ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

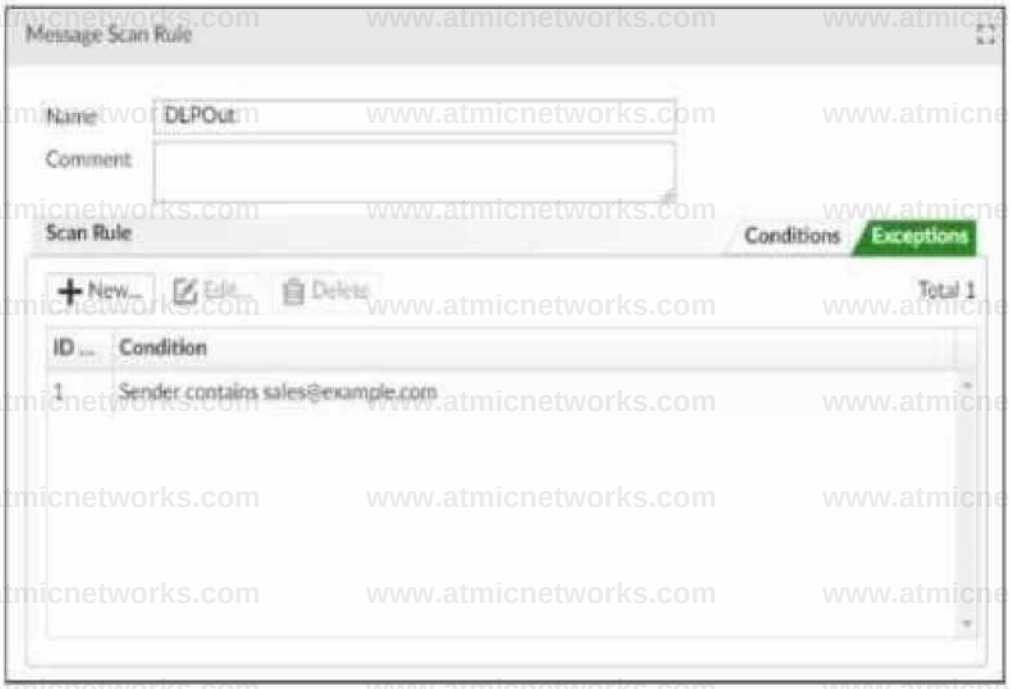
www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Refer to the exhibit.

DLP Scan Rule 2



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

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 sales@internal. lac will trigger this scan rule, even without matching any conditions.

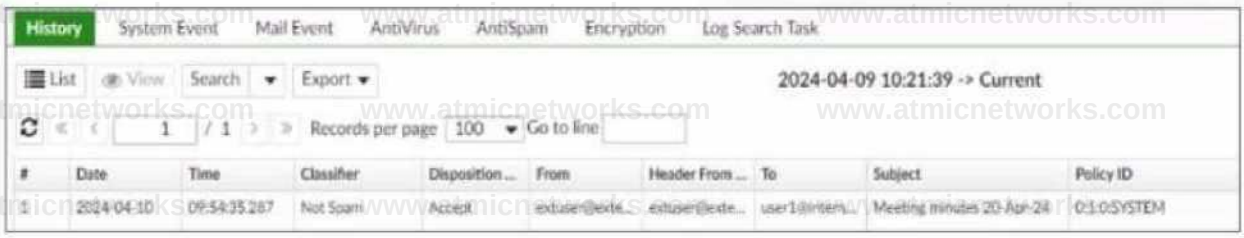
C. An email message that contains credit card numbers in the body will trigger this scan rule.

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

Answer: C, D

Question: 2

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



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

A. The email was dropped by a system blacklist.

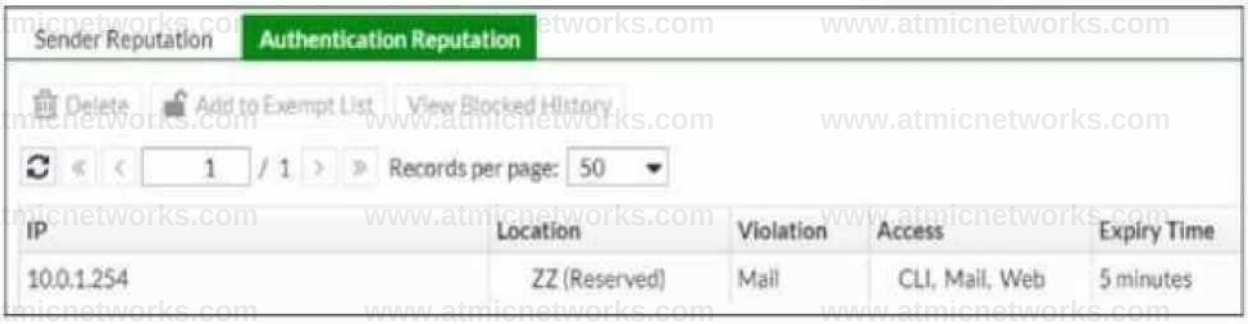
B. The email matched a system-level authentication policy.

C. It is an inbound email.
D. The email did not match a recipient-based policy.

Answer: D

Question: 3

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



Why was the IP address blocked?

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 administrative password failures to FortiMail.
D. The IP address had consecutive SSH login failures to FortiMail.

Answer: A

Question: 4

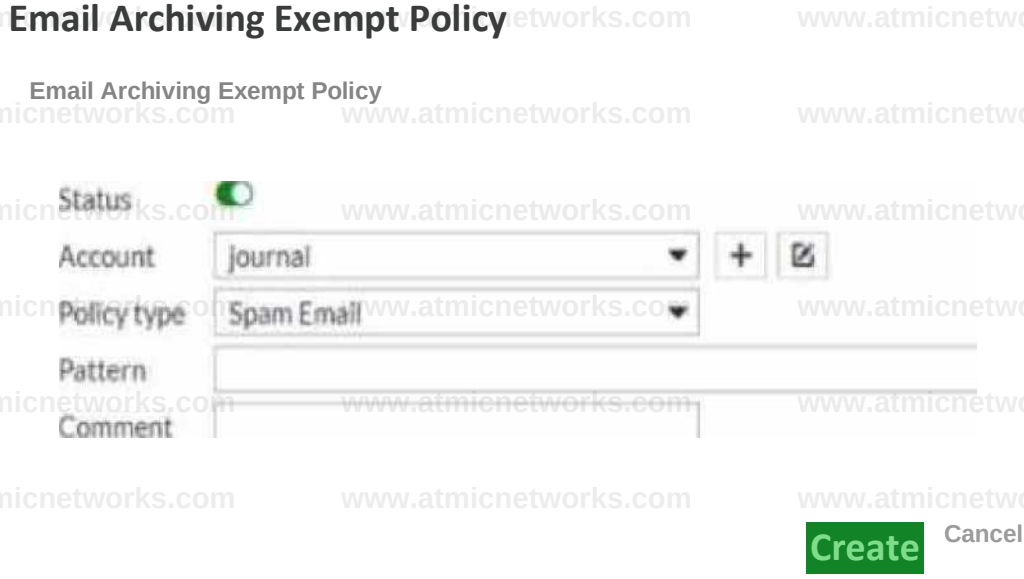
Which three configuration steps must you set to enable DKIM signing for outbound messages on FortiMail? (Choose three.}

A. Generate a public/private key pair in the protected domain configuration.
B. Enable the DKIM checker in a matching session profile.
C. Publish the public key as a TXT record in a public DNS server.
D. Enable the DKIM checker in a matching antispam profile.
E. Enable DKIM signing for outgoing messages in a matching session profile.

