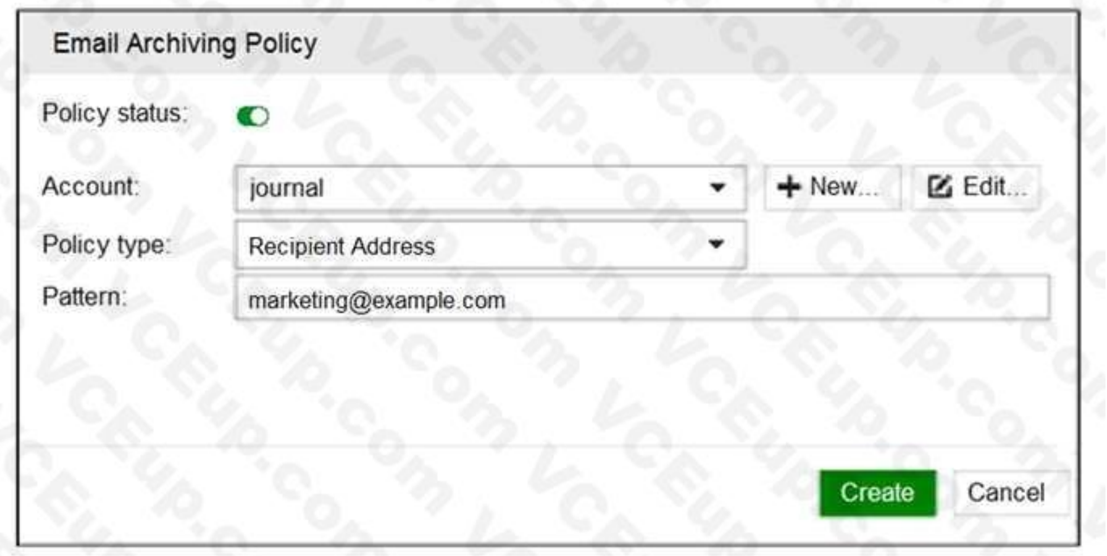
Email Archiving Exempt Policy

Policy status: ●

Account: journal

Policy type: Spam email

Pattern:



Email Archiving Policy

Policy status: ●

Account: journal

Policy type: Recipient Address

Pattern: marketing@example.com

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

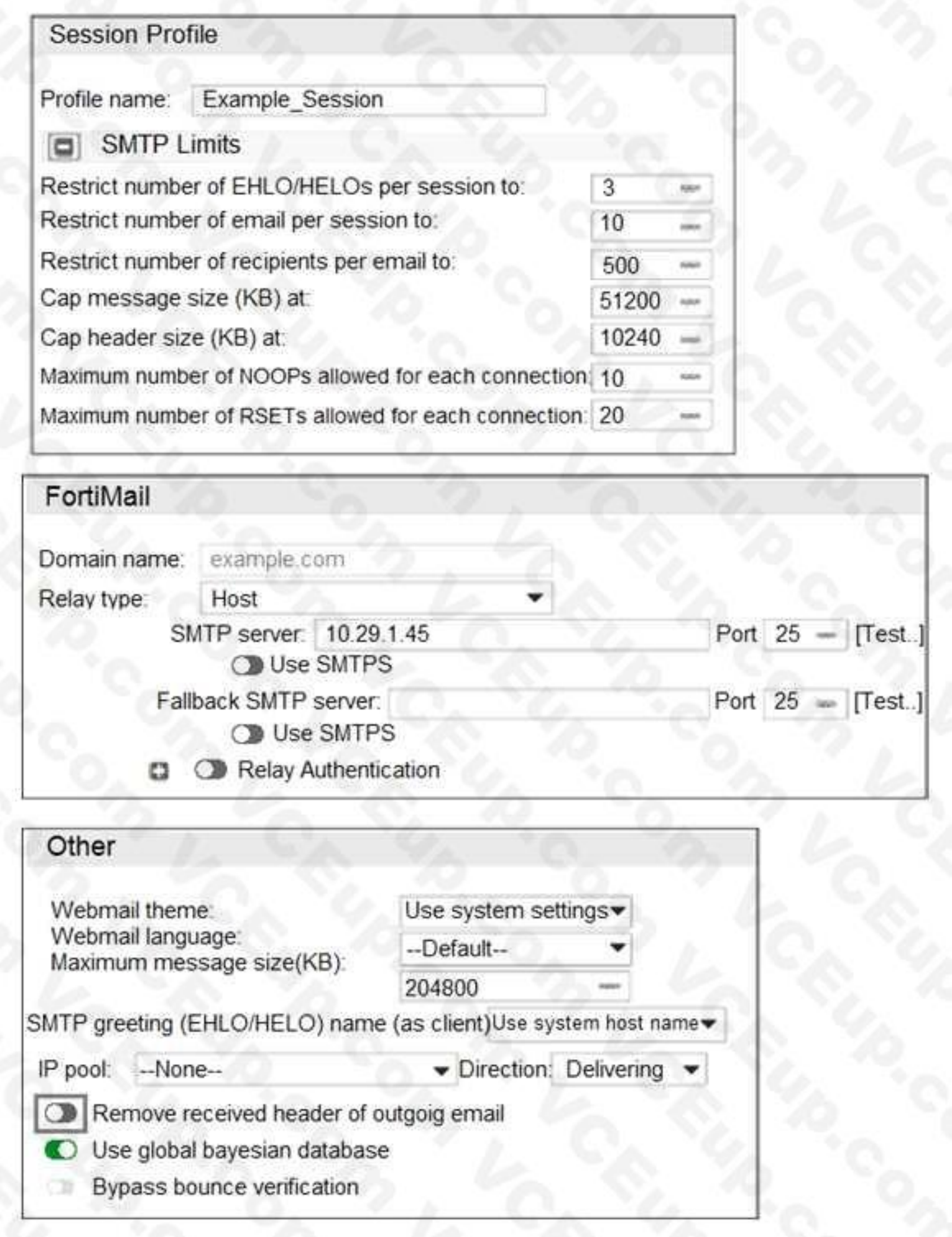
D. FortiMail will archive email sent from marketing@example.com

Answer: AB

Explanation:

Question 19

Refer to the exhibit.



Session Profile

Profile name: Example_Session

SMTP Limits

Restrict number of EHLO/HELOs per session to:	3
Restrict number of email per session to:	10
Restrict number of recipients per email to:	500
Cap message size (KB) at:	51200
Cap header size (KB) at:	10240
Maximum number of NOOPs allowed for each connection:	10
Maximum number of RSETs allowed for each connection:	20

FortiMail

Domain name: example.com

Relay type: Host

SMTP server: 10.29.1.45 Port 25 [Test..]

○ Use SMTPS

Fallback SMTP server: Port 25 [Test..]

○ Use SMTPS

○ Relay Authentication

Other

Webmail theme: Use system settings

Webmail language: --Default--

Maximum message size(KB): 204800

SMTP greeting (EHLO/HELO) name (as client) Use system host name

IP pool: --None-- Direction: Delivering

○ Remove received header of outgoig 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

Answer: A

Explanation:

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

Answer: A

Explanation:

Reference: https://docs.fortinet.com/document/fortimail/6.2.0/administrationguide/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

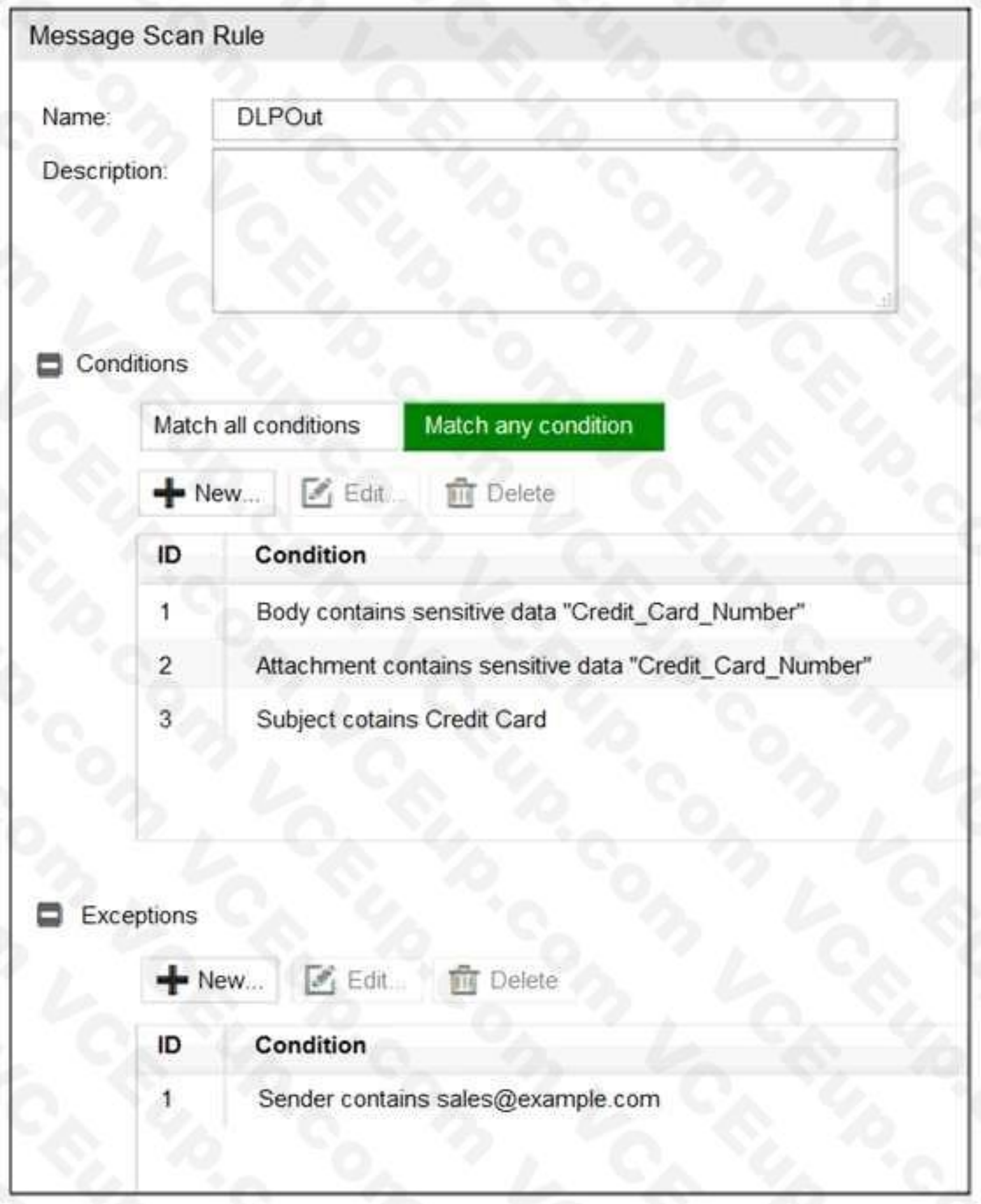
D. FortiMail configuration is missing an access delivery rule

Answer: CD

Explanation:

Question 22

Refer to the exhibit.



Message Scan Rule

Name: DLPOut

Description:

Conditions

Match all conditions | Match any condition

ID	Condition
1	Body contains sensitive data "Credit_Card_Number"
2	Attachment contains sensitive data "Credit_Card_Number"
3	Subject cotains Credit Card

Exceptions

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

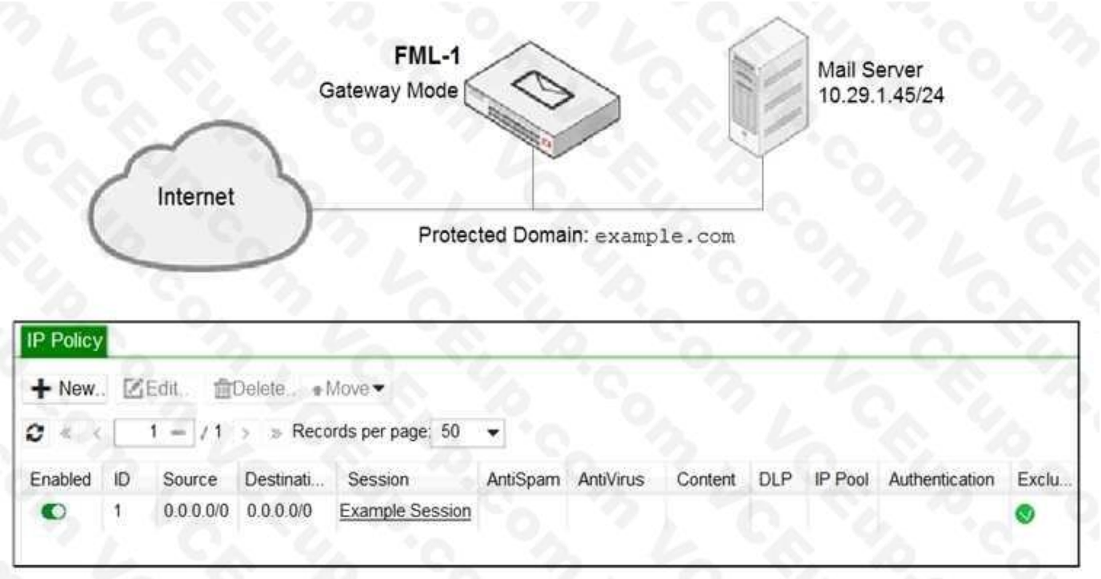
D. An email sent from sales@internal.lab will trigger this scan rule, even without matching any conditions

Answer: BC

Explanation:

Question 23

Refer to the exhibit.



