NSE6_FML-6.0 Q&As

Fortinet NSE 6 - FortiMail 6.0

Pass Fortinet NSE6_FML-6.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/nse6_fml-6-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

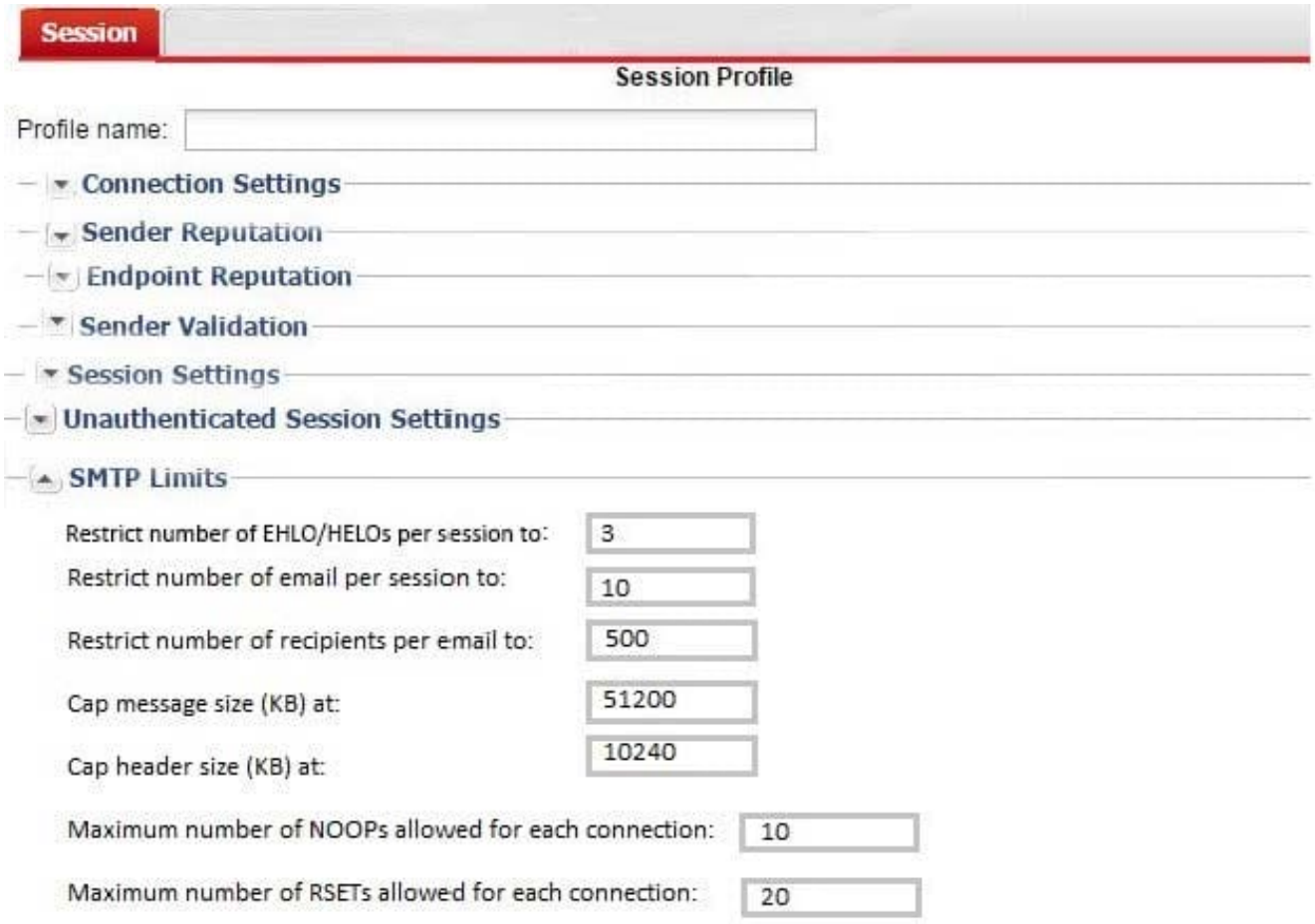
D. The STARTTLS command is used to initiate SMTP over TLS

E. SMTPS encrypts the body of the email message, where the most sensitive content exists

Correct Answer: ABD

QUESTION 2

Examine the FortiMail session profile and protected domain configuration shown in the exhibit; then answer the question below.



Which size limit will FortiMail apply to outbound email?

A. 204800

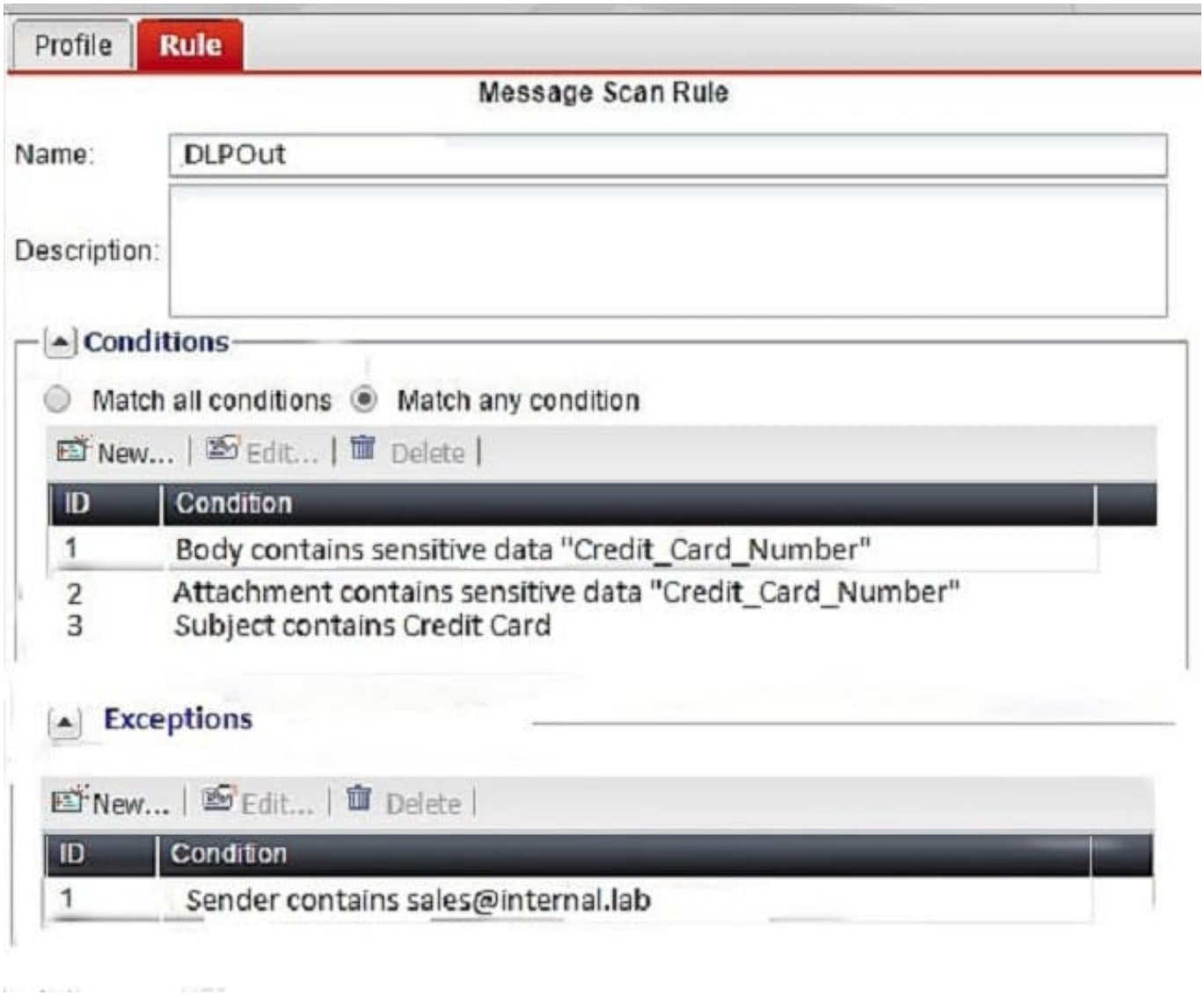
B. 51200 C. 1024

D. 10240

Correct Answer: A

QUESTION 3

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



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

Correct Answer: AC

QUESTION 4

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

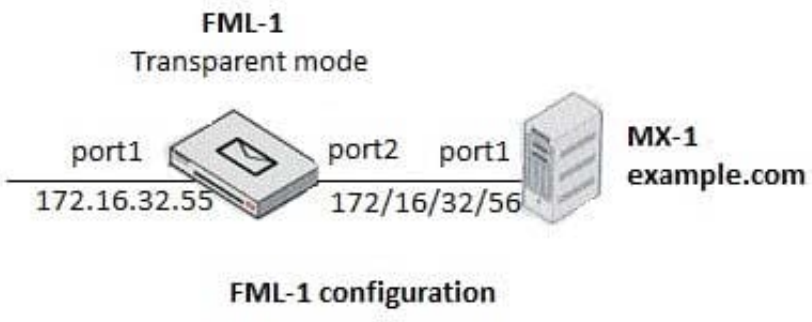
B. Spam outbreak protection

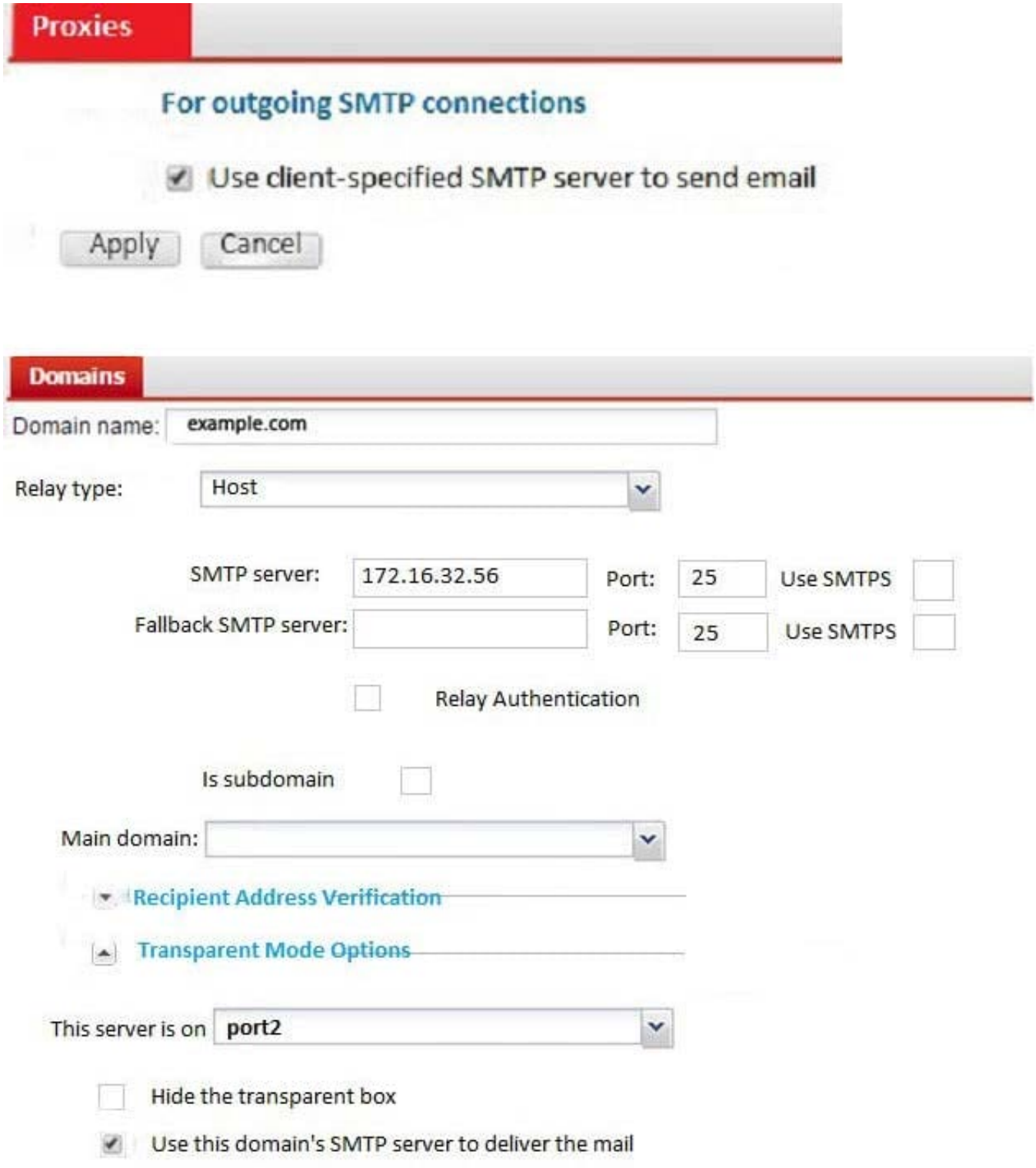
C. Spoofed header detection

D. FortiGuard IP Reputation

Correct Answer: B

QUESTION 5





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

Correct Answer: BC

Latest NSE6_FML-6.0 Dumps NSE6_FML-6.0 VCE Dumps NSE6_FML-6.0 Study Guide