DUMPSQUEEN

Fortinet NSE 6 - FortiMail 6.4

Fortinet NSE6_FML-6.4

Version Demo

Total Demo Questions: 10

Total Premium Questions: 56

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

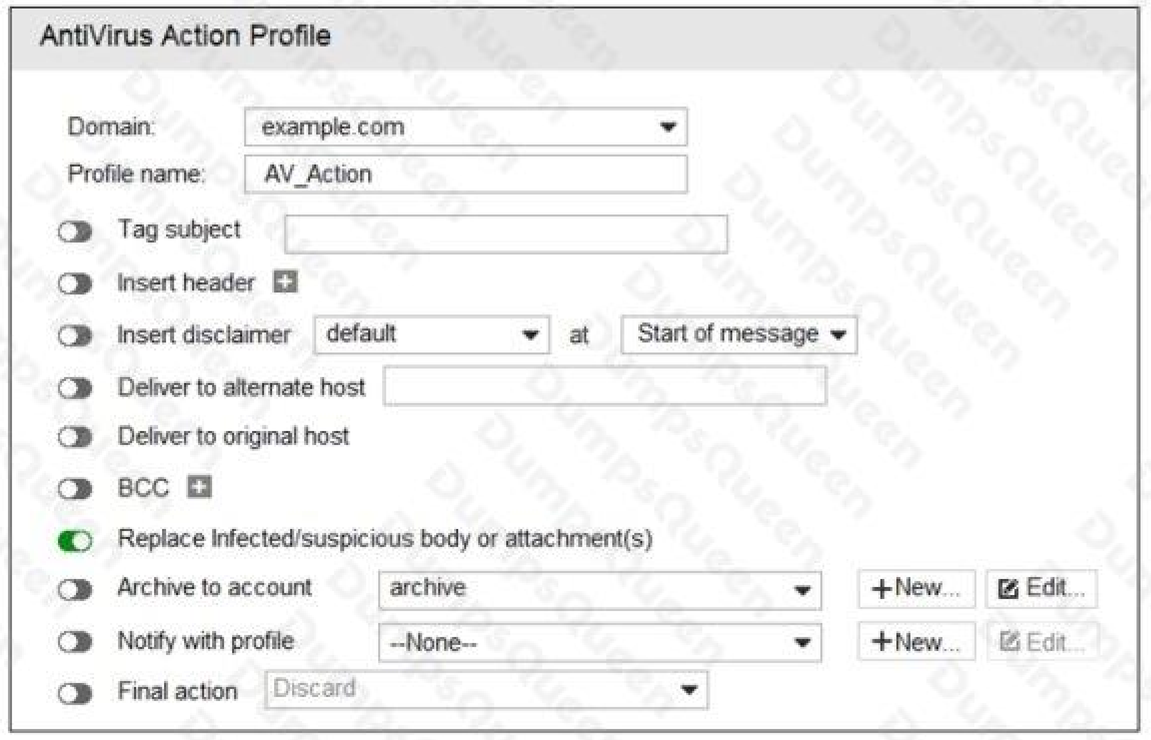
dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Main Questions Pool	34
Topic 2, Extra Main Questions	22
Total	56

QUESTION NO: 1

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

○ Notify with profile --None--

○ 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: B C

QUESTION NO: 2

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

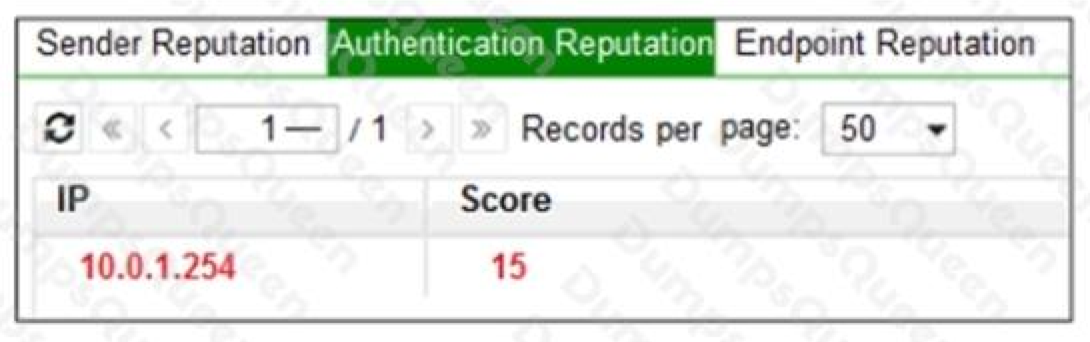
ANSWER: C

Explanation:

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/8c063dd3-bafe-11e9- a989-00505692583a/fortimail-admin-620.pdf (435)

QUESTION NO: 3

Refer to the exhibit.



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

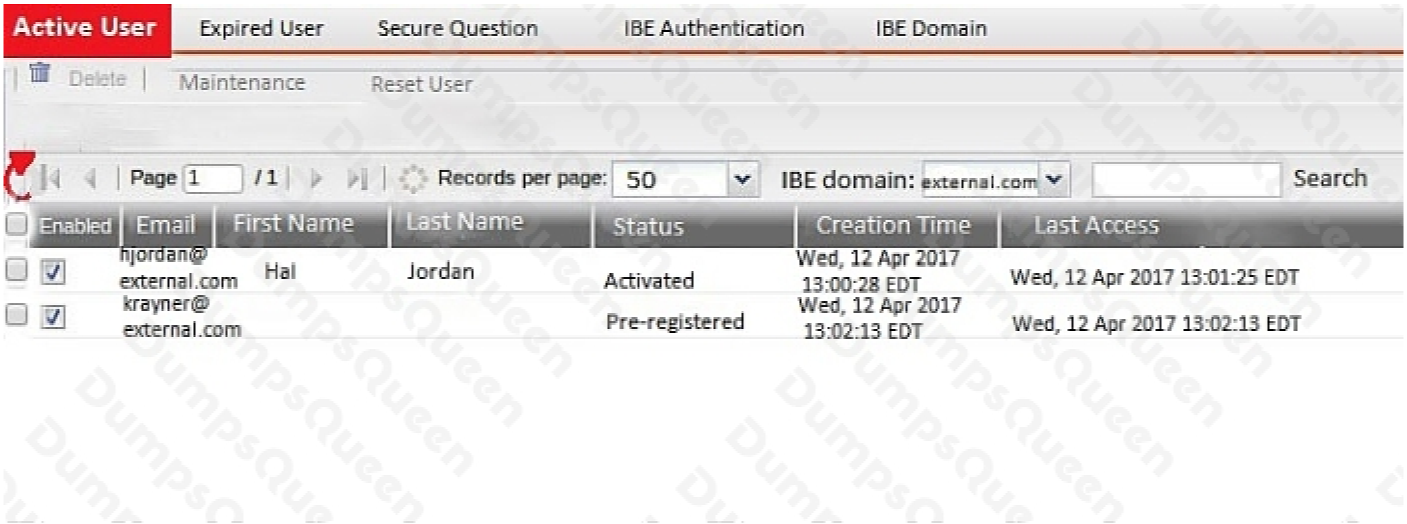
ANSWER: D

Explanation:

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

QUESTION NO: 4

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

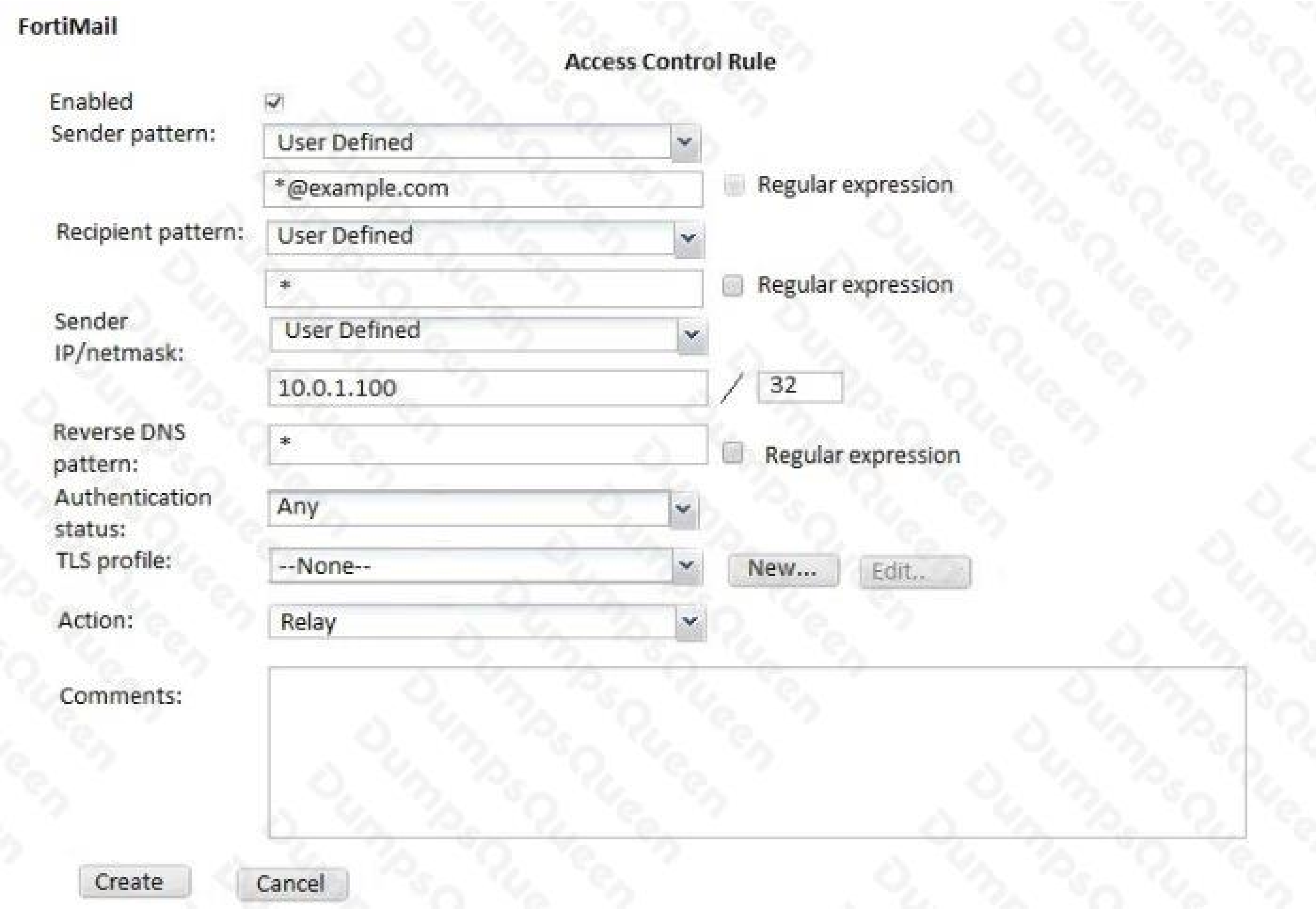
C. The user has received an IBE notification email, but has not accessed the HTTPS URL or attachment yet

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

ANSWER: C

QUESTION NO: 5

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--

Action: Relay

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

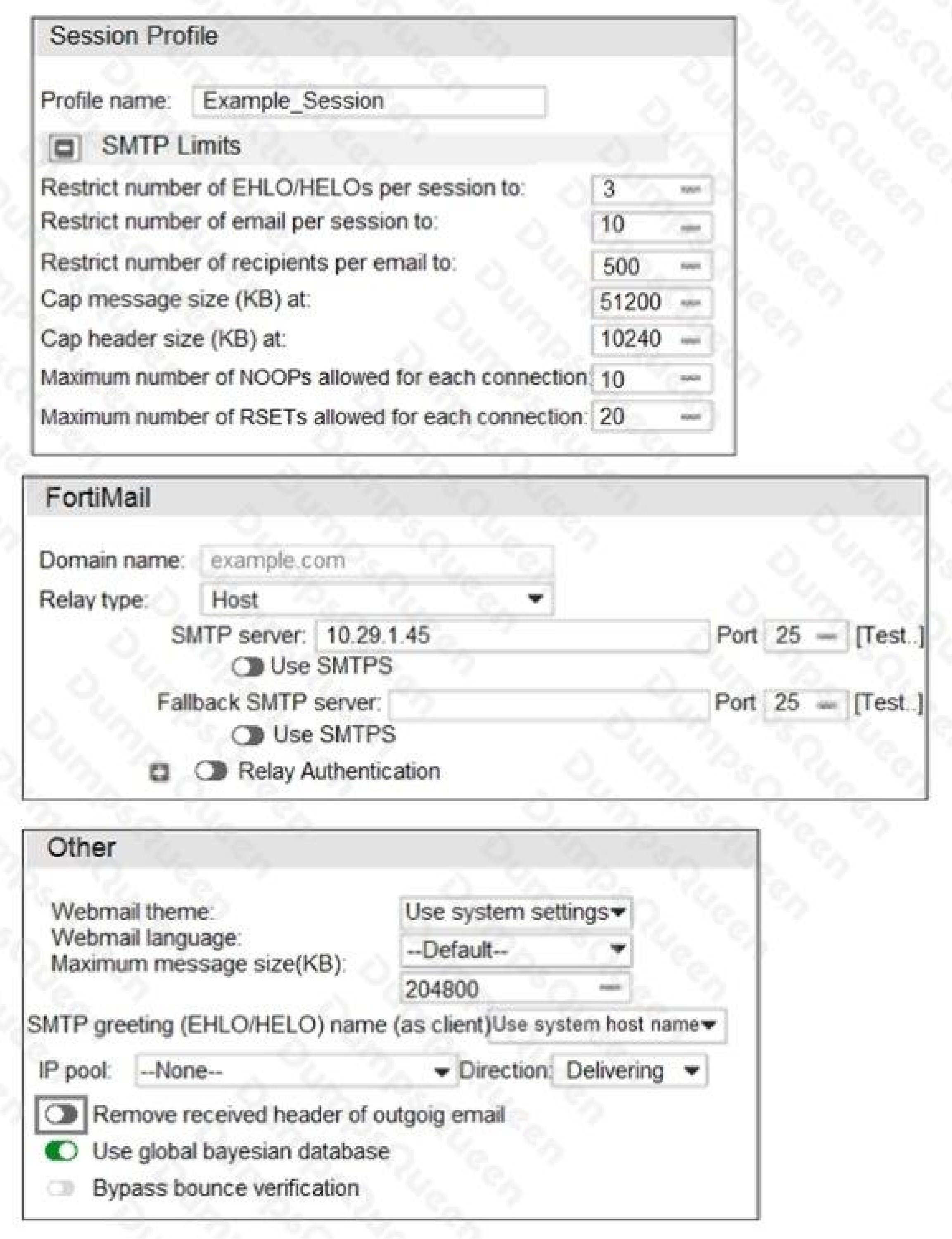
C. Email matching this rule will be relayed