Enabled	ID	Source	Destinati...	Session	AntiSpam	AntiVirus	Content	DLP	IP Pool	Authentication	Exclu...
●	1	0.0.0.0/0	0.0.0.0/0	Example Session							✓

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

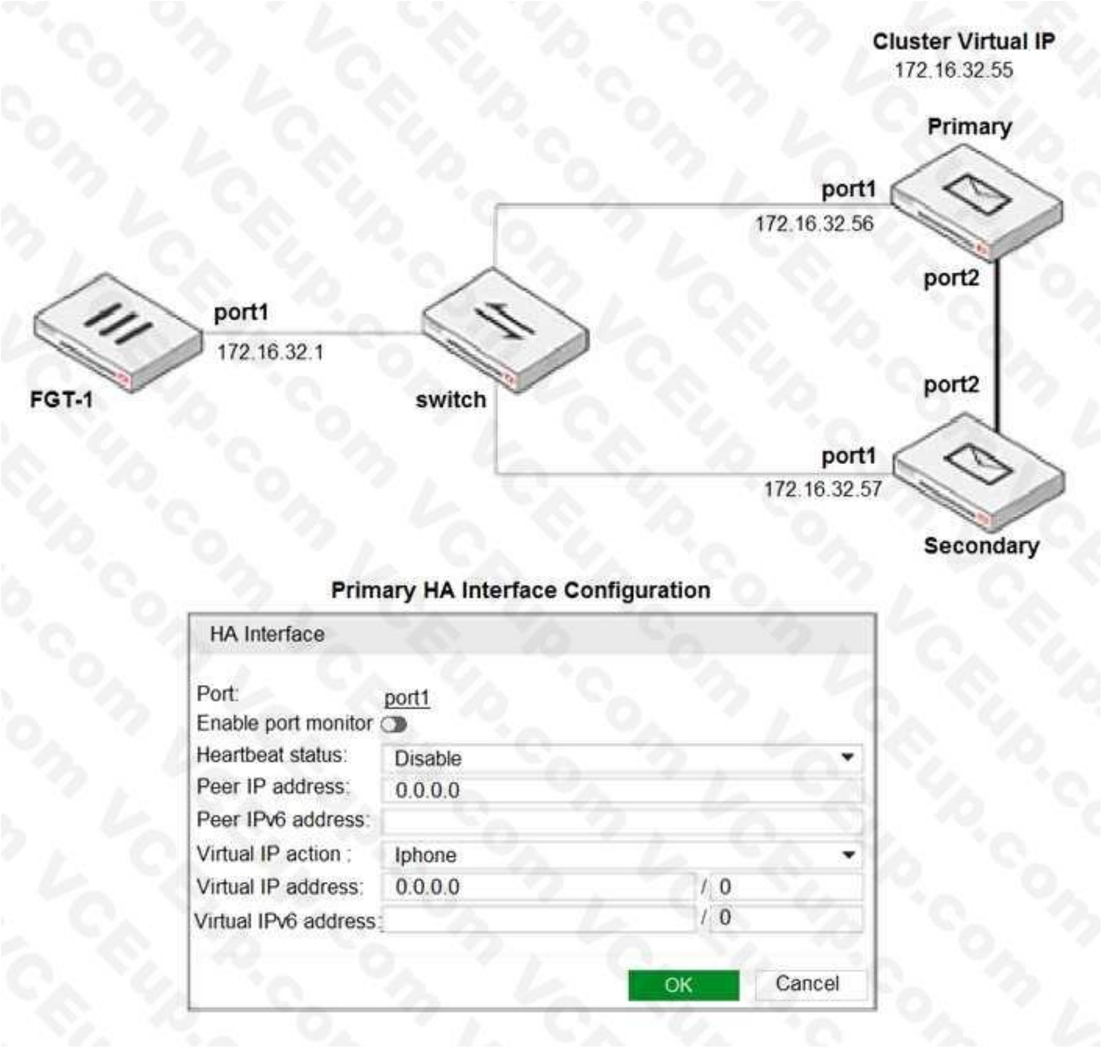
D. Disable the exclusive flag in IP policy ID 1

Answer: AD

Explanation:

Question 24

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

Answer: ABD

Explanation:

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

Answer: CD

Explanation:

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

Answer: C

Explanation:

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

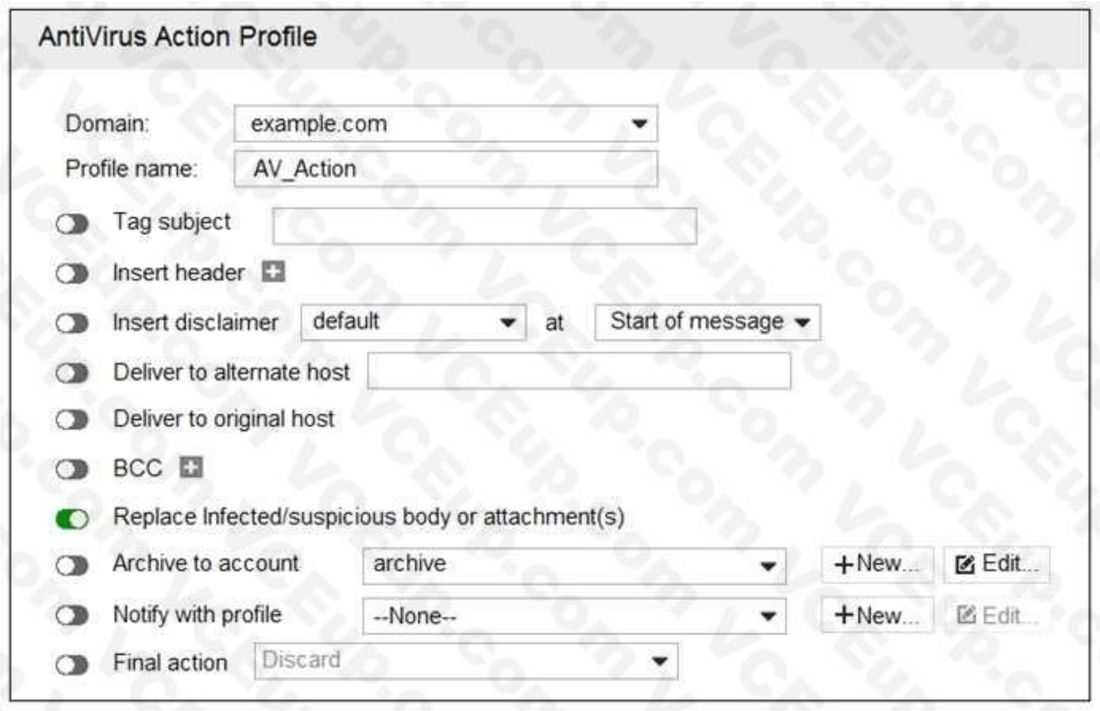
D. There are no access delivery rules configured for outbound email

Answer: CD

Explanation:

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

Answer: BC

Explanation:

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

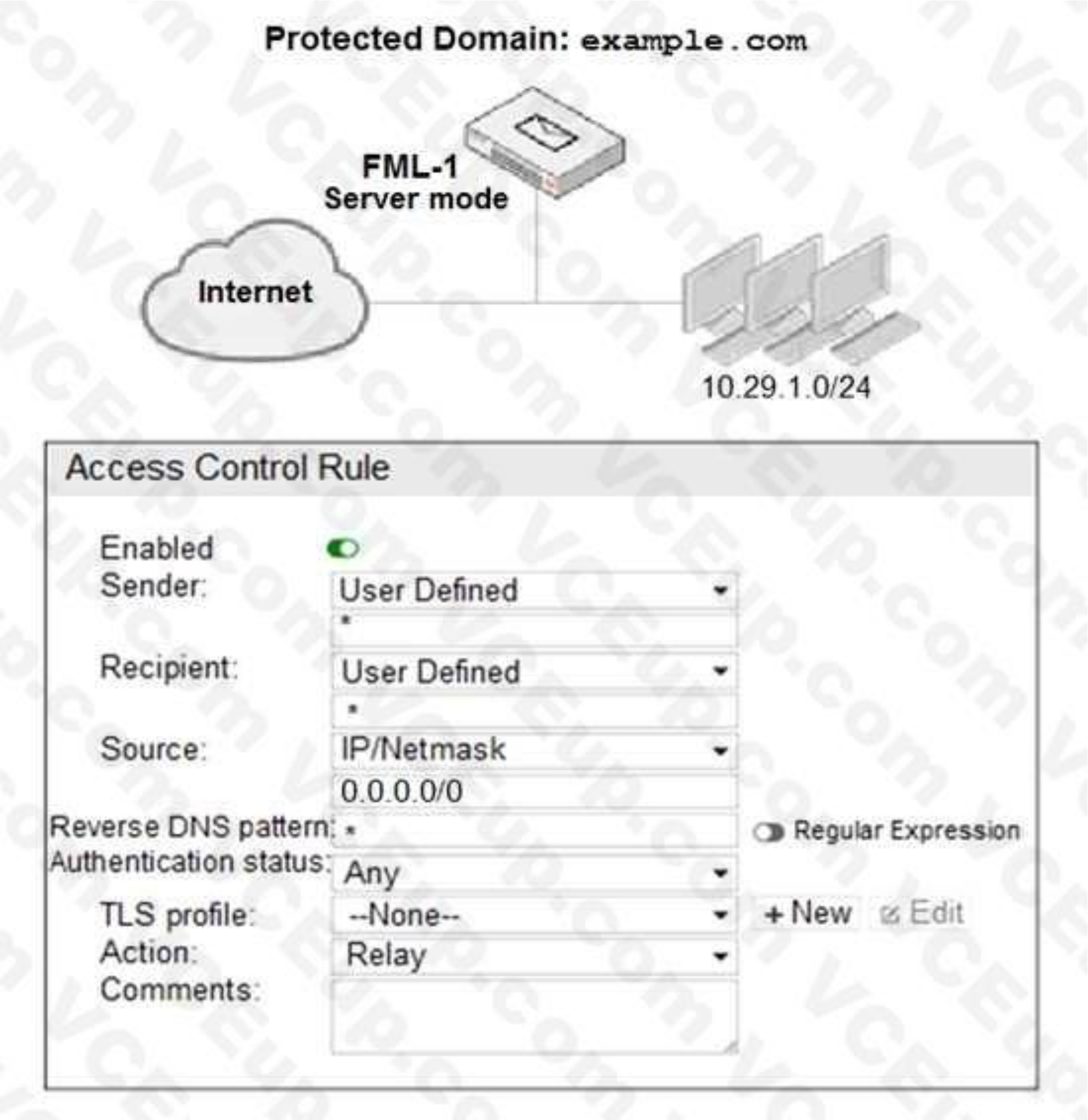
D. Address book management options

Answer: A

Explanation:

Question 30

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

Answer: BC

Explanation:

Question 31

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

Explanation:

Question 32

Which two features are available when you enable HA centralized monitoring on FortiMail? (Choose two.)

