



Download Fortinet FCP_FML_AD-7.4 Exam Dumps Free

Shared by Bowen on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

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

Options:

- 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

Answer:

B, C

Question 2

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 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

Refer to the exhibit which displays a list of IBE users on a FortiMail device.

| Enabled | Email | First Name | Last Name | Status | Creation Time | Last Access |
|-------------------------------------|-----------------------|------------|-----------|----------------|---------------|-------------|
| <input checked="" type="checkbox"/> | extuser@external.lab | Mail | User | Activated | | |
| <input checked="" type="checkbox"/> | extuser2@external.lab | | | Pre-registered | | |

Which statement describes the pre-registered status of the IBE user extuser2@external.lab?

Options:

- A- The user has received an IBE notification email, but has not accessed the HTTPS URL or attachment yet.
- B- The user was registered by an administrator in anticipation of IBE participation.
- C- The user account has been de-activated, and the user must register again the next time they receive an IBE email.
- D- The user has completed the IBE registration process, but has not yet accessed their IBE email.

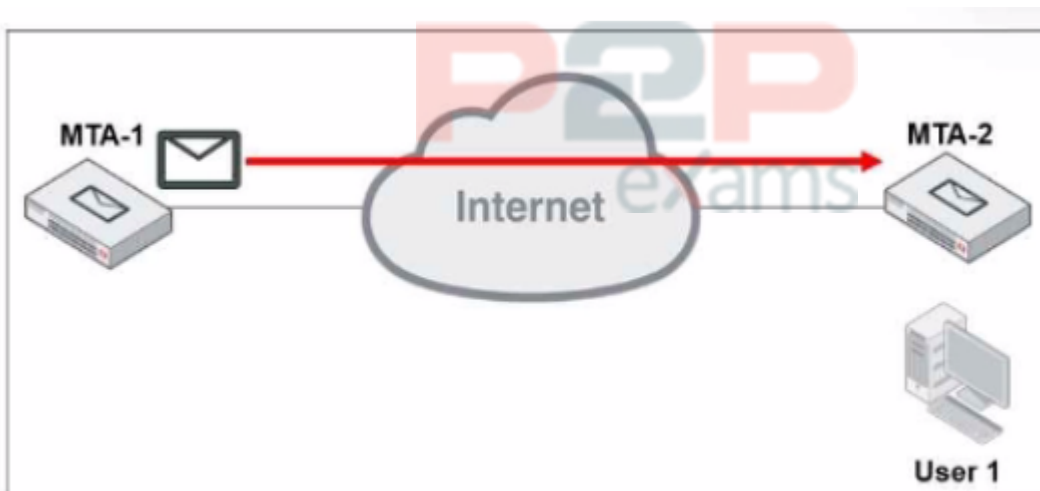
Answer:

A

Question 5

Question Type: MultipleChoice

Refer to the exhibit, which shows a topology diagram of two MTAs.



MTA-1 is delivering an email intended for User 1 to MTA-2. User 1 uses Outlook as an email client. Which two statements about protocol usage between these devices are correct? (Choose two.)

Options:

- A- User 1 will use IMAP or POP3 to download the email message from MTA-2.
- B- MTA-2 will use IMAP to download the email message from MTA-1.
- C- MTA-1 will use SMTP to deliver the email message to MTA-2.
- D- MTA-1 will use POP3 to deliver the email message to User 1 directly.

Answer:

A, C

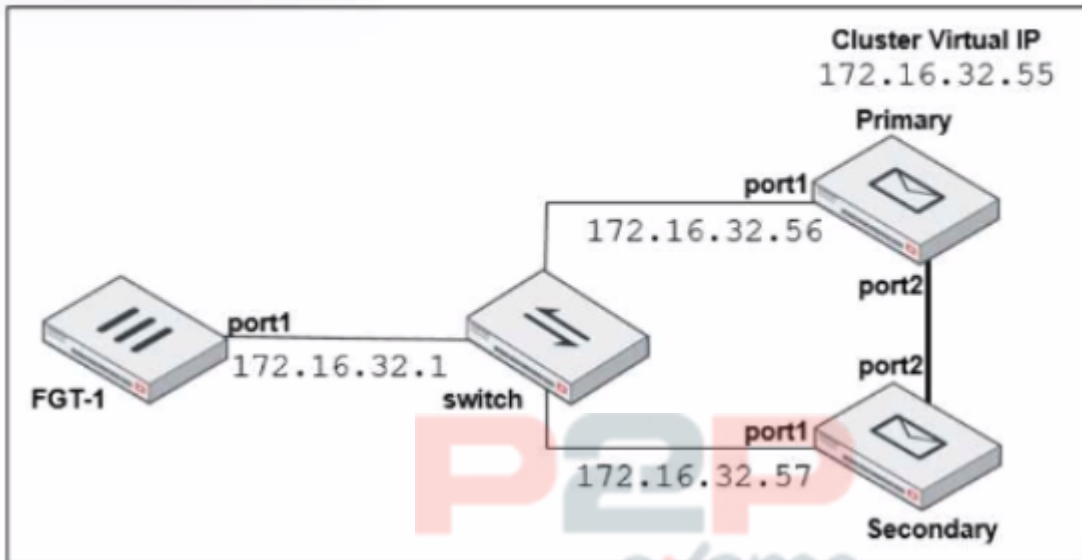
Question 6

Question Type: MultipleChoice

Refer to the exhibits.



Topology



HA Interface Configuration

| HA Interface | |
|----------------------|--------------------------|
| Port | port1... |
| Enable port monitor | <input type="checkbox"/> |
| Heartbeat status | Disable |
| Peer IP address: | 0.0.0.0 |
| Peer IPv6 address: | :: |
| Virtual IP action | Ignore |
| Virtual IP address | 0.0.0.0 / 0 |
| Virtual IPv6 address | :: / 0 |

The exhibits display a topology diagram of a FortiMail cluster (Topology) and the primary HA interface configuration of the Primary FortiMail (HA Interface Configuration)

Which three actions are recommended when configuring the main FortiMail HA interface? (Choose three.)

Options:

- A- In the Heartbeat status drop-down list, select Primary
- B- In the Virtual IP action drop-down list, select Use
- C- In the Virtual IP address field, type 172.16.32.55/24
- D- In the Peer IP address field, type 172.16.32.57
- E- Disable Enable port monitor

Answer:

B, C, D

Question 7

Question Type: MultipleChoice

A FortiMail administrator is concerned about cyber criminals attempting to get sensitive information from employees using whaling phishing attacks. What option can the administrator configure to prevent these types of attacks?

Options:

- A- Impersonation analysis
- B- Dictionary profile with predefined smart identifiers
- C- Bounce tag verification
- D- Content disarm and reconstruction

Answer:

A

Question 8

Question Type: MultipleChoice

Which two antispam techniques query FortiGuard for rating information? (Choose two.)

Options:

- A- DNSBL
- B- IP reputation
- C- URL filter
- D- SURBL

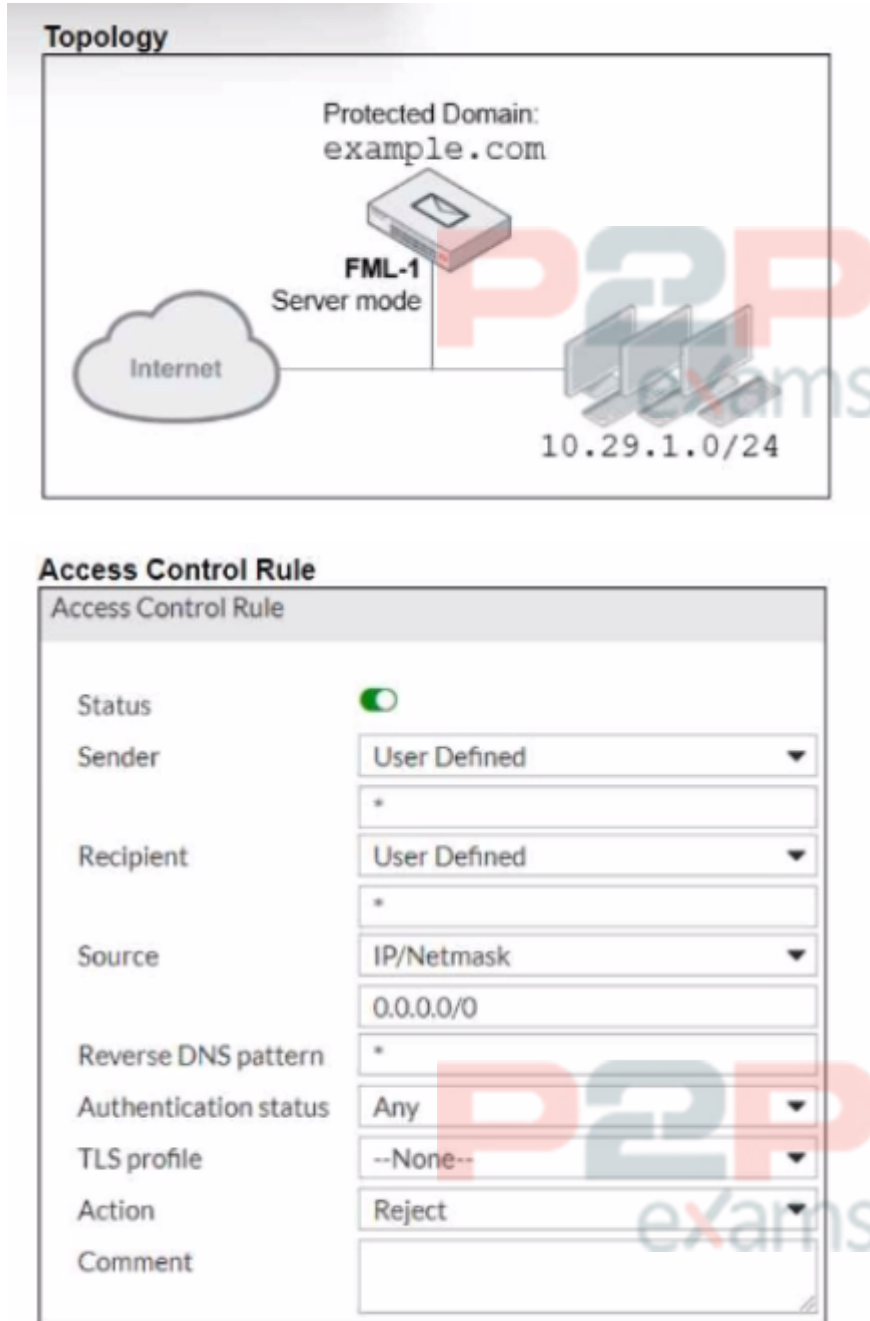
Answer:

B, C

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



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



To Get Premium Files for FCP_FML_AD-7.4
Visit

https://www.p2pexams.com/products/fcp_fml_ad-7.4

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/fcp-fml-ad-7.4>

20%
DISCOUNT

P2P
exams