Answer: A, C, E

Question: 5

Exhibit.



Refer to the exhibits, which show an email archiving configuration (Email Archiving 1 and Email Archiving 2) from a FortiMail device.

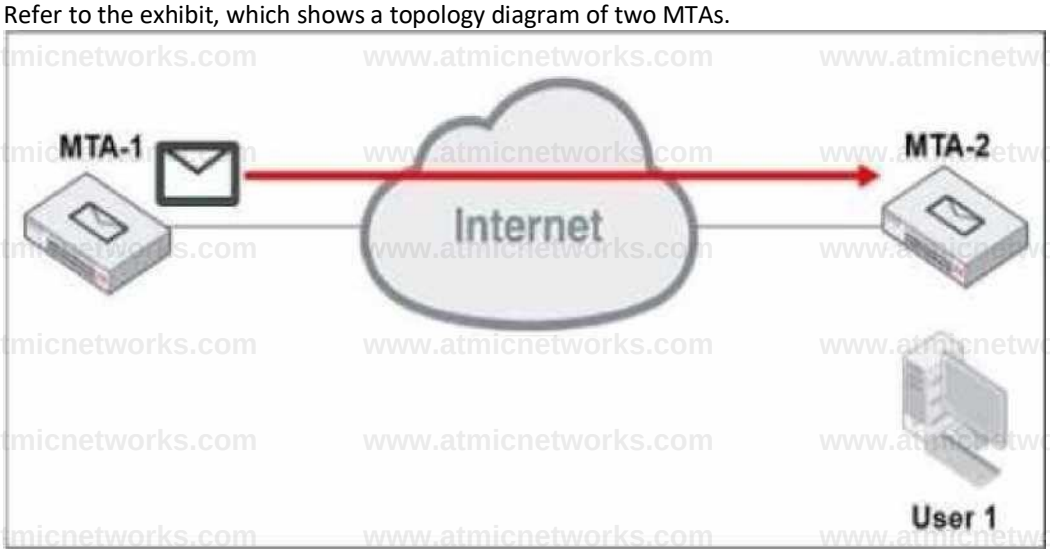
What two archiving actions will FortiMail take when email messages match these archive policies? (Choose two.)

A. FortiMail will save archived email in the journal account.
B. FortiMail will archive email sent from marketingexample. com.
C. FortiMail will exempt spam email from archiving.
D. FortiMail will allow only the marketingeexample.com account to access the archived email.

Answer: A, C

Question: 6

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



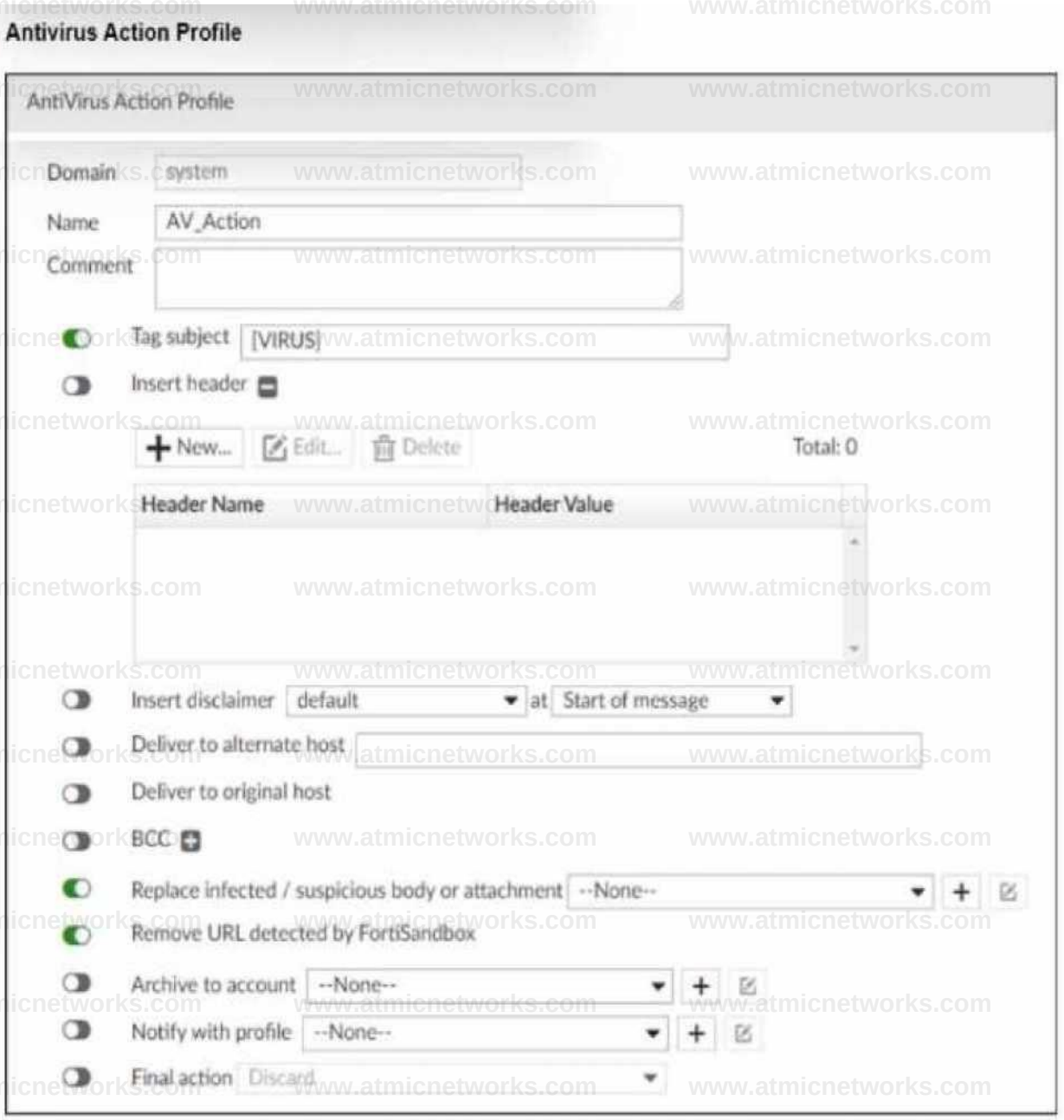
MTA-1 is delivering an email intended for User 1 to MTA-2. User 1 uses Outlook as an email client. Which two statements about protocol usage between these devices are correct? (Choose two.)

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: 7

Refer to the exhibit.



Refer to the exhibit, which shows an antivirus action profile.

What are two expected outcomes if FortiMail applies this antivirus action profile to an email?

(Choose two.)

A. Virus content will be removed from the email.

B. The original email will be sent to the system quarantine.

C. The sanitized email will be sent to the recipient's personal quarantine.

D. A replacement message will be added to the email.

Answer: A, D

Question: 8

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

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

Answer: B, C

Question: 9

While testing outbound MTA functionality, an administrator discovers that all outbound email is being processed using policy ID l: 2:0: SYSTEM. What are two possible reasons why the third policy ID value is o? (Choose two.)

A. IP policy ID 2 has the exclusive flag set.
B. There are no outgoing recipient policies configured.
C. Outbound email is being rejected.
D. There are no access delivery rules configured for outbound email.

Answer: A, B

Question: 10

What are Two reasons for having reliable DNS servers configured on FortiMail? (Choose two.)

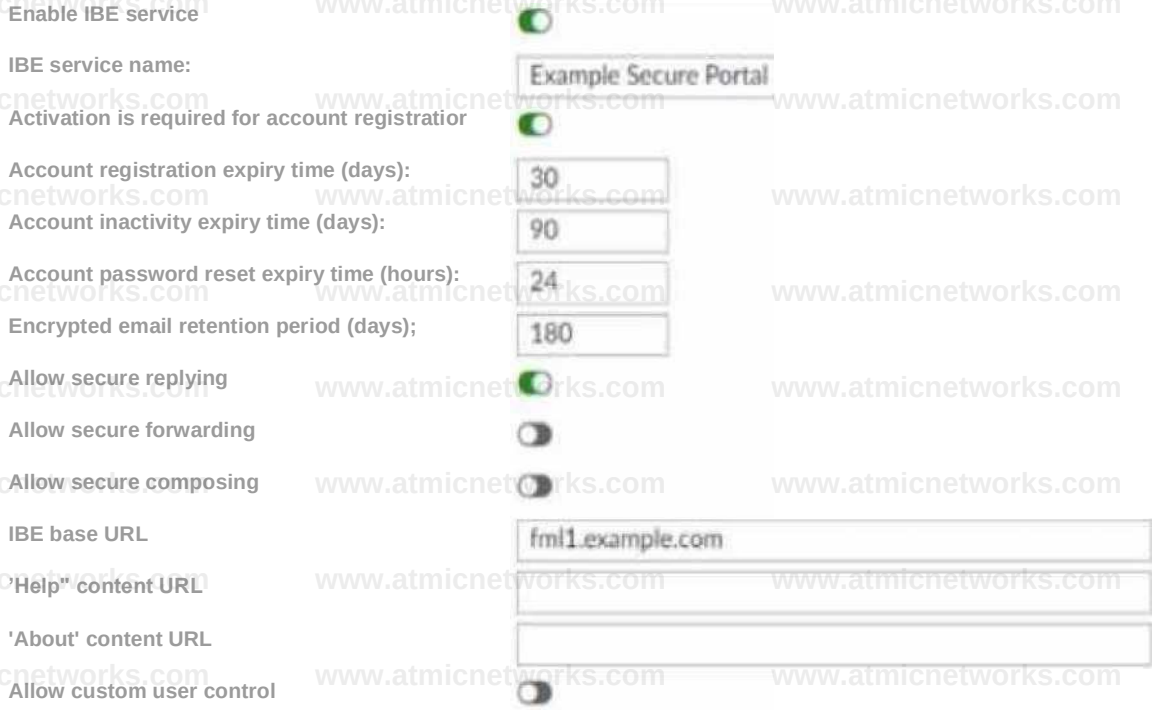
A. Email transmission
B. Firmware updates
C. FortiGuard Connectivity
D. HA synchronization

Answer: A, C

Question: 11

Exhibit.

FortiMail IBE encryption



Reter to the exhibit, which shows the IBE Encryption page of a FortiMail device. Which user account behavior can you expect from these IBE settings?

A. After initial registration. IBE users can access the secure portal without authenticating again for 90 days.

B. Registered IBE users have 90 days from the time they receive a notification email message to access their IBE email.

C. IBE user accounts will expire after 90 days of inactivity and must register again to access new IBE email message.

D. First time IBE users must register to access their email within 90 days of receiving the notification email message

Answer: C

Question: 12

A FortiMail is configured with the protected domain example.com.
On this FortiMail, which two envelope addresses are considered incoming? (Choose two.)

A. EMAIL FROM: nisGhosted.r.et RCPT 70: noceexample.com
B. MAIL FROM: supporteexample.com RCPT TO: marketing@example.com
C. MAIL FROM: accountsGexample.ccm RCPT TO: sales@external.org
D. MAIL FROM: training&external.crg RCPT TO: student30extersal.org

Answer: B, C

Question: 13

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

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

A. FortiMail is experiencing issues accepting the connection from the external. lab MTA.
B. FortiMail is experiencing issues delivering the email to the internal. lab MTA.
C. The FortiMail device is in server mode.
D. The FortiMail device is in gateway or transparent mode.

Answer: B, D

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: <exluset8exLern&l.lab>
250 2.1.0 <extuser8extemal. labx.. Sender ok RCPT TO: <userl8internal.lab>
250 2.1 .5 <u»erl8interna I.lab>_ Recipient ok DATA
354 Enter mail, end with ".*' on a line by itself From: External User 1 <extuser0externa1.lab> To: Mail User 1 <uaerl8internal.lab> Date: 30 Jan 2024 12:24:54 +0100 Subject: Hello, World!
The quick brown tex lumped over the lazy doq.

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 "Subject" is part of the message header.
C. The"220 mx. internal, lab ESMTP Smtpd" message is part of the SMTP banner.
D. The "250 Message accepted for delivery" message is part of the message body.

Answer: B, C

Question: 15

Which license must you apply to a FortiMail device to enable the HA centralized monitoring features?

A. Cloud gateway license
B. Advanced Management and MSSP license
C. Office 365 protection license
D. Enterprise license

Answer: B

Question: 16

A FortiMail administrator is investigating a sudden increase in DSNs being delivered to their protected domain. After searching the logs, the administrator identities 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?

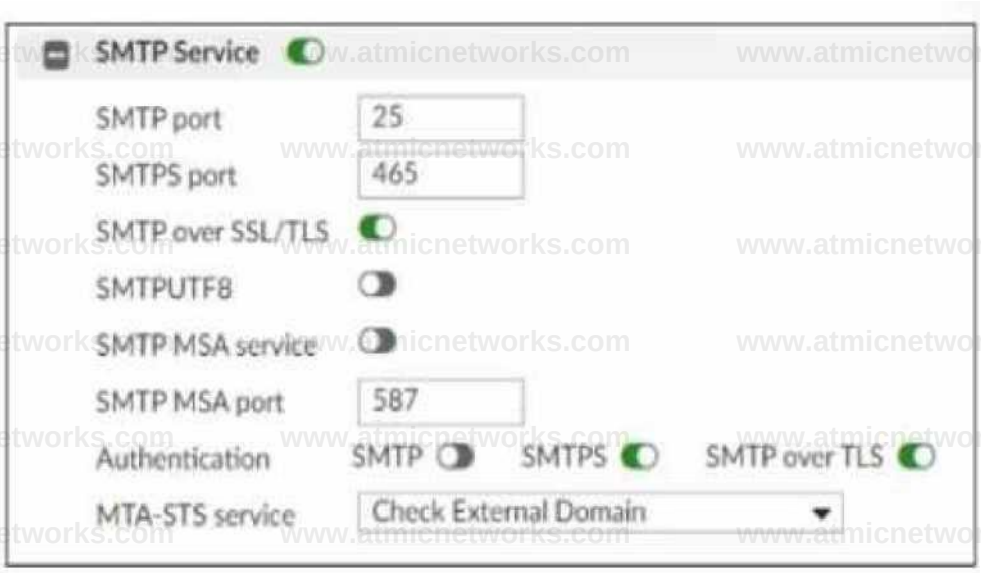
A. Spoofed header detection

B. Spam outbreak protection.
C. FortiGuard IP Reputation
D. Bounce address tag validation

Answer: D

Question: 17

Refer to the exhibit, which displays the Mail Settings page of a FortiMail device running in gateway mode.



In addition to selecting Check External Domain in the MTA-STS service field, what else must an administrator do to enable MTA-STS?

A. Enable MTA-STS in the associated TLS profile.
B. Enable SMTPUTF8 support in the mail server settings.
C. Enable secure authentication in the associated SMTP authentication profile.
D. Enable MTA-STS action in the appropriate inbound recipient policy.

