

Fortinet

NSE6_FML-5.3.8 Exam

Fortinet FortiMail 5.3.8 Specialist Exam

Question: 1

Examine the FortiMail session profile and protected domain configuration shown in the exhibit; then answer the question below.

The screenshot shows the FortiMail configuration interface for a Session Profile. The 'SMTP Limits' section is expanded, showing the following settings:

| Setting | Value |
|--|-------|
| 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 |

Domains

Domain name:

Is subdomain

Main domain:

LDAP User Profile:

Advanced Settings

Mail Routing LDAP profile:

Remove received header of outgoing email

Webmail theme:

Webmail language:

Maximum message size(KB):

Automatically add new users to address book:

Which size limit will FortiMail apply to outbound email?

- A. 204800
- B. 51200
- C. 1024
- D. 10240

Answer: A

Question: 2

Examine the FortiMail antivirus action profile shown in the exhibit; then answer the question below.

AntiVirus **Action**

AntiVirus Action Profile

Domain:

Profile name:

Direction:

Tag email's subject line With value:

Insert new header With value:

Deliver to alternate host

► **BCC**

Replace infected/suspicious body or attachment(s)

Notify with profile

Reject

Discard

System quarantine to folder

► Rewrite recipient email address

Repackage email with customised content*

Repackage email with original text content*

**Original email will be wrapped as attachment*

What is the expected outcome if FortiMail applies this action profile to an email? (Choose two.)

- A. The sanitized email will be sent to the recipient's personal quarantine
- B. A replacement message will be added to the email
- C. Virus content will be removed from the email
- D. The administrator will be notified of the virus detection

Answer: B,C

Question: 3

Examine the FortiMail recipient-based policy shown in the exhibit; then answer the question below.

Policies

Recipient Based Policy

Enable

Direction: Incoming

Domain:

Comments:

Sender Pattern

Type: @

Recipient Pattern

Type: @ @

Profiles

Authentication and Access

Authentication type:

Authentication profile:

Use for SMTP authentication

Allow guaranteed email access through POP3

Allow guaranteed email access through webmail

After creating the policy, an administrator discovered that clients are able to send unauthenticated email using SMTP. What must be done to ensure clients cannot send unauthenticated email?

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

Answer: A