PassQueen
a.k.a dumpsqueen.com

# Fortinet NSE 6 - FortiMail 6.4

## Fortinet NSE6_FML-6.4

**Version Demo**

**Total Demo Questions: 7**

**Total Premium Questions: 79**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Deployment and configuration | 20 |
| Topic 2, Administration | 11 |
| Topic 3, Authentication | 11 |
| Topic 4, Security | 37 |
| Total | 79 |

QUESTION NO: 1

Which two actions can FortiMail apply when antivirus scanning detects a virus in an email message? (Choose two.)

**A.** Reject the message

**B.** Quarantine the message

**C.** Sign the message with DKIM

**D.** Verify the recipient address

**ANSWER: A B**

**Explanation:**

FortiMail can **reject** a virus-infected message during SMTP processing, preventing the message from being accepted for delivery. It can also **quarantine** the message for administrator review, allowing security staff to retain and examine the detection without delivering it to the recipient.

These actions are configured through the applicable antivirus and action-profile settings. FortiMail does not use DKIM signing or recipient verification as actions for a detected virus. Fortinet documents antivirus processing in the FortiMail 6.4 Administration Guide.

**QUESTION NO: 2**

Examine the message column of a log cross search result of an inbound email shown in the exhibit; then answer the question below


Based on logs, which of the following statements are true? (Choose two.)

**A.** The FortiMail is experiencing issues delivering the email to the back-end mail server

**B.** The logs were generated by a server mode FortiMail

**C.** The logs were generated by a gateway or transparent mode FortiMail

**D.** The FortiMail is experiencing issues accepting the connection from the remote sender

**ANSWER: A C**

**Explanation:**

The correct conclusions are that FortiMail is experiencing issues delivering the email to the back-end mail server and that the logs were generated by a gateway or transparent mode FortiMail. The log message shows that FortiMail has already accepted and processed the inbound message, then encountered a delivery problem while attempting SMTP communication with the configured downstream mail server. This places the failure on the delivery leg between FortiMail and the protected mail infrastructure, rather than on the initial SMTP connection from the external sender.

Gateway mode is designed to inspect mail and relay accepted messages to one or more protected downstream mail servers. Transparent mode similarly operates inline for mail inspection and forwarding, with delivery continuing toward the destination mail server. Consequently, a log entry identifying a back-end mail-server delivery issue is consistent with these deployment modes and their role as a mail-security relay in front of the organization's mail system. Fortinet's FortiMail documentation

describes these operating modes and the related mail-flow behavior in the FortiMail 6.4 Administration Guide and the Operating modes documentation.

## QUESTION NO: 3

Refer to the exhibit.


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 account has been de-activated, and the user must register again the next time they receive an IBE email.

**C.** The user was registered by an administrator in anticipation of IBE participation.

**D.** The user has completed the IBE registration process, but has not yet accessed their IBE email.

## ANSWER: A

**Explanation:**

The user has received an IBE notification email, but has not accessed the HTTPS URL or attachment yet. In FortiMail Identity-Based Encryption, FortiMail automatically creates a pre-registered user record when it sends protected content to a recipient who is not already registered. The notification message gives that recipient access to the protected message, typically through the HTTPS webmail URL or, depending on the delivery method, an attached encrypted package. At this stage, FortiMail has an account entry for the recipient but the recipient has not completed the first-use interaction needed to establish their IBE credentials and access the protected content. Therefore, the pre-registered state represents a pending recipient who has been sent IBE-protected mail and is awaiting initial access and registration. This status lets administrators identify recipients for whom IBE delivery has begun before the recipient completes the registration workflow. FortiMail documents IBE user management, including the behavior of automatically created pre-registered users, in its IBE user configuration guidance. See the FortiMail 6.4 Administration Guide: Configuring IBE users and the FortiMail 6.4 Administration Guide.

## QUESTION NO: 4

An administrator wants to block executable attachments while allowing common document attachments to be delivered.

Which FortiMail content-profile feature should the administrator configure?

