Fortinet.NSE6_FML-7.2.by.Mirin.17q

Number: NSE6_FML-7.2
Passing Score: 800
Time Limit: 120 min
File Version: 3.0

Exam Code: NSE6_FML-7.2

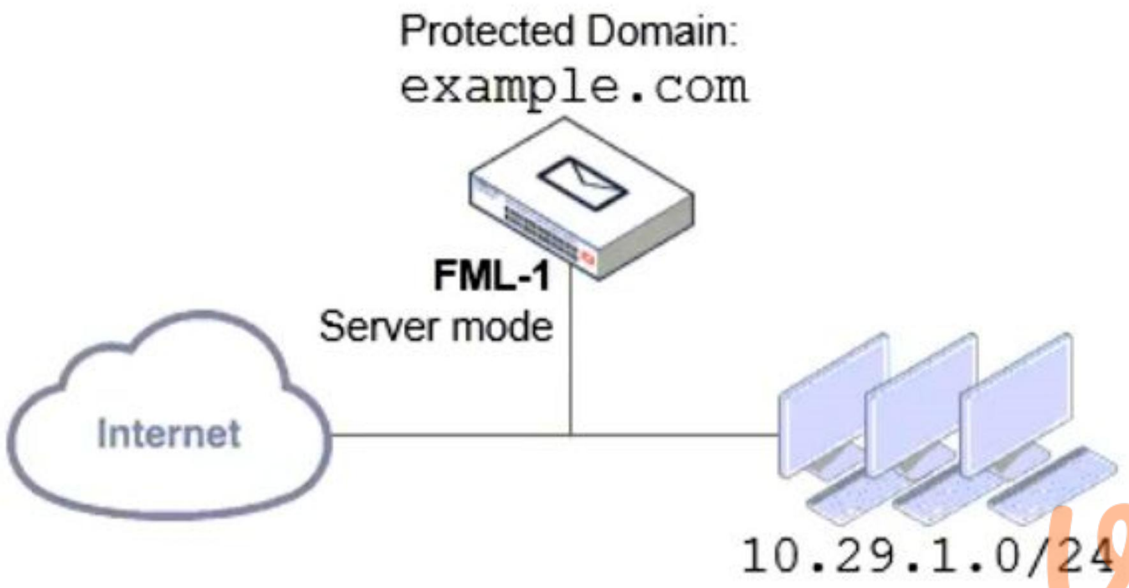
Exam Name: Fortinet NSE 6 - FortiMail 7.2

Exam A

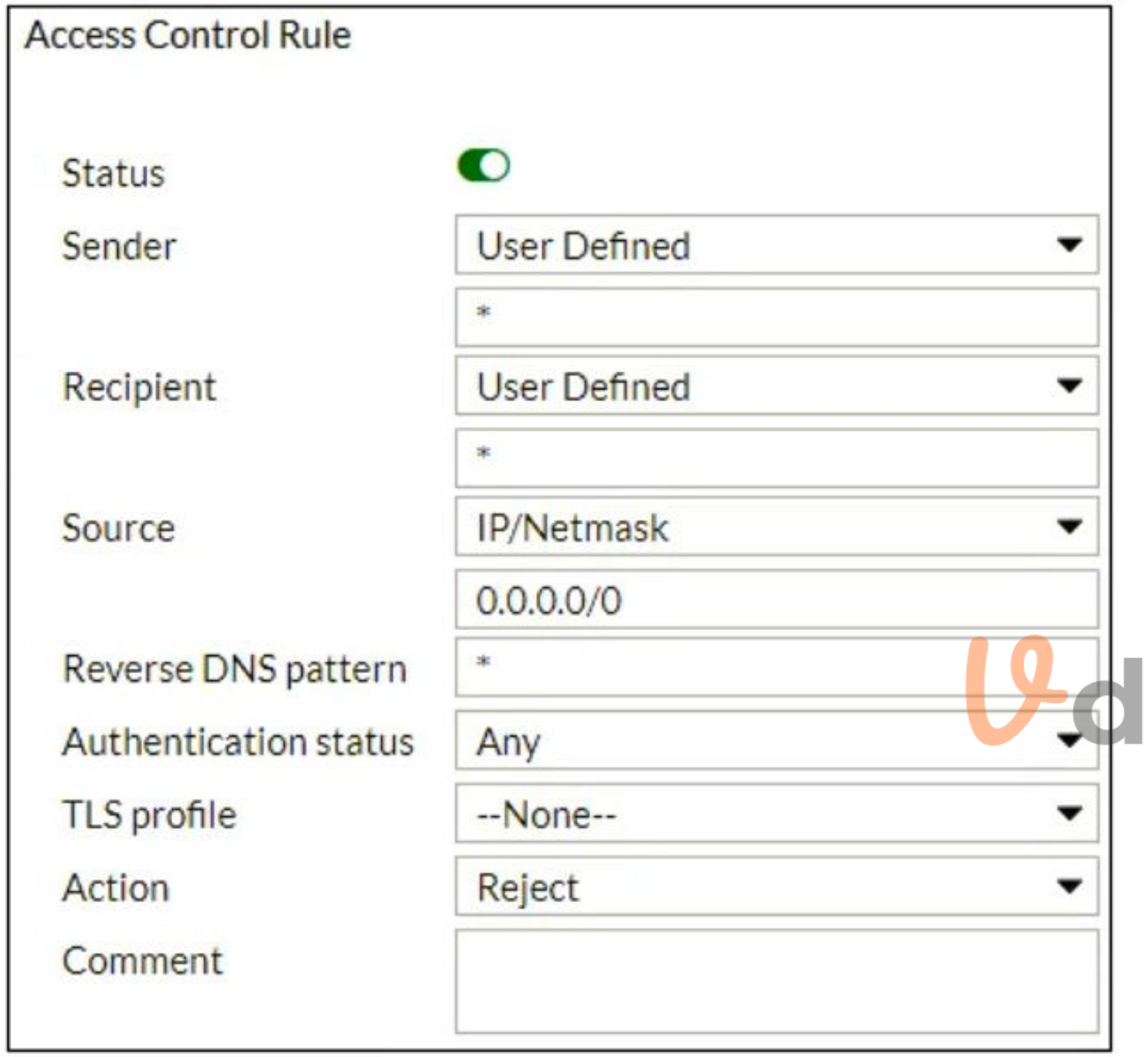
QUESTION 1

Refer to the exhibits which show a topology diagram (Topology), and a configuration element (Access Control Rule).

Topology



Access Control Rule



Access Control Rule

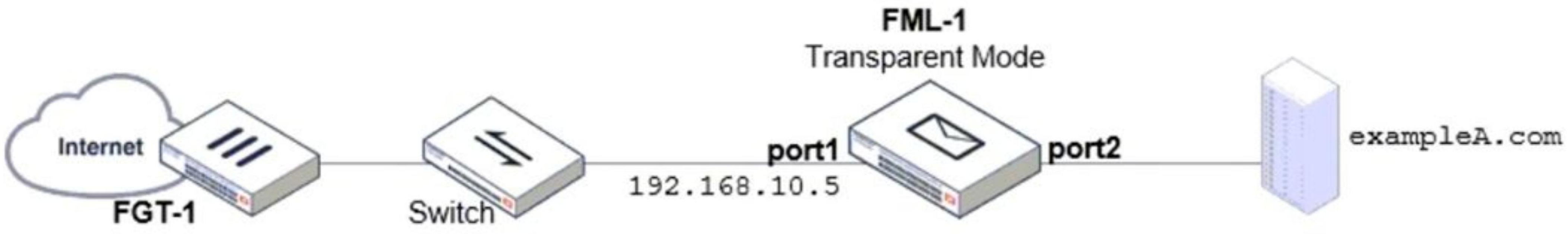
Status	●
Sender	User Defined
	*
Recipient	User Defined
	*
Source	IP/Netmask
	0.0.0.0/0
Reverse DNS pattern	*
Authentication status	Any
TLS profile	--None--
Action	Reject
Comment	

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 Sender IP/netmask should be set to 10.29.1.0/24.
B. The Action should be set to Reject
C. The Recipient pattern should be set to * @example. com.
D. The Authentication status should be set to Authenticated

Correct Answer: A, D
Section:
Explanation:

QUESTION 2
Refer to the exhibit which displays a topology diagram.