A. Policy configuration changes of all cluster members from the primary device.

B. Firmware update of all cluster members from the primary device.

C. Cross-device log searches across all cluster members from the primary device.

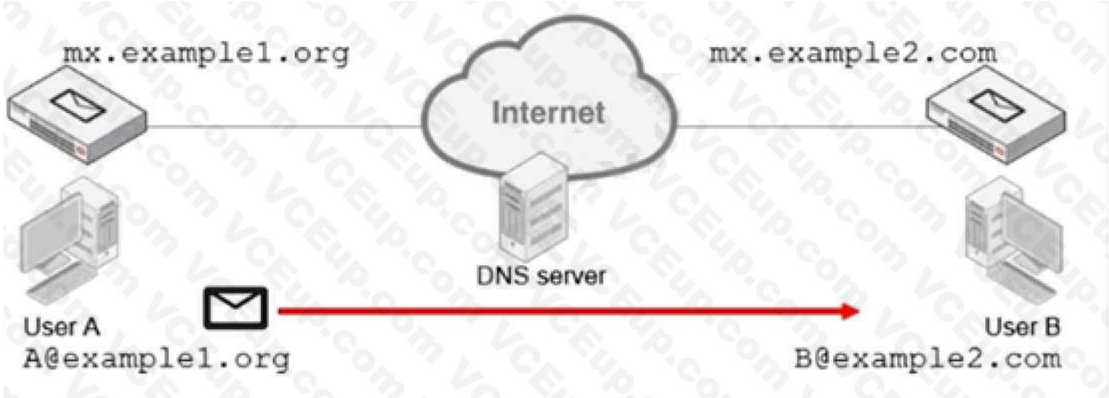
D. Mail statistics of all cluster members on the primary device.

Answer: CD

Explanation:

Question 33

Refer to the exhibit.



Which two statements about email messages sent from User A to User B are correct? (Choose two.)

A. User A's MUA will perform a DNS MX record lookup to send the email message.

B. mx.example1.org will forward the email message to the MX record that has the lowest preference.

C. The DNS server will act as an intermediary MTA.

D. User B will retrieve the email message using either POP3 or IMAP.

Answer: AC

Explanation:

Question 34

Which statement about how impersonation analysis identifies spoofed email addresses is correct?

A. It uses behavior analysis to detect spoofed addresses.

B. It maps the display name to the correct recipient email address.

C. It uses DMARC validation to detect spoofed addresses.

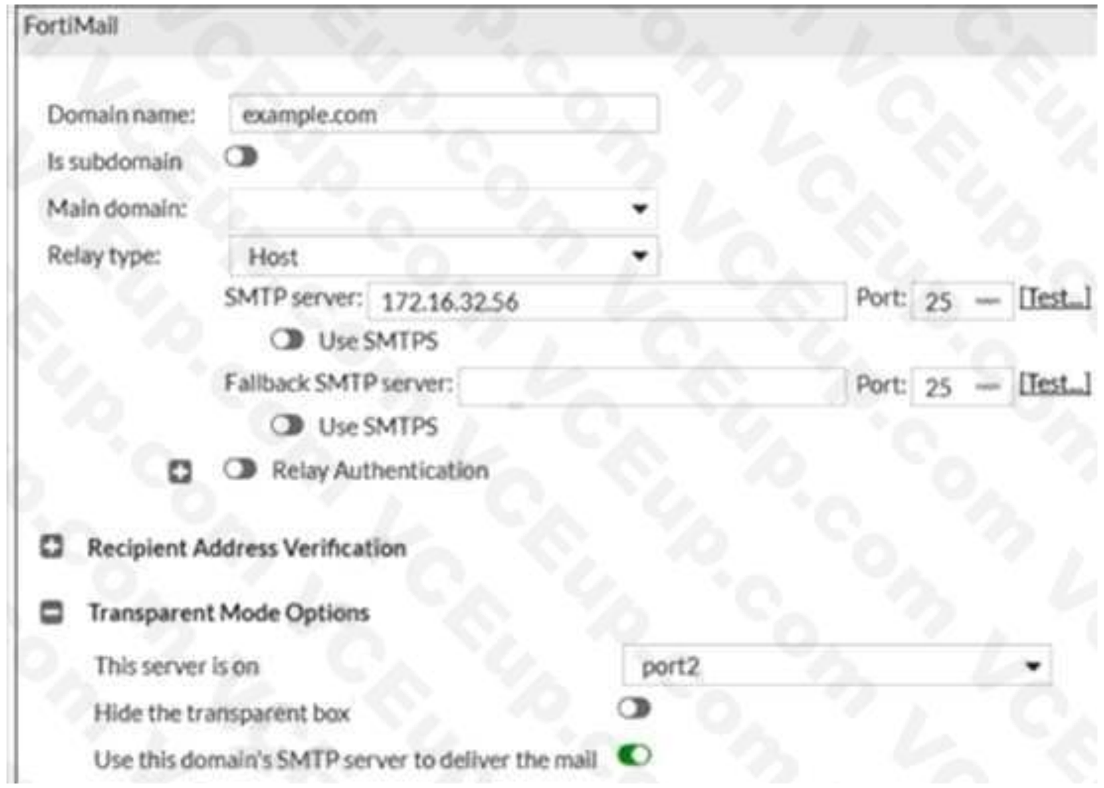
D. It uses SPF validation to detect spoofed addresses.

Answer: A

Explanation:

Question 35

Refer to the exhibit.



FortiMail

Domain name: example.com

○ Is subdomain

Main domain:

Relay type: Host

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 ●

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

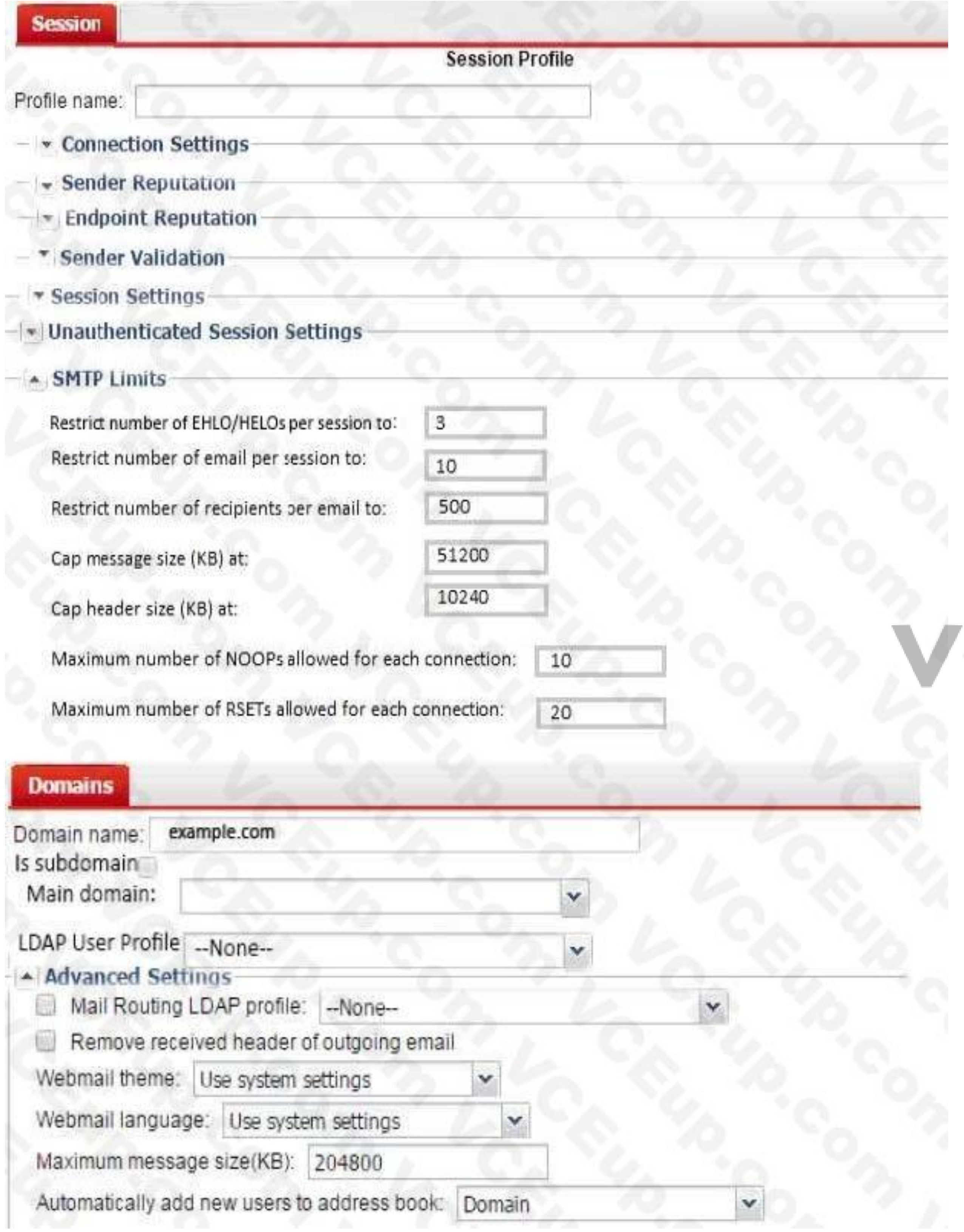
Answer: AC

Explanation:

Topic 2, Extra Main Questions

Question 36

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:	3
Restrict number of email per session to:	10
Restrict number of recipients per email to:	500
Cap message size (KB) at:	51200
Cap header size (KB) at:	10240
Maximum number of NOOPs allowed for each connection:	10
Maximum number of RSETs allowed for each connection:	20

Domains

Domain name: example.com

Is subdomain □

Main domain:

LDAP User Profile --None--

Advanced Settings

□ Mail Routing LDAP profile: --None--

□ Remove received header of outgoing email

Webmail theme: Use system settings

Webmail language: Use system settings

Maximum message size(KB): 204800

Automatically add new users to address book: Domain

Which size limit will FortiMail apply to outbound email?

A. 204800

B. 51200

C. 1024

D. 10240

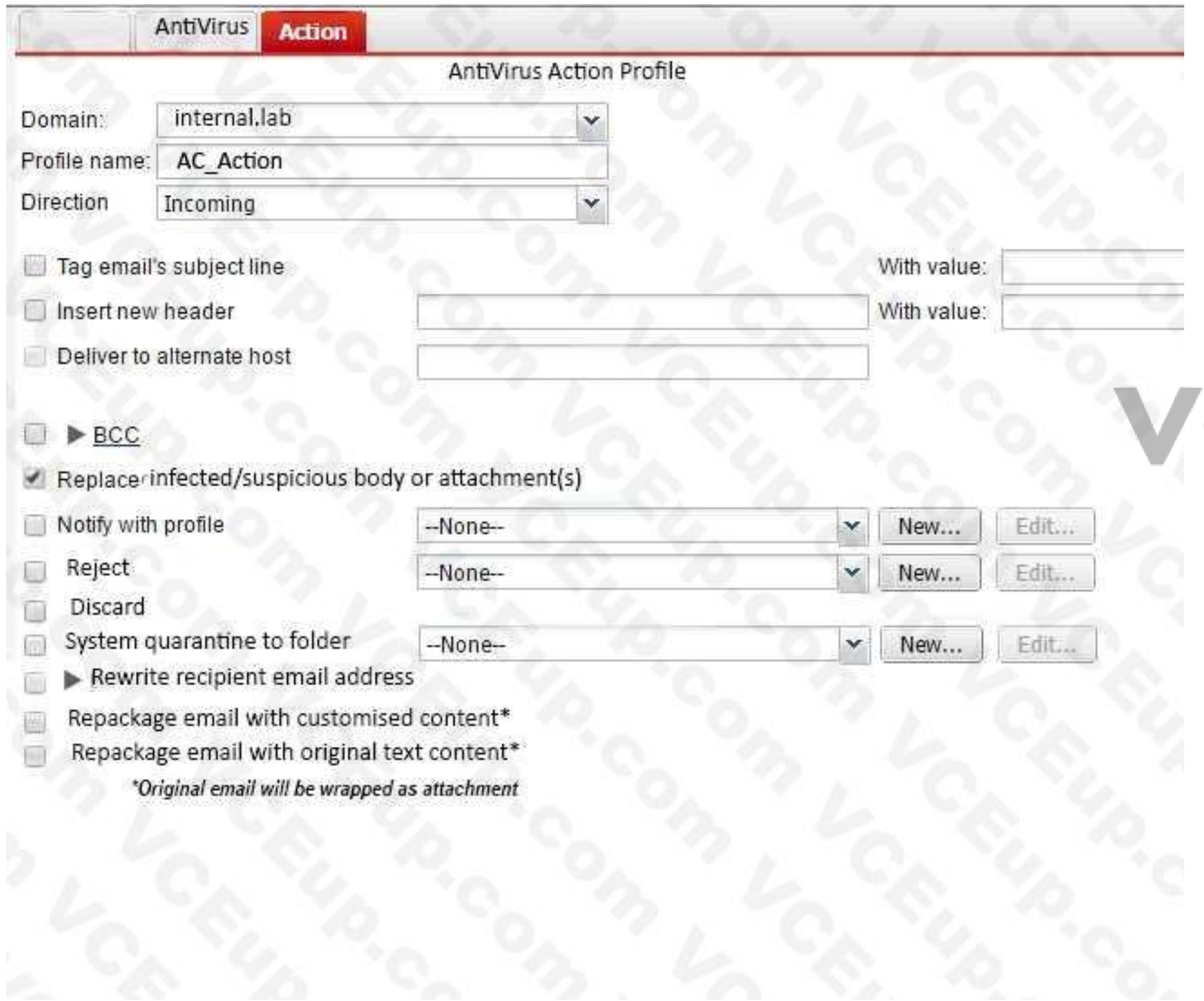
Answer: B

Explanation: domain only applies to inbound.

https://kb.fortinet.com/kb/viewContent.do?externalId=FD31006&sliceId=1

Question 37

Examine the FortiMail antivirus action profile shown in the exhibit; then answer the question below.



AntiVirus Action Profile

Domain: internal.lab

Profile name: AC_Action

Direction: Incoming

□ Tag email's subject line With value:

□ Insert new header With value:

□ Deliver to alternate host

□ ▶ BCC

☑ Replace infected/suspicious body or attachment(s)

□ Notify with profile --None-- New... Edit...

□ Reject --None-- New... Edit...

□ Discard

□ System quarantine to folder --None-- New... Edit...

□ ▶ Rewrite recipient email address

□ Repackage email with customised content*

□ Repackage email with original text content*

*Original email will be wrapped as attachment

What is the expected outcome if FortiMail applies this action profile to an email? (Choose two.)

A. The sanitized email will be sent to the recipient’s personal quarantine

B. A replacement message will be added to the email

C. Virus content will be removed from the email

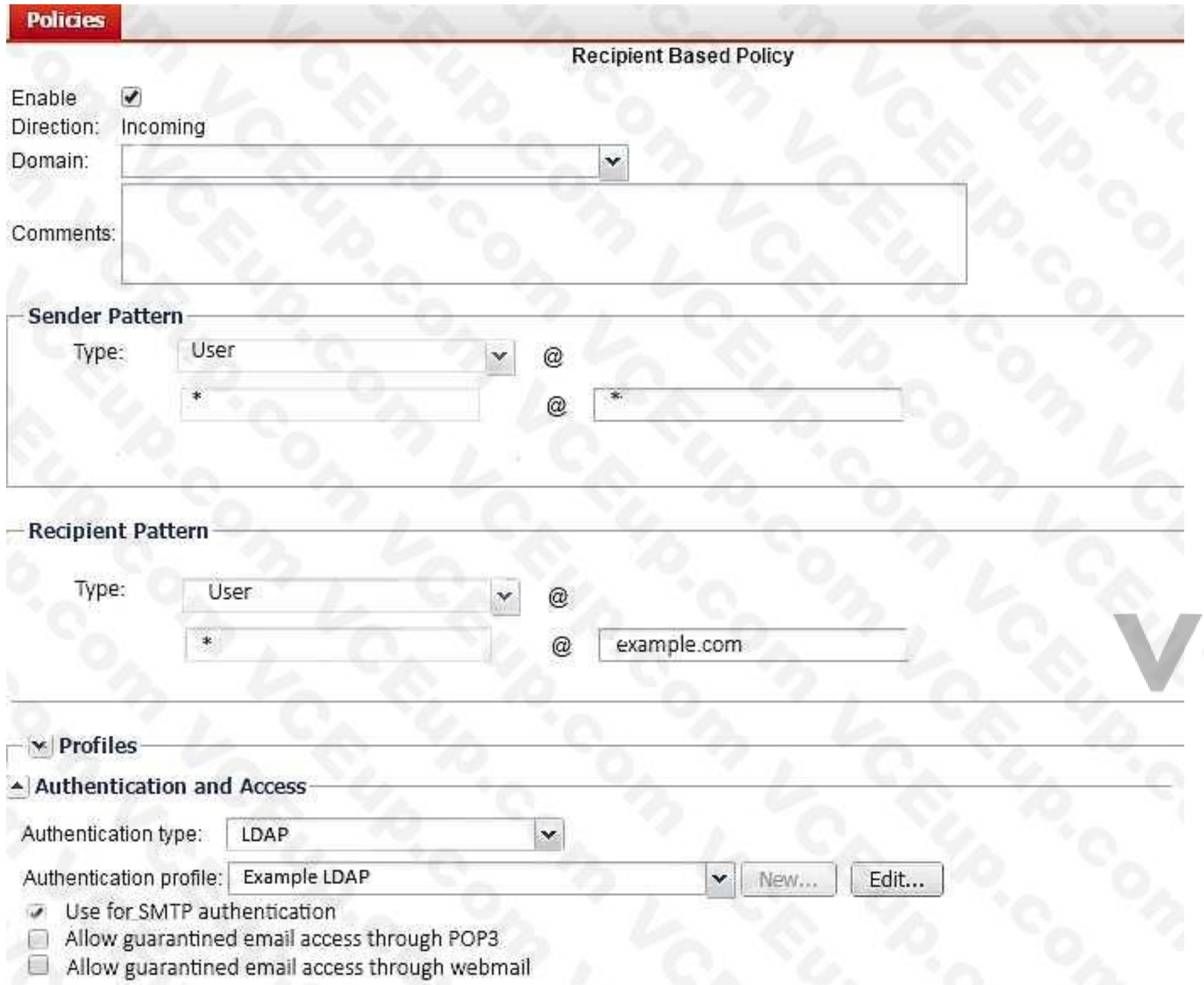
D. The administrator will be notified of the virus detection

Answer: B,C

Explanation:

Question 38

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 quarantined email access through POP3

☐ Allow quarantined 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

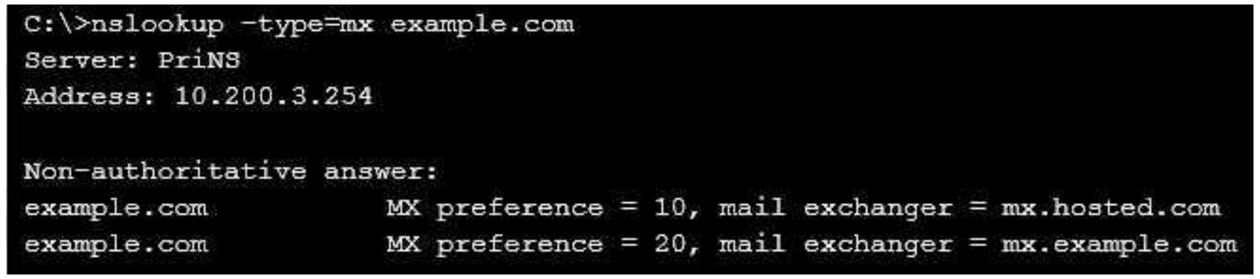
D. Configure an access delivery rule to enforce authentication

Answer: D

Explanation:

Question 39

Examine the nslookup output shown in the exhibit; then answer the question below.



```
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
```

Identify which of the following statements is true regarding the example.com domain's MTAs.

(Choose two.)

A. External MTAs will send email to mx.example.com only if mx.hosted.com is unreachable

B. The primary MTA for the example.com domain is mx.hosted.com

C. The PriNS server should receive all email for the example.com domain

D. The higher preference value is used to load balance more email to the mx.example.com MTA

Answer: AB

Explanation:

Question 40

What are the configuration steps to enable DKIM signing for outbound messages on FortiMail?

(Choose three.)

A. Enable DKIM signing for outgoing messages in a matching session profile

B. Publish the public key as a TXT record in a public DNS server

C. Enable DKIM check in a matching session profile

D. Enable DKIM check in a matching antispam profile

E. Generate a public/private key pair in the protected domain configuration

Answer: A,B,E

Explanation:

DKIM Signing for Outbound Email

• To configure DKIM signing for outgoing messages, you must first generate a public and private key pair for the domain

• DKIM signatures are domain specific

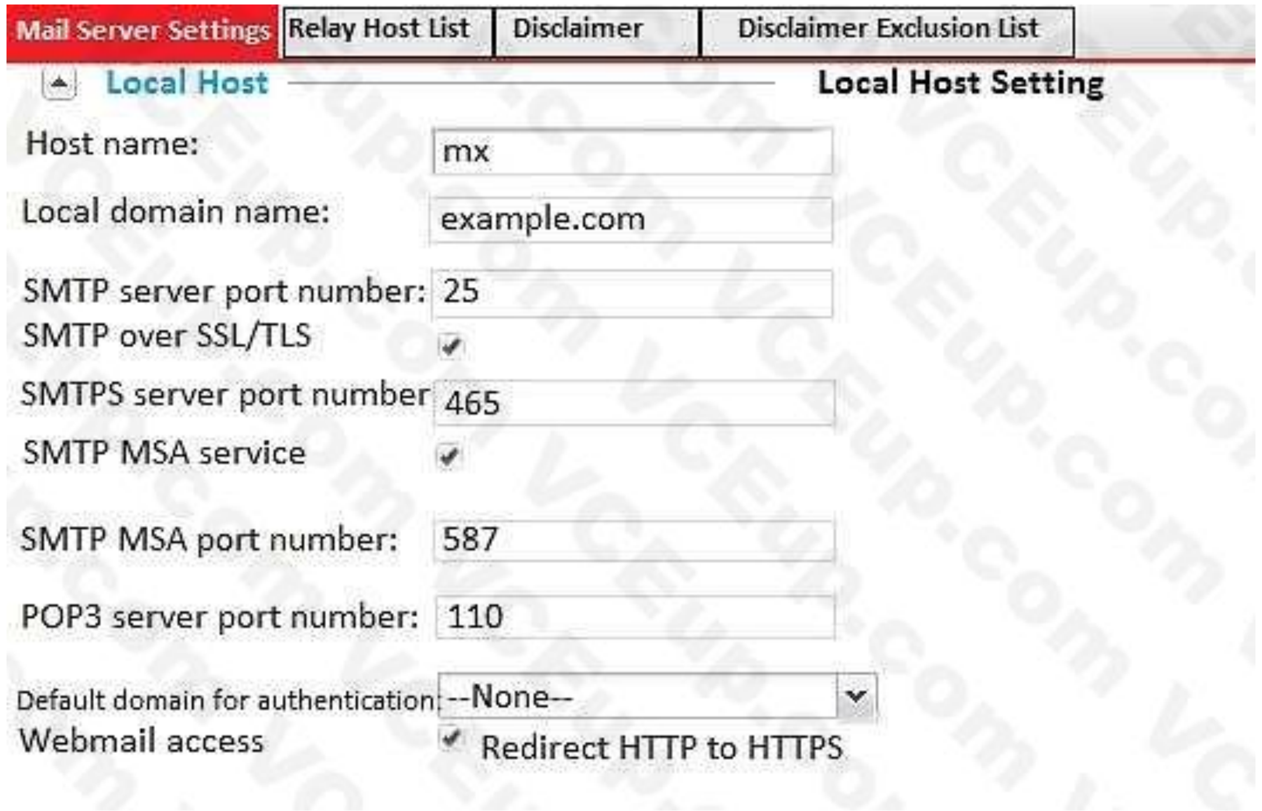
• FortiMail generates and stores the private key, and uses it to generate the DKIM signature