**A.** File filter

**B.** URI filter

**C.** IP reputation

**D.** Impersonation analysis

## ANSWER: A

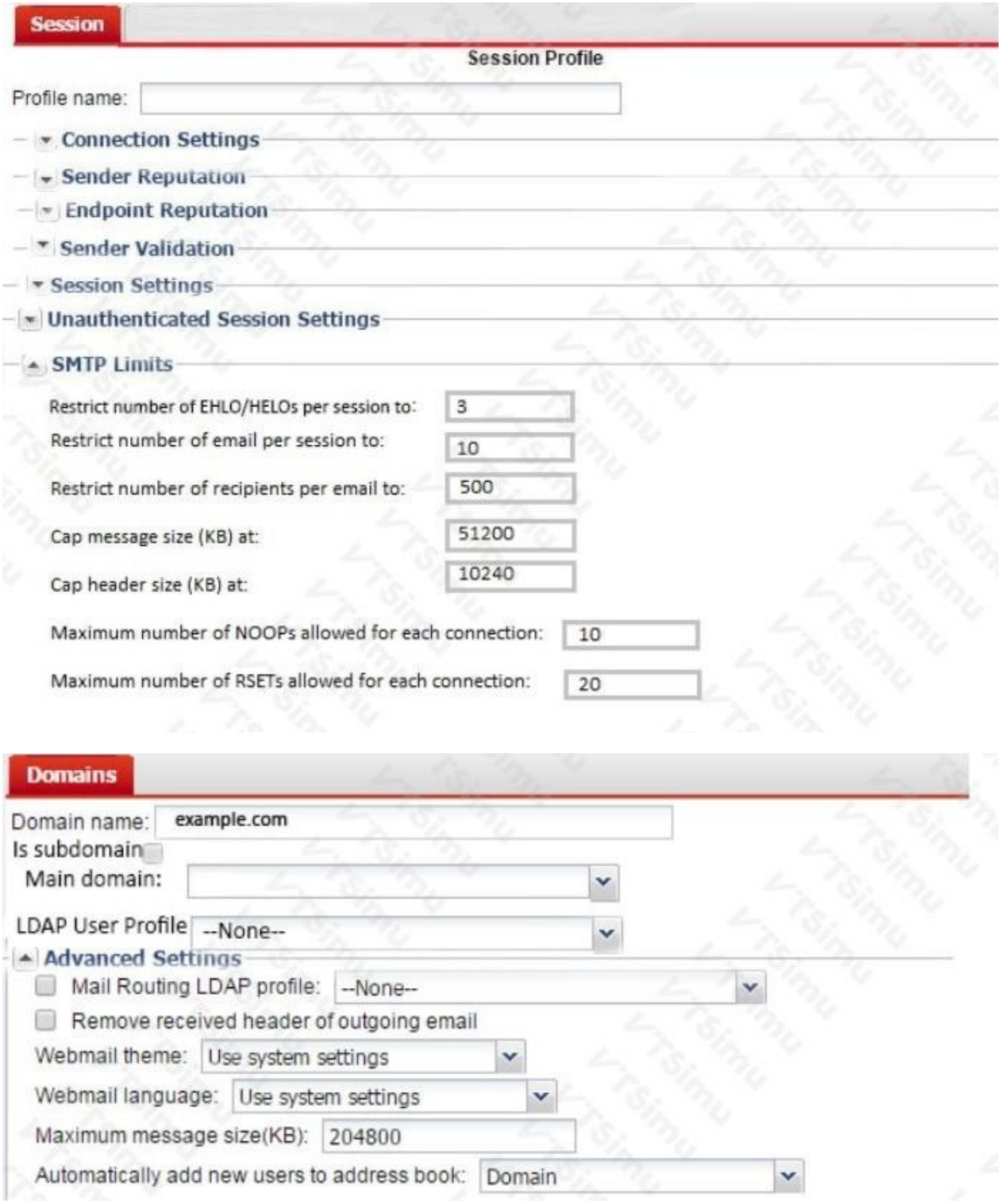
**Explanation:**

**File filter** is used to inspect message attachments and apply actions according to file characteristics, such as file name, extension, or detected file type. The administrator can create rules that block executable files while allowing approved document types.

File filtering is configured in a content profile and can be applied by a matching mail policy. It is distinct from antivirus scanning, which detects known or suspicious malware, and from content disarm and reconstruction, which sanitizes supported document formats. See the FortiMail 6.4 Administration Guide.

## QUESTION NO: 5

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



Which size limit will FortiMail apply to outbound email?

**A.** 204800

**B.** 51200

**C.** 1024

**D.** 10240

**ANSWER: B**

**Explanation:**

FortiMail will apply the **51200** size limit to outbound email because outbound SMTP sessions are governed by the matching session profile. A session profile is applied according to the SMTP connection and its configured direction, so its maximum message-size setting controls the messages accepted and processed for the outbound delivery session. In the exhibited configuration, the applicable outbound session profile specifies a maximum message size of 51200 KB.

The protected-domain maximum message size does not replace this outbound session control. Protected-domain settings are used to define how FortiMail handles mail addressed to a protected recipient domain, which is an inbound-mail context. For outbound mail, FortiMail evaluates the sender-side SMTP session and enforces the limit configured in the outbound session profile. This distinction is important when troubleshooting message-size rejections: administrators should identify the mail direction first, then inspect the session profile selected for that SMTP connection.

Fortinet documents the message-size behavior and the protected-domain scope in its FortiMail knowledge base article FD31006. Configuration concepts for SMTP sessions and profiles are also covered in the FortiMail 6.4 Administration Guide.

**QUESTION NO: 6**

Which two CLI commands, if executed, will erase all data on the log disk partition? (Choose two.)

**A.** execute formatmaildisk

**B.** execute formatmaildisk_backup

**C.** execute formatlogdisk

**D.** execute partitionlogdisk 40

**ANSWER: C D**

**Explanation:**

`execute formatlogdisk` is correct because it explicitly formats FortiMail's log-disk partition. Formatting removes the existing log-disk contents, including stored log data and other information maintained on that partition. This operation is intended for situations in which an administrator needs to clear the log storage before reusing it, and it should be performed only with appropriate backup and retention considerations.

`execute partitionlogdisk 40` is also correct. The `execute partitionlogdisk` command changes the allocation of disk space used for logging; the numeric value specifies the percentage assigned to the log disk. Changing this allocation requires the appliance to repartition and reformat the log-disk area, which erases the data that was stored on that partition. The value `40` is a valid example of such a new allocation and therefore invokes the data-erasing repartitioning process.

Fortinet documents the formatting behavior of the log-disk command in the FortiMail CLI reference: FortiMail CLI Reference: formatlogdisk. Fortinet's product documentation portal also provides the applicable FortiMail 6.4 documentation set: FortiMail 6.4 documentation.

**QUESTION NO: 7**

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

**A.** Break the cluster, upgrade the units independently, and then form the cluster

**B.** Upgrade both units at the same time

**C.** Upgrade the standby unit, and then upgrade the active unit

**D.** Upgrade the active unit, which will upgrade the standby unit automatically

**ANSWER: B**

**Explanation:**

Upgrade both units at the same time is the appropriate method when the priority is the shortest planned service interruption without unnecessary HA role changes. In an active-passive FortiMail cluster, upgrading the cluster members together deliberately treats the firmware installation as one maintenance event. Both appliances restart into the same supported firmware level, rather than requiring the standby appliance to assume the active role while its peer is upgraded. This prevents an avoidable active/standby transition and avoids operating the cluster temporarily with members on different firmware versions.

A brief interruption is expected because the active appliance must reboot, but it is a single, predictable outage window. Administrators should perform the work during a maintenance period, verify that configuration and message queues are healthy beforehand, and confirm that both members return to the expected HA state after the upgrade. Fortinet's FortiMail HA firmware-upgrade guidance specifically documents the process and considerations for upgrading HA units. See the FortiMail 6.4 Administration Guide: Upgrading firmware on HA units and the FortiMail 6.4 Administration Guide.