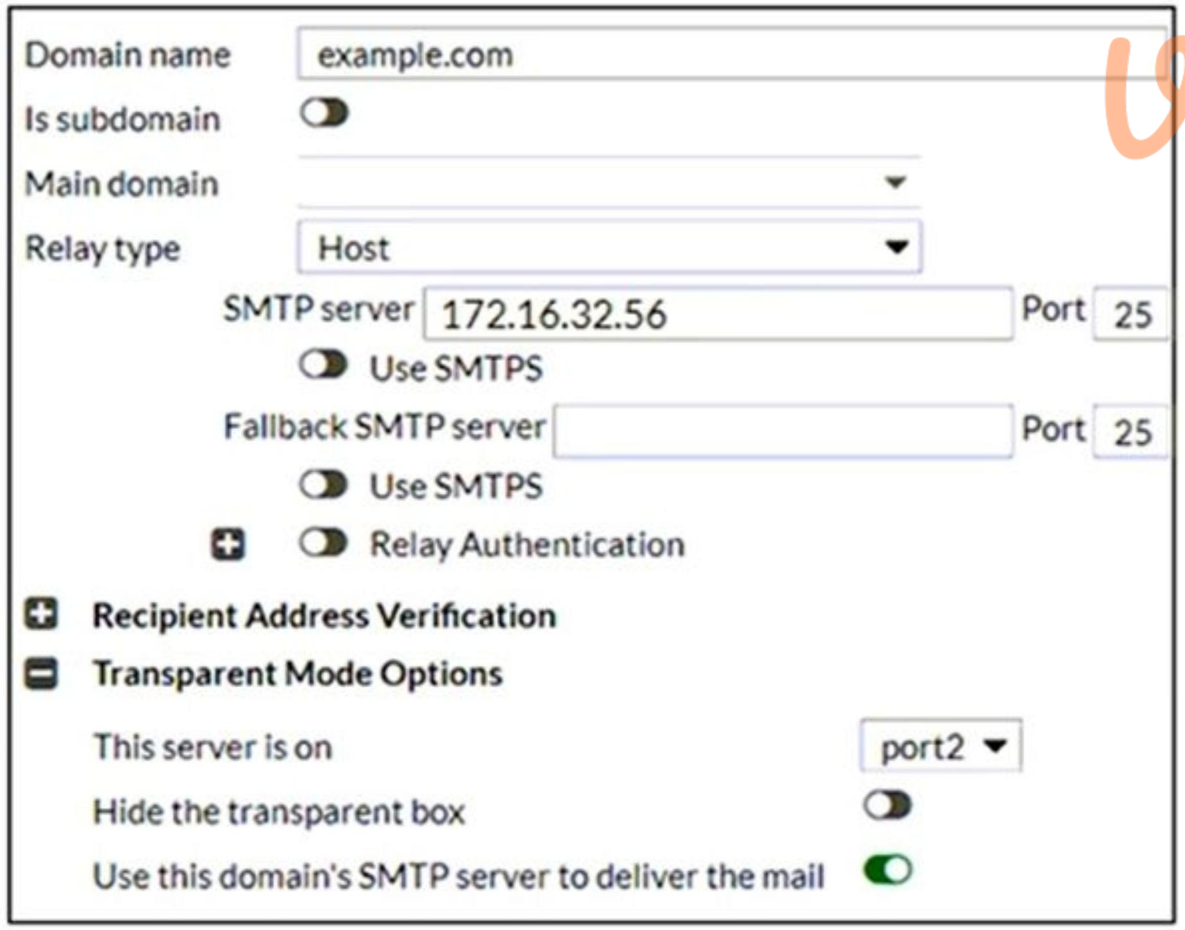
Which two statements describe the built-in bridge functionality on a transparent mode FortiMail? (Choose two.)

A. If port1. is required to process SMTP traffic, it must be configured as a routed interface.
B. All bridge member interfaces belong to the same subnet as the management IP.
C. The management IP is permanently tied to port1, and port1 cannot be removed from the bridge.
D. Any bridge member interface can be removed from the bridge and configured as a routed interface.

Correct Answer: B, C
Section:
Explanation:

QUESTION 3

Refer to the exhibit which displays the domain configuration of a transparent mode FortiMail device.



Domain name	example.com
Is subdomain	○
Main domain	▾
Relay type	Host ▾

SMTP server 172.16.32.56 Port 25

○ Use SMTPS

Fallback SMTP server Port 25

○ 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	●

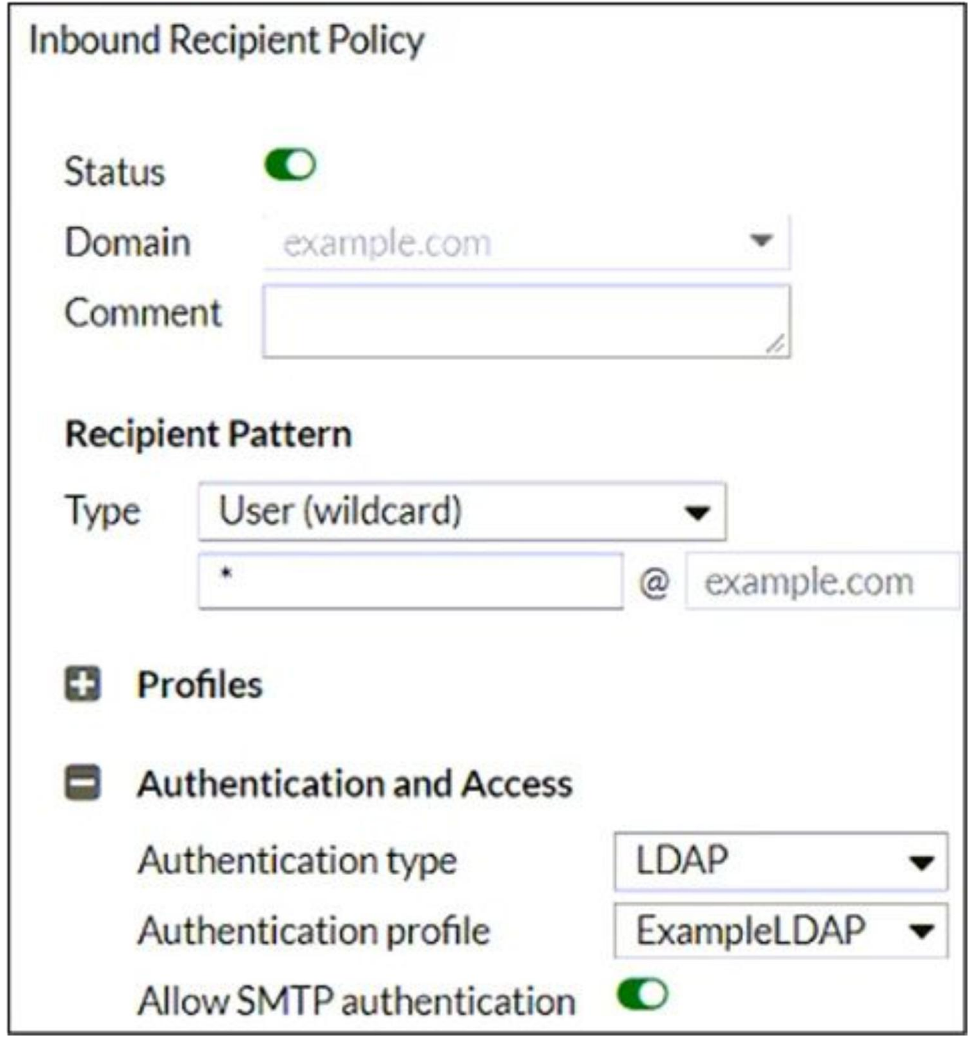
Based on the exhibit, which two sessions are considered incoming sessions? (Choose two.)

A. DESTINATION IP: 172.16.32.56 MAIL FROM: mis@hosted.net RCPT TO: noc@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: support@example.com RCPT TO: marketing@example.com

Correct Answer: A, D
Section:
Explanation:

QUESTION 4
Refer to the exhibit, which shows an inbound recipient policy.



Inbound Recipient Policy

Status ●
Domain example.com
Comment

Recipient Pattern

Type User (wildcard)
* @ example.com

Profiles

Authentication and Access

Authentication type LDAP
Authentication profile ExampleLDAP
Allow SMTP authentication ●

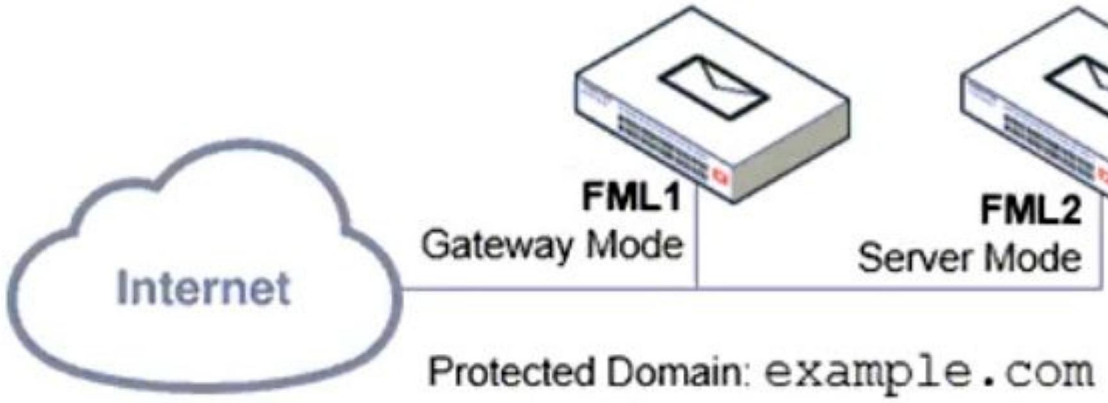
After creating the policy shown in the exhibit, an administrator discovers that clients can send unauthenticated emails using SMTP.
What must the administrator do to enforce authentication?

A. Move this incoming recipient policy to the top of the list.
B. Configure a matching IP policy with the exclusive flag enabled.
C. Configure an access delivery rule to enforce authentication.
D. Configure an access receive rule to verily authentication status.

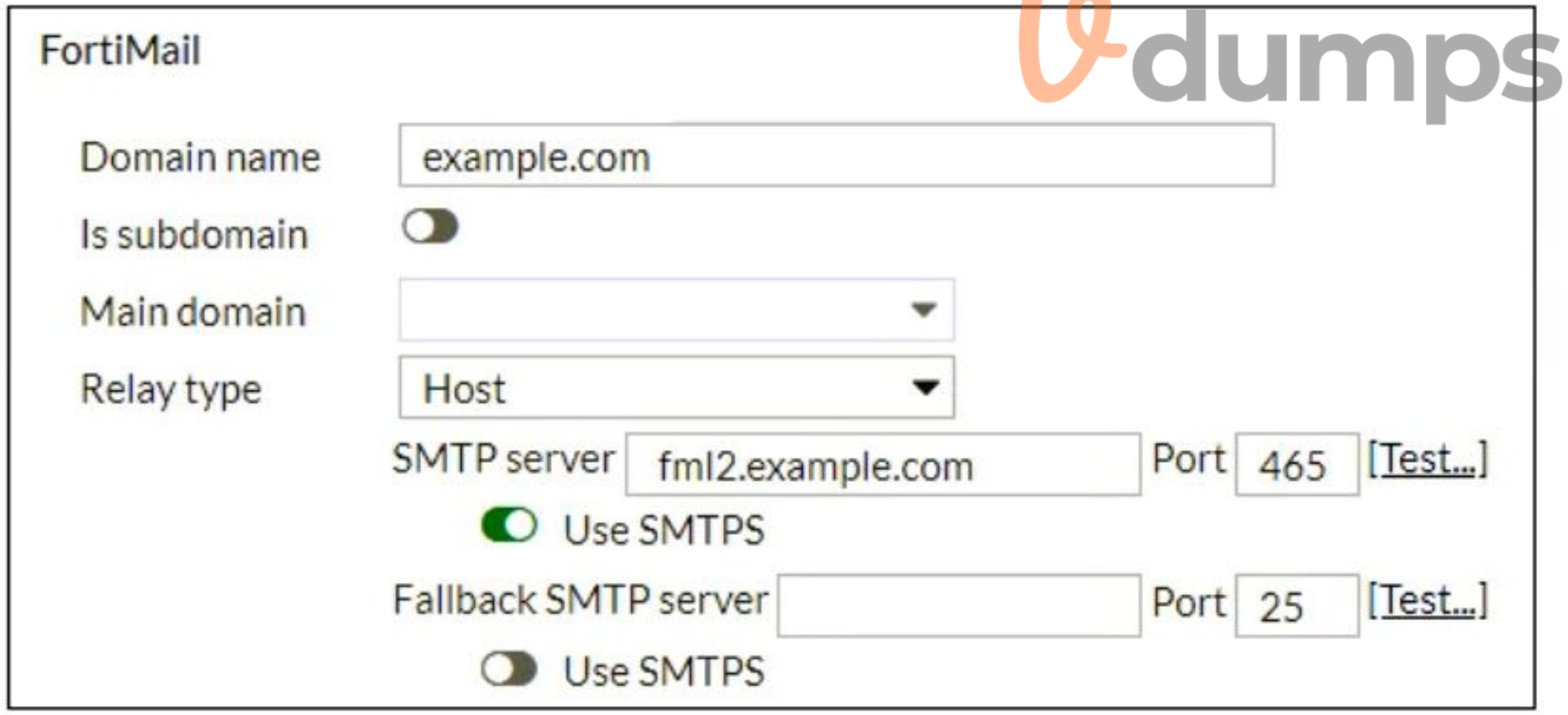
Correct Answer: D
Section:
Explanation:

QUESTION 5
Refer to the exhibits, which display a topology diagram (Topology) and two FortiMail device configurations (FML1 Configuration and FML2 Configuration).

Topology



FML1 Configuration


FortiMail

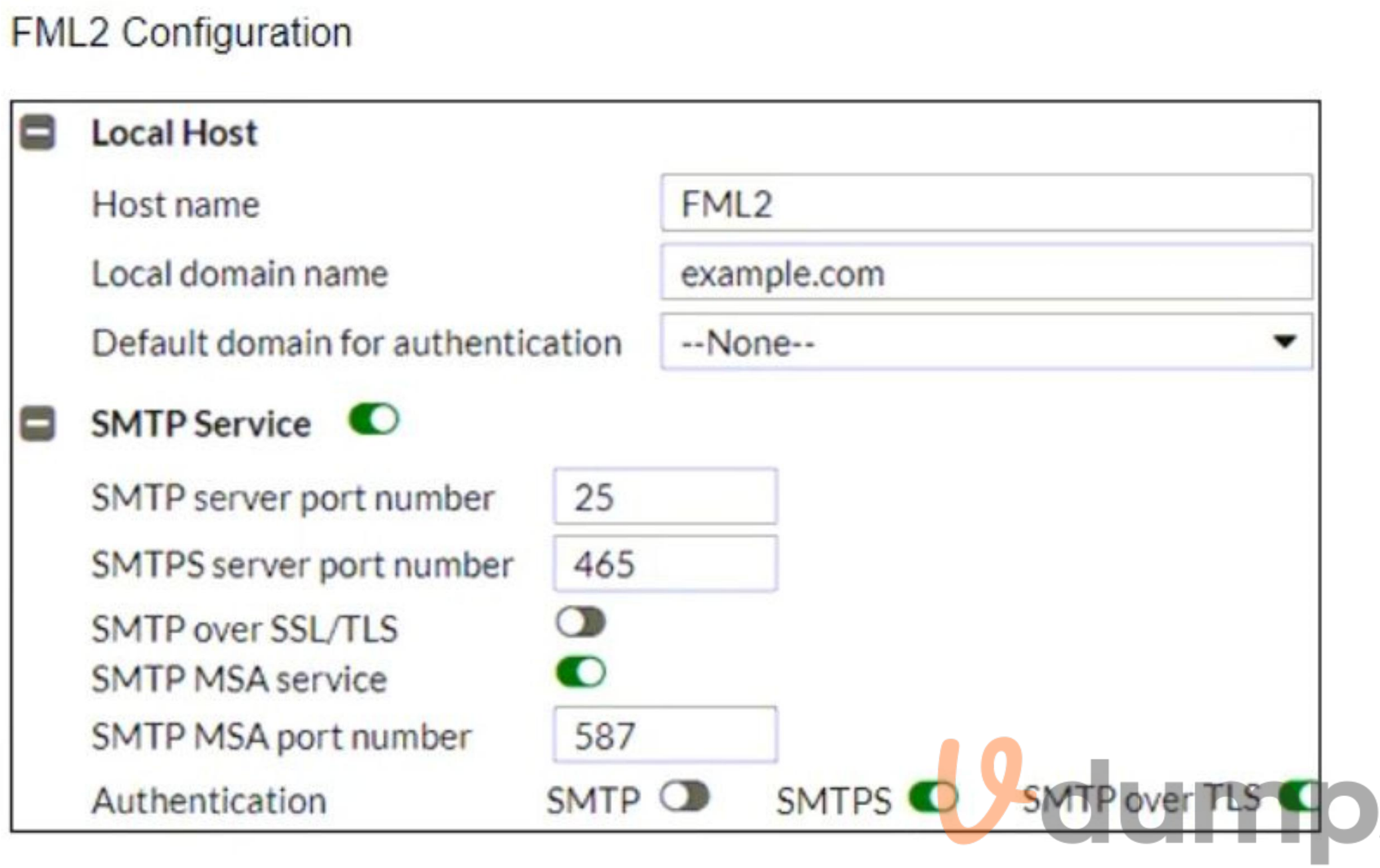
Domain name	example.com
Is subdomain	○
Main domain	▾
Relay type	Host ▾

SMTP server fml2.example.com Port 465 [Test...]

● Use SMTPS

Fallback SMTP server Port 25 [Test...]

○ Use SMTPS



FML2 Configuration

Local Host

Host name: FML2

Local domain name: example.com

Default domain for authentication: --None--

SMTP Service ●

SMTP server port number: 25

SMTPS server port number: 465

SMTP over SSL/TLS ○

SMTP MSA service ●

SMTP MSA port number: 587

Authentication: SMTP ○ SMTPS ● SMTP over TLS ●

What is the expected outcome of SMTP sessions sourced from FML1 and destined for FML2?

A. FML1 will fail to establish any connection with FML2.

B. FML1 will attempt to establish an SMTPS session with FML2. but fail and revert to standard SMTP.

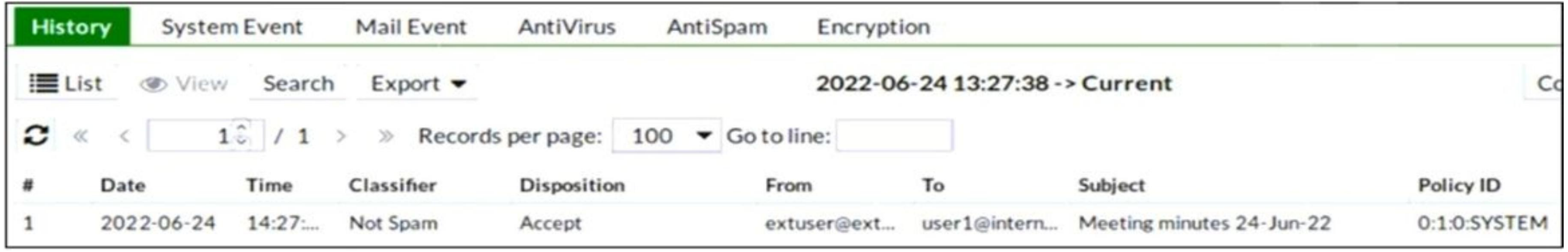
C. FML1 will send the STARTTLS command in the SMTP session, which will be rejected by FML2.

D. FML1 will successfully establish an SMTPS session with FML2.

Correct Answer: D
Section:
Explanation:

QUESTION 6

Refer to the exhibit which displays a history log entry.



2022-06-24 13:27:38 -> Current

#	Date	Time	Classifier	Disposition	From	To	Subject	Policy ID
1	2022-06-24	14:27:...	Not Spam	Accept	extuser@ext...	user1@intern...	Meeting minutes 24-Jun-22	0:1:0:SYSTEM

Why does the last field show SYSTEM in the Policy ID column?

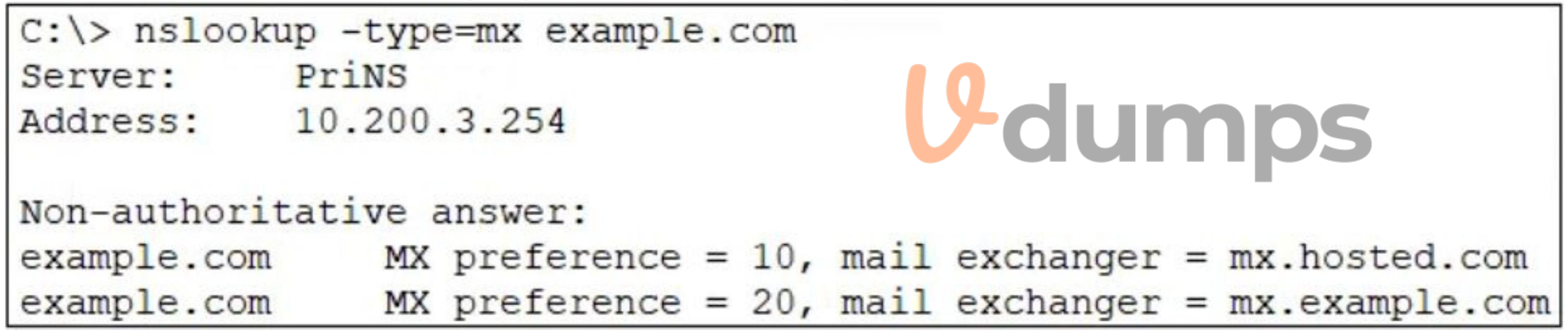
A. The email was dropped by a system blocklist.
B. It is an inbound email.
C. The email matched a system-level authentication policy.
D. The email did not match a recipient-based policy.

Correct Answer: D
Section:
Explanation:

QUESTION 7
Which two FortiMail antispam techniques can you use to combat zero-day spam? (Choose two.)
A. IP reputation
B. Spam outbreak protection
C. DNSBL
D. Behavior analysis

Correct Answer: A, B
Section:
Explanation:

QUESTION 8
Refer to the exhibit which shows an nslookup output of MX records of the example.com domain.



```
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
```

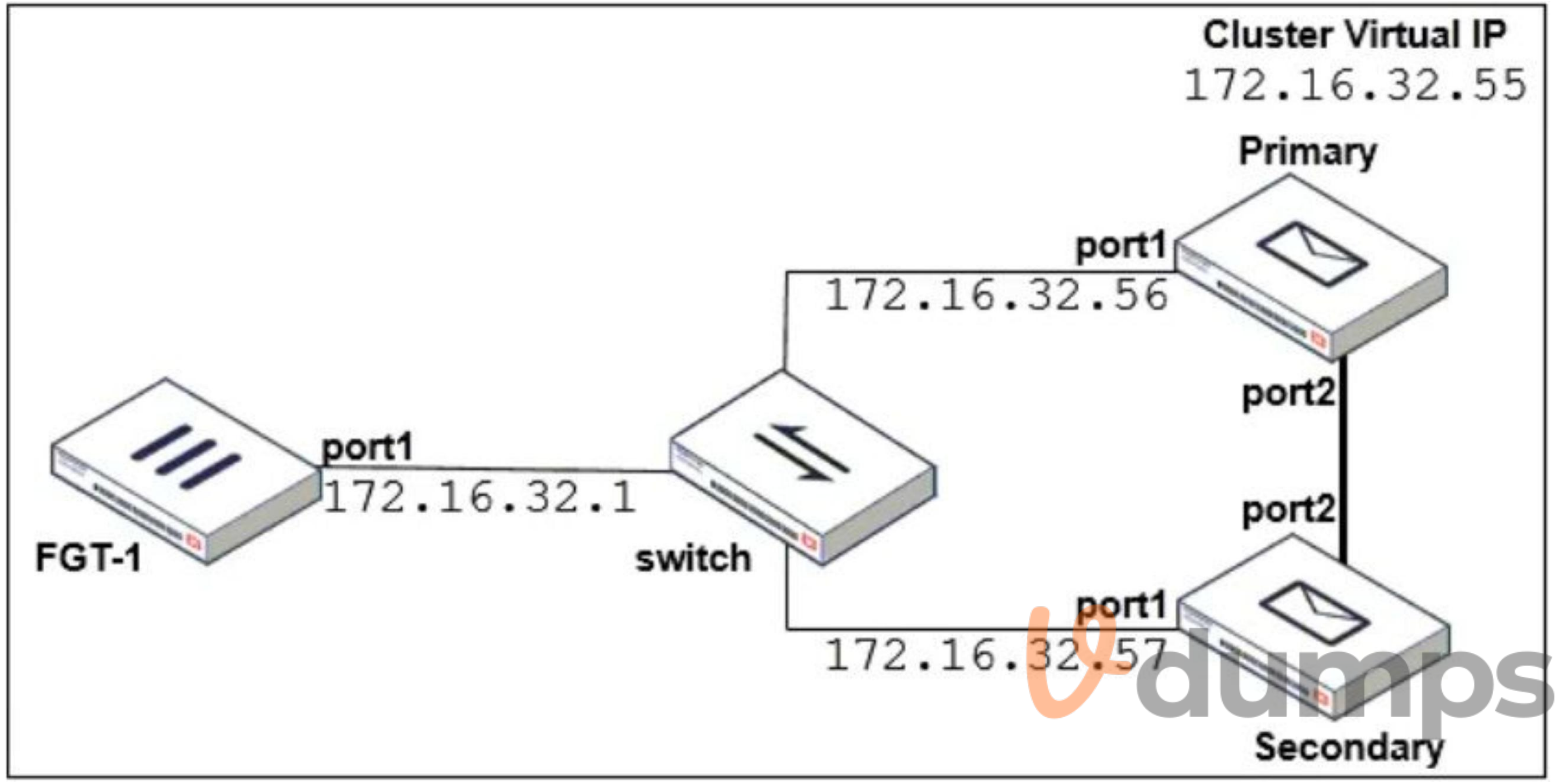
Which two MTA selection behaviors for the example.com domain are correct? (Choose two.)
A. mx.example.com will receive approximately twice the number of email as mx.hosted.com because of its preference value.
B. The primary MTA for the example.com domain is mx.hosted.com.
C. The external MTAs will send email to mx.example.com only if mx.hosted.com is unreachable.
D. The PriNS server should receive all email for the example.com domain.

Correct Answer: B, C
Section:
Explanation:

QUESTION 9
While reviewing logs, an administrator discovers that an incoming email was processed using policy IDs 0:4:9:INTERNAL.
Which two statements describe what this policy ID means? (Choose two.)
A. Access control policy number 9 was used.
B. The FortiMail configuration is missing an access delivery rule.
C. The email was processed using IP-based policy ID 4.
D. FortiMail is applying the default behavior for relaying inbound email.

Correct Answer: A, C
Section:
Explanation:

QUESTION 10
Refer to the exhibit which shows a topology diagram of a FortiMail cluster deployment.



Which IP address must the DNS MX record for this organization resolve to?

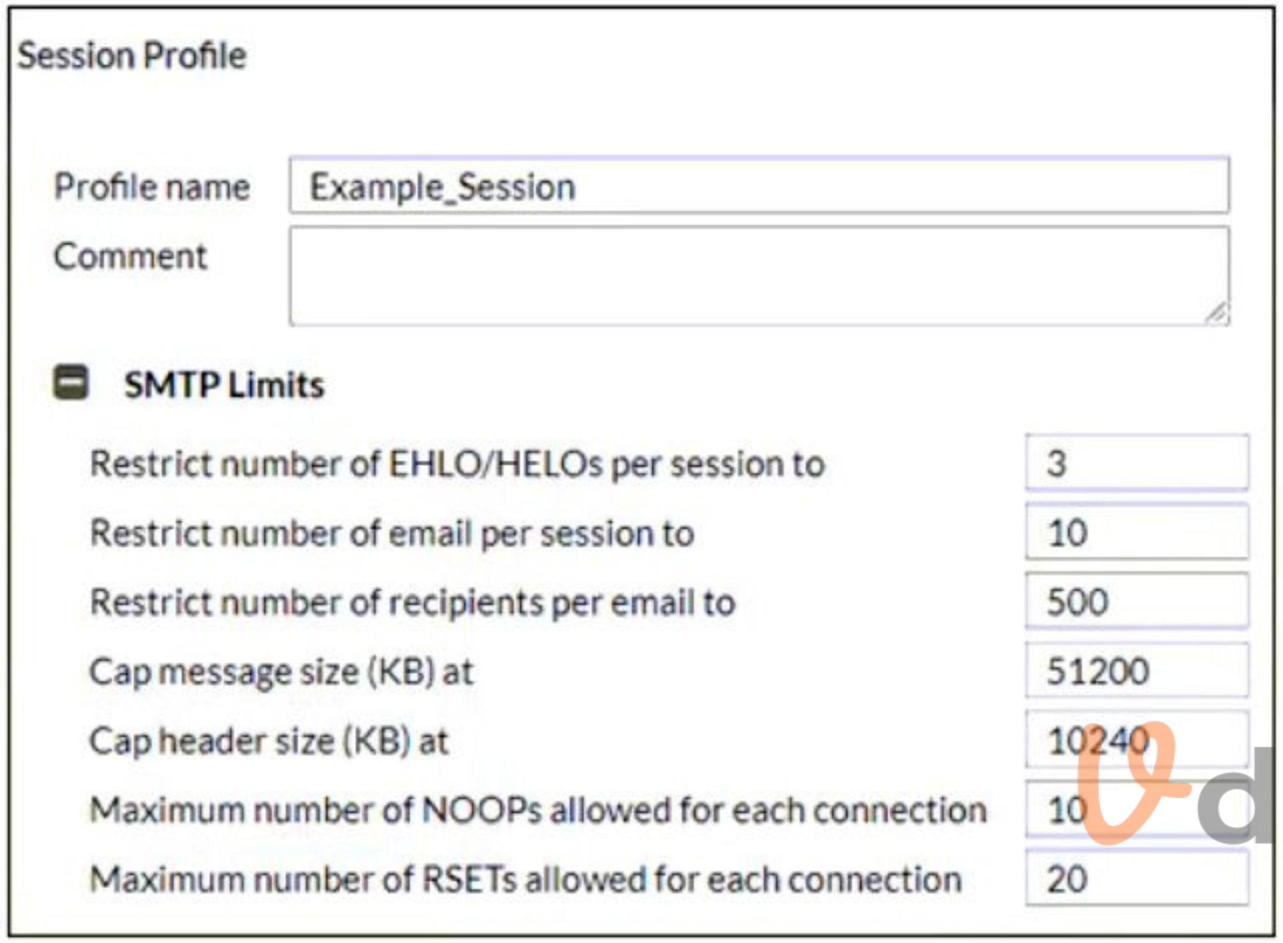
A. 1172 16 32 57
B. 172.16.32.56
C. 172.16.32.55
D. 172.16.32.1

Answer: C

Correct Answer: C
Section:
Explanation:

QUESTION 11
Refer to the exhibits showing SMTP limits (Session Profile --- SMTP Limits), and domain settings (Domain Settings, and Domain Settings --- Other) of a FortiMail device.

Session Profile—SMTP Limits

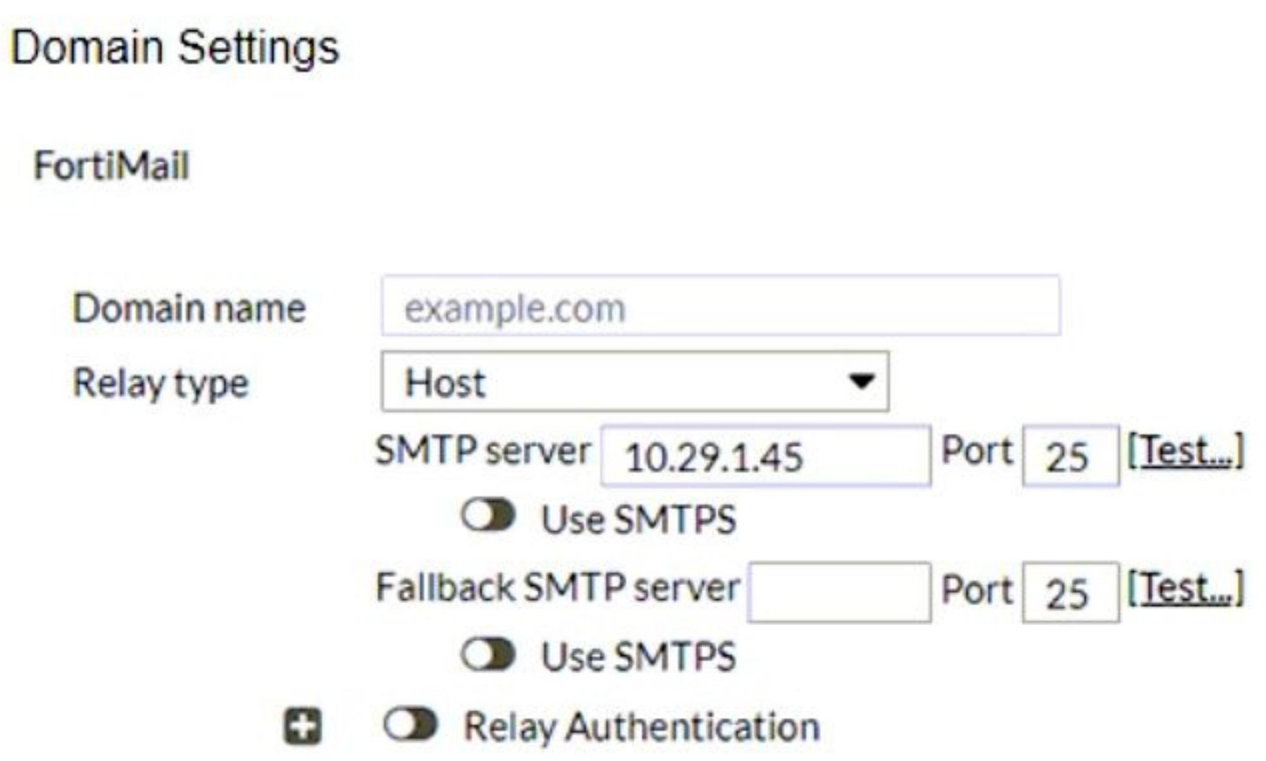


Session Profile

Profile name	Example_Session
Comment	

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



Domain Settings

FortiMail

Domain name: example.com

Relay type: Host

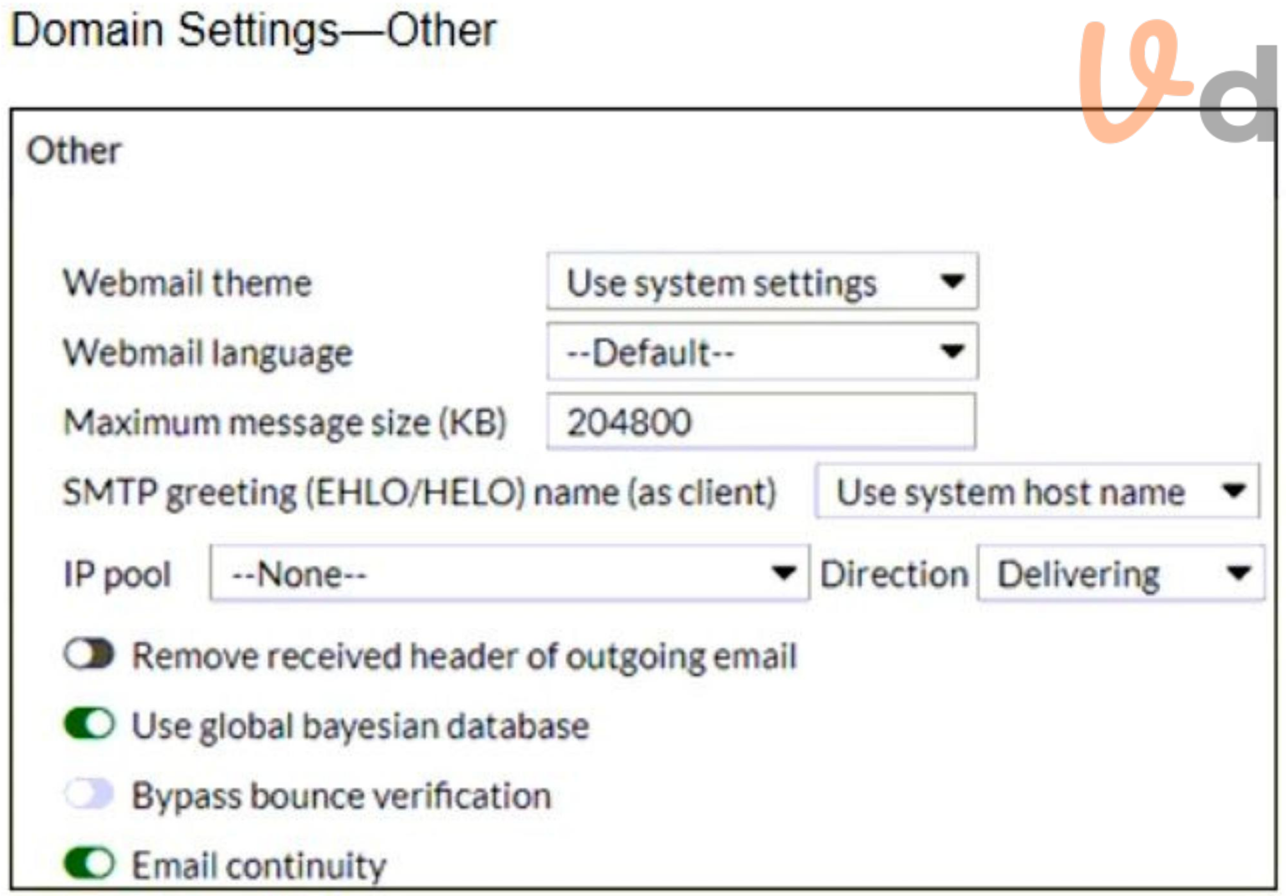
SMTP server: 10.29.1.45 Port: 25 [Test...]

○ Use SMTPS

Fallback SMTP server: Port: 25 [Test...]

○ Use SMTPS

○ Relay Authentication



Domain Settings—Other

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 outgoing email

● Use global bayesian database

○ Bypass bounce verification

● Email continuity

Which message size limit in KB will the FortiMail apply to outbound email?

A. 204300

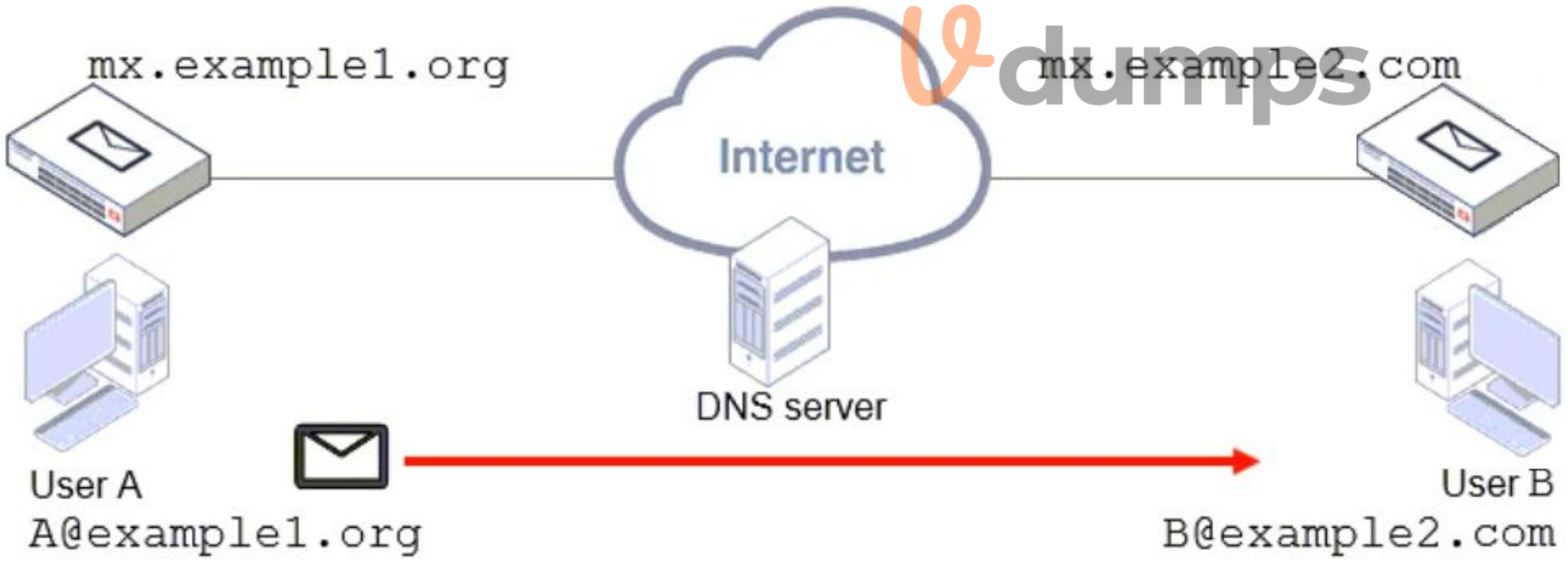
B. There is no message size limit for outbound email from a protected domain.
C. 10240
D. 51200

Correct Answer: D
Section:
Explanation:

QUESTION 12
A FortiMail device is configured with the protected domain example.com.
If none of the senders is authenticated, which two envelope addresses will require an access receive rule? (Choose two.)
A. MAIL FROM: support@example.org RCPT TO: marketing@example.com
B. MAIL FROM: mis@hosted.net RCPT TO: noc@example.com
C. MAIL FROM: accounts@example.com RCPT TO: sales@biz.example.com
D. MAIL FROM: training@example.com RCPT TO: students@external.org

Correct Answer: A, B
Section:
Explanation:

QUESTION 13
Refer to the exhibit, which shows a topology diagram of two separate email domains.

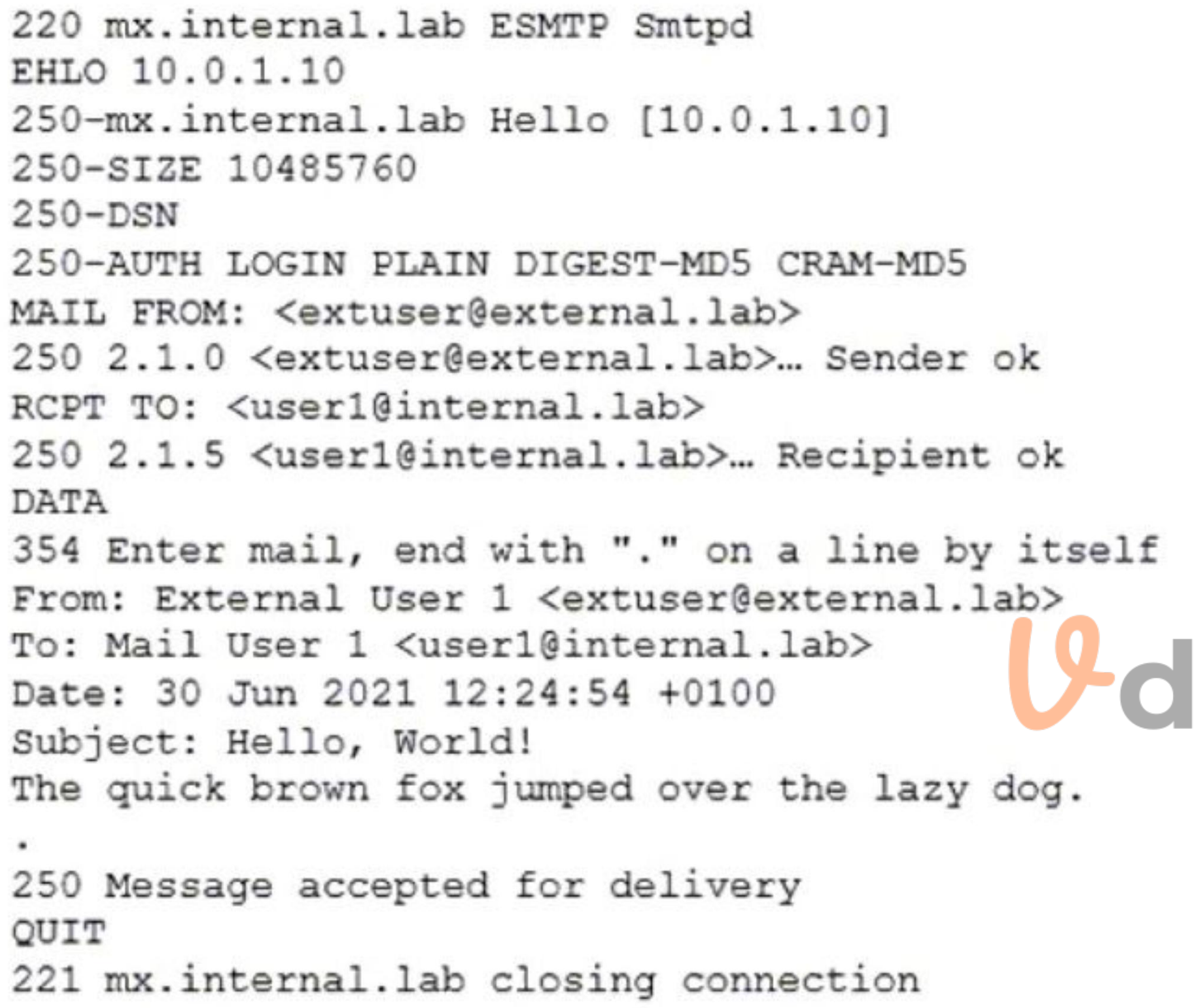


Which two statements correctly describe how an email message is delivered from User A to User B? (Choose two.)
A. mx.example1.org will forward the email message to the MX record that has the lowest preference.
B. User B will retrieve the email message using either POP3 or IMAP.
C. User A's MUA will perform a DNS MX record lookup to send the email message.
D. The DNS server will act as an intermediary MTA.

Correct Answer: A, B
Section:

Explanation:

QUESTION 14
Refer to the exhibit which shows the output of an email transmission using a telnet session.



```
220 mx.internal.lab ESMTP Smtpd
EHLO 10.0.1.10
250-mx.internal.lab Hello [10.0.1.10]
250-SIZE 10485760
250-DSN
250-AUTH LOGIN PLAIN DIGEST-MD5 CRAM-MD5
MAIL FROM: <extuser@external.lab>
250 2.1.0 <extuser@external.lab>… Sender ok
RCPT TO: <user1@internal.lab>
250 2.1.5 <user1@internal.lab>… Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: External User 1 <extuser@external.lab>
To: Mail User 1 <user1@internal.lab>
Date: 30 Jun 2021 12:24:54 +0100
Subject: Hello, World!
The quick brown fox jumped over the lazy dog.
.
250 Message accepted for delivery
QUIT
221 mx.internal.lab closing connection
```

What are two correct observations about this SMTP session? (Choose two.)

A. The SMTP envelope addresses are different from the message header addresses.
B. The '250 Message accepted for delivery' message is part of the message body.
C. The 'Subject' is part of the message header.
D. The '220 mx.internal.lab ESMTP Smtpd' message is part of the SMTP banner.

Correct Answer: C, D
Section:
Explanation:

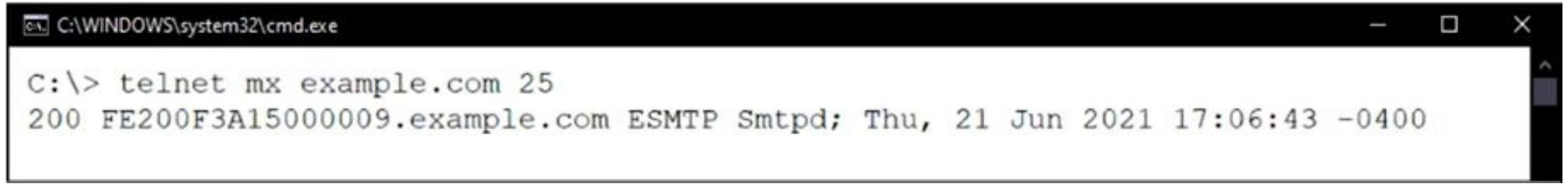
QUESTION 15
Which two features are available when you enable HA centralized monitoring on FortiMail? (Choose two.)

A. Policy configuration changes of all cluster members from the primary device.
B. Mail statistics of all cluster members on the primary device.

C. Cross-device log searches across all cluster members from the primary device.
D. Firmware update of all cluster members from the primary device

Correct Answer: B, C
Section:
Explanation:

QUESTION 16
Refer to the exhibit which shows a command prompt output of a telnet command.


C:\WINDOWS\system32\cmd.exe

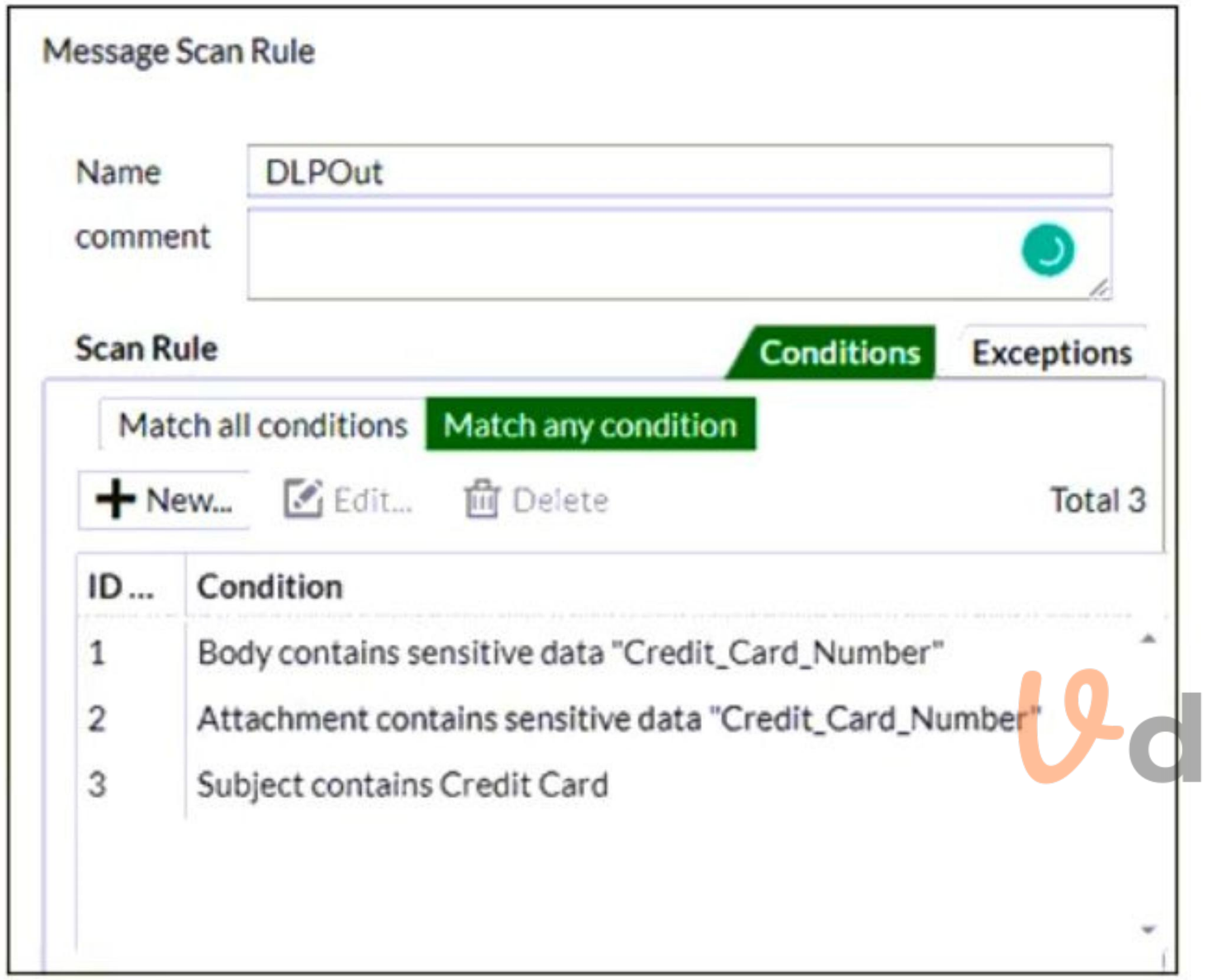
```
C:\> telnet mx example.com 25
200 FE200F3A15000009.example.com ESMTP Smtpd; Thu, 21 Jun 2021 17:06:43 -0400
```

Which configuration change must you make to prevent the banner from displaying the FortiMail serial number?
A. Change the host name
B. Add a protected domain
C. Configure a local domain name
D. Change the operation mode

Correct Answer: A
Section:
Explanation:

QUESTION 17
Refer to the exhibits which shows a DLP scan profile configuration (DLP Scan Rule 1 and DLP Scan Rule 2) from a FortiMail device.

DLP Scan Rule 1



Message Scan Rule

Name: DLPOut

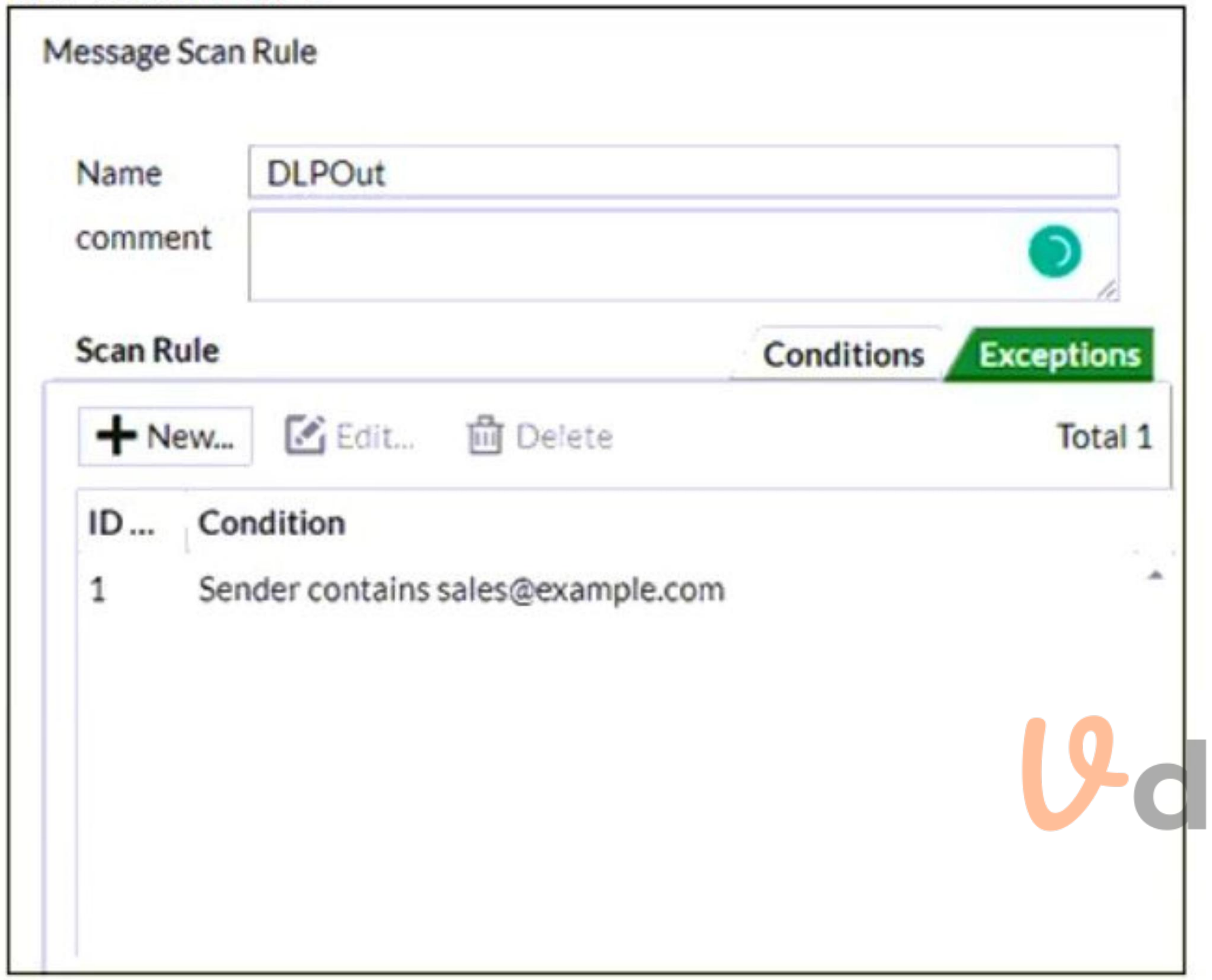
comment:

Scan Rule

Total 3

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

DLP Scan Rule 2



Message Scan Rule

Name: DLPOut

comment:

Scan Rule — Exceptions tab

Total 1

ID ...	Condition
1	Sender contains sales@example.com

Which two message types will trigger this DLP scan rule? (Choose two.)

A. An email that contains credit card numbers in the body, attachment, and subject will trigger this scan rule.

B. An email sent from salesdinternal. lab will trigger this scan rule, even without matching any conditions.

C. An email message with a subject that contains the term 'credit card' will trigger this scan rule.

D. An email message that contains credit card numbers in the body will trigger this scan rule.

Correct Answer: C, D
Section:
Explanation: