

KillTest

Higher Quality, Better Service!



Q&A

<http://www.killtest.com>

We offer free update service for one year.

Exam : NSE6_FML-5.3.8

Title : FortiMail 5.3.8 Specialist

Version : DEMO

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

The screenshot shows the 'Session Profile' configuration page in FortiMail. The 'Profile name' is 'Example_Session'. 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

The screenshot shows the 'Domains' configuration page in FortiMail. The 'Domain name' is 'example.com'. The 'Main domain' is 'jibon.remote'. The 'LDAP User Profile' is '--None--'. The 'Advanced Settings' section is expanded, showing the following settings:

Setting	Value
Mail Routing LDAP profile:	--None--
Remove received header of outgoing email	☐
Webmail theme:	Use system settings
Webmail language:	Use system settings
Maximum message size(KB):	204800
Automatically add new users to address book:	Domain

Which size limit will FortiMail apply to outbound email?

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

Answer: A

Explanation:

<http://kb.fortinet.com/kb/viewContent.do?externalId=FD31006&sliceId=1>

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

AntiVirus Action

AntiVirus Action Profile

Domain: internal.lab

Profile name: AC_Action

☐ 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 --None-- New... Edit...

☐ Reject

☐ Discard

☐ System quarantine to folder --None-- New... Edit...

☐ ► 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: BC

Explanation:

<https://www.fortinetguru.com/2016/04/configuring-profiles/14/>

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

The screenshot shows the 'Policies' configuration page in FortiMail. The 'Recipient Based Policy' is selected. The 'Enable' checkbox is checked. The 'Direction' is set to 'Incoming'. The 'Domain' is set to 'example.com'. The 'Comments' field is empty. The 'Sender Pattern' section has 'Type' set to 'User' and an empty pattern field. The 'Recipient Pattern' section has 'Type' set to 'User' and a pattern field containing 'example.com'. The 'Profiles' section is collapsed. The 'Authentication and Access' section is expanded, showing 'Authentication type' set to 'LDAP' and 'Authentication profile' set to 'ExampleLDAP'. There are 'New...' and 'Edit...' buttons next to the profile. The 'Use for SMTP authentication' checkbox is checked. The 'Allow quarantined email access through POP3' and 'Allow quarantined email access through webmail' checkboxes are unchecked.

After creating this 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

4. FortiMail is configured with the protected domain "example.com". Identify which of the following envelope addresses will require an access receive rule for unauthenticated senders? (Choose two)

- A. MAIL FROM: mis@hosted.net RCPT TO: noc@example.com
- B. MAIL FROM: training@external.org RCPT TO: students@external.org
- C. MAIL FROM: accnts@external.org RCPT TO: sales@external.org
- D. MAIL FROM: support@external.org RCPT TO: marketing@external.org

Answer: C

5.Examine the nslookup output shown in the exhibit; then answer the question below.



```
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
```

Identify which of the following statements is true regarding the example.com domain's MTAs. (Choose two.)

- A. External MTAs will send email to mx.example.com only if mx.hosted.com is unreachable.
- B. The primary MTA for the example.com domain is mx.hosted.com.
- C. The PriNS server should receive all email for the example.com domain.
- D. The higher preference value is used to load balance more email to the mx.example.com MTA.

Answer: CD