Answer: C

Question: 18

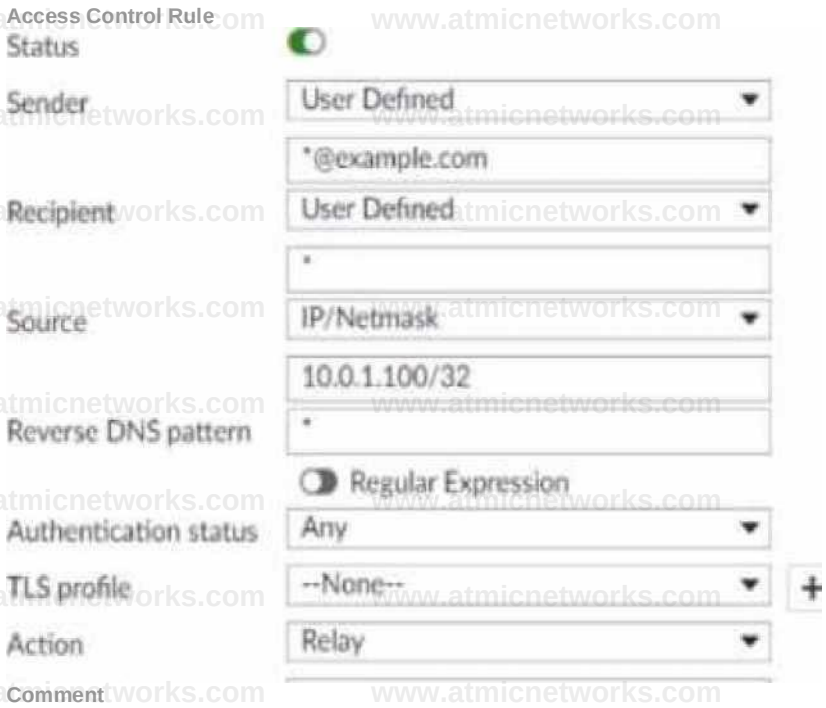
Which two factors are required for an active-active HA configuration of FortiMail in server mode? (Choose two.)

A. Devices must be deployed behind a load balancer.
B. Service monitoring must be configured for remote SMTP
C. A primary must be designated to initially process email.
D. Mail data must be stored on a NAS server.

Answer: AD

Question: 19

Refer to the exhibit, which displays an access control rule.



What are two expected behaviors for this access control rule? (Choose two.)

A. Email must originate from an example. com email address.
B. Senders must be authenticated to match this rule.

C. Email matching this rule will be relayed.

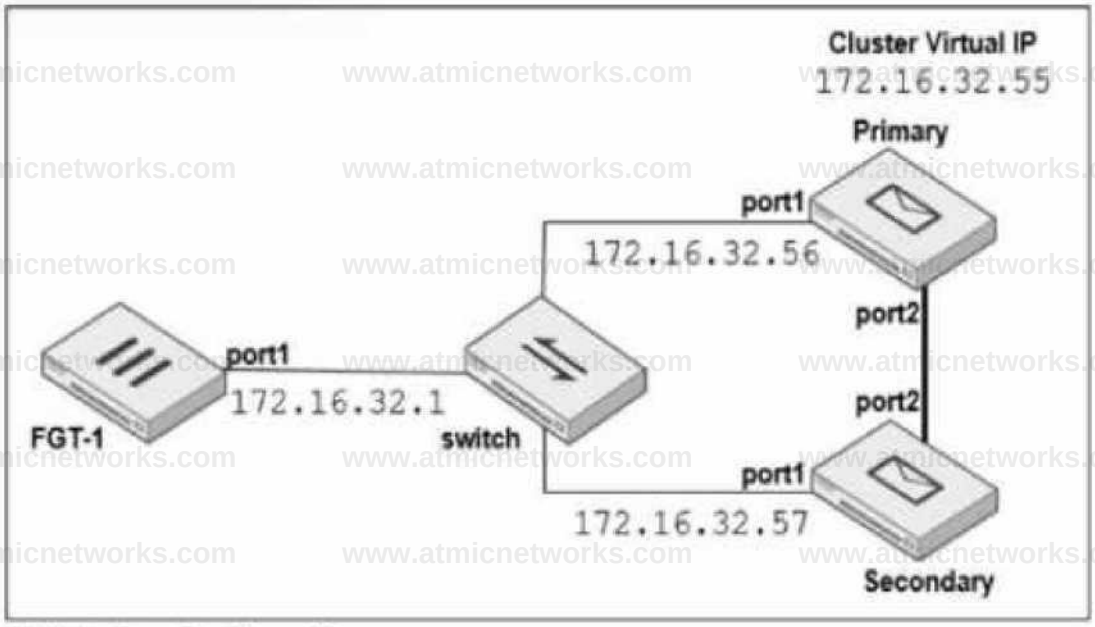
D. Emails must be sent from the 10.0.1.0/24 subnet.

Answer: A, B

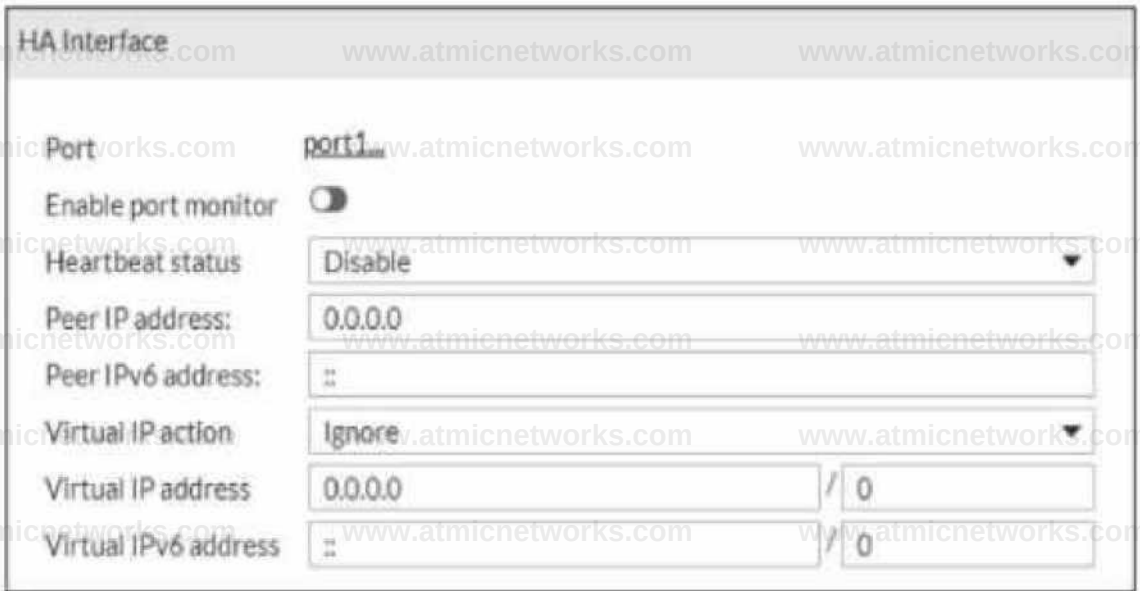
Question: 20

Reter to the exhibits.

Topology



HA Interface Configuration



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 primary FortiMail HA interface?

(Choose three.)

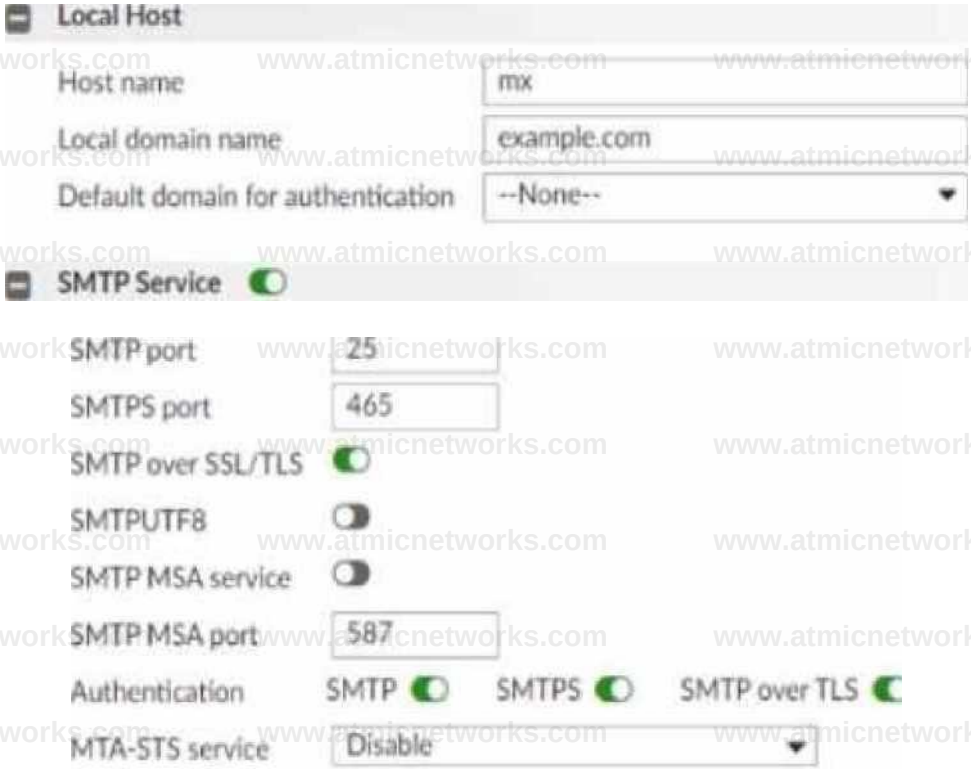
A. In the Heartbeat status drop-down list, select Primary
B. In the Virtual IP action drop-down list, select Use
C. In the Virtual IP address field, type 172.16.32.55/24
D. In the Peer IP address field, type 172.16.32.57
E. Disable Enable port monitor

Answer: B, C, D

Question: 21

Exhibit.

Mail Server settings



Refer to the exhibit, which shows the mail server settings of a FortiMail device. What are two ways this FortiMail device will handle connections? (Choose two.)

A. FortiMail will support the STARTTLS extension.
B. FortiMail will drop any inbound plaintext SMTP connection.
C. FortiMail will accept SMTPS connections.

D. FortiMail will enforce SMTPS on all outbound sessions.

Answer: A, C

Question: 22

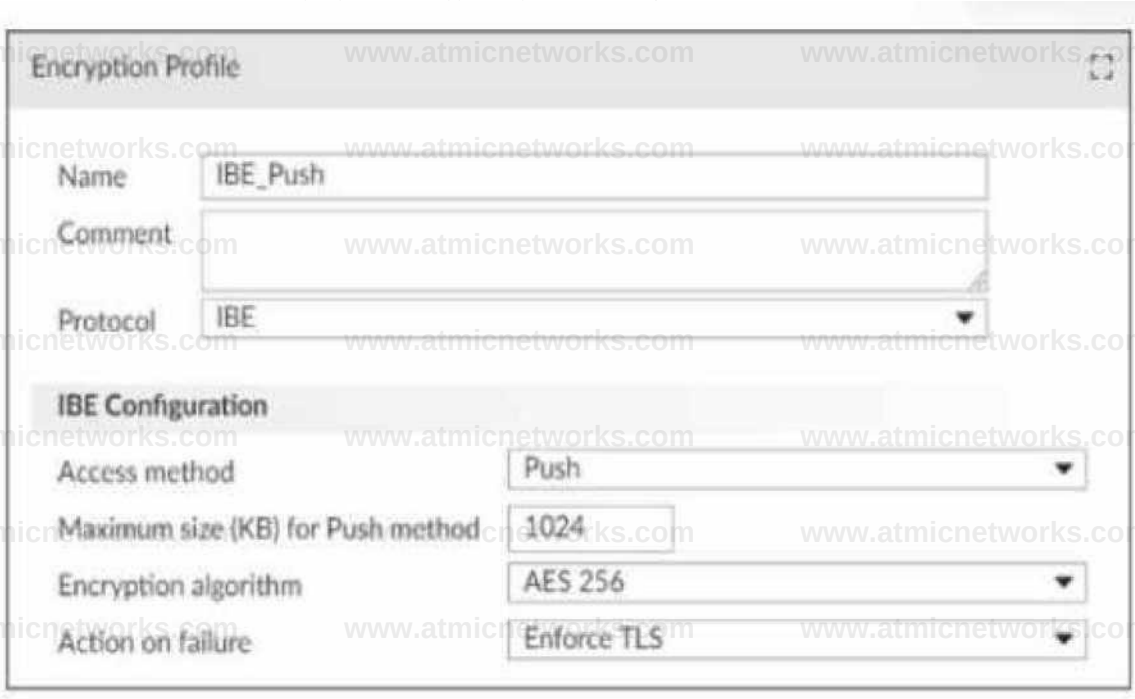
An organization has different groups of users with different needs in email functionality, such as address book access, mobile device access, email retention periods, and disk quotas. Which FortiMail feature specific to server mode can be used to accomplish this?

A. Access profiles
B. Domain-level service settings
C. Resource profiles.
D. Email group profiles

Answer: C

Question: 23

Refer to the exhibit, which displays an encryption profile configuration.



What happens if the attachment size of an IBE email exceeds 1024 KB?

A. Pull delivery will be used.
B. The email message will not be delivered.
C. OTLS will be used.

D. AES 256 will be used.

Answer: A

Question: 24

Refer to the exhibit.

Topology

Access Control Rule Access Control Rule

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

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.

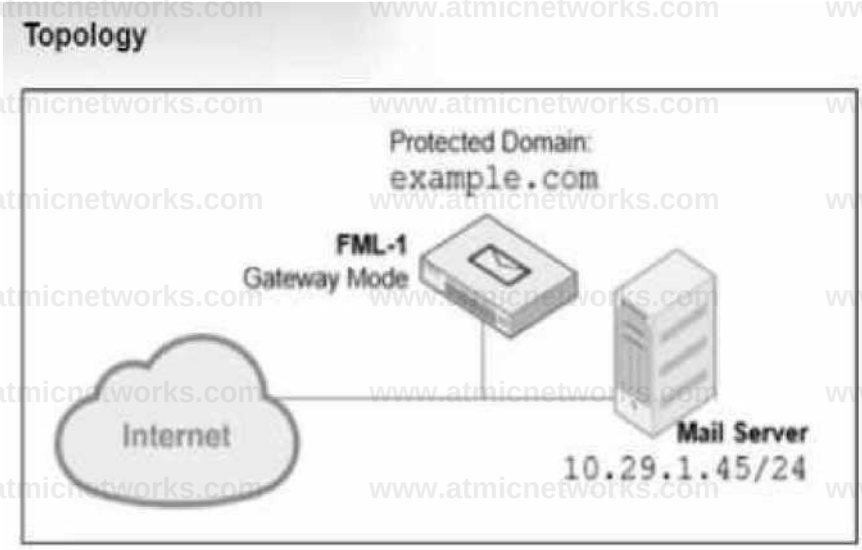
Which two access receive rule settings must the administrator configure? (Choose two.)

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: 25

Refer to the exhibit.



IP Policy

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.)

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: 26

A mail user wants the ability to subscribe or publish to and from their FortiMail calendar using Thunderbird as their mail user agent (MUA). What information does this mail user need from their webmail User Preferences section?

A. Free busy URL
B. Service URLs

C. Secondary account configurations

D. Message tags

Answer: C

Question: 27

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

A. DATA

B. VRFY

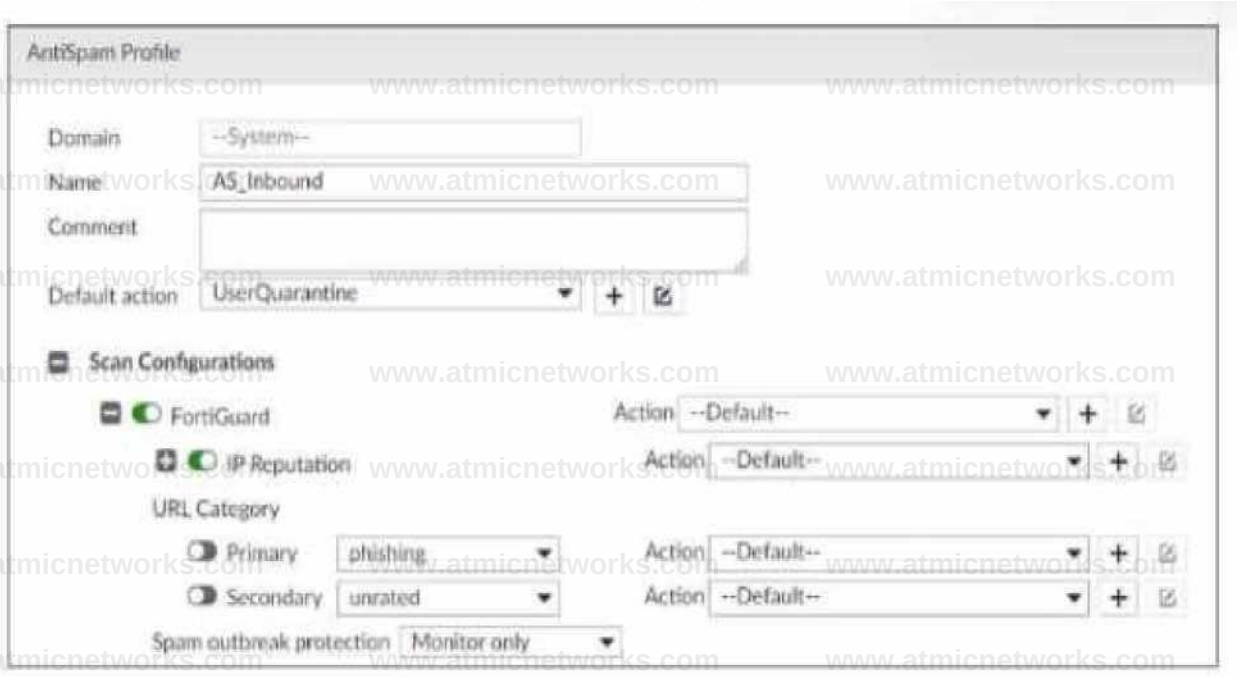
C. EHLO

D. HELO

Answer: A

Question: 28

Refer to the exhibit, which shows a partial antispam profile configuration.



What will happen to an email that triggers Spam outbreak protection?

A. The email is logged.

B. The email is rejected.

C. The email is held in a deferred queue for a period of time.

D. The email is marked as clean and released to the recipient.

Answer: A

Question: 29

When configuring a FortiMail HA group consisting of different models, which two statements are true? (Choose two.)

A. The most powerful model must be configured as the primary unit.
B. Group capacity is limited to the least powerful model.
C. All units must have the same firmware.
D. Configurations will not synchronize between different model types.

Answer: B, C

Question: 30

A FortiMail device is configured with the protected domain example. com.

It senders are not authenticated, which two envelope addresses will require an access receive rule? (Choose two.)

A. MALL FROM: mis@hosted.r.et RCPT TO: noc@example.com
B. MALL FROM: accounts@example.com RCPT TO: aales8biz.example.com
C. MALL FROM: support6example.org RCPT TO: marketing9exainple.com
D. MALL FROM: trainingeexample.com RCPT TO: students@external.org

Answer: B, C

Question: 31

In which two ways does a transparent mode FortiMail use the build-it MTA to process email? (Choose two.)

A. It can queue undeliverable messages and generate DSNs.

B. The built-in MTA must connect to an external relay host to deliver email.
C. MUAs must be configured to connect to the built-in MTA to send email.
D. It ignores the destination set by the sender and uses its own MX record lookup.

Answer: C, D

Question: 32

Refer to the exhibit.

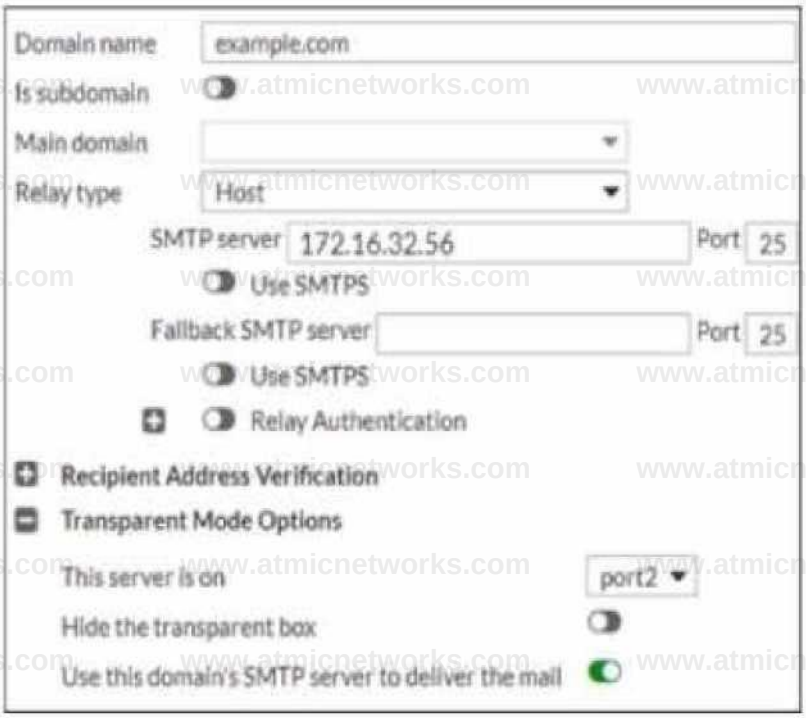
What does the Scan timeout value configure?

A. How long FortiMail will wait for a scan result from FortiSandbox B. How often the local scan results cache will expire on FortiMail C. How often FortiMail will query FortiSandbox for a scan result D. How long FortiMail will wait to send a file or URI to FortiSandbox

Answer: A

Question: 33

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



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

A. DESTINATION IP: 192.163.54.10 MAIL FROM: accour.t3@exaraple.com RCPT TO: saleseexamplc.com
B. BDESTINATION IP: 10.25.32.15 MAIL FROM: trainir.g@example.com RCPT TO: students@external.com
C. DESTINATION IP: 172.16.32.56 MAIL FROM: misfihosted.net RCPT TO: noc9example.com
D. DESTINATION IP: 172.16.32.56 MAIL FROM: support@example.com RCPT TO: marketingeaxampla.com

Answer: A, B

Question: 34

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

C 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	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...!

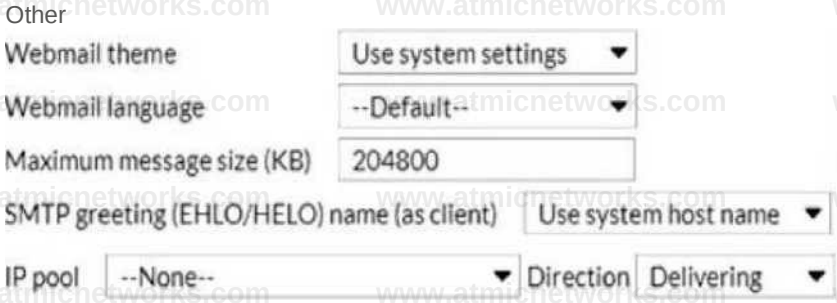
O UseSMTPS

Fallback SMTP server Port 25 ITest..,!

O UseSMTPS

O Relay Authentication

Domain Settings—Other



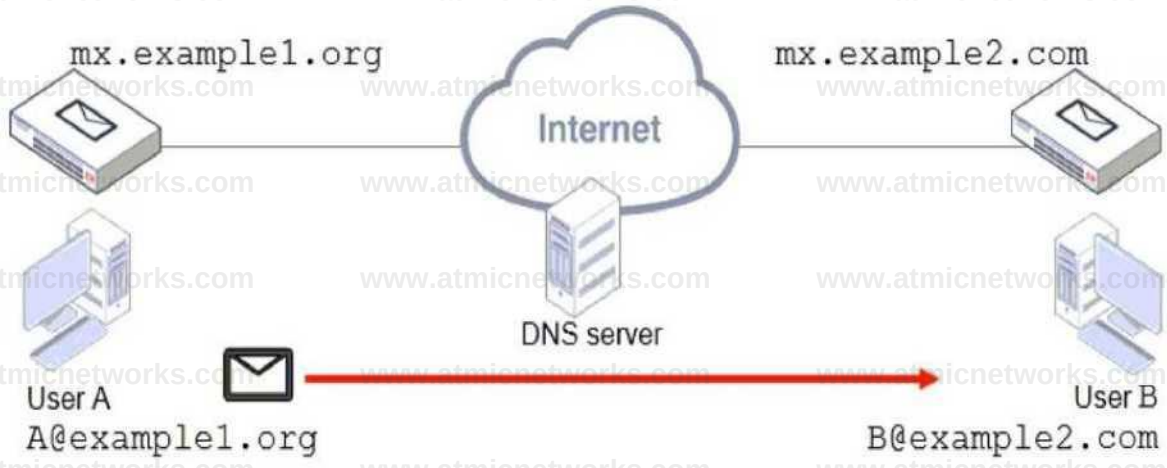
Which message size limit in KB will the FortiMail apply to outbound email?

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

Answer: D

Question: 35

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.

Answer: A, B

Question: 36

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

Answer: B, C

Question: 37

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

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

Answer: A

Question: 38

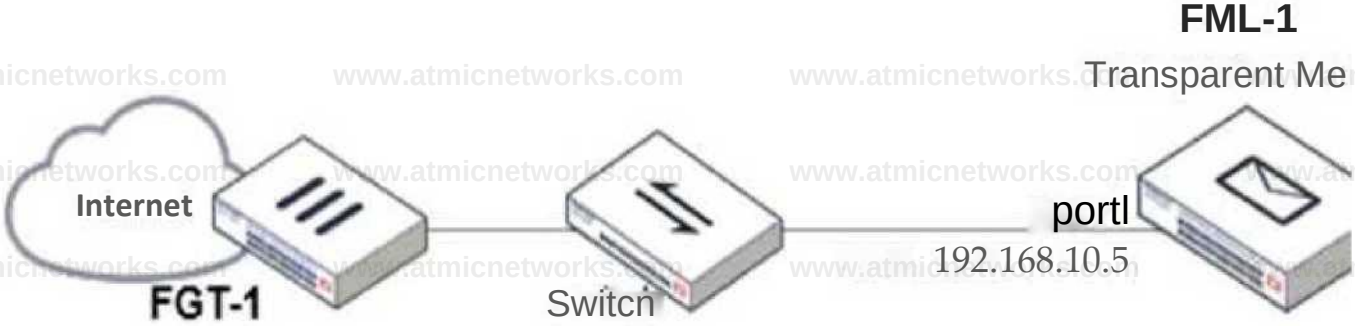
A FortiMail administrator is concerned about cyber criminals attempting to get sensitive information from employees using whaling phishing attacks. What option can the administrator configure to prevent these types of attacks?

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

Answer: A

Question: 39

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.

Answer: B, C

Question: 40

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

1** / I » Records per page: 50 * IBE domain: -All -

Enabled	Email	First Name	Last Name	Status
© CD	extuser@external.lab	Mail	User	Activated
	extuser2@external.lab			Pre-registered

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

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: 41

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

A. IP Policy configuration
B. Protected Domain configuration
C. Resource Profile configuration
D. Session Profile configuration

Answer: B, C

Question: 42

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

A. FortiToken
B. Certificate
C. SMS
D. Security question

Answer: D

Question: 43

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

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: 44

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

A. Outbound recipient policy
B. Inbound recipient policy
C. IP policy
D. Access delivery rule

Answer: C

Question: 45

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?

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

Answer: D

Question: 46

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

log Detain: 0200002400

Column	Content
*	1
Date	2021-06 24
Time	13 29 02 021
Gaisifier	Virus Signature
Disposition	Modify Subject Replace
From	extuser^external Jab
Header From	ex tuser ^external lab
To	user 1 Winter nal lab
Subject	Regist r at ion Informat ion enc losed
Message ID	20210624132901 1 SOOT lTNdO1852^e»ternal lab
Length	936
Session ID	1SOKT 18x002399 1SOKT IC 1002399
Client IP	10064 1 99
Location	ZZ (Reserved)
Client Name	extsrv
Direction	in
Policy ID	0 1 1 internal lab
Domain	internal lab
Destination IP	100 111
Source	External
Mailer	mt a
Virus	EICAR TEST FILE
Resolved	FORGED
Transfer Time	0051818

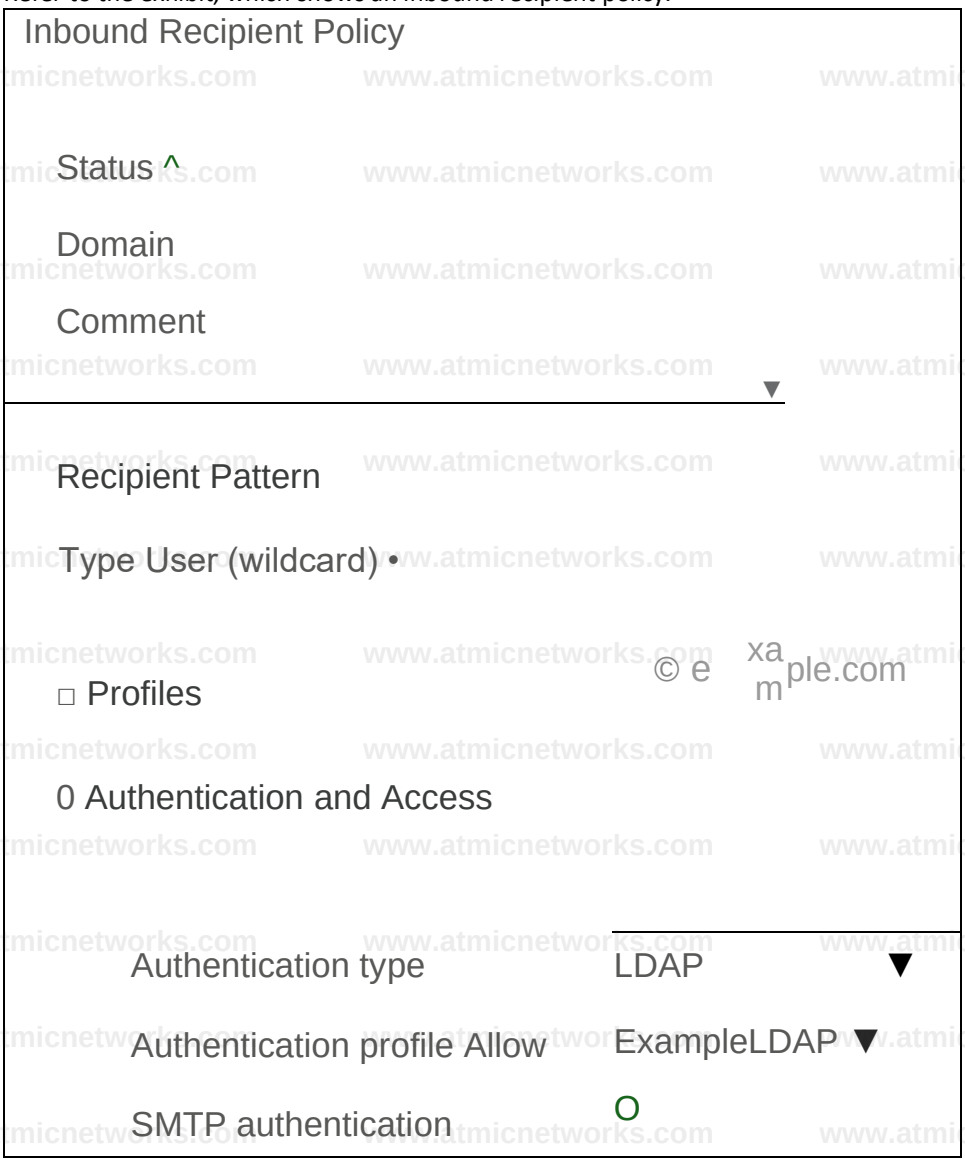
Which two actions did FortiMail take on this email message? (Choose two.)

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: 47

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



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?

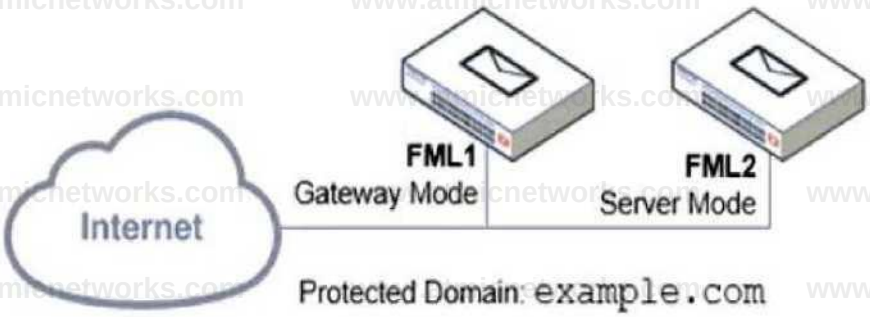
A. Move this incoming recipient policy to the top of the list.
B. Configure a matching IP policy with the exclusive flag enabled.
C. Configure an access delivery rule to enforce authentication.
D. Configure an access receive rule to verify authentication status.

Answer: D

Question: 48

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	
Maindomain	
Relay type	Host
SMTP server fml2.example.com O	Port 465 [Test..]
UseSMTPS	
Fallback SMTP server	Port 25
O UseSMTPS	

FML2 Configuration

O Local Host

Host name	FML2
Local domain name	example.com
Default domain for authentication	-None--

Q SMTP Service O

SMTP server port number	25
SMTPS server port number	465
SMTP over SSL/TLS	
SMTP MSA service	
SMTP MSA port number	587
Authentication	SMTP O SMTPS O SMTP over TLSC

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.

Answer: D

Question: 49

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

Answer: A, B

Question: 50

Which statement about how impersonation analysis identifies spoofed email addresses is correct?

A. It uses behavior analysis to detect spoofed addresses.
B. It uses DMARC validation to detect spoofed addresses.
C. It maps the display name to the correct recipient email address
D. It uses SPF validation to detect spoofed addresses.

Answer: B

Question: 51

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.

Answer: B, C

Question: 52

While reviewing logs, an administrator discovers that an incoming email was processed using policy IDs 0:4:9:INTERNAL.

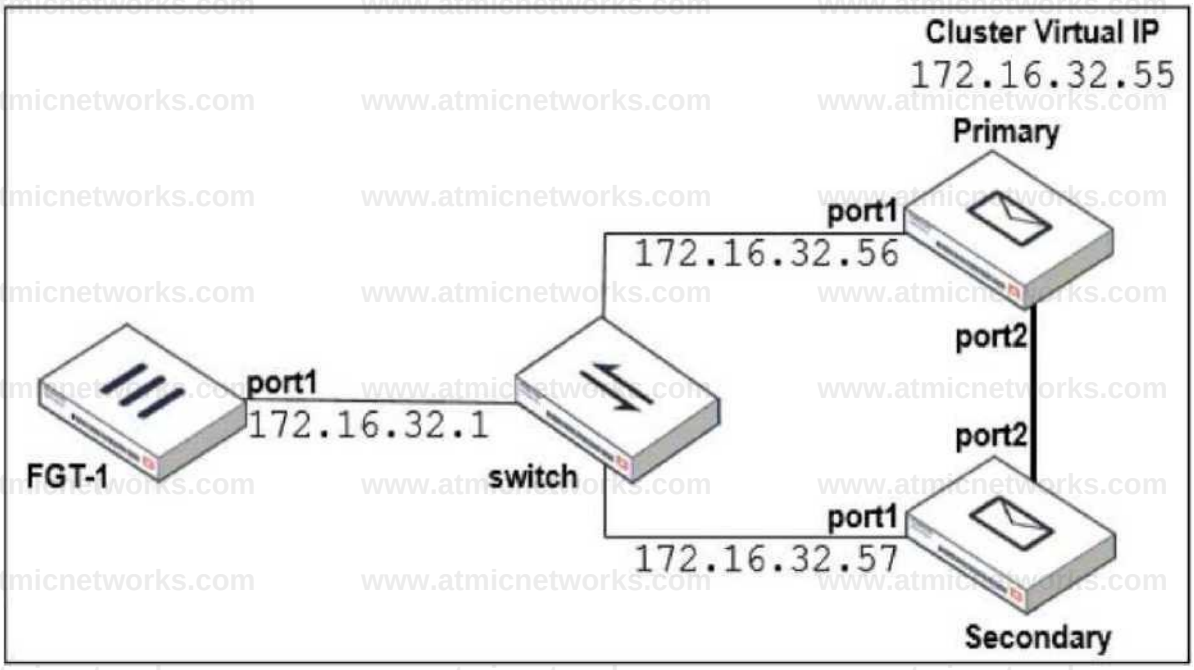
Which two statements describe what this policy ID means? (Choose two.)

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.

Answer: CD

Question: 53

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