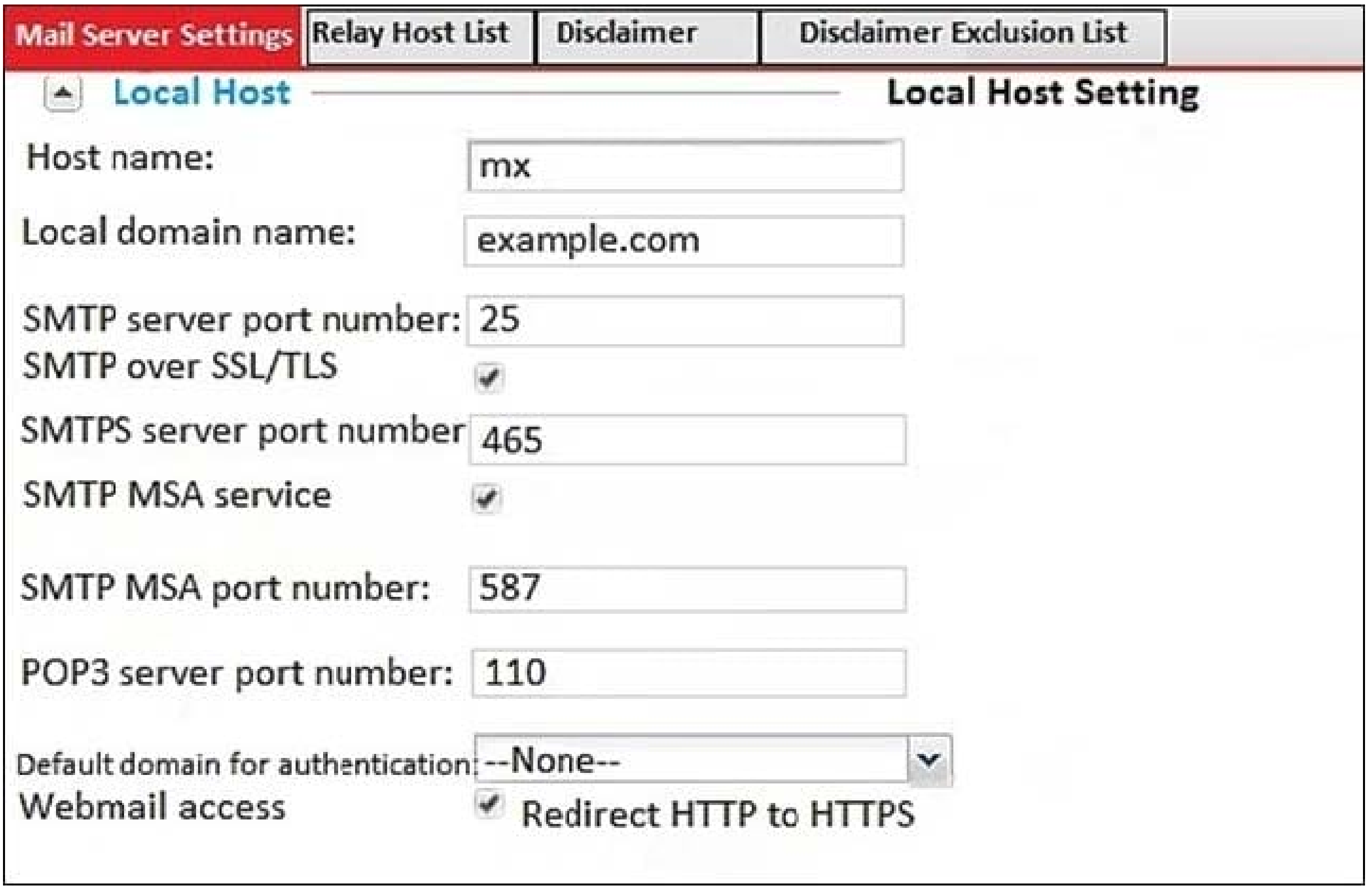
NSE6_FML-6.0$^{Q\&As}$

Fortinet NSE 6 - FortiMail 6.0

QUESTION 1

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



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

Correct Answer: AC

QUESTION 2

FortiMail is configured with the protected domain "example.com". Identify which of the following envelope addresses will require an access receive rule to relay for unauthenticated senders? (Choose two.)

A. MAIL FROM: mis@hosted.net RCPT TO: noc@example.com

B. MAIL FROM: training@external.org RCPT TO: students@external.org

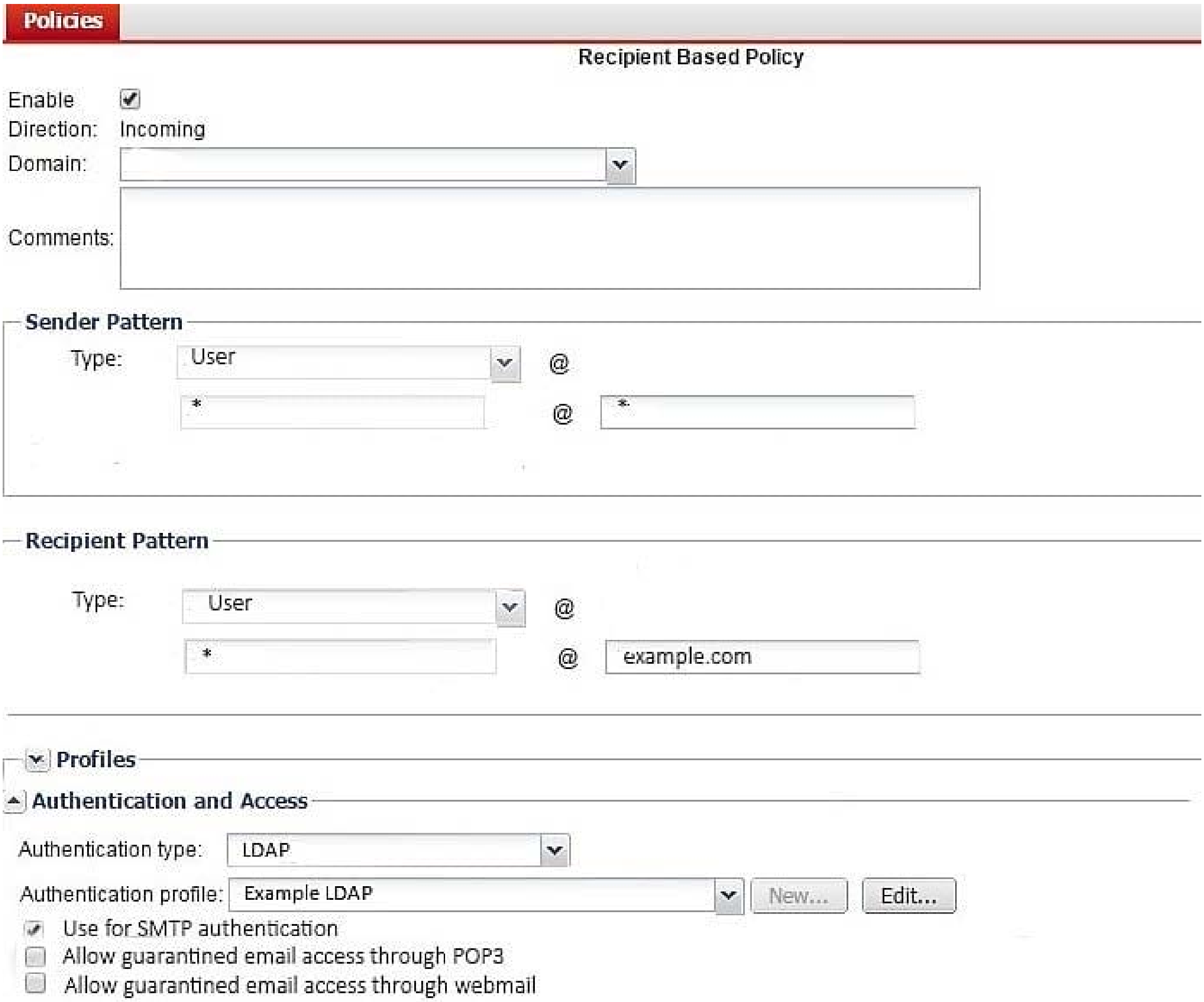
C. MAIL FROM: accounts@example.com RCPT TO: sales@exernal.org

D. MAIL FROM: support@example.com RCPT TO: marketing@example.com

Correct Answer: CD

QUESTION 3

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



Policies

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 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

QUESTION 5

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? (Choose one.)

A. Bounce address tag validation

B. Spam outbreak protection

C. Spoofed header detection

D. FortiGuard IP Reputation

Correct Answer: B