

NSE6_FML-6.0^{Q&As}

Fortinet NSE 6 - FortiMail 6.0

Pass Fortinet NSE6_FML-6.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse6_fml-6-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

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

Session

Session Profile

Profile name:

— **Connection Settings** —

— **Sender Reputation** —

— **Endpoint Reputation** —

— **Sender Validation** —

— **Session Settings** —

— **Unauthenticated Session Settings** —

▲ **SMTP Limits**

Restrict number of EHLO/HELOs per session to:

Restrict number of email per session to:

Restrict number of recipients per email to:

Cap message size (KB) at:

Cap header size (KB) at:

Maximum number of NOOPs allowed for each connection:

Maximum number of RSETs allowed for each connection:

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

Correct Answer: A

QUESTION 2

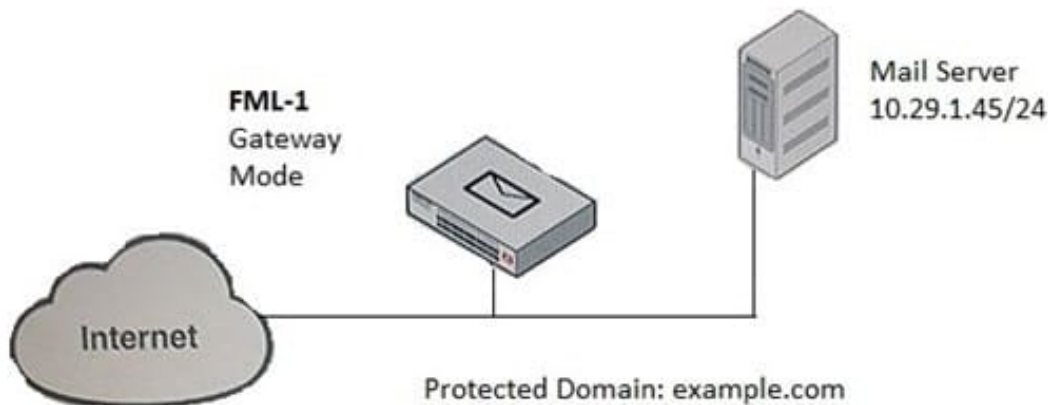
Which firmware upgrade method for an active-passive HA cluster ensures service outage is minimal and there are no unnecessary failovers?

- A. Upgrade the active unit, which will upgrade the standby unit automatically
- B. Upgrade both units at the same time
- C. Upgrade the standby unit, and then upgrade the active unit
- D. Break the cluster, upgrade the units independently, and then form the cluster again as quickly as possible

Correct Answer: D

QUESTION 3

Examine the FortiMail topology and IP-based policy shown in the exhibit; then answer the question below.



The screenshot shows the 'IP Policies' configuration page in FortiMail. The table below contains one policy entry:

Ena...	ID	Source	Destination	Session	AntiSpam	AntiVirus	Content	IP Pool	Excl...
<input checked="" type="checkbox"/>	1	0.0.0.0/0	0.0.0.0/0	Example_session					<input checked="" type="checkbox"/>

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 started filling up with undeliverable email. What changes should the administrator make to fix this issue? (Choose two.)

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

Correct Answer: BC

QUESTION 4

Examine the access receive rule shown in the exhibit; then answer the question below.

FortiMail

Access Control Rule

Enabled	<input checked="" type="checkbox"/>
Sender pattern:	<input type="text" value="User Defined"/> <input type="text" value="*@example.com"/> <input type="checkbox"/> Regular expression
Recipient pattern:	<input type="text" value="User Defined"/> <input type="text" value="*"/> <input type="checkbox"/> Regular expression
Sender IP/netmask:	<input type="text" value="User Defined"/> <input type="text" value="10.0.1.100"/> / <input type="text" value="32"/>
Reverse DNS pattern:	<input type="text" value="*"/> <input type="checkbox"/> Regular expression
Authentication status:	<input type="text" value="Any"/>
TLS profile:	<input type="text" value="--None--"/> <input type="button" value="New..."/> <input type="button" value="Edit.."/>
Action:	<input type="text" value="Relay"/>
Comments:	<input type="text"/>

Which of the following statements are true? (Choose two.)

- A. Email from any host in the 10.0.1.0/24 subnet can match this rule
- B. Senders must be authenticated to match this rule
- C. Email matching this rule will be relayed
- D. Email must originate from an example.com email address to match this rule

Correct Answer: CD

QUESTION 5

What are the configuration steps to enable DKIM signing for outbound messages on FortiMail? (Choose three.)

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

Correct Answer: ACE

[NSE6 FML-6.0 PDF Dumps](#) [NSE6 FML-6.0 VCE Dumps](#)

[NSE6 FML-6.0 Exam Questions](#)