- Download the public key and publish to your external DNS server

- Enable sign outgoing messages with a DKIM signature

Question 41

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



Local Host — Local Host Setting

Host name: mx

Local domain name: example.com

SMTP server port number: 25

SMTP over SSL/TLS ☑

SMTPS server port number 465

SMTP MSA service ☑

SMTP MSA port number: 587

POP3 server port number: 110

Default domain for authentication: --None--

Webmail access ☑ 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

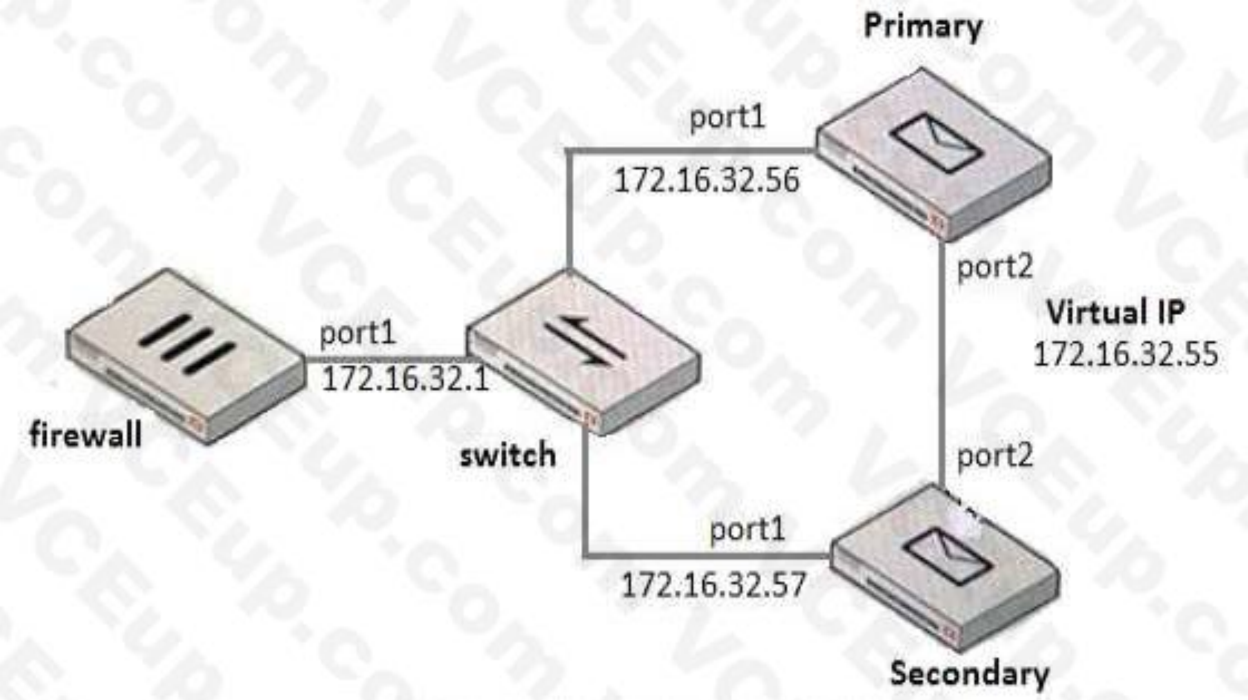
D. mx.example.com will drop any inbound plaintext SMTP connection

Answer: B,C

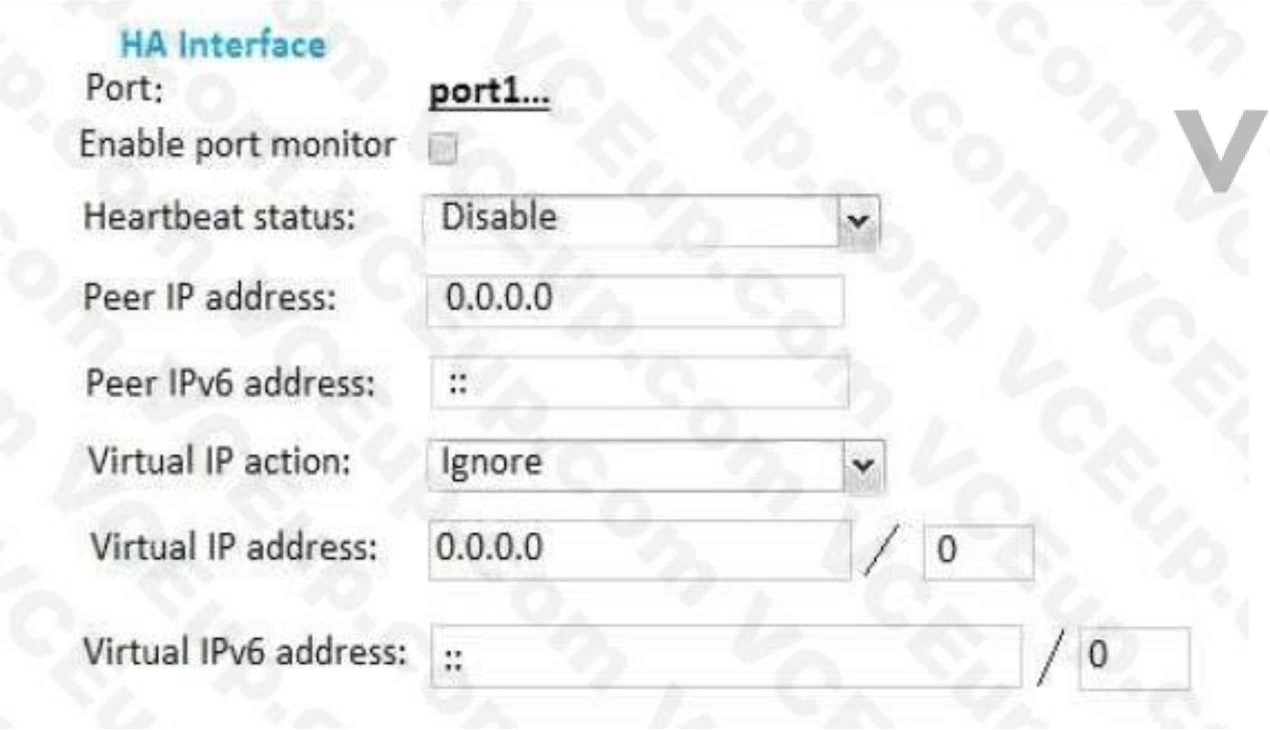
Explanation:

Question 42

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

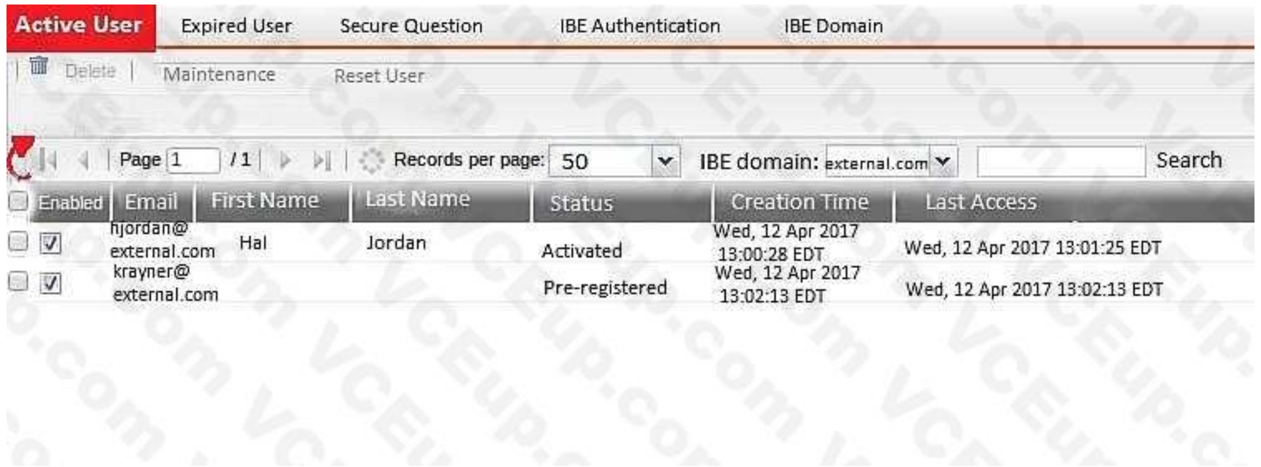
E. Virtual IP action: Use

Answer: C,D,E

Explanation:

Question 43

Examine the FortiMail IBE users shown in the exhibit; then answer the question below



□	Enabled	Email	First Name	Last Name	Status	Creation Time	Last Access
□	☑	hjordan@ external.com	Hal	Jordan	Activated	Wed, 12 Apr 2017 13:00:28 EDT	Wed, 12 Apr 2017 13:01:25 EDT
□	☑	krayner@ external.com			Pre-registered	Wed, 12 Apr 2017 13:02:13 EDT	Wed, 12 Apr 2017 13:02:13 EDT

Which one of the following statements describes the Pre-registered status of the IBE user krayner@external.com?

A. The user was registered by an administrator in anticipation of IBE participation

B. The user has completed the IBE registration process but has not yet accessed their IBE email

C. The user has received an IBE notification email, but has not accessed the HTTPS URL or attachmentyet

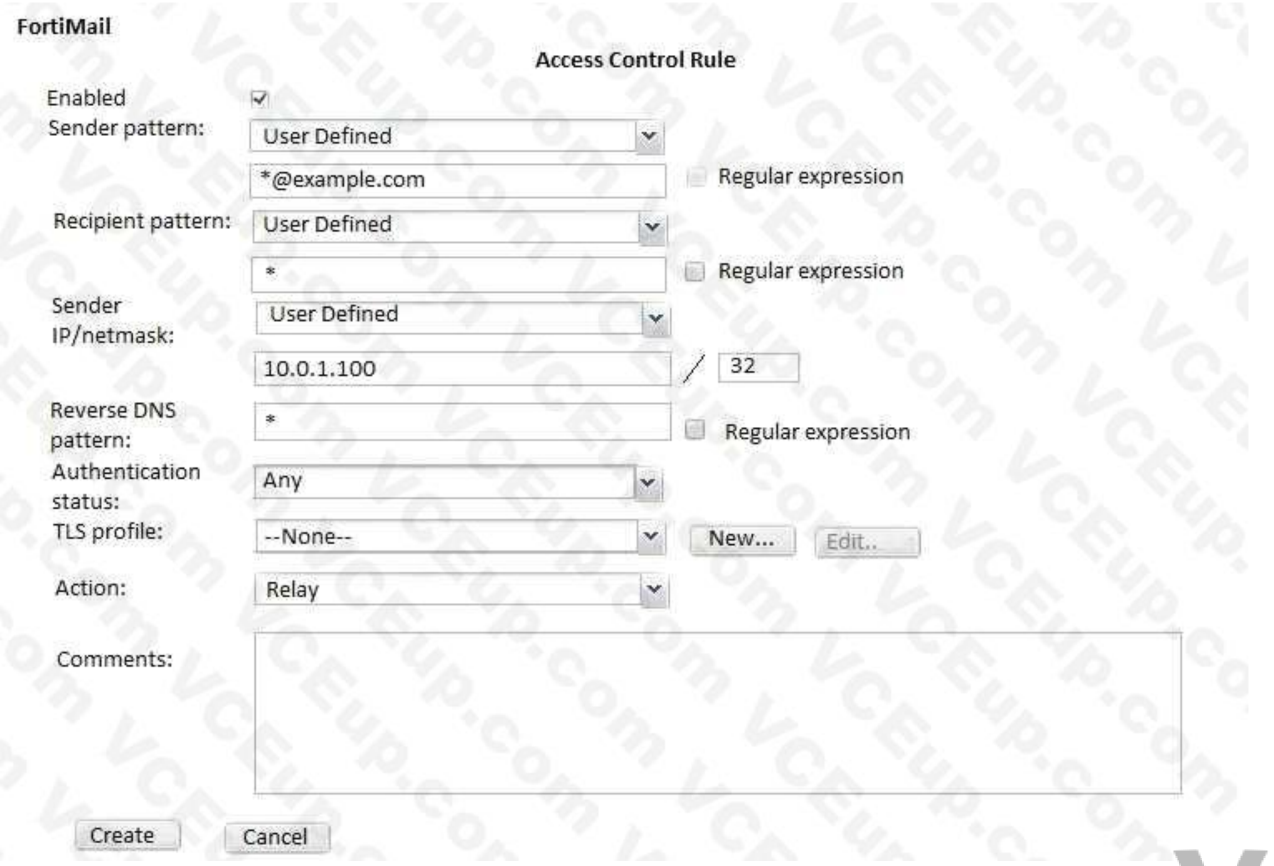
D. The user account has been de-activated, and the user must register again the next time they receive an IBE email

Answer: C

Explanation:

Question 44

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



FortiMail

Access Control Rule

Enabled	☑	
Sender pattern:	User Defined	
	*@example.com	□ Regular expression
Recipient pattern:	User Defined	
	*	□ Regular expression
Sender IP/netmask:	User Defined	
	10.0.1.100 / 32	
Reverse DNS pattern:	*	□ Regular expression
Authentication status:	Any	
TLS profile:	--None--	New... Edit..
Action:	Relay	
Comments:		

Create Cancel

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: C,D

Explanation:

Question 45

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

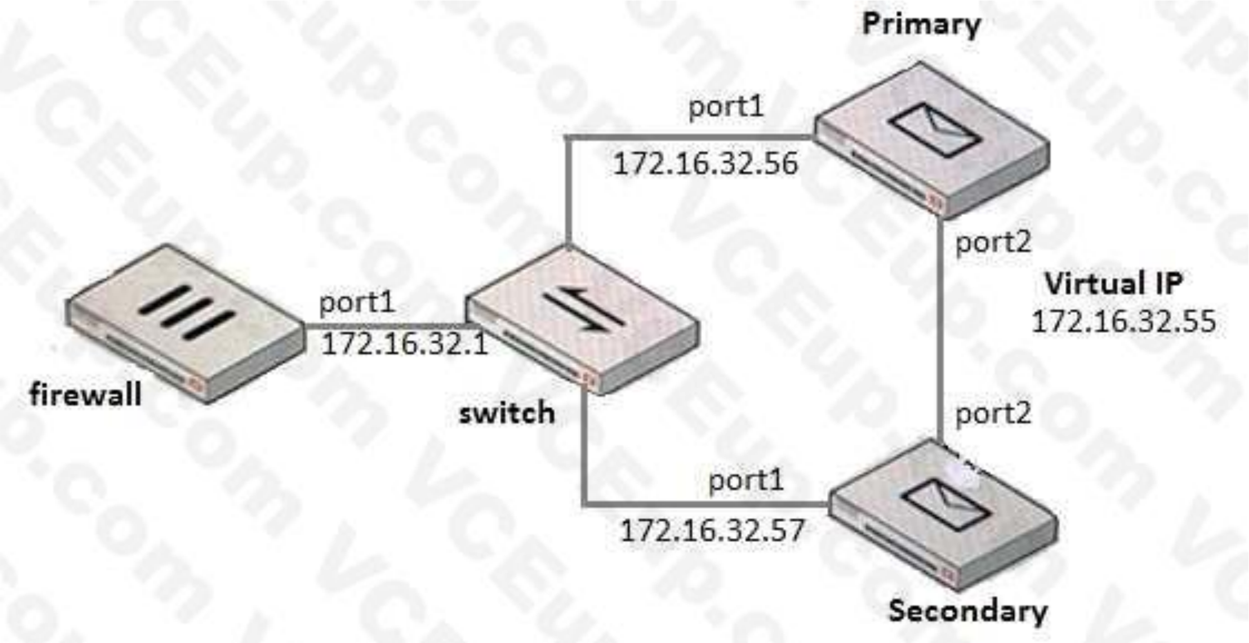
D. MUAs need to be configured to connect to the built-in MTA to send email

Answer: A,C

Explanation:

Question 46

Refer to the exhibit.



What IP address should the DNS MX record for this deployment resolve to?

A. 172.16.32.1

B. 172.16.32.57

C. 172.16.32.55

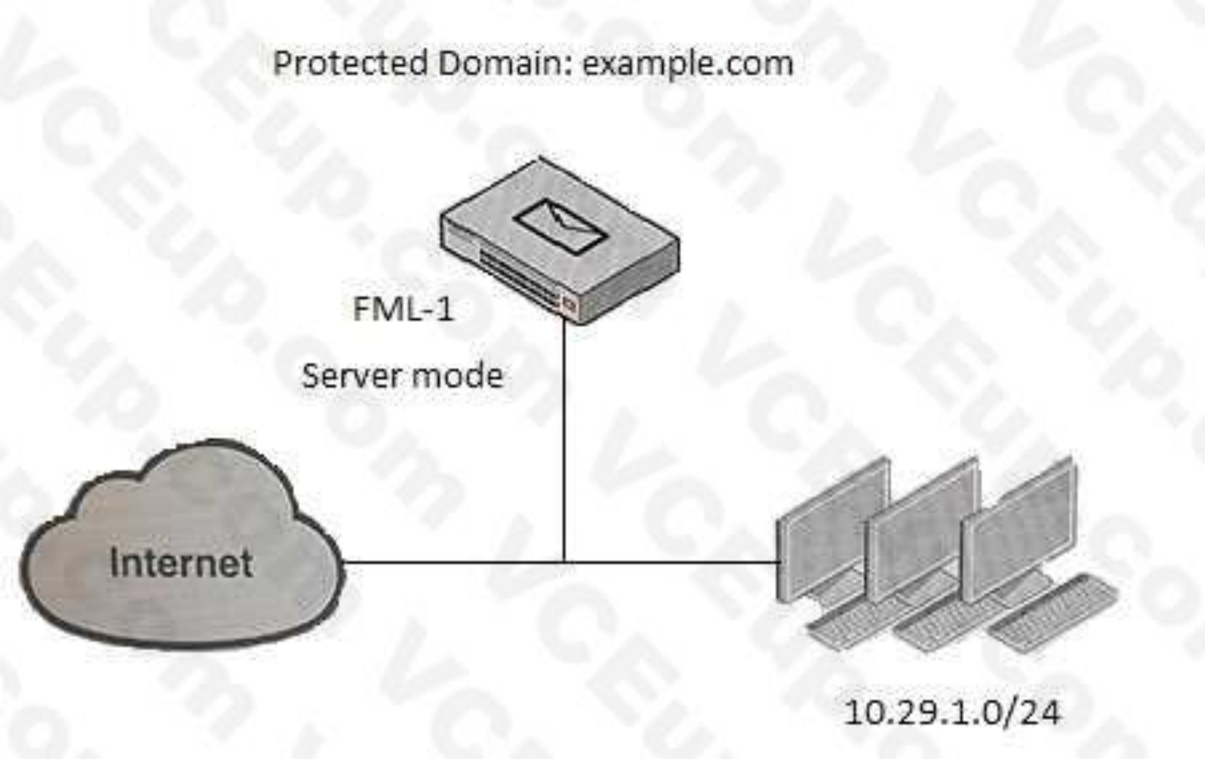
D. 172.16.32.56

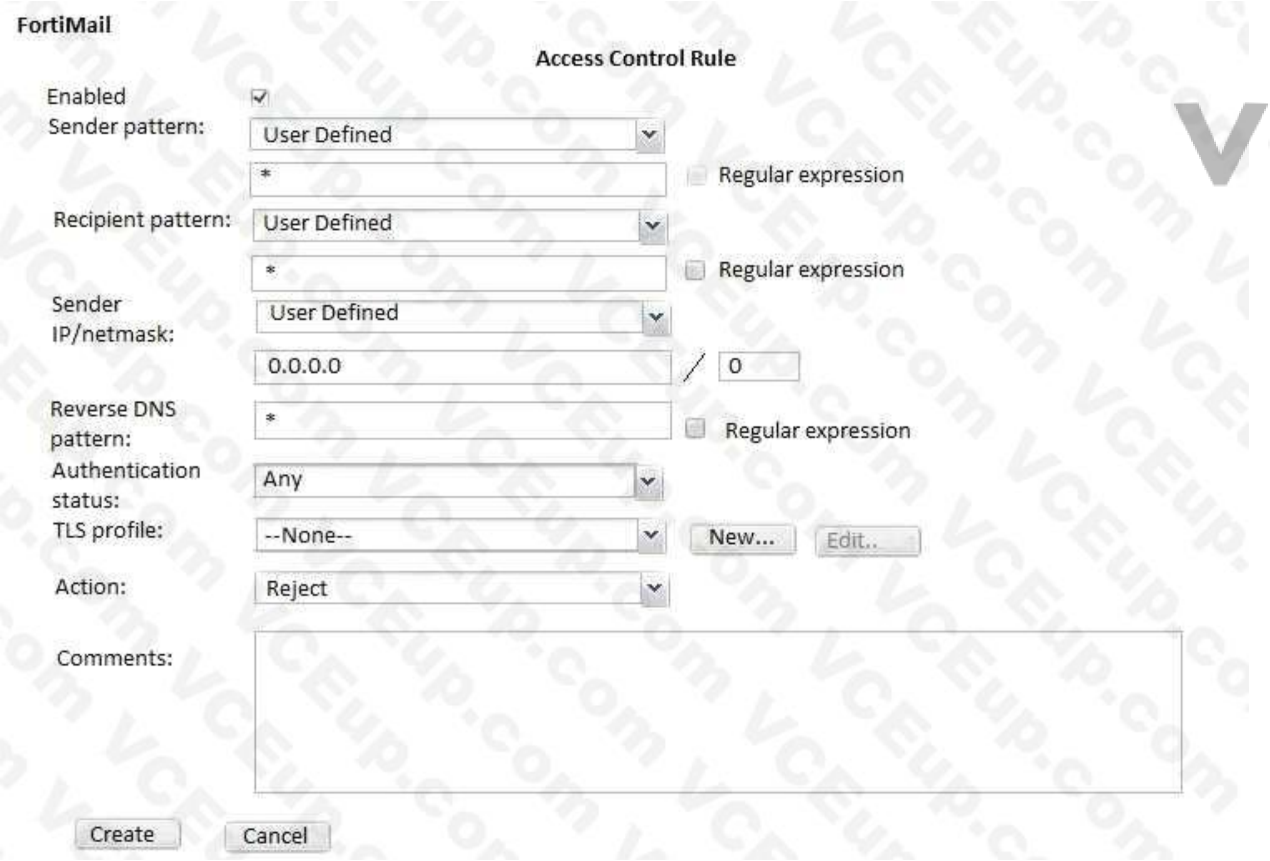
Answer: C

Explanation:

Question 47

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




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:		

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

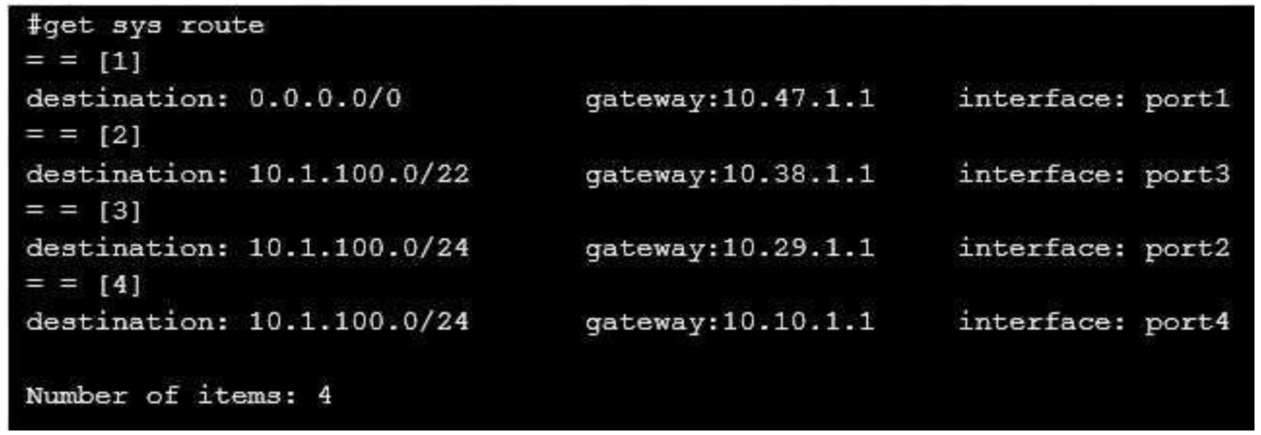
D. The Action should be set to Reject

Answer: AB

Explanation:

Question 48

Examine the configured routes shown in the exhibit; then answer the question below.



```
#get sys route
= = [1]
destination: 0.0.0.0/0          gateway:10.47.1.1     interface: port1
= = [2]
destination: 10.1.100.0/22      gateway:10.38.1.1     interface: port3
= = [3]
destination: 10.1.100.0/24      gateway:10.29.1.1     interface: port2
= = [4]
destination: 10.1.100.0/24      gateway:10.10.1.1     interface: port4

Number of items: 4
```

Which interface will FortiMail use to forward an email message destined for 10.1.100.252?

A. port2

B. port4

C. port3

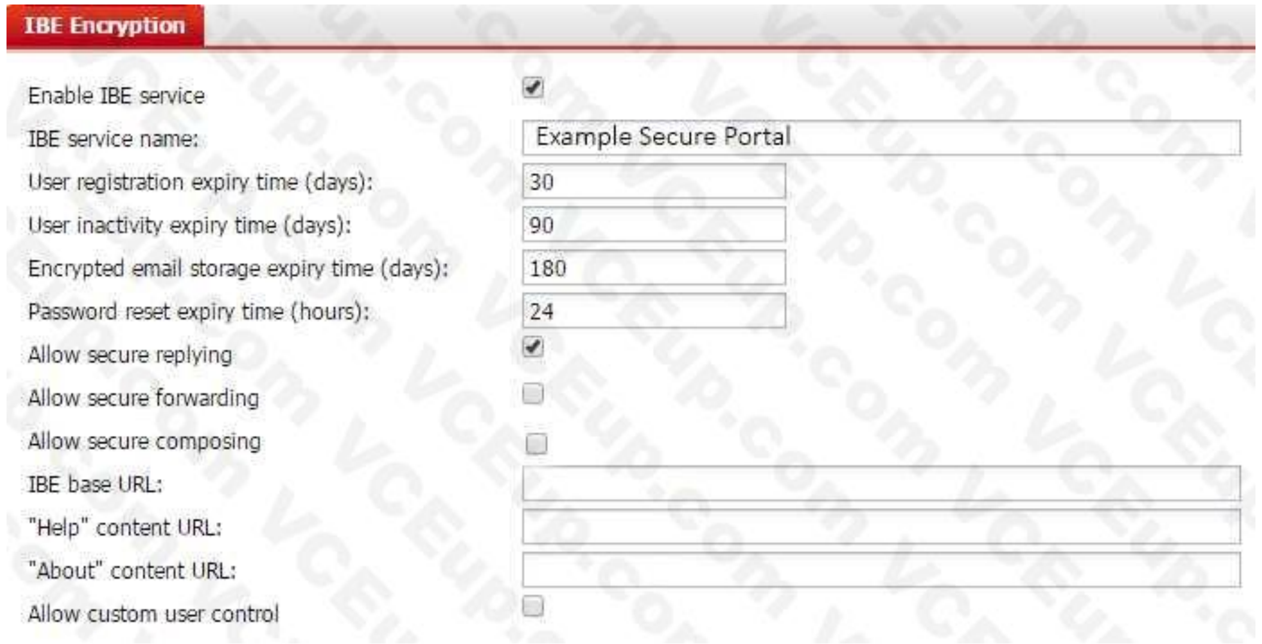
D. port1

Answer: A

Explanation:

Question 49

Examine the FortiMail IBE service configuration shown in the exhibit; then answer the question below.



IBE Encryption

Enable IBE service ☑

IBE service name: Example Secure Portal

User registration expiry time (days): 30

User inactivity expiry time (days): 90

Encrypted email storage expiry time (days): 180

Password reset expiry time (hours): 24

Allow secure replying ☑

Allow secure forwarding □

Allow secure composing □

IBE base URL:

"Help" content URL:

"About" content URL:

Allow custom user control □

Which of the following statements describes the User inactivity expiry time of 90 days?

A. First time IBE users must register to access their email within 90 days of receiving the notification email message

B. After initial registration, IBE users can access the secure portal without authenticating again for 90 days

C. Registered IBE users have 90 days from the time they receive a notification email message to access their IBE email

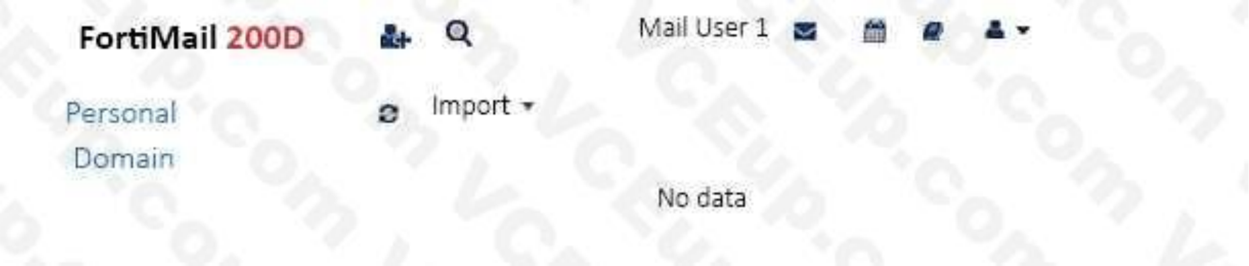
D. IBE user accounts will expire after 90 days of inactivity, and must register again to access new IBE email message

Answer: D

Explanation:

Question 50

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

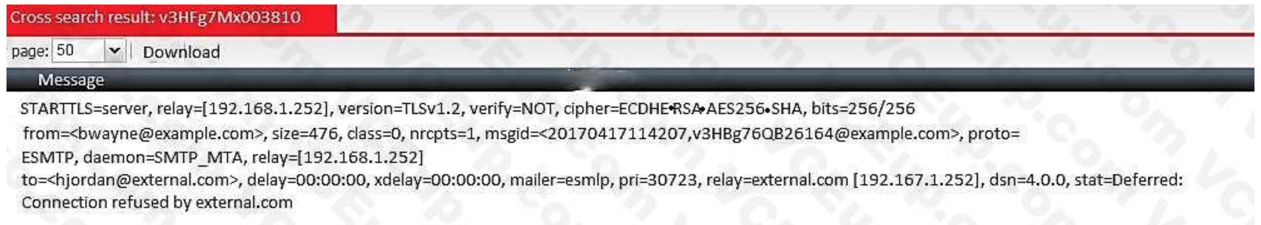
D. The administrator has configured an inbound recipient policy with a customized resource profile

Answer: D

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

Question 51

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



```
STARTTLS=server, relay=[192.168.1.252], version=TLSv1.2, verify=NOT, cipher=ECDHE•RSA•AES256•SHA, bits=256/256
from=<bwayne@example.com>, size=476, class=0, nrcpts=1, msgid=<20170417114207,v3HBg76QB26164@example.com>, proto=
ESMTP, daemon=SMTP_MTA, relay=[192.168.1.252]
to=<hjordan@external.com>, delay=00:00:00, xdelay=00:00:00, mailer=esmlp, pri=30723, relay=external.com [192.167.1.252], dsn=4.0.0, stat=Deferred:
Connection refused by external.com
```

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

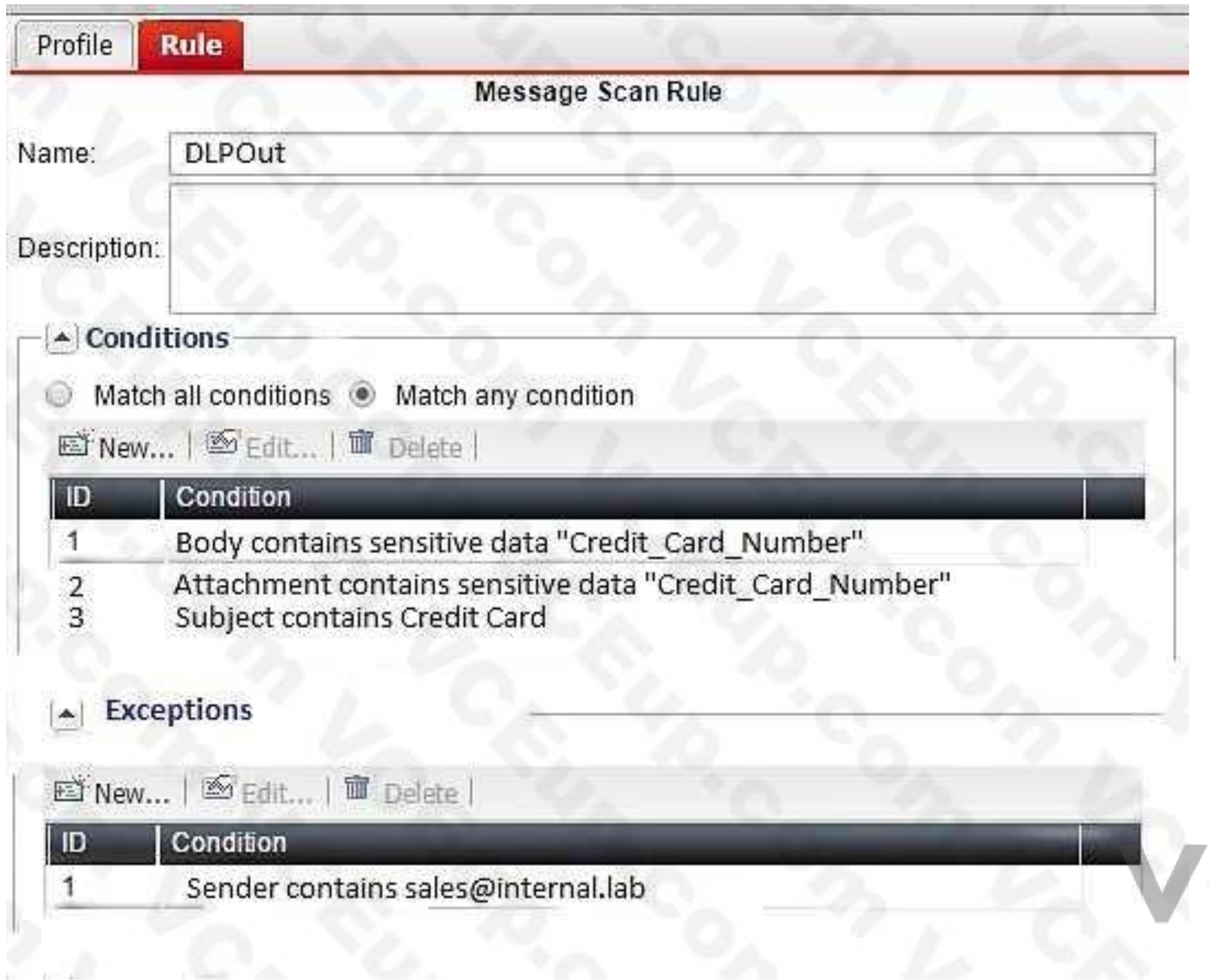
D. The FortiMail is experiencing issues accepting the connection from the remote sender

Answer: AC

Explanation:

Question 52

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



Message Scan Rule

Name: DLPOut

Description:

Conditions

○ Match all conditions ● Match any condition

ID	Condition
1	Body contains sensitive data "Credit_Card_Number"
2	Attachment contains sensitive data "Credit_Card_Number"
3	Subject contains Credit Card

Exceptions

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

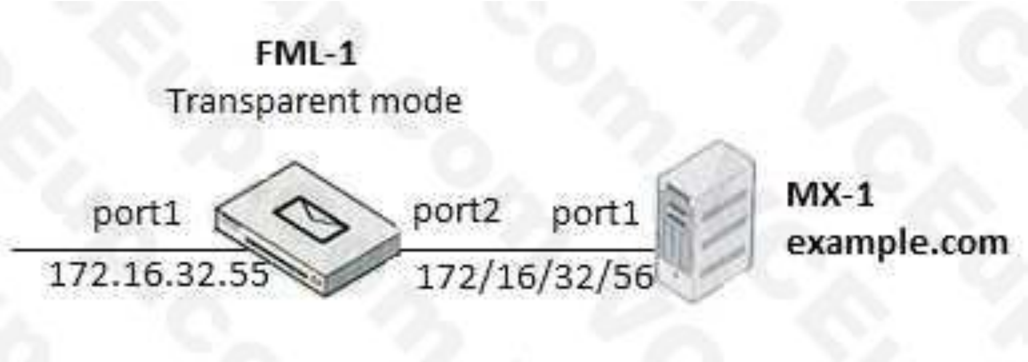
D. An email must contain credit card numbers in the body, attachment, and subject to trigger this scan rule

Answer: A,C

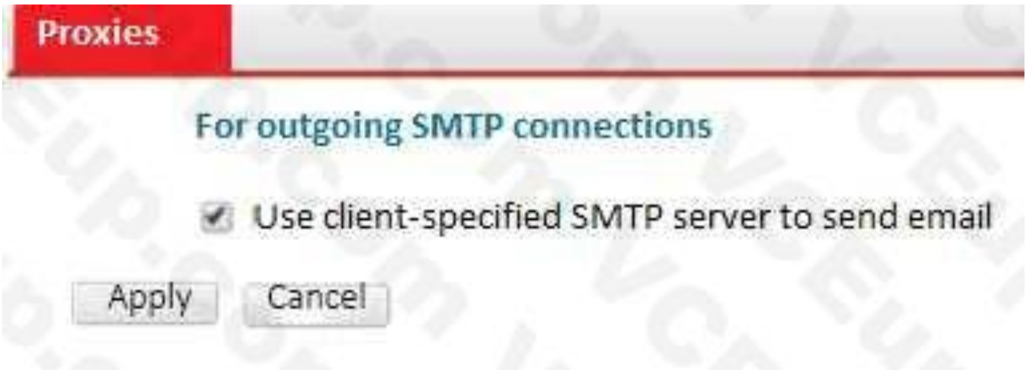
Explanation:

Question 53

Refer to the exhibit.

