ACTUAL
TEST DUMPS

Free Questions for NSE6_FML-7.2 by actualtestdumps

Shared by Brewer on 24-05-2024

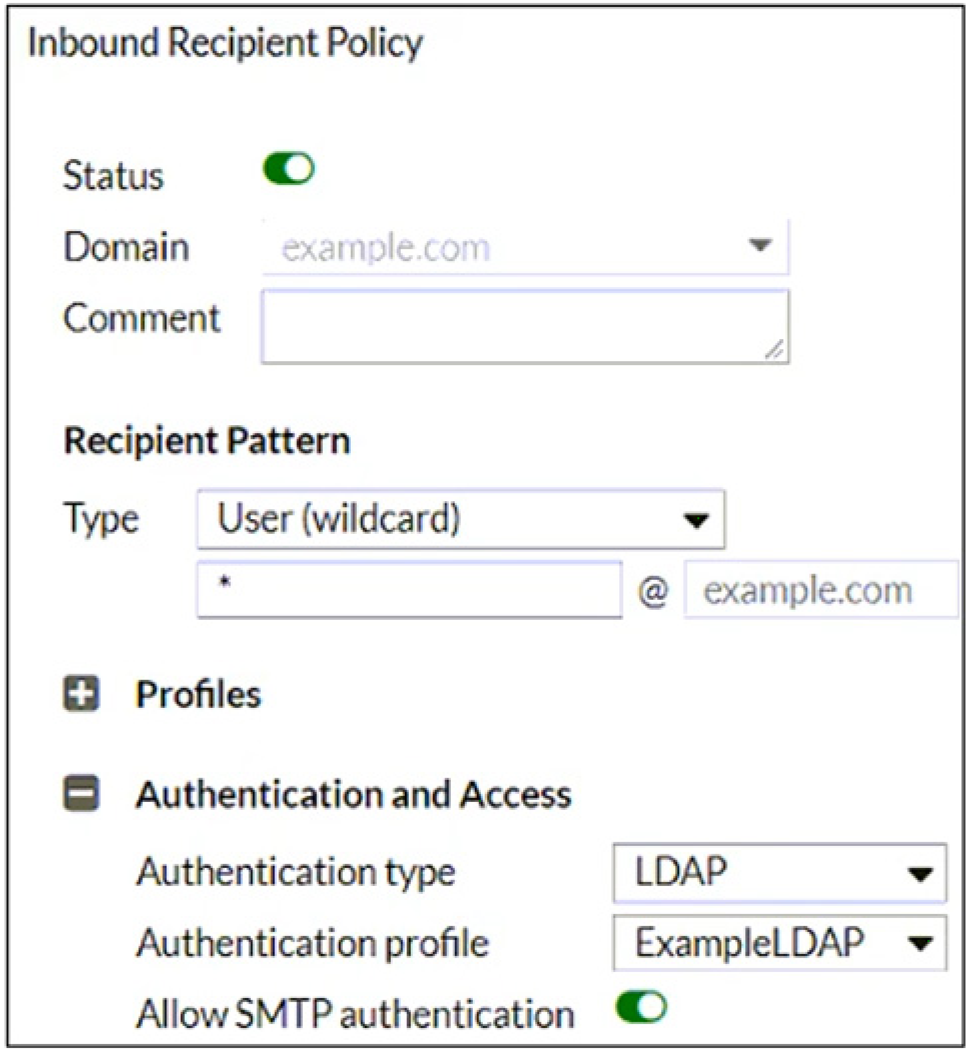
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

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?

Options:

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.

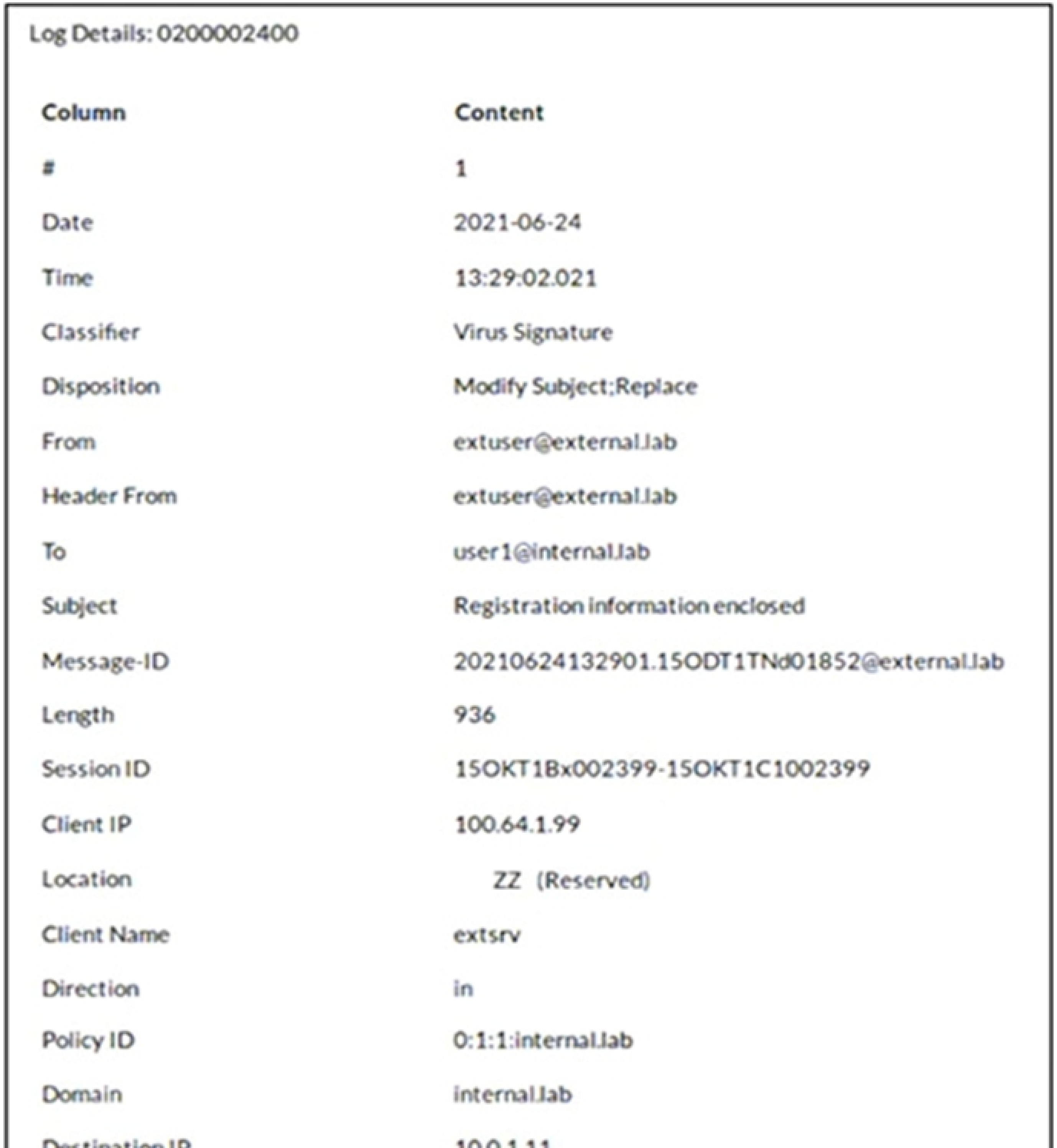
Answer:

D

Question 2

Question Type: MultipleChoice

Refer to the exhibit which shows a detailed history log view.



Log Details: 0200002400

Column	Content
#	1
Date	2021-06-24
Time	13:29:02.021
Classifier	Virus Signature
Disposition	Modify Subject;Replace
From	extuser@external.lab
Header From	extuser@external.lab
To	user1@internal.lab
Subject	Registration information enclosed
Message-ID	20210624132901.15ODT1TNd01852@external.lab
Length	936
Session ID	15OKT1Bx002399-15OKT1C1002399
Client IP	100.64.1.99
Location	ZZ (Reserved)
Client Name	extsrv
Direction	in
Policy ID	0:1:1:internal.lab
Domain	internal.lab
Destination IP	10.0.1.11

Which two actions did FortiMail take on this email message? (Choose two.)

Options:

A- FortJMail replaced the virus content with a message

B- FortiMail modified the subject of the email message.

C- FortiMail forwarded the email to User 1 without scanning.

D- FortiMail sent the email message to User 1's personal quarantine.

Answer:

A, B

Question 3

Question Type: **MultipleChoice**

A FortiMail administrator is investigating a sudden increase in DSNs being delivered to their protected domain. After searching the logs, the administrator identifies that the DSNs were not generated because of any outbound email sent from their organization.

Which FortiMail antispam technique can the administrator use to prevent this scenario?

Options:

A- FortiGuard IP Reputation

B- Spoofed header detection

C- Spam outbreak protection

D- Bounce address tag validation

Answer:

D

Question 4

Question Type: **MultipleChoice**

In which FortiMail configuration object can you assign an outbound session profile?

Options:

A- Outbound recipient policy

B- Inbound recipient policy

C- IP policy

D- Access delivery rule

Answer:

A

Question 5

Question Type: **MultipleChoice**

What are two disadvantages of configuring the dictionary and DLP scan rule aggressiveness too high? (Choose two.)

Options:

A- High aggressiveness scan settings do not support executable file types.

B- It is more resource intensive

C- More false positives could be detected.

D- FortiMail requires more disk space for the additional rules.

Answer:

B, C

Question 6

Question Type: **MultipleChoice**

Which item is a supported one-time secure token for IBE authentication?

Options:

A- FortiToken

B- Certificate

C- SMS

D- Security question

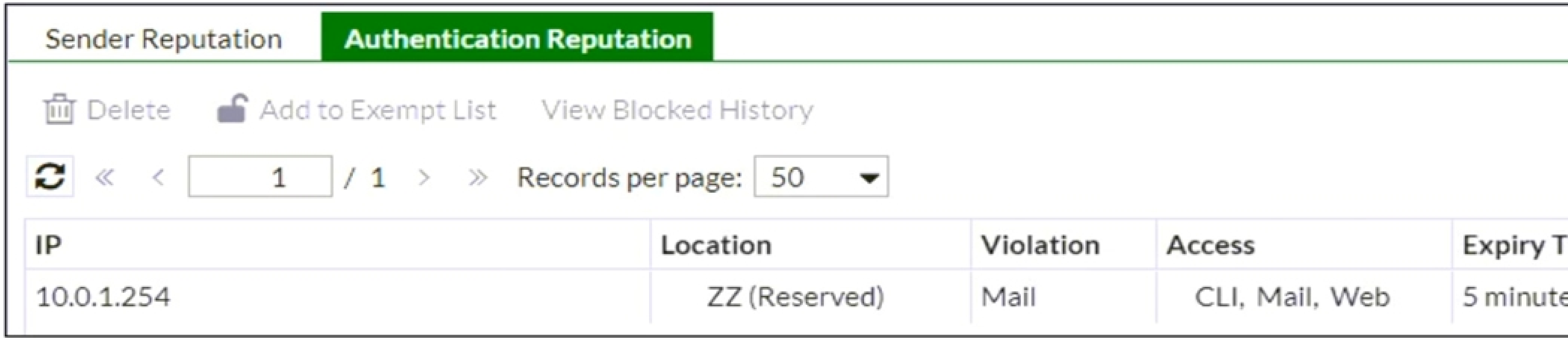
Answer:

D

Question 7

Question Type: **MultipleChoice**

Refer to the exhibit which shows the Authentication Reputation list on a gateway mode FortiMail device.



IP	Location	Violation	Access	Expiry T
10.0.1.254	ZZ (Reserved)	Mail	CLI, Mail, Web	5 minute

Why was the IP address blocked?

Options:

A- The IP address had consecutive SMTPS login failures to FortiMail.

B- The IP address had consecutive IMAP login failures to FortiMail.

C- The IP address had consecutive SSH, SMTPS, and HTTPS login failures to FortiMail.

D- The IP address had consecutive administrative password failures to FortiMai

Answer:

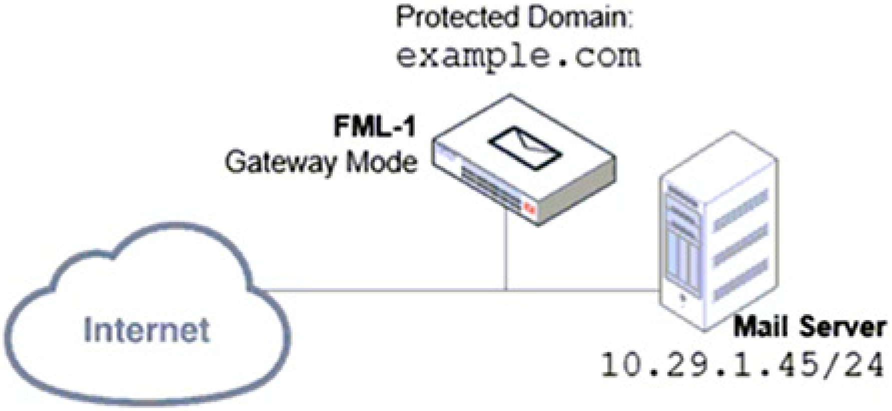
C

Question 8

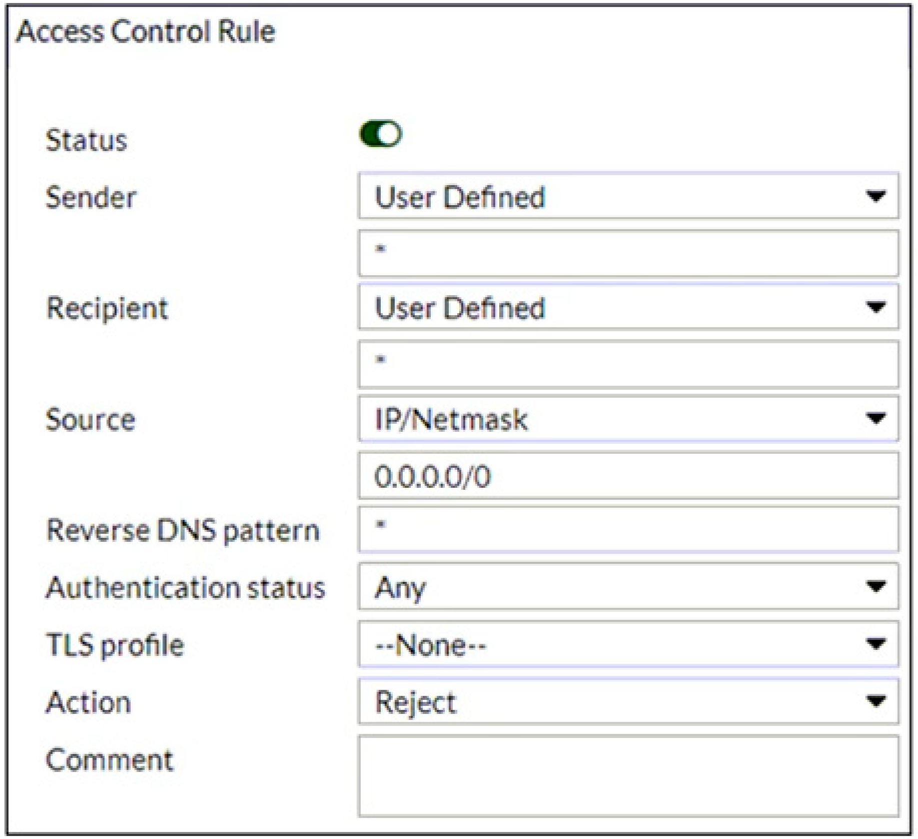
Question Type: **MultipleChoice**

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

Topology


Protected Domain:
example.com
FML-1
Gateway Mode
Internet
Mail Server
10.29.1.45/24

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	

Which three access control settings are recommended to allow outbound email from the example.com domain on FML-1? (Choose three.)

Options:

A- The Sender IP/netmask should be set to 10.29.1.45/32.

B- The Recipient pattern should be set to 10.29.1.45/24

C- The Action should be set to Relay.

D- The Sender pattern should be set to *@example.com.

E- The Enable check box should be cleared.

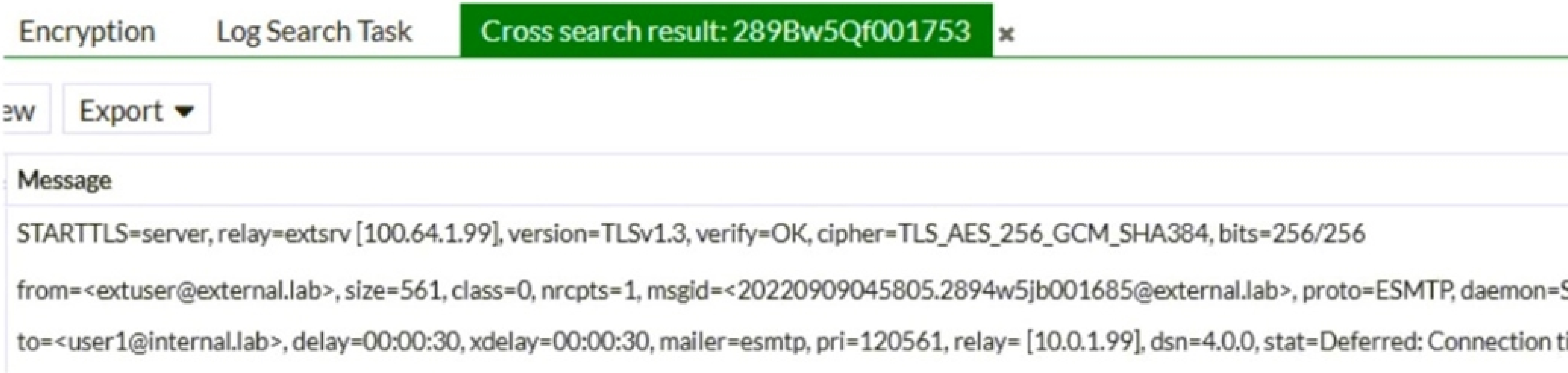
Answer:

A, C, D

Question 9

Question Type: **MultipleChoice**

Refer to the exhibit, which shows a few lines of FortiMail logs.



```
STARTTLS=server, relay=extsrv [100.64.1.99], version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, bits=256/256
from=<extuser@external.lab>, size=561, class=0, nrcpts=1, msgid=<20220909045805.2894w5jb001685@external.lab>, proto=ESMTP, daemon=S
to=<user1@internal.lab>, delay=00:00:30, xdelay=00:00:30, mailer=esmtp, pri=120561, relay= [10.0.1.99], dsn=4.0.0, stat=Deferred: Connection ti
```

Based on these log entries, which two statements correctly describe the operational status of this FortiMail device? (Choose two.)

Options:

A- FortJMail is experiencing issues delivering the email to the internal.lab MTA.

B- The FortiMail device is in sever mode.

C- The FortiMail device is in gateway or transparent mode.

D- FortiMail is experiencing issues accepting the connection from the external. lab MTA.

Answer:

A, C

Question 10

Question Type: MultipleChoice

An organization has different groups of users with different needs in email functionality, such as address book access, mobile device access, email retention periods, and disk quotas.

Which FortiMail feature specific to server mode can be used to accomplish this?

Options:

A- Resource profiles

B- Domain-level service settings

C- Access profiles

D- Address book management options

Answer:

A

Question 11

Question Type: **MultipleChoice**

In which two places can the maximum email size be overridden on FortiMail? (Choose two.)

Options:

A- IP Policy configuration

B- Protected Domain configuration

C- Resource Profile configuration

D- Session Profile configuration

Answer:

B, C