DUMPSARENA

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://dumpsarena.co

sales@dumpsarena.co

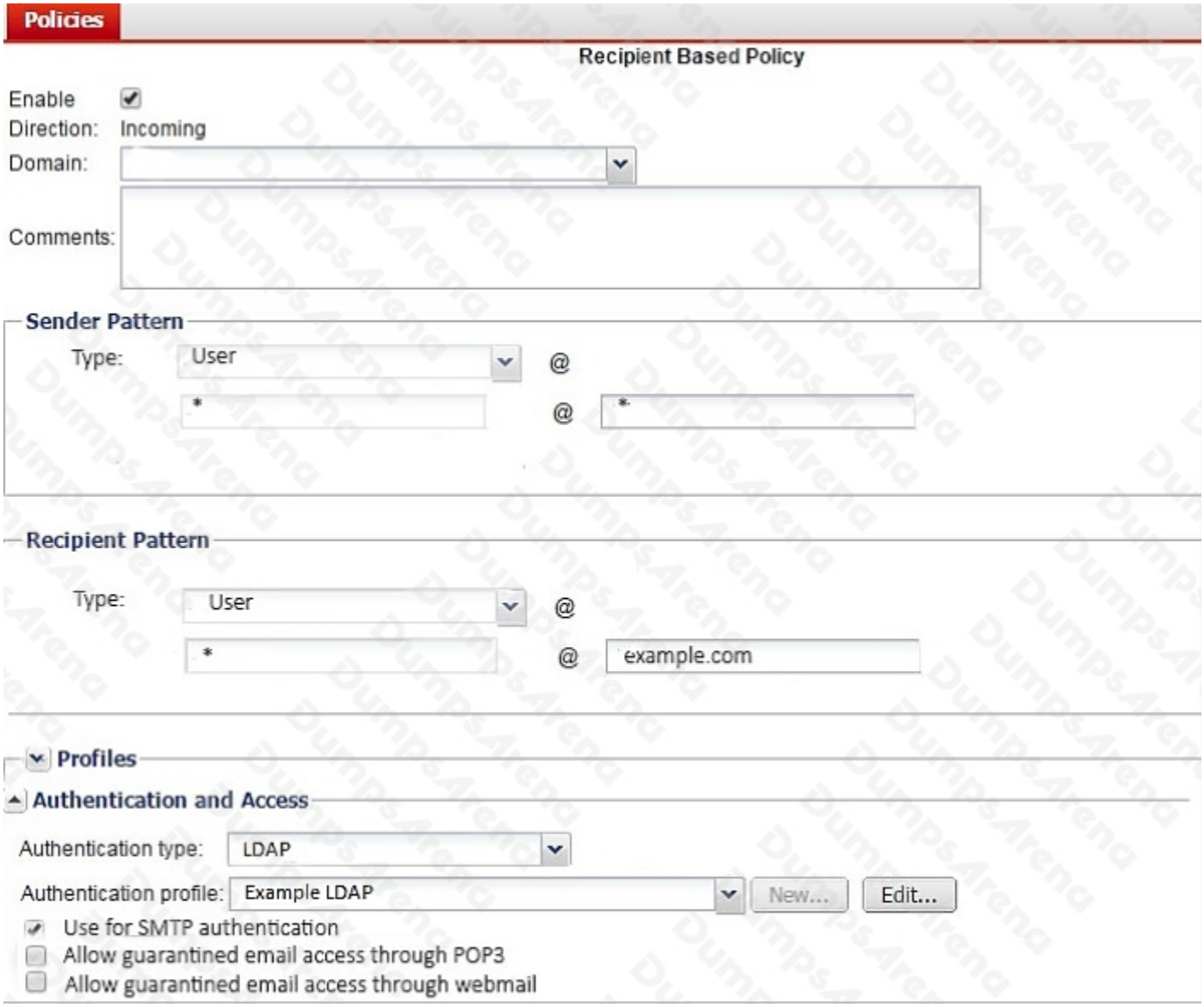
sales@dumpsarena.co
dumpsarena.co

Topic Break Down

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

QUESTION NO: 1

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



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

QUESTION NO: 2

Refer to the exhibit.

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

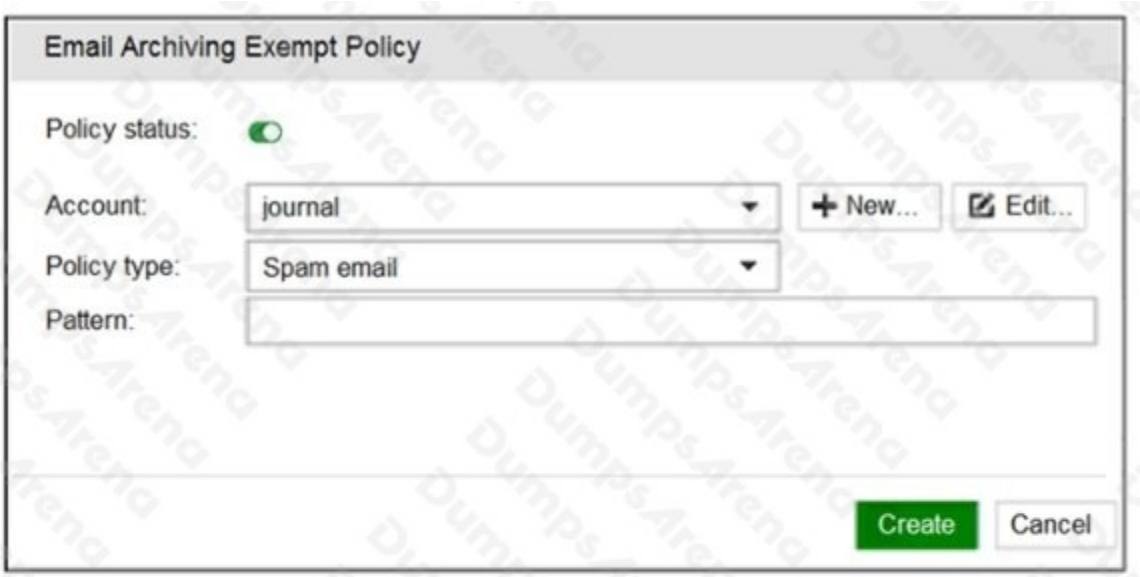
ANSWER: D

Explanation:

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

QUESTION NO: 3

Refer to the exhibit.



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: A B

QUESTION NO: 4

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

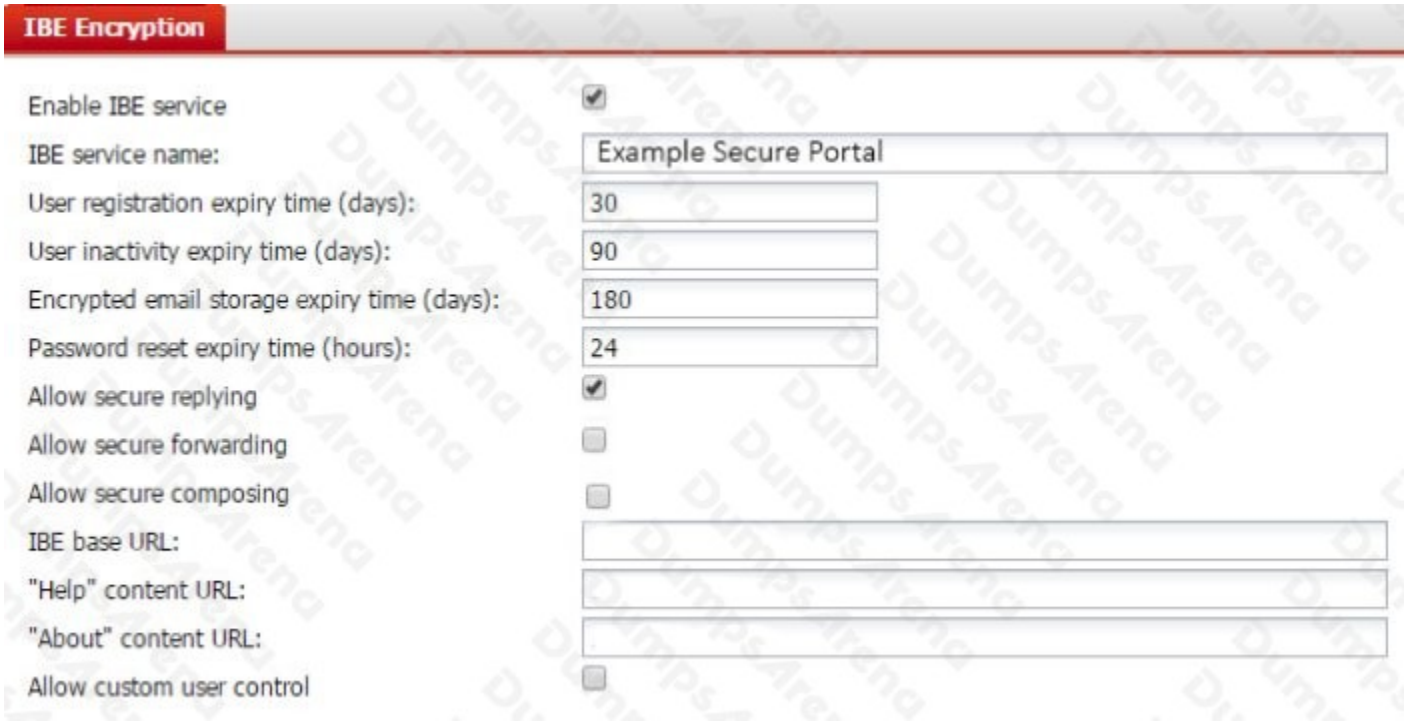
C. The PriNS server should receive all email for the example.com domain

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

ANSWER: A B

QUESTION NO: 5

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



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

QUESTION NO: 6

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 NO: 7

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

A. URI filter

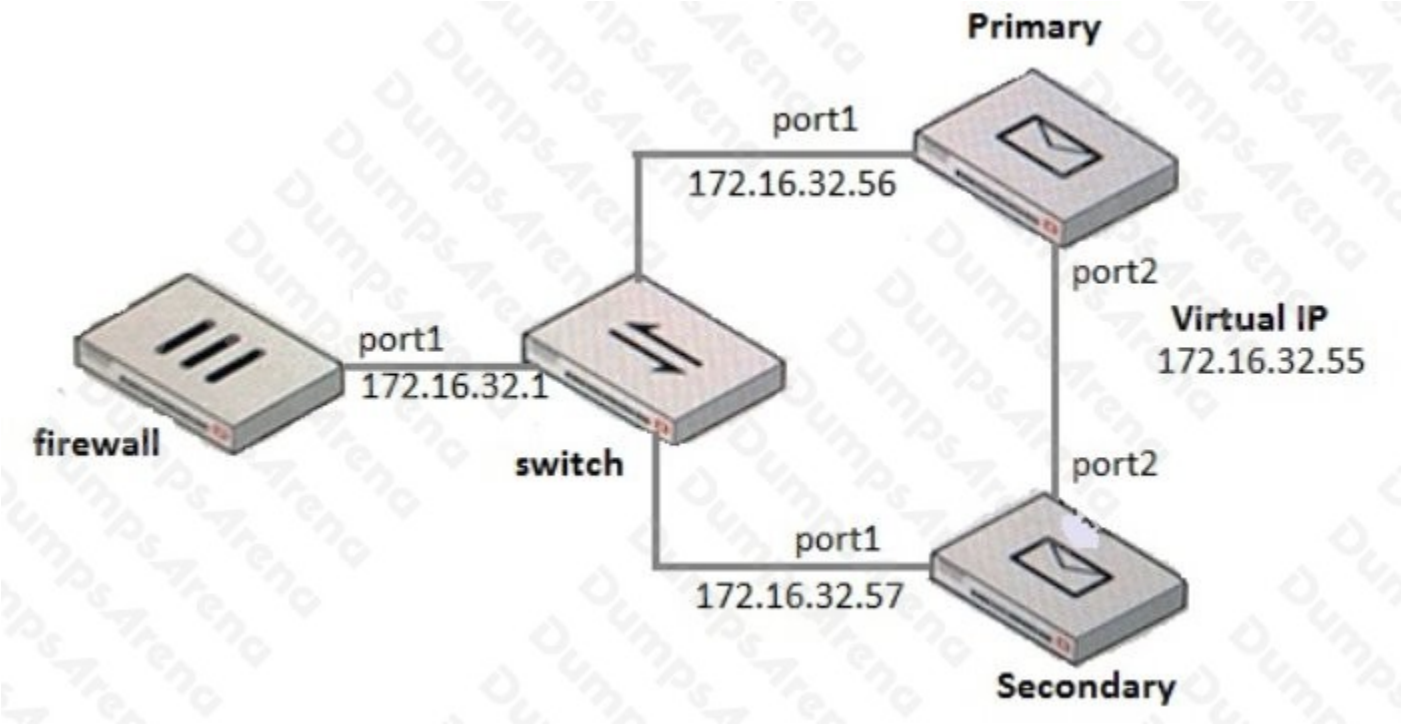
B. IP reputation

C. SURBL

D. DNSBL

ANSWER: A B

QUESTION NO: 8



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

A. 172.16.32.1

B. 172.16.32.57

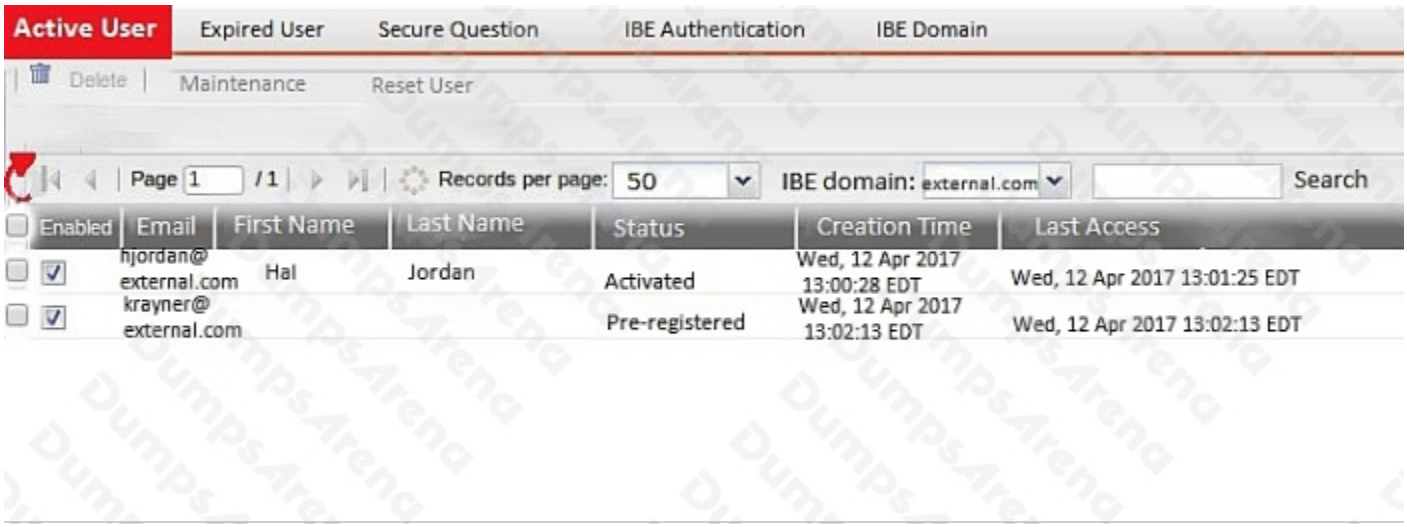
C. 172.16.32.55

D. 172.16.32.56

ANSWER: C

QUESTION NO: 9

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



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: 10

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: B D