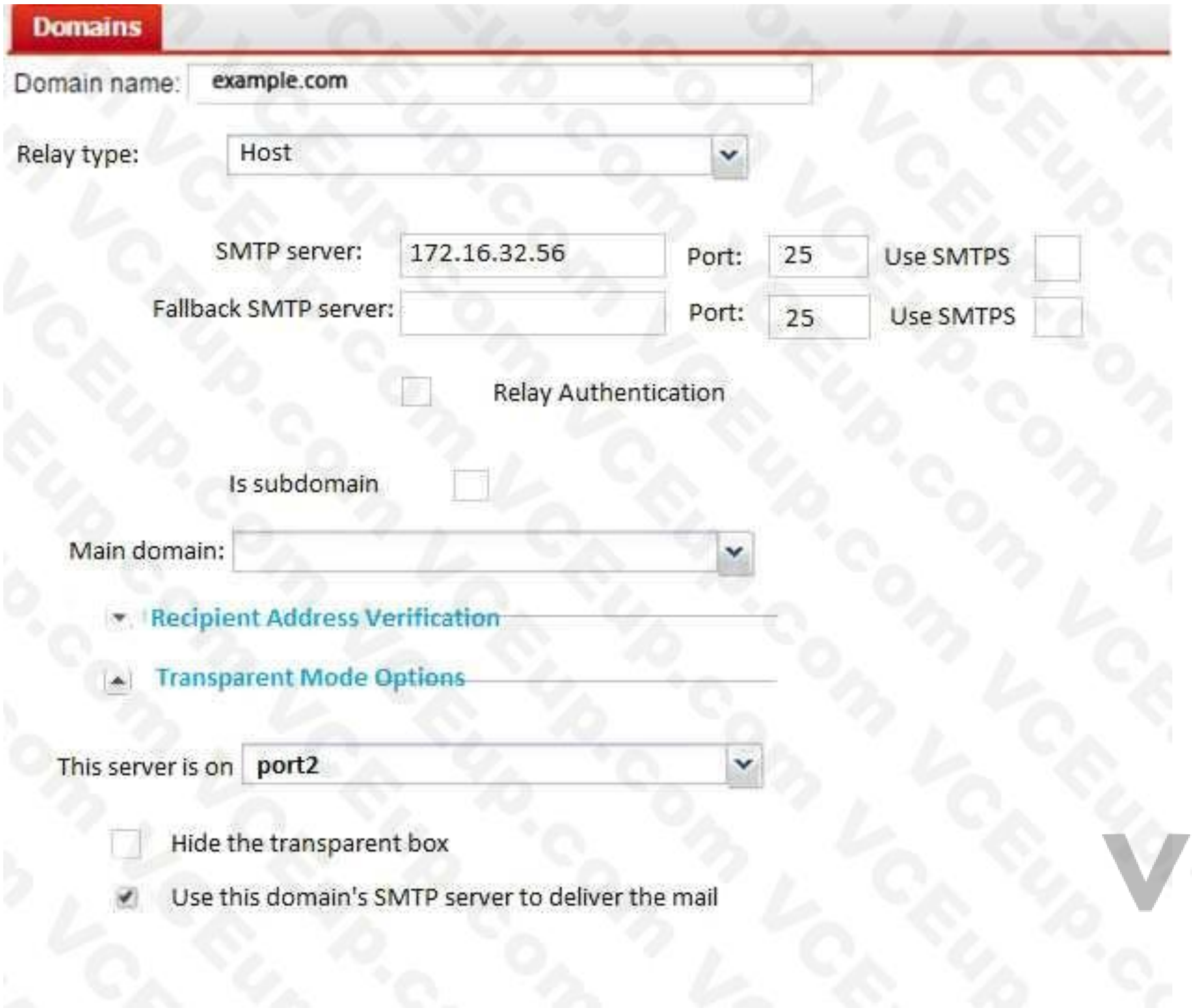


FML-1 configuration



For outgoing SMTP connections

☑ Use client-specified SMTP server to send email



Domains

Domain name: example.com

Relay type: Host

SMTP server: 172.16.32.56 Port: 25 Use SMTPS □

Fallback SMTP server: Port: 25 Use SMTPS □

□ Relay Authentication

Is subdomain □

Main domain:

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 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

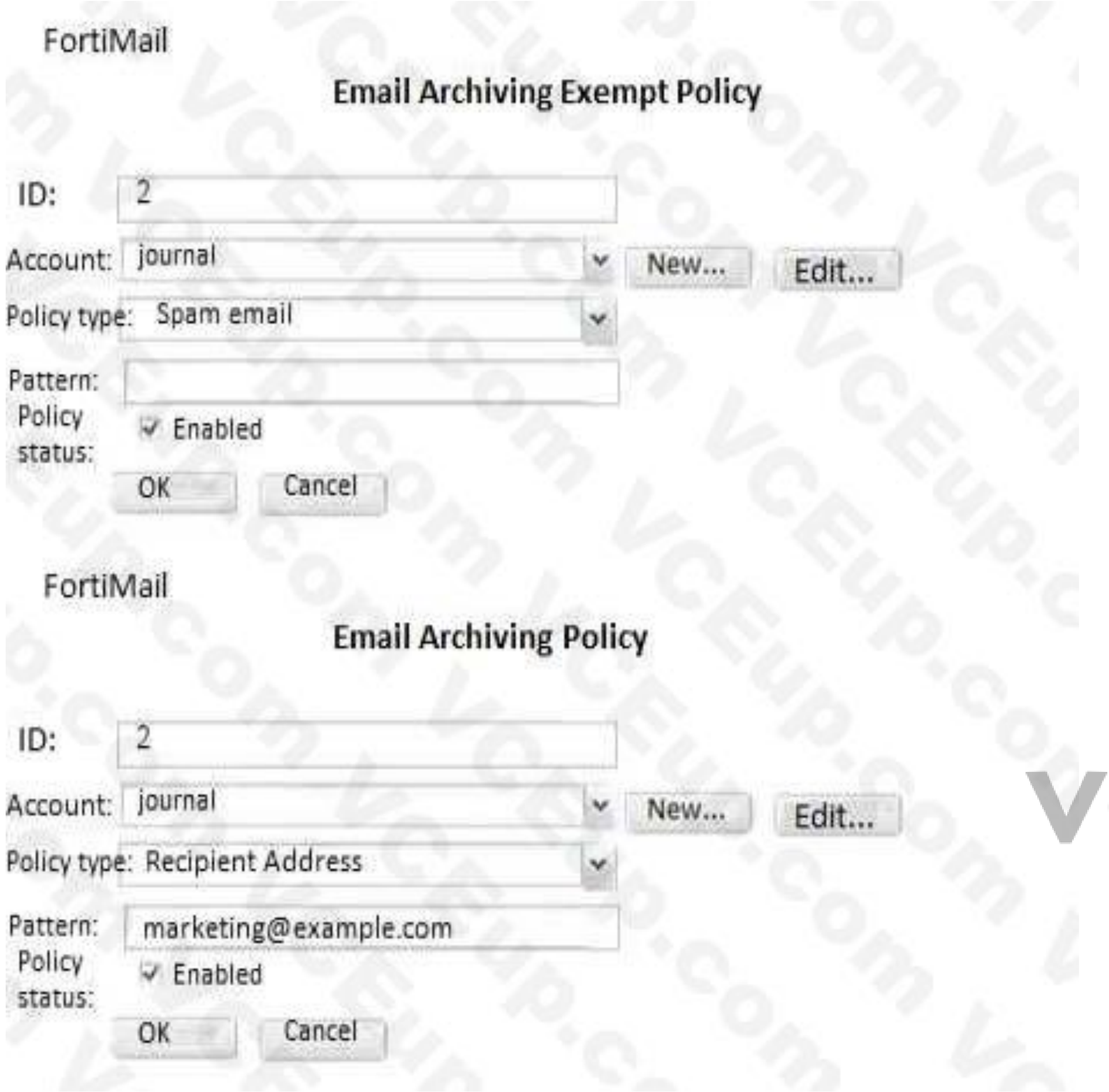
D. If outgoing email messages are undeliverable, FML-1 can queue them to retry later

Answer: B,C

Explanation:

Question 54

Examine the FortiMail archiving policies shown in the exhibit; then answer the question below.



FortiMail

Email Archiving Exempt Policy

ID: 2

Account: journal

Policy type: Spam email

Pattern:

Policy status: ☑ Enabled

FortiMail

Email Archiving Policy

ID: 2

Account: journal

Policy type: Recipient Address

Pattern: marketing@example.com

Policy status: ☑ Enabled

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

A. Spam email will be exempt from archiving

B. Email sent from marketing@example.com will be archived

C. Archived email will be saved in the journal account

D. Only the marketing@example.com account will be able to access the archived email

Answer: A, C

Explanation:

Question 55

Which of the following antispam techniques queries FortiGuard for rating information? (Choose two.)

A. URI filter

B. IP reputation

C. SURBL

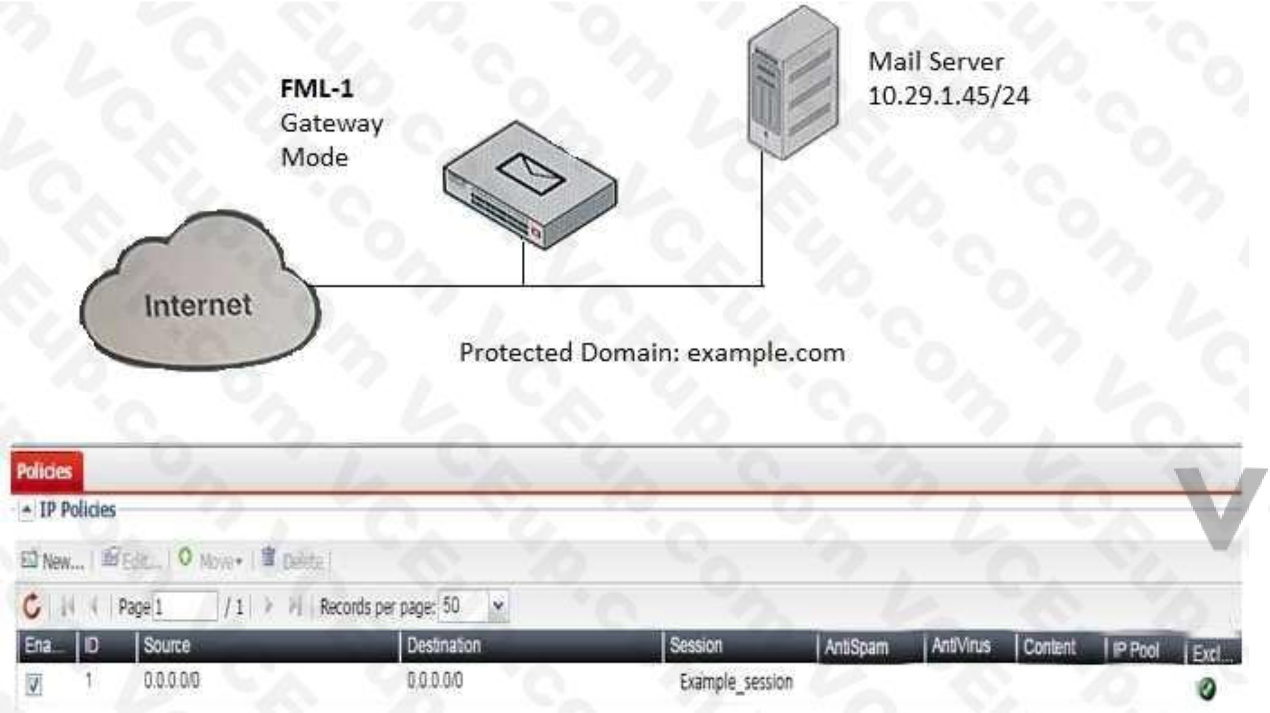
D. DNSBL

Answer: AB

Explanation:

Question 56

Examine the FortiMail topology and IP-based policy shown in the exhibit; then answer the question below.



Ena...	ID	Source	Destination	Session	AntiSpam	AntiVirus	Content	IP Pool	Excl...
☑	1	0.0.0.0/0	0.0.0.0/0	Example_session					✓

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 started filing up with undeliverable email. What changes should the administrator make to fix this issue? (Choose two.)

A. Clear the sender reputation database using the CLI

B. Create an outbound recipient policy to bypass outbound email from session profile inspections

C. Disable the exclusive flag in IP policy ID 1

D. Apply a session profile with sender reputation disabled on a separate IP policy for outbound sessions

Answer: B,C

Explanation: