



Prepare Smart for Success Free Fortinet FCP_FML_AD-7.4 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet FCP - FortiMail 7.4 Administrator exam PDF questions now. Get authentic FCP_FML_AD-7.4 dumps packed with verified answers and secure your certification success with PrepBolt FCP_FML_AD-7.4 exam pdf questions and answers.

Thank you for Downloading FCP_FML_AD-7.4 exam PDF Demo

https://prepbolt.com/FCP_FML_AD-7.4.html

QUESTIONS & ANSWERS
DEMO VERSION
(LIMITED CONTENT)

Question 1

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

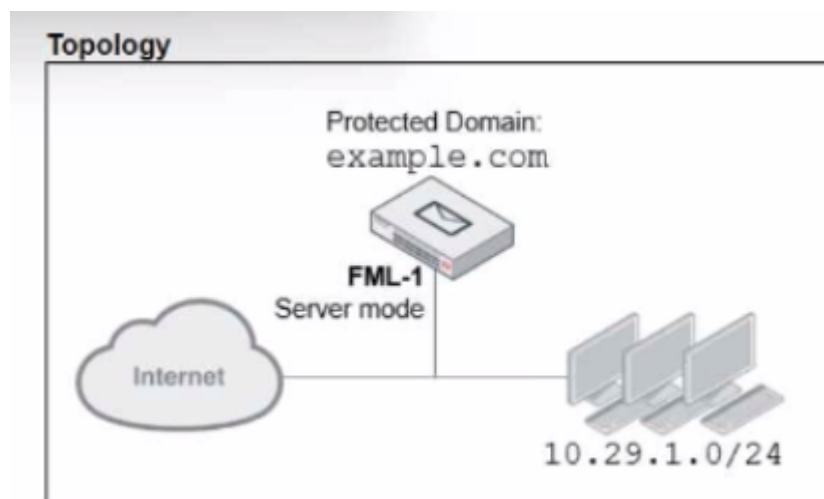
Answer:

C

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



Access Control Rule

Access Control Rule

Status	<input checked="" type="checkbox"/>
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	

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

An administrator wants to configure an access receive rule to match authentication status on FML-1 for all outbound email from the example. co- domain.

Which two access receive rule settings must the administrator configure? (Choose two.)

Options:

- A- The Sender IP/netmask must be set to 10.29.1.0/24.
- B- A TLS profile must be configured and applied.
- C- The Recipient pattern must be set to *@example. com.
- D- The Authentication status must be set to Authenticated

Answer:

C, D

Question 3

Question Type: MultipleChoice

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

Comment

SMTP Limits

Restrict number of EHLO/HELOs per session to	<input type="text" value="3"/>
Restrict number of email per session to	<input type="text" value="10"/>
Restrict number of recipients per email to	<input type="text" value="500"/>
Cap message size (KB) at	<input type="text" value="51200"/>
Cap header size (KB) at	<input type="text" value="10240"/>
Maximum number of NOOPs allowed for each connection	<input type="text" value="10"/>
Maximum number of RSETs allowed for each connection	<input type="text" value="20"/>

Domain Settings

FortiMail

Domain name

Relay type

SMTP server Port [\[Test...\]](#)

Use SMTPS

Fallback SMTP server Port [\[Test...\]](#)

Use SMTPS

Relay Authentication

Domain Settings—Other

Other

Webmail theme

Webmail language

Maximum message size (KB)

SMTP greeting (EHLO/HELO) name (as client)

IP pool Direction

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?

Options:

- A- 204300
- B- There is no message size limit for outbound email from a protected domain.
- C- 10240
- D- 51200

Answer:

D

Question 4

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 enable to prevent this scenario?

Options:

- A- Spoofed header detection
- B- Spam outbreak protection.
- C- FortiGuard IP Reputation
- D- Bounce address tag validation

Answer:

D

Question 5

Question Type: MultipleChoice

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.)

Options:

- 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.

Answer:

B, C

Question 6

Question Type: MultipleChoice

Which SMTP command lists (the supported SMTP service extensions of the recipient MTA)?

Options:

- A- DATA
- B- VRFY
- C- EHLO
- D- HELO

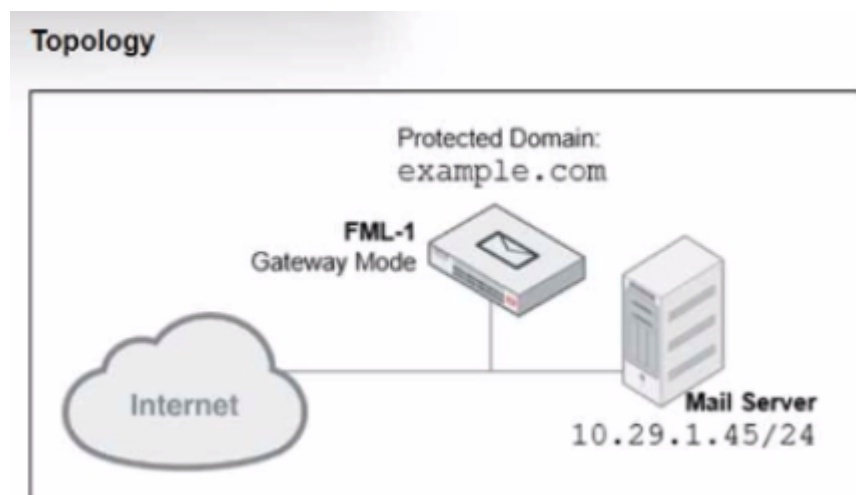
Answer:

A

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



IP Policy

IP Based Policy

Status

Source IP/Netmask 0.0.0.0 / 0

Destination IP/Netmask 0.0.0.0 / 0

Action Scan

Comment

Profiles

Session	Example_Session	+	✎
AntiSpam	--None--	+	✎
AntiVirus	--None--	+	✎
Content	--None--	+	✎
DLP	--None--	+	✎
IP pool	--None--	+	✎

Authentication and Access

Miscellaneous

Reject different SMTP sender identity for authenticated user

Sender identity verification with LDAP server for authenticated user

LDAP profile --None-- + ✎

Take precedence over recipient based policy match

Refer to the exhibits, which show a topology diagram (Topology) and a configuration element (IP Policy).

An administrator has enabled the sender reputation feature in the Example_Session profile on FML-1. After a few hours, the deferred queue on the mail server starts filling up with undeliverable email.

Which two changes must the administrator make to fix this issue? (Choose two.)

Options:

- A- Disable the exclusive flag in IP policy ID 1.
- B- Apply a session profile with sender reputation disabled on a separate IP policy for outbound sessions.
- C- Clear the sender reputation database using the CLI.
- D- Create an outbound recipient policy to bypass outbound email from session profile inspections.

Answer:

B, C

Question 8

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

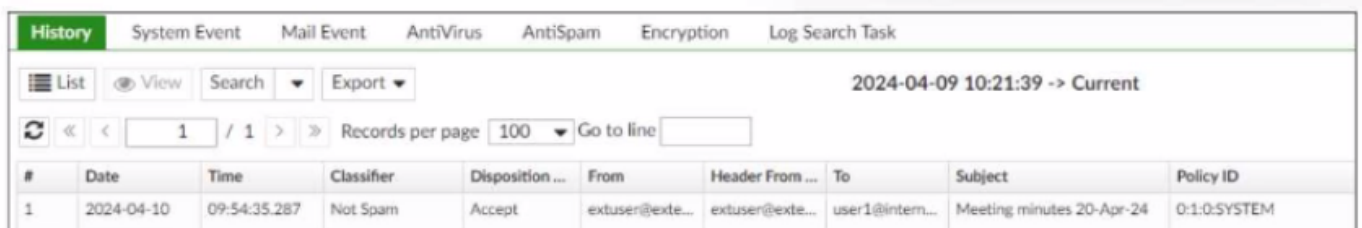
Answer:

D

Question 9

Question Type: MultipleChoice

Refer to the exhibit, which displays a history log entry.



The screenshot shows a web interface for viewing history logs. At the top, there are tabs for 'History', 'System Event', 'Mail Event', 'AntiVirus', 'AntiSpam', 'Encryption', and 'Log Search Task'. Below the tabs, there are controls for 'List', 'View', 'Search', and 'Export'. The current view is for the date '2024-04-09 10:21:39 -> Current'. There are navigation arrows and a 'Records per page' dropdown set to '100'. Below this is a table with the following data:

#	Date	Time	Classifier	Disposition ...	From	Header From ...	To	Subject	Policy ID
1	2024-04-10	09:54:35.287	Not Spam	Accept	extuser@exte...	extuser@exte...	user1@intern...	Meeting minutes 20-Apr-24	0:1:0:SYSTEM

In the Policy ID column, why is the last policy ID value SYSTEM?

Options:

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

Answer:

D

Thank You for trying FCP_FML_AD-7.4 PDF Demo

To try our FCP_FML_AD-7.4 practice exam
software visit link below

https://prepbolt.com/FCP_FML_AD-7.4.html

Start Your FCP_FML_AD-7.4 Preparation

Use Coupon "SAVE50" for extra 50% discount on the purchase of
Practice Test Software. Test your FCP_FML_AD-7.4 preparation with
actual exam questions.