VCE & PDF
Pass4itSure.com

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.pass4itsure.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

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

A. execute formatmaildisk

B. execute formatmaildisk_backup

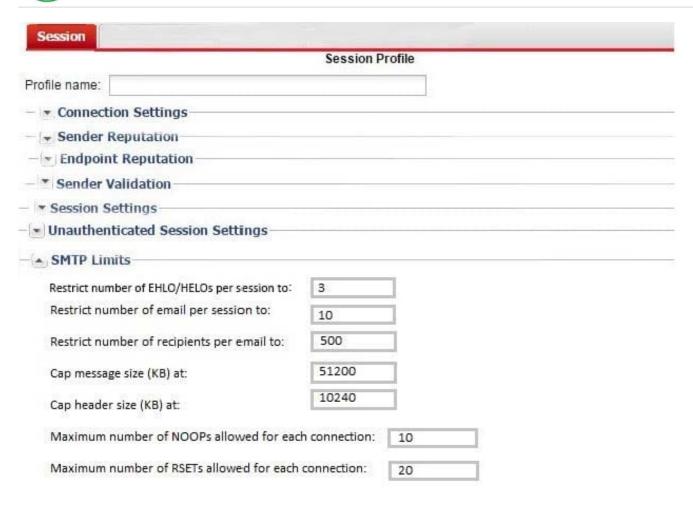C. execute formatlogdisk

D. execute partitionlogdisk 40

Correct Answer: CD

QUESTION 2

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:	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: example.com
Is subdomain ☐
Main domain: [▾]

LDAP User Profile [--None-- ▾]
— ▲ **Advanced Settings**
☐ 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

Correct Answer: A

QUESTION 3

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

A. MAIL FROM: training@external.org RCPT TO: students@external.org

B. MAIL FROM: support@example.com PCPT TO: marketing@example.com
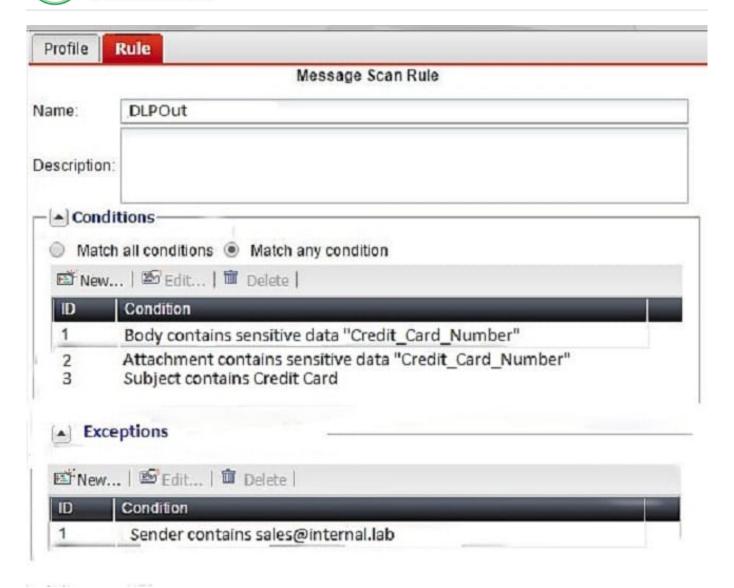
C. MAIL FROM: mis@hosted.net RCPT TO: noc@example.com

D. MAIL FROM: accounts@example.com RCPT TO: sales@external.org

Correct Answer: BD

QUESTION 4

Examine the FortiMail DLP scan rule shown in the exhibit; then answer the question below.

| Profile | Rule |

Message Scan Rule

Name: DLPOut

Description:

Conditions

○ Match all conditions ● Match any condition

New... | Edit... | Delete |

ID	Condition
1	Body contains sensitive data "Credit_Card_Number"
2	Attachment contains sensitive data "Credit_Card_Number"
3	Subject contains Credit Card

Exceptions

New... | Edit... | Delete |

ID	Condition
1	Sender contains sales@internal.lab

Which of the following statements is true regarding this configuration? (Choose two.)

A. An email message containing the words "Credit Card" in the subject will trigger this scan rule

B. If an email is sent from sales@internal.lab the action will be applied without matching any conditions

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

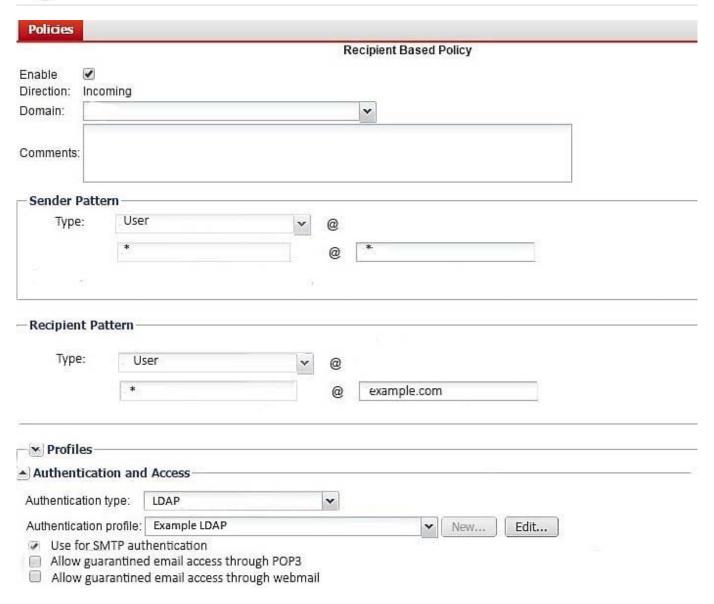D. An email must contain credit card numbers in the body, attachment, and subject to trigger this scan rule

Correct Answer: AC

QUESTION 5

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: [User ▼] @
[*] @ [*.]

Recipient Pattern

Type: [User ▼] @
[*] @ [example.com]

▼ Profiles

▲ Authentication and Access

Authentication type: [LDAP ▼]
Authentication profile: [Example LDAP ▼] [New...] [Edit...]
☑ 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

Correct Answer: A