D. Email must originate from an example.com email address to match this rule

ANSWER: C D

QUESTION NO: 6

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

QUESTION NO: 7

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.

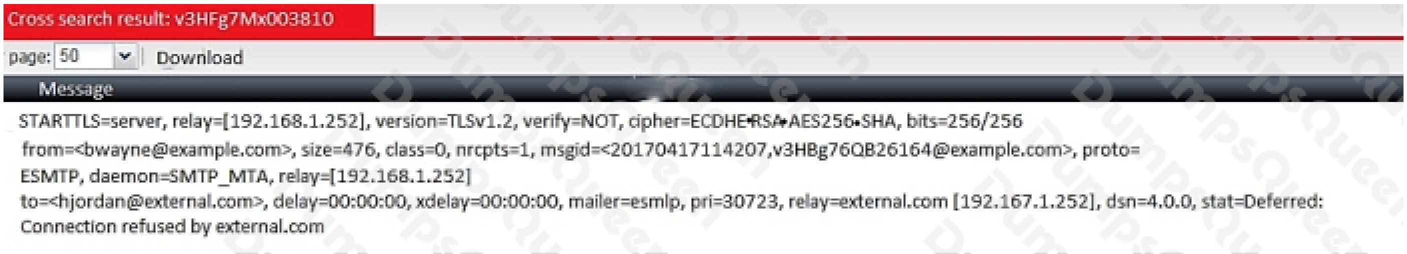
C. It uses DMARC validation to detect spoofed addresses.

D. It uses SPF validation to detect spoofed addresses.

ANSWER: A

QUESTION NO: 8

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

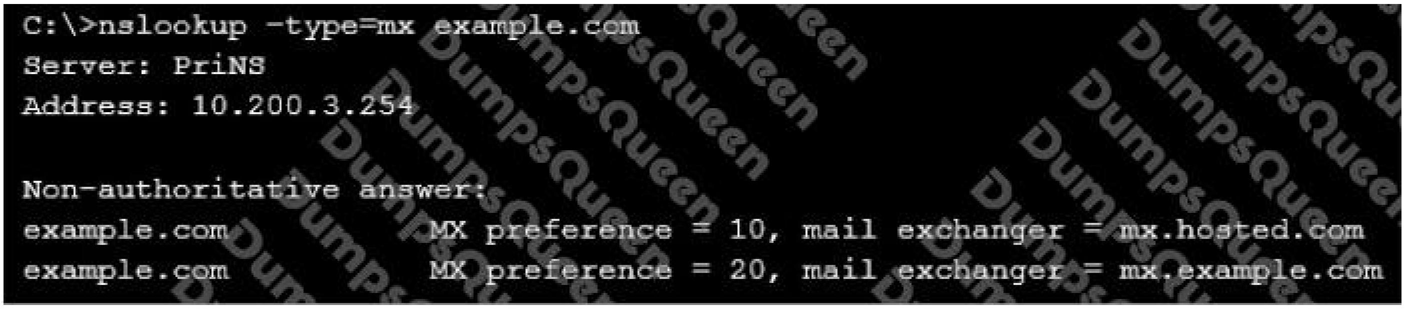
C. The logs were generated by a gateway or transparent mode FortiMail

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

ANSWER: A C

QUESTION NO: 9

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: A B

QUESTION NO: 10

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: C D

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)